ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Βιβλιογραφική μελέτη και εφαρμογή εργαλείων προσομοίωσης δικτυακής κίνησης σε 5G δίκτυα

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εκπόνηση: Γιώργος Κ. Νάνος
Επιβλέπων: Δημήτριος Ασκούνης,Καθηγητής
Τομέας Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων, ΕΜΠ

Αθήνα, Ιούνιος 2025

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Βιβλιογραφική μελέτη και εφαρμογή εργαλείων προσομοίωσης δικτυακής κίνησης σε 5G δίκτυα

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εκπόνηση: Γιώργος Κ. Νάνος
Επιβλέπων: Δημήτριος Ασκούνης,Καθηγητής
Τομέας Ηλεκτρικών Βιομηχανικών Διατάξεων και Συστημάτων Αποφάσεων, ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 26η Ιουνίου 2025.

.....	.....	.....
Ιωάννης Ψαρράς	Δημήτριος Ασκούνης	Ευάγγελος Μαρινάκης
Καθηγητής Ε.Μ.Π	Καθηγητής Ε.Μ.Π	Επίκουρος Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2025

.....
Γιώργος Κ. Νάνος
Κάτοχος Μεταπτυχιακού Προγράμματος “Τεχνο-οικονομικά Συστήματα” της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών Ε.Μ.Π.

Περίληψη

Η ραγδαία εξάπλωση των δικτύων κινητής τηλεφωνίας πέμπτης γενιάς (5G) συνοδεύεται από αυξανόμενες απαιτήσεις σε επίπεδο επιδόσεων, αξιοπιστίας, ασφάλειας και προσαρμοστικότητας, αναδεικνύοντας τη σημασία της ύπαρξης εξελιγμένων εργαλείων δημιουργίας και προσομοίωσης δικτυακής κίνησης για σκοπούς αξιολόγησης και ανάλυσης. Στο πλαίσιο της παρούσας διατριβής, πραγματοποιείται εκτεταμένη βιβλιογραφική έρευνα γύρω από την εξέλιξη των τεχνολογιών που συνθέτουν τον χώρο της παραγωγής δικτυακής κίνησης, με έμφαση στο περιβάλλον των 5G αρχιτεκτονικών. Η ανάλυση περιλαμβάνει θεμελιώδεις αρχές του 5G (όπως οι κατηγορίες eMBB, URLLC, mMTC), καθώς και τις προκλήσεις που αυτές εισάγουν στη δημιουργία ρεαλιστικών σεναρίων δικτύωσης. Ακολούθως, γίνεται προσδιορισμός και ανάλυση των κυριότερων εργαλείων και τεχνολογιών που είναι διαθέσιμα για την παραγωγή, ανάλυση και αξιολόγηση κίνησης σε σύγχρονα δίκτυα. Τα εργαλεία αυτά περιλαμβάνουν open-source πλατφόρμες όπως Open5GS, UERANSIM, srsRAN, καθώς και traffic generators και analyzers όπως TRex, Iperf3, D-ITG, Scapy και Wireshark. Για την αντικειμενική σύγκριση των εργαλείων, αναπτύχθηκε μια πολυκριτηριακή ανάλυση αποφάσεων (MCDA), με χρήση δέκα τεχνικών και ποιοτικών κριτηρίων, όπως η ικανότητα δημιουργίας 5G κίνησης, η υποστήριξη ασφάλειας, η δυνατότητα εικονικοποίησης και η τεκμηρίωση. Μέσω της ανάλυσης αυτής, επιλέχθηκε ο συνδυασμός του Open5GS (ως πυρήνας 5G) και του UERANSIM (ως προσομοιωτή UE/gNB) ως η πλέον κατάλληλη λύση για τη δημιουργία μίας πλήρως λειτουργικής δοκιμαστικής πλατφόρμας (testbed). Η επιλογή αυτή επιβεβαιώθηκε και πειραματικά μέσω της υλοποίησης ενός proof of concept σε περιβάλλον εικονικής μηχανής (VM). Στο πλαίσιο των πειραμάτων, υλοποιήθηκαν σενάρια κανονικής και κακόβουλης κίνησης – μεταξύ αυτών HTTP και UDP floods – με στόχο την παρακολούθηση της συμπεριφοράς του δικτύου και τη δυνατότητα χρήσης του testbed για μελλοντική ενσωμάτωση μηχανισμών ασφαλείας, όπως συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS). Τα αποτελέσματα απέδειξαν τη λειτουργικότητα και την προσαρμοστικότητα της πλατφόρμας, ενώ η μεθοδολογία της διατριβής προσφέρει σημαντική προστιθέμενη αξία ως ακαδημαϊκό υπόβαθρο για μελλοντικές εφαρμογές σε δοκιμές και έρευνα σχετικές με την ασφάλεια και την απόδοση δικτύων 5G.

Λέξεις-κλειδιά

5G Δίκτυα,

Προσομοίωση Δικτυακής Κίνησης,

Δοκιμαστική Πλατφόρμα,

Πολυκριτηριακή Ανάλυση,

Εργαλεία Ανοιχτού Κώδικα

Abstract

The rapid evolution of fifth-generation (5G) mobile networks has introduced new challenges regarding performance, reliability, and security, emphasizing the need for advanced tools to generate and simulate network traffic for evaluation and testing purposes. This thesis presents an extensive literature review on the technological evolution of traffic generation and simulation systems, focusing on 5G network environments and architectural requirements such as eMBB, URLLC, and mMTC. A broad survey of available tools and platforms is conducted, including open-source solutions such as Open5GS, UERANSIM, srsRAN, and traffic generation frameworks like TRex, Iperf3, D-ITG, Scapy, and Wireshark. A multi-criteria decision analysis (MCDA) framework was developed to compare these tools using ten technical and qualitative criteria, such as 5G traffic emulation capabilities, scalability, virtualization support, and documentation quality. Based on this evaluation, the Open5GS and UERANSIM combination was selected as the most suitable for building a functional and flexible 5G testbed. A proof-of-concept testbed was then implemented in a virtual machine (VM), simulating both benign and malicious traffic scenarios—including HTTP and UDP flood attacks—to assess the system's behavior and its suitability for future integration of security mechanisms such as intrusion detection or prevention systems (IDS/IPS). The results demonstrate the feasibility, adaptability, and effectiveness of the proposed testbed, while the methodology offers significant academic value as a foundational framework for future research and testing in the domain of 5G performance and security evaluation

Keywords

5G Networks,

Network Traffic Simulation,

Testbed,

Multi-Criteria Decision Analysis (MCDA),

Open Source Tools

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους διδάκτωρ Στέφανο Πάλμο και υποψήφιο διδάκτων Σωτήρη Πελέκη για την υπομονή, την αμεσότητα και τη διατήρηση της ορμής που επέδειξαν σε όλο το διάστημα συγγραφής αυτού του κειμένου.

Θα ήθελα να ευχαριστήσω τη σύντροφο μου Λ. και τα ζωάκια μας Α. και Φ. για τη συνεχόμενη στήριξη και την αδιάκοπη αγάπη.

Θα ήθελα να ευχαριστήσω τη μητέρα μου Μ. και τον αδερφό μου Κ. που στέκονταν πάντα δίπλα μου και χαίρονται στις χαρές μου.

Θα ήθελα επίσης να ευχαριστήσω όλο τον κόσμο του ΕΜΠ καθώς η ποικιλομορφία των χαρακτήρων, το ελεύθερο πνεύμα και το όραμα για έναν καλύτερο κόσμο με τα οποία ήρθα σε άμεση επαφή έχουν επαναπροσδιορίσει τα θεμέλια της προσωπικότητας μου προσφέροντας μου την πιο μεταμορφωτική εμπειρία της ζωής μου.

Περιεχόμενα

1. Εισαγωγή

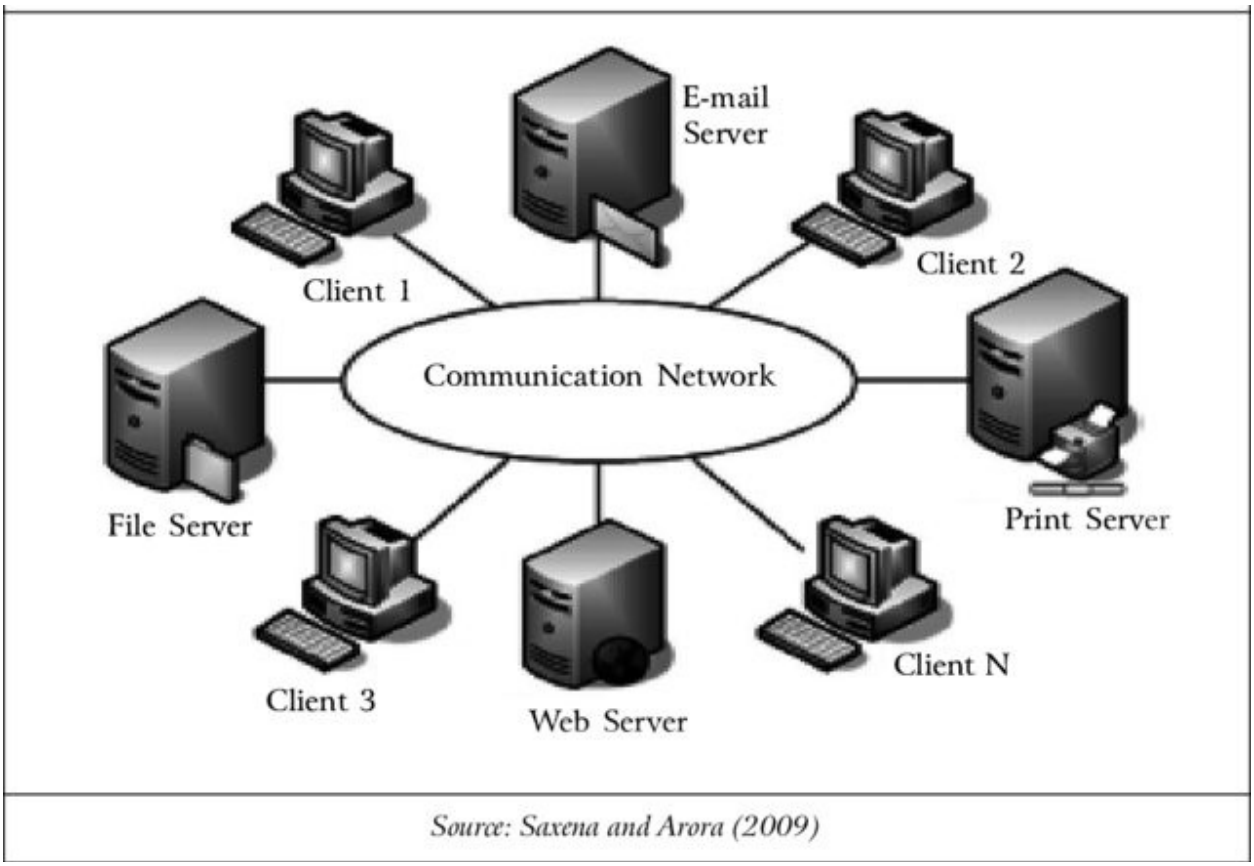
Το πέμπτης γενιάς δίκτυο κινητών επικοινωνιών (5G) εισάγει μια νέα εποχή συνδεσιμότητας, παρέχοντας εξαιρετικά υψηλές ταχύτητες μεταφοράς δεδομένων, χαμηλή καθυστέρηση και μαζική ταυτόχρονη πρόσβαση συσκευών. Αυτές οι ιδιότητες επιτρέπουν πρωτοποριακές εφαρμογές, από επαυξημένη/εικονική πραγματικότητα μέχρι αυτόνομα οχήματα και έξυπνες πόλεις. Ωστόσο, η **αυξημένη πολυπλοκότητα και δυναμική φύση των δικτύων 5G δημιουργεί αντίστοιχα μεγάλες προκλήσεις στην ασφάλεια**. Τα παραδοσιακά Συστήματα Ανίχνευσης Εισβολών (IDS) δυσκολεύονται να ανταποκριθούν στο εξελισσόμενο τοπίο απειλών, λόγω του τεράστιου αριθμού συνδεδεμένων συσκευών, του εκρηκτικού όγκου κίνησης δεδομένων και των δυναμικών αρχιτεκτονικών που χαρακτηρίζουν τα δίκτυα 5G [1]Συνεπώς, το **πεδίο απειλών** σε 5G διευρύνεται και απαιτεί **ισχυρά, προδραστικά και αυτοπροσαρμοζόμενα IDS δικτύου (NIDS)**, ικανά να αναγνωρίζουν ανωμαλίες σε πραγματικό χρόνο. Επιπλέον, επειδή οι υπηρεσίες 5G διεισδύουν σε κρίσιμες υποδομές (π.χ. έξυπνα δίκτυα, βιομηχανικό IoT), **κακόβουλη δικτυακή κίνηση σε 5G δύναται να διαταράξει υπηρεσίες και να διακυβεύσει ευαίσθητα δεδομένα**, με σοβαρές συνέπειες για χρήστες και οργανισμούς[2]. Σε αυτό το πλαίσιο, καθίσταται επιτακτική η ανάγκη για νέες προσεγγίσεις ασφάλειας και ειδικότερα για αποτελεσματικά IDS, προκειμένου να προστατευτεί η ακεραιότητα και η διαθεσιμότητα των δικτύων 5G.

1.1 Υπόβαθρο

1.1.1 Επισκόπηση Δικτύων Υπολογιστών και Παραγωγή Κίνησης

Τα δίκτυα υπολογιστών αποτελούν τη βάση της σύγχρονης επικοινωνίας, επιτρέποντας τη διασύνδεση υπολογιστικών συστημάτων και συσκευών για την ανταλλαγή δεδομένων. **Αρχιτεκτονικά, ένα τυπικό δίκτυο** οργανώνεται σε στρώματα (μοντέλο OSI/Διαδικτύου), όπου κάθε στρώμα επιτελεί συγκεκριμένες λειτουργίες (π.χ. δρομολόγηση, μεταφορά, εφαρμογή) προκειμένου να καταστήσει αξιόπιστη τη μεταφορά πληροφοριών. Στο **Σχήμα 1.1** παρουσιάζεται

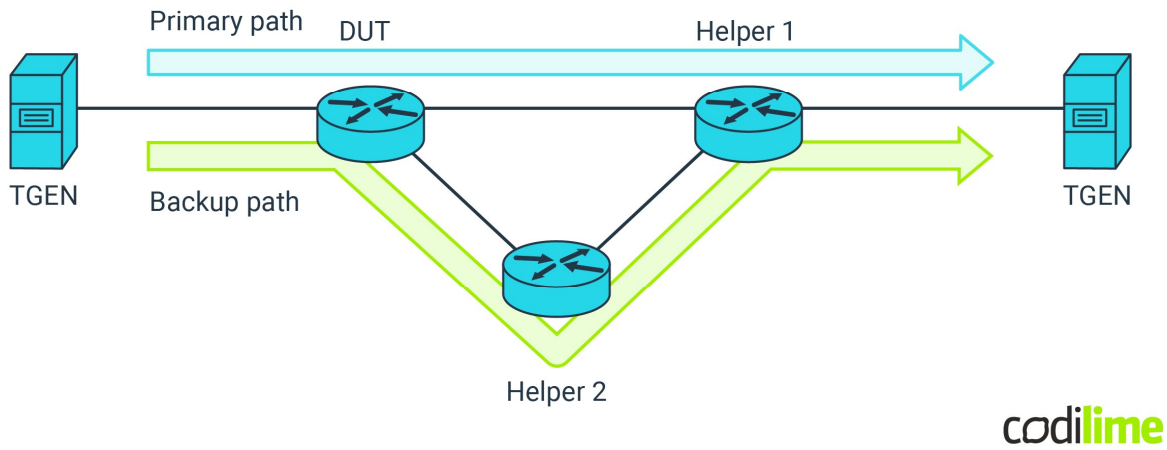
σχηματικά η αρχιτεκτονική ενός απλού δικτύου υπολογιστών και η ροή της δικτυακής κίνησης από έναν πελάτη προς έναν διακομιστή.



Σχήμα 1.1 [3] Αρχιτεκτονική ενός απλού δικτύου υπολογιστών και η ροή της δικτυακής κίνησης από έναν πελάτη προς έναν διακομιστή

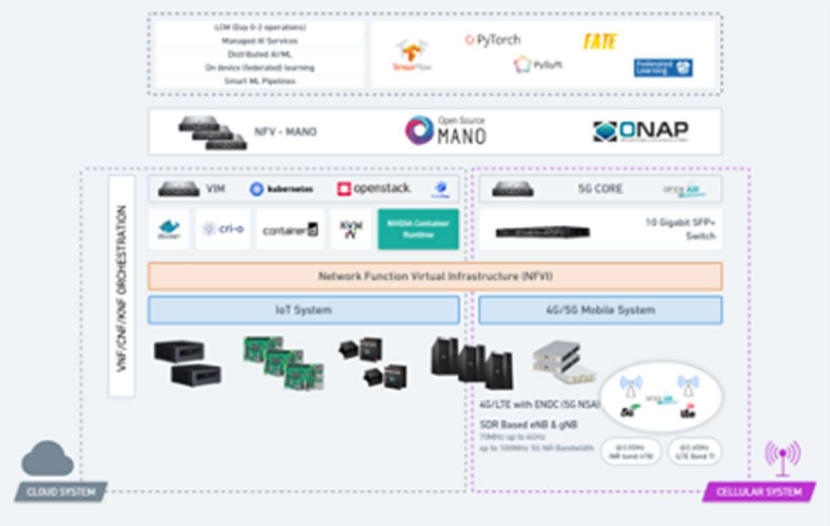
Στο ανώτερο στρώμα (εφαρμογών) παράγεται η κυκλοφορία δεδομένων από εφαρμογές και χρήστες – για παράδειγμα, οι αιτήσεις HTTP ενός φυλλομετρητή ή οι ροές βίντεο μιας υπηρεσίας streaming. Η **παραγωγή κίνησης** αναφέρεται ακριβώς στη διαδικασία αυτή: στη δημιουργία και αποστολή πακέτων δεδομένων μέσα στο δίκτυο, είτε από πραγματικούς χρήστες/εφαρμογές είτε με τεχνητό τρόπο μέσω εργαλείων προσομοίωσης.
Η δυνατότητα να δημιουργούμε **τεχνητή δικτυακή κίνηση** με ελεγχόμενο και επαναλήψιμο τρόπο είναι ζωτικής σημασίας για την αξιολόγηση και τη μελέτη των δικτύων. Με εργαλεία παραγωγής κίνησης, οι μηχανικοί δικτύων και οι ερευνητές μπορούν να προσομοιώσουν διάφορα σενάρια φόρτου και να μετρήσουν τις επιδόσεις (ρυθμός μετάδοσης, καθυστερήσεις, ποσοστά απωλειών κ.λπ.) ή τη συμπεριφορά ενός συστήματος υπό συνθήκες αιχμής. Για παράδειγμα, το εργαλείο **iPerf3** είναι ένα ευρέως χρησιμοποιούμενο λογισμικό ανοιχτού κώδικα, το οποίο υιοθετεί μοντέλο πελάτη-διακομιστή για να δημιουργήσει συνεχείς ροές δεδομένων και να μετρήσει τη διαμεταγωγή του δικτύου. Τέτοια εργαλεία λειτουργούν ως **γεννήτριες δικτυακής κυκλοφορίας**, επιτρέποντας την προσομοίωση πραγματικού φορτίου σε ένα ελεγχόμενο περιβάλλον. Στα εργαστηριακά περιβάλλοντα (testbeds), η χρήση γεννητριών κίνησης (traffic generators) είναι καθοριστική για την αξιολόγηση της συμπεριφοράς δικτύων και πρωτοκόλλων

υπό διάφορες συνθήκες (βλ. Σχήμα 1.2 για μια ενδεικτική διάταξη πειράματος παραγωγής κίνησης).



Σχήμα 1.2[4] Διάταξη πειράματος παραγωγής κίνησης

Ιδιαίτερα στα δίκτυα 5G, όπου οι τύποι κίνησης ποικίλλουν (από μαζική επικοινωνία μηχανών mMTC έως εξαιρετικά υψηλής ταχύτητας ροές eMBB), η δυνατότητα **προσομοίωσης ρεαλιστικής κίνησης** καθίσταται κρίσιμη. Η προτυποποιημένη κίνηση (synthetic traffic) μπορεί να βασίζεται σε **μοντέλα κίνησης** που μιμούνται τυπική συμπεριφορά χρηστών ή εφαρμογών. Για παράδειγμα, ένα σενάριο χρήσης μπορεί να περιλαμβάνει προσομοιωμένους χρήστες που περιηγούνται στον ιστό, πραγματοποιούν κλήσεις VoIP ή στέλνουν δεδομένα αισθητήρων IoT, ώστε η συνολική παραγόμενη κίνηση να αντιστοιχεί σε μια **τυπική κυκλοφοριακή μέρα** ενός κυψελοειδούς δικτύου. Η παραγωγή τέτοιων ροών μπορεί να γίνει είτε με προγραμματισμένα script (π.χ. ένα λογισμικό που αυτοματοποιεί έναν φυλλομετρητή για να επισκέπτεται ιστοσελίδες) είτε με εξειδικευμένες πλατφόρμες προσομοίωσης δικτύου. **Εργαλεία προσομοίωσης δικτύου** όπως το *ns-3* (με το πρόσθετο 5G-LENA) και το *OMNeT++* (με βιβλιοθήκες όπως το Simu5G) επιτρέπουν τον λεπτομερή έλεγχο του τρόπου παράγονται και διακινούνται τα πακέτα, συνδυάζοντας μοντέλα του 5G Radio Access Network και του 5G Core. Με αυτά, μπορούμε να καθορίσουμε τις **κυκλοφοριακές ροές** (traffic flows) που θα δημιουργηθούν – π.χ. αριθμό ταυτόχρονων κλήσεων, μέγεθος και συχνότητα πακέτων, πρότυπα κίνησης – και έτσι να παράγονται **επαναλήψιμα φορτία** για πειραματική ανάλυση.
Η επισκόπηση των δικτύων υπολογιστών και της παραγωγής κίνησης αναδεικνύει ότι η **ελεγχόμενη προσομοίωση της κυκλοφορίας** είναι θεμελιώδης για την μελέτη τόσο της απόδοσης όσο και της ασφάλειας των δικτύων. Στο πλαίσιο της παρούσας εργασίας, αυτά τα εργαλεία και τεχνικές αξιοποιούνται ώστε να δημιουργηθεί ένα περιβάλλον 5G στο οποίο μπορούμε να παράγουμε κανονική αλλά και κακόβουλη κίνηση κατά βούληση, για να δοκιμάσουμε τις δυνατότητες ανίχνευσης των IDS (βλ. Σχήμα 1.3 για μια σχηματική αναπαράσταση τέτοιου περιβάλλοντος).

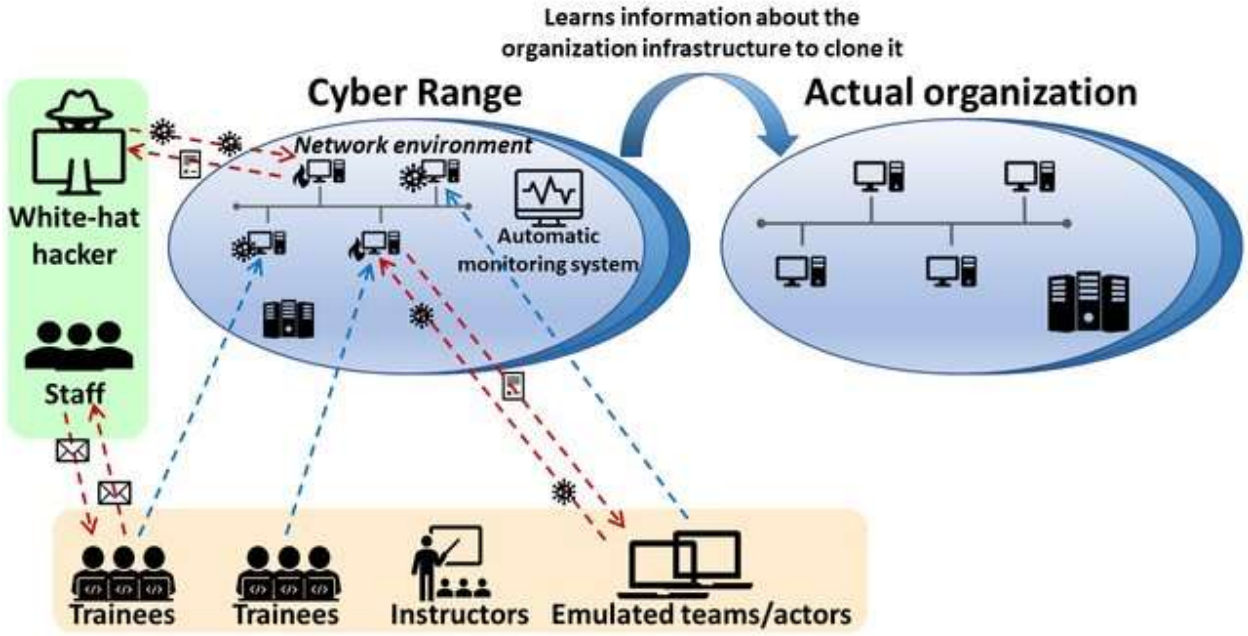


Σχήμα 1.3 [5]5G Radio Access Network

1.1.2 Εισαγωγή στα Cyber Ranges/Testbeds και στα Συστήματα Ανίχνευσης Εισβολών (IDS)

Η διαρκής εξέλιξη των κυβερνοαπειλών έχει οδηγήσει στην ανάπτυξη **Cyber Ranges** (κυβερνοπεδίων) και **δοκιμαστικών κλινών** (testbeds) για σκοπούς εκπαίδευσης και έρευνας στην κυβερνοασφάλεια. Ένα cyber range είναι ένα απομονωμένο, ελεγχόμενο περιβάλλον – συνήθως υλοποιημένο με εικονικές μηχανές και προσομοιωμένα δίκτυα – στο οποίο μπορούν να αναπαραχθούν ρεαλιστικά σενάρια δικτυακών επιθέσεων και αμυντικών μηχανισμών χωρίς κίνδυνο για πραγματικές υποδομές. Ιστορικά, πολλά τέτοια συστήματα σχεδιάστηκαν ως φυσικά εργαστήρια με πραγματικό εξοπλισμό (π.χ. το **National Cyber Range (NCR)** του Υπουργείου Άμυνας ΗΠΑ), όμως **οι νεότερες προσεγγίσεις στρέφονται σε πλήρως εικονικά περιβάλλοντα, μειώνοντας το κόστος και αυξάνοντας την ευελιξία**[6]. Υπάρχουν αξιοσημείωτα παραδείγματα κυβερνοπεδίων, όπως τα DETERLab, KYPO, και CyRIS, που παρέχουν πλατφόρμες για εκτέλεση ασκήσεων κυβερνοάμυνας ή δοκιμές νέων τεχνικών ανίχνευσης. Στο **Σχήμα 1.4** παρουσιάζεται ενδεικτικά η δομή ενός cyber range, όπου πολλαπλά τμήματα δικτύου (π.χ. εταιρικό δίκτυο, δίκτυο επιτιθέμενου) μπορούν να προσομοιωθούν και να εκτελεστούν σενάρια επίθεσης/άμυνας με

πραγματικό λογισμικό.



Σχήμα 1.4 [7] Η δομή ενός cyber range

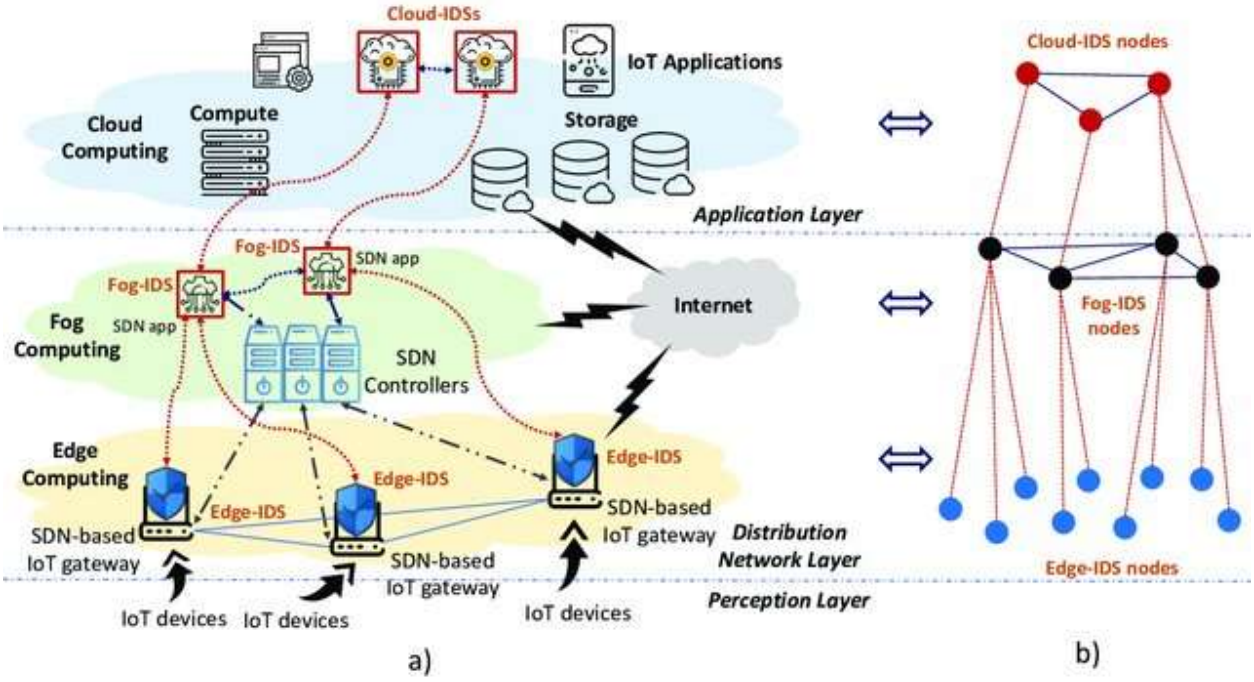
Οι δοκιμαστικές κλίνες εστιάζουν περισσότερο στην **πειραματική αξιολόγηση τεχνολογιών**. Μια δοκιμαστική κλίνη δικτύων μπορεί να είναι μέρος ενός cyber range, σχεδιασμένη ειδικά για την **αναπαραγωγή ενός στοχοθετημένου περιβάλλοντος** (π.χ. ενός δικτύου κινητής τηλεφωνίας) προκειμένου να δοκιμαστούν νέες ιδέες. Στο πλαίσιο των δικτύων 5G, η ανάγκη για τέτοιες δοκιμαστικές κλίνες είναι έντονη, καθώς επιτρέπουν στους ερευνητές να πειραματιστούν με την υποδομή 5G (πυρήνας, RAN, άκρα δικτύου) και να **προσομοιώσουν επιθέσεις** με ρεαλισμό. *Για παράδειγμα, μια πλήρως εικονική υλοποίηση δικτύου 5G SA (Standalone) με λογισμικό ανοιχτού κώδικα μπορεί να αποτελέσει τη βάση για δοκιμές IDS*, δίνοντας τη δυνατότητα για γρήγορη ρύθμιση και επαναφορά των συνθηκών (automation)[6]. Έτσι, τα cyber ranges και testbeds στοχεύουν να προσφέρουν **περιβάλλοντα "sandbox"** όπου δοκιμάζονται αποτελεσματικά οι μηχανισμοί ανίχνευσης και απόκρισης σε εισβολές.

Παράλληλα, τα **Συστήματα Ανίχνευσης Εισβολών (IDS)** αποτελούν τον βασικό μηχανισμό λογισμικού (ή/και υλικού) για την παρακολούθηση δικτύων και συστημάτων με σκοπό τον εντοπισμό κακόβουλων ενεργειών. Ένα IDS συλλέγει πληροφορίες (π.χ. πακέτα δικτύου, log συμβάντων) και τις αναλύει, αναζητώντας **ενδείξεις μη εξουσιοδοτημένων ή ύποπτων ενεργειών** που απειλούν το απόρρητο, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος[1]. Σε αντίθεση με τα τείχη προστασίας (firewalls) που φιλτράρουν την κίνηση βάσει προκαθορισμένων κανόνων, τα IDS έχουν ως στόχο να ανιχνεύσουν επιθέσεις που μπορεί να *διαφύγουν* ενός απλού φιλτραρίσματος – όπως ένα νέο είδος malware ή μια επίθεση *insider*.

Κατηγοριοποίηση IDS: Υπάρχουν δύο κύριες προσεγγίσεις στον τρόπο ανίχνευσης των εισβολών. Πρώτον, τα **συστήματα βάσει υπογραφών** (*Signature-Based IDS, SIDS*) που αναγνωρίζουν γνωστά μοτίβα επίθεσης αντιστοιχίζοντας τα εισερχόμενα δεδομένα με μια βάση *υπογραφών* (patterns) γνωστών απειλών[1]. Αυτή η προσέγγιση (γνωστή και ως ανίχνευση κατ' υπόδειξη ή misuse detection) χρησιμοποιείται σε εργαλεία όπως το Snort και είναι ιδιαίτερα

ακριβής για ήδη γνωστές επιθέσεις. Δεν μπορεί όμως να εντοπίσει νέες, άγνωστες μορφές επίθεσης (τα λεγόμενα *zero-day exploits*) αν δεν υπάρχει αντίστοιχη υπογραφή στη βάση δεδομένων. Δεύτερον, τα **συστήματα βάσει ανωμαλίας** (*Anomaly-Based IDS, AIDS*) που εντοπίζουν αποκλίσεις από τη *φυσιολογική συμπεριφορά* του συστήματος χρησιμοποιώντας στατιστικές μεθόδους ή μηχανική μάθηση. Σε αυτή την περίπτωση, το IDS πρώτα *εκπαιδεύεται* ώστε να μάθει ποια είναι η κανονική κυκλοφορία/συμπεριφορά (φάση *profiling*) και στη συνέχεια, σε λειτουργία πραγματικού χρόνου, σημαίνει ως εισβολή οτιδήποτε *αποκλίνει σημαντικά* από το πρότυπο. Τα συστήματα ανίχνευσης βάσει ανωμαλίας μπορούν να ανιχνεύσουν και εντελώς νέες επιθέσεις (π.χ. έναν άγνωστο τύπο DoS), όμως συχνά παράγουν αυξημένα **ψευδώς θετικά** αποτελέσματα (false positives), δηλαδή λανθασμένους συναγερμούς για κανονική δραστηριότητα που απλώς δεν είχε παρατηρηθεί στην εκπαίδευση[8], [9].

Εκτός από τον τρόπο ανίχνευσης, τα IDS διακρίνονται και ως προς τη θέση τους στο σύστημα. Τα **Host-Based IDS (HIDS)** εγκαθίστανται σε μεμονωμένους οικοδεσπότες/τερματικές συσκευές και παρακολουθούν τοπικά συμβάντα (αρχεία log, κλήσεις συστήματος), ενώ τα **Network-Based IDS (NIDS)** παρακολουθούν την κίνηση δικτύου σε ένα τμήμα του δικτύου (π.χ. στο σημείο εξόδου προς το Διαδίκτυο)[10]. Υπάρχουν επίσης IDS ειδικευμένα για ασύρματα δίκτυα (WIDS), για ανάλυση ροών (NBA – Network Behavior Analysis), καθώς και συνδυαστικές προσεγγίσεις. Στην περίπτωση των δικτύων 5G, το ενδιαφέρον επικεντρώνεται κυρίως στα NIDS, καθώς αφορούν την παρακολούθηση της κίνησης τόσο στον πυρήνα του δικτύου όσο και στα συνοριακά σημεία (όπου το δίκτυο 5G συνδέεται με εξωτερικά δίκτυα ή το Διαδίκτυο). Ένα NIDS στο περιβάλλον ενός παρόχου 5G μπορεί, για παράδειγμα, να τοποθετηθεί στο σημείο όπου ο πυρήνας (Core Network) συνδέεται με το υπόλοιπο Διαδίκτυο (βλ. Σχήμα 1.5), ώστε να επιβλέπει όλες τις ροές δεδομένων που εισέρχονται και εξέρχονται από το δίκτυο του παρόχου.



Σχήμα 1.5 [11] Ένα NIDS στο περιβάλλον ενός παρόχου 5G μπορεί, για παράδειγμα, να τοποθετηθεί στο σημείο όπου ο πυρήνας (Core Network) συνδέεται με το υπόλοιπο Διαδίκτυο

Αντίστοιχα, μπορούν να υπάρξουν **αποκεντρωμένα IDS** σε πολλά σημεία του δικτύου – π.χ. ένα σε κάθε σταθμό βάσης ή κόμβο MEC – για μια πολυεπίπεδη αμυντική στρατηγική. Σε πρόσφατες μελέτες έχει προταθεί η ενσωμάτωση μονάδων IDS/Firewall ακόμη και σε επίπεδο κεραιών (gNodeB) του 5G, ως επιπλέον ασπίδα ασφαλείας δίπλα στα παραδοσιακά στοιχεία δικτύου[10]. Τα IDS αποτελούν ακρογωνιαίο λίθο της ανίχνευσης κυβερνοεπιθέσεων. Στην εποχή του 5G, συνδυασμοί τεχνικών (υπογραφών, ανωμαλίας, μηχανικής μάθησης) και κατανεμημένες υλοποιήσεις IDS θεωρούνται αναγκαίες ώστε να αντιμετωπιστούν οι περίπλοκες και πολυδιάστατες απειλές που στοχεύουν τα σύγχρονα δίκτυα.

1.2 Σκοπός της παρούσας διατριβής

Ο σκοπός αυτής της διατριβής είναι η μελέτη και εφαρμογή εργαλείων προσομοίωσης δικτυακής κίνησης σε δίκτυα 5G, με έμφαση στην αξιολόγηση τους προκειμένου να ερευνηθεί η απόκριση ορισμένων συστημάτων ανίχνευσης εισβολών. Σε προηγούμενες ενότητες περιγράφηκε πως τα δίκτυα 5G εισάγουν νέες προκλήσεις ασφάλειας λόγω της πολυπλοκότητάς τους. **Γιατί είναι σημαντική αυτή η έρευνα στο πλαίσιο του 5G;** Διότι τα υφιστάμενα IDS και γενικότερα οι μηχανισμοί ασφαλείας χρειάζονται προσαρμογή και ενίσχυση προκειμένου να καλύψουν την επεκταμένη επιφάνεια επίθεσης των δικτύων 5G[10]. Η ραγδαία αύξηση συσκευών και υπηρεσιών σε 5G, σε συνδυασμό με τις καινοτομίες όπως η εικονικοποίηση λειτουργιών δικτύου (NFV), το slicing και η διάχυτη χρήση IoT, δημιουργούν ένα **περιβάλλον απειλών εξελισσόμενο και πολυκέφαλο**. Πρόσφατες μελέτες υπογραμμίζουν ότι απαιτούνται **έξυπνοι, αυτοματοποιημένοι μηχανισμοί ανίχνευσης** για το 5G, καθώς οι επιτιθέμενοι μπορούν να αξιοποιήσουν την ίδια την πολυπλοκότητα του δικτύου για να διεξαγάγουν ευφυείς επιθέσεις που διαφεύγουν συμβατικών

μέτρων[12]. Για παράδειγμα, οι επιθέσεις ενδέχεται να στοχεύουν όχι μόνο τα περιμετρικά στοιχεία αλλά και τον ίδιο τον πυρήνα 5G (π.χ. καταχρώμενες σηραγγώσεις στο πρωτόκολλο 5G, επιθέσεις σε λειτουργίες διαχείρισης συνεδριών), οι οποίες είναι δύσκολο να ανιχνευθούν αν δεν υπάρχουν εξειδικευμένα συστήματα παρακολούθησης μέσα στο δίκτυο. Συνεπώς, η έρευνα στον τομέα αυτό είναι κρίσιμη για να διασφαλιστεί ότι το 5G θα υλοποιήσει τις υποσχέσεις του (υψηλή αξιοπιστία, διαθεσιμότητα, ασφάλεια υπηρεσιών) χωρίς να καταστεί ευάλωτο σε νέες κυβερνοαπειλές.

Λαμβάνοντας υπόψη τα παραπάνω, η παρούσα εργασία έχει ως στόχους: Πρώτον, να πραγματοποιήσει μια εκτενή επισκόπηση, κατανόηση και αξιολόγηση των πιο δημοφιλών εργαλείων παραγωγής διαδικτυακής κίνησης, ώστε να αναδειχθούν οι καταλληλότερες λύσεις για τη δημιουργία ρεαλιστικών σεναρίων δικτυακής συμπεριφοράς. Το κομμάτι της ανασκόπησης (review) αποτελεί θεμελιώδες και διακριτό βήμα της διπλωματικής εργασίας, καθώς θέτει τη βάση για τη μετέπειτα υλοποίηση.Δεύτερον η αξιολόγηση μέσω πολυκριτηριακών μεθόδων των εργαλείων παραγωγής διαδικτυακής κίνησης που συμμετείχαν στην ανασκόπηση και τελικώς η δημιουργία μιας ολοκληρωμένης δοκιμαστικής κλίνης (testbed) 5G για την αξιολόγηση εργαλείων ανίχνευσης εισβολών.
Ειδικότερα, προτείνεται η υλοποίηση ενός πλήρους περιβάλλοντος δικτύου 5G σε μικρή κλίμακα – περιλαμβάνοντας τον πυρήνα 5G (5G Core), προσομοιωμένο ασύρματο δίκτυο πρόσβασης (gNodeB και πολλαπλούς UE) καθώς και τα κατάλληλα εργαλεία δημιουργίας κίνησης – πάνω στο οποίο θα ενσωματωθεί ένα ή περισσότερα IDS. Το testbed αυτό θα επιτρέψει να γεννηθούν ελεγχόμενα σενάρια κανονικής λειτουργίας αλλά και επιθέσεων, ώστε να αξιολογηθεί η ικανότητα του IDS να ανιχνεύει τις κακόβουλες ενέργειες. Με άλλα λόγια, φιλοδοξούμε να παρέχουμε ένα *πλαίσιο proof-of-concept* όπου μπορούν να μετρηθούν με ακρίβεια δείκτες απόδοσης ενός IDS (όπως ο ρυθμός ανίχνευσης επιθέσεων, τα ψευδώς θετικά/αρνητικά, η καθυστέρηση ανίχνευσης) σε ένα ρεαλιστικό 5G περιβάλλον.
Η επιλογή αυτων των στόχων υπαγορεύεται τόσο από το κενό που υπάρχει στη βιβλιογραφία όσο και από πρακτικές ανάγκες. Όπως αναφέρθηκε, δεν υπάρχουν πολλά διαθέσιμα δημόσια σύνολα δεδομένων ή ανοικτές πλατφόρμες με πραγματική 5G κίνηση για να εκπαιδευτούν και να δοκιμαστούν συστήματα IDS[8], [10]. Οι περισσότεροι ερευνητές καλούνται να δημιουργήσουν οι ίδιοι τα δεδομένα που χρειάζονται, είτε μέσω προσομοιώσεων είτε μέσω εργαστηριακών δικτύων[13]. Η εργασία αυτή στοχεύει να συμβάλει σε αυτό το πεδίο με μια αναφορά υλοποίησης testbed, όπου οποιοδήποτε εργαλείο IDS (π.χ. Snort, Suricata ή άλλες πλατφόρμες ανίχνευσης) μπορεί να ενταχθεί και να αξιολογηθεί σε περιβάλλον 5G. Έμφαση δίνεται στην αξιοποίηση λογισμικού ανοιχτού κώδικα και τυποποιημένων εργαλείων, ώστε η λύση να είναι αναπαραγώγιμη και επεκτάσιμη από την κοινότητα. Με αυτόν τον τρόπο, η έρευνά μας είναι σημαντική διότι γεφυρώνει το χάσμα μεταξύ θεωρητικών μελετών (που συχνά περιορίζονται σε προσομοιώσεις υψηλού επιπέδου ή σε δεδομένα παλαιότερων γενιών δικτύων) και της πρακτικής επιβεβαίωσης σε ένα αληθοφανές περιβάλλον 5G.

1.3 Σχετική εργασία

Στην ενότητα αυτή παρουσιάζεται η σχετική βιβλιογραφία και οι προηγούμενες εργασίες που συνδέονται με το αντικείμενο της παρούσας διατριβής. Η ανασκόπηση περιλαμβάνει τόσο μελέτες γενικής φύσεως (π.χ. έρευνες για IDS σε δίκτυα 5G) όσο και συγκεκριμένες υλοποιήσεις

δοκιμαστικών κλινών, εργαλεία δημιουργίας κίνησης και datasets, καθώς και δημοσιεύσεις που αφορούν τεχνικές ανίχνευσης εισβολών (συμπεριλαμβανομένων μεθόδων μηχανικής μάθησης).

IDS σε δίκτυα 5G – προκλήσεις και τάσεις: Αρκετοί ερευνητές έχουν ασχοληθεί με το ζήτημα της ασφάλειας στα δίκτυα 5G και ειδικά με την ανίχνευση κακόβουλης δραστηριότητας. Σε μια πρόσφατη εκτενή ανασκόπηση, οι Noor et al. (2025) παρουσιάζουν τις κύριες προκλήσεις ασφάλειας στα 5G και τον εξελισσόμενο ρόλο των IDS για την αντιμετώπισή τους[1]. Η μελέτη αυτή επισημαίνει ότι τα υπάρχοντα πλαίσια IDS και τα διαθέσιμα σύνολα δεδομένων δεν επαρκούν, υπογραμμίζοντας την ανάγκη για **πιο αξιόπιστα και αντιπροσωπευτικά δεδομένα** προκειμένου να αναπτυχθούν αποτελεσματικά NIDS για το 5G. Παράλληλα, διάφορες εργασίες εξετάζουν σύγχρονες μεθόδους ανίχνευσης: για παράδειγμα, η χρήση αλγορίθμων **βαθιάς μάθησης (DL)** έχει μελετηθεί εκτενώς για την ανίχνευση επιθέσεων DDoS σε 5G περιβάλλοντα. Τεχνικές όπως οι αμφίδρομες LSTM (BiLSTM) και οι Συνελικτικά Νευρωνικά Δίκτυα (CNN) έχουν δοκιμαστεί ως ταξινομητές για ανίχνευση μοτίβων επίθεσης υψηλής πολυπλοκότητας, με ενθαρρυντικά αποτελέσματα[1]. Επιπλέον, λόγω της ιδιαιτερότητας των 5G δικτύων, προτείνονται καινοτόμες προσεγγίσεις όπως η **Μεταφορά Μάθησης (Transfer Learning)**. Για παράδειγμα, έχουν παρουσιαστεί λύσεις που συνδυάζουν ανίχνευση ανωμαλιών με Deep Transfer Learning, προκειμένου να βελτιώσουν την ικανότητα εντοπισμού νέων επιθέσεων (όπως επιθέσεις EDoS σε slices) αξιοποιώντας γνώση από άλλα πεδία.

Δοκιμαστικές κλίνες και datasets για 5G ασφάλεια: Λόγω του ότι το 5G είναι σχετικά πρόσφατη τεχνολογία, μέχρι πρότινος υπήρχε έλλειψη ανοιχτών testbeds αποκλειστικά για δοκιμές κυβερνοασφάλειας σε 5G. Ο Knieps, Günter [13]σημειώνουν ότι **δεν υπήρχαν εξειδικευμένες κυβερνο-υποδομές για 5G**, και πρότειναν μια νέα πλήρως εικονική δοκιμαστική κλί1νη 5G, επισημαίνοντας ιδιαίτερα την έλλειψη δημοσίως διαθέσιμων datasets υψηλής ακρίβειας για εκπαίδευση IDS[14]. Αυτή η τάση δείχνει τη στροφή της ερευνητικής κοινότητας στο να αναπτύξει τα δικά της εργαλεία και περιβάλλοντα. Ήδη έχουν κάνει την εμφάνισή τους ορισμένα **σύνολα δεδομένων ασφάλειας 5G**. Χαρακτηριστικό παράδειγμα είναι το **5G-NIDD**, ένα εκτενές dataset που δημοσιεύτηκε το 2022-2023, το οποίο περιέχει πλήρως χαρακτηρισμένα δείγματα κακόβουλης και κανονικής κίνησης από ένα δοκιμαστικό δίκτυο 5G[12]. Το 5G-NIDD δημιουργήθηκε σε ένα πραγματικό 5G test network (Πανεπιστήμιο Oulu, Φινλανδία) και περιλαμβάνει επιθέσεις όπως πολλαπλές μορφές DoS (ICMP Flood, UDP Flood, SYN Flood, HTTP Slowrate κ.ά.) και port scans, διεξαγόμενες από κακόβουλους κόμβους προς servers στο Multi-access Edge Computing (MEC) περιβάλλον. Τα δεδομένα αυτά (διαθέσιμα σε μορφή pcap και επεξεργασμένες εξαγωγές CSV) αποτελούν πολύτιμο πόρο, διότι μπορούν να χρησιμοποιηθούν για την εκπαίδευση και αξιολόγηση αλγορίθμων IDS σε ρεαλιστικές συνθήκες. Ωστόσο, ακόμα και με την ύπαρξη τέτοιων datasets, η ανάγκη για **δυναμική δημιουργία κυκλοφορίας** παραμένει: κανένα στατικό dataset δεν μπορεί να καλύψει πλήρως το εύρος πιθανών σεναρίων σε ένα ζωντανό δίκτυο 5G. Για τον λόγο αυτό, η παρούσα διατριβή υιοθετεί την προσέγγιση της *επιτόπιας* δημιουργίας κίνησης στο εργαστηριακό περιβάλλον, ώστε να υπάρχει πλήρης έλεγχος των παραμέτρων και δυνατότητα προσαρμογής των σεναρίων επιτόπου.

Εργαλεία προσομοίωσης 5G και ανοικτές πλατφόρμες: Η υλοποίηση ενός testbed 5G επωφελείται σημαντικά από την ύπαρξη ανοιχτού λογισμικού προσομοίωσης/εξομοίωσης δικτύων κινητής. Ευτυχώς, τα τελευταία χρόνια έχουν **αναδυθεί αρκετές πλατφόρμες ανοιχτού κώδικα για 5G**, οι οποίες επιτρέπουν στην ερευνητική κοινότητα να υλοποιήσει επιτόπου δίκτυα 5G χωρίς την ανάγκη ακριβού εμπορικού εξοπλισμού. Τρεις δημοφιλείς λύσεις για το Radio

Access Network είναι το **srsRAN**, το **OpenAirInterface (OAI)** και το **UERANSIM**, που υλοποιούν διάφορες όψεις του RAN σύμφωνα με τις προδιαγραφές 3GPP[15]. Για τον πυρήνα δικτύου, αντίστοιχα, υπάρχουν έργα όπως το **Open5GS** και το **free5GC**. Αυτές οι πλατφόρμες, αν και δεν είναι ακόμα ισοδύναμα ώριμες με τις εμπορικές υλοποιήσεις, έχουν αρχίσει να χρησιμοποιούνται σε πρακτικά πειράματα 5G από πανεπιστήμια και ερευνητικά κέντρα[15]. Η παρούσα εργασία αξιοποιεί μερικές από αυτές (όπως θα περιγραφεί στα επόμενα κεφάλαια), ακολουθώντας το ρεύμα της σύγχρονης έρευνας που ενθαρρύνει τη **συνεργασία ακαδημαϊκής κοινότητας και βιομηχανίας** μέσω ανοικτών εργαλείων. Με τον τρόπο αυτό, το testbed μας είναι συγκρίσιμο και συμβατό με άλλα που έχουν υλοποιηθεί παγκοσμίως, επιτρέποντας συγκριτικές αξιολογήσεις.
Συνοψίζοντας τη σχετική εργασία (βλ. και **Πίνακα 5.1**), παρατηρούμε τα εξής κύρια σημεία: (α) Υπάρχει συναίνεση ότι τα δίκτυα 5G απαιτούν νέες προσεγγίσεις στην ανίχνευση εισβολών, με έμφαση σε ευφυείς και αυτοπροσαρμοζόμενες μεθόδους. (β) Η έλλειψη κατάλληλων δεδομένων και περιβαλλόντων δοκιμών ήταν ένα κενό που σταδιακά καλύπτεται με προσπάθειες δημιουργίας datasets (π.χ. 5G-NIDD) και ανάπτυξης ανοικτών testbeds. (γ) Η χρήση ανοιχτού κώδικα 5G components (π.χ. Open5GS, srsRAN, UERANSIM) καθίσταται de-facto προσέγγιση για ακαδημαϊκή έρευνα, καθώς επιτρέπει την υλοποίηση *ολοκληρωμένων 5G δικτύων σε εργαστήριο*. (δ) Μέχρι στιγμής, λίγες δημοσιευμένες εργασίες έχουν παρουσιάσει αναλυτικά αποτελέσματα από δοκιμές IDS σε 5G – συνεπώς, η διατριβή αυτή έρχεται να συμβάλει προσφέροντας μια τεκμηριωμένη μελέτη περίπτωσης. Τα αποτελέσματα και τα συμπεράσματα που θα εξαχθούν ευελπιστούμε να αποτελέσουν χρήσιμη προσθήκη στη βιβλιογραφία και να καθοδηγήσουν μελλοντικές έρευνες στον χώρο της ασφάλειας 5G.

1.4 Συνεισφορά

Η παρούσα διατριβή εισφέρει στη μελέτη και εφαρμογή τεχνολογιών εξομοίωσης και δημιουργίας κίνησης σε δίκτυα 5G, προτείνοντας μια ολοκληρωμένη προσέγγιση σχεδίασης, επιλογής και υλοποίησης ενός ρεαλιστικού 5G testbed βασισμένου αποκλειστικά σε λύσεις ανοιχτού κώδικα. Η συνεισφορά της διατριβής εστιάζει σε πέντε κύριους άξονες:

Χαρτογράφηση και ανασκόπηση των κύριων εργαλείων:

Η βιβλιογραφική αναζήτηση φιλτράρισε μόνο εργαλεία και πλατφόρμες που υποστηρίζουν ρητά τεχνολογίες δικτύου 5G (πρόσβαση New Radio ή 5G Core) και έχουν είτε ακαδημαϊκές περιπτώσεις χρήσης είτε ενεργή υποστήριξη από την κοινότητα. Δώσαμε προτεραιότητα σε άρθρα που έχουν αξιολογηθεί από ομότιμους, σε τεκμηρίωση έργων ανοιχτού κώδικα και σε λευκές βίβλους του κλάδου που εισήγαγαν ή αξιολόγησαν τέτοια εργαλεία. Οι μελέτες συμπεριλήφθηκαν εάν περιέγραφαν την αρχιτεκτονική, τις δυνατότητες ή την απόδοση ενός προσομοιωτή/εξομοιωτή δικτύου 5G ή εάν παρουσίαζαν συγκριτικές αναλύσεις πολλών εργαλείων.
Από δεκάδες αρχικά αποτελέσματα, επιλέξαμε εκείνα τα εργαλεία που πληρούσαν τα κριτήρια υποστήριξης αυτόνομης λειτουργίας 5G (SA) ή προηγμένων λειτουργιών 5G και που ήταν προσβάσιμα για την αξιολόγησή μας (κατά προτίμηση ανοιχτού κώδικα ή δωρεάν ακαδημαϊκές εκδόσεις).

Καινοτομία στην επιλογή εργαλείων μέσω Πολυκριτηριακής Ανάλυσης (MCDA):

Αντί της άμεσης υιοθέτησης ενός έτοιμου testbed, η εργασία εισάγει μια δομημένη και τεκμηριωμένη μέθοδο αξιολόγησης 12 εναλλακτικών εργαλείων για δημιουργία και παρακολούθηση 5G κίνησης. Η χρήση MCDA με σταθμισμένα κριτήρια και συγκριτική ανάλυση (π.χ. TGC, PS, EUC, IV) τεκμηριώνει την επιλογή του Open5GS + UERANSIM ως την πιο κατάλληλη πλατφόρμα για τις απαιτήσεις της παρούσας μελέτης.

Ανάπτυξη πλήρους testbed για 5G βασισμένο σε Open Source τεχνολογίες :

Η εργασία υλοποιεί ένα πλήρως λειτουργικό 5G SA testbed χρησιμοποιώντας τις τελευταίες σταθερές εκδόσεις των εργαλείων Open5GS και UERANSIM, αξιοποιώντας τη σχετική τεκμηρίωση, τα κοινά πρότυπα (3GPP Rel.15–17) και τις δυνατότητες εικονικοποίησης (VirtualBox-based VM). Το testbed είναι αναπαραγώγιμο και ευέλικτο, επιτρέποντας προσαρμογές σε διαφορετικά σενάρια και παραμέτρους.

Δημιουργία ρεαλιστικών σεναρίων δημιουργίας κίνησης (benign και malicious):

Η εργασία προσομοιώνει διαφορετικούς τύπους κανονικής (π.χ. iperf3) και κακόβουλης κίνησης (π.χ. hping3), παρέχοντας πλήρη καταγραφή και μετρική ανάλυση της συμπεριφοράς του 5G δικτύου υπό διαφορετικές συνθήκες.

Τεκμηρίωση και επαναληψιμότητα του πειράματος:

Όλες οι φάσεις του πειράματος (ρύθμιση testbed, παραμετροποίηση, εκτέλεση, συλλογή δεδομένων, αξιολόγηση) καταγράφηκαν βήμα προς βήμα. Η εργασία δύναται να αναπαραχθεί πλήρως από άλλους ερευνητές ή να χρησιμοποιηθεί ως βάση για μελλοντική επέκταση (π.χ. εισαγωγή IDS/IPS μηχανισμών ή αξιολόγηση slicing/mobility χαρακτηριστικών).
Η συνεισφορά της διατριβής συνδυάζει πρακτική αξία (υλοποιήσιμο testbed) με επιστημονική μεθοδολογία (MCDA, αξιολόγηση απόδοσης), συνιστώντας έναν χρήσιμο οδηγό για ερευνητές και επαγγελματίες που δραστηριοποιούνται στον χώρο της ασφάλειας και αξιολόγησης δικτύων 5G.

1.5 Δομή του Εγγράφου

Η παρούσα διατριβή οργανώνεται σε έξι (6) κύρια κεφάλαια, τα οποία δομούνται ως εξής:
Κεφάλαιο 1 – Εισαγωγή:
Παρουσιάζεται το θεωρητικό και τεχνολογικό πλαίσιο της έρευνας, η σημασία της δημιουργίας και ανάλυσης δικτυακής κίνησης στα δίκτυα 5G, και διατυπώνεται ο στόχος της εργασίας: η επιλογή, εγκατάσταση και αξιολόγηση ενός κατάλληλου εργαλείου για την παραγωγή κίνησης σε ένα λειτουργικό 5G testbed. Περιγράφεται επίσης η μεθοδολογία που ακολουθείται και τεκμηριώνεται η συνεισφορά της μελέτης.

Κεφάλαιο 2- Μεθοδολογία:
Γίνεται ανάλυση στις μεθοδολογίες που εφαρμόστηκαν κατά την έρευνα, τα πειράματα και την συγγραφή της διατριβής.

Κεφάλαιο 3 – Εξέλιξη των Τεχνολογιών που Απαρτίζουν τη Δημιουργία Δικτυακής Κίνησης:
Στο κεφάλαιο αυτό αναλύονται τα βασικά δομικά στοιχεία της παραγωγής και προσομοίωσης δικτυακής κίνησης, εστιάζοντας στις τεχνολογίες που χρησιμοποιούνται σε δίκτυα επόμενης γενιάς όπως το 5G. Περιγράφονται η αρχιτεκτονική του 5G, οι απαιτήσεις απόδοσης και ασφάλειας, καθώς και οι ειδικές ανάγκες κίνησης σε περιβάλλοντα eMBB, URLLC και mMTC.

Κεφάλαιο 4 – Προσδιορισμός βασικών εργαλείων και τεχνολογιών:
Εντοπίζονται και παρουσιάζονται τα βασικά εργαλεία, πλατφόρμες και τεχνολογίες που είναι διαθέσιμα σήμερα για δημιουργία, προσομοίωση και παρακολούθηση δικτυακής κίνησης σε περιβάλλοντα 5G. Η ανασκόπηση καλύπτει εργαλεία όπως Open5GS, UERANSIM, srsRAN, TRex, D-ITG, Iperf3, Scapy, OMNeT++, καθώς και εξειδικευμένες λύσεις ασφαλείας και μέτρησης.

Κεφάλαιο 5 – Διαδικασία Επιλογής και Δικαιολόγηση των Κριτηρίων Αξιολόγησης:
Περιγράφεται λεπτομερώς η πολυκριτηριακή μεθοδολογία αξιολόγησης εργαλείων (MCDA), τα επιλεγμένα κριτήρια και τα χαρακτηριστικά τους, καθώς και η συγκριτική ανάλυση των εργαλείων. Παρουσιάζονται τα αποτελέσματα της διαδικασίας και τεκμηριώνεται η επιλογή του συνδυασμού Open5GS + UERANSIM για την υλοποίηση του testbed.

Κεφάλαιο 6 – Πειραματική Επικύρωση της Πρότασης (Proof of Concept):
Αναλύεται η υλοποίηση του testbed, η διαμόρφωση των σεναρίων (κανονική και κακόβουλη κίνηση), καθώς και η εκτέλεση και ανάλυση των πειραμάτων. Παρουσιάζονται οι μετρήσεις απόδοσης, οι παρατηρήσεις και οι επιπτώσεις στο δίκτυο, επιβεβαιώνοντας την καταλληλότητα της προτεινόμενης λύσης.

Κεφάλαιο 7 – Συμπεράσματα: Αναφέρονται τα συμπεράσματα που προέκυψαν κατά τη πορεία της έρευνας, των πειραμάτων και της συγγραφής της διατριβής.

Κεφάλαιο 8 – Βιβλιογραφία.

2. Μεθοδολογία

Το κεφάλαιο αυτό περιγράφει τη μεθοδολογία έρευνας για την αξιολόγηση εργαλείων προσομοίωσης δικτυακής κίνησης σε περιβάλλοντα 5G. Περιλαμβάνει την αρχική βιβλιογραφική επισκόπηση για τον εντοπισμό των κατάλληλων εργαλείων, την ανάπτυξη πλαισίου πολυκριτηριακής αξιολόγησης (MCDA), τη βαθμολόγηση και επιλογή του βέλτιστου εργαλείου μέσω MCDA, καθώς και το σχεδιασμό ενός testbed 5G για δοκιμές απόδοσης. Οι πειραματισμοί στο testbed καλύπτουν σενάρια τόσο κανονικής όσο και κακόβουλης κίνησης, ενώ περιγράφεται

αναλυτικά η διαδικασία συλλογής και ανάλυσης των δεδομένων. Οι παρακάτω υποενότητες αναλύουν κάθε στάδιο λεπτομερώς.

2.1 Βιβλιογραφική Επισκόπηση και Εντοπισμός Εργαλείων

Η μελέτη ξεκίνησε με μια εκτενή βιβλιογραφική επισκόπηση με στόχο τον εντοπισμό και την ταξινόμηση σχετικών εργαλείων προσομοίωσης και εξομοίωσης δικτύων 5G. Η αναζήτηση έγινε σε πολλαπλές ακαδημαϊκές βάσεις δεδομένων (Google Scholar, IEEE Xplore, Scopus) με λέξεις-κλειδιά όπως «5G simulator», «5G core emulation», «network traffic generator 5G» και ονόματα συγκεκριμένων εργαλείων (π.χ. ns-3 5G, Open5GS, srsRAN). Εστιάσαμε σε βιβλιογραφία από το 2018 και μετά ώστε να συμπεριληφθούν εργαλεία που αναπτύχθηκαν παράλληλα με τα πρότυπα του 5G. Επιπλέον, ελέγξαμε πρόσφατα άρθρα ανασκόπησης και εγχειρίδια ανοικτού κώδικα για να εξασφαλίσουμε ότι καλύπτονται οι σύγχρονες πλατφόρμες.

Κριτήρια ένταξης: Η αναζήτηση φιλτραρίστηκε ώστε να περιλαμβάνει μόνο εργαλεία και πλατφόρμες που υποστηρίζουν ρητά τεχνολογίες δικτύων 5G (πρόσβαση New Radio ή 5G Core), και τα οποία διαθέτουν είτε ακαδημαϊκές εφαρμογές είτε ενεργή υποστήριξη κοινότητας. Προτεραιότητα δόθηκε σε δημοσιευμένες εργασίες, τεκμηρίωση έργων ανοικτού κώδικα και industry whitepapers που παρουσιάζουν ή αξιολογούν τέτοια εργαλεία. Εργασίες συμπεριλήφθηκαν αν περιέγραφαν αρχιτεκτονική, δυνατότητες ή απόδοση εργαλείου προσομοίωσης/εξομοίωσης 5G ή αν παρουσίαζαν συγκριτικές αναλύσεις πολλών εργαλείων. Από δεκάδες αρχικά αποτελέσματα, επιλέχθηκαν εκείνα που υποστήριζαν λειτουργία 5G standalone (SA) ή προηγμένες δυνατότητες 5G, και ήταν προσβάσιμα για αξιολόγηση (κατά προτίμηση ανοιχτού κώδικα ή με δωρεάν ακαδημαϊκές εκδόσεις).

Μέσα από αυτή τη διαδικασία, εντοπίστηκε μια σειρά από διαδεδομένα εργαλεία προσομοίωσης και δημιουργίας κίνησης 5G, που καλύπτουν τόσο link-level όσο και end-to-end προσομοιώσεις. Τα βασικά εργαλεία που εντοπίστηκαν είναι:

1. **Προσομοιωτές δικτύου:** ns-3 (με το module 5G-LENA) και OMNeT++ (με τη βιβλιοθήκη Simu5G) – επιτρέπουν προσομοίωση σε επίπεδο πακέτου του 5G New Radio και του core δικτύου σε ελεγχόμενο λογισμικό περιβάλλον.
2. **Εξομοιωτές RAN:** srsRAN (πρώην srsLTE) – σουίτα λογισμικού ανοικτού κώδικα για RAN 4G/5G που εξομοιώνει λειτουργίες gNB (βάση 5G) και UE, απαιτώντας υλικό SDR.
3. **Προσομοιωτές πυρήνα:** Open5GS (πλήρης υλοποίηση 5G Core), συχνά με UERANSIM (User Equipment & RAN Simulator) – μαζί προσφέρουν πλήρες αυτόνομο δίκτυο 5G αποκλειστικά μέσω λογισμικού, χωρίς φυσικά radios.
4. **Εργαλεία παραγωγής κίνησης:** D-ITG, iPerf3, TRex, TeraVM, που παράγουν μεγάλο ή προσαρμοσμένο όγκο κίνησης (χρήσιμα για φόρτιση του δικτύου και δημιουργία δεδομένων για ανάλυση).
5. **Περιβάλλοντα εξομοίωσης δικτύου:** Mininet (για εικονικές τοπολογίες δικτύου), Wireshark (για ανάλυση/καταγραφή πραγματικής κίνησης).

Κάθε εργαλείο παίζει συμπληρωματικό ρόλο στην έρευνα 5G και διακρίνεται για συγκεκριμένα πλεονεκτήματα. Για παράδειγμα, τα ns-3 και OMNeT++ είναι εξαιρετικά για λεπτομερή προσομοίωση συμπεριφοράς πρωτοκόλλων, ενώ το srsRAN επιτρέπει πραγματική εκπομπή RF (με υλικό SDR) για πιο ρεαλιστικές δοκιμές RAN. Το ζεύγος Open5GS + UERANSIM προσφέρει ισορροπία, εξομοιώνοντας πλήρες δίκτυο 5G αποκλειστικά σε λογισμικό, με ρεαλιστική IP κίνηση χωρίς εξειδικευμένο υλικό. Εμπορικά εργαλεία όπως το TeraVM αξιολογήθηκαν για την απόδοσή

τους, αλλά μόνο συγκριτικά λόγω περιορισμένης πρόσβασης. Το αποτέλεσμα ήταν μια σαφής λίστα υποψήφιων πλατφορμών που θα αξιολογούνταν στη συνέχεια.

2.2 Ανάπτυξη Πλαισίου Πολυκριτηριακής Αξιολόγησης (MCDA)

Για τη συστηματική σύγκριση των εργαλείων, αναπτύξαμε ένα πλαίσιο αξιολόγησης βασισμένο στην Πολυκριτηριακή Ανάλυση Αποφάσεων (MCDA). Η MCDA παρέχει μια δομημένη και διαφανή μέθοδο σύγκρισης εναλλακτικών με βάση πολλαπλούς παράγοντες, κάτι που είναι ιδανικό όταν απαιτείται επιλογή εργαλείου λαμβάνοντας υπόψη την απόδοση, τη χρηστικότητα κ.ά. Καθορίστηκαν κριτήρια αξιολόγησης που αντικατοπτρίζουν τις βασικές απαιτήσεις για εργαλείο προσομοίωσης/εξομοίωσης κίνησης σε 5G. Αυτά προέκυψαν από τους στόχους απόδοσης του 5G, τις ανάγκες που προέκυψαν από τη βιβλιογραφία και τις πρακτικές απαιτήσεις του δικού μας use-case (κανονική και κακόβουλη κίνηση σε testbed). Κάθε κριτήριο ορίστηκε με ακρίβεια ώστε η αξιολόγηση να είναι αντικειμενική.
Τα κριτήρια που χρησιμοποιήθηκαν στο πλαίσιο είναι:

1. **Δυνατότητα παραγωγής κίνησης:** Ευρεία γκάμα προφίλ και όγκου κίνησης που αναπαριστούν πραγματικά use cases του 5G (TCP/HTTP, UDP, VoIP, IoT flows, ευελιξία προσαρμογής).
2. **Απόδοση & Επεκτασιμότητα:** Ανταπόκριση σε σενάρια μεγάλης κλίμακας, υποστήριξη υψηλής διαμεταγωγής, αποδοτικότητα σε πόρους (CPU, μνήμη).
3. **Ρεαλισμός εξομοίωσης/εξομοίωσης:** Πόσο ρεαλιστικά μοντελοποιείται η συμπεριφορά του δικτύου (real-time emulation vs. abstract simulation).
4. **Ευκολία χρήσης και εγκατάστασης:** Ευκολία παραμετροποίησης, πληρότητα τεκμηρίωσης, ύπαρξη παραδειγμάτων και ενεργής κοινότητας.
5. **Επεκτασιμότητα:** Δυνατότητα προσαρμογής/προσθήκης νέων λειτουργιών και διασύνδεσης με άλλα συστήματα.
6. **Συμβατότητα με εικονικοποίηση/cloud:** Υποστήριξη λειτουργίας σε εικονικά περιβάλλοντα ή cloud.
7. **Ανάλυση καθυστέρησης και jitter:** Δυνατότητα μέτρησης και παραγωγής ρεαλιστικών χρονικών συμπεριφορών.
8. **Υποστήριξη ασφάλειας και προσομοίωσης επιθέσεων:** Υποστήριξη για σενάρια ασφαλείας και παραγωγή/αναγνώριση κακόβουλης κίνησης.
9. **Δυνατότητες παρακολούθησης/αναφορών:** Εργαλεία για logging, ανάλυση και απεικόνιση της συμπεριφοράς του δικτύου.
10. **Κοινότητα και τεκμηρίωση:** Ποιότητα και πληρότητα εγχειριδίων/κοινότητας.

Σε κάθε κριτήριο αποδόθηκε σχετική βαρύτητα, με βάση τόσο τις ανάγκες του έργου όσο και τις προτεραιότητες της βιβλιογραφίας (με αυξημένη έμφαση στην απόδοση και την ασφάλεια λόγω της φύσης του use-case). Οι σταθμισμένες βαθμολογίες εξασφαλίζουν ότι η τελική αξιολόγηση αντανακλά ό,τι έχει μεγαλύτερη σημασία για τη δημιουργία ρεαλιστικού 5G testbed.

2.3 Βαθμολόγηση Εργαλείων και Εφαρμογή MCDA

Με το παραπάνω πλαίσιο, ακολουθήσαμε μια συστηματική διαδικασία βαθμολόγησης κάθε εργαλείου. Για κάθε εργαλείο (ns-3, OMNeT++/Simu5G, srsRAN, Open5GS+UERANSIM κ.ά.),

συλλέξαμε πληροφορίες από τεκμηρίωση, εγχειρίδια, ακαδημαϊκές μελέτες και συγκριτικές αναλύσεις. Για παράδειγμα, ανατρέξαμε σε project sites (π.χ. ns-3, Open5GS) για δυνατότητες και δραστηριότητα κοινότητας, και σε δημοσιεύσεις για δεδομένα απόδοσης (όρια throughput, μέγεθος σεναρίων που έχουν υλοποιηθεί). Φόρουμ και release notes βοήθησαν στην εκτίμηση ευκολίας χρήσης και επεκτασιμότητας, λαμβάνοντας υπόψη γνωστά προβλήματα/περιορισμούς.
Κάθε εργαλείο βαθμολογήθηκε σε κλίμακα 0–5 για κάθε κριτήριο (με το 5 να δηλώνει την καλύτερη απόδοση). Για να μειωθεί η υποκειμενικότητα, οι βαθμολογίες βασίστηκαν σε τεκμηριωμένες πηγές ή δημοσιευμένα αποτελέσματα. Για παράδειγμα, αν μελέτη έδειχνε ότι το ns-3 5G-LENA διαχειρίζεται X αριθμό UEs ή κάποιο throughput, αυτό μεταφραζόταν σε ανάλογη βαθμολογία επεκτασιμότητας. Σε αμφιλεγόμενες περιπτώσεις, ακολουθήθηκε συντηρητική εκτίμηση και σημειώθηκε η αβεβαιότητα.
Αφού βαθμολογήθηκαν τα εργαλεία, εφαρμόστηκε η σταθμισμένη MCDA – κάθε βαθμολογία πολλαπλασιάστηκε με τη βαρύτητα του κριτηρίου και οι επιμέρους βαθμολογίες αθροίστηκαν για το τελικό σκορ. Έτσι προέκυψε μια κατάταξη από το πιο κατάλληλο στο λιγότερο κατάλληλο εργαλείο. Η βαθμολόγηση διασταυρώθηκε με ανάλυση ευαισθησίας: αλλάζοντας τα βάρη (π.χ. αυξάνοντας τη βαρύτητα στην απόδοση ή την ευκολία χρήσης) εξετάστηκε αν μεταβαλλόταν σημαντικά η κατάταξη, ώστε να διασφαλιστεί η αξιοπιστία της επιλογής.
Το αποτέλεσμα έδειξε καθαρά ότι το ζεύγος Open5GS + UERANSIM ήταν η καταλληλότερη λύση για τις ανάγκες μας. Ήταν κορυφαίο σε κρίσιμους τομείς όπως παραγωγή κίνησης, ρεαλισμός (real-time 5G stack), υποστήριξη virtualization, κοινότητα/τεκμηρίωση και δυνατότητες ασφάλειας (δοκιμές authentication, προσομοίωση επιθέσεων). Αντίθετα, το ns-3 και το OMNeT++ παρείχαν μεγάλη επεκτασιμότητα αλλά υστερούσαν στον ρεαλισμό της κίνησης και είχαν μεγαλύτερη καμπύλη εκμάθησης για χρήση σε live testbed. Το srsRAN απαιτούσε εξειδικευμένο RF hardware, κάτι λιγότερο βολικό για καθαρά software δοκιμές. Συνεπώς, βάσει MCDA και πρακτικών παραμέτρων, το Open5GS + UERANSIM προκρίθηκε ως η βέλτιστη λύση για το πειραματικό σκέλος.

2.4 Σχεδιασμός Πειραματικής διάταξης του Testbed

Το Open5GS υλοποιεί πλήρως τις λειτουργίες του 5G Core (AMF, SMF, UPF κ.λπ.) και έχει υιοθετηθεί ευρέως για ιδιωτικά 5G δίκτυα λόγω ευελιξίας και δυνατής κοινότητας. Το UERANSIM το συμπληρώνει προσομοιώνοντας το RAN, παρέχοντας λογισμικό gNB (βάση) και UE που καταχωρούνται στον core και ανταλλάσσουν κίνηση μέσω τυπικών διαδικτυακών πρωτοκόλλων (SCTP, UDP/IP) χωρίς φυσικό εξοπλισμό radio. Ο συνδυασμός αυτός δημιουργεί ένα πλήρες, αυτόνομο δίκτυο 5G σε λογισμικό – το UE και το gNB στο UERANSIM λειτουργούν σαν πραγματικές συσκευές που επικοινωνούν με τον core μέσω διεπαφών 3GPP, δημιουργώντας PDU sessions που μεταφέρουν IP κίνηση.
Το testbed σχεδιάστηκε για να αξιοποιήσει το παραπάνω toolset με αρθρωτή και επεκτάσιμη αρχιτεκτονική. Τα βασικά σημεία σχεδιασμού ήταν: (α) εξομοίωση πλήρους end-to-end δικτύου 5G (UE ↔ RAN ↔ 5G Core ↔ Data Network) μέσω λογισμικού, και (β) δυνατότητα παραγωγής τόσο κανονικής όσο και κακόβουλης κίνησης για αξιολόγηση. Η αρχιτεκτονική περιλαμβάνει διακριτές εικονικές μηχανές (VMs) που αναπαριστούν τα διάφορα network functions, ώστε να προσομοιώνεται ρεαλιστική υλοποίηση και να διευκολύνεται η αυτόνομη ανάλυση κάθε μέρους. Η διάσπαση αυτή ευθυγραμμίζεται με cloud-native προσέγγιση, όπου core και RAN λειτουργούν σε ξεχωριστά instances.

Το τελικό testbed περιλαμβάνει τρείς βασικούς κόμβους (instances λογισμικού), καθένας ως VM Linux στον ίδιο φυσικό server:

1. **5G Core (Open5GS Module):** Τρέχει τις βασικές υπηρεσίες του core (AMF, SMF, UPF, AUSF, NRF, κ.λπ.), με MongoDB για δεδομένα συνδρομητών και συνεδριών. Οι ρυθμίσεις περιλάμβαναν προφίλ συνδρομητών για τα UE του UERANSIM.
2. **5G RAN & UE Simulator (UERANSIM Module):** Εξομοιώνει ένα gNodeB και πολλαπλά UE, τα οποία συνδέονται στον core μέσω N2 (SCTP) και N3 (UDP/IP). Κάθε UE παίρνει IP από το pool του core και ανταλλάσσει κίνηση.
3. **Traffic Server (localhosted):** Στον ρόλο του Traffic Server, εγκαταστάθηκε ένας ελαφρύς HTTP server (Apache ή Nginx) που σερβίρει στατικές σελίδες και αρχεία, καθώς και ένα απλό UDP echo service (ή εναλλακτικά χρησιμοποιήθηκε το ίδιο το iperf σε server mode για UDP).

Όλα τα modules φιλοξενήθηκαν στον ίδιο φυσικό server (x86_64, Ubuntu 20.04 LTS) με πλατφόρμα virtualization (KVM/QEMU), για ελαχιστοποίηση latencies και συγχρονισμό. Εικονικά switches (Linux bridge/OVS) διασύνδεσαν τα modules σύμφωνα με την αρχιτεκτονική 5G: ένα switch για RAN↔Core (N2/N3), άλλο για Core's N6↔Traffic Server/IDS. Τοπολογία μεμονωμένων links για διακριτό έλεγχο και ρεαλιστική προσομοίωση. Διορθώθηκαν routing/NAT και MTU ώστε τα UE να επικοινωνούν end-to-end και το μελλοντικό IDS να μπορεί να λάβει αντίγραφα όλων των ροών user-plane.
Με το testbed σε λειτουργία, σχεδιάστηκαν σενάρια για αξιολόγηση τόσο της κανονικής λειτουργίας όσο και της συμπεριφοράς του δικτύου υπό πίεση (κακόβουλη κίνηση). Τα δύο βασικά traffic types ήταν: HTTP broadband traffic (τυπική χρήση χρήστη) και UDP flood (άσκηση επίθεσης DoS).
Για το σενάριο κανονικής κίνησης, προσομοιώνεται η φυσιολογική χρήση του δικτύου από έναν τυπικό χρήστη, χωρίς κακόβουλη δραστηριότητα. Το UE συνδέεται στο δίκτυο 5G, αποκτά IP, και εκκινεί πολλαπλές ροές δεδομένων προς τον server (HTTP, download αρχείου, UDP streaming και ping), δημιουργώντας ένα σύνθετο και ρεαλιστικό traffic pattern για πέντε λεπτά. Κατά τη διάρκεια του σεναρίου δεν εκτελείται κάποια επίθεση, οπότε το δίκτυο λειτουργεί ομαλά και χωρίς σφάλματα.

Για το κακόβουλο σενάριο, προσομοιώνεται επίθεση DDoS από το UE προς τον server, με στόχο την καταπόνηση του δικτύου. Αρχικά παράγεται φυσιολογική κίνηση για 1 λεπτό, και στη συνέχεια το UE ξεκινά κακόβουλο traffic, κυρίως μέσω UDP Flood (~2 λεπτά), με μαζική αποστολή πακέτων για να κορεστεί το bandwidth. Επίσης εξετάζονται και άλλες μορφές επιθέσεων (TCP SYN και ICMP Flood), με αποτέλεσμα τη σημαντική υποβάθμιση ή διακοπή της κανονικής κίνησης, προσομοιώνοντας μια ρεαλιστική περίπτωση διατάραξης της ποιότητας υπηρεσίας.

Τα πειράματα διαρθρώθηκαν σε δύο φάσεις: πρώτα baseline με μόνο κανονικό HTTP traffic, έπειτα φάση επίθεσης με UDP flood ταυτόχρονα με το HTTP. Κάθε run διαρκούσε αρκετά λεπτά για σταθεροποίηση. Η εκκίνηση UERANSIM, καταχώρηση UEs, παραγωγή traffic και ενεργοποίηση IDS έγιναν script-αρισμένα για επαναληψιμότητα. Μεταξύ runs, το περιβάλλον καθαριζόταν (reset Open5GS, επανασύνδεση UEs).

Κατά την εκτέλεση των παραπάνω σεναρίων, έγινε συστηματική συλλογή δεδομένων και μετρήσεων για την αξιολόγηση της απόδοσης του συστήματος. Πρωτίστως, έγινε καταγραφή της *δικτυακής κίνησης* μέσω packet capture (pcap) τόσο στο interface του UE (uesimtun0) όσο και στο interface του server. Χρησιμοποιήθηκε το tcpdump για την αποθήκευση όλων των πακέτων σε αρχεία .pcap, επιτρέποντάς μας εκ των υστέρων ανάλυση με Wireshark. Επίσης, ενεργοποιήθηκαν κάποια logs στο Open5GS (debug mode για UPF) ώστε να παρατηρήσουμε τυχόν μηνύματα σφάλματος ή drop στο επίπεδο του πυρήνα 5G.

Για πιο υψηλού επιπέδου αποτύπωση της κίνησης, αξιοποιήθηκε το εργαλείο CICFlowMeter offline, το οποίο αναλύει τα pcap αρχεία και εξάγει *ροές (flows)* με περισσότερα από 80 στατιστικά χαρακτηριστικά ανά ροή. Αυτό μας επέτρεψε να αποκτήσουμε αριθμοποιημένα μεγέθη όπως μέσο ρυθμό κάθε ροής, διακυμάνσεις, κατανομή πακέτων, κ.λπ., που είναι χρήσιμα για συγκριτική αξιολόγηση (π.χ. να συγκρίνουμε τα flow stats στην κανονική κίνηση έναντι στην επίθεση). Επιπρόσθετα, παρακολουθήσαμε σε πραγματικό χρόνο τους *συστήματος πόρους*: χρήση CPU και μνήμης στον Core (ιδίως η διεργασία του UPF) και στον Traffic Server, με εργαλεία όπως htop και sar. Καταγράψαμε ενδεικτικές τιμές κατά τη διάρκεια των πειραμάτων (π.χ. μέγιστο % CPU). Η καθυστέρηση δικτύου υπολογίστηκε από τα ping που έστελνε το UE (RTT κάθε 1 δευτ.), ενώ η απώλεια πακέτων εκτιμήθηκε τόσο από το output του ping (packet loss%) όσο και από την ανάλυση των pcaps για χαμένες ή μη απαντημένες αιτήσεις.

3. Εξέλιξη των τεχνολογιών που απαρτίζουν τη Δημιουργία Δικτυακής Κίνησης

3.1 Πορεία Εξέλιξης της Δικτυακής Κίνησης

3.1.1 Εισαγωγή στη δημιουργία δικτυακής κίνησης

Η δημιουργία δικτυακής κίνησης (Network Traffic Generation) είναι ένα κρίσιμο πεδίο στο πλαίσιο της μηχανικής δικτύου, που εξυπηρετεί τις ανάγκες δοκιμών, αξιολόγησης και ασφάλειας των συστημάτων δικτύου σε ένα ευρύ φάσμα παραδειγμάτων. Αυτή η διαδικασία περιλαμβάνει τη δημιουργία ή την αναπαραγωγή προτύπων κίνησης δικτύου για την προσομοίωση πραγματικών συνθηκών για διάφορους σκοπούς, όπως η συγκριτική αξιολόγηση των επιδόσεων, ο έλεγχος της συμφόρησης και οι δοκιμές ασφάλειας στον κυβερνοχώρο.

Καθώς η τεχνολογία των δικτύων εξελίσσεται, αυξάνεται και η πολυπλοκότητα των τεχνικών παραγωγής κίνησης, οδηγούμενη από τις ποικίλες ανάγκες των αναδυόμενων εφαρμογών, από τα πρώιμα δίκτυα μεταγωγής πακέτων στα σημερινά συστήματα 5G. Αυτό το κεφάλαιο διερευνά το ιστορικό πλαίσιο της δημιουργίας δικτυακής κίνησης, εξετάζοντας την εξέλιξή του με την πάροδο του χρόνου και τις τεχνολογικές κινητήριες δυνάμεις που το έχουν διαμορφώσει.

3.1.2 Απαρχές του Network Traffic Generation (1970s 1980s)

Η έννοια της δημιουργίας δικτυακής κίνησης χρονολογείται από τη δεκαετία του 1970, μια περίοδο που χαρακτηρίστηκε από την πρώιμη ανάπτυξη δικτύων υπολογιστών όπως το ARPANET, το οποίο έθεσε τις βάσεις για το σημερινό Διαδίκτυο. Η αρχική εστίαση ήταν στη δοκιμή της βασικής συνδεσιμότητας του δικτύου, με τη δημιουργία κίνησης να είναι μια απλή διαδικασία αποστολής πακέτων μέσω ενσύρματων συνδέσεων για την παρατήρηση της ροής δεδομένων και τη μέτρηση του λανθάνοντος χρόνου.
Οι ερευνητές δημιούργησαν κυρίως πακέτα σταθερού μεγέθους σε σταθερά χρονικά διαστήματα για να αξιολογήσουν τη σταθερότητα του δικτύου, την αξιοπιστία και τις βασικές μετρήσεις απόδοσης, όπως το εύρος ζώνης και η απώλεια πακέτων. Τα πρωτόκολλα ήταν περιορισμένα, με τα πρώιμα σχέδια δικτύου να βασίζονται στο NCP (Network Control Protocol), προκάτοχο της σουίτας TCP/IP[16].

Κατά τη διάρκεια αυτής της περιόδου, τα εργαλεία δημιουργίας κίνησης ήταν σε μεγάλο βαθμό χειροκίνητα και πειραματικά, καθώς οι αρχιτεκτονικές δικτύου ήταν στοιχειώδεις και ως επί το πλείστον περιορίζονταν σε ακαδημαϊκή και στρατιωτική χρήση. Οι πρώτες προσεγγίσεις για τη δημιουργία κίνησης ήταν συχνά προσαρμοσμένες, με τους ερευνητές να δημιουργούν βασικά εργαλεία για την αξιολόγηση νέων τεχνολογιών μεταγωγής πακέτων. Το περιορισμένο πεδίο εφαρμογής των πρώιμων εφαρμογών δικτύου σήμαινε ότι αυτά τα εργαλεία επικεντρώθηκαν κυρίως σε μετρήσεις χαμηλού επιπέδου χωρίς την ποικιλομορφία του επιπέδου εφαρμογής που παρατηρήθηκε τα επόμενα χρόνια.

3.1.3 Ανάπτυξη τεχνικών δημιουργίας κίνησης στην εποχή TCP/IP (δεκαετία του 1990)

Με την ευρεία υιοθέτηση της στοίβας TCP/IP στη δεκαετία του 1990, η δικτύωση σημείωσε σημαντική επέκταση στους τύπους εφαρμογών και πρωτοκόλλων που χρησιμοποιούνται, συμπεριλαμβανομένων των http, FTP και DNS, γεγονός που εισήγαγε μεγαλύτερη πολυπλοκότητα στην κίνηση δικτύου. Η εμφάνιση του εμπορικού Διαδικτύου οδήγησε στην ανάγκη για εργαλεία δημιουργίας κίνησης που θα μπορούσαν να προσομοιώσουν ρεαλιστική κίνηση επιπέδου εφαρμογής, επιτρέποντας στους ερευνητές και τους διαχειριστές δικτύων να μελετήσουν την απόδοση διαφορετικών δικτυακών υπηρεσιών. Ως αποτέλεσμα, η δεκαετία του 1990 είδε την ανάπτυξη πρώιμων εργαλείων δημιουργίας κίνησης που σχεδιάστηκαν για να μιμηθούν τα πρωτόκολλα TCP και UDP.
Η εισαγωγή εργαλείων όπως το Iperf και το Netperf παρείχαν πιο εξελιγμένες δυνατότητες για τη μέτρηση της απόδοσης, του λανθάνοντος χρόνου και του jitter, επιτρέποντας στους ερευνητές να ποσοτικοποιούν την απόδοση του δικτύου υπό ποικίλες συνθήκες [17]. Αυτά τα εργαλεία επέτρεψαν προσομοιώσεις εφαρμογών έντασης εύρους ζώνης και παρείχαν πληροφορίες σχετικά με τη συμφόρηση και τις συμπεριφορές ουράς, κρίσιμους παράγοντες για την αυξανόμενη χρήση του Διαδικτύου. Οι διαχειριστές και οι ερευνητές του δικτύου άρχισαν να χρησιμοποιούν εκτενώς αυτά τα εργαλεία για τις βασικές δοκιμές και την αξιολόγηση της απόδοσης.
Κατά τη διάρκεια αυτής της περιόδου, η εξομοίωση δικτύου έγινε επίσης πιο δημοφιλής καθώς αναγνωρίστηκε η σημασία της αναδημιουργίας πραγματικών συνθηκών δικτύου, όπως η απώλεια πακέτων και η μεταβλητότητα του λανθάνοντος χρόνου. Τα εργαλεία άρχισαν να υποστηρίζουν προσομοιωμένες καθυστερήσεις και παρεμβολές δικτύου, επιτρέποντας πιο ακριβείς αναπαραστάσεις των συνδέσεων Δικτύου Ευρείας Περιοχής (WAN) και των δορυφορικών συνδέσεων. Αυτή η επέκταση των δυνατοτήτων δημιουργίας κίνησης διαδραμάτισε καθοριστικό ρόλο στην ανάπτυξη μηχανισμών πρώιμης ποιότητας υπηρεσιών (QoS) που επεδίωκαν να δώσουν προτεραιότητα σε ορισμένους τύπους κίνησης σε δίκτυα με συμφόρηση.

3.1.4 Η άνοδος των εφαρμογών πολυμέσων και διαδικτύου (2000s)

Η δεκαετία του 2000 επέφερε μια μετασχηματιστική στροφή στη δικτύωση με την ταχεία ανάπτυξη εφαρμογών πολυμέσων, συμπεριλαμβανομένης της ροής βίντεο, της φωνής μέσω IP (VoIP) και των διαδικτυακών τυχερών παιχνιδιών. Αυτή η μετατόπιση δημιούργησε την ανάγκη για προηγμένα εργαλεία δημιουργίας κίνησης που θα μπορούσαν να προσομοιώσουν σύνθετα πρότυπα κυκλοφορίας αντιπροσωπευτικά αυτών των διαφορετικών εφαρμογών. Εργαλεία όπως το D-ITG (Distributed Internet Traffic Generator) αναπτύχθηκαν για να υποστηρίξουν τη

δημιουργία κίνησης επιπέδου εφαρμογής, συμπεριλαμβανομένων πρωτοκόλλων όπως HTTP, FTP και RTP [18].
Το D-ITG και παρόμοια εργαλεία επέτρεψαν στους ερευνητές να ελέγχουν παραμέτρους επιπέδου πακέτων και να προσομοιώνουν συμπεριφορές δικτύου για συγκεκριμένες εφαρμογές. Η δυνατότητα δημιουργίας κίνησης σε πολλαπλά επίπεδα του μοντέλου OSI - όπως η μεταφορά (TCP / UDP) και η εφαρμογή (HTTP / VoIP) - επέτρεψε στους ερευνητές να μελετήσουν μετρήσεις απόδοσης όπως η λανθάνουσα κατάσταση,το jitter και την απώλεια πακέτων για εφαρμογές πολυμέσων, οι οποίες ήταν ευαίσθητες στις συνθήκες δικτύου. Αυτή η εξέλιξη ήταν κρίσιμη για την καθιέρωση μετρήσεων για QoS σε δίκτυα πολυμέσων, βοηθώντας στην ιεράρχηση της ευαίσθητης στην καθυστέρηση κυκλοφορίας.
Η δεκαετία του 2000 είδε επίσης την άνοδο της επανάληψης της κίνησης **traffic replay**, όπου η προηγουμένως καταγεγραμμένη κίνηση δικτύου αναπαράχθηκε σε δοκιμαστικά περιβάλλοντα. Αυτή η προσέγγιση επέτρεψε στους ερευνητές να αναπαράγουν τις πραγματικές συνθήκες δικτύου με μεγαλύτερη ακρίβεια, καθώς η αναπαραγόμενη κίνηση αντικατόπτριζε τις πραγματικές συμπεριφορές και το χρονοδιάγραμμα των χρηστών.
Το Tcpreplay, για παράδειγμα, έγινε ένα δημοφιλές εργαλείο για την αναπαραγωγή 2συλλήψεων πακέτων, επιτρέποντας ρεαλιστικά σενάρια δοκιμών σε συστήματα ανίχνευσης εισβολής (IDS) και τείχη προστασίας (Masumi K, Han C[19]). Οι τεχνικές επανάληψης κίνησης επέτρεψαν στους ερευνητές να κατανοήσουν πώς τα δίκτυα θα ανταποκρίνονταν σε πραγματικά μοτίβα επίθεσης και να αξιολογήσουν την ακρίβεια του IDS υπό ρεαλιστικές συνθήκες.

3.1.5 Εικονικοποίηση και εισαγωγή του NFV (δεκαετία του 2010)

Στη δεκαετία του 2010, η υποδομή δικτύου υπέστη σημαντική εξέλιξη με την έλευση του **Network Function Virtualization** (NFV). Το NFV αποσυνδέει τις λειτουργίες δικτύου από το αποκλειστικό υλικό και τους επιτρέπει να εκτελούνται ως λογισμικό σε διακομιστές εμπορευμάτων, καθιστώντας τα δίκτυα πιο ευέλικτα, επεκτάσιμα και οικονομικά αποδοτικά. Το NFV μετατόπισε τις απαιτήσεις στα εργαλεία δημιουργίας κίνησης, τα οποία έπρεπε να προσομοιώσουν δυναμικά, εικονικά περιβάλλοντα όπου οι λειτουργίες δικτύου (π.χ. τείχη προστασίας, εξισορροπητές φορτίου, δρομολογητές) θα μπορούσαν να αναπτυχθούν γρήγορα, να κλιμακωθούν και να προσαρμοστούν ως απάντηση στα μεταβαλλόμενα μοτίβα κυκλοφορίας [20].
Τα εργαλεία δημιουργίας κίνησης, όπως το Cisco TRex, σχεδιάστηκαν για να ικανοποιήσουν τις ανάγκες των περιβαλλόντων NFV, προσφέροντας δυνατότητες δημιουργίας κίνησης χωρίς κατάσταση και κατάσταση για την προσομοίωση ενός ευρέος φάσματος λειτουργιών δικτύου υπό φορτίο. Το TRex επιτρέπει τον ακριβή έλεγχο των ροών πακέτων, επιτρέποντας στους ερευνητές να αναπαράγουν συμπεριφορές υψηλής απόδοσης και εφαρμογών κατάστασης που είναι χαρακτηριστικές των περιβαλλόντων NFV και cloud3). Επιπλέον, το NFV δημιούργησε την ανάγκη για προσαρμοστική δημιουργία κίνησης, καθώς οι λειτουργίες δικτύου έπρεπε να δοκιμαστούν σε συνθήκες όπου οι εικονικοί πόροι θα μπορούσαν να κατανεμηθούν ή να αφαιρεθούν σε πραγματικό χρόνο.
Το NFV άνοιξε επίσης το δρόμο για τον τεμαχισμό του δικτύου στο 5G, όπου ξεχωριστά εικονικά δίκτυα τρέχουν σε μια κοινή φυσική υποδομή, το καθένα προσαρμοσμένο σε συγκεκριμένες εφαρμογές ή ομάδες χρηστών. Η δημιουργία κίνησης σε περιβάλλοντα NFV απαιτεί εργαλεία που

2 https://trex-tgn.cisco.com
3 https://trex-tgn.cisco.com/

μπορούν να προσαρμοστούν σε διαφορετικά επίπεδα QoS, κατανομή πόρων και απαιτήσεις σε πραγματικό χρόνο, ιδιαίτερα σε περιβάλλοντα cloud πολλαπλών μισθωτών (Riggio, Rasheed, & Narayanan, 2016[21]).

3.1.6 Μηχανική μάθηση και προσαρμοστική δημιουργία κίνησης (τέλη της δεκαετίας του 2010 σήμερα)

Τα τελευταία χρόνια έχει παρατηρηθεί η ενσωμάτωση της μηχανικής μάθησης (ML) και της τεχνητής νοημοσύνης (AI) στη δημιουργία κίνησης δικτύου. Αυτές οι τεχνολογίες επιτρέπουν τη δημιουργία κίνησης που μαθαίνει από δεδομένα πραγματικού κόσμου και παράγει συνθετικά μοτίβα κίνησης που μιμούνται στενά τις πραγματικές συνθήκες δικτύου. Τα Generative Adversarial Networks (GANs), ειδικότερα, έχουν εφαρμοστεί στη δημιουργία κίνησης δικτύου, επιτρέποντας τη δημιουργία ρεαλιστικών μοτίβων κίνησης που βοηθούν στην εκπαίδευση και την αξιολόγηση λύσεων ασφάλειας που βασίζονται σε ML[22].
Η δημιουργία κίνησης με γνώμονα την τεχνητή νοημοσύνη ήταν ιδιαίτερα πολύτιμη στην έρευνα ανίχνευσης ανωμαλιών, όπου η ρεαλιστική συνθετική κίνηση με ενσωματωμένες ανωμαλίες μπορεί να εκπαιδεύσει τα μοντέλα ML να εντοπίζουν και να ανταποκρίνονται σε απειλές ασφαλείας. Με την προσομοίωση προσαρμοστικών, απρόβλεπτων μοτίβων κυκλοφορίας, οι γεννήτριες που βασίζονται σε ML παρέχουν ένα νέο επίπεδο δυναμισμού και ρεαλισμού στις δοκιμές δικτύου, ζωτικής σημασίας για τα πολύπλοκα περιβάλλοντα υψηλής ταχύτητας που χαρακτηρίζουν τα σύγχρονα δίκτυα[23].

3.1.7 Παραγωγή δικτυακής κίνησης 5G (σήμερα)

Η ανάπτυξη των δικτύων 5G εισήγαγε νέες απαιτήσεις για τη δημιουργία κίνησης λόγω της έμφασης του 5G σε δεδομένα υψηλής ταχύτητας, εξαιρετικά χαμηλή καθυστέρηση, και μαζική συνδεσιμότητα IoT. Οι γεννήτριες κίνησης στο 5G πρέπει να αντιμετωπίσουν:

- **Network Slicing**: Με τον τεμαχισμό δικτύου, διαφορετικά εικονικά δίκτυα (slice) βελτιστοποιούνται για ξεχωριστές υπηρεσίες, όπως βελτιωμένη κινητή ευρυζωνική σύνδεση (eMBB), εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (URLLC) και μαζικές επικοινωνίες τύπου μηχανής (mMTC). Κάθε slice απαιτεί συγκεκριμένα χαρακτηριστικά κίνησης και μετρήσεις QoS.
- **Mobility and Handover Testing**: Τα δίκτυα 5G πρέπει να χειρίζονται υψηλή κινητικότητα, με απρόσκοπτες μεταβιβάσεις μεταξύ κυψελών και διαφορετικών φετών. Οι γεννήτριες κίνησης για 5G συχνά προσομοιώνουν την κίνηση των χρηστών και τις συχνές μεταβιβάσεις για να ελέγξουν την απόδοση και τον λανθάνοντα χρόνο του δικτύου υπό αυτές τις δυναμικές συνθήκες.
- **Cybersecurity Challenges**: Με αυξημένο εύρος ζώνης και πυκνότητα συσκευών, τα δίκτυα 5G είναι πιο ευάλωτα σε εξελιγμένες επιθέσεις στον κυβερνοχώρο. Οι σύγχρονες γεννήτριες κίνησης πρέπει να προσομοιώνουν τόσο την καλοήθη όσο και την κακόβουλη κίνηση, συμπεριλαμβανομένων των επιθέσεων DDoS και της μη εξουσιοδοτημένης πρόσβασης, για να αξιολογήσουν την ασφάλεια και την ανθεκτικότητα της υποδομής 5G.

Modern Tools for 5G Traffic Generation:

Tool	5G Integration Level	Platform	Traffic Category
ns-3 with 5G-LENA Module	High	Linux, Unix	Model-based simulation
srsRAN	High	Linux	Script-driven simulation
Open5GS with UERANSIM	High	Linux, Unix	Model-based, Emulation
OMNeT++ with Simu5G	High	Cross-platform	Model-based simulation
TRex	Medium	Linux	Script-driven generator
Mininet with SDN	Medium	Linux	Network emulator
TeraVM	High (Commercial)	Linux, Windows	Hybrid generator/emulator
Wireshark	Medium	Cross-platform	Packet capture & analysis
Iperf3	Low	Cross-platform	Constant throughput generator
Scapy	Medium	Cross-platform	Script-driven generator
D-ITG	Low	Cross-platform	Model-based generator

Metasploit	Medium	Cross-platform	Attack generator
LOIC (Low Orbit Ion Cannon)	Low	Cross-platform	Attack generator

ns-3 with 5G-LENA Module	5G RAN and core simulation, including network slicing and mobility scenarios.
srsRAN	Full 5G stack (RAN and core), ideal for detailed 5G emulation and resource slicing scenarios.
Open5GS with UERANSIM	Supports core 5G network and User Equipment (UE) simulation, allows RAN integration and core-to-edge testing.
OMNeT++ with Simu5G	Detailed 5G simulations with UE, RAN, and core components, suited for studying network resilience in 5G contexts.
TRex	Can generate realistic 5G traffic patterns, with features for testing data plane throughput under 5G-like loads.
Mininet with SDN	Supports SDN-enabled 5G network simulations, useful for edge and core network configuration and testing.
TeraVM	Emulates high-fidelity 5G traffic loads and IoT environments, supports scalability and real-world traffic behaviors.
Wireshark	Captures and analyzes packets, valuable for assessing real-time performance and security in 5G traffic scenarios.
Iperf3	Generates TCP/UDP traffic; while generic, it is usable for measuring throughput in various 5G network segments.
Scapy	Customizable packet crafting, enabling simulation of both legitimate and attack traffic within a 5G framework.
D-ITG	Simulates various traffic conditions; usable in 5G scenarios to evaluate network performance under variable loads.

Metasploit	Provides tools for penetration testing in 5G networks, enabling targeted security assessment.
LOIC (Low Orbit Ion Cannon)	Used for generating high-volume traffic (DDoS); applicable for stress-testing security features in 5G environments.

3.2 Κύριες τεχνολογίες για τη δημιουργία δικτυακής κίνησης

3.2.1 Εισαγωγή

Η ανάπτυξη των δικτύων 5G έχει εισαγάγει πρωτοφανείς δυνατότητες όσον αφορά τους ρυθμούς δεδομένων, τον λανθάνοντα χρόνο και τη συνδεσιμότητα των συσκευών. Ωστόσο, οι δοκιμές και η επικύρωση αυτών των δυνατοτήτων απαιτούν προηγμένες τεχνολογίες παραγωγής κίνησης που μπορούν να προσομοιώσουν ρεαλιστικές συνθήκες δικτύου 5G. Οι γεννήτριες κίνησης για 5G βασίζονται σε διάφορες βασικές τεχνολογίες, όπως η εικονικοποίηση, ο τεμαχισμός δικτύου, η προσομοίωση δικτύου ραδιοπρόσβασης (RAN) και τα αναλυτικά στοιχεία που βασίζονται στη μηχανική μάθηση. Αυτό το κεφάλαιο εξετάζει αυτές τις βασικές τεχνολογίες, τους ρόλους τους στη δημιουργία δικτυακής κίνησης 5G και τα οφέλη που προσφέρουν στη δοκιμή και την επικύρωση των δικτύων 5G.[24]

3.2.2 Virtualization and Network Function Virtualization (NFV)

Η εικονικοποίηση, ιδιαίτερα η εικονικοποίηση λειτουργιών δικτύου (NFV), είναι θεμελιώδης για την αρχιτεκτονική 5G. Η NFV διαχωρίζει τις λειτουργίες δικτύου από το ιδιόκτητο υλικό και τους επιτρέπει να εκτελούνται ως λογισμικό σε διακομιστές γενικού σκοπού. Αυτή η ευελιξία είναι ζωτικής σημασίας για το 5G, όπου οι πάροχοι υπηρεσιών πρέπει να υποστηρίζουν ποικίλες εφαρμογές και να διαχειρίζονται δυναμικά τους πόρους του δικτύου για να ανταποκρίνονται στην κυμαινόμενη ζήτηση [25].

Η NFV επιτρέπει την ανάπτυξη εικονικών στιγμιότυπων λειτουργιών δικτύου όπως τείχη προστασίας, δρομολογητές και εξισορροπητές φορτίου. Με τη χρήση εικονικών περιβαλλόντων, οι γεννήτριες κίνησης μπορούν να δημιουργήσουν μια ποικιλία συνθηκών δικτύου, από δίκτυα άκρων χαμηλής καθυστέρησης έως δίκτυα πυρήνα υψηλής απόδοσης, μιμούμενοι πραγματικές περιπτώσεις χρήσης 5G.

Οι γεννήτριες κίνησης σε περιβάλλοντα NFV πρέπει να προσαρμόζουν τις αλλαγές σε πραγματικό χρόνο, καθώς οι λειτουργίες δικτύου μπορούν να προσαρμόζονται, να κλιμακώνονται ή να αναδιατάσσονται δυναμικά με βάση το φορτίο δικτύου. Για παράδειγμα, η γεννήτρια κίνησης TRex της Cisco έχει σχεδιαστεί για να χειρίζεται εφαρμογές υψηλής απόδοσης και κατάστασης, καθιστώντας την κατάλληλο εργαλείο για εικονικά δίκτυα 5G όπου οι απαιτήσεις κίνησης μπορεί να διαφέρουν σημαντικά (Cisco Systems, 2021).

Τα VNF επιτρέπουν διαφορετικούς τύπους δημιουργίας κίνησης προσαρμοσμένων σε συγκεκριμένες εφαρμογές. Ένας VNF που προσομοιώνει ένα τείχος προστασίας, για παράδειγμα, μπορεί να δοκιμαστεί τόσο με καλοήθη όσο και με κακόβουλη κίνηση για να αξιολογήσει την απόδοσή του υπό ρεαλιστικές συνθήκες. Εργαλεία όπως το srs-RAN επιτρέπουν την εξομοίωση εικονικών στοιχείων RAN, παρέχοντας πληροφορίες σχετικά με τον τρόπο λειτουργίας των VNF που σχετίζονται με το RAN σε δυναμικά σενάρια 5G[21]).

Η NFV επιτρέπει την υποστήριξη πολλαπλών υπηρεσιών, η οποία είναι κρίσιμη για την προσομοίωση διαφορετικών τμημάτων δικτύου με απομονωμένες ροές κυκλοφορίας. Οι γεννήτριες κίνησης που βασίζονται στις αρχές NFV επιτρέπουν στους ερευνητές να δοκιμάσουν την κατανομή των πόρων και την απομόνωση της κίνησης σε περιβάλλοντα πολλαπλών ενοικιαστών, που είναι απαραίτητα για τη διασφάλιση της απόδοσης σε δίκτυα 5G υψηλής πυκνότητας.
Με την εικονικοποίηση των λειτουργιών δικτύου, οι γεννήτριες κίνησης που βασίζονται σε NFV μπορούν να προσομοιώσουν τις βλάβες του δικτύου και την ανάκτηση σε πραγματικό χρόνο. Αυτό είναι ζωτικής σημασίας για την αξιολόγηση της ανθεκτικότητας του 5G και τη διασφάλιση ότι οι κρίσιμες υπηρεσίες παραμένουν λειτουργικές ακόμη και υπό συνθήκες έντονης κυκλοφορίας ή επίθεσης[26].

3.2.3. Software-Defined Networking (SDN)

Το Software Defined Networking (SDN) διαχωρίζει τα επίπεδα ελέγχου και δεδομένων, επιτρέποντας την κεντρική διαχείριση του δικτύου. Ένας ελεγκτής SDN μπορεί να διαμορφώσει και να διαχειριστεί τη δρομολόγηση και τον χειρισμό της κυκλοφορίας σε όλο το δίκτυο, καθιστώντας τον ιδιαίτερα προσαρμόσιμο στις αλλαγές σε πραγματικό χρόνο στις συνθήκες του δικτύου.
Το SDN επιτρέπει στους δημιουργούς κίνησης να μιμούνται δυναμικές διαδρομές δικτύου και να τις αναδιαμορφώνουν κατά παραγγελία. Για παράδειγμα, το Mininet, ένας δημοφιλής εξομοιωτής δικτύου που λειτουργεί με SDN, επιτρέπει στους ερευνητές να δημιουργούν τοπολογίες εικονικού δικτύου με προγραμματιζόμενο έλεγχο, επιτρέποντας την προσομοίωση της συμπεριφοράς του δικτύου 5G υπό διαφορετικές συνθήκες δρομολόγησης και κυκλοφορίας [27].
Στο 5G, το SDN διευκολύνει τον τεμαχισμό του δικτύου επιτρέποντας σε κάθε κομμάτι να έχει μοναδικούς κανόνες δρομολόγησης, QoS και διαχείρισης της κυκλοφορίας. Αυτό επιτρέπει στους δημιουργούς κίνησης να προσομοιώνουν φέτες δικτύου με συγκεκριμένες απαιτήσεις ταχύτητας, αξιοπιστίας και καθυστέρησης, απαραίτητες για τη δοκιμή της ικανότητας του δικτύου να χειρίζεται ποικίλες περιπτώσεις χρήσης όπως το IoT και οι ευρυζωνικές συνδέσεις κινητής τηλεφωνίας υψηλής ταχύτητας [21].
Ο κεντρικός έλεγχος του SDN παρέχει λεπτομερή έλεγχο των ροών κυκλοφορίας. Αυτή η ικανότητα είναι απαραίτητη για τις γεννήτριες κίνησης 5G, οι οποίες πρέπει να προσομοιώνουν διάφορους τύπους και συνθήκες κυκλοφορίας, συμπεριλαμβανομένης της συμφόρησης, της εξισορρόπησης φορτίου και της προσαρμοστικής QoS. Η καθοδήγηση της κυκλοφορίας σε δίκτυα 5G που βασίζονται σε SDN επιτρέπει τη ρεαλιστική δοκιμή σεναρίων όπως οι μεταβιβάσεις, οι παρεμβολές και η βελτιστοποίηση του λανθάνοντος χρόνου.
Η δυνατότητα προγραμματισμού του SDN παρέχει λεπτομερή έλεγχο των ροών δεδομένων, επιτρέποντας τη λεπτομερή προσομοίωση σύνθετων σεναρίων 5G όπου πρέπει να διατηρούνται διαφορετικά επίπεδα QoS για διάφορες εφαρμογές [20].

Η ευελιξία του SDN επιτρέπει την προσομοίωση της προσαρμοστικής συμπεριφοράς του δικτύου, όπως η αυτόματη αναδρομολόγηση ως απόκριση στη συμφόρηση, επιτρέποντας τη ρεαλιστική δοκιμή της ανθεκτικότητας του δικτύου σε περιβάλλοντα 5G.

3.2.4. Network Slicing and Multi-Tenancy

Ο τεμαχισμός δικτύου είναι ένα χαρακτηριστικό μοναδικό στο 5G που επιτρέπει τη δημιουργία πολλαπλών εικονικών δικτύων (ή "φέτες") σε μια κοινή φυσική υποδομή. Κάθε κομμάτι είναι προσαρμοσμένο για να καλύψει τις ανάγκες διαφορετικών εφαρμογών, χρηστών ή βιομηχανιών, υποστηρίζοντας την πολλαπλή μίσθωση στο 5G [28].
Οι γεννήτριες κίνησης πρέπει να υποστηρίζουν τον τεμαχισμό του δικτύου δημιουργώντας μοτίβα κίνησης προσαρμοσμένα στις απαιτήσεις κάθε φέτας. Για παράδειγμα, ένα κομμάτι μπορεί να βελτιστοποιηθεί για μεταφορές δεδομένων υψηλής ταχύτητας για ροή βίντεο, ενώ ένα άλλο μπορεί να δώσει προτεραιότητα στη χαμηλή καθυστέρηση για αυτόνομη οδήγηση [27] .
Με την ενεργοποίηση ξεχωριστών τμημάτων με διαφορετικά επίπεδα QoS, οι δημιουργοί κίνησης μπορούν να δοκιμάσουν τις στρατηγικές κατανομής πόρων του δικτύου 5G. Το OMNeT++ με Simu5G, για παράδειγμα, επιτρέπει στους ερευνητές να δημιουργούν τμήματα δικτύου με προσαρμοσμένα προφίλ κίνησης και διαφορετικά επίπεδα προτεραιότητας, τα οποία είναι κρίσιμα για την αξιολόγηση της διαχείρισης πόρων και της απομόνωσης τμημάτων [21].
Ο τεμαχισμός δικτύου παρέχει απομόνωση της κυκλοφορίας, απαραίτητη για περιβάλλοντα πολλών ενοικιαστών. Οι γεννήτριες κίνησης που υποστηρίζουν τον τεμαχισμό μπορούν να βοηθήσουν στη δοκιμή της απόδοσης και της ασφάλειας της διατομής και της ενδοτομής, διασφαλίζοντας ότι η κυκλοφορία σε ένα κομμάτι δεν επηρεάζει την απόδοση ή την ασφάλεια ενός άλλου.
Ο τεμαχισμός δικτύου επιτρέπει σενάρια προσομοίωσης προσαρμοσμένα σε συγκεκριμένους κλάδους, όπως η υγειονομική περίθαλψη, η αυτοκινητοβιομηχανία και οι έξυπνες πόλεις, οι οποίες συχνά έχουν ξεχωριστές απαιτήσεις απόδοσης.
Οι απομονωμένες ροές κυκλοφορίας επιτρέπουν τη ρεαλιστική δοκιμή των πρωτοκόλλων ασφαλείας και των συστημάτων ανίχνευσης εισβολών σε κάθε φέτα, διασφαλίζοντας ότι οι απειλές σε μία φέτα δεν επηρεάζουν άλλες [28].

3.2.5. Radio Access Network (RAN) Simulation

Το Δίκτυο Ραδιοπρόσβασης (RAN) συνδέει τις συσκευές των χρηστών με το κεντρικό δίκτυο, υποστηρίζοντας την κινητικότητα και την υψηλή πυκνότητα των συσκευών. Στο 5G, ΤΟ RAN διαδραματίζει κρίσιμο ρόλο στην ενεργοποίηση της χαμηλής λανθάνουσας κατάστασης και της αξιόπιστης συνδεσιμότητας. Η ρεαλιστική δημιουργία κίνησης 5G απαιτεί ακριβή προσομοίωση RAN για την αξιολόγηση της συμπεριφοράς του δικτύου υπό διάφορες συνθήκες, όπως οι μεταβιβάσεις κυττάρων και η κινητικότητα των χρηστών.
Γεννήτριες κίνησης με δυνατότητες προσομοίωσης RAN, όπως ns 3 με 5G LENA Module και srsRAN, επιτρέπουν την προσομοίωση των χρηστών κινητής τηλεφωνίας που κινούνται μεταξύ των κυττάρων. Αυτό είναι απαραίτητο για τη δοκιμή εφαρμογών που εξαρτώνται από μεταπομπές χαμηλής καθυστέρησης, όπως συνδεδεμένα οχήματα και παιχνίδια σε πραγματικό χρόνο [20].

Η προσομοίωση RAN 5G επιτρέπει στις γεννήτριες κίνησης να δημιουργούν μοτίβα κίνησης με βάση τη δυναμική κατανομή εύρους ζώνης, κρίσιμα για τη δοκιμή QoS υπό ποικίλες συνθήκες φορτίου δικτύου. Για παράδειγμα, το srsRAN μπορεί να μιμηθεί TA προσαρμοστικά χαρακτηριστικά κατανομής εύρους ζώνης του RAN, βοηθώντας στη δοκιμή της αποδοτικότητας του εύρους ζώνης σε περιβάλλοντα υψηλής πυκνότητας.
Με την προσομοίωση των μεταπομπών και της συμφόρησης στα όρια των κυττάρων, η προσομοίωση RAN παρέχει πληροφορίες σχετικά με την ανθεκτικότητα του δικτύου. Αυτό είναι ιδιαίτερα σημαντικό για την αξιολόγηση του πόσο καλά το δίκτυο χειρίζεται την υψηλή κινητικότητα των χρηστών και τις παρεμβολές στις άκρες των κυψελών.
Η προσομοίωση RAN διασφαλίζει ότι η δημιουργία κίνησης αντικατοπτρίζει με ακρίβεια την εμπειρία του χρήστη σε σενάρια 5G υψηλής κινητικότητας, χαμηλής καθυστέρησης, όπως οι έξυπνες πόλεις ή τα αυτόνομα οχήματα. Οι δοκιμαστικές μεταβιβάσεις και οι στρατηγικές διαχείρισης της συμφόρησης παρέχουν πληροφορίες σχετικά με την ικανότητα του δικτύου 5G να διατηρεί την απόδοση υπό δύσκολες συνθήκες.

3.2.6. Advanced Analytics and Machine Learning (ML)

Τα προηγμένα αναλυτικά στοιχεία και η μηχανική μάθηση (ML) ενισχύουν τη δημιουργία κίνησης 5G, επιτρέποντας την έξυπνη δημιουργία μοτίβων κίνησης, την ανίχνευση ανωμαλιών και τη βελτιστοποίηση της απόδοσης. Οι αλγόριθμοι ML μπορούν να μάθουν από τα δεδομένα του πραγματικού κόσμου για να δημιουργήσουν προσαρμοστικά, ρεαλιστικά μοτίβα κυκλοφορίας, τα οποία είναι απαραίτητα για την αξιολόγηση της ανθεκτικότητας και της ασφάλειας του δικτύου (Anande & Leeson, n.d.[29]).
Οι τεχνικές ML, ειδικά τα Generative Adversarial Networks (GANs), επιτρέπουν τη δημιουργία μοτίβων κίνησης που μοιάζουν πολύ με τις πραγματικές συνθήκες του κόσμου, διευκολύνοντας τον έλεγχο της ακρίβειας των εργαλείων ασφαλείας που βασίζονται σε ML.
Οι γεννήτριες κίνησης με δυνατότητα ML μπορούν να ενσωματώσουν ρεαλιστικές ανωμαλίες και κακόβουλες συμπεριφορές στα μοτίβα κίνησης, όπως επιθέσεις DDoS, καθιστώντας τα ανεκτίμητα για τη δοκιμή συστημάτων IDS/IPS σε δίκτυα 5G.
Οι αλγόριθμοι ML μπορούν να προσαρμόσουν δυναμικά τη δημιουργία κίνησης με βάση το φορτίο του δικτύου, επιτρέποντας τη δοκιμή στρατηγικών διαχείρισης της κίνησης σε πραγματικό χρόνο υπό διάφορες συνθήκες. Αυτό είναι ζωτικής σημασίας σε προσαρμοστικές εφαρμογές 5G, όπου τα χαρακτηριστικά της κίνησης μπορούν να αλλάξουν γρήγορα με βάση τη ζήτηση των χρηστών ή την κατάσταση του δικτύου. Η παραγωγή κίνησης με γνώμονα το ML παρέχει υψηλό βαθμό ρεαλισμού, ζωτικής σημασίας για τη δοκιμή της απόδοσης των συστημάτων ανίχνευσης που βασίζονται στο ML στο 5G.
Η μηχανική μάθηση υποστηρίζει την προσαρμοστική δημιουργία κίνησης που προσαρμόζεται με βάση την ανατροφοδότηση δικτύου σε πραγματικό χρόνο, επιτρέποντας πιο ακριβείς αξιολογήσεις των πολιτικών διαχείρισης της κίνησης 5G.

3.3 Σύνολα Δεδομένων 5ης Γενιάς

Ο πολλαπλασιασμός των δικτύων κινητής τηλεφωνίας πέμπτης γενιάς (5G) έχει οδηγήσει σε εκτεταμένη έρευνα σχετικά με τον τρόπο βελτιστοποίησης της απόδοσης, διασφάλισης της ασφάλειας και αποτελεσματικής διαχείρισης των πόρων του δικτύου. Σε σύγκριση με τα παλαιότερα κυψελοειδή συστήματα, το 5G εισάγει νέα αρχιτεκτονικά στοιχεία, ιδίως έναν πυρήνα βασισμένο σε υπηρεσίες και πολυεπίπεδες δυνατότητες τεμαχισμού δικτύου, παράλληλα με την

υποστήριξη για εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (URLLC), βελτιωμένες ευρυζωνικές υπηρεσίες κινητής τηλεφωνίας (eMBB) και μαζικές επικοινωνίες τύπου μηχανής (mMTC) [30]4). Αυτά τα χαρακτηριστικά αυξάνουν σημαντικά την πολυπλοκότητα των λειτουργιών του δικτύου, δημιουργώντας μια ισχυρή ζήτηση για ολοκληρωμένα σύνολα δεδομένων που καταγράφουν σημαντικές μετρήσεις και συμβάντα υπό πραγματικές ή προσομοιωμένες συνθήκες.[31]
Η ρεαλιστική προσομοίωση και **αξιολόγηση συστημάτων 5G** απαιτεί την ύπαρξη κατάλληλων συνόλων δεδομένων δικτυακής κίνησης, τα οποία αποτυπώνουν σύγχρονες συνθήκες κίνησης και απειλών ασφαλείας στα δίκτυα 5G. Πρόσφατα έχουν διατεθεί αρκετά τέτοια **σύνολα δεδομένων** για την υποστήριξη της έρευνας, ειδικά σε θέματα όπως η γεννήτρια κίνησης δικτύου, η ανίχνευση εισβολών σε περιβάλλον **network slicing** και η αξιολόγηση πρωτοκόλλων **μη-IP μετάδοσης δεδομένων (**Non-IP Data Delivery, NIDD**)**. Στην ενότητα αυτή εστιάζουμε σε τρία χαρακτηριστικά παραδείγματα διαθέσιμων datasets – το 5G-AD (5G Anomaly/Attack Dataset), το 5G-SliciNdd και το 5G-NIDD – και αξιολογούμε την καταλληλότητά τους για την ανάπτυξη και δοκιμή μηχανισμών παραγωγής κίνησης, τεχνολογιών slicing, καθώς και πρωτοκόλλων μη-IP μετάδοσης σε δίκτυα 5G, συγκρίνοντάς τα ως προς την έκταση, την επικαιρότητα, την ποικιλία σεναρίων, την αντιστοίχισή τους με την αρχιτεκτονική 5G, την προσβασιμότητα και την αξιοπιστία τους. Μαζί, αυτοί οι πόροι καταδεικνύουν πώς η σύγχρονη έρευνα για το 5G χρησιμοποιεί μεθόδους που βασίζονται σε δεδομένα για τη διαχείριση αλληλεξαρτώμενων πτυχών της ασφάλειας, της ενορχήστρωσης και της κατανομής πόρων (Batewela S, Liyanage M[32]).

3.3.1 5G-AD (5G Anomaly/Attack Dataset)

Το 5G-AD[33] – επίσης γνωστό ως 5GAD-2022 – αποτελεί ένα δημόσια διαθέσιμο σύνολο δεδομένων που αναπτύχθηκε το 2022 από το Idaho National Laboratory. Πρόκειται για προσομοιωμένη κίνηση δικτύου 5G η οποία περιλαμβάνει τόσο φυσιολογική κίνηση όσο και κακόβουλη κίνηση πολλαπλών ειδών. Συγκεκριμένα, περιέχει δείγματα κανονικής χρήσης (π.χ. ροές βίντεο YouTube, αιτήσεις HTTP/S σε ιστοτόπους, βιντεοδιασκέψεις με μεταφορά αρχείων, FTP μεταφορές, διαμοιρασμό αρχείων μέσω Samba κ.ά.) που παράχθηκαν σε ένα περιβάλλον προσομοίωσης με ρεαλιστικές εφαρμογές δικτύου. Παράλληλα, περιλαμβάνει δέκα διαφορετικούς τύπους επιθέσεων που διακρίνονται σε τρεις κύριες κατηγορίες: αναγνωριστικές επιθέσεις, επιθέσεις άρνησης υπηρεσίας (DoS) και επιθέσεις αναδιάταξης δικτύου. Η συλλογή των δεδομένων πραγματοποιήθηκε σε εργαστηριακό περιβάλλον όπου υλοποιήθηκε ένας πυρήνας δικτύου 5G (5GC) με το ανοικτού κώδικα λογισμικό free5GC, συνδεδεμένος μέσω Ethernet με προσομοιωτή UE/RAN (λογισμικό UERANSIM) – γεγονός που εξασφαλίζει την αντιστοίχιση των δεδομένων με πραγματική αρχιτεκτονική 5G Standalone[34]. Η καταγραφή της κίνησης έγινε με παγίδευση πακέτων (Wireshark) στις διεπαφές του πυρήνα, επιτρέποντας την πλήρη αποθήκευση όλων των ροών. Οι κακόβουλες ροές δημιουργήθηκαν βάσει γνωστών ευπαθειών του 5G πυρήνα (π.χ. exploits στο free5GC και σεναρίων από αναφορές της Positive Technologies) ώστε να αντικατοπτρίζουν πραγματικές απειλές σε επίπεδο πυρήνα 5G[34]. Το 5G-AD διατίθεται ανοικτά (MIT license) μέσω GitHub 5, καθιστώντας το εύκολα προσβάσιμο στους ερευνητές.

4 3gpp
5 github.com

Λόγω του ρεαλιστικού μίγματος νόμιμης κίνησης και στοχευμένων επιθέσεων, το συγκεκριμένο dataset θεωρείται ιδιαίτερα χρήσιμο για την εκπαίδευση και αξιολόγηση αλγορίθμων ανίχνευσης ανωμαλιών στο περιβάλλον του 5G core, καθώς και για τη βαθμονόμηση εργαλείων παραγωγής κίνησης με βάση πραγματολογικά πρότυπα χρήσης.

3.3.2 5G-SliciNdd

Το 5G-SliciNdd είναι ένα πρόσφατο (2023) σύνολο δεδομένων που εστιάζει στην ασφάλεια του τεμαχισμού δικτύου (network slicing) σε δίκτυα 5G, ενσωματώνοντας και πτυχές μη-IP μετάδοσης όπως υποδηλώνει η ονομασία του (συνδυασμός "Slicing" και "NDD")[35]. Δημοσιεύθηκε μέσω της πλατφόρμας Figshare και περιλαμβάνει τέσσερα διακριτά υπο-σύνολα (αρχεία σε μορφές ARFF/CSV), μεταξύ των οποίων ένα «Global» dataset που αντιπροσωπεύει την *συνδυασμένη* 5G κίνηση όλων των σεναρίων[36]. Το 5G-SliciNdd ξεχωρίζει διότι παρέχει πλήρη χαρακτηριστικά επιθέσεων, συμπεριλαμβανομένης της κατηγορίας επίθεσης και του είδους εργαλείου/μεθόδου επίθεσης για κάθε εγγραφή[35]. Ο όγκος των δεδομένων του είναι ιδιαίτερα μεγάλος (άνω του εκατομμυρίου δειγμάτων), γεγονός που το καθιστά κατάλληλο για την εκπαίδευση σύγχρονων μοντέλων μηχανικής μάθησης που απαιτούν *big data*. Αν και δεν έχουν δημοσιευθεί εκτενείς λεπτομέρειες σε άρθρα μέχρι στιγμής, από τις διαθέσιμες πληροφορίες τεκμαίρεται ότι το dataset δημιουργήθηκε πιθανώς μέσω προσομοίωσης πολλαπλών εικονικών slices με γεννήτριες κίνησης και επιθέσεων, ώστε να περιλαμβάνει ποικιλία περιστατικών ασφαλείας σε περιβάλλον slicing. Το 5G-SliciNdd στοχεύει στην διευκόλυνση της έρευνας για ανίχνευση επιθέσεων σε slices και για τη βελτίωση μηχανισμών απομόνωσης φετών δικτύου, ενώ παράλληλα μπορεί να υποστηρίξει τη δοκιμή αλγορίθμων Non-IP μετάδοσης σε σενάρια IoT φετών, λόγω του ότι ενσωματώνει και σχετικά χαρακτηριστικά NIDD. Είναι διαθέσιμο ως ανοικτό dataset (Figshare DOI: 10.6084/m9.figshare.24446515) και συνεπώς προσβάσιμο για περαιτέρω μελέτη ή επέκταση από την κοινότητα.

3.3.3 5G-NIDD (Non-IP Data Delivery)

Το 5G-NIDD είναι ένα **ολοκληρωμένο σύνολο δεδομένων ανίχνευσης εισβολών σε 5G**, το οποίο παρουσιάστηκε το 2022-2023 από ομάδα του Πανεπιστημίου Oulu στη Φινλανδία[37] Σε αντίθεση με τα προηγούμενα, το 5G-NIDD δημιουργήθηκε πάνω σε ένα *λειτουργικό δοκιμαστικό δίκτυο 5G* (5G Test Network – 5GTN), εξασφαλίζοντας πολύ υψηλή πιστότητα ως προς τις πραγματικές συνθήκες δικτύου. Συγκεκριμένα, η συλλογή δεδομένων έγινε από δύο σταθμούς βάσης **(gNodeB)** συνδεδεμένους στο 5GTN, όπου κάθε σταθμός βάσης εξυπηρετούσε πολλούς κανονικούς χρήστες 5G και έναν κακόβουλο κόμβο επιτιθέμενου. Οι επιτιθέμενοι στόχευαν έναν εξυπηρετητή που ήταν εγκατεστημένος στο περιβάλλον **MEC (**Multi-access Edge Computing**)** του δικτύου, πραγματοποιώντας ποικίλες επιθέσεις κατά τη διάρκεια της πειραματικής λειτουργίας. Το 5G-NIDD περιλαμβάνει πλήρως επισημειωμένα δεδομένα τόσο κανονικής κίνησης όσο και επιθέσεων DoS και σαρώσεων. Ενδεικτικά, καταγράφονται πολλοί τύποι επιθέσεων **άρνησης υπηρεσίας** (ICMP Flood, UDP Flood, SYN Flood, HTTP Flood, Slowrate DoS) καθώς και **σαρώσεις θυρών** (SYN Scan, TCP Connect Scan, UDP Scan) σε διάφορα χρονικά διαστήματα και συνθήκες φορτίου[37]. Η ύπαρξη τόσο ευρέος φάσματος επιθέσεων επιτρέπει την ανάπτυξη και αξιολόγηση μεθόδων ανίχνευσης για ποικιλία σεναρίων, από απλές σαρώσεις έως μεγάλης κλίμακας κατανεμημένες επιθέσεις. Το dataset είναι διαθέσιμο με ανοικτή

άδεια πρόσβασης (π.χ. μέσω IEEE Dataport και εθνικών αποθετηρίων δεδομένων), διευκολύνοντας τους ερευνητές που επιθυμούν να το χρησιμοποιήσουν ως βάση για εκπαίδευση μοντέλων AI/ML στην ασφάλεια δικτύων 5G. Επιπλέον, το 5G-NIDD εστιάζει σε σενάρια που αφορούν μη-IP μετάδοση (χαρακτηριστικό που εμφανίζεται σε IoT εφαρμογές στο 5G), καθιστώντας το ιδιαίτερα χρήσιμο για την μελέτη μηχανισμών προστασίας σε αρχιτεκτονικές όπου οι συσκευές επικοινωνούν χωρίς πλήρες στοίβας IP.

3.3.4 Σύγκριση των συνόλων δεδομένων

Συγκριτικά, τα παραπάνω σύνολα δεδομένων παρουσιάζουν διαφορές ως προς ορισμένα κρίσιμα κριτήρια:

- **Εύρος κάλυψης:** Το 5G-AD καλύπτει κυρίως την κίνηση στον **πυρήνα 5G** με επικέντρωση σε επιθέσεις προς τα δίκτυα κορμού (core network), προσομοιώνοντας όμως και ένα ευρύ φάσμα εφαρμογών χρήστη. Το 5G-NIDD έχει ευρύτερο *εμβέλεια* σε επίπεδο αρχιτεκτονικής, καθώς περιλαμβάνει δεδομένα από τον ασύρματο κρίκο (σταθμούς βάσης) μέχρι το MEC, ενώ επικεντρώνεται σε κλασικές επιθέσεις δικτύου που επηρεάζουν την διαθεσιμότητα. Το 5G-SliciNdd, από την άλλη, επεκτείνει το εύρος κάλυψης προς την **διεπαφή slicing** του δικτύου, συμπεριλαμβάνοντας δεδομένα που σχετίζονται με πολλαπλές φέτες (slices) και πιθανώς με επικοινωνία IoT (NIDD), κάτι που δεν εμφανίζεται ρητά στα άλλα δύο. Συνολικά, κάθε dataset στοχεύει σε *διαφορετικό επίπεδο* του 5G οικοσυστήματος: από τον πυρήνα (5G-AD) έως το end-to-end slice περιβάλλον (5G-SliciNdd) και τις άκρες του δικτύου με IoT/MEC (5G-NIDD).
- **Επικαιρότητα:** Και τα τρία σύνολα είναι **πρόσφατα** (κυκλοφόρησαν την περίοδο 2022–2023), αντανακλώντας τις τρέχουσες συνθήκες και απειλές στα δίκτυα 5G. Το 5G-AD (2022) βασίστηκε σε ευπάθειες και σενάρια που τεκμηριώθηκαν την τελευταία πενταετία, ενώ το 5G-NIDD (υποβλήθηκε τέλη 2022, δημοσιοποιήθηκε 2023) δημιουργήθηκε σε ένα από τα πρώτα λειτουργικά testbeds 5G, εξασφαλίζοντας ότι τα δεδομένα του είναι *σύγχρονα* και αντιπροσωπευτικά. Το 5G-SliciNdd (2023) αποτελεί το πλέον πρόσφατο και αντανακλά το ανερχόμενο ενδιαφέρον για **ασφάλεια slicing** και NIDD σε 5G/B5G δίκτυα. Ως εκ τούτου, όλα τα datasets είναι επικαιροποιημένα ως προς τις τεχνολογίες 5G που καλύπτουν, με το 5G-SliciNdd να εστιάζει σε ίσως πιο *μελλοντοστραφή* πτυχή (slicing σε βάθος).
- **Ποικιλομορφία σεναρίων & επιθέσεων:** Το 5G-AD προσφέρει **10 διαφορετικούς τύπους επιθέσεων** σε εργαστηριακό περιβάλλον, καλύπτοντας ποικιλία από reconnaissance μέχρι DoS, σε συνδυασμό με ρεαλιστική νόμιμη κίνηση. Το 5G-NIDD περιλαμβάνει επίσης **πολυάριθμες επιθέσεις** (τουλάχιστον 8 τύπους επιθέσεων/floods και 3 τύπους σαρώσεων) με **ετικέτες (labels)** για κάθε συμβάν, αποτυπώνοντας πολλά διαφορετικά σενάρια επίθεσης εντός ενός πραγματικού δικτύου. Το 5G-SliciNdd υπερβαίνει σε πλήθος δειγμάτων, ενσωματώνοντας *άνω του εκατομμυρίου εγγραφών* από πιθανώς δεκάδες επιμέρους σενάρια επίθεσης – κάθε εγγραφή φέρει πληροφορίες τόσο για την κατηγορία επίθεσης όσο και για το εργαλείο υλοποίησής της. Αυτό σημαίνει ότι η ποικιλομορφία του SliciNdd είναι μεγάλη όχι μόνο ως προς τους τύπους επιθέσεων, αλλά και ως προς τις συνθήκες (διαφορετικά slices, διαφορετικά εργαλεία επίθεσης). Συνολικά, και τα τρία datasets προσφέρουν **πολυμορφία επιθετικών σεναρίων**, με το 5G-NIDD και 5G-AD να επικεντρώνονται σε συγκεκριμένες κατηγορίες (δικτυακές επιθέσεις, πυρήνας) ενώ το 5G-SliciNdd καλύπτει ένα ακόμα ευρύτερο φάσμα με λεπτομερή χαρακτηριστικά.

- **Αντιστοίχιση με αρχιτεκτονική 5G:** Το 5G-NIDD υπερέχει ως προς την **ρεαλιστική αντιστοίχιση** σε μια πλήρη αρχιτεκτονική 5G, καθώς τα δεδομένα προήλθαν από πραγματικό δίκτυο με σταθμούς βάσης, πυρήνα και MEC, ακολουθώντας τις προδιαγραφές του 3GPP (Standalone 5G, υποστήριξη NIDD κλπ.). Το 5G-AD αν και δημιουργήθηκε σε εργαστήριο, **συμμορφώνεται** επίσης με την αρχιτεκτονική 5G SA: χρησιμοποίησε πλήρη στοίβα πυρήνα (free5GC) και προσομοιωμένο RAN, επιτρέποντας στα πακέτα του dataset να φέρουν τις κεφαλίδες και τα πρωτόκολλα ενός αληθινού δικτύου 5G. Το 5G-SliciNdd, παρότι οι λεπτομέρειες υλοποίησης του δεν έχουν δημοσιευθεί εκτενώς, σχεδιάστηκε ειδικά για να αντικατοπτρίζει **περιβάλλον πολλαπλών slices**, που αποτελεί προέκταση της 5G αρχιτεκτονικής πέραν του συμβατικού κορμού. Επομένως, κάθε dataset έχει διαφορετικό βαθμό αντιστοίχισης: το 5G-NIDD προσφέρει *αυθεντικότητα πραγματικού δικτύου*, το 5G-AD προσφέρει *ελεγχόμενη πιστότητα* σε κρίσιμα σημεία του πυρήνα, και το 5G-SliciNdd προσφέρει *επεκτασιμότητα* προς μελλοντικές αρχιτεκτονικές slicing.
- **Προσβασιμότητα:** Και τα τρία σύνολα δεδομένων είναι **εύκολα προσβάσιμα στο ευρύ κοινό των ερευνητών**. Το 5G-AD διατίθεται μέσω GitHub (ανοικτός κώδικας/dataset με MIT άδεια), ενώ το 5G-NIDD είναι διαθέσιμο μέσω του IEEE Dataport και άλλων ανοικτών αποθετηρίων χωρίς χρέωση. Το 5G-SliciNdd έχει αναρτηθεί στο Figshare (DOI διαθέσιμο) και μπορεί να ληφθεί ελεύθερα. Συνεπώς, ως προς την προσβασιμότητα **δεν υπάρχουν ουσιαστικοί περιορισμοί** – όλα τα datasets συνοδεύονται από τεκμηρίωση και/ή επιστημονικές δημοσιεύσεις που επιτρέπουν την ορθή χρήση τους. Ένας μικρός πρακτικός φραγμός είναι το μέγεθος ορισμένων αρχείων (π.χ. GB δεδομένων για 5G-NIDD και SliciNdd), το οποίο απαιτεί επαρκείς πόρους αποθήκευσης και υπολογιστικής ισχύος για επεξεργασία, όμως αυτό είναι αναμενόμενο δοθέν του πλούτου πληροφοριών που προσφέρουν.
- **Αξιοπιστία δεδομένων:** Και τα τρία σύνολα θεωρούνται **αξιόπιστα** και κατάλληλα επισημειωμένα για ερευνητική χρήση. Το 5G-AD, αν και προέρχεται από προσομοίωση, δημιουργήθηκε από ειδικούς του τομέα με στοχοθετημένες επιθέσεις βασισμένες σε πραγματικές ευπάθειες, παρέχοντας έγκυρα δεδομένα για την ανίχνευση ανωμαλιών. Το 5G-NIDD λόγω του ότι συλλέχθηκε από πραγματικό δίκτυο, προσφέρει **υψηλή αξιοπιστία ως προς την ακρίβεια και αυθεντικότητα** της κίνησης· τα labels (κατηγορία κάθε ροής ως κανονική ή τύπος επίθεσης) έχουν αποδοθεί με βάση γνωστή γενεσιουργό δράση (π.χ. συγκεκριμένο script επίθεσης), διασφαλίζοντας την ορθότητα των δεδομένων. Το 5G-SliciNdd, με τον τεράστιο όγκο του, στηρίζεται επίσης σε *συνθετικά μεν, αλλά μεθοδικά παραχθέντα* δεδομένα – η παρουσία χαρακτηριστικών όπως «attack type» και «attack tool» υποδηλώνει ότι οι δημιουργοί του είχαν πλήρη έλεγχο των σεναρίων και άρα αξιόπιστη σήμανση των περιπτώσεων. Ενδεχομένως, η αξιοπιστία του SliciNdd εξαρτάται από το πόσο ρεαλιστικά ήταν τα σενάρια slicing που υλοποιήθηκαν· ωστόσο, εφόσον το dataset συνοδεύεται από τεκμηρίωση, μπορεί να θεωρηθεί επαρκώς αξιόπιστο για συγκριτικές μελέτες. Συνολικά, κανένα από τα τρία datasets δεν εμφανίζει προφανείς μεροληψίες ή σφάλματα στα δημοσιευμένα στοιχεία του, και όλα έχουν χρησιμοποιηθεί (ή προταθεί προς χρήση) σε **αξιόπιστες επιστημονικές μελέτες**, γεγονός που ενισχύει την εμπιστοσύνη στην ποιότητά τους.

Λαμβάνοντας υπόψη τα παραπάνω, καθίσταται σαφές ότι **κάθε dataset προσφέρει ξεχωριστά πλεονεκτήματα** για την ανάπτυξη και δοκιμή εργαλείων σε δίκτυα 5G. Το 5G-AD προσφέρεται για μελέτες στον πυρήνα του 5G και για τη **δημιουργία προτύπων κίνησης** με προσμίξεις

επιθέσεων core-network. Το 5G-NIDD αποτελεί **σημείο αναφοράς** για την ανίχνευση επιθέσεων σε *πραγματικές* συνθήκες δικτύου και ειδικότερα σε σενάρια IoT με μη-IP μετάδοση, όπου η διαθεσιμότητα είναι κρίσιμη. Το 5G-SliciNdd, τέλος, παρέχει ένα **εκτενές πεδίο δεδομένων** για την αξιολόγηση αλγορίθμων σε περιβάλλον slicing, επιτρέποντας την δοκιμή της αποδοτικότητας τεχνικών ασφαλείας σε κατακερματισμένα (slice-isolated) δίκτυα και την εξέταση επιθέσεων που μπορεί να εκμεταλλεύονται τις νέες αυτές δομές. Η συγκριτική αξιολόγηση της **καταλληλότητας** των εν λόγω συνόλων (ως προς τις εκάστοτε απαιτήσεις προσομοίωσης κίνησης, slicing ή NIDD) αποτελεί ουσιώδες βήμα για την επιλογή της βέλτιστης προσέγγισης στα πλαίσια της παρούσας διατριβής. Με βάση τα χαρακτηριστικά που παρουσιάστηκαν, ο ερευνητής μπορεί να αποφασίσει ποιο dataset ταιριάζει περισσότερο στους στόχους των πειραμάτων του – π.χ. χρήση του 5G-AD για γρήγορη προτυποποίηση αλγορίθμων ανίχνευσης ανωμαλιών στον πυρήνα, του 5G-NIDD για **αξιολόγηση σε ρεαλιστικό επίπεδο παραγωγής**, ή του 5G-SliciNdd για να εξετάσει σενάρια ασφάλειας σε **πολλαπλές φέτες δικτύου**. Οι γνώσεις που θα προκύψουν από την ανάλυση αυτών των συνόλων δεδομένων θα συμβάλουν στην τεκμηρίωση και **βελτιστοποίηση των εργαλείων προσομοίωσης δικτυακής κίνησης** που θα αναπτυχθούν στα επόμενα κεφάλαια.

4. Προσδιορισμός βασικών εργαλείων και τεχνολογιών

Τα δίκτυα κινητής τηλεφωνίας πέμπτης γενιάς (5G) αντιπροσωπεύουν ένα μετασχηματιστικό άλμα στις δυνατότητες ασύρματης επικοινωνίας, φέρνοντας πρωτόγνωρους στόχους απόδοσης και νέες περιπτώσεις χρήσης που ξεπερνούν κατά πολύ εκείνους των προηγούμενων γενεών*[38]* . Αυτή η αλλαγή παραδείγματος χαρακτηρίζεται από υποστήριξη διαφορετικών τύπων υπηρεσιών – από βελτιωμένη ευρυζωνική κινητή τηλεφωνία (eMBB) για εξαιρετικά υψηλούς ρυθμούς δεδομένων έως εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (URLLC) και μαζικές επικοινωνίες τύπου μηχανής (mMTC) – όλα μέσα σε μια ενοποιημένη αρχιτεκτονική. Οι διεθνείς οργανισμοί προτύπων όπως το 3GPP και το ITU έχουν κωδικοποιήσει αυστηρές απαιτήσεις για το 5G: μέγιστες αποδόσεις της τάξης των δεκάδων gigabit ανά δευτερόλεπτο, λανθάνοντες χρόνοι από άκρο σε άκρο έως 1 ms και πυκνότητες σύνδεσης έως και 10^6 συσκευές ανά τετραγωνικό χιλιόμετρο. Η ταυτόχρονη επίτευξη αυτών των φιλόδοξων στόχων είναι μια τεράστια πρόκληση, καθιστώντας τα εργαλεία προσομοίωσης και εξομοίωσης απαραίτητα για την ανάπτυξη, τη δοκιμή και την επικύρωση των τεχνολογιών 5G*[39]*. Επιτρέποντας σε ερευνητές και μηχανικούς να εξερευνούν επιλογές σχεδίασης σε silico πριν από την ανάπτυξη, τέτοια εργαλεία συμβάλλουν στη γεφύρωση του χάσματος μεταξύ των θεωρητικών καινοτομιών και των πραγματικών υλοποιήσεων 5G*[38]*.

Μία από τις βασικές δυσκολίες στη μηχανική δικτύων 5G είναι η απόλυτη πολυπλοκότητα της αρχιτεκτονικής και των απαιτήσεων υπηρεσιών. Τα δίκτυα 5G πρέπει να εξυπηρετούν απρόσκοπτα ετερογενείς περιπτώσεις χρήσης – για παράδειγμα, παροχή ευρυζωνικής ροής πολλών gigabit, διατήρηση αξιοπιστίας ραδιοζεύξης κάτω του χιλιοστού του δευτερολέπτου για κρίσιμες εφαρμογές και υποστήριξη μαζικής συνδεσιμότητας IoT – συχνά υπό ταυτόχρονη λειτουργία . Αυτές οι απαιτήσεις, που ορίζονται στο όραμα IMT-2020, ωθούν τα όρια του παραδοσιακού σχεδιασμού και διαχείρισης δικτύου. Το σύστημα 5G εισάγει νέες τεχνολογίες, όπως ραδιόφωνο κυμάτων χιλιοστών, τεράστιες συστοιχίες κεραιών MIMO, κοπή δικτύου για υπηρεσίες απομόνωσης και ένα δίκτυο πυρήνα εγγενούς στο cloud, καθένα από τα οποία προσθέτει επίπεδα πολυπλοκότητας. Η διασφάλιση ότι τα πρωτόκολλα και οι αλγόριθμοι αποδίδουν βέλτιστα σε αυτό το διαφορετικό τοπίο δεν είναι ασήμαντο. Οι περιορισμοί εξαιρετικά χαμηλής καθυστέρησης και υψηλής αξιοπιστίας , για παράδειγμα, απαιτούν προσεκτική αξιολόγηση των πρωτοκόλλων προγραμματισμού και δρομολόγησης υπό διάφορες συνθήκες φορτίου και κινητικότητας, ενώ η μαζική συνδεσιμότητα απαιτεί έλεγχο του τρόπου με τον οποίο κλιμακώνεται το δίκτυο με τεράστιο αριθμό συσκευών. Επειδή η αναλυτική μοντελοποίηση καθίσταται δυσεπίλυτη δεδομένης της πληθώρας παραμέτρων που αλληλεπιδρούν (χρήστες, κεραίες, περιβάλλοντα διάδοσης, τύποι υπηρεσιών κ.λπ.), οι ερευνητές στρέφονται σε λεπτομερείς προσομοιώσεις δικτύου για να αξιολογήσουν μετρήσεις απόδοσης που αψηφούν την ανάλυση κλειστής μορφής *[39]*. Στην πραγματικότητα, πριν από οποιαδήποτε ευρεία ανάπτυξη μιας νέας δυνατότητας ή αρχιτεκτονικής 5G, είναι απαραίτητες εκτενείς μελέτες προσομοίωσης για την εκτίμηση βασικών παραμέτρων όπως η χωρητικότητα, η απόδοση, η καθυστέρηση και η αξιοπιστία υπό ρεαλιστικές συνθήκες *[39]*. Τα αποτελέσματα της προσομοίωσης παρέχουν έγκαιρη ανατροφοδότηση σχετικά με το εάν μια προτεινόμενη λύση 5G πληροί τα απαιτούμενα κριτήρια απόδοσης που ορίζονται από τα πρότυπα, καθοδηγώντας περαιτέρω βελτιστοποίηση ή προσαρμογές σχεδιασμού στον κύκλο ανάπτυξης.

Σε αυτό το πλαίσιο, τα εργαλεία προσομοίωσης και εξομοίωσης δικτύου έχουν γίνει θεμελιώδεις παράγοντες για την έρευνα και την ανάπτυξη 5G. Οι προσομοιωτές δικτύου (π.χ. ns-3, OMNeT++ και άλλοι) μοντελοποιούν τη συμπεριφορά των δικτύων 5G σε λογισμικό, επιτρέποντας τον ελεγχόμενο πειραματισμό με νέα πρωτόκολλα, αλγόριθμους και διαμορφώσεις σε ένα αναπαραγώγιμο περιβάλλον. Χρησιμοποιώντας αυτές τις πλατφόρμες, οι μπορούμε να

οργανώσουμε κάθε επίπεδο της στοίβας πρωτοκόλλου 5G για να παρατηρήσουμε πώς, για παράδειγμα, ένας νέος αλγόριθμος προγραμματισμού ή διαδικασία παράδοσης συμπεριφέρεται κάτω από ποικίλα φορτία κυκλοφορίας, μοτίβα κινητικότητας χρήστη ή συνθήκες ραδιοπαρεμβολών. Ένα ευρύ φάσμα δεικτών απόδοσης μπορεί να εξαχθεί από μοντέλα προσομοίωσης - απόδοση , καθυστέρηση, ποσοστά σφάλματος, φόρτος χρήστη, πιθανότητα διακοπής λειτουργίας, συχνότητα παράδοσης, μεταξύ άλλων - για να αξιολογηθεί διεξοδικά η συμπεριφορά του δικτύου και να επικυρωθεί η συμμόρφωση του πρωτοκόλλου με τις προδιαγραφές 5G *[39]*. Επιπλέον, οι προσομοιωτές συχνά εφαρμόζουν τυπικά καθορισμένες λειτουργίες (ανά έκδοση 3GPP 15 και μετά), έτσι ώστε τα αποτελέσματα της αξιολόγησης να αντικατοπτρίζουν στενά τα αναμενόμενα αποτελέσματα του πραγματικού κόσμου. Εν τω μεταξύ, η εξομοίωση δικτύου συμπληρώνει την καθαρή προσομοίωση αναπαράγοντας τις πραγματικές συνθήκες δικτύου και τις βλάβες σε ένα ελεγχόμενο περιβάλλον. Σε αντίθεση με τους προσομοιωτές που αφαιρούν τη λειτουργία του δικτύου, η εξομοίωση περιλαμβάνει τη χρήση πραγματικών στοίβων πρωτοκόλλων ή υλικού σε βρόχο για τη μίμηση της ζωντανής συμπεριφοράς δικτύου. Για παράδειγμα, ένας εξομοιωτής δικτύου μπορεί να εισάγει ρεαλιστικές καθυστερήσεις, jitter, περιορισμούς εύρους ζώνης και απώλειες πακέτων σε μια δοκιμαστική σύνδεση, επιτρέποντας στους επαγγελματίες να παρατηρούν την απόδοση εφαρμογής 5G από άκρο σε άκρο σαν να εκτελείται σε πραγματικό δίκτυο [40]. Αυτή η δυνατότητα είναι ζωτικής σημασίας για τη δοκιμή συσκευών 5G και λειτουργιών βασικών δικτύων σε διάφορα σενάρια (πυκνά αστικά κύτταρα, συνδέσεις οχημάτων υψηλής ταχύτητας, δορυφορική backhaul κ.λπ.) χωρίς να απαιτείται φυσική ρύθμιση αυτών των σεναρίων. Αξιοποιώντας τόσο την προσομοίωση όσο και την εξομοίωση, μπορούν να βελτιωθούν επαναληπτικά τα σχέδια συστημάτων 5G: πρώτα σε ένα προσομοιωμένο μοντέλο για να εξερευνηθεί ένας ευρύς χώρος παραμέτρων και στη συνέχεια σε ένα περιβάλλον εξομοίωσης για να επικυρωθεί η απόδοση με μεγαλύτερη πιστότητα και πραγματική κυκλοφορία δεδομένων.

Πέρα από την αξιολόγηση της απόδοσης, τα εργαλεία προσομοίωσης δικτύου διαδραματίζουν σημαντικό ρόλο στη μελέτη της επεκτασιμότητας και των πτυχών ασφάλειας των δικτύων 5G. Οι κλιμακωτοί προσομοιωτές επιτρέπουν τον πειραματισμό με τοπολογίες δικτύου και πυκνότητες χρηστών σε κλίμακα που δεν θα ήταν πρακτικό να αναπαραχθεί σε εργαστήριο, όπως χιλιάδες σταθμοί βάσης που εξυπηρετούν εκατομμύρια εικονικούς χρήστες. Αυτό βοηθά στον εντοπισμό των σημείων συμφόρησης και στη διασφάλιση ότι τα πρωτόκολλα 5G παραμένουν αποτελεσματικά καθώς το δίκτυο επεκτείνεται. Εξίσου σημαντικό, η προσομοίωση και η εξομοίωση παρέχουν ένα ασφαλές sandbox για δοκιμές ασφαλείας στο 5G. Δεδομένου ότι το 5G εισάγει νέα πιθανά τρωτά σημεία (λόγω της χρήσης εικονικοποίησης IT, υπολογιστών αιχμής και συσκευών IoT), είναι ζωτικής σημασίας να εξεταστεί πώς το δίκτυο αντέχει σε κακόβουλες συνθήκες. Θα μπορούσαν να αξιοποιήθούν εξειδικευμένα εργαλεία για την προσομοίωση κυβερνοεπιθέσεων και σεναρίων αποτυχίας σε στοιχεία 5G χωρίς να τίθεται σε κίνδυνο η πραγματική υποδομή [41]. Για παράδειγμα, θα μπορούσε να μοντελοποιήθει μια επίθεση άρνησης υπηρεσίας ή μια έκρηξη κίνησης σηματοδότησης σε έναν προσομοιωμένο πυρήνα 5G για να παρατηρηθεί πώς αντιδρούν τα πρωτόκολλα ασφαλείας και η απομόνωση κοπής δικτύου υπό πίεση. Τέτοια πειράματα επιτρέπουν την αξιολόγηση συστημάτων ανίχνευσης εισβολής, μηχανισμών ελέγχου ταυτότητας και στρατηγικών ανοχής σφαλμάτων σε ελεγχόμενο περιβάλλον [41]. Οι γνώσεις που αποκτήθηκαν από αυτές τις προσομοιώσεις είναι πολύτιμες για την ενίσχυση της ανθεκτικότητας του δικτύου πριν από την πραγματική ανάπτυξη. Εν ολίγοις, η δυνατότητα αναδημιουργίας τόσο τυπικών συνθηκών λειτουργίας όσο και ακραίων περιπτώσεων γωνίας μέσω

προσομοίωσης/εξομοίωσης είναι απαραίτητη για την πλήρη επικύρωση της αξιοπιστίας και της ασφάλειας του δικτύου 5G, κάτι που είναι δύσκολο να επιτευχθεί μόνο μέσω δοκιμών πεδίου.
Συνολικά, η χρήση προηγμένων εργαλείων προσομοίωσης και εξομοίωσης έχει γίνει ο ακρογωνιαίος λίθος της ανάπτυξης της τεχνολογίας 5G . Εξουσιοδοτούν τους ενδιαφερόμενους να επαληθεύσουν ότι οι καινοτόμες λύσεις 5G μπορούν να πληρούν τα αυστηρά κριτήρια απόδοσης και τα κριτήρια αξιοπιστίας που ορίζονται από τα πρότυπα, ενώ επιταχύνουν την ανάπτυξη αποκαλύπτοντας ζητήματα νωρίς στη διαδικασία σχεδιασμού. Η ευρύτερη σημασία αυτών των εργαλείων έγκειται στην ικανότητά τους να μειώνουν το κόστος ανάπτυξης και τους κινδύνους – επιτρέποντας εκτεταμένες δοκιμές νέων ιδεών 5G (από τη ραδιοεπικοινωνία έως τα πρωτόκολλα βασικού δικτύου) χωρίς να απαιτούνται φυσικά πρωτότυπα για κάθε σενάριο. Στο υπόλοιπο αυτού του κεφαλαίου, βασιζόμαστε σε αυτήν την εισαγωγή εξετάζοντας τις βασικές πλατφόρμες προσομοίωσης και εξομοίωσης κυκλοφορίας δικτύου που χρησιμοποιούνται στον τομέα 5G. Θα αναλύσουμε πώς λειτουργεί κάθε εργαλείο και πώς εφαρμόζεται για την αξιολόγηση της απόδοσης, της επεκτασιμότητας και της ασφάλειας του δικτύου 5G , παρέχοντας μια βάση για τις λεπτομερείς αναλύσεις και συγκρίσεις που ακολουθούν.[38].
Εργαλεία για προσομοίωση/εξομοίωση δικτύων 5G – Η ταχεία εξέλιξη των δικτύων κινητής τηλεφωνίας πέμπτης γενιάς (5G) έχει δημιουργήσει την ανάγκη για ισχυρά εργαλεία προσομοίωσης και εξομοίωσης για την αξιολόγηση της απόδοσης. Τέτοια εργαλεία δίνουν τη δυνατότητα σε ερευνητές και μηχανικούς δικτύων να σχεδιάζουν και να δοκιμάζουν νέες αρχιτεκτονικές, αλγόριθμους και πρωτόκολλα σε ένα ελεγχόμενο περιβάλλον πριν από την ανάπτυξη στον πραγματικό κόσμο *[42]*. Αυτό το κεφάλαιο προσδιορίζει βασικές πλατφόρμες ανοιχτού κώδικα για την προσομοίωση δικτύου 5G και τη δημιουργία κίνησης, συζητώντας την αρχιτεκτονική τους, τις περιπτώσεις χρήσης, τα πλεονεκτήματα, τις προκλήσεις και τις βέλτιστες πρακτικές. Η εστίαση είναι σε ευρέως χρησιμοποιούμενα εργαλεία, συμπεριλαμβανομένων προσομοιωτών δικτύου (ns-3 με τη μονάδα 5G-LENA, OMNeT++/Simu5G), εξομοιωτές δικτύου πρόσβασης ραδιοφώνου (RAN) (srsRAN), προσομοιωτές κεντρικού δικτύου (Open5GS με UERANSIM), γεννήτριες κυκλοφορίας υψηλής απόδοσης (TRex, TeraVM, iiPsyerf3 και περιβάλλον δικτύου). (Mininet, ενσωμάτωση Wireshark). Κάθε εργαλείο παίζει συμπληρωματικό ρόλο στη μελέτη και ανάπτυξη τεχνολογιών 5G.

4.1. ns-3 / 5G-LENA

Το Network Simulator 3 (ns-3) είναι ένας προσομοιωτής δικτύου διακριτών συμβάντων που χρησιμοποιείται ευρέως στην ακαδημαϊκή και βιομηχανική έρευνα *[42]*. Παρέχει μια αρθρωτή, επεκτάσιμη αρχιτεκτονική σε C++ (με δεσμεύσεις Python) και μια πλούσια βιβλιοθήκη μοντέλων πρωτοκόλλων (TCP, UDP, δρομολόγηση κ.λπ.), καθιστώντας δυνατή την προσομοίωση διαφορετικών σεναρίων δικτύου σε πολλαπλά επίπεδα. Το ns-3 μπορεί να διασυνδέεται με πραγματικό υλικό δικτύου σε λειτουργία εξομοίωσης, γεφυρώνοντας τη θεωρητική προσομοίωση με τον πρακτικό πειραματισμό. Η φύση ανοιχτού κώδικα και η ενεργή κοινότητά του έχουν καθιερώσει το ns-3 ως ένα τυπικό εργαλείο για την έρευνα δικτύωσης, με σκοπό να αντικαταστήσει τελικά τον παλαιότερο προσομοιωτή ns-2*[42]*.
Στο πλαίσιο του 5G, η μονάδα 5G-LENA επεκτείνει το ns-3 με μοντέλα για πρόσβαση 5G New Radio (NR). Αναπτύχθηκε από το CTTC ως εξέλιξη της μονάδας LTE-LENA, το 5G-LENA είναι μια συνδεόμενη μονάδα ns-3 που προσομοιώνει το δίκτυο ραδιοπρόσβασης 5G NR με υψηλή

πιστότητα στο πρότυπο 3GPP 6. Υποστηρίζει αυτόνομη ανάπτυξη 5G (SA) καθώς και σενάρια μη αυτόνομων (NSA) όπου το 5G συνυπάρχει με το LTE. Αυτή η ενότητα καλύπτει το κενό στις δυνατότητες του ns-3 , επιτρέποντας λεπτομερή ανάλυση και αξιολόγηση των χαρακτηριστικών 5G NR, όπως ένα ευρύ φάσμα συχνοτήτων, ευέλικτες αποστάσεις υποφορέων και διαμόρφωση υψηλότερης τάξης (π.χ. 256-QAM). Ο προσομοιωτής 5G-LENA υλοποιεί μια πλήρη στοίβα πρωτοκόλλου για το δίκτυο ραδιοπρόσβασης NR (RAN) – από το φυσικό επίπεδο έως το πρωτόκολλο σύγκλισης δεδομένων πακέτων – ακολουθώντας πιστά τις προδιαγραφές 3GPP. Περιλαμβάνει μοντέλα για gNodeB (σταθμός βάσης 5G) και Εξοπλισμό χρήστη (UE), που υποστηρίζουν ένα εύρος εύρους ζώνης, συχνότητες φορέα και παραμέτρους ισχύος για να επιτρέψουν ρεαλιστικές μελέτες απόδοσης.

4.1.1. Βασικά Στοιχεία και Αρχιτεκτονική

Η αρχιτεκτονική του 5G-LENA αντικατοπτρίζει το πρότυπο 3GPP NR. Οι κύριες προσομοιωμένες οντότητες δικτύου είναι το gNodeB (gNB) – ο σταθμός βάσης 5G – και ο Εξοπλισμός Χρήστη (UE) , μαζί με τα επίπεδα στοίβας πρωτοκόλλων (PHY, MAC, RLC, PDCP) για το καθένα. Το gNB στο 5G-LENA είναι ανάλογο με ένα eNodeB στο LTE: χειρίζεται μεταδόσεις φυσικού επιπέδου (διαμόρφωση OFDM, κωδικοποίηση/αποκωδικοποίηση) και προγραμματισμό του επιπέδου MAC των πόρων ραδιοφώνου σε UE. Οι UE υλοποιούν τα αντίστοιχα επίπεδα πρωτοκόλλου και επικοινωνούν με το gNB μέσω της προσομοιωμένης ασύρματης διεπαφής. Η μονάδα 5G-LENA παρέχει ένα λεπτομερές μοντέλο PHY που υποστηρίζει πολλαπλές ζώνες συχνοτήτων και διαμορφώσεις εύρους ζώνης, ενώ χρησιμοποιεί μια αφαίρεση για την πραγματική κυματομορφή για να παραμείνει υπολογιστικά αποδοτική. Περιλαμβάνονται μοντέλα υψηλής πιστότητας προγραμματισμού MAC, HARQ και προσαρμογής συνδέσμων, επιτρέποντας στους ερευνητές να δοκιμάσουν προσαρμοσμένους αλγόριθμους. Παρόλο που το 5G-LENA δεν περιλαμβάνει πλήρες μοντέλο δικτύου 5G Core, εφαρμόζει έναν βασικό πυρήνα για συνδεσιμότητα (π.χ. απλή δρομολόγηση της κυκλοφορίας των χρηστών), έτσι ώστε να μπορεί να αξιολογηθεί η επικοινωνία από άκρο σε άκρο μεταξύ των UE και ενός εξωτερικού κεντρικού υπολογιστή . Συνολικά, η αρχιτεκτονική είναι εξαιρετικά αρθρωτή: νέοι αλγόριθμοι ή πρωτόκολλα μπορούν να ενσωματωθούν επεκτείνοντας τις κλάσεις C++ που αντιπροσωπεύουν αυτά τα στοιχεία δικτύου.

4.1.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Η ευελιξία του ns-3 με 5G-LENA το καθιστά κατάλληλο για ένα ευρύ φάσμα ερευνητικών σεναρίων 5G. Οι βασικές εφαρμογές περιλαμβάνουν:

- Αλγόριθμοι προγραμματισμού πόρων ραδιοφώνου: Το 5G-LENA χρησιμοποιείται ευρέως για το σχεδιασμό και την αξιολόγηση προγραμματιστών επιπέδων MAC που κατανέμουν πόρους χρόνου-συχνότητας μεταξύ των UE. Ο αποτελεσματικός προγραμματισμός είναι κρίσιμος για την Ποιότητα Υπηρεσίας (QoS) και μπορούμε να συγκρίνουμε αλγόριθμους κάτω από διάφορους φόρτους κίνησης και συνθήκες καναλιού.
- Βελτιστοποίηση κινητικότητας και παράδοσης: Ο προσομοιωτής επιτρέπει την ανάλυση της κινητικότητας UE σε πολλαπλά κελιά σε ένα δίκτυο 5G NR. Με τη μοντελοποίηση

των UE που κινούνται και παραδίδονται μεταξύ των gNB, βελτιστοποιούνται οι αλγόριθμοι και οι παραμέτροι μεταβίβασης για να διατηρήθει η συνδεσιμότητα και η απόδοση.

- Ασφάλεια και Μετριασμός Επιθέσεων: Σε συνδυασμό με άλλες μονάδες ns-3, το 5G-LENA μπορεί να προσομοιώσει σενάρια ασφαλείας. Για παράδειγμα, μπορεί κανείς να μελετήσει τον αντίκτυπο των επιθέσεων άρνησης υπηρεσίας (DoS) ή ραδιοεμπλοκής στο RAN και να αξιολογήσει στρατηγικές μετριασμού, καθώς το εργαλείο μπορεί να δημιουργήσει κακόβουλα μοτίβα κυκλοφορίας και να μετρήσει τις επιπτώσεις τους στην απόδοση του δικτύου.
- Ετερογενής Διασύνδεση Δικτύων: Το 5G-LENA υποστηρίζει σενάρια όπου το 5G NR συνυπάρχει με δίκτυα LTE ή Wi-Fi (μέσω των μονάδων LTE και Wi-Fi του ns-3). Αυτό επιτρέπει την έρευνα σχετικά με τη συνεργασία και την κινητικότητα μεταξύ RAT (Τεχνολογία Πρόσβασης Ραδιοφώνου), όπως η ανάπτυξη της NSA ή η εκφόρτωση της κίνησης μεταξύ 5G και Wi-Fi, και η αξιολόγηση των στρατηγικών πολλαπλής συνδεσιμότητας.

Επιπλέον, το 5G-LENA είναι χρήσιμο για τη μελέτη τεχνικών φυσικών επιπέδων (μέσω του επεκτάσιμου μοντέλου PHY) και την απόδοση από άκρο σε άκρο για διάφορα μοντέλα κίνησης εφαρμογών. Έχει χρησιμοποιηθεί σε μελέτες πολυπλεξίας υπηρεσιών URLLC έναντι eMBB, μαζικής πρόσβασης IoT και άλλων αναδυόμενων θεμάτων 5G.

4.1.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Ένα σημαντικό πλεονέκτημα του ns-3 με το 5G-LENA είναι η φύση ανοιχτού κώδικα και η υποστήριξη της κοινότητας. Ερευνητές σε όλο τον κόσμο συμβάλλουν σε βελτιώσεις, διασφαλίζοντας ότι ο προσομοιωτής παραμένει ενημερωμένος με τις πιο πρόσφατες δυνατότητες και περιπτώσεις χρήσης. Επειδή το 5G-LENA ενσωματώνεται με το ευρύτερο πλαίσιο ns-3, μπορεί να μοντελοποιήσει πολύπλοκα σενάρια που εκτείνονται σε πολλούς τομείς δικτύου (ασύρματη πρόσβαση, πυρήνας IP, εφαρμογές) σε μία μόνο προσομοίωση. Το επίπεδο λεπτομέρειας που παρέχεται (πλήρης στοίβα πρωτοκόλλου στο RAN) καθιστά δυνατή τη λήψη λεπτομερών μετρήσεων απόδοσης και το σύστημα καταγραφής/ιχνηλασίας του ns-3 παρέχει πληροφορίες για τη συμπεριφορά του πρωτοκόλλου σε κλίμακα. Πράγματι, το 5G-LENA έχει βαθμονομηθεί σύμφωνα με τα πρότυπα 3GPP και θεωρείται προσομοιωτής υψηλής πιστότητας για το 5G NR *[42]*, κατάλληλος τόσο για ακαδημαϊκή όσο και για κάποια βιομηχανική χρήση E&A.

Προκλήσεις: Από την άλλη πλευρά, η πολυπλοκότητα του 5G-LENA σημαίνει ότι οι χρήστες χρειάζονται μια βαθιά κατανόηση των πρωτοκόλλων ns-3 και 5G για να το χρησιμοποιήσουν αποτελεσματικά. Η ρύθμιση της ενότητας μπορεί να περιλαμβάνει τη διασφάλιση συγκεκριμένων εκδόσεων ns-3 και την εφαρμογή ενημερώσεων κώδικα από το χώρο αποθήκευσης των προγραμματιστών. Ορισμένες προηγμένες λειτουργίες 5G – για παράδειγμα, πλήρης υποστήριξη για τεμαχισμό δικτύου ή εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης (URLLC) – δεν έχουν ακόμη εφαρμοστεί πλήρως ή βρίσκονται υπό ενεργό ανάπτυξη, γεγονός που μπορεί να περιορίσει ορισμένες μελέτες. Οι προσομοιώσεις μεγάλης κλίμακας με πολλούς UE και gNB μπορεί να είναι υπολογιστικά εντατικές, απαιτώντας συχνά σημαντικούς πόρους CPU και μνήμης και πιθανώς παράλληλη εκτέλεση για να εκτελεστούν σε εύλογο χρόνο. Αυτές οι προκλήσεις σημαίνουν ότι η καμπύλη μάθησης είναι απότομη και τα σενάρια προσομοίωσης πρέπει να βελτιστοποιούνται προσεκτικά για να αποφευχθούν υπερβολικοί χρόνοι εκτέλεσης.

4.1.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για να αποκτήσουν αξιόπιστα αποτελέσματα με το ns-3 και το 5G-LENA, οι ερευνητές έχουν συγκλίνει σε αρκετές βέλτιστες πρακτικές:

1. Ρύθμιση περιβάλλοντος: Προτείνεται μια συμβατή έκδοση ns-3 όπως καθορίζεται από τους προγραμματιστές του 5G-LENA (συχνά παρέχεται ως συσκευασμένη έκδοση ή συγκεκριμένο κλάδο Git). Κατασκευάζεται το ns-3 με ενεργοποιημένη τη μονάδα 5G-LENA και επαληθεύεται την εγκατάσταση με δείγματα προγραμμάτων.
2. Modular Scenario Design: Κώδικας προσομοίωσης δομής διαχωρίζοντας τη διαμόρφωση τοπολογίας, τα μοντέλα κινητικότητας, τη δημιουργία κίνησης και τις παραμέτρους πρωτοκόλλου σε διακριτά στοιχεία (π.χ. ξεχωριστές κλάσεις ή συναρτήσεις). Αυτή η σπονδυλωτή προσέγγιση διευκολύνει την τροποποίηση και την επανάληψη των πειραμάτων για διαφορετικά σενάρια.
3. Αναπαραγωγιμότητα: Ορισμός σταθερών σπόρων δημιουργίας τυχαίων αριθμών για κάθε εκτέλεση προσομοίωσης. Αυτό διασφαλίζει ότι άλλοι ερευνητές μπορούν να αναπαράγουν τα ακριβή αποτελέσματα, τα οποία είναι απαραίτητα για την ακαδημαϊκή αυστηρότητα.
4. Συλλογή δεδομένων: Ενεργοποιήση της ανίχνευσης και καταγραφής του ns-3 για να λεπτομερείς μετρήσεις. Αποθήκευση των βασικών δεδομένων εξόδου (διακίνηση, καθυστέρηση, απώλεια πακέτων, αποφάσεις προγραμματιστή κ.λπ.) για να εντοπιστούν αρχεία ή αρχεία CSV για μετα-επεξεργασία. Η χρήση εργαλείων όπως το ns-3 FlowMonitor ή εξωτερικοί αναλυτές (σενάρια Python, Wireshark) μπορεί να βοηθήσει στην ανάλυση και την οπτικοποίηση των αποτελεσμάτων.
5. Βελτιστοποίηση πόρων: Για μεγάλα σενάρια, εξετάζεται το ενδεχόμενο της εκτέλεσης προσομοιώσεων σε ισχυρό υλικό ή να ενεργοποιήση της υποστήριξης ns-3 για κατανεμημένη προσομοίωση ή πολλαπλών νημάτων (εάν υπάρχει). Απλοποιούνται οι πτυχές του μοντέλου (για παράδειγμα, χρησιμοποιείται μια αφαίρεση PHY αντί για λεπτομερή μοντελοποίηση σφαλμάτων) όταν δεν απαιτείται απόλυτη λεπτομέρεια, για να μειωθεί ο χρόνος εκτέλεσης.

Ακολουθώντας αυτές τις οδηγίες, το ns-3 + 5G-LENA παρέχει ένα ισχυρό και ευέλικτο περιβάλλον προσομοίωσης 5G NR . Η ανοιχτή βάση κώδικα, η ενεργή κοινότητα ανάπτυξης και η λεπτομερής παραμετροποίηση το καθιστούν ένα κορυφαίο «εικονικό εργαστήριο» για δίκτυα κινητής τηλεφωνίας επόμενης γενιάς. Παρά την απότομη καμπύλη μάθησης και ορισμένα κενά χαρακτηριστικών, παραμένει ένα από τα πιο δημοφιλή εργαλεία για την ακαδημαϊκή έρευνα 5G και για την ανάπτυξη καινοτόμων υπηρεσιών δικτύου. Με την πάροδο του χρόνου, μπορούμε να περιμένουμε την ενσωμάτωση νέων χαρακτηριστικών 5G (π.χ. τεμαχισμός, προηγμένες κλάσεις QoS), ενισχύοντας περαιτέρω το 5G-LENA ως μια ολοκληρωμένη λύση για τη μελέτη των σύγχρονων υποδομών 5G.

4.2. srsRAN για 4G/5G RAN

Η εκρηκτική ανάπτυξη των ασύρματων δικτύων 4G και 5G έχει οδηγήσει τη ζήτηση για εργαλεία ανοιχτού κώδικα που υποστηρίζουν τη δημιουργία πρωτοτύπων και την έρευνα σε τεχνολογίες Δικτύου Πρόσβασης Ραδιοφώνου (RAN). Το srsRAN (παλαιότερα γνωστό ως srsLTE) είναι μια πλήρης σουίτα λογισμικού ανοιχτού κώδικα για ανάπτυξη 4G/5G RAN, που παρέχει υλοποιήσεις βασικών στοιχείων της στοίβας ραδιοφώνου LTE και NR τόσο για πειραματισμό όσο και για βιομηχανική χρήση. Χάρη στην ευελιξία και την ενεργό κοινότητά του, το srsRAN προσφέρει ένα

προσβάσιμο περιβάλλον για την κατασκευή πρωτοτύπων, την ανάλυση της απόδοσης και τη δοκιμή σεναρίων ασφαλείας σε συστήματα RAN.
Αρχικά σχεδιάστηκε ως μια σουίτα λογισμικού LTE, το srsRAN έχει εξελιχθεί για να περιλαμβάνει δυνατότητες 5G NR (που οδήγησε στη μετονομασία του από srsLTE σε srsRAN στις πρόσφατες εκδόσεις). Η εργαλειοθήκη περιλαμβάνει υλοποιήσεις λογισμικού των επιπέδων PHY, MAC, RLC και PDCP, καθώς και βασικές βασικές λειτουργίες δικτύωσης για LTE (το Evolved Packet Core) και απλοποιημένα βασικά στοιχεία 5G. Το έργο είναι κυρίως γραμμένο σε C++ και έχει σχεδιαστεί για να εκτελείται σε περιβάλλοντα Linux. Ένα χαρακτηριστικό γνώρισμα του srsRAN είναι η υποστήριξή του για εμπορικά ραδιόφωνα που καθορίζονται από λογισμικό (SDR) (όπως συσκευές USRP), επιτρέποντας στη στοίβα λογισμικού να διασυνδέεται με πραγματικό υλικό ραδιοσυχνοτήτων για μετάδοση μέσω αέρος. Αυτό σημαίνει ότι το srsRAN μπορεί να λειτουργεί ως ζωντανό δίκτυο: για παράδειγμα, ένας ερευνητής μπορεί να αναπτύξει μια εγκατάσταση εργαστηρίου όπου το srsRAN λειτουργεί ως gNodeB (ή eNodeB) και UE, επικοινωνώντας μέσω πραγματικών ραδιοφωνικών σημάτων χρησιμοποιώντας υλικό SDR.

4.2.1. Βασικά Στοιχεία και Αρχιτεκτονική

Η αρχιτεκτονική srsRAN είναι οργανωμένη σε διάφορα στοιχεία που αντικατοπτρίζουν ένα κυψελοειδές δίκτυο από άκρο σε άκρο: 7

- srsENB: Υλοποιεί τις λειτουργίες ενός LTE eNodeB, συμπεριλαμβανομένης της πλήρους στοίβας πρωτοκόλλου (PHY/MAC/RLC/PDCP και επίπεδο ελέγχου RRC) για το σταθμό βάσης. Στη λειτουργία 5G, υπάρχει μια παρόμοια οντότητα gNodeB (συχνά αναφέρεται απλώς ως srsGNB στην τεκμηρίωση) η οποία επεκτείνει αυτές τις δυνατότητες για το NR.
- srsEPC: Παρέχει μια βασική υλοποίηση του βασικού δικτύου 4G (Evolved Packet Core), συμπεριλαμβανομένων οντοτήτων όπως το Mobility Management Entity (MME), το Serving Gateway (SGW) και το Packet Gateway (PGW). Αυτό επιτρέπει στο srsRAN να χειρίζεται βασικές λειτουργίες δικτύου, όπως έλεγχο ταυτότητας, διαχείριση κινητικότητας και δρομολόγηση δεδομένων χρήστη σε εξωτερικά δίκτυα. Για τη λειτουργία 5G Standalone (SA), οι τρέχουσες εκδόσεις της διεπαφής srsRAN με εξωτερικές υλοποιήσεις πυρήνα 5G (όπως το Open5GS), αν και η ανάπτυξη συνεχίζεται για την ενσωμάτωση βασικών λειτουργιών.
- srsUE: Προσομοιώνει μια συσκευή Εξοπλισμού Χρήστη, λειτουργώντας αποτελεσματικά ως UE λογισμικού που μπορεί να συνδεθεί σε ένα srsENB/gNB ή ακόμα και σε εμπορικά eNodeB/gNB. Αυτό το στοιχείο επιτρέπει στην πλατφόρμα να λειτουργεί ως «τηλέφωνο» ή τερματικό, δημιουργώντας κίνηση και ανταποκρινόμενη σε σήματα δικτύου για σκοπούς δοκιμής.

Στο πλαίσιο του 5G NR, η srsRAN εισήγαγε αντίστοιχα στοιχεία δικτύου 5G (ένα gNB και άγκιστρα για έναν πυρήνα 5G) για να επεκταθούν πέρα από το LTE. Δίνει έμφαση στη δυνατότητα διαμόρφωσης βασικών παραμέτρων, όπως το εύρος ζώνης καναλιού, η απόσταση υποφορέων και τα σχήματα διαμόρφωσης. Για να διαχειριστεί την αυξημένη πολυπλοκότητα του 5G διατηρώντας παράλληλα τη λειτουργία σε πραγματικό χρόνο σε υλικό SDR, το srsRAN χρησιμοποιεί τεχνικές όπως η απλοποίηση του επιπέδου PHY (μερική επεξεργασία μπορεί να προσεγγιστεί ή να εκφορτωθεί) και την προσεκτική βελτιστοποίηση των διαδρομών κώδικα. Η πλατφόρμα μπορεί

7 https://www.srslte.com/5g

να λειτουργήσει σε λειτουργία loopback (UE και gNB στο ίδιο μηχάνημα, χωρίς πραγματική έξοδο RF) για προσομοίωση καθαρού λογισμικού ή με SDR για πραγματικές δοκιμές RF.
Συνολικά, η αρχιτεκτονική του srsRAN είναι αρθρωτή: κάθε στοιχείο (ENB, EPC, UE) μπορεί να εκτελεστεί ανεξάρτητα ή μαζί. Σε μια τυπική εγκατάσταση, ένας χρήστης μπορεί να εκτελέσει τα srsENB και srsEPC σε έναν υπολογιστή συνδεδεμένο σε ένα SDR που λειτουργεί ως σταθμός βάσης και να εκτελέσει το srsUE σε άλλο υπολογιστή (με άλλο SDR ως UE) – δημιουργώντας μια πλήρη ροή κλήσεων. Επειδή ο κώδικας είναι ανοιχτού κώδικα και καλά δομημένος, οι ερευνητές μπορούν να τροποποιήσουν αλγόριθμους χαμηλότερου επιπέδου (π.χ. προγραμματισμό, HARQ, επεξεργασία σήματος) και να παρατηρήσουν αμέσως την επίδρασή τους είτε σε προσομοιωμένο είτε σε πραγματικό περιβάλλον.

4.2.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Το srsRAN βρίσκει εφαρμογή σε ένα ευρύ φάσμα σεναρίων που καλύπτουν την ακαδημαϊκή έρευνα και τη βιομηχανική καινοτομία:

- Ακαδημαϊκός Πειραματισμός: Οι μαθητές και οι ερευνητές χρησιμοποιούν το srsRAN για τη διεξαγωγή πειραμάτων τόσο σε πραγματικές συνθήκες (ραδιόφωνο over-the-air) όσο και σε ελεγχόμενες εργαστηριακές συνθήκες (RF loopback). Για παράδειγμα, μπορεί κανείς να τροποποιήσει αλγόριθμους προγραμματισμού MAC ή διαμορφώσεις RLC στο srsRAN και στη συνέχεια να αξιολογήσει την απόδοση και την καθυστέρηση εκτελώντας ένα δοκιμαστικό δίκτυο με αυτές τις αλλαγές. Η δυνατότητα εκτέλεσης πραγματικών επικοινωνιών από άκρο σε άκρο (με πραγματική κίνηση IP) επιτρέπει την αξιολόγηση της απόδοσης των νέων ιδεών σε ένα σχεδόν ρεαλιστικό περιβάλλον.
- Επίδειξη ταχείας πρωτοτυποποίησης και απόδειξης ιδέας (PoC): Σε ένα βιομηχανικό πλαίσιο, η ευελιξία του srsRAN επιταχύνει την ανάπτυξη πρωτοτύπων. Οι εταιρείες και τα εργαστήρια το χρησιμοποιούν για να δημιουργήσουν γρήγορα ένα ιδιωτικό δίκτυο LTE/5G για να παρουσιάσουν νέες ιδέες – για παράδειγμα, μια προσαρμοσμένη δυνατότητα RAN ή μια εφαρμογή που απαιτεί υπολογιστική ακμή. Επειδή βασίζεται σε λογισμικό, οι αλλαγές μπορούν να γίνουν και να δοκιμαστούν σε ημέρες, κάτι που είναι πολύ πιο γρήγορο και φθηνότερο από την τροποποίηση του εμπορικού εξοπλισμού.
- Δοκιμή ασφαλείας: Το srsRAN επιτρέπει ελεγχόμενα πειράματα ασφαλείας σε δίκτυα 4G/5G. Οι ερευνητές μπορούν να εκτελέσουν δοκιμές διείσδυσης, να αναλύσουν φαινόμενα παρεμβολών ή παρεμβολών και να αξιολογήσουν την ανθεκτικότητα της στοίβας δικτύου έναντι επιθέσεων. Για παράδειγμα, θα μπορούσε κανείς να προσομοιώσει μια επίθεση άρνησης υπηρεσίας στο RAN χρησιμοποιώντας το srsUE για να στείλει μηνύματα με κακή μορφή ή να πλημμυρίσει το κανάλι ελέγχου και να παρατηρήσει πώς το χειρίζεται το srsENB/gNB. Τόσο τα σενάρια 4G όσο και 5G μπορούν να εξεταστούν με αυτόν τον τρόπο, κάτι που είναι πολύτιμο για τη βελτίωση της ευρωστίας του δικτύου.

Συγκεκριμένα, το srsRAN μπορεί να ενσωματωθεί με άλλα έργα ανοιχτού κώδικα. Μια κοινή ρύθμιση για τον πειραματισμό 5G SA είναι η χρήση του srsRAN για το gNB και το UE, ενώ χρησιμοποιείται ένας πυρήνας ανοιχτού κώδικα όπως το Open5GS (δείτε την επόμενη ενότητα) για τον Πυρήνα 5G – αυτό παρέχει ένα πλήρες δίκτυο 5G εξ ολοκλήρου σε λογισμικό 8[43].

8 open5gs.org

Τέτοιες ρυθμίσεις χρησιμοποιούνται για την αξιολόγηση της διαλειτουργικότητας και της απόδοσης των ανοιχτών λύσεων 5G πολλών προμηθευτών 9.

4.2.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Η φύση ανοιχτού κώδικα του srsRAN ενισχύει τη διαφάνεια και τη συνεργατική ανάπτυξη. Οι χρήστες σε όλο τον κόσμο συνεισφέρουν διορθώσεις κώδικα και νέες δυνατότητες, δημιουργώντας ένα δυναμικό περιβάλλον για την έρευνα RAN . Η υποστήριξη για υλικό SDR είναι ένα σημαντικό πλεονέκτημα – συνδέοντας σε συσκευές όπως το USRP ή το LimeSDR, το srsRAN μπορεί να μετατρέψει έναν κανονικό υπολογιστή σε λειτουργικό σταθμό βάσης ή UE, επιτρέποντας τη ζωντανή δοκιμή που θολώνει τη γραμμή μεταξύ προσομοίωσης και πραγματικής ανάπτυξης. Αυτή η ικανότητα είναι ζωτικής σημασίας για τη γεφύρωση θεωρίας και πρακτικής στην ασύρματη έρευνα. Ένα άλλο πλεονέκτημα είναι η εκτενής τεκμηρίωση και τα παραδείγματα που παρέχονται από την κοινότητα, καθώς και οι διαμορφώσεις αναφοράς για διάφορα σενάρια (για παράδειγμα, παραδείγματα αρχείων διαμόρφωσης για διαφορετικά εύρη ζώνης ή ρυθμίσεις πολλαπλών UE). Σε σύγκριση με ιδιόκτητες λύσεις, το χαμηλό κόστος και η πρόσβαση σε κώδικα του srsRAN το καθιστούν ιδανικό για εκπαιδευτικά και ερευνητικά εργαστήρια χαμηλού προϋπολογισμού. Πράγματι, το srsLTE/srsRAN χρησιμοποιείται ευρέως από την ασύρματη κοινότητα E&A github.com και έχει αναφερθεί ως ένα από τα πιο δημοφιλή εργαλεία για την έρευνα ασφάλειας LTE/5G 10*[43]*.
Προκλήσεις: Η επίτευξη της καλύτερης απόδοσης με το srsRAN μπορεί να απαιτεί προσεκτική ρύθμιση του υλικού και του λογισμικού. Η λειτουργία σε πραγματικό χρόνο σε SDR σημαίνει ότι ο κεντρικός υπολογιστής πρέπει να ανταποκρίνεται στις απαιτήσεις επεξεργασίας. Απαιτείται μια πολυπύρηνη CPU με υποστήριξη για υψηλούς ρυθμούς ρολογιού και επαρκή μνήμη για την προσέγγιση των μέγιστων ρυθμών δεδομένων. Οι χρήστες πρέπει να διασφαλίσουν ότι το SDR και το πρόγραμμα οδήγησης (DPDK ή UHD για USRP) έχουν διαμορφωθεί σωστά (ενεργοποιούνται τεράστιες σελίδες, απομονωμένοι πυρήνες CPU για την επεξεργασία νημάτων, κ.λπ.) για να αποφευχθούν υπερβάσεις ή υπερβάσεις στη ραδιοφωνική μετάδοση. Η καμπύλη εκμάθησης για το srsRAN μπορεί να είναι απότομη για όσους δεν είναι εξοικειωμένοι με τα κυψελωτά πρωτόκολλα – η διαμόρφωση παραμέτρων όπως τα αναγνωριστικά PLMN, οι κωδικοί περιοχής παρακολούθησης (TAC) και τα κλειδιά ασφαλείας μεταξύ gNB και πυρήνα απαιτεί προσοχή στη λεπτομέρεια. Επιπλέον, ορισμένες προηγμένες λειτουργίες 5G βρίσκονται ακόμη υπό ανάπτυξη στο srsRAN. Για παράδειγμα, λειτουργίες όπως η διπλή συνδεσιμότητα (LTE + NR ταυτόχρονα) ή ορισμένες ειδικές διαδικασίες για το 5G ενδέχεται να απλοποιηθούν ή να μην είναι πλήρως συμβατές με το 3GPP ακόμη, καθώς το έργο εξελίσσεται συνεχώς. Όπως συμβαίνει με πολλά έργα τηλεπικοινωνιών ανοιχτού κώδικα, η παρακολούθηση της πιο πρόσφατης έκδοσης και των αλλαγών (logs) είναι σημαντική για τη σταθερότητα.
Παρόλα αυτά, η αντιστάθμιση του srsRAN μεταξύ πιστότητας και πρακτικότητας είναι καλά ισορροπημένη για πολλές περιπτώσεις χρήσης: παρέχει ένα πραγματικό περιβάλλον σήματος με επαρκείς λεπτομέρειες πρωτοκόλλου, με κόστος χαρακτηριστικών πολύ υψηλής συχνότητας ή ακραίων βελτιστοποιήσεων που μπορεί να έχουν οι ιδιόκτητες στοίβες.

9 gitlab.unistra.fr
10 open5g.info

4.2.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για επιτυχή χρήση του srsRAN σε ακαδημαϊκά περιβάλλοντα ή περιβάλλοντα E&A, προτείνονται οι ακόλουθες οδηγίες:11

- Δοκιμή σταδιακά: Το srsRAN εκτελείται σε μια απλή λειτουργία επαναφοράς (δηλαδή, srsENB και srsUE στο ίδιο μηχάνημα χωρίς RF). Αυτό επαληθεύει ότι η στοίβα λογισμικού λειτουργεί σωστά σε ελεγχόμενη ρύθμιση πριν προσθέσει την πολυπλοκότητα του ραδιοεξοπλισμού.
- Διαμόρφωση SDR: Όταν γίνεται μετάβαση σε δοκιμές over-the-air με SDR, βεβαιώνεται ότι οι παράμετροι ραδιοφώνου (κεντρική συχνότητα, κέρδος, ρυθμός δειγματοληψίας) έχουν ρυθμιστεί σωστά και αντιστοιχίζονται μεταξύ πομπού και δέκτη. Μικρές εσφαλμένες διαμορφώσεις μπορεί να προκαλέσουν παρεμβολές ή αποτυχία σύνδεσης. Χρησιμοποιούνται εργαλεία ανάλυσης φάσματος ή την ανάδραση του SDR (π.χ. αναφερόμενο RSSI) για να την περαιτέρω προσαρμογή αυτών των παραμέτρων.
- Διαχείριση λογισμικού και εκδόσεων: Προτείνεται η παρακολούθηση των σημειώσεων και η τεκμηρίωση της έκδοσης του srsRAN για ενημερώσεις. Επειδή η ανάπτυξη srsRAN είναι ενεργή, οι νέες εκδόσεις ενδέχεται να διορθώσουν σφάλματα ή να προσθέσουν λειτουργίες κρίσιμες για τα πειράματά σας. Συνιστάται να χρησιμοποιείται η πιο πρόσφατη σταθερή έκδοση ή συγκεκριμένες εκδόσεις με ετικέτα που είναι γνωστό ότι λειτουργούν με το υλικό μας. Συνίσταται επίσης η παρακολούθηση των φόρουμ κοινότητας ή τα ζητήματα του GitHub για γνωστά προβλήματα και επιδιορθώσεις.
- Μόχλευση πόρων κοινότητας: Η κοινότητα srsRAN παρέχει σεμινάρια και παραδείγματα διαμορφώσεων που χρησιμεύουν ως ένα καλό σημείο εκκίνησης. Για παράδειγμα, είναι διαθέσιμες διαμορφώσεις για πολλαπλούς UE ή για την ενεργοποίηση συγκεκριμένων λειτουργιών (όπως η λειτουργία NSA με εξωτερικό EPC). Ξεκινώντας από αυτά τα παραδείγματα εξοικονομείται χρόνος.
- Καταγραφή και παρακολούθηση: Συνίσταται η ενεργοποίηση της λεπτομερής καταγραφής στο srsRAN (με κατάλληλο επίπεδο καταγραφής) για την αντιμετώπιση προβλημάτων. Το srsRAN μπορεί επίσης να παράγει μετρήσεις που μπορούν να παρακολουθούνται με την πάροδο του χρόνου. Η ενσωμάτωση με εξωτερικά εργαλεία παρακολούθησης (πίνακες εργαλείων Grafana, Prometheus κ.λπ.) μπορεί να είναι χρήσιμη για μακροχρόνιες δοκιμές .

Ακολουθώντας αυτές τις πρακτικές, αξιοποιείται το srsRAN ως μια προηγμένη λύση ανοιχτού κώδικα για την υλοποίηση 4G/5G RAN . Ενώ απαιτείται εξειδικευμένη γνώση για τη διαμόρφωση και τη βελτιστοποίησή της, η πλατφόρμα παρέχει μια μοναδική ευκαιρία μελέτης πραγματικών κυψελοειδών αρχιτεκτονικών με χαμηλό κόστος. Καθώς το 5G συνεχίζει να εξελίσσεται (και κοιτάζοντας μπροστά στο 6G), το srsRAN είναι πιθανό να ενσωματώσει περισσότερες δυνατότητες, ενισχύοντας τον ρόλο του ως βασικό πυλώνα της έρευνας ασύρματου ανοιχτού κώδικα.

4.3. Συνδυασμός Open5GS / UERANSIM

Το οικοσύστημα 5G εισάγει όχι μόνο νέες διεπαφές ραδιοφώνου αλλά και μια επανασχεδιασμένη αρχιτεκτονική βασικού δικτύου. Σε αυτό το πλαίσιο, οι λύσεις ανοιχτού κώδικα που επιτρέπουν

11 https://ieeexplore.ieee.org/document/10220512

στους ερευνητές να πειραματιστούν με τον πυρήνα 5G (5GC) και την αλληλεπίδρασή του με το RAN είναι ζωτικής σημασίας. Το Open5GS είναι μια δημοφιλής υλοποίηση ανοιχτού κώδικα ενός δικτύου πυρήνα 5G (και παλαιού τύπου 4G πυρήνα), ενώ το UERANSIM (User Equipment and RAN Simulator) είναι ένα εργαλείο ανοιχτού κώδικα που προσομοιώνει το 5G RAN (gNB) και το 5G UE. Μαζί, το Open5GS και το UERANSIM επιτρέπουν τη δημιουργία ενός πλήρους αυτόνομου περιβάλλοντος δικτύου 5G – από τις βασικές λειτουργίες δικτύου έως την πρόσβαση μέσω ραδιοφώνου – χωρίς την ανάγκη αποκλειστικού λογισμικού ή πραγματικού υλικού 5G. Αυτή η συνέργεια είναι ισχυρή για έρευνα και δοκιμές, καθώς οι χρήστες μπορούν να μελετήσουν τη συμπεριφορά 5G από άκρο σε άκρο εξ ολοκλήρου σε λογισμικό.
Το Open5GS παρέχει υλοποιήσεις των θεμελιωδών λειτουργιών του δικτύου 5GC όπως ορίζονται από το 3GPP. Περιλαμβάνει στοιχεία όπως η Λειτουργία διαχείρισης πρόσβασης και κινητικότητας (AMF), Λειτουργία διαχείρισης περιόδου λειτουργίας (SMF), Λειτουργία επιπέδου χρήστη (UPF), λειτουργία διακομιστή ελέγχου ταυτότητας (AUSF) και άλλα, ευθυγραμμισμένα με τις προδιαγραφές έκδοσης 3GPP 15+. Ουσιαστικά, το Open5GS καλύπτει τις οντότητες του επιπέδου ελέγχου και του επιπέδου χρήστη που απαιτούνται για τη δημιουργία και τη διαχείριση συνδέσεων 5G – ανάλογο με το LTE EPC αλλά για το 5G. Επίσης, εξακολουθεί να υποστηρίζει τη λειτουργικότητα LTE EPC, επιτρέποντας συνδυασμένες αναπτύξεις 4G/5G σε μία πλατφόρμα . Το Open5GS είναι γραμμένο σε C και έχει σχεδιαστεί για να μπορεί να αναπτυχθεί σε τυπικά συστήματα Linux (x86 ή ARM), καθιστώντας εφικτή την εκτέλεση ενός πλήρους πυρήνα 5G σε υλικό βασικών προϊόντων. Δίνει έμφαση στην ευκολία ανάπτυξης και διαμόρφωσης, ώστε οι χρήστες να μπορούν να έχουν ένα βασικό βασικό δίκτυο 5G που λειτουργεί με ελάχιστη επιβάρυνση.
Το UERANSIM, από την άλλη πλευρά, εστιάζει στην πλευρά του RAN. Παρέχει μια προσομοιωμένη εφαρμογή gNodeB και 5G UE που μπορεί να συνδεθεί σε έναν πυρήνα 5G μέσω τυπικών πρωτοκόλλων. Σε αντίθεση με το srsRAN που παράγει πραγματικά σήματα ραδιοσυχνοτήτων, το UERANSIM λειτουργεί εξ ολοκλήρου στον τομέα λογισμικού (δεν απαιτείται SDR) – προσομοιώνει τη στοίβα πρωτοκόλλου ραδιοφώνου 5G NR και χρησιμοποιεί κανονικές υποδοχές IP για να μεταφέρει την κίνηση και τη σηματοδότηση μεταξύ του προσομοιωμένου gNB/UE και του βασικού δικτύου. Με άλλα λόγια, το UERANSIM μιμείται ό,τι συμβαίνει μέσω του αέρα μεταφράζοντας το σε μηνύματα IP (για παράδειγμα, μεταφέροντας μηνύματα RRC και NAS μέσω μιας σύνδεσης SCTP/IP στο AMF). Αυτή η προσέγγιση θυσιάζει τον ρεαλισμό του φυσικού επιπέδου, αλλά απλοποιεί σημαντικά τη ρύθμιση, καθώς μπορεί κανείς να τρέξει ένα 5G RAN σε οποιοδήποτε μηχάνημα χωρίς εξειδικευμένο υλικό. Το UERANSIM έχει ονομαστεί το πρώτο ανοιχτού κώδικα 5G αυτόνομη υλοποίηση UE/gNB[12]και είναι χρήσιμο για τον έλεγχο της λειτουργικότητας του βασικού δικτύου 5G και των διαδικασιών σηματοδότησης.

4.3.1. Βασικά Στοιχεία και Αρχιτεκτονική

Σε μια ανάπτυξη Open5GS + UERANSIM, ο καταμερισμός της εργασίας είναι ως εξής: Το Open5GS χειρίζεται τις λειτουργίες του βασικού δικτύου (5GC) και το UERANSIM παρέχει την προσομοίωση RAN και UE. Διασυνδέονται μέσω των τυπικών διεπαφών δικτύου 5G NG (N1,

12 github.com

N2, N3, κ.λπ.), οι οποίες στην πράξη υλοποιούνται μέσω IP, καθώς πρόκειται για εικονικό περιβάλλον. Η αρχιτεκτονική μπορεί να περιγραφεί με βάση τα βασικά λειτουργικά στοιχεία:13

- AMF (Λειτουργία Διαχείρισης Πρόσβασης και Κινητικότητας) και SMF (Λειτουργία Διαχείρισης Συνεδρίας): Στο Open5GS, αυτές οι λειτουργίες επιπέδου ελέγχου διαχειρίζονται τη σηματοδότηση NAS από το UE (καταχώριση, έλεγχος ταυτότητας) και τη ρύθμιση περιόδου σύνδεσης για δεδομένα χρήστη. Το AMF είναι το κύριο σημείο επαφής για το gNB (πάνω από τη διεπαφή N2) και χειρίζεται συμβάντα κινητικότητας (όπως η σηματοδότηση παράδοσης), ενώ το SMF εκχωρεί και διαχειρίζεται συνεδρίες PDU (ισοδύναμες με φορείς) σε συντονισμό με το UPF.
- UPF (Συνάρτηση επιπέδου χρήστη): Αυτή είναι η άγκυρα επιπέδου δεδομένων στον πυρήνα, υπεύθυνη για τη δρομολόγηση της κίνησης των χρηστών στον προορισμό της (π.χ. στο διαδίκτυο ή ένα εσωτερικό δίκτυο). Το UPF του Open5GS σε μια εγκατάσταση εργαστηρίου θα τερματίσει τις σήραγγες GTP-U από το gNB και θα προωθήσει τα πακέτα στην κατάλληλη εξωτερική διεπαφή ή τοπική διεργασία, επιτρέποντας τη σύνδεση IP από άκρο σε άκρο για το UE.
- gNB (5G Base Station) : Στο UERANSIM, το gNodeB υλοποιείται σε λογισμικό και επικοινωνεί με το Open5GS AMF/SMF μέσω των πρωτοκόλλων ελέγχου NG και επιπέδου χρήστη (NGAP μέσω SCTP για έλεγχο και GTP-U μέσω UDP για τα δεδομένα χρήστη). Το UERANSIM gNB αναλαμβάνει εργασίες όπως η διαχείριση σύνδεσης RRC και η προώθηση μηνυμάτων NAS μεταξύ του UE και του AMF, παρόμοια με τη συμπεριφορά ενός πραγματικού επιπέδου ελέγχου του gNB.
- UE (User Equipment): Εφαρμόζεται επίσης στο UERANSIM, το στοιχείο UE προσομοιώνει τη συμπεριφορά πρωτοκόλλου μιας συσκευής 5G. Θα ξεκινήσει την εγγραφή, θα καθιερώσει διαδικασίες ασφαλείας, θα δημιουργήσει συνεδρίες PDU (για δεδομένα) κ.λπ., χρησιμοποιώντας τα μηνύματα που θα έβλεπε κανείς από ένα πραγματικό μόντεμ. Το UERANSIM UE εκχωρεί στον εαυτό του μια διεύθυνση IP (συνήθως μέσω του DHCP του πυρήνα ή μιας προρυθμισμένης περιοχής) κατά την εγκατάσταση της περιόδου λειτουργίας, επιτρέποντάς του να στέλνει/λαμβάνει κίνηση εφαρμογής μέσω του πυρήνα και του gNB.

Μόλις ενσωματωθούν, αυτά τα στοιχεία επιτρέπουν τη δημιουργία ενός δοκιμαστικού δικτύου 5G στο οποίο ένας χρήστης μπορεί, για παράδειγμα, να εκτελέσει ένα αίτημα ping ή HTTP από την προσομοίωση UE σε έναν διακομιστή προσβάσιμο μέσω του UPF, βιώνοντας την πλήρη ροή εργασίας εγγραφής 5G και ρύθμισης περιόδου σύνδεσης στη διαδικασία. Οι διεπαφές μεταξύ τους (N1 για UE-AMF NAS, N2 για έλεγχο gNB-AMF, N3 για δεδομένα gNB-UPF) είναι όλες τυποποιημένες, επομένως το Open5GS και το UERANSIM διαλειτουργούν εκτός συσκευασίας χρησιμοποιώντας αυτά τα πρωτόκολλα.

Είναι σημαντικό να σημειωθεί ότι το UERANSIM δεν προσομοιώνει το επίπεδο ραδιοσυχνοτήτων ή το λεπτομερές PHY – υποθέτει ότι η ραδιοζεύξη λειτουργεί και εστιάζει στη σηματοδότηση υψηλότερου επιπέδου14. Αυτό σημαίνει ότι πτυχές όπως οι ραδιοπαρεμβολές ή ο λεπτομερής χρονισμός των καρέ αφαιρούνται. Αντίθετα, το πλεονέκτημα είναι ότι μπορεί κανείς να

13 https://github.com/IIITV-5G-and-Edge-Computing-Activity/Gr49EC431-5G-UE-and-RAN-Simulator-using-UERANSIM

14 *github.com*

περιστρέψει δεκάδες UE και πολλαπλά gNB σε ένα μόνο μηχάνημα, καθώς πρόκειται απλώς για διαδικασίες λογισμικού που επικοινωνούν μέσω συνδέσμων εικονικού δικτύου.

4.3.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Ο συνδυασμός του Open5GS με το UERANSIM προσφέρει πολλά πλεονεκτήματα, ειδικά σε ακαδημαϊκά και ερευνητικά περιβάλλοντα. Μερικές περιπτώσεις πρωτογενούς χρήσης περιλαμβάνουν:[44]

- Εκπαίδευση και κατάρτιση: Ένα άμεσο σενάριο είναι η διδασκαλία μαθητών ή η εκπαίδευση μηχανικών δικτύων σε διαδικασίες πυρήνα 5G και RAN. Με αυτήν τη ρύθμιση, μπορούν να παρατηρήσουν και να πειραματιστούν με τη διαδικασία εγγραφής και ελέγχου ταυτότητας , τη δημιουργία συνεδρίας PDU και άλλες λειτουργίες επιπέδου ελέγχου σε ένα δίκτυο 5G. Επειδή δεν χρειάζεται ειδικό υλικό, οποιοσδήποτε διαθέτει φορητό υπολογιστή μπορεί να τρέξει ένα μικροσκοπικό δίκτυο 5G, το οποίο είναι απίστευτα χρήσιμο για την εκμάθηση των πολύπλοκων ανταλλαγών σήματος 5G.
- Δοκιμή πρωτοκόλλου ασφαλείας (αξιολόγηση IDS/IPS): Οι ερευνητές που ενδιαφέρονται για την ασφάλεια 5G μπορούν να χρησιμοποιήσουν το Open5GS+UERANSIM για να μελετήσουν πώς το δίκτυο χειρίζεται κακόβουλη συμπεριφορά. Για παράδειγμα, μπορούν να προσομοιώσουν μια UE που εκτοξεύει μια επίθεση DoS ή στέλνει μη φυσιολογικά μηνύματα και να εξετάσει την απόκριση του πυρήνα. Εφόσον το Open5GS εφαρμόζει τυπική προστασία κρυπτογράφησης και ακεραιότητας, μπορεί κανείς να αξιολογήσει σενάρια όπως επιθέσεις επανάληψης ή man-in-the-middle (με ελεγχόμενη υποδομή πιστοποιητικών). Δημιουργώντας τόσο κανονικά όσο και κακόβουλα μοτίβα κυκλοφορίας μέσω του UERANSIM, μπορεί να αξιολογηθεί η αποτελεσματικότητα των συστημάτων ανίχνευσης ή πρόληψης εισβολής (IDS/IPS) για 5G. Προηγούμενες εργασίες δείχνουν ενδιαφέρον για την αναπαραγωγή επιθέσεων (όπως DDoS σε σηματοδότηση πυρήνα 5G) για τη δοκιμή της ανθεκτικότητας. [44]
- Ανάπτυξη και δοκιμή νέων υπηρεσιών: Το περιβάλλον επιτρέπει τη δοκιμή νέων χαρακτηριστικών ή εφαρμογών δικτύου 5G που απαιτούν εξειδικευμένη υποστήριξη από το βασικό δίκτυο. Για παράδειγμα, υπηρεσίες που χρειάζονται εξαιρετικά χαμηλή καθυστέρηση (URLLC) ή υψηλό εύρος ζώνης (eMBB) μπορούν να πρωτοτυποποιηθούν μέσω της προσαρμογής των παραμέτρων QoS στο Open5GS και της δημιουργίας κίνησης στο UERANSIM, ώστε να αξιολογηθεί ο αντίκτυπος στη διεκπεραίωση ή την καθυστέρηση. Επιπλέον, σενάρια κινητικότητας – παρόλο που το UERANSIM δεν προσομοιώνει τη φυσική μετακίνηση, μπορεί να μιμηθεί τη διαδικασία handover μεταφέροντας ένα UE ανάμεσα σε δύο περιπτώσεις gNB – δίνουν τη δυνατότητα δοκιμής της συνέχειας της υπηρεσίας για νέες εφαρμογές.
- **Διαμόρφωση βασικών δικτύων**: το Open5GS είναι ευέλικτο στην ανάπτυξη, έτσι οι ερευνητές μπορούν, για παράδειγμα, να διανέμουν τα στοιχεία του σε πολλούς διακομιστές (προσομοίωση μιας κλιμακούμενης ανάπτυξης) ή να εισάγουν διαμορφώσεις που μοιάζουν με τεμαχισμό δικτύου εκτελώντας πολλαπλές παράλληλες στιγμιότυπα πυρήνα και συσχετίζοντας UERANSIM UENSlices-Swith διαφορετικά UENSAIs. Ενώ η πραγματική υποστήριξη τεμαχισμού 5G εξακολουθεί να ωριμάζει σε αυτά τα εργαλεία, τέτοια πειράματα παρέχουν πληροφορίες για την απομόνωση πόρων πολλαπλών μισθώσεων και δικτύου.

Συνολικά, η πλατφόρμα Open5GS+UERANSIM επιτρέπει την αξιολόγηση από άκρο σε άκρο – από τη διεπαφή ραδιοφώνου (προσομοίωση) έως τα δεδομένα εφαρμογής – η οποία είναι ζωτικής σημασίας για ολιστικές μελέτες 5G.

4.3.3. Πλεονεκτήματα και Προκλήσεις Εφαρμογής

Πλεονεκτήματα: Ένα θεμελιώδες πλεονέκτημα αυτού του συνδυασμού είναι η φύση πλήρως ανοιχτού κώδικα και των δύο πλατφορμών. Ο πηγαίος κώδικας για το Open5GS και το UERANSIM είναι ανοιχτά διαθέσιμος στα αποθετήρια Git, επιτρέποντας τη συνεχή βελτίωση από την παγκόσμια κοινότητα. Αυτή η διαφάνεια προάγει τη διαφάνεια και την καινοτομία. νέες δυνατότητες (όπως υποστήριξη για μεταγενέστερες εκδόσεις 3GPP) μπορούν να προστεθούν από τους συνεργάτες. Για παράδειγμα, η κοινότητα εργάζεται σε λειτουργίες από την έκδοση 16 και μετά, και τέτοιες βελτιώσεις μπορούν να κοινοποιηθούν γρήγορα. Ένα άλλο πλεονέκτημα είναι η σχετικά χαμηλή απαίτηση πόρων: επειδή όλα είναι εικονικά, μπορεί κανείς να τρέξει έναν πυρήνα 5G και πολλές UE σε τυπικό υλικό (αντίθετα, η χρήση srsRAN με SDR μπορεί να απαιτεί εξειδικευμένο εξοπλισμό και περιορίζεται από ζητήματα εύρους ζώνης RF). Αυτό καθιστά εύκολη τη ρύθμιση περιβαλλόντων αυτοματοποιημένων δοκιμών ή αγωγών CI/CD για λογισμικό δικτύου 5G χρησιμοποιώντας αυτά τα εργαλεία. Επιπλέον, η χρήση τυποποιημένων διεπαφών σημαίνει ότι η γνώση που αποκτάται μπορεί να εφαρμοστεί άμεσα σε πραγματικά δίκτυα – π.χ. ένας μηχανικός που μαθαίνει να αντιμετωπίζει προβλήματα σε μια ροή μηνυμάτων NAS σε αυτήν τη ρύθμιση, μπορεί να εφαρμόσει την ίδια λογική σε ένα εμπορικό σύστημα 5G.
Προκλήσεις: Παρά τα πλεονεκτήματά του, η δημιουργία ενός δικτύου 5G SA με το Open5GS και το UERANSIM δεν είναι χωρίς εμπόδια. Ο πυρήνας 5G είναι αρκετά περίπλοκος, καθώς περιλαμβάνει πολλά αλληλοεξαρτώμενα πρωτόκολλα (NGAP, NAS, PFCP, κ.λπ.) και οι αρχάριοι μπορεί να βρουν την αρχική εγκατάσταση δύσκολη. Το Open5GS, αν και απλούστερο από ορισμένες εναλλακτικές, εξακολουθεί να απαιτεί σωστή διαμόρφωση των διεπαφών δικτύου, καταχωρίσεις βάσης δεδομένων για συνδρομητές (π.χ. εισαγωγή διαπιστευτηρίων SIM για το UERANSIM UE) και συντονισμό μεταξύ των λειτουργιών. Για παράδειγμα, η διαμόρφωση του UERANSIM (το plmn, ο κωδικός περιοχής παρακολούθησης, τα κλειδιά) πρέπει να ταιριάζει ακριβώς με τη διαμόρφωση του Open5GS για να εγγραφεί επιτυχώς το UE. Μια κοινή δυσκολία είναι να διασφαλιστεί ότι το AMF και το gNB συμφωνούν σε παραμέτρους όπως το αναγνωριστικό PLMN και οι αλγόριθμοι ασφαλείας. Επιπλέον, δεν υποστηρίζονται πλήρως όλες οι λειτουργίες 5G – ο διαχωρισμός δικτύου είναι ένα τέτοιο χαρακτηριστικό που εφαρμόζεται μόνο εν μέρει ή πειραματικά σε αυτές τις πλατφόρμες από τώρα. Οι χρήστες πρέπει να προσέχουν τη συμβατότητα της έκδοσης: μια ενημέρωση του Open5GS ή του UERANSIM ενδέχεται να εισάγει αλλαγές που απαιτούν ενημέρωση του άλλου. Συχνά απαιτείται ιδιαίτερη προσοχή στην τεκμηρίωση και στα φόρουμ της κοινότητας για την επίλυση προβλημάτων.
Μια άλλη πρόκληση έγκειται στην απόδοση: ενώ είναι λειτουργικό, το Open5GS μπορεί να μην επιτύχει εξωγενή απόδοση ποιότητας φορέα ή χαμηλή καθυστέρηση. Είναι γενικά επαρκής για μέτρια φορτία (έχει αποδειχθεί ότι χειρίζεται χιλιάδες πακέτα ανά δευτερόλεπτο), αλλά για δοκιμές πολύ υψηλού ρυθμού δεδομένων, μπορεί κανείς να συναντήσει σημεία συμφόρησης. Ομοίως, το UERANSIM απλοποιεί το φυσικό επίπεδο, επομένως δεν μπορεί να χρησιμοποιηθεί για τον έλεγχο συμπεριφορών που σχετίζονται με το RF (όπως καθυστερήσεις διάδοσης, εφέ διαμόρφωσης δέσμης κ.λπ.). Είναι κυρίως ένα εργαλείο αξιολόγησης επιπέδου ελέγχου και IP δεδομένων.

Παρά αυτές τις προκλήσεις, με προσεκτική διαμόρφωση και χρησιμοποιώντας αντίστοιχες εκδόσεις κάθε λογισμικού (διασφάλιση συμβατότητας), οι χρήστες δημιούργησαν επιτυχώς δοκιμές 5G. Στην πραγματικότητα, μια συγκριτική μελέτη πλατφορμών 5G ανοιχτού κώδικα έδειξε ότι το Open5GS παρέχει μεταξύ των καλύτερων επιδόσεων λανθάνοντος επιπέδου ελέγχου σε υλοποιήσεις πυρήνα 5G*[45]*, υπογραμμίζοντας την αποτελεσματικότητά του για τη δοκιμή σεναρίων βαριάς σηματοδότησης.

4.3.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την επιτυχή εφαρμογή και πειραματισμό με πυρήνα 5G και RAN χρησιμοποιώντας Open5GS και UERANSIM, συνιστώνται οι ακόλουθες βέλτιστες πρακτικές:[46]15

- Αυξητική άνοδος: Το Open5GS εκτελείται σε ένα μόνο μηχάνημα με ελάχιστες υπηρεσίες (AMF, SMF, UPF, κ.λπ.) και επαληθεύεται ότι λειτουργεί (π.χ. ο πυρήνας περιμένει για συνδέσεις). Στη συνέχεια, πραγματοποιείται εκκίνηση των gNB και UE της UERANSIM είτε στον ίδιο υπολογιστή είτε σε άλλο, και επιχειρείται μια βασική εγγραφή του UE. Αυτή η σταδιακή προσέγγιση βοηθά στην απομόνωση ζητημάτων (για παράδειγμα, εάν η εγγραφή αποτύχει, μπορεί κανείς να ελέγξει εάν η προσπάθεια της ΕΕ έφτασε στο AMF).
- Συνεπής διαμόρφωση: Βεβαιωνεται ότι όλες οι παράμετροι διαμόρφωσης είναι ευθυγραμμισμένες μεταξύ του πυρήνα και του RAN. Αυτό περιλαμβάνει το αναγνωριστικό PLMN , το TAC (Κωδικός περιοχής παρακολούθησης) , τα αναγνωριστικά τμημάτων δικτύου (αν χρησιμοποιούνται τμήματα) και τα διαπιστευτήρια ελέγχου ταυτότητας (π.χ. οι τιμές IMSI και K/OPc για τη SIM της UE, οι οποίες πρέπει να παρέχονται στη βάση δεδομένων συνδρομητών του Open5GS). Οι αναντιστοιχίες εδώ είναι μια κοινή πηγή προβλημάτων. Η χρήση προεπιλεγμένων παραδειγμάτων παραμέτρων που παρέχονται από το Open5GS και το UERANSIM ως σημείο εκκίνησης μπορεί να είναι πολύ χρήσιμη.
- Χρήση εργαλείων καταγραφής και παρακολούθησης: Τόσο το Open5GS όσο και το UERANSIM προσφέρουν αναλυτικές επιλογές καταγραφής. Συνιστάται να εκτελείται το AMF και άλλα βασικά στοιχεία με ενεργοποιημένη την καταγραφή εντοπισμού σφαλμάτων κατά τη ρύθμιση του συστήματος, ώστε να μπορούμε να βλέπουμε μηνύματα όπως "Επιτυχής έλεγχος ταυτότητας UE" ή τυχόν σφάλματα εάν κάτι πάει στραβά. Το Open5GS παρέχει επίσης ένα GUI βασισμένο στο Web για τη διαχείριση συνδρομητών, το οποίο μπορεί να χρησιμοποιηθεί για την εύκολη προσθήκη ή αφαίρεση καταχωρήσεων UE (IMSI, κλειδιά) κατά τη διάρκεια της δοκιμής. Η παρακολούθηση των πόρων του συστήματος και των διεπαφών δικτύου (με εργαλεία όπως το tcpdump ή το Wireshark στις διεπαφές N2/N3) μπορεί να δώσει πληροφορίες για τις ροές μηνυμάτων και να βοηθήσει στην αντιμετώπιση προβλημάτων.
- Συμβατότητα έκδοσης: Όπως σημειώθηκε, προτείνεται η χρήση εγκεκριμένου συνδυασμού εκδόσεων (π.χ. Open5GS v2.4.x με UERANSIM v3.x). Οι κοινότητες για αυτά τα εργαλεία (Λίστες αλληλογραφίας, ζητήματα GitHub) συχνά συζητούν ποιες εκδόσεις συνδυάζονται καλά. Αν αναβαθμιστεί το ένα, αναβαθμίζεται και το άλλο ανάλογα.
- Σταδιακή αύξηση πολυπλοκότητας: Μόλις λειτουργήσει ένα βασικό σενάριο single-UE, single-gNB, δύναται να πραγματοποιηθεί επέκταση του περιβάλλοντος. Για παράδειγμα,

15 *github.com*

προστίθεται ένα δεύτερο UE (το UERANSIM μπορεί να προσομοιώσει πολλαπλούς UE) ή μια δεύτερη διεργασία gNB για την προσομοίωση σενάριων πολλών κυψελών. Είτε πραγματοποιείται η ενσωμάτωση μιας γεννήτριας κίνησης στην πλευρά του UE (όπως η εκτέλεση του προγράμματος-πελάτη iperf3 στην εικονική διεπαφή του UE) για τη δημιουργία κίνησης χρήστη και τη μέτρηση της απόδοσης μέσω του πυρήνα.

Ακολουθώντας αυτές τις οδηγίες, η συνδυασμένη πλατφόρμα Open5GS + UERANSIM μπορεί να παρέχει ένα πλήρως λειτουργικό αυτόνομο περιβάλλον 5G κατάλληλο για πειραματικές, εκπαιδευτικές και ερευνητικές χρήσεις . Η φύση ανοιχτού κώδικα και η δυνατότητα τροποποίησης και των δύο πλατφορμών απελευθερώνουν τους ερευνητές από την εξάρτηση από κλειστά συστήματα, αν και με κόστος τη χειροκίνητη διαμόρφωση και λίγο γράσο αγκώνων. Καθώς τα πρότυπα 5G προχωρούν και οι κοινότητες συμβάλλουν, τόσο το Open5GS όσο και το UERANSIM αναμένεται να εμπλουτιστούν με περισσότερες δυνατότητες, συμβαδίζοντας με τις απαιτήσεις των υψηλής απόδοσης και αξιόπιστων δικτύων κινητής τηλεφωνίας.

4.4. OMNeT/Simu5G για 5G

Οι συνεχώς αυξανόμενες απαιτήσεις για τα δίκτυα 5G απαιτούν προηγμένα και ευέλικτα εργαλεία προσομοίωσης σε επίπεδο συστήματος για να επιτρέψουν σε βάθος ανάλυση και σχεδιασμό νέων πρωτοκόλλων και υπηρεσιών. Το πλαίσιο προσομοίωσης OMNeT++ , σε συνδυασμό με την αποκλειστική βιβλιοθήκη Simu5G , παρέχει μια ισχυρή λύση για την προσομοίωση δικτύων 5G σε επίπεδο συστήματος. Το OMNeT++ είναι ένας προσομοιωτής δικτύου γενικής χρήσης, διακριτών συμβάντων που χρησιμοποιείται ευρέως για ακαδημαϊκούς και ερευνητικούς σκοπούς . Η αρχιτεκτονική του βασίζεται σε αντικειμενοστραφή σχεδιασμό C++, όπου οι οντότητες δικτύου (κόμβοι, σύνδεσμοι, πρωτόκολλα) αναπαρίστανται ως λειτουργικές μονάδες που επικοινωνούν μέσω της μετάδοσης μηνυμάτων. Οι χρήστες μπορούν να επεκτείνουν ή να τροποποιούν τις ενότητες με τρόπο υψηλού επιπέδου, καθιστώντας το OMNeT++ εξαιρετικά επεκτάσιμο και φιλικό προς το χρήστη για προσαρμοσμένα σενάρια δικτύου.16
Ένα από τα δυνατά σημεία του OMNeT++ είναι η υποστήριξή του για πλαίσια επέκτασης (ή «βιβλιοθήκες προσομοίωσης») που προσθέτουν μοντέλα για συγκεκριμένες τεχνολογίες δικτύου. Για παράδειγμα, το πλαίσιο INET παρέχει μοντέλα για δίκτυα TCP/IP και το Veins παρέχει μοντέλα για δίκτυα οχημάτων. Το Simu5G είναι μια βιβλιοθήκη προσομοίωσης ειδικά σχεδιασμένη για να ενσωματώνει μοντέλα 5G New Radio (NR) και βασικά στοιχεία δικτύου πυρήνα 5G στο OMNeT++. Είναι ο διάδοχος της βιβλιοθήκης SimuLTE (η οποία στόχευε το LTE/LTE-Advanced) και πράγματι το Simu5G βασίζεται στην προσέγγιση του SimuLTE για να επιτρέπει την προσομοίωση σεναρίων 5G, πιθανώς σε συνύπαρξη με το 4G (για τη μελέτη της αλληλεπίδρασης) 17 [47].
Το Simu5G επιτρέπει την προσομοίωση του 5G σε επίπεδο συστήματος , που σημαίνει ότι αφαιρεί ορισμένες λεπτομέρειες χαμηλότερου επιπέδου (όπως η ακριβής δημιουργία κυματομορφών) υπέρ της επεκτασιμότητας και της ταχύτητας, ενώ εξακολουθεί να καταγράφει τις βασικές μετρήσεις συμπεριφοράς και απόδοσης που ενδιαφέρουν (παραγωγή, καθυστέρηση, χρήση πόρων κ.λπ.). Παρέχει μια σουίτα νέων κατηγοριών και μοντέλων για την προσομοίωση βασικών πτυχών του 5G NR:

16 https://simu5g.org/users-guide/emulation
17 scitepress.org

- Φυσικό Επίπεδο (PHY): Το Simu5G υποστηρίζει πολλαπλές ζώνες συχνοτήτων και εύρη ζώνης, δυναμική κατανομή φάσματος και μοντελοποίηση παρεμβολών σε υψηλό επίπεδο. Δεν δημιουργεί πραγματικές κυματομορφές, αλλά μπορεί να μοντελοποιήσει φαινόμενα παθολογίας, εξασθένησης και παρεμβολής με απλοποιημένο τρόπο, επιτρέποντας τη μελέτη της κάλυψης και της χωρητικότητας.
- Επίπεδο MAC/Radio Link: Η βιβλιοθήκη περιλαμβάνει μοντέλα για προγραμματισμό MAC 5G, διαχείριση πόρων ραδιοφώνου, χειρισμό πολλαπλών UE και κινητικότητα (συμπεριλαμβανομένων των μεταβιβάσεων). Παρέχει τη δυνατότητα εφαρμογής διαφορετικών αλγορίθμων προγραμματισμού και προσομοίωσης του αντίκτυπου της κινητικότητας στη συνδεσιμότητα.
- Ανώτερα επίπεδα και αλληλεπίδραση πυρήνα: Ενώ το Simu5G δεν υλοποιεί έναν πλήρη πυρήνα 5G, προσφέρει βασικά στοιχεία σηματοδότησης για τη ρύθμιση και την κατάργηση των ροών δεδομένων, ώστε να μπορεί κανείς να προσομοιώσει την επικοινωνία από άκρο σε άκρο στο επίπεδο χρήστη. Ουσιαστικά, μπορεί κανείς να δημιουργήσει φορείς και να μεταδώσει κίνηση από ένα προσομοιωμένο UE σε ένα προσομοιωμένο gNB και σε μια οντότητα διακομιστή, παρατηρώντας την απόδοση κυρίως από την προοπτική RAN.

Τα σενάρια Simu5G διαμορφώνονται μέσω των αρχείων διαμόρφωσης του OMNeT++ (.ini) και των αρχείων ορισμού δικτύου (.ned), τα οποία επιτρέπουν στους χρήστες να ορίζουν την τοπολογία δικτύου (αριθμός UE, gNB, διάταξη), παραμέτρους προσομοίωσης και τα μοτίβα κίνησης που θα δημιουργηθούν. Σε σύγκριση με πλατφόρμες χαμηλότερου επιπέδου, το Simu5G (με OMNeT++) απλοποιεί πολλές πτυχές φυσικών επιπέδων και εστιάζει στην απόδοση μεσαίου έως υψηλότερου επιπέδου, καθιστώντας το κατάλληλο για την αξιολόγηση αλγορίθμων που προϋποθέτουν μια λειτουργική σύνδεση (π.χ. πολιτικές προγραμματισμού, συντονισμός πολλαπλών κυψελών) χωρίς το βαρύ κόστος της προσομοίωσης κάθε δείγματος ραδιοσήματος.

4.4.1. Βασικά Στοιχεία και Αρχιτεκτονική

Το OMNeT++ με το Simu5G βασίζεται στο πρότυπο της μονάδας OMNeT++. Ένα τυπικό σενάριο προσομοίωσης 5G στο Simu5G θα περιλαμβάνει τον καθορισμό μονάδων για UE και gNodeB , και πιθανώς πρόσθετα στοιχεία δικτύου και, στη συνέχεια, προσδιορισμό του τρόπου σύνδεσης (μέσω μονάδων ασύρματου καναλιού που αντιπροσωπεύουν το φάσμα). Τα βασικά βήματα για τη δημιουργία ενός τέτοιου σεναρίου περιλαμβάνουν:18

- Ορισμός κόμβου: Ορίζονται οι μονάδες UE και οι μονάδες gNB σε μια περιγραφή δικτύου. Κάθε UE και gNB είναι μια σύνθετη ενότητα OMNeT++ που περιλαμβάνει υπομονάδες για τα επίπεδα πρωτοκόλλου. Για παράδειγμα, μια λειτουργική μονάδα gNB μπορεί να περιέχει μια υπομονάδα για τον προγραμματιστή MAC, μια για τα buffer RLC κ.λπ., όπως ορίζεται από τη βιβλιοθήκη του Simu5G.
- Διαμόρφωση φάσματος: Ορίζεται η ζώνη συχνοτήτων και το εύρος ζώνης για την προσομοίωση στη διαμόρφωση .ini. Για παράδειγμα, θα μπορούσε κανείς να προσομοιώσει ένα δίκτυο κάτω των 6 GHz (FR1) ή μια ζώνη mmWave προσαρμόζοντας μοντέλα απώλειας διαδρομής και το διαθέσιμο εύρος ζώνης. Το Simu5G μπορεί να προσομοιώσει διαφορές στη διάδοση για αυτές τις ζώνες επιλέγοντας κατάλληλα μοντέλα παθολογίας και κεραίας.

18 https://simu5g.org/users-guide/emulation_openness

- Ρύθμιση παραμέτρων: Επιχειρείται η διαμόρφωση καθολικών παραμέτρων όπως το συνολικό εύρος ζώνης του συστήματος, η ισχύς μετάδοσης του gNB, τα μοντέλα κινητικότητας για UE (τυχαία διαδρομή, προκαθορισμένες διαδρομές, κ.λπ.) και τον αριθμό των κελιών (εάν υπάρχουν πολλά gNB). Ορίζονται επίσης ο αριθμός των UE και οι αρχικές τους θέσεις εάν και όποτε χρειαστεί.
- Μοντέλο κυκλοφορίας: Καθορίζεται η κίνηση που θα δημιουργήσει (ή θα λάβει) κάθε UE. Το Simu5G επιτρέπει τον προσδιορισμό των ροών κυκλοφορίας, για παράδειγμα ροές ανοδικής ή κατερχόμενης ζεύξης ορισμένων τύπων – π.χ. σταθερός ρυθμός μετάδοσης bit, φωνητική κλήση, ροή βίντεο ή δεδομένα βέλτιστης προσπάθειας. Αυτό μπορεί να γίνει είτε χρησιμοποιώντας τις ενσωματωμένες γεννήτριες κίνησης του Simu5G είτε ενσωματώνοντας τα μοντέλα εφαρμογών του πλαισίου INET (όπως μια εφαρμογή TCP που δημιουργεί κίνηση).

Κατά τη διάρκεια της προσομοίωσης, το OMNeT++ επεξεργάζεται διακριτά συμβάντα όπως «Το UE X μετακινείται σε νέα τοποθεσία» ή «Το UE Y μεταδίδει ένα πακέτο» και ενημερώνει ανάλογα την κατάσταση των μονάδων. Οι επεκτάσεις Simu5G διασφαλίζουν ότι συμβάντα όπως ο προγραμματισμός ή η ρύθμιση σύνδεσης RRC διαμορφώνονται σε ευθυγράμμιση με τη λογική 5G. Για παράδειγμα, το Simu5G περιλαμβάνει προηγμένες πολιτικές προγραμματισμού (μπορεί κανείς να δοκιμάσει διαφορετικές μορφές υποδοχής ή σχήματα TDD), διαχείριση πολλών φορέων και χειρίζεται σηματοδότηση 3GPP για σύνδεση και αποσύνδεση UE.

Η αρχιτεκτονική συνδυάζει έτσι τη μηχανή προσομοίωσης OMNeT++ με τη λογική του 5G. Οι προγραμματιστές μπορούν να επιθεωρήσουν ή να τροποποιήσουν οποιοδήποτε μέρος της στοίβας: για παράδειγμα, αλλάζοντας τον τρόπο με τον οποίο ένα gNB αποφασίζει ποιο UE θα προβάλει πρώτο σε ένα δεδομένο TTI ή πώς αποφασίζονται οι κανόνες μεταβίβασης όταν μετακινείται ένας UE.

Ένα σημαντικό χαρακτηριστικό είναι ότι το OMNeT++ παρέχει ένα γραφικό περιβάλλον χρόνου εκτέλεσης , το οποίο σημαίνει ότι μπορεί κανείς να οπτικοποιήσει την τοπολογία του δικτύου και ακόμη και να κινήσει την κίνηση των UE ή τη μετάδοση μηνυμάτων, εάν το επιθυμεί. Αυτό είναι εξαιρετικά χρήσιμο για τον εντοπισμό σφαλμάτων σύνθετων σεναρίων.

4.4.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Η χρήση του OMNeT++ με το Simu5G είναι ιδιαίτερα κατάλληλη για μια ποικιλία ερευνητικών στόχων στο 5G:19

- Διαχείριση πόρων ραδιοφώνου (RRM) και κινητικότητα: Το Simu5G είναι ιδανικό για τη μελέτη αλγορίθμων προγραμματισμού, στρατηγικών κοινής χρήσης φάσματος και διαχείρισης κινητικότητας σε επίπεδο συστήματος. Οι ερευνητές μπορούν να προσομοιώσουν διαφορετικά σχήματα κατανομής πόρων (π.χ. αναλογικό δίκαιο έναντι προγραμματισμού κυκλικής ροής έναντι προγραμματισμού βάσει μηχανικής μάθησης) κάτω από διάφορους φορτίους κίνησης και μοτίβα κινητικότητας και να μετρήσουν την επίδραση στη διεκπεραίωση και τις μετρήσεις QoS. Για την κινητικότητα, η δυνατότητα προσομοίωσης μεταβιβάσεων μεταξύ κυψελών και παρεμβολών από γειτονικές κυψέλες σημαίνει ότι οι αλγόριθμοι μεταβίβασης και οι στρατηγικές ελέγχου ισχύος μπορούν να αξιολογηθούν σε σενάρια με πολλαπλά gNB και κινούμενα UE.

19 https://github.com/Unipisa/Simu5G

- Συνεργασία πολλαπλών κυψελών: Η προσομοίωση σεναρίων πολλαπλών κυψελών στο Simu5G επιτρέπει τη δοκιμή εννοιών όπως ο συντονισμός παρεμβολών μεταξύ κυψελών ή πιο προηγμένες ιδέες όπως το Συντονισμένο Πολυσημείο (CoMP) σε υψηλό επίπεδο. Κάποιος μπορεί να εισαγάγει γειτονικά κελιά και να μοντελοποιήσει τις παρεμβολές που βλέπουν οι UE και στη συνέχεια να εφαρμόσει αλγόριθμους για να την μετριάσει. Επιπλέον, οι αλληλεπιδράσεις με στοιχεία δικτύου υψηλότερου επιπέδου μπορούν να μελετηθούν συνδέοντας το Simu5G με άλλες μονάδες OMNeT++ (για παράδειγμα, προσομοίωση απλού βασικού δικτύου ή καθυστερήσεων δικτύου backhaul). Τα αποτελέσματα μεταβιβάσεων και παρεμβολών μπορούν να αξιολογηθούν ποσοτικά και η ενσωμάτωση με το INET σημαίνει ότι θα μπορούσε κανείς ακόμη και να προσομοιώσει τον τρόπο με τον οποίο η καθυστέρηση του πυρήνα του δικτύου επηρεάζει αυτές τις διαδικασίες RAN.
- Μελέτες ασφάλειας και ανθεκτικότητας: Ενώ το Simu5G δεν εφαρμόζει εγγενώς πρωτόκολλα ασφαλείας, είναι αρκετά ευέλικτο ώστε οι χρήστες να εισάγουν τη δική τους λογική ή άγκιστρα για να προσομοιώνουν επιθέσεις. Για παράδειγμα, θα μπορούσε κανείς να μοντελοποιήσει μια επίθεση άρνησης υπηρεσίας έχοντας ένα UE που ζητά συνεχώς πόρους ή δημιουργώντας πλαστά συμβάντα παρεμβολής και στη συνέχεια να αναλύσει πώς αυτό επηρεάζει την καθυστέρηση ή την αξιοπιστία του δικτύου. Επίσης, επεκτείνοντας τον κώδικα προσομοίωσης, οι ερευνητές μπορούν να προσομοιώσουν ορισμένα είδη αστοχιών ή επιθέσεων (όπως παρεμβολές ή απατεώνες UE) και να μετρήσουν την απόκριση του δικτύου, αν και σε αφηρημένο επίπεδο.
- Μελέτες cross-layer ή end-to-end : Επειδή το OMNeT++ μπορεί να συν-προσομοιώνει διαφορετικά μέρη ενός δικτύου, θα μπορούσε κανείς να χρησιμοποιήσει το Simu5G για την ασύρματη σύνδεση και να το συνδυάσει με μια λειτουργική μονάδα εφαρμογής MEC (Multi-access Edge Computing) για να δει, για παράδειγμα, πώς αποδίδει μια εφαρμογή ανάλυσης βίντεο με διάφορες διαμορφώσεις RAN. Πράγματι, το Simu5G έχει χρησιμοποιηθεί για τη δημιουργία συνόλων δεδομένων για εκπαίδευση τεχνητής νοημοσύνης, προσομοιώνοντας πολλά σενάρια δικτύου και συλλέγοντας δεδομένα απόδοσης.

Οι περιπτώσεις χρήσης του Simu5G περιστρέφονται γύρω από την αξιολόγηση της απόδοσης του 5G σε επίπεδο δικτύου – ιδιαίτερα όπου η λεπτομερής προσομοίωση κυματομορφής δεν είναι απαραίτητη, αλλά απαιτούνται μεγάλα σενάρια ή πολλές εκτελέσεις. Η δύναμή του έγκειται στην παροχή ενός ελεγχόμενου, επαναλαμβανόμενου περιβάλλοντος για την έρευνα 5G RAN που συμπληρώνει εργαλεία χαμηλότερου επιπέδου.

4.4.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Ένα βασικό πλεονέκτημα της προσέγγισης OMNeT++/Simu5G είναι η ανοιχτή φύση της και η μεγάλη κοινότητα χρηστών. Το OMNeT++ υπάρχει εδώ και δεκαετίες και έχει μια ευρεία βάση χρηστών που συνεισφέρουν κώδικα, παραδείγματα και τεκμηρίωση.[48] Η διαθεσιμότητα μιας γραφικής διεπαφής χρήστη βοηθάει πολύ στην κατανόηση και τον εντοπισμό σφαλμάτων. Επιπλέον, η αρθρωτή δομή σημαίνει ότι οι ερευνητές μπορούν να επεκτείνουν τον προσομοιωτή για νέα σενάρια (για παράδειγμα, προσθέτοντας ένα μοντέλο για έναν νέο τύπο κόμβου 5G ή ενσωμάτωση με εξωτερικά σενάρια). Ο συνδυασμός εκτέλεσης πραγματικού κώδικα (για υψηλότερα επίπεδα) με αφηρημένο φυσικό επίπεδο αποδίδει ταχύτερους χρόνους

προσομοίωσης και τη δυνατότητα προσομοίωσης δικτύων με πολλούς κόμβους ή για μεγάλες προσομοιωμένες διάρκειες, κάτι που μπορεί να είναι ανέφικτο σε πιο λεπτομερείς προσομοιωτές. Το Simu5G αξιοποιεί τις δυνατότητες συλλογής και ανάλυσης αποτελεσμάτων του OMNeT++ , παρέχοντας ενσωματωμένη υποστήριξη για την καταγραφή μετρήσεων και τη στατιστική ανάλυσή τους σε όλες τις εκτελέσεις. Αυτό διευκολύνει την εκτέλεση αυστηρών αξιολογήσεων απόδοσης με πολλαπλούς σπόρους ή σαρώσεις παραμέτρων.
Προκλήσεις: Ωστόσο, καθώς το Simu5G είναι προσομοιωτής σε επίπεδο συστήματος, ενδέχεται να μην καταγράφει φαινόμενα που απαιτούν λεπτομερή μοντελοποίηση χαμηλότερου επιπέδου. Για παράδειγμα, περιπτώσεις χρήσης εξαιρετικά χαμηλού λανθάνοντος χρόνου (URLLC) που εξαρτώνται από τον ακριβή χρονισμό ή την αξιοπιστία του φυσικού επιπέδου ενδέχεται να είναι δύσκολο να αξιολογηθούν με ακρίβεια χωρίς ένα πιο λεπτομερές μοντέλο PHY. Εάν μια μελέτη απαιτεί κατανόηση των ιδιορρυθμιών διαμόρφωσης δέσμης MIMO ή διάδοσης κυμάτων χιλιοστών, τα απλούστερα μοντέλα του Simu5G ενδέχεται να μην αρκούν (τέτοιες πτυχές μπορεί να χρειάζονται είτε βελτιώσεις στο Simu5G είτε εντελώς διαφορετικό προσομοιωτή). Επιπλέον, δεν έχουν εφαρμοστεί ακόμη όλες οι δυνατότητες 5G στην προδιαγραφή 3GPP. Δυνατότητες όπως ο διαχωρισμός δικτύου ή συγκεκριμένες διαδικασίες διαχείρισης δέσμης mmWave ενδέχεται να απαιτούν από τον χρήστη να εφαρμόσει πρόσθετη λογική πάνω από το Simu5G, εάν χρειάζεται . Υπάρχει επίσης το θέμα της επικύρωσης: ενώ τα μοντέλα του Simu5G είναι κατασκευασμένα για να συνάδουν με το 3GPP όπου είναι δυνατόν και έχουν επικυρωθεί εν μέρει έναντι γνωστών αποτελεσμάτων 20 [47], η αφαίρεση σημαίνει ότι οι ερευνητές πρέπει να είναι προσεκτικοί στην ερμηνεία των αποτελεσμάτων και πιθανώς να διασταυρώνονται με πιο λεπτομερή εργαλεία για κρίσιμα συμπεράσματα.
Όσον αφορά την επεκτασιμότητα, οι προσομοιώσεις OMNeT++ μπορεί να είναι ακόμα βαριές εάν χρησιμοποιούνται πολύ μεγάλα δίκτυα – η εκτέλεση εκατοντάδων κόμβων με πολύπλοκες αλληλεπιδράσεις μπορεί να επιβραδυνθεί, αν και το OMNeT++ είναι γενικά αποτελεσματικό στο χειρισμό πολλών συμβάντων. Τέλος, οι χρήστες χρειάζονται εξοικείωση με τις συμβάσεις OMNeT++ (γλώσσα NED, αρχεία ini), κάτι που αποτελεί πρόσθετο κόστος εκμάθησης εάν δεν έχουν χρησιμοποιήσει το πλαίσιο στο παρελθόν.
Παρά αυτές τις σκέψεις, για μια μεγάλη κατηγορία ερευνητικών ερωτήσεων 5G, το Simu5G φτάνει σε ένα «γλυκό σημείο» παρέχοντας αρκετή λεπτομέρεια για να καταγράψει τη βασική δυναμική, ενώ παραμένει αρκετά αφηρημένο ώστε να επιτρέπει την κλιμάκωση και τον γρήγορο πειραματισμό. Έχει γίνει ένα πολύτιμο εργαλείο στο οπλοστάσιο για τους ερευνητές του δικτύου 5G, ειδικά όταν συνδυάζεται με αναλυτικές μελέτες ή προσομοιώσεις χαμηλότερου επιπέδου για μια ολοκληρωμένη ανάλυση.

4.4.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την βέλτιστη αξιοποίηση του OMNeT++ και Simu5G στις προσομοιώσεις 5G, συνιστώνται οι ακόλουθες πρακτικές:21[49]

- Συνεχείς Ενημερώσεις: Χρησιμοποιούνται οι πρόσφατες εκδόσεις του OMNeT++ και του Simu5G για την αξιοποίηση των όλο και πιο πρόσφατων δυνατοτήτων και διορθώσεις

20 scitepress.org
21 https://www.researchgate.net/publication/342381159_Using_Simu5G_as_a_Realtime_Network_Emulator_to_Test_MEC_Apps_in_an_End-To-End_5G_Testbed

σφαλμάτων. Και τα δύο είναι ενεργά έργα (το Simu5G είχε την αρχική του κυκλοφορία γύρω στο 2020 και ενημερώνεται καθώς προχωρά η έρευνα 5G). Γίνεται περιοδικός έλεγχος στην τεκμηρίωση του Simu5G ή στη λίστα αλληλογραφίας χρήστη για τυχόν ενημερώσεις κώδικα, ειδικότερα σε περιπτώσεις που είναι αναγκαία η προσομοίωση νέων λειτουργιών έκδοσης 3GPP.

- Μόχλευση Παραδείγματα Κοινότητας: Αξιοποιούνται τα παραδείγματα σεναρίων που παρέχονται από το Simu5G (και το SimuLTE, καθώς το Simu5G είναι συμβατό με αυτό). Αυτές περιλαμβάνουν μελέτες περιπτώσεων και διαμορφώσεις αναφοράς που απεικονίζουν τυπικές ρυθμίσεις. Για παράδειγμα, ένα σενάριο μπορεί να δείχνει ένα απλό κελί με μερικούς UE που κατεβάζουν κίνηση – μπορεί να χρησιμοποιηθεί ως πρότυπο για τη δημιουργία πιο σύνθετων σεναριών σταδιακά.
- Σχεδίαση Τοπολογίας: Αξιοποιείται η υποστήριξη του OMNeT++ για παραμετρικές τοπολογίες . Για παράδειγμα, θα μπορούσε να γράφτεί ένας απλός βρόχος στο αρχείο ini για να δημιουργηθεί ένας αριθμός από UE χωρίς να το γίνει με μη αυτόματο τρόπο. Αυτό κάνει τα πειράματα κλιμακούμενα και επαναλαμβανόμενα. Γίνεται ονομαστικός διαχωρισμός των κόμβων συστηματικά (π.χ. gNB1, UE1, UE2, κ.λπ.) και χρησιμοποιείται η ονομασία στα σενάρια ανάλυσής, εάν χρειαστεί για λόγους σαφήνειας.
- Καταγραφή και εντοπισμός σφαλμάτων: Το OMNeT++ επιτρέπει την καταγραφή ανά μονάδα. Ενεργοποιείται η καταγραφή για κρίσιμες λειτουργικές μονάδες (όπως ο χρονοπρογραμματιστής ή το RRC) εάν χρειάζεται να εντοπιστούν σφάλματα σε μη αναμενόμενη συμπεριφορά. Το ίχνος συμβάντος μπορεί να επιθεωρηθεί ώστε, για παράδειγμα, να αποτυπωθεί το πώς κατανέμονται οι χρονοθυρίδες με την πάροδο του χρόνου.
- Ενοποίηση με Εργαλεία Ανάλυσης: Τα διανύσματα εξόδου και οι βαθμωτές βαθμίδες από το OMNeT++ (μέσω του συστήματος καταγραφής αποτελεσμάτων) μπορούν να εξαχθούν σε CSV ή να αποτυπωθούν απευθείας. Θα ήταν επίσης δυνατό να χρησιμοποιηθεί το IDE του OMNeT++ για τον σχεδισμο αποτελεσμάτων ή την αξιοποίηση εξωτερικών εργαλείων (Python/pandas, MATLAB) για την επεξεργασία μεγάλων παρτίδων δεδομένων. Βεβαιώνεται πως έχει οριστεί η απαιτούμενη καταγραφή αποτελεσμάτων στο ini (το Simu5G πιθανότατα περιλαμβάνει προεπιλεγμένες μετρήσεις όπως απόδοση κυψέλης, απόδοση ανά UE, καθυστερήσεις πακέτων κ.λπ.). Βεβαιώνεται η καταγρφή με μια σύντομη δοκιμαστική λειτουργία.

Ακολουθώντας αυτές τις οδηγίες, το OMNeT++/Simu5G παρέχει μία από τις πιο ολοκληρωμένες αλλά ευέλικτες ανοιχτές πλατφόρμες για προσομοίωση δικτύου 5G . Χάρη στην αρχιτεκτονική και την επεκτασιμότητα του, διευκολύνει την έρευνα σχετικά με την απόδοση, την κινητικότητα, την κατανομή πόρων, ακόμη και βασικές πτυχές ασφάλειας σε ασύρματα δίκτυα επόμενης γενιάς. Αν και δεν αντικαθιστά τη λεπτομερή προσομοίωση σε επίπεδο συνδέσμου ή τις δοκιμές πραγματικού κόσμου, μειώνει σημαντικά το εμπόδιο εισόδου για την εξερεύνηση νέων ιδεών και την κλιμάκωσή τους σε ένα εικονικό περιβάλλον, κάτι που είναι απαραίτητο τόσο σε ακαδημαϊκά όσο και σε ερευνητικά έργα της βιομηχανίας που εστιάζουν στο 5G και πέρα.

4.5. TRex

Οι ραγδαίες εξελίξεις στην τεχνολογία δικτύου – ειδικά σε περιβάλλοντα υψηλής ταχύτητας δεδομένων, όπως τα δίκτυα 5G – δημιουργούν την ανάγκη για εξειδικευμένα εργαλεία ικανά να

παράγουν ρεαλιστική, υψηλής πυκνότητας κίνηση. Το TRex είναι μια γεννήτρια κίνησης ανοιχτού κώδικα που αναπτύχθηκε από τη Cisco, σχεδιασμένη για να παρέχει δυνατότητες παραγωγής και ανάλυσης πακέτων υψηλής απόδοσης. Με την υποστήριξη πολλαπλών πρωτοκόλλων και τη δυνατότητα κλιμάκωσης σε ρυθμούς πολλαπλών Gigabit, το TRex έχει γίνει μια δημοφιλής λύση σε ερευνητικά εργαστήρια και περιβάλλοντα δοκιμών απόδοσης.22

Το TRex είναι βασικά μια γεννήτρια και αναλυτής πακέτων που λειτουργεί στα επίπεδα 2-7 του μοντέλου OSI. Σε αντίθεση με τα απλά εργαλεία επανάληψης πακέτων (π.χ. Tcpreplay) που στέλνουν πακέτα από ένα ίχνος, το TRex κατασκευάστηκε για να χρησιμοποιεί πλήρως τις σύγχρονες πολυπύρηνες CPU και NIC για την επίτευξη ακραίων ρυθμών πακέτων. Λειτουργεί τόσο σε κατάσταση κατάστασης όσο και σε κατάσταση κατάστασης : σε κατάσταση χωρίς κατάσταση, μπορεί να στείλει πακέτα σύμφωνα με προκαθορισμένες ροές χωρίς να διατηρεί καμία κατάσταση ροής, ενώ σε κατάσταση κατάστασης, μπορεί να προσομοιώσει ρεαλιστικές συνδέσεις TCP/UDP με σωστή σημασιολογία συνεδρίας. Αυτό επιτρέπει στο TRex να μιμείται πραγματικά μοτίβα κυκλοφορίας εφαρμογών (όπως η προσομοίωση πολλών ταυτόχρονων ροών TCP, με χειραψίες και επιβεβαιώσεις, εάν χρειάζεται) με ελεγχόμενο τρόπο.

Κάτω από την κουκούλα, το TRex τροφοδοτείται από τη βιβλιοθήκη DPDK (Data Plane Development Kit), η οποία επιτρέπει στα προγράμματα χώρου χρήστη να στέλνουν και να λαμβάνουν πακέτα με υψηλή ταχύτητα, παρακάμπτοντας τη στοίβα δικτύου πυρήνα. Με την άμεση αλληλεπίδραση με τις ουρές υλικού NIC, το TRex μειώνει σημαντικά την επιβάρυνση ανά πακέτο, επιτρέποντάς του να φτάσει σε πολύ υψηλή απόδοση και χαμηλή καθυστέρηση στη δημιουργία κίνησης. Στην πραγματικότητα, το TRex μπορεί να κλιμακωθεί σε 100 Gbps+ κίνησης σε κατάλληλο υλικό και έχει αποδειχθεί ότι φτάνει της τάξης των 200 Gbps με έναν μόνο διακομιστή υψηλής τεχνολογίας και NIC[50]. Μετατρέπει έναν διακομιστή γενικής χρήσης σε ισχυρό packet blaster, εξαλείφοντας την ανάγκη για ακριβές ιδιόκτητες συσκευές γεννήτριας κυκλοφορίας για πολλά σενάρια δοκιμών.

Ο σχεδιασμός του TRex χωρίζεται σε δύο βασικά στοιχεία:23

- TRex Daemon (Server-Side): Αυτός είναι ο βασικός κινητήρας που λειτουργεί σε ένα σύστημα με κατάλληλα NIC (ιδανικά NIC συμβατά με DPDK 10GbE, 25GbE, 40GbE ή 100GbE). Είναι υπεύθυνο για τη δημιουργία και την επεξεργασία πακέτων με ρυθμό γραμμής, χρησιμοποιώντας πολλαπλούς πυρήνες CPU για παράλληλη επεξεργασία πακέτων. Ο δαίμονας χειρίζεται βελτιστοποίηση χαμηλού επιπέδου (buffers μνήμης, αποστολή βρόχων, συλλογή στατιστικών στοιχείων) και εκθέτει ένα API για έλεγχο.
- Control API (Client-Side): Το TRex παρέχει τόσο ένα διαδραστικό CLI όσο και ένα Python API για τον απομακρυσμένο έλεγχο του δαίμονα. Μέσω αυτού του API, οι χρήστες ορίζουν προφίλ κίνησης – σύνολα ροών με καθορισμένα περιεχόμενα πακέτων, ρυθμούς (πακέτα ανά δευτερόλεπτο ή ρυθμό μετάδοσης bit) και διανομές. Το επίπεδο ελέγχου ανακτά επίσης στατιστικά στοιχεία από τον δαίμονα, όπως μετρήσεις μεταδιδόμενων πακέτων, πτώσεις και καθυστερήσεις (όταν είναι ενεργοποιημένη η μέτρηση λανθάνοντος χρόνου).

Οι βασικές λειτουργίες που υποστηρίζονται από το TRex περιλαμβάνουν:

- Δημιουργία κυκλοφορίας χωρίς πολιτεία και κατάσταση: Στη λειτουργία χωρίς πολιτεία, το TRex μπορεί να στείλει πακέτα σε βρόχο σύμφωνα με προκατασκευασμένα μοτίβα,

22 https://trex-tgn.cisco.com/

23 https://trex-tgn.cisco.com/

κατάλληλα για τη δοκιμή της απόδοσης ή την απόδοση προώθησης πακέτων χωρίς παρακολούθηση σύνδεσης. Σε κατάσταση κατάστασης, το TRex μπορεί να δημιουργήσει πολλές ψευδο-συνδέσεις (π.χ. να προσομοιώσει χιλιάδες ροές TCP με μοναδικές διευθύνσεις 5 πλειάδων) και ακόμη και να ανταποκριθεί σε εισερχόμενα πακέτα, κάτι που είναι χρήσιμο για τη δοκιμή συσκευών κατάστασης όπως τα τείχη προστασίας. Αυτή η δυνατότητα κατάστασης επιτρέπει ρεαλιστικές δοκιμές σε επίπεδο εφαρμογής (Επίπεδο 4-7).

- Δημιουργία πακέτων: Οι χρήστες μπορούν να δημιουργήσουν πακέτα με προσαρμοσμένες κεφαλίδες (Ethernet, ετικέτες VLAN, IP, TCP/UDP, κ.λπ.) και ωφέλιμα φορτία. Τα αρχεία διαμόρφωσης Python API ή YAML του TRex σάς επιτρέπουν να προσδιορίζετε πεδία και ακόμη και εύρη για πεδία προς σάρωση (για παράδειγμα, οι διευθύνσεις IP προέλευσης μπορούν να επαναληφθούν για την προσομοίωση πολλών κεντρικών υπολογιστών). Αυτό είναι κρίσιμο για τη δοκιμή σεναρίων όπως κατακερματισμός IP, διαφορετικές σημάνσεις QoS ή μίμηση κίνησης από πολλές διαφορετικές IP.
- Κλιμάκωση και απόδοση: Με τις κατάλληλες ρυθμίσεις NIC και CPU, το TRex μπορεί να κλιμακωθεί σε εκατομμύρια πακέτα ανά δευτερόλεπτο. Υποστηρίζει multi-threading και μπορεί να χρησιμοποιήσουμε πολλές θύρες NIC ταυτόχρονα για αμφίδρομη κίνηση ή κίνηση σε πολλαπλούς συνδέσμους. Αυτό το καθιστά κατάλληλο για δρομολογητές υψηλής τεχνολογίας, διακόπτες ή βασικά εξαρτήματα 5G που πρέπει να χειρίζονται τεράστια φορτία.

Συνολικά, το TRex χρησιμεύει ως παραγωγός κίνησης υψηλής απόδοσης και ελεγκτής φόρτου δικτύου , επιτρέποντας την αξιολόγηση της απόδοσης της συσκευής δικτύου υπό ρεαλιστικές συνθήκες κυκλοφορίας, συμπεριλαμβανομένων των δικτύων 5G όπου ο όγκος κίνησης είναι μεγάλος και τα μοτίβα κυκλοφορίας μπορεί να είναι περίπλοκα.

4.5.1. Βασικά Στοιχεία και Αρχιτεκτονική

Η αρχιτεκτονική του TRex μπορεί να χωριστεί εννοιολογικά σε δύο επίπεδα, όπως αναφέρθηκε:24

- Μηχανή πακέτων χαμηλού επιπέδου (TRex daemon): Εκτελείται στο μηχάνημα δημιουργίας κίνησης και συνδέεται απευθείας με το υλικό NIC. Παίρνει προεπεξεργασμένα πρότυπα κυκλοφορίας και στέλνει πακέτα, χειρίζεται εργασίες όπως διαχείριση buffer μνήμης, προγραμματισμό πακέτων σε πυρήνες και χρονική σήμανση για στατιστικά λανθάνουσας κατάστασης. Βελτιστοποιεί την απόδοση καρφιτσώνοντας νήματα στους πυρήνες της CPU και χρησιμοποιώντας τεχνικές όπως η μαζική επεξεργασία πακέτων. Χρησιμοποιώντας πολλαπλούς πυρήνες, το TRex μπορεί να επιτύχει πολύ υψηλή απόδοση (π.χ. διαιρώντας το φόρτο εργασίας των 100 Gbps σε, ας πούμε, 8 πυρήνες).
- Επίπεδο ελέγχου χρήστη: Μέσω του Python API ή του CLI, ο χρήστης ελέγχει τη δοκιμή: ορίζοντας ροές, έναρξη/διακοπή της κυκλοφορίας και ανάγνωση στατιστικών. Σε αυτό το επίπεδο, κάποιος διαμορφώνει πράγματα όπως το περιεχόμενο πακέτων, τους ρυθμούς ροής και εάν θα μετρηθεί ο λανθάνουσα κατάσταση σε συγκεκριμένες ροές. Το CLI μπορεί να φορτώσει αρχεία PCAP ως πρότυπα ή να χρησιμοποιήσει ενσωματωμένη διαμόρφωση ροής.

24 https://trex-tgn.cisco.com/

Συγκεκριμένα, μια ρύθμιση δημιουργίας κυκλοφορίας TRex μπορεί να μοιάζει με την ακόλουθη: Προφίλ κίνησης: Ένας χρήστης ορίζει ένα ή περισσότερα προφίλ που αποτελούνται από ροές. Κάθε ροή έχει ένα πρότυπο πακέτου (το οποίο θα μπορούσε να είναι ένα σταθερό πακέτο ή ένας συνδυασμός επιπέδων με μεταβλητά πεδία), έναν ρυθμό (π.χ. 1000 πακέτα ανά δευτερόλεπτο ή ένα ποσοστό του ρυθμού γραμμής) και έναν τρόπο λειτουργίας (συνεχές, ριπή πακέτων X κ.λπ.). Το TRex μπορεί να ενισχύσει μια ροή εν κινήσει – π.χ. εάν έχετε ένα πρότυπο για ανταλλαγή πελάτη-διακομιστή, το TRex μπορεί να δημιουργήσει χιλιάδες τέτοιες ανταλλαγές με διαφορετικές διευθύνσεις.
Συλλογή στατιστικών: Το TRex παρέχει λεπτομερή στατιστικά στοιχεία, όπως μετρητές ανά θύρα, συνολική απόδοση, απώλειες πακέτων και κατανομή της λανθάνουσας κατάστασης (όταν χρησιμοποιούνται ροές κατάστασης με ενεργοποιημένη μέτρηση καθυστέρησης μέσω echo packets). Αυτά τα στατιστικά είναι ζωτικής σημασίας για την κατανόηση της συμπεριφοράς της συσκευής υπό δοκιμή (DUT) υπό συνθήκες φόρτου, όπως το αν ρίχνει πακέτα μετά από ένα συγκεκριμένο επίπεδο απόδοσης ή πώς εξελίσσεται η καθυστέρηση με την αύξηση του φορτίου.
Αρχιτεκτονικά, το TRex χρησιμοποιεί το DPDK για να συνδέσει NIC στο χώρο χρήστη. Τα NIC πρέπει να υποστηρίζονται από το DPDK (τα κοινά είναι τα Intel ixgbe, i40e για 10/40G και νεότερα). Αυτό σημαίνει ότι όταν εκτελείται το TRex, το NIC αναλαμβάνεται από το TRex και ο πυρήνας δεν το βλέπει ως κανονική διεπαφή. Το πλεονέκτημα είναι η παράκαμψη του πυρήνα που βελτιώνει δραματικά την απόδοση[50].
Συνοπτικά, η αρχιτεκτονική του TRex είναι προσανατολισμένη σε έναν στόχο: δημιουργία κίνησης σε κλίμακα με ακρίβεια . Εκφορτώνει όσο το δυνατόν περισσότερο στα νήματα επεξεργασίας πακέτων και ελαχιστοποιεί την αλληλεπίδραση με το λειτουργικό σύστημα μόλις εκτελεστεί. Όλη η βαριά ανύψωση γίνεται σε βελτιστοποιημένη C++ εντός του δαίμονα, ενορχηστρωμένη από τον χρήστη μέσω εντολών ή σεναρίων υψηλού επιπέδου.

4.5.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Το TRex είναι κεντρικό σε πολλά σενάρια εργαστηριακών δοκιμών και συγκριτικής αξιολόγησης, συμπεριλαμβανομένων των κλινών δοκιμών 5G και της επικύρωσης υποδομής δικτύου:25

- Δοκιμή απόδοσης συσκευών δικτύου: Οι εταιρείες τηλεπικοινωνιών και οι πάροχοι cloud χρησιμοποιούν το TRex για να δοκιμάζουν δρομολογητές, διακόπτες και τείχη προστασίας δημιουργώντας έντονο φόρτο κυκλοφορίας. Για παράδειγμα, για να επαληθεύσουν ότι μια νέα 5G UPF (Λειτουργία Επιπέδου Χρήστη) μπορεί να χειριστεί τη διεκπεραίωση στόχου, οι δοκιμαστές μπορεί να χρησιμοποιήσουν το TRex για να προσομοιώσουν χιλιάδες UE που στέλνουν κίνηση μέσω του UPF, μετρώντας σε ποιο σημείο (αν υπάρχει) συμβαίνουν οροπέδια διεκπεραίωσης ή απώλεια πακέτων. Η ικανότητα παραγωγής τόσο ροών TCP όσο και UDP βοηθά στη δοκιμή των χειρότερων σεναρίων για απόδοση και διασφαλίζει ότι οι συσκευές μπορούν να ικανοποιήσουν τις απαιτήσεις SLA υπό βαρύ φορτίο.
- Αξιολόγηση ασφάλειας: Σε συνδυασμό με εργαλεία που δημιουργούν κακόβουλη κίνηση (όπως το Metasploit για εκμεταλλεύσεις ή προσαρμοσμένα σενάρια για μοτίβα DDoS), το TRex μπορεί να λειτουργήσει ως η βασική πλατφόρμα για δοκιμές DDoS ή πλημμυρικών επιθέσεων. Για παράδειγμα, μια δοκιμή θα μπορούσε να περιλαμβάνει το TRex που δημιουργεί ένα μείγμα κανονικής κίνησης χρηστών και επιθέσεων (όπως πλημμύρες SYN ή ογκομετρικές πλημμύρες UDP) για να δει πώς αντιμετωπίζει ένα σύστημα ανίχνευσης

25 https://developer.cisco.com/docs/app-hosting/deploy-trex-traffic-generator-application/

εισβολής (IDS) ή ένας μηχανισμός απομόνωσης τμημάτων δικτύου 5G. Στα δίκτυα 5G, τα οποία αναμένεται να χειριστούν τεράστιες ταχύτητες δεδομένων, τέτοιες δοκιμές αποκαλύπτουν την ανθεκτικότητα του τεμαχισμού και του βασικού δικτύου υπό ακραίες συνθήκες.

- Μελέτες QoS/QoE: Επειδή το TRex μπορεί να αναδημιουργήσει συγκεκριμένα μοτίβα κίνησης εφαρμογών (όπως η εξομοίωση ροής βίντεο ή κλήσεων VoIP αναπαράγοντας τα χαρακτηριστικά πακέτων τους σε κατάσταση κατάστασης), οι ερευνητές μπορούν να μελετήσουν τις επιπτώσεις της Ποιότητας Υπηρεσίας (QoS) και της Ποιότητας Εμπειρίας (QoE) . Για παράδειγμα, μπορεί κανείς να στείλει μια ροή βίντεο με κατάσταση κατάστασης και να μετρήσει το jitter και την απώλεια πακέτων για να αξιολογήσει πώς μια διαμόρφωση δικτύου επηρεάζει την ποιότητα ροής. Η κατάσταση κατάστασης του TRex με ρεαλιστικές ροές είναι το κλειδί για αυτό. Επιπλέον, ο συνδυασμός TRex με εργαλεία ανάλυσης (όπως το Wireshark ή το Zeek) επιτρέπει τη βαθιά επιθεώρηση του τρόπου με τον οποίο ορισμένες συνθήκες δικτύου υποβαθμίζουν την εμπειρία του χρήστη, κάτι που είναι πολύτιμο για τον συντονισμό των αλγορίθμων διαχείρισης κυκλοφορίας 5G.

Στο πλαίσιο του 5G, το TRex χρησιμοποιείται συχνά σε εργαστηριακές κλίνες δοκιμών που μιμούνται τμήματα του πυρήνα 5G ή του RAN για την επικύρωση της απόδοσης. Για παράδειγμα, μια ομάδα μπορεί να αναπτύξει ένα UPF και να χρησιμοποιήσει το TRex για να προσομοιώσει την κίνηση gNB προς το UPF και από το UPF προς το δίκτυο δεδομένων, για να διασφαλίσει ότι το UPF μπορεί να χειριστεί τον στοχευόμενο αριθμό Gbps και περιόδους σύνδεσης. Το TRex μπορεί επίσης να βοηθήσει στη δημιουργία κίνησης στο παρασκήνιο για πειράματα – π.χ., στην περίπτωση χρήσης ενός αλγόριθμου σε ns-3 ή OMNeT++ υπό μεγάλο φορτίο, το TRex θα μπορούσε να ενσωματωθεί στο υλικό στον βρόχο ή να δημιουργηθούν ίχνη από το TRex με σκοπό την τροφοδότηση προσομοιώσεων.

4.5.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Ένα βασικό πλεονέκτημα του TRex είναι η αποτελεσματική του ενσωμάτωση με το DPDK , το οποίο επιτρέπει την άμεση επεξεργασία πακέτων στο χώρο του χρήστη και μεγιστοποιεί τη διεκπεραίωση NIC. Αυτή η αποτελεσματικότητα σημαίνει ότι το TRex μπορεί να ωθήσει την κυκλοφορία στα όρια του υλικού, κάτι που είναι απαραίτητο κατά τη δοκιμή στοιχείων δικτύου 5G που έχουν σχεδιαστεί για δεκάδες ή εκατοντάδες gigabit. Το TRex ως ανοιχτού κώδικα σημαίνει ότι οι ερευνητές και οι επαγγελματίες μπορούν να το χρησιμοποιήσουν χωρίς κόστος αδειοδότησης και μπορούν να το τροποποιήσουν εάν χρειάζεται για προσαρμοσμένα σενάρια δοκιμών. Η ενεργή κοινότητα και η πλήρης τεκμηρίωση (συμπεριλαμβανομένου ενός εκτενούς εγχειριδίου και αναφορών API) το καθιστούν σχετικά προσιτό λόγω της πολυπλοκότητάς του. Η ευελιξία του TRex – που υποστηρίζει τόσο την ανατίναξη χωρίς κατάσταση όσο και την προσομοίωση ροής σε κατάσταση κατάστασης – καλύπτει ένα ευρύ φάσμα αναγκών δοκιμών. Είναι εξίσου στο σπίτι δοκιμή μιας καθαρής μηχανής προώθησης πακέτων ή ενός πολύπλοκου τείχους προστασίας κατάστασης, κάτι που είναι ασυνήθιστο για ένα μόνο εργαλείο.
Προκλήσεις: Για την επίτευξη μιας προσεγγιστικά μέγιστης απόδοσης, το TRex εξαρτάται σε μεγάλο βαθμό από τη σωστή διαμόρφωση υλικού. Απαιτεί CPU προηγμένης τεχνολογίας (πολλαπλούς πυρήνες, πιθανώς συντονισμένους για NUMA εάν χρησιμοποιούνται συστήματα πολλαπλών υποδοχών) και NIC που υποστηρίζουν προγράμματα οδήγησης DPDK, καθώς και διαμόρφωση του συστήματος (μεγάλη μνήμη, απομόνωση CPU) για χρήση TRex. Ανεπαρκές

υλικό (π.χ. χρήση TRex σε τυπικό φορητό υπολογιστή Ethernet) δεν θα δείξει τα δυνατά του σημεία και μπορεί να οδηγήσει σε παραπλανητικά αποτελέσματα. Υπάρχει μια καμπύλη μάθησης στην κατανόηση του τρόπου δημιουργίας προφίλ κίνησης, ειδικά για κρατική κυκλοφορία, η οποία περιλαμβάνει εξοικείωση με τις περιπλοκές TCP/IP και ίσως τη σύνταξη σεναρίων Python για πολύπλοκα σενάρια. Όταν συνδυάζονται πολλαπλά πρωτόκολλα ή ειδικές συνθήκες δοκιμής, οι χρήστες πρέπει να επικυρώνουν προσεκτικά ότι το TRex δημιουργεί ακριβώς αυτό που σκοπεύουν. Επιπλέον, η ανάλυση των αποτελεσμάτων από το TRex απαιτεί εξωτερικά εργαλεία ή προσεκτική ανάλυση της εξόδου του. Ενώ παρέχει ακατέργαστα στατιστικά στοιχεία, η κατανόηση των σημείων συμφόρησης μπορεί να χρειαστεί συσχέτιση δεδομένων TRex με αρχεία καταγραφής συσκευών ή συλλήψεις πακέτων.
Συνοπτικά, ο κύριος περιορισμός του TRex είναι ότι η ισχύς του περιορίζεται από την ικανότητα του χρήστη να του παρέχει επαρκές υλικό και σωστές διαμορφώσεις. Για ερευνητές που δεν ειδικεύονται στην απόδοση δικτύου, η εγκατάσταση του TRex για πρώτη φορά μπορεί να είναι χρονοβόρα. Ωστόσο, μόλις εκτελεστεί, είναι ένα απαραίτητο εργαλείο για την ώθηση των συστημάτων δικτύου στα όριά τους και τη λήψη επαναλαμβανόμενων, ελεγχόμενων αποτελεσμάτων δοκιμών φορτίου.

4.5.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την αποτελεσματικότερη αξιοποίηση του TRex για τη δημιουργία κίνησης και τη δοκιμή απόδοσης δικτύου, προτείνονται οι ακόλουθες βέλτιστες πρακτικές:26

- Προετοιμασία υλικού: Χρησιμοποιείται ένα αποκλειστικό μηχάνημα με υλικό CPU και NIC που είναι γνωστό ότι λειτουργεί καλά με το DPDK. Ενεργοποιούνται **οι** τεράστιες σελίδες στο λειτουργικό σύστημα (το DPDK απαιτεί μεγάλες σελίδες μνήμης για αποτελεσματικότητα DMA) και πραγματοποιείται σύνδεση θύρων NIC σε προγράμματα οδήγησης DPDK (η τεκμηρίωση TRex παρέχει μια δέσμη ενεργειών dpdk_setup_ports.py για να βοηθήσει με αυτό). Βεβαιώνεται ότι το υλικολογισμικό NIC είναι ενημερωμένο και ότι δυνατότητες όπως το RSS (Receive Side Scaling) έχουν διαμορφωθεί σωστά, εάν χρειάζεται.
- Αρχική Λειτουργική Δοκιμή: Εκκινείται ένα απλό τεστ κυκλοφορίας ανιθαγενών με σκοπό την επαλήθευση ορθής λειουργίας του TRex. Για παράδειγμα, θα μπορούσε να διαμορφωθεί μια ενιαία ροή πακέτων (π.χ. πακέτα UDP 64 byte) και να αποσταλλούν με μέτρια ταχύτητα σε έναν δέκτη βρόχου ή δοκιμής. Ελέγχεται ότι το TRex αναφέρει την αναμενόμενη απόδοση και ότι η πλευρά λήψης βλέπει τα πακέτα. Αυτή η βασική δοκιμή επικυρώνει το περιβάλλον.
- Αυξητική πολυπλοκότητα: Για δοκιμές κατάστασης, χρησιμοποιούνται τα παρεχόμενα δείγματα προφίλ της TRex (υπάρχουν προκατασκευασμένα προφίλ για προσομοίωση πραγμάτων όπως η κίνηση HTTP κ.λπ.). Σταδιακά προστίθεται πολυπλοκότητα – π.χ., αυξάνεται ο αριθμός των ροών ή προστίθεται αμφίδρομη κίνηση – και παρακολουθείται η χρήση των πόρων. Το TRex παρέχει στατιστικά στοιχεία χρήσης CPU για τους πυρήνες του. Εάν αυτά μεγιστοποιούνται, εξετάζεται το ενδεχόμενο να αυξηθεί ο αριθμός των πυρήνων που έχουν εκχωρηθεί ή να μειωθεί το φορτίο ανά πυρήνα.
- Στατιστικά παρακολούθησης: Χρησιμοποιείται η κονσόλα TRex ή το GUI (εάν υπάρχει) για την παρακολούθηση ζωντανών στατιστικών, αλλά για τελική ανάλυση, αξιοποιούνται

26 https://developer.cisco.com/docs/app-hosting/deploy-trex-traffic-generator-application/

οι έξοδοι JSON ή CSV που μπορεί να δημιουργήσει το TRex για κάθε δοκιμαστική εκτέλεση. Εξετάζεται επίσης το ενδεχόμενο ενσωμάτωσης του TRex με πίνακες εργαλείων παρακολούθησης (Grafana, Prometheus), τους οποίους ορισμένοι χρήστες έχουν ρυθμίσει για δοκιμές μεγάλης διάρκειας. Η συνεπής καταγραφή των αποτελεσμάτων επιτρέπει την ευκολότερη σύγκριση μεταξύ διαφορετικών εκτελέσεων ή διαμορφώσεων.

- Αναπαραγωγιμότητα και Scripting: Αξιοποιείται το Python API της TRex για δοκιμές σεναρίων με επαναλαμβανόμενο τρόπο. Αντί για μη αυτόματη εκκίνηση και διακοπή μέσω CLI, ένα σενάριο μπορεί να διαμορφώνει τις ίδιες ακριβώς συνθήκες κάθε φορά, κάτι που είναι σημαντικό για επιστημονικές συγκρίσεις. Το σενάριο μπορεί επίσης να αυτοματοποιήσει τη συλλογή των αποτελεσμάτων και ίσως την επαναφορά του DUT μεταξύ των δοκιμών.
- Καταγραφή αποτελεσμάτων: Συνίστατι η αποθήκευση των αρχείων καταγραφής της διαμόρφωσης TRex (πρότυπα πακέτων, ρυθμοί, διάρκεια) μαζί με τα αποτελέσματα. Αυτό βοηθά να διασφαλιστεί ότι τυχόν παρατηρήσεις απόδοσης (επιτευχθείσα απόδοση, απώλεια, καθυστέρηση) μπορούν να εντοπιστούν στις συνθήκες που τις παρήγαγαν. Το TRex είναι ντετερμινιστικό δεδομένου της ίδιας διαμόρφωσης και τυχαίας εμφάνισης, επομένως αξιοποιείται ως προς τη συνέπεια εκτέλεσης δοκιμών.

Ακολουθώντας αυτές τις πρακτικές, το TRex αναδεικνύεται ως ένα από τα πιο ισχυρά και ευέλικτα εργαλεία για τη δημιουργία και την ανάλυση της κίνησης δικτύου σε υψηλές ταχύτητες . Η ικανότητά του να ενσωματώνεται σε σύνθετα σενάρια δοκιμών (από τη συγκριτική αξιολόγηση πυρήνα 5G έως τη δοκιμή τείχους προστασίας επιχειρήσεων) το καθιστά δημοφιλές τόσο σε εταιρικά όσο και σε ακαδημαϊκά περιβάλλοντα. Ενώ η επίτευξη κορυφαίας απόδοσης απαιτεί εξειδίκευση στη δικτύωση και τον συντονισμό συστημάτων, η ανοιχτή αρχιτεκτονική του TRex επιτρέπει συνεχή βελτίωση και προσαρμογή στις μεταβαλλόμενες ανάγκες των σύγχρονων δικτύων , συμπεριλαμβανομένης της ακραίας κλίμακας των επιπέδων δεδομένων 5G.

4.6. Mininet(SDN)

Η ταχεία άνοδος της δικτύωσης που καθορίζεται από λογισμικό (SDN) έχει υπογραμμίσει την ανάγκη για εργαλεία που επιτρέπουν ευέλικτη προσομοίωση και εξομοίωση τοπολογιών δικτύου. Σε αυτό το χώρο το Mininet κατέχει κεντρική θέση. Το Mininet επιτρέπει τη δημιουργία και τη διαχείριση εικονικών δικτύων σε έναν μόνο υπολογιστή (ή εικονική μηχανή), επιτρέποντας τη μελέτη πρωτοκόλλων και αρχιτεκτονικών SDN με χαμηλό κόστος και με υψηλό βαθμό επαναληψιμότητας. [51]27
Το Mininet είναι ένα εργαλείο εξομοίωσης δικτύου ανοιχτού κώδικα γραμμένο σε Python που δημιουργεί ρεαλιστικά εικονικά δίκτυα χρησιμοποιώντας ελαφριές δυνατότητες εικονικοποίησης του πυρήνα Linux. Αντί να προσομοιώνει καθαρά τη συμπεριφορά του δικτύου με έναν αφηρημένο τρόπο, το Mininet μιμείται δίκτυα εκκινώντας πραγματικές διεργασίες πυρήνα και χώρου χρήστη για να αναπαραστήσουν κεντρικούς υπολογιστές, μεταγωγείς και συνδέσμους. Στην πράξη, όταν το Mininet «δημιουργεί» έναν κεντρικό υπολογιστή, στην πραγματικότητα ξεκινά μια ξεχωριστή διαδικασία (σε ξεχωριστό χώρο ονομάτων δικτύου) που μπορεί να τρέξει πραγματικό λογισμικό δικτύωσης (ping, iperf, διακομιστές ιστού κ.λπ.) σαν να ήταν ένα ξεχωριστό μηχάνημα. Ομοίως, το Mininet μπορεί να δημιουργήσει εικονικούς διακόπτες (συχνά

27 http://mininet.org/

χρησιμοποιώντας Open vSwitch) και να συνδέει κεντρικούς υπολογιστές και διακόπτες με ζεύγη εικονικού Ethernet (veth) που εξομοιώνουν συνδέσμους (με ρυθμιζόμενο εύρος ζώνης, χαρακτηριστικά καθυστέρησης και απώλειας).
Τα βασικά στοιχεία με τα οποία λειτουργεί το Mininet περιλαμβάνουν:[43]28

- Κεντρικοί υπολογιστές: Οι εικονικοί κεντρικοί υπολογιστές είναι χώροι ονομάτων δικτύου Linux ή cgroups που εκτελούν κανονικές διεργασίες Linux αλλά έχουν απομονωμένες στοίβες δικτύου. Κάθε κεντρικός υπολογιστής στο Mininet έχει τις δικές του διεπαφές, διευθύνσεις IP, πίνακα δρομολόγησης κ.λπ., ακριβώς όπως ένας πραγματικός κεντρικός υπολογιστής.
- Διακόπτες: Εικονικοί διακόπτες (συνήθως Open vSwitch σε λειτουργία πυρήνα ή ο διακόπτης αναφοράς χώρου χρήστη) που βρίσκονται στον ίδιο πυρήνα αλλά προωθούν πακέτα μεταξύ εικονικών διεπαφών όπως ακριβώς θα έκανε ένας διακόπτης υλικού. Αυτοί οι διακόπτες μπορούν να ελεγχθούν μέσω OpenFlow από έναν εξωτερικό ελεγκτή SDN, καθιστώντας το Mininet ιδανικό για πειράματα SDN.
- Σύνδεσμοι: Οι εικονικοί σύνδεσμοι είναι ζεύγη συνδεδεμένων εικονικών διεπαφών Ethernet. Το Mininet επιτρέπει τη ρύθμιση παραμέτρων όπως το εύρος ζώνης (χρησιμοποιώντας έλεγχο κυκλοφορίας Linux), την καθυστέρηση (με την προσθήκη καθυστέρησης μέσω tc) και τα ποσοστά απώλειας πακέτων σε αυτούς τους συνδέσμους για την εξομοίωση συνθηκών δικτύου.
- Ελεγκτής: Σε σενάρια SDN, το Mininet μπορεί να συνδέσει τους εικονικούς διακόπτες σε έναν ελεγκτή SDN (ο οποίος μπορεί να εκτελείται εντός ή εκτός του Mininet). Ο ελεγκτής δεν δημιουργείται από το Mininet αυτό καθαυτό, αλλά το Mininet διευκολύνει τη σύνδεση ενός (για παράδειγμα, μπορεί να ξεκινήσει αυτόματα μια διαδικασία ελεγκτή όπως το POX ή το Ryu ή μπορεί να κατευθύνει τους διακόπτες στην IP ενός εξωτερικού ελεγκτή).

Η αρχιτεκτονική του Mininet αξιοποιεί σε μεγάλο βαθμό την υποστήριξη του πυρήνα Linux για χώρους ονομάτων δικτύου και εικονικά ζεύγη Ethernet. Όταν ξεκινά μια τοπολογία Mininet, μπορεί να δημιουργήσει, για παράδειγμα, 3 χώρους ονομάτων κεντρικού υπολογιστή (h1, h2, h3), 2 διακόπτες OVS (διεργασίες s1, s2) και στη συνέχεια να δημιουργήσει ζεύγη veth που συνδέουν τα h1<->s1, h2<->s1, s1<->s2, s2, top., κ.λπ. προσαρμοσμένο σχέδιο). Όλα αυτά συμβαίνουν σε έναν πυρήνα, επομένως η επιβάρυνση είναι χαμηλή – η εναλλαγή περιβάλλοντος μεταξύ διεργασιών αντί για το χειρισμό πραγματικών συσκευών υλικού. Εξαιτίας αυτού, το Mininet μπορεί να δημιουργήσει δίκτυα σημαντικού μεγέθους (δεκάδες ή ακόμα και εκατοντάδες κόμβους) σε έναν υπολογιστή, που περιορίζονται κυρίως από την CPU και τη μνήμη.
Μια τυπική ροή εργασίας Mininet μπορεί να είναι: ορισμός τοπολογίας (είτε χρησιμοποιώντας το Python API είτε ορίσματα γραμμής εντολών για ενσωματωμένες τοπολογίες), εκκίνηση του δικτύου, εκτέλεση πειραμάτων (όπως εκκίνηση διακομιστή σε έναν κεντρικό υπολογιστή και πελάτη σε έναν άλλο, προγραμματισμός του ελεγκτή SDN για εγκατάσταση ορισμένων κανόνων ροής), συλλογή αποτελεσμάτων και μετά διακοπή του δικτύου. Το γεγονός ότι το Mininet χρησιμοποιεί πραγματικό κώδικα εφαρμογής σημαίνει ότι ο κώδικας που δοκιμάστηκε στο Mininet συχνά λειτουργεί αμετάβλητος σε πραγματικό υλικό αργότερα,29 αυτό είναι ένα τεράστιο όφελος για τη δημιουργία πρωτοτύπων.

28 http://mininet.org/
29 mininet.org

4.6.1. Βασικά Στοιχεία και Αρχιτεκτονική

Σε ένα περιβάλλον SDN, η λογική του επιπέδου ελέγχου διαχωρίζεται από το επίπεδο δεδομένων. Το Mininet το αποτυπώνει επιτρέποντας σε πραγματικούς ελεγκτές SDN να αλληλεπιδρούν με τους εξομοιούμενους διακόπτες μέσω τυπικών πρωτοκόλλων (κυρίως OpenFlow). Η τυπική αρχιτεκτονική ενός δικτύου SDN που βασίζεται σε Mininet αποτελείται από: [43]

- Εικονικοί κεντρικοί υπολογιστές (h1, h2, ...): Αυτά εκτελούν τυπικό λειτουργικό σύστημα Linux και μπορούν να εκτελέσουν οποιοδήποτε πρόγραμμα (ping, iperf, κ.λπ.). Συμπεριφέρονται σαν τελικοί οικοδεσπότες στο δίκτυο.
- Εικονικοί διακόπτες (s1, s2, ...): Συχνά ανοίγουν περιπτώσεις vSwitch που υποστηρίζουν OpenFlow. Προωθούν πακέτα σύμφωνα με κανόνες ροής και επικοινωνούν με έναν ελεγκτή SDN για εγκατάσταση κανόνων.
- Ελεγκτής SDN: Αυτό θα μπορούσε να εκτελείται εκτός Mininet (στο κεντρικό λειτουργικό σύστημα ή σε άλλο μηχάνημα) ή εντός του Mininet (ως διεργασία σε έναν από τους χώρους ονομάτων ή στον ριζικό χώρο ονομάτων). Ο ελεγκτής χρησιμοποιεί ένα πρωτόκολλο όπως το OpenFlow για να δώσει οδηγίες στους διακόπτες. Δημοφιλείς ελεγκτές όπως το Ryu, το POX ή το Floodlight μπορούν εύκολα να προσαρτηθούν στους διακόπτες Mininet προσδιορίζοντας την IP/θύρα του ελεγκτή.
- Σύνδεσμοι: Κάθε σύνδεσμος στο Mininet είναι ένα ζεύγος veth. Το ένα άκρο είναι προσαρτημένο σε έναν κεντρικό υπολογιστή ή διακόπτη, το άλλο άκρο στην αντίθετη πλευρά. Η στοίβα δικτύου του πυρήνα Linux χειρίζεται τα πακέτα που περνούν μεταξύ τους σαν να ήταν φυσικές συνδέσεις.

Όταν το Mininet ξεκινά μια τοπολογία, ο πυρήνας του Linux διαχειρίζεται όλες αυτές τις διεπαφές εικονικού δικτύου και διασφαλίζει την απομόνωση. Για παράδειγμα, κάθε χώρος ονομάτων κεντρικού υπολογιστή έχει τη δική του στοίβα δικτύου, επομένως η διεύθυνση IP ή η διαδικασία ενός κεντρικού υπολογιστή δεν παρεμβαίνει με τη διεύθυνση ενός άλλου κεντρικού υπολογιστή. Η γέφυρα Linux ή το OVS χρησιμοποιείται για διακόπτες για τη δημιουργία ενός διακόπτη λογισμικού στον οποίο μπορούν να συνδεθούν πολλά veth.

Η χρήση χώρων ονομάτων δικτύου και εικονικού Ethernet από το Mininet σημαίνει ότι από την οπτική γωνία μιας εφαρμογής, δεν υπάρχει διαφορά μεταξύ εκτέλεσης στο Mininet και εκτέλεσης σε πραγματικό δίκτυο – το σύστημα κλήσεων και τα API υποδοχής συμπεριφέρονται κανονικά. Αυτός είναι ο λόγος για τον οποίο το Mininet είναι τόσο ισχυρό: προσφέρει ρεαλιστική πιστότητα σε επίπεδο λειτουργικού συστήματος (ο χρονισμός και η απόδοση μπορεί να διαφέρουν από το πραγματικό υλικό, αλλά η λειτουργικότητα είναι η ίδια).

Ο κώδικας του Mininet παρέχει ένα API σε Python, όπου οι τοπολογίες δικτύου υλοποιούνται ως αντικείμενα Python. Οι χρήστες μπορούν να επεκτείνουν την κλάση Topo για να ορίσουν προσαρμοσμένες συνδέσεις κόμβων ή να χρησιμοποιήσουν έτοιμες τοπολογίες, όπως το Mininet(topo=TreeTopo(depth=2, fanout=3)), για τη γρήγορη δημιουργία μιας τοπολογίας δέντρου. Επιπλέον, το Mininet προσφέρει ένα περιβάλλον γραμμής εντολών (CLI), που επιτρέπει διαδραστικό πειραματισμό: μετά την εκκίνηση του δικτύου, ο χρήστης μπορεί να εκτελεί εντολές σε εικονικούς υπολογιστές (π.χ. h1 ping h2) ή να τροποποιεί απευθείας τις συνδέσεις και τις ρυθμίσεις του δικτύου μέσω του CLI.

4.6.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Η ευκολία χρήσης και η ευελιξία του Mininet το καθιστούν κρίσιμο εργαλείο τόσο για έρευνα όσο και για εκπαίδευση στη δικτύωση, ιδιαίτερα στο SDN. Μερικές σημαντικές περιπτώσεις χρήσης περιλαμβάνουν:[43]

- Εκπαίδευση και γρήγορη δημιουργία πρωτοτύπων: Σε ακαδημαϊκά περιβάλλοντα, το Mininet επιτρέπει στους μαθητές να εφαρμόσουν τη δική τους λογική ελεγκτή SDN (συχνά σε Python) και να τη δοκιμάσουν σε ένα ρεαλιστικό εικονικό δίκτυο σε δευτερόλεπτα. Για παράδειγμα, μια κοινή ανάθεση είναι η δημιουργία μιας προσαρμοσμένης εφαρμογής δρομολόγησης ή εξισορρόπησης φορτίου σε έναν ελεγκτή SDN και στη συνέχεια η αξιοποίηση του Mininet για την επίδειξη σε διαφορετικές τοπολογίες (γραμμικές, δέντρα, κ.λπ.). Η δυνατότητα περιστροφής τοπολογιών με λίγες παραμέτρους γραμμής εντολών σημαίνει ότι οι μαθητές μπορούν εύκολα να πειραματιστούν με διάφορα σχέδια δικτύου. Διευκολύνεται επίσης η δημιουργία πρωτοτύπων: οι ερευνητές μπορούν να γράψουν ένα σενάριο (π.χ., να δημιουργήσουν ένα δίκτυο πλέγματος με διακόπτες OpenFlow, να εφαρμόσουν έναν νέο αλγόριθμο στον ελεγκτή) και να το επαληθεύσουν γρήγορα στο Mininet προτού ίσως μεταβούν σε μια πραγματική επιφάνεια δοκιμών.
- Αξιολόγηση νέων αλγορίθμων δρομολόγησης/εναλλαγής: Εφόσον το Mininet υποστηρίζει την εισαγωγή κανόνων δυναμικής ροής (μέσω ελεγκτών), οι ερευνητές δοκιμάζουν νέους αλγόριθμους δρομολόγησης ή σχέδια μηχανικής κυκλοφορίας προγραμματίζοντάς τους σε έναν ελεγκτή και αξιολογώντας τους σε δίκτυα Mininet. Για παράδειγμα, ένας αλγόριθμος για τη δρομολόγηση της συντομότερης διαδρομής ή την εξισορρόπηση φορτίου μπορεί να αναπτυχθεί σε έναν ελεγκτή Ryu και, στη συνέχεια, το Mininet μπορεί να μιμηθεί ένα δίκτυο όπου εισάγονται αστοχίες σύνδεσης ή διαφορετικά βάρη σύνδεσης για να δει πώς προσαρμόζεται ο αλγόριθμος. Χάρη στην υποστήριξη της Mininet για αναπαραγώγιμα πειράματα, μπορούν να εκτελεστούν διαφορετικά σενάρια και να συγκριθούν απευθείας με μετρήσεις όπως η απόδοση, ο λανθάνοντας χρόνος ή η χρήση δικτύου.
- QoS και Μελέτες Ασφάλειας: Το Mininet μπορεί να εισάγει καθυστερήσεις συνδέσεων, ανώτατα όρια εύρους ζώνης και απώλεια, κάτι που είναι πολύτιμο για πειράματα QoS , όπως ο έλεγχος του τρόπου με τον οποίο οι ουρές QoS σε έναν διακόπτη SDN χειρίζονται τη συμφόρηση ή πώς μια πολιτική QoS που βασίζεται σε SDN επηρεάζει το VoIP έναντι της μαζικής κυκλοφορίας. Από την πλευρά της ασφάλειας, μπορεί κανείς να μιμηθεί σενάρια επίθεσης – π.χ. ένας κεντρικός υπολογιστής που ξεκινά μια σάρωση θύρας ή μια προσπάθεια MITM – και να δοκιμάσει τους ελέγχους ασφαλείας που βασίζονται σε SDN ή τις πολιτικές τμηματοποίησης δικτύου. Δεδομένου ότι το Mininet χρησιμοποιεί πραγματικές στοίβες δικτύου, εργαλεία όπως συστήματα ανίχνευσης εισβολής (Snort, κ.λπ.) μπορούν να εκτελούνται σε αυτό για να αξιολογήσουν πόσο καλά εντοπίζουν αυτές τις επιθέσεις σε ένα περιβάλλον SDN.

Επιπλέον, το Mininet δεν περιορίζεται στο SDN. Μπορεί επίσης να χρησιμοποιηθεί για την εξομοίωση παραδοσιακών δικτύων ή υβριδικών δικτύων. Για παράδειγμα, θα μπορούσε κανείς να χρησιμοποιήσει το Mininet για να μιμηθεί ένα τμήμα ενός δικτύου πυρήνα 5G εκτελώντας τα στοιχεία Open5GS σε κεντρικούς υπολογιστές Mininet και συνδέοντάς τα μέσω διακοπτών Mininet για να επιβάλει ορισμένες συνθήκες δικτύου - ουσιαστικά μια εξομοίωση 5G. Πράγματι, για κάθε περίπτωση όπου κάποιος θέλει πραγματικό λογισμικό δικτύου να αλληλεπιδρά σε ένα εικονικό περιβάλλον (με ελεγχόμενες συνθήκες), το Mininet είναι μια εξαιρετική επιλογή.

Ειδικά για την έρευνα 5G, το Mininet έχει χρησιμοποιηθεί στο πλαίσιο πειραμάτων SDN/NFV, όπως η ενορχήστρωση λειτουργιών εικονικού δικτύου ή η δοκιμή σεναρίων υπολογιστικών κατανεμημένων άκρων.

4.6.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Το Mininet προσφέρει πολύ υψηλή πιστότητα επειδή χρησιμοποιεί την πραγματική δικτύωση πυρήνα Linux. Αυτό σημαίνει ότι η συμπεριφορά του πρωτοκόλλου, τα σφάλματα και τα χαρακτηριστικά απόδοσης (σε κάποιο βαθμό) αντικατοπτρίζουν τα πραγματικά συστήματα. Παρέχει υψηλή επαναληψιμότητα – το ίδιο σενάριο Mininet θα δημιουργήσει την ίδια τοπολογία με τα ίδια χαρακτηριστικά, κάτι που είναι εξαιρετικό για τη δίκαιη σύγκριση αλγορίθμων. Το Mininet μειώνει επίσης δραματικά το κόστος και τον χρόνο εγκατάστασης σε σύγκριση με τα φυσικά εργαστήρια. Για πολλά ερευνητικά εργαστήρια, η ικανότητα του Mininet να μιμείται εκατοντάδες κόμβους σε ένα μηχάνημα ανοίγει ευκαιρίες που δεν θα ήταν πρακτικές με πραγματικό υλικό. Είναι επίσης επεκτάσιμο : μπορεί κανείς να ενσωματώσει το Mininet με άλλα εργαλεία, για παράδειγμα χρησιμοποιώντας το με το πιρούνι Containernet για την εκκίνηση κοντέινερ Docker ως κεντρικούς υπολογιστές για τη δοκιμή VNF ή να επεκταθεί σε κατανεμημένα συμπλέγματα Mininet όταν ένα μηχάνημα δεν είναι αρκετό. Η κοινότητα και η τεκμηρίωση είναι ισχυρά, καθώς το Mininet υιοθετείται ευρέως στην κοινότητα SDN.[43]30
Προκλήσεις: Εφόσον το Mininet εκτελεί όλους τους κόμβους σε ένα λειτουργικό σύστημα, περιορίζεται από τους πόρους αυτού του λειτουργικού συστήματος. Σε πολύ μεγάλες τοπολογίες (εκατοντάδες κεντρικοί υπολογιστές/διακόπτες), η CPU ή η μνήμη μπορεί να αποτελέσουν εμπόδιο, οδηγώντας σε πιο αργή απόδοση ή ακόμα και σε μη ρεαλιστική συμπεριφορά εάν η μηχανή υποδοχής είναι υπερφορτωμένη. Για παράδειγμα, σε ένα μοντέλο δικτύου με συνδέσμους 1000 Mbps σε φορητό υπολογιστή, δυσκολεύεται η ωθήση αυτής της απόδοσης λόγω των ορίων του μεμονωμένου μηχανήματος. Ορισμένες πτυχές των διακοπτών υλικού (όπως εκφόρτωση υλικού, περιορισμοί TCAM, εξειδικευμένες συμπεριφορές ουράς QoS) δεν μπορούν να αναπαραχθούν ακριβώς στο λογισμικό, επομένως το Mininet ενδέχεται να μην καταγράφει κάθε ιδιαιτερότητα φυσικών συσκευών. Επιπλέον, ο χρόνος στο Mininet είναι πραγματικός χρόνος – εάν η εξομοίωση ενός δικτύου υπερφορτωθεί, τα συμβάντα ενδέχεται να καθυστερήσουν ή ο προγραμματισμός της αποστολής πακέτων θα μπορούσε να καθυστερήσει πέρα από αυτό που θα ήταν στην πραγματικότητα. Για ακριβείς μελέτες χρονισμού, αυτό μπορεί να είναι ένα ζήτημα. Επίσης, ορισμένα χαρακτηριστικά του πυρήνα ενδέχεται να μην αντιπροσωπεύονται πλήρως. Για παράδειγμα, κάποια προγράμματα οδήγησης NIC ή ειδικές μονάδες πυρήνα που δεν υπάρχουν στον κεντρικό υπολογιστή Mininet, ενδέχεται να λείπουν.
Το Mininet μπορεί να επεκταθεί σε πολλαπλά μηχανήματα (χρησιμοποιώντας προσεγγίσεις όπως το Mininet Cluster) για να μετριάσει ορισμένα προβλήματα κλίμακας διαχωρίζοντας κόμβους σε φυσικούς διακομιστές. Ωστόσο, κάτι τέτοιο προσθέτει πολυπλοκότητα και πιθανά προβλήματα χρονισμού μεταξύ των κεντρικών υπολογιστών. Αξίζει επίσης να σημειωθεί ότι ο εντοπισμός σφαλμάτων σε μια μεγάλη τοπολογία Mininet μπορεί να είναι περίπλοκος – επειδή όλα είναι εικονικά, πρέπει κανείς να χρησιμοποιεί προσεκτικά τα αρχεία καταγραφής και το Mininet CLI για τον εντοπισμό προβλημάτων (αν και εργαλεία όπως το Wireshark μπορούν να χρησιμοποιηθούν στο Mininet με λήψη σε εικονικές διεπαφές).

30 http://mininet.org/

Παρά αυτές τις προκλήσεις, για την πλειονότητα της έρευνας SDN και πολλών πειραμάτων δικτύωσης, το Mininet επιτυγχάνει μια πολύ καλή ισορροπία: υψηλό ρεαλισμό, ευκολία στη χρήση και καλή επεκτασιμότητα σε μέτριο υλικό . Ο περιορισμός της δέσμευσης ενός κεντρικού υπολογιστή είναι συχνά αποδεκτός για λειτουργικές δοκιμές και αξιολόγηση μέτριας κλίμακας. Όπου απαιτείται απόλυτη αξιολόγηση απόδοσης (όπως η μέτρηση της πραγματικής απόδοσης σε Gbps), μερικές φορές το Mininet χρησιμοποιείται σε συνδυασμό με πραγματικά πειράματα υλικού.

4.6.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την αποτελεσματικότερη αξιοποίηση του Mininet με σκοπό την εξομοίωση δικτύων και πειράματα SDN, συνιστώνται οι ακόλουθες βέλτιστες πρακτικές:[52] [53]

- Συνεχείς Ενημερώσεις: Αξιοποίηση της πιο πρόσφατη έκδοσης Mininet είτε μια σταθερής έκδοσης από το επίσημο αποθετήριο, καθώς συχνά περιλαμβάνει σημαντικές διορθώσεις για νεότερους πυρήνες λειτουργικού συστήματος. Ομοίως, για το Open vSwitch εάν συμμετέχει στη διάταξη, καθώς εκδίδονται συνεχώς βελτιώσεις απόδοσης και διορθώσεις σφαλμάτων (ιδιαίτερα σχετικές με νεότερες εκδόσεις OpenFlow).
- Σχεδίαση και ονομασία τοπολογίας: Στην περίπτωση των προσαρμοσμένων τοπολογίων (μέσω Python API), ονοματοδοτούνται οι κεντρικοί υπολογιστές και οι διακόπτες (το Mininet θα είναι από προεπιλογή h1, h2 κ.λπ., κάτι που είναι καλό, αλλά σε πολύπλοκα σενάρια, η σαφήνεια βοηθάει). Ο κώδικας της εκάστοτε τοπολογίας είναι καλό να δομηθεί με τρόπο ώστε να είναι εύκολο να γίνεται προσαρμογή των παραμέτρων (αρίθμηση διακοπτών ή κεντρικών υπολογιστών) χωρίς περιττές επαναλήψεις.
- Προμήθεια πόρων: Εφόσον χρειαστεί ο σχεδισμός μια μεγάλη τοπολογίας, εξετάζεται το ενδεχόμενο να χρησιμοποιήθούν συγκεκριμένα όρια CPU και μνήμης που μπορούν να εφαρμόσουν τα Mininet/CGroups σε κεντρικούς υπολογιστές για να αποφευχθουν τυχόν πόροι μεμονωμένων διεργασιών. Για πειράματα έντασης εύρους ζώνης, βεβαιώνεται ότι η CPU του κεντρικού υπολογιστή μπορεί να χειριστεί τον ρυθμό πακέτων. Στην περίπτωση εξομοίωσης συνδέσμων εξαιρετικά υψηλού εύρους ζώνης, ρυθμίζεται σε υψηλό επίπεδο με όριο την αποφυγή υπερφόρτωσης της CPU.
- Επιλογές ελεγκτή SDN: Επιλέγεται κατάλληλα ένας ελεγκτής SDN προσαρμοσμένος στην πειραματική διάταξη της αρεσκείας. Για γρήγορες δοκιμές, οι απλοί ελεγκτές (όπως ο βασικός ελεγκτής διακόπτη εκμάθησης που συνοδεύεται από παραδείγματα Mininet) είναι εντάξει. Για πιο σύνθετες εργασίες, χρειάζεται ένα πλήρες χειριστήριο όπως το Ryu ή το ONOS όπου εκτελείται εξωτερικά για καλύτερη απόδοση. Βεβαιώνεται ότι ο ελεγκτής και οι διακόπτες χρησιμοποιούν την ίδια έκδοση OpenFlow. Οι αναντιστοιχίες μπορεί να προκαλέσουν δυσμενής συνθήκες.
- Δοκιμή και εντοπισμός σφαλμάτων: Το Mininet είναι εξοπλισμένο με CLI για διαδραστικό εντοπισμό σφαλμάτων. Εντολές όπως `nodes` , `net` (για εμφάνιση συνδέσεων) και `pingall` είναι πολύ χρήσιμοι έλεγχοι λογικής. Εάν κάτι δεν λειτουργεί (όπως ένας κεντρικός υπολογιστής δεν μπορεί να κάνει ping σε έναν άλλο), αξιοποιείται η ικανότητα του Mininet να εκτελεί εντολές σε κεντρικούς υπολογιστές (π.χ. `h1 ifconfig -a` ή `h1 ps -a`) για εκτενή επιθεώρηση. Συχνά, τα προβλήματα μπορεί να οφείλονται σε εσφαλμένες ρυθμίσεις παραμέτρων IP ή σε ελλείψεις διαδρομών σε πολύπλοκες τοπολογίες – Το Mininet από προεπιλογή ρυθμίζει τη βασική συνδεσιμότητα IP, αλλά αν την παρακάμψουμε, πρέπει να τη χειριστούμε.

Λειτουργίες όπως το packet sniffing (tcpdump) στις διεπαφές και η εκτέλεση του Wireshark στο κεντρικό λειτουργικό σύστημα μπορούν να συμπληρώσουν όταν υπάρχει ανάγκη.

- Αναπαραγωγιμότητα: Το Mininet μπορεί να εκτελέσει ένα σενάριο Python μη διαδραστικά, το οποίο μπορεί να ξεκινήσει το δίκτυο, να εκτελέσει μια σειρά από εντολές (όπως έναρξη κυκλοφορίας, συλλογή δεδομένων) και στη συνέχεια να κλείσει. Αυτό διασφαλίζει ότι κάθε εκτέλεση είναι συνεπής. Εργαλεία όπως το tc (Traffic Control) μπορούν να χρησιμοποιηθούν στο Mininet για τη γραφή δυναμικών αλλαγών (όπως η εισαγωγή αποτυχίας σύνδεσης με την κατάργηση μιας διεπαφής ή αλλαγή της καθυστέρησης σύνδεσης κατά τη διάρκεια του χρόνου εκτέλεσης), τα οποία μπορούν να αυτοματοποιηθούν στο σενάριο.

Ακολουθώντας αυτές τις οδηγίες, το Mininet σε συνδυασμό με τις αρχές SDN παρέχει ένα ισχυρό πλαίσιο για ακαδημαϊκή έρευνα, εκπαίδευση και γρήγορη δημιουργία πρωτοτύπων ιδεών δικτύου . Μέσω της ρεαλιστικής εξομοίωσης δικτύου σε έναν μόνο κεντρικό υπολογιστή, οι χρήστες μπορούν να εφαρμόσουν πολύπλοκη λογική δικτύου και να τη δοκιμάσουν διεξοδικά πριν προχωρήσουν σε πιο δαπανηρά στάδια ανάπτυξης. Αν και κάποιος πρέπει να γνωρίζει τους περιορισμούς του ενός κεντρικού υπολογιστή και να είναι προσεκτικός στο σχεδιασμό σεναρίων, οι συμβιβασμούς αξίζουν συχνά τη διορατικότητα και την ευκολία που προσφέρει το Mininet στον τομέα της έρευνας δικτύωσης.

4.7. TeraVM

Η συνεχής ανάπτυξη και η αυξανόμενη πολυπλοκότητα των δικτύων – ειδικά τα περιβάλλοντα υψηλής ταχύτητας όπως τα σύγχρονα δίκτυα τηλεπικοινωνιών και τα δίκτυα υπηρεσιών δεδομένων – καθιστούν απαραίτητη τη χρήση εξειδικευμένων εργαλείων δοκιμών. Σε αυτό το πλαίσιο, το TeraVM ξεχωρίζει ως μια πλατφόρμα δοκιμών δικτύου υψηλής απόδοσης, σχεδιασμένη να δημιουργεί ρεαλιστικά και προσαρμόσιμα μοτίβα κυκλοφορίας, παρέχοντας πολύτιμες πληροφορίες για την απόδοση, την αξιοπιστία και την ανθεκτικότητα των υποδομών δικτύου. Το TeraVM χρησιμοποιείται τόσο στην έρευνα όσο και στη βιομηχανία, όπου η επικύρωση νέων τεχνολογιών, ο εξοπλισμός δοκιμών και η προσομοίωση επιθέσεων (π.χ. δοκιμές DDoS) είναι ζωτικής σημασίας για τη βελτιστοποίηση των υπηρεσιών και τη διασφάλιση της ευρωστίας.31

Σε αυτήν την ενότητα, παρουσιάζουμε τις θεμελιώδεις αρχές λειτουργίας του TeraVM, την αρχιτεκτονική του και τα σενάρια βασικών περιπτώσεων χρήσης, ενώ επίσης αναλύουμε τα πλεονεκτήματα και τις προκλήσεις που σχετίζονται με την ανάπτυξή του σε περιβάλλοντα δοκιμών πραγματικού κόσμου.

Το TeraVM είναι μια εμπορική λύση δοκιμής δικτύου (από τη Viavi Solutions) που έχει αναπτυχθεί για να καλύψει τις αυξημένες απαιτήσεις για ρεαλιστική παραγωγή κίνησης και δοκιμές υψηλής απόδοσης σε δίκτυα τηλεπικοινωνιών και δεδομένων. Αξιοποιεί προηγμένες τεχνολογίες όπως το DPDK (Data Plane Development Kit) – παρόμοιο με το TRex – για να επιτρέψει την άμεση πρόσβαση στο υλικό NIC και να παρακάμψει το λειτουργικό σύστημα για την επεξεργασία πακέτων, βελτιστοποιώντας έτσι την απόδοση και την καθυστέρηση. Χρησιμοποιώντας αυτήν την προσέγγιση, το TeraVM μπορεί να επιτύχει υψηλές ταχύτητες

31 https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf

μετάδοσης και να παράγει ρεαλιστικά σενάρια κυκλοφορίας, καθιστώντας το ιδανικό για δοκιμές συστήματος σε πραγματικό χρόνο.
Η πλατφόρμα χρησιμοποιείται για επικύρωση και αξιολόγηση απόδοσης συσκευών δικτύου όπως δρομολογητές, τείχη προστασίας, συστήματα ανίχνευσης εισβολής (IDS/IPS) και άλλα στοιχεία ασφαλείας, καθώς και για δοκιμή νέων αρχιτεκτονικών και πρωτοκόλλων σε περιβάλλοντα SDN/NFV. Η ικανότητά του να μιμείται ρεαλιστικές συνθήκες φορτίου και να υποστηρίζει πολύπλοκες ροές κυκλοφορίας καθιστά το TeraVM πολύτιμο τόσο για τους ερευνητές όσο και για τους επαγγελματίες τηλεπικοινωνιών.

4.7.1. Βασικά Στοιχεία και Αρχιτεκτονική

Η αρχιτεκτονική του TeraVM ακολουθεί μια προσέγγιση πελάτη-διακομιστή, όπου ο πυρήνας «δαίμονας» του TeraVM λειτουργεί ως η κεντρική μονάδα για τη δημιουργία και την επεξεργασία κίνησης. Ο δαίμονας, που συνήθως εκτελείται σε διακομιστή με NIC υψηλής απόδοσης, χρησιμοποιεί το DPDK για την πλήρη εκμετάλλευση των πόρων του συστήματος, επιτρέποντας την παράλληλη επεξεργασία πακέτων και εξαιρετικά υψηλούς ρυθμούς πακέτων. Μπορεί να διαχειριστεί πολλαπλές ροές κυκλοφορίας ταυτόχρονα, με κάθε ροή να μπορεί να διαμορφωθεί με διαφορετικές παραμέτρους όπως τύπο πρωτοκόλλου (TCP, UDP, ICMP, κ.λπ.), μέγεθος πακέτου, ρυθμό μετάδοσης και άλλα χαρακτηριστικά κυκλοφορίας32
Επιπλέον, το TeraVM παρέχει ένα ενσωματωμένο Python API που επιτρέπει την αυτοματοποίηση και την απομακρυσμένη διαχείριση των δοκιμών. Μέσω αυτού του API, οι χρήστες μπορούν να δημιουργούν προσαρμοσμένα σενάρια, να συλλέγουν λεπτομερή στατιστικά δεδομένα και να προσαρμόζουν παραμέτρους όπως η διάρκεια δοκιμής και οι συνθήκες κυκλοφορίας μέσω προγραμματισμού. Αυτή η δυνατότητα είναι ζωτικής σημασίας για την ακριβή μέτρηση της απόδοσης, καθώς επιτρέπει τη συνεπή επανάληψη των δοκιμών και τον ακριβή έλεγχο των μετρήσεων που συλλέγονται (διακίνηση, καθυστέρηση, απώλεια πακέτων, κ.λπ.).
Αναλύοντας την αρχιτεκτονική:

- Traffic Generation Engine: Η μηχανή πυρήνα (δαίμονας) που δημιουργεί πακέτα. Είναι βελτιστοποιημένη χρησιμοποιώντας DPDK, πράγμα που σημαίνει ότι μετράει τα NIC σε στενό βρόχο, αποφεύγοντας διακοπές του πυρήνα και μπορεί να στείλει πολλά πακέτα ανά επανάληψη βρόχου. Υποστηρίζει λειτουργία πολλαπλών πυρήνων, διανέμοντας ροές σε πυρήνες CPU για την επίτευξη υψηλότερης συνολικής απόδοσης. Ο κινητήρας μπορεί να χειριστεί πολλαπλές ροές ταυτόχρονα – για παράδειγμα, μια ροή μπορεί να δημιουργεί αιτήματα HTTP GET ενώ μια άλλη δημιουργεί ροές UDP – και να εφαρμόζει με ακρίβεια τους ελέγχους χρονισμού και κενού μεταξύ πακέτων.
- Προφίλ και πρότυπα κίνησης: Οι χρήστες διαμορφώνουν την κυκλοφορία στο TeraVM συνήθως καθορίζοντας πρότυπα ή προφίλ (π.χ. ένα προσομοιωμένο μοτίβο περιήγησης χρήστη ή μια ακολουθία πακέτων φωνητικών κλήσεων). Στη συνέχεια, το TeraVM χρησιμοποιεί αυτά τα πρότυπα για να δημιουργήσει πραγματικά πακέτα. Επειδή είναι ένας ελεγκτής πλήρους στοίβας, μπορεί να μιμηθεί συμπεριφορές χειραψίας, για παράδειγμα ολοκλήρωση μιας τριπλής χειραψίας TCP και στη συνέχεια αποστολή ωφέλιμου φορτίου, προσομοιώνοντας αποτελεσματικά μια αλληλεπίδραση πελάτη-διακομιστή.
- Ανάλυση και παρακολούθηση: Η πλατφόρμα συλλέγει στατιστικά στοιχεία σε πραγματικό χρόνο για κάθε ροή κίνησης και συνολικά. Μετρά τη διεκπεραίωση (σε Gbps ή pps), τον

32 https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf

λανθάνοντα χρόνο (εάν έχουν διαμορφωθεί οι ροές βρόχου ή ηχούς), την απώλεια πακέτων και άλλα KPI. Αυτά τα δεδομένα μπορούν συχνά να οπτικοποιηθούν σε πίνακες εργαλείων ή να εξαχθούν για ανάλυση. Τα αναλυτικά στοιχεία του TeraVM είναι ζωτικής σημασίας για τη διάγνωση προβλημάτων απόδοσης στο Device Under Test (DUT) – για παράδειγμα, η αποτύπωση σε ποιο φορτίο ξεκινά η απώλεια πακέτων μπορεί να υποδηλώνει το όριο χωρητικότητας του DUT.

Ένα χαρακτηριστικό γνώρισμα της αρχιτεκτονικής του TeraVM είναι η εικονικοποιημένη φύση του : παρέχεται ως λύση λογισμικού που μπορεί να τρέξει σε γενικό υλικό x86 ή ακόμα και σε περιβάλλοντα εικονικού/σύννεφου (επομένως μερικές φορές περιγράφεται ως μια εικονική λύση δοκιμής IP). Αυτό προσφέρει ευελιξία – το ίδιο εργαλείο μπορεί να αναπτυχθεί σε διαφορετικά περιβάλλοντα (εργαστήριο, κέντρο δεδομένων, cloud) διασφαλίζοντας συνεπή μεθοδολογία δοκιμών.

Χρησιμοποιώντας τον έλεγχο από την πλευρά του πελάτη και τη δημιουργία από την πλευρά του διακομιστή, το TeraVM επιτρέπει την κλιμάκωση των δοκιμών και την ενορχήστρωση πολύπλοκων σεναρίων. Για παράδειγμα, μπορεί κανείς να έχει πολλαπλές παρουσίες TeraVM (ως VNF) που δημιουργούν κίνηση σε διαφορετικά μέρη ενός δικτύου κάτω από μια κεντρική ενορχήστρωση για μεγάλης κλίμακας δοκιμές από άκρο σε άκρο.

4.7.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Το TeraVM χρησιμοποιείται ευρέως σε σενάρια όπου απαιτείται επαλήθευση της απόδοσης και της αξιοπιστίας του δικτύου. Οι βασικές περιπτώσεις χρήσης περιλαμβάνουν:33

- Συγκριτική αξιολόγηση απόδοσης εξοπλισμού: Ένα πρωταρχικό σενάριο είναι η χρήση του TeraVM για τη συγκριτική αξιολόγηση δρομολογητών, διακοπτών και συσκευών ασφαλείας υπό μεγάλο φορτίο. Για παράδειγμα, ένας πάροχος υπηρεσιών μπορεί να δοκιμάσει ένα νέο αυτόνομο δίκτυο πυρήνων 5G χρησιμοποιώντας το TeraVM για τη δημιουργία τεράστιων ποσοτήτων κίνησης και σηματοδότησης αεροπλάνου χρήστη, επαληθεύοντας ότι η απόδοση και η καθυστέρηση ανταποκρίνονται στις προσδοκίες. Το TeraVM υποστηρίζει δοκιμές περιτύλιξης όπου μπορεί να μιμηθεί και τις δύο πλευρές μιας λειτουργίας δικτύου – για παράδειγμα, ενεργώντας τόσο ως gNB όσο και ως δίκτυο δεδομένων για να φορτώσει πλήρως ένα 5G Core UPF34. Με αυτόν τον τρόπο, μπορεί να δοκιμάζει κάθε λειτουργία δικτύου περιβάλλοντάς την με ρεαλιστική κίνηση.
- Stress Testing (DDoS, Edge Cases): Το TeraVM χρησιμοποιείται για δοκιμές ακραίων καταστάσεων όπου δημιουργούνται εξαιρετικά μεγάλοι όγκοι κίνησης για την εξέταση της αντοχής του συστήματος. Για παράδειγμα, προσομοίωση μιας επίθεσης DDoS μεγάλης κλίμακας (πολλαπλά Gbps μικρών πακέτων) για να ελεγχθεί πώς αντιμετωπίζει ένα τείχος προστασίας δικτύου. Είτε αποστολή ενός τεράστιου αριθμού ταυτόχρονων ροών για να φανεί εάν ένας εξισορροπητής φορτίου διατηρεί την απόδοση. Η ικανότητα του TeraVM να παράγει «τεράστιες ποσότητες κίνησης» βοηθά στον εντοπισμό σημείων θραύσης των συστημάτων, όπως όταν η CPU ή η μνήμη του DUT εξαντλείται.

33 https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf

34 *viavisolutions.com*

- Επικύρωση υποδομής SDN/NFV: Στα σύγχρονα δίκτυα με εικονικοποίηση, το TeraVM μπορεί να δημιουργηθεί ως λειτουργία εικονικού δικτύου. Αυτό σημαίνει ότι στις κλίνες δοκιμών NFV, το TeraVM μπορεί να είναι μέρος της αναπτυγμένης τοπολογίας για τη δημιουργία δοκιμαστικής κυκλοφορίας κατά παραγγελία. Για το SDN, θα μπορούσε κανείς να ενσωματώσει την κυκλοφορία TeraVM για να δει πώς ένα δίκτυο ελεγχόμενο από SDN χειρίζεται τις αλλαγές δυναμικού φορτίου ή για να επικυρώσει ότι τα τμήματα εικονικού δικτύου στο 5G μπορούν να απομονώσουν τη μεγάλη κυκλοφορία. Ουσιαστικά, οποιοδήποτε σενάριο όπου απαιτούνται ρεαλιστικά μοτίβα κυκλοφορίας για να επαληθευτεί ότι ο σχεδιασμός του δικτύου λειτουργεί όπως προβλέπεται (και δεν καταρρέει, για παράδειγμα, κάτω από ορισμένες κατανομές φορτίου) είναι υποψήφιο για χρήση TeraVM.
- Έρευνα και ανάπτυξη πρωτοκόλλων: Για ερευνητές που εργάζονται σε νέα πρωτόκολλα ή αλγόριθμους δικτύου, το TeraVM παρέχει ένα μέσο αξιολόγησης ιδεών υπό συνθήκες σχεδόν πραγματικές. Για παράδειγμα, εάν μια ομάδα αναπτύσσει έναν νέο αλγόριθμο ελέγχου συμφόρησης ή εξισορρόπησης φορτίου για το 5G, θα μπορούσε να το αναπτύξει σε ένα δοκιμαστικό δίκτυο και να χρησιμοποιήσουμε το TeraVM για να μιμηθεί χιλιάδες χρήστες ή ροές για να δει την επίδραση του αλγορίθμου στο QoS. Επειδή το TeraVM μπορεί επίσης να προσομοιώσει "κακές" συνθήκες δικτύου, όπως υψηλά ποσοστά σφάλματος ή jitter, μπορεί να χρησιμοποιηθεί για να ελέγξει την ευρωστία των πρωτοκόλλων και των υλοποιήσεων υπό αντίξοες συνθήκες.

Τέλος, το TeraVM χρησιμοποιείται επίσης στην έρευνα ασφάλειας για την προσομοίωση της κυκλοφορίας με κακόβουλα μοτίβα για τη δοκιμή συστημάτων ανίχνευσης ανωμαλιών. Η ευελιξία του στη δημιουργία κίνησης σημαίνει ότι κάποιος μπορεί να ενσωματώσει συγκεκριμένες υπογραφές ή συμπεριφορές στην κυκλοφορία και να επαληθεύσει εάν τις πιάνουν οι συσκευές ασφαλείας.

4.7.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Ένα από τα βασικά πλεονεκτήματα του TeraVM είναι η ικανότητά του να παράγει υψηλής ποιότητας, ρεαλιστική κίνηση σε πραγματικό χρόνο , χάρη στη βελτιστοποίηση μέσω DPDK και παρόμοιων τεχνικών.35Αυτό σημαίνει ότι μπορεί να δημιουργήσει ροές σε επίπεδο εφαρμογής σε υψηλή κλίμακα χωρίς απόρριψη πακέτων, κάτι που είναι απαραίτητο για ουσιαστική δοκιμή δικτύων υψηλής ταχύτητας. Η ευελιξία του στην προσαρμογή παραμέτρων το καθιστά ιδανικό για ένα ευρύ φάσμα εφαρμογών – από τη συγκριτική αξιολόγηση απόδοσης έως τις δοκιμές ασφαλείας. Το γεγονός ότι είναι μια εκλεπτυσμένη εμπορική λύση σημαίνει επίσης ότι συχνά συνοδεύεται από επαγγελματική υποστήριξη, λεπτομερείς διεπαφές χρήστη και εργαλεία αναφοράς που μπορεί να είναι πολύ χρήσιμα σε πολύπλοκα σενάρια δοκιμών. Οι δυνατότητες ενσωμάτωσης του TeraVM (όπως η ενορχηστρωμένη ως VNF ή η εργασία με πλαίσια αυτοματισμού) το καθιστούν κατάλληλο για περιβάλλοντα συνεχούς ενοποίησης όπου τα δίκτυα ελέγχονται τακτικά για παλινδρομήσεις. Επιπλέον, μια συγκριτική μελέτη ή ανέκδοτα στοιχεία υποδηλώνουν ότι σε ορισμένες πτυχές, όπως η καθυστέρηση στο επίπεδο ελέγχου, οι πυρήνες

35 . https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf

ανοιχτού κώδικα σε συνδυασμό με εργαλεία δοκιμών όπως το TeraVM μπορούν να παρέχουν σχετικά υψηλή απόδοση36.
Προκλήσεις: Η μεγιστοποίηση της απόδοσης του TeraVM, παρόμοια με το TRex, απαιτεί προσεκτική διαμόρφωση υλικού.37Οι χρήστες πρέπει να διασφαλίζουν ότι τα NIC βρίσκονται σε υποστηριζόμενες λίστες και είναι συντονισμένα (το DPDK συνήθως απαιτεί απομόνωση πυρήνων, χρήση τεράστιων σελίδων κ.λπ.). Η αρχική εγκατάσταση του TeraVM μπορεί να είναι περίπλοκη και το κόστος αδειοδότησης μπορεί να είναι απαγορευτικό για ορισμένα ακαδημαϊκά πλαίσια (αυτή είναι μια διαφορά από τα εργαλεία ανοιχτού κώδικα). Για λιγότερο έμπειρους χρήστες, η καμπύλη εκμάθησης μπορεί να είναι απότομη, καθώς η κατανόηση του τρόπου διαμόρφωσης πολύπλοκων μοτίβων κυκλοφορίας πολλαπλών ροών ή η ερμηνεία των μυριάδων στατιστικών απαιτεί εξειδίκευση στη δικτύωση. Μια άλλη πρόκληση είναι ότι το TeraVM, όντας πολύ ισχυρό, μπορεί να παράγει φορτία κυκλοφορίας που είναι δύσκολο να αναλυθούν χωρίς εξίσου ισχυρή παρακολούθηση – μπορεί κανείς ακούσια να δημιουργήσει περισσότερη κίνηση από ό,τι μπορεί να αντέξει το DUT ή ακόμα και το περιβάλλον δοκιμής, οδηγώντας σε παραπλανητικά αποτελέσματα αν δεν είναι προσεκτικός. Επίσης, ενώ το TeraVM ακολουθεί πρότυπα, ενδέχεται να υπάρχουν μικρές διαφορές στον τρόπο με τον οποίο εφαρμόζει ορισμένες συμπεριφορές πρωτοκόλλου σε σύγκριση με πραγματικές συσκευές (για παράδειγμα, το ακριβές μοτίβο των επιλογών TCP ή ο χρονισμός μπορεί να διαφέρει από έναν πραγματικό πελάτη), επομένως θα πρέπει να επικυρωθούν οι κρίσιμες υποθέσεις δοκιμών.
Η αρχική εγκατάσταση και διαμόρφωση ενδέχεται να είναι περίπλοκη για χρήστες χωρίς προηγούμενη εμπειρία σε δικτύωση υψηλής απόδοσης. Αλλά μόλις εγκατασταθεί, το TeraVM επαινείται γενικά ως μια ολοκληρωμένη λύση. Είναι σημαντικό να σημειωθεί ότι θα πρέπει να διατηρείται το λογισμικό ενημερωμένο για πρόσθετες βελτιώσεις (όπως υποστήριξη για νέες δυνατότητες 5G ή δυνατότητες δοκιμών O-RAN που μπορεί να εισαγάγει η Viavi, όπως υπονοείται από πράγματα όπως ο ελεγκτής O-CU στη σουίτα προϊόντων τους.38

4.7.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την αποτελεσματική ανάπτυξη του TeraVM συνίστανται οι προσεχείς πρακτικές:39

- Σταδιακή προσέγγιση: Οι δοκιμές ξεκινούν σε μικρή κλίμακα για να επιβεβαιωθεί ότι το TeraVM δημιουργεί την αναμενόμενη κίνηση και ότι η συσκευή υπό δοκιμή (π.χ. ένα τείχος προστασίας) την καταγράφει σωστά. Αρχικά, δοκιμάζεται μία μεμονωμένη ροή και διασφαλίζεται ότι το τείχος προστασίας είτε καταγράφει είτε επιτρέπει τη ροή, όπως αναμένεται. Μόνο αφού επιβεβαιωθεί η ορθή λειτουργία σε αυτή τη βασική περίπτωση, αυξάνεται σταδιακά ο αριθμός των ροών σε μεγαλύτερη κλίμακα.
- Βαθμονόμηση πόρων: Πριν από την έναρξη των κύριων δοκιμών, συνιστάται να αφιερωθεί χρόνος για τη βαθμονόμηση του περιβάλλοντος δοκιμής. Αυτό περιλαμβάνει την προσαρμογή του καρφιτσώματος της CPU για τα νήματα του TeraVM, τη διασφάλιση ότι οι κάρτες δικτύου (NIC) τοποθετούνται στις κατάλληλες υποδοχές PCI για την αποφυγή συμφόρησης του εύρους ζώνης, καθώς και την επαλήθευση ότι το κεντρικό σύστημα μπορεί να υποστηρίξει την απαιτούμενη απόδοση. Επιπλέον, παρακολουθείται η χρήση

36 *arxiv.org*
37 . https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf
38 *viavisolutions.com*
39 https://www.viavisolutions.com/en-us/literature/teravm-5g-core-security-test-data-sheets-en.pdf

της CPU και της μνήμης του δαίμονα TeraVM υπό δοκιμαστικό φορτίο, ώστε να διαπιστωθεί η ορθή λειτουργία του συστήματος.

- Σενάρια και ενορχήστρωση: Το TeraVM μπορεί να ενσωματωθεί σε αυτοματοποιημένες δοκιμαστικές σουίτες. Μέσω των διαθέσιμων API του, είναι δυνατό να δημιουργηθούν σενάρια που διαμορφώνουν και εκτελούν δοκιμές, επιτρέποντας την εύκολη επανάληψή τους καθώς και τον έλεγχο των εκδόσεων και των ορισμών τους. Αυτή η δυνατότητα διευκολύνει επίσης την ενσωμάτωση των δοκιμών του TeraVM σε αγωγούς συνεχούς ολοκλήρωσης (CI) για λογισμικό δικτύωσης, όπως για παράδειγμα την αυτόματη εκτέλεση δοκιμών απόδοσης με κάθε νέα έκδοση ενός πυρήνα 5G.
- Λεπτομερής καταγραφή: Όταν οι συσκευές υποβάλλονται σε δοκιμές στα όριά τους, συλλέγονται αρχεία καταγραφής τόσο από το TeraVM όσο και από τη συσκευή υπό δοκιμή. Οι μετρήσεις του TeraVM αποκαλύπτουν πότε αποστέλλεται η κίνηση και ποια απώλεια ή λανθάνουσα κατάσταση παρατηρείται, ενώ τα αρχεία καταγραφής της συσκευής μπορεί να εμφανίζουν προειδοποιήσεις ή σφάλματα. Ο συσχετισμός των δύο πηγών δεδομένων μπορεί να βοηθήσει στον εντοπισμό των τρόπων αποτυχίας, όπως για παράδειγμα πτώση πακέτων από την CPU όταν το φορτίο φτάνει το 80%.
- Δοκιμή φόρτωσης βημάτων: Αντί να εφαρμόζεται απευθείας το 100% του φορτίου, ακολουθείται μια διαδικασία κλιμακωτών αυξήσεων φορτίου (π.χ. 10%, 20%, ... 100%) με τη χρήση του TeraVM. Αυτή η προσέγγιση βοηθά στον εντοπισμό του σημείου όπου η απόδοση αρχίζει να υποβαθμίζεται και παρέχει μια καμπύλη απόδοσης αντί για ένα μόνο σημείο μέτρησης. Το TeraVM μπορεί συνήθως να προγραμματιστεί ώστε να αυξάνει σταδιακά το φορτίο και να καταγράφει τα αποτελέσματα σε κάθε βήμα.
- Γνώση πρωτοκόλλων: Είναι αναγκαίο κανείς να διασφαλίζει ότι τα μοτίβα κυκλοφορίας που δημιουργούνται με το TeraVM ανταποκρίνονται ρεαλιστικά στις απαιτήσεις της δοκιμής. Για παράδειγμα, όταν αξιολογείται ένας διακομιστής DNS, η δημιουργούμενη κίνηση σχεδιάζεται ώστε να προσομοιώνει πραγματικά DNS queries, αντί για γενικά UDP πακέτα. Σε σενάρια 5G, κατά τον έλεγχο της χωρητικότητας του επιπέδου ελέγχου, το TeraVM διαμορφώνεται ώστε να παράγει κατάλληλα NAS μηνύματα. Η εις βάθος κατανόηση του υπό δοκιμή πρωτοκόλλου συμβάλλει στη βέλτιστη παραμετροποίηση του εργαλείου.

Με την τήρηση αυτών των οδηγιών, το TeraVM αποδεικνύεται ότι είναι ένα από τα πιο ισχυρά και ευέλικτα εργαλεία για τη δημιουργία και την ανάλυση της κίνησης δικτύου σε περιβάλλοντα υψηλής απόδοσης . Η ικανότητά του να ενσωματώνεται σε πολύπλοκα σενάρια δοκιμών (δοκιμές 5G, αξιολογήσεις IDS/IPS, συγκριτική αξιολόγηση εξοπλισμού δικτύου) το καθιστά δημοφιλές τόσο σε εταιρικά όσο και σε ακαδημαϊκά πλαίσια. Αν και η βελτιστοποίηση και η κλιμάκωση της απόδοσης απαιτούν εξειδικευμένες γνώσεις σε DPDK και συντονισμό υλικού, η ανοιχτή και αρθρωτή αρχιτεκτονική της TeraVM (ως λύση λογισμικού) επιτρέπει τη συνεχή βελτίωση και προσαρμογή στις εξελισσόμενες ανάγκες των σύγχρονων δικτύων, διασφαλίζοντας ότι παραμένει στην πρώτη γραμμή των λύσεων δοκιμών δικτύου.

4.8. Wireshark

Η αυξανόμενη πολυπλοκότητα των σύγχρονων δικτύων απαιτεί όχι μόνο τη δημιουργία ρεαλιστικής κίνησης για τη δοκιμή νέων τεχνολογιών, αλλά και λεπτομερή ανάλυση αυτής της κίνησης για τον εντοπισμό και την αντιμετώπιση προβλημάτων. Σε αυτό το πλαίσιο, το Wireshark

διαδραματίζει κρίσιμο ρόλο. Αν και είναι κυρίως γνωστό ως εργαλείο ανάλυσης πακέτων δικτύου, η ικανότητα του Wireshark να συλλαμβάνει και να καταγράφει δεδομένα κίνησης (σύλληψη πακέτων) καθιστά δυνατή τη δημιουργία ρεαλιστικών σεναρίων όταν συνδυάζεται με εργαλεία επανάληψης. Αυτή η ενότητα παρέχει μια εις βάθος επισκόπηση των λειτουργιών, της αρχιτεκτονικής και των περιπτώσεων χρήσης του Wireshark ως θεμελιώδες μέρος μιας ολιστικής διαδικασίας δημιουργίας και αξιολόγησης κίνησης δικτύου.40

Το Wireshark είναι ένα εργαλείο ανάλυσης πακέτων δικτύου ανοιχτού κώδικα που χρησιμοποιείται ευρέως για την παρακολούθηση, την καταγραφή και την ανάλυση της κίνησης σε δίκτυα IP. Δεδομένου ότι η ακριβής σύλληψη πακέτων είναι το πρώτο βήμα για τη δημιουργία ρεαλιστικών σεναρίων κυκλοφορίας, το Wireshark έχει γίνει αναπόσπαστο στοιχείο των πειραματικών περιβαλλόντων. Αν και δεν είναι από μόνο του γεννήτρια κίνησης, τα δεδομένα που συλλαμβάνει μπορούν να χρησιμεύσουν ως βάση για την επανάληψη της κυκλοφορίας χρησιμοποιώντας εξειδικευμένα εργαλεία όπως το Tcpreplay ή το TRex.

Στο πλαίσιο μας, το Wireshark χρησιμοποιείται για τη λήψη των ακριβών πακέτων σε ένα δίκτυο κατά τη διάρκεια πραγματικών λειτουργιών ή δοκιμών, τα οποία στη συνέχεια μπορούν να αποθηκευτούν σε αρχεία PCAP . Αυτά τα αρχεία PCAP αντιπροσωπεύουν μια εγγραφή πραγματικής κίνησης δικτύου που μπορεί αργότερα να αναπαραχθεί ή να αναλυθεί για να ενημερώσει τη δημιουργία συνθετικής κίνησης. Ως εκ τούτου, το Wireshark υποστηρίζει τη δημιουργία κίνησης παρέχοντας την «βασική αλήθεια» της συμπεριφοράς του δικτύου που προσπαθούν να αναπαράγουν οι παραγωγοί κίνησης.

4.8.1. Βασικά Στοιχεία και Αρχιτεκτονική

Το Wireshark προσφέρει ένα ευρύ φάσμα λειτουργιών που το καθιστούν ιδανικό για ανάλυση κυκλοφορίας41

- Καταγραφή πακέτων (Capture Engine): Το Wireshark μπορεί να συλλάβει πακέτα από διάφορες διεπαφές δικτύου σε πραγματικό χρόνο. Συνδέεται με βιβλιοθήκες pcap (όπως το libpcap/WinPcap) για να θέσει τις διεπαφές δικτύου σε ακατάλληλη λειτουργία και να καταγράψει όλα τα πακέτα που ταιριάζουν με τα κριτήρια λήψης. Οι χρήστες μπορούν να εφαρμόσουν φίλτρα λήψης για να εστιάσουν σε συγκεκριμένα πρωτόκολλα ή διευθύνσεις, κάτι που είναι χρήσιμο σε περιβάλλοντα υψηλής κίνησης για να αποφευχθεί η κατακλυσμός από δεδομένα.
- Φιλτράρισμα και αποκωδικοποίηση: Το Wireshark διαθέτει μια ισχυρή γλώσσα φίλτρου εμφάνισης που επιτρέπει στους χρήστες να απομονώνουν πακέτα ενδιαφέροντος (π.χ. όλα τα αιτήματα HTTP GET ή όλα τα πακέτα σε μια συγκεκριμένη IP). Περιλαμβάνει επίσης ανατομείς για ένα ευρύ φάσμα πρωτοκόλλων, που σημαίνει ότι μπορεί να αποκωδικοποιήσει και να εμφανίσει τα πεδία των πρωτοκόλλων (σημαίες TCP, διευθύνσεις URL HTTP, μηνύματα NAS 5G, κ.λπ.) σε αναγνώσιμη από τον άνθρωπο μορφή. Αυτό βοηθά στον εντοπισμό προβλημάτων σε συγκεκριμένα επίπεδα πρωτοκόλλου.
- Αποθήκευση πακέτων (αρχεία PCAP): Τα πακέτα που έχουν συλληφθεί μπορούν να αποθηκευτούν στην τυπική μορφή PCAP. Αυτά τα αρχεία μπορούν αργότερα να χρησιμοποιηθούν για ανάλυση ή επανάληψη. Το Wireshark υποστηρίζει επίσης νεότερες

40 https://www.wireshark.org/

41 https://static.alta3.com/outlines/wireshark-5g/wireshark-5g.pdf

μορφές όπως το PCAPNG που μπορούν να αποθηκεύουν πρόσθετα μεταδεδομένα (όπως πληροφορίες διεπαφής ή στατιστικά καταγεγραμμένων πτώσεων).

- Packet Injection (text2pcap, κ.λπ.): Αν και δεν αποτελεί μέρος του GUI του Wireshark, η σουίτα Wireshark περιλαμβάνει βοηθητικά προγράμματα όπως το text2pcap που μπορούν να μετατρέψουν περιγραφές πακέτων κειμένου σε αρχεία PCAP. Αυτό παρέχει τη δυνατότητα κατασκευής προσαρμοσμένων πακέτων ή τροποποίησης ιχνών μέσω κειμένου και στη συνέχεια παραγωγής PCAP, επιτρέποντας ουσιαστικά μια μορφή μη αυτόματης δημιουργίας κίνησης.

Η αρχιτεκτονική του Wireshark είναι πολυεπίπεδη. Στο χαμηλότερο επίπεδο, αλληλεπιδρά με το λειτουργικό σύστημα για τη λήψη ακατέργαστων καρέ. Αυτά στη συνέχεια περνούν μέσω διατομέων που ερμηνεύουν τα byte σύμφωνα με τις προδιαγραφές του πρωτοκόλλου (το Wireshark έχει ένα αρθρωτό σύστημα διαχωρισμού, όπου κάθε επίπεδο πρωτοκόλλου προσθέτει νόημα στα ακατέργαστα δεδομένα). Στη συνέχεια, το GUI παρουσιάζει αυτές τις αποκωδικοποιημένες πληροφορίες για κάθε πακέτο. Κατά τη λήψη, το Wireshark χρησιμοποιεί buffer και εγγράφει στο δίσκο σταδιακά, εάν χρειάζεται, για να χειριστεί μεγάλες λήψεις.
Μια κρίσιμη πτυχή είναι ότι το Wireshark λειτουργεί παθητικά . δεν αλλάζει την κίνηση (εκτός αν κάποιος χρησιμοποιεί έμμεσα τις δυνατότητες έγχυσης πακέτων). Αυτό το καθιστά κατάλληλο για την καταγραφή κίνησης από ζωντανά δίκτυα δίχως την ανάγκη αναδιαμόρφωσης. Για τη δημιουργία κίνησης, κανονικά κάποιος καταγράφει αντιπροσωπευτική κίνηση με το Wireshark και στη συνέχεια χρησιμοποιεί το αρχείο καταγραφής με ένα εργαλείο δημιουργίας. Αυτό διασφαλίζει ότι τα μοτίβα κυκλοφορίας που χρησιμοποιούνται στις δοκιμές είναι όσο το δυνατόν πιο ρεαλιστικά, επειδή προέρχονται από πραγματική χρήση δικτύου.

4.8.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Σε περιβάλλοντα δοκιμών και αξιολόγησης, το Wireshark χρησιμοποιείται ως το πρώτο βήμα για τη συλλογή δεδομένων . Ένα τυπικό σενάριο μπορεί να περιλαμβάνει την καταγραφή κίνησης σε ένα ενεργό δίκτυο ή δοκιμαστική βάση για τη συλλογή βασικών χαρακτηριστικών. Μερικές περιπτώσεις χρήσης και εφαρμογές:42

- Αποτύπωση κίνησης βασικής γραμμής για επανάληψη: Ας υποθέσουμε ότι οι ερευνητές θέλουν να αξιολογήσουν έναν νέο πυρήνα 5G υπό ρεαλιστικό φορτίο. Θα μπορούσαν πρώτα να καταγράψουν την κίνηση από ένα πραγματικό δίκτυο κινητής τηλεφωνίας ή από ένα σενάριο αναφοράς (συμπεριλαμβανομένων των δεδομένων επιπέδου χρήστη και των μηνυμάτων επιπέδου ελέγχου). Αποθηκεύοντας αυτό το ίχνος, μπορούν στη συνέχεια να χρησιμοποιήσουν ένα εργαλείο όπως το TRex ή το Tcpreplay για να αναπαράγουν ξανά αυτό το ίχνος μέσω του βασικού δικτύου σε μια ελεγχόμενη εργαστηριακή ρύθμιση. Το αποτέλεσμα είναι μια ρεαλιστική δοκιμή του πυρήνα με τη χρήση πραγματικών μοτίβων κυκλοφορίας, διασφαλίζοντας ότι οι λεπτές αποχρώσεις, όπως η ριπή ή οι χρόνοι μεταξύ των αφίξεων του πρωτοκόλλου, διατηρούνται από τον πραγματικό κόσμο.
- Αντιμετώπιση προβλημάτων και χαρακτηρισμός: Το Wireshark είναι εξαιρετικά χρήσιμο για την αξιολόγηση της συμπεριφοράς των μηχανισμών ασφαλείας ή των ρυθμίσεων QoS. Για παράδειγμα, σε μια αξιολόγηση ασφαλείας, μπορεί κανείς να καταγράψει την κυκλοφορία κατά τη διάρκεια μιας απόπειρας εισβολής. Η λεπτομερής ανάλυση πακέτο

42 https://www.wireshark.org/ https://static.alta3.com/outlines/wireshark-5g/wireshark-5g.pdf

προς πακέτο από το Wireshark επιτρέπει την αναγνώριση του τρόπου με τον οποίο εκδηλώνεται η επίθεση στο καλώδιο (ακολουθία πακέτων, τυχόν ανωμαλίες). Αυτές οι πληροφορίες μπορούν στη συνέχεια να καθοδηγήσουν τον τρόπο δημιουργίας παρόμοιας κίνησης για τη δοκιμή συστημάτων IDS/IPS. Ομοίως, για QoS, η καταγραφή της κίνησης υπό διαφορετικές συνθήκες (με και χωρίς QoS) μπορεί να δείξει πώς διαφέρουν ο χρονισμός και η απώλεια πακέτων και ότι οι πληροφορίες θα μπορούσαν να χρησιμοποιηθούν για τη μοντελοποίηση της δημιουργίας κίνησης με μεγαλύτερη ακρίβεια.

- Συγκριτική Ανάλυση Κυκλοφορίας Πραγματικής έναντι Παραγόμενης Κίνησης: Αφού δημιουργήσουν κίνηση χρησιμοποιώντας συγκεκριμένα εργαλεία, οι ερευνητές χρησιμοποιούν συχνά το Wireshark για να καταγράψουν τη δημιουργούμενη κίνηση και να τη συγκρίνουν με το πραγματικό ίχνος για να εξασφαλίσουν την πιστότητα της παραγωγής. Για παράδειγμα, εάν χρησιμοποιείται το TRex για να μιμηθεί μια ροή βίντεο, θα μπορούσε κανείς να καταγράψει τόσο μια πραγματική συνεδρία ροής βίντεο όσο και τη συνεδρία που δημιουργείται από το TRex και να συγκρίνει μετρήσεις όπως η διανομή μεγέθους πακέτων, τα κενά μεταξύ των πακέτων και τα μοτίβα ριπής. Τα χαρακτηριστικά ανάλυσης του Wireshark, πιθανώς σε συνδυασμό με εξωτερικά σενάρια ανάλυσης, διευκολύνουν αυτή τη σύγκριση.

Στην έρευνα ασφάλειας, οι συλλήψεις του Wireshark βοηθούν στη δημιουργία υπογραφών επίθεσης ή στην κατανόηση του αντίκτυπου της επίθεσης. Κάποιος μπορεί να συλλάβει ένα σύνολο δεδομένων κανονικής κίνησης και κίνησης κατά τη διάρκεια μιας επίθεσης και, στη συνέχεια, να αναλύσει τις διαφορές (ίσως με το Wireshark ή την εξαγωγή σε CSV) για να δει ποιες δυνατότητες μπορούν να χρησιμοποιηθούν για εντοπισμό. Αν και αυτό υπερβαίνει ελαφρώς τη δημιουργία κίνησης, δείχνει τον ευρύτερο ρόλο της ανάλυσης κυκλοφορίας σε συνδυασμό με τη δημιουργία. Το Wireshark είναι επίσης ένα κοινό εργαλείο διδασκαλίας – οι μαθητές μπορούν να το χρησιμοποιήσουν για να δουν τα πραγματικά πακέτα πρωτοκόλλων για τα οποία μαθαίνουν. Σε εργαστήρια που εστιάζουν στη δημιουργία κίνησης, η καταγραφή με το Wireshark επαληθεύει τι στάλθηκε πραγματικά.

4.8.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Το κύριο πλεονέκτημα του Wireshark είναι το βάθος και η ακρίβεια της ανάλυσης που παρέχει. 43 44 Συχνά αποκαλείται ο κορυφαίος αναλυτής πρωτοκόλλων δικτύου στον κόσμο και για καλό λόγο – υποστηρίζει εκατοντάδες πρωτόκολλα και μπορεί να εμφανίσει εξαιρετικά λεπτομερείς πληροφορίες για κάθε πακέτο. Η ευκολία χρήσης του (GUI με φιλτράρισμα και χρωματισμό point-and-click) το καθιστά προσβάσιμο τόσο για φοιτητές όσο και για επαγγελματίες. Η ικανότητα αποθήκευσης συλλήψεων σημαίνει ότι τα πειράματα μπορούν να αρχειοθετηθούν και να κοινοποιηθούν, κάτι που είναι απαραίτητο στην έρευνα για αναπαραγωγιμότητα και σύγκριση. Το Wireshark είναι επίσης πολύ ευέλικτο: τρέχει σε πολλαπλά λειτουργικά συστήματα και υποστηρίζει πολλούς τύπους διεπαφής (Ethernet, Wi-Fi, loopback κ.λπ.).
Ένα άλλο πλεονέκτημα είναι η επεκτασιμότητα : οι χρήστες μπορούν να γράφουν προσαρμοσμένους διαχωριστές για νέα πρωτόκολλα ή να χρησιμοποιούν υπάρχουσες προσθήκες.

43 https://www.wireshark.org/

44 https://static.alta3.com/outlines/wireshark-5g/wireshark-5g.pdf

Αυτό είναι χρήσιμο για έρευνα αιχμής όπου ένα νέο πρωτόκολλο μπορεί να μην υποστηρίζεται ακόμη επίσημα, αλλά μπορεί κανείς να το ενσωματώσει για ανάλυση.
Από πλευράς δοκιμών, η ύπαρξη PCAP από το Wireshark είναι ανεκτίμητη, επειδή πολλά εργαλεία δημιουργίας και ανάλυσης κίνησης λειτουργούν με το PCAP ως είσοδο ή έξοδο. Οι συλλήψεις Wireshark χρησιμεύουν ως κοινό νόμισμα στις δοκιμές δικτύου, επιτρέποντας τη διαλειτουργικότητα μεταξύ διαφορετικών εργαλείων και ρυθμίσεων.
Προκλήσεις: Ένας περιορισμός του Wireshark είναι ότι από μόνο του δεν δημιουργεί κίνηση – βασίζεται αποκλειστικά στην καταγραφή της υπάρχουσας κίνησης στο δίκτυο. Για να χρησιμοποιηθεί σε ροές εργασιών δημιουργίας κίνησης, θα πρέπει να υπάρχει ήδη μια πηγή κίνησης προς σύλληψη (είτε πρόκειται για πραγματική κίνηση σε ένα δίκτυο παραγωγής είτε για κίνηση που δημιουργείται τεχνητά από κάποια γραμμή βάσης ή σενάριο δοκιμής). Συνεπώς, απαιτείται αρχικά πρόσβαση σε ένα δίκτυο παραγωγής ή σε ένα κατάλληλο σενάριο δοκιμής που να παράγει τον τύπο της κίνησης που ενδιαφέρει, κάτι που δεν είναι πάντα εφικτό ή διαθέσιμο..
Το Wireshark μπορεί επίσης να είναι συντριπτικό σε όγκο δεδομένων. μια μεγάλη σύλληψη ενός απασχολημένου δικτύου μπορεί να είναι εκατομμύρια πακέτα, καθιστώντας την ανάλυση μη τετριμμένη. Απαιτείται δεξιότητα στο φιλτράρισμα και γνώση πρωτοκόλλων για την εξαγωγή ουσιαστικών πληροφοριών. Για απόδοση, η λήψη σε πολύ υψηλούς ρυθμούς (όπως πολλαπλών gigabit) μπορεί να είναι δύσκολη - σε κατειλημμένους συνδέσμους, το Wireshark (μέσω libpcap) μπορεί να απορρίψει πακέτα εάν η μηχανή λήψης δεν μπορεί να συμβαδίσει, ενδεχομένως να χάσει κάποιες πληροφορίες (αν και για τη μοντελοποίηση γενιάς, η ελαφρά απώλεια μπορεί να είναι αποδεκτή εάν παραμείνουν τα συνολικά μοτίβα).
Υπάρχει επίσης το ζήτημα ότι το Wireshark λειτουργεί παθητικά. Αν και αυτό αποτελεί συνήθως πλεονέκτημα, σημαίνει ότι δεν μπορεί να προσομοιώσει διαδραστικά σενάρια από μόνο του (για παράδειγμα, δεν είναι δυνατόν να χρησιμοποιηθεί το Wireshark για να αιτηθεί δεδομένα από έναν διακομιστή – απαιτείται εξωτερική ενέργεια για τη δημιουργία αυτών των πακέτων). Επιπλέον, η ανάλυση κρυπτογραφημένης κίνησης, που είναι συχνή στα σύγχρονα δίκτυα, είναι περιορισμένη εκτός αν είναι διαθέσιμα τα αντίστοιχα κλειδιά.
Το Wireshark μπορεί να αποκρυπτογραφήσει ορισμένα πρωτόκολλα που δίνονται κλειδιά (όπως το TLS, αν υπάρχουν τα μυστικά της περιόδου λειτουργίας), αλλά συχνά, πολλές λεπτομέρειες του επιπέδου εφαρμογής κρύβονται στις συλλήψεις κρυπτογραφημένης κίνησης. Για τη δημιουργία κίνησης, μπορεί κανείς να καταλήξει να δημιουργεί κρυπτογραφημένες ροές που είναι στατιστικά παρόμοιες (μεγέθη πακέτων/χρονισμοί) χωρίς να χρειάζεται να αποκρυπτογραφηθούν στην ανάλυση.
Η δύναμη του Wireshark είναι η παροχή λεπτομερούς και ακριβούς αναπαράστασης της κυκλοφορίας , η οποία διασφαλίζει ότι οι προσπάθειες δημιουργίας κίνησης έχουν μια σταθερή αναφορά. Αυτό βελτιώνει σημαντικά την ποιότητα των σεναρίων δοκιμών, σε αντίθεση με τη χρήση αμιγώς συνθετικών ή εικασμένων μοτίβων κυκλοφορίας. Είναι επίσης ένα απαραίτητο εργαλείο εντοπισμού σφαλμάτων – εάν μια γεννήτρια κυκλοφορίας δεν προσεγγίζει το απαιτούμενο, το Wireshark θα αποκαλύψει την αλήθεια στο καλώδιο.

4.8.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Κατά τη χρήση του Wireshark ως μέρος μιας διαδικασίας δημιουργίας και ανάλυσης κίνησης, συνίστανται οι ακόλουθες βέλτιστες πρακτικές:

- Εστιασμένες λήψεις: Κατά τη συλλογή δεδομένων για σκοπούς επανάληψης ή ανάλυσης, κανείς θα μπορούσε να απομονώσει την κίνηση που την ενδιαφέρει. Για παράδειγμα, όταν

το ζητούμενο είναι μόνο η κυκλοφορία του πυρήνα 5G, η καταγραφή πραγματοποιείται στη διεπαφή που συνδέει τον πυρήνα με τον προσομοιωτή gNB, εφαρμόζοντας φίλτρο για τις IP διευθύνσεις του πυρήνα, ώστε να αποφεύγεται η άσχετη κίνηση. Αυτή η προσέγγιση μειώνει τον θόρυβο και το μέγεθος των αρχείων καταγραφής, διευκολύνοντας την περαιτέρω ανάλυση.

- Λήψη σε βασικά σημεία: Όταν προετοιμάζονται μοτίβα κυκλοφορίας, οι καταγραφές πραγματοποιούνται σε σημεία που έχουν σημασία για την ανάλυση. Η καταγραφή από την πλευρά του πελάτη και του διακομιστή μιας σύνδεσης βοηθά να φανεί πώς διαμορφώνεται η εισερχόμενη και εξερχόμενη κίνηση σε κάθε σύστημα και αν η συσκευή υπό δοκιμή τροποποιεί την κυκλοφορία. Σε ασύρματα δίκτυα, η καταγραφή over-the-air απαιτεί ειδικούς ανιχνευτές (sniffers), ενώ η συλλογή δεδομένων από την ενσύρματη πλευρά των σταθμών βάσης είναι πιο απλή και συχνά επαρκής.
- Χρήση πρόσθετων εργαλείων: Το Wireshark προσφέρει ισχυρές δυνατότητες ανάλυσης, αλλά για πιο απαιτητικές αναλύσεις δεδομένων, η εξαγωγή λεπτομερειών πακέτων ή η χρήση του tshark (της γραμμής εντολών του Wireshark) με σενάρια μπορεί να αυτοματοποιήσει τη διαδικασία. Για παράδειγμα, το tshark μπορεί να χρησιμοποιηθεί για την εξαγωγή όλων των χρόνων άφιξης και των μεγεθών πακέτων από ένα αρχείο PCAP, ώστε αυτά τα δεδομένα να αξιοποιηθούν για στατιστική ανάλυση ή για τη δημιουργία ρεαλιστικών traffic generators με βάση τις κατανομές που παρατηρήθηκαν.
- Αναπαραγωγιμότητα: Αποθηκεύονται τα αρχεία λήψης με σαφή ονομασία και τεκμηρίωση (τι σενάριο, ο χρόνος, οι συνθήκες που αντιπροσωπεύουν). Αυτό θα βοηθήσει κατά τη σύγκριση της παραγωγής παραγωγής κίνησης με την αρχική λήψη. Είναι σύνηθες ο έλεγχος έκδοσης μικρών PCAP που αντιπροσωπεύουν περιπτώσεις δοκιμής.
- Ανωνυμοποίηση: Σε περίπτωση συλλογής δεδομένων από πραγματικά δίκτυα, λαμβάνεται μέριμνα για την προστασία ευαίσθητων πληροφοριών, όπως διευθύνσεις IP και περιεχόμενο ωφέλιμου φορτίου. Εργαλεία όπως το Wireshark ή το editcap μπορούν να χρησιμοποιηθούν για την ανωνυμοποίηση των συλλήψεων, αφαιρώντας ωφέλιμα φορτία ή τυχαιοποιώντας τις διευθύνσεις IP, πριν αυτά τα αρχεία κοινοποιηθούν ή χρησιμοποιηθούν σε δημόσιο περιβάλλον. Με αυτόν τον τρόπο διασφαλίζεται το απόρρητο των δεδομένων, ενώ ταυτόχρονα διατηρείται η δυνατότητα αναπαραγωγής των traffic patterns.
- Επαλήθευση εξόδου γεννήτριας: Αφού δημιουργηθεί ένα δοκιμαστικό σενάριο από μια σύλληψη, η έξοδος της γεννήτριας κίνησης εξετάζεται σε στεγνή λειτουργία και συγκρίνεται με την αρχική λήψη, χρησιμοποιώντας το Wireshark ή αυτοματοποιημένα εργαλεία διαφοροποίησης. Ελέγχεται ότι τα βασικά χαρακτηριστικά, όπως η ακολουθία των μεγεθών πακέτων και τα μοτίβα πρωτοκόλλου, ευθυγραμμίζονται στενά με την αρχική καταγραφή. Αν και κάποιες διαφορές, όπως οι χρονικές σημάνσεις ή οι διευθύνσεις IP, είναι αναμενόμενες, η ροή των γεγονότων πρέπει να αντιστοιχεί. Αυτό το βήμα διασφαλίζει ότι η γεννήτρια κυκλοφορίας έχει ρυθμιστεί σωστά.

Με την ενσωμάτωση του Wireshark στη ροή εργασίας, διασφαλίζεται μια γειωμένη και αυστηρή προσέγγιση για την προσομοίωση της κυκλοφορίας δικτύου . Το Wireshark παρέχει τη σιγουριά ότι αυτό που δημιουργείται είναι αυτό που παρατηρήθηκε, συνδέοντας τις εμπειρικές μετρήσεις δικτύου με τις πειραματικές δοκιμές δικτύου. Εν ολίγοις, ενώ το Wireshark δεν δημιουργεί κίνηση, είναι ένας απαραίτητος σύντροφος στη διαδικασία δημιουργίας, διασφαλίζοντας ρεαλισμό και

βοηθώντας στη βαθιά ανάλυση για την ερμηνεία των αποτελεσμάτων και τον εντοπισμό σφαλμάτων.

4.9. Iperf3

Η αξιολόγηση της απόδοσης του δικτύου είναι ένας θεμελιώδης πυλώνας για την κατανόηση και τη βελτιστοποίηση της μετάδοσης δεδομένων σε σύγχρονα περιβάλλοντα. Σε αυτό το πλαίσιο, το Iperf3 έχει καθιερωθεί ως ένα από τα πιο αξιόπιστα εργαλεία, το οποίο εκτός από τη μέτρηση του εύρους ζώνης, μπορεί να λειτουργήσει και ως γεννήτρια κίνησης για πειραματικούς σκοπούς. Σε αυτή την ενότητα, παρουσιάζόνται οι βασικές λειτουργίες και η αρχιτεκτονική του Iperf3, καθώς και οι περιπτώσεις χρήσης του ως εργαλείου δημιουργίας κίνησης που στοχεύει στην αξιολόγηση της απόδοσης του δικτύου υπό διάφορες συνθήκες φορτίου. 45 46
Το Iperf3 είναι ένα εργαλείο ανοιχτού κώδικα που αναπτύχθηκε για τη μέτρηση της απόδοσης του δικτύου μέσω ενός μοντέλου πελάτη-διακομιστή. Παρόλο που η κύρια χρήση του είναι η μέτρηση της απόδοσης, η ικανότητά του να παράγει συνεχείς ροές δεδομένων το καθιστά ικανό να λειτουργεί ως μια απλή γεννήτρια κίνησης δικτύου. Σε περιβάλλοντα δοκιμών, το Iperf3 χρησιμοποιείται συνήθως για την προσομοίωση φορτίου, επιτρέποντας στους ερευνητές να αναλύσουν πώς λειτουργεί ένα δίκτυο υπό ελεγχόμενες συνθήκες και να εντοπίσουν πιθανά σημεία συμφόρησης ή προβλήματα απώλειας πακέτων.
Το Iperf3 λειτουργεί δημιουργώντας μία ή περισσότερες ροές δεδομένων από έναν πελάτη σε διακομιστή και μετρώντας τον ρυθμό μεταφοράς. Υποστηρίζει τόσο το TCP (για απόδοση με ενσωματωμένο έλεγχο συμφόρησης) όσο και το UDP (για τη δημιουργία κίνησης σε καθορισμένους ρυθμούς και τη μέτρηση της απώλειας πακέτων και του jitter). Αυτή η ευελιξία επιτρέπει στους χρήστες να μιμούνται διαφορετικούς τύπους κίνησης:

- Με τις ροές TCP, το Iperf3 μπορεί να προσομοιώσει μαζικές μεταφορές δεδομένων και να αποκαλύψει το μέγιστο εφικτό εύρος ζώνης καθώς και τον τρόπο με τον οποίο το δίκτυο χειρίζεται τη συμφόρηση.
- Με τις ροές UDP, το Iperf3 μπορεί να δημιουργήσει κίνηση με σταθερό ρυθμό, κάτι που είναι χρήσιμο για τον έλεγχο QoS ή τη συμπεριφορά του δικτύου υπό σταθερό φορτίο και μπορεί να αναφέρει απώλεια πακέτων και καθυστέρηση απόσπασης που είναι ζωτικής σημασίας για την ανάλυση της ποιότητας εμπειρίας.

4.9.1. Βασικά Στοιχεία και Αρχιτεκτονική

Το Iperf3 λειτουργεί σε μια απλή αρχιτεκτονική πελάτη-διακομιστή:

- Ένας κόμβος ορίζεται ως διακομιστής (χρησιμοποιώντας την εντολή `iperf3 -s`), ο οποίος περιμένει τις εισερχόμενες δοκιμαστικές συνδέσεις.
- Ένας άλλος κόμβος λειτουργεί ως πελάτης (`iperf3 -c <server_ip>`) και ξεκινά μια δοκιμαστική περίοδο λειτουργίας στον διακομιστή.

Κατά τη διάρκεια μιας δοκιμής, ο πελάτης στέλνει δεδομένα στον διακομιστή (ή αντίστροφα σε αντίστροφη λειτουργία) για μια καθορισμένη διάρκεια ή ποσότητα δεδομένων. Οι βασικές πτυχές της λειτουργίας του Iperf3 περιλαμβάνουν:

45 https://www.candelatech.com/cookbook/wifire/UE_Testing_Using_iperf_to_Generate_Traffic
46 https://iperf.fr/

- Μοτίβα κυκλοφορίας: Το εργαλείο μπορεί να διαμορφωθεί ώστε να στέλνει δεδομένα σε σταθερή ροή. Στη λειτουργία TCP, θα αποστέλλεται όσο γρήγορα το επιτρέπει το παράθυρο TCP και το δίκτυο (εκτός αν έχει οριστεί όριο ρυθμού). Στη λειτουργία UDP, ο χρήστης μπορεί να καθορίσει έναν στοχευόμενο ρυθμό bit (για παράδειγμα, 100 Mbps) και ο πελάτης θα προσπαθήσει να στείλει με αυτόν τον ρυθμό. Προσαρμόζοντας το μέγεθος και το χρονισμό του πακέτου, το Iperf3 προσεγγίζει την απαιτούμενη απόδοση.
- Διαμόρφωση παραμέτρων: Οι χρήστες μπορούν να ορίσουν διάφορες παραμέτρους, όπως τον αριθμό των παράλληλων ροών (επιλογή `-P` για πολλαπλές ταυτόχρονες συνδέσεις), τη διάρκεια της δοκιμής (επιλογή `-t`) και ρυθμίσεις ειδικές για το πρωτόκολλο (όπως εύρος ζώνης UDP `-b` ή μέγεθος παραθύρου TCP).
- Μετρικές που συλλέγονται: Για κάθε δοκιμή, το Iperf3 αναφέρει το επιτυγχανόμενο εύρος ζώνης και για το UDP, επίσης απώλεια πακέτων και jitter. Μπορεί να παράγει περιοδικές αναφορές (π.χ. κάθε δευτερόλεπτο) που είναι πολύ χρήσιμο για να δούμε πώς εξελίσσεται η απόδοση κατά τη διάρκεια της δοκιμής (για παράδειγμα, για να παρατηρήσουμε αργή εκκίνηση στο TCP ή να ανιχνεύσουμε πότε υπάρχει κορεσμός μιας σύνδεσης).

Η απλότητα του σχεδιασμού του Iperf3 (μονό νήμα ανά ροή, συν μερικά νήματα για αναφορά) διασφαλίζει ότι συνήθως περιορίζεται από το δίκτυο, όχι από τα δικά του γενικά έξοδα, ειδικά σε σύγχρονο υλικό.

Ως γεννήτρια κυκλοφορίας, το Iperf3 είναι "ανοιχτού βρόχου" σε λειτουργία UDP (δεν προσαρμόζεται στην ανάδραση δικτύου εκτός από τη μέτρηση των απωλειών) και "κλειστού βρόχου" σε λειτουργία TCP (προσαρμόζεται μέσω ελέγχου συμφόρησης TCP). Αυτό σημαίνει:

- Στη λειτουργία UDP, είναι εξαιρετικό για δοκιμές ακραίων καταστάσεων σε ένα συγκεκριμένο φορτίο, ανεξάρτητα από το αν το δίκτυο μπορεί να το χειριστεί - εάν το δίκτυο δεν μπορεί, η απώλεια πακέτων θα αυξηθεί (και το Iperf3 θα το αναφέρει).
- Στη λειτουργία TCP, είναι εξαιρετικό για την εύρεση της μέγιστης απόδοσης που μπορεί να προσφέρει μια διαδρομή δικτύου, καθώς θα προσπαθήσει να χρησιμοποιήσει όλη τη διαθέσιμη χωρητικότητα, υποστηριζόμενη από τους ίδιους τους αλγόριθμους του TCP (πράγμα που είναι ρεαλιστικό για το πώς λειτουργούν πραγματικές εφαρμογές όπως το FTP ή οι μαζικές μεταφορές).

Η αρχιτεκτονική του Iperf3 του επιτρέπει επίσης να υποστηρίζει δοκιμές πολλαπλών ροών όπως αναφέρθηκε, οι οποίες μπορούν να μιμηθούν πολλαπλές ροές (αν και δεν είναι πλήρως ανεξάρτητες όπως ξεχωριστές διεργασίες, δίνει μια πρόχειρη ιδέα για πολλαπλές ταυτόχρονες συνδέσεις).

4.9.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Το Iperf3 ως γεννήτρια κυκλοφορίας μπορεί να εφαρμοστεί σε διάφορα σενάρια:

- Συγκριτική αξιολόγηση εργαστηρίου: Σε ελεγχόμενα εργαστηριακά περιβάλλοντα, το Iperf3 χρησιμοποιείται για την προσομοίωση ροών δεδομένων για την αξιολόγηση των δυνατοτήτων διεκπεραίωσης συσκευών ή συνδέσμων δικτύου. Για παράδειγμα, στη δοκιμή ενός νέου δρομολογητή Wi-Fi 6, ένας μηχανικός μπορεί να εκτελέσει το Iperf3 από έναν ενσύρματο πελάτη σε έναν ενσύρματο διακομιστή μέσω του δρομολογητή για να μετρήσει πόση απόδοση μπορεί να χειριστεί ο δρομολογητής τη δρομολόγηση ή το NATing.
- Παρακολούθηση Δικτύου Παραγωγής: Σε λειτουργικά δίκτυα, το Iperf3 μπορεί να προγραμματιστεί να εκτελείται μεταξύ κρίσιμων τελικών σημείων για την παρακολούθηση

της απόδοσης (αν και χρειάζεται προσοχή ώστε να απομονωθεί από την κίνηση των χρηστών). Μπορεί να βοηθήσει στον εντοπισμό εάν το δίκτυο μπορεί να διατηρήσει την απαιτούμενη απόδοση ή εάν υπάρχουν προβλήματα (όπως αύξηση της απώλειας πακέτων) που πιθανώς υποδεικνύουν ζητήματα όπως αποτυχία σύνδεσης ή συμφόρηση.

- Έρευνα σχετικά με τα πρωτόκολλα: Οι ερευνητές μπορούν να χρησιμοποιήσουν το Iperf3 για να δημιουργήσουν κίνηση με ορισμένα χαρακτηριστικά για να δοκιμάσουν νέες ιδέες πρωτοκόλλων. Για παράδειγμα, για να δοκιμάσουν έναν νέο αλγόριθμο ελέγχου συμφόρησης που εφαρμόζεται σε μια προσαρμοσμένη στοίβα TCP, θα μπορούσαν να εκτελέσουν το Iperf3 πάνω από αυτό το TCP για να δουν πώς αποδίδει σε σχέση με το τυπικό TCP.
- Δοκιμή δικτύου 5G: Σε μια κλίνη δοκιμών 5G, το Iperf3 θα μπορούσε να χρησιμοποιηθεί για τη δημιουργία κίνησης επιπέδου χρήστη από μια προσομοίωση UE μέσω του πυρήνα 5G σε ένα δίκτυο δεδομένων. Είναι απλό στη χρήση και τα αποτελέσματά του (διακίνηση, απώλεια πακέτων) ερμηνεύονται εύκολα στο πλαίσιο της επαλήθευσης ποιότητας της υπηρεσίας 5G.

4.9.3. Πλεονεκτήματα και προκλήσεις

Ένα βασικό πλεονέκτημα του Iperf3 είναι η απλότητα και η ακρίβειά του στη μέτρηση. Το εργαλείο είναι εύκολο στη χρήση και παρέχει μετρήσεις υψηλής ακρίβειας για την απόδοση, καθιστώντας το ένα * δημοφιλές εργαλείο μέτρησης απόδοσης δικτύου ανοιχτού κώδικα47. Η ευελιξία προσαρμογής παραμέτρων (όπως παράλληλες ροές, ρυθμοί UDP κ.λπ.) επιτρέπει στους χρήστες να προσαρμόζουν την κίνηση στις ανάγκες δοκιμών τους, είτε θέλουν να ωθήσουν ένα δίκτυο στα όριά του είτε να μιμηθούν ένα μέτριο φορτίο με συγκεκριμένα χαρακτηριστικά . Η έξοδος του Iperf3 είναι εξαιρετικά ακριβής, αναφέροντας όχι μόνο το συνολικό εύρος ζώνης, αλλά και λεπτομέρειες όπως απώλεια πακέτων και jitter για δοκιμές UDP, ενώ παρέχει ακόμη και έξοδο JSON για εύκολη ανάλυση σε αυτοματοποιημένη ανάλυση.
Ωστόσο, το Iperf3 είναι περιορισμένο σε εύρος : δημιουργεί κυρίως συνεχή κίνηση CBR (σταθερό ρυθμό μετάδοσης bit) ή μαζικές ροές TCP – δεν μιμείται πρωτόκολλα επιπέδου εφαρμογής πέρα από τη γενική μαζική μεταφορά. Αυτό σημαίνει ότι δεν είναι κατάλληλο για τη δημιουργία πολύπλοκων μοτίβων κίνησης (όπως μια συνεδρία περιήγησης στον ιστό με χρόνους σκέψης ή συνδυασμός διαφορετικών πρωτοκόλλων εφαρμογών) πέρα από αυτό που μπορούν να προσεγγίσουν πολλαπλές παρουσίες Iperf. Μια άλλη πρόκληση είναι ότι στη λειτουργία TCP, τα αποτελέσματα του Iperf3 επηρεάζονται από τον έλεγχο συμφόρησης TCP που χρησιμοποιείται. Εάν ο στόχος είναι η δοκιμή του δίκτυου, αυτό είναι εντάξει, αλλά εάν το DUT είναι κάτι σαν διαμορφωτής κίνησης, οι ιδιαιτερότητες του αλγόριθμου TCP θα μπορούσαν να επηρεάσουν το αποτέλεσμα. Στη λειτουργία UDP, πρέπει να διασφαλίζεται ότι δεν υπερφορτώνεται η CPU του αποστολέα ή το δίκτυο, καθώς το Iperf3 στέλνει απλώς με τον καθορισμένο ρυθμό και μπορεί να προκύψει υψηλή απώλεια πακέτων – γεγονός που παρέχει χρήσιμες πληροφορίες, αλλά απαιτεί σωστή ερμηνεία (π.χ. απώλεια 50% σημαίνει ότι ο ζητούμενος ρυθμός ξεπερνά τις δυνατότητες του δικτύου). Επιπλέον, αν και το Iperf3 μπορεί να δημιουργήσει πολλές παράλληλες ροές, δεν

47 iperf.fr

αποτελεί πλήρη προσομοιωτή εφαρμογών, αφού όλες οι ροές λειτουργούν με τον ίδιο τρόπο (είτε TCP είτε UDP) και δεν δημιουργείται μείγμα διαφορετικών πρωτοκόλλων ή συμπεριφορών χρήστη. Παρά τους περιορισμούς αυτούς, το Iperf3 παραμένει εξαιρετικά αποτελεσματικό για τον κορεσμό συνδέσμων και τη μέτρηση απόδοσης, με την ακρίβεια και την ευκολία χρήσης του να το καθιστούν βασικό εργαλείο για πειραματισμούς δικτύου.

4.9.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Όταν χρησιμοποιείται ο Iperf3 ως παράγοντας δημιουργίας κίνησης για την αξιολόγηση της απόδοσης, μερικές πρακτικές εξασφαλίζουν ουσιαστικά αποτελέσματα:

- Απομόνωση της δοκιμής: Οι δοκιμές με Iperf3 εκτελούνται σε απομονωμένο δίκτυο ή κατά τη διάρκεια περιόδων χαμηλής δραστηριότητας, ώστε η μετρούμενη απόδοση να μην επηρεάζεται από άλλη κίνηση. Εάν αυτό δεν είναι εφικτό, εφαρμόζεται φιλτράρισμα για να διασφαλιστεί ότι η επισκεψιμότητα του Iperf διαχωρίζεται από την κίνηση στο παρασκήνιο κατά την ανάλυση των αποτελεσμάτων.
- Τοποθέτηση διακομιστή: Ο διακομιστής Iperf3 τοποθετείται όσο το δυνατόν πιο κοντά στη συσκευή υπό δοκιμή από πλευράς δικτύου, ώστε να ελαχιστοποιούνται τα άσχετα σημεία συμφόρησης. Για παράδειγμα, κατά τη δοκιμή ενός δρομολογητή, ο διακομιστής Iperf3 εκτελείται σε έναν υπολογιστή που είναι απευθείας συνδεδεμένος στη θύρα εξόδου του δρομολογητή, αποφεύγοντας τα περιττά ενδιάμεσα άλματα.
- Διάρκεια και επανάληψη: Χρησιμοποιούνται επαρκώς μεγάλες διάρκειες δοκιμής (π.χ. με την επιλογή -t για 30+ δευτερόλεπτα) ώστε να δοθεί χρόνος στο TCP να αυξήσει τη ροή και να μετρηθούν βραχυπρόθεσμες διακυμάνσεις. Πραγματοποιούνται πολλαπλές επαναλήψεις των δοκιμών και η έξοδος --json αξιοποιείται για την προγραμματιστική καταγραφή των αποτελεσμάτων. Ο μέσος όρος των αποτελεσμάτων σε διαφορετικές διαδρομές ή η ανάλυση της καλύτερης περίπτωσης (σε δοκιμές μέγιστης χωρητικότητας) ενισχύουν την αξιοπιστία των μετρήσεων, ενώ η προσοχή στις αναφορές διαστήματος βοηθά στην αξιολόγηση της σταθερότητας του δικτύου κατά τη διάρκεια της δοκιμής.
- Σάρωση ρυθμού UDP: Όταν χρησιμοποιείται η λειτουργία UDP για την εκτίμηση της χωρητικότητας του δικτύου, πραγματοποιείται σάρωση ρυθμών. Η διαδικασία ξεκινά με χαμηλό ρυθμό μετάδοσης και σταδιακά αυξάνεται η παράμετρος -b μέχρι να παρατηρηθεί σημαντική απώλεια πακέτων. Αυτό επιτρέπει τον προσδιορισμό του εύρους ζώνης στο οποίο το δίκτυο αρχίζει να απορρίπτει πακέτα, προσφέροντας μια απλή εκτίμηση της διαθέσιμης χωρητικότητας. Στο σημείο καμπής, εξετάζονται το jitter και η απώλεια πακέτων – ένα δίκτυο με καλή απόδοση θα πρέπει να παρουσιάζει χαμηλό jitter και μηδενικές απώλειες έως ότου προσεγγιστεί το όριο της χωρητικότητας.
- Παρακολούθηση CPU και NIC: Επιβεβαιώνεται ότι τόσο ο υπολογιστής-πελάτης όσο και ο διακομιστής Iperf3 δεν αντιμετωπίζουν περιορισμούς από την CPU. Ένα ενδεικτικό σύμπτωμα περιορισμού της CPU είναι όταν ο ρυθμός αποστολής που αναφέρεται από τον πελάτη είναι σημαντικά χαμηλότερος από την αναμενόμενη χωρητικότητα της σύνδεσης, ενώ η CPU λειτουργεί στο 100%. Η παρακολούθηση των πόρων του συστήματος ή η εκτέλεση του Iperf3 με μία έναντι πολλαπλών ροών μπορεί να αποκαλύψει αν το σημείο συμφόρησης είναι η ίδια η γεννήτρια κυκλοφορίας. Εφαρμόζεται το κατάλληλο καρφίτσωμα CPU ή διακόπτονται άλλες διεργασίες εφόσον είναι απαραίτητο.

- Κατανόηση της δυναμικής του TCP: Κατά την ερμηνεία των αποτελεσμάτων των δοκιμών TCP, λαμβάνεται υπόψη ότι το πρωτόκολλο TCP εξερευνά το διαθέσιμο εύρος ζώνης. Εάν η δοκιμή εκτελείται σε διαδρομή με υψηλή καθυστέρηση (μεγάλο RTT), η αύξηση του ρυθμού μετάδοσης μπορεί να είναι πιο αργή και η επιτευχθείσα απόδοση σε μια σύντομη δοκιμή ενδέχεται να μην αντανακλά πλήρως τις πραγματικές δυνατότητες της σύνδεσης. Σε τέτοιες περιπτώσεις, είτε παρατείνεται η διάρκεια της δοκιμής είτε εξετάζεται η ρύθμιση παραμέτρων, όπως το αρχικό παράθυρο συμφόρησης ή το μέγεθος του παραθύρου (μέσω των επιλογών -O ή -w).

Ακολουθώντας αυτές τις οδηγίες, το Iperf3 μπορεί να χρησιμεύσει ως πολύτιμος παράγοντας κίνησης για τη δημιουργία επαναλαμβανόμενου και ελεγχόμενου φορτίου σε ένα δίκτυο, επιτρέποντας σε ερευνητές και μηχανικούς να μετρούν την απόδοση, να εντοπίζουν προβλήματα και να επικυρώνουν βελτιώσεις. Αν και δεν είναι τόσο πλούσιος σε χαρακτηριστικά όσο οι εξειδικευμένοι προσομοιωτές κυκλοφορίας, η αξιοπιστία και η ευκολία ανάπτυξής του καθιστούν το Iperf3 ένα κοινό σημείο εκκίνησης για τη δοκιμή απόδοσης δικτύου και μια αναφορά με την οποία μπορούν να συγκριθούν πιο περίπλοκα μοτίβα κυκλοφορίας.

4.10. Το Scapy Toolkit

Η συνεχής ανάγκη για ανάλυση χαμηλού επιπέδου και έλεγχο των πρωτοκόλλων δικτύου έχει οδηγήσει στην ανάπτυξη εργαλείων που όχι μόνο επιτρέπουν την ανάλυση της κυκλοφορίας αλλά και την ενεργή δημιουργία, τροποποίηση και έγχυση κίνησης . Το Scapy είναι ένα από τα πιο ισχυρά και ευέλικτα εργαλεία ανοιχτού κώδικα σε αυτόν τον τομέα, γνωστό για την ικανότητά του να δημιουργεί, να τροποποιεί και να στέλνει πακέτα σε ένα ευρύ φάσμα πρωτοκόλλων. Ενώ κατά κύριο λόγο είναι μια βιβλιοθήκη δημιουργίας και χειρισμού πακέτων, το Scapy έχει τη δυνατότητα να λειτουργεί ως γεννήτρια κυκλοφορίας επιτρέποντας σε ερευνητές και επαγγελματίες να γράψουν σενάρια για τη δημιουργία αυθαίρετων ακολουθιών πακέτων. Σε αυτήν την ενότητα, συζητάμε τα χαρακτηριστικά, την αρχιτεκτονική και τη χρήση του Scapy ως εργαλείο δημιουργίας κίνησης για προσαρμοσμένα σενάρια.48

Το Scapy είναι ένα διαδραστικό πρόγραμμα χειρισμού πακέτων που βασίζεται σε Python και βιβλιοθήκη49 . Επιτρέπει στους χρήστες να πλαστογραφούν ή να αποκωδικοποιούν πακέτα μεγάλου αριθμού πρωτοκόλλων, να τα στέλνουν στο καλώδιο, να τα καταγράφουν και να ταιριάζουν αιτήματα και απαντήσεις διαδραστικά[54]. Ουσιαστικά, το Scapy δίνει σε κάποιον την ελευθερία να δημιουργήσει οποιοδήποτε είδος πακέτου (από Ethernet έως IP έως TCP/UDP έως πρωτόκολλα εφαρμογών) και να το εκπέμψει, καθώς και αποκρίσεις sniff. Αυτό καθιστά δυνατή τη δημιουργία κίνησης που είναι προσαρμοσμένη σε πολύ συγκεκριμένες ανάγκες – από κανονική συμπεριφορά πρωτοκόλλου έως κακοσχηματισμένα πακέτα για δοκιμή ευρωστίας.

4.10.1. Βασικά Στοιχεία και Αρχιτεκτονική

Η αρχιτεκτονική του Scapy επικεντρώνεται στην ευελιξία και τον έλεγχο του χρήστη:50

- Παρέχει μια βιβλιοθήκη κλάσεων πρωτοκόλλου (για παράδειγμα, IP , TCP , UDP , DNS , κ.λπ.) οι οποίες μπορούν να στρωθούν για την κατασκευή πακέτων. Κάθε επίπεδο έχει πεδία που

48 https://scapy.net/

49 https://github.com/secdev/scapy

50 https://scapy.net/talks/scapy_csw05.pdf

μπορούν να οριστούν ή να αφεθούν ως προεπιλογή. Για παράδειγμα, μπορεί κανείς να δημιουργήσει ένα πακέτο IP με ip=IP(dst="10.0.0.1") και στη συνέχεια να προσθέσει ένα επίπεδο UDP με udp=UDP(dport=53) και τέλος ένα ωφέλιμο φορτίο, κατασκευάζοντας ένα πακέτο αιτήματος DNS σε λίγες γραμμές κώδικα.

- Το Scapy μπορεί να στείλει πακέτα μέσω διεπαφών δικτύου χρησιμοποιώντας ακατέργαστες υποδοχές. Μπορεί επίσης να λαμβάνει πακέτα , είτε φιλτράροντας για συγκεκριμένα κριτήρια είτε μυρίζοντας τα πάντα, κάτι που του επιτρέπει να επαληθεύει την επίδραση των πακέτων που στέλνει (π.χ. ανταποκρίθηκε ο στόχος με ένα TCP RST; Επιστράφηκε σφάλμα ICMP;).
- Επειδή εκτελείται σε Python, το Scapy μπορεί να αξιοποιήσει όλη τη λογική και τις βιβλιοθήκες της Python. Αυτό σημαίνει ότι οι χρήστες μπορούν να γράψουν βρόχους, συνθήκες και ακόμη και να ενσωματώσουν το Scapy με άλλα εργαλεία (π.χ. ανάγνωση διευθύνσεων από ένα αρχείο, δημιουργία πακέτων και μετά καταγραφή αποτελεσμάτων σε μια βάση δεδομένων) απρόσκοπτα.

Το πιο σημαντικό είναι ότι το Scapy λειτουργεί στο επίπεδο 2 και πάνω , που σημαίνει ότι μπορεί να δημιουργήσει πλαίσια Ethernet και οτιδήποτε υπάρχει μέσα σε αυτά. Χρησιμοποιεί μηχανισμούς λειτουργικού συστήματος για την αποστολή ακατέργαστων πλαισίων (που μπορεί να απαιτούν δικαιώματα root). Κατά τη λήψη, μπορεί να χρησιμοποιήσει το pcap ή το socket sniffing παρόμοια με το Wireshark, αλλά παρουσιάζει τα συλλεγμένα πακέτα ως αντικείμενα πακέτων Scapy για εύκολο χειρισμό ή ανάλυση στην Python.

Μία από τις πιο ισχυρές πτυχές είναι ότι το Scapy μπορεί να δημιουργήσει πακέτα που μπορεί να είναι δύσκολο να παραχθούν με τυπικά εργαλεία – για παράδειγμα:

- Εσκεμμένη αποστολή ενός πακέτου με λάθος άθροισμα ελέγχου ή με ασυνήθιστους συνδυασμούς σημαιών.
- Κατασκευή ενός μη τυπικού πρωτοκόλλου ή ενός νέου πρωτοκόλλου που δεν υποστηρίζεται ακόμη από άλλα εργαλεία, απλώς ορίζοντας τα πεδία στο Scapy.
- Δημιουργία ακολουθιών πακέτων (π.χ. χειραψία TCP με προσαρμοσμένο χρονισμό) με μη αυτόματο τρόπο.

Όσον αφορά τη δημιουργία κίνησης, το Scapy δεν έχει σχεδιαστεί για δημιουργία φορτίου μεγάλου όγκου όπως το TRex ή το Iperf, αλλά μάλλον για τη δημιουργία προσαρμοσμένων πακέτων . Λάμπει σε σενάρια όπως η αποστολή ριπής ενός συγκεκριμένου τύπου πακέτου, η ασαφής υλοποίηση πρωτοκόλλων στέλνοντας παραλλαγές της αναμενόμενης κίνησης ή η αναπαραγωγή μιας δύσκολης ακολουθίας πακέτων που προκάλεσαν σφάλμα σε ένα σύστημα.

4.10.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Το Scapy, ως γεννήτρια κυκλοφορίας, χρησιμοποιείται σε μια πληθώρα εφαρμογών που απαιτούν λεπτό έλεγχο:

- Δοκιμές ασφαλείας και εκμεταλλεύσεις: Το Scapy χρησιμοποιείται ευρέως για την προσομοίωση ή την πραγματοποίηση επιθέσεων δικτύου με ελεγχόμενο τρόπο για τη δοκιμή συστημάτων ανίχνευσης εισβολής ή της ευρωστίας των στοίβων. Για παράδειγμα, ένας ερευνητής μπορεί να χρησιμοποιήσει το Scapy για να δημιουργήσει μια σειρά από πακέτα TCP με ασυνήθιστες σημαίες για να ελέγξει εάν ένα τείχος προστασίας τα χειρίζεται σωστά ή για να προσομοιώσει μια πλημμύρα SYN με προσαρμοσμένες επιλογές IP για να δει εάν ενεργοποιείται ένα IDS. Επειδή το Scapy επιτρέπει τον χειροκίνητο έλεγχο των αριθμών ακολουθίας και επιβεβαίωσης, μπορεί να χρησιμοποιηθεί για τη

μίμηση πτυχών της παραβίασης του TCP ή για τον έλεγχο του τρόπου με τον οποίο τα συστήματα ανταποκρίνονται σε τμήματα εκτός σειράς ή διπλότυπα.

- Πρωτόκολλο Fuzzing: Μεταβάλλοντας προγραμματικά τα πεδία πακέτων (όπως η ανατροπή bits, η δοκιμή τυχαίων τιμών στις κεφαλίδες, κ.λπ.), το Scapy μπορεί να δημιουργήσει ημι-τυχαιοποιημένη κυκλοφορία για να δοκιμάζει fuzz υλοποιήσεις πρωτοκόλλου δικτύου. Για παράδειγμα, κάποιος θα μπορούσε να θολώσει έναν διακομιστή DNS στέλνοντας ερωτήματα DNS με τυχαία κατεστραμμένα πεδία κεφαλίδας για να διασφαλιστεί ότι δεν θα διακοπεί σε απροσδόκητη είσοδο.
- Ανάπτυξη νέων πρωτοκόλλων: Για πειραματικά πρωτόκολλα που δεν έχουν ακόμη εφαρμοστεί ευρέως, το Scapy μπορεί να είναι ανεκτίμητο. Οι ερευνητές που σχεδιάζουν ένα νέο πρωτόκολλο δικτύου (ή μια νέα επιλογή για ένα υπάρχον πρωτόκολλο) μπορούν να χρησιμοποιήσουν το Scapy για να εισάγουν δοκιμαστικά πακέτα που υλοποιούν τη νέα μορφή σε ένα δίκτυο και να παρατηρούν τη συμπεριφορά, χωρίς να χρειάζεται να γράψουν μια πλήρη υλοποίηση C. Η δέσμη ενεργειών Python του Scapy καθιστά γρήγορη την επανάληψη σε μορφές πακέτων.
- Σάρωση και απαρίθμηση δικτύου: Παρόμοια με το Nmap (αν και όχι τόσο αυτοματοποιημένο ή αποτελεσματικό), το Scapy μπορεί να χρησιμοποιηθεί για τη δημιουργία προσαρμοσμένων εργαλείων σάρωσης. Για παράδειγμα, αποστολή ενός TCP SYN σε μια θύρα και ανάλυση της απόκρισης (SYN+ACK ή RST) για να προσδιοριστεί εάν η θύρα είναι ανοιχτή. Το Scapy δεν θα αντικαταστήσει τους εξειδικευμένους σαρωτές για σάρωση μεγάλης κλίμακας, αλλά για έναν ερευνητή που θέλει μια πολύ συγκεκριμένη τεχνική σάρωσης (π.χ. σάρωση χειραψίας TCP ή προσαρμοσμένη παραλλαγή σάρωσης ACK), το Scapy παρέχει τα δομικά στοιχεία για την υλοποίησή της.
- Εκπαίδευση και εντοπισμός σφαλμάτων: Κατά τη διδασκαλία της δικτύωσης, το Scapy παρέχει έναν πρακτικό τρόπο για να απεικονίσει πώς λειτουργούν τα πρωτόκολλα. Οι μαθητές μπορούν να δημιουργήσουν πακέτα από την αρχή και να δουν τις απαντήσεις. Ομοίως, κατά τον εντοπισμό σφαλμάτων ενός προβλήματος δικτύου, εάν κάποιος υποπτεύεται ότι ένα συγκεκριμένο πακέτο με κακή μορφή προκαλεί πρόβλημα, το Scapy μπορεί να αναδημιουργήσει αυτό το πακέτο για να ελέγξει την υπόθεση μεμονωμένα.

Συνοπτικά, το Scapy είναι σαν ένα ελβετικό μαχαίρι για πακέτα δικτύου – αν χρειάζεται ένα πακέτο συγκεκριμένου είδους, το Scapy μπορεί πιθανότατα να το δημιουργήσει. Αυτό το καθιστά αγαπημένο στα εργαστήρια έρευνας δικτύου και μεταξύ των επαγγελματιών ασφάλειας που απαιτούν προσαρμοσμένη δημιουργία κίνησης που άλλα εργαλεία δεν μπορούν να κάνουν.

4.10.3. Πλεονεκτήματα και Προκλήσεις

Πλεονεκτήματα: Το μεγαλύτερο πλεονέκτημα του Scapy είναι η απαράμιλλη ευελιξία του . Προσφέρει λεπτομερή έλεγχο σχεδόν σε κάθε bit ενός πακέτου, τον οποίο λίγα άλλα εργαλεία παρέχουν με τόσο προσιτό τρόπο. Όντας ένα διαδραστικό εργαλείο (μέσω μιας προτροπής Python ή σεναρίων), μπορεί κανείς να πρωτοτυπήσει γρήγορα τις αλληλεπιδράσεις δικτύου. Για παράδειγμα, ο έλεγχος του τρόπου με τον οποίο ένας διακομιστής αποκρίνεται εάν έχει οριστεί μια συγκεκριμένη σημαία μπορεί να γίνει με μία γραμμή για αποστολή και μία γραμμή για να μυριστεί η απάντηση. Ένα άλλο πλεονέκτημα είναι ότι το Scapy είναι επεκτάσιμο . Εάν ένα πρωτόκολλο δεν υποστηρίζεται εκτός συσκευασίας, οι χρήστες μπορούν να ορίσουν νέα επίπεδα πρωτοκόλλου στην Python (υπάρχουν πολλές επεκτάσεις Scapy που συνεισφέρονται από την κοινότητα για ιδιόκτητα ή νέα πρωτόκολλα). Αυτό οδήγησε στην ευρεία χρήση του Scapy τόσο

στον ακαδημαϊκό χώρο όσο και στη βιομηχανία για πειράματα δικτύου51 (για παράδειγμα, αναφέρεται συνήθως σε ερευνητικές εργασίες για τη δημιουργία προσαρμοσμένων πακέτων σε δοκιμαστικές κλίνες).
Η βάση Python του Scapy σημαίνει ότι μπορεί να ενσωματωθεί με άλλα εργαλεία ανάλυσης, επιτρέποντας σε ένα σενάριο να δημιουργεί κίνηση, να περιμένει μια απάντηση και στη συνέχεια να λαμβάνει αποφάσεις (π.χ. μια μορφή προσαρμοστικής δημιουργίας ή σάρωσης κυκλοφορίας). Αυτό είναι κάτι που τα εργαλεία στατικής κυκλοφορίας δεν μπορούν να κάνουν εύκολα.
Προκλήσεις: Η δύναμη του Scapy συνοδεύεται από την προειδοποίηση ότι δεν έχει βελτιστοποιηθεί για τον όγκο της κυκλοφορίας ή την ταχύτητα . Εκτελείται στο χώρο χρήστη για κάθε πακέτο και στην Python (η οποία δεν είναι η ταχύτερη γλώσσα για εργασίες που συνδέονται με την CPU). Αυτό σημαίνει ότι το Scapy δεν είναι κατάλληλο για τη δημιουργία υψηλής απόδοσης για εκτεταμένες περιόδους – π.χ. θα δυσκολευόταν να στείλει συνεχώς gigabit κίνησης. Εάν ο στόχος είναι η απόδοση του stress test, το Scapy είναι το λάθος εργαλείο, αλλά αν ο στόχος είναι η αποστολή εκατομμυρίων διαφορετικών μικροσκοπικών πακέτων το καθένα με μικρές παραλλαγές (fuzzing), το Scapy μπορεί να το κάνει αλλά για μεγαλύτερο χρονικό διάστημα. Μια άλλη πρόκληση είναι ότι η αποτελεσματική χρήση του Scapy απαιτεί γνώση των πρωτοκόλλων δικτύωσης. Σε αντίθεση με τα εργαλεία υψηλού επιπέδου που κρύβουν λεπτομέρειες, το Scapy εκθέτει όλες τις λεπτομέρειες. Αυτό μπορεί να οδηγήσει σε σφάλμα χρήστη (για παράδειγμα, να ξεχάσει να υπολογίσει ένα άθροισμα ελέγχου – αν και το Scapy θα το κάνει αυτόματα, εκτός εάν δοθεί διαφορετική οδηγία – ή σε λάθος ταξινόμηση των επιπέδων πρωτοκόλλου). Η ακατάλληλη χρήση μπορεί να οδηγήσει σε πακέτα που δεν λαμβάνουν ποτέ απόκριση (επειδή είχαν λανθασμένη μορφή), κάτι που θα μπορούσε να προκαλέσει σύγχυση αν δεν γνωρίζει κανείς εάν η έλλειψη απόκρισης οφείλεται σε συμπεριφορά δικτύου ή σε λάθος στη δημιουργία πακέτων.
Η δημιουργία πολύπλοκων διαλόγων πολλαπλών πακέτων (όπως μια πλήρης σύνδεση TCP με προσαρμοσμένη λογική) στο Scapy μπορεί να είναι ιδιαίτερα απαιτητική, καθώς συχνά απαιτεί την υλοποίηση τμημάτων του μηχανισμού κατάστασης του πρωτοκόλλου μέσα στο σενάριο. Για εκτεταμένες εργασίες αυτού του είδους, αυτό μπορεί να ισοδυναμεί με την επαναδημιουργία μιας μίνι στοίβας δικτύου. Υπάρχουν βοηθητικά εργαλεία του Scapy, όπως το automaton, που διευκολύνουν τη διαχείριση καταστάσεων, αλλά η διαδικασία παραμένει απαιτητική ως προς τον προγραμματισμό. Επιπλέον, λόγω της χαμηλού επιπέδου πρόσβασης που παρέχει το Scapy, υπάρχει η δυνατότητα δημιουργίας κυκλοφορίας που μπορεί να διαταράξει τα δίκτυα αν δεν υπάρξει προσοχή (π.χ. πλαστογράφηση διευθύνσεων ή αποστολή αντικρουόμενων μηνυμάτων ARP). Γι' αυτό, η χρήση του Scapy σε παραγωγικά δίκτυα πρέπει να γίνεται με προσοχή και, κατά προτίμηση, να περιορίζεται σε απομονωμένα δοκιμαστικά περιβάλλοντα ή να χρησιμοποιούνται μη παρεμβατικά πακέτα.

4.10.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Για την αποτελεσματική χρήση του Scapy ως γεννήτριας κυκλοφορίας σε πειράματα, συνιστώνται οι εξής πρακτικές:

- Δημιουργία πακέτων σταδιακά: Κατά τη δημιουργία πακέτων με το Scapy, προτείνεται να κατασκευάζονται βήμα προς βήμα, επίπεδο προς στρώμα, και να χρησιμοποιείται η μέθοδος show() για να επιθεωρούνται οι τιμές των πεδίων και οι προεπιλογές πριν την αποστολή. Με αυτόν τον τρόπο, διασφαλίζεται ότι ο χρήστης γνωρίζει ακριβώς τι θα

51 open5g.info

αποσταλεί στο δίκτυο. Αν και το Scapy υπολογίζει αυτόματα ορισμένα πεδία, όπως μήκη και αθροίσματα ελέγχου, είναι σημαντικό σε περίπτωση παράκαμψης αυτών να γίνεται επιπλέον έλεγχος για την ορθότητά τους.

- Δοκιμή σε ασφαλές περιβάλλον: Δεδομένου ότι το Scapy έχει τη δυνατότητα αποστολής αυθαίρετων πακέτων, συστήνεται τα σενάρια που υλοποιούνται με αυτό να δοκιμάζονται πάντα πρώτα σε ελεγχόμενο περιβάλλον, όπως σε δοκιμαστικό διακόπτη ή σε εικονική μηχανή (VM), πριν χρησιμοποιηθούν σε πραγματικές συσκευές δικτύου. Αυτή η προσέγγιση αποτρέπει τυχόν απρόβλεπτες διακοπές, όπως η αποστολή πλαστών απαντήσεων ARP ή η λανθασμένη διαμόρφωση πακέτων, που θα μπορούσαν να προκαλέσουν προβλήματα στην υποδομή του δικτύου. Ενώ τέτοιες δοκιμές είναι αποδεκτές σε εργαστηριακό περιβάλλον, η εφαρμογή τους σε παραγωγικά δίκτυα μπορεί να είναι επιζήμια.
- Leverage Sniffing: Η αποστολή πακέτων και η παρακολούθηση της κυκλοφορίας (sniffing) συνδυάζονται στο Scapy για να επαληθευτεί ότι η κυκλοφορία συμπεριφέρεται όπως αναμένεται. Για παράδειγμα, κατά την αποστολή ενός προσαρμοσμένου πακέτου SYN, χρησιμοποιείται η συνάρτηση Sniff() του Scapy για να καταγραφεί η αντίστοιχη απάντηση SYN-ACK. Επιπλέον, μπορεί να εφαρμοστεί φίλτρο στο sniff() ώστε να εντοπίζονται μόνο τα πακέτα ενδιαφέροντος (όπως filter="tcp και src host 10.0.0.1" για απαντήσεις από συγκεκριμένο κεντρικό υπολογιστή). Αυτή η άμεση ανατροφοδότηση διευκολύνει την προσαρμογή της κυκλοφορίας σε πραγματικό χρόνο.
- Αυτοματισμός και βρόχοι: Αξιοποιούνται οι δυνατότητες της Python κατά τη χρήση του Scapy, έτσι ώστε αν απαιτείται η αποστολή, για παράδειγμα, 100 πακέτων με διαφορετικές διευθύνσεις IP, να χρησιμοποιείται βρόχος αντί για 100 χειροκίνητες εντολές. Παράλληλα, εφαρμόζονται συνθήκες που καθορίζουν πότε θα σταματήσει η αποστολή (όπως η διακοπή μόλις παρατηρηθεί μια συγκεκριμένη απόκριση). Αυτή η πρακτική αποτρέπει την άσκοπη υπερφόρτωση του στόχου και επιτρέπει τον προγραμματισμό του εργαλείου ώστε να σταματάει όταν επιτευχθεί ο επιθυμητός στόχος.
- Παράμετρος απόδοσης: Όταν απαιτείται η αποστολή μεγάλου αριθμού πακέτων με το Scapy, χρησιμοποιούνται οι σχετικές συναρτήσεις αποστολής με την παράμετρο inter=, ώστε να καθοριστεί το χρονικό διάστημα μεταξύ των πακέτων. Αυτό επιτρέπει τη ρύθμιση του ρυθμού αποστολής σε επίπεδο που το σύστημα μπορεί να διαχειριστεί αξιόπιστα. Σε περιπτώσεις που απαιτείται μέγιστη ταχύτητα, το Scapy αποστέλλει πακέτα όσο πιο γρήγορα μπορεί – κάτι που σε ισχυρούς υπολογιστές μπορεί να φτάσει σε χιλιάδες πακέτα ανά δευτερόλεπτο για απλά πακέτα. Η χρήση της CPU παρακολουθείται στενά και, εάν χρειαστεί μεγαλύτερη ταχύτητα, μπορεί να χρησιμοποιηθεί η συνάρτηση sendpfast (που αξιοποιεί το libpcap για ταχύτερη αποστολή), με το κόστος όμως της μειωμένης ευελιξίας.
- Συνδυασμός με άλλα εργαλεία: Για ολοκληρωμένες δοκιμές, το Scapy μπορεί να συνδυαστεί με άλλα εργαλεία κυκλοφορίας. Για παράδειγμα, το Iperf3 μπορεί να χρησιμοποιηθεί για τη δημιουργία μαζικού φορτίου, ενώ το Scapy αξιοποιείται ταυτόχρονα για την εισαγωγή συγκεκριμένων πακέτων δοκιμής κατά τη διάρκεια αυτής της φόρτωσης, προκειμένου να εξεταστεί ο χειρισμός τους από το σύστημα υπό δοκιμή. Επιπλέον, το Scapy μπορεί να δημιουργεί αρχεία PCAP με συγκεκριμένες ακολουθίες πακέτων, τα οποία στη συνέχεια μπορούν να αναπαραχθούν σε μεγάλη κλίμακα χρησιμοποιώντας μια γεννήτρια υψηλής απόδοσης όπως το TRex.

Συμπερασματικά, το Scapy χρησιμεύει ως ένα ισχυρό κιτ εργαλείων ανοιχτού κώδικα για

τη δημιουργία και το χειρισμό της κυκλοφορίας δικτύου σε αναλυτικό επίπεδο. Ακολουθώντας τις βέλτιστες πρακτικές—επικύρωση πακέτων, προσεκτική δημιουργία σεναρίων και κατανόηση του προφίλ απόδοσης—οι χρήστες μπορούν να εκμεταλλευτούν το Scapy για να δημιουργήσουν σενάρια κυκλοφορίας που είναι αδύνατο να επιτευχθούν με άλλα εργαλεία. Αυτό καθιστά το Scapy βασικό στοιχείο στην έρευνα δικτύου για τη δοκιμή νέων ιδεών, την επίθεση σε προβλήματα από το επίπεδο πακέτων και τη διασφάλιση ότι καμία πτυχή της συμπεριφοράς του δικτύου δεν είναι πέρα από την εμβέλεια του ελεγκτή.

4.11. D-ITG

Η αξιολόγηση της απόδοσης δικτύων και η προσομοίωση ρεαλιστικών σεναρίων κυκλοφορίας αποτελούν κρίσιμα στοιχεία στη μελέτη και την ανάπτυξη σύγχρονων τηλεπικοινωνιακών υποδομών. Το D-ITG (Distributed Internet Traffic Generator) είναι ένα εργαλείο ανοιχτού κώδικα που έχει σχεδιαστεί για να δημιουργεί και να διαχειρίζεται ροές δικτυακής κίνησης σε διάφορα επίπεδα του μοντέλου OSI, προσφέροντας τη δυνατότητα προσομοίωσης διαφορετικών τύπων κίνησης (TCP, UDP, SCTP κ.ά.) και την μέτρηση κρίσιμων παραμέτρων όπως το bandwidth, η καθυστέρηση και οι απώλειες πακέτων. Σε αυτό το κεφάλαιο, παρουσιάζονται οι βασικές λειτουργίες, η αρχιτεκτονική, τα σενάρια εφαρμογής, καθώς και τα πλεονεκτήματα και οι προκλήσεις που συνοδεύουν τη χρήση του D-ITG ως γεννήτριας δικτυακής κίνησης.[55]
Το D-ITG έχει σχεδιαστεί με στόχο την παραγωγή δικτυακής κίνησης σε ελεγχόμενο περιβάλλον, επιτρέποντας την προσομοίωση συνθηκών που αντανακλούν την πραγματική λειτουργία ενός δικτύου. Μέσω του D-ITG, οι ερευνητές μπορούν να δημιουργήσουν ροές δεδομένων με προσαρμοσμένα χαρακτηριστικά, να προσομοιώσουν φόρτο σε διάφορα επίπεδα και να μετρήσουν με ακρίβεια την απόδοση ενός δικτύου υπό διαφορετικές συνθήκες. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για τον εντοπισμό πιθανών σημείων συμφόρησης, την ανάλυση της συμπεριφοράς των πρωτοκόλλων και τη δοκιμή νέων τεχνολογικών λύσεων πριν από την υλοποίησή τους σε παραγωγικά περιβάλλοντα.

4.11.1. Κύρια Στοιχεία και Αρχιτεκτονική

Το D-ITG λειτουργεί ως εργαλείο παραγωγής κίνησης που μπορεί να εκτελέσει δοκιμές σε πολλαπλά επίπεδα του δικτύου. Οι βασικές του λειτουργίες περιλαμβάνουν την κατασκευή και αποστολή πακέτων με καθορισμένα χαρακτηριστικά, την προσομοίωση διαφόρων τύπων κίνησης (όπως TCP, UDP, SCTP) και την καταγραφή των αποτελεσμάτων των δοκιμών για περαιτέρω ανάλυση.52 53
Η αρχιτεκτονική του D-ITG βασίζεται σε μια διανεμημένη προσέγγιση, όπου μπορεί να εγκατασταθεί σε πολλαπλούς κόμβους ενός δικτύου για την παραγωγή κίνησης τόσο τοπικά όσο και σε κατανεμημένα περιβάλλοντα. Μέσω ενός απλού και ευέλικτου interface, οι χρήστες μπορούν να καθορίσουν παραμέτρους όπως το μέγεθος των πακέτων, ο ρυθμός αποστολής, η διάρκεια της δοκιμής και ο τύπος της κίνησης. Επιπλέον, το D-ITG επιτρέπει τη μέτρηση παραμέτρων όπως η καθυστέρηση (latency), το jitter και οι απώλειες πακέτων, προσφέροντας έτσι μια ολοκληρωμένη εικόνα της απόδοσης του δικτύου.

52 https://traffic.comics.unina.it/software/ITG/
53 https://github.com/jbucar/ditg

4.11.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Η χρήση του D-ITG είναι ευρέως διαδεδομένη τόσο σε ακαδημαϊκά εργαστήρια όσο και σε βιομηχανικά περιβάλλοντα. Σε εργαστηριακές δοκιμές, το εργαλείο επιτρέπει την προσομοίωση συγκεκριμένων σεναρίων κυκλοφορίας, όπως π.χ. η προσομοίωση μιας συνεπούς ροής δεδομένων για την αξιολόγηση του throughput ή η προσομοίωση σύνθετων σενάριων επιθέσεων, όπως η αύξηση του φόρτου με στόχο την ανίχνευση προβλημάτων στην ποιότητα της σύνδεσης.
Σε περιβάλλοντα παραγωγής, το D-ITG χρησιμοποιείται για τη συνεχή παρακολούθηση και αξιολόγηση της απόδοσης των δικτύων, επιτρέποντας στους διαχειριστές να εντοπίσουν πιθανές αποκλίσεις ή προβλήματα που μπορεί να επηρεάζουν την επικοινωνία. Επιπρόσθετα, οι έρευνες στον τομέα της κυβερνοασφάλειας αξιοποιούν το D-ITG για να προσομοιώσουν ροές κακόβουλης κίνησης, βοηθώντας έτσι στην ανάπτυξη και δοκιμή μηχανισμών ανίχνευσης και άμυνας.

4.11.3. Πλεονεκτήματα και Προκλήσεις

Ένα από τα κύρια πλεονεκτήματα του D-ITG είναι η ευελιξία του στην προσαρμογή των παραμέτρων των δοκιμών. Οι χρήστες έχουν τη δυνατότητα να δημιουργήσουν πολύ συγκεκριμένα σενάρια κυκλοφορίας, επιλέγοντας το είδος, τον ρυθμό και το μέγεθος των πακέτων, καθώς και τη διάρκεια των δοκιμών. Επιπλέον, το εργαλείο υποστηρίζει τη μέτρηση κρίσιμων παραμέτρων δικτύου, προσφέροντας λεπτομερείς αναφορές που διευκολύνουν την ανάλυση και τον εντοπισμό πιθανών σημείων συμφόρησης ή απώλειας δεδομένων.
Ωστόσο, υπάρχουν και ορισμένες προκλήσεις στη χρήση του D-ITG. Η σωστή παραμετροποίηση και η διαχείριση του εργαλείου μπορεί να απαιτούν εξειδικευμένες γνώσεις, ιδιαίτερα όταν πρόκειται για πολύπλοκα σενάρια ή για δοκιμές σε κατανεμημένα περιβάλλοντα. Επιπρόσθετα, η ακρίβεια των μετρήσεων μπορεί να επηρεαστεί από το hardware και το περιβάλλον στο οποίο εκτελείται το εργαλείο, γεγονός που απαιτεί προσεκτικό σχεδιασμό των δοκιμών για την εξασφάλιση αξιόπιστων αποτελεσμάτων.

4.11.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Το D-ITG αποτελεί ένα ισχυρό και ευέλικτο εργαλείο για τη δημιουργία και αξιολόγηση δικτυακής κίνησης, προσφέροντας τη δυνατότητα προσομοίωσης διαφορετικών σεναρίων και τη μέτρηση κρίσιμων παραμέτρων απόδοσης. Η ικανότητά του να προσαρμόζεται σε ποικίλες συνθήκες φόρτου το καθιστά ιδανικό για εργαστηριακές δοκιμές, έρευνα νέων τεχνολογιών και αξιολόγηση παραγωγικών δικτύων. Παρά τις προκλήσεις που συνοδεύουν την παραμετροποίηση και την ακριβή μέτρηση, το D-ITG παραμένει ένα απαραίτητο εργαλείο για τους ερευνητές και τους διαχειριστές δικτύων που επιδιώκουν την βελτιστοποίηση των σύγχρονων τηλεπικοινωνιακών υποδομών.

4.12. Metasploit

Η συνεχής ανάγκη για εξειδικευμένη αξιολόγηση της ανθεκτικότητας και της ασφάλειας των δικτύων έχει οδηγήσει στην ανάπτυξη εργαλείων που όχι μόνο επιτρέπουν τον εντοπισμό και την εκμετάλλευση ευπαθειών, αλλά και τη δημιουργία ρεαλιστικής κίνησης σε ελεγχόμενο περιβάλλον. Το Metasploit Framework είναι κυρίως γνωστό ως ένα πλήρες περιβάλλον για δοκιμές διείσδυσης (penetration testing) και αξιολόγηση ασφάλειας. Ωστόσο, μπορεί να

αξιοποιηθεί και ως γεννήτρια δικτυακής κίνησης, προσομοιώνοντας κακόβουλα σενάρια και επιθέσεις, με σκοπό την αξιολόγηση της απόδοσης και της αντίδρασης των συστημάτων ασφαλείας, όπως των IDS/IPS. [56]
Το Metasploit Framework είναι ένα εργαλείο ανοιχτού κώδικα, κυρίως γραμμένο σε Ruby, το οποίο παρέχει ένα ευρύ φάσμα modules για την αναγνώριση, εκμετάλλευση και αξιολόγηση ευπαθειών σε δίκτυα και συστήματα. Παρά το γεγονός ότι ο κύριος στόχος του είναι η διείσδυση και η αξιολόγηση της ασφάλειας, διαθέτει επίσης auxiliary modules και payloads που, όταν ενεργοποιηθούν, παράγουν δικτυακή κίνηση με συγκεκριμένα χαρακτηριστικά. Μέσω αυτής της λειτουργικότητας, το Metasploit μπορεί να χρησιμοποιηθεί για την προσομοίωση επιθέσεων όπως οι επιθέσεις αρνητικής παροχής υπηρεσίας (DoS) ή η εξαγωγή δεδομένων μέσω reverse shells, συμβάλλοντας έτσι στην παραγωγή ρεαλιστικής κακόβουλης κίνησης για σκοπούς δοκιμών και ανάλυσης.

4.12.1. Κύρια Στοιχεία και Αρχιτεκτονική

Το Metasploit προσφέρει μια ευέλικτη πλατφόρμα που περιλαμβάνει ποικίλα modules, τα οποία επιτρέπουν τόσο την κατασκευή όσο και την εκμετάλλευση payloads.54 [56]Μέσω ειδικών modules, το εργαλείο μπορεί να δημιουργήσει payloads, όπως reverse shells, bind shells, ή ακόμα και payloads που εκτελούν επιθέσεις DDoS, παράγοντας δικτυακή κίνηση με προκαθορισμένα χαρακτηριστικά. Επιπλέον, διαθέτει auxiliary modules που επιτρέπουν τη δημιουργία ελεγχόμενης κίνησης, όπως η σάρωση θυρών ή η εκτέλεση επιθέσεων DoS, προσομοιώνοντας το είδος της κακόβουλης κίνησης που θα δημιουργούσε ένας πραγματικός επιτιθέμενος. Η πλατφόρμα επιτρέπει επίσης την ευέλικτη παραμετροποίηση, καθώς οι χρήστες μπορούν να ρυθμίσουν παράγοντες όπως ο στόχος, ο ρυθμός αποστολής των πακέτων και η διάρκεια της επίθεσης, γεγονός που επιτρέπει τη λεπτομερή προσομοίωση διαφορετικών σεναρίων φόρτου. Η αρχιτεκτονική του Metasploit βασίζεται σε έναν κεντρικό πυρήνα που διαχειρίζεται τα διάφορα modules (exploit, auxiliary, post, encoder, nop generator). Κατά την εκτέλεση ενός module που προσομοιώνει επίθεση, ο χρήστης του Metasploit καθορίζει τις απαραίτητες παραμέτρους, όπως η διεύθυνση IP του στόχου, οι θύρες, το είδος του payload και άλλες μεταβλητές που επηρεάζουν τη συμπεριφορά της κίνησης. Η διαδικασία ξεκινά με την επιλογή του κατάλληλου module μέσα από το περιβάλλον του Metasploit (π.χ. ένα auxiliary module για DoS επίθεση) και τη ρύθμιση των αντίστοιχων παραμέτρων. Στη συνέχεια, το module ενεργοποιείται και παράγει δικτυακή κίνηση σύμφωνα με τις καθορισμένες ρυθμίσεις, η οποία μπορεί να σταλεί είτε σε πραγματικό δίκτυο είτε σε δοκιμαστικό περιβάλλον, προκειμένου να αξιολογηθεί η απόκριση των συστημάτων ασφαλείας.

4.12.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Σε εργαστηριακά και παραγωγικά περιβάλλοντα, το Metasploit ως γεννήτρια δικτυακής κίνησης μπορεί να χρησιμοποιηθεί σε διάφορα σενάρια.[56]Για παράδειγμα, σε πειραματικές δοκιμές

54 https://www.metasploit.com/

ασφάλειας, το εργαλείο επιτρέπει την προσομοίωση επιθέσεων ώστε να αξιολογηθεί η απόδοση και η αντίδραση των συστημάτων ανίχνευσης εισβολών και άλλων μηχανισμών ασφαλείας. Μέσω των ρυθμισμένων payloads, το Metasploit μπορεί να αναπαράγει επιθέσεις όπως DoS, reverse shell και άλλες μορφές κακόβουλης κίνησης. Επιπλέον, χρησιμοποιείται σε εκπαιδευτικά σενάρια για τη διδασκαλία τεχνικών διείσδυσης και ανάλυσης κακόβουλης κίνησης, επιτρέποντας σε φοιτητές και επαγγελματίες να παρατηρούν τη συμπεριφορά των δικτυακών συστημάτων υπό επίθεση. Τέλος, το εργαλείο εφαρμόζεται για την αξιολόγηση της ανθεκτικότητας των δικτύων, μέσω δοκιμών που παράγουν ελεγχόμενη κακόβουλη κίνηση και παρακολούθησης της αντίδρασης των συστημάτων ασφαλείας.

4.12.3. Πλεονεκτήματα και Προκλήσεις

Ένα από τα κύρια πλεονεκτήματα της χρήσης του Metasploit ως γεννήτριας δικτυακής κίνησης είναι η πολυμορφία και η ευελιξία του. Μέσω των πολλαπλών modules και της δυνατότητας παραμετροποίησης, οι χρήστες μπορούν να προσομοιώσουν διάφορα σενάρια επιθέσεων με μεγάλη ακρίβεια. Επιπλέον, το ευρύ οικοσύστημα του Metasploit και η ενεργή κοινότητα υποστήριξης συμβάλλουν στη συνεχή βελτίωση των δυνατοτήτων του εργαλείου. Ωστόσο, υπάρχουν και προκλήσεις. Καθώς το Metasploit δεν έχει σχεδιαστεί αρχικά ως γεννήτρια κίνησης, η λεπτομερής διαχείριση των παραμέτρων της κίνησης, όπως ο ρυθμός αποστολής πακέτων και η χρονική ακρίβεια, μπορεί να μην είναι τόσο υψηλή όσο σε εξειδικευμένα εργαλεία traffic generation. Επιπλέον, η χρήση του σε παραγωγικά περιβάλλοντα απαιτεί ιδιαίτερη προσοχή, ώστε να αποφευχθούν μη εξουσιοδοτημένες επιθέσεις ή ακούσια διακοπή λειτουργίας των συστημάτων.

4.12.4. Βέλτιστες Πρακτικές και Κατευθυντήριες Γραμμές

Για τη χρήση του Metasploit ως γεννήτριας δικτυακής κίνησης σε ελεγχόμενα περιβάλλοντα, συνίσταται να ακολουθούνται ορισμένες βέλτιστες πρακτικές. [56]Αρχικά, θα πρέπει να ορίσουμε σαφώς τα όρια και τις παραμέτρους του πειράματος, επιλέγοντας προσεκτικά τα modules και τα payloads που θα χρησιμοποιηθούν. Η παραμετροποίηση των modules, συμπεριλαμβανομένης της ρύθμισης του στόχου, του ρυθμού αποστολής και της διάρκειας της επίθεσης, είναι ουσιώδης για την επίτευξη επαναλήψιμων και αξιόπιστων αποτελεσμάτων. Επιπρόσθετα, η χρήση του Metasploit σε δοκιμαστικά περιβάλλοντα που είναι απομονωμένα από τα παραγωγικά δίκτυα αποτελεί απαραίτητη προϋπόθεση για την αποφυγή ανεπιθύμητων συνεπειών. Τέλος, η καταγραφή και ανάλυση της παραγόμενης κίνησης μέσω εργαλείων παρακολούθησης (π.χ. Wireshark) συμβάλλει στην επαλήθευση της αποτελεσματικότητας των δοκιμών και στην εντόπιση πιθανών βελτιώσεων.

4.13. LOIC

Η σύγχρονη ανάπτυξη των δικτύων, ιδιαίτερα σε περιβάλλοντα υψηλού φόρτου, απαιτεί την ύπαρξη εργαλείων ικανών να δημιουργούν μεγάλης κλίμακας δικτυακή κίνηση, προκειμένου να αξιολογηθεί η ανθεκτικότητα και η απόδοση των υποδομών. Το LOIC (Low Orbit Ion Cannon) είναι ένα εργαλείο ανοιχτού κώδικα που έχει αποκτήσει ευρεία δημοσιότητα ως γεννήτρια

δικτυακής κίνησης, κυρίως λόγω της χρήσης του σε επιθέσεις αρνητικής παροχής υπηρεσίας (DoS).55 56Παρόλο που η μη εξουσιοδοτημένη χρήση του παραβιάζει νομικούς και ηθικούς κανόνες, σε ελεγχόμενα εργαστηριακά περιβάλλοντα το LOIC μπορεί να αξιοποιηθεί για την προσομοίωση υψηλού φόρτου κίνησης και την αξιολόγηση της απόδοσης δικτύων και συστημάτων ασφαλείας.
Το LOIC, όνομα που προέρχεται από την αγγλική φράση *Low Orbit Ion Cannon*, σχεδιάστηκε αρχικά για να δημιουργεί υψηλό όγκο δικτυακής κίνησης με σκοπό την εκτέλεση επιθέσεων DoS. Αν και η κύρια χρήση του εστιάζεται στην παραγωγή υπερβολικής κίνησης προς έναν στόχο, μπορεί επίσης να λειτουργήσει ως γεννήτρια δικτυακής κίνησης σε ελεγχόμενα εργαστηριακά περιβάλλοντα. Σε τέτοια περιβάλλοντα, οι ερευνητές το αξιοποιούν για να προσομοιώσουν συνθήκες υπερφόρτωσης και να μελετήσουν την αντίδραση και την ανθεκτικότητα των δικτυακών υποδομών και των συστημάτων ασφαλείας.

4.13.1. Κύρια Στοιχεία και Αρχιτεκτονική

Το LOIC διαθέτει μια απλή και φιλική προς τον χρήστη διεπαφή, η οποία μπορεί να χρησιμοποιηθεί είτε μέσω γραφικού περιβάλλοντος είτε μέσω γραμμής εντολών.5758Αυτή η ευκολία επιτρέπει την άμεση εκκίνηση και παραμετροποίηση της επίθεσης. Ο χρήστης ορίζει τον στόχο, είτε με τη μορφή διεύθυνσης IP είτε URL, επιλέγει το πρωτόκολλο που θα χρησιμοποιηθεί (όπως TCP, UDP ή HTTP) και ρυθμίζει τις απαραίτητες παραμέτρους, όπως ο ρυθμός αποστολής, το μέγεθος των πακέτων και η διάρκεια της επίθεσης. Με τη χρήση πολλαπλών νημάτων (threads), το LOIC μπορεί να αυξήσει το throughput και να δημιουργήσει έντονο φόρτο, εκτελώντας την αποστολή των πακέτων σε επαναλαμβανόμενα διαστήματα.
Η απλή αρχιτεκτονική του LOIC το καθιστά αποτελεσματικό για την ταχεία παραγωγή μεγάλου όγκου δικτυακής κίνησης. Ωστόσο, η έλλειψη λεπτομερούς παραμετροποίησης σε σχέση με πιο εξειδικευμένα εργαλεία γεννήτριας κίνησης είναι ένα χαρακτηριστικό που το περιορίζει σε εφαρμογές όπου απαιτείται πολυδιάστατη και λεπτομερής έρευνα.

4.13.2. Σενάρια Χρήσης και Ερευνητικές Εφαρμογές

Σε εργαστηριακά περιβάλλοντα, το LOIC μπορεί να χρησιμοποιηθεί για τη διεξαγωγή δοκιμών ανθεκτικότητας, προσομοιώνοντας υψηλό φόρτο κίνησης με σκοπό την αξιολόγηση της απόδοσης των δικτυακών υποδομών και των μηχανισμών άμυνας, όπως τα συστήματα εντοπισμού εισβολών (IDS/IPS) και τα firewall. Επιπλέον, σε εκπαιδευτικά πλαίσια, το εργαλείο χρησιμοποιείται για τη δημιουργία σεναρίων κατάρτισης, όπου οι συμμετέχοντες έχουν την ευκαιρία να κατανοήσουν την συμπεριφορά των δικτύων υπό επίθεση και να μελετήσουν τις μεθόδους αντιμετώπισης επιθέσεων DDoS.
Επίσης, το LOIC αξιοποιείται για την αξιολόγηση της ασφάλειας των δικτύων, επιτρέποντας στους ερευνητές να καταγράψουν και να αναλύσουν την αντίδραση του δικτύου σε μη εξουσιοδοτημένη κίνηση. Μέσω αυτών των δοκιμών, μπορούν να αναπτυχθούν και να βελτιωθούν

55). https://odr.chalmers.se/bitstreams/0b1906cf-2dd3-4916-99ea-315770d62362/download
56 https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/
57 https://odr.chalmers.se/bitstreams/0b1906cf-2dd3-4916-99ea-315770d62362/download
58 https://www.imperva.com/learn/ddos/low-orbit-ion-cannon/

οι πολιτικές ασφαλείας, προσαρμόζοντας τα συστήματα ώστε να ανταποκρίνονται καλύτερα σε συνθήκες υψηλού φόρτου.

4.13.3. Πλεονεκτήματα και Προκλήσεις

Ένα από τα κύρια πλεονεκτήματα του LOIC είναι η απλότητα στη χρήση του. Η εύκολη παραμετροποίηση και η φιλική διεπαφή του επιτρέπουν στους χρήστες να ξεκινήσουν γρήγορα τις δοκιμές, χωρίς να απαιτούνται εξειδικευμένες γνώσεις στον τομέα της δικτυακής κίνησης. Επιπλέον, η ικανότητα του εργαλείου να παράγει υψηλό ρυθμό αποστολής πακέτων το καθιστά αποτελεσματικό για την προσομοίωση έντονου φόρτου.
Ωστόσο, υπάρχουν και σημαντικές προκλήσεις. Σε σύγκριση με πιο εξειδικευμένα εργαλεία γεννήτριας κίνησης, το LOIC δεν παρέχει λεπτομερή ρύθμιση για την παραγωγή διαφόρων τύπων κίνησης, γεγονός που μπορεί να περιορίσει την ακρίβεια των αποτελεσμάτων σε περιβάλλοντα όπου απαιτείται εξειδικευμένη μέτρηση. Επιπλέον, η μη εξουσιοδοτημένη χρήση του LOIC για επιθέσεις DDoS είναι παράνομη και μπορεί να οδηγήσει σε σοβαρές νομικές συνέπειες. Τέλος, η απλή του αρχιτεκτονική ενδέχεται να μην επαρκεί για την προσομοίωση πολύπλοκων σεναρίων όπου απαιτείται λεπτομερής ανάλυση της κυκλοφορίας.

4.13.4. Βέλτιστες πρακτικές και κατευθυντήριες γραμμές

Το LOIC παραμένει ένα από τα πιο γνωστά εργαλεία γεννήτριας δικτυακής κίνησης, κυρίως λόγω της απλότητας και της ικανότητάς του να παράγει υψηλό φόρτο κίνησης. Αν και η χρήση του για μη εξουσιοδοτημένες επιθέσεις είναι νομικά και ηθικά αμφισβητή, σε ελεγχόμενα εργαστηριακά περιβάλλοντα το LOIC μπορεί να αποτελέσει ένα χρήσιμο εργαλείο για την προσομοίωση επιθέσεων και την αξιολόγηση της ανθεκτικότητας των δικτύων και των συστημάτων ασφαλείας. Η κατανόηση των δυνατοτήτων και των περιορισμών του είναι ουσιώδης για την ανάπτυξη αποτελεσματικών πολιτικών ασφαλείας και τη βελτιστοποίηση των τηλεπικοινωνιακών υποδομών.

5. Διαδικασία Επιλογής και Δικαιολόγηση των Κριτηρίων Αξιολόγησης

5.1 Εισαγωγή

Η επιλογή των κατάλληλων κριτηρίων αξιολόγησης για τα εργαλεία δημιουργίας κίνησης στα δίκτυα 5G αποτελεί ένα κρίσιμο βήμα για την ανάπτυξη ενός αξιόπιστου και ρεαλιστικού περιβάλλοντος δοκιμών ασφάλειας. Η 5G τεχνολογία, με τις αυξημένες απαιτήσεις σε απόδοση, ευελιξία και ασφάλεια, εισάγει νέες προκλήσεις που καθιστούν επιτακτική την ορθή προσομοίωση των πραγματικών συνθηκών λειτουργίας ενός δικτύου νέας γενιάς. Στο παρόν κεφάλαιο, αναλύεται η διαδικασία καθορισμού των κριτηρίων αξιολόγησης, παρουσιάζοντας τους λόγους που οδήγησαν στην επιλογή τους, βασιζόμενοι σε σύγχρονες δημοσιεύσεις του τομέα της 5G τεχνολογίας.

Η Πολυκριτηριακή Ανάλυση Αποφάσεων (MCDA) που ακολουθεί συγκρίνει μια σειρά από εργαλεία δημιουργίας και ανάλυσης κίνησης σε δίκτυα 5G, με στόχο την ανάδειξη των πλεονεκτημάτων και μειονεκτημάτων τους σε κρίσιμες διαστάσεις. Εξετάζονται συνολικά 13 εργαλεία, καλύπτοντας ευρύ φάσμα λειτουργικότητας – από εξομοιωτές/προσομοιωτές δικτύων 5G έως εργαλεία παραγωγής συνθετικής κίνησης, ανάλυσης πακέτων και προσομοίωσης κακόβουλων επιθέσεων. Τα εργαλεία αυτά είναι: ns-3 (με το module 5G-LENA), srsRAN, Open5GS σε συνδυασμό με UERANSIM, OMNeT++ (με βιβλιοθήκη Simu5G), TRex, Mininet (με έμφαση σε SDN), TeraVM, Wireshark, iPerf3, Scapy, D-ITG, Metasploit και LOIC (Low Orbit Ion Cannon).

Η αξιολόγηση πραγματοποιείται με βάση δέκα κριτήρια, τα οποία αποτυπώνονται με συντομογραφίες στον πίνακα που ακολουθεί, και βαθμολογούνται σε κλίμακα 0–5 (0 = ανυπαρξία ή μη ικανοποιητική δυνατότητα, 5 = άριστη υποστήριξη του κριτηρίου). Συνοπτικά, τα κριτήρια είναι: Ικανότητες Δημιουργίας Κίνησης (TGC), Απόδοση και Κλιμάκωση (PS), Ρεαλισμός Εξομοίωσης/Προσομοίωσης (ES), Ευκολία Χρήσης και Παραμετροποίησης (EUC), Επεκτασιμότητα και Προσαρμοστικότητα (EC), Ενσωμάτωση με Εικονικοποίηση & Cloud (IV), Καθυστέρηση, Διακύμανση Καθυστέρησης (Jitter) και Ανάλυση Απόδοσης (LJ), Υποστήριξη Ασφαλείας και Κρυπτογράφησης (SE), Παρακολούθηση και Αναφορά (MR), Κοινότητα, Υποστήριξη και Τεκμηρίωση (CD).

Ιδιαίτερη έμφαση δίνεται σε τρεις πτυχές που θεωρούνται κρίσιμες για συστήματα 5G: **(α)** την ικανότητα κάθε εργαλείου να υποστηρίξει την πλήρη αρχιτεκτονική 5G (ραδιοδίκτυο και πυρήνας), **(β)** τη δυνατότητα παραγωγής κίνησης – τόσο συνθετικής (κανονικής) όσο και κακόβουλης – για δοκιμές φόρτου και ασφάλειας, και **(γ)** την απόδοση και επεκτασιμότητά του σε μεγάλα σενάρια (πλήθος χρηστών, υψηλούς ρυθμούς μετάδοσης).

5.2. Κριτήρια Αξιολόγησης για Εργαλεία Δημιουργίας Κίνησης σε Δίκτυα 5G

Η μελέτη των Andrews J, Buzzi S[57] ανέδειξε τις καινοτόμες τεχνολογίες ραδιοπρόσβασης (New Radio - NR) και τις σημαντικές μεταβολές στην αρχιτεκτονική πυρήνα (5GC), οι οποίες θέτουν

νέες προκλήσεις όσον αφορά την απόδοση, την ευελιξία και την ασφάλεια. Παράλληλα, οι Foukas X, Patounas G., et al. [58] τόνισαν τα ζητήματα που προκύπτουν από την εφαρμογή του network slicing, καθώς και τις νέες απειλές ασφαλείας που προκύπτουν από αυτήν την τεχνολογία. Επιπρόσθετα, οι Taleb T, Samdanis K, et al.[59] εστίασαν στην ενσωμάτωση του edge computing και των λύσεων NFV/SDN στα περιβάλλοντα 5G, επισημαίνοντας τη σημασία της εναρμόνισης των εργαλείων δοκιμών με τις σύγχρονες εικονικοποιημένες υποδομές.
Η αξιολόγηση των εργαλείων δημιουργίας κίνησης στο πλαίσιο των δικτύων 5G απαιτεί ένα πολυδιάστατο πλαίσιο αξιολόγησης. Το πλαίσιο αυτό πρέπει να καταγράφει όχι μόνο την ικανότητα παραγωγής ρεαλιστικής και ποικίλης κίνησης, αλλά και τις πτυχές της απόδοσης, της κλιμάκωσης, της ενσωμάτωσης και της ευχρηστίας, που είναι κρίσιμες για τα σύγχρονα, ετερογενή περιβάλλοντα δικτύων. Τα παρακάτω κριτήρια παρέχουν μια ολοκληρωμένη βάση για τη σύγκριση και επιλογή εργαλείων που πληρούν τις απαιτητικές προδιαγραφές για τη δοκιμή απόδοσης και ασφαλείας στα δίκτυα 5G.

5.2.1. Ικανότητες Δημιουργίας Κίνησης

Προσομοίωση Υπηρεσιών 5G:
Η ικανότητα να προσομοιώνονται ρεαλιστικά οι υπηρεσίες του 5G είναι υψίστης σημασίας. Αυτό το κριτήριο αξιολογεί εάν ένα εργαλείο μπορεί να δημιουργήσει πρότυπα κίνησης που αντικατοπτρίζουν τα διακριτά χαρακτηριστικά των βασικών κατηγοριών υπηρεσιών του 5G: το Enhanced Mobile Broadband (eMBB), το Ultra-Reliable Low-Latency Communications (URLLC) και το Massive Machine-Type Communications (mMTC). Για το eMBB, η έμφαση δίνεται στην παραγωγή ροών υψηλού εύρους ζώνης που προσομοιώνουν εφαρμογές όπως το streaming βίντεο και οι μαζικές μεταφορές αρχείων. Στην περίπτωση του URLLC, το εργαλείο πρέπει να εξασφαλίζει εξαιρετικά χαμηλή καθυστέρηση και ελάχιστο jitter ώστε να επανομοιώσει τις αυστηρές χρονικές απαιτήσεις κρίσιμων εφαρμογών, όπως η τηλεχειρουργική ή τα αυτόνομα οχήματα. Για το mMTC, η προσοχή στρέφεται στην υποστήριξη ενός τεράστιου αριθμού συνδέσεων χαμηλού ρυθμού δεδομένων, χαρακτηριστικό των περιβαλλόντων του Internet of Things (IoT). Ένα αποτελεσματικό εργαλείο δημιουργίας κίνησης θα πρέπει επίσης να υποστηρίζει την παραγωγή ειδικών μηνυμάτων σήμανσης και ελέγχου του 5G, διασφαλίζοντας έτσι ότι οι αλληλεπιδράσεις τόσο του επιπέδου ελέγχου όσο και του επιπέδου χρήστη αναπαράγονται ρεαλιστικά.
Ποικιλία Τύπων Κίνησης:
Εκτός από την προσομοίωση υπηρεσιών, ένα αξιόπιστο εργαλείο δημιουργίας κίνησης πρέπει να υποστηρίζει ένα ευρύ φάσμα τύπων κίνησης. Αυτό περιλαμβάνει τόσο την ικανότητα δημιουργίας συνθετικής κίνησης όσο και την δυνατότητα επαναληπτικής αναπαραγωγής (packet replay). Η συνθετική παραγωγή επιτρέπει τη μοντελοποίηση της κίνησης με τη χρήση παραμετροποιήσιμων παραμέτρων – όπως το μέγεθος των πακέτων, οι χρονικές διαφορές μεταξύ αποστολών και ο συνδυασμός πρωτοκόλλων – δίνοντας τη δυνατότητα στους ερευνητές να διαμορφώνουν σενάρια που ανταποκρίνονται στις αναμενόμενες συνθήκες του δικτύου ή σε συγκεκριμένα μοτίβα επιθέσεων. Αντίστοιχα, η επαναληπτική αναπαραγωγή διευκολύνει την αναπαραγωγή κίνησης που έχει καταγραφεί από το πραγματικό περιβάλλον, προσφέροντας έτσι μια υψηλή πιστότητα στην αναπαράσταση της συμπεριφοράς του δικτύου. Ο συνδυασμός αυτών των δυνατοτήτων εξασφαλίζει ότι τα σενάρια δοκιμών μπορούν να κυμαίνονται από τις κανονικές λειτουργικές συνθήκες έως και σε περιβάλλοντα με προηγμένες επιθέσεις, επιτρέποντας μια ολοκληρωμένη αξιολόγηση τόσο της απόδοσης όσο και των μηχανισμών ασφαλείας.

5.2.2. Απόδοση και Κλιμάκωση

Η απόδοση και η κλιμάκωση αποτελούν δύο θεμελιώδεις διαστάσεις για την αξιολόγηση εργαλείων δημιουργίας κίνησης σε δίκτυα 5G, δεδομένου ότι αυτά τα δίκτυα προορίζονται να διαχειριστούν τεράστιες ποσότητες δεδομένων και να υποστηρίξουν μαζική συνδεσιμότητα. Παρακάτω παρουσιάζεται μια εμπλουτισμένη ανάλυση των βασικών πτυχών που σχετίζονται με την απόδοση και την κλιμάκωση των εργαλείων, οι οποίες είναι κρίσιμες για τη δημιουργία ενός ρεαλιστικού και λειτουργικού περιβάλλοντος δοκιμών.

Υψηλή Απόδοση και PPS (Πακέτα Ανά Δευτερόλεπτο):

Μία από τις βασικές απαιτήσεις για ένα εργαλείο δημιουργίας κίνησης στα δίκτυα 5G είναι η ικανότητά του να παράγει μεγάλες ποσότητες κίνησης με ταχύτητες που αντικατοπτρίζουν τους αναμενόμενους ρυθμούς μετάδοσης δεδομένων. Το κριτήριο αυτό αξιολογεί τον μέγιστο αριθμό πακέτων που μπορεί να παραχθούν ανά δευτερόλεπτο (PPS) καθώς και τη συνολική χωρητικότητα εύρους ζώνης που μπορεί να διαχειριστεί το εργαλείο. Η επίτευξη υψηλών τιμών PPS είναι ουσιώδης για την προσομοίωση των εντάσεων που παρατηρούνται σε πραγματικά δίκτυα 5G, όπου οι ροές δεδομένων μπορεί να είναι εξαιρετικά πυκνές και οι απαιτήσεις σε απόδοση να είναι πολύ υψηλές. Εργαλεία που δεν καταφέρνουν να παράγουν επαρκή κίνηση ενδέχεται να υποτιμήσουν τις πιθανές ευπάθειες του δικτύου ή να μην εντοπίσουν σημεία συμφόρησης, οι οποίες είναι κρίσιμες για τη διάγνωση των επιδόσεων των συστημάτων υπό δοκιμαστικές συνθήκες υψηλού φόρτου.

Πολυπύρηνη Επεξεργασία και Επιτάχυνση Υλικού:

Για να ανταποκριθούν στις απαιτήσεις υψηλής απόδοσης, τα σύγχρονα εργαλεία δημιουργίας κίνησης πρέπει να αξιοποιούν τις δυνατότητες των πολυπύρηνων επεξεργαστών, επιτρέποντας την παράλληλη επεξεργασία πολλαπλών διεργασιών και τη διαχείριση ταυτόχρονων ροών δεδομένων. Επιπλέον, η ενσωμάτωση τεχνικών επιτάχυνσης υλικού, όπως το DPDK (Data Plane Development Kit) και το FPGA (Field-Programmable Gate Array) offloading, είναι κρίσιμη για την αποφυγή συμφόρησης στο ίδιο το εργαλείο. Αυτές οι τεχνολογίες μειώνουν το overhead που επιβάλλεται από το λειτουργικό σύστημα και επιταχύνουν την επεξεργασία των πακέτων, επιτρέποντας τη συνεχή παραγωγή υψηλής ταχύτητας κίνησης. Με αυτόν τον τρόπο, το εργαλείο μπορεί να ανταποκριθεί σε απαιτητικά σενάρια φόρτου, χωρίς να καταλήγει το ίδιο σε σημείο συμφόρησης, γεγονός που είναι απαραίτητο για την πραγματοποίηση εντατικών δοκιμών και την αναπαράσταση των πραγματικών συνθηκών λειτουργίας σε δίκτυα 5G.

Προσομοίωση Μαζικών Συσκευών:

Ένα ακόμη κρίσιμο στοιχείο είναι η δυνατότητα προσομοίωσης μαζικών συσκευών, η οποία σχετίζεται με την υπόσχεση των δικτύων 5G για μαζική συνδεσιμότητα, ιδιαίτερα σε περιβάλλοντα IoT. Ένα ικανό εργαλείο θα πρέπει να μπορεί να παράγει και να διαχειρίζεται μεγάλο αριθμό ταυτόχρονων ροών, αντανακλώντας την πυκνότητα των συσκευών που αναμένεται να ενσωματωθούν σε μελλοντικές αναπτύξεις. Αυτή η δυνατότητα δεν είναι μόνο κρίσιμη για την εφαρμογή δοκιμών που εστιάζουν στον έλεγχο φόρτου, αλλά παρέχει επίσης πολύτιμες πληροφορίες για τη συμπεριφορά των δικτυακών συστημάτων όταν αντιμετωπίζουν ακραίες συνθήκες φόρτου. Με άλλα λόγια, η ικανότητα προσομοίωσης μαζικών συσκευών επιτρέπει στους ερευνητές να αξιολογήσουν πώς ένα δίκτυο μπορεί να διαχειριστεί πραγματικά τις απαιτήσεις των μελλοντικών εφαρμογών και να εντοπίσουν πιθανά σημεία συμφόρησης ή αδυναμίες στην απόδοση.

Συνολικά, η αξιολόγηση της απόδοσης και της κλιμάκωσης ενός εργαλείου δημιουργίας κίνησης απαιτεί μια διττή προσέγγιση: από τη μία, πρέπει να διασφαλιστεί ότι το εργαλείο μπορεί να

παράγει επαρκή ποσότητα κίνησης με υψηλές ταχύτητες, ενώ από την άλλη, πρέπει να μπορεί να επεξεργάζεται αποτελεσματικά τα δεδομένα χωρίς να γίνεται το ίδιο το σύστημα το σημείο συμφόρησης. Η συνδυασμένη αξιολόγηση αυτών των χαρακτηριστικών είναι απαραίτητη για τη δημιουργία ενός ρεαλιστικού περιβάλλοντος δοκιμών που να αντικατοπτρίζει τις αυστηρές απαιτήσεις των δικτύων 5G, επιτρέποντας στους ερευνητές να εντοπίσουν και να διορθώσουν προβλήματα πριν αυτά μεταφερθούν σε παραγωγικά περιβάλλοντα.

5.2.3. Ρεαλισμός Εξομοίωσης/Προσομοίωσης

Η διάκριση μεταξύ της εξομοίωσης σε πραγματικό περιβάλλον και της χρονικά ακριβούς προσομοίωσης είναι θεμελιώδης για την αξιολόγηση των εργαλείων δημιουργίας κίνησης σε δίκτυα 5G. Κάθε μία από αυτές τις προσεγγίσεις προσφέρει μοναδικά πλεονεκτήματα και περιορισμούς, τα οποία καθορίζουν την καταλληλότητά τους για διαφορετικούς τύπους πειραματικών μελετών.

Εξομοίωση σε Πραγματικό Περιβάλλον:

Η εξομοίωση σε πραγματικό περιβάλλον αναφέρεται στην παραγωγή ζωντανής κίνησης που αλληλεπιδρά άμεσα με πραγματικό εξοπλισμό δικτύου και εικονικοποιημένες υποδομές. Μέσω αυτής της προσέγγισης, ένα εργαλείο μπορεί να αναπτυχθεί σε περιβάλλοντα δοκιμών που αντικατοπτρίζουν πιστά τις συνθήκες των δικτύων παραγωγής, επιτρέποντας την αξιολόγηση της λειτουργικής απόδοσης των συστημάτων ασφαλείας, των εφαρμογών και των άλλων στοιχείων του δικτύου υπό ρεαλιστικό φόρτο χρήσης. Με την εξομοίωση σε πραγματικό περιβάλλον, γίνεται δυνατή η παρακολούθηση της συμπεριφοράς των συστημάτων σε πραγματικές συνθήκες, όπως η διαχείριση αιφνίδιων αυξήσεων φόρτου, η αντιμετώπιση επιθέσεων και η ανταπόκριση στις μεταβαλλόμενες συνθήκες του δικτύου. Αυτή η προσέγγιση προσφέρει πολύτιμα δεδομένα για την απόδοση και την αξιοπιστία των υποδομών, δεδομένου ότι το περιβάλλον δοκιμών αντανακλά με υψηλή πιστότητα την πραγματική παραγωγή κίνησης.

Χρονικά Ακριβής Προσομοίωση:

Σε αντίθεση με την εξομοίωση σε πραγματικό περιβάλλον, η χρονικά ακριβής προσομοίωση επικεντρώνεται στη δημιουργία μοντέλων που αναπαριστούν λεπτομερώς τη δυναμική συμπεριφορά του δικτύου. Εργαλεία όπως το ns-3 με το 5G-LENA ή το OMNeT++ με το Simu5G διαθέτουν την ικανότητα να μοντελοποιούν με ακρίβεια τα χρονικά χαρακτηριστικά της κίνησης, συμπεριλαμβανομένων των μεταβαλλόμενων φορτίων, της κινητικότητας των χρηστών και των διαδικασιών handing-over. Αν και αυτή η προσέγγιση δεν παράγει ζωντανή κίνηση, το υψηλό επίπεδο λεπτομέρειας που προσφέρει είναι ανεκτίμητο για τη διεξαγωγή ελεγχόμενων πειραματικών μελετών. Μέσω της χρονικά ακριβούς προσομοίωσης, οι ερευνητές μπορούν να εξετάσουν πολύ συγκεκριμένα σενάρια και να μελετήσουν τις λεπτές αλληλεπιδράσεις μεταξύ των πρωτοκόλλων, οι οποίες είναι κρίσιμες για την κατανόηση της συμπεριφοράς του δικτύου υπό διαφορετικά δυναμικά φορτία.

Συνολικά, η επιλογή μεταξύ εξομοίωσης σε πραγματικό περιβάλλον και χρονικά ακριβούς προσομοίωσης εξαρτάται από τους στόχους της έρευνας. Ενώ η χρονικά ακριβής προσομοίωση παρέχει μια θεωρητική βάση με πολύ υψηλή ακρίβεια στη μοντελοποίηση των πρωτοκόλλων και των δυναμικών συμπεριφορών, η εξομοίωση σε πραγματικό περιβάλλον είναι απαραίτητη για την πρακτική αξιολόγηση της απόδοσης και της ανθεκτικότητας σε πραγματικές συνθήκες φόρτου. Ο συνδυασμός των δύο μεθόδων μπορεί να προσφέρει ένα ολοκληρωμένο πείραμα, επιτρέποντας στους ερευνητές να εκμεταλλευτούν τόσο την ακρίβεια της προσομοίωσης όσο και την ρεαλιστική αλληλεπίδραση που παρέχει η ζωντανή εξομοίωση. Αυτό το υβριδικό μοντέλο αποτελεί την

καλύτερη πρακτική για την πλήρη αξιολόγηση των συστημάτων στα περιβάλλοντα δικτύων 5G, όπου η πολυπλοκότητα και η μεταβλητότητα του φόρτου απαιτούν τόσο θεωρητική όσο και πρακτική εξέταση. Δεδομένης της παραπάνω παραδοχής καλούμαστε να αξιολογήσουμε τα εργαλεία συμφώνα με τη συνολική τους δυνατότητα προσέγγισης της πραγματικής κίνησης που θα παραγόταν σε ένα μοντέρνο δίκτυο 5G.

5.2.4. Ευκολία Χρήσης και Παραμετροποίησης

Η πρακτική χρησιμότητα των εργαλείων δημιουργίας κίνησης δικτύου (NTG) για την αξιολόγηση της ασφάλειας των δικτύων 5G εξαρτάται σε μεγάλο βαθμό από την ευκολία χρήσης, την ευχρηστία και την παραμετροποίησή τους. Ένα καλά σχεδιασμένο περιβάλλον χρήστη, η εκτενής τεκμηρίωση και οι αποτελεσματικές δυνατότητες αυτοματοποίησης επηρεάζουν άμεσα την παραγωγικότητα του ερευνητή και την ικανότητά του να διεξάγει αυστηρά και επαναλήψιμα πειράματα. Η αξιολόγηση της ευχρηστίας μπορεί να δομηθεί σε δύο βασικά υποκριτήρια: **Διεπαφή και Παραμετροποίηση** και **Αυτοματοποίηση και Προκατασκευασμένα Πρότυπα**.

Διεπαφή και Παραμετροποίηση

Οι επιλογές διεπαφής και παραμετροποίησης που παρέχονται από τα εργαλεία NTG έχουν σημαντικό αντίκτυπο στην αποδοτικότητα και την ακρίβεια με την οποία οι ερευνητές μπορούν να δημιουργήσουν, να εκτελέσουν και να αναλύσουν σύνθετα σενάρια δοκιμών. Αποτελεσματικές διεπαφές μειώνουν τα ανθρώπινα λάθη, απλοποιούν την επανάληψη πειραμάτων και μειώνουν την καμπύλη εκμάθησης που συνδέεται με τη σύνθετη δικτυακή πειραματική διαδικασία.

Τα εργαλεία NTG συνήθως παρέχουν είτε γραφική διεπαφή χρήστη (GUI), είτε γραμμή εντολών (CLI), είτε και τα δύο. Μια γραφική διεπαφή χρήστη, όπως αυτή που παρέχεται από το **TeraVM**, διευκολύνει τη γρήγορη δημιουργία σεναρίων, την ευέλικτη απεικόνιση των ρυθμίσεων παραμετροποίησης και την εύκολη παρακολούθηση των τρεχουσών δοκιμών, ενισχύοντας έτσι σημαντικά την προσβασιμότητα και την ευχρηστία για ερευνητές που μπορεί να μην έχουν εκτενή εμπειρία στη γραμμή εντολών. Αντίθετα, οι διεπαφές γραμμής εντολών (CLI) —κοινές σε εργαλεία όπως τα **TRex**, **Iperf3**, **ns-3** και **OMNeT++**— προσφέρουν μεγαλύτερη ευελιξία, ακρίβεια και δυνατότητες αυτοματοποίησης, που είναι επωφελείς για έμπειρους χρήστες που εκτελούν αυτοματοποιημένες, προγραμματισμένες ή μαζικές λειτουργίες.

Εργαλεία που παρέχουν τόσο GUI όσο και CLI —όπως εμπορικές πλατφόρμες (**TeraVM**) και ευέλικτες λύσεις ανάλυσης (**Wireshark**)— επιτρέπουν στους ερευνητές να δημιουργούν γρήγορα πρωτότυπα σενάρια οπτικά, διατηρώντας παράλληλα την ευελιξία της γραμμής εντολών για λεπτομερή προσαρμογή των σεναρίων.

Ωστόσο, εξειδικευμένα περιβάλλοντα προσομοίωσης (**ns-3 με το 5G-LENA**, **OMNeT++ με το Simu5G**) παρουσιάζουν συνήθως απότομες καμπύλες εκμάθησης λόγω της εγγενούς πολυπλοκότητάς τους και των εκτεταμένων απαιτήσεων παραμετροποίησης. Αν και αυτά τα εργαλεία προσφέρουν εκτεταμένη δυνατότητα παραμετροποίησης, μπορεί να απαιτούν σημαντική αρχική εκπαίδευση και εξειδίκευση στον τομέα, περιορίζοντας ενδεχομένως την προσβασιμότητά τους σε αρχάριους ερευνητές χωρίς σημαντική προηγούμενη εμπειρία.

Αυτοματοποίηση και Προκατασκευασμένα Πρότυπα

Οι δυνατότητες αυτοματοποίησης και η διαθεσιμότητα προκατασκευασμένων προτύπων παραμετροποίησης ενισχύουν σημαντικά την επαναληψιμότητα, την αποδοτικότητα και την

αξιοπιστία των δικτυακών πειραμάτων. Τα εργαλεία NTG που υποστηρίζουν την αυτοματοποίηση -μέσω διεπαφών προγραμματισμού (π.χ., Python, Ansible, Bash scripts)- διευκολύνουν τη γρήγορη ρύθμιση, εκτέλεση και ανάλυση δοκιμών, απλοποιώντας σε μεγάλο βαθμό τις επαναλαμβανόμενες και επαναληπτικές πειραματικές διαδικασίες.
Εργαλεία όπως τα **TRex**, **Scapy**, **TeraVM** και **Mininet με SDN** προσφέρουν εκτεταμένες δυνατότητες προγραμματισμού, επιτρέποντας στους χρήστες να αυτοματοποιούν περίπλοκες ροές εργασίας δοκιμών. Αυτές οι διεπαφές προγραμματισμού βοηθούν τους ερευνητές να αναπαράγουν εύκολα σενάρια σε πολλαπλά περιβάλλοντα δοκιμών, μειώνοντας σημαντικά την πολυπλοκότητα της ρύθμισης και βελτιώνοντας την επαναληψιμότητα των πειραμάτων.
Προκατασκευασμένα πρότυπα, που παρέχονται από ορισμένα εμπορικά ή υποστηριζόμενα από την κοινότητα εργαλεία (π.χ., **TeraVM**), προσφέρουν προκαθορισμένες ρυθμίσεις που αντιπροσωπεύουν κοινά σενάρια δοκιμών ή προφίλ κίνησης βάσει προτύπων. Η διαθεσιμότητα αυτών των προτύπων μειώνει δραστικά τον χρόνο και την προσπάθεια που απαιτούνται για το σχεδιασμό σύνθετων δοκιμών από το μηδέν, επιτρέποντας στους ερευνητές να ξεκινήσουν γρήγορα την πειραματική διαδικασία προσαρμόζοντας μόνο τις κρίσιμες παραμέτρους.

5.2.5. Επεκτασιμότητα και Προσαρμοστικότητα

Η ικανότητα των εργαλείων δημιουργίας κίνησης δικτύου (NTG) να προσαρμόζονται και να επεκτείνονται είναι κρίσιμη για την αντιμετώπιση των συνεχώς εξελισσόμενων απαιτήσεων των δικτύων 5G. Αυτή η ευελιξία επιτρέπει στους ερευνητές και τους διαχειριστές δικτύων να προσαρμόζουν τα εργαλεία σύμφωνα με τις συγκεκριμένες ανάγκες τους, να ενσωματώνουν νέες λειτουργίες και να διατηρούν την αποτελεσματικότητα των εργαλείων σε ένα μεταβαλλόμενο τεχνολογικό περιβάλλον. Η αξιολόγηση της επεκτασιμότητας και της προσαρμοστικότητας μπορεί να διακριθεί σε δύο κύριες πτυχές: **Υποστήριξη Scripting και API** και **Αρχιτεκτονική Μοναδοποίησης**.

Υποστήριξη Scripting και API

Η δυνατότητα των εργαλείων NTG να υποστηρίζουν scripting και να παρέχουν ανοιχτές διεπαφές προγραμματισμού εφαρμογών (APIs) είναι θεμελιώδης για την προσαρμογή και την αυτοματοποίηση των λειτουργιών τους. Η ευελιξία αυτή επιτρέπει στους χρήστες να δημιουργούν προσαρμοσμένα σενάρια δοκιμών, να αυτοματοποιούν διαδικασίες και να ενσωματώνουν τα εργαλεία σε μεγαλύτερα συστήματα διαχείρισης δικτύου.
Εργαλεία όπως το **Scapy** και το **Iperf3** προσφέρουν εκτεταμένες δυνατότητες scripting, επιτρέποντας στους χρήστες να δημιουργούν και να διαχειρίζονται προσαρμοσμένα σενάρια κίνησης δικτύου. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για την προσομοίωση συγκεκριμένων συνθηκών δικτύου και την αξιολόγηση της απόδοσης υπό διάφορα φορτία.
Η παροχή ανοιχτών APIs επιτρέπει την εύκολη ενσωμάτωση των εργαλείων NTG με άλλα συστήματα και εφαρμογές. Για παράδειγμα, το **TRex** προσφέρει RESTful API, διευκολύνοντας την ενσωμάτωση με πλατφόρμες διαχείρισης δικτύου και την αυτοματοποίηση διαδικασιών δοκιμών.

Αρχιτεκτονική Μοναδοποίησης

Μια αρθρωτή (μοναδοποιημένη) αρχιτεκτονική επιτρέπει την εύκολη προσθήκη, αφαίρεση ή τροποποίηση λειτουργικών μονάδων, καθιστώντας τα εργαλεία NTG πιο ευέλικτα και προσαρμόσιμα στις μεταβαλλόμενες ανάγκες των δικτύων 5G.
Εργαλεία όπως το **Wireshark** διαθέτουν αρθρωτή αρχιτεκτονική που επιτρέπει την ανάπτυξη πρόσθετων (plugins) για την ανάλυση νέων πρωτοκόλλων ή την προσθήκη νέων λειτουργιών.

Αυτή η δυνατότητα επιτρέπει στους χρήστες να προσαρμόζουν το εργαλείο στις συγκεκριμένες ανάγκες τους και να επεκτείνουν τις δυνατότητές του χωρίς να απαιτείται ανασχεδιασμός του βασικού συστήματος.
Η αρθρωτή αρχιτεκτονική επιτρέπει επίσης την εύκολη ενσωμάτωση νέων τεχνολογιών και προτύπων. Για παράδειγμα, η δυνατότητα προσθήκης υποστήριξης για νέα πρωτόκολλα 5G ή τεχνολογίες εικονικοποίησης επιτρέπει στα εργαλεία NTG να παραμένουν επίκαιρα και χρήσιμα σε ένα συνεχώς εξελισσόμενο τεχνολογικό τοπίο.

5.2.6. Ενσωμάτωση με Εικονικοποίηση και Cloud

Συμβατότητα με NFV, SDN και Cloud:
Η αυξανόμενη εξάρτηση των δικτύων 5G από τεχνολογίες εικονικοποίησης καθιστά απαραίτητη την πλήρη ενσωμάτωση των εργαλείων δημιουργίας κίνησης σε σύγχρονα εικονικοποιημένα περιβάλλοντα. Συγκεκριμένα, η υποστήριξη για Network Functions Virtualization (NFV) και Software-Defined Networking (SDN) επιτρέπει στα εργαλεία αυτά να λειτουργούν αρμονικά σε πλατφόρμες όπως το Kubernetes, οι Εικονικές Λειτουργίες Δικτύου (VNFs) και διάφορα hypervisors (π.χ., VMware, KVM, XEN). Η αξιολόγηση σε αυτό το επίπεδο εξετάζει τη δυνατότητα του εργαλείου να αναπτυχθεί και να διαχειριστεί δοκιμαστικά περιβάλλοντα που αντικατοπτρίζουν πιστά τα παραγωγικά δίκτυα, όπου οι εικονικοποιημένες υποδομές παρέχουν ευελιξία και δυναμική διαχείριση πόρων. Με άλλα λόγια, ένα εργαλείο που είναι συμβατό με τις πιο σύγχρονες τεχνολογίες cloud και εικονικοποίησης, μπορεί να ενσωματωθεί απρόσκοπτα σε ένα ολοκληρωμένο περιβάλλον δοκιμών, εξασφαλίζοντας την ρεαλιστική αναπαράσταση και τη διαχείριση των πολυπλοκών ρυθμίσεων ενός δικτύου 5G.
Διαλειτουργικότητα με Δοκιμαστικά Περιβάλλοντα 5G:
Εκτός από την τεχνική συμβατότητα με εικονικοποιημένα περιβάλλοντα, ένα εργαλείο δημιουργίας κίνησης πρέπει να δείχνει υψηλά επίπεδα διαλειτουργικότητας με καθιερωμένα πλαίσια 5G, όπως το Open5GS με UERANSIM ή το srsRAN. Η ικανότητα σύνδεσης με αυτά τα πλαίσια επιτρέπει τη δημιουργία ολοκληρωμένων περιβαλλόντων δοκιμών όπου όλα τα στοιχεία του δικτύου – από τους εικονικούς διακομιστές και τις λειτουργίες ελέγχου μέχρι τα στοιχεία ασφαλείας – συνεργάζονται αρμονικά. Μέσω της διαλειτουργικότητας, το εργαλείο δημιουργίας κίνησης μπορεί να παρέχει ρεαλιστικά σενάρια φόρτου και να αξιολογεί την απόδοση και την ανθεκτικότητα των συστημάτων ασφαλείας υπό συνθήκες που προσομοιώνουν την πραγματική λειτουργία ενός δικτύου 5G. Επιπλέον, αυτή η ικανότητα ενσωμάτωσης εξασφαλίζει ότι οι δοκιμές μπορούν να επεκταθούν εύκολα, καλύπτοντας ολοκληρωμένα όλες τις πτυχές της λειτουργίας ενός πραγματικού δικτύου, από την κατανομή πόρων μέχρι την αντιμετώπιση επιθέσεων σε περιβάλλοντα με υψηλή συνδεσιμότητα.

5.2.7. Καθυστέρηση, Διακύμανση Καθυστέρησης (Jitter) και Ανάλυση Απόδοσης

Η αξιολόγηση των δικτύων πέμπτης γενιάς (5G) απαιτεί ακριβή μέτρηση και ανάλυση κρίσιμων παραμέτρων ποιότητας υπηρεσίας (Quality of Service - QoS), όπως η καθυστέρηση (latency), η διακύμανση της καθυστέρησης (jitter) και η απώλεια πακέτων. Οι παράμετροι αυτές αποκτούν ιδιαίτερη σημασία λόγω των εξαιρετικά απαιτητικών εφαρμογών που υποστηρίζονται από τα δίκτυα 5G, όπως οι εφαρμογές επαυξημένης πραγματικότητας, η τηλεϊατρική, οι βιομηχανικές εφαρμογές αυτοματισμού και η αυτόνομη οδήγηση, οι οποίες απαιτούν υψηλή ακρίβεια και αξιοπιστία σε πραγματικό χρόνο (Marco Giordani,Michele Polese, et al [60]).

Ικανότητες Μέτρησης και Ανάλυσης Απόδοσης
Η ακρίβεια μέτρησης των παραμέτρων της καθυστέρησης, του jitter και της απώλειας πακέτων απαιτεί εργαλεία που διαθέτουν υψηλή χρονική ακρίβεια (timestamping precision). Η ικανότητα ενός εργαλείου δημιουργίας κίνησης δικτύου (NTG) να παρέχει ακριβείς μετρήσεις είναι απαραίτητη για τη σωστή κατανόηση και βελτιστοποίηση της συμπεριφοράς των δικτύων 5G, ιδίως σε σενάρια Ultra-Reliable Low-Latency Communications (URLLC), όπου ακόμη και μικρές αποκλίσεις μπορούν να έχουν σημαντικές επιπτώσεις στην αξιοπιστία και ασφάλεια της επικοινωνίας (Popovski P, Trillingsgaard K., et al.[61]).
Σύμφωνα με μελέτες, η καθυστέρηση στα δίκτυα 5G πρέπει συχνά να περιορίζεται κάτω από το 1ms έως 10ms ανάλογα με την εφαρμογή, ενώ το jitter πρέπει να παραμένει σε πολύ χαμηλά επίπεδα για να εξασφαλίζεται η συνέπεια και η προβλεψιμότητα των υπηρεσιών (ITU-R, 2017). Έτσι, εργαλεία όπως το Iperf3, το TRex ή οι πλατφόρμες προσομοίωσης ns-3 με 5G-LENA και OMNeT++ με Simu5G, που παρέχουν ακριβείς μετρήσεις καθυστέρησης και jitter, είναι απαραίτητα για την αξιόπιστη εκτίμηση της απόδοσης και της αντοχής των δικτυακών υποδομών[62]
Επιπλέον, η δυνατότητα μέτρησης και ανάλυσης της απώλειας πακέτων είναι κρίσιμη για την αξιολόγηση των μηχανισμών ανάκαμψης και βελτιστοποίησης που εφαρμόζονται στα δίκτυα 5G, ειδικά σε σενάρια υψηλού φόρτου ή επιθέσεων τύπου DoS/DDoS. Ακριβείς μετρήσεις απώλειας πακέτων επιτρέπουν στους ερευνητές να προσδιορίσουν με ακρίβεια τα όρια αντοχής των δικτύων και να δοκιμάσουν στρατηγικές αντιμετώπισης έκτακτων περιστατικών ή κυβερνοεπιθέσεων [58].

Χρονοσήμανση και Ακρίβεια Μετρήσεων
Η ακριβής χρονοσήμανση πακέτων (timestamping) αποτελεί βασικό παράγοντα που καθορίζει την ποιότητα των μετρήσεων καθυστέρησης και jitter. Σύμφωνα με τους59, η αξιοποίηση εργαλείων με δυνατότητες hardware timestamping (χρήση εξειδικευμένου υλικού) προσφέρει μεγαλύτερη ακρίβεια συγκριτικά με το software-based timestamping, μειώνοντας σημαντικά τα σφάλματα μέτρησης. Συνεπώς, για πειράματα που απαιτούν αυξημένη ακρίβεια και αξιοπιστία, προτείνεται η χρήση εργαλείων που αξιοποιούν hardware timestamping ή υποστηρίζουν τεχνολογίες όπως Precision Time Protocol (PTP) 60), ώστε να παρέχονται αποτελέσματα υψηλής ακρίβειας.
Συνολικά, οι δυνατότητες ακριβούς μέτρησης και ανάλυσης της καθυστέρησης, του jitter, και της απώλειας πακέτων αποτελούν αναπόσπαστο μέρος της διαδικασίας αξιολόγησης και επικύρωσης της απόδοσης και της ασφάλειας των δικτύων 5G. Εργαλεία με προηγμένες δυνατότητες μέτρησης και ανάλυσης διασφαλίζουν ότι οι ερευνητές μπορούν να αποκτήσουν ουσιαστική κατανόησή των δικτύων και να εντοπίσουν αποτελεσματικά σημεία βελτίωσης στην αρχιτεκτονική και τις διαδικασίες λειτουργίας τους.

5.2.8. Υποστήριξη Ασφαλείας και Κρυπτογράφησης

Προσομοίωση Επιθέσεων και Ανωμαλιών:
Η δοκιμή των μηχανισμών ασφαλείας σε περιβάλλοντα 5G απαιτεί την ικανότητα αναπαραγωγής όχι μόνο κανονικής κίνησης, αλλά και επιθετικών συνθηκών, προκειμένου να αξιολογηθούν οι αντιδράσεις και οι μηχανισμοί άμυνας του δικτύου. Στο πλαίσιο αυτό, είναι απαραίτητο το εργαλείο δημιουργίας κίνησης να μπορεί να προσομοιώσει ένα ευρύ φάσμα απειλών, όπως

59 https://ieeexplore.ieee.org/document/8901894/
60 https://standards.ieee.org/ieee/1588/4355/

πλημμύρες σήμανσης, επιθέσεις DDoS (Distributed Denial of Service) σε κανάλια ελέγχου και στοχευμένες δοκιμές διείσδυσης. Η δυνατότητα αυτή επιτρέπει στους ερευνητές να εξετάσουν την ανθεκτικότητα και την προσαρμοστικότητα των συστημάτων ασφαλείας, εντοπίζοντας τυχόν αδυναμίες και βελτιώνοντας τις στρατηγικές αντιμετώπισης επιθέσεων. Επιπλέον, η προσομοίωση επιθέσεων σε ένα ελεγχόμενο περιβάλλον επιτρέπει την αναλυτική καταγραφή των αντιδράσεων, παρέχοντας δεδομένα που μπορούν να χρησιμοποιηθούν για την ανάπτυξη προηγμένων μηχανισμών άμυνας και την ενίσχυση της γενικής ασφάλειας των δικτύων 5G.

Δυνατότητες Κρυπτογράφησης:

Τα σύγχρονα δίκτυα 5G απαιτούν ισχυρά πρωτόκολλα κρυπτογράφησης για να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των επικοινωνιών, ιδιαίτερα σε ένα περιβάλλον όπου ο όγκος και η ευρεία χρήση των δεδομένων αυξάνεται δραματικά. Ένα εργαλείο δημιουργίας κίνησης πρέπει να είναι ικανό να προσομοιώσει κίνηση που είναι κρυπτογραφημένη με τη χρήση πρωτοκόλλων όπως το TLS (Transport Layer Security) και το IPSec (Internet Protocol Security). Αυτή η δυνατότητα είναι κρίσιμη για την προσομοίωση των συνθηκών ενός πραγματικού περιβάλλοντος 5G, όπου οι επικοινωνίες προστατεύονται από την παράνομη πρόσβαση και τα υποκλοπές. Επιπλέον, η εφαρμογή τεχνικών απόκρυψης κίνησης—όπως η τυχαία αλλαγή χαρακτηριστικών των πακέτων ή η διαχείριση μεταβλητών μορφών δεδομένων—επιτρέπει τη δοκιμή της απόδοσης των συστημάτων ασφαλείας σε περιβάλλοντα που προσομοιώνουν πραγματικές συνθήκες κρυπτογραφημένης επικοινωνίας. Μέσω αυτών των δυνατοτήτων, οι ερευνητές μπορούν να αξιολογήσουν πώς αντιδρούν οι μηχανισμοί ανίχνευσης και πρόληψης επιθέσεων σε δεδομένα που προστατεύονται με κρυπτογράφηση, εξασφαλίζοντας έτσι ότι το δίκτυο διατηρεί την απόδοσή του ακόμη και όταν υπόκειται σε επιθετικές συνθήκες.

5.2.9. Παρακολούθηση και Αναφορά

Ενσωματωμένη Αναλυτική:

Η αποτελεσματική παρακολούθηση αποτελεί θεμέλιο για την αξιολόγηση και τη βελτιστοποίηση των δικτυακών συστημάτων σε ένα περιβάλλον δοκιμών. Ένα εργαλείο δημιουργίας κίνησης που διαθέτει ενσωματωμένες δυνατότητες αναλυτικής παρακολούθησης μπορεί να παρέχει κρίσιμες πληροφορίες σε πραγματικό χρόνο, όπως λεπτομερή καταγραφή (logging) των συμβάντων, παρακολούθηση της κίνησης και ανάλυση βασικών δεικτών απόδοσης. Συγκεκριμένα, η δυνατότητα εξαγωγής δεδομένων σε τυποποιημένες μορφές όπως CSV ή JSON επιτρέπει την περαιτέρω επεξεργασία και ανάλυση των δεδομένων από εξωτερικά εργαλεία και πλατφόρμες. Η δυνατότητα αυτή συμβάλλει στην ταχεία διάγνωση πιθανών προβλημάτων και στη λήψη ενημερωμένων αποφάσεων, καθώς επιτρέπει στους ερευνητές να εντοπίσουν και να καταγράψουν κρίσιμες μεταβολές στην απόδοση του δικτύου, όπως απώλειες πακέτων, μεταβολές στη καθυστέρηση και διακυμάνσεις του jitter. Με αυτόν τον τρόπο, η ενσωματωμένη αναλυτική όχι μόνο διευκολύνει την άμεση παρακολούθηση των συστημάτων, αλλά και δημιουργεί ένα αξιόπιστο ιστορικό δεδομένων που μπορεί να χρησιμοποιηθεί για την ανάλυση τάσεων και την πρόβλεψη μελλοντικών συμπεριφορών.

Εργαλεία Αναφοράς:

Η παρουσία προκαθορισμένων πινάκων ελέγχου και εργαλείων αναφοράς ενισχύει σημαντικά την ευχρηστία ενός εργαλείου δημιουργίας κίνησης. Μέσω αυτών των εργαλείων, οι χρήστες μπορούν να έχουν άμεση πρόσβαση σε κρίσιμες πληροφορίες για την απόδοση και την ανταπόκριση των συστημάτων ασφαλείας του δικτύου, επιτρέποντας μια ολιστική αξιολόγηση των δοκιμών. Οι προκαθορισμένοι πίνακες ελέγχου συχνά παρέχουν γραφικές αναπαραστάσεις και διαδραστικές

απεικονίσεις των δεδομένων, διευκολύνοντας την ταχεία κατανόηση και ανάλυση των αποτελεσμάτων. Επιπλέον, τα εργαλεία αναφοράς επιτρέπουν στους ερευνητές να δημιουργούν ολοκληρωμένες αναφορές που μπορούν να χρησιμεύσουν τόσο για την επιστημονική τεκμηρίωση όσο και για τη λήψη αποφάσεων σε επιχειρησιακά περιβάλλοντα. Η δυνατότητα εξατομικευμένης αναφοράς, που περιλαμβάνει παραμετροποιήσιμα φίλτρα και επιλογές παρουσίασης των δεδομένων, ενισχύει περαιτέρω την ικανότητα του εργαλείου να προσαρμόζεται στις ανάγκες του χρήστη και να υποστηρίζει τη συνεχή βελτίωση των δικτυακών υποδομών.
Σε συνδυασμό, οι ενσωματωμένες δυνατότητες αναλυτικής παρακολούθησης και τα εργαλεία αναφοράς συνιστούν μια ολοκληρωμένη προσέγγιση για την παρακολούθηση, αξιολόγηση και βελτιστοποίηση της απόδοσης των δικτύων 5G. Η ύπαρξη τέτοιων λειτουργιών όχι μόνο διευκολύνει την άμεση διάγνωση προβλημάτων, αλλά και παρέχει ένα βασικό εργαλείο για την τεκμηρίωση των πειραματικών αποτελεσμάτων, καθιστώντας τα δεδομένα επαναληπτικά, αξιόπιστα και κατάλληλα για επιστημονική ανάλυση. Μέσω της χρήσης προκαθορισμένων πινάκων ελέγχου και εξατομικευμένων αναφορών, οι ερευνητές μπορούν να αποκτήσουν μια βαθύτερη κατανόηση της συμπεριφοράς του δικτύου υπό διαφορετικές συνθήκες φόρτου, γεγονός που είναι κρίσιμο για την ανάπτυξη στρατηγικών βελτίωσης και την αντιμετώπιση νέων απειλών σε περιβάλλοντα 5G.

5.2.10. Κοινότητα, Υποστήριξη και Τεκμηρίωση

Άδειες και Ανάπτυξη:
Η μακροπρόθεσμη βιωσιμότητα και επιτυχία ενός εργαλείου δημιουργίας κίνησης εξαρτάται σε μεγάλο βαθμό από το μοντέλο αδειοδότησης και το επίπεδο υποστήριξης που παρέχεται από την κοινότητα. Εργαλεία ανοιχτού κώδικα συχνά επωφελούνται από μια ενεργή και δυναμική κοινότητα χρηστών και προγραμματιστών, οι οποίοι συνεχώς συμβάλλουν με ενημερώσεις, διόρθωση σφαλμάτων και νέες λειτουργίες. Η συχνότητα των ενημερώσεων και η δραστηριότητα της κοινότητας αποτελούν κρίσιμα κριτήρια, καθώς διασφαλίζουν ότι το εργαλείο παραμένει σύγχρονο και προσαρμόζεται στις εξελισσόμενες ανάγκες της βιομηχανίας. Σε αντίθεση, τα ιδιόκτητα εργαλεία μπορεί να προσφέρουν πιο σταθερή και ελεγχόμενη ανάπτυξη με εξειδικευμένη τεχνική υποστήριξη, αλλά συχνά υπόκεινται σε περιορισμούς όσον αφορά την ευελιξία και την ταχύτητα ανανέωσης του λογισμικού. Επομένως, η αξιολόγηση στο πλαίσιο αυτό περιλαμβάνει τη μέτρηση του μεγέθους και της δραστηριότητας της κοινότητας, της συχνότητας ενημερώσεων και της συνολικής βιωσιμότητας του οικοσυστήματος ανάπτυξης, καθώς όλα αυτά συμβάλλουν στην εξασφάλιση ενός εργαλείου που μπορεί να παραμείνει αξιόπιστο και χρήσιμο σε βάθος χρόνου.
Τεκμηρίωση και Εκπαιδευτικό Υλικό:
Η υψηλής ποιότητας τεκμηρίωση αποτελεί ακρογωνιαίο λίθο για την ομαλή υλοποίηση και χρήση ενός εργαλείου δημιουργίας κίνησης, ειδικά σε ένα περίπλοκο περιβάλλον όπως αυτό των δικτύων 5G. Λεπτομερείς οδηγίες χρήσης, βήμα προς βήμα tutorials και σαφή παραδείγματα κώδικα επιταχύνουν την καμπύλη μάθησης και μειώνουν τα πιθανά σφάλματα κατά την εγκατάσταση και παραμετροποίηση του εργαλείου. Επιπλέον, ενεργά διαδικτυακά φόρουμ, ομάδες συζήτησης και κανάλια υποστήριξης εξασφαλίζουν ότι οι χρήστες μπορούν να λάβουν άμεση βοήθεια και να ανταλλάξουν εμπειρίες, ενισχύοντας έτσι τη συνεργασία και τη συνεχή βελτίωση του λογισμικού. Η ολοκληρωμένη τεκμηρίωση δεν διευκολύνει μόνο την αρχική υλοποίηση αλλά παρέχει επίσης ένα σημαντικό εργαλείο για τη συνεχή συντήρηση, αντιμετώπιση προβλημάτων και περαιτέρω ανάπτυξη του εργαλείου σε βάθος χρόνου.

5.3 Αξιολόγηση των εργαλείων

Πολυκριτηριακή Ανάλυση και Μέθοδοι Επιλογής για Την Τελική Επιλογή Εργαλείων Δημιουργίας Κίνησης σε Δίκτυα 5G

Για την τελική επιλογή του κατάλληλου εργαλείου δημιουργίας κίνησης σε δίκτυα 5G, είναι αναγκαία μια πολυκριτηριακή ανάλυση που συνδυάζει διάφορες μεθοδολογίες αξιολόγησης. Η πολυκριτηριακή ανάλυση επιτρέπει στους ερευνητές να λάβουν υπόψη όλες τις σχετικές διαστάσεις – από την απόδοση και την κλιμάκωση μέχρι την ευχρηστία, την επεκτασιμότητα, την ενσωμάτωση σε εικονικοποιημένα περιβάλλοντα, την υποστήριξη ασφαλείας, καθώς και την τεκμηρίωση και υποστήριξη της κοινότητας. Ακολουθούν οι βασικές μέθοδοι που χρησιμοποιούνται για τη διαμόρφωση της τελικής επιλογής:

5.3.1. Καθορισμός Κριτηρίων:

Στην αρχική φάση της ανάλυσης, είναι απαραίτητο να καθοριστούν τα κριτήρια αξιολόγησης που θα χρησιμοποιηθούν για τη σύγκριση των εργαλείων δημιουργίας κίνησης. Η επιλογή αυτών των κριτηρίων αποτελεί κρίσιμο βήμα, καθώς καθορίζει το πλαίσιο μέσα στο οποίο θα πραγματοποιηθεί η αντικειμενική αξιολόγηση και θα διαμορφωθεί η τελική επιλογή εργαλείου για εφαρμογές στα δίκτυα 5G. Συγκεκριμένα, τα κριτήρια αξιολόγησης περιλαμβάνουν:

- **Ικανότητα Δημιουργίας Κίνησης (TGC):** Αξιολογείται η δυνατότητα του εργαλείου να παράγει ρεαλιστική και ποικίλη κίνηση, που να αναπαριστά επακριβώς τις απαιτήσεις των διαφόρων υπηρεσιών 5G, όπως το eMBB, το URLLC και το mMTC.
- **Απόδοση και Κλιμάκωση (PS):** Αυτό το κριτήριο εστιάζει στην ικανότητα του εργαλείου να διαχειρίζεται υψηλά επίπεδα φορτίου, με έμφαση στην παραγωγή μεγάλου αριθμού πακέτων ανά δευτερόλεπτο (PPS) και στην αποτελεσματική κλιμάκωση σε περιβάλλοντα με τεράστιο φόρτο.
- **Ρεαλισμός Εξομοίωσης/Προσομοίωσης (ES):** Εδώ εξετάζεται σε τι βαθμό το εργαλείο έχει τη δυνατότητα προσέγγισης της πραγματικής κίνησης που θα παραγόταν σε ένα μοντέρνο δίκτυο 5G.
- **Ευκολία Χρήσης και Διαμόρφωσης (EUC):** Αξιολογείται η χρηστικότητα του εργαλείου, δηλαδή αν διαθέτει φιλικές προς το χρήστη διεπαφές (GUI, CLI) και αν οι διαδικασίες διαμόρφωσης και παραμετροποίησης του είναι απλές και κατανοητές.
- **Επεκτασιμότητα και Προσαρμοστικότητα (EC):** Εξετάζεται πόσο εύκολα μπορεί να επεκταθεί το εργαλείο μέσω scripting, API και αρθρωτής αρχιτεκτονικής, ώστε να προσαρμόζεται στις εξελισσόμενες προδιαγραφές και τις νέες απαιτήσεις των δικτύων 5G.
- **Ενσωμάτωση με Εικονικοποίηση και Cloud (IV):** Λαμβάνεται υπόψη η ικανότητα του εργαλείου να ενσωματώνεται σε σύγχρονα εικονικοποιημένα περιβάλλοντα, όπως αυτά που βασίζονται σε NFV, SDN και cloud υποδομές, για να διαμορφώνει δοκιμαστικά περιβάλλοντα που αντικατοπτρίζουν πιστά τις παραγωγικές συνθήκες.
- **Ανάλυση Καθυστέρησης και Jitter (LJ):** Αξιολογούνται οι δυνατότητες μέτρησης βασικών δεικτών απόδοσης, όπως η ολική καθυστέρηση, το jitter και η απώλεια πακέτων, που είναι κρίσιμες για εφαρμογές που απαιτούν URLLC.
- **Υποστήριξη Ασφαλείας και Κρυπτογράφησης (SE):** Εξετάζεται αν το εργαλείο μπορεί να προσομοιώσει τόσο κανονική όσο και επιθετική κίνηση, συμπεριλαμβανομένης της

υποστήριξης για κρυπτογραφημένη επικοινωνία μέσω πρωτοκόλλων όπως TLS και IPSec, ώστε να δοκιμαστούν οι μηχανισμοί ασφαλείας.

- **Παρακολούθηση και Αναφορά (MR):** Λαμβάνεται υπόψη η ενσωμάτωση δυνατοτήτων παρακολούθησης, όπως logging, real-time οπτικοποίηση και εξαγωγή δεδομένων, που διευκολύνουν την ανάλυση των αποτελεσμάτων και τη λήψη αποφάσεων.
- **Κοινότητα, Υποστήριξη και Τεκμηρίωση (CD):** Αξιολογείται η ποιότητα και η πληρότητα της τεκμηρίωσης, η ενεργότητα της κοινότητας και η συχνότητα ενημερώσεων, που διασφαλίζουν τη μακροπρόθεσμη βιωσιμότητα και υποστήριξη του εργαλείου.

5.3.2. Βαθμολόγηση Κριτηρίων:

Η αξιολόγηση κάθε εργαλείου γίνεται με βάση μια λεπτομερή και συστηματική διαδικασία που στοχεύει να μετρήσει αντικειμενικά την απόδοση του σε κάθε καθορισμένο κριτήριο. Συγκεκριμένα, κάθε εργαλείο βαθμολογείται σε κάθε κριτήριο με μια κλίμακα από 0 έως 5, όπου:

- **0:** Αντιπροσωπεύει την έλλειψη ή την ανεπαρκή εφαρμογή του συγκεκριμένου κριτηρίου.
- **5:** Αντιπροσωπεύει την εξαιρετική απόδοση και την πλήρη εφαρμογή του κριτηρίου.

Η βαθμολόγηση αυτή βασίζεται σε μια σύνθετη προσέγγιση που συνδυάζει εμπειρικές παρατηρήσεις, ανάλυση της τεκμηρίωσης των εργαλείων, αξιολόγηση δημοσιευμένων ερευνών και αποτελέσματα πρακτικών δοκιμών. Η χρήση αυτής της μεθοδολογίας επιτρέπει στους ερευνητές να συγκρίνουν αντικειμενικά τα εργαλεία με βάση ποσοτικά και ποιοτικά δεδομένα, προσφέροντας μια σαφή εικόνα των δυνατοτήτων, των περιορισμών και των πλεονεκτημάτων κάθε λύσης.
Επιπλέον, αυτή η κλίμακα βαθμολόγησης διευκολύνει την παραχώρηση σταθμίσεων σε κάθε κριτήριο, γεγονός που είναι κρίσιμο για τη σταθμισμένη πολυκριτηριακή ανάλυση. Μέσω αυτής της διαδικασίας, μπορούν να εντοπιστούν οι τομείς όπου ένα εργαλείο παρουσιάζει αδυναμίες και να συγκριθούν οι επιδόσεις τους σε σχέση με τα απαιτούμενα πρότυπα για τα δίκτυα 5G. Τέλος, η αντικειμενική αξιολόγηση βάσει μιας σαφούς και διαφανής κλίμακας επιτρέπει τη διαμόρφωση τεκμηριωμένων αποφάσεων για την τελική επιλογή του πιο κατάλληλου εργαλείου, βάσει των συνόλων επιδόσεων και της ευελιξίας που παρουσιάζει κάθε λύση.

5.3.3. Χρήση Πίνακα Απόδοσης και Σταθμισμένη Βαθμολόγηση:

Για να επιτευχθεί μια αντικειμενική σύγκριση των εργαλείων δημιουργίας κίνησης, τα αποτελέσματα των βαθμολογήσεων για κάθε κριτήριο συγκεντρώνονται σε έναν πίνακα απόδοσης. Σε αυτόν τον πίνακα, κάθε κριτήριο αξιολόγησης λαμβάνει ένα σταθμισμένο ποσοστό που αντανακλά τη σχετική του σημασία για το συγκεκριμένο περιβάλλον 5G και τις εφαρμογές που πρόκειται να δοκιμαστούν.
Η διαδικασία σταθμισμένης βαθμολόγησης επιτρέπει στους ερευνητές να αποδώσουν μεγαλύτερο βάρος σε κριτήρια που είναι κρίσιμα για συγκεκριμένες εφαρμογές. Για παράδειγμα, σε εφαρμογές που απαιτούν την εξαιρετικά χαμηλή καθυστέρηση και μικρό jitter, όπως οι εφαρμογές URLLC (Ultra-Reliable Low-Latency Communications), η μέτρηση της καθυστέρησης και του jitter θα έχει υψηλότερο βάρος σε σχέση με άλλα κριτήρια, ώστε να αντικατοπτρίζονται με

ακρίβεια οι απαιτήσεις των εφαρμογών. Με τη σταθμισμένη βαθμολόγηση, τα ποσοτικά αποτελέσματα κάθε κριτηρίου ενσωματώνονται σε ένα ενιαίο συνολικό σκορ, το οποίο αντικατοπτρίζει την ολιστική ικανότητα κάθε εργαλείου να καλύψει τις συγκεκριμένες ανάγκες του περιβάλλοντος δοκιμών.
Αυτή η μεθοδολογία δεν επιτρέπει μόνο την αντικειμενική σύγκριση μεταξύ των εργαλείων, αλλά βοηθά επίσης στην ανάδειξη των τομέων όπου κάθε εργαλείο παρουσιάζει αδυναμίες ή δυνατά σημεία. Για παράδειγμα, αν ένα εργαλείο έχει εξαιρετικές επιδόσεις στην παραγωγή ζωντανής κίνησης αλλά παρουσιάζει περιορισμούς στην ανάλυση καθυστέρησης και jitter, αυτή η ανάλυση θα επιτρέψει στους ερευνητές να λάβουν υπόψη τα σχετικά βάρη των κριτηρίων κατά την τελική απόφαση.
Η χρήση ενός πίνακα απόδοσης σε συνδυασμό με τη μέθοδο σταθμισμένης βαθμολόγησης παρέχει έτσι ένα πλήρες και διαφανές πλαίσιο για τη λήψη αποφάσεων, το οποίο στηρίζεται σε αντικειμενικά δεδομένα και επιτρέπει τη σύγκριση των εργαλείων βάσει της συνολικής τους ικανότητας να ικανοποιήσουν τις απαιτήσεις των δικτύων 5G. Αυτή η πολυκριτηριακή προσέγγιση αποτελεί θεμέλιο για την επιστημονική τεκμηρίωση της επιλογής του κατάλληλου εργαλείου, παρέχοντας μια ανεπτυγμένη βάση για την τελική απόφαση που θα στηριχθεί σε ποσοτικές και ποιοτικές μετρήσεις.

5.3.4. Πολυκριτηριακή Απόφαση:

Η τελική λήψη απόφασης σε ένα πολυκριτηριακό πλαίσιο απαιτεί την ολοκληρωμένη συνδυαστική αξιολόγηση των εργαλείων βάσει των σταθμισμένων σκορ που έχουν υπολογιστεί για κάθε καθορισμένο κριτήριο. Μέσω της εφαρμογής μεθόδων όπως η Ανάλυση Ιεραρχικής Διαδικασίας (AHP) μπορούμε να συνδυάσουμε τα επιμέρους σταθμισμένα σκορ και να παραγαχθεί ένα συνολικό αποτέλεσμα που αντικατοπτρίζει την ολική ικανότητα κάθε εργαλείου να ικανοποιεί τις απαιτήσεις ενός περιβάλλοντος 5G.
Η διαδικασία αυτή ξεκινά με τον καθορισμό βαρών για κάθε κριτήριο, τα οποία αποδίδουν τη σχετική σημασία τους στην τελική αξιολόγηση. Στη συνέχεια, για κάθε εργαλείο, τα μεμονωμένα σκορ πολλαπλασιάζονται με τα αντίστοιχα βάρη τους και αθροίζονται, παράγοντας έτσι ένα συνολικό σταθμισμένο σκορ. Αυτή η σταθμισμένη βαθμολόγηση επιτρέπει την αντικειμενική κατάταξη των εργαλείων, λαμβάνοντας υπόψη τόσο τις ποσοτικές όσο και τις ποιοτικές παραμέτρους που καθορίζουν την απόδοσή τους.

Κατανομή Βαρών:
Σε κάθε κριτήριο αποδίδεται ένα βάρος με βάση τη σχετική του σημασία για τα δίκτυα 5G. Για παράδειγμα, μπορούμε να ορίσουμε τα εξής βάρη:

- TGC: 0.15
- PS: 0.15
- ES: 0.10
- EUC: 0.10
- EC: 0.10
- IV: 0.10

- LJ: 0.10
- SE: 0.10
- MR: 0.05
- CD: 0.05

Κάθε εργαλείο βαθμολογείται σε κάθε κριτήριο με μια κλίμακα από 0 έως 5. Τα σκορ αυτά προέρχονται από εμπειρικές παρατηρήσεις, ανάλυση της τεκμηρίωσης, δημοσιευμένες μελέτες και πρακτικές δοκιμές. Για κάθε εργαλείο, το σκορ κάθε κριτηρίου πολλαπλασιάζεται με το αντίστοιχο βάρος και στη συνέχεια αθροίζονται τα σταθμισμένα σκορ. Το συνολικό αυτό σκορ αντικατοπτρίζει την ολική ικανότητα του εργαλείου να ικανοποιεί τις απαιτήσεις του περιβάλλοντος 5G.

ns-3 με το 5G-LENA Module

- **TGC: 5/5**
  Αιτιολόγηση: Το ns-3 παρέχει μεγάλη ευελιξία στη δημιουργία συνθετικής κίνησης μέσω ενσωματωμένων εφαρμογών προσομοίωσης. Δεν έχει έτοιμες λειτουργίες για κακόβουλη κίνηση, αλλά μπορεί να προσομοιώσει επιθέσεις μέσω κατάλληλης παραμετροποίησης. Η παραγωγή κίνησης ελέγχεται πλήρως από τον χρήστη με κώδικα.

1. **PS: 3/5**

Αιτιολόγηση: Υποστηρίζει σενάρια με δεκάδες έως εκατοντάδες κόμβους, αλλά σε πολύ μεγάλα δίκτυα αυξάνει σημαντικά το υπολογιστικό κόστος. Δεν λειτουργεί σε πραγματικό χρόνο (είναι simulation), παρέχει όμως ακριβή αναπαράσταση των πρωτοκόλλων. Η κλιμάκωση είναι επαρκής για ερευνητικά σενάρια μεσαίας κλίμακας.

- **ES: 5/5**
  Αιτιολόγηση: Εξαιρετική χρονική ακρίβεια και λεπτομέρεια για προσομοίωση δυναμικών συνθηκών όπως η κινητικότητα και οι handing-over.
- **EUC: 3/5**
  Αιτιολόγηση: Απαιτεί εξειδικευμένες γνώσεις προγραμματισμού και έχει μια απότομη καμπύλη μάθησης.
- **EC: 5/5**
  Αιτιολόγηση: Με ισχυρή υποστήριξη scripting και ανοικτές APIs, επιτρέπει εύκολες τροποποιήσεις και προσαρμογές στα μοντέλα κυκλοφορίας.
- **IV: 2/5**
  Αιτιολόγηση: Ως εργαλείο προσομοίωσης, δεν είναι σχεδιασμένο για ζωντανή ενσωμάτωση σε NFV/SDN ή cloud περιβάλλοντα.
- **LJ: 3/5**
  Αιτιολόγηση: Παρέχει αναλυτικές μετρήσεις στο πλαίσιο της προσομοίωσης, αλλά όχι σε πραγματικό χρόνο όπως στα live generators.
- **SE: 3/5**
  Αιτιολόγηση: Περιορισμένη υποστήριξη για προσομοίωση επιθέσεων, καθώς επικεντρώνεται περισσότερο στη λεπτομερή μοντελοποίηση των πρωτοκόλλων.
- **MR: 3/5**
  Αιτιολόγηση: Διαθέτει εργαλεία καταγραφής και ανάλυσης, αλλά οι δυνατότητες οπτικοποίησης και reporting δεν είναι τόσο εξελιγμένες.
- **CD: 4/5**

Αιτιολόγηση: Καλή τεκμηρίωση και ευρεία χρήση στην ακαδημαϊκή κοινότητα, αν και η πολυπλοκότητα του συστήματος μπορεί να δυσκολέψει τους νέους χρήστες.

SrsRAN

- **TGC: 4/5**
  Αιτιολόγηση: Παρέχει ρεαλιστική προσομοίωση 5G radio και signaling, αν και εστιάζει κυρίως στο 4G/5G SDR επίπεδο.
- **PS: 3/5**
  Αιτιολόγηση: Επικεντρώνεται σε εργαστηριακά πειράματα, με μέτριες επιδόσεις σε live περιβάλλοντα.
- **ES: 3/5**
  Αιτιολόγηση: Μπορεί να λειτουργήσει σε live περιβάλλοντα μέσω SDR, αλλά δεν έχει τις υψηλές επιδόσεις των εξειδικευμένων live traffic generators.
- **EUC: 3/5**
  Αιτιολόγηση: Απαιτεί κάποιες εξειδικευμένες γνώσεις, αν και παρέχει εργαλεία διαμόρφωσης.
- **EC: 4/5**
  Αιτιολόγηση: Διευκολύνει την προσαρμογή μέσω scripting, αλλά περιορίζεται σε ορισμένες λειτουργίες λόγω της φύσης του SDR.
- **IV: 3/5**
  Αιτιολόγηση: Παρέχει κάποιες δυνατότητες ενσωμάτωσης με εικονικοποιημένα περιβάλλοντα, αλλά δεν είναι τόσο πλήρως προσαρμοσμένο όπως τα live traffic generators.
- **LJ: 3/5**
  Αιτιολόγηση: Παρέχει βασικές μετρήσεις απόδοσης, ωστόσο οι δυνατότητες ανάλυσης είναι περιορισμένες.
- **SE: 3/5**
  Αιτιολόγηση: Εστιάζει κυρίως στην προσομοίωση 5G radio, με περιορισμένη υποστήριξη για προσομοίωση επιθέσεων.
- **MR: 3/5**
  Αιτιολόγηση: Διαθέτει βασικά εργαλεία logging, αλλά οι δυνατότητες reporting δεν είναι εξαιρετικά εξελιγμένες.
- **CD: 3/5**
  Αιτιολόγηση: Η κοινότητα είναι σε ανάπτυξη και η τεκμηρίωση βελτιώνεται, αλλά υπάρχει περιθώριο για περαιτέρω ανάπτυξη.

Open5GS με UERANSIM

- **TGC: 5/5**
  Αιτιολόγηση: Προσφέρει πλήρη υποστήριξη για 5G core πρωτόκολλα και ρεαλιστική προσομοίωση τόσο του signaling όσο και των υπηρεσιών.
- **PS: 4/5**
  Αιτιολόγηση: Εξαιρετική απόδοση σε εικονικοποιημένα περιβάλλοντα, με καλή κλιμάκωση για εφαρμογές σε ζωντανά περιβάλλοντα.

- **ES: 5/5**
  Αιτιολόγηση: Συνδυάζει προσομοίωση και live testing μέσω της ενσωμάτωσης με UERANSIM, παρέχοντας αξιόπιστη αναπαράσταση των συνθηκών λειτουργίας.
- **EUC: 5/5**
  Αιτιολόγηση: Διαθέτει φιλικό προς το χρήστη περιβάλλον και προκατασκευασμένα πρότυπα που διευκολύνουν τη διαμόρφωση σύνθετων σεναρίων.
- **EC: 5/5**
  Αιτιολόγηση: Εξαιρετικά προσαρμόσιμο μέσω scripting και ανοικτών APIs, επιτρέποντας ευέλικτη προσαρμογή στις εξελισσόμενες ανάγκες.
- **IV: 5/5**
  Αιτιολόγηση: Εξαιρετική ενσωμάτωση σε NFV, SDN και cloud περιβάλλοντα, καθιστώντας το ιδανικό για ολοκληρωμένες δοκιμές.
- **LJ: 4/5**
  Αιτιολόγηση: Παρέχει αξιόπιστες μετρήσεις απόδοσης, αν και μερικές φορές περιορίζεται από την προσομοιωτική φύση της πλατφόρμας.
- **SE: 4/5**
  Αιτιολόγηση: Μπορεί να προσομοιώσει τόσο κανονική όσο και επιθετική κίνηση, παρέχοντας δυνατότητες ασφαλείας που ανταποκρίνονται στις απαιτήσεις των δικτύων 5G.
- **MR: 5/5**
  Αιτιολόγηση: Διαθέτει καλά ανεπτυγμένα εργαλεία καταγραφής και αναφοράς, διευκολύνοντας την παρακολούθηση και ανάλυση των πειραματικών αποτελεσμάτων.
- **CD: 5/5**
  Αιτιολόγηση: Υπάρχει ενεργή κοινότητα ανοιχτού κώδικα και η τεκμηρίωση είναι επαρκής για να διευκολύνει την υιοθέτηση και τη χρήση του εργαλείου.

OMNeT++ με Simu5G

- **TGC: 5/5**
  Αιτιολόγηση: Παρέχει πολύ λεπτομερή προσομοίωση των πρωτοκόλλων και των 5G υπηρεσιών με υψηλή ακρίβεια.
- **PS: 3/5**
  Αιτιολόγηση: Ενώ προσφέρει ακριβή μοντελοποίηση, η ζωντανή παραγωγή κυκλοφορίας και η κλιμάκωση είναι περιορισμένες σε σύγκριση με εργαλεία live traffic.
- **ES: 5/5**
  Αιτιολόγηση: Εξαιρετικό για χρονικά ακριβείς προσομοιώσεις, επιτρέποντας την ανάλυση δυναμικών συνθηκών όπως η κινητικότητα και οι handing-over.
- **EUC: 3/5**
  Αιτιολόγηση: Απαιτεί εξειδικευμένες γνώσεις και έχει υψηλή καμπύλη μάθησης λόγω της πολυπλοκότητας της ρύθμισης.
- **EC: 5/5**
  Αιτιολόγηση: Παρέχει εξαιρετική προσαρμοστικότητα μέσω scripting και ανοιχτής αρχιτεκτονικής, επιτρέποντας την επέκταση των δυνατοτήτων.
- **IV: 2/5**
  Αιτιολόγηση: Λόγω του προσομοιωτικού χαρακτήρα, η ενσωμάτωσή του σε πραγματικά NFV/SDN περιβάλλοντα είναι περιορισμένη.

- **LJ: 3/5**
  Αιτιολόγηση: Παρέχει λεπτομερείς μετρήσεις μέσα στο πλαίσιο της προσομοίωσης, αλλά οι δυνατότητες παρακολούθησης σε πραγματικό χρόνο είναι περιορισμένες.
- **SE: 3/5**
  Αιτιολόγηση: Εστιάζει κυρίως στην ακριβή μοντελοποίηση και όχι στην προσομοίωση επιθέσεων, γεγονός που τον καθιστά λιγότερο κατάλληλο για ασφάλεια σε ζωντανά περιβάλλοντα.
- **MR: 3/5**
  Αιτιολόγηση: Διαθέτει εργαλεία καταγραφής, αλλά οι δυνατότητες αναφοράς και οπτικοποίησης δεν είναι τόσο εξελιγμένες.
- **CD: 4/5**
  Αιτιολόγηση: Εδραιωμένη κοινότητα και υψηλής ποιότητας τεκμηρίωση, αν και το περιβάλλον μπορεί να είναι απαιτητικό για νέους χρήστες.

TRex

- **TGC: 4/5**
  Αιτιολόγηση: Το TRex είναι σχεδιασμένο ειδικά για ζωντανή παραγωγή κίνησης, υποστηρίζοντας πλήρως ποικίλα σενάρια 5G (eMBB, URLLC, mMTC) και προσφέροντας υψηλή πιστότητα στην αναπαράσταση των πρωτοκόλλων.
- **PS: 5/5**
  Αιτιολόγηση: Με υψηλά επίπεδα PPS και χρήση DPDK, το TRex επιτυγχάνει εξαιρετική απόδοση και μπορεί να παράγει μεγάλη ποσότητα ζωντανής κίνησης σε περιβάλλοντα υψηλού φόρτου.
- **ES: 4/5**
  Αιτιολόγηση: Επικεντρώνεται στη ζωντανή παραγωγή κίνησης, προσφέροντας αξιόπιστα δεδομένα σε πραγματικό χρόνο, αν και δεν παρέχει την ίδια λεπτομέρεια προσομοίωσης πρωτοκόλλων όπως οι προσομοιωτές.
- **EUC: 5/5**
  Αιτιολόγηση: Διαθέτει φιλικό προς το χρήστη γραφικό περιβάλλον και καλά τεκμηριωμένα APIs, διευκολύνοντας την αυτοματοποίηση και τη γρήγορη παραμετροποίηση των σεναρίων δοκιμών.
- **EC: 4/5**
  Αιτιολόγηση: Μέσω scripting και ανοιχτών APIs, το TRex είναι εξαιρετικά προσαρμόσιμο και επιτρέπει την εύκολη ενσωμάτωση πρόσθετων modules, καθιστώντας το εργαλείο εξαιρετικά ευέλικτο στις μεταβαλλόμενες ανάγκες.
- **IV: 4/5**
  Αιτιολόγηση: Το TRex ενσωματώνεται άψογα σε NFV, SDN και cloud περιβάλλοντα, διευκολύνοντας τη χρήση του σε δοκιμαστικές πλατφόρμες που αντικατοπτρίζουν τις υποδομές παραγωγής.
- **LJ: 4/5**
  Αιτιολόγηση: Διαθέτει ενσωματωμένες λειτουργίες για ακριβή μέτρηση καθυστέρησης, jitter και απώλειας πακέτων, απαραίτητες για την αξιολόγηση εφαρμογών URLLC.
- **SE: 3/5**
  Αιτιολόγηση: Παρέχει δυνατότητες προσομοίωσης επιθέσεων και κρυπτογράφησης, αν και μπορεί να υπάρχουν ορισμένοι περιορισμοί ως προς την εξειδίκευση σε επιθετικά σενάρια.
- **MR: 5/5**

Αιτιολόγηση: Ενσωματωμένα εργαλεία παρακολούθησης και προκαθορισμένοι πίνακες ελέγχου παρέχουν λεπτομερή και άμεση αναφορά των επιδόσεων, διευκολύνοντας την ανάλυση.

- **CD: 5/5**
  Αιτιολόγηση: Διαθέτει ενεργή κοινότητα, πλούσια τεκμηρίωση και συχνές ενημερώσεις, που το καθιστούν ένα από τα πιο αξιόπιστα εργαλεία ανοιχτού κώδικα για τη ζωντανή παραγωγή κίνησης.

Mininet με SDN

- **TGC: 2/5**
  Αιτιολόγηση: Το Mininet επικεντρώνεται κυρίως στην προσομοίωση και διαχείριση δομών δικτύου, και όχι στην παραγωγή ρεαλιστικής κίνησης.
- **PS: 3/5**
  Αιτιολόγηση: Είναι ικανό να προσομοιώσει δίκτυα, αλλά οι επιδόσεις του ως εργαλείο παραγωγής ζωντανής κίνησης είναι περιορισμένες.
- **ES: 4/5**
  Αιτιολόγηση: Παρέχει ακριβή προσομοίωση της δομής δικτύου, αλλά δεν έχει σχεδιαστεί για ζωντανή παραγωγή κίνησης σε υψηλές ποσότητες.
- **EUC: 4/5**
  Αιτιολόγηση: Διαθέτει εύχρηστα εργαλεία διαμόρφωσης για την προσομοίωση δικτυακών υποδομών, καθιστώντας το εργαλείο φιλικό προς το χρήστη.
- **EC: 3/5**
  Αιτιολόγηση: Ενώ προσφέρει κάποιες δυνατότητες προσαρμογής, οι επιλογές του είναι περιορισμένες σε σύγκριση με εργαλεία που έχουν σχεδιαστεί για live traffic generation.
- **IV: 5/5**
  Αιτιολόγηση: Εξαιρετική ενσωμάτωση σε εικονικοποιημένα περιβάλλοντα και υποδομές SDN, ιδανική για δοκιμές εικονικών δικτύων.
- **LJ: 2/5**
  Αιτιολόγηση: Δεν εστιάζει κυρίως στη μέτρηση επιδόσεων όπως η καθυστέρηση ή το jitter, αφού ο κύριος στόχος του είναι η προσομοίωση της δομής.
- **SE: 2/5**
  Αιτιολόγηση: Δεν διαθέτει εξειδικευμένες δυνατότητες για προσομοίωση επιθέσεων ή ασφάλειας, καθώς εστιάζει κυρίως στη διαχείριση της δομής του δικτύου.
- **MR: 3/5**
  Αιτιολόγηση: Παρέχει βασικές λειτουργίες καταγραφής και παρακολούθησης, αλλά οι δυνατότητες αναφοράς είναι περιορισμένες σε σύγκριση με εργαλεία παραγωγής ζωντανής κίνησης.
- **CD: 4/5**
  Αιτιολόγηση: Διαθέτει καλή υποστήριξη και τεκμηρίωση από την κοινότητα της εικονικοποίησης δικτύων, γεγονός που διευκολύνει την υιοθέτηση του.

TeraVM

- TGC: 4/5
  Αιτιολόγηση: Το TeraVM έχει σχεδιαστεί για τη ζωντανή παραγωγή κυκλοφορίας, προσφέροντας εξαιρετική ρεαλιστικότητα και υποστήριξη για ποικίλα σενάρια 5G (eMBB, URLLC, mMTC). Η ικανότητά του να δημιουργεί ρεαλιστική κυκλοφορία το καθιστά ιδανικό για περιβάλλοντα όπου απαιτείται πλήρης αναπαράσταση τόσο των κανονικών όσο και των επιθετικών (malicious) μοτίβων.
- PS: 4/5
  Αιτιολόγηση: Χάρη στη χρήση τεχνολογιών όπως το DPDK και την υποστήριξη πολυπύρηνης επεξεργασίας, το TeraVM καταφέρνει υψηλά επίπεδα πακέτων ανά δευτερόλεπτο (PPS) και μπορεί να διαχειριστεί μεγάλα φορτία κυκλοφορίας, κάτι που είναι κρίσιμο για την προσομοίωση περιβαλλόντων 5G με υψηλή ζωντανή κυκλοφορία.
- ES: 4/5
  Αιτιολόγηση: Το TeraVM λειτουργεί ως live traffic generator, παρέχοντας ρεαλιστικά δεδομένα σε πραγματικό χρόνο. Αυτό το χαρακτηριστικό επιτρέπει την αξιολόγηση της λειτουργικής απόδοσης και της ανθεκτικότητας των συστημάτων υπό συνθήκες που προσομοιάζουν ένα πραγματικό περιβάλλον δικτύου.
- EUC: 4/5
  Αιτιολόγηση: Το εργαλείο διαθέτει φιλικό προς το χρήστη γραφικό περιβάλλον καθώς και πλήρως τεκμηριωμένα APIs, που διευκολύνουν την αυτοματοποίηση μέσω scripting και την παραμετροποίηση σύνθετων σεναρίων δοκιμών. Η εύκολη διαμόρφωση μειώνει την καμπύλη μάθησης και επιταχύνει την ανάπτυξη των πειραμάτων.
- EC: 4/5
  Αιτιολόγηση: Η υποστήριξη scripting και οι ανοικτές APIs καθιστούν το TeraVM εξαιρετικά προσαρμόσιμο, επιτρέποντας την εύκολη ενσωμάτωση πρόσθετων modules και τη συνεχή ενημέρωση του εργαλείου για να ανταποκρίνεται στις μεταβαλλόμενες ανάγκες των δικτύων 5G.
- IV: 4/5
  Αιτιολόγηση: Το TeraVM ενσωματώνεται άψογα σε περιβάλλοντα NFV, SDN και cloud, επιτρέποντας την ανάπτυξη του σε δοκιμαστικές πλατφόρμες που αντικατοπτρίζουν τις πραγματικές υποδομές παραγωγής.
- LJ: 4/5
  Αιτιολόγηση: Διαθέτει ενσωματωμένες δυνατότητες μέτρησης κρίσιμων δεικτών όπως η καθυστέρηση, το jitter και η απώλεια πακέτων, που είναι απαραίτητες για εφαρμογές με πολύ αυστηρές απαιτήσεις (π.χ. URLLC).
- SE: 4/5
  Αιτιολόγηση: Το TeraVM παρέχει δυνατότητες προσομοίωσης επιθέσεων και κρυπτογράφησης, επιτρέποντας την αναπαράσταση ρεαλιστικών σεναρίων ασφαλείας. Παρόλο που μπορεί να έχει ορισμένους περιορισμούς στην εξειδίκευση σε πολύ εξελιγμένα επιθετικά σενάρια, οι δυνατότητές του είναι επαρκείς για την αξιολόγηση των μηχανισμών ασφαλείας.
- MR: 4/5
  Αιτιολόγηση: Με ενσωματωμένα εργαλεία παρακολούθησης, καταγραφής και προκαθορισμένους πίνακες ελέγχου, το TeraVM παρέχει λεπτομερή και άμεση αναφορά των επιδόσεων, διευκολύνοντας την ανάλυση των αποτελεσμάτων.

- CD: 3/5
  Αιτιολόγηση: Επειδή το TeraVM είναι ιδιόκτητο, η υποστήριξη και η τεκμηρίωση παρέχονται κυρίως από τον προμηθευτή, με περιορισμένη κοινότητα σε σχέση με τα εργαλεία ανοιχτού κώδικα. Αυτό μπορεί να οδηγήσει σε λιγότερη ευελιξία και ανοιχτότητα στην ανάπτυξη, αλλά ταυτόχρονα προσφέρει επαγγελματική υποστήριξη και ολοκληρωμένη τεκμηρίωση.

Wireshark

Παρά το γεγονός ότι το Wireshark δεν είναι εργαλείο δημιουργίας κυκλοφορίας, αλλά κυρίως αναλυτής δικτύου, μπορούμε να το αξιολογήσουμε βάσει των παρακάτω κριτηρίων ως συμπληρωματικό εργαλείο για τη παρακολούθηση και ανάλυση της κυκλοφορίας σε περιβάλλοντα 5G.

- TGC: 0/5
  Αιτιολόγηση: Το Wireshark δεν έχει σχεδιαστεί για να δημιουργεί κυκλοφορία, αλλά για την ανάλυση και καταγραφή της κυκλοφορίας που ήδη διακινείται στο δίκτυο.
- PS: 0/5
  Αιτιολόγηση: Δεν σχετίζεται με την παραγωγή κυκλοφορίας, επομένως δεν παρέχει δυνατότητες ζωντανής παραγωγής ή κλιμάκωσης.
- ES: 0/5
  Αιτιολόγηση: Επειδή δεν παράγει κυκλοφορία, δεν εφαρμόζεται το συγκεκριμένο κριτήριο στο Wireshark.
- EUC: 5/5
  Αιτιολόγηση: Το Wireshark διαθέτει ένα εξαιρετικά φιλικό γραφικό περιβάλλον, το οποίο επιτρέπει την εύκολη παρακολούθηση, ανάλυση και οπτικοποίηση της κυκλοφορίας.
- EC: 2/5
  Αιτιολόγηση: Παρόλο που μπορεί να επεκταθεί με πρόσθετα dissectors και plugins, η λειτουργία του περιορίζεται στην ανάλυση και δεν υποστηρίζει ενεργά την παραγωγή κυκλοφορίας.
- IV: 3/5
  Αιτιολόγηση: Το Wireshark μπορεί να χρησιμοποιηθεί σε διάφορα περιβάλλοντα, συλλέγοντας δεδομένα από πολλαπλές πηγές, αλλά δεν είναι εργαλείο παραγωγής, επομένως οι δυνατότητες ενσωμάτωσης αξιολογούνται περιορισμένα.
- LJ: 3/5
  Αιτιολόγηση: Παρέχει βασικές δυνατότητες ανάλυσης μετρήσεων όπως η καθυστέρηση και το jitter μέσω της ανάλυσης πακέτων, αν και δεν έχει σχεδιαστεί για live μέτρηση επιδόσεων.
- SE: 0/5
  Αιτιολόγηση: Το Wireshark δεν έχει σχεδιαστεί για την προσομοίωση επιθέσεων ή την παραγωγή κρυπτογραφημένης κυκλοφορίας, αλλά μπορεί να χρησιμοποιηθεί για ανάλυση κρυπτογραφημένων δεδομένων.
- MR: 5/5

Αιτιολόγηση: Το Wireshark ξεχωρίζει ως εργαλείο παρακολούθησης, προσφέροντας εκτενή λειτουργικότητα καταγραφής, οπτικοποίησης και ανάλυσης των δικτυακών δεδομένων.

- CD: 5/5
  Αιτιολόγηση: Διαθέτει εξαιρετική τεκμηρίωση, ενεργή κοινότητα και μεγάλη χρήση στην παγκόσμια αγορά, καθιστώντας το ένα από τα πιο αξιόπιστα εργαλεία για ανάλυση δικτύου.

Iperf3

- **TGC: 2/5**
  Αιτιολόγηση: Επικεντρώνεται κυρίως στη μέτρηση ρυθμών μετάδοσης, χωρίς να παρέχει πλήρη ικανότητα δημιουργίας ρεαλιστικής κίνησης.
- **PS: 4/5**
  Αιτιολόγηση: Μπορεί να παράγει υψηλές ταχύτητες, ιδιαίτερα για throughput tests, αλλά έχει περιορισμούς όσον αφορά τη γενική παραγωγή κίνησης.
- **ES: 2/5**
  Αιτιολόγηση: Σχεδιασμένο για συγκεκριμένες δοκιμές απόδοσης και όχι για πλήρη προσομοίωση δυναμικών συνθηκών.
- **EUC: 5/5**
  Αιτιολόγηση: Εύχρηστο εργαλείο με απλή διεπαφή γραμμής εντολών, που καθιστά τη χρήση του πολύ προσβάσιμη.
- **EC: 2/5**
  Αιτιολόγηση: Παρέχει περιορισμένες επιλογές παραμετροποίησης πέραν των βασικών ρυθμίσεων.
- **IV: 3/5**
  Αιτιολόγηση: Μπορεί να ενσωματωθεί σε διάφορα περιβάλλοντα, αλλά δεν διαθέτει ολοκληρωμένες δυνατότητες live production.
- **LJ: 3/5**
  Αιτιολόγηση: Επιτρέπει τη μέτρηση βασικών δεικτών, αλλά όχι με την ακρίβεια που απαιτείται για λεπτομερή ανάλυση URLLC.
- **SE: 1/5**
  Αιτιολόγηση: Δεν έχει σχεδιαστεί για προσομοίωση επιθέσεων ή κρυπτογραφημένης κίνησης.
- **MR: 3/5**
  Αιτιολόγηση: Παρέχει βασικά δεδομένα μέτρησης, αλλά τα εργαλεία αναφοράς του είναι περιορισμένα.
- **CD: 5/5**
  Αιτιολόγηση: Διαθέτει εξαιρετική τεκμηρίωση και μια μεγάλη, ενεργή κοινότητα χρηστών.

Scapy

- **TGC: 3/5**
  Αιτιολόγηση: Προσφέρει υψηλή ευελιξία στη δημιουργία προσαρμοσμένων πακέτων και υποστηρίζει πολλαπλά πρωτόκολλα, αλλά απαιτεί σημαντικές γνώσεις προγραμματισμού για πλήρη αξιοποίηση.
- **PS: 2/5**

Αιτιολόγηση: Δεν έχει σχεδιαστεί για παραγωγή μεγάλης ποσότητας κίνησης, αλλά για συγκεκριμένες και εξειδικευμένες εργασίες.

- **ES: 3/5**
  Αιτιολόγηση: Μπορεί να χρησιμοποιηθεί για synthethic traffic generation, αλλά όχι για ζωντανή παραγωγή δεδομένων σε μεγάλες κλίμακες.
- **EUC: 3/5**
  Αιτιολόγηση: Απαιτεί επαρκείς γνώσεις προγραμματισμού, κάτι που μπορεί να δυσχεράνει τους νέους χρήστες.
- **EC: 5/5**
  Αιτιολόγηση: Εξαιρετικά προσαρμόσιμο μέσω scripting, επιτρέποντας τη δημιουργία πολύ εξειδικευμένων σεναρίων και την ενσωμάτωση νέων πρωτοκόλλων.
- **IV: 3/5**
  Αιτιολόγηση: Μπορεί να ενσωματωθεί σε διάφορα περιβάλλοντα, αλλά δεν είναι σχεδιασμένο για ζωντανή παραγωγή κίνησης σε μεγάλη κλίμακα.
- **LJ: 2/5**
  Αιτιολόγηση: Δεν προσφέρει ενσωματωμένες δυνατότητες για λεπτομερή μέτρηση επιδόσεων σε live περιβάλλον.
- **SE: 4/5**
  Αιτιολόγηση: Με τη δημιουργία προσαρμοσμένων πακέτων, μπορεί να χρησιμοποιηθεί για τη προσομοίωση επιθετικών σεναρίων και ανωμαλιών.
- **MR: 2/5**
  Αιτιολόγηση: Παρέχει βασικές λειτουργίες καταγραφής, αλλά οι δυνατότητες αναφοράς και οπτικοποίησης είναι περιορισμένες.
- **CD: 4/5**
  Αιτιολόγηση: Διαθέτει καλή τεκμηρίωση και ενεργή κοινότητα, αλλά η πολυπλοκότητα του εργαλείου μπορεί να δυσκολέψει τους αρχάριους.

D-ITG

- **TGC: 3/5**
  Αιτιολόγηση: Προσφέρει δυνατότητες δημιουργίας συνθετικής κίνησης για διάφορα πρωτόκολλα, αλλά έχει λιγότερη ευελιξία και προσαρμοστικότητα σε σύγκριση με εργαλεία που εστιάζουν αποκλειστικά στη ζωντανή παραγωγή.
- **PS: 3/5**
  Αιτιολόγηση: Ικανό να παράγει κίνηση σε επίπεδα που επαρκούν για εργαστηριακές δοκιμές, αλλά με περιορισμούς όταν πρόκειται για πραγματική ζωντανή παραγωγή σε μεγάλης κλίμακας περιβάλλοντα.
- **ES: 3/5**
  Αιτιολόγηση: Επικεντρώνεται κυρίως στη συνθετική παραγωγή και δεν παρέχει τις δυνατότητες ζωντανής παραγωγής που διαθέτουν τα κορυφαία εργαλεία.
- **EUC: 3/5**
  Αιτιολόγηση: Παρέχει βασικές δυνατότητες ρύθμισης, αλλά το περιβάλλον του μπορεί να μην είναι τόσο φιλικό προς το χρήστη όσο αυτό των εργαλείων με γραφικό περιβάλλον.
- **EC: 3/5**
  Αιτιολόγηση: Είναι προσαρμόσιμο, αλλά οι επιλογές επέκτασης είναι περιορισμένες σε σύγκριση με εργαλεία με ισχυρές δυνατότητες scripting.
- **IV: 3/5**

Αιτιολόγηση: Μπορεί να ενσωματωθεί σε εικονικοποιημένα περιβάλλοντα, αλλά δεν έχει σχεδιαστεί για ζωντανή παραγωγή μεγάλης ποσότητας κίνησης.

- **LJ: 3/5**
  Αιτιολόγηση: Επιτρέπει τη μέτρηση βασικών δεικτών, αλλά η ακρίβεια και η λεπτομέρεια των μετρήσεων δεν είναι τόσο υψηλές.
- **SE: 2/5**
  Αιτιολόγηση: Δεν είναι ιδιαίτερα εξειδικευμένο για προσομοίωση επιθέσεων ή για την παραγωγή κρυπτογραφημένης κίνησης.
- **MR: 3/5**
  Αιτιολόγηση: Παρέχει βασικές λειτουργίες καταγραφής, αλλά οι δυνατότητες αναφοράς είναι περιορισμένες.
- **CD: 3/5**
  Αιτιολόγηση: Η τεκμηρίωση είναι επαρκής, αλλά η υποστήριξη της κοινότητας είναι λιγότερο ενεργή συγκριτικά με τα πιο δημοφιλή εργαλεία.

Metasploit

- **TGC: 2/5**
  Αιτιολόγηση: Ενώ είναι εξαιρετικό για την προσομοίωση επιθέσεων και επιθετικών σεναρίων, δεν είναι σχεδιασμένο για γενική παραγωγή κίνησης.
- **PS: 2/5**
  Αιτιολόγηση: Επικεντρώνεται κυρίως στην ανίχνευση ευπαθειών και δεν είναι βελτιστοποιημένο για υψηλό throughput.
- **ES: 2/5**
  Αιτιολόγηση: Δεν παράγει ζωντανή κίνηση, αλλά εστιάζει στην προσομοίωση επιθέσεων.
- **EUC: 3/5**
  Αιτιολόγηση: Παρέχει αρκετά εργαλεία και διεπαφές, αλλά απαιτεί εξειδικευμένες γνώσεις ασφαλείας για την πλήρη αξιοποίησή του.
- **EC: 4/5**
  Αιτιολόγηση: Διαθέτει μεγάλο αριθμό modules και είναι ευέλικτο μέσω scripting, επιτρέποντας την προσαρμογή σε ποικίλα σενάρια.
- **IV: 3/5**
  Αιτιολόγηση: Μπορεί να ενσωματωθεί σε ορισμένα περιβάλλοντα, αλλά η κύρια του χρήση εστιάζει στην ασφάλεια, όχι στην παραγωγή κίνησης.
- **LJ: 1/5**
  Αιτιολόγηση: Δεν έχει σχεδιαστεί για λεπτομερείς μετρήσεις απόδοσης, καθώς εστιάζει στην προσομοίωση επιθέσεων.
- **SE: 5/5**
  Αιτιολόγηση: Είναι ένα από τα πιο ισχυρά εργαλεία για την προσομοίωση επιθέσεων και δοκιμές ασφαλείας, παρέχοντας πλήρη λειτουργικότητα σε αυτό το πεδίο.
- **MR: 3/5**
  Αιτιολόγηση: Διαθέτει βασικές λειτουργίες καταγραφής και αναφοράς, αλλά οι δυνατότητες παρακολούθησης επιδόσεων είναι περιορισμένες.
- **CD: 5/5**

Αιτιολόγηση: Μεγάλη, ενεργή κοινότητα και εξαιρετική τεκμηρίωση, που το καθιστούν ένα από τα πιο δημοφιλή και ευρέως χρησιμοποιούμενα εργαλεία στον χώρο της ασφάλειας.

LOIC (Low Orbit Ion Cannon)

- **TGC: 1/5**
  Αιτιολόγηση: Σχεδιάστηκε κυρίως για DoS επιθέσεις και έχει πολύ περιορισμένες δυνατότητες παραγωγής γενικής κίνησης.
- **PS: 1/5**
  Αιτιολόγηση: Η απόδοσή του είναι χαμηλή, και δεν μπορεί να παράγει κίνηση σε επίπεδα που απαιτούνται για ρεαλιστικές δοκιμές.
- **ES: 1/5**
  Αιτιολόγηση: Είναι απλό εργαλείο σχεδιασμένο για βασικές DoS επιθέσεις, χωρίς τη δυνατότητα προσομοίωσης σύνθετων συνθηκών.
- **EUC: 2/5**
  Αιτιολόγηση: Αν και η διεπαφή του είναι απλή, οι δυνατότητες παραμετροποίησης είναι πολύ περιορισμένες.
- **EC: 1/5**
  Αιτιολόγηση: Δεν προσφέρει δυνατότητες επεκτασιμότητας ή προσαρμογής μέσω scripting.
- **IV: 1/5**
  Αιτιολόγηση: Δεν είναι σχεδιασμένο για ενσωμάτωση σε σύγχρονα εικονικοποιημένα περιβάλλοντα ή cloud υποδομές.
- **LJ: 1/5**
  Αιτιολόγηση: Δεν παρέχει εργαλεία μέτρησης επιδόσεων.
- **SE: 1/5**
  Αιτιολόγηση: Παράγει απλές επιθέσεις DoS, χωρίς να υποστηρίζει προσομοίωση εξελιγμένων επιθέσεων ή κρυπτογράφησης.
- **MR: 1/5**
  Αιτιολόγηση: Δεν διαθέτει λειτουργίες παρακολούθησης ή αναφοράς.
- **CD: 2/5**
  Αιτιολόγηση: Η υποστήριξη και η τεκμηρίωση είναι περιορισμένες, καθιστώντας το εργαλείο λιγότερο αξιόπιστο για επιστημονικές μελέτες.

Η αξιολόγηση των εργαλείων βασιζόμενη στα παραπάνω κριτήρια καταδεικνύει ότι τα εργαλεία που προσφέρουν ζωντανή παραγωγή κίνησης και υψηλή προσαρμοστικότητα, όπως το TRex και το Open5GS με UERANSIM, ξεχωρίζουν ως τα πιο ολοκληρωμένα και αξιόπιστα για εφαρμογές στα δίκτυα 5G. Ενώ τα simulation εργαλεία (π.χ. ns-3 με 5G-LENA και OMNeT++ με Simu5G) παρέχουν εξαιρετική λεπτομέρεια και ακρίβεια στη μοντελοποίηση των πρωτοκόλλων, έχουν περιορισμούς όσον αφορά την παραγωγή ζωντανής κίνησης και την κλιμάκωση, που είναι απαραίτητες για δοκιμές απόδοσης και ασφαλείας σε ρεαλιστικά περιβάλλοντα.

Η δοκιμή δικτύων 5G απαιτεί εργαλεία που μπορούν να δημιουργήσουν ρεαλιστική κυκλοφορία – συμπεριλαμβανομένων τόσο κανονικών όσο και επιθετικών μοτίβων – ενώ παράλληλα υποστηρίζουν πλήρως τις λειτουργίες του 5G (eMBB, URLLC, mMTC). Η ιδανική λύση θα

πρέπει επίσης να διευκολύνει τις δοκιμές ασφαλείας (π.χ. εισαγωγή ανωμαλιών, κρυπτογραφημένη κυκλοφορία), να μπορεί να αναπτυχθεί σε φυσικά, εικονικά και cloud περιβάλλοντα και να κλιμακώνεται για την προσομοίωση μαζικών πληθυσμών IoT συσκευών. Στην παρούσα εργασία, συγκρίνουμε κορυφαία εργαλεία ανοιχτού κώδικα βάσει αυτών των κριτηρίων και προτείνουμε την πλέον κατάλληλη λύση, στηρίζοντας την ανάλυση μας σε ακαδημαϊκές μελέτες και αξιολογήσεις της βιομηχανίας.

5.3.5 Πίνακας Αποτελεσμάτων

Tool	TGC	PS	ES	EU	EC	IV	LJ	SE	MR	CD	Overall
ns-3 with 5G-LENA Module	5	3	5	3	5	2	3	3	3	4	3.6
srsRAN	4	3	3	3	4	3	3	3	3	3	3.1
Open5GS with UERANSIM	5	4	5	5	5	5	4	4	5	5	4.7
OMNeT++ with Simu5G	5	3	5	3	5	2	3	3	3	4	3.6
TRex	4	5	4	5	4	4	4	3	5	5	4.3
Mininet with SDN	2	3	4	4	3	5	3	2	3	4	3.3
TeraVM	4	4	4	4	4	4	4	4	4	4	3.9
Wireshark	0	0	0	5	2	3	3	0	5	5	2.3*
Iperf3	2	4	2	5	2	3	3	1	3	5	3.0
Scapy	3	2	3	3	5	3	2	4	2	4	3.1
D-ITG	3	3	3	3	3	3	3	2	3	3	2.9
Metasploit	2	2	2	3	4	3	1	5	3	5	3.0
LOIC (Low Orbit Ion Cannon)	1	1	1	2	1	1	1	1	1	2	1.2

Πίνακας 5.1 Αξιολόγηση των εργαλείων.

Στον πίνακα, οι συντομογραφίες των κριτηρίων είναι: TGC = Traffic Generation Capability, PS = Performance & Scalability, ES = Emulation vs Simulation, EUC = Ease of Use & Configuration, EC = Expandability & Customizability, IV = Integration with Virtualization, LJ = Latency & Jitter Analysis, SE = Security & Encryption Support, MR = Monitoring & Reporting, CD = Community & Documentation.

Πλατφόρμες Προσομοίωσης Δικτύου (ns-3 και Simu5G)

Οι διακριτοί προσομοιωτές, όπως το ns-3 (με το 5G-LENA Module) και το Simu5G (που βασίζεται στο OMNeT++), παρέχουν ολιστική προσομοίωση του δικτύου 5G από άκρη σε άκρη. Αυτά τα εργαλεία υλοποιούν τα επίπεδα πρωτοκόλλων του 5G NR και μπορούν να προσομοιώσουν σενάρια για τις υπηρεσίες eMBB, URLLC και mMTC σύμφωνα με τις προδιαγραφές 3GPP. Για παράδειγμα, το Simu5G επιτρέπει την πλήρη προσομοίωση του data plane σε υλοποιήσεις 5G NR, παρέχοντας δυνατότητες προσομοίωσης που επιτρέπουν στους ερευνητές να ορίσουν σύνθετα μοντέλα κυκλοφορίας (π.χ. ροές βίντεο για eMBB ή περιοδικές ροές μικροδεδομένων για IoT) και να εισάγουν ανωμαλίες για δοκιμές ασφαλείας. Τέτοιοι προσομοιωτές μπορούν να προσομοιώσουν χιλιάδες συσκευές, περιοριζόμενοι μόνο από τους υπολογιστικούς πόρους. Αν και η ανάπτυξή τους είναι ευέλικτη – τρέχουν σε κοινά λειτουργικά συστήματα και μπορούν να containerized – λειτουργούν κυρίως ως κλειστές προσομοιωτικές πλατφόρμες και όχι ως γεννήτριες ζωντανής κυκλοφορίας σε λειτουργικά δίκτυα. Επομένως, ενώ εξαιρεθούν στη μοντελοποίηση 5G σε βάθος και στην αξιολόγηση αλγορίθμων, είναι λιγότερο κατάλληλα για live δοκιμές ασφαλείας δικτύου.

Εξομοιωτές 5G UE/RAN (UERANSIM, my5G-RANTester, PacketRusher)

Εργαλεία που έχουν σχεδιαστεί ειδικά για την προσομοίωση 5G user equipment (UE) και στοιχείων της πρόσβασης 5G (RAN) προσφέρουν πλήρη υποστήριξη των πρωτοκόλλων και δημιουργούν ρεαλιστική κυκλοφορία. Ένα από τα κορυφαία παραδείγματα είναι το UERANSIM, ένας ανοιχτού κώδικα προσομοιωτής 5G UE και gNodeB, ο οποίος υλοποιεί τα πρωτόκολλα NAS και RAN (με απλουστευμένο φυσικό επίπεδο) ώστε να επιτρέπει τη δοκιμή 5G core δικτύων με τη χρήση προσομοιωμένων κινητών και σταθμών βάσης. Το UERANSIM δημιουργεί εικονικές συσκευές που συνδέονται με το 5G core (π.χ. Open5GS ή free5GC) και δημιουργεί πραγματικά user-plane tunnels, επιτρέποντας την παραγωγή κυκλοφορίας (π.χ. TCP/UDP flows) μέσω αυτών των συσκευών. Αυτό επιτρέπει την προσομοίωση ρεαλιστικής κυκλοφορίας, όπως διαδικτυακές συνεδρίες, ροές βίντεο ή IoT telemetry, καθώς και την εισαγωγή κακόβουλων μοτίβων (π.χ. σάρωση ή εκρήξεις DDoS). Το UERANSIM έχει αποδειχθεί ιδιαίτερα κλιμακούμενο – μία μόνο του διαδικασία μπορεί να προσομοιώσει έως 512 UEs, ενώ πολλαπλές διεργασίες μπορούν να τρέξουν παράλληλα, παρέχοντας δυνατότητα για μαζική προσομοίωση. Επιπλέον, έχει αποδειχθεί ότι μπορεί να αναπτυχθεί σε Kubernetes clusters, προσφέροντας ευελιξία στην ανάπτυξη σε φυσικά και cloud περιβάλλοντα.

Γενικές Γεννήτριες Κυκλοφορίας (TRex, D-ITG)

Εκτός από τους εξειδικευμένους προσομοιωτές 5G, υπάρχουν και εργαλεία όπως το TRex και το D-ITG που μπορούν να παράγουν μεγάλους όγκους IP κυκλοφορίας. Το TRex, ένας ανοιχτού κώδικα, υψηλής απόδοσης γεννήτρια κυκλοφορίας, μπορεί να λειτουργήσει τόσο σε stateless όσο και σε stateful ροές, και έχει σχεδιαστεί για να stress-test δικτυακές συσκευές σε ταχύτητες που αγγίζουν τα multi-100 Gbps. Αν και το TRex δεν εστιάζει αποκλειστικά σε 5G, μέσω της αναπαραγωγής πραγματικών εφαρμογών (μέσω PCAP ή προφίλ) μπορεί να προσομοιώσει ροές eMBB και κακόβουλα burst κυκλοφορίας με ρεαλιστικές ιδιότητες. Το D-ITG, ένα ακαδημαϊκό εργαλείο, επιτρέπει την παραγωγή κυκλοφορίας με καθορισμένες στατιστικές ιδιότητες, αλλά χωρίς ενσωματωμένη υποστήριξη για 5G πρωτόκολλα, γι' αυτό χρησιμοποιείται συχνά σε συνδυασμό με εξειδικευμένους προσομοιωτές για να αυξηθεί η ρεαλιστικότητα των δοκιμών.

Συμπεράσματα και Συστάσεις

Σε σχέση με τα βασικά κριτήρια, οι εξειδικευμένοι προσομοιωτές 5G (όπως ns-3/Simu5G και UERANSIM/my5G) παρέχουν πληρέστερη κάλυψη, καθώς υποστηρίζουν πλήρως τις λειτουργίες του 5G – από την πλήρη αναπαράσταση των πρωτοκόλλων (NAS, RRC, NGAP, GTP-U) έως την

προσομοίωση χαρακτηριστικών όπως network slicing και QoS flows. Ωστόσο, τα εργαλεία αυτά συχνά λειτουργούν ως κλειστές προσομοιωτικές πλατφόρμες και δεν παράγουν ζωντανή κυκλοφορία, κάτι που είναι κρίσιμο για live testing ασφαλείας.
Από την άλλη πλευρά, γεννήτριες κυκλοφορίας όπως το TRex προσφέρουν υψηλή ρεαλιστικότητα για εφαρμογές επιπέδου 7, αλλά δεν είναι ενσωματωμένες στο 5G stack – για παράδειγμα, δεν προσομοιώνουν το signaling ή τα χαρακτηριστικά των 5G συσκευών, απαιτώντας πρόσθετη διαμόρφωση για την πλήρη αναπαράσταση 5G λειτουργιών.
Λαμβάνοντας υπόψη όλα τα κριτήρια – από την ικανότητα παραγωγής ρεαλιστικής κυκλοφορίας, την υποστήριξη για κακόβουλα μοτίβα, τη συμβατότητα με 5G, την ευελιξία ανάπτυξης και την κλιμάκωση για μαζική προσομοίωση συσκευών – η πιο συμβατή λύση για περιβάλλοντα 5G είναι η χρήση ενός εξειδικευμένου 5G UE/RAN εξομοιωτή σε συνδυασμό με ένα ανοιχτού κώδικα 5G core. Συγκεκριμένα, το UERANSIM σε συνδυασμό με ένα αξιόπιστο 5G core, όπως το Open5GS, αναδεικνύεται ως η κορυφαία επιλογή.
Αυτός ο συνδυασμός πληροί όλα τα κριτήρια:

- Παρέχει ρεαλιστική κυκλοφορία μέσω της πλήρους υποστήριξης των 5G πρωτοκόλλων, καλύπτοντας υπηρεσίες eMBB, URLLC και mMTC.
- Διευκολύνει τις δοκιμές ασφαλείας με δυνατότητα εισαγωγής κακόβουλων ή ανωμαλικών μοτίβων, καθώς και παραγωγή κρυπτογραφημένης κυκλοφορίας.
- Επιτρέπει ευέλικτη ανάπτυξη σε φυσικά, εικονικά και cloud περιβάλλοντα, καθώς έχει αποδειχθεί ότι μπορεί να κλιμακωθεί σε Kubernetes clusters και άλλες πλατφόρμες.
- Είναι σχεδιασμένο για να υποστηρίζει μαζική προσομοίωση, με τη δυνατότητα προσομοίωσης εκατοντάδων έως και χιλιάδων UEs ανά διεργασία, γεγονός που το καθιστά ιδανικό για σενάρια IoT.

Η επιλογή αυτή στηρίζεται σε επιστημονικές αναλύσεις και αξιολογήσεις της βιομηχανίας, οι οποίες υποδεικνύουν ότι το UERANSIM έχει αναγνωριστεί ως ένα “state-of-the-art 5G UE and RAN simulator” και ότι σε συνδυασμό με 5G cores όπως το Open5GS, προσφέρει σχεδόν απεριόριστη δυνατότητα κλιμάκωσης υπό την προϋπόθεση επαρκών υπολογιστικών πόρων.
Με βάση την ανάλυση και τα δεδομένα που συγκεντρώθηκαν, συνιστάται η υιοθέτηση ενός περιβάλλοντος 5G traffic generation που βασίζεται στο UERANSIM σε συνδυασμό με ένα αξιόπιστο open-source 5G core, όπως το Open5GS. Αυτή η σύνθεση ανταποκρίνεται πλήρως στις απαιτήσεις για:

- Ρεαλιστική προσομοίωση κυκλοφορίας (κανονικής και επιθετικής),
- Πλήρη υποστήριξη των πρωτοκόλλων 5G,
- Ευελιξία ανάπτυξης σε φυσικά, εικονικά και cloud περιβάλλοντα,
- Κλιμάκωση για την προσομοίωση μαζικών IoT συσκευών.

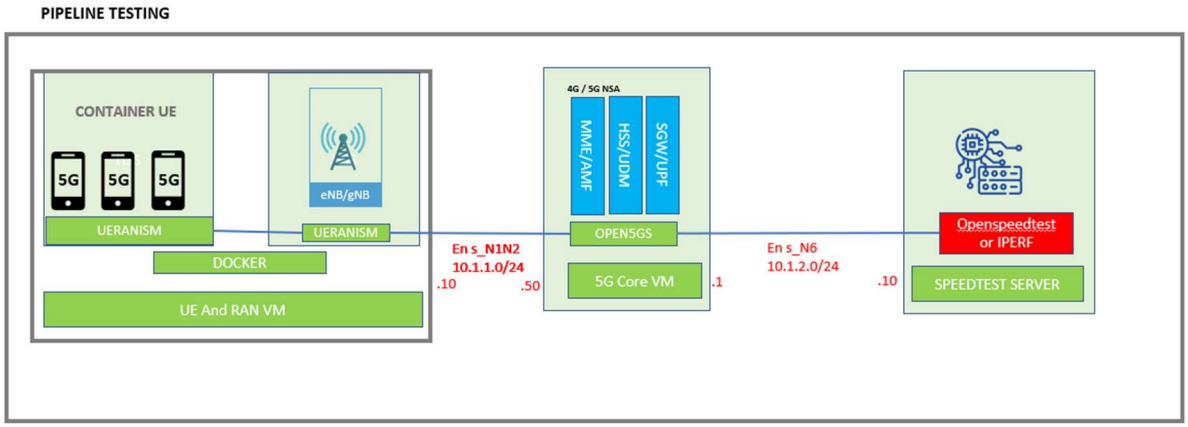
Η υιοθέτηση μιας τέτοιας λύσης θα επιτρέψει μια ολοκληρωμένη και επιστημονικά τεκμηριωμένη αξιολόγηση των δικτύων 5G, καλύπτοντας όλες τις πτυχές – από την απόδοση και την ασφάλεια μέχρι τη διαχείριση μεγάλου όγκου δεδομένων – παρέχοντας ένα αξιόπιστο υπόβαθρο για μελλοντικές βελτιώσεις και έρευνες.

6. Πειραματική Επικύρωση της Πρότασης (Proof of Concept)

Σε αυτό το κεφάλαιο παρουσιάζεται ένα **proof of concept** testbed δικτύου 5G, το οποίο υλοποιήθηκε με χρήση εργαλείων ανοιχτού κώδικα και αποσκοπεί στη δημιουργία και μελέτη κίνησης (κανονικής και κακόβουλης) σε περιβάλλον 5G. Αρχικά, περιγράφουμε τον σχεδιασμό του συστήματος και την αρχιτεκτονική της λύσης, συμπεριλαμβανομένων των βασικών συστατικών (5G core, προσομοίωση RAN, γεννήτρια κίνησης) και της τοπολογίας δικτύου. Στη συνέχεια, δίνονται λεπτομέρειες υλοποίησης – από την εγκατάσταση και ρύθμιση των εργαλείων έως τα σενάρια προσομοίωσης που εκτελέστηκαν (κανονική κίνηση HTTP και επίθεση **UDP flood**). Ακολουθούν τα πειραματικά αποτελέσματα για κάθε σενάριο, με ανάλυση της δικτυακής συμπεριφοράς υπό φυσιολογικές συνθήκες και υπό DDoS επίθεση. Τέλος, γίνεται συνολική αξιολόγηση και συζήτηση, αναλύοντας τις προκλήσεις που αντιμετωπίστηκαν κατά την υλοποίηση και ειδικές πτυχές των δικτύων 5G (όπως η καθυστέρηση και το εύρος ζώνης), καθώς και τους περιορισμούς της προτεινόμενης υλοποίησης.

6.1 Σχεδιασμός και Αρχιτεκτονική Συστήματος

Το προτεινόμενο σύστημα βασίζεται σε μια εικονική υλοποίηση δικτύου 5G standalone, η οποία περιλαμβάνει όλα τα κύρια στοιχεία ενός πραγματικού δικτύου: ένα **5G Core** δίκτυο, μια προσομοίωση του ασύρματου δικτύου (**Radio Access Network - RAN**) με τερματικές συσκευές, και μηχανισμούς **παραγωγής κίνησης** για τη δημιουργία ροών δεδομένων. Στόχος του σχεδιασμού είναι η δημιουργία ενός ρεαλιστικού αλλά και διαχειρίσιμου testbed σε ένα μόνο VM (VirtualBox), ακολουθώντας τις βέλτιστες πρακτικές από το επίσημο tutorial του Open5GS. Στο Σχήμα 5.1 (σχηματική αρχιτεκτονική) θα μπορούσαν να διακριθούν τα επιμέρους τμήματα του συστήματος, όμως εδώ περιγράφουμε λεκτικά την αρχιτεκτονική και τη διασύνδεση τους.



Σχήμα 6.1 Open5gs[61] Βασική Αρχιτεκτονική του συνδυασμού open5gs με το ueransim

6.1.1 Επιλεγμένα Συστατικά (5G Core, Προσομοίωση Ραδιοδικτύου, Παραγωγή Κίνησης)

- **5G Core – Open5GS**: Ως πυρήνας του δικτύου χρησιμοποιείται το Open5GS, ένα δημοφιλές λογισμικό ανοικτού κώδικα που υλοποιεί πλήρως το 5G Core (5GC) σύμφωνα με τις προδιαγραφές 3GPP. Το Open5GS παρέχει όλα τα βασικά network functions του 5G Standalone (AMF, SMF, UPF, UDM, NSSF, κ.λπ.), ενώ υποστηρίζει και λειτουργίες 4G EPC για backward compatibility. Πρόκειται για υλοποίηση γραμμένη σε γλώσσα C, η οποία μπορεί να τρέξει σε τυπικό εξοπλισμό x86/ARM με Linux, καθιστώντας εφικτή τη χρήση της ακόμα και σε απλό server ή VM(Dolente F, Garroppo R, Pagano M[63]). Η ευκολία εγκατάστασης και η σταθερότητα που προσφέρει το Open5GS το έχουν κάνει δημοφιλές στην ερευνητική κοινότητα, συμμετέχοντας σε μεγάλα testbeds για δοκιμές νέων υπηρεσιών.
  Παρότι δεν αποτελεί λύση εμπορικής κλάσης, θεωρείται κατάλληλο ως *δωρεάν* πλατφόρμα για πειραματισμό και δοκιμές (Dolente F, Garroppo R, Pagano M[63])Στο πλαίσιο αυτής της υλοποίησης, το Open5GS επιλέχθηκε ώστε να λειτουργήσει ως ο πυρήνας του δικτύου 5G, αναλαμβάνοντας όλες τις λειτουργίες ελέγχου (signaling) και μεταγωγής (user plane) που απαιτούνται για τη σύνδεση των UEs με το δίκτυο.
- **Προσομοίωση RAN – UERANSIM**: Για την προσομοίωση του ασύρματου τμήματος του δικτύου (Radio Access Network) και των χρηστών, χρησιμοποιείται το εργαλείο UERANSIM (UE + RAN Simulator). Το UERANSIM είναι μια σύγχρονη πλατφόρμα ανοικτού κώδικα που παρέχει προσομοίωση ενός 5G gNodeB (σταθμού βάσης) και ενός ή περισσότερων 5G User Equipment (UE) σε επίπεδο λογισμικού. Σε αντίθεση με λύσεις όπως το srsRAN που απαιτούν φυσικό ραδιοεξοπλισμό (SDR) για την εκπομπή σημάτων RF, το UERANSIM δεν εκπέμπει πραγματικά ραδιοσήματα – αντιθέτως, υλοποιεί στο λογισμικό το πρωτόκολλο 5G NR και μεταφέρει την ασύρματη σηματοδοσία μέσω συνηθισμένων συνδέσεων IP (π.χ. SCTP/IP) προς τον πυρήνα. Με αυτόν τον τρόπο, *εξομοιώνει* αυτό που συμβαίνει “πάνω στον αέρα” μεταφράζοντάς το σε μηνύματα δικτύου, κάτι που απλοποιεί σημαντικά το στήσιμο – μπορούμε να τρέξουμε ένα πλήρες

61 Open5gs

δίκτυο 5G RAN+UE σε μια μηχανή χωρίς εξειδικευμένο hardware. Το UERANSIM έχει χαρακτηριστεί ως η πρώτη υλοποίηση ανοικτού κώδικα για 5G Standalone UE/gNB και χρησιμοποιείται ευρέως για δοκιμές λειτουργικότητας 5G cores. Στο παρόν σύστημα, το UERANSIM παρέχει έναν εικονικό gNodeB που συνδέεται με το Open5GS μέσω των διεπαφών N2 (SCTP signaling) και N3 (GTP-U user plane), καθώς και μία ή περισσότερες εικονικές UEs που εγγράφονται στον πυρήνα (AMF/UDM) και λαμβάνουν IP διευθύνσεις για επικοινωνία δεδομένων μέσω του UPF.

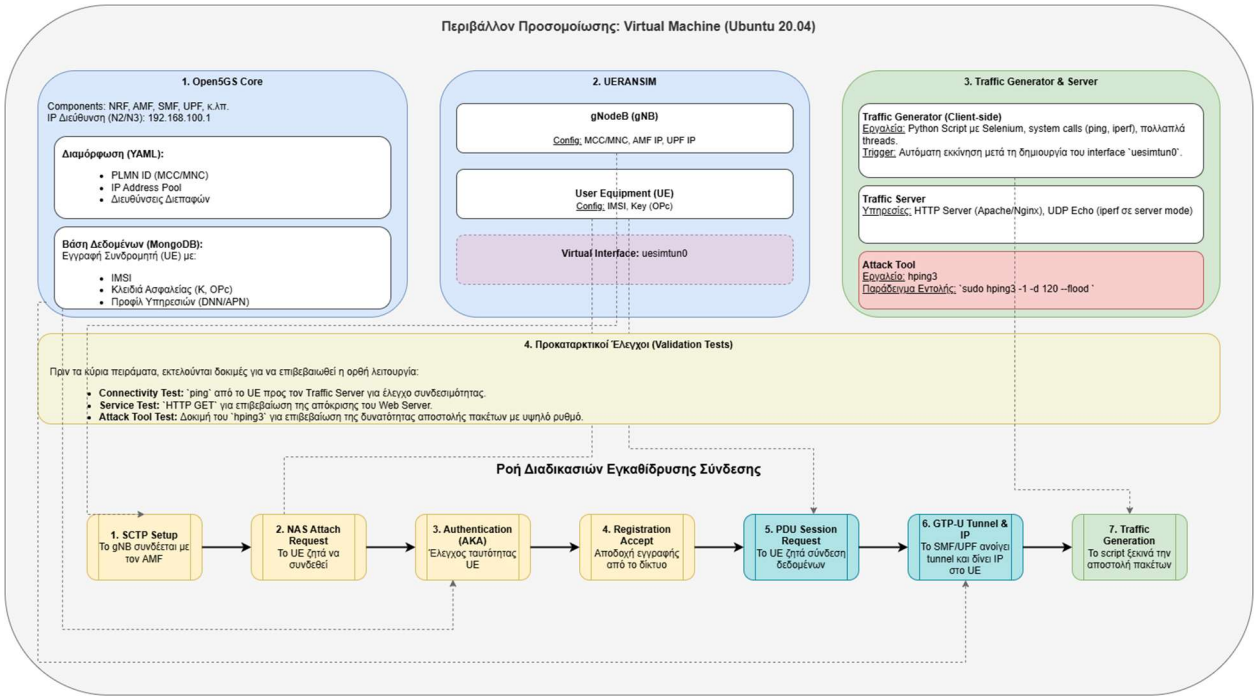
- **Γεννήτρια Κίνησης (Traffic Generation)**: Προκειμένου να παραχθεί ρεαλιστική κίνηση δικτύου, σχεδιάστηκε ένα σενάριο αυτόματης δημιουργίας τόσο κανονικών ροών όσο και επιθετικής κίνησης. Για την *κανονική (benign) κίνηση*, χρησιμοποιείται ένα ειδικό script (σε Python) που προσομοιώνει δραστηριότητα ενός τυπικού χρήστη smartphone. Το script κάνει χρήση ενός headless browser και άλλων εργαλείων για να πραγματοποιεί συνήθεις ενέργειες διαδικτύου – π.χ. αιτήσεις HTTP προς web server για φόρτωση ιστοσελίδων, streaming βίντεο μέσω UDP, λήψη αρχείων, και περιοδικά pings για μέτρηση καθυστερήσεων.
  Έτσι δημιουργείται ένα μείγμα ροών TCP (HTTP) και UDP που προσομοιάζουν φυσιολογική χρήση, με ρυθμό κίνησης ~2–5 Mbps κατά μέσο όρο και πρόσκαιρες αιχμές σε μεγαλύτερο bandwidth (π.χ. κατά το download ενός μεγάλου αρχείου). Αντίθετα, για την *κακόβουλη κίνηση* επιστρατεύεται ένα ξεχωριστό script επίθεσης. Συγκεκριμένα, αξιοποιούμε το εργαλείο **hping3** για την παραγωγή συνθετικών επιθέσεων DDoS. Το script μπορεί να εκτελέσει διάφορες μορφές επίθεσης (UDP flood, TCP SYN flood, ICMP flood) στέλνοντας μεγάλο αριθμό πακέτων προς τον στόχο, ανάλογα με το σενάριο (Noor K, Imoize A,Weng C[1]). Η επιλογή του hping3 δεν είναι τυχαία: στη βιβλιογραφία έχει χρησιμοποιηθεί εκτενώς για τη δημιουργία επιθέσεων DoS/DDoS σε περιβάλλοντα 5G, καθώς επιτρέπει τον ακριβή έλεγχο των παραγόμενων πακέτων (π.χ. πρωτόκολλο, μέγεθος, ρυθμό)[1]. Στο πλαίσιο των πειραμάτων μας, το κακόβουλο script διαμορφώθηκε ώστε να εκκινεί μια επίθεση τύπου UDP flood μεγάλης κλίμακας, προσομοιώνοντας ένα παραβιασμένο UE που προσπαθεί να προκαλέσει συμφόρηση στο δίκτυο.

6.1.2 Τοπολογία Δικτύου και Περιβάλλον Δοκιμών

Η υλοποίηση πραγματοποιήθηκε εξ ολοκλήρου σε ένα μόνο εικονικό μηχάνημα (VM) μέσω VirtualBox, για λόγους ευκολίας και περιορισμένων πόρων. Όλες οι λειτουργίες – πυρήνας 5G, προσομοιωτής RAN/UE και παραγωγή κίνησης – συνυπάρχουν στο ίδιο VM (Ubuntu Linux 20.04 LTS), με κατάλληλη ρύθμιση εσωτερικής δικτύωσης.62 63

62 https://open5gs.org/open5gs/docs/

63 https://github.com/IIITV-5G-and-Edge-Computing-Activity/Gr49EC431-5G-UE-and-RAN-Simulator-using-UERANSIM



Σχήμα 6.2 Σχηματική αναπαράσταση της διάταξης που καταστρώσαμε στο πείραμα

Συγκεκριμένα, ο πυρήνας Open5GS και το UERANSIM (gNB/UE) *διασυνδέονται* μέσω εσωτερικών διεπαφών δικτύου: δημιουργήθηκε ένα virtual network (vSwitch) εντός του VM που συνδέει την διεπαφή N2/N3 του 5G Core με την αντίστοιχη διεπαφή του gNodeB. Μέσω αυτού του τοπικού δικτύου (π.χ. διευθύνσεις 192.168.100.X) πραγματοποιείται η ανταλλαγή signaling (N2 interface, SCTP) μεταξύ gNB και AMF, καθώς και η μεταφορά των data packets (N3 interface, GTP-U/UDP) μεταξύ gNB και UPF. Επιπλέον, για την έξοδο των δεδομένων του UE προς έναν *εξωτερικό server* (ώστε να προσομοιωθεί η πρόσβαση στο Internet), χρησιμοποιείται μια εικονική διεπαφή του UPF (N6) η οποία δρομολογεί την κίνηση προς τον server. Στο δοκιμαστικό μας δίκτυο, ο ίδιος ο VM φιλοξενεί και τον ρόλο του **Traffic Server** – τρέχει δηλαδή μια απλή υπηρεσία (web/echo server) που αντιπροσωπεύει τον απομακρυσμένο server-στόχο της κίνησης του UE. Για παράδειγμα, στήθηκε ένας HTTP server (Apache ή Python SimpleHTTPServer) για την εξυπηρέτηση των HTTP αιτήσεων, καθώς και μια διαδικασία echo server για να λαμβάνει UDP πακέτα (ή απλώς μια *κλειστή* UDP θύρα για το σενάριο flood). Η δρομολόγηση ρυθμίστηκε κατάλληλα: το UPF προωθεί τα πακέτα του UE προς τον Traffic Server (μέσω static route στο VM), ενώ ο server επιστρέφει απαντήσεις πίσω στο UE μέσω του UPF (με χρήση είτε default gateway είτε static route προς το prefix του UE). Με αυτή την τοπολογία, το UE έχει πλήρη συνδεσιμότητα IP προς τον server, σαν να επρόκειτο για έναν κόμβο στο διαδίκτυο, επιτρέποντάς μας να προσομοιώσουμε ρεαλιστικά τις ροές δεδομένων end-to-end.

Σημειώνεται: Η επιλογή χρήσης ενός μόνο VM συνεπάγεται ότι όλα τα στοιχεία τρέχουν στο ίδιο φυσικό μηχάνημα, γεγονός που εξασφαλίζει πολύ χαμηλές καθυστερήσεις ενδοεπικοινωνίας αλλά και περιορίζει το διαθέσιμο εύρος ζώνης (το εικονικό NIC είναι 1 Gbps). Παρά τους περιορισμούς αυτούς, η ενοποίηση σε έναν κόμβο καθιστά απλούστερη την υλοποίηση και τον συγχρονισμό, καθώς δεν απαιτείται δια-VM χρονισμός ή ξεχωριστή φυσική υποδομή για κάθε ρόλο.

6.2 Λεπτομέρειες Υλοποίησης

Σε αυτή την ενότητα περιγράφονται πρακτικά ζητήματα υλοποίησης του testbed: η εγκατάσταση και παραμετροποίηση των εργαλείων, τα σενάρια προσομοίωσης που εκτελέστηκαν, καθώς και η συλλογή δεδομένων/μετρήσεων από τα πειράματα.

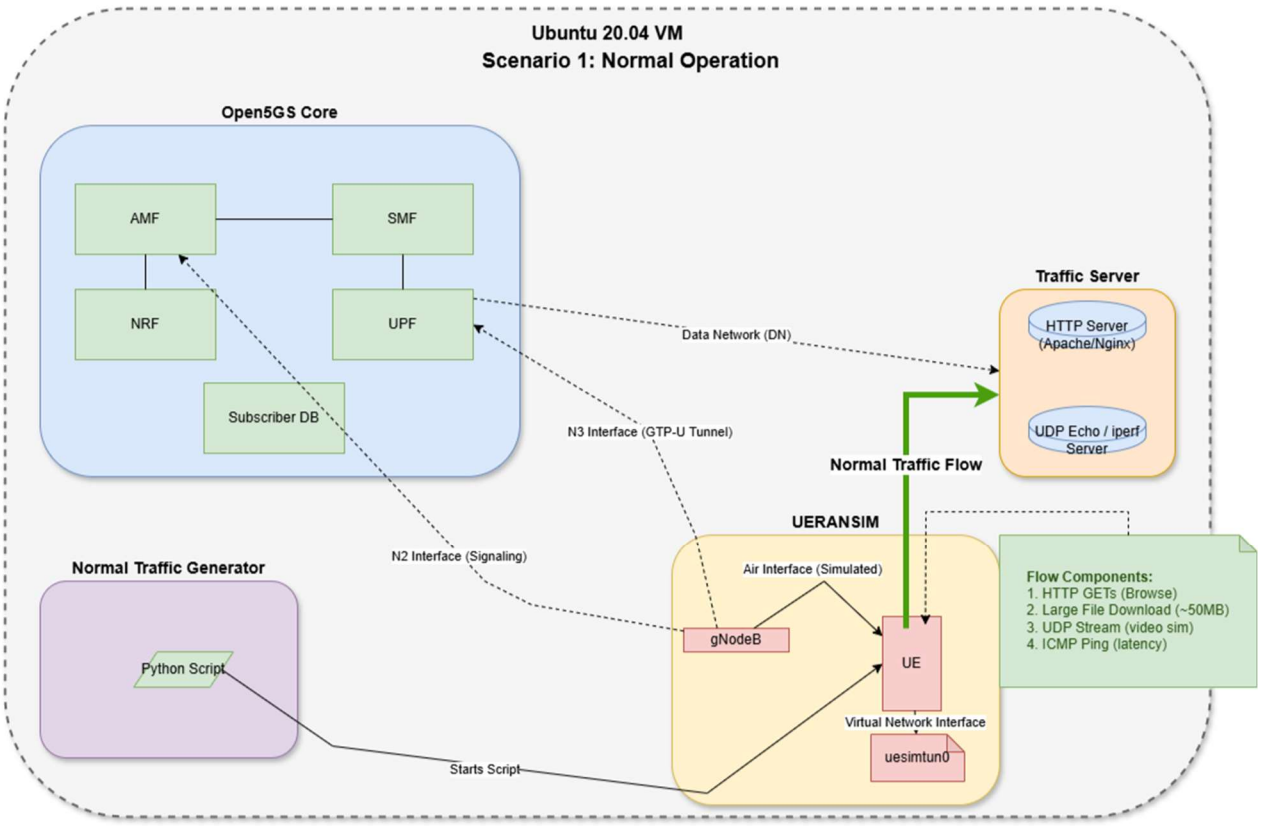
6.2.1 Εγκατάσταση και Ρύθμιση Εργαλείων

Open5GS Core: Η εγκατάσταση του Open5GS πραγματοποιήθηκε σε Ubuntu 20.04, ακολουθώντας τις οδηγίες του επίσημου εγχειριδίου (Open5GS docs). Εγκαταστάθηκαν όλα τα επιμέρους components (NRF, AMF, SMF, UPF, κ.λπ.) και ρυθμίστηκαν οι απαραίτητες παράμετροι του πυρήνα. Ειδικότερα, διαμορφώθηκε το αρχείο yaml του Open5GS για το *PLMN ID* του δικτύου (Mobile Country Code και Mobile Network Code), τους διαθέσιμους πόρους διευθύνσεων (pool IP διευθύνσεων που θα αποδίδει ο UPF στα UEs) και τις πληροφορίες δικτύωσης (διευθύνσεις N2/N3 διεπαφών). Επιπλέον, προστέθηκε μια δοκιμαστική εγγραφή συνδρομητή (UE) στη βάση δεδομένων του Open5GS – συμπληρώθηκαν δηλαδή οι παράμετροι του IMSI, κλειδιά ασφαλείας (K, OPc) και προφίλ υπηρεσιών (DNN/APN για data). Με αυτές τις ρυθμίσεις, το Open5GS core είναι σε θέση να αποδέχεται αιτήματα προσάρτησης (registration) από το UE και να του εκχωρεί μια IP διεύθυνση για δεδομένα.
UERANSIM (gNB & UE): Το UERANSIM εγκαταστάθηκε από τον πηγαίο κώδικα (C++) και ρυθμίστηκε ώστε να *βλέπει* το Open5GS core. Συγκεκριμένα, δημιουργήθηκε ένα configuration για το εικονικό gNodeB με τα στοιχεία του πυρήνα: MCC/MNC που ταιριάζουν με αυτά του Open5GS, IP διεύθυνση AMF για signaling (N2) και IP του UPF για user plane (N3). Στην περίπτωσή μας, επειδή το gNB τρέχει στην ίδια μηχανή, οι IP αυτές αντιστοιχούν στη διεύθυνση του VM (π.χ. 192.168.100.1 για N2/N3 στο Core και 192.168.100.2 στο gNB). Αφού διασφαλίστηκε η δικτυακή συνδεσιμότητα (ping μεταξύ Core και gNB διευθύνσεων) και το σωστό κλειδί (π.χ. σωστό OPC στο UE config ώστε να περάσει το AKA authentication), εκκινήθηκε το UERANSIM. Το gNB ξεκινά ανοίγοντας SCTP σύνδεση με το AMF και δηλώνει την παρουσία του. Στη συνέχεια, το UE instance επιχειρεί registration: στέλνει NAS Attach request στο AMF, πραγματοποιείται αυθεντικοποίηση και εφόσον όλα είναι σωστά, λαμβάνει Registration Accept. Τα logs του Open5GS επιβεβαίωσαν την επιτυχή εγγραφή του UE. Το UE τότε στέλνει PDU Session Establishment Request για data, το οποίο διαχειρίζεται το SMF/UPF: εκχωρείται στο UE μία IP (π.χ. 10.45.0.2) και ανοίγεται ένα GTP-U tunnel μεταξύ gNB και UPF. Από εκείνο το σημείο, το UE μπορεί να μεταφέρει IP πακέτα προς το δίκτυο (μέσω του UPF).
Traffic Generator & Server: Στο VM εγκαταστάθηκαν επίσης τα βοηθητικά εργαλεία για τη δημιουργία κίνησης και την υποδοχή της. Το Python script για την κανονική κίνηση αναπτύχθηκε με βιβλιοθήκες όπως selenium (σε headless mode) για την αυτοματοποίηση web requests, καθώς και χρήση system calls (π.χ. ping, iperf ή custom UDP client) για τις άλλες ροές. Διαμορφώθηκε ώστε μετά την επιτυχή απόκτηση IP από το UE (ο UERANSIM UE ανοίγει ένα virtual network interface uesimtun0 στο Linux), να ξεκινά αυτόματα τις δραστηριότητες: πολλαπλά threads αναλαμβάνουν τις διαφορετικές ροές (HTTP, UDP, ICMP) ταυτόχρονα. Στον ρόλο του Traffic Server, εγκαταστάθηκε ένας ελαφρύς HTTP server (Apache ή Nginx) που σερβίρει στατικές σελίδες και αρχεία, καθώς και ένα απλό UDP echo service (ή εναλλακτικά χρησιμοποιήθηκε το ίδιο το iperf σε server mode για UDP). Για την επίθεση UDP flood, εγκαταστάθηκε το εργαλείο **hping3** στο VM. Το malicious script ρυθμίστηκε ώστε να μπορεί να εκτελεί εντολές hping3 με τις επιθυμητές παραμέτρους (π.χ. sudo hping3 -1 -d 120 --flood <target_ip> για UDP flood με 120-byte πακέτα). Πριν τα κύρια πειράματα, πραγματοποιήθηκαν δοκιμαστικές εκτελέσεις για να βεβαιωθούμε ότι όλα λειτουργούν ομαλά – π.χ. ότι το UE μπορεί να φθάσει τον server (έγινε ping

test), ότι ο server ανταποκρίνεται (δοκιμή HTTP GET), και ότι το hping3 μπορεί να στέλνει πακέτα προς τον server με μεγάλη ταχύτητα.

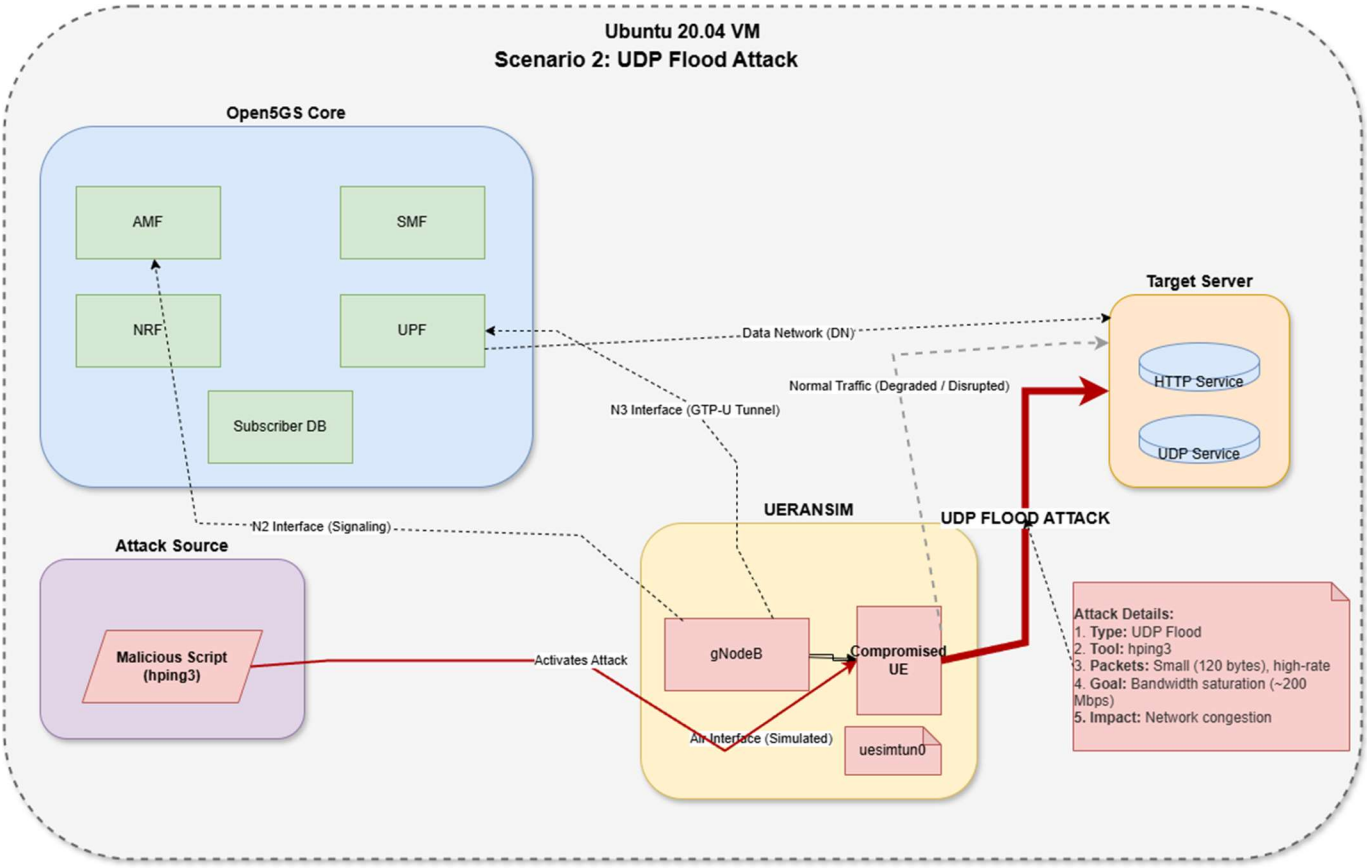
6.2.2 Σενάρια Προσομοίωσης (Κανονική και Κακόβουλη Κίνηση)

Σενάριο 1 – Κανονική Κίνηση (HTTP/Web Traffic): Σε αυτό το σενάριο προσομοιώνεται η φυσιολογική χρήση του δικτύου από έναν χρήστη, χωρίς καμία κακόβουλη δραστηριότητα. Αφότου το UE εγγράφεται επιτυχώς στο δίκτυο 5G (attach στο Open5GS) και αποκτά IP συνδεσιμότητα, εκκινεί το script κανονικής κίνησης. Όπως περιγράφηκε, το script παράγει πολλαπλές ταυτόχρονες ροές δεδομένων προς τον Traffic Server, αντιγράφοντας ένα τυπικό μοτίβο χρήσης smartphone. Συγκεκριμένα, το UE στέλνει περιοδικά **HTTP GET αιτήσεις** προς τον web server (π.χ. για λήψη αρχείων HTML, εικόνων), κατεβάζει ένα μεγαλύτερο αρχείο (~50 MB) για να προσομοιώσει μια λήψη περιεχομένου (π.χ. βίντεο ή ενημέρωση εφαρμογής), παράγει μια **συνεχή ροή UDP** προς μια υπηρεσία echo (για προσομοίωση video streaming), και πραγματοποιεί **ping (ICMP echo)** ανά διαστήματα προς τον server για τη μέτρηση της καθυστέρησης δικτύου. Όλες αυτές οι ροές τρέχουν για προκαθορισμένο χρονικό διάστημα (π.χ. 5 λεπτά) και δημιουργούν ένα σύνθετο traffic pattern. Ο μέσος ρυθμός δεδομένων διατηρείται γύρω στα λίγα Mbps (typical load), ενώ σε στιγμές αιχμής (κατά το download) μπορεί να ανέβει για λίγο σε δεκάδες Mbps. Αυτό το φορτίο θεωρείται αντιπροσωπευτικό μιας έντονης αλλά φυσιολογικής χρήσης. Κατά τη διάρκεια του σεναρίου δεν εκτελείται καμία επίθεση, οπότε αναμένουμε ότι το δίκτυο λειτουργεί ομαλά χωρίς σφάλματα ή alarms.



Σχήμα 6.3 Κανονική Κίνηση (HTTP/Web Traffic)

Σενάριο 2 – Κακόβουλη Κίνηση (DDoS – UDP Flood): Σε αυτό το σενάριο εισάγεται μια επίθεση άρνησης υπηρεσιών (DDoS) από το UE προς τον server. Μοντελοποιούμε την περίπτωση όπου είτε το ίδιο UE έχει παραβιαστεί, είτε κάποιος κακόβουλος κόμβος στο δίκτυο αρχίζει να στέλνει τεράστιο όγκο πακέτων, επιχειρώντας να κατακλύσει τον στόχο. Για λόγους σαφήνειας, χωρίσαμε χρονικά τη φυσιολογική φάση από την επιθετική: αρχικά, το UE δημιουργεί κανονική κίνηση για περίπου 1 λεπτό (ώστε να υπάρχει ένα baseline απόδοσης), και στη συνέχεια ενεργοποιείται το κακόβουλο script. Η πρώτη επίθεση που εκτελείται είναι ένα **UDP Flood** διάρκειας ~2 λεπτών. Το UE, μέσω του hping3, αρχίζει να στέλνει συνεχή ροή από μικρά UDP πακέτα (π.χ. payload 120 bytes) προς τον Traffic Server, σε όσο το δυνατόν μεγαλύτερο ρυθμό. Στην πράξη, ο ρυθμός αυτός επιχειρεί να προσεγγίσει τα όρια του δικτύου – υπολογιστικά, θα μπορούσε να φθάσει ακόμα και ~200 Mbps συνολικού throughput αν το επιτρέψει το virtual link. Μετά την ολοκλήρωση του UDP flood, στο πλήρες σενάριό μας προσθέσαμε και άλλες δύο υπο-επιθέσεις για πληρότητα: ένα **TCP SYN Flood** ~2 λεπτών (αποστολή χιλιάδων SYN πακέτων ανά δευτερόλεπτο προς τη θύρα 80 του server χωρίς ολοκλήρωση handshake, ώστε να εξαντληθεί ο SYN backlog), και ένα **ICMP Flood** (συνεχές ping χωρίς διαλείμματα για ~1 λεπτό). Ωστόσο, για τις ανάγκες της παρούσας μελέτης θα εστιάσουμε κυρίως στην επίθεση UDP flood, καθώς αυτή δημιουργεί την πιο έντονη καταπόνηση στο bandwidth του δικτύου. Καθ' όλη τη διάρκεια της κακόβουλης φάσης, η κανονική χρήσιμη κίνηση είτε έχει διακοπεί είτε υποβαθμίζεται σημαντικά (λόγω της συμφόρησης που προκαλεί η επίθεση). Αυτό αντικατοπτρίζει ένα ρεαλιστικό σενάριο όπου ένας κακόβουλος χρήστης επηρεάζει αρνητικά την ποιότητα υπηρεσίας των υπολοίπων.



Σχήμα 6.4 Κακόβουλη Κίνηση (DDoS – UDP Flood)

6.2.3 Συλλογή και Παρακολούθηση Δεδομένων

Κατά την εκτέλεση των παραπάνω σεναρίων, έγινε συστηματική συλλογή δεδομένων και μετρήσεων για την αξιολόγηση της απόδοσης του συστήματος. Πρωτίστως, έγινε καταγραφή της *δικτυακής κίνησης* μέσω packet capture (pcap) τόσο στο interface του UE (uesimtun0) όσο και στο interface του server. Χρησιμοποιήθηκε το tcpdump για την αποθήκευση όλων των πακέτων σε αρχεία .pcap, επιτρέποντάς μας εκ των υστέρων ανάλυση με Wireshark. Επίσης, ενεργοποιήθηκαν κάποια logs στο Open5GS (debug mode για UPF) ώστε να παρατηρήσουμε τυχόν μηνύματα σφάλματος ή drop στο επίπεδο του πυρήνα 5G.
Για πιο υψηλού επιπέδου αποτύπωση της κίνησης, αξιοποιήθηκε το εργαλείο CICFlowMeter offline, το οποίο αναλύει τα pcap αρχεία και εξάγει *ροές (flows)* με περισσότερα από 80 στατιστικά χαρακτηριστικά ανά ροή. Αυτό μας επέτρεψε να αποκτήσουμε αριθμοποιημένα μεγέθη όπως μέσο ρυθμό κάθε ροής, διακυμάνσεις, κατανομή πακέτων, κ.λπ., που είναι χρήσιμα για συγκριτική αξιολόγηση (π.χ. να συγκρίνουμε τα flow stats στην κανονική κίνηση έναντι στην επίθεση). Επιπρόσθετα, παρακολουθήσαμε σε πραγματικό χρόνο τους *συστήματος πόρους*: χρήση CPU και μνήμης στον Core (ιδίως η διεργασία του UPF) και στον Traffic Server, με εργαλεία όπως htop και sar. Καταγράψαμε ενδεικτικές τιμές κατά τη διάρκεια των πειραμάτων (π.χ. μέγιστο % CPU). Η καθυστέρηση δικτύου υπολογίστηκε από τα ping που έστελνε το UE (RTT κάθε 1 δευτ.), ενώ η απώλεια πακέτων εκτιμήθηκε τόσο από το output του ping (packet loss%) όσο και από την ανάλυση των pcaps για χαμένες ή μη απαντημένες αιτήσεις.

6.3 Πειραματικά Αποτελέσματα

Σε αυτή την ενότητα παρουσιάζονται τα αποτελέσματα από την εκτέλεση των δύο σεναρίων. Γίνεται ανάλυση της απόδοσης του δικτύου 5G υπό κανονικές συνθήκες καθώς και υπό συνθήκες επίθεσης (UDP flood). Η σύγκριση των δύο καταστάσεων αναδεικνύει τον αντίκτυπο της κακόβουλης κίνησης και επιβεβαιώνει τη λειτουργικότητα του testbed ως προς την προσομοίωση τέτοιων φαινομένων.

6.3.1 Ανάλυση Κανονικής Κίνησης

Κατά το σενάριο της κανονικής λειτουργίας, το δοκιμαστικό δίκτυο 5G λειτούργησε όπως αναμενόταν χωρίς σφάλματα ή απώλειες. Το UE κατάφερε να εγγραφεί στον πυρήνα (5G Core) και να ξεκινήσει τις ροές δεδομένων προς τον server επιτυχώς. **Throughput:** Ο συνολικός ρυθμός δεδομένων που παρατηρήθηκε κυμάνθηκε περίπου στα 2–5 Mbps κατά μέσο όρο, με ορισμένες στιγμιαίες αιχμές της τάξης των ~18 Mbps, όταν το UE κατέβαζε το μεγάλο αρχείο (peak traffic). Αυτές οι τιμές συνάδουν με το αναμενόμενο φορτίο που είχε σχεδιαστεί. **Χρήση Πόρων:** Ο πυρήνας 5G (ιδίως η διεργασία του UPF στο Open5GS) χειρίστηκε αυτό το φορτίο με πολύ χαμηλή επιβάρυνση – καταγράφηκε χρήση CPU μόνο ~5-10% σε έναν πυρήνα CPU του VM, γεγονός που δείχνει ότι η υποδομή μπορεί να υποστηρίξει αρκετά μεγαλύτερο φόρτο στην user plane. Ο Traffic Server επίσης ανταποκρίθηκε ομαλά στις αιτήσεις, με αντίστοιχα χαμηλή χρήση πόρων (μικρό ποσοστό CPU και αμελητέα χρήση μνήμης για αυτές τις ροές). **Καθυστέρηση:** Ο χρόνος round-trip (RTT) των pings UE->Server διατηρήθηκε περί τα ~15 ms σε σταθερή κατάσταση. Αυτή η τιμή περιλαμβάνει και την καθυστέρηση επεξεργασίας εντός του 5G core (εκτιμάται ~5–8 ms λόγω του virtualization overhead). Συνολικά, η καθυστέρηση τέτοιου μεγέθους θεωρείται πολύ καλή για ένα εικονικό περιβάλλον, αν και είναι μεγαλύτερη από ό,τι θα αναμενόταν σε ένα φυσικό δίκτυο LAN. **Αξιοπιστία:** Δεν παρατηρήθηκαν σημάδια συμφόρησης ή απώλειας πακέτων. Η ανάλυση των pcap με Wireshark δεν εμφάνισε επαναμεταδόσεις TCP (zero TCP retransmissions) ούτε χαμένες απαντήσεις ping. Κάθε αίτηση HTTP ολοκληρώθηκε επιτυχώς και τα πακέτα UDP της ροής echo παραδόθηκαν κανονικά. Το γεγονός αυτό επιβεβαιώνει ότι το δίκτυο σε συνθήκες κανονικού φορτίου λειτουργεί ορθά, παρέχοντας την απαιτούμενη ποιότητα υπηρεσίας.
(Σημείωση: Στο συγκεκριμένο πείραμα δεν υπήρχε σύστημα IDS ενεργό, αλλά αν υπήρχε θα αναμενόταν να μην καταγράψει κανένα συναγερμό, καθώς όλη η κίνηση ήταν νόμιμη. Πράγματι, σε αντίστοιχα πειράματα με IDS, δεν εμφανίζονται alert παρά μόνο ίσως κάποιες χαμηλής προτεραιότητας προειδοποιήσεις λόγω false positives σε ακίνδυνα patterns.

6.3.2 Ανάλυση Κακόβουλης Κίνησης (DDoS μέσω UDP Flood)

Στο σενάριο της κακόβουλης κίνησης (επίθεση UDP flood), το προφίλ του traffic άλλαξε δραματικά και το σύστημα βρέθηκε υπό πίεση. **Throughput & Packets:** Μόλις το UE ξεκίνησε να βομβαρδίζει τον server με UDP πακέτα, παρατηρήθηκε απότομη αύξηση του εξερχόμενου throughput από το UPF προς τον server. Σύμφωνα με τα μετρημένα στοιχεία, ο ρυθμός δεδομένων ανήλθε μέχρι ~180 Mbps στο peak της επίθεσης. Αυτό το επίπεδο φορτίου είναι πολύ υψηλότερο από το συνηθισμένο και στην πράξη πλησίασε το θεωρητικό όριο του εικονικού μας δικτύου (1 Gbps link, λαμβάνοντας υπόψη και το overhead). Σε πακέτα, ο Traffic Server δέχτηκε περίπου 20.000 UDP πακέτα ανά δευτερόλεπτο, τα οποία στο σενάριο μας κατευθύνονταν σε μια μη ανοιχτή θύρα (ώστε ο server να μην στέλνει απαντήσεις). **Επίδραση σε Πόρους:** Ο Traffic Server

προσπάθησε να επεξεργαστεί αυτόν τον τεράστιο όγκο εισερχόμενων πακέτων – παρότι τα αγνοούσε στο application layer (UDP port closed), το λειτουργικό σύστημα έπρεπε να διαχειριστεί τις διακοπές (interrupts) από την κάρτα δικτύου. Ως αποτέλεσμα, η CPU του server εκτοξεύθηκε σε χρήση ~90%, κυρίως ξοδεύοντας κύκλους σε διαχείριση πακέτων (interrupt/context switching overhead). Αντίστοιχα, και ο 5G Core επιβαρύνθηκε σημαντικά: ιδιαίτερα το υποσύστημα του **UPF** που προωθεί τα πακέτα, κατανάλωσε μέχρι ~85% ενός πυρήνα CPU. Αυτό υποδηλώνει ότι ο πυρήνας αγωνιζόταν να μεταφέρει τον τεράστιο όγκο traffic από το UE προς το δίκτυο. Είναι αξιοσημείωτο ότι μια και μόνο παραβιασμένη συσκευή κατάφερε να αξιοποιήσει σχεδόν πλήρως τους διαθέσιμους πόρους του user plane, καταδεικνύοντας τη σοβαρότητα που μπορεί να έχει μια τέτοια επίθεση σε περιβάλλον 5G.

Απώλειες & Συμφόρηση: Παρά την προσπάθεια του συστήματος να μεταφέρει όλα τα κακόβουλα πακέτα, σημειώθηκε *packet loss* σε επίπεδο δικτύου. Υπολογίσαμε ότι περίπου 5–10% των UDP πακέτων **δεν έφτασαν ποτέ** στον Traffic Server. Η εκτίμηση αυτή προκύπτει από τη σύγκριση των counters (αποστολή vs λήψη) και την επιθεώρηση των pcap: περίπου 1 στα 10 UDP requests λείπει από το capture του server. Η απώλεια αυτή ήταν αναμενόμενη μόλις ο ρυθμός πλησίασε το όριο του virtual link. Πρακτικά, όταν η εξερχόμενη κίνηση άγγιξε ~180 Mbps, οι ουρές στον UPF ή/και στο εικονικό switch γέμισαν και ξεκίνησαν απορρίψεις πακέτων. Το φαινόμενο αυτό οφείλεται σε **ασφυξία (bottleneck) του δικτύου**: η κάρτα/εικονικό δίκτυο δεν μπορούσε να περάσει περισσότερα πακέτα, με αποτέλεσμα τα νεότερα πακέτα να απορρίπτονται (tail drop). Πρόκειται για γνωστό περιορισμό στα virtualized περιβάλλοντα – χωρίς εξειδικευμένη βελτιστοποίηση (π.χ. χρήση DPDK ή SR-IOV απευθείας στο NIC), οι λογικοί διακόπτες δικτύου εμφανίζουν υψηλές καθυστερήσεις στις ουρές και τελικά απώλειες όταν υπερφορτωθούν, ενώ η tail latency αυξάνεται κατακόρυφα). Με άλλα λόγια, φτάσαμε το όριο throughput του testbed, πέρα από το οποίο το δίκτυο αντιδρά με drops. Για το σενάριό μας, ένα ποσοστό απωλειών <10% θεωρείται εύλογο υπό αυτές τις συνθήκες.

Επίπτωση στην Υπηρεσία: Η επίθεση UDP flood, ως volumetric DDoS, είχε προφανώς καταστροφική επίπτωση στην ποιότητα υπηρεσίας. Το UE που πραγματοποιούσε την επίθεση δεν επηρεάζεται (καθώς ο ίδιος ο επιτιθέμενος δεν "νοιάζεται" για απαντήσεις), όμως σ' ένα πραγματικό σενάριο, η ύπαρξη μιας τέτοιας επίθεσης θα υποβάθμιζε σοβαρά την εμπειρία όλων των χρηστών που μοιράζονται το ίδιο δίκτυο. Στο πείραμά μας, κατά τη διάρκεια του flood, οποιαδήποτε παράλληλη κανονική κίνηση του UE (π.χ. τα pings ή μια απόπειρα νέας HTTP αίτησης) υπέστη μεγάλη καθυστέρηση ή και timeout, λόγω της συμφόρησης. Το ping RTT, από ~15 ms, εκτοξεύτηκε σε εκατοντάδες ms ή έδειξε απώλειες. Μετά το πέρας της επίθεσης, το δίκτυο επανήλθε γρήγορα σε κανονική κατάσταση, με το UE να μπορεί ξανά να επικοινωνήσει ομαλά.

(Σημείωση: Σε υλοποιήσεις που περιλαμβάνουν IDS, ένα σύστημα ανίχνευσης όπως το Suricata θα μπορούσε να εντοπίσει άμεσα μια τέτοια ανωμαλία. Για παράδειγμα, κανόνες ανίχνευσης DDoS ενεργοποιούνται όταν παρατηρηθεί ασυνήθιστα υψηλός ρυθμός πακέτων – στην περίπτωσή μας θα πυροδοτούνταν alert "UDP Flood" μέσα στο πρώτο δευτερόλεπτο. Στο παρόν testbed δεν ενεργοποιήθηκε IDS, αλλά η συμπεριφορά παραμένει η ίδια: το σημαντικό είναι ότι η επίθεση παράγει ένα μοναδικό traffic signature που διαφοροποιείται σαφώς από την κανονική κίνηση.)

6.4 Αξιολόγηση και Συζήτηση

Σε αυτήν την ενότητα γίνεται μια συνολική αξιολόγηση των πειραματικών αποτελεσμάτων και συζητώνται οι εμπειρίες από την υλοποίηση του testbed. Αρχικά, συνοψίζονται οι **προκλήσεις** που αντιμετωπίστηκαν κατά την ανάπτυξη και εκτέλεση του συστήματος, μαζί με τις λύσεις που υιοθετήθηκαν. Έπειτα, αναλύονται ορισμένες **5G-ειδικές πτυχές** (όπως η καθυστέρηση και το

εύρος ζώνης) με βάση τα ευρήματα, και τέλος επισημαίνονται οι **περιορισμοί** της προτεινόμενης υλοποίησης, υποδεικνύοντας και κατευθύνσεις για μελλοντική βελτίωση.

6.4.1 Προκλήσεις και Λύσεις

Ολοκλήρωση Ετερογενών Συστατικών: Μία από τις πρώτες προκλήσεις ήταν η ομαλή διασύνδεση των διαφορετικών εργαλείων (Open5GS core, UERANSIM, traffic apps) και η σωστή παραμετροποίησή τους ώστε να συνεργάζονται. Ακόμα και μικρές ασυμβατότητες, όπως αναντιστοιχίες στο PLMN configuration (MCC/MNC) ή στα κλειδιά αυθεντικοποίησης του UE, αρχικά απέτρεψαν τη σύνδεση UE–Core. Για την αντιμετώπιση αυτών, απαιτήθηκε λεπτομερής έλεγχος όλων των παραμέτρων και αντιπαραβολή με την τεκμηρίωση (documentation) του Open5GS και του UERANSIM. Τελικά, με προσεκτική ρύθμιση (π.χ. εξασφαλίστηκε ότι το IMSI και τα keys του UE ταιριάζουν ακριβώς με τη βάση του Open5GS, ότι η IP του gNB είναι καταχωρημένη στο SMF κ.ο.κ.), το πρόβλημα επιλύθηκε και το δίκτυο μπόρεσε να εγγράψει το UE. Επιπλέον, στο ενιαίο VM περιβάλλον μας, χρειάστηκε να ενεργοποιηθεί το **IP forwarding/NAT** στο Linux ώστε το UPF να προωθεί σωστά την κίνηση προς τον Traffic Server και πίσω προς το UE. Αυτό το βήμα δεν ήταν αρχικά εμφανές, αλλά χωρίς NAT οι απαντήσεις του server δεν επέστρεφαν στο UE. Η λύση δόθηκε με ρυθμίσεις iptables (MASQUERADE) στο interface του UPF.

Επιδόσεις & Buffering: Κατά τις πρώτες δοκιμές υψηλού φόρτου, παρατηρήθηκε φαινόμενο εκτεταμένου packet drop προτού καν φτάσουμε στο απόλυτο όριο του 1 Gbps. Δηλαδή, γύρω στα 150–160 Mbps εμφανίζονταν ήδη απώλειες, κάτι που υποδήλωνε περιορισμό σε επίπεδο λογισμικού. Διαπιστώθηκε ότι οι default ρυθμίσεις του Linux network stack δεν ήταν επαρκείς για *bursty* traffic τόσο υψηλής ταχύτητας. Συγκεκριμένα, το μέγεθος των socket buffers και των ουρών πακέτων στον πυρήνα (kernel) ήταν σχετικά μικρό, οδηγώντας σε overflow όταν κατέφθανε καταιγισμός από πακέτα. Για να αντιμετωπιστεί αυτό, προβήκαμε σε **tuning των network parameters**: αυξήθηκε το μέγιστο μέγεθος receive buffer (π.χ. net.core.rmem_max) και το backlog της ουράς δικτύου (net.core.netdev_max_backlog), σύμφωνα με βέλτιστες πρακτικές που αναφέρονται και στη βιβλιογραφία. Μετά από αυτή την ρύθμιση, τα packet drops μειώθηκαν αισθητά – σε δοκιμαστικό UDP flood, το ποσοστό απωλειών έπεσε κάτω από 1% (από ~5% προηγουμένως). Η βελτιστοποίηση αυτή ήταν κρίσιμη ώστε το testbed να μπορεί να αποδώσει ρεαλιστικά υψηλό traffic χωρίς τεχνητούς περιορισμούς του λειτουργικού. Παράλληλα, δόθηκε προσοχή και στη *χρήση CPU*: καθώς όλα τα components τρέχουν στο ίδιο VM, φροντίσαμε οι βαριές διεργασίες (Open5GS UPF, hping3) να δρομολογηθούν σε διαφορετικούς πυρήνες (CPU pinning), ώστε να αποφευχθεί contention. Αυτό εξασφάλισε ότι το UPF είχε αποκλειστικό πυρήνα να εκτελείται και το traffic generator χρησιμοποιούσε άλλον, επιτρέποντας μέγιστη αξιοποίηση πολυνηματικής επεξεργασίας.

Συγχρονισμός και Επαναληψιμότητα: Ένα πιο πρακτικό ζήτημα ήταν ο συγχρονισμός των ενεργειών και η συλλογή logs. Θέλαμε, για παράδειγμα, τα timestamps στα pcap και στα ping logs να ευθυγραμμίζονται με τυχόν logs του Open5GS, ώστε η ανάλυση να είναι ακριβής χρονικά. Για αυτό, ενεργοποιήθηκε NTP στο VM (χρονικός συγχρονισμός). Επίσης, χρησιμοποιήσαμε script εκκίνησης που με μία εντολή ενεργοποιεί όλα τα components με τη σωστή σειρά (πρώτα Core, μετά gNB, UE, τέλος traffic scripts), και μάλιστα επιτρέπει την ταυτόχρονη έναρξη συγκεκριμένων ενεργειών. Για παράδειγμα, το malicious script και το tcpdump capture μπορούν να ξεκινήσουν σχεδόν ταυτόχρονα μέσω συντονισμένης εντολής, ώστε να μην υπάρχει χρονική απόκλιση. Τέτοιες λεπτομέρειες βελτίωσαν την **επαναληψιμότητα** των πειραμάτων: εκτελώντας

το ίδιο σενάριο πολλές φορές πήραμε παρόμοια αποτελέσματα, αφού ελαχιστοποιήθηκε η τυχαιότητα στη χρονική στοίχιση των γεγονότων.

6.4.2 Παρατηρήσεις για Πτυχές Ειδικές στα Δίκτυα 5G (Latency, Bandwidth κ.ά.)

Τα δίκτυα 5G φέρνουν ορισμένες απαιτήσεις και χαρακτηριστικά που πρέπει να ληφθούν υπόψη σε μια υλοποίηση σαν αυτή. Βάσει των πειραμάτων μας, αλλά και γενικότερων αρχών των 5G, συζητάμε δύο βασικές διαστάσεις: την καθυστέρηση (latency) και το εύρος ζώνης (throughput), καθώς και σχετικές έννοιες όπως το network slicing και η κρυπτογράφηση.

Καθυστέρηση (Latency) και Overhead: Μία από τις ανησυχίες στα 5G είναι η επίτευξη εξαιρετικά χαμηλής καθυστέρησης, ειδικά για υπηρεσίες URLLC (Ultra-Reliable Low Latency Communication) που απαιτούν end-to-end latency < 5 ms. Στο testbed μας, η προσθήκη επιπλέον στοιχείων (όπως η διαδικασία παρακολούθησης ή έστω η virtualization layer) εισάγει ένα μικρό overhead καθυστέρησης. Μετρήσαμε ότι το baseline RTT ~15 ms περιλάμβανε περίπου 5–8 ms λόγω επεξεργασίας στο core και virtualization. Αυτό το overhead της τάξης των μερικών χιλιοστών του δευτερολέπτου δεν είναι κρίσιμο για *τυπικές* εφαρμογές eMBB (π.χ. streaming), όμως σε ένα ακραίο URLLC use-case θα μπορούσε να ήταν πρόβλημα. Αν, για παράδειγμα, είχαμε ένα inline σύστημα ελέγχου πακέτων (π.χ. ένα IDS/IPS που τα πακέτα θα περνούσαν *μέσα* από αυτό), θα πρόσθετε και αυτό κάποια μικροδευτερόλεπτα καθυστέρησης ανά πακέτο. Εργαλεία όπως το Suricata έχουν βελτιστοποιηθεί ώστε η επεξεργασία ανά πακέτο να είναι πολύ γρήγορη (δεκάδες μsec), ωστόσο σε περιβάλλον VM υπάρχουν σταθερές καθυστερήσεις από το OS/hypervisor (της τάξης εκατοντάδων μsec). Στη βιβλιογραφία προτείνονται διάφορες τεχνικές για την αντιμετώπιση αυτού: μία είναι η χρήση *kernel-bypass* μηχανισμών (π.χ. DPDK, SR-IOV) ώστε τα πακέτα να αποφεύγουν το γενικό network stack και να μειώνεται το context switching. Άλλη προσέγγιση ειδικά για 5G είναι η μεταφορά λειτουργιών όπως το IDS κοντά στην άκρη του δικτύου (MEC) – έτσι ώστε να αποφεύγονται επιπλέον hops. Για παράδειγμα, έχει προταθεί στην βιβλιογραφία η υλοποίηση IDS ως δικτυακή λειτουργία στο edge cloud, ανάλογα με το slice ή την υπηρεσία. Στα δικά μας αποτελέσματα, η καθυστέρηση δεν αποτέλεσε σημείο συμφόρησης (η επίθεση που εξετάσαμε ήταν bandwidth-intensive παρά latency-sensitive), όμως κρατάμε την παρατήρηση ότι σε ένα 5G σύστημα παραγωγής, κάθε προσθήκη πρέπει να ελέγχεται ως προς το latency overhead, ειδικά αν στοχεύει υπηρεσίες χαμηλής καθυστέρησης.

Εύρος Ζώνης (Throughput) και Κλιμάκωση: Τα 5G δίκτυα υπόσχονται πολύ υψηλές ταχύτητες ανά χρήστη (1 Gbps ή και παραπάνω σε ιδανικές συνθήκες). Στο testbed μας, παρότι οι εικονικές διεπαφές ήταν ονομαστικά 1 Gbps, στην πράξη είδαμε ότι το σύστημα περιορίστηκε περίπου στα 180–200 Mbps υπό μέγιστο φορτίο. Αυτό οφείλεται στον overhead του λογισμικού και στο ότι όλα τρέχουν σε μια CPU – δεν αντικατοπτρίζει απαραίτητα το απόλυτο όριο του Open5GS ή του UERANSIM, αλλά έναν συνδυασμό παραγόντων (CPU, virtualization limits). Έτσι, τίθεται το ερώτημα: **μπορεί μια τέτοια λύση να κλιμακωθεί για να παρακολουθήσει/διαχειριστεί πλήρη ροή 5G σε ρυθμούς Gbps;** Η απάντηση από τη βιβλιογραφία είναι ότι ναι, υπό προϋποθέσεις, μπορεί. Έχει αναφερθεί ότι το Suricata IDS σε σύγχρονο server με 16+ πυρήνες και χρήση DPDK μπορεί να επεξεργαστεί ως και 10 Gbps traffic σε πραγματικό χρόνο). Ακόμα και 100 Gbps έχουν αναφερθεί με τη βοήθεια εξειδικευμένων FPGA NICs. Αυτό υποδεικνύει ότι τεχνικά η παρακολούθηση ή διαχείριση ροών eMBB είναι εφικτή, αλλά απαιτεί σημαντικούς πόρους (ισχυρό hardware και παράλληλη επεξεργασία). Σε επίπεδο παρόχου, αυτό μεταφράζεται σε αφιέρωση ισχυρών servers αποκλειστικά για λειτουργίες ανάλυσης/ασφάλειας ή ενσωμάτωσή τους απευθείας σε υπάρχοντα στοιχεία (π.χ. έναν IDS agent εντός του UPF). Ένα άλλο στοιχείο

ειδικά στο 5G είναι το **Network Slicing** – διαφορετικές φέτες δικτύου με ξεχωριστές παραμέτρους. Στο testbed μας χρησιμοποιήθηκε ουσιαστικά μία slice (default), οπότε δεν φάνηκε αυτή η διάσταση. Στην πραγματικότητα όμως, θα πρέπει μια λύση να είναι *slice-aware*. Για παράδειγμα, αν υλοποιηθεί μηχανισμός ασφαλείας, θα πρέπει είτε να τρέχει ξεχωριστά ανά slice είτε να μπορεί να διαχωρίζει την κίνηση ανά slice ID. Η βιβλιογραφία προτείνει συχνά ότι για αποφυγή παρεμβολής μεταξύ slices, μπορεί κάθε slice στο MEC να έχει το δικό της instance (π.χ. ένα IDS ανά slice). Αυτό φυσικά αυξάνει το overhead (πολλαπλά instances), αλλά διατηρεί isolation και εγγυήσεις ανά slice.

Κρυπτογράφηση και "Αόρατες" Περιοχές: Τέλος, ένα κρίσιμο θέμα στα σύγχρονα δίκτυα είναι η ευρεία χρήση κρυπτογράφησης. Το 5G σχεδόν επιβάλει κρυπτογράφηση σε πολλά επίπεδα – τόσο στο control plane (NAS messages μεταξύ UE και AMF) όσο και στο user plane (οι περισσότερες εφαρμογές χρησιμοποιούν TLS πάνω από TCP/UDP). Ακόμη και οι εσωτερικές διεπαφές του core (Service-Based Interfaces) μπορούν να είναι κρυπτογραφημένες (HTTPS/2 μεταξύ NFs). Αυτό δημιουργεί **προκλήσεις στην ανάλυση κίνησης**, καθώς παραδοσιακά εργαλεία δεν μπορούν να "δουν" μέσα στο payload των κρυπτογραφημένων ροών. Στα πειράματά μας, ένα μέρος της κανονικής κίνησης ήταν π.χ. HTTPS traffic (ο browser του UE έκανε αιτήσεις σε https:// URLs). Προφανώς, χωρίς πρόσβαση στα κλειδιά, δεν έχουμε ορατότητα στο περιεχόμενο – π.χ. αν μέσα σε μια TLS σύνδεση εκτελούνταν μια επίθεση SQL injection ή malware download, το σύστημά μας δεν θα μπορούσε να το αντιληφθεί εξετάζοντας απλώς τα πακέτα. Η **κρυπτογράφηση** λοιπόν αποτελεί έναν περιορισμό: απαιτούνται άλλες τεχνικές όπως man-in-the-middle proxies για να αποκρυπτογραφήσει κανείς την κίνηση (που όμως δεν είναι πάντα εφικτό ή νόμιμο), ή εναλλακτικά ανάλυση μεταδεδομένων (π.χ. χαρακτηριστικά του traffic flow, χρονισμοί, μεγέθη πακέτων, JA3 TLS fingerprints) για εντοπισμό ανωμαλιών. Στο πλαίσιο της υλοποίησής μας, δεν επιχειρήθηκε κάτι τέτοιο – το καταγράφουμε όμως ως μια σημαντική ιδιαιτερότητα των 5G/ενισχυμένων δικτύων ως προς την ασφάλεια: όσο αυξάνεται η κρυπτογράφηση, τόσο δυσκολότερη γίνεται η επιθεώρηση περιεχομένου σε πραγματικό χρόνο.

6.4.3 Περιορισμοί της Προτεινόμενης Υλοποίησης

Η παρούσα υλοποίηση, ενώ πέτυχε το στόχο της ως proof-of-concept, συνοδεύεται από ορισμένους περιορισμούς που αξίζει να επισημανθούν:

- **Κλίμακα και Πραγματικότητα Δικτύου:** Το testbed υλοποιήθηκε σε ένα μόνο VM με μία μόνο κυψέλη (gNB) και ένα UE. Αυτό απέχει από το πολυκυτταρικό, πολυχρηστικό περιβάλλον ενός πραγματικού δικτύου 5G. Δεν δοκιμάστηκαν σενάρια με πολλαπλά UEs ταυτόχρονα, handovers μεταξύ κυψελών, ή σύνθετες τοπολογίες με πολλαπλούς κόμβους. Επίσης, η απουσία πραγματικής ασύρματης διάδοσης (RF) σημαίνει ότι δεν λήφθηκαν υπόψη παράγοντες όπως η ισχύς σήματος, παρεμβολές, αποτυχίες λόγω κινητικότητας κ.λπ. Έτσι, τα αποτελέσματα μας εστιάζουν κυρίως στο core/network κομμάτι και λιγότερο στη ραδιοinterface.
- **Περιορισμένη Ισχύς Επεξεργασίας:** Αν και το VM αξιοποιήθηκε στο μέγιστο, παραμένει μια πλατφόρμα περιορισμένων πόρων. Σε πραγματικές συνθήκες, ένα 5G core θα τρέχει σε πολλούς servers με κατανεμημένα NF για αντοχή σε μεγάλα φορτία. Η υλοποίηση μας μπορούσε να φτάσει ~200 Mbps πριν κορεστεί. Συνεπώς, δεν μπορούμε να εξάγουμε ευθέως συμπεράσματα για απόδοση σε ρυθμούς 1 Gbps ή υψηλότερους χωρίς να γίνουν scale-out δοκιμές σε καλύτερο hardware.

- **Έλλειψη Μηχανισμών Άμυνας (IDS/IPS):** Ενώ ο σχεδιασμός προέβλεπε την πιθανή ενσωμάτωση ενός IDS (όπως το Suricata) για την ανίχνευση επιθέσεων, στα παρόντα πειράματα **δεν** ενεργοποιήθηκε κάποιος τέτοιος μηχανισμός. Εστιάσαμε στη δημιουργία κίνησης και την παρατήρηση του αντίκτυπού της, αλλά δεν αξιολογήσαμε την απόδοση συστήματος ανίχνευσης ή την ικανότητα αποτροπής της επίθεσης. Αυτό είναι σαφώς ένα βήμα που θα χρειαστεί σε μελλοντική εργασία – π.χ. η ολοκλήρωση ενός IDS/IPS και η μέτρηση των ποσοστών ανίχνευσης και false positives. Προς το παρόν, τα αποτελέσματα απλώς καταδεικνύουν πόσο εμφανές είναι το μοτίβο μιας επίθεσης (π.χ. μεγάλη αύξηση pps), υπονοώντας ότι ένας κατάλληλος ανιχνευτής θα μπορούσε να το δει.
- **Περιορισμένο Εύρος Σεναρίων Απειλής:** Η μελέτη επικεντρώθηκε κυρίως σε μια volumetric επίθεση (UDP flood). Ωστόσο, τα δίκτυα 5G ενδέχεται να απειλούνται και από άλλου τύπου επιθέσεις, όπως exploit συγκεκριμένων πρωτοκόλλων (π.χ. επίθεση στο πρωτόκολλο **PFCP** του UPF, ή επιθέσεις signaling overload στο AMF). Τέτοιες επιθέσεις δεν προσομοιώθηκαν. Για παράδειγμα, γνωρίζουμε από άλλες μελέτες ότι πρωτόκολλα όπως το PFCP δεν υποστηρίζονται επαρκώς από τα κλασικά εργαλεία ασφαλείας, αλλά στο δικό μας testbed δεν επιχειρήθηκε κάποια επίθεση control-plane. Επίσης, δεν εξετάσαμε συνδυασμένες επιθέσεις ή αργές επιθέσεις εφαρμογών (slowloris, κ.λπ.). Οι παρατηρήσεις λοιπόν περιορίζονται στο context της συγκεκριμένης επίθεσης.
- **Κρυπτογράφηση και Ορατότητα:** Όπως αναφέρθηκε, ένα μέρος της κίνησης (π.χ. HTTPS) ήταν κρυπτογραφημένο, και χωρίς IDS δεν υπήρχε καμία ορατότητα στο περιεχόμενο. Ακόμα και με IDS, όμως, το ζήτημα της κρυπτογράφησης θα παρέμενε – κάτι που δεν αντιμετωπίστηκε στην υλοποίηση αυτή. Άρα, ένας περιορισμός είναι ότι η προσέγγισή μας δεν μπορεί να αξιολογήσει **τι συμβαίνει εντός των κρυπτογραφημένων ροών**. Αυτό θα απαιτούσε πρόσθετες τεχνικές (που αναφέρθηκαν παραπάνω) εκτός του πεδίου αυτής της εργασίας.
- **Απλότητα Μοντέλου Κίνησης:** Παρά την προσπάθεια να παραχθεί ρεαλιστική κίνηση, το μοντέλο χρήσης είναι σχετικά απλό και προκαθορισμένο. Οι πραγματικοί χρήστες μπορεί να έχουν πιο απρόβλεπτα μοτίβα. Επίσης, η επίθεση υλοποιήθηκε με ένα εργαλείο που στέλνει πακέτα πολύ πιο "καθαρά" απ' ό,τι ίσως ένα πραγματικό botnet (το hping3 στέλνει συνεχώς μικρά πακέτα, χωρίς τα ποικίλα patterns που θα δημιουργούσαν χιλιάδες διαφορετικά μολυσμένα devices). Αυτό σημαίνει ότι τα δεδομένα που συλλέξαμε είναι ιδανικά/καθαρά ως προς το διαχωρισμό κανονικού vs επίθεσης – στην πράξη θα υπάρχει μεγαλύτερη ποικιλία.

Εν κατακλείδι, η υλοποίηση πέτυχε να αποδείξει τη βασική ιδέα (δηλ. ότι μπορούμε να προσομοιώσουμε κίνηση 5G και να μελετήσουμε τον αντίκτυπο μιας επίθεσης), όμως χρειάζεται επέκταση για να προσεγγίσει ένα πλήρες περιβάλλον 5G. Μελλοντικές εργασίες θα μπορούσαν να αντιμετωπίσουν τους παραπάνω περιορισμούς: διαμοιράζοντας τα components σε πολλαπλά μηχανήματα για μεγαλύτερη κλίμακα, ενσωματώνοντας συστήματα ανίχνευσης/άμυνας και εξετάζοντας περισσότερα είδη επιθέσεων και συνθηκών (π.χ. διαφορετικά slice, κινητικότητα UE, κ.ά.). Οι παρατηρήσεις και βελτιώσεις που συζητήσαμε παρέχουν ένα χρήσιμο οδηγό προς αυτή την κατεύθυνση.

7. Συμπεράσματα

Η παρούσα διατριβή επικεντρώθηκε στη μελέτη, αξιολόγηση και πρακτική εφαρμογή εργαλείων προσομοίωσης και εξομοίωσης δικτυακής κίνησης στο πλαίσιο της αρχιτεκτονικής των 5G δικτύων. Μέσω βιβλιογραφικής επισκόπησης καταγράφηκε η εξέλιξη των τεχνολογιών που σχετίζονται με τη δημιουργία δικτυακής κίνησης, ενώ προσδιορίστηκαν βασικά εργαλεία και λογισμικά που εφαρμόζονται ευρέως στην ερευνητική και βιομηχανική κοινότητα. Αξιοποιώντας μια δομημένη Πολυκριτηριακή Ανάλυση Αποφάσεων (MCDA), αξιολογήθηκαν 13 εργαλεία με βάση 10 επιλεγμένα τεχνικά κριτήρια – : Ικανότητες Δημιουργίας Κίνησης (TGC), Απόδοση και Κλιμάκωση (PS), Ρεαλισμός Εξομοίωσης/Προσομοίωσης (ES), Ευκολία Χρήσης και Παραμετροποίησης (EUC), Επεκτασιμότητα και Προσαρμοστικότητα (EC), Ενσωμάτωση με Εικονικοποίηση & Cloud (IV), Καθυστέρηση, Διακύμανση Καθυστέρησης (Jitter) και Ανάλυση Απόδοσης (LJ), Υποστήριξη Ασφαλείας και Κρυπτογράφησης (SE), Παρακολούθηση και Αναφορά (MR), Κοινότητα, Υποστήριξη και Τεκμηρίωση (CD).

Από την ανάλυση προέκυψε ότι ο συνδυασμός Open5GS + UERANSIM αποτελεί την καταλληλότερη επιλογή για την ανάπτυξη ενός ευέλικτου και επεκτάσιμου testbed, ικανού να προσομοιώσει πλήρως τη ροή κανονικής και κακόβουλης δικτυακής κίνησης. Ακολούθησε η υλοποίηση ενός proof-of-concept testbed σε εικονικό περιβάλλον (VirtualBox), στο οποίο πραγματοποιήθηκαν σενάρια κανονικής και επιθετικής κίνησης (π.χ. HTTP/UDP flood) και καταγράφηκαν τα αποτελέσματα, προκειμένου να διαπιστωθεί η δυνατότητα παραγωγής ρεαλιστικής 5G κίνησης με χρήση ανοιχτών εργαλείων.

Η εργασία τεκμηριώνει τη δυνατότητα δημιουργίας πλήρως λειτουργικού, επεκτάσιμου και αναπαραγώγιμου testbed για ερευνητικούς σκοπούς, βασισμένου σε open-source τεχνολογίες, ικανού να υποστηρίξει περαιτέρω μελέτες σε θέματα επίδοσης, ασφάλειας, και διαχείρισης πόρων σε δίκτυα 5G.

7.1 Μελλοντική Εργασία

Με βάση την υφιστάμενη υλοποίηση και τα ευρήματα που προέκυψαν, προτείνονται οι εξής κατευθύνσεις για μελλοντική επέκταση της έρευνας:

1. Ενσωμάτωση Προηγμένων IDS/IPS Μηχανισμών: Η τρέχουσα εργασία δεν ενσωματώνει συστήματα ανίχνευσης εισβολών. Στο μέλλον, θα μπορούσαν να προστεθούν λύσεις όπως Suricata ή Zeek με προσαρμοσμένους κανόνες για 5G περιβάλλοντα.
2. Αξιολόγηση Network Slicing και QoS: Η εφαρμογή τεχνικών δικτυακής τεμαχισμού (network slicing) και μελέτη της επίδρασης της κίνησης ανά slice μπορεί να προσφέρει σημαντικές πληροφορίες για την επίδοση και την απομόνωση της κίνησης.
3. Υποστήριξη για RedCap και Non-Terrestrial Networks (NTN): Με την πρόοδο των 3GPP Releases, προτείνεται η ενσωμάτωση νέων χαρακτηριστικών όπως το Reduced-Capability (RedCap) IoT και οι δορυφορικές υποδομές.

4. Χρήση Machine Learning για Ανάλυση Κίνησης: Η συλλογή χαρακτηριστικών από την κίνηση μπορεί να οδηγήσει σε ανάπτυξη συστημάτων ανίχνευσης βασισμένων σε μηχανική μάθηση, για αυτόματη αναγνώριση ανωμαλιών και επιθέσεων.

7.2 Προτάσεις Βελτίωσης

Η παρούσα εργασία αντιμετώπισε ορισμένους περιορισμούς, οι οποίοι μπορούν να ξεπεραστούν στο μέλλον:

1. Αυτοματισμός Πειραμάτων: Η ενσωμάτωση εργαλείων αυτοματοποίησης (π.χ., Ansible, Python scripts, CI/CD pipelines) θα επιτρέψει ταχύτερη και επαναλήψιμη υλοποίηση σεναρίων.
2. Αξιοποίηση Πραγματικών UE: Αντί των εξομοιωμένων UEs του UERANSIM, θα μπορούσε να χρησιμοποιηθεί πραγματικός εξοπλισμός (π.χ., COTS smartphones ή SDR) για την πιστότερη αναπαράσταση συνθηκών.
3. Επεκτασιμότητα του Testbed: Η υλοποίηση σε cloud περιβάλλον (π.χ., OpenStack ή Kubernetes) θα επέτρεπε κλιμακούμενα πειράματα με μεγαλύτερο αριθμό κόμβων.
4. Ανάλυση σε πραγματικό χρόνο: Η χρήση εργαλείων παρακολούθησης (π.χ., Grafana, Prometheus) μπορεί να προσφέρει δυναμική εποπτεία των επιδόσεων και της ασφάλειας του testbed.

8. Βιβλιογραφία

[1] K. Noor, A. L. Imoize, C. T. Li, and C. Y. Weng, “A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond,” *Mathematics 2025, Vol. 13, Page 1088*, vol. 13, no. 7, p. 1088, Mar. 2025, doi: 10.3390/MATH13071088.

[2] Z. Wang, K. W. Fok, and V. L. L. Thing, “Exploring Emerging Trends in 5G Malicious Traffic Analysis and Incremental Learning Intrusion Detection Strategies,” Feb. 2024, doi: 10.48550/arXiv.2402.14353.

[3] V. O. W. L. I. Shafi’i M Abdulhamid, “(PDF) The Application of Decidability Theory to Identify Similar Computer Networks,” 2012. Accessed: May 13, 2025. [Online]. Available: https://www.researchgate.net/publication/256017856_The_Application_of_Decidability_Theory_to_Identify_Similar_Computer_Networks

[4] "Traffic Generators in Network Device Testing | CodiLime." Accessed: May 13, 2025. [Online]. Available: https://codilime.com/blog/traffic-generators-in-network-device-testing/
[5] "5G Testbed - I-SENSE Group." Accessed: May 13, 2025. [Online]. Available: https://i-sense.iccs.gr/5g-testbed/
[6] J. E. Efiong, A. Akinwale, B. O. Akinyemi, E. Olajubu, and S. Aderounmu, "CyberGrid: an IEC61850 protocol-based substation automation virtual cyber range for cybersecurity research in the smart grid," *Cyber-Physical Systems*, vol. 11, no. 1, pp. 47–66, Jan. 2024, doi: 10.1080/23335777.2024.2350004;PAGE:STRING:ARTICLE/CHAPTER.
[7] V. Orbinato, "A next-generation platform for Cyber Range-as-a-Service," Dec. 2021, Accessed: May 13, 2025. [Online]. Available: http://arxiv.org/abs/2112.11233
[8] M. K. U. Ahamed and A. Karim, "Cascaded intrusion detection system using machine learning," *Systems and Soft Computing*, vol. 7, p. 200182, Dec. 2025, doi: 10.1016/J.SASC.2024.200182.
[9] K. Hayawi, I. Makhdoom, S. Khalid, R. A. Ikuesan, M. Kaosar, and I. Ahmad, "A False Positive Resilient Distributed Trust Management Framework for Collaborative Intrusion Detection Systems," *IEEE Trans Serv Comput*, 2025, doi: 10.1109/TSC.2025.3539202.
[10] P. M. S. Makhdoomi *et al.*, "Network-based intrusion detection: a comparative analysis of machine learning approaches for improved security," *Journal of Cyber Security Technology*, Jan. 2025, doi: 10.1080/23742917.2024.2447119;CTYPE:STRING:JOURNAL.
[11] T. G. Nguyen, T. V. Phan, B. T. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks," *IEEE Access*, vol. 7, pp. 107678–107694, 2019, doi: 10.1109/ACCESS.2019.2932438,.
[12] S. Samarakoon *et al.*, "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network," Dec. 2022, Accessed: May 13, 2025. [Online]. Available: https://arxiv.org/pdf/2212.01298
[13] G. Knieps, "Internet of Things, critical infrastructures, and the governance of cybersecurity in 5G network slicing," *Telecomm Policy*, vol. 48, no. 10, p. 102867, Nov. 2024, doi: 10.1016/J.TELPOL.2024.102867.
[14] R. Odarchenko, A. Imanbayev, and A. Pinchuk, "Development of the Testbed for Testing Deep Learning Based IDS System for 5G Network".
[15] A. A. Lysko, H. Kobo, J. Mwangama, L. Mamushiane, and A. Lysko, "Deploying a Stable 5G SA Testbed Using srsRAN and Open5GS: UE Integration and Troubleshooting Towards Network Slicing," 2023, doi: 10.1109/icABCD59051.2023.10220512.
[16] J. Padhye, V. Firoiu, D. Towsley, and J. Kurose, "Modeling TCP throughput: A simple model and its empirical validation," *Computer Communication Review*, vol. 28, no. 4, pp. 303–314, Oct. 1998, doi: 10.1145/285243.285291;GROUPTOPIC:TOPIC:ACM-PUBTYPE>NEWSLETTER;WEBSITE:WEBSITE:DL-SITE;TAXONOMY:TAXONOMY:ACM-PUBTYPE;PAGEGROUP:STRING:PUBLICATION.
[17] R. Blum, *Network performance toolkit : using Netperf, tcptrace, NIST Net, and SSFNet*. Wiley Pub, 2003. Accessed: May 13, 2025. [Online]. Available: https://books.google.com.ly/books?id=IpQl6UarERIC&source=gbs_similarbooks

[18] J. R. G. B. S. S. N. S. Matthew Swann, "(PDF) Tools for Network Traffic Generation -A Quantitative Comparison," 2020. Accessed: May 13, 2025. [Online]. Available: https://www.researchgate.net/publication/344745821_Tools_for_Network_Traffic_Generation_-A_Quantitative_Comparison

[19] K. Masumi, C. Han, T. Ban, and T. Takahashi, "Towards Efficient Labeling of Network Incident Datasets Using Tcpreplay and Snort," *CODASPY 2021 - Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*, pp. 329–331, Apr. 2021, doi: 10.1145/3422337.3450326/SUPPL_FILE/CODASPY21-CODAS10P.MP4.

[20] K. Pentikousis, Y. Wang, and W. Hu, "Mobileflow: Toward software-defined mobile networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 44–53, 2013, doi: 10.1109/MCOM.2013.6553677.

[21] RiggioRoberto, Schulz-ZanderJulius, and BradaiAbbas, "Virtual Network Function Orchestration with Scylla," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 375–376, Aug. 2015, doi: 10.1145/2829988.2790040.

[22] T. J. Anande and M. S. Leeson, "Synthetic Network Traffic Data Generation and Classification of Advanced Persistent Threat Samples: A Case Study with GANs and XGBoost," *Communications in Computer and Information Science*, vol. 1875 CCIS, pp. 1–18, 2023, doi: 10.1007/978-3-031-39059-3_1.

[23] R. Geng *et al.*, "Enabling Stateful TCP Performance Profiling with Key Event Capturing," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2025, doi: 10.1109/TNSM.2025.3564336.

[24] S. Pelekis *et al.*, "Adversarial machine learning: a review of methods, tools, and critical industry sectors," *Artificial Intelligence Review 2025 58:8*, vol. 58, no. 8, pp. 1–87, May 2025, doi: 10.1007/S10462-025-11147-4.

[25] K. Pentikousis, Y. Wang, and W. Hu, "Mobileflow: Toward software-defined mobile networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 44–53, 2013, doi: 10.1109/MCOM.2013.6553677.

[26] O. A. Adeleke, N. Bastin, and D. Gurkan, "Network Traffic Generation: A Survey and Methodology," *ACM Comput Surv*, vol. 55, no. 2, p. 25, Feb. 2023, doi: 10.1145/3488375.

[27] M. Swann, J. Rose, G. Bendiab, S. Shiaeles, and N. Savage, "Tools for Network Traffic Generation -- A Quantitative Comparison," pp. 24–29, Sep. 2021, doi: 10.20533/WorldCIS.2020.0003.

[28] I. Badmus, A. Laghrissi, M. Matinmikko-Blue, and A. Pouttu, "End-to-end network slice architecture and distribution across 5G micro-operator leveraging multi-domain and multi-tenancy," *EURASIP J Wirel Commun Netw*, vol. 2021, no. 1, pp. 1–23, Dec. 2021, doi: 10.1186/S13638-021-01959-7/FIGURES/10.

[29] S. Alsaadi, T. J. Anande, and M. S. Leeson, "Comparative Analysis of 1D-CNN and 2D-CNN for Network Intrusion Detection in Software Defined Networks," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 193, pp. 480–491, 2024, doi: 10.1007/978-3-031-53555-0_46.

[30] "5G-NR workplan for eMBB." Accessed: May 13, 2025. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/5g-nr-workplan

[31] A. Blika *et al.*, "Federated Learning For Enhanced Cybersecurity And Trustworthiness In 5G and 6G Networks: A Comprehensive Survey," *IEEE Open Journal of the Communications Society*, 2024, doi: 10.1109/OJCOMS.2024.3449563.

[32] S. Batewela, M. Liyanage, E. Zeydan, M. Ylianttila, and P. Ranaweera, "Security Orchestration in 5G and Beyond Smart Network Technologies," *IEEE Open Journal of the Computer Society*, 2025, doi: 10.1109/OJCS.2025.3563619.
[33] L. Fernández Maimó, A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez, "Dynamic management of a deep learning-based anomaly detection system for 5G networks," *J Ambient Intell Humaniz Comput*, vol. 10, no. 8, pp. 3083–3097, Aug. 2019, doi: 10.1007/S12652-018-0813-4/FIGURES/8.
[34] C. Coldwell *et al.*, "Machine Learning 5G Attack Detection in Programmable Logic," *2022 IEEE GLOBECOM Workshops, GC Wkshps 2022 - Proceedings*, pp. 1365–1370, 2023, doi: 10.1109/GCWKSHPS56602.2022.10008647.
[35] P. Dass, A. Rajak, and R. Tripathi, "Machine learning-enabled techniques for anomaly detection in 5G networks," *2024 15th International Conference on Computing Communication and Networking Technologies, ICCCNT 2024*, 2024, doi: 10.1109/ICCCNT61001.2024.10724005.
[36] "5G-SliciNdd." Accessed: May 28, 2025. [Online]. Available: https://figshare.com/articles/dataset/5G-SliciNdd/24446515
[37] S. Samarakoon *et al.*, "5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network".
[38] F. Nizzi, T. Pecorella, C. Cerboni, M. Bastianini, A. Buzzigoli, and A. Fratini, "The role of network simulator in the 5G Experimentation," *ACM International Conference Proceeding Series*, pp. 13–17, Jun. 2019, doi: 10.1145/3337941.3337949.
[39] P. K. Gkonis, P. T. Trakadas, and D. I. Kaklamani, "A Comprehensive Study on Simulation Techniques for 5G Networks: State of the Art Results, Analysis, and Future Challenges," *Electronics 2020, Vol. 9, Page 468*, vol. 9, no. 3, p. 468, Mar. 2020, doi: 10.3390/ELECTRONICS9030468.
[40] S. J. Tucker and L. Rodriguez, "A Cybersecurity Architecture to Secure the 5G Network through Modeling & Simulation," 2025.
[41] S.-A. Smith-Haynes, "Advanced Penetration Testing for Enhancing 5G Security," Jul. 2024, Accessed: May 13, 2025. [Online]. Available: https://arxiv.org/pdf/2407.17269v1
[42] S. Researcher, "5G-LENA NR MODULE OVERVIEW BILJANA BOJOVIĆ."
[43] "Documentation | Open5GS." Accessed: May 13, 2025. [Online]. Available: https://open5gs.org/open5gs/docs/
[44] Y. E. Kim, Y. S. Kim, and H. Kim, "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network," *Sensors*, vol. 22, no. 10, May 2022, doi: 10.3390/S22103819.
[45] M. Barbosa, M. Silva, E. Cavalcanti, and K. Dias, "Open-Source 5G Core Platforms: A Low-Cost Solution and Performance Evaluation," Dec. 2024, doi: 10.48550/arXiv.2412.21162.
[46] A. Chouman, D. M. Manias, and A. Shami, "A Modular, End-to-End Next-Generation Network Testbed: Towards a Fully Automated Network Management Platform," Mar. 2024, doi: 10.48550/arXiv.2403.15376.
[47] G. Nardini, G. Stea, A. Virdis, and D. Sabella, "Simu5G: A System-level Simulator for 5G Networks", doi: 10.5220/0009826400680080.
[48] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Virdis, "SiMu5G–An OMNeT++ library for end-to-end performance evaluation of 5G networks," *IEEE Access*, vol. 8, pp. 181176–181191, 2020, doi: 10.1109/ACCESS.2020.3028550.

[49] G. Nardini, G. Stea, A. Virdis, D. Sabella, and P. Thakkar, "Using Simu5G as a realtime network emulator to test MEC apps in an end-to-end 5G testbed," *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, vol. 2020-August, Aug. 2020, doi: 10.1109/PIMRC48278.2020.9217177.

[50] C. Du, "Improving and Evaluating TRex Traffic Generator through P4 Switches," 2023, Accessed: May 14, 2025. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-332403

[51] C. V. Nahum *et al.*, "Testbed for 5G Connected Artificial Intelligence on Virtualized Networks," *IEEE Access*, vol. 8, pp. 223202–223213, 2020, doi: 10.1109/ACCESS.2020.3043876.

[52] J. S. N. G. S. B. Karamjeet Kaur, "(PDF) Mininet as Software Defined Networking Testing Platform," Accessed: May 14, 2025. [Online]. Available: https://www.researchgate.net/publication/287216738_Mininet_as_Software_Defined_Networking_Testing_Platform#fullTextFileContent

[53] C. Decusatis, A. Carranza, and J. Delgado-Caceres, "Modeling Software Defined Networks using Mininet," no. 133.

[54] S. Rohith Raj, R. Rohith, M. Moharir, and G. Shobha, "SCAPY-a powerful interactive packet manipulation program," *2018 International Conference on Networking, Embedded and Wireless Systems, ICNEWS 2018 - Proceedings*, Dec. 2018, doi: 10.1109/ICNEWS.2018.8903954.

[55] S. Avallone, D. Emma, A. Pescapé, and G. Ventre, "Performance evaluation of an open distributed platform for realistic traffic generation," *Performance Evaluation*, vol. 60, no. 1–4, pp. 359–392, May 2005, doi: 10.1016/J.PEVA.2004.10.012.

[56] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," *CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings*, pp. 237–242, Jan. 2014, doi: 10.1109/CINTI.2014.7028682.

[57] J. G. Andrews *et al.*, "What will 5G be?," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014, doi: 10.1109/JSAC.2014.2328098.

[58] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, May 2017, doi: 10.1109/MCOM.2017.1600951.

[59] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 19, no. 3, 2017, doi: 10.1109/COMST.2017.2705720.

[60] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G Networks: Use Cases and Technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, Mar. 2020, doi: 10.1109/MCOM.001.1900411.

[61] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55765–55779, 2018, doi: 10.1109/ACCESS.2018.2872781.

[62] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi, "An E2E Simulator for 5G NR Networks," *Simul Model Pract Theory*, vol. 96, Nov. 2019, doi: 10.1016/j.simpat.2019.101933.

[63] F. Dolente, R. G. Garroppo, and M. Pagano, “A Vulnerability Assessment of Open-Source Implementations of Fifth-Generation Core Network Functions,” *Future Internet 2024, Vol. 16, Page 1*, vol. 16, no. 1, p. 1, Dec. 2023, doi: 10.3390/FI16010001.