ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αξιοποίηση κρυπτογραφικών τεχνικών για τη βελτίωση της ιδιωτικότητας θέσης σε περιβάλλοντα IoV

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Ι. Κατσούρης

Επιβλέπουσα: Ιωάννα Ρουσσάκη
Επικ. Καθηγήτρια Ε.Μ.Π.

Αθήνα 2021

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αξιοποίηση κρυπτογραφικών τεχνικών για τη βελτίωση της ιδιωτικότητας θέσης σε περιβάλλοντα IoV

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος Ι. Κατσούρης

Επιβλέπουσα: Ιωάννα Ρουσσάκη
Επικ. Καθηγήτρια Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 26 Φεβρουαρίου 2021.

.....	.....	.....
Ιωάννα Ρουσσάκη	Μιλτιάδης Αναγνώστου	Συμεών Παπαβασιλείου
Επικ. Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα 2021

.....
Γεώργιος Ι. Κατσούρης
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π

Περίληψη

Η εξέλιξη του Internet of Things τα τελευταία χρόνια επεκτάθηκε και στον τομέα των μετακινήσεων, οδηγώντας στην ανάδυση ενός νέου ερευνητικού πεδίου το οποίο λέγεται Internet of Vehicles. Στο IoV, τα οχήματα μπορούν να ανταλλάσσουν πληροφορίες μεταξύ τους αλλά και με την υποδομή κάνοντας χρήση των Επι τούτω δικτύων για οχήματα (Vehicular Ad Hoc Network – VANET). Όσο όμως αυτή η τεχνολογία γίνεται όλο και πιο συνηθισμένη στην καθημερινότητα, εγείρονται ερωτήματα σχετικά με την εξασφάλιση της ιδιωτικότητας των χρηστών, καθώς ταυτόχρονα αυξάνεται το ενδιαφέρον κακόβουλων ατόμων ή οργανισμών για αυτά τα δεδομένα. Για αυτό το λόγο, έχουν αναζητηθεί και προταθεί διάφορες τεχνικές για την προστασία της ιδιωτικότητας στο IoV, στρεφόμενες κυρίως γύρω από την συχνή αλλαγή της ταυτότητας των οχημάτων.

Η παρούσα εργασία στοχεύει στην επισκόπηση και αξιολόγηση σύγχρονων τεχνικών προστασίας ιδιωτικότητας θέσης, καθώς επίσης και στη μελέτη κρυπτογραφικών τεχνικών για τη βελτίωση της ασφάλειας των μηνυμάτων. Στο πρώτο σκέλος γίνεται μια παρουσίαση της σύγχρονης βιβλιογραφίας πάνω σε αυτόν τον ερευνητικό τομέα για τις πιο δημοφιλείς τεχνικές προστασίας ιδιωτικότητας θέσης. Όσον αφορά στο δεύτερο σκέλος της εργασίας, πραγματοποιήθηκαν προσομοιώσεις 3 διαφορετικών κρυπτογραφικών αλγορίθμων (RSA, ECC, NTRU) πάνω σε ένα μοντέλο προστασίας ιδιωτικότητας, με σκοπό την εξαγωγή χρήσιμων συμπερασμάτων για την δυνατότητα υλοποίησης του κάθε αλγορίθμου στο συγκεκριμένο πεδίο εφαρμογών.

Λέξεις-Κλειδιά

Διαδίκτυο των Αντικειμένων (IoT), Διαδίκτυο των Οχημάτων (IoV), ιδιωτικότητα θέσης, MixGroup, ψηφιακή υπογραφή, RSA, ECC, NTRU, εντροπία ψευδωνύμου, κατανάλωση ενέργειας, μέγεθος μηνύματος

Abstract

The recent evolution of IoT has been propagated to the transportation field, leading to the emergence of a new research field that is called Internet of Vehicles (IoV). In this paradigm, interconnected vehicles are able to exchange freely information between each other and the infrastructure providing the network, using Vehicular Ad Hoc Networks (VANETs). Nevertheless, while this technology thrives and infiltrates everyday life, issues arise about securing the privacy of users, as the interest of malicious persons or organizations is piqued about sensitive data. For this reason, various privacy enhancing techniques for IoV have been proposed and they mainly revolve around the frequent change of vehicle identity in order to confuse a malicious observer.

This diploma thesis aims to provide an overview and an evaluation of modern location privacy techniques, and also study the use of different cryptographic methods for improving message security. In the first part, we present the state of the art on the field of location privacy protection. Regarding the second part of this work, we have conducted simulations utilizing 3 different cryptographic algorithms (RSA, ECC, NTRU) on a specific location privacy model, aiming to extract useful observations about the application possibility of each algorithm on this field.

Keywords

Internet of Things (IoT), Internet of Vehicles (IoV), location privacy, MixGroup, digital signature, RSA, ECC, NTRU, pseudonym entropy, energy consumption, message size

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαιτέρως την επιβλέπουσα καθηγήτρια κα. Ιωάννα Ρουσσάκη για την ευκαιρία που μου έδωσε να ασχοληθώ με το συγκεκριμένο αντικείμενο, καθώς και για τις πολύτιμες συμβουλές και οδηγίες της κατά την εκπόνηση της παρούσας διπλωματικής εργασίας. Θα ήθελα επίσης να ευχαριστήσω θερμά τον διδακτορικό ερευνητή κο. Γεώργιο Ρούτη για την καθοδήγηση και βοήθεια που μου προσέφερε σε όλη την πορεία της εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τους γονείς μου και τον αδερφό μου για όλη την αγάπη, στήριξη και υπομονή που μου έδειξαν όλα αυτά τα χρόνια. Χωρίς αυτούς δε θα βρισκόμουν εδώ που είμαι και ελπίζω να συνεχίσω να τους δίνω χαρά και περηφάνια.

Τέλος, θα ήθελα να ευχαριστήσω τους φίλους μου που πάντα ήταν δίπλα μου, καθώς και τους συμφοιτητές μου με τους οποίους έζησα τα χρόνια μου στη σχολή. Ειδική μνεία αξίζει στον Φάνη, που μου αποκάλυψε το δρόμο του σωστού μηχανικού.

Πίνακας Περιεχομένων

Περίληψη 5
Λέξεις-Κλειδιά 5
Abstract 7
Keywords 7
Ευχαριστίες 9
Πίνακας Περιεχομένων 11
Πίνακας Εικόνων 14
Περιεχόμενα Πινάκων 15
Κεφάλαιο 1: Εισαγωγή 16
1.1 Κίνητρο Έρευνας 16
1.2 Στόχοι διπλωματικής 16
1.3 Οργάνωση Κειμένου 17
Κεφάλαιο 2: Θεωρητικό Υπόβαθρο 18
2.1 Έννοιες Κρυπτογραφίας 18
2.1.1 Συμμετρική κρυπτογράφηση 18
2.1.2 Ασύμμετρη κρυπτογράφηση 20
2.1.3 Ψηφιακές υπογραφές 22
2.1.4 Πιστοποιητικά Δημοσίου Κλειδιού 23
2.2 Έννοιες Δικτύων 25
2.2.1 OSI model 25
2.2.2 Ethernet 27
2.2.3 Wifi 29
2.3 Ασφάλεια και Ιδιωτικότητα 30
2.3.1 Απαιτήσεις ασφάλειας και ιδιωτικότητας 30
2.3.2 Τύποι επιτιθέμενων 32
2.3.3 Επιθέσεις 33
2.4 Ορισμοί 34
Κεφάλαιο 3: Συναφής βιβλιογραφία 36
3.1 Mix-Zone 36
3.2 Group 38
3.3 Σιωπηλή Περίοδος(Silent Period) 40

3.4 Mix-Group 41
Κεφάλαιο 4: Εργαλεία, αλγόριθμοι και μετρικές 45
4.1 Εργαλεία 45
4.1.1 NS-3 46
4.1.2 SUMO(Simulation of Urban Mobility) 47
4.1.3 NetAnim 49
4.1.4 PyViz 49
4.1.5 Tcpdump 49
4.2 Αλγόριθμοι κρυπτογράφησης 50
4.2.1 AES(Advanced Encryption Standard) 50
4.2.2 RSA 54
4.2.3 ECC(Elliptic Curve Cryptography) 55
4.2.4 NTRU 57
4.3 Μετρικές αξιολόγησης 57
4.3.1 Εντροπία 57
4.3.2 Κρυπτογραφικές μετρικές 58
4.3.2.1 Μήκος κλειδιών 58
4.3.2.2 Χρόνος κρυπτογραφίας 59
4.3.2.3 Χρόνος παραγωγής κλειδιών 59
4.3.2.3 Χρόνος κρυπτογράφησης/αποκρυπτογράφησης 60
4.3.2.4 Χρόνος υπογραφής/επαλήθευσης 60
4.3.3 Μέγεθος μηνυμάτων 60
4.3.4 Κατανάλωση ενέργειας 60
Κεφάλαιο 5: Περιγραφή του προβλήματος – Μοντελοποίηση 62
5.1 Παρουσίαση του προβλήματος 62
5.2 Μοντέλο Δικτύου 62
5.3 Μοντέλο Επιτιθέμενων 64
Κεφάλαιο 6: Λύση-Υλοποίηση 65
6.1 Ανταλλαγή ψευδωνύμων 65
6.2 Ενεργοποίηση ψευδωνύμου 66
6.3 Αξιολόγηση οφέλους ανταλλαγής 66
6.4 Υλοποίηση κρυπτογραφικών τεχνικών 68
6.4.1 AES 68

6.4.2 RSA 70
6.4.3 ECC 72
6.4.4 NTRU 74
6.5 Υλοποίηση μοντέλου ενέργειας 76
6.6 Υλοποίηση οδικού δικτύου και κίνησης οχημάτων 77
6.7 Υλοποίηση δικτύου επικοινωνίας 78
Κεφάλαιο 7: Πειραματική αξιολόγηση και συμπεράσματα 79
7.1 Πειραματική Αξιολόγηση 80
7.1.1 Παραγωγή Κλειδιών 80
7.1.2 Παραγωγή Πιστοποιητικών 81
7.1.3 Χρόνος Κρυπτογράφησης 82
7.1.4 Χρόνος Αποκρυπτογράφησης 83
7.1.5 Παραγωγή Υπογραφής 83
7.1.6 Επαλήθευση Υπογραφής 84
7.1.7 Μέγεθος Μηνυμάτων 85
7.1.8 Κατανάλωση Ενέργειας 88
7.1.9 Εντροπία Ψευδωνύμων 89
7.2 Συμπεράσματα 90
7.2.1 NTRU 90
7.2.2 RSA 90
7.2.3 ECC 91
7.3 Μελλοντικές Επεκτάσεις 91
Κεφάλαιο 8: Επίλογος 93
Κεφάλαιο 9: Βιβλιογραφία 94

Πίνακας Εικόνων

Εικόνα 1: Συμμετρική κρυπτογράφηση 18
Εικόνα 2: Ασύμμετρη κρυπτογράφηση 20
Εικόνα 3: Ψηφιακή υπογραφή 23
Εικόνα 4: Επίθεση Man-in-the-Middle 24
Εικόνα 5: Μοντέλο OSI 27
Εικόνα 6: Δομή πακέτου Ethernet 28
Εικόνα 7: Δομή πλαισίου Wifi 29
Εικόνα 8: Mix-Zone 36
Εικόνα 9: Silent Period 40
Εικόνα 10: MixGroup 42
Εικόνα 11: Λειτουργία MixGroup 43
Εικόνα 12: Κρυπτογράφηση AES 52
Εικόνα 13: Αποκρυπτογράφηση AES 53
Εικόνα 14: Μοντέλο Δικτύου 64
Εικόνα 15: Υλοποίηση κρυπτογράφησης μηνύματος 69
Εικόνα 16: Δομή μηνύματος ασφαλείας 78
Εικόνα 17: Χρόνοι παραγωγής κλειδιών(ms) 80
Εικόνα 18: Χρόνοι παραγωγής πιστοποιητικών(ms) 81
Εικόνα 19: Χρόνοι κρυπτογράφησης(ms) 82
Εικόνα 20: Χρόνοι αποκρυπτογράφηση(ms) 83
Εικόνα 21: Χρόνοι παραγωγής υπογραφής(ms) 83
Εικόνα 22: Χρόνοι επαλήθευσης υπογραφής(ms) 84
Εικόνα 23: Μέγεθος μηνυμάτων(Bytes) στη φάση διαπραγμάτευσης 86
Εικόνα 24: Μέγεθος μηνυμάτων(bytes) στη φάση ανταλλαγής ψευδωνύμων 87
Εικόνα 25: Μέγεθος μηνυμάτων(bytes) στη φάση ενεργοποίησης νέου ψευδωνύμου 87
Εικόνα 26: Κατανάλωση ενέργειας(Joule) στη φάση ανταλλαγής ψευδωνύμων 88
Εικόνα 27: Συνολική εντροπία των οχημάτων στο χρόνο(s) 89

Περιεχόμενα Πινάκων

Πίνακας 1: Σχέση μήκους κλειδιού-αριθμού γύρων στο AES 51
Πίνακας 2: Σύγκριση μήκους κλειδιών ECC και RSA 56

Κεφάλαιο 1: Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται το κίνητρο που οδήγησε στη συγγραφή της παρούσας διπλωματικής, οι στόχοι της καθώς επίσης και ο τρόπος διάρθρωσης τους κειμένου.

1.1 Κίνητρο Έρευνας

Το Διαδίκτυο των Αντικειμένων(Internet of Things - IoT) είναι ένας τεχνολογικός κλάδος που έχει αναπτυχθεί ραγδαία από την εμφάνισή του 20 χρόνια πρίν, με εφαρμογές σε πάρα πολλούς τομείς(υπηρεσίες υγείας, οικιακή διαχείριση, συλλογή και επεξεργασία δεδομένων, ασφάλεια και μεταφορά). Ένας κλάδος στον οποίο η ενσωμάτωση με το IoT παρουσιάζει ιδιαίτερο επιστημονικό και εμπορικό ενδιαφέρον είναι τα Έξυπνα Συστήματα Μεταφοράς(Intelligent Transportation Systems – ITS). Η χρήση του IoT μπορεί να οδηγήσει στην αποφυγή ατυχημάτων, στη βελτίωση των οδικών συνθηκών(ρύθμιση κυκλοφορίας για την αποφυγή συμφόρησης, ενημέρσωη δρομολογίων κτλ.) αλλά και στην παροχή υπηρεσιών προς τους οδηγούς(επιλογή διαδρομής, ενημέρωση για κοντινά σημεία ενδιαφέροντος, αυτόματη πληρωμή διοδίων κτλ.). Η ενσωμάτωση του IoT στα οχήματα οδηγεί στη δημιουργία δίκτύων οχημάτων με δυνατότητα συνεχούς επικοινωνίας, με αποτέλεσμα να οδηγούμαστε στην εμφάνιση του λεγόμενου IoV(Internet of Vehicles), έναν καινοφανή κλάδο του IoT με σημαντικό αντίκτυπο στην καθημερινότητα, κρίνοντας από τον αριθμό των οχημάτων στον κόσμο.

Όπως και σε κάθε κλάδο της τεχνολογίας, έτσι και στο IoV υπάρχει η ανάγκη για τη διασφάλιση του από εσωτερικούς και εξωτερικούς κινδύνους. Πέρα από τη φυσική ασφάλεια των χρηστών, σχεδόν εξίσου σημαντική είναι η ασφάλεια των δεδομένων τους, με τις απαιτήσεις ασφαλείας να είναι ιδιαιτέρως αυστηρές. Επιπλέον, τα τελευταία χρόνια υπάρχει ιδιαίτερο ενδιαφέρον και συζήτηση για την ιδιωτικότητα, με τις απαιτήσεις ιδιωτικότητας να αποκτούν όλο και περισσότερη ισχύ στις νέες εφαρμογές. Η παραπάνω τάση έχει κινητοποιήσει την ερευνητική κοινότητα να μελετήσει μεθόδους εξασφάλισης της ιδιωτικότητας σε διάφορους τομείς της τεχνολογίας. Είναι φανερό λοιπόν, πως και στο IoV έχει ενδιαφέρον η μελέτη και εξασφάλιση της ιδιωτικότητας των χρηστών, ειδικά από τη στιγμή που οι πιθανές επιπλοκές από διαρροή ευαίσθητων δεδομένων μπορεί να είναι άμεσες για τα φυσικά πρόσωπα.

1.2 Στόχοι διπλωματικής

Ο στόχος της παρούσας εργασίας είναι διπλός. Ο πρώτος στόχος είναι η πιστή ανακατασκευή και προσομοίωση μιας προτεινόμενης μεθόδου εξασφάλισης ιδιωτικότητας, προκειμένου να αξιολογηθούν τα αποτελέσματά της και να κατανοήσουμε καλύτερα τον τρόπο λειτουργίας της. Ο δεύτερος στόχος, είναι η τροποποίηση ή επέκταση της παραπάνω μεθόδου, σε σημεία που είναι πιο αφηρημένη, για την εξερεύνηση πιθανών βελτιώσεων πάνω σε πρακτικές μετρικές όπως το μέγεθος και οι χρόνοι επεξεργασίας μηνυμάτων ή ακόμα και η κατανάλωση ενέργειας. Ιδιαίτερη έμφαση δόθηκε στις κρυπτογραφικές μεθόδους που χρησιμοποιούνται στην ανταλλαγή μηνυμάτων.

1.3 Οργάνωση Κειμένου

Η οργάνωση του κειμένου γίνεται ως εξής: Στο κεφάλαιο 2 παρουσιάζονται οι βασικές έννοιες κρυπτογραφίας, δικτύων, ασφάλειας και ιδιωτικότητας καθώς επίσης και κάποιοι απαραίτητοι ορισμοί. Στο κεφάλαιο 3 γίνεται μια επισκόπηση της σύγχρονης συναφούς βιβλιογραφίας πάνω σε διαφορετικές τεχνικές ιδιωτικότητας θέσης των δικτύων οχημάτων. Στο κεφάλαιο 4 παρουσιάζονται τα προγραμματιστικά εργαλεία που χρησιμοποιήθηκαν για τις προσομοιώσεις, αναλύονται οι αλγόριθμοι κρυπτογράφησης που υλοποιήθηκαν και περιγράφονται οι μετρικές αξιολόγησης που χρησιμοποιήθηκαν. Στο κεφάλαιο 5 παρουσιάζεται το πρόβλημα και η σχετική μοντελοποίηση που έγινε. Στη συνέχεια, στο κεφάλαιο 6 αναλύεται η υλοποίηση που ακολουθήσαμε για τα διαφορετικά τμήματα του μοντέλου και για τις διαφορετικές κρυπτογραφικές τεχνικές. Τέλος, στο κεφάλαιο 7 καταγράφονται τα πειραματικά αποτελέσματα των προσομοιώσεων και διατυπώνονται συμπεράσματα καθώς και πιθανές μελλοντικές επεκτάσεις.

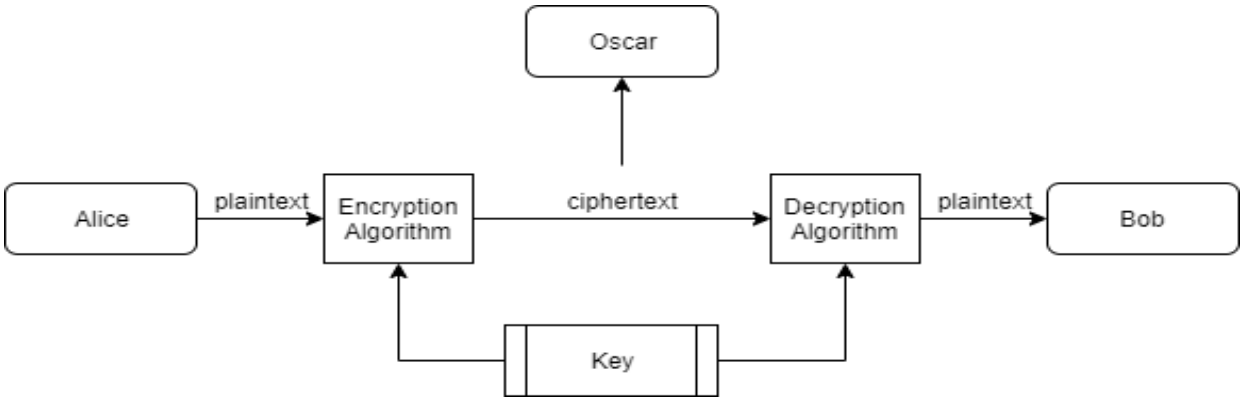
Κεφάλαιο 2: Θεωρητικό Υπόβαθρο

Στο κεφάλαιο αυτό παρουσιάζεται το θεωρητικό υπόβαθρο στο οποίο στηρίζεται η εργασία. Αρχικά, παρουσιάζονται σημαντικές έννοιες κρυπτογραφίας που αξιοποιήσαμε στην έρευνά μας. Στη συνέχεια, γίνεται μια αναφορά σε βασικές έννοιες και τεχνολογίες δικτύων. Ακόμα, παρουσίαζονται οι διαφορετικές απαιτήσεις ασφάλειας και ιδιωτικότητας μαζί με τους διάφορους επιτιθέμενους και τρόπους επίθεσης. Τέλος, γίνεται επεξήγηση της ορολογίας που χρησιμοποιείται στην παρούσα εργασία.

2.1 Έννοιες Κρυπτογραφίας

2.1.1 Συμμετρική κρυπτογράφηση

Συμμετρική κρυπτογράφηση, ή αλλιώς κρυπτογράφηση μυστικού κλειδιού, ονομάζεται η τεχνική στην οποία το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει μια πληροφορία είναι το ίδιο που χρειάζεται για να αποκρυπτογραφηθεί το παραγόμενο κρυπτοκείμενο. Για την καλύτερη κατανόηση της έννοιας, χρησιμοποιείται το γνωστό παράδειγμα της Alice και του Bob:
Έστω ότι έχουμε 2 χρήστες, την Alice και τον Bob, οι οποίοι θέλουν να επικοινωνήσουν μέσα από ένα μη ασφαλές «κανάλι». Ως κανάλι θεωρείται το μέσο επικοινωνίας, όποιο και αν είναι αυτό(Internet, WiFi, Radio, κ.α.). Το μη ασφαλές σημαίνει ότι κάποιος τρίτος, ας τον πούμε Oscar, μπορεί να αποκτήσει πρόσβαση στο κανάλι και να κρυφακούσει το μήνυμα, κάτι το οποίο η Alice και ο Bob δε θέλουν να συμβεί. Για αυτό λοιπόν εφαρμόζουν την παρακάτω μέθοδο: η Alice χρησιμοποιεί ένα συμμετρικό αλγόριθμο και κρυπτογραφεί το μήνυμα της παράγοντας ένα κρυπτοκείμενο, το οποίο μεταδίδεται στον Bob που στη συνέχεια εφαρμόζει τον αντίστροφο αλγόριθμο και αποκτάει το αρχικό κείμενο. Αν ο αλγόριθμος που χρησιμοποιήθηκε είναι ασφαλής και ο Oscar δε γνωρίζει το κλειδί με το οποίο γίνεται η κρυπτογράφηση/αποκρυπτογράφηση, τότε δεν μπορεί να αποκτήσει καμία ουσιώδη πληροφορία από το μήνυμα που υπέκλεψε.



Εικόνα 1: Συμμετρική κρυπτογράφηση

Από το παραπάνω παράδειγμα γίνονται φανερές οι βασικές έννοιες της συμμετρικής κρυπτογράφησης:

- Αρχικό μήνυμα(plaintext): Η πληροφορία που πρέπει να μεταδοθεί.
- Αλγόριθμος κρυπτογράφησης(encryption algorithm): Ένας αλγόριθμος αντιμεταθέσεων και αντικαταστάσεων που εφαρμόζεται πάνω στο αρχικό μήνυμα προκειμένου να το καταστήσει ακατανόητο σε έναν ωτακουστή.
- Μυστικό Κλειδί(secret key): Το μυστικό κλειδί είναι ανεξάρτητο από το μήνυμα και τον αλγόριθμο και για κάθε διαφορετικό κλειδί ο αλγόριθμος παράγει διαφορετικό αποτέλεσμα.
- Κρυπτοκείμενο(ciphertext):Είναι το κείμενο που παράγεται από τον αλγόριθμο κρυπτογράφησης. Εξαρτάται από το αρχικό μήνυμα και το κλειδί και φαινομενικά είναι μια τυχαία σειρά συμβόλων, επομένως είναι μη κατανοητό.
- Αλγόριθμος αποκρυπτογράφησης(decryption algorithm): Είναι η αντίστροφη διαδικασία της κρυπτογράφησης, που δεδομένου του κρυπτοκειμένου και του μυστικού κλειδιού, μπορεί να παράξει το αρχικό μήνυμα.

Προφανώς αν ο επιτιθέμενος με κάποιον τρόπο αποκτήσει το κλειδί ή μπορέσει να εκμεταλλευτεί κάποια αδυναμία του αλγορίθμου που χρησιμοποιείται, το παραπάνω σχήμα καταρρέει. Επομένως, για την ασφαλή χρήση της συμμετρικής κρυπτογράφησης, και γενικά της συμβατικής κρυπτογράφησης, πρέπει να πληρούνται οι παρακάτω απαιτήσεις:

1. Ο αλγόριθμος πρέπει να είναι ισχυρός, το οποίο σημαίνει ένας επιτιθέμενος να μην μπορεί να αποκρυπτογραφήσει το μήνυμα ή να ανακαλύψει το κλειδί ακόμα και αν γνωρίζει ποιος είναι ο αλγόριθμος και έχει στη διάθεσή του ένα πλήθος από κρυπτοκείμενα μαζί με τα αρχικά τους μηνύματα. Η δημοσιοποίηση των αλγορίθμων, παρότι φαίνεται να πηγαίνει ενάντια στην κοινή λογική, είναι ο καλύτερος τρόπος για την εγγύηση της ασφάλειάς τους καθώς μπορούν να αναλυθούν από την κοινότητα για τυχόν αδυναμίες.
2. Το μυστικό κλειδί που χρησιμοποιείται πρέπει να διανέμεται με ασφαλή τρόπο στον αποστολέα και τον παραλήπτη του μηνύματος και να φυλάσσεται μυστικό από οποιονδήποτε άλλον. Ουσιαστικά λοιπόν, το πρόβλημα της ασφαλής μετάδοσης ενός μηνύματος εκφυλίζεται στο πρόβλημα της ασφαλής μετάδοσης και φύλαξης του μυστικού κλειδιού.

Έχουν αναπτυχθεί πάρα πολλοί συμμετρικοί αλγόριθμοι με στόχο να είναι υπολογιστικά ασφαλείς. Ένας αλγόριθμος θεωρείται υπολογιστικά ασφαλής(computationally secure) αν το κόστος που απαιτείται για την παραβίασή του ξεπερνά την αξία της κρυπτογραφημένης πληροφορίας ή αν ο χρόνος που απαιτείται για να παραβιαστεί ξεπερνά το χρονικό διάστημα για το οποίο αυτή η πληροφορία έχει αξία. Στην πράξη, είναι δύσκολο να εκτιμηθεί ακριβώς τι πόροι χρειάζονται για να σπάσει ένα κρυπτοσύστημα καθώς κάποιες επιθέσεις ωφελούνται περισσότερο από την αύξηση της υπολογιστικής ισχύος ενώ άλλες εκμεταλλεύονται απευθείας αδυναμίες των αλγορίθμων.

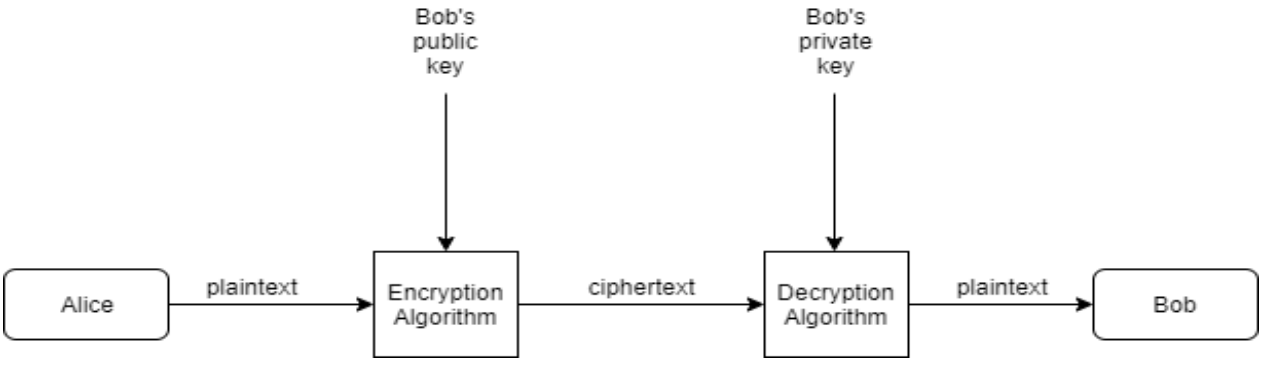
Το πρόβλημα της ασφαλούς μεταφοράς του κλειδιού είναι πολύ σημαντικό και υπάρχει μια πληθώρα μεθόδων και αλγορίθμων που το αντιμετωπίζουν. Από την φυσική μεταφορά των κλειδιών μέχρι τη χρήση ασύμμετρων αλγορίθμων(βλ. Ασύμμετρη κρυπτογράφηση) για τη

μεταφορά ενός τυχαία επιλεγμένου κλειδιού, έχει υπάρξει εκτενής έρευνα στον τομέα αυτό και είναι ένα ζήτημα που απασχολεί οποιαδήποτε κρυπτογραφική υλοποίηση.

Η χρήση αλγορίθμων κρυπτογράφησης είναι απαραίτητη στη σημερινή εποχή, με τον όγκο των ευαίσθητων πληροφοριών που παράγονται καθημερινά. Για αυτό το σκοπό έχουν υλοποιηθεί πολλαπλοί αλγόριθμοι, πολλές φορές με την παρακίνηση και υποστήριξη διεθνών και κρατικών οργανισμών. Η ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης που προσφέρουν οι συμμετρικοί αλγόριθμοι τους καθιστά ιδανική επιλογή για την κρυπτογράφηση μεγάλου όγκου δεδομένων. Επίσης, οι σύγχρονοι συμμετρικοί αλγόριθμοι θεωρούνται σχετικά ασφαλείς απέναντι σε επιθέσεις κβαντικού υπολογισμού σε αντίθεση με την πλειονότητα των ασύμμετρων αλγορίθμων. Ορισμένοι από τους πιο δημοφιλείς συμμετρικούς αλγορίθμους σήμερα είναι οι: Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer+/++ (Bluetooth), IDEA κ.α.

2.1.2 Ασύμμετρη κρυπτογράφηση

Σε αντίθεση με τη συμμετρική κρυπτογράφηση, η οποία έχει τις ρίζες της στην αρχαιότητα και εφαρμόζεται εδώ και χιλιάδες χρόνια, η ασύμμετρη κρυπτογράφηση ή κρυπτογράφηση δημοσίου κλειδιού(οι όροι αυτοί είναι ισοδύναμοι) είναι κατά πολύ νεότερη με την εισαγωγή της να γίνεται από τους Diffie, Hellman και Merkle το 1976. Έφερε τη μεγαλύτερη ίσως επανάσταση στον τομέα της κρυπτογραφίας, καθώς εισήγαγε την έννοια του δημοσίου κλειδιού. Σε αυτό το σχήμα υπάρχουν 2 ειδών κλειδιά, ο αποστολέας χρησιμοποιεί για την κρυπτογράφηση το ένα κλειδί το οποίο δεν είναι μυστικό, το δημόσιο κλειδί, και μόνο ο κάτοχος του δεύτερου κλειδιού που είναι μυστικό μπορεί να αποκρυπτογραφήσει το μήνυμα. Ας δούμε πάλι το προηγούμενο παράδειγμα: Η Alice θέλει να στείλει ένα μήνυμα στον Bob. Ο Bob μοιράζεται το δημόσιο κλειδί του με την Alice(και οποιονδήποτε άλλο είναι σε θέση να το ακούσει), το οποίο χρησιμοποιεί η Alice για να κρυπτογραφήσει το μήνυμά της. Το κρυπτοκείμενο μεταφέρεται μέσα από το μη ασφαλές μέσο και ο Bob για να ανακτήσει το αρχικό κείμενο χρησιμοποιεί το ιδιωτικό του κλειδί, το οποίο γνωρίζει μόνο αυτός. Έτσι, ακόμα και αν κάποιος επιτιθέμενος αποκτήσει το κρυπτοκείμενο και το δημόσιο κλειδί του Bob, δε θα μπορεί να αποκρυπτογραφήσει το μήνυμα γιατί θα του λείπει το ιδιωτικό κλειδί του Bob.



Εικόνα 2: Ασύμμετρη κρυπτογράφηση

Οι βασικές έννοιες που αναφέρθηκαν στη συμμετρική κρυπτογράφηση ισχύουν και εδώ με τη διαφορά ότι το μυστικό κλειδί αντικαθίσταται από 2 διαφορετικά κλειδιά, το δημόσιο και το ιδιωτικό. Οι απαιτήσεις ενός αλγόριθμου ασύμμετρης κρυπτογράφησης όπως ορίστηκαν από τους Diffie και Helman[1] είναι οι εξής:

1. Είναι υπολογιστικά εύκολο για τον Bob να παράξει το ζεύγος κλειδιών.
2. Είναι υπολογιστικά εύκολο για την Alice να παράξει το κρυπτοκείμενο, δεδομένου του αρχικού μηνύματος και του δημοσίου κλειδιού.
3. Είναι υπολογιστικά εύκολο για τον Bob αν αποκρυπτογραφήσει το κρυπτοκείμενο με το ιδιωτικό του κλειδί.
4. Είναι υπολογιστικά ανέφικτο για έναν επιτιθέμενο να ανακαλύψει το ιδιωτικό κλειδί του Bob, με δεδομένο μόνο το δημόσιο κλειδί του.
5. Είναι υπολογιστικά ανέφικτο για έναν επιτιθέμενο να ανακτήσει το αρχικό μήνυμα, δεδομένου του κρυπτοκειμένου και του δημόσιου κλειδιού.

Με βάση τα παραπάνω, είναι εμφανές πως τα σχήματα δημοσίου κλειδιού αντιμετωπίζουν το πρόβλημα της διαχείρισης κλειδιών που παρουσιάζει η συμμετρική κρυπτογράφηση, καθώς δε χρειάζεται η ασφαλής μετάδοση τους ανάμεσα στον αποστολέα και τον παραλήπτη, δεν είναι όμως η μόνη τους εφαρμογή. Πιο συγκεκριμένα, υπάρχουν 3 βασικές κατηγορίες εφαρμογών στις οποίες εφαρμόζονται τα ασύμμετρα κρυπτοσυστήματα:

- Κρυπτογράφηση/αποκρυπτογράφηση: Κάποιοι αλγόριθμοι μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων, όπως φάνηκε και από το παράδειγμα.
- Ανταλλαγή κλειδιών: Αυτά τα σχήματα μπορούν να χρησιμοποιηθούν για την ανταλλαγή κλειδιών πάνω από ένα μη ασφαλές μέσο.
- Ψηφιακή υπογραφή: Επιτρέπει στον παραλήπτη να επιβεβαιώσει την ακεραιότητα του μηνύματος, καθώς και τη μη αποποίηση ευθυνών(non-repudiation) του αποστολέα.

Κάποιοι αλγόριθμοι είναι κατάλληλοι και για τις 3 εφαρμογές, ενώ κάποιοι άλλοι μπορούν να χρησιμοποιηθούν σε 1 ή 2 από αυτές.

Παρά την ικανότητα των αλγορίθμων ασύμμετρης κρυπτογράφησης να καλύψουν τις απαιτήσεις της σύγχρονης ασφάλειας επικοινωνιών, παρουσιάζουν έναν αριθμό από σημαντικά πλεονεκτήματα. Το πιο βασικό από αυτά είναι το υπολογιστικό κόστος κρυπτογράφησης με έναν τέτοιο αλγόριθμο, το οποίο μπορεί να είναι εκατοντάδες ή ακόμα και χιλιάδες φορές μεγαλύτερο από έναν συμμετρικό αλγόριθμο. Για αυτόν το λόγο, η συνηθέστερη πρακτική που ακολουθείται είναι να χρησιμοποιούνται αυτά τα σχήματα για την κρυπτογράφηση ενός συμμετρικού κλειδιού, το οποίο στη συνέχεια μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του κυρίως μηνύματος. Ένας ακόμα περιορισμός που εμφανίζεται είναι συνήθως το μήκος των κλειδιών που χρησιμοποιούνται, καθώς η φύση των μαθηματικών προβλημάτων στα οποία στηρίζονται προϋποθέτει τη χρήση μεγαλύτερου μεγέθους κλειδιών για την επίτευξη του επιθυμητού επιπέδου ασφαλείας. Για παράδειγμα, ο ασύμμετρος αλγόριθμος RSA με μήκος κλειδιού 3072 bits παρουσιάζει αντίστοιχο επίπεδο ασφαλείας με τον συμμετρικό αλγόριθμο AES με μήκος κλειδιού 128 bits.

Όπως προαναφέρθηκε, το βασικότερο πλεονέκτημα των αλγορίθμων δημοσίου κλειδιού από τους συμμετρικούς είναι η ελεύθερη διανομή κλειδιών. Αυτό όμως δημιουργεί το πρόβλημα της αυθεντικότητας των κλειδιών: πώς μπορεί να επιβεβαιωθεί ότι ένα κλειδί ανήκει στον

συγκεκριμένο χρήστη; Εφόσον το μέσο στο οποίο μεταδίδονται τα κλειδιά δεν είναι ασφαλές, κάποιος επιτιθέμενος μπορεί να παρέμβει στην επικοινωνία και να αντικαταστήσει τα αυθεντικά κλειδιά με δικά του, υποδυόμενος το ένα μέρος της επικοινωνίας. Αυτό σημαίνει ότι πρέπει να υπάρχει μια μέθοδος διασφάλισης της ακεραιότητας και αυθεντικότητας των κλειδιών. Αυτό επιτυγχάνεται στην πράξη με τη χρήση ψηφιακών υπογραφών και πιστοποιητικών, τα οποία αναλύονται στη συνέχεια.

2.1.3 Ψηφιακές υπογραφές

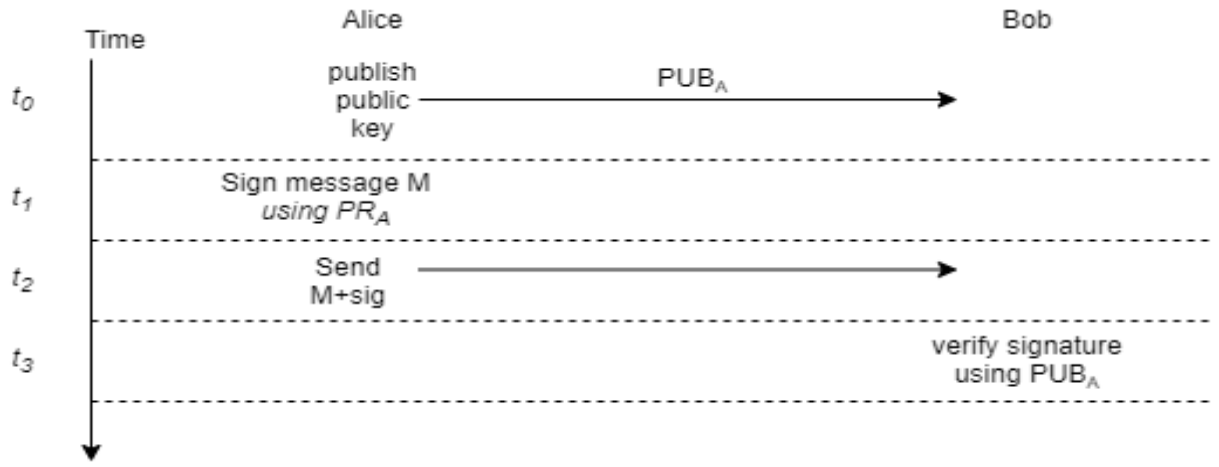
Όπως προαναφέρθηκε, η αυθεντικοποίηση των μηνυμάτων ήταν από πάντα ζωτικής σημασίας στην επικοινωνία. Στο φυσικό κόσμο αυτό το ζήτημα έχει αντιμετωπιστεί με τη χρήση χειρόγραφων υπογραφών. Αντίστοιχα, στη ψηφιακή επικοινωνία έχει αναπτυχθεί η έννοια της ψηφιακής υπογραφής. Οι ψηφιακές υπογραφές πρέπει κατ' ελάχιστο να έχουν τις βασικές ιδιότητες των φυσικών υπογραφών, οι οποίες είναι:

- Πιστοποίηση του υπογράφοντα και της ημερομηνίας και ώρας της υπογραφής.
- Αυθεντικοποίηση των δεδομένων κατά τη στιγμή της υπογραφής.
- Επαλήθευση από κάποιον τρίτο.

Με βάση τις παραπάνω ιδιότητες, μια ψηφιακή υπογραφή πρέπει να καλύπτει τις εξής απαιτήσεις:

- Πρέπει να εξαρτάται από το μήνυμα που υπογράφεται
- Πρέπει να χρησιμοποιεί κάποιες πληροφορίες που γνωρίζει μόνο ο αποστολέας, προκειμένου να αποφευχθεί πιθανή πλαστογραφία ή αποποίηση ευθυνών
- Πρέπει να παράγεται υπολογιστικά εύκολα
- Πρέπει να μπορεί να αναγνωριστεί και να πιστοποιηθεί σχετικά εύκολα
- Πρέπει να είναι υπολογιστικά ανέφικτη η πλαστογράφηση της υπογραφής, είτε με την κατασκευή ενός άλλου μηνύματος για μια δεδομένη υπογραφή, είτε με την κατασκευή μιας πλαστής υπογραφής για ένα δεδομένο μήνυμα.
- Πρέπει να είναι δυνατή η διατήρηση αντιγράφων της υπογραφής.

Για την καλύτερη κατανόηση αυτής της έννοιας, δίνεται το ακόλουθο παράδειγμα: Έστω ότι η Alice θέλει να στείλει ένα μήνυμα στον Bob. Η Mallory επεμβαίνει στην επικοινωνία και αντικαθιστά το μήνυμα της Alice με ένα δικό της. Πώς μπορεί ο Bob να καταλάβει ότι αυτό το μήνυμα έχει τροποποιηθεί(έχει αλλαχτεί μέρος του μηνύματος); Θα κάνουν χρήση της ψηφιακής υπογραφής, όπως φαίνεται στο παρακάτω σχήμα. Η Alice επικοινωνεί το δημόσιο κλειδί της στον Bob στην αρχή της επικοινωνίας, χρησιμοποιεί το ιδιωτικό της κλειδί για να παράξει μια υπογραφή sig για το μήνυμα M, στέλνει το μήνυμα μαζί με την υπογραφή και ο Bob επιβεβαιώνει την ακεραιότητα του μηνύματος χρησιμοποιώντας το δημόσιο κλειδί της Alice. Ταυτόχρονα, η υπογραφή εγγυάται ότι η Alice δεν μπορεί να αποποιηθεί την ευθύνη του μηνύματος καθώς την επιβεβαιώνει το δικό της δημόσιο κλειδί.

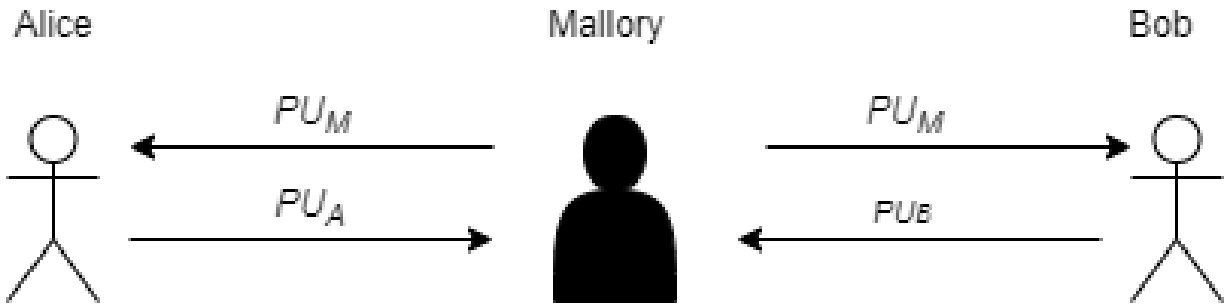


Εικόνα 3: Ψηφιακή υπογραφή

Η χρήση των ψηφιακών υπογραφών με τον παραπάνω τρόπο διασφαλίζει την αυθεντικότητα των μηνυμάτων, Παραμένει όμως, το ζήτημα της αυθεντικότητας των κλειδιών. Στο προηγούμενο παράδειγμα, θα μπορούσε η Mallory να αντικαταστήσει το δημόσιο κλειδί της Alice με το δικό της και να στέλνει έγκυρα μηνύματα στον Bob υποδυόμενη την Alice. Επομένως, είναι αναγκαία μια τεχνική που να ταυτοποιεί τα κλειδιά με τους χρήστες. Αυτή η ταυτοποίηση επιτυγχάνεται με τη χρήση πιστοποιητικών δημοσίου κλειδιού, τα οποία επεκτείνουν τις ψηφιακές υπογραφές και αναλύονται στη συνέχεια.

2.1.4 Πιστοποιητικά Δημοσίου Κλειδιού

Το είδος της επίθεσης στην αυθεντικότητα των δημοσίων κλειδιών που αναφέρθηκε στο προηγούμενο κεφάλαιο ονομάζεται επίθεση Man-in-the-Middle. Η βασική αρχή λειτουργίας της είναι πως ο επιτιθέμενος παρεμβαίνει στην επικοινωνία και αντικαθιστά τα δημόσια κλειδιά του αποστολέα και του παραλήπτη με το δικό του, υποδυόμενος είτε τον έναν είτε τον άλλο. Αυτό γίνεται ευκολότερα κατανοητό με το ακόλουθο παράδειγμα: Η Alice και ο Bob επιθυμούν να ξεκινήσουν μια νέα επικοινωνία. Για αυτόν το σκοπό, ανταλλάσσουν τα δημόσια κλειδιά τους, PUa και PUb αντίστοιχα, αλλά στην επικοινωνία παρεμβάλλεται η Mallory η οποία υποκλέπτει τα κλειδιά και προωθεί στην Alice και τον Bob ένα δικό της δημόσιο κλειδί, PUm. Έπειτα από αυτό το σημείο, η Alice θεωρεί ότι επικοινωνεί με τον Bob και αντίστοιχα ο Bob με την Alice, αλλά στην πραγματικότητα και οι δύο επικοινωνούν με τη Mallory που μπορεί να προωθεί και να τροποποιεί τα μηνύματα ανενόχλητη. Αυτή η επίθεση είναι ευρέως διαδεδομένη και μπορεί να εφαρμοστεί σε όλα τα ασύμμετρα σχήματα που χρησιμοποιούν απροστάτευτα δημόσια κλειδιά.



Εικόνα 4: Επίθεση Man-in-the-Middle

Το παραπάνω πρόβλημα αντιμετωπίζεται με τη χρήση πιστοποιητικών, τα οποία στηρίζονται στη χρήση ψηφιακών υπογραφών και στην ουσία δένουν την ταυτότητα ενός χρήστη με το αντίστοιχο δημόσιο κλειδί. Ένα πιστοποιητικό στην πιο απλοϊκή μορφή του αποτελείται από το κλειδί ενός χρήστη και μια υπογραφή αυτού του κλειδιού. Έτσι, αν κάποιος επιτιθέμενος επιχειρήσει να στείλει ένα παραποιημένο κλειδί η επαλήθευση της υπογραφής θα αποτύχει και θα αποκαλυφθεί. Φυσικά, αν χρησιμοποιούνταν τα κλειδιά των χρηστών για την παραγωγή της υπογραφής τότε θα καταλήγαμε πάλι στο ίδιο πρόβλημα. Για αυτόν το σκοπό, χρησιμοποιείται μια αξιόπιστη εξωτερική οντότητα η οποία ονομάζεται Αρχή Πιστοποιητικών(Certificate Authority - CA). Υποχρέωση αυτής της οντότητας είναι να παράγει και να εκδίδει πιστοποιητικά για κάθε χρήστη του συστήματος.

Υπάρχουν 2 βασικά σενάρια για την παραγωγή πιστοποιητικών: στο πρώτο σενάριο, ο χρήστης παράγει το δικό του ζεύγος ασύμμετρων κλειδιών και στη συνέχεια ζητάει από την Αρχή να υπογράψει το δημόσιο κλειδί. Η γνησιότητα του χρήστη θα πρέπει να επιβεβαιώνεται, ώστε να μην μπορεί να ζητήσει κάποιος πιστοποιητικό στο όνομα άλλου. Στο δεύτερο σενάριο, η Αρχή αναλαμβάνει, πέρα από το πιστοποιητικό, να παράξει τα κλειδιά κάθε χρήστη και να τα κατανείμει μαζί με το πιστοποιητικό. Σε αυτήν την περίπτωση, τόσο η αίτηση του χρήστη πρέπει να περάσει μέσα από ένα αυθεντικοποιημένο κανάλι για να βεβαιωθεί η γνησιότητά της, όσο και η απάντηση της Αρχής καθώς μεταφέρει το ιδιωτικό κλειδί του χρήστη. Από τα παραπάνω προκύπτει πως απαιτείται πάλι η ύπαρξη ενός αυθεντικοποιημένου καναλιού επικοινωνίας. Η διαφορά όμως εδώ έγκειται στο ότι αυτό το κανάλι χρειάζεται μόνο κατά την αρχική ανταλλαγή και μετά δημιουργείται μια αλυσίδα εμπιστοσύνης, στην οποία όλοι οι χρήστες που έχουν κλειδιά υπογεγραμμένα από την Αρχή πιστοποιητικών εμπιστεύονται ο ένας τον άλλον.

Οι Αρχές πιστοποιητικών μαζί με τους υποστηρικτικούς μηχανισμούς τους ονομάζονται Υποδομές Δημοσίου Κλειδιού(Public Key Infrastructures - PKI). Υπάρχουν αρκετές προκλήσεις στην ομαλή και ασφαλή λειτουργία τους, όπως η ταυτοποίηση την χρηστών που αιτούνται πιστοποιητικά και η ασφαλής κατανομή των κλειδιών. Ακόμα, υπάρχουν πρακτικά ζητήματα που απαιτούν λύση, με τα βασικότερα από αυτά να είναι η ύπαρξη πολλαπλών Αρχών και η ανάκληση πιστοποιητικών. Όσον αφορά στο πρώτο ζήτημα, η τακτική που ακολουθείται συνήθως είναι η αλυσιδωτή εμπιστοσύνη μεταξύ των Αρχών καθώς και η δημιουργία μιας ιεραρχικής δομής μεταξύ τους, όπου οι Αρχές του ανώτερου επιπέδου υπογράφουν τα κλειδιά των κατώτερων. Έτσι επιτυγχάνεται η εξάπλωση της εμπιστοσύνης μεταξύ των Αρχών και κατά συνέπεια μεταξύ των χρηστών τους.

Παρά την ασφάλεια που υπόσχεται η χρήση αυτού του συστήματος, υπάρχει πάντα το ενδεχόμενο κάποιο πιστοποιητικό να είναι άκυρο, π.χ. να έχει λήξει η περίοδος εγκυρότητας του.

Σε αυτήν τη περίπτωση, πρέπει να υπάρχει ένας μηχανισμός ανάκλησης άκυρων πιστοποιητικών. Αυτό επιτυγχάνεται με τη χρήση Λιστών Ανάκλησης Πιστοποιητικών(Certificate Revocation List – CRL) οι οποίες διανέμονται στους χρήστες του συστήματος. Κάθε χρήστης διατηρεί ένα αντίγραφο της λίστας, το οποίο πρέπει να είναι ενημερωμένο, και το ζήτημα της ενημέρωσης δεν είναι τετριμμένο. Υπάρχουν 2 βασικές προσεγγίσεις σε αυτό το πρόβλημα: η πρώτη περιλαμβάνει την περιοδική αποστολή της ενημερωμένης λίστας από την Αρχή προς τους χρήστες. Σε αυτήν την προσέγγιση, υπάρχει ο κίνδυνος ένα άκυρο πιστοποιητικό να συνεχίσει να θεωρείται έγκυρο από τους χρήστες μέχρις ότου να ενημερωθεί η λίστα τους. Αυτό μπορεί να βελτιωθεί με τη μείωση της περιόδου ενημέρωσης, εισάγοντας όμως περαιτέρω επιβάρυνση στο δίκτυο. Η δεύτερη προσέγγιση απαιτεί από τους χρήστες να επικοινωνούν με την Αρχή κάθε φορά που λαμβάνουν ένα πιστοποιητικό από κάποιον άλλο χρήστη. Αυτό σημαίνει πως η Αρχή θα εμπλέκεται σε κάθε επικοινωνία, κάτι που προφανώς δεν είναι επιθυμητό. Στην πράξη εφαρμόζεται και είναι απαραίτητος ένας συμβιβασμός των παραπάνω τεχνικών.

Η διαδεδομένη χρήση των ασύμμετρων σχημάτων έχει οδηγήσει στην ευρεία χρήση των υπογραφών καθώς και των πιστοποιητικών, προκειμένου να διασφαλιστεί η ακεραιότητα και η εγκυρότητα της επικοινωνίας. Για το συγκεκριμένο ζήτημα έχει προταθεί μια πληθώρα προσεγγίσεων και υλοποιήσεων, οι οποίες καλύπτουν διαφορετικές απαιτήσεις του προβλήματος, χωρίς όμως να έχει βρεθεί μια καθολική υλοποίηση που να μπορεί να καλύψει όλες τις διαφορετικές πτυχές αυτού του θέματος. Ενδεικτικά αναφέρεται το πρωτόκολλο X.509 το οποίο χρησιμοποιείται κατά κόρον στις σύγχρονες διαδικτυακές επικοινωνίες, όπως στο SSL/TLS και στο IPSec.

2.2 Έννοιες Δικτύων

Σε αυτήν την ενότητα παρουσιάζονται συνοπτικά μερικές βασικές έννοιες και τεχνολογίες δικτύων, οι οποίες αποτελούν τη βάση των συστημάτων επικοινωνίας που μελετούνται στην παρούσα εργασία.

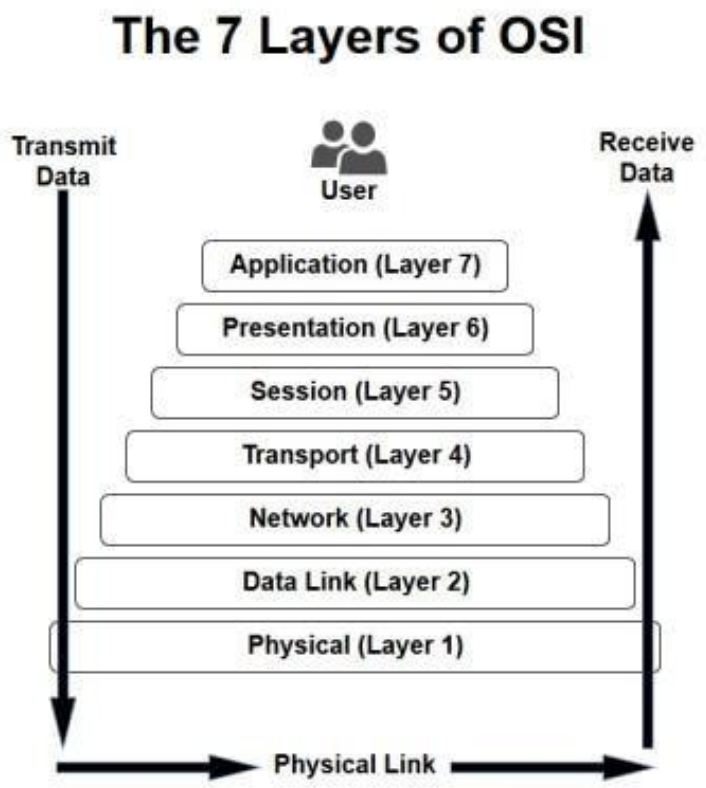
2.2.1 OSI model

Το OSI(Open Systems Interconnection) Model είναι ένα εννοιολογικό μοντέλο που στοχεύει στην παροχή ενός τυποποιημένου πλαισίου επικοινωνίας μεταξύ διαφορετικών συστημάτων. Αποτελείται από 7 αφηρημένα επίπεδα τα οποία περιγράφονται εν συντομία παρακάτω και κάθε επίπεδο επικοινωνεί με τα γειτονικά του:

1. Φυσικό Επίπεδο(Physical Layer): Αυτό το επίπεδο καθορίζει τα μέσα μετάδοσης ακατέργαστων bits πληροφορίας, όπως καλώδια, αέρας κτλ. Οι κύριες λειτουργίες αυτού του επιπέδου είναι: ο καθορισμός των χαρακτηριστικών του υλικού, η κωδικοποίηση της πληροφορίας σε σήμα, η εκπομπή και λήψη των δεδομένων και ο φυσικός σχεδιασμός του δικτύου.
2. Επίπεδο Ζεύξης Δεδομένων(Data Link Layer): Αυτό το επίπεδο είναι υπεύθυνο για τη μεταφορά δεδομένων μεταξύ συσκευών που ανήκουν στο τοπικό δίκτυο και για την

ανίχνευση και διόρθωση σφαλμάτων που προκύπτουν στο φυσικό επίπεδο. Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Ethernet.

3. Επίπεδο Δικτύου(Network Layer): Στο επίπεδο αυτό καθορίζεται ο τρόπος δρομολόγησης πακέτων πληροφορίας μεταξύ ενός αποστολέα και ενός παραλήπτη, οι οποίοι μπορεί να βρίσκονται στο ίδιο φυσικό δίκτυο αλλά και σε διαφορετικό. Εδώ εισάγεται η λογική έννοια της διεύθυνσης και αντίστοιχα το πιο γνωστό πρωτόκολλο δικτύου το IP(Internet Protocol).
4. Επίπεδο Μεταφοράς(Transport Layer): Εδώ αναλαμβάνεται η μεταφορά των δεδομένων από τον αποστολέα στον παραλήπτη. Παρέχεται η δυνατότητα εγκαθίδρυσης σύνδεσης μεταξύ των δύο μερών επικοινωνίας, ο έλεγχος της αξιοπιστίας του καναλιού μέσω κατάτμησης, ελέγχου ροής και σφαλμάτων, έλεγχος συμφόρησης, επανεκπομπή πακέτων κ.α. Το πιο διαδεδομένο πρωτόκολλο αυτού του επιπέδου είναι το TCP(Transmission Control Protocol) που εξασφαλίζει αξιόπιστη μετάδοση πληροφορίας χάρη στη λογική της σύνδεσης που χρησιμοποιεί, σε αντίθεση με το εξίσου γνωστό UDP(User Datagram Protocol) το οποίο δεν απαιτεί σύνδεση αλλά δεν υπόσχεται και απόλυτη αξιοπιστία μετάδοσης. Αυτά τα 2 πρωτόκολλα χρησιμοποιούνται στο συντριπτικό ποσοστό της διαδικτυακής κίνησης και έχουν υλοποιήσεις σε όλα τα λειτουργικά συστήματα ανεξαιρέτως.
5. Επίπεδο Συνόδου(Session Layer): Αυτό το επίπεδο προσφέρει τους απαραίτητους μηχανισμούς για τη διαχείριση των συνόδων(sessions) μεταξύ των τελικών εφαρμογών. Υποστηρίζει λειτουργίες αποθήκευσης, τερματισμού, ανάκτησης και επανεκκίνησης συνόδων και χρησιμοποιείται κυρίως σε εφαρμογές που κάνουν χρήση RPC(Remote Procedure Calls).
6. Επίπεδο Παρουσίασης(Presentation Layer): Αυτό το επίπεδο, το οποίο ονομάζεται ορισμένες φορές Επίπεδο Σύνταξης, αναλαμβάνει το μετασχηματισμό των δεδομένων προκειμένου να γίνουν αποδεκτά από την εφαρμογή στην οποία αποστέλλονται. Οι βασικότερες λειτουργίες του επιπέδου είναι οι: μετατροπή δεδομένων, κωδικοποίηση χαρακτήρων, συμπίεση και κρυπτογράφηση/αποκρυπτογράφηση.
7. Επίπεδο Εφαρμογής(Application Layer): Είναι το επίπεδο που βρίσκεται πιο κοντά στον τελικό χρήστη και του παρέχει τη δυνατότητα της πρόσβασης μέσω κάποιας εφαρμογής στις πληροφορίες ενός δικτύου. Είναι υπεύθυνο για την εμφάνιση των ληφθέντων πληροφοριών στο χρήστη. Οι λειτουργίες σε αυτό το επίπεδο συνήθως περιλαμβάνουν την αναγνώριση των μερών επικοινωνίας, τη διαθεσιμότητα πόρων και το συγχρονισμό της επικοινωνίας. Ορισμένα από τα κυριότερα πρωτόκολλα που άπτονται αυτού του επιπέδου είναι: Telnet, FTP, SMTP, DNS SNMP κ.α.[2]



Εικόνα 5: Μοντέλο OSI

Προκειμένου να υλοποιηθεί αποτελεσματικά μια διαδικτυακή επικοινωνία, όλα τα προαναφερθέντα επίπεδα πρέπει να ληφθούν υπόψη και να χρησιμοποιηθούν στην υλοποίηση. Στην παρούσα εργασία γίνονται αναφορές σε διάφορα σημεία σε πρωτόκολλα τα οποία σχετίζονται με όλα σχεδόν τα επίπεδα, για αυτό και θεωρήθηκε ουσιώδης η καταγραφή τους εδώ.

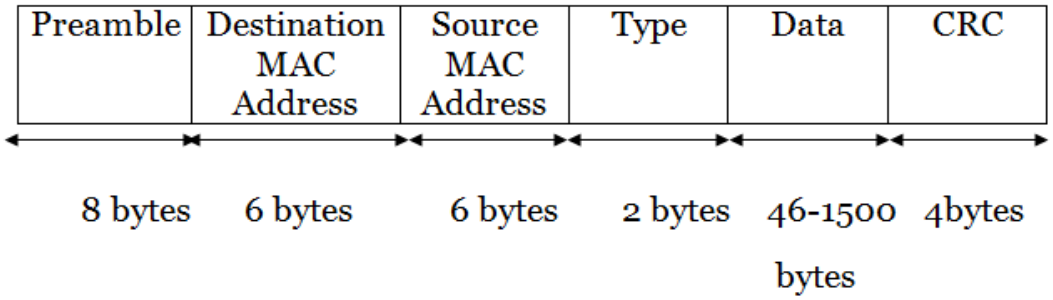
2.2.2 Ethernet

Το Ethernet είναι μια τεχνολογία δικτύωσης που χρησιμοποιείται στα Δίκτυα Περιοχής(LAN, MAN, WAN). Εισήχθηκε πρώτη φορά το 1980 και σύντομα προτυποποιήθηκε στο πρότυπο IEEE 802.3 το 1983 και σήμερα αποτελεί τη δημοφιλέστερη τεχνολογία δικτύωσης μέχρι το Επίπεδο Ζεύξης Δεδομένων. Όσον αφορά στη λειτουργία που παρέχει στο Φυσικό Επίπεδο, αρχικά έκανε χρήση ομοαξονικών καλωδίων ως ένα κοινό μέσο αλλά οι νεότερες εκδόσεις του χρησιμοποιούν καλώδια αντίστροφου ζεύγους και οπτικές ίνες σε συνδυασμό με μεταγωγείς(switches). Ακόμα, ο ρυθμός μεταφοράς δεδομένων που υποστηρίζει έχει αυξηθεί ραγδαία από την εισαγωγή του, από τα αρχικά 2.9Mbps στα 400Gbps.

Το κεντρικό κομμάτι του Ethernet, και αυτό το οποίο έμεινε σταθερό στα περίπου 40 χρόνια που πέρασαν από την έκδοση του, είναι η μορφή του πλαισίου δεδομένων του. Αυτό το πλαίσιο ενθυλακώνει ένα δεδομενόγραμμα(datagram) IP και το μεταφέρει στο φυσικό επίπεδο, το οποίο στον παραλήπτη ανακτάται και προωθείται στο επίπεδο δικτύου. Επιγραμματικά, τα πεδία του πλαισίου είναι:

1. Προοίμιο(Preamble): Το πρώτο πεδίο του πλαισίου έχει μέγεθος 8 bytes και χρησιμοποιείται για να «αφυπνίσει» τους προσαρμογείς λήψης προκειμένου να συγχρονίσουν τα ρολόγια τους και να ειδοποιήσει πως ακολουθεί το σώμα του πλαισίου.
2. Διεύθυνση Προορισμού(Destination Address): Αυτό το πεδίο έχει μέγεθος 6 bytes περιέχει τη διεύθυνση MAC του προσαρμογέα προορισμού σε δεκαεξαδική μορφή(XX-XX-XX-XX-XX-XX). Όταν στον προορισμό έρθει ένα πλαίσιο όπου αυτό το πεδίο έχει τη διεύθυνσή του ή τη διεύθυνση εκπομπής, μεταβιβάζει το πεδίο δεδομένων στο επίπεδο δικτύου και απορρίπτει οποιαδήποτε άλλη διεύθυνση.
3. Διεύθυνση Προέλευσης(Source Address): Αντίστοιχα με το παραπάνω, στο πεδίο αυτό περιέχεται η MAC διεύθυνση του προσαρμογέα που εκπέμπει το πλαίσιο.
4. Πεδίο Τύπου(Type): Το πεδίο αυτό, με μέγεθος 2 bytes, χρησιμοποιείται από το Ethernet για την σήμανση του κατάλληλου πρωτοκόλλου επιπέδου δικτύου, καθώς ένας υπολογιστής μπορεί να υποστηρίζει πολλαπλά πρωτόκολλα.
5. Πεδίο Δεδομένων(Data): Αυτό το πεδίο μεταφέρει το δεδομενόγραμμα IP και μπορεί να έχει μέγεθος από 46 μέχρι 1500 bytes. Αν είναι παραπάνω από 1500, τότε κατακερματίζεται και στέλνεται τμηματικά, ενώ αν είναι κάτω από 46 γεμίζεται(stuffing) μέχρι τα 46. Χρησιμοποιείται το πεδίο μήκους στην κεφαλίδα του δεδομενογράμματος IP για αφαίρεση της γέμισης.
6. Έλεγχος Κυκλικού Πλεονασμού(Cyclic Redundancy Check-CRC): Έχει μέγεθος 4 bytes και επιτρέπει στον προσαρμογέα του παραλήπτη να αναγνωρίζει λάθη bit μέσα στο πλαίσο.[3].

Στην παρούσα εργασία, το Ethernet χρησιμοποιείται στην επικοινωνία μεταξύ των σταθμών υποδομής(RA, RSU) καθώς αυτοί οι κόμβοι είναι στατικοί και μπορούν να επωφεληθούν από καλωδιώσεις, σε αντίθεση με τα οχήματα, τα οποία κάνουν χρήση Wifi, το όποιο αναφέρεται παρακάτω.



Εικόνα 6: Δομή πακέτου Ethernet

2.2.3 Wifi

Το WiFi, ή αλλιώς ασύρματο LAN, όπως λέει το όνομα παρέχει τη δυνατότητα δημιουργίας ενός ασύρματου δικτύου μεταξύ συσκευών σε μια περιορισμένη περιοχή και μέσω gateways τη σύνδεση με το Ίντερνετ. Οι πιο διαδεδομένες τεχνολογίες αυτής της μορφής βασίζονται πάνω στην οικογένεια προτύπων IEEE 802.11(a,b,g,n,p κτλ.) και εφαρμόζονται σε αναρίθμητες πτυχές της καθημερινότητας, καθώς είναι η σημαντικότερη τεχνολογία δικτύων προσπέλασης σήμερα.

Τα πρότυπα 802.11 καθορίζουν πρωτόκολλα επικοινωνίας στο Φυσικό Επίπεδο και στο Επίπεδο Ζεύξης Δεδομένων για την ασύρματη επικοινωνία, λειτουργώντας σε ζώνες συχνοτήτων όπως τα 2.4, και 5 GHz. Εφαρμόζουν τη μέθοδο CSMA/CA(Carrier-Sense Multiple Access with Collision Avoidance), στην οποία πριν αποσταλεί ένα πακέτο από έναν κόμβο ελέγχεται η διαθεσιμότητα του μέσου μετάδοσης έτσι ώστε να μην υπάρξει σύγκρουση και απόρριψη πακέτων[3].

Όπως και στο Ethernet, κεντρικό ρόλο παίζει το πλαίσιο δεδομένων το οποίο στη βασική του μορφή περιλαμβάνει τα παρακάτω πεδία:

1. Έλεγχος πλαισίου:
2. Διάρκεια: Σε αυτό το πεδίο αναγράφεται η διάρκεια για την οποία δεσμεύεται το κανάλι για τη μετάδοση και επιβεβαίωση του πακέτου.
3. Διεύθυνση 1: Είναι η διεύθυνση MAC του σταθμού που πρόκειται να λάβει το πλαίσιο.
4. Διεύθυνση 2: Είναι η διεύθυνση MAC του σταθμού που μεταδίδει το πλαίσιο.
5. Διεύθυνση 3: Είναι η διεύθυνση MAC του δρομολογητή που συνδέει τα υποδίκτυα του δικτύου.
6. Αριθμός ακολουθίας: Το πεδίο αυτό χρησιμοποιείται για το διάκριση μεταξύ ενός μεταδιδόμενου πλαισίου και της επαναμετάδοσης ενός προηγουμένου.
7. Διεύθυνση 4: Χρησιμοποιείται όταν το δίκτυο βρίσκεται σε ad hoc λειτουργία.
8. Ωφέλιμο φορτίο: Τυπικά αποτελείται από ένα δεδομενόγραμμα IP ή ένα πακέτο ARP. Μπορεί να έχει μέγεθος μέχρι 2.312 bytes αλλά συνήθως περιέχει 1500 ή λιγότερα bytes.
9. CRC: Επιτελεί την ίδια λειτουργία με το Ethernet, επιτρέπει δηλαδή στο δέκτη να αναγνωρίζει σφάλματα bit στο πλαίσιο[3].

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0-2312 bytes	4 bytes
Frame Control	Duration	Address 1	Address 2	Address 3	Sequence Control	Address 4	Payload	CRC

Εικόνα 7: Δομή πλαισίου Wifi

Στην παρούσα εργασία, μας ενδιαφέρει κυρίως το πρότυπο 802.11p, το οποίο αποτελεί μια τροποποίηση του 802.11 ώστε να παρέχει υποστήριξη για Ασύρματη Πρόσβαση σε Περιβάλλοντα Οχημάτων(Wireless Access in Vehicular Environments-WAVE). Αναπτύχθηκε το 2005-2009 και εισήχθη στο 802.11 το 2010, αποτελώντας τη βάση για την δημιουργία

συστημάτων επικοινωνίας μεταξύ οχημάτων και σταθμών δρόμου(RSU). Χρησιμοποιεί κανάλια εύρους 10MHz στη ζώνη συχνοτήτων 5.9GHz(5.850-5.925GHz) με σκοπό να επιτύχει την ελάχιστη δυνατή καθυστέρηση στην επικοινωνία[4].

Στις προσομοιώσεις αυτής της εργασίας, χρησιμοποιείται αποκλειστικά το πρότυπο 802.11p για την επικοινωνία μεταξύ των οχημάτων του δικτύου καθώς και την επικοινωνία οχήματος-σταθμού υποδομής(vehicle-RSU).

2.3 Ασφάλεια και Ιδιωτικότητα

2.3.1 Απαιτήσεις ασφάλειας και ιδιωτικότητας

Όπως όλα τα συστήματα επικοινωνίας, έτσι και τα VANETs πρέπει να διαθέτουν κάποια χαρακτηριστικά ασφάλειας και ιδιωτικότητας και να παρέχουν τις κατάλληλες υπηρεσίες προκειμένου να είναι όσο το δυνατόν καλύτερα προστατευμένα απέναντι σε πιθανές επιθέσεις από κακόβουλους παράγοντες. Μια επίθεση σε ένα δίκτυο οχημάτων μπορεί να έχει καταστροφικές συνέπειες για την ίδια τη ζωή των επιβατών, επομένως η ενσωμάτωση υπηρεσιών ασφάλειας στο δίκτυο είναι αναγκαία. Αυτός ο τομέας έχει μελετηθεί διεξοδικά από την επιστημονική κοινότητα στην προσπάθεια να αναγνωριστούν και να κατηγοριοποιηθούν τα χαρακτηριστικά ασφάλειας που πρέπει να διέπουν ένα σύστημα επικοινωνίας οχημάτων, και έχουν δημοσιευτεί αρκετές έρευνες που αναλύουν τα διάφορα προτεινόμενα χαρακτηριστικά. Παρουσιάζονται παρακάτω κάποια βασικά χαρακτηριστικά ασφαλείας:

1. Αυθεντικοποίηση(Authentication). Κάθε κόμβος που συμμετέχει στο δίκτυο πρέπει να παρέχει κάποιες βασικές πληροφορίες, συμπεριλαμβανομένης μιας μορφής ταυτότητα, προκειμένου να μπορεί να αυθεντικοποιηθεί. Η αυθεντικοποίηση είναι ζωτικής σημασίας στην προστασία του συστήματος, καθώς μπορεί να αποτρέψει μια πλειάδα επιθέσεων. Μια εφαρμογή αυθεντικοποίησης είναι η ανάθεση ξεχωριστών ταυτοτήτων στα οχήματα προκειμένου να αποφευχθούν οι επιθέσεις Sybil, όπως π.χ. η προσπάθεια ενός οχήματος να φανεί σαν μια ομάδα οχημάτων προκειμένου να δημιουργήσει μια ψευδή εικόνα κυκλοφοριακής συμφόρησης. Υπάρχουν διάφοροι τύποι αυθεντικοποίησης, με τους κυριότερους να είναι:
    a. Αυθεντικοποίηση ταυτότητας(ID authentication). Επιτρέπει σε ένα κόμβο να ταυτοποιήσει μονοσήμαντα τον αποστολέα ενός μηνύματος, όπως επίσης επιτρέπει την ένταξη των κόμβων στο δίκτυο. Αποτρέπει επιθέσεις που βασίζονται σε μίμηση πραγματικών κόμβων ή δημιουργία ψευδών κόμβων.
    b. Αυθεντικοποίηση ιδιότητας(Property authentication). Αυτός ο τύπος βοηθάει στην αναγνώριση του τύπου της οντότητας που επικοινωνεί, δηλαδή αν είναι όχημα, RSU ή κάτι άλλο.
    c. Αυθεντικοποίηση θέσης(Location authentication). Ιδιαίτερα χρήσιμος σε εφαρμογές που κάνουν χρήση της θέσης ενός οχήματος, βοηθάει στην εξακρίβωση της τοποθεσίας ενός κόμβου[5]-[9].
2. Εμπιστευτικότητα(Confidentiality). Αυτό το χαρακτηριστικό είναι απαραίτητο για την προστασία της πληροφορίας από επίδοξους ωτακουστές. Η προστασία της επικοινωνίας μεταξύ των οντοτήτων του συστήματος, οχημάτων ή σταθμών υποδομής,

επιτυγχάνεται με τη κρυπτογράφηση των εμπιστευτικών πληροφοριών όπως η ταυτότητα του χρήστη. Μπορούν να χρησιμοποιηθούν τόσο ασύμμετρες όσο και συμμετρικές μέθοδοι για την κρυπτογράφηση, και στην πράξη χρησιμοποιούνται διάφοροι συνδυασμοί. Φυσικά, η ανάγκη κρυπτογράφησης εξαρτάται από την εκάστοτε εφαρμογή. Για μηνύματα τα οποία αναμεταδίδονται για λόγους ασφαλείας δεν υπάρχει ανάγκη εμπιστευτικότητας καθώς δεν περιέχουν ευαίσθητες πληροφορίας. Άλλες εφαρμογές, όπως η πληρωμή διοδίων, διακινούν ευαίσθητα στοιχεία μεταξύ οχημάτων και RSU και πρέπει να διασφαλιστεί η εμπιστευτικότητά του.[5]-[9].

3. Ακεραιότητα(Integrity). Αυτό το χαρακτηριστικό αναφέρεται στην απαίτηση ένα μήνυμα να μην τροποποιείται από τη στιγμή που αποστέλλεται μέχρι τη στιγμή που παραλαμβάνεται από τον σωστό παραλήπτη. Η ακεραιότητα, εξασφαλίζει την προστασία απέναντι σε μη-εξουσιοδοτημένη δημιουργία, αλλαγή ή καταστροφή δεδομένων. Ένα πρωτόκολλο θεωρείται ατελές αν μπορεί να δεχτεί αλλοιωμένα μηνύματα, καθώς θεωρείται πως τα δεδομένα ενός μηνύματος μέσα στο σύστημα είναι αξιόπιστα. Με μεθόδους αυθεντικοποίησης, εμποδίζονται χρήστες από το να παρεμβάλλουν κακόβουλα μηνύματα. Στην περίπτωση εφαρμογών VANET, παραποιημένα μηνύματα είναι ιδιαιτέρως επικίνδυνα καθώς περιλαμβάνουν συνήθως συντεταγμένες θέσης. Για αυτό το λόγο, γίνεται χρήση ηλεκτρονικών υπογραφών που επιβεβαιώνουν την εγκυρότητα του μηνύματος, ενώ μια εναλλακτική μέθοδος επαλήθευσης είναι η σύγκριση με αντίστοιχα μηνύματα που παράχθηκαν από την κοντινή γεωγραφική περιοχή[9].
4. Διαθεσιμότητα(Availability). Το δίκτυο και οι εφαρμογές του θα πρέπει να παραμένουν λειτουργικά ακόμα και υπό την εμφάνιση βλαβών ή την ύπαρξη κακόβουλων συνθηκών. Αυτό απαιτεί ασφαλή και ανθεκτική σε λάθη σχεδίαση, άμυνα απέναντι σε επιθέσεις εξάντλησης(depletion attacks) και πρωτόκολλα που δύνανται να συνεχίσουν την κανονική λειτουργία τους μετά την αφαίρεση των προβληματικών κόμβων του συστήματος. Όσον αφορά στα δίκτυα οχημάτων, αν για κάποιο λόγο η διαθεσιμότητα πληγεί, οι συνέπειες θα είναι καταστροφικές καθώς η ίδια η λειτουργία του συστήματος κινδυνεύει. Για αυτό το λόγο, πρέπει να εξασφαλίζεται με πρωτόκολλα δρομολόγησης που είναι ανθεκτικά σε επιθέσεις εξάντλησης πόρων και έχουν ταχεία απόκριση, η οποία είναι αναγκαία λόγω της φύσης αυτών των δικτύων[6],[8],[9].
5. Μη αποποίηση ευθυνών(Non-repudiation). Αυτό το χαρακτηριστικό στοχεύει στην αποτροπή της αποποίησης ευθυνών, δηλαδή ο αποστολέας ενός μηνύματος να μην μπορεί να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα. Αυτός ο μηχανισμός προφανώς καθιστά υπεύθυνο τον αποστολέα για το μήνυμά του. Οι μέθοδοι Non-repudiation έχουν στόχο τη συλλογή αποδεικτικών στοιχείων προκειμένου να ενοχοποιήσουν κακόβουλους χρήστες που αρνούνται τις κατηγορίες. Στα VANETs, τέτοιου είδους πληροφορίες αποθηκεύονται συνήθως σε ένα στοιχείο ονόματι Tamper-proof Device(TPD) και μόνο εξουσιοδοτημένοι χρήστες μπορούν να ανακτήσουν τα εν λόγω δεδομένα[6]-[9].
6. Έλεγχος πρόσβασης(Access-control). Αυτό το χαρακτηριστικό περιγράφει την απαίτηση ύπαρξης ρόλων και δικαιωμάτων στο σύστημα. Ευαίσθητες επικοινωνίες, όπως π.χ. αστυνομικά οχήματα, πρέπει να είναι ορατές μόνο σε εξουσιοδοτημένους κόμβους. Τα δικαιώματα και οι ρόλοι κάθε κόμβου καθορίζονται από τις πολιτικές που

θεσπίζει το σύστημα, και συνήθως τυποποιούνται με τη μορφή διαπιστευτηρίων που μοιράζονται και ελέγχονται από μια κεντρική αρχή, προκειμένου να προσφέρουν ασφάλεια απέναντι σε μη-εξουσιοδοτημένες προσβάσεις[5],[6],[9].

2.3.2 Τύποι επιτιθέμενων

Στη μελέτη της των χαρακτηριστικών ασφαλείας των δικτύων οχημάτων έχει ιδιαίτερο ενδιαφέρον ο εντοπισμός των διαφορετικών τύπων επιτιθέμενων που μπορεί να λειτουργούν. Έχουν προταθεί διάφορες κατηγοριοποιήσεις, οι οποίες έχουν δυαδική μορφή. Οι κυριότερες από αυτές είναι:

- Εξωτερικός/Εσωτερικός(Outsider/Insider). Εξωτερικός επιτιθέμενος θεωρείται κάποιος που βρίσκεται εκτός του VANET, δηλαδή δεν ανήκει στους αυθεντικοποιημένους κόμβους. Αυτός ο τύπος δεν είναι εύκολο να εξαπολύσει αποτελεσματικές επιθέσεις καθώς δεν έχει αυθεντικοποιηθεί στο σύστημα και επομένως θεωρείται εισβολέας από τα μελή του δικτύου. Αυτό που μπορεί να κάνει είναι να κρυφακούει το κοινό δίκτυο για μηνύματα που μπορεί υποκλέψει, να προκαλέσει επίθεση DoS πλημμυρίζοντας το δίκτυο με μηνύματα χωρίς αξία ή να εισάγει ψευδή μηνύματα στο δίκτυο προκειμένου να δημιουργήσει μια εσφαλμένη εικόνα, π.χ. για τη θέση ενός ατυχήματος. Οι εσωτερικοί επιτιθέμενοι από την άλλη, αναφέρονται σε οχήματα που διαθέτουν έγκυρα διαπιστευτήρια για το σύστημα οπότε είναι κανονικά μέλη. Είναι προφανές πως αυτού του είδους ο επιτιθέμενος έχει πρόσβαση σε πολλές πληροφορίες για το δίκτυο και είναι σε θέση να δοκιμάσει όλων των ειδών τις επιθέσεις. Μια ιδιαίτερη κατηγορία εσωτερικών επιτιθέμενων στην περίπτωση των δικτύων οχημάτων, είναι οντότητες στη γραμμή παραγωγής του οχήματος με τη δυνατότητα επέμβασης στο λογισμικό του. Τέτοιοι επιτιθέμενοι μπορούν να εισάγουν κακόβουλο κώδικα στο σύστημα και ταυτόχρονα είναι δύσκολο να εντοπιστεί η δράση τους.[9],[10] Στη συγκεκριμένη εργασία, θεωρούμε πως οι εσωτερικοί επιτιθέμενοι ανήκουν στην πρώτη κατηγορία.
- «Μοχθηρός»/Λογικός(Malicious/Rational). Ως «μοχθηρός» επιτιθέμενος θεωρείται κάποιος ο οποίος δεν έχει κάποιο πραγματικό όφελος να αποκομίσει από την επίθεση, παρά μόνο ευχαρίστηση. Δεν έχει κάποιο συγκεκριμένο στόχο να πετύχει, οπότε ο μοναδικός του σκοπός είναι να προκαλέσει προβλήματα στη λειτουργία του δικτύου. Ένας τέτοιος δράστης μπορεί εσκεμμένα να στείλει ψευδείς πληροφορίες στα οχήματα μιας περιοχής προκειμένου να προκαλέσει κάποιο ατύχημα, ή να «ρίξει» το δίκτυο, όχι για να πετύχει κάποιο στόχο αλλά γιατί το βλέπει ως παιχνίδι. Αντίθετα, ένας λογικός επιτιθέμενος έχει έναν ξεκάθαρο σκοπό που επιδιώκει να πετύχει. Προτιμάει να υποκλέψει πληροφορίες και ταυτότητες διακριτικά από το να προκαλέσει εμφανή προβλήματα, και για αυτό είναι εν δυνάμει πιο επικίνδυνος από τον «μοχθηρό». Από την άλλη, η προσήλωσή του στο στόχο τον κάνει πιο προβλέψιμο στις μεθόδους επίθεσης που θα ακολουθήσει[9],[10].
- Ενεργός/Παθητικός(Active/Passive). Ένας ενεργός επιτιθέμενος είναι ένας κόμβος ο οποίος επικοινωνεί με τα υπόλοιπα οχήματα ή την υποδομή προκειμένου να προξενήσει προβλήματα. Στις περισσότερες περιπτώσεις αυτοί οι επιτιθέμενοι είναι και εσωτερικοί κόμβοι στο δίκτυο οπότε, όπως προαναφέρθηκε, μπορούν να χρησιμοποιήσουν μια

πληθώρα επιθέσεων. Οι παθητικοί επιτιθέμενοι δεν εκκινούν κάποια επικοινωνία στο δίκτυο οχημάτων, ούτε χρειάζεται να έχουν κάποια ιδιαίτερη πρόσβαση. Απλά κρυφακούν τη διερχόμενη επικοινωνία προκειμένου να συλλέξουν όσο το δυνατόν περισσότερες πληροφορίες, οι οποίες μπορεί να χρησιμοποιηθούν σε μετέπειτα επίθεση από κάποιον ενεργό δράστη. Τέτοιες οντότητες είναι κυρίως εξωτερικές[9],[10].

- Καθολικός/Τοπικός(Global/Local). Αυτός ο διαχωρισμός αναφέρεται στην έκταση της επίδρασης που μπορεί να έχει ένας επιτιθέμενος. Ένας τοπικός επιτιθέμενος είναι περιορισμένος σε ένα συγκεκριμένο αριθμό οντοτήτων που ελέγχει ή μια περιοχή που μπορεί να παρακολουθήσει. Για παράδειγμα, ένας τέτοιος επιτιθέμενος μπορεί να έχει μολύνει έναν περιορισμένο αριθμό από RSUs, επομένως μπορεί να παρακολουθήσει ένα εκτεταμένο μεν αλλά περιορισμένο δε μέρος του δικτύου. Αντίθετα, ένας καθολικός επιτιθέμενος έχει τη δυνατότητα να παρακολουθήσει, αν το επιθυμεί, ολόκληρο το δίκτυο[9],[10].
- Στατικός/Δυναμικός(Static/Adaptive). Ένας στατικός επιτιθέμενος επιλέγει τη μέθοδο επίθεσης εκ των προτέρων και την ακολουθεί ανεξαρτήτως της προόδου της. Ο δυναμικός επιτιθέμενος θα προσαρμόσει τις μεθόδους του στις πληροφορίες που θα πάρει από το σύστημα και από προηγούμενες απόπειρες. Όσον αφορά στην ιδιωτικότητα θέσης, τα περισσότερα μοντέλα χρησιμοποιούν δυναμικούς δράστες, που χρησιμοποιούν τις λεγόμενες συμπερασματικές επιθέσεις(inference attacks)[7].

2.3.3 Επιθέσεις

Όπως σε όλα τα δίκτυα, έτσι και στα VANETs υπάρχει μια πληθώρα διαφορετικών επιθέσεων που μπορούν να χρησιμοποιηθούν από κακόβουλες οντότητες. Οι διάφοροι τύποι επιθέσεων σε δίκτυα οχημάτων έχουν μελετηθεί εκτενώς στη διεθνή βιβλιογραφία, καθώς είναι αναγκαία η κατανόηση των πιθανών κινδύνων για την βέλτιστη αντιμετώπισή τους. Ενδεικτικά, αναφέρονται οι παρακάτω τύποι επιθέσεων όπως περιγράφονται στο [6]:

- Επιθέσεις στην αυθεντικοποίηση(Authentication attacks). Οι επιθέσεις αυτού του τύπου σχετίζονται με την ταυτότητα, ή την απουσία, των οχημάτων. Χαρακτηριστικό παράδειγμα τέτοιας επίθεσης είναι η επίθεση Sybil, στην οποία ένας κακόβουλος κόμβος υποδύεται πολλαπλά οχήματα προκειμένου να αποκτήσει μεγαλύτερη επιρροή πάνω στο δίκτυο. Άλλες πιθανές επιθέσεις περιλαμβάνουν το GPS spoofing στο οποίο στέλνονται επίτηδες λανθασμένες συντεταγμένες GPS, τη Μεταμφίεση(Masquerade) πολλών οχημάτων με το ίδιο αναγνωριστικό(ID) και τη Σκουληκότρυπα(Wormhole) στην οποία 2 κακόβουλα οχήματα αποκτούν έλεγχο στη δρομολόγηση των πακέτων επιλέγοντας στρατηγικές θέσεις πάνω στο δίκτυο. Όλες αυτές οι επιθέσεις αποθαρρύνονται με την εφαρμογή μεθόδων αυθεντικοποίησης, όπως αναφέρθηκε σε προηγούμενη ενότητα.
- Επιθέσεις στη διαθεσιμότητα(Availability attacks). Αυτές οι επιθέσεις έχουν ως στόχο να πλήξουν την ποιότητα των υπηρεσιών του δικτύου με διάφορες μεθόδους. Ο πιο γνωστός τρόπος είναι η επίθεση Άρνησης Υπηρεσίας(Denial of Service – DoS), στην οποία ο επιτιθέμενος κατακλύζει το δίκτυο με άχρηστα μηνύματα αποσκοπώντας στον κορεσμό του μέσου επικοινωνίας και την απόρριψη έγκυρων πακέτων. Αν πολλοί κόμβοι εξαπολύουν την επίθεση ταυτόχρονα, τότε η επίθεση είναι κατανεμημένη(Distributed

DoS). Πολλές φορές, τέτοιες επιθέσεις στοχεύουν τους κόμβους σε φυσικό επίπεδο και μπορούν να προκαλέσουν άμεση και μη αναστρέψιμη ζημιά, όπως π.χ. η καταστροφή ενός σταθμού υποδομής(RSU).

- Επιθέσεις στη μυστικότητα(Secrecy attacks). Ο στόχος αυτών των επιθέσεων είναι η απόκτηση πληροφοριών που είναι «μυστικές», δηλαδή είναι άγνωστες στο επίπεδο εξουσιοδότησης που διαθέτουν οι κακόβουλοι χρήστες. Η συνηθέστερη τακτική που ακολουθείται είναι ο επιτιθέμενος να αποκτά πρόσβαση σε ένα έγκυρο μέλος του συστήματος(όχημα ή RSU) και στη συνέχεια να κρυφακούει για ευαίσθητες πληροφορίες. Αυτό οδηγεί στην διαρροή των προσωπικών δεδομένων των χρηστών και την απώλεια της ιδιωτικότητάς τους.
- Επιθέσεις δρομολόγησης(Routing attacks). Αυτές οι επιθέσεις λαμβάνουν χώρα στο επίπεδο δικτύου και εκμεταλλεύονται την εγγενή πολυπλοκότητα των μηχανισμών δρομολόγησης στο IoV. Στοχεύουν κυρίως στην υποκλοπή και ανακατεύθυνση πακέτων προκειμένου να βλάψουν το σύστημα.
- Επιθέσεις στην αυθεντικότητα των δεδομένων(Data authenticity attacks). Αυτές οι επιθέσεις επικεντρώνονται στο περιεχόμενο των πακέτων. Μπορεί να στείλουν πολλές φορές το ίδιο μήνυμα(Replay), να αλλοιώσουν κάποιο μήνυμα που υπέκλεψαν(tampering) ή να το πλαστογραφήσουν. Ένας σχετικά πρόσφατος τύπος επίθεσης περιλαμβάνει την αποστολή παραπλανητικών μηνυμάτων(ατυχήματα, συνωστισμός κτλ.) προκειμένου να επηρεαστεί η κυκλοφορία των οχημάτων(Illusion attack).

Οι προαναφερθείσες κατηγορίες και επιθέσεις αποτελούν ένα μικρό μέρος των κινδύνων που μπορούν να προκληθούν στα VANETs από κακόβουλους φορείς. Προτείνονται οι δημοσιεύσεις [6], [7], [8] και [10] για περαιτέρω εμβάθυνση στο ζήτημα. Στην παρούσα εργασία, μας ενδιαφέρουν πρωτίστως οι επιθέσεις στη μυστικότητα και σε κάποιο βαθμό οι επιθέσεις στη διαθεσιμότητα.

2.4 Ορισμοί

Εδώ ορίζονται μερικές βασικές έννοιες οι οποίες απαντώνται συχνά στην υπόλοιπη εργασία.

VANET: Ως VANET(Vehicular ad-hoc Network) ορίζεται ένα δίκτυο οχημάτων με ικανότητα ασύρματης επικοινωνίας το οποίο δημιουργείται αυθόρμητα. Ο όρος εισήχθη πρώτη φορά από τον Chai Keong Toh το 2001[11] ως μια υποκατηγορία ασύρματων κινητών δικτύων. Αποτελεί ένα βασικό κομμάτι των Έξυπνων Συστημάτων Μεταφοράς(Intelligent Transport Systems -ITS), καθώς μέσω της επικοινωνίας μεταξύ κινούμενων οχημάτων και σταθερών σημείων στο δρόμο(RSU) παρέχεται μια πληθώρα εφαρμογών, όπως οδική ασφάλεια και εξατομικευμένες υπηρεσίες θέσης.
IoV: Το Διαδίκτυο των Οχημάτων(Internet of Vehicles) στηρίζεται πάνω στα VANETs και ο κύριος στόχος του είναι η διασύνδεση και ανταλλαγή πληροφοριών σε πραγματικό χρόνο

μεταξύ όλων των εμπλεκομένων στα δίκτυα οχημάτων(οδηγοί, πεζοί, RSUs, αρχές ελέγχου κτλ.). Αποτελεί ουσιαστικά μια εφαρμογή του IoT εξειδικευμένη για συστήματα μεταφορών.

Pseudonym: Για την προστασία της ιδιωτικότητας των οχημάτων, κατά την επικοινωνία δε χρησιμοποιούνται τα πραγματικά αναγνωριστικά τους αλλά κάποιες άλλες ταυτότητες, οι οποίες ονομάζονται ψευδώνυμα.

RSU: Αυτές οι μονάδες υποδομής(Road Side Units) λειτουργούν ως σημεία διεπαφής για τα οχήματα του δικτύου. Παρέχουν ασύρματη κάλυψη και πρόσβαση στο διαδίκτυο στα οχήματα που βρίσκονται στην εμβέλειά τους, και είναι σε θέση να επικοινωνήσουν ασύρματα με αυτά. Ταυτόχρονα, διατηρούν μια σύνδεση με κάποιο κεντρικό διακομιστή ο οποίος εκτελεί την επεξεργασία των εισερχόμενων μηνυμάτων και παράγει μηνύματα τα οποία μέσω των RSUs προωθούνται πίσω στα οχήματα. Είναι στατικές μονάδες, και σε πραγματικά οδικά δίκτυα το κόστος τους είναι υψηλό, οπότε είναι τοποθετημένες στρατηγικά ώστε να παρέχουν τη μεγαλύτερη δυνατή κάλυψη χωρίς ωστόσο να μπορούν να καλύψουν όλο το οδικό δίκτυο.

RA: Ένα απαραίτητο στοιχείο της υποδομής είναι η Έμπιστη Αρχή(Register Authority). Αυτή η οντότητα θεωρείται αδιάβλητη και έμπιστη, επομένως είναι υπεύθυνη για την τήρηση εμπιστευτικών πληροφοριών, όπως δημόσια και ιδιωτικά κλειδιά, πιστοποιητικά, λίστες με ψευδώνυμα και ό,τι άλλο χρειάζεται για την ασφαλή λειτουργία του συστήματος. Έχει την εξουσία να αποκλείει ύποπτα οχήματα εντάσσοντάς τα σε μια «Μαύρη Λίστα»(blacklist) και να παράγει νέα διαπιστευτήρια όποτε της ζητούνται μέσω των RSUs. Την RA, στην πλειονότητα των περιπτώσεων, διαχειρίζεται κάποιος κρατικός φορέας.

Adversary: Είναι οποιοσδήποτε επιτίθεται στο σύστημα, για οποιοδήποτε λόγο. Μπορεί να είναι μέλος του συστήματος ή εξωτερικός, μπορεί να είναι παθητικός ή να προσπαθεί ενεργά να βλάψει το σύστημα, μπορεί να έχει πολλά διαφορετικά κίνητρα ή και κανένα. Σε κάθε περίπτωση, είναι ο «εχθρός» του συστήματος και ψάχνει να εκμεταλλευτεί οποιαδήποτε ευπάθεια και αδυναμία για να διεισδύσει ή να καταστρέψει.

Privacy: Στα δίκτυα οχημάτων πρέπει να εξασφαλίζεται, πέρα από την ασφάλεια των φυσικών προσώπων και η ιδιωτικότητά τους. Αυτό σημαίνει πως το σύστημα πρέπει να είναι σε θέση να προστατεύσει τα ευαίσθητα δεδομένα τους ή να τα κρυπτογραφεί καταλλήλως, έτσι ώστε να μην μπορούν να ταυτοποιηθούν από κάποιον επιτιθέμενο σε περίπτωση που διαρρεύσουν.

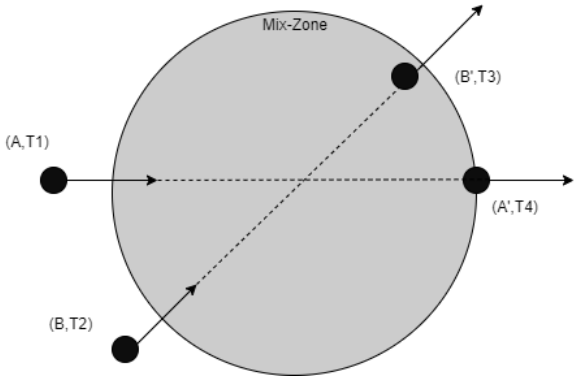
Location Privacy: Όλες οι πληροφορίες θέσης που αφορούν τους χρήστες του δικτύου, όπως η τροχιά τους ή σημεία ενδιαφέροντος(Points of Interest), θα πρέπει να προστατεύονται από μη εξουσιοδοτημένους χρήστες[7].

Κεφάλαιο 3: Συναφής βιβλιογραφία

Σε αυτό το κεφάλαιο παρατίθενται οι σχετικές δημοσιεύσεις στον επιστημονικό τομέα που ασχολήθηκαν με τις τεχνικές εξασφάλισης ιδιωτικότητας θέσης και αποτέλεσαν τη βάση της παρούσας διπλωματικής. Οι τεχνικές που θα αναφερθούν περιλαμβάνουν την ανταλλαγή ψευδωνύμων μεταξύ των οχημάτων, την ένταξή τους σε ομάδες για τη χρήση μιας κοινής ταυτότητας, τη χρήση τυχαίων σιωπηλών διαστημάτων και το συνδυασμό όλων των παραπάνω.

3.1 Mix-Zone

Η έννοια της Mix-Zone εισήχθη από τους Beresford & Stajano το 2003 με στόχο στην εξασφάλιση της ανωνυμίας των χρηστών σχετικά με τις Υπηρεσίες Βάσει Θέσης(Location Based Services – LBS). Όρισαν τη Mix-Zone για μια ομάδα χρηστών ως: «μια συνδεδεμένη χωρική περιοχή μέγιστου μεγέθους, μέσα στην οποία κανένας χρήστης δεν καταχωρεί επανακλήσεις εφαρμογών»[12]. Η ανωνυμία επιτυγχάνεται αν οι χρήστες που μπαίνουν σε αυτήν την περιοχή αλλάξουν τα ψευδώνυμά τους, καλύπτοντας έτσι το ίχνος τους. Ένα απλοϊκό παράδειγμα Mix-Zone φαίνεται στην εικόνα 8, όπου στην μη παρατηρήσιμη περιοχή εισέρχονται δύο χρήστες με ψευδώνυμα A,B αντίστοιχα, τα ενημερώνουν σε A',B' και εξέρχονται από τη ζώνη μετά από κάποιο διάστημα, οπότε ξαναγίνονται ορατοί στους παρόχους LBS. Η ιδιωτικότητα των χρηστών προστατεύεται από το γεγονός πως ένας επιτιθέμενος δεν μπορεί να συνδέσει με βεβαιότητα τα ψευδώνυμα που υπήρχαν κατά την είσοδο στην ζώνη με τα ψευδώνυμα που βγήκαν από αυτήν.



Εικόνα 8: Mix-Zone

Είναι προφανές πως η επιλογή της ζώνης είναι καθοριστική για την επίτευξη ενός ικανοποιητικού ποσοστού ιδιωτικότητας. Αν η πυκνότητα των οχημάτων που βρίσκονται ταυτόχρονα στη ζώνη κατά την διάρκεια ενημέρωσης των ψευδωνύμων είναι σχετικά μικρή, τότε κάποιος εξωτερικός παρατηρητής έχει υψηλότερες πιθανότητες να συνδέσει σωστά τα ψευδώνυμα εισόδου με τα ψευδώνυμα εξόδου. Το ίδιο συμβαίνει και αν τα οχήματα περνάνε σταθερό χρόνο μέσα στη ζώνη, καθώς ουσιαστικά εκφυλίζεται σε μια ουρά FIFO. Ένα πλαίσιο για την κατασκευή Mix-Zones(MobiMix) προτάθηκε από τους Liu κ.α.[13], προσπαθώντας να αντιμετωπίσει κυρίως τις επιθέσεις χρονισμού(timing attacks) με τη χρήση χρονικών περιθωρίων(time windows) για την ομαδοποίηση των αφιχθέντων οχημάτων. Ακόμα, περιοχές

όπου η συχνότητα των διερχόμενων οχημάτων είναι υψηλή, όπως διασταυρώσεις και χώροι στάθμευσης καταστημάτων, αποτελούν κατάλληλα σημεία για τη δημιουργία Mix-Zones.

Πέρα από το ζήτημα της προστασίας της ιδιωτικότητας των οχημάτων/χρηστών από αναξιόπιστους παρόχους LBS, υπάρχει το ζήτημα των μηνυμάτων ασφαλείας(Broadcast Safety Message – BSM) που πρέπει να εκπέμπουν τα οχήματα και περιέχουν εξίσου χρήσιμες πληροφορίες για κάποιον κακόβουλο παρατηρητή. Προς αυτήν την κατεύθυνση, οι Freudiger κ.α.[14] πρότειναν την δημιουργία κρυπτογραφημένων Mix-Zones(CMIX) σε σημεία υψηλής συγκέντρωσης οχημάτων, π.χ. διασταυρώσεις, στις οποίες τα BSM θα κρυπτογραφούνταν με ένα κοινό συμμετρικό κλειδί που θα διένειμαν οι RSUs σε όποιο όχημα έμπαινε στην περιοχή. Η κρυπτογράφηση των μηνυμάτων με ένα κοινό κλειδί για όλα τα οχήματα μπορεί να εμποδίσει έναν εξωτερικό επιτιθέμενο αλλά είναι αναποτελεσματική απέναντι σε έναν εσωτερικό επιτιθέμενο, δηλαδή κάποιον που έχει ένα όχημα με γνήσια διαπιστευτήρια και λειτουργεί κακόβουλα.

Μια λύση στο παραπάνω πρόβλημα προτάθηκε από τους Scheuer κ.α.[15] και περιλάμβανε τη χρήση ενδιάμεσων χειριστών(Proxy). Η αρχή λειτουργίας του μοντέλου έχει ως εξής: σε κάθε Mix-Zone υπάρχει ένας ανεξάρτητος Proxy ο οποίος έχει ένα σετ από έγκυρα διαπιστευτήρια(public/private key, certificate) και κάθε όχημα που εισέρχεται στη ζώνη γνωρίζει το δημόσιο κλειδί και το πιστοποιητικό του. Τα οχήματα που κινούνται μέσα στη ProMix-Zone σταματούν να στέλνουν απλά BSM και αρχίζουν να στέλνουν μηνύματα κρυπτογραφημένα με το κλειδί του Proxy, ώστε μόνο αυτός να μπορεί να τα αποκρυπτογραφήσει. Ο Proxy συλλέγει όλα τα μηνύματα, αποφασίζει πως πρέπει να διανεμηθούν στα οχήματα και στέλνει τη λίστα με τα κατάλληλα μηνύματα στο κάθε όχημα κρυπτογραφημένη με το αντίστοιχο δημόσιο κλειδί. Θεωρείται πως ο εσωτερικός επιτιθέμενος δεν μπορεί να σπάσει την κρυπτογράφηση σε βιώσιμο χρονικό διάστημα, επομένως δεν μπορεί να παρακολουθήσει μηνύματα που δεν προορίζονται για τον ίδιο. Ιδιαίτερη προσοχή πρέπει να δοθεί από τον Proxy στην επιλογή των οχημάτων που πρέπει να λαμβάνουν τα μηνύματα του οχήματος-στόχου, καθώς μια πολύ ευρεία επιλογή αυξάνει τις πιθανότητες του επιτιθέμενου να συμπεριληφθεί στη λίστα αλλά μια πολύ στενή επιλογή μπορεί να θέσει σε κίνδυνο την ασφάλεια των οχημάτων. Στην έρευνά τους, πρότειναν αυτή η επιλογή να γίνεται με βάση κάποιους γενικούς κανόνες, π.χ. «σχετικό» θεωρείται ένα όχημα που βρίσκεται ακριβώς από πίσω αλλά όχι ένα όχημα που περνάει από τη γέφυρα που βρίσκεται από πάνω, εμπειρικά δεδομένα για την κίνηση του οδικού δικτύου και από τα δεδομένα που χρειάζονται τα αυτόματα συστήματα των οχημάτων για να λειτουργήσουν(Automated Driver-Assistance Systems-ADAS).

Οι Ying κ.α.[16] πρότειναν μια εναλλακτική μορφή Mix-Zone, ονόματι Dynamic Mix-Zone for Location Privacy(DMLP). Σε αυτήν την τεχνική, ένα όχημα που επιθυμεί να αλλάξει ψευδώνυμο μπορεί να δημιουργήσει μια δυναμική Mix-Zone ανεξάρτητα από το σημείο του δρόμου που βρίσκεται ακολουθώντας την εξής διαδικασία: 1)στέλνει ένα αίτημα αλλαγής ψευδωνύμου στην υποδομή μέσω των RSUs, 2) οι servers της υποδομής στέλνουν εντολή σε όλα τα οχήματα που βρίσκονται σε μια περιοχή γύρω από το όχημα(η επιλογή αυτής της περιοχής εξαρτάται από το επίπεδο ιδιωτικότητας που απαιτείται) να αλλάξουν τα ψευδώνυμά τους, 3) τα οχήματα για ένα διάστημα στέλνουν κρυπτογραφημένα μηνύματα προκειμένου να αποπροσανατολίσουν τους επιτιθέμενους και 4) επιστρέφουν στην αποστολή κανονικών μηνυμάτων με τα νέα ψευδώνυμα. Η μέθοδος αυτή έχει το πλεονέκτημα ότι μπορεί να

χρησιμοποιηθεί ανεξαρτήτως της φύσης του οδικού δικτύου στο οποίο βρίσκεται το όχημα και είναι σχετικά απλή στην υλοποίησή της.

3.2 Group

Το 2007, οι Guo κ.α.[17] στην προσπάθεια τους να διατηρήσουν τα οφέλη στην ιδιωτικότητα που προσφέρουν οι τεχνικές PKI(Public Key Infrastructure), αλλά ταυτόχρονα και να μειώσουν τον αριθμό των κλειδιών που χρειαζόταν να διατηρούν τα οχήματα προκειμένου να αλλάζουν συχνά ψευδώνυμα – ο οποίος μπορεί και να ανερχόταν στις 44.000 το χρόνο, πρότειναν ένα μοντέλο βασισμένο στη χρήση ομαδικών υπογραφών. Ένα μοντέλο ομαδικής υπογραφής(Group Signature Scheme) επιτρέπει στα μέλη μιας συγκεκριμένης ομάδας να υπογράφουν τα μηνύματά τους εκ μέρους της ομάδας. Αυτό σημαίνει ότι όλες οι υπογραφές μπορούν να επαληθευτούν από το κοινό δημόσιο κλειδί της ομάδας αλλά δεν μπορούν να οδηγήσουν πίσω στους χρήστες, δηλαδή είναι αδύνατο να αποφανθεί κάποιος μη εξουσιοδοτημένος ότι 2 υπογραφές ανήκουν στο ίδιο μέλος. Συνήθως, υπάρχει μια οντότητα η οποία ονομάζεται Διαχειριστής ή Αρχηγός Ομάδας(Group Manager/Leader) που έχει τη δυνατότητα να συνδέσει τα μέλη με τις υπογραφές τους, για λόγους ταυτοποίησης ή μη αποποίησης ευθυνών(non-repudiation).

Αυτό το μοντέλο έχει ορισμένα ιδιαίτερα χρήσιμα χαρακτηριστικά που είναι επιθυμητά στην περίπτωση των VANETs:

- Privacy: Η βασικότερη ιδιότητα, η οποία εγγυάται πως δεν μπορεί ένα συγκεκριμένο μέλος να ταυτοποιηθεί από την υπογραφή του από κανέναν άλλο παρά μόνο από τον Group Manager.
- Accountability: Σε περίπτωση που παραστεί ανάγκη να βρεθεί ο αποστολέας ενός μηνύματος, π.χ. γιατί το μήνυμα περιείχε εσφαλμένες πληροφορίες, μόνο ο Group Manager μπορεί να ανοίξει την υπογραφή και να εντοπίσει την ταυτότητα του αποστολέα χρησιμοποιώντας το ιδιωτικό κλειδί διαχειριστή που διαθέτει. Χωρίς αυτό το κλειδί πρέπει να είναι υπολογιστικά ανέφικτο για κάποιο άτομο να βρει την ταυτότητα του αποστολέα από την υπογραφή του.
- Unlinkability: Οι υπογραφές του ίδιου μέλους για διαφορετικά μηνύματα δεν μπορούν να συσχετιστούν ώστε να αποκαλύψουν την ταυτότητά του. Δηλαδή, οι διαφορετικές υπογραφές δεν έχουν κάποιο κοινό χαρακτηριστικό που να δηλώνουν ότι έχουν προέλθει από τον ίδιο υπογράφοντα.
- Exculpability: Αυτή η ιδιότητα εγγυάται ότι κανένα μέλος της ομάδας δεν μπορεί να στείλει ένα μήνυμα με υπογραφή τέτοια ώστε να φαίνεται ότι είναι από διαφορετικό μέλος. Αυτό σημαίνει ότι ο Group Manager μπορεί πάντα να αναγνωρίσει τον πραγματικό αποστολέα ενός μηνύματος.
- Unforgeability: Αυτή η ιδιότητα είναι παρόμοια με την παραπάνω, με τη διαφορά ότι αντιστοιχεί σε εξωτερικά άτομα. Δηλαδή, δεν μπορεί κάποιος που δεν είναι μέλος της ομάδας να πλαστογραφήσει μια υπογραφή έτσι ώστε να φαίνεται ως μέλος της ομάδας.
- Coalition-Resistance: Αυτή η ιδιότητα προστατεύει το σύστημα από τη συνεργασία των μελών, δηλαδή ακόμα και αν πολλαπλά μέλη συνεργαστούν για να δημιουργήσουν μια

υπογραφή από κοινού με σκοπό να μην είναι ταυτοποιήσιμη, ο Group Manager θα μπορέσει να την αποδώσει σε κάποιο από τα μέλη που συνωμότησαν.

Ένα μειονέκτημα των ομαδικών υπογραφών είναι ότι δεν είναι το ίδιο αποδοτικές με τις συμβατικές ψηφιακές υπογραφές, αν και έχουν προταθεί διάφορα μοντέλα κυρίως πάνω στο Short Signature Scheme των Boneh-Boyen όπως στα [18],[19]. Μια πιθανή βελτιστοποίηση που προτάθηκε στο [17] είναι η πιθανοτική επαλήθευση των υπογραφών από τα οχήματα της ομάδας, δηλαδή το κάθε όχημα να επαληθεύει κάποια από τα μηνύματα. Αν σε ένα δίκτυο 1000 κόμβων που βρίσκονται όλοι σε ακτίνα επικοινωνίας μεταξύ τους κάθε κόμβος επαληθεύει 3 τυχαία μηνύματα από τα 1000 που στέλνονται, η πιθανότητα κάθε μήνυμα να επαληθευτεί από τουλάχιστον 1 κόμβο είναι πάνω από 95%. Αυτό σημαίνει ότι ένα τροποποιημένο μήνυμα ή ένας μη εξουσιοδοτημένος αποστολέας μπορεί να βρεθεί γρήγορα χωρίς να χρειάζεται όλα τα οχήματα να το επιβεβαιώσουν.

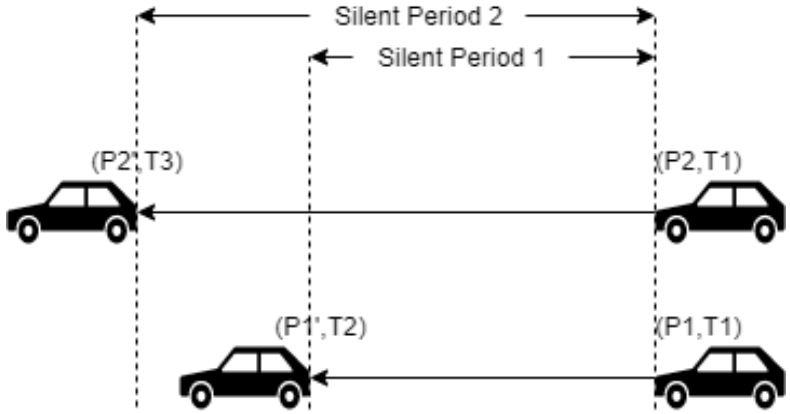
Όπως έχει γίνει φανερό, ο Group Manager παίζει καθοριστικό ρόλο στην εύρυθμη λειτουργία της ομάδας, και αυτό με τη σειρά του εγείρει ερωτήματα σχετικά με τον καλύτερο τρόπο επιλογής αλλά και την αξιοπιστία του. Έχουν προταθεί διάφοροι τρόποι επιλογής, με τους πιο συνηθισμένους να είναι η τυχαία επιλογή από την υποδομή ανάμεσα στα οχήματα του group ή η από πριν τοποθέτηση συγκεκριμένων οχημάτων ως αρχηγών(π.χ. σχολικά λεωφορεία, ασθενοφόρα) ανάλογα με τη φύση της ομάδας. Σχετικά με την αξιοπιστία των αρχηγών, μια πιθανή απάντηση είναι η κατανομή των αρμοδιοτήτων του σε διαφορετικές οντότητες.[17] Αν διάφορες οντότητες κατέχουν μέρους του Διαχειριστικού Ιδιωτικού Κλειδιού, τότε προκειμένου να ανοιχτεί μια υπογραφή και να ταυτοποιηθεί ένας αποστολέας θα πρέπει να συνεργαστούν πολλαπλά άτομα/οχήματα. Αυτό απελευθερώνει το σύστημα από το ελάττωμα του Μοναδικού Σημείου Αποτυχίας(Single Point of Failure) και προσφέρει μεγαλύτερη ασφάλεια στους χρήστες ότι δε θα γίνει κατάχρηση των αρμοδιοτήτων. Στην παραπάνω φιλοσοφία, οι Zhang κ.α.[20] πρότειναν την ανάθεση του διαχειριστικού ρόλου των ομάδων στις RSUs, δίνοντας τους τη δυνατότητα να κατανέμουν κλειδιά σε οχήματα που εισέρχονται στην εμβέλειά τους. Έχουν προταθεί διάφορες μέθοδοι κατανομής κλειδιών και διαχείρισης, όπως από τους Park κ.α.[21] που πρότειναν τη δημιουργία ενός κατανεμημένου συστήματος διαχείρισης κλειδιών με βάση τις RSUs.

Οι Sampigethaya κ.α.[22] το 2007 πρότειναν ένα μοντέλο, ονόματι AMOEBA, το οποίο επιχειρούσε να προστατέψει τόσο την ιδιωτικότητα θέσης του οχήματος από παρακολούθηση θέσης αλλά και την ιδιωτικότητα του χρήστη με παροχή ανώνυμης πρόσβασης σε υπηρεσίες LBS. Ομαδοποιώντας συστάδες οχημάτων που κινούνταν προς την ίδια κατεύθυνση με παρόμοια ταχύτητα στην ίδια ομάδα, κατάφεραν να δημιουργήσουν μια εκτεταμένη Σιωπηλή Περίοδο(βλ. κεφ. 3.3) στην οποία μπορούσαν να αλλάξουν τα ψευδώνυμά τους και να είναι αρκετά δύσκολο για έναν επιτιθέμενο να τα συνδέσει με τα προηγούμενα. Φυσικά, αυτή η τεχνική εισάγει ένα κόστος στη φυσική ασφάλεια των οχημάτων γιατί αν δεν εκπέμπουν σήματα ασφαλείας αυξάνεται ο κίνδυνος πρόκλησης ατυχημάτων. Στην περίπτωση όμως μηνυμάτων που η περίοδός τους δεν είναι της τάξης των δεκάτων του δευτερολέπτου, όπως τα μηνύματα προς τις RSU για τη συλλογή δεδομένων, που μπορεί να στέλνονται κάθε κάποια δευτερόλεπτα, υπάρχουν ορισμένα σημαντικά πλεονεκτήματα: 1) αυξάνεται η περίοδος αλλαγής των ψευδωνύμων ανάμεσα στα μηνύματα οπότε χρειάζεται λιγότερος αποθηκευτικός χώρος, 2) μειώνεται η κίνηση στο δίκτυο καθώς μόνο ο αρχηγός στέλνει μηνύματα στις RSU και 3) η

εκτεταμένη Σιωπηλή Περίοδος προσφέρει καλύτερη ιδιωτικότητα θέσης. Ακόμα, αν τοποθετηθεί ο Αρχηγός Ομάδας ως proxy ανάμεσα στα οχήματα και στις LBS, μπορεί να προστατευτεί η ιδιωτικότητα των χρηστών καθώς δε θα μπορεί ένας κακόβουλος πάροχος LBS να συνδυάσει τα αιτήματα με τα οχήματα γιατί όλα θα περνάνε μέσω του Proxy. Μελέτησαν ακόμα την αντοχή του μοντέλου απέναντι σε διάφορους τύπους επιτιθέμενων, όπως ο GPA, RPA, LAA κ.α. και πρότειναν συνδυασμούς μεθόδων όπως silent period, RSU separation, transmission power control.

3.3 Σιωπηλή Περίοδος(Silent Period)

Η τεχνική αυτή προτάθηκε το 2005 από τους Huang κ.α.[23] και στη δημοσίευσή τους ορίζεται ως: «η μεταβατική περίοδος ανάμεσα στη χρήση νέων ή προηγούμενων ψευδωνύμων, κατά την οποία οι σταθμοί δεν επιτρέπεται να μεταδώσουν πληροφορία». Αυτό έχει ως αποτέλεσμα να δυσχεραίνει τη συσχέτιση ενός κινούμενου σταθμού με ένα συγκεκριμένο ψευδώνυμο, καθώς ο επιτιθέμενος δεν μπορεί να εξάγει αξιόπιστα συμπεράσματα από τα χωροχρονικά στοιχεία των μεταδιδόμενων πακέτων. Αν πολλαπλά οχήματα στην ίδια περιοχή χρησιμοποιούν Σιωπηλές Περιόδους, δημιουργείται ουσιαστικά μια εικονική Ζώνη Ανάμειξης στην οποία η κίνηση των χρηστών δεν μπορεί να παρακολουθηθεί. Ένα παράδειγμα αποτυπώνεται καλύτερα στην εικόνα 9, όπου 2 οχήματα με ψευδώνυμα P1, P2 παραμένουν σιωπηλά για τυχαία χρονική περίοδο το καθένα και ξαναρχίζουν να εκπέμπουν μηνύματα τις στιγμές T2, T3 με τα ψευδώνυμα P1', P2' αντίστοιχα. Ένας επίδοξος ωτακουστής δεν μπορεί πλέον να ξεχωρίσει αν το μήνυμα που υπέκλεψε τη στιγμή T2 ανήκει στο όχημα 1 ή στο όχημα 2.



Εικόνα 9: Silent Period

Παρά την ασφάλεια που προσφέρει αυτή η μέθοδος απέναντι σε επιθέσεις συσχέτισης, υπάρχει το εξής μειονέκτημα: το διάστημα που το όχημα παραμένει σιωπηλό αυξάνει το ρίσκο για την πρόκληση ατυχήματος, καθώς τα οχήματα γύρω του δε θα είναι ενήμερα για την τοποθεσία του και αντίστροφα. Το βέλτιστο διάστημα που μπορεί να μένει ένα όχημα σιωπηλό εξαρτάται από πολλούς παράγοντες, όπως την κίνηση στο δρόμο, την ταχύτητα των οχημάτων κ.α., ωστόσο αυτό το διάστημα για την αποφυγή ατυχημάτων είναι στην πλειονότητα των περιπτώσεων της τάξης των 100-300ms[10] που μπορεί να μην είναι αρκετό για να εγγυηθεί την

ιδιωτικότητα των οχημάτων. Οι Sampigethaya κ.α.[24], μέσω προσομοιώσεων, έδειξαν πώς για να επιτευχθεί ουσιαστική ιδιωτικότητα των οχημάτων απαιτούνται Σιωπηλές Περίοδοι μεγαλύτερες των 2s. Σε έρευνα που πραγματοποιήθηκε από τους Petit κ.α.[25], επιβεβαιώθηκε πως σιωπηλά διαστήματα μεγαλύτερα των 2s, παρότι βελτίωναν δραστικά την ιδιωτικότητα των οχημάτων, επηρέαζαν σημαντικά την ασφάλεια του συστήματος. Τέτοιοι χρόνοι θα μπορούσαν να είναι αποδεκτοί σε μηνύματα ανάμεσα στα οχήματα και την υποδομή(V2I), επομένως αυτή η τεχνική θα μπορούσε να είναι βιώσιμη για τέτοιου είδους μηνύματα, όχι όμως και για BSMs. Μια πρόταση στο [22] σχετικά με τέτοιου είδους μηνύματα ήταν, να εφαρμόζεται η Σιωπηλή Περίοδος στις εισόδους και εξόδους από αυτοκινητοδρόμους, καθώς αποτελούν πιο ασφαλείς τοποθεσίες από τις κύριες λωρίδες κυκλοφορίας. Κατ' αυτόν τον τρόπο επιτυγχάνεται μια ισορροπία ανάμεσα στην φυσική ασφάλεια του οχήματος και την ιδιωτικότητά του.

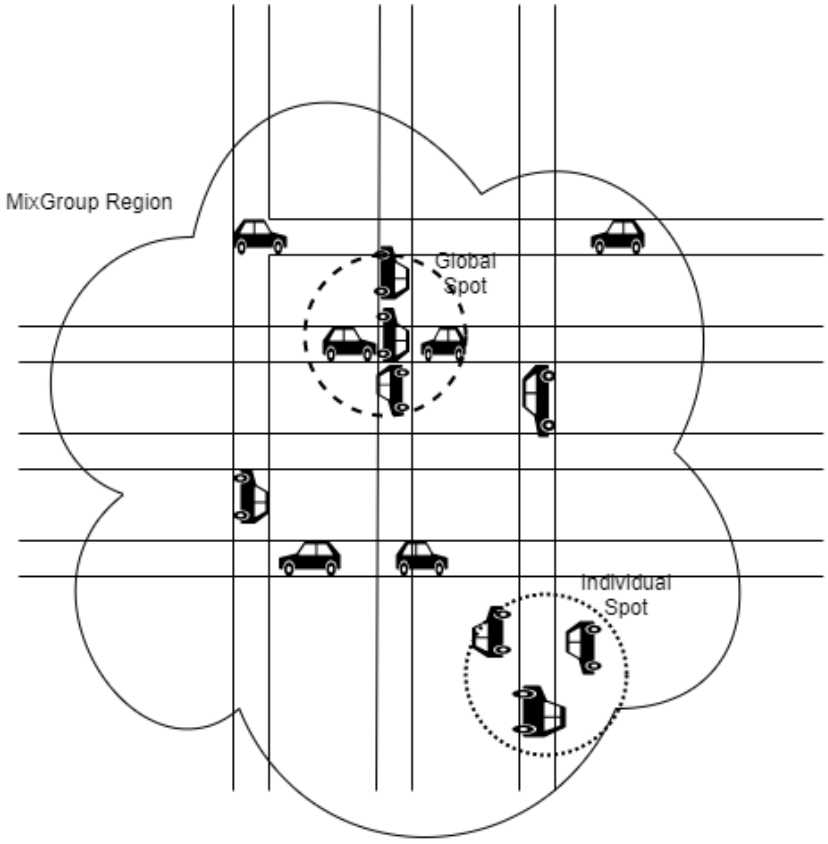
3.4 Mix-Group

Στο επίκεντρο της παρούσας εργασίας βρίσκεται η τεχνική του Mix-Group, η οποία αναλύεται παρακάτω. Αυτή η μέθοδος προτάθηκε από τους Huang κ.α.[26] το 2016, οι οποίοι έκαναν τις εξής παρατηρήσεις:

- Λίγα οχήματα συναντώνται στα καθολικά κοινωνικά σημεία(global social spots) καθώς η πλειονότητα των οχημάτων συναντώνται σε διαφορετικά σημεία κατά την κίνησή τους στο οδικό δίκτυο.
- Τα περισσότερα οχήματα διαθέτουν ατομικά κοινωνικά σημεία(individual social spots) στα οποία συναντάνε το μεγαλύτερο αριθμό άλλων οχημάτων μέσα στη μέρα. Ακόμα, αυτά τα σημεία παραμένουν σταθερά σε βάθος χρόνου, όπως και η στιγμή της ημέρας κατά την οποία τα επισκέπτονται. Αυτό οφείλεται στην κοινωνική φύση των οδηγών, καθώς τέτοια σημεία είναι συνήθως η κατοικία, ο χώρος εργασίας και άλλα αντίστοιχα μέρη.

Από τις παραπάνω παρατηρήσεις προέκυψε ο διαχωρισμός των κοινωνικών σημείων σε καθολικά και ατομικά. Προκειμένου να επιτευχθεί η βέλτιστη ιδιωτικότητα, είναι απαραίτητη η αξιοποίηση και των δύο αυτών χαρακτηριστικών. Σε αυτόν τον τρόπο σκέψης κινείται και η μέθοδος Mix-Group.

Η τεχνική αυτή στοχεύει στο συνδυασμό των καθολικών και ατομικών κοινωνικών σημείων στην πορεία ενός οχήματος προκειμένου να κατασκευαστεί μια εκτεταμένη περιοχή ανταλλαγής ψευδωνύμων. Μέσα σε αυτήν την περιοχή, ένα όχημα μπορεί να αλλάζει διαδοχικά ψευδώνυμα με σκοπό να πετύχει την βέλτιστη απόκρυψη της ταυτότητάς του. Όσα οχήματα εισέρχονται στην περιοχή γίνονται μέλη μιας ομάδας και χρησιμοποιούν μια κοινή ταυτότητα για την επικοινωνία τους με άλλα οχήματα και την υποδομή για όσο χρόνο κινούνται μέσα στην περιοχή και είναι μέλη της ομάδας. Με αυτόν τον τρόπο αξιοποιούνται και οι δύο τύποι κοινωνικών σημείων, καθώς συμπεριλαμβάνονται στην εκτεταμένη περιοχή και είναι έγκυρα σημεία ανταλλαγής ψευδωνύμων.



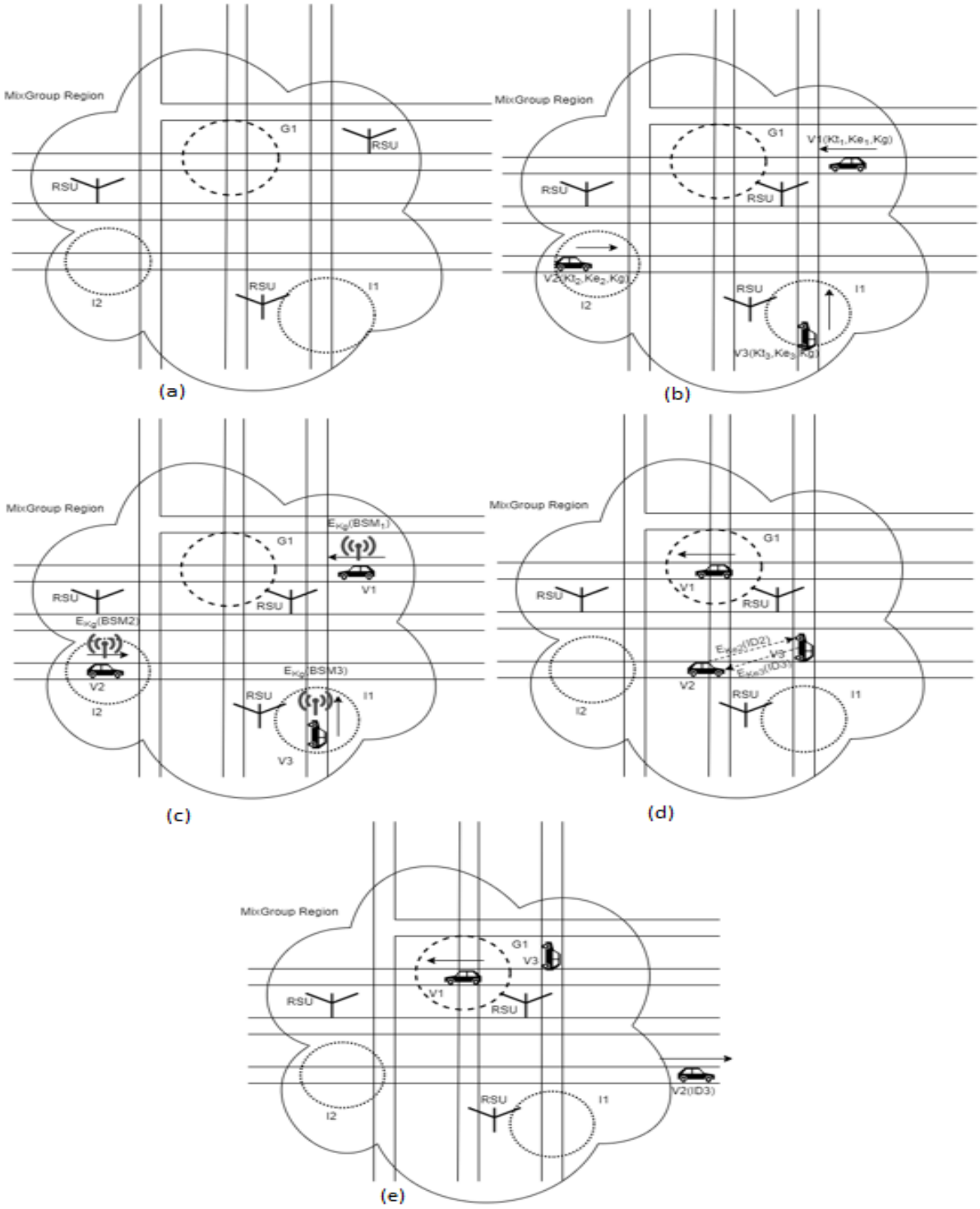
Εικόνα 10: MixGroup

Πιο λεπτομερώς, το σχήμα λειτουργεί ως εξής:

- Καθορίζεται μια περιοχή η οποία θα λειτουργεί ως περιοχή Mix-Group και περιλαμβάνει έναν αριθμό από καθολικά και ατομικά κοινωνικά σημεία.
- Όλα τα οχήματα που εισέρχονται στην περιοχή αιτούνται να γίνουν μέλη της κοινής ομάδας και αποκτούν μια κοινή ταυτότητα(group identity) την οποία χρησιμοποιούν στην εκπομπή(broadcast) μηνυμάτων.
- Ταυτόχρονα, εφοδιάζονται με ένα σύνολο από προσωρινά κλειδιά(temporary and exchange identity) τα οποία χρησιμοποιούν στη διαδικασία ανταλλαγής ψευδωνύμων με άλλα οχήματα εντός της ομάδας.
- Το κάθε όχημα, κατά την κίνησή του μέσα στην περιοχή, υπολογίζει το όφελος στην ιδιωτικότητα που θα αποκομίσει ανταλλάσσοντας ψευδώνυμα τη δεδομένη χρονική στιγμή και αποφασίζει με σκοπό τη βέλτιστη ιδιωτικότητα.
- Η ανταλλαγή των ψευδωνύμων γίνεται υπό την κάλυψη των προσωρινών ταυτοτήτων των οχημάτων.
- Κατά την έξοδο του από την ομάδα, το όχημα ενεργοποιεί το νέο ψευδώνυμο και το χρησιμοποιεί για τις μελλοντικές επικοινωνίες του.

Η παραπάνω λειτουργία γίνεται ευκολότερα κατανοητή με το ακόλουθο παράδειγμα: Στην εικόνα 11.a φαίνεται η αρχική κατάσταση του συστήματος, στην οποία η περιοχή MG απαρτίζεται από τα καθολικά κοινωνικά σημεία Gx και τα ατομικά Ix. Στην εικόνα 11.b τα

οχήματα Vx εισέρχονται στην περιοχή και λαμβάνουν τα κλειδιά Kt, Ke και Kg, τα οποία αντιστοιχούν στα προσωρινά κλειδιά, κλειδιά ανταλλαγής και ομαδικά κλειδιά αντίστοιχα. Στην εικόνα 11.c φαίνεται ένα τυπικό broadcast των οχημάτων μέσα στην περιοχή, χρησιμοποιώντας το Kg. Στην εικόνα 1.d αποτυπώνεται μια ανταλλαγή ψευδωνύμων μεταξύ δύο οχημάτων. Τέλος, στην εικόνα 11.e φαίνεται η αποχώρηση ενός οχήματος από την περιοχή MG.



Εικόνα 11: Λειτουργία MixGroup

Το παραπάνω σχήμα παρουσιάζει ανθεκτικότητα απέναντι σε μια πληθώρα επιθέσεων διαφόρων τύπων. Αρχικά, η χρήση προτυποποιημένων τεχνικών κρυπτογράφησης και αυθεντικοποίησης εγγυάται την ασφάλεια του συστήματος απέναντι σε επιθέσεις εξαντλητικής αναζήτησης καθώς είναι υπολογιστικά ανέφικτο για κάποιον να εξάγει χρήσιμες πληροφορίες χωρίς να διαθέτει τα απαιτούμενα κλειδιά. Ακόμα, η χρήση ψηφιακών υπογραφών αποτρέπει έναν επιτιθέμενο από το να υποδυθεί ένα έγκυρο όχημα ή να παραποιήσει μηνύματα. Αντιστοίχως, δεν μπορεί να πλαστογραφηθεί η ταυτότητα και τα μηνύματα των RSUs. Οι επιθέσεις επανάληψης είναι ανέφικτες χάρη στη χρήση χρονοσφραγίδων(timestamps). Ένας επίδοξος ωτακουστής(GPA, RPA) δεν είναι σε θέση να παρακολουθήσει συνεχόμενα ένα όχημα που εισέρχεται σε αυτήν την περιοχή μέχρι την έξοδό του από αυτήν, όπως και μετέπειτα καθότι δε θα μπορεί να συνδέσει το νέο ψευδώνυμο που χρησιμοποιεί το όχημα με αυτό που είχε κατά την είσοδό του. Στην περίπτωση που ένας εσωτερικός επιτιθέμενος εκπέμψει μηνύματα με εσφαλμένες πληροφορίες θέσης, αποσκοπώντας στη δημιουργία χάους και ατυχημάτων στο σύστημα, η υπογραφή κάθε μηνύματος επιτρέπει την ανακάλυψη και εντοπισμό του υπαίτιου προκειμένου να αποδοθούν ευθύνες. Παρομοίως, η επίθεση στην αξιοπιστία ενός οχήματος από κάποιον που αντιγράφει την ταυτότητα του, αποφεύγεται με την υπογραφή των μηνυμάτων κάνοντας χρήση πιστοποιητικών εκδιδόμενων από μια αξιόπιστη αρχή(Register Authority - RA). Τέλος, το σύστημα είναι ανθεκτικό και στην περίπτωση που υπάρχει ένας συνδυασμός εσωτερικού και εξωτερικού επιτιθέμενου. Σε αυτήν την επίθεση, ο εσωτερικός επιτιθέμενος μετά την ανταλλαγή του με κάποιο όχημα θα μεταφέρει τις πληροφορίες της ανταλλαγής στον εξωτερικό ωτακουστή με σκοπό την παρακολούθησή του. Αυτό εμποδίζεται αν το όχημα υπό παρακολούθηση ανταλλάξει ξανά ψευδώνυμα, το οποίο εκ σχεδιασμού είναι αρκετά πιθανό.

Η αποτελεσματικότητα του σχήματος ενισχύεται από τον κατάλληλο συνδυασμό των πλεονεκτημάτων των τεχνικών του Group και της Mix-Zone. Το Mix-Group παρέχει ικανοποιητικά επίπεδα ιδιωτικότητας ακόμη και σε συνθήκες χαμηλής κυκλοφορίας, λόγω της συσσώρευσης ανταλλαγών ψευδωνύμων στα κοινωνικά σημεία, κάτι το οποίο δεν επιτυγχάνει το Mix-Zone. Επίσης, η χρήση ομάδων επιτρέπει τη συνέχιση εκπομπών μηνυμάτων ασφαλείας προκειμένου να μην υπάρξει αύξηση της πιθανότητας ατυχημάτων. Από όλα τα παραπάνω, γίνονται εμφανείς οι δυνατότητες αυτού του σχήματος για την επίτευξη της βέλτιστης ιδιωτικότητας θέσης.

Κεφάλαιο 4: Εργαλεία, αλγόριθμοι και μετρικές

Σε αυτό το κεφάλαιο, αρχικά γίνεται αναφορά στα προγραμματισικά εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση των προσομοιώσεων της παρούσας εργασίας. Στη συνέχεια, παρουσιάζονται οι διαφορετικοί κρυπτογραφικοί αλγόριθμοι που χρησιμοποιήθηκαν. Τέλος, αναλύονται οι μετρικές αξιολόγησης που χρησιμοποιήθηκαν για να κρίνουν τις επιδόσεις της παρούσας υλοποίησης.

4.1 Εργαλεία

Σε αυτό το κεφάλαιο γίνεται η παρουσίαση κάποιων από τα βασικότερα εργαλεία που χρησιμοποιήθηκαν κατά τη συγγραφή αυτής της ερευνητικής μελέτης. Τα εργαλεία θα μπορούσαν να χωριστούν σε 3 κύριες κατηγορίες:

Η πρώτη κατηγορία αφορά εργαλεία προσομοίωσης δικτύων. Τα εργαλεία προσομοίωσης δικτύων είναι εργαλεία λογισμικού τα οποία μοντελοποιούν διαφόρων ειδών δίκτυα υπολογιστών και προβλέπουν τη συμπεριφορά τους. Τέτοιου είδους εργαλεία επιτρέπουν την απεικόνιση διαφορετικών δικτυακών τοπολογιών και προτύπων επικοινωνίας(WiFi, LAN, 5G), τη αλληλεπίδραση μεταξύ συνδεδεμένων κόμβων, τη μέτρηση της επίδοσης των λόγω δικτύων καθώς και πληθώρα άλλων εφαρμογών. Η χρήση τους είναι απαραίτητη, καθώς τα σύγχρονα δίκτυα επικοινωνιών παρουσιάζουν τέτοιο μέγεθος και πολυπλοκότητα που οι τυπικές αναλυτικές μέθοδοι δεν αρκούν για τη μελέτη τους.

Η επόμενη κύρια ομάδα εργαλείων που χρησιμοποιήθηκαν είναι τα εργαλεία προσομοίωσης κίνησης. Αυτά τα εργαλεία είναι υπεύθυνα για τη μαθηματική μοντελοποίηση φυσικών συστημάτων μεταφορών. Μέσω της εφαρμογής λογισμικού υπολογιστών, συνεισφέρουν στη σχεδίαση, συντήρηση, βελτίωση και λειτουργία των εν λόγω συστημάτων. Η κύρια χρήση αυτών των εργαλείων είναι η μοντελοποίηση οδικών δικτύων και η προσομοίωση της κίνησης των οχημάτων μέσα σε αυτά. Τέτοιου είδους εργαλεία έχουν πληθώρα εφαρμογών στο συγκεκριμένο ερευνητικό τομέα, καθώς επιτρέπουν καλύτερο σχεδιασμό και πρόβλεψη πολύπλοκων συστημάτων μεταφορών.

Μια ομάδα που χρησιμοποιήθηκε σε συνδυασμό με τα παραπάνω εργαλεία είναι τα εργαλεία απεικόνισης. Η ανάγκη για οπτικοποίηση οδήγησε στην ανάπτυξη τέτοιων εργαλείων, τα οποία είναι υπεύθυνα για την παρουσίαση μιας κατανοητής εικόνας της κατάστασης. Παρόλο που τέτοια εργαλεία δεν προσθέτουν κάποια επιπλέον πληροφορία στην προσομοίωση, ο τρόπος παρουσίασής της παίζει καθοριστικό ρόλο στην κατανόηση, ερμηνεία και εξαγωγή συμπερασμάτων πάνω σε αυτήν. Οι εφαρμογές τους εκτείνονται σε πολλαπλές ερευνητικές περιοχές, με τις κυριότερες να είναι: στην ιατρική, στις οικονομικές επιστήμες και στις θετικές επιστήμες. Στη δική μας έρευνα χρησιμοποιήσαμε αυτά τα εργαλεία για να απεικονίσουμε την κατάσταση των οδικών και υπολογιστικών δικτύων. Η ακριβής αναπαράσταση των μοντέλων είναι ζωτικής σημασίας στην εξαγωγή αξιόπιστων συμπερασμάτων.

Εξίσου σημαντική ήταν η συνεισφορά συμβατικών εργαλείων που χρησιμοποιήθηκαν για την καταγραφή ενδιάμεσων αποτελεσμάτων, παρακολούθηση των συστημάτων και αποσφαλμάτωση(debugging). Παρά την κοινοτοπία αυτών των εργαλείων, διαδραματίζουν καθοριστικό ρόλο στην επιτυχημένη διεξαγωγή πειραμάτων και στην ομαλοποίηση των

διαδικασιών. Συνήθως, τέτοια εργαλεία βρίσκονται στον πυρήνα σχεδόν όλων των εφαρμογών, καθώς η παρατήρηση, διόρθωση και ανατροφοδότηση είναι απαραίτητο στάδιο στην ανάπτυξη οποιασδήποτε εφαρμογής. Η κατάλληλη χρήση αυτών των εργαλείων επιτρέπει τον εντοπισμό και την άμεση διόρθωση προβλημάτων, επιταχύνοντας την παραγωγή ορθών αποτελεσμάτων.

4.1.1 NS-3

Το NS-3[27] ανήκει στην πρώτη κατηγορία εργαλείων, επομένως είναι ένας προσομοιωτής δικτύων υπολογιστών. Η χρήση και ανάπτυξή του είναι δωρεάν στα πλαίσια της GNU GPLv2 άδειας, και προορίζεται κυρίως για ακαδημαϊκή και ερευνητική χρήση. Για την εγκατάσταση του απαιτείται η ύπαρξη κάποιας διανομής Linux(στην περίπτωση που είναι απαραίτητο να εγκατασταθεί σε Windows, προτείνεται virtualization ή χρήση του Windows Subsystem for Linux) Είναι γραμμένο στη γλώσσα προγραμματισμού C++, υποστηρίζοντας Python scripting, και αποτελεί το διάδοχο του NS-2. Η κύρια λειτουργία του είναι η κατασκευή εικονικών τοπολογιών δικτύων τόσο ασύρματης όσο και ενσύρματης επικοινωνίας. Ανήκει στην κατηγορία προσομοιωτών διακριτών γεγονότων. Υποστηρίζει το integration με μια πληθώρα εφαρμογών όπως ένα από τα άλλα εργαλεία που χρησιμοποιήθηκαν, το SUMO, για το οποίο περισσότερες λεπτομέρειες αναφέρονται παρακάτω.

Ένα από τα βασικά πλεονεκτήματα του NS-3 είναι πως μέσω ενός εύχρηστου API επιτρέπει τη σχεδίαση, παραμετροποίηση και προσομοίωση συστημάτων που προσεγγίζουν σε ικανοποιητικό βαθμό τα δεδομένα του φυσικού κόσμου. Η δημιουργία τέτοιων δικτύων σε πραγματικές συνθήκες για καθαρά πειραματικούς σκοπούς δεν είναι αποδοτική, καθώς ο χρόνος μελέτης ενός πραγματικού συστήματος ξεπερνά κατά πολύ το χρόνο μια αντίστοιχης προσομοίωσης. Ακόμα, το υλικό κόστος είναι πολύ μικρότερο καθώς δε χρειάζεται η κατασκευή και τοποθέτηση φυσικών μηχανημάτων για τη δημιουργία του απαιτούμενου συστήματος. Λόγω των πλεονεκτημάτων που αναφέρθηκαν παραπάνω, παρέχει τη δυνατότητα μελέτης πολλαπλών σεναρίων σε σύντομο χρονικό διάστημα οδηγώντας σε καλύτερη πρόβλεψη της συμπεριφοράς του συστήματος.

Υπάρχουν 2 βασικές κατηγορίες προσομοιωτών: οι προσομοιωτές διακριτού χρόνου και οι προσομοιωτές συνεχούς χρόνου. Το NS-3 ανήκει στην πρώτη κατηγορία. Προσομοιώνει σενάρια μέσω διακριτών γεγονότων, δηλαδή μοντελοποιεί τη λειτουργία ενός συστήματος ως μια διακριτή ακολουθία γεγονότων στο χρόνο. Κάθε γεγονός λαμβάνει χώρα σε μια συγκεκριμένη χρονική στιγμή και προκαλεί μια αλλαγή στην κατάσταση του συστήματος. Αυτά τα γεγονότα μπορούν να τίθενται είτε στατικά είτε δυναμικά σε μια προσομοίωση, χαρακτηριστικό που καθιστά το NS-3 ιδανική επιλογή για ευμετάβλητα συστήματα. Η ύπαρξη δυναμικών γεγονότων φάνηκε ιδιαίτερα χρήσιμη καθώς μας επέτρεψε την υλοποίηση της επικοινωνίας κατά τη διάρκεια της προσομοίωσης χωρίς να χρειάζεται αυτή να έχει προκαθοριστεί από πριν αλλά μόνο το μοντέλο της.

Αυτό το εργαλείο υποστηρίζει την πλειονότητα των τυποποιημένων(standarized) πρωτοκόλλων ασύρματης και ενσύρματης επικοινωνίας. Παρέχει υποστήριξη για τα εξής επίπεδα επικοινωνίας:

1. Physical layer
2. Data link layer

3. Internet layer
4. Transport layer
5. Application layer

Για κάθε ένα από τα παραπάνω επίπεδα, τα πρωτόκολλα είναι υλοποιημένα βάσει των διεθνών προτύπων(IEEE) επομένως θεωρούνται αξιόπιστα και έχουν γίνει αποδεκτά από την επιστημονική κοινότητα. Το εργαλείο ενημερώνεται και βελτιώνεται ανά τακτά χρονικά διαστήματα, προκειμένου να διατηρεί την αξιοπιστία του στην πάροδο του χρόνου και να ενσωματώνει τα νεότερα πρότυπα στον τομέα.

Στην παρούσα εργασία υπήρξε η ανάγκη για χρήση τόσο ασύρματων όσο και ενσύρματων πρωτοκόλλων για την προσομοίωση της επικοινωνίας. Στο κομμάτι της ασύρματης επικοινωνίας, το NS-3 υποστηρίζει το πρωτόκολλο WAVE(Wireless Access in Vehicular Environments) όπως αυτό ορίζεται στα πρότυπα IEEE 1609 και IEEE 802.11p και προσομοιώνει τη δυναμική επικοινωνία μεταξύ των οχημάτων του δικτύου αλλά και μεταξύ των οχημάτων και των σταθμών υποδομής(RSU). Για την ενσύρματη διασύνδεση της υποδομής, μια από τις επιλογές που παρέχονται από το εργαλείο είναι το μοντέλο CSMA που λειτουργεί στη φιλοσοφία του Ethernet, δημιουργώντας ένα κοινό δίαυλο μεταφοράς δεδομένων. Μια σημαντική παρατήρηση είναι πως αυτό το μοντέλο αποτελεί μια απλοποιημένη εκδοχή του Ethernet και δεν μπορεί να προσομοιώσει πλήρως ένα πραγματικό δίκτυο τέτοιου είδους στα πρότυπα του IEEE 802.3, αλλά παρέχει ένα ενδιαφέρον υποσύνολο δυνατοτήτων. Τα πρωτόκολλα αυτά είναι πλήρως παραμετροποιήσιμα στο εργαλείο επιτρέποντας τη δοκιμή διαφορετικών σεναρίων.

Μια ακόμα σημαντική λειτουργικότητα που παρέχεται από το εργαλείο είναι η υποστήριξη πρωτοκόλλων UDP και TCP. Στην επικοινωνία οχημάτων, λόγω της φύσης του δικτύου, είναι προτιμότερη η χρήση του πρωτοκόλλου UDP για τη μεταφορά πακέτων από του TCP. Η περιορισμένη εμβέλεια των οχημάτων, η αστάθεια του μέσου μεταφοράς και η ταχύτητα μεταβολής του συστήματος καθιστούν μη αποδοτική τη δημιουργία σταθερών συνδέσεων για τη μεταφορά ροής δεδομένων όπως γίνεται στο TCP. Το πρωτόκολλο UDP που υποστηρίζεται είναι υλοποιημένο βάσει του προτύπου RFC 768 και επιτρέπει την επικοινωνία άνευ σύνδεσης μεταξύ των οχημάτων μην παρέχοντας φυσικά κάποια εγγύηση για την επιτυχημένη μεταφορά της πληροφορίας. Όπως και στα πραγματικά συστήματα, η απώλεια πακέτων μπορεί να αντιμετωπιστεί απλά με επανάληψη του εν λόγω πακέτου μέχρι να φτάσει στον προορισμό του.

Τέλος, το εργαλείο δίνει τη δυνατότητα προσομοίωσης μοντέλων κατανάλωσης ενέργειας. Η δομή που παρέχεται επιτρέπει τον ακριβή καθορισμό πηγών ενέργειας και μοντέλων κατανάλωσης και ανανέωσης ενέργειας. Επίσης, δίνει ένα μοντέλο κατανάλωσης ενέργειας για WiFi(WiFi Radio Energy Model) με αρκετές δυνατότητες παραμετροποίησης για ένα πλήθος σεναρίων.

4.1.2 SUMO(Simulation of Urban Mobility)

Το SUMO[28],[29] ανήκει στη δεύτερη κατηγορία και είναι μια σουίτα εργαλείων προσομοίωσης συνεχούς οδικής κίνησης, σχεδιασμένη για την υποστήριξη μεγάλων οδικών δικτύων. Ο κώδικας του είναι ανοιχτός και η χρήση του υπόκειται στην άδεια EPLv2. Χρησιμοποιείται για την προσομοίωση της συμπεριφορά της κίνησης που προκύπτει από

πολλαπλά οχήματα μέσα σε ένα δεδομένο οδικό δίκτυο. Επιτρέπει τη μικροσκοπική παρατήρηση του οδικού συστήματος, δηλαδή κάθε όχημα θεωρείται ως μοναδική οντότητα με ξεχωριστά χαρακτηριστικά και συμπεριφορά στη διάρκεια του χρόνου. Η ευρεία γκάμα από εργαλεία που διαθέτει του επιτρέπουν να αντιμετωπίσει ένα μεγάλο σύνολο ζητημάτων διαχείρισης οδικής κυκλοφορίας.

Ένα σημαντικό πλεονέκτημα του SUMO έγκειται στην ποικιλία των οδικών συνθηκών που μπορεί να προσομοιώσει. Παρέχει τη δυνατότητα προσομοίωσης οχημάτων διαφορετικού τύπου και μεγέθους, υποστήριξη για κανόνες προτεραιότητας και κανονισμούς οδικής κυκλοφορίας γενικότερα, πολλαπλές τοπολογίες οδικών δικτύων με πολλαπλές λωρίδες καθώς και σήμανση με πινακίδες και φωτεινούς σηματοδότες. Μπορεί να διαχειριστεί δίκτυα με πολλές χιλιάδες δρόμους και οχήματα και είναι ικανό για ταχεία εκτέλεση προσομοιώσεων, με πάνω από 100.000 ενημερώσεις οχημάτων ανά δευτερόλεπτο.

Όπως προαναφέρθηκε, το εργαλείο αυτό ακολουθεί μια μικροσκοπική στρατηγική για τα οχήματα. Το κάθε όχημα έχει τη δική του διαδρομή μέσα στο σύστημα η οποία καθορίζεται από τα σημεία αναχώρησης και προορισμού του. Παρέχονται διάφορες μέθοδοι υπολογισμού των διαδρομών, από την απλοϊκή εκτέλεση ενός αλγορίθμου συντομότερων διαδρομών(Dijkstra, A*), στην οποία θεωρείται ότι κάθε όχημα βρίσκεται μόνο του στο δίκτυο και συνήθως οδηγεί σε κυκλοφοριακή συμφόρηση, μέχρι ένα σύστημα δυναμικής δρομολόγησης, στο οποίο η διαδρομή των οχημάτων επιλέγεται μέσω εξερεύνησης όλων των εναλλακτικών δρομολογίων με κριτήριο τη συνολική υγεία του δικτύου.

Στο κομμάτι της σχεδίασης των οδικών δικτύων, πέρα από τις προεπιλεγμένες τοπολογίες που παρέχονται(grid, spider, random) δίνεται η δυνατότητα εισαγωγής οδικών δικτύων από διαφορετικές πηγές(VISUM, OpenDRIVE, OSM κ.α.). Ακόμα, το SUMO μπορεί να καλύψει πιθανές παραλείψεις που μπορεί να έχουν τα αρχεία εισόδου, χρησιμοποιώντας ευριστικές συναρτήσεις για να υποθέσει τις ελλιπείς τιμές. Με αυτόν τον τρόπο, μπορούν να αναπαρασταθούν και να προσομοιωθούν πραγματικά οδικά δίκτυα, καλύπτοντας μια σειρά ρεαλιστικών ζητημάτων και δίνοντας παράλληλα μεγαλύτερη αξιοπιστία στα αποτελέσματα.

Πέρα από την απεικόνιση σε ένα ενσωματωμένο γραφικό περιβάλλον που διαθέτει για την άμεση παρατήρηση της προσομοίωσης, τα αποτελέσματα μπορούν να εξαχθούν σε αρχεία γενικού τύπου(XML) και να τροφοδοτηθούν σε άλλα σχετικά εργαλεία. Το εργαλείο διαθέτει ενσωματωμένη υποστήριξη για άλλους προσομοιωτές οδικής κίνησης και για προσομοιωτές δικτύων υπολογιστών. Στη συγκεκριμένη περίπτωση, μετατρέψαμε την τοπολογία του οδικού δικτύου, τα οχήματα και τις διαδρομές τους σε ένα αρχείο το οποίο στη συνέχεια εισαγάγαμε στον προσομοιωτή δικτύου NS-3.

Η σουίτα αναπτύχθηκε με σκοπό πέρα από υψηλή ταχύτητα, να παρέχει και υψηλή φορητότητα. Υπάρχουν διαθέσιμες εκδόσεις για τις βασικότερες διανομές Linux, καθώς και για Windows. Ο πυρήνας του εργαλείου είναι γραμμένος σε standard C++ και έχουν χρησιμοποιηθεί προτυποποιημένες βιβλιοθήκες για να εξασφαλιστεί η διαλειτουργικότητά του σε άλλα συστήματα. Ένας σταθερός κύκλος βελτιώσεων και ενημερώσεων του λογισμικού το διατηρεί ενημερωμένο σχετικά με τις νεότερες εξελίξεις στον τομέα των οδικών δικτύων. Η συμβατότητά με τα διάφορα λειτουργικά συστήματα και η ευκολία εγκατάστασης και παραμετροποίησης του το καθιστούν ιδανική επιλογή για γρήγορη ανάπτυξη προσομοιώσεων και παραγωγή αποτελεσμάτων άμεσα.

4.1.3 NetAnim

Το NetAnim[30] ανήκει στην τρίτη κατηγορία εργαλείων που χρησιμοποιήθηκαν και είναι ένας offline animator, βασισμένος στην εργαλειοθήκη Qt, που εμπεριέχεται στην εγκατάσταση του NS-3. Ως είσοδο δέχεται ένα αρχείο XML που παράγεται στο τέλος της προσομοίωσης και δημιουργεί μια ζωντανή απεικόνιση του δικτύου με βάση αυτό. Οι βασικότερες λειτουργίες που παρέχει είναι οι εξής:

- Απεικόνιση πακέτων τόσο από ενσύρματες όσο και από ασύρματες συνδέσεις
- Χρονολογική απεικόνιση πακέτων με δυνατότητα φιλτραρίσματος με βάση τα metadata τους
- Στατιστικά για τη θέση κόμβων και απεικόνιση της πορείας κινούμενων κόμβων
- Εκτύπωση metadata των πακέτων
- Δυνατότητα επεξεργασίας αρχείων μέτρησης ροής και απεικόνιση στατιστικών για κάθε ροή
- Απεικόνιση IP και MAC διευθύνσεων
- Πάγωμα της προσομοίωσης σε ένα συγκεκριμένο χρόνο
- Εκτύπωση του πίνακα δρομολόγησης

Σε αυτήν την ερευνητική εργασία χρησιμοποιήθηκε το NetAnim για να οπτικοποιήσει την τοπολογία του δικτύου αλλά και την επικοινωνία των διαφορετικών οντοτήτων(όχημα, RSU, RA) μεταξύ τους.

4.1.4 PyViz

Το PyViz(Python Visualizer) ανήκει επίσης στην κατηγορία των εργαλείων απεικόνισης και είναι ενσωματωμένο στην κύρια διανομή του NS-3. Είναι γραμμένο στη γλώσσα προγραμματισμού Python, αλλά μπορεί να υποστηρίξει προσομοιώσεις γραμμένες και σε C++. Το βασικότερο σημείο στο οποίο διαφέρει από το NetAnim είναι ότι δίνει μια ζωντανή απεικόνιση της προσομοίωσης κατά τη διάρκεια της εκτέλεσης, σε αντίθεση με το NetAnim που χρειάζεται να περιμένει να τελειώσει η προσομοίωση για να επεξεργαστεί το XML αρχείο που παράγεται. Κάποια βασικά χαρακτηριστικά είναι:

- Απεικόνιση της δικτυακής τοπολογίας της προσομοίωσης
- Εμφάνιση πληροφοριών δικτύου(IP, interface) σε κάθε κόμβο
- Απεικόνιση της κίνησης των πακέτων
- Δυνατότητα διακοπής και συνέχισης της προσομοίωσης
- Ενσωματωμένη γραμμή εντολών για αποσφαλμάτωση της προσομοίωσης

Στην παρούσα έρευνα χρησιμοποιήθηκε κυρίως ως εργαλείο debugging, καθώς ο τρόπος παρουσίασης των δικτυακών διεπαφών ήταν ιδιαίτερα κατανοητός.

4.1.5 Tcpdump

Το tcpdump[32] αποτελεί ένα από τα βασικότερα συμβατικά εργαλεία παρακολούθησης δικτύων. Έρχεται με τη μορφή εκτελέσιμου προγράμματος που τρέχει σε γραμμή εντολών και

υποστηρίζεται στα περισσότερα λειτουργικά συστήματα τύπου Unix. Η βασικότερη λειτουργία του είναι η ανάλυση πακέτων δικτύου, τα οποία μπορεί είτε να επεξεργάζεται δυναμικά παρακολουθώντας την αντίστοιχη δικτυακή διεπαφή, είτε να δέχεται ως είσοδο ένα αρχείο καταγραφής πακέτων. Μεταξύ άλλων, εμφανίζει πληροφορίες για τις διευθύνσεις αποστολέα και παραλήπτη ενός πακέτου, αν υφίσταται κατακερματισμό λόγω του μέσου, το μέγεθος του και αν το πακέτο έφτασε επιτυχώς στον προορισμό του. Είναι ένα εργαλείο που χρησιμοποιείται ευρέως σε όλες τις δικτυακές υποδομές για την παρακολούθηση της υγείας των συστημάτων και την ανάλυση πιθανών προβλημάτων στο δίκτυο.

Στην εργασία μας, το πρόγραμμα αυτό χρησιμοποιήθηκε ως εργαλείο ανάλυσης των πακέτων που δημιουργήθηκαν κατά τη διάρκεια της προσομοίωσης. Το NS-3 παραμετροποιήθηκε προκειμένου να παράγει αρχεία καταγραφής πακέτων(.pcap files) για κάθε κόμβο του συστήματος με δυνατότητα δικτυακής επικοινωνίας, τα οποία στη συνέχεια τροφοδοτήθηκαν στο tcpdump προκειμένου να γίνει μια εκτενέστερη ανάλυση της κίνησης του δικτύου, η οποία πολλές φορές δεν ήταν δυνατή με τα εργαλεία απεικόνισης που αναφέρθηκαν παραπάνω.

4.2 Αλγόριθμοι κρυπτογράφησης

Σε αυτό το κεφάλαιο αναλύονται οι βασικοί αλγόριθμοι που χρησιμοποιήθηκαν για την κρυπτογράφηση της επικοινωνίας μεταξύ των οντοτήτων του συστήματος.

4.2.1 AES(Advanced Encryption Standard)

Η εφαρμογή του αλγορίθμου Rijndael για μέγεθος block 128 bits είναι ευρέως διαδεδομένη ως AES. Ο αλγόριθμος αυτός αναπτύχθηκε από τους Ολλανδούς RIjmen και Daemen για το διαγωνισμό επιλογής ενός νέου προτύπου κρυπτογράφησης που διεξήχθη από το NIST(National Institute of Standards and Technology) από το 1997 έως το 2000. Το 2001, ο αλγόριθμος αυτός εγκρίθηκε επίσημα στις ΗΠΑ με το πρότυπο FIPS PUB 197 και περιλαμβάνεται επίσης στο πρότυπο ISO/IEC 18033-3. Αξιοσημείωτο είναι το γεγονός πως είναι ο πρώτος δημόσιος αλγόριθμος που από το 2003 επιτρέπει η NSA να χρησιμοποιηθεί για την κρυπτογράφηση εμπιστευτικών εγγράφων της[33].

Ο AES είναι ένας αλγόριθμος συμμετρικής κρυπτογράφησης, δηλαδή κρυπτογραφεί το μήνυμα χρησιμοποιώντας ένα μυστικό κλειδί το οποίο πρέπει να γνωρίζει ο αποδέκτης του μηνύματος για να μπορέσει να αποκρυπτογραφήσει το μήνυμα. Το μήκος αυτού του κλειδιού μπορεί να λάβει τις εξής τιμές: 128, 192 και 256 bits και χρησιμοποιείται ως δείκτης του επιπέδου ασφαλείας που παρέχεται από τον αλγόριθμο. Θεωρείται κρυπτογραφικά ασφαλής καθώς μέχρι σήμερα δεν έχει προταθεί κάποια μέθοδος κρυπτανάλυσης που να τον λύνει σε αποδεκτό χρονικό διάστημα και για αυτόν το λόγο είναι ο πιο διαδεδομένος συμμετρικός αλγόριθμος σε ακαδημαϊκό και εμπορικό επίπεδο.

Η κρυπτογράφηση πραγματοποιείται σε blocks, δηλαδή το αρχικό κείμενο(plaintext) χωρίζεται σε κομμάτια συγκεκριμένου μεγέθους και το καθένα κρυπτογραφείται ξεχωριστά. Σε αντίθεση με το μήκος κλειδιού που είναι μεταβλητό, το μέγεθος του block που χρησιμοποιείται παραμένει σταθερό στα 128 bits. Το κάθε block υφίσταται μια σειρά μετατροπών περνώντας από

τα διάφορα στάδια του αλγορίθμου και μετά από ένα συγκεκριμένο αριθμό επαναλήψεων(γύρων) παράγεται το κρυπτογραφημένο αποτέλεσμα. Το μέγεθος του κλειδιού καθορίζει τον αριθμό των γύρων ως εξής:

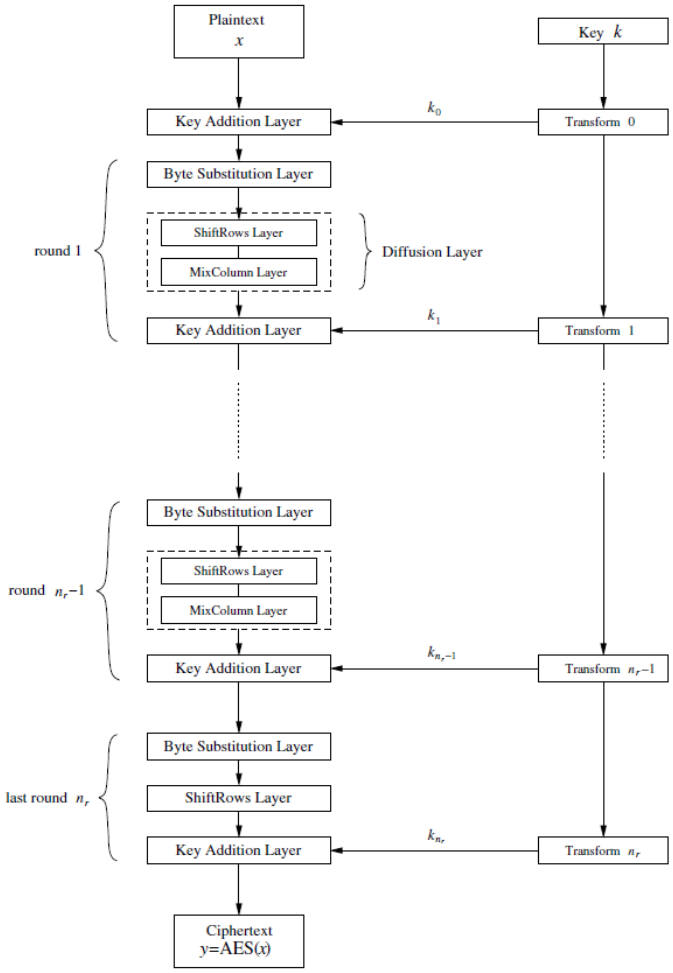
Key size(bits)	Number of rounds
128	10
192	12
256	14

Πίνακας 1: Σχέση μήκους κλειδιού-αριθμού γύρων στο AES

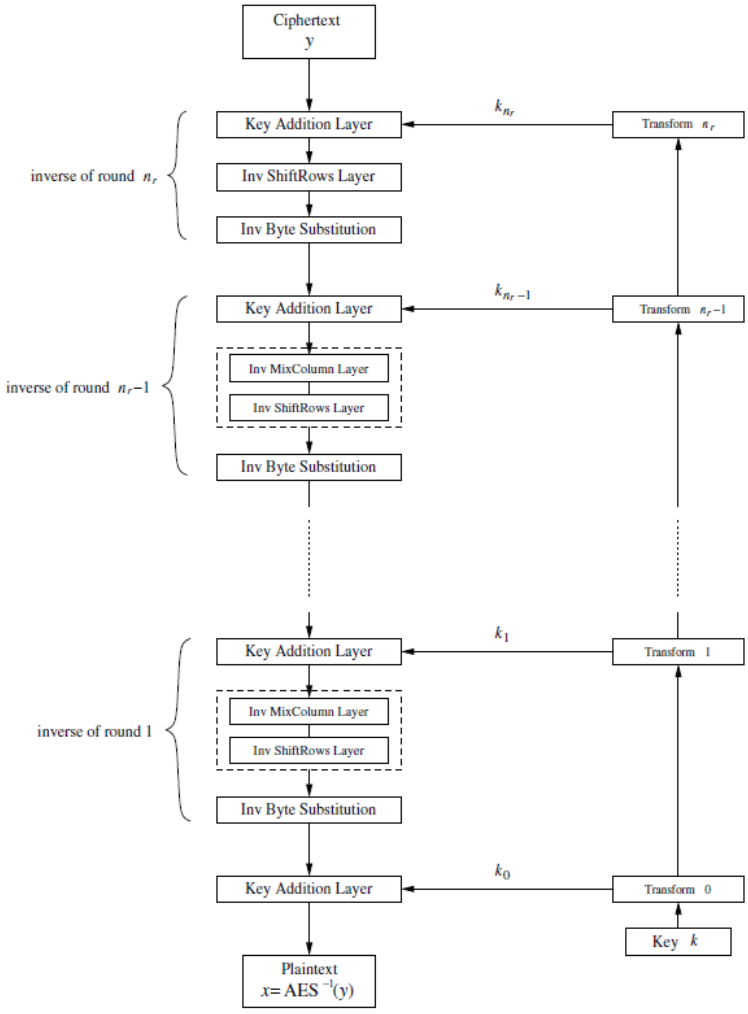
Σε κάθε γύρο, τα δεδομένα περνούν από τα 3 στάδια που διαθέτει ο αλγόριθμος. Τα στάδια αυτά είναι:

1. Στάδιο Key Addition. Στο στάδιο αυτό, ένα κλειδί μεγέθους 128 bits που έχει παραχθεί από το αρχικό κλειδί εφαρμόζεται στο block μέσω bitwise XOR.
2. Στάδιο Byte Substitution. Εδώ, πραγματοποιούνται μη γραμμικοί μετασχηματισμοί στα δεδομένα, κάνοντας χρήση ειδικών πινάκων αναφοράς. Αυτό το στάδιο εισάγει την απαραίτητη «σύγχυση»(confusion) στη ροή των δεδομένων.
3. Στάδιο Diffusion. Αυτό το στάδιο αποτελείται από 2 υποεπίπεδα, στα οποία τελούνται γραμμικοί μετασχηματισμοί. Το πρώτο επίπεδο ονομάζεται ShiftRows, και εκεί πραγματοποιείται μια μετάθεση των bytes του block ανάλογα με τη γραμμή που βρίσκονται, π.χ. τα bytes της δεύτερης σειράς ολισθαίνουν 1 θέση αριστερά. Το δεύτερο επίπεδο, το οποίο δεν εφαρμόζεται στον τελευταίο γύρο της κρυπτογράφησης και αντίστοιχα στον πρώτο γύρο της αποκρυπτογράφησης, λέγεται MixColumns και χρησιμοποιεί έναν αντιστρέψιμο γραμμικό μετασχηματισμό για να αναμείξει κάθε στήλη των 4 bytes. Το στάδιο MixColumn, σε συνδυασμό με το στάδιο ShitftRows, παρέχει στον αλγόριθμο την ιδιότητα της «διάχυσης»(diffusion).

Για την αποκρυπτογράφηση, με εξαίρεση το στάδιο Key Addition το οποίο λόγω του ότι αποτελείται από απλές XOR παραμένει το ίδιο και στο αντίστροφο, όλα τα υπόλοιπα επίπεδα πρέπει να αντιστραφούν και να εφαρμοστούν στο κρυπτοκείμενο με την αντίστροφη σειρά. Επειδή στο τελευταίο στάδιο της κρυπτογράφησης λείπει το στάδιο MixColumns, απουσιάζει και από το πρώτο στάδιο της αποκρυπτογράφησης όμως τα υπόλοιπα στάδια περιλαμβάνουν όλα τα στάδια. Αξίζει να σημειωθεί πως επειδή χρειάζονται τα επιμέρους κλειδιά με την ανάποδη σειρά στην αποκρυπτογράφηση, πρέπει να υπολογιστούν αναδρομικά όλα τα επιμέρους κλειδιά και μετά να εφαρμοστούν σε κάθε γύρο της αποκρυπτογράφησης. Αυτός ο προϋπολογισμός προσθέτει μια μικρή καθυστέρηση στην αποκρυπτογράφηση σε σχέση με την κρυπτογράφηση. Τα παρακάτω σχήματα δείχνουν τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα.



Εικόνα 12: Κρυπτογράφηση AES



Εικόνα 13: Αποκρυπτογράφηση AES

Ο αλγόριθμος αυτός έχει αποδειχτεί ανθεκτικός σε κάθε είδους επίθεση τα τελευταία 20 χρόνια, καθώς η ταχύτερη επίθεση στο πλήρες κλειδί μέχρι στιγμής, δημοσιεύτηκε το 2011, κάνει χρήση bicliques και είναι 4 φορές γρηγορότερη από την επίθεση εξαντλητικής αναζήτησης(brute force), καθιστώντας την πρακτικά ανέφικτη για τα μεγέθη κλειδιού που χρησιμοποιούνται από τον AES. Αποτελεί και αναμένεται να συνεχίσει να αποτελεί για τις επόμενες δεκαετίες τον πιο διαδεδομένο αλγόριθμο συμμετρικής κρυπτογράφησης στον επιστημονικό και βιομηχανικό τομέα, με πληθώρα εφαρμογών καθώς περιλαμβάνεται σε πρότυπα όπως το IPSec, το TLS, το WiFi 802.11i, το SSH, το Skype κ.α.

Οι κύριες απαιτήσεις κατά το σχεδιασμό του AES, πέρα από την ασφάλεια, ήταν η ταχύτητα και η αποδοτικότητα σε επίπεδο λογισμικού και υλικού. Ο αλγόριθμος έχει υψηλές επιδόσεις στους σύγχρονους υπολογιστές, ακόμα και με throughput της τάξεως των 10Gb/s σε σύγχρονους επεξεργαστές της Intel και της AMD, οι οποίοι είναι εξοπλισμένοι με ειδικά σύνολα εντολών για να επιταχύνουν τις πράξεις του AES. Τα χαρακτηριστικά του αλγορίθμου επιτρέπουν το scalability στο υλικό, καθώς και τις αποδοτικές υλοποιήσεις σε λογισμικό.

Στην παρούσα εργασία, ο AES χρησιμοποιήθηκε ως ο βασικός αλγόριθμος κρυπτογράφησης του κυρίου μέρους των πακέτων που ανταλλάσσονταν κατά την επικοινωνία των οχημάτων. Αυτή η επιλογή έγινε με βάση τα χαρακτηριστικά του που προαναφέρθηκαν, δηλαδή την υψηλή επίδοση ανεξαρτήτως υλικού και λογισμικού, τη στιβαρή ασφάλεια που προσφέρει σε θεωρητικό και πρακτικό επίπεδο, την ευρεία χρήση του σε πραγματικές εφαρμογές και την ύπαρξη μιας πληθώρας αποδοτικών υλοποιήσεων με ικανότητα ενσωμάτωσης σε οποιοδήποτε σύστημα.

4.2.2 RSA

Το σχήμα RSA δημοσιεύτηκε από τους Rivest, Shamir και Adleman το 1978[34] και έκτοτε έχει εδραιωθεί ως ο πιο ευρέως διαδεδομένος, κοινά αποδεκτός, γενικού σκοπού αλγόριθμος κρυπτογράφησης δημοσίου κλειδιού. Παρότι ο αλγόριθμος αυτός έχει μια πληθώρα πρακτικών εφαρμογών, χρησιμοποιείται κυρίως για την κρυπτογράφηση μικρού όγκου πληροφορίας, όπως στη μεταφορά κλειδιών, και στις ψηφιακές υπογραφές.

Η ασφάλεια του RSA στηρίζεται στο πρόβλημα της παραγοντοποίησης ακεραίων: ο πολλαπλασιασμός 2 ακεραίων είναι υπολογιστικά εύκολος, αλλά η αντίστροφη διαδικασία, δηλαδή η απόκτηση των αρχικών παραγόντων από το τελικό γινόμενο είναι υπολογιστικά δύσκολη. Συνήθως ως παράγοντες χρησιμοποιούνται 2 μεγάλοι πρώτοι αριθμοί παρόμοιου μεγέθους, οπότε το πρόβλημα μετατρέπεται στο λεγόμενο πρόβλημα παραγοντοποίησης πρώτων. Το μήκος σε bits του γινομένου αυτών των 2 αναφέρεται καταχρηστικά ως το μέγεθος κλειδιού του αλγορίθμου, π.χ. RSA-3072 αναφέρεται σε μήκος κλειδιού 3072 bits, αλλά στην πραγματικότητα 3072 bits είναι το μήκος του γινομένου N που έχει παραχθεί από τον πολλαπλασιασμό 2 πρώτων αριθμών P,Q με μήκος περίπου 1536 bits ο καθένας. Η μαθηματική ανάλυση του αλγορίθμου είναι πέρα του scope της παρούσας έρευνας, οπότε στη συνέχεια θα αναφερθούν κάποια γενικά στοιχεία για τον RSA και θα παραλειφθούν οι ακριβείς λεπτομέρειες της υλοποίησης.

Ως αλγόριθμος δημοσίου κλειδιού, ο RSA κάνει χρήση ενός ζεύγους κλειδιών, ενός δημοσίου κλειδιού και ενός ιδιωτικού. Ο αποστολέας και ο παραλήπτης διαθέτουν από ένα ζεύγος και ο αποστολέας χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Η λειτουργία του αλγορίθμου διαχωρίζεται σε 4 βασικά στάδια:

1. Παραγωγή κλειδιών: Είναι το στάδιο δημιουργίας του ζεύγους των κλειδιών. Ιδιαίτερα σημαντική είναι η κατάλληλη επιλογή των 2 πρώτων αριθμών που θα χρησιμοποιηθούν.
2. Διανομή κλειδιών: Σε αυτό το στάδιο, το δημόσιο κλειδί του παραλήπτη μεταδίδεται στον αποστολέα μέσα από ένα αξιόπιστο αν και όχι απαραίτητα ασφαλές μέσο. Το ιδιωτικό κλειδί του παραλήπτη δεν αποκαλύπτεται ποτέ, καθώς θα χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος.
3. Κρυπτογράφηση: Το μήνυμα M κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και παράγεται ένα κρυπτοκείμενο C. Αξίζει να σημειωθεί πως το μήκος τόσο του αρχικού κειμένου όσο και του κρυπτοκειμένου σε bits, εξ ορισμού δε γίνεται να ξεπεράσουν τον αριθμό N.
4. Αποκρυπτογράφηση: Ο παραλήπτης χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το C και στο τέλος πρέπει να έχει τα χέρια του το αρχικό μήνυμα M.

Οι μαθηματικές πράξεις που πραγματοποιούνται κατά την εκτέλεση του αλγορίθμου έχουν υψηλό υπολογιστικό κόστος καθώς περιλαμβάνουν αριθμούς πολύ μεγάλου μεγέθους, επομένως είναι απαραίτητο να ενσωματωθούν οι μέγιστες βελτιστοποιήσεις προκειμένου να έχει πρακτική εφαρμογή. Αναφέρονται επιγραμματικά ορισμένες από τις πιο βασικές τεχνικές που χρησιμοποιούνται για να επιταχύνουν τη διαδικασία:

- Αλγόριθμος square-and-multiply: Αυτή η τεχνική αντιμετωπίζει το πρόβλημα της ύψωσης εκθέτη σε δύναμη, μειώνοντας δραστικά τον αριθμό των πράξεων που χρειάζονται για τον υπολογισμό ενός μεγάλου εκθέτη.
- Encryption with Short Public Exponent: Η χρήση ενός μικρού δημόσιου εκθέτη e επιταχύνει δραστικά τη διαδικασία κρυπτογράφησης, χωρίς να μειώνει την ασφάλεια του αλγορίθμου.
- Decryption with Chinese Remainder Theorem(CRT): Χρησιμοποιώντας μια μέθοδο βασισμένη στο CRT, η αποκρυπτογράφηση γίνεται αποδοτικά χωρίς να χρειάζεται να μειωθεί το μήκος του ιδιωτικού κλειδιού, κάτι που θα το καθιστούσε λιγότερο ασφαλές.

Ο βασικός αλγόριθμος RSA είναι ευάλωτος σε επιθέσεις επιλεγμένου κρυπτοκειμένου(Chosen Ciphertext Attacks-CCA). Σε αυτήν την τεχνική, ο επιτιθέμενος επιλέγει κρυπτοκείμενα για τα οποία μπορεί να μάθει το αρχικό μήνυμα και χρησιμοποιώντας κομμάτια τους και τις ιδιότητες του αλγορίθμου μπορεί να εξάγει χρήσιμες πληροφορίες για άλλα μηνύματα. Αυτού του είδους οι επιθέσεις μπορούν να αντιμετωπιστούν με συμπλήρωση(padding), με πιο διαδεδομένη την τεχνική βέλτιστης συμπλήρωσης ασύμμετρης κρυπτογράφησης(Optimal Assymetric Encryption Padding-OAEP) η οποία περιγράφεται και στο πρότυπο PKCS#1.

Όπως προαναφέρθηκε, ο RSA, και γενικά οι ασύμμετροι αλγόριθμοι, είναι ένας υπολογιστικά απαιτητικός αλγόριθμος, που απαιτεί τη χρήση σημαντικής επεξεργαστικής ισχύος για να έχει ικανοποιητική επίδοση. Με την συνεχή βελτίωση του υλικού των υπολογιστών, οι RSA υλοποιήσεις έχουν επιτύχει ταχύτερες επιδόσεις αλλά και πάλι είναι έως και 1000 φορές πιο αργές από τις συμμετρικές μεθόδους. Για αυτό το λόγο, στην πράξη χρησιμοποιείται ένας συνδυασμός και των 2 με τον RSA να είναι υπεύθυνος για την κρυπτογράφηση ενός κλειδιού το οποίο στη συνέχεια θα χρησιμοποιηθεί από έναν συμμετρικό αλγόριθμο, π.χ. AES, για την προστασία του κυρίως όγκου των δεδομένων. Μια αντίστοιχη τεχνική εφαρμόστηκε και σε αυτήν την έρευνα, καθώς η ταχύτητα κρυπτογράφησης/αποκρυπτογράφησης είναι ζωτικής σημασίας στην επικοινωνία των οχημάτων.

4.2.3 ECC(Elliptic Curve Cryptography)

Η κρυπτογραφία ελλειπτικών καμπύλων αποτελεί μια νεότερη κατηγορία αλγορίθμων δημοσίου κλειδιού, η οποία ξεκίνησε να μελετάται από τη δεκαετία του 1980. Η ακριβής μαθηματική θεμελίωση της μεθόδου ξεφεύγει από τους σκοπούς της παρούσας εργασίας, οπότε θα αναφερθούμε κυρίως στις εφαρμογές της και στα πλεονεκτήματα έναντι του RSA.

Το πιο ελκυστικό χαρακτηριστικό αυτής της μεθόδου είναι πως υπόσχεται ασφάλεια με σημαντικά μικρότερο μήκος κλειδιού έναντι του RSA, επομένως μειώνεται ο επεξεργαστικός φόρτος, η κατανάλωση ενέργειας και ο απαιτούμενος αποθηκευτικός χώρος. Σύμφωνα με τον παρακάτω πίνακα, το απαιτούμενο μήκος κλειδιού για συμμετρική ασφάλεια 128 bits σε ECC είναι 12 φορές μικρότερο από το αντίστοιχο του RSA.

Symmetric(bits)	ECC(bits)	RSA(bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Πίνακας 2: Σύγκριση μήκους κλειδιών ECC και RSA

Η ECC στηρίζεται πάνω σε ένα σύνολο από αυθαίρετες πράξεις πάνω στα σημεία των καμπύλων αυτών, οι οποίες αναφέρονται ως πρόσθεση σημείου(point addition) και διπλασιασμός σημείου(point doubling). Η ασφάλεια του σχήματος βασίζεται στο λεγόμενο πρόβλημα διακριτού λογαρίθμου ελλειπτικής καμπύλης(elliptic curve discrete logarithm problem – ECDLP), το οποίο υποστηρίζει πως δεδομένων 2 σημείων A,B είναι δύσκολο να βρεθεί ένας θετικός ακέραιος k τέτοιος ώστε kA = B. Σε αυτήν την περίπτωση το k αντιστοιχεί στο πόσες φορές έχει προστεθεί το σημείο A στον εαυτό του και αποτελεί το ιδιωτικό κλειδί του σχήματος, ενώ οι συντεταγμένες του σημείου B αποτελούν το δημόσιο κλειδί. Ένα μειονέκτημα της ECC είναι ότι δεν παρέχουν όλες οι καμπύλες την ίδια ασφάλεια, καθώς κάποιες οικογένειες παρουσιάζουν εγγενείς αδυναμίες(π.χ. supersingular curves), και για αυτό το λόγο χρησιμοποιούνται κυρίως προτυποποιημένες καμπύλες σε πρακτικές εφαρμογές.

Οι κυριότερες εφαρμογές της ECC βρίσκονται στην ανταλλαγή κλειδιών και στις ψηφιακές υπογραφές, με τους αλγορίθμους ECDH και ECDSA αντίστοιχα. Ο ECDH(Elliptic Curve Diffie Helman) είναι ανάλογος με το συμβατικό αλγόριθμο Diffie-Helman, μόνο που χρησιμοποιεί τις συντεταγμένες των σημείων για να παράξει το κοινό μυστικό που μπορεί στη συνέχεια να χρησιμοποιηθεί για συμμετρική κρυπτογράφηση. Αν έχει επιλεγεί μια ασφαλής καμπύλη, τότε οι πιο αποτελεσματικοί αναλυτικοί αλγόριθμοι επίθεσης που μπορούν να χρησιμοποιηθούν είναι αυτοί που λύνουν το πρόβλημα των διακριτών λογαρίθμων, το οποίο μέχρι στιγμής θεωρείται υπολογιστικά δύσκολο, επομένως το σπάσιμο του ECDH θεωρείται υπολογιστικά ανέφικτο. Αντίστοιχα, ο ECDSA(Elliptic Curve Digital Signature Algorithm) εφαρμόζει τη βασική διαδικασία του DSA(παραγωγή κλειδιών, υπογραφή, επαλήθευση) χρησιμοποιώντας αριθμητική ελλειπτικών καμπύλων για να κατασκευάσει το πρόβλημα διακριτού λογαρίθμου. Με αυτόν τον τρόπο επιτυγχάνει υψηλή επίδοση με μειωμένο μέγεθος υπογραφής καθώς χρησιμοποιείται μικρότερο μήκος κλειδιού από ότι στον RSA.

Συγκριτικά με τον RSA, η ECC έχει έναν πολύ μικρότερο αριθμό από υλοποιήσεις για εφαρμογές. Αυτό οφείλεται σε ιστορικούς και νομικούς λόγους κυρίως, καθώς πέρα από το γεγονός ότι είναι 10 χρόνια νεότερη από το RSA υπάρχουν πολλές εν ενεργεία πατέντες σε ECC υλοποιήσεις, οι οποίες περιορίζουν νομικά την ανεξάρτητη ανάπτυξη υλοποιήσεων. Παρόλα αυτά, η ECC θεωρείται η κύρια μέθοδος κρυπτογράφησης δημοσίου κλειδιού σε ενσωματωμένες συσκευές, όπου η μικρότερη κατανάλωση αποθηκευτικού χώρου είναι ζωτικής σημασίας[34].

4.2.4 NTRU

Υπάρχει ένα είδος επίθεσης στην οποία είναι ευάλωτοι όλοι οι αλγόριθμοι που βασίζονται στο πρόβλημα της παραγοντοποίησης ακεραίων(RSA) ή στο πρόβλημα εύρεσης του διακριτού λογαρίθμου(ECC): επίθεση με χρήση αλγορίθμων κβαντικού υπολογισμού(Shor's, Grovel's, etc.) οι οποίοι είναι ικανοί να λύσουν τα παραπάνω προβλήματα σε πολυωνυμικό χρόνο, καθιστώντας τα μη ασφαλή. Μέχρι στιγμής, δεν έχει αναπτυχθεί κάποιος κβαντικός υπολογιστής ικανός αρκετά ώστε να λύσει αυτά τα προβλήματα, όμως υπάρχει ένα συνεχές ερευνητικό ενδιαφέρον σε αυτόν τον τομέα και αναμένεται στο άμεσο μέλλον να υπάρξουν σημαντικές εξελίξεις. Προς αυτήν την κατεύθυνση, οι Hoffstein, Pipher και Silverman[35] ανέπτυξαν το 1996 το NTRU κρυπτοσύστημα το οποίο στηρίζεται στην εύρεση διανυσμάτων σε διατεταγμένες ομάδες(Shortest/Closest Vector Problems in Lattices). Οι αλγόριθμοι που είναι βασισμένοι στις διατεταγμένες ομάδες θεωρούνται ασφαλείς απέναντι σε κβαντικούς υπολογιστές, καθώς αυτού του είδους τα προβλήματα θεωρούνται NP-δύσκολα και δεν έχει αναπτυχθεί ακόμα κάποιος αποδοτικός κβαντικός αλγόριθμος που να τα επιλύει.

Η κρυπτογράφηση NTRU προσφέρει υψηλότερες επιδόσεις τόσο από τον RSA όσο και από την ECC για το ίδιο επίπεδο ασφαλείας. Σύμφωνα με έρευνες[36], η NTRU παρουσιάζει μεγαλύτερη ταχύτητα στην παραγωγή κλειδιών, στην κρυπτογράφηση και στην αποκρυπτογράφηση. Υπάρχουν 2 βασικές υλοποιήσεις: η NTRUEncrypt που προσφέρει κρυπτογράφηση/αποκρυπτογράφηση και η NTRUSign που προσφέρει ψηφιακές υπογραφές. Το βασικότερο μειονέκτημα που παρουσιάζει αυτή η τεχνική, σε σχέση με την ECC κυρίως, είναι ότι παράγονται κλειδιά μεγαλύτερου μεγέθους με μέγεθος συγκρίσιμο με του RSA. Ένας ακόμα παράγοντας που επιβράδυνε την ευρεία επιθεώρηση και εφαρμογή αυτής της μεθόδου είναι το νομικό καθεστώς υπό το οποίο βρισκόταν, καθώς μέχρι το 2011 δεν είχαν αναπτυχθεί υλοποιήσεις ανοιχτού κώδικα και η εταιρεία που κατέχει τα δικαιώματα ελευθέρωσε μια υλοποίηση κάτω από την άδεια GPLv2 μόλις το 2013. Στα επόμενα χρόνια, αναμένεται να υπάρξουν περισσότερες υλοποιήσεις βασισμένες σε αυτήν τη μέθοδο. Αξίζει επίσης να σημειωθεί πως ενώ η NTRUEncrypt έχει γίνει ενσωματωθεί στο πρότυπο IEEE P1363.1 και θεωρείται ευρέως αποδεκτή, η NTRUSign αντίθετα δεν έχει προτυποποιηθεί, και μάλιστα υπάρχουν γνωστές αποδοτικές επιθέσεις στην ασφάλειά της με πιο πρόσφατη από τους Ducas και Nguyen το 2012[37]. Για αυτόν το λόγο δεν συνίσταται η χρήση της NTRUSign για πρακτικές εφαρμογές.

4.3 Μετρικές αξιολόγησης

4.3.1 Εντροπία

Μια από τις πιο συμβατικές και ευρέως διαδεδομένες μετρικές που χρησιμοποιούνται για την αξιολόγηση της ιδιωτικότητας θέσης είναι η εντροπία ιδιωτικότητας θέσης. Οι Beresford και Stajano[12] το 2003 πρότειναν ένα μοντέλο μέτρησης της ιδιωτικότητας θέσης βασισμένο στην αβεβαιότητα εντοπισμού ενός οχήματος μέσα στο σύστημα. Όρισαν ως σύνολο ανωνυμίας(anonymity set) το πλήθος των οχημάτων που βρίσκονταν ταυτόχρονα σε μια Ζώνη Μίξης και βασισμένοι στις παρατηρήσεις των Serjantov κ.α.[38] για την κατανομή της

πιθανότητας εντοπισμού ενός στόχου μέσα σε αυτές τις περιοχές κατέληξαν στη γνωστή σχέση του Shannon[39]:

$$E = -\sum_{i=1}^{N} p_i \log p_i \quad (4.3.1)$$

Όπου Ε είναι η εντροπία σε bits του συστήματος, δηλαδή πόσα bits πληροφορίας χρειάζεται ένας επιτιθέμενος για να εντοπίσει ένα συγκεκριμένο στόχο, p η πιθανότητα της σωστής ταυτοποίηση του στόχου i και N ο συνολικός αριθμός των οχημάτων. Ουσιαστικά, αν η εντροπία είναι X bits, τότε 2^X οχήματα είναι μη διακριτά μεταξύ τους[40]

Όσο μεγαλύτερη είναι η εντροπία, τόσο μεγαλύτερη είναι η αβεβαιότητα με την οποία ένας επιτιθέμενος μπορεί να συνδέσει την ταυτότητα ενός οχήματος τη στιγμή τ-1 με την ταυτότητά του τη στιγμή τ. Επομένως, είναι επιθυμητό κατά τη λειτουργία ενός συστήματος οχημάτων να διατηρείται υψηλή η εντροπία του προκειμένου να επιτυγχάνεται η μέγιστη ιδιωτικότητα θέσης. Έχουν δημοσιευθεί έρευνες στις οποίες ο βασικός σκοπός των οχημάτων είναι να αυξήσουν την εντροπία τους και λειτουργούν με αυτήν τη νοοτροπία. Στο [26] τα οχήματα μετρούν ενεργά την εντροπία τους και αποφασίζουν για την ανταλλαγή ή όχι ψευδωνύμων με γνώμονα την αύξησή της. Όπως προκύπτει από τον παραπάνω τύπο, στην περίπτωση που ένα όχημα αποκαλυφθεί η εντροπία του μηδενίζεται με αποτέλεσμα να επιδιώξει συνεχόμενες ανταλλαγές προκειμένου να την επαναφέρει σε αποδεκτά επίπεδα.

Δύο είναι οι παράγοντες που επηρεάζουν αυξητικά την εντροπία: 1) ο αριθμός των οχημάτων που κινούνται μέσα στη ζώνη και 2) η ομοιότητα της κατανομής της πιθανότητας επιτυχημένου εντοπισμού με την ομοιόμορφη κατανομή, το οποίο εξαρτάται από την ακρίβεια των δεδομένων που διαθέτει ο επιτιθέμενος και τους πόρους του[24]. Από τα παραπάνω προκύπτει ότι η αύξηση της εντροπίας δε βρίσκεται στον άμεσο έλεγχο των οχημάτων, επομένως ο υπολογισμός της μέσης εντροπίας μιας Ζώνης Μίξης για ένα χρονικό διάστημα είναι χρήσιμος για την αξιολόγηση της αποτελεσματικότητας της εν λόγω ζώνης στην παροχή ιδιωτικότητας. Η μέση εντροπία ενός συστήματος για n διαδοχικά χρονικά διαστήματα υπολογίζεται ως εξής:

$$E[H(i)] = \frac{1}{n}\sum_{\upsilon=1}^{n} H_{T_\upsilon}(i) \quad (4.3.2)$$

4.3.2 Κρυπτογραφικές μετρικές

4.3.2.1 Μήκος κλειδιών

Η πιο συνηθισμένη μετρική που έχει συνδεθεί με τους αλγορίθμους κρυπτογράφησης είναι το μήκος των κλειδιών που χρησιμοποιούνται. Το μήκος , στην πλειονότητα των περιπτώσεων μετριέται σε bits και πολλές φορές είναι συνώνυμο με το επίπεδο ασφαλείας που προσφέρει ο εκάστοτε αλγόριθμος συγκρίνοντας το με αλγορίθμους συμμετρικής κρυπτογράφησης που έχουν ίδιο μέγεθος κλειδιού. Δηλαδή, έχει επικρατήσει η ασφάλεια που

προσφέρει ένας αλγόριθμος να καθορίζεται από το μέγεθος του κλειδιού του, συγκρινόμενο με την αντίστοιχη ασφάλεια που προσφέρει το ίδιο μέγεθος κλειδιού ενός προτυποποιημένου συμμετρικού αλγορίθμου, πχ. AES. Το μήκος του κλειδιού ή των κλειδιών εξαρτάται άμεσα από τη φύση του αλγορίθμου. Τα ποσά της ασφάλειας και του μήκους κλειδιού δεν είναι απαραιτήτως ανάλογα, δηλαδή δεν είναι αναγκαίο πως μεγαλύτερο μήκος κλειδιού συνεπάγεται μεγαλύτερη ασφάλεια. Ακόμα, λόγω της ανάγκης των σύγχρονων εφαρμογών για μειωμένο αποθηκευτικό χώρο, χαμηλή κατανάλωση ισχύος και ταχύτητα επεξεργασίας είναι επιθυμητό ως και αναγκαίο σε κάποιες περιπτώσεις το ελάχιστο δυνατό μήκος κλειδιού με τη μέγιστη δυνατή ασφάλεια, πχ. ενσωματωμένα συστήματα οχημάτων.

4.3.2.2 Χρόνος κρυπτογραφίας

Μια θεμελιώδης απαίτηση στα πρωτόκολλα επικοινωνίας μεταξύ οχημάτων είναι η ταχύτητα απόκρισης. Αυτό οφείλεται στην ίδια τη φύση του αντικειμένου, καθώς ακόμα και η ελάχιστη καθυστέρηση στη λήψη, επεξεργασία και απάντηση ενός μηνύματος μπορεί να προκαλέσει σημαντικά προβλήματα, από την υποβάθμιση των υπηρεσιών βάσει τοποθεσίας(LBS) στην δημιουργία κυκλοφοριακής συμφόρησης και στην πρόκληση φυσικών ατυχημάτων με κίνδυνο της ανθρώπινης ζωής. Από τα παραπάνω λοιπόν είναι φανερό πως όλα τα στάδια της επικοινωνίας θα πρέπει να είναι βελτιστοποιημένα για τη λειτουργία τους στο μικρότερο δυνατό χρονικό διάστημα.

Στην παρούσα εργασία επικεντρωνόμαστε στη χρονική επίδραση των διάφορων τεχνικών κρυπτογραφίας στο σύστημα, καθώς αποτελούν το πιο κοστοβόρο στοιχείο της επικοινωνίας. Οι μετρικές που μελετάμε είναι οι παρακάτω:

1. Χρόνος παραγωγής κλειδιών.
2. Χρόνος κρυπτογράφησης/αποκρυπτογράφησης
3. Χρόνος υπογραφών/επαλήθευσης

4.3.2.3 Χρόνος παραγωγής κλειδιών

Ως χρόνο παραγωγής κλειδιών ορίζουμε το χρόνο που χρειάζεται προκειμένου να δημιουργηθούν και να αρχικοποιηθούν τα απαραίτητα κλειδιά κρυπτογράφησης που χρησιμοποιεί ο κάθε αλγόριθμος. Στην περίπτωση που ένα σύστημα χρησιμοποιεί στατικά κλειδιά, δηλαδή παράγονται μια φορά και παραμένουν σταθερά κατά τη λειτουργία του συστήματος, αυτή η παράμετρος θα μπορούσε να ενσωματωθεί στη συνολική αρχικοποίηση του συστήματος, όμως στην πλειονότητα των περιπτώσεων γίνεται δυναμική χρήση κλειδιών για επίτευξη μεγαλύτερης ασφάλειας. Σε αυτές τις περιπτώσεις, κάθε φορά που δημιουργείται ένα νέο κλειδί πρέπει να μετριέται ο χρόνος του, π.χ. κατά την έναρξη μιας καινούριας επικοινωνίας. Είναι απαραίτητο λοιπόν να υπάρχει ένας δυναμικός τρόπος μέτρησης του χρόνου που χρειάζεται για να γίνουν διαθέσιμα τα κλειδιά προς χρήση, με σκοπό την όσο το δυνατό γρηγορότερη παραγωγή τους για αποφυγή bottlenecks. Στις προσομοιώσεις μας, για τη μέτρηση αυτού του χρόνου χρησιμοποιούμε συναρτήσεις που αντλούν πληροφορίες απευθείας από τα

ρολόγια του υλικού και μετράνε το χρόνο εκτέλεσης του κώδικα που αναλαμβάνει την παραγωγή των κλειδιών.

Αυτός ο χρόνος εξαρτάται άμεσα από τη φύση του αλγορίθμου, το μέγεθος του κλειδιού, και από το υλικό το οποίο παρέχει τις κρυπτογραφικές δυνατότητες. Στην πράξη, για να επιτευχθούν οι ταχύτεροι δυνατοί χρόνοι χρησιμοποιείται εξειδικευμένο υλικό για την εκτέλεση των απαραίτητων κρυπτογραφικών πράξεων με τη μέγιστη ταχύτητα.

4.3.2.3 Χρόνος κρυπτογράφησης/αποκρυπτογράφησης

Αυτή η μετρική είναι μια από τις ευκολότερα κατανοητές μετρικές που χρησιμοποιούνται στην πρακτική αξιολόγηση της επίδοσης των διάφορων κρυπτογραφικών μοντέλων. Στην περίπτωση της κρυπτογράφησης είναι ο χρόνος που χρειάζεται για την παραγωγή ενός κρυπτοκειμένου από ένα μήνυμα, και αντίστροφα στην αποκρυπτογράφηση ο χρόνος που χρειάζεται για την εξαγωγή του αρχικού μηνύματος από το κρυπτοκείμενο. Είναι άρρηκτα συνδεδεμένη με τον εκάστοτε αλγόριθμο που χρησιμοποιείται, ωστόσο υπάρχουν αρκετές άλλες παράμετροι που επηρεάζουν την επίδοση, όπως το υλικό που χρησιμοποιείται, η υλοποίηση του αλγορίθμου κ.α.

4.3.2.4 Χρόνος υπογραφής/επαλήθευσης

Αυτή η μετρική αναφέρεται στις λειτουργίες ψηφιακής υπογραφής. Στην παρούσα εργασία, επικεντρωθήκαμε στη μέτρηση δύο συγκεκριμένων χρονικών περιόδων: 1)το χρόνο που χρειάζεται για να δημιουργηθεί η υπογραφή ενός μηνύματος από τον αποστολέα και 2) το χρόνο που χρειάζεται ο παραλήπτης για να επαληθεύσει την εγκυρότητα του μηνύματος που έλαβε. Καθώς η αυθεντικοποίηση των μηνυμάτων είναι ζωτικής σημασίας προκειμένου να διασφαλιστεί η ασφάλεια της επικοινωνίας, η βελτιστοποίηση του χρόνου που απαιτείται για αυτήν τη διαδικασία είναι απαραίτητη.

4.3.3 Μέγεθος μηνυμάτων

Αυτή η μετρική χρησιμοποιείται για να δώσει μια εκτίμηση του όγκου της πληροφορίας που κινείται μεταξύ των μελών του δικτύου. Κάθε διαφορετικός τύπος μηνύματος έχει διαφορετικό μέγεθος και αυτό πρέπει να μπορεί να αποτυπώνεται προκειμένου να προβλεφθεί μια πιθανή συμφόρηση του δικτύου. Στις προσομοιώσεις μας μετράμε το συνολικό μέγεθος του πακέτου σε bytes που παραλαμβάνει ένας κόμβος.

4.3.4 Κατανάλωση ενέργειας

Αυτή η μετρική χρησιμοποιείται προκειμένου να δώσει μια αίσθηση του φόρτου που θέτουν οι διάφορες κρυπτογραφικές μέθοδοι πάνω στα ενσωματωμένα συστήματα των οχημάτων. Είναι μια ενδιαφέρουσα μετρική, καθώς ένας μηχανισμός με υψηλή κατανάλωση ισχύος μπορεί να οδηγήσει σε πρόωρη εξάντληση των πόρων του οχήματος και κατά συνέπεια σε απώλεια επικοινωνίας. Στις προσομοιώσεις μετράμε την ενέργεια που καταναλώθηκε κατά τη

διάρκεια επεξεργασίας ενός μηνύματος, χρησιμοποιώντας την υποδομή που παρέχεται από το NS-3.

Κεφάλαιο 5: Περιγραφή του προβλήματος – Μοντελοποίηση

Στο κεφάλαιο αυτό παρουσίαζεται το πρόβλημα το οποίο πραγματεύεται η παρούσα διπλωματική εργασία, το μοντέλο δικτύου που χρησιμοποιήθηκε, όπως επίσης και οι διαφορετικοί τύποι επιτιθέμενων που λήφθηκαν υπόψην.

5.1 Παρουσίαση του προβλήματος

Η ραγδαία ανάπτυξη του IoT τα τελευταία χρόνια δεν άφησε ανεπηρέαστα τα οχήματα. Ολοένα και περισσότερα οχήματα με δυνατότητα σύνδεσης στο διαδίκτυο κυκλοφορούν στους δρόμους, αξιοποιώντας ένα αυξανόμενο σύνολο από τεχνολογίες δικτύων, όπως η μηχανική μάθηση και η τεχνητή νοημοσύνη, προκειμένου να ενσωματώσουν αποδοτικά τις συνεργαζόμενες οντότητες(οχήματα, ανθρώπους, αντικείμενα και περιβάλλον). Αυτό το φαινόμενο έχει οδηγήσει στην εξέλιξη των δικτύων οχημάτων από τα VANETs στο λεγόμενο IoV, του οποίου οι αυξημένες επεξεργαστικές ικανότητες και η διευρυμένη κλίμακα εφαρμογής ελκύουν πλέον το ερευνητικό και εμπορικό ενδιαφέρον για την ανάπτυξη εφαρμογών και υπηρεσιών.

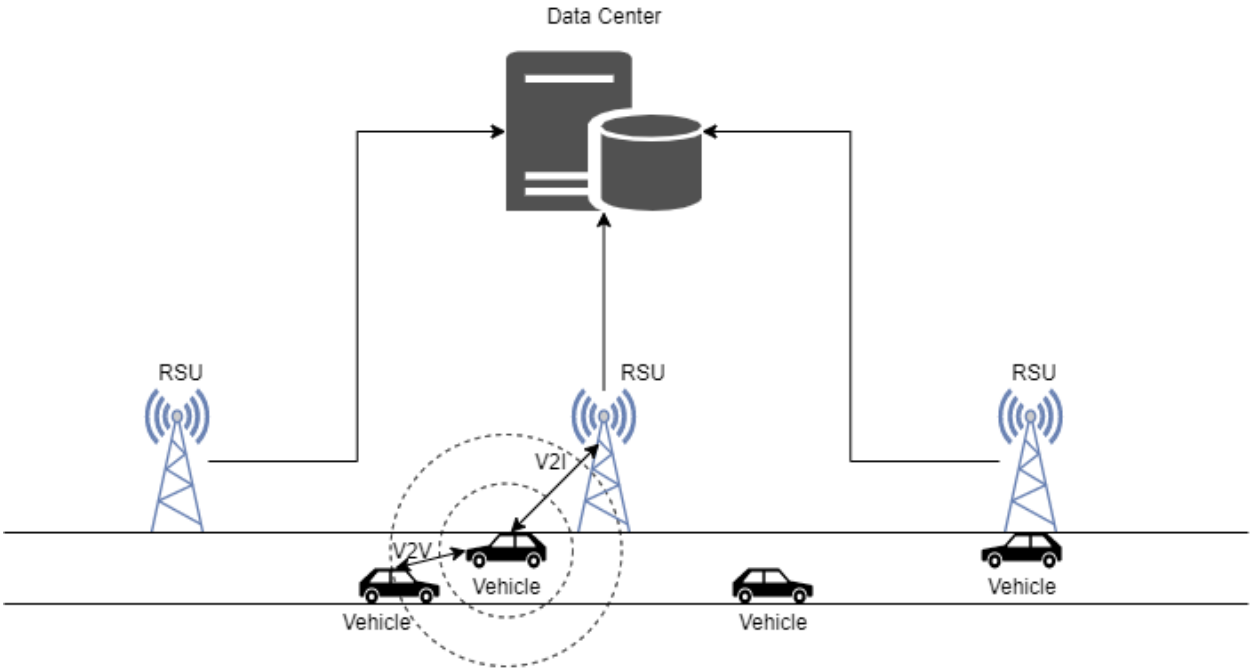
Αυτή η ανάπτυξη, όπως σε κάθε τεχνολογία με άμεσο αντίκτυπο στο γενικό πληθυσμό, έχει φέρει στο προσκήνιο τα ζητήματα της ασφάλειας και της ιδιωτικότητας. Το ρίσκο από την παραβίαση ασφαλείας σε ένα δίκτυο οχημάτων είναι εξ' ορισμού υψηλό, καθώς επηρεάζονται άμεσα ανθρώπινες ζωές. Έτσι, ένα σημαντικό μέρος της έρευνας στον τομέα τα τελευταία χρόνια έχει αφιερωθεί στην ανάπτυξη μεθόδων εξασφάλισης της ασφάλειας αυτών των δικτύων, τόσο σε φυσικό επίπεδο όσο και σε επίπεδο επικοινωνίας, με χρήση κρυπτογραφικών μεθόδων, μοντέλων επαλήθευσης και κοινωνικών δικτύων. Όμως, πέρα από την ασφάλεια, μια εξίσου σημαντική απαίτηση που υφίσταται στο IoV είναι αυτή της ιδιωτικότητας. Αυτή η απαίτηση γίνεται πιο άμεση από τη στροφή της τεχνολογίας προς την παραγωγή και αξιοποίηση δεδομένων(Big Data), καθώς δεδομένα τα οποία μέχρι πρότινος δεν είχαν κάποια αξία πλέον χρησιμοποιούνται και μπορούν να εξάγουν συμπεράσματα τα οποία παραβιάζουν την ιδιωτικότητα των χρηστών. Το πιο απτό παράδειγμα είναι η ιδιωτικότητα θέσης, καθώς είναι δυνατόν από τα μηνύματα ασφαλείας και μόνο που στέλνει ένα όχημα να ανακατασκευαστεί η πορεία του και να βρεθούν πληροφορίες για τον ιδιοκτήτη όπως η κατοικία του, ο χώρος εργασίας, σημεία κτλ. Για την προστασία της ιδιωτικότητας των χρηστών έχουν προταθεί διάφορες μέθοδοι, όπως αναφέρθηκε στο κεφάλαιο 3, και συνεχίζουν να εξελισσόνται ακολουθώντας την εξέλιξη του IoV. Επομένως, υπάρχει σημαντικό ενδιαφέρον στην εύρεση όσο το δυνατόν καλύτερων και αποδοτικότερων τεχνικών ιδιωτικότητας, προκειμένου το IoV να εδραιωθεί στην καθημερινότητα του μέλλοντος.

5.2 Μοντέλο Δικτύου

Στην παρούσα εργασία θεωρούμε ένα δίκτυο οχημάτων τοποθετημένο σε ένα αστικό κέντρο, το οποίο απαρτίζεται από οχήματα, μονάδες υποδομής και ένα κέντρο επεξεργασίας δεδομένων. Στη συνέχεια εξηγούνται περαιτέρω τα στοιχεία αυτά:

1. Όχημα: Περιγράφει ένα τυπικό όχημα που κινείται στους δρόμους μιας πόλης. Κάθε όχημα είναι εφοδιασμένο με ειδικό εξοπλισμό για την επικοινωνία με τα άλλα οχήματα(V2V) αλλά και τις μονάδες υποδομής(V2I). Αυτή η μονάδα ονομάζεται On-Board Unit(OBU) και προσφέρει τη δυνατότητα ασύρματης επικοινωνίας, στη συγκεκριμένη εργασία χρησιμοποιώντας WiFi 802.11p. Για την ασφάλεια του συστήματος, κάθε όχημα μεταδίδει περιοδικά, κάθε 200-300ms, ένα σύνολο πληροφοριών(θέση, ταχύτητα, επιτάχυνση, timestamp) σε όλους τους κόμβους του δικτύου που βρίσκονται γύρω του. Σε αυτήν την επικοινωνία χρησιμοποιεί ένα προκαθορισμένο ψευδώνυμο αντί της πραγματικής του ταυτότητας, και ο στόχος είναι μέσω αυτού να προστατεύσει την ιδιωτικότητα θέσης του.

   Για την ασφάλεια της επικοινωνίας, η OBU θα πρέπει να διαθέτει 2 συγκεκριμένα υλικά στοιχεία: ένα καταγραφέα δεδομένων(Event Data Recorder–EDR) και μια αμετάβλητη συσκευή(Tamper-Proof Device–TPD). Το EDR στην ουσία αποθηκεύει σημαντικές πληροφορίες σε περίπτωση κρίσιμων συμβάντων, σαν ένα «μαύρο κουτί» αεροπλάνου, και μπορεί να επεκταθεί για την καταγραφή των μηνυμάτων ασφαλείας ενός οχήματος. Το TPD από την άλλη, προσφέρει ένα ασφαλή χώρο αποθήκευσης των κρυπτογραφικών διαπιστευτηρίων του οχήματος(κλειδιά, πιστοποιητικά, υπογραφές) και ταυτόχρονα αναλαμβάνει να εκτελέσει την κρυπτογραφική επεξεργασία των μηνυμάτων. Το TPD εξασφαλίζει την ιδιότητα του accountability εφόσον τα κλειδιά είναι δεμένα με την ταυτότητα του οχήματος. Για αυτόν το λόγο, το TPD πρέπει να είναι όσο το δυνατόν πιο ανεξάρτητο από το περιβάλλον, απαιτώντας ξεχωριστούς πόρους όπως δικό του ρολόι και μπαταρία προκειμένου να εξασφαλιστεί η ομαλή λειτουργία του.
2. Μονάδα Υποδομής(RSU): Είναι μια στατική μονάδα επικοινωνίας που τοποθετείται πάνω στο οδικό δίκτυο. Έχει ένα σύνολο από αρμοδιότητες, όπως να παρέχει κάλυψη δικτύου στα οχήματα, να συλλέγει πληροφορίες από αυτά και να τις μεταφέρει στο κέντρο επεξεργασίας, να προωθεί μηνύματα σε άλλες RSUs στο δίκτυο και να μεταφέρει μηνύματα από την υποδομή στα οχήματα(ειδοποιήσεις ατυχημάτων κτλ.). Για οικονομικούς λόγους τα RSUs τοποθετούνται αραιά μέσα σε ένα οδικό δίκτυο, το οποίο έχει ως αποτέλεσμα στην πραγματικότητα να μην παρέχουν κάλυψη σε όλη την έκταση του δικτύου. Κάθε RSU έχει τη δυνατότητα ασύρματης επικοινωνίας μέσω WiFi με τα οχήματα που βρίσκονται εντός της εμβέλειάς της, και παράλληλα είναι συνδεδεμένη ενσύρματα μέσω Ethernet με τις υπόλοιπες RSUs και το κέντρο επεξεργασίας.
3. Κέντρο επεξεργασίας δεδομένων(Data Center): Το κέντρο του δικτύου, υπεύθυνο για όλες τις αποφάσεις σχετικά με τη λειτουργία του. Απαρτίζεται από την Έμπιστη Αρχή(Register Authority-RA), το διακομιστή θέσης και τη βάση ψευδωνύμων. Η RA είναι συνήθως ένας έμπιστος φορέας υπό κυβερνητική δικαιοδοσία που αναλαμβάνει τη διαχείριση των ταυτοτήτων και διαπιστευτηρίων όλων των οχημάτων του δικτύου που είναι καταγεγραμμένα. Το κέντρο επεξεργασίας είναι ο μόνος αρμόδιος για την δημιουργία ψευδωνύμων και των αντίστοιχων διαπιστευτηρίων κατά απαίτηση των οχημάτων, καθώς επίσης και για την ανάκληση τους σε περίπτωση διαρροής ή επίθεσης.



Εικόνα 14: Μοντέλο Δικτύου

5.3 Μοντέλο Επιτιθέμενων

Στην παρούσα εργασία λαμβάνονται υπόψη οι παρακάτω τύποι επιτιθέμενων:

1. Καθολικός παθητικός επιτιθέμενος(Global Passive Adversary): Είναι ένας εξωτερικός κακόβουλος ωτακουστής ο οποίος έχει τη δυνατότητα να υποκλέψει μηνύματα κατά μήκος ολόκληρου του δικτύου και εν δυνάμει να παρακολουθήσει όλα τα οχήματα.
2. Τοπικός παθητικός επιτιθέμενος(Restricted Passive Adversary): Αυτός ο εξωτερικός επιτιθέμενος είναι περιορισμένος στο εύρος των RSUs για να μπορέσει να παρακολουθήσει την επικοινωνία, επομένως η περιοχή που απειλεί εξαρτάται από την απόσταση μεταξύ 2 διαδοχικών RSU και την εμβέλεια μετάδοσης των οχημάτων.
3. Εσωτερικός κατάσκοπος(Internal Betrayal Adversary): Αυτός είναι ένας πολύ επικίνδυνος τύπος εσωτερικού επιτιθέμενου, καθώς μεταμφιέζεται σε έγκυρο μέλος του δικτύου και συμμετέχει κανονικά στη λειτουργία του, με απώτερο σκοπό την απόκτηση και διαρροή χρήσιμων πληροφοριών για τα οχήματα. Πολύ συχνά συνεργάζεται με κάποιον από τους προηγούμενους τύπους επιτιθέμενων, έτσι ώστε αφού αποκτήσει πληροφορίες για έναν «στόχο» τις μεταδίδει στον εξωτερικό επιτιθέμενο με σκοπό να εντοπίσει και να ανακατασκευάσει την πορεία του οχήματος που παρακολουθείται.
4. Εσωτερικός ταραχοποιός(Internal Tricking Adversary): Αυτός ο εσωτερικός επιτιθέμενος σκοπεύει στη δημιουργία χάους μέσα στο δίκτυο και χρησιμοποιεί εσφαλμένα ψευδώνυμα ή μηνύματα για να το προκαλέσει.

Επιθέσεις στη φυσική υποδομή του δικτύου, παρότι ρεαλιστικές και πολλές φορές πολύ αποτελεσματικές, δε λαμβάνονται υπόψη στα πλαίσια της παρούσας εργασίας.

Κεφάλαιο 6: Λύση-Υλοποίηση

Στο κεφάλαιο αυτό αναλύεται η προτεινόμενη υλοποίηση που ακολουθήθηκε. Αρχικά, αναλύονται οι μέθοδοι ανταλλαγής και ενεργοποίησης ψευδωνύμων. Στη συνέχεια, παρουσιάζεται η μετρική αξιολόγησης του οφέλους ανταλλαγής. Έπειτα, αναλύονται οι προγραμματιστικές υλοποιήσεις των κρυπτογραφικών τεχνικών που χρησιμοποιήθηκαν, καθώς επίσης και η υλοποίηση του μοντέλου κατανάλωσης ενέργειας. Τέλος, παρουσιάζονται οι υλοποιήσεις του οδικού δικτύου, της κίνησης των οχημάτων και της επικοινωνίας αυτών.

6.1 Ανταλλαγή ψευδωνύμων

Στην καρδιά του σχήματος MixGroup βρίσκεται η ανταλλαγή ψευδωνύμων μεταξύ των οχημάτων, καθώς αυτή εξασφαλίζει την ιδιωτικότητα του συστήματος. Τα οχήματα ενός group έχουν τη δυνατότητα να ανταλλάξουν άμεσα τα ψευδώνυμά μεταξύ τους χωρίς τη διαμεσολάβηση κάποιας RSU, το οποίο επιτρέπει την ανταλλαγή και σε περιοχές που δεν καλύπτονται από την υποδομή. Στη συνέχεια, όταν παραστεί ανάγκη για τη χρήση αυτών των ψευδωνύμων, δηλαδή όταν ένα όχημα φύγει από την ομάδα, τότε το ενεργοποιεί με τη βοήθεια της ίδιας RSU που ενημερώνει για την έξοδό του.

Η διαδικασία ανταλλαγής αποτελείται από αρκετά βήματα. Αρχικά, η διαδικασία εκκινείται όταν ένας κατάλληλος αριθμός οχημάτων της ίδιας ομάδας βρίσκεται σε κοντινή απόσταση, όπου κοντινή απόσταση είναι η εμβέλεια των μηνυμάτων ασφαλείας, και υπάρχουν κάποια οχήματα που να θέλουν να αυξήσουν την ιδιωτικότητά τους. Κάθε τέτοιο όχημα εκπέμπει μια αίτηση αλλαγής ψευδωνύμου προς τα υπόλοιπα και περιμένει απάντηση. Ο παραλήπτης ενός τέτοιου μηνύματος εκτιμά τη δική του κατάσταση της ιδιωτικότητας μετά από μια πιθανή ανταλλαγή, και αν τη βρει θετική στέλνει προς ένα τυχαίο υποψήφιο μια πρόταση για ανταλλαγή. Στη συνέχεια, εγκαθίσταται μια επικοινωνία μεταξύ τους στην οποία ανταλλάσσουν τα απαραίτητα κλειδιά για την ανταλλαγή(Exchange keys) και ξεκινάνε την ανταλλαγή. Κατά τη διάρκεια της ανταλλαγής, κάθε μήνυμα ελέγχεται προς την εγκυρότητά του και παράγονται οι κατάλληλες υπογραφές σε κάθε βήμα με αποτέλεσμα στο τέλος να έχει εκτελεστεί η ανταλλαγή και να έχει δημιουργηθεί ένα αρχείο ανταλλαγής σε κάθε όχημα το οποίο θα χρησιμοποιηθεί στην ενεργοποίηση του νέου ψευδωνύμου. Συνολικά, η διαδικασία μπορεί να περιγραφεί με τον παρακάτω ψευδοκώδικα:

1: Το όχημα1 λαμβάνει μηνύματα ασφαλείας από N γείτονες
2: Αν (το όχημα1 θέλει ανταλλαγή)
3: όχημα1->γείτονες:
Αίτηση ανταλλαγής(PK_1,$Cert_1$, $Cert_G$,Timestamp)
4: Αλλιώς πήγαινε στο 1

5: Το όχημα2 λαμβάνει αιτήσεις ανταλλαγής
6: Το όχημα2 εκτιμά το όφελος ανταλλαγής μέσω της εντροπίας
7: Αν (μεταβολή εντροπίας > κατώφλι)
8: Το όχημα2 επιλέγει ένα τυχαίο όχημα που έκανε αίτηση(έστω το 1)
9: όχημα2->όχημα1:

$Encr_{o1}$(Πρόταση ανταλλαγής($Cert_2$,Sig[Cert],Timestamp))
10: Αλλιώς πήγαινε στο 1
11: Αν (όχημα1 θέλει ακόμα ανταλλαγή)
12: όχημα1->όχημα2:
$Encr_{02}$(Αποδοχή,στοιχεία ανταλλαγής,υπογραφή στοιχείων,Timestamp)
13: Αλλιώς πήγαινε στο 8
14: Ανταλλαγή κλειδιών ανταλλαγής(όχημα2, όχημα1)
15: Ανταλλαγή ψευδωνύμων(όχημα1, όχημα2)
16: Δημιουργία αρχείου ανταλλαγής(Record1, Record2)
17: Έλεγχος αρχείων ότι είναι πανομοιότυπα
18: Πήγαινε στο 1

6.2 Ενεργοποίηση ψευδωνύμου

Ένα όχημα μπορεί στη διάρκεια της κίνησής του μέσα στην ομάδα να πραγματοποιήσει πολλές ανταλλαγές ψευδωνύμων. Όμως, προτού μπορέσει να χρησιμοποιήσει το πιο πρόσφατο από αυτά στην επικοινωνία του, πρέπει να το ενεργοποιήσει. Αυτό σημαίνει να το διασταυρώσει με την αξιόπιστη αρχή(RA) και αν είναι έγκυρο μπορεί να το υιοθετήσει από αυτό το σημείο και πέρα όταν φύγει από την ομάδα. Σε αυτήν τη διαδικασία σημαντικό ρόλο παίζουν οι RSUs, καθώς αυτές είναι υπεύθυνες για τη μεταφορά της αίτησης ενεργοποίησης από το όχημα στο RA και αντίστοιχα της απάντησης του RA πίσω στο όχημα. Σε μορφή ψευδοκώδικα η διαδικασία αναπαριστάται ως εξής:

1: Το όχημα1 έχει πραγματοποιήσει N ανταλλαγές ψευδωνύμων
2: Το όχημα1 λαμβάνει σήμα από μια κοντινή RSU και αποφασίζει να ενεργοποιήσει το ψευδώνυμο πριν φύγει από την εμβέλειά της
3: όχημα1->RSU:
$Encr_{RA}$(Αίτηση ενεργοποίησης(δεδομένα οχήματος, δεδομένα ανταλλαγής))
4: RSU->RA: Προώθηση αιτήματος από όχημα1
5: Η RA επαληθεύει τα δεδομένα
6: Αν (έγκυρα δεδομένα)
7: RA->RSU:
$Encr_{01}$(Άδεια χρήσης ψευδωνύμου(αντίστοιχα κλειδιά))
8: RSU->όχημα1: Προώθηση απάντησης από RA
9: Αλλιώς ακύρωσε αυτά τα ψευδώνυμα σε όλο το δίκτυο

6.3 Αξιολόγηση οφέλους ανταλλαγής

Δεν είναι όλες οι ανταλλαγές θεμιτές για ένα όχημα καθώς, λαμβάνοντας υπόψιν τους εσωτερικούς επιτιθέμενους, υπάρχει ο κίνδυνος διαρροής των πληροφοριών του. Έτσι, κάθε όχημα είναι εφοδιασμένο με ένα μηχανισμό που του επιτρέπει να εκτιμά το όφελος που θα προσφέρει στην ιδιωτικότητά του κάθε ανταλλαγή και να αποφεύγει μη ιδανικές ανταλλαγές. Αυτός ο μηχανισμός κάνει χρήση της λεγόμενης *εντροπίας ψευδωνύμου*, η οποία στηρίζεται πάνω στην εντροπία που αναφέρθηκε στο κεφάλαιο 2 και ορίζεται αναλυτικά στο [26]. Παρακάτω αναγράφονται οι βασικές σχέσεις που χρησιμοποιήθηκαν στη παρούσα εργασία:

$$\Pr\{v_j \in V_{IA}\} = \frac{B}{N-1} \tag{6.3.1}$$

$$\Delta h = \sum_{i=1}^{B} \frac{\binom{B}{i}\binom{N-1}{N-1-i}}{\binom{N-1}{K-1}} \log_2(K-i) \tag{6.3.2}$$

$$H_{v_i}(k) = \begin{cases} 0, & v_j \in V_{IA} \\ H_{v_i}(k-1) + \Delta h, & v_j \notin V_{IA} \end{cases} \tag{6.3.3}$$

$$\Delta h > \frac{\Pr\{v_j \in V_{IA}\} H_{v_i}(k-1)}{1 - \Pr\{v_j \in V_{IA}\}} \tag{6.3.4}$$

Όπου:
N: ο συνολικός αριθμός των οχημάτων στο δίκτυο
B: ο συνολικός αριθμός των εσωτερικών επιτιθέμενων
v_i: Ένα όχημα i που βρίσκεται σε μια περιοχή ενδιαφέροντος
V_{IA}: Το σύνολο των οχημάτων που λειτουργούν ως εσωτερικοί επιτιθέμενοι
K: Το πλήθος των οχημάτων σε μια περιοχή ενδιαφέροντος
Δh: Η μεταβολή της εντροπίας ψευδωνύμου ενός οχήματος i
$H_{vi}(k)$: Η εντροπία του οχήματος i μετά από k ανταλλαγές ψευδωνύμων
$\Pr\{v_j \varepsilon V_{IA}\}$: Η πιθανότητα το όχημα v_i να ανήκει στο σύνολο V_{IA}, δηλαδή να είναι επιτιθέμενος

Οι παραπάνω σχέσεις υλοποιήθηκαν με το εξής πακέτο συναρτήσεων στη γλώσσα C/C++:

- gcd(u,v): Συνάρτηση που βρίσκει το μέγιστο κοινό διαιρέτη 2 ακεραίων.
- fast_comb(n,r): Συνάρτηση που βρίσκει το συνδυασμό (n,r) με χρήση gcd.
- tracking_prob(B,N): Συνάρτηση που υπολογίζει το $\Pr\{v_j \varepsilon V_{IA}\}$.
- entropy_change(B,N,K). Συνάρτηση που υπολογίζει το Δh.
- should_exchange(Δh,Hv_i,Pr): Συνάρτηση που αποφαίνεται αν πρέπει να γίνει ανταλλαγή.

Όπως φαίνεται από τη σχέση (2), στην περίπτωση που ο αριθμός των επιτιθέμενων είναι ίσος ή μεγαλύτερος από το πλήθος των οχημάτων στην περιοχή ενδιαφέροντος τότε το Δh δεν μπορεί να υπολογιστεί λόγω του λογαρίθμου. Έτσι, κάναμε την παραδοχή πως η σχέση (2) έχει νόημα μόνο όταν B < K και επομένως για να υπάρξει μεταβολή εντροπίας και πιθανότητα για ανταλλαγή θα πρέπει ο αριθμός των γειτονικών οχημάτων να είναι πάντα μεγαλύτερος του B.

6.4 Υλοποίηση κρυπτογραφικών τεχνικών

Όπως γίνεται εμφανές από το κεφάλαιο 6.1, ένα μεγάλο ποσοστό των μηνυμάτων που ανταλλάσσονται κατά τη λειτουργία του σχήματος MixGroup περιέχουν κρυπτογραφημένη πληροφορία προκειμένου να διασφαλίσουν την ακεραιότητα των δεδομένων, την ταυτοποίηση των αποστολέων και την προστασία από ωτακουστές. Συνεπώς, η επιλογή κρυπτογραφικής μεθόδου είναι ιδιαιτέρως σημαντική για τη λειτουργία και την απόδοση του μοντέλου, και θα πρέπει να συνεισφέρει στην όσο το δυνατόν καλύτερη κάλυψη των απαιτήσεων ασφάλειας και ιδιωτικότητας που παρουσιάστηκαν στο κεφάλαιο 3. Ακόμα, λόγω της απαίτησης των δικτύων οχημάτων για πολύ γρήγορη απόκριση με περιορισμένους πόρους, θα πρέπει να έχει το ελάχιστο δυνατό κόστος σε υπολογιστικό χρόνο, μέγεθος δεδομένων και κατανάλωση ενέργειας. Συνεπώς, παρουσιάζει ιδιαίτερο ενδιαφέρον η επιλογή της κατάλληλης μεθόδου για το συγκεκριμένο μοντέλο ιδιωτικότητας, και είναι το θέμα που πραγματεύεται το παρόν κεφάλαιο.

Στην υλοποίηση που αναπτύχθηκε, οι κρυπτογραφικές μέθοδοι χρησιμοποιήθηκαν για τις παρακάτω εφαρμογές:

1. Παραγωγή κλειδιών.
2. Κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.
3. Παραγωγή και επαλήθευση ψηφιακών υπογραφών.
4. Παραγωγή και επαλήθευση πιστοποιητικών ασφαλείας.

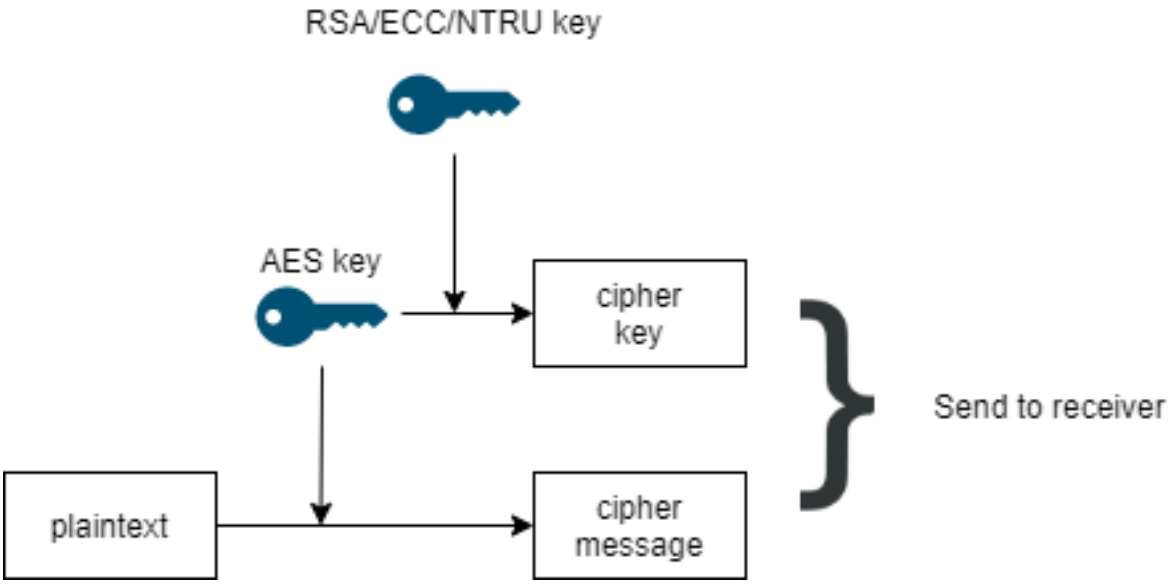
Στα πλαίσια των προσομοιώσεών μας και για την καλύτερη δόμηση και ευκολία χρήσης, επιδιώχθηκε η υλοποίηση να διαμορφωθεί με τρόπο τέτοιο ώστε να μπορεί να εναλλάσσεται μεταξύ των εξεταζόμενων μεθόδων με τη χρήση μια απλής λογικής μεταβλητής. Επομένως, κάθε διαφορετική κρυπτογραφική μέθοδος που μελετήθηκε βρίσκεται σε ξεχωριστό αρχείο/βιβλιοθήκη που περιέχει τις C/C++ συναρτήσεις που υλοποιούν τις παραπάνω εφαρμογές. Στη συνέχεια του κεφαλαίου παρατίθενται οι υλοποιήσεις των κρυπτογραφικών αλγορίθμων που αναφέρθηκαν στο κεφάλαιο 2.

6.4.1 AES

Όπως προαναφέρθηκε στο κεφάλαιο 2, ο συγκεκριμένος αλγόριθμος αποτέλεσε τη βάση κάθε κρυπτογραφημένου μηνύματος, καθώς χρησιμοποιήθηκε για να κρυπτογραφήσει την πληροφορία προς μετάδοση, και στη συνέχεια το συμμετρικό του κλειδί κρυπτογραφήθηκε με έναν από τους αλγορίθμους που μελετήσαμε. Αυτό σημαίνει, πως και οι 3 μέθοδοι που μελετήσαμε έχουν ως κοινό στοιχείο τη χρήση του AES για την ουσιαστική κρυπτογράφηση της πληροφορίας. Το σχήμα 1 αναπαριστά σχηματικά τη διαδικασία κρυπτογράφησης για όλες τις μεθόδους κρυπτογράφησης, από το οποίο φαίνεται πως γίνεται χρήση ενός συμμετρικού αλγορίθμου και ενός ασύμμετρου.

Η συγκεκριμένη υλοποίηση του αλγορίθμου AES που χρησιμοποιήθηκε παρέχεται από την ελεύθερη βιβλιοθήκη Crypto++[41], και τέθηκαν οι εξής παράμετροι:

- Μέθοδος λειτουργίας: Cipher Block Chaining(CBC)
- Μήκος κλειδιού: 256 bits
- Μήκος block: 128 bits



Εικόνα 15: Υλοποίηση κρυπτογράφησης μηνύματος

Παρακάτω φαίνεται η υλοποίηση της διαδικασίας συμμετρικής κρυπτογράφησης, κατά την οποία παράγεται ένα τυχαίο συμμετρικό κλειδί μήκους 256 bits και αρχικοποιείται με ένα διάνυσμα αρχικοποίησης(initialization vector). Στη συνέχεια, το κείμενο μεταφράζεται σε δεκαεξαδική μορφή και δίνεται ως είσοδο στον αλγόριθμο κρυπτογράφησης. Στο τέλος της διαδικασίας έχει παραχθεί το κρυπτογραφημένο κείμενο σε δεκαεξαδική μορφή.

```
uint8_t *symm_key = (uint8_t*)calloc(AES::MAX_KEYLENGTH, sizeof(uint8_t));
prng.GenerateBlock(symm_key, AES::MAX_KEYLENGTH);
string symm_key_string = string((char*)symm_key, AES::MAX_KEYLENGTH);

CryptoPP::CBC_Mode< CryptoPP::AES >::Encryption e_AES;
e_AES.SetKeyWithIV(symm_key, AES::MAX_KEYLENGTH, iv, AES::BLOCKSIZE);

string plain;
CryptoPP::StringSource(string((char*)buffer, size), true, newCryptoPP::HexEncoder(new
                                                                    CryptoPP::StringSink(plain)));
string cipher;
CryptoPP::StringSource(plain, true, new CryptoPP::StreamTransformationFilter(e_AES,
                                    new CryptoPP::StringSink(cipher)));
```

Για την αποκρυπτογράφηση, ακολουθείται η ακριβώς αντίστροφη διαδικασία: το κείμενο μετατρέπεται από δεκαεξαδική μορφή σε byte αναπαράσταση, και αφού αποκρυπτογραφηθεί το συμμετρικό κλειδί με χρήση κάποιου εκ των 3 αλγορίθμων δημοσίου κλειδιού που μελετάμε, αποκρυπτογραφείται το μήνυμα. Παρακάτω φαίνεται η υλοποίηση:

```
string cipher;
CryptoPP::StringSource(string((char*)buffer, size), true, new
        CryptoPP::HexDecoder(new CryptoPP::StringSink(cipher)));
```

```
<public key algorithm recovers the symmetric key...>

uint8_t *symm_key = (uint8_t*)calloc(AES::MAX_KEYLENGTH, sizeof(uint8_t));
memcpy(symm_key, recovered_key.data(), AES::MAX_KEYLENGTH);
CryptoPP::CBC_Mode< AES >::Decryption d_AES;
d_AES.SetKeyWithIV(symm_key, AES::MAX_KEYLENGTH, iv, AES::BLOCKSIZE);
string recovered;
CryptoPP::StringSource(actual_cipher, true, new CryptoPP::StreamTransformationFilter(
                                                    d_AES, new CryptoPP::StringSink(recovered)));
string plain;
CryptoPP::StringSource(recovered, true, new CryptoPP::HexDecoder(new
                                                    CryptoPP::StringSink(plain)));
```

6.4.2 RSA

Όπως και στην περίπτωση του AES, χρησιμοποιήσαμε την υλοποίηση που παρείχε η βιβλιοθήκη Crypto++ για την εφαρμογή του αλγορίθμου RSA. Η βιβλιοθήκη αυτή είναι υλοποιημένη σε C++, που υποστηρίζεται από το εργαλείο προσομοίωσης NS-3. Η μοναδική παράμετρος που επηρεάσαμε στη συγκεκριμένη υλοποίηση ήταν το μήκος κλειδιού του αλγορίθμου, η οποία έλαβε τρεις διακριτές τιμές: 1024, 2048 και 3072 bits. Στη συνέχεια, αναλύονται τα επιμέρους σημεία εφαρμογής του RSA μαζί με τα αντίστοιχα κομμάτια κώδικα.

Παραγωγή κλειδιών

Σε αυτό το στάδιο παράγεται το ζεύγος ιδιωτικού και δημόσιου κλειδιού κάνοντας χρήση μιας γεννήτριας τυχαίων αριθμών και του μήκους κλειδιού που έχουμε επιλέξει.

```
CryptoPP::AutoSeededRandomPool prng;
CryptoPP::InvertibleRSAFunction params;
params.GenerateRandomWithKeySize(prng, RSA_BIT_KEY_LENGTH);
RSA::PrivateKey SK = RSA::PrivateKey(params);
RSA::PublicKey PK = RSA::PublicKey(params);
```

Κρυπτογράφηση μηνύματος

Για την κρυπτογράφηση του μηνύματος, το οποίο είναι το συμμετρικό κλειδί του AES, χρησιμοποιείται το προκαθορισμένο σχήμα OAEP_SHA το οποίο μεταχειρίζεται τους αλγόριθμους OAEP και SHA-256 για να «γεμίσει» και να κατακερματίσει το μήνυμα. Δέχεται ως είσοδο το δημόσιο κλειδί του παραλήπτη που παρήχθη πιο πάνω και το συμμετρικό κλειδί και παράγει το κρυπτοκείμενο μέσω μιας ροής χαρακτήρων, κάνοντας ταυτόχρονη χρήση της γεννήτριας τυχαίων αριθμών.

```
string cipher_key;
CryptoPP::RSAES_OAEP_SHA_Encryptor e_RSA(PK);
CryptoPP::StringSource ss1(symm_key_string, true, new
        CryptoPP::PK_EncryptorFilter(prng,e_RSA,new
        CryptoPP::StringSink(cipher_key)));
```

Αποκρυπτογράφηση μηνύματος

Η διαδικασία είναι πανομοιότυπη με αυτήν της κρυπτογράφησης, με τη διαφορά ότι εδώ χρησιμοποιείται το ιδιωτικό κλειδί του παραλήπτη, το οποίο είναι γνωστό μόνο στον ίδιο.

```
CryptoPP::RSAES_OAEP_SHA_Decryptor d_RSA(SK);
CryptoPP::StringSource(cipher_key, true, new
        CryptoPP::PK_DecryptorFilter(prng, d_RSA, new
        CryptoPP::StringSink(recovered_key)));
```

Παραγωγή ψηφιακής υπογραφής

Για την παραγωγή της υπογραφής, χρησιμοποιείται το ενσωματωμένο σχήμα υπογραφής RSASS το οποίο κάνει χρήση του σχήματος PSS και του αλγορίθμου SHA-256. Δέχεται ως είσοδο το ιδιωτικό κλειδί του υπογράφοντα και το μήνυμα προς υπογραφή και δίνει ως έξοδο την υπογραφή σε μορφή ακολουθίας χαρακτήρων.

```
CryptoPP::RSASS<CryptoPP::PSS, CryptoPP::SHA256>::Signer signer(SK);
string signature;
CryptoPP::StringSource ss1(message, true, new
        CryptoPP::SignerFilter(prng, signer, new
        CryptoPP::StringSink(signature)));
```

Επαλήθευση ψηφιακής υπογραφής

Αντίστοιχα με την υπογραφή, χρησιμοποιείται η ενσωματωμένη δομή RSASS με είσοδο το δημόσιο κλειδί και έξοδο την αληθοτιμή της επαλήθευσης. Η τιμή αυτή είναι 1 σε περίπτωση επιτυχημένης επαλήθευσης και 0 σε περίπτωση αποτυχημένης.

```
CryptoPP::RSASS<CryptoPP::PSS, CryptoPP::SHA256>::Verifier verifier(PubKey.PK);
string recovered;
try
{
        CryptoPP::StringSource ss2(message+sig.Sig, true, new
        CryptoPP::SignatureVerificationFilter(verifier, new
CryptoPP::StringSink(recovered),
                                CryptoPP::SignatureVerificationFilter::THROW_EXCEPTION |
                        CryptoPP::SignatureVerificationFilter::PUT_MESSAGE));
}
catch (...)
{
        return 0;
}
return 1;
```

Παραγωγή πιστοποιητικού

Στα πλαίσια της παρούσας εργασίας χρησιμοποιούμε ένα θεωρητικό πιστοποιητικό, το οποίο σημαίνει ότι μέσα του περιέχει μόνο την ταυτότητα του κατόχου(ένα ψευδώνυμο) ενωμένη με το δημόσιο κλειδί του και την υπογραφή της ένωσης. Για την παραγωγή της υπογραφής χρησιμοποιείται η μέθοδος που προαναφέρθηκε, μαζί με το ιδιωτικό κλειδί του RA, καθώς αυτός είναι ο μοναδικός υπεύθυνος για την έκδοση πιστοποιητικών.

Επαλήθευση πιστοποιητικού

Η επαλήθευση του πιστοποιητικού δε διαφέρει καθόλου από την επαλήθευση υπογραφής που αναφέρθηκε παραπάνω. Για την επαλήθευση αρκεί η γνώση του πιστοποιητικού και του δημοσίου κλειδιού του RA, το οποίο σημαίνει πως όλοι μπορούν να επαληθεύσουν την εγκυρότητα του συγκεκριμένου πιστοποιητικού καθώς το δημόσιο κλειδί του RA θεωρείται γνωστό.

6.4.3 ECC

Για την υλοποίηση χρησιμοποιήθηκε η βιβλιοθήκη ελεύθερης χρήσης easy-ecc[42] Η βιβλιοθήκη αυτή είναι υλοποιημένη σε C, η οποία υποστηρίζεται από το εργαλείο προσομοίωσης NS-3, και υποστηρίζει τις εξής ελλειπτικές καμπύλες: secp128r1, secp192r1, secp256r1 και secp384r1. Η καμπύλη που χρησιμοποιήθηκε στην παρούσα εργασία ήταν η secp256r1, που προσφέρει ασφάλεια επιπέδου 128 bits, επομένως το μήκος του ιδιωτικού κλειδιού είναι 256 bits(32 bytes) και, λόγω του ότι η συγκεκριμένη βιβλιοθήκη χρησιμοποιεί συμπιεσμένη αναπαράσταση, το μήκος του δημοσίου κλειδιού είναι 264 bits(33 bytes).

Παραγωγή κλειδιών

Σε αυτό το στάδιο παράγεται το ζεύγος κλειδιών κάνοντας χρήση της συνάρτησης ecc_make_key της βιβλιοθήκης, η οποία δέχεται ως είσοδο 2 πίνακες χαρακτήρων στους οποίους θα καταλήξουν τα κλειδιά.

```
#define ECC_BYTES 32
uint8_t SK[ECC_BYTES];
uint8_t PK[ECC_BYTES+1]
ecc_make_key(PK, SK);
```

Κρυπτογράφηση μηνύματος

Όπως και στην περίπτωση του RSA, η κρυπτογράφηση γίνεται σε 2 στάδια: πρώτα παράγεται ένα κλειδί με τη χρήση ελλειπτικών καμπύλων και στη συνέχεια χρησιμοποιείται για να κρυπτογραφήσει το μήνυμα με τον αλγόριθμο AES. Η διαφορά με τον RSA έγκειται στο ότι η παραγωγή του κλειδιού χρησιμοποιεί την τεχνική ECDH(Elliptic Curve Diffie-Helman), που σημαίνει ότι δημιουργείται ένα κοινό μυστικό κλειδί σύμφωνα με τον αλγόριθμο Diffie-Helman για ελλειπτικές καμπύλες ο οποίος είναι υλοποιημένος στη βιβλιοθήκη. Δέχεται ως είσοδο το δημόσιο κλειδί του παραλήπτη και το ιδιωτικό κλειδί του αποστολέα και παράγει ως έξοδο το κοινό κλειδί. Στη συνέχεια αυτό το κλειδί περνάει από τον αλγόριθμο κατακερματισμού SHA-256 για βελτίωση της ασφάλειας και μετά χρησιμοποιείται σαν συμμετρικό κλειδί του AES.

```
uint8_t p_shared[ECC_BYTES];
ecdh_shared_secret(PK, SK, p_shared);
string T_digest = Hash_Function(p_shared, ECC_BYTES);
memcpy(output, T_digest.c_str(), ECC_BYTES);

string     plain, cipher, encoded;
CryptoPP::CBC_Mode< CryptoPP::AES >::Encryption e;
```

```
e.SetKeyWithIV(output, AES::MAX_KEYLENGTH, iv, AES::BLOCKSIZE);
CryptoPP::StringSource(string((char*)buffer, size), true, new CryptoPP::HexEncoder(new
CryptoPP::StringSink(plain)));
CryptoPP::StringSource(plain, true, new CryptoPP::StreamTransformationFilter(e, new
                                        CryptoPP::StringSink(cipher)));
CryptoPP::StringSource(cipher, true, new CryptoPP::HexEncoder(new
                                        CryptoPP::StringSink(encoded)));
```

Αποκρυπτογράφηση μηνύματος

Σε αυτό το στάδιο ακολουθείται διαδικασία πανομοιότυπη με αυτήν της κρυπτογράφησης: δημιουργείται πρώτα το κοινό μυστικό κλειδί με ECDH και SHA, και στη συνέχεια χρησιμοποιείται για να αποκρυπτογραφήσει το μήνυμα με AES.

```
uint8_t p_shared[ECC_BYTES];
ecdh_shared_secret(PK, SK, p_shared);
string T_digest = Hash_Function(p_shared, ECC_BYTES);
memcpy(output, T_digest.c_str(), ECC_BYTES);
string  decoded, recovered, plain;
CryptoPP::CBC_Mode< AES >::Decryption d;
d.SetKeyWithIV(output, AES::MAX_KEYLENGTH, iv, AES::BLOCKSIZE);
CryptoPP::StringSource(string((char*)buffer, size), true, new CryptoPP::HexDecoder(new
CryptoPP::StringSink(decoded)));
CryptoPP::StringSource(decoded, true, new CryptoPP::StreamTransformationFilter(d, new
                                    CryptoPP::StringSink(recovered)));
CryptoPP::StringSource(recovered, true, new CryptoPP::HexDecoder(new
                                        CryptoPP::StringSink(plain)));
```

Παραγωγή ψηφιακής υπογραφής

Για την παραγωγή της υπογραφής χρησιμοποιείται η μέθοδος ECDSA(Elliptic Curve Digital Signature Algorithms), η οποία υποστηρίζεται από τη βιβλιοθήκη. Δέχεται ως είσοδο το ιδιωτικό κλειδί του υπογράφοντα και το μήνυμα που θα υπογραφεί(το οποίο έχει πρώτα περάσει από τον SHA-256) και δίνει ως έξοδο την υπογραφή του μηνύματος. Το μέγεθος της υπογραφής είναι 64 bytes.

```
ecdsa_sign(SecretKey, hashed_value, signature);
```

Επαλήθευση ψηφιακής υπογραφής

Για την επαλήθευση της ψηφιακής υπογραφής με ECC, η συνάρτηση δέχεται ως είσοδο το δημόσιο κλειδί του υπογράφοντα, την υπογραφή και τα δεδομένα που έχουν δεχτεί το ίδιο hash με το αρχικό μήνυμα, και επιστρέφει 1 σε περίπτωση έγκυρης υπογραφής και 0 σε περίπτωση άκυρης.

```
int result = ecdsa_verify(PublicKey, hashed_value, signature);
```

Παραγωγή πιστοποιητικού

Τα πιστοποιητικά που χρησιμοποιούνται σε αυτή τη μέθοδο έχουν την ίδια ακριβώς δομή με αυτήν που περιγράφηκε στη μέθοδο RSA και για την παραγωγή τους χρησιμοποιούνται οι

μέθοδοι κατακερματισμού και υπογραφής που περιγράφηκαν σε αυτό το κεφάλαιο. Ομοίως με την προηγούμενη περίπτωση, ο RA είναι ο μόνος υπεύθυνος για την έκδοση των πιστοποιητικών.

Επαλήθευση πιστοποιητικού

Η επαλήθευση ενός πιστοποιητικού, όπως και αναφέρθηκε και στην προηγούμενη μέθοδο, δε διαφέρει καθόλου από την επαλήθευση μιας ψηφιακής υπογραφής όπως περιγράφηκε σε αυτό το κεφάλαιο, με τα μόνα απαραίτητα στοιχεία το πιστοποιητικό και το δημόσιο κλειδί του RA.

6.4.4 NTRU

Για την υλοποίηση αυτής της μεθόδου χρησιμοποιήθηκε η βιβλιοθήκη ελεύθερης χρήσης NTRU-Crypto[43], και συγκεκριμένα η υλοποίηση σε γλώσσα προγραμματισμού C του αλγορίθμου κρυπτογράφησης δημοσίου κλειδιού NTRUEncrypt. Η βιβλιοθήκη υποστηρίζει όλα τα σύνολα παραμέτρων τα οποία ορίζονται στο πρότυπο IEEE 1363.1. Το σύνολο παραμέτρων που χρησιμοποιήθηκε ήταν το ES449EP1, το οποίο υπόσχεται ασφάλεια 128 bits με μέγεθος δημοσίου κλειδιού 623 bytes και μέγεθος ιδιωτικού κλειδιού 713 bytes.

Ο αλγόριθμος NTRUEncrypt χρειάζεται την ύπαρξη μιας κρυπτογραφικά ασφαλούς πηγής τυχαίων bits. Για αυτό το σκοπό χρησιμοποιείται μια ντετερμινιστική γεννήτρια τυχαίων bits(deterministic random bit generator – DRBG), η οποία μπορεί είτε να υλοποιηθεί εσωτερικά είτε να χρησιμοποιήσει μια υπάρχουσα εξωτερική πηγή τυχαίων bits. Στην παρούσα εργασία επιλέχθηκε η δεύτερη μέθοδος, κάνοντας χρήση του ειδικού αρχείου **/dev/urandom**[44] που είναι διαθέσιμο στα λειτουργικά συστήματα τύπου Unix. Η γεννήτρια αυτή αρχικοποιείται μια φορά στην αρχή της προσομοίωσης και χρησιμοποιείται στη συνέχεια σε όλες τις κρυπτογραφικές διαδικασίες. Παρακάτω φαίνεται η αρχικοποίηση, με τη randombytes να είναι η συνάρτηση τυχαίων αριθμών που έχει υλοποιηθεί και drbg ο δείκτης στην γεννήτρια τυχαίων αριθμών που θα χρησιμοποιηθεί στη συνέχεια:

```
ntru_crypto_drbg_external_instantiate((RANDOM_BYTES_FN) &randombytes, &drbg);
```

Σε αυτό το σημείο σημειώνουμε, πως δεν κάναμε χρήση NTRU για την εφαρμογή ψηφιακών υπογραφών και πιστοποιητικών δημοσίου κλειδιού. Ο αλγόριθμος ψηφιακών υπογραφών NTRUSign, όπως αναφέρθηκε και στο κεφάλαιο 3, αποδείχτηκε αδύναμος σε επιθέσεις καθώς υπάρχει η δυνατότητα διαρροής του ιδιωτικού κλειδιού. Βελτιωμένοι αλγόριθμοι υπογραφών με χρήση NTRU έχουν προταθεί για προτυποποίηση από το NIST, αλλά δεν έχει γίνει ακόμα αποδεκτοί. Με βάση τα παραπάνω, αποφασίστηκε να μην εξεταστεί κάποιος αλγόριθμος NTRU για την απόδοση στο τομέα των ψηφιακών υπογραφών, καθώς δεν υπάρχει κάποια προτυποποιημένη υλοποίηση που θα μπορούσαμε να χρησιμοποιήσουμε.

Παραγωγή κλειδιών

Η παραγωγή κλειδιών συμπεριλαμβάνει 3 στάδια: την απόκτηση του μήκους ιδιωτικού και δημοσίου κλειδιού, την παραγωγή των κλειδιών και τον έλεγχο ορθότητάς του μέσω μιας τετριμμένης κρυπτογράφησης και αποκρυπτογράφησης. Για τα πρώτα 2 στάδια χρησιμοποιείται

η συνάρτηση ntru_crypto_ntru_encrypt_keygen, ενώ για το 3ο στάδιο χρησιμοποιούνται οι ntru_crypto_ntru_encrypt και ntru_crypto_ntru_decrypt.

```
/* Get public/private key lengths */
ntru_crypto_ntru_encrypt_keygen(drbg, param_set_id, &public_key_len, NULL,
                                                    &private_key_len, NULL);

public_key_len = PUB_KEY_LENGTH;
private_key_len = PRV_KEY_LENGTH;

/* Generate a key */
ntru_crypto_ntru_encrypt_keygen(drbg, param_set_id, &public_key_len,
                                                        PubK.PK,
                                                        &private_key_len,
                                                        SecK.SK);

rc = ntru_crypto_ntru_encrypt(drbg, public_key_len, PubKey, 0, NULL, &ciphertext_len, NULL);
if (rc != NTRU_OK)
        fprintf(stderr,"\tError: Invalid public key");

rc = ntru_crypto_ntru_decrypt(private_key_len, SecKey, 0, NULL, &max_msg_len, NULL);
if (rc != NTRU_OK)
        fprintf(stderr,"\tError: Invalid private key");
```

Κρυπτογράφηση μηνύματος

Η διαδικασία κρυπτογράφησης ακολουθεί, όπως και στις άλλες μεθόδους, 2 βασικά βήματα: κρυπτογράφηση του μηνύματος με τον αλγόριθμο AES και κρυπτογράφηση του κλειδιού του AES με τον αλγόριθμο NTRUEncrypt. Η συμμετρική κρυπτογράφηση είναι πανομοιότυπη με τις προηγούμενες υλοποιήσεις, οπότε η διαφορά εστιάζεται στην κρυπτογράφηση δημοσίου κλειδιού. Όπως και στην παραγωγή κλειδιών, πρώτα εκτελείται η συνάρτηση κρυπτογράφησης με κενά ορίσματα προκειμένου να αποκτηθεί το μήκος του δημοσίου κλειδιού και να δεσμευτεί ο κατάλληλος χώρος στη μνήμη. Στη συνέχεια, το κλειδί που χρησιμοποιήθηκε στον AES κρυπτογραφείται με την ίδια συνάρτηση και αποστέλετται μαζί με το υπόλοιπο κρυπτογραφημένο μήνυμα.

```
uint16_t short_size = AES::MAX_KEYLENGTH;
uint32_t rc = ntru_crypto_ntru_encrypt(drbg, PUB_KEY_LENGTH, PK_remote.PK, 0, NULL,
                                                    &short_size, NULL);
if (rc != NTRU_OK)
        fprintf(stderr,"\tError: Bad public key");
uint8_t *cipher_key = (uint8_t *) malloc(short_size * sizeof(uint8_t));
rc = ntru_crypto_ntru_encrypt(drbg, PUB_KEY_LENGTH, PK_remote.PK, AES::MAX_KEYLENGTH,
                                        symm_key, &short_size, cipher_key);

string encoded;
CryptoPP::StringSource(string((char*)cipher_key,short_size)+cipher, true, new
        CryptoPP::HexEncoder(new CryptoPP::StringSink(encoded)));
```

Αποκρυπτογράφηση μηνύματος

Για την αποκρυπτογράφηση ακολουθείται η αντίστροφη διαδικασία της κρυπτογράφησης. Αρχικά το κρυπτοκείμενο μετασχηματίζεται από δεκαεξαδική αναπαράσταση σε αναπαράσταση bytes. Στη συνέχεια, αφού αποκτηθεί το μήκος του ιδιωτικού κλειδιού που θα χρησιμοποιηθεί στην διαδικασία, αποκρυπτογραφείται το συμμετρικό κλειδί με χρήση NTRU, και στη συνέχεια αυτό χρησιμοποιείται στην αποκρυπτογράφηση με AES του ουσιαστικού μηνύματος όπως περιγράφηκε στο αντίστοιχο κεφάλαιο.

```
string cipher;
CryptoPP::StringSource(string((char*)buffer, size), true, new
        CryptoPP::HexDecoder(new CryptoPP::StringSink(cipher)));

string recovered_key, cipher_key = cipher.substr(0,CIPHER_LENGTH);
string actual_cipher = cipher.substr(CIPHER_LENGTH, cipher.npos);
uint16_t max_msg_len = PLAIN_LENGTH;

uint32_t rc = ntru_crypto_ntru_decrypt(PRV_KEY_LENGTH, Reg_Auth.Creds.SK.SK, 0, NULL,
                                                        &max_msg_len, NULL);
if (rc != NTRU_OK)
                fprintf(stderr,"\tError: Invalid private key");

uint8_t *plaintext = (uint8_t *) malloc(max_msg_len * sizeof(uint8_t));
rc = ntru_crypto_ntru_decrypt(PRV_KEY_LENGTH, creds.SK.SK, cipher_key.length(),
        (uint8_t*) cipher_key.c_str(), &max_msg_len, plaintext);
```

6.5 Υλοποίηση μοντέλου ενέργειας

Το εργαλείο NS-3 παρέχει μηχανισμούς που προσομοιώνουν διάφορα μοντέλα πηγής, κατανάλωσης και ανανέωσης ενέργειας[45]. Αυτά τα μοντέλα μπορούν να εφαρμοστούν πάνω σε κάθε κόμβο της προσομοίωσης και να εξαχθούν χρήσιμα συμπεράσματα με βάση αυτά τα δεδομένα. Στην παρούσα εργασία επικεντρωθήκαμε στην κατανάλωση ενέργειας των οχημάτων κατά τη διάρκεια της διαδικασίας ανταλλαγής ψευδωνύμων, προκειμένου να πάρουμε μια εκτίμηση του κόστους των διαφορετικών τεχνικών που χρησιμοποιήσαμε.

Το μοντέλο που χρησιμοποιήθηκε ονομάζεται Wifi Radio Energy Model, και προσομοιάζει την κατανάλωση ενέργειας μιας συσκευής με δυνατότητα Wifi. Το μοντέλο αυτό υποστηρίζει τις πιθανές καταστάσεις της συσκευής στο φυσικό στρώμα: Idle, CcaBusy, Tx, Rx, ChannelSwitch, Sleep, Off. Κάθε μια από αυτές τις καταστάσεις είναι συνδεδεμένη με μια τιμή κατανάλωσης ρεύματος(μετρημένη σε Ampere) και σε κάθε μετάβαση από τη μια κατάσταση στην άλλη, μέσω ενός listener, υπολογίζεται η εναπομείνουσα ενέργεια της συσκευής. Ακόμα, παρέχεται η δυνατότητα ενημέρωσης της συσκευής για την εξάντληση του διαθέσιμου αποθέματος ενέργειας προκειμένου η συσκευή να σταματήσει τη λήψη και μετάδοση μηνυμάτων, προσομοιώνοντας έτσι ένα ρεαλιστικό σενάριο εξάντλησης πόρων.

Η παρούσα υλοποίηση έχει ως εξής: κάθε όχημα εφοδιάζεται με μια πηγή ενέργειας η οποία αρχικοποιείται σε μια αυθαίρετη ποσότητα ενέργειας αρκετά μεγάλη ώστε να μην εξαντληθεί κατά τη διάρκεια της προσομοίωσης. Στη συνέχεια, σε κάθε ανταλλαγή μηνύματος για ένα όχημα συλλέγεται η διαφορά ανάμεσα στην προηγούμενη και την τωρινή στάθμη

ενέργειας, και έτσι μετράται η κατανάλωση ενέργειας ανά μήνυμα. Σημειώνεται πως μετράμε την κατανάλωση σε Joules. Παρακάτω φαίνονται η αρχικοποίηση της πηγής και η εφαρμογή του μοντέλου Wifi Radio Energy στα οχήματα του δικτύου:

```
/* energy source */
BasicEnergySourceHelper basicSourceHelper;
// configure energy source
basicSourceHelper.Set ("BasicEnergySourceInitialEnergyJ", DoubleValue (1000.0));
// install source
EnergySourceContainer Vehicle_sources = basicSourceHelper.Install (V);
/* device energy model */
WifiRadioEnergyModelHelper radioEnergyHelper;
// install device model
DeviceEnergyModelContainer deviceModels = radioEnergyHelper.Install (Vehicle_devices,
                                                                     Vehicle_sources);
```

Μετά την επεξεργασία ενός μηνύματος καλείται η συνάρτηση **update_entry_EnergyMap_Recv** η οποία αναλαμβάνει να ενημερώσει έναν πίνακα κατακερματισμού που κρατάει κάθε όχημα με την ενέργεια που καταναλώθηκε για ένα συγκεκριμένο τύπο μηνύματος. Το energy_pivot ξεκινάει από την αρχική τιμή της πηγής και ενημερώνεται με κάθε νέο μήνυμα.

```
this_V.update_entry_EnergyMap_Recv(key, this_V.basicSourcePtr->GetRemainingEnergy());

void update_entry_EnergyMap_Recv(uint8_t key, float value)
{
        EnergyMap[key] += energy_pivot - value;
        EnergyCnt[key] += 1;
        energy_pivot = value;
}
```

6.6 Υλοποίηση οδικού δικτύου και κίνησης οχημάτων

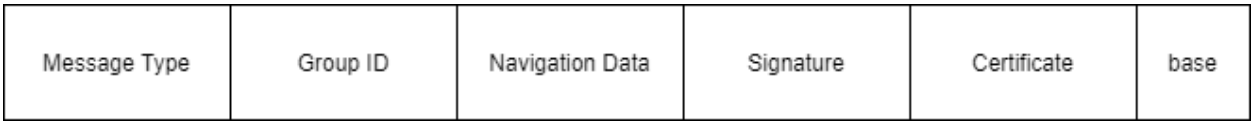
Για την υλοποίηση του οδικού δικτύου και της κίνησης των οχημάτων μέσα σε αυτό χρησιμοποιήθηκε το εργαλείο SUMO, το οποίο αναφέρθηκε στο κεφάλαιο 3. Σε αντιστοιχία με τις παραμέτρους που χρησιμοποιήθηκαν στο [26], υλοποιήθηκε μια τοπολογία πλέγματος 10x10, όπου κάθε κόμβος απείχε από τους γειτονικούς του 500 μέτρα, καλύπτοντας συνολική έκταση 20 km^2. Από τους 100 κόμβους της τοπολογίας, επιλέχτηκαν 40 προκειμένου να λειτουργήσουν ως διασταυρώσεις και με βάση αυτές κατασκευάστηκε το τελικό οδικό δίκτυο αποκόπτοντας αδιέξοδα και κενές ακμές. Η επιλογή έγινε μέσω του προγράμματος παραγωγής τυχαίων συντεταγμένων **grid_generator**, που αναπτύχθηκε για αυτόν το σκοπό. Η μέγιστη ταχύτητα καθορίστηκε στα 19.45 m/s ή 70 km/h, το πλάτος των λωρίδων κυκλοφορίας καθορίστηκε στα 3 m και ο δρόμοι αποτελούνται από 2 λωρίδες μονής κυκλοφορίας που είναι αντίρροπες. Στη συνέχεια, παράχθηκαν οι διαδρομές των οχημάτων μέσα σε αυτό το δίκτυο με χρήση του παρεχόμενου python script **randomTrips.py,** το οποίο παράγει τυχαίες διαδρομές για ένα καθορισμένο αριθμό οχημάτων. Τα αρχεία με τη μορφολογία του δικτύου και τις διαδρομές των

οχημάτων δόθηκαν ως είσοδοι στο SUMO, το οποίο εκτέλεσε την προσομοίωση και παρήγαγε ένα αρχείο με τις θέσεις κάθε οχήματος κατά τη διάρκεια εκτέλεσης. Αυτό το αρχείο, με τη χρήση ενός άλλου script - του **traceExporter.py**, μετασχηματίστηκε σε κατάλληλη μορφή για να μπορέσει να περάσει ως είσοδος στο NS-3.

6.7 Υλοποίηση δικτύου επικοινωνίας

Η υλοποίηση της επικοινωνίας μεταξύ των οντοτήτων του δικτύου έγινε εξολοκλήρου στην πλατφόρμα NS-3, με χρήση των γλωσσών προγραμματισμού C και C++. Αρχικά, δημιουργήθηκε ένα σύνολο κόμβων για κάθε μια από τις οντότητες του δικτύου, δηλαδή για τα οχήματα, τις RSU και τον RA. Στη συνέχεια, οι κόμβοι των οχημάτων αντιστοιχήθηκαν με το αρχείο εισόδου που παρήχθη από το SUMO ενώ οι RSU και RA τοποθετήθηκαν στατικά σε συγκεκριμένες θέσεις. Συγκεκριμένα, ο RA τοποθετήθηκε στο κέντρο της τοπολογίας και οι RSU διασκορπίστηκαν ανάλογα με τον αριθμό τους σε ίσες αποστάσεις μέσα στο grid. Έπειτα, τα οχήματα και οι RSU εφοδιάστηκαν με Wifi 802.11p συνδεσιμότητα και τις κατάλληλες IPs(στο υποδίκτυο 10.1.0X.X), και οι RSU και ο RA συνδέθηκαν με CSMA σε ένα άλλο υποδίκτυο(στο 192.168.0.X). Η επικοινωνία μεταξύ των διαφόρων οντοτήτων υλοποιήθηκε με χρήση UDP sockets, που σημαίνει ότι όλοι οι κόμβοι ήταν εφοδιασμένοι με 2 ειδών sockets: send και receive. Για την προσομοίωση, δρομολογήθηκαν τα μηνύματα ασφαλείας για τα οχήματα και τις RSUs ανά 1s. Ο χειρισμός αυτών των μηνυμάτων έγινε με χρήση συναρτήσεων callback οι οποίες καλούνταν στη λήψη κάθε μηνύματος.

Ο διαχωρισμός των μηνυμάτων και η επιλογή της εκάστοτε συνάρτησης χειρισμού έγινε με χρήση ειδικών επικεφαλίδων. Οι επικεφαλίδες αυτές αποτέλεσαν μια επέκταση της κλάσης Header που παρέχεται από το NS-3 και ήταν ζωτικής σημασίας στην υλοποίηση. Επί της ουσίας, όλη η πληροφορία ενσωματώθηκε σε μια σειρά απο επικεφαλίδες οι οποίες ενθυλακώνονταν με συγκεκριμένη σειρά πάνω από ένα dummy μήνυμα, και ανακτούνταν στον προορισμό του μηνύματος. Στην εικόνα 16 φαίνεται ένα παράδειγμα ενός απλού μηνύματος ασφαλείας.



Εικόνα 16: Δομή μηνύματος ασφαλείας

Κεφάλαιο 7: Πειραματική αξιολόγηση και συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάζονται και επεξηγούνται τα πειραματικά αποτελέσματα που παρήχθησαν κατά την εκπόνηση αυτής της εργασίας για την απόδοση των διαφόρων κρυπτογραφικών τεχνικών σε περιβάλλοντα IoV.

Για την εξαγωγή των μετρήσεων προσομοιώθηκε η τυχαία κίνηση 50-150 οχημάτων στο οδικό δίκτυο που περιγράφηκε στο κεφάλαιο 5, υπό την επίβλεψη 10 RSUs και 1 RA. Η ασύρματη εμβέλεια λήψης και μετάδοσης μηνυμάτων για τα οχήματα και τις RSUs ορίστηκε στα 500m. Προκειμένου να περιοριστεί το πρόβλημα σύγκρουσης πακέτων που αντιμετωπίσαμε λόγω της ταυτόχρονης μετάδοσης μηνυμάτων, εισήχθη μια τεχνητή μετατόπιση στην περίοδο μετάδοσης για κάθε όχημα. Αυτή η χρονική καθυστέρηση τέθηκε εμπειρικά για κάθε σύνολο παραμέτρων της προσομοίωσης και κυμαινόταν στο εύρος 20-500ms.

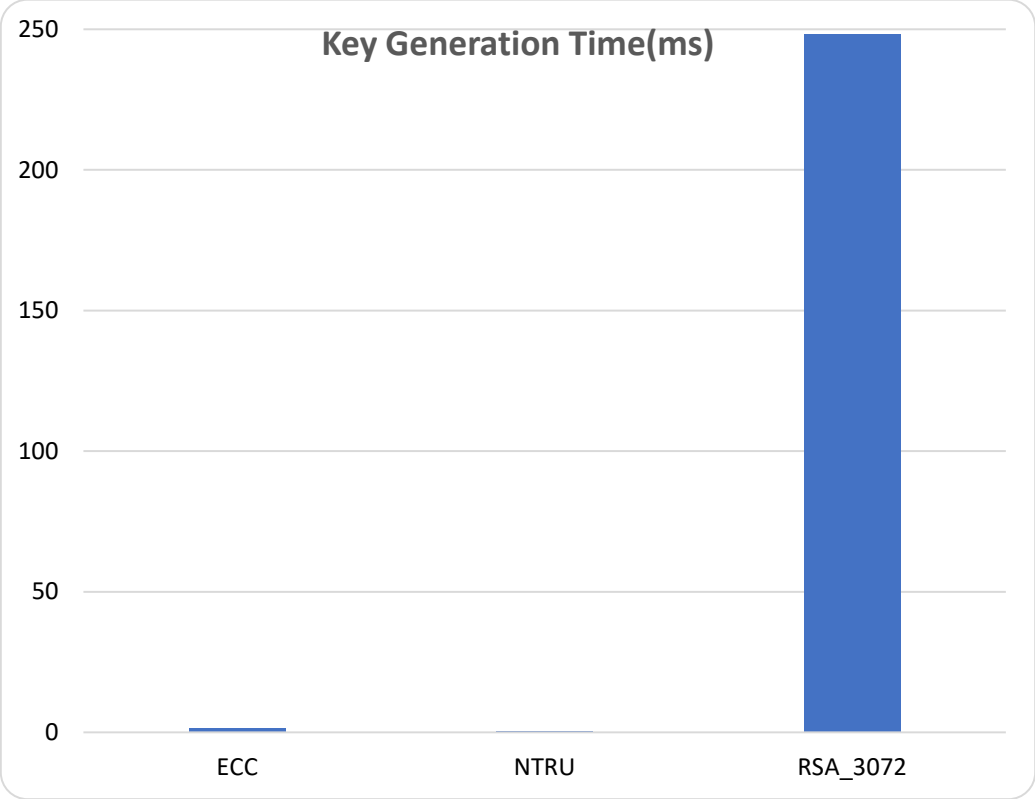
Για τη μέτρηση των χρόνων υπολογισμού έγινε χρήση μετρητών που καλούσαν τη συνάρτηση **gettimeofday**() στην αρχή και στο τέλος κάθε υπολογισμού. Στα διαγράμματα χρησιμοποιείται ο μέσος όρος των μετρήσεων για όλα τα οχήματα, αγνοώντας οχήματα που δε συμμετείχαν σε κάποια ανταλλαγή. Για τη μέτρηση του μεγέθους των διαφόρων μηνυμάτων που ανταλλάχθηκαν κατά την διαδικασία ανταλλαγής ψευδωνύμων αξιοποιήθηκαν οι επικεφαλίδες που αναφέρθηκαν στο προηγούμενο κεφάλαιο. Κάθε όχημα συντηρούσε 2 πίνακες κατακερματισμού: 1 πίνακα που αποτελούνταν από το συνολικό μέγεθος κάθε μηνύματος που λάμβανε και 1 πίνακα με το πλήθος του κάθε τύπου μηνύματος. Και στους 2 πίνακες το κλειδί ήταν ο τύπος μηνύματος, επομένως ήταν εύκολο στο τέλος της προσομοίωσης να ανακτηθεί το μέσο μέγεθος μηνύματος για κάθε διαφορετικό τύπο. Αντίστοιχη μέθοδος χρησιμοποιήθηκε και για την μέτρηση της κατανάλωσης ενέργειας ανά μήνυμα.

Οι προσομοιώσεις πραγματοποιήθηκαν σε εικονικό περιβάλλον Ubuntu Linux 14.0.4, με ξενιστή Windows 10, διαθέσιμη μνήμη 4GB και 1 πυρήνα επεξεργαστή Ryzen R7 2700X με συχνότητα 3.7GHz. Χρησιμοποιήθηκαν οι παρακάτω εκδόσεις λογισμικού:

- NS-3: 3.25
- Netanim: 3.107
- SUMO: 0.31.0

7.1 Πειραματική Αξιολόγηση

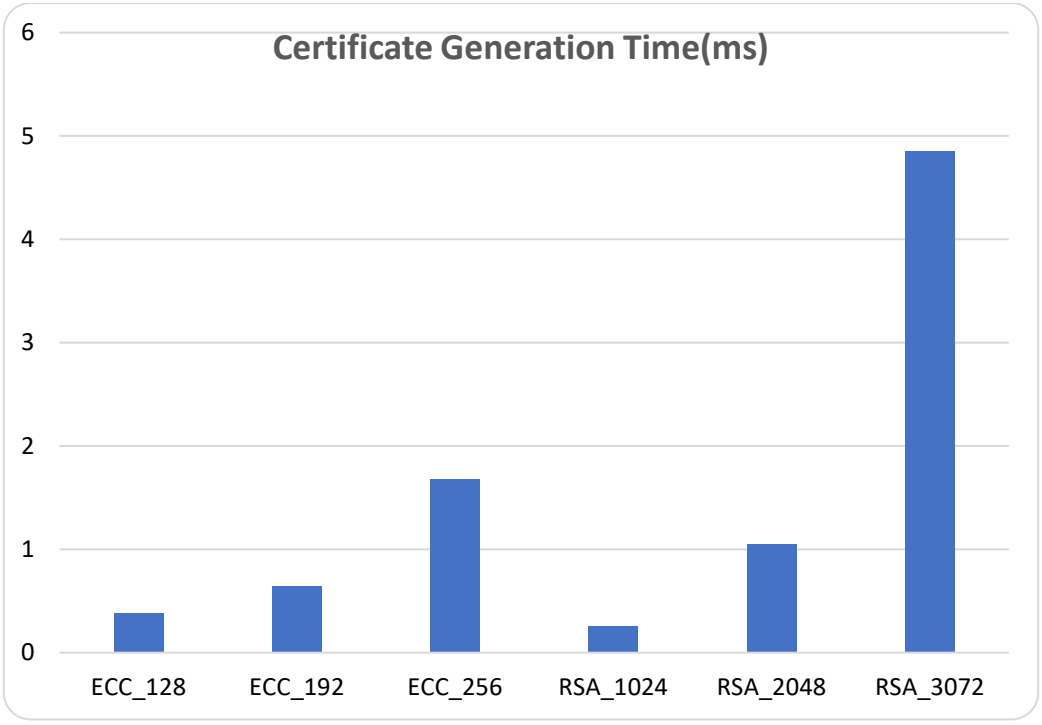
7.1.1 Παραγωγή Κλειδιών



Εικόνα 17: Χρόνοι παραγωγής κλειδιών(ms)

Παρατηρείται πως, για το ίδιο επίπεδο ασφάλειας, η κρυπτογραφική μέθοδος NTRU είναι περίπου 3 φορές πιο γρήγορη από την ECC στην παραγωγή του ζεύγους κρυπτογραφικών κλειδιών και πάνω από 400 φορές γρηγορότερη από τον RSA, ο οποίος παραδοσιακά μειονεκτεί σε αυτόν τον τομέα.

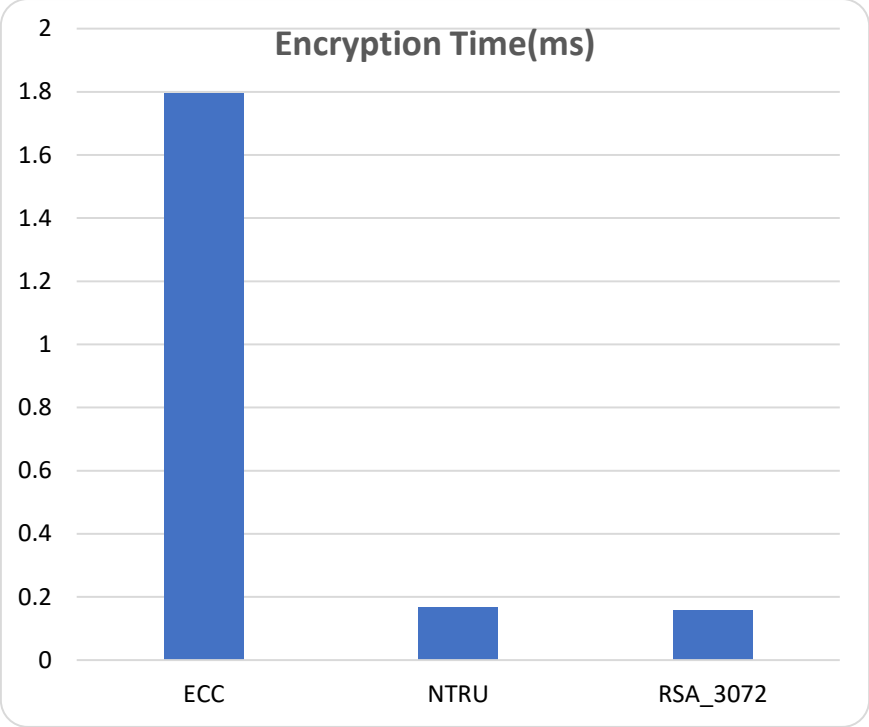
7.1.2 Παραγωγή Πιστοποιητικών



Εικόνα 18: Χρόνοι παραγωγής πιστοποιητικών(ms)

Εδώ, όπως προαναφέρθηκε, δε χρησιμοποιήθηκε η μέθοδος NTRU οπότε συγκρίναμε τον αλγόριθμο ECDSA με τον RSA. Συμπεριλάβαμε 3 διαφορετικά μήκη κλειδιών για κάθε αλγόριθμο για να δείξουμε καλύτερα την υποβάθμιση της απόδοσης με την αύξηση του μεγέθους. Από το σχήμα φαίνεται πως ο RSA επηρεάζεται πολύ πιο δραστικά από από την αύξηση στο μήκος κλειδιού από ότι η ECC, και για το επίπεδο ασφαλείας που μας ενδιαφέρει κυρίως τα 128 bits, ο RSA είναι 3 φορές πιο αργός στην παραγωγή πιστοποιητικών. Εδώ αξίζει να αναφερθεί ξανά πως τα πιστοποιητικά που χρησιμοποιήσαμε είναι επί της ουσίας απλές ψηφιακές υπογραφές, επομένως επιβεβαιώνεται η γνωστή αδυναμία του RSA στην παραγωγή υπογραφών και σε αυτήν την περίπτωση.

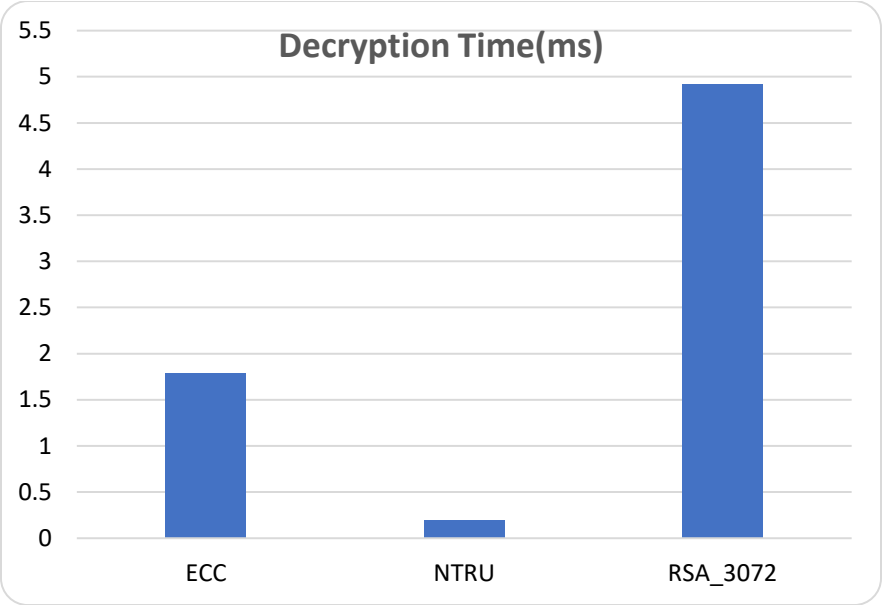
7.1.3 Χρόνος Κρυπτογράφησης



Εικόνα 19: Χρόνοι κρυπτογράφησης(ms)

Εδώ παρατηρούμε την ECC να έχει περίπου 10 φορές χειρότερη απόδοση από την NTRU και τον RSA κατά τη διαδικασία κρυπτογράφησης. Στην ουσία εδώ συγκρίνεται ο αλγόριθμος ECDH, καθώς υποθέτουμε πως κάθε αίτηση κρυπτογράφησης απαιτεί τον υπολογισμό του κοινού μυστικού από την αρχή, δηλαδή ακόμα και αν 2 οχήματα έχουν ξεπεράσει το αρχικό στάδιο επικοινωνίας θα πρέπει να υπολογίζουν κάθε φορά το κοινό μυστικό.

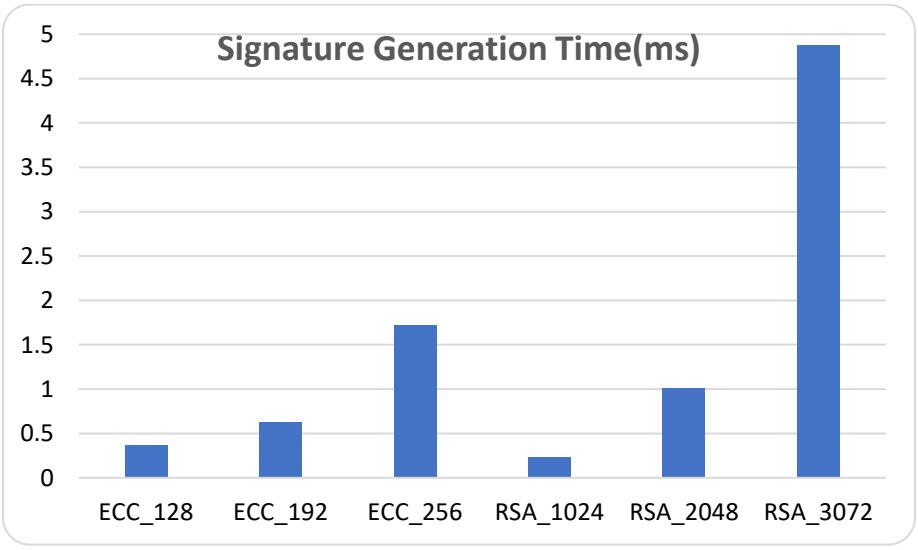
7.1.4 Χρόνος Αποκρυπτογράφησης



Εικόνα 20: Χρόνοι αποκρυπτογράφηση(ms)

Εδώ παρατηρείται πως πάλι ο αλγόριθμος NTRU είναι ο πιο αποδοτικός από τους 3 καθώς είναι 9 φορές πιο γρήγορος από την ECC και 25 από τον RSA , αλλά ο ECDH κερδίζει έδαφος σε σχέση με τον RSA, καθώς είναι σχεδόν 3 φορές πιο γρήγορος από αυτόν.

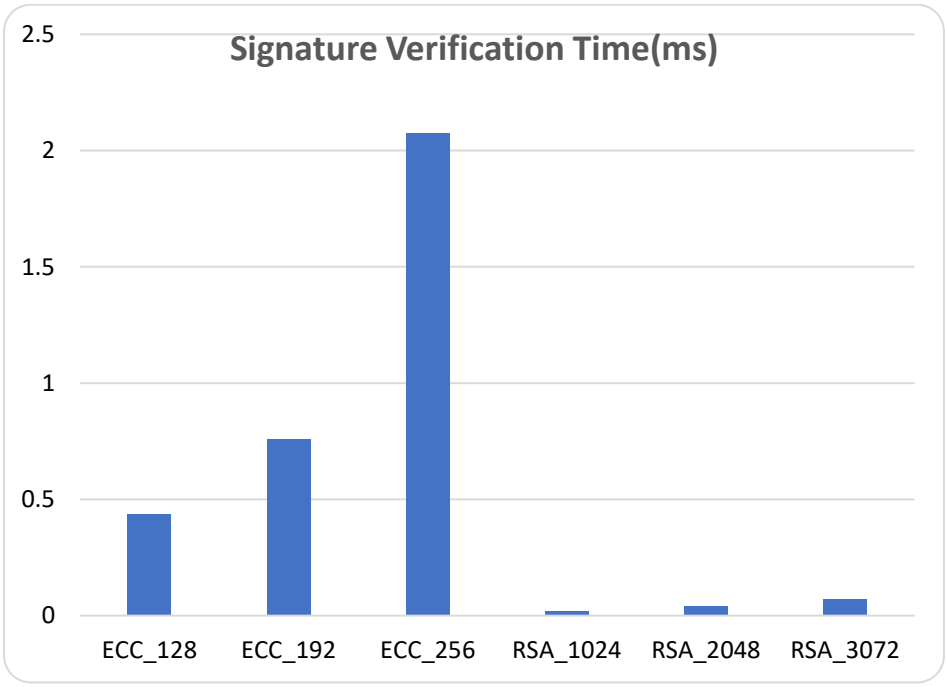
7.1.5 Παραγωγή Υπογραφής



Εικόνα 21: Χρόνοι παραγωγής υπογραφής(ms)

Παρατηρείται, όπως ήταν αναμενόμενο, πανομοιότυπη συμπεριφορά με την παραγωγή πιστοποιητικών. Η μόνη διαφορά είναι πως αυτές οι μετρήσεις προήλθαν από τα οχήματα, ενώ τα πιστοποιητικά παράγονται μόνο από τον RA, επομένως αυτό το διάγραμμα επαληθεύει την ορθότητα λειτουργίας της μεθόδου στους 2 τύπους κόμβων. Συνολικά, η ECC παραμένει πιο αποδοτική στην υπογραφή μηνυμάτων, το οποίο συνάδει με τα θεωρητικά και πειραματικά στοιχεία της υπάρχουσας βιβλιογραφίας. Αξίζει να αναφερθεί πως δεν υπήρχε διαφορά στους πόρους του RA και των οχημάτων, και αυτό αποτυπώνεται στην αμελητέα διαφορά των απόλυτων χρόνων εκτέλεσης.

7.1.6 Επαλήθευση Υπογραφής



Εικόνα 22: Χρόνοι επαλήθευσης υπογραφής(ms)

Εδώ παρατηρείται μια αντιστροφή της προηγούμενης κατάστασης, με την ECC να είναι κατά πολύ κατώτερη σε απόδοση από τον RSA στην επαλήθευση της υπογραφής. Μάλιστα, η διαφορά εδώ είναι πολύ μεγαλύτερη καθώς για το επίπεδο ασφαλείας 128 bit (ECC_256/RSA_3072) ο RSA είναι 29 φορές πιο γρήγορος από την ECC. Επίσης, παρατηρούμε πως ο RSA δεν επηρεάζεται τόσο δραστικά από την αύξηση του μήκους κλειδιού σε σχέση με την ECC, καθώς για διπλασιασμό του κλειδιού ο χρόνος της ECC αυξήθηκε κατά 4.8 φορές ενώ του RSA κατά 3.6.

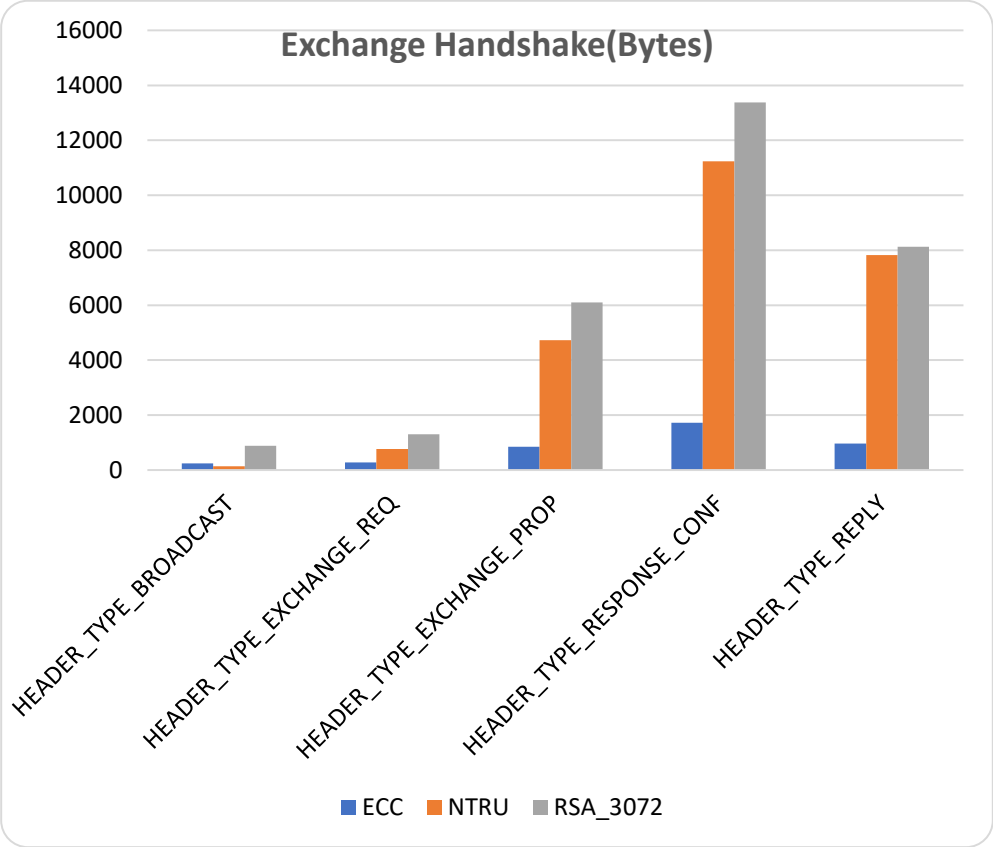
7.1.7 Μέγεθος Μηνυμάτων

Για την προσομοίωση της επικοινωνίας του δικτύου και την ανταλλαγή των ψευδωνύμων χρησιμοποιήθηκαν διαφορετικοί τύποι μηνυμάτων, οι οποίοι αναλύονται ως εξής:

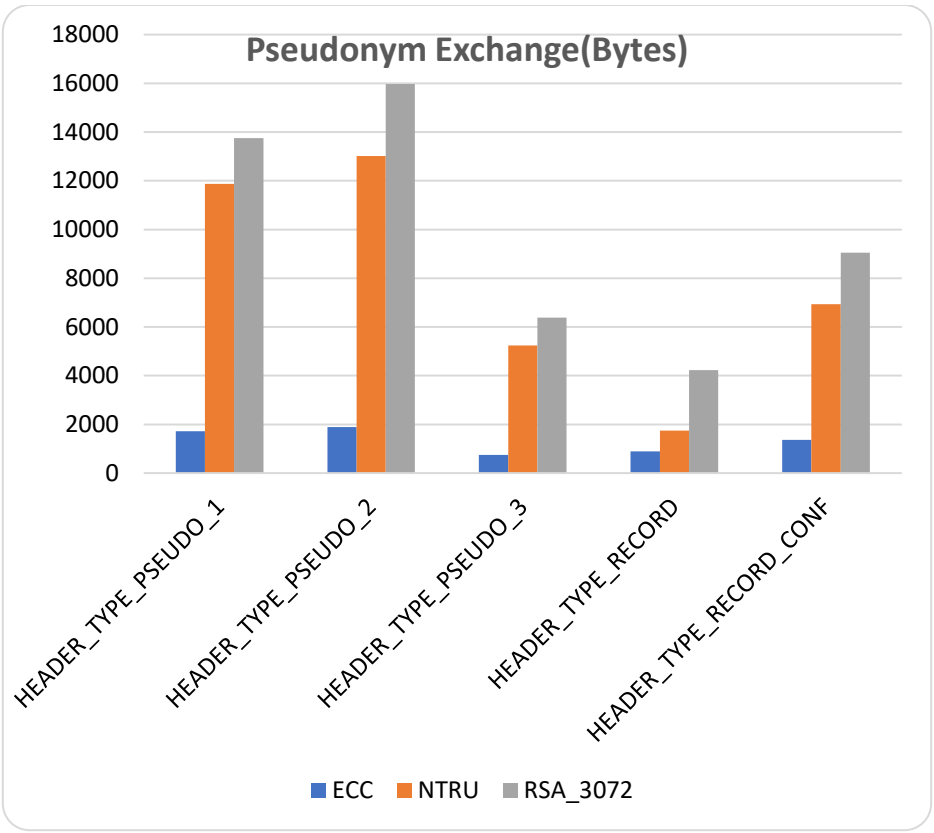
- **HEADER_TYPE_BROADCAST**: Το μήνυμα ασφαλείας που εκπέμπουν περιοδικά τα οχήματα. Αποτελείται από τις πληροφορίες θέσης, την υπογραφή τους και το πιστοποιητικό της ομάδας που ανήκει το όχημα.
- **HEADER_TYPE_EXCHANGE_REQ:** Είναι το αίτημα ανταλλαγής που στέλνει ένα όχημα Α που θέλει να αυξήσει την ιδιωτικότητά του. Αποτελείται από το προσωρινό δημόσιο κλειδί και πιστοποιητικό του αποστολέα, το πιστοποιητικό της ομάδας και ένα timestamp.
- **HEADER_TYPE_EXCHANGE_PROP:** Η πρόταση ανταλλαγής που στέλνει ένα όχημα Β πρόθυμο να ανταλλάξει με ένα τυχαίο γείτονά Α. Αποτελείται από το δημόσιο κλειδί του και το κρυπτογραφημένο πιστοποιητικό μαζί με την υπογραφή και το timestamp.
- **HEADER_TYPE_RESPONSE_CONF:** Εφόσον η πρόταση ανταλλαγής επαληθευτεί και είναι ωφέλιμη για το όχημα Α, αποστέλλεται αυτό το μήνυμα το οποίο περιλαμβάνει το δημόσιο κλειδί του Β και κρυπτογραφημένες όλες τις πληροφορίες που θα χρειαστούν στην ανταλλαγή, δηλαδή το δημόσιο κλειδί και πιστοποιητικό ανταλλαγής του Α μαζί με τις κατάλληλες υπογραφές και timestamps.
- **HEADER_TYPE_REPLY:** Η απάντηση στο προηγούμενο μήνυμα και περιλαμβάνει τα αντίστοιχα στοιχεία από την πλευρά του Β (κλειδί και πιστοποιητικό ανταλλαγής, υπογραφές, timestamp).
- **HEADER_TYPE_PSEUDO_1:** Το μήνυμα με τα στοιχεία του οχήματος Α (ταυτότητα, πιστοποιητικό, υπογραφή), όλα κρυπτογραφημένα με το δημόσιο κλειδί ανταλλαγής του Β.
- **HEADER_TYPE_PSEUDO_2:** Το αντίστοιχο μήνυμα με τα στοιχεία του Β, κρυπτογραφημένα με το δημόσιο κλειδί του Α. Εδώ περιλαμβάνεται και η πρώτη διπλή υπογραφή, δηλαδή η υπογραφή των δεδομένων που έστειλε ο Α.
- **HEADER_TYPE_PSEUDO_3:** Η απάντηση επαλήθευσης του Α, κατά την οποία αποστέλλονται κρυπτογραφημένες η διπλή υπογραφή και η χρονική στιγμή που έλαβε χώρα η ανταλλαγή.
- **HEADER_TYPE_RECORD:** Αυτό το μήνυμα το ανταλλάσουν ο Α με το Β και περιλαμβάνει τα πιστοποιητικά ανταλλαγής και των 2 μαζί με τις ταυτότητες που ανταλλάχθηκαν. Όλο το μήνυμα είναι κρυπτογραφημένο με το δημόσιο κλειδί του RA.
- **HEADER_TYPE_RECORD_CONF:** Μήνυμα επαλήθευσης ότι τα 2 records που έχουν τα οχήματα Α και Β είναι πανομοιότυπα.
- **HEADER_TYPE_RSU_BROADCAST:** Μήνυμα που εκπέμπει κατά περιόδους κάθε RSU προς όλα τα οχήματα στην εμβέλειά της, με την θέση της και το δημόσιο κλειδί της.
- **HEADER_TYPE_RSU_ACTIVATION:** Μήνυμα που αποστέλλει ένα όχημα που θέλει να ενεργοποιήσει το νέο του ψευδώνυμο στην πιο κοντινή RSU και περιλαμβάνει κρυπτογραφημένα με το δημόσιο κλειδί του RA όλα τα δεδομένα της ανταλλαγής.

- **HEADER_TYPE_RA_ACTIVATION:** Αυτό είναι το μήνυμα που προωθεί η RSU στον RA και είναι ίδιο με το HEADER_TYPE_RSU_ACTIVATION.
- **HEADER_TYPE_RA_NEW_KEYS:** Η απάντηση του RA στην αίτηση ενεργοποίησης ενός οχήματος. Περιλαμβάνει την νέα ταυτότητα του οχήματος μαζί με το ζεύγος κλειδιών και το πιστοποιητικό της. Όλα τα δεδομένα είναι κρυπτογραφημένα με το δημόσιο κλειδί του οχήματος.

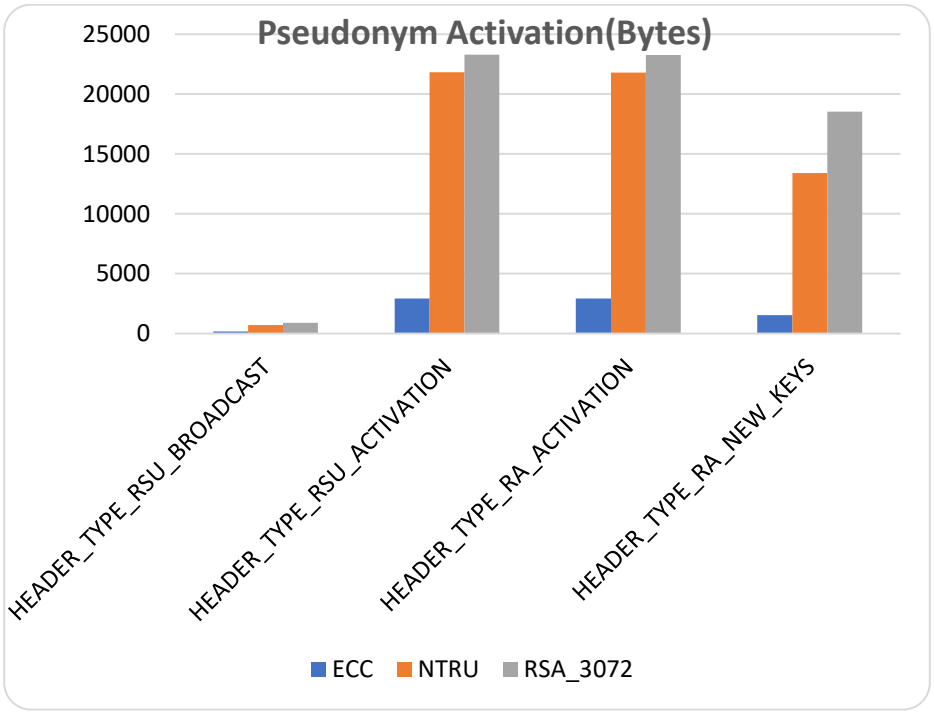
Στα διαγράμματα που ακολουθούν φαίνεται το μέγεθος κάθε τύπου μηνύματος όπως μετρήθηκε στις προσομοιώσεις:



Εικόνα 23: Μέγεθος μηνυμάτων(Bytes) στη φάση διαπραγμάτευσης



Εικόνα 24: Μέγεθος μηνυμάτων(bytes) στη φάση ανταλλαγής ψευδωνύμων

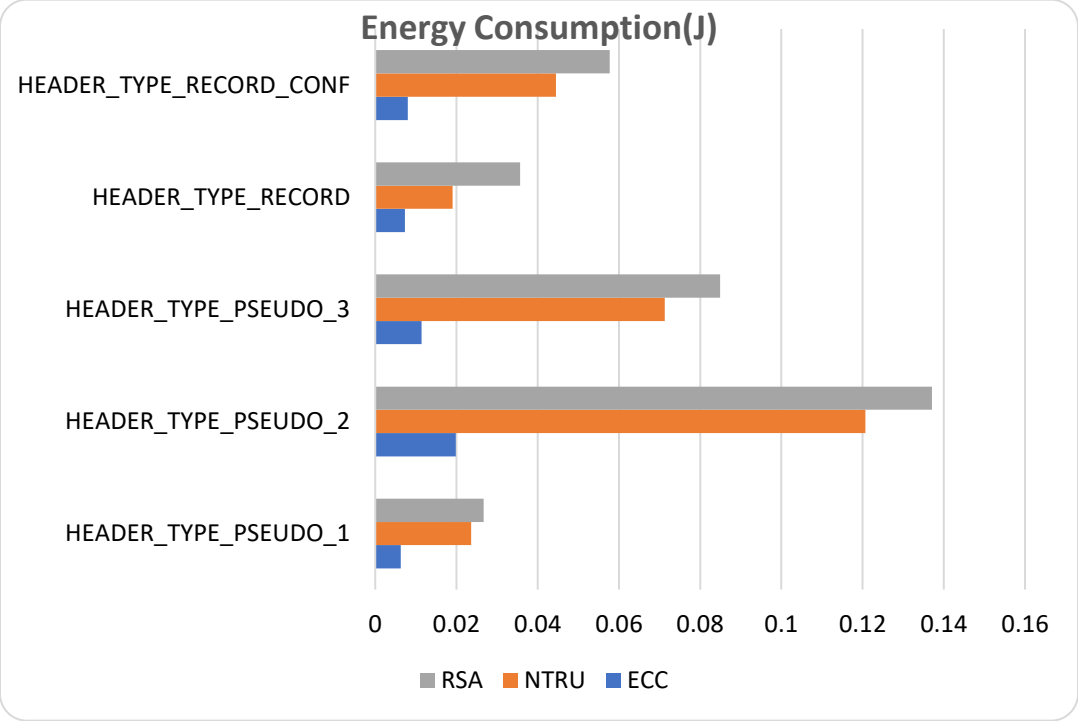


Εικόνα 25: Μέγεθος μηνυμάτων(bytes) στη φάση ενεργοποίησης νέου ψευδωνύμου

Παρατηρείται πως η ECC παράγει μακράν το μικρότερο μέγεθος μηνυμάτων, το οποίο είναι εύκολα κατανοητό δεδομένου ότι τα μηνύματα αυτά εμπεριέχουν σε πολλά σημεία τα κλειδιά και τα πιστοποιητικά που χρησιμοποιούνται. Η μεταφορά των κρυπτογραφικών πληροφοριών ευθύνεται για το μεγαλύτερο μέρος του κάθε μηνύματος επομένως είναι άρρηκτα συνδεδεμένη με τα μεγέθη που χρησιμοποιεί κάθε αλγόριθμος. Το μήκος δημοσίου κλειδιού για την ECC είναι 33 bytes, για την NTRU είναι 623 και για τον RSA 384. Με βάση αυτά τα νούμερα, είναι λογική η διαφορά που παρατηρείται ανάμεσα στην ECC και τον RSA. Όσον αφορά στην NTRU, δεν έχει ληφθεί υπόψιν στο μέγεθος μηνυμάτων κάποια μέθοδος ψηφιακής υπογραφής, το οποίο σημαίνει πως σε ένα ρεαλιστικό σενάριο το μέγεθος μηνυμάτων θα ήταν ακόμα μεγαλύτερο.

7.1.8 Κατανάλωση Ενέργειας

Για τις μετρήσεις ενέργειας επικεντρωθήκαμε στο στάδιο ανταλλαγής ψευδωνύμων για την μέτρηση της κατανάλωσης ενέργειας(μετρημένη σε Joule) καθώς είναι το πιο σταθερό στάδιο. Στο στάδιο της διαπραγμάτευσης υπάρχει διακύμανση των μηνυμάτων που λαμβάνονται και στέλνονται, καθώς κάποια οχήματα μπορεί να μην ανταλλάξουν και άλλα μπορεί να στείλουν σε πολλούς αιτήσεις. Το στάδιο ενεργοποίησης από την άλλη αφορά κυρίως τους κόμβους υποδομής και τα οχήματα δεν έχουν τόσο μεγάλο φορτίο επομένως δεν έχει τόσο ενδιαφέρον η κατανάλωση ενέργειας για εκείνα τα μηνύματα. Παρακάτω φαίνονται τα αποτελέσματα για το στάδιο ανταλλαγής ψευδωνύμων:

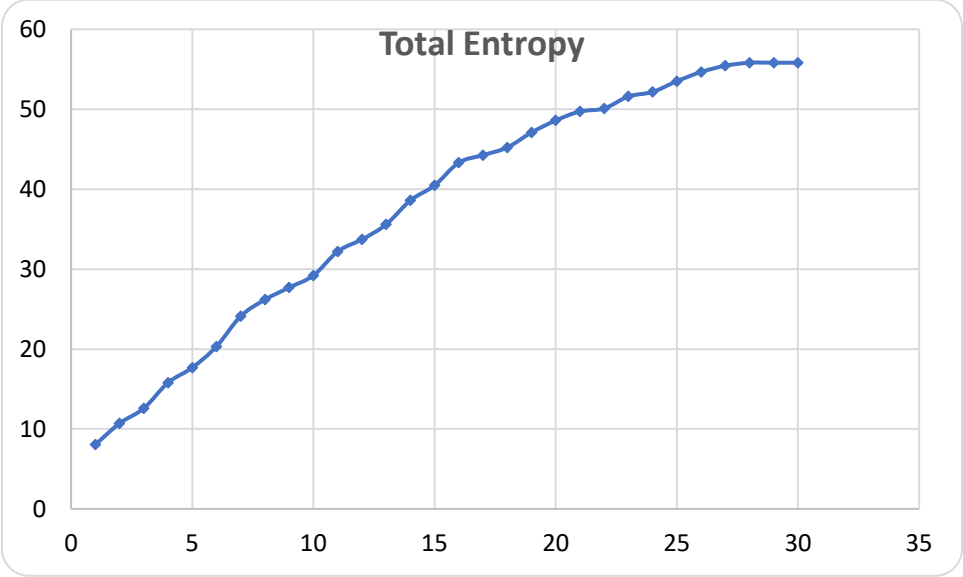


Εικόνα 26: Κατανάλωση ενέργειας(Joule) στη φάση ανταλλαγής ψευδωνύμων

Παρατηρείται πως τη μεγαλύτερη κατανάλωση ενέργειας την έχει ο RSA, ακολουθούμενος από την NTRU, με την ECC να έχει μακράν την χαμηλότερη κατανάλωση. Συγκρίνοντας με τα διαγράμματα μεγέθους, υπάρχει μια ξεκάθαρη συσχέτιση μεταξύ του μεγέθους του μηνύματος και της κατανάλωσης ενέργειας. Αυτή η συσχέτιση ενδεχομένως να σχετίζεται με το fragmentation που υφίσταται τα πακέτα, το οποίο λόγω μεγέθους εμφανίζεται περισσότερο στις υλοποιήσεις με NTRU και RSA, και αυξάνει την κατανάλωση ενέργειας.

7.1.9 Εντροπία Ψευδωνύμων

Για την πειραματική μέτρηση της εντροπίας του συστήματος χρησιμοποιήσαμε τις σχέσεις που περιγράφηκαν στο κεφάλαιο 5, θεωρώντας ένα σταθερό αριθμό από 5 εσωτερικούς επιτιθέμενους, οι οποίοι μηδένιζαν την εντροπία των οχημάτων με τα οποία αντάλλασσαν. Πήραμε μετρήσεις για 150 οχήματα σε βάθος χρόνου 30 δευτερολέπτων.



Εικόνα 27: Συνολική εντροπία των οχημάτων στο χρόνο(s)

Παρατηρείται πως η εντροπία του συστήματος αυξάνεται πολύ γρήγορα στην αρχή, και με την πάροδο του χρόνου σταθεροποιείται. Αυτό οφείλεται στο ότι καθώς περνάει ο χρόνος, όλο και περισσότερα οχήματα φτάνουν στο επιθυμητό επίπεδο ανωνυμίας.

7.2 Συμπεράσματα

Με βάση τα πειραματικά αποτελέσματα του κεφαλαίου 6.1, μπορούμε να εξάγουμε κάποια συμπεράσματα σχετικά με τη πιθανή βελτιστοποίηση της λειτουργίας του σχήματος MixGroup μέσω διαφορετικών τεχνικών κρυπτογράφησης. Στην συνέχεια του κεφαλαίου αναφέρονται οι παρατηρήσεις για κάθε μια από τις μεθόδους που ακολουθήθηκαν.

7.2.1 NTRU

Για το επίπεδο ασφαλείας που μελετήσαμε, η υλοποίηση NTRU ήταν η ταχύτερη στην παραγωγή κρυπτογραφικών κλειδιών. Σε ένα σύστημα IoV, υπεύθυνος για αυτή τη διαδικασία είναι ο RA, ο οποίος τα παράγει κατά την αρχικοποίηση του συστήματος. Όμως, κατά τη λειτουργία του συστήματος μπορεί να χρειαστεί να δημιουργηθούν εκ νέου κλειδιά, π.χ. λόγω της εισόδου ενός νέος οχήματος ή της διαρροής ενός σετ κλειδιών, στην οποία περίπτωση η διαδικασία θα πρέπει να γίνεται όσο το δυνατόν πιο γρήγορα, κάνοντας την NTRU μια δελεαστική επιλογή. Ακόμα, όσον αφορά στην κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος, ο αλγόριθμος NTRUEncrypt παρέχει πολύ ανώτερη απόδοση συγκριτικά με τους άλλους 2 αλγορίθμους. Αυτό τον κάνει ιδιαίτερα ελκυστικό, καθώς ο χρόνος απόκρισης σε ένα μήνυμα θα πρέπει να είναι ο ελάχιστος δυνατός και επομένως είναι επιθυμητή η όσο δυνατόν μικρότερη καθυστέρηση στην κρυπτογράφηση και αποκρυπτογράφηση.

Από την άλλη πλευρά η χρήση του αλγορίθμου αυτού συνεπάγεται μια ξεκάθαρη επιβάρυνση στο μέγεθος των μηνυμάτων, η οποία μπορεί να οδηγήσει σε συμφόρηση του δικτύου. Επίσης, παρατηρήθηκε σημαντική κατανάλωση ενέργειας στα οχήματα, το οποίο υποδηλώνει μεγαλύτερο φόρτο στο υλικό ή ακόμα και εξάντληση των πόρων των οχημάτων, τα οποία σε πραγματικά σενάρια έχουν περιορισμένες δυνατότητες υλικού. Αξιοσημείωτη ακόμα είναι η έλλειψη ευρέως αποδεκτών υλοποιήσεων ψηφιακής υπογραφής με χρήση NTRU, καθώς αναμένεται ακόμα η προτυποποίηση τους από διεθνείς οργανισμούς όπως ο NIST. Αυτό καθιστά την υλοποίηση του πλήρους φάσματος των κρυπτογραφικών διαδικασιών του σχήματος MixGroup με NTRU προς το παρόν ριψοκίνδυνη, καθώς οι ψηφιακές υπογραφές είναι ένα πολύ σημαντικό στοιχείο του σχήματος.

7.2.2 RSA

Τα αποτελέσματα που πήραμε από τις προσομοιώσεις μας σχετικά με τον αλγόριθμο RSA επιβεβαιώνουν τη γνωστή συμπεριφορά του. Στον τομέα της παραγωγής κλειδιών είχε πολύ χαμηλή απόδοση, όπως και στην αποκρυπτογράφηση μηνυμάτων, όπου ήταν ο πιο αργός από τους 3 αλγορίθμους. Αντίθετα, στην κρυπτογράφηση μηνυμάτων είχε την καλύτερη απόδοση, ισοσταθμίζοντας την καθυστέρηση στην αποκρυπτογράφηση συνολικά, δεδομένου ότι συνήθως αυτές οι 2 διαδικασίες συνυπολογίζονται λόγω του ότι κάθε μήνυμα που κρυπτογραφείται πρέπει και να αποκρυπτογραφείται. Αυτή η παραδοχή ισχύει και στο σύστημα που μελετήσαμε, καθώς τα οχήματα μπορούν να ξεχωρίσουν ποια μηνύματα τα αφορούν ώστε να μη χάσουν χρόνο σε άσκοπους υπολογισμούς. Στην περίπτωση που είχαμε 1 κρυπτογραφημένο μήνυμα προς πολλούς παραλήπτες, τότε θα είχαμε και μεγάλο κόστος λόγω

της φύσης του RSA. Ομοίως, η παραγωγή μιας ψηφιακής υπογραφής είναι πολύ πιο χρονοβόρα από την επαλήθευσή της. Αυτό, όμως στο συγκεκριμένο σενάριο είναι πλεονέκτημα καθώς όλα τα μηνύματα ασφαλείας υπογράφονται και στη συνέχεια επαληθεύονται, άρα σε ένα σύστημα όπου N οχήματα βρίσκονται σε εμβέλεια επικοινωνίας έχουμε N υπογραφές και N(N-1) επαληθεύσεις. Με το βάρος των υπολογισμών να πέφτει στην επαλήθευση, η χρήση του RSA φαίνεται να πλεονεκτεί έναντι των άλλων 2 αλγορίθμων για τα συγκεκριμένα μηνύματα, που αποτελούν την πλειοψηφία στο σύστημα.

Ένα ακόμα σημαντικό μειονέκτημα του RSA είναι το μέγεθος των κλειδιών που απαιτείται, και το μέγεθος των μηνυμάτων που συνεπάγεται. Όπως και στην περίπτωση του αλγορίθμου NTRU, το μεγάλο μέγεθος των μηνυμάτων και η υψηλότερη κατανάλωση ενέργειας, δρουν αποθαρρυντικά για την υιοθέτησή του στο συγκεκριμένο σχήμα, λόγω των περιορισμένων πόρων αλλά και αποθηκευτικού χώρου. Παρόλα αυτά, υπάρχουν πολλές προτυποποιημένες και βελτιστοποιημένες υλοποιήσεις αυτού του αλγορίθμου, ακόμα και σε επίπεδο ενσωματωμένου υλικού, οπότε λόγω αυτής της πληθώρας υλοποιήσεων παραμένει ακόμα ανταγωνιστικός.

7.2.3 ECC

Με βάση τα πειραματικά δεδομένα, ο αλγόριθμος ECC ήταν πολύ αποδοτικός στην παραγωγή κλειδιών, σε συγκρίσιμο επίπεδο με τον NTRU. Επίσης, στους χρόνους αποκρυπτογράφησης και κρυπτογράφησης παρουσίασε ανάποδη συμπεριφορά από τον RSA, με «αργή» κρυπτογράφηση και «γρήγορη» αποκρυπτογράφηση, με το συνολικό χρόνο να είναι 30% καλύτερος από τον RSA στο επίπεδο ασφαλείας 128 bit. Παρομοίως στις υπογραφές, ήταν πιο αργή στην επαλήθευση από ότι στην υπογραφή με το συνολικό χρόνο να είναι 25% καλύτερος από του RSA για το επίπεδο ασφαλείας 128 bit. Όμως, όπως αναφέρθηκε παραπάνω, ο αργός χρόνος επαλήθευσης αποτελεί σημαντικό μειονέκτημα στην συγκεκριμένη εφαρμογή, καθώς επιβαρύνεται συνολικά το σύστημα.

Το μεγαλύτερο πλεονέκτημα της υλοποίησης με ECC είναι το μέγεθος των κλειδιών και κατά συνέπεια το μέγεθος των μηνυμάτων που παράγονται. Η συγκεκριμένη υλοποίηση είναι μακράν η πιο αποδοτική στην κατανάλωση χώρου και ενέργειας, που είναι 2 πολύ σημαντικοί παράγοντες στους τύπους δικτύων που μελετάμε. Τέλος, οι υλοποιήσεις σε ECC έχουν αρχίσει να αναπτύσσονται και να βελτιστοποιούνται στα τελευταία χρόνια, χωρίς να έχουν φτάσει ακόμα στην πληθώρα που έχει να παρουσιάσει ο RSA αλλά συνεχώς αυξάνεται η υποστήριξη σε εφαρμογές.

7.3 Μελλοντικές Επεκτάσεις

Ένα σημαντικό στοιχείο του MixGroup το οποίο δεν ερευνήσαμε πειραματικά στην παρούσα εργασία, είναι η κοινωνική φύση των οχημάτων και η δημιουργία και διατήρηση ομάδων. Επομένως, μια πιθανή επέκταση είναι η υλοποίηση και προσομοίωση τεχνικών ένταξης σε ομάδες προκειμένου να επαληθεύσουμε περαιτέρω την αξιοπιστία αυτού του μηχανισμού αλλά και να εντοπίσουμε κάποια βελτίωση στο συγκεκριμένο μοντέλο.

Μια ακόμα μελλοντική επέκταση είναι η εξέταση μιας υλοποίησης ψηφιακής υπογραφής με χρήση NTRU, προκειμένου να έχουμε μια καλύτερη απεικόνιση της επίδοσής της. Αναμένεται σύντομα ο NIST να προτυποποιήσει μια τέτοια μέθοδο, καθώς τον Ιούλιο του 2020 ανακοίνωσε πως 2 υλοποιήσεις βρίσκονται στον $3^{ο}$ γύρο αξιολόγησης[46]. Αν κάποια από αυτές γίνει τελικά δεκτή, μπορεί να χρησιμοποιηθεί στην έρευνά μας σε συνδυασμό με την NTRUEncrypt προκειμένου να εξεταστεί η αποδοτικότητα της από άκρη σε άκρη.

Το σύστημα προσομοιώσεων που χρησιμοποιήθηκε, παρά την πληθώρα των εφαρμογών που υποστηρίζει, παρουσιάζει κάποιους εγγενείς περιορισμούς. Ένα πολύ σημαντικό ζήτημα που αντιμετωπίσαμε ήταν ο συγχρονισμός των οχημάτων και η απώλεια πακέτων λόγω συγκρούσεων. Για αυτό το λόγο, μια πολύ σημαντική μελλοντική επέκταση είναι η δημιουργία ενός πειραματικού δικτύου οχημάτων στο φυσικό κόσμο με σκοπό την επαλήθευση των αποτελεσμάτων μας σε πραγματικά δεδομένα. Ως φυσικό επακόλουθο της προηγούμενης επέκτασης έρχεται η δοκιμή των υλοποιήσεων σε μεγαλύτερες τοπολογίες, με σκοπό την βελτίωση των μηχανισμών ιδιωτικότητας προκειμένου να προλάβουμε τις απαιτήσεις ασφαλείας και ιδιωτικότητας που αυξάνονται με την ανάπτυξη του IoV.

Κεφάλαιο 8: Επίλογος

Στα πλαίσια της παρούσας διπλωματικής εργασίας εξετάστηκε η επίδραση διαφορετικών κρυπτογραφικών τεχνικών πάνω σε δίκτυα οχημάτων. Ξεκινήσαμε από την συνοπτική παρουσίαση και επεξήγηση των βασικών θεωρητικών εννοιών δικτύων, κρυπτογραφίας, ασφάλειας και ιδιωτικότητα. Έπειτα, ακολούθησε μια βιβλιογραφική παρουσίαση και αξιολόγηση των διαφορέτικων μεθόδων ιδιωτικότητας που έχουν προταθεί για τους συγκεκριμένους τύπους δικτύων, καθώς επίσης και των εργαλείων και κρυπτογραφικών μεθόδων που χρησιμόποιησαμε. Ιδιαίτερη έμφαση δόθηκε στον ορισμό των μετρικών αξιολόγησης που χρησιμοποιήσαμε.

Στο πρακτικό σκέλος της εργασίας, αναλύθηκε η προσπάθεια υλοποίησης της τεχνικής MixGroup με τη δυνατότητα υποστήριξης 3 διακριτών κρυπτογραφικών μοντέλων: RSA, ECC και NTRU. Επιπλέον, παρουσιαστήκαν και αναλύθηκαν τα πειραματικά αποτελέσματα που προέκυψαν από τις προσομοιώσεις που εκτελέσαμε για κάθε διαφορετικό κρυπτογραφικό μοντέλο για τις μετρικές που είχαμε ορίσει. Από αυτά τα αποτελέσματα εξήγαμε συμπεράσματα για την καταλληλότητα κάθε μεθόδου στη συγκεκριμένη εφαρμογή και για πιθανά οφέλη και περιορισμούς ανά μέθοδο. Τέλος, προτάθηκαν μερικές μελλοντικές επεκτάσεις πάνω στην παρούσα εργασία, προκειμένου να κατανοήσουμε καλύτερα τη φύση αυτών των τεχνικών και να πετύχουμε ακόμα και κάποια βελτιστοποίηση στην ιδιωτικότητα των δικτύων οχημάτων.

Κεφάλαιο 9: Βιβλιογραφία

[1] W. Diffie, M. E. Hellman, “Multiuser cryptographic techniques”, AFIPS ’76, national computer conference and exposition, pp. 109-112, June 1976

[2] https://en.wikipedia.org/wiki/OSI_model

[3] J. Kurose, K. Ross, Computer Networking: A Top-Down Approach(6th edition), 2013

[4] https://en.wikipedia.org/wiki/IEEE_802.11p

[5] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, Computer Networks, Vol. 76, 2015, pp. 146-164

[6] Z. A. Abdulkader, A. Abudllah, M. T. Abudllah, Z. A. Zukarnain, “Vehicular Ad Hoc Networks and Scurity Issues: Survey”, Modern Applied Science, Vol. 11, No. 5, 2017

[7] P. Asuquo, H. Cruckshank, J. Morley, C. P. Anyigor Ogah, A. Lei, W. Hathal, S. Bao, Z. Sun, “Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures”, IEEE Internet of Things Journal, Vol. 5, No. 6, December 2018

[8] M. S. Sheikh, J. Liang, W. Wang, “Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey”, Hindawi, Wireless Communications and Mobile Computing, Volume 2020, Article ID 5129620, 25 pages, 2020

[9] R. G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, “VANET security surveys”, Computer Communications, Vol. 44, 2014, pp. 1-13

[10] M. Raya, J.-P. Hubaux, “Securing vehicular ad hoc networks”, Journal of Computer Security 15 (2007), pp. 39-68

[11] C.-K Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Prentice-Hall, 2001

[12] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," in *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46-55, Jan.-March 2003

[13] B. Palanisamy and L. Liu, "Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495-508, 1 March 2015

[14] J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, “Mix-Zones for Location Privacy in Vehicular Networks”, In Association for Computing Machinery (ACM) Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007

[15] F. Scheuer, K.-P. Fuchs, H. Federrath, “A Safety-Preserving Mix Zone for VANETs”, Trust, Privacy and Security in Digital Business, 2011, Volume 6863, pp. 37-48

[16] B. Ying, D. Makrakis and H. T. Mouftah, "Dynamic Mix-Zone for Location Privacy in Vehicular Networks," in *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524-1527, August 2013

[17] J. Guo, J. P. Baugh and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," *2007 Mobile Networking for Vehicular Environments*, Anchorage, AK, 2007, pp. 103-108

[18] Hefeng Chen, Wenping Ma, Youjiao Zou and Changxia Sun, "Strongly secure group signature scheme," *2014 Communications Security Conference (CSC 2014)*, Beijing, 2014, pp. 1-8

[19] M. Xia and X. Sun, "An Efficient Group Signatures Based on Discrete Logarithm," *2009 International Conference on Wireless Networks and Information Systems*, Shanghai, 2009, pp. 50-53

[20] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606-1617, May 2010

[21] M. Park, G. Gwon, S. Seo and H. Jeong, "RSU-Based Distributed Key Management (RDKM) For Secure Vehicular Multicast Communications," in *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 644-658, March 2011

[22] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," in *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569-1589, Oct. 2007

[23] Leping Huang, K. Matsuura, H. Yamane and K. Sezaki, "Enhancing wireless location privacy using silent period," *IEEE Wireless Communications and Networking Conference, 2005*, New Orleans, LA, 2005, pp. 1187-1192 Vol. 2

[24] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "CARAVAN: Providing Location Privacy for VANET," in Proceedings of the Embedded Security in Cars (ESCAR) Workshop, Cologne, Germany, November 2005

[25] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," *2013 IEEE Vehicular Networking Conference*, Boston, MA, 2013, pp. 71-78

[26] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang and S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93-105, 1 Jan.-Feb. 2016

[27] https://www.nsnam.org/

[28] https://www.eclipse.org/sumo/

[29] D. Krajzewics, J. Erdmann, M. Behrisch, L. Bieker, “Recent Development and Applications of SUMO – Simulation of Urban Mobility”, International Journal on Advances in Systems and Measurements, issn 1942-261x, vol. 5, no. 3&4, year 2012, pp. 128-137.

[30] https://www.nsnam.org/wiki/NetAnim_3.108

[31] https://pyviz.org/

[32] https://www.tcpdump.org/manpages/tcpdump.1.html

[33] C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer-Verlag New York Inc, 2010

[34] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120–126.

[35] Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science, vol 1423. Springer, Berlin, Heidelberg

[36] H. B. Nguyen, “An Overview of the NTRU Cryptographic System”, Thesis, San Diego State University, Fall 2014

[37] Ducas L., Nguyen P.Q. (2012) Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures. In: Wang X., Sako K. (eds) Advances in Cryptology – ASIACRYPT 2012. ASIACRYPT 2012. Lecture Notes in Computer Science, vol 7658. Springer, Berlin, Heidelberg

[38] Serjantov A., Danezis G. (2003) Towards an Information Theoretic Metric for Anonymity. In: Dingledine R., Syverson P. (eds) Privacy Enhancing Technologies. PET 2002. Lecture Notes in Computer Science, vol 2482. Springer, Berlin, Heidelberg

[39] C. E. Shannon, "A mathematical theory of communication," in *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379-423, July 1948

[40] A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," *IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second*, Orlando, FL, USA, 2004, pp. 127-131

[41] https://www.cryptopp.com/

[42] https://github.com/arekinath/easy-ecc

[43] https://github.com/NTRUOpenSourceProject/ntru-crypto

[44] https://linux.die.net/man/4/urandom

[45] https://www.nsnam.org/docs/models/html/energy.html

[46] https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement