ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΕΝΤΡΟΠΟΙΗΜΕΝΟ ΣΥΣΤΗΜΑ ΑΙΣΘΗΤΗΡΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΔΙΚΤΥΟΥ ΓΙΑ ΕΞΥΠΝΗ ΠΟΛΗ

ΔΗΜΗΤΡΟΠΟΥΛΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΑΡΣΕΝΙΟΣ

Επιβλέπων: Αθανάσιος Δ. Παναγόπουλος

Καθηγητής Ε.Μ.Π

Αθήνα, Σεπτέμβριος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΕΝΤΡΟΠΟΙΗΜΕΝΟ ΣΥΣΤΗΜΑ ΑΙΣΘΗΤΗΡΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ ΔΙΚΤΥΟΥ ΓΙΑ ΕΞΥΠΝΗ ΠΟΛΗ

ΔΗΜΗΤΡΟΠΟΥΛΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ ΑΡΣΕΝΙΟΣ

Επιβλέπων: Αθανάσιος Δ. Παναγόπουλος

Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 21η Σεπτεμβρίου 2023

.....	.....	.....
Αθ. Παναγόπουλος	**Γ. Ματσόπουλος**	**Γ. Φικιώρης**
Καθηγητής Ε.Μ.Π.	**Καθηγητής Ε.Μ.Π.**	**Καθηγητής Ε.Μ.Π.**

Αθήνα, Σεπτέμβριος 2023

.....

Κωνσταντίνος Αρσένιος Δημητρόπουλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός & Μηχανικός Υπολογιστών Ε.Μ.Π

Περίληψη

Στην παρούσα διπλωματική εργασία γίνεται προσπάθεια να αναλυθεί το πρόβλημα της υλοποίησης ενός κεντροποιημένου συστήματος αισθητήρων ανίχνευσης εισβολών δικτύου για έξυπνη πόλη.

Αρχικά στο κεφάλαιο 1 μέσω μιας εκτενούς βιβλιογραφικής ανασκόπησης μελετήθηκαν πρωτοβουλίες ανάπτυξης έξυπνων πόλεων και αναλύθηκαν τα θεωρητικά κομμάτια της διπλωματικής όπως είναι οι έννοιες των ασύρματων δικτύων των αισθητήρων και της διαχείρισης των Big Data.

Στη συνέχεια στο κεφάλαιο 2 επικεντρώσαμε το ενδιαφέρον μας στα θέματα ασφάλειας σε συνδυασμό με τις επιθέσεις σε ασύρματα δίκτυα αισθητήρων. Γίνεται επίσης αναφορά στα βασικά αντίμετρα αυτών των επιθέσεων.

Στο κεφάλαιο 3 περνάμε στην παρουσίαση της αρχιτεκτονικής ενός δικτύου αισθητήρων ανίχνευσης ανωμαλιών και αναλύουμε το σενάριο μιας εισβολής.

Μεγάλο κομμάτι της παρούσας διπλωματικής εργασίας είναι αφιερωμένο στην έννοια της ανθεκτικότητας (resiliency) των έξυπνων πόλεων και στο πώς συνδυάζεται η τελευταία με τη διαχείριση των μεγάλων δεδομένων. Οι παράγοντες και τα εμπόδια για την υιοθέτηση της ανάλυσης μεγάλων δεδομένων παρουσιάζονται στο κεφάλαιο 4.

Τέλος, στο κεφάλαιο 5 εκτίθενται κάποια θέματα κυβερνοασφάλειας των έξυπνων πόλεων και μία σειρά από συστήματα ανίχνευσης και πρόληψης εισβολών.

Λέξεις Κλειδιά

Έξυπνη Πόλη, Ασύρματα Δίκτυα Αισθητήρων, Αρχιτεκτονική Δικτύου Ανίχνευσης Ανωμαλιών, Ανθεκτικότητα, Κυβερνοασφάλεια

Abstract

In this thesis, an attempt is made to analyse the problem of implementing a centralized network intrusion detection sensor system for smart city.

Initially in chapter 1 through an extensive literature review, smart city development initiatives were studied and the theoretical parts of the thesis such as the concepts of wireless sensor networks and Big Data management were analysed.

Then in chapter 2 we focused on security issues in connection with attacks on wireless sensor networks. We also discuss the key countermeasures of these attacks.

In chapter 3 we move on to present the architecture of an anomaly detection sensor network and analyse the scenario of an intrusion.

A large part of this thesis is devoted to the concept of resiliency of smart cities and how the latter is combined with big data management. The factors and barriers to the adoption of big data analytics are presented in chapter 4.

Finally, Chapter 5 exposes some cybersecurity issues of smart cities and a number of intrusion detection and prevention systems.

Key-Words

Smart City, Wireless Sensor Networks, Anomaly Detection Network Architecture, Resilience, Cybersecurity

Ευχαριστίες

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή κ. Αθανάσιο Παναγόπουλο, για την καθοδήγηση και τις συμβουλές που μου παρείχε, σε όλα τα στάδια εκπόνησης της παρούσας διπλωματικής εργασίας.

Για την πίστη και τη στήριξη που μου παρείχαν οι κοντινοί μου άνθρωποι, οικογένεια & φίλοι, οφείλω το μεγαλύτερο ευχαριστώ.

Περιεχόμενα

Κατάλογος Σχημάτων-Πινάκων

1 ΕΙΣΑΓΩΓΗ

Τις επόμενες δεκαετίες, οι πόλεις αντιμετωπίζουν νέες προκλήσεις που χαρακτηρίζουν τις σύγχρονες κοινωνίες: γήρανση του πληθυσμού, μείωση της κατανάλωσης ενέργειας και των εκπομπών διοξειδίου του άνθρακα, αγώνας για μεγαλύτερη βιωσιμότητα, οικονομική ανάπτυξη κ.λπ. Επιπλέον, οι μεταναστευτικές κινήσεις αυξάνουν με ταχείς ρυθμούς το μέγεθος των πόλεων. Σήμερα, το 50% του παγκόσμιου πληθυσμού ζει σε πόλεις και προβλέπεται ότι μέχρι το 2050 το ποσοστό αυτό θα είναι περίπου 70% [1].

Για την αντιμετώπιση αυτών των προκλήσεων, έχουν εμφανιστεί πρωτοβουλίες για έξυπνες πόλεις, οι οποίες προτείνουν νέους τρόπους θεώρησης της ανάπτυξης και της διαχείρισης των πόλεων. Επί του παρόντος, δεν υπάρχει ένας διεθνώς αποδεκτός ορισμός της έξυπνης πόλης. Ωστόσο, οι συγγραφείς του [2] έχουν προτείνει έναν ορισμό που έχει γίνει δημοφιλής: Πιστεύουμε ότι μια πόλη είναι έξυπνη όταν οι επενδύσεις στο ανθρώπινο και κοινωνικό κεφάλαιο και οι παραδοσιακές (μεταφορές) και σύγχρονες (ΤΠΕ) υποδομές επικοινωνίας τροφοδοτούν τη βιώσιμη οικονομική ανάπτυξη και την υψηλή ποιότητα ζωής, με συνετή διαχείριση των φυσικών πόρων, μέσω συμμετοχικής διακυβέρνησης.

Γενικά, τα έργα έξυπνων πόλεων έχουν ως στόχο τη βελτίωση του σχεδιασμού των μητροπολιτικών υποδομών, την αυτοματοποίηση των αστικών λειτουργιών, τη μείωση του κόστους, την αύξηση της ανταγωνιστικότητας της πόλης, το άνοιγμα νέων επιχειρηματικών γραμμών, τη δημιουργία θέσεων εργασίας και την ενίσχυση της διαφάνειας και του ανοίγματος [3]. Ανάλογα με τις συγκεκριμένες ανάγκες, κάθε πόλη υλοποιεί πρωτοβουλίες έξυπνης πόλης που εστιάζουν σε διαφορετικούς τομείς. Το Smart City Project , το οποίο στοχεύει στη σκιαγράφηση και τη συγκριτική αξιολόγηση μεσαίων και μεγάλων πόλεων στην Ευρώπη (έχει καλύψει σχεδόν 1.600 πόλεις), έχει προτείνει ένα μοντέλο έξυπνης πόλης που περιλαμβάνει έξι βασικούς τομείς: έξυπνη οικονομία, έξυπνη κινητικότητα, έξυπνο περιβάλλον, έξυπνοι άνθρωποι, έξυπνη διαβίωση και έξυπνη διακυβέρνηση. Από αυτόν τον κατάλογο, οι ευρωπαϊκές πόλεις εφαρμόζουν κυρίως το έξυπνο περιβάλλον και την έξυπνη κινητικότητα [4].

Από τεχνολογική άποψη, τα πληροφοριακά συστήματα αναπτύσσονται για να μετασχηματίσουν τη διαχείριση των υποδομών προς μια προσέγγιση με βάση τα δεδομένα, ακολουθώντας τέσσερα βασικά δομικά στοιχεία: δεδομένα, ανάλυση, ανατροφοδότηση και προσαρμοστικότητα [5]. Για την τροφοδότηση των πληροφοριακών συστημάτων, οι έξυπνες πόλεις χρησιμοποιούν στοιχεία του Διαδικτύου των πραγμάτων (IoT: Internet of Things) ως κύρια πηγή δεδομένων, όπως κινητά τηλέφωνα, κάρτες αναγνώρισης ραδιοσυχνοτήτων (RFID: Radio Frequency Identification) και ασύρματα δίκτυα αισθητήρων (WSN: Wireless Sensor Networks). Τα δεδομένα που συλλέγονται από τα τελευταία χρησιμοποιούνται σε πληθώρα εφαρμογών. Για παράδειγμα, οι αισθητήρες παρακολούθησης της κυκλοφορίας χρησιμοποιούνται για τον έλεγχο των φωτεινών σηματοδοτών [6] και οι ασύρματοι μετρητές εγκαθίστανται σε σωλήνες για την παρακολούθηση διαρροών και ρήξεων [7]. Επιπλέον, τα δεδομένα αυτά δίνουν στους διαχειριστές των πόλεων και σε άλλους ενδιαφερόμενους την ευκαιρία να σχεδιάσουν μελλοντικές εγκαταστάσεις με βάση μια καλύτερη εικόνα της συμπεριφοράς των πολιτών και της πραγματικής χρήσης των υφιστάμενων υποδομών. Τα σαφή οφέλη που παρέχει η τεχνολογία των έξυπνων πόλεων έχουν ωθήσει πολλές πόλεις να αφιερώσουν σημαντικό μέρος των προσπαθειών τους για καινοτομία στην ανάπτυξη της έννοιας της έξυπνης πόλης.

Αυτό προκάλεσε σημαντική και ταχεία αύξηση του αριθμού των αναπτύξεων WSN στους δρόμους, η οποία είχε ως αποτέλεσμα την εμφάνιση νέων εφαρμογών με πολλές διαφορετικές τεχνολογίες, λύσεις, απαιτήσεις κ.λπ. Ωστόσο, αυτή η επιταχυνόμενη ανάπτυξη της τεχνολογίας της έξυπνης πόλης είχε συχνά ως αποτέλεσμα να παραμεριστεί η ασφάλεια ως δευτερεύον ζήτημα. Για παράδειγμα, ορισμένες μελέτες [8, 9] έχουν αποδείξει ότι τα συστήματα ελέγχου της κυκλοφορίας μπορούν να χειραγωγηθούν σε πραγματικές εφαρμογές στις Ηνωμένες Πολιτείες λόγω της έλλειψης συστημάτων κρυπτογράφησης και ελέγχου ταυτότητας στους αισθητήρες και, γενικά, λόγω της συστηματικής έλλειψης συνείδησης ασφάλειας. Επιπλέον, προκειμένου να αναπτύξουν γρήγορα τα WSNs και την τεχνολογία έξυπνων πόλεων, οι πόλεις έχουν επωφεληθεί από υπηρεσίες

που προμηθεύονται από εξωτερικούς παρόχους. Ωστόσο, η εξωτερική ανάθεση δημόσιων υπηρεσιών έχει επίσης εγείρει ανησυχίες σχετικά με την ασφάλεια [10].

Ο αντίκτυπος αυτών των πολιτικών εξωτερικής ανάθεσης στην ασφάλεια μπορεί να αποδοθεί κυρίως σε δύο βασικούς παράγοντες: την απώλεια ελέγχου επί των συσκευών δικτύου και την έλλειψη ορατότητας σχετικά με τα πιθανά προβλήματα ασφάλειας που επηρεάζουν αυτές τις συσκευές. Πράγματι, οι δημόσιες διοικήσεις αναθέτουν συνήθως σε εξωτερικούς συνεργάτες όχι μόνο την υλοποίηση και την ανάπτυξη των WSN τους, αλλά και τη διαχείρισή τους. Με αυτόν τον τρόπο, τα αντίμετρα ασφαλείας και τα αρχεία καταγραφής συστημάτων διαχειρίζονται αποκλειστικά από εξωτερικούς παρόχους. Παρόλο που οι πάροχοι υπηρεσιών υποχρεούνται συμβατικά να διασφαλίζουν ορισμένα επίπεδα ασφάλειας, στην πράξη, οι διαχειριστές έξυπνων πόλεων δεν μπορούν να προσδιορίσουν το βαθμό στον οποίο τα δεδομένα που λαμβάνουν είναι ακριβή και ακριβή. Στην πραγματικότητα, η Βασιλική Ακαδημία Μηχανικής έχει προσδιορίσει την ποιότητα των δεδομένων ως ένα από τα έξι σημαντικότερα εμπόδια για την αποτελεσματική βελτιστοποίηση των έξυπνων υποδομών [5].

1.1 Πρωτοβουλίες για τις έξυπνες πόλεις

Πόλεις, ιδιωτικές εταιρείες και άλλα ιδρύματα συμμετέχουν ήδη σε έργα έξυπνων πόλεων για να δώσουν λύσεις στις σύγχρονες προκλήσεις που αντιμετωπίζουν οι πόλεις. Στις σελίδες που ακολουθούν περιγράφονται ορισμένες εξέχουσες πρωτοβουλίες.

Το PlanIT Urban Operating System είναι ένα πολυεπίπεδο λειτουργικό σύστημα για αστικά περιβάλλοντα. Το στρώμα ελέγχου του είναι υπεύθυνο για την ανταπόκριση με χαμηλή καθυστέρηση σε περιστατικά στην υποδομή αισθητήρων/ενεργοποιητών. Ένα εποπτικό στρώμα προσφέρει διεπαφές προγραμματισμού εφαρμογών (API), καθώς και ενότητες διαχείρισης, ανάλυσης, αποθήκευσης, προσομοίωσης, ασφάλειας κ.λπ. Το PlaceApps είναι ένα στρώμα για τη δημοσίευση εφαρμογών. Όλα τα στρώματα έχουν σχεδιαστεί σύμφωνα με αρχιτεκτονικές προσανατολισμένες στις υπηρεσίες (SOA), ώστε να διευκολύνεται η

δημιουργία εφαρμογών, η χρήση υπηρεσιών της πλατφόρμας και η ενσωμάτωση μονάδων τρίτων.

Το Rio Operation Center αναπτύχθηκε από την IBM στο Ρίο ντε Τζανέιρο για την ενσωμάτωση δημόσιων πληροφοριών από πολλαπλά κυβερνητικά ιδρύματα. Το κέντρο αυτό αποσκοπεί στη βελτίωση της δημόσιας ασφάλειας και στην αύξηση της αποτελεσματικότητας της αντιμετώπισης περιστατικών, κυρίως ενόψει φυσικών καταστροφών.

Στο [11], οι συγγραφείς περιγράφουν ένα ενδιάμεσο λογισμικό που υλοποιήθηκε στο Oulu (Φινλανδία). Αυτό το ενδιάμεσο λογισμικό είναι ένα επίπεδο που αναπτύσσεται πάνω από μια σειρά δικτύων επικοινωνίας (π.χ. τοπικό δίκτυο (LAN), Bluetooth, Wi-Fi), υπεύθυνο για την ενεργοποίηση της συνδεσιμότητας με αυτά τα δίκτυα και την παροχή πρόσβασης σε δεδομένα που συλλέγονται από αισθητήρες της πόλης. Ο απώτερος στόχος του έργου αυτού είναι η δημιουργία ενός πραγματικού δοκιμαστικού περιβάλλοντος για τη βελτίωση της επικοινωνίας μεταξύ των πολιτών και της κυβέρνησης.

Το Ubiquitous city (u-city)[12] είναι ένα νοτιοκορεατικό μη παρεμβατικό έργο με επίκεντρο τον χρήστη για τη διασύνδεση των αστικών υπηρεσιών που χωρίζονται ανά τομέα ενδιαφέροντος (π.χ. αυτοματισμοί κτιρίων, επιχειρήσεις, διακυβέρνηση).

Στο [13], ο συγγραφέας προτείνει μια αρχιτεκτονική τεσσάρων επιπέδων για την ενσωμάτωση στοιχείων του IoT στις έξυπνες πόλεις. Βασικό χαρακτηριστικό αυτής της λύσης είναι η συμπερίληψη μέσων για την τόνωση της συνεργασίας μεταξύ των στοιχείων του συστήματος. Για παράδειγμα, συσκευές χαμηλής ισχύος, όπως τα smartphones, στέλνουν τμήματα πολύπλοκων διαδικασιών στο σύννεφο για να υπολογιστούν.

Από μια φουτουριστική θεωρητική άποψη, οι συγγραφείς του [14] παρουσιάζουν ένα πλαίσιο που βασίζεται σε ενδιάμεσο λογισμικό υπολογιστικού νέφους και σε ένα εξαιρετικά διασυνδεδεμένο δίκτυο IoT. Βασικά, οι συγγραφείς υποστηρίζουν ότι το IoT θα χρησιμοποιηθεί για την ανίχνευση και την

αλληλεπίδραση με το περιβάλλον με εφαρμογές από κάθε είδους τομείς (π.χ. οικιακός αυτοματισμός, μεταφορές, κοινοτικές υπηρεσίες, λειτουργία υποδομών, υγειονομική περίθαλψη). Το ενδιάμεσο λογισμικό θα χρησιμοποιεί παραδείγματα όπως software-as-a-service, platform-as-a-service και infrastructure-as-a-service για να συνδέσει τις εφαρμογές και το IoT μεταξύ τους.

Το SmartSantander είναι μια πρωτοβουλία με έδρα την πόλη Santander, στη βόρεια Ισπανία, όπου έχουν αναπτυχθεί μαζικά στοιχεία του IoT ως πεδίο δοκιμών για έργα έξυπνης πόλης.

Ως αποτέλεσμα, οι ερευνητές μπορούν να πειραματιστούν σε ένα περιβάλλον που λαμβάνει υπόψη πραγματικές συνθήκες έξυπνης πόλης: ανάπτυξη μεγάλης κλίμακας, ετερογένεια συσκευών, στατικές και κινητές αισθητήρες, πραγματικοί χρήστες κ.λπ. Στο [15], οι συγγραφείς παρουσιάζουν περισσότερες λεπτομέρειες σχετικά με την αρχιτεκτονική του συστήματος.

Η Βαρκελώνη αναλαμβάνει ηγετικό ρόλο και έχει προτείνει το CityOS, ένα λειτουργικό σύστημα για πόλεις που συγκεντρώνει μονάδες επεξεργασίας δεδομένων, ανάλυσης, διαχείρισης ιστορικών δεδομένων, επιχειρηματικής ευφυΐας κ.λπ. Ένας σημαντικός στόχος της έξυπνης πόλης της Βαρκελώνης είναι να αναπτύξει ένα σύστημα για την εύκολη ενσωμάτωση μονάδων τρίτων κατασκευαστών. Για παράδειγμα, το CityOS περιλαμβάνει την ενότητα City Service Development Kit (CitySDK), η οποία προσφέρει ένα σύνολο εργαλείων ανοικτού κώδικα για να βοηθήσει τις πόλεις να ανοίξουν τα δεδομένα τους και να βοηθήσει τους προγραμματιστές να δημιουργήσουν ψηφιακές υπηρεσίες για την πόλη. Άλλα αξιοσημείωτα έργα που περιλαμβάνονται στην έξυπνη πόλη της Βαρκελώνης είναι:

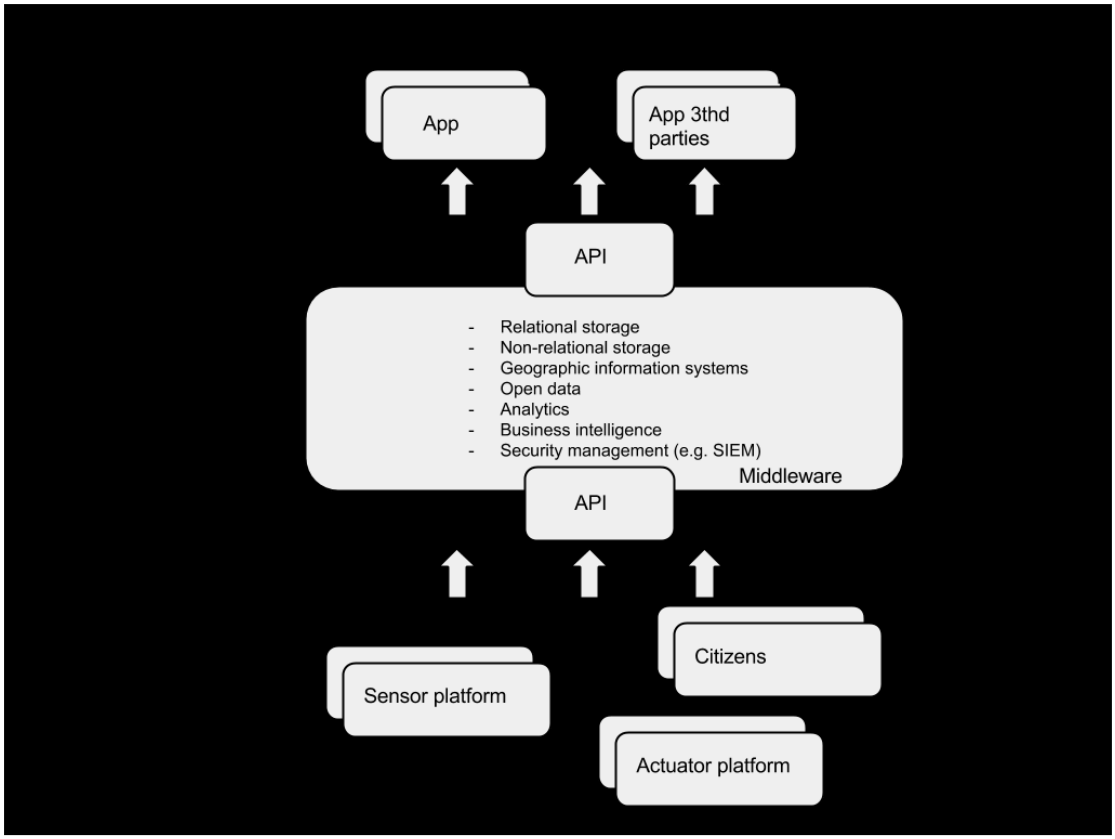
- Sentilo, μια πλατφόρμα για τη συλλογή δεδομένων από αστικούς αισθητήρες
- iCity8, μια πλατφόρμα για την παροχή κινήτρων σε τρίτους. έργων με τη χρήση δημόσιων πληροφοριών
- Open Cities, το οποίο είναι ένα έργο για την επικύρωση μεθοδολογιών με επίκεντρο τον χρήστη για τη χρήση ανοικτών δεδομένων στο δημόσιο τομέα.

1.2 Γενική αρχιτεκτονική έξυπνης πόλης

Σε γενικές γραμμές, αναλύοντας τις πρωτοβουλίες που παρουσιάστηκαν στην προηγούμενη ενότητα, μπορεί να διαπιστωθεί ότι η αρχιτεκτονική των πληροφοριακών συστημάτων έξυπνων πόλεων ακολουθεί ορισμένα κοινά πρότυπα. Η παρούσα ενότητα περιγράφει αυτά τα πρότυπα, τα οποία εντοπίζονται εύκολα στις περισσότερες έξυπνες πόλεις.

Πρώτα απ' όλα, τα συστήματα ΤΠΕ αναπτύσσονται συνήθως με τη λεγόμενη προοπτική του σιλό. Αυτό σημαίνει ότι για κάθε υποδομή σχεδιάζεται ένα ανεξάρτητο νέο σύστημα. Ως εκ τούτου, η συνεργασία και η διασυνδεσιμότητα μεταξύ των υποδομών παραμένει πολύ περιορισμένη. Τα πλαίσια έξυπνων πόλεων εμφανίστηκαν με στόχο να σπάσουν αυτά τα σιλό, να διευκολύνουν την ανάπτυξη εφαρμογών που αφορούν πολλούς ενδιαφερόμενους και να παρέχουν μια πλατφόρμα με κοινές υπηρεσίες.

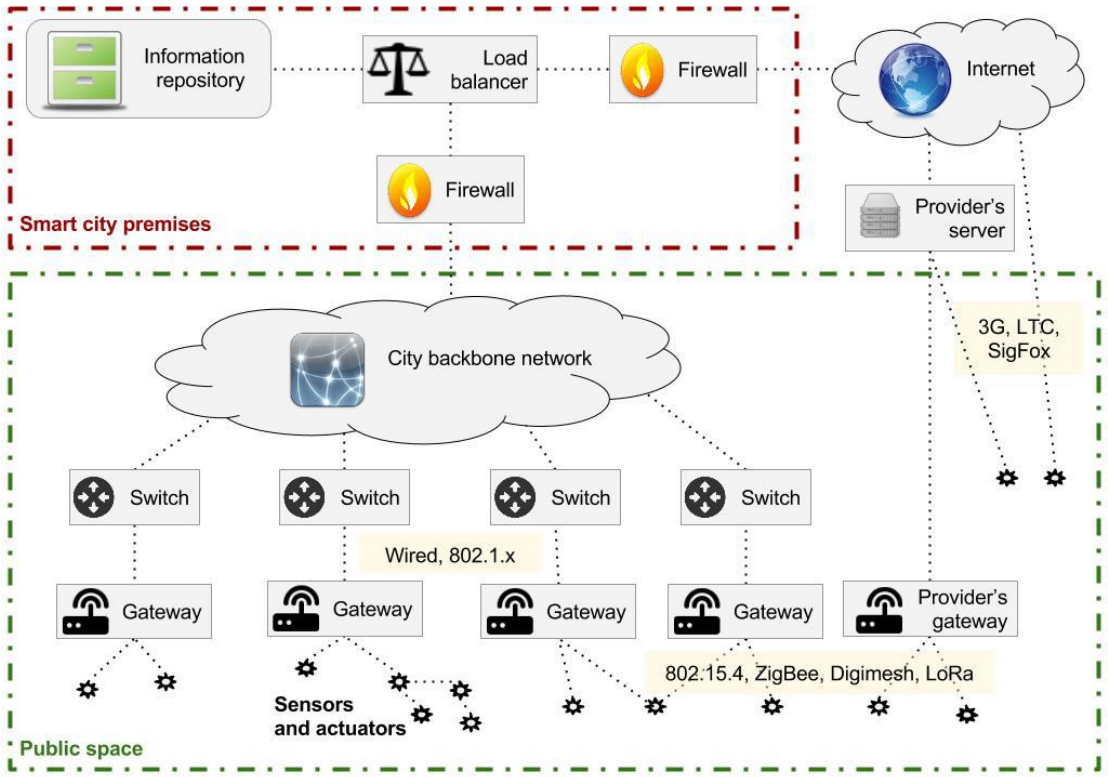
Δεύτερον, τα συστήματα έξυπνων πόλεων σχεδιάζονται συνήθως ως αρχιτεκτονικές προσανατολισμένες στις υπηρεσίες που χωρίζονται σε τρία επίπεδα. Το πρώτο στρώμα περιλαμβάνει τα στοιχεία που συλλέγουν πληροφορίες από την πόλη (π.χ. αισθητήρες, κάμερες παρακολούθησης, κοινωνικά δίκτυα, εφαρμογές καταγγελιών πολιτών, συστήματα εποπτικού ελέγχου και συλλογής δεδομένων (SCADA)). Το δεύτερο στρώμα λειτουργεί ως ενδιάμεσο λογισμικό, το οποίο παρέχει στην πόλη ένα API για τη σύνδεση των στοιχείων του πρώτου στρώματος με τις υπηρεσίες που προσφέρονται σε αυτό το στρώμα. Μεταξύ άλλων, οι υπηρεσίες αυτές περιλαμβάνουν σχεσιακή και μη σχεσιακή αποθήκευση, γεωγραφικά συστήματα πληροφοριών, ανάλυση δεδομένων, υπολογιστικό νέφος, επεξεργασία φυσικής γλώσσας, επιχειρηματική ευφυΐα ή ανοικτά δεδομένα. Τέλος, το τρίτο στρώμα είναι ένα στρώμα εφαρμογών, στο οποίο το δημοτικό συμβούλιο και τρίτα μέρη υλοποιούν εφαρμογές με βάση τα δεδομένα και τις υπηρεσίες που προσφέρονται από το μεσαίο στρώμα. Ένα σχήμα αυτής της αρχιτεκτονικής παρουσιάζεται στο σχήμα 1.1. Σε γενικές γραμμές, οι αρχιτεκτονικές αυτές αποσκοπούν στη μεγιστοποίηση της διαλειτουργικότητας μεταξύ των ενοτήτων με SOA, προκειμένου να ενθαρρυνθεί η ανάπτυξη τρίτων εφαρμογών και να διευκολύνουν την πρόσβαση σε υπηρεσίες και δεδομένα της πόλης.



Σχήμα 1.1: Γενική Αρχιτεκτονική Έξυπνης Πόλης [16]

Το κανάλι επικοινωνίας μεταξύ των αισθητήρων δρόμου και των κεντρικών διακομιστών έξυπνης πόλης απεικονίζεται στο Σχήμα 1.2. Όπως φαίνεται στο σχήμα, ορισμένα WSNs είναι επίσης εξοπλισμένα με ενεργοποιητές, οι οποίοι μπορούν να λειτουργήσουν από τους κεντρικούς διακομιστές με μετάδοση downlink ή να ενεργοποιηθούν από άλλα συστήματα πρώτου επιπέδου χρησιμοποιώντας επικοινωνία μηχανής προς μηχανή (M2M). Για παράδειγμα, αισθητήρες ανίχνευσης οχημάτων ενσωματωμένοι στην άσφαλτο στέλνουν πληροφορίες σε ελεγκτές κυκλοφορίας εγκατεστημένους σε φωτεινούς σηματοδότες [16]. Ωστόσο, κατά βάση, η υποδομή που παρουσιάζεται στο Σχήμα 1.2 έχει σχεδιαστεί για να συλλέγει τις πληροφορίες που παράγονται από τους αισθητήρες και να τις αποστέλλει στους διακομιστές της πόλης. Τα στοιχεία αυτού του σχήματος αποτελούν μέρος των στοιχείων από το πρώτο και το δεύτερο επίπεδο του Σχήματος 1.1. Η ροή πληροφοριών σε αυτό το σχήμα ξεκινά από τους αισθητήρες, οι οποίοι συλλέγουν δεδομένα για το περιβάλλον τους και στη

συνέχεια τα στέλνουν σε μια πύλη. Οι πύλες παραδίδουν τελικά τα δεδομένα των αισθητήρων στις εγκαταστάσεις της έξυπνης πόλης.



Σχήμα 1.2: Ασύρματη Υποδομή Συλλογής Δεδομένων [16]

1.3 Έξυπνη πόλη και Μεγάλα Δεδομένα (Big Data)

Όπως αναφέρθηκε παραπάνω, η τεχνολογία που αναπτύσσεται στις έξυπνες πόλεις έχει μεγάλες δυνατότητες ως μέσο βελτίωσης της οικονομικής προόδου, της κοινωνικής ευημερίας και της ποιότητας ζωής τους, εξασφαλίζοντας παράλληλα μια πιο ορθολογική και αποτελεσματική προσέγγιση του τρόπου λειτουργίας και παροχής υπηρεσιών. Ωστόσο, η τρέχουσα αρχιτεκτονική των πληροφοριακών συστημάτων θέτει ορισμένες προκλήσεις στον τομέα της ασφάλειας λόγω των ακόλουθων γεγονότων:

- Η πόλη περιλαμβάνει πολλά συστήματα από διαφορετικές υπηρεσίες (π.χ. οδοφωτισμός, αποκομιδή απορριμμάτων, παροχή νερού), καθένα από τα οποία έχει συγκεκριμένες ανάγκες και απαιτήσεις. Κατά συνέπεια, τα WSN

από κάθε σύστημα υλοποιούνται με διαφορετική τεχνολογία και αναπτύσσονται από διαφορετικούς παρόχους.

- Όπως θα φανεί στο Κεφάλαιο 2, οι λύσεις ασφάλειας στον τομέα των WSNs επικεντρώνονται συνήθως στην προστασία σεναρίων με πολύ συγκεκριμένα χαρακτηριστικά. Σήμερα, οι λύσεις ασφάλειας για τα WSNs δεν είναι ικανές να προστατεύσουν ένα ολόκληρο σύστημα τόσο ετερογενές όσο η έξυπνη πόλη.
- Από τη σκοπιά των διαχειριστών των έξυπνων πόλεων, η ανάθεση της ανάπτυξης και συντήρησης των WSNs σε εξωτερικούς συνεργάτες έχει ως αποτέλεσμα την απώλεια της ορατότητας της πραγματικής αποτελεσματικότητας των μέτρων ασφαλείας που εφαρμόζονται στα δίκτυα των παρόχων.
- Λόγω των περιορισμών της υπολογιστικής ισχύος και της μπαταρίας των κόμβων αισθητήρων, τα WSN συχνά αποφεύγουν να στέλνουν πληροφορίες για την κατάσταση του συστήματος, γεγονός που δυσχεραίνει την επακόλουθη ανάλυση ασφάλειας.

Έτσι, γίνεται αντιληπτό ότι τα εγγενή χαρακτηριστικά μιας έξυπνης πόλης δημιουργούν πρόσθετες προκλήσεις ασφαλείας που δεν ξεπερνιούνται εύκολα μόνο με παραδοσιακές λύσεις. Παρακάτω, δίνονται λεπτομέρειες για τα θέματα τα οποία θα διαπραγματευτεί η παρούσα εργασία:

1. Ορισμός της αρχιτεκτονικής μιας πλατφόρμας ανίχνευσης εισβολών. Ο πρώτος στόχος είναι να καθοριστούν οι κύριες ενότητες μιας πλατφόρμας ανίχνευσης εισβολής που είναι:

- ικανή να συλλέγει, να ευρετηριάζει και να επεξεργάζεται δεδομένα WSN,

- επεκτάσιμη,

- ικανή να διαχειρίζεται μεγάλα δεδομένα,

- διαφανής για τους παρόχους, και

- συμβατή με την υπάρχουσα υποδομή.

2. Ορισμός του αγωγού των υποδιαδικασιών που εμπλέκονται στην ανίχνευση επιθέσεων. Η ανίχνευση επιθέσεων περιλαμβάνει διάφορες υποδιαδικασίες. Αυτές πρέπει να οριστούν και να προσδιοριστούν και να μελετηθούν οι αλληλεπιδράσεις μεταξύ των διαφόρων υποδιαδικασιών, ώστε να διασφαλιστεί η βιώσιμη και κλιμακούμενη εκτέλεση του αγωγού.

3. Προσδιορισμός κατάλληλων αλγορίθμων για ένα σύστημα ανίχνευσης εισβολών με βάση τις ανωμαλίες. Η παρούσα διατριβή πρέπει να προσδιορίσει τους κατάλληλους αλγορίθμους για το σύστημα ανίχνευσης εισβολής με βάση τις ανωμαλίες, λαμβάνοντας υπόψη τις απαιτήσεις του πλαισίου της έξυπνης πόλης και τα χαρακτηριστικά της τεχνολογίας WSN.

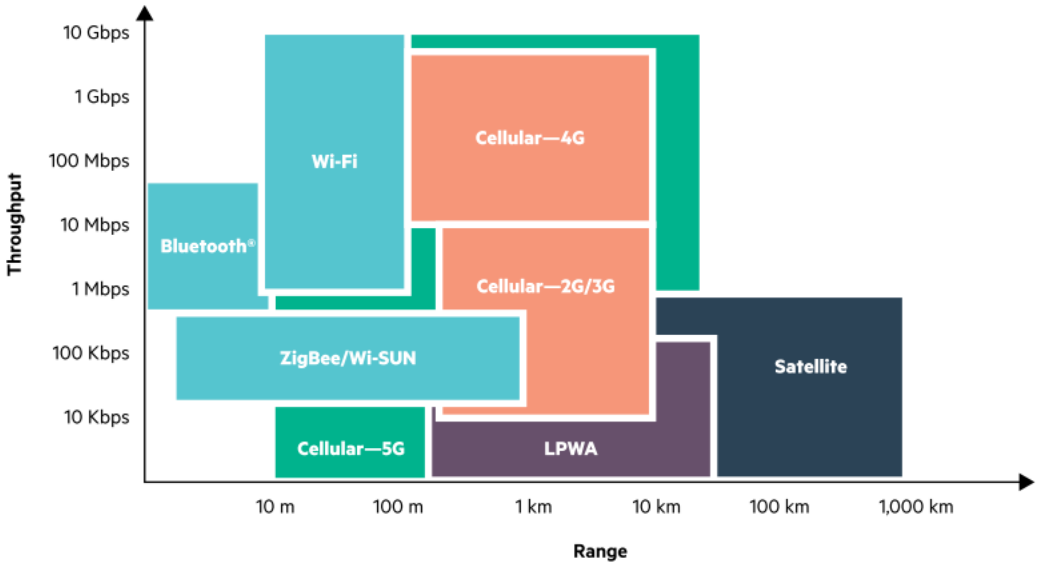
4. Παροχή ενός μηχανισμού για τον εντοπισμό επιθέσεων. Σε περίπτωση περιστατικού ασφαλείας στα WSN, είναι απαραίτητο όχι μόνο να εντοπιστεί ότι το δίκτυο έχει παραβιαστεί, αλλά και να εντοπιστεί η επίθεση και ο παραβιασμένος εξοπλισμός. Πρέπει να προβλεφθεί ένας μηχανισμός που θα καθοδηγεί την έξυπνη πόλη διαχειριστές στον εντοπισμό των πιο πιθανών επιθέσεων.

Αξίζει να αναφερθεί ότι η μελέτη αλγορίθμων και τεχνικών για την επίλυση προβλημάτων ασφάλειας για συγκεκριμένες επιχειρηματικές περιπτώσεις έξυπνων πόλεων, τύπους επιθέσεων ή διαμορφώσεις δικτύων ξεφεύγει από το πεδίο εφαρμογής της παρούσας διατριβής. Για παράδειγμα, είναι σημαντικό να προσδιοριστούν κατώτατα όρια για ορισμένες μεταβλητές κατάστασης του συστήματος, πέραν των οποίων οι διαχειριστές έξυπνων πόλεων είναι βέβαιοι ότι ορισμένα πρωτόκολλα WSN δεν λειτουργούν σωστά. Είναι επίσης σημαντικό να βρεθούν οι καλύτεροι αλγόριθμοι για την ανακάλυψη δυσλειτουργιών για κάθε μία από τις υπηρεσίες που προσφέρει η έξυπνη πόλη. Καθώς αυτοί οι αλγόριθμοι μπορεί να είναι πολύ διαφορετικοί ανάλογα με τη συγκεκριμένη υπηρεσία, δεν έχουν ληφθεί υπόψη στην έρευνά μας. Ως εκ τούτου, η παρούσα εργασία έχει ως στόχο να συμβάλει με γενικεύσιμες λύσεις που μπορούν να εφαρμοστούν σε διάφορες έξυπνες πόλεις, διαφορετικές υπηρεσίες, τεχνολογίες κ.λπ.

1.4 Ασύρματα Δίκτυα Αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων είναι δίκτυα που επικοινωνούν με τη χρήση ασύρματης τεχνολογίας, όπου οι κόμβοι, γνωστοί και ως μοτέρ, είναι εξοπλισμένοι με έναν ή περισσότερους αισθητήρες για να καταγράφουν πληροφορίες σχετικά με το περιβάλλον τους. Όταν οι κόμβοι είναι επίσης εξοπλισμένοι με ενεργοποιητές που τους επιτρέπουν να εκτελούν μια συγκεκριμένη ενέργεια, τότε τα δίκτυα αυτά είναι γνωστά ως ασύρματα δίκτυα αισθητήρων και ενεργοποιητών (WSAN).

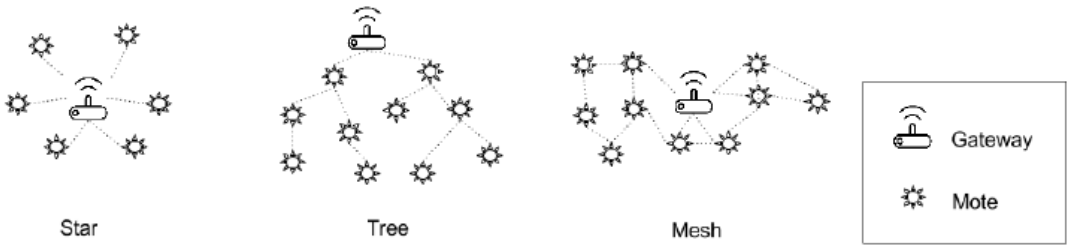
Στις έξυπνες πόλεις, είναι σύνηθες οι κινητήρες να έχουν αυτόνομη συνεργατική επικοινωνία για να στέλνουν τις τιμές που διαβάζουν οι αισθητήρες τους σε μια συσκευή στην άκρη του WSN, γνωστή ως πύλη ή σταθμός βάσης. Οι πύλες είναι εξοπλισμένες με διάφορες διεπαφές επικοινωνίας με στόχο τη μετάδοση δεδομένων WSN στα κέντρα δεδομένων έξυπνων πόλεων μέσω ενός συμβατικού και αξιόπιστο δίκτυο (π.χ. Διαδίκτυο).



Σχήμα 1.3: Σύγκριση εμβέλειας και απόδοσης μεταξύ ασύρματων τεχνολογιών[17]

Υπάρχουν πολλοί τύποι πρωτοκόλλων ασύρματης επικοινωνίας που δημιουργούν διαφορετικά είδη ασύρματων δικτύων. Στο Σχήμα 1.3 συγκρίνονται οι σημαντικότερες τεχνολογίες ανάλογα με την εμβέλεια και την απόδοση τους. Βασικά, οι πιο σημαντικές τεχνολογίες WSN στις έξυπνες πόλεις είναι:

- Τα ασύρματα δίκτυα προσωπικής περιοχής (WPAN) είναι ασύρματα δίκτυα χαμηλής ισχύος, χαμηλής απόδοσης, μικρής εμβέλειας (έως λίγα μέτρα) που βασίζονται στο πρότυπο IEEE 802.15. Σχετικές τεχνολογίες που περιλαμβάνονται σε αυτή την κατηγορία είναι το ZigBee, το IPv6 μέσω ασύρματων δικτύων προσωπικής περιοχής χαμηλής ισχύος (6LoWPAN) και το Bluetooth. Υπάρχουν πολλές περιπτώσεις χρήσης στις έξυπνες πόλεις που χρησιμοποιούν αυτά τα πρωτόκολλα. Για παράδειγμα, το ZigBee χρησιμοποιείται στο [17] για τον έλεγχο του φωτισμού των δρόμων.
- Τα ασύρματα τοπικά δίκτυα (WLAN), όπως το Wi-Fi, παρέχουν ασύρματα δίκτυα χαμηλής εμβέλειας αλλά ευρείας απόδοσης. Ορισμένες πόλεις, όπως το Σαν Χοσέ στην Καλιφόρνια [18], αναπτύσσουν συνδεσιμότητα Wi-Fi στους δρόμους όχι μόνο για να προσφέρουν Διαδίκτυο στους πολίτες, αλλά και για να συνδέσουν στοιχεία IoT που απαιτούν μεγαλύτερο εύρος ζώνης από τις συνήθεις εφαρμογές αισθητήρων, όπως οι κάμερες κυκλοφορίας που βασίζονται σε IP.
- Τα ασύρματα μητροπολιτικά δίκτυα (WMAN) ακολουθούν τα πρότυπα IEEE 802.16. Τα πρωτόκολλα που ακολουθούν αυτή την οικογένεια προτύπων είναι ευρέως γνωστά ως WiMAX. Αυτή η τεχνολογία χρησιμοποιείται κυρίως για εφαρμογές που απαιτούν μεγάλες αναπτύξεις (έως 25 km) και μη περιορισμένη απόδοση (< 150 Mb/s). Στο [19], οι συγγραφείς προτείνουν τη χρήση του WiMAX για έργα έξυπνου δικτύου.
- Τα δίκτυα ευρείας περιοχής χαμηλής ισχύος (LPWAN) είναι ασύρματα δίκτυα χαμηλής ισχύος, μεγάλης εμβέλειας (έως 10 km) και χαμηλής απόδοσης (<5 Kb/s) [20]. Το SigFox 18 και το LoRaWAN 19 είναι οι πιο δημοφιλείς τεχνολογίες αυτή τη στιγμή. Και οι δύο τεχνολογίες έχουν χρησιμοποιηθεί σε πολλές εφαρμογές έξυπνων χώρων στάθμευσης [21].



Σχήμα 1.4: Τοπολογίες Ασύρματων Δικτύων [17]

Μεταξύ αυτών των τύπων δικτύων, τα WPAN θεωρούνται ιδιαίτερα ευάλωτα. Αυτά αποτελούνται από συσκευές χαμηλής ισχύος και μονάδες επικοινωνίας μικρής εμβέλειας, οι οποίες βασίζονται σε πολλές περιπτώσεις στις δυνατότητες πολλαπλών βημάτων για τη δημιουργία ενός εκτεταμένου δικτύου και την παράδοση πακέτων από τους πιο απομακρυσμένους κόμβους στο σταθμό βάσης. Εξάλλου, οι κινητήρες λειτουργούν συχνά με μπαταρίες και, ως εκ τούτου, σχεδιάζονται επίσης με περιορισμένη ικανότητα επεξεργασίας για εξοικονόμηση ενέργειας.

Ως εκ τούτου, η παρούσα διατριβή επικεντρώνεται σε αυτόν τον τύπο WSN για την εκτέλεση επιθέσεων και την ανάλυση εισβολών. Ωστόσο, τα αποτελέσματα μπορούν να γενικευτούν και σε άλλους τύπους WSN. Όπως αναφέρθηκε παραπάνω, πολλά WSN βασίζονται σε δυνατότητες πολλαπλών διαδρομών για την παράδοση πακέτων από το ένα άκρο του δικτύου στο άλλο άκρο. Αυτό επιτρέπει τρεις βασικές τοπολογίες που παρουσιάζονται στο Σχήμα 1.4: αστέρι, δέντρο και πλέγμα. Αυτές οι τοπολογίες μπορούν να περιλαμβάνουν τρεις τύπους κόμβων: πύλες, κινητήρες με δυνατότητες δρομολόγησης και κινητήρες φύλλων. Οι πύλες και οι κόμβοι δρομολόγησης καταναλώνουν μεγάλες ποσότητες ενέργειας για την προώθηση πακέτων και, ως εκ τούτου, είναι γενικά συνδεδεμένοι στο ηλεκτρικό δίκτυο. Ωστόσο, οι κόμβοι-φύλλα μπορούν να λειτουργούν με μπαταρία, επειδή η μόνη τους ευθύνη είναι η ανίχνευση του περιβάλλοντος και η αποστολή των δικών τους πακέτων προς τις Οι ακόλουθες ενότητες συνοψίζουν τις αρμοδιότητες των πιο σημαντικών επιπέδων της στοίβας επικοινωνίας για τα WSN. Αυτά είναι το φυσικό επίπεδο, το επίπεδο ζεύξης δεδομένων, το επίπεδο δικτύου και το επίπεδο εφαρμογής. στρώματα.

1.4.1 Φυσικό Στρώμα

Το φυσικό επίπεδο χειρίζεται τον τρόπο με τον οποίο τα bits μεταδίδονται μέσω του μέσου (του αέρα στα WSN). Έτσι, οι κύριες αρμοδιότητές του περιλαμβάνουν τον καθορισμό των συχνοτήτων λειτουργίας, της διαμόρφωσης, της αίσθησης του φέροντος, του ρυθμού μετάδοσης κ.λπ. Στο ZigBee και στο 6LoWPAN αυτό το επίπεδο ορίζεται από το πρότυπο IEEE 802.15.4 [22].

1.4.2 Στρώμα Ζεύξης Δεδομένων

Το επίπεδο ζεύξης δεδομένων είναι υπεύθυνο για τη μεταφορά δεδομένων μεταξύ γειτονικών κόμβων σε ένα δίκτυο. Στα WSN, το υποεπίπεδο ελέγχου πρόσβασης στα μέσα (MAC) είναι ιδιαίτερα σημαντικό. Αυτό το υποεπίπεδο οργανώνει τους κόμβους του δικτύου έτσι ώστε η πρόσβαση στο μέσο μετάδοσης να γίνεται με διατεταγμένο τρόπο, γεγονός που επιτρέπει τη σωστή επικοινωνία. Όπως και το φυσικό επίπεδο, το επίπεδο MAC ορίζεται επίσης από το πρότυπο IEEE 802.15.4 [23].

Σύμφωνα με αυτό το πρότυπο, οι κόμβοι μπορούν να αναλάβουν το ρόλο μιας συσκευής πλήρους λειτουργίας (FFD), η οποία έχει δυνατότητες δρομολόγησης, ή το ρόλο μιας συσκευής μειωμένης λειτουργίας (RFD), η οποία περιορίζει τους κόμβους μόνο στη μετάδοση των δικών τους δεδομένων. Με αυτόν τον τρόπο, δύο τύποι τοπολογιών είναι δυνατοί σε αυτό το επίπεδο: αστέρι και ομότιμοι. Σε μια τοπολογία αστέρα, μια ενιαία FFD λαμβάνει μηνύματα από διάφορες FFD ή RFD. Σε μια ομότιμη τοπολογία, πολλά FFD μπορούν να επικοινωνούν μεταξύ τους. Είναι σημαντικό να σημειωθεί ότι τα FFDs συνήθως καταναλώνουν περισσότερη ενέργεια από τα RFDs και, ως εκ τούτου, γενικά, δεν μπορούν να λειτουργούν με μπαταρία. Όσον αφορά την πρόσβαση στα μέσα, τα πρωτόκολλα χρησιμοποιούν δύο κύριους τύπους στρατηγικών. Αφενός, τα πρωτόκολλα που βασίζονται στην πολλαπλή πρόσβαση με διαίρεση χρόνου (TDMA) διαιρούν το χρόνο σε χρονοθυρίδες και οι πομποί κρατούν μια χρονοθυρίδα πριν από τη μετάδοση. Αυτός ο τύπος πρωτοκόλλου απαιτεί φάρους για το συγχρονισμό των πομπών και των δεκτών. Σε άλλους τύπους πρωτοκόλλων, ωστόσο, οι κόμβοι δεν μπορούν να κρατήσουν χρονοθυρίδες, αλλά τους παρέχεται ένας μηχανισμός για την αποτελεσματική μετάδοση πακέτων χωρίς να δημιουργούν παρεμβολές στις

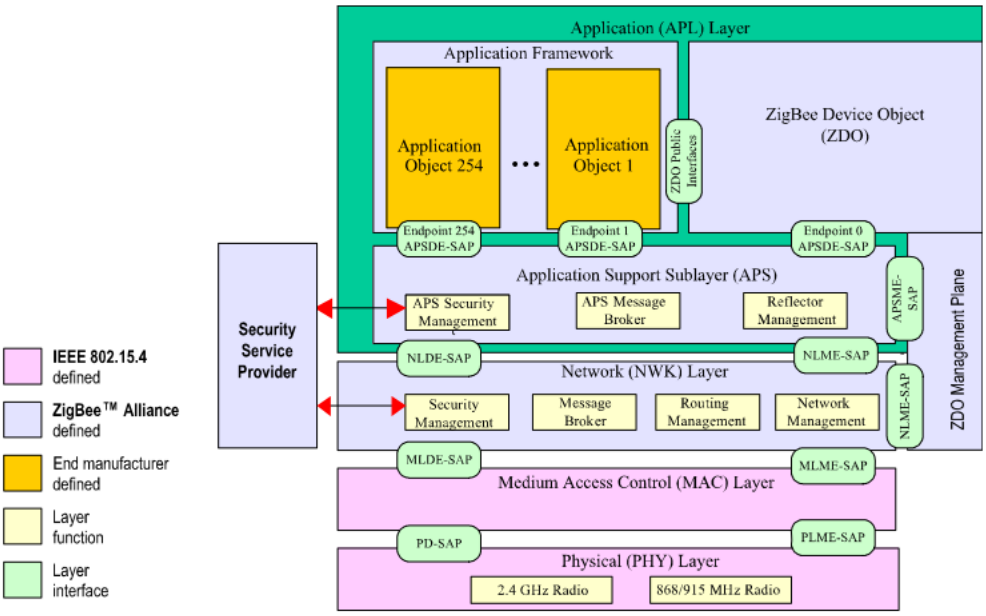
επικοινωνίες από τους άλλους κόμβους του δικτύου. Για παράδειγμα, το CSMA-CA (carrier sense multiple access with collision avoidance) ουσιαστικά ορίζει ότι, πριν από τη μετάδοση, ένας κόμβος πρέπει να ανιχνεύσει το μέσο και απλώς να ξεκινήσει μια μετάδοση εάν το κανάλι είναι ελεύθερο. Στο [24], οι συγγραφείς αναλύουν πολλαπλά πρωτόκολλα MAC για WSNs. Επιπλέον, το πρότυπο IEEE 802.15.4 ορίζει επίσης μηχανισμούς επαλήθευσης δεδομένων (δηλ. κυκλικός έλεγχος πλεονασμού (CRC)) και ασφάλειας για τη διασφάλιση της εμπιστευτικότητας των δεδομένων, της αυθεντικότητας και την προστασία αναπαραγωγής σε επικοινωνίες μονής ζεύξης.

1.4.3 Στρώμα Δικτύου

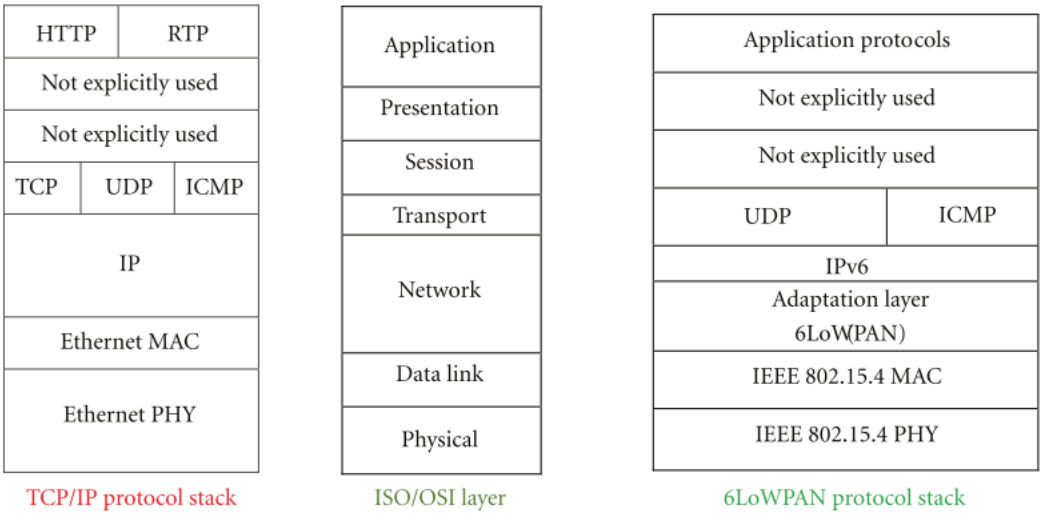
Το επίπεδο δικτύου επιτρέπει τοπολογίες δικτύων πολλαπλών βημάτων. Οι κόμβοι που υλοποιούν αυτό το επίπεδο μπορούν να γίνουν ενδιάμεσοι, αναπτύσσοντας ικανότητες δρομολόγησης και προωθώντας πακέτα από άλλους κόμβους. Στο WPAN, υπάρχουν δύο κύρια πρότυπα για ενσωματωμένα συστήματα που περιλαμβάνουν τις προδιαγραφές για ένα στρώμα δικτύου: ZigBee (στοίβα πρωτοκόλλων που παρουσιάζεται στο Σχήμα 1.5) και 6LoWPAN (στοίβα πρωτοκόλλων που παρουσιάζεται στο Σχήμα 1.6). Όπως φαίνεται στα σχήματα, αυτά τα πρότυπα ορίζουν όλα τα απαραίτητα στρώματα της στοίβας επικοινωνίας. Αν και δεν είναι υποχρεωτικό, και τα δύο πρωτόκολλα ορίζονται πάνω από το IEEE 802.15.4. Και τα δύο προσφέρουν τυπικές υπηρεσίες δικτύου, όπως ανακάλυψη γείτονα, ανακάλυψη διαδρομής, διευθυνσιοδότηση, δρομολόγηση κ.λπ. Το ZigBee [25] έχει προταθεί από την ZigBee Alliance 20 και περισσότερες πληροφορίες μπορείτε να βρείτε στο [26].

Το 6LoWPAN έχει οριστεί από την IETF 21 στο [27]. Αυτός ο ορισμός πρωτοκόλλου προτείνει ένα επίπεδο διαλειτουργικότητας για την αποστολή πακέτων IPv6 σε δίκτυα χαμηλής ισχύος και με απώλειες. Έτσι, αυτό το πρωτόκολλο είναι εύκολα ενσωματώσιμο με τα συμβατικά δίκτυα: οι πύλες είναι απλές, μπορεί να χρησιμοποιηθεί ο ίδιος χώρος διευθύνσεων δικτύου και τα πρωτόκολλα πάνω από το IP, όπως το User Datagram Protocol (UDP) ή το Internet Control Message Protocol (ICMP), είναι συμβατά. Το επίπεδο δικτύου περιέχει πολλαπλά πρωτόκολλα για την αντιμετώπιση των διαφορετικών αρμοδιοτήτων του επιπέδου.

Για παράδειγμα, το Ad hoc On-Demand Distance Vector (AODV) [28] είναι ένα πολύ δημοφιλές πρωτόκολλο δρομολόγησης που μπορεί να χρησιμοποιηθεί όχι μόνο στο ZigBee και το 6LoWPAN, αλλά και σε άλλα κινητά δίκτυα.



Σχήμα 1.5: Στοίβα πρωτοκόλλων για το ZigBee [25]



Σχήμα 1.6: 6LoWPAN στοίβα πρωτοκόλλων [27]

1.4.4 Στρώμα Εφαρμογής

Το επίπεδο εφαρμογής βρίσκεται στην κορυφή της στοίβας επικοινωνίας. Σε αυτό το στρώμα υλοποιούνται λειτουργίες που αφορούν συγκεκριμένες εφαρμογές. Επιπλέον, το Πρωτόκολλο Περιορισμένης Εφαρμογής (CoAP) [29] έχει αναδειχθεί ως

ένα πρωτόκολλο παρόμοιο με το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HTTP) για το συμβατικό Διαδίκτυο. Το CoAP λειτουργεί πάνω από το UDP, υποστηρίζει τις μεθόδους Representational State Transfer (ReST) του HTTP και παρέχει συνδρομές και push notifications. Έτσι, το CoAP παρέχει ένα διαλειτουργικό πρωτόκολλο περιορισμένων εφαρμογών για το IoT.

2 ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΘΕΣΕΙΣ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΑΙΣΘΗΤΗΡΩΝ

2.1 Επιθέσεις σε ασύρματα δίκτυα αισθητήρων

Οι περιορισμένοι υπολογιστικοί και ενεργειακοί περιορισμοί των κόμβων αποτελούν εμπόδιο στην εφαρμογή των συμβατικών αντιμέτρων ασφάλειας δικτύων υπολογιστών στα WSN. Επιπλέον, σε αυτά τα δίκτυα, οι κόμβοι γίνονται πιο ευάλωτοι όταν τοποθετούνται σε απροστάτευτα περιβάλλοντα όπως οι δρόμοι. Υπό αυτές τις συνθήκες, οι επιτιθέμενοι μπορούν εύκολα να αιχμαλωτίσουν τους κόμβους, να αποκτήσουν πρόσβαση σε εμπιστευτικές πληροφορίες στη μνήμη τους (π.χ. κρυπτογραφικά κλειδιά) και να επαναπρογραμματίσουν τη συμπεριφορά τους. Είναι επίσης σύνηθες οι επιτιθέμενοι να επωφελούνται από την ασύρματη φύση των επικοινωνιών για να υποκλέπτουν τα μηνύματα ή να παρεμποδίζουν τις ζώνες συχνοτήτων ώστε να παρεμποδίζουν την ορθή λήψη ορισμένων πακέτων. Στις επόμενες ενότητες, παρουσιάζονται οι σημαντικότερες επιθέσεις που επηρεάζουν κάθε μία από τις στρώματα των πρωτοκόλλων επικοινωνίας [30].

2.1.1 Επιθέσεις ενάντια στο Φυσικό Στρώμα

- Παραποίηση δεδομένων (Data tampering): Τα δεδομένα που διακινούνται μεταξύ δύο κόμβων τροποποιούνται.

- Παραποίηση κόμβων (Node tampering): Ένας κόμβος συλλαμβάνεται με σκοπό να καταστραφεί ή να εξαχθούν πληροφορίες από τη μνήμη του.

- Αντιγραφή κόμβων (Node replication): Προστίθενται νέοι κόμβοι στο δίκτυο με αντιγραφή κόμβων που είναι ήδη νόμιμα μέλη του δικτύου.

- Παρεμπόδιση (Jamming): Οι επιτιθέμενοι στέλνουν σήμα υψηλής ισχύος προκειμένου να δημιουργήσουν παρεμβολές και να αποφύγουν την ορθή λήψη νόμιμων πακέτων.

2.1.2 Επιθέσεις ενάντια στο Στρώμα Ζεύξης Δεδομένων

- Sybil: Ένας κόμβος παίρνει διάφορες ταυτότητες για να αλλάξει τη συμπεριφορά των πρωτοκόλλων σύνδεσης δεδομένων. Αυτό έχει συνέπειες για τα πρωτόκολλα επικοινωνίας που βασίζονται στη συνάθροιση δεδομένων (δηλ. για να προωθήσουν λιγότερα πακέτα, οι ενδιάμεσοι κόμβοι συναθροίζουν τα δεδομένα που λαμβάνουν

από διάφορους κόμβους και στέλνουν ένα νέο πακέτο με τα συναθροισμένα δεδομένα) ή στην ψηφοφορία (δηλ. οι ενδιάμεσοι κόμβοι λαμβάνουν αποφάσεις, όπως η απόφαση για την καλύτερη σύνδεση, σύμφωνα με τις ψήφους που δίνουν άλλοι κόμβοι).

- Ανάκριση (Interrogation): Οι επιτιθέμενοι εκμεταλλεύονται πρωτόκολλα MAC που βασίζονται σε αμφίδρομη χειραψία (π.χ. πρωτόκολλα που στέλνουν πακέτα ελέγχου, όπως τα Ready To Send (RTS) και Clear To Send (CTS)). Οι επιτιθέμενοι στέλνουν πολλά RTS, έτσι ώστε οι κόμβοι που ακούνε να απαντούν με ένα CTS για κάθε λαμβανόμενο RTS και, επομένως, καταναλώνουν πόρους.

- Εξάντληση (Exhaustion): Οι επιτιθέμενοι καταλαμβάνουν συνεχώς το κανάλι επικοινωνίας. Ως εκ τούτου, οι νόμιμοι κόμβοι που χρησιμοποιούν πρωτόκολλα ανίχνευσης φέροντος (τα οποία χρησιμοποιούνται πριν από τη μετάδοση για να ελέγξουν αν το μέσο μετάδοσης είναι ελεύθερο) καθυστερούν ή ακόμη και ακυρώνουν τις μεταδόσεις τους.

- Σύγκρουση (Collision): Οι επιτιθέμενοι δημιουργούν παρεμβολές κατά τη διάρκεια νόμιμων μεταδόσεων. Με αυτόν τον τρόπο, οι μηχανισμοί ελέγχου απορρίπτουν τα ληφθέντα μηνύματα και οι πομποί πρέπει να στείλουν εκ νέου μηνύματα.

- Αδικία (Unfairness): Επιμονή σε επιθέσεις όπως η εξάντληση ή η σύγκρουση, προκειμένου να μειωθεί σημαντικά η ποιότητα της υπηρεσίας και να δημιουργηθεί ολική ή μερική άρνηση παροχής υπηρεσιών. (DoS).

2.1.3 Επιθέσεις Ενάντια στο Στρώμα Δικτύου

- Στέρηση ύπνου (Sleep deprivation): Οι επιτιθέμενοι δημιουργούν μεγάλη κίνηση μέσω πακέτων εκπομπής ή δημιουργώντας βρόχους δικτύου, ώστε να κρατούν πολλούς κόμβους ξύπνιους με επαναμετάδοση πακέτων.

- Στρουμφάκι του Διαδικτύου (Internet smurf): Οι επιτιθέμενοι υποδύονται έναν κόμβο και στη συνέχεια στέλνουν πολλαπλά αιτήματα ECHO σε εκπομπή. Οι επαναλήψεις ECHO κορεστούν το θύμα που έχει υποδυθεί την ταυτότητα.

- Παρεκτροπή (Misdirection): Επιτιθέμενοι με δυνατότητες δρομολόγησης προωθούν πακέτα προς συνδέσεις όπου ο τελικός προορισμός δεν είναι προσβάσιμος.

- Παραποίηση επιβεβαίωσης (Acknowledgement spoofing): Οι επιτιθέμενοι υποδύονται έναν νόμιμο κόμβο και στέλνουν πακέτα επιβεβαίωσης (ACK) που υποδεικνύουν τη λήψη λανθασμένα ληφθέντων πακέτων. Αυτό εμποδίζει τους πομπούς να ξαναστείλουν τα πακέτα.

- Πλαστογραφημένες, αλλοιωμένες ή αναπαραγόμενες πληροφορίες δρομολόγησης (Spoofed, altered, or replayed routing information): Οι πληροφορίες δρομολόγησης που αποστέλλονται μεταξύ νόμιμων κόμβων συλλαμβάνονται, τροποποιούνται και ξαναστέλνονται με σκοπό τη δημιουργία βρόχων, την προσέλκυση κίνησης σε κόμβους-στόχους, την κατάτμηση του δικτύου κ.λπ.

- Σκουληκότρυπα (Wormhole): Δημιουργείται ένα κανάλι μετάδοσης χαμηλής καθυστέρησης μεταξύ δύο απομακρυσμένων επιτιθέμενων. Ο επιτιθέμενος που βρίσκεται σε μεγαλύτερη απόσταση από το σταθμό βάσης επωφελείται από καλύτερες επικοινωνίες από τους γείτονές του για να αποκτήσει καλύτερες μετρικές δρομολόγησης. Ως εκ τούτου, αυτός ο επιτιθέμενος γίνεται ο καλύτερος κόμβος δρομολόγησης στην περιοχή και προσελκύει κίνηση.

- Sybil: Οι επιτιθέμενοι παίρνουν διαφορετικές ταυτότητες από τους νόμιμους κόμβους. Στη συνέχεια, οι επιτιθέμενοι μπορούν να παραπλανήσουν άλλους κόμβους δρομολόγησης ώστε να αλλάξουν το μονοπάτι δρομολόγησης προς ή μακριά από τους κόμβους που υποδύονται την ταυτότητα.

- Επιλεκτική προώθηση και μαύρη τρύπα (Selective forwarding and blackhole) : Οι επιτιθέμενοι σε μια θέση δρομολόγησης απορρίπτουν ορισμένα (επιλεκτική προώθηση) ή όλα τα πακέτα (μαύρη τρύπα) από ορισμένους κόμβους.

- Πλημμύρα χαιρετισμών (Hello flood): Οι επιτιθέμενοι χρησιμοποιούν έναν ισχυρό πομπό για να στείλουν μηνύματα HELLO για να ενταχθούν στο δίκτυο σε μεγάλο αριθμό κόμβων. Οι κόμβοι ακροατές απαντούν σε αυτό το ψεύτικο αίτημα με μάταια μηνύματα.

- Sinkhole: Ορισμένοι κόμβοι σε μια περιοχή παραπλανώνται και πιστεύουν ότι είτε ένας κόμβος-στόχος είτε ένας επιτιθέμενος είναι ο καλύτερος σύνδεσμος δρομολόγησης. Στην πρώτη περίπτωση, ο κόμβος-στόχος πρέπει να καταναλώνει επιπλέον πόρους για την προώθηση πακέτων. Στη δεύτερη περίπτωση, ο επιτιθέμενος αρχίζει να προωθεί πακέτα από πολλούς κόμβους και, ως εκ τούτου, μπορεί να εκτελέσει άλλες επιθέσεις, όπως επιλεκτική προώθηση.

- Εντοπισμός (Homing): Πραγματοποιείται ανάλυση της κίνησης και του δικτύου προκειμένου να προσδιοριστούν οι βασικοί κόμβοι του δικτύου. Αυτοί οι κόμβοι γίνονται οι καλύτεροι υποψήφιοι για άλλες επιθέσεις.

2.1.4 Επιθέσεις ενάντια στο στρώμα μεταφοράς

- Αποσυγχρονισμός (De-synchronization): Πρώτον, οι επιτιθέμενοι υποδύονται έναν νόμιμο κόμβο. Στη συνέχεια, ζητούν την επαναμετάδοση σωστά μεταδιδόμενων πακέτων σε μια νόμιμη σύνδεση που έχει δημιουργηθεί με έναν άλλο κόμβο του δικτύου. Με αυτόν τον τρόπο, οι νόμιμοι κόμβοι κάνουν κατάχρηση των πόρων τους σε ανώφελες επαναμεταδόσεις.

- Πλημμύρα (Flooding): Οι επιτιθέμενοι στέλνουν επανειλημμένα αιτήματα σύνδεσης σε άλλους κόμβους, έτσι ώστε αυτοί να δεσμεύουν και να εξαντλούν τους πόρους τους.

2.1.5 Επιθέσεις ενάντια στο στρώμα εφαρμογής

- Κατακλυσμός (Deluge): Οι επιτιθέμενοι εκμεταλλεύονται τα συστήματα over-the-air για τον απομακρυσμένο επαναπρογραμματισμό των κόμβων.

- DoS με βάση τη διαδρομή (Path-based DoS): Διπλά πακέτα εφαρμογών εισάγονται σε κόμβους φύλλων. Με τον τρόπο αυτό, τα πακέτα προωθούνται μέχρι το σταθμό βάσης, όπου απορρίπτονται. Αυτό καταναλώνει πόρους και εμποδίζει άλλους κόμβους να στείλουν τα πακέτα τους.

- Υπερφόρτωση (Overwhelm): Υπερδιέγερση των αισθητήρων στους κόμβους φύλλων για τη δημιουργία μεγάλων ποσοτήτων πακέτων που διασχίζουν και κορεστούν πολλαπλές διαδρομές.

- Υποκλοπή (Eavesdropping) : Οι επιτιθέμενοι διαβάζουν πακέτα που μεταδίδονται μεταξύ δύο νόμιμων κόμβων.

- Επανάληψη (Re-play): Οι επιτιθέμενοι μεταδίδουν εκ νέου ήδη αποσταλμένα νόμιμα πακέτα.

2.2 Βασικά Αντίμετρα

Οι επιθέσεις που αναφέρθηκαν στην προηγούμενη ενότητα μπορούν να χρησιμοποιηθούν για να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και τη μη απόρριψη δεδομένων. Για την προστασία των δικτύων από αυτές τις επιθέσεις, οι ερευνητές έχουν προτείνει πολλά αντίμετρα [31]. Στην παρούσα ενότητα συζητούνται οι κυριότεροι μηχανισμοί προστασίας που έχουν βρεθεί στη βιβλιογραφία. Βασικά, οι επιθέσεις εμπιστευτικότητας έχουν δύο κύριες προελεύσεις: φυσική πρόσβαση στη μνήμη του κόμβου ή υποκλοπή των ασύρματων μεταδόσεων. Στα WSN έξυπνων πόλεων, η φυσική πρόσβαση είναι εύκολη σε πολλές περιπτώσεις, καθώς οι κόμβοι αισθητήρων αναπτύσσονται απροστάτευτοι στους δρόμους. Το ανθεκτικό στην παραβίαση υλικό είναι ένα ισχυρό αντίμετρο σε αυτή την περίπτωση. Ωστόσο, για τις περισσότερες υπηρεσίες έξυπνης πόλης είναι πολύ ακριβό για να εφαρμοστεί σε όλους τους κόμβους. Έχουν προταθεί άλλες πιο οικονομικές εναλλακτικές λύσεις: η συσκότιση κώδικα και η πιστοποίηση κώδικα [32]. Στην απόκρυψη κώδικα, χρησιμοποιούνται ορισμένες τεχνικές για να καταστήσουν τον κώδικα και τα δεδομένα πιο δυσανάγνωστα, αυξάνοντας, έτσι, τον χρόνο που απαιτείται για την εκτέλεση μιας επίθεσης. Η βεβαίωση κώδικα χρησιμοποιείται για να ελεγχθεί εάν ο εκτελούμενος κώδικας έχει τροποποιηθεί.

Τα προβλήματα εμπιστευτικότητας λόγω της ασύρματης φύσης των WSN αντιμετωπίζονται συνήθως με κρυπτογραφικές λύσεις. Δεδομένου ότι οι πρώτοι κόμβοι WSN σχεδιάστηκαν με ελάχιστη επεξεργαστική ισχύ, τα παλαιά συστήματα που βασίζονται σε αυτά τα δίκτυα δεν είναι σε θέση να εκτελέσουν οποιονδήποτε κρυπτογραφικό αλγόριθμο. Ωστόσο, τα τελευταία χρόνια, οι κατασκευαστές έχουν αναπτύξει πιο ισχυρούς κόμβους και έχουν σχεδιαστεί νέα πρωτόκολλα που λαμβάνουν υπόψη τους κρυπτογραφικές απαιτήσεις. Για παράδειγμα, οι

προδιαγραφές των πιο δημοφιλών πρωτοκόλλων επικοινωνίας για WSN, π.χ. το πρότυπο IEEE 802.15.4 και το ZigBee, περιλαμβάνουν διαφορετικούς τρόπους ασφαλείας που βασίζονται στη συμμετρική κρυπτογραφία. Για ορισμένες περιπτώσεις έχει επίσης προταθεί η ασύμμετρη κρυπτογραφία.

Η κρυπτογραφία είναι επίσης ένας μηχανισμός για την αποφυγή επιθέσεων ακεραιότητας και μη απόρριψης. Τα αθροίσματα ελέγχου και οι κώδικες ελέγχου ταυτότητας μηνύματος είναι τα συνήθη αντίμετρα για την παρεμπόδιση μη αντιληπτών τροποποιήσεων των πακέτων κατά τη μεταφορά. Ο κόμβος προορισμού ενός τροποποιημένου πακέτου το απορρίπτει εάν το πακέτο που λαμβάνει και ο κώδικας που παράγεται από τον μηχανισμό ακεραιότητας μηνύματος δεν ταιριάζουν. Ωστόσο, οι επιθέσεις ακεραιότητας δύσκολα γίνονται αντιληπτές από τους διαχειριστές της πόλης, καθώς τα περισσότερα WSN δεν στέλνουν πληροφορίες στο σταθμό βάσης που να υποδεικνύουν τους λόγους για τους οποίους απορρίπτονται πακέτα. Ως εκ τούτου, από την κεντρική οπτική γωνία των διαχειριστών έξυπνων πόλεων, τα ίχνη αυτού του τύπου επίθεσης μπορούν να εξομοιωθούν με τα ίχνη των επιθέσεων κατά της διαθεσιμότητας δεδομένων.

Οι επιθέσεις διαθεσιμότητας συνήθως επικεντρώνονται στη διακοπή της επικοινωνίας σε ορισμένες περιοχές και στην εξάντληση των μπαταριών των κόμβων. Αν και υπάρχουν λύσεις στη βιβλιογραφία για την αποφυγή αυτού του τύπου επιθέσεων, δεν είναι πάντα αποτελεσματικές ή εφαρμόσιμες. Για παράδειγμα, η μεταπήδηση συχνότητας

διασποράς φάσματος χρησιμοποιείται για την αποφυγή ορισμένων τύπων επιθέσεων παρεμβολής με τη συνεχή αλλαγή του καναλιού μετάδοσης εντός της ζώνης συχνοτήτων του πρωτοκόλλου. Ωστόσο, οι συσκευές παρεμβολής που διατίθενται σήμερα στην αγορά μπορούν να παρεμβάλλουν όλα τα κανάλια που χρησιμοποιούνται από πολλά πρωτόκολλα ταυτόχρονα.

Ως εκ τούτου, γίνεται αντιληπτό ότι οι επιθέσεις μπορούν να επιτύχουν και να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και τη μη άρνηση απόρριψης δεδομένων. Αν και υπάρχουν αντίμετρα για να σταματήσουν ή τουλάχιστον να επιβραδύνουν τις επιθέσεις, στο πλαίσιο αυτό τα εμπόδια

ασφαλείας είναι συχνά διαπερατά. Επομένως, η καλύτερη προσέγγιση μετριασμού είναι μια καλή στρατηγική ανίχνευσης. Παρόλο που πολλές πληροφορίες για τον εντοπισμό των επιθέσεων έχουν ήδη χαθεί όταν φτάνουν στα κέντρα δεδομένων των έξυπνων πόλεων, είναι σημαντικό τουλάχιστον να ανιχνεύεται ότι τα δίκτυα δέχονται επιθέσεις, προκειμένου να αυξηθεί η ισχύς των εφαρμοζόμενων μέτρων ασφαλείας και να ωθηθούν οι πάροχοι WSN να βελτιώσουν την ασφάλεια του δικτύου τους. Πράγματι, σε ένα πλαίσιο έξυπνης πόλης, η ανακάλυψη ότι ορισμένα στοιχεία WSN δέχονται επίθεση είναι ιδιαίτερα σημαντική, δεδομένου ότι πολλά από τα στοιχεία χρησιμοποιούνται από κοινού από διαφορετικά δίκτυα (π.χ. πύλες). Έτσι, ορισμένες επιθέσεις δεν παραμένουν απομονωμένες σε ένα μόνο σύστημα και μπορεί να έχουν συνέπειες για πολλές υπηρεσίες και παρόχους.

2.3 Ανίχνευση Εισβολής

Στον ερευνητικό τομέα της ανίχνευσης εισβολών, μπορούν να διακριθούν δύο τύποι τεχνικών: η ανίχνευση κακής χρήσης και η ανίχνευση ανωμαλιών. Ενώ η πρώτη αναζητά ίχνη που αφήνουν οι επιτιθέμενοι στα δεδομένα ασφαλείας (π.χ. αρχεία καταγραφής συστήματος), η δεύτερη αναλύει την κανονική συμπεριφορά του συστήματος και επισημαίνει ασυνήθιστες αλλαγές. Οι τεχνικές ανίχνευσης εισβολών που αναζητούν καταχρήσεις βασίζονται σε μια εκτεταμένη βάση δεδομένων με υπογραφές επιθέσεων. Μια υπογραφή επίθεσης είναι μια ακολουθία τυπικών ενεργειών που μπορούν να καταγραφούν σε ένα αρχείο καταγραφής ασφαλείας. Η υπογραφή μπορεί να χρησιμοποιηθεί για τον εντοπισμό της προσπάθειας ενός επιτιθέμενου να εκμεταλλευτεί μια γνωστή ευπάθεια δικτύου, λειτουργικού συστήματος ή εφαρμογής. Οι συναγερμοί ενεργοποιούνται όταν το σύστημα ανίχνευσης ανακαλύπτει μια ακολουθία γεγονότων που ταιριάζει με κάποια από τις υπογραφές. Το κύριο πλεονέκτημα αυτού του τύπου ανίχνευσης είναι το χαμηλό ποσοστό ψευδώς θετικών αποτελεσμάτων. Στο πλαίσιο των WSN σε έξυπνες πόλεις, η ανίχνευση βάσει υπογραφών είναι χρήσιμη για τον εντοπισμό επιθέσεων που στοχεύουν σε δίκτυα με τακτική συμπεριφορά (π.χ. περιβαλλοντικοί αισθητήρες που στέλνουν μετρήσεις κάθε μέρα την ίδια ώρα) ή σε εξαιρετικά αξιόπιστες υπηρεσίες. Σε αυτές τις δύο περιπτώσεις μπορούν να δημιουργηθούν απλοί κανόνες για την ενεργοποίηση ειδοποιήσεων όταν δεν λαμβάνονται οι

αναμενόμενες μετρήσεις ή όταν χάνεται ένας συγκεκριμένος αριθμός πακέτων. Παρόλα αυτά, πολλές υπηρεσίες έξυπνων πόλεων δεν ακολουθούν ένα κανονικό μοτίβο και το WSN είναι μια αναξιόπιστη τεχνολογία, όπου ορισμένα πακέτα περιστασιακά δεν παραδίδονται [33].

Εναλλακτικά, οι τεχνικές ανίχνευσης εισβολών που αναζητούν ανωμαλίες είναι σε θέση να εντοπίσουν αλλαγές στο σύστημα που δεν ταιριάζουν με την κανονική συμπεριφορά. Δεδομένης της σημασίας αυτού του τύπου ανίχνευσης εισβολής για την παρούσα διατριβή, η επόμενη ενότητα παρέχει περισσότερες λεπτομέρειες σχετικά με σχετικά με αυτό.

2.4 Ανίχνευση Ανωμαλιών

Η ανίχνευση ανωμαλιών έχει χρησιμοποιηθεί ευρέως σε πολλούς τομείς εφαρμογών. Οι πιο συνηθισμένες τεχνικές εμπίπτουν στο πεδίο της στατιστικής, της ομαδοποίησης και της μηχανικής μάθησης. Ανάλογα με τους τύπους των δειγμάτων που απαιτούνται για την επεξεργασία των δεδομένων, οι τεχνικές αυτές διακρίνονται σε επιβλεπόμενες, ημιεπιβλεπόμενες ή μη επιβλεπόμενες. Οι τεχνικές με επίβλεψη απαιτούν ένα σύνολο δεδομένων εκπαίδευσης με ετικέτες που υποδεικνύουν την κατηγορία κάθε δείγματος (π.χ. "καμία επίθεση", "παρεμβολές" ή "επιλεκτική προώθηση"). Στη συνέχεια, δημιουργείται ένα μοντέλο για την ταξινόμηση νέων μη επισημασμένων δειγμάτων σε μία από τις καθορισμένες κατηγορίες. Οι τεχνικές με ημιεπίβλεψη απαιτούν ένα σύνολο δεδομένων εκπαίδευσης με δείγματα μιας μόνο κατηγορίας προκειμένου να δημιουργηθεί ένα μοντέλο που ταξινομεί τα νέα δείγματα ως ανήκοντα σε αυτή την κατηγορία ή όχι. Τέλος, οι τεχνικές χωρίς επίβλεψη δεν απαιτούν επισημειωμένα δεδομένα εκπαίδευσης και είναι ικανές να χωρίζουν ένα σύνολο δεδομένων σε διάφορα υποσύνολα χωρίς να έχουν προηγουμένως μάθει κάποιο μοντέλο. Επιπλέον, οι αλγόριθμοι ανίχνευσης ανωμαλιών μπορούν επίσης να διαχωριστούν σαφώς μεταξύ μονομεταβλητών αλγορίθμων (μόνο μία μεταβλητή χρησιμοποιείται στην ανάλυση) και πολυμεταβλητών αλγορίθμων (πολλές μεταβλητές χρησιμοποιούνται στην ανάλυση). Στους μονομεταβλητούς αλγορίθμους, συνηθίζεται ο υπολογισμός ενός ανώτερου και ενός κατώτερου ορίου πέρα από το οποίο τα δεδομένα θεωρούνται ανώμαλα. Ως παράδειγμα, η μέθοδος Tukey [34] είναι δημοφιλής για

τον υπολογισμό αυτών των ορίων από ένα αριθμητικό σύνολο δεδομένων. Στη μέθοδο αυτή ορίζονται δύο τύποι ορίων: οι εσωτερικοί και οι εξωτερικοί φράκτες. Οι πρώτοι υπολογίζονται αφαιρώντας και προσθέτοντας 1,5 φορά τη διατεταρτημοριακή απόσταση του συνόλου δεδομένων (δηλαδή την απόσταση μεταξύ του πρώτου και του τρίτου τεταρτημορίου) στο πρώτο και το τρίτο τεταρτημόριο αντίστοιχα. Αυτό ορίζει πολύ αυστηρά κατώτατα όρια, γεγονός που συνεπάγεται υψηλή πιθανότητα εντοπισμού ορισμένων κανονικών περιπτώσεων ως ακραίων τιμών. Οι εξωτερικοί φράκτες αντιπροσωπεύουν έναν πιο χαλαρό τρόπο ορισμού των ορίων. Οι εξωτερικοί φράκτες υπολογίζονται με την αφαίρεση και την πρόσθεση 3 φορές της ενδοτεταρτημοριακής απόστασης στο πρώτο και στο τρίτο τεταρτημόριο αντίστοιχα. Για τον υπολογισμό των ορίων με αυτή τη μέθοδο, συνιστάται τα μεγάλα σύνολα δεδομένων να μην είναι ιδιαίτερα λοξά. Ένας άλλος τρόπος υπολογισμού των ορίων με μονομεταβλητούς αλγορίθμους είναι η χρήση αυτοπαλίνδρομων μοντέλων [35], όπως ο αυτοπαλίνδρομος ολοκληρωμένος κινητός μέσος όρος (ARIMA). Αυτά τα μοντέλα βασίζονται στην υπόθεση ότι κάθε τιμή συσχετίζεται κατά κάποιο τρόπο με τις προηγούμενες καταγεγραμμένες τιμές. Με αυτόν τον τρόπο, τα αυτοπαλινδρομικά μοντέλα χρησιμοποιούν προηγούμενες τιμές για να προβλέψουν μελλοντικές τιμές εντός ενός διαστήματος εμπιστοσύνης. Το κατώτερο και το ανώτερο όριο του διαστήματος μπορούν να χρησιμοποιηθούν ως κατώτατα όρια για την επισήμανση ανωμαλιών. Τα αυτοπαλινδρομικά μοντέλα είναι πολύ συνηθισμένα στην ανάλυση χρονοσειρών.

Η ανίχνευση πολυμεταβλητών ανωμαλιών αντιμετωπίζεται γενικά με τεχνικές μηχανικής μάθησης και ομαδοποίησης. Οι ευρέως χρησιμοποιούμενοι αλγόριθμοι είναι οι μηχανές διανυσμάτων υποστήριξης, ο πλησιέστερος γείτονας και ο τοπικός παράγοντας εξαιρέσεων. Ανάλογα με τα χαρακτηριστικά του συγκεκριμένου σεναρίου και τις απαιτήσεις της εφαρμογής, ορισμένοι αλγόριθμοι αποδίδουν καλύτερα από άλλους. Για παράδειγμα, οι συγγραφείς συγκρίνουν διάφορες μη επιβλεπόμενες προσεγγίσεις που βασίζονται στον τοπικό παράγοντα ακραίων τιμών, στους κοντινούς γείτονες, στην απόσταση Mahalanobis και στις μηχανές διανυσμάτων υποστήριξης για την ανίχνευση εισβολών σε συμβατικά δίκτυα υπολογιστών. Τα πειράματά τους δείχνουν ότι η προσέγγιση του τοπικού

παράγοντα ακραίων τιμών είναι η πιο κατάλληλη στο πλαίσιο αυτό. Η ανίχνευση ανωμαλιών έχει επίσης χρησιμοποιηθεί σε συστήματα ανίχνευσης εισβολών (IDS) για WSN. Γενικά, οι κόμβοι που περιέχουν στοιχεία IDS συγκεντρώνουν ή/και αναλύουν δεδομένα κατάστασης του δικτύου σχετικά με δραστηριότητες ανώμαλης λειτουργίας των γειτόνων τους. Όταν αυτό συμβαίνει, οι κόμβοι ενεργοποιούν έναν συναγερμό στο σταθμό βάσης. Οι τεχνικές ανίχνευσης ανωμαλιών έχουν εφαρμοστεί σε πολλές εφαρμογές που σχετίζονται με τα WSNs. Για παράδειγμα, οι συγγραφείς της χρησιμοποιούν γεωστατιστική και ανάλυση χρονοσειρών για την ανίχνευση ακραίων τιμών στις μετρήσεις μετεωρολογικών αισθητήρων. Οι συγγραφείς επιλέγουν τη χρονική και χωρική ανίχνευση ακραίων τιμών με βάση πραγματικά δεδομένα (TSOD) ως την πλέον κατάλληλη τεχνική σε αυτό το πλαίσιο. Στα πειράματά τους, οι συγγραφείς υποστηρίζουν ότι η TSOD έχει υψηλή απόδοση και είναι σε θέση να εντοπίσει όλες τις ακραίες τιμές με χαμηλό ποσοστό ψευδώς θετικών αποτελεσμάτων, περίπου 3%. Ωστόσο, αυτές οι τεχνικές είναι εφαρμόσιμες μόνο σε ορισμένα σενάρια στα οποία υπάρχει μια χωροχρονική συσχέτιση και το WSN είναι αρκετά πυκνό.

Η απόσταση Mahalanobis χρησιμοποιείται για την ανίχνευση επιθέσεων εκ των έσω με υψηλή ακρίβεια ανίχνευσης και ανθεκτικότητα (δηλ. το ποσοστό ψευδώς θετικών αποτελεσμάτων παραμένει χαμηλό ακόμη και αν ο αριθμός των απομακρυσμένων αισθητήρων αυξάνεται). Ορισμένοι συγγραφείς υποστηρίζουν ότι οι τεχνικές ανίχνευσης ανωμαλιών που βασίζονται στην απόσταση από τους γείτονες δεν πρέπει να χρησιμοποιούνται στα WSN λόγω της υψηλής υπολογιστικής πολυπλοκότητας. Παρόλα αυτά, από την άποψη των διαχειριστών έξυπνων πόλεων, οι τεχνικές αυτές μπορούν να εξεταστούν επειδή η ανάλυση ανωμαλιών μπορεί να υπολογιστεί σε κέντρα δεδομένων με τη χρήση ισχυρών υπολογιστών. Παρόλο που ορισμένες από τις προαναφερθείσες τεχνικές ανίχνευσης ανωμαλιών και IDS αποδίδουν καλά στην ανίχνευση επιθέσεων, δεν αποτελούν γενικεύσιμη λύση σε ένα ετερογενές πλαίσιο όπως η έξυπνη πόλη. Αυτό οφείλεται στο γεγονός ότι, αφενός, ορισμένες τεχνικές εξαρτώνται υπερβολικά από το πλαίσιο του WSN. Από την άλλη πλευρά, τα IDS συνήθως σχεδιάζονται ad-hoc για να ενσωματώνονται σε ορισμένους ή όλους τους κόμβους συγκεκριμένων WSN. Ως εκ τούτου, τα IDS

μπορούν να θεωρηθούν μόνο ως ένας πρώτος μηχανισμός προστασίας που πρέπει να εφαρμοστεί από τους παρόχους WSN για τα συγκεκριμένα δίκτυά τους. Από την κεντρική προοπτική της διοίκησης έξυπνων πόλεων, η λύση δεν πρέπει να απαιτεί πρόσβαση στους κόμβους WSN ούτε γνώση της συγκεκριμένης τεχνολογίας που χρησιμοποιείται από κάθε εξωτερικό πάροχο.

3 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΝΟΣ ΔΙΚΤΥΟΥ ΑΙΣΘΗΤΗΡΩΝ ΑΝΙΧΝΕΥΣΗΣ ΑΝΩΜΑΛΙΩΝ

Τα προηγούμενα κεφάλαια έδειξαν πώς τα συστήματα έξυπνων πόλεων αυξάνουν τη διασυνδεσιμότητα μεταξύ των υποδομών και δημιουργούν νέους τρόπους διάδοσης ευπαθειών και εκμετάλλευσης των εξαρτήσεων των υποδομών, προκαλώντας ζημίες σε τρίτους. Είδαμε επίσης ότι τα WSN αποτελούν βασικά στοιχεία για τη συλλογή αστικών δεδομένων, αλλά, ταυτόχρονα, χρησιμοποιούν τεχνολογία που είναι λιγότερο αξιόπιστη και ευκολότερα προσβλητή από τα συμβατικά δίκτυα. Προκειμένου να επιτύχουν την ταχεία ανάπτυξη των WSNs και της τεχνολογίας έξυπνων πόλεων, οι πόλεις έχουν επωφεληθεί από υπηρεσίες που προμηθεύονται από εξωτερικούς παρόχους- αυτή η εξωτερική ανάθεση δημόσιων υπηρεσιών έχει, ωστόσο, εγείρει ανησυχίες σχετικά με την ασφάλεια. Βασικά, έχουμε παρατηρήσει ότι οι διαχειριστές των έξυπνων πόλεων έχουν χάσει τον έλεγχο των συσκευών του δικτύου και η ορατότητα των WSN για τον εντοπισμό πιθανών ζητημάτων ασφαλείας έχει μειωθεί. Επιπλέον, δεν είναι εφικτό να σχεδιαστούν στρατηγικές και αντίμετρα ασφαλείας που να εφαρμόζονται σε όλους τους τύπους WSN που μπορούν να αναπτυχθούν σε μια πόλη. Παρόλο που οι έξυπνες πόλεις βρίσκονται ακόμη στο ξεκίνημά τους, η ταχεία ανάπτυξή τους έχει οδηγήσει στην ανάπτυξη της πλέον σύγχρονης τεχνολογίας σε ένα νέο πεδίο (δηλαδή την πόλη), με τρόπο που καθιστά δύσκολη την εφαρμογή καθολικών λύσεων ασφάλειας στα WSNs. Τα ακόλουθα χαρακτηριστικά των έξυπνων πόλεων αποτελούν τα τρία βασικά εμπόδια για την εφαρμογή γενικευμένων λύσεων:

- Ετερογένεια: Πολλαπλοί πάροχοι εφαρμόζουν διαφορετικές τεχνολογικές λύσεις, υπό διαφορετικές απαιτήσεις ασφαλείας. Τα παραδοσιακά μέτρα ασφαλείας δεν μπορούν να εφαρμοστούν στα WSN και τα αντίμετρα των WSN δεν καλύπτουν όλες τις περιστάσεις.
- Περιορισμένη πρόσβαση: Οι πάροχοι συνήθως περιορίζουν την πρόσβαση των δημόσιων διοικήσεων στον εξοπλισμό τους. Κατά συνέπεια, η ενδελεχής ανάλυση της ασφάλειας στα WSN μπορεί να πραγματοποιηθεί μόνο από τους παρόχους. Παρ' όλα αυτά, οι διαχειριστές έξυπνων πόλεων είναι οι μόνοι φορείς που διαθέτουν πληροφορίες από όλους τους παρόχους και τις

υπηρεσίες. Ως εκ τούτου, περιστατικά που αφορούν πολλούς παρόχους ή προκαλούν αλυσιδωτές επιπτώσεις μπορούν να μελετηθούν μόνο από τους διαχειριστές έξυπνων πόλεων.

- Δυσκολία ενημέρωσης: Οι ενημερώσεις του συστήματος γίνονται πολύ δαπανηρές και μερικές φορές ακόμη και αδύνατες στα WSN, επειδή ορισμένα δίκτυα δεν προσφέρουν κανάλι επικοινωνίας downlink από τα κέντρα δεδομένων στους αισθητήρες και, επομένως, οι αισθητήρες πρέπει να έχουν φυσική πρόσβαση προκειμένου να ενημερώσουν το λογισμικό τους. Ως εκ τούτου, τα πρόσφατα ανακαλυφθέντα τρωτά σημεία στα WSNs συχνά μένουν ανεκμετάλλευτα μετά την ανάπτυξή τους.

Ως εκ τούτου, δεν υπάρχουν επί του παρόντος λύσεις ασφαλείας που να μπορούν να χρησιμοποιήσουν οι διαχειριστές έξυπνων πόλεων για να διαχειριστούν επιτυχώς την ασφάλεια των WSN με ολιστικό τρόπο. Έτσι, τα κύρια εμπόδια ασφαλείας εφαρμόζονται και ελέγχονται μόνο από τους παρόχους. Στην παρούσα διατριβή, προτείνουμε τη βελτίωση της ασφάλειας των WSN στις έξυπνες πόλεις με μια πλατφόρμα ανίχνευσης εισβολών για τους διαχειριστές των έξυπνων πόλεων. Με αυτόν τον τρόπο, τα δεδομένα WSN που αποστέλλονται από τους παρόχους μπορούν να αναλύονται αναζητώντας επιθέσεις και άλλες αστοχίες και, ως εκ τούτου, οι διαχειριστές των έξυπνων πόλεων μπορούν να πιέσουν τους παρόχους να εφαρμόσουν τα καταλληλότερα αντίμετρα ασφαλείας στα δίκτυά τους. Στο παρόν κεφάλαιο παρουσιάζεται η αρχιτεκτονική αυτής της πλατφόρμας. Η προτεινόμενη αρχιτεκτονική προβλέπεται ως ένα πρόσθετο επίπεδο στην αρχιτεκτονική της έξυπνης πόλης πάνω από τα στοιχεία που αναπτύσσουν οι πάροχοι. Με τον τρόπο αυτό, η αρχιτεκτονική είναι διαφανής για τους παρόχους, δεν προσθέτει επιπλέον απαιτήσεις για τους κόμβους WSN, οι οποίοι είναι πολύ περιορισμένοι όσον αφορά την επεξεργαστική ισχύ και την μπαταρία, και είναι συμβατή με τα WSN που έχουν ήδη αναπτυχθεί στις δρόμους.

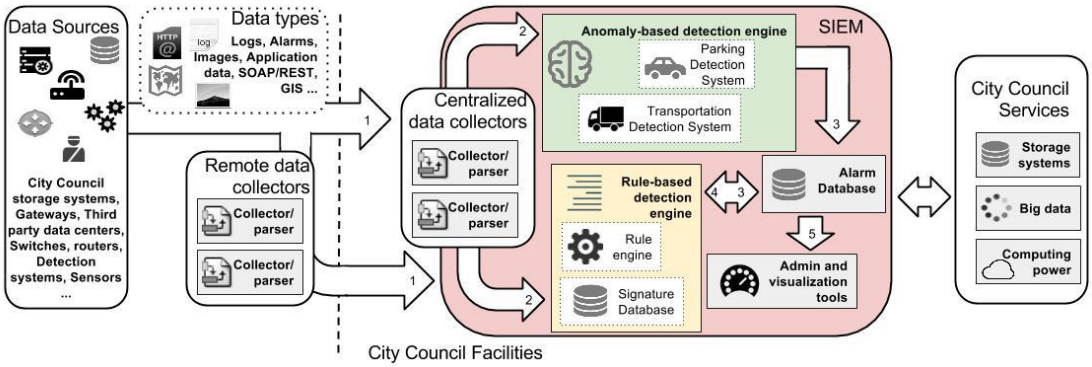
3.1 Κύριες Απαιτήσεις της Αρχιτεκτονικής

Μια γενική πλατφόρμα για την ανίχνευση εισβολών σε WSNs έξυπνων πόλεων πρέπει να σχεδιαστεί από τη σκοπιά των διαχειριστών των έξυπνων πόλεων. Πρώτον, αυτό σημαίνει ότι πρέπει να ληφθεί υπόψη ότι οι διαχειριστές

των έξυπνων πόλεων έχουν μια συγκεντρωτική οπτική γωνία. Ως εκ τούτου, η αρχιτεκτονική πρέπει να είναι ικανή να συλλέγει και να επεξεργάζεται μεγάλο όγκο αδόμητων και ημιδομημένων δεδομένων που αποστέλλονται από τα αστικά WSN. Δεύτερον, συνεπάγεται την αποφυγή των εμποδίων που σχετίζονται με την υψηλή ετερογένεια και την περιορισμένη πρόσβαση των συστημάτων και τις δυσκολίες στην ενημέρωσή τους. Τέλος, η αρχιτεκτονική πρέπει να είναι διαφανής για τους εξωτερικούς παρόχους WSN. Αυτό την καθιστά συμβατή με τα ήδη αναπτυγμένα δίκτυα και με τις χαμηλές δυνατότητες επεξεργασίας ορισμένων κόμβων αισθητήρων. Όσον αφορά τις απαιτήσεις επεξεργασίας δεδομένων, αυτό μπορεί να εξεταστεί στο πλαίσιο των μεγάλων δεδομένων. Η αρχιτεκτονική πρέπει να είναι έτοιμη να συλλέγει, να ευρετηριάζει και να επεξεργάζεται μεγάλο όγκο δεδομένων με υψηλή ταχύτητα και ποικιλία. Υποθέτουμε ότι οι έξυπνες πόλεις διαθέτουν, στους κεντρικούς διακομιστές τους, υψηλή υπολογιστική ισχύ, μεγάλο αποθηκευτικό χώρο και το υπόλοιπο υλικό και απαιτήσεις δικτύου που είναι απαραίτητες για την ανάπτυξη λύσεων μεγάλων δεδομένων.

3.2 Επισκόπηση Αρχιτεκτονικής

Η παρούσα ενότητα λαμβάνει υπόψη τις απαιτήσεις που παρουσιάστηκαν στην προηγούμενη ενότητα και περιγράφει μια κεντρική αρχιτεκτονική για τη συλλογή δεδομένων WSN και την επεξεργασία τους με μια υβριδική μηχανή ανίχνευσης που συνδυάζει μια μηχανή βασισμένη σε κανόνες και μια μηχανή βασισμένη σε ανωμαλίες για την αποκάλυψη περιστατικά στα WSN τρίτων. Τα κύρια στοιχεία και η ροή δεδομένων που απεικονίζονται στο σχήμα 3.1 είναι τα εξής [36]:



Σχήμα 3.1: Επισκόπηση της Αρχιτεκτονικής της πόλης με τους Έξυπνους Αισθητήρες [36]

1. Τα δεδομένα προέρχονται από διάφορες πηγές σε διαφορετικούς τύπους δεδομένων. Γενικά, τα δεδομένα εφαρμογής προέρχονται από τις μετρήσεις των αισθητήρων και τα δεδομένα κατάστασης του δικτύου προέρχονται από πύλες, παρατηρητές ή άλλες συσκευές με αρκετή ικανότητα παρακολούθησης των WSN. Σε ορισμένες περιπτώσεις, προκειμένου να αποκτήσουν μια ακριβή εικόνα του δικτύου, οι κόμβοι WSN καταγράφουν πληροφορίες για την κατάσταση του συστήματος, οι οποίες αποστέλλονται τακτικά ή κατόπιν αιτήματος. Αυτά τα δεδομένα, στη συνέχεια, συλλέγονται, αναλύονται και κανονικοποιούνται από απομακρυσμένους συλλέκτες δεδομένων που κατανέμονται κοντά στις πηγές ή από κεντρικούς συλλέκτες δεδομένων που εγκαθίστανται κοντά στις μηχανές επεξεργασίας.

2. Τα κανονικοποιημένα δεδομένα αποτελούν την είσοδο των δύο μηχανών ανίχνευσης. Από τη μία πλευρά, υπάρχει η μηχανή ανίχνευσης βάσει κανόνων, στόχος της οποίας είναι η ανίχνευση γνωστών επιθέσεων και η συσχέτιση δεδομένων από διαφορετικές πηγές, και, από την άλλη πλευρά, η μηχανή ανίχνευσης βάσει ανωμαλιών, η οποία χρησιμοποιεί τεχνικές μηχανικής μάθησης και στατιστικές τεχνικές για την ανίχνευση ανωμαλιών και άγνωστων επιθέσεων [37].

3. Οι μηχανές ανίχνευσης αναλύουν ανεξάρτητα τα δεδομένα εισόδου και ενεργοποιούν συναγερμούς που αποθηκεύονται σε μια κοινή βάση δεδομένων συναγερμών.

4. Οι συναγερμοί από τη βάση δεδομένων συσχετίζονται από τη μηχανή ανίχνευσης βάσει κανόνων δημιουργώντας νέους συναγερμούς, οι οποίοι είναι πιο αξιόπιστοι, έχουν υψηλότερη προτεραιότητα και γίνονται υποψήφιοι για συσχετισμό σε μελλοντικές επαναλήψεις.

5. Τα εργαλεία διαχείρισης και απεικόνισης προσφέρουν διεπαφές (π.χ. πίνακες οργάνων, ειδοποιήσεις SMS) και μηχανισμούς συνδρομής για την παροχή πληροφοριών σχετικά με τους συναγερμούς και για τη διαχείριση του συστήματος [38].

Η λύση μας αναπτύσσει ένα νέο επίπεδο στους διακομιστές των διαχειριστών έξυπνων πόλεων. Αυτό το στρώμα βρίσκεται εννοιολογικά πάνω από τις συσκευές που χρησιμοποιούνται από τους διάφορους παρόχους. Ως εκ τούτου, δεν επηρεάζεται από την ετερογένεια των διαφορετικών διαμορφώσεων, δεν απαιτεί ειδικά δικαιώματα πάνω σε συσκευές τρίτων και είναι εύκολα προσβάσιμο και επικαιροποιήσιμο.

Επιπλέον, ένα SIEM αποτελεί τον πυρήνα της αρχιτεκτονικής και αυτός ο τύπος συστήματος είναι ικανός να επεξεργάζεται μεγάλα δεδομένα όπως απαιτείται και προσφέρει μηχανισμούς συλλογής δεδομένων από τοπικές και απομακρυσμένες τοποθεσίες κατάλληλες για ανάπτυξη σε ένα πλαίσιο έξυπνης πόλης. Όσον αφορά τα WSN, τα δεδομένα μπορούν να βρεθούν αποθηκευμένα σε διακομιστές έξυπνης πόλης ή σε απομακρυσμένες συσκευές στους δρόμους. Οι μετρήσεις των αισθητήρων, για παράδειγμα, έχουν συνήθως αξία για συγκεκριμένες υπηρεσίες της πόλης. Αυτά τα δεδομένα, επομένως, αποθηκεύονται συνήθως σε έναν συμβατικό διακομιστή και είναι προσβάσιμα εντός των εγκαταστάσεων της έξυπνης πόλης. Ωστόσο, τα δεδομένα κατάστασης του συστήματος (π.χ. αρχεία καταγραφής συσκευών), τα οποία μπορεί να μην έχουν σημασία για οποιοδήποτε άλλο τμήμα έξυπνης πόλης, πρέπει να συλλέγονται απευθείας από τα WSN. Ως εκ τούτου, η προτεινόμενη αρχιτεκτονική που βασίζεται στο SIEM είναι ικανή να συλλέγει απομακρυσμένα και τοπικά δεδομένα χρησιμοποιώντας διαφορετικούς συλλέκτες δεδομένων και προσφέρει μια κεντρική ενιαία πλατφόρμα στην οποία θα επεξεργάζεται και θα συσχετίζει όλες τις

πληροφορίες μαζί. Επιπλέον, η συσχέτιση δεδομένων και η διαχείριση ιστορικών δεδομένων, οι οποίες είναι γενικά πολύ σημαντικές στην ανάλυση ανίχνευσης εισβολών, είναι ιδιαίτερα αποτελεσματικές σε αυτού του είδους την πλατφόρμα. Τέλος, τα παραδείγματα παράλληλου προγραμματισμού, όπως το MapReduce, αποτελούν σύνηθες χαρακτηριστικό των συστημάτων SIEM. Όσον αφορά τα χαρακτηριστικά ανίχνευσης εισβολών της προτεινόμενης αρχιτεκτονικής, καλύπτονται δύο περιπτώσεις. Πρώτον, η μηχανή ανίχνευσης βάσει κανόνων είναι ικανή να βρίσκει μοτίβα στα δεδομένα για τον εντοπισμό επιθέσεων που έχουν ήδη αναφερθεί στη βιβλιογραφία και είναι γνωστές στους ερευνητές ασφάλειας πληροφοριών. Δεύτερον, η μηχανή ανίχνευσης βάσει ανωμαλιών είναι ικανή να προειδοποιεί τους διαχειριστές σε περιπτώσεις καταστάσεων που δεν ακολουθούν την κανονική συμπεριφορά του συστήματος, παρόλο που δεν υπάρχουν μοτίβα που να ταιριάζουν με γνωστές επιθέσεις. Με αυτόν τον τρόπο, οι δημοφιλείς επιθέσεις μπορούν εύκολα να εντοπιστούν και να αποτραπούν, ενώ οι νέες επιθέσεις, που εκμεταλλεύονται άγνωστες ευπάθειες, ενεργοποιούν συναγερμούς που δίνουν στους διαχειριστές έξυπνων πόλεων τα πρώτα προειδοποιητικά σημάδια προκειμένου να ξεκινήσουν πιο εμπεριστατωμένες έρευνες. Επιπλέον, κατά τη στιγμή της δημιουργίας ενός συναγερμού, οι διαχειριστές μπορούν να συσχετίσουν ένα επίπεδο σοβαρότητας με τον συναγερμό και επίσης να ορίσουν μια ενέργεια που θα εκτελεστεί αμέσως μόλις ενεργοποιηθεί ο συναγερμός.

Οι ακόλουθες ενότητες περιγράφουν τα βασικά δεδομένα WSN που είναι διαθέσιμα στους κεντρικούς διακομιστές και μπορούν να χρησιμοποιηθούν από τις μηχανές ανίχνευσης για την αποκάλυψη περιστατικών ασφαλείας. Στη συνέχεια, δίνονται περισσότερες λεπτομέρειες σχετικά με τις δύο μηχανές ανίχνευσης.

3.2.1 Τύποι Δεδομένων

Ακολουθούν οι πιο σημαντικοί τύποι δεδομένων που λαμβάνονται από το WSN στα κέντρα δεδομένων έξυπνων πόλεων. Παρέχονται ορισμένα παραδείγματα για το πώς μπορούν να χρησιμοποιηθούν για την ανίχνευση εισβολών:

- Βασικές πληροφορίες σχετικά με τους κόμβους: ID, γεωγραφικό πλάτος, γεωγραφικό μήκος κ.λπ. Η γεωγραφική θέση αποτελεί βασική παράμετρο για τον προσδιορισμό της περιοχής που επηρεάζεται από τις επιθέσεις.
- Βασικές πληροφορίες για το WSN: σκοπός υπηρεσίας (π.χ. στάθμευση, παρακολούθηση περιβάλλοντος), πρωτόκολλο επικοινωνίας (π.χ. ZigBee, LoRa), κ.λπ. Από αυτές τις πληροφορίες μπορούν να εξαχθούν άλλες πληροφορίες σχετικά με το WSN. Για παράδειγμα, το ZigBee έχει δύο πιθανές τοπολογίες (δηλ. δέντρο και αστέρι) και οι ζώνες συχνοτήτων του στην Ευρώπη είναι είτε 868 MHz είτε 2,4 GHz. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για την απόρριψη πιθανών επιθέσεων κατά μιας υπηρεσίας και για τη συγκέντρωση δεδομένων σε ομάδες.
- Βασικές πληροφορίες για τα πακέτα: αριθμός πακέτου, αναγνωριστικό πύλης, χρονοσφραγίδες κ.λπ. Πρόσθετα πεδία μπορούν να υπολογιστούν από αυτές τις βασικές πληροφορίες, όπως η μονόδρομη καθυστέρηση (OWD), η οποία υποδεικνύει το χρόνο που χρειάζονται τα πακέτα από τους κόμβους αισθητήρων στον διακομιστή. Αυτό είναι ένα σημαντικό πεδίο για την ανίχνευση ορισμένων επιθέσεων, όπως το DoS, καθώς οι επιθέσεις αυτές τείνουν να επιβραδύνουν τη λήψη των πακέτων.
- Βασικές πληροφορίες σχετικά με την κατάσταση του συστήματος: δείκτης ισχύος λαμβανόμενου σήματος (RSSI), λόγος σήματος προς θόρυβο (SNR) κ.λπ. Ορισμένες επιθέσεις έχουν άμεσο αντίκτυπο σε ορισμένες από αυτές τις μεταβλητές. Για παράδειγμα, οι επιθέσεις που δημιουργούν παρεμβολές επηρεάζουν το RSSI.
- Πληροφορίες σχετικά με τις υπηρεσίες: ενδείξεις αισθητήρων, δεδομένα υπηρεσιών συγκεντρωμένα σε χρονικά διαστήματα, κ.λπ. Τα δεδομένα αυτά αποστέλλονται είτε σε προγραμματισμένα τακτικά χρονικά διαστήματα (π.χ. περιβαλλοντικά δεδομένα) είτε όταν οι αισθητήρες έχουν αντιδράσει σε μια περιβαλλοντική κατάσταση. (π.χ. δραστηριότητα στάθμευσης). Οι ανωμαλίες σε αυτά τα δεδομένα μπορεί να υποδηλώνουν κακή βαθμονόμηση αισθητήρες και επιθέσεις ακεραιότητας δεδομένων.

- Κατάσταση μπαταρίας: Στόχος πολλών επιθέσεων WSN είναι η εξάντληση των μπαταριών των αισθητήρων. Ως εκ τούτου, η πληροφορία αυτή είναι πολύ χρήσιμη για την ανίχνευση αυτού του είδους των επίθεσης.

3.2.2 Μηχανή ανίχνευσης βασισμένη σε κανόνες

Η μηχανή ανίχνευσης βάσει κανόνων παρέχει στο σύστημα μια μονάδα συναγερμού ικανή να εντοπίζει επιθέσεις που καταγράφονται ως υπογραφές σε μια βάση δεδομένων. Οι κανόνες που ορίζουν τις υπογραφές στη βάση δεδομένων καθορίζουν τα ίχνη που πρέπει να εμφανίζονται στα δεδομένα για να ενεργοποιηθεί ένας συναγερμός. Επιπλέον, υλοποιούνται συναγερμοί που ορίζουν ένα χρονοδιάγραμμα, ένα επίπεδο σοβαρότητας και τις ενέργειες που πρέπει να εκτελεστούν (π.χ. προειδοποίηση διαχειριστή, εκτέλεση ορισμένων διεργασιών).

Οι κανόνες δημιουργούνται με δύο σκοπούς- πρώτον, για την εύρεση αποδείξεων ανεπιθύμητων καταστάσεων (π.χ. ίχνη απορριπτόμενων συνδέσεων, παράμετροι που υπερβαίνουν ένα όριο). Δεύτερον, οι κανόνες κατασκευάζονται επίσης για να συσχετίσουν πολλαπλά στοιχεία που βρέθηκαν σε διαφορετικά στοιχεία του δικτύου ή/και σε διαφορετικές χρονικές στιγμές. Οι κανόνες συσχέτισης εκμεταλλεύονται το γεγονός ότι ορισμένες επιθέσεις αφήνουν ίχνη σε διάφορα μέρη του συστήματος εντός ενός περιορισμένου χρονικού παραθύρου. Αυτά τα ίχνη είναι συνήθως συνέπεια των διαφόρων βημάτων που απαιτούνται για την εκτέλεση μιας επίθεσης ή της επιμονής του επιτιθέμενου μετά την αποτυχία.

Η προτεινόμενη αρχιτεκτονική συγκεντρώνει όλα τα στοιχεία ύποπτης συμπεριφοράς στα WSN της έξυπνης πόλης σε ένα ενιαίο σύστημα. Και οι δύο μηχανές ανίχνευσης ενεργοποιούν συναγερμούς σε περίπτωση θεωρητικών ανεπιθύμητων συμβάντων. Ωστόσο, ένας μεγάλος αριθμός αυτών των συναγερμών μπορεί να ταξινομηθεί ως ψευδείς συναγερμοί ή οφείλονται σε ασήμαντες ή παροδικές καταστάσεις. Ως εκ τούτου, η πραγματική πρόκληση δεν είναι μόνο η σύνταξη αποτελεσματικών συναγερμών, αλλά και η προειδοποίηση των διαχειριστών μόνο όταν η αξιοπιστία και η σοβαρότητα των συναγερμών είναι αρκετά υψηλές. Αυτό μπορεί να επιτευχθεί με τη δημιουργία συναγερμών που βασίζονται σε κανόνες συσχέτισης, όπως δείχνει το Σχήμα 3.1. Σε αυτό το σχήμα, το

4 στο σχήμα ροής δεδομένων υποδηλώνει ότι οι συναγερμοί, οι οποίοι έχουν ήδη ενεργοποιηθεί, χρησιμοποιούνται ξανά στη μηχανή ανίχνευσης βάσει κανόνων. Με αυτόν τον τρόπο, οι συναγερμοί που επηρεάζουν τα ίδια εξαρτήματα, την ίδια περιοχή, το ίδιο εύρος ζώνης κ.λπ. συσχετίζονται, ενεργοποιώντας έναν πιο αξιόπιστο συναγερμό. Για να απλοποιηθεί ο ορισμός κανόνων για μια ολόκληρη έξυπνη πόλη, οι διαχειριστές του συστήματος μπορούν να χρησιμοποιούν δημόσια διαθέσιμες βάσεις δεδομένων υπογραφών.

Επιπλέον, μια έξυπνη πόλη είναι ένα πολύ μεταβλητό σενάριο. Οι δημόσιες βάσεις δεδομένων μπορούν να βοηθήσουν τους διαχειριστές να διατηρούν μια ενημερωμένη συλλογή υπογραφών που περιλαμβάνει πρόσφατα ανακαλυφθείσες ευπάθειες, νέα στοιχεία, διαμορφώσεις δικτύου κ.λπ. Ωστόσο, εξακολουθεί να αποτελεί ανοιχτό πρόβλημα η εξεύρεση ενός κατάλληλου τρόπου διαχείρισης βάσεων δεδομένων υπογραφών σε μεγάλα και εξαιρετικά ετερογενή συστήματα όπως οι έξυπνες πόλεις. Στην επόμενη ενότητα παρουσιάζεται η μηχανή ανίχνευσης με βάση τις ανωμαλίες, η οποία μπορεί να ανιχνεύει άγνωστες επιθέσεις και, ως εκ τούτου, μπορεί να βοηθήσει τους διαχειριστές να ανακαλύψουν ότι ορισμένες υπογραφές λείπουν ή είναι ξεπερασμένες.

3.2.2 Μηχανή Ανίχνευσης με Βάση τις ανωμαλίες

Η μηχανή ανίχνευσης βάσει κανόνων παρέχει στους διαχειριστές ένα εύχρηστο εργαλείο για τον εντοπισμό επιθέσεων, αναζητώντας τα ίχνη που αφήνουν οι επιθέσεις στα δεδομένα. Ωστόσο, αυτή η μηχανή έχει αρκετούς περιορισμούς, οι οποίοι αποκλείουν τη στήριξη αποκλειστικά σε αυτόν τον μηχανισμό ανίχνευσης εισβολών για την αποτελεσματική ανίχνευση επιθέσεων στο πλαίσιο που περιγράφεται στην παρούσα διατριβή. Οι κυριότεροι περιορισμοί είναι οι εξής:

- Ο μηχανισμός ανίχνευσης βάσει κανόνων είναι ιδιαίτερα χρήσιμος έναντι επιθέσεων που είναι σαφώς αναγνωρίσιμες μέσω κατωφλίων και οι οποίες θεωρούνται σταθερές μακροπρόθεσμα. Ωστόσο, σε ένα μεταβαλλόμενο περιβάλλον όπως η έξυπνη πόλη, τα στατικά κατώφλια είναι συνήθως δύσκολο να καθοριστούν, επειδή το περιβάλλον είναι δυναμικό και αλλάζει

ανάλογα με την ώρα της ημέρας, την εποχή του έτους, τις καιρικές συνθήκες κ.λπ.

- Οι άγνωστες επιθέσεις, για τις οποίες δεν ορίζονται κανόνες, παραμένουν απαρατήρητες.
- Οι κανόνες που περιλαμβάνουν πολλές μεταβλητές γίνονται πολύ πολύπλοκοι και είναι δύσκολο να συντηρηθούν.
- Η εύρεση προκαθορισμένων κατωφλίων για ορισμένες μεταβλητές δεν είναι μερικές φορές δυνατή.
- Το σύνολο των κανόνων που ορίζονται ad hoc από τους διαχειριστές απαιτεί χειροκίνητη συντήρηση, η οποία είναι δαπανηρή και δεν κλιμακώνεται καλά.

Για να ξεπεραστούν αυτά τα προβλήματα, είναι απαραίτητο να συμπληρωθεί η μηχανή ανίχνευσης βάσει κανόνων με άλλους μηχανισμούς. Για το σκοπό αυτό, η προτεινόμενη αρχιτεκτονική περιλαμβάνει μια μηχανή ανίχνευσης με βάση τις ανωμαλίες. Αυτή η μηχανή έχει την ευθύνη του αυτόματου υπολογισμού των κατωφλίων και της εκπαίδευσης σύνθετων μοντέλων μηχανικής μάθησης ικανών να εντοπίζουν περιπτώσεις ανώμαλων δεδομένων που οφείλονται σε επιθέσεις ή αποτυχίες στα WSN της έξυπνης πόλης. Όπως είδαμε στην ενότητα 3.2.1, τα δεδομένα που αναλύονται με αυτή τη μηχανή περιλαμβάνουν μετρήσεις αισθητήρων, αρχεία καταγραφής κατάστασης δικτύου κ.λπ. Στο εξής, τα πεδία ενός συνόλου δεδομένων που μπορούν να χρησιμοποιηθούν για την ανάλυση ανωμαλιών αναφέρονται ως μεταβλητές. Η ενότητα 2.4 έδειξε ότι, στη βιβλιογραφία, υπάρχουν πολλαπλές τεχνικές ανίχνευσης ανωμαλιών ικανές να εκτελέσουν ανάλυση σε δεδομένα για την αποκάλυψη τέτοιων τύπων καταστάσεων. Γενικά, οι τεχνικές αυτές απαιτούν ένα σύνολο δεδομένων από δείγματα για την εκπαίδευση των μοντέλων. Τα μοντέλα χρησιμοποιούνται στη συνέχεια για να προβλέψουν αν τα νέα δείγματα είναι φυσιολογικά ή όχι. Λαμβάνοντας αυτό υπόψη, τα κύρια χαρακτηριστικά της μηχανής ανίχνευσης προβολής μπορούν να συνοψιστούν στα ακόλουθα τέσσερα σημεία:

1. Χρησιμοποιεί αλγορίθμους χωρίς επίβλεψη ή με ημιεπίβλεψη.

2. Η συντριπτική πλειονότητα των δειγμάτων στα σύνολα δεδομένων εκπαίδευσης συλλαμβάνονται κατά τη διάρκεια κανονικών καταστάσεων μη επίθεσης.

3. Τα σύνολα δεδομένων εκπαίδευσης συλλέγονται δειγματοληπτικά περιλαμβάνοντας παρατηρήσεις από τις περισσότερες από τις διαφορετικές καταστάσεις που μπορεί να εμφανιστούν στην παρακολουθούμενη υπηρεσία.

4. Τα σύνολα δεδομένων εκπαίδευσης είναι μεγάλα.

Όσον αφορά το πρώτο σημείο, οι αλγόριθμοι μηχανικής μάθησης με επίβλεψη απαιτούν την επισήμανση κάθε δείγματος εκπαίδευσης με την κλάση στην οποία ανήκει. Για τους αλγορίθμους αυτούς, στο πλαίσιο της ανίχνευσης εισβολών, θα πρέπει να περιλαμβάνεται στα δείγματα ένα πρόσθετο πεδίο που να υποδεικνύει αν το δείγμα είναι κανονικό ή ανώμαλο ή, στην περίπτωση υπολογισμού ενός μοντέλου με μία κλάση για κάθε τύπο ανώμαλης κατάστασης, η ετικέτα θα πρέπει να είναι πιο συγκεκριμένη και να υποδεικνύει τον τύπο της κατάστασης (π.χ. "επίθεση παρεμβολής", "επίθεση επιλεκτικής προώθησης"). Στο πλαίσιο της έξυπνης πόλης, είναι πολύ δύσκολο να συγκεντρωθεί μεγάλος όγκος δεδομένων με ετικέτες. Οι διαχειριστές θα μπορούσαν να εκτελέσουν κάποιες προσομοιώσεις επιθέσεων σε ένα testbed ή ακόμη και κατά της πραγματικής υποδομής WSN- ωστόσο, είναι μη ρεαλιστικό να συγκεντρώνονται συστηματικά ολοκληρωμένα σύνολα δεδομένων, που να περιλαμβάνουν πολλά δείγματα από όλες τις επιθέσεις που αναφέρονται στη βιβλιογραφία κάθε φορά που πρέπει να εκπαιδευτούν νέα μοντέλα. Επιπλέον, επιθέσεις που δεν έχουν ακόμη ανακαλυφθεί ή που εκμεταλλεύονται άγνωστα τρωτά σημεία θα περνούσαν απαρατήρητες.

Κατά συνέπεια, η μηχανή ανίχνευσης ανωμαλιών πρέπει να χρησιμοποιεί κυρίως ημι-επιτηρούμενους ή μη-επιτηρούμενους αλγορίθμους. Όσον αφορά το δεύτερο σημείο, τα σύνολα δεδομένων εκπαίδευσης πρέπει να περιέχουν ένα πολύ μεγάλο ποσοστό κανονικών δειγμάτων, επειδή τα μοντέλα ανίχνευσης ανωμαλιών υπολογίζονται συνήθως με την εύρεση ενός ορίου που περικλείει τα περισσότερα δείγματα στο σύνολο δεδομένων εκπαίδευσης. Εάν ένα σύνολο δεδομένων εκπαίδευσης περιέχει υπερβολικά μεγάλο ποσοστό μη φυσιολογικών δειγμάτων, τότε είναι πιθανό ορισμένα από αυτά τα δείγματα να συμπεριληφθούν εντός των

ορίων κανονικότητας. Όσον αφορά το τρίτο σημείο, τα σύνολα δεδομένων εκπαίδευσης πρέπει να περιέχουν μια ολοκληρωμένη αντιπροσώπευση δειγμάτων από τις διάφορες πιθανές κανονικές καταστάσεις και καταστάσεις στην παρακολουθούμενη υπηρεσία. Διαφορετικά, οι κανονικές καταστάσεις που δεν αντιπροσωπεύονται στο σύνολο δεδομένων εκπαίδευσης μπορεί να βρεθούν εκτός των υπολογισμένων ορίων κανονικότητας. Τέλος, όσον αφορά το τέταρτο σημείο, τα σύνολα δεδομένων εκπαίδευσης πρέπει να είναι μεγάλα για τους λόγους που αναφέρθηκαν στα δύο προηγούμενα σημεία. Η χρήση λίγων μόνο δειγμάτων μπορεί να οδηγήσει σε μοντέλα που εκπαιδεύονται με πάρα πολλά δείγματα από παροδικές καταστάσεις του δικτύου ή ασήμαντα παροδικά σφάλματα που δεν αποτυπώνουν την κανονική συμπεριφορά του συστήματος. Επιπλέον, με μικρά σύνολα δεδομένων εκπαίδευσης, η αναλογία των μεταβλητών σε σχέση με τον αριθμό των δειγμάτων αυξάνεται και, επομένως, είναι πιο πιθανό να συμβεί υπερπροσαρμογή [39].

3.3 Σχεδιασμός της μηχανής ανίχνευσης με βάση τις ανωμαλίες

Λαμβάνοντας υπόψη την πολυπλοκότητα της ανίχνευσης εισβολών που βασίζεται στην αποκάλυψη ανωμαλιών στα δεδομένα, η παρούσα ενότητα περιγράφει τις κύριες εκτιμήσεις που πρέπει να ληφθούν υπόψη κατά το σχεδιασμό της μηχανής ανίχνευσης με βάση τις ανωμαλίες. Με σκοπό την εκτέλεση μιας πλήρους και αποτελεσματικής ανάλυσης ανωμαλιών σε μια έξυπνη πόλη, είναι απαραίτητο να αναπτυχθούν τουλάχιστον δύο τύποι αλγορίθμων:

- Μονομεταβλητοί αλγόριθμοι. Με αυτόν τον τύπο αλγορίθμου, οι διαχειριστές μπορούν να παρακολουθούν τη συμπεριφορά μιας μεμονωμένης αριθμητικής μεταβλητής και να εντοπίζουν ανώμαλες τιμές που βρίσκονται εκτός του κανονικού εύρους της. Για παράδειγμα, ανίχνευση μιας ανώμαλης ένδειξης -50°C σε έναν αισθητήρα θερμοκρασίας που βρίσκεται σε μια πόλη με ήπιο κλίμα.
- Πολυμεταβλητοί αλγόριθμοι. Με αυτόν τον τύπο αλγορίθμου, οι διαχειριστές μπορούν να επισημάνουν ανωμαλίες λαμβάνοντας υπόψη πολλές μεταβλητές ταυτόχρονα, ακόμη και όταν κάθε μία από τις μεταβλητές που αναλύονται παραμένει εντός των κανονικών ορίων της. Για

παράδειγμα, μια ένδειξη 0°C σε έναν αισθητήρα θερμοκρασίας μπορεί να θεωρηθεί φυσιολογική το χειμώνα, αλλά μπορεί επίσης να θεωρηθεί ως ανώμαλη το καλοκαίρι, εάν ο αλγόριθμος ανίχνευσης λαμβάνει επίσης υπόψη την εποχή του έτους, τις ενδείξεις άλλων θερμοκρασιών αισθητήρων, κ.λπ.

Αυτά είναι απλά παραδείγματα τυπικής ανάλυσης ανωμαλιών. Ωστόσο, πρέπει να έχουμε κατά νου ότι η ανάλυση ανωμαλιών στις έξυπνες πόλεις μπορεί να είναι πολύ περίπλοκη. Οι ανωμαλίες που εντοπίζονται από μονομεταβλητούς αλγορίθμους που μελετούν μια μόνο μεταβλητή μπορεί να παρέχουν πολύτιμες πληροφορίες για την αποκάλυψη της πηγής ενός συμβάντος. Για παράδειγμα, είναι ευρέως γνωστό ότι οι μη φυσιολογικές τιμές στο RSSI μπορεί να οφείλονται σε παρεμβολές [40]. Επίσης, η μονομεταβλητή ανάλυση στις μετρήσεις αισθητήρων επιτρέπει τον εντοπισμό ακραίων τιμών που προέρχονται από επιθέσεις ακεραιότητας ή αισθητήρες που δεν είναι σωστά βαθμονομημένοι. Ωστόσο, υπάρχουν πολλές επιθέσεις κατά των WSN που δεν μπορούν να εντοπιστούν άμεσα με μονομεταβλητούς αλγορίθμους, επειδή οι επιθέσεις έχουν μειωμένο αντίκτυπο σε μία μόνο από τις λαμβανόμενες μεταβλητές. Η χρήση πολυμεταβλητών αλγορίθμων είναι πιο κατάλληλη για την εξέταση του αντίκτυπου σε πολλές μεταβλητές ταυτόχρονα, αλλά ένας συναγερμός που ενεργοποιείται από έναν από αυτούς τους αλγορίθμους είναι γενικά πιο δύσκολο να συνδεθεί με τις συγκεκριμένες αιτίες του προβλήματος. Ως εκ τούτου, η ανίχνευση εισβολών στα WSN έξυπνων πόλεων δεν είναι ένα απλό έργο και δεν μπορεί να αυτοματοποιηθεί πλήρως και να αντιμετωπιστεί σαν ένα μαύρο κουτί στο οποίο το σύνολο των αλγορίθμων ανίχνευσης ανωμαλιών που παρέχονται μπορεί να χρησιμοποιηθεί για οποιοδήποτε πλαίσιο. Οι διαχειριστές πρέπει να επιλέγουν τις μεταβλητές που θα παρακολουθούνται, να εξάγουν συμπεράσματα στην περίπτωση συναγερμών, να δημιουργούν κανόνες συσχέτισης για την ενεργοποίηση ουσιαστικών συναγερμών που αξίζουν το προσοχή του διαχειριστή, κ.λπ.

- Καταστάσεις στις οποίες η κατανομή της μεταβλητής είναι σχετικά σταθερή στο χρόνο. Με αυτόν τον τρόπο, τα κατώτατα όρια μπορούν να υπολογιστούν από μεγάλες ποσότητες σχετικών τιμών και μπορούν να

χρησιμοποιηθούν για την πρόβλεψη ανωμαλιών σε πολλά δείγματα στο μέλλον. Σε αυτού του είδους τις καταστάσεις, οι διαχειριστές έξυπνων πόλεων θα πρέπει να εξετάσουν το ενδεχόμενο χρήσης της μεθόδου Tukey για τον καθορισμό των κατωφλίων. Πολυάριθμες μελέτες στη βιβλιογραφία έχουν χρησιμοποιήσει με επιτυχία αλγορίθμους που βασίζονται στη μέθοδο Tukey για την εύρεση ακραίων τιμών με καλά αποτελέσματα [41]. Αυτή η στατιστική μέθοδος είναι κατάλληλη σε αυτό το πλαίσιο επειδή είναι απλή, έχει χαμηλό επίπεδο υπολογιστικής πολυπλοκότητας και δεν κάνει υποθέσεις σχετικά με τη στατιστική κατανομή της μεταβλητής.

- Καταστάσεις όπου οι νέες τιμές της μεταβλητής παρουσιάζουν ισχυρή συσχέτιση με τις αμέσως προηγούμενες τιμές. Σε αυτού του είδους τις καταστάσεις, οι διαχειριστές έξυπνων πόλεων θα πρέπει να εξετάσουν το ενδεχόμενο χρήσης αυτοπαλίνδρομων αλγορίθμων, όπως ο ARIMA. Οι αυτοπαλίνδρομοι αλγόριθμοι έχουν χρησιμοποιηθεί ευρέως για την ανίχνευση ακραίων τιμών σε δεδομένα WSN [42]. Αυτά τα μοντέλα απαιτούν πολύ μικρά σύνολα δεδομένων εκπαίδευσης, αλλά πρέπει να υπολογίζονται εκ νέου κάθε φορά που λαμβάνεται μια νέα τιμή. Όλοι αυτοί οι τύποι μοντέλων, σε διαφορετικό βαθμό, δεν είναι πολυετή και τελικά πρέπει να να επαναϋπολογιστούν για να προσαρμοστούν στις αλλαγές του συστήματος. Η επόμενη ενότητα παρέχει ορισμένες ενδείξεις σχετικά με τον τρόπο συντήρησης των μοντέλων.

Όλοι αυτοί οι τύποι μοντέλων, σε διάφορους βαθμούς, δεν είναι αιώνιοι και τελικά πρέπει να επαναϋπολογιστούν για να προσαρμοστούν στις αλλαγές του συστήματος. Η επόμενη ενότητα παρέχει ορισμένες ενδείξεις για τον τρόπο με τον οποίο μπορεί να πραγματοποιηθεί η συντήρηση των μοντέλων.

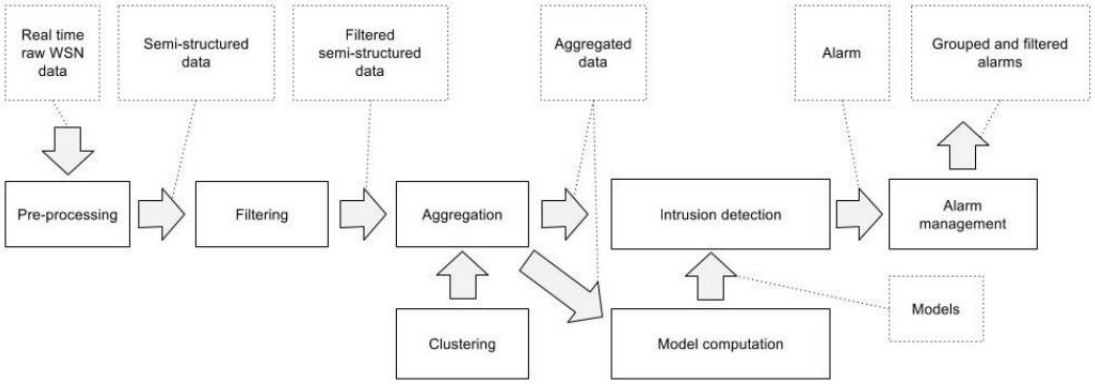
3.4 Συντήρηση μοντέλων μηχανικής μάθησης

Η δυναμική συμπεριφορά των πόλεων πρέπει να λαμβάνεται υπόψη όταν πρόκειται για την ενημέρωση των μοντέλων. Ως εκ τούτου, είναι απαραίτητος ο επαναϋπολογισμός των μοντέλων όταν αυτά παύουν να αποτυπώνουν την κανονική συμπεριφορά του συστήματος. Από τη μία πλευρά, ορισμένοι τύποι μοντέλων έχουν ήδη σχεδιαστεί για να είναι μεταβατικοί. Για παράδειγμα, τα

αυτοπαλίνδρομα μοντέλα υπολογίζονται εκ νέου μετά από κάθε νέα παρατήρηση. Από την άλλη πλευρά, άλλοι τύποι μοντέλων είναι πιο ανθεκτικοί και κατάλληλοι για λιγότερο μεταβλητά δεδομένα. Προκειμένου να γνωρίζουμε πότε αυτά τα μοντέλα καθίστανται ξεπερασμένα, είναι απαραίτητο να υπολογίζονται τακτικά ορισμένες μετρικές για την αξιολόγηση της απόδοσης κάθε μοντέλου. Κάθε σύνολο μετρικών που επιλέγεται για την αξιολόγηση μοντέλων ανίχνευσης ανωμαλιών πρέπει να λαμβάνει υπόψη τέσσερις καταστάσεις: περιπτώσεις στις οποίες δεν ανιχνεύονται επιθέσεις (ψευδώς αρνητικές), περιπτώσεις στις οποίες οι αλγόριθμοι επισημαίνουν εσφαλμένα επιθέσεις που δεν έχουν συμβεί (ψευδώς θετικές), περιπτώσεις στις οποίες οι επιθέσεις ανιχνεύονται σωστά (αληθώς θετικές) και περιπτώσεις στις οποίες εντοπίζονται σωστά ότι δεν υφίστανται επιθέσεις (αληθώς αρνητικές).

Το αληθώς θετικό ποσοστό (επίσης γνωστό ως ποσοστό ανίχνευσης, ευαισθησία ή ανάκληση) μετρά το ποσοστό των επιθέσεων που έχουν ανιχνευθεί σωστά. Το ψευδώς θετικό ποσοστό (επίσης γνωστό ως ποσοστό ψευδούς συναγερμού) δείχνει το ποσοστό των κανονικών δειγμάτων που έχουν ταξινομηθεί εσφαλμένα ως επιθέσεις. Τέλος, το f-score χρησιμοποιείται ως γενική επισκόπηση της απόδοσης του αλγορίθμου. Αυτή η μετρική λαμβάνει υπόψη τον αριθμό των αληθώς θετικών επί του αριθμητικού μέσου όρου των προβλεπόμενων θετικών και των πραγματικών θετικών. Χρησιμοποιώντας αυτές τις μετρικές, οι διαχειριστές μπορούν να καθορίσουν όρια, πέραν των οποίων τα μοντέλα πρέπει να θεωρούνται ξεπερασμένα και να υπολογίζονται εκ νέου. Για τον υπολογισμό αυτών των μετρικών και τον καθορισμό των ορίων, είναι σημαντικό να υπάρχουν επισημειωμένα σύνολα δοκιμαστικών δεδομένων. Οι προβλέψεις για κάθε δείγμα σε ένα σύνολο δοκιμαστικών δεδομένων πρέπει να συγκριθούν με τις ετικέτες που υποδεικνύουν την πραγματική κλάση του δείγματος, με αποτέλεσμα να προκύψει μία από τις τέσσερις περιπτώσεις που αναφέρθηκαν παραπάνω: ψευδώς αρνητική, ψευδώς θετική, αληθώς αρνητική ή αληθώς θετική. Ο σκοπός αυτών των ετικετών δεν πρέπει να συγχέεται με τις ετικέτες που απαιτούνται για την εκπαίδευση μοντέλων με αλγορίθμους με επίβλεψη, οι οποίοι απαιτούν πολύ μεγαλύτερα σύνολα δεδομένων. Για τον υπολογισμό αυτών των μετρικών μπορούν να

χρησιμοποιηθούν μικρότερα σύνολα δεδομένων. Ακολουθούν παραδείγματα μεθόδων που μπορούν να χρησιμοποιηθούν για την επισήμανση ενός μικρού συνόλου δεδομένων [43]:



Σχήμα 3.2: Διάγραμμα Ροής που περιγράφει τη γενική διαδικασία ανίχνευσης εισβολών από έξυπνες δεδομένα WSN της πόλης [44].

- Εκτελέστε επιθέσεις εναντίον πραγματικών WSNs έξυπνων πόλεων υπό επιτήρηση, σε δοκιμαστικά περιβάλλοντα ή σε προσομοιωτές.
- Αναπτύξτε honeypots για να δελεάσετε τους επιτιθέμενους να επιτεθούν στο σύστημα και να παρακολουθείτε τη δραστηριότητά τους.
- Χρησιμοποιήστε ένα σύστημα διαχείρισης συναγερμών στο οποίο οι διαχειριστές μπορούν να χαρακτηρίζουν τους συναγερμούς ως ψευδώς θετικούς ή πραγματικά θετικούς.

Όπως είδαμε σε αυτές τις ενότητες, η ανάλυση εισβολών περιλαμβάνει διάφορα βήματα, όπως η εκπαίδευση μοντέλων ή η πρόβλεψη ανωμαλιών σε νέες παρατηρήσεις. Στην επόμενη ενότητα παρουσιάζεται ένας αγωγός με τα απαραίτητα βήματα και τις υποδιαδικασίες που εμπλέκονται στην ανάλυση εισβολής με την προτεινόμενη αρχιτεκτονική.

3.5 Περίγραμμα ανάλυσης εισβολής

Πρώτον, όταν τα δεδομένα φτάνουν στους διακομιστές πρέπει να υποστούν προεπεξεργασία σε πραγματικό χρόνο. Στη συνέχεια, τα δεδομένα μπορούν να φιλτραριστούν και να συγκεντρωθούν. Η συνάθροιση δεδομένων μπορεί να γίνει με διάφορα κριτήρια. Ένα σύνηθες κριτήριο είναι σύμφωνα με κάποιες προηγουμένως καθορισμένες συστάδες. Τα προεπεξεργασμένα, φιλτραρισμένα και συγκεντρωμένα

δεδομένα χρησιμοποιούνται για τον υπολογισμό μοντέλων, τα οποία θα χρησιμοποιηθούν αργότερα για την ανίχνευση ανωμαλιών προκειμένου να αποκαλυφθούν επιθέσεις και άλλες αποτυχίες σε μια υποδιαδικασία ανίχνευσης εισβολών. Οι συναγερμοί που ενεργοποιούνται από την ανάλυση ανίχνευσης ανωμαλιών υποβάλλονται σε επεξεργασία από μια υποδιαδικασία διαχείρισης συναγερμών, προκειμένου να συσχετίζονται, να μειώνεται ο αριθμός των ψευδώς θετικών αποτελεσμάτων και να προειδοποιούνται οι διαχειριστές μόνο στην περίπτωση σχετικών καταστάσεων. Παρακάτω θα περιγραφεί εν συντομία κάθε μία από αυτές τις υποδιεργασίες.

3.5.1 Προεπεξεργασία

Ως πρώτο βήμα πριν από την εκτέλεση οποιουδήποτε τύπου ανάλυσης, είναι απαραίτητο να γίνει κάποιου είδους μετασχηματισμός των δεδομένων, προκειμένου να διευκολυνθούν οι μετέπειτα εργασίες [45]:

- Ανάλυση: τα μηνύματα εισέρχονται στο σύστημα με πολλαπλές μορφές (π.χ. συμβολοσειρά που περιέχει πολλές μεταβλητές χωρισμένες με #). Τα δεδομένα αυτά πρέπει να αναλυθούν και να μετασχηματιστούν τουλάχιστον σε έναν ημιδομημένο τύπο δεδομένων (π.χ. JavaScript object notation (JSON)), ο οποίος συνδέεται με κάποια μεταδεδομένα για να δώσει περιεχόμενο στα διάφορα πεδία.
- Ευρετηρίαση: τα μηνύματα εισέρχονται στο σύστημα με άτακτο τρόπο, αλλά περιέχουν ένα πεδίο με τη χρονοσφραγίδα δημιουργίας τους. Προκειμένου να διευκολυνθούν ορισμένες άλλες διαδικασίες προεπεξεργασίας που απαιτούν προηγουμένως ληφθέντα μηνύματα και επίσης να διευκολυνθούν οι επόμενες υποεπεξεργασίες, τα μηνύματα πρέπει να ευρετηριάζονται σύμφωνα με μια χρονική συνιστώσα. Τα δεδομένα WSN δεν φθάνουν με απόλυτη σειρά επειδή [45]:
- Ορισμένοι αισθητήρες αποθηκεύουν αρκετές μετρήσεις στη μνήμη, οι οποίες αποστέλλονται από κοινού μετά την παρέλευση ορισμένου χρονικού διαστήματος.
- Οι πάροχοι έχουν διάφορες εναλλακτικές λύσεις για την αποστολή δεδομένων από WSN σε κεντρικούς διακομιστές έξυπνων πόλεων (π.χ. μέσω

δημοτικών τηλεπικοινωνιακών δικτύων ή μέσω ιδιωτικής υποδομής μέσω διακομιστών που ανήκουν στους παρόχους). Οι διάφορες εναλλακτικές λύσεις δημιουργούν διαφορετικές καθυστερήσεις μεταξύ της αρχικής μετάδοσης δεδομένων και της λήψης τους στον τελικό προορισμό.

- Μέσα σε ένα ενιαίο WSN πολλαπλών βημάτων, τα πακέτα μπορούν να ακολουθήσουν διαφορετικές διαδρομές, γεγονός που οδηγεί σε διαφορετικές καθυστερήσεις.
- Τα σφάλματα μετάδοσης καθιστούν αναγκαία την επαναποστολή των πακέτων, γεγονός που αυξάνει τις καθυστερήσεις των μηνυμάτων.
- Απλή δημιουργία μεταβλητών: δημιουργούνται νέες μεταβλητές με την εφαρμογή απλών συναρτήσεων για τη συγκέντρωση ή το μετασχηματισμό ενός ή περισσότερων πεδίων από το τρέχον μήνυμα (π.χ. μετατροπή μονάδας).
- Δημιουργία σύνθετων μεταβλητών: δημιουργούνται νέες μεταβλητές που εφαρμόζουν σύνθετες συναρτήσεις για τη συγκέντρωση ή το μετασχηματισμό ενός ή περισσότερων πεδίων από το τρέχον μήνυμα ή από προηγούμενο μήνυμα (π.χ. υπολογισμός της μπαταρίας που καταναλώθηκε από το τελευταίο μήνυμα που ελήφθη).

Τα ακατέργαστα δεδομένα WSN πρέπει να μετασχηματιστούν και να ευρετηριαστούν προκειμένου να διευκολυνθούν τα επόμενα βήματα.Οι πράξεις μετασχηματισμού για αυτή την υποδιαδικασία έχουν γενικά πολύ χαμηλή υπολογιστική πολυπλοκότητα, δηλαδή O(1), καθώς πολλές από αυτές είναι απλές πράξεις που εφαρμόζονται σε ένα μόνο δείγμα (π.χ. μετατροπές μονάδων). Άλλες πράξεις απαιτούν επίσης δεδομένα που έχουν ληφθεί προηγουμένως. Ωστόσο, γενικά, μόνο το αμέσως προηγούμενο δείγμα είναι απαραίτητο (π.χ. η κατανάλωση της μπαταρίας μπορεί να υπολογιστεί αφαιρώντας την προηγούμενη στάθμη της μπαταρίας από την τρέχουσα στάθμη). Αυτό μπορεί επίσης να υπολογιστεί σε O(1). Θεωρούμε αυτή την υποδιαδικασία ως μη κρίσιμη. Υποθέτουμε ότι, εάν το σύστημα είναι ικανό να συλλέγει και να ευρετηριάζει μεγάλες ποσότητες δεδομένων, τότε είναι επίσης ικανό να προ-επεξεργάζεται τους.

3.5.2 Φιλτράρισμα

Σε αυτή την υποδιαδικασία, τα δεδομένα επιλέγονται με τυπικές λειτουργίες φιλτραρίσματος, όπως η σύγκριση μεταβλητών με τιμές που ορίζει ο χρήστης ή με άλλες μεταβλητές. Με αυτόν τον τρόπο, οι διαχειριστές μπορούν να εξάγουν μόνο τα σημαντικά δείγματα από την πληθώρα των δεδομένων που φτάνουν στο σύστημα. Για παράδειγμα, οι διαχειριστές μπορούν να ορίσουν φίλτρα για να λαμβάνουν δεδομένα μόνο από ορισμένους αισθητήρες, από μια συγκεκριμένη περιοχή κ.λπ [46].

Σε αυτή την υποδιαδικασία, τα προεπεξεργασμένα δεδομένα φιλτράρονται χρησιμοποιώντας πράξεις σύγκρισης με άλλες μεταβλητές ή σταθερές (π.χ. μεταβλητή > τιμή), οι οποίες έχουν υπολογιστικό κόστος O(1). Επιπλέον, πιο σύνθετες λειτουργίες φίλτρου, όπως μια διχοτομική αναζήτηση όπου μια μεταβλητή συγκρίνεται με πολλαπλές άλλες διατεταγμένες τιμές, έχουν κόστος O(log(n)). Θεωρούμε ότι δεν πρόκειται για κρίσιμη υποδιαδικασία. Όπως και στην προηγούμενη περίπτωση, εάν το σύστημα είναι ικανό να συγκεντρώνει και να ευρετηριάζει μεγάλες ποσότητες δεδομένων, τότε είναι επίσης ικανό να τα φιλτράρει.

3.5.3 Συσταδοποίηση (Clustering)

Ο κύριος σκοπός αυτής της υποδιαδικασίας είναι να δημιουργηθούν ορισμένες διαιρέσεις στα δεδομένα, ώστε να εξαχθούν χρήσιμα συμπεράσματα μετά την ανάλυση ανωμαλιών. Οι διαιρέσεις μπορούν να δημιουργηθούν ad-hoc από τους διαχειριστές του συστήματος ή με τη χρήση αλγορίθμων ομαδοποίησης. Ο σκοπός αυτής της υποδιαδικασίας είναι διττός. Πρώτον, με τη χρήση συστάδων, οι κόμβοι που μπορεί να επηρεαστούν από τις ίδιες επιθέσεις μπορούν να ομαδοποιηθούν και να αναλυθούν μαζί (π.χ. γειτονικοί κόμβοι που εκπέμπουν στην ίδια ζώνη συχνοτήτων). Δεύτερον, μειώνεται ο χώρος αναζήτησης, γεγονός που απλοποιεί την εύρεση της αιτίας των περιστατικών ασφαλείας.

Όσον αφορά το υπολογιστικό κόστος, η ομαδοποίηση περιλαμβάνει αλγορίθμους που μπορεί να είναι υπολογιστικά εντατικοί. Παρόλα αυτά, αφού πραγματοποιηθεί η συσταδοποίηση, οι συστάδες δεν χρειάζεται να υπολογίζονται

συχνά εκ νέου. Βασικά, οι συστάδες δεν ισχύουν πλέον τη στιγμή που οι μεταβλητές για τις οποίες έχουν ομαδοποιηθεί τα δεδομένα αλλάζουν ή όταν οι κόμβοι εντάσσονται ή απομακρύνονται από το δίκτυο. Αυτό δεν συμβαίνει πολύ συχνά, επειδή οι μεταβλητές αυτές τείνουν να είναι σταθερές (π.χ. ζώνη συχνοτήτων, τοποθεσία) [47].

3.5.4 Συγκέντρωση

Αυτή η υποδιαδικασία είναι υπεύθυνη για το συνδυασμό των δεδομένων που εξάγονται από την υποδιαδικασία φιλτραρίσματος, κατά τρόπο ώστε τα δεδομένα να παραμένουν ομαδοποιημένα σύμφωνα με ένα συγκεκριμένο κριτήριο, όπως χρονικά διαστήματα, ομάδες κ.λπ. Τυπικές πράξεις ομαδοποίησης δεδομένων είναι: το ελάχιστο, το μέγιστο, το άθροισμα, ο μέσος όρος, η διάμεσος, ο τρόπος, κ.λπ. Για παράδειγμα, συνοπτικές πληροφορίες από ένα περιβαλλοντικό WSN μπορούν να λαμβάνονται περιοδικά με τον υπολογισμό του ελάχιστου, του μέγιστου και του μέσου όρου των ενδείξεων των αισθητήρων [48].

Οι λειτουργίες συνάθροισης δεδομένων έχουν υπολογιστικό κόστος που εξαρτάται από τον αριθμό των δειγμάτων προς συνάθροιση. Για παράδειγμα, η συνάθροιση των τελευταίων n δειγμάτων σε μια ενιαία μεταβλητή με μια λειτουργία όπως η mode έχει μέγιστο υπολογιστικό κόστος O(nlog(n)). Άλλες πράξεις συνάθροισης έχουν χαμηλότερο υπολογιστικό κόστος (π.χ. το ελάχιστο, το μέγιστο, το άθροισμα, ο μέσος όρος και η διάμεσος μπορούν να υπολογιστούν σε χρόνο O(n)). Οι πιο σύνθετες πράξεις συνάθροισης απαιτούν ταξινόμηση του καταλόγου των δειγμάτων, η οποία είναι η υπο-λειτουργία με το υψηλότερο κόστος. Ωστόσο, δεδομένου ότι αυτή η υπο-λειτουργία μπορεί, τουλάχιστον εν μέρει, να επαναχρησιμοποιηθεί μεταξύ επόμενων λειτουργιών συνάθροισης στην ίδια πηγή δεδομένων, η συνολική υπολογιστική πολυπλοκότητα αυτών των λειτουργιών συνάθροισης μπορεί να μειωθεί σημαντικά. Επιπλέον, το n δεν είναι γενικά μεγάλο για πράξεις συνάθροισης που έχουν χρονικούς περιορισμούς. Σε αυτές τις περιπτώσεις, υψηλότεροι χρονικοί περιορισμοί συνεπάγονται μικρότερα διαστήματα και, επομένως, συνεπάγονται επίσης τη συμπερίληψη λιγότερων δειγμάτων στο χρονικό διάστημα. Ως εκ τούτου, θεωρούμε ότι αυτή η

υποδιαδικασία δεν είναι κρίσιμη και μπορεί να γίνει από οποιοδήποτε μεγάλο δεδομένο σύστημα [49].

3.5.5 Υπολογισμός μοντέλου

Όπως είδαμε προηγουμένως, η ανίχνευση ανωμαλιών βασίζεται στη χρήση προηγουμένως υπολογισμένων μοντέλων για να προβλέψει αν μια παρατήρηση είναι φυσιολογική ή όχι. Αυτά τα μοντέλα μπορεί να είναι πολύ απλά, όπως τα κατώτατα όρια, ή πολύπλοκα, όπως τα μοντέλα μηχανικής μάθησης. Και στις δύο περιπτώσεις, το κόστος υπολογισμού των μοντέλων δεν είναι συνήθως αμελητέο. Ως εκ τούτου, τα μοντέλα πρέπει να έχουν ήδη υπολογιστεί πριν από τη χρήση τους σε εφαρμογές πραγματικού χρόνου [50].

Στην περίπτωση των μονομεταβλητών μοντέλων, η πολυπλοκότητα οφείλεται στο γεγονός ότι πρέπει να υπολογιστεί διαφορετικό μοντέλο για κάθε μεταβλητή που απαιτεί παρακολούθηση. Κατ' αυτόν τον τρόπο, αν και οι μονομεταβλητές τεχνικές έχουν χαμηλή υπολογιστική πολυπλοκότητα (π.χ. η μέθοδος Tukey μπορεί να υπολογιστεί σε O(nlog(n)) ή και λιγότερο αν ο κατάλογος των δειγμάτων είναι ήδη ταξινομημένος), τα μοντέλα πρέπει να υπολογιστούν για κάθε μία από τις m απαραίτητες μεταβλητές του συνόλου δεδομένων και, επομένως, είναι βολικό να παραλληλιστεί ο υπολογισμός.

3.5.6 Ανίχνευση εισβολής

Η ανίχνευση εισβολής πραγματοποιείται σε προεπεξεργασμένα, φιλτραρισμένα, ομαδοποιημένα ή/και συγκεντρωτικά δεδομένα χρησιμοποιώντας είτε τη μηχανή ανίχνευσης βάσει κανόνων είτε τη μηχανή ανίχνευσης βάσει ανωμαλιών. Όπως είδαμε προηγουμένως, η πρώτη χρησιμοποιεί υπογραφές επιθέσεων για να αναζητήσει ίχνη επιθέσεων, ενώ η δεύτερη χρησιμοποιεί τα μοντέλα που έχουν υπολογιστεί εκ των προτέρων για να προβλέψει αν πρέπει να γίνουν νέες θεωρούνται μη φυσιολογικά.

Τα βήματα για το διαχωρισμό των αρχικών δεδομένων μέχρι την εκπαίδευση του μοντέλου (δηλαδή ο διαχωρισμός, η αντιστοίχιση και το ανακάτεμα) είναι ισοδύναμα. Στη συνέχεια, φορτώνεται ένα μοντέλο που έχει αποθηκευτεί στην προηγούμενη υποδιαδικασία και χρησιμοποιείται για να ελεγχθεί εάν τα δεδομένα

εισόδου στην υποδιαδικασία ανίχνευσης εισβολών περιέχουν ανωμαλίες. Ως εκ τούτου, λαμβάνοντας υπόψη αυτές τις διαφορές, το σχήμα του αλγορίθμου που παρουσιάστηκε στην προηγούμενη ενότητα ισχύει και για αυτή την υποδιαδικασία. Επιπλέον, οι ενέργειες που εμπλέκονται σε αυτή την υποδιαδικασία είναι υπολογιστικά λιγότερο δαπανηρές από ό,τι για την υποδιαδικασία εκπαίδευσης. Η φόρτωση ενός μοντέλου από μια δομή τιμών-κλειδιών (π.χ. έναν πίνακα κατακερματισμού) μπορεί να γίνει σε O(1) κατά μέσο όρο. Ο έλεγχος αν μια τιμή εμπίπτει σε δύο κατώτατα όρια μπορεί επίσης να γίνει σε O(1) [51]. Για πιο σύνθετα πολυμεταβλητά μοντέλα, η υπολογιστική πολυπλοκότητα ποικίλλει ανάλογα με τον συγκεκριμένο αλγόριθμο. Το υπολογιστικό κόστος της δοκιμής με μη γραμμικά SVM με χαμηλό αριθμό διαστάσεων αυξάνεται γραμμικά με τον αριθμό των διανυσμάτων υποστήριξης του μοντέλου. Ο αριθμός αυτός περιορίζεται από το μέγεθος του συνόλου εκπαίδευσης επί το ποσοστό σφάλματος του συνόλου εκπαίδευσης. Αυτό είναι σαφώς χαμηλότερο από την υπολογιστική πολυπλοκότητα της εκπαίδευσης του μοντέλου.

3.5.7 Διαχείριση συναγερμών

Οι προβλέψεις εισβολής που αναφέρθηκαν στο προηγούμενο βήμα χρησιμοποιούνται από μια υποδιαδικασία διαχείρισης συναγερμών για τη δημιουργία συναγερμών και την προειδοποίηση των διαχειριστών. Αυτή η υποδιαδικασία μπορεί να χρησιμοποιήσει μεταβλητές όπως η κρισιμότητα του WSN ή ο βαθμός ανωμαλίας που εξάγεται από ορισμένους αλγορίθμους ανίχνευσης ανωμαλιών για να ταξινομήσει τους συναγερμούς ανάλογα με τη σημασία τους. Επιπλέον, οι διαχειριστές μπορούν να συσχετίσουν τους συναγερμούς με τη μηχανή ανίχνευσης βάσει κανόνων προκειμένου να συγκεντρώσουν διάφορους συναγερμούς σε έναν ενιαίο και πιο σχετικό συναγερμό, να αναζητήσουν βλάβες σε διάφορα δίκτυα σε ταυτόχρονα, κ.λπ [52].

Με την προτεινόμενη αρχιτεκτονική, οι μηχανές ανίχνευσης δημιουργούν συναγερμούς. Οι κύριες αρμοδιότητες αυτής της υποδιαδικασίας είναι ο συνδυασμός και η συσχέτιση αυτών των συναγερμών σε νέους και πιο αξιόπιστους συναγερμούς, οι οποίοι τελικά προειδοποιούν τους διαχειριστές του συστήματος. Παρόλο που ο όγκος των συναγερμών που παράγονται από τις μηχανές ανίχνευσης

μπορεί να είναι πολύ μεγάλος για να τον χειριστεί ένας άνθρωπος, δεν είναι πολύ μεγάλος για να τον χειριστεί μια μηχανή που χρησιμοποιεί συμβατικές τεχνικές επεξεργασίας. Ως εκ τούτου, αυτή η υποδιαδικασία δεν θεωρείται κρίσιμη όσον αφορά τις απαιτήσεις επεξεργασίας [53].

3.6 Συμπεράσματα

Σε αυτό το κεφάλαιο, προτείναμε μια αρχιτεκτονική, η οποία παρέχει εργαλεία για να διευκολυνθεί το πολύπλοκο πρόβλημα της αποκάλυψης εισβολών σε ένα μεγάλο και ετερογενές περιβάλλον, όπως η έξυπνη πόλη. Είδαμε ότι η παραδοσιακή ασφάλεια πρέπει να ενισχυθεί προκειμένου να εντοπιστούν ανωμαλίες σε WSN έξυπνων πόλεων που λειτουργούν από τρίτους. Η μειωμένη πρόσβαση στις συσκευές του δικτύου των παρόχων υπηρεσιών περιορίζει την ορατότητα των WSNs στους διαχειριστές της έξυπνης πόλης και εμποδίζει τη συμβατική ανάλυση ασφάλειας. Για να το ξεπεράσουμε αυτό, προτείναμε μια μη παρεμβατική αρχιτεκτονική που συνδυάζει μια μηχανή ανίχνευσης βασισμένη σε κανόνες και μια μηχανή ανίχνευσης με βάση τις ανωμαλίες. Αυτή η αρχιτεκτονική αναπτύσσει ένα νέο επίπεδο ασφάλειας στους κεντρικούς διακομιστές πάνω από τον διάφορο εξοπλισμό των παρόχων. Έτσι, αποφεύγονται τα προβλήματα που οφείλονται στην ετερογένεια, την περιορισμένη πρόσβαση ή τις δυσκολίες ενημέρωσης ορισμένων συσκευών. Η προτεινόμενη αρχιτεκτονική είναι συμβατή με την ήδη αναπτυγμένη υποδομή, καθώς δεν προσθέτει απαιτήσεις στην υπάρχουσα υποδομή. Επιπλέον, περιγράψαμε έναν αγωγό με τις απαραίτητες υποδιεργασίες για την επεξεργασία δεδομένων WSN και την αποκάλυψη εισβολών χρησιμοποιώντας την προτεινόμενη αρχιτεκτονική με συμβατικές τεχνικές ανίχνευσης ανωμαλιών.

Είδαμε ότι η ανίχνευση εισβολών στην έξυπνη πόλη είναι ένα πολύ σύνθετο πρόβλημα. Μια λύση "μαύρου κουτιού" με έναν αλγόριθμο ανίχνευσης πολλαπλών χρήσεων που καλύπτει τις περισσότερες επιθέσεις για τις περισσότερες διαμορφώσεις δεν είναι εφικτή. Για να αντιμετωπιστεί η ανίχνευση εισβολών σε αυτό το πλαίσιο, πρέπει πρώτα να επιλεγούν οι καταλληλότεροι αλγόριθμοι. Σε αυτό το κεφάλαιο, υποδείξαμε ορισμένους κατάλληλους αλγορίθμους για την υλοποίηση της ανάλυσης ανωμαλιών στην πλαίσιο της έξυπνης πόλης.

4 ΑΝΘΕΚΤΙΚΟΤΗΤΑ (RESILIENCY) ΣΕ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Οι έξυπνες πόλεις πρέπει επίσης να είναι ανθεκτικές. Η έννοια της ανθεκτικότητας (resiliency) εισήχθη αρχικά από έναν γνωστό οικολόγο, τον CS. Holling, ο οποίος το 1973 πρότεινε δύο γενικές προσεγγίσεις, δηλαδή, πρώτον, ο άνθρωπος και η φύση είναι στενά συνδεδεμένοι και εξελίσσονται από κοινού και πρέπει συνεπώς να εκλαμβάνονται ως ένα ενιαίο σύστημα κοινωνικής οικολογίας- δεύτερον, οι αντιδράσεις αυτού του συστήματος απέναντι στις αλλαγές είναι απρόβλεπτες, αλλά όχι αποδεδειγμένες [54]. Μετά από αυτό, η εστίαση είναι στην ανθεκτικότητα, στη συνέχεια η κοινωνική μελέτη και εισήλθε στον τομέα του σχεδιασμού. Η κατανόηση της έννοιας του σχεδιασμού έξυπνων πόλεων με την ενσωμάτωση στοιχείων ανθεκτικότητας μπορεί να επανερμηνευτεί για να βρεθεί ένας νέος ορισμός. Στο πλαίσιο του αστικού σχεδιασμού, ιδίως για τις έννοιες της έξυπνης πόλης, η ανθεκτική πόλη διαδραματίζει σημαντικό ρόλο. Μια πόλη είναι ένα πολύπλοκο σύστημα και πρέπει να αναπτυχθεί η ανθεκτική ικανότητά της- η ικανότητα πολλαπλών συνιστωσών, η οποία είναι η διαδικασία και η αλληλεπίδραση που την ανεβάζει πάνω από τα φυσικά όρια της πόλης. Όταν μια πόλη θεωρείται έξυπνη είναι σημαντικό να είναι ανθεκτική ανά πάσα στιγμή. Ως εκ τούτου, η έννοια της ανθεκτικότητας είναι ένας από τους βασικούς παράγοντες στον σχεδιασμό έξυπνων πόλεων. Καθώς η έννοια της ανθεκτικότητας εμβαθύνει, είναι σαφές ότι μας επιτρέπει να κάνουμε το πρώτο βήμα για την προσαρμογή σε φαινόμενα που μπορεί να οδηγήσουν σε μετασχηματισμό του αστικού οικοσυστήματος.

Η πτυχή της έξυπνης ανάπτυξης μιας πόλης έχει αναδειχθεί ως στρατηγική για τον μετριασμό των προβλημάτων που προκαλούνται από την αύξηση του αστικού πληθυσμού και την ταχεία αστικοποίηση. Η συνολική έννοια της έξυπνης πόλης έχει κερδίσει όλο και μεγαλύτερη προσοχή από τον ακαδημαϊκό κόσμο, τους επαγγελματίες και τους υπεύθυνους λήψης αποφάσεων. Η έννοια χρησιμοποιείται σε όλο τον κόσμο με διαφορετικές ονοματολογίες, πλαίσιο και έννοιες. Μια έξυπνη πόλη ορίζεται επίσης ως μια πόλη που παρακολουθεί και ενσωματώνει τις συνθήκες όλων των κρίσιμων υποδομών της, σχεδιάζει τις δραστηριότητες

προληπτικής συντήρησης και παρακολουθεί τις πτυχές της ασφάλειας, μεγιστοποιώντας παράλληλα τις υπηρεσίες προς τους πολίτες της.

Από την άλλη πλευρά, η θεωρία της ανθεκτικότητας έχει διεπιστημονικές ρίζες στους κλάδους της μηχανικής, της βιολογίας και της οικολογίας, και γίνεται γενικά κατανοητή ως ένας τρόπος κατανόησης του τρόπου με τον οποίο τα συστήματα αντιδρούν σε ακραίες πιέσεις, είτε παρακμάζουν και πεθαίνουν, είτε προσαρμόζονται και ευδοκιμούν. Η ανθεκτικότητα είναι ένας σχετικά νέος όρος που χρησιμοποιείται στις συζητήσεις για τον αστικό σχεδιασμό, την ακαδημαϊκή έρευνα και την πρακτική, γεγονός που οφείλεται κυρίως στην αυξανόμενη προσοχή που δίνεται στα ακραία και καταστροφικά γεγονότα και τις συνέπειές τους, όπως η κλιματική αλλαγή, οι τυφώνες, οι τρομοκρατικές επιθέσεις, οι σεισμοί, οι πυρκαγιές, οι πετρελαιοκηλίδες, το έγκλημα στον κυβερνοχώρο, οι επιδημίες καθώς και οι οικονομικές κρίσεις. Οι περισσότεροι κοινώς χρησιμοποιούμενοι ορισμοί της ανθεκτικής πόλης έχουν λάβει υπόψη τους διαφορετικές επιστημονικές προοπτικές, λαμβάνοντας υπόψη κοινωνικούς, οικονομικούς και περιβαλλοντικούς παράγοντες, κάτι ανάλογο ισχύει και για τον ορισμό της έξυπνης πόλης. Οι ορισμοί αυτοί λαμβάνουν επίσης υπόψη τις μεταξύ τους σχέσεις ως κλειδί για την αποτελεσματική κατανόηση της πολυπλοκότητας των αστικών συστημάτων και της συμπεριφοράς τους απέναντι σε ετερογενείς πιέσεις.

Μια ανθεκτική έξυπνη πόλη προωθεί ένα όραμα της έξυπνης πόλης στο οποίο οι προσπάθειες απευθύνονται στην αύξηση της ικανότητας της πόλης να ανταποκρίνεται σε ετερογενείς παράγοντες πίεσης, όπως οι κλιματικοί, περιβαλλοντικοί, ενεργειακοί και οικονομικοί, με απώτερο στόχο την εξασφάλιση υψηλότερης ποιότητας ζωής και βιώσιμης αστικής ανάπτυξης. Από την άλλη πλευρά, οι έξυπνες πόλεις έχουν τις ρίζες τους στην εξέλιξη και την εξάπλωση των ΤΠΕ και στα αποτελέσματά τους όσον αφορά την παγκοσμιοποίηση της οικονομίας και των αγορών. Παρά τις διαφορές των όρων, υπάρχει μια συνέργεια σε αυτούς τους δύο όρους. Η έννοια της ανθεκτικότητας στις "έξυπνες πόλεις" υπογραμμίζει ότι οι έξυπνες πρωτοβουλίες θα πρέπει να επιτρέπουν στις πόλεις να γίνονται πιο βιώσιμες και ανθεκτικές και, ως εκ τούτου, να είναι σε θέση να ανταποκρίνονται ταχύτερα στις νέες προκλήσεις. Για να κατανοήσουμε τη σύνδεση και τις

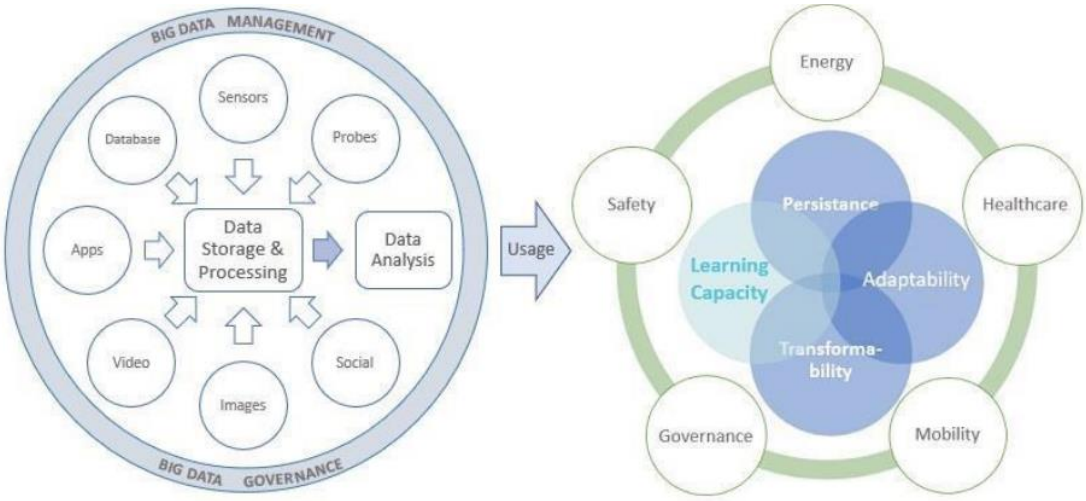
αλληλεπιδράσεις μεταξύ των δύο εννοιών, είναι σημαντικό να κατανοήσουμε τις κοινές έννοιες μεταξύ της έξυπνης πόλης και της ανθεκτικότητας.

Μια ανθεκτική έξυπνη πόλη προωθεί ένα όραμα της έξυπνης πόλης στο οποίο οι προσπάθειες απευθύνονται στην αύξηση της ικανότητας της πόλης να ανταποκρίνεται σε ετερογενείς παράγοντες πίεσης, όπως οι κλιματικοί, περιβαλλοντικοί, ενεργειακοί και οικονομικοί, με απώτερο στόχο την εξασφάλιση υψηλότερης ποιότητας ζωής και βιώσιμης αστικής ανάπτυξης. Από την άλλη πλευρά, οι έξυπνες πόλεις έχουν τις ρίζες τους στην εξέλιξη και την εξάπλωση των ΤΠΕ και στα αποτελέσματά τους όσον αφορά την παγκοσμιοποίηση της οικονομίας και των αγορών. Παρά τις διαφορές των όρων, υπάρχει μια συνέργεια σε αυτούς τους δύο όρους. Η έννοια της ανθεκτικότητας στις "έξυπνες πόλεις" υπογραμμίζει ότι οι έξυπνες πρωτοβουλίες θα πρέπει να επιτρέπουν στις πόλεις να γίνονται πιο βιώσιμες και ανθεκτικές και, ως εκ τούτου, να είναι σε θέση να ανταποκρίνονται ταχύτερα στις νέες προκλήσεις. Για να κατανοήσουμε τη σύνδεση και τις αλληλεπιδράσεις μεταξύ των δύο εννοιών, είναι σημαντικό να κατανοήσουμε τις κοινές έννοιες μεταξύ της έξυπνης πόλης και της ανθεκτικότητας. Η ανθεκτικότητα της έξυπνης πόλης, που αποτελεί ένα ευρύτερο γνωστικό πεδίο, μπορεί να εφαρμοστεί σε διάφορα στοιχεία μιας έξυπνης πόλης. Αυτό μπορεί να είναι από την παροχή κατανόησης της πολυπλοκότητας των πόλεων και των παραγόντων που συμβάλλουν στην ανθεκτικότητά τους έως τον εντοπισμό κρίσιμων τομέων αδυναμίας και τον προσδιορισμό δράσεων και προγραμμάτων για τη βελτίωση της ανθεκτικότητας της πόλης [55].

4.1 Ανάλυση μεγάλων δεδομένων στο πλαίσιο της ανθεκτικότητας των έξυπνων πόλεων

Προκειμένου να έχουμε εικόνα των σημαντικών παραγόντων που περιβάλλουν την υιοθέτηση της ανάλυσης μεγάλων δεδομένων στην ανθεκτικότητα των έξυπνων πόλεων, η παρούσα ενότητα διερευνά τον τρόπο με τον οποίο χρησιμοποιείται αυτή η τεχνολογία στο πλαίσιο. Καθώς οι υπηρεσίες της πόλης εξαρτώνται όλο και περισσότερο από τις ροές δεδομένων της έξυπνης πόλης, οι υπηρεσίες γίνονται επίσης πιο ευάλωτες σε διαταραχές. Για τον λόγο αυτό, οι υπηρεσίες έξυπνης πόλης απαιτούν ένα επίπεδο ανθεκτικότητας στις διαταραχές.

Οι ΤΠΕ, οι οποίες έχουν αυξήσει την αστική εξυπνάδα, διαδραματίζουν σημαντικό ρόλο στη μείωση της ευπάθειας και στη βελτίωση της ανθεκτικότητας των έξυπνων πόλεων. Μέσω των αναπτυγμένων τεχνολογιών έξυπνων πόλεων, μπορεί να συλλεχθεί, να επεξεργαστεί, να ενσωματωθεί και να αναλυθεί μεγάλος όγκος και ποικιλία δεδομένων που σχετίζονται με την κατάσταση και την απόδοση των συστημάτων υποδομής, καθώς και με τις συμπεριφορές των πολιτών, μέσω πλατφορμών ανάλυσης μεγάλων δεδομένων. Τα δεδομένα αυτά μπορούν να παραχθούν από διάφορες πηγές, όπως βάσεις δεδομένων, αισθητήρες, μέσα κοινωνικής δικτύωσης, εξωτερικές εφαρμογές, βίντεο και εικόνες. Τα δεδομένα αυτά απαιτείται να αναλυθούν και να βελτιωθούν με τη χρήση μοντέλων για την πρόβλεψη μελλοντικών αποτελεσμάτων με υψηλή αξιοπιστία και την εξαγωγή αξιοποιήσιμων πληροφοριών για τη λήψη ακριβών αποφάσεων. Αυτές οι γνώσεις θεωρείται ότι συμβάλλουν στη μείωση των προβλέψιμων κινδύνων σε διάφορους τομείς μιας έξυπνης πόλης, όπως η κοινωνική κινητικότητα και η κλιματική αλλαγή, και έτσι επιτρέπουν τον αποτελεσματικό σχεδιασμό προκειμένου να καταστούν οι έξυπνες πόλεις ανθεκτικές [56].



Σχήμα 4.1: Απλοποιημένη απεικόνιση της ερμηνείας της ανάλυσης των μεγάλων δεδομένων στην ανθεκτικότητα των έξυπνων πόλεων σε αυτό το έγγραφο[56]

4.2 Περιπτώσεις χρήσης της ανάλυσης μεγάλων δεδομένων στην ανθεκτικότητα των έξυπνων πόλεων

Στην παρούσα ενότητα παρατίθενται παραδείγματα για το πώς χρησιμοποιείται η ανάλυση μεγάλων δεδομένων για την επίτευξη της ανθεκτικότητας των έξυπνων πόλεων. Οι υποκείμενες περιπτώσεις βασίζονται σε στοιχεία των έξυπνων ανθεκτικών πόλεων.

4.2.1 Ανάλυση μεγάλων δεδομένων στην υγειονομική περίθαλψη και την ασφάλεια

Οι δυνατότητες των αναλύσεων μεγάλων δεδομένων να συμβάλλουν στην υγειονομική περίθαλψη και την ασφάλεια για μια εξωτερική διαταραχή, όπως μια φυσική καταστροφή, αποδεικνύονται σε ορισμένες πόλεις. Για παράδειγμα, το 2012, ο τυφώνας Sandy έπληξε την ανατολική ακτή των Ηνωμένων Πολιτειών. Η πρόβλεψη της τροχιάς ενός τυφώνα δεν είναι πάντα ακριβής, ωστόσο, η χρήση ιστορικών δεδομένων, μετεωρολογικών συνθηκών και κατάλληλων υπολογιστικών μοντέλων, επέτρεψε στους μετεωρολόγους να προβλέψουν την τροχιά του τυφώνα Sandy με μεγαλύτερη ακρίβεια. Με τη βοήθεια των τεχνολογιών μεγάλων δεδομένων, το εθνικό κέντρο τυφώνων των ΗΠΑ μπόρεσε να προβλέψει την προσγείωση του τυφώνα Sandy 5 ημέρες νωρίτερα και με ακρίβεια 30 μιλίων, προκειμένου να διασφαλίσει την ασφάλεια των πολιτών. Αντίστοιχα, ο μη κερδοσκοπικός οργανισμός, δηλαδή η Direct Relief, χρησιμοποίησε αναλύσεις μεγάλων δεδομένων για να σχεδιάσει και να διαχειριστεί καταστάσεις έκτακτης ανάγκης σχεδόν σε πραγματικό χρόνο, όπως για να εντοπίσει ευάλωτες περιοχές, να αποθηκεύσει και να διανείμει συνταγογραφούμενα φάρμακα στον πληγέντα πληθυσμό σε περίοδο κρίσης [57].

4.2.2 Ανάλυση μεγάλων δεδομένων στην ενέργεια και τη διακυβέρνηση

Έχουν αναλυθεί διάφορες πρωτοβουλίες σχετικά με την ενέργεια και τη διακυβέρνηση για έξυπνες πόλεις από πόλεις σε όλο τον κόσμο. Παράδειγμα αποτελεί η δέσμευση που ανέλαβε το Δημοτικό Συμβούλιο της Κοπεγχάγης, το οποίο το 2012 αποφάσισε να υιοθετήσει το σχέδιο για το κλίμα "Κοπεγχάγη 2025", ώστε να γίνει η πρώτη πρωτεύουσα του κόσμου με ουδέτερο ισοζύγιο άνθρακα έως το 2025. Σύμφωνα με την πόλη της Κοπεγχάγης, η εφαρμογή των μεγάλων

δεδομένων και της ανάλυσης είναι ζωτικής σημασίας, ώστε να είναι σε θέση να λαμβάνουν αποφάσεις σε πραγματικό χρόνο και να προβλέπουν πιθανά σενάρια. Η Κοπεγχάγη σχεδιάζει να χρησιμοποιήσει τα δεδομένα που συλλέγονται όχι μόνο ως εργαλείο για τη μείωση της ενέργειας, αλλά να τα χρησιμοποιήσει για να συμβάλει ανάλογα στη χάραξη πολιτικής. Παρόμοια με την Κοπεγχάγη, το Μάλμε στοχεύει να συνδυάσει διάφορες πηγές δεδομένων προκειμένου να αναπτύξει στοχευμένες πολιτικές εντός της πόλης, ώστε να μπορεί να αντιδράσει ανάλογα απέναντι σε διάφορες καταστάσεις. Παρομοίως, το Ελσίνκι μέσω ενός φορέα, του Helsinki Region Infoshare Project, συγκεντρώνει σύνολα δεδομένων από την επόμενη μητροπολιτική περιοχή του και θέτει τα δεδομένα ανοιχτά, ώστε οι προγραμματιστές λογισμικού, οι ερευνητές και οι δημοσιογράφοι να μπορούν να χρησιμοποιούν τα δεδομένα για ανάλυση. Η ανάλυση αυτών των πηγών δεδομένων επέτρεψε τη διαθεσιμότητα πληροφοριών όπως η θέση των εκχιονιστικών μηχανημάτων σε πραγματικό χρόνο, ο χάρτης των επιπέδων κυκλοφοριακού θορύβου και άλλα, για να αναφέρουμε μερικά από αυτά [58].

4.2.3 Ανάλυση μεγάλων δεδομένων στην κινητικότητα

Η κινητικότητα και η στέγαση είναι στοιχεία που σχετίζονται καλά με τα μεγάλα δεδομένα και τις αναλύσεις. Ένα σαφές παράδειγμα μπορεί να βρεθεί στην πόλη του Λος Άντζελες, η οποία χρησιμοποιεί αυτοματοποιημένο σύστημα παρακολούθησης και ελέγχου της κυκλοφορίας. Το σύστημα είναι προετοιμασμένο να αντιμετωπίζει διάφορα είδη ζητημάτων, όπως ατυχήματα ή τη διατήρηση των δημόσιων συγκοινωνιών στην ώρα τους, προσαρμόζοντας την καθυστέρηση μεταξύ των αλλαγών των φωτεινών σηματοδοτών, όταν αυτό είναι απαραίτητο. Ένα άλλο παράδειγμα είναι αυτό που κάνει η Κοπεγχάγη εφαρμόζοντας αισθητήρες για τη συλλογή δεδομένων από τις θέσεις στάθμευσης, τη ροή της κυκλοφορίας, τους κάδους απορριμμάτων και τη διανομή νερού για τη λήψη αποφάσεων σε πραγματικό χρόνο. Αυτές οι πρωτοβουλίες της πόλης επικεντρώνονται στην ενσωμάτωση των μεταφορών και στη χρήση των ΤΠΕ για να έχουμε καλύτερη γνώση της πόλης στο σύνολό της και να λαμβάνουν πιο τεκμηριωμένες αποφάσεις [59].

4.3 Βασικοί παράγοντες και εμπόδια για την υιοθέτηση της ανάλυσης μεγάλων δεδομένων για την επίτευξη ανθεκτικότητας των έξυπνων πόλεων

Η προσαρμογή της ανάλυσης μεγάλων δεδομένων στην ανθεκτικότητα των έξυπνων πόλεων εξετάζεται με τρόπο που να επιτρέπει στους ενδιαφερόμενους φορείς να παράγουν πιθανές στρατηγικές. Στην παρούσα ενότητα γίνεται ανασκόπηση της βιβλιογραφίας που εξετάζει τις δυνατότητες της ανάλυσης μεγάλων δεδομένων για την επίτευξη της ανθεκτικότητας των έξυπνων πόλεων. Μια πτυχή που συζητήθηκε είναι η κοινή χρήση δεδομένων. Η ανάλυση δεδομένων Big επιτρέπει την ανταλλαγή δεδομένων μέσω διαφορετικών συστημάτων υποδομής με διαλειτουργικό και συνεπή τρόπο, για τον αποτελεσματικό σχεδιασμό έξυπνων πόλεων και την ανάπτυξη κατάλληλων προγραμμάτων ανθεκτικότητας και βιωσιμότητας. Σε συνδυασμό με αυτό, η ανάλυση μεγάλων δεδομένων υποστηρίζει τη συνεργασία ιδίως στη διαχείριση της αντιμετώπισης έκτακτων αναγκών μέσω κατανεμημένου περιβάλλοντος οπτικοποίησης για γεωγραφικά διασκορπισμένους χρήστες στην αντιμετώπιση καταστροφών. Ομοίως, η ανάλυση μεγάλων δεδομένων επιτρέπει την ανταλλαγή πληροφοριών βάσει δεδομένων, όπως η ανταλλαγή κρίσιμων πληροφοριών σε καταστροφές. Η ανάλυση μεγάλων δεδομένων συζητείται για να επιτρέψει στις έξυπνες πόλεις να επεξεργάζονται πολλαπλές διαφορετικές πηγές δεδομένων που κατανέμονται μεταξύ συνδεδεμένων οντοτήτων και πηγών δεδομένων, δημιουργώντας έτσι μια βάση γνώσης για την πόλη. Οι δυνατότητες της ανάλυσης μεγάλων δεδομένων για να μπορέσουν οι έξυπνες πόλεις να αναλύσουν και να εργαστούν με δεδομένα από πολλαπλές πηγές, όπως τα δεδομένα που σχετίζονται με τις περιβαλλοντικές συνθήκες μπορούν να συγκεντρωθούν και να αναλυθούν για την κατανόηση και τη λήψη αποφάσεων. Τα δεδομένα αυτά συλλέγονται από ένα δίκτυο αισθητήρων που είναι κατανεμημένα σε όλη την έξυπνη πόλη, για παράδειγμα μέτρηση της ατμοσφαιρικής ρύπανσης, της στάθμης του νερού ή της σεισμικής δραστηριότητας. Σαφώς τα δεδομένα από πολλαπλές πηγές της έξυπνης πόλης οδηγούν σε μεγάλο όγκο δεδομένων. Η ανάλυση δεδομένων Big Data επιτρέπει στις έξυπνες πόλεις να εργάζονται με μεγάλους όγκους δεδομένων, όπως τα εργαλεία μεγάλων δεδομένων που μπορούν να αξιοποιηθούν για την επεξεργασία των μεγάλων ποσοτήτων δεδομένων που

σχετίζονται με κρίσεις, ώστε να παρέχουν μια εικόνα της ταχέως μεταβαλλόμενης κατάστασης και να βοηθήσουν στην προώθηση μια αποτελεσματικής αντιμετώπισης της καταστροφής.

Η ανάλυση μεγάλων δεδομένων διαδραματίζει ζωτικό ρόλο στη βελτίωση της διαδικασίας λήψης αποφάσεων μέσω της αξιοποίησης χαρακτηριστικών όπως διαφορετικές μέθοδοι οπτικοποίησης και άλλα περιουσιακά στοιχεία μεγάλων δεδομένων, όπως εικόνες, βίντεο, ήχος, για την αύξηση της αξιοπιστίας κατά τη διαδικασία λήψης αποφάσεων. Ομοίως, η αναλυτική μεγάλων δεδομένων επιτρέπει την επίγνωση της κατάστασης, την υποστήριξη της συνεργασίας, τη λήψη αποφάσεων και την αξιολόγηση της ίδιας της αναλυτικής διαδικασίας με τη χρήση εργαλείων όπως η γεωεικονική ανάλυση.

Από την άλλη πλευρά, η ανάλυση μεγάλων δεδομένων επιτρέπει τη δημιουργία προγνωστικών μοντέλων για τη διερεύνηση συγκεκριμένων πτυχών της ζωής της πόλης που μεταβάλλονται με την πάροδο του χρόνου, καθώς και τη δημιουργία προγνωστικών μοντέλων σε σχέση με την καθημερινή ανάπτυξη και διαχείριση της πόλης και καταστάσεις καταστροφών, όπως οι πλημμύρες. Τα μεγάλα δεδομένα αλλάζουν δραματικά τις ανθρωπιστικές επιχειρήσεις και τη διαχείριση κρίσεων μέσω της πρόβλεψης σε πραγματικό χρόνο, δίνοντας στις έξυπνες πόλεις τη δυνατότητα οπτικοποίησης, ανάλυσης και πρόβλεψης των καταστροφών. Η ανάλυση της συμπεριφοράς του κοινού κατά τη διαχείριση κρίσεων καθίσταται επίσης δυνατή μέσω της ανάλυσης. Παρά τις πολλά υποσχόμενες ευκαιρίες, η βιβλιογραφία συζητά επίσης τις προκλήσεις και τους κινδύνους που αντιμετωπίζει ο σχεδιασμός, η ανάπτυξη και η ανάπτυξη της ανάλυσης μεγάλων δεδομένων για την επίτευξη της ανθεκτικότητας των έξυπνων πόλεων. Οι προκλήσεις αυτές αποτελούν εμπόδια που επηρεάζουν τις προσπάθειες ανθεκτικότητας των έξυπνων πόλεων. Μία από τις προκλήσεις που συζητούνται στη βιβλιογραφία είναι οι ασυνέπειες του νομικού και κανονιστικού πλαισίου, αυτό επηρεάζει τους ενδιαφερόμενους φορείς, όπως οι ιδιωτικές εταιρείες που συγκεντρώνουν και αναλύουν δεδομένα της πόλης. Οι οργανισμοί εξακολουθούν να αντιμετωπίζουν δυσκολίες όσον αφορά τη δημιουργία τεχνικών και οργανωτικών

δεξιοτήτων και ικανοτήτων για την αντιμετώπιση της ανάλυσης μεγάλων δεδομένων για την αποτελεσματική εφαρμογή της [60].

Η ικανότητα αξιοποίησης των μεγάλων δεδομένων από τους πολεοδόμους για την επίτευξη συγκεκριμένων στόχων έξυπνης πόλης είναι περιορισμένη. Οι έξυπνες πόλεις έρχονται επίσης αντιμέτωπες με υψηλό κόστος όσον αφορά την ύπαρξη επαγγελματιών πληροφορικής, τη συμβουλευτική και την κατάρτιση και το υπολογιστικό κόστος της επεξεργασίας δεδομένων. Από την άλλη πλευρά, υπάρχουν προκλήσεις διαδικασίας για την εύρεση του κατάλληλου μοντέλου για ανάλυση και την ικανότητα γρήγορης επανάληψης. Ολοκλήρωση δεδομένων και σιλό δεδομένων ως πρόκληση και περιορισμένη πρόσβαση σε πληροφορίες που συλλέγονται από ιδιωτικές εταιρείες και μαζί με την ολοκλήρωση. Έλλειψη πλατφόρμας ανάλυσης μεγάλων δεδομένων μεταξύ εφαρμογών και υπηρεσιών για την παροχή ευφυΐας δεδομένων. Η ασφάλεια και η ιδιωτικότητα είναι ζωτικοί παράγοντες επιτυχίας για τις λύσεις ανάλυσης στην έξυπνη πόλη, συμπεριλαμβανομένης της ανθεκτικότητας της έξυπνης πόλης. Η ανεξέλεγκτη συσσώρευση δεδομένων από πολυάριθμους οργανισμούς κοινωνικής δικτύωσης αποτελεί τη μεγαλύτερη απειλή για την ασφάλεια, καθώς τα μεγάλα σύνολα δεδομένων βάζουν σε πειρασμό τους επιτιθέμενους στον κυβερνοχώρο. Η πιθανότητα παράνομης πρόσβασης ή κακόβουλων επιθέσεων στις υποδομές δεδομένων μπορεί να οδηγήσει σε καταστροφικά αποτελέσματα που επηρεάζουν τις υποδομές της πόλης, τους κυβερνητικούς φορείς και τους κατοίκους της. Άλλες προκλήσεις που συζητούνται στη βιβλιογραφία περιλαμβάνουν τον τεχνολογικό εγκλωβισμό από ορισμένα από τα συστήματα και τις λύσεις έξυπνων πόλεων, τη διαχείριση μεγάλων δεδομένων ως πρόκληση από τον υπερπληθυσμό δεδομένων και τον πλεονασμό δεδομένων και την αδυναμία παροχής ποιοτικών υπηρεσιών στους χρήστες με τη χρήση γρήγορων μηχανών επεξεργασίας για την έγκαιρη ανάλυση μεγάλων συνόλων δεδομένων [61].

4.4 Θεωρητικό πλαίσιο υιοθέτησης

Η κατανόηση της υιοθέτησης της τεχνολογίας σε έναν οργανισμό μπορεί να προσεγγιστεί από διαφορετικές θεωρητικές προοπτικές. Με βάση το ερώτημα για τον προσδιορισμό των βασικών παραγόντων για την υιοθέτηση της ανάλυσης

μεγάλων δεδομένων για την επίτευξη της ανθεκτικότητας των έξυπνων πόλεων, η παρούσα μελέτη χρησιμοποίησε το εννοιολογικό μοντέλο για τη διαδικασία υιοθέτησης της πληροφορικής. Οι επακόλουθες περιγραφές σε αυτή την ενότητα παρέχουν τους λόγους για την επιλογή αυτού του θεωρητικού μοντέλου και τη λεπτομερή εξήγησή του σε σχέση με την υιοθέτηση της ανάλυσης μεγάλων δεδομένων για την επίτευξη έξυπνης ανθεκτικότητας των πόλεων.

Τα ραγδαία βήματα που κάνουν οι τεχνολογικές καινοτομίες καθημερινά έχουν κάνει την υιοθέτηση της τεχνολογίας να αποκτά όλο και μεγαλύτερη σημασία τον τελευταίο καιρό. Τεράστιες επενδύσεις γίνονται από οργανισμούς και κυβερνήσεις για την εισαγωγή νέων τεχνολογιών που έχουν τη δυνατότητα να φέρουν νέα αλλαγή παραδείγματος στο στυλ των χρηστών, όπως μπορεί να φανεί στο σχεδιασμό και την ανάπτυξη έξυπνων πόλεων και την υιοθέτηση της ανάλυσης μεγάλων δεδομένων. Παρά το επιχείρημα αυτό, οι επενδύσεις αυτές μπορεί να μην αποδώσουν αποτελέσματα εάν οι καινοτομίες υιοθετηθούν από τους προβλεπόμενους χρήστες, οι προκλήσεις και τα εμπόδια δεν εντοπιστούν και δεν επιλυθούν πριν από την επένδυση και οι δυνατότητες αυτών των καινοτομιών δεν αναγνωριστούν και δεν αξιοποιηθούν πλήρως. Αρκετές μελέτες, συμπεριλαμβανομένων εκείνων της υιοθέτησης της ανάλυσης μεγάλων δεδομένων στις έξυπνες πόλεις, έχουν επικεντρωθεί στις πτυχές της τεχνολογίας ως πρόκληση για την υιοθέτηση της τεχνολογίας, ωστόσο η υιοθέτηση της τεχνολογίας δεν σχετίζεται μόνο με τις πτυχές της τεχνολογίας. Οι μελέτες αποκαλύπτουν ότι υπάρχουν και άλλοι παράγοντες που έχουν εξελιχθεί ως πολύ πιο σύνθετοι στην υιοθέτηση της τεχνολογίας, όπως η ηγεσία, η κοινωνική επιρροή, η κουλτούρα και η στρατηγική. Ως εκ τούτου, είναι σημαντικό η θεωρία που πρέπει να υιοθετηθεί να καλύπτει διάφορες πτυχές της υιοθέτησης της ΤΠ εντός των οργανισμών [62].

Το μοντέλο αποτελείται από πέντε κατηγορίες χαρακτηριστικών που επηρεάζουν την υιοθέτηση της καινοτομίας ΤΠ σε οργανωτικό επίπεδο. Σε οργανωτικό επίπεδο, τα χαρακτηριστικά καινοτομίας εξετάζουν τους παράγοντες καινοτομίας που ωθούν τους οργανισμούς να υιοθετήσουν την ΤΠ, όπως η συμβατότητα, η πολυπλοκότητα και το κόστος. Αυτό είναι σύμφωνο με το ερευνητικό ερώτημα που προσπαθούμε να απαντήσουμε, καθώς μας οδηγεί στην

αξιολόγηση του τι οδηγεί τους φορείς υλοποίησης, όπως τα δημοτικά και αστικά συμβούλια, να υιοθετήσουν την ανάλυση μεγάλων δεδομένων στην ανθεκτικότητα της έξυπνης πόλης. Τα οργανωσιακά χαρακτηριστικά εξετάζουν τα χαρακτηριστικά ενός οργανισμού όπως η ετοιμότητα, η υποστήριξη της ανώτατης διοίκησης, η υποδομή του ΠΣ, η κουλτούρα και οι πόροι εντός των ορίων ενός οργανισμού. Από την άλλη πλευρά, τα περιβαλλοντικά χαρακτηριστικά, περιλαμβάνουν εξωτερικούς παράγοντες που επηρεάζουν την οργανωτική υιοθέτηση της ΤΠ, αυτοί περιλαμβάνουν την πίεση από τους εταίρους, την κυβερνητική υποστήριξη, την ετοιμότητα των εταίρων και την εξωτερική πίεση. Στο πλαίσιο της παρούσας έρευνας, θα θεωρήσουμε τα περιβαλλοντικά χαρακτηριστικά ως εξωτερικά χαρακτηριστικά. Από το πλαίσιο του ατομικού επιπέδου, το εννοιολογικό μοντέλο εξετάζει τα χαρακτηριστικά του CEO, τα οποία βασικά εστιάζουν στα ατομικά χαρακτηριστικά που συμβάλλουν στην οργανωτική υιοθέτηση της ΤΠ. Αυτό το χαρακτηριστικό, περιλαμβάνει παράγοντες όπως η στάση του CEO απέναντι στην αλλαγή και οι γνώσεις του CEO για την ΤΠ.

Ο τελευταίος καθοριστικός παράγοντας είναι το χαρακτηριστικό αποδοχής από τον χρήστη. Αυτή η πτυχή εξετάζεται από οργανωτική άποψη και περιλαμβάνει παράγοντες όπως η αντιλαμβανόμενη χρησιμότητα, η εμπειρία του χρήστη και η στάση απέναντι στη χρήση. Ωστόσο, με βάση την οριοθέτηση της διατριβής μας. Δεν θα συμπεριλάβουμε το πλαίσιο του εννοιολογικού μοντέλου σε ατομικό επίπεδο. Σε συνδυασμό με την παραπάνω περιγραφή, η διαδικασία υιοθέτησης αποτελείται από τρεις φάσεις, δηλαδή την έναρξη, την απόφαση υιοθέτησης και την εφαρμογή. Η παρούσα μελέτη θεωρεί το στάδιο της έναρξης ως το στάδιο που αποτελείται από δραστηριότητες που σχετίζονται με την αναγνώριση μιας ανάγκης, την απόκτηση γνώσης ή ευαισθητοποίησης, τη διαμόρφωση στάσης απέναντι στην καινοτομία και την πρόταση καινοτομίας για υιοθέτηση. Το στάδιο της υιοθέτησης-απόφασης εξετάζει την απόφαση αποδοχής της ιδέας και αξιολογεί τις προτεινόμενες ιδέες από διάφορες οργανωτικές προοπτικές, όπως τεχνική, οικονομική, επίσης το στάδιο αυτό εξετάζει την κατανομή των πόρων για την απόκτηση και την εφαρμογή της. Το στάδιο της υλοποίησης περιλαμβάνει την απόκτηση της καινοτομίας, την

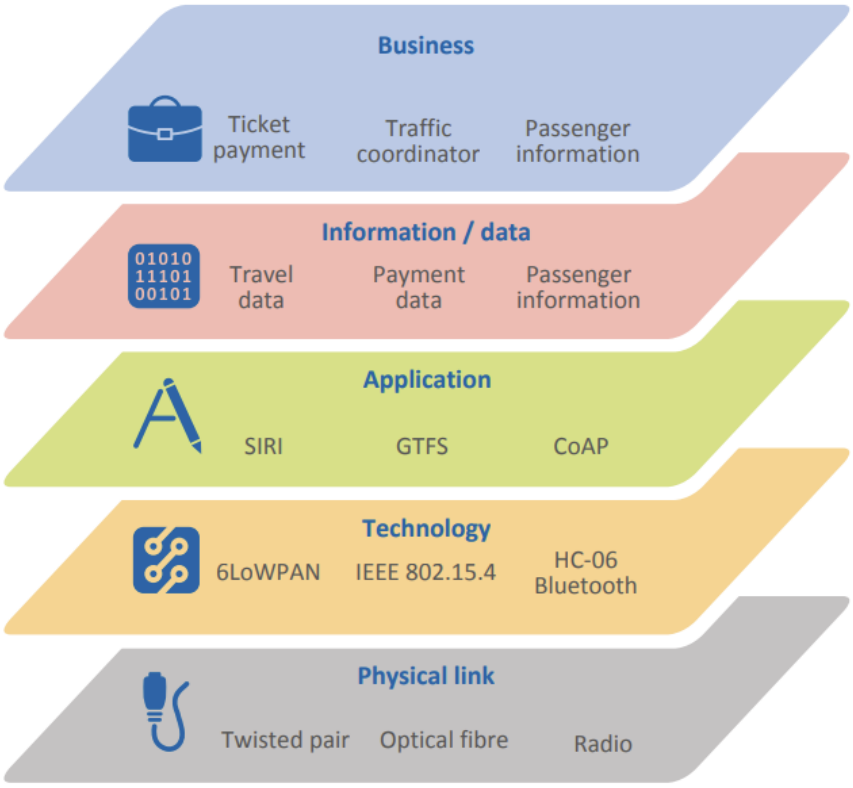
προετοιμασία του οργανισμού για τη χρήση της καινοτομίας, την πραγματοποίηση μιας δοκιμής για επιβεβαίωση της καινοτομίας [63].

5 CYBER SECURITY ΣΕ ΕΞΥΠΝΕΣ ΠΟΛΕΙΣ

Με τον όρο κυβερνοχώρο εννοούμε το εικονικό περιβάλλον στο οποίο πραγματοποιούνται ηλεκτρονικές επικοινωνίες, όπως και το διαδίκτυο στο οποίο γίνεται ανταλλαγή ηλεκτρονικών μηνυμάτων. Με βάση λοιπόν αυτόν τον όρο, ο κυβερνοχώρος αποτελεί ένα δίκτυο ψηφιακών πληροφοριών και επικοινωνιακών υποδομών, το οποίο είναι συνδεδεμένο παγκοσμίως [64].

Σαν ορισμός έγινε γνωστός στο ευρύ κοινό την δεκαετία του ’90, την περίοδο δηλαδή που αυξανόταν δραματικά οι χρήστες του διαδικτύου, οι οποίοι ξεκίνησαν να επικοινωνούν ψηφιακά και να δικτυώνονται ενώ ο όρος «κυβερνοχώρος» κατάφερε να αντιπροσωπεύσει τις ποικίλες καινούριες ιδέες και τα φαινόμενα που εμφανίστηκαν.

Ο κυβερνοχώρος θεωρείται η πέμπτη πολεμική απειλή μετά τις επιθέσεις από ξηρά, από αέρα, από θάλασσα και από το διάστημα, με την διαφορά ότι αυτή είναι δημιούργημα του ίδιου του ανθρώπου . Το συγκεκριμένο χαρακτηριστικό είναι υψίστης σημασίας αφού επιτρέπει να αναπτύσσεται γρήγορα λόγω της ανάπτυξης της τεχνολογίας και γοργών ρυθμών που ακολουθεί. Το εικονικό περιβάλλον που προσφέρει ο κυβερνοχώρος αποτελείται από πολλούς χρήστες όπου ένας αλληλεπιδρά με τον άλλο οπότε και το καθιστά εξαιρετικά επικίνδυνο για την εθνική ασφάλεια . Η κάθε απειλή του κυβερνοχώρου μπορεί να οδηγήσει στην διακοπή των δυνατοτήτων που έχει ο χρήστης η οποία είναι θέμα χρόνου να μετατρέψει την ψηφιακή εποχή σε σκοτεινή [65]. Στο σχήμα 5.1 που ακολουθεί φαίνονται μία διαστρωματωποιημένη αρχιτεκτονική αντίστοιχη του OSI και αφορά τα δεδομένα μιας έξυπνης πόλης.



Σχήμα 5.1: Ανταλλαγή δεδομένων σε στρώματα αντίστοιχη του OSI [73]

5.1 Κυβερνοασφάλεια

Με το πρόθεμα «κυβερνό-» αναλύονται οι όροι που έχουν σχέση με το διαδίκτυο αλλά και τους ηλεκτρονικούς υπολογιστές. Στην ακαδημαϊκή κοινότητα δεν μπορεί να επιτευχθεί πλήρης συμφωνία σε σχέση με την έννοια των όρων, με αποτέλεσμα την πραγματοποίηση εναλλακτικών προσεγγίσεων. Ο όρος «κυβερνοχώρος» περιλαμβάνει τον ψηφιακό χώρο, που δημιουργεί η χρήση του διαδικτύου και των ηλεκτρονικών υπολογιστών. Ωστόσο, ο συγκεκριμένος ορισμός δεν μπορεί να εκφράσει την απεριόριστη φύση του διαδικτύου, οπότε και καθιστά απαραίτητη την επιπλέον διεύρυνσή του. Έτσι, ανάλογα με την προσέγγιση, χρησιμοποιούνται άλλοι περισσότερο περιγραφικοί όροι. Η άποψη πως ο κυβερνοχώρος αποτελεί το εικονικό περιβάλλον εντός του οποίου δραστηριοποιείται ο χρήστης του διαδικτύου, θεωρείται περισσότερο ακριβής και οικείος. Η δραστηριότητα αυτή περιλαμβάνει συναλλαγές και αγοραπωλησίες, επικοινωνίες, έρευνες, μελέτες και άλλα. Το διαδίκτυο αποτελεί έναν περίπλοκο εικονικό κόσμο. Ο κυβερνοχώρος δεν μπορεί να οριοθετηθεί και δεν μπορεί να περιοριστεί, παρουσιάζοντας ένα εξαιρετικά μεγάλο μέγεθος το μεγαλύτερο τμήμα

του οποίου εξακολουθεί να είναι άγνωστο στο ευρύ κοινό. Έτσι, η πρόσβαση ενός χρήστη σε όλο τον κυβερνοχώρο που δεν διαθέτει ειδικές γνώσεις πάνω στο αντικείμενο και ένα εξειδικευμένο μηχάνημα είναι αδύνατη. Το τμήμα αυτό ονομάζεται «σκοτεινό δίκτυο» ή «dark web». Στον κυβερνοχώρο, οι παράνομες δράσεις που πραγματοποιούνται έχουν αφετηρία το ψηφιακό περιβάλλον του διαδικτύου, αλλά είναι στενά συνδεδεμένες και με το πραγματικό περιβάλλον. Οι εγκληματικές οργανώσεις οι οποίες απειλούν τόσο την εθνική όσο και την διεθνή ασφάλεια, μέσα από τις δραστηριότητές τους στον κυβερνοχώρο είναι πιθανό να ασχολούνται με το «χακάρισμα», εν ολίγοις την παραβίαση στα συστήματα ασφαλείας είτε φορέων, είτε ιδιωτών, την διάδοση πληροφοριών χωρίς τις απαραίτητες άδειες ή την παράνομη πρόσβαση σε τραπεζικά συστήματα με την χρήση του διαδικτύου. Στην καθημερινότητα, στο διαδίκτυο πραγματοποιούνται ύποπτες δραστηριότητες και απειλές που αφορούν την παράνομη εκτέλεση συναλλαγών και αγοραπωλησιών σε εικονικό χώρο, το παρεμπόριο, τις απειλές και άλλα. Παράνομες δράσεις, που παρουσιάζουν τα προαναφερθέντα στοιχεία, που πραγματοποιούνται στο ψηφιακό περιβάλλον ταξινομούνται στην κατηγορία των κυβερνοεπιθέσεων. Οι επιθέσεις παρουσιάζουν μια ιδιαιτερότητα η οποία είναι η δυσκολία τόσο να εντοπιστούν, όσο και να αντιμετωπιστούν, αφού τις περισσότερες φορές, πραγματοποιούνται την ίδια στιγμή από διαφορετικά σημεία σε όλο τον κόσμο, καθιστώντας δύσκολο την εύρεση τόσο του αρχικού, όσο και του τελικού αποδέκτη. Το μεγαλύτερο ποσοστό των επιθέσεων του κυβερνοχώρου στοχεύει στην επίτευξη οικονομικού κέρδους ή στην πρόκληση χάους. Στην προκειμένη περίπτωση οι εγκληματικές δραστηριότητες μπορεί να προκαλέσουν μια γενικότερη κρίση. Οι πιθανότητες δημιουργίας κρίσεων οι οποίες είναι ικανές να πλήξουν μια χώρα είτε σε πολιτικό, είτε σε οικονομικό επίπεδο, αυξάνονται σημαντικά σε περιπτώσεις που παραβιάζονται συστήματα ασφαλείας με σκοπό την υποκλοπή και στη συνέχεια πώληση των πληροφοριών ή ακόμα και τον χαρακτηρισμό των φορέων αλλά και των εταιρειών ως αναξιόπιστες να προστατέψουν τόσο τους πελάτες τους όσο και τα προσωπικά τους δεδομένα και τις βάσεις δεδομένων τους. Είναι γεγονός πως πολλά ισχυρά κράτη αλλά και ομάδες που εμπλέκονται στο οργανωμένο έγκλημα, πολύ συχνά κρύβονται πίσω από επιθέσεις στον κυβερνοχώρο. Κάποιοι χάκερς, διαθέτουν εξαιρετικά εξελιγμένη τεχνογνωσία, την

οποία και χρησιμοποιούν για να διαταράξουν την ισορροπία σε παγκόσμιο επίπεδο, διεισδύοντας σε επίπεδο που ένας απλός χρήστης του διαδικτύου αδυνατεί. Τέλος, η ισχύς του κυβερνοχώρου είναι ακόμα ένας ορισμός με πολύ ενδιαφέρον.

Η οδηγία NIS αναλύει ένα «νομοθετικό ορισμό», ο οποίος αναφέρει πως η κυβερνοασφάλεια είναι η δυνατότητα των συστημάτων δικτύου και πληροφοριών να αμύνονται σε συγκεκριμένο βαθμό αξιοπιστίας, σε δράσεις που πλήττουν τη διαθεσιμότητα, την ανθεκτικότητα, την ακεραιότητα ή το απόρρητο των στοιχείων που αποθηκεύονται, μεταφέρονται ή επεξεργάζονται ή των συναφών υπηρεσιών που παρέχονται ή είναι προσιτές μέσω αυτών των συστημάτων δικτύου και πληροφοριών [66].

Οι διάφοροι τομείς που περιλαμβάνει ο όρος της κυβερνοασφάλειας είναι [67]:

• Ασφάλεια Επικοινωνιών: είναι μέτρα που αφορούν την προστασία από απειλές για την υποδομή τεχνικής φύσης του κυβερνοχώρου που είναι ικανά να μεταβάλλουν τα χαρακτηριστικά στοιχεία του έτσι ώστε να επιδοθεί σε δραστηριότητες ενώ δεν είχαν προγραμματιστεί ούτε από τους ιδιοκτήτες και τους σχεδιαστές, όσο και από τους χρήστες του.

• Ασφάλεια Λειτουργιών: είναι μέτρα που αφορούν την προστασία από την προγραμματισμένη διαφθορά διαδικασιών ή από την ροή της εργασίας που θα φέρουν αποτελέσματα τα οποία δεν είχαν προγραμματιστεί ούτε από τους ιδιοκτήτες και τους σχεδιαστές, όσο και από τους χρήστες.

• Ασφάλεια Πληροφοριών: είναι μέτρα που αφορούν την προστασία από τον κίνδυνο κλοπής, διαγραφής ή μεταβολής των δεδομένων που είναι αποθηκευμένα ή που μεταδίδονται στον κυβερνοχώρο.

• Φυσική ασφάλεια: είναι μέτρα που αφορούν την προστασία από τους φυσικούς κινδύνους οι οποίοι είναι ικανοί να επηρεάσουν ή να διαταράξουν την ευημερία του κυβερνοχώρου. Για παράδειγμα η άσκηση πίεσης των χρηστών και των οικογενειών τους να κάνουν κάτι παρά την θέλησή τους.

• Δημόσια και Εθνική ασφάλεια: είναι μέτρα που αφορούν την προστασία από κυβερνοεπιθέσεις, οι οποίες απειλούν στοιχεία της είτε φυσικής, είτε κυβερνητικής περιουσίας, με τέτοιο τρόπο που επιφέρει όφελος στον επιτιθέμενο. Για παράδειγμα, οι επιθέσεις DOS που έχουν πραγματοποιηθεί στις κοινωφελείς επιχειρήσεις και σε διάφορες άλλες βασικές υποδομές.

5.2 Απειλές στον Κυβερνοχώρο

Η Κυβερνοασφάλεια αποτελεί την μέθοδο εκείνη που εφαρμόζεται με στόχο την προστασία των συστημάτων δικτύων και προγραμμάτων από τις διάφορες ψηφιακές απειλές που παρουσιάζονται κατά την χρήση τους. Ειδικότερα όταν αναφέρεται ο όρος Κυβερνοασφάλεια, νοείται το περιβάλλον εκείνο που έχει δημιουργηθεί από δίκτυα επικοινωνιών, με την χρήση ψηφιακών τεχνολογιών στον κυβερνοχώρο. Το διαδίκτυο δεν είναι ένας ενιαίος χώρος και μπορεί να διαχωριστεί σε τρία μέρη [68]:

1. Στο διαδίκτυο, το οποίο και χρησιμοποιούν οι περισσότεροι χρήστες, στο οποίο περιέχονται σημαντικές και μη πληροφορίες που μπορούν να ανακτηθούν με ευκολία με την χρήση ειδικών μηχανών αναζήτησης, όπως για παράδειγμα είναι το Google, το Yahoo Search, το Bing και άλλα.

2. Στο deep web, το οποίο περιλαμβάνει πληροφορίες οι οποίες δεν καταχωρούνται στις δημοφιλείς πλατφόρμες που χρησιμοποιούνται για αναζήτηση και αποτελεί το σημαντικότερο και πιο μεγάλο μέρος αυτού.

3. Στο σκοτεινό δίκτυο (dark web), στο οποίο ως επί το πλείστον λαμβάνουν χώρα παράνομες αγοραπωλησίες, παρέχεται υλικό που δεν δημοσιοποιείται ή διανέμεται σε νόμιμες ιστοσελίδες, όπως για παράδειγμα φωτογραφίες παιδικής πορνογραφίας. Συχνά επίσης πραγματοποιούνται επικοινωνίες ανεπίσημες, οι οποίες σε πραγματικό περιβάλλον χαρακτηρίζονται ως κακουργήματα, όπως για παράδειγμα είναι οι συμφωνίες ανάμεσα σε εγκληματικές οργανώσεις. Παρόλο που όλα τα κράτη καταβάλλουν προσπάθειες, το σκοτεινό δίκτυο εξακολουθεί να είναι ένα περιβάλλον όπου δεν είναι καθόλου εύκολο ούτε να παρακολουθηθεί, αλλά ούτε να ελεγχθεί, ενώ την ίδια στιγμή αναπτύσσεται συνεχώς. Εξάλλου λόγω της αδυναμίας ταξινόμησης που παρουσιάζουν οι πληροφορίες οι οποίες

εμπεριέχονται τόσο στο dark web όσο και στο deep web, καθιστά αδύνατο τον έλεγχο.

Οι κύριες εγκληματικές δράσεις που πραγματοποιούνται στο dark web και αποτελούν απειλή για την ασφάλεια του κυβερνοχώρου περιλαμβάνουν, ανάμεσα σε άλλα [69]:

• Ποικίλες παράνομες αγοραπωλησίες και συναλλαγές οι οποίες αποτελούν εγκληματικές ενέργειες τόσο από το κράτος στο οποίο και πραγματοποιούνται όσο και από το διεθνές δίκαιο. Σε αυτήν την κατηγορία μπορεί να περιληφθούν η αγορά ή πώληση προϊόντων, η κατοχή των οποίων θεωρείται παράνομη. Τέτοια αγαθά αποτελούν τα ζώα από εξωτικές χώρες, οι ναρκωτικές ουσίες, τα όπλα αλλά και διάφορα φαρμακευτικά σκευάσματα. Ακόμα στην συγκεκριμένη κατηγορία συμπεριλαμβάνονται το εμπόριο λευκής σαρκός αλλά και το εμπόριο βρεφών.

• Η ανταλλαγή αλλά και η πώληση αγαθών και πληροφοριών που έχουν προκύψει από υποκλοπή. Τα αγαθά αυτά είναι αρχαία αντικείμενα, διάφορα παράνομα φορτία, τηλεφωνικά νούμερα, πελατολόγια, υλικό πορνογραφίας, αλλά και φωτογραφίες.

• Τις κινήσεις που υποστηρίζουν και υποκινούν την δραστηριότητα μαφίας και τρομοκρατικών ομάδων. Σε αυτήν την κατηγορία περιλαμβάνεται και ο εντοπισμός νέων μελών για την στελέχωση παράνομων και εγκληματικών ομάδων.

• Την διανομή μουσικών μελωδιών, βίντεο και άλλου υλικού παράνομα με την χρήση του διαδικτύου, χωρίς την κατοχύρωση πνευματικών δικαιωμάτων.

• Το παράνομο στοίχημα και η χαρτοπαιξία περιλαμβάνονται στην συγκεκριμένη κατηγορία εκτός από αυτές για τις οποίες έχουν καταβληθεί στο κράτος οι ανάλογες εισφορές από τις εταιρίες στοιχημάτων που λειτουργούν νόμιμα, οι οποίες και παρέχουν προστασία στον χρήστη.

• Δολοφονικές επιθέσεις αλλά και δράσεις εκφοβισμού υψηλών προσώπων συνήθως οργανώνονται στο dark web.

Συνήθως επικρατεί η εσφαλμένη εντύπωση πως οι δράστες των κυβερνοεπιθέσεων είναι άτομα που δρουν μεμονωμένα ή ομάδες ατόμων που διαθέτουν εγκληματικό χαρακτήρα. Δεν είναι όμως σπάνιο οι δράστες των επιθέσεων στον κυβερνοχώρο να είναι πολυεθνικές εταιρίες οι οποίες εκμεταλλεύονται τις θέσεις υπεροχής που διαθέτουν, υποκλέπτοντας βάσεις δεδομένων από ανταγωνίστριες εταιρίες ή και από άλλα κράτη. Η λειτουργία των ομάδων στο dark web είναι ακριβώς η ίδια με αυτή του φυσικού περιβάλλοντος. Και μόνο που υφίστανται dark web δημιουργεί πρόβλημα στις κυβερνήσεις, αφού κινδυνεύει η διεθνής ασφάλεια. Τα κράτη τα οποία ειδικεύονται στην διαχείριση των εγκληματικών οργανώσεων, παρουσιάζουν αδυναμία σύλληψης των παρανόμων. Πολλές φορές, επικρατεί ο προβληματισμός σχετικά με τον καθορισμό των τρόπων και μεθόδων εντοπισμού των εγκληματιών αλλά και της σύλληψής τους, με δεδομένο πως από την εικονική φύση του κυβερνοχώρου που θα εντοπιστούν, θα συλληφθούν σε πραγματικό περιβάλλον. Πέρα από τις συνέπειες που έχει κάθε παράνομη δραστηριότητα στον κυβερνοχώρο, οι εγκληματικές δράσεις είναι πιθανό να επηρεάσουν το σύνολο των χρηστών και έμμεσα. Η παραοικονομία, αλλά και η «μαύρη αγορά» προκαλούν προβλήματα τόσο στην οικονομία, όσο και στην παραγωγικότητα της χώρας και καθιστούν επικίνδυνη την εύρυθμη λειτουργία των θεσμών. Οι έλεγχοι δεν είναι δυνατόν να πραγματοποιηθούν εξαιτίας της μη καταβολής των ανάλογων εισφορών. Έτσι τα αγαθά που διατίθενται προς πώληση ακόμα και τα νομίμως αποκτηθέντα, δεν πληρούν πάντα τις απαραίτητες προϋποθέσεις ασφαλείας και το επίπεδο της ποιότητάς τους είναι πιθανό να διαφέρει από αυτό που οι αγοραστές απαιτούν.

5.3 Συστήματα ανίχνευσης και συστήματα πρόληψης εισβολής

Μία προσέγγιση για την πρόληψη των ιών και των "σκουληκιών" από την είσοδό τους σ' ένα δίκτυο είναι για έναν διαχειριστή να παρακολουθεί συνεχώς το δίκτυο και να αναλύει τα αρχεία καταγραφής που δημιουργούνται από τις συσκευές του δικτύου. Αυτή η λύση δεν είναι πολύ επεκτάσιμη. Μη αυτόματη ανάλυση των πληροφοριών του αρχείου καταγραφής είναι μια χρονοβόρα διαδικασία και παρέχει μια περιορισμένη εικόνα των επιθέσεων που ξεκίνησαν εναντίον ενός δικτύου. Ώσπου οι καταγραφές αναλύονται, η επίθεση έχει ήδη αρχίσει. Τα

Συστήματα Ανίχνευσης Εισβολών (IDSs) υλοποιήθηκαν για να παρακολουθούν παθητικά την κίνηση στο δίκτυο. Μία IDS-enabled συσκευή αντιγράφει το ρεύμα της κυκλοφορίας και αναλύει την κυκλοφορία υπό παρακολούθηση παρά τα πραγματικά προωθούμενα πακέτα. Η εργασία χωρίς σύνδεση, συγκρίνει το καταγεγραμμένο ρεύμα κυκλοφορίας με τις γνωστές κακόβουλες υπογραφές, παρόμοια με το λογισμικό που ελέγχει για ιούς. Αυτό η offline IDS εφαρμογή αναφέρεται ως ετερόκλητη λειτουργία. Το πλεονέκτημα της λειτουργίας με ένα αντίγραφο της κίνησης είναι ότι το IDS δεν επηρεάζει αρνητικά την πραγματική ροή των πακέτων της διαβιβαζόμενης κίνησης. Το μειονέκτημα της λειτουργίας σ' ένα αντίγραφο της κίνησης είναι ότι το IDS δεν μπορεί να σταματήσει κακόβουλες single-packet επιθέσεις από την επίτευξη του στόχου πριν απαντήσει στην επίθεση. Ένα IDS απαιτεί συχνά βοήθεια από άλλες συσκευές δικτύωσης, όπως δρομολογητές και τείχη προστασίας, για να ανταποκριθεί σε μια επίθεση. Είναι καλύτερη η εφαρμογή μιας λύσης που ανιχνεύει και αντιμετωπίζει αμέσως ένα πρόβλημα δικτύου, όπως απαιτείται [70].

5.3.1 Intrusion Prevention Systems

Ένα σύστημα πρόληψης εισβολής (IPS) βασίζεται σε τεχνολογία IDS. Σε αντίθεση με το IDS, μια IPS συσκευή υλοποιείται σε inline λειτουργία. Αυτό σημαίνει ότι όλη η κίνηση εισόδου και εξόδου πρέπει να ρέει μέσα από αυτό για επεξεργασία. Ένα IPS δεν επιτρέπει τα πακέτα να εισέλθουν στην έμπιστη πλευρά του δικτύου, χωρίς πρώτα να αναλυθούν. Μπορεί να ανιχνεύσει και να αντιμετωπίσει άμεσα ένα πρόβλημα δικτύου, όπως απαιτείται. Ένα IPS παρακολουθεί την Layer 3 και Layer 4 κυκλοφορία και αναλύει τα περιεχόμενα και το ωφέλιμο φορτίο των πακέτων για πιο εξελιγμένες ενσωματωμένες επιθέσεις που θα μπορούσαν να περιλαμβάνουν κακόβουλο δεδομένα στα στρώματα 2 έως 7. Οι πλατφόρμες Cisco IPS χρησιμοποιούν ένα μίγμα των τεχνολογιών ανίχνευσης, συμπεριλαμβανομένου του signature-based, profile-based και ανάλυση πρωτοκόλλων ανίχνευσης εισβολής. Αυτή η βαθύτερη ανάλυση επιτρέπει το IPS να εντοπίζει, σταματάει και μπλοκάρει επιθέσεις που θα διαπερνούν μια παραδοσιακή συσκευή τείχους προστασίας. Όταν ένα πακέτο έρχεται μέσα από μια διεπαφή σ'ένα IPS, αυτό το πακέτο δεν αποστέλλεται στην εξερχόμενη ή έμπιστη διεπαφή

έως ότου να αναλυθεί το πακέτο. Το πλεονέκτημα της λειτουργίας σε inline mode είναι ότι το IPS μπορεί να σταματήσει τις single-packet επιθέσεις από το να φθάσουν στον στόχο του συστήματος. Το μειονέκτημα είναι ότι ένα κακώς διαμορφωμένο IPS ή μια ακατάλληλη λύση IPS μπορεί να επηρεάσει αρνητικά τη ροή των πακέτων της διαβιβαζόμενης κυκλοφορίας. Η μεγαλύτερη διαφορά μεταξύ των IDS και IPS είναι ότι το IPS ανταποκρίνεται αμέσως και δεν επιτρέπει καμία κακόβουλη κυκλοφορία να περάσει, ενώ ένα IDS μπορεί να επιτρέψει κακόβουλη κυκλοφορίας να περάσει πριν απαντήσει. Οι IDS και IPS τεχνολογίες μοιράζονται πολλά χαρακτηριστικά. Και οι δύο IDS και IPS τεχνολογίες αναπτύσσονται ως αισθητήρες. Ένας IDS ή IPS αισθητήρας μπορεί να είναι οποιοσδήποτε από τις ακόλουθες συσκευές: Δρομολογητής διαμορφωμένος με το Cisco IOS IPS λογισμικό. Συσκευή που έχει σχεδιαστεί ειδικά για να παρέχει ειδικές IDS ή IPS υπηρεσίες Μονάδα δικτύου που είναι εγκατεστημένη σε ένα προσαρμοστικό συσκευής ασφαλείας, διακόπτη ή δρομολογητή. Οι IDS και IPS τεχνολογίες χρησιμοποιούν υπογραφές για να εντοπίζουν μοτίβα της κακής χρήσης της κίνησης του δικτύου. Μια υπογραφή είναι ένα σύνολο κανόνων που χρησιμοποιεί ένα IDS ή IPS για την ανίχνευση τυπικής παρεμβατικής δραστηριότητας. Οι υπογραφές μπορεί να χρησιμοποιηθούν για την ανίχνευση σοβαρών παραβιάσεων της ασφάλειας, κοινές επιθέσεις στο δίκτυο, καθώς και τη συλλογή πληροφοριών. Οι IDS και IPS τεχνολογίες μπορούν να ανιχνεύσουν μοτίβα ατομικής υπογραφής (single-packet) ή μοτίβα σύνθετης υπογραφής (multi-packet) [71].

5.3.2 Πλεονεκτήματα και μειονεκτήματα IDS

Ένα βασικό πλεονέκτημα μιας πλατφόρμας IDS είναι ότι έχει αναπτυχθεί σε promiscuous mode. Επειδή ο αισθητήρας IDS δεν είναι ενσωματωμένος, δεν έχει καμία επίπτωση στην απόδοση του δικτύου. Δεν εισάγει το latency, jitter, ή άλλα θέματα της κυκλοφοριακής ροής. Επιπλέον, εάν ένας αισθητήρας αποτύχει, αυτό δεν επηρεάζει τη λειτουργικότητα του δικτύου. Επηρεάζει μόνο την ικανότητα του IDS να αναλύσει τα δεδομένα. Αλλά υπάρχουν πολλά μειονεκτήματα από την ανάπτυξη μιας πλατφόρμας IDS σε promiscuous mode. Οι ενέργειες απόκρισης του IDS αισθητήρα δεν μπορούν να σταματήσουν το trigger πακέτο και δεν είναι εγγυημένα για να σταματήσουν μια σύνδεση. Επίσης, είναι λιγότερο χρήσιμες για τη

διακοπή των ιών ηλεκτρονικού ταχυδρομείου και τις αυτοματοποιημένες επιθέσεις, όπως τα "σκουλήκια". Οι χρήστες που αναπτύσσουν ενέργειες απόκρισης του IDS αισθητήρα πρέπει να έχουν μια καλά μελετημένη πολιτική ασφάλειας, σε συνδυασμό με μια καλή επιχειρησιακή κατανόηση των IDS αναπτύξεών τους. Οι χρήστες πρέπει να περνούν το χρόνο του συντονίζοντας τους IDS αισθητήρες για να επιτύχουν τα αναμενόμενα επίπεδα ανίχνευσης εισβολής. Τέλος, επειδή οι αισθητήρες IDS δεν είναι inline, μια εφαρμογή IDS είναι πιο ευάλωτη σε τεχνικές υπεκφυγής της ασφάλειας δικτύου που χρησιμοποιείται από διάφορες μεθόδους σύνδεσης δικτύου.

5.3.3 IPS πλεονεκτήματα και μειονεκτήματα

Η ανάπτυξη μιας πλατφόρμας IPS σε λειτουργία inline έχει και πλεονεκτήματα και μειονεκτήματα. Ένα πλεονέκτημα σε σχέση με IDS είναι ότι ένας αισθητήρας IPS μπορεί να ρυθμιστεί ώστε να εκτελεί ένα packet drop που μπορεί να σταματήσει το trigger πακέτο, τα πακέτα σε μια σύνδεση, ή πακέτα από μια IP διεύθυνση προέλευσης. Επιπλέον, ένας αισθητήρας IPS μπορεί να χρησιμοποιήσει τεχνικές κανονικοποίησης ρεύματος για τη μείωση ή την εξάλειψη πολλών δυνατοτήτων υπεκφυγής ασφαλείας δικτύου που υπάρχουν. Ένα μειονέκτημα του IPS είναι ότι τα σφάλματα, η αποτυχία, και η υπέρβαση του αισθητήρα IPS με πάρα πολύ κίνηση μπορεί να έχει αρνητική επίδραση στην απόδοση του δικτύου. Αυτό οφείλεται στο γεγονός ότι το IPS θα πρέπει να αναπτυχθεί inline και η κίνηση πρέπει να είναι σε θέση να περάσει μέσα από αυτό. Ένας αισθητήρας IPS μπορεί να επηρεάσει την απόδοση του δικτύου με την εισαγωγή του latency και jitter. Ένας αισθητήρας IPS πρέπει να είναι κατάλληλου μεγέθους και εφαρμοσμένος έτσι ώστε οι ευαίσθητες στον χρόνο εφαρμογές, όπως το VoIP, να μην επηρεάζονται αρνητικά.

Στην πραγματικότητα, οι IDS και IPS τεχνολογίες μπορούν να συμπληρώσουν η μία την άλλη. Για παράδειγμα, ένα IDS μπορεί να εφαρμοστεί για την επικύρωση της λειτουργίας του IPS, επειδή το IDS μπορεί να ρυθμιστεί για βαθύτερο έλεγχο πακέτου εκτός σύνδεσης. Αυτό επιτρέπει το IPS να επικεντρωθεί σε λιγότερα αλλά πιο κρίσιμα μοτίβα κίνησης inline. Αποφασίζοντας ποια εφαρμογή να χρησιμοποιήσετε βασίζεται στους στόχους ασφάλειας του οργανισμού, όπως αναφέρεται στην πολιτική ασφάλειας των δικτύων.

5.3.4 Άμυνα σε Βάθος

Η εφαρμογή του ακραίου δρομολογητή ποικίλλει ανάλογα με το μέγεθος του οργανισμού και την πολυπλοκότητα της επιθυμητής ποιότητας σχεδιασμού του δικτύου. Οι υλοποιήσεις του Router μπορούν να περιλαμβάνουν ένα ενιαίο router προστατεύοντας ένα ολόκληρο εσωτερικό του δικτύου ή δρομολογητή ως την πρώτη γραμμή άμυνας της προσέγγιση άμυνας σε βάθος. Ενιαία προσέγγιση Router. Στην ενιαία προσέγγιση router, ένα ενιαίο router συνδέει το προστατευόμενο δίκτυο, ή εσωτερικό LAN, στο Internet. Όλες οι πολιτικές ασφαλείας έχουν ρυθμιστεί σε αυτή τη συσκευή. Αυτό πιο συχνά αναπτύσσεται σε μικρότερες υλοποιήσεις site όπως κλάδοι και σελίδες SOHO. Σε μικρότερα δίκτυα, τα απαιτούμενα χαρακτηριστικά ασφαλείας μπορούν να υποστηριχθούν από τα ISRs χωρίς να εμποδίζουν τις επιδόσεις του δρομολογητή.

Μια παραλλαγή της προσέγγισης άμυνας σε βάθος είναι να προσφέρει μια ενδιάμεση περιοχή, που συχνά αποκαλείται η αποστρατικοποιημένη ζώνη(DMZ).Το DMZ μπορεί να χρησιμοποιηθεί για τους διακομιστές που πρέπει να είναι προσβάσιμοι από το διαδίκτυο ή κάποιο άλλο εξωτερικό δίκτυο. Το DMZ μπορεί να δημιουργηθεί ανάμεσα σε δύο δρομολογητές, με εσωτερικό δρομολογητή που συνδέεται με το προστατευόμενο δίκτυο και ενός εξωτερικού δρομολογητή που συνδέεται με το μη προστατευμένο δίκτυο. Εναλλακτικά,το DMZ μπορεί απλά να είναι μια πρόσθετη θύρα από ένα μόνο δρομολογητή. Το τείχος προστασίας, το οποίο βρίσκεται ανάμεσα στα προστατευόμενα και μη προστατευόμενα δίκτυα, έχει συσταθεί για να επιτρέπει τις απαραίτητες συνδέσεις(για παράδειγμα,HTTP) από τα εξωτερικά(μη αξιόπιστα) δίκτυα στους δημόσιους servers μέσα στο DMZ. Το τείχος προστασίας χρησιμεύει ως κύρια προστασία για όλες τις συσκευές στο DMZ. Στην προσέγγιση DMZ,ο δρομολογητής παρέχει κάποια προστασία με το φιλτράρισμα κάποιας κίνησης, αλλά αφήνει το μεγαλύτερο μέρος της προστασίας για το τείχος προστασίας [72].

6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα τελευταία χρόνια, τα έργα έξυπνων πόλεων αποκτούν ολοένα και μεγαλύτερη σημασία στην αστική ανάπτυξη πολλών πόλεων σε όλο τον κόσμο. Αυτό συνεπάγεται την απόκτηση νέων τρόπων διαχείρισης των πόλεων, οι οποίοι γενικά βασίζονται σε τεχνολογικές λύσεις που συγκεντρώνουν και επεξεργάζονται μεγάλες ποσότητες δεδομένων της πόλης. Για το σκοπό αυτό, οι δημόσιες διοικήσεις, οι οποίες στοχεύουν στην ανάπτυξη λύσεων έξυπνης πόλης, αναπτύσσουν συνήθως WSNs προκειμένου να συλλέγουν δεδομένα από τους δρόμους και, με τον τρόπο αυτό, να λαμβάνουν πληροφορίες σχετικά με τη λειτουργία της μητροπολιτικής υποδομών της μητρόπολης.

Ωστόσο, η μαζική ανάπτυξη WSNs σε ένα απροστάτευτο περιβάλλον, όπως οι δρόμοι, εγείρει ορισμένες ανησυχίες για την ασφάλεια. Επιπλέον, οι δημόσιες διοικήσεις αναθέτουν γενικά την εγκατάσταση και τη συντήρηση των WSNs σε εξωτερικούς παρόχους. Τα γεγονότα αυτά δημιουργούν σενάρια με διάφορα εμπόδια στην ασφάλεια, από τα οποία η παρούσα διατριβή ανέδειξε τρία. Πρώτον, η εξωτερική ανάθεση ενισχύει το ετερογενές περιβάλλον της έξυπνης πόλης. Κάθε αστική υπηρεσία απαιτεί διαφορετικό επίπεδο ασφάλειας και κάθε πάροχος προσφέρει διαφορετική λύση για την υλοποίηση ενός συστήματος. Δεύτερον, οι δικτυακές συσκευές που διαχειρίζονται οι πάροχοι καθίστανται λιγότερο προσβάσιμες από τη δημόσια διοίκηση. Αυτό, σε πολλές περιπτώσεις, αποτελεί εμπόδιο για την πρόσβαση στα αρχεία καταγραφής του συστήματος και την παρακολούθηση της κατάστασης της ασφάλειας του δικτύου. Και τρίτον, τα WSN είναι γενικά σχεδιασμένα ώστε να είναι ιδιαίτερα αποδοτικά για να μειώσουν την κατανάλωση ενέργειας και να παρατείνουν τη διάρκεια ζωής της μπαταρίας. Αυτό έχει ως αποτέλεσμα, σε ορισμένες περιπτώσεις, να μην υλοποιείται η επικοινωνία κατάντη, γεγονός που δυσχεραίνει τις ενημερώσεις λογισμικού, την ανταλλαγή κλειδιών κ.λπ. Επομένως, η εύρεση γενικεύσιμων λύσεων ασφάλειας για την προστασία των WSNs που να μπορούν να αντιμετωπίσουν την ετερογένεια της έξυπνης πόλης και οι οποίες να είναι επίσης αρκετά αποτελεσματικές και προσαρμόσιμες ώστε να μπορούν να εγκατασταθούν στους κόμβους αισθητήρων είναι ανέφικτη.

Επί του παρόντος, για την προστασία των WSN, οι δημόσιες διοικήσεις περιλαμβάνουν ρήτρες ασφαλείας στις συμφωνίες επιπέδου υπηρεσιών με τους εξωτερικούς παρόχους. Κατά συνέπεια, οι μηχανισμοί ασφαλείας βρίσκονται στα χέρια των παρόχων. Γενικά, οι πάροχοι ενσωματώνουν στους κόμβους αισθητήρων αντίμετρα που βασίζονται στην κρυπτογραφία, την απόκρυψη, την αλτική μεταπήδηση συχνότητας και ούτω καθεξής. Ωστόσο, αυτά τα μέτρα ασφαλείας είναι αποτελεσματικά μόνο εάν εφαρμόζονται και συντηρούνται σωστά, ενώ, μπροστά σε σοβαρές επιθέσεις, είναι εντελώς μάταια. Έτσι, σε αυτό το σενάριο, οι διαχειριστές των έξυπνων πόλεων πρέπει να διαθέτουν μηχανισμούς επαλήθευσης της λειτουργίας των WSN τους, ώστε να μπορούν να παροτρύνουν, αν χρειαστεί, εξωτερικούς παρόχους να εφαρμόσουν τα απαιτούμενα μέτρα ασφαλείας. Σε αυτό το πλαίσιο, η παρούσα ερευνητική εργασία έχει ως στόχο να συμβάλει στην αύξηση της ασφάλειας των WSN των έξυπνων πόλεων από τη σκοπιά των διαχειριστών έξυπνων πόλεων.

Ως πρώτη συνεισφορά σε αυτή τη διατριβή, προτείναμε μια κεντρική αρχιτεκτονική για τη συλλογή όλων των διαθέσιμων δεδομένων εφαρμογής και κατάστασης δικτύου από τα αστικά WSN, προκειμένου να τα αναλύσουμε και να αποκαλύψουμε επιθέσεις. Με αυτόν τον τρόπο, η αρχιτεκτονική αυτή συμβάλλει προς την κατεύθυνση μιας κεντρικής πλατφόρμας ανίχνευσης εισβολών για έξυπνες πόλεις. Η προτεινόμενη αρχιτεκτονική έχει σχεδιαστεί έτσι ώστε να είναι μη παρεμβατική και διαφανής για τους παρόχους WSN. Ο σχεδιασμός της αρχιτεκτονικής λαμβάνει επίσης υπόψη ότι διαφορετικές έξυπνες πόλεις απαιτούν διαφορετικές υπηρεσίες και ότι διαφορετικοί πάροχοι χρησιμοποιούν διαφορετικές τεχνολογίες. Η αρχιτεκτονική και οι αλγόριθμοι που περιλαμβάνονται σε αυτή τη διατριβή σκοπεύουν να είναι φορητοί σε πολλά μοντέλα έξυπνων πόλεων. Κατά συνέπεια, μελετήσαμε τα χαρακτηριστικά των σημερινών έργων έξυπνων πόλεων και αφαιρέσαμε την προτεινόμενη αρχιτεκτονική από οποιαδήποτε συγκεκριμένη διαμόρφωση έξυπνης πόλης. Ως εκ τούτου, το προτεινόμενο σύστημα είναι εύκολα ενσωματώσιμο και προσαρμόσιμο σε πολλές έξυπνες πόλεις και οι προτεινόμενοι αλγόριθμοι ανίχνευσης μπορούν να εφαρμοστούν σε πολλούς τύπους WSN.

Στην προτεινόμενη αρχιτεκτονική, η ανίχνευση εισβολών αντιμετωπίζεται βασικά από δύο μηχανές ανίχνευσης: μια μηχανή ανίχνευσης βάσει κανόνων και μια μηχανή ανίχνευσης βάσει ανωμαλιών. Η μηχανή ανίχνευσης βάσει κανόνων αναζητά μοτίβα επιθέσεων που έχουν προηγουμένως καταγραφεί σε βάσεις δεδομένων υπογραφών. Αν και αυτός ο μηχανισμός είναι ιδιαίτερα αποτελεσματικός για την ανίχνευση ορισμένων επιθέσεων, έχει το κύριο μειονέκτημα ότι άγνωστες επιθέσεις, για τις οποίες δεν υπάρχουν ακόμη υπογραφές, περνούν απαρατήρητες. Επιπλέον, η δημιουργία κανόνων που περιλαμβάνουν πολλές μεταβλητές καθίσταται υπερβολικά πολύπλοκη και δύσκολα συντηρήσιμη, ενώ ο ορισμός στατικών κατωφλίων για ιδιαίτερα δυναμικά συστήματα είναι μερικές φορές ανέφικτος. Από την άλλη πλευρά, η ανίχνευση με βάση τις ανωμαλίες χρησιμοποιεί συνήθως τεχνικές μηχανικής μάθησης και στατιστικές τεχνικές για την ανακάλυψη δεδομένων που αποκλίνουν από την κανονικότητα. Με αυτόν τον τρόπο, αυτού του είδους οι τεχνικές είναι ικανές να αποκαλύπτουν άγνωστες επιθέσεις. Ωστόσο, δεν είναι πλήρως αξιόπιστες και προκαλούν ένα ορισμένο ποσοστό ψευδών συναγερμών. Ως εκ τούτου, είναι απαραίτητος ο συνδυασμός των δύο τύπων μηχανών ανίχνευσης προκειμένου να αποφευχθεί υπερβολικός αριθμός ψευδώς θετικών αποτελεσμάτων και επίσης να είναι δυνατή η ανίχνευση άγνωστων επιθέσεων. Η ενσωμάτωση ενός συστήματος συσχέτισης το οποίο συγκεντρώνει συναγερμούς που ενεργοποιούνται και από τις δύο μηχανές ανίχνευσης έδειξε σημαντική αύξηση του ποσοστού ανίχνευσης. Επιπλέον, μειώνει τον αριθμό των συναφών συναγερμών που χρειάζονται την προσοχή του διαχειριστή.

Η παρούσα διατριβή έχει δώσει μεγαλύτερη έμφαση στη μηχανή ανίχνευσης ανωμαλιών, επειδή μπορεί να προσφέρει μεγαλύτερη ευελιξία και προσαρμοστικότητα σε διαφορετικά WSN σε σχέση με τη μηχανή ανίχνευσης που βασίζεται σε κανόνες. Αντί να χρησιμοποιεί στατικούς κανόνες, η μηχανή που βασίζεται σε ανωμαλίες χρησιμοποιεί μαθηματικά μοντέλα που ενημερώνονται συνεχώς χρησιμοποιώντας τα δεδομένα που συλλέγονται από τα WSN. Με αυτόν τον τρόπο, η μηχανή αυτή είναι υπεύθυνη για τη δημιουργία των μοντέλων που καθορίζουν την κανονική συμπεριφορά των μεταβλητών και, στη συνέχεια,

χρησιμοποιεί αυτά τα μοντέλα για να επαληθεύσει ότι τα νέα δεδομένα από τα WSNs προέρχονται χωρίς ανωμαλίες. Αυτή η μηχανή πρέπει να είναι ικανή να βρίσκει όρια κανονικότητας για μεμονωμένες μεταβλητές και να εντοπίζει επίσης μη κανονικές καταστάσεις λαμβάνοντας υπόψη τη σχέση μεταξύ πολλών μεταβλητών ταυτόχρονα.

Επιπλέον, η παρούσα διατριβή έδειξε ότι η ανίχνευση εισβολών με τις προτεινόμενες μεθόδους απαιτεί αρκετά βήματα. Για παράδειγμα, τα δεδομένα πρέπει να υποστούν προεπεξεργασία και να συγκεντρωθούν, και τα μοντέλα μηχανικής μάθησης πρέπει να εκπαιδευτούν και, στη συνέχεια, μπορεί να πραγματοποιηθεί ανάλυση ανωμαλιών. Αναλύσαμε την υπολογιστική πολυπλοκότητα των διαφόρων βημάτων και εντοπίσαμε τον υπολογισμό του μοντέλου και την ανίχνευση εισβολής ως τις πιο κρίσιμες υποδιαδικασίες μεταξύ αυτών των βημάτων. Από τη μία πλευρά, ο υπολογισμός του μοντέλου πρέπει να θεωρείται κρίσιμος, επειδή η υπολογιστική πολυπλοκότητα της εκπαίδευσης μοντέλων μηχανικής μάθησης είναι γενικά πολύ υψηλή. Ωστόσο, η ενέργεια αυτή εκτελείται πολύ σπάνια. Από την άλλη πλευρά, η ανίχνευση ανωμαλιών είναι γενικά υπολογιστικά ανέξοδη, αλλά πρέπει να εκτελείται πολύ συχνά. Η παρούσα διατριβή επικυρώνει ότι ο αγωγός που περιλαμβάνει όλα τα απαιτούμενα βήματα είναι βιώσιμος ακόμη και σε σενάρια που αφορούν μεγάλα δεδομένα, χωρίς να χρειάζεται να βασιστεί σε μια αρχιτεκτονική υλικού με εξαιρετικά υψηλούς υπολογιστικούς πόρους.

Επιπλέον, μία από τις κύριες προκλήσεις για τους διαχειριστές των έξυπνων πόλεων δεν είναι μόνο η ανίχνευση ότι μια επίθεση θέτει σε κίνδυνο τα WSN των εξωτερικών παρόχων, αλλά και ο εντοπισμός της συγκεκριμένης επίθεσης. Η παρούσα διατριβή παρείχε κατευθυντήριες γραμμές για τη συλλογή των αποδεικτικών στοιχείων της επίθεσης και στη συνέχεια επισήμανε ένα από τα επτά προτεινόμενα μοντέλα επίθεσης. Με αυτόν τον τρόπο, οι διαχειριστές των έξυπνων πόλεων περιορίζουν τον πιθανό τύπο επίθεσης που επηρεάζει τα δίκτυά τους και μπορούν επίσης να καταλάβουν τις συσκευές που έχουν εκτεθεί και κάποιες στρατηγικές μετριασμού για να περιορίσουν τις βραχυπρόθεσμες και μεσοπρόθεσμες επιβλαβείς συνέπειες των επιθέσεων. Συνοψίζοντας, στην παρούσα

διατριβή προτείναμε ένα σύστημα που συμβάλλει στη βελτίωση της ασφάλειας των WSN των έξυπνων πόλεων με γενικό τρόπο. Οι λύσεις που προτείνονται σε αυτή τη διατριβή είναι κατάλληλες για να προσαρμοστούν και να αναπτυχθούν σε διάφορα μοντέλα έξυπνων πόλεων. Προκειμένου να προσαρμοστούν οι προτεινόμενες λύσεις, οι έξυπνες πόλεις πρέπει να μελετήσουν περαιτέρω τις συνέπειες των επιθέσεων στα συγκεκριμένα σενάριά τους και να επεκτείνουν ή να μειώσουν τις λύσεις που προτείνονται στην παρούσα διατριβή ανάλογα με τις συνθήκες τους. Με αυτόν τον τρόπο, οι προτεινόμενες λύσεις μπορούν να βοηθήσουν τους διαχειριστές των έξυπνων πόλεων να ενισχύσουν την ασφάλεια, να μετριάσουν τις συνέπειες των επιθέσεων, να αυξήσουν την ποιότητα των δεδομένων, να παρακολουθήσουν ότι οι πάροχοι εφαρμόζουν τα απαραίτητα αντίμετρα ασφαλείας στα δίκτυά τους και, γενικά, να βελτιώσουν την ασφάλεια των WSN συνολικά.

Είδαμε ότι η παραδοσιακή ασφάλεια πρέπει να ενισχυθεί προκειμένου να ανιχνεύονται ανωμαλίες στα WSN έξυπνων πόλεων που λειτουργούν από τρίτους. Η μειωμένη πρόσβαση στις συσκευές του δικτύου του παρόχου υπηρεσιών περιορίζει την ορατότητα των WSN στους διαχειριστές των έξυπνων πόλεων και εμποδίζει τη συμβατική ανάλυση ασφάλειας. Για να το ξεπεράσουμε αυτό, προτείναμε μια μη παρεμβατική αρχιτεκτονική που συνδυάζει μια μηχανή ανίχνευσης βασισμένη σε κανόνες και μια μηχανή ανίχνευσης ανωμαλιών. Αυτή η αρχιτεκτονική αναπτύσσει ένα νέο επίπεδο ασφάλειας στους κεντρικούς διακομιστές πάνω από τον διάφορο εξοπλισμό των παρόχων. Έτσι, αποφεύγονται τα προβλήματα που οφείλονται στην ετερογένεια, την περιορισμένη πρόσβαση ή τις δυσκολίες ενημέρωσης ορισμένων συσκευών. Η προτεινόμενη αρχιτεκτονική είναι συμβατή με την ήδη αναπτυγμένη υποδομή, καθώς δεν προσθέτει απαιτήσεις στην υπάρχουσα υποδομή. Επιπλέον, περιγράψαμε έναν αγωγό με τις απαραίτητες υποδιεργασίες για την επεξεργασία δεδομένων WSN και την αποκάλυψη εισβολών χρησιμοποιώντας την προτεινόμενη αρχιτεκτονική με συμβατικές τεχνικές ανίχνευσης ανωμαλιών.

Από τη μία πλευρά, ο μηχανισμός ανίχνευσης με βάση τις ανωμαλίες είναι ικανός να ανιχνεύει άγνωστες επιθέσεις και η φύση της μάθησης χωρίς επίβλεψη του παρέχει ευελιξία σε ένα μεταβαλλόμενο περιβάλλον όπως η έξυπνη πόλη.

Ωστόσο, σε ορισμένες περιπτώσεις, η ανίχνευση με βάση τις ανωμαλίες προκαλεί υπερβολικούς ψευδείς συναγερμούς. Από την άλλη πλευρά, η μηχανή ανίχνευσης βάσει κανόνων δεν έχει τόση ευελιξία όσο η μηχανή ανίχνευσης βάσει ανωμαλιών, αλλά προκαλεί εξαιρετικά αξιόπιστους συναγερμούς. Στην περίπτωση χρήσης, υλοποιήσαμε διάφορους κανόνες που επαληθεύουν την ορθή άφιξη δεδομένων WSN με κανονική συμπεριφορά. Επιπλέον, δημιουργήσαμε κανόνες συσχέτισης που ενώνουν τους συναγερμούς που παράγονται και από τις δύο μηχανές ανίχνευσης. Αυτό αύξησε την αξιοπιστία των συναγερμών με βάση τις ανωμαλίες και επέτρεψε στους διαχειριστές του συστήματος να προειδοποιούνται σε περίπτωση πιο σημαντικών καταστάσεων.

Είδαμε ότι η ανίχνευση εισβολών στην έξυπνη πόλη είναι ένα πολύ σύνθετο πρόβλημα. Μια λύση black-box με έναν αλγόριθμο ανίχνευσης πολλαπλών χρήσεων που καλύπτει τις περισσότερες επιθέσεις για τις περισσότερες διαμορφώσεις δεν είναι εφικτή. Για να αντιμετωπιστεί η ανίχνευση εισβολών σε αυτό το πλαίσιο, πρέπει πρώτα να επιλεγούν οι καταλληλότεροι αλγόριθμοι. Σε αυτό το κεφάλαιο, υποδείξαμε ορισμένους κατάλληλους αλγορίθμους για την εφαρμογή της ανάλυσης ανωμαλιών στο πλαίσιο της έξυπνης πόλης. Με αυτές τις υποδείξεις, η παρούσα διατριβή συμβάλλει στην απλούστευση του έργου του διαχειριστή του συστήματος κατά τη στιγμή της ρύθμισης της μηχανής ανίχνευσης ανωμαλιών.

Βιβλιογραφία-Αναφορές

[1] Milind Naphade et al. “Smarter cities and their innovation challenges”. In: Computer 44.6 (2011), pp. 32–39.

[2] Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp. “Smart cities in Europe”. In: Journal of urban technology 18.2 (2011), pp. 65–82.

[3] Constantin Gurdgiev, S Dirks, and M Keeling. “Smarter cities for smarter growth”. In: IBM Institute for Business Value (2010).

[4] C Manville. Mapping Smart Cities in the EU. European Parliament, Directorate General for Internal Policies, Policy Department–Economic and Scientific Policy. Tech. rep. IP/A/ITRE/ST/2013-02

[5] The Royal Academy of Engineering. Smart infrastructure: the future. Tech. rep. The Royal Academy of Engineering, 2012, pp. 16–17.

[6] Malik Tubaishat et al. “Wireless sensor-based traffic light control”. In: Conf. Consumer Communications and Networking. IEEE. 2008, pp. 702–706.

[7] Ivan Stoianov et al. “PIPENET: A wireless sensor network for pipeline monitoring”. In: Int. Symp. Information Processing in Sensor Networks. IEEE. 2007, pp. 264–273.

[8] N. Perlroth. Smart City Technology May Be Vulnerable to Hackers. http:// bits.blogs.nytimes.com/2015/04/21/smart- city- technology- may- bevulnerable-to-hackers/.

[9] Branden Ghena et al. “Green lights forever: analyzing the security of traffic infrastructure”. In: Workshop on Offensive Technologies. USENIX. 2014.

[10] Jhoana Mutiangpili. Government Sector Outsourcing. Tech. rep. Tholons, 2010, p. 18.

[11] Felipe Gil-Castineira et al. “Experiences inside the ubiquitous Oulu smart city”. In: Computer 44.6 (2011), pp. 48–55.

[12] Yong Woo Lee and Seungwoo Rho. “U-city portal for smart ubiquitous middleware”. In: Int. Conf. Advanced Communication Technology (ICACT). Vol. 1.IEEE. 2010, pp. 609–613.

[13] Min Chen. “Towards smart city: M2M communications with software agent intelligence”. In: Multimedia Tools and Applications 67.1 (2013), pp. 167–178.

[14] Jayavardhana Gubbi et al. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: Future Generation Computer Systems 29.7 (2013), pp. 1645–1660.

[15] Luis Sanchez et al. “SmartSantander: IoT experimentation over a smart city testbed”. In: Computer Networks 61 (2014), pp. 217–238.

[16] Stephen Sorkin. Large-Scale, Unstructured Data Retrieval and Analysis Using Splunk. Tech. rep. Accessed: 2016-08-09. Splunk Inc., 2011, p. 7. url: https://www.splunk.com/web_assets/pdfs/secure/Splunk_and_MapReduce.pdf.

[17] Juan Manuel Lorenzo. AlienVault Installation Guide. Tech. rep. AlienVault LC, 2010, p. 52.

[18] Chris Meering and Paolo Balella. Smart cities and the Internet of Things. Municipal transformation with the HPE Universal IoT Platform. Tech. rep. Hewlett Packard Enterprise Development LP, 2016.

[19] Fabio Leccese, Marco Cagnetti, and Daniele Trinca. “A smart city application: A fully controlled street lighting isle based on Raspberry-Pi card, a ZigBee sensor network and WiMAX”. In: Sensors 14.12 (2014), pp. 24408–24424.

[20] Inc. Ruckus Wireless. Public Access: City of San Jose. Tech. rep. Ruckus Wireless, Inc., 2014.

[21] Mark Anderson. “WiMax for smart grids”. In: IEEE Spectrum 47.7 (2010), pp. 14–14.

[22] Inc. LinkLabs. A comprehensive look at Low Power, Wide Area Networks For Internet of Things Engineers and Decision Makers. Tech. rep. LinkLabs, Inc., 2016.

[23] Libelium Comunicaciones Distribuidas S.L. Plug & Sense! Smart parking. Tech. rep. Libelium Comunicaciones Distribuidas S.L., 2016.

[24] IEEE Computer Society. IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). Tech. rep. IEEE Computer Society, 2011, p. 294.

[25] Lamia Chaari and Lotfi Kamoun. “Wireless sensors networks MAC protocols analysis”. In: arXiv preprint arXiv:1004.4600 (2010).

[26] ZigBee Standards Organization. Zigbee specification. Tech. rep. ZigBee Standards Organization, 2012, p. 594.

[27] Gabriel Montenegro et al. Transmission of IPv6 packets over IEEE 802.15. 4 networks. Tech. rep. The IETF Trust, 2007.

[28] Vinay Kumar and Sudarshan Tiwari. “Routing in IPv6 over low-power wireless personal area networks (6LoWPAN): A survey”. In: Journal of Computer Networks and Communications 2012 (2012).

[29] Charles Perkins, Elizabeth Belding-Royer, and Samir Das. Ad hoc on-demand distance vector (AODV) routing. Tech. rep. The IETF Trust, 2003.

[30] T Kavitha and D Sridharan. “Security vulnerabilities in wireless sensor networks: A survey”. In: Journal of information Assurance and Security 5.1 (2010), pp. 31–44.

[31] Hero Modares, Rosli Salleh, and Amirhossein Moravejosharieh. “Overview of security issues in wireless sensor networks”. In: Int. Conf. Computational Intelligence, Modelling and Simulation. IEEE. 2011, pp. 308–311.

[32] Javier Lopez and Jianying Zhou. “Overview of wireless sensor network security”. In: Wireless sensor network security. IOS Press, incorporated (2008), pp. 1–21.

[33] Corinna Cortes and Vladimir Vapnik. “Support-vector networks”. In: Machine learning 20.3 (1995), pp. 273–297.

[34] Edwin M Knorr and Raymond T Ng. “Finding intensional knowledge of distancebased outliers”. In: VLDB. Vol. 99. 1999, pp. 211–222.

[35] Markus M Breunig et al. “LOF: identifying density-based local outliers”. In: ACM sigmod record. Vol. 29. ACM. 2000, pp. 93–104.

[36] Sergio Marti et al. “Mitigating routing misbehavior in mobile ad hoc networks”. In: Int. Conf. Mobile Computing and Networking. ACM. 2000, pp. 255–265.

[37] Sumit Gupta, Rong Zheng, and Albert MK Cheng. “ANDES: an anomaly detection system for wireless sensor networks”. In: Int. Conf. Mobile Adhoc and Sensor Systems. IEEE. 2007, pp. 1–9.

[38] Nithya Ramanathan et al. “Sympathy for the sensor network debugger”. In: Int. Conf. Embedded Networked Sensor Systems. ACM. 2005, pp. 255–267.

[39] Pedro Domingos. “A few useful things to know about machine learning”. In: Communications of the ACM 55.10 (2012), pp. 78–87.

[40] Sven Zacharias et al. “Identifying sources of interference in RSSI traces of a single IEEE 802.15. 4 channel”. In: Int. Conf. on Wireless and Mobile Communications, Venice, Italy. 2012.

[41] Georgy Shevlyakov et al. “Robust versions of the Tukey boxplot with their application to detection of outliers”. In: 2013 IEEE Int. Conf. on Acoustics, Speech and Signal Processing. IEEE. 2013, pp. 6506–6510.

[42] Chengwei Wang et al. “Statistical techniques for online anomaly detection in data centers”. In: 12th IFIP/IEEE Int. Symp. on Integrated Network Management (IM 2011) and Workshops. IEEE. 2011, pp. 385–392.

[43] Osman Salem et al. “Online anomaly detection in wireless body area networks for reliable healthcare monitoring”. In: IEEE journal of biomedical and health informatics 18.5 (2014), pp. 1541–1551.

[44] Aleksandar Lazarevic et al. “A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection.” In: Int. Conf. Data Mining. SIAM. 2003, pp. 25–36.

[45] F. Pedregosa et al. “Scikit-learn: Machine Learning in Python”. In: Journal of Machine Learning Research 12 (2011), pp. 2825–2830.

[46] Chesner Désir et al. “One class random forests”. In: Pattern Recognition 46.12 (2013), pp. 3490–3506.

[47] Geoffrey E Hinton, Simon Osindero, and Yee-Whye Teh. “A fast learning algorithm for deep belief nets”. In: Neural computation 18.7 (2006), pp. 1527–1554.

[48] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. “ImageNet Classification with Deep Convolutional Neural Networks”. In: Advances in Neural Information Processing Systems 25. Curran Associates, Inc., 2012, pp. 1097–1105.

[49] Richard Socher et al. “Parsing natural scenes and natural language with recursive neural networks”. In: Int. conf. on machine learning (ICML-11). 2011, pp. 129– 136.

[50] Sarah M Erfani et al. “High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning”. In: Pattern Recognition (2016).

[51] Victoria J Hodge and Jim Austin. “A survey of outlier detection methodologies”. In: Artificial Intelligence Review 22.2 (2004), pp. 85–126.

[52] Lior Rokach and Oded Maimon. “Data mining and knowledge discovery handbook”. In: Springer, 2005. Chap. Clustering methods, pp. 321–352.

[53] Fionn Murtagh and Pierre Legendre. “Ward’s Hierarchical Agglomerative Clustering Method: Which Algorithms Implement Ward’s Criterion?” In: Journal of Classification 31.3 (2014), pp. 274–295.

[54] Holling, C.S. Resilience and Stability of Ecological Systems. Annu. Rev. Ecol. Syst. 1973, 4, 1–23. [CrossRef]

[55] Papa, R., Galderisi, A., Vigo Majello, M. C., & Saretta, E. (2015). Smart and Resilient Cities a Systemic Approach for Developing Cross-Sectoral Strategies in the Face of Climate Change. Tema-Journal of Land Use Mobility and Environment, 8(1), 19–49. https://doi.org/10.6092/1970-9870/2883

[56] City of Copenhagen. (2015). Copenhagen Smart City. Retrieved from http://www.almanacproject.eu/downloads/M2M_Workshop_Presentations/Session 4/Mia_Copenhagen_smart_city_2015.pdf

[57] Ghose, T. (2012). Sandy Lives Up to Hype: Predictions Were on Track. Retrieved from https://www.livescience.com/24433-hurricane-sandy-predictions.html

[58] Sulopuisto, O. (2014). How Helsinki Became the Most Successful Open-Data City in the World. Retrieved from https://www.citylab.com/life/2014/04/how-helsinki mashedopendata-regionalism/8994/

[59] Lovett, I. (2013). To Fight Gridlock, Los Angeles Synchronizes Every Red Light. The New York Times. Retrieved from https://www.nytimes.com/2013/04/02/us/to-fightgridlocklos-angeles-synchronizes-every-red-light.html

[60] Phillips-Wren, G., Iyer, L. S., Kulkarni, U., & Ariyachandra, T. (2015). Business Analytics in the Context of Big Data. Commun Assoc Inf Syst, 37(23), 448–472.

[61] Sharma, R., & Mishra, R. (2014). A Review of Evolution of Theories and Models of Technology Adoption. Indore Management Journal, 6(2), 17–29.

[62] Davenport, T. (2017). How Analytics Has Changed in the Last 10 Years (and How It's Stayed the Same). Harvard Business Review. Retrieved from https://hbr.org/2017/06/howanalytics-has-changed-in-the-last-10-years-and-how-itsstayed-the-same

[63] Hameed, M. A., Counsell, S., & Swift, S. (2012). A conceptual model for the process of IT innovation adoption in organizations. Journal of Engineering and Technology Management - JET-M, 29(3), 358–390. https://doi.org/10.1016/j.jengtecman.2012.03.007

[64] G. Robin, "Cyber Warfare: Implications for Non-international Armed Conflicts", vol. 89, no. 627, 2013.

[65] A. P. Zachary, "Cyber Neutrality: A Textual Analysis of Traditional Jus in. Bello Neutrality Rules through a Purpose - Based Lens", The Air Force Law, vol. 69, 2014.

[66] N. Provos, M. Rajab and P. Mavrommatis, "Cybercrime 2.0", Communications of the ACM, vol. 52, no. 4, pp. 42-47, 2009. Available: 10.1145/1498765.1498782.

[67] "Governance framework for European standardisation Aligning Policy, Industry and Research V1.0 DECEMBER", Enisa.europa.eu, 2015.

[68] T. Fu, A. Abbasi and H. Chen, "A focused crawler for Dark Web forums", Journal of the American Society for Information Science and Technology, p. n/an/a, 2010. Available: 10.1002/asi.21323.

[69] M. Chertoff and T. Simon, The impact of the dark web on internet goverannce and cyber security. 2015

[70] K. Al-Rowaily, M. Abulaish, N. Al-Hasan Haldar and M. Al-Rubaian, "BiSAL – A bilingual sentiment analysis lexicon to analyze Dark Web forums for cyber security", Digital Investigation, vol. 14, pp. 53-62, 2015. Available: 10.1016/j.diin.2015.07.006

[71] "Οι 5 καταστροφικοτέρες κυβερνο-απειλές στην Ευρώπη το 2020 | IT SECURITY PRO: Περιοδικό για το Business IT και την ασφάλεια πληροφοριών!", IT SECURITY PRO: Περιοδικό για το Business IT και την ασφάλεια πληροφοριών!, 2021.

[72] V. Cerdeira, "Κυβερνοασφάλεια: Το Συμβούλιο εγκρίνει συμπεράσματα για τη στρατηγική της ΕΕ", Consilium.europa.eu, 2021.

[73] Cyber security for Smart Cities: An architecture model for public transport