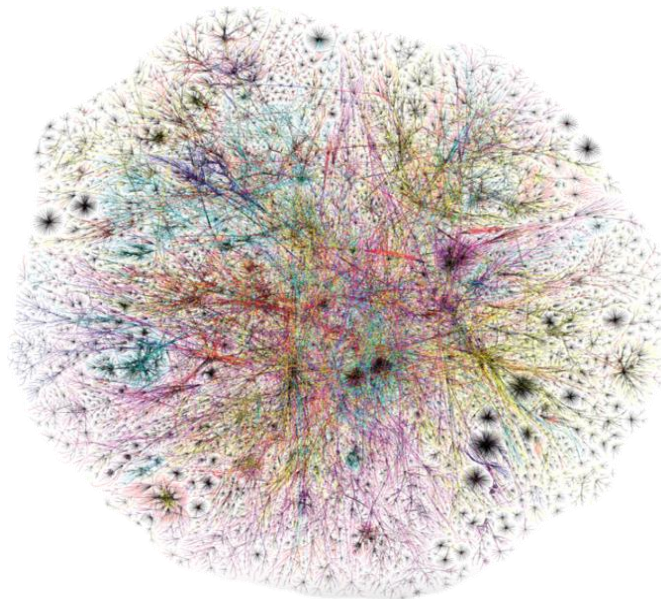


ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Μελέτη της Ασφάλειας Πρωτοκόλλων για Ασύρματα
Δίκτυα Αισθητήρων»



Της φοιτήτριας
Ανδριτσούδη Δέσποινα Αμαλία
Αρ. Μητρώου: 185357

Επιβλέπων Καθηγητής
Δημήτρης Αμανατιάδης

Σεπτέμβριος 2026

Τίτλος Π.Ε. Μελέτη της ασφάλειας πρωτοκόλλων για ασύρματα δίκτυα αισθητήρων
Κωδικός Π.Ε. 25140

Ονοματεπώνυμο φοιτητή/τών : Ανδριτσούδη Δέσποινα Αμαλία

Ονοματεπώνυμο εισηγητή : Δημήτρης Αμανατιάδης

Ημερομηνία ανάληψης Π.Ε. 06-03-2025

Ημερομηνία περάτωσης Π.Ε. ...

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία της φοιτήτριας Ανδριτσούδη Δέσποινα Αμαλία που την εκπόνησε/αν. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσί-ασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιο-κτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώ-ληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετά-φραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προη-γούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η παρούσα πτυχιακή εργασία εκπονήθηκε στο πλαίσιο των προπτυχιακών σπουδών στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων και πραγματεύεται το κρίσιμο ζήτημα της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων (WSNs - Wireless Sensor Networks). Σε μια εποχή όπου το Internet of Things (IoT) μεταμορφώνει τις σύγχρονες κοινωνίες σε «Εξυπνες Πόλεις», η ανάγκη για αξιόπιστη και ασφαλή μεταφορά δεδομένων αποτελεί μια από τις σημαντικότερες προκλήσεις για τη διεθνή επιστημονική κοινότητα.

Το έναυσμα για την ενασχόληση με το συγκεκριμένο αντικείμενο αποτέλεσε η διαπίστωση ότι οι παραδοσιακοί μηχανισμοί ασφάλειας δεν επαρκούν για να καλύψουν τις ιδιαίτερες απαιτήσεις των ασύρματων δικτύων αισθητήρων, κυρίως εξαιτίας των περιορισμένων ενεργειακών και υπολογιστικών τους πόρων. Μέσα από αυτή τη διαπίστωση, η παρούσα μελέτη επιδιώκει να διερευνήσει τη συμβολή σύγχρονων τεχνολογιών, όπως η Μηχανική Μάθηση (Machine Learning) και το Fog Computing, στην ανάπτυξη αποδοτικότερων λύσεων ασφάλειας. Το όφελος της προσέγγισης αυτής έγκειται στην ανάδειξη μεθόδων που επιτυγχάνουν ισορροπία μεταξύ υψηλού επιπέδου προστασίας και ενεργειακής αποδοτικότητας, συμβάλλοντας έτσι στη βιώσιμη και αξιόπιστη λειτουργία των δικτύων αισθητήρων.

Η δομή της εργασίας ακολουθεί μια λογική και κλιμακωτή πορεία. Ξεκινά με την ανάλυση της αρχιτεκτονικής των WSNs και την κατηγοριοποίηση των πιθανών απειλών. Στη συνέχεια, εμβαθύνει στις σύγχρονες μεθόδους ανίχνευσης εισβολών και καταλήγει σε μια λεπτομερή συγκριτική αξιολόγηση αλγορίθμων, όπου τεκμηριώνεται η αποτελεσματικότητα των προτεινόμενων λύσεων βάσει ποσοτικών δεδομένων.

Τέλος, ευελπιστώ ότι η παρούσα μελέτη θα αποτελέσει ένα χρήσιμο έναυσμα και βοήθημα για περαιτέρω έρευνα στον τομέα της κυβερνοασφάλειας των ασύρματων δικτύων αισθητήρων.

Περίληψη

Αντικείμενο της παρούσας πτυχιακής εργασίας είναι η μελέτη και η αξιολόγηση μηχανισμών ασφάλειας σε Ασύρματα Δίκτυα Αισθητήρων (WSNs - Wireless Sensor Networks), με έμφαση στην ανίχνευση εισβολών μέσω τεχνικών Μηχανικής Μάθησης. Τα δίκτυα αυτά αποτελούν βασικό στοιχείο σύγχρονων υποδομών, όπως οι «Εξυπνες Πόλεις», ωστόσο η ευάλωτη φύση τους και οι περιορισμένοι πόροι των κόμβων δημιουργούν σημαντικές προκλήσεις ως προς την ασφάλειά τους.

Η μεθοδολογία της εργασίας βασίζεται στην ανάλυση της λειτουργίας ενός Συστήματος Ανίχνευσης Εισβολών (IDS - Intrusion Detection System), από τη συλλογή και επεξεργασία δεδομένων έως την εφαρμογή τεχνικών ταξινόμησης μέσω εποπτευόμενης μάθησης. Στο πλαίσιο αυτό, εξετάζονται και συγκρίνονται διαφορετικοί αλγόριθμοι μηχανικής μάθησης, καθώς και τεχνικές επιλογής χαρακτηριστικών, με στόχο τη βελτίωση της αποδοτικότητας και τη μείωση της υπολογιστικής πολυπλοκότητας.

Τα αποτελέσματα της μελέτης αναδεικνύουν τη δυνατότητα των σύγχρονων μεθόδων να ενισχύσουν σημαντικά την ασφάλεια των δικτύων, διατηρώντας παράλληλα την αποδοτική αξιοποίηση των περιορισμένων πόρων τους. Τέλος, επισημαίνεται η ανάγκη υιοθέτησης υβριδικών προσεγγίσεων που συνδυάζουν τεχνικές ανίχνευσης και αποδοτικούς μηχανισμούς προστασίας, με στόχο τη διασφάλιση της αξιοπιστίας και της βιωσιμότητας των μελλοντικών ασύρματων δικτύων.

Η μελέτη επεκτείνεται επίσης στις εξελίξεις της περιόδου 2024-2026, καλύπτοντας την τυποποίηση της ελαφριάς κρυπτογραφίας Ascon, τη μετάβαση προς τη μετακβαντική κρυπτογραφία, τις κατανεμημένες προσεγγίσεις ομόσπονδης μάθησης και TinyML, την αντιπαραθετική ευπάθεια των ίδιων των συστημάτων ανίχνευσης, καθώς και το νέο ευρωπαϊκό κανονιστικό πλαίσιο. Παράλληλα ασκείται μεθοδολογική κριτική στα καθιερωμένα σύνολα δεδομένων αξιολόγησης και στους κινδύνους υπερεκτίμησης της απόδοσης.

Λέξεις-κλειδιά: Ασύρματα Δίκτυα Αισθητήρων (WSNs), Μηχανική Μάθηση, Ανίχνευση Εισβολών (IDS), Random Forest, Ενεργειακή Αποδοτικότητα, Sybil Attack.

«A STUDY OF SECURITY PROTOCOLS FOR WIRELESS SENSOR NETWORK»

«Andritsoudi Despoina Amalia»

Abstract

The subject of this undergraduate thesis is the study and evaluation of security mechanisms in Wireless Sensor Networks (WSNs), with an emphasis on intrusion detection through Machine Learning techniques. These networks constitute a fundamental component of modern infrastructures, such as Smart Cities; however, their vulnerable nature and the limited resources of sensor nodes pose significant security challenges.

The methodology of this study is based on the analysis of the operation of an Intrusion Detection System (IDS), from data collection and processing to the application of classification techniques using supervised learning. Within this framework, different machine learning algorithms and feature selection techniques are examined and compared, aiming to improve efficiency and reduce computational complexity.

The results of the study highlight the potential of modern approaches to significantly enhance network security while maintaining efficient use of limited resources. Finally, the need for hybrid approaches that combine intelligent detection techniques with efficient protection mechanisms is emphasized, in order to ensure the reliability and sustainability of future wireless networks.

The study is further extended to developments of the 2024-2026 period, covering the standardisation of Ascon lightweight cryptography, the transition towards post-quantum cryptography, distributed approaches based on federated learning and TinyML, the adversarial vulnerability of the detection systems themselves, and the new European regulatory framework. A methodological critique of the established evaluation datasets and of the risks of performance overestimation is also provided.

Keywords: Wireless Sensor Networks (WSNs), Machine Learning, Intrusion Detection System (IDS), Random Forest, Energy Efficiency, Sybil Attack.

Ευχαριστίες

Ολοκληρώνοντας αυτή την προσπάθεια, θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα καθηγητή για την πολύτιμη καθοδήγηση, την επιστημονική υποστήριξη και τις παρατηρήσεις του καθ' όλη τη διάρκεια της εκπόνησης. Επίσης, ευχαριστώ θερμά την οικογένεια και τους οικείους μου για την αμέριστη συμπαράσταση, την υπομονή και την ενθάρρυνση που μου παρείχαν.

Περιεχόμενα

Πρόλογος.....	iii
Περίληψη.....	iv
Abstract	v
Ευχαριστίες	vi
Περιεχόμενα	vii
Κατάλογος Σχημάτων	x
Κατάλογος Εικόνων	x
Κατάλογος Πινάκων.....	x
Συνοτομογραφίες.....	xi
Κεφάλαιο 1ο: Εισαγωγή στα Ασύρματα Δίκτυα Αισθητήρων (WSNs).....	1
1.1 Εισαγωγή.....	1
1.2 Ιστορική Αναδρομή: Από τα Ενσύρματα στα Ασύρματα Δίκτυα.....	1
1.3 Ορισμός και Βασικά Χαρακτηριστικά των WSNs.....	3
1.3.1 Ανατομία του Κόμβου Αισθητήρα.....	3
1.3.2 Δομή Δικτύου και Σταθμός Βάσης (Sink Node)	4
1.3.3 Η Στοιίβα Πρωτοκόλλων και Τεχνικά Χαρακτηριστικά.....	5
1.3.4 Σύγχρονα Πρότυπα Συνδεσιμότητας: IEEE 802.15.4e/TSCH, 6LoWPAN/RPL και LPWAN 6	
1.4 Τοπολογίες Δικτύων (Star, Mesh, Hybrid).....	8
1.5 Τομείς Εφαρμογών.....	9
1.6 Περιορισμοί και Προκλήσεις (Ενέργεια, Υπολογιστική Ισχύς, Μνήμη)	12
1.7 Επίλογος	13
Κεφάλαιο 2ο: Απειλές και Τρωτά Σημεία στα WSNs.....	14
2.1 Εισαγωγή.....	14
2.2 Βασικές Αρχές Ασφάλειας.....	14
2.3 Ταξινόμηση Επιθέσεων ανά Επίπεδο Στοιίβας Πρωτοκόλλων	16
2.3.1 Επιθέσεις Φυσικού Επιπέδου	17
2.3.2 Επιθέσεις Επιπέδου Συνδέσμου	18
2.3.3 Επιθέσεις Επιπέδου Δικτύου (Routing Attacks)	19
2.3.4 Επιθέσεις στο Πρωτόκολλο Δρομολόγησης RPL	22

2.3.5	Επιθέσεις Επιπέδου Μεταφοράς	23
2.3.6	Επιθέσεις Εξάντλησης Ενέργειας και Άρνησης Ύπνου	24
2.3.7	Επιθέσεις Πλευρικού Καναλιού και Παραβίαση Υλικού.....	25
2.4	Ιδιαιτερότητες Ασφάλειας σε IoT-based WSNs.....	25
2.4.1	Περιορισμοί Πόρων και Ανάγκη για Lightweight Λύσεις	26
2.4.2	Κλιμακωσιμότητα, Ετερογένεια και Κινητικότητα.....	26
2.4.3	Κρίσιμες Εφαρμογές	27
2.5	Μοντελοποίηση Απειλών και Προφίλ Επιτιθέμενου	27
2.6	Η Κβαντική Απειλή και το Μοντέλο «Harvest Now, Decrypt Later»	28
2.7	Επίλογος.....	29
Κεφάλαιο 3ο:	Μηχανισμοί και Πρωτόκολλα Ασφαλείας	30
3.1	Εισαγωγή.....	30
3.2	Κρυπτογραφικές Τεχνικές για Περιορισμένους Πόρους.....	30
3.2.1	Συμμετρική Κρυπτογραφία	30
3.2.2	Το Πρότυπο Ascon και η Τυποποίηση της Ελαφριάς Κρυπτογραφίας.....	32
3.2.3	Ασύμμετρη Κρυπτογραφία.....	32
3.2.4	Μετακβαντική Κρυπτογραφία σε Δίκτυα Περιορισμένων Πόρων	34
3.3	Διαχείριση Κλειδιών και Μοντέλα Εμπιστοσύνης.....	35
3.4	Ανάλυση Πρωτοκόλλων Ασφαλείας.....	37
3.4.1	Πρωτόκολλο SPINS	37
3.4.2	Πρωτόκολλο TinySec και LEAP+	38
3.4.3	Το Πρότυπο ZigBee και η Ασφάλειά του	39
3.4.4	Σύγκριση Πρωτοκόλλων	41
3.5	Ασφαλής Συνάθροιση Δεδομένων και Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης.....	42
3.6	Συστήματα Ανίχνευσης Εισβολών	42
3.7	Επίλογος.....	47
Κεφάλαιο 4ο:	Σύγχρονες Τεχνολογίες στην Ασφάλεια των WSNs	48
4.1	Εισαγωγή.....	48
4.2	Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στην Ανίχνευση Επιθέσεων.....	48
4.3	Ομόσπονδη Μάθηση για Κατανεμημένη Ανίχνευση Εισβολών	50
4.4	TinyML: Ανίχνευση Εισβολών στον Ίδιο τον Κόμβο	51
4.5	Αρχιτεκτονικές Βαθιάς Μάθησης με Μηχανισμούς Προσοχής.....	52
4.6	Επεξηγήσιμη Τεχνητή Νοημοσύνη στα Συστήματα Ανίχνευσης	52
4.7	Αντιπαραθετική Μηχανική Μάθηση: Όταν το Σύστημα Ανίχνευσης Γίνεται Στόχος.....	53
4.8	Μεγάλα Γλωσσικά Μοντέλα στην Ανάλυση Ασφάλειας.....	53

4.9	Εφαρμογή του Blockchain για Αποκεντρωμένη Ασφάλεια στα WSNs.....	54
4.9.1	Σύγχρονες Υβριδικές Αρχιτεκτονικές Blockchain και Μηχανικής Μάθησης	56
4.10	Edge & Fog Computing	57
4.11	Προστασία Ιδιωτικότητας (Privacy-preserving Techniques)	59
4.12	Δυναμική Αξιολόγηση Εμπιστοσύνης και Ενισχυτική Μάθηση στη Δρομολόγηση	61
4.13	Επίλογος	62
Κεφάλαιο 5ο:	Μελέτη και Συγκριτική Αξιολόγηση.....	63
5.1	Εισαγωγή	63
5.2	Εισαγωγή στη Μεθοδολογία Αξιολόγησης	63
5.2.1	Μοντελοποίηση Επιθέσεων και Πλαίσιο Ελέγχου.....	63
5.2.2	Το Σύνολο Δεδομένων NSL-KDD και WSN-DS	65
5.2.3	Κριτική Αποτίμηση των Συνόλων Δεδομένων και Μεθοδολογικοί Κίνδυνοι	66
5.2.4	Προεπεξεργασία και Επιλογή Χαρακτηριστικών (Feature Selection)	67
5.2.5	Ροή Εργασίας του Συστήματος (System Workflow).....	68
5.3	Συγκριτική Ανάλυση Αλγορίθμων Μηχανικής Μάθησης.....	69
5.3.1	Ανάλυση Αποτελεσμάτων Ακρίβειας	69
5.3.2	Σχολιασμός και Συμπεράσματα Συγκρίσεων	70
5.4	Ανάλυση Μετρικών Απόδοσης	72
5.5	Αξιολόγηση με Βάση την Ενεργειακή Κατανάλωση vs Επίπεδο Ασφάλειας.....	73
5.5.1	Ποσοτικοποίηση του Ενεργειακού Κόστους με Βάση τη Σύγχρονη Βιβλιογραφία	74
5.6	Πλεονεκτήματα και Μειονεκτήματα Υπαρχουσών Λύσεων	75
5.7	Μελέτη Ασφάλειας WSNs για Εφαρμογές Ελέγχου Κυκλοφορίας και Συλλογής Ηλιακής Ενέργειας.....	76
5.8	Συγκριτική Επισκόπηση Σύγχρονων Προσεγγίσεων (2024-2026).....	78
5.9	Κανονιστικό Πλαίσιο και Απαιτήσεις Συμμόρφωσης.....	79
5.10	Μελλοντικές Τάσεις και Ανοιχτά Ερευνητικά Προβλήματα	80
5.11	Επίλογος	81
Κεφάλαιο 6ο:	Συμπεράσματα και Προτάσεις βελτίωσης.....	82
6.1	Συμπεράσματα.....	82
6.2	Προτάσεις βελτίωσης	84
BIBΛΙΟΓΡΑΦΙΑ.....		87

Κατάλογος Σχημάτων

Σχήμα 1 Ιστορική Αναδρομή	2
---------------------------------	---

Κατάλογος Εικόνων

Εικόνα 1 WSNs Communication Model	4
Εικόνα 2 Wireless Sensor Network	5
Εικόνα 3 Communication Protocol Stack of WSNs	6
Εικόνα 4 UAV-WSN Monitoring System in Agriculture Sector	10
Εικόνα 5 Smart Grid Architecture	11
Εικόνα 6 Η Τριάδα CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) στο πλαίσιο των WSNs	14
Εικόνα 7 Απεικόνιση επίθεσης παρεμβολής (Jamming) όπου ο εισβολέας διακόπτει την επικοινωνία μεταξύ των αισθητήρων και του σταθμού βάσης.....	18
Εικόνα 8 Μοντέλο συστήματος με εκδήλωση επίθεσης παρεμβολής (Jamming) σε ένα ασύρματο Ad-Hoc δίκτυο.....	20
Εικόνα 9 Incorporating Internet with WSNs.....	26
Εικόνα 10 Γενικό μπλοκ διάγραμμα ενός IDS.....	43
Εικόνα 11 Ροή εργασίας Εποπτευόμενης Μάθησης (Supervised Learning).....	44
Εικόνα 12 Framework of the security testing approach for WSNs protocols	54
Εικόνα 13 System Workflow	68

Κατάλογος Πινάκων

Πίνακας 1 Συγκριτικά χαρακτηριστικά υλικού μεταξύ κόμβου αισθητήρα και πύλης δικτύου.....	6
Πίνακας 2 Συγκριτική αξιολόγηση ακρίβειας αλγορίθμων Μηχανικής Μάθησης.....	49
Πίνακας 3 Confusion Matrix.....	61
Πίνακας 4 Μετρικές απόδοσης του μοντέλου IDS.....	61
Πίνακας 5 Συγκριτική επισκόπηση σύγχρονων προσεγγίσεων ασφάλειας WSNs (2024-2026).....	79

Συντομογραφίες

ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BiLSTM	Bidirectional Long Short-Term Memory
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CIA	Confidentiality, Integrity, Availability
DIS	DODAG Information Solicitation
DODAG	Destination-Oriented Directed Acyclic Graph
DoS	Denial of Service
DPA	Differential Power Analysis
ECC	Elliptic Curve Cryptography
FL	Federated Learning
HNDL	Harvest Now, Decrypt Later
IDS	Intrusion Detection System
IoT	Internet of Things
LEACH	Low-Energy Adaptive Clustering Hierarchy
LLMs	Large Language Models
LPWAN	Low-Power Wide-Area Network
MAC	Medium Access Control
ML	Machine Learning
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
MRMR	Minimum Redundancy Maximum Relevance

NSL-KDD	Network Security Laboratory – Knowledge Discovery and Data mining
PDR	Packet Delivery Ratio
PQC	Post-Quantum Cryptography
PUF	Physical Unclonable Function
RPL	Routing Protocol for Low-Power and Lossy Networks
RSSI	Received Signal Strength Indication
SHAP	SHapley Additive exPlanations
SNEP	Sensor Network Encryption Protocol
SVM	Support Vector Machine
TC	Trust Center
TSCH	Time-Slotted Channel Hopping
UAV	Unmanned Aerial Vehicle
WSNs	Wireless Sensor Networks
XAI	Explainable Artificial Intelligence
ZTA	Zero Trust Architecture
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks

Κεφάλαιο 1ο: Εισαγωγή στα Ασύρματα Δίκτυα Αισθητήρων (WSNs)

1.1 Εισαγωγή

Τα Ασύρματα Δίκτυα Αισθητήρων (WSNs - Wireless Sensor Networks) αποτελούν μία από τις πιο δυναμικές τεχνολογίες του 21ου αιώνα, λειτουργώντας ως γέφυρα μεταξύ του φυσικού και του ψηφιακού κόσμου και ως θεμελιώδες συστατικό του Διαδικτύου των Πραγμάτων. Ένα τυπικό δίκτυο αποτελείται από δεκάδες έως χιλιάδες μικροσκοπικούς, χαμηλού κόστους κόμβους αισθητήρων, διασκορπισμένους σε μια περιοχή ενδιαφέροντος, οι οποίοι συνεργάζονται για να παρακολουθούν φυσικά φαινόμενα όπως η θερμοκρασία, η υγρασία ή η κίνηση. Σε αντίθεση με τα παραδοσιακά ασύρματα δίκτυα, η φιλοσοφία τους δεν βασίζεται απλώς στην επικοινωνία, αλλά στη συνεργατική επεξεργασία των πληροφοριών.

1.2 Ιστορική Αναδρομή: Από τα Ενσύρματα στα Ασύρματα Δίκτυα

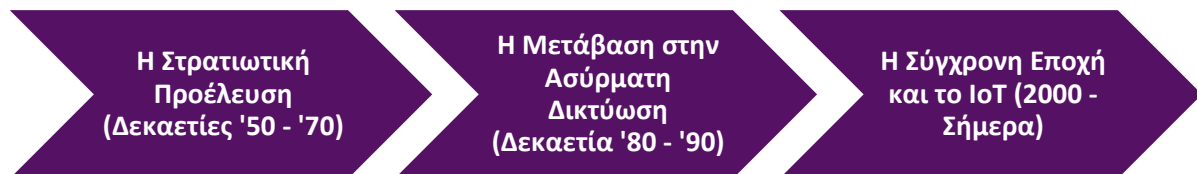
Πριν την ανάλυση της ιστορικής εξέλιξης, είναι απαραίτητο να αποσαφηνιστούν οι βασικές έννοιες που συνθέτουν την τεχνολογία των δικτύων αισθητήρων. Τα δίκτυα αποτελούνται από ένα σύνολο διασυνδεδεμένων οντοτήτων (κόμβων) που ανταλλάσσουν πληροφορίες μέσω ενός κοινού μέσου επικοινωνίας. Στην περίπτωση των WSNs, οι κόμβοι αυτοί είναι οι αισθητήρες, μικροσκοπικές συσκευές που έχουν την ικανότητα να ανιχνεύουν φυσικά φαινόμενα (θερμοκρασία, κίνηση, πίεση) και να τα μετατρέπουν σε ψηφιακά δεδομένα.

Η μετάβαση από τα ενσύρματα στα ασύρματα δίκτυα αποτέλεσε ορόσημο. Τα ενσύρματα δίκτυα χρησιμοποιούν φυσικά μέσα (καλώδια χαλκού, οπτικές ίνες) για τη μεταφορά δεδομένων, προσφέροντας υψηλή ταχύτητα και ασφάλεια, αλλά με μεγάλο κόστος εγκατάστασης και μηδενική ευελιξία σε δύσβατα περιβάλλοντα. Αντίθετα, τα ασύρματα δίκτυα χρησιμοποιούν ηλεκτρομαγνητικά κύματα, επιτρέποντας την ανάπτυξη συστημάτων σε περιοχές όπου η καλωδίωση είναι πρακτικά αδύνατη (όπως ηφαίστεια, εμπόλεμες ζώνες ή βαθιές δασικές εκτάσεις) [1], [2].

Η ιστορική διαδρομή της τεχνολογίας αυτής μπορεί να χωριστεί σε τρεις κύριες περιόδους:

- Δεκαετίες '50 - '70 (Η Στρατιωτική Προέλευση): Οι ρίζες των WSNs εντοπίζονται στην περίοδο του Ψυχρού Πολέμου. Η πρώτη ουσιαστική εφαρμογή που προσομοιάζει στη φιλοσοφία των WSNs ήταν το σύστημα SOSUS (Sound Surveillance System), το οποίο αναπτύχθηκε από τις ΗΠΑ τη δεκαετία του 1950 για την ανίχνευση σοβιετικών υποβρυχίων μέσω υποβρυχίων ακουστικών αισθητήρων. Αν και ενσύρματο στην αρχή, έθεσε τις βάσεις για τη συνεργατική επεξεργασία δεδομένων από πολλαπλά σημεία εισόδου [1].
- Δεκαετία '80 - '90 Η πραγματική επανάσταση ξεκίνησε με το πρόγραμμα DSN (Distributed Sensor Networks) της DARPA (Defense Advanced Research Projects Agency). Η DARPA είναι ο κεντρικός ερευνητικός οργανισμός του Υπουργείου Άμυνας των Ηνωμένων Πολιτειών, υπεύθυνος για την ανάπτυξη αναδυόμενων τεχνολογιών που προορίζονται για στρατιωτική χρήση, αλλά συχνά καταλήγουν σε ευρεία εμπορική εφαρμογή (όπως το διαδίκτυο). Το πρόγραμμα αυτό ξεκίνησε το 1980 με στόχο την ανάπτυξη κατακεντρωμένων δικτύων αυτόνομων κόμβων που συνεργάζονται χωρίς σταθερή υποδομή [3].

- 2000 - Σήμερα (Η Σύγχρονη Εποχή και το IoT - Internet of Things): Με την αυγή του 21ου αιώνα, τα WSNs διείσδυσαν στον εμπορικό τομέα. Η δημιουργία πρωτοκόλλων χαμηλής κατανάλωσης, όπως το ZigBee (IEEE 802.15.4) και το LEACH (Low-Energy Adaptive Clustering Hierarchy), επέτρεψε στα δίκτυα να λειτουργούν για μεγάλα διαστήματα με απλές μπαταρίες [4], [5]. Σήμερα, τα WSNs ενσωματώνονται στο IoT, αποτελώντας ένα παγκόσμιο πλέγμα δισεκατομμυρίων συσκευών που επιτρέπουν την έξυπνη διαχείριση πόρων σε "Έξυπνες Πόλεις" (Smart Cities) και "Έξυπνα Δίκτυα Ενέργειας" (Smart Grids) [6], [7].



Σχήμα 1 Ιστορική Αναδρομή [1], [3]

Η εξέλιξη των ασύρματων δικτύων αισθητήρων δεν υπήρξε γραμμική, αλλά καθορίστηκε από τη σύγκλιση τριών ανεξάρτητων τεχνολογικών ρευμάτων: της μικροηλεκτρονικής, των ασύρματων επικοινωνιών χαμηλής ισχύος και των ενσωματωμένων λειτουργικών συστημάτων. Η ραγδαία σμίκρυνση των ολοκληρωμένων κυκλωμάτων, ενόψει με τον νόμο του Moore, επέτρεψε την κατασκευή μικροελεγκτών ικανών να εκτελούν αλγορίθμους δρομολόγησης με κατανάλωση ισχύος της τάξης των μερικών milliwatt. Παράλληλα, η ανάπτυξη τεχνολογιών διαμόρφωσης φάσματος διασποράς (spread spectrum) έκανε εφικτή την αξιόπιστη ασύρματη μετάδοση σε θορυβώδη περιβάλλοντα χωρίς υψηλή κατανάλωση. Η σύζευξη αυτών των παραγόντων μετέτρεψε τα WSNs από ένα ακριβό στρατιωτικό εργαλείο σε μια προσιτή και ευρέως διαθέσιμη τεχνολογία, ικανή να υποστηρίξει εφαρμογές μαζικής κλίμακας [1], [2].

Ένα κομβικό ορόσημο στην ακαδημαϊκή και εμπορική καθιέρωση των WSNs υπήρξε η ανάπτυξη της πλατφόρμας «Smart Dust» στο Πανεπιστήμιο του Μπέρκλεϊ στα τέλη της δεκαετίας του 1990. Το όραμα της συγκεκριμένης ερευνητικής προσπάθειας ήταν η δημιουργία αυτόνομων κόμβων με μέγεθος κόκκου σκόνης, οι οποίοι θα μπορούσαν να διασκορπιστούν στο περιβάλλον και να σχηματίσουν αυθόρμητα ένα δίκτυο παρακολούθησης. Παρότι ο στόχος του πραγματικά μικροσκοπικού μεγέθους δεν επιτεύχθηκε πλήρως, η προσπάθεια αυτή γέννησε το λειτουργικό σύστημα TinyOS και τη γλώσσα προγραμματισμού nesC, τα οποία αποτέλεσαν για χρόνια το de facto πρότυπο ανάπτυξης εφαρμογών για κόμβους αισθητήρων. Η συνεισφορά αυτή ήταν καθοριστική, καθώς για πρώτη φορά προσέφερε ένα τυποποιημένο περιβάλλον ανάπτυξης πάνω στο οποίο η ερευνητική κοινότητα μπορούσε να οικοδομήσει και να συγκρίνει πρωτόκολλα [3], [4].

Η τυποποίηση των φυσικών και των επιπέδων συνδέσμου αποτέλεσε την επόμενη κρίσιμη φάση ωρίμανσης. Η υιοθέτηση του προτύπου IEEE 802.15.4 το 2003 παρείχε ένα κοινό θεμέλιο για την ασύρματη επικοινωνία χαμηλού ρυθμού δεδομένων και χαμηλής κατανάλωσης, πάνω στο οποίο οικοδομήθηκαν πρωτόκολλα ανώτερου επιπέδου όπως το ZigBee, το 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) και αργότερα το Thread. Η ύπαρξη ενός κοινού προτύπου είχε διττή σημασία: αφενός εξασφάλισε τη διαλειτουργικότητα μεταξύ συσκευών διαφορετικών κατασκευαστών και αφετέρου επέτρεψε την οικονομία κλίμακας που μείωσε δραστικά το κόστος ανά κόμβο. Ωστόσο, η ίδια τυποποίηση εισήγαγε και νέες προκλήσεις ασφάλειας, καθώς η ομοιογένεια του υλικού και του λογισμικού κατέστησε τις επιθέσεις πιο εύκολα μεταφέρσιμες από το ένα σύστημα στο άλλο. Η

παρατήρηση αυτή είναι θεμελιώδης για την κατανόηση του γιατί η ασφάλεια αναδείχθηκε σε κεντρικό ζήτημα της σύγχρονης έρευνας στα WSNs [4], [6].

1.3 Ορισμός και Βασικά Χαρακτηριστικά των WSNs

Ως Ασύρματο Δίκτυο Αισθητήρων (WSNs) ορίζεται ένα δίκτυο που αποτελείται από έναν μεγάλο αριθμό αυτόνομων συσκευών, οι οποίες είναι καταναμεμημένες στον χώρο και χρησιμοποιούν αισθητήρες για την παρακολούθηση φυσικών ή περιβαλλοντικών συνθηκών. Τα βασικά χαρακτηριστικά των WSNs είναι:

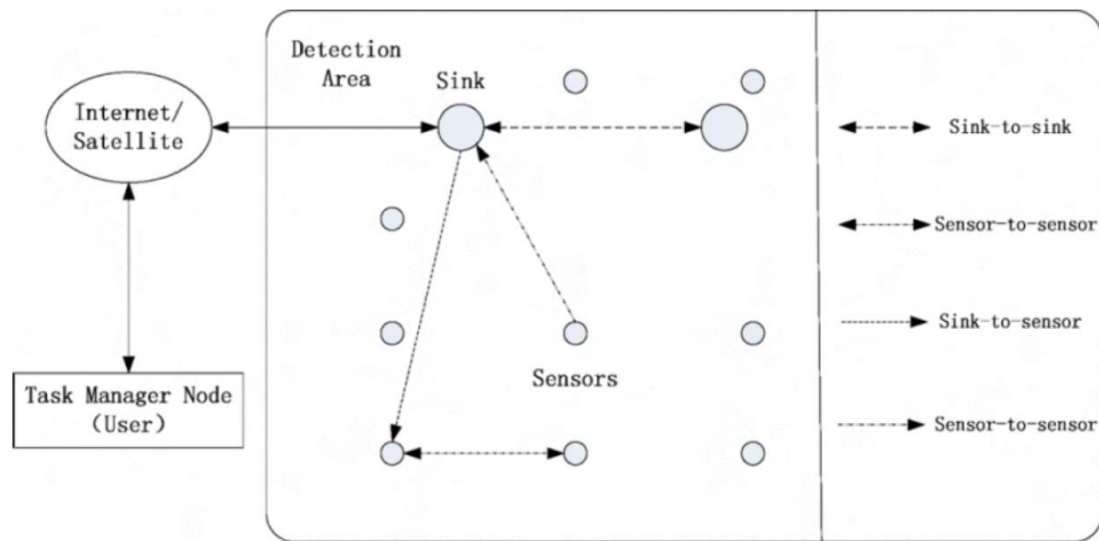
1. Αυτόνομη λειτουργία και αυτο-οργάνωση: Οι κόμβοι μπορούν να λειτουργούν χωρίς κεντρικό έλεγχο και να προσαρμόζονται σε αλλαγές στο δίκτυο.
2. Συνεργασία και καταναμεμημένη επεξεργασία: Οι κόμβοι ανταλλάσσουν πληροφορίες και επεξεργάζονται δεδομένα συλλογικά για καλύτερη ακρίβεια και αξιοπιστία.
3. Περιορισμένοι πόροι: Οι κόμβοι έχουν περιορισμένη ενέργεια, μνήμη και υπολογιστική ισχύ, γεγονός που επηρεάζει τον σχεδιασμό των αλγορίθμων.
4. Ευελιξία και προσαρμοστικότητα: Μπορούν να αναπροσαρμόζουν τη λειτουργία τους σε δύσκολες ή δυναμικές συνθήκες, όπως αλλαγές στην τοπολογία ή εξωτερικές παρεμβολές.
5. Κλιμακούμενη δομή: Τα δίκτυα μπορούν να αναπτυχθούν σε μεγάλες περιοχές και να ενσωματώσουν εκατοντάδες ή χιλιάδες κόμβους.

Η ειδοποιός διαφορά τους από άλλα δίκτυα είναι η αυτο-οργάνωση και η ικανότητα συνεργασίας για την επίτευξη ενός κοινού στόχου [4], [8].

1.3.1 Ανατομία του Κόμβου Αισθητήρα

Κάθε κόμβος αισθητήρα αποτελεί ένα πλήρες ενσωματωμένο σύστημα (Embedded System). Στο [8] και [9], η εσωτερική δομή ενός κόμβου βασίζεται σε τέσσερα κύρια υποσυστήματα:

1. Μονάδα Αισθητήρα (Sensing Unit): Αποτελείται από τους φυσικούς αισθητήρες και έναν μετατροπέα αναλογικού σε ψηφιακό σήμα (ADC - Analog-to-Digital Converter), ώστε να μπορούν να επεξεργαστούν από τον κόμβο. Ο αισθητήρας καταγράφει φυσικά μεγέθη (π.χ. θερμοκρασία, υγρασία, πίεση) σε αναλογική μορφή και ο ADC τα μετατρέπει σε ψηφιακά δεδομένα έτοιμα για επεξεργασία.
2. Μονάδα Επεξεργασίας (Processing Unit): Περιλαμβάνει έναν μικροελεγκτή (Microcontroller Unit - MCU) — ένα ολοκληρωμένο κύκλωμα χαμηλής κατανάλωσης που ενσωματώνει τον επεξεργαστή και τα βασικά περιφερειακά του κόμβου — και μνήμη (συνήθως Flash και RAM). Είναι υπεύθυνη για την εκτέλεση των αλγορίθμων δρομολόγησης και τη διαχείριση της επικοινωνίας.
3. Μονάδα Επικοινωνίας (Communication Unit): Αποτελείται από έναν ραδιοπομποδέκτη (Transceiver) χαμηλής ισχύος. Είναι το τμήμα με τη μεγαλύτερη κατανάλωση ενέργειας στον κόμβο [2], [8].
4. Μονάδα Ισχύος (Power Unit): Περιλαμβάνει την μπαταρία και κυκλώματα διαχείρισης ενέργειας. Λόγω της δυσκολίας αντικατάστασης μπαταριών σε πεδία εφαρμογής, χρησιμοποιούνται συχνά τεχνικές συλλογής ενέργειας (Energy Harvesting) [4], [6].



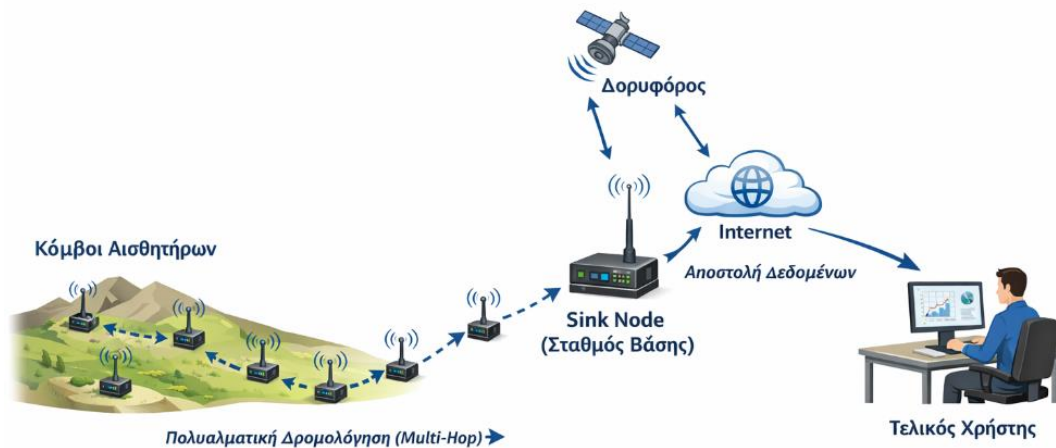
Εικόνα 1 WSN Communication Model [1]

Η κατανόηση της εσωτερικής δομής του κόμβου έχει άμεσες επιπτώσεις στον σχεδιασμό των μηχανισμών ασφάλειας, καθώς κάθε υποσύστημα συνιστά και ένα δυνητικό σημείο επίθεσης. Η μονάδα επικοινωνίας, ως το πλέον ενεργοβόρο τμήμα, αποτελεί τον προφανή στόχο επιθέσεων εξάντλησης πόρων, όπου ο επιτιθέμενος προκαλεί συνεχείς, περιττές μεταδόσεις για να αποστραγγίσει την μπαταρία. Η μονάδα επεξεργασίας, με την περιορισμένη υπολογιστική της ισχύ, θέτει αυστηρά όρια στην πολυπλοκότητα των κρυπτογραφικών αλγορίθμων που μπορούν να εκτελεστούν, ενώ η μονάδα μνήμης, λόγω του μικρού της μεγέθους, περιορίζει τον αριθμό των κλειδιών που μπορούν να αποθηκευτούν. Ακόμη και η μονάδα αισθητήρα μπορεί να γίνει στόχος μέσω επιθέσεων ψευδούς δεδομένων (false data injection), όπου ο επιτιθέμενος χειραγωγεί τις φυσικές συνθήκες ώστε να εισαγάγει παραπλανητικές μετρήσεις. Η ολιστική αυτή θεώρηση καταδεικνύει ότι η ασφάλεια ενός κόμβου δεν μπορεί να εστιάζει σε ένα μόνο υποσύστημα, αλλά οφείλει να λαμβάνει υπόψη το σύνολο της αρχιτεκτονικής του [2], [8].

1.3.2 Δομή Δικτύου και Σταθμός Βάσης (Sink Node)

Η αρχιτεκτονική του δικτύου δεν περιορίζεται στους κόμβους, αλλά επεκτείνεται στον τρόπο που αυτοί αλληλεπιδρούν με τον εξωτερικό κόσμο:

- **Κόμβος Sink (Σταθμός Βάσης):** Λειτουργεί ως η πύλη (Gateway) του δικτύου. Συλλέγει τα δεδομένα από όλους τους αισθητήρες και τα προωθεί μέσω Internet ή δορυφορικών συνδέσεων στον τελικό χρήστη. Διαθέτει σαφώς μεγαλύτερους πόρους επεξεργασίας και μνήμης σε σχέση με τους απλούς κόμβους [10].
- **Πολυαλματική Δρομολόγηση (Multi-hop Routing):** Επειδή η ισχύς εκπομπής των κόμβων είναι χαμηλή για εξοικονόμηση ενέργειας, τα δεδομένα μεταδίδονται "άλμα-άλμα" μέσω ενδιάμεσων κόμβων μέχρι να φτάσουν στον Sink [1], [10].



Εικόνα 2 Wireless Sensor Network [8]

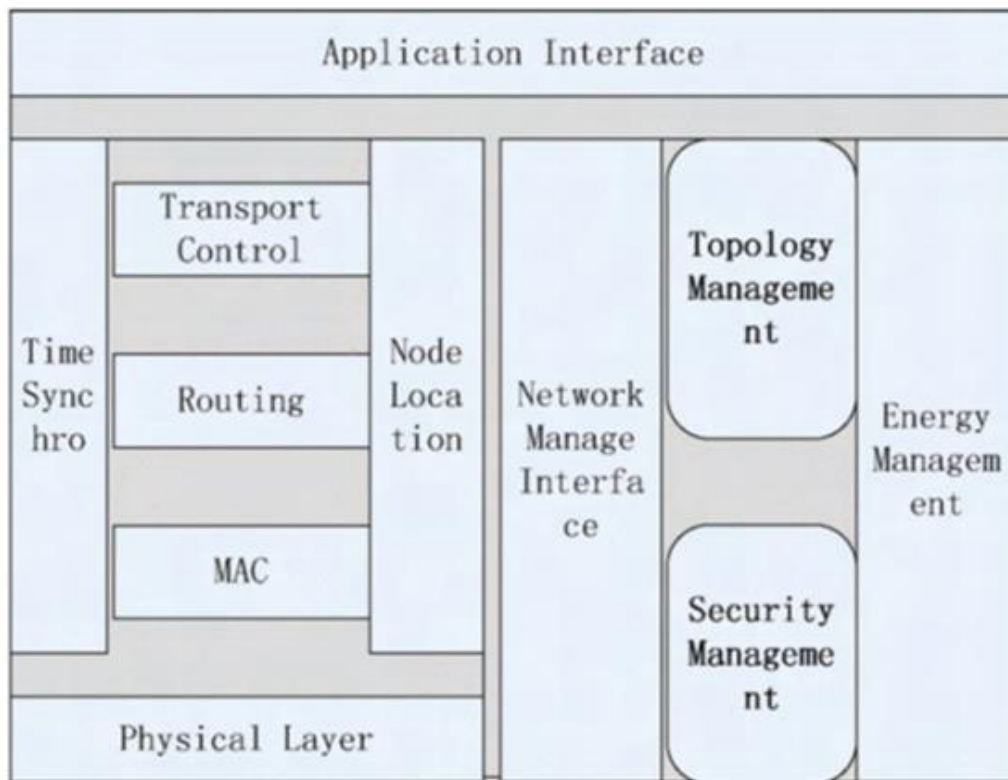
1.3.3 Η Στοιίβα Πρωτοκόλλων και Τεχνικά Χαρακτηριστικά

Η λειτουργία ενός WSN βασίζεται στη συνεργασία επιμέρους πρωτοκόλλων επικοινωνίας. Ως πρωτόκολλο ορίζεται ένα σύνολο κανόνων και διαδικασιών που καθορίζουν τον τρόπο με τον οποίο οι κόμβοι ενός δικτύου ανταλλάσσουν δεδομένα με αξιόπιστο και αποδοτικό τρόπο.

Σε αντίθεση με τα παραδοσιακά δίκτυα υπολογιστών, όπου υπάρχουν αυστηρά καθορισμένα πρότυπα (όπως το μοντέλο OSI), στα συστήματα IoT και στα WSNs δεν έχει καθιερωθεί ένα ενιαίο και πλήρως τυποποιημένο μοντέλο στοιβάς πρωτοκόλλων. Αυτό οφείλεται κυρίως στην ετερογένεια των εφαρμογών και στους περιορισμούς των συσκευών (ενέργεια, μνήμη, υπολογιστική ισχύς). Ωστόσο, για λόγους ανάλυσης και σχεδιασμού, συχνά χρησιμοποιείται μια λογική διαστρωμάτωση παρόμοια με τα κλασικά μοντέλα.

Μια ενδεικτική στοιίβα πρωτοκόλλων για WSNs περιλαμβάνει τα ακόλουθα επίπεδα:

- Φυσικό (Physical): Καθορίζει τη συχνότητα και τη διαμόρφωση του σήματος.
- Συνδέσμου Δεδομένων (Data Link): Διαχειρίζεται την πρόσβαση στο μέσο (Message Authentication Code) για την αποφυγή συγκρούσεων πακέτων.
- Δικτύου (Network): Υπεύθυνο για τη δρομολόγηση και την ασφάλεια των μονοπατιών.
- Μεταφοράς και Εφαρμογής: Διασφαλίζουν την αξιοπιστία της ροής δεδομένων και την παρουσίαση στον χρήστη [3], [4].



Εικόνα 3 Communication Protocol Stack of WSN [1]

Για την καλύτερη κατανόηση των δυνατοτήτων των υπάρχοντων συστημάτων, παρατίθενται στον ακόλουθο πίνακα τα χαρακτηριστικά δύο ευρέως χρησιμοποιούμενων πλατφόρμων [2]:

Πίνακας 1 Συγκριτικά χαρακτηριστικά υλικού μεταξύ κόμβου αισθητήρα και πύλης δικτύου [2]

Χαρακτηριστικό	MicaZ (Τυπικός Κόμβος)	Raspberry Pi 2 (Ως Sniffer/Gateway)
Επεξεργαστής	Atmel ATmega128L (8-bit)	Broadcom BCM2836 (32-bit Quad Core)
Μνήμη Flash/RAM	128 KB / 4 KB	Micro-SD / 1 GB RAM
Ραδιοσυχνότητα	2.4 GHz	Ieee WiFi (μέσω USB adapter)
Λειτουργικό Σύστημα	TinyOS	Raspbian (Linux)
Κατανάλωση (Sleep)	Πολύ χαμηλή (μΑ)	Μέτρια (mA)

1.3.4 Σύγχρονα Πρότυπα Συνδεσιμότητας: IEEE 802.15.4e/TSCH, 6LoWPAN/RPL και LPWAN

Η στοίβα πρωτοκόλλων που περιγράφηκε παραπάνω αποτυπώνει τη λογική δομή ενός WSN, δεν αποδίδει όμως την πραγματική ετερογένεια των υλοποιήσεων που κυριαρχούν σήμερα στην αγορά και στην

έρευνα. Από τα μέσα της δεκαετίας του 2010 και εντεύθεν, η κοινότητα έχει συγκλίνει σε τρεις διακριτές οικογένειες προτύπων, καθεμία από τις οποίες εισάγει διαφορετικό μοντέλο απειλής. Η κατανόηση αυτής της διαφοροποίησης είναι απαραίτητη, διότι η ανάλυση ασφάλειας που ακολουθεί στα επόμενα κεφάλαια δεν μπορεί να είναι αγνωστικιστική ως προς το υποκείμενο πρότυπο.

Η πρώτη οικογένεια αφορά την εξέλιξη του IEEE 802.15.4 μέσω της τροποποίησης 802.15.4e, η οποία εισήγαγε τη λειτουργία Χρονοθυρίδων με Μεταπήδηση Συχνότητας (TSCH - Time-Slotted Channel Hopping). Στη λειτουργία αυτή, ο χρόνος διαιρείται σε αυστηρά συγχρονισμένες χρονοθυρίδες και κάθε μετάδοση εκτελείται σε διαφορετικό κανάλι σύμφωνα με μια προκαθορισμένη ακολουθία. Το άμεσο όφελος για την ασφάλεια είναι σημαντικό: η μεταπήδηση συχνότητας μειώνει δραστικά την αποτελεσματικότητα των στατικών επιθέσεων παρεμβολής, καθώς ο επιτιθέμενος αναγκάζεται είτε να παρεμβάλλει σε ολόκληρο το φάσμα, με τεράστιο ενεργειακό κόστος, είτε να ανακατασκευάσει την ακολουθία μεταπήδησης. Ταυτόχρονα όμως εισάγεται μια νέα εξάρτηση: ο ακριβής χρονικός συγχρονισμός. Ένας επιτιθέμενος που καταφέρνει να διαταράξει τα πλαίσια συγχρονισμού μπορεί να αποσυνδέσει κόμβους από το δίκτυο χωρίς να χρειαστεί να παρεμβληθεί στα ίδια τα δεδομένα, μετατοπίζοντας έτσι το πεδίο της επίθεσης από το περιεχόμενο στον χρόνο [11].

Η δεύτερη οικογένεια αφορά τη διαδικτύωση των κόμβων μέσω IPv6. Το πρότυπο 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) επιτρέπει τη συμπίεση κεφαλίδων IPv6 ώστε να χωρούν στα 127 bytes του πλαισίου 802.15.4, ενώ το πρωτόκολλο RPL (Routing Protocol for Low-Power and Lossy Networks) οργανώνει τους κόμβους σε έναν Κατευθυνόμενο Ακυκλικό Γράφο προς Προορισμό (DODAG - Destination-Oriented Directed Acyclic Graph). Η υιοθέτηση του IPv6 στους κόμβους αισθητήρων υπήρξε τεχνολογικά καθοριστική, καθώς κατέστησε κάθε αισθητήρα απευθείας διευθυνσιοδοτήσιμο από το Διαδίκτυο. Η ίδια όμως εξέλιξη κατάργησε την «ασφάλεια μέσω απομόνωσης» που παραδοσιακά προστάτευε τα κλειστά δίκτυα αισθητήρων: το πεδίο επίθεσης δεν περιορίζεται πλέον στη γειτονία ραδιοκάλυψης αλλά επεκτείνεται δυνητικά σε ολόκληρο το Διαδίκτυο [12].

Η τρίτη οικογένεια είναι τα Δίκτυα Ευρείας Περιοχής Χαμηλής Ισχύος (LPWAN - Low-Power Wide-Area Networks), με κυριότερους εκπροσώπους το LoRaWAN, το NB-IoT και το Sigfox. Τα δίκτυα αυτά θυσιάζουν τον ρυθμό μετάδοσης για εμβέλεια δεκάδων χιλιομέτρων και διάρκεια ζωής μπαταρίας που μπορεί να ξεπεράσει τη δεκαετία. Η αρχιτεκτονική τους είναι κατά βάση αστέρας μέσω πυλών, γεγονός που απλοποιεί τη δρομολόγηση αλλά συγκεντρώνει τον κίνδυνο στην πύλη. Πρόσφατη πειραματική ανάλυση σε ναυτιλιακές εφαρμογές LoRaWAN κατέδειξε ότι, ακόμη και με ενεργή κρυπτογράφηση AES-128, παραμένουν εκμεταλλεύσιμες τρεις κατηγορίες αδυναμιών: επιθέσεις επανάλυσης σε διαμορφώσεις ενεργοποίησης ABP όπου δεν επιβάλλεται αυστηρός έλεγχος του μετρητή πλαισίων, στοχευμένη παρεμβολή στενής ζώνης που υποβαθμίζει τον λόγο σήματος προς θόρυβο σε συγκεκριμένα κανάλια, συναγωγή επιχειρησιακών προτύπων από τα μεταδεδομένα της κίνησης χωρίς αποκρυπτογράφηση του ωφέλιμου φορτίου [13].

Η τελευταία αυτή διαπίστωση αξίζει ιδιαίτερης προσοχής, καθώς αναδεικνύει ένα ζήτημα που διατρέχει ολόκληρη την παρούσα εργασία: η κρυπτογράφηση του περιεχομένου δεν συνεπάγεται προστασία της πληροφορίας. Ο χρόνος άφιξης ενός πακέτου, η συχνότητα των μεταδόσεων και το μέγεθος του ωφέλιμου φορτίου συνιστούν από μόνα τους ένα κανάλι διαρροής, το οποίο σε εφαρμογές όπως η παρακολούθηση υγείας ή η επιτήρηση υποδομών μπορεί να αποκαλύψει περισσότερα από το ίδιο το περιεχόμενο των μετρήσεων.

1.4 Τοπολογίες Δικτύων (Star, Mesh, Hybrid)

Η τοπολογία ενός Ασύρματου Δικτύου Αισθητήρων δεν αποτελεί απλώς μια γεωμετρική διάταξη των κόμβων στο χώρο, αλλά καθορίζει το μονοπάτι που ακολουθεί η πληροφορία, επηρεάζοντας άμεσα την κατανάλωση ενέργειας, την πολυπλοκότητα της δρομολόγησης και τη συνολική αξιοπιστία του συστήματος. Η επιλογή της κατάλληλης τοπολογίας εξαρτάται από τις απαιτήσεις της εφαρμογής, όπως η έκταση της περιοχής κάλυψης και η ανάγκη για ανθεκτικότητα σε αποτυχίες κόμβων [8].

Στην Τοπολογία Αστέρα (Star Topology), η δομή είναι συγκεντρωτική, καθώς κάθε κόμβος αισθητήρα επικοινωνεί απευθείας και αποκλειστικά με τον κεντρικό σταθμό βάσης (Sink). Πρόκειται για την απλούστερη μορφή δικτύωσης, η οποία εξασφαλίζει χαμηλή καθυστέρηση (latency) στη μετάδοση, αφού η πληροφορία απαιτεί μόνο ένα "άλμα" (single-hop) για να φτάσει στον προορισμό της. Ωστόσο, η τοπολογία αυτή περιορίζεται σημαντικά από την εμβέλεια της ασύρματης εκπομπής των κόμβων και παρουσιάζει ένα κρίσιμο σημείο αποτυχίας (single point of failure): αν ο σταθμός βάσης τεθεί εκτός λειτουργίας, ολόκληρο το δίκτυο καταρρέει ακαριαία [10].

Αντίθετα, η Τοπολογία Πλέγματος (Mesh Topology) προσφέρει μια αποκεντρωμένη προσέγγιση, επιτρέποντας στους κόμβους να επικοινωνούν όχι μόνο με τον Sink αλλά και με τους γείτονές τους. Αυτή η διασύνδεση δημιουργεί πολλαπλές εναλλακτικές διαδρομές για τη μεταφορά των δεδομένων, προσφέροντας υψηλή ανθεκτικότητα (fault tolerance). Σε περίπτωση που ένας κόμβος εξαντλήσει την ενέργειά του ή υποστεί βλάβη, το δίκτυο αυτο-οργανώνεται και αναδρομολογεί την πληροφορία μέσω άλλων ενεργών μονοπατιών [8]. Παρά την αξιοπιστία της, η τοπολογία πλέγματος απαιτεί πιο σύνθετα πρωτόκολλα δρομολόγησης και μπορεί να οδηγήσει σε ταχύτερη εξάντληση της μπαταρίας των κόμβων που βρίσκονται κοντά στον Sink, λόγω του μεγάλου όγκου πακέτων που καλούνται να προωθήσουν.

Καταλήγοντας, οι Υβριδικές Τοπολογίες και τα Ιεραρχικά Δίκτυα (Clustered Networks) επιδιώκουν να συνδυάσουν την απλότητα του αστέρα με την επεκτασιμότητα του πλέγματος. Στα δίκτυα αυτά, οι κόμβοι οργανώνονται σε ομάδες (clusters). Κάθε ομάδα διαθέτει έναν "αρχηγό" (Cluster Head), ο οποίος συγκεντρώνει τα δεδομένα από τους κόμβους-μέλη της ομάδας του, εκτελεί μια πρώτη επεξεργασία ή συμπίεση (data aggregation) και στη συνέχεια τα προωθεί στον σταθμό βάσης. Αυτή η προσέγγιση είναι η πλέον διαδεδομένη στα WSNs, καθώς βελτιστοποιεί την κατανάλωση ενέργειας. Το πρωτόκολλο LEACH, το οποίο αποτελεί σημείο αναφοράς στη βιβλιογραφία, βασίζεται ακριβώς σε αυτή τη λογική, εναλλάσσοντας περιοδικά τον ρόλο του Cluster Head μεταξύ των κόμβων για να διασφαλίσει την ομοιόμορφη κατανάλωση της ενέργειας σε όλο το δίκτυο [4], [5].

Πέραν της γεωμετρικής τους διάταξης, οι τοπολογίες των WSNs διαφοροποιούνται ουσιαστικά ως προς το προφίλ ασφάλειας που παρουσιάζουν, ένα ζήτημα που συχνά παραβλέπεται στη φάση του σχεδιασμού. Η τοπολογία αστέρα, λόγω της απευθείας σύνδεσης κάθε κόμβου με τον σταθμό βάσης, περιορίζει την επιφάνεια επίθεσης στο επίπεδο του μεμονωμένου συνδέσμου, καθιστώντας ευκολότερη την επιβολή κεντρικών πολιτικών αυθεντικοποίησης. Αντίθετα, στην τοπολογία πλέγματος η ανάγκη συνεργασίας μεταξύ γειτονικών κόμβων για την προώθηση πακέτων εισάγει εγγενώς το πρόβλημα της εμπιστοσύνης: ένας κακόβουλος ενδιάμεσος κόμβος μπορεί να απορρίψει, να αλλοιώσει ή να ανακατευθύνει την κίνηση που διέρχεται από αυτόν. Συνεπώς, η αυξημένη ανθεκτικότητα του πλέγματος έναντι αστοχιών υλικού συνοδεύεται από αυξημένη ευπάθεια σε επιθέσεις δρομολόγησης, μια αντιστάθμιση (trade-off) που πρέπει να σταθμίζεται προσεκτικά ανάλογα με το μοντέλο απειλής της εκάστοτε εφαρμογής [8], [10].

Η επιλογή της τοπολογίας επηρεάζει επίσης άμεσα την κλιμάκωση των μηχανισμών διαχείρισης κλειδών, μια παρατήρηση κρίσιμη για τη σύνδεση του παρόντος κεφαλαίου με την ανάλυση ασφάλειας που ακολουθεί. Σε ένα δίκτυο αστέρα, ένα απλό σχήμα ζευγαρωτών κλειδιών (pairwise keys) μεταξύ κάθε κόμβου και του σταθμού βάσης επαρκεί, διατηρώντας χαμηλή την πολυπλοκότητα. Ωστόσο, σε ένα εκτεταμένο δίκτυο πλέγματος με χιλιάδες κόμβους, η ανάγκη ασφαλούς επικοινωνίας μεταξύ αυθαίρετων ζευγών κόμβων καθιστά τα στατικά σχήματα κλειδιών μη βιώσιμα, οδηγώντας στην υιοθέτηση πιθανοτικών σχημάτων προ-διανομής κλειδιών (probabilistic key pre-distribution). Στις ιεραρχικές τοπολογίες, ο ρόλος του Cluster Head ως σημείου συγκέντρωσης δεδομένων τον καθιστά ταυτόχρονα και προνομιακό στόχο επίθεσης, καθώς η παραβίασή του εκθέτει το σύνολο των δεδομένων της ομάδας. Η κατανόηση αυτών των αλληλεξαρτήσεων μεταξύ τοπολογίας και ασφάλειας αποτελεί προϋπόθεση για τον ορθολογικό σχεδιασμό ανθεκτικών δικτύων [4], [10].

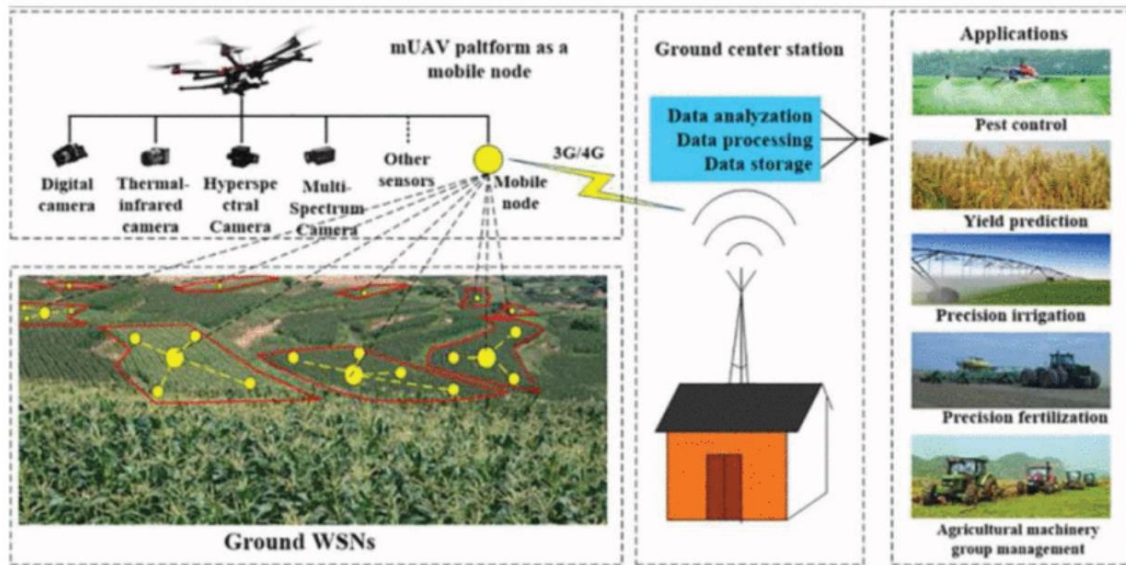
Μια σύγχρονη τάση που διαφοροποιεί τις κλασικές τοπολογίες είναι η εισαγωγή κινητών κόμβων (mobile nodes) και η αξιοποίηση μη επανδρωμένων εναέριων οχημάτων (UAVs - Unmanned Aerial Vehicles) ως κινούμενων σταθμών συλλογής δεδομένων. Στις δυναμικές αυτές τοπολογίες, η τοπολογία του δικτύου μεταβάλλεται συνεχώς στον χρόνο, καθιστώντας τα παραδοσιακά πρωτόκολλα δρομολόγησης ανεπαρκή και απαιτώντας μηχανισμούς που προσαρμόζονται σε πραγματικό χρόνο. Η κινητικότητα προσφέρει σημαντικά πλεονεκτήματα ως προς την ενεργειακή ισορροπία, καθώς ένας κινούμενος συλλέκτης μπορεί να πλησιάζει διαδοχικά τους κόμβους και να μειώνει το πλήθος των αναγκαίων αλμάτων. Από την άλλη πλευρά, η συνεχής αναδιαμόρφωση της τοπολογίας περιπλέκει τη διατήρηση ασφαλών συσχετίσεων εμπιστοσύνης, καθώς οι κόμβοι καλούνται να αυθεντικοποιούν διαρκώς νέους γείτονες υπό συνθήκες αβεβαιότητας. Οι προκλήσεις αυτές αναδεικνύουν ότι η τοπολογία δεν είναι στατική παράμετρος αλλά δυναμικό χαρακτηριστικό με βαθιές επιπτώσεις στην ασφάλεια [7], [8].

Πέρα από τις κλασικές κατηγορίες, αξίζει να σημειωθεί ότι στην πράξη τα περισσότερα μεγάλης κλίμακας δίκτυα υιοθετούν υβριδικές προσεγγίσεις, συνδυάζοντας τοπικές συστάδες αστέρα με ένα ραχιαίο δίκτυο πλέγματος που διασυνδέει τους επικεφαλής των συστάδων. Η αρχιτεκτονική αυτή επιτρέπει την τοπική συγκέντρωση δεδομένων με χαμηλή ενεργειακή επιβάρυνση, ενώ ταυτόχρονα διατηρεί την ανθεκτικότητα του πλέγματος στο επίπεδο της ραχιαίας υποδομής. Η ευελιξία αυτή καθιστά τις υβριδικές τοπολογίες την προτιμώμενη επιλογή για εφαρμογές μεγάλης γεωγραφικής έκτασης, όπως η περιβαλλοντική παρακολούθηση και η γεωργία ακριβείας, όπου η ισορροπία μεταξύ ενεργειακής αποδοτικότητας και αξιοπιστίας είναι κρίσιμη.

1.5 Τομείς Εφαρμογών

Η ευελιξία και το χαμηλό κόστος των WSNs έχουν επιτρέψει τη διείσδυσή τους σε κρίσιμους τομείς της σύγχρονης οικονομίας και κοινωνίας. Η δυνατότητα των κόμβων να λειτουργούν σε εχθρικά περιβάλλοντα ή σε περιοχές μεγάλης κλίμακας καθιστά τα WSNs αναπόσπαστο κομμάτι της τεχνολογικής εξέλιξης [6].

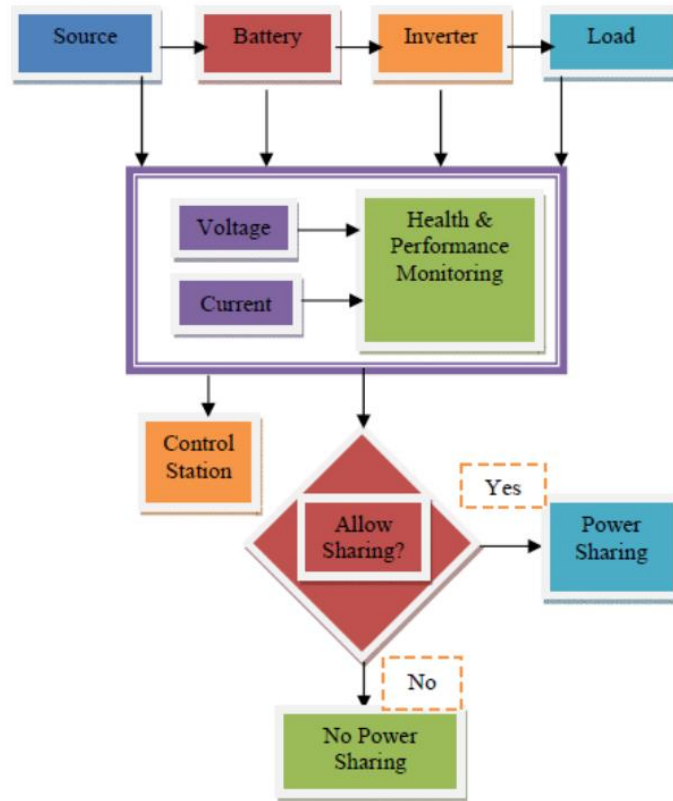
Μία από τις πλέον υποσχόμενες εφαρμογές εντοπίζεται στη Γεωργία Ακριβείας (Modern Agriculture). Οι αισθητήρες χρησιμοποιούνται για τη συνεχή παρακολούθηση παραμέτρων όπως η θερμοκρασία του αέρα, η υγρασία του εδάφους και τα επίπεδα φωτεινότητας, παράγοντες που επηρεάζουν άμεσα την ποιότητα και την ποσότητα της παραγωγής. Στις εκτάσεις μεγάλης κλίμακας, τα προαναφερθέντα UAVs αξιοποιούνται και εδώ ως κινητοί συλλέκτες ή αναμεταδότες, βελτιώνοντας την κάλυψη της επικοινωνίας σε τεράστιες αγροτικές περιοχές [14].



Εικόνα 4 UAV-WSN Monitoring System in Agriculture Sector [14]

Στον τομέα της Διαχείρισης Καταστροφών (Disaster Monitoring and Management), τα WSNs προσφέρουν λύσεις για την επιτήρηση περιοχών μετά από φυσικές καταστροφές, όπου οι παραδοσιακές υποδομές τηλεπικοινωνιών έχουν καταρρεύσει. Η χρήση αισθητήρων για την ανίχνευση δασικών πυρκαγιών, πλημμυρών ή την παρακολούθηση της στατικότητας κτιρίων μετά από σεισμό, επιτρέπει στις αρχές να λαμβάνουν κρίσιμες αποφάσεις σε πραγματικό χρόνο. Όπως επισημαίνεται στη βιβλιογραφία, ο συνδυασμός επίγειων WSNs και εναέριων UAVs δημιουργεί ένα υβριδικό σύστημα ικανό να παρέχει εικόνα από το πεδίο ακόμη και στις πιο αντίξοες συνθήκες [14].

Εξίσου σημαντική είναι η εφαρμογή των WSNs στα Έξυπνα Δίκτυα Ενέργειας (Smart Grids). Η ενσωμάτωση του IoT στα δίκτυα ηλεκτρισμού επιτρέπει την αμφίδρομη επικοινωνία μεταξύ παρόχου και καταναλωτή, διευκολύνοντας τη διαχείριση της ζήτησης και την πρόβλεψη βλαβών. Ιδιαίτερο ενδιαφέρον παρουσιάζει η χρήση αισθητήρων σε συστήματα Ηλιακής Ενέργειας (Solar Energy Harvesting) σε "Έξυπνες Πόλεις". Οι αισθητήρες παρακολουθούν την απόδοση των φωτοβολταϊκών πλαισίων και την κατάσταση των μπαταριών, επιτρέποντας τον διαμοιρασμό της ενέργειας μεταξύ κτιρίων ανάλογα με τις τρέχουσες ανάγκες και την παραγωγή, καθιστώντας το δίκτυο πιο αξιόπιστο και οικονομικά αποδοτικό [6].



Εικόνα 5 Smart Grid Architecture [6]

Τα WSNs παίζουν καθοριστικό ρόλο στην Υγεία (Healthcare) μέσω της απομακρυσμένης παρακολούθησης ζωτικών σημείων ασθενών, στη Βιομηχανία (Industrial Automation) για τον έλεγχο διαδικασιών παραγωγής και στον Στρατιωτικό τομέα για την επιτήρηση συνόρων και την ανίχνευση χημικών ή βιολογικών απειλών. Η ικανότητα αυτών των δικτύων να παρέχουν "έξυπνη" πληροφορία σε πραγματικό χρόνο αποτελεί το κοινό χαρακτηριστικό που τα καθιστά απαραίτητα σε κάθε σύγχρονη εφαρμογή [1], [10].

Πέρα από τους τομείς που προαναφέρθηκαν, η εφαρμογή των WSNs στην παρακολούθηση δομικής ακεραιότητας (Structural Health Monitoring) αναδεικνύει με σαφήνεια τη σημασία της αξιοπιστίας και της ασφάλειας των δεδομένων. Δίκτυα αισθητήρων επιταχυνσιόμετρων και τάσης ενσωματώνονται σε γέφυρες, φράγματα και ουρανοξύστες, καταγράφοντας μικρομετακινήσεις και δονήσεις που προμηνύουν δομικές αστοχίες. Σε αυτές τις εφαρμογές κρίσιμης ασφάλειας (safety-critical), η αλλοίωση των μετρήσεων από κακόβουλο τρίτο δεν συνιστά απλώς απώλεια πληροφορίας, αλλά μπορεί να οδηγήσει σε εσφαλμένες αποφάσεις με κίνδυνο ανθρώπινων ζωών. Συνεπώς, η ακεραιότητα και η αυθεντικότητα των δεδομένων αναβαθμίζονται από επιθυμητά χαρακτηριστικά σε απαραίτητες απαιτήσεις, υπογραμμίζοντας ότι η ασφάλεια στα WSNs δεν αποτελεί πολυτέλεια αλλά θεμελιώδη προϋπόθεση λειτουργίας [1], [6].

Ο τομέας της υγείας μέσω των δικτύων σώματος (Wireless Body Area Networks - WBAN) αποτελεί ίσως το πιο ευαίσθητο πεδίο εφαρμογής από άποψη ιδιωτικότητας. Φορητοί και εμφυτευσιμοί αισθητήρες παρακολουθούν συνεχώς ζωτικά σημεία όπως ο καρδιακός ρυθμός, τα επίπεδα γλυκόζης και η εγκεφαλική δραστηριότητα, μεταδίδοντας τα δεδομένα αυτά ασύρματα προς ιατρικές πλατφόρμες. Η

διαρροή τέτοιων δεδομένων δεν θέτει απλώς ζήτημα παραβίασης προσωπικών δεδομένων υπό το πρίσμα κανονιστικών πλαισίων όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation – GDPR, Κανονισμός (ΕΕ) 2016/679), δηλαδή το ενιαίο θεσμικό πλαίσιο της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων προσωπικού χαρακτήρα, ο οποίος θέτει αυστηρές απαιτήσεις για τη νόμιμη και διαφανή επεξεργασία δεδομένων προσωπικού χαρακτήρα και προβλέπει βαρύτατα πρόστιμα σε περίπτωση παραβίασης, αλλά μπορεί να οδηγήσει σε διακρίσεις ή σε στοχευμένες επιθέσεις. Ακόμη σοβαρότερα, η παραβίαση εμφυτεύσιμων ιατρικών συσκευών, όπως οι αντλίες ινσουλίνης ή οι βηματοδότες, αποτελεί ευθεία απειλή για τη ζωή του ασθενούς. Οι ιδιαιτερότητες αυτές καθιστούν τα WBAN ένα από τα πλέον απαιτητικά πεδία για τον σχεδιασμό ελαφρών αλλά ισχυρών μηχανισμών ασφάλειας [7], [10].

1.6 Περιορισμοί και Προκλήσεις (Ενέργεια, Υπολογιστική Ισχύς, Μνήμη)

Παρά την ευρεία διάδοση και την ευελιξία τους, τα Ασύρματα Δίκτυα Αισθητήρων διέπονται από αυστηρούς περιορισμούς που πηγάζουν κυρίως από τους φυσικούς πόρους των κόμβων (hardware constraints). Η κυριότερη πρόκληση εντοπίζεται στον ενεργειακό τομέα, καθώς οι περισσότεροι κόμβοι τροφοδοτούνται από μπαταρίες περιορισμένης χωρητικότητας και συχνά λειτουργούν σε αφιλόξενα ή δυσπρόσιτα περιβάλλοντα, όπου η αντικατάστασή τους είναι πρακτικά αδύνατη. Όπως επισημαίνεται στη βιβλιογραφία, η ασύρματη μετάδοση και λήψη δεδομένων αποτελεί την πιο ενεργοβόρα διαδικασία, καταναλώνοντας πολλαπλάσια ισχύ σε σχέση με την τοπική επεξεργασία της πληροφορίας. Για τον λόγο αυτό, ο σχεδιασμός των πρωτοκόλλων επικεντρώνεται στη μεγιστοποίηση της διάρκειας ζωής του δικτύου (Network Lifetime) μέσω τεχνικών «έξυπνου ύπνου» (duty cycling) και ενεργειακά αποδοτικής δρομολόγησης [6], [14].

Παράλληλα, οι περιορισμοί στην υπολογιστική ισχύ και τη μνήμη καθορίζουν το εύρος των λειτουργιών που μπορεί να εκτελέσει ένας κόμβος. Οι μικροεπεξεργαστές χαμηλής κατανάλωσης και η περιορισμένη μνήμη RAM/Flash καθιστούν απαγορευτική τη χρήση σύνθετων αλγορίθμων κρυπτογράφησης ή βαριάς επεξεργασίας σήματος απευθείας στο πεδίο. Η αδυναμία εκτεταμένης προσωρινής αποθήκευσης δεδομένων (buffering) επιβάλλει την άμεση μετάδοση της πληροφορίας, γεγονός που αυξάνει την πολυπλοκότητα στη διαχείριση της κυκλοφορίας του δικτύου [1], [6].

Η αξιοπιστία της επικοινωνίας αποτελεί μια συνεχή πρόκληση λόγω της φύσης του ασύρματου μέσου. Τα WSNs είναι ιδιαίτερα επιρρεπή σε παρεμβολές, θόρυβο και απώλεια πακέτων, ειδικά σε βιομηχανικά περιβάλλοντα ή περιοχές με έντονα γεωφυσικά φαινόμενα [14]. Η δυναμική τοπολογία του δικτύου, όπου οι κόμβοι μπορεί να τεθούν εκτός λειτουργίας απροειδοποίητα λόγω εξάντλησης μπαταρίας, απαιτεί από το σύστημα να διαθέτει μηχανισμούς αυτο-ίασης (self-healing). Επιπλέον, το ζήτημα της κλιμακωσιμότητας (scalability) παραμένει κρίσιμο, καθώς το δίκτυο πρέπει να διαχειρίζεται αποτελεσματικά τις συγκρούσεις (collisions) στο κοινό μέσο επικοινωνίας, είτε αυτό αποτελείται από μερικούς δεκάδες είτε από χιλιάδες κόμβους [6], [10].

Ένας περιορισμός που συχνά υποτιμάται, αλλά έχει καθοριστική σημασία για την ασφάλεια, είναι η φυσική προσβασιμότητα των κόμβων (physical exposure). Σε αντίθεση με τους διακομιστές ενός κέντρου δεδομένων που προστατεύονται εντός ελεγχόμενων εγκαταστάσεων, οι κόμβοι ενός WSN αναπτύσσονται συχνά σε ανοιχτά, μη επιτηρούμενα περιβάλλοντα όπου ένας επιτιθέμενος μπορεί να τους προσεγγίσει φυσικά. Η πρόσβαση αυτή επιτρέπει επιθέσεις παραβίασης υλικού (physical tampering), κατά τις οποίες ο εισβολέας μπορεί να εξαγάγει κρυπτογραφικά κλειδιά από τη μνήμη του κόμβου ή να

τον αντικαταστήσει με κακόβουλο κόμβο. Το γεγονός αυτό διαφοροποιεί θεμελιωδώς το μοντέλο απειλής των WSNs από εκείνο των παραδοσιακών δικτύων, καθώς η υπόθεση ότι το υλικό είναι έμπιστο (trusted hardware) δεν ισχύει πλέον. Η αδυναμία διασφάλισης της φυσικής ακεραιότητας επιβάλλει τον σχεδιασμό πρωτοκόλλων που παραμένουν ανθεκτικά ακόμη και όταν ένα υποσύνολο κόμβων έχει παρβιαστεί (resilience under node compromise) [1], [10].

Οι ανωτέρω περιορισμοί δεν λειτουργούν μεμονωμένα, αλλά συνθέτουν ένα πλέγμα αλληλεξαρτήσεων που καθιστά τον σχεδιασμό ασφαλών WSNs ένα πρόβλημα πολυκριτηριακής βελτιστοποίησης. Κάθε μηχανισμός ασφάλειας που προστίθεται —είτε πρόκειται για κρυπτογράφηση, είτε για ψηφιακές υπογραφές, είτε για συστήματα ανίχνευσης εισβολών— καταναλώνει ενέργεια, μνήμη και υπολογιστικούς κύκλους, πόρους που είναι ήδη σπάνιοι. Δημιουργείται έτσι μια θεμελιώδης αντιστάθμιση μεταξύ του επιπέδου ασφάλειας και της διάρκειας ζωής του δικτύου, η οποία θα αναλυθεί ποσοτικά σε επόμενο κεφάλαιο της παρούσας εργασίας. Η αναγνώριση αυτής της σύγκρουσης απαιτήσεων αποτελεί το κεντρικό νήμα που διατρέχει το σύνολο της μελέτης ασφάλειας στα ασύρματα δίκτυα αισθητήρων, καθώς κάθε προτεινόμενη λύση οφείλει να αξιολογείται όχι μόνο ως προς την κρυπτογραφική της ισχύ, αλλά και ως προς το ενεργειακό της αποτύπωμα [6], [10].

1.7 Επίλογος

Στο παρόν κεφάλαιο παρουσιάστηκαν οι θεμελιώδεις έννοιες των Ασύρματων Δικτύων Αισθητήρων, περιλαμβάνοντας την ιστορική τους εξέλιξη, τη δομή και τη λειτουργία τους, καθώς και τις βασικές τοπολογίες και τους τομείς εφαρμογής τους. Ιδιαίτερη έμφαση δόθηκε στα χαρακτηριστικά των κόμβων και στην αρχιτεκτονική των δικτύων, αναδεικνύοντας τον τρόπο με τον οποίο επιτυγχάνεται η συλλογή και επεξεργασία δεδομένων σε πραγματικό χρόνο. Παράλληλα, αναλύθηκαν οι κύριοι περιορισμοί που σχετίζονται με την κατανάλωση ενέργειας, την υπολογιστική ισχύ και την αξιοπιστία της επικοινωνίας, οι οποίοι καθιστούν τον σχεδιασμό των WSNs ιδιαίτερα απαιτητικό και αναδεικνύουν την ανάγκη για αποδοτικούς και ασφαλείς μηχανισμούς λειτουργίας, θέτοντας έτσι το υπόβαθρο για την περαιτέρω ανάλυση των ζητημάτων ασφάλειας στα επόμενα κεφάλαια.

Κεφάλαιο 2ο: Απειλές και Τρωτά Σημεία στα WSNs

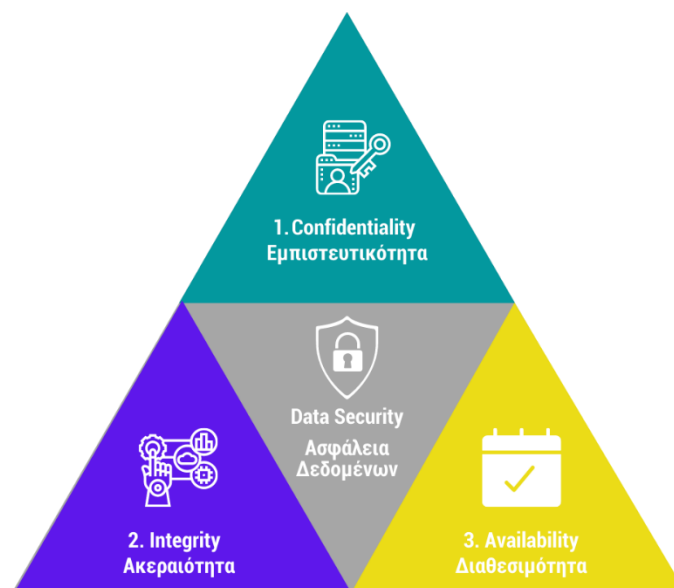
2.1 Εισαγωγή

Στο παρόν κεφάλαιο, εξετάζονται αρχικά οι θεμελιώδεις αρχές που πρέπει να διέπουν ένα ασφαλές WSN, ενώ στη συνέχεια αναλύονται διεξοδικά οι απειλές και οι επιθέσεις που εκδηλώνονται σε κάθε επίπεδο της στοιβάς πρωτοκόλλων, αναδεικνύοντας τις προκλήσεις που προκύπτουν από τον συνδυασμό της τεχνολογικής εξέλιξης και των κακόβουλων πρακτικών.

2.2 Βασικές Αρχές Ασφάλειας

Η ευρεία εξάπλωση των WSNs σε κρίσιμες υποδομές, από την εθνική άμυνα έως την έξυπνη ενέργεια, καθιστά την ασφάλειά τους ζήτημα υψίστης σημασίας για την κοινωνική και οικονομική σταθερότητα. Λόγω της φύσης τους, τα δίκτυα αυτά παρουσιάζουν ένα διευρυμένο «πεδίο επίθεσης» (attack surface), καθώς οι κόμβοι είναι συχνά εγκατεστημένοι σε μη ελεγχόμενα ή εχθρικά περιβάλλοντα, καθιστώντας τους ευάλωτους όχι μόνο σε ψηφιακές αλλά και σε φυσικές παρεμβάσεις. Η χρήση του ελεύθερου ασύρματου μέσου για τη μετάδοση πληροφοριών επιτρέπει σε οποιονδήποτε κακόβουλο χρήστη με τον κατάλληλο εξοπλισμό να παρακολουθήσει (eavesdropping) ή να παρεμβληθεί στην επικοινωνία, χωρίς να απαιτείται φυσική πρόσβαση στο δίκτυο [1], [6].

Επιπλέον, οι εγγενείς περιορισμοί των συσκευών, όπως η περιορισμένη επεξεργαστική ισχύς και η χαμηλή ενέργεια, καθιστούν αδύνατη την εφαρμογή παραδοσιακών, "βαριών" μηχανισμών ασφαλείας (όπως η κρυπτογράφηση δημόσιου κλειδιού υψηλής υπολογιστικής απαίτησης), δημιουργώντας έτσι κενά ασφαλείας που οι επιτιθέμενοι μπορούν να εκμεταλλευτούν. Η ασφάλεια στα WSNs δεν είναι μια ενιαία λύση, αλλά ένα πολυεπίπεδο πρόβλημα που απαιτεί την κατανόηση των τρωτών σημείων σε κάθε στάδιο της λειτουργίας του δικτύου [1], [14].



Εικόνα 6 Η Τριάδα CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) στο πλαίσιο των WSNs [6]

Για να διασφαλιστεί η αξιοπιστία ενός δικτύου αισθητήρων, είναι απαραίτητο να ικανοποιούνται οι τρεις θεμελιώδεις αρχές της ασφάλειας πληροφοριών, γνωστές ως «Τριάδα CIA» (Confidentiality, Integrity, Availability), οι οποίες όμως στα WSNs αποκτούν ιδιαίτερη σημασία λόγω των περιορισμένων πόρων των κόμβων. Η πρώτη αρχή, η Εμπιστευτικότητα (Confidentiality), στοχεύει στη διασφάλιση ότι τα δεδομένα που συλλέγονται και μεταδίδονται παραμένουν απρόσιτα σε μη εξουσιοδοτημένες οντότητες. Αυτό καθίσταται κρίσιμο σε ευαίσθητες εφαρμογές, όπως η απομακρυσμένη ιατρική παρακολούθηση ή η στρατιωτική επιτήρηση, όπου η υποκλοπή της πληροφορίας μπορεί να εκθέσει προσωπικά δεδομένα ή στρατηγικά μυστικά. Παράλληλα, η Ακεραιότητα (Integrity) εγγυάται ότι η πληροφορία δεν έχει υποστεί κακόβουλη τροποποίηση ή αλλοίωση κατά τη διαδρομή της από τον αισθητήρα προς τον σταθμό βάσης. Σε βιομηχανικά περιβάλλοντα, για παράδειγμα, μια αλλοιωμένη μέτρηση της πίεσης ή της θερμοκρασίας θα μπορούσε να προκαλέσει εσφαλμένη ενεργοποίηση συστημάτων ασφαλείας με καταστροφικές συνέπειες. Η τρίτη αρχή, η Διαθεσιμότητα (Availability), διασφαλίζει ότι οι υπηρεσίες του δικτύου και τα δεδομένα των αισθητήρων είναι προσβάσιμα στους εξουσιοδοτημένους χρήστες ανά πάσα στιγμή. Επιθέσεις που πλήττουν τη διαθεσιμότητα, όπως οι επιθέσεις άρνησης υπηρεσίας (DoS - Denial of Service), στοχεύουν στη διακοπή της λειτουργίας του δικτύου, εμποδίζοντας την επικοινωνία ή εξαντλώντας τους πόρους των κόμβων, καθιστώντας τα δεδομένα και τις υπηρεσίες μη διαθέσιμα.

Συγκεκριμένα, οι επιθέσεις DoS στα WSNs παρουσιάζουν ιδιαίτερη επικινδυνότητα λόγω της περιορισμένης ενεργειακής εφεδρείας των κόμβων. Μια επίθεση DoS μπορεί να εκδηλωθεί είτε ως παρεμβολή (jamming) στο φυσικό επίπεδο, εμποδίζοντας τη μετάδοση, είτε ως επίθεση εξάντλησης πόρων (exhaustion attack). Στη δεύτερη περίπτωση, ο επιτιθέμενος αναγκάζει τους κόμβους να εκτελούν συνεχείς και άσκοπους υπολογισμούς ή μεταδόσεις, με απώτερο σκοπό την ταχεία εξάντληση της μπαταρίας τους. Η απώλεια της διαθεσιμότητας σε αυτή την περίπτωση είναι μόνιμη για τον συγκεκριμένο κόμβο, καθιστώντας την αποκατάσταση του δικτύου εξαιρετικά δύσκολη και δαπανηρή, καθώς απαιτεί φυσική παρέμβαση για την αντικατάσταση των πηγών ενέργειας [1], [6]. Συμπερασματικά, πέρα από την παραδοσιακή τριάδα, στα WSNs κρίνεται επιβεβλημένη η Αυθεντικοποίηση (Authentication), η οποία επιτρέπει στον παραλήπτη να επιβεβαιώσει την ταυτότητα του αποστολέοντος κόμβου, αποκλείοντας την περίπτωση εισαγωγής πλαστών δεδομένων από εξωτερικούς εισβολείς. [1], [14].

Πέραν της κλασικής τριάδας και της αυθεντικοποίησης, η ιδιαίτερη φύση των ασύρματων δικτύων αισθητήρων επιβάλλει την υιοθέτηση πρόσθετων αρχών ασφάλειας που στα παραδοσιακά συστήματα θεωρούνται δευτερεύουσες. Μια τέτοια αρχή είναι η Φρεσκάδα των Δεδομένων (Data Freshness), η οποία εγγυάται ότι τα λαμβανόμενα δεδομένα είναι πρόσφατα και δεν αποτελούν επανάληψη παλαιότερων, νόμιμων μηνυμάτων. Χωρίς τη διασφάλιση της φρεσκάδας, ένας επιτιθέμενος θα μπορούσε να καταγράψει έγκυρα κρυπτογραφημένα πακέτα και να τα αναμεταδώσει αργότερα (replay attack), παραπλανώντας τον σταθμό βάσης με παρωχημένες μετρήσεις. Η αρχή αυτή υλοποιείται τυπικά μέσω μετρητών (counters), χρονοσφραγίδων (timestamps) ή τυχαίων αριθμών μιας χρήσης (nonces), μηχανισμών που ενσωματώνονται σε πρωτόκολλα όπως το SNEP (Sensor Network Encryption Protocol) που θα αναλυθεί σε επόμενο κεφάλαιο. Η σημασία της φρεσκάδας αναδεικνύεται ιδιαίτερα σε εφαρμογές ελέγχου, όπου μια καθυστερημένη ή επαναλαμβανόμενη εντολή μπορεί να οδηγήσει σε εσφαλμένη δράση του συστήματος [1], [4].

Μια δεύτερη επικουρική αρχή, κρίσιμη για την κατανομημένη φύση των WSNs, είναι η Μη-Αποποίηση (Non-repudiation), η οποία διασφαλίζει ότι ένας κόμβος δεν μπορεί να αρνηθεί την αποστολή ενός μηνύματος που πράγματι απέστειλε. Η ιδιότητα αυτή αποκτά ιδιαίτερη βαρύτητα σε σενάρια όπου απαιτείται λογοδοσία, όπως στις οικονομικές συναλλαγές μεταξύ συσκευών ή στην καταγραφή κρίσιμων συμβάντων για μελλοντική δικαστική χρήση. Συμπληρωματικά, η αρχή της Αυτο-οργάνωσης

Ασφάλειας (Self-organization of security) απαιτεί από το δίκτυο να εγκαθιστά και να διαχειρίζεται τις σχέσεις εμπιστοσύνης χωρίς την παρουσία προκαθορισμένης υποδομής ή κεντρικής αρχής πιστοποίησης. Η απαίτηση αυτή είναι αντιφατική ως προς τη φύση της, καθώς η απουσία κεντρικού σημείου ελέγχου, ενώ ενισχύει την ανθεκτικότητα, ταυτόχρονα δυσχεραίνει τη θεμελίωση της αρχικής εμπιστοσύνης μεταξύ αγνώστων κόμβων. Η επίλυση αυτής της αντίφασης αποτελεί ένα από τα δυσκολότερα ανοιχτά προβλήματα στον σχεδιασμό ασφαλών WSNs [1], [10].

Είναι σημαντικό να τονιστεί ότι οι ανωτέρω αρχές δεν είναι ανεξάρτητες μεταξύ τους, αλλά συχνά βρίσκονται σε σχέση αντιστάθμισης. Η ενίσχυση της εμπιστευτικότητας μέσω ισχυρής κρυπτογράφησης αυξάνει το υπολογιστικό κόστος και επομένως μειώνει τη διαθεσιμότητα ενέργειας, ενώ η επιβολή αυστηρής αυθεντικοποίησης σε κάθε πακέτο επιβαρύνει την καθυστέρηση του δικτύου. Ο σχεδιαστής ενός ασφαλούς WSNs καλείται συνεπώς να ιεραρχήσει τις αρχές ανάλογα με το μοντέλο απειλής και τις απαιτήσεις της εφαρμογής, αντί να επιδιώκει την ταυτόχρονη μεγιστοποίηση όλων. Σε μια εφαρμογή στρατιωτικής επιτήρησης, για παράδειγμα, η εμπιστευτικότητα προηγείται, ενώ σε ένα σύστημα έγκαιρης προειδοποίησης για φυσικές καταστροφές, η διαθεσιμότητα και η ακεραιότητα τίθενται σε προτεραιότητα. Η συνειδητή αυτή ιεράρχηση αποτελεί τη βάση κάθε ορθολογικής πολιτικής ασφάλειας και θα διαπνέει την αξιολόγηση των μηχανισμών στα επόμενα κεφάλαια [6], [10].

Η εφαρμογή των τριών θεμελιωδών αρχών της ασφάλειας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, προσλαμβάνει ιδιαίτερες διαστάσεις στο πλαίσιο των WSNs. Σε αντίθεση με τα παραδοσιακά πληροφοριακά συστήματα, όπου η εμπιστευτικότητα συχνά θεωρείται η ύψιστη προτεραιότητα, στα δίκτυα αισθητήρων η ιεράρχηση των αρχών αυτών εξαρτάται άμεσα από τη φύση της εφαρμογής. Σε ένα σύστημα παρακολούθησης πυρκαγιών, για παράδειγμα, η διαθεσιμότητα και η ακεραιότητα των δεδομένων είναι κρίσιμότερες από την εμπιστευτικότητα, καθώς η έγκαιρη και αξιόπιστη ειδοποίηση είναι ζωτικής σημασίας, ενώ τα ίδια τα δεδομένα θερμοκρασίας δεν είναι απόρρητα. Αντίθετα, σε στρατιωτικές ή ιατρικές εφαρμογές, η εμπιστευτικότητα ανάγεται σε πρωταρχική απαίτηση. Στα WSNs προστίθενται και εξειδικευμένες απαιτήσεις, όπως η φρεσκάδα των δεδομένων (data freshness), που διασφαλίζει ότι ο παραλήπτης λαμβάνει πρόσφατες και όχι επαναλαμβανόμενες παλαιές μετρήσεις, στοιχείο κρίσιμο για την αποτροπή επιθέσεων επανάληψης.

Πέρα από τα τρία θεμελιώδη ζητούμενα της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας, η ασφάλεια των WSNs απαιτεί την ικανοποίηση ενός ευρύτερου συνόλου ιδιοτήτων που προκύπτουν από τη φύση της κατανεμημένης και συνεργατικής λειτουργίας τους. Η αυθεντικοποίηση δεδομένων προέλευσης (data origin authentication) διασφαλίζει ότι μια μέτρηση προέρχεται πράγματι από τον νόμιμο κόμβο και όχι από έναν πλαστοπροσωπούντα εισβολέα. Η φρεσκάδα των δεδομένων (data freshness) εγγυάται ότι τα λαμβανόμενα μηνύματα είναι πρόσφατα και δεν αποτελούν αναμετάδοση παλαιότερων, παρωχημένων πακέτων, αποτρέποντας έτσι τις επιθέσεις επανάληψης. Τέλος, η μη αποποίηση (non-repudiation) εξασφαλίζει ότι ένας κόμβος δεν μπορεί να αρνηθεί τη συμμετοχή του σε μια συναλλαγή, ιδιότητα ιδιαίτερα σημαντική σε εφαρμογές όπου απαιτείται λογοδοσία. Η ταυτόχρονη ικανοποίηση όλων αυτών των ιδιοτήτων υπό τους αυστηρούς ενεργειακούς περιορισμούς των αισθητήρων συνιστά τη θεμελιώδη πρόκληση που διαπερνά το σύνολο του πεδίου της ασφάλειας των δικτύων αισθητήρων [1], [3].

2.3 Ταξινόμηση Επιθέσεων ανά Επίπεδο Στοιβάς Πρωτοκόλλων

Η ασφάλεια στα WSNs προσεγγίζεται παραδοσιακά μέσω της ανάλυσης της στοιβάς πρωτοκόλλων (protocol stack) όπως φαίνεται στην εικόνα 3, καθώς κάθε επίπεδο επιτελεί διαφορετικές λειτουργίες και παρουσιάζει μοναδικά τρωτά σημεία. Μια αποτελεσματική ταξινόμηση των απειλών βασίζεται στο

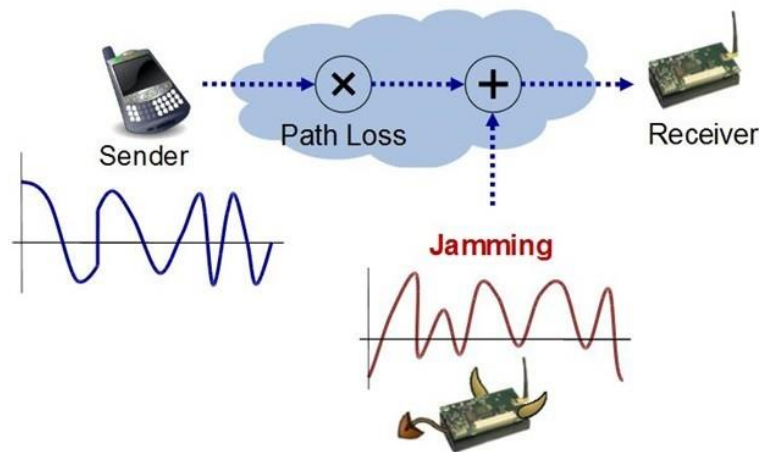
επίπεδο στο οποίο εκδηλώνεται η επίθεση, ξεκινώντας από το χαμηλότερο επίπεδο του υλικού και φτάνοντας μέχρι το επίπεδο εφαρμογής. Η πολυεπίπεδη αυτή ανάλυση επιτρέπει στους ερευνητές να αναπτύξουν εξειδικευμένους μηχανισμούς άμυνας, καθώς μια επίθεση σε ένα επίπεδο μπορεί συχνά να προκαλέσει αλυσιδωτές αντιδράσεις σε ολόκληρο το δίκτυο [1], [14].

2.3.1 Επιθέσεις Φυσικού Επιπέδου

Το Φυσικό Επίπεδο είναι υπεύθυνο για την επιλογή συχνότητας, την παραγωγή φέροντος σήματος, τη διαμόρφωση και την ανίχνευση δεδομένων. Λόγω της έκθεσης των κόμβων σε ανοιχτούς χώρους, οι επιθέσεις σε αυτό το επίπεδο είναι συχνές και ιδιαίτερα αποτελεσματικές. Η πλέον διαδεδομένη επίθεση είναι το Jamming (Παρεμβολή), κατά την οποία ο επιτιθέμενος εκπέμπει σήματα ραδιοσυχνοτήτων που προκαλούν θόρυβο και παρεμβολές στο κανάλι επικοινωνίας. Αυτό έχει ως αποτέλεσμα τη διακοπή της νόμιμης ανταλλαγής μηνυμάτων μεταξύ των κόμβων, προκαλώντας άρνηση υπηρεσίας (DoS). Το Jamming μπορεί να είναι συνεχές, τυχαίο ή στοχευμένο (reactive), με το τελευταίο να είναι το πιο επικίνδυνο, καθώς ο εισβολέας ενεργοποιείται μόνο όταν ανιχνεύσει κίνηση στο δίκτυο, εξοικονομώντας έτσι τη δική του ενέργεια [1], [6].

Μια εξίσου σοβαρή απειλή είναι το Physical Tampering (Φυσική Παραβίαση). Δεδομένου ότι οι κόμβοι των WSNs είναι συχνά χαμηλού κόστους και δεν διαθέτουν εξελιγμένα συστήματα προστασίας κελύφους, ένας εισβολέας μπορεί να αποκτήσει φυσική πρόσβαση σε αυτούς. Μέσω της φυσικής παραβίασης, ο επιτιθέμενος μπορεί να καταστρέψει τον κόμβο, να αντικαταστήσει το λογισμικό του (firmware) ή ακόμα και να εξαγάγει ευαίσθητες πληροφορίες, όπως κρυπτογραφικά κλειδιά, από τη μνήμη της συσκευής. Αυτού του είδους οι επιθέσεις είναι ιδιαίτερα κρίσιμες, καθώς ένας παραβιασμένος κόμβος μπορεί στη συνέχεια να χρησιμοποιηθεί ως "δούρειος ίππος" για την εξαπόλυση επιθέσεων σε ανώτερα επίπεδα της στοίβας πρωτοκόλλων [1], [14].

Η αντιμετώπιση των επιθέσεων στο φυσικό επίπεδο είναι ιδιαίτερα απαιτητική, καθώς αυτές δεν εκμεταλλεύονται αδυναμίες λογισμικού αλλά εγγενή χαρακτηριστικά του ασύρματου μέσου. Έναντι του Jamming, η βιβλιογραφία προτείνει τεχνικές όπως η μεταπήδηση συχνότητας (Frequency Hopping Spread Spectrum - FHSS) και η διασπορά φάσματος ακολουθίας (Direct Sequence Spread Spectrum - DSSS), οι οποίες δυσχεραίνουν τη στόχευση ενός συγκεκριμένου καναλιού από τον επιτιθέμενο. Συμπληρωματικά, μηχανισμοί χωρικής απομόνωσης (spatial retreat), όπου οι κόμβοι μετακινούνται ή αναδρομολογούν την κίνηση μακριά από την παρεμβαλλόμενη περιοχή, μπορούν να μετριάσουν τις επιπτώσεις. Ωστόσο, καμία από αυτές τις τεχνικές δεν προσφέρει πλήρη προστασία, καθώς ένας επιτιθέμενος με επαρκή ισχύ εκπομπής μπορεί να καλύψει ολόκληρο το διαθέσιμο φάσμα. Η παρατήρηση αυτή αναδεικνύει ότι η ασφάλεια στο φυσικό επίπεδο αποτελεί κατά βάση ζήτημα ανθεκτικότητας και ταχείας ανάκαμψης, παρά πλήρους αποτροπής [1], [6].



Εικόνα 7 Απεικόνιση επίθεσης παρεμβολής (Jamming) όπου ο εισβολέας διακόπτει την επικοινωνία μεταξύ των αισθητήρων και του σταθμού βάσης [1]

Όσον αφορά τη φυσική παραβίαση, η σύγχρονη προσέγγιση εστιάζει στη χρήση υλικού ανθεκτικού σε παραβίαση (tamper-resistant hardware) και σε μηχανισμούς αυτοκαταστροφής κρίσιμων δεδομένων. Συγκεκριμένα, η ενσωμάτωση μονάδων ασφαλούς αποθήκευσης κλειδιών, όπως τα trusted platform modules (TPM) ή οι φυσικά μη κλωνοποιήσιμες συναρτήσεις (physically unclonable functions - PUFs), επιτρέπει την παραγωγή μοναδικών αναγνωριστικών που δεν μπορούν να αντιγραφούν, ακόμη και αν ο επιτιθέμενος αποκτήσει φυσικό έλεγχο της συσκευής. Οι PUFs αξιοποιούν τις μικροσκοπικές, τυχαίες διαφοροποιήσεις της κατασκευής κάθε ολοκληρωμένου κυκλώματος ως «δακτυλικό αποτύπωμα» του υλικού, προσφέροντας μια ελαφριά εναλλακτική στην αποθήκευση μυστικών κλειδιών. Παρά τα πλεονεκτήματά τους, οι λύσεις αυτές αυξάνουν το κόστος ανά κόμβο, γεγονός που περιορίζει την υιοθέτησή τους σε εφαρμογές υψηλής αξίας. Έτσι, στην πράξη, η προστασία έναντι φυσικής παραβίασης παραμένει μια οικονομοτεχνική απόφαση που σταθμίζει το κόστος του υλικού έναντι της αξίας των προστατευόμενων δεδομένων [1], [14].

2.3.2 Επιθέσεις Επιπέδου Συνδέσμου

Το Επίπεδο Συνδέσμου είναι υπεύθυνο για την πολυπλεξία των ροών δεδομένων, την ανίχνευση σφαλμάτων και, κυρίως, για τον έλεγχο πρόσβασης στο μέσο (Medium Access Control). Μία από τις πιο αποτελεσματικές επιθέσεις σε αυτό το επίπεδο είναι η Σύγκρουση (Collision). Σε αυτή την περίπτωση, ο επιτιθέμενος παρακολουθεί το δίκτυο και, μόλις ανιχνεύσει την έναρξη μετάδοσης ενός πακέτου από έναν νόμιμο κόμβο, εκπέμπει μια σύντομη ριπή σήματος. Αυτή η σκόπιμη παρεμβολή προκαλεί αλλοίωση στα δεδομένα του πακέτου, με αποτέλεσμα ο παραλήπτης να το απορρίπτει λόγω αποτυχίας του ελέγχου κυκλικού πλεονασμού (CRC - Cyclic Redundancy Check). Η συνεχής επανεκπομπή των κατεστραμμένων πακέτων οδηγεί σε σημαντική καθυστέρηση και πτώση της απόδοσης του δικτύου [1], [10].

Άμεσα συνδεδεμένη με τις συγκρούσεις είναι η επίθεση Εξάντλησης Πόρων (Resource Exhaustion). Επειδή τα πρωτόκολλα του επιπέδου συνδέσμου προβλέπουν την επανεκπομπή πακέτων σε περίπτωση σφάλματος, ο επιτιθέμενος μπορεί να προκαλεί διαδοχικές συγκρούσεις μέχρι ο νόμιμος κόμβος να καταναλώσει όλη την ενέργεια της μπαταρίας του στην προσπάθεια να στείλει επιτυχώς την πληροφορία. Επιπλέον, ο εισβολέας μπορεί να παραβιάσει τους κανόνες του πρωτοκόλλου Message

Authentication Code (π.χ. στέλνοντας συνεχή αιτήματα "Request to Send" - RTS), αναγκάζοντας τους γειτονικούς κόμβους να παραμένουν σε κατάσταση αναμονής ή να επεξεργάζονται άχρηστα δεδομένα, εξαντλώντας έτσι την υπολογιστική τους ισχύ και τη μνήμη τους. Αυτή η μορφή επίθεσης είναι ιδιαίτερα ύπουλη, καθώς «στραγγίζει» το δίκτυο αργά αλλά σταθερά, μειώνοντας δραματικά το χρόνο ζωής του χωρίς να προκαλεί ολική κατάρρευση από την πρώτη στιγμή [6], [14].

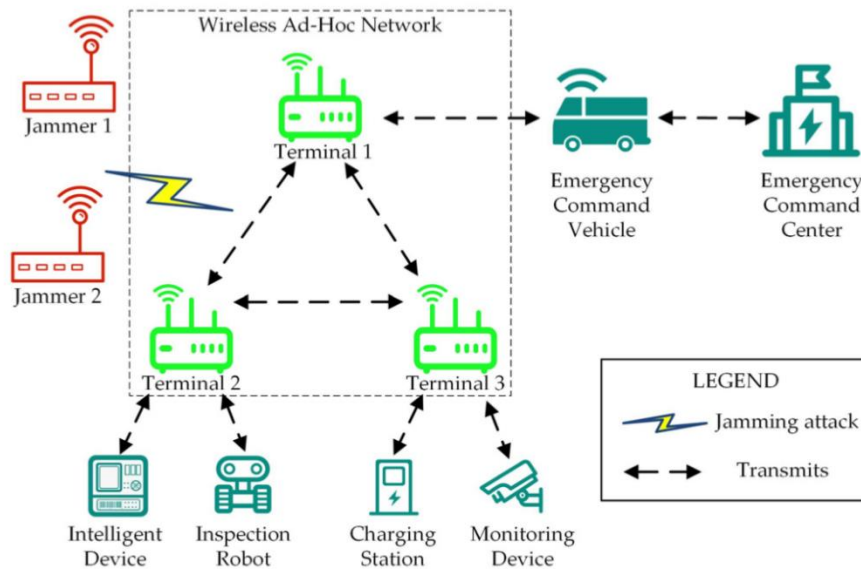
Μια ιδιαίτερα ύπουλη παραλλαγή των επιθέσεων στο επίπεδο συνδέσμου είναι η επίθεση αδικίας (unfairness attack), η οποία δεν στοχεύει στην ολική παρεμπόδιση της επικοινωνίας αλλά στη συστηματική υποβάθμιση της ποιότητας υπηρεσίας για επιλεγμένους κόμβους. Ο επιτιθέμενος εκμεταλλεύεται διακριτικά τους μηχανισμούς προτεραιότητας του πρωτοκόλλου ελέγχου πρόσβασης στο μέσο, καταλαμβάνοντας το κανάλι συχνότερα από όσο του αναλογεί και στερώντας έτσι από τους νόμιμους κόμβους δίκαιη πρόσβαση στο μέσο. Επειδή η επίθεση αυτή δεν προκαλεί πλήρη διακοπή αλλά μόνο μερική υποβάθμιση, είναι εξαιρετικά δύσκολο να εντοπιστεί με συμβατικά εργαλεία παρακολούθησης, καθώς η συμπεριφορά της προσομοιάζει με φυσιολογική συμφόρηση του δικτύου. Η αντιμετώπισή της απαιτεί μηχανισμούς που παρακολουθούν στατιστικά την κατανομή της πρόσβασης στο κανάλι ανά κόμβο και εντοπίζουν αποκλίσεις από τα αναμενόμενα πρότυπα δικαιοσύνης.

Η αντιμετώπιση των επιθέσεων στο επίπεδο συνδέσμου βασίζεται σε ένα συνδυασμό προληπτικών και ανιχνευτικών τεχνικών, καθεμία με τους δικούς της συμβιβασμούς. Η χρήση κωδίκων διόρθωσης σφαλμάτων (Error Correcting Codes) επιτρέπει την ανάκτηση πακέτων που έχουν υποστεί μερική αλλοίωση, μειώνοντας την ανάγκη για ενεργοβόρες επανεκπομπές, αλλά με κόστος επιπλέον υπολογιστικής επιβάρυνσης. Η τεχνική του time diversity, κατά την οποία τα πακέτα μεταδίδονται σε διαφορετικές χρονικές στιγμές, μειώνει την πιθανότητα επιτυχούς στοχευμένης σύγκρουσης, ενώ ο περιορισμός του ρυθμού (rate limiting) στα αιτήματα πρόσβασης μετριάξει τις επιθέσεις εξάντλησης πόρων. Καμία από αυτές τις τεχνικές δεν προσφέρει απόλυτη προστασία μεμονωμένα· η αποτελεσματική άμυνα προκύπτει από τον συνδυασμό τους σε μια στρατηγική που λαμβάνει υπόψη τόσο τη φύση της απειλής όσο και το διαθέσιμο ενεργειακό απόθεμα του δικτύου [6], [14].

2.3.3 Επιθέσεις Επιπέδου Δικτύου (Routing Attacks)

Οι επιθέσεις δρομολόγησης (Routing Attacks) στοχεύουν στις διαδικασίες ανακάλυψης και συντήρησης των μονοπατιών επικοινωνίας μέσα στο δίκτυο. Δεδομένου ότι τα WSNs βασίζονται σε συνεργατικά πρωτόκολλα, ένας κακόβουλος κόμβος μπορεί εύκολα να διαταράξει τη λειτουργία ολόκληρου του δικτύου επηρεάζοντας τις αποφάσεις δρομολόγησης. Οι επιθέσεις αυτές διακρίνονται για την ικανότητά τους να απομονώνουν τμήματα του δικτύου ή να κατευθύνουν την κυκλοφορία μέσω ελεγχόμενων από τον εισβολέα σημείων, επιτρέποντας την υποκλοπή ή την αλλοίωση των δεδομένων [1], [6].

Οι επιθέσεις επιπέδου δικτύου είναι ιδιαίτερα επικίνδυνες γιατί μπορούν να εκτελεστούν με ελάχιστη κατανάλωση ενέργειας από την πλευρά του επιτιθέμενου, αλλά με καταστροφικά αποτελέσματα για την ακεραιότητα και τη διαθεσιμότητα του συστήματος. Όπως επισημαίνεται στην αναφορά, η έλλειψη ισοχυρών μηχανισμών αυθεντικοποίησης στα παραδοσιακά πρωτόκολλα δρομολόγησης επιτρέπει σε εξωτερικούς ή εσωτερικούς εισβολείς να εισάγουν ψευδείς πληροφορίες δρομολόγησης, προκαλώντας βρόχους (loops), αυξημένη καθυστέρηση ή πλήρη απώλεια πακέτων. Λόγω της πολυπλοκότητάς τους, οι επιθέσεις αυτές υποδιαιρούνται σε επιμέρους κατηγορίες, όπως η επιλεκτική προώθηση, οι επιθέσεις Sybil και οι επιθέσεις Sinkhole [1], [14].



Εικόνα 8 Μοντέλο συστήματος με εκδήλωση επίθεσης παρεμβολής (Jamming) σε ένα ασύρματο Ad-Hoc δίκτυο [10]

Οι επιθέσεις στο επίπεδο δικτύου θεωρούνται από τις πλέον επικίνδυνες, καθώς στοχεύουν στον ίδιο τον πυρήνα της λειτουργίας του δικτύου, τη δρομολόγηση των δεδομένων. Μια ιδιαίτερα ύπουλη παραλλαγή είναι η επιλεκτική προώθηση (selective forwarding), κατά την οποία ένας παραβιασμένος κόμβος δεν απορρίπτει όλα τα πακέτα —κάτι που θα τον καθιστούσε εύκολα ανιχνεύσιμο— αλλά μόνο ένα επιλεγμένο υποσύνολο, διατηρώντας έτσι μια φαινομενικά φυσιολογική συμπεριφορά. Η επίθεση αυτή συχνά συνδυάζεται με μια επίθεση sinkhole, ώστε ο κακόβουλος κόμβος να προσελκύσει πρώτα το μεγαλύτερο δυνατό μέρος της κίνησης πριν αρχίσει την επιλεκτική απόρριψη. Ο εντοπισμός τέτοιων επιθέσεων είναι εξαιρετικά δύσκολος, καθώς η περιστασιακή απώλεια πακέτων μπορεί να αποδοθεί σε φυσιολογικές συνθήκες του ασύρματου μέσου, όπως οι παρεμβολές ή η συμφόρηση. Η αποτελεσματική αντιμετώπιση απαιτεί τη συνεργατική παρακολούθηση πολλαπλών κόμβων και τη στατιστική ανάλυση των ποσοστών παράδοσης σε βάθος χρόνου, ώστε να διακριθεί η κακόβουλη συμπεριφορά από τις φυσικές διακυμάνσεις του δικτύου [10], [14].

Κάποιες επιθέσεις που στοχεύουν στην ακεραιότητα της ροής των δεδομένων μέσω της απόρριψης πακέτων είναι:

- **Selective Forwarding (Επιλεκτική Προώθηση):** Βασίζεται στην παραδοχή ότι οι κόμβοι σε ένα WSN προωθούν πιστά τα πακέτα που λαμβάνουν. Σε αυτή την περίπτωση, ένας κακόβουλος κόμβος αρνείται να προωθήσει ορισμένα κρίσιμα μηνύματα, «πετώντας» τα (dropping), ενώ επιτρέπει σε άλλα να περάσουν κανονικά ώστε να μην γίνει εύκολα αντιληπτός. Η τακτική αυτή είναι ιδιαίτερα αποτελεσματική όταν ο εισβολέας στοχεύει συγκεκριμένους τύπους δεδομένων, προκαλώντας κενά στην πληροφορία που φτάνει στον σταθμό βάσης χωρίς να διακόπτει πλήρως την επικοινωνία [1], [10].
- **Blackhole (Μαύρη Τρύπα):** Αποτελεί την ακραία μορφή της επιλεκτικής προώθησης. Εδώ, ο κακόβουλος κόμβος απορρίπτει το σύνολο της κίνησης που διέρχεται από αυτόν, λειτουργώντας ως «μαύρη τρύπα» για τα δεδομένα του δικτύου. Συχνά, ο εισβολέας προσπαθεί πρώτα να καταστεί ελκυστικός (π.χ. διαδίδοντας ψευδείς πληροφορίες για βέλτιστη διαδρομή), ώστε να αναγκάσει μεγάλο μέρος της κυκλοφορίας να διέλθει από αυτόν. Το αποτέλεσμα είναι η δημιουργία "τυφλών"

περιοχών στο δίκτυο και η άσκοπη εξάντληση ενεργειακών πόρων από τους νόμιμους κόμβους που προσπαθούν να επανεκπέμψουν τα χαμένα δεδομένα [1], [14].

Απειλές που επικεντρώνονται στην παραβίαση της ταυτότητας των κόμβων:

- Sybil Attack: Ένας μοναδικός κακόβουλος κόμβος παρουσιάζει πολλαπλές ψευδείς ταυτότητες στο υπόλοιπο δίκτυο. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να εμφανίζεται ως μια ομάδα γειτονικών κόμβων, επηρεάζοντας δυσανάλογα τις αποφάσεις δρομολόγησης, παρακάμπτοντας μηχανισμούς πλεονασμού ή αλλοιώνοντας αποτελέσματα ψηφοφοριών σε πρωτόκολλα πλειοψηφίας. Η επίθεση αυτή υπονομεύει την εμπιστοσύνη, καθώς το δίκτυο αδυνατεί να διακρίνει αν η πληροφορία προέρχεται από διαφορετικές πηγές ή από μία κακόβουλη οντότητα [1], [6].
- Identity Theft (Κλοπή Ταυτότητας): Σε αντίθεση με την επίθεση Sybil, ο εισβολέας υποκλέπτει τα διαπιστευτήρια και τις διευθύνσεις έγκυρων, νόμιμων κόμβων. Έτσι, μπορεί να εισχωρήσει σε ασφαλείς ζώνες επικοινωνίας και να αποκτήσει πρόσβαση σε κρυπτογραφημένες πληροφορίες. Η αντιμετώπιση απαιτεί ισχυρούς μηχανισμούς αυθεντικοποίησης και χρήση μοναδικών κρυπτογραφικών κλειδιών για κάθε κόμβο, ώστε να αποτρέπεται η μαζική υποκλοπή ταυτοτήτων [1], [14].

Επιθέσεις που χειραγωγούν την τοπολογία και τη δρομολόγηση του δικτύου:

- Wormhole Attack: Δύο ή περισσότεροι κακόβουλοι κόμβοι συνεργάζονται δημιουργώντας μια "σήραγγα" (tunnel) χαμηλής καθυστέρησης μεταξύ απομακρυσμένων σημείων. Ο ένας επιτιθέμενος λαμβάνει πακέτα, τα διοχετεύει μέσω της σήραγγας και τα επανεκπέμπει στο άλλο άκρο. Αυτό δημιουργεί την ψευδαίσθηση στους νόμιμους κόμβους ότι βρίσκονται γεωγραφικά κοντά, με αποτέλεσμα να επιλέγουν λανθασμένα αυτό το μονοπάτι ως βέλτιστο, επιτρέποντας στους εισβολείς να παρακολουθούν ή να απορρίπτουν την κυκλοφορία [1], [3].
- Sinkhole Attack: Στοχεύει στην προσέλκυση της κυκλοφορίας μιας περιοχής προς έναν παραβιασμένο κόμβο. Ο επιτιθέμενος παρουσιάζει τον εαυτό του ως την ιδανική διαδρομή (π.χ. μικρότερος αριθμός αλμάτων) προς τον Σταθμό Βάσης. Οι γειτονικοί κόμβοι κατευθύνουν τα δεδομένα τους προς τον κακόβουλο κόμβο, ο οποίος μπορεί στη συνέχεια να εξαπολύσει περαιτέρω επιθέσεις. Η επικινδυνότητα αυξάνεται όταν συνδυάζεται με Wormholes, καθιστώντας τον κακόβουλο κόμβο εξαιρετικά "ελκυστικό" για το δίκτυο [3], [6].

Η αντιμετώπιση των επιθέσεων δρομολόγησης απαιτεί την υιοθέτηση ασφαλών πρωτοκόλλων δρομολόγησης (secure routing protocols), τα οποία ενσωματώνουν μηχανισμούς αυθεντικοποίησης και επαλήθευσης διαδρομής ήδη από τον σχεδιασμό τους. Μια θεμελιώδης αρχή είναι η χρήση αυθεντικοποιημένων μηνυμάτων ελέγχου δρομολόγησης, ώστε ένας κακόβουλος κόμβος να μην μπορεί να διαφημίσει ψευδείς διαδρομές χωρίς να γίνει αντιληπτός. Ειδικά για τις επιθέσεις τύπου Wormhole, οι οποίες δεν παραβιάζουν την κρυπτογραφία αλλά εκμεταλλεύονται τη χωροχρονική συμπεριφορά του δικτύου, αναπτύχθηκαν τεχνικές περιορισμού όπως τα packet leashes. Οι μηχανισμοί αυτοί προσθέτουν στα πακέτα πληροφορία για τον χρόνο ή τη γεωγραφική θέση αποστολής, επιτρέποντας στον παραλήπτη να εντοπίσει αν ένα πακέτο διένυσε αφύσικα μεγάλη απόσταση σε μη ρεαλιστικό χρόνο. Η προσέγγιση αυτή καταδεικνύει ότι ορισμένες απειλές απαιτούν λύσεις πέραν της κρυπτογραφίας, αξιοποιώντας τα φυσικά χαρακτηριστικά της διάδοσης του σήματος.

Παράλληλα με τους κρυπτογραφικούς και χωροχρονικούς μηχανισμούς, σημαντικό ρόλο στην άμυνα έναντι των επιθέσεων δικτύου διαδραματίζουν τα συστήματα φήμης και εμπιστοσύνης (trust and

reputation systems). Σε αυτά, κάθε κόμβος παρακολουθεί τη συμπεριφορά των γειτόνων του και διατηρεί μια δυναμική βαθμολογία εμπιστοσύνης, η οποία αυξάνεται όταν ο γείτονας προωθεί σωστά τα πακέτα και μειώνεται όταν παρατηρείται ύποπτη συμπεριφορά, όπως η επιλεκτική απόρριψη μηνυμάτων. Οι κόμβοι με χαμηλή βαθμολογία αποκλείονται σταδιακά από τις διαδρομές δρομολόγησης, απομονώνοντας έτσι τους παραβιασμένους κόμβους χωρίς την ανάγκη κεντρικής παρέμβασης. Η ισχύς αυτής της προσέγγισης έγκειται στην προσαρμοστικότητα της και στην ικανότητά της να αντιμετωπίζει ακόμη και επιθέσεις που δεν είχαν προβλεφθεί κατά τον σχεδιασμό. Ωστόσο, τα συστήματα αυτά παθαίνουν ευάλωτα σε εξελιγμένες στρατηγικές, όπως οι επιθέσεις on-off, κατά τις οποίες ο επιτιθέμενος εναλλάσσει καλή και κακόβουλη συμπεριφορά για να διατηρεί τεχνητά υψηλή τη φήμη του [10], [14].

2.3.4 Επιθέσεις στο Πρωτόκολλο Δρομολόγησης RPL

Η ανάλυση των επιθέσεων δρομολόγησης που προηγήθηκε βασίζεται σε ένα γενικευμένο μοντέλο πολυαλματικού δικτύου. Στα σύγχρονα IPv6-based WSNs όμως, η δρομολόγηση υλοποιείται στη συντριπτική πλειονότητα των περιπτώσεων μέσω του RPL, το οποίο διαθέτει τη δική του, ιδιαίτερη επιφάνεια επίθεσης. Πρόσφατη συστηματική επισκόπηση της βιβλιογραφίας της περιόδου 2011-2024 καταγράφει τριάντα επτά διακριτές επιθέσεις δρομολόγησης κατά του RPL, οργανωμένες σε δώδεκα κατηγορίες, αριθμός σχεδόν διπλάσιος από εκείνον που κατέγραφαν οι προγενέστερες επισκοπήσεις [12]. Η έκταση αυτή δικαιολογεί την ξεχωριστή πραγμάτευση του πρωτοκόλλου.

Η επίθεση αριθμού έκδοσης (Version Number Attack) αποτελεί ίσως το πιο χαρακτηριστικό παράδειγμα του πώς ένας μηχανισμός σχεδιασμένος για ανθεκτικότητα μπορεί να μετατραπεί σε όπλο. Το RPL προβλέπει ότι ο ριζικός κόμβος μπορεί να αυξήσει τον αριθμό έκδοσης του DODAG ώστε να επιβάλει καθολική ανακατασκευή του γράφου όταν η τοπολογία έχει υποβαθμιστεί. Ένας κακόβουλος εσωτερικός κόμβος που πλαστογραφεί αυξημένους αριθμούς έκδοσης προκαλεί επαναλαμβανόμενες, περιττές ανακατασκευές. Το κόστος δεν είναι απλώς η στιγμιαία απώλεια συνδεσιμότητας: κάθε ανακατασκευή συνεπάγεται καταιγισμό μηνυμάτων ελέγχου σε ολόκληρο το δίκτυο, με αποτέλεσμα η επίθεση να λειτουργεί ταυτόχρονα ως μηχανισμός εξάντλησης ενέργειας. Πρόκειται για μια επίθεση με εξαιρετικά ασύμμετρη οικονομία, καθώς το κόστος για τον επιτιθέμενο περιορίζεται στην αποστολή λίγων πλαστών μηνυμάτων.

Η επίθεση βαθμίδας (Rank Attack) εκμεταλλεύεται τον μηχανισμό με τον οποίο κάθε κόμβος διαφημίζει τη λογική του απόσταση από τη ρίζα. Δηλώνοντας τεχνητά χαμηλή βαθμίδα, ο επιτιθέμενος πείθει τους γείτονές του ότι προσφέρει σύντομο μονοπάτι προς τον σταθμό βάσης και προσελκύει την κίνησή τους. Το αποτέλεσμα είναι λειτουργικά ισοδύναμο με μια επίθεση Sinkhole, όπως αυτή περιγράφηκε κλασικά στη βιβλιογραφία της ασφαλούς δρομολόγησης [15], με τη διαφορά ότι εδώ ο επιτιθέμενος δεν χρειάζεται να παραβιάσει κάποιον κρυπτογραφικό μηχανισμό: αρκεί να υποβάλει μια ψευδή αλλά συντακτικά έγκυρη τιμή σε ένα πεδίο που το πρωτόκολλο εμπιστεύεται εξ ορισμού. Η αντίστροφη παραλλαγή, η μείωση βαθμίδας από νόμιμο κόμβο, οδηγεί σε βρόχους δρομολόγησης και σε κατακερματισμό του γράφου [12].

Η πλημμύρα μηνυμάτων DIS (DIS Flooding) στοχεύει ευθέως στον ενεργειακό προϋπολογισμό των γειτόνων. Τα μηνύματα αναζήτησης πληροφοριών DODAG προορίζονται για νεοεισερχόμενους κόμβους που επιθυμούν να ενταχθούν στον γράφο· η μαζική και επαναλαμβανόμενη εκπομπή τους υποχρεώνει τους γείτονες να επαναφέρουν τον χρονιστή Trickle και να απαντούν με μηνύματα DIO, ακυρώνοντας τον μηχανισμό εξοικονόμησης ενέργειας που ο ίδιος ο χρονιστής υλοποιεί. Παρόμοια λογική διέπει τις εσωτερικές επιθέσεις DAO, όπου η πλαστογράφηση μηνυμάτων αντικειμενικού προορισμού διογκώνει τεχνητά τους πίνακες δρομολόγησης των ενδιαμέσων κόμβων μέχρι την εξάντληση της περιορισμένης μνήμης τους.

Το κοινό χαρακτηριστικό των επιθέσεων αυτών είναι διδακτικό. Καμία δεν απαιτεί σπάσιμο κρυπτογράφησης· όλες εκμεταλλεύονται το γεγονός ότι το RPL, σχεδιασμένο για συνεργατικά περιβάλλοντα με περιορισμένους πόρους, εμπιστεύεται εξ ορισμού τις πληροφορίες ελέγχου που ανταλλάσσουν οι κόμβοι. Η βασική λειτουργία ασφάλειας του προτύπου προβλέπει προαιρετικούς μηχανισμούς αυθεντικοποίησης μηνυμάτων ελέγχου, οι οποίοι όμως σπανίως ενεργοποιούνται σε πραγματικές αναπτύξεις λόγω κόστους. Η διαπίστωση αυτή τεκμηριώνει έναν ισχυρισμό που θα επανέλθει στο Κεφάλαιο 3: η ασφάλεια δρομολόγησης στα WSNs δεν είναι πρωτίστως κρυπτογραφικό, αλλά αρχιτεκτονικό πρόβλημα, η αντιμετώπισή του απαιτεί συνδυασμό αυθεντικοποίησης μηνυμάτων ελέγχου με μηχανισμούς αξιολόγησης εμπιστοσύνης και ανίχνευσης ανωμαλιών [12].

2.3.5 Επιθέσεις Επιπέδου Μεταφοράς

Το Επίπεδο Μεταφοράς στα WSNs είναι ιδιαίτερα ευαίσθητο σε επιθέσεις που στοχεύουν στην εξάντληση των περιορισμένων πόρων των κόμβων και στη διακοπή της συνεδρίας επικοινωνίας. Η πλέον χαρακτηριστική επίθεση σε αυτό το επίπεδο είναι ο Κατακλυσμός (Flooding), όπου ο εισβολέας αποστέλλει μαζικά αιτήματα σύνδεσης προς έναν κόμβο-θύμα, εκμεταλλευόμενος πρωτόκολλα που απαιτούν διατήρηση κατάστασης (state). Ο στοχευμένος κόμβος αναγκάζεται να δεσμεύσει πολύτιμους πόρους και μνήμη για να διατηρήσει αυτές τις ημιτελείς συνδέσεις, με αποτέλεσμα την ταχεία εξάντληση της μνήμης του και την ολοκληρωτική αδυναμία εξυπηρέτησης νόμιμων αιτημάτων. Πέρα από τους περιορισμούς στη μνήμη, ο κατακλυσμός πακέτων προκαλεί υπερβολική κατανάλωση ενέργειας λόγω της συνεχούς επεξεργασίας και της διαχείρισης του φόρτου, μειώνοντας δραματικά τον συνολικό χρόνο ζωής του κόμβου και κατ' επέκταση ολόκληρου του δικτύου [1], [6].

Μια πιο εξεζητημένη απειλή αποτελεί η επίθεση Αποσυγχρονισμού (Desynchronization), κατά την οποία ο επιτιθέμενος παρεμβάλλεται σε μια υπάρχουσα ενεργή σύνδεση μεταξύ δύο νόμιμων κόμβων. Ο εισβολέας παραποιεί τις πληροφορίες ελέγχου, όπως τους αριθμούς ακολουθίας (sequence numbers), ή αποστέλλει πλαστά πακέτα με λανθασμένες παραμέτρους, αναγκάζοντας τους κόμβους να θεωρήσουν ότι η επικοινωνία έχει αποτύχει ή ότι τα δεδομένα χάθηκαν. Αυτό οδηγεί τους κόμβους-θύματα σε μια ατέρμονη και ενεργοβόρα διαδικασία επανεκπομπής πακέτων για τη διόρθωση του υποτιθέμενου σφάλματος. Όπως επισημαίνεται στη βιβλιογραφία, ο αποσυγχρονισμός δεν διακόπτει απλώς τη ροή των δεδομένων, αλλά λειτουργεί και ως μια έμμεση επίθεση εξάντλησης πόρων (Resource Exhaustion), καθώς οι κόμβοι αναλώνουν τα αποθέματα της μπαταρίας τους σε άσκοπες προσπάθειες αποκατάστασης μιας σύνδεσης που τελεί υπό τον έλεγχο του επιτιθέμενου [1], [14].

Ο μετριασμός των επιθέσεων κατακλυσμού στο επίπεδο μεταφοράς βασίζεται κυρίως στην τεχνική των παζλ-πρόκλησης (client puzzles), όπου ο κόμβος που λαμβάνει αίτημα σύνδεσης απαιτεί από τον αιτούντα να επιλύσει ένα υπολογιστικά κοστοβόρο πρόβλημα πριν δεσμεύσει πόρους. Με τον τρόπο αυτό, το κόστος μετατοπίζεται προς τον επιτιθέμενο, καθιστώντας ασύμφορη τη μαζική αποστολή αιτημάτων. Ωστόσο, η εφαρμογή τέτοιων μηχανισμών σε WSNs είναι προβληματική, καθώς η επίλυση των παζλ απαιτεί επεξεργαστική ισχύ που οι νόμιμοι κόμβοι χαμηλής κατανάλωσης δύσκολα διαθέτουν. Δημιουργείται έτσι ένα παράδοξο, όπου ο αμυντικός μηχανισμός επιβαρύνει το θύμα σχεδόν όσο και τον επιτιθέμενο. Η παρατήρηση αυτή ενισχύει το γενικότερο συμπέρασμα ότι οι αμυντικές τεχνικές που αναπτύχθηκαν για τα παραδοσιακά δίκτυα δεν μεταφέρονται αυτούσιες στα WSNs, αλλά απαιτούν ουσιαστική προσαρμογή στους ενεργειακούς τους περιορισμούς [1], [6].

Η αντιμετώπιση του αποσυγχρονισμού, από την άλλη, επιτυγχάνεται μέσω της αυθεντικοποίησης των πεδίων ελέγχου των πακέτων, ιδίως των αριθμών ακολουθίας και των σημαιών συγχρονισμού. Όταν

κάθε πληροφορία ελέγχου συνοδεύεται από έναν κωδικό αυθεντικοποίησης μηνύματος (Message Authentication Code), ο επιτιθέμενος αδυνατεί να παραποιήσει τα πεδία αυτά χωρίς να κατέχει το μυστικό κλειδί, με αποτέλεσμα ο αποσυγχρονισμός να καθίσταται ανέφικτος. Η λύση αυτή, ωστόσο, εισάγει επιπλέον υπολογιστικό φόρτο σε κάθε ανταλλαγή πακέτου, επιβεβαιώνοντας για άλλη μια φορά την κεντρική αντιστάθμιση μεταξύ ασφάλειας και κατανάλωσης ενέργειας. Συνολικά, η ανάλυση των επιθέσεων ανά επίπεδο της στοίβας καταδεικνύει ότι καμία άμυνα δεν είναι από μόνη της επαρκής: αντιθέτως, απαιτείται μια στρωματοποιημένη προσέγγιση (defense in depth) που συνδυάζει μηχανισμούς σε όλα τα επίπεδα, με συνειδητή διαχείριση του ενεργειακού κόστους που κάθε στρώμα προστασίας συνεπάγεται [1], [14].

2.3.6 Επιθέσεις Εξάντλησης Ενέργειας και Άρνησης Ύπνου

Στα δίκτυα με απεριόριστη τροφοδοσία, ο τελικός στόχος μιας επίθεσης άρνησης υπηρεσίας είναι η κατανάλωση εύρους ζώνης ή υπολογιστικών πόρων. Στα WSNs ο στόχος διαφοροποιείται ριζικά: το πραγματικό διακύβευμα είναι η μπαταρία. Πρόσφατη επισκόπηση αφιερωμένη ειδικά στις επιθέσεις εξάντλησης ενέργειας αναδεικνύει την κατηγορία αυτή ως αυτοτελές πεδίο μελέτης, διακριτό από τις κλασικές επιθέσεις άρνησης υπηρεσίας που καταγράφουν οι πρώιμες επισκοπήσεις ασφάλειας των WSNs [16], ακριβώς επειδή η μετρική επιτυχίας δεν είναι η στιγμιαία διακοπή αλλά η μη αναστρέψιμη μείωση του χρόνου ζωής του δικτύου [17].

Ο πλέον αποδοτικός μηχανισμός της κατηγορίας είναι η επίθεση άρνησης ύπνου (Denial-of-Sleep). Η ενεργειακή βιωσιμότητα ενός κόμβου στηρίζεται στον κύκλο λειτουργίας, δηλαδή στο γεγονός ότι ο πομποδέκτης παραμένει ανενεργός για ποσοστό που συχνά υπερβαίνει το 99% του χρόνου. Ένας επιτιθέμενος που εκπέμπει περιοδικά ελάχιστα πλαίσια, ακόμη και μη έγκυρα, υποχρεώνει τον κόμβο-θύμα να ενεργοποιεί τον δέκτη του και να εκτελεί επεξεργασία απόρριψης. Η ασυμμετρία κόστους είναι δραματική: με ενεργειακή δαπάνη μερικών χιλιοστών του συνολικού προϋπολογισμού του, ο επιτιθέμενος μπορεί να συντομεύσει τη ζωή του θύματος από έτη σε ημέρες. Κρίσιμο είναι ότι η επίθεση δεν παραβάλλει καμία κρυπτογραφική εγγύηση και, ως εκ τούτου, είναι εντελώς αόρατη σε μηχανισμούς που ελέγχουν αποκλειστικά την ακεραιότητα και την αυθεντικότητα των μηνυμάτων.

Η ίδια ενεργειακή λογική διέπει και τις σύγχρονες μορφές παρεμβολής. Συστηματική ανασκόπηση 62 μελετών σε δίκτυα συμβατά με IEEE 802.15.4 καταλήγει ότι η αντιδραστική παρεμβολή, δηλαδή η εκπομπή θορύβου μόνο κατά τη στιγμή ανίχνευσης νόμιμης μετάδοσης, επιτυγχάνει συγκρίσιμη διαταραχή με την αδιάλειπτη παρεμβολή καταναλώνοντας κλάσμα της ενέργειάς της. Η ίδια εργασία επισημαίνει ένα μεθοδολογικό πρόβλημα με άμεσες συνέπειες για τη συγκρισιμότητα των αποτελεσμάτων: οι δημοσιευμένες μελέτες χρησιμοποιούν ετερογενείς συμβάσεις μέτρησης της ενέργειας και, στην πλειονότητά τους, στηρίζονται αποκλειστικά σε προσομοίωση χωρίς επικύρωση σε πραγματικό υλικό [11].

Η παρατήρηση αυτή έχει μεθοδολογική σημασία για την παρούσα εργασία. Όταν η βιβλιογραφία αναφέρει ότι ένας αμυντικός μηχανισμός «μειώνει την κατανάλωση ενέργειας κατά x%», το νούμερο αυτό είναι ερμηνεύσιμο μόνο σε συνάρτηση με το μοντέλο ενέργειας, τον κύκλο λειτουργίας και τη ραδιοπλατφόρμα που χρησιμοποιήθηκαν. Η απουσία κοινού πλαισίου αναφοράς αποτελεί έναν από τους βασικούς λόγους για τους οποίους η συγκριτική αξιολόγηση του Κεφαλαίου 5 πρέπει να αντιμετωπίζεται ως ενδεικτική και όχι ως απόλυτη κατάταξη.

2.3.7 Επιθέσεις Πλευρικού Καναλιού και Παραβίαση Υλικού

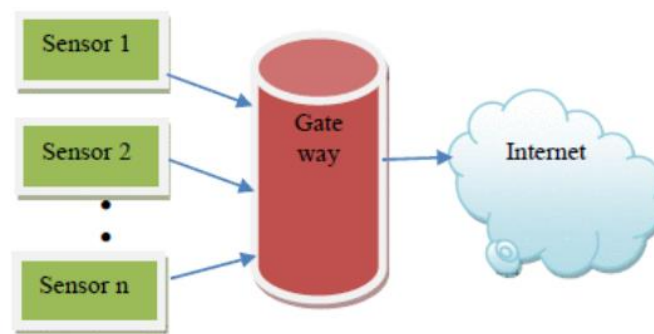
Οι επιθέσεις που εξετάστηκαν έως εδώ προϋποθέτουν ότι ο επιτιθέμενος αλληλεπιδρά με το δίκτυο μέσω του ασύρματου μέσου. Υπάρχει όμως μια κατηγορία απειλών που παρακάμπτει εντελώς αυτό το κανάλι, εκμεταλλευόμενη τη φυσική προσβασιμότητα των κόμβων που επισημάνθηκε στο Κεφάλαιο 1. Στις επιθέσεις πλευρικού καναλιού, ο επιτιθέμενος δεν επιχειρεί να σπάσει μαθηματικά τον αλγόριθμο κρυπτογράφησης, αλλά να συναγάγει το κλειδί από τις παρατηρήσιμες φυσικές εκδηλώσεις της εκτέλεσής του: την κατανάλωση ρεύματος, τον χρόνο εκτέλεσης ή την ηλεκτρομαγνητική ακτινοβολία του μικροελεγκτή.

Η ανάλυση διαφορικής ισχύος (DPA - Differential Power Analysis) αποτελεί την πιο μελετημένη τεχνική της κατηγορίας. Καταγράφοντας ένα πλήθος ιχνών κατανάλωσης κατά την εκτέλεση κρυπτογραφίσεων με διαφορετικά δεδομένα εισόδου και εφαρμόζοντας στατιστική συσχέτιση, ο επιτιθέμενος μπορεί να ανακτήσει το κλειδί ενός λογισμικού AES σε χρόνο που μετριέται σε λεπτά. Η ευπάθεια αυτή είναι ιδιαίτερα οξεία στα WSNs για δύο λόγους: οι κόμβοι είναι φυσικά προσβάσιμοι, οι υλοποιήσεις σε λογισμικό είναι ο κανόνας λόγω κόστους. Πρόσφατη πειραματική εργασία σε πλατφόρμα STM32L5 κατέδειξε ότι η μετάβαση από υλοποίηση AES σε λογισμικό σε επιταχυντή υλικού μειώνει σημαντικά την εκθεσιμότητα σε DPA, ενώ ταυτόχρονα βελτιώνει τον ενεργειακό απολογισμό, με προβλεπόμενη διάρκεια ζωής μπαταρίας που προσεγγίζει τα δεκατέσσερα έτη σε εφαρμογές παρακολούθησης υποδομών [18].

Το εύρημα αυτό είναι σημαντικό γιατί ανατρέπει μια διαδεδομένη παραδοχή. Η ασφάλεια και η ενεργειακή αποδοτικότητα παρουσιάζονται συνήθως ως αντικρουόμενοι στόχοι και η παρούσα εργασία θα επανέλθει στο δίλημμα αυτό. Στην περίπτωση όμως της κρυπτογραφικής επιτάχυνσης σε υλικό, οι δύο στόχοι συμβαδίζουν: η ίδια σχεδιαστική επιλογή ενισχύει την αντοχή σε πλευρικά κανάλια και μειώνει την κατανάλωση. Η γενικότερη διδαχή είναι ότι το ισοζύγιο ασφάλειας-ενέργειας δεν είναι μονοδιάστατο και εξαρτάται κρίσιμα από το επίπεδο στο οποίο υλοποιείται ο μηχανισμός προστασίας.

2.4 Ιδιαιτερότητες Ασφάλειας σε IoT-based WSNs

Η σύγκλιση των Ασύρματων Δικτύων Αισθητήρων (WSNs) με το IoT, δηλαδή το δίκτυο διασυνδεδεμένων αισθητήρων και «έξυπνων» συσκευών που συλλέγουν, ανταλλάσσουν και επεξεργάζονται δεδομένα μέσω του διαδικτύου, μετασχηματίζει τις παραδοσιακές αρχιτεκτονικές. Τα δεδομένα δεν περιορίζονται πλέον σε τοπική επεξεργασία, αλλά γίνονται προσβάσιμα παγκοσμίως, διευρύνοντας τη λειτουργικότητα και την αξία των συστημάτων. Ωστόσο, η διασύνδεση εκατομμυρίων ετερογενών συσκευών — όπως έξυπνα ρολόγια, αισθητήρες περιβάλλοντος, έξυπνες οικιακές συσκευές, κάμερες ασφαλείας και βιομηχανικοί αισθητήρες — αυξάνει εκθετικά το «πεδίο επίθεσης» (attack surface), καθιστώντας την ασφάλεια κρίσιμη για την υιοθέτηση τέτοιων συστημάτων. Οι ιδιαιτερότητες ασφάλειας σε αυτό το περιβάλλον επικεντρώνονται σε τρεις κύριους άξονες: την ανάγκη για ελαφριά κρυπτογραφία, την πολυπλοκότητα λόγω κλίμακας και τις απαιτήσεις κρίσιμων εφαρμογών όπως τα Smart Grids και η Γεωργία Ακριβείας. [6], [14].



Εικόνα 9 Incorporating Internet with WSN [6]

2.4.1 Περιορισμοί Πόρων και Ανάγκη για Lightweight Λύσεις

Σε αντίθεση με τα παραδοσιακά δίκτυα, οι κόμβοι στα IoT-based WSNs χαρακτηρίζονται από σοβαρή έλλειψη ενέργειας, υπολογιστικής ισχύος και μνήμης. Όπως επισημαίνεται στη βιβλιογραφία, η εφαρμογή συμβατικών κρυπτογραφικών αλγορίθμων, όπως ο RSA, θεωρείται συχνά μη πρακτική για αισθητήρες λόγω του υψηλού υπολογιστικού κόστους και των απαιτήσεων σε μνήμη RAM. Ως αποτέλεσμα, η έρευνα στρέφεται σε λύσεις όπως η Κρυπτογραφία Ελλειπτικής Καμπύλης (ECC - Elliptic Curve Cryptography), μια μορφή ασύμμετρης κρυπτογραφίας που βασίζεται σε μαθηματικές ιδιότητες των ελλειπτικών καμπυλών πάνω σε πεπερασμένα σώματα. Η ECC επιτρέπει την υλοποίηση μηχανισμών όπως η ανταλλαγή κλειδιών και η ψηφιακή υπογραφή με υψηλό επίπεδο ασφάλειας, χρησιμοποιώντας σημαντικά μικρότερα μεγέθη κλειδιών. Συγκεκριμένα, προσφέρει το ίδιο επίπεδο ασφάλειας με σημαντικά μικρότερο μέγεθος κλειδιού (π.χ. 160 bits έναντι 1024 bits του RSA), γεγονός που μειώνει δραματικά την ενέργεια που καταναλώνεται κατά τη διάρκεια των διεργασιών αυθεντικοποίησης και της ανταλλαγής κλειδιών. [1], [8].

2.4.2 Κλιμακωσιμότητα, Ετερογένεια και Κινητικότητα

Το οικοσύστημα του IoT απαιτεί από τα WSNs να διαχειρίζονται έναν τεράστιο αριθμό ετερογενών συσκευών που συχνά κινούνται με υψηλές ταχύτητες. Η δυναμική τοπολογία και η υψηλή κινητικότητα των κόμβων, όπως συμβαίνει στα Οχηματικά Δίκτυα (Vehicular Pattern WSNs - V-WSNs), καθιστούν τη διατήρηση μιας σταθερής στάσης ασφαλείας εξαιρετικά δύσκολη. Τα δίκτυα αυτά παρουσιάζουν μοναδικές προκλήσεις:

- **Δυναμική Μεταβολή Τοπολογίας:** Λόγω της συνεχούς κίνησης των οχημάτων, οι ασύρματοι σύνδεσμοι (links) είναι βραχύβιοι. Αυτό έχει ως αποτέλεσμα συχνούς διαμελισμούς και επανασυνδέσεις του δικτύου, καθιστώντας τα παραδοσιακά σχήματα ανταλλαγής κλειδιών αναποτελεσματικά, καθώς ο χρόνος που απαιτείται για την αυθεντικοποίηση μπορεί να υπερβαίνει τον χρόνο επαφής των δύο οχημάτων [9], [19].
- **Ανάγκη για Πρόβλεψη Θέσης (Sink Position Prediction):** Σε οχηματικά περιβάλλοντα, η ασφαλής δρομολόγηση εξαρτάται από την ακριβή γνώση της θέσης του κινητού σταθμού βάσης (Mobile Sink). Κακόβουλοι κόμβοι μπορούν να εκμεταλλευτούν την κινητικότητα για να εξαπολύσουν επιθέσεις "παραπλάνησης", στέλνοντας δεδομένα σε λανθασμένες κατευθύνσεις. Η χρήση τεχνικών

Μηχανικής και Βαθιάς Μάθησης κρίνεται απαραίτητη για την πρόβλεψη της κίνησης του Sink, διασφαλίζοντας ότι η πληροφορία θα φτάσει στον προορισμό της παρά την ταχύτητα μεταβολής του δικτύου [19].

- Διαχείριση Εμπιστοσύνης σε Πραγματικό Χρόνο: Λόγω της έλλειψης κεντρικής διακυβέρνησης στο δρόμο, τα οχήματα πρέπει να αξιολογούν την αξιοπιστία των μηνυμάτων που λαμβάνουν (π.χ. προειδοποιήσεις για ατύχημα). Ένας εισβολέας μπορεί να χρησιμοποιήσει μια επίθεση Sybil, δημιουργώντας δεκάδες πλαστές οντότητες οχημάτων για να προκαλέσει τεχνητή κυκλοφοριακή συμφόρηση ή να αλλοιώσει τους μηχανισμούς συναίνεσης του δικτύου [7], [20].
- V2V και V2I Επικοινωνία: Η ασφάλεια πρέπει να καλύπτει τόσο την επικοινωνία μεταξύ οχημάτων (Vehicle-to-Vehicle) όσο και με τις σταθερές υποδομές (Vehicle-to-Infrastructure), όπως οι έξυπνοι φωτεινοί σηματοδότες. Η ετερογένεια αυτή απαιτεί πρωτόκολλα που να εξισορροπούν την ανάγκη για χαμηλή καθυστέρηση (low latency) με την ισχυρή κρυπτογραφική αυθεντικοποίηση [6], [10].

2.4.3 Κρίσιμες Εφαρμογές

Μία από τις πλέον κρίσιμες εφαρμογές των IoT-WSNs είναι τα έξυπνα δίκτυα (Smart Grids), όπου η ασφάλεια συνδέεται άμεσα με την αξιοπιστία της ενεργειακής υποδομής. Σε αυτά τα συστήματα, η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικοποίησης είναι απαραίτητη για την προστασία των προσωπικών δεδομένων των καταναλωτών και την αποφυγή επιθέσεων DoS που θα μπορούσαν να οδηγήσουν σε διακοπές ρεύματος. αντίστοιχα, στη σύγχρονη γεωργία, η ενσωμάτωση μη επανδρωμένων αεροσκαφών (UAVs) για τη συλλογή δεδομένων από επίγεια WSNs δημιουργεί νέες προκλήσεις, καθώς η ασφάλεια της επικοινωνίας μεταξύ UAV και αισθητήρων είναι κρίσιμη για τη λήψη ορθών αποφάσεων παραγωγής [6], [14].

Η σύγκλιση των WSNs με το ευρύτερο οικοσύστημα του Διαδικτύου των Πραγμάτων (IoT) μεταβάλλει ριζικά το τοπίο των απειλών, καθώς οι κόμβοι παύουν να αποτελούν ένα απομονωμένο δίκτυο και καθίστανται άμεσα προσβάσιμοι μέσω του παγκόσμιου διαδικτύου. Η διασύνδεση αυτή, αν και προσφέρει τεράστια λειτουργική ευελιξία, εκθέτει τους ενεργειακά περιορισμένους αισθητήρες σε επιθέσεις που προέρχονται από οποιοδήποτε σημείο του πλανήτη, διευρύνοντας δραματικά την επιφάνεια επίθεσης. Χαρακτηριστικό παράδειγμα αποτελεί η αξιοποίηση εύαλτων συσκευών IoT για τη συγκρότηση δικτύων bot (botnets), τα οποία στη συνέχεια χρησιμοποιούνται για μαζικές κατανεμημένες επιθέσεις άρνησης υπηρεσίας. Επιπλέον, η ετερογένεια των συσκευών και των πρωτοκόλλων στο οικοσύστημα IoT δυσχεραίνει την επιβολή ενιαίων πολιτικών ασφάλειας, καθώς η ασφάλεια του συνολικού συστήματος καθορίζεται από τον πιο αδύναμο κρίκο του. Η πραγματικότητα αυτή επιβάλλει την υιοθέτηση μηχανισμών ασφάλειας από άκρο σε άκρο, που διασφαλίζουν την προστασία των δεδομένων σε ολόκληρη τη διαδρομή τους, από τον αισθητήρα έως την πλατφόρμα ανάλυσης στο νέφος [6], [7].

2.5 Μοντελοποίηση Απειλών και Προφίλ Επιτιθέμενου

Η συστηματική μελέτη της ασφάλειας ενός δικτύου αισθητήρων δεν μπορεί να περιοριστεί στην απαρτίωση μεμονωμένων επιθέσεων, αλλά απαιτεί την υιοθέτηση μιας δομημένης μεθοδολογίας μοντελοποίησης απειλών (threat modeling). Η μοντελοποίηση απειλών αποτελεί μια διαδικασία κατά την οποία ο σχεδιαστής ταυτοποιεί συστηματικά τα περιουσιακά στοιχεία του συστήματος που χρήζουν προστασίας, τους πιθανούς επιτιθέμενους, τις δυνατότητές τους και τα διαθέσιμα διανύσματα επίθεσης. Στο πλαίσιο των WSNs, τα κρίσιμα περιουσιακά στοιχεία περιλαμβάνουν όχι μόνο τα ίδια τα δεδομένα των αισθητήρων, αλλά και τα κρυπτογραφικά κλειδιά, την τοπολογία δρομολόγησης και την ενεργειακή εφεδρεία των κόμβων. Η ρητή καταγραφή αυτών των στοιχείων επιτρέπει την ιεράρχηση των

αμυντικών προτεραιοτήτων με βάση την αξία και την τρωτότητα κάθε στοιχείου. Χωρίς ένα τέτοιο μοντέλο, οι επενδύσεις σε ασφάλεια κινδυνεύουν να κατευθυνθούν σε δευτερεύουσες απειλές, αφήνοντας εκτεθειμένα τα πλέον κρίσιμα σημεία του συστήματος [10], [14].

Ένα θεμελιώδες κριτήριο ταξινόμησης των επιτιθέμενων αφορά τη θέση τους σε σχέση με το δίκτυο. Διακρίνονται έτσι οι εξωτερικοί επιτιθέμενοι (outsiders), οι οποίοι δεν διαθέτουν έγκυρα κρυπτογραφικά διαπιστευτήρια και επιχειρούν να παρεισφρήσουν από έξω και οι εσωτερικοί επιτιθέμενοι (insiders), οι οποίοι έχουν αποκτήσει τον έλεγχο νόμιμων κόμβων μέσω φυσικής παραβίασης. Οι εσωτερικοί επιτιθέμενοι είναι κατά κανόνα πολύ πιο επικίνδυνοι, καθώς κατέχουν έγκυρα κλειδιά και μπορούν να συμμετέχουν στα πρωτόκολλα του δικτύου ως φαινομενικά αξιόπιστες οντότητες. Η διάκριση αυτή είναι καθοριστική, διότι οι κρυπτογραφικοί μηχανισμοί που αποκλείουν αποτελεσματικά τους εξωτερικούς επιτιθέμενους αποδεικνύονται συχνά ανίσχυροι έναντι των εσωτερικών. Για τον λόγο αυτό, η σύγχρονη έρευνα συμπληρώνει την κρυπτογραφία με μηχανισμούς διαχείρισης εμπιστοσύνης και ανίχνευσης ανωμαλιών, ικανούς να εντοπίσουν την κακόβουλη συμπεριφορά ακόμη και νόμιμων κόμβων [14], [20].

Ένας δεύτερος άξονας διαφοροποίησης αφορά τις δυνατότητες και τους πόρους του επιτιθέμενου, που οδηγούν σε δύο ευρείες κατηγορίες μοντέλων:

Επιτιθέμενος τύπου mote-class: Διαθέτει υλικό αντίστοιχο με εκείνο των κόμβων του δικτύου, δηλαδή περιορισμένη ενέργεια, επεξεργαστική ισχύ και εμβέλεια εκπομπής. Οι επιθέσεις του είναι τοπικού χαρακτήρα και η εμβέλειά του περιορισμένη, γεγονός που τον καθιστά σχετικά ευκολότερο στην αντιμετώπιση μέσω κατανεμημένων μηχανισμών επιτήρησης [10], [14].

Επιτιθέμενος τύπου laptop-class: Διαθέτει σημαντικά ανώτερους πόρους, όπως ισχυρό επεξεργαστή, μεγάλη μνήμη, ισχυρή κεραία και ουσιαστικά απεριόριστη ενέργεια. Μπορεί να υποκλέψει ολόκληρο το δίκτυο, να εξαπολύσει επιθέσεις wormhole μεγάλης εμβέλειας και να επεξεργαστεί κρυπτογραφικά δεδομένα με ταχύτητες απρόσιτες για τους νόμιμους κόμβους. Η αντιμετώπιση αυτού του τύπου επιτιθέμενου απαιτεί ισχυρότερους κρυπτογραφικούς μηχανισμούς και συχνά υπερβαίνει τις δυνατότητες ενός αμιγώς αποκεντρωμένου δικτύου [10], [14].

Η αξία της μοντελοποίησης απειλών έγκειται στο ότι μετατρέπει τον σχεδιασμό ασφάλειας από μια αντιδραστική σε μια προληπτική διαδικασία. Αντί να προστίθενται αμυντικοί μηχανισμοί εκ των υστέρων, ως αντίδραση σε επιθέσεις που έχουν ήδη παρατηρηθεί, το μοντέλο απειλής επιτρέπει την πρόβλεψη των πιθανών διανυσμάτων επίθεσης κατά τη φάση του σχεδιασμού. Πλαίσια όπως το STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) — μια δομημένη μεθοδολογία κατηγοριοποίησης απειλών κατά κατηγορία —, αρχικά αναπτυγμένα για συστήματα λογισμικού, προσαρμόζονται σταδιακά στο πεδίο των WSNs, προσφέροντας μια συστηματική κατηγοριοποίηση των απειλών ανά τύπο. Παρά την αξία τους, τα πλαίσια αυτά πρέπει να εφαρμόζονται με κριτική διάθεση, λαμβάνοντας υπόψη τις ιδιαιτερότητες των ενεργειακά περιορισμένων δικτύων. Συμπερασματικά, η ενσωμάτωση της μοντελοποίησης απειλών στον κύκλο ανάπτυξης ενός WSNs αποτελεί προϋπόθεση για τον σχεδιασμό συστημάτων που είναι ασφαλή εκ κατασκευής (secure by design) και όχι απλώς θωρακισμένα εκ των υστέρων [14], [20].

2.6 Η Κβαντική Απειλή και το Μοντέλο «Harvest Now, Decrypt Later»

Το μοντέλο απειλών που περιγράφηκε στην προηγούμενη ενότητα αποτυπώνει τον επιτιθέμενο ως οντότητα που δρα στο παρόν. Υπάρχει ωστόσο μια κατηγορία απειλής της οποίας η υλοποίηση τοποθετείται στο μέλλον, ενώ η προετοιμασία της συντελείται ήδη σήμερα. Πρόκειται για τη στρατηγική «συλλογή τώρα, αποκρυπτογράφηση αργότερα» (HNDL - Harvest Now, Decrypt Later), κατά την οποία ο

αντίπαλος καταγράφει και αποθηκεύει κρυπτογραφημένη κίνηση χωρίς να μπορεί να την αποκρυπτογραφήσει, αναμένοντας τη διαθεσιμότητα κβαντικού υπολογιστή επαρκούς κλίμακας.

Η θεωρητική βάση της απειλής είναι γνωστή: ο αλγόριθμος του Shor επιλύει σε πολυωνυμικό χρόνο τα προβλήματα παραγοντοποίησης ακεραίων και διακριτού λογαρίθμου, στα οποία στηρίζονται τόσο το RSA όσο και η κρυπτογραφία ελλειπτικών καμπυλών. Η επίπτωση για τα WSNs είναι ιδιαίτερα σοβαρή, διότι, όπως αναλύεται στο Κεφάλαιο 3, η ECC έχει επικρατήσει ως η προτιμώμενη λύση ασύμμετρης κρυπτογραφίας για περιορισμένους πόρους ακριβώς λόγω των μικρών μεγεθών κλειδιού που προσφέρει. Ο αλγόριθμος του Grover, από την άλλη, υποδιπλασιάζει το αποτελεσματικό επίπεδο ασφάλειας των συμμετρικών σχημάτων, πράγμα που μεταφράζεται σε απαίτηση για κλειδιά AES των 256 bit εκεί όπου σήμερα θεωρούνται επαρκή τα 128.

Ο λόγος για τον οποίο η απειλή αυτή αφορά την παρούσα, όχι μια μελλοντική, μελέτη έγκειται σε ένα ιδιαίτερο χαρακτηριστικό των δικτύων αισθητήρων: τον κύκλο ζωής τους. Ένα δίκτυο παρακολούθησης δομικής ακεραιότητας γέφυρας ή ένα σύστημα μέτρησης σε έξυπνο δίκτυο ενέργειας σχεδιάζεται για λειτουργία δεκαπέντε ή είκοσι ετών, με κόμβους των οποίων το υλικολογισμικό συχνά δεν είναι πρακτικά αναβαθμίσιμο μετά την εγκατάσταση. Ένας κόμβος που εγκαθίσταται σήμερα με ECC-256 και δεν προβλέπει δυνατότητα κρυπτογραφικής ευελιξίας θα εξακολουθεί να λειτουργεί σε ένα περιβάλλον όπου το σχήμα αυτό θα έχει καταστεί παρωχημένο. Η απειλή, επομένως, δεν αφορά τον επιτιθέμενο του 2040 αλλά την απόφαση σχεδιασμού του 2026.

Η τυποποίηση των μετακβαντικών αλγορίθμων από το NIST τον Αύγουστο του 2024, με πρώτο το πρότυπο FIPS 203 για τον μηχανισμό ενθυλάκωσης κλειδιού ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), μετέτρεψε το ζήτημα από ερευνητικό σε μηχανικό [21]. Η μετάβαση όμως δεν είναι ούτε αυτόματη ούτε ανώδυνη για τους περιορισμένους κόμβους, όπως αναλύεται διεξοδικά στο Κεφάλαιο 3.

2.7 Επίλογος

Η ασφάλεια των Ασυρμάτων Δικτύων Αισθητήρων αποτελεί πολυδιάστατο και κρίσιμο ζήτημα, καθώς οι περιορισμένοι πόροι των κόμβων σε συνδυασμό με την έκθεση τους σε φυσικές και ψηφιακές απειλές καθιστούν τα δίκτυα αυτά ιδιαίτερα ευάλωτα. Η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα σε συνδυασμό με την αυθεντικοποίηση, παρέχει τη βασική θεωρητική βάση για την προστασία των δεδομένων, ενώ η ανάλυση των επιθέσεων ανά επίπεδο της στοίβας πρωτοκόλλων αναδεικνύει την πολυπλοκότητα των κινδύνων, από τις φυσικές παρεμβολές και τις συγκρούσεις στο επίπεδο συνδέσμου, έως τις στοχευμένες επιθέσεις δρομολόγησης όπως Sybil, Wormhole και Sinkhole. Η εξέλιξη των WSNs σε IoT-πλαίσια πολλαπλασιάζει το «πεδίο επίθεσης», απαιτώντας ελαφριά κρυπτογραφία, ευέλικτους μηχανισμούς αυθεντικοποίησης και προσαρμοστικότητα σε κλιμακούμενα, ετερογενή και κινητικά δίκτυα. Η προστασία των κρίσιμων εφαρμογών, όπως τα Smart Grids και η Γεωργία Ακριβείας, αναδεικνύει ότι η ασφάλεια δεν είναι απλώς τεχνικό ζήτημα, αλλά συνδέεται άμεσα με την αξιοπιστία και τη σταθερότητα υποδομών ζωτικής σημασίας για την κοινωνία και την οικονομία.

Κεφάλαιο 3ο: Μηχανισμοί και Πρωτόκολλα Ασφαλείας

3.1 Εισαγωγή

Στο παρόν κεφάλαιο εξετάζονται οι σύγχρονες κρυπτογραφικές τεχνικές που επιτρέπουν την ασφαλή επικοινωνία με το ελάχιστο δυνατό ενεργειακό κόστος, καθώς και τα μοντέλα διαχείρισης κλειδίων και εμπιστοσύνης που αποτελούν τη ραχοκοκαλιά της δικτυακής ασφάλειας. Επιπλέον, πραγματοποιείται εκτενής ανάλυση των σημαντικότερων πρωτοκόλλων ασφαλείας, όπως το SPINS και το πρότυπο ZigBee, ενώ παρουσιάζεται και ο ρόλος των Συστημάτων Ανίχνευσης Εισβολών (IDS) ως δεύτερη γραμμή άμυνας για την αναγνώριση ανωμαλιών και κακόβουλων συμπεριφορών στο πεδίο.

3.2 Κρυπτογραφικές Τεχνικές για Περιορισμένους Πόρους

Η παραδοσιακή ασφάλεια των πληροφοριών βασίζεται κατά κύριο λόγο στην κρυπτογραφία, η οποία διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικοποίηση των δεδομένων. Η κρυπτογραφία χωρίζεται σε δύο κύριες κατηγορίες: συμμετρική κρυπτογραφία, όπου ο ίδιος κωδικός (κλειδί) χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση και ασύμμετρη κρυπτογραφία, όπου χρησιμοποιούνται διαφορετικά κλειδιά για τις δύο διαδικασίες (δημόσιο και ιδιωτικό). Η κρυπτογραφία αποτελεί τον θεμέλιο λίθο για την επίτευξη της εμπιστευτικότητας και της ακεραιότητας στα WSNs. Ωστόσο, η επιλογή των αλγορίθμων είναι άρρηκτα συνδεδεμένη με την κατανάλωση ενέργειας και τη μνήμη των κόμβων. Η πρόκληση έγκειται στην εξεύρεση μιας ισορροπίας (trade-off) μεταξύ του επιπέδου ασφάλειας και της υπολογιστικής πολυπλοκότητας. [4], [6].

3.2.1 Συμμετρική Κρυπτογραφία

Η συμμετρική κρυπτογραφία (Lightweight Block Ciphers) αποτελεί τον ακρογωνιαίο λίθο της ασφάλειας στα WSNs, καθώς η υπολογιστική της αποδοτικότητα ευθυγραμμίζεται με τους περιορισμούς των μικροελεγκτών (π.χ. 8-bit ή 16-bit επεξεργαστές). Η χρήση ενός κοινού κλειδού επιτρέπει την εκτέλεση κρυπτογραφικών πράξεων με ελάχιστους κύκλους ρολογιού της CPU, κάτι που μεταφράζεται απευθείας σε εξοικονόμηση της πολύτιμης ενέργειας της μπαταρίας [3], [4].

Lightweight Block Ciphers και AES-128: Αν και ο AES-128 αποτελεί το χρυσό πρότυπο (de facto standard), στα WSNs χρησιμοποιούνται εξειδικευμένες "ελαφριές" (lightweight) υλοποιήσεις του. Η πρόκληση στον AES (Advanced Encryption Standard) έγκειται στην αποθήκευση των S-Boxes (Substitution Boxes) και των πινάκων lookup, οι οποίοι μπορούν να καταλάβουν σημαντικό μέρος της μνήμης RAM. Για τον λόγο αυτό, αναπτύσσονται αλγόριθμοι που χρησιμοποιούν λιγότερους γύρους κρυπτογράφησης ή μικρότερα μεγέθη block, διατηρώντας όμως την ανθεκτικότητα έναντι διαφορικής και γραμμικής κρυπτοανάλυσης [5], [22].

Λειτουργία CCM {Counter with CBC (Cipher Block Chaining) – Message Authentication Code} και Ακεραιότητα Δεδομένων: Η συμμετρική κρυπτογραφία στα WSNs δεν περιορίζεται στην απλή κρυπτογράφηση για εμπιστευτικότητα. Χρησιμοποιείται συχνά η λειτουργία CCM, η οποία συνδυάζει:

- CTR mode (Counter Mode): Για την κρυπτογράφηση, επιτρέποντας την παράλληλη επεξεργασία.
- CBC-MAC: Για την παραγωγή του Message Authentication Code, διασφαλίζοντας ότι το πακέτο δεν έχει αλλοιωθεί κατά τη διαδρομή. Αυτή η προσέγγιση είναι κρίσιμη για την αποτροπή επιθέσεων

έγχυσης πακέτων (packet injection), καθώς ο παραλήπτης μπορεί να επαληθεύσει την πηγή πριν επεξεργαστεί τα δεδομένα [4], [9].

Προκλήσεις Διανομής και Ανακατάληψης Κλειδιών (Key Revocation): Η μεγαλύτερη αδυναμία της συμμετρικής κρυπτογραφίας παραμένει η στατική φύση των κλειδιών σε πολλά απλά συστήματα. Εάν ένας εισβολέας αποκτήσει φυσική πρόσβαση σε έναν κόμβο (node compromise), μπορεί μέσω τεχνικών side-channel analysis να ανακτήσει το κλειδί από την EEPROM ή τη RAM [20]. Για να μετριαστεί αυτός ο κίνδυνος, εφαρμόζονται:

- Pairwise Keys: Μοναδικά κλειδιά ανά ζεύγος κόμβων, ώστε η παραβίαση ενός κόμβου να μην επηρεάζει το υπόλοιπο δίκτυο.
- Key Rotation: Τακτική ανανέωση των κλειδιών μέσω του Trust Center, μια διαδικασία που όμως αυξάνει το επικοινωνιακό overhead (overhead μηνυμάτων ελέγχου) [9], [22].

Η επιλογή του αλγορίθμου πρέπει να λαμβάνει υπόψη το "Trade-off" μεταξύ του μήκους του κλειδιού και του χρόνου ζωής του δικτύου. Η χρήση του Random Forest ή άλλων τεχνικών μηχανικής μάθησης στα IDS βοηθά στον εντοπισμό περιπτώσεων όπου κλειδιά έχουν διαρρεύσει, αναγνωρίζοντας ανωμαλίες στη συχνότητα και τη δομή της κρυπτογραφημένης κίνησης [23].

Η επιλογή ενός κατάλληλου κρυπτοαλγορίθμου (lightweight block cipher) να είναι ελαφρύς στην επεξεργαστική ισχύ, για τα WSNs δεν αποτελεί απλή υπόθεση, καθώς απαιτεί τη συνεκτίμηση πολλαπλών παραγόντων πέραν της καθαρής κρυπτογραφικής ισχύος. Αλγόριθμοι όπως οι PRESENT, SPECK και SIMON σχεδιάστηκαν εξ αρχής με γνώμονα την ελαχιστοποίηση του αποτυπώματος σε υλικό (hardware footprint) και την κατανάλωση ενέργειας, καθιστώντας τους ιδανικούς για ενσωματωμένα συστήματα. Ο PRESENT, για παράδειγμα, χρησιμοποιεί δομή υποκατάστασης-μετάθεσης με μικρό μέγεθος μπλοκ και απλές λογικές πράξεις, επιτρέποντας την υλοποίησή του με ελάχιστες λογικές πύλες. Οι αλγόριθμοι SIMON και SPECK, που αναπτύχθηκαν από την NSA, ακολουθούν διαφορετική φιλοσοφία σχεδίασης, βασισμένη σε μια ελαφριά δομή τύπου Feistel με απλές πράξεις (AND, XOR και κυκλικές ολισθήσεις) και σε πολλαπλά υποστηριζόμενα μεγέθη μπλοκ και κλειδιού. Ο SIMON είναι βελτιστοποιημένος για αποδοτική υλοποίηση σε υλικό (hardware), ενώ ο SPECK για ταχύτητα σε υλοποιήσεις λογισμικού (software), γεγονός που καθιστά το ζεύγος τους κατάλληλο για ευρύ φάσμα ενσωματωμένων συσκευών με διαφορετικούς περιορισμούς. Ωστόσο, η μείωση της πολυπλοκότητας δεν πρέπει να υπονομεύει την ασφάλεια· κάθε ελαφρύς αλγόριθμος οφείλει να έχει υποβληθεί σε ενδελεχή κρυπτανάλυση ώστε να διασφαλιστεί η ανθεκτικότητά του έναντι γνωστών επιθέσεων. Η ισορροπία μεταξύ απλότητας υλοποίησης και κρυπτογραφικής ασφάλειας αποτελεί το κεντρικό κριτήριο επιλογής στο πεδίο αυτό.

Πέρα από τον ίδιο τον αλγόριθμο, καθοριστική σημασία για την ασφάλεια έχει και η κατάσταση λειτουργίας (mode of operation) που επιλέγεται για την κρυπτογράφηση. Η απλή κατάσταση ηλεκτρονικού κωδικοβιβλίου (Electronic Codebook - ECB), στην οποία κάθε μπλοκ δεδομένων κρυπτογραφείται ανεξάρτητα με το ίδιο κλειδί και η οποία, αν και υπολογιστικά ελαφριά, είναι ανασφαλής καθώς αποκάλυπτει μοτίβα στα δεδομένα, ενώ καταστάσεις όπως η CTR mode ή CBC-MAC προσφέρουν ισχυρότερη προστασία με μικρή πρόσθετη επιβάρυνση. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι αυθεντικοποιημένες καταστάσεις κρυπτογράφησης (authenticated encryption), όπως η AES-CCM που υιοθετείται από το πρότυπο IEEE 802.15.4, καθώς παρέχουν ταυτόχρονα εμπιστευτικότητα και ακεραιότητα σε ένα ενιαίο πέρασμα. Η ενοποίηση αυτή είναι ιδιαίτερα ωφέλιμη για τα WSNs, διότι αποφεύγει την ανάγκη ξεχωριστών λειτουργιών για την κρυπτογράφηση και την αυθεντικοποίηση, εξοικονομώντας

πολύτιμους υπολογιστικούς και ενεργειακούς πόρους. Η σωστή επιλογή κατάστασης λειτουργίας αναδεικνύεται έτσι εξίσου σημαντική με την επιλογή του ίδιου του αλγορίθμου [3], [4].

3.2.2 Το Πρότυπο Ascon και η Τυποποίηση της Ελαφριάς Κρυπτογραφίας

Η ανάλυση της συμμετρικής κρυπτογραφίας που προηγήθηκε βασίζεται σε μεγάλο βαθμό στον AES και στις καταστάσεις λειτουργίας του. Επί δύο δεκαετίες, η επιλογή ενός κρυπτοαλγορίθμου για κόμβο αισθητήρα ήταν ουσιαστικά ένας συμβιβασμός: είτε χρήση του AES, σχεδιασμένου για επεξεργαστές γενικού σκοπού και όχι για μικροελεγκτές των 8 bit, είτε καταφυγή σε έναν από τους δεκάδες «ελαφρείς» αλγορίθμους της βιβλιογραφίας, οι οποίοι όμως δεν διέθεταν την κρυπτανάλυση και τη θεσμική στήριξη ενός προτύπου.

Το τοπίο αυτό μεταβλήθηκε ουσιαστικά τον Αύγουστο του 2025, με τη δημοσίευση από το NIST της ειδικής έκδοσης SP 800-232, η οποία τυποποιεί την οικογένεια Ascon ως πρότυπο ελαφριάς κρυπτογραφίας για περιορισμένες συσκευές [24]. Η οικογένεια περιλαμβάνει τον αλγόριθμο Ascon-AEAD128 για αυθεντικοποιημένη κρυπτογράφηση με συσχετισμένα δεδομένα, τη συνάρτηση κατακερματισμού Ascon-Hash256 και τις συναρτήσεις εκτεινόμενης εξόδου Ascon-XOF128 και Ascon-CXOF128. Η επιλογή του Ascon προέκυψε μετά από πολυετή διαγωνιστική διαδικασία στην οποία αξιολογήθηκαν πάνω από πενήντα υποψήφιοι.

Η σημασία της εξέλιξης αυτής για τα WSNs είναι πρακτική και όχι απλώς συμβολική. Πρώτον, το Ascon βασίζεται σε αρχιτεκτονική μετάθεσης-σφουγγαριού (sponge), η οποία επιτρέπει την υλοποίηση κρυπτογράφησης, αυθεντικοποίησης και κατακερματισμού με μία και μόνη κρυπτογραφική πρωτογενή συνάρτηση. Σε έναν κόμβο με 4 KB μνήμης RAM, όπως ο MicaZ του Πίνακα 1, η δυνατότητα να καλυφθούν και οι τρεις λειτουργίες χωρίς την ενσωμάτωση τριών ανεξάρτητων υλοποιήσεων συνιστά ουσιαστική εξοικονόμηση. Δεύτερον, η αυθεντικοποιημένη κρυπτογράφηση παρέχεται εγγενώς και όχι ως σύνθεση κρυπτογράφησης και MAC, εξαλείφοντας μια κατηγορία σφαλμάτων υλοποίησης που έχει ιστορικά ταλαιπωρήσει τα ενσωματωμένα συστήματα. Τρίτον, η δομή σφουγγαριού προσφέρεται για υλοποιήσεις με μάσκες που αντιστέκονται σε επιθέσεις πλευρικού καναλιού με σχετικά μικρή επιβάρυνση.

Σε σχέση με τα πρωτόκολλα που αναλύονται στη συνέχεια του κεφαλαίου, η τυποποίηση του Ascon επιτρέπει μια κριτική επανατοποθέτηση. Το TinySec και το SPINS σχεδιάστηκαν σε μια εποχή κατά την οποία δεν υπήρχε τυποποιημένη ελαφριά εναλλακτική στον AES, οι σχεδιαστικοί τους συμβιβασμοί, όπως η χρήση MAC μειωμένου μήκους, αντανakλούσαν ακριβώς αυτή την έλλειψη. Μια σύγχρονη επανασχεδίαση των ίδιων πρωτοκόλλων επί του Ascon θα μπορούσε να προσφέρει ισοδύναμη ή μεγαλύτερη ασφάλεια με μικρότερο αποτύπωμα, γεγονός που καθιστά την επικαιροποίηση των κλασικών πρωτοκόλλων ασφαλείας των WSNs ένα ώριμο και πρακτικά χρήσιμο ερευνητικό ζήτημα.

3.2.3 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία (ECC) ή Κρυπτογραφία Δημοσίου Κλειδιού (Public Key Cryptography - PKC) αποτελούσε παραδοσιακά το «απαγορευμένο» πεδίο για τα WSNs λόγω της τεράστιας υπολογιστικής επιβάρυνσης αλγορίθμων όπως ο RSA. Η ασφάλεια του RSA βασίζεται στο πρόβλημα της παραγοντοποίησης πρώτων αριθμών (Integer Factorization). Για να θεωρηθεί ασφαλής σήμερα, απαιτεί κλειδιά μεγέθους τουλάχιστον 1024 ή 2048 bits. Η διαδικασία κρυπτογράφησης και αυθεντικοποίησης στον RSA περιλαμβάνει σύνθετες πράξεις εκθετοποίησης (modular exponentiation) μεγάλων αριθμών. Οι πράξεις αυτές απαιτούν χιλιάδες κύκλους ρολογιού της CPU, τεράστια αποθέματα μνήμης RAM για τους ενδιάμεσους υπολογισμούς και, κατά συνέπεια, προκαλούν ταχεία εξάντληση της μπαταρίας των

κόμβων [4]. Η έλευση της Κρυπτογραφίας Ελλειπτικής Καμπύλης (ECC) αποτέλεσε σημείο καμπής, καθώς η ασφάλειά της βασίζεται στο πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες (ECDLP). Το πρόβλημα αυτό είναι μαθηματικά πολύ πιο δυσεπίλυτο από την παραγοντοποίηση του RSA, επιτρέποντας στην ECC να επιτυγχάνει την ίδια ισχύ προστασίας με εκθετικά μικρότερα κλειδιά [3].

Αποδοτικότητα Κλειδιών και Εξοικονόμηση Πόρων: Το κύριο πλεονέκτημα της ECC είναι η ικανότητά της να παρέχει το ίδιο επίπεδο ασφάλειας με πολύ μικρότερα κλειδιά. Όπως αναφέρεται στις πηγές [3] και [20], ένα κλειδί ECC 160-bit προσφέρει την ίδια προστασία με ένα κλειδί RSA 1024-bit. Αυτή η διαφορά συνεπάγεται:

- Λιγότερη κατανάλωση μνήμης: Πολύτιμη για συσκευές με περιορισμένη RAM και Flash.
- Ταχύτερη μετάδοση: Μικρότερα κλειδιά σημαίνουν λιγότερα πακέτα στον αέρα, άρα μικρότερη κατανάλωση ενέργειας από τη μονάδα επικοινωνίας.
- Χαμηλότερο υπολογιστικό κόστος: Οι πράξεις επί της ελλειπτικής καμπύλης (scalar multiplication) είναι πιο αποδοτικές για τους μικροελεγκτές των αισθητήρων [4].

Ανάλυση Ενεργειακού Κόστους και Handshake: Στην αναλυτική μελέτη της [4], η ενεργειακή βιωσιμότητα της ECC είναι πλέον δεδομένη. Η διαδικασία εγκαθίδρυσης σύνδεσης (handshake) μεταξύ ενός αισθητήρα και του Σταθμού Βάσης (Base Station) απαιτεί συνολικά 32,16 mJ. Η ενέργεια αυτή αναλύεται σε επιμέρους διεργασίες:

- Κρυπτογράφηση session key: 22,82 mJ.
- Αποστολή/Λήψη κλειδιών: 5,61 mJ.
- Αποκρυπτογράφηση μηνυμάτων επιβεβαίωσης: 3,73 mJ.

Οι τιμές αυτές αποδεικνύουν ότι η ECC μπορεί να χρησιμοποιηθεί όχι μόνο για την αρχική ανταλλαγή κλειδιών αλλά και για την περιοδική επαλήθευση της ταυτότητας των κόμβων χωρίς να εξαντλείται η μπαταρία τους [4].

Επίλυση του προβλήματος Διανομής Κλειδιών: Η ECC λύνει το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας: την ανάγκη για ασφαλή προ-εγκατάσταση κλειδιών. Μέσω πρωτοκόλλων όπως το ECDH (Elliptic Curve Diffie-Hellman), δύο κόμβοι μπορούν να δημιουργήσουν ένα κοινό μυστικό κλειδί συνεδρίας (session key) επικοινωνώντας μέσω ενός μη ασφαλούς καναλιού, χωρίς να έχουν μοιραστεί ποτέ τίποτα στο παρελθόν [10], [22].

Αυθεντικοποίηση και Μη Αποποίηση (Non-repudiation): Επιπλέον, η ECC επιτρέπει τη χρήση Ψηφιακών Υπογραφών (ECDSA). Αυτό είναι κρίσιμο για την προστασία από επιθέσεις κλοπής ταυτότητας (Identity Theft), καθώς κάθε κόμβος μπορεί να αποδείξει την ταυτότητά του χρησιμοποιώντας το ιδιωτικό του κλειδί. Η ιδιότητα της «μη αποποίησης» διασφαλίζει ότι ένας κόμβος δεν μπορεί να αρνηθεί την αποστολή ενός μηνύματος [4], [6].

Η επιλογή μεταξύ συμμετρικής και ασύμμετρης κρυπτογραφίας στα WSNs δεν συνιστά διαζευκτικό δίλημμα, αλλά μάλλον ζήτημα κατάλληλης αξιοποίησης του κάθε παραδείγματος στον ρόλο για τον οποίο είναι βέλτιστο. Η συμμετρική κρυπτογραφία, χάρη στο χαμηλό υπολογιστικό της κόστος, αποτελεί την προφανή επιλογή για την κρυπτογράφηση του κύριου όγκου των δεδομένων (bulk encryption)

που ανταλλάσσονται κατά τη λειτουργία του δικτύου. Αντίθετα, η ασύμμετρη κρυπτογραφία, ιδίως η κρυπτογραφία ελλειπτικών καμπυλών, ενδείκνυται για τις λειτουργίες αρχικής εγκαθίδρυσης εμπιστοσύνης και ανταλλαγής κλειδιών, οι οποίες εκτελούνται σπανιότερα και δικαιολογούν το αυξημένο τους κόστος. Η αρχιτεκτονική αυτή, που συνδυάζει ένα ασύμμετρο στρώμα για τη χειραψία και ένα συμμετρικό στρώμα για την επικοινωνία, αποτελεί το θεμέλιο των περισσότερων σύγχρονων ασφαλών πρωτοκόλλων και αντικατοπτρίζει τη γενικότερη φιλοσοφία της υβριδικής σχεδίασης που διέπει την ασφάλεια των περιορισμένων συστημάτων.

Ένα κρίσιμο αλλά συχνά παραγνωρισμένο στοιχείο της κρυπτογραφικής ασφάλειας στα WSNs είναι η ποιότητα της γεννήτριας τυχαίων αριθμών (Random Number Generator). Πολλές κρυπτογραφικές λειτουργίες, από τη δημιουργία κλειδιών έως την παραγωγή διανυσμάτων αρχικοποίησης, στηρίζονται στην υπόθεση ότι οι παραγόμενοι αριθμοί είναι πραγματικά απρόβλεπτοι. Στους περιορισμένους μικροελεγκτές των αισθητήρων, ωστόσο, η έλλειψη ισχυρών πηγών εντροπίας μπορεί να οδηγήσει σε προβλέψιμες ακολουθίες, υπονομεύοντας ακόμη και τον ισχυρότερο αλγόριθμο. Επιθέσεις που εκμεταλλεύονται αδύναμες γεννήτριες τυχαίων αριθμών έχουν αποδειχθεί ιδιαίτερα καταστροφικές, καθώς επιτρέπουν την ανακατασκευή μυστικών κλειδιών χωρίς την ανάγκη επίθεσης ωμής βίας. Για τον λόγο αυτό, η σύγχρονη έρευνα στρέφεται προς την αξιοποίηση φυσικών πηγών εντροπίας, όπως ο θόρυβος των ίδιων των αισθητήρων ή οι διακυμάνσεις του ραδιοκαναλιού, για την παραγωγή κρυπτογραφικά ισχυρής τυχαιότητας απευθείας από το περιβάλλον λειτουργίας [3], [22].

3.2.4 Μετακβαντική Κρυπτογραφία σε Δίκτυα Περιορισμένων Πόρων

Η ανάλυση της ασύμμετρης κρυπτογραφίας κατέδειξε ότι η ECC αποτελεί σήμερα την πρακτικά μοναδική βιώσιμη επιλογή για κόμβους αισθητήρων, χάρη στα μικρά μεγέθη κλειδιού που προσφέρει για δεδομένο επίπεδο ασφάλειας. Το πλεονέκτημα αυτό όμως στηρίζεται εξ ολοκλήρου στη δυσκολία του προβλήματος του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες, δηλαδή ακριβώς στο πρόβλημα που ο αλγόριθμος του Shor επιλύει αποδοτικά. Η μετάβαση σε μετακβαντική κρυπτογραφία (PQC - Post-Quantum Cryptography) δεν είναι, συνεπώς, ζήτημα προαιρετικής ενίσχυσης αλλά αντικατάστασης θεμελίου.

Τα τυποποιημένα από το NIST σχήματα βασίζονται κατά κύριο λόγο σε δομημένα πλέγματα. Το ML-KEM, που τυποποιείται στο FIPS 203, είναι μηχανισμός ενθυλάκωσης κλειδιού βασισμένος σε πλέγματα ενοτήτων και προορίζεται να αντικαταστήσει τις ανταλλαγές κλειδιού τύπου Diffie-Hellman [21]. Από υπολογιστική άποψη, τα σχήματα πλεγμάτων είναι ευνοϊκά για ενσωματωμένα συστήματα, καθώς οι πράξεις τους ανάγονται σε πολλαπλασιασμούς πολυωνύμων με ακέραιους συντελεστές και όχι σε αριθμητική μεγάλων ακεραίων· ο χρόνος εκτέλεσης μπορεί έτσι να είναι συγκρίσιμος ή και καλύτερος από εκείνον της ECC.

Το πραγματικό εμπόδιο δεν είναι ο χρόνος αλλά το μέγεθος. Ενώ ένα δημόσιο κλειδί ECC στα 256 bit καταλαμβάνει 32 bytes, το αντίστοιχο κλειδί ML-KEM στο επίπεδο ασφάλειας 1 προσεγγίζει τα 800 bytes και το κρυπτόγραμμα υπερβαίνει τα 760 bytes. Σε ένα πλαίσιο IEEE 802.15.4 με ωφέλιμο φορτίο περίπου 100 bytes, τούτο σημαίνει ότι μια απλή ανταλλαγή κλειδιού απαιτεί κατάτμηση σε δεκάδες πακέτα. Δεδομένου ότι η μετάδοση αποτελεί τη δαπανηρότερη ενεργειακά λειτουργία του κόμβου, το κόστος μιας μετακβαντικής χειραψίας μπορεί να υπερβαίνει κατά τάξη μεγέθους εκείνο της αντίστοιχης χειραψίας ECC. Το πρόβλημα, δηλαδή, μετατοπίζεται από την επεξεργασία στην επικοινωνία, γεγονός που αντιστρέφει τις παραδοσιακές παραδοχές βελτιστοποίησης των πρωτοκόλλων ασφαλείας για WSNs.

Πρόσφατη ερευνητική πρόταση αντιμετωπίζει το ζήτημα μέσω προσαρμοστικής αρχιτεκτονικής: κρυπτογράφηση βασισμένη σε πλέγματα χρησιμοποιείται αποκλειστικά για την εγκαθίδρυση κλειδιών, ενώ η τρέχουσα προστασία των δεδομένων ανατίθεται σε ελαφρές συμμετρικές πρωτογενείς συναρτήσεις, με τις κρυπτογραφικές παραμέτρους να ρυθμίζονται δυναμικά ανάλογα με τις συνθήκες του δικτύου και το εναπομείναν ενεργειακό απόθεμα. Η πειραματική αποτίμηση του πλαισίου αναφέρει μείωση της κατανάλωσης ενέργειας κατά 14% έναντι στατικών προσεγγίσεων, με αξιοποίηση επεξεργαστή που παραμένει κάτω από 24% [25]. Ανάλογη λογική ακολουθεί και το πλαίσιο ZT-IoTrust, το οποίο συνδυάζει μετακβαντικά πρωτόκολλα βασισμένα σε προβλήματα πλεγμάτων με ομόσπονδη μάθηση για τον έλεγχο πρόσβασης, αναφέροντας ποσοστό ανίχνευσης επιθέσεων 92,5% με 1,2% ψευδώς θετικά [26].

Η ρεαλιστική διαχείριση της μετάβασης δεν έγκειται πάντως στην άμεση καθολική αντικατάσταση αλλά στην αρχή της κρυπτογραφικής ευελιξίας. Ένας κόμβος που σχεδιάζεται σήμερα οφείλει να επιτρέψει την αντικατάσταση των κρυπτογραφικών του πρωτογενών συναρτήσεων μέσω ασφαλούς ενημέρωσης υλικολογισμικού, ακόμη και αν αρχικά αναπτυχθεί με ECC. Η μεταβατική πρακτική των υβριδικών σχημάτων, όπου το τελικό κλειδί προκύπτει από συνδυασμό κλασικής και μετακβαντικής ανταλλαγής, εξασφαλίζει ότι η συνολική ασφάλεια δεν υποβαθμίζεται ούτε αν ανακαλυφθεί αδυναμία στους νέους αλγορίθμους ούτε αν καταστεί διαθέσιμος κβαντικός υπολογιστής.

3.3 Διαχείριση Κλειδιών και Μοντέλα Εμπιστοσύνης

Η διαχείριση κλειδιών αποτελεί μία από τις μεγαλύτερες προκλήσεις στα WSNs, καθώς πρέπει να εξασφαλίζει την ασφαλή εγκαθίδρυση επικοινωνίας μεταξύ των κόμβων χωρίς να επιβαρύνει υπερβολικά τους περιορισμένους πόρους τους. Οι στρατηγικές διανομής κλειδιών χωρίζονται σε τρεις κύριες κατηγορίες: την προ-εγκατάσταση κλειδιών (key pre-distribution), τη δυναμική παραγωγή μέσω έμπιστων τρίτων οντοτήτων και τη χρήση ασύμμετρων αλγορίθμων. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι τεχνικές αυθαίρετης ανάπτυξης κλειδιών (arbitrary key-deployment), οι οποίες χρησιμοποιούν απλή θεωρία συνόλων για να δημιουργήσουν κοινά κλειδιά μεταξύ γειτονικών κόμβων, μειώνοντας δραματικά την πολυπλοκότητα χρόνου και τον απαιτούμενο χώρο αποθήκευσης. Η χρήση τέτοιων μοντέλων, όπως το MLKS (Multi Level Key Security), επιτρέπει την ανανέωση των κλειδιών μετά από κάθε επικοινωνία (volatility), προστατεύοντας το δίκτυο από τη χρήση "μπαγιάτικων" (stale) κλειδιών που θα μπορούσαν να υποκλαπούν από έναν εισβολέα [1], [22].

Παράλληλα με την κρυπτογραφία, η εισαγωγή Μοντέλων Εμπιστοσύνης (Trust Models) είναι απαραίτητη για την αντιμετώπιση εσωτερικών απειλών, όπου ένας νόμιμος κόμβος παραβιάζεται και αρχίζει να συμπεριφέρεται κακόβουλα. Τα μοντέλα εμπιστοσύνης λειτουργούν συμπληρωματικά με τα πρωτόκολλα ασφαλείας, αξιολογώντας τη συμπεριφορά κάθε κόμβου με βάση παραμέτρους όπως ο ρυθμός παράδοσης πακέτων (PDR - Packet Delivery Ratio) και η ακεραιότητα των δεδομένων. Όπως επισημαίνεται στην [7], ο συνδυασμός κρυπτογραφικής αυθεντικοποίησης και αλγορίθμων εμπιστοσύνης, όπως ο ASSFO (Artificial Shark Swarm Optimization), ενισχύει την ασφάλεια του δικτύου. Ο αλγόριθμος αυτός, εμπνευσμένος από τη συμπεριφορά αναζήτησης τροφής των καρχαριών, χρησιμοποιείται στα WSNs για την αξιολόγηση της αξιοπιστίας των κόμβων σε πραγματικό χρόνο. Μέσω της ανάλυσης παραμέτρων όπως η ενέργεια του κόμβου και η συνέπεια στην προώθηση πακέτων, ο ASSFO επιτρέπει την επιλογή των πιο αξιόπιστων μονοπατιών δρομολόγησης, απομονώνοντας κόμβους που εκτελούν επιθέσεις τύπου Sinkhole ή Blackhole. Η ολιστική αυτή προσέγγιση διασφαλίζει ότι ακόμη και αν ένας εισβολέας παρακάμψει την κρυπτογράφηση, η κακόβουλη δράση του θα ανιχνευθεί μέσω της πτώσης του επιπέδου εμπιστοσύνης του στο δίκτυο [7], [19].

Το πρόβλημα της αρχικής εγκαθίδρυσης εμπιστοσύνης, γνωστό ως bootstrapping, αποτελεί την πλέον θεμελιώδη πρόκληση της διαχείρισης κλειδιών στα WSNs. Καθώς οι κόμβοι αναπτύσσονται συχνά σε μη ελεγχόμενα περιβάλλοντα χωρίς προηγούμενη γνώση των γειτόνων τους, πρέπει να καθιερώσουν ασφαλείς διαύλους επικοινωνίας χωρίς την παρουσία μιας έμπιστης κεντρικής αρχής κατά τη φάση λειτουργίας. Η πλέον διαδεδομένη απάντηση σε αυτό το πρόβλημα είναι το σχήμα προ-διανομής κλειδιών τύπου Eschenauer–Gligor, κατά το οποίο κάθε κόμβος εφοδιάζεται πριν την ανάπτυξη με ένα τυχαίο υποσύνολο κλειδιών αντλημένο από μια μεγαλύτερη δεξαμενή (key pool). Δύο γειτονικοί κόμβοι μπορούν να επικοινωνήσουν ασφαλώς εφόσον μοιράζονται τουλάχιστον ένα κοινό κλειδί, ενώ η πιθανότητα αυτή ρυθμίζεται από το μέγεθος της δεξαμενής και του υποσυνόλου. Η προσέγγιση αυτή προσφέρει εξαιρετική κλιμακωσιμότητα και ανθεκτικότητα, καθώς η παραβίαση ενός κόμβου αποκαλύπτει μόνο ένα μικρό κλάσμα των συνολικών κλειδιών του δικτύου [1], [22].

Η αξιολόγηση κάθε σχήματος διαχείρισης κλειδιών στηρίζεται σε ένα σύνολο ανταγωνιστικών κριτηρίων, τα οποία σπανίως μπορούν να ικανοποιηθούν ταυτόχρονα στο σύνολό τους:

Ανθεκτικότητα (Resilience): Εκφράζει τον βαθμό στον οποίο η παραβίαση ενός ή περισσότερων κόμβων εκθέτει την επικοινωνία των υπολοίπων. Ένα ανθεκτικό σχήμα διασφαλίζει ότι τα κλειδιά ενός παραβιασμένου κόμβου δεν αποκαλύπτουν τις συνεδρίες τρίτων κόμβων [1], [22].

Κλιμακωσιμότητα (Scalability): Αφορά την ικανότητα του σχήματος να υποστηρίζει την προσθήκη νέων κόμβων χωρίς δυσανάλογη αύξηση των αποθηκευτικών ή υπολογιστικών απαιτήσεων, ζήτημα κρίσιμο για δίκτυα χιλιάδων κόμβων.

Αποτύπωμα Μνήμης (Storage Overhead): Εκφράζει τον αριθμό των κλειδιών που πρέπει να αποθηκεύει κάθε κόμβος. Δεδομένης της περιορισμένης μνήμης των αισθητήρων, η ελαχιστοποίηση του αποτυπώματος αυτού αποτελεί πρωταρχικό σχεδιαστικό στόχο [22].

Η σύγκριση των διαφόρων σχημάτων αναδεικνύει ότι δεν υπάρχει καθολικά βέλτιστη λύση, αλλά μόνο επιλογές κατάλληλες για συγκεκριμένα σενάρια. Τα σχήματα προ-διανομής υπερτερούν σε ενεργειακή αποδοτικότητα αλλά υστερούν σε τέλεια ανθεκτικότητα, ενώ οι προσεγγίσεις που βασίζονται σε δημόσιο κλειδί προσφέρουν ισχυρότερες εγγυήσεις με κόστος αυξημένης υπολογιστικής επιβάρυνσης. Η επιλογή του κατάλληλου σχήματος συνιστά συνεπώς μια απόφαση που εξαρτάται από το μοντέλο απειλής, την αναμενόμενη πυκνότητα του δικτύου και την ενεργειακή του αυτονομία. Η τάση της σύγχρονης έρευνας κινείται προς υβριδικά σχήματα που συνδυάζουν την αποδοτικότητα της συμμετρικής προ-διανομής με την ευελιξία περιορισμένων ασύμμετρων λειτουργιών, επιχειρώντας να αξιοποιήσουν τα πλεονεκτήματα και των δύο κόσμων [1], [22].

Η έννοια της εμπιστοσύνης στα WSNs διαφοροποιείται θεμελιωδώς από εκείνη των παραδοσιακών δικτύων, καθώς δεν μπορεί να βασιστεί αποκλειστικά σε στατικά διαπιστευτήρια ή σε μια κεντρική αρχή πιστοποίησης. Αντίθετα, η εμπιστοσύνη πρέπει να οικοδομείται και να συντηρείται δυναμικά, μέσα από τη συνεχή παρατήρηση της συμπεριφοράς των κόμβων. Τα μοντέλα εμπιστοσύνης που έχουν προταθεί διακρίνονται σε δύο βασικές κατηγορίες: τα άμεσα μοντέλα, όπου κάθε κόμβος αξιολογεί τους γείτονές του με βάση τις δικές του παρατηρήσεις και τα έμμεσα ή φημολογικά μοντέλα, όπου η αξιολόγηση ενός κόμβου προκύπτει και από τις συστάσεις τρίτων. Ο συνδυασμός των δύο προσεγγίσεων προσφέρει μεγαλύτερη ακρίβεια αλλά εισάγει και την ευπάθεια σε επιθέσεις δυσφήμισης, όπου κακόβουλοι κόμβοι διαδίδουν ψευδείς αρνητικές συστάσεις για νόμιμους γείτονες. Η σχεδίαση ανθεκτικών μοντέλων εμπιστοσύνης, ικανών να φιλτράρουν τις παραπλανητικές συστάσεις και να προσαρμόζονται σε μεταβαλλόμενες συνθήκες, παραμένει ένα ενεργό ερευνητικό πεδίο με άμεση πρακτική σημασία για την αυτονομία και την ανθεκτικότητα των δικτύων [1], [22].

Η επιλογή του κατάλληλου μοντέλου εμπιστοσύνης επηρεάζει καθοριστικά τη συνολική ανθεκτικότητα του δικτύου. Στα καταμετρημένα μοντέλα, όπου κάθε κόμβος αξιολογεί αυτόνομα την αξιοπιστία των γειτόνων του, η απουσία ενός κεντρικού σημείου αποτυχίας ενισχύει την ανθεκτικότητα, αλλά εισάγει την πρόκληση της συνέπειας: διαφορετικοί κόμβοι ενδέχεται να καταλήγουν σε αντιφατικές εκτιμήσεις για τον ίδιο γείτονα. Αντίθετα, τα ιεραρχικά μοντέλα, όπου οι επικεφαλής των συστάδων συγκεντρώνουν και συνθέτουν τις εκτιμήσεις εμπιστοσύνης, προσφέρουν μεγαλύτερη συνέπεια αλλά δημιουργούν προνομιακούς στόχους επίθεσης. Ιδιαίτερη μέριμνα απαιτείται για την αντιμετώπιση συνεργατικών επιθέσεων κατά των ίδιων των συστημάτων φήμης, όπως οι επιθέσεις δυσφήμισης (badmouthing), κατά τις οποίες ομάδες κακόβουλων κόμβων συνασπίζονται για να υποβαθμίσουν ψευδώς τη φήμη ενός νόμιμου κόμβου. Η σχεδίαση ανθεκτικών μηχανισμών εμπιστοσύνης, ικανών να αντιστέκονται σε τέτοιες συντονισμένες επιθέσεις, αποτελεί ενεργό πεδίο έρευνας με άμεση πρακτική σημασία για την αξιοπιστία των αυτο-οργανούμενων δικτύων [10], [14].

3.4 Ανάλυση Πρωτοκόλλων Ασφαλείας

Η θεωρητική ανάλυση των μηχανισμών ασφαλείας μετουσιώνεται σε πρακτικές λύσεις μέσω των πρωτοκόλλων ασφαλείας, τα οποία καθορίζουν τους κανόνες ανταλλαγής πληροφοριών με προστασία έναντι επιθέσεων. Λόγω της εγγενούς αδυναμίας των WSNs να υποστηρίζουν τα κλασικά πρωτόκολλα του διαδικτύου (όπως το IPsec ή το SSL/TLS), η ερευνητική κοινότητα ανέπτυξε λύσεις που ελαχιστοποιούν το υπολογιστικό και επικοινωνιακό overhead. Τα πρωτόκολλα αυτά ενσωματώνουν μηχανισμούς για την επίτευξη εμπιστευτικότητας, αυθεντικοποίησης και φρεσκάδας δεδομένων (data freshness), διασφαλίζοντας ότι παλαιότερα μηνύματα δεν μπορούν να χρησιμοποιηθούν σε επιθέσεις επανάληψης (replay attacks) [1], [4].

Η επιλογή του κατάλληλου πρωτοκόλλου εξαρτάται από την εφαρμογή, καθώς διαφορετικές απαιτήσεις παρουσιάζει ένα δίκτυο παρακολούθησης σε ένα Smart Grid και διαφορετικές ένα σύστημα Γεωργίας Ακρίβειας που υποστηρίζεται από UAVs [1], [14].

3.4.1 Πρωτόκολλο SPINS

Η σουίτα πρωτοκόλλων SPINS (Security Protocols for Sensor Networks) σχεδιάστηκε για να παρέχει ένα ολοκληρωμένο πλαίσιο ασφαλείας, βελτιστοποιημένο για τις περιορισμένες δυνατότητες των αισθητήρων. Η καινοτομία της έγκειται στον διαχωρισμό της επικοινωνίας σε δύο μοντέλα: την άμεση επικοινωνία (unicast) και την εκπομπή προς πολλούς (broadcast) [1], [27].

SNEP: (Sensor Network Encryption Protocol) επιτυγχάνει τρεις βασικούς στόχους, την εμπιστευτικότητα, την αυθεντικοποίηση και τη φρεσκάδα των δεδομένων με Μηδενικό Overhead [3].

- Μηχανισμός Counter: Αντί για την αποστολή τυχαίων διανυσμάτων (Initialization Vector - IV) που θα επιβάρυναν το μέγεθος του πακέτου, ο αποστολέας και ο παραλήπτης διατηρούν έναν εσωτερικό μετρητή (counter). Κάθε φορά που ανταλλάσσεται ένα μήνυμα, ο μετρητής αυξάνεται. Αυτό διασφαλίζει ότι ακόμα και αν το ίδιο κείμενο κρυπτογραφηθεί δύο φορές, το αποτέλεσμα θα είναι διαφορετικό.
- Προστασία Replay: Επειδή ο παραλήπτης δέχεται μόνο μηνύματα με μετρητή μεγαλύτερο από τον προηγούμενο, οι επιθέσεις επανάληψης (replay attacks) καθίστανται αδύνατες.

- Message Authentication Code και Αυθεντικοποίηση: Το SNEP χρησιμοποιεί έναν κωδικό Message Authentication Code για να επαληθεύσει ότι το πακέτο προέρχεται από τον νόμιμο κάτοχο του κλειδιού, διασφαλίζοντας την ακεραιότητα [1], [4].

μTESLA: αποτελεί την απάντηση στο πρόβλημα της αυθεντικοποιημένης εκπομπής (broadcast authentication). Ενώ η ασύμμετρη κρυπτογραφία (ψηφιακές υπογραφές) είναι πολύ βαριά για τους αισθητήρες, το μTESLA δημιουργεί μια «τεχνητή ασυμμετρία» χρησιμοποιώντας τον χρόνο [1], [27].

- Αλυσίδα Κλειδιών (Key Chain): Ο Σταθμός Βάσης δημιουργεί μια αλυσίδα κλειδιών χρησιμοποιώντας μια συνάρτηση κατακερματισμού (one-way hash function). Τα κλειδιά αποκαλύπτονται με την αντίστροφη σειρά.
- Delayed Key Disclosure: Όταν ο Σταθμός Βάσης στέλνει ένα μήνυμα, το υπογράφει με ένα κλειδί K_i το οποίο δεν έχει αποκαλύψει ακόμα. Οι αισθητήρες αποθηκεύουν το μήνυμα προσωρινά. Μετά από ένα προκαθορισμένο χρονικό διάστημα (time slot), ο Σταθμός Βάσης δημοσιεύει το κλειδί K_i .
- Επαλήθευση: Οι αισθητήρες, έχοντας λάβει το κλειδί, επαληθεύουν την εγκυρότητά του (συσχετίζοντάς το με το προηγούμενο γνωστό κλειδί της αλυσίδας) και στη συνέχεια αυθεντικοποιούν το αποθηκευμένο μήνυμα. Αυτός ο μηχανισμός διασφαλίζει ότι κανένας εισβολέας δεν μπορεί να παραιοποιήσει το μήνυμα όσο αυτό βρίσκεται "στον αέρα", καθώς δεν κατέχει ακόμα το κλειδί [1], [4].

Συμπερασματικά, το SPINS αποδεικνύει ότι η ασφάλεια στα WSNs δεν απαιτεί απαραίτητα περίπλοκους μαθηματικούς υπολογισμούς, αλλά μπορεί να επιτευχθεί μέσω έξυπνου σχεδιασμού των πρωτοκόλλων επικοινωνίας. Στην αναφορά [4], η στοιβα πρωτοκόλλων που υποστηρίζει το SPINS είναι η βάση για τη διαχείριση της ενέργειας και της ασφάλειας σε κρίσιμα περιβάλλοντα [1], [10].

Παρά τη σχεδιαστική του κομψότητα, το πρωτόκολλο SPINS παρουσιάζει ορισμένους πρακτικούς περιορισμούς που αναδείχθηκαν κατά την εφαρμογή του. Ο μηχανισμός μTESLA, αν και αποδοτικός, εισάγει μια εγγενή καθυστέρηση στην αυθεντικοποίηση, καθώς ο παραλήπτης πρέπει να αναμείνει την αποκάλυψη του κλειδιού στο επόμενο χρονικό διάστημα πριν επαληθεύσει το μήνυμα. Η καθυστέρηση αυτή μπορεί να είναι ανεκτή σε εφαρμογές περιοδικής παρακολούθησης, αλλά καθίσταται προβληματική σε σενάρια που απαιτούν άμεση αντίδραση σε πραγματικό χρόνο. Επιπλέον, η ανάγκη χαλαρού συγχρονισμού των ρολογιών μεταξύ των κόμβων εισάγει μια πρόσθετη ευπάθεια, καθώς επιθέσεις που στοχεύουν στον συγχρονισμό του χρόνου μπορούν να υπονομεύσουν την ορθή λειτουργία του μηχανισμού. Οι περιορισμοί αυτοί δεν αναιρούν την πρωτοποριακή συνεισφορά του SPINS, αλλά υπογραμμίζουν ότι κάθε σχεδιαστική επιλογή στα WSNs συνοδεύεται από συγκεκριμένες αντισταθμίσεις που πρέπει να αξιολογούνται στο πλαίσιο της εκάστοτε εφαρμογής [1], [4].

3.4.2 Πρωτόκολλο TinySec και LEAP+

Το TinySec και το LEAP+ αποτελούν δύο συμπληρωματικές λύσεις που καλύπτουν διαφορετικές ανάγκες στο επίπεδο της ασφάλειας των WSNs: το TinySec εξασφαλίζει την προστασία των δεδομένων κατά τη μετάδοση (data-in-transit), ενώ το LEAP+ διαχειρίζεται το κρίσιμο ζήτημα της διανομής και οργάνωσης των κλειδιών [1].

Το TinySec αντικαθιστά το τυπικό πακέτο του TinyOS με μια ασφαλή δομή, η οποία παρά την προσθήκη κρυπτογραφικών στοιχείων, διατηρεί το overhead σε χαμηλά επίπεδα (μόλις 5 επιπλέον bytes ανά πακέτο) [4].

- Μηχανισμοί Ασφάλειας: Χρησιμοποιεί τον αλγόριθμο Skipjack σε λειτουργία CBC-MAC με διανύσματα αρχικοποίησης (IV) 8-bit. Αυτό διασφαλίζει ότι ακόμα και πανομοιότυπα πακέτα παράγουν διαφορετικά κρυπτογραφημένα κείμενα.
- TinySec-Auth vs TinySec-AE: Στην πρώτη περίπτωση, το πρωτόκολλο αυθεντικοποιεί ολόκληρο το πακέτο (συμπεριλαμβανομένης της επικεφαλίδας) χρησιμοποιώντας έναν κωδικό Message Authentication Code, ενώ στη δεύτερη περίπτωση κρυπτογραφεί και την επικεφαλίδα και το ωφέλιμο φορτίο (payload).
- Περιορισμοί: Η χρήση 8-bit Message Authentication Code σημαίνει ότι ένας εισβολέας μπορεί θεωρητικά να πλαστογραφήσει ένα πακέτο μετά από $2^8 = 256$ προσπάθειες. Παρόλο που αυτό φαίνεται χαμηλό, η βιβλιογραφία [1] επισημαίνει ότι στα WSNs, ο περιορισμένος ρυθμός μετάδοσης καθιστά τέτοιες επιθέσεις χρονοβόρες και εύκολα ανιχνεύσιμες.

Το LEAP+ (Localized Encryption and Authentication Protocol) βασίζεται στην παραδοχή ότι διαφορετικοί τύποι μηνυμάτων απαιτούν διαφορετικά επίπεδα ασφάλειας [22], [28]. Εισάγει μια ιεραρχία τεσσάρων κλειδιών:

- Individual Key (Ατομικό Κλειδί): Μοναδικό κλειδί μεταξύ κάθε κόμβου και του Σταθμού Βάσης για κρίσιμες εντολές.
- Group Key (Κλειδί Ομάδας): Κοινό κλειδί για όλους τους κόμβους, χρήσιμο για broadcast μηνύματα από τον Σταθμό Βάσης.
- Cluster Key (Κλειδί Συμπλέγματος): Για επικοινωνία μεταξύ ενός Cluster Head και των μελών της ομάδας του.
- Pairwise Key (Κλειδί Γειτονιάς): Μοναδικό κλειδί ανάμεσα σε δύο άμεσα συνδεδεμένους γείτονες, προσφέροντας ανθεκτικότητα σε περίπτωση παραβίασης ενός κόμβου (node compromise resilience) [9].

Για την ολιστική διαχείριση της ασφάλειας, τα παραπάνω πρωτόκολλα εντάσσονται σε ένα ευρύτερο πλαίσιο που ονομάζεται Security Management Platform (SMP). Το SMP λειτουργεί ως το "λειτουργικό κέντρο" ασφαλείας του δικτύου, αναλαμβάνοντας τον συντονισμό των κρυπτογραφικών διεργασιών και τη βελτιστοποίηση των πόρων.

Η αποτελεσματικότητα του TinySec (το οποίο παρέχει κρυπτογράφηση και αυθεντικοποίηση στο επίπεδο συνδέσμου) και του LEAP+ (Localized Encryption and Authentication Protocol, το οποίο διαχειρίζεται τη διανομή πολλαπλών τύπων κλειδιών) μεγιστοποιείται μέσω του SMP. Το SMP λειτουργεί ως κεντρικό πλαίσιο συντονισμού που διασφαλίζει ότι η εφαρμογή αυτών των μηχανισμών ασφάλειας δεν θα οδηγήσει σε πρόωρη εξάντληση της μπαταρίας των κόμβων. Επιπλέον, όπως τονίζεται στην [5], το SMP μπορεί να συνεργαστεί με μηχανισμούς επιλογής χαρακτηριστικών (Feature Selection) για να μειώσει τον χρόνο ανίχνευσης επιθέσεων, όπως οι επιθέσεις "Replay" (επανάληψης) ή "Flooding" (κατακλυσμού), βελτιώνοντας την απόκριση του δικτύου σε πραγματικό χρόνο.

3.4.3 Το Πρότυπο ZigBee και η Ασφάλειά του

Το ZigBee αποτελεί ένα παγκόσμιο πρότυπο ασύρματης επικοινωνίας που αναπτύχθηκε από τη ZigBee Alliance (πλέον Connectivity Standards Alliance - CSA) για την κάλυψη των αναγκών δικτύων χαμηλής κατανάλωσης, χαμηλού ρυθμού μετάδοσης δεδομένων και μικρής εμβέλειας. Βασίζεται στο πρότυπο

IEEE 802.15.4, το οποίο καθορίζει τα δύο κατώτερα επίπεδα (Φυσικό και MAC), ενώ το ZigBee προσθέτει τα επίπεδα δικτύου και εφαρμογής, καθώς και το πλαίσιο ασφάλειας.

Τα κύρια χαρακτηριστικά που καθιστούν το ZigBee ιδανικό για WSNs είναι:

- Τοπολογία Πλέγματος (Mesh Networking): Επιτρέπει τη δημιουργία δικτύων μεγάλης κλίμακας με υψηλή αξιοπιστία, καθώς τα δεδομένα μπορούν να αναδρομολογηθούν αν ένας κόμβος αποτύχει.
- Ενεργειακή Αποδοτικότητα: Σχεδιάστηκε ώστε οι κόμβοι (End Devices) να παραμένουν σε κατάσταση ύπνου για μεγάλα διαστήματα, επιτρέποντας τη λειτουργία τους με μια μπαταρία για χρόνια.
- Υποστήριξη μεγάλου αριθμού κόμβων: Ένα δίκτυο ZigBee μπορεί θεωρητικά να υποστηρίξει έως και 65.000 συσκευές.

Η δομή ενός δικτύου ZigBee περιλαμβάνει τρεις τύπους συσκευών:

1. ZigBee Coordinator (ZC): Η πιο υπεύθυνη συσκευή που σχηματίζει το δίκτυο και διατηρεί τις πληροφορίες ασφαλείας.
2. ZigBee Router (ZR): Ενδιάμεσοι κόμβοι που προωθούν τα δεδομένα άλλων συσκευών.
3. ZigBee End Device (ZED): Τερματικοί αισθητήρες που επικοινωνούν μόνο με τον γονικό τους κόμβο (Router ή Coordinator) [4], [6].

Η αρχιτεκτονική ασφαλείας του ZigBee είναι δομημένη με τέτοιο τρόπο ώστε να εξυπηρετεί τις ανάγκες των δικτύων LR-WPAN (Low-Rate Wireless Personal Area Networks – Ασύρματα Προσωπικά Δίκτυα Χαμηλού Ρυθμού Μετάδοσης). Τα δίκτυα αυτά χαρακτηρίζονται από χαμηλή κατανάλωση ενέργειας και περιορισμένη εμβέλεια, βασιζόμενα στο πρότυπο IEEE 802.15.4 για τα επίπεδα Φυσικό (PHY) και Ελέγχου Πρόσβασης Μέσου (MAC). Η καρδιά της ασφάλειας του προτύπου είναι ο αλγόριθμος AES-128, ο οποίος εφαρμόζεται σε λειτουργία CCM, επιτυγχάνοντας ταυτόχρονα κρυπτογράφηση για εμπιστευτικότητα και παραγωγή κώδικα ελέγχου ακεραιότητας μηνύματος (Message Integrity Code – MIC). Η ασφάλεια εφαρμόζεται "end-to-end" στο επίπεδο εφαρμογής (APS layer - Application Support Sub-layer) και "hop-by-hop" στο επίπεδο δικτύου (NWK layer), διασφαλίζοντας ότι η πληροφορία προστατεύεται καθ' όλη τη διαδρομή της από τον αισθητήρα έως τον τελικό αποδέκτη [4], [6].

Κεντρικό ρόλο στη διατήρηση της ακεραιότητας του δικτύου παίζει ο ZigBee Coordinator, ο οποίος λειτουργεί ως το Trust Center (TC) [9]. Το TC είναι υπεύθυνο για την έκδοση και τη διανομή των κλειδιών, την αυθεντικοποίηση των συσκευών και τον ορισμό των πολιτικών ασφαλείας. Οι δύο βασικοί τύποι κλειδιών που χρησιμοποιούνται είναι:

- Network Key (Κλειδί Δικτύου): Είναι ένα κλειδί 128-bit που μοιράζονται όλοι οι κόμβοι και χρησιμοποιείται για την κρυπτογράφηση της κίνησης σε επίπεδο δικτύου, αποτρέποντας εξωτερικούς εισβολείς από το να παρακολουθούν τη δρομολόγηση [22].
- Link Key (Κλειδί Συνδέσμου): Χρησιμοποιείται για την προστασία της επικοινωνίας μεταξύ δύο συγκεκριμένων κόμβων (unicast). Αυτό το κλειδί είναι κρίσιμο για την προστασία ευαίσθητων δεδομένων εφαρμογής, καθώς ακόμη και αν το κλειδί δικτύου παραβιαστεί, η επικοινωνία μεταξύ των συγκεκριμένων κόμβων παραμένει ασφαλής [6], [9].

Παρά την ισχυρή κρυπτογραφική βάση, το ZigBee παρουσιάζει ευπάθειες, ειδικά κατά τη φάση της «ένταξης» (joining) μιας συσκευής στο δίκτυο. Στην "Standard Security" λειτουργία, το κλειδί δικτύου

αποστέλλεται συχνά κρυπτογραφημένο με ένα προεπιλεγμένο κλειδί (Default Trust Center Link Key), το οποίο είναι ευρέως γνωστό, καθιστώντας το δίκτυο εύαλωτο σε επιθέσεις κλοπής ταυτότητας (Identity Theft) [3]. Όπως επισημαίνεται στην αναφορά [6], σε κρίσιμες εφαρμογές όπως τα Smart Grids, αυτή η αδυναμία αντιμετωπίζεται μέσω της "High Security" λειτουργίας, η οποία απαιτεί προ-εγκατεστημένα (out-of-band) κλειδιά.

Επιπλέον, οι νεότερες εκδόσεις (ZigBee 3.0) επιβάλλουν τη χρήση πιο σύνθετων μηχανισμών, όπως η περιοδική ανανέωση των κλειδιών (key rotation) και η χρήση μετρητών πλαισίου (Frame Counters) για την πλήρη εξάλειψη των επιθέσεων επανάληψης (replay attacks) [6], [10].

Παρά την ευρεία υιοθέτησή του, το πρότυπο ZigBee έχει αποτελέσει αντικείμενο κριτικής ως προς ορισμένες σχεδιαστικές του επιλογές που επηρεάζουν την ασφάλεια. Η πλέον γνωστή ευπάθεια σχετίζεται με τη διαχείριση των κλειδιών κατά τη φάση εισόδου ενός νέου κόμβου στο δίκτυο, όπου σε ορισμένες υλοποιήσεις το κλειδί δικτύου μεταδίδεται με προστασία ενός προκαθορισμένου, γνωστού κλειδιού μεταφοράς. Ένας επιτιθέμενος που παρακολουθεί την κίνηση τη στιγμή της εισόδου ενός κόμβου μπορεί δυνητικά να υποκλέψει το κλειδί δικτύου και να αποκτήσει πρόσβαση στην επικοινωνία. Η αδυναμία αυτή υπογραμμίζει ότι ακόμη και ένα ώριμο και τυποποιημένο πρωτόκολλο μπορεί να παρουσιάζει κενά ασφαλείας όταν η ασφάλεια εξαρτάται από τη σωστή διαχείριση των κρίσιμων φάσεων του κύκλου ζωής. Οι νεότερες εκδόσεις του προτύπου εισήγαγαν ενισχυμένους μηχανισμούς, όπως η εγκαθίδρυση κλειδιών εγκατάστασης ανά συσκευή, μετριάζοντας σημαντικά τον κίνδυνο αυτό [3], [4].

3.4.4 Σύγκριση Πρωτοκόλλων

Η συγκριτική θεώρηση των τριών πρωτοκόλλων που αναλύθηκαν —SPINS, TinySec/LEAP+ και ZigBee— αναδεικνύει μια σαφή εξελικτική πορεία στη φιλοσοφία σχεδιασμού της ασφάλειας των WSNs. Το SPINS αντιπροσωπεύει την ακαδημαϊκή προσέγγιση της ελαχιστοποίησης του overhead μέσω έξυπνων μηχανισμών, όπως ο διαμοιραζόμενος μετρητής και η καθυστερημένη αποκάλυψη κλειδιών. Το TinySec και το LEAP+ μετατοπίζουν την εστίαση στην πρακτική ενσωμάτωση εντός υπάρχοντων λειτουργικών συστημάτων, όπως το TinyOS και στην ιεραρχική διαχείριση κλειδιών ανάλογα με τον τύπο της επικοινωνίας. Το ZigBee, τέλος, εκπροσωπεί την τυποποιημένη, εμπορική ωρίμανση των αρχών αυτών, ενσωματώνοντας ισχυρή κρυπτογραφία AES-128 σε ένα πλήρως καθορισμένο βιομηχανικό πρότυπο. Η πορεία αυτή από το ερευνητικό πρωτότυπο στο εμπορικό προϊόν καταδεικνύει ότι οι θεμελιώδεις αρχές της ελαφριότητας και ιεραρχικής ασφάλειας παραμένουν σταθερές, ανεξαρτήτως του επιπέδου ωριμότητας της εκάστοτε υλοποίησης.

Παρά τις διαφορές τους και τα τρία πρωτόκολλα μοιράζονται μια κοινή θεμελιώδη ευπάθεια: την κρισιμότητα της φάσης αρχικής εγκαθίδρυσης εμπιστοσύνης. Όπως αναδείχθηκε στην περίπτωση του ZigBee με το προεπιλεγμένο κλειδί κατά τη διαδικασία ένταξης, το ασθενέστερο σημείο ενός κατά τα άλλα ισχυρού συστήματος είναι συχνά η στιγμή κατά την οποία ένας νέος κόμβος εισέρχεται στο δίκτυο. Η παρατήρηση αυτή έχει γενικότερη ισχύ στην ασφάλεια των WSNs: η κρυπτογραφική ισχύς ενός αλγορίθμου είναι ανώφελη αν τα κλειδιά μπορούν να υποκλαπούν κατά τη διανομή τους. Συνεπώς, η ασφαλής διαχείριση του κύκλου ζωής των κλειδιών —από τη γέννηση και τη διανομή έως την ανανέωση και την ανάκλησή τους— αποτελεί εξίσου κρίσιμο παράγοντα με την επιλογή του ίδιου του κρυπτογραφικού αλγορίθμου. Η διαπίστωση αυτή αιτιολογεί γιατί η σύγχρονη έρευνα δίνει αυξανόμενη έμφαση στους μηχανισμούς δυναμικής ανανέωσης κλειδιών και στις αρχιτεκτονικές μηδενικής εμπιστοσύνης που ελαχιστοποιούν την εξάρτηση από μια ασφαλή αρχική φάση [4], [6].

3.5 Ασφαλής Συνάθροιση Δεδομένων και Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης

Η ανάλυση των πρωτοκόλλων που προηγήθηκε εστίασε στην προστασία της επικοινωνίας μεταξύ δύο οντοτήτων. Στα WSNs όμως, η κυρίαρχη επικοινωνιακή διεργασία δεν είναι η μεταφορά ενός μηνύματος από άκρο σε άκρο αλλά η συνάθροιση: οι επικεφαλής συστάδων συλλέγουν μετρήσεις από δεκάδες κόμβους και προωθούν προς τον σταθμό βάσης μια συγκεντρωτική τιμή, όπως μέσο όρο ή μέγιστο. Η τεχνική αυτή είναι ενεργειακά απαραίτητη, καθώς μειώνει δραστικά τον όγκο των μεταδόσεων, δημιουργεί όμως ένα θεμελιώδες πρόβλημα ασφάλειας: για να υπολογίσει τη συγκεντρωτική τιμή, ο επικεφαλής πρέπει καταρχήν να αποκρυπτογραφήσει τα επιμέρους δεδομένα, καθιστάμενος έτσι σημείο συγκέντρωσης ευαίσθητης πληροφορίας και προνομιακός στόχος επίθεσης.

Η ομοιομορφική κρυπτογράφηση προσφέρει θεωρητικά την κομψότερη λύση, επιτρέποντας την εκτέλεση αριθμητικών πράξεων απευθείας επί των κρυπτογραφημένων τιμών. Στην πράξη, τα πλήρως ομοιομορφικά σχήματα παραμένουν απαγορευτικά για κόμβους αισθητήρων, ενώ τα μερικώς ομοιομορφικά, που υποστηρίζουν μόνο πρόσθεση, καλύπτουν επαρκώς τις πιο συνήθεις λειτουργίες συνάθροισης με ανεκτό κόστος. Η βιβλιογραφία της περιόδου επισημαίνει ωστόσο ότι η κρυπτογραφική διάσταση δεν επαρκεί από μόνη της: πρόσφατο πρωτόκολλο ασφαλούς συνάθροισης καταδεικνύει ότι η προστασία της ιδιωτικότητας απαιτεί τον συνδυασμό αυθεντικοποίησης με ρητό μηχανισμό εξουσιοδότησης των κόμβων και έλεγχο φρεσκάδας των δεδομένων, ώστε να αποτρέπεται τόσο η εισαγωγή πλαστών μετρήσεων όσο και η επαναχρησιμοποίηση παλαιότερων [29].

Η απαίτηση αυτή οδηγεί φυσιολογικά στην έννοια της αρχιτεκτονικής μηδενικής εμπιστοσύνης (ZTA - Zero Trust Architecture). Το παραδοσιακό μοντέλο ασφάλειας των WSNs είναι περιμετρικό: ένας κόμβος που έχει ολοκληρώσει επιτυχώς την αρχική διαδικασία εγκαθίδρυσης κλειδιών θεωρείται έμπιστος για το υπόλοιπο του κύκλου ζωής του. Η παραδοχή αυτή καταρρέει μπροστά στην απειλή της φυσικής παραβίασης κόμβου, όπου ο επιτιθέμενος αποκτά νόμιμα κρυπτογραφικά διαπιστευτήρια. Η προσέγγιση μηδενικής εμπιστοσύνης αντικαθιστά τη διακριτή στιγμή της αυθεντικοποίησης με συνεχή επαλήθευση, όπου κάθε αίτημα αξιολογείται με βάση την τρέχουσα συμπεριφορά του κόμβου και όχι με βάση την ιστορική του πιστοποίηση.

Η εφαρμογή της αρχής αυτής σε δίκτυα περιορισμένων πόρων απαιτεί προσεκτική σχεδίαση, καθώς η συνεχής επαναξιολόγηση συνεπάγεται πρόσθετη επικοινωνία και επεξεργασία. Οι σύγχρονες υλοποιήσεις αντιμετωπίζουν το πρόβλημα μεταθέτοντας το υπολογιστικό βάρος της αξιολόγησης στους ισχυρότερους κόμβους της ιεραρχίας, ενώ οι περιορισμένοι κόμβοι περιορίζονται στην εκπομπή ενδείξεων συμπεριφοράς. Το πλαίσιο ZT-IoTrust αποτελεί χαρακτηριστικό παράδειγμα της κατεύθυνσης αυτής, συνδυάζοντας τη συνεχή αξιολόγηση εμπιστοσύνης με κατανεμημένη εκπαίδευση μοντέλου, ώστε καμία κεντρική οντότητα να μη διαθέτει πλήρη εικόνα της συμπεριφοράς όλων των κόμβων [26].

Παράλληλη είναι η εξέλιξη στον χώρο των κινητών κόμβων. Σε δίκτυα όπου η συλλογή δεδομένων γίνεται μέσω μη επανδρωμένων εναέριων οχημάτων, η δυναμική τοπολογία καθιστά αδύνατη την προεγκατάσταση ζευγαρωτών κλειδιών για κάθε πιθανό συνδυασμό επικοινωνούντων οντοτήτων. Πρόσφατη πρόταση αυθεντικοποίησης για ασύρματα δίκτυα UAV αντιμετωπίζει το ζήτημα με ελαφρύ πρωτόκολλο αμοιβαίας πιστοποίησης που εγκαθιδρύει εφήμερα κλειδιά συνόδου κατά τη στιγμή της συνάντησης, χωρίς εξάρτηση από διαρκή σύνδεση με κεντρική αρχή [30].

3.6 Συστήματα Ανίχνευσης Εισβολών

Τα IDS στα WSNs είναι απαραίτητα για τον εντοπισμό τόσο εξωτερικών όσο και εσωτερικών επιθέσεων (insider attacks), όπου ένας νόμιμος κόμβος έχει παραβιαστεί και ενεργεί κακόβουλα. Λόγω της

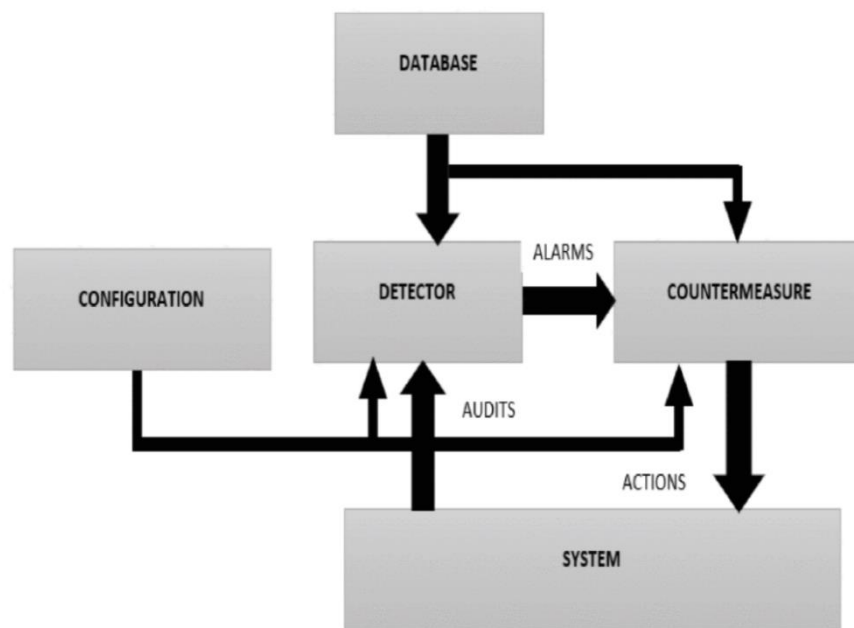
εγγενούς έλλειψης κεντρικής διακυβέρνησης και των περιορισμένων πόρων, τα IDS πρέπει να είναι ελαφριά, κλιμακωτά και ικανά να λειτουργούν σε περιβάλλοντα με υψηλά επίπεδα θορύβου [20], [23].

1. Αρχιτεκτονική και Τύποι Ανίχνευσης

Τα IDS ταξινομούνται με βάση τη στρατηγική ανίχνευσης που χρησιμοποιούν [3]:

- Ανίχνευση Υπογραφών (Signature-based): Συγκρίνουν τη δραστηριότητα με βάση δεδομένων γνωστών επιθέσεων.
- Ανίχνευση Ανωμαλιών (Anomaly-based): Ορίζουν ένα προφίλ «φυσιολογικής συμπεριφοράς» και ειδοποιούν για αποκλίσεις.

Η λειτουργική δομή ενός τυπικού IDS περιλαμβάνει την αλληλεπίδραση μεταξύ της παρακολούθησης του συστήματος, του εντοπισμού μέσω βάσης δεδομένων και της λήψης αντιμέτρων.



Εικόνα 10 Γενικό μπλοκ διάγραμμα ενός IDS [23]

Ανάλυση Αρχιτεκτονικής Συστήματος (Block Diagram)

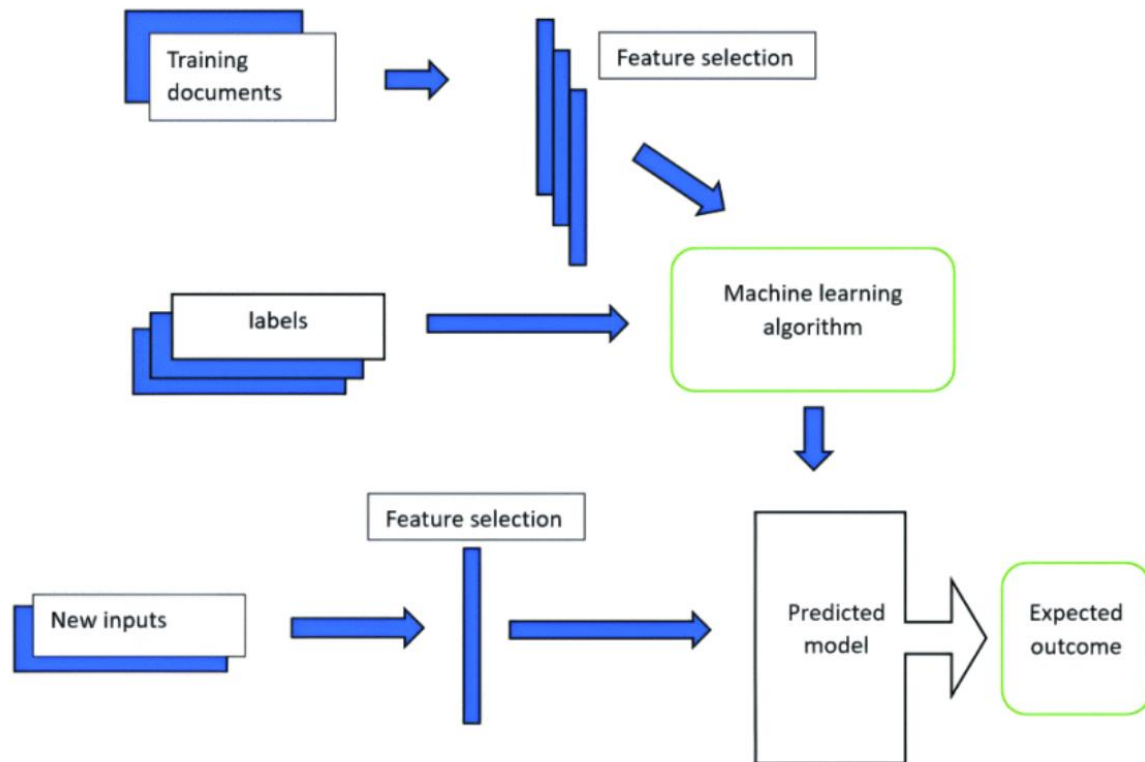
Η Εικόνα 10 παρουσιάζει τη δομική οργάνωση του Συστήματος Ανίχνευσης Εισβολών και τις ροές πληροφορίας μεταξύ των υποσυστημάτων του:

- Σύστημα (System): Πρόκειται για το δίκτυο αισθητήρων (WSNs) που παρακολουθείται. Από εδώ συλλέγονται τα δεδομένα ελέγχου (Audits) που αντικατοπτρίζουν τη δραστηριότητα των κόμβων.
- Ανιχνευτής (Detector): Είναι το κεντρικό στοιχείο επεξεργασίας. Λαμβάνει τα δεδομένα ελέγχου και, σε συνδυασμό με τις παραμέτρους από τη Διαμόρφωση (Configuration) και τις πληροφορίες της Βάσης Δεδομένων (Database), αποφασίζει αν η δραστηριότητα είναι ύποπτη.
- Βάση Δεδομένων (Database): Αποθηκεύει τα πρότυπα γνωστών επιθέσεων (signatures) ή τα προφίλ φυσιολογικής συμπεριφοράς, τροφοδοτώντας τόσο τον ανιχνευτή όσο και το τμήμα των αντιμέτρων.
- Αντίμετρα (Countermeasure) & Συναγερμοί (Alarms): Μόλις ο ανιχνευτής εντοπίσει μια εισβολή, αποστέλλει σήμα συναγερμού. Το τμήμα των αντιμέτρων αναλαμβάνει τη λήψη συγκεκριμένων

ενεργειών (Actions) προς το σύστημα, όπως τον αποκλεισμό ενός κακόβουλου κόμβου ή την απομόνωση ενός τμήματος του δικτύου.

2. IDS βασισμένα σε Μηχανική Μάθηση (ML - Machine Learning)

Η σύγχρονη έρευνα επικεντρώνεται στη χρήση αλγορίθμων ML για την αυτοματοποίηση της ανίχνευσης. Η διαδικασία αυτή βασίζεται στην εκπαίδευση μοντέλων με ιστορικά δεδομένα ώστε να μπορούν να προβλέπουν κακόβουλες ενέργειες σε νέα δεδομένα εισόδου.



Εικόνα 11 Ροή εργασίας Εποπτευόμενης Μάθησης (Supervised Learning) [20]

Ανάλυση Ροής Εποπτευόμενης Μάθησης

Η αποτελεσματικότητα των αλγορίθμων μηχανικής μάθησης βασίζεται σε μια δομημένη διαδικασία, η οποία απεικονίζεται στην Εικόνα 11. Η διαδικασία χωρίζεται σε δύο κύριες φάσεις:

Φάση Εκπαίδευσης (Training Phase)

- **Δεδομένα Εκπαίδευσης & Ετικέτες:** Το σύστημα τροφοδοτείται με έγγραφα εκπαίδευσης (training documents) και τις αντίστοιχες ετικέτες (labels) τους. Οι ετικέτες αυτές ορίζουν αν μια κίνηση είναι «φυσιολογική» ή «επίθεση», επιτρέποντας στον αλγόριθμο να μαθαίνει από παραδείγματα.
- **Επιλογή Χαρακτηριστικών (Feature Selection):** Πριν την εισαγωγή στον αλγόριθμο, πραγματοποιείται φιλτράρισμα των δεδομένων για την εξαγωγή των πιο σημαντικών χαρακτηριστικών. Η μείωση των χαρακτηριστικών είναι κρίσιμη για την εξοικονόμηση πόρων στα WSNs.
- **Αλγόριθμος Μηχανικής Μάθησης:** Ο αλγόριθμος επεξεργάζεται τα επιλεγμένα χαρακτηριστικά και τις ετικέτες για να δημιουργήσει το Προβλεπτικό Μοντέλο (Predicted Model).

Φάση Πρόβλεψης (Prediction Phase)

- Νέες Είσοδοι (New Inputs): Όταν το δίκτυο λειτουργεί, νέα, άγνωστα δεδομένα εισέρχονται στο σύστημα.
- Εφαρμογή Μοντέλου: Τα νέα δεδομένα περνούν από την ίδια διαδικασία επιλογής χαρακτηριστικών και εισάγονται στο ήδη εκπαιδευμένο μοντέλο.
- Αναμενόμενο Αποτέλεσμα (Expected Outcome): Το μοντέλο ταξινομεί τη νέα είσοδο και παράγει το τελικό αποτέλεσμα, προσδιορίζοντας με υψηλή ακρίβεια αν πρόκειται για απειλή ή όχι.

3. Επιδόσεις και Επιλογή Χαρακτηριστικών (Feature Selection)

Ένα κρίσιμο ζήτημα στα συστήματα ανίχνευσης εισβολών (IDS) αποτελεί ο χρόνος απόκρισης, ιδιαίτερα σε περιβάλλοντα με περιορισμένους πόρους, όπως τα ασύρματα δίκτυα αισθητήρων. Τα 41 χαρακτηριστικά του συνόλου δεδομένων (NSL-KDD - Network Security Laboratory – Knowledge Discovery and Data mining) —μιας βελτιωμένης εκδοχής του ιστορικού συνόλου KDD Cup 1999, από την οποία έχουν αφαιρεθεί οι διπλότυπες εγγραφές ώστε να μην μεροληπτούν οι ταξινομητές υπέρ των συχνότερα εμφανιζόμενων επιθέσεων— παρέχουν μια ολοκληρωμένη εικόνα της κίνησης του δικτύου και ταξινομούνται σε τέσσερις κύριες ομάδες:

- Βασικά χαρακτηριστικά (Basic features): (Χαρακτηριστικά 1-9) Περιλαμβάνουν θεμελιώδεις ιδιότητες της σύνδεσης, όπως η διάρκεια (duration), ο τύπος πρωτοκόλλου (protocol_type), η υπηρεσία προορισμού (service) και ο όγκος των δεδομένων σε bytes (src_bytes, dst_bytes).
- Χαρακτηριστικά περιεχομένου (Content features): (Χαρακτηριστικά 10-22) Αναζητούν ύποπτα μοτίβα εντός του payload, όπως ο αριθμός των αποτυχημένων προσπαθειών σύνδεσης (num_failed_logins), η πρόσβαση ως root (root_shell) και ο αριθμός των ενεργειών σε αρχεία (num_file_creations).
- Χαρακτηριστικά κίνησης βάσει χρόνου (Time-based traffic features): (Χαρακτηριστικά 23-31) Εξετάζουν στατιστικά στοιχεία σε παράθυρο 2 δευτερολέπτων, όπως ο αριθμός συνδέσεων προς τον ίδιο host (count) και το ποσοστό συνδέσεων με σφάλματα τύπου S0 (serror_rate).
- Χαρακτηριστικά κίνησης βάσει κεντρικού υπολογιστή (Host-based traffic features): (Χαρακτηριστικά 32-41) Αναλύουν τις τελευταίες 100 συνδέσεις προς τον ίδιο προορισμό, αξιολογώντας παραμέτρους όπως το ποσοστό συνδέσεων από την ίδια θύρα προέλευσης (dst_host_same_src_port_rate).

Η ανάλυση και των 41 αυτών παραμέτρων σε πραγματικό χρόνο συνεπάγεται αυξημένο υπολογιστικό κόστος και κατανάλωση ενέργειας. Για την αντιμετώπιση αυτού του προβλήματος, εφαρμόζεται η μέθοδος MRMR (Minimum Redundancy Maximum Relevance), η οποία μειώνει τον αριθμό των χαρακτηριστικών σε μόλις 12, επιτυγχάνοντας μείωση του χρόνου επεξεργασίας έως και επτά φορές, ενώ παράλληλα διατηρείται υψηλή ακρίβεια που υπερβαίνει το 98,5% [5].

- Η αναλυτική συγκριτική αξιολόγηση της ακρίβειας των αλγορίθμων αυτών (Random Forest, Decision Tree και SVM - Support Vector Machine), καθώς και η σύγκρισή τους με τη σχετική βιβλιογραφία, παρουσιάζεται διεξοδικά στο Κεφάλαιο 5 (ενότητα 5.3).

4. Κατανεμημένα και Υβριδικά Συστήματα

Στα σύγχρονα IoT-based WSNs, η χρήση ενός κεντρικού IDS στον Σταθμό Βάσης είναι συχνά αναποτελεσματική λόγω της τεράστιας κατανάλωσης ενέργειας που απαιτείται για τη συνεχή αποστολή

δεδομένων ελέγχου. Για τον λόγο αυτό, υιοθετούνται ιεραρχικές και υβριδικές δομές, οι οποίες κατανέμουν το υπολογιστικό φορτίο της ανίχνευσης σε διαφορετικά επίπεδα του δικτύου [23]:

- Τοπικό Επίπεδο Ανίχνευσης (Node Level): Κάθε κόμβος αισθητήρα λειτουργεί ως ένας "ελαφρύς" ανιχνευτής (lightweight IDS agent). Σε αυτό το επίπεδο, ο κόμβος παρακολουθεί τη συμπεριφορά των άμεσων γειτόνων του (neighbor monitoring) και συλλέγει στατιστικά στοιχεία, όπως ο αριθμός των χαμένων πακέτων ή οι ασυνήθιστες μεταβολές στην ισχύ του σήματος (RSSI - Received Signal Strength Indication, δηλαδή ο δείκτης ισχύος του λαμβανόμενου σήματος, ο οποίος αξιοποιείται ως ένδειξη ανωμαλιών στο φυσικό επίπεδο). Αν εντοπιστεί μια προφανής ανωμαλία (π.χ. jamming), ο κόμβος μπορεί να ενεργοποιήσει άμεσα έναν τοπικό συναγερμό χωρίς να περιμένει έγκριση από το δίκτυο.
- Επίπεδο Ομάδας (Cluster Head Level): Οι αρχηγοί των ομάδων (Cluster Heads) παίζουν τον ρόλο του "ενδιάμεσου αναλυτή". Συγκεντρώνουν τις αναφορές από τους κόμβους-μέλη τους και εφαρμόζουν τεχνικές συγκέντρωσης δεδομένων (data aggregation). Αυτό το επίπεδο είναι κρίσιμο για τον εντοπισμό επιθέσεων που δεν είναι ορατές σε έναν μόνο κόμβο, όπως οι επιθέσεις Wormhole ή Sinkhole, όπου απαιτείται σύγκριση των μονοπατιών δρομολόγησης από πολλαπλές πηγές [10].
- Συγκεντρωτικό Επίπεδο (Base Station / Sink Level): Ο Σταθμός Βάσης, διαθέτοντας απεριόριστους πόρους, εκτελεί τους πιο "βαριούς" αλγορίθμους Μηχανικής Μάθησης (όπως το Random Forest με τα 41 χαρακτηριστικά). Εδώ πραγματοποιείται η τελική επιβεβαίωση της επίθεσης και η λήψη αποφάσεων για ολόκληρο το δίκτυο (π.χ. καθολική απομόνωση ενός κακόβουλου κόμβου).

Η υβριδική αυτή προσέγγιση προσφέρει το πλεονέκτημα της κλιμακωσιμότητας (scalability), καθώς το δίκτυο μπορεί να μεγαλώνει χωρίς να υπερφορτώνεται ο Σταθμός Βάσης, ενώ παράλληλα εξασφαλίζει τη μέγιστη δυνατή ενεργειακή αποδοτικότητα, αφού η "βαριά" ανάλυση γίνεται μόνο όταν οι τοπικοί ανιχνευτές δώσουν σοβαρές ενδείξεις εισβολής [5], [20].

Παρά την αναμφισβήτητη αποτελεσματικότητά τους, τα συστήματα ανίχνευσης εισβολών που βασίζονται σε μηχανική μάθηση αντιμετωπίζουν ένα σύνολο εγγενών περιορισμών στο πλαίσιο των WSNs. Το σημαντικότερο ζήτημα είναι η αντιστάθμιση μεταξύ του ποσοστού ανίχνευσης (detection rate) και του ποσοστού των ψευδών συναγερμών (false positive rate). Ένα υπερβολικά ευαίσθητο σύστημα παράγει πλήθος ψευδών ειδοποιήσεων, οι οποίες όχι μόνο καταναλώνουν πολύτιμη ενέργεια για την επεξεργασία και τη μετάδοσή τους, αλλά υπονομεύουν και την εμπιστοσύνη του διαχειριστή στο σύστημα. Αντίθετα, ένα σύστημα ρυθμισμένο για ελαχιστοποίηση των ψευδών συναγερμών κινδυνεύει να μην εντοπίσει εξελιγμένες ή νέες μορφές επίθεσης. Η εξεύρεση της βέλτιστης ισορροπίας μεταξύ των δύο αυτών μεγεθών αποτελεί ένα διαρκές ερευνητικό αντικείμενο, το οποίο επηρεάζεται καθοριστικά από τη φύση της εκάστοτε εφαρμογής και την ανοχή της σε σφάλματα.

Μια αναδυόμενη και ιδιαίτερα ανησυχητική απειλή για τα IDS που βασίζονται σε μηχανική μάθηση είναι οι ανταγωνιστικές επιθέσεις (adversarial attacks). Σε αυτές, ο επιτιθέμενος κατασκευάζει προσεκτικά την κακόβουλη κίνηση ώστε να μοιάζει στατιστικά με φυσιολογική συμπεριφορά, παρακάμπτοντας έτσι το εκπαιδευμένο μοντέλο ταξινόμησης. Η ευπάθεια αυτή αναδεικνύει ένα παράδοξο: το ίδιο το εργαλείο που σχεδιάστηκε για την ανίχνευση επιθέσεων καθίσταται με τη σειρά του στόχος επίθεσης. Επιπλέον, η ποιότητα και η αντιπροσωπευτικότητα των δεδομένων εκπαίδευσης επηρεάζουν καθοριστικά την απόδοση· ένα μοντέλο εκπαιδευμένο σε παρωχημένα ή μη ισορροπημένα σύνολα δεδομένων θα αποτύχει να γενικεύσει σε πραγματικές συνθήκες δικτύου. Για τον λόγο αυτό, η περιοδική επανεκπαίδευση των μοντέλων με επικαιροποιημένα δεδομένα και η χρήση τεχνικών ενίσχυσης της

ανθεκτικότητας έναντι ανταγωνιστικών παραδειγμάτων αποτελούν αναγκαίες προϋποθέσεις για την αξιόπιστη λειτουργία ενός σύγχρονου IDS.

Συμπερασματικά, η εξέλιξη των συστημάτων ανίχνευσης εισβολών αντανάκλα τη γενικότερη μετατόπιση της ασφάλειας των WSNs από στατικούς, κανονιστικούς μηχανισμούς προς δυναμικά, προσαρμοστικά συστήματα που μαθαίνουν από τη συμπεριφορά του δικτύου. Η ενσωμάτωση της μηχανικής μάθησης, ιδίως σε υβριδικές και ιεραρχικές αρχιτεκτονικές, επιτρέπει τον εντοπισμό απειλών που θα ήταν αδύνατο να προβλεφθούν με κλασικές τεχνικές υπογραφών. Ωστόσο, η αξιοποίηση αυτών των δυνατοτήτων δεν είναι αυτονόητη, καθώς απαιτεί προσεκτική διαχείριση του ενεργειακού κόστους, της ποιότητας των δεδομένων και της ανθεκτικότητας έναντι στοχευμένων επιθέσεων. Η ισορροπημένη αυτή προσέγγιση, που συνδυάζει την υπολογιστική ευφυΐα με τη συνείδηση των φυσικών περιορισμών, αποτελεί τον ακρογωνιαίο λίθο της επόμενης γενιάς ασφαλών δικτύων αισθητήρων [20], [23].

3.7 Επίλογος

Κλείνοντας το κεφάλαιο, η ασφάλεια στα WSNs και τα IoT δίκτυα απαιτεί τον συνδυασμό μηχανισμών προστασίας των δεδομένων κατά τη μετάδοση με αξιόπιστη διαχείριση κλειδιών: το TinySec προσφέρει εμπιστευτικότητα και ακεραιότητα με χαμηλό overhead, το LEAP+ πολυεπίπεδη διαχείριση κλειδιών ανθεκτική σε παραβιάσεις κόμβων και το ZigBee (AES-128/CCM) ασφάλεια end-to-end σε κρίσιμες εφαρμογές όπως τα Smart Grids. Συμπληρωματικά, τα Συστήματα Ανίχνευσης Εισβολών (IDS) —με τεχνικές όπως η επιλογή χαρακτηριστικών και οι κατανεμημένες/υβριδικές αρχιτεκτονικές— παρέχουν έγκαιρη ανίχνευση εξωτερικών και εσωτερικών απειλών, διατηρώντας υψηλή ακρίβεια και χαμηλή καθυστέρηση ακόμη και σε περιβάλλοντα περιορισμένων πόρων.

Κεφάλαιο 4ο: Σύγχρονες Τεχνολογίες στην Ασφάλεια των WSNs

4.1 Εισαγωγή

Στο παρόν κεφάλαιο εξετάζονται οι τεχνολογίες αιχμής που αναδιαμορφώνουν την ασφάλεια στα WSNs. Αναλύεται ο ρόλος της Τεχνητής Νοημοσύνης (AI - Artificial Intelligence) και της Μηχανικής Μάθησης (ML - Machine Learning) στην αυτοματοποιημένη ανίχνευση απειλών, καθώς και η συμβολή του Blockchain στην ακεραιότητα των δεδομένων και την αποκεντρωμένη διαχείριση ταυτότητας. Στη συνέχεια παρουσιάζεται πώς το Edge και το Fog Computing μεταφέρουν την επεξεργασία κοντά στην πηγή των δεδομένων και το κεφάλαιο ολοκληρώνεται με τεχνικές προστασίας της ιδιωτικότητας των χρηστών και της τοποθεσίας των κόμβων.

4.2 Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στην Ανίχνευση Επιθέσεων

Η ραγδαία εξέλιξη του Διαδικτύου των Πραγμάτων (IoT) και η ενσωμάτωση των Ασύρματων Δικτύων Αισθητήρων (WSNs) σε κρίσιμες υποδομές, όπως η έξυπνη γεωργία, η βιομηχανία 4.0 και η υγεία, κατέστησαν τις παραδοσιακές μεθόδους ασφαλείας ανεπαρκείς. Οι περιορισμένοι πόροι των κόμβων, σε συνδυασμό με την αυξανόμενη πολυπλοκότητα των κυβερνοεπιθέσεων, απαιτούν τη μετάβαση από στατικά συστήματα προστασίας σε δυναμικές, ευφυείς και αποκεντρωμένες λύσεις.

Η ενσωμάτωση της Τεχνητής Νοημοσύνης (AI) και της Μηχανικής Μάθησης (ML) αποτελεί τη σύγχρονη απάντηση στις εξελιγμένες απειλές που αντιμετωπίζουν τα WSNs. Σε αντίθεση με τις παραδοσιακές μεθόδους που βασίζονται σε στατικούς κανόνες, οι αλγόριθμοι ML έχουν την ικανότητα να "μαθαίνουν" από τα δεδομένα του δικτύου, επιτρέποντας την αυτοματοποιημένη αναγνώριση κακόβουλων μοτίβων και την ταξινόμηση επιθέσεων με υψηλή ακρίβεια.

Η Λειτουργική Δομή της Ανίχνευσης

Η εφαρμογή αυτών των τεχνολογιών υλοποιείται μέσω ενός Συστήματος Ανίχνευσης Εισβολών (IDS), η αρχιτεκτονική του οποίου βασίζεται σε έναν κλειστό βρόχο ελέγχου. Όπως απεικονίζεται στην Εικόνα 10, η διαδικασία ξεκινά με τη συνεχή συλλογή δεδομένων ελέγχου (Audits) από το Σύστημα. Ο Ανιχνευτής (Detector), χρησιμοποιώντας μοντέλα AI, συγκρίνει αυτή τη δραστηριότητα με τη Βάση Δεδομένων του και, σε περίπτωση απόκλισης, ενεργοποιεί Συναγερμούς και Αντίμετρα (Countermeasures) για την άμεση προστασία των κόμβων.

Μεθοδολογία Εποπτευόμενης Μάθησης

Η πιο διαδεδομένη προσέγγιση είναι η Εποπτευόμενη Μάθηση (Supervised Learning), η οποία ακολουθεί μια συγκεκριμένη ροή εργασίας (Workflow). Ειδικότερα, η διαδικασία περιλαμβάνει:

- Εκπαίδευση: Χρήση ιστορικών δεδομένων (Training documents) με προκαθορισμένες ετικέτες (labels) που ορίζουν την κανονική ή επιθετική συμπεριφορά.
- Επιλογή Χαρακτηριστικών (Feature Selection): Η τεχνική αυτή είναι κρίσιμη, καθώς μειώνει τον όγκο των δεδομένων (π.χ. από 41 σε 12 χαρακτηριστικά στο σύνολο NSL-KDD), μειώνοντας τον χρόνο επεξεργασίας κατά 7 φορές χωρίς να θυσιάζεται η ακρίβεια.

- Πρόβλεψη: Το εκπαιδευμένο μοντέλο δέχεται νέες εισόδους (New inputs) και παράγει το αναμενόμενο αποτέλεσμα (Expected outcome), ταξινομώντας την κίνηση σε πραγματικό χρόνο.

Αξιολόγηση Αλγορίθμων και Επιδόσεις

Πίνακας 2 Συγκριτική αξιολόγηση ακρίβειας αλγορίθμων Μηχανικής Μάθησης [5], [23]

Algorithm	Accuracy [19]	Accuracy [5]	Difference
Random Forest	79%	98%	+19%
SVM	93%	91%	-2%
Decision Tree	83%	96%	+13%

Η έρευνα δείχνει ότι η επιλογή του κατάλληλου αλγορίθμου επηρεάζει καθοριστικά την αποτελεσματικότητα του συστήματος. Στον παραπάνω Πίνακα, παρουσιάζεται η σύγκριση επιδόσεων μεταξύ διαφορετικών μοντέλων ML.

Ο αλγόριθμος Random Forest αναδεικνύεται ως ο πλέον αποτελεσματικός, επιτυγχάνοντας βελτίωση 19% σε σχέση με προγενέστερες μελέτες. Παράλληλα, εξειδικευμένες προσεγγίσεις όπως το μοντέλο Optimal SVM (OSVM), το οποίο χρησιμοποιεί τον αλγόριθμο βελτιστοποίησης Whale Optimization Algorithm (WOA), επιτυγχάνουν ακρίβεια 94.09%. Αυτά τα δεδομένα επιβεβαιώνουν ότι η ΑΙ όχι μόνο αυτοματοποιεί την ασφάλεια, αλλά αυξάνει σημαντικά την αξιοπιστία της ανίχνευσης σε περιβάλλοντα με υψηλό θόρυβο και περιορισμένους πόρους, όπως τα WSNs.

Πέρα από τους κλασικούς αλγορίθμους εποπτευόμενης μάθησης, η πρόοδος της βαθιάς μάθησης (Deep Learning) έχει ανοίξει νέους ορίζοντες στην ανίχνευση εισβολών σε WSNs. Αρχιτεκτονικές όπως τα συνελκτικά νευρωνικά δίκτυα (Convolutional Neural Networks - CNN) και τα αναδρομικά δίκτυα μακράς βραχείας μνήμης (Long Short-Term Memory - LSTM) επιτυγχάνουν την αυτόματη εξαγωγή χαρακτηριστικών απευθείας από την ακατέργαστη κίνηση του δικτύου, καταργώντας την ανάγκη για χειροκίνητη επιλογή χαρακτηριστικών από ειδικούς. Τα δίκτυα LSTM, ειδικότερα, αποδεικνύονται ιδιαίτερα αποτελεσματικά στην ανίχνευση επιθέσεων που εκδηλώνονται ως χρονικές ακολουθίες, όπως οι σταδιακές επιθέσεις εξάντλησης πόρων ή οι επιθέσεις κατακλυσμού (flooding). Ωστόσο, το αυξημένο υπολογιστικό κόστος των μοντέλων βαθιάς μάθησης τα καθιστά ακατάλληλα για εκτέλεση απευθείας στους περιορισμένους κόμβους, επιβάλλοντας την τοποθέτησή τους στον Σταθμό Βάσης ή σε κόμβους άκρου (edge nodes) με ενισχυμένους πόρους [20], [23].

Μια ιδιαίτερα υποσχόμενη εξέλιξη για το προστατευόμενο από ιδιωτικότητα μοντέλο ασφάλειας είναι η ομοσπονδιακή μάθηση (Federated Learning). Στο παράδειγμα αυτό, οι κόμβοι εκπαιδεύουν τοπικά μοντέλα χρησιμοποιώντας τα δικά τους δεδομένα και αποστέλλουν προς τον κεντρικό συντονιστή μόνο τις παραμέτρους του μοντέλου και όχι τα ίδια τα ευαίσθητα δεδομένα. Με τον τρόπο αυτό επιτυγχάνεται η συλλογική βελτίωση ενός παγκόσμιου μοντέλου ανίχνευσης χωρίς να διακυβεύεται η ιδιωτικότητα των μετρήσεων κάθε επιμέρους κόμβου. Η προσέγγιση αυτή αντιμετωπίζει ταυτόχρονα δύο κρίσιμα ζητήματα των WSNs: αφενός μειώνει τον όγκο των μεταδιδόμενων δεδομένων, εξοικονομώντας ενέργεια και αφετέρου περιορίζει την έκθεση ευαίσθητων πληροφοριών. Παρά τα πλεονεκτήματα αυτά, η ομοσπονδιακή μάθηση εισάγει νέες προκλήσεις, όπως η ευπάθεια σε επιθέσεις δηλητηρίασης μοντέλου

(model poisoning), κατά τις οποίες ένας παραβιασμένος κόμβος αποστέλλει κακόβουλες παραμέτρους για να υπονομεύσει το παγκόσμιο μοντέλο [7], [23].

Συγκρίνοντας κριτικά τις διαθέσιμες προσεγγίσεις, διαπιστώνεται ότι δεν υφίσταται ένας καθολικά ανώτερος αλγόριθμος, αλλά μια ιεραρχία επιλογών εξαρτώμενη από το λειτουργικό πλαίσιο. Οι αλγόριθμοι συνόλου (ensemble), όπως το Random Forest, προσφέρουν εξαιρετική ισορροπία μεταξύ ακρίβειας και ερμηνευσιμότητας με μέτριο υπολογιστικό κόστος, καθιστώντας τους ιδανικούς για ανάπτυξη σε κόμβους άκρου. Αντίθετα, τα μοντέλα βαθιάς μάθησης υπερτερούν σε ακρίβεια αλλά απαιτούν συγκεντρωτική επεξεργασία, ενώ οι μέθοδοι μη εποπτευόμενης μάθησης ενδείκνυνται για την ανίχνευση άγνωστων, μηδενικής ημέρας (zero-day) επιθέσεων εις βάρος της ερμηνευσιμότητας. Η σύγχρονη τάση κινείται προς υβριδικές αρχιτεκτονικές πολλαπλών επιπέδων, όπου ελαφριά μοντέλα φιλτράρουν την προφανή κίνηση στους κόμβους και πολυπλοκότερα μοντέλα αναλύουν τις αμφίβολες περιπτώσεις κεντρικά, βελτιστοποιώντας έτσι τη συνολική ενεργειακή και υπολογιστική απόδοση του συστήματος [20], [23].

Η ενσωμάτωση της τεχνητής νοημοσύνης στην ασφάλεια των WSNs δεν περιορίζεται στην ανίχνευση γνωστών τύπων επίθεσης, αλλά επεκτείνεται στην ικανότητα αναγνώρισης πρωτοεμφανιζόμενων, άγνωστων απειλών μέσω της ανίχνευσης ανωμαλιών (anomaly detection). Σε αντίθεση με τις μεθόδους που βασίζονται σε υπογραφές, οι οποίες απαιτούν προηγούμενη γνώση κάθε επίθεσης, οι τεχνικές μη εποπτευόμενης μάθησης μοντελοποιούν τη φυσιολογική συμπεριφορά του δικτύου και σημαίνουν συναγερμό για κάθε σημαντική απόκλιση από αυτήν. Η προσέγγιση αυτή είναι ιδιαίτερα πολύτιμη σε ένα συνεχώς εξελισσόμενο τοπίο απειλών, όπου νέες παραλλαγές επιθέσεων εμφανίζονται διαρκώς. Ωστόσο, η ισχύς αυτή συνοδεύεται από την πρόκληση της διάκρισης μεταξύ μιας πραγματικής επίθεσης και μιας απλής, καλοήθους μεταβολής στη συμπεριφορά του δικτύου, όπως η αλλαγή στη συχνότητα μετρήσεων λόγω εξωτερικών συνθηκών. Η μείωση των ψευδών συναγερμών στην ανίχνευση ανωμαλιών παραμένει ένα ανοιχτό ερευνητικό ζήτημα που καθορίζει την πρακτική εφαρμοσιμότητα της προσέγγισης [20], [23].

Η επιλογή του κατάλληλου αλγορίθμου μηχανικής μάθησης για ένα σύστημα ανίχνευσης εισβολών εξαρτάται από ένα σύνολο παραγόντων που υπερβαίνουν την καθαρή ακρίβεια ταξινόμησης. Οι αλγόριθμοι που βασίζονται σε δέντρα απόφασης, όπως τα τυχαία δάση, προσφέρουν το πλεονέκτημα της ερμηνευσιμότητας, που είναι ένα κρίσιμο χαρακτηριστικό για την εμπιστοσύνη του διαχειριστή. Αντίθετα, τα βαθιά νευρωνικά δίκτυα, αν και συχνά επιτυγχάνουν υψηλότερη ακρίβεια σε σύνθετα μοτίβα, λειτουργούν ως «μαύρα κουτιά» των οποίων η λογική είναι δυσδιάκριτη, ενώ απαιτούν σημαντικά μεγαλύτερους υπολογιστικούς πόρους. Στο περιβάλλον των WSNs, όπου η διαφάνεια και η ενεργειακή οικονομία είναι πρωταρχικής σημασίας, η επιλογή κλίνει συχνά προς ελαφρύτερους και ερμηνεύσιμους αλγορίθμους, ιδίως όταν η ανίχνευση πραγματοποιείται στο άκρο του δικτύου. Η τάση που διαμορφώνεται στη σύγχρονη έρευνα είναι η ανάπτυξη υβριδικών συστημάτων, όπου ένας ελαφρύς ταξινομητής εκτελεί την πρωτογενή διαλογή στους κόμβους και ένα ισχυρότερο μοντέλο αναλαμβάνει τη βαθύτερη ανάλυση στο ομιχλώδες επίπεδο, συνδυάζοντας έτσι την ταχύτητα με την ακρίβεια [20], [23].

4.3 Ομόσπονδη Μάθηση για Κατανεμημένη Ανίχνευση Εισβολών

Η ανάλυση της μηχανικής μάθησης που προηγήθηκε προϋποθέτει σιωπηρά ένα κεντρικό μοντέλο: τα δεδομένα κίνησης συλλέγονται από τους κόμβους, μεταφέρονται στον σταθμό βάσης ή στο νέφος, εκεί εκπαιδεύεται ο ταξινομητής. Το μοντέλο αυτό προσκρούει σε τρεις διακριτούς περιορισμούς. Ο πρώτος είναι ενεργειακός, καθώς η αποστολή πλήρων χαρακτηριστικών κίνησης από κάθε κόμβο ακυρώνει το όφελος της τοπικής επεξεργασίας. Ο δεύτερος αφορά την ιδιωτικότητα, ιδίως σε εφαρμογές δικτύων σώματος ή έξυπνων μετρητών, όπου τα ίδια τα πρότυπα κίνησης αποκαλύπτουν ευαίσθητη πληροφορία.

Ο τρίτος είναι αρχιτεκτονικός: η κεντρική συλλογή δημιουργεί ένα μοναδικό σημείο αστοχίας και ταυτόχρονα έναν προνομιακό στόχο.

Η ομόσπονδη μάθηση (FL - Federated Learning) αντιστρέφει τη ροή. Αντί τα δεδομένα να ταξιδεύουν προς το μοντέλο, το μοντέλο ταξιδεύει προς τα δεδομένα: κάθε συμμετέχων κόμβος ή επικεφαλής συστάδας εκπαιδεύει τοπικά ένα αντίγραφο του ταξινομητή επί των δικών του παρατηρήσεων και αποστέλλει προς τον συντονιστή μόνο τις ενημερώσεις των παραμέτρων, οι οποίες συναθροίζονται σε ένα καθολικό μοντέλο. Τα ακατέργαστα δεδομένα δεν εγκαταλείπουν ποτέ τον κόμβο.

Η αποτελεσματικότητα της προσέγγισης σε περιβάλλον δικτύων αισθητήρων έχει τεκμηριωθεί πειραματικά. Πλαίσιο ομόσπονδης μάθησης με δίκτυα μακράς βραχυπρόθεσμης μνήμης, αξιολογημένο σε πολλαπλά σύνολα δεδομένων ώστε να ελεγχθεί η γενικευσιμότητά του, αναδεικνύει ότι η κατανεμημένη εκπαίδευση μπορεί να προσεγγίσει την ακρίβεια της κεντρικής χωρίς μεταφορά ακατέργαστων δεδομένων [31]. Συστηματική αποτίμηση της επίδρασης της κλίμακας των δεδομένων δείχνει ωστόσο ότι η επίδοση εξαρτάται κρίσιμα από τον τρόπο κατανομής τους μεταξύ των συμμετεχόντων: όταν η κατανομή είναι έντονα μη ανεξάρτητη και μη ομοιόμορφη, όπως συμβαίνει τυπικά σε πραγματικά WSNs όπου κάθε κόμβος παρατηρεί διαφορετικό υποσύνολο επιθέσεων, η σύγκλιση επιβραδύνεται και απαιτούνται περισσότεροι γύροι ομοσπονδίας [32].

Η παρατήρηση αυτή έχει άμεση πρακτική σημασία. Σε ένα δίκτυο όπου μόνο ορισμένοι κόμβοι δέχονται επίθεση, οι υπόλοιποι συνεισφέρουν ενημερώσεις που περιγράφουν αποκλειστικά φυσιολογική κίνηση, με αποτέλεσμα η συνάθροιση να τείνει να «αραιώσει» τη γνώση για την επίθεση. Επιπλέον, η ίδια η αρχιτεκτονική εισάγει μια νέα επιφάνεια επίθεσης: ένας παραβιασμένος κόμβος μπορεί να υποβάλει σκόπιμα δηλητηριασμένες ενημερώσεις παραμέτρων, αλλοιώνοντας το καθολικό μοντέλο. Η ομόσπονδη μάθηση, επομένως, δεν λύνει το πρόβλημα της εμπιστοσύνης· το μετατοπίζει από το επίπεδο των δεδομένων στο επίπεδο των ενημερώσεων, όπου απαιτεί δικούς του μηχανισμούς ανθεκτικής συνάθροισης.

4.4 TinyML: Ανίχνευση Εισβολών στον Ίδιο τον Κόμβο

Η επόμενη λογική βαθμίδα μετά την ομόσπονδη μάθηση είναι η πλήρης μετάθεση του συμπερασμού στον κόμβο. Ο όρος TinyML περιγράφει το σύνολο των τεχνικών που επιτρέπουν την εκτέλεση μοντέλων μηχανικής μάθησης σε μικροελεγκτές με μνήμη μερικών δεκάδων kilobyte και κατανάλωση της τάξης των milliwatt. Οι βασικές τεχνικές είναι η κβαντοποίηση των βαρών, τυπικά από κινητή υποδιαστολή 32 bit σε ακέραιους 8 bit, το κλάδεμα των συνδέσεων με αμελητέα συνεισφορά, η απόσταση γνώσης από μεγαλύτερο μοντέλο-δάσκαλο προς μικρότερο μοντέλο-μαθητή.

Το όφελος για την ασφάλεια των WSNs είναι ουσιαστικό και όχι απλώς ποσοτικό. Ένας κόμβος που εκτελεί τοπικά ανίχνευση ανωμαλιών μπορεί να απορρίψει κακόβουλη κίνηση πριν αυτή καταναλώσει πόρους δρομολόγησης του δικτύου, εξακολουθεί να προστατεύεται ακόμη και όταν η σύνδεσή του με τον σταθμό βάσης έχει διακοπεί, κατάσταση που αποτελεί συχνά το ίδιο το αποτέλεσμα της επίθεσης. Πρόσφατη υλοποίηση ελαφρού και ενεργειακά συνειδητοποιημένου συστήματος ανίχνευσης για βιομηχανικό IoT, βασισμένη σε δίκτυα προσοχής γράφων με κατανεμημένη εκπαίδευση στα άκρα, αναφέρει ακρίβεια ανίχνευσης της τάξης του 95% έναντι ποικίλων κατηγοριών επίθεσης [33].

Η ίδια εργασία διατυπώνει ωστόσο μια επιφύλαξη που αξίζει να υπογραμμιστεί, καθώς επανέρχεται συστηματικά στη βιβλιογραφία του πεδίου: η επικύρωση της πραγματικής δυνατότητας εκτέλεσης σε πραγματικό χρόνο επί περιορισμένου υλικού απαιτεί περαιτέρω τεκμηρίωση. Η διαπίστωση αυτή αποτυπώνει ένα διαρθρωτικό χάσμα ανάμεσα στη μετρούμενη ακρίβεια ταξινόμησης, που αναφέρεται σχεδόν πάντοτε, στο μετρούμενο κόστος εκτέλεσης σε πραγματικό κόμβο, που αναφέρεται σπάνια. Για

τους σκοπούς της παρούσας εργασίας, η ακρίβεια ενός μοντέλου που δεν χωρά στη μνήμη του στοχευόμενου μικροελεγκτή είναι πρακτικά άνευ αντικειμένου.

4.5 Αρχιτεκτονικές Βαθιάς Μάθησης με Μηχανισμούς Προσοχής

Οι κλασικοί αλγόριθμοι ταξινόμησης που εξετάστηκαν, όπως τα τυχαία δάση και οι μηχανές διανυσμάτων υποστήριξης, αντιμετωπίζουν κάθε εγγραφή κίνησης ως ανεξάρτητο διάνυσμα χαρακτηριστικών. Η παραδοχή αυτή αγνοεί δύο δομικές ιδιότητες της δικτυακής κίνησης: τη χρονική της συνέχεια, καθώς μια επίθεση εκδηλώνεται ως ακολουθία γεγονότων και όχι ως μεμονωμένο πακέτο, τη χωρική της δομή, καθώς οι κόμβοι συνδέονται σε συγκεκριμένη τοπολογία που καθορίζει ποιες αλληλεπιδράσεις είναι εξαρχής δυνατές.

Οι σύγχρονες αρχιτεκτονικές βαθιάς μάθησης αξιοποιούν ακριβώς αυτές τις δομές. Υβριδικό πλαίσιο που συνδυάζει μονοδιάστατα συνελκτικά επίπεδα για την εξαγωγή τοπικών προτύπων, πυλωτές επαναληπτικές μονάδες για τη μοντελοποίηση της χρονικής εξέλιξης και μηχανισμό αυτοπροσοχής για τη στάθμιση της σημασίας κάθε χρονικού βήματος, αναφέρει επί του συνόλου WSN-DS ακρίβεια 98,6% με τιμή ROC-AUC 0,9994, ενσωματώνοντας παράλληλα συνεργατική μάθηση σε επίπεδο κόμβου [34]. Η προσθήκη του μηχανισμού προσοχής είναι κρίσιμη, διότι επιτρέπει στο μοντέλο να εντοπίζει ποιο τμήμα μιας ακολουθίας φέρει την ένδειξη της επίθεσης, αντί να συμπιέζει ολόκληρη την ακολουθία σε ένα ενιαίο διάνυσμα.

Ακόμη πιο ενδιαφέρουσα από αρχιτεκτονική άποψη είναι η εισαγωγή συνελκτικών δικτύων γράφων. Ένα δίκτυο αισθητήρων είναι εξ ορισμού γράφος, επιθέσεις όπως το Wormhole ή η Sybil εκδηλώνονται πρωτίστως ως ανωμαλίες της δομής του γράφου και όχι ως ανωμαλίες μεμονωμένων ροών: μια σύνδεση μεταξύ κόμβων που γεωγραφικά δεν θα έπρεπε να είναι γείτονες, ή ένας κόμβος με αφύσικα υψηλή κεντρικότητα. Πλαίσιο διπλής προσοχής που συνδυάζει συνελκτικά επίπεδα, συνελκτικά δίκτυα γράφων και αμφίδρομα δίκτυα μακράς βραχυπρόθεσμης μνήμης επιχειρεί να συλλάβει ταυτόχρονα τη χωρική και τη χρονική διάσταση των επιθέσεων [35]. Η προσέγγιση αυτή είναι εννοιολογικά συνεπέστερη με τη φύση των απειλών των WSNs από ό,τι η επίπεδη ταξινόμηση διανυσμάτων.

4.6 Επεξηγήσιμη Τεχνητή Νοημοσύνη στα Συστήματα Ανίχνευσης

Η αύξηση της πολυπλοκότητας των μοντέλων συνοδεύεται από ένα κόστος που η βιβλιογραφία των μετρικών ακρίβειας δεν αποτυπώνει: την απώλεια διαφάνειας. Ένα βαθύ νευρωνικό δίκτυο που ταξινομεί μια ροή ως κακόβουλη δεν παρέχει από μόνο του καμία ένδειξη για τους λόγους της απόφασής του. Σε ένα σύστημα ανίχνευσης εισβολών, η αδυναμία αυτή δεν είναι ακαδημαϊκή. Ο διαχειριστής του δικτύου καλείται να αποφασίσει αν θα απομονώσει έναν κόμβο, ενέργεια που σε ένα δίκτυο παρακολούθησης κρίσιμης υποδομής έχει πραγματικό λειτουργικό κόστος και χρειάζεται να γνωρίζει σε ποια ένδειξη στηρίχθηκε η ειδοποίηση.

Η επεξηγήσιμη τεχνητή νοημοσύνη (XAI - Explainable Artificial Intelligence) αντιμετωπίζει το ζήτημα με τεχνικές απόδοσης συνεισφοράς ανά χαρακτηριστικό. Οι δύο επικρατέστερες, οι τιμές SHAP και η μέθοδος LIME, αποδίδουν σε κάθε χαρακτηριστικό εισόδου ένα μέτρο της συμβολής του στη συγκεκριμένη πρόβλεψη. Σύστημα ανίχνευσης επί ροών δεδομένων IoT που ενσωματώνει και τις δύο τεχνικές σε συνδυασμό με μοντέλα συνελκτικών και πυκνών νευρωνικών δικτύων, αξιολογημένο σε επτά σύνολα της συλλογής TON_IoT, καταδεικνύει ότι η επεξηγησιμότητα μπορεί να προστεθεί χωρίς υποβάθμιση της επίδοσης ταξινόμησης [36].

Πέραν της υποστήριξης του διαχειριστή, η επεξηγησιμότητα επιτελεί και μια δεύτερη, λιγότερο προφανή λειτουργία: αποτελεί εργαλείο επικύρωσης του ίδιου του μοντέλου. Όταν η ανάλυση συνεισφοράς

αποκαλύπτει ότι ένας ταξινομητής στηρίζεται πρωτίστως σε χαρακτηριστικά χωρίς αιτιώδη σχέση με την επίθεση, όπως ένα αναγνωριστικό ροής ή μια χρονοσφραγίδα, τότε η υψηλή του ακρίβεια στο σύνολο δοκιμής είναι πιθανότατα τεχνούργημα του συνόλου δεδομένων και δεν θα μεταφερθεί σε πραγματική ανάπτυξη. Το ζήτημα αυτό συνδέεται άμεσα με τη μεθοδολογική κριτική που αναπτύσσεται στο Κεφάλαιο 5.

4.7 Αντιπαραθετική Μηχανική Μάθηση: Όταν το Σύστημα Ανίχνευσης Γίνεται Στόχος

Ολόκληρη η συζήτηση για τη μηχανική μάθηση στην ασφάλεια των WSNs στηρίζεται σε μια σιωπηρή και μη τεκμηριωμένη παραδοχή: ότι ο επιτιθέμενος αγνοεί την ύπαρξη του ταξινομητή ή, εν πάση περιπτώσει, δεν προσαρμόζεται σε αυτόν. Η παραδοχή αυτή είναι μεθοδολογικά ασθενής, διότι έρχεται σε αντίθεση με το βασικό μοντέλο απειλής που η ίδια η εργασία υιοθετεί, όπου ο αντίπαλος θεωρείται ορθολογικός και προσαρμοστικός. Η προσθήκη ενός μοντέλου μηχανικής μάθησης στην αμυντική διάταξη δεν εξαλείφει την επιφάνεια επίθεσης· προσθέτει μία νέα.

Η ταξινομία που έχει διαμορφώσει το NIST για την αντιπαραθετική μηχανική μάθηση διακρίνει τις σχετικές επιθέσεις σε τέσσερις κύριες κατηγορίες: επιθέσεις υπεκφυγής, όπου ο επιτιθέμενος τροποποιεί ελάχιστα την είσοδο ώστε να ταξινομηθεί εσφαλμένα· επιθέσεις δηλητηρίασης, όπου αλλοιώνονται τα δεδομένα εκπαίδευσης· επιθέσεις παραβίασης ιδιωτικότητας, όπου ανακτάται πληροφορία για τα δεδομένα εκπαίδευσης από το ίδιο το μοντέλο· και κατάχρηση, όπου το μοντέλο αξιοποιείται για σκοπό διαφορετικό από τον προβλεπόμενο [37].

Και οι τέσσερις κατηγορίες βρίσκουν άμεση εφαρμογή στα WSNs, με ιδιαιτερότητες που καθιστούν το πρόβλημα οξύτερο παρά σε συμβατικά δίκτυα. Η υπεκφυγή είναι ευκολότερη, διότι τα χαρακτηριστικά που χρησιμοποιούν τα IDS των WSNs, όπως ο ρυθμός αποστολής πακέτων ή η συχνότητα μηνυμάτων ελέγχου, βρίσκονται εξ ολοκλήρου υπό τον έλεγχο του επιτιθέμενου: αρκεί να κατανείμει την επίθεσή του χρονικά ώστε οι τιμές να παραμείνουν εντός του φυσιολογικού εύρους. Η δηλητηρίαση είναι επίσης ευκολότερη, ιδίως σε συστήματα που επανεκπαιδεύονται επιγραμμικά ή σε ομόσπονδα σχήματα, όπου ένας παραβιασμένος κόμβος συμμετέχει νόμιμα στη διαδικασία εκπαίδευσης. Ένας επιτιθέμενος με υπομονή μπορεί να αυξάνει σταδιακά την ένταση της κακόβουλης συμπεριφοράς του, μετατοπίζοντας το όριο του «φυσιολογικού» μέχρι η επίθεση να καταστεί αόρατη.

Οι διαθέσιμες αντισταθμίσεις, όπως η αντιπαραθετική εκπαίδευση, η ανθεκτική συνάθροιση ενημερώσεων στα ομόσπονδα σχήματα και η χρήση συνόλων ταξινομητών με ετερογενή χαρακτηριστικά, μειώνουν αλλά δεν εξαλείφουν τον κίνδυνο, ενώ επιβαρύνουν το υπολογιστικό κόστος. Στο πλαίσιο ενός δικτύου αισθητήρων, όπου το κόστος αυτό είναι ήδη οριακό, η ρεαλιστική στάση δεν είναι η αναζήτηση άτρωτου ταξινομητή αλλά η αποδοχή ότι το IDS αποτελεί ένα μόνο επίπεδο άμυνας, το οποίο οφείλει να συνοδεύεται από κρυπτογραφικούς μηχανισμούς που δεν υπόκεινται στην ίδια κατηγορία απειλής. Η διαπίστωση αυτή ενισχύει την επιχειρηματολογία υπέρ των υβριδικών λύσεων που διατρέχει την παρούσα εργασία [38].

4.8 Μεγάλα Γλωσσικά Μοντέλα στην Ανάλυση Ασφάλειας

Η πλέον πρόσφατη τάση στο πεδίο αφορά την αξιοποίηση μεγάλων γλωσσικών μοντέλων (LLMs - Large Language Models) για την ανάλυση δικτυακής κίνησης. Η ιδέα μοιάζει αρχικά αταίριαστη με το αντικείμενο, καθώς η κίνηση ενός δικτύου αισθητήρων δεν είναι κείμενο. Η σύνδεση προκύπτει από την παρατήρηση ότι μεγάλο μέρος των διαθέσιμων ενδείξεων ασφάλειας είναι πράγματι κειμενικής μορφής: καταγραφές συμβάντων, ονόματα πρωτοκόλλων, σημαίες πακέτων και μηνύματα σφάλματος. Τα μοντέλα που έχουν προεκπαιδευτεί σε τεράστια σώματα κειμένου διαθέτουν ικανότητα

αναγνώρισης προτύπων σε ακολουθίες συμβόλων, η οποία μπορεί να μεταφερθεί σε αυτού του είδους τα δεδομένα.

Πρόσφατο υβριδικό πλαίσιο για βιομηχανικό IoT συνδυάζει κωδικοποίηση κειμενικών χαρακτηριστικών ροής μέσω μοντέλου BERT με ταξινομητές βασισμένους σε δέντρα για τα αριθμητικά χαρακτηριστικά, αναφέροντας ακρίβεια 98,19% στο σύνολο Edge-IoTset και 99,15% στο ToN_IoT [39]. Ιδιαίτερα αξιοσημείωτη είναι η μεθοδολογική επιμέλεια της εργασίας, η οποία εφαρμόζει τεχνικές εξισορρόπησης κλάσεων αποκλειστικά επί των δεδομένων εκπαίδευσης ώστε να αποφευχθεί η διαρροή πληροφορίας προς το σύνολο δοκιμής, πρακτική που, όπως αναλύεται στο Κεφάλαιο 5, απουσιάζει από σημαντικό μέρος της βιβλιογραφίας.

Για τα WSNs, η άμεση εκτέλεση τέτοιων μοντέλων στους κόμβους είναι εκτός συζήτησης, καθώς ακόμη και τα μικρότερα μοντέλα υπερβαίνουν κατά τάξεις μεγέθους τους διαθέσιμους πόρους. Η πραγματική αρχιτεκτονική είναι κλιμακωτή: ελαφρύς ταξινομητής στον κόμβο ή στον επικεφαλής συστάδας για την ταχεία απόρριψη της προφανώς φυσιολογικής κίνησης, ανάλυση μέσω γλωσσικού μοντέλου στο επίπεδο ομίχλης ή νέφους αποκλειστικά για τις αμφίβολες περιπτώσεις και για τη συσχέτιση συμβάντων. Πρέπει πάντως να σημειωθεί ότι τα μοντέλα αυτά εισάγουν και δικές τους ευπάθειες, με χαρακτηριστικότερη την ένεση εντολών μέσω κατάλληλα διαμορφωμένων δεδομένων εισόδου, ζήτημα που παραμένει ανοιχτό.

4.9 Εφαρμογή του Blockchain για Αποκεντρωμένη Ασφάλεια στα WSNs

Η τεχνολογία Blockchain προσφέρει ένα αποκεντρωμένο και αμετάβλητο καθολικό (ledger), το οποίο μπορεί να ενισχύσει σημαντικά την εμπιστοσύνη και την ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων (WSNs). Λόγω της φύσης τους, τα WSNs είναι συχνά εκτεθειμένα σε εξωτερικές και εσωτερικές επιθέσεις (insider attacks), όπου ένας νόμιμος κόμβος παραβιάζεται και ενεργεί κακόβουλα [20]. Το Blockchain αντιμετωπίζει αυτές τις προκλήσεις παρέχοντας έναν μηχανισμό όπου κάθε συναλλαγή ή ανταλλαγή δεδομένων καταγράφεται με τρόπο που είναι αδύνατο να τροποποιηθεί εκ των υστέρων.

Αποκεντρωμένη Διαχείριση και Ακεραιότητα Δεδομένων

Σε ένα παραδοσιακό WSNs, ο Σταθμός Βάσης (Base Station) αποτελεί το κεντρικό σημείο ελέγχου. Εάν αυτός παραβιαστεί, ολόκληρο το δίκτυο καταρρέει. Η ενσωμάτωση του Blockchain επιτρέπει:

- **Κατανεμημένη Εμπιστοσύνη:** Η επαλήθευση των δεδομένων δεν βασίζεται σε έναν κεντρικό διακομιστή, αλλά σε έναν μηχανισμό συναίνεσης (consensus mechanism) μεταξύ των κόμβων ή των Cluster Heads [23].
- **Αμετάβλητη Καταγραφή:** Κάθε πακέτο δεδομένων που συλλέγεται μπορεί να σφραγίζεται κρυπτογραφικά και να αποθηκεύεται, διασφαλίζοντας ότι η πληροφορία δεν έχει αλλοιωθεί κατά τη μεταφορά από επιθέσεις όπως το "Zero-day" που συχνά διαφεύγουν από τα παραδοσιακά συστήματα [3].
- **Αυτοματοποίηση μέσω Έξυπνων Συμβολαίων (Smart Contracts):** Τα έξυπνα συμβόλαια μπορούν να εκτελούν αυτόματα πρωτόκολλα ασφαλείας, όπως η αποβολή ενός κόμβου που εμφανίζει ύποπτη συμπεριφορά, ενισχύοντας τη λειτουργία του Detector που παρουσιάστηκε στο μπλοκ διάγραμμα του IDS.

Προκλήσεις και Ελαφριές Λύσεις (Lightweight Blockchain)

Παρά τα πλεονεκτήματα, η εφαρμογή του Blockchain στα WSNs αντιμετωπίζει τον περιορισμό των πόρων (μνήμη, επεξεργαστική ισχύς, ενέργεια), παρόμοια με τα IDS που πρέπει να είναι "ελαφριά" και κλιμακωτά [5], [23]. Για το λόγο αυτό, η σύγχρονη έρευνα προτείνει:

- **Lightweight Consensus:** Χρήση αλγορίθμων που απαιτούν ελάχιστη ενέργεια, αποφεύγοντας ενεργό διαδικασίες που θα μείωναν τη διάρκεια ζωής του δικτύου [5].
- **Ιεραρχική Δομή:** Οι απλοί κόμβοι στέλνουν δεδομένα, ενώ μόνο οι ισχυρότεροι κόμβοι (Cluster Heads) συμμετέχουν στη συντήρηση της αλυσίδας, μια προσέγγιση που ευθυγραμμίζεται με την ιεραρχική δομή των IoT-based WSNs [23].
- **Off-chain Storage:** Αποθήκευση μόνο των κρίσιμων στοιχείων στην αλυσίδα για τη μείωση του φόρτου επεξεργασίας, ο οποίος μπορεί να μειωθεί έως και 7 φορές με σωστή επιλογή χαρακτηριστικών και δεδομένων [5].

Συνέργασία Blockchain και IDS

Ο συνδυασμός του Blockchain με τα συστήματα ανίχνευσης εισβολών (IDS) δημιουργεί μια πολυεπίπεδη άμυνα. Ενώ το IDS ανιχνεύει την επίθεση μέσω Μηχανικής Μάθησης με υψηλή ακρίβεια (π.χ. 98% με Random Forest [20]), το Blockchain διασφαλίζει ότι οι ειδοποιήσεις (Alarms) και τα αντίμετρα (Actions) που λαμβάνονται είναι γνήσια και δεν έχουν παραποιηθεί. Με αυτόν τον τρόπο, επιτυγχάνεται μια "συλλογική νοημοσύνη" στο δίκτυο, όπου όλοι οι κόμβοι συμφωνούν για την κατάσταση ασφαλείας, προστατεύοντας το σύστημα από επιθέσεις ευρείας κλίμακας όπως το Wormhole ή το Flooding [10], [23].

Η επιλογή του μηχανισμού συναίνεσης (consensus mechanism) αποτελεί την κρίσιμότερη σχεδιαστική απόφαση κατά την ενσωμάτωση του Blockchain σε WSNs, καθώς καθορίζει άμεσα το ενεργειακό αποτύπωμα του συστήματος. Ο κλασικός μηχανισμός Proof of Work (PoW), που χρησιμοποιείται σε δημόσια κρυπτονομίσματα, κρίνεται παντελώς ακατάλληλος λόγω της τεράστιας υπολογιστικής και ενεργειακής του απαίτησης, η οποία θα εξαντλούσε άμεσα τις μπαταρίες των κόμβων. Για τον λόγο αυτό, η έρευνα στρέφεται σε ελαφρύτερες εναλλακτικές, όπως οι μηχανισμοί Proof of Stake (PoS), Proof of Authority (PoA) και οι παραλλαγές της Πρακτικής Βυζαντινής Ανοχής Σφαλμάτων (Practical Byzantine Fault Tolerance - PBFT). Οι μηχανισμοί αυτοί επιτυγχάνουν συναίνεση με δραστικά μειωμένο κόστος, καθιστώντας εφικτή την υιοθέτηση κατανεμημένης εμπιστοσύνης ακόμη και σε δίκτυα περιορισμένων πόρων. Η επιλογή μεταξύ τους εξαρτάται από το επιθυμητό επίπεδο αποκέντρωσης και την ανοχή του δικτύου σε κακόβουλους κόμβους [5], [20].

Παρά την υπόσχεση που ενσωματώνει, η τεχνολογία Blockchain εισάγει και μια εγγενή αντίφαση όταν εφαρμόζεται σε δίκτυα αισθητήρων πραγματικού χρόνου. Η διαδικασία επίτευξης συναίνεσης και επικύρωσης των μπλοκ εισάγει αναπόφευκτη καθυστέρηση (latency), η οποία μπορεί να είναι απαγορευτική για εφαρμογές που απαιτούν άμεση αντίδραση, όπως τα συστήματα έγκαιρης προειδοποίησης ή ο βιομηχανικός έλεγχος. Επιπλέον, το διαρκώς αυξανόμενο μέγεθος του καθολικού (ledger bloat) έρχεται σε ευθεία αντίθεση με την περιορισμένη αποθηκευτική ικανότητα των κόμβων, καθιστώντας αναγκαία τη χρήση τεχνικών αποθήκευσης εκτός αλυσίδας (off-chain). Η κριτική αυτή αποτίμηση οδηγεί στο συμπέρασμα ότι το Blockchain δεν αποτελεί καθολική λύση, αλλά ένα εργαλείο με σαφώς οριοθετημένο πεδίο εφαρμογής: ενδείκνυται για τη διασφάλιση της ακεραιότητας και της μη αποποίησης σε σενάρια όπου η ανθεκτικότητα υπερτερεί της χαμηλής καθυστέρησης και όχι ως υποκατάστατο των ελαφρών κρυπτογραφικών μηχανισμών της επικοινωνίας πραγματικού χρόνου [10], [23].

Η εφαρμογή του blockchain στα WSNs δεν περιορίζεται στη διαχείριση της εμπιστοσύνης, αλλά επεκτείνεται και στη διασφάλιση της προέλευσης των δεδομένων (data provenance). Σε ένα κατακεντρωμένο δίκτυο αισθητήρων, η δυνατότητα αδιάψευστης τεκμηρίωσης της πορείας ενός δεδομένου, από τη στιγμή της συλλογής του έως την τελική του αποθήκευση, είναι κρίσιμη για εφαρμογές όπου η αξιοπιστία της πληροφορίας έχει νομικές ή οικονομικές προεκτάσεις. Καταχωρώντας τις μετρήσεις και τις μεταξύ τους μεταβιβάσεις σε ένα αμετάβλητο κατακεντρωμένο καθολικό, το blockchain παρέχει μια ελεγχόμενη και επαληθεύσιμη αλυσίδα ευθύνης. Ωστόσο, η πρακτική υλοποίηση αυτής της δυνατότητας προσκρούει στους περιορισμούς αποθήκευσης των κόμβων, καθώς το μέγεθος του καθολικού αυξάνεται μονοτονικά με τον χρόνο. Για την αντιμετώπιση του προβλήματος αυτού, αναπτύσσονται ελαφριές παραλλαγές, όπως τα δίκτυα κατευθυνόμενων ακυκλικών γράφων (Directed Acyclic Graphs - DAG), τα οποία εγκαταλείπουν τη γραμμική δομή της αλυσίδας υπέρ μιας πιο κλιμακώσιμης και ενεργειακά αποδοτικής τοπολογίας.

Παρά τις υποσχέσεις του, το blockchain δεν αποτελεί καθολική λύση για την ασφάλεια των WSNs και η κριτική του αποτίμηση είναι απαραίτητη. Το θεμελιώδες εμπόδιο παραμένει η αναντιστοιχία μεταξύ των απαιτήσεων των μηχανισμών συναίνεσης και των διαθέσιμων πόρων των αισθητήρων. Ακόμη και οι ελαφρύτεροι αλγόριθμοι συναίνεσης εισάγουν καθυστέρηση και επικοινωνιακό κόστος που μπορεί να είναι απαγορευτικά για εφαρμογές πραγματικού χρόνου. Επιπλέον, η αποκέντρωση, αν και ενισχύει την ανθεκτικότητα έναντι μεμονωμένων σημείων αστοχίας, δεν εξαλείφει όλες τις απειλές· επιθέσεις όπως η επίθεση των 51% — κατά την οποία ένας κακόβουλος δρων που ελέγχει την πλειοψηφία της υπολογιστικής ισχύος του δικτύου blockchain μπορεί να αναιρέσει επιβεβαιωμένες συναλλαγές ή να επιβάλει τη δική του εκδοχή του κατακεντρωμένου καθολικού—, αν και δυσχερείς, παραμένουν θεωρητικά εφικτές σε δίκτυα με μικρό αριθμό κόμβων. Συνεπώς, το blockchain πρέπει να θεωρείται ως ένα συμπληρωματικό εργαλείο εντός μιας ευρύτερης στρατηγικής άμυνας σε βάθος και όχι ως αυτοτελής λύση που υποκαθιστά τους κλασικούς κρυπτογραφικούς μηχανισμούς [19], [20].

Η ενσωμάτωση του blockchain στα δίκτυα αισθητήρων δεν αποτελεί μαγική λύση, αλλά μια στοχευμένη λύση κατάλληλη για συγκεκριμένες κατηγορίες προβλημάτων. Η πλέον υποσχόμενη εφαρμογή του εντοπίζεται στη διαχείριση της ταυτότητας και της εμπιστοσύνης, όπου το αμετάβλητο και αποκεντρωμένο μητρώο μπορεί να καταγράφει αξιόπιστα την κατάσταση και τη φήμη κάθε κόμβου χωρίς την ανάγκη μιας κεντρικής αρχής. Σε αυτό το πλαίσιο, ένας παραβιασμένος κόμβος δεν μπορεί να διαγράψει ή να αλλοιώσει το ιστορικό της κακόβουλης συμπεριφοράς του, καθώς αυτό είναι μόνιμα εγγεγραμμένο στην αλυσίδα και επαληθεύσιμο από όλους τους συμμετέχοντες. Ωστόσο, η υιοθέτηση του blockchain στους περιορισμένους κόμβους απαιτεί προσεκτικό σχεδιασμό, καθώς το πλήρες βάρος της διατήρησης και επαλήθευσης της αλυσίδας ανατίθεται κατά κανόνα στους ισχυρότερους κόμβους ή στο ομιχλώδες επίπεδο, ενώ οι απλοί αισθητήρες λειτουργούν ως ελαφρείς πελάτες. Η αρχιτεκτονική αυτή διαφοροποίηση είναι θεμελιώδης για τη βιωσιμότητα της λύσης σε πραγματικές συνθήκες [9], [19].

4.9.1 Σύγχρονες Υβριδικές Αρχιτεκτονικές Blockchain και Μηχανικής Μάθησης

Η κριτική που ασκήθηκε παραπάνω στην εφαρμογή του blockchain στα WSNs και συγκεκριμένα το απαγορευτικό κόστος των μηχανισμών συναίνεσης για περιορισμένους κόμβους, έχει οδηγήσει την πρόσφατη έρευνα σε μια σαφή αρχιτεκτονική στροφή. Αντί το blockchain να επεκτείνεται σε ολόκληρο το δίκτυο, περιορίζεται στο ανώτερο επίπεδο της ιεραρχίας, όπου οι κόμβοι διαθέτουν επαρκείς πόρους, ενώ οι απλοί αισθητήρες παραμένουν παθητικοί συμμετέχοντες.

Χαρακτηριστική εφαρμογή της λογικής αυτής αποτελεί διστρωματικό πλαίσιο ανίχνευσης στο οποίο ένα ελαφρύ πρωτόκολλο blockchain λειτουργεί αποκλειστικά μεταξύ των επικεφαλής συστάδων και του σταθμού βάσης, καταγράφοντας αμετάβλητα τις συνόψεις των δεδομένων ώστε να ανιχνεύονται

παραβιάσεις ακεραιότητας, ενώ ένα τεχνητό νευρωνικό δίκτυο εγκατεστημένο στον σταθμό βάσης αναλαμβάνει τον εντοπισμό των επιθέσεων που παρακάμπτουν τον έλεγχο της αλυσίδας. Η επίδοση που αναφέρεται ανέρχεται σε 97,42% ακρίβεια και 98,35% ανάκληση, με ποσοστά ανίχνευσης άνω του 99,98% ακόμη και υπό συνθήκες τριάντα ταυτόχρονων επιτιθέμενων, χωρίς πρόσθετη επεξεργαστική επιβάρυνση των κόμβων αισθητήρων [40].

Παρόμοια αρχιτεκτονική λογική διέπει και πλαίσια που αναθέτουν στο blockchain τη διαχείριση ταυτότητας και εμπιστοσύνης μέσω έξυπνων συμβολαίων, διατηρώντας την ανίχνευση εσωτερικών απειλών σε ξεχωριστή ενότητα μηχανικής μάθησης με αλγορίθμους ενίσχυσης κλίσης [41]. Το κοινό συμπέρασμα των εργασιών αυτών είναι ότι το blockchain στα WSNs έχει αξία όχι ως γενικός μηχανισμός εμπιστοσύνης, αλλά ως εξειδικευμένο μητρώο αμετάβλητης καταγραφής για συγκεκριμένες, χαμηλής συχνότητας λειτουργίες: εγγραφή κόμβων, ανάκληση διαπιστευτηρίων και επικύρωση συνόψεων. Η προσπάθεια επέκτασής του στην καταγραφή κάθε μέτρησης παραμένει ενεργειακά ασύμφορη.

4.10 Edge & Fog Computing

Η παραδοσιακή αρχιτεκτονική των WSNs βασιζόταν στη μεταφορά όλων των δεδομένων σε έναν κεντρικό Σταθμό Βάσης ή στο Cloud για επεξεργασία. Ωστόσο, η προσέγγιση αυτή δημιουργεί σημαντικές καθυστερήσεις (latency) και εκθέτει τα δεδομένα σε κινδύνους κατά τη διαδρομή τους. Το Edge και το Fog Computing ενισχύοντας την Ασφάλεια στο Άκρο του Δικτύου εισάγουν ενδιάμεσα επίπεδα επεξεργασίας που επιτρέπουν την ανίχνευση απειλών σε πραγματικό χρόνο, ακριβώς εκεί που παράγεται η πληροφορία, αντιμετωπίζοντας την ανάγκη για συστήματα που είναι ελαφριά, κλιμακωτά και ικανά να λειτουργούν σε περιβάλλοντα με υψηλό θόρυβο.

Τοπική Ανίχνευση και Μείωση Καθυστερήσης

Στα IoT-based WSNs, η υιοθέτηση μιας ιεραρχικής δομής είναι απαραίτητη για την αντιμετώπιση επιθέσεων ευρείας κλίμακας. Η επεξεργασία στο επίπεδο του Edge επιτρέπει:

- Τοπική Ανίχνευση: Κάθε κόμβος παρακολουθεί τους άμεσους γείτονές του, επιτρέποντας την έγκαιρη αναγνώριση εσωτερικών επιθέσεων (insider attacks).
- Ταχεία Απόκριση: Η ανίχνευση επιθέσεων όπως το Flooding στο επίπεδο μεταφοράς ή το Wormhole απαιτεί άμεση αντίδραση, η οποία διευκολύνεται από τη συγκεντρωτική ανάλυση σε τοπικό επίπεδο.
- Φιλτράρισμα Δεδομένων: Το Edge επίπεδο μπορεί να απορρίψει κακόβουλα πακέτα πριν αυτά επιβαρύνουν το υπόλοιπο δίκτυο, λειτουργώντας ως πρώτο στάδιο προστασίας.

Βελτιστοποίηση Πόρων μέσω Fog Computing

Το επίπεδο Fog λειτουργεί ως γέφυρα μεταξύ των περιορισμένων σε πόρους αισθητήρων και του Cloud. Λόγω των λιγοστών ενεργειακών αποθεμάτων των WSNs, η χρήση του Fog είναι καταλυτική για την υποστήριξη συστημάτων IDS:

- Κατανεμημένη Επεξεργασία: Το Fog Computing επιτρέπει την εκτέλεση σύνθετων αλγορίθμων, όπως το μοντέλο Random Forest που επιτυγχάνει συνολική ακρίβεια έως και 98%.
- Μείωση Όγκου Δεδομένων: Μέσω τεχνικών επιλογής χαρακτηριστικών (Feature Selection), όπως το MRMR, ο αριθμός των χαρακτηριστικών μειώνεται από 41 σε 12. Αυτό μειώνει τον χρόνο

εκπαίδευσης και επεξεργασίας κατά 7 φορές, διατηρώντας παράλληλα την ακρίβεια πάνω από το 98.5%.

- Συγκεντρωτική Ανάλυση: Οι Cluster Heads ή οι Fog Nodes αναλύουν δεδομένα για τον εντοπισμό σύνθετων απειλών που απαιτούν ευρύτερη εικόνα του δικτύου.

Ενίσχυση της Ιδιωτικότητας και της Ανθεκτικότητας

Η επεξεργασία στο άκρο του δικτύου περιορίζει την έκθεση ευαίσθητων πληροφοριών, καθώς μειώνεται η απόσταση που διανύουν τα δεδομένα.

- Ανθεκτικότητα σε Αποσύνδεση: Σε περίπτωση επίθεσης, οι Edge κόμβοι μπορούν να λειτουργήσουν αυτόνομα, λαμβάνοντας τοπικά αντίμετρα (Actions) και ενεργοποιώντας συναγερμούς (Alarms) βάσει του λειτουργικού διαγράμματος του IDS.
- Προστασία Ιδιοτήτων: Η τοπική επεξεργασία επιτρέπει την αφαίρεση πλεονάζουσας πληροφορίας πριν τη μετάδοση, διασφαλίζοντας ότι μόνο τα απαραίτητα δεδομένα προωθούνται για περαιτέρω ανάλυση, γεγονός που μειώνει την ενεργειακή κατανάλωση.

Η αρχιτεκτονική του ομίχλωσης υπολογισμού (fog computing) εισάγει ένα ενδιάμεσο επίπεδο επεξεργασίας μεταξύ των κόμβων αισθητήρων και του απομακρυσμένου υπολογιστικού νέφους (cloud), μετατοπίζοντας την ευφυΐα πλησιέστερα στην πηγή των δεδομένων. Στο πλαίσιο της ασφάλειας, η προσέγγιση αυτή προσφέρει πολλαπλά οφέλη: η τοπική επεξεργασία και ανάλυση της κίνησης στους κόμβους ομίχλης (fog nodes) μειώνει δραστικά την ποσότητα των ευαίσθητων δεδομένων που διασχίζουν το δίκτυο, περιορίζοντας την επιφάνεια επίθεσης. Παράλληλα, η εγγύτητα του επιπέδου ομίχλης επιτρέπει την ανίχνευση και την αντιμετώπιση απειλών με χαμηλή καθυστέρηση, κάτι που είναι αδύνατο όταν η ανάλυση πραγματοποιείται αποκλειστικά στο απομακρυσμένο νέφος. Η κατανομημένη αυτή τοπολογία ενισχύει επιπλέον την ανθεκτικότητα του συστήματος, καθώς η αστοχία ή η παραβίαση ενός κόμβου ομίχλης δεν συνεπάγεται την κατάρρευση ολόκληρης της υποδομής ασφαλείας [7], [23].

Ωστόσο, η μετατόπιση της επεξεργασίας προς το άκρο του δικτύου δεν είναι απαλλαγμένη από κινδύνους, καθώς διευρύνει η ίδια την επιφάνεια επίθεσης. Οι κόμβοι ομίχλης και άκρου, βρίσκόμενοι συχνά σε φυσικά εκτεθειμένες τοποθεσίες, καθίστανται ελκυστικοί στόχοι για επιθέσεις παραβίασης, ενώ η ετερογένειά τους δυσχεραίνει την ενιαία διαχείριση της ασφάλειας. Δημιουργείται έτσι μια κρίσιμη αντιστάθμιση: η αποκέντρωση ενισχύει την ανθεκτικότητα και μειώνει την καθυστέρηση, αλλά ταυτόχρονα πολλαπλασιάζει τα σημεία που πρέπει να προστατευθούν και να παρακολουθηθούν. Η ορθή αξιοποίηση του παραδείγματος edge και fog computing απαιτεί συνεπώς μια ολιστική προσέγγιση ασφαλείας, η οποία να εκτείνεται ομοιόμορφα σε όλα τα επίπεδα του συστήματος, από τον απλούστερο αισθητήρα έως τον ισχυρότερο κόμβο ομίχλης, διασφαλίζοντας ότι κανένα επίπεδο δεν αποτελεί τον αδύναμο κρίκο της συνολικής άμυνας [7], [10].

Η αρχιτεκτονική του ομίχλωσης υπολογισμού (fog computing) επιτρέπει την υλοποίηση μιας ιεραρχικής στρατηγικής ασφάλειας, στην οποία οι υπολογιστικές απαιτητικές λειτουργίες ανατίθενται στους κόμβους ομίχλης, ενώ οι αισθητήρες επιφορτίζονται μόνο με ελαφρείς ελέγχους. Στο μοντέλο αυτό, ο κόμβος ομίχλης λειτουργεί ως ένα τοπικό κέντρο ανάλυσης, ικανό να εκτελεί σύνθετους αλγορίθμους ανίχνευσης εισβολών, να συσσωρεύει και να συσχετίζει δεδομένα από πολλαπλούς αισθητήρες και να λαμβάνει αποφάσεις ασφαλείας με χαμηλή καθυστέρηση, χωρίς την ανάγκη επικοινωνίας με το απομακρυσμένο νέφος. Η εγγύτητα αυτή στο σημείο παραγωγής των δεδομένων μειώνει δραστικά τόσο την κατανάλωση ενέργειας όσο και τον χρόνο απόκρισης, καθιστώντας εφικτή την ανίχνευση και

αντιμετώπιση απειλών σχεδόν σε πραγματικό χρόνο. Παράλληλα, η τοπική επεξεργασία περιορίζει την έκθεση ευαίσθητων δεδομένων στο διαδίκτυο, ενισχύοντας την ιδιωτικότητα.

Η μετατόπιση της επεξεργασίας προς το άκρο του δικτύου, ωστόσο, εισάγει και νέες προκλήσεις ασφάλειας που πρέπει να εξεταστούν κριτικά. Οι κόμβοι ομίχλης (fog computing), λόγω της αυξημένης τους ισχύος και της κεντρικής τους θέσης στην αρχιτεκτονική, αποτελούν ελκυστικούς στόχους για επιτιθέμενους· η παραβίαση ενός τέτοιου κόμβου μπορεί να έχει δυσανάλογα μεγαλύτερες συνέπειες από την παραβίαση ενός απλού αισθητήρα, καθώς ελέγχει την ασφάλεια ολόκληρης της τοπικής συστάδας. Επιπλέον, η κατανεμημένη φύση της αρχιτεκτονικής ομίχλης διευρύνει την επιφάνεια επίθεσης και περιπλέκει τη διαχείριση της εμπιστοσύνης μεταξύ των διαφόρων επιπέδων. Συνεπώς, η ασφάλεια του fog computing απαιτεί ισχυρή αμοιβαία αυθεντικοποίηση μεταξύ αισθητήρων, κόμβων ομίχλης και νέφους, καθώς και μηχανισμούς που διασφαλίζουν ότι η παραβίαση ενός επιπέδου δεν διαδίδεται στα υπόλοιπα. Η ισορροπημένη αξιοποίηση των πλεονεκτημάτων της εγγύτητας, με ταυτόχρονη θωράκιση των νέων σημείων ευπάθειας, αποτελεί το κλειδί για την επιτυχή ενσωμάτωση του fog computing στην ασφάλεια των WSNs [10], [19].

Σε αντιδιαστολή με το fog computing, το edge computing μετακινεί την επεξεργασία ακόμη πιο κοντά στην πηγή —στον ίδιο τον αισθητήρα ή στην πύλη (gateway)— επιτρέποντας άμεση αντίδραση χωρίς εξάρτηση από το υπόλοιπο δίκτυο. Έτσι αναδύεται μια φυσική ιεραρχία εργασιών: οι κόμβοι στο άκρο (edge) αναλαμβάνουν ελαφρείς, άμεσους ελέγχους βασισμένους σε φυσικά χαρακτηριστικά, οι κόμβοι του ομιχλώδους επιπέδου (fog layer) εκτελούν ενδιάμεση συνάθροιση και ανάλυση συμπεριφοράς, ενώ οι πλατφόρμες του νέφους αναλαμβάνουν τη βαριά ανάλυση και την εκπαίδευση των μοντέλων. Η επεξεργασία στο άκρο ενισχύει επιπλέον την ιδιωτικότητα, καθώς τα ευαίσθητα δεδομένα μπορούν να αναλυθούν και να φιλτραριστούν επιτόπου, χωρίς να εγκαταλείψουν τη συσκευή. Η κατανομή αυτή επιτρέπει την ταχεία τοπική αντίδραση σε προφανείς απειλές, διατηρώντας παράλληλα τη δυνατότητα σύνθετης ανάλυσης για πιο εξελιγμένες επιθέσεις στα ανώτερα επίπεδα [19], [23].

Η ασφάλεια στο επίπεδο του άκρου απαιτεί ιδιαίτερη ανάλυση, καθώς οι περιορισμοί των συσκευών edge διαφέρουν ουσιαδώς από εκείνους των ισχυρότερων κόμβων ομίχλης. Η εκτέλεση της ανίχνευσης απευθείας στον αισθητήρα ή στην πύλη (on-device inference) επιβάλλει τη χρήση εξαιρετικά ελαφρών μοντέλων —όπως κλαδεμένα δέντρα απόφασης ή κβαντισμένοι ταξινομητές— ώστε η επεξεργασία να χωρά στη διαθέσιμη μνήμη και να μην εξαντλεί την μπαταρία. Ταυτόχρονα, η φυσική έκθεση των συσκευών άκρου, οι οποίες συχνά εγκαθίστανται σε μη ελεγχόμενα σημεία, τις καθιστά εύαλωτες σε επιθέσεις παραβίασης υλικού (physical tampering), εξαγωγής κλειδιών από τη μνήμη και πλαστογράφησης μετρήσεων. Το πλεονέκτημα της άμεσης απόκρισης και της τοπικής προστασίας της ιδιωτικότητας —τα δεδομένα φιλτράρονται πριν εγκαταλείψουν τη συσκευή— πρέπει επομένως να σταθμίζεται έναντι της αδυναμίας του άκρου να υποστηρίξει βαρείς κρυπτογραφικούς μηχανισμούς και της ανάγκης για ασφαλή αποθήκευση κλειδιών. Η αποτελεσματική θωράκιση του edge επιπέδου στηρίζεται συνεπώς σε ελαφριά κρυπτογραφία, τακτική επικαιροποίηση των τοπικών μοντέλων και μηχανισμούς διασφάλισης της ακεραιότητας του υλικολογισμικού (firmware integrity) [19], [23].

4.11 Προστασία Ιδιωτικότητας (Privacy-preserving Techniques)

Η προστασία της ιδιωτικότητας στα WSNs είναι εξίσου κρίσιμη με την ασφάλεια του δικτύου, καθώς οι αισθητήρες συχνά συλλέγουν ευαίσθητα δεδομένα (π.χ. ιατρικά δεδομένα ή δεδομένα τοποθεσίας). Λόγω των περιορισμένων πόρων και της έλλειψης κεντρικής διακυβέρνησης, τα συστήματα πρέπει να είναι ελαφριά και ανθεκτικά σε εσωτερικές επιθέσεις (insider attacks), όπου ένας παραβιασμένος κόμβος μπορεί να προσπαθήσει να διαρρεύσει πληροφορίες.

Στρατηγικές Προστασίας και Ανωνυμοποίησης

Οι τεχνικές προστασίας της ιδιωτικότητας εστιάζουν στην απόκρυψη της ταυτότητας του αποστολέα και του περιεχομένου των δεδομένων:

- **Ανωνυμοποίηση μέσω Επιλογής Χαρακτηριστικών:** Η χρήση τεχνικών επιλογής χαρακτηριστικών (Feature Selection), όπως το MRMR, επιτρέπει τη διατήρηση μόνο των απαραίτητων μεταβλητών για την ανάλυση, αφαιρώντας πλεονάζουσες πληροφορίες που θα μπορούσαν να ταυτοποιήσουν τον χρήστη.
- **Προστασία Τοποθεσίας (Location Privacy):** Χρησιμοποιούνται τεχνικές όπως η προσθήκη "θορύβου" ή η χρήση ενδιάμεσων κόμβων (proxy nodes) για να αποτραπεί ο εντοπισμός της φυσικής θέσης του Σταθμού Βάσης ή της πηγής των δεδομένων.
- **Διαφορική Ιδιωτικότητα (Differential Privacy):** Εισάγεται στατιστικός θόρυβος στα συγκεντρωτικά δεδομένα που αναλύονται από τον Detector, έτσι ώστε να είναι αδύνατο να εξαχθούν συμπεράσματα για έναν συγκεκριμένο κόμβο, διατηρώντας όμως την ακρίβεια του συνόλου.

Ιδιωτικότητα στην Ανίχνευση Ανωμαλιών

Τα συστήματα ανίχνευσης ανωμαλιών (Anomaly-based IDS) διαδραματίζουν διπλό ρόλο στην προστασία της ιδιωτικότητας:

- **Αυτοματοποιημένη Προστασία:** Ορίζοντας προφίλ «φυσιολογικής συμπεριφοράς», το σύστημα μπορεί να ανιχνεύσει μη εξουσιοδοτημένες προσπάθειες πρόσβασης σε ευαίσθητα αρχεία ή βάσεις δεδομένων.
- **Αποτελεσματική Ταξινόμηση:** Αλγόριθμοι όπως ο Random Forest επιτυγχάνουν ακρίβεια 98% στην ταξινόμηση της κίνησης, διασφαλίζοντας ότι οι κακόβουλες προσπάθειες υποκλοπής δεδομένων αναγνωρίζονται άμεσα.
- **Περιορισμός Ψευδώς Θετικών:** Η βελτιστοποίηση των μοντέλων, όπως ο Decision Tree που επιτυγχάνει 96% ακρίβεια, μειώνει τα False Positives, αποτρέποντας άσκοπες διακοπές στη μετάδοση ευαίσθητων δεδομένων.

Συμπερασματική Προσέγγιση

Η προστασία της ιδιωτικότητας επιτυγχάνεται μέσω μιας ιεραρχικής δομής, όπου η τοπική ανίχνευση στους κόμβους και η συγκεντρωτική ανάλυση στους Cluster Heads διασφαλίζουν ότι τα δεδομένα παραμένουν προστατευμένα σε κάθε στάδιο. Με την εφαρμογή τεχνικών που μειώνουν τον χρόνο επεξεργασίας κατά 7 φορές, οι μηχανισμοί ιδιωτικότητας γίνονται πρακτικά εφαρμόσιμοι ακόμη και στους πιο αδύναμους αισθητήρες του δικτύου.

Μια θεμελιώδης πρόκληση που διατρέχει το σύνολο των τεχνικών προστασίας ιδιωτικότητας στα WSNs είναι η εγγενής ένταση μεταξύ της χρησιμότητας των δεδομένων (data utility) και του βαθμού προστασίας. Κάθε μηχανισμός που αποσκοπεί στην απόκρυψη ή τη διατάραξη της πληροφορίας —είτε πρόκειται για διαφορική ιδιωτικότητα, είτε για ανωνυμοποίηση, είτε για προσθήκη θορύβου— μειώνει αναπόφευκτα την ακρίβεια και τη λεπτομέρεια των δεδομένων που τελικά αξιοποιούνται. Σε εφαρμογές

κρίσιμης σημασίας, όπως η ιατρική παρακολούθηση, η υπερβολική διατάραξη μπορεί να καταστήσει τα δεδομένα άχρηστα για κλινική χρήση, ενώ η ανεπαρκής προστασία εκθέτει τον ασθενή. Η εξεύρεση του βέλτιστου σημείου ισορροπίας μεταξύ αυτών των δύο αντικρουόμενων στόχων δεν αποτελεί απλώς τεχνικό ζήτημα, αλλά απαιτεί τη συνεκτίμηση του εκάστοτε κανονιστικού πλαισίου και των ηθικών διαστάσεων της εφαρμογής [7], [10].

Η ασφάλεια και η ιδιωτικότητα στα WSNs δεν πρέπει να αντιμετωπίζονται ως ανεξάρτητοι στόχοι, αλλά ως αλληλένδετες διαστάσεις ενός ενιαίου προβλήματος εμπιστοσύνης. Ένα δίκτυο μπορεί να είναι απολύτως ασφαλές έναντι εξωτερικών εισβολέων αλλά να παραβιάζει την ιδιωτικότητα των υποκειμένων μέσω της ίδιας της συλλογής και συγκέντρωσης δεδομένων· αντίστροφα, υπερβολικά αυστηροί μηχανισμοί ιδιωτικότητας μπορεί να υπονομεύσουν τους ίδιους τους μηχανισμούς ασφάλειας που στηρίζονται στην ανάλυση της κίνησης. Η σύγχρονη ερευνητική κατεύθυνση αναγνωρίζει αυτή τη συμπληρωματικότητα και προτείνει ολοκληρωμένα πλαίσια που σχεδιάζουν την ασφάλεια και την ιδιωτικότητα εκ των προτέρων (privacy by design), αντί να τις προσθέτουν εκ των υστέρων ως αντισταθμίσματα. Η προσέγγιση αυτή αποτελεί το πλέον ώριμο στάδιο της εξέλιξης των μηχανισμών προστασίας στα δίκτυα αισθητήρων [7], [10].

Ένας θεμελιώδης διαχωρισμός στο πεδίο της ιδιωτικότητας των WSNs αφορά τη διάκριση μεταξύ της ιδιωτικότητας περιεχομένου (content privacy) και της ιδιωτικότητας συμφραζομένων (contextual privacy). Η πρώτη αναφέρεται στην προστασία του ίδιου του περιεχομένου των μετρήσεων, κάτι που επιτυγχάνεται κατά κανόνα μέσω κρυπτογράφησης. Η δεύτερη, ωστόσο, αφορά την προστασία μετα-πληροφορίας που μπορεί να αποκαλυφθεί ακόμη και όταν το περιεχόμενο είναι κρυπτογραφημένο, όπως η ταυτότητα και η θέση του κόμβου που εκπέμπει ή ο χρόνος και η συχνότητα των μεταδόσεων. Η προστασία της ιδιωτικότητας θέσης (location privacy) είναι ιδιαίτερα κρίσιμη σε εφαρμογές παρακολούθησης άγριας ζωής ή στρατιωτικές εφαρμογές, όπου η αποκάλυψη της θέσης μιας πηγής δεδομένων θα μπορούσε να θέσει σε κίνδυνο το παρακολουθούμενο υποκείμενο. Η αντιμετώπιση αυτής της απειλής απαιτεί εξειδικευμένες τεχνικές, όπως η δρομολόγηση μέσω πλασματικών πηγών (fake source routing), που αποπροσανατολίζουν έναν παρατηρητή ο οποίος αναλύει την κίνηση του δικτύου.

Η τεχνική της διαφορικής ιδιωτικότητας (differential privacy), που αναφέρθηκε ως μηχανισμός προστασίας, αξίζει περαιτέρω ανάλυσης ως προς τις πρακτικές της επιπτώσεις στα δίκτυα αισθητήρων. Η βασική της αρχή συνίσταται στην προσθήκη ελεγχόμενου στατιστικού θορύβου στα συναθροισμένα δεδομένα, ώστε η συμμετοχή ή μη ενός μεμονωμένου κόμβου να μην μπορεί να συναχθεί από το τελικό αποτέλεσμα. Η κρισιμότητα της προσέγγισης έγκειται στη ρύθμιση της παραμέτρου ιδιωτικότητας, η οποία καθορίζει την ένταση του θορύβου, ο υψηλότερος θόρυβος προσφέρει ισχυρότερη προστασία αλλά υποβαθμίζει την ακρίβεια των δεδομένων, ενώ αντίστροφα χαμηλότερος θόρυβος διατηρεί τη χρησιμότητα εις βάρος της ιδιωτικότητας. Η εξεύρεση της σωστής ισορροπίας μεταξύ ιδιωτικότητας και χρησιμότητας (privacy-utility trade-off) αποτελεί το κεντρικό ζήτημα στην εφαρμογή της τεχνικής και εξαρτάται άμεσα από την ευαισθησία της εκάστοτε εφαρμογής. Η ενσωμάτωση της διαφορικής ιδιωτικότητας σε πρωτόκολλα ασφαλούς συνάθροισης αναδεικνύεται ως μια από τις πλέον υποσχόμενες κατευθύνσεις για τη συμμόρφωση των WSNs με αυστηρά κανονιστικά πλαίσια προστασίας δεδομένων [7], [9].

4.12 Δυναμική Αξιολόγηση Εμπιστοσύνης και Ενισχυτική Μάθηση στη Δρομολόγηση

Οι μηχανισμοί εμπιστοσύνης που παρουσιάστηκαν στο Κεφάλαιο 3 στηρίζονται κατά κανόνα σε στατικούς κανόνες: ένας κόμβος χάνει βαθμούς εμπιστοσύνης όταν παραλείπει να προωθήσει πακέτα ή όταν αποκλίνει από ένα προκαθορισμένο πρότυπο συμπεριφοράς. Η προσέγγιση αυτή είναι απλή και ενεργειακά οικονομική, αλλά αδυνατεί να διακρίνει τη κακόβουλη δράση από τη νόμιμη υποβάθμιση

απόδοσης λόγω εξάντλησης μπαταρίας ή περιβαλλοντικών παρεμβολών, με αποτέλεσμα τον άδικο αποκλεισμό υγιών κόμβων.

Οι σύγχρονες προσεγγίσεις αντιμετωπίζουν το πρόβλημα με πολυδιάστατη, μαθησιακή εκτίμηση της εμπιστοσύνης. Πρόσφατο πλαίσιο εξάγει χαρακτηριστικά όπως η σχέση συντοπικότητας, η σχέση συνεργασίας και η τριάδα συνεργατικότητας-συχνότητας-διάρκειας και τα επεξεργάζεται με συνδυασμό ομαδοποίησης, ανάλυσης κύριων συνιστωσών και μηχανών διανυσμάτων υποστήριξης. Το αναφερόμενο ποσοστό ανίχνευσης φτάνει το 96% με ποσοστό ψευδώς αρνητικών 0,7%, ακόμη και παρουσία πενήντα παραβιασμένων κόμβων [42]. Η ουσιώδης διαφορά έναντι των στατικών σχημάτων είναι ότι η εμπιστοσύνη δεν αποτιμάται από μία μεμονωμένη μετρική αλλά από το συνολικό προφίλ αλληλεπίδρασης του κόμβου με τους γείτονές του, γεγονός που δυσχεραίνει σημαντικά την προσποίηση καλής συμπεριφοράς.

Η φυσική συνέχεια της λογικής αυτής είναι η ενσωμάτωση της εμπιστοσύνης στην ίδια την απόφαση δρομολόγησης μέσω ενισχυτικής μάθησης. Σε πλαίσιο βαθιάς ενισχυτικής μάθησης για ασφαλή δρομολόγηση σε στρατιωτικά δίκτυα αισθητήρων, ο πράκτορας μαθαίνει πολιτική επιλογής επόμενου άλματος που βελτιστοποιεί ταυτόχρονα την ενεργειακή αποδοτικότητα και την ανθεκτικότητα σε επιθέσεις Sinkhole, άρνησης υπηρεσίας και ανάλυσης κίνησης, με αναφερόμενη βελτίωση της αποδοτικότητας δρομολόγησης κατά περίπου 20% και ακρίβεια ανίχνευσης εισβολών 99,46% [43].

Η κριτική παρατήρηση που αρμόζει εδώ αφορά το κόστος εξερεύνησης. Ένας πράκτορας ενισχυτικής μάθησης βελτιώνει την πολιτική του δοκιμάζοντας ενέργειες και οι δοκιμές αυτές συνεπάγονται μεταδόσεις. Σε ένα δίκτυο όπου κάθε μετάδοση αφαιρεί από ένα πεπερασμένο ενεργειακό απόθεμα, το κόστος της φάσης εκμάθησης δεν είναι αμελητέο και σπανίως συνυπολογίζεται στους δημοσιευμένους απολογισμούς. Η προεκπαίδευση σε προσομοιωτή με επακόλουθη σταδιακή προσαρμογή στο πεδίο αποτελεί την πλέον ρεαλιστική διέξοδο, εισάγει όμως εξάρτηση από την πιστότητα του προσομοιωτή.

4.13 Επίλογος

Στο κεφάλαιο αυτό αναδείχθηκε η σημασία των σύγχρονων τεχνολογιών στην ασφάλεια των Ασύρματων Δικτύων Αισθητήρων (WSNs), οι οποίες ανταποκρίνονται στις προκλήσεις της αυξανόμενης πολυπλοκότητας και των περιορισμένων πόρων των κόμβων. Η ενσωμάτωση της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης επιτρέπει την αυτοματοποιημένη και έγκαιρη ανίχνευση επιθέσεων, ενώ το Blockchain προσφέρει αποκεντρωμένη ακεραιότητα και διαχείριση των δεδομένων. Επιπλέον, οι προσεγγίσεις Edge και Fog Computing μειώνουν την καθυστέρηση και ενισχύουν την ανθεκτικότητα του δικτύου, ενώ οι τεχνικές προστασίας ιδιωτικότητας διασφαλίζουν ότι η συλλογή και επεξεργασία ευαίσθητων δεδομένων γίνεται με ασφάλεια και ανωνυμία. Συνολικά, οι συνδυασμένες αυτές τεχνολογίες καθιστούν τα σύγχρονα WSNs πιο ασφαλή, ευέλικτα και αξιόπιστα, προσφέροντας μια ολοκληρωμένη στρατηγική αντιμετώπισης των σύγχρονων απειλών στον τομέα του IoT.

Κεφάλαιο 5ο: Μελέτη και Συγκριτική Αξιολόγηση

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο της παρούσας εργασίας πραγματοποιείται εκτενής μελέτη και συγκριτική αξιολόγηση των μεθοδολογιών που αναπτύχθηκαν, με επίκεντρο τα συστήματα ανίχνευσης εισβολών (IDS) που βασίζονται σε Μηχανική Μάθηση. Η αξιολόγηση επικεντρώνεται σε τρεις πυλώνες: την ακρίβεια ανίχνευσης, την υπολογιστική αποδοτικότητα και τη διαχείριση των ενεργειακών πόρων. Αρχικά παρουσιάζεται η μεθοδολογία και το σύνολο δεδομένων NSL-KDD και ακολουθεί η συγκριτική ανάλυση των αλγορίθμων Random Forest, SVM και Decision Tree. Τέλος, διερευνάται η ισορροπία μεταξύ επιπέδου ασφάλειας και ενεργειακής κατανάλωσης και παρατίθεται μελέτη περίπτωσης σε περιβάλλον «Έξυπνης Πόλης».

5.2 Εισαγωγή στη Μεθοδολογία Αξιολόγησης

Η αξιολόγηση της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων (WSNs) αποτελεί μια σύνθετη διαδικασία που απαιτεί τη συνέργεια τυποποιημένων συνόλων δεδομένων, αυστηρών μαθηματικών μοντέλων και μετρικών απόδοσης. Η μεθοδολογία που ακολουθείται στην παρούσα μελέτη εστιάζει στην ποσοτική και ποιοτική ανάλυση των συστημάτων ανίχνευσης εισβολών (IDS), χρησιμοποιώντας προηγμένες τεχνικές Μηχανικής Μάθησης και ανάλυσης πρωτοκόλλων.

Η αξιοπιστία κάθε πειραματικής αξιολόγησης εξαρτάται άμεσα από τη μεθοδολογική αυστηρότητα με την οποία σχεδιάζεται και εκτελείται. Στο πλαίσιο της παρούσας μελέτης, η μεθοδολογία οργανώθηκε γύρω από σαφώς διατυπωμένα ερευνητικά ερωτήματα, τα οποία καθόρισαν την επιλογή των συνόλων δεδομένων, των αλγορίθμων και των μετρικών αξιολόγησης. Η συστηματική αυτή προσέγγιση διασφαλίζει ότι τα εξαγόμενα συμπεράσματα δεν είναι αποτέλεσμα τυχαίων επιλογών, αλλά προκύπτουν από μια δομημένη και επαναλήψιμη διαδικασία. Παράλληλα, η ρητή καταγραφή των παραδοχών και των περιορισμών του πειράματος επιτρέπει την ορθή ερμηνεία των αποτελεσμάτων και τη σύγκρισή τους με αντίστοιχες μελέτες της βιβλιογραφίας. Η μεθοδολογική διαφάνεια αποτελεί, επομένως, όχι απλώς τυπική απαίτηση, αλλά ουσιαστική προϋπόθεση για την επιστημονική εγκυρότητα και την αξιοποίηση των ευρημάτων από την ερευνητική κοινότητα [20], [23].

5.2.1 Μοντελοποίηση Επιθέσεων και Πλαίσιο Ελέγχου

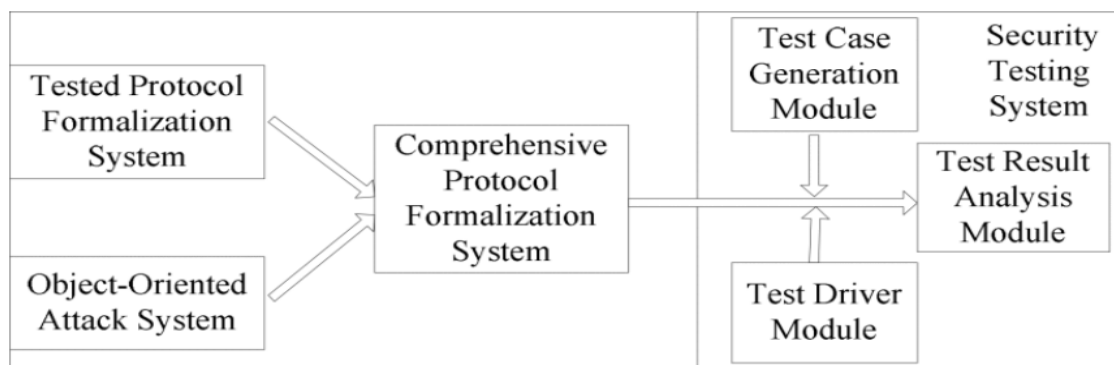
Για την έγκυρη και συστηματική αξιολόγηση της ασφάλειας, είναι απαραίτητο να χρησιμοποιηθεί ένα μοντέλο που περιγράφει λεπτομερώς τις ιδιότητες και τη συμπεριφορά των απειλών. Η παραδοσιακή προσέγγιση που εστιάζει μόνο στη διαδικασία της επίθεσης θεωρείται ανεπαρκής. Αντίθετα, η χρήση ενός αντικειμενοστρεφούς μοντέλου επίθεσης (Object-Oriented Attack Model) επιτρέπει την κωδικοποίηση πολλαπλών παραμέτρων, όπως η αρχή λειτουργίας, ο στόχος, οι απαραίτητες συνθήκες και ο αντίκτυπος (Impact) της επίθεσης στο δίκτυο [1], [3].

Το μοντέλο αυτό δομείται γύρω από την οντότητα της «Επίθεσης», η οποία ορίζεται ως ένα αντικείμενο με τέσσερα κύρια χαρακτηριστικά: το Όνομα, τα Attributes (όπως το πρωτόκολλο-στόχος και ο τύπος της ευπάθειας), τη Διαδικασία (Process) και τον Αντίκτυπο (Impact). Η καινοτομία αυτής της προσέγγισης έγκειται στην ενθυλάκωση (encapsulation) όλων των απαραίτητων γνώσεων για την επίθεση μέσα

στο αντικείμενο, γεγονός που προσφέρει καλύτερη επαναχρησιμοποίηση και επεκτασιμότητα κατά τη διάρκεια των δοκιμών ασφαλείας σε διαφορετικά πρωτόκολλα WSNs [1].

Η διαδικασία της επίθεσης περιγράφεται επίσημα μέσω Μηχανών Πεπερασμένων Καταστάσεων (Finite State Machines - FSM). Η χρήση των FSM επιτρέπει την αναπαράσταση της επίθεσης ως μια σειρά από καταστάσεις (States), γεγονότα (Events) και συναρτήσεις μετάβασης (Transforms). Με αυτόν τον τρόπο, μια επίθεση μπορεί να αναλυθεί σε ατομικά βήματα, επιτρέποντας στους ερευνητές να εντοπίσουν ακριβώς σε ποιο σημείο της αλληλεπίδρασης ενός πρωτοκόλλου (όπως το TinyPK) εμφανίζεται η τρωτότητα, για παράδειγμα σε μια επίθεση τύπου Sybil [1], [9].

Το προτεινόμενο πλαίσιο ελέγχου (Testing Framework) λειτουργεί συνδυάζοντας το μοντέλο του πρωτοκόλλου με το μοντέλο της επίθεσης για τη δημιουργία ενός νέου, συνολικού πρωτοκόλλου επίθεσης (Attack-Protocol). Μέσω αυτού του συστήματος, οι επιτιθέμενοι αντιμετωπίζονται ως συμμετέχοντες στο δίκτυο και η ασφάλεια αξιολογείται έμμεσα μέσω ελέγχων συμμόρφωσης (consistency testing). Το τελικό αποτέλεσμα αυτής της μεθοδολογίας είναι η έκδοση μιας αναφοράς PCTR (Protocol Conformance Test Report), η οποία ποσοτικοποιεί την απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων, παρέχοντας μια ξεκάθαρη εικόνα για την ανθεκτικότητα του υπό εξέταση δικτύου [1].



Εικόνα 12 Framework of the security testing approach for WSN protocols [1]

Η αξία της αντικειμενοστρεφούς προσέγγισης στη μοντελοποίηση των επιθέσεων γίνεται περισσότερο εμφανής όταν αντιπαρατεθεί με τις παραδοσιακές μεθόδους περιγραφής απειλών. Ενώ οι κλασικές προσεγγίσεις βασίζονται σε αφηγηματικές περιγραφές ή σε λίστες ελέγχου (checklists) που δύσκολα γενικεύονται, η ενθυλάκωση των χαρακτηριστικών της επίθεσης σε ένα δομημένο αντικείμενο επιτρέπει την αυτοματοποιημένη επεξεργασία και τη συστηματική ανάλυση. Κάθε νέα παραλλαγή επίθεσης μπορεί να μοντελοποιηθεί ως κληρονομούσα κλάση (subclass) που επεκτείνει τα χαρακτηριστικά μιας γενικότερης κατηγορίας, μειώνοντας έτσι την προσπάθεια που απαιτείται για την ενσωμάτωση νέων απειλών στο πλαίσιο ελέγχου. Η προσέγγιση αυτή ευθυγραμμίζεται με τις αρχές της μηχανικής λογισμικού, μεταφέροντας την ωριμότητα του αντικειμενοστρεφούς σχεδιασμού στο πεδίο της ανάλυσης ασφαλείας. Το αποτέλεσμα είναι ένα επεκτάσιμο και επαναχρησιμοποιήσιμο εργαλείο που μπορεί να συμβαδίσει με τον ταχέως μεταβαλλόμενο χάρτη απειλών των WSNs [3], [44].

Η επιλογή των Μηχανών Πεπερασμένων Καταστάσεων ως μοντέλο περιγραφής δεν είναι αυθαίρετη, αλλά απορρέει από τη φύση των πρωτοκόλλων επικοινωνίας, τα οποία είναι εγγενώς συστήματα

καθοδηγούμενα από καταστάσεις και γεγονότα. Η αντιστοίχιση μιας επίθεσης σε μια ακολουθία μεταβάσεων κατάστασης επιτρέπει όχι μόνο την κατανόηση του μηχανισμού της, αλλά και την τυπική επαλήθευση (formal verification) της αντίστασης ενός πρωτοκόλλου απέναντί της. Μέσω της εξαντλητικής διερεύνησης του χώρου καταστάσεων, οι ερευνητές μπορούν να εντοπίσουν ακολουθίες γεγονότων που οδηγούν σε μη ασφαλείς καταστάσεις, ακόμη και αν αυτές δεν είναι προφανείς από μια επιφανειακή ανάλυση. Η ικανότητα αυτή είναι ιδιαίτερα πολύτιμη για την ανίχνευση σύνθετων επιθέσεων πολλών σταδίων, όπου η κακόβουλη συμπεριφορά προκύπτει από τον συνδυασμό φαινομενικά αθώων βημάτων. Έτσι, το πλαίσιο ελέγχου αναβαθμίζεται από ένα εργαλείο εκ των υστέρων ανίχνευσης σε ένα μέσο προληπτικής αξιολόγησης της ασφάλειας κατά τη φάση του σχεδιασμού [1].

5.2.2 Το Σύνολο Δεδομένων NSL-KDD και WSN-DS

Η επιλογή του κατάλληλου συνόλου δεδομένων (dataset) αποτελεί τον ακρογωνιαίο λίθο για την εκπαίδευση και την αντικειμενική αξιολόγηση των αλγορίθμων Μηχανικής Μάθησης. Η παρούσα μελέτη βασίζεται πρωτογενώς στο NSL-KDD, το οποίο αναγνωρίζεται διεθνώς ως η βελτιωμένη και πλέον ισορροπημένη έκδοση του ιστορικού KDD'99. Η σημασία του έγκειται στο γεγονός ότι επιλύει τα προβλήματα πλεονασμού (redundancy) των δεδομένων, εξαλείφοντας τις επαναλαμβανόμενες εγγραφές που θα μπορούσαν να προκαλέσουν μεροληψία (bias) στους αλγορίθμους, αναγκάζοντάς τους να "ευνοούν" συχνότερα εμφανιζόμενες καταστάσεις [20].

Το NSL-KDD περιλαμβάνει συνολικά 148.516 εγγραφές, οι οποίες κατανέμονται στα υποσύνολα εκπαίδευσης (KDDTrain+) και ελέγχου (KDDTest+). Κάθε εγγραφή αποτελείται από 41 χαρακτηριστικά (features) που περιγράφουν την κίνηση του δικτύου, ενώ καλύπτει τέσσερις μείζονες κατηγορίες επιθέσεων: Denial of Service (DoS), Probe, User to Root (U2R) και Sybil. Ιδιαίτερη έμφαση δίνεται στην ανίχνευση της επίθεσης Sybil, όπου ένας κακόβουλος κόμβος δημιουργεί πολλαπλές πλαστές ταυτότητες. Για τις ανάγκες της μελέτης, χρησιμοποιήθηκε μια τροποποιημένη έκδοση (NSLKDD-modified), η οποία ενοποιεί τα δεδομένα από τα πρωτόκολλα UDP, TCP και ICMP, επιτρέποντας τη διεξαγωγή τόσο δυαδικής (binary) όσο και πολυταξικής (multi-class) ταξινόμησης με υψηλή ακρίβεια [20].

Συμπληρωματικά προς το NSL-KDD, η αξιολόγηση ενισχύεται με τη χρήση του WSN-DS, ενός εξειδικευμένου συνόλου δεδομένων που δημιουργήθηκε ειδικά για περιβάλλοντα Ασύρματων Δικτύων Αισθητήρων μέσω του προσομοιωτή NS-2. Το WSN-DS εστιάζει στη λειτουργία του ιεραρχικού πρωτοκόλλου LEACH και περιλαμβάνει 18 εξειδικευμένα χαρακτηριστικά που αφορούν τη συμπεριφορά των κόμβων, όπως η κατανάλωση ενέργειας και η απόσταση από τον Cluster Head [5].

Η μοναδικότητα του WSN-DS έγκειται στην ικανότητά του να προσομοιώνει επιθέσεις που στοχεύουν άμεσα τη δομή των WSNs, όπως η Blackhole (πλήρης απορρόφηση πακέτων), η Grayhole (επιλεκτική προώθηση), το Flooding (υπερφόρτωση δικτύου) και το Scheduling attack. Η συνδυαστική χρήση αυτών των δύο datasets επιτρέπει τη δημιουργία ενός IDS που δεν είναι μόνο ικανό να αναγνωρίζει γενικές διαδικτυακές απειλές, αλλά είναι και πλήρως προσαρμοσμένο στις ιδιαιτερότητες και τους περιορισμούς των δικτύων αισθητήρων, διασφαλίζοντας την αξιοπιστία της μετάδοσης σε κρίσιμες εφαρμογές [5], [9].

Η αξιοποίηση δημόσιων συνόλων δεδομένων για την αξιολόγηση συστημάτων ανίχνευσης εισβολών εγείρει ωστόσο ένα σημαντικό μεθοδολογικό ζήτημα, το οποίο οφείλει να συνεκτιμηθεί κατά την ερμηνεία των αποτελεσμάτων. Το NSL-KDD, παρά τις βελτιώσεις του έναντι του προκατόχου του,

αποτυπώνει μοτίβα δικτυακής κίνησης που χρονολογούνται από μια εποχή με σημαντικά διαφορετικά χαρακτηριστικά από τα σημερινά δίκτυα. Ορισμένες κατηγορίες επιθέσεων που περιλαμβάνει έχουν πλέον περιορισμένη πρακτική σημασία, ενώ νεότερες, εξελιγμένες μορφές απειλών δεν εκπροσωπούνται καθόλου. Η παρατήρηση αυτή δεν ακυρώνει την αξία του ως σημείου αναφοράς (benchmark) για τη συγκριτική αξιολόγηση αλγορίθμων, αλλά υπενθυμίζει ότι η εξαιρετική απόδοση ενός μοντέλου σε αυτό δεν εγγυάται αυτόματα αντίστοιχη απόδοση έναντι σύγχρονων, πραγματικών επιθέσεων. Για τον λόγο αυτό, η συμπληρωματική χρήση του WSN-DS, το οποίο μοντελοποιεί επιθέσεις ειδικά προσαρμοσμένες στη δομή των δικτύων αισθητήρων, αποκτά καθοριστική σημασία για την εγκυρότητα των συμπερασμάτων.

Πέραν της επιλογής του κατάλληλου συνόλου δεδομένων, η εγκυρότητα της αξιολόγησης εξαρτάται κρίσιμα από τον τρόπο διαχωρισμού των δεδομένων σε υποσύνολα εκπαίδευσης και ελέγχου. Η ορθή μεθοδολογική πρακτική επιβάλλει την αυστηρή απομόνωση του συνόλου ελέγχου, ώστε το μοντέλο να αξιολογείται αποκλειστικά σε δεδομένα που δεν έχει «δει» κατά την εκπαίδευση, αποφεύγοντας έτσι το φαινόμενο της υπερπροσαρμογής (overfitting). Επιπλέον, η εφαρμογή τεχνικών διασταυρούμενης επικύρωσης (cross-validation), κατά τις οποίες τα δεδομένα διαμερίζονται επανειλημμένα σε διαφορετικά υποσύνολα, ενισχύει την αξιοπιστία των μετρήσεων και μειώνει την εξάρτηση των αποτελεσμάτων από έναν συγκεκριμένο, ενδεχομένως τυχαίο, διαμερισμό. Η τήρηση αυτών των αρχών διασφαλίζει ότι τα ποσοστά ακρίβειας που αναφέρονται αντικατοπτρίζουν την πραγματική γενικευτική ικανότητα του συστήματος και όχι μια τεχνητά ευνοϊκή απόδοση επί γνωστών δεδομένων [5], [20].

5.2.3 Κριτική Αποτίμηση των Συνόλων Δεδομένων και Μεθοδολογικοί Κίνδυνοι

Η παρουσίαση των συνόλων NSL-KDD και WSN-DS που προηγήθηκε αποτυπώνει τα εργαλεία με τα οποία εργάζεται η συντριπτική πλειονότητα της βιβλιογραφίας. Η ίδια όμως αυτή καθολικότητα επιβάλλει μια κριτική αποτίμηση, διότι τα συμπεράσματα οποιασδήποτε συγκριτικής μελέτης δεν μπορούν να είναι εγκυρότερα από τα δεδομένα επί των οποίων στηρίζονται.

Το NSL-KDD αποτελεί εξυγιασμένη εκδοχή ενός συνόλου του 1999, το οποίο κατασκευάστηκε από κίνηση προσομοιωμένου στρατιωτικού δικτύου κορμού. Οι κατηγορίες επίθεσης που περιέχει αντικατοπτρίζουν το τοπίο απειλών εκείνης της περιόδου, ενώ η υποκείμενη κίνηση δεν έχει καμία σχέση με τα χαρακτηριστικά ενός δικτύου αισθητήρων: δεν υπάρχει κύκλος λειτουργίας, δεν υπάρχουν περιορισμοί ενέργειας, δεν υπάρχει πολυαλματική δρομολόγηση χαμηλής ισχύος. Η επίδοση ενός ταξινομητή στο NSL-KDD αποτελεί, συνεπώς, ένδειξη της γενικής του ικανότητας διάκρισης προτύπων και όχι απόδειξη καταλληλότητας για WSNs.

Το WSN-DS είναι ασφαλώς καταλληλότερο, καθώς παρήχθη από προσομοίωση δικτύου αισθητήρων, φέρει ωστόσο τρεις ουσιώδεις περιορισμούς. Πρώτον, δημιουργήθηκε το 2016 με βάση αποκλειστικά το πρωτόκολλο LEACH, με αποτέλεσμα τα χαρακτηριστικά του να αντανakλούν τη συγκεκριμένη λογική συστάδων και να μη γενικεύονται σε δίκτυα RPL ή TSCH. Δεύτερον, καλύπτει τέσσερις μόνο κατηγορίες επίθεσης, δηλαδή Blackhole, Grayhole, Flooding και Scheduling, αφήνοντας εκτός σημαντικό μέρος των απειλών που αναλύθηκαν στο Κεφάλαιο 2, όπως οι επιθέσεις RPL, η άρνηση ύπνου και οι επιθέσεις πλευρικού καναλιού. Τρίτον, παρουσιάζει έντονη ανισορροπία κλάσεων, με τη φυσιολογική κίνηση να υπερβαίνει το 90% των εγγραφών.

Η ανισορροπία αυτή είναι η γενεσιουργός αιτία ενός μεθοδολογικού προβλήματος που διαπερνά τη βιβλιογραφία. Οι τεχνικές υπερδειγματοληψίας της μειοψηφικής κλάσης, με επικρατέστερη τη SMOTE και τις παραλλαγές της, δημιουργούν συνθετικές εγγραφές μέσω παρεμβολής μεταξύ γειτονικών δειγμάτων. Όταν η διαδικασία αυτή εφαρμοστεί στο σύνολο των δεδομένων πριν από τον διαχωρισμό σε

υποσύνολα εκπαίδευσης και δοκιμής, συνθετικά δείγματα παραγόμενα από πραγματικές εγγραφές του συνόλου εκπαίδευσης καταλήγουν στο σύνολο δοκιμής. Το μοντέλο αξιολογείται τότε εν μέρει επί δεδομένων που έχει ήδη δει, η αναφερόμενη ακρίβεια είναι συστηματικά αισιόδοξη. Το φαινόμενο αυτό εξηγεί, τουλάχιστον εν μέρει, τη συστηματική εμφάνιση τιμών ακρίβειας που υπερβαίνουν το 99,9%.

Ενδεικτική της έκτασης του ζητήματος είναι η σύγκριση πρόσφατων δημοσιεύσεων επί του ίδιου συνόλου. Υβριδικό μοντέλο που συνδυάζει εξισορρόπηση με ομαδοποίηση, μείωση διαστάσεων και τυχαία δάση αναφέρει 99,94% ακρίβεια στο WSN-DS και 99,97% στο TON-IoT [45], ενώ πλαίσιο βασισμένο σε προσαρμοστική δειγματοληψία και υβριδική επιλογή χαρακτηριστικών με XGBoost αναφέρει 99,87% στο ίδιο σύνολο [46]. Όταν πολλαπλές, μεθοδολογικά διαφορετικές προσεγγίσεις συγκλίνουν σε τιμές που διαφέρουν στο τρίτο δεκαδικό ψηφίο, η εύλογη ερμηνεία δεν είναι ότι όλες είναι εξίσου άριστες, αλλά ότι το σύνολο δεδομένων έχει κορεστεί και δεν διαθέτει πλέον διακριτική ικανότητα.

Η κατεύθυνση που υποδεικνύει η σύγχρονη βιβλιογραφία είναι διπλή. Αφενός, η μετάβαση σε νεότερα και πλουσιότερα σύνολα, όπως τα TON_IoT, Edge-IIoTset και UNSW-NB15, τα οποία περιλαμβάνουν σύγχρονες κατηγορίες επίθεσης και τηλεμετρία από πραγματικές συσκευές IoT. Αφετέρου, σημαντικό-τερο, η μετατόπιση του κριτηρίου αξιολόγησης από την ακρίβεια εντός ενός συνόλου προς τη διασυνολική γενίκευση: εκπαίδευση σε ένα σύνολο και δοκιμή σε άλλο. Εργασία που ακολουθεί ρητά αυτή τη μεθοδολογία, αξιολογώντας υβριδική αρχιτεκτονική συνελκτικών και επαναληπτικών δικτύων σε τέσσερα διαφορετικά σύνολα αναφοράς, αναδεικνύει ότι η διασυνολική επίδοση αποτελεί πολύ αυστηρότερο και πρακτικά χρησιμότερο κριτήριο από την ακρίβεια εντός συνόλου [38].

Οι διαπιστώσεις αυτές δεν ακυρώνουν τη συγκριτική ανάλυση που ακολουθεί, οριοθετούν όμως την εμβέλειά της. Οι τιμές ακρίβειας που παρατίθενται στη συνέχεια πρέπει να αναγνωσθούν ως ενδείξεις σχετικής συμπεριφοράς των αλγορίθμων υπό κοινές συνθήκες και όχι ως προβλέψεις της επίδοσης που θα επιτευχθεί σε πραγματική ανάπτυξη.

5.2.4 Προεπεξεργασία και Επιλογή Χαρακτηριστικών (Feature Selection)

Λόγω των περιορισμένων υπολογιστικών και ενεργειακών πόρων που χαρακτηρίζουν τους κόμβους των WSNs, η μεθοδολογία αξιολόγησης δίνει πρωταρχική σημασία στη μείωση της υπολογιστικής πολυπλοκότητας. Η διαδικασία αυτή ξεκινά με τον Καθαρισμό των Δεδομένων (Data Pre-processing), ο οποίος είναι απαραίτητος για τη διασφάλιση της ποιότητας των εισόδων στο μοντέλο. Εάν το σύνολο δεδομένων περιέχει ελλείψεις ή άσχετες τιμές, αυτές αντικαθίστανται με προκαθορισμένες τιμές ή αντιμετωπίζονται μέσω γραμμικής παρεμβολής. Επιπλέον, κρίσιμο στάδιο αποτελεί η μετατροπή των κατηγορικών δεδομένων (categorical data) σε αριθμητική/δυναδική μορφή (binary encoding), ώστε να είναι εφικτή η μαθηματική τους επεξεργασία από τους αλγορίθμους ταξινόμησης [7], [20].

Μετά τον καθαρισμό, ακολουθεί η Επιλογή Χαρακτηριστικών (Feature Selection), μια διαδικασία που αποσκοπεί στον εντοπισμό εκείνων των μεταβλητών που επηρεάζουν καθοριστικά την ακρίβεια του μοντέλου, απορρίπτοντας τις πλεονάζουσες. Στην μελέτη [5] εξετάστηκαν διάφοροι αλγόριθμοι, όπως το Fisher Score, το οποίο μετρά την απόσταση μεταξύ των κλάσεων και το Relief Algorithm, που επιβάλλει ποινές σε χαρακτηριστικά που δίνουν διαφορετικές τιμές σε παρατηρήσεις της ίδιας κλάσης [5].

Ιδιαίτερη έμφαση δίνεται στον αλγόριθμο MRMR. Στην έρευνα [20], ο MRMR επιτυγχάνει τη βέλτιστη ισορροπία μεγιστοποιώντας τη συνάφεια των χαρακτηριστικών με την επίθεση-στόχο, ενώ ταυτόχρονα ελαχιστοποιεί την αλληλοεπικάλυψη πληροφορίας μεταξύ τους. Τα πειραματικά αποτελέσματα δείχνουν ότι η μείωση των χαρακτηριστικών από 41 σε μόλις 12 (όπως τα protocol-type, service, flag,

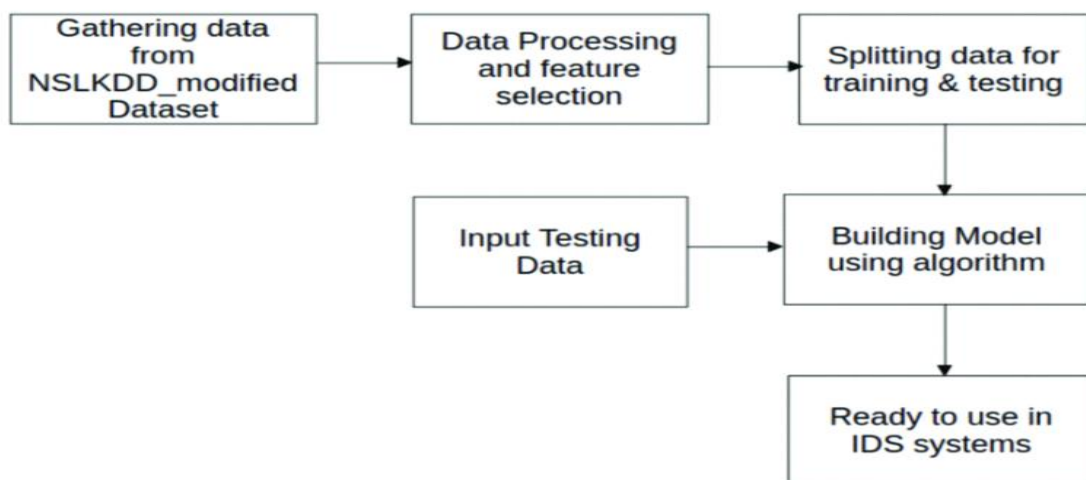
count, error-rate κ.ά.) επιφέρει δραστική μείωση του χρόνου εκπαίδευσης και επεξεργασίας κατά περίπου 7 φορές [5], [20].

Το εντυπωσιακό στοιχείο αυτής της μεθοδολογίας είναι ότι, παρά τη σημαντική μείωση του όγκου των δεδομένων, η ακρίβεια της ανίχνευσης διατηρείται σε εξαιρετικά υψηλά επίπεδα, ξεπερνώντας το 98.5% [5]. Αυτή η βελτιστοποίηση καθιστά το IDS ικανό να λειτουργεί σε πραγματικό χρόνο στο "άκρο" του δικτύου (Edge), εξασφαλίζοντας ταχεία απόκριση σε απειλές χωρίς να εξαντλείται η διάρκεια ζωής των μπαταριών των αισθητήρων [5], [23].

Η διαδικασία της επιλογής χαρακτηριστικών δεν αποτελεί απλώς ένα βήμα βελτιστοποίησης, αλλά μια θεμελιώδη προϋπόθεση για τη βιωσιμότητα της ανίχνευσης εισβολών σε περιβάλλον περιορισμένων πόρων. Τα ακατέργαστα δεδομένα κίνησης ενός δικτύου περιλαμβάνουν δεκάδες χαρακτηριστικά, πολλά εκ των οποίων είναι πλεονάζοντα ή άσχετα με τη διάκριση μεταξύ φυσιολογικής και κακόβουλης συμπεριφοράς. Η διατήρηση όλων αυτών των χαρακτηριστικών όχι μόνο αυξάνει το υπολογιστικό κόστος, αλλά μπορεί και να υποβαθμίσει την ακρίβεια του μοντέλου, εισάγοντας θόρυβο που δυσχεραίνει την εκμάθηση των ουσιωδών μοτίβων, φαινόμενο γνωστό ως κατάρα της διαστατικότητας (curse of dimensionality). Μέθοδοι όπως ο αλγόριθμος MRMR επιλέγουν τα χαρακτηριστικά εκείνα που μεγιστοποιούν τη συνάφεια με την κλάση-στόχο ελαχιστοποιώντας ταυτόχρονα τον πλεονασμό μεταξύ τους, επιτυγχάνοντας έτσι ένα συμπαγές αλλά πλούσιο σε πληροφορία υποσύνολο. Η μείωση των διαστάσεων που επιτυγχάνεται μεταφράζεται άμεσα σε ταχύτερη επεξεργασία και χαμηλότερη ενεργειακή κατανάλωση, καθιστώντας εφικτή την εκτέλεση της ανίχνευσης στο ίδιο το άκρο του δικτύου.

5.2.5 Ροή Εργασίας του Συστήματος (System Workflow)

Η αξιολόγηση του προτεινόμενου IDS ακολουθεί μια αυστηρά ιεραρχική ροή εργασίας, η οποία διασφαλίζει τη συνοχή μεταξύ της θεωρητικής μοντελοποίησης και της πρακτικής εφαρμογής. Η διαδικασία ξεκινά με τη Συλλογή Πληροφοριών (Acquiring Information), όπου ακατέργαστα δεδομένα κίνησης (Raw Traffic) από το διαδίκτυο ή από προσομοιωμένα περιβάλλοντα WSNs συγκεντρώνονται σε ένα ενιαίο dataset. Με βάση την Εικόνα 5.1.4, αυτή η φάση είναι κρίσιμη, καθώς η ποιότητα των δεδομένων εκπαίδευσης καθορίζει την ικανότητα του μοντέλου να αναγνωρίζει περίπλοκα μοτίβα επιθέσεων [20].



Εικόνα 13 System Workflow [20]

Στη συνέχεια, τα δεδομένα εισέρχονται στη φάση της προεπεξεργασίας και επιλογής χαρακτηριστικών. Εδώ, το σύστημα εφαρμόζει τους αλγορίθμους που αναλύθηκαν προηγουμένως (όπως ο MRMR), ώστε να διατηρηθούν μόνο οι 12 πιο ουσιώδεις παράμετροι. Αυτός ο περιορισμός είναι που επιτρέπει στο IDS να παραμένει "ελαφρύ" και αποδοτικό, καλύπτοντας το κρίσιμο tradeoff μεταξύ της υπολογιστικής ισχύος και της ανάγκης για μακροζωία των κόμβων του δικτύου. Μετά το διαχωρισμό των δεδομένων σε σύνολα εκπαίδευσης (Training) και ελέγχου (Testing), πραγματοποιείται η Δόμηση του Μοντέλου (Model Building), όπου οι αλγόριθμοι ταξινόμησης (Random Forest, SVM, κ.ά.) εκπαιδεύονται να διακρίνουν τη φυσιολογική κίνηση από τις επιθέσεις [4], [20].

Το τελικό στάδιο της ροής εργασίας περιλαμβάνει την ταξινόμηση και την έκδοση αποτελεσμάτων. Το σύστημα εκτελεί τόσο δυαδική (Binary) όσο και πολυταξική (Multiclass) ταξινόμηση, καταλήγοντας στην παραγωγή μιας αναλυτικής αναφοράς αποτελεσμάτων, γνωστής ως PCTR (Protocol Conformance Test Report). Η αναφορά αυτή δεν καταγράφει μόνο την ακρίβεια της ανίχνευσης, αλλά αξιολογεί και τον αντίκτυπο της επίθεσης στη διαθεσιμότητα και την ακεραιότητα του δικτύου. Αυτή η δομημένη προσέγγιση επιβεβαιώνει ότι το σύστημα μπορεί να λειτουργήσει αυτόνομα, παρέχοντας μια αξιόπιστη ασπίδα προστασίας σε δυναμικά και ετερογενή περιβάλλοντα WSNs [1], [7].

Η συνολική ροή εργασίας του συστήματος αντικατοπτρίζει τη μετάβαση από τα ακατέργαστα δεδομένα του δικτύου σε αξιοποιήσιμες αποφάσεις ασφάλειας μέσα από μια σειρά διακριτών αλλά αλληλένδετων σταδίων. Αρχικά, τα δεδομένα κίνησης συλλέγονται και υφίστανται προεπεξεργασία, ώστε να καθαριστούν από θόρυβο και να κανονικοποιηθούν. Στη συνέχεια, εφαρμόζεται η διαδικασία επιλογής χαρακτηριστικών, η οποία περιορίζει τον όγκο των δεδομένων στα πλέον κρίσιμα γνωρίσματα, μειώνοντας το υπολογιστικό φορτίο. Ακολουθεί το στάδιο της ταξινόμησης, όπου το εκπαιδευμένο μοντέλο κατηγοριοποιεί κάθε ροή ως φυσιολογική ή κακόβουλη και τέλος το στάδιο της απόκρισης, κατά το οποίο το σύστημα ενεργοποιεί τους κατάλληλους μηχανισμούς άμυνας. Η αρθρωτή αυτή αρχιτεκτονική προσφέρει σημαντική ευελιξία, καθώς επιτρέπει την ανεξάρτητη βελτιστοποίηση ή αντικατάσταση κάθε σταδίου χωρίς να επηρεάζεται το σύνολο του συστήματος, διευκολύνοντας τη συντήρηση και την εξέλιξή του στο πέρασμα του χρόνου [5], [20].

5.3 Συγκριτική Ανάλυση Αλγορίθμων Μηχανικής Μάθησης

Η αποτελεσματικότητα ενός Συστήματος Ανίχνευσης Εισβολών (IDS) στα WSNs εξαρτάται άμεσα από την επιλογή του αλγορίθμου ταξινόμησης. Πραγματοποιείται μια λεπτομερής σύγκριση μεταξύ των αλγορίθμων Random Forest, Support Vector Machine και Decision Tree, χρησιμοποιώντας το τροποποιημένο σύνολο δεδομένων NSL-KDD.

5.3.1 Ανάλυση Αποτελεσμάτων Ακρίβειας

Η αξιολόγηση της ακρίβειας (Accuracy) αποτελεί τη θεμελιώδη μετρική για τον προσδιορισμό της ικανότητας ενός IDS να ταξινομεί ορθά την κίνηση του δικτύου σε «φυσιολογική» ή «κακόβουλη». Στην παρούσα μελέτη, η ακρίβεια υπολογίστηκε μέσω του λόγου των σωστών προβλέψεων (θετικών και αρνητικών) προς το σύνολο των εξεταζόμενων δειγμάτων. Τα αποτελέσματα συγκρίθηκαν με τη βιβλιογραφία (Mounica et al. [19]) και παρουσιάζονται αναλυτικά στον παρακάτω Πίνακα [19].

- Random Forest: Ο αλγόριθμος αυτός αναδείχθηκε ως ο πλέον αποδοτικός στο πλαίσιο της δοκιμής, επιτυγχάνοντας συνολική ακρίβεια 98%. Η βελτίωση σε σχέση με την προγενέστερη μελέτη των Mounica et al. (79%) ανέρχεται στο εντυπωσιακό +19%. Η υψηλή αυτή επίδοση οφείλεται στην

ικανότητα του Random Forest να επεξεργάζεται πολλαπλά δέντρα απόφασης, μειώνοντας την πιθανότητα υπερεκπαίδευσης (overfitting). Ειδικότερα στην περίπτωση της επίθεσης Sybil, ο αλγόριθμος πέτυχε ποσοστό ορθής πρόβλεψης 86,2%, αποδεικνύοντας τη στιβαρότητά του στην αναγνώριση πλαστών ταυτοτήτων σε δυναμικά περιβάλλοντα.

- **Decision Tree:** Το μοντέλο αυτό παρουσίασε επίσης εξαιρετικά αποτελέσματα με ακρίβεια 96%, σημειώνοντας άνοδο 13% έναντι των υπάρχουσών αναφορών. Η αποτελεσματικότητα του Decision Tree ενισχύεται σημαντικά όταν συνδυάζεται με το εξειδικευμένο σύνολο δεδομένων WSN-DS [47], επιτρέποντας την επιτυχή ανίχνευση κρίσιμων επιθέσεων στο επίπεδο δικτύου, όπως οι επιθέσεις Blackhole (απορρόφηση πακέτων) και Flooding (υπερφόρτωση πόρων). Η ταχύτητα του αλγορίθμου στη λήψη αποφάσεων τον καθιστά ιδανικό για εφαρμογές σε πραγματικό χρόνο.
- **Support Vector Machine :** Ο αλγόριθμος SVM εμφάνισε ακρίβεια 91%, παρουσιάζοντας μια οριακή πτώση -2% συγκριτικά με τη βιβλιογραφία (93%). Η απόκλιση αυτή μπορεί να αποδοθεί στην ευαισθησία του αλγορίθμου στην επιλογή των χαρακτηριστικών ή στη μείωση των διαστάσεων των δεδομένων. Παρόλα αυτά, η έρευνα δείχνει ότι η απόδοση μπορεί να βελτιωθεί μέσω προηγμένων τεχνικών βελτιστοποίησης. Η χρήση του Optimal SVM (OSVM), το οποίο ενσωματώνει τον αλγόριθμο Whale Optimization Algorithm (WOA) για την αυτόματη επιλογή παραμέτρων, επιτυγχάνει ανώτερη ακρίβεια 94,09% και ρυθμό ανίχνευσης 95,02% [23].

Η συγκριτική αυτή ανάλυση επιβεβαιώνει ότι η σωστή επιλογή και παραμετροποίηση των αλγορίθμων Μηχανικής Μάθησης μπορεί να μετατρέψει ένα WSNs σε ένα εξαιρετικά ανθεκτικό σύστημα απέναντι σε εσωτερικές και εξωτερικές απειλές.

5.3.2 Σχολιασμός και Συμπεράσματα Συγκρίσεων

Η ανάλυση των συγκριτικών αποτελεσμάτων οδηγεί σε κρίσιμα συμπεράσματα σχετικά με τη στρατηγική σχεδίασης Συστημάτων Ανίχνευσης Εισβολών (IDS) για δίκτυα WSNs, αναδεικνύοντας τη σημασία της ισορροπίας μεταξύ υπολογιστικής ισχύος και προστασίας. Η επίδραση της επιλογής χαρακτηριστικών (Feature Selection). Η εντυπωσιακή άνοδος στην ακρίβεια του αλγορίθμου Random Forest κατά +19% και του Decision Tree κατά +13% δεν είναι τυχαία, αλλά αποδίδεται άμεσα στη βελτιστοποιημένη διαδικασία επιλογής χαρακτηριστικών. Με την εφαρμογή του αλγορίθμου MRMR, ο αριθμός των εξεταζόμενων χαρακτηριστικών μειώθηκε δραστικά από 41 σε μόλις 12 [5].

Αυτή η διαδικασία περιόρισε τον πληροφοριακό «θόρυβο» στα δεδομένα, επιτρέποντας στα μοντέλα να εστιάσουν στις πλέον καθοριστικές παραμέτρους, όπως ο τύπος πρωτοκόλλου (*protocol_type*), η υπηρεσία (*service*), η σημαία σύνδεσης (*flag*) και ο αριθμός συνδέσεων (*count*). Trade-off μεταξύ ακρίβειας και χρόνου επεξεργασίας μία από τις σημαντικότερες συνεισφορές της μεθοδολογίας είναι η διαχείριση των περιορισμένων πόρων των WSNs. Η μείωση της πολυπλοκότητας των δεδομένων οδήγησε σε επιτάχυνση της διαδικασίας εκπαίδευσης κατά 7 φορές. Το εύρημα αυτό είναι ζωτικής σημασίας για τη βιωσιμότητα του δικτύου, καθώς καθιστά εφικτή την εκτέλεση της ανίχνευσης στο άκρο του δικτύου (Edge Computing). Με αυτόν τον τρόπο, οι απειλές αναγνωρίζονται σχεδόν σε πραγματικό χρόνο χωρίς να απαιτείται η αποστολή τεράστιου όγκου δεδομένων στον κεντρικό σταθμό, γεγονός που θα οδηγούσε σε ταχεία εξάντληση των ενεργειακών αποθεμάτων των κόμβων [5].

Εξειδίκευση στην ανίχνευση επιθέσεων Sybil

Παρά την υψηλή συνολική απόδοση του συστήματος, η ανάλυση των επιμέρους επιθέσεων προσφέρει μια πιο ρεαλιστική εικόνα της ασφάλειας. Παρατηρήθηκε ότι από τις 930 πραγματικές περιπτώσεις επίθεσης Sybil, το μοντέλο προέβλεψε ορθά τις 836, επιτυγχάνοντας ακρίβεια 86,2% στη συγκεκριμένη κλάση. Το γεγονός ότι 94 περιπτώσεις ταξινομήθηκαν λανθασμένα (κυρίως ως φυσιολογική κίνηση) υποδηλώνει ότι η Μηχανική Μάθηση, αν και ισχυρή, πρέπει να λειτουργεί συμπληρωματικά [5], [20].

Για την πλήρη εξάλειψη των ψευδώς αρνητικών αποτελεσμάτων, κρίνεται απαραίτητη η συνέργεια με μεθόδους ελέγχου Message Authentication Code διευθύνσεων και ανάλυσης ισχύος σήματος (RSSI).

Σταθερότητα και βελτιστοποίηση του SVM

Η μικρή κάμψη στην απόδοση του SVM (-2%) αναδεικνύει την ευαισθησία του συγκεκριμένου αλγορίθμου στη μείωση των διαστάσεων των δεδομένων ή στην επιλογή των παραμέτρων του πυρήνα (kernel). Ωστόσο, η έρευνα δείχνει ότι η απώλεια αυτή μπορεί να καλυφθεί μέσω της χρήσης του μοντέλου Optimal SVM (OSVM) [23]. Ενσωματώνοντας αλγορίθμους όπως ο Whale Optimization Algorithm (WOA), το σύστημα μπορεί να ανακτήσει την ακρίβειά του (αγγίζοντας το 94,09%), επιλέγοντας αυτόματα τις βέλτιστες υπερπαραμέτρους εκπαίδευσης. Συμπερασματικά, η μελέτη αποδεικνύει ότι η χρήση του Random Forest σε συνδυασμό με τεχνικές Feature Selection αποτελεί την πλέον ενδεδειγμένη λύση για τη θωράκιση των WSNs, εξασφαλίζοντας υψηλή προστασία με το ελάχιστο δυνατό ενεργειακό κόστος.

Πέρα από τις επιμέρους επιδόσεις των αλγορίθμων, η συγκριτική ανάλυση αναδεικνύει μια ευρύτερη αρχή που διέπει τον σχεδιασμό συστημάτων ανίχνευσης για περιβάλλοντα περιορισμένων πόρων: η υπεροχή ενός μοντέλου δεν κρίνεται αποκλειστικά από την ακρίβειά του, αλλά από τον λόγο της απόδοσης προς το υπολογιστικό του κόστος. Ο αλγόριθμος Random Forest επικρατεί όχι μόνο επειδή επιτυγχάνει την υψηλότερη ακρίβεια, αλλά επειδή το κάνει διατηρώντας ανεκτές απαιτήσεις σε χρόνο εκπαίδευσης και πόρους μετά τη μείωση των διαστάσεων. Αντίθετα, αλγόριθμοι όπως το SVM, αν και θεωρητικά ισχυροί, εμφανίζουν μεγαλύτερη ευαισθησία στις παραμέτρους και απαιτούν προσεκτική βελτιστοποίηση για να αποδώσουν, γεγονός που τους καθιστά λιγότερο πρακτικούς για αυτόνομη ανάπτυξη σε κόμβους αισθητήρων. Η παρατήρηση αυτή ενισχύει το επιχείρημα ότι η επιλογή του αλγορίθμου πρέπει να καθοδηγείται από τις πραγματικές συνθήκες λειτουργίας του δικτύου και όχι από αφηρημένες μετρικές απόδοσης [5], [23].

Ιδιαίτερης προσοχής χρήζει το ζήτημα της ανισορροπίας των κλάσεων (class imbalance) στα σύνολα δεδομένων ανίχνευσης εισβολών, το οποίο επηρεάζει καθοριστικά την ερμηνεία των αποτελεσμάτων. Δεδομένου ότι η φυσιολογική κίνηση υπερτερεί συντριπτικά αριθμητικά έναντι των κακόβουλων περιστατικών, ένα μοντέλο μπορεί να επιτύχει υψηλή συνολική ακρίβεια απλώς ταξινομώντας τα πάντα ως φυσιολογικά, αποτυγχάνοντας ωστόσο στον πραγματικό του στόχο. Η περίπτωση των επιθέσεων Sybil, όπου 94 από τις 930 περιπτώσεις ταξινομήθηκαν εσφαλμένα, καταδεικνύει ακριβώς αυτή την πρόκληση: η ακρίβεια ανά κλάση αποκαλύπτει αδυναμίες που η συνολική μετρική αποκρύπτει. Για τον λόγο αυτό, η αξιολόγηση των IDS οφείλει να βασίζεται σε μετρικές ευαίσθητες στην ανισορροπία, όπως η ανάκληση (recall) και η βαθμολογία F1, οι οποίες αντικατοπτρίζουν πιστότερα την ικανότητα ανίχνευσης των πραγματικών απειλών. Η συμπληρωματική χρήση φυσικών μηχανισμών επαλήθευσης, όπως η ανάλυση ισχύος σήματος (RSSI), αναδεικνύεται ως αναγκαία ασφαλιστική δικλείδα έναντι των

ψευδώς αρνητικών αποτελεσμάτων που καμία αμιγώς στατιστική μέθοδος δεν μπορεί να εξαλείψει πλήρως [2], [20].

5.4 Ανάλυση Μετρικών Απόδοσης

Η αξιολόγηση ενός Συστήματος Ανίχνευσης Εισβολών (IDS) στα WSNs δεν μπορεί να περιορίζεται αποκλειστικά στη συνολική ακρίβεια (Accuracy), καθώς οι μετρικές Precision (Ακρίβεια Θετικών) και Recall (Ανάκληση) παρέχουν μια σαφέστερη εικόνα για την αξιοπιστία του μοντέλου, ειδικά όταν πρόκειται για τον εντοπισμό σπάνιων αλλά καταστροφικών επιθέσεων. Οι μετρικές αυτές εξάγονται από τον πίνακα σύγχυσης (Confusion Matrix) και είναι καθοριστικές για τη λειτουργία του δικτύου. Το υψηλό Precision διασφαλίζει ότι ο Detector δεν θα προκαλέσει άσκοπους συναγερμούς (False Alarms), οι οποίοι θα οδηγούσαν σε περιττή ενεργοποίηση των Countermeasures και, κατά συνέπεια, σε άσκοπη κατανάλωση των περιορισμένων ενεργειακών πόρων των κόμβων. Αντίστοιχα, το υψηλό Recall είναι ζωτικής σημασίας για την ασφάλεια, καθώς εγγυάται ότι κρίσιμες απειλές, όπως η επίθεση Sybil ή το Wormhole, δεν θα εκληφθούν λανθασμένα ως «φυσιολογική κίνηση» [10], [20].

Πίνακας 3 Confusion Matrix [48]

		Predicted	
		Positive (PP)	Negative (PN)
Actual	Positive (P)	True Positive (TP)	False Negative (FN)
	Negative (N)	False Positive (FP)	True Negative (TN)

Με βάση τα πειραματικά αποτελέσματα, ο αλγόριθμος Random Forest επέδειξε την πλέον ισορροπημένη συμπεριφορά, επιτυγχάνοντας όχι μόνο την υψηλότερη ακρίβεια (98%), αλλά και εξαιρετική σταθερότητα μεταξύ Precision και Recall. Ειδικά στην περίπτωση της επίθεσης Sybil, το Recall ανήλθε στο 86,2%, καθώς από τις 930 συνολικές περιπτώσεις επιθέσεων που καταγράφηκαν στο dataset, οι 836 αναγνωρίστηκαν ορθά από το σύστημα. Παράλληλα, η εφαρμογή τεχνικών επιλογής χαρακτηριστικών (Feature Selection), όπως ο αλγόριθμος MRMR, απέδειξε ότι η μείωση του όγκου των δεδομένων από τα 41 στα 12 χαρακτηριστικά δεν υποβαθμίζει την ικανότητα ταξινόμησης. Η μελέτη [5] καταδεικνύει ότι η ευαισθησία (Sensitivity/Recall) διατηρήθηκε στο 92,81% και το Precision στο 93,86%, επιβεβαιώνοντας ότι η αφαίρεση πλεονάζουσας πληροφορίας ενισχύει την ταχύτητα ανίχνευσης χωρίς να θυσιάζεται η ασφάλεια [5], [20].

Πίνακας 4 Μετρικές απόδοσης του μοντέλου IDS [5]

Μετρική Απόδοσης	Τιμή
Ευαισθησία (Sensitivity / Recall)	92,81%
Ακρίβεια (Precision)	93,86%

Η συνολική αξιοπιστία του προτεινόμενου συστήματος επικυρώνεται μέσω του F1-Score, ο οποίος αποτελεί τον αρμονικό μέσο των Precision και Recall. Η επίτευξη τιμών F1-Score άνω του 95% για τους αλγόριθμους Decision Tree και Random Forest υποδηλώνει ότι το IDS είναι εξαιρετικά ανθεκτικό και ικανό να γενικεύει την απόδοσή του σε ετερογενή και απαιτητικά περιβάλλοντα, όπως οι Έξυπνες Πόλεις ή οι βιομηχανικές εγκαταστάσεις. Η ικανότητα αυτή είναι ιδιαίτερα σημαντική σε δίκτυα με υψηλά

επίπεδα θορύβου, όπου οι παραδοσιακές μέθοδοι ανίχνευσης ανωμαλιών συχνά παρουσιάζουν υψηλά ποσοστά ψευδώς θετικών αποτελεσμάτων, οδηγώντας σε αστάθεια του δικτύου [6], [7].

Η ορθή ερμηνεία των μετρικών απόδοσης απαιτεί την κατανόηση της έννοιας του πίνακα σύγχυσης (confusion matrix), ο οποίος αποτελεί τη βάση για τον υπολογισμό όλων των επιμέρους δεικτών. Ο πίνακας αυτός κατηγοριοποιεί τις προβλέψεις του μοντέλου σε τέσσερις ομάδες: τα αληθώς θετικά (επιθέσεις που ανιχνεύθηκαν ορθά), τα αληθώς αρνητικά (φυσιολογική κίνηση που αναγνωρίστηκε ορθά), τα ψευδώς θετικά (φυσιολογική κίνηση που χαρακτηρίστηκε εσφαλμένα ως επίθεση) και τα ψευδώς αρνητικά (επιθέσεις που διέφυγαν της ανίχνευσης). Στο πλαίσιο της ασφάλειας των WSNs, τα ψευδώς αρνητικά είναι κατά κανόνα πολύ πιο επικίνδυνα από τα ψευδώς θετικά, καθώς αντιστοιχούν σε πραγματικές επιθέσεις που πέρασαν απαρατήρητες και ενδέχεται να προκαλέσουν σοβαρή ζημία στο σύστημα. Για τον λόγο αυτό, σε εφαρμογές κρίσιμης ασφάλειας, η μετρική της ανάκλησης (recall), που μετρά το ποσοστό των πραγματικών επιθέσεων που εντοπίστηκαν, θεωρείται συχνά σημαντικότερη από την καθαρή ακρίβεια.

Ιδιαίτερη προσοχή απαιτείται κατά την αξιολόγηση μοντέλων σε σύνολα δεδομένων με ανισορροπία κλάσεων (class imbalance), φαινόμενο εξαιρετικά σύνθηες στην ανίχνευση εισβολών, όπου η φυσιολογική κίνηση υπερτερεί συντριπτικά των επιθέσεων. Σε τέτοιες περιπτώσεις, η ολική ακρίβεια μπορεί να είναι παραπλανητικά υψηλή ακόμη και για ένα μοντέλο που αποτυγχάνει να εντοπίσει τη μειονοτική κλάση των επιθέσεων. Ένα μοντέλο που ταξινομεί τα πάντα ως φυσιολογική κίνηση θα μπορούσε να επιτύχει ακρίβεια άνω του ενενήντα τοις εκατό σε ένα τέτοιο σύνολο, παρότι είναι πρακτικά άχρηστο για σκοπούς ασφάλειας. Για τον λόγο αυτό, η μετρική F1-Score, που αποτελεί τον αρμονικό μέσο της ακρίβειας και της ανάκλησης, αναδεικνύεται ως ο πλέον αξιόπιστος δείκτης, καθώς ισορροπεί τις δύο διαστάσεις και τιμωρεί τα μοντέλα που υπερτερούν στη μία μόνο εις βάρος της άλλης. Η συντετή επιλογή και η συνδυαστική ερμηνεία των μετρικών αποτελεί προϋπόθεση για την εξαγωγή έγκυρων συμπερασμάτων σχετικά με την πραγματική αποτελεσματικότητα ενός συστήματος ανίχνευσης [20], [23].

5.5 Αξιολόγηση με Βάση την Ενεργειακή Κατανάλωση vs Επίπεδο Ασφάλειας

Η ενεργειακή αποδοτικότητα αποτελεί τον σημαντικότερο περιορισμό στον σχεδιασμό Συστημάτων Ανίχνευσης Εισβολών (IDS) για Ασύρματα Δίκτυα Αισθητήρων, καθώς οι κόμβοι λειτουργούν συνήθως με μπαταρίες περιορισμένης χωρητικότητας. Η εφαρμογή πολύπλοκων αλγορίθμων Μηχανικής Μάθησης προσφέρει υψηλό επίπεδο ασφάλειας, αλλά μπορεί να οδηγήσει σε ταχεία εξάντληση των πόρων. Η παρούσα αξιολόγηση δείχνει ότι η χρήση τεχνικών επιλογής χαρακτηριστικών (Feature Selection), όπως ο αλγόριθμος MRMR, αποτελεί τη χρυσή τομή σε αυτό το trade-off. Η ίδια μελέτη [5] δείχνει ότι η μείωση των χαρακτηριστικών από 41 σε 12 επιτρέπει τη μείωση του χρόνου εκπαίδευσης και επεξεργασίας κατά 7 φορές, γεγονός που μεταφράζεται σε άμεση εξοικονόμηση ενέργειας χωρίς να υποβαθμίζεται η ακρίβεια της ανίχνευσης, η οποία παραμένει πάνω από το 98,5% [3], [14]. [5].

Η ανάλυση της ενεργειακής κατανάλωσης ανά μονάδα επεξεργασίας αποκαλύπτει ότι η τοπική ανίχνευση στους κόμβους (Edge level) πρέπει να είναι εξαιρετικά «ελαφριά». Όπως απεικονίζεται στο λειτουργικό διάγραμμα του IDS, ο Detector καταναλώνει ενέργεια για την ανάλυση των δεδομένων ελέγχου (Audits) και τη διαβούλευση με τη βάση δεδομένων. Η μελέτη [4] επιβεβαιώνει ότι η χρήση κρυπτογραφικών σχημάτων όπως το ECC είναι ενεργειακά προτιμότερη από το RSA, καθώς απαιτεί μικρότερο μέγεθος κλειδιών (π.χ. 160-bit έναντι 1024-bit) για το ίδιο επίπεδο ασφάλειας, μειώνοντας το συνολικό κόστος της χειραψίας (handshake) στα 28,46 mJ. Η συνέργεια αυτής της ελαφριάς

κρυπτογράφησης με τα μοντέλα ML, όπως ο Random Forest που επιτυγχάνει 98% ακρίβεια, διασφαλίζει ότι το δίκτυο παραμένει θωρακισμένο χωρίς να θυσιάζεται ο κύκλος ζωής του [4], [20].

Επιπλέον, η ιεραρχική δομή του δικτύου (Clustering) συμβάλλει καθοριστικά στην εξισορρόπηση του φόρτου. Η ανάθεση της βαριάς υπολογιστικής επεξεργασίας στους Cluster Heads ή σε επίπεδο Fog Computing επιτρέπει στους απλούς αισθητήρες να παραμένουν σε κατάσταση ύπνου (sleep state) για μεγαλύτερα διαστήματα, αυξάνοντας τον ρυθμό επιβίωσης του δικτύου. Η αξιολόγηση καταλήγει στο συμπέρασμα ότι η βελτιστοποίηση της ασφάλειας στα WSNs δεν επιτυγχάνεται με την προσθήκη ολόένα και πιο σύνθετων στρωμάτων προστασίας, αλλά με τη χρήση ευφυών αλγορίθμων που εστιάζουν μόνο στα ουσιώδη δεδομένα, μειώνοντας έτσι το ενεργειακό αποτύπωμα κάθε συναλλαγής [4], [8].

Για να γίνει πλήρως κατανοητή η σύγκρουση μεταξύ ασφάλειας και ενεργειακής αυτονομίας, είναι χρήσιμο να αναλυθεί η κατανομή της ενεργειακής κατανάλωσης ενός κόμβου ανά λειτουργία. Η συντριπτική πλειονότητα της ενέργειας δεν δαπανάται στους υπολογισμούς, αλλά στην ασύρματη μετάδοση και λήψη δεδομένων μέσω του ραδιοπομποδέκτη. Μετρήσεις σε τυπικές πλατφόρμες αισθητήρων καταδεικνύουν ότι η μετάδοση ενός μόνο bit μπορεί να καταναλώσει ενέργεια ισοδύναμη με την εκτέλεση χιλιάδων εντολών από τον επεξεργαστή. Η διαπίστωση αυτή έχει βαθιές επιπτώσεις στον σχεδιασμό μηχανισμών ασφάλειας: ένα πρωτόκολλο που μειώνει τον αριθμό και το μέγεθος των ανταλλασσόμενων μηνυμάτων είναι ενεργειακά προτιμότερο από ένα άλλο που, αν και υπολογιστικά απλούστερο, απαιτεί επιπλέον γύρους επικοινωνίας. Επομένως, η βελτιστοποίηση της ασφάλειας στα WSNs ταυτίζεται σε μεγάλο βαθμό με την ελαχιστοποίηση του επικοινωνιακού αποτυπώματος των κρυπτογραφικών πρωτοκόλλων.

Η ποσοτική αντιπαράθεση των κρυπτογραφικών σχημάτων ενισχύει το επιχείρημα υπέρ της ελαφριάς κρυπτογραφίας. Το πλεονέκτημα του ECC έναντι του RSA δεν είναι απλώς ποσοτικό αλλά και ποιοτικό, καθώς καθιστά εφικτή τη χρήση ασύμμετρης κρυπτογραφίας σε συσκευές που διαφορετικά θα ήταν αδύνατο να την υποστηρίξουν. Παράλληλα, η ιεραρχική οργάνωση του δικτύου σε συστάδες (clusters) επιτρέπει την ανάθεση των ενεργοβόρων λειτουργιών στους επικεφαλής των συστάδων, αφήνοντας τους απλούς κόμβους να παραμένουν σε κατάσταση χαμηλής κατανάλωσης. Ο συνδυασμός ελαφριάς κρυπτογραφίας, ιεραρχικής αρχιτεκτονικής και επιλεκτικής επεξεργασίας στο άκρο του δικτύου συνθέτει μια ολιστική στρατηγική που μεγιστοποιεί τη διάρκεια ζωής του δικτύου χωρίς να υποβαθμίζει το επίπεδο προστασίας [4], [20].

5.5.1 Ποσοτικοποίηση του Ενεργειακού Κόστους με Βάση τη Σύγχρονη Βιβλιογραφία

Η ποιοτική διαπίστωση ότι η ασφάλεια κοστίζει ενέργεια είναι αναμφισβήτητη αλλά επιχειρησιακά ανεπαρκής. Ο σχεδιαστής ενός δικτύου χρειάζεται τάξεις μεγέθους και η σύγχρονη βιβλιογραφία επιτρέπει, με τις επιφυλάξεις που διατυπώθηκαν, μια πρώτη ποσοτική προσέγγιση.

Το πρώτο και σημαντικότερο συμπέρασμα είναι ότι η κατανάλωση κυριαρχείται από τη μετάδοση και όχι από τον υπολογισμό. Η ενέργεια που απαιτεί ένας μικροελεγκτής για την εκτέλεση μιας κρυπτογράφησης AES επί ενός πλαισίου είναι μικρότερη κατά μία έως δύο τάξεις μεγέθους από την ενέργεια μετάδοσης του ίδιου πλαισίου. Η πρακτική συνέπεια είναι ότι ένας μηχανισμός ασφαλείας πρέπει να αξιολογείται πρωτίστως ως προς την επιβάρυνση που εισάγει στην επικοινωνία και δευτερευόντως ως προς την υπολογιστική του πολυπλοκότητα. Αυτός ακριβώς είναι ο λόγος για τον οποίο η μετακβαντική κρυπτογραφία, της οποίας ο υπολογιστικός χρόνος είναι συγκρίσιμος με εκείνον της ECC, συνιστά παρ' όλα αυτά σοβαρή ενεργειακή πρόκληση: το κόστος της βρίσκεται στα μεγέθη κλειδιών και κρυπτογραφημάτων, δηλαδή στον αριθμό των πακέτων που πρέπει να μεταδοθούν.

Το δεύτερο συμπέρασμα αφορά τη διάκριση μεταξύ πάγιου και επαναλαμβανόμενου κόστους. Οι διαδικασίες εγκαθίδρυσης κλειδιών και αμοιβαίας αυθεντικοποίησης είναι ενεργειακά δαπανηρές αλλά εκτελούνται σπάνια, ενώ η ανά πακέτο κρυπτογράφηση και ο υπολογισμός κώδικα αυθεντικοποίησης εκτελούνται συνεχώς. Ένα προσαρμοστικό πλαίσιο μετακβαντικής ασφάλειας που περιορίζει τις πράξεις πλεγμάτων αποκλειστικά στη φάση εγκαθίδρυσης κλειδιών και αναθέτει την τρέχουσα προστασία σε ελαφρές συμμετρικές πρωτογενείς συναρτήσεις αναφέρει μείωση της συνολικής κατανάλωσης κατά 14% έναντι στατικών σχημάτων, ακριβώς επειδή βελτιστοποιεί το επαναλαμβανόμενο και όχι το πάγιο σκέλος [25].

Το τρίτο συμπέρασμα αφορά τη συνέργεια συμπίεσης και κρυπτογράφησης. Πειραματική εργασία σε ακουστικούς αισθητήρες παρακολούθησης υποδομών καταδεικνύει ότι η προσαρμοστική συμπίεση του ωφέλιμου φορτίου, με τον βαθμό συμπίεσης να καθορίζεται από τη σημασία του σήματος, επιτυγχάνει μέση μείωση του φορτίου κατά 5,91 φορές διατηρώντας πλήρη ακρίβεια ανίχνευσης συμβάντων. Σε συνδυασμό με επιτάχυνση AES σε υλικό, η προβλεπόμενη διάρκεια ζωής μπαταρίας προσεγγίζει τα δεκατέσσερα έτη [18]. Το εύρημα αυτό υποδεικνύει μια σχεδιαστική αρχή που δεν αποτυπώνεται στα κλασικά πρωτόκολλα: η φθηνότερη ασφαλής μετάδοση είναι εκείνη που δεν πραγματοποιείται καθόλου και η μείωση του όγκου των δεδομένων αποτελεί εξίσου ουσιώδη μηχανισμό εξοικονόμησης με τη βελτιστοποίηση του ίδιου του κρυπτοαλγορίθμου.

Το τέταρτο και τελευταίο συμπέρασμα είναι μεθοδολογικής φύσεως. Οι παραπάνω τιμές προέρχονται από διαφορετικές πλατφόρμες, διαφορετικά μοντέλα ενέργειας και διαφορετικά σενάρια κίνησης και δεν είναι αυστηρά συγκρίσιμες μεταξύ τους. Η απουσία τυποποιημένου πλαισίου ενεργειακής αποτίμησης, την οποία επισημαίνει ρητά η σύγχρονη βιβλιογραφία της παρεμβολής [11], αποτελεί από μόνη της ένα ανοιχτό ερευνητικό πρόβλημα με πρακτική σημασία μεγαλύτερη από εκείνη πολλών επιμέρους αλγοριθμικών βελτιώσεων.

5.6 Πλεονεκτήματα και Μειονεκτήματα Υπαρχουσών Λύσεων

Η συγκριτική θεώρηση των υπαρχουσών λύσεων αναδεικνύει ένα επαναλαμβανόμενο μοτίβο: κάθε προσέγγιση βελτιστοποιεί μία διάσταση του προβλήματος εις βάρος κάποιας άλλης. Οι κρυπτογραφικές λύσεις προσφέρουν ισχυρές μαθηματικές εγγυήσεις αλλά καταναλώνουν πόρους, τα συστήματα ανίχνευσης με μηχανική μάθηση προσφέρουν προσαρμοστικότητα αλλά απαιτούν δεδομένα εκπαίδευσης και υπολογιστική ισχύ, ενώ οι αποκεντρωμένες προσεγγίσεις βασισμένες στο blockchain ενισχύουν την εμπιστοσύνη αλλά εισάγουν καθυστέρηση και επιβάρυνση αποθήκευσης. Η απουσία μιας καθολικά βέλτιστης λύσης δεν συνιστά αδυναμία του πεδίου, αλλά αντανακλά την εγγενή πολυπλοκότητα του προβλήματος της ασφάλειας υπό περιορισμούς. Το πραγματικό ζητούμενο, επομένως, δεν είναι η αναζήτηση μιας ενιαίας τέλει λύσης, αλλά η ανάπτυξη μεθοδολογιών που επιτρέπουν τη συνειδητή και τεκμηριωμένη επιλογή του κατάλληλου συνδυασμού μηχανισμών για κάθε συγκεκριμένο σενάριο εφαρμογής. Η προσέγγιση αυτή μετατοπίζει το βάρος από την τεχνολογία αυτή καθαυτή στη σχεδιαστική κρίση του μηχανικού, ο οποίος καλείται να σταθμίσει τις αντικρουόμενες απαιτήσεις και να καταλήξει στη βέλτιστη ισορροπία [1], [20].

Η ανάλυση των υπαρχουσών λύσεων ασφαλείας αναδεικνύει μια σαφή εξέλιξη από τα στατικά κρυπτογραφικά σχήματα προς τα δυναμικά συστήματα που βασίζονται στην τεχνητή νοημοσύνη. Τα παραδοσιακά πρωτόκολλα, όπως το TinyPK και το TinySec, προσφέρουν βασική προστασία μέσω κρυπτογράφησης, αλλά παρουσιάζουν σημαντικά μειονεκτήματα, όπως η αδυναμία αντιμετώπισης εσωτερικών επιθέσεων (insider attacks) και η ευπάθεια σε επιθέσεις τύπου Sybil, όπου ένας παραβιασμένος κόμβος μπορεί να υπονομεύσει την εμπιστοσύνη ολόκληρου του δικτύου. Αντίθετα, οι λύσεις που βασίζονται

στην Ελλειπτική Κρυπτογραφία (ECC) πλεονεκτούν λόγω του μικρού μεγέθους κλειδιών, το οποίο μειώνει το υπολογιστικό κόστος και την ενεργειακή κατανάλωση, καθιστώντας τις ιδανικές για τους περιορισμένους πόρους των αισθητήρων [1], [4].

Τα Συστήματα Ανίχνευσης Εισβολών (IDS) που χρησιμοποιούν Μηχανική Μάθηση προσφέρουν το σημαντικό πλεονέκτημα της αυτοματοποιημένης αναγνώρισης ανωμαλιών σε πραγματικό χρόνο. Αλγόριθμοι όπως ο Random Forest υπερέχουν σε ακρίβεια, αγγίζοντας το 98% και επιδεικνύουν υψηλή ανθεκτικότητα σε πολύπλοκα σενάρια επιθέσεων. Ωστόσο, η εφαρμογή τους συνοδεύεται από το μειονέκτημα της υψηλής αρχικής υπολογιστικής πολυπλοκότητας κατά τη φάση της εκπαίδευσης. Η χρήση τεχνικών Feature Selection, όπως ο MRMR, μετριάζει αυτό το πρόβλημα μειώνοντας τον χρόνο επεξεργασίας κατά 7 φορές, αλλά απαιτεί προσεκτική επιλογή των χαρακτηριστικών για να αποφευχθεί η απώλεια κρίσιμης πληροφορίας. Επιπλέον, οι λύσεις ανίχνευσης που βασίζονται αποκλειστικά σε μετρικές όπως το RSSI είναι μεν ελαφριές (lightweight), αλλά παραμένουν ευάλωτες σε περιβαλλοντικό θόρυβο και παρεμβολές, γεγονός που μπορεί να αυξήσει το ποσοστό των ψευδώς θετικών αποτελεσμάτων [9], [20].

Οι αρχιτεκτονικές που ενσωματώνουν Edge και Fog Computing προσφέρουν το πλεονέκτημα της τοπικής επεξεργασίας, περιορίζοντας την καθυστέρηση (latency) και ενισχύοντας την ιδιωτικότητα των δεδομένων. Παρόλα αυτά, η διαχείριση τέτοιων ιεραρχικών συστημάτων είναι πιο περίπλοκη και απαιτεί εξειδικευμένα πρωτόκολλα δρομολόγησης που να λαμβάνουν υπόψη την ενεργειακή κατανάλωση και την απόσταση, όπως οι πολυμονοπατικοί αλγόριθμοι (multipath routing). Συμπερασματικά, καμία μεμονωμένη λύση δεν είναι καθολική. Η βέλτιστη στρατηγική έγκειται σε μια υβριδική προσέγγιση που συνδυάζει την αποδοτική κρυπτογράφηση ECC για την αυθεντικοποίηση, με την ευφυή ανίχνευση Random Forest για την εποπτεία της συμπεριφοράς του δικτύου [4], [8].

Η συνολική αποτίμηση των υπάρχουσών λύσεων αναδεικνύει ότι καμία μεμονωμένη τεχνολογία δεν μπορεί να θεωρηθεί καθολική λύση για την ασφάλεια των WSNs. Κάθε προσέγγιση που εξετάστηκε κουβαλά ένα συγκεκριμένο προφίλ συμβιβασμών: η κρυπτογραφία προσφέρει ισχυρές εγγυήσεις εμπιστευτικότητας αλλά καταναλώνει πόρους, τα συστήματα ανίχνευσης εισβολών εντοπίζουν εξελιγμένες επιθέσεις αλλά απαιτούν δεδομένα εκπαίδευσης και υπολογιστική ισχύ, ενώ το blockchain εξασφαλίζει αποκεντρωμένη εμπιστοσύνη με κόστος καθυστέρησης και αποθηκευτικού χώρου. Η ωριμότητα του πεδίου έγκειται ακριβώς στην αναγνώριση ότι η βέλτιστη λύση είναι πάντοτε συμφραζόμενη, εξαρτώμενη από το μοντέλο απειλής, τους διαθέσιμους πόρους και τις λειτουργικές απαιτήσεις της εκάστοτε εφαρμογής. Αντί της αναζήτησης μιας καθολικά ανώτερης τεχνολογίας, η σύγχρονη πρακτική προσανατολίζεται στον έξυπνο συνδυασμό συμπληρωματικών μηχανισμών, ώστε τα πλεονεκτήματα του ενός να καλύπτουν τις αδυναμίες του άλλου. Αυτή η ολιστική, πολυεπίπεδη θεώρηση αποτελεί το ωριμότερο συμπέρασμα που προκύπτει από τη συγκριτική μελέτη των διαθέσιμων λύσεων [1], [20].

5.7 Μελέτη Ασφάλειας WSNs για Εφαρμογές Ελέγχου Κυκλοφορίας και Συλλογής Ηλιακής Ενέργειας

Η εφαρμογή των Ασύρματων Δικτύων Αισθητήρων στο πλαίσιο μιας «Έξυπνης Πόλης» (Smart City) περιλαμβάνει κρίσιμες υποδομές όπως ο αυτοματοποιημένος έλεγχος των μεταφορών, η έξυπνη διαχείριση ενέργειας μέσω Smart Grids, η περιβαλλοντική παρακολούθηση και τα συστήματα δημόσιας ασφάλειας. Σε ένα τέτοιο ετερογενές περιβάλλον, εκατομμύρια συσκευές διασυνδέονται μέσω του Cloud, καθιστώντας την ασφάλεια των προσωπικών δεδομένων και των υποδομών ζωτικής σημασίας,

καθώς μια πιθανή παραβίαση θα μπορούσε να οδηγήσει σε κατάρρευση των υπηρεσιών της πόλης. Για παράδειγμα, η ενσωμάτωση του IoT στα Smart Grids επιτρέπει την αμφίδρομη ανταλλαγή πληροφοριών μεταξύ παρόχων και καταναλωτών, αλλά ταυτόχρονα εκθέτει το δίκτυο σε κυβερνοεπιθέσεις που στοχεύουν στη διακοπή της ηλεκτροδότησης ή την κλοπή δεδομένων κατανάλωσης.

Στο σενάριο αυτό, η χρήση ενός IDS βασισμένου σε Μηχανική Μάθηση αποδεικνύεται καταλυτική. Η ανάλυση της κίνησης του δικτύου σε πραγματικό χρόνο επιτρέπει στον Detector να εντοπίζει ανωμαλίες που υποδηλώνουν επιθέσεις Sybil ή Sinkhole, οι οποίες είναι ιδιαίτερα διαδεδομένες σε αστικά δίκτυα λόγω της υψηλής πυκνότητας των κόμβων. Με την υιοθέτηση του αλγορίθμου Random Forest, το σύστημα μπορεί να ταξινομεί την κίνηση με ακρίβεια 98%, διασφαλίζοντας ότι οι υπηρεσίες της πόλης παραμένουν διαθέσιμες ακόμη και υπό καθεστώς επίθεσης. Επιπλέον, η εφαρμογή τεχνικών όπως η Διαφορική Ιδιωτικότητα (Differential Privacy) προστατεύει την τοποθεσία των πολιτών και τις ευαίσθητες πληροφορίες τους, προσθέτοντας στατιστικό θόρυβο στα συγκεντρωτικά δεδομένα που αναλύονται. Η μελέτη περίπτωσης αναδεικνύει επίσης τη σημασία της ενεργειακής βιωσιμότητας μέσω της χρήσης Solar Energy Harvesters. Σε μια έξυπνη πόλη, κάθε κτίριο μπορεί να διαθέτει συστήματα συλλογής ηλιακής ενέργειας που επικοινωνούν μεταξύ τους μέσω WSNs για τον διαμοιρασμό της ισχύος βάσει των αναγκών. Η ασφάλεια αυτών των συναλλαγών ενισχύεται από την ελαφριά κρυπτογράφηση ECC, η οποία προσφέρει το ίδιο επίπεδο προστασίας με το RSA αλλά με πολύ μικρότερο υπολογιστικό κόστος, γεγονός που την καθιστά ιδανική για τους περιορισμένους πόρους των αισθητήρων. Συμπερασματικά, η «Έξυπνη Πόλη» απαιτεί μια πολυεπίπεδη αρχιτεκτονική ασφαλείας που συνδυάζει την ευφυή ανίχνευση στο άκρο του δικτύου με την αποδοτική διαχείριση της ενέργειας, διασφαλίζοντας τη λειτουργική συνέχεια και την εμπιστοσύνη των χρηστών.

Για να γίνει πιο συγκεκριμένη η ανάλυση, αξίζει να εξεταστεί ένα ρεαλιστικό σενάριο επίθεσης εντός της υποδομής της έξυπνης πόλης. Ας υποτεθεί ότι ένας επιτιθέμενος εγκαθιστά έναν κακόβουλο κόμβο κοντά σε μια συστάδα αισθητήρων που παρακολουθεί την κυκλοφορία σε έναν κεντρικό οδικό άξονα, με στόχο την εξαπόλυση επίθεσης Sinkhole. Ο κακόβουλος κόμβος διαφημίζει ψευδώς ότι διαθέτει τη βέλτιστη διαδρομή προς τον σταθμό βάσης, προσελκύοντας έτσι την κίνηση ολόκληρης της συστάδας. Έχοντας αποκτήσει αυτή τη θέση-κλειδί, ο επιτιθέμενος μπορεί στη συνέχεια είτε να απορρίψει επιλεκτικά τα δεδομένα κυκλοφορίας, προκαλώντας εσφαλμένη ρύθμιση των φωτεινών σηματοδοτών, είτε να αλλοιώσει τις μετρήσεις ώστε να δημιουργήσει τεχνητή συμφόρηση. Το συγκεκριμένο παράδειγμα καταδεικνύει με ενάργεια πώς μια καθαρά τεχνική ευπάθεια στο επίπεδο δρομολόγησης μπορεί να μεταφραστεί σε απτές επιπτώσεις στην καθημερινότητα των πολιτών και στην ασφάλεια της πόλης.

Η αντιμετώπιση ενός τέτοιου σεναρίου αναδεικνύει τη χρησιμότητα της πολυεπίπεδης άμυνας που φαίνεται στο [20]. Σε πρώτο επίπεδο, οι ελαφριοί έλεγχοι που εκτελούνται τοπικά στους κόμβους, βασισμένοι σε φυσικές παραμέτρους όπως η ισχύς του λαμβανόμενου σήματος (RSSI), μπορούν να εντοπίσουν ασυνέπειες που υποδηλώνουν την παρουσία ενός κόμβου ο οποίος διαφημίζει αδικαιολόγητα ευνοϊκές διαδρομές. Σε δεύτερο επίπεδο, η ανάλυση της κίνησης από έναν κόμβο fog, εξοπλισμένο με το μοντέλο Random Forest, επιβεβαιώνει τη στατιστική ανωμαλία στη ροή των δεδομένων και ταξινομεί την επίθεση. Τέλος, ο μηχανισμός αυτο-ίασης απομονώνει τον παραβιασμένο κόμβο και αναδρομολογεί την κίνηση μέσω εναλλακτικού μονοπατιού, αποκαθιστώντας τη λειτουργία του δικτύου χωρίς ανθρώπινη παρέμβαση. Το ολοκληρωμένο αυτό παράδειγμα επιβεβαιώνει ότι καμία μεμονωμένη τεχνική δεν επαρκεί, αλλά μόνο η συνέργεια πολλαπλών αμυντικών επιπέδων μπορεί να εγγυηθεί την ανθεκτικότητα μιας κρίσιμης αστικής υποδομής [10], [20].

Η αξία μιας μελέτης περίπτωσης έγκειται στην ανάδειξη του τρόπου με τον οποίο οι θεωρητικές αρχές μεταφράζονται σε λειτουργικές αποφάσεις υπό πραγματικούς περιορισμούς. Στο σενάριο της έξυπνης πόλης, ο σχεδιαστής καλείται να ισορροπήσει μεταξύ αντικρουόμενων απαιτήσεων: αφενός την ανάγκη για ισχυρή προστασία των δεδομένων των πολιτών και αφετέρου την απαίτηση για χαμηλό κόστος και μακρά διάρκεια ζωής χιλιάδων διεσπαρμένων αισθητήρων. Η ανάλυση καταδεικνύει ότι καμία μεμονωμένη τεχνολογία δεν επαρκεί για να καλύψει το σύνολο των απαιτήσεων· αντίθετα, απαιτείται μια προσεκτικά ενορχηστρωμένη σύνθεση μηχανισμών που λειτουργούν συμπληρωματικά. Η ελαφριά κρυπτογραφία διασφαλίζει τη βασική εμπιστευτικότητα, τα συστήματα φήμης εντοπίζουν την ανώμαλη συμπεριφορά και η ανάλυση στο ομιχλώδες επίπεδο παρέχει την υπολογιστική ισχύ για την ανίχνευση εξελιγμένων επιθέσεων. Το παράδειγμα αυτό επιβεβαιώνει ότι η ασφάλεια στην πράξη δεν είναι ζήτημα επιλογής της «καλύτερης» τεχνολογίας, αλλά της βέλτιστης σύνθεσης πολλαπλών τεχνολογιών σε ένα συνεκτικό σύστημα άμυνας [1], [20].

5.8 Συγκριτική Επισκόπηση Σύγχρονων Προσεγγίσεων (2024-2026)

Η συγκριτική αξιολόγηση που προηγήθηκε εστίασε σε κλασικούς αλγορίθμους μηχανικής μάθησης επί καθιερωμένων συνόλων δεδομένων. Για να αποτυπωθεί η τρέχουσα κατάσταση του πεδίου, ο ακόλουθος πίνακας συνοψίζει αντιπροσωπευτικές προσεγγίσεις της τελευταίας τριετίας, καταγράφοντας για καθεμία τον τύπο του μηχανισμού, το σύνολο δεδομένων αξιολόγησης, την αναφερόμενη επίδοση και τον βασικό περιορισμό της. Η τελευταία στήλη είναι η σημαντικότερη, καθώς οι αναφερόμενες τιμές ακρίβειας, όπως εξηγήθηκε, δεν είναι απευθείας συγκρίσιμες.

Πίνακας 5 Συγκριτική επισκόπηση αντιπροσωπευτικών προσεγγίσεων ασφάλειας WSNs της περιόδου 2024-2026

Προσέγγιση	Τύπος μηχανισμού	Σύνολο δεδομένων	Αναφερόμενη επίδοση	Βασικός περιορισμός
Conv1D-GRU-Self Attention [34]	Βαθιά μάθηση με προσοχή	WSN-DS	Ακρίβεια 98,6% / ROC-AUC 0,9994	Χωρίς επικύρωση σε πραγματικό υλικό
CNN-GCN-BiLSTM διπλής προσοχής [35]	Βαθιά μάθηση σε γράφους	WSN-DS	Υψηλή ακρίβεια πολυκλασικής ταξινόμησης	Υψηλό υπολογιστικό κόστος για κόμβο
Υβριδικό KMeans-SMOTE + PCA + RF [45]	Κλασική μηχανική μάθηση	WSN-DS, TON-IoT	Ακρίβεια 99,94% / 99,97%	Κίνδυνος κορεσμού συνόλου δεδομένων
ADASYN + XGBoost [46]	Κλασική μηχανική μάθηση	WSN-DS	Ακρίβεια 99,87%	Περιορισμένο εύρος κατηγοριών επίθεσης
Ομόσπονδη μάθηση με LSTM [31]	Κατανεμημένη μάθηση	Πολλαπλά σύνολα	Επίδοση συγκρίσιμη με κεντρική εκπαίδευση	Ευπάθεια σε δηλητηρίαση ενημερώσεων
TinyML με δίκτυα προσοχής γράφων [33]	Συμπερασμός στον κόμβο	Σύνολα βιομηχανικού IoT	Ακρίβεια περίπου 95%	Αναπόδεικτη λειτουργία σε πραγματικό χρόνο
Υβριδικό BERT + δέντρα [39]	Γλωσσικό μοντέλο	Edge-IoTset, ToN_IoT	Ακρίβεια 98,19% / 99,15%	Μη εκτελέσιμο σε κόμβο αισθητήρα
Blockchain + ANN δύο επιπέδων [40]	Υβριδικό blockchain	Προσομοίωση WSN	Ακρίβεια 97,42% / Ανάκληση 98,35%	Απαιτεί ικανούς επικεφαλής συστάδων

SMART δυναμική εμπιστοσύνη [42]	Διαχείριση εμπιστοσύνης	Προσομοίωση WSN	Ανίχνευση 96% / ΨΑ 0,7%	Ευαισθησία στη ρύθμιση κατωφλίων
Προσαρμοστικό πλαίσιο PQC [25]	Μετακβαντική κρυπτογραφία	Προσομοίωση WSN	Μείωση ενέργειας 14%	Μεγάλα μεγέθη κλειδίων και μηνυμάτων
ZT-IoTrust [26]	Μηδενική εμπιστοσύνη	Πρότυπα σύνολα κυβερνοασφάλειας	Ανίχνευση 92,5% / ΨΘ 1,2%	Επιβάρυνση συνεχούς επαλήθευσης

Από τον πίνακα προκύπτουν τρεις παρατηρήσεις. Πρώτον, οι προσεγγίσεις με τις υψηλότερες αναφερόμενες τιμές ακρίβειας είναι εκείνες που αξιολογούνται στα παλαιότερα και κορεσμένα σύνολα δεδομένων, γεγονός που ενισχύει τη μεθοδολογική κριτική που προηγήθηκε. Δεύτερον, οι προσεγγίσεις που αντιμετωπίζουν ρεαλιστικότερα σενάρια, όπως η ομόσπονδη μάθηση και η μηδενική εμπιστοσύνη, αναφέρουν χαμηλότερες τιμές, γεγονός που πιθανότατα αντανακλά μεγαλύτερη ρεαλιστικότητα και όχι κατώτερη ποιότητα. Τρίτον, η στήλη των περιορισμών αποκαλύπτει ένα κοινό μοτίβο: το σοβαρότερο ανοιχτό ζήτημα δεν είναι η ακρίβεια ανίχνευσης αλλά η εκτελεσιμότητα στους πραγματικούς κόμβους.

5.9 Κανονιστικό Πλαίσιο και Απαιτήσεις Συμμόρφωσης

Η ανάλυση που προηγήθηκε αντιμετωπίζει την ασφάλεια ως τεχνικό πρόβλημα βελτιστοποίησης. Από το 2024 και εξής, ωστόσο, στην Ευρωπαϊκή Ένωση η ασφάλεια των συνδεδεμένων συσκευών έχει καταστεί και νομική υποχρέωση, γεγονός που μεταβάλλει ουσιαδώς τους όρους του σχεδιασμού. Η παράλειψη αναφοράς στη διάσταση αυτή θα άφηνε την παρούσα μελέτη ελλιπή, καθώς οι αποφάσεις που αναλύθηκαν παύουν πλέον να είναι αμιγώς οικονομοτεχνικές.

Ο Κανονισμός για την Ανθεκτικότητα στον Κυβερνοχώρο, γνωστός ως Cyber Resilience Act, θεσπίζει οριζόντιες απαιτήσεις κυβερνοασφάλειας για όλα τα προϊόντα με ψηφιακά στοιχεία που διατίθενται στην αγορά της Ένωσης [49]. Οι κόμβοι αισθητήρων και οι πύλες δικτύου εμπίπτουν ρητά στο πεδίο εφαρμογής του. Τέσσερις από τις απαιτήσεις του έχουν άμεσο αντίκτυπο στα ζητήματα που εξετάστηκαν. Πρώτον, τα προϊόντα οφείλουν να διατίθενται χωρίς γνωστές εκμεταλλεύσιμες ευπάθειες και με ασφαλή προεπιλεγμένη διαμόρφωση, πρακτική που καθιστά μη συμμορφούμενα τα πολυάριθμα εμπορικά συστήματα που εξακολουθούν να αποστέλλονται με προεγκατεστημένα εργοστασιακά κλειδιά, ζήτημα που επισημάνθηκε κατά την ανάλυση του ZigBee. Δεύτερον, απαιτείται μηχανισμός ασφαλών ενημερώσεων ασφαλείας καθ' όλη τη διάρκεια του υποστηριζόμενου κύκλου ζωής, απαίτηση που για κόμβους με 128 KB μνήμης flash συνιστά μη τετριμμένη σχεδιαστική πρόκληση, συνδέεται όμως άμεσα με την ανάγκη κρυπτογραφικής ευελιξίας ενόψει της μετακβαντικής μετάβασης. Τρίτον, επιβάλλεται η τήρηση καταλόγου υλικών λογισμικού. Τέταρτον, θεσπίζεται υποχρέωση αναφοράς ενεργά εκμεταλλευόμενων ευπαθειών εντός αυστηρών προθεσμιών.

Συμπληρωματικά, το ευρωπαϊκό πρότυπο ETSI EN 303 645 καθορίζει τις βασικές απαιτήσεις κυβερνοασφάλειας για καταναλωτικές συσκευές IoT και λειτουργεί ως πρακτικός οδηγός συμμόρφωσης [50]. Οι διατάξεις του, όπως η απαγόρευση καθολικών προεπιλεγμένων κωδικών, η υποχρέωση ασφαλών αποθήκευσης ευαίσθητων παραμέτρων ασφαλείας, η ελαχιστοποίηση των εκτεθειμένων διεπαφών και η κρυπτογράφηση των επικοινωνιών, αντιστοιχούν σχεδόν ένα προς ένα στους μηχανισμούς που αναλύθηκαν στο Κεφάλαιο 3.

Η ουσιαστική επίπτωση του κανονιστικού αυτού πλαισίου έγκειται στη μεταβολή της οικονομίας του σχεδιασμού. Στην ανάλυση κόστους-οφέλους που διατρέχει την παρούσα εργασία, η επιλογή παράλειψης ενός μηχανισμού ασφαλείας για λόγους εξοικονόμησης ενέργειας ή κόστους αντιμετωπιζόταν ως θεμιτός τεχνικός συμβιβασμός. Υπό το νέο καθεστώς, ορισμένοι από τους συμβιβασμούς αυτούς παύουν να είναι διαθέσιμοι, ανεξαρτήτως του ενεργειακού τους κόστους. Η ασφάλεια μετατοπίζεται έτσι

από επιθυμητό χαρακτηριστικό σε προϋπόθεση διάθεσης στην αγορά και η βελτιστοποίηση δεν αφορά πλέον το αν θα υπάρξει προστασία αλλά το πώς θα επιτευχθεί με το ελάχιστο δυνατό ενεργειακό αποτύπωμα.

5.10 Μελλοντικές Τάσεις και Ανοιχτά Ερευνητικά Προβλήματα

Η εξέλιξη των Ασύρματων Δικτύων Αισθητήρων προς το οικοσύστημα του IoT και των δικτύων 5G/6G δημιουργεί νέες προκλήσεις που απαιτούν πιο δυναμικές και αυτοπροσαρμοζόμενες λύσεις ασφαλείας. Μία από τις κυρίαρχες μελλοντικές τάσεις είναι η μετάβαση από την κλασική Μηχανική Μάθηση στη Βαθιά Μάθηση (Deep Learning) και τη Μεταφορική Μάθηση (Transfer Learning). Η χρήση μοντέλων όπως τα CNN και LSTM επιτρέπει την αυτόματη εξαγωγή χωρικών και χρονικών χαρακτηριστικών από τα δεδομένα των αισθητήρων, προσφέροντας ακρίβεια που αγγίζει το 96.8% ακόμα και σε ετερογενή περιβάλλοντα όπου τα δεδομένα εκπαίδευσης είναι περιορισμένα. Η πρόκληση εδώ παραμένει η βελτιστοποίηση αυτών των "βαρέων" μοντέλων ώστε να μπορούν να εκτελούνται σε πραγματικό χρόνο σε κόμβους με εξαιρετικά περιορισμένους πόρους [7], [19].

Παράλληλα, η ενσωμάτωση της τεχνολογίας Blockchain αναδύεται ως μια ισχυρή λύση για τη διασφάλιση της ακεραιότητας των δεδομένων και την αποκεντρωμένη διαχείριση της εμπιστοσύνης. Τα έξυπνα συμβόλαια (Smart Contracts) μπορούν να αυτοματοποιήσουν την αποβολή κακόβουλων κόμβων χωρίς την ανάγκη κεντρικής αρχής, αντιμετωπίζοντας αποτελεσματικά επιθέσεις όπως η Sybil και το Worm-hole. Ωστόσο, το "ανοιχτό" ερευνητικό πρόβλημα παραμένει το υψηλό υπολογιστικό και ενεργειακό κόστος των μηχανισμών συναίνεσης του Blockchain, το οποίο συγκρούεται με την ανάγκη για χαμηλή κατανάλωση ενέργειας στα WSNs. Η ανάπτυξη ελαφριών αλγορίθμων συναίνεσης (Lightweight Consensus) αποτελεί πεδίο έντονης επιστημονικής δραστηριότητας [4], [6].

Η ασφάλεια σε δυναμικά περιβάλλοντα, όπως τα Vehicular WSNs (V-WSNs) και τα δίκτυα που υποστηρίζονται από UAV, αποτελεί μια από τις δυσκολότερες προκλήσεις. Η υψηλή κινητικότητα των κόμβων οδηγεί σε συχνές αλλαγές στην τοπολογία, καθιστώντας τα παραδοσιακά πρωτόκολλα δρομολόγησης εφάλατα. Η έρευνα στρέφεται πλέον προς την ανάπτυξη "έξυπνων" mobile sinks και αυτόνομων συστημάτων ανίχνευσης που χρησιμοποιούν την ενισχυτική μάθηση (Reinforcement Learning) για να προσαρμόζουν τη στρατηγική άμυνας σε πραγματικό χρόνο ανάλογα με τη συμπεριφορά του επιτιθέμενου. Η επίτευξη μιας πλήρους ισορροπίας μεταξύ ασφάλειας, ιδιωτικότητας και ενεργειακής αυτονομίας παραμένει ο τελικός στόχος για τη βιωσιμότητα των έξυπνων υποδομών του μέλλοντος [14], [22].

Μια αναδυόμενη ερευνητική κατεύθυνση που αναμένεται να αναδιαμορφώσει το τοπίο της ασφάλειας είναι η ομόμορφη κρυπτογραφία (Homomorphic Encryption), η οποία επιτρέπει την εκτέλεση υπολογισμών απευθείας πάνω σε κρυπτογραφημένα δεδομένα χωρίς την προηγούμενη αποκρυπτογράφησή τους. Στο πλαίσιο των WSNs, η δυνατότητα αυτή θα επέτρεπε τη συνάθροιση δεδομένων (data aggregation) στους ενδιάμεσους κόμβους χωρίς να εκτίθεται το περιεχόμενό τους, διασφαλίζοντας την εμπιστευτικότητα από άκρο σε άκρο ακόμη και σε μη έμπιστους κόμβους. Παρά τη θεωρητική της κομψότητα, η πλήρης ομόμορφη κρυπτογραφία παραμένει υπολογιστικά απαγορευτική για τους σημεινούς αισθητήρες. Ωστόσο, οι μερικώς ομόμορφες παραλλαγές, οι οποίες υποστηρίζουν περιορισμένο σύνολο πράξεων με ανεκτό κόστος, αρχίζουν ήδη να εφαρμόζονται σε σενάρια ασφαλούς συνάθροισης, ανοίγοντας έναν υποσχόμενο δρόμο για την προστασία της ιδιωτικότητας στο επίπεδο του δικτύου.

Μια δεύτερη, εξίσου σημαντική τάση, είναι η ενσωμάτωση της αρχιτεκτονικής μηδενικής εμπιστοσύνης (Zero Trust Architecture) στα δίκτυα αισθητήρων. Σε αντίθεση με το παραδοσιακό μοντέλο που εμπιστεύεται αυτόματα κάθε κόμβο εντός της περιμέτρου του δικτύου, η προσέγγιση μηδενικής

εμπιστοσύνης απαιτεί τη συνεχή επαλήθευση της ταυτότητας και της συμπεριφοράς κάθε οντότητας πριν από κάθε αλληλεπίδραση. Η φιλοσοφία αυτή ευθυγραμμίζεται απόλυτα με τη φύση των WSNs, όπου η φυσική προσβασιμότητα των κόμβων καθιστά την υπόθεση μιας έμπιστης περιμέτρου επικίνδυνη. Η υλοποίηση ενός τέτοιου μοντέλου σε περιβάλλον περιορισμένων πόρων απαιτεί ελαφρείς μηχανισμούς συνεχούς αυθεντικοποίησης και δυναμικά συστήματα αξιολόγησης φήμης (reputation systems), τα οποία προσαρμόζουν το επίπεδο εμπιστοσύνης κάθε κόμβου με βάση το ιστορικό της συμπεριφοράς του. Η σύγκλιση της αρχιτεκτονικής μηδενικής εμπιστοσύνης με τις τεχνικές ενισχυτικής μάθησης αναμένεται να αποτελέσει έναν από τους πλέον γόνιμους τομείς έρευνας για τη θωράκιση των έξυπνων υποδομών της επόμενης δεκαετίας [10], [19].

Πέραν των τάσεων που προαναφέρθηκαν, η τυποποίηση των μετακβαντικών αλγορίθμων από το NIST το 2024 μετέτρεψε την κβαντική απειλή από θεωρητικό ζήτημα σε συγκεκριμένο πρόβλημα μηχανικής μετάβασης. Το ανοιχτό ερευνητικό ερώτημα δεν είναι πλέον ποιοι αλγόριθμοι θα χρησιμοποιηθούν, αλλά πώς μπορούν τα μεγέθη κλειδιών και κρυπτογραφημάτων που αυτοί συνεπάγονται να συμβιβαστούν με πλαίσια των 127 bytes και με μικροελεγκτές λίγων kilobyte μνήμης. Η κατεύθυνση των υβριδικών και προσαρμοστικών σχημάτων, όπου η μετακβαντική κρυπτογραφία περιορίζεται στη φάση εγκαθίδρυσης κλειδιών, φαίνεται σήμερα η πλέον υποσχόμενη [25].

Μια δεύτερη κατεύθυνση που αναδύεται ισχυρά αφορά την ασφάλεια των ίδιων των μηχανισμών τεχνητής νοημοσύνης. Καθώς τα συστήματα ανίχνευσης βασίζονται ολοένα περισσότερο σε μοντέλα μηχανικής μάθησης, τα μοντέλα αυτά καθίστανται τα ίδια στόχος. Η ανθεκτικότητα σε επιθέσεις υπεκφυγής και δηλητηρίασης, η ασφαλής συνάθροιση σε ομόσπονδα σχήματα και η επεξηγησιμότητα ως εργαλείο επικύρωσης αποτελούν ερευνητικά πεδία με άμεση πρακτική σημασία, τα οποία σήμερα υποεκπροσωπούνται στη βιβλιογραφία των WSNs σε σχέση με τη σημασία τους [37].

Τέλος, η αυξανόμενη ενσωμάτωση των WSNs σε ψηφιακά δίδυμα κρίσιμων υποδομών ανοίγει ένα πεδίο με διπλή όψη. Αφενός, το ψηφιακό δίδυμο προσφέρει ένα μοντέλο αναφοράς της αναμενόμενης συμπεριφοράς του φυσικού συστήματος, επιτρέποντας την ανίχνευση ανωμαλιών μέσω σύγκρισης και όχι μέσω στατιστικού ορίου, προσέγγιση εγγενώς ανθεκτικότερη σε επιθέσεις σταδιακής μετατόπισης. Αφετέρου, το ίδιο το δίδυμο συνιστά συγκεντρωμένη αναπαράσταση της υποδομής και, ως εκ τούτου, στόχο υψηλής αξίας του οποίου η παραβίαση θα προσέφερε στον επιτιθέμενο πλήρη γνώση του συστήματος. Η ασφάλεια του διδύμου αναδεικνύεται έτσι σε προϋπόθεση της ασφάλειας του ίδιου του δικτύου.

5.11 Επίλογος

Σε αυτό το κεφάλαιο αποτυπώθηκε η απόδοση των Συστημάτων Ανίχνευσης Εισβολών (IDS) σε Ασύρματα Δίκτυα Αισθητήρων, με έμφαση σε μετρικές όπως Accuracy, Precision, Recall και F1-Score. Ο αλγόριθμος Random Forest αποδείχθηκε ιδιαίτερα αποτελεσματικός, ενώ η επιλογή χαρακτηριστικών (MRMR) βελτιώνει την ταχύτητα και μειώνει την κατανάλωση ενέργειας χωρίς να χάνει ακρίβεια. Η μελέτη περίπτωσης σε «Έξυπνη Πόλη» δείχνει ότι η συνδυαστική χρήση έξυπνης ανίχνευσης, ελαφριάς κρυπτογράφησης και ενεργειακής διαχείρισης διασφαλίζει ασφάλεια και βιωσιμότητα. Τέλος, οι μελλοντικές τάσεις στρέφονται σε βαθιά μάθηση, Blockchain και Reinforcement Learning για πιο δυναμικά και αυτό προσαρμοζόμενα δίκτυα, ισορροπώντας ασφάλεια, ιδιωτικότητα και ενεργειακή απόδοση.

Κεφάλαιο 6ο: Συμπεράσματα και Προτάσεις βελτίωσης

6.1 Συμπεράσματα

Το σημαντικότερο συμπέρασμα της συγκριτικής αξιολόγησης αφορά την υπεροχή των αλγορίθμων εμποτευόμενης μάθησης. Ο αλγόριθμος Random Forest αναδείχθηκε ως η βέλτιστη λύση, επιτυγχάνοντας ακρίβεια 98%, σημειώνοντας μια θεαματική βελτίωση +19% σε σχέση με προγενέστερα μοντέλα. Παράλληλα, η μελέτη απέδειξε ότι η υπολογιστική επιβάρυνση, που αποτελεί το παραδοσιακό εμπόδιο για την εφαρμογή ΑΙ σε αισθητήρες, μπορεί να αντιμετωπιστεί αποτελεσματικά. Η χρήση τεχνικών επιλογής χαρακτηριστικών, όπως ο αλγόριθμος MRMR, επέτρεψε τη μείωση των εξεταζόμενων παραμέτρων από 41 σε 12, επιτυγχάνοντας επιτάχυνση της επεξεργασίας κατά 7 φορές. Αυτό το εύρημα είναι καθοριστικό, καθώς επιτρέπει την ανίχνευση στο άκρο του δικτύου (Edge), επεκτείνοντας σημαντικά τον κύκλο ζωής των κόμβων [5], [20].

Η παρούσα εργασία ανέλυσε διεξοδικά το κρίσιμο ζήτημα της ασφάλειας στα Ασύρματα Δίκτυα Αισθητήρων (WSNs), αναδεικνύοντας την πολυπλοκότητα των απειλών σε κάθε επίπεδο του πρωτοκόλλου επικοινωνίας. Μέσα από τη μελέτη, κατέστη σαφές ότι οι παραδοσιακές κρυπτογραφικές μέθοδοι, αν και απαραίτητες για την αυθεντικοποίηση, δεν επαρκούν από μόνες τους για την αντιμετώπιση εξελιγμένων επιθέσεων όπως η Sybil, το Wormhole και η εξάντληση πόρων (DoS). Η υιοθέτηση Συστημάτων Ανίχνευσης Εισβολών (IDS) που βασίζονται σε Μηχανική Μάθηση αποτελεί πλέον επιτακτική ανάγκη για τη διασφάλιση της ακεραιότητας και της διαθεσιμότητας των δεδομένων σε κρίσιμες εφαρμογές, όπως οι Έξυπνες Πόλεις και η βιομηχανία [1], [20].

Επιπλέον, η εργασία ανέδειξε τη σημασία της ιεραρχικής δομής και της χρήσης ελαφριάς κρυπτογραφίας, όπως η ECC, η οποία προσφέρει υψηλή ασφάλεια με ελάχιστο ενεργειακό κόστος σε σύγκριση με το RSA. Η συνέργεια αυτών των τεχνολογιών διασφαλίζει ότι το IDS δεν λειτουργεί μόνο ως μηχανισμός ανίχνευσης, αλλά και ως σύστημα προστασίας της ιδιωτικότητας των χρηστών μέσω τεχνικών όπως η διαφορική ιδιωτικότητα. Συνολικά, η μελέτη επιβεβαιώνει ότι η ασφάλεια στα WSNs δεν είναι ένα στατικό προϊόν, αλλά μια δυναμική διαδικασία που απαιτεί τη συνεχή προσαρμογή των αλγορίθμων στα νέα δεδομένα και τις μεταβαλλόμενες συνθήκες του περιβάλλοντος [3], [4].

Πέρα από τα επιμέρους τεχνικά ευρήματα, η συνολική θεώρηση της εργασίας οδηγεί σε ένα ευρύτερο εννοιολογικό συμπέρασμα: η ασφάλεια στα ασύρματα δίκτυα αισθητήρων δεν μπορεί να αντιμετωπιστεί ως ένα αυτόνομο στρώμα που προστίθεται εκ των υστέρων σε ένα ήδη σχεδιασμένο σύστημα, αλλά οφείλει να ενσωματώνεται οργανικά σε κάθε φάση του σχεδιασμού, από το υλικό έως το επίπεδο εφαρμογής. Η προσέγγιση αυτή, γνωστή ως ασφάλεια εκ σχεδιασμού (security by design), αναδείχθηκε ως κοινός παρονομαστής όλων των αποτελεσματικών λύσεων που εξετάστηκαν. Καθεμία από τις τεχνολογίες που αναλύθηκαν —η ελαφριά κρυπτογραφία, τα συστήματα ανίχνευσης εισβολών, το blockchain και η επεξεργασία στο άκρο του δικτύου— προσφέρει μερική μόνο προστασία όταν εφαρμόζεται μεμονωμένα. Η πραγματική ανθεκτικότητα προκύπτει από τη συνέργειά τους, μέσα από μια αρχιτεκτονική άμυνας σε βάθος (defense in depth) που συνδυάζει πολλαπλά, αλληλοϋποστηριζόμενα επίπεδα προστασίας.

Είναι επίσης σημαντικό να τονιστεί ότι τα ποσοτικά αποτελέσματα της παρούσας μελέτης, αν και ενθαρρυντικά, οφείλουν να ερμηνεύονται εντός των ορίων του πειραματικού πλαισίου στο οποίο προέκυψαν. Η αξιολόγηση βασίστηκε σε δημόσια διαθέσιμα σύνολα δεδομένων, τα οποία, παρά την ευρεία

αποδοχή τους στην ερευνητική κοινότητα, δεν αποτυπώνουν πλήρως την ποικιλομορφία και τη δυναμικότητα ενός πραγματικού δικτύου σε λειτουργία. Συνεπώς, η μεταφορά των ευρημάτων σε επιχειρησιακό περιβάλλον απαιτεί περαιτέρω επικύρωση μέσω δοκιμών πεδίου και πειραμάτων σε φυσικές υποδομές. Η επίγνωση αυτών των περιορισμών δεν αναιρεί την αξία των συμπερασμάτων, αλλά αντίθετα ενισχύει την επιστημονική τους εγκυρότητα, οριοθετώντας με σαφήνεια το πεδίο εφαρμογής τους και ανοίγοντας τον δρόμο για μελλοντική, βαθύτερη διερεύνηση.

Παρά τα ενθαρρυντικά ευρήματα, η παρούσα μελέτη υπόκειται σε ορισμένους περιορισμούς που είναι σημαντικό να αναγνωριστούν ρητά, καθώς οριοθετούν το πεδίο εφαρμογής των συμπερασμάτων και κατευθύνουν τη μελλοντική έρευνα. Ο πρώτος και σημαντικότερος περιορισμός σχετίζεται με τη φύση των δεδομένων αξιολόγησης. Η συγκριτική ανάλυση των αλγορίθμων βασίστηκε σε δημόσια διαθέσιμα σύνολα δεδομένων, όπως τα NSL-KDD και WSN-DS, τα οποία, αν και αποτελούν καθιερωμένα σημεία αναφοράς (benchmarks) στην ερευνητική κοινότητα, δεν αποτυπώνουν πλήρως τη δυναμικότητα και την ετερογένεια ενός πραγματικού δικτύου αισθητήρων σε συνθήκες παραγωγής. Οι κατανομές της κυκλοφορίας, τα πρότυπα θορύβου και οι συνθήκες περιβάλλοντος σε ένα φυσικό δίκτυο ενδέχεται να αποκλίνουν σημαντικά από τα σενάρια που περιγράφονται στα εν λόγω σύνολα δεδομένων [5], [20].

Ένας δεύτερος περιορισμός αφορά τη μεθοδολογία της αξιολόγησης. Η μέτρηση της απόδοσης των αλγορίθμων πραγματοποιήθηκε σε περιβάλλον προσομοίωσης και όχι σε πραγματικούς, ενεργειακά περιορισμένους κόμβους αισθητήρων. Συνεπώς, οι μετρήσεις της υπολογιστικής επιβάρυνσης και της κατανάλωσης ενέργειας αποτελούν εκτιμήσεις βασισμένες σε θεωρητικά μοντέλα, οι οποίες ενδέχεται να διαφοροποιηθούν κατά την υλοποίηση σε πραγματικό υλικό (hardware) με συγκεκριμένους περιορισμούς μνήμης και επεξεργαστικής ισχύος. Η επικύρωση των ευρημάτων σε πλατφόρμες όπως οι κόμβοι TelosB ή Arduino αποτελεί απαραίτητο επόμενο βήμα για την επιβεβαίωση της πρακτικής εφαρμοσιμότητας των προτεινόμενων λύσεων [4], [23].

Τέλος, η μελέτη εστίασε κατά κύριο λόγο σε ένα συγκεκριμένο φάσμα επιθέσεων και αλγορίθμων μηχανικής μάθησης. Η ταχεία εξέλιξη τόσο των τεχνικών επίθεσης όσο και των μοντέλων βαθιάς μάθησης σημαίνει ότι ορισμένες πιο πρόσφατες προσεγγίσεις, όπως τα adversarial attacks έναντι των ίδιων των συστημάτων ανίχνευσης ή οι αρχιτεκτονικές transformer για ανάλυση χρονοσειρών, δεν εξετάστηκαν στο πλήρες εύρος τους. Η επίγνωση αυτών των περιορισμών δεν αναιρεί την αξία των αποτελεσμάτων· αντίθετα, ενισχύει την επιστημονική τους εγκυρότητα, οριοθετώντας με σαφήνεια τις συνθήκες υπό τις οποίες ισχύουν και προετοιμάζοντας το έδαφος για βαθύτερη, στοχευμένη διερεύνηση στο μέλλον [7], [19].

Μια τέταρτη και σημαντική διάσταση που ανέδειξε η επισκόπηση της σύγχρονης βιβλιογραφίας αφορά την αξιοπιστία των ίδιων των δημοσιευμένων αποτελεσμάτων. Η συστηματική εμφάνιση τιμών ακρίβειας που υπερβαίνουν το 99,9% σε καθιερωμένα σύνολα δεδομένων δεν αποτελεί ένδειξη επίλυσης του προβλήματος, αλλά μάλλον ένδειξη κορεσμού των συνόλων αυτών και, σε αρκετές περιπτώσεις, μεθοδολογικών αδυναμιών όπως η εφαρμογή τεχνικών εξισορρόπησης πριν από τον διαχωρισμό εκπαίδευσης και δοκιμής. Η μετατόπιση του κριτηρίου αξιολόγησης προς τη διασυνολική γενίκευση και προς τη μετρημένη επίδοση σε πραγματικό υλικό αποτελεί, κατά την κρίση της παρούσας εργασίας, την πλέον επείγουσα μεθοδολογική ανάγκη του πεδίου.

Μια πέμπτη διαπίστωση αφορά τη μεταβολή του ίδιου του πλαισίου εντός του οποίου λαμβάνονται οι σχεδιαστικές αποφάσεις. Η τυποποίηση της ελαφριάς κρυπτογραφίας μέσω του Ascon και της μετακβαντικής κρυπτογραφίας μέσω των προτύπων FIPS, σε συνδυασμό με τις δεσμευτικές πλέον κανονιστικές απαιτήσεις του ευρωπαϊκού πλαισίου, αφαιρεί από τον μηχανικό ορισμένους από τους συμβιβασμούς που μέχρι πρόσφατα θεωρούνταν θεμιτοί. Η ασφάλεια παύει να αποτελεί μεταβλητή

βελτιστοποίησης και μετατρέπεται σε περιορισμό του προβλήματος, με τη βελτιστοποίηση να μετατοπίζεται στον τρόπο επίτευξής της με το ελάχιστο δυνατό ενεργειακό κόστος.

Τέλος, η συνολική εικόνα που προκύπτει από την επισκόπηση της περιόδου 2024-2026 είναι εκείνη ενός πεδίου που έχει ωριμάσει ως προς τους αλγορίθμους αλλά παραμένει ανώριμο ως προς τη μεθοδολογία επικύρωσης. Οι διαθέσιμοι μηχανισμοί, από την τυποποιημένη ελαφριά κρυπτογραφία έως τα καταναμεμένα μοντέλα μηχανικής μάθησης, επαρκούν για την αντιμετώπιση του μεγαλύτερου μέρους των γνωστών απειλών. Το πραγματικό εμπόδιο δεν είναι η απουσία λύσεων, αλλά η δυσκολία τεκμηριωμένης επιλογής μεταξύ τους υπό συνθήκες όπου τα δημοσιευμένα αποτελέσματα δεν είναι συγκρίσιμα και το κόστος εκτέλεσης σπανίως μετριέται στο υλικό-στόχο.

Η παρούσα διπλωματική εργασία επιχείρησε να καλύψει το κενό που εντοπίζεται μεταξύ της θεωρητικής ανάλυσης των απειλών ασφαλείας στα Ασύρματα Δίκτυα Αισθητήρων και της πρακτικής αξιολόγησης σύγχρονων μηχανισμών άμυνας. Η βασική συμβολή της έγκειται στη συστηματική και ενοποιημένη παρουσίαση ενός πεδίου που συχνά μελετάται αποσπασματικά: από την ταξινόμηση των επιθέσεων ανά επίπεδο της στοίβας πρωτοκόλλων, έως τη συγκριτική αποτίμηση κρυπτογραφικών τεχνικών, πρωτοκόλλων ασφαλείας και σύγχρονων τεχνολογιών όπως η τεχνητή νοημοσύνη και το blockchain. Η ολιστική αυτή προσέγγιση επιτρέπει στον αναγνώστη να αντιληφθεί τη διασύνδεση των επιμέρους μηχανισμών και τη σημασία της πολυεπίπεδης άμυνας [1], [3].

Σε επίπεδο εφαρμοσμένης έρευνας, η εργασία συνεισφέρει μέσω της συγκριτικής αξιολόγησης αλγορίθμων μηχανικής μάθησης για την ανίχνευση εισβολών, καταδεικνύοντας ποσοτικά ότι η συνδυασμένη χρήση του αλγορίθμου Random Forest με τεχνικές επιλογής χαρακτηριστικών (MRMR) επιτυγχάνει υψηλή ακρίβεια ανίχνευσης διατηρώντας ταυτόχρονα χαμηλή υπολογιστική επιβάρυνση. Το εύρημα αυτό έχει άμεση πρακτική αξία, καθώς αποδεικνύει ότι η εφαρμογή προηγμένων τεχνικών τεχνητής νοημοσύνης σε ενεργειακά περιορισμένες συσκευές δεν είναι απλώς θεωρητικά εφικτή, αλλά και βιώσιμη υπό συγκεκριμένες προϋποθέσεις βελτιστοποίησης [20], [23].

Τέλος, η εργασία προσφέρει μια σειρά τεκμηριωμένων προτάσεων και κατευθύνσεων που μπορούν να αξιοποιηθούν τόσο από την ακαδημαϊκή κοινότητα όσο και από μηχανικούς που σχεδιάζουν πραγματικές υποδομές WSNs. Η ανάδειξη της αρχής της «ασφάλειας εκ σχεδιασμού» (security by design), η έμφαση στην ενεργειακή βιωσιμότητα ως κριτήριο σχεδιασμού και η σύνδεση των μελλοντικών απειλών (6G, κβαντικός υπολογισμός) με συγκεκριμένες ερευνητικές προτεραιότητες, συνθέτουν ένα πλαίσιο που μπορεί να λειτουργήσει ως αφετηρία για περαιτέρω μελέτη. Με τον τρόπο αυτό, η συμβολή της εργασίας δεν περιορίζεται στην καταγραφή της υπάρχουσας γνώσης, αλλά επεκτείνεται στη διαμόρφωση ενός οδικού χάρτη για την ανθεκτική ασφάλεια των δικτύων αισθητήρων της επόμενης γενιάς [7], [9].

6.2 Προτάσεις βελτίωσης

Η μετάβαση προς τα δίκτυα έκτης γενιάς (6G) υπόσχεται υπερ-υψηλές ταχύτητες και σχεδόν μηδενική καθυστέρηση, γεγονός που θα επιτρέψει τη διασύνδεση δισεκατομμυρίων νέων συσκευών WSNs σε εφαρμογές όπως το Internet of Everything (IoE) και οι Έξυπνες Πόλεις. Ωστόσο, η αυξημένη αυτή πολυπλοκότητα διευρύνει την επιφάνεια επίθεσης, καθώς η διαχείριση της ασφάλειας σε τόσο μαζική κλίμακα καθίσταται εξαιρετικά δύσκολη. Στο περιβάλλον του 6G, οι παραδοσιακές κεντροποιημένες λύσεις άμυνας θα είναι ανεπαρκείς, απαιτώντας τη χρήση καταναμεμένης τεχνητής νοημοσύνης (Distributed AI) και Federated Learning, όπου οι κόμβοι θα εκπαιδεύουν τοπικά μοντέλα ανίχνευσης χωρίς να μοιράζονται τα ακατέργαστα δεδομένα τους, ενισχύοντας έτσι την ιδιωτικότητα.

Παράλληλα, η σημαντικότερη ίσως απειλή για το μέλλον της κρυπτογραφίας στα WSNs προέρχεται από την άνοδο του Κβαντικού Υπολογισμού (Quantum Computing). Οι κβαντικοί υπολογιστές αναμένεται να έχουν την ισχύ να σπάσουν τους υπάρχοντες ασύμμετρους αλγορίθμους, όπως το RSA και το ECC, οι οποίοι αποτελούν τη βάση για την αυθεντικοποίηση και την ανταλλαγή κλειδιών στα σημερινά δίκτυα. Αυτή η εξέλιξη δημιουργεί την ανάγκη για άμεση έρευνα και μετάβαση σε Μετα-κβαντική Κρυπτογραφία (Post-Quantum Cryptography - PQC). Η πρόκληση εδώ είναι διπλή: οι νέοι κβαντικά-ανθεκτικοί αλγόριθμοι πρέπει να είναι αρκετά ελαφριοί ώστε να μπορούν να εκτελεστούν από τους ενεργειακά περιορισμένους αισθητήρες, χωρίς να θυσιάζεται η ταχύτητα επικοινωνίας.

Εκτός από τις κρυπτογραφικές απειλές, τα μελλοντικά WSNs θα αντιμετωπίσουν και την πρόκληση της δυναμικής κινητικότητας. Με την ενσωμάτωση αισθητήρων σε σμήνη drones (UAVs) και αυτόνομα οχήματα (V-WSN), η τοπολογία του δικτύου θα αλλάζει σε χιλιοστά του δευτερολέπτου, καθιστώντας τον εντοπισμό επιθέσεων όπως το Wormhole μια συνεχή πρόκληση [10], [14]. Η αυριανή ασφάλεια θα βασίζεται σε υβριδικά συστήματα που θα συνδυάζουν το Blockchain για την αποκεντρωμένη διαχείριση της εμπιστοσύνης με τη Βαθιά Μάθηση (Deep Learning) για την πρόβλεψη των κινήσεων των επιτιθέμενων, διασφαλίζοντας τη λειτουργική συνέχεια σε έναν κόσμο πλήρως διασυνδεδεμένο.

Μια διάσταση που συχνά παραβλέπεται στη συζήτηση για τις μελλοντικές προκλήσεις είναι το ζήτημα της εφοδιαστικής αλυσίδας (supply chain security) των κόμβων αισθητήρων. Καθώς η παραγωγή υλικού και λογισμικού για συσκευές IoT είναι παγκοσμιοποιημένη και κατακερματισμένη, αυξάνεται ο κίνδυνος εισαγωγής κακόβουλων στοιχείων ή κρυφών παραθύρων (backdoors) ήδη από το στάδιο της κατασκευής. Ένας παραβιασμένος κόμβος που φτάνει στο πεδίο εφαρμογής ήδη μολυσμένος υπονομεύει εκ των προτέρων κάθε μηχανισμό ασφάλειας που εφαρμόζεται κατά τη λειτουργία. Η αντιμετώπιση αυτής της απειλής απαιτεί μηχανισμούς επαλήθευσης της ακεραιότητας του υλικολογισμικού (firmware attestation) και ασφαλούς εκκίνησης (secure boot), οι οποίοι διασφαλίζουν ότι ο κόμβος εκτελεί μόνο πιστοποιημένο και αναλλοίωτο κώδικα. Η ενσωμάτωση τέτοιων εγγυήσεων σε συσκευές περιορισμένων πόρων αποτελεί μια ανοιχτή ερευνητική πρόκληση με αυξανόμενη πρακτική σημασία.

Τέλος, η ωρίμανση των τεχνολογιών αυτών εγείρει αναπόφευκτα και μη τεχνικά ζητήματα, τα οποία θα διαμορφώσουν καθοριστικά το μέλλον της ασφάλειας των WSNs. Η ραγδαία διεξόδος δεσεκατομμυρίων αισθητήρων στον δημόσιο και ιδιωτικό χώρο θέτει επιτακτικά ερωτήματα διακυβέρνησης, λογοδοσίας και κανονιστικής συμμόρφωσης, ιδίως σε ό,τι αφορά την προστασία των προσωπικών δεδομένων. Η απουσία ενός ενιαίου διεθνούς πλαισίου τυποποίησης δυσχεραίνει τη διαλειτουργικότητα και αφήνει περιθώρια για ανομοιομορφα επίπεδα προστασίας μεταξύ διαφορετικών κατασκευαστών και δικαιοδοσιών. Η μελλοντική πρόοδος, επομένως, δεν θα κριθεί αποκλειστικά από την κρυπτογραφική ισχύ των αλγορίθμων, αλλά και από την ικανότητα της ερευνητικής κοινότητας, της βιομηχανίας και των ρυθμιστικών αρχών να συνεργαστούν για τη θέσπιση κοινών προτύπων που θα εγγυώνται την ασφάλεια και την εμπιστοσύνη σε κλίμακα παγκόσμιας υποδομής.

Προτάσεις για Βελτίωση της Ασφάλειας

Με βάση τη διεξοδική ανάλυση και τα αποτελέσματα της συγκριτικής αξιολόγησης, η πρώτη βασική πρόταση αφορά την καθολική υιοθέτηση δυναμικών συστημάτων Feature Selection (Επιλογής Χαρακτηριστικών) σε κάθε κόμβο του δικτύου. Όπως αποδείχθηκε, η εστίαση στα 12 πιο σημαντικά χαρακτηριστικά μέσω του αλγορίθμου MRMR δεν αποτελεί απλώς μια επιλογή βελτιστοποίησης, αλλά αναγκαία προϋπόθεση για τη βιωσιμότητα του IDS. Προτείνεται η δημιουργία ενός μηχανισμού που θα προσαρμόζει αυτόματα τα εξεταζόμενα χαρακτηριστικά ανάλογα με το τρέχον επίπεδο ενέργειας του

κόμβου, επιτρέποντας μια «διαβάθμιση ασφαλείας» που θα εξισορροπεί την προστασία με τον χρόνο ζωής της μπαταρίας.

Επιπλέον, κρίνεται απαραίτητη η μετάβαση από τα μεμονωμένα συστήματα ανίχνευσης σε υβριδικές αρχιτεκτονικές συνεργατικής άμυνας. Τα WSNs θα πρέπει να αξιοποιούν το Fog Computing για τη διεξαγωγή σύνθετων αναλύσεων με τον αλγόριθμο Random Forest (που επιτυγχάνει ακρίβεια 98%), ενώ ταυτόχρονα οι απλοί κόμβοι θα εκτελούν ελαφριούς ελέγχους βασισμένους σε φυσικές παραμέτρους, όπως το RSSI και οι MAC διευθύνσεις, για την άμεση αναγνώριση επιθέσεων Sybil. Αυτή η πολυεπίπεδη προσέγγιση διασφαλίζει ότι ακόμη και αν ένας επιτιθέμενος παρακάμψει την κρυπτογραφική αυθεντικοποίηση, η ανώμαλη συμπεριφορά του θα εντοπιστεί από το σύστημα παρακολούθησης συμπεριφοράς.

Προτείνεται η ενσωμάτωση τεχνικών αυτο-ίασης (Self-healing) μέσω της χρήσης ελαφριών έξυπνων συμβολαίων (Smart Contracts). Σε περίπτωση που ο Detector επιβεβαιώσει την παρουσία ενός κακόβουλου κόμβου, το δίκτυο θα πρέπει να είναι σε θέση να αναδρομολογεί αυτόματα την κίνηση μέσω πολυμονοπατικών αλγορίθμων (Multipath Routing) και να απομονώνει τον παραβιασμένο κόμβο χωρίς την παρέμβαση κεντρικού διαχειριστή. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ανάπτυξη κβαντικά-ανθεκτικών βιβλιοθηκών ECC, ώστε να θωρακιστούν οι υποδομές των έξυπνων πόλεων απέναντι στις επερχόμενες απειλές του κβαντικού υπολογισμού, διασφαλίζοντας την εμπιστοσύνη των χρηστών στις τεχνολογίες του αύριο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Y. Qi, Q. Pei, Y. Zeng, C. Yang, and S.-p. Bu, "A security testing approach for WSN protocols based on object-oriented attack model," in Proc. 7th Int. Conf. Comput. Intell. Security (CIS), Sanya, China, 2011, pp. 517–520.
- [2] M. I. Jais et al., "Hardware comparison capturing received signal strength indication (RSSI) for wireless sensors network (WSN)," in Proc. IEEE Student Conf. Res. Dev. (SCORED), Kuala Lumpur, Malaysia, 2015, pp. 278–282.
- [3] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," in Proc. 3rd Int. Conf. Comput. Intell., Model. Simulation (CIMSIM), Langkawi, Malaysia, 2011, pp. 308–311.
- [4] G. Xiaowang and Z. Jianyong, "Analysis and design of energy-oriented security protocols for Wireless Sensor Networks," in Proc. Int. Conf. Electron. Mech. Eng. Inf. Technol. (EMEIT), Harbin, China, 2011, pp. 2298–2301.
- [5] S. Umamaheshwari, S. A. Kumar, and S. Sasikala, "Towards Building Robust Intrusion Detection System in Wireless Sensor Networks using Machine Learning and Feature Selection," in Proc. Int. Conf. Adv. Electr., Electron., Commun., Comput. Autom. (ICAECA), Coimbatore, India, 2021, pp. 1–6.
- [6] A. Viswanathan, N. B. Sai Shibu, S. N. Rao, and M. V. Ramesh, "Security Challenges in the Integration of IoT with WSN for Smart Grid Applications," in Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC), Coimbatore, India, 2017, pp. 1–4.
- [7] S. Saraswathi, "Cross-Domain Anomaly Detection in Wireless Sensor Networks Using Hybrid Deep Transfer Learning," in Proc. 11th Int. Conf. Smart Comput. Commun. (ICSCC), Kochi, India, 2025, pp. 1–8.
- [8] M. Benaddy, B. E. Habel, M. E. Ouali, O. E. Meslouhi, and S. Krit, "A mutlipath routing algorithm for wireless sensor networks under distance and energy consumption constraints for reliable data transmission," in Proc. Int. Conf. Eng. MIS (ICEMIS), Monastir, Tunisia, 2017, pp. 1–4.
- [9] R. Lakhanpal and S. Sharma, "Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique," in Proc. Int. Conf. Comput. Power, Energy Inf. Commun. (ICCPEIC), Melmaruvathur, India, 2016, pp. 283–287.
- [10] R. Kumar Dwivedi, P. Sharma, and R. Kumar, "Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network," in Proc. 8th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence), Noida, India, 2018, pp. 727–732.
- [11] C. Herrera-Loera, C. Del-Valle-Soto, L. J. Valdivia, J. Vázquez-Castillo, and C. Mex-Perera, "A Systematic Review and Energy-Centric Taxonomy of Jamming Attacks and Countermeasures in Wireless Sensor Networks," *Sensors*, vol. 26, no. 2, Art. no. 579, 2026, doi: 10.3390/s26020579.
- [12] A. K. Prajapati, E. S. Pilli, R. B. Battula, V. Varadharajan, A. Verma, and R. C. Joshi, "A comprehensive survey on RPL routing-based attacks, defences and future directions in Internet of Things," *Computers and Electrical Engineering*, Art. no. 110071, 2025, doi: 10.1016/j.compeleceng.2025.110071.

- [13] Z. Larkin and C. Easttom, "An Examination of LPWAN Security in Maritime Applications," *Journal of Cybersecurity and Privacy*, vol. 6, no. 2, Art. no. 65, 2026, doi: 10.3390/jcp6020065.
- [14] M. A. Al-Mashhadani, M. M. Hamdi, and A. S. Mustafa, "Role and challenges of the use of UAV-aided WSN monitoring system in large-scale sectors," in *Proc. 3rd Int. Congr. Hum.-Comput. Interact., Optim. Rob. Appl. (HORA)*, Ankara, Turkey, 2021, pp. 1–6.
- [15] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp. 293–315, 2003.
- [16] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.
- [17] J.-K. Lee, Y.-R. Choi, B.-K. Suh, S.-W. Jung, and K.-I. Kim, "A Survey on Energy Drainage Attacks and Countermeasures in Wireless Sensor Networks," *Applied Sciences*, vol. 15, no. 4, Art. no. 2213, 2025, doi: 10.3390/app15042213.
- [18] Y.-R. Choi, H.-Y. Jeong, and S. Moon, "Hybrid Framework for Secure Low-Power Data Encryption with Adaptive Payload Compression in Resource-Constrained IoT Systems," *Sensors*, vol. 26, no. 7, Art. no. 2253, 2026, doi: 10.3390/s26072253.
- [19] D. K. Shareef and V. Jyothsna, "A Survey on Deep Learning Techniques for Secure and Accurate Mobile Sink Position Prediction in Vehicular Pattern WSN," in *Proc. 8th Int. Conf. Inventive Syst. Control (ICISC)*, Coimbatore, India, 2024, pp. 596–603.
- [20] S. Chandra, A. Giri, B. Ghosal, and B. Mondal, "Exposing Sybil Attacks: A New Paradigm for WSN Defense," in *Proc. Int. Conf. Comput., Intell., Appl. (CIACON)*, Durgapur, India, 2025, pp. 1–6.
- [21] National Institute of Standards and Technology, "Module-Lattice-Based Key-Encapsulation Mechanism Standard," *Federal Information Processing Standards Publication FIPS 203*, Gaithersburg, MD, USA, Aug. 2024.
- [22] J. Metan and K. N. Narasimha Murthy, "Robust and secure key management in WSN using arbitrary key-deployment," in *Proc. Int. Conf. Emerg. Res. Electron., Comput. Sci. Technol. (ICERECT)*, Mandya, India, 2015, pp. 246–250.
- [23] S. Amaran and R. M. Mohan, "Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks," in *Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Coimbatore, India, 2021, pp. 1100–1104.
- [24] National Institute of Standards and Technology, "Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions," *NIST Special Publication SP 800-232*, Gaithersburg, MD, USA, Aug. 2025.
- [25] H. Hayouni, "Adaptive post-quantum security framework for wireless sensor networks using lightweight cryptography and context-aware key management," *The Journal of Supercomputing*, vol. 81, no. 15, Art. no. 1426, 2025, doi: 10.1007/s11227-025-07916-1.
- [26] J. Wang, N. Huang, B. Wang, R. Ao, Q. Fu, and X. Guo, "ZT-IoTrust: A Quantum-Resistant Zero Trust Framework for Secure IoT Access Control," *Electronics*, vol. 14, no. 22, Art. no. 4469, 2025, doi: 10.3390/electronics14224469.
- [27] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.

- [28] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500–528, 2006.
- [29] S. K. Erskine, "Secure Data Aggregation Using Authentication and Authorization for Privacy Preservation in Wireless Sensor Networks," *Sensors*, vol. 24, no. 7, Art. no. 2090, 2024, doi: 10.3390/s24072090.
- [30] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, "Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications," *Sensors*, vol. 25, no. 4, Art. no. 1194, 2025, doi: 10.3390/s25041194.
- [31] R. W. Anwar, M. Abrar, A. Salam, and F. Ullah, "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis," *PeerJ Computer Science*, vol. 11, Art. no. e2751, 2025, doi: 10.7717/peerj-cs.2751.
- [32] N. Albanbay, Y. Tursynbek, K. Graffi, R. Uskenbayeva, Z. Kalpeyeva, Z. Abilkaiyr, and Y. Ayapov, "Federated Learning-Based Intrusion Detection in IoT Networks: Performance Evaluation and Data Scaling Study," *Journal of Sensor and Actuator Networks*, vol. 14, no. 4, Art. no. 78, 2025, doi: 10.3390/jsan14040078.
- [33] L. Nassef, M. I. Alghamdi, S. Ben Chaabane, Q. Abbas, W. M. Alawad, O. H. Albalawi, O. I. Alqaisi, and B. Fakieh, "Lightweight and Energy-Aware Intrusion Detection for Industrial IoT Using TinyML and Edge AI," *Scientific Reports*, vol. 16, Art. no. 18524, 2026, doi: 10.1038/s41598-026-50690-0.
- [34] K. H. R. Mbongo, K. Ahmed, O. Mamyrbayev, G. Wang, F. Zuo, A. Akhmediyarova, N. Mukazhanov, and A. Ayapbergenova, "Conv1D-GRU-Self Attention: An Efficient Deep Learning Framework for Detecting Intrusions in Wireless Sensor Networks," *Future Internet*, vol. 17, no. 7, Art. no. 301, 2025, doi: 10.3390/fi17070301.
- [35] L. H. Baniata, A. ALDabbas, J. M. Atwan, H. Alahmer, B. Elmasri, and C. Bunternghit, "A Dual-Attention CNN-GCN-BiLSTM Framework for Intelligent Intrusion Detection in Wireless Sensor Networks," *Future Internet*, vol. 18, no. 1, Art. no. 5, 2026, doi: 10.3390/fi18010005.
- [36] A. Alabbadi and F. Bajaber, "An Intrusion Detection System over the IoT Data Streams Using eXplainable Artificial Intelligence (XAI)," *Sensors*, vol. 25, no. 3, Art. no. 847, 2025, doi: 10.3390/s25030847.
- [37] A. Vassilev, A. Oprea, A. Fordyce, H. Anderson, X. Davies, and M. Hamin, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," *NIST Trustworthy and Responsible AI Report NIST AI 100-2e2025*, Gaithersburg, MD, USA, Mar. 2025.
- [38] P. Sinha, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, V. K. Pandey, and I. Hunko, "An efficient data driven framework for intrusion detection in wireless sensor networks using deep learning," *Scientific Reports*, vol. 15, Art. no. 34046, 2025, doi: 10.1038/s41598-025-12867-x.
- [39] M. Algarni, M. Y. Dahab, A. A. Alsulami, B. Alturki, and R. Alsini, "Toward a Hybrid Intrusion Detection Framework for IIoT Using a Large Language Model," *Sensors*, vol. 26, no. 4, Art. no. 1231, 2026, doi: 10.3390/s26041231.
- [40] M. S. Jabor, A. S. Azez, J. C. Campelo, and A. Bonastre, "A Lightweight IDS Based on Blockchain and Machine Learning for Detecting Physical Attacks in Wireless Sensor Networks," *Sensors*, vol. 26, no. 6, Art. no. 1961, 2026, doi: 10.3390/s26061961.

- [41] D. K. Murala, S. Ahmad, V. A. S. Ponnappalli, V. A. Vuyyuru, and E. Hitimana, "ChainShieldML: an intelligent decentralized security framework for next generation wireless sensor networks," *Scientific Reports*, vol. 15, Art. no. 42960, 2025, doi: 10.1038/s41598-025-27077-8.
- [42] P. Goswami, T. Khan, V. Pathak, and A. Alabdultif, "Machine learning based dynamic trust estimation framework for securing wireless sensor networks," *Scientific Reports*, vol. 15, Art. no. 35821, 2025, doi: 10.1038/s41598-025-19768-z.
- [43] R. Gupta, S. K. Gupta, S. B. Singh, R. Kumar, and R. Muthukkumar, "Adaptive deep reinforcement learning-based secure routing for wireless sensor networks," *Scientific Reports*, vol. 16, 2026, doi: 10.1038/s41598-026-62519-x.
- [44] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.
- [45] M. A. Talukder, M. Khalid, and N. Sultana, "A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction," *Scientific Reports*, vol. 15, Art. no. 4617, 2025, doi: 10.1038/s41598-025-87028-1.
- [46] Y. Y. Munaye, A. D. Gebeyehu, L.-C. Tai, Z. A. Abebe, A. B. Workneh, R. B. Tarekegn, Y. B. Chekol, and G. B. Tarekegn, "Machine Learning-Driven Intrusion Detection for Securing IoT-Based Wireless Sensor Networks," *Future Internet*, vol. 18, no. 2, Art. no. 113, 2026, doi: 10.3390/fi18020113.
- [47] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors*, vol. 2016, Art. no. 4731953, 2016.
- [48] Ripon Patgiri, Udit Varshney, Tanya Akutota, Rakesh Kunde, "An Investigation on Intrusion Detection System Using Machine Learning," *IEEE Symposium Series on Computational intelligence (SSCI)*, Bangalore, India, pp. 1688, 2018.
- [49] European Parliament and Council of the European Union, "Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)," *Official Journal of the European Union*, L series, Nov. 2024.
- [50] ETSI, "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements," *ETSI EN 303 645 V3.1.3*, Sophia Antipolis, France, Sep. 2024.