ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Αναγνώριση και Αντιμετώπιση Κακόβουλων Επιθέσεων σε Ασύρματα Τοπικά Δίκτυα με Τεχνικές Μηχανικής Μάθησης

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Παναγιώτης Μυλωνάς (ΑΜ: 3120296)

Επιβλέπων: Ξενάκης Απόστολος, *Επίκουρος Καθηγητής*

ΛΑΡΙΣΑ, Σεπτέμβριος 2025

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Recognition and Mitigation of Malicious Attacks on Wireless Local Area Networks Using Machine Learning Techniques

BACHELOR THESIS

Panagiotis Mylonas (RN: 3120296)

Supervisor: ***Xenakis Apostolos, Associate Professor***

LARISSA, September 2025

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η Δηλών/ούσα

(Υπογραφή)

Ονοματεπώνυμο Φοιτητή/-ήτριας

Ημερομηνία

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων **Απόστολος Ξενάκης**

Επίκουρος Καθηγητής/Ασύρματα Δίκτυα Αισθητήρων με Εφαρμογές στην Πρωτογενή Παραγωγή ,

Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Μέλος **Κωνσταντίνος Χαϊκάλης**

Αναπληρωτής Καθηγητής /Επανασχηματιζόμενες δομές κωδικών ανίχνευσης και διόρθωσης σφαλμάτων σε τηλεπικοινωνιακά συστήματα

, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Μέλος **Δημήτριος Κοσμάνος**

Ακαδημαϊκός Υπότροφος /Εφαρμογές Ψηφιακών Συστημάτων, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης: dd-mm-yyyy

Περίληψη

Η παρούσα πτυχιακή είχε στόχο τη σχεδίαση και υλοποίηση ενός πρακτικού συστήματος ανίχνευσης εισβολών σε δίκτυα (IDS/WIDS) βασισμένου σε μηχανική μάθηση, ικανού να λειτουργεί σε πραγματικές συνθήκες. Επιδιώχθηκε συνέπεια μεταξύ εκπαίδευσης και παραγωγικής ανίχνευσης, μικρό και εκφραστικό σύνολο γνωρισμάτων, καθώς και διπλή λειτουργία (ζωντανή παρακολούθηση και ανάλυση αρχείων pcap). Η μεθοδολογία στηρίχθηκε σε ενιαίο αγωγό «capture → flows → features → model → alerts». Τα πακέτα ομαδοποιήθηκαν σε ροές με βάση πεντάπτυχο (πηγή/προορισμός IP, θύρες, πρωτόκολλο), οι ροές «έκλειναν» σε FIN/RST ή μετά από αδράνεια και, κατά το κλείσιμο, εξάγονταν έξι γνωρίσματα χαμηλού κόστους αλλά υψηλής πληροφορίας: διάρκεια, bytes προς/από την πηγή, τύπος πρωτοκόλλου, υπηρεσία βάσει θύρας και συνοπτική ένδειξη TCP flags. Τα δεδομένα προεπεξεργάστηκαν με τυποποίηση στα αριθμητικά και ασφαλές one-hot στα κατηγορικά, και ο προεπεξεργαστής «δέθηκε» με τον ταξινομητή σε ενιαίο pipeline που αποθηκεύτηκε και επαναχρησιμοποιήθηκε αυτούσιο. Ως ταξινομητής χρησιμοποιήθηκε κατά προτίμηση XGBoost, με εναλλακτική Random Forest όταν δεν ήταν διαθέσιμο, ενώ η απόφαση βασίστηκε σε πιθανότητα ανωμαλίας και ρυθμιζόμενο κατώφλι ώστε να ελέγχεται η ευαισθησία/θόρυβος. Η αξιολόγηση πραγματοποιήθηκε με διαχωρισμό εκπαίδευσης–ελέγχου και μετρικές precision/recall/F1 για την κλάση «anomaly», καθώς και με offline δοκιμές σε pcap για επιβεβαίωση της ροής από άκρο σε άκρο. Η υλοποίηση κατέγραψε τα alerts σε βάση δεδομένων, παρείχε ειδοποίηση μέσω email και τήρησε δομημένα logs για αποσφαλμάτωση και ιχνηλασιμότητα.

Η τελική έκβαση του εγχειρήματος ήταν ένα πλήρως λειτουργικό IDS που λαμβάνει κίνηση, συναρμολογεί ροές, εξάγει συνεπή γνωρίσματα, εφαρμόζει συνεπές pipeline μηχανικής μάθησης και παράγει τεκμηριωμένους συναγερμούς σε πραγματικό χρόνο ή εκτός σύνδεσης. Το σύστημα απέδειξε τη βιωσιμότητά του σε πραγματικές ροές και pcap, ενώ ανέδειξε και σαφείς κατευθύνσεις ωρίμανσης για παραγωγή (διαχείριση μυστικών, έλεγχος ακεραιότητας μοντέλου, retries/rate-limiting, βασικές μετρικές υγείας).

Συνολικά, επιτεύχθηκε ο στόχος ενός λιτού, επεξηγήσιμου και επεκτάσιμου IDS με σταθερή συμπεριφορά, χαμηλό υπολογιστικό κόστος και εύκολη προσαρμογή ευαισθησίας, το οποίο μπορεί να αποτελέσει βάση για περαιτέρω έρευνα και ενσωμάτωση σε επιχειρησιακά περιβάλλοντα.

Abstract

This thesis set out to design and implement a practical intrusion detection system (IDS/WIDS) based on machine learning that can operate under real-world conditions. The objectives were to ensure strict consistency between training and production inference, to employ a small yet expressive feature set, and to support both live monitoring and offline analysis of packet captures. The methodology followed a unified, end-to-end pipeline: capture → flow assembly → feature extraction → model inference → alerting. Network packets were grouped into flows by 5-tuple (source/destination IP, ports, protocol); each flow closed on TCP FIN/RST or after inactivity. At closure, six low-cost, high-signal features were extracted: duration, bytes from and to the source, transport protocol type, inferred service from destination port, and a compact TCP-flag indicator. Numeric features were standardized and categorical features one-hot encoded with "unknown-safe" handling. Preprocessing and classifier were bound into a single persisted pipeline and reused verbatim at inference. XGBoost was used as the preferred classifier, with Random Forest as a compatible fallback; decisions were based on anomaly probability and a configurable threshold to tune sensitivity versus noise.

Evaluation employed a stratified train/test split and reported precision, recall, and F1 for the anomaly class, complemented by offline end-to-end tests on pcap files to verify the full path from capture to alert. The implementation persisted alerts in a relational database, supported email notifications, and produced structured logs for debugging and traceability.

The outcome is a fully functional IDS that ingests traffic, assembles flows, extracts consistent features, applies a unified ML pipeline, and produces documented alerts in real time or offline. The system demonstrated viability and low computational cost, while highlighting clear hardening steps for production (secrets management, model integrity checks, retries/rate limiting, health metrics). Overall, the project achieved a lean, explainable, and extensible IDS with stable behavior and adjustable sensitivity—providing a solid base for further research and operational integration.

Ευχαριστίες

Αρχικά, θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Ξενάκη Απόστολο για την πολύτιμη καθοδήγηση, τις ουσιαστικές παρατηρήσεις και τη διαρκή υποστήριξη που μου προσέφερε κατά τη διάρκεια της εκπόνησης της παρούσας πτυχιακής εργασίας. Η εργασία αυτή αποτέλεσε για εμένα την πρώτη απαιτητική πρόκληση, έθεσα τον πήχη ψηλά, όμως οι γνώσεις και οι εμπειρίες που αποκόμισα είναι ανεκτίμητες. Είμαι ιδιαίτερα χαρούμενος που κατάφερα να φέρω εις πέρας ένα τόσο σημαντικό εγχείρημα ήδη από το προπτυχιακό μου επίπεδο.

Μυλωνάς Παναγιώτης

25/9/2025

Περιεχόμενα

1 Εισαγωγή

Τα ασύρματα τοπικά δίκτυα (WLAN/Wi-Fi) έχουν καταστεί βασική υποδομή για οργανισμούς, πανεπιστήμια και οικιακά περιβάλλοντα. Η ίδια η φύση τους, εκπομπή μέσω αέρα, εύκολη πρόσβαση πέρα από τα «τείχη» ενός κτηρίου τα καθιστά ελκυστικό στόχο για επιτιθέμενους. Λανθασμένες ρυθμίσεις, αδύναμοι μηχανισμοί προστασίας, «κρυφές» συσκευές ή rogue σημεία πρόσβασης και εξελισσόμενες τεχνικές (π.χ. αποαυθεντικοποίηση, evil-twin, στοχευμένο DoS) έχουν δείξει ότι τα προληπτικά μέτρα από μόνα τους δεν αρκούν. Σε αυτό το πλαίσιο, τα συστήματα ανίχνευσης εισβολών (IDS/WIDS) λειτουργούν ως η δεύτερη γραμμή άμυνας: παρακολουθούν τη συμπεριφορά του δικτύου και αναδεικνύουν έγκαιρα αποκλίσεις που αξίζουν διερεύνηση, μειώνοντας τον χρόνο εντοπισμού και τον πιθανό αντίκτυπο ενός συμβάντος.

Κεντρική θέση στην πρακτική αποτελεσματικότητα κάθε IDS έχει η βαθιά γνώση της αρχιτεκτονικής του δικτύου. Η ασφάλεια δεν είναι αφηρημένη έννοια· υλοποιείται πάνω σε συγκεκριμένη τοπολογία: διάταξη και ισχύς των σημείων πρόσβασης, κανάλια και ζώνες κάλυψης, διαχωρισμός δικτύων (εταιρικό, επισκεπτών, IoT), σημεία διασύνδεσης με το ενσύρματο backbone, κρίσιμα συστήματα και ροές δεδομένων. Η χαρτογράφηση αυτών των στοιχείων επιτρέπει: (α) στρατηγική τοποθέτηση αισθητήρων/συλλεκτών ώστε να μην υπάρχουν «τυφλές ζώνες», (β) προτεραιοποίηση των τμημάτων υψηλής αξίας και (γ) ρεαλιστικούς κανόνες ανίχνευσης που λαμβάνουν υπόψη φυσιολογικά πρότυπα κάθε τμήματος. Με απλά λόγια, όσο καλύτερα γνωρίζουμε το δίκτυό μας, τόσο πιο ακριβές και ωφέλιμο γίνεται το IDS λιγότερος θόρυβος, περισσότερη ουσία.

Σκοπός της παρούσας εργασίας είναι να παρουσιάσει μια πρακτική προσέγγιση για ανίχνευση εισβολών σε WLAN με αξιοποίηση τεχνικών μηχανικής μάθησης, δίνοντας έμφαση στην απλότητα, την αναπαραγωγιμότητα και τη λειτουργικότητα σε πραγματικές συνθήκες. Εξετάζουμε πώς μπορούν να απομονωθούν πληροφοριακά σήματα από την ασύρματη κίνηση, πώς εντάσσονται σε έναν συνεπή αγωγό ανίχνευσης και με ποιον

τρόπο ρυθμίζεται η ευαισθησία του συστήματος ώστε να υπηρετεί διαφορετικές επιχειρησιακές ανάγκες (π.χ. ελάχιστες χαμένες επιθέσεις ή ελάχιστος θόρυβος).

Συνεισφορά της εργασίας είναι η συστηματική σύνδεση τριών στοιχείων: (1) σαφές λειτουργικό κίνητρο για IDS σε Wi-Fi, (2) αρχιτεκτονική οπτική που κατευθύνει τη συλλογή/εποπτεία και (3) μια ρεαλιστική υλοποίηση ανίχνευσης με μηχανική μάθηση, έτοιμη να αξιολογηθεί σε ζωντανά ή offline σενάρια.

Διάρθρωση Πτυχιακής

Κεφάλαιο 1 παρουσιάζει το πλαίσιο, τους στόχους, τη συνεισφορά και τη μεθοδολογία, καθώς και τη συνοπτική διάρθρωση του κειμένου. Κεφάλαιο 2 συνοψίζει τα τεχνικά θεμέλια των δικτύων WLAN (802.11), τα βασικά πρωτόκολλα/μηχανισμούς ασφαλείας και τον χάρτη απειλών. Κεφάλαιο 3 χαρτογραφεί τη σχετική έρευνα και τις κύριες προσεγγίσεις WIDS με έμφαση σε τεχνικές μηχανικής μάθησης. Κεφάλαιο 4 παρουσιάζει την αρχιτεκτονική της προτεινόμενης λύσης και τον τρόπο ένταξής της στο δίκτυο (πηγή δεδομένων, Flow Aggregator, αγωγός χαρακτηριστικών, μοντέλο, πολιτική ειδοποιήσεων). Κεφάλαιο 5 περιγράφει την υλοποίηση και τις σχεδιαστικές αποφάσεις (pipeline προεπεξεργασίας, scripts εκπαίδευσης/εξυπηρέτησης, συμβατότητα χαρακτηριστικών). Κεφάλαιο 6 επικεντρώνεται στα δεδομένα και στη διαδικασία εκπαίδευσης (split, ισορροπία κλάσεων, hyperparameters), καθώς και στη βαθμονόμηση πιθανοτήτων (isotonic) και στην επιλογή επιχειρησιακού κατωφλίου. Κεφάλαιο 7 παρουσιάζει την πειραματική αξιολόγηση και τα ευρήματα (ROC-AUC, PR-AUC, classification report, confusion matrices, ανάλυση ευαισθησίας κατωφλίου). Κεφάλαιο 8 συγκεντρώνει τη λειτουργική αξιολόγηση και τα ζητήματα παραγωγικής χρήσης (απόδοση/καθυστέρηση, κλιμάκωση, ανθεκτικότητα), συζητά περιορισμούς και κινδύνους και καταλήγει σε συμπεράσματα και προτεινόμενες επεκτάσεις.

2 Τεχνολογίες Δικτύωσης

Η εις βάθος κατανόηση των τεχνολογιών δικτύωσης αποτελεί πάντα πρωταρχική θεμελιώδη προϋπόθεση για τη κάθε σχεδίαση και την υλοποίηση ενός αποτελεσματικού και ασφαλούς συστήματος ανίχνευσης εισβολών σε ασύρματα δίκτυα. Το παρόν κεφάλαιο που θα αναλύσουμε, επικεντρώνεται στην παρουσίαση των βασικών αρχών, των συσκευών που στελεχώνουν την δικτυακή δομή και των τεχνολογιών που διαμορφώνουν τη λειτουργία των σύγχρονων δικτύων, με μεγάλη έμφαση στις ιδιαιτερότητες της ασύρματης επικοινωνίας.

2.1 Ορισμός και Βασική Δομή ενός Δικτύου

Για κατανοήσουμε τα βασικά ενα δίκτυο επικοινωνίας αποτελείται από ένα σύνολο διασυνδεδεμένων συσκευών μεταξύ τους, που επιτρέπουν τη μετάδοση και ανταλλαγή πακέτων με δεδομένα κύριως μέσω προκαθορισμένων πρωτοκόλλων που καθορίζουν τους κανόνες επικοινωνίας. Μια δικτυακή υποδομή, λοιπόν μπορεί να λειτουργεί είτε ενσύρματα ένα κομμάτι της, μέσω φυσικών μέσων μετάδοσης όπως καλώδια οπτικών ινών ή χαλκού, είτε ασύρματα αντίστοιχα, αξιοποιώντας έτσι λοιπόν τα ηλεκτρομαγνητικά κύματα για τη μεταφορά πληροφοριών και των δεδομένων. Πιο αναλυτικά η κύρια βασική αρχιτεκτονική ενός δικτύου μπορεί να περιλαμβάνει κόμβους επικοινωνίας (όπως υπολογιστές, αισθητήρες και κινητές συσκευές), ειδικούς δρομολογητές (routers) για την κατεύθυνση της κίνησης και συνδέσμους μετάδοσης (μέσα επικοινωνίας).

Ωστόσο στην περίπτωση των ασύρματων δικτύων, η μετάδοση των δεδομένων πραγματοποιείται διαφορετικά. Συμμετέχουν μέσω ραδιοσυχνοτήτων, παρέχοντας μεγαλύτερη ευελιξία και διαλειτουργικότητα. Ωστόσο, η απουσία των φυσικών συνδέσεων συνεπάγεται με αυξημένες προκλήσεις ασφάλειας για τους αναλυτές και προπάντων για τα ανιχνευτικά συστήματα εισβολών (IDS, IPS), καθώς οι επιθέσεις τύπου παρακολούθησης (eavesdropping) - αρκετά σημαντική επίθεση που δηλώνει

παρόν ως απειλή στις μέρες μας και θα την αναλύσουμε ως τρόπο επίθεσης παρακάτω, επίσης οι παρεμβολές (jamming) και πλαστογράφησης πακέτων (spoofing) είναι πιο πιθανές να συμβούν. Για την αντιμετώπιση αυτών των απειλών, οι σύγχρονες τεχνολογίες ασύρματης επικοινωνίας έχουν εξελιχθεί σημαντικά και μέσω προτύπων ασφάλειας (WPA3), ενσωματώνοντας βελτιωμένους μηχανισμούς κρυπτογράφησης, ελέγχου πρόσβασης και διαχείρισης φάσματος.

Συγκεκριμένα οι πρόσφατες καινοτομίες στα ασύρματα πρωτόκολλα, όπως το Wi-Fi 6/6E και το επερχόμενο κατά εκτιμήσεις τέλη 2024 σύμφωνα με τους μηχανικούς ανάπτυξης του Wi-Fi 7 (802. 11be), προσφέρουν σημαντικές βελτιώσεις στη χωρητικότητα, την ανθεκτικότητα στις παρεμβολές και την ενεργειακή απόδοση. Ειδικότερα, το Wi-Fi 7 αναμένεται να εισάγει τεχνικές όπως η πολυκαναλική λειτουργία (multi-link operation) και οι εξελιγμένοι αλγόριθμοι διαχείρισης πακέτων, επιτρέποντας υψηλότερους ρυθμούς μετάδοσης και χαμηλότερη καθυστέρηση, χαρακτηριστικά κρίσιμα για εφαρμογές υψηλής απόδοσης, όπως το cloud computing και το διαδίκτυο των πραγμάτων (IoT) [17][18]. Ήδη απο τα τέλη του έτους 2024 συναντούμε πολλούς κόμβους και δρομολογητές να υποστηρίζουν το ταχύτερο και ασφαλέστερο Wi-Fi 7.

2.2 Ad-hoc Δίκτυα

Τα ad-hoc δίκτυα μπορούμε να τα περιγράψουμε ως προσωρινού χαρακτήρα συνδέσεις μεταξύ συσκευών, οι οποίες δεν απαιτούν κάποια σταθερή υποδομή όπως είναι οι δρομολογητές (routers) ή οι μεταγωγείς (switches) που συμμετέχουν ως διαμεσολαβητές. Έγιναν γνωστά για το κύριο πλεονέκτημά τους την ευελιξία, καθώς κάθε συσκευή μπορεί να λειτουργήσει ταυτόχρονα και ως κόμβος και ως δρομολογητής, πολλά σενάρια δικτύου μπορούμε να συναντήσουμε κατα αυτόν τον τρόπο σήμερα. Έτσι διευκολύνεται η επικοινωνία σε μέρη όπου η χρήση συμβατικών δικτύων είναι δύσκολη ή και αδύνατη. Παρόλα αυτά, τα ad-hoc δίκτυα παρουσιάζουν αρκετά μειονεκτήματα, όπως περιορισμένη χωρητικότητα μετάδοσης δεδομένων και μεγαλύτερη ευπάθεια σε κακόβουλες επιθέσεις. Παρόλες αυτές τις δυσκολίες, έχουν αποδειχθεί ιδιαίτερα χρήσιμα σε περιπτώσεις όπως οι φυσικές καταστροφές, οι στρατιωτικές αποστολές και οι εφαρμογές του Διαδικτύου των Πραγμάτων (IoT) [19].

Παράλληλα, τα ad-hoc δίκτυα μπορεί να γίνουν κίνδυνος για την ασφάλεια των ασύρματων δικτύων, κυρίως λόγω της απουσίας κεντρικού σημείου πρόσβασης που συνήθως εξασφαλίζει τη σύνδεση με το ενσύρματο δίκτυο. Αυτό έχει ως αποτέλεσμα την περιορισμένη επικοινωνία μόνο μεταξύ των συσκευών, χωρίς δυνατότητα εύκολης σύνδεσης με εξωτερικά δίκτυα, ή σε κάποιες περιπτώσεις, μια στοιχειώδη πρόσβαση στο διαδίκτυο.

Γιατί όμως τα ad-hoc δίκτυα αποτελούν σοβαρό ζήτημα ασφάλειας αφού δεν είναι τα κατάλληλα;

Τα ad-hoc δίκτυα, επίσης γνωστά ως δίκτυα peer-to-peer, παρουσιάζουν σημαντικά προβλήματα ασφάλειας κυρίως λόγω απουσίας κεντρικού ελέγχου και διαχείρισης των συσκευών του δικτύου. Σε αντίθεση με δίκτυα που βασίζονται σε σημεία πρόσβασης (access points) όπου υπάρχει κεντρικός διαχειριστής που θέτει κανόνες ασφαλείας της κίνησης, σε ένα ad-hoc δίκτυο κάθε συσκευή μπορεί να συνδεθεί χωρίς περιορισμούς. Έτσι αυτό αυξάνει σημαντικά την πιθανότητα ανεπιθύμητης πρόσβασης στο δίκτυο μας από κακόβουλους χρήστες [20].

Επιπλέον, στα ad-hoc δίκτυα, η κρυπτογράφηση είναι συχνά ανεπαρκής ή ακόμη και ανύπαρκτη. Για παράδειγμα, το πρωτόκολλο WEP (Wired Equivalent Privacy) που χρησιμοποιείται σε κάποια ad-hoc δίκτυα θεωρείται ξεπερασμένο και ιδιαίτερα ευάλωτο, καθώς μπορεί εύκολα να αποκρυπτογραφηθεί μέσα σε λίγα μόλις λεπτά. Το WPA/WPA2 Personal, που είναι πιο αξιόπιστο, δεν υποστηρίζεται πάντα, αφήνοντας τα δίκτυα ευάλωτα σε επιθέσεις [21].

Τα δίκτυα αυτά είναι επίσης ευάλωτα σε επιθέσεις τύπου man-in-the-middle (MitM), κατά τις οποίες ένας επιτιθέμενος παρεμβάλλεται στην επικοινωνία δύο συσκευών και καταγράφει ή κλέβει τα δεδομένα που ανταλλάσσονται [22]. Χωρίς κεντρικό σύστημα ελέγχου και ταυτοποίησης, οι χρήστες δεν μπορούν να είναι σίγουροι αν επικοινωνούν με τον σωστό παραλήπτη ή αν πρόκειται για κάποιον που υποδύεται νόμιμη συσκευή.

Επιπρόσθετα, τα ad-hoc δίκτυα είναι ιδιαίτερα εκτεθειμένα σε επιθέσεις άρνησης υπηρεσίας (Denial of Service - DoS). Εφόσον οι συσκευές επικοινωνούν απευθείας, δεν υπάρχει αποτελεσματικός μηχανισμός εντοπισμού και προστασίας από τέτοιου τύπου επιθέσεις, οι οποίες μπορεί να προκαλέσουν ολοκληρωτική διακοπή της επικοινωνίας. Ουσιαστικά η έλλειψη κεντρικής αρχής δυσκολεύει την ανίχνευση και απομόνωση κακόβουλων χρηστών που υπερφορτώνουν το δίκτυο, καταναλώνοντας πόρους και προκαλώντας προβλήματα στη λειτουργία του [23].

Συνοψίζοντας, η έλλειψη κεντρικού ελέγχου, η ανεπαρκής κρυπτογράφηση, η ευαισθησία σε επιθέσεις MitM και DoS, και η δυσκολία ελέγχου των συνδεδεμένων συσκευών καθιστούν τα ad-hoc δίκτυα ανασφαλή, ιδιαίτερα όταν απαιτείται υψηλός βαθμός προστασίας δεδομένων.

Παρά τους παραπάνω κινδύνους, τα ad-hoc δίκτυα προσφέρουν και σημαντικά πλεονεκτήματα, όπως η γρήγορη εγκατάσταση και η εύκολη ανταλλαγή δεδομένων μεταξύ φορητών συσκευών, smartphones και άλλων έξυπνων συσκευών. Επομένως, είναι πολύ σημαντικό οι χρήστες να εκπαιδεύονται ώστε να γνωρίζουν πώς να διαμορφώνουν ένα τέτοιο δίκτυο χρησιμοποιώντας τουλάχιστον βασικά μέτρα ασφαλείας, όπως η δημιουργία ισχυρών κωδικών πρόσβασης.

2.3 Δρομολογητές (Routers)

Οι δρομολογητές (routers) αποτελούν ένα από τα βασικότερα μέρη κάθε δικτύου, αφού η δουλειά τους είναι να μεταφέρουν τα δεδομένα ανάμεσα σε διαφορετικά υποδίκτυα. Για να πετύχουν αυτή τη λειτουργία, χρησιμοποιούν πρωτόκολλα δρομολόγησης, όπως το OSPF (Open Shortest Path First), που είναι από τα πιο διαδεδομένα σήμερα, το παλαιότερο RIP (Routing Information Protocol), το οποίο όμως έχει περιορισμένη χρήση πλέον, και το EIGRP (Enhanced Interior Gateway Routing Protocol), που συναντάται κυρίως σε συσκευές της Cisco. Αυτά τα πρωτόκολλα αξιοποιούν ειδικούς αλγορίθμους για να αποφασίσουν ποια είναι η καλύτερη δυνατή διαδρομή ώστε τα πακέτα δεδομένων να φτάσουν γρήγορα και με ασφάλεια στον προορισμό τους στο τρίτο επίπεδο του OSI (Network Layer).

Σε ένα ασύρματο δίκτυο, οι δρομολογητές έχουν και το ρόλο του σημείου πρόσβασης (access point). Αυτό σημαίνει ότι επιτρέπουν στις συσκευές να συνδέονται ασύρματα, ενώ έχουν τη δυνατότητα να διαχειρίζονται πολλά διαφορετικά ασύρματα δίκτυα (SSIDs) ταυτόχρονα, σε συχνότητες όπως τα 2.4 GHz και τα 5 GHz. Επιπλέον, οι σύγχρονοι δρομολογητές διαθέτουν ισχυρά πρωτόκολλα ασφαλείας, όπως WPA2 και WPA3, που παρέχουν καλύτερη προστασία απέναντι σε επιθέσεις.

Ένα ακόμη πλεονέκτημα των σύγχρονων routers είναι ότι συχνά περιλαμβάνουν ενσωματωμένα συστήματα ασφαλείας, όπως είναι τα συστήματα ανίχνευσης εισβολών (Wireless-IDS). Αυτά τα εργαλεία βοηθούν στην έγκαιρη αναγνώριση επιθέσεων, έτσι ώστε να μπορεί να περιοριστεί άμεσα οποιαδήποτε προσπάθεια παραβίασης του δικτύου.

2.4 Διακόπτες (Switches) σε Ασύρματα Τοπικά Δίκτυα (WLANs)

2.4.1 Εισαγωγή στους Διακόπτες

Οι διακόπτες ή στην αγγλική τους ορολογία switches αποτελούν αναπόσπαστο κομμάτι των ενσύρματων τοπικών δικτύων μικρών μεγάλων , καθώς διευκολύνουν την ομαλή και αποδοτική μεταφορά δεδομένων μεταξύ των συνδεδεμένων συσκευών σε ένα δίκτυο. Συγκεκριμένα λειτουργούν σε ένα τυπικό LAN, οι διακόπτες λειτουργούν στο επίπεδο 2 του μοντέλου OSI (επίπεδο ζεύξης δεδομένων) αφού δρομολογούν μονάχα mac addresses και όχι εξωτερικές IP, κατευθύνοντας τα δεδομένα προς τον σωστό προορισμό με βάση τη διεύθυνση MAC κάθε συσκευής. Συχνά συναντούμε μια σύγχηση με το σε ποιο επίπεδο του OSI κατατάσονται.

Αλλά ας εξηγήσουμε γιατί υπάρχει με μία σύντομη απάντηση. Το παραδοσιακό switch θεωρείται συσκευή Επιπέδου 2 (Data Link Layer - Access Layer) , καθώς βασίζεται στις διευθύνσεις MAC (Media Access Control) για τη λήψη αποφάσεων προώθησης πακέτων, οι οποίες δεν δρομολούγντε πέρα απο το τοπικό-εσωτερικό δίκτυο. Ωστόσο, με την πρόοδο της τεχνολογίας, έχουν αναπτυχθεί και switches Επιπέδου 3 (Network Layer) που λειτουργούν με βάση τις διευθύνσεις IP και υποστηρίζουν δυναμική δρομολόγηση. Είναι δύο διαφορετικές συσκευές και χρησιμοποιούντε για διαφορετικό τελείως σκοπό.

2.4.2 Διακόπτες σε Ασύρματα Δίκτυα (WLANs)

Όταν μιλάμε για ασύρματα τοπικά δίκτυα (WLANs), οι διακόπτες αποκτούν μια πιο εξειδικευμένη λειτουργία, προσαρμοσμένη στην ασύρματη επικοινωνία. Οι βασικές δομικές μονάδες ενός WLAN περιλαμβάνουν:

Τα Σημεία Πρόσβασης (Access Points - APs): Αυτές οι συσκευές όπως θα εξηγήσουμε και στο επόμενο κεφάλαιο λειτουργούν ως γέφυρες, συνδέοντας τις ασύρματες συσκευές με το ενσύρματο δίκτυο, επιτρέποντας έτσι την αμφίδρομη επικοινωνία μεταξύ τους.

Ασύρματοι Διακόπτες (Wireless Switches): Δεν είναι πολλοί γνωστοί αλλά μπορούν και αναλαμβάνουν τον έλεγχο της κυκλοφορίας δεδομένων μεταξύ των APs και του υπόλοιπου δικτύου, ενώ ταυτόχρονα ενισχύουν την ασφάλεια του συστήματος. Η αποτελεσματικότητα ενός WLAN εξαρτάται σε μεγάλο βαθμό από το πόσο καλά προστατεύονται αυτά τα στοιχεία [24].

2.4.3 Ο Ρόλος των Διακοπτών στην Ασφάλεια των WLANs

Οι διακόπτες διαδραματίζουν καθοριστικό ρόλο στην ασφάλεια των ασύρματων δικτύων και για αυτό πρέπει να λαμβάνουμε σημαντικά την υγεία του συστήματος του καθώς δρομολογείται όλη η κίνηση του δικτύου μας μέσω αυτών. Η σωστή διαμόρφωση και διαχείρισή τους μπορεί να αποτρέψει επιθέσεις όπως η υποκλοπή δεδομένων μέσω επιθέσεων man-in-the-middle, αλλά και επιθέσεις άρνησης υπηρεσίας (DoS) που αποσκοπούν στην αποσταθεροποίηση του δικτύου. Επιπλέον, η ενσωμάτωση τεχνικών μηχανικής μάθησης στους διακόπτες μπορεί να βοηθήσει στην ανίχνευση ύποπτων μοτίβων στην κίνηση των δεδομένων, συμβάλλοντας έτσι στην έγκαιρη αντιμετώπιση πιθανών επιθέσεων.

2.4.4 Συμπεράσματα

Οι διακόπτες αποτελούν βασικά δομικά στοιχεία τόσο των ενσύρματων όσο και των ασύρματων δικτύων, διασφαλίζοντας την ομαλή επικοινωνία μεταξύ των συσκευών. Η σωστή διαχείρισή τους είναι ζωτικής σημασίας για τη σταθερότητα και την ασφάλεια των WLANs, ειδικά όταν εφαρμόζονται τεχνικές μηχανικής μάθησης για την αναγνώριση και την αποτροπή κακόβουλων επιθέσεων. Σε έναν κόσμο όπου οι επιθέσεις στα δίκτυα γίνονται όλο και πιο εξελιγμένες, η βελτιστοποίηση της λειτουργίας των διακοπτών αποτελεί ουσιαστικό βήμα προς τη δημιουργία ασφαλέστερων και πιο αποδοτικών δικτυακών υποδομών.

2.5 Access Points

Τα access points (σημεία πρόσβασης) σε πολύ γενικές γραμμές είναι συσκευές που επιτρέπουν τη σύνδεση ασύρματων συσκευών σε ένα ενσύρματο δίκτυο. Βέβαια αυτά τα κρίσιμα στοιχεία δικτυακής υποδομής δεν περιορίζονται απλώς στη μετάδοση σημάτων, αλλά πλέον πολύ συχνά ενσωματώνουν και προηγμένες λειτουργίες που ενισχύουν αποτελεσματικά την αποδοτικότητα και την ασφάλεια ενός δικτύου.

Στη σύγχρονη εποχή, τα access points υποστηρίζουν τεχνολογίες αιχμής όπως το MU-MIMO (Multi-User Multiple-Input Multiple-Output). Πιο συγκεκριμένα αυτή η τεχνολογία επιτρέπει τη διαχείριση ταυτόχρονων συνδέσεων για πολλαπλούς χρήστες, μειώνοντας τις καθυστερήσεις και αυξάνοντας τη χωρητικότητα του δικτύου, και αποτελεί μέρος του Quality of Service, δηλαδή την ποιοτική και ομαλή λειτουργία.

Επιπλέον, μια σημαντική επίσημανση που θα πρέπει να κάνουμε είναι ότι η υιοθέτηση προηγμένων πρωτοκόλλων όπως το 802.11ax (Wi-Fi 6) στα AP (Access Points) βρίσκεται παρόν και υπερτερεί στην τεχνολογία μας σήμερα και ενισχύει την ταχύτητα και την απόδοση σε περιβάλλοντα με υψηλή πυκνότητα χρηστών.

Εκτός από τον βασικό τους ρόλο στη διασύνδεση συσκευών, πολλά access points επίσης μπορούν να διαθέτουν ενσωματωμένες λειτουργίες ασφαλείας, όπως τα γνωστά

συστήματα Intrusion Prevention System (IPS) και Intrusion Detection System (IDS) για την αποτροπή των επιθέσεων.

Αυτά τα συστήματα παίζουν στην "πρώτη αμυντική γράμμη του μετώπου" του δικτύου πολλές φορές καθώς επιτρέπουν την ανίχνευση ύποπτων δραστηριοτήτων σε πραγματικό χρόνο και μπορούν να αντιδράσουν άμεσα σε πιθανές απειλές, αναλύοντας τα δεδομένα που διακινούνται στο δίκτυο αφήνοντας χρόνο στους αναλυτές να τα ερευνήσουν.

Σε περιβάλλοντα όπου η ασφάλεια αποτελεί προτεραιότητα, τα access points συνεργάζονται κυρίως με τεχνολογίες που μπορούν να ανιχνεύουν rogue access points (θα τα αναλύσουμε σε παρακάτω κεφάλαιο) και παρακολουθούν ασυνήθιστες MAC διευθύνσεις. Έτσι, εξασφαλίζεται ότι το δίκτυο παραμένει προστατευμένο από μη εξουσιοδοτημένες συνδέσεις και πιθανές επιθέσεις από κακόβουλους χρήστες.

Επιπλέον, τον τελευταίο καιρό και συγκεκριμένα τα τελευταία 5 χρόνια όλο και περισσότερες εταιρίες οδεύουν προς τον εικονικό κόσμο τον λεγόμενο "cloudικο" γιατί με την εξέλιξη των cloud-based συστημάτων διαχείρισης, οι διαχειριστές καταφέρνουν να ελέγχουν και να προσαρμόζουν το δίκτυο τους απομακρυσμένα, ενισχύοντας τόσο την αποτελεσματικότητα στην εργασία τους όσο και την ευελιξία της διαχείρισης αλλά και τέλος την ασφάλεια τους αφού ανα πάσα στιγμή μπορούν να έχουν πρόσβαση στο δίκτυο. Και όλα αυτά με τις κατάλληλες μετατροπές σε συσκευές AP του δικτύου μας, για να μας "φέρνουν" την κίνηση.
Περισσότερο στα της νέας γενιάς, τα access points δεν περιορίζονται πλέον μόνο στην παροχή σύνδεσης αλλά και με τη βοήθεια τεχνολογιών τεχνητής νοημοσύνης (AI) των τελευταίων καιρών, μπορούν να αναλύουν την κυκλοφορία δεδομένων και να προβλέπουν πιθανά προβλήματα πριν καν αυτά επηρεάσουν τη λειτουργία του δικτύου.

Έτσι λοιπόν συμβάλλουν στη δημιουργία έξυπνων, δυναμικών δικτύων που προσαρμόζονται στις ανάγκες των χρηστών, βελτιώνοντας συνολικά την απόδοση σε περιπτώσεις μεγάλου όγκου δικτύου και προπάντων την ασφάλεια.

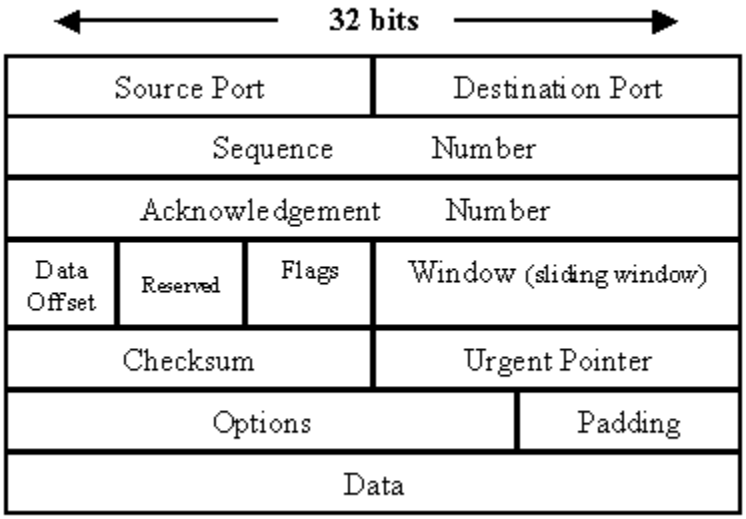
2.6 Δρομολόγηση Πακέτων

Η δρομολόγηση των πακέτων δεδομένων αποτελεί μια από τις πιο κρίσιμες λειτουργίες σε ένα δίκτυο που θα πρέπει να γνωρίζουν οι αναλυτές του και γενικότερα οι επαγγελματίες της κυβερνοασφάλειας. Είναι τόσο σημαντικά αφού κάθε πακέτο δεδομένων αντιπροσωπεύει μια μονάδα πληροφορίας που διακινείται από την πηγή προς τον προορισμό του, ακολουθώντας προκαθορισμένα μονοπάτια. Οι κανόνες δρομολόγηση του κάθε πακέτο ξεχωριστά εξαρτάται κυρίως από τους αλγόριθμους που βρίσκονται στους δρομολογητές του δικτύου που επιλέγουν τις βέλτιστες διαδρομές με βάση παράγοντες όπως η ταχύτητα, η αξιοπιστία και η ασφάλεια.

Όπως αναφέρθηκε ήδη τα ασύρματα δίκτυα βασίζονται, κυρίως, σε οικουμενικά πρωτόκολλα δρομολόγησης όπως το OSPF (Open Shortest Path First) και το BGP (Border Gateway Protocol) για δρομολογητές που είναι τοποθετημένοι στην “άκρη'' και συνδέουν το δίκτυο τους με την επόμενη περιοχή δικτύου, τα οποία διασφαλίζουν τη συνεχή επικοινωνία ακόμα και σε περιπτώσεις συμφόρησης ή αλλαγών στη δομή του δικτύου. Παράλληλα, η χρήση ασφαλών πρωτοκόλλων, όπως το IPsec, προστατεύει τα δεδομένα από υποκλοπές ή παραποιήσεις.

2.6.1 Packet Formation - Headers

Η κεφαλίδα (header) ενός πακέτου δεδομένων είναι το πιο σημαντικό τμήμα για τη δρομολόγηση και την ανάλυση της ασφάλειας. Περιλαμβάνει πληροφορίες που χρησιμοποιούνται από τις συσκευές δικτύου για την επεξεργασία και τη διαβίβαση του πακέτου. Επίσης θα αναφερθούμε σε μερικά παραδείγματα για την καλύτερη κατανόηση. Τα βασικά πεδία μιας κεφαλίδας περιλαμβάνουν:



Εικόνα 1: TCP/IP Packet Headers

Πεδίο Προέλευσης και Προορισμού: Περιέχει τις διευθύνσεις IP του αποστολέα (source IP address) και του παραλήπτη (destination IP address). Το πεδίο αυτό είναι ζωτικής σημασίας για τη σωστή δρομολόγηση του πακέτου, και η ανάλυσή του απαιτεί ιδιαίτερη προσοχή. Όσο περισσότερο εμβαθύνουμε στην ανάλυση οποιουδήποτε συστήματος και προσεγγίζουμε τα θεμέλια της υποδομής και της αρχιτεκτονικής του όπως συμβαίνει στην περίπτωση των δικτυακών πακέτων τόσο πιο αναγκαίο γίνεται να εξετάζουμε προσεκτικά όλους τους εμπλεκόμενους παράγοντες και να υιοθετούμε μια πιο αυστηρή προσέγγιση μηδενικής εμπιστοσύνης (zero-trust).

Πρωτόκολλο: Καθορίζει το ανώτερο πρωτόκολλο που χρησιμοποιείται, όπως το TCP (Transmission Control Protocol) ή το UDP (User Datagram Protocol). Το πεδίο αυτό επιτρέπει την αναγνώριση της φύσης των δεδομένων.

Σημαία (Flag): Περιγράφει ειδικές οδηγίες για το πακέτο, όπως η αναγκαιότητα κατακερματισμού το "hash" δηλαδη στα αγγλικα ή επανασυναρμολόγησης.

Checksum: Παρέχει μηχανισμούς ανίχνευσης σφαλμάτων, διασφαλίζοντας την ακεραιότητα του πακέτου κατά τη μετάδοση.

Όπως ήδη ανάφεραμε και πιο πάω η ανάλυση των headers είναι κρίσιμη αλλά μπορεί να εκμεταλευτεί και για την ανάπτυξη ενός WIDS (Wireless Intrusion Detection System). Μέσα από τα headers μπορούν να εντοπιστούν ανωμαλίες, όπως:

Ύποπτες IP διευθύνσεις ή μη αναγνωρίσιμες πηγές δεδομένων.

Πακέτα με μη αναμενόμενα flags που μπορεί να υποδεικνύουν επιθέσεις (π.χ., SYN floods).

Χρονικός Ζωής (Time-to-Live - TTL): Καθορίζει τον μέγιστο αριθμό hops (ενδιάμεσων συσκευών) που μπορεί να διανύσει το πακέτο πριν απορριφθεί. Αυτό προστατεύει το δίκτυο από αέναη κυκλοφορία δεδομένων. Αναλυτικά η μέτρηση του ξεκινάει με τη μέγιστη τιμή του να αφαιρείται κατα 1 αναπήδηση κόμβου τη φορά.

Επίσης είναι πολύ σημαντικό να αναφέρουμε ότι οι επιθέσεις απενάντι Time-to-Live (TTL) χρησιμοποιούνται κυρίως ως μέσο αποφυγής εντοπισμού από επιτιθέμενους. Συγκεκριμένα, ο επιτιθέμενος ρυθμίζει σκόπιμα μια πολύ χαμηλή τιμή TTL στα IP πακέτα του, προκειμένου να παρακάμψει συστήματα όπως τα firewalls, τα IDS (Intrusion Detection Systems) και τα IPS (Intrusion Prevention Systems). Αυτή η τεχνική λειτουργεί ως εξής:

Ο επιτιθέμενος δημιουργεί ένα IP πακέτο με σκόπιμα χαμηλή τιμή TTL (π.χ. 1, 2, 3 κ.λπ.).

Καθώς το πακέτο περνά από κάθε host στη διαδρομή του, η τιμή TTL μειώνεται κατά ένα, μέχρι να φτάσει στο μηδέν.

Όταν η τιμή φτάσει στο μηδέν, το πακέτο απορρίπτεται.

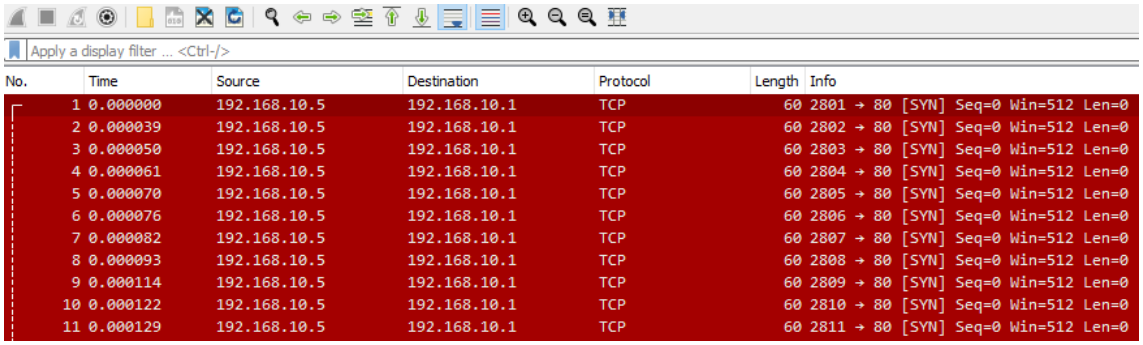
Ο επιτιθέμενος επιδιώκει να απορριφθεί το πακέτο πριν φτάσει σε ένα firewall ή σε ένα σύστημα φιλτραρίσματος, ώστε να αποφύγει τον εντοπισμό.

Όταν τα πακέτα λήγουν, οι δρομολογητές στη διαδρομή παράγουν μηνύματα ICMP "Time Exceeded" και τα στέλνουν πίσω στη διεύθυνση IP προέλευσης.

Για να ξεκινήσουμε, μπορούμε να συλλέξουμε την κυκλοφορία μας και να την αναλύσουμε με το γνωστό εργαλείο ανάλυσης δικτύου το Wireshark.

Ο εντοπισμός τέτοιων πακέτων σε μικρές ποσότητες μπορεί να είναι δύσκολος, αλλά ευτυχώς, οι επιτιθέμενοι χρησιμοποιούν συχνά την παραποίηση TTL σε προσπάθειες σάρωσης θυρών. Κατά την ανάλυση, μπορεί να παρατηρήσουμε κάτι όπως:

IP TTL 1



Εικόνα 2: From Wireshark analysis

Ένα πακέτο με εξαιρετικά χαμηλή τιμή TTL, πιθανώς προϊόν παραποίησης καθώς τα πρότυπα μέσω των κανόνων σχεδόν ποτέ δεν μετατρέπουν συχνα την τιμή αυτή.

Αλλά για να δούμε πως θα μπορύσαμε να αντιμετωπίσουμε αυτον τον τρόπο επίθεσης.

Για να αντιμετωπιστεί αυτή η μορφή επίθεσης, αρχικά μπορούμε να εφαρμόσουμε ένα σύστημα ελέγχου που απορρίπτει ή να φιλτράρει πακέτα με πολύ χαμηλή τιμή TTL, και τοποθετώντας το ακριβώς στον εξωτερικό δρομολογητή στην αρχιτεκτονική του δικτύου μας από την πλευρά που εισέρχεται η κίνηση από άλλα δίκτυα. Με αυτόν τον τρόπο, μπορούμε να αποτρέψουμε τέτοιες μορφές επιθέσεων παραποίησης IP πακέτων. Στην ουσία δεν εισέρχοντε πακέτα στο δίκτυο μας που δεν καλύπτουν τις προυποθέσεις που ορίσαμε. Αυτοί οι κανόνες δημιουργούντε κύριως για αυτό τον σκοπό και είναι γνωστοί και ως ACL ή Access Control Lists.

Επιπλέον, η συλλογή δεδομένων από τις κεφαλίδες μπορεί να βοηθήσει στην εκπαίδευση μοντέλων μηχανικής μάθησης, που θα είναι σε θέση να αναγνωρίζουν μοτίβα κακόβουλης δραστηριότητας με υψηλή ακρίβεια.

Το Κεφάλαιο 2 παρέχει τις απαραίτητες βάσεις για την κατανόηση των τεχνολογιών δικτύωσης, δίνοντας έμφαση στις συσκευές, τα πρωτόκολλα και τις λειτουργίες που σχετίζονται με την ασύρματη επικοινωνία. Η εις βάθος κατανόηση αυτών των εννοιών μπορεί να γίνει εύκολα καθοριστική για την ανάπτυξη ενός συστήματος ανίχνευσης εισβολών που βασίζεται στη μηχανική μάθηση.

3 Πρωτόκολλα Ασύρματου Μέσου

Η κατανόηση των πρωτοκόλλων ασύρματου μέσου αποτελεί ακρογωνιαίο λίθο για τη μελέτη και την εφαρμογή ασύρματων δικτύων, ειδικά όσον αφορά την ασφάλεια και την αποδοτικότητα. Τα πρωτόκολλα λειτουργούν σαν κανόνες αφού καθορίζουν πώς μεταδίδονται τα δεδομένα μέσω του ασύρματου καναλιού, εξασφαλίζοντας τη συμβατότητα, την ταχύτητα και την αξιοπιστία της επικοινωνίας. Οι εξελίξεις στις τεχνολογίες αυτές έχουν οδηγήσει άμεσα σε πρωτόκολλα που προάγουν όχι μόνο την απόδοση αλλά και την ασφάλεια, εξυπηρετώντας τις σύγχρονες ανάγκες δικτύωσης.

3.1 Τεχνολογίες Wi-Fi

Οι τεχνολογίες Wi-Fi αποτελούν τη βάση της ασύρματης δικτύωσης, προσφέροντας ταχύτητα και ευελιξία στη σύνδεση συσκευών. Οι εξελίξεις στις τεχνολογίες αυτές έχουν οδηγήσει σε διαδοχικές γενιές προτύπων, καθεμία από τις οποίες εισάγει σημαντικές βελτιώσεις.

3.1.1 Wi-Fi 2.4 GHz

Το Wi-Fi στη συχνότητα των 2.4 GHz αποτελεί ένα από τα παλαιότερα και πιο διαδεδομένα πρότυπα, υποστηρίζοντας πρότυπα όπως το 802.11b, το 802.11g και το 802.11n. Η λειτουργία του βασίζεται στη χρήση 14 καναλιών, από τα οποία τα περισσότερα επικαλύπτονται, γεγονός που περιορίζει την αποδοτικότητα σε περιβάλλοντα με μεγάλη πυκνότητα δικτύων, άρα πολύ γρήγορα συναντάμε περιορισμούς για τις ανάγκες της εποχής μας. Η συχνότητα αυτή διακρίνεται για τη μεγάλη εμβέλειά της, καθιστώντας την κατάλληλη για εφαρμογές όπου η απόσταση έχει μεγαλύτερη σημασία από την ταχύτητα, αν και η απόδοσή της επηρεάζεται έντονα από παρεμβολές που προέρχονται από άλλες συσκευές, όπως φούρνοι μικροκυμάτων και Bluetooth.

Ένα από τα βασικά προβλήματα του Wi-Fi 2.4 GHz είναι η ευπάθεια στα κανάλια επικάλυψης, κάτι που αυξάνει τον κίνδυνο παρεμβολών και επιθέσεων τύπου jamming(θα αναλυθεί σε παρακάτω κεφάλαιο). Οι συσκευές που λειτουργούν με αυτό το φάσμα είναι επίσης συχνά παγιδευμένες σε παλαιότερα και λιγότερο ασφαλή πρωτόκολλα, όπως το WEP, το οποίο μπορεί εύκολα να παραβιαστεί μέσω επιθέσεων λόγω αρκετά ασθενής κρυπτογράφησης. Επιπλέον, επιθέσεις παρακολούθησης πακέτων (packet sniffing) είναι συχνές, καθώς η βασική κρυπτογράφηση των δεδομένων είναι συχνά ανεπαρκής. Τα παλαιότερα συστήματα κρυπτογράφησης, όπως το WPA, παραμένουν ευάλωτα σε επιθέσεις τύπου KRACK (Key Reinstallation Attack), ενώ η γενική ευπάθεια στη συχνότητα αυτή αυξάνεται από την ευρεία χρήση μη ασφαλών δικτύων.

3.1.2 Wi-Fi 5 GHz

Έτσι λοιπόν δημιουργήθηκε η ανάγκη για το Wi-Fi στη συχνότητα των 5 GHz το οποίο εισήγαγε βελτιώσεις στις ταχύτητες και τη συνολική απόδοση των δικτύων, υποστηρίζοντας πρότυπα όπως το 802.11n και το 802.11ac. Το φάσμα αυτής της αυξημένης συχνότητας των 5 GHz προσφέρει περισσότερα μη επικαλυπτόμενα κανάλια, γεγονός που μειώνει τις παρεμβολές και επιτρέπει μεγαλύτερη χωρητικότητα δεδομένων. Σε σύγκριση με το 2.4 GHz, η συχνότητα αυτή παρέχει ταχύτερες συνδέσεις, αν και η εμβέλειά της είναι μικρότερη λόγω της φύσης του υψηλότερου φάσματος. Άρα πολύ συνοπτικά το 2.4GHz είναι προτιμότερο να επιλέγεται όταν η συνδεδεμένη συσκευή βρίσκεται σχετικά μακρύτερα των 7~10 μέτρων με κόστος τις μικρότερες ταχύτητες και η συχνότητα 5GHz όταν βρίσκεται σχετικά κοντά και φυσικά να μην υπάρχουν εμπόδια όπως τοίχοι οι οποίοι θα ρίξουν την ισχύ.

Ωστόσο, η τεχνολογία των 5 GHz δεν είναι χωρίς προβλήματα. Ενώ η μειωμένη επικάλυψη των καναλιών μειώνει τις τυχαίες παρεμβολές, τα δίκτυα αυτά είναι ευάλωτα σε στοχευμένες επιθέσεις jamming. Οι συσκευές που βασίζονται στο Wi-Fi 5 GHz παραμένουν επίσης εκτεθειμένες σε επιθέσεις τύπου evil twin, όπου ένας κακόβουλος δρομολογητής προσποιείται ότι είναι νόμιμος, εξαπατώντας τους χρήστες ώστε να συνδεθούν. Τα προβλήματα αυτά επιδεινώνονται από την εξάρτηση του πρωτοκόλλου

WPA2, το οποίο, παρά την ισχυρή του κρυπτογράφηση, είναι ευάλωτο σε συγκεκριμένες επιθέσεις αποκρυπτογράφησης όταν ο επιτιθέμενος καταφέρει να υποκλέψει αρχικές ανταλλαγές κλειδιών.

3.1.3 Wi-Fi 6/6E

Το Wi-Fi 6, γνωστό και ως 802.11ax, και η επέκτασή του Wi-Fi 6E, που προσθέτει λειτουργία στο φάσμα των 6 GHz, αντιπροσωπεύουν σημαντική πρόοδο στην απόδοση των δικτύων Wi-Fi. Η τεχνολογία αυτή εισάγει μηχανισμούς όπως η ορθογώνια πολλαπλή πρόσβαση διαίρεσης συχνότητας (OFDMA) και η τεχνολογία πολλαπλών χρηστών MIMO (MU-MIMO), επιτρέποντας την ταυτόχρονη εξυπηρέτηση πολλών συσκευών με υψηλές ταχύτητες. Η δυνατότητα λειτουργίας σε φάσμα 6 GHz μέσω του Wi-Fi 6E αυξάνει δραματικά τη διαθέσιμη χωρητικότητα δεδομένων, μειώνοντας σημαντικά την κυκλοφοριακή συμφόρηση σε πυκνοκατοικημένα περιβάλλοντα.

Παρά τα οφέλη αυτά, όλα θα έχουν τις αδυναμίες τους έτσι και το Wi-Fi 6/6E παραμένει ευάλωτο σε κακόβουλες ενέργειες. Οι επιθέσεις τύπου deauthentication παραμένουν απειλή, καθώς οι επιτιθέμενοι μπορούν να διακόψουν τη σύνδεση μιας συσκευής, αναγκάζοντάς την να επανασυνδεθεί και να στείλει ξανά ευαίσθητα δεδομένα. Επιπλέον, οι υψηλότερες ταχύτητες και η μεγαλύτερη χωρητικότητα μπορούν να γίνουν στόχος επιθέσεων Man-in-the-Middle (MITM), όπου ο επιτιθέμενος αποκτά πρόσβαση σε ευαίσθητα δεδομένα, εκμεταλλευόμενος αδυναμίες στην ασύρματη μετάδοση.

3.1.4 Wi-Fi 7 - 802.11be

Το WiFi 7 (αναμενόμενο να παρουσιαστεί το 2024), γνωστό και ως IEEE 802.11be - Extremely High Throughput (EHT), αποτελεί την πιο πρόσφατη καινοτομία στις τεχνολογίες ασύρματης δικτύωσης, σχεδιασμένη να προσφέρει εξαιρετικά υψηλές ταχύτητες και βελτιωμένη απόδοση. Σε αντίθεση με τις προηγούμενες γενιές, το WiFi 7 αξιοποιεί ταυτόχρονα και τις τρεις συχνότητες λειτουργίας – 2.4 GHz, 5 GHz και 6 GHz – επιτρέποντας την πλήρη εκμετάλλευση του διαθέσιμου φάσματος. Ενώ το WiFi 6 αναπτύχθηκε κυρίως για να αντιμετωπίσει τη ραγδαία αύξηση του αριθμού των συνδεδεμένων συσκευών, ο πρωταρχικός στόχος του WiFi 7 είναι η παροχή εκπληκτικών

ταχυτήτων και υψηλής απόδοσης, μειώνοντας προβλήματα όπως η καθυστέρηση, η προσωρινή αποθήκευση (buffering) και η συμφόρηση του δικτύου.

Η τεχνολογία WiFi 7 είναι σίγουρα τεχνολογία αιχμής στο κόσμο αυτή την στιγμή και εισάγει σημαντικές βελτιώσεις, όπως το εξαιρετικά ευρύ φάσμα ζώνης 320 MHz, την προηγμένη διαμόρφωση σήματος 4096-QAM, την τεχνική Multi-RU και τη δυνατότητα Multi-Link Operation (MLO), που συνδυαστικά επιτυγχάνουν ταχύτητες έως και 4.8 φορές υψηλότερες σε σχέση με το WiFi 6 και 13 φορές ταχύτερες από το WiFi 5. Αν και το WiFi 6 πρόσφερε περίπου 37% αύξηση στην ταχύτητα συγκριτικά με το WiFi 5, η βελτίωση αυτή δεν ήταν τόσο δραματική όσο η δεκαπλάσια αύξηση που είχε επιφέρει η μετάβαση από το WiFi 4 στο WiFi 5. Αυτό οφείλεται στο γεγονός ότι το WiFi 6 είχε σχεδιαστεί πρωτίστως για να βελτιώσει την αποδοτικότητα του δικτύου και όχι απλώς τον ρυθμό μετάδοσης δεδομένων. Αντιθέτως, το WiFi 7 εστιάζει στην απόδοση και στις υψηλότερες ταχύτητες, καθιστώντας το ιδανικό για εφαρμογές που απαιτούν υπερταχείες συνδέσεις, όπως το cloud gaming, η εικονική και επαυξημένη πραγματικότητα (VR/AR) και η ροή περιεχομένου σε ανάλυση 8K.

Με τις προηγμένες δυνατότητές του, το WiFi 7 προσφέρει έως και 480% καλύτερη απόδοση σε σύγκριση με τις προηγούμενες γενιές, καθιστώντας το ένα τεράστιο άλμα στην τεχνολογία ασύρματης σύνδεσης. Παράλληλα, διατηρεί συμβατότητα με τις παλαιότερες εκδόσεις WiFi, επιτρέποντας στους χρήστες να αναβαθμίσουν σταδιακά τις συσκευές τους χωρίς να θυσιάζουν τη συνδεσιμότητα. Με έναν δρομολογητή WiFi 7, σε ένα οικιακό δίκτυο μπορεί να προσφέρει ασύγκριτες ταχύτητες και σταθερότητα, επιτρέποντας την ομαλή εκτέλεση ακόμα και των πιο απαιτητικών διαδικτυακών εφαρμογών. Είναι εμφανές πως για να καλυφθεί πλήρως το WiFi 7 χρειάζεται το δικό του κεφάλαιο, όμως η εως τώρα αναφορά του είναι αρκετή για εμάς.

3.1.5 Wi-Fi 8 - 802.11bn

Το Wi-Fi 8 βρίσκεται ακόμα στο στάδιο της ανάπτυξης του από τους ερευνητές του, αλλά είναι βέβαια και στο μέλλον θα είναι αναγκαίο να φέρει ακόμα μεγαλύτερες εξελίξεις στον τομέα των ασύρματων επικοινωνιών. Αυτή η συναρπαστική μελλοντική νέα

τεχνολογία αναμένεται να ενσωματώσει αυξημένο εύρος ζώνης, υποστηρίζοντας συχνότητες άνω των 6 GHz, ώστε να εξασφαλίζεται μεγαλύτερη ταχύτητα και να ελαχιστοποιούνται οι παρεμβολές. Παράλληλα, υπόσχεται ότι θα ενσωματώσει προηγμένα συστήματα διαχείρισης με τη βοήθεια τεχνητής νοημοσύνης (AI), επιτρέποντας την αυτόματη βελτιστοποίηση της απόδοσης του δικτύου ανάλογα με τις απαιτήσεις. Στα σχέδια είναι επίσης να είναι απόλυτα συμβατό με μελλοντικές τεχνολογίες, εξυπηρετώντας εφαρμογές έξυπνων πόλεων και εξελιγμένων IoT συστημάτων.

Από την αυξημένη εμβέλεια και ευκολία πρόσβασης του Wi-Fi 2.4 GHz μέχρι την αξιοποίηση πολυζωνικών λειτουργιών στο Wi-Fi 7, η τεχνολογία Wi-Fi προσαρμόζεται διαρκώς στις ανάγκες τόσο των χρηστών όσο και των σύγχρονων εφαρμογών. Με την είσοδο της τεχνητής νοημοσύνης και της αυξημένης ευρυζωνικότητας στις μελλοντικές εκδόσεις, η δυναμική των ασύρματων δικτύων υπόσχεται να ανοίξει νέους ορίζοντες στην επικοινωνία, την παραγωγικότητα και την ανάπτυξη έξυπνων συστημάτων.

Είναι προφανές πως η συνεχής βελτίωση της τεχνολογίας Wi-Fi δεν καλύπτει μόνο τις τρέχουσες ανάγκες, αλλά διαμορφώνει και το μέλλον της ασύρματης συνδεσιμότητας. Η επερχόμενη γενιά Wi-Fi 8 αναμένεται να αποτελέσει το θεμέλιο για πιο εξελιγμένα και αποδοτικά δίκτυα, διασφαλίζοντας ότι οι χρήστες και οι συσκευές παραμένουν συνδεδεμένοι, αποδοτικοί και ασφαλείς σε ένα ταχύτατα εξελισσόμενο τεχνολογικό περιβάλλον.

3.2 Bluetooth

Το Bluetooth αποτέλεσε τελικά απόλυτα σημαντική εφεύρεση για τη ευελιξία στην καθημερινότητα μας αφού αποτελεί μια ασύρματη τεχνολογία επικοινωνίας μικρής εμβέλειας που επιτρέπει τη σύνδεση και ανταλλαγή δεδομένων μεταξύ ηλεκτρονικών συσκευών.

Αρχικά σχεδιάστηκε και αναπτύχθηκε από την Bluetooth Special Interest Group (SIG) το 1998 και έχει εξελιχθεί μέσα από διάφορες εκδόσεις, με κάθε νέα αναβάθμιση να

προσφέρει βελτιωμένη ταχύτητα, εμβέλεια και ασφάλεια. Ωστόσο, παρά τις βελτιώσεις, το Bluetooth συνεχίζει να αποτελεί στόχο επιθέσεων μέχρι και σήμερα, λόγω της εκτεταμένης χρήσης του σε συσκευές χαμηλής ισχύος, όπως κινητά τηλέφωνα, έξυπνα ρολόγια, ασύρματα ακουστικά, IoT συσκευές και συστήματα αυτοκινήτων.

Κατά καιρούς έχουν υπάρξει αρκετές αξιόπιστες έρευνες έχουν ερευνήσει την ασφάλεια του οπως :

- " Investigating Bluetooth Vulnerabilities to Defend from Attacks"

Αυτή η μελέτη δημοσιεύθηκε στο “2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)” και παρέχει μια εκτενή ανασκόπηση των γνωστών απειλών ασφάλειας στο πρωτόκολλο Bluetooth. Περιληπτικά η έρευνα αναλύει ευπάθειες που μπορούν να εκμεταλευτούν με διάφορους τρόπους, οδηγώντας σε σοβαρή απώλεια δεδομένων. Στις περισσότερες περιπτώσεις, οι επιτιθέμενοι χρησιμοποιούν τεχνικές όπως επιθέσεις άρνησης υπηρεσίας (Denial of Service - DoS), υποκλοπή επικοινωνιών, κακόβουλη εκμετάλλευση πόρων και τροποποίηση μηνυμάτων. Όλες αυτές οι επιθέσεις θέτουν σε κίνδυνο την ασφάλεια των δεδομένων των χρηστών, επιτρέποντας την αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες σύμφωνα με την έρευνα. Περισσότερα για τις επιθέσεις θα αναλύσουμε και εμείς παρακάτω.

Επίσης αναφέρετε και η πειραματική αξιολόγηση που πραγματοποιήθηκε στη συγκεκριμένη μελέτη, χρησιμοποιήθηκε η πλατφόρμα Kali Linux σε συνδυασμό με εργαλεία τρίτων κατασκευαστών, με σκοπό τη δοκιμή τεσσάρων μεθόδων επίθεσης Bluetooth: Bluejacking, Bluesmacking, Bluesnarfing και Social Engineering. Οι επιθέσεις εφαρμόστηκαν σε τρεις διαφορετικές συσκευές Bluetooth: ένα ηχείο HMDX Jam, ένα iPhone 6 και ένα Nexus 7.

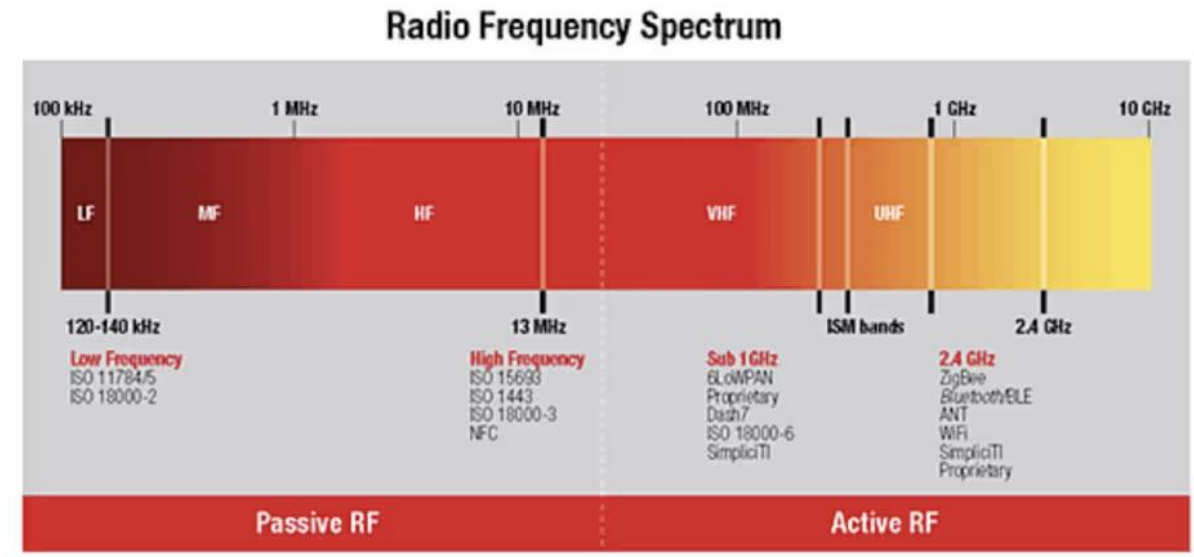
Τα αποτελέσματα της έρευνας έδειξαν ότι οι χάκερ μπορούν να εκτελέσουν αυτές τις επιθέσεις με σχετικά χαμηλό επίπεδο δυσκολίας, θέτοντας έτσι σε μεγάλο κίνδυνο την ασφάλεια του συστήματος-δικτύου και την ακεραιότητα των δεδομένων.

Παράλληλα, η μελέτη εξέτασε πώς οι χρήστες μπορούν να εφαρμόσουν διάφορα πρωτόκολλα ασφαλείας για να προστατεύσουν τις συσκευές τους και να μειώσουν τον κίνδυνο εισβολών από κακόβουλους παράγοντες.

Μια από τις αρχές μας ως ερευνητές ασφάλειας ασύρματων δικτύων και τεχνολογιών είναι ότι θα πρέπει να νιώθουμε στο μέγιστο σίγουροι ότι γνωρίζουμε εις βάθος την αρχιτεκτονική του δίκτυο μας. Έτσι για την πλήρη και σωστή κατανόηση της τεχνολογίας του bluetooth στο επόμενο κεφάλαιο θα αναφερθούμε στη αρχιτεκτονική και στα θεμέλια της λειτουργίας για να αντιληφθούμε καλύτερα τον τρόπο που επικοινωνούν οι συσκευές.

3.2.1 Αρχιτεκτονική και λειτουργία

Σε μεγάλη ανάλυση θα παρατηρήσουμε οτι το Bluetooth λειτουργεί σε ένα φάσμα συχνοτήτων 2402 MHz έως 2480 MHz, το οποίο είναι σημαντικά χαμηλότερο από τις συχνότητες που μπορεί να αντιληφθεί το ανθρώπινο μάτι. Συγκεκριμένα, το ορατό φάσμα του φωτός κυμαίνεται από περίπου 400 nm έως 700 nm, με τις υψηλότερες συχνότητες να αντιστοιχούν σε σκούρες αποχρώσεις του μπλε-μωβ, ενώ οι χαμηλότερες σε βαθύ κόκκινο.



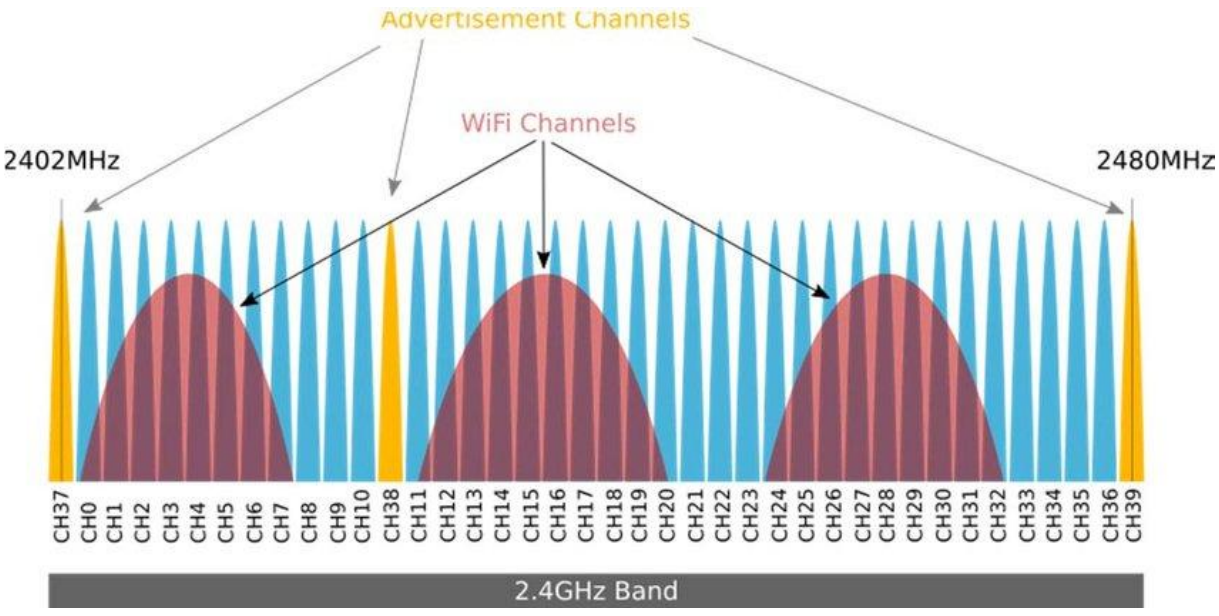
Εικόνα 3: Εύρος συχνοτήτων

Οι ασύρματες τεχνολογίες, συμπεριλαμβανομένου του Bluetooth, λειτουργούν σε μήκη κύματος της τάξης των 123 mm, τα οποία ανήκουν στο ραδιοφωνικό φάσμα και

βρίσκονται πολύ δεξιότερα στο ηλεκτρομαγνητικό φάσμα σε σχέση με το ορατό φως. Δεδομένου ότι αυτά τα κύματα έχουν μεγαλύτερο μήκος κύματος και χαμηλότερη συχνότητα, δεν είναι αντιληπτά από το ανθρώπινο μάτι και παρουσιάζουν διαφορετικές φυσικές ιδιότητες από τις οπτικές ακτινοβολίες, όπως η δυνατότητα διάδοσης μέσω εμποδίων (π.χ. τοίχοι, έπιπλα) σε αντίθεση με το φως που ανακλάται ή απορροφάται.

Ο συγκεκριμένος εύρος συχνοτήτων επιλέχθηκε σκόπιμα για την ανάπτυξη ασύρματων επικοινωνιών, καθώς εξασφαλίζει ικανοποιητική εμβέλεια, χαμηλή κατανάλωση ενέργειας και ελάχιστη αλληλεπίδραση με άλλες ηλεκτρομαγνητικές ακτινοβολίες. Παράλληλα, η ένταση της εκπεμπόμενης ακτινοβολίας είναι ιδιαιτέρως χαμηλή και θεωρείται ακίνδυνη για τον άνθρωπο, γεγονός που καταρρίπτει συχνές παρερμηνείες σχετικά με τις πιθανές επιπτώσεις της αυξημένης συχνότητας στην ανθρώπινη υγεία.

Στην παρακάτω εικόνα παρουσιάζεται το εύρος του φάσματος των 2.4 GHz, τα κανάλια, το οποίο χρησιμοποιείται όχι μόνο από το Bluetooth, αλλά και από άλλες ασύρματες τεχνολογίες, όπως το Wi-Fi.



Εικόνα 4: Το Εύρος Συχνοτήτων στα 2.4GHz

Ας δώσουμε μια πιο ξεκάθαρη εικόνα όμως για τις διάφορες τους σε παρακάτω ενότητα.

Πως λοιπόν γίνεται επιτυχής η ανταλλαγή δεδομένων με την χρήση του Bluetooth;

Η ανταλλαγή δεδομένων μεταξύ δύο συσκευών που χρησιμοποιούν Bluetooth ή Bluetooth Low Energy (BLE) βασίζεται στην κωδικοποίηση δυαδικών ψηφίων (0 και 1) μέσω διαφορών στο μήκος κύματος της εκπεμπόμενης ηλεκτρομαγνητικής ακτινοβολίας.

Πολύ απλά, η συσκευή που επιθυμεί να μεταδώσει δεδομένα χρησιμοποιεί είτε

- Μήκος κύματος 121 mm για την αναπαράσταση του δυαδικού ψηφίου "1", είτε το,
- Μήκος κύματος 124 mm για την αναπαράσταση του δυαδικού ψηφίου "0".

Αυτή η διαφοροποίηση των συχνοτήτων επιτρέπει στη συσκευή λήψης να αποδιαμορφώσει το σήμα και να αναγνωρίσει τα μεταδιδόμενα δεδομένα. Η τεχνική αυτή αποτελεί βασικό μηχανισμό λειτουργίας του BLE, καθώς εξασφαλίζει αξιόπιστη και ενεργειακά αποδοτική επικοινωνία μεταξύ συσκευών, μειώνοντας τις παρεμβολές και την κατανάλωση ισχύος.

Οι σύγχρονες ασύρματες επικοινωνίες, όπως αυτές που πραγματοποιούνται μέσω των κινητών τηλεφώνων, βασίζονται στη μετάδοση δεδομένων μέσω ηλεκτρομαγνητικών κυμάτων. Οι κεραίες που λειτουργούν ως πομποί και δέκτες μεταδίδουν πληροφορίες χρησιμοποιώντας τη δυαδική κωδικοποίηση των ψηφίων "0" και "1", με εξαιρετικά υψηλή ταχύτητα εναλλαγής. Η μετάδοση αυτή επιτυγχάνεται μέσω ταχείας μεταβολής της συχνότητας ή του πλάτους του ηλεκτρομαγνητικού κύματος, μια διαδικασία που λαμβάνει χώρα σχεδόν ακαριαία.

Συγκεκριμένα, η εναλλαγή μεταξύ των δυαδικών καταστάσεων πραγματοποιείται σε χρονικό διάστημα της τάξης του 1 μικροδευτερολέπτου (1 μs ή 0.000001 δευτερολέπτων), γεγονός που επιτρέπει τη γρήγορη και αξιόπιστη μετάδοση δεδομένων, όπως φωνητικές κλήσεις, βίντεο και διαδικτυακή επικοινωνία, χωρίς αισθητή καθυστέρηση για τον χρήστη. Η περαιτέρω ανάλυση των μηχανισμών διαμόρφωσης και της τεχνολογίας πίσω από αυτή τη διαδικασία θα μπορούσε να αποτελέσει αντικείμενο ξεχωριστής μελέτης. Ωστόσο, στο πλαίσιο της παρούσας εργασίας, η εμβάθυνση σε τέτοιες τεχνικές λεπτομέρειες δεν κρίνεται τόσο αναγκαία, καθώς η εστίαση παραμένει στην ασφάλεια και την αποτελεσματικότητα των ασύρματων τεχνολογιών. Η εμβάθυνση έγινε για να δείξουμε το βαθμό που θα πρέπει να γνωρίζουμε τις τεχνολογίες στο δίκτυο

μας για είμαστε σε θέση να θέτουμε σωστά τα πλαίσια και τους κανόνες ασφάλειας και ακεραιότητας σε κάθε σημείο του δικτύου μας. Ας δώσουμε μια πιο ξεκάθαρη εικόνα όμως για τις διάφορες τους σε παρακάτω ενότητα.

3.2.2 Bluetooth και Wi-Fi: Διαφορές στις Τεχνικές Μετάδοσης

Αυτήν την στιγμή είναι οι δύο κυρίαρχες τεχνολογίες ασύρματης επικοινωνίας μικρής και μεσαίας εμβέλειας, το Bluetooth και το Wi-Fi. Μπορούν να λειτουργούν στην ίδια ζώνη συχνοτήτων των 2.4 GHz, ωστόσο παρουσιάζουν σημαντικές διαφορές ως προς τον τρόπο μετάδοσης, την κατανάλωση ενέργειας και τη συνολική απόδοσή τους.

Το Bluetooth βασίζεται στη μέθοδο Frequency Hopping Spread Spectrum (FHSS), όπου το σήμα μεταδίδεται σε κανάλια εύρους 1 MHz, πραγματοποιώντας 1.600 αλλαγές συχνότητας το δευτερόλεπτο ανάμεσα σε 79 διαφορετικά κανάλια. Αυτή η προσέγγιση μειώνει τον κίνδυνο παρεμβολών και βελτιώνει την ασφάλεια της επικοινωνίας, καθώς δυσκολεύει την παγίδευση των δεδομένων από κακόβουλους χρήστες.

Αντίθετα, το Wi-Fi χρησιμοποιεί είτε τη μέθοδο Direct Sequence Spread Spectrum (DSSS) είτε την Orthogonal Frequency Division Multiplexing (OFDM), ανάλογα με το πρότυπο που έχει οριστεί από τους μηχανικούς για το δίκτυο. Οι τεχνικές αυτές επιτρέπουν τη μετάδοση μεγάλου όγκου δεδομένων σε σταθερά κανάλια εύρους 20-80 MHz, προσφέροντας υψηλότερες ταχύτητες και σταθερότητα στη σύνδεση, κάτι που καθιστά το Wi-Fi κατάλληλο για εφαρμογές υψηλών απαιτήσεων, όπως η ροή βίντεο και η περιήγηση στο διαδίκτυο.

3.2.3 Εμβέλεια και Κατανάλωση Ενέργειας

Η σχεδιαστική φιλοσοφία των δύο τεχνολογιών αντανακλάται και στη διαφορετική εμβέλεια και κατανάλωση ενέργειας που μπορούν να προσφέρουν:

Συγκεκριμένα το Bluetooth έχει σχεδιαστεί για επικοινωνία μικρών αποστάσεων, συνήθως έως 10 μέτρα, και δίνει έμφαση στη χαμηλή κατανάλωση ενέργειας, γεγονός που το καθιστά ιδανικό για φορητές συσκευές και IoT εφαρμογές.

Το Wi-Fi, αντίθετα, υποστηρίζει μεγαλύτερη εμβέλεια (έως και 100 μέτρα) και υψηλότερες ταχύτητες μετάδοσης δεδομένων. Ωστόσο, η αυξημένη απόδοσή του συνεπάγεται πολύ λογικά με τη μεγαλύτερη κατανάλωση ενέργειας, κάτι που το καθιστά πιο κατάλληλο για σταθερές συσκευές με μόνιμη παροχή ρεύματος.

Σύμφωνα με μελέτες της Texas Instruments, η συνύπαρξη Bluetooth και Wi-Fi στο ίδιο φάσμα μπορεί να οδηγήσει σε παρεμβολές, λόγω των διαφορετικών μεθόδων μετάδοσης που χρησιμοποιούν. Η κατανόηση αυτών των διαφορών είναι κρίσιμη για τον σχεδιασμό αποδοτικών και ασφαλών ασύρματων δικτύων.

3.2.4 Εξέλιξη και Ασφάλεια και Συμπεράσματα

Η τεχνολογία Bluetooth έχει εξελιχθεί σημαντικά τα τελευταία χρόνια, προσφέροντας βελτιώσεις τόσο στην ταχύτητα μετάδοσης όσο και στην ασφάλεια των επικοινωνιών. Καθώς το Bluetooth βελτιώθηκε με την πάροδο του χρόνου, ενσωμάτωσε μηχανισμούς ασφαλείας όπως το Secure Simple Pairing (SSP) και ισχυρότερους αλγορίθμους κρυπτογράφησης. Ωστόσο, πολλές συσκευές εξακολουθούν να χρησιμοποιούν παλαιότερες εκδόσεις του πρωτοκόλλου, καθιστώντας τες ευάλωτες σε γνωστές επιθέσεις, όπως Bluejacking, BlueSnarfing και Man-in-the-Middle (MITM) Attacks.

Η σύγκριση του Bluetooth και του Wi-Fi αποκαλύπτει ότι, παρόλο που λειτουργούν στην ίδια ζώνη συχνοτήτων, διαφέρουν σημαντικά σε τεχνικές μετάδοσης, κατανάλωση ενέργειας και εφαρμογές. Το Bluetooth είναι βέλτιστο για συνδέσεις μικρών αποστάσεων και συσκευές χαμηλής κατανάλωσης, ενώ το Wi-Fi είναι η προτιμώμενη επιλογή για υψηλής ταχύτητας ασύρματη δικτύωση.

Η εξέλιξη του Bluetooth έχει οδηγήσει σε βελτιωμένες ταχύτητες, μεγαλύτερη εμβέλεια και ενισχυμένη ασφάλεια, αλλά η ύπαρξη παλαιότερων συσκευών εξακολουθεί να αποτελεί πρόκληση για την προστασία των δεδομένων. Η κατανόηση αυτών των διαφορών είναι ζωτικής σημασίας για την ανάπτυξη αποδοτικών και ασφαλών ασύρματων επικοινωνιών.

3.2.5 Επιθέσεις σε Bluetooth και Αντιμετώπιση με Τεχνητή Νοημοσύνη

Το Bluetooth είναι μια δημοφιλής τεχνολογία ασύρματης επικοινωνίας μικρής εμβέλειας, η οποία χρησιμοποιείται σε ένα ευρύ φάσμα συσκευών, από κινητά τηλέφωνα και ακουστικά μέχρι IoT συσκευές και βιομηχανικά συστήματα. Ωστόσο, η διαδεδομένη χρήση του Bluetooth το καθιστά ευάλωτο σε διάφορες μορφές κυβερνοεπιθέσεων, που εκμεταλλεύονται αδυναμίες στο πρωτόκολλο ή στην υλοποίηση των συσκευών.

Στην παρούσα ενότητα, θα αναλύσουμε τις πιο γνωστές επιθέσεις στο Bluetooth και θα εξετάσουμε πώς η Τεχνητή Νοημοσύνη (AI) και οι τεχνικές Μηχανικής Μάθησης (ML) μπορούν να συμβάλουν στην ανίχνευση και αντιμετώπισή τους.

Οι επιθέσεις που στοχεύουν συσκευές με Bluetooth ποικίλλουν σε στόχους και μεθοδολογίες. Ορισμένες από τις πιο γνωστές περιλαμβάνουν:

3.2.6 BlueSnarfing

Το BlueSnarfing είναι μια επίθεση όπου ο επιτιθέμενος εκμεταλλεύεται ευπάθειες σε παλιότερες εκδόσεις του Bluetooth (κυρίως πριν την έκδοση 2.1) για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αρχεία της συσκευής-στόχου. Συνήθως, ο εισβολέας μπορεί να υποκλέψει λίστες επαφών, μηνύματα και άλλα προσωπικά δεδομένα.

Πως θα γίνει μια αντιμετώπιση με AI;

- Ανίχνευση ανωμαλιών: Η Μηχανική Μάθηση μπορεί να χρησιμοποιηθεί για την εκπαίδευση αλγορίθμων που ανιχνεύουν ύποπτη δραστηριότητα πρόσβασης στα αρχεία.
- Εφαρμογή αυτοματοποιημένων φίλτρων που αναλύουν τη συμπεριφορά συνδέσεων και απορρίπτουν ύποπτα αιτήματα πρόσβασης.

3.2.7 Bluejacking

Το Bluejacking είναι μια επίθεση όπου ο εισβολέας στέλνει ανεπιθύμητα μηνύματα σε μια συσκευή μέσω Bluetooth. Αν και δεν πρόκειται για άμεση παραβίαση ασφάλειας, μπορεί να χρησιμοποιηθεί για phishing ή εξαπάτηση χρηστών.

Πως θα γίνει μια αντιμετώπιση με AI;

- Φίλτρα ταξινόμησης μηνυμάτων: Το AI μπορεί να αναγνωρίσει μοτίβα ανεπιθύμητων μηνυμάτων και να τα απορρίπτει αυτόματα.
- Εκπαίδευση μοντέλων NLP (Natural Language Processing) για τον εντοπισμό phishing επιθέσεων μέσω Bluetooth μηνυμάτων.

3.2.8 BlueBugging

Το BlueBugging επιτρέπει στον επιτιθέμενο να αποκτήσει πλήρη έλεγχο μιας Bluetooth συσκευής, επιτρέποντάς του να υποκλέψει κλήσεις, να στέλνει μηνύματα ή ακόμα και να ενεργοποιήσει το μικρόφωνο της συσκευής-θύματος.

Πως θα γίνει μια αντιμετώπιση με AI;

- Συστήματα πρόβλεψης ανωμαλιών μπορούν να αναλύουν τη συμπεριφορά της συσκευής και να ανιχνεύουν μη εξουσιοδοτημένες αλλαγές στις ρυθμίσεις Bluetooth.
- AI-driven Intrusion Detection Systems (IDS) μπορούν να εντοπίζουν εισβολές σε πραγματικό χρόνο και να αποτρέπουν μη φυσιολογικές δραστηριότητες.

3.2.9 Bluetooth Spoofing (BD_ADDR Spoofing)

Σε αυτήν την επίθεση, ο εισβολέας πλαστογραφεί τη διεύθυνση MAC μιας έμπιστης συσκευής, ξεγελώντας τον χρήστη ώστε να συνδεθεί στη συσκευή του εισβολέα.

Πως θα γίνει μια αντιμετώπιση με AI;

- Χρήση αλγορίθμων ανίχνευσης spoofing, οι οποίοι αναλύουν μοτίβα συμπεριφοράς των συσκευών και εντοπίζουν αποκλίσεις.
- Βελτιωμένοι αλγόριθμοι ταυτοποίησης μέσω AI, που λαμβάνουν υπόψη πολλαπλές παραμέτρους πέρα από τη MAC address.

3.2.10 Ανάπτυξη Έξυπνων Συστημάτων Άμυνας με Τεχνητή Νοημοσύνη

Θα αναφερθούν σύντομα οι τρόποι καθώς υπάρχει στη συνέχεια σχετικό συγκεκριμένο κεφάλαιο. Οι τεχνικές Μηχανικής Μάθησης (Machine Learning) μπορούν να ενσωματωθούν σε συστήματα ασφαλείας Bluetooth για τη βελτίωση της ανίχνευσης και πρόληψης επιθέσεων. Ορισμένες στρατηγικές περιλαμβάνουν:

- Αξιοποίηση αλγορίθμων επιτήρησης δικτύου, όπως Νευρωνικά Δίκτυα και Random Forest, για την αναγνώριση ύποπτης δραστηριότητας.
- Εκπαίδευση AI μοντέλων σε κανονική και κακόβουλη δραστηριότητα για τη δημιουργία προφίλ συμπεριφοράς Bluetooth επικοινωνιών.

Τα AI-based IDS μπορούν να λειτουργούν σε επίπεδο λογισμικού ή hardware και να προσφέρουν real-time προστασία από επιθέσεις όπως BlueBugging και Bluetooth Spoofing.

Αυτόματη ενημέρωση των μοντέλων AI με νέα δεδομένα απειλών, εξασφαλίζοντας προσαρμογή σε νέες μορφές επιθέσεων.

Συμπερασματικά η ασφάλεια του Bluetooth αποτελεί κρίσιμη πρόκληση, καθώς οι επιθέσεις στο πρωτόκολλο εξελίσσονται συνεχώς. Οι παραδοσιακές τεχνικές άμυνας, όπως ισχυροί κρυπτογραφικοί αλγόριθμοι και πολιτικές πρόσβασης, προσφέρουν βασική προστασία, αλλά συχνά δεν επαρκούν για την αντιμετώπιση εξελιγμένων απειλών.

Η Τεχνητή Νοημοσύνη και η Μηχανική Μάθηση παρέχουν νέες δυνατότητες στην ανίχνευση και πρόληψη κυβερνοεπιθέσεων, μέσω ανάλυσης ανωμαλιών, αυτοματοποιημένης ταξινόμησης απειλών και real-time ανίχνευσης εισβολών. Η ενσωμάτωση έξυπνων συστημάτων άμυνας σε συσκευές Bluetooth μπορεί να βελτιώσει

την ανθεκτικότητα των δικτύων και να προσφέρει μια δυναμική προσέγγιση στην κυβερνοασφάλεια.

4 Πρωτόκολλα Αυθεντικοποίησης

Όπως αναφερθήκαμε ήδη, και θα αναλύσουμε εκτενώς σε παρακάτω κεφάλαιο σχετικά με τις ευπάθειες, εύκολα έως τώρα κατανοούμε την σημαντικότητα της ασφάλειας στα ασύρματα δίκτυα. Η ασφάλεια εξαρτάται σε πολύ μεγάλο βαθμό από τα πρωτόκολλα αυθεντικοποίησης, τα οποία εξασφαλίζουν ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να συνδεθούν στο δίκτυο και να ανταλλάξουν δεδομένα. Καθώς τα ασύρματα δίκτυα εξελίσσονται, κάθε γενιά πρωτοκόλλων προσφέρει βελτιώσεις στην ασφάλεια, αν και κανένα δεν είναι εντελώς απαλλαγμένο από τρωτά σημεία, και ίσως ποτέ να μην υπάρξει. Στη γενικότερη συνολική εικόνα, η έννοια της απόλυτης ασφάλειας παραμένει μια θεωρία έως τώρα και η πράξη της θα δεν θα αποδώσει όσο εμπλέκεται η μεγαλύτερη ευπάθεια, ο ανθρώπινος παράγοντας. Η συνεχή έρευνα για την εξέλιξη και αναβάθμιση σε ασφαλέστερα πρότυπα, πρακτικές και τεχνικές είναι το κύριο καθήκον για τους επαγγελματίες στην ασφάλεια πληροφοριακών συστημάτων. Συνοψίζοντας σε αυτό το κεφάλαιο αναλύονται τα βασικά πρωτόκολλα αυθεντικοποίησης, ο τρόπος λειτουργίας τους, οι αδυναμίες τους και οι συνηθέστερες επιθέσεις που μπορούν να τα στοχεύσουν.

4.1 WEP (Wired Equivalent Privacy)

Το WEP ήταν το πρώτο πρωτόκολλο που σχεδιάστηκε για να προσφέρει μια πρωτότυπη ασφάλεια σε ασύρματα δίκτυα, βασιζόμενο σε συμμετρική κρυπτογράφηση δεδομένων. Πιο συγκεκριμένα χρησιμοποιεί τον αλγόριθμο RC4 και ένα κλειδί μήκους 40 ή 104 bit, το οποίο συνδυάζεται με έναν αρχικοποιητή (IV - Initialization Vector) για την κρυπτογράφηση των δεδομένων.

Παρά, όμως, τη σημαντική πρόοδο που προσέφερε τη δεκαετία του 1990, το WEP έχει αποδειχθεί ιδιαίτερα ευάλωτο λόγω της περιορισμένης ασφάλειας που παρέχει ο μηχανισμός κρυπτογράφησής του. Ο αλγόριθμος RC4 παρουσιάζει επαναλαμβανόμενα μοτίβα, επιτρέποντας στους κακόβουλους χρήστες να υποκλέψουν αρκετά πακέτα για να αποκρυπτογραφήσουν το κλειδί μέσω τεχνικών όπως η ανάλυση του IV.

Οι συχνότερες επιθέσεις στο WEP περιλαμβάνουν την υποκλοπή δεδομένων μέσω επιθέσεων brute force και την παρακολούθηση πακέτων (packet sniffing). Επιπλέον, η στατική φύση του κλειδιού κρυπτογράφησης καθιστά το πρωτόκολλο ευάλωτο σε replay attacks, όπου οι επιτιθέμενοι επαναλαμβάνουν τη μετάδοση υποκλαπέντων πακέτων για να παρακάμψουν την ασφάλεια.

4.2 WPS (Wi-Fi Protected Setup)

Το WPS σχεδιάστηκε για να απλοποιήσει τη διαδικασία σύνδεσης συσκευών σε ασφαλή ασύρματα δίκτυα, χρησιμοποιώντας έναν οκταψήφιο PIN για την αυθεντικοποίηση. Η μέθοδος αυτή ήταν ιδιαίτερα δημοφιλής λόγω της ευκολίας χρήσης της, αλλά αποδείχθηκε ότι περιλαμβάνει σοβαρές αδυναμίες ασφαλείας.

Η κύρια ευπάθεια του WPS σχετίζεται με την προβλεψιμότητα του PIN, το οποίο ελέγχεται σε δύο ξεχωριστά μέρη, μειώνοντας δραματικά το πλήθος των πιθανών συνδυασμών. Αυτό επιτρέπει επιθέσεις brute force, όπου ένας επιτιθέμενος δοκιμάζει όλους τους πιθανούς συνδυασμούς PIN έως ότου αποκτήσει πρόσβαση στο δίκτυο.

Η πιο συχνή επίθεση στο WPS είναι η χρήση εργαλείων όπως το Reaver, τα οποία μπορούν να παραβιάσουν το PIN μέσα σε λίγες ώρες. Επιπλέον, η έλλειψη μηχανισμών περιορισμού προσπαθειών εισαγωγής του PIN διευκολύνει περαιτέρω τις επιθέσεις brute force.

4.3 WPA (Wi-Fi Protected Access)

Το WPA αποτέλεσε το διάδοχο του WEP και σχεδιάστηκε ως ενδιάμεση λύση μέχρι την ανάπτυξη του WPA2. Βασίζεται επίσης στον αλγόριθμο RC4, αλλά εισήγαγε τον μηχανισμό Temporal Key Integrity Protocol (TKIP), ο οποίος αυξάνει τη δυναμικότητα του κλειδιού, προσφέροντας μερική περισσότερη ασφάλεια σε σχέση με τα προηγούμενα πρότυπα. Έτσι καθε πακέτο δεδομένων κρυπτογραφείται με ένα μοναδικό κλειδί, μειώνοντας τις πιθανότητες αποκρυπτογράφησης από επιτιθέμενους.

Παρά την πρόοδο που επέφερε, το WPA εξακολουθεί να είναι ευάλωτο σε συγκεκριμένες επιθέσεις. Ο TKIP δεν καταφέρνει να εξαλείψει όλα τα προβλήματα του RC4, ενώ η εξάρτηση από προκοινοποιημένα κλειδιά (Pre-Shared Keys - PSK) δημιουργεί κινδύνους ασφαλείας.

Επιθέσεις:

Οι πιο συνηθισμένες επιθέσεις στο WPA περιλαμβάνουν την υποκλοπή του handshake, όπου ένας επιτιθέμενος αποκτά πρόσβαση σε κρυπτογραφημένα δεδομένα και τα αναλύει με εργαλεία όπως το Aircrack-ng για να αποκρυπτογραφήσει το PSK. Επιθέσεις τύπου Man-in-the-Middle (MITM) είναι επίσης δυνατές όταν το πρωτόκολλο χρησιμοποιείται σε μη ασφαλή δίκτυα.

4.4 WPA2 (Wi-Fi Protected Access II) – CCMP

Το WPA2 (Wi-Fi Protected Access II) είναι το δεύτερο και πιο διαδεδομένο πρότυπο ασφάλειας για ασύρματα δίκτυα, το οποίο υιοθετήθηκε επίσημα το 2004 ως διάδοχος του WPA. Σχεδιάστηκε για να παρέχει αυξημένη ασφάλεια και προστασία των δεδομένων, αντιμετωπίζοντας τις σοβαρές ευπάθειες που είχαν διαπιστωθεί στα προηγούμενα πρωτόκολλα, όπως το WEP και το WPA. Το WPA2 βασίζεται στον αλγόριθμο κρυπτογράφησης **AES (Advanced Encryption Standard)** και τον μηχανισμό **CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)**, παρέχοντας αυξημένα επίπεδα ασφάλειας και απόδοσης.

Τρόπος Λειτουργίας του WPA2

Το WPA2 εισάγει σημαντικές βελτιώσεις σε σύγκριση με το WPA, βασιζόμενο στην αντικατάσταση του αλγορίθμου RC4 με τον AES και στην εισαγωγή του CCMP, που είναι υπεύθυνος για την κρυπτογράφηση και την ακεραιότητα των δεδομένων. Παρακάτω αναλύεται λεπτομερώς ο τρόπος λειτουργίας του.

1. Σχετικα με τη Κρυπτογράφηση Δεδομένων με τον AES:
Ο AES αποτελεί έναν συμμετρικό αλγόριθμο κρυπτογράφησης μπλοκ, ο οποίος επιλέχθηκε για το WPA2 λόγω της υψηλής ασφάλειας και της αποδοτικότητάς του. Στη

λειτουργία του WPA2, τα δεδομένα που μεταδίδονται στο δίκτυο χωρίζονται σε μπλοκ σταθερού μεγέθους (συνήθως 128 bits) και κρυπτογραφούνται χρησιμοποιώντας το ίδιο κλειδί σε κάθε μπλοκ. Ο AES στο WPA2 υλοποιείται σε **Counter Mode**, όπου κάθε μπλοκ δεδομένων κρυπτογραφείται με ένα μοναδικό κλειδί που βασίζεται σε έναν μετρητή (counter) που αυξάνεται σε κάθε μπλοκ. Αυτό αποτρέπει την αποκρυπτογράφηση δεδομένων ακόμα κι αν κάποιος καταφέρει να υποκλέψει προηγούμενα μπλοκ.

2. Έλεγχος Ακεραιότητας με CCMP:

Το CCMP είναι υπεύθυνο για την εξασφάλιση ότι τα δεδομένα που μεταδίδονται στο δίκτυο δεν έχουν αλλοιωθεί. Ο μηχανισμός αυτός βασίζεται στη χρήση του CBC-MAC (Cipher Block Chaining Message Authentication Code), που προσθέτει έναν έλεγχο ακεραιότητας στο τέλος κάθε πακέτου δεδομένων. Κατά τη διάρκεια της μετάδοσης:

- Το CCMP δημιουργεί έναν κώδικα ελέγχου (MAC) για κάθε πακέτο δεδομένων, ο οποίος ελέγχεται από τον παραλήπτη.
- Αν ο κώδικας αυτός δεν ταιριάζει με τον υπολογισμένο κώδικα του παραλήπτη, τότε το πακέτο θεωρειται κατεστραμένο και απορρίπτεται.

3. Διαδικασία Αυθεντικοποίησης:

Το WPA2 υποστηρίζει δύο διαφορετικούς τρόπους αυθεντικοποίησης:

- **Προσωπική Λειτουργία (Personal Mode – WPA2-PSK):** Η αυθεντικοποίηση βασίζεται στη χρήση ενός προκοινοποιημένου κωδικού πρόσβασης (Pre-Shared Key - PSK). Κατά τη διαδικασία σύνδεσης, η συσκευή και το access point δημιουργούν ένα **Pairwise Transient Key (PTK)**, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων. Η δημιουργία του PTK βασίζεται στην ανταλλαγή ενός αρχικού κλειδιού (PMK - Pairwise Master Key) και μιας διαδικασίας τετραπλού handshake (4-way handshake). Το 4-way handshake εξασφαλίζει ότι ο χρήστης έχει εισάγει σωστά τον κωδικό πρόσβασης χωρίς αυτός να μεταδίδεται απευθείας μέσω του δικτύου.
- **Επιχειρησιακή Λειτουργία (Enterprise Mode – WPA2-Enterprise):** Χρησιμοποιεί το πρωτόκολλο 802.1X και έναν εξωτερικό διακομιστή αυθεντικοποίησης (RADIUS server) για τη διαχείριση χρηστών και κωδικών

πρόσβασης. Αυτή η μέθοδος είναι πιο ασφαλής, καθώς κάθε χρήστης έχει μοναδικά διαπιστευτήρια σύνδεσης.

4. Ανταλλαγή Κλειδιών (4-Way Handshake):

Η διαδικασία 4-way handshake είναι το κεντρικό στοιχείο της λειτουργίας του WPA2 και εκτελείται κατά την έναρξη κάθε σύνδεσης μεταξύ μιας συσκευής και του access point.

Περιλαμβάνει τα εξής βήματα:

1. Το access point στέλνει έναν τυχαίο αριθμό (nonce) στη συσκευή.
2. Η συσκευή χρησιμοποιεί το nonce και το PMK για να δημιουργήσει το PTK και επιστρέφει έναν δεύτερο nonce στο access point.
3. Το access point υπολογίζει επίσης το PTK και στέλνει ένα μήνυμα επιβεβαίωσης στη συσκευή.
4. Η συσκευή επιβεβαιώνει ότι όλα τα δεδομένα είναι σωστά και η σύνδεση ολοκληρώνεται.

Τρωτά Σημεία του WPA2

Παρά την ισχυρή κρυπτογράφηση του AES και τη βελτίωση που εισήγαγε το CCMP, το WPA2 δεν είναι άτρωτο σε όλες τις επιθέσεις. Τα κυριότερα τρωτά σημεία του περιλαμβάνουν:

1. **Ευπάθεια στις επιθέσεις KRACK (Key Reinstallation Attack):**
   Η KRACK εκμεταλλεύεται αδυναμίες στη διαδικασία του 4-way handshake. Ο επιτιθέμενος μπορεί να υποκλέψει τα μηνύματα του handshake και να τα επαναλάβει, αναγκάζοντας τη συσκευή να επανεγκαταστήσει το ίδιο κλειδί κρυπτογράφησης. Αυτό μπορεί να οδηγήσει σε αποκρυπτογράφηση δεδομένων ή εισαγωγή κακόβουλων πακέτων.
2. **Brute Force και Dictionary Attacks:**
   Στη λειτουργία PSK, η ασφάλεια βασίζεται στον κωδικό πρόσβασης του δικτύου. Αν ο κωδικός είναι αδύναμος, μπορεί να παραβιαστεί μέσω επιθέσεων brute force ή dictionary, όπου δοκιμάζονται πολλαπλοί συνδυασμοί λέξεων και αριθμών μέχρι να βρεθεί ο σωστός.

3. **Man-in-the-Middle Attacks (MITM):**
   Σε δημόσια δίκτυα ή μη ασφαλείς συνδέσεις, ένας επιτιθέμενος μπορεί να παρέμβει στη σύνδεση και να αποκτήσει πρόσβαση στα δεδομένα του χρήστη.
4. **Packet Sniffing και Replay Attacks:**
   Οι επιθέσεις παρακολούθησης πακέτων και επανάληψης (replay) εξακολουθούν να είναι πιθανές, ειδικά σε δίκτυα όπου το 4-way handshake επαναλαμβάνεται συχνά.

Οφέλη και Περιορισμοί

Το WPA2 παραμένει ένα από τα πιο ασφαλή πρωτόκολλα για ασύρματα δίκτυα, όταν υλοποιείται σωστά και χρησιμοποιείται με ισχυρούς κωδικούς πρόσβασης. Παρέχει υψηλό επίπεδο κρυπτογράφησης μέσω AES και CCMP, ενώ η χρήση του 4-way hand-shake μειώνει τις πιθανότητες αποκρυπτογράφησης των δεδομένων. Ωστόσο, η εξάρτηση από στατικούς κωδικούς πρόσβασης στη λειτουργία PSK και η ευπάθεια στις επιθέσεις KRACK τονίζουν την ανάγκη για περαιτέρω βελτιώσεις, οι οποίες εισήχθησαν στο WPA3.

Με τη χρήση ισχυρών πρωτοκόλλων και την σωστή διαχείριση, το WPA2 προσέφερε για χρόνια ένα σταθερό επίπεδο ασφάλειας, αν και οι νέες απειλές και η εξέλιξη των μεθόδων επιθέσεων ανέδειξαν την ανάγκη για το επόμενο βήμα στην ασφάλεια των ασύρματων δικτύων.

Ωστόσο, το WPA2 δεν είναι απόλυτα ασφαλές. Η επίθεση KRACK είναι από τις πιο γνωστές, επιτρέποντας στους επιτιθέμενους να αποκρυπτογραφούν δεδομένα και να εισάγουν κακόβουλα πακέτα. Επίσης, επιθέσεις brute force και dictionary attacks στο PSK αποτελούν συχνά προβλήματα.

4.5 WPA3 - SAE

Το WPA3 αποτελεί το πιο πρόσφατο πρωτόκολλο ασφαλείας για ασύρματα δίκτυα, εισάγοντας σημαντικές βελτιώσεις σε σχέση με το WPA2. Βασίζεται κυρίως στον μηχανισμό Simultaneous Authentication of Equals (SAE), ο οποίος αντικαθιστά το

PSK και προσφέρει ισχυρότερη προστασία ενάντια σε επιθέσεις brute force. Ο SAE χρησιμοποιεί το Dragonfly Key Exchange και τον αλγόριθμο Diffie-Hellman, έτσι ώστε ο πραγματικός κωδικός να μην μεταδίδεται ποτέ μέσω του δικτύου. Η μέθοδος αυτή καθιστά τις προσπάθειες παραβίασης ιδιαίτερα χρονοβόρες και μη πρακτικές, ακόμα κι όταν οι χρήστες χρησιμοποιούν σχετικά απλούς κωδικούς.

Επιπλέον, το WPA3 εισάγει την έννοια της Forward Secrecy, δηλαδή τη δημιουργία μοναδικών προσωρινών κλειδιών για κάθε σύνδεση. Αυτό σημαίνει πως ακόμα κι αν διαρρεύσει ένα κλειδί, δεν είναι δυνατό να αποκρυπτογραφηθούν δεδομένα από παλαιότερες ή μελλοντικές συνδέσεις, προσφέροντας έτσι αυξημένη ανθεκτικότητα απέναντι σε μελλοντικές παραβιάσεις.

Ένα ακόμη σημαντικό χαρακτηριστικό είναι η κρυπτογράφηση ανά συσκευή (Individualized Data Encryption). Για κάθε νέα σύνδεση δημιουργείται διαφορετικό κλειδί, εξασφαλίζοντας ότι ακόμα και σε κοινόχρηστα δίκτυα, τα δεδομένα μιας συσκευής δεν μπορούν να υποκλαπούν από άλλες συνδεδεμένες.

Συμπληρωματικά, το WPA3 ενσωματώνει το πρωτόκολλο Opportunistic Wireless Encryption (OWE), το οποίο βελτιώνει την ασφάλεια των ανοιχτών δικτύων. Το OWE επιτρέπει την αυτόματη δημιουργία ασφαλούς συνόδου χωρίς να απαιτείται κωδικός πρόσβασης, προστατεύοντας έτσι τους χρήστες σε δημόσια hotspots.

Τα βασικά οφέλη του WPA3 συνοψίζονται στα εξής:

- Αντοχή σε brute force και dictionary attacks μέσω περιορισμού αποτυχημένων προσπαθειών.
- Υποστήριξη κρυπτογράφησης 192-bit στο WPA3-Enterprise, για περιβάλλοντα υψηλής ασφάλειας σύμφωνα με οδηγίες της NSA.

Παρά τις βελτιώσεις, το WPA3 δεν είναι άτρωτο. Η πολυπλοκότητα του SAE και αδυναμίες στην υλοποίηση έχουν επιτρέψει επιθέσεις όπως το Dragonblood. Επιπλέον, υπάρχουν καταγεγραμμένες ευπάθειες όπως:

- CVE-2019-13377: timing side-channel attack στο Dragonfly handshake.
- CVE-2019-13456: information leak στο FreeRADIUS EAP-pwd.

Συνολικά, το WPA3 αποτελεί τη μέχρι τώρα πιο ασφαλή επιλογή για Wi-Fi δίκτυα, θέτοντας νέες βάσεις για την ασύρματη ασφάλεια, με την προϋπόθεση ότι υλοποιείται σωστά από τις συσκευές.

5 802.11 Frames Και Τύποι

Για την ουσιαστική κατανόηση της λειτουργίας και της επικοινωνίας των ασύρματων δικτύων μέσω του πρωτοκόλλου IEEE 802.11, είναι απαραίτητο να αναλυθεί η δομή των πλαισίων, οι τύποι και οι υπότυποί τους. Στην επικοινωνία 802.11, χρησιμοποιούνται διάφοροι τύποι πλαισίων, οι οποίοι εκτελούν διαφορετικές λειτουργίες, αποτελώντας αναπόσπαστο μέρος του κύκλου σύνδεσης και της ανταλλαγής δεδομένων. Κατά τη διάρκεια κακόβουλων ενεργειών, όπως δοκιμές διείσδυσης ή επιθέσεις, γίνεται συχνά χρήση τεχνικών παραποίησης ή δημιουργίας πλαισίων, προκειμένου να πραγματοποιηθούν ενέργειες όπως η αποσύνδεση μιας συσκευής-πελάτη από το δίκτυο μέσω αιτημάτων αποαυθεντικοποίησης (deauthentication) ή αποσυσχέτισης (disassociation).

5.1 Το Πλαίσιο MAC στο IEEE 802.11

Το 802.11 βασίζεται στο MAC frame, τη θεμελιώδη μονάδα ανταλλαγής πληροφοριών ανάμεσα σε AP–πελάτη ή σε ad-hoc δίκτυα. Η δομή του έχει 9 πεδία, καθένα με συγκεκριμένο ρόλο στη δρομολόγηση, τον συγχρονισμό και την ακεραιότητα.

- Frame Control
  Καθορίζει τύπο/υπότυπο (Management, Control, Data), την έκδοση πρωτοκόλλου και flags όπως to DS / from DS και Order. Ορίζει πώς θα ερμηνευτεί και θα προωθηθεί το πλαίσιο.
- Duration / ID
  Δηλώνει το χρονικό διάστημα που δεσμεύεται το μέσο για τη μετάδοση. Βοηθά στη συνύπαρξη πολλών ταυτόχρονων ροών και στη μείωση συγκρούσεων.
- Address 1, 2, 3, 4
  Περιλαμβάνουν τις MAC διευθύνσεις των εμπλεκόμενων συσκευών. Συνήθως υπάρχουν το BSSID (του AP) και η MAC του πελάτη. Η ακριβής σημασία κάθε πεδίου εξαρτάται από προέλευση/προορισμό· το Address 4 χρησιμοποιείται μόνο σε ειδικές περιπτώσεις (π.χ. bridging).

- Sequence Control (SC)
  Διαχειρίζεται την ακολουθία και τον κατακερματισμό των πλαισίων (sequence/fragment). Αποτρέπει διπλότυπα και διατηρεί συνεκτική ροή.
- Data (Frame Body)
  Το ωφέλιμο φορτίο της μετάδοσης: τα πραγματικά δεδομένα/μήνυμα που στέλνει ο αποστολέας στον παραλήπτη.
- CRC / FCS (32-bit)

Έλεγχος ακεραιότητας (checksum) για ανίχνευση σφαλμάτων. Πλαίσια με λάθη απορρίπτονται ώστε να προστατεύονται τα ανώτερα επίπεδα.

Συνολικά, αυτά τα πεδία συγκροτούν τον «σκελετό» της επικοινωνίας στα Wi-Fi δίκτυα, εξασφαλίζοντας ομαλή ροή δεδομένων και αξιόπιστη ανταλλαγή μηνυμάτων.

5.2 Τύποι Πλαισίων IEEE 802.11

Το 802.11 ταξινομεί τα πλαίσια σε κατηγορίες ανάλογα με τον σκοπό τους. Έτσι οργανώνεται η δημιουργία, η ροή και ο τερματισμός των συνδέσεων μεταξύ AP και πελάτη (ή σε ad-hoc).

Βασικοί τύποι πλαισίων

- Management: διαχείριση της σχέσης AP–πελάτη (δημιουργία, διατήρηση, τερματισμός).
- Control: ρύθμιση/συντονισμός της μετάδοσης των Data frames για ομαλή λειτουργία.
- Data: μεταφέρουν το ωφέλιμο περιεχόμενο (αρχεία, φωνή, βίντεο κ.λπ.).
- Υπότυποι Management (ασφάλεια & λειτουργία)
- Beacon: περιοδική εκπομπή από το AP· περιέχει SSID, υποστηριζόμενη κρυπτογράφηση/αυθεντικοποίηση, ρυθμούς μετάδοσης.
- Probe Request/Response: ο πελάτης «ψάχνει» γειτονικά AP (και κρυφά SSID) με request· το AP απαντά με τις πληροφορίες που χρειάζονται για σύνδεση.

- Authentication: πρώτο βήμα σύνδεσης· ο πελάτης αιτείται αυθεντικοποίηση και το AP αποδέχεται/απορρίπτει.
- Association: ακολουθεί την αυθεντικοποίηση· ο πελάτης ζητά συσχέτιση και, αν γίνει δεκτή, αποκτά πλήρη πρόσβαση στο δίκτυο.
- Deauthentication / Disassociation: τερματίζουν τη σχέση πελάτη–AP, με reason code που εξηγεί το γιατί· σε δοκιμές διείσδυσης χρησιμοποιούνται για DoS ή συλλογή handshake.

Συνολικά, η κατανόηση των τύπων/υποτύπων 802.11 βοηθά να βλέπουμε πού υπάρχουν ευκαιρίες και κίνδυνοι—από τη φυσιολογική λειτουργία ως τα σενάρια κακόβουλων επιθέσεων ή ελέγχων ασφάλειας.

5.3 Ο Κύκλος Σύνδεσης

Αφού εξετάσαμε τους τύπους πλαισίων IEEE 802.11 και τους υπότυπους των πλαισίων διαχείρισης, μπορούμε να επικεντρωθούμε στη διαδικασία σύνδεσης μεταξύ των συσκευών-πελατών και των σημείων πρόσβασης (Access Points), γνωστή ως κύκλος σύνδεσης. Σε αυτήν την ανάλυση, θα επικεντρωθούμε στη βασική αυθεντικοποίηση WPA2, αν και η διαδικασία μπορεί να διαφέρει ελαφρώς ανάλογα με το πρότυπο Wi-Fi που χρησιμοποιείται. Παρόλα αυτά, η γενική δομή της διαδικασίας παραμένει παρόμοια και περιλαμβάνει τα εξής βήματα σχετικά με τα πλαίσια:

1) Πλαίσια Beacon
2) Αιτήσεις και Απαντήσεις Ελέγχου (Probe Request και Probe Response)
3) Αιτήσεις και Απαντήσεις Αυθεντικοποίησης (Authentication Request και Response)
4) Αιτήσεις και Απαντήσεις Συσχέτισης (Association Request και Response)
5) Ανταλλαγή Handshake ή άλλου μηχανισμού ασφαλείας
6) Αποσυσχέτιση ή Αποαυθεντικοποίηση (Disassociation/Deauthentication)

Η ανάλυση αυτής της διαδικασίας μπορεί να γίνει παρακολουθώντας την ακατέργαστη κίνηση του δικτύου μέσω εργαλείων όπως το Wireshark. Ένα επιτυχές handshake μπορεί να καταγραφεί, και στη συνέχεια το αρχείο καταγραφής μπορεί να αναλυθεί λεπτομερώς με το Wireshark, προκειμένου να εξεταστεί η αλληλουχία των πλαισίων.

Τα Πλαίσια Στον Κύκλο Σύνδεσης:

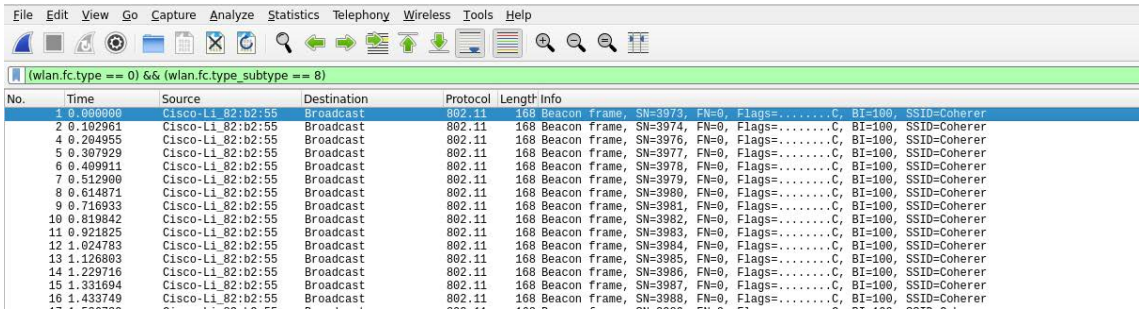
Για την παρακολούθηση και την κατανόηση των διαφορετικών σταδίων του κύκλου σύνδεσης, κάθε τύπος πλαισίου μπορεί να εντοπιστεί με συγκεκριμένα φίλτρα Wireshark. Παρακάτω περιγράφονται τα βασικά στάδια, μαζί με τα φίλτρα που μπορούν να χρησιμοποιηθούν.

1. Πλαίσια Beacon

Τα πλαίσια Beacon αποστέλλονται από το σημείο πρόσβασης, διαφημίζοντας την παρουσία του δικτύου στους πελάτες. Περιέχουν σημαντικές πληροφορίες όπως το SSID, τους υποστηριζόμενους τύπους αυθεντικοποίησης και τις ταχύτητες δεδομένων.

Στο Wireshark, αυτά τα πλαίσια μπορούν να εντοπιστούν με το εξής φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 8)

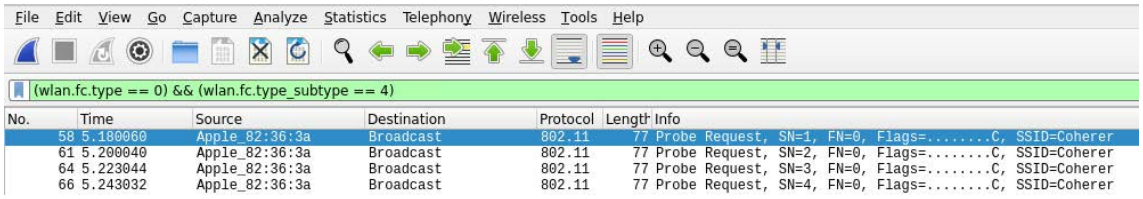


2. Αιτήσεις και Απαντήσεις Ελέγχου (Probe Request και Response)

Κατά τη διάρκεια της φάσης ελέγχου, οι συσκευές-πελάτες αναζητούν διαθέσιμα σημεία πρόσβασης αποστέλλοντας αιτήσεις Probe (Probe Request). Τα σημεία πρόσβασης που λαμβάνουν αυτές τις αιτήσεις ανταποκρίνονται με πληροφορίες για το δίκτυο (Probe Response).

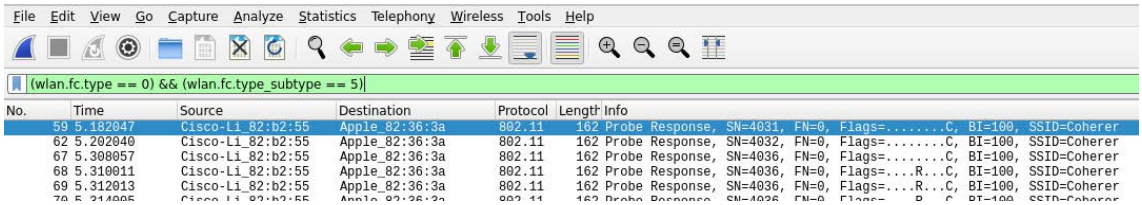
Τα πλαίσια Probe Request μπορούν να εντοπιστούν με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 4)



Τα πλαίσια Probe Response μπορούν να εντοπιστούν με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 5)

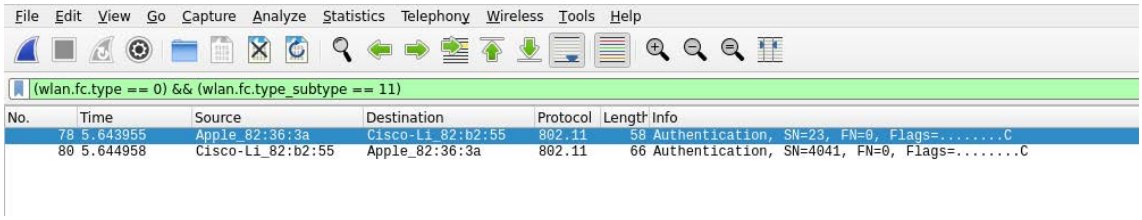


3. Αιτήσεις και Απαντήσεις Αυθεντικοποίησης

Η αυθεντικοποίηση είναι το πρώτο βήμα για τη δημιουργία της σύνδεσης. Η συσκευή-πελάτης αποστέλλει αίτηση αυθεντικοποίησης στο σημείο πρόσβασης, το οποίο απαντά είτε επιτρέποντας είτε απορρίπτοντας τη σύνδεση.

Αυτά τα πλαίσια μπορούν να εντοπιστούν με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 11)

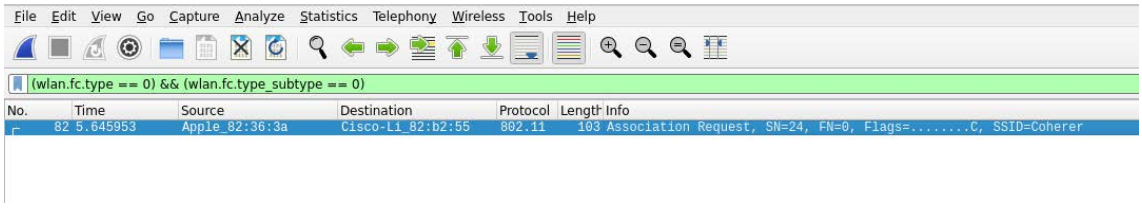


4. Αιτήσεις και Απαντήσεις Συσχέτισης

Μετά την επιτυχή αυθεντικοποίηση, η συσκευή-πελάτης αποστέλλει αίτηση συσχέτισης (Association Request) στο σημείο πρόσβασης. Το σημείο πρόσβασης απαντά με πλαίσιο συσχέτισης (Association Response), δηλώνοντας εάν η σύνδεση εγκρίθηκε ή όχι.

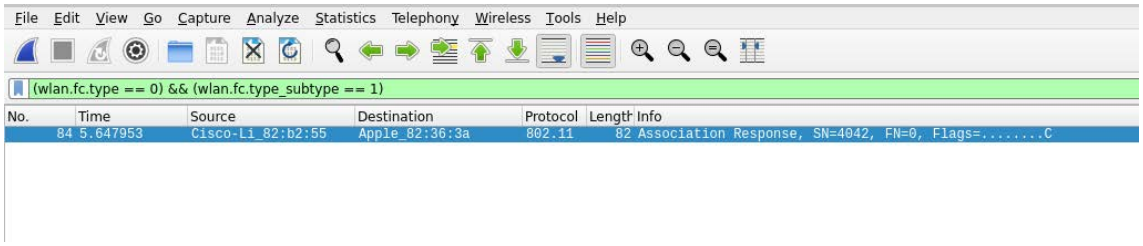
Η αίτηση συσχέτισης εντοπίζεται με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 0)



Η απάντηση συσχέτισης εντοπίζεται με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 1)

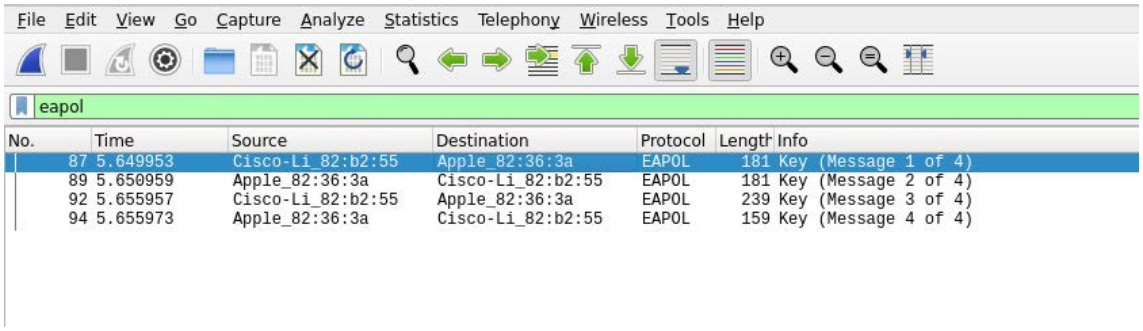


5. Ανταλλαγή Handshake

Εάν το δίκτυο χρησιμοποιεί WPA2, η διαδικασία του handshake πραγματοποιείται μέσω του πρωτοκόλλου EAPOL (Extensible Authentication Protocol over LAN). Κατά τη διάρκεια του handshake, ανταλλάσσονται τα κλειδιά κρυπτογράφησης που απαιτούνται για την ασφαλή επικοινωνία μεταξύ του πελάτη και του σημείου πρόσβασης.

Τα πλαίσια EAPOL μπορούν να εντοπιστούν με το φίλτρο:

eapol

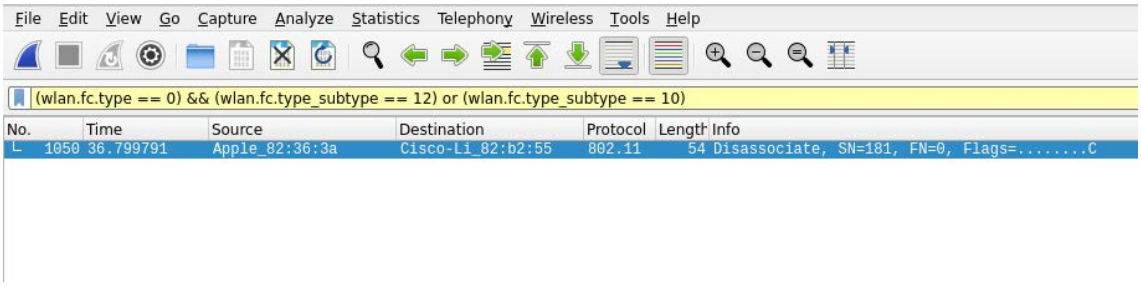


6. Αποσυσχέτιση ή Αποαυθεντικοποίηση

Όταν ολοκληρωθεί η επικοινωνία ή όταν προκύψει πρόβλημα στο δίκτυο, η σύνδεση τερματίζεται με την αποστολή πλαισίων αποσυσχέτισης (Disassociation) ή αποαυθεντικοποίησης (Deauthentication). Αυτά τα πλαίσια αποστέλλονται είτε από τη συσκευή-πελάτη είτε από το σημείο πρόσβασης και περιλαμβάνουν κωδικό αιτιολόγησης (reason code) που εξηγεί τον λόγο της αποσύνδεσης.

Τα πλαίσια αποσυσχέτισης ή αποαυθεντικοποίησης μπορούν να εντοπιστούν με το φίλτρο:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 12) or (wlan.fc.type_subtype == 10)



Η κατανόηση του κύκλου σύνδεσης είναι θεμελιώδης για την ανάλυση της λειτουργίας των ασύρματων δικτύων. Ο κύκλος περιλαμβάνει διαδοχικά βήματα που εξασφαλίζουν την ασφαλή σύνδεση, τη διαχείριση της επικοινωνίας και τον τερματισμό της σύνδεσης όταν χρειάζεται. Οι μηχανισμοί όπως το handshake διασφαλίζουν ότι η μετάδοση των δεδομένων παραμένει κρυπτογραφημένη, ενώ πλαίσια όπως τα beacon και τα probe διευκολύνουν την ανακάλυψη και την πρόσβαση στο δίκτυο.

Η παρακολούθηση της ακατέργαστης κίνησης μέσω εργαλείων όπως το Wireshark μας επιτρέπει να κατανοήσουμε τη δομή αυτών των πλαισίων, να αναλύσουμε πιθανές αδυναμίες στο δίκτυο και να εντοπίσουμε τις αιτίες μιας πιθανής αποσύνδεσης. Στις επόμενες ενότητες, θα εξετάσουμε μεθόδους αυθεντικοποίησης και θα αναλύσουμε πιο αναλυτικά τις διαφορετικές διαδικασίες ασφαλείας.

6 Τεχνικές Επίθεσης

6.1 Επιλέγοντας Την Κατάλληλη Διεπαφή

Η κατάλληλη ασύρματη διεπαφή αποτελεί θεμελιώδες στοιχείο για τις δοκιμές διείσδυσης σε Wi-Fi δίκτυα. Αυτές οι διεπαφές είναι υπεύθυνες για τη μετάδοση και λήψη δεδομένων, επιτρέποντας την επικοινωνία μεταξύ των συσκευών στο δίκτυο. Η σωστή επιλογή διεπαφής είναι κρίσιμη, καθώς μια αδύναμη διεπαφή μπορεί να καταστήσει αδύνατη την καταγραφή κρίσιμων δεδομένων, σε μεγάλες αποστάσεις, με πολλά δίκτυα να παρουσιάζονται κατά τη διάρκεια των δοκιμών. Στην παρούσα ενότητα, αναλύουμε τις παραμέτρους που πρέπει να ληφθούν υπόψη κατά την επιλογή μιας διεπαφής για το penetration testing σε Wi-Fi δίκτυα, επικεντρώνοντας σε τρεις κρίσιμες λειτουργίες: το monitor mode, το packet injection και το master mode.

Κριτήρια Επιλογής της Ιδανικής Διεπαφής.

Το πρώτο κριτήριο που πρέπει να εξετάσουμε πολύ αναλυτικά είναι οι δυνατότητες της διεπαφής. Είναι σημαντικό η διεπαφή να υποστηρίζει τις συχνότητες 2.4G και 5G, για να είναι δυνατή η σάρωση δικτύων σε όλες τις διαθέσιμες ζώνες συχνοτήτων. Είναι απαραίτητο να κατανοήσουμε ότι οι dual-band κάρτες δικτύου, οι οποίες υποστηρίζουν τόσο τη συχνότητα 2.4 GHz όσο και 5 GHz, δεν είναι πάντα ανώτερες σε απόδοση σε σύγκριση με μια κάρτα που λειτουργεί αποκλειστικά στη ζώνη των 2.4 GHz. Σε πολλές περιπτώσεις, μια μονή (single-band) κάρτα 2.4 GHz μπορεί να προσφέρει βελτιωμένη απόδοση και σταθερότητα σε σχέση με μια dual-band κάρτα, ιδιαίτερα όταν το 2.4 GHz αποτελεί την κύρια ή μοναδική ζώνη λειτουργίας της.

Αυτό συμβαίνει επειδή οι single-band κάρτες 2.4 GHz συχνά διαθέτουν βελτιστοποιημένες κεραίες και καλύτερο σχεδιασμό λήψης σήματος για αυτή τη συγκεκριμένη συχνότητα. Αντίθετα, σε μια dual-band κάρτα, οι διαθέσιμοι πόροι μοιράζονται μεταξύ των δύο ζωνών συχνοτήτων, γεγονός που μπορεί να οδηγήσει σε ελαφρώς χαμηλότερη απόδοση στη ζώνη των 2.4 GHz. Επιπλέον, ορισμένες dual-band συσκευές μπορεί να έχουν ασθενέστερους ενισχυτές σήματος στη χαμηλότερη

συχνότητα, δίνοντας προτεραιότητα στο 5 GHz, το οποίο προσφέρει υψηλότερες ταχύτητες αλλά μικρότερη εμβέλεια.

Συνεπώς, η επιλογή μεταξύ single-band και dual-band κάρτας δικτύου δεν πρέπει να γίνεται αποκλειστικά με βάση τον αριθμό των υποστηριζόμενων ζωνών, αλλά λαμβάνοντας υπόψη τις πραγματικές συνθήκες λειτουργίας, τις ιδιαιτερότητες του εκάστοτε περιβάλλοντος και τις απαιτήσεις της εκάστοτε χρήσης.

Επιπλέον, η διεπαφή θα πρέπει να διαθέτει υποστήριξη για τα πρότυπα IEEE 802.11ac ή IEEE 802.11ax. Ειδικότερα, θα πρέπει να γνωρίζουμε τις διαφορές ανάμεσα στις λειτουργίες monitor mode, packet injection και master mode αφού καθορίζουν τη κύρια λειτουργία της ασύρματης διεπαφής για το penetration testing. Πιο αναλυτικά όλες οι λειτουργίες είναι:

- Monitor Mode: Αυτή η λειτουργία επιτρέπει στην ασύρματη κάρτα να «συμμετέχει» στο δίκτυο και να λειτουργεί σε μια παθητική κατάσταση, καταγράφοντας όλη την κυκλοφορία του αέρα στην εμβέλεια της. Είναι ιδανική για την ανάλυση και την επιτήρηση του δικτύου χωρίς να επηρεάσει την κυκλοφορία των δεδομένων.
- Packet Injection: Θα πρέπει η κάρτα δικτύου να έχει τη δυνατότητα να επιτρέπει στον ερευνητή να δημιουργεί και να αποστέλλει πακέτα στο δίκτυο, επεμβαίνοντας στην κοινοτική κυκλοφορία. Ουσιαστικά, επιτρέπει στη συσκευή να "εισάγει" αυθαίρετα πακέτα σε ένα δίκτυο, ακόμα κι αν δεν είναι συνδεδεμένη σε αυτό. Είναι σχεδόν αναγκαίο χαρακτηριστικό για τη δοκιμή ασφαλείας και την εκτέλεση επιθέσεων σε σενάρια δοκιμών διείσδυσης όπου υπάρχει χειραγώγηση-μετατροπή πακέτων για την επιτυχία της επίθεσης.
- Master Mode: Η λειτουργία αυτή επιτρέπει στην κάρτα να λειτουργήσει ως ασύρματος πρόσβασης, προσομοιάζοντας ένα αυθεντικό ασύρματο δίκτυο. Αυτό είναι χρήσιμο για τη δημιουργία ελεγχόμενων περιβαλλόντων δοκιμών ή για τη διεξαγωγή επιθέσεων ψευδο-δικτύων (rogue APs).

  Υπάρχουν επίσης και οι λειτουργίες:

- Mesh Mode: Αυτή η λειτουργία επιτρέπει στην ασύρματη κάρτα να συμμετέχει σε ένα δίκτυο mesh. Σε ένα δίκτυο mesh, οι συσκευές συνδέονται η μία με την

άλλη σε ένα δίκτυο πλέγματος, διασφαλίζοντας μεγαλύτερη κάλυψη και αξιοπιστία. Η λειτουργία mesh είναι ιδανική για περιβάλλοντα όπου τα φυσικά εμπόδια εμποδίζουν τη συνεχή κάλυψη δικτύου, καθώς επιτρέπει στα δεδομένα να διαδίδονται μέσω διαφόρων διαδρομών για να φτάσουν στον τελικό προορισμό.

- Manage Mode: Αυτή η λειτουργία επιτρέπει στον χρήστη να διαχειρίζεται τη διαμόρφωση της ασύρματης κάρτας και να επιβλέπει τη λειτουργία της. Σε αυτή τη λειτουργία, ο διαχειριστής μπορεί να ορίσει παραμέτρους όπως η ισχύς σήματος, η επιλογή καναλιού, και η εφαρμογή πολιτικών ασφαλείας. Είναι κρίσιμη για τη διασφάλιση ότι η ασύρματη κάρτα λειτουργεί με βάση τις ανάγκες του δικτύου και τις απαιτήσεις ασφαλείας.

Σε αυτό το σημείο είναι αναγκαίο να αναφερθεί ένα από τα μεγαλύτερα κριτήρια τα οποία μπορούν να καθορίσουν την επιτυχία στο Wi-Fi penetration testing η οποία εξαρτάται επίσης από τη φυσική θέση του δοκιμαστή, όταν δεν μπορεί να το καλύψει η κεραία. Μια αδύναμη κάρτα μπορεί να αποδειχθεί ανεπαρκής για την αποτελεσματική λήψη σημάτων και συγκεκριμένα πακέτων και ¨ακέραιων ενεργειών¨ σε μεγάλες αποστάσεις.

Γνωστά πειράματα που έχουν διεξαχθεί με κάρτες δικτύου ALFA, οι οποίες χρησιμοποιούν chipsets της Realtek, έχουν δείξει ότι η αποτελεσματική συλλογή handshake κατά τη λειτουργία σε monitor mode εξαρτάται σημαντικά από την ισχύ του σήματος (RX power). Συγκεκριμένα, έχει παρατηρηθεί ότι μέσα από έρευνες ότι, όταν το λαμβανόμενο σήμα κυμαίνεται πέριπου στα -80 dBm με -85 dBm, η πιθανότητα επιτυχούς καταγραφής του handshake βρίσκεται πραγματικά στα όρια, πολλές φορές δε θα επιτευχθεί καθώς παίζει ρόλο και η κεραία. Παρόλο που η συλλογή handshake είναι τεχνικά εφικτή και σε χαμηλότερα επίπεδα σήματος, η επιτυχία της εξαρτάται από τον λόγο σήματος προς θόρυβο (SNR), καθώς ένα σήμα -85 dBm με χαμηλό noise floor μπορεί να είναι πιο χρήσιμο από ένα σήμα -70 dBm σε περιβάλλον με υψηλές παρεμβολές.

Επίσης, καθοριστικό ρόλο διαδραματίζουν οι υπάρχουσες παρεμβολές από άλλες ασύρματες συχνότητες που λειτουργούν στο ίδιο φάσμα, καθώς και ο συνολικός όγκος των δεδομένων που διακινούνται στο δίκτυο. Όταν η κίνηση δεδομένων είναι

περιορισμένη, η διαδικασία sniffing καθίσταται πιο δύσκολη, ιδιαίτερα σε μεγάλες αποστάσεις, καθώς μειώνεται η πιθανότητα καταγραφής πακέτων. Αυτό ισχύει ακόμα περισσότερο για τη συλλογή handshake, η οποία απαιτεί την καταγραφή συγκεκριμένων πακέτων αυθεντικοποίησης που ενδέχεται να εμφανίζονται σπάνια σε δίκτυα με χαμηλή δραστηριότητα.

Οι κάρτες ALFA με Realtek chipsets είναι δημοφιλείς στην ανάλυση ασύρματων δικτύων λόγω της υψηλής ισχύος εκπομπής (TX power) που προσφέρουν, καθώς και της υποστήριξής τους από εργαλεία penetration testing όπως το Aircrack-ng, Bettercap και Kismet. Ωστόσο, έχει παρατηρηθεί πειραματικά και είναι σημαντικό να σημειωθεί ότι τα Realtek chipsets δεν θεωρούνται πάντα η βέλτιστη επιλογή για packet injection και monitor mode, καθώς έχουν παρατηρηθεί περιορισμοί στη σταθερότητα και τη συμβατότητά τους με νεότερες εκδόσεις σε Linux Kernels. Πιο συγκεκριμένα σε νεότερες εκδόσεις των linux kernel αποτρέπει τη λειτουργία Virtual Interface – VIF λόγω αυτων των περιορισμών, για ενδεχόμενη επίθεση με συνδιασμό evil twin attack.

Αντιθέτως, είναι γνωστό στην κοινότητα οτι τα chipsets όπως Atheros (AR9271) και Mediatek (MT7612U) έχουν αποδειχθεί πιο αξιόπιστα για τέτοιες λειτουργίες, ειδικά όταν απαιτείται παρατεταμένη παρακολούθηση δικτύου και συνεχής συλλογή δεδομένων.

Επιπλέον, η απόδοση μιας κάρτας δικτύου σε monitor mode δεν εξαρτάται αποκλειστικά από την ισχύ εκπομπής της (TX power), αλλά και από την ευαισθησία λήψης (RX sensitivity), την ποιότητα της κεραίας και το περιβάλλον λειτουργίας. Αν και οι κάρτες ALFA διαθέτουν ισχυρούς πομποδέκτες (με TX power που μπορεί να φτάσει έως και τα 2000 mW σε ορισμένα μοντέλα), αυτό δεν σημαίνει απαραίτητα καλύτερη λήψη handshake, καθώς η απόσταση από το σημείο πρόσβασης (AP), οι φυσικές παρεμβολές και η κεραία που χρησιμοποιείται επηρεάζουν άμεσα την ποιότητα του σήματος.

Συμπερασματικά, η επιλογή της κατάλληλης κάρτας δικτύου για τη συλλογή handshake πρέπει να βασίζεται όχι μόνο στην υποστήριξη monitor mode και packet injection, αλλά και στη σταθερότητα του chipset, την ευαισθησία λήψης, την ποιότητα της κεραίας και τις πραγματικές συνθήκες του περιβάλλοντος λειτουργίας.

Σε συγκεκριμένο σενάριο δοκιμής επίθεσης σε δίκτυο η απόσταση γίνεται πλέον καθοριστική για την ποιότητα της διείσδυση. Συνεπώς, οι ερευνητές θα πρέπει να επιλέγουν κάρτες με ικανότητα λειτουργίας σε μεγάλες εμβέλειες, όπως επιβεβαιώνεται με τη χρήση του εργαλείου «iwconfig».

Η σωστή κατανόηση και επιλογή της διεπαφής συνήθως ρυθμίζεται στα 20 dBm, αλλά μπορεί να αυξηθεί στα 30 dBm με συγκεκριμένες μεθόδους.

Η εντολή σε Linux συστήματα ορίζεται ως :

~ sudo iwconfig wlan0 txpower 30

Ωστόσο, αυτή η ρύθμιση μπορεί να είναι παράνομη σε ορισμένες χώρες, καθώς υπερβαίνει τα επιτρεπόμενα όρια εκπομπής. Για παράδειγμα, στην Ελλάδα, τα όρια ασφαλούς έκθεσης του γενικού πληθυσμού σε ηλεκτρομαγνητικά πεδία υψηλών συχνοτήτων καθορίζονται από τον νόμο 4070/2012 και δεν πρέπει να ξεπερνούν το 70% των τιμών που ορίζονται από τις διεθνείς κατευθυντήριες γραμμές.

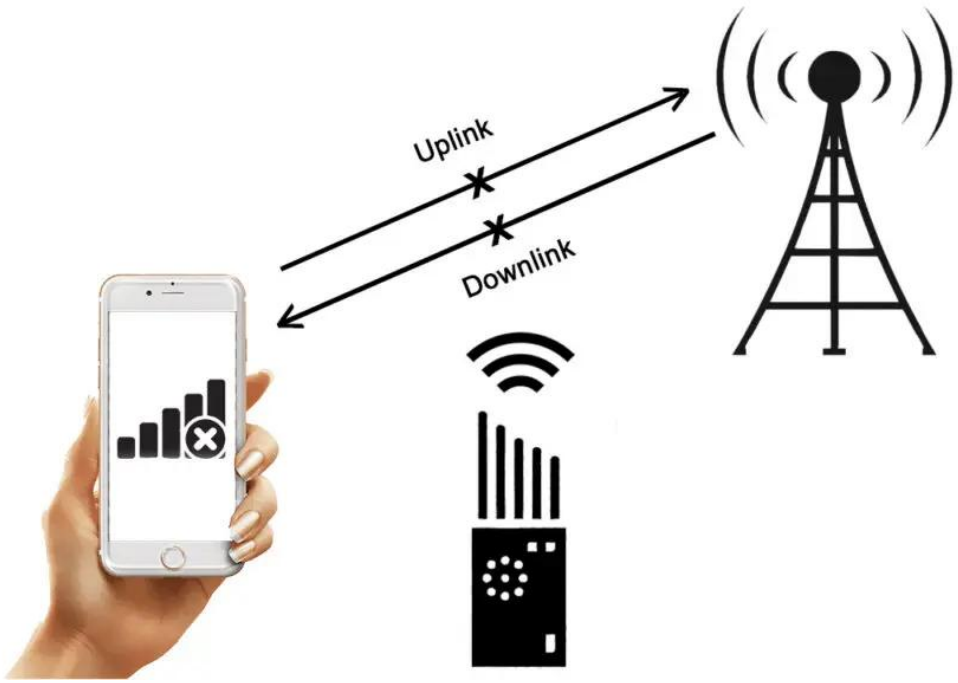
Επιπλέον, ορισμένα μοντέλα ασύρματων συσκευών ενδέχεται να μην υποστηρίζουν αυτές τις ρυθμίσεις. Ακόμη και αν το ασύρματο τσιπ είναι τεχνικά ικανό να εκπέμπει σε υψηλότερη ισχύ, ο κατασκευαστής μπορεί να μην έχει εξοπλίσει τη συσκευή με τον απαραίτητο μηχανισμό ψύξης για να διαχειριστεί με ασφάλεια την αυξημένη εκπομπή. Με αποτέλεσμα η αύξηση της ισχύος εκπομπής να οδηγήσει σε υπερθέρμανση της συσκευής, προκαλώντας πιθανές βλάβες ή μειώνοντας τη διάρκεια ζωής της.

Ωστόσο, σε ορισμένες περιπτώσεις, αυτή η αλλαγή ενδέχεται να μην έχει αποτέλεσμα, υποδηλώνοντας ότι το λειτουργικό σύστημα και συγκεκριμένα ο πυρήνας έχει τροποποιηθεί για να αποτρέπει τέτοιες ρυθμίσεις, πιθανώς για λόγους συμμόρφωσης με τους κανονισμούς ή για την προστασία του υλικού.

Η επιλογή της σωστής ασύρματης διεπαφής είναι ζωτικής σημασίας για οποιαδήποτε δοκιμή διείσδυσης σε Wi-Fi δίκτυα. Δεν αρκεί απλώς να έχουμε μια κάρτα με υψηλή ισχύ εκπομπής (TX power) η πραγματική απόδοση εξαρτάται από πολλούς παράγοντες, όπως η ευαισθησία λήψης (RX power), η ποιότητα της κεραίας, το chipset που χρησιμοποιείται και οι συνθήκες του περιβάλλοντος.

6.2 Jammers

Οι συσκευές jamming (διατάραξης σημάτων) είναι κρίσιμο εργαλείο ηλεκτρονικού πολέμου τα τελευταία χρόνια. Στόχος τους είναι η παράλυση επικοινωνιών, συστημάτων πλοήγησης ή ακόμη και οπλικών συστημάτων, μέσω εκπομπής εσκεμμένου θορύβου στις ίδιες συχνότητες με τον στόχο, ώστε να αυξάνεται το SNR και να μπλοκάρεται η σύνδεση πομπού–δέκτη. Το κεφάλαιο εξετάζει τόσο την τεχνική λειτουργία και κατηγοριοποίηση των jammers, όσο και τη στρατηγική χρήση τους, με έμφαση σε τεχνικές αντιμετώπισης μέσω TN.



Εικόνα 5: Jammering σε δίκτυο Κινητής Τηλεφωνίας

Σε γενικές γραμμές, ένας RF jammer εκπέμπει ισχυρά ηλεκτρομαγνητικά κύματα στη ζώνη συχνοτήτων του στόχου (π.χ. GSM, GPS, ραντάρ).

Έτσι, οι δέκτες (κινητά, Wi-Fi routers, τηλεχειριστήρια) δεν «ακούν» το σωστό σήμα λόγω της παρεμβολής.

- Κομβικοί παράγοντες αποτελεσματικότητας:
- Φασματική ακρίβεια: στοχεύει συγκεκριμένες ζώνες χωρίς ανεπιθύμητες παρενέργειες σε γειτονικές συχνότητες.
- Ισχύς εκπομπής: περισσότερη ισχύς αυξάνει εμβέλεια, αλλά απαιτεί περισσότερη ενέργεια και αυξάνει τον κίνδυνο εντοπισμού, ειδικά σε μικρές αποστάσεις. Έρευνες δείχνουν ότι για κάθε σενάριο υπάρχει θέση του επιτιθέμενου που μειώνει κατανάλωση και πιθανότητα ανίχνευσης με ικανοποιητικό αντίκτυπο στα δίκτυα [15].
- Δυναμική προσαρμογή (SDR): αυτόματη ανίχνευση/παρακολούθηση συχνοτήτων και προσαρμογή του παρεμβαλλόμενου σήματος ακόμη κι όταν ο στόχος αλλάζει συχνότητα (frequency hopping), εξασφαλίζοντας συνεχή παρεμπόδιση.

Οι στρατιωτικού τύπου jammers διακρίνονται σε δύο κύριες κατηγορίες. Ηλεκτρονικού Πολέμου (EW): στοχεύουν εχθρικά συστήματα όπως ραντάρ ανίχνευσης (ενδεικτικά, το ρωσικό Krasukha-4 έχει αναφερθεί ότι διαταράσσει ακόμη και δορυφορικές επικοινωνίες σε μεγάλη ακτίνα, π.χ. ~300 km). Κατευθυντικής Ενέργειας (DEW): αξιοποιούν λέιζερ ή μικροκύματα για φυσική καταστροφή ηλεκτρονικών (π.χ. το αμερικανικό CHAMP).

Εικόνα 6: Κινητό σύστημα jamming (EW) με διπλές κατευθυντικές κεραίες σε ρυμουλκούμενη πλατφόρμα.

(πηγή: https://www.afmc.af.mil/News/Article-Display/Article/3094367/746th-test-squadron-develops-high-power-jammer-system-for-continuous-tracking/)

Στη συνέχεια, εξετάζονται τεχνικές αντι-jamming με Τεχνητή Νοημοσύνη: ανίχνευση προτύπων παρεμβολής, προσαρμοστική επιλογή καναλιών/διαμόρφωσης και βελτιστοποίηση θέσης/ισχύος για διατήρηση αξιόπιστης επικοινωνίας σε δυναμικά περιβάλλοντα.

Παραπάνω αναφερθήκαμε για στρατηγική χρήση σε σύγχρονους πολέμους ένα πολύ επίκαιρο θέμα με μια μικρή ανάλυση, αλλά ας το αναλύσουμε περισσότερο όμως με γνωστά παραδείγματα καθώς είναι τεχνολογίες αιχμής.

Αρχικά η στρατιωτική αξία των jammers εκδηλώνεται σε δύο επίπεδα:

Στο αμυντικό (προστασία ευαίσθητων στόχων) και στο επιθετικό (παράλυση εχθρικής υποδομής). Παραδείγματα από πρόσφατες συρράξεις είναι:

Α. Πόλεμος Ουκρανίας-Ρωσίας (2022-σήμερα 2025):

Η Ρωσία έχει αναπτύξει ποιοτικά ολοκληρωμένα συστήματα ηλεκτρονικού πολέμου σε όλη τη γραμμή μετώπου της. Τα συστήματα της Murmansk-BN και Leer-3 διατάραξαν τα δορυφορικά συστήματα Starlink της αμερικάνικης εταιρίας SpaceX του Elon Musk, μειώνοντας έτσι ην αποτελεσματικότητα των ουκρανικών μη επανδρωμένων αεροσκαφών (UAVs).

Σε απάντηση προς τη Ρωσία, η Ουκρανία άμεσα με τη βοήθεια της δύσης ενσωμάτωσε εφεδρικά αναλογικά συστήματα επικοινωνίας και χρησιμοποίησε drones με αυτόνομη πλοήγηση, με τη βοήθεια της τεχνητής νοημοσύνης (AI-based), ανθεκτικά σε διαταραχές.

Β. Πόλεμος Ναγκόρνο-Καραμπάχ (2020)

Τα αζερικά στρατεύματα ανέπτυξαν το τουρκικό σύστημα Koral, που απενεργοποίησε τα αρμενικά ραντάρ και δορυφορικές επικοινωνίες, επιτρέποντας την ανεμπόδιστη προέλαση των Bayraktar TB2 drones. Δημιουργούσε σημαντική υπεροχή στην περιοχή με την δική τους τεχνολογική ανάπτυξη.

Εικόνα 7: Φορητό σύστημα **RF jamming** για προστασία από IED/DRONE απειλές (πηγή: https://defensescoop.com/2023/09/15/army-awards-contract-for-dismounted-electronic-jammer/)

Γ. Αντιμετώπιση Μη Επανδρωμένων Συστημάτων (UAVs)

Στην Υεμένη, τα χουθικά στρατεύματα χρησιμοποιούν εμπορικούς jammer (π.χ., Skygrabber) για διατάραξη των σηματοδοτήσεων GPS των saudic αεροσκαφών MQ-9 Reaper, αναγκάζοντάς τα σε αναγκαστική προσγείωση. Η συγκεκριμένη τεχνική βρίσκεται παρόν στις τελευταίες τρόπους επίθεσεις. Είναι ενδιαφέρων να δούμε πιο αναλυτικά με μεγαλύτερη λεπτομέρεια αυτήν την επίθεση καθώς είναι τεχνολογίες αιχμής.

Το GPS spoofing είναι μια επίθεση κατά την οποία ο επιτιθέμενος παράγει και εκπέμπει ψευδή δορυφορικά σήματα, με σκοπό να παραπλανήσει τον δέκτη ενός UAV ώστε να "νομίζει" ότι βρίσκεται σε λάθος θέση [14]. Ο επιτιθέμενος συγχρονίζεται αρχικά με τα αυθεντικά σήματα, και στη συνέχεια εκπέμπει πλαστά σήματα με ελαφρώς υψηλότερη ισχύ, με αποτέλεσμα ο δέκτης να τα “κλειδώνει” ως έγκυρα [14]. Αυτό οδηγεί το drone

να τροποποιεί την πορεία του, με αποτέλεσμα πιθανές εσφαλμένες πορείες ή ακόμη και ανεπιθύμητες προσγειώσεις.

Αναλυτικά η επίθεση υλοποιείται με τη χρήση πλατφορμών λογισμικού-οριζόμενου ραδιοφώνου (SDR) σε συνδυασμό με ένα εξειδικευμένο λογισμικό που μπορεί να δημιουργεί πλαστά σήματα, η αλλιώς γνωστό και ως "spoofing". Από την άλλη πλευρά ο επιτιθέμενος συλλέγει τα αυθεντικά δεδομένα, υπολογίζει τη λύση θέσης του UAV και, μέσω της αύξησης της ισχύος των πλαστών σημάτων για να υπερισχύουν και να σιγουρευτούμεν οτί τα λαμβάνει, αναγκάζει το drone να προσαρμόσει την πορεία του βάσει των ψευδών δεδομένων που μόλις έλαβε [14].

6.2.1 Ανίχνευση και Αντιμετώπιση του Jamming με Τεχνητή Νοημοσύνη

Η ενσωμάτωση τεχνολογιών τεχνητής νοημοσύνης σε μη επανδρωμένα συστήματα (UAV) έχει ανοίξει το δρόμο για την ανάπτυξη καινοτόμων μεθόδων εντοπισμού και αντιμετώπισης επιθέσεων jamming. Συγκεκριμένα, μεταξύ των προσεγγίσεων αυτών περιλαμβάνονται:

Ανίχνευση Ανωμαλιών με Μη Επιβλεπόμενη Μάθηση Μέσω της εφαρμογής τεχνικών μη επιβλεπόμενης μάθησης, όπως ο One-Class SVM και οι Autoencoders, τα συστήματα καταγράφουν το τυπικό μοτίβο των εισερχόμενων σημάτων. Σε περιπτώσεις όπου παρατηρείται απότομη αύξηση του signal-to-noise ratio ή ασυνήθιστες μεταβολές στην ισχύ, εντοπίζονται αυτόματα αποκλίσεις που μπορεί να υποδηλώνουν επίθεση jamming [16].

Εποπτευόμενη Μάθηση για Ταξινόμηση Σημάτων Με τη βοήθεια προκαταρτισμένων μοντέλων, όπως τα Random Forest και τα νευρωνικά δίκτυα, τα συστήματα είναι σε θέση να διακρίνουν τα εισερχόμενα σήματα, χαρακτηρίζοντάς τα ως «κανονικά» ή «παρεμβαλλόμενα». Μέσα από την ανάλυση δεδομένων από προγενέστερες επιθέσεις jamming, τα μοντέλα αναγνωρίζουν χαρακτηριστικά μοτίβα που υποδεικνύουν παρεμβολή, προσφέροντας έτσι έγκαιρη ειδοποίηση [17]. Τα UAV μπορούν να

υιοθετήσουν αλγορίθμους ενισχυτικής μάθησης για να ανταποκρίνονται αυτόματα σε περιβάλλοντα που πλήττονται από jamming.

Μετά την ανίχνευση παρεμβολής, το σύστημα έχει τη δυνατότητα να:

Μεταβεί αυτόματα σε μια συχνότητα επικοινωνίας με μικρότερη ευπάθεια, και

Ενεργοποιήσει εναλλακτικές μεθόδους πλοήγησης (π.χ. χρήση δεδομένων από INS ή οπτικές μετρήσεις) για να διατηρήσει τη σωστή πορεία του UAV [18].

Μέσω αυτής της δυναμικής προσαρμογής, που βασίζεται στην ενισχυτική μάθηση, το UAV «μαθαίνει» από κάθε επίθεση και επιλέγει την καταλληλότερη στρατηγική αντιμετώπισης σε πραγματικό χρόνο [18][19].

Συγχώνευση Αισθητήρων και Βαθιά Μάθηση Η συνδυασμένη αξιοποίηση δεδομένων από διάφορους αισθητήρες (όπως GPS, IMU, και οπτικά συστήματα) μέσω τεχνικών sensor fusion ενισχύει την ικανότητα ανίχνευσης. Επιπλέον, οι αλγόριθμοι βαθιάς μάθησης που εφαρμόζονται στην ανάλυση αυτών των δεδομένων συγκρίνουν τις πληροφορίες από διαφορετικές πηγές, εντοπίζοντας τυχόν ασυμφωνίες που μπορεί να υποδηλώνουν επίθεση jamming. Με αυτόν τον τρόπο, μειώνονται τα ψευδώς θετικά αποτελέσματα και βελτιώνεται η ακρίβεια της ανίχνευσης σε πραγματικό χρόνο [20][21].

Σε πρόσφατες στρατιωτικές επιχειρήσεις και περιβάλλοντα ηλεκτρονικού πολέμου, συστήματα που συνδυάζουν τεχνητή νοημοσύνη και sensor fusion έχουν αποδειχθεί κρίσιμα για την αντιμετώπιση του jamming. Για παράδειγμα, σε εργαστηριακές δοκιμές και πραγματικές επιχειρήσεις, UAV εξοπλισμένα με AI-based συστήματα εναλλαγής καναλιών και αυτόματης επιλογής εφεδρικών πηγών πλοήγησης κατάφεραν να διατηρήσουν τη συνέχεια της επικοινωνίας τους παρά την παρουσία έντονων επιθέσεων jamming [17][20]. Αυτές οι λύσεις αποδεικνύουν ότι η ενσωμάτωση της τεχνητής νοημοσύνης επιτρέπει την αυτόματη προσαρμογή σε δυναμικά περιβάλλοντα, όπου ο χρόνος αντίδρασης είναι κρίσιμος για την επιτυχή ολοκλήρωση των αποστολών.

Συμπεράσματα:

Η χρήση της τεχνητής νοημοσύνης για την αντιμετώπιση των επιθέσεων jamming σε UAV προσφέρει μια ολοκληρωμένη λύση, η οποία συνδυάζει ανίχνευση ανωμαλιών,

εποπτευόμενη μάθηση, reinforcement learning και sensor fusion. Και αυτή την στιγμή οι μεγαλύτερες εταιρίες χρηματοδοτούντε για την ανάπτυξη λύσεων και γενική ανάπτυξη της. Μέσω των παραπάνω τεχνολογιών, τα UAV μπορούν να ανιχνεύουν σε πραγματικό χρόνο την παρουσία παρεμβολής, να προσαρμόζουν αυτόματα τις παραμέτρους λειτουργίας τους και να διατηρούν την επικοινωνία και την πλοήγησή τους, ακόμη και σε περιβάλλοντα υψηλού ραδιολογικού θορύβου. Η ενσωμάτωση αυτών των μεθόδων μειώνει σημαντικά τα ρίσκα από jamming επιθέσεις και διασφαλίζει την αξιοπιστία και την ασφάλεια των UAV σε στρατιωτικές και πολιτικές εφαρμογές.

6.3 De-Authentication Attack

Τα ασύρματα δίκτυα εδώ και πολύ καιρό έχουν γίνει απαραίτητα για την καθημερινή μας επικοινωνία, όμως η ασφάλειά τους συνεχίζει να είναι ένα σημαντικό πρόβλημα. Μία από τις επιθέσεις που ξεχωρίζει, κυρίως λόγω της απλότητας και της αποτελεσματικότητάς της, είναι η επίθεση αποσύνδεσης (de-authentication). Η συγκεκριμένη επίθεση εκμεταλλεύεται ευπάθειες του προτύπου IEEE 802.11.

Για να το κατανοήσυμε ας το πιάσπυμε από την αρχή. Η πρώτη μέθοδος κρυπτογράφησης που χρησιμοποίησαν τα ασύρματα δίκτυα ήταν το Wired Equivalent Privacy (WEP), το οποίο δημιούργησε ο γνωστός φορέας IEEE. Ωστόσο, είχε αρκετές αδυναμίες που το έκαναν ευάλωτο σε επιθέσεις. Τα προβλήματα αυτά αντιμετωπίστηκαν στην συνέχεια με την ανάπτυξη πιο ισχυρών μηχανισμών κρυπτογράφησης στο πρότυπο IEEE 802.11, που εισήγαγε και τη δυνατότητα πιστοποίησης των χρηστών, ένα στοιχείο που έλειπε από το WEP.

Παρ’ όλα αυτά, ακόμη και το βελτιωμένο πρότυπο 802.11 προστατεύει μόνο τα δεδομένα, αφήνοντας εκτεθειμένα τα πλαίσια διαχείρισης και ελέγχου. Αυτό δίνει την ευκαιρία σε κακόβουλους χρήστες να πραγματοποιούν επιθέσεις τύπου DoS, όπως η αποσύνδεση (de-authentication).

Πως και Γιατί;

Τα συγκεκριμένα πλαίσια χρησιμοποιούνται για την αρχικοποίηση, τη διατήρηση και την ανταλλαγή πληροφοριών ανάμεσα στις συσκευές, και μπορούν εύκολα να αξιοποιηθούν για τέτοιες επιθέσεις.

Αν και οι επιθέσεις αυτές περιορίζονται με βελτιώσεις στην κρυπτογράφηση, αλλαγές στα πρωτόκολλα, αναβαθμίσεις στο λογισμικό και στο υλικό, μια ιδιαίτερα αποτελεσματική λύση προσφέρουν τα Συστήματα Εντοπισμού Εισβολών (IDS) που βασίζονται στη μηχανική μάθηση. Χρησιμοποιώντας αλγορίθμους ταξινόμησης, όπως πιθανοτικούς κανόνες, δέντρα αποφάσεων ή μεθόδους πυρήνων, μπορεί κανείς να συγκρίνει εύκολα την αποτελεσματικότητά τους στην ανίχνευση επιθέσεων. Σύμφωνα με πειραματικά αποτελέσματα, τέτοια συστήματα εντοπισμού εισβολών που βασίζονται στη μηχανική μάθηση πετυχαίνουν πολύ υψηλά ποσοστά επιτυχίας, αγγίζοντας έως και το 96%, καθιστώντας την τεχνητή νοημοσύνη αναγκαία λύση.

6.3.1 Πλαίσια διαχείρισης (Management Frames) των ασύρματων δικτύων

Όπως αναφέρθηκαμε και στο προηγούμενο κεφάλαιο στα ασύρματα τοπικά δίκτυα (WLANs), τα οποία λειτουργούν σύμφωνα με το πρότυπο IEEE 802.11, τα πλαίσια διαχείρισης (Management Frames) έχουν ως ρόλο την εγκατάσταση, τη διατήρηση και τη διακοπή της σύνδεσης ανάμεσα σε έναν σταθμό (STA) και ένα σημείο πρόσβασης (AP) [1]. Ωστόσο, είναι σημαντικό να σημειωθεί ότι στα αρχικά στάδια του προτύπου 802.11, αλλά και στις πρώτες εκδόσεις των προτύπων ασφαλείας WPA και WPA2 (οχι στο WPA3 γιατί ελέγχοναται), τα συγκεκριμένα πλαίσια διαχείρισης δεν προστατεύονταν μέσω κρυπτογράφησης, κάτι που άφηνε το δίκτυο εκτεθειμένο σε σοβαρές ευπάθειες και παραβιάσεις ασφάλειας [2].

Η επίθεση αποσύνδεσης (γνωστή ως Deauthentication ή deauth attack) εκμεταλλεύεται ακριβώς αυτήν την αδυναμία προστασίας των πλαισίων διαχείρισης. Συγκεκριμένα, ο επιτιθέμενος αποστέλλει τα πλαστά (spoofed) πλαίσια που κατασκεύασε (δηλαδή πακέτα υπεύθυνα να ενημερώσουν για την αποσύνδεση) με στόχο την ξαφνική και αδικαιολόγητη αποσύνδεση των χρηστών (STA) από το σημείο πρόσβασης (AP), χωρίς οι χρήστες να ενημερώνονται για τον λόγο της αποσύνδεσης. Αυτό έχει ως αποτέλεσμα

είτε τη διακοπή της σύνδεσης είτε τη δημιουργία ευνοϊκών συνθηκών για πιο προηγμένες επιθέσεις, όπως την επίθεση Evil Twin ή την υποχρεωτική σύνδεση των χρηστών σε κακόβουλα σημεία πρόσβασης (rogue AP) [3].

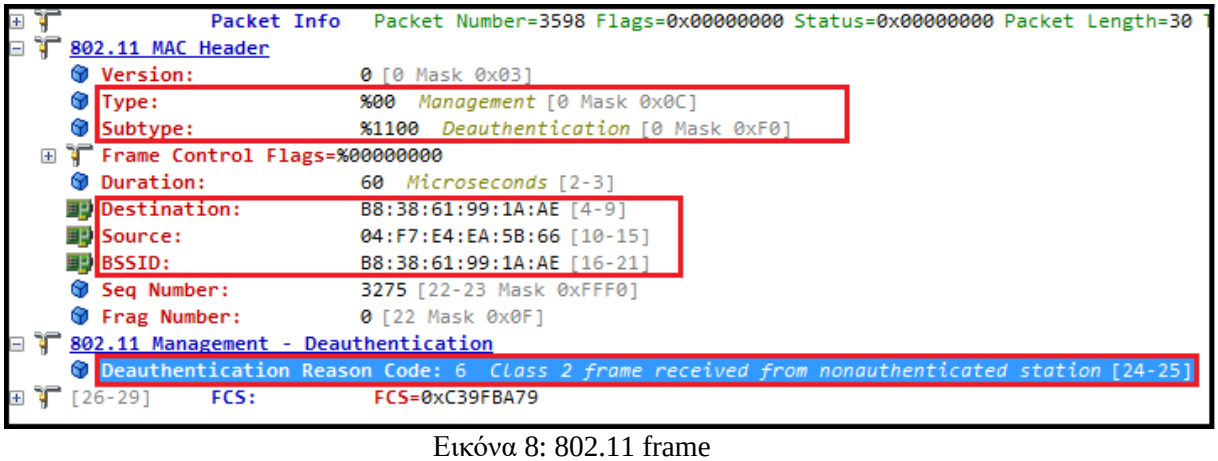
6.3.2 Δομή και Λειτουργία του Deauthentication Frame

Σύμφωνα με το πρότυπο IEEE 802.11, το πλαίσιο Deauthentication ανήκει στην κατηγορία των πλαισίων διαχείρισης (Management Frames) και συγκεκριμένα στο υποείδος των Authentication Frames [4]. Η βασική λειτουργία του είναι να ενημερώνει τον σταθμό του ότι τερματίζεται η διαδικασία αυθεντικοποίησης, με αποτέλεσμα ο σταθμός να «χάνει» την πρόσβαση στο δίκτυο.

Ποια είναι η δομή αυτού του Frame όμως;

Ας τα εξετάσουμε με λεπτομέρεια.

Frame Control: Περιέχει πληροφορίες για τον τύπο του πλαισίου (Management, Control ή Data) και διάφορα flag bits (π.χ. προστατευμένο πλαίσιο, retry κ.ά.).



Εικόνα 8: 802.11 frame

Το πλαίσιο Deauthentication ακολουθεί την τυπική δομή ενός 802.11 Management Frame και περιλαμβάνει τα παρακάτω πεδία:

- MAC Header (Επικεφαλίδα MAC 802.11)
- Type: Ορίζεται ως Management Frame (00), που σημαίνει ότι το πλαίσιο χρησιμοποιείται για διαχείριση συνδέσεων.

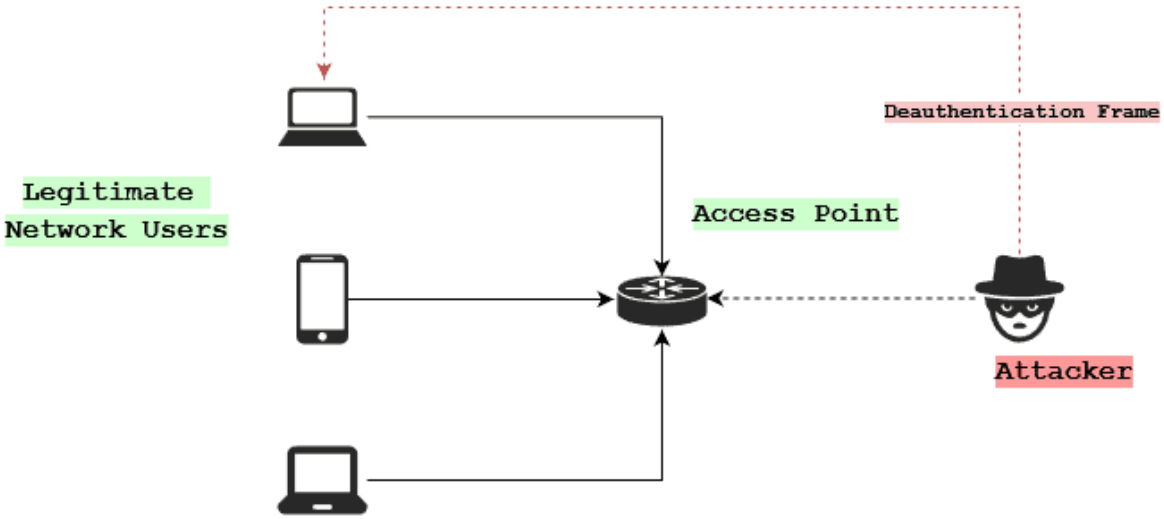
- Subtype: Έχει την τιμή 0xC (12), που αντιστοιχεί στο Deauthentication Frame.
- Frame Control Flags: Περιέχει πληροφορίες για τον τύπο και τη δομή του πλαισίου.
- Διευθύνσεις MAC
- Destination: Η MAC διεύθυνση της συσκευής-παραλήπτη (π.χ. του θύματος).
- Source: Η MAC διεύθυνση της συσκευής που αποστέλλει το πλαίσιο (π.χ. του AP).
- BSSID: Η MAC διεύθυνση του σημείου πρόσβασης (AP) στο οποίο ήταν συνδεδεμένος ο πελάτης.
- Sequence Number: Χρησιμοποιείται για τον αριθμό της ακολουθίας του πλαισίου.

Deauthentication Fixed Parameters

- Reason Code: Ένας κωδικός που υποδεικνύει τον λόγο αποσύνδεσης. Στην εικόνα, ο Reason Code: 6 σημαίνει ότι ένα Class 2 frame ελήφθη από μη αυθεντικοποιημένη συσκευή, κάτι που μπορεί να συμβεί σε μια επίθεση deauthentication.
- Frame Check Sequence (FCS): Χρησιμοποιείται για την ανίχνευση σφαλμάτων στο πλαίσιο.
-

6.3.3 Η επίθεση Deauthentication στη πράξη

Η **Deauthentication Attack** είναι από τις πιο διαδεδομένες επιθέσεις σήμερα, επειδή εκμεταλλεύεται την έλλειψη επαλήθευσης/κρυπτογράφησης στα management frames και υλοποιείται πολύ εύκολα (ακόμη και από αρχάριους). Είναι κομβική για την έρευνά μας: εφαρμόζεται γρήγορα και έχει έντονο αντίκτυπο.



Εικόνα 9: Deauthentication Attack

Βασικά βήματα επίθεσης

1. Sniffing: συλλογή MAC διευθύνσεων σταθμών και AP με Wireshark/tcpdump/Aircrack-ng.
2. Spoofing: δημιουργία πλαστών deauth frames· ο δράστης συνήθως «παριστάνει» το AP για να φαίνεται ότι το ίδιο το δίκτυο αποσυνδέει χρήστες [3].
3. Flooding: μαζική αποστολή των ψευδεπίγραφων πλαισίων· οι σταθμοί δεν ξεχωρίζουν άμεσα την προέλευση και αποσυνδέονται.
4. Διακοπή & εκμετάλλευση: οι χρήστες προσπαθούν να επανασυνδεθούν· εδώ συχνά ακολουθούν Evil Twin ή Man-in-the-Middle (π.χ. ARP poisoning).

Επιπτώσεις & κίνητρα

DoS/υποβάθμιση υπηρεσίας: ο χρήστης χάνει ακαριαία τη σύνδεση με το AP/Internet, κάτι κρίσιμο σε εταιρικά περιβάλλοντα ή εφαρμογές που απαιτούν αδιάλειπτη συνδεσιμότητα [7].

Παράθυρο ευπάθειας: στη φάση επανασύνδεσης αυξάνονται οι πιθανότητες για social engineering ή σύνδεση σε πλαστό AP, με κίνδυνο υποκλοπής διαπιστευτηρίων.

Παραβίαση απορρήτου: συχνός συνδυασμός με MAC spoofing και MITM ώστε να κρυφτούν ίχνη και να παρακολουθηθεί/τροποποιηθεί η κίνηση.

Προστασία & αντιμετώπιση

- PMF / IEEE 802.11w: προστατευμένα management frames (υπογραφή/κρυπτογράφηση) μπλοκάρουν την εύκολη παραποίηση [9].
- WPA3 + SAE: καθιστά υποχρεωτικό το PMF και ενισχύει την αρχική αυθεντικοποίηση, μειώνοντας δραστικά τα deauth.
- Wireless IDS/IPS: εντοπίζουν spikes σε management frames και μπορούν να απομονώσουν επιτιθέμενους.
- MAC filtering: μόνο συμπληρωματικό μέτρο· οι MAC διευθύνσεις πλαστογραφούνται εύκολα.
- Συνεχής παρακολούθηση & logging: ανίχνευση ανωμαλιών (απότομη αύξηση deauth/disassoc) και άμεσος συναγερμός.

6.3.4 Χρήση Τεχνικών Μηχανικής Μάθησης για Αναγνώριση και Μετριασμό

Η μηχανική μάθηση αποτελεί ένα από τα πιο ισχυρά εργαλεία αυτή την στιγμή για την ανάλυση μεγάλων όγκων δεδομένων δικτύου καθώς δεν είναι καθόλου εύκολα διαχειρίσιμα από τον άνθρωπο, επιτρέποντας την ανίχνευση ύποπτων μοτίβων μέσα σε αχανές βάσεις δεδομένων που μπορεί να υποδεικνύουν επιθέσεις deauthentication attacks. Είναι πολύ δύσκολο να τις διαχειριστεί ο άνθρωπος σε ένα σύντομο χρονικό όριο, αλλά και να μπορούσε είναι σίγουρο ότι θα οδηγούνταν στο γνωστό burn out, που παθαίνουν οι αναλυτές δικτύου.

Από την άλλη ως μια βοήθεια, υπάρχουν τεχνικές που εφαρμόζονται με επιτυχία όπως η ανίχνευση ανωμαλιών στη ροή δεδομένων του δικτύου (anomaly detection) και η εποπτευόμενη μάθηση (supervised learning) έχουν χρησιμοποιηθεί για την αναγνώριση τέτοιων επιθέσεων. Καθιστώντας το ένα πολύ σημαντικό εργαλείο αφού η αποτελεσματικότητα της διαχείρισης ρίσκου, και απάντησης περιστατικού γίνεται πιο άμεσα σε κρίσιμες λεπτά της επίθεσης για την αντιμετώπιση της.

Για παράδειγμα, η ανάλυση της κυκλοφορίας στο δίκτυο μπορεί να αποκαλύψει απότομες αυξήσεις στα πακέτα deauthentication ή ασυνήθιστες συμπεριφορές που διαφέρουν από τη φυσιολογική λειτουργία του δικτύου. Μέσω της εκπαίδευσης μοντέλων μηχανικής μάθησης σε πραγματικά δεδομένα, μπορούμε να εντοπίζουμε

τέτοιες επιθέσεις με μεγαλύτερη ακρίβεια και ταχύτητα, πριν αυτές προκαλέσουν σοβαρά προβλήματα στη λειτουργία του δικτύου.

Μετριασμός Επιθέσεων Deauthentication:

Εκτός από την αναγνώριση των επιθέσεων, οι τεχνικές μηχανικής μάθησης μπορούν να συμβάλουν στην ανάπτυξη μηχανισμών άμυνας (δηλαδή αυτοματοποιημένης απάντησης) ενάντια στις επιθέσεις deauthentication. Ένας από τους τρόπους αντιμετώπισης είναι η αυτόματη προσαρμογή των ρυθμίσεων ασφαλείας του δικτύου με βάση την ανίχνευση ύποπτων δραστηριοτήτων.

Επιπλέον, η ενισχυτική μάθηση (reinforcement learning) μπορεί να βοηθήσει ακόμη περισσότερο τα συστήματα ασφαλείας να αναγνωρίζουν νέες και πιο εξελιγμένες μορφές επιθέσεων, επιτρέποντας τη συνεχή προσαρμογή και βελτίωση της άμυνας του δικτύου. Ένας άλλος πιθανός μηχανισμός είναι η απομόνωση των κακόβουλων συσκευών το λεγόμενο “Isolation” με τον αγγλικό τεχνικό όρο, αποκλείοντάς τες προσωρινά ή μόνιμα από το δίκτυο για την αποτροπή περαιτέρω επιθέσεων, και το πιο σημαντικό για να αποφευχθεί η μεταπήδηση του επιτιθέμενου σε άλλη συσκευή στο δίκτυο.

Προκλήσεις και Μελλοντικές Κατευθύνσεις:

Παρά τις σημαντικές δυνατότητες της μηχανικής μάθησης στην ανίχνευση και τον μετριασμό των επιθέσεων deauthentication, υπάρχουν αρκετές προκλήσεις που πρέπει να αντιμετωπιστούν. Μία από τις βασικότερες είναι η ανάγκη για μεγάλα και ποικίλα σύνολα δεδομένων, ώστε τα μοντέλα να μπορούν να εκπαιδευτούν με ακρίβεια και να γενικεύουν σωστά σε διαφορετικά περιβάλλοντα δικτύου. Γενικότερα η ακρίβεια στην εκπαίδευση των δεδομένων είναι κυρίως ο παράγοντας που θα καθορίσει την αποτελεσματικότητα της αυτοματοποιημένης ακριβείς απάντησης.

Επιπλέον, να αναφέρουμε και τις adversarial attacks, πολύ επικίνδυνες επιθέσεις που στοχεύουν τα ίδια τα συστήματα μηχανικής μάθησης, αποτελούν μια ανερχόμενη απειλή που πρέπει να ληφθεί υπόψη κατά την ανάπτυξη αμυντικών μηχανισμών. Ο κίνδυνος αυτός δηλώνει παρόν και για αυτό η συνεχής έρευνα στον τομέα της ασφαλούς μηχανικής μάθησης (secure machine learning) είναι απαραίτητη για την κατασκευή πιο ανθεκτικών αλγορίθμων ενάντια σε ύποπτες κακόβουλες προς αυτά επιθέσεις .

6.4 KRACK – Key Reinstallation Attack

Η KRACK (Key Reinstallation Attack) παρουσιάστηκε το 2017 από τον Mathy Vanhoef και αποκάλυψε θεμελιώδη αδυναμία στον σχεδιασμό του WPA2. Δεν ήταν σφάλμα υλοποίησης συγκεκριμένου κατασκευαστή, αλλά προβληματικό σημείο του ίδιου του πρωτοκόλλου. Η επίθεση στοχεύει το 4-way handshake. Ο δράστης εξαναγκάζει επανεκπομπή του Message 3, ώστε ο client να επανεγκαταστήσει το ίδιο PTK και να μηδενίσει nonce/replay counter. Έτσι επαναχρησιμοποιείται ο ίδιος keystream κάτι που ακυρώνει τη μοναδικότητα της κρυπτογράφησης ανά σύνδεση.

Συνέπειες

- Υποκλοπή και αποκρυπτογράφηση πακέτων.
- Εισαγωγή/τροποποίηση δεδομένων (packet injection, session hijacking).
- Μεγαλύτερη έκθεση σε Android/Linux λόγω τρόπου λειτουργίας του WPA supplicant.

Αντιμετώπιση

- Patches σε λειτουργικά και firmware (να αγνοούν επαναλήψεις του M3 και να μην επαναμηδενίζουν counters).
- Αναβάθμιση σε WPA3/SAE, που κλείνει τον συγκεκριμένο δρόμο επίθεσης και σκληραίνει τη διαδικασία αυθεντικοποίησης.

Με λίγα λόγια, η KRACK εκμεταλλεύεται την επανεγκατάσταση κλειδιού στο handshake τα patches μειώνουν τον κίνδυνο στο WPA2, ενώ το WPA3 δίνει οριστική λύση.

6.5 Κακόβουλα Σημεία Πρόσβασης (Rogue Access Points)

Τα κακόβουλα σημεία πρόσβασης (Rogue Access Points) είναι μη εξουσιοδοτημένες και συχνά παράνομα εγκατεστημένες συσκευές δικτύου, οι οποίες στήνονται από επιτιθέμενους με σκοπό να παραπλανήσουν χρήστες ώστε να συνδεθούν σε αυτές, θεωρώντας ότι αποτελούν αξιόπιστο μέρος του δικτύου. Αυτές οι συσκευές μπορεί να μιμούνται τα χαρακτηριστικά ενός νόμιμου Wi-Fi δικτύου, χρησιμοποιώντας το ίδιο SSID (όνομα δικτύου) ή ακόμα και παρόμοια φυσική τοποθέτηση για να ενισχύσουν την απάτη.

Μόλις ο ανυποψίαστος χρήστης συνδεθεί σε ένα τέτοιο σημείο πρόσβασης, ο επιτιθέμενος αποκτά δυνατότητα παρακολούθησης και ενδεχομένως αλλοίωσης της δικτυακής κυκλοφορίας. Αυτό σημαίνει ότι μπορεί να καταγράψει ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης ή προσωπικές πληροφορίες, να ανακατευθύνει τον χρήστη σε κακόβουλες ιστοσελίδες ή ακόμη και να εισάγει αλλοιωμένα δεδομένα στην επικοινωνία.

Η ύπαρξη rogue access points αποτελεί μια σοβαρή απειλή για την ασφάλεια των ασύρματων δικτύων, ιδίως σε περιβάλλοντα υψηλής επισκεψιμότητας, όπως πανεπιστήμια, καφετέριες ή αεροδρόμια, όπου οι χρήστες συχνά συνδέονται σε δημόσια δίκτυα χωρίς να επαληθεύουν την αυθεντικότητα του παρόχου.

6.6 Επίθεση Evil Twin Attack

Η επίθεση τύπου Evil Twin είναι μια πολύ γνωστή multi layer επίθεση και βασίζεται στη δημιουργία ενός παραπλανητικού κακόβουλου σημείου πρόσβασης (rogue access point), το οποίο μιμείται σχεδόν στο 100% ένα νόμιμο και αξιόπιστο δίκτυο Wi-Fi στον ίδιο χώρο με αυτό. Ο επιτιθέμενος επιλέγει προσεκτικά τα στοιχεία του αυθεντικού δικτύου που θέλει να μιμηθεί, όπως το όνομα (SSID), τον τύπο ασφάλειας και ακόμη και τη φυσική τοποθεσία, ώστε να κατασκευάσει έναν «κακόβουλο δίδυμο» του πραγματικού access point με σκοπό την εξαπάτηση μέσω ψαρέματος.

Ως αποτέλεσμα στην συνέχεια οι ανυποψίαστοι χρήστες που βρίσκονται στην εμβέλεια αυτού του ψεύτικου AP συνδέονται σε αυτό χωρίς να αντιληφθούν τη διαφορά με το πραγματικό. Συνήθως όμως για να μην συνδεθεί το θύμα στο πραγματικό AP ο επιτιθέμενος παράλληλα εκτελεί επίθεση Deauthentication ενάντια στο πραγματικό ώστε

να μην φαίνεται σαν επιλογή στην εμβέλεια του θύματος. Με αποτέλεσμα η επιλογή να γίνει μια για το θύμα, αυτή του κακόβουλου χρήστη. Είναι σχεδόν ακατόρθωτο να το καταλάβει ένας κοινός χρήστης, χρειάζονται οι γνώσεις αλλά και η καχυποψία για να αντιληφθεί τη διαφορά πριν συνδεθεί.

Γιατί πριν όμως συνδεθεί;

Διότι από τη στιγμή της σύνδεσης, ο επιτιθέμενος έχει τη δυνατότητα να υποκλέψει όλη την στεγνή κυκλοφορία δεδομένων, να τροποποιήσει το περιεχόμενο των επικοινωνιών, ή ακόμη να ανακατευθύνει τον χρήστη σε πλαστές ιστοσελίδες για περαιτέρω επιθέσεις, όπως κλοπή διαπιστευτηρίων ή εγκατάσταση κακόβουλου λογισμικού.

Μια τέτοια επίθεση είναι άκρως επικίνδυνη διότι δεν απαιτεί φυσική παραβίαση του δικτύου, αλλά εκμεταλλεύεται την εμπιστοσύνη του χρήστη και την έλλειψη ελέγχου ταυτότητας σε δημόσια Wi-Fi. Λόγω της δυσκολίας ανίχνευσής της, αποτελεί ένα από τα πιο διαδεδομένα μέσα για επιθέσεις τύπου "άνθρωπος στη μέση" (Man-in-the-Middle – MitM) στα ασύρματα δίκτυα.

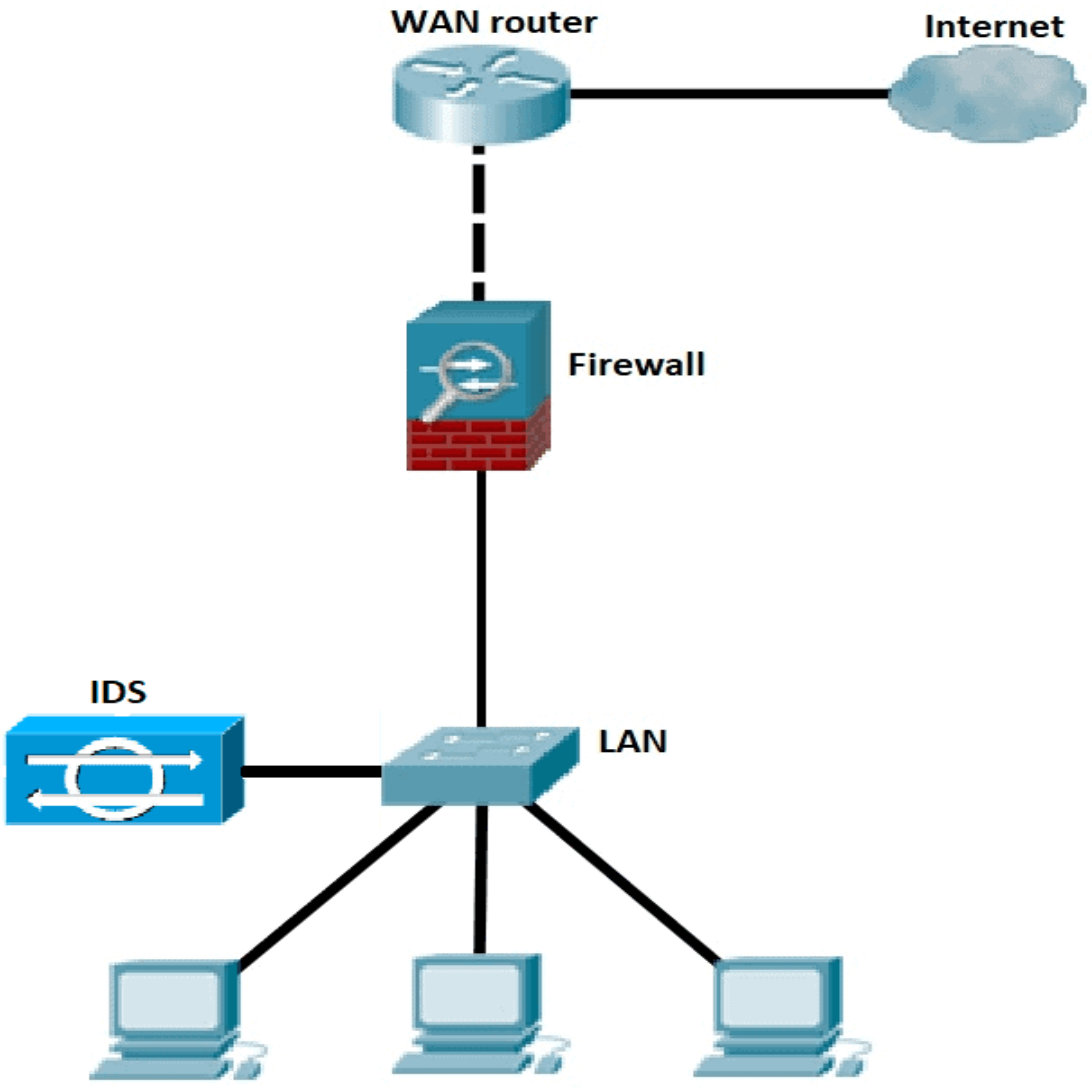
7 Ανάπτυξη και Εφαρμογή Συστήματος Ανίχνευσης Επιθέσεων (Α' ΜΕΡΟΣ)

7.1 Ορισμός και Λειτουργία των IDS

Τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDS) αποτελούν ένα από τα πλέον θεμελιώδη εργαλεία στη σύγχρονη αρχιτεκτονική κυβερνοασφάλειας. Ο βασικός τους στόχος είναι η παρακολούθηση της δραστηριότητας ενός συστήματος ή δικτύου και η αναγνώριση ενδεχόμενων παραβιάσεων πολιτικών ασφαλείας ή επιθέσεων, είτε σε πραγματικό χρόνο είτε εκ των υστέρων [26]. Η σημασία τους αυξάνεται

κατακόρυφα σε περιβάλλοντα ασύρματης επικοινωνίας, όπου η φύση του καναλιού καθιστά πιο εφικτή την παρακολούθηση ή την παρεμβολή από κακόβουλους παράγοντες.

Η βασική λειτουργική αρχιτεκτονική ενός IDS περιλαμβάνει τέσσερα κύρια στάδια: συλλογή δεδομένων από το περιβάλλον λειτουργίας, ανάλυση της δραστηριότητας, λήψη απόφασης ως προς τη φύση της συμπεριφοράς (κανονική ή ύποπτη) και, τέλος, αναφορά ή ενεργή παρέμβαση. Ειδικότερα, σε σύγχρονες υλοποιήσεις, τα IDS ενσωματώνουν συχνά συστήματα κατηγοριοποίησης, επεξεργασίας ροής δεδομένων και μαθησιακές μεθόδους, προκειμένου να επιτυγχάνεται βελτιστοποιημένος εντοπισμός επιθέσεων, ακόμη και σε περιβάλλοντα υψηλής αβεβαιότητας [27].



Εικόνα 10: Τοπολογία με εγκατεστημένο IDS

Στην παραπάνω εικόνα, το IDS είναι παθητικά συνδεδεμένο στο switch (μέσω SPAN/TAP) ώστε να παρακολουθεί όλη την κίνηση προς/από το firewall και τους σταθμούς εργασίας, να ανιχνεύει επιθέσεις σε πραγματικό χρόνο και να ειδοποιεί χωρίς να επηρεάζει τη ροή.

Σε αντίθεση με τα Συστήματα Πρόληψης Εισβολών (Intrusion Prevention Systems – IPS), τα IDS λειτουργούν κυρίως παθητικά, καταγράφοντας και αξιολογώντας συμπεριφορές χωρίς άμεση παρέμβαση, επιτρέποντας έτσι καλύτερη ανάλυση του φαινομένου και συλλογή αποδείξεων για μελλοντική αξιοποίηση ή επανεκπαίδευση των μοντέλων [28].

7.2 Τύποι IDS και Μοντέλα Ανάλυσης

Η τυπολογία των IDS βασίζεται τόσο στη θέση τους στο δίκτυο όσο και στον τρόπο που ερμηνεύουν τα δεδομένα. Από πλευράς αρχιτεκτονικής, τα Network-based IDS (NIDS) παρακολουθούν και αναλύουν την κυκλοφορία του δικτύου μέσω παθητικής ακρόασης, επιτρέποντας την ανίχνευση επιθέσεων όπως η υπερφόρτωση (DoS) ή η καταγραφή πακέτων (packet sniffing). Αντίθετα, τα Host-based IDS (HIDS) είναι εγκατεστημένα απευθείας στους τελικούς κόμβους, εξετάζοντας στοιχεία όπως αρχείο καταγραφών (logs), χρήση μνήμης ή εκτελούμενες διεργασίες, προσφέροντας καλύτερη ορατότητα στην τοπική συμπεριφορά του συστήματος [29].

Ως προς τη μεθοδολογία ανάλυσης, δύο βασικές κατηγορίες δεσπόζουν: τα συστήματα βασισμένα σε υπογραφές (signature-based) και τα συστήματα βασισμένα σε ανωμαλίες (anomaly-based). Τα πρώτα συγκρίνουν την εισερχόμενη δραστηριότητα με βάση γνωστά πρότυπα επιθέσεων, επιτυγχάνοντας εξαιρετικά χαμηλά ποσοστά ψευδών θετικών όταν πρόκειται για καλά καταγεγραμμένες απειλές [30]. Ωστόσο, υπολείπονται σε αποτελεσματικότητα απέναντι σε νέες ή παραλλαγμένες μορφές επιθέσεων, οι οποίες δεν εμπίπτουν σε προκαθορισμένα μοτίβα.

Αντιθέτως, τα anomaly-based IDS μαθαίνουν το "κανονικό" πρότυπο συμπεριφοράς του συστήματος και επιχειρούν να εντοπίσουν αποκλίσεις. Η συγκεκριμένη προσέγγιση

ευνοείται ιδιαίτερα από την εφαρμογή τεχνικών Μηχανικής Μάθησης, οι οποίες ενισχύουν την ικανότητα γενίκευσης του συστήματος, ανιχνεύοντας καινοφανείς επιθέσεις ακόμη και χωρίς άμεση γνώση των χαρακτηριστικών τους [31]. Ωστόσο, η προσέγγιση αυτή συνοδεύεται από μεγαλύτερα ποσοστά ψευδώς θετικών, γεγονός που απαιτεί επιπλέον τεχνικές φιλτραρίσματος και επιβεβαίωσης.

Υβριδικά μοντέλα, τα οποία συνδυάζουν ανάλυση υπογραφών και ανωμαλιών, προτείνονται ως η πλέον υποσχόμενη λύση, ιδίως σε πολύπλοκα ή ευμετάβλητα περιβάλλοντα όπως τα WLANs [32].

7.3 Εξειδικευμένη Εφαρμογή IDS σε WLANs

Η ανάπτυξη ενός αποτελεσματικού IDS για ασύρματα τοπικά δίκτυα ενέχει ειδικές τεχνικές και επιστημονικές προκλήσεις. Τα WLANs διακρίνονται για τη δυναμική φύση τους, την ανοιχτή πρόσβαση στο μέσο μετάδοσης και την αυξημένη ποικιλομορφία των συσκευών που συνδέονται. Αυτοί οι παράγοντες ευνοούν την εμφάνιση επιθέσεων όπως η δημιουργία ψευδο-access points (Evil Twin), η εισαγωγή παραποιημένων πακέτων αποσύνδεσης (Deauthentication Attacks), ή οι επιθέσεις τύπου Bluejacking και BlueSnarfing μέσω Bluetooth [33].

Στο πλαίσιο αυτό, ένα WLAN IDS απαιτεί υψηλό επίπεδο ευελιξίας και προσαρμοστικότητας. Η συνεχής ανανέωση της πληροφορίας, η ανάγκη ανάλυσης σημάτων σε πραγματικό χρόνο, και η δυνατότητα αντίδρασης σε επιθέσεις χωρίς την ανάγκη ανθρώπινης παρέμβασης καθιστούν αναγκαία την υιοθέτηση έξυπνων, μαθησιακών αλγορίθμων. Οι πλέον πρόσφατες ερευνητικές εργασίες δείχνουν ότι τα αλγοριθμικά μοντέλα όπως τα Support Vector Machines (SVM), Decision Trees, καθώς και βαθιά νευρωνικά δίκτυα, προσφέρουν αξιοσημείωτη ακρίβεια στην αναγνώριση και ταξινόμηση επιθέσεων σε WLANs [34].

Επιπλέον, η ενσωμάτωση των IDS με υποδομές ανάλυσης ροών (flow analysis) και μεθόδων προεπεξεργασίας (π.χ. feature selection, dimensionality reduction) ενισχύει την ακρίβεια και τη συνολική απόδοση του συστήματος. Σύμφωνα με [35], η επιτυχής εφαρμογή ενός τέτοιου συστήματος βασίζεται όχι μόνο στην επιλογή του κατάλληλου

αλγορίθμου, αλλά και στη σωστή διαχείριση του δικτυακού θορύβου και των ασυνεπειών των δεδομένων, οι οποίες είναι ιδιαίτερα έντονες στο ασύρματο περιβάλλον.

7.4 Ο Ρόλος της Μηχανικής Μάθησης στην Ανίχνευση Επιθέσεων

Η ταχεία εξέλιξη και η πολυπλοκότητα των απειλών που στοχεύουν ασύρματα δίκτυα έχουν καταστήσει ανεπαρκείς τις παραδοσιακές, στατικές μεθόδους ανίχνευσης επιθέσεων. Στο πλαίσιο αυτό, η Μηχανική Μάθηση (Machine Learning – ML) αναδεικνύεται ως μια κρίσιμη τεχνολογία για την ανάπτυξη έξυπνων και προσαρμοστικών Συστήματων Ανίχνευσης Εισβολών (IDS), ικανών να ανταποκρίνονται σε δυναμικά περιβάλλοντα όπως τα WLANs.

Σε αντίθεση με τα συμβατικά IDS που στηρίζονται σε αυστηρά καθορισμένους κανόνες ή υπογραφές, τα ML-based IDS είναι σε θέση να μαθαίνουν αυτόματα τα μοτίβα συμπεριφοράς του δικτύου και να εντοπίζουν αποκλίσεις, ακόμα κι αν αυτές δεν αντιστοιχούν σε γνωστές επιθέσεις [36]. Η ικανότητα αυτή προσδίδει στα ML μοντέλα χαρακτηριστικά γενίκευσης, που επιτρέπουν την έγκαιρη αναγνώριση νέων, εξελιγμένων ή μεταλλαγμένων απειλών (zero-day attacks) [37].

Τα πιο συχνά χρησιμοποιούμενα μοντέλα ML στην ανίχνευση εισβολών περιλαμβάνουν αλγορίθμους επιβλεπόμενης μάθησης όπως τα Support Vector Machines (SVM), Random Forests, Naive Bayes, αλλά και μη επιβλεπόμενες τεχνικές όπως το k-Means Clustering, που αποδεικνύονται αποτελεσματικές για την ανίχνευση ανωμαλιών χωρίς την ανάγκη εκ των προτέρων κατηγοριοποιημένων δεδομένων [38]. Τα τελευταία χρόνια, έχουν προταθεί επίσης και μέθοδοι βαθιάς μάθησης (Deep Learning), όπως Autoencoders και Recurrent Neural Networks (RNNs), οι οποίες επιδεικνύουν υψηλή απόδοση σε πολύπλοκα datasets και μπορούν να διαχειριστούν την πολυπλοκότητα της ροής δεδομένων σε πραγματικό χρόνο [39].

Η διαδικασία ενσωμάτωσης της μηχανικής μάθησης σε ένα IDS απαιτεί συγκεκριμένα βήματα: συλλογή και προεπεξεργασία δεδομένων, επιλογή χαρακτηριστικών (feature selection), εκπαίδευση του μοντέλου, και αξιολόγηση της απόδοσής του με βάση μετρικές όπως accuracy, precision, recall και F1-score. Ιδιαίτερα σημαντικό είναι το στάδιο της εξισορρόπησης του dataset, δεδομένου ότι στις περισσότερες περιπτώσεις τα δεδομένα είναι μη ισομερώς κατανεμημένα (π.χ. οι επιθέσεις αποτελούν μικρό ποσοστό σε σχέση με τις κανονικές συνδέσεις) [40].

Στη βιβλιογραφία, πολλά πειραματικά μοντέλα έχουν αξιοποιήσει το NSL-KDD και το CICIDS2017 ως datasets αναφοράς για εκπαίδευση και αξιολόγηση IDS. Σε αυτά τα περιβάλλοντα, μοντέλα όπως τα Decision Trees και τα SVMs έχουν φτάσει σε ακρίβειες άνω του 95%, ενώ τα μοντέλα βαθιάς μάθησης αγγίζουν ακόμη υψηλότερες επιδόσεις, ειδικά όταν ενσωματώνουν τεχνικές κανονικοποίησης, dropout και parallel processing [41].

Αξίζει να σημειωθεί ότι, πέρα από την ακριβή ανίχνευση, η χρήση ML σε WLAN IDS επιτρέπει και τη δυναμική προσαρμογή σε νέο κυκλοφοριακό πρότυπο μέσω συνεχούς εκπαίδευσης (online learning), καθώς και τη μείωση των ψευδών θετικών με τη χρήση ensemble learning τεχνικών [42].

Τέλος, η χρήση ανοιχτών και επεκτάσιμων ML frameworks, όπως τα Scikit-learn, TensorFlow, και PyTorch, επιτρέπει την υλοποίηση προηγμένων ML-based IDS σε πραγματικό περιβάλλον WLAN, ενισχύοντας τόσο την αξιοπιστία όσο και τη δυνατότητα ελέγχου του συστήματος από τον διαχειριστή [43].

8 Ανάπτυξη και Εφαρμογή Συστήματος Ανίχνευσης Επιθέσεων (Β' ΜΕΡΟΣ)

Το σύστημα υλοποιήθηκε έτσι ώστε ο δρόμος από το πακέτο δικτύου μέχρι την απόφαση «anomaly/normal» να είναι σταθερός, αναπαραγωγικός και εύκολα επαληθεύσιμος.

Η βασική ιδέα είναι απλή: πολύ συνοπτικά συναρμολογούμε ροές από πακέτα, εξάγουμε λίγα αλλά εκφραστικά γνωρίσματα ανά ροή, περνάμε τα γνωρίσματα από ένα ενιαίο pipeline προεπεξεργασίας+μοντέλου, παράγουμε πιθανότητα ανωμαλίας και, αν ξεπεράσει ένα ρυθμιζόμενο κατώφλι, το όριο που έχουμε θεσπίσει δηλαδή, καταχωρίζουμε συναγερμό και ειδοποιούμε με τη δημιουργία περιστατικού. Το ίδιο pipeline που «έμαθε» στο Train_data αποθηκεύεται και φορτώνεται αυτούσιο στη φάση ανίχνευσης, ώστε να μην υπάρχουν ασυνέπειες.

8.1 Σύνολο δεδομένων και πυρήνας γνωρισμάτων

Στόχος.

Ανίχνευση κακόβουλων ροών (flows) σε WLAN, συνδυάζοντας μετρικές IP/Transport με συμφραζόμενα Wi-Fi (SSID/BSSID/VLAN, ισχύ σήματος RSSI, ρυθμός deauth).Μοντέλο απειλής.

Καλύπτουμε δραστηριότητες όπως: ανώμαλος ρυθμός πακέτων (DoS/scan), κακόβουλα handshakes, ανεπιθύμητα management frames (π.χ. deauth floods), και ύποπτα patterns σε θύρες/πρωτόκολλα. Πυρήνας ML (ids_pipeline.py): preprocessing γνωρισμάτων, εκπαίδευση (XGBoost / fallback: RandomForest), επιλογή κατωφλίου (threshold), αποθήκευση pipeline + μεταδεδομένων (meta).

Εκπαίδευση (train.py): CLI για φόρτωση CSV (Train_data.csv) και παραγωγή ids_pipeline.joblib (+ .meta.json).

Λειτουργία (serve.py): λήψη πακέτων (JSON Lines) σε πραγματικό χρόνο ή offline replay, συναρμολόγηση σε ροές, inference, alerts και rotating logs.

Ζωντανό & offline. Το ίδιο σύστημα λειτουργεί:

- Live: sniffer → JSONL → serve.py (π.χ. SPAN/mirror port).
- Offline: cat traffic.jsonl | python serve.py --model ids_pipeline.joblib.

8.2 Εκπαίδευση Μοντέλου

Δομή δεδομένων. Το Train_data.csv είναι flow-level: κάθε γραμμή συνοψίζει κυκλοφορία για (src_ip, dst_ip, src_port, dst_port, proto) με ετικέτα label (0: κανονική, 1: κακόβουλη).

Γνωρίσματα που χρησιμοποιούμε:

Αριθμητικά:
duration, packets, bytes, mean_pkt_size, pps, bps, syn, fin, rst, rssi, deauth_rate. duration (διάρκεια ροής), pps/bps (ρυθμοί), mean_pkt_size (μέσο μέγεθος πακέτου), syn/fin/rst (TCP flags counts), rssi (μέση ισχύς), deauth_rate (deauths/sec).

Κατηγορικά:
proto, ssid, bssid, vlan, src_port_bucket, dst_port_bucket.

Κρίσιμα σημεία σχεδίασης:

Θύρες → θυρίδες (bucketization). Οι θύρες δεν συμπεριφέρονται «συνεχόμενα».

Τις αντιστοιχίζουμε σε:
well_known (≤1023), registered (1024–49151), dynamic (>49151), unknown. Αυτό μας βοηθάει στο να βελτιώνουμε τη γενίκευση και καταφέρνουμε να μειώνουμε το overfitting.

High Cardinality (έχει πάρα πολλές μοναδικές τιμές (π.χ. χιλιάδες SSID/BSSID/VLAN). (ssid/bssid/vlan)). Χρησιμοποιούμε One-Hot Encoder με ομαδοποίηση σπάνιων

κατηγοριών (infrequent binning, ή ασφαλές fallback) ώστε να μην εκραγούν οι διαστάσεις, διατηρώντας παράλληλα διακριτική ισχύ.

Ανθεκτικότητα σε ελλείψεις/τύπους. Επιβάλλουμε τύπους, συμπληρώνουμε λείποντα με ασφαλή defaults, και δημιουργούμε τα port buckets.

Ακολουθεί το αντίστοιχο κομμάτι κώδικα:

```
def _port_bucket(p):

try: v = int(p) except: return "unknown" if v < 0:

return "unknown" if v <= 1023: return "well_known" if v <= 49151:

return "registered" return "dynamic"

def _make_ohe(): try:

return OneHotEncoder(handle_unknown="infrequent_if_exist",

min_frequency=0.01, sparse_output=False) except

Exception: try: return OneHotEncoder(handle_unknown="ignore", sparse=False)

except Exception: return OneHotEncoder(handle_unknown="ignore")

def build_preprocessor():

num_tf = Pipeline([("scaler", StandardScaler())])

cat_tf = Pipeline([("oh", _make_ohe())])

return ColumnTransformer([("num", num_tf, NUMERIC_FEATURES),

("cat", cat_tf, CATEGORICAL_FEATURES), ])
```

8.3 Εκπαίδευση Calibration και Επιλογή Κατωφλίου

Απο εδώ και στο εξής η διαδικασία συνεχίζει ως εξής:

- Split 80/20 (stratify) για διατήρηση λόγου κλάσεων.
- Μοντέλο: XGBoost (scale_pos_weight = Neg/Pos για ανισορροπία).
- Calibration (προαιρετικό): isotonic πάνω στο holdout (βελτιώνει την αξιοπιστία πιθανοτήτων).
- Threshold (κατώφλι): επιλέγεται με μέγιστο F1 από την καμπύλη Precision-Recall (PR).
- Αποθήκευση: ids_pipeline.joblib και metadata .meta.json (ROC-AUC, PR-AUC, sampled PR points, best_threshold_f1, schema hash, versions).

Ορισμοί μετρικών.

- Precision = TP / (TP+FP), Recall = TP / (TP+FN), F1 = 2·(P·R)/(P+R).
- PR-AUC είναι πιο κατάλληλο από ROC-AUC όταν η θετική κλάση είναι σπάνια.

Ακολουθεί σημείο κώδικα όπου φαίνεται το threshold.

```
from sklearn.metrics import precision_recall_curve

def _best_threshold_by_f1(y_true, y_prob):

prec, rec,

thr = precision_recall_curve(y_true, y_prob) f1 = (2*prec*rec) / np.clip(prec+rec, 1e-9, None)

if len(thr) == 0: return 0.5 best_idx = int(np.nanargmax(f1))

return float(max(0.01, min(0.99, thr[max(0, best_idx - 1)])))
```

Και για την εκπαιδευση μεσω CLI:

pip install -r requirements.txt

python train.py --csv Train_data.csv --out ids_pipeline.joblib --calibrate

Τι αποθηκεύεται στο meta?
Μετρικές (ROC/PR AUC), έκδοση pipeline (version), δείγματα PR curve για επιχειρησιακό tuning, schema_hash (για έλεγχο συμβατότητας features), εκδόσεις βιβλιοθηκών (sklearn/xgboost), και το best_threshold_f1.

8.4 Απόφαση, συναγερμοί και επιμονή δεδομένων

```
Είσοδος (stdin/JSONL). Το serve.pycfg, store):
   feats = flow_to_features(flow, cfg.port_service)
   try:
      proba = float(pipe.predict_proba(feats)[0, 1])
   except Exception:
      proba = float(pipe.predict(feats)[0])
   if proba >= cfg.threshold:
      store.insert(flow['last_ts'], flow['src_ip'], flow['dst_ip'],
                   flow['src_port'], flow['dst_port'],
                   feats['protocol_type'].iloc[0], 'anomaly', proba)
      send_email(
         subject=f"IDS Alert {flow['src_ip']}->{flow['dst_ip']} score={proba:.2f}",
         body=f"Time: {flow['last_ts']:.3f}\nFlow: {flow['src_ip']}:{flow['src_port']} ->
"
              f"{flow['dst_ip']}:{flow['dst_port']}\nProto: {feats['proto-
col_type'].iloc[0]}\n"
              f"Score: {proba:.3f}\n",
         cfg=cfg
      )
```

Η επιμονή των alerts υλοποιείται με απλό πίνακα σε PostgreSQL και ελάχιστα πεδία που επιτρέπουν γρήγορη αναζήτηση και συσχέτιση. Αν η βάση δεν είναι διαθέσιμη, υπάρχει ασφαλές fallback σε log, ώστε να μη χαθεί γεγονός.

```
class AlertStore:
 def __init__(self, db_uri):
```

```
        self.ok, self.conn = False, None
        if psycopg2 is None:
            logging.warning("DB logging disabled.")
            return
        try:
            self.conn = psycopg2.connect(db_uri, cursor_factory=RealDictCursor)
            self.conn.autocommit = True
            with self.conn.cursor() as cur:
                cur.execute("""
                  CREATE TABLE IF NOT EXISTS alerts(
                    id SERIAL PRIMARY KEY,
                    timestamp DOUBLE PRECISION,
                    src_ip TEXT, dst_ip TEXT,
                    src_port INTEGER, dst_port INTEGER,
                    protocol TEXT, label TEXT, score DOUBLE PRECISION);
                """)
            self.ok = True
        except Exception as e:
            logging.error(f"DB connection failed: {e}")

    def insert(self, ts, src_ip, dst_ip, sport, dport, proto, label, score):
        if not self.ok:
            logging.info(f"[NO-DB] ALERT {ts:.3f} {src_ip}:{sport}->{dst_ip}:{dport}
{proto} {label} {score:.3f}")
            return
        with self.conn.cursor() as cur:
            cur.execute(
              "INSERT INTO alerts(timestamp, src_ip, dst_ip, src_port, dst_port, protocol,
label, score) "
              "VALUES (%s,%s,%s,%s,%s,%s,%s,%s)",
              (ts, src_ip, dst_ip, sport, dport, proto, label, score)
            )
def send_email(subject, body, cfg):
    try:
```

```
        msg = MIMEText(body, _charset="utf-8")
        msg['Subject'], msg['From'], msg['To'] = subject, cfg.email_user, cfg.alert_recipi-
ent
        with smtplib.SMTP(cfg.email_smtp, cfg.email_port, timeout=10) as s:
            s.starttls(); s.login(cfg.email_user, cfg.email_pass); s.send_message(msg)
    except Exception as e:
        logging.error(f"Failed to send email: {e}")
```

Η επιλογή να μείνουν τα alerts «λιτά» κάνει τη βάση γρήγορη. Αν αργότερα χρειαστεί εμπλουτισμός (π.χ. GeoIP, reverse DNS, tags), προστίθενται στήλες χωρίς να αλλάξει ο πυρήνας. Παρακάτω θα προχωρήσουμε στο να παρουσιάσουμε με μεγαλύτερη λεπτομέρεια τις ρυθμίσεις, καταγραφή και λειτουργικότητα του συστήματος/κώδικα.

Πιο αναλυτικά λοιπόν, οι ρυθμίσεις συγκεντρώνονται σε ένα dataclass με προεπιλογές που μπορούν να υπερκαλυφθούν από αρχείο YAML ή μεταβλητές περιβάλλοντος. Η καταγραφή συμβάντων γίνεται με περιστροφή αρχείων, ώστε να υπάρχει ιστορικό χωρίς να γεμίζει ο δίσκος, είναι μια τεχνική που επιλέχθηκε κυρίως για την πρακτικότα. Έτσι εξασφαλίζεται ιχνηλασιμότητα σε πραγματικό χρόνο και forensic δυνατότητες εκ των υστέρων.

```
from dataclasses import dataclass
from logging.handlers import RotatingFileHandler
@dataclass
class IDSConfig:
    db_uri: str = os.getenv('IDS_DB_URI', 'postgresql://user:pass@lo-
calhost:5432/idsdb')
    pcap_interface: str = os.getenv('IDS_PCAP_INTERFACE', 'eth0')
    model_path: str = os.getenv('IDS_MODEL_PATH', 'models/model_pipeline.pkl')
    threshold: float = float(os.getenv('IDS_SCORE_THRESHOLD', 0.5))
    email_smtp: str = os.getenv('IDS_EMAIL_SMTP', 'smtp.example.com')
    email_port: int = int(os.getenv('IDS_EMAIL_PORT', 587))
    email_user: str = os.getenv('IDS_EMAIL_USER', 'alert@example.com')
    email_pass: str = os.getenv('IDS_EMAIL_PASS', 'password')
    alert_recipient: str = os.getenv('IDS_ALERT_RECIPIENT', 'soc@example.com')
```

```
    log_file: str = os.getenv('IDS_LOG_FILE', 'ids.log')
    port_service: dict = DEFAULT_PORT_SERVICE


def setup_logging(log_file):
    os.makedirs(os.path.dirname(log_file) or ".", exist_ok=True)
    logger = logging.getLogger(); logger.setLevel(logging.INFO)
    fmt = logging.Formatter('[%(asctime)s] %(levelname)s %(name)s: %(message)s')
    fh = RotatingFileHandler(log_file, maxBytes=5_000_000, backupCount=3); fh.set-
Formatter(fmt)
    ch = logging.StreamHandler(sys.stdout); ch.setFormatter(fmt)
    logger.addHandler(fh); logger.addHandler(ch)
```

Η ύπαρξη ενιαίου σημείου διαμόρφωσης διευκολύνει την εγκατάσταση σε διαφορετικά περιβάλλοντα και επιτρέπει ρύθμιση του κατωφλίου, της διεπαφής, των διαδρομών και των ειδοποιήσεων χωρίς αλλαγή κώδικα.

8.5 Μεθοδολογία αξιολόγησης και συντονισμός κατωφλίου

Χρησιμοποιείται προκαθορισμένος διαχωρισμός σε train / validation / holdout με ετικέτα label ∈ {0,1}. Η ίδια ακριβώς προεπεξεργασία εφαρμόζεται σε εκπαίδευση και εξυπηρέτηση (ασφαλές imputation για ελλείποντα, κανονικοποίηση αριθμητικών γνωρισμάτων, one-hot κωδικοποίηση κατηγορικών) μέσα σε ενιαίο pipeline, ώστε να διατηρείται απόλυτη συμβατότητα χαρακτηριστικών. Ως βασικός ταξινομητής χρησιμοποιείται XGBoost με tree_method=hist και αυτόματο scale_pos_weight για την ανισορροπία κλάσεων όπου το XGBoost δεν είναι διαθέσιμο, υπάρχει εναλλακτικά RandomForest.

Η αξιολόγηση γίνεται στο holdout και περιλαμβάνει ROC-AUC, PR-AUC (Average Precision/AP), classification report (precision/recall/F1 ανά κλάση) και confusion matrix. Επειδή το σύνολο δεδομένων είναι ανισόρροπο, δίνεται ιδιαίτερη έμφαση στο PR-AUC και στη σύζευξη precision–recall.

Το κατώφλι λειτουργίας ορίζεται αλγοριθμικά ως το κατώφλι που μεγιστοποιεί το F1 στο holdout. Υπολογίζονται τα σκορ όλων των δειγμάτων, σαρώνονται υποψήφια κατώφλια στο [0,1] και επιλέγεται το βέλτιστο κατώφλι t*. Το t* αποθηκεύεται μαζί με τα βασικά μετρικά στο συνοδευτικό αρχείο meta (.meta.json) για πλήρη αναπαραγωγιμότητα στο runtime. Για να τεκμηριωθεί η πρακτική επίδραση του κατωφλίου, παρουσιάζεται confusion matrix στο t* (και συνοπτικά στο t* ± 0,05), ώστε να αποτυπώνεται καθαρά ο επιχειρησιακός συμβιβασμός μεταξύ ψευδώς θετικών και ψευδώς αρνητικών.

Όταν ενεργοποιείται isotonic calibration στο holdout, επανυπολογίζεται το κατώφλι πάνω στις βαθμονομημένες πιθανότητες και παρουσιάζονται πριν/μετά οι κύριες μετρικές (PR-AUC, ROC-AUC, F1 στο t*), προαιρετικά και ο Brier Score με σύντομη ερμηνεία της calibration curve (reliability plot).

Στο περιβάλλον παραγωγής η εφαρμογή του κατωφλίου ακολουθεί σαφή προτεραιότητα, ώστε να συνδυάζεται λειτουργική ευελιξία με αναπαραγωγιμότητα:

1) Ρύθμιση από τη γραμμή εντολών μέσω --threshold όταν απαιτείται επιχειρησιακή παράκαμψη,
2) Τιμή από το .meta.json (το βέλτιστο κατώφλι t* που προέκυψε από την αξιολόγηση)
3) Προεπιλεγμένη τιμή όταν λείπουν τα προηγούμενα (π.χ. 0,70).

Για να αποφεύγονται ασυνέπειες, τεκμηριώνεται ρητά το όνομα/μονοπάτι του αρχείου δεδομένων που δίνεται στο train.py (μέσω της παραμέτρου --data) και χρησιμοποιούνται σταθεροί τυχαίοι σπόροι όπου χρειάζεται. Το αποτέλεσμα είναι μια μεθοδολογία που δένει αυστηρά την εκπαίδευση με το serving και προετοιμάζει ομαλά το έδαφος για τα θέματα απόδοσης του Κεφ. 8.6.

8.6 Απόδοση, κλιμάκωση και λειτουργική ανθεκτικότητα

Η εξυπηρέτηση σε πραγματικό χρόνο υλοποιείται με Flow Aggregator που ομαδοποιεί πακέτα σε ροές με κλειδιά (src_ip, dst_ip, src_port, dst_port, proto), inactivity timeout και περιοδικές εκκαθαρίσεις. Για κάθε ροή παράγονται ελαφρά

features (π.χ. pps, bps, mean_pkt_size, flags SYN/FIN/RST, διάρκεια) και Wi-Fi context (SSID/BSSID/VLAN, rssi_mean, deauths, deauth_rate), πλήρως συμβατά με τα features του training. Το inference είναι stream-friendly: τα ολοκληρωμένα flows μετατρέπονται σε DataFrame, περνούν από το αποθηκευμένο pipeline και παράγεται score· στη συνέχεια εφαρμόζεται η πολιτική κατωφλίου (προτεραιότητα όπως παραπάνω) και παράγονται alerts με cooldown ανά πηγή για αποφυγή storm. Η ανθεκτικότητα διασφαλίζεται με ensure_columns/imputation για ελλείποντα πεδία, απομόνωση εξαιρέσεων (το loop δεν πέφτει) και κλιμακωτές ενέργειες: notify_only για οριακά scores, quarantine_vlan για υψηλή βεβαιότητα. Η κλιμάκωση επιτυγχάνεται οριζόντια (πολλαπλά serve πίσω από stream splitter, π.χ. per-VLAN/per-AP). Για συνέπεια στο alerting μεταξύ instances προτείνεται κοινό κατάστημα κατάστασης (π.χ. Redis) μόνο για το cooldown. Αν απαιτηθεί υψηλότερος ρυθμός I/O, προβλέπεται στρώμα REST/Socket αντί αποκλειστικά stdin.

8.7 Περιορισμοί, Αξιολόγηση Κινδύνων & Επεκτάσεις

Κύριοι τεχνικοί περιορισμοί: ανισορροπία κλάσεων (παρότι μετριάζεται με scale_pos_weight χρειάζεται συνεχής παρακολούθηση PR-AUC/F1), concept drift σε περιβάλλοντα Wi-Fi (αλλαγές σε RF/clients/APs) και ποιότητα σημάτων (RSSI/802.11 management frames) που μπορεί να αυξήσει FP/FN. Το imputation με default τιμές είναι ασφαλές επιχειρησιακά αλλά ενδέχεται να εισάγει bias προτείνεται προσθήκη missing-indicators (δυαδικές στήλες “ήταν κενό”).

Από πλευράς ρίσκου, συζητούμε ρητά το trade-off FP vs FN: αν το κόστος FN είναι μεγάλο (κίνδυνος διαφυγής επίθεσης) μετατοπίζουμε ελαφρά κάτω από το (t*) υπέρ του recall αν το κόστος FP είναι μεγάλο (κόπωση SOC/λειτουργικός θόρυβος), μετατοπίζουμε πάνω από το (t*) υπέρ του precision και τα δύο χωρίς retrain μέσω -- threshold.

Ως επόμενα βήματα προτείνουμε monitoring drift/health (κύλιση PR-AUC/F1, calibration curves, schema checks), online/periodic re-calibration με επανυπολογισμό (t*), ερμηνευσιμότητα (SHAP/Permutation Importance) και εμπλουτισμό

χαρακτηριστικών με περισσότερα 802.11 management/control frames και χρονικά/περι-AP στατιστικά.

Βιβλιογραφία

[1] IEEE Std 802.11-2016, IEEE Standard for Information technology Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. IEEE, 2016.

[2] Mishra, A., & Arbaugh, W. A., "An Initial Security Analysis of the IEEE 802.1X Standard," Proceedings of the 2002 IEEE Computer and Communications Societies, pp. 1700-1709, 2002.

[3] Bellardo, J., & Savage, S., "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," USENIX Security Symposium, 2003.

[4] He, C., & Mitchell, J. C., "Security Analysis and Improvements for IEEE 802.11i," NDSS, 2005.

[5] Cam-Winget, N., Housley, R., Wagner, D., & Walker, J., "Security flaws in 802.11 data link protocols," Communications of the ACM, vol. 46, no. 5, pp. 35–39, 2003.

[6] Bittau, A., Handley, M., & Lackey, J., "The final nail in WEP's coffin," 2006 IEEE Symposium on Security and Privacy (S&P), pp. 386–400, 2006.

[7] Denning, D. E., "An Intrusion-Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222–232, 1987.

[8] Gast, M., 802.11 Wireless Networks: The Definitive Guide, 2nd ed. O'Reilly, 2005. 999 IEEE Std 802.11w-2009, Amendment 4: Protected Management Frames. IEEE, 2009.

[10] S. Vanhoef & M. Piessens, "Advanced Wi-Fi attacks using commodity hardware," Proceedings of the 30th Annual Computer Security Applications Conference, pp. 226–235, 2014.

[11] Scalabrino, S., "Wireless IDS/IPS Systems," IEEE Security & Privacy, vol. 12, no. 6, pp. 74–77, 2014.

[12] Shetty, S., "Using Machine Learning to Enhance Wireless Security," IEEE Communications Magazine, vol. 58, no. 4, pp. 98–104, 2020.

[13] Inhyok Cha, JaeSeung Song, Wan-Seon Lim, “Detecting malicious deauthentication attacks in wireless LAN using supervised learning,” IEEE International Conference on Communications (ICC), 2018.

[14] Shepard, D. et al. (2012). Evaluation of UAV Vulnerability to GPS Spoofing. Radionavigation Lab, UT Austin.

[15] S. R. Ratna and R. Ravi, "Survey on jamming wireless networks: Attacks and prevention strategies", International Journal of Computer and Information Engineering, vol. 9, no. 2, pp. 642-648, 2015.

[16] L. R and R. M. Bommi, "Deauthentication Attack Detection in the Wi-Fi network by Using ML Techniques," 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/ICSTCEE56972.2022.10099975.

[17] Evgeny Khorov, Anton Kiryanov, Andrey Lyakhov, Giuseppe Bianchi. "A Tutorial on IEEE 802.11ax High Efficiency WLANs." IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 197–216, First quarter 2019.

[18] "What Is Wi-Fi 7? Here's Everything You Need to Know." WIRED, 14 September 2024.

[19] Ενότητα 11: Ασύρματα Ad Hoc Δίκτυα, Πανεπιστήμιο Πατρών.

[20] Αδυναμίες Ασφάλειας και Επιθέσεις σε Manet Δίκτυα, Πανεπιστήμιο Πειραιώς.

[21] Ασφάλεια Δρομολόγησης σε Ασύρματα Αδόμητα (Ad Hoc) Δίκτυα, Ελληνικό Ανοικτό Πανεπιστήμιο.

[22] Ad hoc δίκτυο - Βικιπαίδεια.

[23] Χαρακτήρες ασύρματων κινητών ad hoc δικτύων, iWave Communications

[24] National Institute of Standards and Technology (NIST), "Guidelines for Securing Wireless Local Area Networks (WLANs)", Special Publication 800-153, 2011.

[25] Wikipedia, "Spanning Tree Protocol"

[26] Debar, H., Dacier, M., & Wespi, A. (2000). "A revised taxonomy for intrusion-detection systems." *Annales des télécommunications*.

[27] Scarfone, K., & Mell, P. (2007). "Guide to intrusion detection and prevention systems (IDPS)." *NIST Special Publication*.

[28] Axelsson, S. (2000). "Intrusion detection systems: A survey and taxonomy." *Technical report, Chalmers University*.

[29] Bace, R., & Mell, P. (2001). "Intrusion detection systems." *NIST Computer Security Resource Center*.

[30] Roesch, M. (1999). "Snort - Lightweight Intrusion Detection for Networks." *USENIX LISA*.

[31] Patcha, A., & Park, J. M. (2007). "An overview of anomaly detection techniques: Existing solutions and latest technological trends." *Computer networks*.

[32] Chatzigiannakis, I., et al. (2007). "Hybrid intrusion detection systems in wireless sensor networks." *Mobile Networks and Applications*.

[33] Wright, J., Cache, J., & Liu, V. (2011). "Hacking Exposed Wireless: Wireless Security Secrets & Solutions." *McGraw-Hill*.

[34] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). "A deep learning approach to network intrusion detection." *IEEE Transactions on Emerging Topics in Computational Intelligence*.

[35] Dhanabal, L., & Shantharajah, S. P. (2015). "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms." *International Journal of Advanced Research in Computer and Communication Engineering*.

[36] Sommer, R., & Paxson, V. (2010). "Outside the closed world: On using machine learning for network intrusion detection." *IEEE Symposium on Security and Privacy*.

[37] Buczak, A. L., & Guven, E. (2016). "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications Surveys & Tutorials*.

[38] Revathi, S., & Malathi, A. (2013). "A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection." *International Journal of Engineering Research and Technology*.

[39] Kim, G., Lee, S., & Kim, S. (2016). "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection." *Expert Systems with Applications*.

[40] Moustafa, N., & Slay, J. (2015). "UNSW-NB15: a comprehensive data set for network intrusion detection systems." *Military Communications and Information Systems Conference*.

[41] Diro, A. A., & Chilamkurti, N. (2018). "Distributed attack detection scheme using deep learning approach for Internet of Things." *Future Generation Computer Systems*.

[42] Zhao, L., & Wang, K. (2018). "Intrusion detection model based on deep belief network and improved Gaussian mixture model." *Computer Communications*.

[43] Amirahmad, A., & Khoshraftar, S. (2021). "Lightweight IDS using feature reduction and ensemble classifiers." *Computers & Security*.

Παράρτημα Α — Χάρτης Αποθετηρίου & Αναπαραγωγιμότητα

- Δομή φακέλων/αρχείων: train.py, serve.py, ids_pipeline.py, requirements.txt, Train_data.csv.
- Περιβάλλον: έκδοση Python, virtualenv, pip install -r requirements.txt.
- Εντολές “τέλος-σε-τέλος”:

Command Line:
python train.py --data Train_data.csv --calibrate
python serve.py --model artifacts/ids_pipeline.joblib --meta artifacts/ids_pipeline.meta.json --threshold 0.70 --cooldown 120

 # train.py

```
from __future__ import annotations
import argparse
import json
from ids_pipeline import train_and_save

def main():
    ap = argparse.ArgumentParser(description="Train WIDS IDS pipeline from traindata.csv")
    ap.add_argument("--csv", default="traindata.csv", help="Path to training CSV")
    ap.add_argument("--out", default="ids_pipeline.joblib", help="Output model path")
    ap.add_argument("--calibrate", action="store_true", help="Enable isotonic calibration on holdout")
    args = ap.parse_args()

    metrics = train_and_save(args.csv, args.out, calibrate=args.calibrate)
    print(json.dumps(metrics, indent=2))

if __name__ == "__main__":
    main()
```

Παράρτημα Β — Serve.py (Κύριος Βρόγχος)

def main():

```
    ap = argparse.ArgumentParser(description="Serve WIDS model over stdin packet stream")
    ap.add_argument("--model", default="ids_pipeline.joblib", help="Path to model .joblib")
    ap.add_argument("--threshold", type=float, default=None, help="Override alert threshold (0-1)")
    ap.add_argument("--cooldown", type=float, default=DEFAULT_COOLDOWN_S, help="Cooldown seconds per source")
    ap.add_argument("--timeout", type=float, default=DEFAULT_FLOW_TIMEOUT_S, help="Flow inactivity timeout seconds")
    ap.add_argument("--yield-interval", type=float, default=DEFAULT_YIELD_INTERVAL_S, help="Seconds between expirations")
    args = ap.parse_args()

    model_path = args.model
    model = load_model(model_path)

    # Threshold: CLI > meta > default
    meta_threshold = load_threshold_from_meta(model_path)
    threshold = float(args.threshold if args.threshold is not None else meta_threshold)
    threshold = max(0.01, min(0.99, threshold))

    agg = FlowAggregator(timeout_s=args.timeout)
    cooldown_map: Dict[str, float] = defaultdict(lambda: 0.0)

    last_yield = 0.0
    for pkt in stdin_packets():
        agg.add_packet(pkt)
        now = float(pkt["ts"])
        if (now - last_yield) > args.yield_interval:
            last_yield = now
            for flow in agg.expire_and_yield(now):
                X = flow_to_df(flow)
                try:
                    if hasattr(model, "predict_proba"):
                        prob = float(model.predict_proba(X)[0, 1])
                    else:
                        prob = float(model.predict(X)[0])
                except Exception:
```

```
                    # Αν κάτι πάει στραβά στην πρόβλεψη, αγνοούμε τη ροή
                    continue

                alert = decide_and_build_alert(flow, prob, threshold,
cooldown_map, args.cooldown)
                if alert:
                    sys.stdout.write(json.dumps({"type": "ALERT", "data":
alert}) + "\n")
                    sys.stdout.flush()
```

Παράρτημα Γ — Pipeline Code

```
# ids_pipeline.py

from __future__ import annotations
import json
from pathlib import Path
from typing import Tuple, List, Optional, Dict, Any

import numpy as np
import pandas as pd

from sklearn.pipeline import Pipeline
from sklearn.compose import ColumnTransformer
from sklearn.preprocessing import StandardScaler, OneHotEncoder
from sklearn.metrics import (
    classification_report,
    roc_auc_score,
    average_precision_score,
    precision_recall_curve,
)
from sklearn.model_selection import train_test_split

from joblib import dump, load

# Προσπαθούμε XGBoost· αν λείπει, κάνουμε graceful fallback σε RandomForest
try:
    from xgboost import XGBClassifier
    _HAS_XGB = True
except Exception:  # pragma: no cover
    from sklearn.ensemble import RandomForestClassifier
    _HAS_XGB = False


# ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ (με Wi-Fi)

# Κατηγορίες (one-hot)
CATEGORICAL_FEATURES: List[str] = ["proto", "ssid", "bssid", "vlan"]

# Αριθμητικά
NUMERIC_FEATURES: List[str] = [
    "duration", "packets", "bytes",
    "mean_pkt_size", "pps", "bps",
    "syn", "fin", "rst",
    "src_port", "dst_port",
```

```
    # Wi-Fi metrics
    "rssi", "deauth_rate",
]
ALL_FEATURES: List[str] = CATEGORICAL_FEATURES + NUMERIC_FEATURES

TARGET_COL = "label"  # 0=benign, 1=malicious


def build_preprocessor() -> ColumnTransformer:
    num_tf = Pipeline(steps=[("scaler", StandardScaler())])
    cat_tf = Pipeline(steps=[("oh", OneHotEncoder(handle_unknown="ignore",
sparse_output=False))])
    pre = ColumnTransformer(
        transformers=[
            ("num", num_tf, NUMERIC_FEATURES),
            ("cat", cat_tf, CATEGORICAL_FEATURES),
        ],
        remainder="drop",
        sparse_threshold=0.3,
    )
    return pre


def _compute_scale_pos_weight(y: np.ndarray) -> float:
    pos = float((y == 1).sum())
    neg = float((y == 0).sum())
    return (neg / max(1.0, pos))


def build_model(y: np.ndarray):
    if _HAS_XGB:
        spw = _compute_scale_pos_weight(y)
        model = XGBClassifier(
            n_estimators=300,
            max_depth=6,
            learning_rate=0.05,
            subsample=0.8,
            colsample_bytree=0.8,
            reg_alpha=0.0,
            reg_lambda=1.0,
            tree_method="hist",
            n_jobs=-1,
            random_state=42,
            objective="binary:logistic",
            scale_pos_weight=spw,
            eval_metric="logloss",
```

```
        )
    else:
        from sklearn.ensemble import RandomForestClassifier
        model = RandomForestClassifier(
            n_estimators=400,
            max_depth=None,
            n_jobs=-1,
            random_state=42,
            class_weight="balanced_subsample",
        )
    return model


def build_pipeline(y_for_weights: np.ndarray) -> Pipeline:
    pre = build_preprocessor()
    clf = build_model(y_for_weights)
    pipe = Pipeline(steps=[("pre", pre), ("clf", clf)])
    return pipe


def ensure_columns(df: pd.DataFrame) -> pd.DataFrame:
    """Εγγυάται ότι υπάρχουν όλα τα απαιτούμενα columns με σωστούς τύπους."""
    out = df.copy()

    # Δημιουργούμε ελλείποντα πεδία με ασφαλή defaults
    for col in ALL_FEATURES:
        if col not in out.columns:
            # Κατηγορικά → κενή συμβολοσειρά, Αριθμητικά → 0
            out[col] = "" if col in CATEGORICAL_FEATURES else 0.0

    # Τύποι
    out["proto"] = out["proto"].astype(str)
    out["ssid"] = out["ssid"].astype(str)
    out["bssid"] = out["bssid"].astype(str)
    out["vlan"] = out["vlan"].astype(str)

    for col in NUMERIC_FEATURES:
        out[col] = pd.to_numeric(out[col], errors="coerce").fillna(0.0)

    # Θύρες ολόκληροι (παρότι τις τυποποιούμε αριθμητικά πιο πάνω)
    out["src_port"] = out["src_port"].astype(int)
    out["dst_port"] = out["dst_port"].astype(int)

    return out[ALL_FEATURES]
```

```
def _label_to_int(s: Any) -> int:
    """Αντιστοίχιση ετικετών σε 0/1 με αντοχή σε μορφές."""
    if isinstance(s, (int, np.integer)):
        return int(s)
    if isinstance(s, str):
        ls = s.strip().lower()
        if ls in ("1", "malicious", "attack", "bad", "evil"):
            return 1
        if ls in ("0", "benign", "normal", "good"):
            return 0
    # Fallback: θεωρούμε 0
    return 0


def _best_threshold_by_f1(y_true: np.ndarray, y_prob: np.ndarray) -> float:
    prec, rec, thr = precision_recall_curve(y_true, y_prob)
    f1 = (2 * prec * rec) / np.clip(prec + rec, 1e-9, None)
    if len(thr) == 0:
        return 0.5
    best_idx = int(np.nanargmax(f1))
    # Το precision_recall_curve δίνει thresholds για όλα εκτός από το πρώτο
σημείο
    return float(max(0.01, min(0.99, thr[max(0, best_idx - 1)])))


def _meta_path_for(joblib_path: str | Path) -> Path:
    p = Path(joblib_path)
    return p.with_suffix(".meta.json")


def train_and_save(
    csv_path: str,
    out_joblib: str = "ids_pipeline.joblib",
    calibrate: bool = False,
) -> Dict[str, Any]:
    df = pd.read_csv(csv_path)

    # Χαρτογράφηση ετικετών
    if TARGET_COL not in df.columns:
        raise ValueError(f"Column '{TARGET_COL}' not found in CSV")
    y = df[TARGET_COL].apply(_label_to_int).astype(int).values

    # Χαρακτηριστικά
    X = ensure_columns(df)
```

```
    X_tr, X_te, y_tr, y_te = train_test_split(
        X, y, test_size=0.2, random_state=42, stratify=y
    )

    pipe = build_pipeline(y_tr)
    pipe.fit(X_tr, y_tr)

    # Βασικές μετρικές σε holdout
    y_prob = pipe.predict_proba(X_te)[:, 1]
    y_hat_50 = (y_prob >= 0.5).astype(int)
    report = classification_report(y_te, y_hat_50, digits=3, out-
put_dict=True)
    roc = roc_auc_score(y_te, y_prob)
    prauc = average_precision_score(y_te, y_prob)
    best_t = _best_threshold_by_f1(y_te, y_prob)

    # Προαιρετικό calibration
    model_ref: Any = pipe
    calibrated_flag = False
    if calibrate:
        from sklearn.calibration import CalibratedClassifierCV
        cal = CalibratedClassifierCV(pipe, method="isotonic", cv="prefit")
        cal.fit(X_te, y_te)  # calibration πάνω στο holdout
        model_ref = cal
        calibrated_flag = True

        # Re-evaluate threshold on calibrated scores
        y_prob_cal = cal.predict_proba(X_te)[:, 1]
        best_t = _best_threshold_by_f1(y_te, y_prob_cal)

    # Αποθήκευση μοντέλου
    dump(model_ref, out_joblib)

    # Αποθήκευση META (για χρήση στο serve)
    meta = {
        "model_path": out_joblib,
        "calibrated": calibrated_flag,
        "metrics": {
            "roc_auc": float(roc),
            "pr_auc": float(prauc),
            "report": report,
        },
        "class_balance": {
            "positives": int((y == 1).sum()),
            "negatives": int((y == 0).sum()),
        },
        "features": {
```

```
            "categorical": CATEGORICAL_FEATURES,
            "numeric": NUMERIC_FEATURES,
        },
        "best_threshold_f1": float(best_t),
        "random_state": 42,
        "library": "xgboost" if _HAS_XGB else "random_forest",
        "version": 1,
    }
    meta_path = _meta_path_for(out_joblib)
    meta_path.write_text(json.dumps(meta, indent=2), encoding="utf-8")

    return {
        "roc_auc": float(roc),
        "pr_auc": float(prauc),
        "report": report,
        "model_path": out_joblib,
        "meta_path": str(meta_path),
        "best_threshold_f1": float(best_t),
        "calibrated": bool(calibrated_flag),
    }
def load_model(model_path: str = "ids_pipeline.joblib"):
    return load(model_path)
```

Παράρτημα Δ — Προδιαγραφή Serving & Alerting (Serving Spec)

- FlowAggregator: keys (src_ip,dst_ip,ports,proto), timeouts, Wi-Fi context (SSID/BSSID/VLAN, RSSI, deauth counters).
- Συμβατότητα features με το training (ALL_FEATURES).
- Προτεραιότητα κατωφλίου: --threshold > .meta.json > default.
- Cooldown per source (anti-storm).
- Σχήματα JSON - Alert output:


```
{
  "type": "ALERT",
  "data": {
    "when": 1750073105.742,
    "score": 0.932,
    "src_ip": "10.0.12.34",
    "dst_ip": "172.16.0.10",
    "proto": "TCP",
    "src_port": 51876,
    "dst_port": 443,
    "ssid": "CorpWiFi",
    "bssid": "ac:de:48:00:11:22",
    "vlan": "VLAN20",
    "rssi": -67.5,
```

```
    "action": "quarantine_vlan=Q-100"
  }
}
```