Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Πληροφορικής

Διδακτορική διατριβή

# Ασφάλεια Υπηρεσιών Ευφυών Μεταφορών: Μοντελοποίηση και Αξιολόγηση

# Security of Intelligent Transportation Services: Modelling and Assessment

**Ζαχαρένια Γαροφαλάκη**

Πειραιάς, Οκτώβριος 2023

**Πανεπιστήμιο Πειραιώς**
Τμήμα Πληροφορικής

Διδακτορική διατριβή

# Ασφάλεια Υπηρεσιών Ευφυών Μεταφορών: Μοντελοποίηση και Αξιολόγηση

**Ζαχαρένια Γαροφαλάκη**

*Τριμελής συμβουλευτική επιτροπή*

| | | |
|---|---|---|
| **Επιβλέπων:** | Χρήστος Δουληγέρης, | Καθηγητής Πανεπιστημίου Πειραιώς |
| **Μέλη:** | Δημήτριος Βέργαδος, | Καθηγητής Πανεπιστημίου Πειραιώς |
| | Ιωάννης Έλληνας, | Ομότιμος Καθηγητής Πανεπιστημίου Δυτικής Αττικής |

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή 5/10/2023.

| | | |
|---|---|---|
| **Χρήστος Δουληγέρης**<br>Καθηγητής<br>Πανεπιστημίου Πειραιώς | **Δημήτριος Βέργαδος**<br>Καθηγητής<br>Πανεπιστημίου Πειραιώς | **Ιωάννης Έλληνας**<br>Ομότιμος Καθηγητής<br>Πανεπιστημίου Δυτικής Αττικής |
| **Δημήτριος Καραγιάννης**<br>Καθηγητής<br>University of Vienna | **Δέσποινα Πολέμη**<br>Καθηγήτρια<br>Πανεπιστημίου Πειραιώς | **Σωτήρης Μοσχογιάννης**<br>Αναπληρωτής Καθηγητής<br>University of Surrey |

**Παναγιώτης Κοτζανικολάου**
Αναπληρωτής Καθηγητής
Πανεπιστημίου Πειραιώς

*”Distrust and caution are the parents of security”*
*Benjamin Franklin*

# Ευχαριστίες

Με την ολοκλήρωση της διατριβής μου, θα ήθελα να ευχαριστήσω κατ' αρχάς τον επιβλέποντα καθηγητή κ. Χρήστο Δουληγέρη. Τον ευχαριστώ που με εμπιστεύτηκε και μου έδωσε την ευκαιρία να εντρυφήσω στο πεδίο που με ενδιέφερε. Τον ευχαριστώ επίσης για την υπομονή του και για τη συνεργασία που είχαμε σε πολλά επίπεδα στην πορεία των τελευταίων χρόνων και ελπίζω αυτή η συνεργασία να ξεπεράσει το χρονικό πλαίσιο της σχέσης μεταξύ επιβλέποντα και υποψήφιας διδάκτορος.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τους δύο άλλους καθηγητές της τριμελούς επιτροπής παρακολούθησης της διατριβής μου, τον κ. Δ. Βέργαδο και τον κ. Ι. Έλληνα για το ενδιαφέρον τους όλα αυτά τα χρόνια. Θα ήθελα να αναφερθώ ειδικά στον κ. Έλληνα ο οποίος με προέτρεψε στην εκπόνηση της διατριβής μου, όταν κάτι τέτοιο μου φαινόταν πολύ πέραν των δυνατοτήτων μου.

Πολύτιμη για την αρτιότητα της διατριβής μου ήταν και η συνεισφορά από τα μέλη της επταμελούς επιτροπής, κ. Δ. Καραγιάννη, κ. Δ. Πολέμη, κ. Σ. Μοσχογιάννη και κ. Π. Κοτζανικολάου.

Επιπλέον, θέλω να εκφράσω την ευγνωμοσύνη μου στον Δημήτρη Καλλέργη με τον οποίο συνεργαστήκαμε σε σημαντικό μέρος των ερευνητικών προσπαθειών που άπτονται της παρούσας διατριβής. Υπήρξε δίπλα μου σε πολλές νέες εμπειρίες, σε όλες τις δυσκολίες και με βοήθησε να σταθώ στα πόδια μου μετά από κάθε αναποδιά και να συνεχίσω για την ολοκλήρωση της διατριβής μου.

Ευχαριστώ ολόψυχα την οικογένειά μου Εύη, Γιάννη, Νίκη, Μαξ, Μαρίνα και Ζωίτσα για την αμέριστη συμπαράσταση, κατανόηση και υποστήριξη που μου παρείχαν στη διάρκεια της δύσκολης και μοναχικής αυτής πορείας. Είναι όλοι τους, πάντα, το σημαντικότερο κίνητρό μου.

Οκτώβριος, 2023

Ζαχαρένια Γαροφαλάκη

# Περίληψη

Στην εποχή του Διαδικτύου των Αντικειμένων (Internet of Things, IoT), οι ευφυείς υπηρεσίες μεταφορών ενδείκνυνται για την αντιμετώπιση των σχετικών με τις μεταφορές ζητημάτων εντός αστικού περιβάλλοντος, με παράλληλο περιορισμό των εκπομπών διοξειδίου του άνθρακα και της κατανάλωσης ενέργειας μετακίνησης. Οι ευφυείς υπηρεσίες μεταφορών μπορούν να αποτελέσουν μια χρήσιμη λύση για τη μετακίνηση επιβατών που βρίσκονται μακριά από σταθμούς των μέσων μαζικής μεταφοράς. Πρόκειται για το πρόβλημα αναφερόμενο ως *πρόβλημα του πρώτου/τελευταίου μιλίου*, το οποίο συναντάται συχνά σε αστικά ή περιαστικά περιβάλλοντα καθώς και στα περιορισμένα/ιδιωτικά οδικά δίκτυα.

Μια ευφυής υπηρεσία μεταφορών αξιοποιεί τεχνολογικά και λειτουργικά χαρακτηριστικά του IoT, όπως η ασφαλής, κοινή χρήση δεδομένων με τριτομερείς υπηρεσίες. Ωστόσο, τα IoT χαρακτηριστικά της υπηρεσίας, μπορεί να αλλάξουν την αρχική μορφή των επιμέρους λειτουργιών της και να επηρεάσουν βασικές διαδικασίες της, όπως είναι η διαχείριση του στόλου των οχημάτων. Κατ' επέκταση, η ασφάλεια της υπηρεσίας, που εξαρτάται από τις επιμέρους αδυναμίες του κάθε στοιχείου υλικού ή λογισμικού εντός της υπηρεσίας, εξαρτάται και από τις σχετικές αδυναμίες της τριτομερούς υπηρεσίας.

Η πυρηνική διαδικασία διαχείρισης του στόλου μιας υπηρεσίας μεταφορών στο οικοσύστημα του IoT εμπεριέχει και τη σημαντική υποδιεργασία της στάθμευσης και της φόρτισης του στόλου. Η υποδιεργασία αυτή είναι πολύ κρίσιμη καθώς καθορίζει τη διαθεσιμότητα της υπηρεσίας. Σε πολλές εφαρμογές ο στόλος αποτελείται από ηλεκτρικά οχήματα (Electric Vehicle, EV), τα οποία αποτελούν σημαντικό μέρος των έξυπνων μεταφορών. Λειτουργούν εντός των έξυπνων ηλεκτρικών υποδομών με τις οποίες συνδέονται, σχηματίζοντας το δίκτυο φόρτισης ηλεκτρικών οχημάτων (Plug-in Electric Vehicle, PEV). Σε αυτά τα δίκτυα φόρτισης PEV, πληθώρα πρωτοκόλλων και προτύπων καθορίζουν τον τρόπο επικοινωνίας. Μεταξύ αυτών, ξεχωρίζει το Open Charge Point Protocol (OCPP) ως το πλέον χρησιμοποιούμενο πρωτόκολλο. Ωστόσο, μόλις το 2015 το πρωτόκολλο OCPP ενσωμάτωσε κάποιες δυνατότητες σχετικά με ζητήματα ασφάλειας.

Η διατριβή αυτή μελετά τη δυνατότητα αξιολόγησης και διατήρησης του επιπέδου ασφάλειας μιας υπηρεσίας μεταφορών, παρά τις προκλήσεις που συνδέονται με χαρακτηριστικά του IoT και τις ευπάθειες της διαδικασίας φόρτισης των οχημάτων της υπηρεσίας. Παρουσιάζεται μια πρωτότυπη υπηρεσία μεταφορών βασισμένη στο IoT, το έξυπνο λεωφορείο σε Πανεπιστημιούπολη (intelligent Bus on Campus, iBuC), η οποία λειτουργεί στο ιδιωτικό οδικό δίκτυο μιας πανεπιστημιούπολης. Μελετώνται ποια είναι τα IoT χαρακτηριστικά που καθιστούν την υπηρεσία iBuC μέρος του IoT οικοσυστήματος

και πώς διαμορφώνεται η φύση και η αρχιτεκτονική της, ενσωματώνοντας τα χαρακτηριστικά αυτά. Παρουσιάζεται στη συνέχεια η πλατφόρμα μοντελοποίησης SAPnet που περιλαμβάνει την εργαλειοθήκη οντολογίας μοντελοποίησης Stochastic Petri net (SPN), εμπλουτισμένη με τα κατάλληλα εργαλεία για την αξιολόγηση της ασφάλειας μιας υπηρεσίας μεταφορών με IoT χαρακτηριστικά. Η SAPnet αξιοποιείται για τη διερεύνηση των αλλαγών της συμπεριφοράς και του επιπέδου της ασφάλειας της υπηρεσίας iBuC. Επίσης, καταγράφεται ο βαθμός κατά τον οποίο η SAPnet διευκολύνει και επιταχύνει τη διαδικασία αξιολόγησης της ασφάλειας. Τέλος, προτείνεται μια τυπική αρχιτεκτονική ενός συστήματος φόρτισης που βασίζεται στο OCPP. Παρουσιάζονται επίσης, θέματα ασφάλειας, απειλές και σχετικά αντίμετρα ενός συστήματος φόρτισης EV και επαναξιολογείται η ασφάλεια της υπηρεσίας iBuC, λαμβάνοντας υπόψη τις ευπάθειες και τις αδυναμίες του συστήματος φόρτισης EV.

Σχετικά με την υπηρεσία μεταφορών iBuC, αναδεικνύεται πως αποτελεί μια ενδιαφέρουσα λύση στο πρόβλημα του πρώτου/τελευταίου μιλίου και πως ενσωματώνει αρκετά IoT χαρακτηριστικά ώστε να χαρακτηρίζεται από διαφάνεια, πολλαπλή αξιοποίηση και καινοτομία των λειτουργιών και των δεδομένων της. Σχετικά με το πρόβλημα της αξιολόγησης ασφάλειας μιας υπηρεσίας μεταφορών βασισμένης στο IoT, παρουσιάζεται μέθοδος μοντελοποίησης και αξιολόγησης της ασφάλειας με χρήση του φορμαλισμού SPN και εφαρμόζεται για πρώτη φορά σε υπηρεσία μεταφορών βασισμένη στο IoT, την iBuC. Η παραπάνω αξιολόγηση αναδεικνύει και την αλλαγή στη συμπεριφορά και στο επίπεδο της ασφάλειας της υπηρεσίας iBuC, εξαιτίας της αλλαγής ενός IoT χαρακτηριστικού της iBuC, δηλαδή της τριτομερούς υπηρεσίας με την οποία υπάρχει διαλειτουργικότητα. Επίσης, παρουσιάζεται η προτεινόμενη πλατφόρμα μοντελοποίησης SAPnet που επιτρέπει την έγκυρη αξιολόγηση του επιπέδου της ασφάλειας μιας οποιαδήποτε υπηρεσίας σε πραγματικό χρόνο και τη γρήγορη επανάληψη της διαδικασίας μετά από οποιαδήποτε αλλαγή στην υπηρεσία. Τέλος, η αξιολόγηση της υπηρεσίας με την ενσωμάτωση των ευπαθειών του δικτύου φόρτισης PEV αναδεικνύει ότι η επίλυση των ανοικτών ζητημάτων ασφάλειας στο δίκτυο φόρτισης PEV θα επηρεάσει αισθητά και το επίπεδο ασφάλειας της υπηρεσίας μεταφορών.

# Abstract

In the Internet of Things (IoT) era, intelligent transport services are suitable for addressing transport issues within an urban environment, while limiting carbon dioxide emissions and energy consumption. Intelligent transport services can be a useful solution for passengers who are located far from public transport nodes. This problem is referred to as the *first/last mile problem*, which is often encountered in urban or peri-urban environments as well as on restricted/private road networks.

An intelligent IoT transport service leverages technological and functional IoT features, such as the secure data sharing with third-party services. However, these IoT features may change the original form of the individual functions and affect core processes, such as the fleet management. By extension, the security of the service which depends on the individual weaknesses of each hardware or software component within the service, depends additionally on the relative weaknesses and vulnerabilities of the third-party service.

The core process of the fleet management of an IoT transport service includes the important sub-process of fleet parking and charging. This sub-process affects the availability of the service. Electric Vehicles (EVs) are an important part of smart transport and operate within the smart electric infrastructures and participate to the Plug-in Electric Vehicle (PEV) charging network. In these PEV charging networks, a multitude of protocols and standards defines the communication of the participating elements. Open Charge Point Protocol (OCPP) stands out as the most used protocol. However, it wasn't until 2015 that OCPP incorporated some security-related features.

This thesis studies the feasibility of assessing and maintaining the security level of a transport service, despite the challenges associated with the IoT characteristics of the service and the introduced vulnerabilities of the vehicles charging process. A prototype IoT transport service is presented, the intelligent Bus on Campus (iBuC), which operates on the private road network of a university campus. The IoT features that make the iBuC service a part of the IoT ecosystem are studied these features shape the service's nature and architecture. The SAPnet modeling platform is then presented, which includes the Stochastic Petri net (SPN) modeling ontology toolbox enriched with the appropriate tools to allow and facilitate the security assessment of an IoT service. SAPnet is used to highlight the changes of the behavior and the security level of the iBuC service. The extent to which SAPnet facilitates and accelerates the security assessment process is noted. Finally, a typical architecture of an OCPP charging system is proposed. The security issues, the threats, and the related countermeasures of an EV charging system are presented. The security of the iBuC service is, then, reassessed considering the vulnerabilities and

weaknesses of the EV charging system.

The iBuC service emerges as an interesting solution to the first/last mile problem and incorporates enough IoT features, such as transparency, multiple utilization and innovation of its operations and data. Regarding the security evaluation problem of an IoT-based transport service, a security modeling and evaluation method using the SPN formalism is presented and applied for the first time to an IoT service, the iBuC. The above evaluation highlights the change in the behavior and the security level of the iBuC service, due to the change of an IoT feature of the service, that is, the third-party service. Also, the proposed SAPnet modeling platform allows the valid assessment of the security level of any service in real time and the quick feasibility to reassess after any change to the service model. Finally, the assessment of the service incorporating the vulnerabilities of the PEV charging network highlights that solving the open security issues in the PEV charging network will also significantly affect the security level of the transport service.

# Περιεχόμενα

# Ευρετήριο εικόνων

# Ευρετήριο πινάκων

# Όροι και ακρωνύμια

| Ακρωνύμιο | Αγγλικός όρος | Ελληνικός όρος |
|---|---|---|
| MMM | | Μέσα Μαζικής Μεταφοράς |
| ARP | Address Resolution Protocol | |
| AES | Advanced Encryption Standard | |
| AMI | Advanced Metering Infrastructure | Προηγμένη υποδομή μέτρησης AMI |
| AC | Alternating Current | Εναλλασσόμενο ρεύμα |
| API | Application Programming Interface | Διασύνδεση προγραμματισμού εφαρμογών ή διεπαφή API ή διασύνδεση API |
| ARM | Architectural Reference Model | Αρχιτεκτονικό μοντέλο αναφοράς ή αρχιτεκτονική αναφοράς |
| | ARP spoofing | Πλαστογράφηση ARP |
| AI | Artificial Intelligence | Τεχνητή Νοημοσύνη |
| AV | Autonomous Vehicle | Αυτόνομο όχημα |
| AR | Availiability Requirement metric | Μετρική απαίτησης διαθεσιμότητας AR |
| BPNN | Back Propagation Neural Network | Νευρωνικό δίκτυο οπισθοδιάδοσης |
| BC | Blockchain | Αλυσίδα συστοιχιών |
| B2B | Business-to-Business | Διεπιχειρησιακά |
| B2C | Business-to-Consumer | Επιχειρησιοκαταναλωτικά |
| CS | Charging Station | Σταθμός φόρτισης CS |
| CSMS | Charging Station Management System | Σύστημα διαχείρισης CSMS |
| CSO/CPO | Charging System (or Point) Operator | Χειριστής σταθμού (ή σημείου) φόρτισης CSO (ή CPO) |
| CVE | Common Vulnerabilities and Exposures | (Βάση δεδομένων ή) Λίστα κοινών ευπαθειών CVE |
| CVSS | Common Vulnerability Scoring System | |
| CWE | Common Weakness Enumeration | (Βάση δεδομένων ή) Λίστα κοινών αδυναμιών CWE |
| CR | Confidentiality Requirement metric | Μετρική απαίτησης εμπιστευτικότητας CR |
| CU | Control Unit | Κεντρική μονάδα ελέγχου CU |
| CAN | Controller Area Network | (Ελεγκτής) σειριακού δικτύου αισθητήρων οχήματος CAN |
| | CVSS Base Score | Βασική βαθμολογία CVSS |
| | CVSS Temporal Score | Χρονική βαθμολογία CVSS |
| | Cyber attack | Κυβερνοχωρική επίθεση |

| Ακρωνύμιο | Αγγλικός όρος | Ελληνικός όρος |
|---|---|---|
| | Cyber-physical attack | Κυβερνοφυσική επίθεση |
| DoS | Denial of Service | Επίθεση άρνησης υπηρεσίας |
| DAA | Direct Anonymous Attestation | Πρωτόκολλο άμεσης ανώνυμης βεβαίωσης |
| DC | Direct Current | Συνεχές ρεύμα |
| DDoS | Distributed Denial-of-service | Κατανεμημένη επίθεση άρνησης υπηρεσίας |
| DER | Distributed Energy Resources | Κατανεμημένοι ενεργειακοί πόροι DER |
| DSO | Distribution System Operator | Διαχειριστής (συστήματος) διανομής DSO |
| EMSP | E-Mobility Service Provider | Πάροχος υπηρεσιών ηλεκτρικής κινητικότητας EMSP |
| EV | Electric Vehicle | Ηλεκτρικό όχημα |
| EVCC | Electric Vehicle Communication Controller | Ενσωματωμένος ελεγκτής επικοινωνίας οχήματος |
| EVSE | Electric Vehicle Supply Equipment | Εξοπλισμός παροχής ενέργειας (ή εξοπλισμός σύνδεσης) EVSE |
| ECU | Electronic Control Unit | (Ηλεκτρονική) μονάδα ελέγχου οχήματος ECU |
| ECC | Elliptic-Curve Cryptography | Κρυπτογράφηση ελλειπτικής καμπύλης ECC |
| EMS | Energy Management System | Σύστημα διαχείρισης ενέργειας EMS |
| ETDS | Energy Theft Detection System | Σύστημα ανίχνευσης κλοπής ενέργειας ETDS |
| ETA | Estimated Time of Arrival | Εκτιμώμενη ώρα άφιξης ETA |
| XML | Extensible Markup Language | |
| FDIA | False Data Injection Attack | Επίθεση (έγχυσης) εισαγωγής ψευδών δεδομένων |
| FPR | False Positive Rate | Ψευδο-θετικός ρυθμός (ή ποσοστό) |
| | Firing | Πυροδότηση μεταβάσεων |
| GPS | Global Positioning System | |
| GSM | Global System for Mobile Communications | |
| | Grid | Πλέγμα ή δίκτυο ενέργειας |
| GRT | Group Rapid Transit | Ταχεία μαζική μεταγωγή GRT |
| iBuC-PTS | iBuC-Public Transport Service | |
| iBuC-WFS | iBuC-Weather Forecasting Service | |
| | Insider attack | Εσωτερική (ή εκ των έσω) επίθεση |
| IEEE | Institute of Electrical and Electronics Engineers | Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών |
| IR | Integrity Requirement metric | Μετρική απαίτησης ακεραιότητας IR |
| iBuC | Intelligent Bus on Campus | |
| ITS | Intelligent Transportation System | Σύστημα Ευφυών Μεταφορών |
| IEC | International Electrotechnical Commission | Διεθνής Ηλεκτρομηχανική Επιτροπή |
| ISO | International Organization for Standardization | Διεθνής Οργανισμός Τυποποίησης |

| Ακρωνύμιο | Αγγλικός όρος | Ελληνικός όρος |
|---|---|---|
| IoT | Internet of Things | Διαδίκτυο των Αντικειμένων |
| IDS | Intrusion Detection System | Σύστημα ανίχνευσης εισβολών IDS |
| JSON | Java-Script Object Notation | |
| LAGs | Link Aggregation Groups | Διεπαφές πολυσύνδεσης LAGs |
| LC | Local Controller | (Τοπικός) Ελεγκτής LC |
| LP | Local Proxy | (Τοπικός) Πληρεξούσιος LP |
| M2M | Machine-to-Machine | Διαμηχανική |
| | Malware | (Επίθεση) κακόβουλου λογισμικού |
| MitM | Man-in-the-Middle | |
| | Masquerading/impersonation | Μεταμφίεση και απομίμηση |
| MITRE | Massachusetts Institute of Technology Research & Engineering | |
| MAC (address) | Media Access Control (address) | Φυσική διεύθυνση MAC |
| MAC | Message Authentication Code | Κώδικας επαλήθευσης (ταυτότητας) μηνυμάτων |
| | Meter bypassing attack | Επίθεση παράκαμψης μετρητή |
| NIST | National Institute of Standards and Technology | |
| NVD | National Vulnerability Database | |
| OCA | Open Charge Alliance | |
| OCPP | Open Charge Point Protocol | |
| OSI | Open System Interconnection | |
| OEM | Original Equipment Manufacturer | Αρχικός κατασκευαστής εξοπλισμού |
| | OTA updates tampering | Παραβίαση ραδιοδιεπαφών |
| | (Packet) replay attack | Επίθεση επανάληψης (πακέτων) |
| PRT | Personal Rapid Transit | Ταχεία προσωπική μεταγωγή PRT |
| PN | Petri net | |
| PUF | Physical Unclonable Functions | |
| PnC | Plug & Charge | |
| PEV | Plug-in Electric Vehicle | Εμβυσβατούμενο ηλεκτρικό όχημα |
| PLC | Power Line Communication | |
| | Power outage/overload | Επίθεση διακοπής/υπερφόρτωσης (ρεύματος) |
| PKI | Public Key Infrastructure | Υποδομή δημόσιου κλειδιού |
| PTS | Public Transportation System | Σύστημα δημοσίων μεταφορών |
| PWM | Pulse Width Modulation | Διαμόρφωση πλάτους σήματος |
| QoS | Quality of Service | Ποιότητα της υπηρεσίας |
| RFID | Radio Frequency Identification | Ταυτοποίηση μέσω ραδιοσυχνοτήτων RFID |
| | RKE cloning | Κλωνοποίηση κωδικών απομακρυσμένης εισόδου RKE |
| RBAC | Role-Based Access Control | Έλεγχος πρόσβασης βάσει ρόλων RBAC |
| SAPnet | Security Assessment Platform for Stochastic Petri net | Πλατφόρμα μετα-μοντελοποίησης και αξιολόγησης |
| SLAC | Signal-Level Attenuation Characterization | |

| Ακρωνύμιο | Αγγλικός όρος | Ελληνικός όρος |
|---|---|---|
| SOAP | Simple Object Access Protocol | |
| | Sinkhole attack | Επίθεση «καταβόθρας» |
| | Smart card cloning | Κλωνοποίηση έξυπνης κάρτας |
| SG | Smart Grid | Έξυπνο πλέγμα SG |
| SAE | Society of Automotive Engineers | Εταιρεία Μηχανικών Αυτοκινήτου |
| SDN | Software Defined Networking | Δικτύωση οριζόμενη από το λογισμικό |
| SOC | State Of Charge | Κατάσταση φόρτισης |
| SPN | Stochastic Petri net | Στοχαστική μοντελοποίηση Petri net |
| SQL | Structured Query Language | |
| | Substitution attack | Επίθεση αντικατάστασης |
| SECC | Supply Equipment Communication Controller | Ελεγκτής επικοινωνίας εξοπλισμού παροχής ενέργειας SECC |
| | Switching attack | Επίθεση μεταγωγής |
| SoC | System on Chip | Σύστημα σε ψηφίδα |
| | Tokens | Κουπόνια ή μάρκες |
| TCP/IP | Transmission Control Protocol/ Internet Protocol | |
| TLS | Transport Layer Security | |
| TPM | Trusted Platform Module | Μονάδα αξιόπιστης πλατφόρμας |
| USB | Universal Serial Bus | |
| uBSS | University Business Support System | Πανεπιστημιακό σύστημα υποστήριξης λειτουργιών uBSS |
| VAS | Value-Added Service | Υπηρεσία προστιθέμενης αξίας VAS |
| V2G | Vehicle-to-Grid | Όχημα-προς-πλέγμα |
| WFS | Weather Forecasting Service | Υπηρεσία πρόγνωσης καιρού |
| Wi-Fi | Wireless Fidelity | |
| | Wormhole attack | Επίθεση «σκουληκότρυπας» |

# Κεφάλαιο 1

# Εισαγωγή

## 1.1 Ευφυείς μεταφορές και ασφάλεια διεργασιών

Στην εποχή του Διαδικτύου των Αντικειμένων (Internet of Things, IoT), οποιοδήποτε αντικείμενο ή συσκευή μπορεί να διασυνδέεται και να ανταλλάσσει πληροφορίες και δεδομένα με άψυχα αντικείμενα ή με ζωντανούς οργανισμούς. Η αξιοποίηση αυτής της ευρείας δυνατότητας διασύνδεσης συσκευών αναβαθμίζει πολλές από τις υπάρχουσες υπηρεσίες, όπως είναι οι υπηρεσίες μεταφορών. Οι υπηρεσίες μεταφορών είναι μια από τις πιο σημαντικές δραστηριότητες στις σύγχρονες πόλεις και σε αυτό το πλαίσιο, έχουν προταθεί ποικίλες ερευνητικές και βιομηχανικές προσεγγίσεις ευφυών συστημάτων μεταφορών εντός του οικοσυστήματος του IoT [1],[2],[3],[4],[5]. Τα ζητήματα μεταφορών εντός του αστικού περιβάλλοντος, με παράλληλο περιορισμό των εκπομπών διοξειδίου του άνθρακα και της κατανάλωσης ενέργειας μετακίνησης, είναι δυνατό να αντιμετωπιστούν με την αξιοποίηση των αυτόνομων οχημάτων (Autonomous Vehicle, AV).

Τα αυτόνομα οχήματα είναι σε πολλές περιπτώσεις ηλεκτρικά τροφοδοτούμενα και φέρουν όλα τα απαραίτητα συστήματα ώστε να μπορούν να κινηθούν, να σταθμεύσουν και να φορτιστούν χωρίς την ανθρώπινη παρέμβαση. Μια ενδιαφέρουσα καινοτομία που φέρνουν τα οχήματα αυτά είναι η δυνατότητα να εκτελούν διαδρομές κατ' απαίτηση, που σημαίνει ότι ένα αυτόνομο όχημα που λειτουργεί ως Μέσο Μαζικής Μεταφοράς (ΜΜΜ) δεν απαιτείται να είναι σε συνεχή κίνηση, όπως συνηθίζεται στην περίπτωση των συμβατικών ΜΜΜ. Η λειτουργία κατ' απαίτηση των αυτόνομων οχημάτων είναι σίγουρα ένας σημαντικός παράγοντας μετριασμού για τις εκπομπές ρύπων και την κατανάλωση ενέργειας. Επιπλέον, η χρήση αυτόνομων οχημάτων αναμένεται να μειώσει προβλήματα κυκλοφοριακής συμφόρησης περιορίζοντας τα περιττά δρομολόγια των οχημάτων, όταν δεν υπάρχει ανάλογη ζήτηση από την πλευρά των επιβατών.

Τα προαναφερθέντα χαρακτηριστικά των αυτόνομων οχημάτων τα καθιστούν μια χρήσιμη λύση για τη μετακίνηση επιβατών που βρίσκονται μακριά από σταθμούς των Μέσων Μαζικής Μεταφοράς. Πρόκειται για το πρόβλημα αναφερόμενο ως *πρόβλημα του πρώτου/τελευταίου μιλίου (first/last mile problem)* [6], το οποίο συναντάται συχνά σε αστικά ή περιαστικά περιβάλλοντα καθώς και στα περιορισμένα/ιδιωτικά οδικά δίκτυα.

Οι λύσεις μεταφοράς που βασίζονται στο IoT ενσωματώνουν ευφυείς υπηρεσίες για τη βελτίωση της ποιότητας, της διαθεσιμότητας και της διαλειτουργικότητάς τους. Ένα από τα οφέλη της ενσωμάτωσης ευφυών υπηρεσιών είναι η επιτάχυνση της διαδικασίας λήψης αποφάσεων. Για τον σκοπό αυτό, αξιοποιούνται τεχνολογικά και λειτουργικά IoT χαρακτηριστικά των ευφυών υπηρεσιών, όπως η ασφαλής, κοινή χρήση δεδομένων με τριτομερείς υπηρεσίες. Ωστόσο, τα ίδια αυτά χαρακτηριστικά μπορεί να αλλάξουν την αρχική μορφή των επιμέρους λειτουργιών της υπηρεσίας μεταφοράς, καθώς εισάγονται νέοι παράγοντες στη διαδικασία λήψης αποφάσεων. Αυτές οι αλλαγές στη διαδικασία λήψης αποφάσεων, αναπόφευκτα θα επηρεάσουν βασικές διαδικασίες της υπηρεσίας, όπως είναι η διαχείριση του στόλου οχημάτων.

Η ασφάλεια της διαδικασίας διαχείρισης στόλου είναι ζωτικής σημασίας για την ευρύτερη αποδοχή και ανάπτυξη μιας υπηρεσίας μεταφοράς, μέρους του IoT οικοσυστήματος. Επειδή μια τέτοια υπηρεσία ενσωματώνει πολλές συσκευές και εφαρμογές, η συνολική ασφάλειά της εξαρτάται από τις επιμέρους αδυναμίες του κάθε στοιχείου υλικού ή λογισμικού εντός της υπηρεσίας. Κατά την ενσωμάτωση δεδομένων μιας τριτομερούς υπηρεσίας, οι σχετικές αδυναμίες της τριτομερούς υπηρεσίας γίνονται παράγοντες ασφάλειας και για την υπηρεσία μεταφοράς.

Η διαδικασία διαχείρισης στόλου μιας υπηρεσίας μεταφορών που βασίζεται στο IoT εμπεριέχει και τη σημαντική υποδιεργασία της στάθμευσης του στόλου, όταν δεν απαιτείται η εκτέλεση δρομολογίων. Η κρισιμότητα της υποδιεργασίας αυτής αυξάνεται, αν ο στόλος αποτελείται από έξυπνα ηλεκτρικά οχήματα (Electric Vehicle, EV), καθώς η διάρκεια της στάθμευσης θα πρέπει να αξιοποιείται στον μέγιστο δυνατό βαθμό για την ηλεκτρική φόρτιση των οχημάτων και τη διαφύλαξη της διαθεσιμότητάς τους και της διαθεσιμότητας της υπηρεσίας.

Τα οχήματα EV αποτελούν μέρος των έξυπνων μεταφορών και λειτουργούν εντός των έξυπνων ηλεκτρικών υποδομών με τις οποίες συνδέονται, σχηματίζοντας ένα σύνθετο σύστημα που αποτελείται από μια ποικιλία οντοτήτων και τεχνολογιών [7]. Αυτό το νέο σύστημα που προκύπτει από τη διασύνδεση των έξυπνων οχημάτων με το έξυπνο πλέγμα συμπεριλαμβάνει κινητές συσκευές, αυτόνομα οχήματα και ετερογενή κυβερνο-φυσικά συστήματα, εκθέτοντας όλα τα παραπάνω σε νέες απειλές και ευπάθειες [8]. Παρόλο που τεχνολογίες ασφάλειας έχουν ήδη ενσωματωθεί σε ορισμένα συστήματα [9], υπάρχει ανάγκη αυτές οι τεχνολογίες να προσαρμοστούν για την αντιμετώπιση των ειδικών προκλήσεων της υποδομής φόρτισης των οχημάτων EV.

Δεδομένου ότι πολλές οντότητες πρέπει να επικοινωνούν με ασφαλή και αποτελεσματικό τρόπο σε ένα σύστημα φόρτισης οχημάτων EV, που αναφέρεται επίσης ως δίκτυο Εμβυσβατούμενων Ηλεκτρικών Οχημάτων (Plug-in Electric Vehicle, PEV), μια πληθώρα πρωτοκόλλων και προτύπων χρησιμοποιούνται για τη ρύθμιση της επικοινωνίας αυτών των δικτύων. Οργανισμοί όπως ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization, ISO), η Διεθνής Ηλεκτρομηχανική Επιτροπή (International Electrotechnical Commission, IEC), η Εταιρεία Μηχανικών Αυτοκινήτου (Society of Automotive Engineers, SAE) και το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers, IEEE), συμβάλλουν στην προσπάθεια τυποποίησης αυτών των δικτύων.

Μεταξύ των πρωτοκόλλων για τα δίκτυα φόρτισης οχημάτων EV, το Open Charge Point Protocol (OCPP) ξεχωρίζει ως το de facto χρησιμοποιούμενο πρωτόκολλο σε 148 χώρες και στις 6 ηπείρους και υποστηρίζεται από περισσότερους από 65.000 ήδη εγκατεστημένους και λειτουργικούς σταθμούς φόρτισης [10]. Αναφέρεται επίσης ότι περισσότεροι από 40 κατασκευαστές σταθμών φόρτισης ενσωματώνουν το OCPP στα προϊόντα τους [11],[12]. Το πρωτόκολλο υποστηρίζεται από την παγκόσμια κοινοπραξία ηγετών δημόσιων και ιδιωτικών υποδομών ηλεκτρικών οχημάτων Open Charge Alliance (OCA), η οποία απαρτίζεται από περισσότερες από 220 εταιρείες-μέλη που δραστηριοποιούνται στον τομέα της ηλεκτρικής κινητικότητας [13]. Το OCPP [14] υποστηρίζει τις διαδικασίες κρατήσεων της υπηρεσίας, καθώς και τη διαχείριση των διαδικασιών χρέωσης, ώστε να διασφαλίσει την ποιότητα της υπηρεσίας (Quality of Service, QoS) και την αποτελεσματικότητα-εγκυρότητα της χρέωσης. Τα κύρια πλεονεκτήματα που οδήγησαν στην επικράτηση του OCPP έναντι άλλων πρωτοκόλλων είναι ότι είναι ένα ανοιχτό και δωρεάν πρωτόκολλο και υποστηρίζει τη λειτουργικότητα ανεξαρτήτως προμηθευτών, καθώς και τη γρήγορη και εύκολη ενσωμάτωση συσκευών.

## 1.2 Σκοπός και συμβολή της διατριβής

Σκοπός της διατριβής είναι η αξιολόγηση και διατήρηση του επιπέδου ασφάλειας μιας υπηρεσίας μεταφορών, παρά τις προκλήσεις που συνδέονται:

*(α)* με βασικά χαρακτηριστικά του Διαδικτύου των Αντικειμένων, όπως η ανταλλαγή δεδομένων με άλλες υπηρεσίες, και

*(β)* με τη διαδικασία φόρτισης των οχημάτων του στόλου της υπηρεσίας.

Σχετικά με το πρόβλημα του πρώτου/τελευταίου μιλίου, υπάρχουν προτάσεις για την επίλυσή του με υλοποιήσεις βασιζόμενες στα αυτόνομα οχήματα. Ορισμένες από τις προτεινόμενες λύσεις έχουν ήδη εφαρμοστεί με επιτυχία και χρησιμοποιούνται αυτήν τη στιγμή, όπως το ULTra (Urban Light Transit) [15] στο αεροδρόμιο Heathrow του Λονδίνου, το Masdar PRT [16] στην πόλη Masdar στην Ινδία και το SkyCube PRT [17] στην πόλη Suncheon στην Κορέα. Ωστόσο, η συνύπαρξη αυτόνομων και ελεγχόμενων από τον άνθρωπο οχημάτων στο ίδιο οδικό δίκτυο, δεν έχει αντιμετωπιστεί πλήρως και με επιτυχία [18]. Για παράδειγμα, το υπάρχον νομικό σύστημα στην πλειοψηφία των κρατών δεν προβλέπει μια τέτοια συνύπαρξη στο δημόσιο/ανοιχτό οδικό δίκτυο και δεν απαντά σε ζητήματα που θα προκύψουν λόγω πιθανών περιστατικών με την εμπλοκή και των δύο τύπων οχημάτων. Αυτός είναι ένας από τους λόγους για τους οποίους τα αυτόνομα οχήματα δοκιμάζονται και χρησιμοποιούνται, ως επί το πλείστον, σε περιορισμένα/ιδιωτικά οδικά δίκτυα, όπως σε πανεπιστημιουπόλεις, περιοχές αεροδρομίων πολλαπλών τερματικών σταθμών, συγκροτήματα κτιρίων νοσοκομείων ή μαζικούς χώρους αθλητικών εκδηλώσεων.

Με την ταχεία εξέλιξη του IoT, αυτές οι προτεινόμενες λύσεις που βασίζονταν στην μηχανή-προς-μηχανή ή διαμηχανική επικοινωνία (Machine-to-Machine, M2M), μπορεί να ενσωματωθούν στο οικοσύστημα του IoT και να ωφεληθούν από τα χαρακτηριστικά μιας τέτοιας υλοποίησης, όπως είναι η ανταλλαγή πληροφοριών με άλλα διαθέσιμα συστήματα πληροφοριών. Για παράδειγμα, οι λειτουργίες των αυτόνομων οχημάτων θα μπορούσαν να είναι ακόμα πιο αποτελεσματικές εάν παραμετροποιούνταν από δεδομένα

εισόδου ενός τριτομερούς συστήματος πληροφοριών και πρόβλεψης καιρικών συνθηκών. Από την άλλη πλευρά, ένα σύστημα παρακολούθησης της κυκλοφορίας μπορεί να ωφεληθεί χρησιμοποιώντας στατιστικά δεδομένα που παράγονται από τα αυτόνομα οχήματα που χρησιμοποιούνται σε μια περιοχή. Αυτή η ανταλλαγή δεδομένων θα συνέβαλε ώστε οι υπάρχουσες λύσεις M2M να γίνουν μέρος του οικοσυστήματος IoT.

Στην παρούσα διατριβή εισάγεται η υπόθεση πως το πρόβλημα του πρώτου/τελευταίου μιλίου μπορεί να επιλυθεί επαρκώς με μια υπηρεσία μεταφορών η οποία δεν θα περιορίζεται στην M2M επικοινωνία των δρώντων στοιχείων που τη συνθέτουν, αντιθέτως θα ενσωματώνει και θα ωφελείται από IoT χαρακτηριστικά λειτουργίας. Η υπόθεση αυτή στηρίζεται από την παρουσίαση του πρωτότυπου μιας υπηρεσίας μεταφορών, που βασίζεται στο IoT και λειτουργεί με στόχο την επίλυση του προβλήματος αυτού στο ιδιωτικό/περιορισμένο οδικό δίκτυο μιας πανεπιστημιούπολης. Επίσης, μελετάται το ερευνητικό ερώτημα σχετικά με το ποια είναι αυτά τα IoT χαρακτηριστικά που καθιστούν την προτεινόμενη υπηρεσία μεταφορών μέρος του IoT οικοσυστήματος και πώς διαμορφώνεται η φύση και η αρχιτεκτονική της υπηρεσίας, ενσωματώνοντας τα χαρακτηριστικά αυτά.

Η συμβολή αυτής της διατριβής σχετικά με το υπό μελέτη πρόβλημα του πρώτου/ τελευταίου μιλίου συνοψίζεται στα ακόλουθα:

- Πρόταση της πρωτότυπης υπηρεσίας μεταφορών, το έξυπνο λεωφορείο στην Πανεπιστημιούπολη (Intelligent Bus on Campus, iBuC).
- Παρουσίαση του αρχιτεκτονικού μοντέλου εφαρμογής της υπηρεσίας iBuC, των λειτουργιών και των IoT χαρακτηριστικών της σε ένα προσαρμοσμένο σενάριο πραγματικής λειτουργίας.

Η ενσωμάτωση δεδομένων από τριτομερή υπηρεσία εισάγει, παράλληλα, γεγονότα που δεν μπορεί να προβλεφθούν πλήρως ή εγκαίρως από τα συστήματα και το λογισμικό της υπηρεσίας μεταφοράς που βασίζεται στο IoT. Η έλλειψη μιας λεπτομερούς χρονικής ακολουθίας για τα γεγονότα αυτά και η εγγενής πολυπλοκότητα της υπηρεσίας που βασίζεται στο IoT είναι δυνατό να απεικονιστούν επαρκώς με τη χρήση της στοχαστικής μεθόδου μοντελοποίησης Stochastic Petri net (SPN) [19]. Ο φορμαλισμός SPN επιτρέπει τη μοντελοποίηση της διάρκειας των δραστηριοτήτων και της καθυστέρησης μεταξύ των γεγονότων χρησιμοποιώντας κουπόνια ή μάρκες (tokens) και αξιοποιώντας τη δυνατότητα πυροδότησης (firing) μεταβάσεων από κατάσταση σε κατάσταση της υπηρεσίας [20], [21]. Έτσι, η υιοθέτηση του μοντέλου SPN μπορεί να αποτελέσει βάση για την ανάπτυξη μιας μεθόδου αξιολόγησης της ασφάλειας για τις υπηρεσίες που βασίζονται στο IoT, ακόμα και στη φάση σχεδιασμού των υπηρεσιών αυτών.

Οι πρόσφατες μελέτες για τη διαχείριση στόλου επικεντρώνονται κυρίως στον προγραμματισμό δρομολογίων και στην έξυπνη κατανομή πόρων. Σε αυτές τις μελέτες [22], [23], η πρόσβαση σε πραγματικό χρόνο σε πληροφορίες σχετικά με τις περιβαλλοντικές συνθήκες, τις συνθήκες κυκλοφορίας και τις καιρικές συνθήκες θεωρείται παράγοντας αποδοτικότητας, αποτελεσματικότητας και βελτίωσης της ποιότητας. Ωστόσο, γεγονός είναι ότι οι πληροφορίες σχετικά με αυτές τις συνθήκες ενδέχεται να παρέχονται από μια τριτομερή υπηρεσία, ενώ η ενσωμάτωση τέτοιων εξωγενών δεδομένων τροποποιεί τη διαδικασία διαχείρισης στόλου. Επιπλέον, αν και

οι απειλές ασφάλειας στα συστήματα μεταφορών που βασίζονται στο IoT έχουν προσελκύσει το ενδιαφέρον της ερευνητικής κοινότητας [24], προηγούμενες εργασίες δεν διενεργούν αξιολόγηση ασφάλειας της διαχείρισης του στόλου και, κατά συνέπεια, δεν μελετούν το πώς η ενσωμάτωση εξωγενών δεδομένων επηρεάζει την ασφάλεια της υπηρεσίας.

Σχετικά με το πρόβλημα της αξιολόγησης ασφάλειας μιας υπηρεσίας μεταφορών που βασίζεται στο IoT, έχει αναδειχθεί στη βιβλιογραφία πως η χρήση του φορμαλισμού SPN βοηθά στον σχεδιασμό μοντέλου μιας υπηρεσίας και μπορεί να αποτελέσει τη βάση για την ανάπτυξη μιας μεθόδου αξιολόγησης ασφάλειας της υπηρεσίας. Διερευνάται η υπόθεση πως ο φορμαλισμός SPN μπορεί να αξιοποιηθεί για την επαρκή μοντελοποίηση και την αξιολόγηση ασφάλειας μιας υπηρεσίας μεταφορών, όπως η προτεινόμενη iBuC. Η υπόθεση αυτή στηρίζεται από την προτεινόμενη πλατφόρμα μετα-μοντελοποίησης και αξιολόγησης (Security Assessment Platform for Stochastic Petri net, SAPnet), που περιλαμβάνει την εργαλειοθήκη οντολογίας SPN, εμπλουτισμένη με τα κατάλληλα εργαλεία για την αξιολόγηση ασφάλειας του μοντέλου. Με τη βοήθεια της προτεινόμενης πλατφόρμας, ερευνάται το αν και πώς επηρεάζεται η συμπεριφορά και το επίπεδο ασφάλειας της IoT υπηρεσίας μεταφορών από την αλλαγή ενός IoT χαρακτηριστικού της, όπως η φύση της ενσωματωμένης τριτομερούς υπηρεσίας. Επίσης, καταγράφεται ο βαθμός κατά τον οποίο η SAPnet διευκολύνει και επιταχύνει τη διαδικασία αξιολόγησης ασφάλειας της υπηρεσίας.

Η συμβολή αυτής της διατριβής σχετικά με το υπό μελέτη πρόβλημα της αξιολόγησης της ασφάλειας μιας υπηρεσίας μεταφορών όπως η προτεινόμενη iBuC, συνοψίζεται στα ακόλουθα:

- Παρουσίαση της πλατφόρμας μοντελοποίησης SAPnet που περιλαμβάνει την εργαλειοθήκη οντολογίας μοντελοποίησης SPN, εμπλουτισμένη με τα κατάλληλα εργαλεία για την αξιολόγηση ασφάλειας μιας υπηρεσίας που βασίζεται στο IoT.
- Μοντελοποίηση της διεργασίας διαχείρισης στόλου της προτεινόμενης υπηρεσίας μεταφορών iBuC σε δύο σενάρια ανταλλαγής δεδομένων με διαφορετική ανά περίπτωση τριτομερή υπηρεσία.
- Αξιολόγηση ασφάλειας της προτεινόμενης υπηρεσίας μεταφορών iBuC στα δύο προαναφερθέντα σενάρια πραγματικής λειτουργίας.

Η ασφάλεια της διαχείρισης στόλου μιας υπηρεσίας μεταφορών που βασίζεται στο IoT επηρεάζεται, μεταξύ άλλων και από την ασφάλεια των συστημάτων φόρτισης του στόλου οχημάτων EV. Άρα συνδέεται με την ασφάλεια των ίδιων των EVs, των οδηγών τους, της υποδομής του συστήματος φόρτισης, του παρόχου ηλεκτρικής ενέργειας και του ηλεκτρικού δικτύου. Καθώς η ηλεκτρική κινητικότητα γίνεται όλο και πιο δημοφιλής, οι επιθέσεις ασφάλειας εναντίον αυτών των στοιχείων είναι όλο και πιο συχνές. Την περίοδο 2019-2021, οι επιθέσεις στον κυβερνοχώρο κατά των EVs αυξήθηκαν κατά 225% [25] σε σχέση με τις προηγούμενες χρονιές. Μελέτη αποκάλυψε, επίσης, σοβαρές ευπάθειες που μπορεί να αποτελέσουν αντικείμενο εκμετάλλευσης στους σταθμούς φόρτισης 16 διαφορετικών κατασκευαστών [26] και οι Acharya et al. [27] ανέφεραν ότι τα τοπικά ηλεκτρικά μικρο-πλέγματα γίνονται περισσότερο ευάλωτα εξαιτίας της έλλειψης ασφάλειας στα δεδομένα των EVs και των σταθμών φόρτισης EV.

Η τρέχουσα διατριβή συγκεντρώνει τα θέματα ασφάλειας και απορρήτου όλων των ενεργών στοιχείων ενός συστήματος φόρτισης οχημάτων EV, που λειτουργεί βασιζόμενο στην πιο πρόσφατη από τις τέσσερεις εκδόσεις του πρωτοκόλλου OCPP που κυκλοφόρησαν, την έκδοση OCPP 2.0.1 [28]. Αυτή η έκδοση, που αναφέρεται και ως OCPP 2.0, κυκλοφόρησε το 2018 και περιλαμβάνει βελτιωμένα χαρακτηριστικά ασφάλειας. Το OCPP 2.0 είναι η βελτίωση της προηγούμενης έκδοσης 1.6 [29], που πρώτη εισήγαγε περιορισμένες δυνατότητες ασφάλειας για το πρωτόκολλο το 2015. Το OCPP 2.0 ενσωματώνει λειτουργίες, όπως την ασφαλή ενημέρωση υλικο-λογισμικού, την καταγραφή και ειδοποίηση συμβάντων, τον ασφαλή έλεγχο της ταυτότητας [30], την υποστήριξη ασφάλειας του επιπέδου μεταφοράς (Transport Layer Security, TLS) και τη διαχείριση κλειδιών των πιστοποιητικών από την πλευρά του χρήστη της υπηρεσίας φόρτισης.

Λαμβάνεται υπόψη πως η διαχείριση στόλου της υπηρεσίας μεταφορών iBuC επηρεάζεται από τις ευπάθειες ασφάλειας της υποδιεργασίας φόρτισης του στόλου οχημάτων της. Για τον λόγο αυτό και εξαιτίας του οτι η ασφάλεια των συστημάτων φόρτισης οχημάτων είναι ένα πεδίο έρευνας της τελευταίας δεκαετίας, καταγράφονται αναλυτικές πληροφορίες σχετικά με τα θέματα ασφάλειας, τις απειλές και τα αντίμετρα για τα συστήματα φόρτισης οχημάτων EV. Επίσης, γίνεται η συσχέτιση των προαναφερθέντων απειλών ασφάλειας με κάθε στοιχείο του συστήματος φόρτισης EV, έτσι ώστε οι απειλές αυτές να συμπεριληφθούν στη διαδικασία αξιολόγησης ασφάλειας της υπηρεσίας μεταφορών iBuC.

Η συμβολή αυτής της διατριβής σχετικά με το υπό μελέτη πρόβλημα της ασφάλειας της υποδιεργασίας φόρτισης του στόλου οχημάτων συνοψίζεται στα ακόλουθα:

- Πρόταση μιας τυπικής αρχιτεκτονικής και περιγραφή των οντοτήτων που συμμετέχουν σε ένα σύστημα φόρτισης οχημάτων EV που βασίζεται στο OCPP.
- Παρουσίαση των θεμάτων ασφάλειας, των απειλών, και των σχετικών αντίμετρων σε συσχέτιση τους με τα δρώντα στοιχεία εντός του συστήματος φόρτισης EV.
- Αξιολόγηση της ασφάλειας της προτεινόμενης υπηρεσίας μεταφορών iBuC λαμβάνοντας υπόψη τις ευπάθειες και τις αδυναμίες του συστήματος φόρτισης EV.

## 1.3 Δομή της διατριβής

Το δεύτερο κεφάλαιο που ακολουθεί, περιλαμβάνει την αναλυτική παρουσίαση της υπάρχουσας βιβλιογραφίας σχετικά με:

*(α)* τις προτάσεις υπηρεσιών μεταφοράς βασιζόμενες σε αυτόνομα οχήματα,

*(β)* τις μεθόδους μοντελοποίησης και αξιολόγησης ασφάλειας υπηρεσιών που βασίζονται στο IoT, και

*(γ)* τις υπάρχουσες έρευνες για τα συστήματα φόρτισης ηλεκτρικών οχημάτων EV και τα ζητήματα ασφάλειας που τα διέπουν.

Στο τρίτο κεφάλαιο παρουσιάζεται η πρωτότυπη υπηρεσία μεταφορών iBuC. Πιο συγκεκριμένα:

*(α)* προτείνεται το αρχιτεκτονικό μοντέλο εφαρμογής της υπηρεσίας,

*(β)* περιγράφονται οι λειτουργίες της, και

*(γ)* αναλύονται τα IoT χαρακτηριστικά της υπό το πρίσμα ενός προσαρμοσμένου σεναρίου πραγματικής λειτουργίας της υπηρεσίας.

Το τέταρτο κεφάλαιο περιλαμβάνει:

*(α)* την παρουσίαση της μεθόδου αξιολόγησης της ασφάλειας για μια υπηρεσία του IoT οικοσυστήματος, που βασίζεται στο μοντέλο SPN της υπηρεσίας και στη λίστα κοινών ευπαθειών (Common Vulnerabilities and Exposures, CVE) των επιμέρους στοιχείων,

*(β)* την παρουσίαση του μετα-μοντέλου, της σημασιολογίας και των αλγόριθμων που συνθέτουν το εργαλείο μετα-μοντελοποίησης SAPnet, που βασίζεται στην πλατφόρμα ADOxx©, και

*(γ)* την αξιοποίηση της SAPnet, για την αξιολόγηση της ασφάλειας του στοχαστικού μοντέλου της υπηρεσίας iBuC σε δύο σενάρια πραγματικής λειτουργίας.

Το πέμπτο κεφάλαιο περιλαμβάνει:

*(α)* την περιγραφή των OCPP συστημάτων φόρτισης οχημάτων EV, καθώς και των δρώντων στοιχείων που συμμετέχουν σε αυτά,

*(β)* την παρουσίαση των καταγεγραμμένων επιθέσεων ασφάλειας και των αντίστοιχων αντίμετρων, σε σχέση με τα επιμέρους δρώντα στοιχεία που επηρεάζονται από κάθε τύπο επίθεσης,

*(γ)* την παρουσίαση των τεχνικών διαφύλαξης του απορρήτου, των μηχανισμών επαλήθευσης της ταυτότητας και εξουσιοδότησης, καθώς και των μηχανισμών ανίχνευσης και εκτροπής επιθέσεων ασφάλειας, και

*(δ)* την επικεντρωμένη μελέτη και ανάδειξη των επιπτώσεων ασφάλειας που εισάγονται από τις ευπάθειες του πρωτοκόλλου OCPP και επηρεάζουν τη διαδικασία φόρτισης οχημάτων και κατ' επέκταση την υπηρεσία iBuC.

Στο έκτο κεφάλαιο παρατίθενται:

*(α)* τα συμπεράσματα που εξήχθησαν στο πλαίσιο μελέτης της τρέχουσας διατριβής,

*(β)* οι προτάσεις για μελλοντικές βελτιώσεις των προτεινόμενων λύσεων, καθώς και

*(γ)* προτάσεις διεύρυνσης της μελλοντικής ερευνητικής μελέτης στο πεδίο της διατριβής.

# Κεφάλαιο 2

# Βιβλιογραφική έρευνα

## 2.1 Προτάσεις υπηρεσιών μεταφοράς

Οι μελέτες για τα αυτόνομα οχήματα, γνωστά και ως οχήματα χωρίς οδηγό, μπορεί να κατηγοριοποιηθούν ανάλογα με την οπτική γωνία στην οποία επικεντρώνονται οι μελέτες. Μια από αυτές τις κατηγορίες περιλαμβάνει τις μεθόδους ή τους αλγόριθμους που χρησιμοποιούνται για τον έλεγχο των οχημάτων (όπως σωστή στάση, εκκίνηση, επιτάχυνση, αποφυγή εμποδίων, χειρισμός διαδρομής και στάθμευση). Μια δεύτερη κατηγορία περιλαμβάνει τις μελέτες σχετικά με τις φυσικές ρυθμίσεις των οχημάτων, καθώς τα AVs κατασκευάζονται με προσθήκη εξοπλισμού σε συμβατικά οχήματα ή σχεδιάζονται από την αρχή. Ένα άλλο μέρος της βιβλιογραφίας μελετά τη χρήση των AVs στον τομέα των δημόσιων μεταφορών. Οι μελέτες αυτές καταλήγουν στο συμπέρασμα ότι μια τέτοια χρήση παρέχει βελτιώσεις σε διάφορους τομείς όπως την κυκλοφορία, τη ρύπανση του περιβάλλοντος, την κατανάλωση ενέργειας και τον αριθμό των επιβατών που εξυπηρετούνται ανά έτος.

Προκύπτουν αναφορές σε δύο κύριους τύπους αυτόνομων οχημάτων. Ο τύπος Personal Rapid Transit (PRT) [31] περιλαμβάνει τα αυτόνομα οχήματα που έχουν μέγεθος ανάλογο με ένα προσωπικό όχημα ιδιωτικής χρήσης (IX) και χωρητικότητα επιβατών 4-6 άτομα. Ο τύπος Group Rapid Transit (GRT) [31] περιλαμβάνει τα αυτόνομα οχήματα με μεγαλύτερη χωρητικότητα επιβατών (έως 70 άτομα), που τα καθιστά καταλληλότερα για μαζικές μεταφορές. Το PRT και το GRT είναι αστικά συστήματα μεταφοράς που μπορούν να αξιοποιηθούν σε υπηρεσίες μεταφορών σε τμήματα μιας πόλης ή τοποθεσίες με περιορισμένα/ιδιωτικά οδικά δίκτυα, όπως αυτά των αεροδρομίων πολλαπλών τερματικών σταθμών ή των πανεπιστημιουπόλεων.

Υπάρχουν προτάσεις σχετικές με τον προσδιορισμό της καλύτερης διαδρομής για κάθε ταξίδι ενός αυτόνομου οχήματος. Ένα σύστημα PRT που αποτελείται από ένα στόλο οχημάτων και έχει πολλούς κόμβους/σταθμούς στην περιοχή λειτουργίας του, μπορεί να επωφεληθεί από κάποιον αλγόριθμο [32], μέσω του οποίου ελέγχεται η ορθή πορεία των οχημάτων σε σχέση με την προδιαγεγραμμένη διαδρομή. Επίσης, ο αλγόριθμος βοηθάει στη διαχείριση των αδρανών οχημάτων του στόλου, για την καλύτερη χρήση του οδικού δικτύου.

Υπάρχουν επίσης μελέτες για αυτόνομα οχήματα που λειτουργούν με ηλεκτρικό ρεύμα και όχι καύσιμα [6],[33],[34],[35]. Το πρωτότυπο όχημα της εταιρείας Google [33] είναι ένα πλήρως ηλεκτρικό όχημα, που μπορεί να ανιχνεύσει αντικείμενα γύρω του, προς όλες τις κατευθύνσεις. Το όχημα αυτό είναι εξοπλισμένο με σύστημα αυτόματου πιλότου για αυτόνομη οδήγηση, διεύθυνση και πέδηση. Εμπνευσμένο από το αυτόνομο όχημα της Google, έχει προταθεί και παρόμοιο όχημα που υποστηρίζει αυστηρά έναν επιβάτη [34]. Ο επιβάτης επιλέγει τον προορισμό του ταξιδιού και το όχημα ακολουθεί μία από τις προκαθορισμένες διαδρομές του. Το όχημα διατηρείται σε σωστή τροχιά, μέσω υπολογισμών των δεδομένων Global Positioning System (GPS) του οχήματος. Στο ευρωπαϊκό έργο City Automated Transport System (CATS) [6], πραγματοποιήθηκε μια επίδειξη χρησιμοποιώντας πρωτότυπα του ηλεκτρικού λεωφορείου με το όνομα Navya [36]. Το σύστημα ελέγχου των οχημάτων δημιουργεί τρισδιάστατους χάρτες του χώρου εξυπηρέτησης σε πραγματικό χρόνο, ενώ παράλληλα συγκεντρώνει δεδομένα σχετικά με τη θέση και την κατάσταση των οχημάτων. Ωστόσο, κάποια ανθρώπινη παρέμβαση θεωρείται απαραίτητη σε αυτή την υλοποίηση, για την περίπτωση που διασταυρώνονται οι διαδρομές δύο οχημάτων. Άλλη πρόταση αναδεικνύει την αξιοποίηση οχήματος που κινείται αυτόνομα ακολουθώντας μια συγκεκριμένη χρωματική διαδρομή ενώ υπακούει στα οδικά σήματα [35]. Σε αυτή την περίπτωση, ο ψηφιακός χάρτης προσαρμόζεται συνεχώς στην είσοδο δεδομένων των αισθητήρων του οχήματος. Γενικά, οι προτεινόμενες υλοποιήσεις περιγράφουν οχήματα που φέρουν διάφορους τύπους αισθητήρων, όπως:

*(α)* λέιζερ (laser) [33],

*(β)* ραντάρ (radars) [33],

*(γ)* αισθητήρια απόστασης με σάρωση laser (Light Detection And Ranging, LiDAR) [6],[35],

*(δ)* κάμερες [6],[33],

*(ε)* αισθητήρες υπερήχων μέτρησης απόστασης (ultra-sonic sensors) [34],

*(στ)* δέκτες/πομπούς GPS [6],[35],

*(ζ)* αισθητήρες υπερύθρων (infrared sensors) [35].

Επιπρόσθετα, όλα τα οχήματα περιλαμβάνουν ένα σύστημα ελέγχου και έχουν κάποια διεπαφή επικοινωνίας. Τα παραπάνω επιτρέπουν στα οχήματα την κίνηση με αποφυγή εμποδίων.

Το 2015, πραγματοποιήθηκε παρουσίαση των αποτελεσμάτων του έργου CityMobil2 στην ελληνική πόλη των Τρικάλων [37]. Στο πλαίσιο του έργου, προτεινόταν η χρήση ενός αυτοματοποιημένου οχήματος δημοσίων μεταφορών (Automated Public Transport Vehicle, APTV) για την υποστήριξη του κύριου δικτύου μαζικής μεταφοράς ως απάντηση στο πρόβλημα του πρώτου/τελευταίου μιλίου. Το αυτόνομο όχημα μπορούσε να κινείται στο δημόσιο οδικό δίκτυο (δηλαδή παράλληλα με την κίνηση πεζών και συμβατικών οχημάτων) και υποστήριζε λειτουργίες κίνησης/στάσης (start/stop) και αποφυγής εμποδίων. Η περιοχή κάλυψης του οχήματος CityMobil2 είχε αδιάλειπτη κάλυψη σημάτων Global System for Mobile Communications (GSM) και Wi-Fi. Μέσω του προγράμματος αυτού, διερευνήθηκε η προβλεπόμενη επίδραση ενός αυτοματοποιημένου οχήματος μαζικής μεταφοράς στην κυκλοφορική κατάσταση της πόλης. Παρόμοιες προτάσεις κατατέθηκαν για την προσθήκη αυτόνομων οχημάτων τύπου GRT στο δίκτυο

μεταφορών της πόλης Guangzhou [31] και για τη χρήση αυτής της τεχνολογίας στη μητροπολιτική περιοχή της Ουάσιγκτον [18].

Οι προαναφερόμενες προτάσεις έχουν κυρίως χαρακτηριστικά διαμηχανικής επικοινωνίας M2M, δηλαδή επιδιώκουν επίλυση συγκεκριμένων προβλημάτων, αναπτύσσονται με κύριο στόχο την εξυπηρέτηση των λειτουργιών του ίδιου του παρόχου/δημιουργού (Business-to-Business, B2B) και ενσωματώνουν εξειδικευμένο λογισμικό. Αντίθετα, με μια λύση που βασίζεται στο IoT επιδιώκεται πρωτίστως η καινοτομία. Επίσης, μια λύση που βασίζεται στο IoT αναπτύσσεται με στόχο την εξυπηρέτηση των λειτουργιών του παρόχου/δημιουργού καθώς και των χρηστών/πελατών του (Business-to-Consumer, B2C) και ενσωματώνει λογισμικό ανοιχτού κώδικα. Επομένως, υπάρχει ανάγκη να εντοπιστούν τα απαραίτητα πρόσθετα χαρακτηριστικά για τη μετάβαση από μια λύση με M2M χαρακτηριστικά σε μια λύση στο μοντέλο του IoT.

## 2.2 Μελέτες ασφάλειας συστημάτων φόρτισης οχημάτων EV

Σε αυτήν την ενότητα παρουσιάζονται οι υπάρχουσες μελέτες σχετικά με την ασφάλεια των συστημάτων φόρτισης οχημάτων EV. Ο Πίνακας 1 περιλαμβάνει:

*(α)* το αρχιτεκτονικό μοντέλο που παρουσιάζεται σε κάθε μελέτη και, ως εκ τούτου, το σύνολο των υπό μελέτη δρώντων στοιχείων ενός συστήματος φόρτισης EV,

*(β)* το σύνολο των αντίμετρων ασφάλειας που τυχόν παρατίθενται,

*(γ)* την παρουσίαση κάποιας συσχέτισης μεταξύ των απειλών ασφάλειας και των επηρεαζόμενων δρώντων στοιχείων,

*(δ)* τη μελέτη των θεμάτων ασφάλειας του πρωτοκόλλου OCPP συγκεκριμένα, αν συμπεριλαμβάνεται, και

*(ε)* την ύπαρξη αναφοράς σε ανοικτά ζητήματα ασφάλειας.

Ο Πίνακας 1 καταδεικνύει επίσης τι μελετήθηκε, μερικώς ή σφαιρικά, τι δεν εξετάστηκε από την κάθε σχετική μελέτη στη βιβλιογραφία, καθώς και μια σύγκριση μεταξύ αυτών των μελετών, βάσει των παραπάνω κριτηρίων.

Σε εργασία που παρουσιάστηκε στις αρχές του 2016, οι Han και Xiao [38] επικεντρώθηκαν στα προβλήματα διατήρησης του απορρήτου σε δίκτυα V2G. Παρουσίασαν σειρά τυπικών επιθέσεων κατά του απορρήτου των δεδομένων, καθώς και λύσεις με στόχο την προστασία του. Επιπλέον, παρουσίασαν άλυτα ζητήματα και πιθανά αντίμετρα που προέκυπταν βάσει των τότε υπαρχουσών λύσεων. Το άρθρο παρείχε μια πλήρη ανάλυση σχετικά με τα ζητήματα διατήρησης του απορρήτου σε εφαρμογές Vehicle-to-Grid (V2G). Η εργασία επικεντρώθηκε κυρίως σε ζητήματα σχετικά με το απόρρητο των δεδομένων τοποθεσίας, της ταυτότητας και της χρέωσης, καθώς και με τη διαφύλαξη του απορρήτου κατά τις διαδικασίες ελέγχου της ταυτότητας και χρέωσης. Παρόλο που η έρευνα εξέτασε τα ζητήματα ασφάλειας και απορρήτου ενός συστήματος φόρτισης οχημάτων EV, οι ευπάθειες του πρωτοκόλλου φόρτισης δεν αναλύθηκαν. Επίσης, η ανάλυση επικεντρώθηκε στην αρχιτεκτονική του δικτύου V2G και όχι στα δρώντα στοιχεία φόρτισης EV. Επιπλέον, δεν παρασχέθηκε κάποια συσχέτιση μεταξύ

Πίνακας 1. Μελέτες για την ασφάλεια συστημάτων φόρτισης οχημάτων EV

| # | Έτος | Επίκεντρο μελέτης | Αντίμετρα | Συσχετισμός απειλών-δρώντων στοιχείων | Εκδόσεις OCPP | Ζητήματα ασφάλειας |
|---|---|---|---|---|---|---|
| [38] | 2016 | Δίκτυο V2G | ✓ | - | - | ✓ |
| [39] | 2017 | Υποδομή φόρτισης | - | - | - | ✓ |
| [40] | 2017 | Δεδομενόγραμμα στοιχείου φόρτισης | ✓ | ✓ | 1.6 | ✓ |
| [41] | 2020 | Υποδομή φόρτισης στην Ολλανδία | - | - | 1.6, 2.0* | ✓ |
| [42] | 2020 | Σύστημα φόρτισης | ✓ | ✓ | 1.6, 2.0* | ✓ |
| [43] | 2021 | Πρωτόκολλα μετωπιαίου και νωτιαίου άκρου οικοσυστήματος οχημάτων | - | ✓ | 1.6, 2.0* | ✓ |
| [44] | 2021 | Σταθμοί φόρτισης στο ηλεκτρικό πλέγμα | ✓ | - | 1.6 | - |
| [45] | 2021 | Αρχιτεκτονική σταθμού φόρτισης | ✓ | - | 1.5, 1.6 | - |
| ** | 2022 | OCPP συστήματα φόρτισης | ✓ | ✓ | 1.2 - 2.0* | ✓ |

[✓]: Σφαιρική ανάλυση [✓]: Μερική ανάλυση [-]: Δεν αναφέρονται
*OCPP έκδοση 2.0.1 (ή OCPP 2.0)
**Τρέχουσα μελέτη

των απειλών ασφάλειας και απορρήτου με τα περιουσιακά στοιχεία ενός συστήματος φόρτισης EV.

Οι Bernardini, Asghar και Crispo [39] διεξήγαγαν μια ενδελεχή έρευνα για τον εντοπισμό των ζητημάτων ασφάλειας και απορρήτου στις οχηματικές επικοινωνίες. Ταξινόμησαν την ανάλυσή τους σε τρεις κατηγορίες: την ενδο-οχηματική επικοινωνία, την επικοινωνία μεταξύ οχημάτων και πυλών (gateways) και την επικοινωνία μεταξύ οχημάτων. Αν και κατέγραψαν τα περισσότερα δρώντα στοιχεία τα οποία συμμετέχουν σε ένα σενάριο φόρτισης οχημάτων EV, η ανάλυσή τους περιλάμβανε μόνο τα ζητήματα ασφάλειας που σχετίζονται με τον τριτομερή διαχειριστή διανομής DSO, τους σταθμούς φόρτισης (Charging Station, CS) και τα οχήματα EV. Επιπλέον, δεν παρείχαν συσχετισμό μεταξύ των απειλών ασφάλειας και ιδιωτικότητας και των περιουσιακών στοιχείων συστήματος φόρτισης EV. Τα θέματα ασφάλειας του πρωτοκόλλου OCPP συζητούνται μόνο εν μέρει.

Τα ζητήματα ασφάλειας που σχετίζονται με την έκδοση OCPP 1.6 παρουσιάστηκαν από τους Alcaraz, Lopez και Wolthusen [40]. Αναλύθηκαν αρκετές ευπάθειες του πρωτοκόλλου που σχετίζονται με τη δυνατότητα ειδοποίησης εκκίνησης και τη χρήση του πρωτοκόλλου σε συνεργασία με το πρωτόκολλο TLS. Επιπλέον, η μελέτη αυτή προσπάθησε να προσδιορίσει τον αντίκτυπο των απειλών που παραθέτει σε διαφορετικά περιουσιακά στοιχεία και συστήματα επικοινωνίας. Οι προκλήσεις που παρουσιάστηκαν σχετίζονταν με την προηγούμενη της τρέχουσας έκδοση του πρωτοκόλλου, δηλαδή το OCPP 1.6, η οποία δεν διέθετε ορισμένα από τα χαρακτηριστικά ασφάλειας της σύγχρονης έκδοσης και η οποία μελετάται εδώ. Επιπλέον, η μελέτη εκείνη [40] επικεντρώθηκε στην επικοινωνία που βασίζεται στο OCPP μεταξύ των οχημάτων EV και των σταθμών φόρτισης CS, αφήνοντας κατά μέρος δρώντα στοιχεία όπως ο οδηγός του οχήματος EV, ο διαχειριστής διανομής DSO, ο ελεγκτής LC, ο πληρεξούσιος LP και οι αισθητήρες/ελεγκτές ενέργειας. Ωστόσο, παρουσιάστηκε μια συσχέτιση μεταξύ των απειλών ασφάλειας και των υπό μελέτη περιουσιακών στοιχείων και επισημάνθηκαν ανοιχτά ζητήματα ασφάλειας της τότε πρόσφατης έκδοσης του πρωτοκόλλου OCPP.

Σε ένα πρόσφατο άρθρο, οι Audel και Poll [41] παρείχαν μια επισκόπηση των κύριων ρόλων και πρωτοκόλλων για τη φόρτιση οχημάτων EV στην Ολλανδία. Υποστήριξαν ότι το πρωτόκολλο TLS δεν επαρκεί να καλύψει τις απαιτήσεις ασφάλειας και απορρήτου των συστημάτων φόρτισης EV. Πρότειναν ότι θα ήταν εφικτό να προστεθεί μια διαδικασία για την από άκρο σε άκρο (end-to-end) μακροπρόθεσμη αυθεντικότητα και εμπιστευτικότητα στα δεδομένα που ανταλλάσσονται μεταξύ διαφορετικών οντοτήτων εντός του συστήματος. Το άρθρο είναι πολύ ενδιαφέρον και έχει εντοπίσει ζητήματα ασφάλειας μελετώντας τις ολλανδικές υποδομές φόρτισης EV. Ωστόσο, δεν ελήφθησαν υπόψη οι ενεργειακοί αισθητήρες/ελεγκτές και τα σχετικά με αυτούς θέματα ασφάλειας. Επιπλέον, δεν παρασχέθηκε συσχέτιση μεταξύ των απειλών ασφάλειας και ιδιωτικότητας και των περιουσιακών στοιχείων και συζητήθηκαν μόνο εν μέρει τα ζητήματα ασφάλειας του πρωτοκόλλου OCPP. Το ανοιχτό ζήτημα που εντοπίστηκε είναι ο αδύναμος έλεγχος ταυτότητας για τον οδηγό του οχήματος EV.

Οι Antoun et al. [42] παρουσίασαν μια λεπτομερή αναφορά σχετικά με τα συστήματα φόρτισης οχημάτων EV και τα σχετικά θέματα ασφάλειας και απορρήτου. Παρουσίασαν με γραφικό τρόπο τις βασικές ευπάθειες που υπάρχουν τόσο σε οικιακές όσο και σε δημόσιες υποδομές φόρτισης και εντόπισαν ορισμένα κενά ασφάλειας που πρέπει να αντιμετωπιστούν στο άμεσο μέλλον. Ωστόσο, τα περιουσιακά στοιχεία που μελετήθηκαν σχετικά με τις απειλές ασφάλειας ήταν μόνο τα οχήματα EV, οι σταθμοί φόρτισης CS και το μέσο της επικοινωνίας, με αποτέλεσμα να προκύψει μια περιορισμένη λίστα συσχέτισης περιουσιακών στοιχείων και απειλών. Παρόμοιοι περιορισμοί επηρέασαν την καταγραφή των αντίμετρων, καθώς συμπεριέλαβαν μόνο λύσεις που προστατεύουν την επικοινωνία μεταξύ:

*(α)* του σταθμού φόρτισης CS και του συστήματος διαχείρισης Charging Station Management System (CSMS), και

*(β)* μεταξύ του σταθμού φόρτισης CS και του οχήματος EV.

Συζητήθηκαν ανοιχτά θέματα ασφάλειας του πρωτοκόλλου, όπως η περιορισμένη χρήση κρυπτογραφίας, η έλλειψη επιβεβλημένων ελέγχων αυθεντικότητας και η ασφάλεια των υποδομών του δικτύου ηλεκτρικής ενέργειας.

Οι Metere et al. [43] εξέτασαν ζητήματα ασφάλειας και απορρήτου που σχετίζονται με το οικοσύστημα φόρτισης οχημάτων EV, εστιάζοντας στην έξυπνη φόρτιση και τις εφαρμογές V2G. Αρχικά παρουσιάστηκαν αρκετές συστάσεις και οδηγίες για την ασφάλεια της υποδομής φόρτισης EV, και ακολούθησε λεπτομερής ανάλυση των ζητημάτων ασφάλειας και απορρήτου που αντιμετωπίζει ένα τόσο περίπλοκο σύστημα. Υποστηρίχθηκε ότι η τεχνολογία ασφάλειας υπάρχει ήδη, ωστόσο πρέπει να προσαρμοστεί ώστε να ληφθούν υπόψη οι ιδιαίτερες προκλήσεις της υποδομής φόρτισης EV. Σύμφωνα με τη μελέτη [43], πρέπει να επιτευχθεί ισορροπία μεταξύ της ποιότητας και της ασφάλειας της υπηρεσίας. Ζητήματα που σχετίζονται με το πρωτόκολλο OCPP παρουσιάστηκαν μόνο εν συντομία. Επιπλέον, ορισμένα περιουσιακά στοιχεία και τα ζητήματα ασφάλειάς τους, όπως ο οδηγός EV, δεν μελετήθηκαν ενώ τα τα ζητήματα ασφάλειας των σταθμών φόρτισης CS και η συσχέτιση μεταξύ απειλών και περιουσιακών στοιχείων μελετήθηκαν εν μέρει. Η εργασία ανέλυσε σε βάθος την εφαρμογή μιας υποδομής δημόσιων κλειδιών PKI για ηλεκτρικά οχήματα ως αντίμετρο για τα ζητήματα ασφάλειας του οικοσυστήματος EV. Οι Metere et al. [43] αναφέρθηκαν στην ανάγκη

για την ύπαρξη και αποκλειστική χρήση PKI για τη φόρτιση οχημάτων EV, ως ανοιχτό μελλοντικό ζήτημα.

Οι Pourmirza και Walker [44] εξέτασαν τις ευπάθειες και τα ζητήματα κυβερνοασφάλειας των σταθμών φόρτισης CS που λειτουργούσαν στην επικράτεια του Ηνωμένου Βασιλείου. Ανέδειξαν τις επιθέσεις παραπληροφόρησης κατά των CS που ενδέχεται να εκθέσουν τα διαπιστευτήρια και τα δεδομένα του οδηγού EV. Πέρα από τους σταθμούς φόρτισης CS, εξετάστηκαν τα θέματα ασφάλειας άλλων τριών περιουσιακών στοιχείων, δηλαδή του οχήματος EV, του οδηγού EV και του συστήματος διαχείρισης CSMS. Τα ζητήματα ασφάλειας και απορρήτου, καθώς και τα αντίμετρα μελετήθηκαν για τους σταθμούς φόρτισης CS που υποστηρίζονται από την έκδοση OCPP 1.6. Δεν παρασχέθηκε συσχέτιση απειλών και περιουσιακών στοιχείων ή συζήτηση για ανοιχτά θέματα ασφάλειας.

Στην τελευταία μελέτη που σχετίζεται με το πρωτόκολλο OCPP, οι Raboaca et al. [45] επικεντρώθηκαν στον σχεδιασμό της εφαρμογής για ένα σύστημα φόρτισης οχημάτων EV που υποστηρίζεται από την έκδοση OCPP 1.6. Έκαναν επισκόπηση των σχετικών τοπολογιών και αρχιτεκτονικών και ανέλυσαν τα λειτουργικά χαρακτηριστικά του OCPP για να αναπτύξουν μια εφαρμογή κράτησης σταθμού φόρτισης CS για τους οδηγούς EV. Αν και εξέτασαν τα ζητήματα ασφάλειας στα βασικά δρώντα στοιχεία, οι επιθέσεις ασφάλειας δεν συσχετίστηκαν με τα στοιχεία που επηρεάζονται περισσότερο. Υποστήριξαν ότι η καλύτερη πρακτική για τη βελτίωση της ασφάλειας του πρωτοκόλλου OCPP είναι η ενσωμάτωση τεχνικών Blockchain και Τεχνητής Νοημοσύνης (Artificial Intelligence, AI). Για το μέλλον, τα ανοιχτά θέματα που συζητήθηκαν αφορούσαν στη σταθερότητα της προσδοκούμενης απόδοσης των σταθμών φόρτισης CS και όχι στον τομέα της ασφάλειας.

## 2.3 Προτάσεις μοντελοποίησης και αξιολόγησης ασφάλειας IoT υπηρεσίας

Έχουν καταβληθεί σημαντικές προσπάθειες για την ανάπτυξη ευφυών και βιώσιμων συστημάτων μεταφορών και καινοτόμες εφαρμογές έχουν προταθεί στους τομείς της διαχείρισης στόλου, του σχεδιασμού δρομολογίων και της έξυπνης κατανομής πόρων. Οι Aazam και Fernando [22] και οι Tilocca et al. [23] μελετούν παράγοντες, όπως οι περιβαλλοντικές, οι κυκλοφοριακές και οι καιρικές συνθήκες και την αξιοποίησή τους για να βελτιωθεί η ποιότητα στις υπηρεσίες οδικής συγκοινωνίας, ενώ οι Remy et al. [46] προτείνουν την αρχιτεκτονική και τις λειτουργίες λήψης αποφάσεων σε ένα σύστημα κράτησης οχημάτων και προγραμματισμού δρομολογίων, το οποίο βασίζεται στη χαρτογράφηση του δρόμου και στην καταγραφή και τον συνυπολογισμό των καιρικών συνθηκών.

Τα ζητήματα ασφάλειας των επικοινωνιών στο οικοσύστημα των μεταφορών είναι επίσης ζωτικής σημασίας. Οι Stellios et al. [47] μελετούν επιθέσεις βασιζόμενες σε συσκευές με IoT χαρακτηριστικά, μέσω της αξιολόγησης των μονοπατιών επίθεσης και καταλήγουν στο συμπέρασμα ότι η επιτυχία μιας τέτοιας επίθεσης σχετίζεται με:

*(α)* τη φυσική εγγύτητα της συσκευής με IoT χαρακτηριστικά στον στόχο,

*(β)* την πληρέστερη εκμετάλλευση των διεπαφών επικοινωνίας (φυσικών ή δικτυακών), και

*(γ)* τη μέγιστη δυνατή επέκταση της λειτουργικότητας που παρέχεται από τη συσκευή με IoT χαρακτηριστικά.

Η μοντελοποίηση μιας υπηρεσίας που βασίζεται στο IoT χρησιμοποιώντας ειδικές, για τον τομέα, γλώσσες και σημασιολογία μοντελοποίησης δεν μπορεί να απαντήσει επαρκώς στην πρόκληση της απεικόνισης της συμπεριφοράς κατανεμημένων και ετερογενών διασυνδεδεμένων κόμβων. Για τους λόγους αυτούς, οι Mavropoulos et al. [48] παρουσιάζουν ένα εργαλείο με το όνομα Apparatus για τη μοντελοποίηση και την ανάλυση ασφάλειας [49] μιας υπηρεσίας που βασίζεται στο IoT. Το πλαίσιο δημιουργίας κώδικα "Thing" Modeling Language (ThingML) [50] και η ομώνυμη υποστηριζόμενη γλώσσα μοντελοποίησης, παρέχουν τη σημασιολογία για τη μοντελοποίηση των στοιχείων λογισμικού και τη δημιουργία προγραμματιστικού κώδικα από το μοντέλο. Το μοντέλο αναπαράστασης ιεραρχικής επίθεσης Hierarchical Attack Representation Model (HARM) [51] χρησιμοποιείται για τη μοντελοποίηση ενός δικτύου που βασίζεται στο IoT. Η αξιολόγηση με το HARM βασίζεται στις μετρικές ασφάλειας για τις αντίστοιχες ευπάθειες, όπως αυτές παρέχονται από τη National Vulnerability Database (NVD) [52]. Αυτή η αξιολόγηση διεξάγεται σε διαφορετικά χρονικά στιγμιότυπα και, ως εκ τούτου, λαμβάνει υπόψη την κινητικότητα των κόμβων. Στην εργασία [53], οι μετρικές ασφάλειας ταξινομούνται σε δύο κατηγορίες, τις ξενιστοπαγείς (host-based) και τις δικτυοπαγείς (network-based). Η πρώτη κατηγορία μελετάται με βάση την πιθανότητα επιτυχίας της επίθεσης, ενώ η δεύτερη με βάση την εγγύτητα του εισβολέα σε ένα ή περισσότερα στοιχεία της στοχοποιημένης υπηρεσίας.

Η ανάλυση της ασφάλειας υπηρεσιών που βασίζονται στο IoT χρησιμοποιώντας μια προσέγγιση μοντελοποίησης Petri net (PN) προτείνεται στη μελέτη [54]. Οι Yamaguchi και Tanaka [55] μοντελοποιούν χρησιμοποιώντας PN μια πολύ γνωστή επίθεση με κακόβουλο λογισμικό και αξιολογούν μια μέθοδο μετριασμού της. Επιπλέον, στη βιβλιογραφία χρησιμοποιούνται τα μοντέλα PN για τη σχεδίαση υιοθέτησης μηχανισμών και ενορχήστρωσης υπηρεσιών που βασίζονται στο IoT [56]. Η ανάπτυξη μιας υπηρεσίας που βασίζεται στο IoT δεν μπορεί να αγνοήσει ζητήματα, όπως οι αλλαγές στις οντότητες ή στο περιβάλλον της υπηρεσίας και, ως εκ τούτου, δεν μπορεί να βασιστεί πλήρως σε στατικά μοντέλα. Οι Fortino et al. [57] δηλώνουν ότι οι αναπαραστάσεις λειτουργιών του IoT με μετα-μοντέλα δύναται να επιτρέψουν την επαλήθευση και την προσομοίωση σε διάφορα πεδία, όπως στην ασφάλεια.

# Κεφάλαιο 3

# Ευφυής υπηρεσία μεταφορών

## 3.1 Δομικά στοιχεία και κύκλος λειτουργίας

Σε αυτό το κεφάλαιο παρουσιάζεται η πρωτότυπη υπηρεσία ενός ευφυούς συστήματος μεταφορών (Intelligent Transport System, ITS) που βασίζεται στο IoT, με την ονομασία Intelligent Bus on Campus (iBuC). Πρόκειται για μια υπηρεσία που βασίζεται σε ένα καινοτόμο σύστημα ταχείας προσωπικής μεταγωγής PRT [32], δηλαδή ενός συστήματος μεταφοράς που μπορεί να χρησιμοποιηθεί σε ένα τοπικό οδικό δίκτυο, όπως μια πανεπιστημιούπολη. Η iBuC παρέχει μεταφορά εντός του οδικού δικτύου της πανεπιστημιούπολης από κτίριο σε κτίριο και εξυπηρέτηση πρόσβασης των μελών της κοινότητας και των επισκεπτών στους κόμβους/στάσεις των MMM, που βρίσκονται στην περίμετρο της πανεπιστημιούπολης.

Η iBuC έχει τα ακόλουθα δομικά στοιχεία:

*(α)* τα οχήματα της υπηρεσίας είναι ηλεκτρικά (για τον μετριασμό των εκπομπών διοξειδίου του άνθρακα [18]) με χωρητικότητα τεσσάρων επιβατών,

*(β)* ο στόλος της υπηρεσίας αποτελείται από τέσσερα οχήματα,

*(γ)* τα οχήματα φέρουν ομάδα αισθητήρων για τον έλεγχο της κίνησής τους (δηλαδή GPS, αισθητήρες μέτρησης απόστασης υπερήχων, κάμερες, σύστημα ελέγχου),

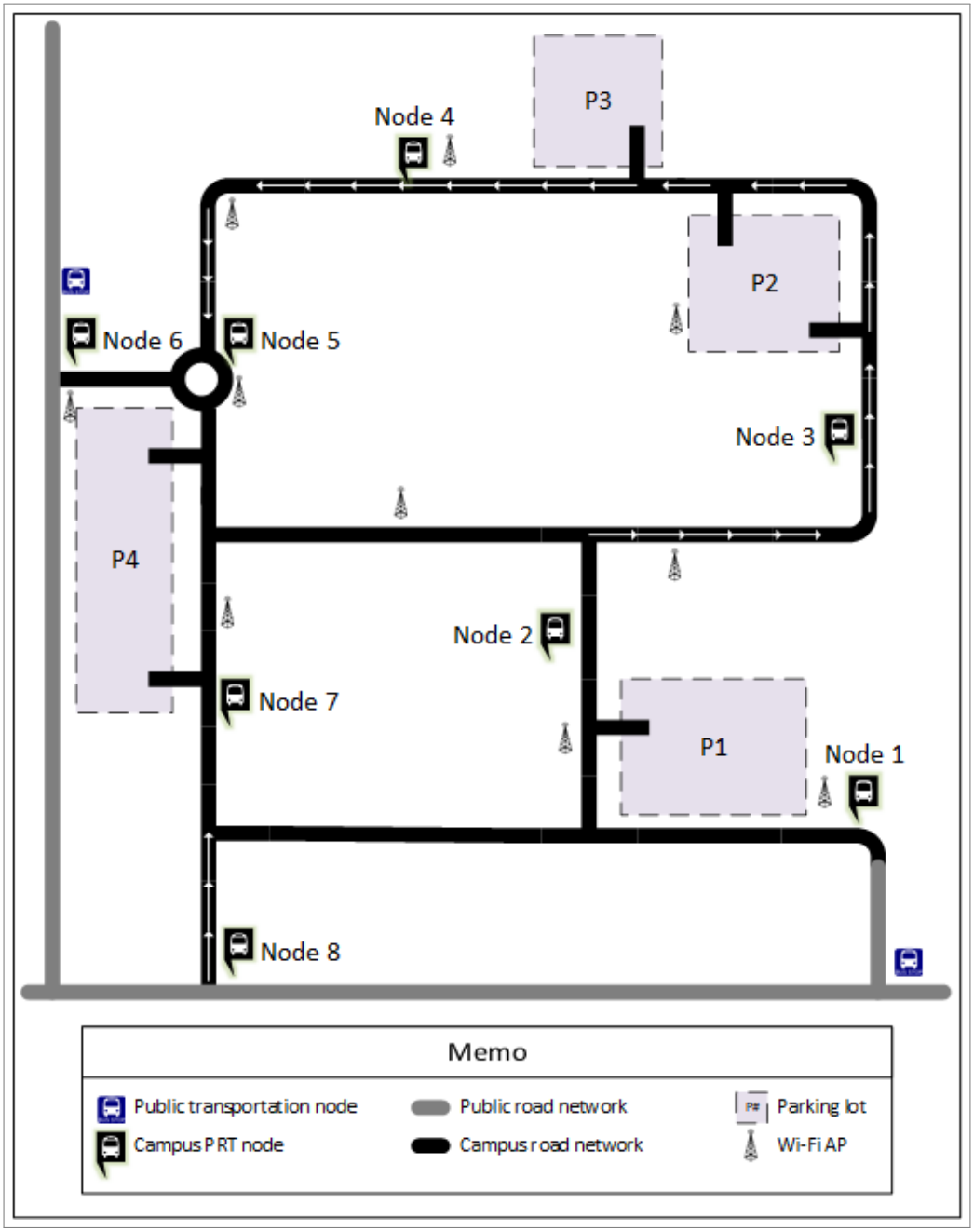
*(δ)* μια κεντρική μονάδα ελέγχου (Control Unit, CU) συλλέγει και αναλύει τα δεδομένα του στόλου (δηλαδή θέση, κατεύθυνση και ταχύτητα του οχήματος, αριθμός επιβατών στο όχημα, εκκρεμή αιτήματα επιβατών),

*(ε)* το δίκτυο Wi-Fi της πανεπιστημιούπολης χρησιμοποιείται για την επικοινωνία των οχημάτων και του κεντρικού συστήματος ελέγχου,

*(στ)* μια εφαρμογή έξυπνων συσκευών και μια εφαρμογή ιστού προσφέρουν στους χρήστες της υπηρεσίας μια διεπαφή για την υποβολή αιτημάτων και για την παρακολούθηση της κατάστασης του στόλου, και

*(ζ)* μια τριτομερής διεπαφή (Application Programming Interface, API) υποστηρίζει την ανταλλαγή δεδομένων μεταξύ της υπηρεσίας iBuC και του συστήματος υποστήριξης λειτουργιών (University Business Support System, uBSS) του πανεπιστημίου.

Η υπηρεσία iBuC σχεδιάστηκε προσαρμοσμένη στις ανάγκες του πρώτου/τελευταίου μιλίου της κοινότητας μιας πανεπιστημιούπολης (Εικόνα 1). Η πανεπιστημιούπολη έχει συνολικά οκτώ κόμβους, στους οποίους οι επιβάτες μπορούν να επιβιβαστούν ή να αποβιβαστούν.




Εικόνα 1. Χάρτης της πανεπιστημιούπολης που υποστηρίζεται από την iBuC

Όταν ο στόλος της iBuC είναι σε αδράνεια, κάθε ένα από τα οχήματά του είναι σταθμευμένο στους χώρους στάθμευσης (P1-P4), που βρίσκονται στην περιοχή της πανεπιστημιούπολης. Κατά προτίμηση, η κεντρική μονάδα ελέγχου CU, η οποία συγκεντρώνει τα δεδομένα της υπηρεσίας και εκτελεί αλγόριθμους για τη λήψη αποφάσεων της υπηρεσίας, επιλέγει τη διασπορά των τεσσάρων οχημάτων του στόλου στους τέσσερεις χώρους στάθμευσης, όταν αυτό είναι εφικτό. Με τον τρόπο αυτό, η

κάλυψη/απάντηση νέων αιτημάτων της υπηρεσίας θα προκύψει χωρίς περιττές διαδρομές των οχημάτων.

Ένα αίτημα τίθεται από κάποιο μέλος της κοινότητας, μέσω της εφαρμογής της υπηρεσίας iBuC και με χρήση συσκευής με δυνατότητα GPS. Ο αιτών (επιβάτης E) πρέπει ταυτόχρονα να δηλώσει τον επιθυμητό κόμβο προορισμού (Node 6). Η υπηρεσία προτείνει στον επιβάτη E τον κόμβο επιβίβασης (Node 3), ανάλογα με την τρέχουσα θέση του και την τρέχουσα διαθεσιμότητα του στόλου της υπηρεσίας. Ο επιβάτης E ενημερώνεται μέσω της εφαρμογής για την εκτιμώμενη ώρα άφιξης (Estimated Time of Arrival, ETA) του οχήματος (όχημα V1 από τον χώρο στάθμευσης P2) στον κόμβο επιβίβασης Node 3.

Ταυτόχρονα, το σύστημα ελέγχου επιλέγει το πλησιέστερο διαθέσιμο όχημα V1 προς εξυπηρέτηση του αιτήματος του επιβάτη E και αποστέλλει σε αυτό δεδομένα (διαδρομή, ETA, σταθμός επιβίβασης) ώστε το όχημα V1 να μεταβεί στον κόμβο Node 3. Τα δεδομένα που λαμβάνει το όχημα V1 αφορούν:

*(α)* στον κόμβο επιβίβασης,

*(β)* στον χρόνο ETA στον οποίο θα πρέπει να βρίσκεται στον κόμβο επιβίβασης,

*(γ)* στον χρόνο κατά τον οποίο το όχημα V1 θα πρέπει να παραμείνει στον κόμβο επιβίβασης για την άφιξη και επιβίβαση του επιβάτη E,

*(δ)* στον κόμβο προορισμού του επιβάτη E,

*(ε)* στον χρόνο ETA στον οποίο θα πρέπει να βρίσκεται στον κόμβο προορισμού, και

*(στ)* στα δεδομένα για τις διαδρομές (χώρος στάθμευσης P2 προς κόμβο επιβίβασης Node 3, κόμβος επιβίβασης Node 3 προς κόμβο προορισμού Node 6) που θα ακολουθήσει το όχημα V1, έως ότου ο επιβάτης E αφιχθεί στον κόμβο προορισμού.

Να σημειωθεί ότι το οδικό δίκτυο της Πανεπιστημιούπολης είναι σηματοδοτημένο και κάποια τμήματα του δρόμου είναι μονής κατεύθυνσης. Αυτό περιορίζει τις πιθανές διαδρομές του οχήματος από το ένα σημείο στο άλλο. Στο χρονικό αυτό σημείο του κύκλου ζωής της υπηρεσίας, ο επιβάτης E και το όχημα V1 συναντώνται στον κόμβο Node 3, στον υπολογισμένο χρόνο που προκύπτει από τον συνυπολογισμό της χρονικής στιγμής ($t_0$) τοποθέτησης του αιτήματος από τον επιβάτη E και την εκτίμηση ETA της κεντρικής μονάδας ελέγχου CU. Κατόπιν, εκτελείται η διαδρομή από τον κόμβο Node 3 στον κόμβο Node 6.

Από τη χρονική στιγμή υποβολής του αιτήματος του επιβάτη E, οποιοσδήποτε άλλος χρήστης έχει πρόσβαση στην εφαρμογή της iBuC, θα ενημερώνεται για την υπό εκτέλεση διαδρομή του οχήματος V1, για τον αριθμό των κενών θέσεων στο όχημα, για την ώρα αναχώρησης ($t_{BN}$) από τον κόμβο Node 3 και την εκτιμώμενη ώρα άφιξης ($t_{DN}$) στον κόμβο Node 6. Ο χρόνος αναχώρησης $t_{BN}$ υπολογίζεται από την κεντρική μονάδα ελέγχου CU και επιβεβαιώνεται ή αλλάζει από τα δεδομένα του οχήματος V1, όταν αυτό αφιχθεί στον κόμβο επιβίβασης. Αντίστοιχα, ο χρόνος άφιξης $t_{DN}$ υπολογίζεται από την κεντρική μονάδα ελέγχου CU και επιβεβαιώνεται ή αλλάζει από τα δεδομένα του οχήματος V1, όταν αυτό αφιχθεί στον κόμβο προορισμού. Σε περίπτωση που υποβληθεί νέο αίτημα (επιβάτης F) εντός του κύκλου της υπηρεσίας για την εξυπηρέτηση του επιβάτη E, η θέση

και η κατεύθυνση του οχήματος V1 σε πραγματικό χρόνο λαμβάνεται υπόψη από την κεντρική μονάδα ελέγχου CU, για την περίπτωση το νέο αίτημα να ικανοποιηθεί εντός του τρέχοντος κύκλου της υπηρεσίας από το όχημα V1.

Στο τέλος του κύκλου της υπηρεσίας, το όχημα V1 στέλνει ενημέρωση στην κεντρική μονάδα ελέγχου CU σχετικά με την αποβίβαση του επιβάτη E στον κόμβο προορισμού Node 6 και σηματοδοτείται η ολοκλήρωση του κύκλου της υπηρεσίας. Κατόπιν, η κεντρική μονάδα ελέγχου CU λαμβάνει απόφαση για τη βέλτιστη επιλογή θέσης στάθμευσης του οχήματος V1, σύμφωνα με τις τρέχουσες συνθήκες της υπηρεσίας και του χώρου της πανεπιστημιούπολης. Το όχημα V1 λαμβάνει δεδομένα σχετικά με:

*(α)* την επιλεγμένη θέση στάθμευσης,

*(β)* τον χρόνο ETA στον οποίο θα πρέπει να βρίσκεται στη θέση στάθμευσης, και

*(γ)* δεδομένα για τη διαδρομή από την τρέχουσα θέση του οχήματος προς τον επιλεγμένο χώρο στάθμευσης.

### 3.1.1 Υπολογισμός θέσης οχημάτων και επιβατών

Όπως αναφέρθηκε, μια συσκευή με δυνατότητα GPS επιτρέπει στον χρήστη της υπηρεσίας iBuC να θέσει το αίτημά του. Ωστόσο, στην περίπτωση που η συσκευή του χρήστη δεν έχει δυνατότητα GPS, τότε θα πρέπει ο χρήστης να δηλώσει τον επιθυμητό κόμβο προορισμού του, καθώς και τον επιθυμητό κατ' αυτόν κόμβο επιβίβασης.

Στην περίπτωση που ο χρήστης διαθέτει συσκευή με δυνατότητα GPS, ωστόσο βρίσκεται σε εσωτερικό χώρο όταν υποβάλλει το αίτημά του, το σήμα GPS κάλυψης της θέσης του θα είναι χαμηλό ή ανεπαρκές. Στην περίπτωση αυτή η θέση του θα πρέπει να υπολογιστεί με βάση τα χαρακτηριστικά της σύνδεσης Wi-Fi της συσκευής, ώστε να μπορεί να προταθεί από την κεντρική μονάδα ελέγχου CU ο κόμβος επιβίβασης.

Ο αλγόριθμος προσδιορισμού Sample Size Determination Algorithm (SSDA) [58] μπορεί να υπολογίσει τη θέση ενός δέκτη Wi-Fi με απόκλιση λάθους 0.25 m και ο αλγόριθμος MUltiple SIgnal Classification (MUSIC) [59] με απόκλιση λάθους 0.40 m. Οι αποκλίσεις αυτές είναι κατά πολύ μικρότερες από την εκτιμώμενη απόκλιση του 1.00 m περίπου [60], του υπολογισμού θέσης με τη χρήση δεδομένων GPS. Συμπερασματικά, ο υπολογισμός θέσης επιβατών και οχημάτων μπορεί να γίνει μέσω ενός συνδυασμού των δεδομένων GPS και της εκτίμησης θέσης του δέκτη Wi-Fi, για μεγαλύτερη ακρίβεια του υπολογισμού σε εξωτερικούς χώρους και ως εναλλακτική λύση στη χαμηλή σηματοδότηση GPS σε εσωτερικούς χώρους. Κάτι τέτοιο είναι εφικτό καθώς η περιοχή της πανεπιστημιούπολης έχει κάλυψη Wi-Fi στο μεγαλύτερο μέρος της έκτασής της.

### 3.1.2 Διαλειτουργικότητα με τριτομερή υπηρεσία

Η συνεργασία μεταξύ της κεντρικής μονάδας ελέγχου CU της υπηρεσίας iBuC (δηλαδή του συστήματος λήψης αποφάσεων) και του συστήματος υποστήριξης λειτουργιών uBSS του πανεπιστημίου θα μπορούσε να παρέχει πρόσθετες πληροφορίες για την καλύτερη λειτουργία της iBuC. Το uBSS περιέχει και συλλέγει πληροφορίες σχετικά με την πρόσβαση των κτιρίων, το πρόγραμμα των διαλέξεων και την παρουσία προσωπικού, μεταξύ άλλων. Αυτές οι πληροφορίες μπορούν να βοηθήσουν στη διαδικασία λήψης

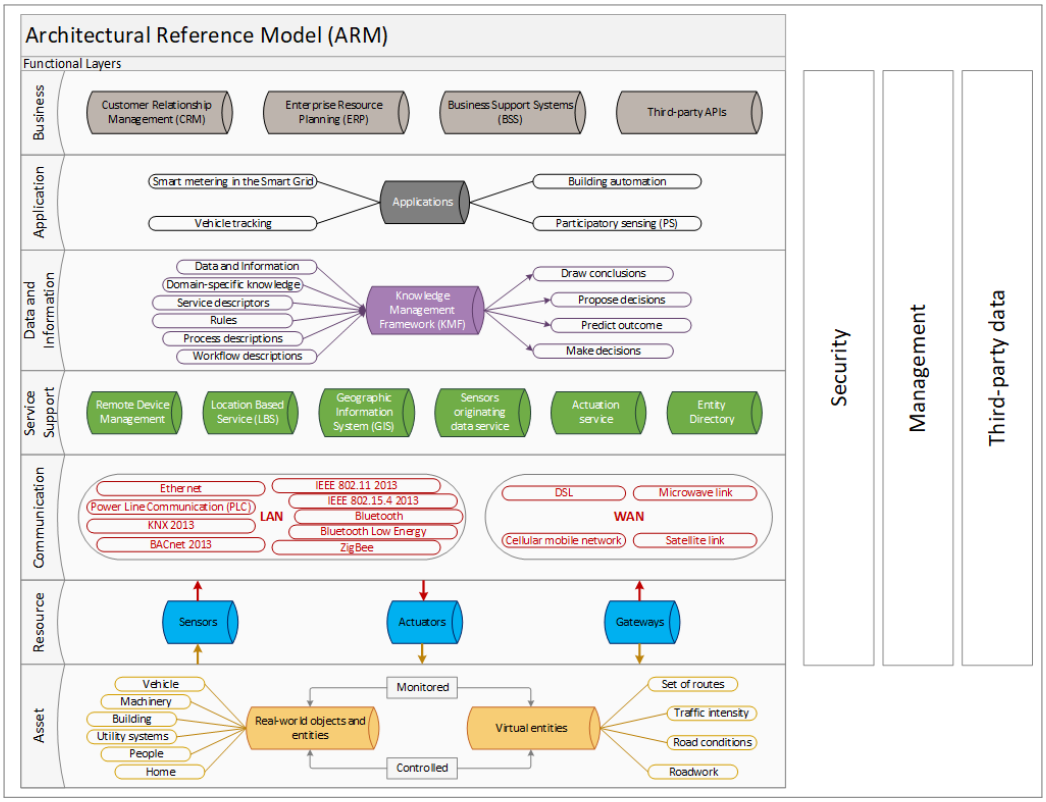
αποφάσεων της κεντρικής μονάδας ελέγχου CU. Για παράδειγμα, ένα μήνυμα όπως *η διάλεξη Χ στο Κτίριο Α πρόκειται να τελειώσει σε 1 ώρα* από το uBSS στην iBuC, σημαίνει ότι θα πρέπει να αναμένεται αυξημένη ζήτηση οχημάτων από τους κόμβους κοντά σε αυτό το κτίριο. Σε αυτήν την περίπτωση, η υπηρεσία μπορεί να κινητοποιήσει περισσότερα οχήματα να βρίσκονται σε αυτούς τους κόμβους ή σε κοντινή απόσταση, κατά την προμηνυόμενη ώρα λήξης, ώστε να ελαχιστοποιηθεί ο χρόνος που απαιτείται για τα οχήματα για να αφιχθούν στον κόμβο επιβίβασης κάποιου αιτήματος. Επίσης, με τον τρόπο αυτό θα εξυπηρετηθούν περισσότεροι χρήστες με λιγότερες διαδρομές των οχημάτων.

Αυτή η ανταλλαγή δεδομένων μεταξύ της κεντρικής μονάδας ελέγχου CU της υπηρεσίας iBuC και του συστήματος uBSS θα είναι επωφελής και για τα δύο μέρη. Το σύστημα uBSS, θα εντάσσει στα δεδομένα που συγκεντρώνει και τα δεδομένα που θα δέχεται από την κεντρική μονάδα ελέγχου CU, βελτιώνοντας με αυτό τον τρόπο την ποιότητα των πληροφοριών που διαθέτει. Για παράδειγμα, δεδομένα σχετικά με τις μετακινήσεις των μελών της κοινότητας θα επικαιροποιούσαν τις πληροφορίες του uBSS σχετικά με την πρόσβαση των κτιρίων. Αξίζει να σημειωθεί πως, μεταξύ άλλων, το uBSS είναι η πηγή πληροφόρησης της κοινότητας σχετικά με την τρέχουσα κατάσταση της πανεπιστημιούπολης. Συνεπώς, η διαλειτουργικότητα της υπηρεσίας iBuC με το σύστημα uBSS είναι μια λύση που εξυπηρετεί τις λειτουργίες του ίδιου του παρόχου/δημιουργού (διεπιχειρησιακή λύση B2B), που σε αυτή την περίπτωση είναι ο οργανισμός του πανεπιστημίου, εξυπηρετώντας παράλληλα και τα μέλη της κοινότητας (επιχειρησιοκαταναλωτική λύση B2C), ως καταναλωτές της υπηρεσίας μεταφορών iBuC και ως δέκτες πληροφοριών που παρέχονται από την υπηρεσία.

## 3.2 Αρχιτεκτονική εφαρμογής

Το Διαδίκτυο των Αντικειμένων, η Νεφοϋπολογιστική και τα Κυβερνο-συστήματα είναι οι τρεις κύριοι πυλώνες της 4ης Βιομηχανικής Επανάστασης (Industrie 4.0) [61]. Πολλοί οργανισμοί όπως το κονσόρτιο World Wide Web Consortium (W3C) [62], το ινστιτούτο European Telecommunications Standards Institute (ETSI) [63], το ινστιτούτο National Institute of Standards and Technology (NIST) [64], ο οργανισμός προτυποποίησης Internet Engineering Task Force (IETF) [65] και η επαγγελματική ένωση μηχανικών IEEE [66] προσπάθησαν να περιχαράξουν τον όρο IoT και να σχεδιάσουν ένα αρχιτεκτονικό μοντέλο αναφοράς για οποιαδήποτε υλοποίηση εντός αυτής της περιοχής. Παράλληλα, το ευρωπαϊκά χρηματοδοτούμενο πρόγραμμα EU FP7 με τίτλο *IoT-A* [67] επικεντρώνεται στο αρχιτεκτονικό μοντέλο αναφοράς του IoT.

Οποιαδήποτε αρχιτεκτονική λύση στο IoT μπορεί να περιγραφεί με βάση το IoT-A και την προσέγγιση των Holler et al. [68]. Σύμφωνα με την προσέγγιση αυτή, το προσχέδιο οποιασδήποτε IoT λύσης ή αλλιώς η εφαρμοσμένη αρχιτεκτονική της λύσης είναι μέρος ενός ευρύτερου μοντέλου, του Αρχιτεκτονικού Μοντέλου Αναφοράς (Architectural Reference Model, ARM), αναφερόμενη και ως Αρχιτεκτονική Αναφοράς (Εικόνα 2).




Εικόνα 2. Η αρχιτεκτονική αναφοράς για λύσεις που βασίζονται στο IoT

Η ARM εισάγει μια άτυπη διαίρεση επιπέδων για όλα τα στοιχεία μιας λύσης που βασίζεται στο IoT ή στη M2M επικοινωνία. Αυτά τα επίπεδα δεν είναι αυστηρά και για τη σχεδίαση μιας λύσης δεν είναι απαραίτητο να συμπεριληφθούν όλα τα επίπεδα ARM. Τα βασικά επίπεδα μιας λύσης που βασίζεται στο IoT είναι τα ακόλουθα:

*(α)* το επίπεδο περιουσιακών στοιχείων,

*(β)* το επίπεδο πόρων,

*(γ)* το επίπεδο επικοινωνίας,

*(δ)* το επίπεδο υποστήριξης υπηρεσιών,

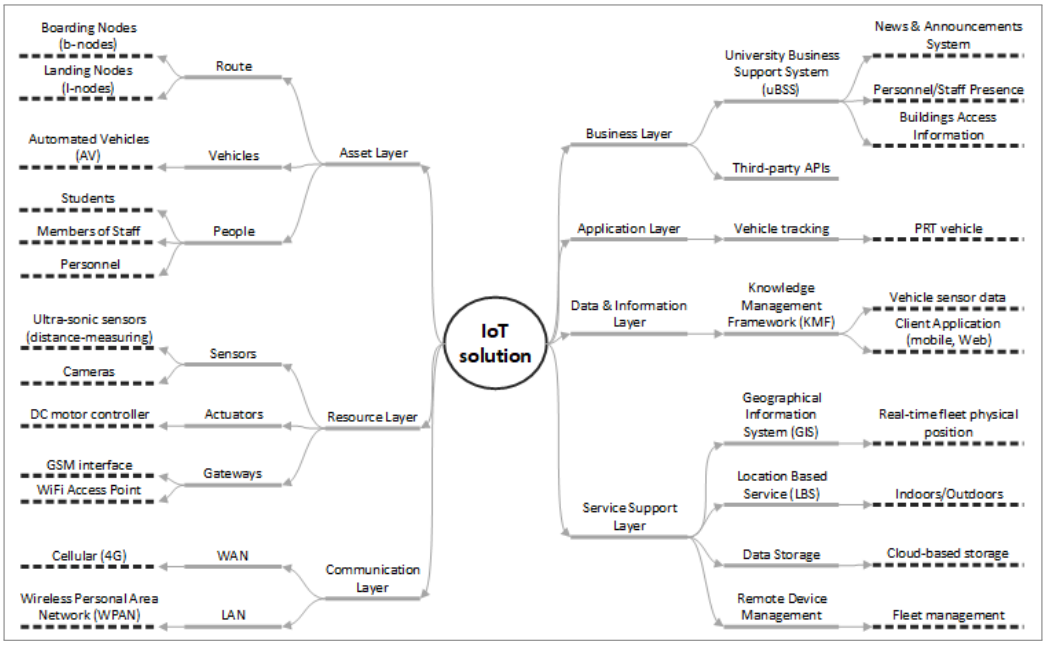
*(ε)* το επίπεδο δεδομένων και πληροφοριών,

*(στ)* το επίπεδο εφαρμογής, και

*(ζ)* το επιχειρησιακό επίπεδο.

Αξίζει να αναφερθεί πως τα επίπεδα ασφάλειας, διαχείρισης και τριτομερών δεδομένων, θεωρούνται κάθετα στην ARM, δηλαδή υπάρχουν στοιχεία που σχετίζονται με τα επίπεδα αυτά σε κάθε επίπεδο της αρχιτεκτονικής, από το επίπεδο πόρων έως το επιχειρησιακό.

Το εφαρμοσμένο αρχιτεκτονικό μοντέλο της υπηρεσίας iBuC που ακολουθεί την αρχιτεκτονική αναφοράς ARM φαίνεται στην Εικόνα 3. Οι διακεκομμένες γραμμές στην Εικόνα 3 υποδηλώνουν τα προτεινόμενα στοιχεία του μοντέλου αρχιτεκτονικής της iBuC.




Εικόνα 3. Η εφαρμοσμένη αρχιτεκτονική της προτεινόμενης υπηρεσίας iBuC

- **Επίπεδο περιουσιακών στοιχείων (Asset Layer)**

  Το επίπεδο περιουσιακών στοιχείων περιλαμβάνει τα αντικείμενα των οποίων η συμπεριφορά παρακολουθείται. Τα περιουσιακά στοιχεία της iBuC είναι:

  *(α)* ο στόλος των οχημάτων,

  *(β)* η διαδρομή των εν κινήσει οχημάτων, και

  *(γ)* οι επιβάτες.

  Ο στόλος περιλαμβάνει τέσσερα ηλεκτρικά αυτόνομα οχήματα AV τα οποία φέρουν αισθητήρες και ενεργοποιητές, τα δεδομένα των οποίων είναι επίσης περιουσιακό στοιχείο της υπηρεσίας iBuC. Η διαδρομή του οχήματος εξαρτάται από:

  *(α)* τον κόμβο επιβίβασης,

  *(β)* τον κόμβο προορισμού,

  *(γ)* την οδική σήμανση του οδικού δικτύου της πανεπιστημιούπολης, και

  *(δ)* τις τρέχουσες συνθήκες (όπως κυκλοφορίας και καιρού).

  Η διαδρομή είναι εν μέρει προκαθορισμένη από τη σχεσιακή θέση των δύο κόμβων και τα προαναφερόμενα κριτήρια επιλογής της διαδρομής. Η τρίτη περίπτωση περιουσιακού στοιχείου της iBuC είναι τα δεδομένα των επιβατών, που είναι πιο πιθανό να συμμετέχουν στην υπηρεσία μέσω μιας έξυπνης συσκευής.

- **Επίπεδο πόρων (Resource Layer)**

  Οι πόροι της υπηρεσίας είναι:

  *(α)* οι αισθητήρες,

  *(β)* οι ενεργοποιητές οχημάτων, και

  *(γ)* οι πύλες για την επικοινωνία δεδομένων μεταξύ των οχημάτων και της κεντρικής μονάδας ελέγχου CU.

  Οι αισθητήρες που απαιτούνται είναι οι αισθητήρες υπερήχων και οι οπτικές κάμερες, που δίνουν πληροφορίες για την απόσταση μεταξύ του κάθε οχήματος AV και οποιουδήποτε εμποδίου. Ένας εποχούμενος ενεργοποιητής ελέγχει τον κινητήρα του οχήματος, έτσι ώστε να ακολουθείται η προδιαγεγραμμένη διαδρομή. Μια διεπαφή ασύρματου δικτύου έχει τον ρόλο της πύλης επικοινωνίας μεταξύ των στοιχείων του επιπέδου πόρων και των στοιχείων του επιπέδου υποστήριξης υπηρεσιών.

- **Επίπεδο επικοινωνίας (Communication Layer)**

  Το επίπεδο επικοινωνίας περιλαμβάνει τα μέσα επικοινωνίας μεταξύ των στοιχείων του επιπέδου πόρων και του επιπέδου υποστήριξης υπηρεσίας. Εκτός από την ασύρματη επικοινωνία μεταξύ της κεντρικής μονάδας ελέγχου CU και των οχημάτων AV, το δίκτυο κινητής τηλεφωνίας (δηλαδή 3G, 4G, 5G και νεότερες δομές GSM) χρησιμοποιείται για την παροχή αδιάλειπτης επικοινωνίας, ακόμη και όταν το τοπικό δίκτυο Local Area Network (LAN) ή το δίκτυο Wi-Fi της πανεπιστημιούπολης δεν είναι ενεργό.

- **Επίπεδο υποστήριξης υπηρεσιών (Service Support Layer)**

  Στον πυρήνα του επιπέδου υποστήριξης υπηρεσιών βρίσκεται ένα υπολογιστικό/αποθηκευτικό σύστημα ή ένα σύμπλεγμα συστημάτων που αλληλεπιδρούν με τα στοιχεία του επιπέδου πόρων. Η βάση της προτεινόμενης υπηρεσίας iBuC είναι η απομακρυσμένη διαχείριση του στόλου με σύστημα ελέγχου Remote Device Management (RDM), όπου το σύστημα ελέγχου λειτουργεί για την αποθήκευση δεδομένων και τη λήψη αποφάσεων σχετικά με τον στόλο. Στην υλοποίηση της απομακρυσμένης διαχείρισης RDM, το σύστημα ελέγχου καθοδηγεί, κάθε φορά και για κάθε αίτημα υπηρεσίας που δέχεται, το πλησιέστερο διαθέσιμο όχημα στον κόμβο επιβίβασης για την παραλαβή επιβατών και επιλέγει τη βέλτιστη θέση στάθμευσης (δηλαδή την πλησιέστερη διαθέσιμη) μετά την ολοκλήρωση ενός κύκλου της υπηρεσίας. Ένα σύστημα γεωγραφικών πληροφοριών (Geographical Information System, GIS) και μια υπηρεσία υπολογισμού θέσης (Location Based Service, LBS) αξιοποιούνται τόσο για τον υπολογισμό θέσης του στόλου όσο και για τον εντοπισμό θέσης του επιβάτη και παρέχουν δεδομένα εισόδου για τη διαδικασία λήψης αποφάσεων.

  Η κεντρική μονάδα ελέγχου CU είναι προσχεδιασμένη να φιλοξενείται σε νεφοϋπολογιστική υποδομή, η οποία διευκολύνει τόσο τη συγκέντρωση όσο και τη διαχείριση των δεδομένων από την iBuC. Επίσης, η αξιοποίηση της νεφοϋπολογιστικής υποδομής διευκολύνει την εύκολη μετάβαση μιας υπηρεσίας παλαιού τύπου στην προτεινόμενη αρχιτεκτονική καθώς και την ομαλή ενσωμάτωση νέων στοιχείων λογισμικού για την επέκταση των δυνατοτήτων της iBuC.

- **Επίπεδο δεδομένων και πληροφοριών (Data and Information Layer)**
  Οι λειτουργίες της κεντρικής μονάδας ελέγχου CU αποτελούν τον πυρήνα του επιπέδου δεδομένων και πληροφοριών. Η κεντρική μονάδα ελέγχου CU, εκτός από τη συλλογή και αποθήκευση σε πραγματικό χρόνο των πληροφοριών που προέρχονται από τους αισθητήρες των οχημάτων και την εφαρμογή του τελικού χρήστη, διαθέτει και εκτελεί τους κατάλληλους αλγόριθμους για τη λήψη αποφάσεων της υπηρεσίας. Οι αποφάσεις αυτές μπορεί να σχετίζονται με την επιλογή του κόμβου επιβίβασης, τη βέλτιστη διαδρομή που πρέπει να ακολουθήσει ένα όχημα και τον πλησιέστερο χώρο στάθμευσης οχημάτων. Τα κριτήρια λήψης αποφάσεων είναι:

  *(α)* η ελαχιστοποίηση της ταυτόχρονης κίνησης δύο ή περισσοτέρων οχημάτων,

  *(β)* η ελαχιστοποίηση των επιβατών σε αναμονή εξυπηρέτησης αιτήματός τους,

  *(γ)* η μεγιστοποίηση του πλήθους των επιβατών ανά όχημα και διαδρομή, και

  *(δ)* η ελαχιστοποίηση των ενδιάμεσων στάσεων ανά διαδρομή.

- **Επίπεδο εφαρμογής (Application Layer)**
  Το επίπεδο εφαρμογής περιλαμβάνει μία ή περισσότερες διεπαφές για την αλληλεπίδραση μεταξύ της υπηρεσίας και του τελικού χρήστη. Οι διεπαφές αυτές επιτρέπουν στον τελικό χρήστη να υποβάλει αίτημα για την υπηρεσία, να έχει πρόσβαση σε πραγματικό χρόνο σε πληροφορίες σχετικά με την κατάσταση του στόλου οχημάτων (δηλαδή κίνηση/στάση), να μπορεί να ακυρώσει κάποιο αίτημα που έχει ήδη υποβάλει ή να καθορίσει παραμέτρους σχετικά με το αίτημά του, όπως τον κόμβο επιβίβασης, τον χρόνο άφιξής του στον κόμβο επιβίβασης και άλλες. Όλες οι πληροφορίες και τα δεδομένα των διεπαφών τελικού χρήστη υποστηρίζονται από την κεντρική μονάδα ελέγχου CU.

- **Επιχειρησιακό επίπεδο (Business Layer)**
  Στο επιχειρησιακό επίπεδο, περιγράφεται η ανταλλαγή δεδομένων μεταξύ της υπηρεσίας iBuC και τριτομερών υπηρεσιών ή συστημάτων. Ως τριτομερή, θεωρούνται άλλα πανεπιστημιακά πληροφοριακά συστήματα ή οποιαδήποτε άλλη πηγή πληροφοριών/δεδομένων. Η iBuC ανταλλάσσει δεδομένα με το σύστημα υποστήριξης λειτουργιών uBSS του πανεπιστημίου, το οποίο περιέχει πληροφορίες σχετικά με την πρόσβαση στα κτίρια της πανεπιστημιούπολης ή πληροφορίες σχετικά με την παρουσία προσωπικού εντός της πανεπιστημιούπολης στην iBuC. Αυτά τα πρόσθετα δεδομένα βοηθούν την κεντρική μονάδα ελέγχου CU στη διαδικασία λήψης αποφάσεων. Αντίστοιχα και το uBSS μπορεί να χρησιμοποιεί τα παρεχόμενα από την iBuC δεδομένα. Αυτή η διασύνδεση της iBuC με το τροτομερές σύστημα uBSS, γίνεται μέσω ενός API. Έτσι, η iBuC και το uBSS μοιράζονται δεδομένα και, ως εκ τούτου, και τα δύο συστήματα διαθέτουν πιο πλήρη σύνολα δεδομένων σχετικά με τη συγκέντρωση και την κίνηση του πληθυσμού της κοινότητας στην πανεπιστημιούπολη.

## 3.3 Χαρακτηριστικά της IoT συμπεριφοράς

Η υπηρεσία iBuC, όπως περιγράφηκε ήδη, εμπεριέχει στοιχεία από όλα τα επίπεδα της αρχιτεκτονικής αναφοράς ARM μιας λύσης που βασίζεται στο IoT. Ωστόσο, το αρχιτεκτονικό μοντέλο εφαρμογής μιας λύσης από μόνο του δεν αναδεικνύει το κατά πόσο η περιγραφόμενη λύση είναι μέρος του IoT οικοσυστήματος ή πρόκειται για μια λύση που βασίζεται στην M2M επικοινωνία. Για αυτόν τον διαχωρισμό αξιολογείται η υπηρεσία και βάσει άλλων κριτηρίων [37], όπως:

*(α)* η τεχνολογία στην οποία βασίζεται,

*(β)* τα χαρακτηριστικά εφαρμογής και υπηρεσιών που περιλαμβάνει, και

*(γ)* η επιχειρησιακή στόχευση της λύσης.

Μια αντιπαραβολή των λύσεων που βασίζονται στο IoT και των λύσεων που βασίζονται σε M2M βάσει των παραπάνω κριτηρίων, φαίνεται στον Πίνακα 2.

Πίνακας 2. Χαρακτηριστικά λύσεων/υλοποιήσεων IoT και M2M

| **Έποψη** | **Υλοποίηση M2M** | **Υλοποίηση IoT** |
|---|---|---|
| **Εφαρμογές και Υπηρεσίες** | Καθοδηγούμενη από το πρόβλημα | Καθοδηγούμενη από την καινοτομία |
| | Εξειδικευμένες εφαρμογές | Εφαρμογές γενικής χρήσης |
| | Επικεντρωμένη στην επικοινωνία/ συσκευή | Επικεντρωμένη στην πληροφορία/ υπηρεσία |
| **Επιχειρησιακή στόχευση** | Διεπιχειρησιακή B2B | Διεπιχειρησιακή B2B, Επιχειρησιοκαταναλωτική B2C |
| | Καθιερωμένη αλυσίδα αξιών | Αναδυόμενα οικοσυστήματα |
| | Εσωτερική/ενδοεταιρική ανάπτυξη | Νεφοϋπολογιστική ανάπτυξη |
| **Τεχνολογία** | Εξειδικευμένες συσκευές | Συσκευές γενικής χρήσης |
| | De facto και ιδιοταγής | Πρότυπα και ανοικτός κώδικας |
| | Συγκεκριμένες/κλειστές μορφές δεδομένων και περιγραφές υπηρεσιών | Ανοιχτά APIs και προδιαγραφές δεδομένων |
| | Κλειστό/εξειδικευμένο λογισμικό | Λογισμικό ανοικτού κώδικα |

Το γενικό συμπέρασμα που προκύπτει από την αντιπαραβολή των M2M και IoT χαρακτηριστικών είναι πως μια λύση που βασίζεται σε M2M επικεντρώνεται στην επίλυση ενός προβλήματος, σε ένα συγκεκριμένο σημείο, για έναν φορέα ή για μια μικρή μερίδα ενδιαφερόμενων. Αντιθέτως, μια λύση που βασίζεται στο IoT στοχεύει στην επίλυση περισσότερων του ενός προβλημάτων ή προβλημάτων που έχουν μεγαλύτερη μερίδα ενδιαφερομένων. Γενικότερα, μια λύση που βασίζεται στο IoT χαρακτηρίζεται από διαφάνεια, πολλαπλή αξιοποίηση και καινοτομία των λειτουργιών και των δεδομένων της.

Η υπηρεσία iBuC πληροί τα χαρακτηριστικά αυτά καθώς έχει διαλειτουργικότητα και με το σύστημα υποστήριξης λειτουργιών uBSS του πανεπιστημίου. Η διαλειτουργικότητα αυτή διευκολύνει την επίλυση και άλλων ζητημάτων εκτός του προβλήματος του πρώτου/τελευταίου μιλίου, όπως είναι η καταγραφή της κινητικότητας του πληθυσμού της κοινότητας στην πανεπιστημιούπολη. Συνεπώς, εκτός από το ότι η διαλειτουργικότητα

διευρύνει το πλήθος των ζητημάτων που απαντώνται, συνδέεται και με την πολλαπλή αξιοποίηση των δεδομένων της υπηρεσίας. Η διαλειτουργικότητα αυτή θα μπορούσε να επεκταθεί και προς άλλα συστήματα ή υπηρεσίες.

Επίσης, η υποστήριξη αυτής της διαλειτουργικότητας με άλλα συστήματα και υπηρεσίες απαιτεί τη διαφανή πρόσβαση τρίτων στα δεδομένα της υπηρεσίας. Αυτή η πρόσβαση διευκολύνεται από την ανάπτυξη της κεντρικής μονάδας ελέγχου CU, η οποία έχει και τον ρόλο της τράπεζας δεδομένων της υπηρεσίας, στη νεφοϋπολογιστική υποδομή. Αξίζει, τέλος, να σημειωθεί, πως η διαλειτουργικότητα διευρύνει και τη μερίδα ενδιαφερομένων στην εξυπηρέτηση των οποίων συνδράμει η iBuC.

Συμπερασματικά, η υπηρεσία iBuC σε σχέση με τα χαρακτηριστικά μιας λύσης που βασίζεται στο IoT, πληροί τα ακόλουθα:

- Οδηγείται από την καινοτομία και στοχεύει στην επίλυση περισσότερων του ενός προβλημάτων.
- Ενσωματώνει εφαρμογές γενικής χρήσης, όπως είναι οι εφαρμογές χαρτογράφησης.
- Επικεντρώνεται στην υπηρεσία και στα δεδομένα που πηγάζουν από αυτή.
- Είναι B2B για τον φορέα του πανεπιστημίου και B2C καθώς απευθύνεται σε μεγαλύτερη μερίδα ενδιαφερομένων (επισκέπτες της πανεπιστημιούπολης, συστήματα και υπηρεσίες που ενημερώνονται από το uBSS).
- Πρόκειται για ένα αναδυόμενο οικοσύστημα, καθώς αναπτύσσεται προς επίλυση του αναπάντητου προβλήματος του πρώτου/τελευταίου μιλίου σε μια πανεπιστημιούπολη.
- Υποστηρίζεται από τη νεφοϋπολογιστική υποδομή.
- Χρησιμοποιεί ανοικτά APIs, προδιαγραφές δεδομένων και λογισμικό.

Ωστόσο, η διαλειτουργικότητα της υπηρεσίας μεταφορών με τριτομερή υπηρεσία ή τριτομερές σύστημα, ενδέχεται να αλλάξει τη φύση της ίδιας της υπηρεσίας. Τυχόν αλλαγές θα πρέπει να ληφθούν υπόψη και για την επίδρασή τους στη διαδικασία λήψης αποφάσεων της υπηρεσίας και για την επίδρασή τους σε σημαντικές διεργασίες, όπως είναι η διαχείριση στόλου της iBuC. Για τον λόγο αυτό, παρακάτω μελετάται ο βαθμός διαφοροποίησης της διαχείρισης στόλου της iBuC λαμβάνοντας υπόψη δύο σενάρια: στο πρώτο σενάριο η iBuC ενσωματώνει τα δεδομένα υπηρεσίας από ένα Σύστημα Δημοσίων Μεταφορών (Public Transportation System, PTS) και στο δεύτερο σενάριο η iBuC ενσωματώνει τα δεδομένα από μια υπηρεσία πρόγνωσης καιρού (Weather Forecasting Service, WFS).

# Κεφάλαιο 4

# Πλατφόρμα μοντελοποίησης και αξιολόγησης ασφάλειας SAPnet

## 4.1 Διαδικασία αξιολόγησης ασφάλειας

Για την αξιολόγηση ασφάλειας μιας υπηρεσίας που βασίζεται στο IoT χρησιμοποιείται μια μέθοδος που βασίζεται στο μοντέλο SPN και τη λίστα κοινών ευπαθειών CVE των επιμέρους στοιχείων της υπηρεσίας. Η διαδικασία που ακολουθείται έχει τρία στάδια:

*(α)* τη διερεύνυση της δυνατότητας να αποδοθεί με στοχαστική μοντελοποίηση η υπό μελέτη υπηρεσία,

*(β)* τη σύσταση της λίστας (διεξοδική ή επιλεκτική) των κοινών ευπαθειών CVE της υπηρεσίας, και

*(γ)* τον υπολογισμό των μετρικών ασφάλειας της υπηρεσίας.

Η μεθοδολογία αυτή αποτελεί τον οδηγό για την ανάπτυξη της σχεδιαστικής πλατφόρμας SAPnet. Το μετα-μοντέλο, η σημασιολογία και οι αλγόριθμοι που συνθέτουν το ADOxx© εργαλείο μοντελοποίησης SAPnet περιγράφονται ακολούθως. Παρουσιάζεται, επίσης, η αξιοποίηση της SAPnet για τη μοντελοποίηση και την αξιολόγηση ασφάλειας της υπηρεσίας μεταφορών που βασίζεται στο IoT που περιγράφηκε στο προηγούμενο κεφάλαιο, της υπηρεσίας iBuC. Με τη βοήθεια της προτεινόμενης πλατφόρμας, ερευνάται το αν και πώς επηρεάζεται η συμπεριφορά και το επίπεδο ασφάλειας της IoT υπηρεσίας μεταφορών από την αλλαγή ενός IoT χαρακτηριστικού της, όπως η φύση της ενσωματωμένης τριτομερούς υπηρεσίας. Επίσης, καταγράφεται ο βαθμός κατά τον οποίο η SAPnet διευκολύνει και επιταχύνει τη διαδικασία αξιολόγησης ασφάλειας της υπηρεσίας.

### 4.1.1 Μοντελοποίηση ευφυούς υπηρεσίας

Η Petri net (PN) είναι μια μαθηματική γλώσσα μοντελοποίησης με λιτή σημασιολογία. Η μέθοδος εξυπηρετεί την περιγραφή κατανεμημένων συστημάτων και τα μοντέλα που παράγονται με αυτή μπορούν να απεικονίσουν με απλότητα τις δυναμικές αλλαγές ενός τέτοιου συστήματος. Τα βασικά στοιχεία του συμβολισμού PN είναι η *κατάσταση (Place)*,

η *μετάβαση (Transition)*, το *τόξο ή ροή (Arc)* και το *κουπόνι ή μάρκα (Token)*, που χρησιμοποιούνται για την απεικόνιση των καταστάσεων, των αλλαγών ή των ενεργειών, της ροής κατάσταση-προς-κατάσταση, και της σήμανσης ή ενεργοποίησης καταστάσεων, αντίστοιχα. Οι μεταβάσεις ενεργοποιούνται εάν η προηγούμενη κατάσταση περιέχει έστω ένα κουπόνι. Με την ενεργοποίηση μιας μετάβασης μετακινείται το σχετικό κουπόνι στην επόμενη κατάσταση. Η αξιολόγηση μπορεί να πιστοποιήσει την εγκυρότητα ενός μοντέλου PN [20] μέσω του ελέγχου:

*(α)* της προσβασιμότητας όλων των καταστάσεων,

*(β)* της μη ύπαρξης κινδύνου αδιεξόδου, και

*(γ)* της ζωτικότητας των μεταβάσεων.

Μια επέκταση της Petri net είναι ο φορμαλισμός SPN. Η SPN σχετίζεται στενά με τη μαθηματική διαδικασία Markov. Σε αντίθεση με την PN, στην SPN απεικονίζεται η διάρκεια των δραστηριοτήτων και η καθυστέρηση μεταξύ των συμβάντων [19]. Αυτό επιτυγχάνεται με τα *κουπόνια ή μάρκες (Tokens)* και τις ρυθμίσεις *πυροδότησης των μεταβάσεων (transitions firing)*. Αυτή η δυνατότητα είναι σημαντική για τη μοντελοποίηση διεργασιών ή λειτουργιών πραγματικού χρόνου, αφού ο χρόνος που καταναλώνεται ανά κατάσταση επηρεάζει όλες τις ακόλουθες καταστάσεις του συστήματος ή της υπηρεσίας.

Όταν το κύριο ζήτημα είναι η μελέτη του επιπέδου ασφάλειας ενός συστήματος ή μιας υπηρεσίας, η χρήση της SPN μπορεί να φανεί χρήσιμη, λόγω της σαφούς απεικόνισης των καταστάσεων και της μετάβασης από τη μια κατάσταση στην επόμενη. Το επίπεδο ασφάλειας του συστήματος ή της υπηρεσίας μπορεί να αυξηθεί εάν αντιμετωπιστούν ή μετριαστούν οι ευπάθειες που σχετίζονται με κάθε κατάσταση [69]. Η μοντελοποίηση ενός συστήματος ή μιας υπηρεσίας με τη χρήση της SPN μπορεί να αναδείξει τις καταστάσεις οι οποίες πρέπει να βελτιωθούν από άποψη ασφάλειας. Αυτά τα χαρακτηριστικά αναδεικνύουν τη μοντελοποίηση SPN ως πολύτιμο εργαλείο σχεδιασμού για μια υπηρεσία που βασίζεται στο IoT.

Η διαδικασία της κοινής χρήσης δεδομένων μιας υπηρεσίας που βασίζεται στο IoT με τριτομερείς υπηρεσίες, είναι ένα χαρακτηριστικό του οικοσυστήματος του IoT, που διευκολύνει στην επίτευξη λειτουργιών με επίκεντρο τις πληροφορίες και τις υπηρεσίες [68]. Αυτή η δυνατότητα επιτρέπει τη μεγιστοποίηση της χρηστικότητας των δεδομένων που παράγονται στις επιμέρους υπηρεσίες και ωφελεί τις συνεργαζόμενες πλευρές όσον αφορά στη λήψη αποφάσεων, στον έλεγχο και στην ποιότητα της προσφερόμενης υπηρεσίας. Ωστόσο, αυτή η ενσωμάτωση δεδομένων μπορεί να επηρεάσει τη λειτουργία της κάθε εμπλεκόμενης υπηρεσίας, καθώς και των διαδικασιών που περιλαμβάνονται σε αυτήν, λόγω της εισροής νέων δεδομένων στη διαδικασία λήψης αποφάσεων και λόγω της ύπαρξης της τριτομερούς υπηρεσίας η οποία αποτελεί πρόσθετο παράγοντα λειτουργίας και ασφάλειας.

Η δυναμική συμπεριφορά μιας υπηρεσίας μπορεί να απεικονιστεί χρησιμοποιώντας διάφορες μεθόδους μοντελοποίησης. Ωστόσο, στην περίπτωση μιας υπηρεσίας που βασίζεται στο IoT και λειτουργεί με την ενσωμάτωση δεδομένων μιας τριτομερούς υπηρεσίας, τα γεγονότα σε έναν κύκλο της υπηρεσίας μπορεί να μην ακολουθούν μια καθορισμένη χρονική διαδοχή. Ως εκ τούτου, μια τέτοια υπηρεσία δεν μπορεί εύκολα να

αποδοθεί με μεθόδους στατικής μοντελοποίησης, καθιστώντας τη στοχαστική προσέγγιση αναγκαία. Ο φορμαλισμός SPN δίνει τη δυνατότητα μοντελοποίησης της διάρκειας των δραστηριοτήτων και της καθυστέρησης μεταξύ των γεγονότων [19]. Αυτό επιτυγχάνεται με τη χρήση κουπονιών (tokens) και τη δυνατότητα της πυροδότησης της μετάβασης (transition firing). Οι καταστάσεις SPN είναι η απεικόνιση των καταστάσεων των δρώντων στοιχείων εντός της υπηρεσίας. Η μοντελοποίηση με τον φορμαλισμό SPN επιτρέπει την αξιολόγηση ασφάλειας της υπηρεσίας σε συνάρτηση με την κατάσταση του κάθε δρώντος στοιχείου σε έναν κύκλο λειτουργίας της υπηρεσίας.

### 4.1.2 Αδυναμίες και ευπάθειες της υπηρεσίας

Τα συνολικά ζητήματα ασφάλειας μιας υπηρεσίας σχετίζονται με τις αδυναμίες (weaknesses) των βασικών ενεργοποιητών της υπηρεσίας. Οι αδυναμίες στον έλεγχο πρόσβασης, στον έλεγχο της ταυτότητας ή στην έκθεση πληροφοριών εκφράζονται από τα τρωτά σημεία ή ευπάθειες (vulnerabilities) κάθε στοιχείου υλικού ή λογισμικού. Μια αδυναμία περιγράφει τα σφάλματα και τις βλάβες μιας υπηρεσίας, ανεξάρτητα από συγκεκριμένα στοιχεία, προϊόντα ή προμηθευτές/κατασκευαστές. Επίσης, μια αδυναμία σχετίζεται με πολλές ευπάθειες. Το σύνολο των ευπαθειών μιας υπηρεσίας εξαρτάται από τα συγκεκριμένα στοιχεία, το λογισμικό, το υλικό καθώς και τον αρχιτεκτονικό σχεδιασμό της υπηρεσίας.

Το πρώτο στάδιο στη διαδικασία αξιολόγησης της υπηρεσίας είναι η μοντελοποίηση των καταστάσεων της υπηρεσίας με τη σημασιολογία της SPN.

Ως δεύτερο στάδιο στη διαδικασία αξιολόγησης της υπηρεσίας αναπτύσσεται μια λίστα αδυναμιών χρησιμοποιώντας τη λίστα Architectural Concepts (CWE-1008) που παρέχεται από τη βάση δεδομένων κοινών αδυναμιών (Common Weakness Enumeration, CWE) του οργανισμού Massachusetts Institute of Technology Research & Engineering (MITRE) [70]. Για τη λίστα αυτή, επιλέγεται μια ενδεικτική ευπάθεια για κάθε αδυναμία, με βάση τα ακόλουθα δύο κριτήρια:

*(α)* τη συνάφεια μεταξύ της ευπάθειας και των στοιχείων της υπηρεσίας, και

*(β)* τον αντίκτυπο της ευπάθειας στην ακεραιότητα και το απόρρητο δεδομένων της υπηρεσίας, όπως αυτός αποδίδεται με τη βαθμολογία ασφάλειας [52] της ευπάθειας.

Αυτά τα κριτήρια επιτρέπουν τη δημιουργία μιας λίστας, όπου κάθε ευπάθεια στη λίστα αυτή είναι η πιο σημαντική για την αντίστοιχη αδυναμία της υπηρεσίας υπό αξιολόγηση.

Η συνάφεια μιας ευπάθειας ορίζεται από τη λογική συσχέτιση της ευπάθειας αυτής με τις καταστάσεις της υπηρεσίας. Το κριτήριο συνάφειας βοηθά στην επιλογή της ομάδας των *συναφών ευπαθειών*, που είναι εγγενείς για το λογισμικό και το υλικό της υπηρεσίας. Μέσα σε αυτήν την ομάδα σχετικών ευπαθειών, ορισμένες έχουν μεγαλύτερο αντίκτυπο, λόγω της συχνότητας εκμετάλλευσής τους από επιθέσεις. Η χρήση της βασικής βαθμολογίας Common Vulnerability Scoring System (CVSS) [52] επιτρέπει την ποσοτικοποίηση του αντίκτυπου για τη συγκεκριμένη οντότητα που πάσχει από την ευπάθεια (δηλαδή, λογισμικό, στοιχείο υλικού και λειτουργικό σύστημα, μεταξύ άλλων). Η βασική βαθμολογία CVSS βαθμονομεί τη σοβαρότητα της ευπάθειας σε μια κλίμακα από το 0 έως το 10, όπου το 10 είναι η πιο κρίσιμη τιμή. Αυτό το κριτήριο επίπτωσης

της κάθε ευπάθειας, βοηθά στην επιλογή των *πλέον κρίσιμων συναφών ευπαθειών* από το σύνολο των συναφών με την υπηρεσία ευπαθειών.

Το τρίτο στάδιο της διαδικασίας αξιολόγησης της υπηρεσίας είναι ο υπολογισμός της μετρικής ασφάλειας SM(0) της υπηρεσίας για τη λίστα των ευπαθειών που φέρει και βάσει των βασικών βαθμολογιών CVSS των ευπαθειών της και ο υπολογισμός της μετρικής ασφάλειας SM(t) της υπηρεσίας για τη λίστα των ευπαθειών που φέρει και βάσει των χρονικών βαθμολογιών CVSS των ευπαθειών της. Η μέθοδος υπολογισμού των μετρικών αυτών, περιγράφεται παρακάτω.

### 4.1.3 Υπολογισμός της μετρικής ασφάλειας

Το τρίτο στάδιο της διαδικασίας αξιολόγησης είναι ο υπολογισμός της μετρικής ασφάλειας, που ξεκινά με τον υπολογισμό της *συχνότητας εμφάνισης* ($R_n$) κάθε αδυναμίας $n$ από ένα πλήθος αδυναμιών $l$. Στην περίπτωση που η *συχνότητα εμφάνισης* ($R_n$) υπολογίζεται με βάση το μοντέλο SPN ενός συστήματος ή υπηρεσίας [71], τότε χρησιμοποιείται η ακόλουθη σχέση:

$$R_n = \frac{k}{\Sigma_{i=1}^{m} A_i}, \tag{4.1}$$

όπου:

- $k$ είναι το πλήθος των επιλεγμένων ευπαθειών της αδυναμίας,
- $m$ είναι το συνολικό πλήθος των καταστάσεων του μοντέλου SPN, και
- $A_i$ είναι η μεταβλητή ακεραίου που έχει τιμή 1 σε κάθε κατάσταση του μοντέλου SPN που επηρεάζεται από αυτές τις ευπάθειες.

Το άθροισμα του παρονομαστή της Εξίσωσης 4.1 υπολογίζει το πλήθος των καταστάσεων του μοντέλου SPN όπου $A_i = 1$.

Η *δριμύτητα* ($W_n$) κάθε αδυναμίας υπολογίζεται με την ακόλουθη σχέση:

$$W_n = \Sigma_{i=1}^{k} \frac{V_i}{k \cdot CR \cdot IR \cdot AR}, \tag{4.2}$$

όπου:

- $V_i$ είναι η βασική βαθμολογία CVSS για κάθε ευπάθεια $i$ από τις συνολικές $k$ ευπάθειες της αδυναμίας, και
- $CR$, $IR$ και $AR$ είναι οι Περιβαλλοντικές Μετρικές κάθε ευπάθειας.

Η δριμύτητα επηρεάζεται από τις τιμές των Περιβαλλοντικών Μετρικών, οι οποίες αλλάζουν ως αποτέλεσμα του όποιου μετριασμού μιας ευπάθειας. Η μετρική απαίτησης εμπιστευτικότητας (Confidentiality Requirement, CR), η μετρική απαίτησης ακεραιότητας (Integrity Requirement, IR) και η μετρική απαίτησης διαθεσιμότητας (Availiability Requirement, AR) ενδέχεται να λάβουν μια από τις τιμές 0.5 (χαμηλής δριμύτητας ευπάθεια), 1.0 (άγνωστης ή μέτριας δριμύτητας ευπάθεια) ή 1.51 (υψηλής δριμύτητας ευπάθεια) [52].

Ο *κίνδυνος* ($P_n$) κάθε αδυναμίας δίνεται από την ακόλουθη σχέση:

$$P_n = \frac{R_n}{\Sigma_{n=1}^{l} R_n}, \tag{4.3}$$

όπου:

- textitR$_n$ είναι το αποτέλεσμα υπολογισμού της *συχνότητας εμφάνισης* χρησιμοποιώντας την Εξίσωση 4.1,
- ο παρονομαστής υπολογίζει το άθροισμα όλων των $R_n$ των αδυναμιών, και
- $l$ είναι το πλήθος των αδυναμιών.

Το τελευταίο βήμα είναι ο υπολογισμός της *μετρικής ασφάλειας SM(0)* με την ακόλουθη σχέση:

$$SM(0) = \Sigma_{n=1}^{l}(P_n \cdot W_n), \tag{4.4}$$

όπου:

- $P_n$ είναι το αποτέλεσμα υπολογισμού του *κινδύνου* της κάθε αδυναμίας χρησιμοποιώντας την Εξίσωση 4.3 για τον αριθμό $l$ των αδυναμιών, και
- $W_n$ είναι το αποτέλεσμα υπολογισμού της *δριμύτητας* κάθε αδυναμίας χρησιμοποιώντας την Εξίσωση 4.2.

Εάν το *SM(0)* έχει υψηλή τιμή, τότε η υπηρεσία βρίσκεται σε κρίσιμη κατάσταση σε θέματα ασφάλειας. Η μετρική ασφάλειας *SM(t)* της υπηρεσίας προκύπτει με την ίδια διαδικασία μετά τον μετριασμό των ευπαθειών και με τη χρήση της χρονικής αντί της βασικής βαθμολογίας CVSS κάθε ευπάθειας, που χρησιμοποιείται στον υπολογισμό της *SM(0)*.

## 4.2 Μετα-μοντέλο, σημασιολογία και αλγόριθμοι

Το υβριδικό εργαλείο μετα-μοντελοποίησης Bee-Up [21], που υποστηρίζεται από την πλατφόρμα meta$^2$-modeling ADOxx©, παρέχει τη βιβλιοθήκη με τη σημασιολογία της Petri net (Petri net Dynamic Library). Η SAPnet (Εικόνα 4) επεκτείνει τη βιβλιοθήκη αυτή, κυρίως με δύο στοιχεία μετα-μοντέλου:

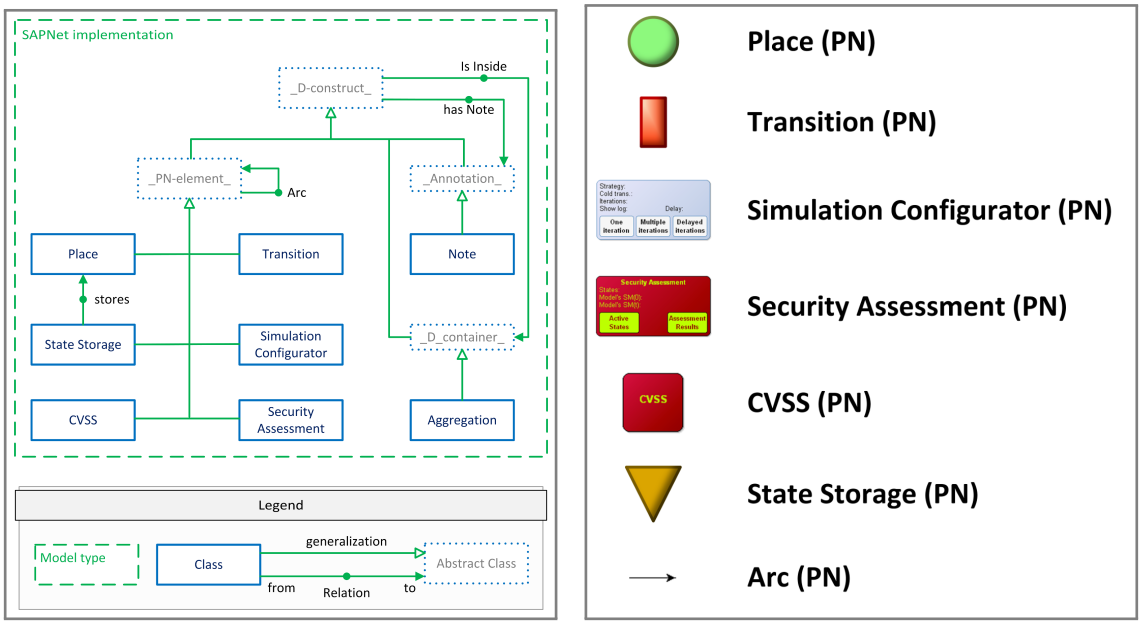
*(α)* την κλάση *CVSS*, και

*(β)* την κλάση *Security Assessment*.

Το μετα-μοντέλο της SAPnet φαίνεται στην Εικόνα 4α και τα σημασιολογικά στοιχεία *CVSS (PN)* και *Security Assessment (PN)* των αντίστοιχων κλάσεων παρουσιάζονται στην Εικόνα 4β.

Οι νέες κλάσεις είναι στοιχεία της αφηρημένης κλάσης *PN-element*. Οι κλάσεις αυτές επιτρέπουν στον μηχανικό να χρησιμοποιεί δεδομένα του μοντέλου, όπως για παράδειγμα τη λίστα των καταστάσεων του μοντέλου, σε πραγματικό χρόνο κατά τη διαδικασία αξιολόγησης της ασφάλειας. Ως εκ τούτου, η διαδικασία της αξιολόγησης διευκολύνεται και επιταχύνεται και τα αποτελέσματα είναι πιο ακριβή και επίκαιρα. Οι νέες κλάσεις

και οι αλγόριθμοι που περιλαμβάνει η κάθε μια από αυτές, περιγράφονται αναλυτικά στη συνέχεια.




(α) Μετα-μοντέλο (β) Σημασιολογία

Εικόνα 4. Υλοποίηση SAPnet

### 4.2.1 Πλατφόρμα μετα-μετα-μοντελοποίησης ADOxx

Το ADOxx© είναι μια πλατφόρμα ανάπτυξης και διαμόρφωσης μετα-μοντέλων για τη μοντελοποίηση βάσει διαφόρων μεθόδων. Η πλατφόρμα μετα$^2$-μοντελοποίησης η οποία υποστηρίζει πληθώρα σημασιολογιών, μηχανισμών και αλγορίθμων. Η πλατφόρμα μετα$^2$-μοντελοποίησης ADOxx©, καθώς και οι επιμέρους πλατφόρμες μετα-μοντελοποίησης που αναπτύσσονται στο ADOxx© υποστηρίζονται από μια ευρεία κοινότητα ειδικών [72].

Η πλατφόρμα ADOxx© χρησιμοποιείται από τα τέλη της δεκαετίας του 1990 σε μεγάλο αριθμό ερευνών και βιομηχανικών έργων, ορισμένα από τα οποία απευθύνονταν σε μεγάλες γερμανικές και αυστριακές εταιρείες ως πελάτες [73]. Η εξάπλωση της χρήσης της πλατφόρμας ADOxx© ξεκίνησε με την υιοθέτηση της χρήσης της από την αυστριακή ένωση Open Models Initiative [74],[75]. Σήμερα, ο βασικός συντονιστής της κοινότητας ειδικών σε θέματα ανάπτυξης της πλατφόρμας ADOxx© είναι το εργαστήριο Open Models Laboratory (OMiLAB) [76] του τμήματος Knowledge Engineering του Πανεπιστημίου της Βιέννης.

Με βάση την πλαρφόρμα ADOxx©, έχουν αναπτυχθεί πολλά εργαλεία μετα-μοντελοποίησης στην πάροδο της τελευταίας δεκαετίας. Μεταξύ αυτών είναι και το υβριδικό εργαλείο μετα-μοντελοποίησης Bee-Up [21], που παρέχει τη βιβλιοθήκη με τη σημασιολογία της SPN (Petri net Dynamic Library). Η βιβλιοθήκη αυτή υπήρξε η βάση ανάπτυξης της πλατφόρμας μετα-μοντελοποίησης SAPnet.

### 4.2.2 Διεπαφή ευπαθειών

Η κλάση *CVSS* παρέχει μια διεπαφή, φιλική προς τον μηχανικό, για τη δημιουργία της λίστας ευπαθειών της περιγραφόμενης, μέσω του μοντέλου, υπηρεσίας. Αυτή η διεπαφή υποβοηθούμενης κατασκευής λίστας υποστηρίζει τις ακόλουθες δυνατότητες:

- **Ο μηχανικός μπορεί να εισάγει τις ευπάθειες μεμονωμένα**
  Σε αυτήν την περίπτωση, ο μηχανικός καθοδηγείται με μηνύματα και ειδοποιήσεις περιορισμών πεδίων, έτσι ώστε η λίστα να περιέχει μόνο ευπάθειες με έγκυρη βασική βαθμολογία CVSS (δηλαδή, μεγαλύτερη από 0 και μικρότερη ή ίση με 10). Ωστόσο, ο μηχανικός μπορεί να εισάγει μια ευπάθεια για την οποία δεν υπάρχουν μέτρα προστασίας ή μετριασμού και, ως εκ τούτου, δεν διαθέτει χρονική βαθμολογία CVSS. Σε αυτήν την περίπτωση, ο κώδικας της κλάσης θα αντιστοιχίσει τη χρονική βαθμολογία CVSS *(CVSS_Temporal)* με τη βασική βαθμολογία CVSS *(CVSS_Base)* για την ευπάθεια με το συγκεκριμένο *CVE_ID*. Αφού εισαχθούν οι τιμές για μια ευπάθεια, ο μηχανικός μπορεί να χρησιμοποιήσει την επιλογή *csv2table* (Αλγόριθμος 1). Η επιλογή *csv2table* ενεργοποιεί τον κώδικα προγραμματισμού για τους ελέγχους επικύρωσης της νέας υπό υποβολή ευπάθειας. Επιπλέον, ο κώδικας *csv2table* εκτελεί συγκρίσεις της νέας αυτής εγγραφής με όλες τις ήδη αποθηκευμένες εγγραφές με σκοπό να αποτρέπονται τα διπλότυπα ευπαθειών.

**Αλγόριθμος 1** Ιδιοχαρακτηριστικό *csv2table*

**Input:** $CVE\_ID \in \mathbb{N}^*$
$CVSS\_Base \in \mathbb{R}^+$
$CVSS\_Temporal \in \mathbb{R}^+$
**Output:** new record [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*] in *CVE_choices* table

1: **if** $CVSS\_Temporal = \text{null}$ **then**
2: $CVSS\_Temporal \leftarrow CVSS\_Base$
3: **for each** $CVE\_ID \in CVE\_choices[]$ **do**
4: **if** *CVE_ID* does not exist **then**
5: **create** new record [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*]

- **Ο μηχανικός μπορεί να καλέσει μια προκαθορισμένη λίστα**
  Αυτή η δυνατότητα, η οποία παρέχεται από την επιλογή *Load_CVE_List* (Αλγόριθμος 2), επιτρέπει την εισαγωγή λίστας από ένα οριοθετημένο αρχείο που είναι αποθηκευμένο στη διαδρομή:

  ```
  "%ProgramFiles%/BOC/ADOxx15_EN_SA"
  ```

  Το αρχείο πρέπει να περιλαμβάνει τα στοιχεία τουλάχιστον μίας ευπάθειας για να θεωρηθεί έγκυρο. Τα στοιχεία κάθε ευπάθειας καταλαμβάνουν μία γραμμή στα περιεχόμενα του αρχείου, με το αναγνωριστικό *CVE_ID*, τη βασική βαθμολογία *CVSS_Base* και τη χρονική βαθμολογία *CVSS_Temporal* της ευπάθειας να διαχωρίζονται από τον οριοθέτη (έχει προκαθοριστεί ο ειδικός χαρακτήρας «;» ως οριοθέτης), για παράδειγμα:

  ```
  CVE-2017-7214;9.8;9.1
  ```

Εάν το αρχείο υπάρχει και δεν είναι κενό, τα περιεχόμενά του θα υποβληθούν σε επεξεργασία γραμμή-προς-γραμμή και θα χρησιμοποιηθούν για την εισαγωγή της λίστας.

**Αλγόριθμος 2** Ιδιοχαρακτηριστικό *Load_CVE_List*

**Input:** *LFILE* name of comma-delimited file
**Output:** new records [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*] in *CVE_choices* table

1: **for each** line ∈ *LFILE* **do**
2: **create** new record [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*]

- **Αλλαγές και αποθήκευση κατά τη δημιουργία και εκ των υστέρων**

  Οι προηγούμενες δύο δυνατότητες λειτουργίας ενδέχεται να χρησιμοποιηθούν περισσότερες από μία φορά κατά τη διαδικασία μοντελοποίησης. Ο μηχανικός μπορεί να αναθεωρήσει μια λίστα που έχει ήδη δημιουργήσει, καταργώντας/τροποποιώντας μεμονωμένες εγγραφές της λίστας ή εισάγοντας μια νέα λίστα από ένα αρχείο. Επίσης, ο μηχανικός μπορεί να αποφασίσει τη δημιουργία μιας νέας λίστας από την αρχή. Για τον λόγο αυτό, παρέχεται η δυνατότητα εκκαθάρισης της λίστας με την επιλογή *Clear_CVE_List* (Αλγόριθμος 3). Ο κώδικας της επιλογής αυτής περιέχει ελέγχους για τα περιεχόμενα της λίστας. Εάν η λίστα δεν είναι κενή, η επιλογή *Clear_CVE_List* οδηγεί σε διαγραφή των περιεχομένων, αφού ο μηχανικός επιβεβαιώσει, μέσω ενός σχετικού μηνύματος, την επιλογή του αυτή. Ο μηχανικός έχει την επιλογή να αποθηκεύσει τη λίστα για μελλοντική χρήση σε ένα εξωτερικό οριοθετημένο αρχείο. Αυτή η δυνατότητα παρέχεται από την επιλογή *Save_CVE_List* (Αλγόριθμος 4). Αυτή η δυνατότητα εξαγωγής της λίστας σε αρχείο όπως και η δυνατότητα αποθήκευσης της λίστας, στοχεύουν στη διευκόλυνση του μηχανικού να χρησιμοποιήσει τη λίστα αυτή για την αξιολόγηση της ασφάλειας του μοντέλου. Η διαδικασία αποθήκευσης της λίστας υποστηρίζεται από την κλάση εγγραφών *cvss2table*.

**Αλγόριθμος 3** Ιδιοχαρακτηριστικό *Clear_CVE_List*

**Input:** records [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*] in *CVE_choices* table

1: **for each** record ∈ *CVE_choices[]* **do**
2: **delete** record [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*]

**Αλγόριθμος 4** Ιδιοχαρακτηριστικό *Save_CVE_List*

**Input:** records [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*] in *CVE_choices* table
**Output:** *LFILE* name of comma-delimited file

1: **for each** record ∈ *CVE_choices[]* **do**
2: **create** new *LFILE* line *"CVE_ID*;*CVSS_Base*;*CVSS_Temporal"*

Η δημιουργία μιας έγκυρης και καθαρής λίστας ευπαθειών είναι ένα σημαντικό βήμα στη διαδικασία αξιολόγησης της ασφάλειας. Χρησιμοποιώντας την κλάση *CVSS*, αυτή η διαδικασία εξακολουθεί να είναι πολύπλοκη και χρονοβόρα για τον μηχανικό που την ακολουθεί, ωστόσο, η κλάση *CVSS* διευκολύνει:

*(α)* τον έλεγχο εγκυρότητας των εγγραφών της λίστας και των επιμέρους τιμών της εγγραφής,

*(β)* την αναθεώρηση και προσαρμογή των περιεχομένων της λίστας, και

*(γ)* την εισαγωγή/εξαγωγή της λίστας από την πλατφόρμα SAPnet σε άλλο λογισμικό και αντίστροφα.

### 4.2.3 Διεπαφή αξιολόγησης της ασφάλειας

Η κλάση *Security Assessment* υποστηρίζει τον μηχανισμό της αξιολόγησης της ασφάλειας και παρέχει σε πραγματικό χρόνο δυναμικά ενημερωμένες πληροφορίες σχετικά με το ενεργό μοντέλο καθώς και για τα αποτελέσματα της αξιολόγησης. Ο αρχικός στόχος του μηχανικού σε αυτή τη φάση είναι να κάνει έναν συσχετισμό μεταξύ των επιλεγμένων ευπαθειών και των καταστάσεων του μοντέλου που επηρεάζονται από αυτές τις ευπάθειες. Αυτή η συσχέτιση είναι απαραίτητη για τους υπολογισμούς της διαδικασίας αξιολόγησης της ασφάλειας. Η κλάση παρέχει στον μηχανικό τις ακόλουθες δυνατότητες:

- **Διατίθενται επιλογές φόρτωσης, τροποποίησης και αποθήκευσης**
  Αυτή η κλάση στοχεύει κυρίως στη βοήθεια του μηχανικού να προχωρήσει στην αξιολόγηση της ασφάλειας του μοντέλου. Ωστόσο, ο μηχανικός έχει και στο περιβάλλον της κλάσης αυτής τη δυνατότητα να χειριστεί τα περιεχόμενα της λίστας ευπαθειών πριν τη χρήση της για την αξιολόγηση. Μια νέα λίστα μπορεί να φορτωθεί από ένα οριοθετημένο αρχείο με την επιλογή *Load CVE List* (Αλγόριθμος 5), να τροποποιηθεί σε επιμέρους εγγραφές ή τιμές ή ακόμα και να απαλειφθεί καθολικά με την επιλογή *Clear CVE List* (Αλγόριθμος 6) και να αποθηκευτεί σε ένα εξωτερικό οριοθετημένο αρχείο για μελλοντική χρήση με την επιλογή *Save CVE List* (Αλγόριθμος 7 ).

**Αλγόριθμος 5** Ιδιοχαρακτηριστικό *Load CVE List*

**Input:** *LFILE* name of comma-delimited file
**Output:** new records [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*] in *CVE_choices* table
*sm0_tag* value on *Model SM(0)* attribute
*smt_tag* value on *Model SM(t)* attribute

1: **for each** line $\in$ *LFILE* **do**
2: **create** new record [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*]
3: **update** *sm0_tag* $\leftarrow$ null, *smt_tag* $\leftarrow$ null

**Αλγόριθμος 6** Ιδιοχαρακτηριστικό *Clear CVE List*

**Input:** records in *CVE_choices* table

1: **for each** record ∈ *CVE_choices[]* **do**
2: **delete** record

**Αλγόριθμος 7** Ιδιοχαρακτηριστικό *Save CVE List*

**Input:** records in *CVE_choices* table
**Output:** *LFILE* name of comma-delimited file

1: **for each** record ∈ *CVE_choices[]* **do**
2: **create** new *LFILE* line *"CVE_ID*;*CVSS_Base*;*CVSS_Temporal*;*NofStates*;*Rn*;*Pn"*
3: **create** new *LFILE* line *"SM(0)*;*SM(t)"*

- **Συσχετισμός ευπαθειών και καταστάσεων**

  Η επιλογή *Affected States* (Αλγόριθμος 8) παρέχει στον μηχανικό έναν οδηγό για τη διευκόλυνση της συσχέτισης των ευπαθειών με τις καταστάσεις του ενεργού μοντέλου. Ο σχετικός κώδικας καλεί τον μηχανικό:

  *(α)* να επιλέξει ένα CVE_ID από τη λίστα του, και

  *(β)* να επιλέξει μία ή περισσότερες καταστάσεις που υπάρχουν στο μοντέλο και που επηρεάζονται από την ευπάθεια που έχει ήδη επιλεγεί.

  Στο τρίτο βήμα αυτού του οδηγού, ο μηχανικός λαμβάνει ένα μήνυμα οθόνης σχετικά με τις επιλογές του για λόγους επαλήθευσης και επιβεβαίωσης. Εάν οι συσχετίσεις επιβεβαιωθούν, η λίστα ευπαθειών ενημερώνεται με το πλήθος των καταστάσεων που επηρεάζονται ανά ευπάθεια (δηλαδή, ενημερώνεται η στήλη με τίτλο *NofStates* της λίστας).

**Αλγόριθμος 8** Ιδιοχαρακτηριστικό *Affected States*

**Input:** *selCVE* ∈ *listCVE*
*selNOS* ∈ *listPLACES*
**Output:** *listCVE* ⊂ *CVE_choices[CVE_ID]*
*listPLACES* ⊂ Places (PN) in model
value for [*NofStates*] in *CVE_choices* table

1: **for each** *selNOS* ∈ *listPLACES* **do**
2: *csNOS* ← **count** *selNOS*
3: **for each** *CVE_ID* ∈ *CVE_choices[]* **do**
4: **if** *CVE_ID* = *selCVE* **then**
5: **update** record [*NofStates*] ← *csNOS*

- **Διαδικασία αξιολόγησης**

  Ο πυρήνας της διαδικασίας αξιολόγησης ενεργοποιείται με τις επιλογές *SM(0)* και *SM(t)* (Αλγόριθμος 9). Και οι δύο επιλογές καλούν την εκτέλεση του κώδικα που απαιτείται για την υλοποίηση της διαδικασίας που περιγράφηκε προηγουμένως

**Αλγόριθμος 9** Ιδιοχαρακτηριστικά *SM(0)* και *SM(t)*

**Input:** records [*CVE_ID*, *CVSS_Base*, *CVSS_Temporal*, *NofStates*] in *CVE_choices* table
**Output:** *CVE_choices* table
*sm0_tag* on *Model SM(0)* attribute
*smt_tag* on *Model SM(t)* attribute

1: **if** *SM(0)* **then**
2: **for each** record ∈ *CVE_choices[]* **do**
3: **compute** $R_n$, $P_n$ and *SM(0)* values
4: **update** record [*Rn*, *Pn*, *SM(0)*] ← ($R_n$, $P_n$, *SM(0)*)
5: **update** *sm0_tag* ← *SM(0)*
6: **else if** *SM(t)* **then**
7: **for each** record ∈ *CVE_choices[]* **do**
8: **compute** $R_n$, $P_n$ and *SM(t)* values
9: **update** record [*Rn*, *Pn*, *SM(t)*] ← ($R_n$, $P_n$, *SM(t)*)
10: **update** *smt_tag* ← *SM(t)*

σε αυτό το κεφάλαιο και καταλήγουν στον υπολογισμό των μετρικών ασφάλειας *SM(0)* και *SM(t)*, αντίστοιχα. Η μαθηματική διαδικασία εκτελείται με βάση τις επιλογές του μηχανικού σχετικά με τις ευπάθειες και τις επηρεαζόμενες καταστάσεις του μοντέλου. Επομένως, αυτές οι επιλογές θα πρέπει να είναι οι τελευταίες που θα χρησιμοποιηθούν από τον μηχανικό για την ολοκλήρωση της αξιολόγησης της ασφάλειας του μοντέλου.

Η κλάση *Security Assessment* συμπληρώνει την κλάση *CVSS* και παρέχει στον μηχανικό ένα σύνολο εργαλείων για την αξιολόγηση του μοντέλου σε θέματα ασφάλειας. Αυτή η κλάση επιτρέπει στον μηχανικό:

*(α)* να τροποποιεί εν μέρει ή πλήρως τη λίστα, σε οποιοδήποτε σημείο της διαδικασίας σχεδιασμού,

*(β)* να επιλέγει εύκολα και γρήγορα τον αριθμό των καταστάσεων μοντέλου που επηρεάζονται από κάθε ευπάθεια υπό μελέτη, και

*(γ)* να υπολογίζει τις μετρικές ασφάλειας του μοντέλου γρήγορα και με ακρίβεια για τις επιλεγμένες ευπάθειες.

Αυτά τα χαρακτηριστικά κάνουν τη διαδικασία της αξιολόγησης της ασφάλειας ταχύτερη, ακριβέστερη και επιτρέπουν στον μηχανικό να ζητά την ενημέρωσή τους γρήγορα και σωστά μετά από οποιαδήποτε αλλαγή στο μοντέλο ή στη λίστα των επιλεγμένων ευπαθειών.

## 4.3 Μοντελοποίηση και αξιολόγηση της iBuC

Σε αυτήν την ενότητα, περιγράφεται η εφαρμογή της μεθόδου αξιολόγησης της ασφάλειας με δύο τρόπους:

*(α)* με τη χρήση του μαθηματικού μοντέλου και των εξισώσεων που παρουσιάστηκαν, και

*(β)* με τη χρήση της πλατφόρμας μοντελοποίησης και αξιολόγησης της ασφάλειας SAPnet.

Για την περιπτωσιακή μελέτη χρησιμοποιείται η διαχείριση στόλου της υπηρεσίας iBuC σε δύο σενάρια πραγματικής λειτουργίας. Η διαχείριση στόλου της iBuC και στα δύο σενάρια μοντελοποιείται με βάση τον φορμαλισμό SPN και στη συνέχεια τα δύο παραγόμενα μοντέλα αξιολογούνται ως προς την ασφάλεια.

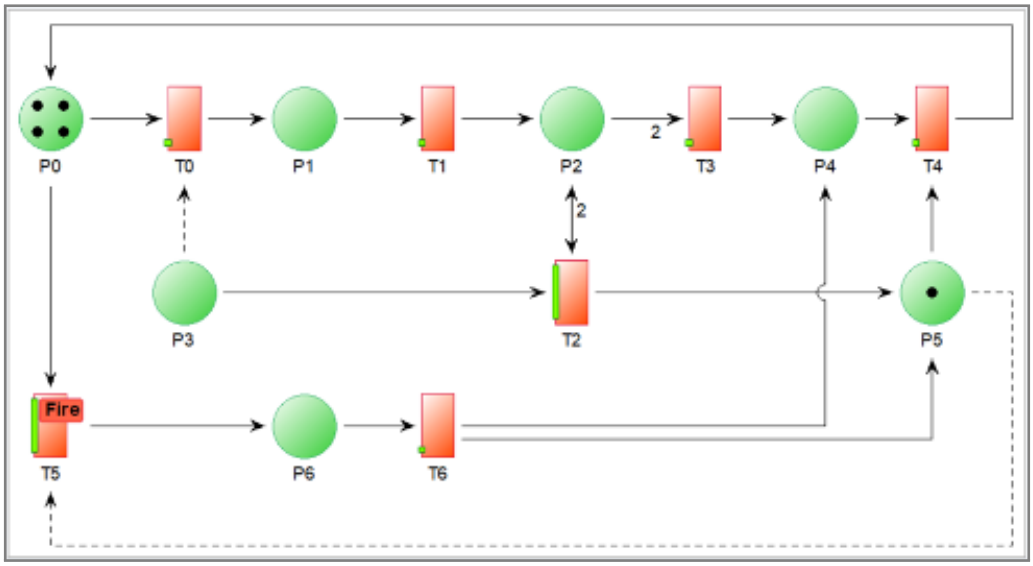
### 4.3.1 Διαλειτουργικότητα και σενάρια λειτουργίας

Η διαχείριση του στόλου της iBuC υλοποιείται λαμβάνοντας υπόψη δύο σενάρια: στο πρώτο σενάριο η iBuC ενσωματώνει τα δεδομένα υπηρεσίας από ένα σύστημα δημοσίων μεταφορών (Public Transportation System, PTS) και στο δεύτερο σενάριο η iBuC ενσωματώνει τα δεδομένα από το πληροφοριακό σύστημα μιας υπηρεσίας πρόγνωσης καιρού (Weather Forecasting Service, WFS).

#### 4.3.1.1 Διαλειτουργικότητα υπηρεσίας iBuC με πληροφοριακό σύστημα δημόσιων μεταφορών

Στην περίπτωση της iBuC-Public Transport Service (iBuC-PTS), οι πληροφορίες που μοιράζεται η iBuC μπορούν να βοηθήσουν στην πρόβλεψη του πλήθους των αναμενόμενων επιβατών στους κόμβους (στάσεις) δημόσιων συγκοινωνιών, που βρίσκονται στην περίμετρο της πανεπιστημιούπολης. Οι πληροφορίες αυτές μπορεί να χρησιμοποιηθούν από το κέντρο ελέγχου των MMM για τον προσαρμοστικό προγραμματισμό διαδρομών των οχημάτων που εξυπηρετούν τις συγκεκριμένες στάσεις. Για τον σκοπό αυτό, η κεντρική μονάδα ελέγχου CU της iBuC στέλνει δεδομένα σε πραγματικό χρόνο σχετικά με την κατάσταση του στόλου στην υπηρεσία PTS.

Οι εισερχόμενες πληροφορίες δρομολογίων από την υπηρεσία PTS χρησιμοποιούνται στη διαδικασία διαχείρισης στόλου της iBuC για τη μείωση του χρόνου αναμονής στις στάσεις των MMM και για την ταυτόχρονη αύξηση του πλήθους των επιβατών που καταφτάνουν σε αυτές εγκαίρως ώστε να εξυπηρετηθούν από διαδρομή της υπηρεσίας PTS. Όταν οι εισερχόμενες πληροφορίες υποδεικνύουν ότι ένα όχημα της υπηρεσίας PTS προσεγγίζει σε δημόσιο κόμβο (Public Node, PN) στην περίμετρο της πανεπιστημιούπολης, η κεντρική μονάδα ελέγχου CU ενεργοποιεί όλα τα AVs για να εκτελέσει το καθένα μια πλήρη διαδρομή, περνώντας από όλους τους κόμβους επιβίβασης (Boarding Node, BN) εντός της πανεπιστημιούπολης και τερματίζοντας στον κόμβο προορισμού (Destination Node, DN) της πανεπιστημιούπολης, που βρίσκεται πιο κοντά στον δημόσιο κόμβο PN. Το μοντέλο SPN στην Εικόνα 5 δείχνει τη διαχείριση στόλου της υπηρεσίας iBuC-PTS.




Εικόνα 5. Μοντέλο της διαχείρισης στόλου της υπηρεσίας iBuC-PTS

Για την εις βάθος κατανόηση του μοντέλου, η σημασία των καταστάσεων (δηλαδή των P0 έως P6) και των μεταβάσεων (δηλαδή των T0 έως T6) φαίνεται στον Πίνακα 3. Οι μάρκες στην κατάσταση P0 αντιπροσωπεύουν τον αριθμό των AVs του στόλου και η μάρκα στην κατάσταση P3 δείχνει ότι έχει υποβληθεί κάποιο αίτημα καταναλωτή. Οι μεταβάσεις T5, T6 και οι καταστάσεις P5, P6 περιγράφουν την ενσωμάτωση δεδομένων του PTS στην υπηρεσία iBuC και τη διαδικασία πλήρους εξυπηρέτησης από τον στόλο οχημάτων AV στην περίπτωση εισερχόμενων πληροφοριών επικείμενου δρομολογίου PTS, πλησίον της πανεπιστημιούπολης.

Πίνακας 3. Καταστάσεις και μεταβάσεις διαχείρισης στόλου

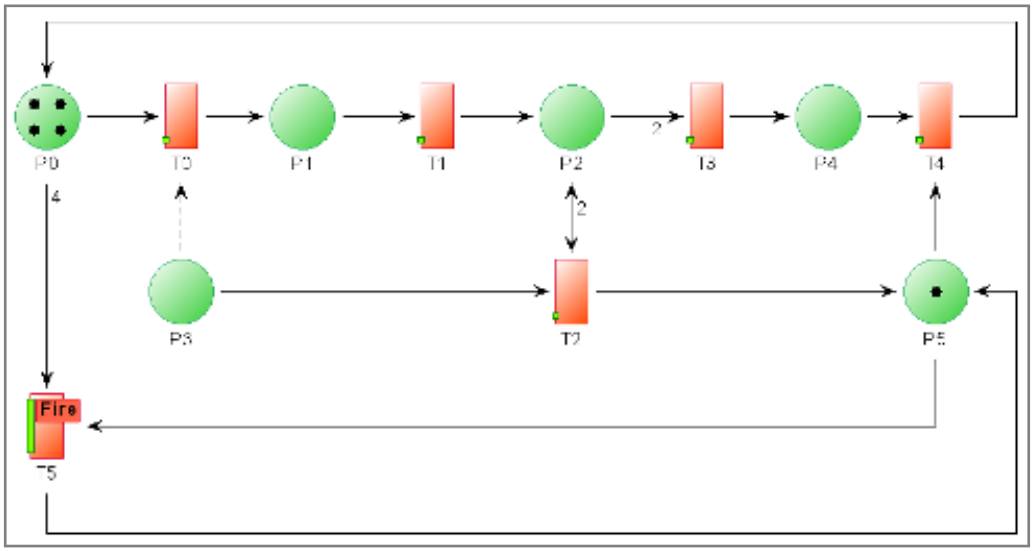
| **Καταστάσεις** | | **Μεταβάσεις** | |
|---|---|---|---|
| P0 | Στόλος σε αναμονή | T0 | CU: έλεγχος διαθεριμότητας στόλου, επιλογή AV |
| P1 | AV: ενεργοποίηση | T1 | CU: αποστολή δεδομένων υπηρεσίας σε AV<br>*(a)* Σταθμός επιβίβασης (BN)<br>*(b)* Ώρα συνάντησης (AT)<br>*(c)* Σταθμός αποβίβασης (DN)<br>*(d)* Δεδομένα επαναδρομολόγησης |
| P2 | AV: άφιξη σε BN | T2 | Επιβάτης: επιβίβαση σε AV |
| P3 | Επιβάτης: αίτηση | T3 | AV: μετάβαση από BN σε DN |
| P4 | AV: άφιξη σε DN | T4 | Επιβάτης: αποβίβαση, AV: στάθμευση/φόρτιση |
| P5 | CU: εισερχόμενη PTS πληροφορία | T5 | CU: έλεγχος διαθεριμότητας στόλου |
| P6 | AV: ενεργοποίηση για πλήρη διαδρομή (όλοι οι σταθμοί είναι BN) | T6 | CU: αποστολή δεδομένων υπηρεσίας σε AV<br>*(a)* Διαδρομή (όλοι οι σταθμοί είναι BN)<br>*(b)* Προκαθορισμένος σταθμός αποβίβασης DN |

#### 4.3.1.2 Διαλειτουργικότητα υπηρεσίας iBuC με πληροφοριακό σύστημα πρόγνωσης καιρού

Στην περίπτωση της υπηρεσίας iBuC-Weather Forecasting Service (iBuC-WFS), χρησιμοποιούνται περιβαλλοντικές μετρικές από τον χώρο της πανεπιστημιούπολης, οι οποίες μπορούν να βοηθήσουν στην παρακολούθηση του μικροκλίματος για τη βέλτιστη διαχείριση του στόλου υπό ειδικές καιρικές συνθήκες. Για τον σκοπό αυτό, η κεντρική μονάδα ελέγχου CU στέλνει σε πραγματικό χρόνο περιβαλλοντικές πληροφορίες που συλλέγονται από τους αισθητήρες των AVs.

Μια εισερχόμενη ειδοποίηση WFS για ακραία καιρικά φαινόμενα χρησιμοποιείται στη διαχείριση του στόλου για την ολοκλήρωση οποιωνδήποτε διαδρομών βρίσκονται σε εξέλιξη και, στη συνέχεια, για την αναστολή της υπηρεσίας, εάν και για όσο χρόνο αυτό κριθεί απαραίτητο.

Η διαχείριση του στόλου με την ενσωμάτωση δεδομένων από την τριτομερή υπηρεσία WFS, φαίνεται στην Εικόνα 6, όπου η μετάβαση T5 και η κατάσταση P5 περιγράφουν την ενσωμάτωση δεδομένων της WFS και την αναστολή της υπηρεσίας iBuC στην περίπτωση εισερχόμενων ειδοποιήσεων σχετικά με ακραία καιρικά φαινόμενα από την WFS.




Εικόνα 6. Μοντέλο της διαχείρισης στόλου της υπηρεσίας iBuC-WFS

Η μοντελοποίηση της υπηρεσίας iBuC σύμφωνα με τα δύο παραπάνω σενάρια δείχνει ότι η διαδικασία διαχείρισης στόλου αλλάζει ανάλογα με τη φύση των ενσωματωμένων δεδομένων της τριτομερούς υπηρεσίας. Αυτή η διαφοροποίηση μπορεί επίσης να επηρεάσει άλλες πτυχές της υπηρεσίας, όπως η ασφάλεια. Αυτές οι αλλαγές της υπηρεσίας θα αξιολογηθούν στις επόμενες ενότητες.

### 4.3.2 Εφαρμογή της μεθόδου μοντελοποίησης και αξιολόγησης

Τα θέματα ασφάλειας της υπηρεσίας iBuC εξαρτώνται από τις αδυναμίες (weaknesses) που φέρουν η κεντρική μονάδα ελέγχου CU, ο στόλος των οχημάτων AV και οι καταναλωτές/επιβάτες της υπηρεσίας, δηλαδή οι αδυναμίες της έξυπνης συσκευής τους ή της εφαρμογής επιβατών της υπηρεσίας. Η κεντρική μονάδα ελέγχου CU κληρονομεί

τις ευπάθειες (vulnerabilities) του λειτουργικού συστήματός της, του υλικού και του λογισμικού των υποσυστημάτων της. Επιπλέον, δεδομένου ότι τα AVs είναι εξοπλισμένα με αισθητήρες, μικροελεγκτές, διεπαφές επικοινωνίας και πομποδέκτες για την επίτευξη αυτόνομης πλοήγησης εφαρμόζοντας λειτουργίες όπως η αποφυγή εμποδίων, αυτές οι συσκευές και το λογισμικό υποστήριξής τους έχουν τις δικές τους ευπάθειες. Καθώς ο καταναλωτής/επιβάτης χρησιμοποιεί κάποια συσκευή για να αλληλεπιδρά με τα στοιχεία της υπηρεσίας iBuC, θα πρέπει να ληφθούν υπόψη οι ευπάθειες και αυτής της συσκευής. Η τελική επιλογή των συναφών ευπαθειών της iBuC γίνεται λαμβάνοντας υπόψη τις επιμέρους ευπάθειες όλων των προαναφερθέντων στοιχείων.

Το μοντέλο SPN της διαχείρισης στόλου της υπηρεσίας iBuC-PTS έχει περισσότερες καταστάσεις και μεταβάσεις σε σύγκριση με το αντίστοιχο της υπηρεσίας iBuC-WFS. Για τον λόγο αυτό, η διαδικασία αξιολόγησης της ασφάλειας διεξάγεται χωριστά για τα μοντέλα iBuC-PTS και iBuC-WFS.

Η αξιολόγηση της ασφάλειας εστιάζει στις πιο συναφείς και επιδραστικές αδυναμίες, όπως αυτές περιγράφονται σύμφωνα με την CVSS βαθμολόγησή τους. Επίσης, για κάθε αδυναμία, επιλέγουμε την πιο κρίσιμη και συναφή ευπάθεια από τη βάση δεδομένων CVE [70]. Στη βάση δεδομένων CVE και, κατά συνέπεια, στη λίστα CVE, κάθε ευπάθεια χαρακτηρίζεται από ένα μοναδικό CVEID και έχει μετρικές που αντικατοπτρίζουν τη δυνατότητα εκμετάλλευσης και τον αντίκτυπο της ευπάθειας [52], όπως φαίνεται στον Πίνακα 4.

Πίνακας 4. Λίστα CVE ευπαθειών υπηρεσίας iBuC

| **CVE** | **Description** | **CVSS** | |
|---|---|---|---|
| | | Base | Temporal |
| CVE-2017-7214 | Information Exposure | 9.8 | 9.1 |
| CVE-2018-4878 | (Resource) Use After Free | 9.8 | 9.1 |
| CVE-2018-8174 | Failure to Constrain Operations | 7.5 | 7.3 |
| CVE-2017-0199 | Access Control (Authorization) Issues | 7.8 | 6.6 |
| CVE-2018-7600 | Improper Input Validation | 9.8 | 8.5 |
| CVE-2018-12942 | OS Command Injection | 8.8 | 8.1 |
| CVE-2018-14643 | Improper Authentication | 9.8 | 8.8 |
| CVE-2018-10635 | Missing Critical Function Authentication | 9.8 | 7.9 |
| CVE-2016-6829 | Use of Hard-coded Credentials | 9.8 | 8.7 |
| CVE-2016-5788 | Improper Authorisation | 10 | 8.3 |
| CVE-2016-5062 | Incorrect Resource Transfer | 9.8 | 8.3 |
| CVE-2016-8209 | Improper Check | 7.5 | 6.6 |
| CVE-2017-5239 | Inadequate Encryption Strength | 7.5 | 7.1 |
| CVE-2017-17717 | Broken Cryptographic Algorithm | 9.8 | 9.3 |
| CVE-2017-7901 | Use of Insufficiently Random Values | 8.6 | 7.6 |
| CVE-2017-18146 | Improper Crypto Verification | 9.8 | 8.5 |
| CVE-2016-5069 | Insufficient Session Expiration | 9.8 | 9.1 |
| CVE-2016-7124 | Deserialization of Untrusted Data | 9.8 | 8.5 |
| CVE-2018-12689 | LDAP Injection | 9.8 | 9.3 |

Το ινστιτούτο NIST [52] παρέχει αναφορές σε συμβουλές, λύσεις και εργαλεία, εάν αυτά είναι διαθέσιμα, για την αντιμετώπιση ή μετριασμό κάθε ευπάθειας. Εφαρμόζοντας τις ενημερώσεις κώδικα ή τις διορθώσεις που προτείνονται ή διατίθενται, η *βασική βαθμολογία CVSS (CVSS Base Score)* της ευπάθειας αλλάζει σε *χρονική βαθμολογία CVSS (CVSS Temporal Score)*. Σε περίπτωση που δεν υπάρχει ενημέρωση κώδικα ή επιδιόρθωση, η χρονική βαθμολογία CVSS είναι ίση με τη βασική βαθμολογία CVSS. Ο Πίνακας 5 δείχνει τη λίστα CVE υπό μελέτη και την αξιολόγηση της ασφάλειας των μοντέλων iBuC-PTS και iBuC-WFS, πριν και μετά τον μετριασμό των ευπαθειών τους.

Πίνακας 5. Επηρεαζόμενες καταστάσεις και μετρικές ασφάλειας υπηρεσίας iBuC

| **CVE** | **Affected States** | **iBuC-PTS** | | | | | **iBuC-WFS** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | Rn | Pn | SM(0) | SM(t) | A | Rn | Pn | SM(0) | SM(t) |
| CVE-2017-7214 | P0,P1,P2,P3,P4,P5,P6 | 7 | 0.14 | 0.04 | 0.34 | 0.32 | 6 | 0.17 | 0.03 | 0.32 | 0.29 |
| CVE-2018-4878 | P1,P2,P3,P5 | 4 | 0.25 | 0.06 | 0.60 | 0.56 | 4 | 0.25 | 0.05 | 0.47 | 0.44 |
| CVE-2018-8174 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.05 | 0.37 | 0.36 | 4 | 0.25 | 0.05 | 0.36 | 0.35 |
| CVE-2017-0199 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.05 | 0.38 | 0.32 | 4 | 0.25 | 0.05 | 0.38 | 0.32 |
| CVE-2018-7600 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.05 | 0.48 | 0.42 | 4 | 0.25 | 0.05 | 0.47 | 0.41 |
| CVE-2018-12942 | P0,P1,P2,P3,P4,P5,P6 | 7 | 0.14 | 0.04 | 0.31 | 0.28 | 6 | 0.17 | 0.03 | 0.28 | 0.26 |
| CVE-2018-14643 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.04 | 0.40 | 0.36 | 5 | 0.20 | 0.04 | 0.38 | 0.34 |
| CVE-2018-10635 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.04 | 0.40 | 0.32 | 5 | 0.20 | 0.04 | 0.38 | 0.31 |
| CVE-2016-6829 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.04 | 0.40 | 0.36 | 5 | 0.20 | 0.04 | 0.38 | 0.34 |
| CVE-2016-5788 | P1,P5,P6 | 3 | 0.33 | 0.08 | 0.82 | 0.68 | 2 | 0.50 | 0.10 | 0.97 | 0.80 |
| CVE-2016-5062 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.05 | 0.48 | 0.41 | 4 | 0.25 | 0.05 | 0.47 | 0.40 |
| CVE-2016-8209 | P1,P5,P6 | 3 | 0.33 | 0.08 | 0.61 | 0.54 | 2 | 0.50 | 0.10 | 0.73 | 0.64 |
| CVE-2017-5239 | P0,P1,P3,P6 | 4 | 0.25 | 0.06 | 0.46 | 0.44 | 3 | 0.33 | 0.06 | 0.48 | 0.46 |
| CVE-2017-17717 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.05 | 0.48 | 0.46 | 4 | 0.25 | 0.05 | 0.47 | 0.45 |
| CVE-2017-7901 | P1,P5,P6 | 3 | 0.33 | 0.08 | 0.70 | 0.62 | 2 | 0.50 | 0.10 | 0.83 | 0.74 |
| CVE-2017-18146 | P1,P2,P3,P5 | 4 | 0.25 | 0.06 | 0.60 | 0.52 | 4 | 0.25 | 0.05 | 0.47 | 0.41 |
| CVE-2016-5069 | P0,P1,P2,P4,P6 | 5 | 0.20 | 0.05 | 0.48 | 0.45 | 4 | 0.25 | 0.05 | 0.47 | 0.44 |
| CVE-2016-7124 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.04 | 0.40 | 0.35 | 5 | 0.20 | 0.04 | 0.38 | 0.33 |
| CVE-2018-12689 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.04 | 0.40 | 0.38 | 5 | 0.20 | 0.04 | 0.38 | 0.36 |
| **TOTALS** | | | | | **9.14** | **8.15** | | | | **9.09** | **8.09** |

Στη συνέχεια απαιτείται μια αντιστοίχιση μεταξύ της λίστας αδυναμιών και των καταστάσεων των δύο μοντέλων, με βάση τα στοιχεία (υλικό ή λογισμικό) που εμπλέκονται σε κάθε κατάσταση. Θα πρέπει να σημειωθεί ότι η διαφορά στο πλήθος των επηρεαζόμενων καταστάσεων στα δύο μοντέλα για κάποιες ευπάθειες, καθώς και συνολικά, οφείλεται στην ύπαρξη της κατάστασης P6, η οποία υπάρχει μόνο στο μοντέλο iBuC-PTS.

Το πλήθος των καταστάσεων (δηλαδή οι τιμές στον Πίνακα 5, στις στήλες *A*) χρησιμοποιείται για τον υπολογισμό της μετρικής ασφάλειας *SM(0)* για την υπηρεσία iBuC και για όλες τις αδυναμίες της. Η διαδικασία υπολογισμού περιγράφεται από τις εξισώσεις (4.1) – (4.4). Το *SM(t)* αντιπροσωπεύει τη μετρική ασφάλειας της υπηρεσίας μετά τον μετριασμό, λαμβάνοντας υπόψη τη χρονική αντί της βασικής βαθμολογίας CVSS των ευπαθειών.

Παρόλο που η μετρική *SM(0)* διαφοροποιείται στα δύο μοντέλα, η απόκλιση είναι μικρή. Αυτό συμβαίνει επειδή οι καταστάσεις των δύο μοντέλων δεν έχουν μεγάλες αποκλίσεις σε πλήθος ή σε εμπλεκόμενα στοιχεία ανά κατάσταση (δρώντες, υλικό, λογισμικό). Τα

δύο μοντέλα διαφοροποιούνται κυρίως στο πλήθος και στη φύση των μεταβάσεων και όχι των καταστάσεων. Γενικότερα, η δυναμική προσαρμογή της διαχείρισης στόλου της iBuC στην ενσωμάτωση δεδομένων της τριτομερούς υπηρεσίας επηρεάζει την ασφάλεια μόνο όσο και όταν προκύπτουν πρόσθετες καταστάσεις για την υπηρεσία.

Πίνακας 6. Μετρικές ασφάλειας *(α)* iBuC-PTS και *(β)* iBuC-WFS

| **Μετρικές** | ***(α)*** | ***(β)*** | ***(α)-(β)%*** |
|---|---|---|---|
| Βασική SM(0) | 9.14 | 9.09 | +0.55% |
| Χρονική SM(t) | 8.15 | 8.09 | +0.70% |

Στον Πίνακα 6 αντιπαραβάλονται οι μετρικές ασφάλειας (βασική και χρονική) των δύο σεναρίων iBuC-PTS και iBuC-WFS. Διαπιστώνεται το αναμενόμενο, δηλαδή πως μετά τον μετριασμό, η μετρική ασφάλειας *SM(t)* για το iBuC-PTS μειώνεται σε 8.15 σε σύγκριση με τη μετρική *SM(0)* πριν από τον μετριασμό, η οποία έχει την τιμή 9.14. Το ίδιο συμβαίνει και για το iBuC-WFS, όπου η μετρική *SM(t)* μειώνεται στο 8.09 σε σύγκριση με την τιμή *SM(0)* του 9.09, προ του μετριασμού. Και στις δύο περιπτώσεις, το *SM(t)* έχει μικρότερη τιμή από το *SM(0)*, υποδεικνύοντας ότι το επίπεδο ασφάλειας της υπηρεσίας βελτιώνεται. Ωστόσο, η διαφορά της τιμής *SM(t)* στις δύο περιπτώσεις είναι συνυφασμένη με την ύπαρξη πρόσθετων καταστάσεων στο μοντέλο iBuC-PTS, καθώς και με τον διαφορετικό βαθμό μετριασμού των ευπαθειών που επηρεάζουν αυτές τις πρόσθετες καταστάσεις. Αποδεικνύεται πως αυτή η διαφορά καταστάσεων στα δύο μοντέλα αλλάζει τις μετρικές ασφάλειας, με αυτές του μοντέλου iBuC-PTS να είναι υψηλότερες κατά 0.55% - 0.70%. Ως εκ τούτου, η δυναμική προσαρμογή της iBuC επηρεάζει και την ασφάλειά της, εάν οι πρόσθετες καταστάσεις που σχετίζονται με την τριτομερή υπηρεσία επηρεάζονται από κρίσιμες ευπάθειες, δηλαδή:

*(α)* ευπάθειες με υψηλή βασική βαθμολογία CVSS,

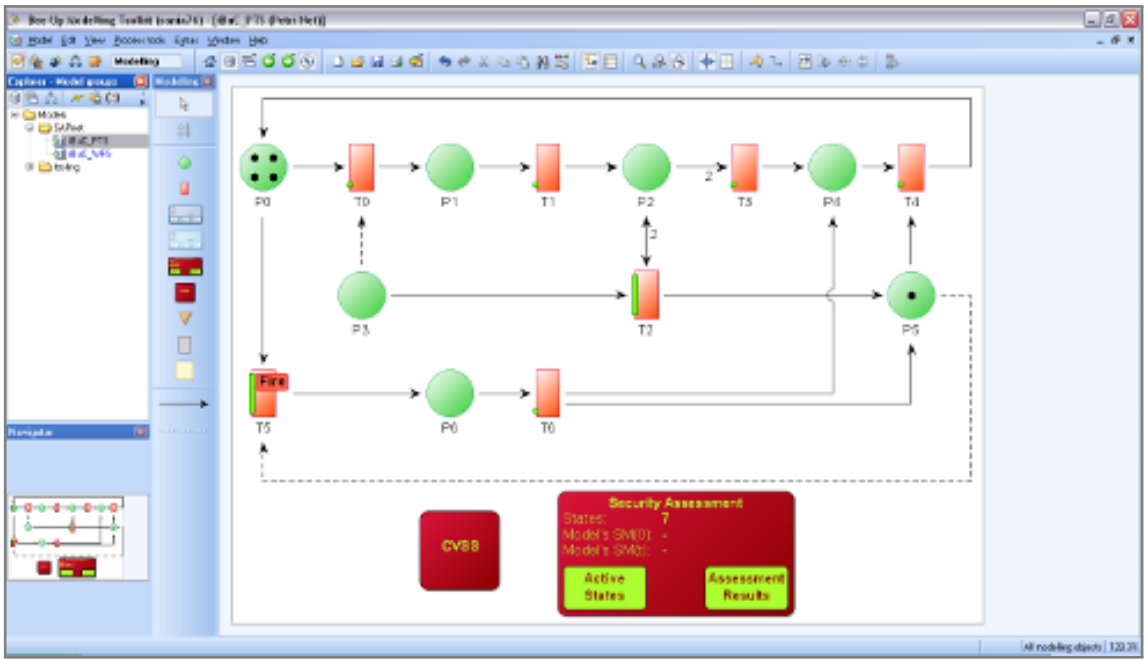
*(β)* ευπάθειες με δυνατότητα μετριασμού σε σεβαστό ποσοστό (μεγάλη απόκλιση μεταξύ βασικής και χρονικής βαθμολογίας CVSS), και

*(γ)* ευπάθειες των δρώντων που συμμετέχουν σε πολλές καταστάσεις της υπηρεσίας.

### 4.3.3 Χρήση της πλατφόρμας SAPnet

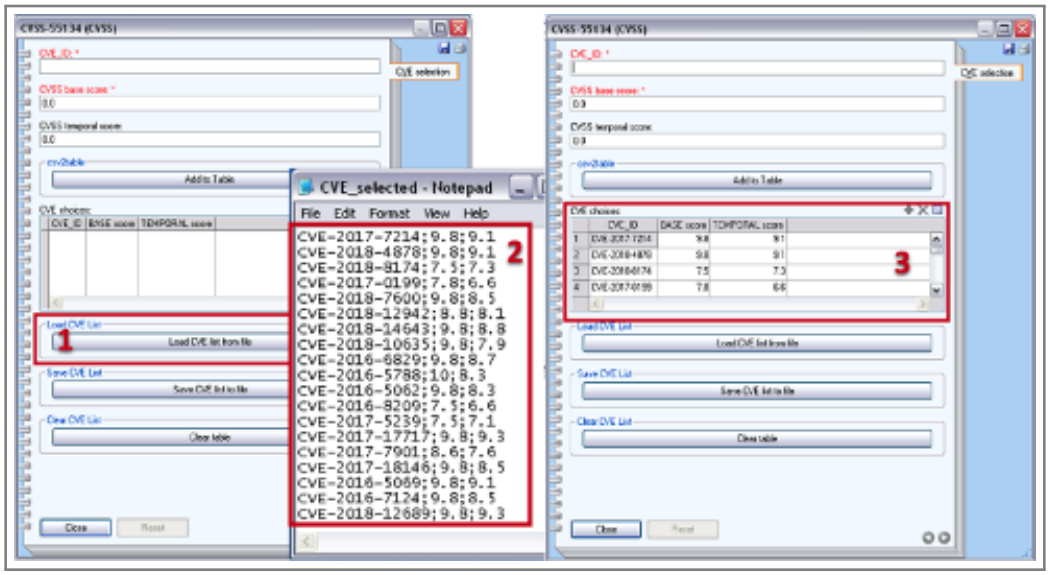
Η ίδια διαδικασία αξιολόγησης για τα δύο μοντέλα της διαχείρισης στόλου με ενσωμάτωση δεδομένων από τριτομερή υπηρεσία, το iBuC-PTS και το iBuC-WFS, πραγματοποιείται χρησιμοποιώντας την πλατφόρμα μοντελοποίησης και αξιολόγησης SAPnet. Η SAPnet χρησιμοποιείται για τη δημιουργία των δύο μοντέλων χρησιμοποιώντας τον φορμαλισμό SPN. Επιπλέον, τα σημασιολογικά στοιχεία *CVSS (PN)* και *Security Assessment (PN)* τοποθετούνται στην περιοχή σχεδίασης και των δύο μοντέλων, ώστε να μπορούν να ενεργοποιηθούν και να διατεθούν για χρήση (Εικόνα 7).

Για λόγους σύγκρισης, η υπό μελέτη λίστα των ευπαθειών διατηρείται ίδια με αυτήν που χρησιμοποιήθηκε στη θεωρητική προσέγγιση. Η λίστα έχει ήδη κατασκευαστεί κατά τη διαδικασία της θεωρητικής αξιολόγησης και αποθηκεύτηκε σε οριοθετημένο αρχείο. Η SAPnet υποστηρίζει τη δυνατότητα εισαγωγής μιας λίστας απευθείας από ένα αρχείο, μια




Εικόνα 7. Σχεδίαση και κλάσεις *CVSS* και *Security Assessment*

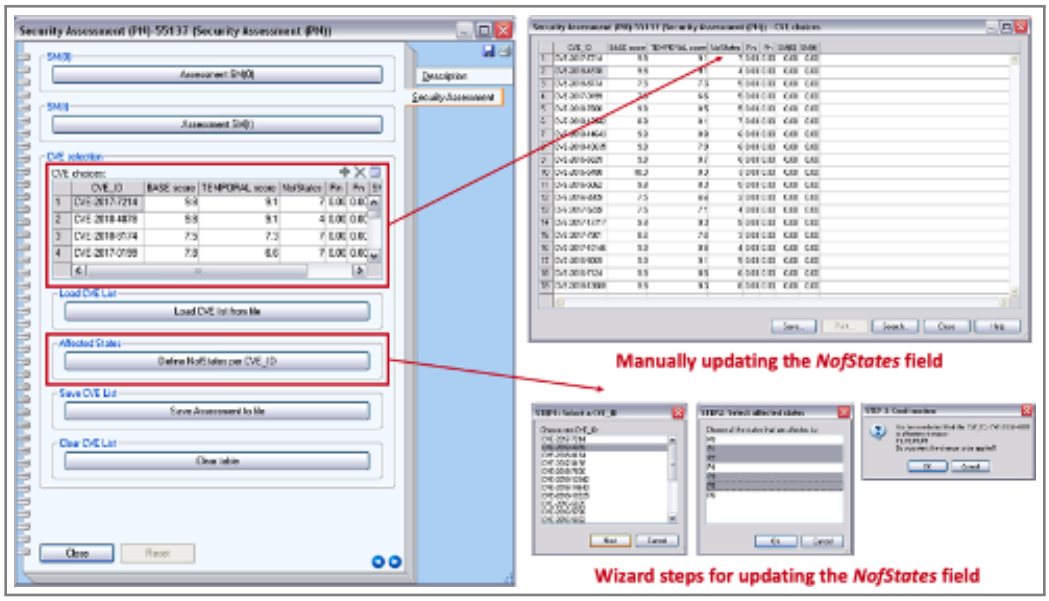
επιλογή που παρέχεται από την κλάση *CVSS*. Η Εικόνα 8 δείχνει τα βήματα που έγιναν για την εισαγωγή της λίστας.



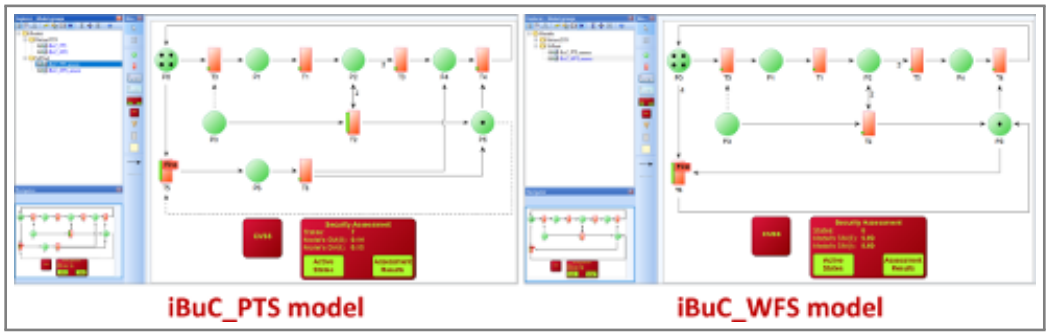

Εικόνα 8. Εισαγωγή λίστας ευπαθειών με την κλάση *CVSS*

Το επόμενο βήμα είναι ο συσχετισμός του πλήθους των καταστάσεων του μοντέλου, που επηρεάζονται από την κάθε ευπάθεια. Ο συσχετισμός αυτός γίνεται για κάθε εγγραφή της λίστας ευπαθειών. Όπως συζητήθηκε στη θεωρητική προσέγγιση της αξιολόγησης, το ποσοστό των καταστάσεων του μοντέλου που επηρεάζονται συνολικά είναι ένας παράγοντας της μετρικής ασφάλειας του μοντέλου. Η κλάση *Security Assessment* επιτρέπει στον μηχανικό να ενημερώσει τη λίστα των ευπαθειών με τον αριθμό των επηρεαζόμενων καταστάσεων ανά ευπάθεια, στο πεδίο *NofStates*. Η ενημέρωση του

πεδίου *NofStates* μπορεί να γίνει χειροκίνητα ή με τη βοήθεια ενός οδηγού που παρέχεται από την κλάση *Security Assessment* (Εικόνα 9).




Εικόνα 9. Ενημέρωση του πεδίου *NofStates* στη λίστα ευπαθειών




Εικόνα 10. Μοντέλα και μετρικές ασφάλειας στην περιοχή σχεδίασης

Ο πυρήνας της διαδικασίας αξιολόγησης της ασφάλειας, που έχει ως αποτέλεσμα τον υπολογισμό των μετρικών ασφάλειας για το μοντέλο, εκτελείται από τον κώδικα των επιλογών *SM(0)* και *SM(t)* στο περιβάλλον της κλάσης *Security Assessment*, που ενεργοποιούνται με τη χρήση των κουμπιών *Assessment SM(0)* και *Assessment SM(t)* αντίστοιχα. Ο υπολογισμός των μετρικών είναι γρήγορος και ακριβής ακόμη και στην περίπτωση ενός σύνθετου μοντέλου ή μιας εξαντλητικής λίστας ευπαθειών. Επιπλέον, το αποτέλεσμα της αξιολόγησης είναι ορατό στην περιοχή σχεδίασης, χάρη στις ιδιότητες της κλάσης *Security Assessment* (Εικόνα 10). Αυτή η δυνατότητα επιτρέπει στον μηχανικό να έχει άμεση παρακολούθηση και επανυπολογισμό των αποτελεσμάτων κατά την αλλαγή, την ενημέρωση ή την επανασχεδίαση του υπό μελέτη μοντέλου.

# Κεφάλαιο 5

# Ασφάλεια δικτύων φόρτισης οχημάτων

## 5.1 Υπηρεσία φόρτισης οχημάτων

Σε μια υπηρεσία μεταφορών βασισμένη στο IoT, η διαχείριση στόλου είναι ο πυρήνας και καθορίζει σε μεγάλο βαθμό την ποιότητα της υπηρεσίας. Επίσης, το επίπεδο ασφάλειας της υπηρεσίας είναι συνυφασμένο με το επίπεδο ασφάλειας της διαχείρισης στόλου και όλων των δρώντων στοιχείων σε αυτήν.

Ωστόσο και η διαχείριση στόλου, με τη σειρά της, επηρεάζεται και καθορίζεται και από άλλες διεργασίες στις οποίες εμπλέκονται όλα τα δρώντα στοιχεία της υπηρεσίας που βασίζεται στο IoT ή μέρος αυτών. Ένα τέτοιο παράδειγμα είναι η υπηρεσία φόρτισης των ηλεκτρικών οχημάτων του στόλου, αν ο στόλος εμπεριέχει τέτοιου τύπου οχήματα, όπως συμβαίνει στην περίπτωση της προτεινόμενης υπηρεσίας iBuC.

Η προτυποποίηση και η ανάπτυξη πρωτοκόλλων για την υπηρεσία φόρτισης ηλεκτρικών οχημάτων EV είναι ένα δυναμικά εξελισσόμενο πεδίο. Στο πλαίσιο αυτό, το Open Charge Point Protocol (OCPP) ξεχωρίζει ως το de facto χρησιμοποιούμενο πρωτόκολλο σε 148 χώρες και στις 6 ηπείρους και υποστηρίζεται από περισσότερους από 65.000 ήδη εγκατεστημένους και λειτουργικούς σταθμούς φόρτισης [10]. Αναφέρεται επίσης ότι περισσότεροι από 40 κατασκευαστές σταθμών φόρτισης ενσωματώνουν το OCPP στα προϊόντα τους [11],[12]. Ωστόσο, πρόκειται για ένα πρωτόκολλο το οποίο παρουσιάστηκε μόλις το 2012 και εμπλουτίστηκε με τις πρώτες δυνατότητες ασφάλειας το 2015. Συνεπώς, η ασφάλεια της υπηρεσίας φόρτισης των ηλεκτρικών οχημάτων του στόλου έχει άμεση επίδραση στη διαχείριση του στόλου και, άρα, συνολικά στην υπηρεσία iBuC. Επίσης, η ασφάλεια της υπηρεσίας φόρτισης των ηλεκτρικών οχημάτων είναι ένα σχετικά νέο ερευνητικό πεδίο, καθώς μελετάται επισταμένα την τελευταία 10ετία.

Έχει αναδειχθεί ήδη πως η αξιολόγηση ασφάλειας μιας υπηρεσίας όπως η iBuC βασίζεται στις αδυναμίες και στις ευπάθειες που σχετίζονται με τα δρώντα στοιχεία της υπηρεσίας. Ακόμα πιο συγκεκριμένα, ο υπολογισμός της μετρικής ασφάλειας της υπηρεσίας προϋποθέτει τον συσχετισμό μεταξύ των δρώντων στοιχείων και των απειλών ασφάλειας που μπορεί αυτά να δεχθούν.

Στο κεφάλαιο αυτό παρατίθενται οι καταγεγραμμένες επιθέσεις κατά των δικτύων φόρτισης ηλεκτρικών οχημάτων EV ή αλλιώς των δικτύων PEV. Επίσης, γίνεται και ο

συσχετισμός της κάθε επίθεσης με τα επιμέρους δρώντα στοιχεία της αρχιτεκτονικής των δικτύων φόρτισης EV, ώστε να είναι δυνατή η αξιολόγηση της ασφάλειας της διεργασίας φόρτισης οχημάτων EV.

Εκτός της περιγραφής της φύσης και του τρόπου εκδήλωσης της κάθε επίθεσης, καταγράφονται και οποιαδήποτε αντίμετρα ή προτάσεις καλής πρακτικής σχετίζονται με την κάθε επίθεση. Και σε αυτή την περίπτωση επισημαίνεται το μέρος των δρώντων στοιχείων της αρχιτεκτονικής που προφυλάσσεται ή έστω λαμβάνεται υπόψιν από την εκάστοτε προτεινόμενη λύση/αντίμετρο. Ακόμα γίνεται ειδική αναφορά στις τεχνικές διαφύλαξης του απορρήτου, στους μηχανισμούς επαλήθευσης της ταυτότητας και εξουσιοδότησης και στους μηχανισμούς ανίχνευσης και εκτροπής που αφορούν στα δίκτυα φόρτισης οχημάτων EV.

Τέλος, καταγράφονται και περιγράφονται αναλυτικά οι ευπάθειες της διεργασίας φόρτισης οχημάτων που σχετίζονται με τα δρώντα στοιχεία της υπηρεσίας iBuC. Βάσει αυτών, επαναξιολογείται η μετρική ασφάλειας της διαχείρισης στόλου των δύο περιπτώσεων που έχουν ήδη παρουσιαστεί, της iBuC-PTS και της iBuC-WFS, με στόχο να αναδειχθεί πώς το επίπεδο ασφάλειας της υπηρεσίας που βασίζεται στο IoT επηρεάζεται περαιτέρω από τα ζητήματα ασφάλειας της υπηρεσίας φόρτισης οχημάτων του στόλου.

### 5.1.1 Αρχιτεκτονική συστήματος φόρτισης ηλεκτρικών οχημάτων

Η αρχιτεκτονική ενός OCPP συστήματος φόρτισης οχημάτων EV, όπως φαίνεται στην Εικόνα 11, περιέχει τις κύριες οντότητες που συνεργάζονται σε έναν κύκλο ζωής της υπηρεσίας φόρτισης. Η αρχιτεκτονική απεικονίζει:

*(α)* όλες τις συσκευές που βρίσκονται στην τοποθεσία φόρτισης, συμπεριλαμβανομένου του οχήματος-καταναλωτή EV ενός στιγμιότυπου της υπηρεσίας,

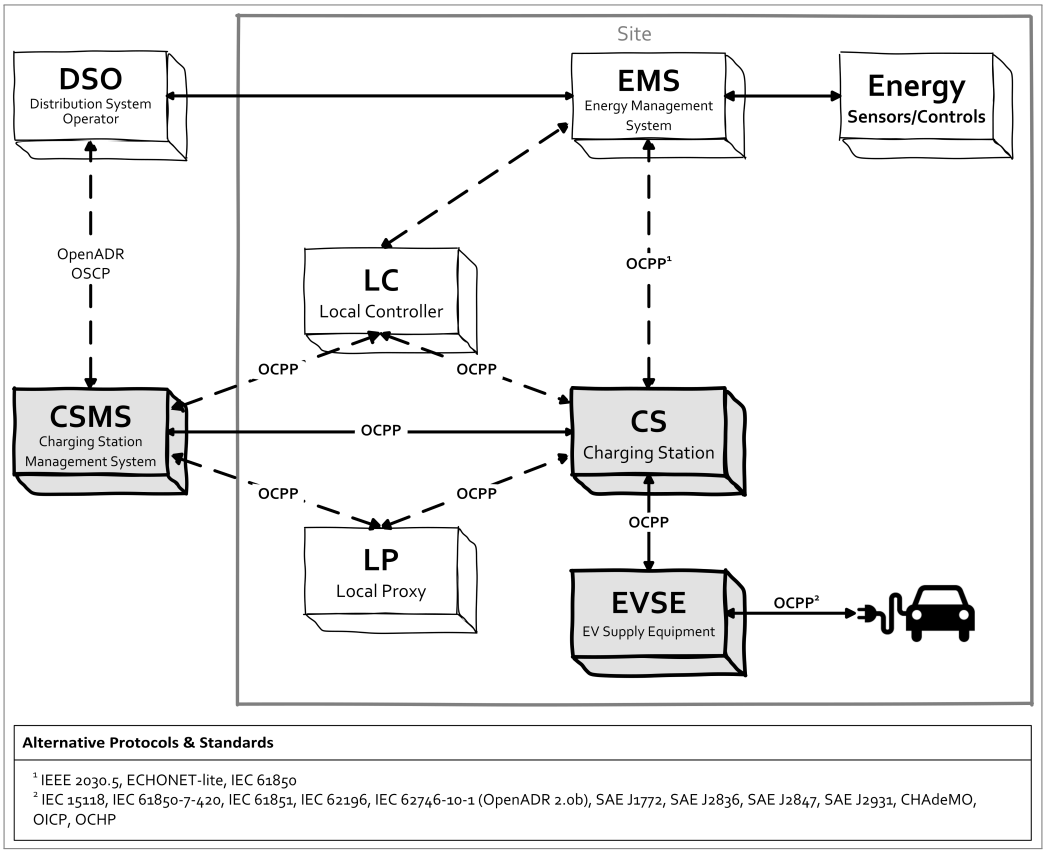
*(β)* το σύστημα διαχείρισης CSMS και τον διαχειριστή διανομής DSO, και

*(γ)* τα πρωτόκολλα ή τα πρότυπα που εφαρμόζονται για την επικοινωνία στοιχείου-προς-στοιχείο της αρχιτεκτονικής.

Αυτή η αρχιτεκτονική βασίζεται στις τοπολογίες που υποστηρίζονται από το OCPP και οι οποίες εισήχθησαν από τον OCA [77].

Κάθε εφαρμογή συστήματος φόρτισης EV μπορεί να ενσωματώνει ορισμένα ή όλα τα στοιχεία που περιγράφονται στην αρχιτεκτονική αναφοράς. Η ελάχιστη υλοποίηση, ωστόσο, απαιτεί τα *κύρια στοιχεία*, δηλαδή ένα σύστημα διαχείρισης CSMS, τουλάχιστον έναν σταθμό φόρτισης CS και τον εξοπλισμό παροχής ηλεκτρικού οχήματος (Electric Vehicle Supply Equipment, EVSE) για τη σύνδεση και τη φόρτιση του οχήματος.

Η ύπαρξη απευθείας επικοινωνίας μεταξύ ορισμένων στοιχείων είναι υποχρεωτική. Σε ορισμένες περιπτώσεις, η επικοινωνία μεταξύ δύο στοιχείων μπορεί να μην είναι σαφής. Για παράδειγμα, εάν η υλοποίηση περιλαμβάνει ένα διαχειριστή διανομής DSO, δηλαδή ένα τριτομερές στοιχείο, αυτή η συμμετοχή πραγματοποιείται με την άμεση επικοινωνία μεταξύ του DSO και του συστήματος διαχείρισης ενέργειας (Energy Management System, EMS). Μπορεί επίσης να υπάρχει επικοινωνία μεταξύ του DSO και του CSMS, εάν αυτό διευκολύνει τόσο το σύστημα χρέωσης του EV όσο και το τρίτο μέρος.




Εικόνα 11. Αρχιτεκτονική αναφοράς του συστήματος φόρτισης ηλεκτρικών οχημάτων

Η λίστα των πρωτοκόλλων και των προτύπων που περιλαμβάνονται στην αρχιτεκτονική περιορίζεται σε αυτά που καθορίζουν την επικοινωνία των *κύριων στοιχείων*, επομένως σε αυτά που ορίζουν τη λειτουργία του πυρήνα ενός συστήματος φόρτισης EV. Το OCPP υποστηρίζει κυρίως την επικοινωνία μεταξύ των τριών αυτών *κύριων στοιχείων*. Αυτό αναλύεται στο ότι τον CS και τον EVSE έχουν μια επικοινωνία που βασίζεται στο OCPP και το ίδιο συμβαίνει μεταξύ του CSMS και του CS, όταν συνδέονται απευθείας ή ακόμα και όταν μεσολαβεί στη μεταξύ τους σύνδεση ένας τοπικός ελεγκτής (LC) ή ένας τοπικός διακομιστής μεσολάβησης (LP). Επιπλέον, το OCPP υποστηρίζει την επικοινωνία μεταξύ:

*(α)* του σταθμού φόρτισης CS και του συστήματος διαχείρισης ενέργειας EMS,

*(β)* του οχήματος EV και του εξολπισμού σύνδεσης EVSE [78].

Θα πρέπει να σημειωθεί ότι το OCPP είναι ένα πρωτόκολλο ζήτησης/απόκρισης που χρησιμοποιείται από συσκευές συνδεδεμένες με IP, που επικοινωνούν βάσει της στοίβας πρωτοκόλλων Transmission Control Protocol/Internet Protocol (TCP/IP). Επομένως, οι λειτουργίες και η ασφάλεια του πρωτοκόλλου OCPP εξαρτώνται από τα στοιχεία της αρχιτεκτονικής, τα λειτουργικά χαρακτηριστικά τους και τη συνδεσιμότητα τους.

### 5.1.2 Στοιχεία της υποδομής φόρτισης

Τα στοιχεία μιας αρχιτεκτονικής συστήματος φόρτισης EV είναι τα ακόλουθα.

#### 5.1.2.1 Εξοπλισμός σύνδεσης/παροχής ηλεκτρικού οχήματος EVSE

Ο εξοπλισμός σύνδεσης Electric Vehicle Supply Equipment (EVSE) είναι το βασικό υποσύστημα ενός σταθμού φόρτισης CS. Ο EVSE παρέχει τη διεπαφή για τη σύνδεση και τη φόρτιση του οχήματος-καταναλωτή. Ο EVSE είναι το σύστημα αιχμής του συστήματος φόρτισης που συλλέγει τα δεδομένα του οχήματος EV σχετικά με τη φόρτιση και την κατάσταση συνδεσιμότητάς του. Το OCPP 2.0 υποστηρίζει την ανταλλαγή δεδομένων μεταξύ του EVSE και του EV κατά τη σύνδεση [79] και παρέχει ένα σύνολο τυπικών μηνυμάτων για την επικοινωνία μεταξύ του EVSE και του συστήματος διαχείρισης CSMS [80].

#### 5.1.2.2 Σταθμός φόρτισης CS

Ο σταθμός φόρτισης (Charging Station, CS) είναι το σύστημα διαχείρισης ενός ή μιας ομάδας σημείων φόρτισης και βρίσκεται εντός μιας περιοχής μικρής εμβέλειας, του χώρου παρεχόμενης φόρτισης. Το σημείο φόρτισης φιλοξενεί τον εξοπλισμό σύνδεσης EVSE και την απόληξη φόρτισης του οχήματος EV. Ο CS ελέγχεται από το σύστημα διαχείρισης CSMS. Το CSMS ορίζει, με τη χρήση μηνυμάτων, τα όρια ισχύος και την κατάσταση λειτουργίας του CS σε όλες τις φάσεις του κύκλου ζωής της υπηρεσίας φόρτισης. Κατόπιν, ο CS τροφοδοτείται με τα παραπάνω μηνύματα και ελέγχει τη διαδικασία φόρτισης των συνδεδεμένων EV, επιβάλλοντας τα θεσπισμένα, από το CSMS, όρια. Το OCPP 2.0 υποστηρίζει τις απαιτήσεις ελέγχου της ταυτότητας, της συναλλαγής και της χρέωσης, οδηγώντας στον καθορισμό των ορίων ανά περίπτωση [81],[82].

#### 5.1.2.3 Τοπικός ελεγκτής LC

Ο τοπικός ελεγκτής ή ελεγκτής (Local Controller, LC) είναι ένας προαιρετικός ελεγκτής για τον έλεγχο ενός ή περισσότερων σταθμών φόρτισης CS. Ο LC παρεμβαίνει και διευκολύνει την επικοινωνία CS-CSMS, ελέγχοντας τα όρια χρέωσης στον CS όταν χάνεται ή διακόπτεται η επικοινωνία CS-CSMS. Η χρήση διάσπαρτων LC σε ένα δίκτυο PEV μπορεί να εφαρμοστεί για την υποστήριξη και τη δημιουργία αντιγράφων ασφάλειας του συστήματος διαχείρισης CSMS και για την κατανομή των διαδικασιών ελέγχου και του υπολογιστικού τους κόστους. Το OCPP υποστηρίζει λειτουργίες για περιπτώσεις χρήσης που περιλαμβάνουν LC. Αυτές οι λειτουργίες βασίζονται στην υπόθεση ότι ένας LC είναι ένας CS, χωρίς EVSE ή οποιοδήποτε άλλο σύνδεσμο [77].

#### 5.1.2.4 Τοπικός πληρεξούσιος LP

Ο τοπικός πληρεξούσιος ή πληρεξούσιος (Local Proxy, LP) είναι μια προαιρετική μονάδα που λειτουργεί ως δρομολογητής. Ο LP χρησιμοποιείται για τη δρομολόγηση μηνυμάτων από και προς έναν ή περισσότερους CS, ειδικά εάν οι CSs δεν έχουν πρόσβαση στο δίκτυο, λόγω της θέσης τους, όπως για παράδειγμα στην περίπτωση που έχουν τοποθετηθεί υπόγεια. Σε μια τέτοια τοπολογία, η δομή του OCPP υπαγορεύει η επικοινωνία CS-LP να γίνεται με τέτοιο τρόπο, ώστε ο LP να λειτουργεί ως CSMS.

#### 5.1.2.5 Σύστημα διαχείρισης σταθμών φόρτισης CSMS

Το σύστημα διαχείρισης (Charging Station Management System, CSMS) είναι ο συντονιστής ενός συστήματος φόρτισης EV. Οι κύριες εργασίες του CSMS [78] είναι οι εξής:

*(α)* η επικοινωνία του με τον CS και τον EVSE,

*(β)* ο καθορισμός των παραμέτρων της υπηρεσίας λαμβάνοντας υπόψη τις επιλογές του οδηγού/χρήστη, τις ανάγκες του EV και την κατάσταση του δικτύου ηλεκτρικής ενέργειας,

*(γ)* η συλλογή και αποθήκευση των δεδομένων του συστήματος φόρτισης,

*(δ)* η φιλοξενία της εφαρμογής χρήστη, και

*(ε)* η διατήρηση ενός μητρώου κρατήσεων για την υπηρεσία.

Το CSMS επικοινωνεί με τα στοιχεία του συστήματος φόρτισης μέσω του OCPP, με εξαίρεση την επικοινωνία του με τον διαχειριστή ενέργειας DSO που διέπεται από άλλα πρότυπα. Το OCPP υποστηρίζει πολιτικές έξυπνης χρέωσης και επιτρέπει στο CSMS να εφαρμόζει προσαρμοσμένα προφίλ για τις διαδικασίες φόρτισης [80].

#### 5.1.2.6 Διαχειριστής (συστήματος) διανομής DSO

Ο διαχειριστής συστήματος διανομής ή διαχειριστής διανομής (Distribution System Operator, DSO) είναι το σύστημα ή ο οργανισμός που είναι υπεύθυνος για τη διανομή της ηλεκτρικής ενέργειας στους τελικούς χρήστες. Ο DSO επιτρέπει ή απαγορεύει τη ροή ισχύος προς την τοποθεσία φόρτισης και, με βάση τα δεδομένα των συνδεδεμένων EVs, διασφαλίζει την ισορροπία και την αποσυμφόρηση στο πλέγμα [83]. Τουλάχιστον ένα σύστημα αιχμής (edge system) του υπεύθυνου για τη διανομή ηλεκτρικής ενέργειας, θεωρείται τριτομερές στοιχείο και μέρος του συστήματος φόρτισης EV. Αυτό το σύστημα αιχμής επηρεάζει έμμεσα τις λειτουργίες του OCPP 2.0, λόγω της τριτομερούς του φύσης. Στο αρχιτεκτονικό σχήμα, ο DSO αντιπροσωπεύει αυτόν τον τριτομερή οργανισμό. Ομοίως, ο οργανισμός ή το φυσικό πρόσωπο που διαχειρίζεται το σύστημα φόρτισης EV, αναφέρεται ως χειριστής σημείου ή σταθμού φόρτισης (Charging System (Point) Operator, CSO ή CPO). Ο CSO δεν απεικονίζεται στην αρχιτεκτονική, θεωρείται, ωστόσο, ότι οι αποφάσεις του λαμβάνονται και εφαρμόζονται από το CSMS.

#### 5.1.2.7 Σύστημα διαχείρισης ενέργειας EMS

Το σύστημα διαχείρισης ενέργειας (Energy Management System, EMS) είναι ένα ενδιάμεσο σύστημα στην επικοινωνία CSMS-CS. Το EMS ελέγχει μια διαδικασία φόρτισης αξιολογώντας ενεργειακά δεδομένα που παρέχονται από το EV-καταναλωτή [30]. Εάν ένα EMS περιλαμβάνεται στο σύστημα φόρτισης EV, η υπηρεσία φόρτισης μπορεί να στηρίζεται στην ηλεκτρική ενέργεια ή σε εναλλακτικές πηγές, όπως ανανεώσιμες πηγές ενέργειας. Αυτές οι εναλλακτικές πηγές ενέργειας αναφέρονται επίσης ως Κατανεμημένοι Ενεργειακοί Πόροι (Distributed Energy Resources, DER). Το OCPP 2.0 υποστηρίζει την επικοινωνία του EMS με τον CS και την αναφορά των ορίων ελέγχου έξυπνης φόρτισης που επιβάλλονται από το πρώτο στον δεύτερο [77].

#### 5.1.2.8 Πάροχος υπηρεσιών ηλεκτρικής κινητικότητας EMSP

Ο ρόλος του παρόχου υπηρεσιών ηλεκτρικής κινητικότητας (E-Mobility Service Provider, EMSP) είναι να διαχειρίζεται τις οικονομικές ρυθμίσεις και τους όρους σχετικά με την υπηρεσία φόρτισης EV. Ο EMSP εκδίδει συμβάσεις ανά EV ή ανά οδηγό EV και διαχειρίζεται τις διαδικασίες χρέωσης. Είναι σύνηθες ότι ο ρόλος του EMSP εκπληρώνεται από τον διαχειριστή διανομής DSO ή από τον χειριστή CSO [41]. Σε κάθε περίπτωση, οι αποφάσεις και διεργασίες του DSO και, όπως έχει προαναφερθεί, αυτές του CSO μπορεί να υλοποιούνται και από το CSMS. Για τον λόγο αυτό, ο EMSP δεν απεικονίζεται στην αρχιτεκτονική αναφοράς.

#### 5.1.2.9 Χρήστης/οδηγός ηλεκτρικού οχήματος EV

Αν και δεν απεικονίζεται στην αρχιτεκτονική αναφοράς, ο χρήστης/οδηγός EV είναι ένας σημαντικός παράγοντας του συστήματος φόρτισης [78]. Οι περισσότερες υλοποιήσεις παρέχουν μια διεπαφή ή διεπιφάνεια χρήστη για τον καθορισμό των παραμέτρων χρέωσης ή για τον ορισμό των κρατήσεων της υπηρεσίας. Ο χρήστης μέσω μιας έξυπνης συσκευής συμμετέχει στη διαμόρφωση της διαδικασίας φόρτισης. Οι ενέργειες του χρήστη, οι ευπάθειες της συσκευής που χρησιμοποιεί για την αλληλεπίδραση με την υπηρεσία και η εφαρμογή χρήστη προσθέτουν δεδομένα και παραμέτρους στην υπηρεσία, επηρεάζοντας έτσι έμμεσα τις λειτουργίες και την ασφάλεια του OCPP. Αξίζει να σημειωθεί ότι πολλές μέθοδοι ασφάλειας για την αναγνώριση/ταυτοποίηση του καταναλωτή βασίζονται στα στοιχεία πιστοποίησης του χρήστη/οδηγού EV.

### 5.1.3 Πρωτόκολλο επικοινωνίας OCPP και κοινή χρήση δεδομένων

Το πρωτόκολλο OCPP ήταν το αποτέλεσμα μιας ιδέας που ξεκίνησε από το ElaadNL, ένα κέντρο γνώσης και καινοτομίας στον τομέα της υποδομής έξυπνης φόρτισης με έδρα στην Ολλανδία. Το ίδρυμα ElaadNL εργάστηκε για την ανάπτυξη ενός ανοικτού πρωτοκόλλου για την υποστήριξη της επικοινωνίας μεταξύ των σημείων φόρτισης και των συστημάτων υποστήριξης. Η πρόταση του ιδρύματος ήταν ότι το OCPP πρέπει να τυποποιηθεί και να πιστοποιηθεί από την OCA, καθώς έτσι θα εξασφαλιστεί η ομοιομορφία και συμβατότητα μεταξύ των κατασκευαστών [84]. Από το 2014, το OCPP ανήκει στην OCA [85].

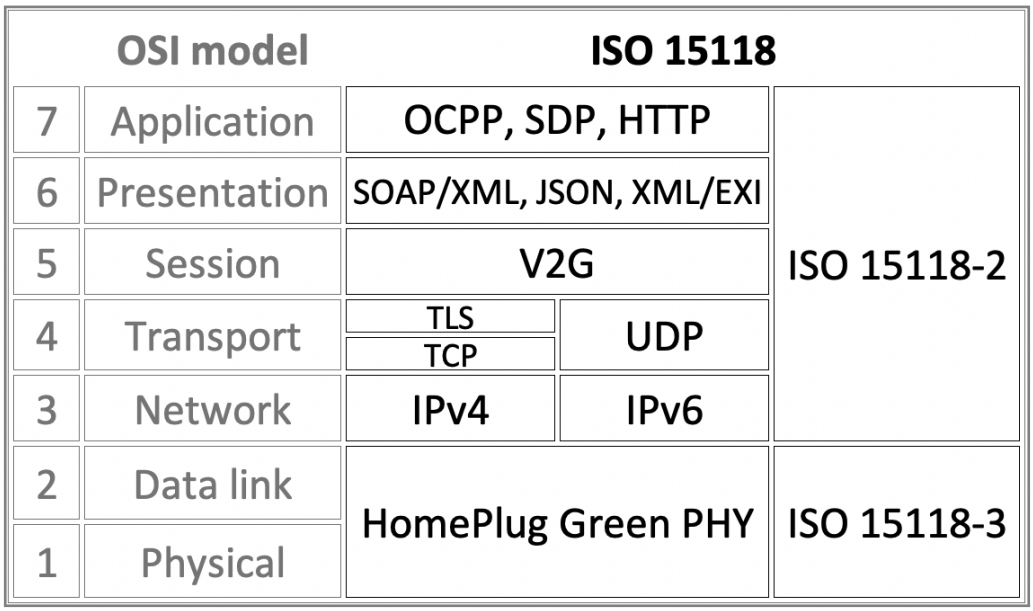
Το OCPP είναι ένα πρωτόκολλο αίτησης/απόκρισης που βασικά παρέχει τα μηνύματα για την επικοινωνία μεταξύ του σταθμού φόρτισης CS και του συστήματος διαχείρισης CSMS, αν και στην πράξη δεν χρησιμοποιείται κατ' αποκλειστικότητα για αυτήν την επικοινωνία. Σε αυτήν την ενότητα, παρουσιάζουμε ένα αρχιτεκτονικό μοντέλο αναφοράς ARM της τοπολογίας ενός δικτύου φόρτισης ηλεκτρικών οχημάτων PEV που υποστηρίζεται από το πρωτόκολλο OCPP, μια σύντομη περιγραφή των κύριων στοιχείων της αρχιτεκτονικής αναφοράς ARM, η παρουσίαση του μοντέλου επικοινωνίας βάσει του πρωτοκόλλου OCPP, η παρουσίαση της διαδικασίας διαχείρισης συναλλαγών ενέργειας και η αναφορά των πρωτοκόλλων και των προτύπων που συνυπάρχουν σε ένα δίκτυο PEV.

Η ανάπτυξη του OCPP ξεκίνησε το 2009 και μέχρι σήμερα έχουν κυκλοφορήσει τέσσερεις εκδόσεις:

- η έκδοση OCPP 1.2 [86] το 2011,
- η έκδοση OCPP 1.5 [86] το 2012,
- η έκδοση OCPP 1.6 [29] το 2015, και
- η έκδοση OCPP 2.0.1 [28] το 2018.

Η τελευταία έκδοση 2.0.1, που αναφέρεται επίσης ως OCPP 2.0 και είναι το επίκεντρο αυτής της έρευνας, έχει βελτιώσεις που παρέχουν το πιο πλήρες, έως τώρα, σύνολο απαρτιζόμενο από 65 μηνύματα αιτήματος/απόκρισης για την επικοινωνία CS-CSMS καθώς επίσης και βελτιωμένες δυνατότητες ασφάλειας. Το OCPP 2.0 υποστηρίζει το πρότυπο ISO 15118 για την επικοινωνία των EVs με τα υπόλοιπα στοιχεία του δικτύου PEV, μέσω του εξοπλισμού EVSE [87]. Το ISO 15118 βελτιώνει το προηγούμενο πρότυπο IEC 61851, εισάγοντας τις λειτουργίες Plug & Charge (PnC) και Smart Charging [88]. Το OCPP υποστηρίζει αυτές τις δύο δυνατότητες [89].

Στο μοντέλο διασύνδεσης Open System Interconnection (OSI) και στο μοντέλο TCP/IP, το OCPP είναι ένα πρωτόκολλο επιπέδου Εφαρμογής. Το OCPP απεικονίζεται στην ενδεικτική λίστα των πρωτοκόλλων συμβατών με το ISO 15118 [87],[88],[90],[91],[92],[93],[94] στην Εικόνα 12. Το πρωτόκολλο Supply Equipment Communication Controller (SECC) Discovery Protocol (SDP) [90] είναι μια εναλλακτική λύση στο πρωτόκολλο επιπέδου Εφαρμογής OCPP. Τα πρωτόκολλα για τα επίπεδα Δικτύου, Μεταφοράς, Συνόδου, Παρουσίασης και Εφαρμογής περιγράφονται στο τμήμα του προτύπου ISO 15118-3 [94], ενώ τα πρωτόκολλα για τα επίπεδα Φυσικό και Ζεύξης Δεδομένων περιγράφονται στο μέρος του προτύπου ISO 15118-2 [87].




Εικόνα 12. Θέση του πρωτοκόλλου OCPP στη στοίβα κατά OSI του προτύπου ISO 15118

Τα OCPP μηνύματα μορφοποιούνται με βάση το πρωτόκολλο Simple Object Access Protocol (SOAP) / Extensible Markup Language (XML). Εναλλακτικά, το πρότυπο

Java-Script Object Notation (JSON) είναι η προτιμώμενη επιλογή για το επίπεδο Παρουσίασης [41], αφού παρέχει μηνύματα μικρότερου μεγέθους και ταχύτερης επεξεργασίας [90].

Οι λειτουργίες στο επίπεδο Συνόδου εκπληρώνονται από το πρωτόκολλο V2G [95]. Το V2G διαχειρίζεται τις διατερματικές συνεδρίες για το αντίστοιχο πρωτόκολλο επιπέδου Εφαρμογής. Στη διαδικασία ενθυλάκωσης, το V2G προσθέτει μια κεφαλίδα μήκους οκτώ (8) bytes στο ωφέλιμο φορτίο, αναφερόμενη και ως κεφαλίδα Vehicle to Grid Transport Protocol (V2GTP). Η V2GTP είναι, φυσικά, το χαρακτηριστικό αναγνώρισης του μηνύματος V2G όταν αυτό μεταφέρεται μέσα σε μια ροή δεδομένων [90].

Η επικοινωνία που βασίζεται στο OCPP υποστηρίζεται από διάφορα πρωτόκολλα στο επίπεδο Μεταφοράς, όπως το TLS, το TCP και το User Datagram Protocol (UDP). Το TLS παρέχει μια ασφαλή διατερματική επικοινωνία μέσω κρυπτογραφημένου καναλιού στο επίπεδο Μεταφοράς και προστατεύει το ωφέλιμο φορτίο του επιπέδου Εφαρμογής [96].

### 5.1.4 Διαχείριση των συναλλαγών ενέργειας

Το OCPP 2.0 συμμορφώνεται με το πρότυπο ISO 15118. Για την πλήρη διαχείριση των συναλλαγών ενέργειας περιλαμβάνει συναφείς δυνατότητες χρέωσης, τιμολόγησης και άλλες. Το πρότυπο ISO 15118 περιγράφει την υπηρεσία δικτύου φόρτισης PEV που υποστηρίζει τη λειτουργία PnC, δηλαδή επιτρέπει τη διατήρηση της επικοινωνίας V2G μέσω της γραμμής ηλεκτρικής τροφοδοσίας του οχήματος.

Σε ένα δίκτυο PEV που βασίζεται στο OCPP, ο σταθμός φόρτισης CS λειτουργεί ως μια πύλη επικοινωνίας μεταξύ του οχήματος EV και των συστημάτων υποστήριξης, όπως το σύστημα διαχείρισης CSMS (Εικόνα 13).

Όσον αφορά στη διαχείριση των συναλλαγών ενέργειας, ο σταθμός φόρτισης CS συλλέγει τις πληροφορίες χρέωσης του συνδεδεμένου οχήματος EV [97]. Η διαχείριση των συναλλαγών ενέργειας του OCPP μπορεί να προσφέρει στον χρήστη/οδηγό EV διάφορες επιλογές, όπως την επιλογή του τρόπου χρέωσης και πληρωμής, την επιλογή ύψιστου ορίου κόστους και λήψη ανάλογης υπηρεσίας και την επιλογή ισοτιμίας νομίσματος [98].

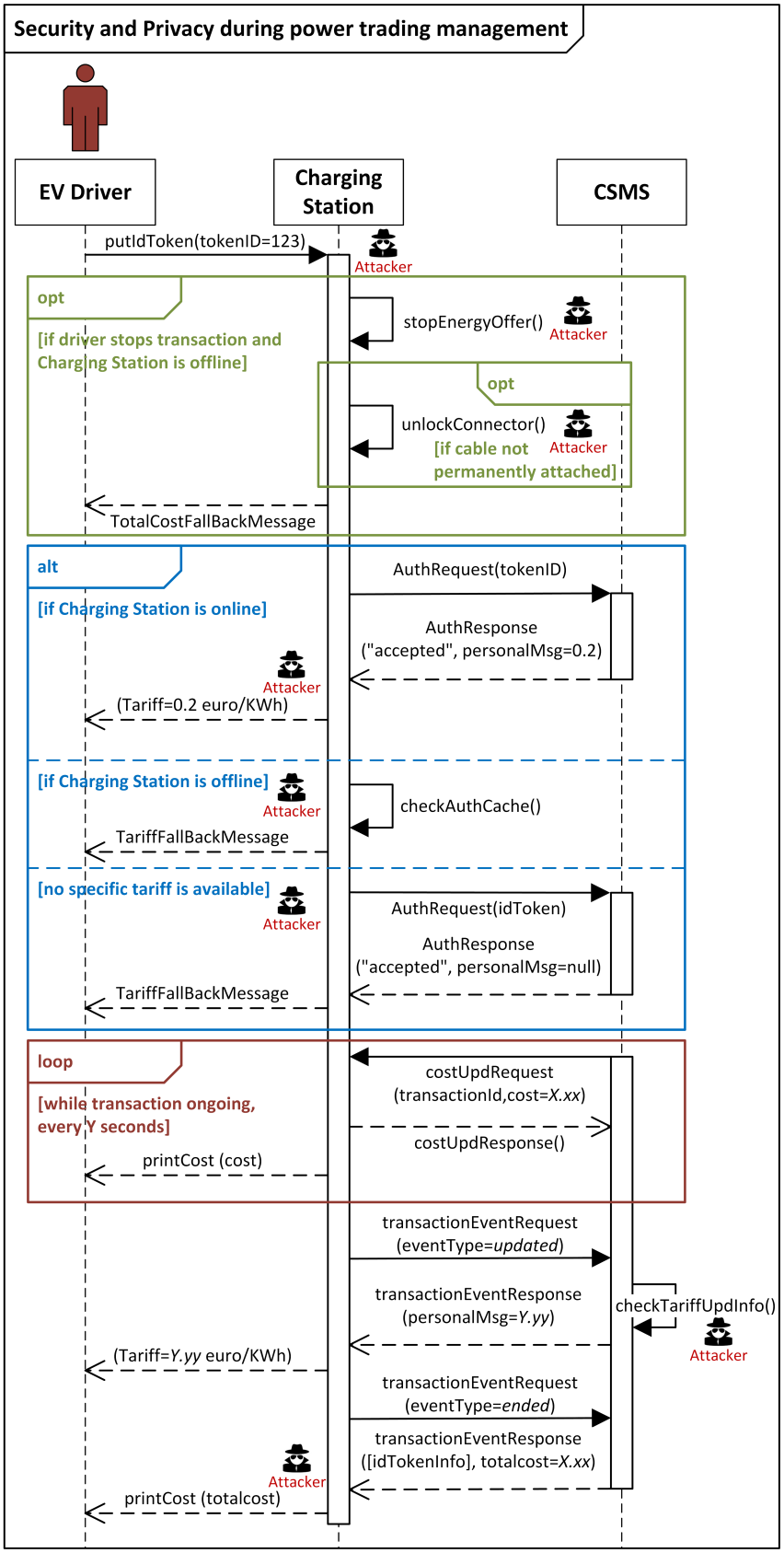
Το OCPP 2.0 είναι η πρώτη έκδοση του πρωτοκόλλου που εισάγει τη λειτουργία υπό το όνομα *TariffAndCost*, ο κώδικας της οποίας περιέχει τα μηνύματα και τους τύπους δεδομένων για τη διαδικασία της συναλλαγής ενέργειας [30]. Σύμφωνα με τις προδιαγραφές του OCPP, αυτή η λειτουργία λαμβάνει υπόψη μια λίστα απαιτήσεων που στοχεύουν στην προστασία:

*(α)* της διαδικασίας χρέωσης,

*(β)* του απορρήτου χρήστη/οδηγού του οχήματος EV (π.χ. του αναγνωριστικού του οδηγού), και

*(γ)* της επικοινωνίας μεταξύ του συστήματος διαχείρισης CSMS και του σταθμού φόρτισης CS.

Το μπλοκ *TariffAndCost* επιτρέπει στο δίκτυο PEV να παρέχει στον χρήστη/οδηγό του οχήματος EV πληροφορίες σχετικά με το κόστος χρέωσης μιας υπηρεσίας φόρτισης πριν



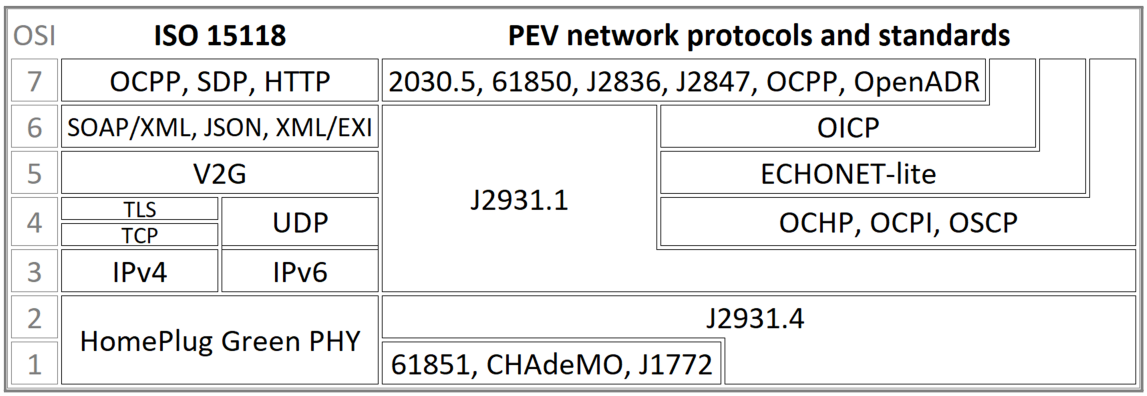

Εικόνα 13. Επικοινωνία κατά τη διαδικασία της συναλλαγής ενέργειας

από την έναρξη της υπηρεσίας, να ενημερώνει το σχετικό τιμολόγιο όταν υπάρχουν αλλαγές στην παρεχόμενη υπηρεσία και να επιβεβαιώνει το κόστος μετά την ολοκλήρωση της υπηρεσίας [89].

Όπως φαίνεται στην Εικόνα 13, οι πληροφορίες χρέωσης που ανταλλάσσονται εντός του δικτύου PEV εγείρουν ορισμένα ζητήματα ασφάλειας και απορρήτου. Η ασφάλεια των δεδομένων που ανταλλάσσονται εξαρτάται από τις λειτουργίες του πρωτοκόλλου και από το επίπεδο προστασίας των δεδομένων χρέωσης κατά την αποθήκευση, καθώς και από τη διατερματική μετάδοσή τους.

### 5.1.5 Πρωτόκολλα και πρότυπα δικτύου φόρτισης PEV

Το OCPP σχεδιάστηκε για να είναι διαλειτουργικό με άλλα πρωτόκολλα εντός του δικτύου PEV. Σε ένα δίκτυο PEV που βασίζεται στο OCPP, κάποιες επιμέρους διατερματικές επικοινωνίες μπορεί να καλύπτονται και από άλλα πρωτόκολλα. Το αποτέλεσμα αυτής της συνύπαρξης άλλων πρωτοκόλλων, ωστόσο, επηρεάζει και τις λειτουργίες του OCPP. Η Εικόνα 14 δείχνει τα πρωτόκολλα και τα πρότυπα που μπορεί να συνυπάρχουν με το OCPP σε ένα δίκτυο PEV. Αυτά τα πρωτόκολλα και τα πρότυπα παρουσιάζονται με αναφορά στη στοίβα πρωτοκόλλων ISO 15118 και στη συνέχεια περιγράφονται κατά τα επίπεδα του de jure μοντέλου του OSI.




Εικόνα 14. Πρότυπα και πρωτόκολλα δικτύου PEV ανά επίπεδο της στοίβας OSI

#### 5.1.5.1 Φυσικό επίπεδο

Το πρότυπο IEC 61851 περιγράφει ένα αγώγιμο σύστημα φόρτισης με εναλλασσόμενο (AC) ή συνεχές ρεύμα (DC). Περιγράφει επίσης τη χρήση του πιλοτικού σήματος ελέγχου [87] για την επικοινωνία EVSE-EV του, συνδεδεμένου στον εξοπλισμό, οχήματος. Πιο συγκεκριμένα, το σήμα πιλότου ελέγχου χρησιμοποιείται για την επαλήθευση της αδιάλειπτης σύνδεσης του οχήματος EV πριν από την έναρξη μετάδοσης δεδομένων καθώς και κατά τη διάρκεια της διαδικασίας φόρτισης. Άξιο αναφοράς είναι πως για την επικοινωνία CS-EMS, το IEC 61851 και το IEC 61850 δεν υποστηρίζουν την αντίστροφη ροή ηλεκτρικού ρεύματος από το όχημα EV στο πλέγμα [8], κάτι που δεν ισχύει για όλα τα υπόλοιπα πρότυπα/πρωτόκολλα που προσδιορίζουν τη συγκεκριμένη επικοινωνία.

Το SAE J1772 περιγράφει την επικοινωνία γρήγορης φόρτισης EVSE-CS [42]. Το J1772 ή Type 1 είναι ένας από τους συνηθισμένους τύπους συνδέσεων που χρησιμοποιούνται

στις Η.Π.Α., με τους άλλους δύο να είναι ο CHAdeMO και ο σύνθετος τύπος Tesla [99]. Η υποδοχή J1772 υποστηρίζει την εκφόρτιση του οχήματος EV με εναλλασσόμενη τάση ρεύματος (Alternating Current, AC), ενώ το CHAdeMO την εκφόρτιση του οχήματος EV με συνεχή τάση ρεύματος (Direct Current, DC). Η λειτουργική ομάδα *CPPWMController* του OCPP, η οποία χρησιμοποιείται για τη διαμόρφωση πλάτους του πιλοτικού σήματος ελέγχου (Pulse Width Modulation, PWM), υιοθετεί τη SAE J1772, χαμηλής τάσης DC και PWM, σηματοδότηση [30].

Όπως αναφέρθηκε ήδη, το CHAdeMO είναι, όπως και το J1772, ένας τυποποιημένος σύνδεσμος αμφίδρομης ροής για τη σύνδεση του οχήματος EV στον εξοπλισμό EVSE ενός σταθμού φόρτισης CS. Το CHAdeMO είναι το προϊόν έρευνας της αυτοκινητοβιομηχανίας Nissan και ενός ιαπωνικού προμηθευτή υλικού, της Nichicon. Το CHAdeMO υποστηρίζει την OCPP επικοινωνία EVSE-EV [100]. Η OCPP λειτουργική ομάδα *CHAdeMOCtrlr* διαχειρίζεται τη σύνδεση και επικοινωνία μέσω του ελεγκτή CHAdeMO [30].

Το πρότυπο SAE J2931 περιλαμβάνει τις απαιτήσεις της επικοινωνίας CS-EV μεταξύ του σταθμού φόρτισης CS και του οχήματος EV. Το πρότυπο είναι το ισοδύναμο προϊόν του οργανισμού SAE με το IEC 15118.2 και το IEC 15118.3 με τα μέρη J2931.1 και J2931.4, αντίστοιχα. Το J2931.4 ορίζει την ευρυζωνική επικοινωνία του CS και του EV στα OSI επίπεδα L1 και L2, μέσω ενεργειακών συνδέσεων (Power Line Communication, PLC), ενώ το J2931.1 ορίζει το πρωτόκολλο για τα OSI επίπεδα L3 έως L6 [91]. Το πρότυπο καλύπτει την εναλλακτική της PLC μεθόδου, την Orthogonal Frequency Division Multiplexing (OFDM) μέθοδο [14].

#### 5.1.5.2 Επίπεδα Ζεύξης Δεδομένων και Δικτύου

Πρέπει να σημειωθεί ότι το SAE J2931 είναι το δεύτερο πρότυπο εκτός από το ISO 15118, που αναφέρεται στις λειτουργίες των OSI επιπέδων L2 και L3.

#### 5.1.5.3 Επίπεδο Μεταφοράς

Το Open Smart Charging Protocol (OSCP) είναι ένα πρωτόκολλο που καλύπτει τα OSI επίπεδα L4 έως L7 για την επικοινωνία των DSO-CSO [41]. Το OSCP εισήχθη για πρώτη φορά ως εναλλακτική λύση στο πρωτόκολλο του OSI επιπέδου L7 με την ονομασία OpenADR και σύντομα επεκτάθηκε για να καλύψει όλα τα OSI επίπεδα L4 έως L7. Τα ίδια επίπεδα καλύπτονται από τα πρωτόκολλα περιαγωγής CSO-EMSP, δηλαδή το Open Charge Point Interface (OCPI) και το Open Clearing House Protocol (OCHP).

Το Open Charge Point Interface (OCPI) είναι ένα πρωτόκολλο των OSI επιπέδων L4 έως L7 που επιτρέπει στα οχήματα EV να φορτίζουν σε διαφορετικά δίκτυα PEV. Το OCPI βασίζεται σε JSON. Επίσης, το TLS αξιοποιείται προαιρετικά από το πρωτόκολλο OCPI [41].

Το πρωτόκολλο Open Clearing House Protocol (OCHP) επιτρέπει συνδέσεις μεταξύ του φέροντα ρόλου Clearing House (ονομασία που αποδίδει ρόλο ο οποίος συνήθως εκπληρώνεται από το σύστημα διαχείρισης CSMS, προσφέροντας μια πλατφόρμα επικοινωνίας μεταξύ των CSO-EMSP, ανεξαρτήτως του χώρου παροχής φόρτισης), καθώς και μεταξύ του παρόχου EMSP και διαφορετικών χειριστών CSO. Το OCHP είναι ένα

πρωτόκολλο OSI επιπέδων L4 έως L7 που βασίζεται στο SOAP. Για το OCHP, όπως αναφέρθηκε και για το OCPI, το TLS είναι προαιρετικό [41].

#### 5.1.5.4 Επίπεδο Συνόδου

Η ιαπωνική κοινοπραξία Echonet παρουσίασε το πρωτόκολλο ECHONET-lite [101] το οποίο εστιάζει, αν και όχι αποκλειστικά, στην επικοινωνία CS-EMS [102]. Σε σύγκριση με το OCPP, το ECHONET-lite είναι ένα πρωτόκολλο OSI επιπέδων L5 έως L7 [103] που χρησιμοποιεί μηνύματα δυαδικής μορφής. Η ασφάλεια των δεδομένων δεν εμπίπτει στις λειτουργίες του πρωτοκόλλου [104]. Ωστόσο, το ECHONET-lite υποστηρίζει επικοινωνία μέσω PLC, μέσω Bluetooth σύνδεσης και μέσω δικτύου Ethernet ή ασύρματου, μεταξύ άλλων [105].

#### 5.1.5.5 Επίπεδο Παρουσίασης

Το πρωτόκολλο Open InterChange Protocol (OICP) [106] είναι ένα πρωτόκολλο OSI επιπέδων L6 και L7 που υποστηρίζει ό,τι και το πρωτόκολλο OCHP και το οποίο βασίζεται τόσο σε JSON όσο και σε SOAP. Το OICP αναφέρεται και αυτό ως πρωτόκολλο περιαγωγής.

#### 5.1.5.6 Επίπεδο Εφαρμογής

Το 2020, οι ISO και IEC εισήγαγαν το πρότυπο ISO/IEC 15118 για την επικοινωνία μεταξύ των οντοτήτων ενός συστήματος φόρτισης οχήματος EV [87],[88],[94],[107],[108], [109],[110]. Το ISO/IEC 15118 περιγράφει τα πρωτόκολλα επικοινωνίας V2G ανά επίπεδο OSI. Το πρότυπο εισάγει τη δυνατότητα PnC, η οποία επιτρέπει την εξουσιοδοτημένη διαδικασία φόρτισης οχήματος EV. Το OCPP έχει αναπτυχθεί σύμφωνα με αυτό το πρότυπο.

Το πρότυπο SAE J2836 περιλαμβάνει τις περιπτώσεις χρήσης και το πρότυπο SAE J2847 περιλαμβάνει τις προδιαγραφές για την επικοινωνία V2G στο OSI επίπεδο L7. Τα J2836 και J2847 είναι τα ισοδύναμα του οργανισμού SAE για το IEC 15118.1 [91].

Η IEEE υιοθέτησε το πρωτόκολλο Smart Energy Profile (SEP2) από τη ZigBee Alliance και πρότεινε την εξέλιξή του, το πρωτόκολλο IEEE 2030.5 [111]. Το IEEE 2030.5 είναι ένα πρωτόκολλο [104] που βασίζεται στο πρωτόκολλο IP, προσδιορίζει τις λειτουργίες του OSI επιπέδου L7 και καλύπτει την επικοινωνία EVSE-EV και DSO-EMS, όπου ο διαχειριστής διανομής DSO είναι τριτομερής [112]. Τα μηνύματα του πρωτοκόλλου έχουν μορφοποίηση XML ή Efficient XML Interchange (EXI) και το TLS χρησιμοποιείται στο OSI επίπεδο L4 για την ασφάλεια των δεδομένων. Όσον αφορά στη διαδικασία πιστοποίησης, το IEEE 2030.5 υποστηρίζει μη ανακληθέντα ιδιωτικά πιστοποιητικά διαρκείας, σε αντίθεση με τη χρήση των υποδομών δημόσιων κλειδιών PKI [43]. Μέχρι στιγμής, το πρωτόκολλο έχει χρησιμοποιηθεί μόνο σε έργα στις ΗΠΑ.

Το IEC 61850 είναι ένα πρότυπο που μοντελοποιεί την ενοποιημένη δομή που συμπεριλαμβάνει τις υποδομές φόρτισης και το έξυπνο πλέγμα [104]. Το IEC 61850 αναπτύχθηκε από την ένωση CHAdeMO ως εναλλακτική λύση των IEEE 2030.5 και OCPP για την επικοινωνία CS-EMS στο OSI επίπεδο L7 [113]. Το πρότυπο υποστηρίζει ένα τοπικό δίκτυο εντός του σταθμού φόρτισης CS για τον περιορισμό

της οριζόντιας καλωδίωσης στο χώρο φόρτισης [114]. Το πρότυπο υποστηρίζει, επίσης, τις επικοινωνίες CSMS-DSO, CS-CSMS και CS-CSO. Το OCPP και το IEC 61850 αλληλοσυμπληρώνονται για την επικοινωνία EVSE-DER, καθώς προβλέπουν την ύπαρξη εναλλακτικών πηγών ενέργειας εντός του συστήματος φόρτισης οχημάτων EV [115]. Τα συστήματα επικοινωνίας DER περιγράφονται λεπτομερώς από το IEC 61850-7-420 [116].

Το OpenADR, νεότερη ονομασία για το IEC 62746-10-1, είναι ένα ανοικτό πρωτόκολλο αίτησης/απόκρισης του OSI επιπέδου L7 [117] και παρέχεται από την OpenADR Alliance. Το OpenADR έχει αναπτυχθεί για να υποστηρίζει την επικοινωνία CSMS-DSO [118]. Σε ορισμένες περιπτώσεις, το OpenADR έχει χρησιμοποιηθεί για την επικοινωνία DSO-CSO [119] και για την επικοινωνία των DSO-EMS [112]. Η συμμόρφωση με αυτό το πρότυπο επιτρέπει τη μείωση της μέγιστης ζήτησης ισχύος, τη μετατόπιση φορτίου και τη δυναμική τιμολόγηση [120]. Όσον αφορά στην ασφάλεια, το TLS είναι υποχρεωτικό στο επίπεδο μεταφοράς για το OpenADR. Ο έλεγχος της ταυτότητας OpenADR βασίζεται στο PKI και σε αρχές έκδοσης πιστοποιητικών (Certificate Authorities, CA) [43]. Το OpenADR σε συνδυασμό με το OCPP δίνει μια δυναμική φύση στο σύστημα διαχείρισης CSMS με δυνατότητες προσαρμογής σε πραγματικό χρόνο σε συμβάντα πλέγματος.

## 5.2 Απαιτήσεις και ζητήματα ασφάλειας

### 5.2.1 Απαιτήσεις ασφάλειας υπηρεσίας φόρτισης

Οι απαιτήσεις ασφάλειας για την υπηρεσία φόρτισης οχημάτων EV βασισμένη στο OCPP, περιλαμβάνουν την ακεραιότητα, την αυθεντικότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριών του οδηγού/χρήστη του EV, των δεδομένων του οχήματος EV, ιδίως σχετικά με την κατάσταση φόρτισής του (State Of Charge, SOC), των δεδομένων του τοπικού μικρο-πλέγματος ισχύος και των δεδομένων της διαδικασίας χρέωσης της υπηρεσίας.

#### 5.2.1.1 Πληροφορίες του οδηγού/χρήστη οχήματος EV

Σχετικά με τη διαδικασία χρέωσης και τις πληροφορίες του οδηγού οχήματος EV, η επιβολή αναποκηρυξίας (non-repudiation) και ο έγκυρος καθορισμός/αναγνώριση υπευθύνου (accountability) είναι σημαντικά στοιχεία για να διασφαλιστεί:

*(α)* η πληρωμή/αποζημίωση κάθε κύκλου υπηρεσίας, και

*(β)* ότι όλα τα μηνύματα/ειδοποιήσεις που σχετίζονται με τη χρέωση θα αποστέλλονται προς και θα λαμβάνονται από τον κατάλληλο παραλήπτη [121].

#### 5.2.1.2 Εξοπλισμός σύνδεσης EVSE

Η ανάπτυξη της χρήσης οχημάτων EV και PEV, παρακίνησε τον οργανισμό ElaadNL να μελετήσει τις απαιτήσεις ασφάλειας για ένα δίκτυο PEV και όλες τις συσκευές και στοιχεία που συμμετέχουν σε αυτό. Σύμφωνα με το αποτέλεσμα, οι απαιτήσεις ασφάλειας συγκεκριμένα για τον εξοπλισμό σύνδεσης EVSE είναι οι ακόλουθες [84]:

*(α)* η δυνατότητα εφαρμογής απομακρυσμένων ενημερώσεων/αναβαθμίσεων,

*(β)* ο περιορισμός των εμφανίσεων και της διάρκειας διακοπών λειτουργίας, και

*(γ)* η διαλειτουργικότητα μεταξύ διεπαφών, ανεξάρτητα από τον κατασκευαστή/ προμηθευτή.

Ο συμβατικός σχεδιασμός του εξοπλισμού σύνδεσης EVSE πρέπει να υποστηρίζει τη δυνατότητα της εξ αποστάσεως ενημέρωσης ή αναβάθμισης του λογισμικού ή του υλικο-λογισμικού του εξοπλισμού σύνδεσης EVSE ή του σταθμού φόρτισης CS στον οποίο εντάσσεται ο εξοπλισμός. Η έλλειψη αυτής της δυνατότητας, σε συνδυασμό με το γεγονός ότι οι σταθμοί φόρτισης CS είναι συνήθως διάσπαρτα τοποθετημένοι σε δημόσιους χώρους και μακριά από την άμεση πρόσβαση ενός χειριστή πληροφορικής, θα μπορούσε να οδηγήσει σε καθυστέρηση των ενημερώσεων και, ως εκ τούτου, σε μείζον ζήτημα ασφάλειας.

Η διάρθρωση (configuration) του εξοπλισμού σύνδεσης EVSE πρέπει να μπορεί να τροποποιηθεί, χωρίς να απαιτείται επανεκκίνησή του. Η ίδια απαίτηση υπάρχει για τυχόν ενημερώσεις υλικο-λογισμικού, οι οποίες ενδέχεται επίσης να απαιτούν επανεκκίνηση. Αυτή η δυνατότητα θα επέτρεπε τη συχνή προσαρμογή της διάρθρωσης χωρίς απώλεια επικοινωνίας κατά τη διαδικασία επανεκκίνησης. Για τον σταθμό φόρτισης CS, ο οποίος θα πρέπει να είναι πάντα προσβάσιμος σε οχήματα EV και ο οποίος θα πρέπει να έχει τον ελάχιστο δυνατό χρόνο διακοπής λειτουργίας και ταυτόχρονα ενημερωμένη διάρθρωση, αυτό είναι ένα κρίσιμο χαρακτηριστικό από πλευράς λειτουργίας και ασφάλειας. Ως εκ τούτου, η επικοινωνία μεταξύ του σταθμού φόρτισης CS και των συστημάτων υποστήριξης πρέπει να είναι όσο το δυνατόν αδιάλειπτη.

Η απομακρυσμένη ενοποιημένη μετεγκατάσταση των παραμέτρων διάρθρωσης ενός σταθμού φόρτισης CS, θα πρέπει να είναι μια δυνατότητα ανεξάρτητη από τον κατασκευαστή/προμηθευτή των σταθμών φόρτισης CS, έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα διαφορετικών μοντέλων/τύπων CSs μέσα σε ένα δίκτυο PEV. Για τον ίδιο λόγο, καμία πληροφορία δεν θα πρέπει να κωδικοποιείται στο σταθμό φόρτισης CS από τον κατασκευαστή/προμηθευτή του.

#### 5.2.1.3 Συστήματα υποστήριξης υπηρεσίας φόρτισης

Οι απαιτήσεις ασφάλειας για τα σύστηματα υποστήριξης της υπηρεσίας φόρτισης είναι τα ακόλουθα:

*(α)* η δυνατότητα διαχείρισης δικτύου συσκευών διαφορετικών κατασκευαστών/ προμηθευτών,

*(β)* η υποστήριξη «έξυπνης φόρτισης», και

*(γ)* η δυνατότητα επίλυσης λειτουργικών ζητημάτων συσκευών διαφορετικών κατασκευαστών/ προμηθευτών.

#### 5.2.1.4 Απαιτήσεις πρωτοκόλλου OCPP

Η τεκμηρίωση του πρωτοκόλλου OCPP αναφέρει τις απαιτήσεις που λήφθηκαν υπόψη για την ανάπτυξη και ενσωμάτωση λειτουργιών ασφάλειας στην έκδοση OCPP 2.0 [30].

Αυτή η λίστα προέκυψε ως μια στοχευμένη επιλογή μέσα από τις προαναφερθείσες λίστες απαιτήσεων και τη μελέτη του οργανισμού ElaadNL σχετικά με τα συστήματα φόρτισης EV [122]. Οι απαιτήσεις του πρωτοκόλλου OCPP που επιλέχθηκαν είναι οι ακόλουθες:

*(α)* Η ασφαλής σύνδεση μεταξύ του συστήματος διαχείρισης CSMS και του σταθμού φόρτισης CS, με χρήση μεθόδων κρυπτογράφησης για τη διασφάλιση της ακεραιότητας και του απορρήτου των μηνυμάτων.

*(β)* Ο αμοιβαίος έλεγχος της ταυτότητας μεταξύ του συστήματος διαχείρισης CSMS και του σταθμού φόρτισης CS.

*(γ)* Η ασφαλής διαδικασία ενημέρωσης υλικο-λογισμικού για τον σταθμό φόρτισης CS με τη χρήση προελεγμένων και εγκεκριμένων όσον αφορά στην ακεραιότητα και στην αναποκηρυξία ειδώλων υλικο-λογισμικού.

*(δ)* Η καταγραφή/παρακολούθηση της υπηρεσίας *έξυπνης φόρτισης*.

### 5.2.2 Κατηγοριοποίηση επιθέσεων σε υπηρεσία φόρτισης

Η κατηγοριοποίηση των επιθέσεων που σχετίζονται με το πρωτόκολλο OCPP, βασίζεται στον τύπο και στον αντίκτυπο της επίθεσης. Ο *τύπος επιθέσης* σε ένα κυβερνοφυσικό σύστημα (Cyber-Physical System, CPS) όπως είναι το σύστημα φόρτισης οχημάτων EV σχετίζεται με τον τρόπο εκδήλωσης ή ανάπτυξης της επίθεσης και μπορεί να εκδηλώνεται φυσικά, κυβερνοχωρικά ή και τα δύο [123]. Αντίστοιχα, ο *αντίκτυπος επίθεσης*, δηλαδή η φύση των συνεπειών της, μπορεί επίσης να είναι φυσικός, κυβερνοχωρικός ή και τα δύο. Για παράδειγμα, ένας κυβερνοφυσικός τύπος επίθεσης είναι αυτός που αναπτύσσεται τόσο με φυσική πρόσβαση όσο και με το κατάλληλο εργαλείο στον κυβερνοχώρο, και μια επίθεση με κυβερνοφυσικό αντίκτυπο είναι αυτή που επηρεάζει τόσο το πεδίο του κυβερνοχώρου όσο και τη φυσική υποδομή.

Με βάση τα παραπάνω κριτήρια, οι επιθέσεις και τα σχετικά με αυτές αντίμετρα που έχουν ήδη αναπτυχθεί και δοκιμαστεί σε δίκτυα PEV βασιζόμενα στο OCPP, μπορούν να κατηγοριοποιηθούν σε τρεις ομάδες:

*(α)* τις φυσικές επιθέσεις,

*(β)* τις επιθέσεις στον κυβερνοχώρο ή κυβερνοχωρικές επιθέσεις, και

*(γ)* τις κυβερνοφυσικές επιθέσεις.

Στην πρώτη ομάδα, εντάσσονται οι επιθέσεις που χρειάζονται φυσική πρόσβαση σε μια τοποθεσία δικτύου PEV ή οποιοδήποτε αρχιτεκτονικό στοιχείο αυτού για να εξαπολυθούν. Στη δεύτερη ομάδα, εντάσσονται οι κυβερνο-επιθέσεις σε δίκτυα PEV που εξαπολύονται με ψηφιακό/δικτυακό τρόπο χωρίς να απαιτείται φυσική πρόσβαση, και στην τελευταία ομάδα οι επιθέσεις που αναπτύσσονται με κυβερνοφυσικό τρόπο, συνδυάζοντας τις προηγούμενες δύο περιπτώσεις. Αυτή η ταξινόμηση εμφανίζεται στον Πίνακα 7. Ακολουθούν η περιγραφή, τα αντίμετρα και τα επηρεαζόμενα στοιχεία φόρτισης οχημάτων EV για τις φυσικές επιθέσεις, τις κυβερνοεπιθέσεις και τις κυβερνοφυσικές επιθέσεις.

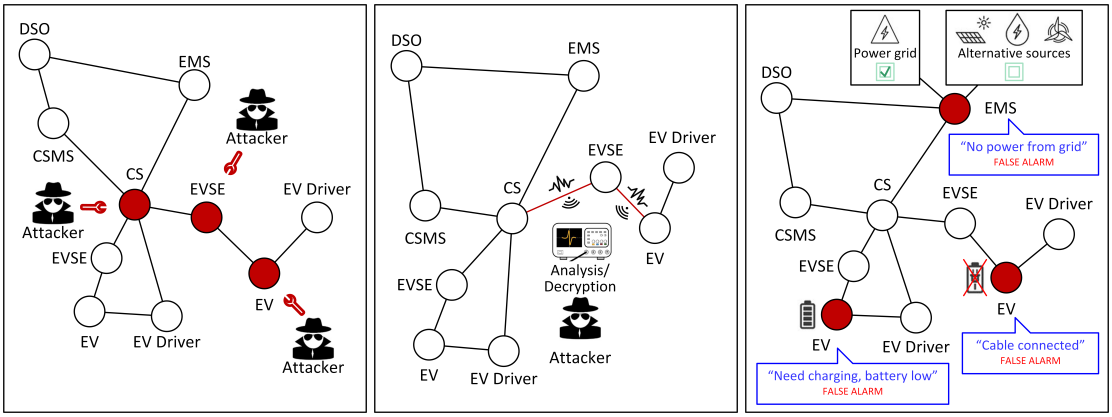
Πίνακας 7. Κατηγοριοποίηση των επιθέσεων ασφάλειας



### 5.2.3 Φυσικές επιθέσεις

Η πρώτη ομάδα επιθέσεων, δηλαδή οι φυσικές επιθέσεις (Εικόνα 15) και τα σχετικά αντίμετρα που προτείνονται περιγράφονται σε αυτό το υποκεφάλαιο. Πρόκειται για τις επιθέσεις που εξαπολύονται φυσικά (τύπος επίθεσης) ή έχουν φυσικές συνέπειες (αντίκτυπος επίθεσης) στα περιουσιακά στοιχεία του συστήματος φόρτισης EV.

Στον Πίνακα 8, εμφανίζονται όλα τα αντίμετρα που σχετίζονται με την κάθε φυσική επίθεση, ακολουθούμενα από τα περιουσιακά στοιχεία ενός συστήματος φόρτισης EV. Εάν ένα στοιχείο επηρεάζεται από την επίθεση και προστατεύεται από αυτήν από το προτεινόμενο αντίμετρο, τότε το στοιχείο σημειώνεται ως *Προστατευμένο στοιχείο* στον πίνακα. Διαφορετικά, το στοιχείο σημειώνεται ως *Στοχευμένο στοιχείο* στην περίπτωση που επηρεάζεται και δεν προστατεύεται. Εάν η συγκεκριμένη επίθεση δεν επηρεάζει καθόλου το στοιχείο, τότε αυτό το στοιχείο δεν σημειώνεται με κανέναν τρόπο.




(α) Παραβιάσεις (β) Επιθέσεις πλευρικού καναλιού (γ) Επιθέσεις αισθητήρων

Εικόνα 15. Φυσικές επιθέσεις σε δίκτυα φόρτισης PEV

Πίνακας 8. Φυσικές επιθέσεις και αντίμετρα

| Attacks | Countermeasures | Assets | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Driver | EV | EVSE | CS | EMS | CSMS | Data | Grid |
| Tampering | Constructional EVSE design [96] | ○ | ○ | ● | ○ | ○ | ○ | ● | ● |
| | In-vehicle credentials generation/storage [97],[124] | ○ | ● | ○ | ○ | ○ | ○ | ● | |
| | OCPP encryption and firmware updating [125] | ○ | ○ | ● | ● | ○ | ○ | ○ | |
| | Smart card chip for signatures [126],[127],[128] | ○ | ○ | ○ | ● | ○ | ● | ● | |
| | Intelligent electronics device on EV [129] | ○ | ● | ○ | ○ | ○ | ○ | ○ | |
| | Limited lifetime of EV authentication [130] | ○ | ● | ○ | ○ | ○ | ○ | ○ | |
| | OCPP PnC mechanism [120] | ○ | ● | ○ | ○ | ○ | ○ | ○ | |
| | Elliptic-curve keypair for AutoCharge [131] | ● | ● | ● | ○ | ○ | ○ | ● | |
| | Decentralized firmware attestation [132],[133] | ○ | ● | ○ | ○ | ○ | ○ | ● | |
| | Direct anonymous attestation protocol [134] | ○ | ● | ○ | ○ | ○ | ○ | ● | |
| | EV reservation w/ smart contract [135] | ● | ● | ○ | ● | ○ | ○ | ● | |
| | Authentication scheme w/ smart contracts [136] | ● | ● | ○ | ● | ○ | ○ | ● | |
| | Pseudonym-based authentication scheme [137],[138] | ● | ● | ○ | ● | ○ | ○ | ● | |
| | Physical unloneable functions [139],[140] | ● | ● | ● | ○ | ○ | ○ | ○ | |
| | Secure User Key-exchange Authentication [141] | ● | ● | ● | ○ | ○ | ● | ○ | |
| Side-channel | In-vehicle credentials generation/storage [97],[124] | ○ | ● | ○ | ○ | | | ● | |
| | Dedicated in-vehicle hardware [142],[143] | ○ | ● | ○ | ○ | | | ● | |
| | Physical security policies [113] | ○ | ○ | ○ | ● | | ● | ● | ● |
| | Decentralized smart charging controller [144] | ○ | ○ | ○ | ● | | ● | ● | |
| State/sensor | N/A | | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

○ Στοχευμένο στοιχείο ● Προστατευόμενο στοιχείο

### 5.2.3.1 Επιθέσεις παραβίασης

Ο έλεγχος φυσικής πρόσβασης μπορεί να προστατεύσει όχι μόνο τα διάσπαρτα στοιχεία του συστήματος φόρτισης EV, όπως τα οχήματα EV, την έξυπνη συσκευή του οδηγού/χρήστη του EV, τον εξοπλισμό σύνδεσης EVSE, καθώς και τα υπόλοιπα στοιχεία του συστήματος. Τα προαναφερόμενα στοιχεία είναι ιδιαίτερα εκτεθειμένα σε φυσική πρόσβαση με το να εγκαθίστανται ή να σταθμεύουν σε χώρους με ελεύθερη πρόσβαση στο κοινό. Εκτός από αυτήν την έκθεση, καθένα από αυτά τα στοιχεία έχει λειτουργικά ή κατασκευαστικά χαρακτηριστικά που μπορεί να διευκολύνουν επιθέσεις φυσικής πρόσβασης με πιο χαρακτηριστική περίπτωση τις επιθέσεις παραβίασης (tampering).

Τα ακόλουθα προτεινόμενα αντίμετρα για τις επιθέσεις παραβίασης ομαδοποιούνται με βάση το στοιχείο φόρτισης EV που χρησιμοποιείται ως σημείο εισόδου για την επίθεση.

**Παραβίαση εξοπλισμού σύνδεσης σταθμού φόρτισης EVSE/CS**

Ο εξοπλισμός σύνδεσης EVSE είναι η συσκευή αιχμής που φιλοξενείται στο στοιχείο αιχμής, δηλαδή στον σταθμό φόρτισης CS. Ο εξοπλισμός σύνδεσης EVSE είναι προσβάσιμος στον οδηγό του οχήματος EV και, όταν ο σταθμός φόρτισης CS βρίσκεται σε δημόσιους χώρους φόρτισης, είναι προσβάσιμος και σε οποιονδήποτε άλλο. Επιπλέον, οι περισσότεροι τύποι EVSE διαθέτουν εξωτερικές θύρες και Universal Serial Bus (USB) ή σειριακές θύρες για τη σύνδεση του οχήματος EV. Πρόκειται για θύρες που επιτρέπουν και ενδέχεται να χρησιμοποιηθούν κατά την επίθεση φυσικής πρόσβασης, επιτρέποντας την αλλοίωση των λειτουργιών, του λογισμικού και του υλικού του εξοπλισμού EVSE ή ακόμα και των προσωπικών δεδομένων του οδηγού του οχήματος EV. Ο εξοπλισμός σύνδεσης EVSE είναι ευάλωτος κυρίως λόγω του ενσωματωμένου διαποδιαμορφωτή (modem) κυψελοειδούς επικοινωνίας, το οποίο χρησιμοποιείται για την ανταλλαγή των δεδομένων, που συλλέγονται μέσω του αναγνώστη καρτών, μεταξύ του εξοπλισμού σύνδεσης EVSE και του εκδότη της πιστωτικής/χρεωστικής κάρτας [145]. Σε περίπτωση που ο διαποδιαμορφωτής παραβιαστεί, τότε η διαδικασία πληρωμής μπορεί να γίνει αναξιόπιστη, τα διαπιστευτήρια κατόχου της κάρτας μπορεί να εκτεθούν και η υπηρεσία χρέωσης να μην ολοκληρωθεί ποτέ.

Όπως προτείνεται στην έκθεση που συντάχθηκε από το Εθνικό Εργαστήριο Ανανεώσιμων Πηγών Ενέργειας για το Υπουργείο Ενέργειας των ΗΠΑ (Department of Energy, DOE) [96], ο κατασκευαστικός σχεδιασμός του EVSE μπορεί να μετριάσει τις επιθέσεις τύπου φυσικής πρόσβασης μέσω:

*(α)* της μείωσης του αριθμού των εξωτερικών θυρών πρόσβασης,

*(β)* της επιβολής μεθόδων κρυπτογράφησης για τα εισερχόμενα δεδομένα,

*(γ)* της ενεργοποίησης ειδοποιήσεων παραβίασης, και

*(δ)* της διενέργειας τακτικών τεχνικών ελέγχων.

Το OCPP 2.0 ενσωματώνει κρυπτογραφική υπογραφή και λειτουργίες ενημέρωσης υλικο-λογισμικού [125]. Για τον λόγο αυτό, το OCPP προτείνεται ως το βέλτιστο πρωτόκολλο κατά της παραβίασης του σταθμού φόρτισης CS και, πιο συγκεκριμένα, της παραβίασης του EVSE [42].

Ο εξοπλισμός σύνδεσης EVSE δεν είναι το μόνο περιουσιακό στοιχείο του σταθμού φόρτισης CS που μπορεί να παραβιαστεί. Ο CS διαθέτει δημόσια και ιδιωτικά πιστοποιητικά για την επικυρωμένη επικοινωνία με το όχημα EV και το σύστημα διαχείρισης CSMS. Μια λύση κατά της παραβίασης είναι η χρήση ενός πλινθίου (chip) έξυπνης κάρτας για τη δημιουργία και την αποθήκευση των ψηφιακών υπογραφών [126]. Εάν ένα τέτοιο πλινθίο έξυπνης κάρτας παραποιηθεί, τότε ο σταθμός φόρτισης CS θα ειδοποιηθεί και το σχετικό πιστοποιητικό θα ανακληθεί από το σύστημα διαχείρισης CSMS. Εκτός από αυτή τη λειτουργία, οι σύγχρονες έξυπνες κάρτες ενσωματώνουν μικροεπεξεργαστές που τους επιτρέπουν να φιλοξενούν κρυπτογραφικές λειτουργίες [127]. Η χρήση έξυπνης κάρτας ως λύση κατά της παραβίασης έχει προταθεί για την

προστασία και των δεδομένων του οδηγού του οχήματος EV [128], κατά τη διαδικασία πληρωμής.

### Παραβίαση οχήματος EV

Ως τελικό σημείο της υπηρεσίας χρέωσης, κάθε όχημα EV αναγνωρίζεται και πιστοποιείται από το σύστημα διαχείρισης CSMS της υπηρεσίας. Η αναγνώριση και ο έλεγχος ταυτότητας του οχήματος EV βασίζεται συνήθως στην επικύρωση του οχήματος EV και των διαπιστευτηρίων του οδηγού/χρήστη EV. Μια επίθεση παραβίασης EV μπορεί να οδηγήσει σε ένα αλλοιωμένο σύνολο διαπιστευτηρίων ή στην έκθεση του οχήματος EV, του σταθμού φόρτισης CS ή ευαίσθητων δεδομένων του οδηγού/χρήστη του EV. Ένα παραβιασμένο όχημα EV μπορεί να επηρεάσει τη διαδικασία πληρωμής/χρέωσης ή να διοχετεύσει ψευδή δεδομένα στον σταθμό φόρτισης CS και, κατά συνέπεια, στο σύστημα διαχείρισης CSMS με ψευδείς μετρήσεις χρέωσης και ψευδείς ενδείξεις.

Για να υλοποιήσουν τον έλεγχο ταυτότητας του EV, ο Chan και ο Zhou [129] υπέθεσαν ότι κάθε όχημα EV θα πρέπει να είναι εξοπλισμένο με μια ενσωματωμένη Intelligent Electronics Device (IED) που θα χρησιμεύει ως διακριτικό ελέγχου ταυτότητας για το EV εντός του συστήματος φόρτισης EV. Το IED πρέπει να είναι ανθεκτικό σε παραβιάσεις και το κλειδί που είναι αποθηκευμένο σε αυτό θα πρέπει να είναι προσβάσιμο, να μπορεί να ανακληθεί και να εκδοθεί μόνο από τον χειριστή του συστήματος φόρτισης (δηλαδή το άτομο ή την αρχή που χειρίζεται το σύστημα διαχείρισης CSMS). Οι απαραίτητες προσαρμογές ώστε το EV να περιλαμβάνει το IED θεωρούνται εύκολες και χαμηλού κόστους.

Με βάση το πρότυπο IEC 61850 και την αναμενόμενη υιοθέτηση της τεχνολογίας δικτύωσης οριζόμενης από το λογισμικό (Software Defined Networking, SDN), οι Soares et al. [130] πρότειναν έναν μηχανισμό ελέγχου ταυτότητας για ηλεκτρικά οχήματα με περιορισμένο φορτίο ελέγχου και διάρκεια ζωής της επαλήθευσης της ταυτότητας.

Η τελευταία έκδοση του πρωτοκόλλου OCPP 2.0 υποστηρίζει τον μηχανισμό PnC για την αναγνώριση και τον έλεγχο ταυτότητας του οχήματος EV [120] μέσω του καλωδίου φόρτισης. Το PnC είναι ευθυγραμμισμένο με το πρότυπο ISO/IEC 15118 και επιτρέπει τον έλεγχο ταυτότητας του EV χωρίς ανθρώπινη παρέμβαση. Ωστόσο, ο μηχανισμός PnC φέρει μια ευπάθεια που σχετίζεται με τη μετάδοση των διαπιστευτηρίων του EV μεταξύ του σταθμού φόρτισης CS και του συστήματος διαχείρισης CSMS κατά τη διάρκεια της διαδικασίας ελέγχου της ταυτότητας. Ένα μέτρο μετριασμού για αυτό το ζήτημα είναι η δημιουργία και η αποθήκευση των διαπιστευτηρίων στο ίδιο το όχημα EV [97],[124].

Μια εναλλακτική λύση στο PnC είναι ο μηχανισμός αυτόματης φόρτισης Autocharge [146]. Η Autocharge υποστηρίζεται από τις προηγούμενες εκδόσεις του OCPP, ωστόσο αρκετές υπάρχουσες υλοποιήσεις συστημάτων φόρτισης υποστηρίζονται από αυτές τις εκδόσεις του πρωτοκόλλου, επομένως τα σχετικά ζητήματα ασφάλειας αποτελούν ακόμη θέματα προς επίλυση. Ο μηχανισμός Autocharge περιλαμβάνει το πρωτόκολλο ISO/IEC 15118 Signal-Level Attenuation Characterization (SLAC) για τη σύνδεση του οχήματος σε φορτιστή. Το SLAC είναι ένα πρωτόκολλο αίτησης/απόκρισης που χρησιμοποιείται όταν το όχημα EV και ο σταθμός φόρτισης CS μοιράζονται μια σύνδεση PLC. Το EV και ο CS συμφωνούν σε ένα μοναδικό κλειδί ID ανά περίοδο λειτουργίας και οποιαδήποτε

ανταλλαγή δεδομένων μεταξύ τους εμπεριέχει αυτό το κλειδί. Το SLAC ID παρέχεται από τον σταθμό φόρτισης CS και από την υπηρεσία PKI. Εκτός από την περίπτωση που η υπηρεσία PKI δεν είναι προσβάσιμη, τα μηνύματα αρχικοποίησης SLAC ανταλλάσσονται σε απλό κείμενο, αφήνοντας το αναγνωριστικό και, κατά συνέπεια, τη συνεδρία εκτεθειμένη σε επιθέσεις υποκλοπής. Οι Baker και Martinovic [131] προτείνουν τη χρήση ενός προσωρινού ζεύγους κλειδιών βάσει της μεθόδου Elliptic-Curve Cryptography (ECC) για τα μηνύματα αρχικοποίησης SLAC, έως ότου δημιουργηθεί το κλειδί της συνεδρίας και γίνει γνωστό και στα δύο μέρη.

Μια άλλη πρόκληση στην περίπτωση παραβίασης οχήματος EV είναι η ακεραιότητα της μονάδας ελέγχου Electronic Control Unit (ECU) του EV. Μια παραβίαση της ECU μπορεί να έχει ως στόχο την αλλαγή της διαδικασίας φόρτισης, ωστόσο η ECU ελέγχει και άλλες πολύ πιο κρίσιμες διεργασίες που μπορεί επίσης να επηρεαστούν, όπως για παράδειγμα ο έλεγχος του κινητήρα. Η ECU ελέγχει τη διαδικασία φόρτισης του EV και, επομένως, μια επίθεση τύπου man-in-the-middle (MitM) στο OCPP μπορεί τελικά να επηρεάσει και την ECU. Στις εργασίες [132] και [133] προτείνεται ένα αποκεντρωμένο σύστημα πιστοποίησης υλικο-λογισμικού για τον εντοπισμό της παραβίασης της μνήμης flash της ECU ή για τον εντοπισμό ύπαρξης παλιού υλικο-λογισμικού στην ECU.

Η επικοινωνία μεταξύ του οχήματος EV και του σταθμού φόρτισης CS κατά ISO 15118, πραγματοποιείται από την πλευρά του EV μέσω του ενσωματωμένου ελεγκτή επικοινωνίας Electric Vehicle Communication Controller (EVCC). Ο EVCC χειρίζεται την επικοινωνία και, ως εκ τούτου, μεταφέρει ευαίσθητα δεδομένα σχετικά με τα Original Equipment Manufacturer (OEM) πιστοποιητικά παροχής και σύμβασης από τον κατασκευαστή, καθώς και τα σχετικά κλειδιά του οχήματος EV. Οι Zelle et al. [134] προτείνουν τη χρήση του πρωτοκόλλου άμεσης ανώνυμης βεβαίωσης Direct Anonymous Attestation (DAA) και μιας μονάδας αξιόπιστης πλατφόρμας εντός του οχήματος, την Trusted Platform Module (TPM), για την προστασία του EVCC και των δεδομένων από παραβιάσεις σε όλη την αλυσίδα διαδικασίας PnC. Η TPM προστατεύει τα κλειδιά και τα πιστοποιητικά, καθώς φιλοξενεί τις διαδικασίες δημιουργίας και αποθήκευσής τους και το DAA υποστηρίζει τις διαδικασίες κρυπτογράφησης και εξουσιοδότησης καθόλη τη διάρκεια του κύκλου ζωής της υπηρεσίας φόρτισης.

#### Παραβίαση δεδομένων κράτησης/χρέωσης

Η παραποίηση του εξοπλισμού σύνδεσης EVSE, του σταθμού φόρτισης CS, του οχήματος EV ή οποιουδήποτε άλλου στοιχείου του συστήματος που συμμετέχει στη διαδικασία χρέωσης της υπηρεσίας φόρτισης EV αποσκοπεί, τελικά, στην υποκλοπή ή στην παραβίαση των δεδομένων και, ως εκ τούτου, στην ανάκτηση του ελέγχου της κράτησης ή της διαδικασίας πληρωμής/χρέωσης από τον επιτιθέμενο. Η παραβίαση δεδομένων συνδέεται έντονα με την κλοπή ενέργειας, του μικρο-πλέγματος ενέργειας στο οποίο υπάγεται το σύστημα φόρτισης και, κατά συνέπεια, του ευρύτερου τοπικού πλέγματος ενέργειας [40].

Το BlockEV [135], ένα πρωτόκολλο φόρτισης οχήματος EV που βασίζεται στην τεχνολογία blockchain, υποστηρίζει την επικοινωνία μεταξύ του οχήματος EV και του σταθμού φόρτισης CS χωρίς καμία κοινή χρήση ιδιωτικών πληροφοριών από τις δύο πλευρές. Αυτό επιτυγχάνεται με τη χρήση έξυπνων συμβολαίων και ενός κατανεμημένου

καθολικού για τα σχετικά με τις συμβάσεις δεδομένα [147],[148]. Τα χαρακτηριστικά του πρωτοκόλλου BlockEV διασφαλίζουν:

*(α)* τη διαθεσιμότητα του σταθμού φόρτισης CS που επιλέγεται για κράτηση,
*(β)* την εγκυρότητα της κράτησης που γίνεται από το όχημα EV,
*(γ)* την αξιοπιστία του οχήματος EV ή του οδηγού/χρήστη του,
*(δ)* την τιμή χρέωσης για τη δεσμευμένη υπηρεσία,
*(ε)* την ταυτότητα του ηλεκτρικού οχήματος που όντως εξυπηρετήθηκε, και
*(στ)* την ποσότητα της ηλεκτρικής ενέργειας που καταναλώνεται.

Τα έξυπνα συμβόλαια χρησιμοποιούνται και για τη διατήρηση του απορρήτου του σχήματος επαλήθευσης της ταυτότητας [136]. Στην περίπτωση αυτή, για την ανώνυμη ολοκλήρωση της διαδικασίας επαλήθευσης της ταυτότητας, χρησιμοποιείται η δέσμευση Pederson και ο μηχανισμός που βασίζεται σε διακριτικά.

Η προστασία δεδομένων του οχήματος και του οδηγού/χρήστη του EV από παραβιάσεις μελετάται στην εργασία [137], που προτείνει ένα σχήμα επαλήθευσης ταυτότητας για την επικοινωνία μεταξύ του οχήματος EV και του σταθμού φόρτισης CS. Για την επίτευξη της προστασίας του απορρήτου των δεδομένων του οχήματος και του οδηγού EV, η αναγνώριση του EV βασίζεται σε ένα ψευδώνυμο που παράγεται για κάθε σύνδεση EV-CS. Το ψευδώνυμο αλλάζει εάν το EV συνδεθεί σε διαφορετικό σταθμό φόρτισης CS και λήγει όταν το όχημα EV εγκαταλείψει την περιοχή φόρτισης. Μόνο ένα κεντρικό στοιχείο, όπως το σύστημα διαχείρισης CSMS, χρειάζεται να τηρεί αρχείο για οποιαδήποτε αλλαγή ή λήξη των υπαρχόντων ψευδωνύμων. Με το πρωτόκολλο Portunes [138] προτείνεται η επαλήθευση ταυτότητας των οχημάτων EV με έναν μηχανισμό ψευδωνύμων που παράλληλα προστατεύει το απόρρητο της τοποθεσίας του οχήματος EV. Το Portunes συγκρίθηκε με τον αλγόριθμο ψηφιακής υπογραφής Elliptic Curve Digital Signature Algorithm (ECDSA) για τη δημιουργία και επαλήθευση υπογραφών και βρέθηκε ότι ήταν πολύ πιο γρήγορο.

**Παραβίαση διαφόρων δρώντων στοιχείων**

Οποιαδήποτε παραβίαση του οχήματος EV, της έξυπνης συσκευής του οδηγού ή του εξοπλισμού σύνδεσης EVSE μπορεί να μετριαστεί με την ενσωμάτωση των Physical Unclonable Functions (PUF) [139],[140]. Τα PUFs αλλάζουν τη συμπεριφορά του εξοπλισμού σύνδεσης EVSE, διασφαλίζοντας πως η τυχόν παραβιασμένη συσκευή θα καταστεί αναγνωρίσιμη στο σύστημα φόρτισης EV. Εάν εντοπιστεί η παραβιασμένη συσκευή, τότε η επίθεση της παραβίασης και η δράση του επιτιθέμενου μπορεί να περιοριστεί πιο εύκολα. Το ασφαλές πρωτόκολλο επαλήθευσης της ταυτότητας με ανταλλαγή κλειδιών χρήστη με το όνομα Secure User Key-Exchange Authentication (SUKA) [141] βασίζεται επίσης σε PUF. Το SUKA επιτυγχάνει έναν αμοιβαίο έλεγχο της ταυτότητας δύο βημάτων μεταξύ ενός EV και του διακομιστή δικτύου ενέργειας. Το SUKA μπορεί να παρέχει ασφάλεια κλειδιού συνεδρίας, φυσική ασφάλεια, ακεραιότητα μηνυμάτων και προστασία της ταυτότητας. Επιπλέον, το SUKA μπορεί να προστατεύσει την επικοινωνία V2G από απομίμηση, επιθέσεις επανάληψη και επιθέσεις MitM.

#### 5.2.3.2 Επιθέσεις πλευρικού καναλιού

Η συμμετοχή των δρώντων στοιχείων στις OCPP διαδικασίες φόρτισης και χρέωσης εισάγει έναν κίνδυνο που σχετίζεται με τις επιθέσεις πλευρικού καναλιού (side-channel) για αυτά τα στοιχεία και, ως εκ τούτου, για το ίδιο το πρωτόκολλο. Η επίθεση ανάλυσης ισχύος (power analysis attack) είναι μια επίθεση υλικού και μια από τις κύριες κατηγορίες επιθέσεων πλευρικού καναλιού. Αυτή η επίθεση μπορεί να επηρεάσει τα στοιχεία του συστήματος φόρτισης που παράγουν ή φιλοξενούν ευαίσθητες πληροφορίες και, πιο συγκεκριμένα, τα κλειδιά και τα διαπιστευτήρια του οχήματος και του οδηγού/χρήστη του [47]. Τα πιο ευάλωτα δρώντα στοιχεία σε επιθέσεις ανάλυσης ισχύος είναι:

*(α)* ο οδηγός/χρήστης του οχήματος,

*(β)* το όχημα,

*(γ)* ο εξοπλισμός σύνδεσης EVSE και

*(δ)* ο σταθμός φόρτισης CS.

Όλα αυτά τα βασικά στοιχεία φόρτισης παράγουν, αποθηκεύουν ή ανταλλάσσουν μηνύματα που εμπεριέχουν ευαίσθητες πληροφορίες, καθώς επίσης περιλαμβάνουν υλικό που μπορεί να χρησιμοποιηθεί για την παρακολούθηση του επίπεδου κατανάλωσης ενέργειας. Ανάλογα με το στοχευόμενο στοιχείο και τα αποκτηθέντα διαπιστευτήρια και κλειδιά, η ανάλυση ισχύος μπορεί να οδηγήσει σε απομίμηση, απάτη χρέωσης ή επιθέσεις παράκαμψης μετρητή [134].

Το πρωτόκολλο OCPP επηρεάζεται επίσης από ηλεκτρομαγνητικές επιθέσεις, μια άλλη κατηγορία επιθέσεων πλευρικού καναλιού, που βασίζονται στη διαρροή ηλεκτρομαγνητικής ακτινοβολίας, στις περιπτώσεις όπου υπάρχει μια σύνδεση PLC μεταξύ του οχήματος EV και του σταθμού φόρτισης CS [131]. Το κύκλωμα PLC λειτουργεί από κατασκευής ως κεραία και οι κυματομορφές μιας επικοινωνίας PLC μπορούν να υποκλαπούν ασύρματα και να διαχειριστούν με ευκολία.

Στις επιθέσεις πλευρικού καναλιού ο επιτιθέμενος στοχεύει κυρίως στην απόκτηση των διαπιστευτηρίων του οχήματος ή του οδηγού. Αυτά τα διαπιστευτήρια δεν είναι απλώς χρήσιμα για τον εισβολέα, είναι και εκτεθειμένα σε τέτοιου τύπου επιθέσεις. Ο μηχανισμός PnC του πρωτοκόλλου OCPP είναι ευάλωτος σε επιθέσεις πλευρικού καναλιού, λόγω της μετάδοσης των διαπιστευτηρίων του οχήματος μεταξύ του σταθμού φόρτισης CS και του συστήματος διαχείρισης CSMS και αντίστροφα. Η μετάδοση αυτή λαμβάνει χώρα κατά τη διαδικασία επαλήθευσης της ταυτότητας [134].

Τα περισσότερα αντίμετρα για επιθέσεις πλευρικού καναλιού στοχεύουν περισσότερο στην προστασία των περιουσιακών στοιχείων, που επηρεάζονται, παρά στην πρόληψη μιας ενδεχόμενης επίθεσης εναντίον τους. Ένα μέτρο περιορισμού για αυτό το ζήτημα είναι η δημιουργία και αποθήκευση διαπιστευτηρίων εντός του οχήματος [97],[124]. Η παραγωγή και η αποθήκευση πραγματοποιούνται από μια μονάδα ασφάλειας υλικού (Hardware Security Module, HSM) που είναι ενσωματωμένη για τον σκοπό αυτό στο όχημα. Τα σχετικά μηνύματα που ανταλλάσσονται μεταξύ του σταθμού φόρτισης CS και του συστήματος διαχείρισης CSMS υποστηρίζονται εγγενώς από το OCPP με τη μορφή μηνυμάτων που περιγράφονται από το πρωτόκολλο ως *DataTransfer*. Αυτή η χρήση υλικού με αποκλειστικό στόχο την παραγωγή και αποθήκευση διαπιστευτηρίων είναι

προτιμότερη από την εναλλακτική λύση ενσωματωμένου συστήματος σε ψηφίδα (System on Chip, SoC), όσον αφορά στη λειτουργική ανεξαρτησία και στην ευκολία πρόσβασης.

Μια προηγούμενη εφαρμογή με αποκλειστική χρήση υλικού, το TPM 2.0 [142], έχει ήδη ενσωματωθεί σε ηλεκτρικά οχήματα που χρησιμοποιούνται. Το TPM 2.0 υποστηρίζει την ασφαλή αποθήκευση κλειδιών δεδομένων και πιστοποιητικών, κρυπτογραφικές λειτουργίες και λειτουργίες εξουσιοδότησης και μια μέθοδο ανίχνευσης υλικο-λογισμικού στο οποίο έχει εφαρμοστεί χειρισμός. Τα TPMs είναι ευθυγραμμισμένα με το πρότυπο AEC-Q100 και συμμορφώνονται με την πιστοποίηση ασφάλειας EAL4+ των κοινών κριτηρίων (Common Criteria, CC). Οι Fuchs et al. [143] προτείνουν μια ασφαλή αρχιτεκτονική που εκμεταλλεύεται τις λειτουργίες ασφάλειας των TPMs.

Ακόμη και στην περίπτωση αναγνώρισης και επαλήθευσης της ταυτότητας τόσο του οχήματος EV όσο και του οδηγού/χρήστη του, οι ευαίσθητες πληροφορίες μπορεί να υποβληθούν σε επιτόπου επεξεργασία στο σταθμό φόρτισης CS, αντί να μεταδοθούν στο σύστημα διαχείρισης CSMS για επεξεργασία και επιστροφή. Αυτό το σχήμα μπορεί να καλύπτει τις απαιτήσεις ασφαλούς επικοινωνίας του δικτύου PEV. Ωστόσο, οι επιπλέον συσκευές ανά σταθμό φόρτισης CS που απαιτούνται για τη κατανομή της διαδικασίας ελέγχου της ταυτότητας εισάγουν τα δικά τους πρόσθετα προβλήματα φυσικής ασφάλειας. Προτείνεται η εφαρμογή πολιτικών φυσικής ασφάλειας σε αυτές τις ενσωματωμένες συσκευές για την προστασία της ακεραιότητας των συσκευών και της αξιοπιστίας του ηλεκτρικού πλέγματος [113].

Η ομάδα έργου που υλοποιεί μια πλατφόρμα λογισμικού ανοιχτής αρχιτεκτονικής για την έξυπνη φόρτιση οχημάτων EV προτείνει την εφαρμογή ενός αποκεντρωμένου ελεγκτή που υποστηρίζεται από το OCPP σε κάθε σταθμό φόρτισης CS, δηλαδή του ελεγκτή XBOS-V [144]. Οι διάσπαρτοι αποκεντρωμένοι ελεγκτές συντονίζονται από το σύστημα διαχείρισης CSMS και απαλλάσσουν τόσο το CSMS όσο και τους σταθμούς φόρτισης CS από την υπολογιστική υπερφόρτωση. Οι σταθμοί φόρτισης CS δεν χρειάζεται να φέρουν δικτυακές διεπαφές ή να εκτελούν πολύπλοκες διαδικασίες επικοινωνίας.

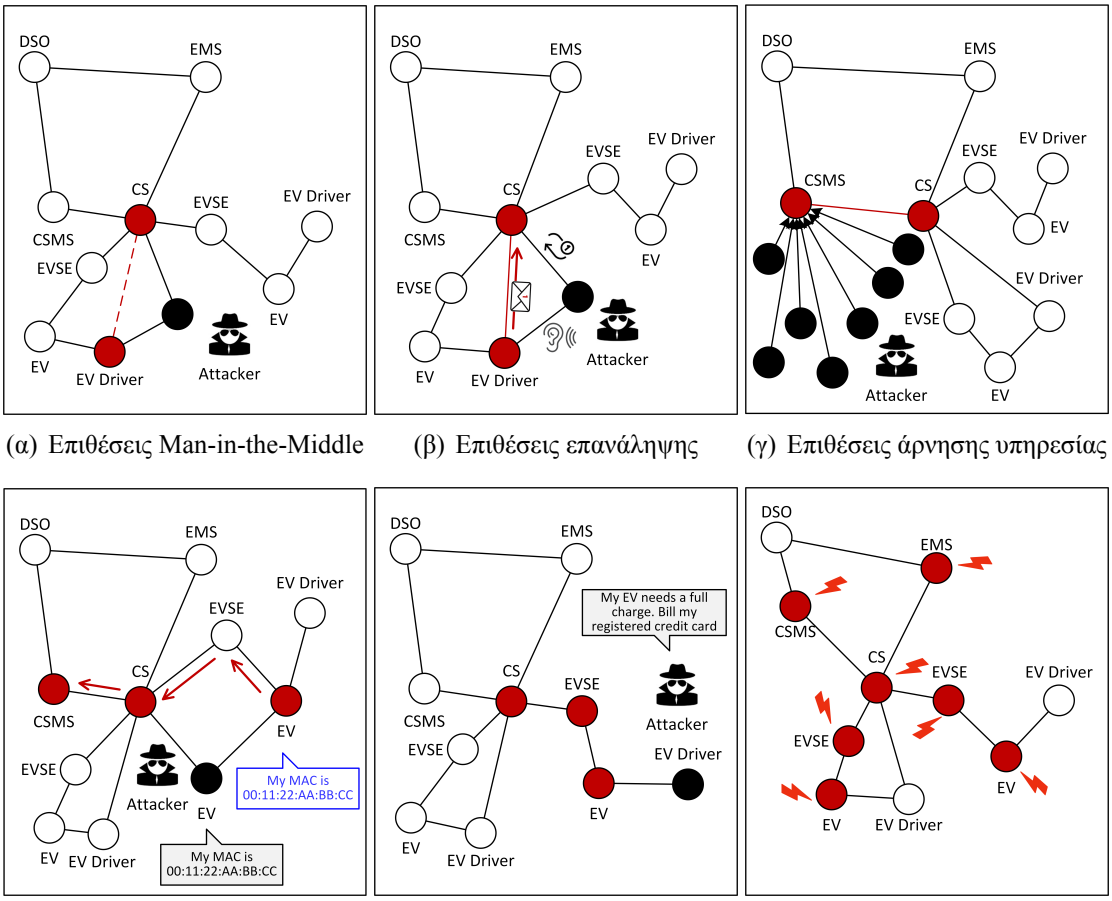
#### 5.2.3.3 Επιθέσεις κατάστασης/αισθητήρων

Καθώς το δίκτυο PEV είναι ευθέως εξαρτώμενο από αισθητήρες, μια υπηρεσία μπορεί να επηρεαστεί ποικιλοτρόπως από κακόβουλες τιμές αισθητήρων. Οι επιθέσεις αισθητήρων (state/sensor) συνήθως οδηγούν σε επιθέσεις έγχυσης ψευδών δεδομένων (False Data Injection Attack, FDIA) [149], επιθέσεις παρεμπόδισης της επικοινωνίας του βαλλόμενου αισθητήρα με τη μονάδα ελέγχου ECU του οχήματος, επιθέσεις εξαπάτησης μέσω GPS ή ακόμα και επιθέσεις άρνησης υπηρεσίας (DoS) κατά της μονάδας ελέγχου ECU του οχήματος [150]. Όλες αυτές οι επακόλουθες επιθέσεις μπορεί επίσης να επηρεάσουν τις επικοινωνίες εντός μιας ECU ή μεταξύ του οχήματος EV και άλλων δρώντων στοιχείων του συστήματος φόρτισης και, επομένως, μπορεί να επηρεάσουν και το πρωτόκολλο OCPP και τις λειτουργίες του. Από όσο γνωρίζει η συγγραφέας, η βιβλιογραφία δεν περιέχει μέχρι στιγμής εργασία ή μελέτη σχετικά με κάποιο αντίμετρο ειδικά για αυτήν τη φυσική επίθεση.

### 5.2.4 Κυβερνοχωρικές επιθέσεις

Η δεύτερη κατηγορία επιθέσεων περιλαμβάνει τις επιθέσεις στον κυβερνοχώρο (Εικόνα 16), δηλαδή τις επιθέσεις που έχουν κυβερνοχωρικές συνέπειες στα περιουσιακά στοιχεία ενός συστήματος φόρτισης οχημάτων EV. Ακολούθως περιγράφονται λεπτομέρειες σχετικά με τις επιθέσεις αυτές, καθώς και σχετικά αντίμετρα.

Στον Πίνακα 9, εμφανίζονται τα αντίμετρα που σχετίζονται με κάθε κυβερνοχωρική επίθεση και τα δρώντα στοιχεία ενός συστήματος φόρτισης οχημάτων EV. Τα στοιχεία δεν σημειώνονται εάν η επίθεση δεν τα επηρεάζει, σημειώνονται ως *Στοχευμένο στοιχείο* εάν η επίθεση τα επηρεάζει και δεν υπάρχει αντίμετρο ή σημειώνονται ως *Προστατευμένο στοιχείο* εάν το προτεινόμενο αντίμετρο προστατεύει το συγκεκριμένο στοιχείο.




(α) Επιθέσεις Man-in-the-Middle (β) Επιθέσεις επανάληψης (γ) Επιθέσεις άρνησης υπηρεσίας

(δ) Πλαστογράφηση ARP (ε) Κλωνοποίηση RKE (στ) Κακόβουλο λογισμικό

Εικόνα 16. Κυβερνοχωρικές επιθέσεις σε δίκτυα φόρτισης PEV

#### 5.2.4.1 Επιθέσεις Man-in-the-Middle

Στο πλαίσιο ενός δικτύου PEV μια Man-in-the-Middle (MitM) επίθεση μπορεί να αναπτυχθεί έχοντας ως σημεία εισόδου τις ευπάθειες και τα τρωτά χαρακτηριστικά ενός ή περισσότερων δρώντων στοιχείων. Μία από αυτές τις περιπτώσεις σημείων εισόδου είναι οι θύρες USB των σταθμών φόρτισης CS, οι οποίες είναι προσβάσιμες από το κοινό. Αυτή η ανοιχτή πρόσβαση στις θύρες USB των σταθμών φόρτισης CS

Πίνακας 9. Κυβερνοχωρικές επιθέσεις και αντίμετρα

| Attacks | Countermeasures | Assets | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Driver | EV | EVSE | CS | EMS | CSMS | Data | Grid |
| MitM | Elliptic-curve keypair for Autocharge [131] | ● | ● | ● | ○ | ○ | ○ | ● | |
| | Decentralized firmware attestation scheme [132],[133] | ○ | ● | ○ | ○ | ○ | ○ | ● | |
| | Direct anonymous attestation protocol [134] | ○ | ● | ● | ○ | ○ | ○ | ● | |
| | EV reservation w/ smart contract [135] | ● | ● | ● | ● | ○ | ○ | ● | |
| | Three-factor authentication protocol [151] | ● | ○ | ○ | ● | ○ | ○ | ● | |
| | Back propagation neural network scheme [152] | ○ | ● | ○ | ● | ○ | ● | ○ | |
| | OCPP *DataTransfer* block [153] | ○ | ○ | ○ | ● | ○ | ● | ● | |
| | Multimodal, multi-pass authentication w/ contract certificate [154] | ● | ● | ● | ○ | ○ | ○ | ● | |
| | Power trading decentralized architecture [155],[156] | ● | ● | ● | ○ | ○ | ○ | ● | |
| Packet replay | Message authentication code [125] | | ● | ○ | ○ | | | ● | |
| | Three-factor authentication protocol [151] | | ○ | ● | ● | | | ● | |
| | Abnormal behavior detection system [157],[158] | | ● | ○ | ○ | | | ● | |
| | BC-enabled EV charging system [159] | | ● | ○ | ● | | | ● | |
| | Distance bounding algorithm [160] | | ● | ● | ○ | | | ● | |
| DoS/DDoS | Three-factor authentication protocol [151] | ● | ○ | ○ | ● | ○ | ○ | ● | |
| | Power trading decentralized architecture [161] | | ● | ● | ● | ○ | ● | ● | ● |
| | Traffic detection, back propagation neural network [162] | ● | ○ | ○ | ● | ○ | ○ | ○ | |
| | BC-based EV bidding protocol [163] | ● | ● | ○ | ● | ○ | ○ | ● | |
| | BC-based distributed ledger technology [164],[165] | ● | ● | ○ | ● | ○ | ○ | ● | |
| ARP spoofing | N/A | | ○ | | ○ | | ○ | ○ | |
| RKE cloning | N/A | | ○ | ○ | ○ | | | | |
| Malware | IDS, SNMP MIBs [113] | | ● | ● | ● | ● | ● | ○ | |
| | Trusted platform module [166] | | ● | ○ | ● | ● | ● | ○ | |

○ Στοχευμένο στοιχείο ● Προστατευόμενο στοιχείο

επιτρέπει στον εισβολέα να αποκτήσει αρχεία καταγραφής και κρίσιμα δεδομένα του ίδιου του σταθμού φόρτισης CS ή και των οχημάτων EV που έχουν εξυπηρετηθεί στον σταθμό αυτό. Επίσης, αυτές οι επιθέσεις μπορεί να έχουν ως αποτέλεσμα την εγκατάσταση κακόβουλου υλικο-λογισμικού ή λογισμικού στο σταθμό φόρτισης ή την αλλαγή του χρονιστή συστήματος του σταθμού, με επίδραση στην ίδια την προσφερόμενη υπηρεσία [42]. Στις περισσότερες περιπτώσεις, ωστόσο, οι επιθέσεις MitM στοχεύουν τις επικοινωνίες μεταξύ των σταθμών φόρτισης CS και του συστήματος διαχείρισης CSMS ή τις επικοινωνίες μεταξύ του οχήματος EV και του σταθμού φόρτισης CS/EVSE [96] καθώς και τα δεδομένα που ανταλλάσσονται σε αυτές.

Τα οχήματα EV είναι επίσης ένα προτιμώμενο σημείο εισόδου για επιθέσεις MitM. Σε αυτές τις περιπτώσεις, οι επιθέσεις εκμεταλλεύονται τις ευπάθειες της μονάδας ελέγχου του οχήματος ECU για να πάρουν τον έλεγχο του οχήματος EV και στη συνέχεια να εξαπλώσουν την επίθεση και στο υπόλοιπο δίκτυο PEV. Το αποκεντρωμένο σχήμα πιστοποίησης υλικο-λογισμικού που προτείνεται στις [132],[133], χρησιμοποιεί τη μνήμη flash και το υλικο-λογισμικό της ίδιας της μονάδας ελέγχου του οχήματος ECU για την προστασία της και για να μετριάσει τις ευπάθειές της.

Οι επιθέσεις MitM στην επικοινωνία μεταξύ των σταθμών φόρτισης CS και του συστήματος διαχείρισης CSMS ενδέχεται να διαρρεύσουν τις πληροφορίες που ανταλλάσσονται σχετικά με την κοστολόγηση της υπηρεσίας, το υλικο-λογισμικό των δρώντων στοιχείων ή/και τις πολιτικές ελέγχου πρόσβασης που εφαρμόζονται από την υπηρεσία. Η προστασία της επικοινωνίας CS-CSMS έναντι των επιθέσεων υποστηρίζεται από τα μηνύματα της λειτουργίας OCPP *DataTransfer* [153] τα οποία

χρησιμοποιούνται για την ανταλλαγή σημαντικών δεδομένων όπως η τιμή του μετρητή, με κρυπτογραφημένο τρόπο. Επιπλέον, τα δεδομένα κατακερματίζονται σε μερίδια και κάθε μερίδιο μεταδίδεται με ξεχωριστό μήνυμα. Έτσι, ένας MitM εισβολέας θα χρειαστεί να συγκεντρώσει και να αποκρυπτογραφήσει όλα τα μερίδια, για να μπορέσει να ανακτήσει τα αρχικά δεδομένα.

Μια επίθεση MitM στην επικοινωνία μεταξύ οχήματος EV και εξοπλισμού σύνδεσης EVSE ενδέχεται να παραβιάσει δεδομένα σχετικά με την τοποθεσία του οχήματος EV, τις οικονομικές πληροφορίες της υπηρεσίας ή του οδηγού/χρήστη του οχήματος EV και τα διαπιστευτήρια ασφάλειας/ταυτότητας του οχήματος ή του οδηγού/χρήστη του. Εάν μια τέτοια επίθεση πετύχει και ο εισβολέας καταφέρει να αποκτήσει συνδεσιμότητα, για παράδειγμα με τον εξοπλισμού σύνδεσης EVSE, τότε μπορεί να προχωρήσει και να κατευθύνει τον εξοπλισμού σύνδεσης EVSE ώστε να διοχετεύει ενέργεια καθώς και δεδομένα προς τον επιτιθέμενο, (γνωστή και ως επίθεση «καταβόθρας» ή sinkhole) ή να επιλέξει τυχαία δρώντα στοιχεία εντός του δικτύου PEV και να αναπτύξει μια κατανεμημένη επίθεση (γνωστή και ως επίθεση «σκουληκότρυπας» ή wormhole) [40].

Για την αντιμετώπιση του προβλήματος αυτών των επιθέσεων, προτάθηκε ένα σύστημα πολυτροπικού ελέγχου της ταυτότητας πολλαπλών διελεύσεων με χρήση πιστοποιητικού σύμβασης (Multimodal and Multi-pass Authentication using Contract Certificate, MMA-CC) [154]. Με τη χρήση του προτεινόμενου MMA-CC, μια υπηρεσία χρέωσης ενεργοποιείται μόνο για ένα ηλεκτρικό όχημα με έγκυρο πιστοποιητικό σύμβασης, το οποίο υποβάλλεται μαζί με τα διαπιστευτήρια του οδηγού/χρήστη του οχήματος EV. Η επικοινωνία EV-CS μπορεί να προστατευτεί και μέσω μιας αποκεντρωμένης αρχιτεκτονικής για τη διαπραγμάτευση της ηλεκτρικής φόρτισης οχήματος EV, που βασίζεται στο blockchain [155],[156], όπου η ψηφιακή υπογραφή του εμπόρου/παρόχου είναι ενσωματωμένη στα δεδομένα και στη συνέχεια κρυπτογραφείται με το δημόσιο κλειδί του πελάτη. Το πρωτόκολλο άμεσης ανώνυμης πιστοποίησης DAA και μια μονάδα αξιόπιστης πλατφόρμας TPM που βρίσκεται εντός οχήματος [134] προτείνονται για τον μετριασμό των επιθέσεων MitM κατά την επικοινωνία μεταξύ του ενσωματωμένου ελεγκτή επικοινωνίας του οχήματος EVCC και του ελεγκτή επικοινωνίας εξοπλισμού παροχής ενέργειας SECC, με την εισαγωγή κρυπτογράφησης και διαδικασιών εξουσιοδότησης. Επιπλέον, μια δομή φόρτισης οχημάτων EV που βασίζεται σε blockchain μπορεί να ενεργοποιήσει την επικοινωνία μεταξύ οχήματος και σταθμού φόρτισης EV-CS χωρίς να διαχέονται ευαίσθητες πληροφορίες της επικοινωνίας αυτής σε τρίτα δρώντα στοιχεία, με τη χρήση έξυπνων συμβολαίων [135].

Μία τεχνική αντιμετώπισης αυτών των επιθέσεων για την προστασία της επικοινωνίας μεταξύ του οχήματος και του σταθμού φόρτισης EV-CS, καθώς και των μηνυμάτων αρχικοποίησης SLAC που ανταλλάσσουν αυτά τα δύο δρώντα στοιχεία, είναι η πρόταση για τη χρήση ενός προσωρινού ζεύγους κλειδιών, παραγόμενου με τη μέθοδο κρυπτογράφησης Elliptic-Curve, μέχρι να παραχθεί και να κοινοποιηθεί και στα δύο μέρη το μόνιμο κλειδί της μεταξύ τους συνεδρίας [131]. Με την εφαρμογή του ζεύγους κλειδιών Elliptic-Curve προστατεύονται το όχημα, ο οδηγός του οχήματος EV και τα διαπιστευτήριά τους κατά την επικοινωνία EV-CS. Αυτές οι διαπραγματεύσεις που λαμβάνουν χώρα πριν τις διαδικασίες κοστολόγησης/χρέωσης, μπορεί να προστατευτούν με τη χρήση του πρωτοκόλλου ελέγχου της ταυτότητας τριών παραγόντων [151]. Ωστόσο, αυτό το πρωτόκολλο έχει σχεδιαστεί κυρίως για την εσωτερική επικοινωνία του σταθμού

φόρτισης EVSE-CS.

Η ασφάλεια του OCPP βασίζεται σε πρωτόκολλα χαμηλότερου επιπέδου, όπως στο TLS, το οποίο με τη σειρά του δεν είναι απολύτως θωρακισμένο κατά των επιθέσεων MitM. Ειδικά στο πλαίσιο της διαφύλαξης της ασφάλειας του OCPP, το TLS δεν επαρκεί, καθώς [167]:

*(α)* δεν παρέχει μακροπρόθεσμη πιστοποίηση αυθεντικότητας ή δυνατότητα αναποκηρυξίας με μακροπρόθεσμη επίδραση,

*(β)* δεν παρέχει ασφαλή επικύρωση πιστοποιητικών,

*(γ)* προκαλεί αύξηση του υπολογιστικού φόρτου, και

*(δ)* επιτρέπει τη μετάδοση δεδομένων πληρεξούσιων μέσω απλού κειμένου.

Κατά των επιθέσεων MitM, έχει προταθεί και ένα σχήμα Back Propagation Neural Network (BPNN) που θα πρέπει φιλοξενείται από το σύστημα διαχείρισης CSMS της υπηρεσίας φόρτισης [152]. Το BPNN μπορεί να ανιχνεύσει μια επίθεση MitM αναλύοντας τα αιτήματα φόρτισης/εκφόρτισης που συγκεντρώνει το CSMS και μπορεί να μετριάσει την επίθεση με τεχνητή καθυστέρηση ή επιβολή μιας απόφασης για απόρριψη του αιτήματος.

#### 5.2.4.2 Επιθέσεις επανάληψης

Μία από τις απειλές κατά του πρωτοκόλλου OCPP είναι η αποκάλυψη δεδομένων. Στην επίθεση με αποκάλυψη δεδομένων, ένας εισβολέας μπορεί να αντιγράψει, να διαβάσει ή να αναπαραγάγει ευαίσθητες πληροφορίες σχετικά με το όχημα EV και τον οδηγό/χρήστη του. Αυτές οι πληροφορίες μπορεί να χρησιμοποιηθούν κακόβουλα για οικονομικά οφέλη [96]. Αυτές οι πληροφορίες αντλούνται συνήθως με υποκλοπή/λαθρακρόαση ή με επίθεση επανάληψης πακέτων (packet replay), όπου ο επιτιθέμενος παρεμποδίζει την επικοινωνία μεταξύ οχήματος EV και διεπαφής φόρτισης EVSE μέσω καθυστερήσεων. Αυτές οι καθυστερήσεις οδηγούν σε επαναλήψεις (αποστολής) πακέτων, οι οποίες διακυβεύουν το επίκαιρο των μηνυμάτων OCPP. Οι επιθέσεις επανάληψης ενδέχεται να προκύψουν όταν τα μηνύματα που ανταλλάσσονται δεν είναι κρυπτογραφημένα και/ή δεν έχουν επικυρωθεί.

Για την προστασία από αυτούς τους τύπους επιθέσεων, η μέθοδος επαλήθευσης ταυτότητας των μηνυμάτων Message Authentication Code (MAC) μπορεί να χρησιμοποιηθεί [125] για να διασφαλίσει τη δικτυακή κίνηση του δικτύου αισθητήρων του οχήματος EV (Controller Area Network, CAN), όταν αυτή πραγματοποιείται μεταξύ των μονάδων ελέγχου του οχήματος ECU. Ωστόσο, η μέθοδος MAC συχνά δεν χωράει στα τυπικά πεδία δεδομένων του πρωτοκόλλου CAN, τα οποία επιτρέπουν μηνύματα έως και 8 bytes. Επιπλέον, τα μηνύματα CAN μεταδίδονται σε όλους τους κόμβους (broadcast) χωρίς διάκριση ή δυνατότητα περιορισμού της μετάδοσης σε συγκεκριμένους κόμβους, πράγμα που σημαίνει ότι είναι ευάλωτα σε επιθέσεις υποκλοπής/λαθρακρόασης ή μεταμφίεσης. Ένα σύστημα ανίχνευσης εισβολών (Intrusion Detection System, IDS) [157],[158] που προτείνεται με τη δυνατότητα αναγνώρισης μη φυσιολογικής συμπεριφοράς, μπορεί να προσφέρει μια εναλλακτική ή ένα συμπλήρωμα στη μέθοδο MAC.

Αυτό το είδος επίθεσης μπορεί να μετριαστεί με εφαρμογή διάφορων τεχνικών. Ένα πρωτόκολλο ελέγχου της ταυτότητας τριών παραγόντων μπορεί να χρησιμοποιηθεί για τις προ-φόρτισης διαπραγματεύσεις μεταξύ του εξοπλισμού σύνδεσης EVSE και του σταθμού φόρτισης CS [151]. Ένα πλαίσιο ανίχνευσης ανωμαλιών με ενσωμάτωση τεχνικών μηχανικής μάθησης ή βασιζόμενο σε ένα νευρωνικό δίκτυο διάδοσης, μπορεί να χρησιμοποιηθεί για τον εντοπισμό κακόβουλης δικτυακής κίνησης πακέτων OCPP [162]. Συγκεκριμένα, σε περίπτωση που υπάρχει η ίδια έκδοση του πρωτοκόλλου OCPP τόσο στον σταθμό φόρτισης CS όσο και στο σύστημα διαχείρισης CSMS, η ομοιότητα μεταξύ δύο διαδοχικών αιτημάτων και αποκρίσεων μπορεί να αξιολογηθεί για να φανεί εάν ένα ζεύγος αιτήματος/απόκρισης είναι έγκυρο. Έτσι, ο παραβιασμένος σταθμός φόρτισης μπορεί να εντοπιστεί και να εξαιρεθεί από τη διαδικασία φόρτισης.

Αυτός ο τύπος κυβερνοεπίθεσης μπορεί επίσης να μετριαστεί με τον έλεγχο ταυτότητας των μηνυμάτων OCPP μέσω του πρωτοκόλλου TLS, το οποίο προστατεύει την επικοινωνία μεταξύ του οχήματος EV και του εξοπλισμού σύνδεσης EVSE. Εάν εφαρμοστεί το πρωτόκολλο TLS, η κρυπτογράφηση των μηνυμάτων με χρήση ασύμμετρου κλειδιού θα αποτρέψει την υποκλοπήλαθρακρόαση της συνεδρίας και την πειρατεία [42]. Ωστόσο, το TLS εισάγει ανεπιθύμητο πρόσθετο υπολογιστικό φόρτο, ειδικά για την επικοινωνία μέσω δικτύων κινητής τηλεφωνίας. Έτσι, ένα πλαίσιο βασισμένο σε blockchain για διαχείριση κρατήσεων από τα οχήματα EV με χρήση έξυπνου συμβολαίου θα ήταν χρήσιμο για την επαλήθευση ταυτότητας του οχήματος EV και του σταθμού φόρτισης CS. Επομένως, έγκυρες πληροφορίες και μηνύματα δεν θα αναπαραχθούν ή υποκλαπούν/λαθρακουστούν [135]. Ένα τέτοιο σύστημα φόρτισης οχημάτων EV με δυνατότητα blockchain προτάθηκε στο [159], όπου δίνεται έμφαση στη μείωση του φόρτου στο δίκτυο, στην αύξηση της ποιότητας εξυπηρέτησης των χρηστών και στη διασφάλιση της προστασίας. Σε αυτά τα συστήματα, το όχημα EV και ο σταθμός φόρτισης CS μπορούν να αυτό-επικυρωθούν με παραγωγή τυχαίων αριθμών, που χρησιμοποιούνται άμεσα και για μικρό χρονικό διάστημα μετά την παραγωγή τους. Ωστόσο, τέτοιες υλοποιήσεις δεν διαθέτουν την ευελιξία προσαρμογής στις διαρκώς μεταβαλλόμενες προτιμήσεις του οδηγού/χρήστη του οχήματος EV και στις δυναμικά μεταβαλλόμενες συνθήκες του δικτύου φόρτισης. Έτσι, για ένα προστατευμένο δίκτυο φόρτισης PEV, η τεχνητή νοημοσύνη AI και το Blockchain θα πρέπει να αλληλοσυμπληρώνονται. Ένας αλγόριθμος οριοθέτησης απόστασης [160] προτείνεται για την αντιμετώπιση επιθέσεων επανάληψης πακέτων στην επικοινωνία οχήματος EV και εξοπλισμού σύνδεσης EVSE, ο οποίος εκμεταλλεύεται τις χρονικές καθυστερήσεις που δημιουργούνται από την επίθεση στις ροές επικοινωνίας, ώστε να την αποτρέψει ή να την ανακόψει.

Μια επίθεση επανάληψης πακέτων θα μπορούσε επίσης να μετριαστεί με τη χρήση πρωτοκόλλων ελέγχου της ταυτότητας που βασίζονται σε χρήση κλειδιών κατά τις προ της φόρτισης διαπραγματεύσεις μεταξύ του εξοπλισμού σύνδεσης EVSE και του σταθμού φόρτισης CS [151].

#### 5.2.4.3 Επιθέσεις άρνησης υπηρεσίας

Το κύριο πρόβλημα για την υποδομή ενός έξυπνου πλέγματος (smart grid, SG) είναι η βέλτιστη αντιμετώπιση προβλημάτων που σχετίζονται με τον σχεδιασμό δικτύου και η γεφύρωση του υφιστάμενου χάσματος μεταξύ των απαιτήσεων

ασφάλειας/ανθεκτικότητας και της παροχής επικοινωνιών έξυπνου πλέγματος SG με χαμηλό κόστος. Οι απαιτήσεις ασφάλειας ικανοποιούνται από την παρακολούθηση των επικοινωνιών εντός του έξυπνου πλέγματος SG με σύστημα ανίχνευσης IDS, ενώ οι απαιτήσεις ανθεκτικότητας εκφράζονται με την ικανότητα του έξυπνου πλέγματος SG να λειτουργεί παρουσία διαταραχών, όπως διακοπές ρεύματος ή κυβερνοεπιθέσεις. Η επιβάρυνση του έξυπνου πλέγματος SG από τη χρήση συστημάτων ανίχνευσης εισβολών IDS και τη χρήση ικανού αριθμού συναθροιστών (aggregators) μπορεί να μελετηθεί με βάση τρία στοιχεία: την κατανάλωση ενέργειας κάθε συναθροιστή, το κόστος των συναθροιστών και των ηλεκτρονόμων (relays) και η σχετική προκαλούμενη καθυστέρηση [168]. Η χρήση του πρωτοκόλλου TLS/SSL (Secure Sockets Layer, SSL) σε συνδυασμό με τα πρωτόκολλα Hypertext Transfer Protocol Secure (HTTPS) και WebSocket Secure (WSS) προτείνεται για τη διασφάλιση της επικοινωνίας εντός του έξυπνου πλέγματος SG [162]. Ωστόσο, η χρήση του TLS αυξάνει τον υπολογιστικό φόρτο ιδίως για τους σταθμούς φόρτισης CS που χρησιμοποιούν ένα κυψελοειδές δίκτυο επικοινωνίας. Ακόμη και με τη χρήση ασφαλούς σύνδεσης, οι βασικές απαιτήσεις, όπως η ασφάλεια από άκρο σε άκρο και η δυνατότητα αναποκηρυξίας, δεν είναι πάντα εγγυημένες.

Σοβαρές απειλές στο έξυπνο πλέγμα είναι οι επιθέσεις άρνησης υπηρεσίας DoS και οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας (Distributed Denial-of-service, DDoS) που απειλούν σοβαρά τη διαθεσιμότητα των πόρων επικοινωνίας ενός προηγμένου δικτύου μετρητών (Advanced Metering Infrastructure, AMI). Αυτές οι επιθέσεις στοχεύουν το σύστημα διαχείρισης CSMS, τους σταθμούς φόρτισης CS και τις συνδέσεις επικοινωνίας εντός της υπηρεσίας που χρησιμοποιούν το πρωτόκολλο OCPP. Τα διάφορα ηλεκτρικά οχήματα που συμμετέχουν στη διαδικασία φόρτισης μπορεί να χρησιμοποιηθούν από έναν εισβολέα για να ξεκινήσει μια επίθεση DoS ή DDoS πλημμυρίζοντας το δίκτυο με ψεύτικα/περιττά αιτήματα φόρτισης και δέσμευση χρονοθυρίδων της υπηρεσίας. Αυτός ο τύπος επίθεσης υπερφορτώνει τα χρονοδιαγράμματα φόρτισης των σταθμών CS και τους αποτρέπει από τη δυνατότητα να εξυπηρετήσουν καλόβουλα αιτήματα οχημάτων EV [42]. Επιπλέον, οι επιθέσεις αυτές μπορεί να επηρεάσουν τα κανάλια επικοινωνίας μέσω της διεπαφής EVSE αναστέλλοντας τη φόρτιση ή διακόπτοντας τις υπηρεσίες δικτύου και, πιθανώς, προξενώντας ένα ασταθές δίκτυο. Αυτό το είδος κυβερνοεπίθεσης είναι μια ειδική επίθεση τύπου διακοπής που υπερκερνάει τη διαγραφή ή την απόρριψη μηνυμάτων. Ορισμένες υποκατηγορίες επιθέσεων DoS, όπως οι επιθέσεις «γκρίζας τρύπας» (δηλαδή μόνο την επιλεκτική προώθηση πακέτων στον επόμενο κόμβο ή hop) ή οι επιθέσεις «μαύρης τρύπας» (δηλαδή την απόρριψη όλων των πακέτων), ενδέχεται να επηρεάσουν σοβαρά τη λειτουργικότητα του πρωτοκόλλου OCPP [40].

Το πρωτόκολλο φόρτισης οχημάτων EV θα πρέπει να περιλαμβάνει διεργασίες για ένα σενάριο στο οποίο το όχημα EV θέτει προ-κράτηση για ένα χρονικό διάστημα φόρτισης σε ένα σταθμό φόρτισης CS, κοινοποιώντας τις ευαίσθητες πληροφορίες του στον σταθμό φόρτισης και, μέσω αυτού, στην αξιόπιστη κεντρική διαχείριση (δηλαδή το σύστημα διαχείρισης CSMS). Το CSMS και ο σταθμός φόρτισης CS λαμβάνουν τις αποφάσεις σχετικά με την κράτηση υπηρεσίας [163]. Επιπλέον, αξιόπιστα τρίτα μέρη ή κεντρικά συστήματα της υπηρεσίας αναμένεται επίσης να χειρίζονται τις πληροφορίες του οχήματος EV. Έτσι, η ασφάλεια και το απόρρητο του οχήματος EV έχουν σε μεγάλο βαθμό παρακαμφθεί. Αυτές οι ιδιωτικές πληροφορίες ενδέχεται να διαγραφούν ή να απορριφθούν από έναν κακόβουλο εισβολέα που πραγματοποιεί επίθεση DoS. Μια σημαντική ερευνητική πρόκληση είναι πώς ένα μεμονωμένο όχημα EV θα μπορούσε να

κάνει μια αποτελεσματική επιλογή σταθμού φόρτισης CS με αποκεντρωμένο τρόπο, χωρίς να διαχέει τις ευαίσθητες πληροφορίες του ούτε προς τον σταθμό φόρτισης CS ούτε προς άλλες οντότητες του δικτύου.

Προκειμένου να αντιμετωπιστούν τα προαναφερθέντα προβλήματα απορρήτου και ασφάλειας, προτείνεται η χρήση τεχνητής νοημοσύνης AI για τον εντοπισμό τόσο της τυχαίας όσο και της άσκοπης δικτυακής κίνησης με τη χρήση ενός μόνο νευρωνικού δικτύου [162]. Έχει προταθεί ένα πρωτόκολλο επαλήθευσης της ταυτότητας τριών παραγόντων [151] για τις προ-φόρτισης διαπραγματεύσεις μεταξύ του εξοπλισμού σύνδεσης EVSE και του σταθμού φόρτισης CS. Σε άλλες περιπτώσεις, προτείνεται η χρήση της blockchain τεχνολογίας κατανεμημένου καθολικού (Distributed Ledger Technology, DLT) [164],[165]. Πιο συγκεκριμένα, μια επίθεση DoS μπορεί να μετριαστεί χρησιμοποιώντας ένα blockchain κατανεμημένο πρωτόκολλο αποτελεσματικής επιλογής σταθμού φόρτισης CS για να διασφαλιστεί το απόρρητο των δεδομένων των οχημάτων EV, η διαθεσιμότητα των προ-δεσμευμένων χρονοθυρίδων στους σταθμούς φόρτισης CS και η υψηλή ποιότητα υπηρεσίας. Αυτή η λύση τύπου blockchain για τη φόρτιση οχημάτων EV επιτρέπει στα οχήματα να επικοινωνούν με τους σταθμούς φόρτισης CS χωρίς να μοιράζονται ευαίσθητες πληροφορίες, χρησιμοποιώντας κάποιο έξυπνο συμβόλαιο ή δεσμευτικά σχήματα με ιδιότητες απόκρυψης, όσο λαμβάνουν χώρα οι διαπραγματεύσεις για την τιμολόγηση της υπηρεσίας μεταξύ του οχήματος και του σταθμού φόρτισης CS [135],[139]. Μπορεί, επίσης, να χρησιμοποιηθεί το μερικώς αποκεντρωμένο Consortium BC [161]. Σε αυτή τη λύση, μόνο τμήματα των διακριτικών και των πόρων των εξουσιοδοτημένων κόμβων συμμετέχουν στη διαδικασία επίτευξης συναίνεσης, βελτιώνοντας έτσι την αποτελεσματικότητα της διαδικασίας. Το Consortium BC μπορεί επίσης να αντιμετωπίσει επιθέσεις πλαστοπροσωπίας, στις οποίες είναι ευάλωτο το πρωτόκολλο OCPP, όπου ένας εισβολέας προσποιείται ότι είναι ο σταθμός φόρτισης CS ή το σύστημα διαχείρισης CSMS.

#### 5.2.4.4 Επιθέσεις πλαστογράφησης ARP

Στην επίθεση πλαστογράφησης μηνυμάτων του πρωτοκόλλου Address Resolution Protocol (ARP), ο εισβολέας χειρίζεται τα μηνύματα ARP για να συσχετίσει τη δική του διεύθυνση MAC με μια νόμιμη διεύθυνση IP και να λάβει δεδομένα που προορίζονται για την πλαστογραφημένη αυτή διεύθυνση IP. Στην περίπτωση επίθεσης πλαστογράφησης ARP, οι πληροφορίες του δικτύου PEV σχετικά με τον σταθμό φόρτισης CS (όπως τοποθεσία, διαθεσιμότητα, κατάσταση, προφίλ φόρτισης, χρονοδιαγράμματα) και το όχημα EV (δηλαδή τοποθεσία, αναγνωριστικό ή άλλα διαπιστευτήρια αναγνώρισης) ενδέχεται να εκτεθούν [118]. Αυτή η επίθεση ακεραιότητας της δικτυακής κίνησης ακολουθείται συνήθως από μια επίθεση MitM, όπου ο κόμβος MitM είναι αυτός που διαπράττει την πλαστογράφηση ARP [125].

Αν και η πλαστογράφηση ARP αναδεικνύεται ως κυβερνοεπίθεση στα δρώντα στοιχεία του δικτύου PEV, δεν έχουν προκύψει ή προταθεί, μέχρι στιγμής, αντίμετρα ειδικά για το πρωτόκολλο OCPP ή για το δίκτυο PEV. Η πλαστογράφηση ARP στα δίκτυα PEV αντιμετωπίζεται επί του παρόντος χρησιμοποιώντας τα συμβατικά αντίμετρα για τον εντοπισμό μιας τέτοιας επίθεσης, δηλαδή με χρήση των εικονικών δικτύων Virtual Private Networks (VPN) και στατικών ARP, και με τεχνικές όπως η χρήση συστημάτων ανίχνευσης εισβολών IDS και το φιλτράρισμα πακέτων.

#### 5.2.4.5 Κλωνοποίηση κωδικών απομακρυσμένης εισόδου

Τα συστήματα Remote Keyless Entry (RKE) επιτρέπουν την πρόσβαση χωρίς κλειδί σε ένα όχημα EV, τόσο για τον οδηγό του οχήματος όσο, δυστυχώς και για έναν πιθανό εισβολέα. Η πρόσβαση σε ένα όχημα EV που υποστηρίζεται από RKE γίνεται με ένα πάτημα κουμπιού, το οποίο ενεργοποιεί ένα σήμα κυλιόμενα εναλλασσόμενου κωδικού. Ωστόσο, τα σχήματα κυλιόμενων εναλλασσόμενων κωδικών μπορεί να υποκλαπούν και, επομένως, το όχημα EV είναι ευάλωτο σε επίθεση κλωνοποίησης RKE [125]. Μια επίθεση κατά των συστημάτων RKE στοχεύει κυρίως τους αισθητήρες του οχήματος EV. Όσο πιο αυτόνομο είναι ένα όχημα EV, τόσο πιο επικίνδυνη μπορεί να αποδειχθεί μια τέτοια επίθεση [47]. Κατά συνέπεια, και οι λειτουργίες του OCPP επηρεάζονται από τις επιθέσεις κλωνοποίησης RKE, όταν ένα παραβιασμένο όχημα EV εισέρχεται και συνδέεται στο δίκτυο PEV.

#### 5.2.4.6 Επιθέσεις κακόβουλου λογισμικού

Ένα σύστημα φόρτισης οχημάτων EV βασίζεται στην ασφαλή και αδιάλειπτη επικοινωνία μεταξύ των δρώντων στοιχείων του, δηλαδή του οχήματος EV, του εξοπλισμού σύνδεσης EVSE, των σταθμών φόρτισης CS και του συστήματος διαχείρισης CSMS [8]. Όλες αυτές οι οντότητες ενδέχεται να δεχθούν επίθεση από κακόβουλο λογισμικό (malware) που μπορεί να οδηγήσει σε κλοπή ενέργειας, διαρροή δεδομένων ή άρνηση υπηρεσίας. Οι τρεις πρώτες οντότητες είναι ακόμη πιο πιθανό να δεχθούν επίθεση με χρήση κακόβουλου λογισμικού, λόγω της φυσικής έκθεσής τους και της ευκολίας πρόσβασης σε αυτές από οποιονδήποτε και άρα και από έναν εισβολέα. Μια επίθεση κακόβουλου λογισμικού είναι πιο πιθανό να εκτελεστεί από κάποιον που έχει φυσική πρόσβαση ή προνομιακό λογαριασμό πρόσβασης στο δίκτυο PEV, δηλαδή να πρόκειται για μια εσωτερική επίθεση (insider attack) [118].

Δύο περιπτώσεις τέτοιων επιθέσεων στον κυβερνοχώρο που βασίζονται σε κακόβουλο λογισμικό περιγράφονται ως επίθεση για τη μείωση του κόστους και επίθεση για πρόκληση υψηλού ενεργειακού φορτίου [169]. Στην επίθεση για μείωση κόστους, ο εισβολέας παραπλανά τους μελλοντικούς πελάτες του δικτύου PEV, ενημερώνοντάς τους για αυξημένη τιμή κόστους ρεύματος για το χρονικό διάστημα που θέλει εκείνος να φορτίσει και αποθαρρύνοντάς τους να επιδιώξουν πρόσβαση στην υπηρεσία ταυτόχρονα με αυτόν. Η προκαλούμενη μείωση της ζήτησης έχει ως συνέπεια τη μείωση της πραγματικής τιμής κόστους της ηλεκτρικής ενέργειας για τα συγκεκριμένα χρονικά διαστήματα και ο εισβολέας επιτυγχάνει να εξυπηρετηθεί με αυτό το μειωμένο κόστος. Στην επίθεση για την πρόκληση υψηλού ενεργειακού φορτίου, ο εισβολέας προσδιορίζει ένα χρονικό διάστημα αιχμής της ενεργειακής κατανάλωσης και παραπλανά τους επίδοξους πελάτες του δικτύου PEV δείχνοντάς τους μια χαμηλή τιμή κόστους της ηλεκτρικής ενέργειας για το χρονικό αυτό διάστημα, ενθαρρύνοντάς τους να επιδιώξουν φόρτιση σε εκείνη τη χρονική περίοδο. Αυτό έχει ως αποτέλεσμα την αύξηση του ενεργειακού φορτίου κατά τη διάρκεια της περιόδου αιχμής και μπορεί να οδηγήσει σε υπερφόρτωση ισχύος.

Για τον εντοπισμό κακόβουλου λογισμικού σε ένα δίκτυο PEV, μπορεί να χρησιμοποιηθούν τα συστήματα ανίχνευσης εισβολών IDS και οι μέθοδοι παρακολούθησης με χρήση των βάσεων δεδομένων Simple Network Management Protocol (SNMP) και Management Information Base (MIB) (IEC 62351-7) [113]. Εάν το

κακόβουλο λογισμικό χρησιμοποιεί τον εξοπλισμό σύνδεσης EVSE ως σημείο εισόδου, η επικοινωνία εντός του δικτύου PEV πιθανότατα θα διακοπεί, ενώ η υπηρεσία φόρτισης θα συνεχίσει να λειτουργεί με βάση τις τοπικές προεπιλεγμένες λειτουργίες του EVSE [113]. Οι Gharaibeh et al. [166] προτείνουν τη χρήση μονάδας αξιόπιστης πλατφόρμας TPM, που λειτουργεί κατ' αποκλειστικότητα για τις ανάγκες κρυπτογράφησης και η οποία θα λειτουργεί επικουρικά στο υπό προστασία σύστημα. Η TPM ελέγχει το σύστημα σε κάθε εκκίνησή του και αποτρέπει την εκκίνηση εάν εντοπιστεί οποιαδήποτε αλλαγή.

### 5.2.5 Κυβερνοφυσικές επιθέσεις

Η τελευταία κατηγορία επιθέσεων, οι κυβερνοφυσικές επιθέσεις (Εικόνα 17), περιλαμβάνει τις επιθέσεις που έχουν κυβερνοφυσικές επιπτώσεις στα περιουσιακά στοιχεία ενός συστήματος φόρτισης οχημάτων EV ή τις επιθέσεις των οποίων ο τύπος, δηλαδή ο τρόπος εκδήλωσής τους, είναι κυβερνοφυσικός. Ακολούθως περιγράφονται λεπτομέρειες σχετικά με τις επιθέσεις αυτές, καθώς και σχετικά αντίμετρα.

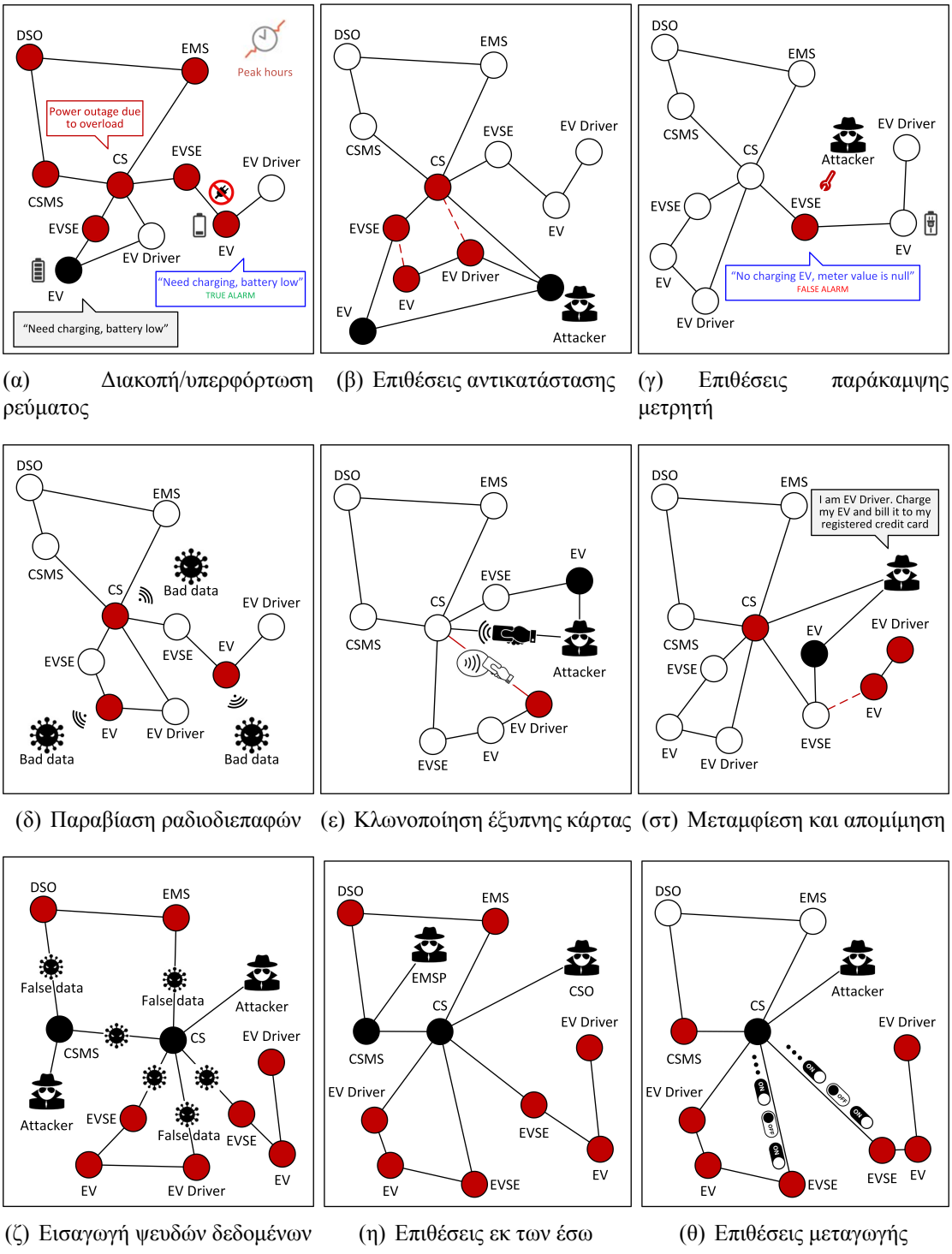
Στον Πίνακα 10, εμφανίζονται τα αντίμετρα που σχετίζονται με κάθε κυβερνοφυσική επίθεση και τα δρώντα στοιχεία ενός συστήματος φόρτισης οχημάτων EV. Τα στοιχεία δεν σημειώνονται εάν η επίθεση δεν τα επηρεάζει, σημειώνονται ως *Στοχευμένο στοιχείο* εάν η επίθεση τα επηρεάζει και δεν υπάρχει αντίμετρο ή σημειώνονται ως *Προστατευμένο στοιχείο* εάν το προτεινόμενο αντίμετρο προστατεύει το συγκεκριμένο στοιχείο.

#### 5.2.5.1 Επιθέσεις διακοπής/υπερφόρτωσης ρεύματος

Τόσο το δίκτυο ηλεκτρικής ενέργειας όσο και το δίκτυο PEV είναι ευάλωτα σε κυβερνοφυσικές επιθέσεις. Η διακοπή ρεύματος (power outage) μπορεί να είναι αποτέλεσμα μιας κυβερνοφυσικής επίθεσης και προκαλεί τη μη διαθεσιμότητα της υπηρεσίας φόρτισης και, ως εκ τούτου, προβλήματα κινητικότητας και ενεργειακής αυτονομίας των οχημάτων EV. Η υπερφόρτωση τάσης (power overload) είναι η άλλη όψη του ίδιου νομίσματος, όπου ο επιτιθέμενος στοχεύει στην αύξηση του ενεργειακού φορτίου για να διαταράξει την ισορροπία στο τοπικό μικρο-πλέγμα (δηλαδή στο τοπικό τμήμα του δικτύου ηλεκτρικής ενέργειας), προκαλώντας κατάσταση πλήρους διακοπής ηλεκτροδότησης (blackout) και, ως εκ τούτου, καταστρέφοντας την ενεργειακή υποδομή [169]. Η κλοπή ενέργειας είναι μια υποκατηγορία αυτών των επιθέσεων, στην οποία ο επιτιθέμενος έχει ως κύριο στόχο να πληρώσει λιγότερο από την πραγματική αξία της ενέργειας που καταναλώνει [170]. Η υπερφόρτωση θεωρείται, επίσης, κυβερνοφυσική επίθεση. Οι επιχειρήσεις ηλεκτρισμού μοιράζονται δημόσια πληροφορίες σχετικά με το δίκτυο (όπως αρχεία καταγραφής ή ανακοινώσεις διακοπών, προγράμματα συντήρησης, αναβαθμίσεων και εγκαταστάσεων) σε πραγματικό χρόνο. Αυτά τα δεδομένα, αν εκτεθούν, μπορεί να χρησιμοποιηθούν στην περίπτωση εξ' αποστάσεως επιθέσεων κατά του δικτύου [190].

**Προστασία του μικρο-πλέγματος**

Ο διαρκώς αυξανόμενος αριθμός ηλεκτρικών οχημάτων και η επικείμενη αύξηση των ενεργειακών αναγκών που θα προκύψουν απαιτούν βελτιωμένες δικτυακές υποδομές και ευέλικτη παραγωγή ενέργειας, που να ενσωματώνει ενεργειακούς πόρους παραγόμενους




(α) Διακοπή/υπερφόρτωση ρεύματος (β) Επιθέσεις αντικατάστασης (γ) Επιθέσεις παράκαμψης μετρητή

(δ) Παραβίαση ραδιοδιεπαφών (ε) Κλωνοποίηση έξυπνης κάρτας (στ) Μεταμφίεση και απομίμηση

(ζ) Εισαγωγή ψευδών δεδομένων (η) Επιθέσεις εκ των έσω (θ) Επιθέσεις μεταγωγής

Εικόνα 17. Κυβερνοφυσικές επιθέσεις σε δίκτυα φόρτισης PEV

με συμβατικό τρόπο (όπως καύση ορυκτών) καθώς και μέσω ανανεώσιμων πηγών ενέργειας. Σε αυτό το πνεύμα, οι Uhlig et al. [171] και Kubis et al. [172] προτείνουν ένα αυτόνομο σύστημα, συγκεκριμένα το InGO, για την ενίσχυση του μικρο-πλέγματος. Το InGO διαχωρίζει το δίκτυο ηλεκτρικής ενέργειας (ή πλέγμα) σε μικρο-πλέγματα χαμηλής τάσης και, λειτουργικώς, ανεξάρτητα.

Πίνακας 10. Κυβερνοφυσικές επιθέσεις και αντίμετρα

| Attacks | Countermeasures | Assets | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Driver | EV | EVSE | CS | EMS | CSMS | Data | Grid |
| Power outage/ overload | Independent system operator [118] | | ● | ● | ● | ● | ● | ○ | ● |
| | Anomaly detection w/ regression decision trees [169] | | ● | ● | ● | ● | ● | ○ | ○ |
| | Consumption pattern-based energy theft detector [170] | | ○ | ○ | ● | ● | ○ | ○ | ● |
| | Autonomous grid operation system w/ firewall [171],[172] | | ○ | ○ | ○ | ○ | ○ | ○ | ● |
| | Charging distributed decision-making algorithm [173] | | ● | ● | ● | ● | ● | ○ | ○ |
| | Supplemental reserve capacity & limited SOC [174] | | ○ | ○ | ○ | ○ | ○ | ○ | ● |
| | Distributed energy resources model optimizer [100] | | ● | ● | ● | ● | ● | ○ | ● |
| | Outage and restoration management [114] | | ● | ● | ● | ● | ● | ○ | ● |
| | Outage management system [116],[175] | | ● | ● | ● | ● | ● | ○ | ● |
| | Physical control pilot conductor [176] | | ● | ● | ○ | ○ | ○ | ○ | ● |
| | Interval observers [149] | | ● | ● | ● | ○ | ● | ● | ● |
| | OCPP-encrypted CS-CSMS communication [177] | | ● | ● | ● | ○ | ● | ● | ● |
| | SOC-aware software-defined controller [178] | | ● | ● | ● | ○ | ● | ● | ● |
| | Smart meters [105] | | ● | ● | ● | ● | ● | ○ | ● |
| Substitution | Two-factor authentication [129] | ○ | ● | | | | | | |
| | Three-factor authentication protocol [151] | ● | ○ | | ● | | | ● | |
| | Multimodal multi-pass authentication [154] | ● | ● | | | | | | |
| Meter bypassing | Autonomous grid operation system w/ firewall [171],[172] | ○ | ○ | ○ | ● | | ● | ● | ● |
| | BC-based encryption, signatures [179] | ○ | ● | ● | ● | | ● | ● | ● |
| | EV localisation w/ road surface detectors [180] | ○ | ● | ● | ● | | ● | ● | ● |
| | Smart metering and peak shaving feature [181] | ○ | ● | ● | ● | | ○ | ○ | ● |
| | Role-based access control policies [182] | ○ | ● | ● | ● | | ○ | ● | ● |
| OTA updates tampering | AES 256 encryption [96] | | ○ | | ○ | | | ● | |
| | OCPP PnC mechanism [97] | | ● | | ○ | | | ● | |
| | Masked authenticated messaging module [183] | | ○ | | ○ | | | ● | |
| Smart card cloning | OCPP PnC mechanism [120] | ○ | ● | ● | ● | | | ● | |
| | Contactless banking cards [41] | ● | ● | ● | ● | | | ● | |
| | Location, time span, consumed energy monitoring [127] | ● | ● | ○ | ● | | | ● | |
| | Multimodal multi-pass authentication w/ smart card [154] | ● | ● | ● | ● | | | ● | |
| Masquerading/ impersonation | Cipher/hash-based message authentication code [39],[125] | ○ | ● | | ○ | | | ○ | |
| | BC payment [135],[161] | ● | ● | | ● | | | ● | |
| | Three-factor authentication protocol [151] | ● | ○ | | ● | | | ● | |
| | Multimodal multi-pass authentication [154] | ● | ● | | ○ | | | ○ | |
| | BC-enabled security architecture [155],[156],[184] | ● | ● | | ● | | | ● | |
| | Certificate revocation mechanism [166] | ● | ● | | ○ | | | ○ | |
| | Filtering using polynomials [185] | ○ | ● | | ● | | | ○ | |
| | Elliptic curve cryptography [186] | ○ | ● | | ● | | | ○ | |
| | Mutual server/EV authentication process [187] | ○ | ● | | ○ | | | ● | |
| FDIA | Interval observers [149] | | | | ○ | | ● | ● | ● |
| | Estimate network topology [188] | | | | ○ | | ● | ● | ○ |
| | Sequential change detection [189] | | | | ○ | | ● | ● | ○ |
| Insider | Role-based access control [153] | ● | ● | ● | ● | | ● | ● | |
| Switching | Back propagation neural network scheme [152] | ○ | ● | ● | ● | | ● | | ● |

○ Στοχευμένο στοιχείο ● Προστατευόμενο στοιχείο

Σε κάθε περίπτωση, οι διακοπές ρεύματος είναι μια παράμετρος που επηρεάζει και το σύστημα φόρτισης και μπορεί να μετριαστεί μόνο από ένα προσεκτικά σχεδιασμένο ηλεκτρικό δίκτυο. Ωστόσο δεν μπορεί να εξαλειφθεί ως πρόβλημα. Η έλλειψη οποιασδήποτε εναλλακτικής λύσης, από πλευράς ενέργειας για τους σταθμούς φόρτισης CS που βρίσκονται στην αναφερόμενη περιοχή διακοπής της ρευματοδότησης, θα οδηγούσε στην ακινησία οποιουδήποτε ηλεκτρικού οχήματος και, ως εκ τούτου, στην

καθήλωση των επιβατών σε αυτήν την περιοχή. Οι Amini, Mohammadi και Kar [173] προτείνουν έναν κατανεμημένο αλγόριθμο λήψης αποφάσεων που επιτρέπει στους εναλλακτικούς πόρους ενέργειας να υποστηρίζουν τους σταθμούς φόρτισης CS σε περίπτωση διακοπής τροφοδοσίας από το δίκτυο ηλεκτρικής ενέργειας και να διατηρείται η διαθεσιμότητα της υπηρεσίας.

Η επιβάρυνση του δικτύου ηλεκτρικής ενέργειας από το αυξημένο φορτίο σε μικρο-πλέγμα λόγω φόρτισης ηλεκτρικών οχημάτων, ειδικά κατά τις ώρες αιχμής, μελετήθηκε από τους συμμετέχοντες στο έργο *My Electric Avenue Project* [174]. Το συμπέρασμα ήταν ότι το φορτίο του μικρο-πλέγματος μπορεί να ελεγχθεί σημαντικά εάν κάθε σύστημα φόρτισης οχημάτων εφαρμόζει ένα σύντομο διάλειμμα, μικρότερο των δεκαπέντε (15) λεπτών, κατά τη διάρκεια κάθε κύκλου φόρτισης. Αυτή η διαλειμματική συμπεριφορά στη φόρτιση, αναφερόμενη και ως συμπληρωματική εφεδρική χωρητικότητα (supplemental reserve capacity), θα οδηγούσε σε μικρότερο χρόνο ουσιαστικής φόρτισης SOC σε ορισμένα από τα οχήματα EV. Κάτι τέτοιο μπορεί να γίνει αποδεκτό χάρη στη συνεχώς αυξανόμενη αυτονομία των μπαταριών, στις μέρες μας.

Ένα από τα αποτελέσματα των διακοπών ρεύματος σε μια υπηρεσία φόρτισης OCPP είναι η διαρροή πληροφοριών τοποθεσίας [100]. Η αναφορά παρουσιάζει το αποτέλεσμα μελέτης ενός στόλου οχημάτων EV και των διάσπαρτων σταθμών φόρτισης CS σε στρατιωτική βάση της Πολεμικής Αεροπορίας του Λος Άντζελες, ΗΠΑ. Η μελέτη καταλήγει σε μια διαδικασία διαχωρισμού φορτίου υλικού (Hardware Load Separation, HLS) για τον εξοπλισμό σύνδεσης EVSE και το τοπικό μικρο-πλέγμα, καθώς και την τροφοδοσία του εξοπλισμού σύνδεσης EVSE μέσω εναλλακτικών πηγών ενέργειας, όπως ενός συστήματος αποθήκευσης ενέργειας ή μέσω μιας γεννήτριας καυσίμου diesel. Η HLS διαδικασία θα διαφύλασσε την αδιάλειπτη λειτουργία της υπηρεσίας φόρτισης κατά τη διάρκεια μιας διακοπής και το τοπικό μικρο-πλέγμα θα απαλλάσσονταν από ένα πρόσθετο φορτίο εκκίνησης στη φάση αποκατάστασης της τάσης.

Στο προαναφερόμενο έργο, το δίκτυο PEV περιλαμβάνει ένα σύστημα διαχείρισης ενέργειας EMS, περιγραφόμενο ως Distributed Energy Resources Customer Adoption Model Optimizer (DER-CAM). Το DER-CAM συνδυάζει δεδομένα από τον στόλο και από ένα σύστημα πρόβλεψης και διαχειρίζεται το χρονοδιάγραμμα της υπηρεσίας φόρτισης. Διαφυλάσσει παράλληλα την αυτονομία της υπηρεσίας σε περίπτωση διακοπής ρευματοδότησης με την επιβολή ενός σταθερά υψηλού SOC για κάθε όχημα/καταναλωτή EV. Ένα παρόμοιο EMS, το ISO (Independent System Operator) [118], είναι ένας ανεξάρτητος διαχειριστής για τη διαχείριση του φορτίου τάσης σε ώρες αιχμής, του κόστους φόρτισης και του χρονοδιαγράμματος και για την υποστήριξη της υπηρεσίας με εφεδρική τάση σε περίπτωση διακοπής ρευματοδότησης. Το Outage and Restoration Management (ORM) είναι ένα άλλο παράδειγμα συστήματος διαχείρισης ενέργειας EMS που έχει σχεδιαστεί για να λειτουργεί στο δίκτυο περιοχής πεδίου (Field Area Network, FAN) της υποδομής του έξυπνου πλέγματος, όπως περιγράφεται στην αναφορά του προγράμματος *ebalance-plus* [114]. Στο ευρωπαϊκά χρηματοδοτούμενο ερευνητικό πρόγραμμα με το όνομα *SmartNet* [116] για τα συστήματα έξυπνης αλληλεπίδρασης μεταξύ του διαχειριστή συστήματος μεταφοράς (Transmission System Operator, TSO) και του διαχειριστή διανομής DSO. Επίσης, στο ευρωπαϊκά χρηματοδοτούμενο ερευνητικό πρόγραμμα με το όνομα *PlanGridEV* [175] για τον σχεδιασμό του δικτύου και τις

λειτουργικές αρχές της μαζικής ανάπτυξης οχημάτων EV, ένα σύστημα διαχείρισης διακοπών (Outage Management System, OMS) περιλαμβάνεται στην αρχιτεκτονική για τον εντοπισμό και την επίλυση των διακοπών και για τη διατήρηση αρχείων καταγραφής της συμπεριφοράς του πλέγματος.

Οι Korba et al. [169] εισάγουν ένα πλαίσιο ανίχνευσης ανωμαλιών δύο επιπέδων που βασίζεται σε δενδροειδείς αποφάσεις παλινδρόμησης για να αξιοποιήσουν τις παραμέτρους κανονικής λειτουργίας της κατανάλωσης ενέργειας, να οδηγηθούν σε προβλέψεις/ προγνώσεις και να δημιουργήσουν πρότυπα κατανάλωσης για οικιακά μικρο-πλέγματα και, τελικά, να προβλέψουν επερχόμενες επιθέσεις υπερφόρτωσης τάσης. Αυτή η λύση εστιάζει στα οικιακά δίκτυα PEV.

**Προστασία του πλέγματος**

Σε ένα σύστημα φόρτισης οχημάτων EV, θα πρέπει να επαληθεύεται η σύνδεση του οχήματος EV στο πλέγμα, πριν ξεκινήσει η διαδικασία φόρτισης. Κατά τη διαδικασία φόρτισης, οποιαδήποτε αλλαγή στη σύνδεση ή η ύπαρξη αντίστασης γείωσης θα πρέπει να οδηγεί σε διακοπή ή τερματισμό της διαδικασίας φόρτισης, έτσι ώστε να μην επηρεαστούν τόσο η μπαταρία και τα ηλεκτρικά κυκλώματα του ηλεκτρικού οχήματος όσο και η ροή ισχύος του πλέγματος. Για τον λόγο αυτό προτείνεται η χρήση φυσικού αγωγού με οδηγό ελέγχου για τα επίπεδα φορτίου του οχήματος EV [176]. Ο αγωγός και ο έλεγχος της ροής τάσης με τη χρήση πιλοτικού σήματος περιγράφεται στο πρότυπο ISO/IEC 15118 [87].

Ορισμένες κυβερνοφυσικές επιθέσεις εκμεταλλεύονται το πρωτόκολλο OCPP για να επηρεάσουν την υποδομή του δικτύου φόρτισης και, τελικά, το ηλεκτρικό πλέγμα. Μια επίθεση FDIA είναι ένα τέτοιο παράδειγμα. Ο επιτιθέμενος χρησιμοποιεί τους αισθητήρες που λειτουργούν εντός του δικτύου PEV και αλλοιώνει τις τιμές της κατάστασης φόρτισης ενός οχήματος EV ή ενός σταθμού φόρτισης CS, χωρίς να μπορεί εύκολα αυτή η αλλοίωση να εντοπιστεί. Μια μέθοδος που προτείνεται ως λύση, βασίζεται σε παρατηρητές χρονικών διαστημάτων μεταδόσεων για την ανίχνευση FDIA [149]. Σε αυτήν την περίπτωση, το σύστημα διαχείρισης CSMS μπορεί να εντοπίσει τους αισθητήρες που επηρεάζονται από την επίθεση FDIA, αξιολογώντας τα χρονικά διαστήματα διακοπής στις μεταδόσεις δεδομένων των αισθητήρων.

Η τεχνολογία ασύρματης φόρτισης Wireless Power Transfer (WPT) είναι μια σύγχρονη μέθοδος για την παροχή υπηρεσίας εντός ενός δικτύου PEV. Ωστόσο, η WPT πάσχει από ευπάθειες που θα μπορούσαν να οδηγήσουν σε ξαφνικό υψηλό φορτίο ή σε απότομη αλλαγή φορτίου που προκαλείται από πηγές στατικής ενέργειας, όπως η μπαταρία του οχήματος EV. Αυτές οι ευπάθειες θα μπορούσαν να επηρεάσουν τη σταθερότητα του ηλεκτρικού πλέγματος. Η μέθοδος κρυπτογράφησης που υποστηρίζεται από το πρωτόκολλο OCPP, για την προστασία της επικοινωνίας μεταξύ του σταθμού φόρτισης CS και του συστήματος διαχείρισης CSMS του δικτύου PEV, θεωρείται μια σωστή πρακτική έναντι των περισσότερων ευπαθειών της WPT [177].

Ορισμένα από τα συστήματα ανίχνευσης εισβολών IDS που προτείνονται ασχολούνται επίσης με την κλοπή ενέργειας και την υπερφόρτωση του ηλεκτρικού δικτύου. Αν και αντιμετωπίζονται παρόμοια, οι δύο επιθέσεις διαφέρουν σε πολλά σημεία, όπως στον τρόπο λειτουργίας του επιτιθέμενου, την καθυστέρηση ανίχνευσης και τον αντίκτυπο

στο προηγμένο δίκτυο μετρητών AMI. Για παράδειγμα, μια επίθεση υπερφόρτωσης δικτύου προκαλεί άμεση ζημιά και η καθυστέρηση ανίχνευσής της είναι πιο κρίσιμη σε σύγκριση με την αντίστοιχη καθυστέρηση ανίχνευσης των επιθέσεων κλοπής ενέργειας. Επομένως, χρειάζεται ένα σύστημα ανίχνευσης κλοπής ενέργειας (Energy Theft Detection System, ETDS) που μπορεί να ανιχνεύει αποτελεσματικά επιθέσεις κλοπής ενέργειας κατά του δικτύου AMI και να τις διαχωρίζει από άλλες επιθέσεις στον κυβερνοχώρο. Ένα ETDS θα αντιμετωπίσει δύο βασικά ζητήματα. Το πρώτο ζήτημα είναι ο εντοπισμός κακόβουλων δειγμάτων. Το δεύτερο ζήτημα είναι η δειγματοληψία των έξυπνων μετρητών για την επίτευξη καλύτερης διαχείρισης φορτίου και ταχύτερης απόκρισης στη ζήτηση. Όσο υψηλότερο είναι το ποσοστό δειγματοληψίας, τόσο μεγαλύτερος είναι ο κίνδυνος αποκάλυψης ευαίσθητων πληροφοριών των πελατών/καταναλωτών της υπηρεσίας φόρτισης.

Οι Jokar, Arianpoo και Leung [170] προτείνουν έναν ανιχνευτή κλοπής ενέργειας με βάση το πρότυπο κατανάλωσης (Consumption Pattern-Based Energy Theft Detector, CPBETD) που χρησιμοποιεί νέες τεχνικές για να ξεπεραστούν τα προβλήματα που σχετίζονται με τα υπάρχοντα συστήματα ανίχνευσης κλοπής ενέργειας ETDS, τα οποία βασίζονται σε ταξινόμηση. Ο CPBETD χρησιμοποιεί κατάλληλες τεχνικές ομαδοποίησης και δημιουργεί ένα σύνθετο σύνολο περιλαμβάνοντας τα δεδομένα της επίθεσης. Αυτό οδηγεί σε ένα ισχυρό σύστημα κατά των επιθέσεων, το οποίο επιτυγχάνει υψηλό ποσοστό ανίχνευσης και χαμηλό ψευδο-θετικό ποσοστό (False Positive Rate, FPR).

Ωστόσο, πρέπει να σημειωθεί ότι τα οχήματα EV, ανάλογα με τις ρυθμίσεις του διαχειριστή διανομής DSO του ηλεκτρικού δικτύου, ενδέχεται να χρησιμοποιηθούν ως εφεδρικές πηγές τάσης σε περίπτωση διακοπής ρευματοδοσίας μέσω του πλέγματος, καθώς οι μπαταρίες των οχημάτων EV έχουν την ικανότητα στρεφόμενης εφεδρείας. Οι μπαταρίες υποστηρίζουν, επίσης, υπηρεσίες black start, δηλαδή τη δυνατότητα ενεργειακής αποκατάστασης βάσει κατανεμημένης εσωτερικά διακινούμενης ενέργειας και όχι αναγκαστικά βάσει εξωτερικών πηγών και έτσι μπορεί να χρησιμοποιηθούν ως δομικό στοιχείο αποκατάστασης μετά από διακοπή τροφοδοσίας του πλέγματος [191],[192]. Αυτά τα χαρακτηριστικά, εάν αξιοποιηθούν από μια κυβερνοφυσική επίθεση, μπορεί να διαταράξουν το ηλεκτρικό δίκτυο προκαλώντας:

*(α)* μια ξαφνική αύξηση της ζήτησης (δηλαδή πολλά οχήματα EV να «φαίνεται» ότι ζητούν φόρτιση ταυτόχρονα),

*(β)* μια ξαφνική αύξηση της τροφοδοσίας (δηλαδή πολλά οχήματα EV να εκφορτίζουν/τροφοδοτούν το πλέγμα ταυτόχρονα) ή

*(γ)* μια επίθεση μεταγωγής (δηλαδή πολλαπλές εναλλαγές φόρτισης και εκφόρτισης σε μικρά χρονικά διαστήματα για την αποσταθεροποίηση του δικτύου).

Στο ίδιο πνεύμα, οι Li et al. [178] προτείνουν τη χρήση ενός ελεγκτή που ορίζεται από λογισμικό, του Software-Defined controller Vehicle-to-Grid (SD-V2G), ο οποίος αξιολογεί συνεχώς την κατάσταση φόρτισης SOC του οχήματος EV και διευκολύνει τη μετάβασή του από κατάσταση σε κατάσταση (δηλαδή τις καταστάσεις φόρτισης, αναστολής και εκφόρτισης). Επίσης, η δυνατότητα παράλληλης ροής δεδομένων και ηλεκτρικής ενέργειας από το ίδιο μέσο, που αναφέρεται και ως Vehicle-to-Home (V2H) [105], είναι εμπνευσμένη από τη λειτουργία των οικιακών σταθμών φόρτισης CS. Σε αυτή την περίπτωση, προτείνεται η ενσωμάτωση έξυπνων μετρητών, οι οποίοι ανιχνεύουν

διακοπές στο μικρο-πλέγμα ή δυσλειτουργίες των διαχειριστικών συστημάτων του πλέγματος.

#### 5.2.5.2 Επιθέσεις αντικατάστασης

Η αναγνώριση και ο έλεγχος της ταυτότητας μέσω των διεργασιών του πλέγματος ηλεκτρικής ενέργειας μπορεί να παρακαμφθεί με φυσικό τρόπο από ένα όχημα EV που συνδέεται στη θέση ή τον εξοπλισμό σύνδεσης EVSE ενός άλλου, ήδη εξουσιοδοτημένου EV. Αυτές οι επιθέσεις, που ονομάζονται επιθέσεις αντικατάστασης (substitution attacks), είναι μια κυβερνοφυσική παραλλαγή των επιθέσεων MitM. Η διαδικασία επαλήθευσης στοιχείων της ταυτότητας του οχήματος EV, ειδικά όταν το EV είναι ασύρματα συνδεδεμένο με το σύστημα φόρτισης, ενδέχεται να εκθέσει τα διαπιστευτήρια αναγνώρισης του EV. Τα σενάρια μιας επιτυχημένης επίθεσης αντικατάστασης περιλαμβάνουν την ενεργοποίηση των διαδικασιών φόρτισης και χρέωσης για ένα εσφαλμένα ταυτοποιημένο EV με βάση [129]:

*(α)* μόνο τα διαπιστευτήρια του οδηγού του οχήματος EV ή

*(β)* μόνο τα διαπιστευτήρια του οχήματος EV.

Οι επιθέσεις αντικατάστασης εκτελούνται με απώτερο στόχο την κλοπή έγκυρων διαπιστευτηρίων οχημάτων EV εκ μέρους ενός μη αναγνωρισμένου/εξουσιοδοτούμενου EV και μπορεί να κλιμακωθούν σε παραβίαση του οχήματος EV ή του εξοπλισμού σύνδεσης EVSE, που εκφράζεται με κλοπή δεδομένων της μονάδας ελέγχου του οχήματος ECU, όπου φιλοξενούνται τα διαπιστευτήρια του EV [87] ή με την απλή χρήση του καλωδίου φόρτισης και, άρα, της διεπαφής ενός νόμιμα εξυπηρετούμενου οχήματος από ένα άλλο όχημα.

Άλλη πρόταση αντιμετώπισης των επιθέσεων αντικατάστασης περιγράφει μια διεργασία ελέγχου της ταυτότητας δύο παραγόντων του οχήματος EV στην οποία η παράμετρος φυσικής συνδεσιμότητας αξιολογείται μαζί με το ψηφιακό αναγνωριστικό του οχήματος EV [129]. Επίσης, οι Vaidya και Mouftah [154] προτείνουν τον μηχανισμό Multimodal Multi-pass Authentication (MMA) που επιτρέπει την από κοινού αναγνώριση και επαλήθευση στοιχείων πρόσβασης του οχήματος EV και του οδηγού, ενώ τα διαπιστευτήρια αυτών λαμβάνονται από διαφορετικές διαδρομές. Ο μηχανισμός MMA έχει δοκιμαστεί με τη χρήση πιστοποιητικών συμβολαίου που συμφωνούν με το πρότυπο ISO/IEC 15118. Οι Irshad et al. [151] προτείνουν ένα πρωτόκολλο ελέγχου της ταυτότητας τριών παραγόντων για τις προ φόρτισης διαπραγματεύσεις μεταξύ του οχήματος EV και του σταθμού φόρτισης CS. Το όχημα EV ελέγχεται με βάση τα διαπιστευτήρια του οδηγού, τα οποία περιλαμβάνουν και έναν βιομετρικό παράγοντα. Το πρωτόκολλο χρησιμοποιείται συμπληρωματικά του OCPP και είναι αποδεδειγμένα ανθεκτικό σε επιθέσεις αντικατάστασης, MitM, πλαστοπροσωπίας και άρνησης υπηρεσίας.

#### 5.2.5.3 Επιθέσεις παράκαμψης μετρητή

Η κυβερνοφυσική επίθεση που αναφέρεται ως «παράκαμψη του μετρητή» λαμβάνει χώρα στον εξοπλισμό σύνδεσης EVSE [118] και, καθώς έχει ως αποτέλεσμα την αλλοίωση της διαδικασίας χρέωσης, επηρεάζει επίσης τον οδηγό του οχήματος EV. Παρόλο που η παράκαμψη μετρητή (meter bypassing) απαιτεί φυσική πρόσβαση και χειρισμό του

υλικού του εξοπλισμού σύνδεσης EVSE, μπορεί να διεξαχθεί και κυβερνοφυσικά με την εκμετάλλευση των δυνατοτήτων που παρέχουν οι εφαρμογές έξυπνης μέτρησης. Η παράκαμψη μετρητή μπορεί να επηρεάσει:

*(α)* τον οδηγό του οχήματος EV όσον αφορά στην υπηρεσία και στη χρέωσή της,

*(β)* το όχημα EV, το οποίο ενδέχεται να μην φορτιστεί και

*(γ)* το ηλεκτρικό δίκτυο/πλέγμα, που μπορεί να υπερφορτωθεί ενεργειακά ή να υποτιμηθεί λογιστικά.

Το OCPP υποστηρίζει τις έξυπνες μετρήσεις για την επικοινωνία μεταξύ του χειριστή σταθμού φόρτισης CSO και των χειριστών του δικτύου ηλεκτρικής ενέργειας (όπως ο διαχειριστής διανομής DSO) και παρέχει προστασία των διαδικασιών μέτρησης και χρέωσης. Η ασφάλεια της επικοινωνίας OCPP μεταξύ των παρόχων ενέργειας και του συστήματος χρέωσης της υπηρεσίας φόρτισης αποτελεί μέλημα της Penta Security, της νοτιοκορεατικής εταιρείας που ανέπτυξε το AutoCrypt V2G [179]. Το AutoCrypt V2G είναι λογισμικό που βασίζεται σε blockchain και παρέχει κρυπτογράφηση δεδομένων και ψηφιακές υπογραφές για τον έλεγχο της ταυτότητας και για την εξουσιοδότηση των οντοτήτων που συμμετέχουν σε ένα σύστημα χρέωσης. Το AutoCrypt V2G υποστηρίζει επίσης τη δυνατότητα PnC του OCPP.

Η διαδικασία της έξυπνης μέτρησης στα δημόσια συστήματα φόρτισης βασίζεται, συνήθως, στον εντοπισμό θέσης του οχήματος EV προς χρέωση. Για τον λόγο αυτό, μια κοινή πρακτική είναι η διαθεσιμότητα ενός σταθμού φόρτισης CS για κάθε θέση στάθμευσης. Η ακεραιότητα της διαδικασίας χρέωσης βασίζεται σε δύο υποθέσεις:

*(α)* ότι η θέση που υποστηρίζεται από έναν σταθμό φόρτισης CS θα καταλαμβάνεται μόνο από ένα όχημα EV και

*(β)* ότι κάθε όχημα EV θα συνδέεται με τον αντίστοιχο της θέσης του σταθμό φόρτισης CS και όχι με κάποιον άλλο παρακείμενο CS.

Και οι δύο υποθέσεις, ωστόσο, δεν διασφαλίζονται στην περίπτωση που ο οδηγός μετακινεί το καλώδιο φόρτισης του οχήματός του από τον ένα σταθμό φόρτισης CS στον άλλο. Οι Nürnberg και Iwan [180] προτείνουν τη χρήση μαγνητικών, επαγωγικών ή ηλεκτρομαγνητικών ανιχνευτών τοποθετημένων στην επιφάνεια του δρόμου που να παρέχουν δεδομένα εντοπισμού σε πραγματικό χρόνο για όλα τα ηλεκτρικά οχήματα στον χώρο στάθμευσης.

Η παράκαμψη μετρητή είναι ένα ζήτημα ασφάλειας για το σύστημα φόρτισης οχημάτων EV και την παρεχόμενη υπηρεσία, καθώς και για το ηλεκτρικό πλέγμα και τα συστήματα υποστήριξης στην πλευρά του παρόχου. Η έξυπνη μέτρηση που διευκολύνει τις αυξημένες ανάγκες σε ηλεκτρική ενέργεια, ενεργοποιεί παράλληλα δυνατότητες, όπως η αποφυγή αιχμών [193]. Η αποφυγή αιχμών επιτρέπει στον διαχειριστή διανομής DSO ή σε οποιονδήποτε χειριστή από την πλευρά ελέγχου του δικτύου ηλεκτρικής ενέργειας να μειώσει την κατανάλωση ενέργειας σε ώρες αιχμής για την προστασία του πλέγματος. Αυτό προτείνεται στην περίπτωση της Motown [181], μιας πλατφόρμας ανοιχτού κώδικα που προτείνεται από τη σύμπραξη των ElaadNL, Alliander Mobility Services (AMS ή Allego), iHomer και NewMotion.

Ο συνεχώς αυξανόμενος αριθμός ηλεκτρικών οχημάτων και η επικείμενη αύξηση των ενεργειακών αναγκών απαιτούν ισχυρές δικτυακές υποδομές και ευέλικτη παραγωγή ενέργειας που να συνδυάζει και ανανεώσιμους ενεργειακούς πόρους. Σε αυτό το πνεύμα, οι Uhlig et al. [171] και Kubis et al. [172] προτείνουν ένα αυτόνομο λειτουργικό σύστημα, το InGO, για την ενίσχυση του πλέγματος. Το InGO αποτελείται από μονάδες που χωρίζουν το πλέγμα σε μικρο-πλέγματα χαμηλής τάσης, τα οποία είναι ανεξάρτητα διαχειριζόμενα. Στην περίπτωση ενός OCPP συστήματος φόρτισης οχημάτων EV, το InGO παρεμβαίνει στην επικοινωνία μεταξύ των σταθμών φόρτισης CS και του συστήματος διαχείρισης CSMS και προστατεύει τα δεδομένα που ανταλλάσσονται με το τείχος προστασίας που διαθέτει, με αποτέλεσμα την ασφαλή επεξεργασία των δεδομένων των έξυπνων μετρητών.

Η ερευνητική ομάδα του προγράμματος της Ευρωπαϊκής Ένωσης *NOBEL GRID* προτείνει την ενίσχυση των έξυπνων μετρητών με τη χρήση μιας μονάδας επέκτασης έξυπνου μετρητή (Smart Meter eXtension module, SMX) [182]. Η μονάδα SMX εφαρμόζει πολιτικές ελέγχου πρόσβασης βάσει ρόλων (Role-Based Access Control, RBAC) για τον περιορισμό της μη εξουσιοδοτημένης πρόσβασης στους έξυπνους μετρητές.

#### 5.2.5.4 Επιθέσεις παραβίασης ραδιοδιεπαφών

Τα οχήματα EV και οι σταθμοί φόρτισης CS περιέχουν ένα σύμπλεγμα υλικού και κάθε στοιχείο υλικού φέρει διαφορετικό υλικο-λογισμικό. Λαμβάνοντας υπόψη τις συνεχείς αλλαγές στο υλικο-λογισμικό, το κόστος της ανάκλησης και το κόστος του χρόνου κλήσης ενός οχήματος EV για την ενημέρωση υλικο-λογισμικού, η προσέγγιση ενημέρωσης Over-The-Air (OTA) είναι μια ελκυστική εναλλακτική λύση. Η OTA διευκολύνεται από τη σχεδόν αδιάλειπτη δικτυακή σύνδεση των σύγχρονων οχημάτων EV. Ωστόσο, οι ενημερώσεις OTA αποτελούν ταυτόχρονα κίνδυνο και αντίμετρο ασφάλειας. Η παραβίαση OTA ή η παραβίαση ραδιοδιεπαφών (OTA updates tampering) ενός υλικο-λογισμικού ή ενός λογισμικού μπορεί να εκθέσει ζωτικής σημασίας λειτουργίες/πληροφορίες του οχήματος EV σε επιθέσεις από απόσταση (όπως επιθέσεις παράκαμψης ελέγχου ή επιθέσεις εξ' αποστάσεως ελέγχου εκτέλεσης (Remote Control Execution, RCE) [159],[194] και, την ίδια στιγμή, ένα όχημα EV με ξεπερασμένο υλικο-λογισμικό ή λογισμικό μπορεί να είναι ευάλωτο στις πιο επίκαιρες επιθέσεις του κυβερνοχώρου [125].

Τα ίδια προβλήματα αντιμετωπίζονται και στους σταθμούς φόρτισης CS. Ενώ η τύπου OTA ενημέρωση και επιδιόρθωση του υλικο-λογισμικού είναι ένας βολικός τρόπος για να παρακαμφθούν οι ανακλήσεις και να μειωθούν οι εκτός λειτουργίας περίοδοι ενός οχήματος EV, το υλικο-λογισμικό παραμένει εκτεθειμένο σε παραβιάσεις κατά τη μετάδοση OTA στο όχημα EV. Επιπλέον, η OTA δεν υποστηρίζεται πάντα από το όχημα EV, ειδικά στην περίπτωση παλαιότερων μοντέλων. Οι Buschlinger, Springer και Zhdanova [97] προτείνουν οι ενημερώσεις να γίνονται μέσω της σύνδεσης PnC του οχήματος EV στον σταθμό φόρτισης CS. Η μετάδοση του υλικο-λογισμικού θα γίνεται μέσω του καλωδίου φόρτισης και με αυτό τον τρόπο το υλικο-λογισμικό θα είναι ανθεκτικό σε παραβιάσεις. Ο μέσος χρόνος μιας διαδικασίας φόρτισης υπολογίζεται στα 30 min και είναι αρκετός για μια ταυτόχρονη ενημέρωση, που θα προσφέρεται ως υπηρεσία προστιθέμενης αξίας (Value-Added Service, VAS) στον χώρο φόρτισης [97].

Τέτοιες υπηρεσίες βρίσκονται ήδη υπό μελέτη και ανάπτυξη [195].

Μια λύση κατά της παραβίασης του υλικο-λογισμικού ή του λογισμικού που μεταδίδονται ως ενημέρωση OTA είναι η χρήση της προτεινόμενης μονάδας Masked Authenticated Messaging (MAM) [183]. Η MAM επιτρέπει τη διασπορά δεδομένων μέσω καναλιών. Ο κάτοχος των αρχικών δεδομένων και του καναλιού μπορεί να αλλάξει το δικαίωμα πρόσβασης σε δημόσιο, ιδιωτικό ή περιορισμένο και, ως εκ τούτου, να ελέγξει ποιος θα έχει πρόσβαση στα δεδομένα και με τι δικαιώματα.

Μια λίστα ενεργειών για την ελαχιστοποίηση του κινδύνου απομακρυσμένης πρόσβασης προτείνεται στους κατασκευαστές οχημάτων EV. Η απομακρυσμένη πρόσβαση έχει άμεση σχέση με την παραβίαση των ενημερώσεων OTA [96]. Η λίστα περιλαμβάνει τα ακόλουθα αντίμετρα:

*(α)* Η διαδικασία εξουσιοδότησης και ελέγχου της ταυτότητας να εκτελείται πριν από τη διαδικασία ενημέρωσης.

*(β)* Να γίνεται κρυπτογράφηση των αρχείων της ενημέρωσης, των δεδομένων του οχήματος EV και των μηνυμάτων που ανταλλάσσονται πάνω από τη μονάδα ελέγχου του οχήματος ECU, και

*(γ)* Να υποστηρίζεται η αποκατάσταση/επαναφορά σε περίπτωση αποτυχίας λήψης ή παραβίασης της ενημέρωσης OTA.

Η κρυπτογράφηση θα πρέπει να γίνεται με τον αλγόριθμο Advanced Encryption Standard (AES) 256 ή άλλες αποδεκτές τυποποιημένες εναλλακτικές λύσεις.

#### 5.2.5.5 Επιθέσεις κλωνοποίησης έξυπνης κάρτας

Ο οδηγός του οχήματος EV συνήθως ταυτοποιείται εντός του δικτύου PEV βάσει του μοναδικού αναγνωριστικού (Unique Identifier, UID) μιας έξυπνης κάρτας ταυτοποίησης μέσω ραδιοσυχνοτήτων (Radio Frequency Identification, RFID) [127]. Οι έξυπνες κάρτες χρησιμοποιούνται επίσης ως μικροεπεξεργαστές και συσκευές αποθήκευσης για την προστασία των δεδομένων του οδηγού από παραβίαση [126],[128]. Οι κάρτες εκδίδονται από τη διαχειριστική αρχή του δικτύου PEV (στα σύγχρονα δίκτυα PEV η αρχή αυτή έχει και τον ρόλο του χειριστή CSO βάσει της σύμβασης με τον οδηγό EV). Ωστόσο, οι έξυπνες κάρτες μπορεί να κλωνοποιηθούν, κάτι που είναι μια παραλλαγή της επίθεσης πλαστοπροσωπίας OCPP. Το πρωτόκολλο μπορεί να επηρεαστεί σοβαρά από μια τέτοια επίθεση, εάν ο επιτιθέμενος αποκτήσει πρόσβαση στο γονικό OCPP idTag, με το οποίο μπορεί να παραποιήσει μια ομάδα διακριτικών [40].

Οι επιθέσεις κλωνοποίησης έξυπνων καρτών είναι ήδη δημοφιλείς παρά τις τρέχουσες χαμηλές τιμές χρέωσης, επειδή είναι εύκολο να εκτελεστούν και έχουν άμεσο οικονομικό όφελος όταν οι κλωνοποιημένες κάρτες μεταπωλούνται ή χρησιμοποιούνται για δωρεάν υπηρεσία. Ωστόσο, υπάρχουν τεχνικές όπως η παρακολούθηση της θέσης, του χρονικού διαστήματος και της ποσότητας ενέργειας που καταναλώνεται που μπορούν να βοηθήσουν στην αναγνώριση χρήσης μιας κλωνοποιημένης κάρτας σε ένα δίκτυο PEV [127]. Για τον λόγο αυτό χαρακτηρίζονται ως επιθέσεις μέτριας έως υψηλής επίπτωσης, υψηλής εφικτότητας και χαμηλής ανιχνευσιμότητας.

Το αναγνωριστικό ID μιας έξυπνης κάρτας RFID, το οποίο διαβάζεται σε ένα σταθμό φόρτισης CS, σε συνδυασμό με τα διαπιστευτήρια σύνδεσης του οδηγού EV στην εφαρμογή προγραμματισμού/χρέωσης φόρτισης, χρησιμοποιούνται για την εξουσιοδότηση μιας υπηρεσίας φόρτισης στο προτεινόμενο σύστημα ελέγχου της ταυτότητας πολλαπλών μέσων και πολλαπλών διελεύσεων με χρήση έξυπνων καρτών (Multimodal and Multi-pass Authentication scheme using Smart Cards, MMA-SC) [154]. Η υπηρεσία φόρτισης ενεργοποιείται μόνο για τον σταθμό φόρτισης CS όπου διαβάστηκε η κάρτα.

Οι Aubel και Poll [41] προτείνουν την αντικατάσταση των έξυπνων καρτών RFID από τις τραπεζικές κάρτες με δυνατότητα ανέπαφης λειτουργίας, που υποστηρίζουν το πρότυπο EMV (το EMV πήρε το όνομά του από τις τρεις εταιρείες Europay, Mastercard και Visa από τις οποίες και δημιουργήθηκε αρχικά). Σύμφωνα με το EMV, είναι δυνατή η επαλήθευση της κάρτας με την ισχυρότερη, από άποψη ασφάλειας, ασύμμετρη κρυπτογραφία. Η ευθυγράμμιση με το EMV σημαίνει ότι οι συσκευές ανάγνωσης καρτών που είναι ενσωματωμένες στους σταθμούς φόρτισης CS θα πρέπει και αυτές να υποστηρίζουν τη μέθοδο επαλήθευσης EMV.

Η πλέον πρόσφατη έκδοση του πρωτοκόλλου OCPP 2.0, υποστηρίζει τον μηχανισμό PnC για την αναγνώριση και την επαλήθευση των διακριτικών του οχήματος EV κατά τη σύνδεση στο σταθμό φόρτισης CS [120], για τη βέλτιστη αντιμετώπιση της έκθεσης των διακριτικών του οδηγού EV εξαιτίας της χρήσης έξυπνης κάρτας.

#### 5.2.5.6 Επιθέσεις μεταμφίεσης και απομίμησης

Ένα δίκτυο PEV μπορεί να δεχθεί επιθέσεις μεταμφίεσης (όπως η παράνομη φόρτιση οχήματος EV με τα διαπιστευτήρια άλλου EV) ή επιθέσεις πλαστοπροσωπίας (όπως ένας οδηγός οχήματος EV που φορτίζει το EV του και χρεώνει άλλον οδηγό EV) [153]. Τα κύρια σημεία εισόδου και για τους δύο αυτούς τύπους επιθέσεων είναι το όχημα EV, ο οδηγός του οχήματος EV (τα διαπιστευτήρια της πιστωτικής του κάρτας, ο λογαριασμός πρόσβασής του στην εφαρμογή κράτησης/χρέωσης της υπηρεσίας) και ο σταθμός φόρτισης CS [83],[42],[38]. Οι επιθέσεις μεταμφίεσης (masquerading) χρησιμοποιούνται ως επί το πλείστον για να διαταράξουν και να επηρεάσουν την ακεραιότητα της χρέωσης της υπηρεσίας, ενώ οι επιθέσεις πλαστοπροσωπίας (impersonation) χρησιμοποιούνται από το κακόβουλο μέρος, έτσι ώστε να αναληφθεί ο έλεγχος και να διακοπεί η διαθεσιμότητα της υπηρεσίας [196].

Ένα γενικό πλην όμως έγκυρο αντίμετρο για την αποτροπή επιθέσεων μεταμφίεσης είναι η χρήση μιας μεθόδου αναγνώρισης, που βασίζεται σε πιστοποιητικά εκδοθέντα από αξιόπιστες αρχές. Έχει προταθεί ένας μηχανισμός ανάκλησης πιστοποιητικού [166] για να διασφαλιστεί η εγκυρότητα των πιστοποιητικών έναντι μεταμφιέσεων μετά την έκδοσή τους. Ο μηχανισμός Multimodal Multi-pass Authentication (MMA) [154] είναι μια άλλη συναφής περίπτωση, όπου επιτυγχάνεται η προστασία των διαπιστευτηρίων του οχήματος EV. Το προαναφερόμενο πρωτόκολλο ελέγχου της ταυτότητας τριών παραγόντων για τις προ φόρτισης διαπραγματεύσεις, επίσης προστατεύει το OCPP από επιθέσεις πλαστοπροσωπίας κατά του οδηγού EV [151].

Οι επιθέσεις μεταμφίεσης ενδέχεται να συμβούν όταν τα μηνύματα που ανταλλάσσονται μεταξύ των μονάδων ελέγχου του οχήματος ECU δεν είναι κρυπτογραφημένα και

πιστοποιημένα. Δεδομένου ότι τα μηνύματα του σειριακού δικτύου αισθητήρων CAN μεταδίδονται σε όλους τους κόμβους χωρίς ευχέρεια διάκρισης, είναι ευάλωτα σε επιθέσεις μεταμφίεσης. Τα πλαίσια CAN δεν είναι κρυπτογραφημένα, οπότε ο επιτιθέμενος μπορεί να έχει πρόσβαση στα μεταφερόμενα δεδομένα και βάσει αυτών να μπορέσει να εντοπίσει τα σημεία εισόδου του συστήματος. Για την προστασία από αυτού του τύπου επιθέσεις, ο έλεγχος της ταυτότητας των μηνυμάτων που βασίζεται σε κατακερματισμό (Hash-based Message Authentication Code, HMAC) [125], μπορεί να χρησιμοποιηθεί για την ασφάλεια της κυκλοφορίας CAN μηνυμάτων μεταξύ των μονάδων ελέγχου του οχήματος ECU. Η παραλλαγή του κώδικα επαλήθευσης μηνυμάτων MAC (Cipher-based MAC, CMAC) [39], που βασίζεται σε κρυπτογράφηση, διασφαλίζει την επικοινωνία εντός μιας μονάδας ελέγχου του οχήματος ECU, χρησιμοποιώντας την κρυπτογράφηση AES και κοινόχρηστα κλειδιά. Ένα άλλο προτεινόμενο σχήμα φιλτραρίσματος, χρησιμοποιεί πολυώνυμα αντί για τον κώδικα επαλήθευσης μηνυμάτων MAC για την προστασία των κόμβων [185]. Η κρυπτογράφηση της επικοινωνίας V2G σε αυτή την περίπτωση αντιμετωπίζεται με το προτεινόμενο πρωτόκολλο, που ενσωματώνει κρυπτογράφηση ελλειπτικής καμπύλης ECC [186].

Ως προσέγγιση μετριασμού, οι Danish et al. [135] εφαρμόζουν λειτουργία πληρωμής βασιζόμενη στο blockchain για να διασφαλίσουν ότι δεν μπορούν να εισαχθούν ψευδείς πληροφορίες στο σύστημα και ότι το όχημα EV θα πληρώσει με ασφάλεια και μόνο για την παρεχόμενη υπηρεσία. Καθώς το όχημα EV και ο σταθμός φόρτισης CS κάνουν κρατήσεις και διεκπεραιώνουν πληρωμές σε ένα δίκτυο blockchain, είναι σημαντικό να μην μπορεί να πλαστογραφήσει την ταυτότητά τους κατά τη διαδικασία φόρτισης/χρέωσης καμία κακόβουλη οντότητα. Οι αξιολογήσεις δείχνουν ότι το προτεινόμενο BlockEV είναι επεκτάσιμο και επιφέρει ένα αισθητά χαμηλό φόρτο συναλλαγών και αποθήκευσης blockchain.

Ωστόσο, η χρήση έξυπνων συμβολαίων στο blockchain δεν παρέχει την επιθυμητή ευελιξία προσαρμογής στη δυναμική συμπεριφορά των οδηγών οχημάτων EV και στις συνθήκες του ηλεκτρικού δικτύου/πλέγματος. Στη προτεινόμενη λύση consortium blockchain [161], μόνο τμήματα των εξουσιοδοτημένων κόμβων συμμετέχουν στη διαδικασία συναίνεσης και, επομένως, περιορίζονται οι στόχοι ενδεχόμενων επιθέσεων πλαστοπροσωπίας κατά του πρωτοκόλλου OCPP. Η λύση consortium blockchain επιτρέπει μόνο κόμβους που επαληθεύονται από πολλά ζεύγη κλειδιών. Επιπλέον, τα κλειδιά είναι διαφορετικά για κάθε συναλλαγή του κόμβου. Παρόμοια προσέγγιση παρουσιάζεται και με την αποκεντρωμένη αρχιτεκτονική διαπραγμάτευσης ηλεκτρικής ενέργειας οχημάτων EV, που βασίζεται στην consortium blockchain, όπου οι επιθέσεις πλαστοπροσωπίας κατά των οχημάτων EV αποτρέπεται χρησιμοποιώντας ένα ιδιωτικό κλειδί (Private Key, PK) και ένα μυστικό κλειδί (Secret Key, SK) για κάθε νόμιμη ψηφιακή υπογραφή και έναν βελτιωμένο αλγόριθμο Krill Herd (KH) [155],[156]. Ομοίως, η blockchain αρχιτεκτονική ασφάλειας που βασίζεται στο νέφος και την ακροδικτυακή υπολογιστική [184] χρησιμοποιεί δεδομένα blockchain και ενεργειακά κρυπτο-νομίσματα (πρόκειται για ένα κρυπτο-νόμισμα που πρωτοεμφανίστηκε το 2014 για να ενισχύσει την ”πράσινη” οικονομία και να σταθεροποιήσει την αξία της βιώσιμης ενέργειας) [197], ενώ η συχνότητα αποστολής δεδομένων και το ποσό συνεισφερόμενης ενέργειας αξιολογούνται για τον προσδιορισμό του επιπέδου ασφάλειας του κάθε κόμβου.

Όπως αναφέρθηκε προηγουμένως, η δυνατότητα PnC του πρωτοκόλλου OCPP είναι ένα εργαλείο κατά της παραβίασης του οχήματος EV και του υλικού του. Ωστόσο, εάν ένας επιτιθέμενος καταφέρει να αποκτήσει τα διαπιστευτήρια PnC, μπορεί να αναπτύξει μια επίθεση αντικατάστασης του οχήματος EV και:

*(α)* να διαπράξει απάτη χρεώνοντας κάποιον άλλο νόμιμα πιστοποιημένο πελάτη,

*(β)* να αποκτήσει δωρεάν πρόσβαση στις υπηρεσίες προστιθέμενης αξίας VAS ή

*(γ)* να αιτηθεί ανανεωμένα διαπιστευτήρια PnC και να επικυρωθεί νόμιμα παρότι παρανόμως.

Η δημιουργία και η αποθήκευση εντός του οχήματος EV μπορεί να αποτελέσει τη λύση προστασίας των διαπιστευτηρίων PnC [143].

Μια πιο γενική και εξίσου αποτελεσματική λύση, η ενσωμάτωση PUF στο εκτεθειμένο όχημα EV και στους σταθμούς φόρτισης CS [139],[140],[141] θα επέτρεπε την αναγνώριση μιας μιμητικής ή μιας μεταμφιεσμένης συσκευής στο PEV. Είναι άξιο αναφοράς πως κατά το ISO 15118-2 ο έλεγχος της ταυτότητας στην πλευρά του διακομιστή (εδώ ως διακομιστής θα λειτουργούσε ο σταθμός φόρτισης CS ή το σύστημα διαχείρισης CSMS) θεωρείται υποχρεωτικός, ενώ αναγνωρίζεται πως μια αμοιβαία διαδικασία ελέγχου της ταυτότητας στον διακομιστή και στο όχημα EV θα απέτρεπε επιθέσεις πλαστοπροσωπίας [187].

#### 5.2.5.7 Επιθέσεις εισαγωγής ψευδών δεδομένων

Συνήθως, μια επίθεση FDIA διεξάγεται με παραβίαση των στοιχείων της αρχιτεκτονικής φόρτισης χρησιμοποιώντας το πρωτόκολλο OCPP ή με πρόσβαση και παραποίηση της βάσης δεδομένων του συστήματος διαχείρισης CSMS.

Μια επίθεση FDIA στα δίκτυα φόρτισης οχημάτων EV στοχεύει πρωτίστως να θέσει σε κίνδυνο τις μετρήσεις φόρτισης, κατανάλωσης ενέργειας και στάθμης ενέργειας. Το σύστημα φόρτισης, συμπεριλαμβανομένων των επικοινωνιών μέσω του δικτύου PEV, ρυθμίζεται σε μεγάλο βαθμό με βάση τις προβλεπόμενες καταστάσεις και τις εναλλαγές καταστάσεων των οχημάτων EV. Οι επιθέσεις στοχεύουν ακριβώς αυτές τις εκτιμήσεις καταστάσεων και, στην περίπτωση επιτυχίας, οδηγούν σε λανθασμένες αποφάσεις σχετικά με το επίπεδο χρέωσης, τους χρόνους φόρτισης ή ακόμα και τις τιμές κοστολόγησης της υπηρεσίας. Υπάρχουν αποτελεσματικές μέθοδοι για τον εντοπισμό αλλοιωμένων δεδομένων σε δικτυωμένα συστήματα, όπως τα συστήματα ανίχνευσης εισβολών που βασίζονται σε εκτιμητές ελαχίστων τετραγώνων (least squares, LS), όπου τα δυαδικά διαγράμματα απόφασης (Binary Decision Diagrams, BDD) χρησιμοποιούνται για την ανίχνευση αλλοιωμένων δεδομένων εξαιτίας τυχαίου θορύβου και σφαλμάτων, όχι όμως εξαιτίας μιας επίθεσης FDIA. Οι Bobba et al. [198] στοχεύουν στον περιορισμό των επιθέσεων σε συγκεκριμένο μόνο αριθμό μετρητών ή κόμβων. Οι Sou, Sandberg και Johansson [188] στοχεύουν στην αντιμετώπιση των επιθέσεων που ξεκινούν αφού ο δράστης έχει συγκεντρώσει δεδομένα εκτός σύνδεσης ή κατανάλωσης ηλεκτρικής ενέργειας και τα χρησιμοποιεί για να αναγνωρίσει την τοπολογία του δικτύου και να επιτεθεί στοχευμένα.

Οι Kurt, Yilmaz και Wang [189] χρησιμοποίησαν μια προσέγγιση ανίχνευσης διαδοχικών αλλαγών ως τον πιο γρήγορο τρόπο για τον εντοπισμό μιας επίθεσης FDIA. Η ιδέα στηρίζεται στο γεγονός ότι οι μέθοδοι με εκτιμητές ελαχίστων τετραγώνων εξαρτώνται μόνο από τις τρέχουσες μετρήσεις, ενώ η δική τους προσέγγιση υιοθετεί ένα μοντέλο χώρου-κατάστασης που επιτρέπει την επεξεργασία τόσο των τρεχουσών όσο και των προηγούμενων τιμών μέτρησης, έτσι ώστε να βελτιώνεται η ακρίβεια. Σε άλλη περίπτωση, προτείνεται ο σχεδιασμός μιας σειράς παρατηρητών χρονικών διαστημάτων μεταξύ των καταστάσεων, που θα λαμβάνουν υπόψη τα όρια των καταστάσεων αυτών [149]. Αυτή η περίπτωση προβλέπει την αξιολόγηση των σφαλμάτων και των διαταραχών για την εκτίμηση των χρονικών διαστημάτων μεταξύ των καταστάσεων του πλέγματος, εντός του οποίου λειτουργεί το πρωτόκολλο OCPP. Η ανίχνευση των επιθέσεων FDIA μπορεί να επιτευχθεί ακόμα και αξιολογώντας τις αποκλίσεις στα χρονικά διαστήματα που καταγράφουν οι παρατηρητές. Τα δεδομένα μέτρησης του κάθε αισθητήρα χρησιμοποιούνται ως είσοδος στον παρατηρητή διαστήματος. Βάσει αυτών, κατασκευάζεται ένας λογικός πίνακας τιμών θέσης για τον εντοπισμό του αισθητήρα στον οποίο έχει λάβει χώρα μια FDIA [149]. Αυτή η προσέγγιση παρουσιάζεται στο πλέγμα του κατανεμημένου συστήματος IEEE 36-bus και μπορεί να προσαρμοστεί με απλό τρόπο σε έξυπνα πλέγματα/δίκτυα που εκτελούν το πρωτόκολλο OCPP.

#### 5.2.5.8 Επιθέσεις εκ των έσω

Οι επιθέσεις παραβίασης του εξοπλισμού σύνδεσης EVSE και του σταθμού φόρτισης CS είναι μια συνήθης έκφραση εσωτερικών επιθέσεων (insider attack). Ως εσωτερικός χαρακτηρίζεται το φυσικό πρόσωπο που θεωρείται αξιόπιστο από τους χειριστές του συστήματος φόρτισης οχημάτων EV και, ως εκ τούτου, του παρέχονται δικαιώματα πρόσβασης. Ένας εσωτερικός χρήστης μπορεί να είναι ο δράστης σε επιθέσεις κλοπής ενέργειας [40]. Υπάρχουν επίσης ορισμένοι «υβριδικοί» ρόλοι, όπως ο ρόλος του παρόχου υπηρεσιών ηλεκτρικής κινητικότητας EMSP και του χειριστή CSO, που δεν εκπληρώνονται πάντα από μια ξεχωριστή οντότητα, αλλά, μερικές φορές, εκπληρώνονται από το φυσικό πρόσωπο ή τη συσκευή που έχει ήδη και κάποιον άλλο ρόλο. Η ύπαρξη αυτών των υβριδικών ρόλων είναι ένα κενό ασφάλειας, που μπορεί να εκμεταλλευτεί κάποιος εσωτερικός χρήστης. Οι στοχευμένες επικοινωνίες από εσωτερικό χρήστη είναι κυρίως αυτές που λαμβάνουν χώρα μεταξύ του χειριστή CSO, του ελεγκτή LC και του σταθμού φόρτισης CS, λόγω της διευκόλυνσης εκτέλεσης των επιθέσεων, στις οποίες αυτός συμμετέχει [127].

Η μέθοδος ελέγχου πρόσβασης βάσει ρόλων IEC 62351-8 RBAC [153] εισάγει ρόλους και κληρονομικότητα δικαιωμάτων και περιορίζει την πρόσβαση σε επιτιθέμενους, ακόμα κι αν αυτοί είναι εσωτερικοί. Το RBAC μπορεί να προστατεύσει τις συσκευές, τους δρώντες και τα δεδομένα της υπηρεσίας φόρτισης EV και, κατά συνέπεια, την επικοινωνία με OCPP.

#### 5.2.5.9 Επιθέσεις μεταγωγής

Οι επιθέσεις μεταγωγής (switching attacks) είναι επιθέσεις με κυβερνοφυσικό αντίκτυπο. Χρησιμοποιούν τα αιτήματα OCPP τύπου *setChargingProfile* ή *startTransactions* στο σταθμό φόρτισης CS. Όταν ο CS παραβιάζεται, αυτά τα μηνύματα OCPP επιτρέπουν στον επιτιθέμενο να εγκαταστήσει κακόβουλα προφίλ φόρτισης. Με αυτά τα προφίλ σε

δράση και τον έλεγχο του CS, ο επιτιθέμενος μπορεί να ενεργοποιήσει δραστηριότητες φόρτισης/εκφόρτισης σε μικρά χρονικά διαστήματα και, τελικά, να αποσταθεροποιήσει την υπηρεσία και το πλέγμα [8].

Οι επιθέσεις μεταγωγής μπορεί να μετριαστούν χρησιμοποιώντας το σχήμα BPNN [152]. Ο αλγόριθμος BPNN που προτείνεται βοηθά στον εντοπισμό ύποπτων αιτημάτων, αναλύοντας τα αιτήματα φόρτισης/εκφόρτισης. Εάν εντοπιστούν τέτοια αιτήματα, ο αλγόριθμος τα απορρίπτει ή εισάγει καθυστερήσεις στον χρόνο εκτέλεσής τους για να περιορίσει τον αντίκτυπο της επίθεσης.

Άλλα αντίμετρα για την αποτροπή των επιθέσεων μεταγωγής είναι τα ακόλουθα [8]:

*(α)* Αυστηρή πολιτική ελέγχου πρόσβασης δεδομένων στους σταθμούς φόρτισης CS, περιορισμένη πρόσβαση σε φυσικές ή δικτυακές θύρες, ισχυρά διαπιστευτήρια και μέθοδοι ελέγχου της ταυτότητας.

*(β)* Μηχανή ανίχνευσης ανωμαλιών στα χρονοδιαγράμματα της υπηρεσίας φόρτισης EV.

*(γ)* Έγκριση/απόρριψη οδηγού EV για οποιαδήποτε αλλαγή του προγράμματος φόρτισης.

*(δ)* Ύπαρξη σχεδίου έκτακτης ανάγκης για το ηλεκτρικό πλέγμα.

*(ε)* Μηχανή ανίχνευσης ανωμαλιών για την παρακολούθηση των ροών δεδομένων των έξυπνων μετρητών.

*(στ)* Τυποποίηση των στοιχείων υλικού και λογισμικού της υποδομής φόρτισης.

### 5.2.6 Απόρρητο και μηχανισμοί ανίχνευσης/εκτροπής

Λαμβάνοντας υπόψη την αρχιτεκτονική και την υποκείμενη υποδομή για τη φόρτιση των οχημάτων EV, μπορεί να διαρρεύσουν ευαίσθητα δεδομένα από διάφορα σημεία. Τα δεδομένα αυτά περιλαμβάνουν πληροφορίες των ιδιοκτητών/οδηγών EV, όπως τα μοτίβα κατανάλωσης ενέργειας, οι τύποι ηλεκτρικών οχημάτων που χρησιμοποιούν και το μοτίβο κίνησής τους με το όχημα. Τα ευαίσθητα δεδομένα του ίδιου του οχήματος EV περιλαμβάνουν τους χρόνους στους οποίους συνήθως φορτίζεται, σε ποια τοποθεσία(ες) συνήθως συμβαίνει αυτό, δεδομένα του ιδιοκτήτη/οδηγού, λεπτομέρειες και στοιχεία προηγούμενων πληρωμών, κατανάλωση ενέργειας και συχνότητα φόρτισης. Όταν το απόρρητο τέτοιων δεδομένων τίθεται σε κίνδυνο, ένας επιτιθέμενος μπορεί να γνωρίζει λεπτομέρειες σχετικά με τις μετακινήσεις του ιδιοκτήτη του οχήματος, το πρόγραμμα των μετακινήσεων αυτών, ακόμα και τους επιλεγμένους προορισμούς του. Εάν κλαπεί το ID του οχήματος EV, ο επιτιθέμενος μπορεί να χρεώσει άλλα οχήματα EV στη θέση του δικού του και να επηρεάσει οικονομικά τον χρήστη ή τους χρήστες του παραβιασμένου οχήματος EV. Για τους λόγους αυτούς, οι μηχανισμοί ανίχνευσης και εκτροπής έχουν μεγάλη σημασία για την ελαχιστοποίηση των επιπτώσεων τέτοιων παράνομων ενεργειών.

Όσον αφορά στα ζητήματα απορρήτου, τα οχήματα EV πρέπει να παρέχουν τα αναγνωριστικά τους, να συνδέονται σε σημεία ή σταθμούς φόρτισης, να συνδέονται σε διεπαφές πολυσύνδεσης (Link Aggregation Groups, LAGs) και να επικοινωνούν με τα συστήματα των παρόχων υπηρεσιών. Αυτό οδηγεί σε δυνητική έκθεση δεδομένων τους, όπως η τρέχουσα τοποθεσία φόρτισης/εκφόρτισής τους [199]. Το απόρρητο της

τοποθεσίας για τις διαδικασίες πληρωμής και τιμολόγησης, προσπαθεί να διαφυλάξει η ενσωμάτωση της αρχιτεκτονικής μονάδας Judging Authority (JA), ενός προτεινόμενου συστήματος διαχείρισης χρεώσεων και πληρωμών υπηρεσίας φόρτισης EV [200].

Η διαχείριση της μπαταρίας αποτελεί επίσης μια πιθανή απειλή για το απόρρητο των δεδομένων, καθώς οι πληροφορίες της μπαταρίας μπορούν να οδηγήσουν τον επιτιθέμενο στη δημιουργία του προφίλ κινητικότητας του κατόχου του οχήματος EV. Επιπλέον, είναι πολύ πιο εύκολη στην υλοποίησή της μια επίθεση σε δίκτυα V2G παρά στο ηλεκτρικό πλέγμα, λόγω της αμφίδρομης επικοινωνίας και της παράλληλης ανταλλαγής ενέργειας και δεδομένων που λαμβάνουν χώρα μεταξύ του οχήματος EV και του πλέγματος [201].

Η διαχείριση δεδομένων σε δίκτυα V2G περιλαμβάνει τη συλλογή, τη συγκέντρωση, την αποθήκευση και τη δημοσίευση δεδομένων. Οι επιτιθέμενοι δείχνουν συχνά μεγάλο ενδιαφέρον στην παραβίαση της βάσης δεδομένων ή των συστημάτων αποθήκευσης. Επιπλέον, έχουν αναπτυχθεί πολλά κακόβουλα λογισμικά και εργαλεία επιθέσεων κατά των βάσεων δεδομένων και των συστημάτων αποθήκευσης.

Η διαδικασία χρέωσης γίνεται διαφορετικά στα δίκτυα V2G από ό,τι στο παραδοσιακό ηλεκτρικό πλέγμα. Παρότι μια πιστωτική κάρτα μπορεί να χρησιμοποιηθεί για τις ανάγκες χρέωσης εντός των δικτύων V2G, δεν είναι ασφαλής λύση ως προς την προστασία του απορρήτου, καθώς σε πολλές εφαρμογές χρέωσης/τιμολόγησης, παρόλο που ο αριθμός της κάρτας κρυπτογραφείται, άλλες πληροφορίες της κάρτας μπορεί να μεταδίδονται χωρίς κρυπτογράφηση [202].

Τα δίκτυα V2G ενδέχεται να χρησιμοποιούν το OCPP οριζόντια ή μπορεί να χρησιμοποιούν το ISO/IEC 15118 ως πρωτόκολλο φόρτισης και για την επικοινωνία μεταξύ των οχημάτων EV και των σημείων φόρτισης, το IEC 61850 για την επικοινωνία μεταξύ σημείων φόρτισης και συστημάτων των παρόχων ενέργειας και το OCPP ως πρωτόκολλο επικοινωνίας μεταξύ των σημείων φόρτισης και των χειριστών κινητικότητας εντός της υπηρεσίας. Όλα αυτά τα πρωτόκολλα φέρουν συγκεκριμένες ευπάθειες. Οι πιθανοί επιτιθέμενοι ενδέχεται να χρησιμοποιήσουν τα κενά σε αυτά τα πρωτόκολλα για κακόβουλους σκοπούς.

Με βάση τη μέθοδο που χρησιμοποιείται κάθε φορά, ο Πίνακας 11 παρέχει μια ταξινόμηση των ευρημάτων σχετικά με τις τεχνικές διατήρησης του απορρήτου, τους μηχανισμούς ελέγχου της ταυτότητας, τους μηχανισμούς εξουσιοδότησης και τους μηχανισμούς ανίχνευσης και εκτροπής, που ισχύουν για συστήματα φόρτισης οχημάτων EV τα οποία βασίζονται στο OCPP. Αυτές οι τεχνικές, οι μηχανισμοί και τα εργαλεία συζητούνται στις ακόλουθες ενότητες.

#### 5.2.6.1 Τεχνικές διαφύλαξης του απορρήτου

Ορισμένες από τις τεχνικές διατήρησης του απορρήτου σε δίκτυα V2G αναπτύχθηκαν πρόσφατα. Κάποιες προσεγγίσεις υιοθετούν την έννοια της *υπογραφής (signature)* ως το κλειδί για τα σχήματα ελέγχου της ταυτότητας. Υπάρχουν συστήματα που χρησιμοποιούν πλήρως τυφλή υπογραφή (ή υπογραφή με απόκρυψη) [203], μερικώς τυφλή υπογραφή [204] και περιοριστική τυφλή υπογραφή [205]. Μια επισκόπηση των τυφλών υπογραφών στο πλαίσιο των δικτύων V2G δίνεται στο [38]. Η μέθοδος της τυφλής υπογραφής είναι κατάλληλη για συστήματα που σχετίζονται με το απόρρητο, όπως ένα δίκτυο PEV, όπου οι ψηφιακές πληρωμές πραγματοποιούνται σε δημόσια προσβάσιμους χώρους, καθώς

Πίνακας 11. Ζητήματα απορρήτου και μηχανισμοί ανίχνευσης/εκτροπής

| | Reference | Method |
|---|---|---|
| **Privacy preservation/ Authentication/Authorization** | [203],[204],[205] | Fully/partially/restrictive blind signature |
| | [206],[207] | Master-/Manager-based group signature |
| | [208] | Ring signature |
| | [209] | Link Aggregation Groups (LAGs) secret sharing |
| | [210],[211],[212] | Homomorphic/symmetric/asymmetric encryption |
| | [128] | Third-party anonymity |
| | [213] | Anonymity networks |
| | [214] | EV mobility in destributed/centralized V2G |
| | [109],[215],[216] | Plug-and-Charge (PnC) EV mode |
| | [154] | Contract certificate (CCert) and V2G PKI |
| **Detection/ Deflection** | [217],[218] | Distributed IDS in AMI network |
| | [170] | Energy Theft Detection Systems (ETDS) |
| | [219] | Honeypots in AMI network |
| | [168],[217],[218],[219] | Low energy consumption |
| | [220],[221] | Anti-jamming/spoofing |
| | [157],[158] | Machine learning abnormal behavior detection |

τα δεδομένα συγκαλύπτονται πριν από την υπογραφή τους και, επομένως, μπορούν να επαληθευτούν δημόσια με περιορισμένη έκθεση.

Υπάρχουν επίσης σχήματα που προτείνουν τη χρήση *ομαδικής υπογραφής (group signature)* που επιτρέπει σε ένα μέλος μιας ομάδας να υπογράφει ανώνυμα εκ μέρους όλης της ομάδας. Αυτές οι ομαδικές υπογραφές απαντώνται σε περιπτώσεις όπου είναι οριζόμενες από το *κύριο μέλος της ομάδας (master-based)* [206] και σε άλλες όπου είναι οριζόμενες από το *διαχειριστικό μέλος της ομάδας (manager-based)* [207]. Στα δίκτυα PEV, ένα σχήμα ομαδικής υπογραφής θα επέτρεπε στον σταθμό φόρτισης CS να επαληθεύει ανώνυμα και να διαχειρίζεται δυναμικά τα συνδεδεμένα οχήματα EV, απαλλάσσοντας το σύστημα διαχείρισης CSMS από τον αντίστοιχο υπολογιστικό φόρτο [222].

Επιπλέον, έχουν προταθεί σχήματα που βασίζονται στην *υπογραφή δακτυλίου (ring signature)*. Αυτή η μέθοδος επιτρέπει σε κάθε μέλος μιας ομάδας να υπογράψει ένα μήνυμα χωρίς να αποκαλύψει την ταυτότητά του [208]. Σε αντίθεση με την ομαδική υπογραφή, η ομάδα σε μια υλοποίηση με υπογραφή δακτυλίου σχηματίζεται κατά περίσταση (ad hoc). Η χρήση της υπογραφής δακτυλίου προτείνεται για την προστασία του απορρήτου ενός οχήματος EV το οποίο αποκτά διαφορετικούς ρόλους εντός του V2G [208]: τον ρόλο του πελάτη/καταναλωτή όταν φορτίζει, τον ρόλο της γεννήτριας/ παρόχου όταν εκφορτίζει στο δίκτυο ή παρέχει ηλεκτρική ενέργεια σε άλλα ηλεκτρικά οχήματα ή τον ρόλο συστήματος αποθήκευσης όταν δεν χρειάζεται φόρτιση ή εκφόρτιση.

Η τεχνική *μεριζόμενων μυστικών κλειδιών (secret sharing)* έχει προταθεί για την αντιμετώπιση της ανώνυμης συγκέντρωσης δεδομένων. Στο [209], ένα μυστικό αναλύεται σε πολλά μέρη που κρατούν διαφορετικά μέλη. Για να αποκατασταθεί το μυστικό, απαιτούνται όλα ή τουλάχιστον κάποια από τα μέρη αυτά. Ο χρόνος σύνδεσης, το τρέχον επίπεδο φόρτισης της μπαταρίας και η ποσότητα ηλεκτρικής ενέργειας που έχει καταναλωθεί από το όχημα είναι τρεις τύποι δεδομένων που συνήθως διατηρούνται σε διαφορετικές LAGs στο πλαίσιο ενός κύκλου της υπηρεσίας φόρτισης EV. Για να παραβιαστούν τα δεδομένα αυτά του οχήματος EV, όλες οι LAGs ή πολλές από αυτές θα πρέπει να παραβιαστούν ταυτόχρονα.

Η *ομομορφική κρυπτογράφηση (homomorphic encryption)* είναι μια άλλη προσέγγιση για την αντιμετώπιση της συγκέντρωσης δεδομένων. Υλοποιείται σε διαφορετικές παραλλαγές, όπως της πλήρους ή της μερικής ομομορφικής κρυπτογράφησης [210] και της συμμετρικής [211] ή της ασύμμετρης ομομορφικής κρυπτογράφησης [212].

Άλλες προσεγγίσεις περιλαμβάνουν την *ανωνυμία τρίτου μέρους (third-party anonymity)* [128], η οποία εισάγει τη χρήση μιας ασφαλούς και αξιόπιστης συσκευής τρίτου μέρους για τη διατήρηση των ευαίσθητων πληροφοριών άλλων μη ασφαλών συσκευών (όπως είναι τα οχήματα EV) και τα *δίκτυα ανωνυμίας (anonymity networks)* [213], τα οποία είναι επικοινωνιακά δίκτυα που περιλαμβάνουν ένα κέντρο παροχής πιστοποιητικών και μια υποδομή δημόσιων κλειδιών PKI για την απόκρυψη αναγνωριστικών του επιπέδου Δικτύου (OSI επίπεδο 3).

Οι προαναφερόμενες τεχνικές εισάγουν ένα πρόσθετο υπολογιστικό φορτίο στα αρχιτεκτονικά στοιχεία ενός δικτύου PEV, ώστε να υποστηρίζουν το απόρρητο των δεδομένων. Ανάλογα με την υποδομή και τους διαθέσιμους πόρους της κάθε τοποθεσίας φόρτισης PEV δημόσιας πρόσβασης ή οικιακής/ιδιωτικής χρήσης εφαρμόζεται το καταλληλότερο σχήμα για τη διατήρηση του απορρήτου.

#### 5.2.6.2 Μηχανισμοί επαλήθευσης της ταυτότητας και εξουσιοδότησης

Ο έλεγχος της ταυτότητας και η εξουσιοδότηση είναι βασικά ζητήματα για τη διατήρηση του απορρήτου της διαδικασίας φόρτισης οχημάτων EV [42] και των διαπιστευτηρίων του οχήματος και του οδηγού EV. Για τον σκοπό αυτό, προτείνεται ένα σχήμα ελέγχου της ταυτότητας που λαμβάνει υπόψη την κινητικότητα των οχημάτων EV σε κατανεμημένα καθώς και σε κεντρικοποιημένα δίκτυα V2G [214].

Όσον αφορά στον έλεγχο ταυτότητας ενός οχήματος EV, το πρότυπο ISO/IEC 15118 [109] περιλαμβάνει μια διάταξη για την ασφαλή σύνδεση του οχήματος EV στις εγκαταστάσεις φόρτισης. Αυτή διατίθεται σε δύο λειτουργίες αναγνώρισης, δηλαδή τη *λειτουργία PnC* και τη *λειτουργία εξωτερικής αναγνώρισης (External Identification Mode, EIM)*. Ωστόσο, έχει αναδειχθεί ότι το πρότυπο έχει ορισμένα μειονεκτήματα [215],[216]. Για παράδειγμα, η λειτουργία PnC μπορεί να πιστοποιήσει μόνο ένα νόμιμα συνδεδεμένο όχημα EV, ενώ η λειτουργία εξωτερικής αναγνώρισης EIM μπορεί να ελέγξει μόνο έναν νόμιμα συνδεδεμένο οδηγό EV. Αυτό σημαίνει ότι ένα μη εξουσιοδοτημένο όχημα EV μπορεί να φορτιστεί με την επιβάρυνση μιας έγκυρης έξυπνης κάρτας οδηγού EV. Σημαίνει επίσης ότι ένα όχημα EV με εξουσιοδοτημένο ψηφιακό πιστοποιητικό μπορεί να φορτιστεί ακόμη και αν ο οδηγός του EV δεν είναι εξουσιοδοτημένος χρήστης.

Εν ολίγοις, το πρότυπο ορίζει μια μέθοδο που βασίζεται στη χρήση πιστοποιητικών για τον έλεγχο της ταυτότητας και την εξουσιοδότηση, η οποία όμως είναι μονότροπη και μονολιθική και, ως εκ τούτου, παρέχει χαμηλά επίπεδα ασφάλειας. Οι αντίπαλοι μπορούν να το εκμεταλλευτούν για να ενεργοποιήσουν επιθέσεις MitM [215] και επιθέσεις αντικατάστασης [223].

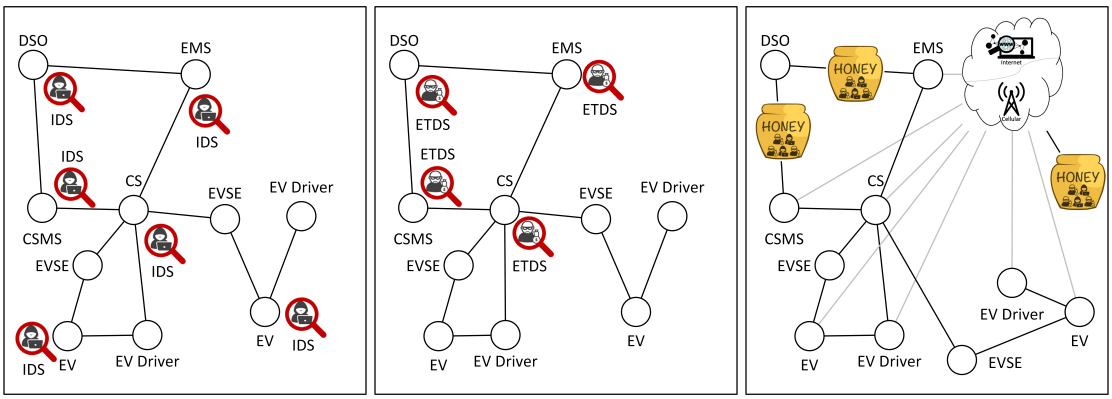
Οι πρόσφατες προτάσεις για τον μετριασμό τέτοιων επιθέσεων περιλαμβάνουν μηχανισμούς ελέγχου της ταυτότητας που αναπτύσσουν πολλαπλούς τρόπους διαπίστευσης με διαπιστευτήρια που λαμβάνονται από πολλαπλές διαδρομές, προτού ο σταθμός φόρτισης CS επιτρέψει στον οδηγό/ ιδιοκτήτη του οχήματος EV να ξεκινήσει τη διαδικασία φόρτισης. Ένα σύστημα ελέγχου της ταυτότητας πολλαπλών μέσων και πολλαπλών διελεύσεων με χρήση πιστοποιητικού σύμβασης (Multimodal and Multi-pass Authentication Scheme using Contract Certificate, MMA-CC) έχει πρόσφατα προταθεί [154]. Αυτό το σχήμα έχει δύο φάσεις. Πρώτον, μια φάση εκκίνησης όπου εκδίδεται ένα πιστοποιητικό σύμβασης (CCert) στο όχημα EV για την υποστήριξη ασφαλών και αξιόπιστων ενημερώσεων από τον αρχικό κατασκευαστή εξοπλισμού OEM [97]. Στη συνέχεια, και μόνο αφού ληφθεί το CCert, η διαδικασία φόρτισης προχωράει στη φάση λειτουργίας MMA-CC, όπου το CCert αποστέλλεται για επικύρωση. Η φόρτιση μπορεί να ξεκινήσει μόνο αφού ληφθεί μια απάντηση σχετικά με τη νομιμότητα των διαπιστευτηρίων.

Από την ίδια ερευνητική ομάδα έχει προταθεί, επίσης, μια λύση που βασίζεται σε έξυπνες κάρτες και ονομάζεται σύστημα ελέγχου της ταυτότητας πολλαπλών μέσων και πολλαπλών διελεύσεων με χρήση έξυπνης κάρτας (Multimodal and Multi-pass Authentication Scheme using Smart Card, MMA-SC). Το MMA-SC αξιοποιεί έξυπνες κάρτες τεχνολογίας RFID ή επικοινωνίας κοντινού πεδίου (Near-field communication, NFC) και στοχεύει σε οχήματα EV που δεν διαθέτουν ψηφιακά πιστοποιητικά ούτε υποστηρίζουν το V2G PKI [154]. Αυτή η λύση είναι ευάλωτη σε κλασικές επιθέσεις κλωνοποίησης έξυπνων καρτών, αν και η πολύτροπη φύση της διασφαλίζει ότι αυτές οι επιθέσεις κλωνοποίησης δεν θα είναι αποτελεσματικές.

Επιπλέον, στο σχήμα MMA-CC απαιτούνται ένα νόμιμο πιστοποιητικό σύμβασης και έγκυρα διαπιστευτήρια χρήστη, ενώ ένα νόμιμο αναγνωριστικό ετικέτας έξυπνης κάρτας και έγκυρα διαπιστευτήρια χρήστη απαιτούνται επίσης στο MMA-SC, για μια επιτυχημένη διαδικασία φόρτισης οχήματος EV. Επομένως, μπορεί να μετριαστούν οι επιθέσεις MitM. Όσον αφορά στις επιθέσεις αντικατάστασης και στα δύο σχήματα, η διαδικασία φόρτισης EV δεν προχωρά έως ότου επικυρωθεί ο έλεγχος της ταυτότητας πολλαπλών μέσων και πολλαπλών διελεύσεων, δηλαδή το CCert ή η έξυπνη κάρτα και τα διαπιστευτήρια χρήστη, επομένως δεν είναι δυνατή μια επίθεση αντικατάστασης.

#### 5.2.6.3 Μηχανισμοί ανίχνευσης και εκτροπής

Οι διαδικασίες έξυπνης φόρτισης EV κληρονομούν ένα πλήθος ζητημάτων και ευπαθειών ασφάλειας από τα συμμετέχοντα σε αυτές δρώντα στοιχεία. Αυτές οι ευπάθειες σχετίζονται με τα ίδια τα δρώντα στοιχεία, δηλαδή τα οχήματα EV (όπως πλαστοπροσωπία, φυσικές βλάβες), τα μηνύματα που ανταλλάσσονται μεταξύ των σταθμών φόρτισης CS (όπως απόρρητο δεδομένων, παραβίαση) και το μέσο επικοινωνίας που χρησιμοποιείται (όπως DoS, DDoS, MitM, παρεμβολές RF, υποκλοπή) [42]. Οι απειλές που σχετίζονται με την αρχιτεκτονική του OCPP και την ασύρματη επικοινωνία,




(α) Κατανεμημένα IDS (β) ETDS (γ) Honeypots

Εικόνα 18. Μηχανισμοί ανίχνευσης και εκτροπής σε δίκτυα φόρτισης PEV

ενδέχεται να σχετίζονται και με τα ακόλουθα [40]:

*(α)* Αποκάλυψη πληροφοριών ή παράνομη ανάγνωση/αντιγραφή πληροφοριών.

*(β)* Παραμόρφωση πληροφοριών, εισαγωγή (πλαστών) δεδομένων, πλαστογράφηση ή τροποποίηση δεδομένων, διεργασιών, διαμορφώσεων.

*(γ)* Παραποίηση πληροφοριών, διαγραφή ή απόρριψη μηνυμάτων, διαδικασιών, ενεργειών.

Για την αντιμετώπιση αυτών των προβλημάτων ασφάλειας σε μια αρχιτεκτονική OCPP, το κατανεμημένο σύστημα ανίχνευσης εισβολών IDS μπορεί να λειτουργεί από διάφορες θέσεις αισθητήρων του δικτύου [217] (Εικόνα 18α). Οι κατανεμημένοι ανιχνευτές IDS που χρησιμοποιούνται στα δίκτυα PEV είναι προσαρμοσμένοι στις των δικτύων PEV για [40]:

*(α)* ελαφρούς μηχανισμούς ανίχνευσης που βασίζονται στη γνώση του περιβάλλοντος, όπως τα περιορισμένα IDS, και

*(β)* ελαφρά συστήματα βασισμένα στην αξιοπιστία για να διασφαλιστεί ότι οι πληροφορίες που λαμβάνονται από έναν κόμβο είναι αξιόπιστες και ότι η συνδεσιμότητα δικτύου των κόμβων είναι αδιάλειπτη.

Οι πληροφορίες που απαιτούνται για τον εντοπισμό επιθέσεων σε κατανεμημένες υποδομές μέτρησης τάσεως, όπως τα δίκτυα μετρητών AMI και τα δίκτυα PEV, ταξινομούνται ως ακολούθως [217]:

*(α)* *Πληροφορίες συστήματος*: οι αναφορές καλής λειτουργίας των μετρητών, η κατανάλωση της μπαταρίας, η υπερφόρτωση του ρεύματος, η κλοπή ενέργειας, η ακεραιότητα του λογισμικού των συσκευών AMI και ο συγχρονισμός ρολογιού.

*(β)* *Πληροφορίες δικτύου*: ο ρυθμός των συγκρούσεων, η απώλεια των πακέτων, ο χρόνος απόκρισης των κόμβων, ο ρυθμός της κίνησης δεδομένων, η καλή λειτουργία και η ακεραιότητα μετάδοσης των μηνυμάτων, οι συσχετισμοί μεταξύ των φυσικών διευθύνσεων και της ταυτότητας του κόμβου.

Οι επιθέσεις που αφορούν στην κατηγορία *πληροφοριών συστήματος* επηρεάζουν το AMI, το οποίο υποστηρίζει την αμφίδρομη επικοινωνία μεταξύ έξυπνων μετρητών και συστημάτων κοινής ωφέλειας. Τέτοιες επιθέσεις στον κυβερνοχώρο αφορούν στην υπερφόρτωση ενέργειας ή στην επίθεση κλοπής ενέργειας και μπορεί να μετριαστούν με ένα σύστημα ανίχνευσης κλοπής ενέργειας ETDS, που μπορεί αποτελεσματικά να ανιχνεύσει επιθέσεις κλοπής ενέργειας κατά των δικτύων μετρητών AMI και να τις διαφοροποιήσει από άλλες επιθέσεις στον κυβερνοχώρο (Εικόνα 18β). Τα ETDS χρησιμοποιούν λύσεις βασισμένες σε ταξινόμηση ή λύσεις βασισμένες σε συστάδες για τον σχεδιασμό ενός πλαισίου ανίχνευσης ανωμαλιών που βασίζεται σε μοτίβα. Αυτός ο τύπος συνεχούς παρακολούθησης πολλαπλών επιπέδων του φορτίου κατανάλωσης ενέργειας επιτρέπει τον αποτελεσματικό και έγκαιρο εντοπισμό τέτοιων επιθέσεων. Ένα παράδειγμα χρήσης ενός ETDS είναι ο ανιχνευτής κλοπής ενέργειας βάσει μοτίβων κατανάλωσης (Consumption Pattern-Based Energy Theft Detector, CPBETD) [170], ο οποίος είναι ανθεκτικός ενάντια σε επιθέσεις μόλυνσης και μη κακόβουλες αλλαγές στα πρότυπα κατανάλωσης, επιτυγχάνει υψηλό ποσοστό ανίχνευσης και έχει χαμηλό ψευδο-θετικό ποσοστό FPR.

Στις επιθέσεις που σχετίζονται με την κατηγορία *πληροφοριών δικτύου*, το κύριο πρόβλημα για την υποδομή έξυπνου πλέγματος SG είναι ο σχεδιασμός του δικτύου, το οποίο δεν έχει τη δυνατότητα να αντιμετωπίσει το υπάρχον χάσμα μεταξύ των απαιτήσεων ασφάλειας/ανθεκτικότητας και της υποστήριξης οικονομικά ανεκτών επικοινωνιών έξυπνου πλέγματος SG. Ένα τέτοιο δίκτυο πρέπει να υποστηρίζει την παρακολούθηση όλων των επικοινωνιών από ένα IDS και να παρέχει αδιάλειπτη λειτουργικότητα ακόμη και σε περίπτωση αποτυχίας ή επίθεσης. Η τοποθέτηση των συστημάτων IDS και του βέλτιστου αριθμού συναθροιστών θα πρέπει να γίνεται λαμβάνοντας υπόψη την κατανάλωση ενέργειας κάθε συναθροιστή, το κόστος του ηλεκτρονόμου (relay) και του συναθροιστή, καθώς και τις καθυστερήσεις που προκύπτουν [168].

Ένα σημαντικό ζήτημα είναι η θέση των συστημάτων IDS στο δίκτυο και η αντιστάθμιση μεταξύ κόστους και ασφάλειας. Έχει προταθεί η χρήση honeypot στο δίκτυο AMI ως δόλωμα για τον εντοπισμό DDoS/DoS και τη συλλογή πληροφοριών επίθεσης (Εικόνα 18γ) [219]. Επίσης, έχει προταθεί ο σχεδιασμός μιας ανθεκτικής υποδομής επικοινωνίας SG, όπου τα συστήματα IDS θα είναι κατανεμημένα για να διασφαλίζεται η παρακολούθηση των ροών με το ελάχιστο δυνατό κόστος [218]. Στην περίπτωση αυτή διερευνάται μια προσέγγιση βασισμένη σε μοντέλα παραγωγής στήλης για την αντιμετώπιση των προβλημάτων που εντοπίστηκαν σε σύντομο υπολογιστικό χρόνο. Παρομοίως, προτείνεται ένα πλαίσιο βασισμένο σε μοντέλο κόστους για να βοηθήσει στις διαδικασίες ανίχνευσης των συστημάτων IDS [217]. Το πλαίσιο αυτό χρησιμοποιεί τα αποτελέσματα των μεθοδολογιών αξιολόγησης του κινδύνου, οι οποίες αντιπροσωπεύουν την είσοδο σε ένα μοντέλο συστήματος υποστήριξης αποφάσεων. Το μοντέλο μπορεί να χρησιμοποιηθεί για την ανάλυση της αντιστάθμισης μεταξύ κόστους και οφέλους από την εγκατάσταση IDS σε διαφορετικές τοποθεσίες. Αυτή η περίπτωση λαμβάνει υπόψη και το δίκτυο επικοινωνίας (μήτρα συνδεσιμότητας) στη διαδικασία λήψης αποφάσεων και, τελικά, προσδιορίζει τις βέλτιστες θέσεις για το σύστημα IDS.

Τέλος, υπάρχουν μηχανισμοί άμυνας που μπορούν να προστατεύσουν τη φόρτιση των οχημάτων EV και να ανιχνεύσουν επιθέσεις παρεμβολής και πλαστογράφησης. Ένα νέο αναγνωριστικό πολλαπλών επιπέδων για την ανίχνευση επιθέσεων πλαστογράφησης κατά

της ασύρματης επικοινωνίας των συνδεδεμένων EV προτείνεται στο [220]. Οι Gai et al. [221] εισάγουν έναν νέο μηχανισμό επίθεσης που χρησιμοποιεί τόσο παρεμβολές όσο και πλαστογράφηση για να παρέμβει στις κανονικές ασύρματες επικοινωνίες του έξυπνου πλέγματος υιοθετώντας προσεγγίσεις γνωσιακής ραδιο-δικτύωσης.

Όλα τα προαναφερθέντα IDS βοηθούν στην ανίχνευση επιθέσεων, που ξεκινούν από το δίκτυο AMI και κινούνται προς επιθέσεις φυσικού επιπέδου MAC ή PHY, και διατερματικές επιθέσεις επιπέδου εφαρμογής μεταξύ κόμβων του δικτύου AMI. Οι κύριες μετρικές που χρησιμοποιούνται για τον εντοπισμό τους είναι κάποιες παράμετροι, όπως ο λόγος σήματος προς παρεμβολές και θόρυβο (Signal to Interference and Noise Ratio, SINR), ο ρυθμός παράδοσης πακέτων (Packet Delivery Ratio, PDR) και οι διατερματικές καθυστερήσεις.

Οι επιθέσεις μεταμφίεσης, υποκλοπής, έγχυσης δεδομένων και επανάληψης μεταδόσεων μπορεί να συμβούν όταν τα μηνύματα μεταξύ των μονάδων ελέγχου των οχημάτων ECU δεν είναι κρυπτογραφημένα και πιστοποιημένα. Για την προστασία από αυτούς τους τύπους επιθέσεων, ο κώδικας επαλήθευσης μηνυμάτων MAC [125] μπορεί να χρησιμοποιηθεί για την ασφάλεια της κυκλοφορίας μηνυμάτων CAN μεταξύ των υποσυστημάτων της ECU. Ωστόσο, το MAC συχνά δεν μπορεί να ενταχθεί στα τυπικά πεδία δεδομένων CAN. Επιπλέον, τα μηνύματα CAN μεταδίδονται σε όλους τους κόμβους χωρίς διάκριση. Ένα IDS που ενσωματώνει τη μηχανική μάθηση για την εκπαίδευση και την αναγνώριση της μη φυσιολογικής συμπεριφοράς, προτείνεται ως εναλλακτική ή συμπλήρωμα του MAC στα [157],[158].

Συμπερασματικά, ένα ανοιχτό ζήτημα σχετικά με την ασφάλεια του OCPP είναι η ενοποίηση των IDS που σχετίζονται με το δίκτυο και των IDS που σχετίζονται με την αρχιτεκτονική του συστήματος, με κύριο στόχο τον σχεδιασμό ενός IDS πολλαπλών επιπέδων, ικανού να ανιχνεύει κάθε είδους επίθεση που αφορά στο επίπεδο εφαρμογής καθώς και στα κατώτερα επίπεδα. Έτσι, η εύρεση της καλύτερης αντιστάθμισης για ένα επεκτάσιμο και ολοκληρωμένο IDS πολλαπλών επιπέδων είναι το κλειδί για την ανάπτυξη αισθητήρων και συστημάτων στις βέλτιστες θέσεις εντός του δικτύου.

## 5.3 Ευπάθειες του δικτύου φόρτισης και επιπτώσεις στην iBuC

Η ασφάλεια ενός δικτύου φόρτισης PEV συναρτάται από την ασφάλεια των δρώντων στοιχείων που συμμετέχουν σε αυτό. Συνεπώς, όλες οι προαναφερθείσες επιθέσεις ασφάλειας που επηρεάζουν ένα ή περισσότερα από τα δομικά στοιχεία του δικτύου φόρτισης PEV, πρέπει να ληφθούν υπόψη και στο θέμα της ασφάλειας του ίδιου του δικτύου. Για την εφαρμογή της διαδικασίας αξιολόγησης της ασφάλειας είναι σημαντικές, επίσης, οι αδυναμίες ή οι ευπάθειες των δρώντων στοιχείων του δικτύου φόρτισης PEV, τις οποίες είναι πιθανό να εκμεταλλευτούν οι προαναφερθείσες επιθέσεις.

### 5.3.1 Ευπάθειες του δικτύου φόρτισης

Οι ευπάθειες που είναι καταγεγραμμένες και σχετίζονται άμεσα με τα δρώντα στοιχεία ενός δικτύου φόρτισης PEV, που βασίζεται στο πρωτόκολλο OCPP, είναι οι ακόλουθες:

- **CVE-2018-7800** - Η ευπάθεια αυτή επιτρέπει πρόσβαση του επιτιθέμενου στον εξοπλισμό σύνδεσης EVSE με πλήρη δικαιώματα. Μέσω αυτής της πρόσβασης μπορεί να αποκτήσει τον πλήρη έλεγχο και να επηρεάσει τη διαθεσιμότητα της υπηρεσίας [224],[225]:

  *(α)* σταματώντας τις διεργασίες φόρτισης,

  *(β)* θέτοντας τον σταθμό φόρτισης CS σε κατάσταση μη διαθέσιμου/κατειλημμένου ή

  *(γ)* απασφαλίζοντας το καλώδιο φόρτισης προς κακόβουλη ή ανεξέλεγκτη χρήση.

  Η CVE-2018-7800 υπάγεται στην αδυναμία [CWE-798: Use of Hard-coded Credentials] και χαρακτηρίζεται ως κρίσιμης δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 9.8) [52].
- **CVE-2018-7801** - Πρόκειται για ευπάθεια υψηλού κινδύνου, η ύπαρξη της οποίας επιτρέπει πρόσβαση του επιτιθέμενου στον εξοπλισμό σύνδεσης EVSE με πλήρη δικαιώματα, με χρήση αυθαίρετου κώδικα. Μέσω αυτής της πρόσβασης μπορεί να αποκτήσει τον πλήρη έλεγχο του λειτουργικού συστήματος του σταθμού φόρτισης CS [224],[225]. Η CVE-2018-7801 υπάγεται στην αδυναμία [CWE-94: Improper Control of Generation of Code ('Code Injection')] και χαρακτηρίζεται ως υψηλής δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 8.8) [52].
- **CVE-2018-7802** - Η ευπάθεια αυτή επιτρέπει πρόσβαση του επιτιθέμενου στη δικτυακή διεπαφή του εξοπλισμού σύνδεσης EVSE με πλήρη δικαιώματα, μέσω έγχυσης Structured Query Language (SQL) κώδικα [224], [225]. Η CVE-2018-7802 υπάγεται στην αδυναμία [CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')] και χαρακτηρίζεται ως υψηλής δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 8.8) [52].
- **CVE-2020-27813** - Η ευπάθεια αυτή επιτρέπει επιθέσεις κατά των μηνυμάτων του OCPP, μέσω παράτυπων μηνυμάτων JSON, με τα οποία παραβιάζονται οι περιορισμοί που διέπουν τον χώρο παροχής της υπηρεσίας φόρτισης. Τα παράτυπα μηνύματα ενδέχεται να περιλαμβάνουν και κυκλικές ή ενθυλακωμένες δομές [226]. Η CVE-2020-27813 υπάγεται στις αδυναμίες [CWE-190: Integer Overflow or Wrap-around] και [CWE-400: Uncontrolled Resource Consumption] και χαρακτηρίζεται ως υψηλής δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 7.5) [52].
- **CVE-2021-22706** - Η ευπάθεια αυτή επιτρέπει στον επιτιθέμενο να υποδυθεί τον αξιόπιστο χρήστη σταθμού φόρτισης και να πραγματοποιήσει ενέργειες εκ μέρους του, μέσω υποβολής κακόβουλων παραμέτρων στον διακομιστή ιστού του σταθμού φόρτισης CS [227]. Η CVE-2021-22706 υπάγεται στην αδυναμία [CWE-79: Improper Neutralization of Input During Web Page Generation

('Cross-site Scripting')] και χαρακτηρίζεται ως μέτριας δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 6.1) [52].

- **CVE-2021-22722** - Η ευπάθεια αυτή επιτρέπει στον επιτιθέμενο να αλλάξει τις παραμέτρους λειτουργίας του σταθμού φόρτισης CS με την έγχυση κακόβουλου κώδικα μέσω αρχείων CSV [227]. Η CVE-2021-22722 υπάγεται στην αδυναμία [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')] και χαρακτηρίζεται ως μέτριας δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 5.4) [52].
- **CVE-2021-22729** - Η ευπάθεια αυτή επιτρέπει στον επιτιθέμενο να παρακάμψει τους σχετικούς ελέγχους εξουσιοδότησης και να αποκτήσει δικαιώματα διαχειριστή κατά την πρόσβαση στον διακομιστή ιστού του σταθμού φόρτισης CS [227]. Η CVE-2021-22729 υπάγεται στην αδυναμία [CWE-259: Use of Hard-coded Password] και χαρακτηρίζεται ως κρίσιμης δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 9.8) [52].
- **CVE-2021-22730** - Η ευπάθεια αυτή επιτρέπει στον επιτιθέμενο να παρακάμψει τους σχετικούς ελέγχους εξουσιοδότησης και να αποκτήσει δικαιώματα διαχειριστή κατά την πρόσβαση στον διακομιστή ιστού του σταθμού φόρτισης CS [227]. Η CVE-2021-22730 υπάγεται στην αδυναμία [CWE-798: Use of Hard-coded Credentials] και χαρακτηρίζεται ως κρίσιμης δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 9.8) [52].
- **CVE-2018-16669** - Η ευπάθεια αυτή επιτρέπει στον επιτιθέμενο την ανακάλυψη των διαπιστευτηρίων του διαχειριστή της υπηρεσίας, καθώς αυτά αποθηκεύονται σε αρχεία XML [52]. Η CVE-2018-16669 υπάγεται στην αδυναμία [CWE-522: Insufficiently Protected Credentials] και χαρακτηρίζεται ως κρίσιμης δριμύτητας ευπάθεια (βασική βαθμολογία CVSS 9.8) [52].

Η ευπάθεια CVE-2018-16669 αντλήθηκε από τη βάση δεδομένων NVD του οργανισμού NIST, ως η μοναδική ευπάθεια, απολύτως συναφής με το πρωτόκολλο OCPP.

Από τις εννέα (9) αυτές καταγεγραμμένες ευπάθειες, οι επτά (7) εντάσσονται στη λίστα ευπαθειών CVE της iBuC με υπηρεσία φόρτισης στόλου βασιζόμενη στο πρωτόκολλο OCPP (Πίνακας 12). Αξίζει να αναφερθούν τα ακόλουθα:

*(α)* Η ευπάθεια CVE-2021-22730 εισάγεται σε αντικατάσταση των CVE-2016-6829 και CVE-2018-7800 της ίδιας αδυναμίας [CWE-798: Use of Hard-coded Credentials]. Η CVE-2021-22730 επικράτησε ως πιο επίκαιρη και λόγω της συνάφειάς της με την υποδιεργασία φόρτισης οχημάτων.

*(β)* Η ευπάθεια CVE-2021-22706 επικράτησε της συναφούς CVE-2021-22722 [CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')], λόγω υψηλότερης δριμύτητας (βασική βαθμολογία CVSS 6.1 αντί 5.4).

Οι παραπάνω ευπάθειες, μετά την επεξεργασία που περιγράφεται παραπάνω, διαμόρφωσαν τη σχετική λίστα των ευπαθειών ενός δικτύου φόρτισης PEV, που βασίζεται στο πρωτόκολλο OCPP, όπως αυτή εμφανίζεται στον Πίνακα 12. Να σημειωθεί πως, στο στάδιο αυτό, συμπεριλήφθηκαν οι ευπάθειες που σχετίζονται ευθέως

με τα δρώντα στοιχεία του δικτύου φόρτισης. Οι ευπάθειες αυτές αντιπαραβλήθηκαν με τις ευπάθειες που σχετίζονται και με τα υπόλοιπα στοιχεία που συμμετέχουν στη διεργασία της διαχείρισης του στόλου και που έχουν μελετηθεί σε προηγούμενο κεφάλαιο. Το αποτέλεσμα της αντιπαραβολής ήταν η προσθήκη μίας νέας ευπάθειας προς αντικατάσταση υπάρχουσας. Στον Πίνακα 12 η νέα καταχώρηση σημειώνεται με γραμματοσειρά χρώματος κόκκινου, η δε υπάρχουσα που αντικαταστάθηκε σημειώνεται με γραμματοσειρά διαγράμμισης. Τέλος, η προσθήκη των υπόλοιπων έξι (6) νέων ευπαθειών σημειώνονται με γραμματοσειρά χρώματος μπλε.

Πίνακας 12. Λίστα CVE ευπαθειών iBuC με OCPP υπηρεσία φόρτισης στόλου

| **CVE** | **Description** | **CVSS** | |
|---|---|---|---|
| | | Base | Temporal |
| CVE-2017-7214 | Information Exposure | 9.8 | 9.1 |
| CVE-2018-4878 | (Resource) Use After Free | 9.8 | 9.1 |
| CVE-2018-8174 | Failure to Constrain Operations | 7.5 | 7.3 |
| CVE-2017-0199 | Access Control (Authorization) Issues | 7.8 | 6.6 |
| CVE-2018-7600 | Improper Input Validation | 9.8 | 8.5 |
| CVE-2018-12942 | OS Command Injection | 8.8 | 8.1 |
| CVE-2018-14643 | Improper Authentication | 9.8 | 8.8 |
| CVE-2018-10635 | Missing Critical Function Authentication | 9.8 | 7.9 |
| ~~CVE-2016-6829~~ | ~~Use of Hard-coded Credentials~~ | ~~9.8~~ | ~~8.7~~ |
| CVE-2021-22730 | Use of Hard-coded Credentials | 9.8 | 8.8 |
| CVE-2016-5788 | Improper Authorisation | 10 | 8.3 |
| CVE-2016-5062 | Incorrect Resource Transfer | 9.8 | 8.3 |
| CVE-2016-8209 | Improper Check | 7.5 | 6.6 |
| CVE-2017-5239 | Inadequate Encryption Strength | 7.5 | 7.1 |
| CVE-2017-17717 | Broken Cryptographic Algorithm | 9.8 | 9.3 |
| CVE-2017-7901 | Use of Insufficiently Random Values | 8.6 | 7.6 |
| CVE-2017-18146 | Improper Crypto Verification | 9.8 | 8.5 |
| CVE-2016-5069 | Insufficient Session Expiration | 9.8 | 9.1 |
| CVE-2016-7124 | Deserialization of Untrusted Data | 9.8 | 8.5 |
| CVE-2018-12689 | LDAP Injection | 9.8 | 9.3 |
| CVE-2018-7801 | Improper Code Generation Control | 8.8 | 8.2 |
| CVE-2018-7802 | SQL Injection | 8.8 | 7.9 |
| CVE-2020-27813 | Uncontrolled Resource Consumption | 7.5 | 6.7 |
| CVE-2021-22706 | Cross-site Scripting | 6.1 | 5.7 |
| CVE-2021-22729 | Use of Hard-coded Password | 9.8 | 8.8 |
| CVE-2018-16669 | Insufficiently Protected Credentials | 9.8 | 8.7 |

### 5.3.2 Επιπτώσεις στην ασφάλεια της iBuC

Η ασφάλεια της διαχείρισης στόλου της υπηρεσίας iBuC, όπως έχει ήδη περιγραφεί, επηρεάζεται από την ασφάλεια της υποδιεργασίας της φόρτισης των οχημάτων του στόλου. Για τον λόγο αυτό, οι ευπάθειες του πρωτοκόλλου OCPP, θα πρέπει να συμπεριληφθούν στην αξιολόγηση ασφάλειας της υπηρεσίας.

Πιο συγκεκριμένα, στο σενάριο iBuC-PTS επηρεάζονται οι ακόλουθες καταστάσεις:

*(α)* P0: Στόλος σε αναμονή,

*(β)* P4: Άφιξη σε προορισμό, στάθμευση/φόρτιση οχήματος,

*(γ)* P6: Ενεργοποίηση για πλήρη διαδρομή.

Και στις τρεις καταστάσεις, προβλήματα της υποδιεργασίας φόρτισης οχημάτων περιορίζουν τη διαθεσιμότητα του στόλου και άρα της υπηρεσίας iBuC. Αντίστοιχα, στο σενάριο iBuC-WFS επηρεάζονται μόνο οι καταστάσεις P0 και P4.

Πίνακας 13. Υπολογισμός μετρικών ασφάλειας με τις ευπάθειες της υπηρεσίας φόρτισης στόλου

| **CVE** | **Affected States** | **iBuC-PTS** | | | | | **iBuC-WFS** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | Rn | Pn | SM(0) | SM(t) | A | Rn | Pn | SM(0) | SM(t) |
| CVE-2017-7214 | P0,P1,P2,P3,P4,P5,P6 | 7 | 0.14 | 0.02 | 0.23 | 0.21 | 6 | 0.17 | 0.02 | 0.20 | 0.19 |
| CVE-2018-4878 | P1,P2,P3,P5 | 4 | 0.25 | 0.04 | 0.40 | 0.37 | 4 | 0.25 | 0.03 | 0.30 | 0.28 |
| CVE-2018-8174 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.03 | 0.25 | 0.24 | 4 | 0.25 | 0.03 | 0.23 | 0.22 |
| CVE-2017-0199 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.03 | 0.26 | 0.22 | 4 | 0.25 | 0.03 | 0.24 | 0.20 |
| CVE-2018-7600 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.03 | 0.32 | 0.28 | 4 | 0.25 | 0.03 | 0.30 | 0.26 |
| CVE-2018-12942 | P0,P1,P2,P3,P4,P5,P6 | 7 | 0.14 | 0.02 | 0.21 | 0.19 | 6 | 0.17 | 0.02 | 0.18 | 0.17 |
| CVE-2018-14643 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.03 | 0.27 | 0.24 | 5 | 0.20 | 0.02 | 0.24 | 0.22 |
| CVE-2018-10635 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.03 | 0.27 | 0.22 | 5 | 0.20 | 0.02 | 0.24 | 0.19 |
| CVE-2021-22730 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.03 | 0.27 | 0.24 | 5 | 0.20 | 0.02 | 0.24 | 0.22 |
| CVE-2016-5788 | P1,P5,P6 | 3 | 0.33 | 0.05 | 0.55 | 0.46 | 2 | 0.50 | 0.06 | 0.61 | 0.51 |
| CVE-2016-5062 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.03 | 0.32 | 0.27 | 4 | 0.25 | 0.03 | 0.30 | 0.25 |
| CVE-2016-8209 | P1,P5,P6 | 3 | 0.33 | 0.05 | 0.41 | 0.36 | 2 | 0.50 | 0.06 | 0.46 | 0.40 |
| CVE-2017-5239 | P0,P1,P3,P6 | 4 | 0.25 | 0.04 | 0.31 | 0.29 | 3 | 0.33 | 0.04 | 0.31 | 0.29 |
| CVE-2017-17717 | P0,P1,P3,P5,P6 | 5 | 0.20 | 0.03 | 0.32 | 0.31 | 4 | 0.25 | 0.03 | 0.30 | 0.28 |
| CVE-2017-7901 | P1,P5,P6 | 3 | 0.33 | 0.05 | 0.47 | 0.42 | 2 | 0.50 | 0.06 | 0.53 | 0.47 |
| CVE-2017-18146 | P1,P2,P3,P5 | 4 | 0.25 | 0.04 | 0.40 | 0.35 | 4 | 0.25 | 0.03 | 0.30 | 0.26 |
| CVE-2016-5069 | P0,P1,P2,P4,P6 | 5 | 0.20 | 0.03 | 0.32 | 0.30 | 4 | 0.25 | 0.03 | 0.30 | 0.28 |
| CVE-2016-7124 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.03 | 0.27 | 0.23 | 5 | 0.20 | 0.02 | 0.24 | 0.21 |
| CVE-2018-12689 | P0,P1,P2,P4,P5,P6 | 6 | 0.17 | 0.03 | 0.27 | 0.26 | 5 | 0.20 | 0.02 | 0.24 | 0.23 |
| CVE-2018-7801 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.48 | 0.45 | 2 | 0.50 | 0.06 | 0.54 | 0.50 |
| CVE-2018-7802 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.48 | 0.43 | 2 | 0.50 | 0.06 | 0.54 | 0.48 |
| CVE-2020-27813 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.41 | 0.37 | 2 | 0.50 | 0.06 | 0.46 | 0.41 |
| CVE-2021-22706 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.34 | 0.31 | 2 | 0.50 | 0.06 | 0.37 | 0.35 |
| CVE-2021-22729 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.54 | 0.48 | 2 | 0.50 | 0.06 | 0.60 | 0.54 |
| CVE-2018-16669 | P0,P4,P6 | 3 | 0.33 | 0.05 | 0.54 | 0.48 | 2 | 0.50 | 0.06 | 0.60 | 0.53 |
| **TOTALS** | | | | | **8.92** | **7.99** | | | | **8.86** | **7.94** |

Τα αποτελέσματα της αξιολόγησης, λαμβάνοντας υπόψιν τις ευπάθειες της υποδιεργασίας φόρτισης οχημάτων και του πρωτοκόλλου OCPP φαίνονται στον Πίνακα 13. Εκεί

βλέπουμε τις επτά (7) νέες ευπάθειες που έχουν προκύψει λόγω της υποδιεργασίας φόρτισης οχημάτων.

Πίνακας 14. Μετρικές ασφάλειας *(α)* με και *(β)* χωρίς τις ευπάθειες της υπηρεσίας φόρτισης στόλου

| **Μετρικές** | ***(α)*** | ***(β)*** | ***(α)-(β)%*** |
|---|---|---|---|
| Βασική SM(0) - iBuC-PTS | 8.92 | 9.14 | -2.43% |
| Χρονική SM(t) - iBuC-PTS | 7.99 | 8.15 | -1.91% |
| Βασική SM(0) - iBuC-WFS | 8.86 | 9.09 | -2.53% |
| Χρονική SM(t) - iBuC-WFS | 7.94 | 8.09 | -1.89% |

Στον Πίνακα 14 αντιπαραβάλλονται οι μετρικές ασφάλειας (βασική και χρονική) των δύο σεναρίων iBuC-PTS και iBuC-WFS, στις περιπτώσεις αξιολόγησης της ασφάλειας:

*(α)* με τη συμπερίληψη των ευπαθειών της υποδιεργασίας φόρτισης οχημάτων, και

*(β)* χωρίς τη συμπερίληψη των ευπαθειών της υποδιεργασίας φόρτισης οχημάτων.

Φαίνεται πως στην περίπτωση *(α)* για κάθε σενάριο οι μετρικές είναι βελτιωμένες κατά 1.89% - 2.52% σε σχέση με τις αντίστοιχες μετρικές της περίπτωσης *(β)*. Η μείωση αυτή οφείλεται στο ότι στην *(α)* περίπτωση έχουμε περισσότερες ευπάθειες υπό μελέτη, άρα το άθροισμα των συχνοτήτων εμφάνισης κάθε ευπάθειας $(R_i)$ αυξάνεται, μειώνοντας τον αντιστρόφως ανάλογο κίνδυνο κάθε ευπάθειας $(P_n)$ και τελικά μειώνοντας τις μετρικές ασφάλειας *SM(0)* και *SM(t)*.

Επίσης, είναι σημαντικό πως τέσσερεις από τις επτά ευπάθειες που εισάγει η υποδιεργασία φόρτισης οχημάτων έχουν βασική βαθμολογία CVSS μικρότερη από 8.9 και, άρα, πρόκειται για υψηλής και όχι κρίσιμης δριμύτητας ευπάθειες. Αναμενόμενα, και οι επτά ευπάθειες έχουν χρονική βαθμολογία CVSS μικρότερη από 8.9 και μάλιστα, δύο από τις επτά έχουν χρονική βαθμολογία CVSS μικρότερη από 6.9, που τις καθιστά μεσαίας δριμύτητας ευπάθειες.

# Κεφάλαιο 6

# Συμπεράσματα

## 6.1 Πλαίσιο και σκοπός

Στην εποχή του Διαδικτύου των Αντικειμένων, οι ευφυείς υπηρεσίες μεταφορών ενδείκνυνται για την επίλυση του προβλήματος πρώτου/τελευταίου μιλίου στα αστικά περιβάλλοντα. Η ασφάλεια και η φύση των λειτουργιών μιας τέτοιας υπηρεσίας ενδεχομένως να επηρεάζεται από τα χαρακτηριστικά της τριτομερούς υπηρεσίας, με την οποία έχει κοινή χρήση δεδομένων, στο πλαίσιο της διαλειτουργικότητάς της. Η ασφάλεια της υπηρεσίας ενδέχεται να επηρεάζεται και από υποδιεργασίες, όπως η στάθμευση και φόρτιση του στόλου. Η επικρατούσα διεθνώς υλοποίηση δικτύων φόρτισης οχημάτων με βάσει το πρωτόκολλο OCPP ενέχει ευπάθειες ασφάλειας, καθώς το πρωτόκολλο αναπτύσσεται κατά την τελευταία 10ετία.

Σκοπός της διατριβής αυτής ήταν η αξιολόγηση και διατήρηση του επιπέδου ασφάλειας μιας υπηρεσίας μεταφορών, παρά τις προκλήσεις που συνδέονται:

*(α)* με βασικά χαρακτηριστικά του Διαδικτύου των Αντικειμένων, όπως η ανταλλαγή δεδομένων με άλλες υπηρεσίες και

*(β)* με τη διαδικασία φόρτισης των οχημάτων της υπηρεσίας.

Σχετικά με το πρόβλημα του πρώτου/τελευταίου μιλίου παρουσιάστηκε το πρωτότυπο μιας υπηρεσίας μεταφορών με IoT χαρακτηριστικά με το όνομα iBuC, τα δομικά στοιχεία της υπηρεσίας, καθώς και ένας πλήρης κύκλος λειτουργίας της iBuC. Επίσης παρουσιάστηκε το αρχιτεκτονικό μοντέλο εφαρμογής της υπηρεσίας iBuC.

Σχετικά με την αξιολόγηση ασφάλειας μιας υπηρεσίας μεταφορών που βασίζεται στο IoT προτάθηκε η πλατφόρμα μετα-μοντελοποίησης και αξιολόγησης SAPnet. Περιγράφηκε η διαδικασία αξιολόγησης της ασφάλειας, παρουσιάστηκε αναλυτικά το μετα-μοντέλο, η σημασιολογία και οι αλγόριθμοι της SAPnet και παρουσιάστηκε η μοντελοποίηση και αξιολόγηση ασφάλειας της διεργασίας διαχείρισης στόλου της προτεινόμενης υπηρεσίας μεταφορών iBuC σε δύο σενάρια.

Σχετικά με την ασφάλεια των συστημάτων φόρτισης του στόλου οχημάτων EV, παρατέθηκαν οι καταγεγραμμένες επιθέσεις κατά των δικτύων φόρτισης οχημάτων EV και έγινε ο συσχετισμός της κάθε επίθεσης με τα επιμέρους δρώντα στοιχεία της

αρχιτεκτονικής των δικτύων φόρτισης EV, ώστε να είναι δυνατή η αξιολόγηση ασφάλειας της διεργασίας φόρτισης οχημάτων EV. Οι ευπάθειες του συστήματος φόρτισης του στόλου οχημάτων EV συνυπολογίστηκαν στην αξιολόγηση ασφάλειας της διαχείρισης στόλου της προτεινόμενης υπηρεσίας μεταφορών iBuC.

## 6.2 Ευφυής υπηρεσία μεταφορών iBuC

Σχετικά με την προτεινόμενη υπηρεσία μεταφορών iBuC, αναδείχθηκε η IoT φύση της καθώς φάνηκε πως πληροί τους δύο βασικούς όρους που απαιτούνται ώστε μια υπηρεσία να μπορεί να θεωρηθεί μέρος του IoT οικοσυστήματος:

*(α)* το αρχιτεκτονικό μοντέλο εφαρμογής της υπηρεσίας συμβαδίζει με το αρχιτεκτονικό μοντέλο αναφοράς ARM [68] των υλοποιήσεων που βασίζονται στο IoT και

*(β)* η υπηρεσία ενσωματώνει αρκετά IoT χαρακτηριστικά ώστε να χαρακτηρίζεται από διαφάνεια, πολλαπλή αξιοποίηση και καινοτομία των λειτουργιών και των δεδομένων της [37].

Το αρχιτεκτονικό μοντέλο εφαρμογής της iBuC συμβαδίζει απόλυτα και εμπεριέχει στοιχεία από όλα τα επίπεδα της αρχιτεκτονικής αναφοράς ARM μιας λύσης που βασίζεται στο IoT. Επίσης, η iBuC ενσωματώνει IoT χαρακτηριστικά ώστε να υποστηρίζει:

- τη διαφάνεια, καθώς υπηρεσίες και συστήματα τρίτων έχουν πρόσβαση στα δεδομένα της, τα οποία φυλάσσονται και επεξεργάζονται σε νεφοϋπολογιστική υποδομή,
- την πολλαπλή αξιοποίηση, καθώς τα δεδομένα της αξιοποιούνται και από άλλες υπηρεσίες, όπως η uBSS, και
- την καινοτομία, καθώς συνδράμει με τα δεδομένα της στην επίλυση και άλλων ζητημάτων εκτός του προβλήματος του πρώτου/τελευταίου μιλίου, όπως είναι η καταγραφή της κινητικότητας του πληθυσμού της κοινότητας στην πανεπιστημιούπολη.

## 6.3 Μοντελοποίηση και αξιολόγηση ασφάλειας

Σχετικά με το πρόβλημα της αξιολόγησης ασφάλειας μιας υπηρεσίας μεταφορών που βασίζεται στο IoT προτάθηκε η πλατφόρμα μετα-μοντελοποίησης και αξιολόγησης SAPnet, που περιλαμβάνει την εργαλειοθήκη οντολογίας SPN, εμπλουτισμένη με τα κατάλληλα εργαλεία για την αξιολόγηση της ασφάλειας του μοντέλου. Περιγράφηκε η διαδικασία αξιολόγησης της ασφάλειας που βασίζεται στο στοχαστικό μοντέλο SPN της υπηρεσίας. Επίσης, παρουσιάστηκε αναλυτικά το μετα-μοντέλο, η σημασιολογία και οι αλγόριθμοι της SAPnet. Ακόμα, παρουσιάστηκε η μοντελοποίηση και αξιολόγηση ασφάλειας της διεργασίας διαχείρισης στόλου της προτεινόμενης υπηρεσίας μεταφορών iBuC σε δύο σενάρια ανταλλαγής δεδομένων με διαφορετική ανά περίπτωση τριτομερή υπηρεσία.

Η μέθοδος μοντελοποίησης με χρήση του φορμαλισμού SPN και η αξιολόγηση της ασφάλειας βάσει του παραγόμενου μοντέλου, δεν είχε εφαρμοστεί σε υπηρεσία που βασίζεται στο IoT, όπως η iBuC. Ωστόσο, φάνηκε πως χάρη στα *κουπόνια ή μάρκες (Tokens)* και τις ρυθμίσεις *πυροδότησης των μεταβάσεων (transitions firing)*, στην SPN απεικονίζεται η διάρκεια των δραστηριοτήτων και η καθυστέρηση μεταξύ των συμβάντων και έτσι είναι εφικτή η μοντελοποίηση διεργασιών ή λειτουργιών πραγματικού χρόνου, αφού ο χρόνος που καταναλώνεται ανά κατάσταση επηρεάζει όλες τις ακόλουθες καταστάσεις του συστήματος ή της υπηρεσίας.

Με τη μοντελοποίηση της διαχείρισης στόλου της iBuC με αυτού του τύπου την καταστατική μοντελοποίηση, αναδείχθηκαν οι καταστάσεις της υπηρεσίας σε δύο σενάρια: στο πρώτο σενάριο η iBuC ενσωμάτωνε τα δεδομένα υπηρεσίας από ένα σύστημα δημόσιων μεταφορών PTS και, στο δεύτερο σενάριο η iBuC ενσωμάτωνε τα δεδομένα από το πληροφοριακό σύστημα μιας υπηρεσίας πρόγνωσης καιρού WFS. Έτσι αποδείχθηκε πως η αλλαγή τριτομερούς υπηρεσίας και η φύση των δεδομένων τα οποία δέχεται σε κάθε περίπτωση η υπηρεσία iBuC, αλλάζει την ίδια την υπηρεσία, όπως φάνηκε από τα μοντέλα iBuC-PTS και iBuC-WFS των δύο σεναρίων, αντίστοιχα.

Αυτή η αλλαγή της υπηρεσίας iBuC, όπως ήταν αναμενόμενο, επηρέασε και το επίπεδο ασφάλειας της iBuC στις δύο περιπτώσεις. Πιο συγκεκριμένα, τα μοντέλα iBuC-PTS και iBuC-WFS αξιολογήθηκαν για την ίδια λίστα ευπαθειών και διαπιστώθηκε πως η βασική μετρική *SM(0)* ήταν ελάχιστα μεγαλύτερη στην περίπτωση του μοντέλου iBuC-PTS, εξαιτίας της μίας επιπλέον κατάστασης (P6), σε σύγκριση με το μοντέλο iBuC-WFS. Το ίδιο παρατηρήθηκε και μετά τον μετριασμό των ευπαθειών, για τις τιμές των χρονικών μετρικών ασφάλειας *SM(t)*. Συνεπώς, φάνηκε πως η δυναμική προσαρμογή της iBuC σε τριτομερείς υπηρεσίες επηρεάζει και την ασφάλεια της, εάν οι πρόσθετες καταστάσεις που εισάγει η τριτομερής υπηρεσία επηρεάζονται από κρίσιμες ευπάθειες:

*(α)* με υψηλή βασική βαθμολογία CVSS,

*(β)* με δυνατότητα μετριασμού σε σεβαστό ποσοστό (μεγάλη απόκλιση μεταξύ βασικής και χρονικής βαθμολογίας CVSS) και

*(γ)* με επίδραση σε δρώντα στοιχεία που συμμετέχουν σε αρκετές καταστάσεις της υπηρεσίας.

Η διαδικασία μοντελοποίησης και αξιολόγησης εφαρμόστηκε και με την SAPnet, η οποία παρέχει μια φιλική διεπαφή για τη δημιουργία της λίστας ευπαθειών CVE του μοντέλου. Επίσης, παρέχει επιλογές εισαγωγής, εξαγωγής, αποθήκευσης και μετεγκατάστασης για τη δημιουργία της λίστας, διαδικασίες οι οποίες είναι χρονοβόρες στην περίπτωση της υλοποίησής τους μέσω της θεωρητικής προσέγγισης. Αυτά τα χαρακτηριστικά επιταχύνουν τη σύνθεση της λίστας και τυχόν ενημερώσεις της λίστας, σε περίπτωση αλλαγών του μοντέλου. Επιπλέον, μπορεί εύκολα να δημιουργηθεί η συσχέτιση μεταξύ των καταστάσεων και της λίστας CVE του μοντέλου και οι υπολογισμοί βάσει της μεθόδου αξιολόγησης εκτελούνται με ακρίβεια και ταχύτητα. Ως εκ τούτου, η SAPnet επιτρέπει τη γρήγορη επαναξιολόγηση της μετρικής ασφάλειας μετά από οποιαδήποτε πιθανή αλλαγή:

*(α)* των καταστάσεων του μοντέλου ή

*(β)* της λίστας των υπό μελέτη ευπαθειών.

## 6.4 Ασφάλεια δικτύων φόρτισης οχημάτων

Σχετικά με την ασφάλεια των συστημάτων φόρτισης του στόλου οχημάτων EV, παρατέθηκαν οι καταγεγραμμένες επιθέσεις κατά των δικτύων φόρτισης οχημάτων EV ή αλλιώς των δικτύων PEV και έγινε ο συσχετισμός της κάθε επίθεσης με τα επιμέρους δρώντα στοιχεία της αρχιτεκτονικής των δικτύων φόρτισης EV, ώστε να είναι δυνατή η αξιολόγηση ασφάλειας της διεργασίας φόρτισης οχημάτων EV. Καταγράφηκαν, επίσης σχετικά αντίμετρα ή προτάσεις καλής πρακτικής και επισημάνθηκε το μέρος των δρώντων στοιχείων της αρχιτεκτονικής που προφυλάσσεται ή έστω λαμβάνεται υπόψιν από την εκάστοτε προτεινόμενη λύση/αντίμετρο. Έγινε ειδική αναφορά στις τεχνικές διαφύλαξης απορρήτου, στους μηχανισμούς επαλήθευσης της ταυτότητας και εξουσιοδότησης και στους μηχανισμούς ανίχνευσης και εκτροπής που αφορούν στα δίκτυα φόρτισης οχημάτων EV.

Τέλος, καταγράφηκαν αναλυτικά οι ευπάθειες της διεργασίας φόρτισης οχημάτων που σχετίζονται με τα δρώντα στοιχεία της υπηρεσίας iBuC. Βάσει αυτών, επανυπολογίστηκε η μετρική ασφάλειας της διαχείρισης στόλου των δύο περιπτώσεων που έχουν ήδη παρουσιαστεί, της iBuC-PTS και της iBuC-WFS.

Το αρχιτεκτονικό μοντέλο εφαρμογής των δικτύων φόρτισης οχημάτων που παρουσιάστηκε, συστάθηκε βάσει των τοπολογιών που εισήχθησαν από τον φορέα OCA [77]. Το μοντέλο απεικονίζει τις κύριες οντότητες που συνεργάζονται σε έναν κύκλο ζωής της υπηρεσίας φόρτισης, δηλαδή:

*(α)* όλες τις συσκευές που βρίσκονται στην τοποθεσία φόρτισης, συμπεριλαμβανομένου του οχήματος-καταναλωτή σε ένα στιγμιότυπο της υπηρεσίας,

*(β)* τα συστήματα κορμού όπως, το σύστημα διαχείρισης CSMS και το σύστημα του διαχειριστή διανομής DSO και

*(γ)* όλα τα πρωτόκολλα και τα πρότυπα που εφαρμόζονται για την επικοινωνία στοιχείου-προς-στοιχείο των δικτύων αυτών.

Στη συνέχεια, ο συσχετισμός των επιθέσεων με τα επιμέρους δρώντα στοιχεία της αρχιτεκτονικής των δικτύων φόρτισης EV ανέδειξε κάποια κενά στην κάλυψη των ζητημάτων ασφάλειας των δικτύων αυτών, όπως:

- Στις επιθέσεις παραβίασης και στις επιθέσεις Man-in-the-middle, δεν υπάρχει συγκεκριμένο αντίμετρο για την προστασία του συστήματος διαχείρισης ενέργειας EMS.
- Στις επιθέσεις κατάστασης/αισθητήρων, πλαστογράφησης ARP και κλωνοποίησης κωδικών RKE δεν υπάρχει αντίμετρο για την προστασία οποιουδήποτε περιουσιακού στοιχείου.

Στο ίδιο πλαίσιο, μόλις εννέα ευπάθειες βρέθηκαν να σχετίζονται άμεσα με τα δρώντα στοιχεία ενός δικτύου φόρτισης PEV, που βασίζεται στο πρωτόκολλο OCPP, μία εκ των οποίων ήταν απολύτως συναφής με το πρωτόκολλο OCPP.

Οι ευπάθειες δικτύου φόρτισης PEV, που βασίζεται στο πρωτόκολλο OCPP συμπεριλήφθηκαν στην εκ νέου αξιολόγηση ασφάλειας της υπηρεσίας iBuC, για τις περιπτώσεις των σεναρίων iBuC-PTS και iBuC-WFS. Διαπιστώθηκε πως οι μετρικές ήταν ελάχιστα μικρότερες με την προσθήκη των ευπαθειών του δικτύου φόρτισης PEV, που οφείλεται στο ότι η διεύρυνση της λίστας των υπό μελέτη ευπαθειών, μεγαλώνει το άθροισμα των συχνοτήτων εμφάνισης κάθε ευπάθειας $(R_i)$, μειώνει τον αντιστρόφως ανάλογο κίνδυνο κάθε ευπάθειας $(P_n)$ και τελικά μειώνει τις μετρικές ασφάλειας $SM(0)$ και $SM(t)$. Επίσης, παρατηρήθηκε πως οι περισσότερες ευπάθειες που εισήγαγε η υποδιεργασία φόρτισης οχημάτων ήταν υψηλής και όχι κρίσιμης δριμύτητας και μετριαζόμενες μετατρέπονταν σε μεσαίας δριμύτητας. Καταλήγοντας, αποδείχθηκε πως το επίπεδο ασφάλειας της IoT υπηρεσίας μεταφορών επηρεάζεται περαιτέρω από τα ζητήματα ασφάλειας της υπηρεσίας φόρτισης οχημάτων του στόλου.

## 6.5 Μελλοντικές επεκτάσεις

Το επίπεδο υποστήριξης υπηρεσιών της προτεινόμενης υπηρεσίας μεταφορών iBuC θα μπορούσε να αποτελέσει τον πυρήνα μελλοντικής εργασίας, καθώς προέκυψε το ερώτημα εάν τα δεδομένα που σχετίζονται με τον εντοπισμό θέσης οχημάτων ή επιβατών, θα μπορούσαν να επηρεαστούν ως προς την ακρίβεια και την ταχύτητα υπολογισμού στην περίπτωση της συνδυαστικής παραγωγής τους από:

*(α)* το σύστημα GPS και

*(β)* μια μέθοδο εντοπισμού που βασίζεται σε σήματα Wi-Fi.

Η iBuC βασίζεται στην αυτόνομη λειτουργία των οχημάτων του στόλου της στο επίπεδο της μετακίνησης από σημείο σε σημείο, μέσω διαδρομής συμβατής με την σήμανση του οδικού δικτύου. Επίσης, τα οχήματα του στόλου είναι απαραίτητο να εκτελούν αποφυγή εμποδίων και να έχουν ομαλή οδηγική συμπεριφορά (για παράδειγμα να κινούνται με ομαλές αυξομειώσεις ταχύτητας). Τα AV οχήματα του στόλου και οι διαδικασίες λήψης αποφάσεων που εκτελούνται εντός των συστημάτων που αυτά φέρουν θα μπορούσαν μελλοντικά να βελτιωθούν με την ενσωμάτωση αλγορίθμων τεχνητής νοημοσύνης και συγκεκριμένα με την εφαρμογή Ενισχυτικής Μάθησης (Reinforcement Learning), όπου οι αλγόριθμοι λήψης αποφάσεων αναπροσαρμόζονται διαρκώς βάσει της αλληλεπίδρασης με το περιβάλλον.

Η προτεινόμενη υπηρεσία μεταφορών iBuC μελετήθηκε ως προς τα IoT χαρακτηριστικά της και πιο συγκεκριμένα μελετήθηκε πώς η υπηρεσία επηρεάζεται ως προς τις λειτουργίες της αλλά και ως προς το επίπεδο ασφάλειάς της, όταν ένα IoT χαρακτηριστικό της αλλάζει. Το δομικό IoT χαρακτηριστικό που μελετήθηκε ήταν η διαλειτουργικότητα με τριτομερή υπηρεσία και η αλλαγή αυτής. Ωστόσο, η ίδια μέθοδος θα μπορούσε να ακολουθηθεί και για τη μελέτη της επίδρασης άλλων IoT χαρακτηριστικών στη φύση μιας υπηρεσίας μεταφορών όπως η iBuC.

Η υπηρεσία μεταφορών iBuC είναι σχεδιασμένη για την εξυπηρέτηση μετακινήσεων εντός ενός ιδιωτικού/περιορισμένου τμήματος οδικού δικτύου και συγκεκριμένα λειτουργεί στο ιδιωτικό οδικό δίκτυο μιας πανεπιστημιούπολης. Ωστόσο, παρόμοια οδικά δίκτυα, όπως το οδικό δίκτυο αεροδρομίων πολλαπλών τερματικών σταθμών,

το οδικό δίκτυο μεταξύ συγκροτημάτων κτιρίων νοσοκομείων, το οδικό δίκτυο μιας στρατιωτικής βάσης ή το οδικό δίκτυο μαζικών χώρων αθλητικών εκδηλώσεων. Όλες αυτές οι περιπτώσεις ιδιωτικού/περιορισμένου τμήματος οδικού δικτύου θα μπορούσαν να αξιοποιήσουν τις δυνατότητες της υπηρεσίας iBuC. Μελλοντικός στόχος είναι η προσαρμογή των χαρακτηριστικών και η μελέτη της υπηρεσίας σε ένα διαφορετικό από το πανεπιστημιακό, ιδιωτικό οδικό δίκτυο.

Στόχος μελλοντικής αναβάθμισης της πλατφόρμας SAPnet είναι η ενσωμάτωση μιας πρόσθετης δυνατότητας για την απεικόνιση των δρώντων στοιχείων που συμμετέχουν σε κάθε κατάσταση του μοντέλου. Αυτή η δυνατότητα θα διευκολύνει τη συσχέτιση μεταξύ των καταστάσεων και των ευπαθειών. Επίσης, υπάρχουν περιπτώσεις όπου μια ακολουθία δύο ή περισσότερων ευπαθειών συνδέονται μεταξύ τους και ο αντίκτυπος της μιας διευκολύνει τις λειτουργίες της άλλης. Ως μελλοντική εργασία, θα αναπτυχθούν συναρτήσεις και κλάσεις στη SAPnet, έτσι ώστε να είναι εφικτός ο ορισμός τέτοιων αλυσίδων ευπαθειών στο μοντέλο. Ακόμα πιο καθοριστική μελλοντική αναβάθμιση της πλατφόρμας SAPnet θα είναι η προσθήκη της δυνατότητας καταγραφής των αδυναμιών που φέρουν τα δρώντα στοιχεία που συμμετέχουν σε κάθε κατάσταση του μοντέλου. Αυτή η δυνατότητα θα αυτοματοποιήσει σε μεγάλο βαθμό την αξιολόγηση ασφάλειας του μοντέλου, καθώς οι μετρικές θα προκύπτουν συνυπολογίζοντας και τα εγγενή χαρακτηριστικά των δρώντων στοιχείων.

Τέλος, σχετικά με την ασφάλεια των δικτύων φόρτισης οχημάτων, υπάρχουν επιθέσεις ασφάλειας, όπως η πλαστογράφηση ARP, η κλωνοποίηση RKE και οι επιθέσεις κατάστασης/αισθητήρα για τις οποίες δεν έχουν προταθεί έγκυρα αντίμετρα ή καλές πρακτικές. Επιπλέον, ορισμένα περιουσιακά στοιχεία, όπως το EMS, ενδεχομένως να μην έχουν κάλυψη από συγκεκριμένες επιθέσεις, σε αντίθεση με άλλα περιουσιακά στοιχεία. Επίσης, η επίσημη καταγραφή ευπαθειών των δρώντων στοιχείων δικτύων φόρτισης οχημάτων είναι μια σχετικά πρόσφατη διαδικασία, ως εκ τούτου η λίστα των ευπαθειών αυτών είναι σχετικά περιορισμένη. Η μελλοντική επαρκής κάλυψη των κενών αυτών, θα βελτιώσει το επίπεδο ασφάλειας των δικτύων φόρτισης οχημάτων και των συναφών υπηρεσιών, όπως μια υπηρεσία μεταφορών βασιζόμενη στο IoT.

# Δημοσιεύσεις


[1] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D. and Douligeris, C. (2022). Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP). In *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1504-1533, doi: 10.1109/COMST.2022.3184448.

[2] Garofalaki, Z., Kallergis, D., Douligeris, C. (2022). A Security Assessment Platform for Stochastic Petri Net (SPN) Modelling in the Internet of Things (IoT) Ecosystem. In: Karagiannis, D., Lee, M., Hinkelmann, K., Utz, W. (eds) Domain-Specific Conceptual Modeling. Springer, Cham. https://doi.org/10.1007/978-3-030-93547-4_13

[3] Kallergis, D., Garofalaki, Z., Katsikogiannis, G., Douligeris, C. (2020). CAPODAZ: A Containerised Authorisation and Policy-driven Architecture using Microservices. *Ad Hoc Networks*, (104), pp.102-153. https://doi.org/10.1016/j.adhoc.2020.102153

[4] Garofalaki, Z. and Kallergis, D. (2019). *On the Security of an IoT-based Intelligent Transportation Service*. In 2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDACECNSM), 20-22 Sep, Piraeus, Greece, pp.1-5.

[5] Garofalaki, Z., Kallergis, D. and C. Douligeris (2019). *Secure Fleet Management of an Intelligent Transportation Service in the IoT ecosystem*. In 3rd International Balkan Conference on Communications and Networking (BalkanCom2019), 10-12 Jun, Skopje, North Macedonia.

[6] Katsikogiannis, G., Kallergis, D., Garofalaki, Z., Mitropoulos, S. and Douligeris, C. (2018). A Policy-aware Service Oriented Architecture for Secure Machine-to-Machine Communications. *Ad Hoc Networks*, (80), pp.70-80. https://doi.org/10.1016/j.adhoc.2018.06.003

[7] Katsikogiannis, G., Garofalaki, Z., Kallergis, D. and Douligeris, C. (2018). *PDA: A Policy-driven for authorizations scheme with μServices*. In 2nd International Balkan Conference on Communications and Networking (BalkanCom2018), 6-8 Jun, Podgorica, Montenegro.

[8] Garofalaki, Z., Kallergis, D., Katsikogiannis, G., Ellinas, I. and Douligeris, C. (2017). *A DSS model for IoT-based intelligent transportation systems*. In 2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT2017), 18-20 Dec, Bilbao, Spain, pp.276-281.

[9] Garofalaki Z., Kallergis D., Katsikogiannis G. and Douligeris C. (2017). *A Policy-Aware Model for Intelligent Transportation Systems*. In 1st International Balkan Conference on Communications and Networking (BalkanCom2017), May 30-June 2, Tirana, Albania. arXiv preprint arXiv:1706.04803

[10] Garofalaki Z., Kallergis D., Katsikogiannis G., Ellinas I. and Douligeris C. (2016). *Transport services within the IoT ecosystem using localisation parameters*. 16th IEEE Symposium on Signal Processing and Information Technology (ISSPIT2016), 12-14 Dec, Limassol, Cyprus, pp.87-92.

# Βιβλιογραφικές Αναφορές


[1] T. M. Bojan, U. R. Kumar, and V. M. Bojan, "An internet of things based intelligent transportation system," in *2014 IEEE International Conference on Vehicular Electronics and Safety*, 16-17 Dec, Hyderabad, India, 2014, pp. 174–179. DOI: 10.1109/ICVES.2014.7063743.

[2] R. Neisse, G. Baldini, G. Steri, and V. Mahieu, "Informed consent in Internet of Things: The case study of cooperative intelligent transport systems," in *2016 23rd International Conference on Telecommunications (ICT)*, 16-18 May, Thessaloniki, Greece, 2016, pp. 1–5. DOI: 10.1109/ICT.2016.7500480.

[3] V. Cañas, A. García, J. Blanco, and J. de las Morenas, "The Internet of Things Applied to the Automotive Sector: A Unified Intelligent Transport System Approach," in *Service Orientation in Holonic and Multi-Agent Manufacturing*, T. Borangiu, D. Trentesaux, A. Thomas, and D. McFarlane, Eds. Cham: Springer International Publishing, 2016, pp. 53–60, ISBN: 978-3-319-30337-6. DOI: 10.1007/978-3-319-30337-6_5.

[4] J. Lawson, "Building an Intelligent Transportation System with the Internet of Things (IoT)," Intel Inc., Tech. Rep., 2017. [Online]. Available: https://silo.tips/download/building-an-intelligent-transportation-system-with-the-internet-of-things-iot.

[5] Lopez Research LLC, "Smart Cities Are Built On The Internet Of Things," Cisco Systems, Inc., Tech. Rep., 2014. [Online]. Available: http://www.cisco.com/web/solutions/trends/iot/docs/smart_cities_are_built_on_iot_lopez_research.pdf.

[6] D. Christie, A. Koymans, T. Chanard, J.-M. Lasgouttes, and V. Kaufmann, "Pioneering Driverless Electric Vehicles in Europe: The City Automated Transport System (CATS)," *Transportation Research Procedia*, vol. 13, pp. 30–39, 2016, ISSN: 2352-1465. DOI: 10.1016/j.trpro.2016.05.004.

[7] K. Bhargavi, N. Jayalaksmi, S. Malagi, and V. K. Jadoun, "Integration of Plug-in Electric Vehicles in Smart Grid: A Review," in *IEEE International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, 28-29 Feb, Mathura, India, 2020, pp. 214–219.

[8] H. ElHussini, C. Assi, B. Moussa, R. Atallah, and A. Ghrayeb, "A tale of two entities: Contextualizing the security of electric vehicle charging stations on the power grid," *ACM Transactions on Internet of Things*, vol. 2, no. 2, pp. 1–21, 2021.

[9] K. Kim, J. S. Kim, S. Jeong, J. H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers and Security*,

vol. 103, p. 102 150, 2021, ISSN: 01674048. DOI: 10.1016/j.cose.2020.102150.

[10] "Open Charge Alliance," Open Charge Alliance (OCA), Tech. Rep., 2020. [Online]. Available: https://www.openchargealliance.org/.

[11] Ampeco LTD, Ed., *Enable innovation and cost efficiency with OCPP*, 2022. [Online]. Available: https://www.ampeco.com/ocpp-open-charge-point-protocol/#cpo-benefits.

[12] Current AS, Ed., *Innovation and cost-efficiency in four letters: OCPP*, 2021. [Online]. Available: http://www.current.eco/platform/ocpp.

[13] Open Charge Alliance, Ed., *Open Charge Alliance - Our mission*, 2022. [Online]. Available: https://www.openchargealliance.org/about-us/.

[14] H. T. Mouftah and M. Erol-Kantarci, *Smart grid: networking, data management, and business models*. CRC Press, 2017.

[15] "Ultra Global PRT - Low cost transport for a sustainable future," Ultra Global PRT, Tech. Rep., 2012. [Online]. Available: https://www.ultraglobalprt.com/wp-content/uploads/2012/07/Ultra-Global-Brochure-PDF.pdf.

[16] J. Gustafsson, R. Lohmann, and M. Lowson, "Personal Rapid Transit Live Applications Challenges," in *Third International Conference on Urban Public Transportation Systems (ICUTS)*, 17-20 Nov, Paris, France: American Society of Civil Engineers (ASCE), 2013, pp. 347–356. DOI: 10.1061/9780784413210.031.

[17] "Korea's First Personal Rapid Transit (PRT), SkyCube," POSCO Holdings Inc., Tech. Rep., 2014. [Online]. Available: https://newsroom.posco.com/en/koreas-first-personal-rapid-transit-prt-skycube.

[18] J. N. Bajpai, "Emerging vehicle technologies & the search for urban mobility solutions," *Urban, Planning and Transport Research*, vol. 4, no. 1, pp. 83–100, 2016. DOI: 10.1080/21650020.2016.1185964.

[19] Z. Yu, L. Zhou, Z. Ma, and M. A. El-Meligy, "Trustworthiness Modeling and Analysis of Cyber-physical Manufacturing Systems," *IEEE Access*, vol. 5, pp. 26 076–26 085, 2017.

[20] D. Karagiannis, R. A. Buchmann, P. Burzynski, U. Reimer, and M. Walch, "Fundamental Conceptual Modeling Languages in OMiLAB," in *Domain-Specific Conceptual Modeling: Concepts, Methods and Tools*. Springer, 2016, pp. 3–30.

[21] D. Karagiannis, P. Burzynski, and E.-T. Miron, *The Imker Case Study - Practice with the Bee-Up Tool*, Zenodo, 2017. DOI: 10.5281/zenodo.345846.

[22] M. Aazam and X. Fernando, "Fog Assisted Driver Behavior Monitoring for Intelligent Transportation System," in *IEEE 86th Vehicular Technology Conference (VTC-Fall)*, IEEE, 2017, pp. 1–5.

[23] P. Tilocca, S. Farris, S. Angius, R. Argiolas, A. Obino, S. Secchi, S. Mozzoni, and B. Barabino, "Managing Data and Rethinking Applications in an Innovative Mid-sized Bus Fleet," *Transportation Research Procedia*, vol. 25, pp. 1899–1919, 2017.

[24] T. Kenyon, "Transportation Cyber-Physical Systems Security and Privacy," in *Transportation Cyber-Physical Systems*, Elsevier, 2018, pp. 115–151.

[25] B. Blum, "Cyberattacks on cars increased 225% in last three years," ISRAEL21c, Tech. Rep., 2022. [Online]. Available: https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/.

[26] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102 511, 2022.

[27] S. Acharya, Y. Dvorkin, and R. Karri, "Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020. DOI: 10.1109/TSG.2020.2994177.

[28] "Open Charge Point Protocol 2.0.1," Open Charge Alliance (OCA), Tech. Rep., 2018. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/.

[29] "Open Charge Point Protocol 1.6," Open Charge Alliance (OCA), Tech. Rep., 2015. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-16/.

[30] F. Buve, M. Jansen, P. Klapwijk, and R. d. Leeuw, "OCPP 2.0.1, Part 2 - Specification," Open Charge Alliance (OCA), Tech. Rep., 2020. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/.

[31] R.-j. Zhao and W. H. Moh, "Development of New Modality Municipal Public Transportation for Guangzhou—Group Rapid Transit System as Supplementary Linkage from Guangzhou City Center to its Eastern Tourism Zone," *Frontiers of Engineering Management*, vol. 2, no. 4, pp. 378–390, 2016. DOI: 10.15302/J-FEM-2015061.

[32] W. B. Daszczuk, J. Mieścicki, and W. Grabski, "Distributed algorithm for empty vehicles management in personal rapid transit (PRT) network," *Journal of Advanced Transportation*, vol. 50, no. 4, pp. 608–629, 2016. DOI: 10.1002/atr.1365.

[33] D. Etherington, *Google's self-driving car project is a world's fair fantasy turned city street reality*, 2014. [Online]. Available: https://techcrunch.com/2014/05/14/googles-self-driving-car-project-is-a-worlds-fair-fantasy-turned-city-street-reality/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANybo0B_ikDnPiCeGvWJeAy2aPsyQq8so0IC8tuVFIPcTySqDG4P4soPeVjnv7pvu75kPoR3A41tJn_HVv9NRzGGaNSqqbilWZFadqeNvlSBRmEiFKb6vjhc9vgPScFhwYANgCgfwobLq5YsbzqcysJFMYUkkwfy7SXbvY_ZjOkz.

[34] P. R. Jape and A. R. Wadhekar, "Minimum Cost Implementation of Autonomous Vehicle," *International Journal of Research in Engineering and Technology (IJRET)*, vol. 5, no. 2, pp. 113–116, 2016. DOI: 10.15623/ijret.2016.0502020.

[35] R. C. Teja, S. Poornima, K. Manisha, K. Mamatha Reddy, P. Sainath, and U. Prem Kumar, "Smart Eco Car," *International Journal of New Innovations in Engineering and Technology (IJNIET)*, vol. 4, no. 4, pp. 10–18, 2016.

[36] S. Blanco, *Ride in an autonomous Navya Arma shuttle for just 9,500 Euros a month*, 2017. [Online]. Available: https://insideevs.com/news/332417/ride-in-an-autonomous-navya-arma-shuttle-for-just-9500-euros-a-month/.

[37] I. Karaseitanidis, P. Lytrivis, A. Ballis, O. Raptis, and A. Amditis, "Automated Road Transport Systems in Mixed Urban Scenarios–Trikala City Case," in *22nd ITS World Congress*, 5-9 Oct, Bordeaux, France: National Academy of Sciences, 2015, pp. 1–8. DOI: 10.1145/2976767.2976812.

[38] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Computer Communications*, vol. 91-92, pp. 17–28, 2016, ISSN: 0140-3664. DOI: 10.1016/j.comcom.2016.06.006.

[39] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications*, vol. 10, pp. 13–28, 2017.

[40] C. Alcaraz, J. Lopez, and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017. DOI: 10.1109/TSG.2017.2669647.

[41] P. Van Aubel and E. Poll, "Security of EV-Charging Protocols," *(in press)*, 2021. [Online]. Available: https://www.polvanaubel.com/research/chargego/protocol-security-evaluation/protocol-security-evaluation-draft-2020-03-10.pdf.

[42] J. Antoun, M. E. Kabir, B. Moussa, R. Atallah, and C. Assi, "A Detailed Security Assessment of the EV Charging Ecosystem," *IEEE Network*, vol. 34, no. 3, pp. 200–207, 2020, ISSN: 1558156X. DOI: 10.1109/MNET.001.1900348.

[43] R. Metere, M. Neaimeh, C. Morisset, C. Maple, X. Bellekens, and R. M. Czekster, "Securing the Electric Vehicle Charging Infrastructure," *arXiv preprint arXiv:2105.02905*, p. 39, 2021.

[44] Z. Pourmirza and S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," in *IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, 11-13 Aug, Oshawa, Canada, 2021, pp. 111–116. DOI: 10.1109/SEGE52446.2021.9535052.

[45] M. S. Raboaca *et al.*, "An overview and performance evaluation of open charge point protocol from an electromobility concept perspective," *International Journal of Energy Research*, pp. 1–21, 2021.

[46] G. Rémy, S. Mehar, T. Sophy, S.-M. Senouci, F. Jan, and Y. Gourhant, "Green fleet management architecture: Application to economic itinerary planning," in *IEEE Globecom Workshops*, IEEE, 2012, pp. 369–373.

[47] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[48] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "Apparatus: A framework for security analysis in internet of things systems," *Ad Hoc Networks*, vol. 92, p. 101 743, 2019.

[49] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "ASTo: A tool for security analysis of IoT systems," in *IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, IEEE, 2017, pp. 395–400.

[50] N. Harrand, F. Fleurey, B. Morin, and K. E. Husa, "ThingML: A Language and Code Generation Framework for Heterogeneous Targets," in *Proceedings of the ACM/IEEE 19th International Conference on Model Driven Engineering*

*Languages and Systems*, ser. MODELS '16, Saint-malo, France: Association for Computing Machinery, 2016, pp. 125–135, ISBN: 9781450343213. DOI: 10.1145/2976767.2976812.

[51] A. Samandari, M. Ge, J. B. Hong, and D. S. Kim, "EEvaluating the Security of IoT Networks with Mobile Devices," in *IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC)*, IEEE, 2018, pp. 171–180.

[52] National Institute of Standards and Technology (NIST), *National Vulnerability Database (NVD)*, https://nvd.nist.gov/, 2019.

[53] S. Y. Enoch, J. B. Hong, M. Ge, and D. S. Kim, "Composite Metrics for Network Security Analysis," *CoRR*, 2020.

[54] M. A. B. Ahmadon, S. Yamaguchi, S. Saon, *et al.*, "On service security analysis for event log of IoT system based on data Petri Net," in *IEEE International Symposium on Consumer Electronics (ISCE)*, IEEE, 2017, pp. 4–8.

[55] S. Yamaguchi and H. Tanaka, "Modeling of Infection Phenomenon and Evaluation of Mitigation Methods for IoT Malware Mirai by Agent-Oriented Petri Net $PN^2$," in *IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, IEEE, 2018, pp. 1–2.

[56] M. A. B. Ahmadon and S. Yamaguchi, "On service orchestration of cyber physical system and its verification based on Petri Net," in *IEEE 5th Global Conference on Consumer Electronics*, IEEE, 2016, pp. 1–4.

[57] G. Fortino, W. Russo, C. Savaglio, M. Viroli, and M. Zhou, "Opportunistic cyberphysical services: A novel paradigm for the future Internet of Things," in *IEEE 4th World Forum on Internet of Things (WF-IoT)*, IEEE, 2018, pp. 488–492.

[58] L. Kanaris, A. Kokkinis, G. Fortino, A. Liotta, and S. Stavrou, "Sample Size Determination Algorithm for fingerprint-based indoor localization systems," *Computer Networks*, vol. 101, pp. 169–177, 2016.

[59] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter Level Localization Using WiFi," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication (SIGCOMM '15)*, 17-21 Aug, London, UK, 2015, pp. 269–282. DOI: 10.1145/2785956.2787487.

[60] D. Yoon, C. Kee, J. Seo, and B. Park, "Position Accuracy Improvement by Implementing the DGNSS-CP Algorithm in Smartphones," *Sensors*, vol. 16, no. 6, 2016. DOI: 10.3390/s16060910.

[61] W. MacDougall, "Industrie 4.0: Smart Manufacturing for the Future," Germany Trade and Invest, Gesellschaft für Außenwirtschaft und Standortmarketing mbH, Tech. Rep., 2014.

[62] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEEE Internet Initiative*, vol. 1, pp. 1–86, 2015.

[63] E. T. Specification, "Machine-to-Machine Communications (M2M); M2M Service Requirements. Technical Specification," Tech. Rep. 2010I08, 2010.

[64] S. Rhee, "Catalyzing the Internet of Things and smart cities: Global City Teams Challenge," in *2016 1st International Workshop on Science of Smart City Operations and Platforms Engineering (SCOPE) in partnership with Global City Teams Challenge (GCTC)(SCOPE-GCTC)*, IEEE, 2016, pp. 1–4. DOI: 10.1109/SCOPE.2016.7515058.

[65] G. Lee, J. Park, N. Kong, and N. Crespi, "The Internet of Things - Concept and Problem Statement," Internet Engineering Task Force, Tech. Rep., 2012.

[66] *The Institute Special Report: The Internet of Things*, 2014. [Online]. Available: https://iot.ieee.org/images/files/pdf/The_Institute-IoT.pdf.

[67] A. Pastor, "Project Deliverable D6.2 – Updated Requirements List. IoT-A, the European Lighthouse Integrated Project," IoT-A (257521), Tech. Rep., 2014. [Online]. Available: https://cocoa.ethz.ch/downloads/2014/01/1371_D6.2_Updated%20Requirements%20List.pdf.

[68] J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, "From Machine-to-Machine to the Internet of Things - Introduction to a New Age of Intelligence," in Academic Press, 2014.

[69] P. Ping, Z. Xuan, and M. Xinyue, "Research on Security Test for Application Software Based on SPN," *Procedia Engineering*, vol. 174, pp. 1140–1147, 2017.

[70] MITRE Corporation, *Common Vulnerabilities and Exposures: the Standard for Information Security Vulnerability Names*, https://cve.mitre.org, 2007.

[71] A. Khamparia and B. Pandey, "Threat driven modeling framework using petri nets for e-learning system," *SpringerPlus*, vol. 5, no. 446, pp. 1–16, 2016.

[72] *The ADOxx Metamodelling Platform - Welcome to ADOxx.org - ADOxx.org*, 2000. [Online]. Available: https://www.adoxx.org/live/web/home.

[73] H.-G. Fill and D. Karagiannis, "On the conceptualisation of modelling methods using the ADOxx meta modelling platform," *Enterprise Modelling and Information Systems Architectures (EMISAJ)*, vol. 8, no. 1, pp. 4–25, 2013.

[74] D. Karagiannis, W. Grossmann, and P. Höfferer, "Open model initiative: A feasibility study," *URL: www. openmodels. at*, 2008.

[75] S. Koch, S. Strecker, and U. Frank, "Conceptual Modelling as a New Entry in the Bazaar: The Open Model Approach," in *Open Source Systems*, E. Damiani, B. Fitzgerald, W. Scacchi, M. Scotto, and G. Succi, Eds., 8-10 Jun, Como, Italy: Springer, 2006, pp. 9–20. DOI: 10.1007/0-387-34226-5_2.

[76] D. Karagiannis, R. A. Buchmann, X. Boucher, S. Cavalieri, A. Florea, D. Kiritsis, and M. Lee, "OMiLAB: A Smart Innovation Environment for Digital Engineers," in *Boosting Collaborative Networks 4.0*, L. M. Camarinha-Matos, H. Afsarmanesh, and A. Ortiz, Eds., Springer International Publishing, 2020, pp. 273–282. DOI: 10.1007/978-3-030-62412-5_23.

[77] F. Buve, M. Jansen, and P. Klapwijk, "OCPP 2.0.1, Part 1 - Architecture & Topology," Open Charge Alliance (OCA), Tech. Rep., 2020. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/.

[78] S. Orcioni and M. Conti, "EV smart charging with advance reservation extension to the OCPP standard," *Energies*, vol. 13, no. 12, pp. 3263–3284, 2020, ISSN: 19961073. DOI: 10.3390/en13123263.

[79] J. Schlund, M. Pruckner, and R. German, "FlexAbility-Modeling and Maximizing the Bidirec-tional Flexibility Availability of Unidirectional Charging of Large Pools of Electric Vehicles," in *Proc. of the Eleventh ACM International Conference on Future Energy Systems*, 22-26 Jun, virtual event, Australia, 2020, pp. 121–132.

[80] E. Ancillotti, R. Bruno, S. Palumbo, C. Capasso, and O. Veneri, "Experimental set-up of DC PEV charging station supported by open and interoperable communication technologies," in *IEEE International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, 22-24 Jun, Anacapri Capri Island, Italy, 2016, pp. 677–682.

[81] J. W. Heron, J. Jiang, H. Sun, V. Gezerlis, and T. Doukoglou, "Demand-response round-trip latency of IoT smartgrid network topologies," *IEEE Access*, vol. 6, pp. 22 930–22 937, 2018.

[82] J. W. Heron and H. Sun, "Smart electric vehicle charging with ideal and practical com-munications in smart grids," in *IEEE Global Communications Conference (GLOBECOM)*, 9-13 Dec, Big Island, Hawaii, USA, 2019, pp. 1–6.

[83] L. Noel, G. Z. de Rubens, J. Kester, and B. K. Sovacool, *Vehicle-to-Grid: A Sociotechnical Transition Beyond Electric Mobility*. Springer, 2019.

[84] A. Wargers and D. Frenkel, "The world's first large-scale migration of OCPP based PEV charging infrastructure," Open Charge Alliance (OCA), Tech. Rep., pp. 1–24. [Online]. Available: https://www.openchargealliance.org/uploads/files/OCA-White_paper_on_OCPP_based_migration_version_5.0.pdf.

[85] M. van Amstel, R. Ghatikar, and A. Wargers, "Importance of Open Charge Point Protocol for the Electric Vehicle Industry," Open Charge Alliance (OCA), Tech. Rep., 2016. [Online]. Available: https://www.openchargealliance.org/uploads/files/OCA-EN_whitepaper_OCPP_vs_proprietary_protocols_v1.0.pdf.

[86] "Background Open Charge Alliance," Open Charge Alliance (OCA), Tech. Rep., 2009. [Online]. Available: https://www.openchargealliance.org/about-us/background/.

[87] "Road Vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and Applica-tion Protocol Requirements," International Organization for Standardization (ISO), Tech. Rep., 2014. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-2:ed-1:v1:en.

[88] "Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition," International Organization for Standardization (ISO), Tech. Rep., 2019. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-1:ed-2:v1:en.

[89] F. Buve, P. Klapwijk, and R. de Leeuw, "OCPP 2.0.1, Part 0 - Introduction," Open Charge Alliance (OCA), Tech. Rep., 2020. [Online]. Available: https://www.openchargealliance.org/protocols/ocpp-201/.

[90] D. Wellisch, J. Lenz, A. Faschingbauer, R. Pöschl, and S. Kunze, "Vehicle-to-grid AC charging station: an approach for smart charging development," *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 55–60, 2015.

[91] I. Buamod, E. Abdelmoghith, and H. T. Mouftah, "A review of OSI-based charging standards and eMobility open protocols," in *IEEE 6th International Conference on the Network of the Future (NOF)*, 30 Sep-2 Oct, Montreal, Canada, 2015, 9:1–9:7.

[92] M. Emre *et al.*, "Task 3.3.1 Review of existing power transfer solutions," EU Seventh Framework Programme, Tech. Rep., 2014, p. 189.

[93] D. Wellisch, S. Kunze, and R. Pöschl, "A modular software implementation for smart charging stations," in *IEEE International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, 8-11 Sep, Vienna, Austria, 2015, pp. 254–259.

[94] "Road Vehicles - Vehicle-to-Grid Communication Interface - Part 3: Physical and data link layer requirements," International Organization for Standardization

(ISO), Tech. Rep., 2015. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-3:en.

[95] M. Parchomiuk, A. Moradewicz, and H. Gawiński, "An Overview of Electric Vehicles Fast Charging Infrastructure," in *IEEE Progress in Applied Electrical Engineering (PAEE)*, 17-21 Jun, Koscielisko, Poland, 2019, 26:1–26:5.

[96] C. Hodge *et al.*, "Vehicle Cybersecurity Threats and Mitigation Approaches," National Renewable Energy Laboratory (NREL), Tech. Rep. NREL/TP-5400-74247, 2019, pp. 1–41. eprint: TP - 5400 - 74247 (NREL). [Online]. Available: https://www.nrel.gov/docs/fy19osti/74247.pdf.

[97] L. Buschlinger, M. Springer, and M. Zhdanova, "Plug-and-patch: Secure value added services for electric vehicle charging," in *ACM Proc. of the 14th International Conference on Availability, Reliability and Security*, 26-29 Aug, Canterbury, UK, 2019, 2:1–2:10, ISBN: 9781450371643. DOI: 10.1145/3339252.3339269.

[98] Z. Jakó and Á. Knapp, "Business Scenarios and Data Flow in NeMo Hyper-Network," in *IEEE International Conference on Smart Systems and Technologies (SST)*, 10-12 Oct, Osijek, Croatia, 2018, pp. 139–144.

[99] R. Bilolikar, A. Magal, N. Lepre, and J. Korsh, "Scaling Up Electric Vehicle Charging Infrastructure," Natural Resources Defense Council (NRDC), Tech. Rep., 2020. [Online]. Available: https://www.nrdc.org/sites/default/files/charging-infrastructure-best-parctices-202007.pdf.

[100] B. Douglas, J. McDonald, N. DeForest, and C. Gehbauer, "Los Angeles Air Force Base Vehicle-to-Grid Demonstration: Final Project Report," California Energy Commission, Tech. Rep. CEC-500-2018-025, 2017.

[101] "ECHONET Lite Specification, Version 1.13," ECHONET Consortium, Tech. Rep., 2018. [Online]. Available: https://echonet.jp/spec_v113_lite_en/.

[102] U. Willrett, "Grid integration e-mobility–Developments and challenges," in *19. Internationales Stuttgarter Symposium*, 19-20 Mar, Stuttgart, Germany: Springer, 2019, pp. 320–330.

[103] V. C. Pham, Y. Makino, K. Pho, Y. Lim, and Y. Tan, "IoT Area Network Simulator For Network Dataset Generation," *Journal of Information Processing*, vol. 28, pp. 668–678, 2020. DOI: 10.2197/ipsjjip.28.668.

[104] U. Willrett, "Standards for Implementing Smart Charging," *ATZ worldwide*, vol. 122, no. 12, pp. 64–67, 2020.

[105] M. Erol-Kantarci and H. T. Mouftah, "Pervasive Energy Management for the Smart Grid: Towards a Low Carbon Economy," in *Pervasive Communications Handbook*, CRC Press, 2017, pp. 251–269.

[106] "Open Intercharge Protocol," Hubject GMBH, Tech. Rep., 2018. [Online]. Available: https://www.hubject.com/en/downloads/oicp/.

[107] "Road vehicles — Vehicle to grid communication interface — Part 4: Network and application protocol conformance test," International Organization for Standardization (ISO), Tech. Rep., 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-4:ed-1:v1:en.

[108] "Road vehicles — Vehicle to grid communication interface — Part 5: Physical layer and data link layer conformance test," International Organization for Standardization (ISO), Tech. Rep., 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-5:ed-1:v2:en.

[109] "Road vehicles – Vehicle to grid communication interface – Part 8: Physical layer and data link layer requirements for wireless communication," International Organization for Standardization (ISO), Tech. Rep., 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-8:ed-2:v1:en.

[110] "Road vehicles — Vehicle to grid communication interface — Part 9: Physical and data link layer conformance test for wireless communication," International Organization for Standardization (ISO), Tech. Rep., 2021. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:15118:-9:dis:ed-1:v1:en.

[111] U. Willrett, "Electric vehicles–enablers for the energy transition?" In *Netzintegration der Elektromobilität 2018*, Springer, 2018, pp. 56–65.

[112] M. Neaimeh and P. B. Andersen, "Mind the gap-open communication protocols for vehicle grid integration," *Energy Informatics*, vol. 3, no. 1, 1:1–1:17, 2020.

[113] A. Gopstein, C. Nguyen, C. O'Fallon, D. Wollman, and N. Hasting, "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0," NIST Special Publication 800-53, Tech. Rep., 2020.

[114] D. G. Márquez, C. M. Fernández, P. R. Pinos, and K. Piotrowski, "Networking layer specification," EU Horizon 2020, Tech. Rep., 2020, p. 59.

[115] I. S. F. Gomes, Y. Perez, and E. Suomalainen, "Coupling small batteries and PV generation: a review," *Renewable and Sustainable Energy Reviews*, vol. 126, p. 109 835, 2020.

[116] R. Rodríguez *et al.*, "ICT requirements specifications," EU Horizon 2020, Tech. Rep., 2016.

[117] A. Sundararajan, A. Chavan, D. Saleem, and A. I. Sarwat, "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security," *Energies*, vol. 11, no. 9, pp. 2360–2381, 2018. DOI: 10.3390/en11092360.

[118] Y.-W. Chung, *Electric Vehicle–Smart Grid Integration: Load Modeling, Scheduling, and Cyber Security*. University of California, Los Angeles, 2020, p. 24.

[119] M. Marinelli *et al.*, "Electric Vehicles Demonstration Projects-An Overview Across Europe," in *IEEE 55th International Universities Power Engineering Conference (UPEC)*, 1-4 Sep, Turin, Italy, 2020, 19:1–19:6.

[120] "Open vs Closed Charging Stations: Advantages and Disadvantages," Greenlots, Tech. Rep., 2018, p. 8. [Online]. Available: https://greenlots.com/wp-content/uploads/2018/10/Open-Standards-White%20Paper-compressed.pdf.

[121] C. Levy-Bencheton, E. Darra, D. Bachlechner, and M. Friedewald, "Cyber security for smart cities—An architecture model for public transport," European Union Agency for Network and Information Security (ENISA), Tech. Rep., 2015.

[122] H. van den Brink, "EV charging Systems Security Requirements," European Network for Cyber Security (ENCS), Tech. Rep., 2017.

[123] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[124] A. Fuchs, D. Kern, C. Krauß, and M. Zhdanova, "HIP: HSM-based identities for plug-and-charge," in *ACM Proc. of the 15th International Conference on Availability, Reliability and Security*, 25-28 Aug, Dublin, Ireland, 2020, 33:1–33:6.

[125] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, pp. 100 214–100 242, 2020, ISSN: 22142096. DOI: 10.1016/j.vehcom.2019.100214.

[126] H. van den Brink, "The need for cybersecurity within the electric vehicle infrastructure - A study on the use of digital signatures in the electric vehicle infrastructure," in *30th International Electric Vehicle Symposium & Exhibition, EVS30*, 9-11 Oct, Stuttgart, Germany: European Association for Electromobility (AVERE), 2017, 7:5:1–7:5:10.

[127] M. van Eekelen, E. Poll, E. Hubbers, B. Vieira, and F. van den Broek, "An end-to-end security design for smart EV-charging for Enexis and ElaadNL," Technische Universiteit Eindhoven and Radboud Universiteit Nijmegen, Tech. Rep., 2014.

[128] M. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: an anonymous multi-user protocol," in *Proc. of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 3-6 Nov, Venice, Italy, 2014, pp. 939–945.

[129] A. C.-F. Chan and J. Zhou, "Cyber–physical device authentication for the smart grid electric vehicle ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.

[130] A. A. Soares, D. M. Mattos, Y. Lopes, D. S. Medeiros, N. C. Fernandes, and D. C. Muchaluat-Saade, "An Efficient Authentication Mechanism based on Software-Defined Networks for Electric Vehicles," in *IEEE 28th International Symposium on Industrial Electronics (ISIE)*, 12-14 Jun, Vancouver, Canada, 2019, pp. 2471–2476.

[131] R. Baker and I. Martinovic, "Losing the car keys: Wireless phy-layer insecurity in EV charging," in *Proc. of the 28th USENIX Security Symposium*, 14-16 Aug, Santa Clara, CA, USA, 2019, pp. 407–424, ISBN: 9781939133069.

[132] M. Khodari, A. Rawat, M. Asplund, and A. Gurtov, "Decentralized firmware attestation for in-vehicle networks," in *CPSS 2019 - Proc. of the 5th ACM Cyber-Physical System Security Workshop*, 8 Jul, Auckland, Australia, 2019, pp. 47–56, ISBN: 9781450367875. DOI: 10.1145/3327961.3329529.

[133] A. Rawat, M. Khodari, M. Asplund, and A. Gurtov, "Decentralized Firmware Attestation for In-Vehicle Networks," *ACM Trans. Cyber-Phys. Syst*, vol. 5, no. 1, p. 23, 2020. DOI: 10.1145/3418685.

[134] D. Zelle, M. Springer, M. Zhdanova, and C. Krauß, "Anonymous charging and billing of electric vehicles," in *ACM Proc. of the 13th International Conference on Availability, Reliability and Security*, 27-30 Aug, Hamburg, Germany, 2018, 22:1–22:10, ISBN: 9781450364485. DOI: 10.1145/3230833.3230850.

[135] S. M. Danish, K. Zhang, H. .-. Jacobsen, N. Ashraf, and H. K. Qureshi, "BlockEV: Efficient and Secure Charging Station Selection for Electric Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4194–4211, 2020. DOI: 10.1109/TITS.2020.3044890.

[136] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving Authentication scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5760–5772, 2020. DOI: 10.1109/TVT.2020.2977361.

[137] H. Nicanfar, S. Hosseininezhad, P. TalebiFard, and V. C. Leung, "Robust privacy-preserving authentication scheme for communication between Electric Vehicle as Power Energy Storage and power stations," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 14-19 Apr, Turin, Italy, 2013, pp. 55–60. DOI: 10.1109/INFCOMW.2013.6562908.

[138] H. Li, G. Dán, and K. Nahrstedt, "Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2305–2313, 2016.

[139] P. Gope and B. Sikdar, "An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6607–6618, 2019.

[140] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet-Based Vehicle-to-Grid Technology Framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.

[141] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight Mutual Authentication Protocol for V2G Using Physical Unclonable Function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, 2020. DOI: 10.1109/TVT.2020.2976960.

[142] "Trusted Platform Module Library 2.0, Revision 01.59," Trusted Computing Group (TCG), Tech. Rep., 2019. [Online]. Available: https://trustedcomputinggroup.org/resource/tpm-library-specification/.

[143] A. Fuchs, D. Kern, C. Krauss, and M. Zhdanova, "TrustEV: trustworthy electric vehicle charging and billing," in *Proc. of the 35th Annual ACM Symposium on Applied Computing*, 30 Mar-3 Apr, Brno, Czech Republic, 2020, pp. 1706–1715. DOI: 10.1145/3341105.3373879.

[144] T. Lipman *et al.*, "Open-Source, Open-Architecture Software Platform for Plug-In Electric Vehicle Smart Charging in California," University of California – Berkeley, Transportation Sustainability Research Center, Tech. Rep., 2020, p. 230.

[145] S. Lightman and T. Brewer, *Symposium on federally funded research on cybersecurity of electric vehicle supply equipment (EVSE)*. US Department of Commerce, National Institute of Standards and Technology (NIST), 2020.

[146] A. Heinrich and R. Heddergott, "Secure and User-Friendly EV Charging A Comparison of Autocharge and ISO 15118's Plug & Charge," V2G Clarity, Hubject, Tech. Rep., 2019. [Online]. Available: https://uploads-ssl.webflow.com/607417b42ba2bfea543956dd/60c33c6cc823f9bb6bd4f275_Whitepaper-Autocharge-vs-ISO15118-Plug-and-Charge.pdf.

[147] A. R. Short, H. C. Leligou, and E. Theocharis, "Execution of a Federated Learning process within a smart contract," in *IEEE International Conference on Consumer Electronics (ICCE)*, 10-12 Jan, Las Vegas, NV, USA, 2021, pp. 1–4. DOI: 10.1109/ICCE50685.2021.9427734.

[148] G. Dhanush, K. S. Raj, and P. Kumar, "Blockchain Aided Predictive Time Series Analysis in Supply Chain System," in *Innovations in Electrical and Electronic Engineering*, Springer, 2021, pp. 913–925.

[149] X. Luo, Y. Li, X. Wang, and X. Guan, "Interval Observer-Based Detection and Localization against False Data Injection Attack in Smart Grids," *IEEE Internet*

*of Things Journal*, vol. 8, no. 2, pp. 657–671, 2021, ISSN: 23274662. DOI: 10.1109/JIOT.2020.3005926.

[150] Y. Fraiji, L. B. Azzouz, W. Trojet, and L. A. Saidane, "Cyber security issues of Internet of Electric Vehicles," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 15-18 Apr, Barcelona, Spain, 2018, pp. 1–6.

[151] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for Energy Internet based Vehicle-to-Grid technology framework," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4425–4435, 2020.

[152] M. E. Kabir, M. Ghafouri, B. Moussa, and C. Assi, "A Two-Stage Protection Method for Detection and Mitigation of Coordinated EVSE Switching Attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4377–4388, 2021.

[153] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing Security in OCPP: Protection Against Man-in-The-Middle Attacks," in *IEEE 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, vol. 2018-January, 26-28 Feb, Paris, France, 2018, 6:1–6:5, ISBN: 9781538636626. DOI: 10.1109/NTMS.2018.8328675.

[154] B. Vaidya and H. T. Mouftah, "Multimodal and Multi-pass Authentication Mechanisms for Electric Vehicle Charging Networks," in *IEEE International Wireless Communications and Mobile Computing, IWCMC 2020*, 15-19 Jun, Limassol, Cyprus, 2020, pp. 371–376, ISBN: 9781728131290. DOI: 10.1109/IWCMC48107.2020.9148231.

[155] Y. Li and B. Hu, "A Consortium Blockchain-Enabled Secure and Privacy-Preserving Optimized Charging and Discharging Trading Scheme for Electric Vehicles," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1968–1977, 2020.

[156] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2627–2637, 2019.

[157] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee, "Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 4757–4770, 2018. DOI: 10.1109/TVT.2018.2810232.

[158] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2114–2129, 2018. DOI: 10.1109/TIFS.2018.2812149.

[159] H. ElHusseini, C. Assi, B. Moussa, R. Attallah, and A. Ghrayeb, "Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 24–29, 2020, ISSN: 2576-3180. DOI: 10.1109/iotm.0001.1900081.

[160] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "EVExchange: A Relay Attack on Electric Vehicle Charging System," *arXiv preprint arXiv:2203.05266*, p. 20, 2022.

[161] Y. Li and B. Hu, "An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain," *IEEE*

*Transactions on Smart Grid*, vol. 11, no. 3, pp. 2627–2637, 2020. DOI: 10.1109/TSG.2019.2958971.

[162] A. G. Morosan and F. Pop, "OCPP security - Neural network for detecting malicious traffic," in *ACM Proc. of the 2017 Research in Adaptive and Convergent Systems, RACS 2017*, vol. 2017-January, 13-16 Oct, Gwangju , Republic of Korea, 2017, pp. 190–195, ISBN: 9781450350273. DOI: 10.1145/3129676.3129693.

[163] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Computer Science - Research and Development*, vol. 33, pp. 71–79, 2017.

[164] J. Li *et al.*, "Decentralized On-Demand Energy Supply for Blockchain in Internet of Things: A Microgrids Approach," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1395–1406, 2019. DOI: 10.1109/TCSS.2019.2917335.

[165] S. M. Danish, K. Zhang, and H. .-. Jacobsen, "A Blockchain-Based Privacy-Preserving Intelligent Charging Station Selection for Electric Vehicles," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2-6 May, Toronto, ON, Canada, 2020, PD2A6:1–PD2A6:3. DOI: 10.1109/ICBC48266.2020.9169419.

[166] A. Gharaibeh *et al.*, "Smart cities: A survey on data management, security, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456–2501, 2017.

[167] P. van Aubel, E. Poll, and J. Rijneveld, "Non-Repudiation and End-to-End Security for Electric-Vehicle Charging," in *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 29 Sep-2 Oct, Bucharest, Romania, 2019, pp. 191–195. DOI: 10.1109/ISGTEurope.2019.8905444.

[168] A. Ghasempour and J. H. Gunther, "Finding the optimal number of aggregators in machine-to-machine advanced metering infrastructure architecture of smart grid based on cost, delay, and energy consumption," in *13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 9-12 Jan, Las Vegas, NV, USA, 2016, pp. 960–963. DOI: 10.1109/CCNC.2016.7444917.

[169] A. A. Korba, N. Tamani, Y. Ghamri-Doudane, and N. E. I. Karabadji, "Anomaly-based framework for detecting power overloading cyberattacks in smart grid AMI," *Computers & Security*, vol. 96, p. 101 896, 2020. DOI: 10.1016/j.cose.2020.101896.

[170] P. Jokar, N. Arianpoo, and V. C. M. Leung, "Electricity Theft Detection in AMI Using Customers' Consumption Patterns," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, 2016. DOI: 10.1109/TSG.2015.2425222.

[171] R. Uhlig, M. Stoetzel, M. Stiegler, S. Lamberth, and A. Kubis, "Hybrid Cascaded Operation of Distribution Grids," in *International ETG-Congress 2019; ETG Symposium*, 8-9 May, Esslingen, Germany: VDE, 2019, 7:1–7:6.

[172] A. Kubis, M. Boller, J. Kemper, R. Uhlig, M. Stötzel, and M. Stiegler, "Enhancing operational awareness of distribution system operators with a semi-autonomous intelligent grid control suite," in *CIRED 25th International Conference on Electricity Distribution, CIRED 2019*, 3-6 Jun, Madrid, Spain: AIM, 2019, 1850:1–1850:5. DOI: 20.500.12455/607.

[173] M. H. Amini, J. Mohammadi, and S. Kar, "Distributed holistic framework for smart city infrastructures: tale of interdependent electrified transportation network and power grid," *IEEE Access*, vol. 7, pp. 157 535–157 554, 2019.

[174] G. Putrus *et al.*, "Overview SEEV4-city playing field state-of-the-art assessment of smart charging and vehicle 2 Grid services," Amsterdam University of Applied Sciences, Tech. Rep., 2020.

[175] S. Übermasser *et al.*, "Optimized and enhanced grid architecture for electric vehicles in Europe," *Elektrotech. Inftech.*, vol. 134, no. 1, pp. 78–85, 2017. DOI: 10.1007/s00502-016-0454-2.

[176] J. Kirby and F. Hassan, "AC Recharging Infrastructure for EVs and future smart grids - A review," *IEEE Proc. of the Universities Power Engineering Conference*, pp. 1–6, 2012. DOI: 10.1109/UPEC.2012.6398639.

[177] B. Zhang, R. B. Carlson, J. G. Smart, E. J. Dufek, and B. Liaw, "Challenges of future high power wireless power transfer for light-duty electric vehicles—-technology and risk management," *eTransportation*, vol. 2, p. 100 012, 2019. DOI: 10.1016/j.etran.2019.100012.

[178] G. Li, J. Wu, J. Li, T. Ye, and R. Morello, "Battery status sensing software-defined multicast for V2G regulation in smart grid," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7838–7848, 2017.

[179] T. Kobashi *et al.*, "Chapter 9 - Smart city and ICT infrastructure with vehicle to X applications toward urban decarbonization," in *Urban Systems Design*, Elsevier, 2020, pp. 289–333. DOI: 10.1016/B978-0-12-816055-8.00009-9.

[180] M. Nürnberg and S. Iwan, "Application of Telematics Solutions for Improvement the Availability of Electric Vehicles Charging Stations," in *Development of Transport by Telematics*, vol. 1049, Springer, 2019, pp. 287–301.

[181] M. Aspragkathos, *A systems approach to designing new mobility and smart grid services: the World's Smartest Grid showcase*. Technische Universiteit Eindhoven, 2014.

[182] V. Delgado-Gomes *et al.*, "H2020-646184 NOBEL GRID New Cost Efficient Business Models for Flexible Smart Grids," Athens University of Economics and Business (AUEB), Tech. Rep., 2016. [Online]. Available: http://stecon.cs.aueb.gr/media/1203/nobel-grid-d26-final-nobelgrid-business-models.pdf.

[183] Y. Zhang, R. Nakanishi, M. Sasabe, and S. Kasahara, "Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things," *Sensors*, vol. 21, no. 15:5053, 2021. DOI: 10.3390/s21155053.

[184] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[185] G. Xu, P. Moulema, L. Ge, H. Song, and W. Yu, "A Unified Framework for Secured Energy Resource Management," *Smart Grid: Networking, Data Management, and Business Models*, pp. 73–96, 2016.

[186] A. Iqbal, A. A. Khan, V. Kumar, and M. Ahmad, "A Mutual Authentication and Key Agreement Protocol for Vehicle to Grid Technology," in *Innovations in Electrical and Electronic Engineering*, vol. 756, Springer, 2021, pp. 863–875.

[187] J. Kester, L. Noel, X. Lin, G. Zarazua de Rubens, and B. K. Sovacool, "The coproduction of electric mobility: Selectivity, conformity and fragmentation in the sociotechnical acceptance of vehicle-to-grid (V2G) standards," *Journal of*

*Cleaner Production*, vol. 207, pp. 400–410, 2019. DOI: 10.1016/j.jclepro.2018.10.018.

[188] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *50th IEEE Conference on Decision and Control and European Control Conference*, 12-15 Dec, Orlando, FL, USA, 2011, pp. 4054–4059. DOI: 10.1109/CDC.2011.6160456.

[189] M. N. Kurt, Y. Yilmaz, and X. Wang, "Distributed Quickest Detection of Cyber-Attacks in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, pp. 2015–2030, 8 2018.

[190] S. Acharya, Y. Dvorkin, and R. Karri, "Public plug-in electric vehicles+ grid data: Is a new cyberattack vector viable?" *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 5099–5113, 2020.

[191] D. Hall and N. Lutsey, "Literature review on power utility best practices regarding electric vehicles," International Council on Clean Transportation (ICCT), Tech. Rep., 2017.

[192] F. Wu, J. Gibbs, S. Kleinbaum, and C. Schutte, "FY2017 Materials Annual Progress Report," US Dept. of Energy (DOE), Washington DC (United States), Tech. Rep., 2018.

[193] D. Wohlschlager, S. Haas, and A. Neitz-Regett, "Comparative environmental impact assessment of ICT for smart charging of electric vehicles in Germany," *Procedia CIRP*, vol. 105, pp. 583–588, 2022.

[194] J. Howden, L. Maglaras, and M. A. Ferrag, "The security aspects of automotive over-the-air updates," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 10, no. 2, pp. 64–81, 2020.

[195] J. Díaz *et al.*, "Electric vehicle charging points mobile application," Google Patents, Tech. Rep., 2018, US Patent App. 15/849,811.

[196] U. Satapathy, B. K. Mohanta, D. Jena, and S. Sobhanayak, "An ECC based Lightweight Authentication Protocol for Mobile Phone in Smart Home," in *IEEE 13th International Conference on industrial and information systems (ICIIS)*, 1-2 Dec, Rupnagar, India, 2018, pp. 303–308.

[197] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018. DOI: 10.1109{/}TII.2017.2786307.

[198] R. B. Bobba, K. M. Rogers, Q. Wang, K. N. Himanshu Khurana, and T. J. Overbye, "Detecting False Data Injection Attacks on DC State Estimation," in *1st Workshop on Secure Control Systems (SCS 2010), CPSWEEK2010*, 12 Apr, Stockholm, Sweden, 2010, pp. 1–9.

[199] M. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Smart electric vehicle charging: Security Analysis," in *Proc. of the IEEE PES Innovative Smart Grid Technologies (ISGT)*, 24-27 Feb, Washington, DC, USA, 2013, 46:1–46:6. DOI: 10.1109/ISGT.2013.6497830.

[200] J. Liu, M. Au, W. Susilo, and J. Zhou, "Enhancing location privacy for electric vehicles (at the right time)," in *Proc. of the 17th European Symposium on Research in Computer Security*, 10-12 Sep, Pisa, Italy: Springer, 2012, pp. 397–414.

[201] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L. Yang, and M. Guizani, "Securing vehicle–to-grid communications in the smart grid," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 66–73, 2013.

[202] Y. Zhang, Y. Xiao, K. Ghaboosi, J. Zhang, and H. Deng, "A survey of cyber crimes," *Security and Communication Networks*, vol. 5, no. 4, pp. 422–437, 2012.

[203] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology*, pp. 199–203, 1983. DOI: 10.1007/978-1-4757-0602-4_18.

[204] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-p- reserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2340–2346, 2015.

[205] M. Au, J. Liu, J. Fang, Z. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 3–18, 2014.

[206] A. Agarwal and R. Saraswat, "A survey of group signature technique, its applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 10, pp. 28–35, 2013.

[207] H. H. Liu Ning, Y. Zhang, and M. Guizani, "Battery status-aware authentication scheme for V2G networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 99–110, 2013.

[208] H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. Yan, "Role-dependent privacy preservation for secure V2G networks in the smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 208–220, 2014.

[209] C. Rottondi, S. Fontana, and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging," *Energies*, vol. 7, no. 5, pp. 2780–2798, 2014.

[210] S. Ozdemir and Y. Xiao, "Integrity protecting hierarchical concealed data aggregation for wireless sensor networks," *Computer Networks*, vol. 55, no. 8, pp. 1735–1746, 2011.

[211] Z. Wang and G. Zheng, "Residential Appliances Identification and Monitoring by a Nonintrusive Method," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 80–92, 2012. DOI: 10.1109/TSG.2011.2163950.

[212] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[213] H. Chen, Y. Xiao, X. Hong, F. Hu, and J. Xi, "A survey of anonymity in wireless communication systems," *Security and Communication Networks*, vol. 2, no. 5, pp. 427–444, 2009.

[214] N. Saxena and B. J. Choi, "Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, 2016, ISSN: 15566013. DOI: 10.1109/TIFS.2016.2532840.

[215] S. Lee, Y. Park, H. Lim, and T. Shon, "Study on analysis of security vulnerabilities and countermeasures in ISO/IEC 15118 based electric vehicle charging technology," in *IEEE Proc. of International Conference on IT Convergence and Security (ICITCS)*, 28-30 Oct, Beijing, China, 2018, T8P1:1–T8P1:4.

[216] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol ISO 15118," *Computer Science - Research and Development*, vol. 33, pp. 3–12, 2018.

[217] A. A. Cárdenas *et al.*, "A Framework for Evaluating Intrusion Detection Architectures in Advanced Metering Infrastructures," *IEEE Transactions on Smart Grid*, vol. 5, no. 2, pp. 906–915, 2014. DOI: 10.1109/TSG.2013.2291004.

[218] B. Genge, P. Haller, C. Dumitru, and C. Enăchescu, "Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2440–2451, 2017. DOI: 10.1109/TSG.2017.2665654.

[219] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017. DOI: 10.1109/TSG.2017.2670144.

[220] D. Kosmanos *et al.*, "A novel Intrusion Detection System against Spoofing Attacks in Connected Electric Vehicles," *Array*, vol. 5, p. 100 013, 2020. DOI: 10.1016/j.array.2019.100013.

[221] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu, "Spoofing-Jamming Attack Strategy Using Optimal Power Distributions in Wireless Smart Grid Networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2431–2439, 2017. DOI: 10.1109/TSG.2017.2664043.

[222] J. Chen, Y. Zhang, and W. Su, "An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks," *IEEE China Comm.*, vol. 12, no. 3, pp. 9–19, 2015.

[223] A. C.-F. Chan and J. Zhou, "Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014. DOI: 10.1109/JSAC.2014.2332121.

[224] K. Harnett, G. Watson, G. Brown, *et al.*, "Government Fleet and Public Sector Electric Vehicle Supply Equipment (EVSE) Cybersecurity Best Practices and Procurement Language Report," John A. Volpe National Transportation Systems Center (US), Tech. Rep., 2019.

[225] S. Saadat, S. Maingot, and S. Bahizad, "Electric vehicle charging station security enhancement measures," in *2020 5th IEEE Workshop on the Electronic Grid (eGRID)*, IEEE, 2020, pp. 1–8.

[226] D. Coats, H. Suryanarayana, Z. Wang, A. Brissette, Y. Zhang, V. Ramanan, D. Scoffield, D. Woodbury, N. Haltmeyer, and A. Benzinger, "Final Scientific/Technical Report-Cybersecurity for Grid Connected eXtreme Fast Charging (XFC) Station (CyberX)," ABB, Inc., Cary, NC (United States), Tech. Rep., 2021.

[227] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems," pp. 1–18, 2023. DOI: 10.14722/ndss.2023.23084.