ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Προκλήσεις Ασφάλειας και Κατηγοριοποίηση Επιθέσεων σε Εφαρμογές Αυτόνομων Οχημάτων (V2V) και Συστημάτων IoV

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ζήσης – Ραφαήλ Τζοάννος (ΑΜ: 3119062)

Επιβλέπων: ***Δρ. Ξενάκης Απόστολος, Επίκουρος Καθηγητής***

ΛΑΡΙΣΑ, Ιούνιος 2023

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Security Challenges and Attacks Classifications in Autonomous Vehicles and IoV Systems

BACHELOR THESIS

Zisis – Rafail Tzoannos (RN: 3119062)

Supervisor: ***Dr. Xenakis Apostolos, Assistant Professor***

LARISSA, June 2023

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

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

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

Ο Δηλών

Ζήσης – Ραφαήλ Τζοάννος

20/6/2023

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων	**Δρ. Απόστολος Ξενάκης** Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Δρ. Κωνσταντίνος Χαϊκάλης** Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Δρ. Όμηρος Ιατρέλλης** Επίκουρος Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Ημερομηνία έγκρισης: 27-06-2023

Περίληψη

Το Διαδίκτυο των πραγμάτων (IoT) είναι μία τεχνολογία που χρησιμοποιείται από πολύ μεγάλο αριθμό χρηστών τα τελευταία χρόνια, διότι διευκολύνει την χρήση συνδεδεμένων συσκευών στο διαδίκτυο σε πολλούς τομείς ένας εκ των οποίων είναι τα οχήματα. Το διαδίκτυο των οχημάτων (IoV) είναι μία τεχνολογία η οποία αναπτύσσεται ραγδαία. Πολλές εταιρίες επενδύουν αρκετά εκατομμύρια στον τομέα αυτό με σκοπό την δημιουργία αυτόνομων οχημάτων. Τα Connected and Autonomous Vehicles (CAV) χρησιμοποιούνται στις υπηρεσίες έξυπνων μεταφορών και προσφέρουν πολλά οφέλη τόσο στην κοινωνία όσο και στο περιβάλλον. Η μεγάλη εξέλιξη των αυτόνομων οχημάτων δημιουργεί ευπάθειες στα συστήματα ασφαλείας μέσω των οποίων μπορούν να πραγματοποιηθούν επιθέσεις με σκοπό να πλήξουν τόσο τα οχήματα όσο και τους επιβαίνοντες σε αυτά. Εξαιτίας αυτών των επιθέσεων δημιουργείται η ανάγκη για την λήψη μέτρων προστασίας καθώς και για την εύρεση αντιμέτρων με σκοπό την αποφυγή των επιθέσεων.

Η παρούσα πτυχιακή εργασία παρουσιάζει τις προκλήσεις ασφαλείας και τις μορφές επιθέσεων στα αυτόνομα οχήματα και στα συστήματα IoV. Γίνεται εκτενής αναφορά στο δίκτυο IoV, στην λειτουργία του καθώς και στα βασικά στοιχεία των αυτόνομων οχημάτων. Αναλύονται οι τομείς ευπάθειας των αυτόνομων οχημάτων, παρουσιάζονται διάφορες μορφές επιθέσεων αλλά προτείνονται και διάφορα αντίμετρα ενάντια σε αυτές τις επιθέσεις. Επιπλέον αυτή η εργασία επικεντρώνεται στα συστήματα CAV και στο δίκτυο VANET παραθέτοντας τους κινδύνους ασφαλείας και τους τρόπους αντιμετώπισης των επιθέσεων σε αυτά. Ακόμη, γίνεται σύγκριση των λύσεων-αλγορίθμων για την προστασία από τις διάφορες επιθέσεις καθώς και προσομοιώσεις επικοινωνίας μεταξύ οχημάτων χρησιμοποιώντας τα λογισμικά OMNeT++, VEINS και SUMO. Τέλος, γίνεται αναφορά στα συμπεράσματα της εργασίας καθώς και στις μελλοντικές προοπτικές σχετικά με την ασφάλεια των αυτόνομων οχημάτων και των συστημάτων IoV.

Abstract

The Internet of Things (IoT) is a technology that has been used by a very large number of users in recent years because it facilitates the use of internet-connected devices in many areas, one of which is vehicles. The Internet of Vehicles (IoV) is a rapidly developing technology. A lot of companies are investing several million in this field to create autonomous vehicles. The Connected and Autonomous Vehicles (CAV) are used in smart transport services and offer benefits to both society and the environment. The development of autonomous vehicles creates vulnerabilities in security systems through which attacks can be conducted to harm both the vehicles and their occupants. Because of these attacks, there is a need to take protective measures as well as to find countermeasures to avoid them.

This thesis presents the security challenges and attacks on autonomous vehicles and IoV systems. Extensive reference is made to the IoV network, its operation as well as the basic elements of autonomous vehicles. The areas of vulnerability of autonomous vehicles are analyzed, various attacks are presented but also various countermeasures against these attacks are proposed. In addition, this thesis focuses on CAV systems and VANET network, listing the security risks and ways to deal with attacks on them. Also, a comparison of the solutions-algorithms for the protection against the various attacks as well as simulations of communication between vehicles using the software OMNeT++, VEINS and SUMO is done. Finally, reference is made to the conclusions as well as future perspectives on the safety of autonomous vehicles and IoV systems.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον επίκουρο καθηγητή κ. Ξενάκη Απόστολο, επιβλέποντα της πτυχιακής μου εργασίας, για την καθοδήγηση και την βοήθεια που μου παρείχε. Επίσης, θεωρώ υποχρέωση μου να ευχαριστήσω τον υποψήφιο διδάκτορα κ. Καραμήτρο Γεώργιο για την βοήθεια που μου παρείχε σχετικά με την χρήση των λογισμικών προσομοίωσης. Τέλος, ευχαριστώ τους γονείς μου Σωτήριο Τζοάννο και Χρυσούλα – Αποστολία Παπαδημητρίου για την υλική και ηθική υποστήριξη που μου παρείχαν κατά την εκπόνηση της πτυχιακής μου εργασίας αλλά και καθ' όλη την διάρκεια των σπουδών μου.

Ζήσης – Ραφαήλ Τζοάννος

20/6/2023

Περιεχόμενα

1 Εισαγωγή

Η εξέλιξη της τεχνολογίας τις τελευταίες δεκαετίες είναι εντυπωσιακή. Αυτό έχει ως αποτέλεσμα διαφορετικές συσκευές που χρησιμοποιούνται στην καθημερινή μας ζωή να συνδέονται στο διαδίκτυο, να επικοινωνούν και να ανταλλάσσουν μηνύματα μεταξύ τους. Αυτό ονομάζεται Internet of Things (IoT) και περιγράφει φυσικά αντικείμενα ή ομάδες τέτοιων αντικειμένων με αισθητήρες, ικανότητα επεξεργασίας, λογισμικό και άλλες τεχνολογίες που συνδέονται και ανταλλάσσουν μηνύματα με άλλες συσκευές και συστήματα μέσω του διαδικτύου ή άλλων δικτύων επικοινωνιών. Ο όρος IoT εμφανίστηκε το 1999 όταν ο Kevin Ashton από το MIT το χρησιμοποίησε σε μια παρουσίαση του.

Το IoT είναι μία κορυφαία τεχνολογία που βρίσκεται σε συνεχή ανάπτυξη και επέκταση και περιλαμβάνει νέες βελτιωμένες συσκευές και υπηρεσίες. Αυτή η επέκταση έχει κάνει το IoT πολύ δημοφιλή και του δίνει την δυνατότητα να εφαρμόζεται σε διάφορους τομείς της έρευνας. Ένας τέτοιος τομέας είναι το δίκτυο ad hoc οχημάτων (VANET) που με την πάροδο του χρόνου εξελίχθηκε στο διαδίκτυο των οχημάτων (IoV). Χαρακτηριστικό παράδειγμα του IoT είναι η έννοια του έξυπνου σπιτιού που συμπεριλαμβάνει συσκευές όπως φωτιστικά, θερμοστάτες, συστήματα οικιακής ασφάλειας που υποστηρίζουν ένα ή περισσότερα οικοσυστήματα και μπορεί να ελεγχθεί μέσω συσκευών όπως τα έξυπνα κινητά τηλέφωνα και τα έξυπνα ηχεία. (P.A. Laplante κ.α., 2018; Sharma κ.α., 2018)

Το IoV είναι ένα δίκτυο οχημάτων που έχει ως σκοπό τη συλλογή δεδομένων χρησιμοποιώντας τους αισθητήρες που υπάρχουν στα οχήματα ή τις οδικές μονάδες όπως μονάδες GPS, LIDAR, αισθητήρες εικόνας κ.α. Αφενός, τα δεδομένα που συλλέγονται από τα οχήματα περιλαμβάνουν διάφορες παραμέτρους όπως την ταχύτητα ενός οχήματος, τη θέση του και την κατεύθυνση κίνησης του. Αφετέρου τα δεδομένα που συλλέγονται από τις οδικές μονάδες μπορούν να περιλαμβάνουν συνολικές πληροφορίες κυκλοφορίας. Όλα αυτά τα δεδομένα που συλλέγονται υποβάλλονται σε επεξεργασία με σκοπό την παροχή καλύτερης ταξιδιωτικής εμπειρίας, τη βελτίωση της οδηγικής ασφάλειας και την καλύτερη αντιμετώπιση των ατυχημάτων.

Χαρακτηριστική εφαρμογή του IoV αποτελούν οι οδικές μονάδες που τοποθετούνται κοντά στις διαβάσεις και μπορούν να ανιχνεύσουν την συμφόρηση των οχημάτων χρησιμοποιώντας είτε κάμερα είτε αισθητήρες που τοποθετούνται στους δρόμους. Τα συγκεκριμένα δεδομένα μπορούν να χρησιμοποιηθούν μαζί με άλλα δεδομένα που έχουν συλλεγεί από άλλες διαβάσεις για να παρέχουν μια ολοκληρωμένη εικόνα της κυκλοφορίας σε μία περιοχή. Μία άλλη εφαρμογή του IoV που έχει ως σκοπό την ασφάλεια είναι το σύστημα ενημέρωσης και ψυχαγωγίας που εφοδιάζονται τα οχήματα της εταιρείας Subaru. Αυτό το σύστημα είναι σε θέση να αντιλαμβάνεται την κούραση του οδηγού και να ηχεί κάποιο μήνυμα με σκοπό ο οδηγός να σταματήσει για να ξεκουραστεί. Ακόμη οι τεχνολογίες του IoV κυριαρχούν στα συστήματα των έξυπνων πόλεων και στα αυτοκίνητα χωρίς οδηγό. (A. Khelifi κ.α., 2019; D. Takahashi, 2020; Nanda κ.α., 2019)

Η ραγδαία εξέλιξη της τεχνολογίας στον τομέα του IoV έχει δημιουργήσει την ανάγκη για διαρκή και αυξημένη ασφάλεια των συστημάτων. Αυτό συμβαίνει, διότι η παραβίαση αυτών των συστημάτων θα επιφέρει επιπτώσεις τόσο στα δεδομένα των χρηστών όσο πιθανόν και στην σωματική τους ασφάλεια. Για την πρόληψη των επιθέσεων και την ενίσχυση της ασφάλειας των συστημάτων IoV χρησιμοποιούνται διάφοροι αλγόριθμοι οι περισσότεροι εκ των οποίων είναι βασισμένοι στην μηχανική μάθηση. Ως μηχανική μάθηση εννοούμε τον τομέα της επιστήμης που ασχολείται με την κατανόηση και την δημιουργία μεθόδων. Οι μέθοδοι αυτοί αξιοποιούν δεδομένα με σκοπό την βελτίωση της απόδοσης σε ένα σύνολο εργασιών. Αυτή αποτελεί τμήμα ενός ευρύτερου επιστημονικού συνόλου που ονομάζεται τεχνητή νοημοσύνη.

Οι αλγόριθμοι της μηχανικής μάθησης βασίζονται σε δείγματα δεδομένων, τα οποία ονομάζονται δεδομένα εκπαίδευσης. Μέσω αυτών των δεδομένων οι αλγόριθμοι μπορούν να κάνουν προβλέψεις και να λαμβάνουν αποφάσεις χωρίς να έχουν ρητά προγραμματιστεί για αυτό. Οι αλγόριθμοι αυτοί βρίσκουν εφαρμογή σε πολλούς επιστημονικούς τομείς πέραν της πληροφορικής. Τέτοιοι είναι η ιατρική, η γεωργία, τα οικονομικά κ.α. (J. Hu κ.α., 2020; M. Yoosefzadeh-Najafabadi κ.α., 2021)

Η παρούσα πτυχιακή εργασία αναφέρεται στην κατηγοριοποίηση των επιθέσεων αλλά και στις προκλήσεις ασφαλείας στα αυτόνομα οχήματα και στα συστήματα IoV. Για την εκπόνηση αυτής της πτυχιακής χρησιμοποιείται υλικό από επιστημονικά άρθρα και βιβλία της τελευταίας πενταετίας με σκοπό την παρουσίαση των πιο πρόσφατων δεδομένων σχετικά με την ασφάλεια στα συστήματα IoV. Η εργασία αυτή αναφέρεται ακόμη στην ασφάλεια των συστημάτων CAV αλλά και στα ad-hoc δίκτυα οχημάτων

VANET. Τέλος, γίνεται σύγκριση των λύσεων-αλγορίθμων για την προστασία από τις διάφορες επιθέσεις καθώς και προσομοιώσεις επικοινωνίας μεταξύ οχημάτων χρησιμοποιώντας τα λογισμικά OMNeT++, VEINS και SUMO.

2 Μοντέλο δικτύου του Διαδικτύου των Οχημάτων

Τα δίκτυα οχημάτων IoV αποτελούνται από διάφορα συστήματα επικοινωνίας μεταξύ των οχημάτων μαζί με διάφορους αισθητήρες για την συλλογή των δεδομένων. Αυτά τροφοδοτούνται από την τοπική μονάδα υπολογισμού και αναλύονται. Τα δίκτυα οχημάτων όπως όλα τα δίκτυα ακολουθούν μια δομή. Για να αντιμετωπιστούν διάφορα προβλήματα όπως η διαλειτουργικότητα, η επεκτασιμότητα, η αξιοπιστία πρέπει τα δίκτυα να έχουν μια ανοικτή και ευέλικτη δομή βασισμένη σε επίπεδα.

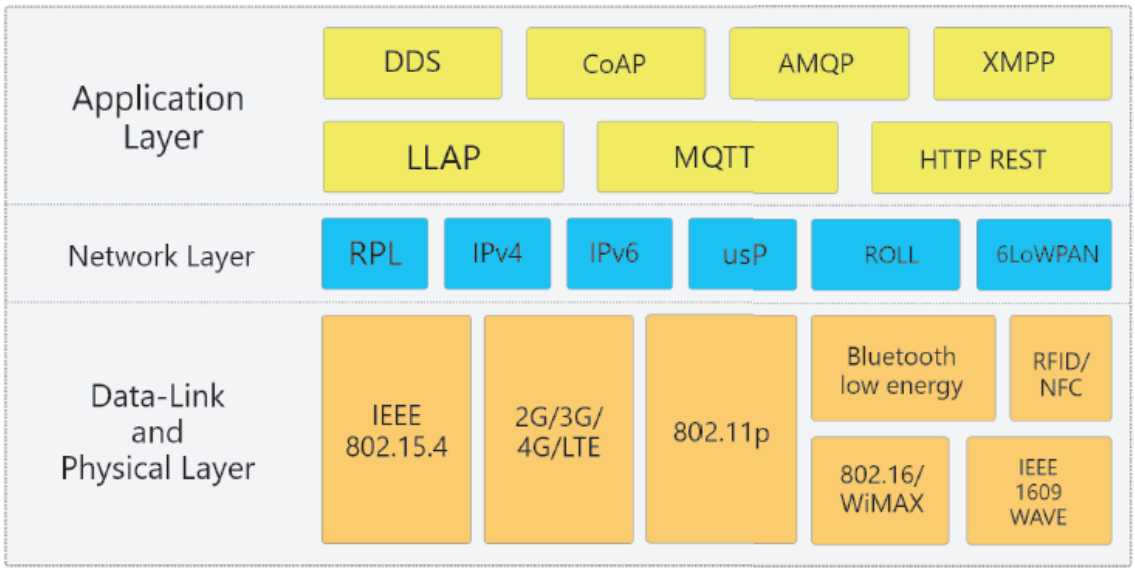
2.1 Ταξινόμηση επιπέδων

Η πιο διαδεδομένη αρχιτεκτονική δικτύου για τα συστήματα IoV αποτελείται από τρία επίπεδα:

1. *Επίπεδο ανίχνευσης (Sensing Layer)*: Το επίπεδο ανίχνευσης είναι ο συνδυασμός του φυσικού επιπέδου (physical layer) και του επιπέδου σύνδεσης δεδομένων (data-link layer). Αυτό αποτελεί το κατώτερο επίπεδο αυτής της αρχιτεκτονικής. Το επίπεδο αυτό αποτελείται από τεχνολογίες ανίχνευσης όπως τα RFID tags, τα ασύρματα δίκτυα αισθητήρων (WSN) και το NFC. Το επίπεδο αυτό είναι υπεύθυνο για την συλλογή πληροφοριών από το περιβάλλον μέσω των διαθέσιμων αισθητήρων. Τα δεδομένα που συλλέγει αφορούν τα μοτίβα οδήγησης, τις περιβαλλοντικές συνθήκες και την κατάσταση των οχημάτων. Οι κυριότερες λειτουργίες που εκτελούνται από αυτό το στρώμα είναι:
    - Αναγνώριση των φυσικών αντικειμένων που περιβάλλουν το σύστημα IoV και συλλογή δεδομένων για τα αντικείμενα αυτά.
    - Μετατροπή των δεδομένων ανίχνευσης σε ψηφιακά σήματα.
    - Αποστολή των δεδομένων που έχουν συλλεχθεί στα ανώτερα στρώματα για την μετάδοση και επεξεργασία του δικτύου.
2. *Επίπεδο δικτύου (Network Layer):* Το επίπεδο δικτύου είναι υπεύθυνο για την επεξεργασία των δεδομένων που λαμβάνονται στο προηγούμενο επίπεδο και την

μετάδοση τους στο ανώτερο επίπεδο. Για την επεξεργασία των πολλών δεδομένων που έχουν συλλεχθεί χρησιμοποιούνται τεχνικές δικτύου όπως ασύρματα και ενσύρματα δίκτυα, δίκτυα LAN. Για την μετάδοση των δεδομένων χρησιμοποιούνται πρωτόκολλα όπως το Wi-Fi, το Bluetooth ή το Zigbee. Ακόμη το επίπεδο αυτό είναι υπεύθυνο για παροχή της σύνδεσης καθώς χειρίζεται την επικοινωνία μεταξύ των οχημάτων: με άλλα οχήματα (V2V), με τις υποδομές (V2I), με τους πεζούς (V2P) και με τους άλλους αισθητήρες (V2S). Για την επικοινωνία χρησιμοποιείται το Bluetooth, το GSM, το LTE ή και το Wi-Fi με σκοπό την απρόσκοπτη συνδεσιμότητα. Επιπλέον το επίπεδο αυτό εκχωρεί διευθύνσεις IPV6 στα φυσικά αντικείμενα για την ασφαλή μετάδοση των δεδομένων.

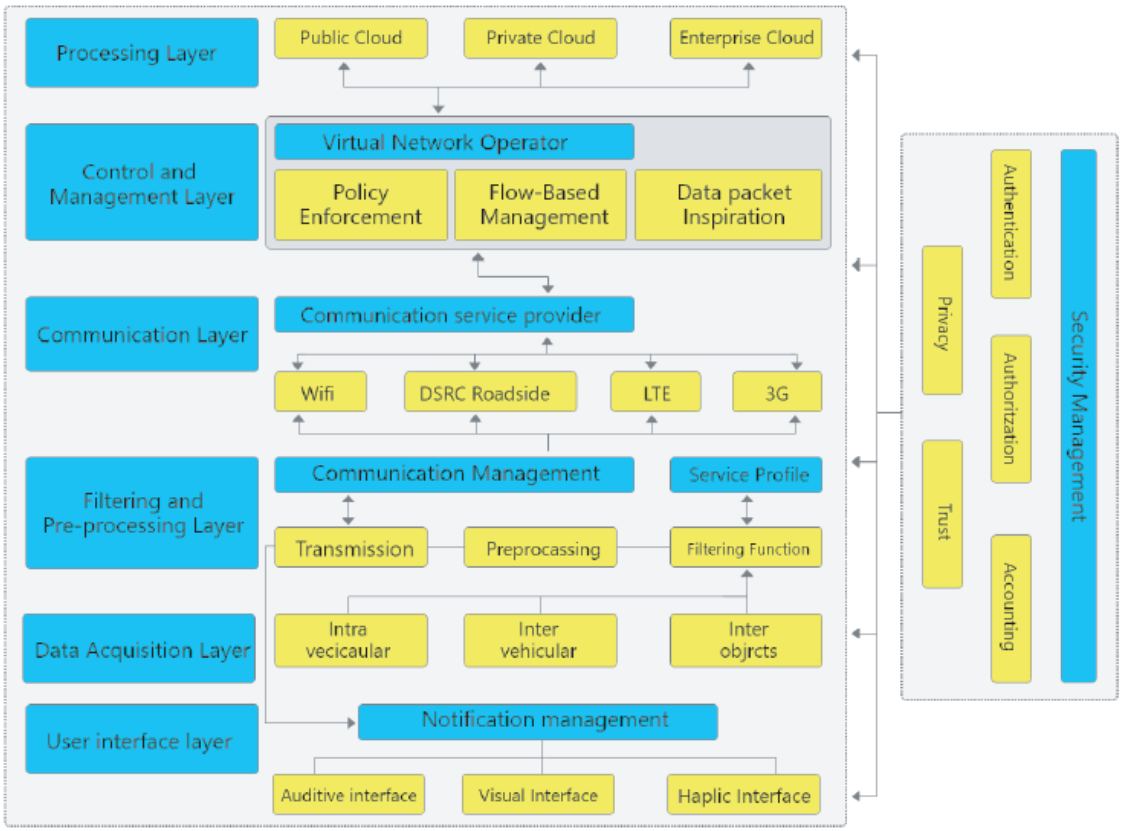
3. *Επίπεδο εφαρμογής (Application Layer):* Το επίπεδο εφαρμογής είναι υπεύθυνο για την διαχείριση, την αποθήκευση, την επεξεργασία των δεδομένων και την λήψη αποφάσεων. Αυτό παρέχει υποστήριξη για big data, WSN και cloud. Το επίπεδο αυτό μπορεί να διαιρεθεί σε application layer και business layer το οποίο λειτουργεί ως front-end για ολόκληρο το IoV. Σκοπός του business layer είναι να διευκολύνει την διαχείριση των διαφορετικών εφαρμογών. Αυτό διαχειρίζεται τα τελικά δεδομένα και ασχολείται με την ασφάλεια τους.



Εικόνα 1: Ταξινόμηση βασισμένη σε επίπεδα [16]

Η ταξινόμηση των τριών επιπέδων παρουσιάζεται στην Εικόνα 1. Η αρχιτεκτονική αυτή μπορεί να αναλυθεί περαιτέρω και να προκύψει η διευρυμένη πολυεπίπεδη δομή του IoV. Αυτή αποτελείται από την περαιτέρω ταξινόμηση καθενός εκ των τριών επιπέδων σε δύο επιπλέον επίπεδα, ενώ ταυτόχρονα κάθε επίπεδο αναλύεται στα συστατικά

του. Όλα αυτά διαχειρίζονται από ένα επίπεδο ασφαλείας. Η δομή αυτή αναπαρίσταται από την Εικόνα 2.



Εικόνα 2: Διευρυμένη δομή επιπέδου δικτύου [16]

Σε συμπλήρωση της αρχιτεκτονικής των τριών επιπέδων η CISCO όρισε ένα τέταρτο επίπεδο vehicle-to-business (V2B). Το V2B αποτελείται από δύο στοιχεία: την πλατφόρμα ενσωμάτωσης οχημάτων (VIP) για ανταλλαγή πληροφοριών και τον διαχειριστή ολοκλήρωσης back-end (BIM) με σκοπό την σύνδεση διαφόρων εξαρτημάτων στο όχημα. (Nanda κ.α., 2019)

2.2 Δομικά στοιχεία δικτύου

Το μοντέλο δικτύου του IoV αποτελείται από τρία δομικά στοιχεία. Αυτά είναι: οι χρήστες, η επικοινωνία και το cloud.

1. *Χρήστης:* Χρήστης στο σύστημα IoV είναι ο πελάτης που χρησιμοποιεί υπηρεσίες που παρέχονται από αυτό. Χρήστης θεωρείται ο οδηγός του οχήματος που λαμβάνει οδηγίες κυκλοφορίας από το σύστημα, οι επιβάτες που είναι συνδεδεμένοι στο σύστημα IoV μέσω έξυπνων κινητών, laptop κ.α. Χρήστης θεωρείται και ο

πεζός ο οποίος χρησιμοποιεί τις υπηρεσίες του IoV π.χ. για την εύρεση διαθέσιμου ταξί. Οι υπηρεσίες χρηστών χωρίζονται σε δύο κατηγορίες:

i. Υπηρεσίες ασφαλείας: Αυτές είναι ο κύριος στόχος του IoV καθώς στοχεύουν στην βελτίωση της οδικής ασφάλειας και στη μείωση των τροχαίων ατυχημάτων. Παραδείγματα τέτοιων υπηρεσιών είναι: η κλήση έκτακτης ανάγκης, η προειδοποίηση αλλαγής λωρίδας, το αυτόματο φρενάρισμα, οι πληροφορίες κυκλοφορίας σε πραγματικό χρόνο κ.α.
ii. Εμπορικές και ψυχαγωγικές υπηρεσίες: Αυτές στοχεύουν στην ευχάριστη παραμονή των επιβατών στο όχημα καθώς και στην εύρεση χρήσιμων πληροφοριών. Παράδειγμα τέτοιων υπηρεσιών είναι: η διαδικτυακή ροή μουσικής, οι προτάσεις ξενοδοχείων και βενζινάδικων, η πληρωμή διοδίων κ.α.

2. *Επικοινωνία:* Η επικοινωνία είναι ο πυρήνας του συστήματος μέσω του οποίου όλα τα συνδεδεμένα οχήματα διαμοιράζονται τα δεδομένα τους και τους παρέχονται υπηρεσίες cloud. Καθώς διαφορετικές συσκευές και οχήματα κατασκευάζονται από διαφορετικούς κατασκευαστές είναι πολύπλοκο να ενσωματωθούν όλες οι τεχνολογίες επικοινωνίας σε ένα δίκτυο. Η διασύνδεση διαφορετικών τεχνολογιών όπως το LTE και το Wi-Fi αποτελούν πρόκληση. Γι' αυτό το IoV περιλαμβάνει πέντε τύπους επικοινωνίας. Όπως:
    - Οχήματος με άλλο όχημα (V2V)
    - Οχήματος με υποδομές (V2I)
    - Οχήματος με τις οδικές μονάδες (V2R)
    - Οχήματος με τους αισθητήρες (V2S)
    - Οχήματος με προσωπικές συσκευές (V2T)

Καθένας από αυτούς τους τύπους επικοινωνίας χρησιμοποιεί διαφορετική τεχνολογία ασύρματης πρόσβασης (WAT). Οι τύποι V2V, V2I και V2R χρησιμοποιούν το IEEE WAVE, το Wi-Fi και το 4G/LTE για να επικοινωνήσουν, ενώ το V2T επικοινωνεί χρησιμοποιώντας τεχνολογίες NFC και CarPlay. Όλες αυτές οι έννοιες απεικονίζονται στην Εικόνα 3.

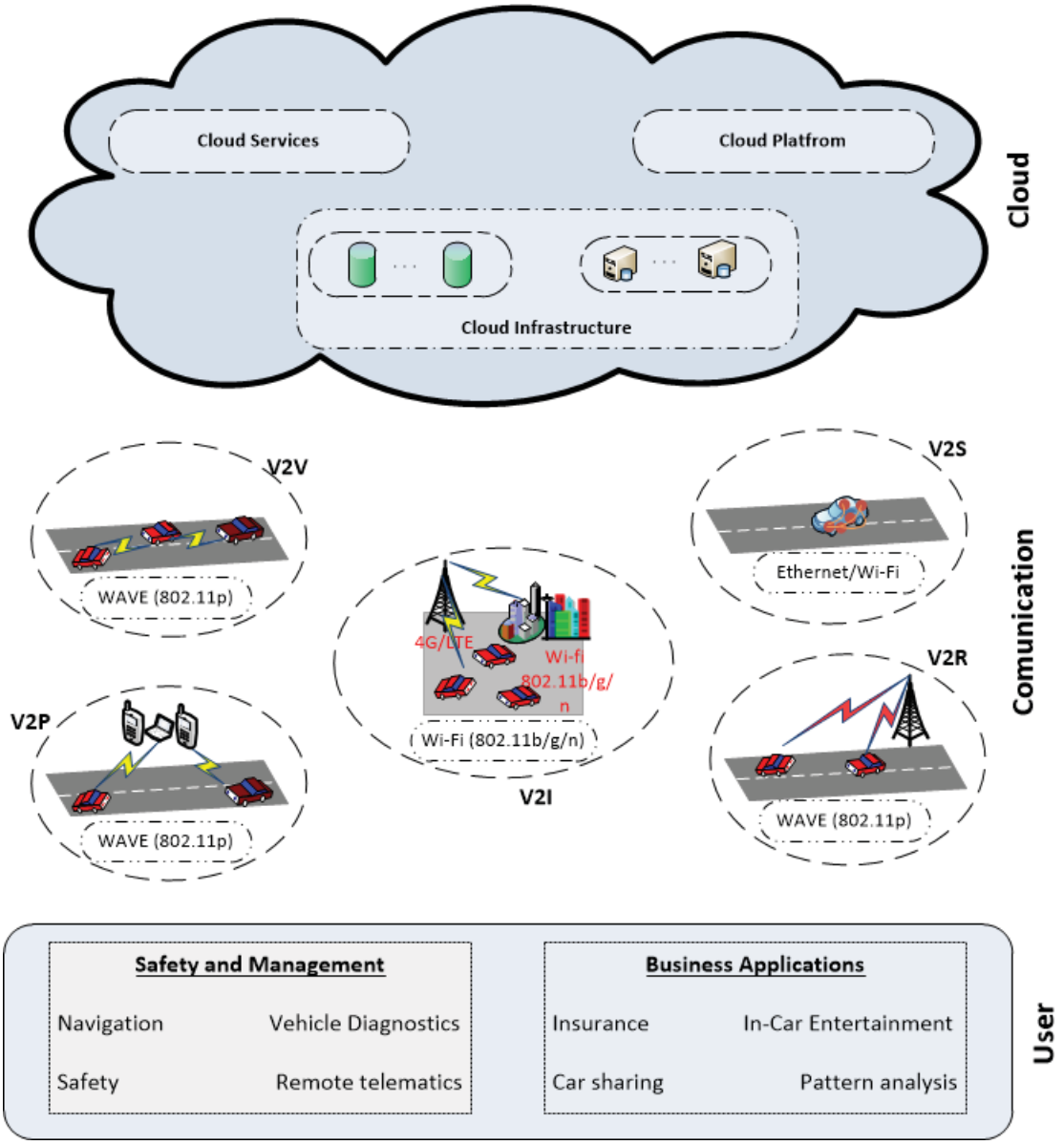
3. *Cloud:* Αυτό αποτελεί τον εγκέφαλο του συστήματος μέσα στο οποίο γίνονται όλοι οι υπολογισμοί και οι αναλύσεις. Λόγω των πολλών αισθητήρων που έχει κάθε όχημα παράγεται μεγάλος όγκος δεδομένων. Γι' αυτό είναι απαραίτητο τα

δεδομένα να αποθηκεύονται στο cloud. Το μοντέλο δικτύου cloud χωρίζεται σε τρία κύρια σημεία:

i. Υποδομή Cloud, η οποία παρέχει χώρο αποθήκευσης για τον μεγάλο όγκο δεδομένων που παράγεται από τα συστήματα IoV.

ii. Υπηρεσίες Cloud, οι οποίες αποτελούν τις βασικές υπηρεσίες που παρέχονται στο χρήστη όπως αποθήκευση, υπολογιστική, δίκτυο και δεδομένα.

iii. Cloud Storage, το οποίο περιλαμβάνει διακομιστές για την αποθήκευση, επεξεργασία και ανάλυση big data. (Sharma κ.α., 2018)



Εικόνα 3: Μοντέλο δικτύου του IoV [18]

2.3 Σενάρια προσομοίωσης επικοινωνίας αυτόνομων οχημάτων

Σε αυτή την υποενότητα παρουσιάζονται δύο προσομοιώσεις επικοινωνίας μεταξύ των αυτόνομων οχημάτων χρησιμοποιώντας τα λογισμικά VEINS, OMNeT++ και SUMO. Αναλυτικός οδηγός εγκατάστασης των λογισμικών παρατίθεται στο Παράρτημα Β. Το λογισμικό VEINS προσομοιώνει ένα οδικό δίκτυο ενώ το λογισμικό SUMO υλοποιεί το traffic simulation. Το λογισμικό OMNeT++ χρησιμεύει για το δικτυακό κομμάτι της προσομοίωσης. Στα σενάρια χρησιμοποιείται ένα flow 6 οχημάτων και θέλουμε να παρακολουθήσουμε την συμπεριφορά τους. Αυτά έχουν ένα κοινό σημείο αφετηρίας και κινούνται προς μία συγκεκριμένη κατεύθυνση, ενώ η απόσταση μεταξύ των οχημάτων παραμένει σταθερή. Η κίνηση των αυτόνομων οχημάτων με αυτά τα χαρακτηριστικά ονομάζεται platoon formation.

Στα σενάρια που ακολουθούν κατά την διάρκεια της πορείας των οχημάτων το πρώτο συνήθως όχημα εμπλέκεται σε κάποιο ατύχημα και στέλνει μήνυμα στα οχήματα που ακολουθούν δίνοντας τους την εντολή να αλλάξουν κατεύθυνση ή να σταματήσουν. Τα μηνύματα αυτά βασίζονται στην τεχνολογία Cooperative Adaptive Cruise Control (CACC). Μετά από ένα ατύχημα η διάταξη των οχημάτων επηρεάζεται, δηλαδή οι αποστάσεις μεταξύ τους καθώς και η ταχύτητα τους αλλάζουν ενώ και κάποια οχήματα ακολουθούν διαφορετική διαδρομή. (Κουκούτσης Ιωάννης, 2022)

Για να συγκεντρώσουμε όλες τις απαραίτητες πληροφορίες, λαμβάνουμε από κάθε όχημα μέσω μηνυμάτων διάφορες τιμές όπως την ταχύτητα που έχει αναπτύξει, την απόσταση που έχει διανύσει κ.α. Όλες αυτές οι πληροφορίες απεικονίζονται με την βοήθεια των γραφημάτων του OMNeT++. Έτσι, φαίνεται πως η διατήρηση ενός platoon επηρεάζεται από πολλούς παράγοντες όπως μία φυσική διαταραχή με αποτέλεσμα την αλλοίωση του platoon ή την πρόκληση σφαλμάτων. Επίσης, μέσω των σεναρίων φαίνεται πως υπάρχει συνδυασμός μεταξύ του physical κομματιού και του δικτύου, δηλαδή μία φυσική διαταραχή επηρεάζει την επικοινωνία μεταξύ των οχημάτων.

2.3.1 1ο Σενάριο

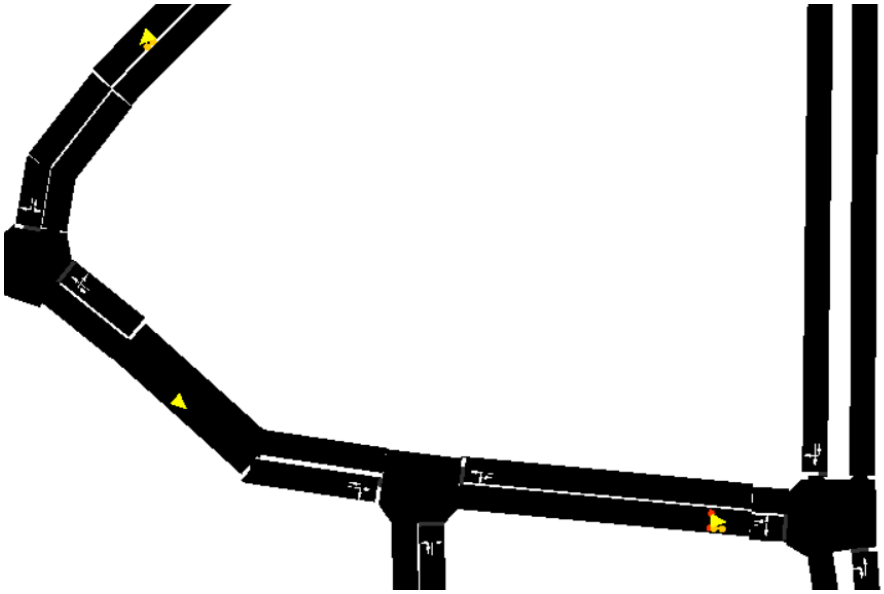
1 Row σε δρόμο διπλής κυκλοφορίας με 1 λωρίδα κυκλοφορίας ανά κατεύθυνση.

Σε αυτό το σενάριο παρουσιάζονται τα αποτελέσματα που δόθηκαν από τις προσομοιώσεις σε δύο διαφορετικές περιπτώσεις. Στην πρώτη περίπτωση του πειράματος τα οχήματα -κόμβοι- ακολουθούν μια πορεία η οποία δεν διακόπτεται από κάποιο απρόσμενο

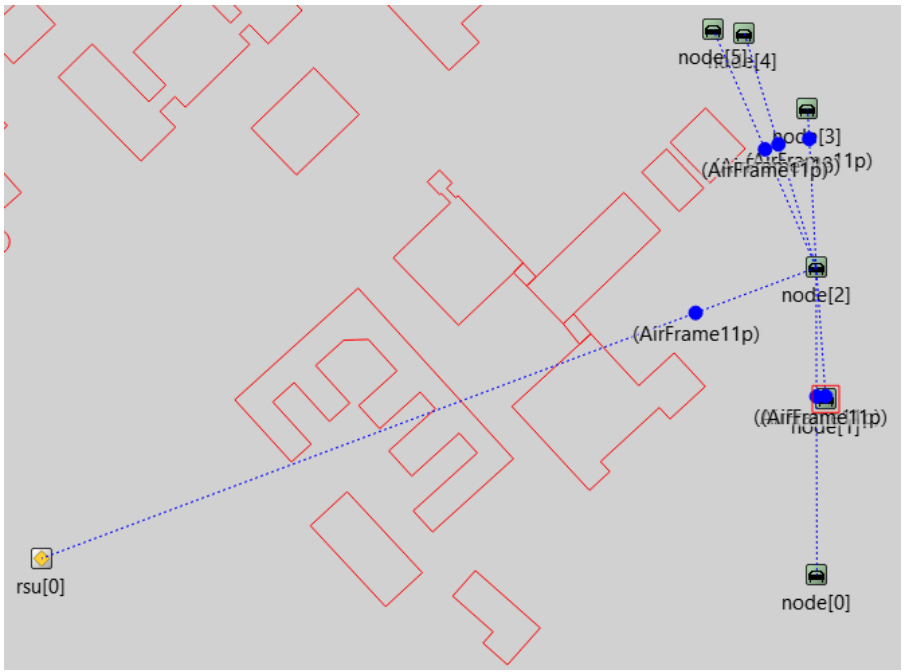
συμβάν. Τα οχήματα ξεκινούν από ένα κοινό σημείο, διαγράφοντας την ίδια πορεία, καταλήγοντας στο τερματικό σημείο. Στη δεύτερη περίπτωση υπάρχει η ιδιαιτερότητα ότι οι κόμβοι ξεκινούν από το ίδιο σημείο με τα ίδια ακριβώς χαρακτηριστικά αλλά με την διαφορά ότι υπάρχει μια φυσική διαταραχή (ατύχημα) είκοσι δευτερόλεπτα μετά την εκκίνηση σε δρόμο διπλής κυκλοφορίας με μία λωρίδα κυκλοφορίας ανά κατεύθυνση.

Α. Περίπτωση πορείας χωρίς ατύχημα:

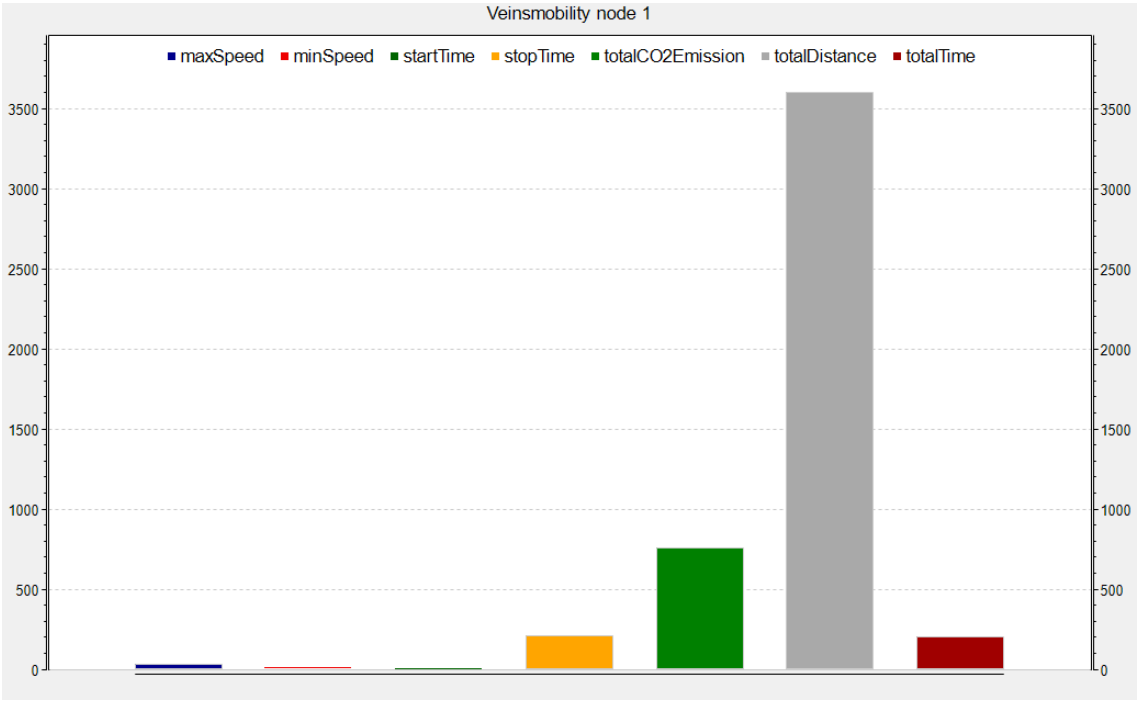
Row: 1 Vehicles: 6 Max Speed: 50 m/s Acceleration: 6.0 m/s²



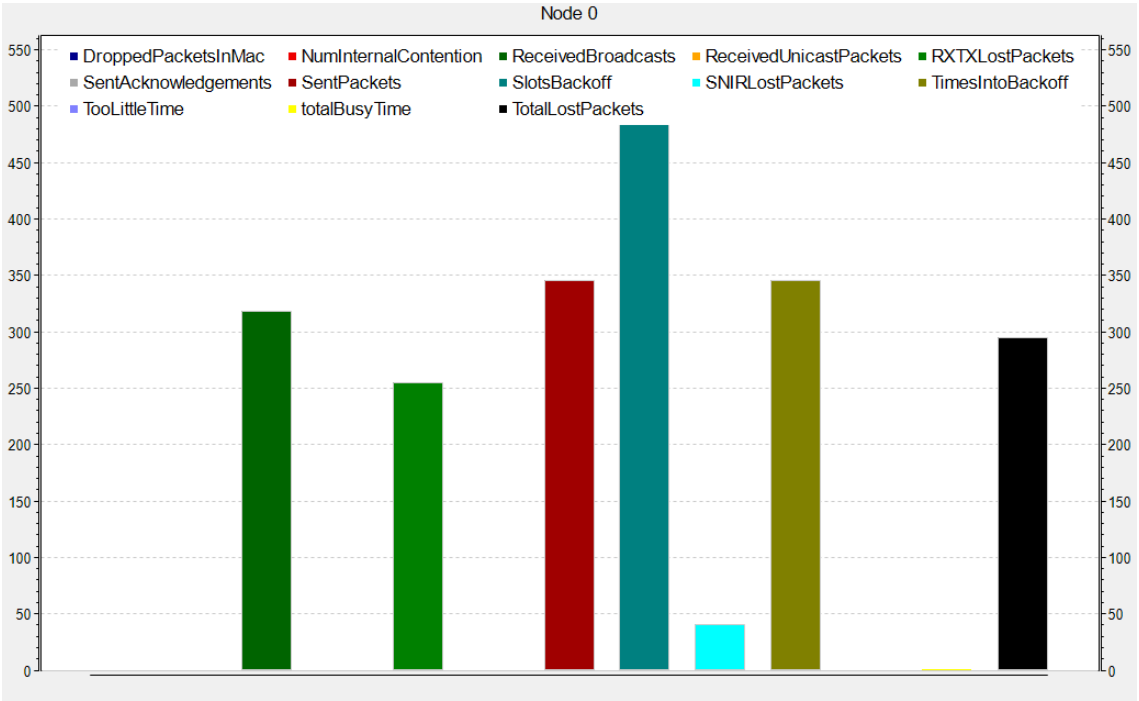
Εικόνα 4: Προσομοίωση της κίνησης των οχημάτων



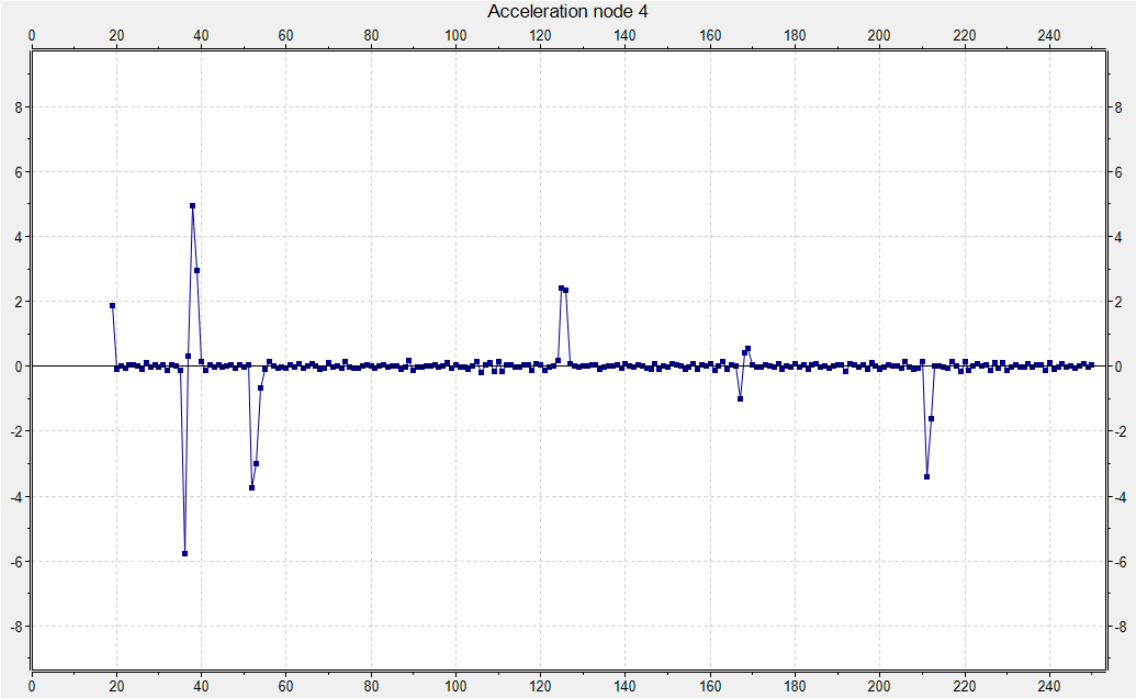
Εικόνα 5: Επικοινωνία μεταξύ οχημάτων και RSU



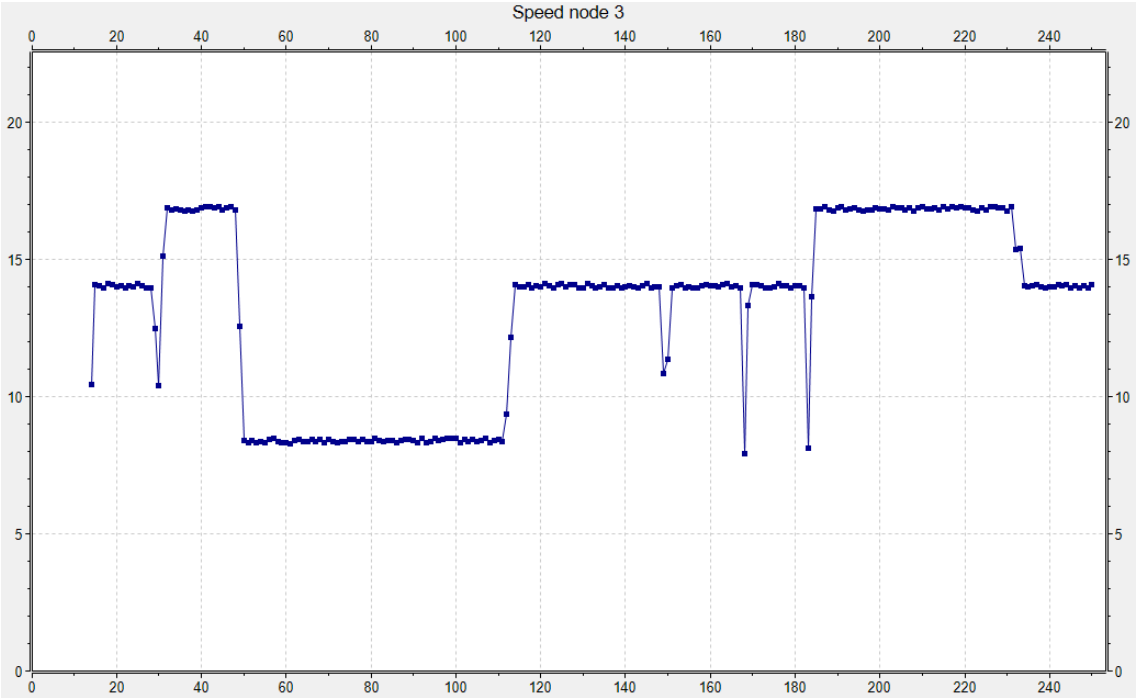
Εικόνα 6: Διάγραμμα αποτελεσμάτων για το 2ο όχημα



Εικόνα 7: Αποτελέσματα επικοινωνίας 1ου οχήματος



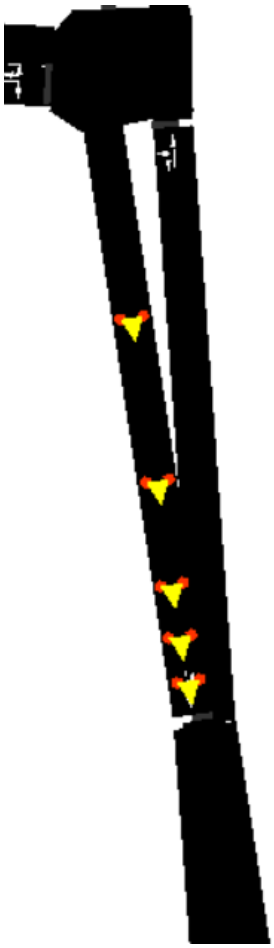
Εικόνα 8: Η μεταβολή της επιτάχυνσης του 5ου οχήματος κατά την προσομοίωση



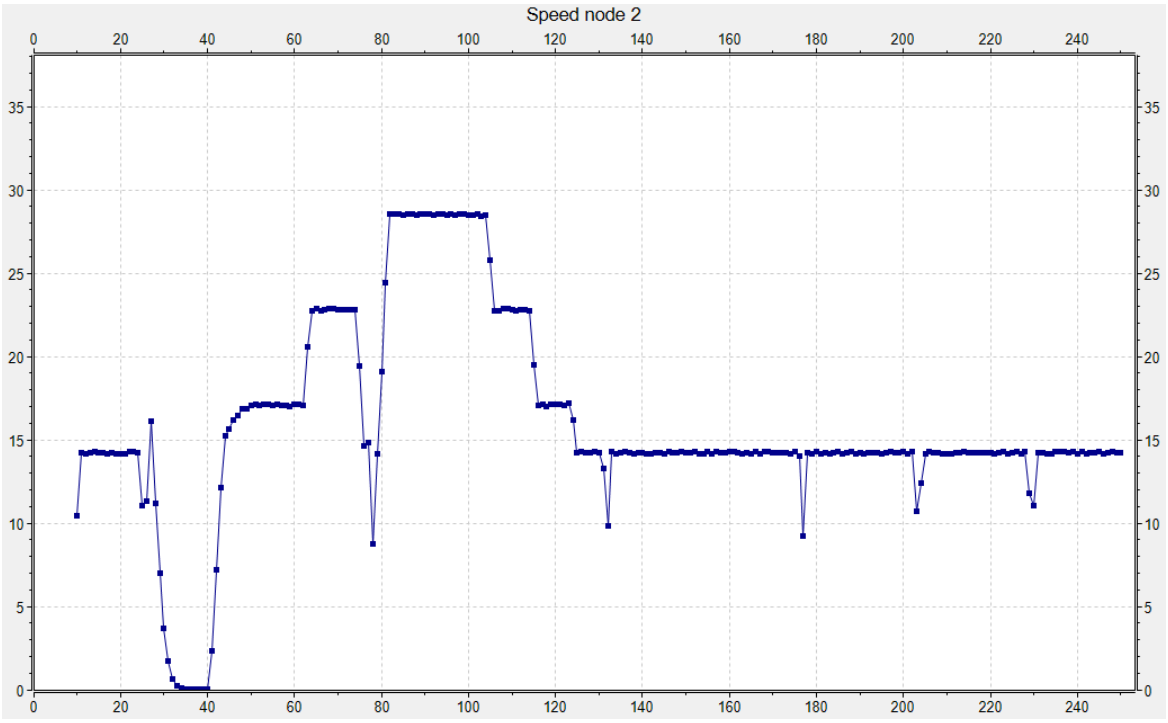
Εικόνα 9: Η μεταβολή της ταχύτητα του 4ου οχήματος κατά την προσομοίωση

B. Περίπτωση πορείας με ατύχημα:

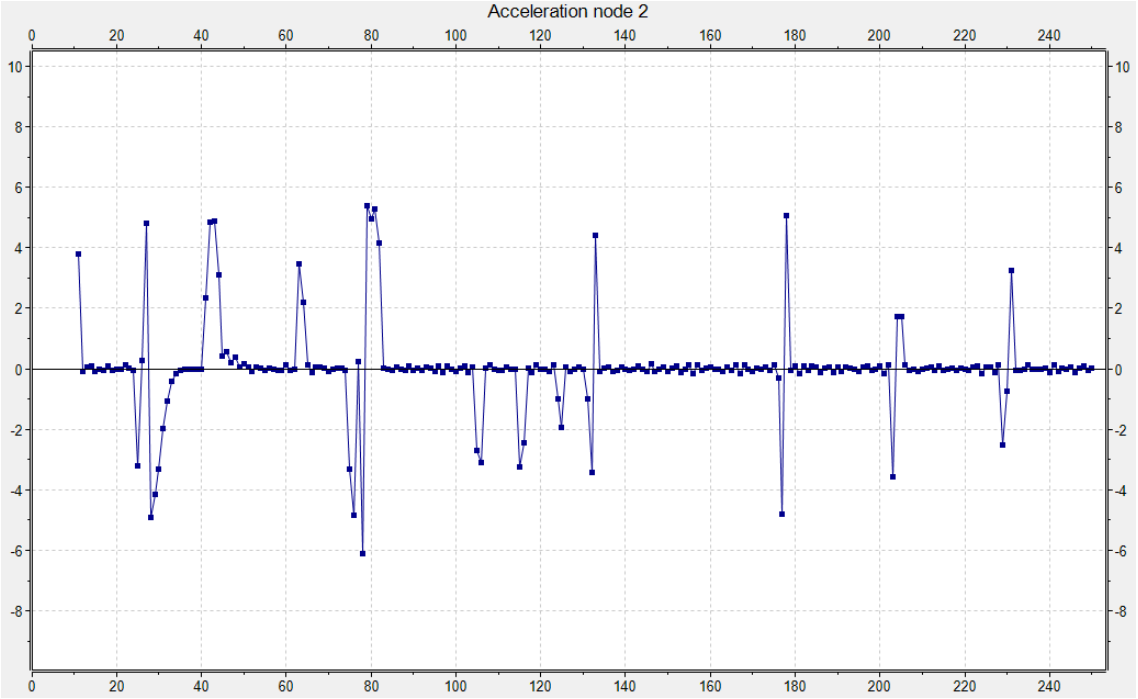
Row: 1 Vehicles: 6 Max Speed: 50 m/s Acceleration: 6.0 m/s^2
Deceleration: 7.5 m/s^2 Accident start: 20 sec Accident duration: 20 sec



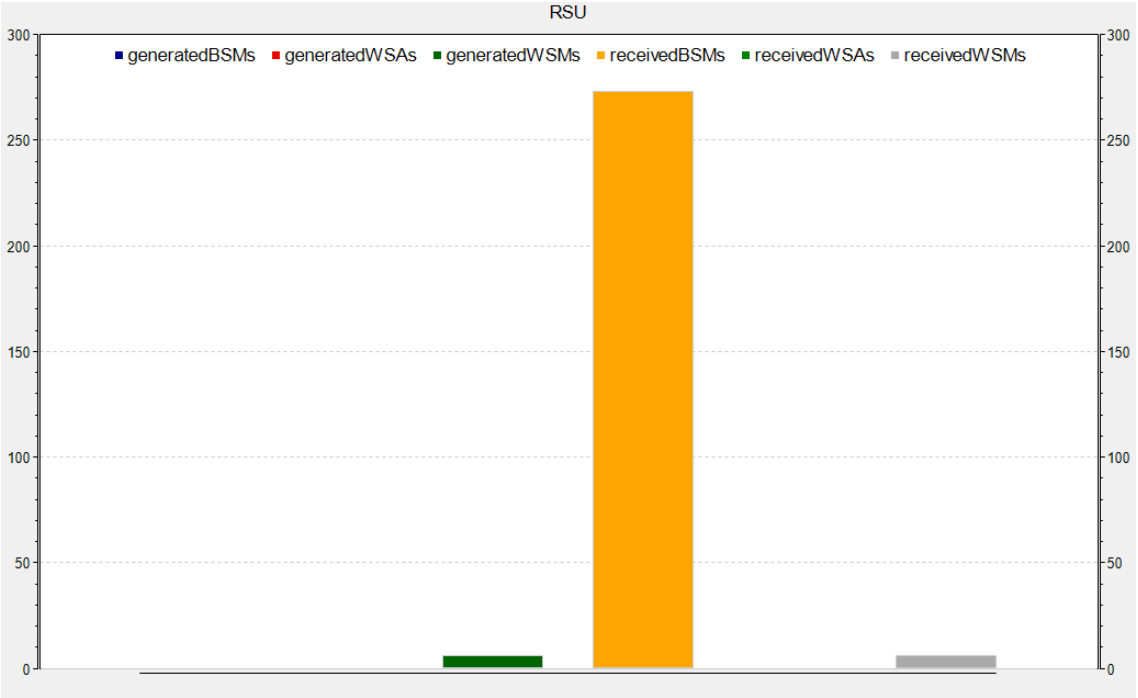
Εικόνα 10: Προσομοίωση της κίνησης των οχημάτων



Εικόνα 11: Η μεταβολή της ταχύτητας του 3^{ου} οχήματος



Εικόνα 12: Η μεταβολή της επιτάχυνσης του 3ου οχήματος



Εικόνα 13: Διάγραμμα ανταλλαγής μηνυμάτων για την RSU

Στην περίπτωση Α όπως φαίνεται και από την Εικόνα 6 το δεύτερο όχημα έχει μέγιστη ταχύτητα 29m/s και ελάχιστη ταχύτητα 8m/s. Το όχημα άρχισε να κινείται το 5ο δευτερόλεπτο και σταμάτησε το 204ο δευτερόλεπτο. Η συνολική τιμή καυσαερίων (CO_2) που εξέπεμψε είναι 754 ενώ η συνολική απόσταση που διένυσε είναι 3600m. Σύμφωνα

με την Εικόνα 7 το πρώτο όχημα έχει στείλει 345 πακέτα, έχει χάσει λόγω θορύβου και παρεμβολών 40 πακέτα ενώ ο συνολικός αριθμός των πακέτων που χάθηκαν είναι 295. Στην περίπτωση Β επειδή συμβαίνει ένα ατύχημα υπάρχει ξαφνική αλλαγή στην επιτάχυνση και στη ταχύτητα των οχημάτων. Αυτό φαίνεται στην Εικόνα 11 και στην Εικόνα 12 σε σύγκριση με την Εικόνα 8 και την Εικόνα 9. Τέλος σύμφωνα με την Εικόνα 13 η RSU δημιούργησε 6 WSM (Wave Short Messages) μηνύματα ενώ έλαβε 273 BSM (Basic Safety Messages) μηνύματα και 6 WSM μηνύματα.

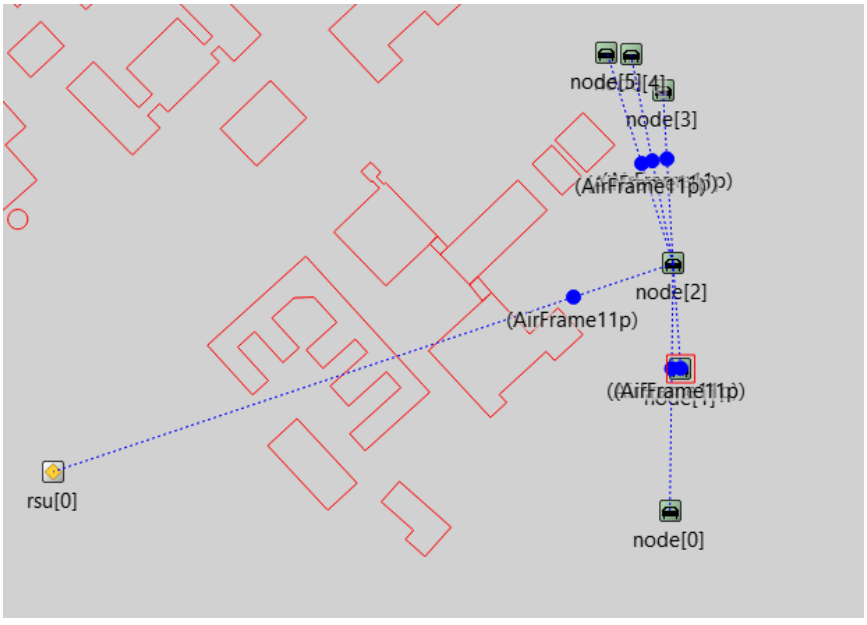
2.3.2 2ο Σενάριο

1 Row σε δρόμο διπλής κυκλοφορίας με 2 λωρίδες κυκλοφορίας ανά κατεύθυνση.

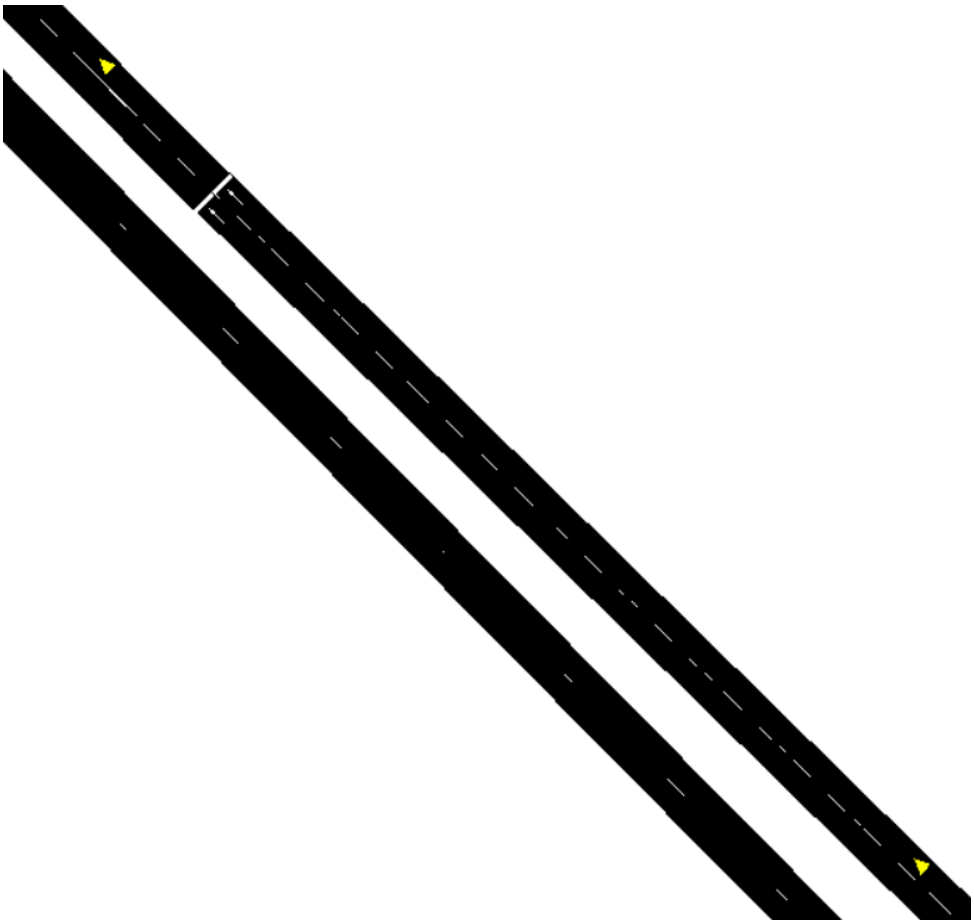
Σε αυτό το σενάριο παρουσιάζονται τα αποτελέσματα που δόθηκαν από τις προσομοιώσεις σε δύο διαφορετικές περιπτώσεις. Στην πρώτη περίπτωση του πειράματος τα οχήματα -κόμβοι- ακολουθούν μια πορεία η οποία δεν διακόπτεται από κάποιο απρόσμενο συμβάν. Τα οχήματα ξεκινούν από ένα κοινό σημείο, διαγράφοντας την ίδια πορεία, καταλήγοντας στο τερματικό σημείο. Στη δεύτερη περίπτωση υπάρχει η ιδιαιτερότητα ότι οι κόμβοι ξεκινούν από το ίδιο σημείο με τα ίδια ακριβώς χαρακτηριστικά αλλά με την διαφορά ότι υπάρχει μια φυσική διαταραχή (ατύχημα) ογδόντα τρία δευτερόλεπτα μετά την εκκίνηση σε δρόμο διπλής κυκλοφορίας με δύο λωρίδες κυκλοφορίας ανά κατεύθυνση.

Α. Περίπτωση πορείας χωρίς ατύχημα:

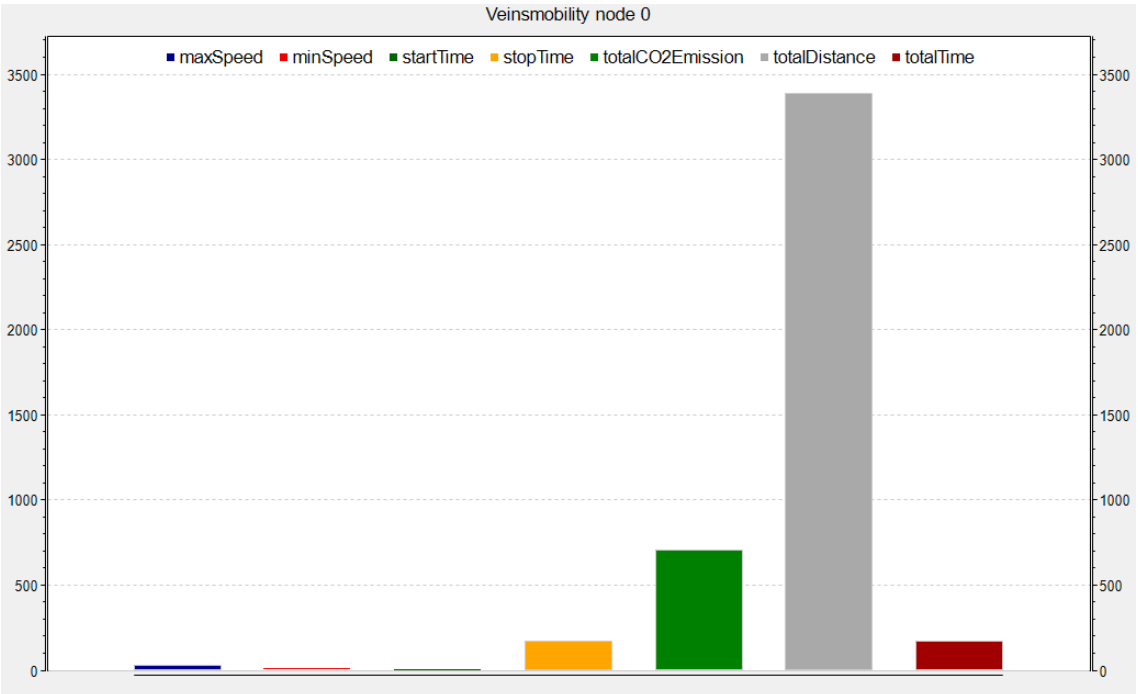
Row: 1 Vehicles: 6 Max Speed: 50 m/s Acceleration: 6.0 m/s²



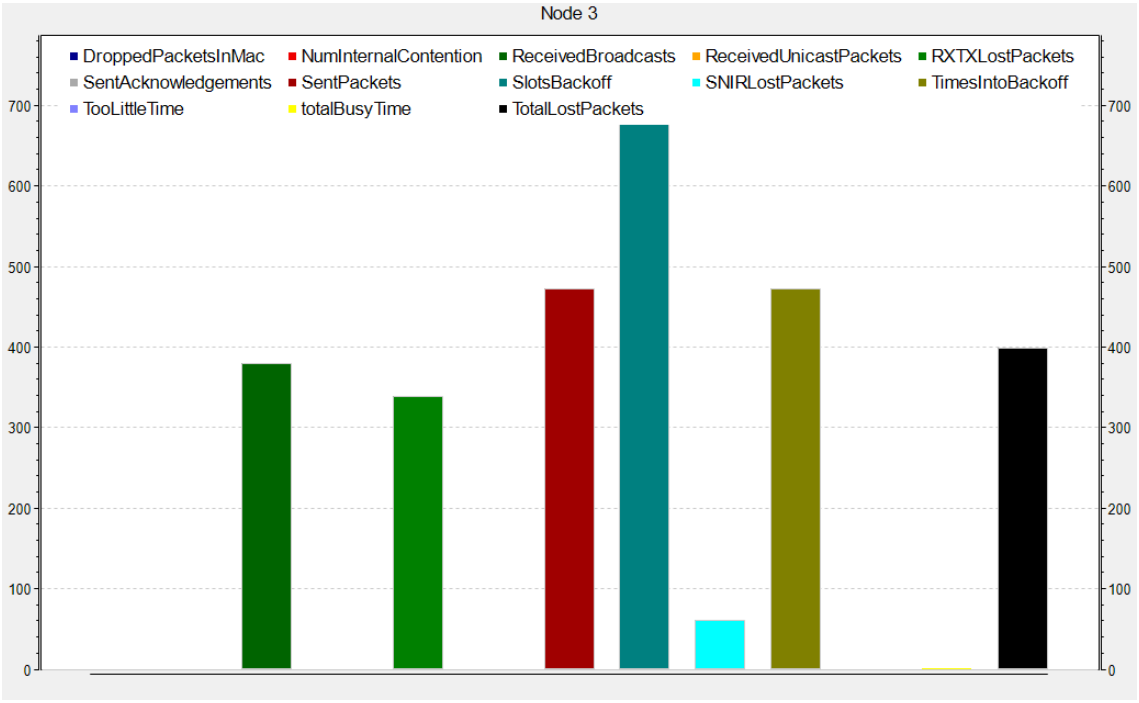
Εικόνα 14: Επικοινωνία μεταξύ οχημάτων και RSU



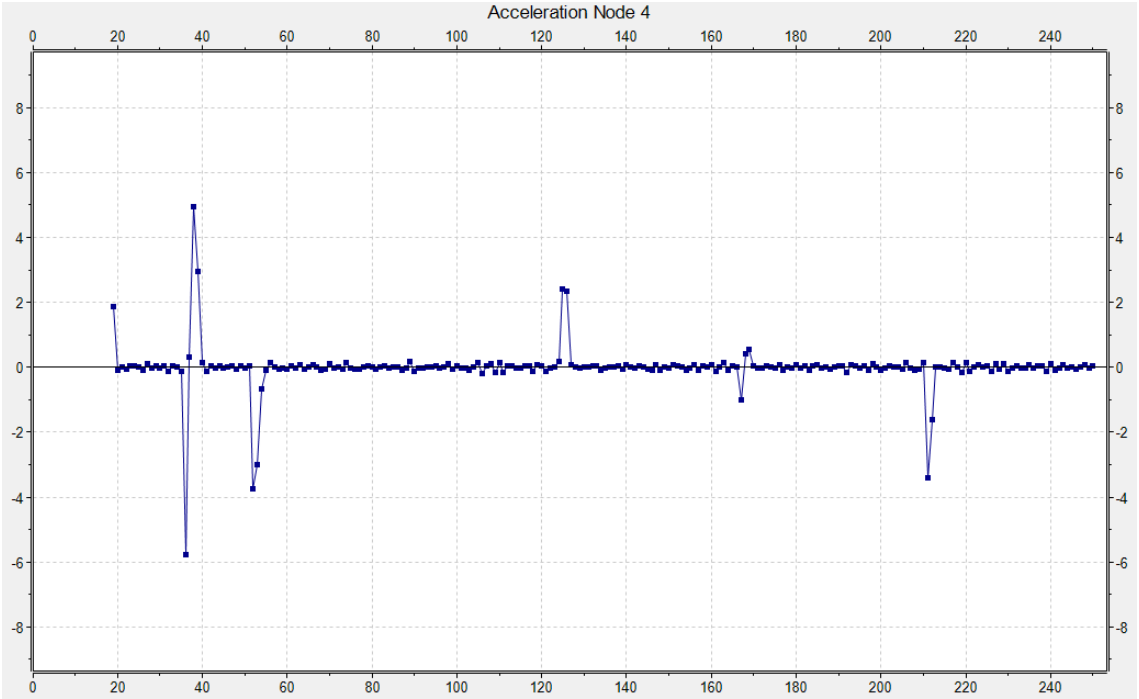
Εικόνα 15: Προσομοίωση της κίνησης των οχημάτων



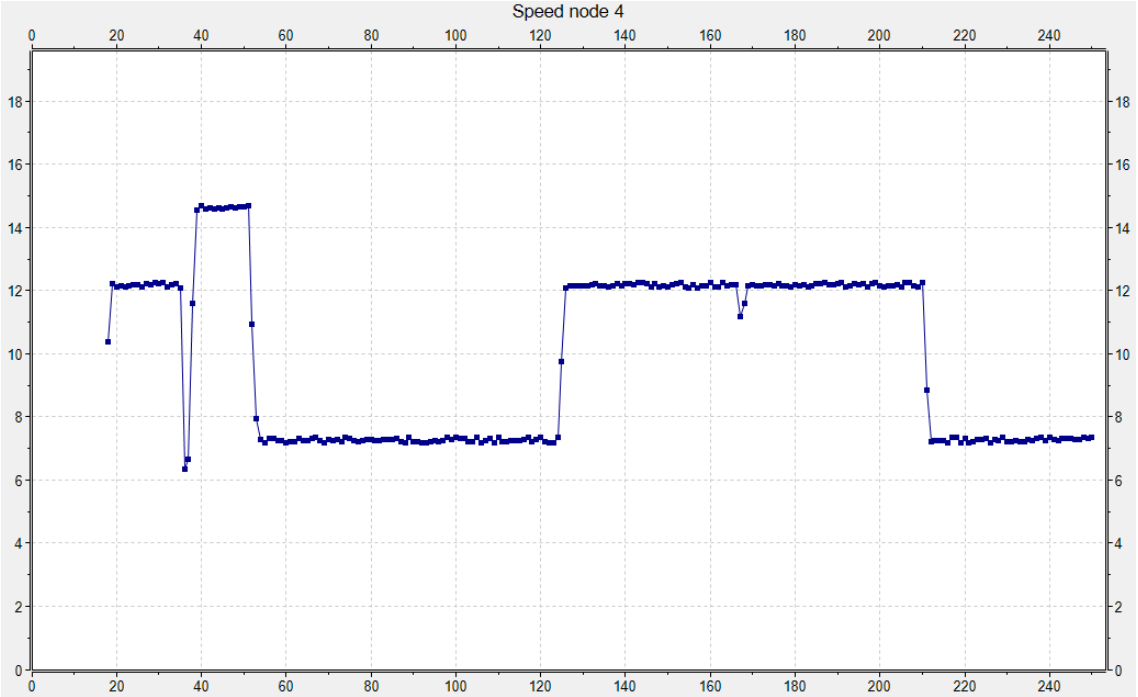
Εικόνα 16: Διάγραμμα αποτελεσμάτων για το 1ο όχημα



Εικόνα 17: Αποτελέσματα επικοινωνίας 4ου οχήματος



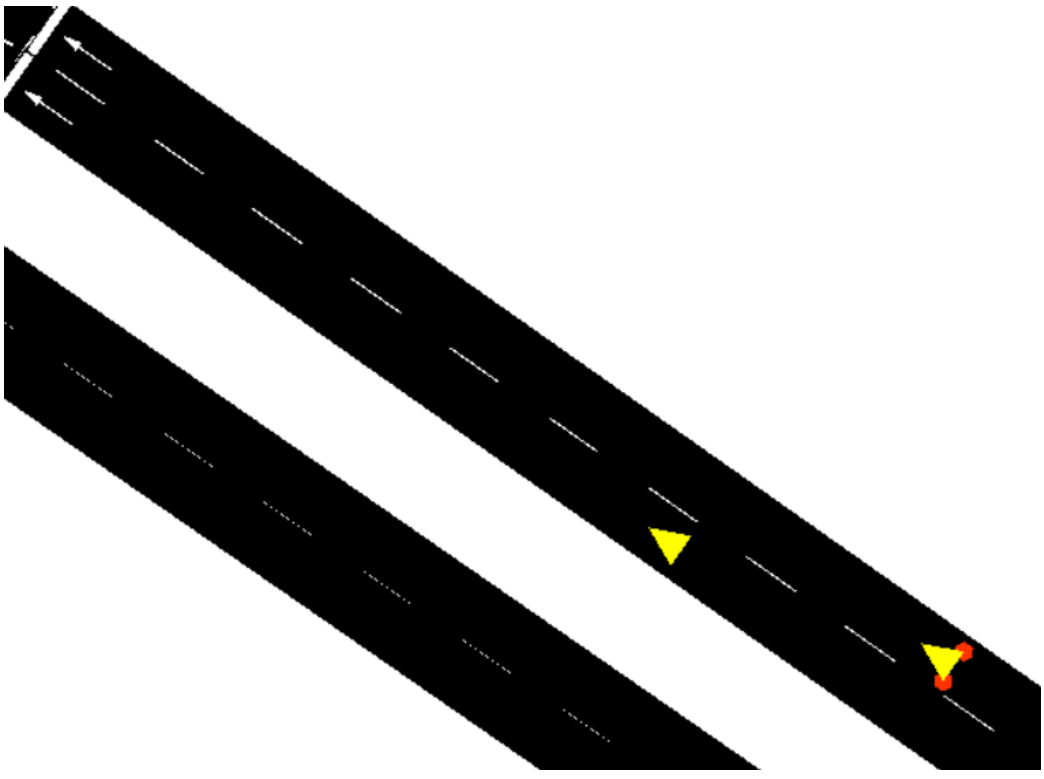
Εικόνα 18: Η μεταβολή της επιτάχυνσης του 5ου οχήματος κατά την προσομοίωση



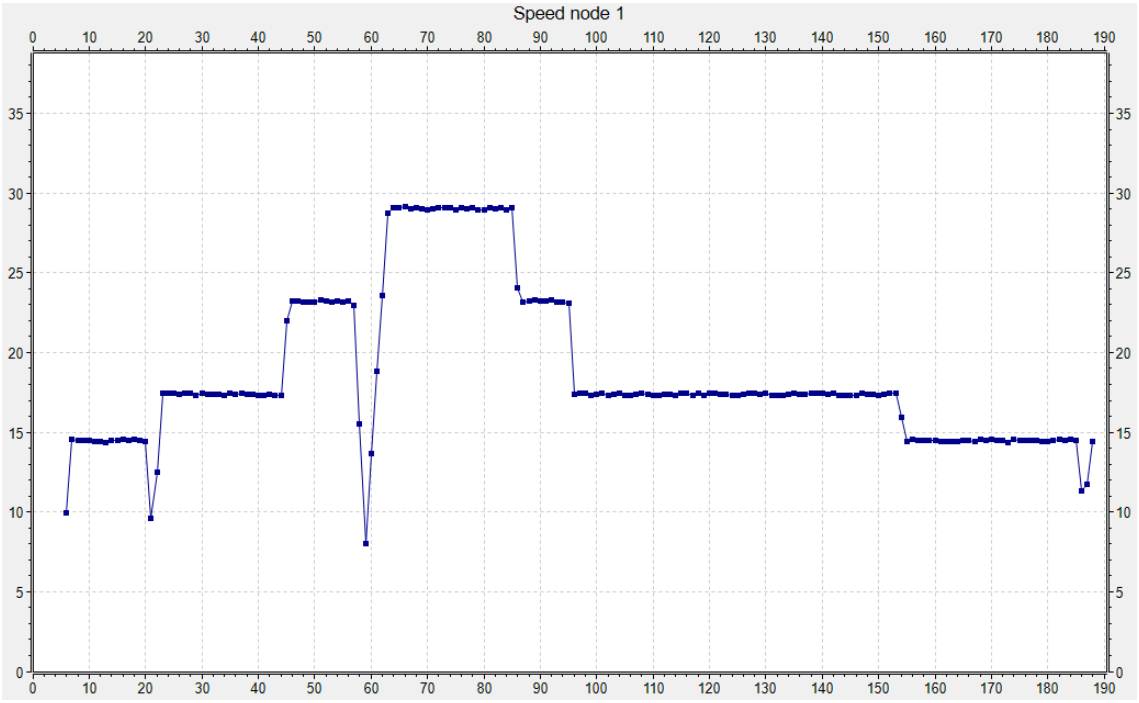
Εικόνα 19: Η μεταβολή της ταχύτητα του 5ου οχήματος κατά την προσομοίωση

B. Περίπτωση πορείας με ατύχημα:

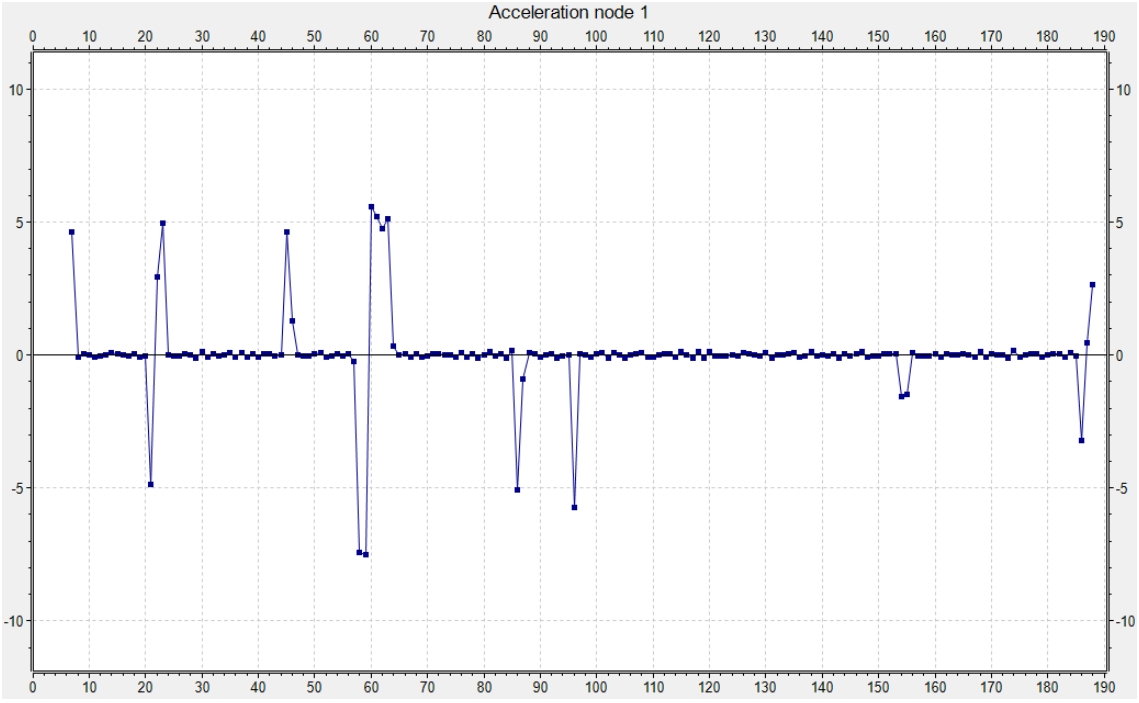
Row: 1 Vehicles: 6 Max Speed: 50 m/s Acceleration: 6.0 m/s^2
Accident start: 83 sec Accident duration: 20 sec



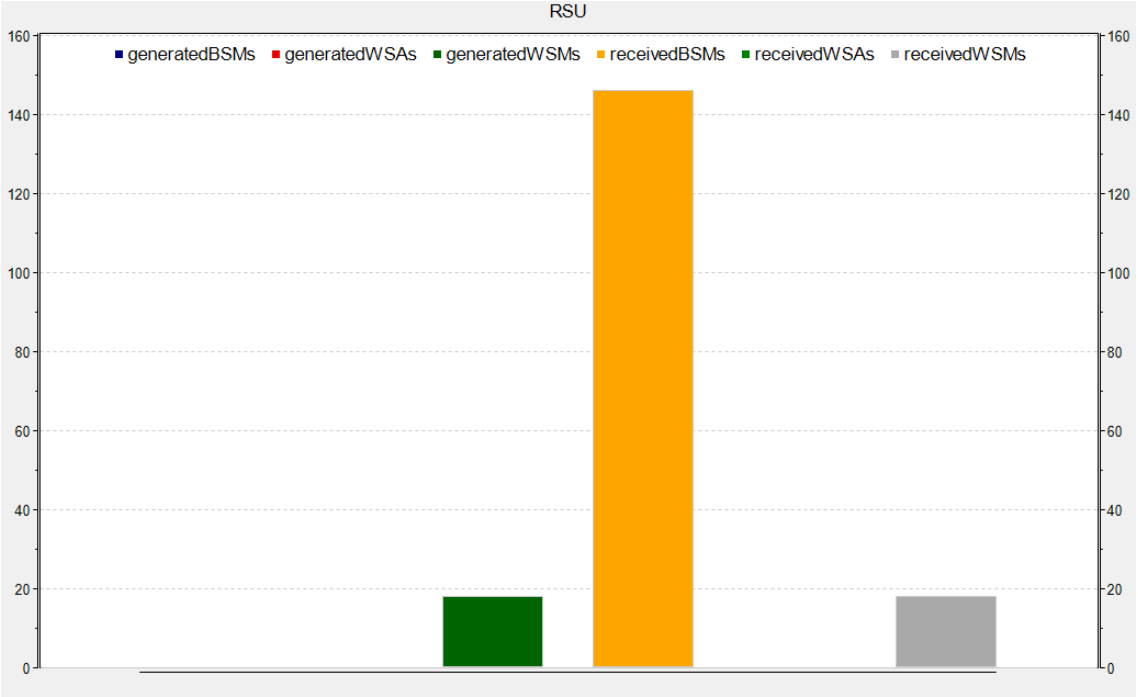
Εικόνα 20: Προσομοίωση της κίνησης των οχημάτων



Εικόνα 21: Η μεταβολή της ταχύτητας του 2ου οχήματος



Εικόνα 22: Η μεταβολή της επιτάχυνσης του 2ου οχήματος



Εικόνα 23: Διάγραμμα ανταλλαγής μηνυμάτων για την RSU

Στην περίπτωση Α όπως φαίνεται και από την Εικόνα 16 το πρώτο όχημα έχει μέγιστη ταχύτητα 31m/s και ελάχιστη ταχύτητα 8m/s. Το όχημα άρχισε να κινείται το 1ο δευτερόλεπτο και σταμάτησε το 174ο δευτερόλεπτο. Η συνολική τιμή καυσαερίων (CO2) που εξέπεμψε είναι 703 ενώ η συνολική απόσταση που διένυσε είναι 3387m. Σύμφωνα με την Εικόνα 17 το πρώτο όχημα έχει στείλει 472 πακέτα, έχει χάσει λόγω θορύβου και παρεμβολών 60 πακέτα ενώ ο συνολικός αριθμός των πακέτων που χάθηκαν είναι 398. Στην περίπτωση Β επειδή συμβαίνει ένα ατύχημα υπάρχει ξαφνική αλλαγή στην επιτάχυνση και στη ταχύτητα των οχημάτων. Αυτό φαίνεται στην Εικόνα 21 και στην Εικόνα 22 σε σύγκριση με την Εικόνα 18 και την Εικόνα 19. Τέλος σύμφωνα με την Εικόνα 23 η RSU δημιούργησε 18 WSM (Wave Short Messages) μηνύματα ενώ έλαβε 146 BSM (Basic Safety Messages) μηνύματα και 18 WSM μηνύματα.

Συνοψίζοντας μέσω των παραπάνω σεναρίων φαίνεται η επικοινωνία των αυτόνομων οχημάτων με την RSU και οι ενέργειες τους όταν συμβεί κάποιο ατύχημα. Σύμφωνα με τα σενάρια στην Α περίπτωση τα οχήματα κινούνται στην πορεία τους χωρίς να αντιμετωπίζουν κάποιο πρόβλημα. Στην Β περίπτωση που το πρώτο όχημα έχει ένα ατύχημα, μέσω των μηνυμάτων που ανταλλάσσονται μεταξύ των οχημάτων και της RSU, στο 1^{ο} σενάριο τα υπόλοιπα οχήματα μειώνουν την ταχύτητα τους και σταματούν, διότι κινούνται σε δρόμο με μία λωρίδα κυκλοφορίας ανά κατεύθυνση ενώ στο 2^{ο} σενάριο τα οχήματα μειώνουν την ταχύτητα τους και προσπερνούν το σταματημένο όχημα συνεχίζοντας

την πορεία τους, διότι βρίσκονται σε δρόμο με δύο λωρίδες κυκλοφορίας ανά κατεύθυνση. Όλα αυτά περιγράφονται στα παραπάνω διαγράμματα μεταβολής της ταχύτητας και της επιτάχυνσης των οχημάτων καθώς και από τα διαγράμματα ανταλλαγής μηνυμάτων.

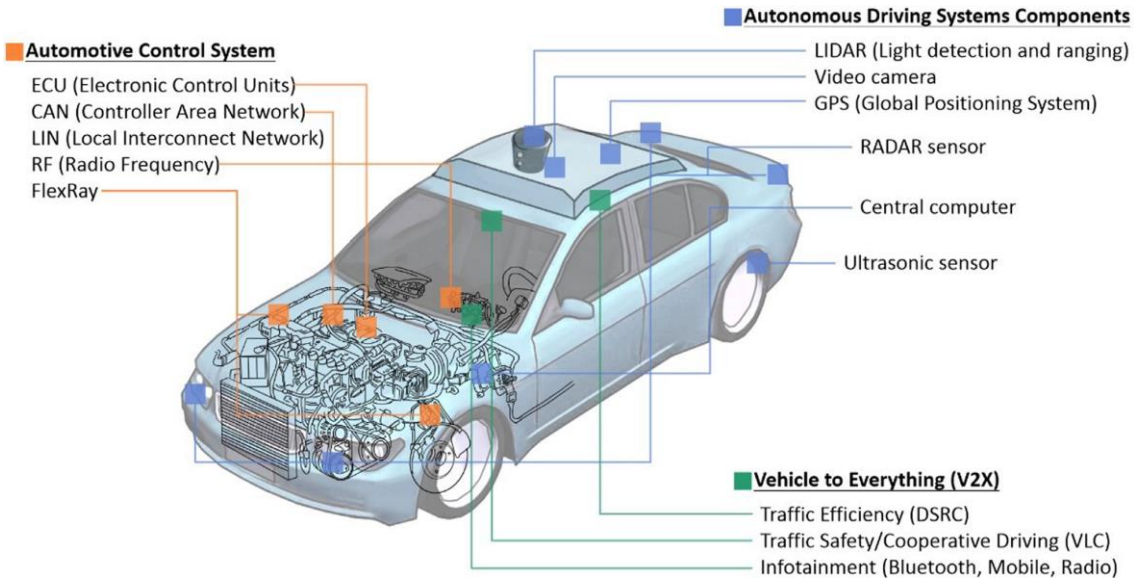
2.4 Βασικά στοιχεία αυτόνομων οχημάτων

Τα αυτόνομα οχήματα είναι εφοδιασμένα με πολλά και πολύπλοκα συστήματα όπως αισθητήρες, κάμερες κ.α. Η κατηγοριοποίηση όλων αυτών των εξαρτημάτων γίνεται σε τρείς κατηγορίες:

1. *Σύστημα ελέγχου αυτοκινήτου:* Το σύστημα ελέγχου αποτελείται από ένα εσωτερικό δίκτυο του οχήματος που συνδέει την κύρια συσκευή με άλλες συσκευές. Το σύστημα αυτό χωρίζεται σε μονάδες και δίκτυα. Οι πιο σημαντικές μονάδες είναι οι ηλεκτρονικές μονάδες ελέγχου (ECU). Ο ρόλος της ECU είναι ο έλεγχος του αυτόματου κιβωτίου ταχυτήτων και η διαχείριση των αισθητήρων του οχήματος. Ορισμένοι τύποι ECU είναι οι μονάδες ελέγχου αμαξώματος και οι μονάδες ελέγχου του συστήματος μετάδοσης κίνησης. Οι μονάδες ελέγχου αμαξώματος περιλαμβάνουν μονάδες για τις πόρτες, τα καθίσματα, το ηλεκτρικό κλείδωμα κ.α., ενώ οι μονάδες ελέγχου του συστήματος μετάδοσης κίνησης περιλαμβάνουν το σύστημα φρένων ABS, μονάδα ελέγχου κινητήρα και κιβωτίου ταχυτήτων. Συνήθως ένα μεσαίο αυτοκίνητο εξοπλίζεται με περίπου 50 ECUs, ενώ ένα πολυτελές αυτοκίνητο με τουλάχιστον 70 ECUs.

   Το εσωτερικό δίκτυο του οχήματος διασυνδέει τις ECUs και μεταφέρει τα δεδομένα μεταξύ αυτών. Το δίκτυο αυτό περιλαμβάνει το δίκτυο περιοχής ελεγκτή (CAN), το τοπικό δίκτυο διασύνδεσης (LIN), το FlexRay, το δίκτυο Ethernet κ.α. Το πρωτόκολλο CAN είναι ένα πρότυπο ISO για την επικοινωνία των δεδομένων. Το LIN είναι ένα single-master network που χρησιμοποιείται συνήθως για το κλείδωμα των θυρών του αυτοκινήτου, τον έλεγχο των καθρεπτών, τον έλεγχο της ηλιοροφής κ.α. Τέλος, το FlexRay είναι ένας δίαυλος επικοινωνίας που έχει σχεδιαστεί για να εξασφαλίζει υψηλούς ρυθμούς δεδομένων και ανοχή σφαλμάτων.
2. *Στοιχεία συστήματος αυτόνομης οδήγησης:* Τα κυριότερα στοιχεία του συστήματος αυτόνομης οδήγησης είναι ο αισθητήρας light detector and ranging (LIDAR), η κάμερα, το σύστημα GPS, ο αισθητήρας RADAR, ο κεντρικός υπολογιστής κ.α.

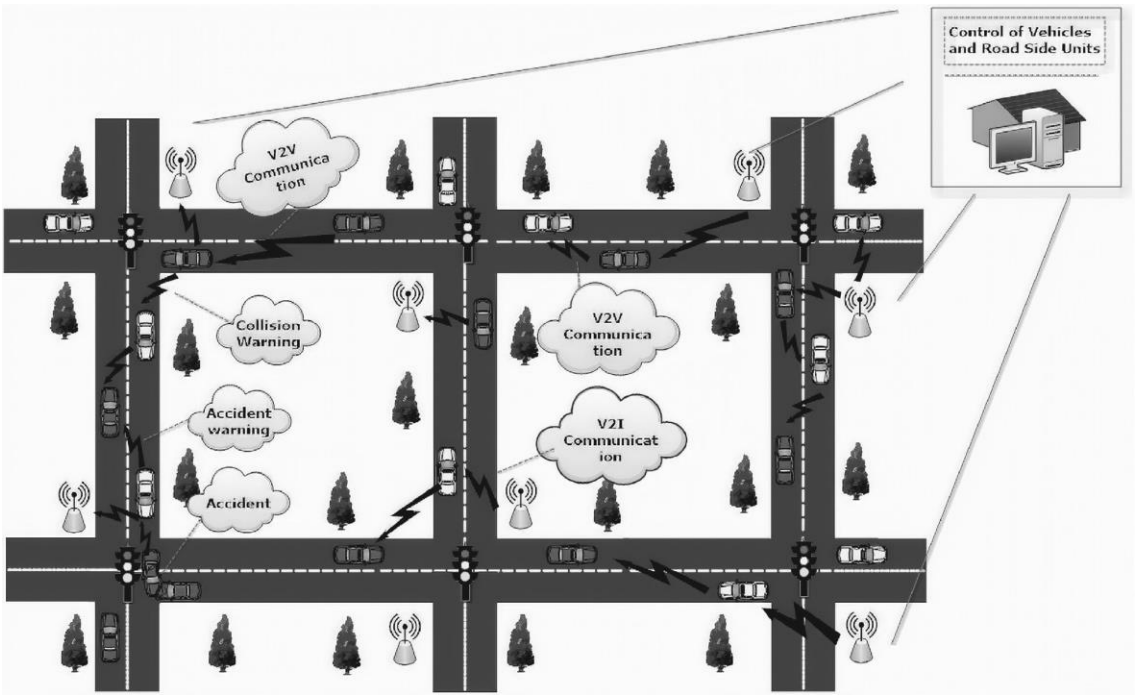
Το LIDAR είναι μία τεχνολογία που χρησιμοποιεί το φως για την ανίχνευση α-ντικειμένων και την μέτρηση αποστάσεων. Αυτό χρησιμοποιεί laser μικρότερου μήκους κύματος που επιτυγχάνει μεγαλύτερη ακρίβεια μέτρησης και καλύτερη ανάλυση από ότι το RADAR. Η κάμερα 'διαβάζει' την κυκλοφορία, την οδική σήμανση, τους διερχόμενους πεζούς αλλά και τα εμπόδια. Το σύστημα GPS λαμ-βάνει σήματα εκπεμπόμενα από τρείς ή περισσότερους δορυφόρους. Το RADAR χρησιμοποιείται για την αναγνώριση του περιβάλλοντος ενός οχήματος σε πραγ-ματικό χρόνο. Τέλος, ο κεντρικός υπολογιστής λαμβάνει πληροφορίες από όλους τους αισθητήρες και διαχειρίζεται το τιμόνι, το γκάζι και τα φρένα. Το λογισμικό του ερμηνεύει εάν οι οδικές συνθήκες είναι κανονικές ή μη. Αυτά τα στοιχεία περιγράφονται στην Εικόνα 24.



Εικόνα 24: Βασικά στοιχεία αυτόνομου οχήματος [8]

3. *Τεχνολογίες επικοινωνίας V2X*: Το δίκτυο επικοινωνίας μεταξύ του αυτοκινήτου και του εξωτερικού περιβάλλοντος αναφέρεται ως V2X. Τέτοια παραδείγματα είναι οι επικοινωνίες V2V, V2I κ.α. Το δίκτυο ad-hoc οχημάτων (VANET) είναι ένας τομέας σημαντικού ενδιαφέροντος για τις επικοινωνίες V2X. Αυτό χρησι-μοποιεί αποκλειστικές επικοινωνίες μικρής εμβέλειας (DSRC). Μία άλλη δομή επικοινωνίας που απαιτείται για το V2X είναι το δίκτυο κινητής τηλεφωνίας που αναφέρεται ως Cellular V2X το οποίο χρησιμοποιεί την τεχνολογία μακροπρόθε-σμης εξέλιξης CV2X και είναι ανώτερο από το DSRC ως αναφορά την επικοινω-νία. Ακόμη, χρησιμοποιούνται και άλλες τεχνολογίες όπως Bluetooth για V2X,

σήματα μέσω δορυφόρου κ.α. Χαρακτηριστικό παράδειγμα αυτών αποτελεί η Εικόνα 25. (Kim κ.α., 2021)



Εικόνα 25: Επικοινωνία V2X [8]

3 Ζητήματα ασφαλείας και μορφές επιθέσεων αυτόνομων οχημάτων

Τα σύγχρονα οχήματα είναι εφοδιασμένα με τεχνολογία αιχμής όπως κάμερες, αισθητήρες και άλλες έξυπνες συσκευές με σκοπό την παρακολούθηση, τη μετάδοση και τη λήψη πληροφοριών. Αυτά αποθηκεύουν προσωπικά δεδομένα όπως μηνύματα, οικονομικές πληροφορίες κ.α. Διάφοροι κακόβουλοι προσπαθούν να αποκτήσουν απομακρυσμένη πρόσβαση στις αποθηκευμένες πληροφορίες και να τις υποκλέψουν. Υπάρχουν διάφορες μορφές επιθέσεων των αυτόνομων οχημάτων αλλά υπάρχουν και διάφορα μέσα προστασίας από αυτές.

3.1 Προκλήσεις ασφαλείας και απορρήτου

Οι προκλήσεις των αυτόνομων οχημάτων χωρίζονται σε δύο κατηγορίες.

1. *Προκλήσεις ασφαλείας*. Η ασφάλεια αποτελεί βασική ανησυχία για το δίκτυο IoV, διότι μπορεί να υπάρξει αντίκτυπο και στην ανθρώπινη ζωή. Γι' αυτό το λόγο τα αυτόνομα οχήματα απαιτούν μία πολύ ισχυρή δομή ασφάλειας. Το δίκτυο IoV χρησιμοποιεί πληθώρα συστημάτων και μοντέλων επικοινωνίας κάνοντας το ευάλωτο σε επιθέσεις. Για να διασφαλιστεί η ασφαλής οδήγηση πρέπει τα οχήματα και οι χρήστες να προστατεύονται από διάφορες επιθέσεις όπως παρεμβολές, υποκλοπές κ.α. Η ασφάλεια εξαρτάται και από το μέσο επικοινωνίας, διότι τυχόν καθυστερήσεις στην παράδοση των πληροφοριών καθιστά το σύστημα ευάλωτο σε επιθέσεις.

   Ακόμη λόγω της γρήγορης κίνησης των οχημάτων και της διαρκούς αλλαγής της τοποθεσίας τους σε συνδυασμό με την προϋπόθεση για χαμηλό λανθάνοντα χρόνο του δικτύου είναι αναγκαίο ο τρέχον αλγόριθμος ασφαλείας για τα δίκτυα οχημάτων IoV να βελτιωθεί ανάλογα.

   Οι προκλήσεις ασφαλείας μπορούν να χωριστούν σε τρεις υποκατηγορίες:

   - *Απαιτήσεις υλικού (Hardware Requirement)*: Ο όρος ασφάλεια του υλικού αναφέρεται στην προστασία των στοιχείων του υλικού από τις επιθέσεις

στο δίκτυο IoV εξαιτίας των τρωτών σημείων των συσκευών. Αυτές αποτελούνται από διάφορες μονάδες επικοινωνίας όπως chips, αισθητήρες και διαύλους που συνεργάζονται στο δίκτυο αλλά και από υλικολογισμικό που αποτελεί στόχο επιθέσεων. Το υλικολογισμικό πρέπει να είναι πάντα ενημερωμένο με σκοπό την αποφυγή της επίθεσης. Οι επιθέσεις στο υλικό μπορεί να γίνουν όχι μόνο σε αυτό των οχημάτων αλλά και στο υλικό των υποδομών του δικτύου. Για το λόγο αυτό συσκευές όπως οι κεραίες εκπομπής θα πρέπει να φυλάσσονται σε ασφαλή περιοχή για την αποφυγή της μη εξουσιοδοτημένης πρόσβασης. Αυτό πρέπει να γίνει, διότι διάφοροι κακόβουλοι μπορούν να εμφυτεύσουν κακόβουλο λογισμικό με σκοπό να επηρεάσουν ολόκληρο το δίκτυο.

- *Απαιτήσεις λογισμικού (Software Requirement)*: Στο δίκτυο οχημάτων IoV οι συσκευές συλλέγουν πολλά και λεπτομερή δεδομένα από το περιβάλλον και τα οχήματα. Τα δεδομένα αυτά είναι αναγκαία για τη σωστή λειτουργία του δικτύου. Αν αυτά τα δεδομένα δεν είναι προστατευμένα διάφοροι εισβολείς μπορούν να εισχωρήσουν στο δίκτυο. Μία σημαντική πρόκληση στην ασφάλεια των αυτόνομων οχημάτων αποτελεί το σύστημα Infotainment. Μέσω αυτού οι χρήστες μπορούν να εγκαταστήσουν κακόβουλο λογισμικό εν αγνοία τους. Τότε διάφοροι κακόβουλοι μπορούν να τους παρακολουθούν, να τους υποκλέψουν ευαίσθητες πληροφορίες αλλά και να επιτεθούν στα συστήματα προκαλώντας επιθέσεις τύπου DoS ή DDoS. Οι επιθέσεις DDoS είναι από τις πιο συχνές τα τελευταία χρόνια.
- *Απαιτήσεις Radio (Radio Requirement)*: Οι έξυπνες συσκευές των αυτόνομων οχημάτων αλλά και οι έξυπνες υποδομές του δικτύου όπως τα φανάρια ελέγχου κυκλοφορίας καθιστούν το IoV ένα έξυπνο περιβάλλον. Οι συσκευές αυτές συλλέγουν και στέλνουν πληροφορίες στο cloud επικοινωνώντας με πρωτόκολλα όπως το Wi-Fi, το Zigbee, και το Bluetooth. Τα κανάλια επικοινωνίας δημιουργούν μία σύνδεση μεταξύ των διαφόρων στοιχείων του IoV και ως εκ τούτου χρειάζονται ισχυρή ασφάλεια για την αποτροπή κακόβουλων επιθέσεων στο δίκτυο.

  Το IoV σε συνδυασμό με το 5G έχει τη δυνατότητα να στέλνει περισσότερα δεδομένα, με γρηγορότερους ρυθμούς σε πολλές συσκευές ταυτόχρονα σε σύγκριση με το 4G. Λόγω του φάσματος του 5G και των πολλών

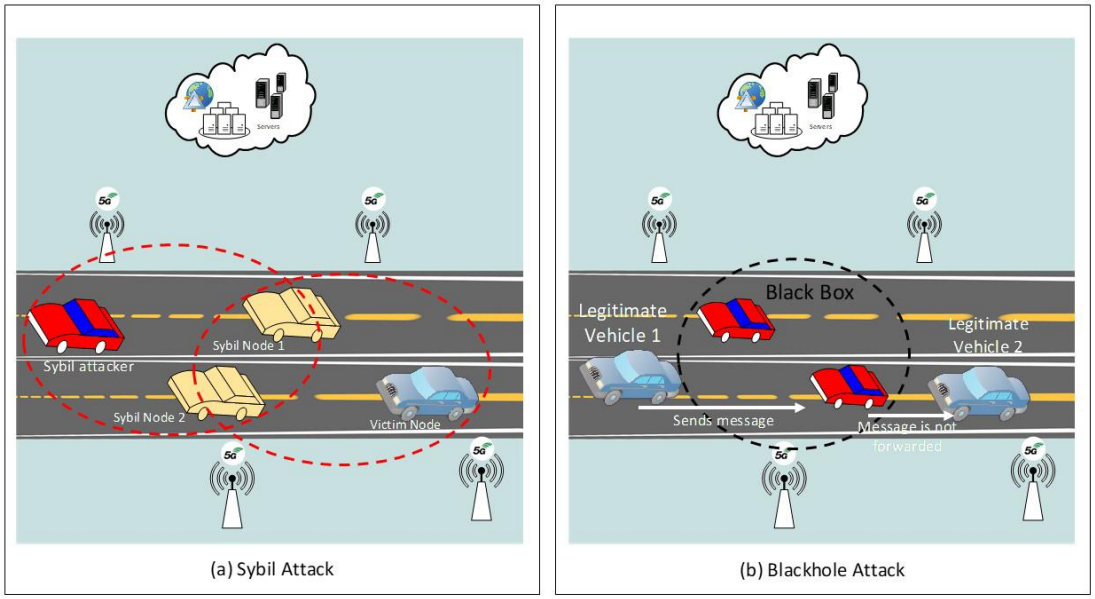
τεχνολογιών που διαθέτει απαιτείται να ληφθούν πολιτικές και μέτρα με σκοπό την προστασία του δικτύου.

2. *Προκλήσεις απορρήτου*: Στα δίκτυα αυτόνομων οχημάτων μπορεί να γίνουν διάφορες επιθέσεις στο απόρρητο. Οι κακόβουλοι συνήθως στοχεύουν πληροφορίες όπως η ταχύτητα του αυτοκινήτου, η κατάσταση του αυτοκινήτου και η τοποθεσία του. Ακόμη στοχεύουν και σε προσωπικές πληροφορίες των επιβαινόντων μέσω του συστήματος Infotainment. Υπάρχουν τρεις κρίσιμοι τομείς που συνήθως γίνονται στόχοι. Αυτοί είναι:
    - *Απόρρητο των πληροφοριών του οχήματος (Vehicular Information Privacy):* Διάφορες πληροφορίες των οχημάτων όπως η κατάσταση τους, οι πληροφορίες εγγραφής αλλά και τα δεδομένα που διακινούνται από αυτά πρέπει να έχουν κατάλληλη προστασία. Κατά την διάρκεια της εκφόρτωσης δεδομένων (offloading) της εφαρμογής τα δεδομένα μεταφέρονται από το όχημα σε πιο ισχυρές μονάδες για επεξεργασία. Τα δεδομένα αυτά είναι αναγκαίο να προστατεύονται από αυτούς που προσπαθούν να τα υποκλέψουν.
    - *Απόρρητο των προσωπικών πληροφοριών (Personal Information Privacy):* Μία πληθώρα πληροφοριών των ιδιοκτητών ή των οδηγών των αυτόνομων οχημάτων πρέπει να μην μπορούν να αποκαλυφθούν σε τρίτους. Τέτοιες πληροφορίες είναι τα ονόματα τους, ο αριθμός της άδειας οδήγησης κ.α. Ακόμη, πληροφορίες όπως τα μηνύματα και οι επαφές τα οποία αποθηκεύονται στο σύστημα Infotainment πρέπει να προστατεύονται επαρκώς, διότι αποτελούν στόχο υποκλοπής.
    - *Απόρρητο της τοποθεσίας (Location Privacy):* Η τοποθεσία του οχήματος καθώς και οι πληροφορίες ταξιδιού είναι ιδιωτικά στοιχεία του οχήματος. Αυτές πρέπει να διατηρούνται ασφαλείς από διάφορες προσπάθειες υποκλοπής τους. (Garg κ.α., 2020; Osibo κ.α., 2021)

3.2 Κατηγοριοποίηση επιθέσεων

Στο σύστημα IoV όλες οι συσκευές είναι συνδεδεμένες στο διαδίκτυο. Γι' αυτό το λόγο εγείρονται ανησυχίες σχετικά με την προστασία τους. Αυτό συμβαίνει, διότι πολλοί κακόβουλοι προσπαθούν να εκμεταλλευτούν διάφορα κενά ασφαλείας ή μη, με σκοπό την επίθεση στα συστήματα. Χαρακτηριστικοί τύποι επιθέσεων είναι:

1. *Επίθεση Sybil:* Η επίθεση Sybil χαρακτηρίζεται ως μία σοβαρή επίθεση όπου οι εισβολείς χρησιμοποιούν κακόβουλα πολλαπλές πλαστές ταυτότητες ή κόμβους με σκοπό να ελέγξουν τα οχήματα του περιβάλλοντος IoV. Τα οχήματα που πλήττονται από την επίθεση αντιλαμβάνονται τις πλαστές ταυτότητες ως μοναδικά χαρακτηριστικά κάποιων άλλων οχημάτων, αλλά υπάρχει μόνο ένας εισβολέας που ελέγχει τους ψεύτικους κόμβους ταυτόχρονα. Αυτό φαίνεται και στο πρώτο μισό στην Εικόνα 26.
2. *Επίθεση Blackhole:* Η επίθεση Blackhole αποτελεί μία πολύ γνωστή απειλή ασφαλείας στα δίκτυα οχημάτων. Σε αυτή οι εισβολείς προσπαθούν να εκμεταλλευτούν τα κενά ασφαλείας με σκοπό να πραγματοποιήσουν κακόβουλες δραστηριότητες ή να ανακατευθύνουν συγκεκριμένα πακέτα του δικτύου. Οι κακόβουλοι έχουν ως στόχο την διακοπή της ροής των πακέτων του δικτύου για να εισχωρήσουν σε αυτά ψεύτικες πληροφορίες ή να προκαλέσουν την απώλεια τους. Αυτό αναπαρίσταται στο δεύτερο μισό στην Εικόνα 26.



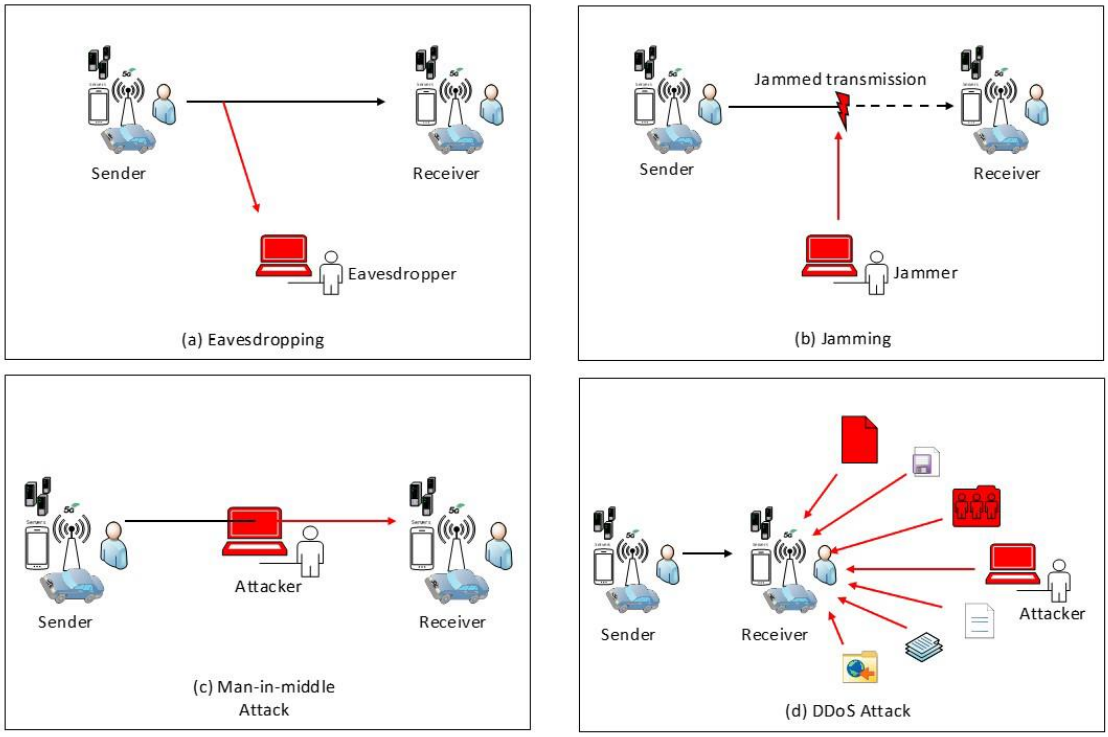
Εικόνα 26: Επίθεση Sybil και επίθεση Blackhole σε 5G IoV περιβάλλον [17]

3. *Επίθεση Υποκλοπής:* Η επίθεση υποκλοπής (Eavesdropping) συμβαίνει όταν κακόβουλοι αποκτούν μη εξουσιοδοτημένη πρόσβαση στην επικοινωνία των οχημάτων. Σε αυτή την μορφή επίθεσης αυτοί εκμεταλλεύονται τα δίκτυα οχημάτων που έχουν πλημμελή συστήματα ασφαλείας παρεμποδίζοντας την αποστολή και την λήψη δεδομένων από και προς το δίκτυο. Εκτός των οχημάτων στόχο αποτε-

λούν και οι οδικές μονάδες (RSU) του συστήματος IoV επειδή μεταφέρουν πληροφορίες κυκλοφορίας. Οι πληροφορίες αυτές δεν αλλοιώνονται μέσω της επίθεσης από τους επιτιθέμενους αλλά αυτοί έχουν ως στόχο την μυστική απόκτηση πρόσβασης σε αυτές. Γι' αυτό το συγκεκριμένο είδος επίθεσης είναι πολύ δύσκολο να ανιχνευθεί. Τέλος, η επίθεση υποκλοπής είναι γνωστή και ως επίθεση sniffing ή snooping.

4. *Επίθεση Μπλοκάρισμα:* Η επίθεση μπλοκάρισμα (Jamming) είναι ένα από τα μέσα που χρησιμοποιούν οι κακόβουλοι για να παραβιάσουν τα δίκτυα οχημάτων. Η επίθεση αυτή κατατάσσεται στις επιθέσεις DoS, διότι οι επιτιθέμενοι προκαλούν άρνηση υπηρεσιών στα εξουσιοδοτημένα συστήματα κατακλύζοντας τα με κίνηση δεδομένων και διατηρώντας απασχολημένο το μέσο επικοινωνίας.
5. *Επίθεση Man-In-The-Middle:* Η επίθεση MITM αποσκοπεί στην παραβίαση και στην υποκλοπή των επικοινωνιών μεταξύ δύο μερών του δικτύου. Αυτή είναι μια επικίνδυνη επίθεση στο δίκτυο, διότι ο επιτιθέμενος παρακολουθεί κρυφά, καταγράφει και ελέγχει την επικοινωνία μεταξύ των συστημάτων.
6. *Επιθέσεις DoS και DDoS:* Μία επίθεση άρνησης υπηρεσίας (DoS) συμβαίνει όταν μία υπηρεσία είναι μη διαθέσιμη για κάποιο χρονικό διάστημα λόγω υπερφόρτωσης της χωρητικότητας ή εξάντλησης των πόρων του δικτύου. Αυτή η επίθεση είναι σοβαρή, διότι μπορεί να καταστρέψει ολόκληρο το δίκτυο των οχημάτων κάνοντας τις υποδομές και τις υπηρεσίες μη διαθέσιμες για τους χρήστες. Σε μία επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) οι κακόβουλοι χρησιμοποιούν μεγαλύτερο αριθμό παραβιασμένων συστημάτων για να επιτεθούν. Αυτό κάνει δύσκολο τον εντοπισμό και την άμυνα κατά της επίθεσης. Οι επιτιθέμενοι δεν έχουν ως σκοπό την υποκλοπή των πληροφοριών αλλά να καταστήσουν το δίκτυο μη διαθέσιμο. Λόγω του αντίκτυπου που έχει ένα μη διαθέσιμο δίκτυο στους χρήστες αυτή η επίθεση είναι η πιο διαδεδομένη μεταξύ τω υπολοίπων.

   Αυτές οι επιθέσεις αναπαρίστανται στην Εικόνα 27. Επίσης εκτός από τις προαναφερθείσες επιθέσεις υπάρχουν και πολλές ακόμη επιθέσεις όπως επίθεση πλαστοπροσωπίας, επίθεση επανάληψης, επίθεση πλαστογραφίας κ.α. (Garg κ.α., 2020; Osibo κ.α., 2021)



Εικόνα 27: Αναπαράσταση διαφόρων μορφών επιθέσεων αυτόνομων οχημάτων [17]

3.3 Αντίμετρα Επιθέσεων

Για την αντιμετώπιση των προκλήσεων ασφαλείας αλλά και των διάφορων μορφών επιθέσεων υπάρχουν μια σειρά από προτεινόμενα αντίμετρα. Τα συστήματα αυτόνομης οδήγησης χρησιμοποιώντας αυτές τις λύσεις θα εξασφαλίσουν την ασφάλεια και θα αποτρέψουν τυχόν επιθέσεις. Τα αντίμετρα κατηγοριοποιούνται με βάση τα χαρακτηριστικά των συστημάτων που δέχονται συχνά επιθέσεις.

1. *Διαθεσιμότητα:* Η διαθεσιμότητα αναφέρεται στο συνολικό χρόνο λειτουργίας για τα δίκτυα (V2V, V2I κτλ.) και τα συστήματα του περιβάλλοντος του IoV. Αυτή είναι μία πολύ σημαντική απαίτηση ασφαλείας για τα συστήματα IoV, διότι τα οχήματα εξαρτώνται από την κυκλοφορία και τις πληροφορίες για το οδικό δίκτυο. Εάν τα συστήματα δεν είναι διαθέσιμα τότε ολόκληρο το περιβάλλον του IoV μπορεί να καταστεί μη λειτουργικό.

   Διάφοροι ερευνητές έχουν προτείνει κατά καιρούς διάφορες λύσεις. Οι Lyamin et al. προτείνουν μία προσέγγιση βασισμένη στην εξόρυξη δεδομένων για τον εντοπισμό επιθέσεων Jamming και DoS στις V2V επικοινωνίες. Η μέθοδος αυτή επιχειρεί να κατανοήσει πως χάνονται τα εκπεμπόμενα μηνύματα μεταξύ των ο-

χημάτων. Η ανίχνευση των επιθέσεων βασίζεται στο πρότυπο IEEE 802.11p. Επίσης οι Kumar et al. προτείνουν έναν αλγόριθμο ανίχνευσης πακέτων για την πρόληψη των επιθέσεων DoS στα δίκτυα οχημάτων. Ο αλγόριθμος αυτός ανιχνεύει τους κακόβουλους κόμβους στα δίκτυα οχημάτων που στέλνουν διάφορα πακέτα με σκοπό να μπλοκάρουν το δίκτυο.

2. *Ακεραιότητα δεδομένων:* Με τον όρο ακεραιότητα των δεδομένων εννοούμε ότι οι πληροφορίες που διανέμονται στο περιβάλλον IoV δεν έχουν αλλοιωθεί ή τροποποιηθεί από μη εξουσιοδοτημένα άτομα. Δηλαδή τα δεδομένα που λαμβάνονται είναι τα ίδια δεδομένα με αυτά που αποστέλλονται. Οι Admad et al. πρότειναν ένα μοντέλο με σκοπό την αντιμετώπιση των επιθέσεων Man-In-The-Middle στα δίκτυα οχημάτων. Το μοντέλο αυτό αναγνωρίζει τους κακόβουλους κόμβους που επιτίθενται στο δίκτυο και προσπαθεί να ανακαλέσει τα διαπιστευτήρια τους. Οι Alazzawi et al. προτείνουν ένα μοντέλο ασφαλούς επικοινωνίας βασισμένο σε ψεύτικες ταυτότητες για τα δίκτυα οχημάτων. Αυτό επιτυγχάνεται με τεχνικές κρυπτογράφησης που βασίζονται σε ταυτότητες (ID) για την παροχή ασφαλούς επικοινωνίας μεταξύ V2V και V2I. Αυτό το μοντέλο παρέχει ασφάλεια από τις επιθέσεις Man-In-The-Middle και πλαστοπροσωπίας.
3. *Εμπιστευτικότητα:* Η έννοια εμπιστευτικότητα αφορά την διατήρηση της μυστικότητας των πληροφοριών του οχήματος και των χρηστών από μη εξουσιοδοτημένα άτομα. Τα άτομα αυτά πρέπει να αποκλείονται από την πρόσβαση στα δεδομένα του οχήματος όπως η τοποθεσία ή η διαδρομή που έχει ακολουθήσει. Οι Huang et al. προτείνουν ένα μοντέλο με σκοπό την αποτροπή της υποκλοπής στα συστήματα IoV. Το μοντέλο αυτό δημιουργεί εικονικά πακέτα κυκλοφορίας και τα κατευθύνει σε συγκεκριμένα RSU με σκοπό να παραπληροφορήσουν τα στατιστικά στοιχεία κυκλοφορίας και να προστατεύσουν τα RSU hotspots από τους εισβολείς. Οι Xu et al. προτείνουν ένα μοντέλο προληπτικής υποκλοπής βασισμένο σε ανεστραμμένη εμπλοκή (rotated-jamming). Αυτό έχει ως σκοπό την παρακολούθηση της ύποπτης σύνδεσης μεταξύ μίας πηγής και του προορισμού. Αυτό εκτελεί δύο κύριες λειτουργίες την υποκλοπή της πληροφορίας και την παρεμβολή ενός ύποπτου συνδέσμου.
4. *Αυθεντικοποίηση:* Ο έλεγχος ταυτότητας είναι ένα σημαντικό μοντέλο ασφάλειας στο IoV, διότι επιβεβαιώνει την ταυτότητα των χρηστών ή των συστημάτων. Όταν ένα όχημα ή ένας κόμβος εισέρχεται στο δίκτυο πρέπει να υπάρχει ένα σύστημα ελέγχου ταυτότητας για την επαλήθευση της ταυτότητας τους αλλά και

των δεδομένων που αποστέλλουν. Οι ευαίσθητες αυτές πληροφορίες πρέπει να είναι κρυπτογραφημένες. Αυτό όμως προκαλεί εμπόδιο στην ανταλλαγή και στην αναζήτηση πληροφοριών, διότι τα διαμοιραζόμενα δεδομένα χρησιμοποιούνται από άλλα οχήματα στο δίκτυο ώστε να γνωρίζουν τις πληροφορίες κυκλοφορίας σε πραγματικό χρόνο. Οι Kumari et al. προτείνουν ένα αμυντικό μηχανισμό ενάντια στις επιθέσεις Sybil για ανώνυμη δρομολόγηση βάσει της τοποθεσίας. Ο μηχανισμός αυτός κατά την ανίχνευση λαμβάνει υπόψη προηγούμενες ανταλλαγές μηνυμάτων σε μία περιοχή και στη συνέχεια με βάση τη γωνία άφιξης οι κόμβοι ομαδοποιούνται σε περιοχές όπως ασφαλείς ή μη ασφαλείς.

5. *Αξιοπιστία:* Με την αξιοπιστία είμαστε βέβαιοι ότι τα δεδομένα που συλλέγονται από τους κόμβους και τα έξυπνα οχήματα δεν είναι εικονικά ή αναληθή. Για την ύπαρξη αξιοπιστίας οι δρομολογητές πρέπει να δρομολογούν τα πακέτα μόνο στο κεντρικό σύστημα ελέγχοντας την τοποθεσία του ώστε να μην υπάρχει σύγχυση των δεδομένων. Επίσης τα δεδομένα που λαμβάνονται θα πρέπει να έχουν χρονική σήμανση και να λαμβάνονται σε ένα συγκεκριμένο περιθώριο χρόνου, ειδάλλως το πακέτο θα απορριφθεί και θα πρέπει να αποσταλούν νέες πληροφορίες. Οι χρήστες που τις αποστέλλουν πρέπει να είναι εγγεγραμμένοι στο σύστημα. Αυτό είναι υποχρεωτικό, διότι πρέπει να υπάρχει εμπιστοσύνη μεταξύ των συστημάτων. Αυτά είναι εφοδιασμένα με κατάλληλα μοντέλα τα οποία μπορούν να αξιολογήσουν την αξιοπιστία των δεδομένων λήψης και αποστολής. (Garg κ.α., 2020; Osibo κ.α., 2021)

3.4 Ανάλυση και σύγκριση αλγορίθμων αποφυγής επιθέσεων

Σε αυτή την υποενότητα αναλύουμε διάφορους αλγορίθμους επιθέσεων και άμυνας κατά των επιθέσεων στα αυτόνομα οχήματα. Οι αλγόριθμοι παρατίθενται ολόκληροι στο Παράρτημα Α. Αρχικά αναφερόμαστε στους αλγορίθμους επιθέσεων κατά της βαθιάς μάθησης στα αυτόνομα οχήματα. Σύμφωνα με τους Jiang et al. υπάρχουν δύο κύριοι τύποι επιθέσεων κατά της βαθιάς μάθησης. Αυτοί είναι οι επιθέσεις PAPSO (poisoning attack with particle swarm optimization) και οι επιθέσεις EAPSO (evasion attack with particle swarm optimization).Οι επιθέσεις PAPSO επηρεάζουν την διαδικασία εκπαίδευσης του μοντέλου εισάγοντας επεξεργασμένα δείγματα στο σύνολο δεδομένων ενώ οι επιθέσεις

EAPSO επηρεάζουν την διαδικασία πρόβλεψης του μοντέλου βαθιάς μάθησης προσθέτοντας δυσδιάκριτες διαταραχές σε κανονικά δείγματα προκαλώντας τη λανθασμένη ταξινόμηση τους. Οι δύο τύποι επιθέσεων ανήκουν στις επιθέσεις μαύρου κουτιού.

Ο αλγόριθμος PAPSO βασίζεται στον αλγόριθμο PSO (Particle Swarm Optimization) ο οποίος παρουσιάστηκε από τους Eberhart και Kennedy το 1995. Ο στόχος του PSO είναι η δημιουργία πολυάριθμων σωματιδίων τα οποία κατανέμονται τυχαία στο χώρο των λύσεων. Κάθε πιθανή λύση έχει δύο ιδιότητες την ταχύτητα v_i και την θέση p_i. Η καλύτερη θέση του σωματιδίου συμβολίζεται ως *pbest* και η καλύτερη θέση ολόκληρης της ομάδας συμβολίζεται ως *gbest*. Κάθε σωματίδιο προσαρμόζει την ταχύτητα του και ενημερώνει τη θέση του με βάση τα *pbest* και *gbest* δημιουργώντας έτσι μία νέα γενιά ομάδων. Η βέλτιστη λύση βρίσκεται μετά από αρκετούς γύρους επαναλήψεων και μέσω της ανταλλαγής πληροφοριών μεταξύ των σωματιδίων της ομάδας.

Σκοπός της επίθεσης PASPO είναι η μείωση της ακρίβειας της ταξινόμησης του μοντέλου βαθιάς μάθησης. Αυτό επιτυγχάνεται μέσω της εισαγωγής μολυσμένων δεδομένων στο σύνολο των δεδομένων εκπαίδευσης. Τα μολυσμένα δεδομένα πρέπει να είναι κρυφά και να μην ανιχνεύονται από το μοντέλο. Αυτό επιτυγχάνεται με την προσθήκη ανεπαίσθητων διαταραχών στα κανονικά δείγματα. Σύμφωνα με τους Jiang et al. στον *Αλγόριθμο 1* γίνεται αρχικοποίηση της επίθεσης PAPSO επιλέγοντας ένα κανονικό δείγμα και δημιουργώντας του τυχαίες διαταραχές ενώ ο *Αλγόριθμος 2* περιγράφει την επίθεση PASPO. Όπως φαίνεται σε αυτούς τους αλγορίθμους το εύρος που λαμβάνει η τιμή p_i εκφράζει τις διαφορετικές διαταραχές που θα προστεθούν στο κανονικό δείγμα (x_n, y_n), ενώ η τιμή $acc(p_i)$ αντιπροσωπεύει την ακρίβεια της ταξινόμησης του εκπαιδευμένου μοντέλου σε σύνολο δεδομένων D_{tr}. Το μολυσμένο δείγμα χαρακτηρίζεται από την τιμή (x_n+p_i, y_n) και συνδυάζεται με το κανονικό δείγμα (x_n, y_n) και την θέση p_i. Με p_i* συμβολίζεται το *pbest* του p_i και με p_{gb} συμβολίζεται το *gbest.*

Ο στόχος της επίθεσης EAPSO είναι η μείωση της πιθανότητας του στοχευμένου δείγματος δοκιμής να ταξινομηθεί σωστά. Αυτό επιτυγχάνεται με την προσθήκη μικρών διαταραχών στο δείγμα. Σύμφωνα με τους Jiang et al. στον *Αλγόριθμο 3* γίνεται η αρχικοποίηση του EAPSO ενώ ο *Αλγόριθμος 4* παρουσιάζει την επίθεση EAPSO. Σε αυτούς το στοχευμένο δείγμα συμβολίζεται ως (x_t, y_t) και με p_j συμβολίζονται οι διαταραχές που θα προστεθούν στο στοχευμένο δείγμα δοκιμής. Η πιθανότητα του μολυσμένου δείγματος (x_t+p_j, y_t) να ταξινομηθεί σωστά περιγράφεται από τον όρο $pro(p_j)$ ενώ το *pbest* του p_j συμβολίζεται με p_j* και το *gbest* συμβολίζεται με p_{gb}. Σημαντικό είναι να αναφέρουμε

πως εφόσον αυτές οι επιθέσεις ανήκουν στην κατηγορία του μαύρου κουτιού ο επιτιθέμενος δεν γνωρίζει πληροφορίες για τα υπό επίθεση συστήματα.

Μια χαρακτηριστική εφαρμογή αυτών των αλγορίθμων είναι οι επιθέσεις στο σύστημα αναγνώρισης των σημάτων κυκλοφορίας. Αρχικά, για τον αλγόριθμο PASPO ορίζουμε ως M_1 τον αριθμό των σωματιδίων, επιλέγουμε μία κανονική εικόνα από το σύνολο των δεδομένων εκπαίδευσης και αρχικοποιούμε τον αλγόριθμο. Στην συνέχεια ορίζουμε τις παραμέτρους και εκτελούμε τον αλγόριθμο. Μέσω των T_1 επαναλήψεων επιλέγουμε το σωματίδιο που ελαχιστοποιεί την ακρίβεια του μοντέλου, το θέτουμε ως μολυσμένο δείγμα και το επανατοποθετούμε στο αρχικό σύνολο δεδομένων εκπαίδευσης D_{tr}. Μετά από αυτήν την ενέργεια επαναλαμβάνουμε όλη την διαδικασία από την αρχή. Τέλος, το σύνολο των μολυσμένων δεδομένων Dp που παράγεται από αυτή την διαδικασία είναι το βέλτιστο σύνολο.

Για τον αλγόριθμο EAPSO στις επιθέσεις κατά της ανίχνευσης των σημάτων κυκλοφορίας γίνονται οι εξής ενέργειες. Αρχικά, ορίζουμε ως M_2 τον αριθμό των σωματιδίων, διαλέγουμε τη στοχευμένη πινακίδα κυκλοφορίας και αρχικοποιούμε τον αλγόριθμο. Στην συνέχεια ορίζουμε τις απαιτούμενες παραμέτρους και εκτελούμε τον αλγόριθμο. Μέσω των T_2 επαναλήψεων επιλέγουμε το σωματίδιο που ελαχιστοποιεί την πιθανότητα να ταξινομηθεί σωστά το στοχευμένο δείγμα δοκιμής. Τέλος, το βέλτιστο δείγμα επίθεσης είναι ο συνδυασμός του σωματιδίου και του στοχευμένου δείγματος δοκιμής.

Οι Jiang et al. διεξήγαγαν επιθέσεις στην αναγνώριση των σημάτων κυκλοφορίας καθώς και άλλες επιθέσεις και παρήγαγαν κάποια πολύ σημαντικά αποτελέσματα. Σύμφωνα με αυτά αποδεικνύεται ότι η ακρίβεια της ταξινόμησης του εκπαιδευμένου μοντέλου μειώθηκε από 95% σε 33% με μόλυνση μόνο του 10% των δειγμάτων. Επίσης η πιθανότητα το στοχευμένο δείγμα να ταξινομηθεί σωστά πέφτει από το 93% στο 22% προσθέτοντας κάποιες μη αντιληπτές διαταραχές. Μέσα από αυτά φαίνεται πως αυτές οι επιθέσεις είναι πολύ πετυχημένες. (W. Jiang et al., 2020)

Παράλληλα με τους αλγορίθμους επιθέσεων πολλοί επιστήμονες ερευνούν και παρουσιάζουν διάφορους αλγορίθμους άμυνας. Παράδειγμα αποτελεί η έρευνα των Aldhyani και Alkahtani οι οποίοι παρουσίασαν ένα σύστημα με χρήση τεχνητής νοημοσύνης για την προστασία του δικτύου των αυτόνομων οχημάτων από τις κυβερνοεπιθέσεις. Το σύστημα αυτό βασίζεται στη βαθιά μάθηση και εφαρμόστηκε σε δεδομένα επιθέσεων spoofing, flood, replay και σε benign πακέτα. Τα δεδομένα των επιθέσεων επεξεργάστηκαν από ένα μοντέλο CNN και από ένα υβριδικό δίκτυο το οποίο συνδυάζει το

μοντέλο CNN και το μοντέλο της βραχύχρονης μνήμης (CNN-LSTM) για την αναγνώριση των μηνυμάτων των επιθέσεων.

Το σύνολο δεδομένων που χρησιμοποιήθηκε για την εκπαίδευση του μοντέλου προήλθε από αληθινά δεδομένα CAV οχημάτων στα οποία διενεργήθηκαν οι προαναφερθείσες επιθέσεις. Για την μεταφορά των μολυσμένων μηνυμάτων και την παραγωγή του συνόλου δεδομένων χρησιμοποιήθηκε ο δίαυλος CAN και η θύρα OBD-II των οχημάτων CAV. Οι επιθέσεις διενεργούνταν κάθε 3 με 5 δευτερόλεπτα και η κίνηση του CAV διήρκησε 30 με 40 λεπτά. Για την διενέργεια αυτού χρησιμοποιήθηκε η γεννήτρια CAN πακέτων OCTANE (Open Cav Testbed and Network Experiments). Για την χρησιμοποίηση του συνόλου δεδομένων έγινε μία προεπεξεργασία τους ώστε να γίνουν όλα αριθμητικές τιμές. Επίσης, χρησιμοποιήθηκαν μέθοδοι κανονικοποίησης όπως ο αλγόριθμος max-min για την αποφυγή της επικάλυψης κατά την εκπαίδευση.

Στην έρευνα των Aldhyani και Alkahtani παρουσιάστηκαν προσεγγίσεις βαθιάς μάθησης για τον εντοπισμό των επιθέσεων στα CAV. Αυτό έγινε παρουσιάζοντας την τεχνική LSTM ως ένα RNN μοντέλο για την μακροπρόθεσμη εξάρτηση από την γνώση. Η διαφορά μεταξύ του LSTM και του RNN βρίσκεται στον τρόπο με τον οποίο λειτουργούν τα κελιά στην περίπτωση του πρώτου. Κάθε LSTM έχει τέσσερις πύλες: i) Input ii) Candidate iii) Forget iv) Output. Η πύλη Forget ταξινομεί τα δεδομένα για το εάν πρέπει να αποθηκευτούν ή εάν πρέπει να απορριφθούν, η πύλη Input ανανεώνει τα κελιά και από την πύλη Output καθορίζεται η κρυφή κατάσταση του LSTM. Ακόμη αυτό έχει ενσωματωμένη μνήμη και πύλες ώστε να επιλύει τις διάφορες δυσκολίες όπως τις επιπλοκές κατά την διαδικασία μάθησης του RNN.

Ο αλγόριθμος CNN-LSTM, ο οποίος παρατίθεται ολόκληρος στο Παράρτημα Α, είναι ένας ολοκληρωμένος αλγόριθμος βαθιάς μάθησης που βασίζεται στα νευρωνικά δίκτυα. Σκοπός της δημιουργίας του είναι η επίλυση προβλημάτων οπτικής πρόβλεψης χρονοσειρών και η δημιουργία κειμένου από τις ακολουθίες εικόνων. Τα επίπεδα του μοντέλου CNN χρησιμοποιούνται για την εξαγωγή πληροφοριών από τα δεδομένα εισόδου ενώ το μοντέλο LSTM συνδυάζεται με το CNN για την διαδοχική πρόβλεψη του συστήματος. Άρα, το μοντέλο CNN λαμβάνει πληροφορίες από τα δεδομένα, τις εφαρμόζει στο μοντέλο LSTM για να δημιουργηθεί η περιγραφή και μετά ταξινομεί το σύστημα ανίχνευσης εισβολής.

Κατά την διενέργεια των πειραμάτων με την χρήση των αλγορίθμων χρησιμοποιήθηκε η γεννήτρια CAN πακέτων OCTANE ώστε να γίνει η συλλογή των δεδομένων εκπαίδευσης. Στο πείραμα εφαρμόστηκαν οι αλγόριθμοι CNN και CNN-LSTM. Το σύνολο δεδομένων χωρίστηκε 70% για εκπαίδευση και 30% για έλεγχο. Σύμφωνα με τα αποτελέσματα το μοντέλο CNN κατάφερε 86% precision, 100% recall, 93% specificity και 100% F1-score. Όμως το μοντέλο CNN δεν μπόρεσε να εντοπίσει τα πακέτα επίθεσης. Έτσι, η συνολική του απόδοση στην αναγνώριση των μηνυμάτων επίθεσης είναι 86%, διότι υπάρχει υπερπροσαρμογή του μοντέλου. Οι τιμές των μετρικών για το μοντέλο CNN-LSTM απεικονίζονται στον Πίνακας 1. Όπως φαίνεται στις επιθέσεις Benign, Flood, Fuzzy καταφέρνει πολύ υψηλά αποτελέσματα. Ωστόσο, δεν μπορεί να ανιχνεύσει τις επιθέσεις Replay και Spoofing. Η απόδοση του είναι βελτιωμένη σε σχέση με του CNN φτάνοντας άνω του 95%. Εάν βέβαια δεν χρησιμοποιηθούν οι επιθέσεις τις οποίες δεν μπορεί να ανιχνεύσει το μοντέλο, το accuracy ξεπερνά το 97%.

Πίνακας 1: Πίνακας αποτελεσμάτων μετρικών του μοντέλου CNN-LSTM [2]

Attacks	**Precision %**	**Recall %**	**F1-Score %**
Benign	95	100	97
Flood	91	0.09	0.16
Replaying	0.0	0.0	0.0
Spoofing	0.0	0.0	0.0
Fuzzy	96	100	98
Accuracy		95.44%	
Weighted average	93	95	93
Loss		0.20	

Σύμφωνα με την σύγκριση των Adhyani και Alkahtani παρόλο που ο αλγόριθμος CNN-LSTM δεν ανιχνεύει όλες τις επιθέσεις έχει καλύτερη απόδοση σε σχέση με αυτούς των υπολοίπων επιστημόνων. Ο αλγόριθμος αυτός επιτυγχάνει απόδοση έως 97% ενώ άλλοι αλγόριθμοι επιτυγχάνουν απόδοση της τάξης του 80-85%. Τέλος, με βάση τα αποτελέσματα το μοντέλο πέτυχε υψηλή απόδοση κάτι το οποίο φαίνεται μέσα από τους δείκτες precision, recall, F1 score, accuracy και μέσω της σύγκρισης του με άλλα μοντέλα-αλγορίθμους. (Aldhyani, H., Alkahtani, 2022)

Σε αυτή την υποενότητα αναλύθηκαν δύο κατηγορίες αλγορίθμων. Αυτοί είναι οι αλγόριθμοι επιθέσεων και οι αλγόριθμοι άμυνας κατά των επιθέσεων στα αυτόνομα οχήματα. Όλοι οι αλγόριθμοι βασίζονται στην τεχνητή νοημοσύνη και συγκεκριμένα στην

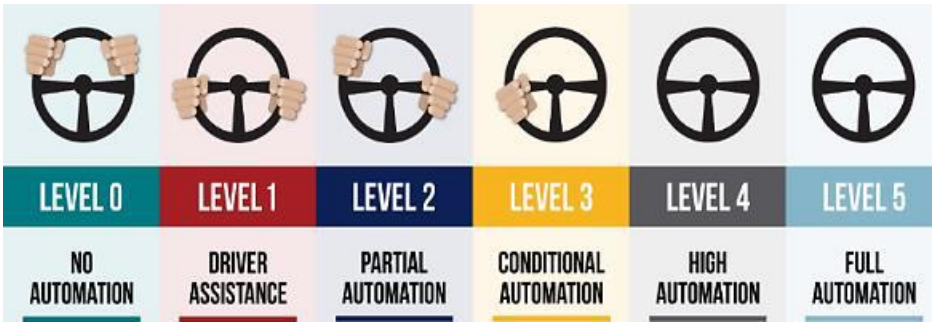
βαθιά μάθηση. Στην πρώτη κατηγορία αναλύθηκαν δύο αλγόριθμοι. Αυτοί αφορούν τις επιθέσεις PAPSO και EAPSO κατά της διαδικασίας εκπαίδευσης του μοντέλου βαθιάς μάθησης. Ο μεν πρώτος αποσκοπεί στην μείωση της ακρίβειας ταξινόμησης του μοντέλου βαθιάς μάθησης ενώ ο δεύτερος αποσκοπεί στην μείωση της πιθανότητας του στοχευμένου δείγματος να ταξινομηθεί σωστά. Με βάση τα αποτελέσματα από διάφορες έρευνες όπως π.χ. επιθέσεις κατά της ανίχνευσης κατά των σημάτων κυκλοφορίας φαίνεται πώς αυτοί οι αλγόριθμοι επιτυγχάνουν τον στόχο τους σε μεγάλο βαθμό. Επίσης το σύνολο δεδομένων προς μόλυνση που αποφασίζουν να χρησιμοποιήσουν αυτοί οι αλγόριθμοι είναι το βέλτιστο σύνολο δεδομένων. Αυτό φαίνεται από τα μεγάλα ποσοστά επιτυχίας των επιθέσεων που αυτοί κατέχουν.

Η δεύτερη κατηγορία αλγορίθμων που παρουσιάστηκαν αναφέρονταν στους αλγορίθμους άμυνας κατά των επιθέσεων. Αυτοί οι αλγόριθμοι είναι ο CNN και ο CNN-LSTM. Μέσω πειραμάτων έχει αποδειχθεί πως ο αλγόριθμος CNN δεν εντοπίζει τα πακέτα επίθεσης, ενώ ο αλγόριθμος CNN-LSTM εντοπίζει αρκετές μορφές επιθέσεων. Βάση αυτών συμπεραίνουμε πως οι αλγόριθμοι αυτοί δεν είναι βέλτιστοι, ωστόσο η απόδοση τους υπερτερεί έναντι των υπολοίπων αλγορίθμων που υπάρχουν στην βιβλιογραφία σχετικά με αυτό το αντικείμενο. Ως αποτέλεσμα της ανάλυσης και της σύγκρισης αυτών των αλγορίθμων φαίνεται πως οι αλγόριθμοι επίθεσης είναι πολύ εξελιγμένοι και επιτυγχάνουν σε συντριπτική πλειοψηφία τους στόχους που θέτουν ενώ οι αλγόριθμοι άμυνας επιδέχονται βελτίωση, διότι παρόλο που έχουν μεγάλο ποσοστό απόδοσης δεν επιτυγχάνουν τους στόχους τους οι οποίοι είναι ο εντοπισμός των επιθέσεων.

4 Ανίχνευση και πρόληψη επιθέσεων σε συστήματα (CAV)

Τα Connected and Autonomous Vehicles (CAV) είναι ένα είδος αυτοκινήτου που είναι εξοπλισμένο με πληθώρα τεχνολογιών όπως αισθητήρες, ρομποτική και πολύπλοκο λογισμικό. Τα οχήματα αυτά εκτελούν διάφορες λειτουργίες όπως επικοινωνία Vehicle to Everything (V2X) και μετάδοση δεδομένων In Vehicle Network (IVN) μέσω ασύρματης τεχνολογίας. Το IVN είναι ο θεμέλιος λίθος του CAV για τον υπολογισμό των δεδομένων και για την επικοινωνία μεταξύ των διαφορετικών αισθητήρων και των μηχανικών εξαρτημάτων σε ένα όχημα. Αυτό χρησιμοποιεί το πρωτόκολλο CAN για αποτελεσματικό ρυθμό μετάδοσης των δεδομένων και την τοπολογία διαύλου για την σύνδεση των Electric Control Units (ECU). Τα CAV ή αλλιώς τα αυτοκίνητα χωρίς οδηγό είναι μια καινούργια τεχνολογία η οποία εντάσσεται στο ευφυές σύστημα μεταφοράς (ITS). Τα οχήματα αυτά αντιλαμβάνονται το περιβάλλον μέσω των διάφορων αισθητήρων και οδηγούν με ασφάλεια χωρίς ανθρώπινη παρέμβαση.

Τα οχήματα αυτά προσφέρουν τεράστια οφέλη στην κοινωνία και στο περιβάλλον όπως μείωση των τροχαίων ατυχημάτων, της κυκλοφοριακής συμφόρησης και εξάλειψη των CO_2 εκπομπών λόγω της χρήσης ηλεκτρικών οχημάτων. Ο έλεγχος των διάφορων στοιχείων των οχημάτων CAV γίνεται αυτόματα από το όχημα και όχι από τον οδηγό. Ανάλογα με το επίπεδο αυτονομίας των οχημάτων έχει δημιουργηθεί μία κλίμακα έξι επιπέδων η οποία δείχνει το επίπεδο ελέγχου του οχήματος και του οδηγού. Το επίπεδο 0 υποδεικνύει μη αυτοματισμό ενώ το επίπεδο 5 πλήρη αυτοματισμό όπως φαίνεται και στην Εικόνα 28. (Masood M., Saeed Z. & Khan M. U., 2023; Limbasiya κ.α., 2022)



Εικόνα 28: Τα έξι επίπεδα αυτονομίας των οχημάτων [14]

4.1 Απαιτήσεις ασφάλειας και απορρήτου

Η χρήση των οχημάτων CAV αυξάνεται συνεχώς λόγω των πλεονεκτημάτων τους. Γι' αυτό το λόγο είναι αναγκαία η ύπαρξη ασφάλειας τόσο στο λογισμικό όσο και στην επικοινωνία μεταξύ των διαφορετικών τεχνολογιών που διαθέτουν.

1. *Διαθεσιμότητα:* Με τον όρο διαθεσιμότητα εννοούμε την αξιοπιστία των πληροφοριών που λαμβάνονται από τον παραλήπτη σε καθορισμένο χρόνο, με σκοπό την προώθηση τους για περεταίρω ενέργειες. Εάν οι πληροφορίες αυτές δεν είναι διαθέσιμες όταν τις χρειάζεται το σύστημα τότε θα προκληθούν διάφορα προβλήματα σε αυτό. Τα οχήματα CAV έχουν σχεδιαστεί με το δίκτυο CAN για να εκτελούν διάφορες αυτοματοποιημένες λειτουργίες με βάση τα δεδομένα τα οποία συλλέγονται από το όχημα μέσω της λειτουργικότητας του δικτύου IVN. Τα κρίσιμα στοιχεία των οχημάτων πρέπει να λαμβάνουν τις οδηγίες χωρίς καθυστέρηση με σκοπό την εκτέλεση διάφορων αναγκαίων για τα οχήματα λειτουργιών. Τέτοια στοιχεία είναι ο κινητήρας, το σύστημα μετάδοσης κίνησης κ.α. Εάν τα δεδομένα δεν είναι άμεσα διαθέσιμα στα κρίσιμα στοιχεία του αυτοκινήτου μπορεί να προκληθούν ατυχήματα με επακόλουθο τραυματισμό των επιβαινόντων ή και άλλων ανθρώπων. Ακόμη είναι απαραίτητη η αποστολή κατάλληλου μηνύματος στην περίπτωση που αποτύχει η παράδοση των δεδομένων. Μέσα από όλα αυτά φαίνεται πόσο σημαντική είναι η διαθεσιμότητα των δεδομένων στα οχήματα CAV.
2. *Αυθεντικοποίηση:* Η ανταλλαγή μηνυμάτων επιτυγχάνεται μέσω διάφορων καναλιών. Όταν ο παραλήπτης λάβει το μήνυμα πρέπει να επιβεβαιώσει τον αποστολέα και να διαπιστώσει την ακρίβεια των δεδομένων του μηνύματος. Με αυτόν τον τρόπο αποφεύγονται οι εσφαλμένες πληροφορίες ή οι πλαστογραφίες. Η επιβεβαίωση του αποστολέα και του παραλήπτη γίνεται μέσω αμοιβαίων μηχανισμών ελέγχου ταυτότητας και κλειδιών. Αλλιώς θα προκληθούν επιθέσεις πλαστοπροσωπίας και τροποποίησης των δεδομένων γεγονός που μπορεί να προκαλέσει ζημιές υποδομής και κίνδυνο για την ζωή των επιβατών. Οι μονάδες ελέγχου ECU των οχημάτων είναι συνδεδεμένες στο δίαυλο CAN για την αποστολή μηνυμάτων και την εκτέλεση διάφορων λειτουργιών στα αυτόνομα οχήματα. Έτσι είναι απαραίτητος ο έλεγχος ταυτότητας του αποστολέα για την αποφυγή πλαστών πληροφοριών. Εάν ο αποστολέας δεν είναι πιστοποιημένος τότε μπορεί να

συμβούν κακόβουλες ενέργειες με σκοπό την διακοπή του δικτύου IVN και την βλάβη των συστημάτων των οχημάτων CAV.

3. *Ακεραιότητα:* Οι πληροφορίες τις οποίες λαμβάνει ο παραλήπτης πρέπει να είναι ίδιες με αυτές που έστειλε ο αποστολέας. Εάν ο παραλήπτης λάβει τροποποιημένες πληροφορίες τα μηνύματα που μεταδίδονται αλλοιώνονται και υπάρχει έλλειψη ακεραιότητας των δεδομένων. Μηνύματα με τροποποιημένες πληροφορίες πρέπει να απορρίπτονται από τον παραλήπτη, διότι εάν τα αποδεχθεί θα οδηγηθεί σε λάθος αποφάσεις καθώς οι πληροφορίες που λαμβάνονται χρησιμοποιούνται στην απόφαση των περεταίρω ενεργειών των συστημάτων. Οι λειτουργίες των οχημάτων CAV είναι αυτοματοποιημένες και δεν υπάρχει ανθρώπινη παρέμβαση σε αυτές. Γι' αυτό είναι απαραίτητη η ακεραιότητα των δεδομένων ώστε να επαληθεύονται τα μηνύματα που λαμβάνονται.
4. *Εμπιστευτικότητα:* Τα μηνύματα μεταφέρονται μέσω δημοσίων καναλιών. Έτσι, είναι αναγκαίο να διασφαλιστεί ότι μόνο οι νόμιμοι παραλήπτες κατανοούν τις πληροφορίες των μηνυμάτων διατηρώντας τα δεδομένα τους απόρρητα. Η εμπιστευτικότητα των δεδομένων χάνεται όταν διάφοροι κακόβουλοι μπορούν να εξάγουν πληροφορίες υποκλέπτοντας τα μηνύματα. Εάν μία συσκευή παραβιαστεί μπορεί να αποκαλύψει εμπιστευτικές πληροφορίες κατά την αποστολή δεδομένων στο σύστημα. Τα μηνύματα που αποστέλλονται από το δίκτυο IVN μέσω του διαύλου CAN περιλαμβάνουν δεδομένα που είναι απαραίτητα για τις επόμενες ενέργειες του συστήματος. Τα μηνύματα αυτά είναι διαθέσιμα σε όλες τις συνδεδεμένες μονάδες ECU λόγω της εκπομπής του CAN. Έτσι παραβιάζοντας μία μονάδα ECU κάποιος κακόβουλος μπορεί να έχει πρόσβαση σε όλα τα μηνύματα επηρεάζοντας την λειτουργία του οχήματος.
5. *Απόρρητο χρηστών:* Το δίκτυο CAN είναι πολύ χρήσιμο σε αυτόνομα συστήματα όπως τα οχήματα CAV, διότι μειώνει την ανθρώπινη παρέμβαση στις διάφορες λειτουργίες του. Στα αυτόνομα οχήματα CAV τα συστήματα είναι συνδεδεμένα με διάφορες συσκευές για την ανάλυση των δεδομένων μέσω της ανταλλαγής σημαντικών στοιχείων. Τα δεδομένα αυτά είναι ιδιαίτερα κρίσιμα και θα υπάρξουν σημαντικές επιπτώσεις στο σύστημα αλλά και στους χρήστες εάν δεν υπάρχει η απαραίτητη προστασία τους. Η διαρροή των δεδομένων αυτών μπορεί να αποκαλύψει τις δραστηριότητες των χρηστών του οχήματος, τα μέρη που έχουν επισκεφτεί αλλά και τις διάφορες ενέργειες που έχουν γίνει στο όχημα. Για την

αποφυγή τέτοιων ενεργειών είναι απαραίτητο να διασφαλιστεί ότι μόνο εξουσιοδοτημένες υπηρεσίες μπορούν να γνωρίζουν τις δραστηριότητες των χρηστών των οχημάτων. (Limbasiya κ.α., 2022)

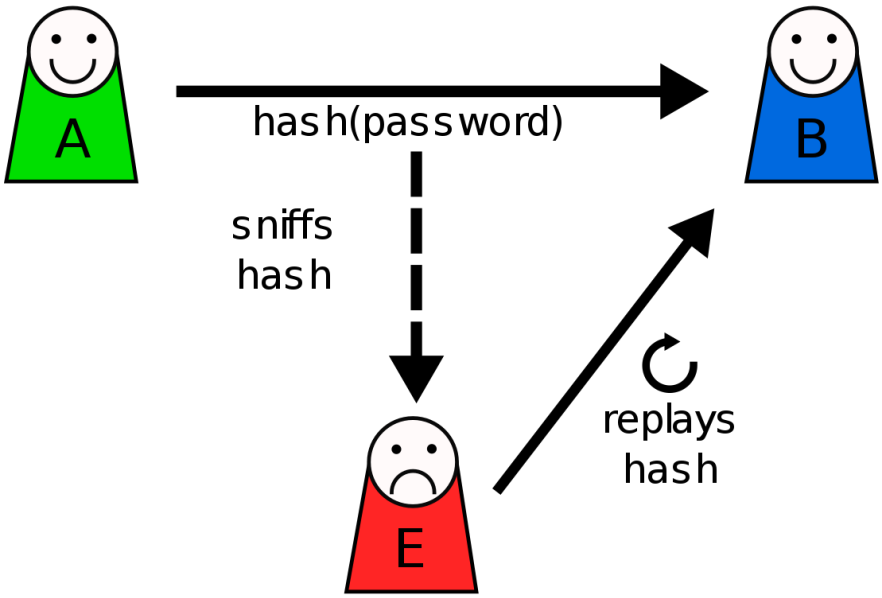
4.2 Μορφές επιθέσεων

Τα οχήματα CAV είναι υποχρεωτικό να συνδέονται με άλλες οντότητες για την ορθή λειτουργία τους. Η σύνδεση αυτή όμως τα κάνει ευάλωτα σε διάφορες μορφές επιθέσεων. Υπάρχουν δύο κύρια είδη επιθέσεων οι παθητικές και οι ενεργές.

1. *Παθητικές επιθέσεις*: Όταν συμβαίνει μία παθητική επίθεση είναι πολύ δύσκολο να εντοπιστεί. Αυτό γίνεται, διότι ο εισβολέας δεν μπορεί να αλλάξει το περιεχόμενο των δεδομένων του μηνύματος. Επίσης, ο αποστολέας και ο παραλήπτης δεν γνωρίζουν ότι παρεμβάλει κάποιος κακόβουλος στην μεταξύ τους επικοινωνία. Οι επιθέσεις αυτές έχουν ως σκοπό την παρακολούθηση της κυκλοφορίας των δεδομένων.
    - *Υποκλοπή*: Οι επιθέσεις υποκλοπής έχουν ως σκοπό την κλοπή των μηνυμάτων από το κανάλι επικοινωνίας V2X. Πιθανές ευπάθειες του διαύλου CAN έχουν ως αποτέλεσμα οι εισβολείς να αποκτούν πρόσβαση στο δίκτυο του οχήματος και να παρακολουθούν την μετάδοση των μηνυμάτων. Το γεγονός ότι τα οχήματα CAV επικοινωνούν με διάφορους άλλους όπως πεζούς, υποδομές κ.α. κάνει τις επιθέσεις υποκλοπής μείζονος σημασίας, διότι οι κακόβουλοι μπορούν να παρακολουθούν ιδιωτικές πληροφορίες.
    - *Ανάλυση κυκλοφορίας δεδομένων:* Επειδή οι επιθέσεις υποκλοπής μπορούν να αποφευχθούν με τη χρήση κρυπτογραφημένων μηνυμάτων, οι κακόβουλοι χρησιμοποιούν τεχνικές ανάλυσης της κυκλοφορίας των δεδομένων για να αντλήσουν πληροφορίες μέσω της κίνησης αυτών. Τέτοιες πληροφορίες είναι η διάρκεια, ο χρόνος, η συχνότητα των μηνυμάτων αλλά και η παρουσία ή μη του οδηγού. Οι κακόβουλοι μέσα από αυτά τα δεδομένα μπορούν να εξάγουν πληροφορίες για την καθημερινότητα των χρηστών των CAV.
2. *Ενεργές επιθέσεις:* Σε αυτό το είδος επιθέσεων οι κακόβουλοι εισχωρούν στο δίκτυο επικοινωνίας και μπορούν να αλλάξουν τα περιεχόμενα των μηνυμάτων ή να παράγουν νέα πακέτα δεδομένων. Οι επιθέσεις αυτές είναι σοβαρότερες από

τις παθητικές στα συστήματα των CAV, διότι η αλλαγή των μηνυμάτων μπορεί να προκαλέσει βλάβη στο ίδιο το όχημα αλλά και τραυματισμό των επιβαινόντων.

- *Επιθέσεις Spoofing*: Με τον όρο επιθέσεις πλαστογράφησης εννοούμε την εισβολή ενός μη εξουσιοδοτημένου ατόμου στο δίκτυο του οχήματος και την παρουσίαση του ως εξουσιοδοτημένου. Ο εισβολέας εκπέμπει ψευδή μηνύματα και έχει ως σκοπό τη λήψη λάθος αποφάσεων από τα συστήματα του CAV. Παράδειγμα αποτελεί το ατύχημα που θα συμβεί εάν το CAV πιστεύει, λόγω ψευδούς μηνύματος που έχει λάβει, πως δεν υπάρχει κάποιο εμπόδιο στην πορεία του ενώ υπάρχει. Ακόμη, οι εισβολείς μπορούν να κατευθύνουν πολλά αυτοκίνητα μαζί προς μία κατεύθυνση δημιουργώντας κυκλοφοριακή συμφόρηση.
- *Επιθέσεις επανάληψης:* Αυτές οι επιθέσεις συμβαίνουν όταν κάποιος κακόβουλος υποκλέπτει τα δεδομένα της επικοινωνίας του καναλιού, τα καταγράφει και τα αναμεταδίδει. Ενώ ο αποστολέας και ο παραλήπτης είναι πιστοποιημένοι δεν γνωρίζουν πως κάποιος έχει εισχωρήσει ανάμεσα τους και παρεμποδίζει τα μηνύματα. Αυτό αναπαριστάται στην Εικόνα 29.



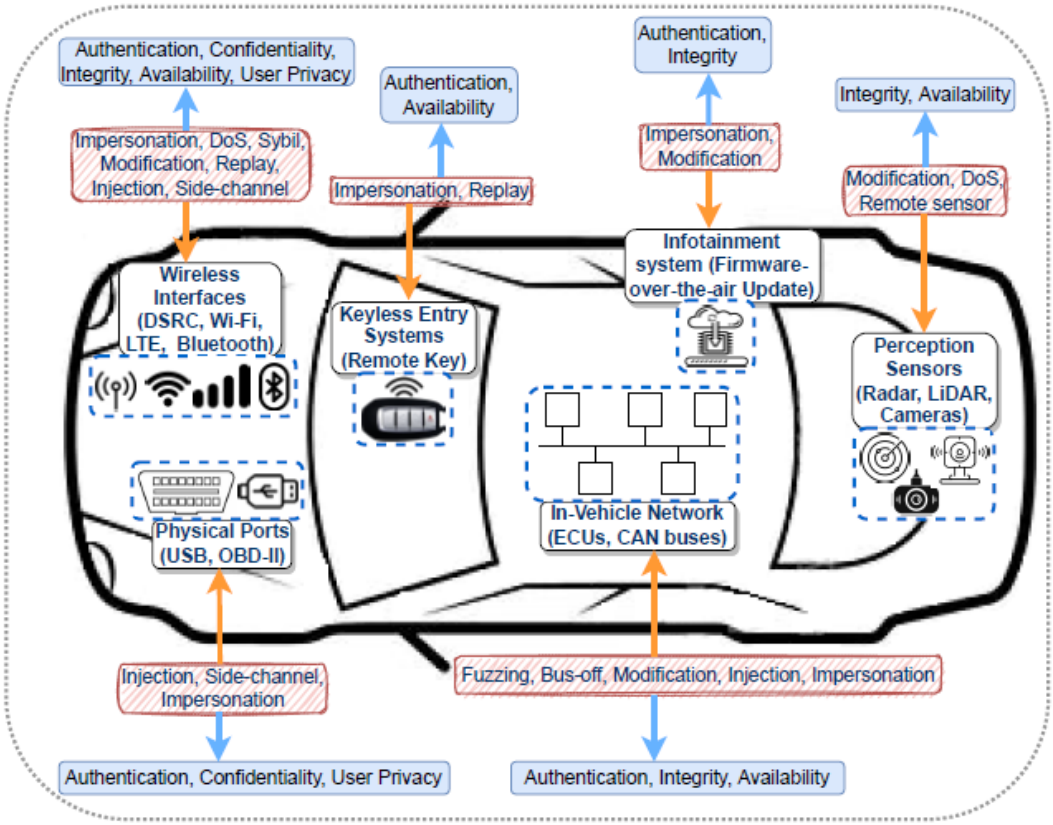
Εικόνα 29: Αναπαράσταση της επίθεσης επανάληψης
[https://en.wikipedia.org/wiki/Replay_attack]

- *Επιθέσεις Masquerade:* Στις επιθέσεις μεταμφίεσης κάποιος μη εξουσιοδοτημένος υποδύεται ένα νόμιμο κόμβο και αποκτά εξουσιοδοτημένη

πρόσβαση σε διάφορες πληροφορίες. Οι επιθέσεις αυτές διευκολύνονται από την έλλειψη ελέγχου της ταυτότητας των μηνυμάτων και την πλημμελή κρυπτογράφηση. Σε ένα περιβάλλον οχημάτων CAV το όχημα που έχει δεχθεί επίθεση προσποιείται ένα άλλο όχημα π.χ. ένα ασθενοφόρο για να παρακάμψει τους κανόνες κυκλοφορίας.

- *Τροποποίηση μηνυμάτων:* Σε επιθέσεις τροποποίησης μηνυμάτων οι κακόβουλοι εισάγουν ψευδή μηνύματα στο δίκτυο IVN μέσω της θύρας (On-Board Diagnostic) OBD-II ή άλλου συστήματος τηλεματικής. Το πρωτόκολλο CAN δεν διαθέτει κάποιο μηχανισμό ελέγχου ταυτότητας των μηνυμάτων και ως εκ τούτου μπορεί να δεχθεί επίθεση από κακόβουλους. Ακόμη η τροποποίηση μηνυμάτων περιλαμβάνει την καθυστέρηση ενός μηνύματος, την αναδιάταξη ή διαγραφή ορισμένων πακέτων του μηνύματος ή την εισαγωγή νέων. Παράδειγμα αποτελεί η καθυστέρηση του μηνύματος για έκτακτο φρενάρισμα το οποίο μπορεί να προκαλέσει σοβαρό ατύχημα.
- *Επίθεση άρνησης υπηρεσίας (DoS):* Στις επιθέσεις αυτές εισάγονται εικονικά μηνύματα με σκοπό την υπερφόρτωση του δικτύου. Έτσι, η αποτελεσματικότητα και η απόδοση του δικτύου μειώνονται. Υπάρχουν πολλά είδη επιθέσεων DoS. Αρχικά, οι επιτιθέμενοι μπορούν να αλλάξουν την προτεραιότητα του μηνύματος και να πάρουν τον έλεγχο του αυτοκινήτου. Επίσης, άλλες επιθέσεις επηρεάζουν το σύστημα ενημέρωσης και ψυχαγωγίας. Ακόμη υπάρχουν επιθέσεις που στοχεύουν στο δίαυλο CAN και έχουν ως σκοπό να επηρεάσουν τα κρίσιμα μέρη του οχήματος όπως το τιμόνι, το γκάζι, το φρένο. Τέλος, οι μονάδες ECU υπερφορτώνονται από τις επιθέσεις DoS και δεν μπορούν να ελέγξουν το όχημα σε πραγματικό χρόνο.

Τα διάφορα στοιχεία των οχημάτων CAV όπως το δίκτυο IVN, η είσοδος χωρίς κλειδί, το σύστημα ενημέρωσης και ψυχαγωγίας κ.α. μπορούν να γίνουν στόχοι κακόβουλων χρηστών. Αυτοί διενεργούν διάφορες επιθέσεις, όπως αυτές που αναφέρθηκαν παραπάνω, στο αυτόνομο σύστημα οδήγησης για την διακοπή της λειτουργίας του οχήματος και την απόκτηση του ελέγχου του CAV με σκοπό την υποκλοπή πληροφοριών. Το μοντέλο πιθανής επίθεσης σε οχήματα CAV παρουσιάζεται στην Εικόνα 30. (Masood M., Saeed Z. & Khan M. U., 2023; Limbasiya κ.α., 2022)



Εικόνα 30: Μοντέλο επίθεσης οχήματος CAV [13]

4.3 Επιθέσεις μέσω διαύλου CAN

Το Controller Area Network (CAN) είναι ένα απλό και ισχυρό πρωτόκολλο σειριακής επικοινωνίας που έχει σχεδιαστεί για την αυτοκινητοβιομηχανία και μπορεί να εφαρμοστεί με επιτυχία σε συστήματα πραγματικού χρόνου. Το πρωτόκολλο αυτό επιτρέπει την επικοινωνία μεταξύ διαφορετικών αισθητήρων και ενεργοποιητών. Γι' αυτό χρησιμοποιείται από τις μεγαλύτερες αυτοκινητοβιομηχανίες όπως η General Motors, η Volkswagen κ.α. Στα σύγχρονα οχήματα εκατοντάδες μονάδες ECU είναι ενσωματωμένες για τον έλεγχο των διάφορων λειτουργιών των οχημάτων. Αυτές οι μονάδες ECU συνδέονται και επικοινωνούν μέσω του διαύλου CAN.

Ο δίαυλος CAN κατέχει σημαντικό ρόλο στην αυτόνομη οδήγηση, διότι μέσω αυτού γίνεται ο έλεγχος, η διάγνωση και μεταφέρονται τα διαφορετικά σήματα μεταξύ των ECU. Ο δίαυλος CAN όντας ο κεντρικός δίαυλος εντός του οχήματος γίνεται στόχος των hackers. Παραβιάζοντας κανείς τον δίαυλο CAN μπορεί να αποκτήσει πρόσβαση στις ECU και να απειληθεί τόσο η ασφάλεια του οχήματος όσο και των επιβαινόντων. Οι επιθέσεις στον δίαυλο CAN ταυτίζονται με αυτές των οχημάτων CAV, όπως επιθέσεις

επανάληψης, επιθέσεις τροποποίησης των δεομένων κ.α., καθώς αυτό αποτελεί μέρος του αυτόνομου οχήματος. Ωστόσο υπάρχουν τρεις κύριες κατηγορίες επιθέσεων του διαύλου CAN:

1. *Επιθέσεις ECU:* Πολλοί ερευνητές μελετούν τις επιθέσεις στις μονάδες ECU. Οι Koscher et al. επικεντρώθηκαν στις προκλήσεις ασφαλείας που αντιμετωπίζει το δίκτυο CAN, όπως έλλειψη αυθεντικοποίησης, αδυναμία ελέγχου πρόσβασης και άρνηση υπηρεσίας. (DoS). Αυτοί πραγματοποίησαν επιθέσεις στο δίκτυο CAN χρησιμοποιώντας τεχνικές όπως sniffing, revenge-engineering, fuzzing κ.α. Η μέθοδος fuzzing αποδείχτηκε πολύ αποτελεσματική μέθοδος για την εύρεση ευπαθειών στο CAN. Με την διενέργεια των πειραμάτων αποδείχθηκε ότι κάποιος εισβολέας μπορεί να επηρεάσει κακόβουλα την ταχύτητα του οχήματος και να εμφανίσει πληροφορίες στον πίνακα οργάνων μέσω των παραβιασμένων μονάδων τηλεματικής. Αυτό αναπαρίσταται από την Εικόνα 31.

Εικόνα 31: Εμφάνιση αυθαίρετου μηνύματος και ψευδής ανάγνωση της ταχύτητας [8]

Η αυτοκινητοβιομηχανία Tesla είναι από τις πρώτες εταιρείες που κατασκευάζουν αυτόνομα οχήματα. Πολλοί ερευνητές ερευνούν τις ευπάθειες τέτοιων οχημάτων με σκοπό την αποτροπή επιθέσεων από διάφορους κακόβουλους. Η έρευνα των Nie et al. επικεντρώθηκε στις ευπάθειες ασφαλείας αυτών των οχημάτων.

Αυτοί απέδειξαν ότι οι μονάδες ECU μπορούν να ελεγχθούν εξ αποστάσεως μέσω της αποστολής πακέτων στο δίκτυο CAN αυτών των οχημάτων. Το πείραμα διεξήχθη σε νέα Tesla Model S που είχαν λάβει όλες τις αναβαθμίσεις λογισμικού. Οι ερευνητές διερευνώντας τις ευπάθειες του προγράμματος περιήγησης, επιτέθηκαν στο όχημα προσελκύοντας τους χρήστες μέσω του Wi-Fi hotspot. Αυτοί κατάφεραν να πλήξουν διάφορα συστήματα του οχήματος όπως ολοκληρωμένα κυκλώματα, πύλες αλλά και να στείλουν μολυσμένα μηνύματα στο δίκτυο CAN.

2. *Επιθέσεις IVN:* Οι επιθέσεις στο δίκτυο IVN απασχολούν πολύ την ερευνητική κοινότητα. Οι Miller & Valasek διεξήγαγαν μία εξαιρετική έρευνα σχετικά με την παραβίαση της ασφάλειας των οχημάτων. Μέσω της έρευνας αποδείχθηκε ότι οι μονάδες ECU μπορούν να επιτρέψουν την εξ αποστάσεως εκτέλεση κώδικα μέσω διεπαφών όπως το Bluetooth και οι συσκευές τηλεματικής. Η έρευνα πραγματοποιήθηκε σε συστήματα των οχημάτων Ford Escape και Toyota Prius. Οι επιθέσεις πραγματοποιήθηκαν μέσω της θύρας OBD-II. Η επίθεση στο Toyota Prius πραγματοποιήθηκε στέλνοντας ένα αποκλειστικό μήνυμα στην ECU. Το μήνυμα περιείχε ένα άθροισμα ελέγχου μηνύματος στα τελευταία bits των δεδομένων κάτι που συμβαίνει μόνο στα σημαντικά μηνύματα του δικτύου CAN. Στο όχημα της Ford ο κινητήρας έχει μια δικλίδα μη λειτουργίας σε περίπτωση έκχυσης πολύ λίγου ή πάρα πολύ μείγματος βενζίνης ή αέρα. Ο κωδικός ελέγχου αυτού είναι το 4044. Οι ερευνητές στην επίθεση τους απέστειλαν το ακόλουθο πακέτο:

   [IDH: 07, IDL: E0, Len: 08, Data: 05 31 01 40 44 FF 00 00]

   Κάθε παράμετρος του απεικονίζεται από bits. Λόγω της υπερφόρτωσης του δικτύου CAN από πακέτα η υπηρεσία απορρίφθηκε παρόλο που δεν θα έπρεπε. Αυτό φαίνεται και στην Εικόνα 32.

   Στην έρευνα τους οι Lie et al. επιτέθηκαν στο σύστημα ψυχαγωγίας και ενημέρωσης ενός οχήματος. Το σύστημα ψυχαγωγίας και ενημέρωσης γίνεται στόχος επιθέσεων, διότι μπορεί να ελέγξει τον δίαυλο CAN και τις μονάδες ECU. Για την διενέργεια της επίθεσης χρησιμοποιήθηκαν οι τεχνικές της αντίστροφης ECU και της επίθεσης μέσω side-channel. Η μέθοδος επίθεσης side-channel χρησιμοποιήθηκε για τον καθορισμό του κλειδιού χρησιμοποιώντας σήματα που διέρρευσαν από την διαδικασία κρυπτογράφησης ή μέσω μιας επίθεσης επανάληψης. Αυτό επιτεύχθηκε μέσω της ανάλυσης των πακέτων του δικτύου CAN του αυτόνομου οχήματος.

Εικόνα 32: Απεικόνιση οργάνων οχήματος και λανθασμένη ένδειξη χαμηλής στάθμης βενζίνης [8]

3. *Επιθέσεις σχετικά με το κλειδί του αυτοκινήτου:* Πλήθος ερευνητικών εργασιών έχουν ως θέμα τις επιθέσεις αυτές. Οι Francillon et al. στην έρευνα τους επιτέθηκαν στα συστήματα παθητικής εισόδου και εκκίνησης χωρίς κλειδί (PKES), τα οποία βρίσκουν ευρεία εφαρμογή στα σύγχρονα αυτοκίνητα. Αυτοί χρησιμοποίησαν ως μέθοδο επίθεσης την επανάληψη αντιγράφοντας το υπάρχον σήμα. Απέδειξαν ότι μπορούν να γίνουν επιθέσεις εξ αποστάσεως μέσω πομποδέκτη. Ακόμη οι ερευνητές έκαναν μία κατάταξη σχετικά με τον κίνδυνο τέτοιων επιθέσεων σε δέκα μοντέλα οχημάτων από οκτώ κατασκευαστές.

   Οι Garcia et al. στην έρευνα τους περιγράφουν τις ευπάθειες του immobilizer κλειδιού που χρησιμοποιείται από τις εταιρείες κατασκευής οχημάτων. Αρχικά αυτοί βρήκαν τους αλγόριθμους κωδικοποίησης και το κοινό κλειδί κωδικοποίησης μεταξύ του immobilizer και του οχήματος. Στη συνέχεια οι ερευνητές χρησιμοποίησαν ένα τηλεχειριστήριο της αυτοκινητοβιομηχανίας Volkswagen αξιοποιώντας το ανακληθέν κλειδί κρυπτογράφησης. Τότε το σήμα που στάλθηκε από το όχημα υποκλάπηκε με σκοπό την αυθαίρετη πρόσβαση στο όχημα. Μέσω της επίθεσης αποδείχθηκε ότι μπορεί να ανακτηθεί το κλειδί της κρυπτογράφησης και

να αναπαραχθεί από τηλεχειριστήριο με τέσσερεις έως οκτώ κυλιόμενους κωδικούς και σύντομο χρόνο υπολογισμού.

Τα αποτελέσματα των προαναφερθέντων ερευνών επηρεάζουν εκατομμύρια οχήματα καθώς και τους χειριστές τους. Γι' αυτό οι αυτοκινητοβιομηχανίες έχουν προβεί σε αντίμετρα για τέτοιου είδους επιθέσεις. Ωστόσο ακόμα υπάρχουν ευπάθειες στα συστήματα οι οποίες ερευνώνται, ώστε να μην τύχουν εκμετάλλευσης από κακόβουλους. (Masood M., Saeed Z. & Khan M. U., 2023; Kim κ.α., 2021)

4.4 Τρόποι προστασίας κακόβουλων επιθέσεων

Τα οχήματα CAV αποτελούνται από πολλές διαφορετικές τεχνολογίες με τις οποίες πρέπει να επικοινωνούν. Αυτό τα καθιστά ευάλωτα σε κακόβουλες επιθέσεις. Σύμφωνα με έρευνα το 2019 μόνο το 38% των επιθέσεων ήταν για ερευνητικούς σκοπούς. Το 57% των επιθέσεων πραγματοποιήθηκαν από κακόβουλους με σκοπό να πλήξουν το όχημα και να υποκλέψουν τις προσωπικές πληροφορίες των χρηστών του. Για την αντιμετώπιση των επιθέσεων αλλά και για την καλύτερη θωράκιση των οχημάτων παρουσιάζονται ορισμένα αντίμετρα.

1. *Κρυπτογράφηση:* Μία λύση αποτελεί η κρυπτογράφηση των μηνυμάτων. Είναι πολύ σημαντικό να έχουν πρόσβαση στα μηνύματα μόνο οι νόμιμοι χρήστες. Αυτό επιτυγχάνεται με ένα καλό σύστημα κρυπτογράφησης – αποκρυπτογράφησης. Μέσω της κρυπτογράφησης προστατεύονται τα μηνύματα και η επικοινωνία γίνεται πιο ασφαλής. Αυτή η μέθοδος είναι καίριο μέρος των σύγχρονων οχημάτων διασφαλίζοντας την ασφάλεια και την ακεραιότητα των δεδομένων. Άρα, η επικοινωνία πρέπει να είναι επαρκώς κρυπτογραφημένη και η διεύθυνση IP των τηλεματικών συσκευών να μην αποκαλύπτεται σε εξωτερικές συσκευές.
2. *Εγκατάσταση πυλών:* Οι πύλες (gateways) είναι αναπόσπαστο μέρος των δικτύων επικοινωνίας των οχημάτων. Αυτό συμβαίνει, διότι οι ECU επικοινωνούν μεταξύ τους μέσω πυλών. Οι πύλες λειτουργούν ως μεταφραστές μεταξύ των κόμβων που χρησιμοποιούν διαφορετικά πρωτόκολλα και των διάφορων μορφών data frame. Παράδειγμα αποτελεί όταν μία χαμηλής ταχύτητας ECU θέλει να στείλει μήνυμα σε μία ECU υψηλής ταχύτητας. Τότε οι πύλες προσαρμόζουν το baud rate με σκοπό την συμβατότητα μεταξύ του αποστολέα και του παραλήπτη. Πα-

ρόλο που οι πύλες χρησιμοποιούνται αρκετά χρόνια στα δίκτυα οχημάτων οι σύγχρονες πύλες είναι αρκετά πολύπλοκες λόγω των αυξημένων μονάδων ECU των οχημάτων.

3. *Απομόνωση απειλών:* Η διασύνδεση του εσωτερικού δικτύου των οχημάτων με τον εξωτερικό κόσμο είναι ένα σύνηθες σημείο επίθεσης. Η θύρα OBD και το σύστημα τηλεματικής αποτελούν τις διεπαφές σύνδεσης του CAV με τις εξωτερικές συσκευές. Η θύρα OBD χρησιμοποιείται για διαγνωστικούς σκοπούς. Από την άλλη το σύστημα τηλεματικής συλλέγει πληροφορίες για την τοποθεσία του οχήματος, την δραστηριότητα του οδηγού κ.α. τις οποίες στέλνει στους διακομιστές χρησιμοποιώντας το δίκτυο κινητής τηλεφωνίας. Η απομόνωση της θύρας OBD από το εσωτερικό δίκτυο είναι δύσκολη καθώς χρησιμοποιείται για τον εντοπισμό των βλαβών του οχήματος αλλά και για την ενημέρωση του υλικολογισμικού. Εγκαθιστώντας έναν ανιχνευτή σε αυτήν τη θύρα θα εντοπιστεί εάν γίνει προσπάθεια αποστολής μολυσμένων δεδομένων προς το εσωτερικό δίκτυο του οχήματος κατά την διαδικασία εύρεσης βλαβών.
4. *Σύστημα ανίχνευσης εισβολής:* Το σύστημα Intrusion Detection System (IDS) έχει σχεδιαστεί για το δίκτυο CAN. Αυτό χρησιμοποιεί τις γνωστές επιθέσεις όπως η επίθεση DoS για να αναγνωρίσει τυχόν επιθέσεις στο όχημα. Όμως με τη χρήση αυτού του συστήματος αυξάνεται πολύ η πολυπλοκότητα. Άλλες τεχνικές για τον ίδιο σκοπό είναι η βαθιά μάθηση, τα συστήματα ανίχνευσης ανωμαλιών κ.α. Επομένως, οι σχεδιαστές των αυτόνομων οχημάτων πρέπει να τοποθετήσουν συστήματα προστασίας από εισβολές στα δίκτυα οχημάτων με σκοπό τον εντοπισμό των εισβολέων και την αναφορά τους. Στον Πίνακας 2 παρουσιάζονται οι διάφορες μορφές επιθέσεων καθώς και προτεινόμενα αντίμετρα.

Εκτός από τα προαναφερθέντα αντίμετρα υπάρχουν και προτάσεις διάφορων επιστημόνων. Οι Argawal et al. πρότειναν μια αρχιτεκτονική ασφαλούς επικοινωνίας μεταξύ των μονάδων ECU σε διαφορετικά κανάλια μέσω μονάδων που συμπεριφέρονται ως πύλες. Πρότειναν ένα ασφαλές σύστημα επικοινωνίας για το δίκτυο CAN με ευέλικτο ρυθμό δεδομένων. Αυτοί ισχυρίζονται πως το σύστημα κρυπτογράφησης που προτείνουν παρέχει καλύτερη απόδοση από την απλή κρυπτογράφηση και τον έλεγχο ταυτότητας.

Οι Olufowobi et al. προτείνουν έναν αλγόριθμο για τον εντοπισμό και την διόρθωση μηνυμάτων που πλαστογραφήθηκαν από τους εισβολείς μέσω του δικτύου CAN. Σύμφωνα με την έρευνα τους η διαδικασία ανάκτησης της κατεστραμμένης ECU γίνεται εξ

αποστάσεως. Αυτοί πρότειναν ένα σύστημα IDS το οποίο απενεργοποιεί το μη φυσιολογικό κόμβο στο δίαυλο αποκαθιστώντας την επικοινωνία. Αυτό επιτεύχθηκε ορίζοντας ένα όριο κατωφλίου 6ms αντί του κανονικού πλαισίου μηνύματος.

Οι Song et al. πρότειναν ένα σύστημα IDS βασισμένο σε βαθύ συνελικτικό νευρονικό δίκτυο για την προστασία του διαύλου CAN. Κατά την διάρκεια της έρευνας οι ερευνητές συνέκριναν αλγορίθμους μηχανικής μάθησης (όπως δέντρο αποφάσεων, αφελή ταξινόμηση Bayes, κ-πλησιέστεροι γείτονες, τεχνητά νευρωνικά δίκτυα κ.α.) για επιθέσεις DoS, RPM spoofing, fuzzy attack. Οι ερευνητές πειραματίστηκαν με αποστολή τεσσάρων κατηγοριών μολυσμένων μηνυμάτων στο σύστημα IDS που κατασκεύασαν. (Kim κ.α., 2021; Masood M., Saeed Z. & Khan M. U., 2023)

Πίνακας 2: Μορφές επιθέσεων και προτεινόμενα αντίμετρα [14]

Type of attack	**Proposed Countermeasure**
Eavesdropping	Authentication, Encryption, Cryptography
Traffic Analysis	Intrusion Detection System (IDS), Encryption
Spoofing	Authentication, IDS
Replay Attacks	Gateway installation, Encryption
Masquerades	Authentication, Gateways, Encryption
Message Modification	Authentications, Encryption
Denial-of-Service Attack	Gateways installation, IDS, Encryption, Authentication.

5 Κατηγοριοποίηση επιθέσεων και λύσεων σε συστήματα (VANET)

Το Vehicular Ad-hoc Network (VANET) είναι ένας τύπος δικτύου που δημιουργήθηκε χρησιμοποιώντας τις αρχές των Mobile Ad-hoc Networks (MANETs), έχοντας μία πλήρως αυτό-οργανωμένη διαμόρφωση. Το δίκτυο αυτό έγινε γνωστό το 2001 στις εφαρμογές ad-hoc κινητής επικοινωνίας και δικτύωσης car-to-car, δημιουργώντας δίκτυα με σκοπό την ανταλλαγή πληροφοριών μεταξύ των οχημάτων. Γνωστές εφαρμογές του δικτύου VANET αποτελούν η αποτελεσματική διαχείριση της κυκλοφορίας, η παρακολούθηση της οδικής συμπεριφοράς και η προσφορά ασφάλειας και άνεσης στους οδηγούς. Τα VANET αναφέρονται ως έξυπνα δίκτυα μεταφορών (ITS) και αποτελούν τον προπομπό του διαδικτύου των οχημάτων (IoV). Παρόλο που κατά την δημιουργία του, το δίκτυο VANET θεωρήθηκε μία απλή εφαρμογή των αρχών των MANET, σήμερα αποτελεί έναν ξεχωριστό ερευνητικό τομέα έχοντας γίνει συνώνυμο με τον όρο της επικοινωνίας μεταξύ των οχημάτων (IVC). (C.K. Toh, 2008; Manar Abu Talib κ.α., 2018)

5.1 Είδη επιθέσεων

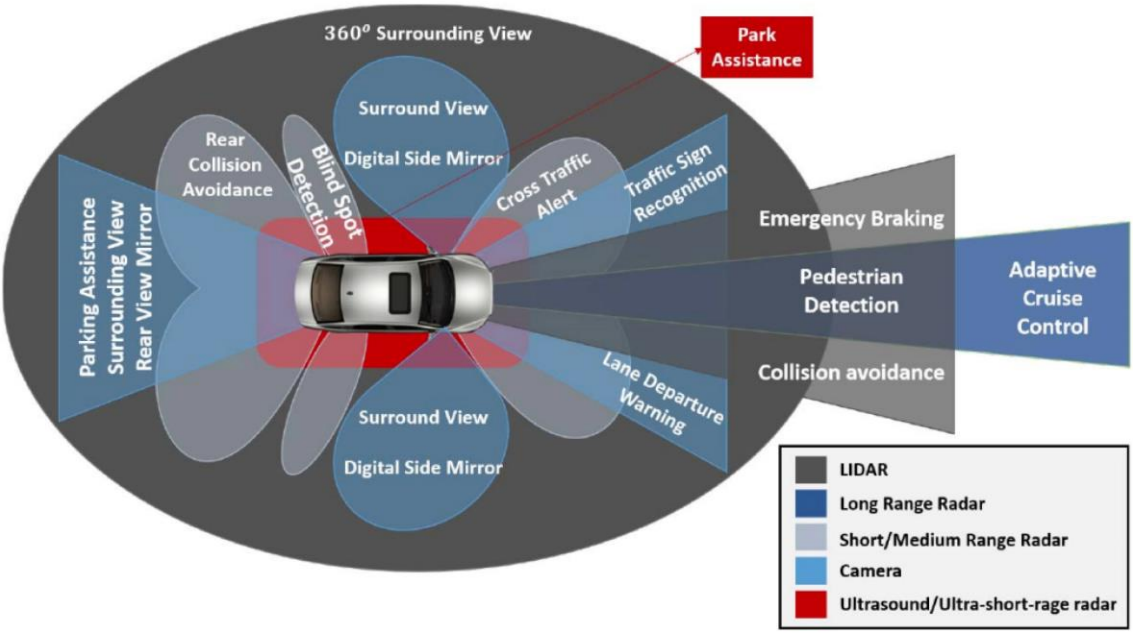
Τα δίκτυα VANET χρησιμοποιούν πληθώρα νέων τεχνολογιών καθώς και διάφορους τρόπους επικοινωνίας μεταξύ των οχημάτων γεγονός που δημιουργεί ευπάθειες τις οποίες μπορούν να εκμεταλλευτούν διάφοροι κακόβουλοι. Τρεις κύριες κατηγορίες επιθέσεων είναι:

1. *Επιθέσεις στο δίκτυο οχημάτων (VANET):* Όταν ένα όχημα ή μία υποδομή συνδέεται στο δίκτυο VANET επιτρέπεται η μεταξύ τους επικοινωνία προσφέροντας τους πολλές δυνατότητες. Τέτοιες είναι οι πληροφορίες σχετικά με την κίνηση, την κατάσταση του δρόμου καθώς και τη θέση των οχημάτων και των πεζών με σκοπό την αποφυγή των ατυχημάτων και της κυκλοφοριακής συμφόρησης. Εφόσον στο δίκτυο VANET δεν παρέχεται κεντρική διαχείριση, διάφορα πρωτόκολλα ασφαλείας τα οποία απαιτούν κεντρικό trusted third party (TTP) ή απαιτούν διαρκή συνδεσιμότητα όπως η υποδομή δημοσίου κλειδιού (PKI) δεν μπορούν να χρησιμοποιηθούν δημιουργώντας ευπάθειες.

Η ασφάλεια του δικτύου μπορεί να γίνει στόχος επιθέσεων όπως οι επιθέσεις κωδικού πρόσβασης ή οι επιθέσεις κλειδιού. Μία άλλη επίθεση είναι η υποκλοπή δεδομένων κατά την διάρκεια της ασύρματης σύνδεσης, μέσω της οποίας δίνεται πρόσβαση στους εισβολείς στα ιδιωτικά δεδομένα του οχήματος όπως είναι η τοποθεσία. Άλλη μια επίθεση είναι η επίθεση Sybil όπου ένα κακόβουλο όχημα εκπέμπει διάφορα μηνύματα χρησιμοποιώντας πλαστά διαπιστευτήρια. Άλλες επιθέσεις στις οποίες είναι ευάλωτο το δίκτυο VANET είναι οι επιθέσεις black-hole, οι επιθέσεις wormhole και οι επιθέσεις DoS τόσο σε μεμονωμένα οχήματα όσο και σε ομάδες οχημάτων. Επιπλέον καθώς οι ασύρματες επικοινωνίες γίνονται με την χρήση των πρωτοκόλλων Wi-Fi, Bluetooth, GSM, τα οχήματα μπορεί να γίνουν στόχοι επιθέσεων λόγω των ευπαθειών των πρωτοκόλλων.

2. *Επιθέσεις στους αισθητήρες:* Τα οχήματα και κυρίως τα αυτόνομα οχήματα εξοπλίζονται με πληθώρα αισθητήρων οι οποίοι είναι υπεύθυνοι για διάφορες διεργασίες. Τέτοιες είναι ο έλεγχος της απόστασης μεταξύ των οχημάτων, οι οδικές συνθήκες, η ανίχνευση καπνού ή φωτιάς, το σύστημα επιτάχυνσης – επιβράδυνσης του οχήματος καθώς και η ανίχνευση εμποδίων. Οι αισθητήρες αποτελούν σημαντικό στοιχείο των αυτόνομων οχημάτων καθώς παρέχουν πληροφορίες με σκοπό την ασφαλή οδήγηση. Επίθεση σε αυτούς συνεπάγεται αλλοίωση των δεδομένων γεγονός που μπορεί να οδηγήσει στην πρόκληση ατυχημάτων και στον τραυματισμό των επιβαινόντων στο όχημα. Παράδειγμα αποτελεί η απενεργοποίηση του συστήματος πέδησης ή του τιμονιού ενός αυτόνομου οχήματος από κάποιον κακόβουλο. Άλλες μορφές επιθέσεων στους αισθητήρες είναι:
    - οι επιθέσεις Jamming στον αισθητήρα Lidar
    - οι επιθέσεις αλλοίωσης της ποιότητας της κάμερας
    - οι επιθέσεις Spoofing στο σήμα του GPS ή του Lidar κ.α.

    Όλες αυτές οι επιθέσεις επηρεάζουν άμεσα την λειτουργία του οχήματος καθώς τα δεδομένα που παρέχονται σε αυτό έχουν αλλοιωθεί και οι αποφάσεις που λαμβάνει θα είναι λανθασμένες. Στην Εικόνα 33 απεικονίζονται διάφοροι αισθητήρες των αυτόνομων οχημάτων οι οποίοι μπορούν να αποτελέσουν στόχο επίθεσης, καθώς και η θέση τους στο όχημα και η εμβέλεια τους.



Εικόνα 33: Αισθητήρες αυτόνομου οχήματος, θέση και εμβέλεια τους [10]

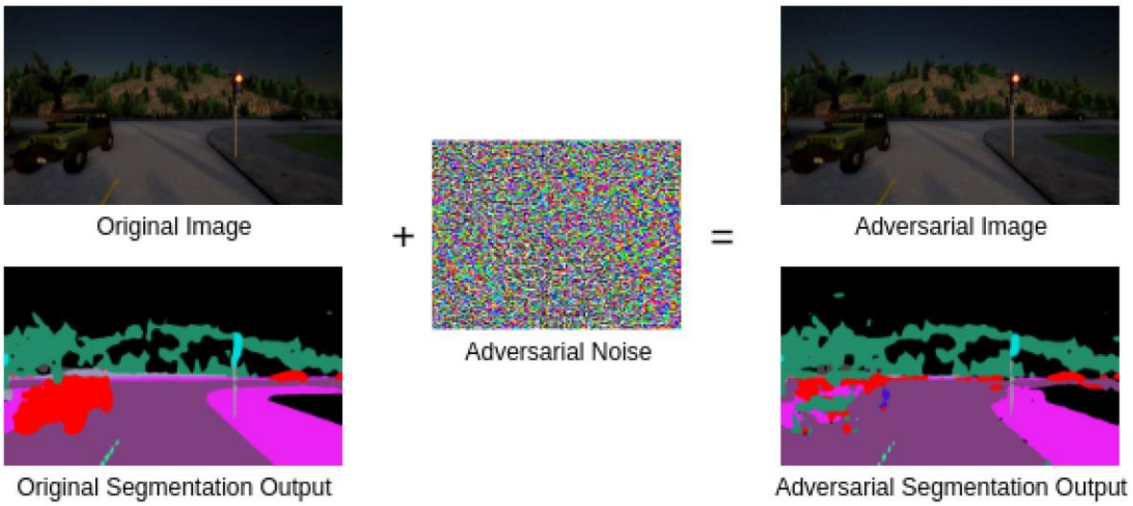
3. *Επίθεση στο Hardware:* Εκτός από τις επιθέσεις που διεξάγονται από κακόβουλους οι οποίοι βρίσκονται μακριά από το όχημα και αποσκοπούν στην αλλοίωση των δεδομένων των αισθητήρων ή στην υποκλοπή των δεδομένων, υπάρχουν και επιθέσεις που διεξάγονται από άτομα που έχουν πρόσβαση στο όχημα. Τέτοιοι είναι οι μηχανικοί που επισκευάζουν τα οχήματα. Αυτοί αποκτώντας πρόσβαση στο υλικό των αυτόνομων οχημάτων μπορεί να εκμεταλλευτούν τα δεδομένα των αισθητήρων και να προκαλέσουν βλάβη στα συστήματα επικοινωνίας. Αυτοί μπορούν ακόμη να εισάγουν ιούς ή κακόβουλο λογισμικό στο framework του οχήματος. Αυτό μπορεί να συμβεί ενημερώνοντας το firmware της μονάδας ECU με προσαρμοσμένες βιβλιοθήκες που έχουν ως σκοπό την πρόκληση των κακόβουλων λειτουργιών στο όχημα. (Manar Abu Talib κ.α., 2018; Kloukiniotis κ.α., 2022)

5.2 Επιθέσεις Adversarial Attack σε αυτόνομα οχήματα

Μία επιπλέον σημαντική μορφή επιθέσεων στα αυτόνομα οχήματα είναι οι επιθέσεις Adversarial Attack. Οι επιθέσεις αυτές περιλαμβάνουν μικρές διαταραχές οι οποίες δεν γίνονται αντιληπτές από το ανθρώπινο μάτι αλλά μολύνουν τις εικόνες που καταγράφει το όχημα με σκοπό την πρόκληση λάθος αποφάσεων. Αυτό συμβαίνει διότι οι μολυσμένες εικόνες παραπλανούν τα μοντέλα βαθιάς μάθησης, τα οποία χρησιμοποιούν τις εικόνες

που συλλέγονται από τους αισθητήρες του οχήματος ώστε να λάβουν τις απαραίτητες αποφάσεις. Υπάρχουν δύο τύποι τέτοιων επιθέσεων. Αυτές είναι οι evasion και poisoning attacks.

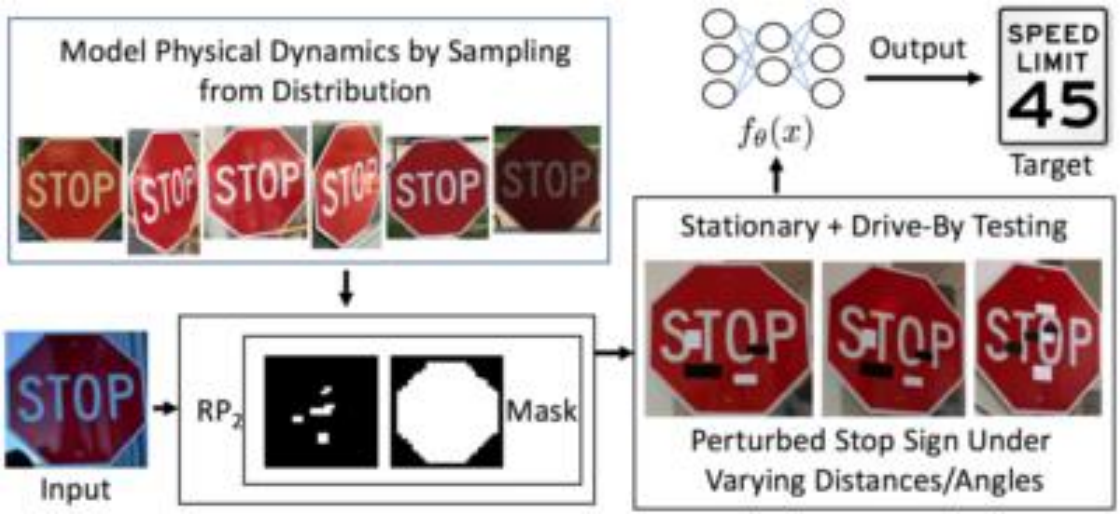
Στις επιθέσεις evasion παραποιούνται τα δεδομένα ελέγχου με σκοπό την εσφαλμένη ταξινόμηση τους. Οι επιθέσεις αυτές πραγματοποιούνται στο μοντέλο της μηχανικής μάθησης κατά την διάρκεια της εξαγωγής των συμπερασμάτων. Κατά την επίθεση σχεδιάζονται δεδομένα εισόδου με συγκεκριμένες ιδιότητες μη αντιληπτές από τον άνθρωπο οι οποίες μπορούν να χειραγωγήσουν το μοντέλο στόχου με αποτέλεσμα να παραχθούν λανθασμένες αποφάσεις. Στις επιθέσεις poisoning παραποιούνται τα δεδομένα εκπαίδευσης με σκοπό να επηρεαστεί το επίπεδο αντίληψης του μοντέλου και να προκληθεί άρνηση εξυπηρέτησης. Κάποιοι τρόποι χειραγώγησης του μοντέλου στόχου είναι η καταστροφή της λογικής του, ο χειρισμός και η μόλυνση των δεδομένων του κ.α. Ένα χαρακτηριστικό παράδειγμα επιθέσεων Adversarial Attack απεικονίζεται στην Εικόνα 34 η οποία δείχνει την εξαφάνιση ενός μέρος του οχήματος από τον αισθητήρα της κάμερας μετά από επίθεση.



Εικόνα 34: Προσομοίωση επίθεσης Adversarial Attack [10]

Οι κακόβουλοι για να πετύχουν όσο το δυνατόν περισσότερο επιτυχημένες επιθέσεις, εκμεταλλεύονται τα τρωτά σημεία των αυτόνομων οχημάτων. Ένα από τα τρωτά σημεία είναι οι αισθητήρες. Αυτοί μπορεί να δεχθούν επίθεση επηρεάζοντας τα δεδομένα που αυτοί συλλέγουν. Αυτό μπορεί να επιτευχθεί μέσω της προσθήκης κάποιων αυτοκόλλητων (stickers) τόσο στο όχημα, όσο και σε ένα σήμα κυκλοφορίας ή σε ένα κάδο απορριμμάτων. Με την χρήση των αυτοκόλλητων οι αλγόριθμοι της βαθιάς μάθησης είναι

πολύ πιθανό να μπερδευτούν και να ταξινομήσουν ένα αντικείμενο λάθος. Πολλοί ερευνητές ασχολούνται με το συγκεκριμένο αντικείμενο και διεξάγουν πειράματα με σκοπό να βρουν λύσεις σε αυτές τις ευπάθειες. Οι Szegedy et al. μελετώντας τις ιδιότητες των νευρωνικών δικτύων και εφαρμόζοντας τις κατάλληλες διαταραχές κατάφεραν να ταξινομηθεί μία εικόνα εσφαλμένα από το δίκτυο. Οι Eykholt et al. με την χρήση sticker στο σήμα κυκλοφορίας stop παραπλάνησαν τον αλγόριθμο μάθησης κάνοντας τον να το αντιληφθεί ως σήμα που περιορίζει την ταχύτητα. Αυτό φαίνεται στην Εικόνα 35.



Εικόνα 35: Αποτέλεσμα παραπλάνησης του αλγορίθμου μάθησης [4]

Ένα άλλο τρωτό σημείο είναι οι αλγόριθμοι που χρησιμοποιούνται για την επεξεργασία των δεδομένων. Αυτό μπορεί να συμβεί όταν ένας μηχανικός που επισκευάζει το όχημα εγκαταστήσει κάποιο κακόβουλο λογισμικό. Για να είναι επιτυχημένες οι επιθέσεις οι αντίπαλοι χρειάζεται να γνωρίζουν ορισμένες παραμέτρους του δικτύου ή της αρχιτεκτονικής του μοντέλου μάθησης. Ανάλογα με τις γνώσεις που μπορεί να γνωρίζει ο αντίπαλος έχουν δημιουργηθεί τρία μοντέλα απειλών.

1. *Μοντέλο Μαύρου Κουτιού (Black Box):* Στο μοντέλο αυτό ο αντίπαλος δεν γνωρίζει την δομή και τις παραμέτρους του στόχου. Το μόνο που μπορεί να κάνει είναι να στείλει δεδομένα εισόδου στο δίκτυο και να αναλύσει την έξοδο του μοντέλου με σκοπό να βρει τυχόν ευπάθειες.
2. *Μοντέλο Γκρίζου Κουτιού (Grey Box):* Στο μοντέλο αυτό ο αντίπαλος γνωρίζει όλη την αρχιτεκτονική του μοντέλου αλλά δεν γνωρίζει τα καθορισμένα βάρη ή τις παραμέτρους του δικτύου. Επιθέσεις σε αυτό το μοντέλο έχουν μεγαλύτερο ποσοστό επιτυχίας από όσο στο μοντέλο μαύρου κουτιού, λόγω των περισσότερων διαθέσιμων πληροφοριών.

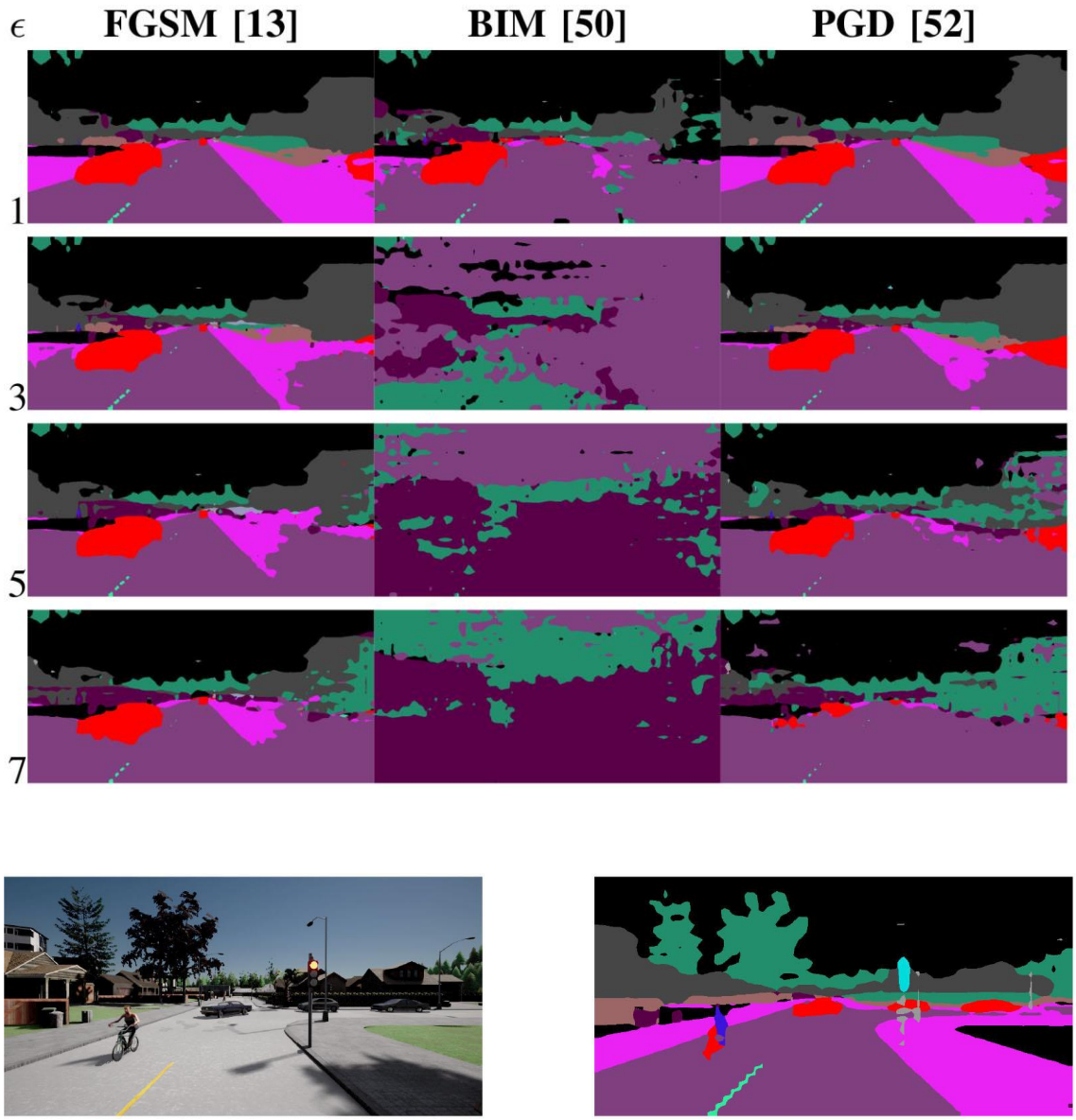
3. *Μοντέλο Λευκού Κουτιού (White Box):* Στο μοντέλο αυτό ο αντίπαλος γνωρίζει τόσο τις παραμέτρους του δικτύου όσο και την αρχιτεκτονική του μοντέλου. Επιπλέον αυτός γνωρίζει τα δεδομένα εκπαίδευσης και ό,τι σχετίζεται με αυτά. Λόγω αυτών ο αντίπαλος εντοπίζει τα τρωτά σημεία του μοντέλου και πραγματοποιεί επιτυχημένες επιθέσεις.

Με σκοπό την οπτικοποίηση των επιδράσεων των επιθέσεων Adversarial Attack στα αυτόνομα οχήματα οι Koumiotis et al. εκπαίδευσαν το δίκτυο τμηματοποίησης (segmentation) Deeplabv3 χρησιμοποιώντας κάποιο δικό τους σύνολο δεδομένων εκπαίδευσης και ελέγχου. Τα δεδομένα τους αφού πέρασαν από το Deeplabv3 εκτέθηκαν σε διάφορες επιθέσεις όπως Fast Gradient Sign Method (FGSM), Basic Iterative Method (BIM), Projected Gradient Descent (PGM). Όπως φαίνεται και από τους πίνακες που ακολουθούν η ακρίβεια των μοντέλων τμηματοποίησης επηρεάζεται καθώς αυξάνεται το μέγεθος της επίθεσης, ιδιαίτερα στην περίπτωση του BIM. Η Εικόνα 36 και η Εικόνα 37 απεικονίζουν δύο αρχικές εικόνες από το σύνολο δεδομένων πριν και μετά την τμηματοποίηση του Deeplabv3. Ο Πίνακας 3 και ο Πίνακας 4 απεικονίζουν τα επίπεδα διαταραχής κατά την διάρκεια των Adversarial Attack.

Μέσω αυτού του παραδείγματος γίνεται αντιληπτό ότι οι παρούσες τεχνικές βαθιάς μάθησης μπορούν εύκολα να γίνουν στόχοι επιθέσεων. Αυτό πρέπει μέσω της έρευνας να αλλάξει ώστε να παρέχεται ακόμη περισσότερη ασφάλεια και αυθεντικότητα κατά των επιθέσεων στα αυτόνομα οχήματα αλλά και στους χρήστες τους. (Eykholt κ.α., 2018; Kloukiniotis κ.α., 2022; Amirkhani κ.α., 2022)

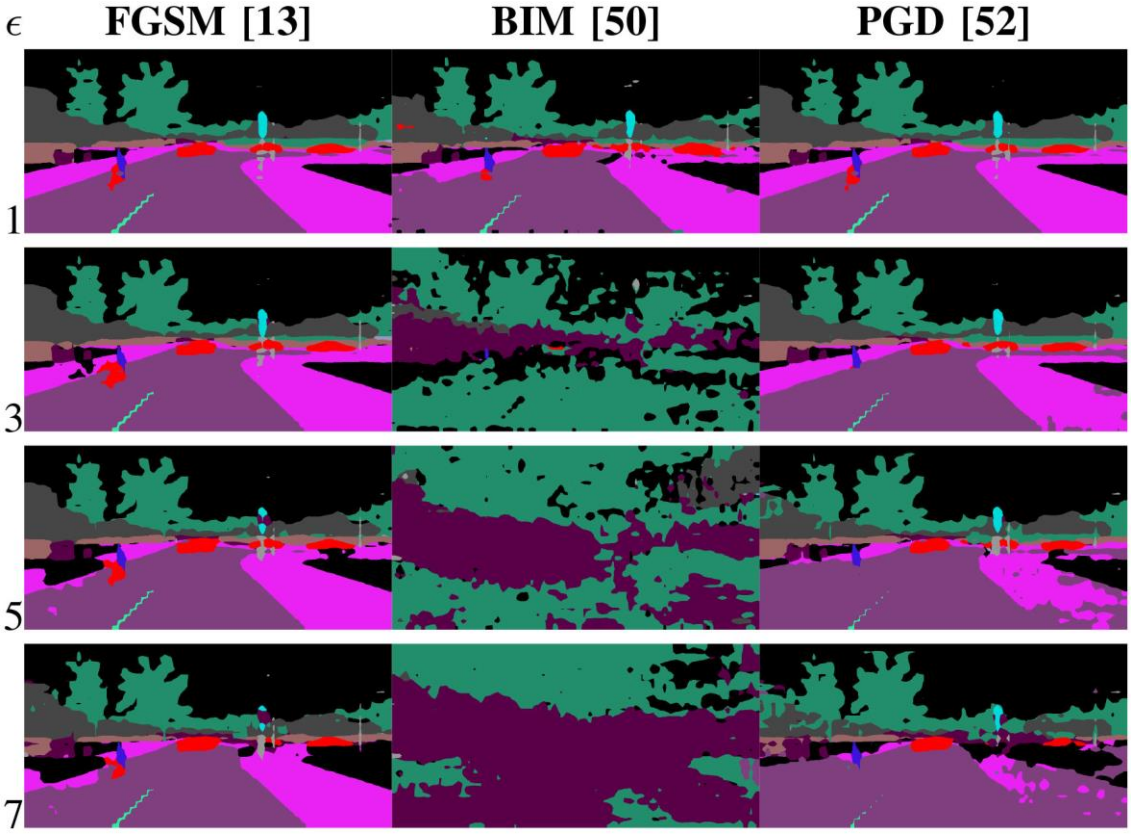
Εικόνα 36: Αρχική εικόνα και τμηματοποίηση της με την χρήση του Deeplabv3 [10]

Πίνακας 3: Αποτέλεσμα επιθέσεων Adversarial Attack Εικόνας 36 [10]



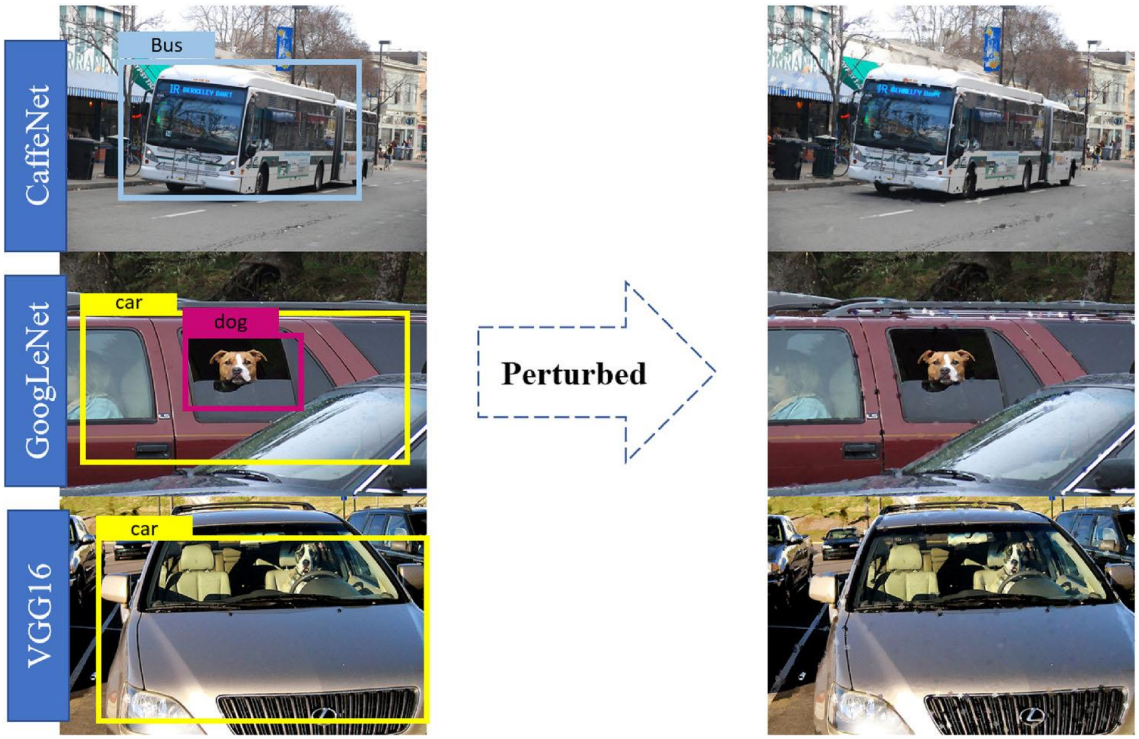
Εικόνα 37: Αρχική εικόνα και τμηματοποίηση της με την χρήση του Deeplabv3 [10]

Πίνακας 4: Αποτέλεσμα επιθέσεων Adversarial Attack Εικόνας 37 [10]



5.3 Τύποι επιθέσεων στην ανίχνευση αντικειμένων

Η ανίχνευση αντικειμένων είναι μία από τις πιο σημαντικές εφαρμογές βαθιάς μάθησης. Οι τεχνικές ανίχνευσης αντικειμένων γίνονται συχνά στόχοι επιθέσεων Adversarial Attack χάνοντας έτσι την αξιοπιστία και την αποτελεσματικότητα τους. Δύο κύριες μορφές επιθέσεων Adversarial Attack που έχουν ως σκοπό την παραπλάνηση των τεχνικών της μηχανικής μάθησης είναι οι στοχευμένες και οι μη στοχευμένες επιθέσεις. Οι μη στοχευμένες επιθέσεις θέλουν να εξαπατήσουν ένα μοντέλο ανίχνευσης αντικειμένων και δεν δίνουν σημασία στην τελική ετικέτα ή στις παραπλανητικές ετικέτες. Σε αυτές τις επιθέσεις τα αντικείμενα λαμβάνουν λανθασμένες ετικέτες. Από την άλλη οι στοχευμένες επιθέσεις έχουν ως στόχο την εξαπάτηση του μοντέλου ώστε να ορίζει συγκεκριμένες ετικέτες στα αντικείμενα. Αυτές οι επιθέσεις πραγματοποιούνται για μία συγκεκριμένη κατηγορία αντικειμένων. Παράδειγμα αποτελεί η Εικόνα 38 στην οποία απεικονίζονται παραδείγματα καθαρών εικόνων στις οποίες μπορεί να γίνει ανίχνευση αντικειμένων και παραδείγματα διαταραγμένων εικόνων που κανένα από τα τρία δίκτυα δεν μπορεί να ανιχνεύσει τα αντικείμενα. Ακόμη στην ανίχνευση αντικειμένων πραγματοποιούνται και επιθέσεις μαύρου και λευκού κουτιού.



Εικόνα 38: Καθαρές εικόνες και εικόνες με διαταραχή στις οποίες δεν μπορεί να γίνει ανίχνευση αντικειμένων [3]

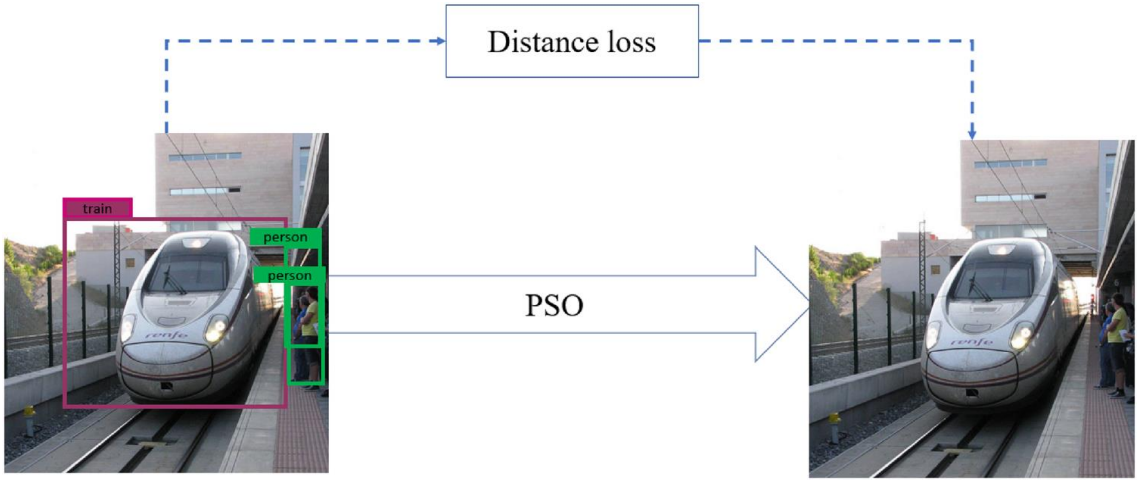
Υπάρχουν διάφορες μορφές επιθέσεων κατά της ανίχνευσης των αντικειμένων σε αυτόνομα οχήματα. Κάποιες μορφές επιθέσεων είναι οι εξής:

1. *Επιθέσεις TOG:* Οι επιθέσεις Targeted Objectness Gradient (TOG) παρουσιάστηκαν από τους Chow et al. και αποδείχθηκαν αποτελεσματικές μειώνοντας την ακρίβεια των εξεταζόμενων μοντέλων σε ποικιλία πολλών δεδομένων. Οι αντίπαλες επιθέσεις του TOG πραγματοποιούνται αντιστρέφοντας την διαδικασία εκπαίδευσης. Υπάρχουν τέσσερις τύποι επιθέσεων TOG:
    a. *TOG-untargeted attack:* Αυτή η επίθεση στοχεύει στην εξαπάτηση των μοντέλων ανίχνευσης ώστε να μην μπορούν να ανιχνεύσουν σωστά τα αντικείμενα στην εικόνα. Οι επιθέσεις αυτές δεν έχουν ως στόχο μόνο μία συγκεκριμένη κατηγορία αντικειμένων.
    b. *TOG-vanishing attack:* Αυτή η επίθεση στοχεύει στην δημιουργία θορύβου σε μία εικόνα με σκοπό την μη ανίχνευση και αναγνώριση αντικειμένων σε αυτή.
    c. *TOG-fabrication attack:* Αυτή η επίθεση στοχεύει στην προσθήκη εσφαλμένων ανιχνεύσεων στην εικόνα σε αντίθεση με την επίθεση TOG-vanishing. Ως αποτέλεσμα της επίθεσης παράγεται μία εικόνα με πολλά λανθασμένα εντοπισμένα αντικείμενα.

d. *TOG-mislabeling attack:* Σε αυτή την επίθεση γίνεται ανίχνευση των αντικειμένων και της σωστής θέσης τους στην εικόνα, ωστόσο ο ανιχνευτής διαλέγει λανθασμένες ετικέτες για τα αντικείμενα των εικόνων. Παραδείγματα επιθέσεων TOG φαίνονται στην Εικόνα 39.

Εικόνα 39: Τύποι επιθέσεων TOG [3]

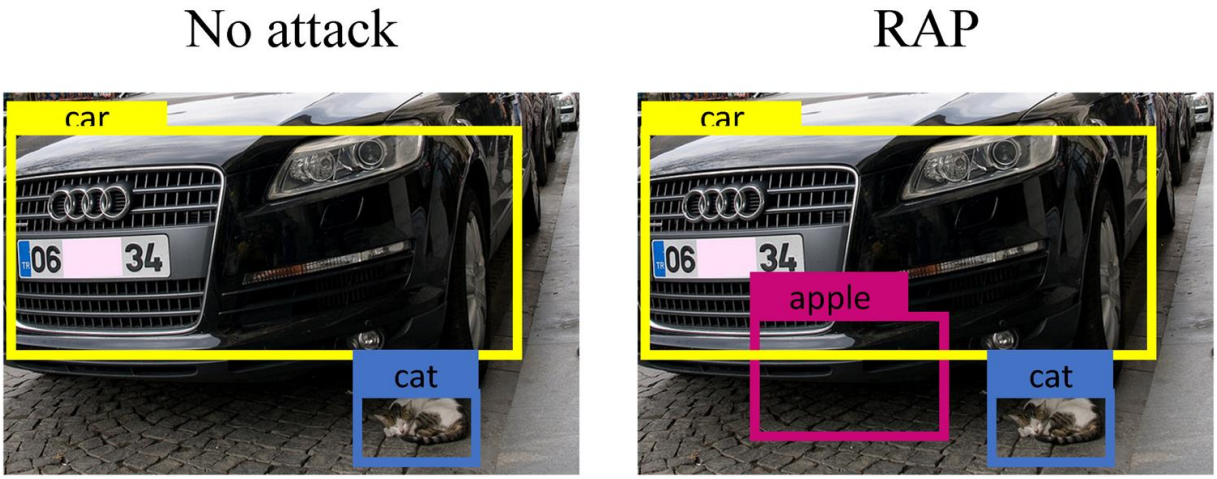
2. *Επιθέσεις evaporate:* Οι επιθέσεις αυτές ανήκουν στις επιθέσεις μαύρου κουτιού και μπορούν να κρύψουν τα αντικείμενα στόχους από τον ανιχνευτή αντικειμένων χωρίς να υπάρχει γνώση του δικτύου. Οι επιθέσεις αυτές διεξάγονται επαναλαμβανόμενα και θα επαναληφθούν στα επόμενα βήματα εάν οι προηγούμενες εικόνες που ελήφθησαν δεν είναι ευκρινείς. Παραδείγματα αυτού του είδους επίθεσης αποτελεί η Εικόνα 40.



Εικόνα 40: Επίθεση evaporate [3]

3. *Επιθέσεις DeepFool:* Κατά την διάρκεια της επίθεσης πραγματοποιείται προσθήκη διαταραχών σε εικόνες. Αυτή η προσθήκη ακολουθεί έναν επαναληπτικό αλγόριθμο ο οποίος προσθέτει διαταραχές σε κάθε βήμα του έως μία συγκεκριμένη τιμή κατωφλίου. Ο αλγόριθμος επαναλαμβάνεται όταν ένας ανιχνευτής αντικειμένων αλλάξει την αρχική του ανίχνευση. Τέτοιες επιθέσεις χρησιμοποιούνται σε πολλούς τύπους DNN.

4. *Επιθέσεις RAP:* Οι επιθέσεις Robust Adversarial Perturbation (RAP) είναι επιθέσεις μαύρου κουτιού. Οι επιθέσεις αυτές σχεδιάζονται μέσω μίας εξίσωσης βελτιστοποίησης και θα συνεχίζουν έως ότου να επιτευχθεί το επιθυμητό αποτέλεσμα. Οι RAP επιτίθενται στους ανιχνευτές αντικειμένων προσθέτοντας ελάχιστο θόρυβο στις εικόνες εισόδου. Σε αυτήν την προσέγγιση χρησιμοποιείται μία εικόνα εισόδου, ένα εκπαιδευμένο RPN και σχεδιάζεται μία ειδική αντικειμενική συνάρτηση. Ακόμη, χρησιμοποιείται μία τεχνική επαναληπτικών διαβαθμίσεων για την βελτίωση της αντικειμενικής συνάρτησης σε σχέση με την αρχική εικόνα εισόδου. Η δημιουργία των Adversarial διαταραχών θεωρείται πρόβλημα βελτιστοποίησης. Παράδειγμα αποτελεί η Εικόνα 41.



Εικόνα 41: Επίθεση RAP [3]

5. *Επιθέσεις GAT:* Οι επιθέσεις Generative Adversarial Training (GAT) είναι σχεδιασμένες για τον εντοπισμό των τρωτών αλλά και των δυνατών σημείων του δικτύου στόχου. Ο αλγόριθμος των επιθέσεων έχει σχεδιαστεί με στόχο την εξάλειψη των αδυναμιών των επιθέσεων και την βελτιστοποίηση αυτών. Σε κάθε βήμα εκπαίδευσης ο αλγόριθμος των επιθέσεων GAT μαθαίνει να παράγει την καλύτερη διαταραχή αναλόγως των δεδομένων εισόδου. Ακόμη, ταυτόχρονα με την εκπαίδευση του GAT εκπαιδεύεται από αυτό ένα δίκτυο ταξινόμησης με σκοπό την σωστή ταξινόμηση των πρωτότυπων εικόνων και των εικόνων που έχουν δεχθεί επίθεση. (Amirkhani κ.α., 2022)

5.4 Μέθοδοι προστασίας από τις επιθέσεις

Υπάρχουν πολλές μορφές επιθέσεων που έχουν ως στόχο τόσο το δίκτυο VANET όσο και τα διάφορα συστήματα των αυτόνομων οχημάτων. Πολλοί επιστήμονες ερευνούν διάφορους τρόπους προστασίας έναντι αυτών των επιθέσεων. Τρεις κύριοι τομείς έρευνας για αντίμετρα είναι οι επιθέσεις στα συστήματα VANET, η αποφυγή των Adversarial Attack και η πρόληψη κατά των επιθέσεων στην ανίχνευση αντικειμένων.

5.4.1 Τρόποι προστασίας στα VANET

Το δίκτυο VANET μπορεί να δεχθεί πολλές μορφές επιθέσεων. Γι' αυτό το λόγο έχουν αναπτυχθεί αρκετοί τρόποι αντιμετώπισης των επιθέσεων. Ένας από αυτούς είναι η χρήση διάφορων αλγορίθμων κρυπτογράφησης όπως η υποδομή δημοσίου κλειδιού οχημάτων (VPKI). Σύμφωνα με αυτόν τον αλγόριθμο το όχημα αποστολέας πρέπει να κρυπτογραφήσει με το ιδιωτικό κλειδί το μήνυμα. Το όχημα παραλήπτης θα αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί. Έτσι πιστοποιείται η αυθεντικότητα του απεσταλμένου μηνύματος. Άλλοι αλγόριθμοι κρυπτογράφησης που μπορούν να χρησιμοποιηθούν είναι η συμμετρική κρυπτογράφηση, η υβριδική κρυπτογράφηση και η μέθοδος ομαδικού κλειδιού στην οποία χρησιμοποιείται ένα προσωρινό κλειδί για κάθε session. Το κλειδί αυτό προκύπτει από το κύριο κλειδί.

Ένας άλλος τρόπος είναι η ανίχνευση κακόβουλου λογισμικού. Αυτό μπορεί να γίνει είτε με βάση την υπογραφή, όπου αναλύοντας το κακόβουλο λογισμικό παράγεται μία υπογραφή η οποία χρησιμοποιείται για τον μετέπειτα εντοπισμό του, είτε με βάση την συμπεριφορά όπου παρατηρώντας την συμπεριφορά του συστήματος οι αλγόριθμοι μπορούν να εντοπίσουν την μη φυσιολογική συμπεριφορά που προκαλείται λόγω της επίθεσης. Το κακόβουλο λογισμικό μπορεί να εντοπιστεί και με την χρήση υπηρεσιών cloud. Μέσω του cloud εντοπίζεται το κακόβουλο λογισμικό, γίνεται ανάλυση του και τα αποτελέσματα παρέχονται στο όχημα. Αυτό χρησιμοποιείται κυρίως για να μειωθεί ο φόρτος εργασίας από τις μονάδες RSU. Τέτοιου είδους αλγόριθμοι χρησιμοποιούνται συχνά στους τομείς της μηχανικής μάθησης και της εξόρυξης δεδομένων.

Για την προστασία από τις επιθέσεις η αυτοκινητοβιομηχανία TESLA εφαρμόζει μία τεχνική στιγμιαίου κλειδιού με το όνομα TIK. Αυτό βασίζεται στην συμμετρική κρυπτογράφηση κλειδιού και χρησιμοποιείται όταν όλα τα μέρη της επικοινωνίας πρέπει να είναι συγχρονισμένα με ακρίβεια. Επίσης κάθε κόμβος οφείλει να γνωρίζει μόνο το δημό-

σιο κλειδί του κόμβου αποστολέα. Σε αυτήν την τεχνική χρησιμοποιείται ένας συνδυασμός RSA και συμμετρικής κρυπτογράφησης με σκοπό την μετάδοση των πακέτων από την πηγή στον προορισμό με ασφάλεια και αποτελεσματικότητα. Ένα άλλο πρωτόκολλο που χρησιμοποιεί η TESLA είναι το πρωτόκολλο ARIADNE. Αυτό είναι μία επέκταση του DSR σε συνδυασμό με την συμμετρική κρυπτογράφηση. Αυτό χρησιμοποιεί το σχήμα ασφάλειας της TESLA για την δρομολόγηση και προσθέτει ένα HMAC κλειδί για τον έλεγχο ταυτότητας των κόμβων. Το πρωτόκολλο αυτό προστατεύει το DSR από διάφορες επιθέσεις όπως replay attack κ.α. Ωστόσο μέσω αυτού αυξάνεται η καθυστέρηση end-to-end λόγω των μηχανισμών ασφάλειας που παρέχει. Το πρωτόκολλο ARIADNE για τον έλεγχο της ταυτότητας και της επικοινωνίας μεταξύ των κόμβων χρησιμοποιεί δημόσιο κλειδί αλλά και έναν συνδυασμό μεταξύ MAC και μονόδρομης συνάρτησης κατακερματισμού.

Υπάρχουν πολλοί ακόμη τρόποι προστασίας από τις επιθέσεις στο δίκτυοVANET. Ένας από αυτούς είναι το πρωτόκολλο κατά των επιθέσεων replay. Σε αυτό το πρωτόκολλο το μήνυμα που λαμβάνεται, στέλνεται στην RSU για έλεγχο ορθότητας και για τον εντοπισμό του κακόβουλου αποστολέα. Μία άλλη μέθοδος είναι η μέθοδος Robust για επιθέσεις Sybil (RobSAD). Σε αυτή αναγνωρίζονται οι κόμβοι Sybil μέσω της ολόιδιας οδηγικής συμπεριφοράς, καθώς δύο ή περισσότερα άτομα δεν μπορούν να έχουν ολόιδια οδηγική συμπεριφορά. Παρόλο που υπάρχουν όλοι αυτοί οι τρόποι προστασίας οι επιθέσεις εξακολουθούν να υφίστανται και γι’ αυτό είναι αναγκαίο να συνεχιστεί η έρευνα ώστε να βρεθούν και νέοι τρόποι προστασίας. (Talib κ.α., 2018)

5.4.2 Τρόποι προστασίας από τις επιθέσεις Adversarial Attack

Μία πολύ συχνή μορφή επίθεσης των αυτόνομων οχημάτων αποτελούν οι επιθέσεις Adversarial Attack. Λόγω αυτού έχουν ανακαλυφθεί διάφοροι μηχανισμοί άμυνας. Τρεις κύριοι μηχανισμοί είναι οι εξής:

1. *Τροποποίηση δεδομένων:* Η μέθοδος αυτή αποτελείται από τρία είδη τροποποίησης τα οποία αφορούν είτε τα δεδομένα εκπαίδευσης είτε τα χαρακτηριστικά τους.
    a. *Feature Denoising:* Αυτή η μέθοδος έχει ως στόχο την αφαίρεση του Adversarial θορύβου από τα χαρακτηριστικά του δικτύου στόχου. Η μέθοδος αυτή επικεντρώνεται μόνο στα σημαντικά δεδομένα και όχι σε όλα τα δεδομένα εισόδου.

b. *Input Transformation:* Αυτή η μέθοδος τροποποιεί τα δεδομένα ώστε να αφαιρεθούν οι διαταραχές που προκλήθηκαν μέσω των adversarial επιθέσεων και τα τροφοδοτεί στο μοντέλο στόχου. Η μη διαφοροποίηση και η τυχαιότητα αυτών των τεχνικών τις καθιστά πολύ αποτελεσματικές.

c. *Adversarial Training:* Την μέθοδο αυτή την εφηύραν οι Goodfellow et al. Αυτή στοχεύει στο να εισάγει δεδομένα που έχουν δεχθεί επίθεση Adversarial Attack στα δεδομένα εκπαίδευσης του μοντέλου. Μέσω αυτού το μοντέλο βελτιώνεται τόσο στην ευρωστία αντιμετώπισης των επιθέσεων όσο και στην γενικότερη επίδοση του κατά την είσοδο και μη μολυσμένων δεδομένων.

2. *Προσθήκη μοντέλου:* Η μέθοδος αυτή στοχεύει στην αύξηση των μοντέλων ώστε το μοντέλο στόχος να είναι πιο ανθεκτικό στις adversarial επιθέσεις. Αυτό επιτυγχάνεται με δύο τρόπους:

   a. *Ανίχνευση Adversarial:* Στην τεχνική αυτή χρησιμοποιείται ένας δυαδικός ταξινομητής ο οποίος είναι εκπαιδευμένος να αναγνωρίζει πότε τα δεδομένα εισόδου είναι νόμιμα και πότε όχι. Μία προσέγγιση που χρησιμοποιείται ευρέως είναι η εισαγωγή μίας outlier κλάσης κατά την εκπαίδευση του DNN μοντέλου. Έτσι, το μοντέλο ταξινομεί τα δεδομένα των adversarial επιθέσεων ως outliers.

   b. *Αλγόριθμοι συνόλου:* Η τεχνική αυτή αποσκοπεί στον συνδυασμό διαφορετικών μεθόδων. Αυτές διεξάγονται παράλληλα με στόχο να επιτευχθεί η προστασία έναντι των επιθέσεων και τα μοντέλα να αποκτήσουν γνώση της κατάστασης που επικρατεί. Αυτή η τεχνική αποδείχθηκε αποτελεσματική σε μεγάλη ποικιλία επιθέσεων.

3. *Τροποποίηση μοντέλου:* Η μέθοδος αυτή αποτελείται από τεχνικές που τροποποιούν είτε τις παραμέτρους είτε τα χαρακτηριστικά κάθε μοντέλου.

   a. *Απόκρυψη κλίσης (Gradient Hiding):* Αυτή η τεχνική υλοποιείται όταν οι μηχανισμοί άμυνας αποκρύπτουν σημαντικές πληροφορίες σχετικά με την κλίση του μοντέλου ώστε να δυσκολέψουν τους αντιπάλους να την χρησιμοποιήσουν για να επιτεθούν. Όμως αυτή η τεχνική παρέχει μία ψευδή αίσθηση ασφάλειας έναντι των επιθέσεων.

   b. *Αμυντική Απόσταξη (Defensive Distillation):* Αυτή η τεχνική υλοποιήθηκε από τους Hinton et al. και έχει ως στόχο να μεταφέρει γνώσεις από ένα μεγαλύτερο μοντέλο σε ένα μικρότερο. Η τεχνική αυτή χρησιμοποιείται

και από άλλους επιστήμονες όπως τους Papernot et al. οι οποίοι δημιούργησαν έναν αμυντικό αλγόριθμο κατά των adversarial επιθέσεων. Αυτή η τεχνική χρησιμοποιήθηκε σε πολλαπλές αρχιτεκτονικές DNN μοντέλων έχοντας ως αποτέλεσμα την αύξηση της αντοχής των μοντέλων έναντι των επιθέσεων.

c. *Επαλήθευση Δικτύου (Network Verification):* Κάθε δίκτυο χαρακτηρίζεται από συγκεκριμένες ιδιότητες και χαρακτηριστικά. Έτσι, για την ανίχνευση των επιθέσεων μπορούμε να εξετάσουμε αν ικανοποιούνται κάποιες συγκεκριμένες ιδιότητες. Η τεχνική της επαλήθευσης δικτύου στοχεύει στην παροχή της εξέτασης των χαρακτηριστικών του δικτύου και στον περιορισμό των νέων επιθέσεων. Μία τεχνική επαλήθευσης δικτύου προτάθηκε από τους Katz et al. σε εφαρμογή DNN χρησιμοποιώντας την συνάρτηση ενεργοποίησης ReLU. (Kloukiniotis κ.α., 2022)

5.4.3 Τρόποι προστασίας επιθέσεων στην ανίχνευση αντικειμένων

Άλλη μία σημαντική μορφή επιθέσεων στα αυτόνομα οχήματα είναι οι επιθέσεις στην ανίχνευση αντικειμένων. Για την αντιμετώπιση αυτών των επιθέσεων πολλοί επιστήμονες ασχολούνται ερευνητικά με το θέμα και προτείνουν διάφορους τρόπους αντιμετώπισης. Ένας τέτοιος τρόπος είναι η εκπαίδευση με στοιχεία επιθέσεων. Στόχος αυτού είναι η χρήση των εικόνων που έχουν υποστεί διαταραχές για την εκπαίδευση του δικτύου. Σύμφωνα με τους Zhang et al. η μέθοδος αυτή επέφερε θετικά αποτελέσματα σε όλα τα σύνολα δεδομένων που χρησιμοποίησαν.

Ένας άλλος τρόπος αντιμετώπισης είναι η συμπίεση JPG. Με την χρήση αυτής της μεθόδου φαίνεται πως μειώνοντας τα δεδομένα των εικόνων, δηλαδή συμπιέζοντας τες, μειώνονται οι επιθέσεις. Αυτό συμβαίνει διότι εξαλείφεται η ικανότητα ανίχνευσης των μοντέλων DNN από τους επιτιθέμενους. Σύμφωνα με τους Amirkhami et al. οι περισσότερες εικόνες στα σύνολα δεδομένων βρίσκονται σε μορφή JPG. Έτσι, συμπιέζοντας τες και διενεργώντας επιθέσεις της μορφής FGSM απέδειξαν ότι η τεχνική της συμπίεσης απέτρεψε σημαντικά την απώλεια της ακρίβειας ταξινόμησης. Ωστόσο, η υπερβολική συμπίεση των εικόνων μειώνει την απόδοση των νευρωνικών δικτύων.

Έχουν προταθεί από τους επιστήμονες και άλλοι τρόποι αντιμετώπισης των επιθέσεων κατά της ανίχνευσης των αντικειμένων. Ένας από αυτούς είναι η μέθοδος ADNet η οποία βασίζεται στην ανίχνευση adversarial επιθέσεων. Αυτή εκπαιδεύει τις ικανότητες

ανίχνευσης από τις εικόνες εισόδου μέσω μίας ιεραρχικής διαδικασίας. Κατά την διαδικασία αυτή οι εικόνες εισόδου περνούν από το συνελικτικό και το συνθετικό επίπεδο και μέσω διεργασιών καταλήγουν σε ένα πλήρως συνδεδεμένο αλγόριθμο SoftMax με δύο πιθανές τιμές για τις αρχικές και τις διαταραγμένες εικόνες. Ακόμη μια μέθοδος είναι τα δίκτυα Parseval. Αυτά δημιουργήθηκαν από τους Cisse et al. και χρησιμοποιούν μία σταθερά Lipschitz. Θεωρώντας ότι το δίκτυο είναι ένας συνδυασμός συναρτήσεων, αυτό μπορεί να αντισταθεί στις διαταραχές κρατώντας μικρή την σταθερά Lipschitz. Τα δίκτυα αυτά αναπτύχθηκαν ελέγχοντας την κανονιστική θέση των πινάκων βάρους του δικτύου και παραμετροποιώντας τους μέσω του Parseval framework. Καθώς η έρευνα προχωρά όλο και πιο αποτελεσματικοί αλγόριθμοι θα ανακαλύπτονται, διότι οι επιθέσεις κατά των αυτόνομων οχημάτων συνεχίζονται και οι αυτοκινητοβιομηχανίες αναζητούν λύσεις σε αυτές. (Amirkhami κ.α., 2022)

6 Συμπεράσματα

Η παρούσα πτυχιακή αναφέρθηκε τόσο στις προκλήσεις ασφαλείας όσο και στην κατηγοριοποίηση επιθέσεων στα αυτόνομα οχήματα και στα συστήματα IoV. Τα συστήματα IoV είναι ένα ερευνητικό θέμα με το οποίο ασχολούνται πολλοί ερευνητές και αρκετές αυτοκινητοβιομηχανίες σε όλο τον κόσμο. Το IoV εξαρτάται από τις σύγχρονες υποδομές και αρχιτεκτονικές που κατανέμουν τον υπολογιστικό φόρτο σε πολλαπλές μονάδες επεξεργασίας σε ένα δίκτυο (M. Nahri κ.α., 2018). Αυτό αποτελεί το σύστημα επικοινωνίας μεταξύ των αυτόνομων οχημάτων. Με την χρήση των αυτόνομων οχημάτων παρέχονται δυνατότητες όπως βελτιωμένες μεταφορές, βελτιωμένα πρότυπα ασφάλειας, καλύτερη οικονομία καυσίμου και πιο ξεκούραστα ταξίδια. Με την όλο και πιο ευρεία χρήση αυτών των οχημάτων υπάρχουν πολλοί κακόβουλοι που προσπαθούν να εκμεταλλευτούν τυχόν ευπάθειες στην ασφάλεια τους και να βλάψουν τους χρήστες τους.

Σε αυτή την εργασία αναλύθηκαν οι διάφοροι τομείς στους οποίους υπάρχουν ευπάθειες όπως η μονάδα ECU, οι τρόποι επιθέσεων όπως η επίθεση Sybil αλλά και οι μέθοδοι προστασίας από αυτές τις επιθέσεις. Η εργασία αυτή εστίασε επίσης στα συστήματα CAV και στο δίκτυο VANET αναλύοντας τόσο τις μορφές επιθέσεων όσο και τις απαιτήσεις ασφαλείας και απορρήτου των συστημάτων αυτών. Για την συγγραφή της εργασίας χρησιμοποιήθηκαν άρθρα από επιστημονικά περιοδικά και βιβλία πληρώντας κάποια κριτήρια ένταξης. Τέτοια κριτήρια ήταν η συνάφεια με το θέμα της πτυχιακής, η ημερομηνία συγγραφής τους να είναι της τελευταίας πενταετίας, να είναι δημοσιευμένα από έγκριτους εκδοτικούς οίκους κ.α. Η εργασία αυτή είχε ως σκοπό της διερεύνηση του θέματος των αυτόνομων οχημάτων καθώς και του δικτύου IoV τα οποία εξελίσσονται διαρκώς και αποτελούν κλάδο προς έρευνα από τους επιστήμονες.

Τα αυτόνομα οχήματα είναι ένας τεχνολογικός τομέας που συνεχώς εξελίσσεται και βελτιώνεται. Οι ερευνητές μελετούν τις επιθέσεις στα συστήματα αυτά και προτείνουν λύσεις αλλά διαρκώς εμφανίζονται νέες μορφές επιθέσεων. Γι’ αυτό το λόγο η έρευνα σχετικά με τις ευπάθειες των αυτόνομων οχημάτων πρέπει να συνεχιστεί και να βρεθούν νέα αντίμετρα κατά των επιθέσεων. Ένας τομέας μελλοντικής βελτίωσης είναι η επεξεργασία των δεδομένων. Καθώς αυξάνονται οι χρήστες αυτών των οχημάτων πρέπει να αναβαθμίζονται οι διαθέσιμοι πόροι του δικτύου με σκοπό την επεξεργασία της μεγάλης

συλλεγόμενης ποσότητας δεδομένων. Για να γίνει αυτό πρέπει να βρεθούν πιο αποτελεσματικοί αλγόριθμοι και να υπάρξει περισσότερη υπολογιστική ισχύ. Ένας άλλος τομέας που μπορεί να βελτιωθεί είναι η ασφάλεια των επιβατών των αυτόνομων οχημάτων. Μέσω του δικτύου IoV μπορεί να παρακολουθείται η υγεία των επιβατών σε πραγματικό χρόνο και το όχημα να επικοινωνεί με δομές υγείας σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στους επιβάτες (A. Nanda κ.α., 2019). Καθώς τα αυτόνομα οχήματα εξελίσσονται θα βρίσκονται και νέοι τομείς στους οποίους θα χρειάζονται εξέλιξη. Αυτή η εξέλιξη θα συνεχίσει να συμβαίνει μέσω τη συνεργασίας των ερευνητών και των αυτοκινητοβιομηχανιών.

Βιβλιογραφία

[1] M. Adhikari, A. Munusamy, A. Hazra, V.G. Menon, V. Anavangot, D. Puthal, "Security in Edge-Centric Intelligent Internet of Vehicles: Issues and Remedies", IEEE, 2021

[2] T.H.H. Aldhyani, H. Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity", Sensors MDPI, 2022

[3] A. Amirkhani, M.P. Karimi, A. Banitalebi-Dehkordi, "A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles", Springer-Verlag, 2022

[4] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, "Robust Physical-World Attacks on Deep Learning Visual Classification", Computer Vision and Pattern Recognition Conference (CVPR), 2018

[5] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, S. Deshmukh, "A survey on security and privacy issues in IoV", International Journal of Electrical and Computer Engineering (IJECE), 2020

[6] J. Hu, H. Niu, J. Carrasco, B. Lennox and F. Arvin, "Voronoi-Based Multi-Robot Autonomous Exploration in Unknown Environments via Deep Reinforcement Learning", IEEE Transactions on Vehicular Technology Journal, 2020

[7] W. Jiang, H. Li, S. Liu, X. Luo, R. Lu, "Poisoning and Evasion Attacks Against Deep Learning Algorithms in Autonomous Vehicles", IEEE Transactions on Vehicular Technology, 2020

[8] K. Kim, J.S. Kim, S. Jeong, J.H. Park, H.K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense", Elsevier Ltd., 2021

[9] A. Khelifi, M. Abu Talib, D. Nouichi, M.S. Eltawil, "Toward an Efficient Deployment of Open-Source Software in the Internet of Vehicles Field" Arabian Journal for Science and Engineering, 2019

[10] A. Kloukiniotis, A. Papandreou, A. Lalos, P. Kapsalas, D.-V. Nguyen, K. Moustakas, "Countering Adversarial Attacks on Autonomous Vehicles Using Denoising Techniques: A Review", IEEE Journal of Intelligent Transportation Systems, 2022

[11] I. Koukoutsis, "Εξομοίωση με το software VEINS και ανάλυση αποτελεσμάτων", Bachelor Thesis, University of Thessaly, 2022

[12] P.A. Laplante, M. Kassab, NL. Laplante, JM. Voas, "Building Caring Healthcare Systems in the Internet of Things", IEEE Syst J., 2018

[13] T. Limbasiya, K.Z. Teng, S. Chattopadhyay, J. Zhou, "A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles", Elsevier, 2022

[14] M. Masood, Z. Saeed, M.U. Khan, "A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs)", Journal on Advanced Research in Electrical Engineering (JAREE), 2023

[15] M. Nahri, A. Boulmakoul, L. Karim, A. Lbath, "IoV distributed architecture for real-time traffic data analytics", Elsevier, 2018

[16] A. Nanda, D. Puthal, J.J.P.C. Rodrigues, S.A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions", IEEE Wireless Communications, 2019

[17] B.K. Osibo, C. Zhang, C. Xia, G. Zhao, Z. Jin, "Security and Privacy in 5G Internet of Vehicles (IoV) Environment", Journal on Internet of Things (JIOT), 2021

[18] N. Sharma, N. Chauhan, N. Chand, "Security challenges in Internet of Vehicles (IoV) environment", First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018

[19] D. Takahashi, "Subaru Legacy 2020 review: Sensors that detect a drowsy or distracted driver", venturebeat.com, 2020

[20] M.A. Talib, S. Abbas, Q. Nasir, M.F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security", International Journal of Distributed Sensor Networks, 2018

[21] C.K. Toh, "Research Challenges in Intelligent Transportation Networks", Nanyang Technological University, 2008

[22] M. Yoosefzadeh-Najafabadi, HJ. Earl, D. Tulpan, J. Sulik, M. Eskandari, "Application of Machine Learning Algorithms in Plant Breeding: Predicting Yield from Hyperspectral Reflectance in Soybean", Front Plant Sci., 2021

Παράρτημα Α

Σε αυτό το παράρτημα παρατίθενται οι αλγόριθμοι επίθεσης και άμυνας κατά των επιθέσεων που αναλύονται στο κεφάλαιο 3.4.

Πίνακας 5: Επεξήγηση του συμβολισμού των αλγορίθμων [7]

Notations	Description
$\boldsymbol{v_i}$	velocity of the ith particle in PSO
$\boldsymbol{p_i}$	position of the ith particle in PSO
r_1, r_2	random numbers in $(0, 1)$
c_1, c_2	acceleration factors
α	inertia weight in PSO
$(\boldsymbol{x_n}, y_n)$	the normal sample and its label (unmodified data)
$(\boldsymbol{x_p}, y_n)$	the poisoned sample and its label
$(\boldsymbol{x_t}, y_t)$	the targeted sample and its label (unmodified data)
$(\boldsymbol{x_a}, y_t)$	the adversarial sample and its label
M_1, M_2	the number of particles in the swarm
$\boldsymbol{p_i^*}$	the best position of the ith particle
$\boldsymbol{p_{gb}}$	the best position of the whole swarm
T_1, T_2	the number of iteration
D_{tr}	the original training dataset
D_p	the optimal set of poisoned samples

Algorithm 1: Initialization of the PAPSO.

Input: M_1 is the number of particles in the swarm; a normal sample $(\boldsymbol{x_n}, y_n)$

1: **for** each particle $i = 1, \ldots, M_1$ **do**
2: Initialize the particle's position $\boldsymbol{p_i}$
3: Initialize the particle's velocity $\boldsymbol{v_i}$
4: Initialize $pbest$: $\boldsymbol{p_i^*} \leftarrow \boldsymbol{p_i}$
5: **end for**
6: Initialize $gbest$: Choose $acc(\boldsymbol{p_{max}})$ from $acc(\boldsymbol{p_1})$ to $acc(\boldsymbol{p_{M_1}})$ where $acc(\boldsymbol{p_{max}})$ is the maximum value.
7: $\boldsymbol{p_{gb}} \leftarrow \boldsymbol{p_{max}}$

Εικόνα 42: Αρχικοποίηση αλγορίθμου PAPSO [7]

Algorithm 2: Poisoning Attack With Particle Swarm Optimization.

Input: acceleration factors c_1, c_2; random numbers r_1, r_2; inertia weight α; T_1 is the number of iteration; M_1 is the number of particles in the swarm; a normal sample $(\boldsymbol{x_n}, y_n)$

Output: one optimal poisoned sample $(\boldsymbol{x_p}, y_n)$

$p_1, p_2, \ldots, p_{M_1}$ = initialization of the PAPSO(M_1, $(\boldsymbol{x_n}, y_n)$)
for $t = 1$ to T_1 (iteration counter) **do**
  for each particle $i = 1, \ldots, M_1$ **do**
    $\boldsymbol{v_i} \leftarrow \alpha \boldsymbol{v_i} + c_1 r_1 (\boldsymbol{p_i^*} - \boldsymbol{p_i}) + c_2 r_2 (\boldsymbol{p_{gb}} - \boldsymbol{p_i})$
    $\boldsymbol{p_i} \leftarrow \boldsymbol{p_i} + \boldsymbol{v_i}$
    if $acc(\boldsymbol{p_i}) > acc(\boldsymbol{p_i^*})$ **then**
      $\boldsymbol{p_i^*} \leftarrow \boldsymbol{p_i}$
    end if
    if $acc(\boldsymbol{p_i}) > acc(\boldsymbol{p_{gb}})$ **then**
      $\boldsymbol{p_{gb}} \leftarrow \boldsymbol{p_i}$
    end if
  end for
end for
$(\boldsymbol{x_p}, y_n) \leftarrow (\boldsymbol{p_{gb}} + \boldsymbol{x_n}, y_n)$
return $(\boldsymbol{x_p}, y_n)$

Εικόνα 43: Αλγόριθμος επίθεσης PAPSO [7]

Algorithm 3: Initialization of the EAPSO.

Input: M_2 is the number of particles in the swarm; the targeted test sample $(\boldsymbol{x_t}, y_t)$

for each particle $j = 1, \ldots, M_2$ **do**
  Initialize the particle's position $\boldsymbol{p_j}$
  Initialize the particle's velocity $\boldsymbol{v_j}$
  Initialize $pbest$: $\boldsymbol{p_j^*} \leftarrow \boldsymbol{p_j}$
end for
Initialize $gbest$: Choose $pro(\boldsymbol{p_{min}})$ from $pro(\boldsymbol{p_1})$ to $pro(\boldsymbol{p_{M_2}})$ where $pro(\boldsymbol{p_{min}})$ is the minimum value.
$\boldsymbol{p_{gb}} \leftarrow \boldsymbol{p_{min}}$

Εικόνα 44: Αρχικοποίηση αλγορίθμου EAPSO [7]

Algorithm 4: Evasion Attack With Particle Swarm Optimization.

Input: acceleration factors c_1, c_2; random numbers r_1, r_2; inertia weight α; T_2 is the number of iteration; M_2 is the number of particles in the swarm; the targeted test sample $(\boldsymbol{x_t}, y_t)$

Output: the optimal adversarial sample $(\boldsymbol{x_a}, y_t)$

$p_1, p_2, \ldots, p_{M_2}$ = initialization of the EAPSO(M_2, $(\boldsymbol{x_t}, y_t)$)
for $t = 1$ to T_2 (iteration counter) **do**
  for each particle $j = 1, \ldots, M_2$ **do**
    $\boldsymbol{v_j} \leftarrow \alpha \boldsymbol{v_j} + c_1 r_1 (\boldsymbol{p_j^*} - \boldsymbol{p_j}) + c_2 r_2 (\boldsymbol{p_{gb}} - \boldsymbol{p_j})$
    $\boldsymbol{p_j} \leftarrow \boldsymbol{p_j} + \boldsymbol{v_j}$
    if $pro(\boldsymbol{p_j}) > pro(\boldsymbol{p_j^*})$ **then**
      $\boldsymbol{p_j^*} \leftarrow \boldsymbol{p_j}$
    end if
    if $pro(\boldsymbol{p_j}) > pro(\boldsymbol{p_{gb}})$ **then**
      $\boldsymbol{p_{gb}} \leftarrow \boldsymbol{p_j}$
    end if
  end for
end for
$(\boldsymbol{x_a}, y_t) \leftarrow (\boldsymbol{p_{gb}} + \boldsymbol{x_t}, y_t)$
return $(\boldsymbol{x_a}, y_t)$

Εικόνα 45: Αλγόριθμος επίθεσης EAPSO [7]

Algorithm 1. Algorithm of CNN-LSTM

```
Preprocessing data
Class 4, input data 22222
Model = Sequential()
model. Add(Conv1D(filters = 128, kernel_size = 1, strides = 1, padding = 'same',
input shape = (train_data_st.shape [1], 1)))
model. Add(Conv1D(filters = 128, kernel size = 1, strides = 1, padding = 'same'))
model. Add(LSTM(64, activation = 'relu', return sequences = True))
model. Add(LSTM(64, return sequences = True))
model. Add(Flatten())
model.add(Dense(128, activation = 'relu'))
model.add(Dense(256, activation = 'relu'))
Build Model
Input = Input(shape = (train_data_st.shape[1],1))
C = Conv1D(filters = 32, kernel_size = 1, strides = 1)(inp)
C2 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(C)
A1 = Activation("relu")(C11)
C3 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(A11)
S13 = Add()([C12, C])
A1 = Activation("relu")(S11)
M11 = MaxPooling1D(pool_size = 1, strides = 2)(A12)
C3 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(M11)
A3 = Activation("relu")(C21)
C4 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(A21)
S4 = Add()([C22, M11])
A4 = Activation("relu")(S11)
M4 = MaxPooling1D(pool_size = 1, strides = 2)(A22)
C5 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(M21)
A5 = Activation("relu")(C31)
C6 = Conv1D(filters = 32, kernel_size = 1, strides = 1, padding = 'same')(A31)
S5 = Add()([C32, M21])
A5 = Activation("relu")(S31)
M31 = MaxPooling1D(pool_size = 1, strides = 2)(A32)
F1 = Flatten()(M31)
D1 = Dense(32)(F1)
A66 = Activation("relu")(D1)
D22 = Dense(32)(A66)
D33 = Dense(labels.shape[1])(D22)
A77 = Activation("softmax")(D33)
model = Model(inputs = inp, outputs = A7)
# opotimmaztion
Paramters patience = 3, verbose = 1, factor = 0.5, lr = 0.00001 and optimizer = rms, epochs = 10
batch_size = 64
For → rms = keras.optimizers.rms = RMSprop(learning_rate = 0.001, rho = 0.9)
history = model.fit(x_train_cnn,y_train, batch_size = batch_size,
steps_per_epoch = x_train.shape[0]//batch_size,
epochs = epochs,
validation_data = (x_validate_cnn,y_validate),
#validation_split = 0.10,
callbacks = [learning_rate_reduction, checkpoint]
```

Εικόνα 46: Αλγόριθμος προστασίας επιθέσεων [2]

Παράρτημα Β

Στο παράρτημα αυτό παρατίθεται ο οδηγός εγκατάστασης των λογισμικών που χρησιμοποιούνται για τα σενάρια προσομοίωσης του κεφαλαίου 2.3.

Το Veins μπορεί να τρέξει σε Linux. Mac OS X και Windows περιβάλλοντα. Προτιμάται όμως το Linux λόγω των εκτεταμένων δυνατοτήτων debugging που προσφέρει. Για να κατασκευαστεί σε Linux χρειάζεται πρώτα να εγκατασταθούν κάποια πακέτα με την παρακάτω εντολή στο τερματικό :

```
sudo apt-get install build-essential gcc g++ bison flex perl tcl-dev tk-dev
blt libxml2-dev zlib1g-dev default-jre doxygen graphviz libwebkitgtk-1.0-0
openmpi-bin libopenmpi-dev libpcap-dev autoconf automake libtool libproj-dev
libgdal1-dev libfox-1.6-dev libgdal-dev libxerces-c-dev qt4-dev-tools
```

Στο Mac OS X θα χρειαστεί να εγκατασταθούν τα αντίστοιχα πακέτα μέσω Macports τρέχοντας την εντολή στο τερματικό :

```
sudo port install bison zlib tk blt libxml2 libtool xercesc3 proj gdal fox
```

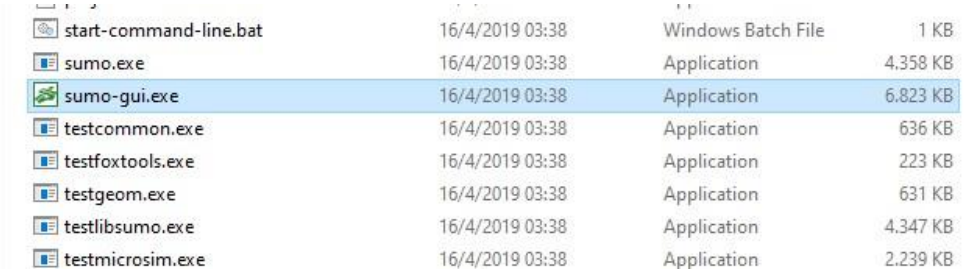
Η εγκατάσταση που επιλέχθηκε ήταν στα Windows.

Υποθέτοντας ότι το home directory είναι το C:\Users\user και το απαραίτητο software θα εγκατασταθεί στον φάκελο C:\Users\user\src (ο οποίος έχει δημιουργηθεί) τα βήματα είναι τα εξής.

Βήμα πρώτο

Κατεβάζετε το Sumo 1.9.2 και κάνετε αποσυμπίεση στον φάκελο C:\Users\user\src\sumo-1.9.2 στον οποίο μέσα θα βρείτε το αρχείο C:\Users\user\src\sumo-1.9.2\bin\sumogui.exe.

Εδώ ας σημειωθεί ότι οι συντομότερες εκδόσεις του Sumo προϋποθέτουν να είναι εγκατεστημένο το Microsoft Visual C++ 2010 Redistributable Package (x86).

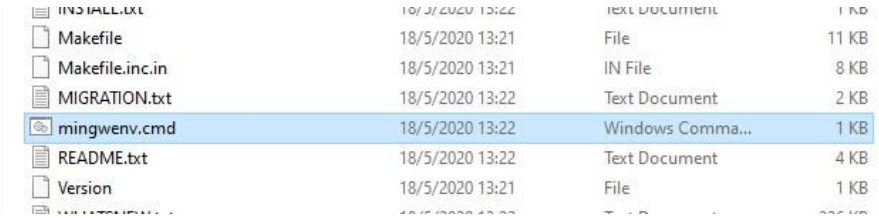


Προσοχή πρέπει να δοθεί και στην έκδοση του Sumo, πρέπει να χρησιμοποιηθεί η συγκεκριμένη έκδοση για το Veins-5.0.

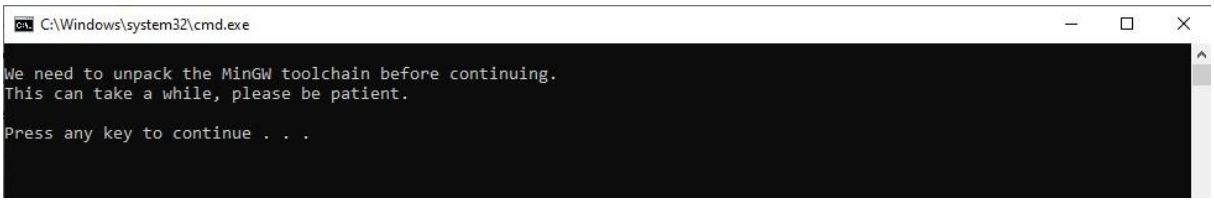
Βήμα δεύτερο

Κατεβάζετε το OMNeT++ 5.6.2 for Windows και το κάνετε αποσυμπίεση στον φάκελο C:\Users\user\src\omnetpp-5.6.2.. Σημείωση ότι πρέπει να μην υπάρχουν κενά στο όνομα του φακέλου. Μέσα στον φάκελο θα πρέπει να βρείτε το Script :

```
C:\Users\user\src\omnetpp-5.6.2\mingwenv.cmd
```



Τρέχοντάς το βλέπετε ένα περιβάλλον MinGW το οποίο μοιάζει με το terminal του Linux.



Για να κάνετε Build το OmneT++ 5 θα πρέπει να γράψετε την εντολή :

```
./configure
```

Και μετά την εντολή :

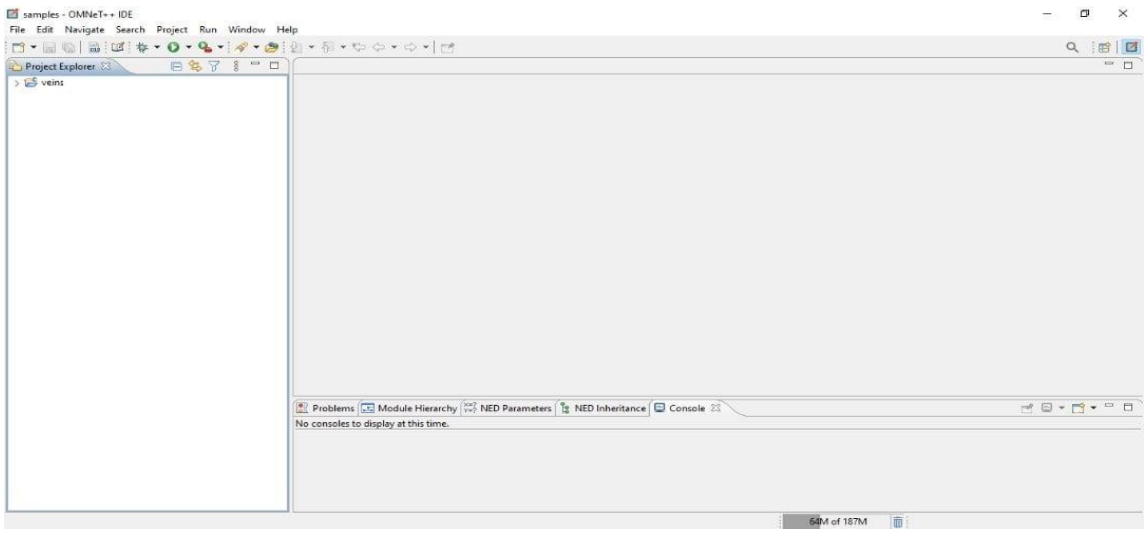
```
make
```

για να ξεκινήσει η διαδικασία της εγκατάστασης η οποία θα διαρκέσει μερικά λεπτά. Όταν ολοκληρωθεί και όλα έχουν πάει καλά το αποτέλεσμα θα είναι το

/c/Users/user/src/omnetpp-5.6.2/bin/omnetpp. Για να τρέξετε το OMNeT πληκτρολογήστε την εντολή :

```
omnetpp
```

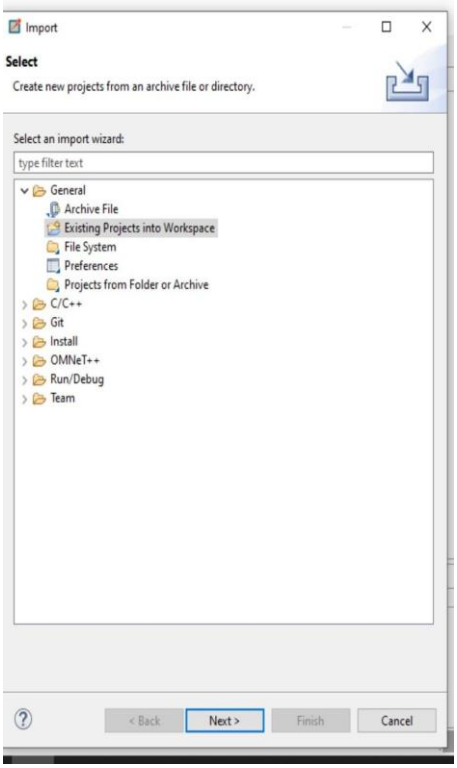
Αυτό θα ανοίξει το OMNeT++ IDE. Όλα αυτά υπό την προϋπόθεση ότι έχει επιλεχθεί το C:\ Users\user\src\omnetpp-5.6.2\samples ως workspace.



Εικόνα 47: Περιβάλλον OMNeT++.

Βήμα τρίτο

Κατεβάστε και το Veins 5.0 και αποσυμπιέστε στον φάκελο C:\Users\user\src\veins-5.0. Εισάγετε το project στο OMNeT++ IDE workspace πατώντας File > Import > General: Existing Projects into Workspace και επιλέξτε τον φάκελο που κάνατε αποσυμπίεση το Framework



Κάντε build το project επιλέγοντας Project > Build All στο περιβάλλον του OMNeT++5. Αφού δημιουργηθεί το project είστε έτοιμοι να τρέξετε την πρώτη IVC προσομοίωση.

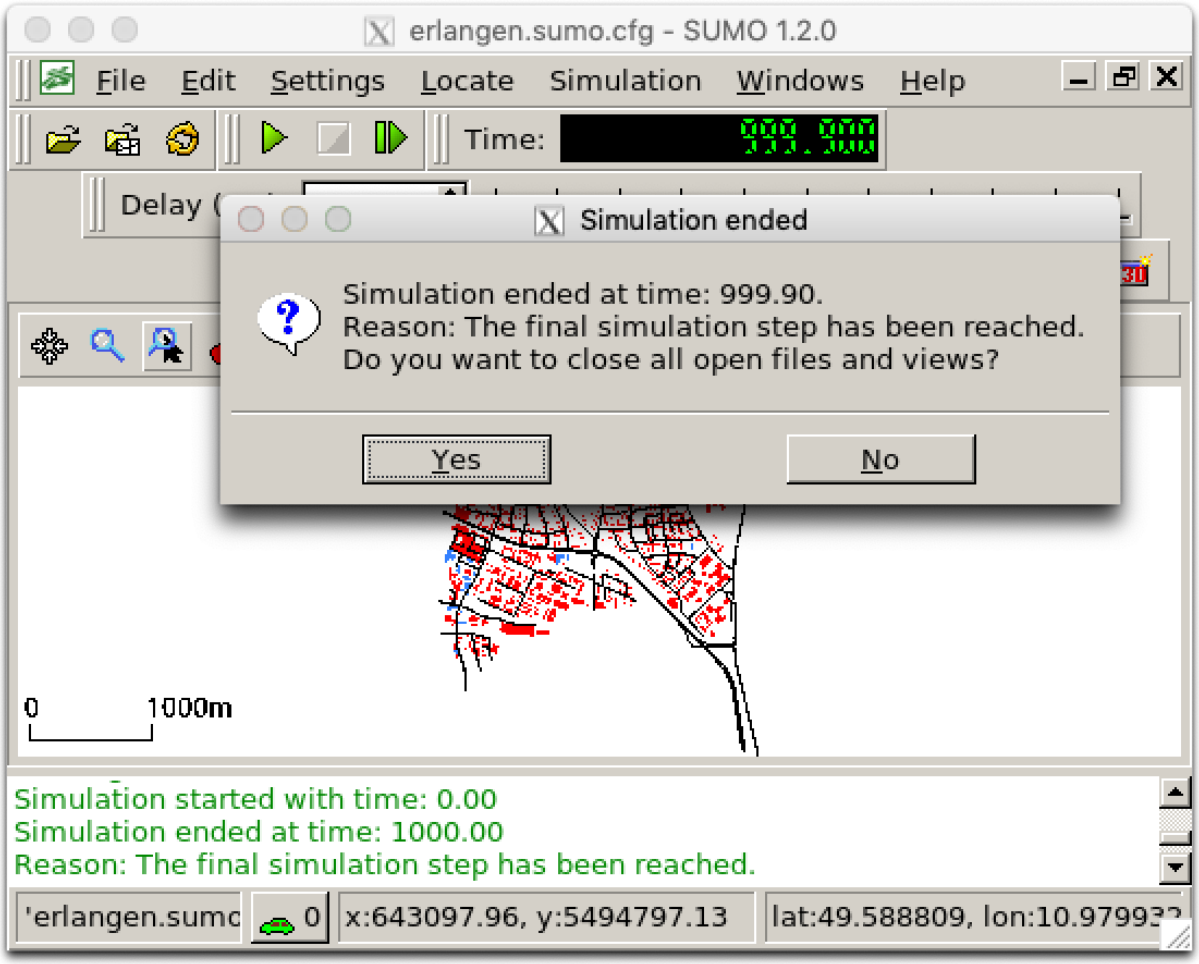
Βήμα τέταρτο

Σιγουρευτείτε ότι το Sumo λειτουργεί πηγαίνοντας στο τερματικό MinGW του OMNeT++ αλλάξτε το τρέχον directory σε /c/Users/user/src/veins-5.0/examples/veins/ χρησιμοποιώντας της εξής εντολή: cd ../veins-5.0/examples/veins. Έπειτα τρέξτε αυτήν την εντολή για να ξεκινήσει το Sumo.

```
/c/Users/user/src/sumo-1.9.2/bin/sumo.exe -c erlangen.sumo.cfg
```

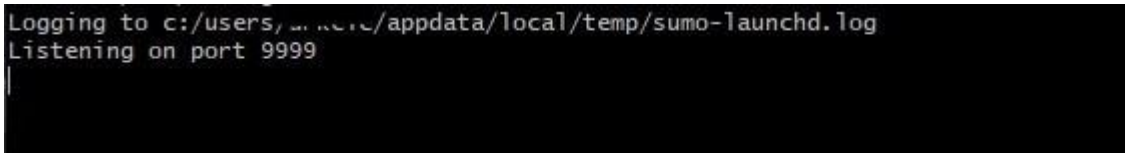
Στην συνέχεια θα πρέπει να δείτε μια γραμμή που λέει "Loading configuration... done.", στην συνέχεια μετά από λίγο δεν θα εμφανιστεί κάτι άλλο στην γραμμή εντολών.

Εάν εγκαταστήσατε σε άλλο path το Sumo, να θυμάστε ποια εντολή χρησιμοποιήσατε αντί του /c/Users/user/src/sumo-1.9.2/bin/sumo.exe. Θα χρειαστεί να προσθέσετε αυτήν την εντολή στην -c επιλογή του sumo-launchd.py του επόμενου βήματος.



Τελευταίο βήμα είναι να τρέξετε το σενάριο του Veins. Αρχικά ανοίγετε το OMNeT++ και στην συνέχεια πληκτρολογείτε την παρακάτω εντολή στην γραμμή εντολών (python script).

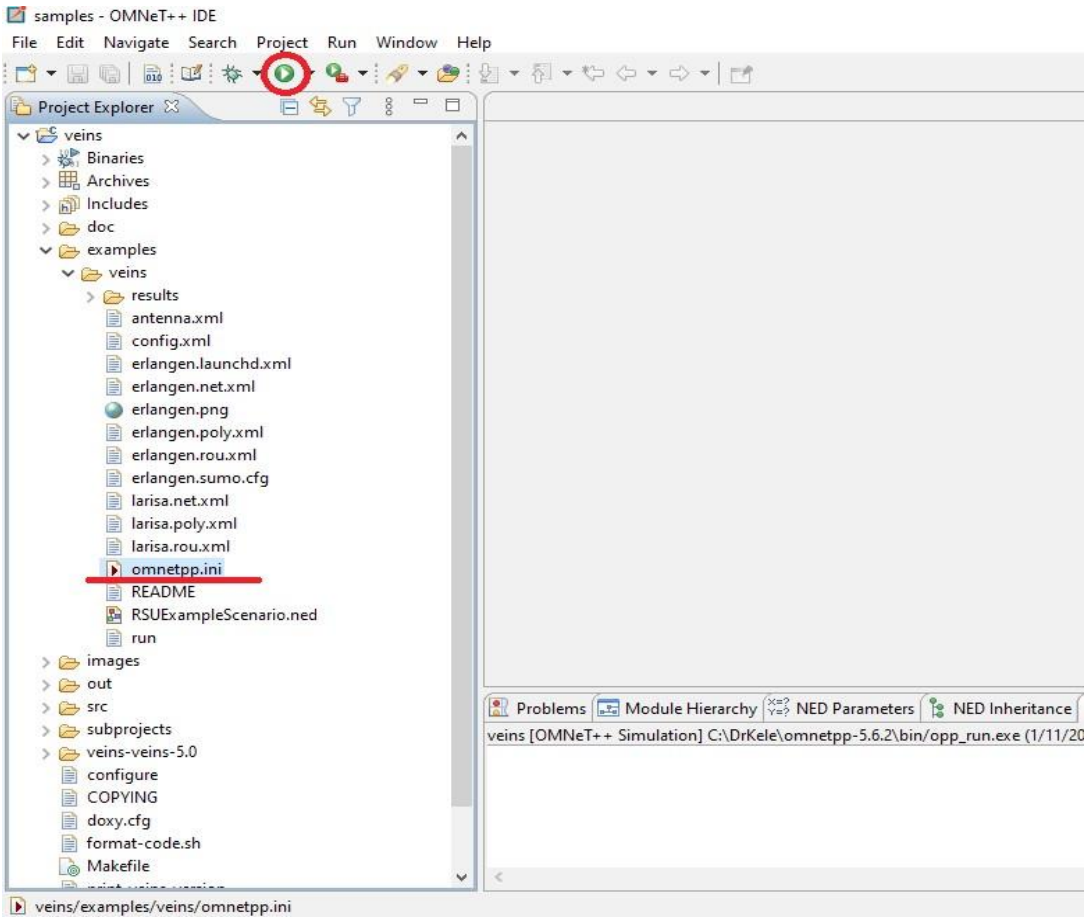
```
/c/Users/user/src/veins-5.0/sumo-launchd.py -vv -c /c/Users/user/src/sumo-1.2.0/bin/sumo.exe
```



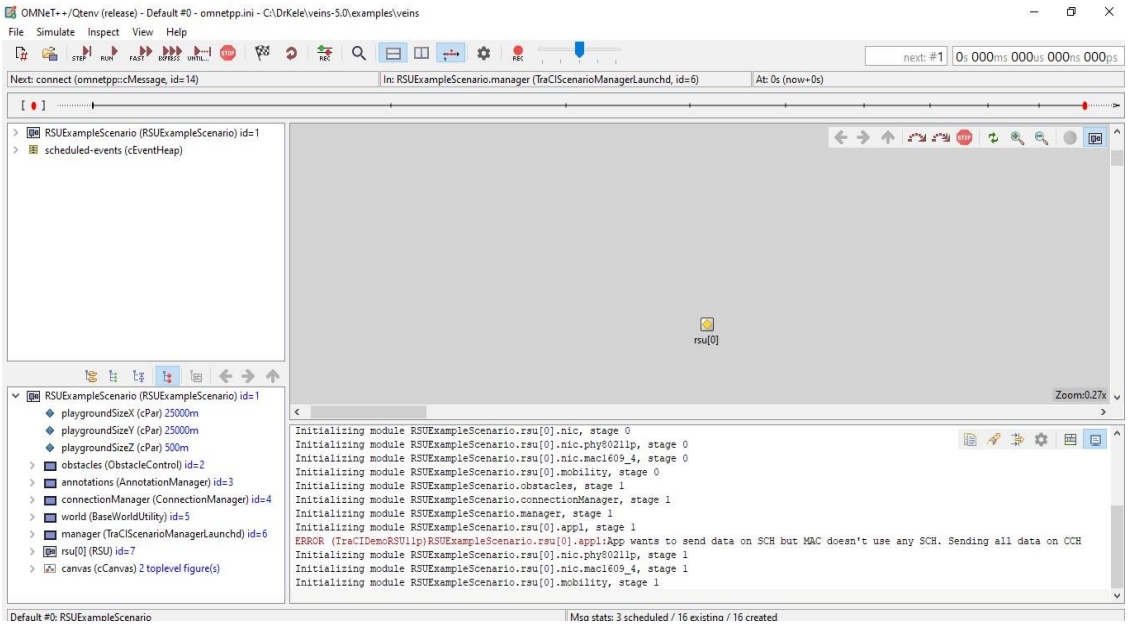
Εικόνα 48: Μετά την ενεργοποίηση του script

Αυτό το script θα δώσει την εντολή να ξεκινήσουν TCP συνδέσεις μεταξύ του OMNeT++ και του Sumo, δημιουργώντας ένα νέο αντίγραφο της προσομοίωσης Sumo για κάθε προσομοίωση που συνδέεται με το OMNeT++. Μόλις ενεργοποιήσετε το Script, αφήστε ανοιχτό το τερματικό και συνεχίστε στο OMNeT++ IDE.

Στο IDE τρέξτε το σενάριο του Veins κάνοντας δεξί κλικ στο εξής path veins-5.0/examples/veins/omnetpp.ini στο παράθυρο αριστερά. Στην συνέχεια επιλέγετε Run As > OMNeT++ simulation. Μην ξεχάσετε να δώσετε πρόσβαση στο Sumo σε οποιοδήποτε Firewall χρησιμοποιείτε. Παρομοίως με το προηγούμενο παράδειγμα, αυτό πρέπει να δημιουργήσει και να ανοίξει ένα δεύτερο παράθυρο. Στην συνέχεια μπορείτε να ξανά τρέξετε την προσομοίωση πατώντας το πράσινο “play” button στο OMNeT++ IDE.



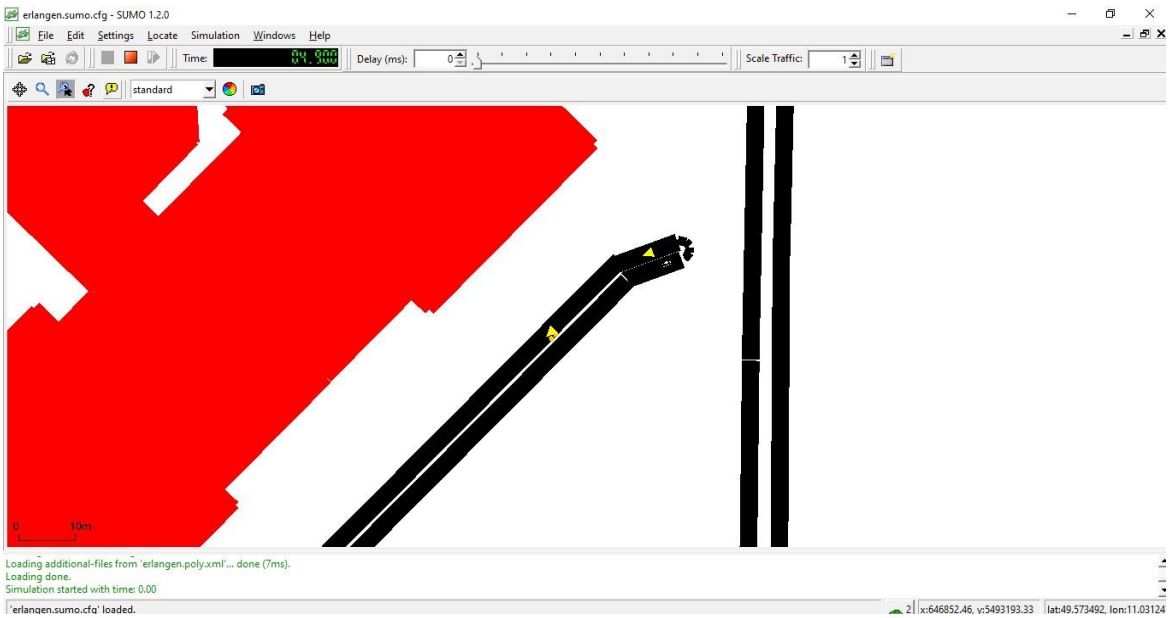
Στη Εικόνα 49 διακρίνετε με κόκκινο σημάδι το play button και το σενάριο προς υλοποίηση.



Εικόνα 49: Περιβάλλον OMNET++

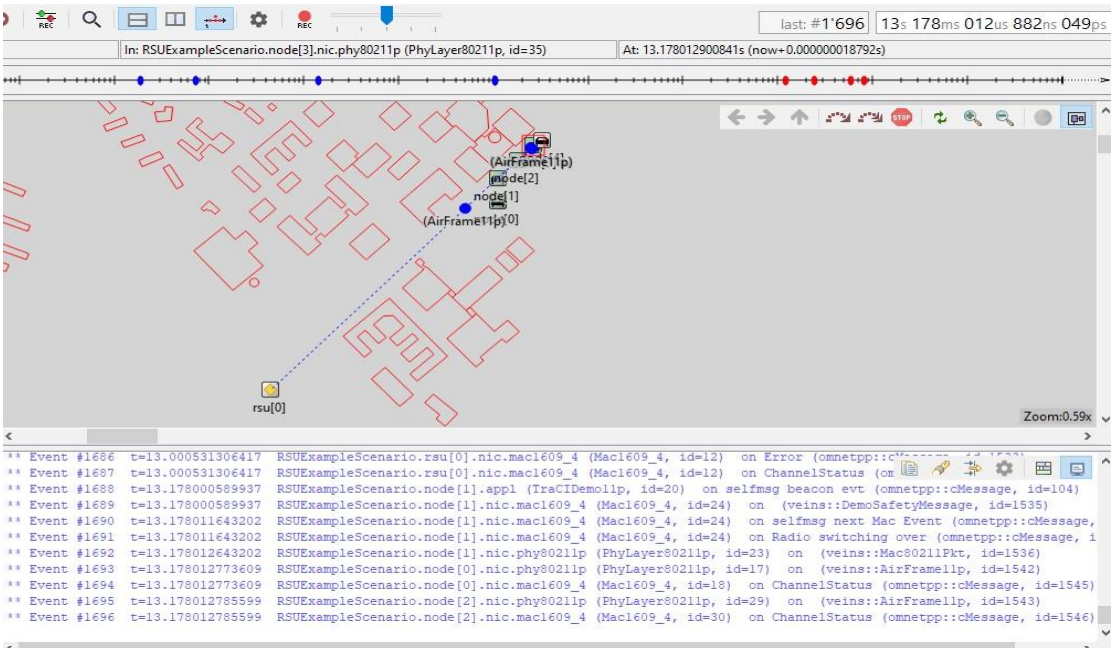
Σε αυτήν την εικόνα παρουσιάζεται το παράθυρο που ανοίγει όταν πατήσετε το play button. Αν μέχρι εδώ όλα πήγαν σωστά θα πρέπει να ανοίξει η προσομοίωση στο sumo μόλις πατήσετε το Run. Εκεί θα δείτε έναν χάρτη (erlangen) και μια σειρά οχημάτων να εκτελούν ένα σενάριο στο οποίο θα γίνεται ένα ατύχημα.

Στην Εικόνα 50 φαίνεται το σημείο εκκίνησης των οχημάτων που μετέχουν στο σενάριο.



Εικόνα 50: Αναδυόμενο παράθυρο Sumo

Στην Εικόνα 51 φαίνονται τα οχήματα και τα μηνύματα που ανταλλάσσουν μεταξύ τους (OMNeT++ IDE).



Εικόνα 51: Ανταλλαγή μηνυμάτων μεταξύ των οχημάτων στο περιβάλλον OMNeT ++

Επίσης μπορείτε να τρέξετε το σενάριο σε debug mode. Αυτό μπορείτε να το κάνετε επιλέγοντας debug as αντί του Run as όταν τρέχετε την προσομοίωση κάνοντας δεξί κλικ στο omnetpp.ini. Κάνοντας το θα δείτε πολλές πληροφορίες στο τερματικό, ωστόσο η προσομοίωση θα εκτελεσθεί με χαμηλότερη ταχύτητα. Αν ενδιαφέρεστε να δείτε τον πηγαίο κώδικα της εφαρμογής που εκτελείται στα προσομοιωμένα οχήματα, ελέγξτε omnetpp.ini αρχείο και θα δείτε ότι είναι TraCIDemo11p. Ο κώδικας του βρίσκεται στο αρχείο src/veins/modules/application/traci/TraCIDemo11p.cc. Μπορείτε να δείτε την μέθοδο handlePositionUpdate η οποία καθορίζει πως αντιδρά ένα όχημα όταν λαμβάνεται ένα position update από το Sumo, ελέγχοντας αν έμεινε ακίνητο για αρκετή ώρα και στέλνει broadcast μηνύματα στα υπόλοιπα οχήματα με σκοπό να ειδοποιήσει για πιθανή εμπλοκή στον τρέχοντα δρόμο τους. Μπορείτε επίσης να δείτε την μέθοδο αρχικοποίησης η οποία ορίζει sentMessage = false για αυτό το όχημα κατά την εκκίνηση της εφαρμογής.

Η μέθοδος onWSM καθορίζει την αντίδραση που υπάρχει στα δεδομένα που λαμβάνονται καλώντας την changeroute για να αποφύγει τον δρόμο για τον οποίο δέχθηκε πληροφορίες και αν η sentMessage είναι ακόμα false προγραμματίζει μια υπενθύμιση να στείλει ξανά το μήνυμα σε δύο δευτερόλεπτα και θέτοντας το sentMessage flag. Η handleSelfMsg καθορίζει τον τρόπο που αντιδρά σε τέτοιου είδους υπενθυμίσεις. Καλώντας την sendDown να στείλει το broadcast. (Κουκούτσης Ιωάννης, 2022)