ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια σε Αδόμητα Δίκτυα Οχημάτων

ΑΛΕΞΑΝΔΡΟΣ ΚΙΚΗΣ
Α.Μ. 711161110

Εισηγητής: Καθηγητής Ιωάννης Βογιατζής

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια σε Αδόμητα Δίκτυα Οχημάτων

ΑΛΕΞΑΝΔΡΟΣ ΚΙΚΗΣ
Α.Μ. 711161110

Εισηγητής:

Καθηγητής Ιωάννης Βογιατζής

Εξεταστική Επιτροπή:

Ιωάννης Βογιατζής, Καθηγητής

Ioannis Voyiatzis Digitally signed by Ioannis Voyiatzis Date: 2024.04.10 07:22:53 +02'00'

Δημήτριος Καλλέργης, Λέκτορας Εφ.

Digitally signed by Dimitrios Kallergis Date: 2024.04.05 19:55:56 +03'00'

Ζαχαρένια Γαροφαλάκη, Μέλος ΕΔΙΠ

Digitally signed by Zacharenia Garofalaki Date: 2024.04.05 22:21:00 +03'00'

Ημερομηνία εξέτασης: 22-03-2024

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Κίκης Αλέξανδρος του Φιλίππου, με αριθμό μητρώου 711161110 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ioannis Voyiatzis

Digitally signed by Ioannis Voyiatzis
Date: 2024.04.10 07:24:34 +02'00'

Ο Δηλών

A. Kikis

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της ασφάλειας των αδόμητων δικτύων οχημάτων. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου, τον οποίο θα ήθελα να ευχαριστήσω. Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για τη συμπαράσταση κατά τη διάρκεια των σπουδών μου.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Τα αδόμητα δίκτυα οχημάτων επιτρέπουν την επικοινωνία οχημάτων σταθερής ή μεταβαλλόμενης τροχιάς με τη χρήση πρωτοκόλλων τα οποία είτε απαιτούν τη διαμεσολάβηση σταθμών βάσης είτε όχι. Ενώ η εξέλιξη της τεχνολογίας έχει επιφέρει πληθώρα οφελών στον τομέα των αδόμητων δικτύων οχημάτων, όπως βελτίωση της ασφάλειας και της ευχρηστίας, έχουν εμφανιστεί και νέες προκλήσεις, ιδίως σε ό,τι αφορά την ασφάλεια.

Λαμβάνοντας υπόψη τα γνωστά από τη βιβλιογραφία ζητήματα ασφάλειας οχηματικών δικτύων, η παρούσα διπλωματική εστιάζει σε περιπτώσεις επιθέσεων με σενάρια κίνησης οχημάτων στον αστικό ιστό. Μέσω προσομοιώσεων και αναλύσεων, εξετάζονται οι επιπτώσεις των διαφόρων τύπων επιθέσεων στην ασφάλεια των αδόμητων δικτύων οχημάτων. Ο στόχος είναι η ανάπτυξη των προσομοιώσεων αυτών με σκοπό την εξαγωγή συμπερασμάτων για τον αντίκτυπο, τον οποίο έχουν τα ζητήματα αυτά σε ένα πραγματικό αδόμητο οχηματικό δίκτυο.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Αδόμητα δίκτυα οχημάτων, Πρωτόκολλα επικοινωνίας, ζητήματα ασφάλειας.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Οχήματα, αδόμητα δίκτυα οχημάτων, ζητήματα ασφάλειας, επιθέσεις, σταθμοί βάσης.

ABSTRACT

Vehicular Ad-Hoc Networks enable communication among vehicles on either fixed or changing trajectories using protocols that may or may not require base station mediation. While technological advancements have brought a plethora of benefits to the field of unstructured vehicular networks, such as improved safety and usability, new challenges have emerged, particularly regarding security.

Considering well-known security issues from the literature, this thesis focuses on scenarios of attacks involving vehicular movement in urban environments. Through simulations and analyses, the impacts of various types of attacks on the security of unstructured vehicular networks are examined. The objective is to develop these simulations to draw conclusions about the impact of these issues on a real-world Vehicular Ad-Hoc Network.

Πίνακας περιεχομένων

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

VANET	Vehicular Ad-Hoc Network
RSU	Road-Side Unit
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
OBU	On-Board Unit
AU	Application Unit
GPRS	General Packet Radio Service
DSRC	Dedicated Short Range Communication
LTE	Long Term Evolution
GSM	Global System for Mobile Communications
TDMA	Time Division Multiple Access
FDMA	Frequency Division Multiple Access
UTMS	Universal Mobile Telecommunications System
WAVE	Wireless Access in Vehicular Enviroment
CCH	Control Channel
SCH	Service Channel
MIMO	Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
CPE	Customer Premises Equipment
VoIP	Voice over IP
ISM	Industrial Scientific and Medical
FHSS	Frequency Hopping Spread Sprectrum
PAN	Personal Area Network
SSP	Secure Simple Pairing
IEEE	Institute of Electrical and Electronics Engineers
VLC	Visible Light Communication
IR	Infrared Radiotation
UV	Ultraviolet
ITS	Intelligent Transport System
DDoS	Distributed Denial of Service

CVE	Common Vulnerabilities and Exposures
DoS	Denial of Service
CPU	Central Processing Unit
MiTM	Man in The Middle
SUMO	Simulation of Urban MObility
NED	NEtwork Description
IDE	Integrated Development Environment
AODV	Ad hoc On Demand Distance Vector
OSLR	Optimized Link State Routing
GUI	Graphical User Interface
TRACI	Traffic Control Interface
SCEP	Simple Certificat Enrollment Protocol
OTP	One Time Password
OBD	On Board Diagnostics

Κεφάλαιο 1: Εισαγωγή

1.1 Πρόβλημα

Σε μια εποχή, η οποία χαρακτηρίζεται από διαρκείς τεχνολογικές εξελίξεις, οι αλλαγές στα συστήματα μεταφοράς αποτελούν ένα σημαντικό κομμάτι στη δημιουργία έξυπνων και διασυνδεδεμένων πόλεων. Τα αδόμητα οχηματικά δίκτυα (VANETs) είναι μέρος αυτής της αλλαγής και θεωρούνται ως μια ελπιδοφόρα τεχνολογία. Στόχος των αδόμητων οχηματικών δικτύων είναι η βελτίωση της οδικής ασφάλειας, της κυκλοφοριακής αποδοτικότητας και της διευκόλυνσης των οδηγών. Οι στόχοι αυτοί πραγματοποιούνται μέσω της επικοινωνίας των οχημάτων μεταξύ τους και με τις παρόδιες μονάδες (RSUs), που υπάρχουν στο δίκτυο. Επιπλέον, τα αδόμητα οχηματικά δίκτυα θεωρούνται ικανά να αλλάξουν τον τρόπο, με τον οποίο κινούνται τα οχήματα εντός του αστικού ιστού μέσω α) της παροχής ενημερώσεων σε πραγματικό χρόνο για την κυκλοφορία, β) της διευκόλυνσης αποφυγής ατυχημάτων και γ) της υποστήριξης έξυπνων εφαρμογών.

Ωστόσο, όμως, μαζί με τα παραπάνω πλεονεκτήματα έρχονται και σημαντικές προκλήσεις. Η πιο σημαντική πρόκληση, που αντιμετωπίζουν τα αδόμητα οχηματικά δίκτυα, είναι αυτή της ασφάλειας. Από τη φύση τους τα αδόμητα οχηματικά δίκτυα είναι ευάλωτα σε απειλές και επιθέσεις ασφάλειας. Τα συστατικά των αδόμητων οχηματικών δικτύων συχνά επικοινωνούν ανταλλάσσοντας ευαίσθητες πληροφορίες, όπως η θέση, η ταχύτητα και ο προορισμός, γεγονός το οποίο τα καθιστά ελκυστικό στόχο κακόβουλων χρηστών. Επομένως, η διασφάλιση της ασφάλειας στα αδόμητα οχηματικά δίκτυα αποτελεί ζωτικής σημασίας, όχι μόνο για τους οδηγούς και τους επιβάτες αλλά και για την καθολική λειτουργία του δικτύου. Στην παρούσα διπλωματική εργασία, θα εστιάσουμε στα θέματα ασφαλείας, τα οποία παρατηρούνται στα αδόμητα οχηματικά δίκτυα δίνοντας έμφαση στις επιθέσεις, που είναι εφικτό να υλοποιηθούν σε αυτά.

1.2 Σκοπός και αντικείμενο μελέτης

Η παρούσα διπλωματική εργασία έχει ως στόχο τη διερεύνηση των ζητημάτων ασφαλείας, που παρουσιάζονται στα αδόμητα οχηματικά δίκτυα.

Αντικείμενο μελέτης αποτελεί η υλοποίηση σεναρίων επιθέσεων εντός του αστικού ιστού κάνοντας χρήση προσομοιωτών για πιο ρεαλιστικά αποτελέσματα και η ανάλυση αποτελεσμάτων της κάθε επίθεσης στο δίκτυο. Πιο συγκεκριμένα, εξετάζονται ζητήματα ασφάλειας, τα οποία προκύπτουν στα αδόμητα οχηματικά δίκτυα και στη συνέχεια πραγματοποιούνται προσομοιώσεις επιθέσεων, με σκοπό την ανάλυση των αποτελεσμάτων της κάθε επίθεσης στο δίκτυο.

1.3 Διάρθρωση μελέτης

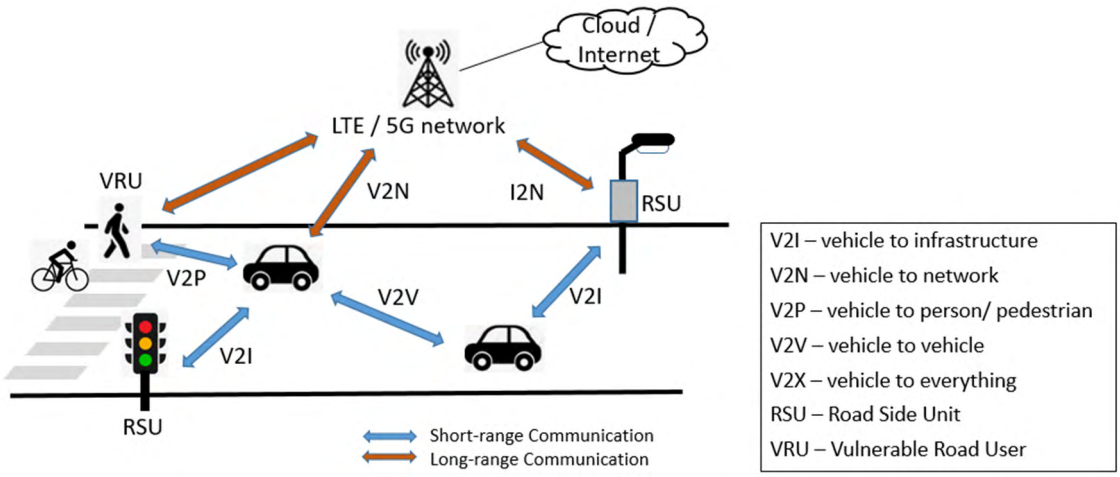
Η διπλωματική εργασία χωρίζεται σε 6 διακριτά κεφάλαια, τα οποία παρουσιάζονται παρακάτω:

- Στο πρώτο κεφάλαιο της εργασίας, παρουσιάζεται το αντικείμενο έρευνας, ο σκοπός, η συνεισφορά, καθώς επίσης και η διάρθρωση της μελέτης, που πραγματοποιήθηκε.
- Στο δεύτερο κεφάλαιο, αναλύεται το θεωρητικό υπόβαθρο της παρούσας διπλωματικής εργασία. Πιο συγκεκριμένα, γίνεται ανάλυση των αδόμητων οχηματικών δικτύων, των τεχνολογιών επικοινωνίας, που υπάρχουν σε αυτά, καθώς επίσης αναλύονται τα ζητήματα ασφαλείας, που υπάρχουν, σε συνδυασμό με τις επιθέσεις, οι οποίες μπορούν να υλοποιηθούν σε αυτά.
- Στο τρίτο κεφάλαιο, περιγράφονται τα εργαλεία και οι μέθοδοι, που χρησιμοποιήθηκαν, για να την υλοποίηση των προσομοιώσεων. Ειδικά, πραγματοποιείται ανάλυση των διαθέσιμων εργαλείων για την προσομοίωση των σεναρίων επίθεσης, όπως προσομοιωτές κίνησης, δικτύου και τα συνδυαστικά περιβάλλοντα.
- Στο τέταρτο κεφάλαιο, παρουσιάζεται ο τρόπος εργασίας, ο οποίος ακολουθήθηκε, για την υλοποίηση των προσομοιώσεων επίθεσης. Πιο συγκεκριμένα, παρουσιάζεται το σενάριο της κάθε επίθεσης, καθώς επίσης και τα εργαλεία, τα οποία χρησιμοποιήθηκαν, για την δημιουργία κίνησης και διασύνδεσης στους κόμβους της προσομοίωσης.
- Στο πέμπτο κεφάλαιο, αναλύονται τα αποτελέσματα, που προέκυψαν από την προσομοίωση της κάθε επίθεσης.
- Στο έκτο κεφάλαιο, παρουσιάζονται τα συμπεράσματα, που προέκυψαν από αυτήν την έρευνα, καθώς επίσης και πιθανές μελλοντικές επεκτάσεις, που μπορούν να εφαρμοστούν σε αυτή.

Κεφάλαιο 2: Θεωρητική προσέγγιση

2.1 Αρχιτεκτονική των αδόμητων οχηματικών δικτύων

Τα αδόμητα οχηματικά δίκτυα (VANETs) έχουν δυο κύριους τρόπους επικοινωνίας μεταξύ των συστατικών, που τα απαρτίζουν. Αρχικά, υπάρχει η επικοινωνία μεταξύ οχήματος και μιας παρόδιας μονάδας, η οποία ονομάζεται RSU (Road-Side Unit) και βρίσκεται τοποθετημένη σε κοντινή απόσταση με τις οδούς. Ο τρόπος αυτός, λοιπόν, χαρακτηρίζεται ως επικοινωνία οχήματος προς υποδομή (Vehicle to Infrastructure-V2I). Στη συνέχεια, ο δεύτερος τρόπος που παρατηρείται σε τέτοιου είδους δίκτυα, είναι η επικοινωνία όχημα προς όχημα (Vehicle to Vehicle-V2V), όπου η ανταλλαγή της πληροφορίας γίνεται μεταξύ των οχημάτων. Επιπλέον, υπάρχει και ο τρόπος επικοινωνίας οχήματος προς άλλες συσκευές (Vehicle to Everything-V2X), όπου γίνεται συνδυασμός των δύο παραπάνω, καθώς στην V2X επικοινωνία τα οχήματα στέλνουν και λαμβάνουν πληροφορίες, όχι μόνο από άλλα οχήματα ή παρόδιες μονάδες, αλλά και από άλλες οντότητες του δικτύου, όπως για παράδειγμα τους πεζούς ή φωτεινούς σηματοδότες.



Εικόνα 2.1 *Αρχιτεκτονική επικοινωνιών, όχημα προς όχημα (V2V), όχημα προς υποδομή (V2I), όχημα προς άλλες συσκευές (V2X) [3]*

Για να επιτευχθεί η δημιουργία ενός δικτύου, όπως στην Εικόνα 2.1, είναι απαραίτητο τα οχήματα να είναι εξοπλισμένα με μια επεξεργαστική μονάδα OBU (On Board Unit) και μια μονάδα εφαρμογών AU (Application Unit). Παράλληλα, είναι σημαντικό να επισημανθεί ότι η παρόδια μονάδα RSU (Road-Side Unit) είναι εξίσου απαραίτητη [1],[1].

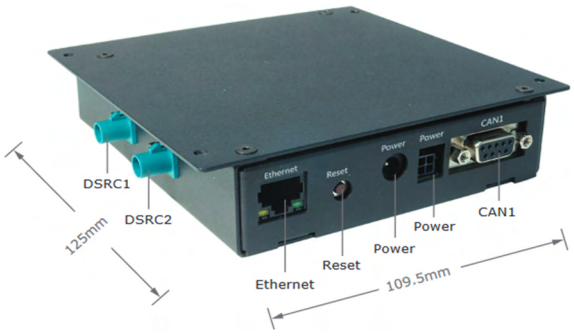
2.1.1 Επεξεργαστική Μονάδα OBU (On Board Unit)

Μια από τις σημαντικότερες συσκευές, που πρέπει να έχουν τα οχήματα εγκατεστημένη, είναι η επεξεργαστική μονάδα (OBU). Η μονάδα αυτή είναι συνήθως μικρού κόστους και συμβατή με

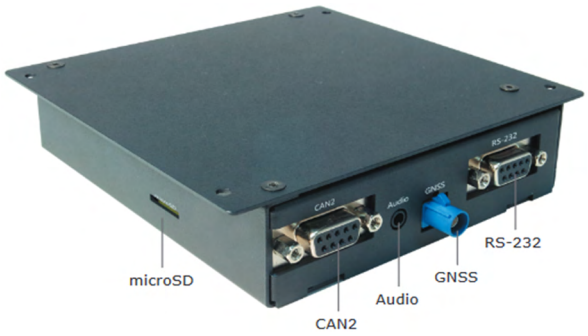
πολλών ειδών τεχνολογίες, ώστε να υπάρχει μεγάλη συνδεσιμότητα και να ικανοποιεί τα κριτήρια ενός αδόμητου οχηματικού δικτύου.

Οι κύριες λειτουργίες μιας τέτοιας μονάδας αφορούν την αποθήκευση της τρέχουσας τοποθεσίας του οχήματος, καθώς επίσης, και την απόσταση την οποία έχει διανύσει συνολικά, έτσι ώστε να μπορούν αυτές οι πληροφορίες να χρησιμοποιηθούν από κάποια εφαρμογή του συστήματος. Επιπλέον, οι λειτουργίες αφορούν την επικοινωνία με OBUs άλλων οχημάτων, είτε μέσα στο δίκτυο είτε με παρόδιες μονάδες (RSU), αλλά και την συλλογή δεδομένων από διάφορα είδη αισθητήρων, που βρίσκονται εγκατεστημένα στο όχημα, όπως επίσης και τη λήψη αποφάσεων, οι οποίες έχουν πρώτα μεταφερθεί και επεξεργαστεί από την εκάστοτε εφαρμογή (πχ εφαρμογές αποφυγής ατυχημάτων). Τέλος, πρέπει να τονιστεί ότι η OBU θα πρέπει να είναι σε θέση να παρέχει διαφόρων τύπων διεπαφές, όπως USB, RS-232 και Wi-Fi, ώστε να είναι εφικτή η επικοινωνία τόσο εσωτερικά του οχήματος όσο και με τον υπόλοιπο κόσμο.

Για να μπορούν να επιτευχθούν οι λειτουργίες που αναφέρονται παραπάνω, κρίνεται καίριο να επισημανθεί ότι η OBU αποτελείται από έναν επεξεργαστή, έναν πομπό, έναν δέκτη, μια μνήμη (ανάγνωσης/εγγραφής), διαφορετικού τύπου αισθητήρες, ένα γραφικό περιβάλλον για τον χρήστη και μια δικτυακή διεπαφή, η οποία θα πρέπει να βασίζεται στο IEEE 802.11p πρότυπο. Παρακάτω, στις Εικόνες 2.2α και 2.2β παρουσιάζονται δυο διαφορετικοί τύποι επεξεργαστικών μονάδων (OBU) [1],[4].



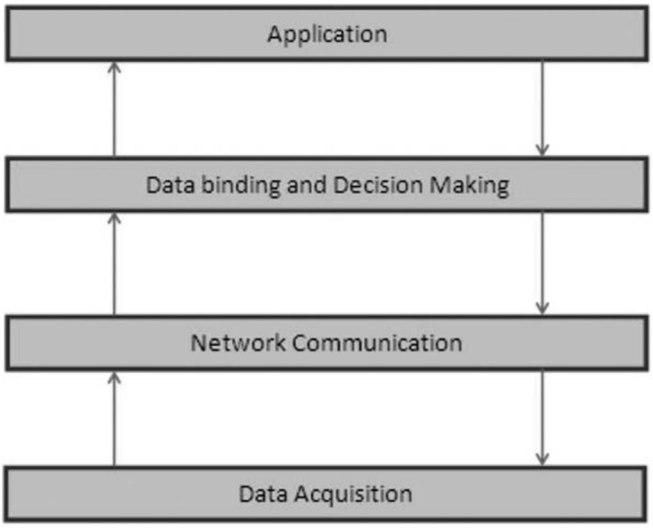
Εικόνα 2.2α *Επεξεργαστική μονάδα (OBU)*[1]



Εικόνα 2.2β *Επεξεργαστική μονάδα (OBU)*

[1] https://info.taiwantrade.com/EP/resources/member/1329/productcatalog/740799f5-fbec-4e08-91f2-b204e0edda3d.pdf

Στην Εικόνα 2.3 παρουσιάζεται ο τρόπος λειτουργίας μιας επεξεργαστικής μονάδας (OBU).



Εικόνα 2.3 *Τρόπος λειτουργίας επεξεργαστικής μονάδας OBU [1]*

2.1.2 Παρόδια μονάδα RSU (Road-Side Unit)

Ένα από τα χαρακτηριστικά των αδόμητων οχηματικών δικτύων, είναι το μέγεθός τους. Επομένως, τα οχήματα μπορεί να βρίσκονται σε πολύ μεγάλη απόσταση μεταξύ τους, κάτι που καθιστά την επικοινωνία μεταξύ των οχημάτων (V2V) σχεδόν αδύνατη. Ένα όχημα, το οποίο βρίσκεται σε μια πολύ μεγάλη απόσταση, δεν είναι ικανό να στείλει την απαραίτητη πληροφορία, (πχ για κάποιο ατύχημα που συνέβη), στα άλλα οχήματα του δικτύου, ώστε να τα ενημερώσει εγκαίρως. Για να λυθεί αυτό το πρόβλημα, λοιπόν, γίνεται η χρήση των παρόδιων μονάδων (RSU), οι οποίες βρίσκονται συνήθως τοποθετημένες σε σημεία κλειδιά ενός οδικού δικτύου, όπως για παράδειγμα σε κόμβους ή παραπλεύρως των οδών. Οι μονάδες αυτές έχουν, ως κύριο ρόλο, να επεκτείνουν την εμβέλεια του δικτύου, καθώς και να βελτιώσουν την απόδοση αυτού. Επίσης, οι χρήσεις μιας παρόδιας μονάδας δεν σταματούν εδώ, διότι μπορεί είτε να στείλει, είτε να προωθήσει μηνύματα σε οχήματα με τη βοήθεια των επεξεργαστικών μονάδων του κάθε οχήματος, εντός της εμβέλειας της, ενώ, παράλληλα, είναι ικανή να παρέχει πρόσβαση στο διαδίκτυο και στους κόμβους. Τέλος, έχει τη δυνατότητα να τρέχει εφαρμογές ασφαλείας, οι οποίες δέχονται τα δεδομένα, τα οποία αποστέλλουν τα οχήματα του δικτύου. Ο τρόπος με τον οποίο λειτουργεί μια RSU είναι ο εξής [1],[4]:

- Δέχεται μηνύματα (πακέτα) από τα οχήματα που βρίσκονται σε κατάλληλη εμβέλεια και τα στοιβάζει σε μια ουρά, όπου στην συνέχεια, βάσει προτεραιότητας, επεξεργάζεται.
- Στην συνέχεια, οι απαντήσεις, που είναι έτοιμες προς αποστολή, στοιβάζονται και αυτές σε μια ουρά, όπου στέλνονται με βάση την προτεραιότητά τους.
- Η προτεραιότητα, τόσο των πακέτων που λαμβάνονται, όσο και των απαντήσεων, ορίζεται από έναν χρονοπρογραμματιστή.

Στην Εικόνα 2.4 παρουσιάζεται μια παρόδια μονάδα (RSU).

Εικόνα 2.4 *Παρόδια μονάδα (RSU)* [2]

2.1.3 Μονάδα εφαρμογών AU (Application Unit)

Τα οχήματα, τα οποία απαρτίζουν ένα αδόμητο οχηματικό δίκτυο, είναι ικανά να τρέξουν πολλών ειδών εφαρμογές, οι οποίες έχουν ως στόχο να βοηθήσουν ή να προειδοποιήσουν τους οδηγούς, όπως για παράδειγμα οι εφαρμογές ασφαλείας. Για να επιτευχθεί αυτό, γίνεται χρήση μιας ξεχωριστής μονάδας η οποία ονομάζεται μονάδα εφαρμογών (AU). Τη μονάδα εφαρμογών την τοποθετούν στα οχήματα με σκοπό να τρέχει τις εφαρμογές, που παρέχει ο εκάστοτε πάροχος. Το είδος της μονάδας αυτής διαφέρει, καθώς μπορούμε να την εντοπίσουμε αφενός ως συσκευή, η οποία επιτελεί λειτουργίες αποκλειστικά για εφαρμογές ασφαλείας ή άλλου παρόμοιου είδους εφαρμογές και αφετέρου ως μια απλή έξυπνη συσκευή, η οποία έχει την δυνατότητα να συνδέεται και στο διαδίκτυο. Η μονάδα εφαρμογών συνεργάζεται στενά με την επεξεργαστική μονάδα, όπως αναλύεται παραπάνω, ώστε να επιτευχθούν οι λειτουργίες τους, ενώ ταυτόχρονα η συνεργασία αυτή επιτυγχάνεται μέσω της ενσύρματης ή ασύρματης διασύνδεσης. Σε πολλές περιπτώσεις, τόσο η μονάδα εφαρμογών όσο και η επεξεργαστική μονάδα μπορεί να βρίσκονται σε μια ενιαία μονάδα [4],[5].

2.2 Χαρακτηριστικά των αδόμητων οχηματικών δικτύων

Όπως αναφέρθηκε, σε ένα αδόμητο οχηματικό δίκτυο παρατηρούμε από τη μία τα οχήματα, τα οποία κινούνται σε μεγάλες ταχύτητες, και από την άλλη, τις παρόδιες μονάδες, οι οποίες είναι

[2] https://uploads-ssl.webflow.com/5d0d3167acec7aeffe71a888/5f6b177b2c8d3b8f043f14da_CV_RoadsideUnit.pdf

σταθερές. Λόγω της αρχιτεκτονικής στην οποία βασίζονται τα δίκτυα αυτά, έχουν συγκεκριμένα χαρακτηριστικά συγκριτικά με κάθε άλλου είδους δίκτυο, τα οποία βοηθούν στη διασφάλιση της ασφάλειας και της ιδιωτικότητας. Τα χαρακτηριστικά αυτά αναλύονται παρακάτω [6].

2.2.1 Υψηλή κινητικότητα

Τα οχήματα θεωρούνται ως το βασικό συστατικό ενός αδόμητου οχηματικού δικτύου. Μέσα σε ένα οδικό δίκτυο η ταχύτητα κίνησης των κόμβων μεταβάλλεται διαρκώς από τα 30 έως τα 200χλμ., κάτι το οποίο πολλές φορές δημιουργεί προβλήματα, όταν πρόκειται για πολύ μεγάλες ή πολύ μικρές ταχύτητες. Αυτό συμβαίνει, διότι τα οχήματα θα πρέπει να προσαρμόσουν τις παραμέτρους επικοινωνίας, με τις οποίες λειτουργούν, λόγω του μικρού χρονικού διαστήματος που δημιουργείται για την αποστολή πληροφοριών σε άλλα οχήματα [1],[4],[5],[6],[7],[8].

2.2.2 Γρήγορες εναλλαγές τοπολογίας

Μέσα σε ένα οδικό δίκτυο υπάρχουν πολλοί παράγοντες, οι οποίοι επηρεάζουν τον τρόπο με τον οποίο κινείται ένα όχημα. Μερικοί από αυτούς τους παράγοντες είναι οι δρόμοι ταχείας κυκλοφορίας, όπου οι οδηγοί αναπτύσσουν μεγάλες ταχύτητες και τα εμπόδια που συναντά ένα όχημα, που βρίσκεται εντός μιας πόλης (π.χ. τα κτήρια), τα οποία αλλοιώνουν την ποιότητα σήματος από και προς αυτό. Λόγω των παραπάνω παραγόντων, υπάρχει διαρκής και ταχεία εναλλαγή στην τοπολογία του δικτύου [4],[5],[6],[7],[8].

2.2.3 Προβλέψιμη κινητικότητα

Τα VANETs είναι ένα είδος αδόμητου δικτύου, ωστόσο, διαφέρει με τα υπόλοιπα δίκτυα της ίδια κατηγορίας, επειδή οι κόμβοι του δεν μπορούν να κινηθούν σε εντελώς τυχαίες τοποθεσίες. Αυτό συμβαίνει, διότι τα οχήματα κινούνται στο πλαίσιο ενός οδικού δικτύου, το οποίο απαρτίζεται από οδούς, φανάρια και σήματα. Επομένως, στην περίπτωση που γνωρίζουμε τον δρόμο, κατά μήκος του οποίου κινείται ένα όχημα, όπως και την ταχύτητα κίνησης, είναι εύκολο να προβλέψουμε την τοποθεσία αυτού [1],[4],[5],[6],[8].

2.2.4 Μέγεθος δικτύου

Το μέγεθος του δικτύου αποτελεί ένα ακόμα χαρακτηριστικό των αδόμητων οχηματικών δικτύων, καθώς μπορεί να είναι αρκετά μεγάλο σε οδούς ταχείας κυκλοφορίας, σε κεντρικά σημεία μιας πόλης ή ακόμα και στην είσοδο αυτής [6].

2.2.5 Πυκνότητα δικτύου

Ο τρόπος με τον οποίο επιτρέπεται να κινούνται τα οχήματα μέσα σε ένα οδικό δίκτυο, έχει ως αποτέλεσμα, σε πολλές περιοχές του δικτύου, να συγκεντρώνεται μεγάλος αριθμός οχημάτων και έτσι, να αυξάνεται η πυκνότητά του στο συγκεκριμένο σημείο. Λόγω του τρόπου με τον οποίο επικοινωνούν τα οχήματα, σε σημεία, όπου παρατηρείται μεγάλη συγκέντρωση κόμβων, υπάρχει δυσκολία στην διάδοση της πληροφορίας και στη λειτουργία των εφαρμογών, που τρέχουν σε κάθε όχημα. Επομένως, αυτό καθιστά την πυκνότητα του δικτύου, ένα επίσης σημαντικό χαρακτηριστικό [7].

2.2.6 Ενεργειακή διαθεσιμότητα

Ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν αρκετοί τύποι δικτύων, είναι οι περιορισμένοι ενεργειακοί πόροι, καθώς σε πολλές περιπτώσεις οι κόμβοι είναι ηλεκτρικές συσκευές, όπως κινητά και φορητοί υπολογιστές. Οι συσκευές αυτές έχουν μικρής χωρητικότητας μπαταρίες, με αποτέλεσμα, οι υπολογιστικές τους δυνατότητες να είναι περιορισμένες. Στα αδόμητα οχηματικά δίκτυα αυτό το ζήτημα έχει λυθεί, εφόσον οι κόμβοι είναι οχήματα, τα οποία έχουν μεγάλης χωρητικότητας μπαταρίες, οι οποίες μπορούν να αποδίδουν διαρκώς ενέργεια στην επεξεργαστική μονάδα του οχήματος, διότι επιτρέπουν τη χρήση συσκευών με μεγαλύτερη υπολογιστική ισχύ [1],[4],[5].

2.2.7 Υψηλή υπολογιστική ισχύ

Ένα ακόμα χαρακτηριστικό των αδόμητων οχηματικών δικτύων είναι η υψηλή υπολογιστική ισχύ, την οποία διαθέτουν. Αυτό προκύπτει από το γεγονός, ότι οι κόμβοι του δικτύου είναι οχήματα, όπου τα τελευταία χρόνια οι κατασκευαστές τους είναι ικανοί να τα εξοπλίσουν με μεγάλους χώρους αποθήκευσης αρχείων και εφαρμογών, τελευταίας γενιάς αισθητήρες, πρόσβαση στο διαδίκτυο, με σύστημα GPRS και άλλες τεχνικές επικοινωνίας. Όλα αυτά συντελούν με τέτοιο τρόπο, ώστε τα οχήματα να έχουν αυξημένες δυνατότητες, όσον αφορά την υπολογιστική ισχύ [4],[5],[7].

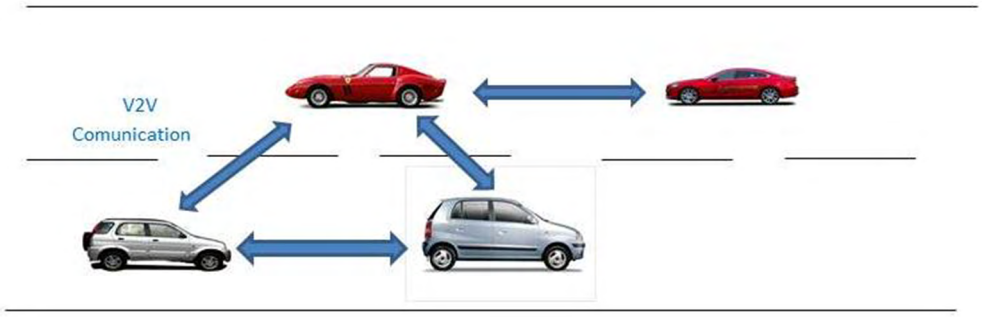
2.3 Τύποι επικοινωνίας

Τα αδόμητα οχηματικά δίκτυα θεωρούνται ως η εξέλιξη των αδόμητων κινητών δικτύων και έχουν ως στόχο την βελτίωση της οδικής ασφάλειας και της αποδοτικότητας, μέσω της ανταλλαγής χρήσιμων πληροφοριών, ανάμεσα στους κόμβους που απαρτίζουν το δίκτυο. Τα αδόμητα οχηματικά δίκτυα διαφέρουν από τα υπόλοιπα αδόμητα δίκτυα (ad-hoc networks) λόγω του ότι οι κόμβοι τους είναι οχήματα, τα οποία κινούνται σε μεγάλες ταχύτητες και παρόδιες μονάδες (RSU). Παρακάτω

αναλύονται οι βασικοί τύποι επικοινωνίας, που παρατηρούνται μεταξύ των κόμβων, η επικοινωνία μεταξύ οχημάτων Vehicle to Vehicle (V2V), η επικοινωνία μεταξύ οχημάτων και υποδομής Vehicle to Infrastructure (V2I) και επικοινωνία οχημάτων με τα πάντα Vehicle to Everything (V2X) [1],[4],[5],[7],[9].

2.3.1 Επικοινωνία όχημα προς όχημα (Vehicle to Vehicle-V2V)

Τα αδόμητα δίκτυα βασίζονται στην επικοινωνία μεταξύ των κόμβων, που, σε πολλές περιπτώσεις, δεν είναι αναγκαία η σταθερή υποδομή. Η ανταλλαγή των πληροφοριών γίνεται ανάμεσα στα οχήματα, με βασική προϋπόθεση το όχημα να βρίσκεται στην εμβέλεια μετάδοσης κάποιου άλλου οχήματος. Στην επικοινωνία μεταξύ οχημάτων (V2V) γίνεται χρήση της τεχνικής hop to hop, όπου το μήνυμα, μέχρι να φτάσει στον τελικό του προορισμό, κάνει μια σειρά από "άλματα", δηλαδή μεταφέρεται από κόμβο σε κόμβο μέχρι τον τελικό αποδέκτη. Για να επιτευχθεί μια επικοινωνία μεταξύ οχημάτων (V2V), τα οχήματα χρησιμοποιούν κάποια πρωτόκολλα επικοινωνίας, όπως το DSRC (Dedicated Short Range Communication) πρωτόκολλο, το Wi-Fi και το Bluetooth. Στην Εικόνα 2.5 παρουσιάζεται η επικοινωνία όχημα προς όχημα (V2V) [1],[6],[7],[10].

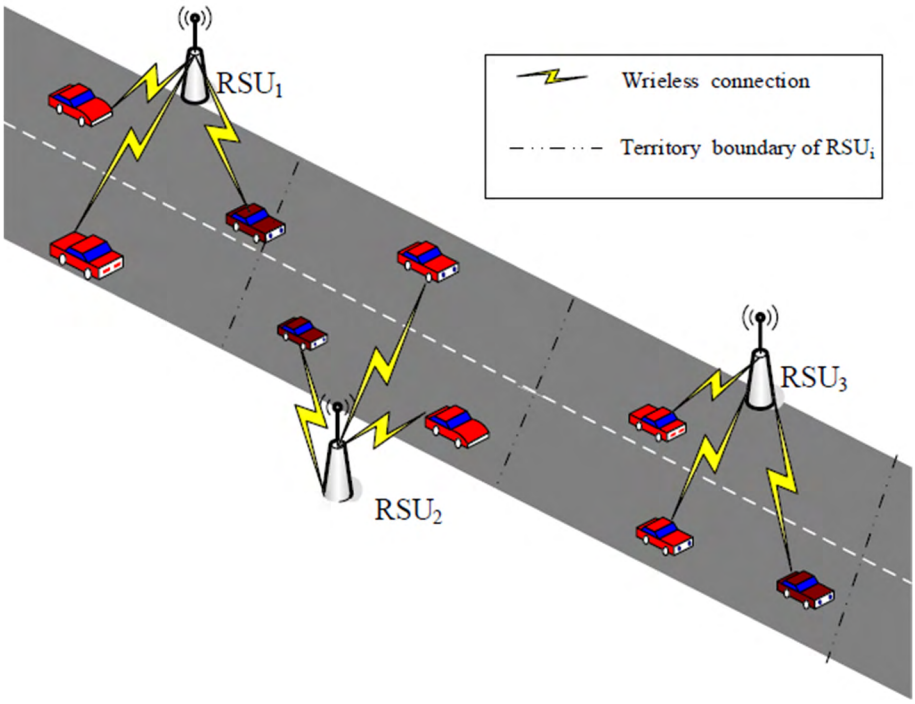


Εικόνα 2.5 *Επικοινωνία όχημα προς όχημα (V2V-Vehicle to Vehicle) [11]*

2.3.2 Επικοινωνία όχημα προς υποδομή (Vehicle to Infrastructure-V2I)

Ένας ακόμα τύπος επικοινωνίας, που παρατηρείται στα αδόμητα οχηματικά δίκτυα, είναι η επικοινωνία οχήματος προς την υποδομή (Vehicle to Infrastructure-V2I). Η αρχή της επικοινωνίας αυτής γίνεται, όταν ένα όχημα βρεθεί στην εμβέλεια εκπομπής μιας παρόδιας μονάδας (RSU), όπου τα οχήματα στέλνουν διαφόρων ειδών αιτήματα και η παρόδια μονάδα επιστρέφει κάποια απάντηση. Ωστόσο, δεν είναι αυτή η μοναδική χρήση μιας παρόδιας μονάδας σε μια τέτοιου είδους επικοινωνία, διότι, στην περίπτωση που ένα όχημα θέλει να επικοινωνήσει με κάποιο άλλο εκτός της εμβέλειας του, τότε παρεμβάλλεται η παρόδια μονάδα, η οποία είτε προωθεί το μήνυμα στο όχημα είτε με την σειρά της το προωθεί σε κάποια άλλη παρόδια μονάδα, ώστε να φτάσει στον τελικό

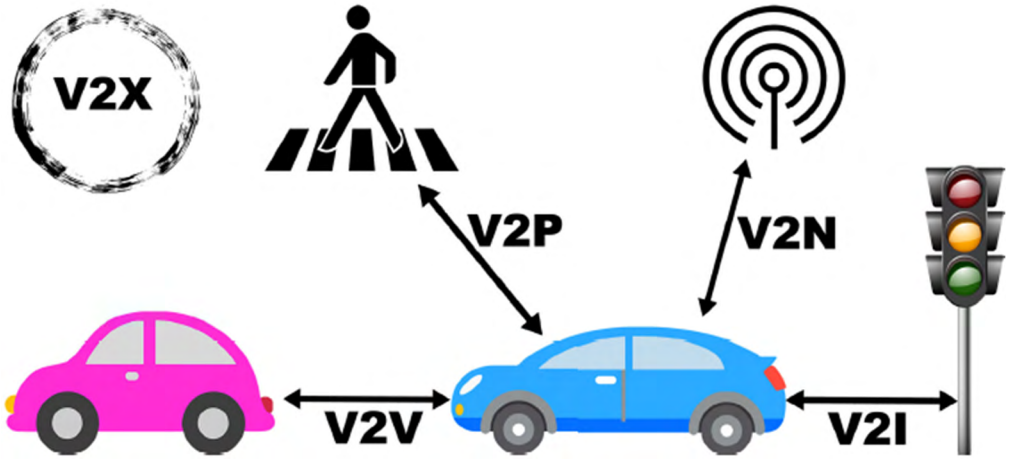
παραλήπτη. Ο V2I τρόπος δεν χαρακτηρίζεται ως πλήρως αδόμητος αλλά ως μερικώς, καθώς οι παρόδιες μονάδες δεν κινούνται και παραμένουν σταθερές. Τέλος για την επικοινωνία μεταξύ οχημάτων και παρόδιας μονάδας γίνεται η χρήση των πρωτοκόλλων Wi-Fi, DSRC και Bluetooth. Στην Εικόνα 2.6 παρουσιάζεται ο V2I τρόπος επικοινωνίας [1],[7],[12].



Εικόνα 2.6 *Επικοινωνία όχημα προς υποδομή (V2I-Vehicle to Infrastructure) [12]*

2.3.3 Επικοινωνία όχημα προς άλλες συσκευές (Vehicle to Everything-V2X)

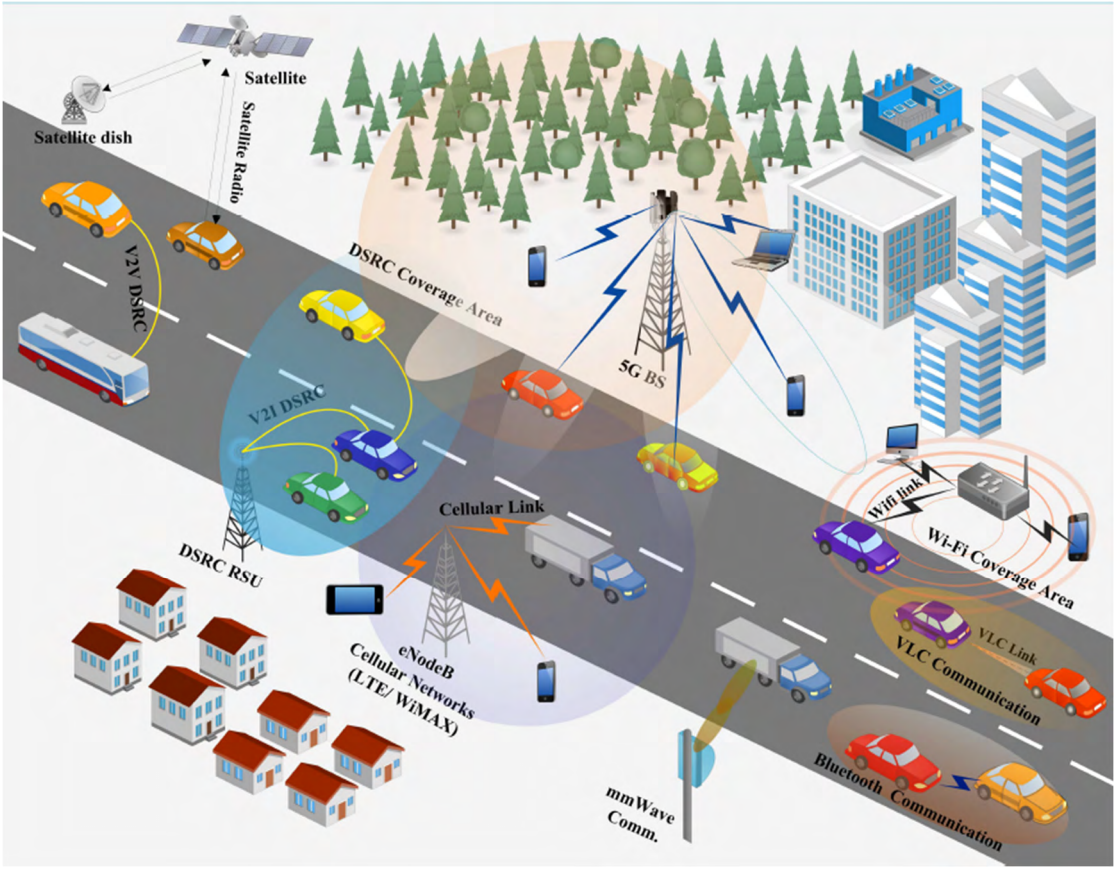
Ο τελευταίος τύπος επικοινωνίας είναι η επικοινωνία οχήματος προς άλλες συσκευές (Vehicle to Everything-V2X). Με τον όρο Vehicle to Everything, εννοούμε την επικοινωνία κατά την οποία τα οχήματα μπορούν να στέλνουν και να λαμβάνουν πληροφορίες σχετικά με την ταχύτητα και την τοποθεσία τους από διάφορες οντότητες ενός οδικού δικτύου, όπως για παράδειγμα, τους φωτεινούς σηματοδότες, τους ποδηλάτες και τους πεζούς. Τα δύο βασικότερα συστατικά της αρχιτεκτονικής αυτής της επικοινωνίας είναι η επικοινωνία μεταξύ οχημάτων (V2V), καθώς και η επικοινωνία οχημάτων προς την υποδομή (V2I). Για να επιτευχθεί η V2X γίνεται χρήση των τεχνολογιών Wi-Fi, DSRC και 4G LTE. Η V2X μπορεί να συμβάλλει στη βελτίωση της ασφάλειας ενός οδηγού, στην μείωση κατανάλωσης καυσίμου και στη γενικότερη εμπειρία χρήσης του οδικού δικτύου από κάποιον χρήστη, που δεν είναι απαραίτητα οδηγός αυτοκινήτου. Στην Εικόνα 2.7 παρουσιάζεται η επικοινωνία οχήματος με άλλες συσκευές (V2X) [9],[13],[14],[15],[16].



Εικόνα 2.7 *Επικοινωνία οχήματος με άλλες συσκευές (V2X-Vehicle to Everything) [16]*

2.4 Τεχνολογίες επικοινωνίας στα αδόμητα οχηματικά δίκτυα

Για να επιτευχθούν οι τρόποι επικοινωνίας, που παρατηρούμε σε ένα αδόμητο οχηματικό δίκτυο, όπως η επικοινωνία των οχημάτων μεταξύ τους (V2V), η επικοινωνία των οχημάτων με άλλες οντότητες του οδικού δικτύου (V2X) και η επικοινωνία των οχημάτων με παρόδιες μονάδες (V2I), είναι απαραίτητη η χρήση διαφόρων τεχνολογιών διασύνδεσης. Η διασύνδεση αυτή των συστατικών του δικτύου επιτυγχάνεται με σκοπό τη βελτίωση διαφόρων τομέων μέσα στο οδικό δίκτυο, μέσω εφαρμογών που τρέχουν στα συστήματα των οχημάτων και όχι μόνο. Οι τεχνολογίες, οι οποίες χρησιμοποιούνται και γίνεται αναφορά σε αυτές, διαφέρουν μεταξύ τους, καθώς κάποιες από αυτές λειτουργούν με βάση τις αρχές της αδόμητης επικοινωνίας (ad-hoc) και κάποιες χρειάζονται υποδομή, ώστε να λειτουργήσουν. Στην συνέχεια, αναλύονται μερικές από τις σημαντικότερες τεχνολογίες, που παρατηρούνται στα αδόμητα οχηματικά δίκτυα. Στην Εικόνα 2.8 απεικονίζονται οι τεχνολογίες, που θα αναλυθούν παρακάτω. Επίσης ο Πίνακας 2.1 απεικονίζει τη σύγκριση των τεχνολογιών αυτών.



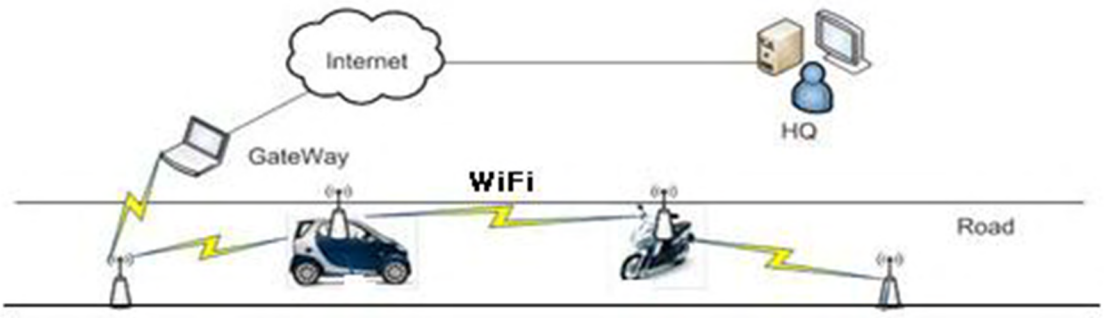
Εικόνα 2.8 *Τεχνολογίες επικοινωνίας στα αδόμητα οχηματικά δίκτυα (VANETs) [17]*

2.4.1 Wi-Fi/WLAN

Η τεχνολογία Wi-Fi βασίζεται στην οικογένεια προτύπων IEEE 802.11, όπου στις αρχές του λειτουργούσε σε ένα μη αδειοδοτημένο φάσμα με ρυθμό μετάδοσης δεδομένων ανάμεσα σε 1 και 2 Mbps. Οι προδιαγραφές, τις οποίες έχει τόσο σε φυσικό επίπεδο, όσο και σε επίπεδο MAC, κάνουν την τεχνολογία του Wi-Fi κατάλληλη, τόσο για επικοινωνία που αφορά μόνο τα οχήματα του δικτύου (V2V), όσο και για επικοινωνία με παρόδιες μονάδες (V2I) [18].

Τα πρότυπα αναβαθμίζονται συνεχώς και για τον λόγο αυτό, δημιουργήθηκε το πρότυπο IEEE 802.11a, όπου λειτουργεί στο φάσμα των 5GHz και είναι ικανό να παρέχει ρυθμό μετάδοσης δεδομένων από 6 έως 54 Mbps. Το πρότυπο αυτό έχει εμβέλεια από 100 έως 300 μέτρα ανάλογα με τα εμπόδια που παρεμβάλλονται. Αμέσως μετά από το πρότυπο IEEE 802.11a, ακολουθεί το IEEE 802.11b, το οποίο λειτουργεί στο φάσμα των 2.4GHz και είναι ικανό να παρέχει ρυθμό μετάδοσης δεδομένων, που φτάνει τα 11 Mbps. Το πιο βελτιωμένο πρότυπο αυτής της οικογενείας είναι το IEEE 802.11g, το οποίο λειτουργεί στο φάσμα των 2.4 GHz, καθώς έχει προς τα πίσω συμβατότητα με το b πρότυπο και ρυθμό μετάδοσης δεδομένων ίδιο με το πρότυπο a, δηλαδή 54 Mbps. Τα οχήματα που λειτουργούν με Wi-Fi εντός ενός αδόμητου οχηματικού δικτύου, μπορούν να αναπτύξουν ταχύτητα μέχρι 250 χλμ. ανά ώρα. Το Wi-Fi προσφέρει σχετικά μικρή καθυστέρηση, σε σχέση με τις άλλες

τεχνολογίες που υπάρχουν διαθέσιμες για ένα οχηματικό δίκτυο, με την καθυστέρηση να κυμαίνεται από 3 έως 10 ms. Επιπλέον, η τεχνολογία Wi-Fi παρέχει και μηχανισμό ασφαλείας με τα πρωτόκολλα TLS και SSL, κάτι που την καθιστά ασφαλέστερη από άλλες τεχνολογίες. Τέλος, για να επιτευχθεί η επικοινωνία μέσω Wi-Fi σε ένα δίκτυο, είναι απαραίτητη η ύπαρξη σταθερής υποδομής. Στην Εικόνα 2.9 παρουσιάζεται η διασύνδεση με χρήση Wi-Fi [18],[19].



Εικόνα 2.9 *Διασύνδεση μέσω Wi-Fi [18]*

2.4.2 Κυψελοειδείς επικοινωνίες

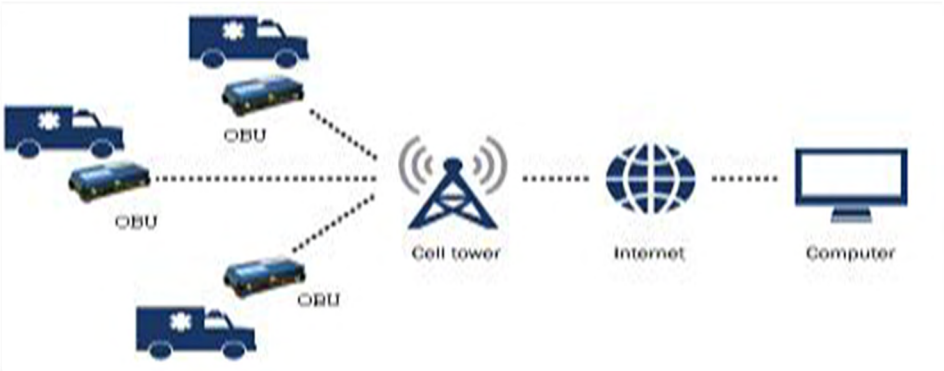
Μια οικογένεια τεχνολογιών επικοινωνίας που συναντάμε, επίσης, στα αδόμητα οχηματικά δίκτυα, είναι αυτή των κυψελοειδών επικοινωνιών. Τέτοιου είδους τεχνολογίες ενσωματώνονται διαρκώς στην καθημερινότητα των χρηστών, καθώς εξελίσσονται με ταχύτατους ρυθμούς. Στην ιδέα της επαναχρησιμοποίησης της περιορισμένης συχνότητας βασίζονται οι κυψελοειδής τεχνολογίες. Η πιο διαδεδομένη μορφή για κινητές συσκευές θεωρείται το παγκόσμιο σύστημα κινητών επικοινωνιών (GSM), το οποίο, σε φυσικό επίπεδο, κάνει χρήση τόσο της πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), όσο και της πολλαπλής πρόσβασης διαίρεσης συχνότητας (FDMA). Το GSM λειτουργεί σε δυο ζώνες συχνοτήτων: α) τη ζώνη 890-915 MHz, η οποία χρησιμοποιείται για εκπομπή από τις κινητές συσκευές και β) τη ζώνη 935-960 MHz, η οποία χρησιμοποιείται για εκπομπή από τους σταθμούς βάσης και είναι ικανή να παρέχει ρυθμό μετάδοσης δεδομένων μέχρι 9.6Kbps. Η κάθε ζώνη συχνοτήτων, που αναφέραμε, χωρίζεται σε επιμέρους κανάλια, των οποίων η χωρητικότητα είναι 200 KHz. Ένα πολύ σημαντικό χαρακτηριστικό του GSM που το κάνει κατάλληλο για χρήση σε αδόμητα οχηματικά δίκτυα, είναι η δυνατότητα της μεταπομπής, το οποίο είναι χρήσιμο λόγω της διαρκούς κίνησης που έχουν οι κόμβοι.

Η οικογένεια των κυψελοειδών τεχνολογιών εξελίσσεται με ταχύτατους ρυθμούς, έτσι, την εξέλιξη του GSM αποτελεί το GPRS, το οποίο είναι ικανό να υποστηρίξει ρυθμούς μετάδοσης δεδομένων μέχρι 140.8 Kbps, όπως επίσης και μειωμένους χρόνους πρόσβασης. Οι ζώνες συχνοτήτων, που λειτουργεί το GPRS, είναι οι ίδιες με το GSM, δηλαδή οι 890-915 MHz και 935-960 MHz, όμως μπορεί να λειτουργήσει και στις ζώνες 1710-1785 MHz και 1805-1880 MHz. Μια βελτίωση

τόσο του GSM, όσο και του GPRS αποτελεί το EDGE, το οποίο παρέχει ρυθμούς μετάδοσης δεδομένων μέχρι 180 Kbps.

Η επόμενη μεγάλη εξέλιξη είναι το παγκόσμιο σύστημα κινητών τηλεπικοινωνιών (UTMS), το οποίο παρέχει δυνατότητες λήψης εικόνας και ήχου σε πραγματικό χρόνο. Είναι ικανό να προσφέρει ρυθμούς μετάδοσης δεδομένων, που αγγίζουν τα 2 Mbps, και μικρές καθυστερήσεις, όσον αφορά τη λήψη πακέτων. Το UTMS λειτουργεί στις ζώνες συχνοτήτων 1885-2025 MHz.

Τέλος, τις τελευταίες εξελίξεις αποτελούν τα δίκτυα μακροχρόνιας εξέλιξης (LTE) ή αλλιώς τα 4G δίκτυα και τα νεότερα 5G δίκτυα. Τα 4G δίκτυα λειτουργούν στις ζώνες συχνοτήτων από 450 MHz έως 3.8 GHz και είναι ικανά να προσφέρουν ρυθμό μετάδοσης δεδομένων έως και 300 Mbps. Τα 5G δίκτυα αποτελούν την πιο σύγχρονη έκδοση κυψελοειδών δικτύων, με αποτέλεσμα να βρίσκονται υπό διαρκή ανάπτυξη. Λειτουργούν σε ένα εύρος συχνοτήτων από 450 MHz έως 6GHz, το οποίο περιέχει και το εύρος των LTE συχνοτήτων και από 24.25 GHz έως 52.5 GHz, το οποίο ονομάζεται mmWave φάσμα. Το 5G δίκτυα μπορούν να παρέχουν ρυθμό μετάδοσης δεδομένων έως τα 10 Gbps, όπως επίσης δίνουν και τη δυνατότητα στους κόμβους να αναπτύξουν ταχύτητες κοντά στα 500 χλμ. ανά ώρα, σε αντίθεση με τα δίκτυα 4G που επιτρέπουν μέχρι 200-300 χλμ. ανά ώρα. Στην εικόνα 2.10 παρουσιάζεται ένα παράδειγμα της κυψελοειδούς τεχνολογίας [18],[19],[20],[21],[22].



Εικόνα 2.10 *Κυψελοειδείς τεχνολογίες [18]*

2.4.3 Τεχνολογία DSRC/Wave

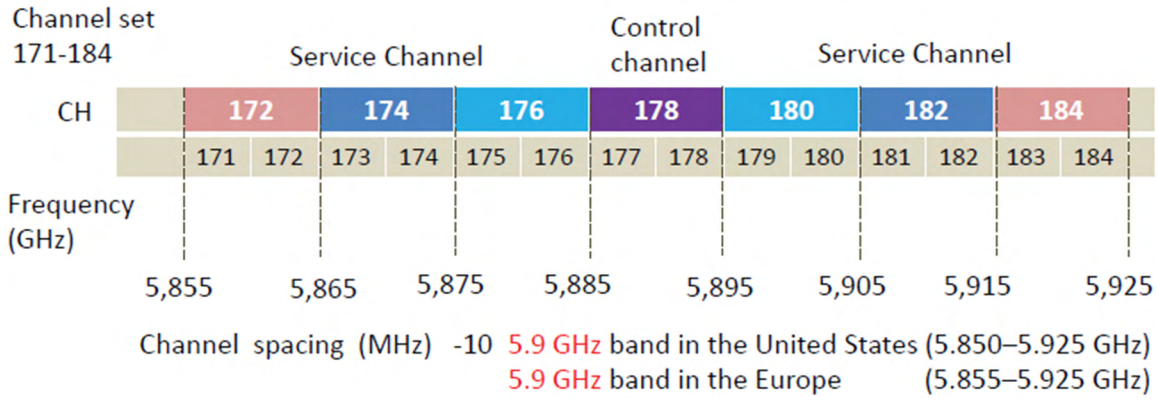
Η τεχνολογία DSRC/WAVE είναι ένα αδειοδοτημένο φάσμα των 75 MHz στην μπάντα των 5.9 GHz , το όποιο έχει καθοριστεί από την ομοσπονδιακή επιτροπή επικοινωνιών των ΗΠΑ (US FCC) το 1999 και έχει, ως κύριο στόχο, την επικοινωνία μεταξύ οχημάτων και υποδομών. Η τεχνολογία του DSRC βασίζεται στο πρότυπο 802.11p [18],[25].

Οι δύο ομάδες προτύπων οι οποίες είναι γνωστό ότι υποστηρίζουν εφαρμογές που κάνουν χρήση του DSRC, λειτουργούν σε δύο διαφορετικές ζώνες συχνοτήτων. Η πρώτη ομάδα προτύπων λειτουργεί στα 915 MHz και χρησιμοποιείται κυρίως από εφαρμογές εμπορικών οχημάτων και εφαρμογές διαχείρισης πληρωμής των διοδίων. Η δεύτερη ομάδα προτύπων, αυτή που λειτουργεί

στα 5.9 GHz, στοχεύει σε μια ευρύτερη ποικιλία εφαρμογών όπως i) η πρόληψη για πιθανή σύγκρουση, ii) ο προηγμένος έλεγχος οχημάτων, iii)οι πληροφορίες που αφορούν τους ταξιδιώτες, iv)η ενισχυμένη υποστήριξη σε ό,τι αφορά την μεταφορά αγαθών, v)οι δημόσιες θέσεις στάθμευσης, vi)η καλύτερη διαχείριση του μποτιλιαρίσματος, καθώς επίσης και vii)η υποστήριξη άλλων ιδιωτικών εφαρμογών.

Όσον αφορά την άμεση επικοινωνία μεταξύ οχημάτων V2V, το DSRC/WAVE πρότυπο θεωρείται ως το μοναδικό, που είναι ικανό να την υποστηρίξει. Οι ασύρματες υποδομές παρουσιάζουν μειονεκτήματα, τα οποία λύνει αποτελεσματικά το DSRC/WAVE πρότυπο, μέσω της χαμηλής καθυστέρησης που παρέχει και της επικοινωνίας, όταν οι κόμβοι κινούνται διαρκώς και με μεγάλη ταχύτητα. Το DSRC/WAVE μπορεί να χρησιμοποιηθεί, τόσο για επικοινωνίες μεταξύ οχημάτων, όσο και για επικοινωνίες μεταξύ οχημάτων και παρόδιων μονάδων. Επίσης, είναι ικανό να προσφέρει μεγάλο ρυθμό μετάδοσης δεδομένων, ο οποίος κυμαίνεται από τα 6 έως τα 27 Mbps σε εμβέλεια μέχρι 1 χλμ. καθώς και 7 αδειοδοτημένα κανάλια τα οποία ξεκινούν από τον αριθμό 172 και τελειώνουν στον αριθμό 184. Τα οχήματα τα οποία κάνουν χρήση του DSRC/WAVE, μπορούν να αναπτύξουν ταχύτητες έως και 300 χλμ. ανά ώρα.

Τέλος, υπάρχουν δυο είδη καναλιών όπου όλα έχουν το ίδιο πλάτος δηλαδή 10 MHz. Το πρώτο κανάλι ονομάζεται κανάλι ελέγχου (CCH) και αφορά κυρίως εφαρμογές ασφαλείας. Το δεύτερο κανάλι ονομάζεται κανάλι υπηρεσιών (SCH) και αφορά ταυτόχρονα και εφαρμογές ασφαλείας αλλά και άλλων ειδών εφαρμογές. Τα κανάλια με αριθμό 172 έως 184 χρησιμοποιούνται για επικοινωνίες, που αφορούν την ασφάλεια. Το κανάλι 178 είναι το κανάλι ελέγχου (CCH) και χρησιμοποιείται αποκλειστικά για επικοινωνίες ασφάλειας, όπως φαίνεται και στην Εικόνα 2.11. Οι εφαρμογές για τις επικοινωνίες μεταξύ οχημάτων μπορούν να χωριστούν σε τρεις κατηγορίες: α) αυτές που αφορούν την ασφάλεια κίνησης, β) αυτές που αφορούν την απόδοση της κίνησης και γ) αυτές που αφορούν την ψυχαγωγία [6],[17],[18],[24],[25].

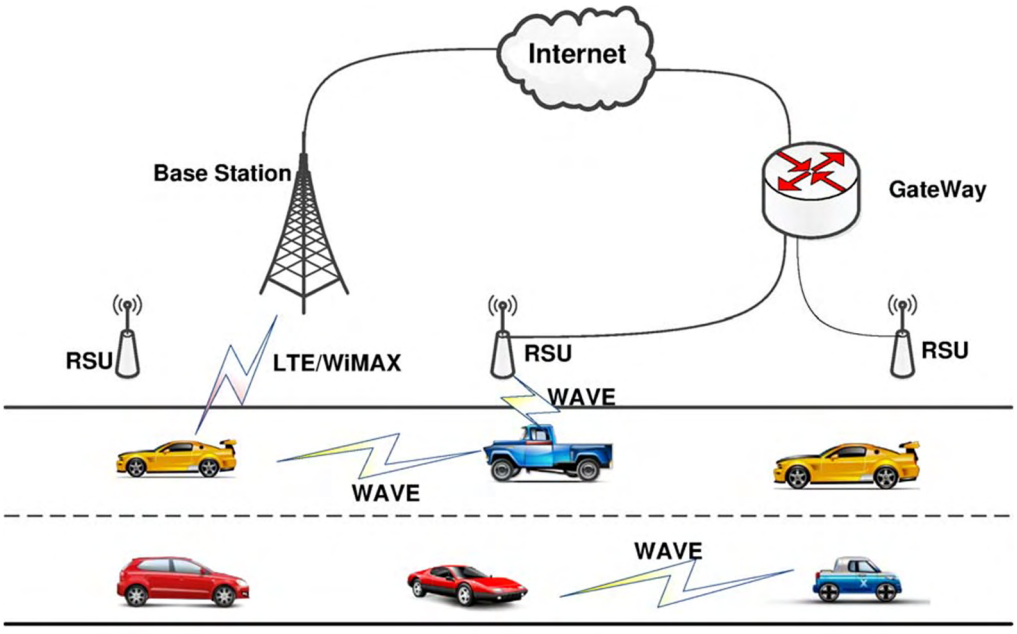


Εικόνα 2.11 *Κανάλια του φάσματος των 75 MHz [23]*

2.4.4 WiMAX τεχνολογία

Η τεχνολογία WiMAX λειτουργεί με παρόμοιο τρόπο με την τεχνολογία του Wi-Fi, όμως έχει μεγαλύτερη εμβέλεια σε σχέση με αυτό, όπως επίσης παρέχει και μεγαλύτερο ρυθμό μετάδοσης δεδομένων. Συσκευές, οι οποίες είναι συμβατές με το WiMAX, μπορούν να παραμένουν συνδεδεμένες ακόμα και σε περιοχές μεγάλης έκτασης. Η τεχνολογία αυτή βασίζεται στο πρότυπο 802.16 και είναι ικανή να προσφέρει από μία μόνο κεραία συνδεσιμότητα σε εμβέλεια, περίπου, 60 χιλιομέτρων από αυτήν. Παράλληλα, προσφέρει και ρυθμούς μετάδοσης δεδομένων μέχρι τα 70 Mbps, εκμεταλλευόμενο την τεχνική πολλαπλής εισόδου και πολλαπλής εξόδου (MIMO) με πολυπλεξία ορθογωνικής διαίρεσης συχνότητας (OFDM). Τα οχήματα, που κάνουν χρήση της τεχνολογίας αυτής, μπορούν να αναπτύξουν ταχύτητες έως τα 70 χλμ. ανά ώρα.

Επιπλέον το WiMAX είναι ικανό να παρέχει σε τοπικές διατάξεις Wi-Fi σύνδεση στο διαδίκτυο. Λόγω της αρχιτεκτονικής του, το WiMAX, μπορεί να χειρίζεται απρόσκοπτα από έναν μέχρι εκατοντάδες εξοπλισμούς πελατών (CPE) με κάθε CPE, να έχει έναν πολύ μεγάλο αριθμό συνδρομητών. Γίνεται χρήση καναλιών μεταβλητού εύρους από 1.5 MHz έως 20 MHz. Λειτουργώντας σε συχνότητα 5 bps/Hz και σε κανάλι των 20 MHz, μπορεί να αγγίξει ρυθμούς μετάδοσης δεδομένων έως 100 Mbps. Τέλος, με βάση τα χαρακτηριστικά του, θεωρείται κατάλληλο για εφαρμογές πολυμέσων και VoIP. Στην Εικόνα 2.12 απεικονίζεται η επικοινωνία με την χρήση WiMAX [17],[18].



Εικόνα 2.12 *WiMAX τεχνολογία [26]*

2.4.5 Υπέρυθρη τεχνολογία

Στον διαρκώς εξελισσόμενο χώρο των ασύρματων τεχνολογιών, βρίσκεται η μέθοδος της υπέρυθρης επικοινωνίας, η οποία βασίζεται στο αόρατο φάσμα του φωτός για τη μετάδοση των δεδομένων. Η τεχνολογία αυτή λειτουργεί εντός ενός μεγάλου φάσματος συχνοτήτων, που κυμαίνεται από τα 300 GHz έως και τα 400 THz. Το συγκεκριμένο εκτεταμένο φάσμα είναι οργανωμένο σε τρεις διακριτές ζώνες: την κοντινή υπέρυθρη ζώνη (near-infrared), την κεντρική υπέρυθρη ζώνη (mid-infrared), και την άπω υπέρυθρη ζώνη. Ανάλογα με τη ζώνη, ο ρυθμός μετάδοσης των δεδομένων κυμαίνεται από τα 115 Kbps έως και τα 4 Mbps.

Η υπέρυθρη τεχνολογία παρουσιάζει περιορισμούς, όπως η ευαισθησία που έχει στα φυσικά εμπόδια, τα οποία είναι ικανά να παρεμποδίσουν τα υπέρυθρα σήματα. Για τον λόγο αυτό, είναι σύνηθες, αυτός ο τρόπος επικοινωνίας, να χρησιμοποιείται κυρίως σε επικοινωνίες βραχείας απόστασης μέχρι τα 100 μέτρα περίπου. Παρά τη χαμηλή κατανάλωση ισχύος που παρατηρείται στη συγκεκριμένη μέθοδο, οι ρυθμοί μετάδοσης των δεδομένων είναι χαμηλοί συγκριτικά με πιο σύγχρονα πρότυπα, όπως αυτό του Bluetooth.

Μέσω της τεχνικής αυτής, είναι εφικτό να μεταδοθούν πληροφορίες, όπως φωνή, δεδομένα, ακόμη και βίντεο με πολύ μεγάλη ασφάλεια. Η υπέρυθρη τεχνολογία θεωρείται ότι μπορεί να υποστηρίξει υψηλή δικτυακή κίνηση, όπως επίσης και μεγάλο εύρος ζώνης, κάτι που την κάνει κατάλληλη για χρήση σε εφαρμογές ασφαλείας στα οδικά δίκτυα. Για παράδειγμα, η υλοποίηση της Ιαπωνικής εφαρμογής VICS, στην οποία γίνεται χρήση τόσο σημάτων ραδιοφάρου (beacons) μέσω ραδιοκυμάτων, όσο και σημάτων ραδιοφάρου μέσω υπέρυθρων σε σημαντικές οδικές αρτηρίες του δικτύου. Τέλος, τα οχήματα, που κάνουν χρήση της τεχνολογίας αυτής, μπορούν να αναπτύξουν ταχύτητες έως και τα 70 χλμ. ανά ώρα [18].

2.4.6 Bluetooth τεχνολογία

Το Bluetooth (IEEE 802.15.1) αποτελεί ένα ευρέως διαδεδομένο πρωτόκολλο επικοινωνίας, το οποίο λειτουργεί στη ζώνη συχνοτήτων ISM (Industrial, Scientific and Medical). Είναι σχεδιασμένο με τρόπο , όπου μπορεί να προσφέρει ρυθμούς μετάδοσης δεδομένων από 1 Mbps έως 4 Mbps, με την προϋπόθεση ότι οι κόμβοι βρίσκονται σε απόσταση μόλις 100 μέτρων. Η λειτουργία του πραγματοποιείται στην συχνότητα των 2.4 GHz και για να αντιμετωπίσει τυχόν παρεμβολές ή διακοπές, κάνει χρήση μιας τεχνικής, η οποία είναι γνωστή ως φασματική εξάπλωση με αναπήδηση συχνότητας (FHSS), που προσαρμόζει δυναμικά τις συχνότητες, για να διατηρηθεί σταθερή η σύνδεση.

Όπως όλες οι τεχνολογίες επικοινωνίας εξελίσσονται, έτσι και η τεχνολογία του Bluetooth έχει τις εκδόσεις 3 και 4. Η έκδοση 3 λειτουργεί σε ένα εύρος συχνοτήτων από 6 GHz έως 9 GHz, όμως για

να έρθει σε επικοινωνία με άλλες συσκευές χρησιμοποιεί την συχνότητα 2.4 GHz. Η έκδοση 4 περιέχει κάποιες αλλαγές, όπως την χαμηλότερη κατανάλωση ενέργειας αλλά και την έλλειψη συμβατότητας προς τα πίσω με παλαιότερες εκδόσεις.

Το Bluetooth χρησιμοποιείται με σκοπό τη δημιουργία ενός δικτύου προσωπικού χώρου (PAN) και για τον λόγο αυτό θεωρείται κατάλληλη τεχνολογία, να υποστηρίξει εφαρμογές τόσο V2V, όσο και V2I. Οι κόμβοι, οι οποίοι είναι συνδεδεμένοι με Bluetooth, μπορούν να αναπτύξουν ταχύτητες έως 30 χλμ. ανά ώρα. Συγκριτικά με άλλες τεχνολογίες, όπως το Wi-Fi το Bluetooth, εμφανίζεται ως πιο αποδοτικό ενεργειακά, ωστόσο όμως, λόγω των περιορισμών που αντιμετωπίζει, όπως ο αργός ρυθμός μετάδοσης δεδομένων, η μικρή εμβέλεια και οι παρεμβολές που προκαλεί το φυσικό περιβάλλον, δεν θεωρείται κατάλληλο για εφαρμογές που απαιτούν μεγάλος εύρος ζώνης, όπως η πλοήγηση στο διαδίκτυο και η φωνή μέσω IP (VoIP). Τέλος, το Bluetooth κάνει χρήση του Secure Simple Pairing (SSP) πρωτοκόλλου με σκοπό να εξασφαλίσει ασφάλεια μεταξύ των συνδεδεμένων συσκευών [17],[18].

2.4.7 Δορυφορική τεχνολογία

Η δορυφορική τεχνολογία θεωρείται ως μια ακόμη λύση για επικοινωνία στα αδόμητα οχηματικά δίκτυα. Ένα από τα σημαντικά της πλεονεκτήματα είναι η πολύ μεγάλη εμβέλεια, όπου σε συνδυασμό με την υψηλή συχνότητα των 90 MHz και τη δυνατότητα της για κλιμάκωση, την καθιστά κατάλληλη για μετάδοση δεδομένων. Επίσης, όταν οι κυψελοειδείς επικοινωνίες δεν επαρκούν, μπορεί να λειτουργήσει και ως εφεδρική λύση επικοινωνίας, ώστε να μην διακοπεί η ροή των δεδομένων. Ο ρυθμός μετάδοσης δεδομένων αγγίζει το 100 Mbps και τα οχήματα μπορούν να αναπτύξουν ταχύτητες έως και 120 χλμ. ανά ώρα.

Επιπλέον η δορυφορική επικοινωνία είναι ικανή να βελτιώσει την αξιοπιστία των GPS συστημάτων αλλά και να παρέχει V2V επικοινωνία. Ερευνώντας περαιτέρω τη χρήση της δορυφορικής τεχνολογίας, παρατηρούμε ότι μπορεί να χρησιμοποιηθεί για διαμοιρασμό δεδομένων μεταξύ των οχημάτων από αισθητήρες, την επικοινωνία μέσω του σύννεφου (Cloud Communication), την παρακολούθηση οχημάτων σε πραγματικό χρόνο ακόμα και σε απομονωμένες περιοχές, που δεν υπάρχει δικτυακή κάλυψη.

Παρόλα αυτά, συναντάμε και μειονεκτήματα στη δορυφορική επικοινωνία, όπως την πολύ μεγάλη καθυστέρηση, η οποία παρατηρείται στις δορυφορικές μεταδόσεις και στο μέγεθος των κεραιών. Λόγω των μειονεκτημάτων αυτών, η χρήση της δορυφορικής επικοινωνίας σε ένα αδόμητο οχηματικό δίκτυο καθίσταται δύσκολη, όχι όμως ανέφικτη, καθώς σε συνδυασμό με τεχνολογίες, όπως το LTE και το 5G, παρατηρούνται θετικά αποτελέσματα [17].

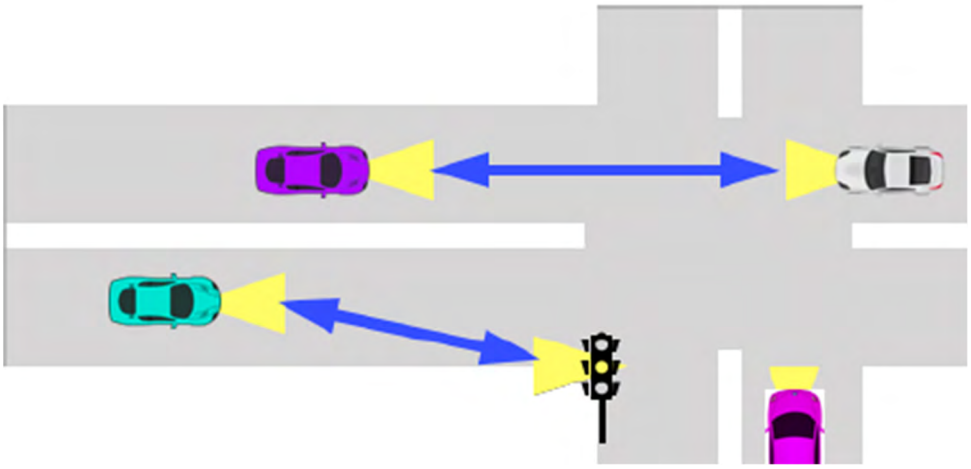
2.4.8 Τεχνολογία VLC (Visible Light Communication)

Ο οργανισμός IEEE, το 2012 δημιούργησε ένα νέο πρότυπο επικοινωνίας με την ονομασία IEEE 802.15.7. Το νέο αυτό πρότυπο είναι βασισμένο στις αρχές της επικοινωνίας ορατού φωτός (VLC). Μελετώντας τις τεχνικές λεπτομέρειες, το VLC είναι ικανό να προσφέρει οπτική ασύρματη επικοινωνία μικρού μήκους κύματος, εκμεταλλευόμενο τις μπάντες ορατού φωτός που κυμαίνονται από 380 έως και 780 νανόμετρα. Το VLC μπορεί να λειτουργήσει σε διάφορες μπάντες, οι κυριότερες αυτών είναι: α) μπάντα των υπέρυθρων (IR), β) το γενικό φάσμα ορατού φωτός και γ) οι μπάντες των υπεριωδών (UV), οι οποίες κυμαίνονται από 430 έως 790 THz. Ο ρυθμός μετάδοσης δεδομένων κυμαίνεται από το 1 Mbps έως τα 500 Mbps και η εμβέλεια του ανάμεσα σε οχήματα φτάνει τα 20 μέτρα, ενώ ανάμεσα στην σταθερή υποδομή και το όχημα φτάνει τα 50 μέτρα.

Σε πιθανή ενσωμάτωση του VLC σε ένα αδόμητο οχηματικό δίκτυο μπορούμε να παρατηρήσουμε αρκετά πλεονεκτήματα. Συγκριτικά με το πρωτόκολλο DSRC, το VLC είναι πιο ανθεκτικό στην παρεμβολή από άλλα ηλεκτρομαγνητικά σήματα, είναι ικανό να παρέχει σημαντικά μειωμένη καθυστέρηση (περίπου 1-3 ms), περισσότερες ζώνες συχνοτήτων που είναι διαθέσιμες και δείχνει αντοχή σε πιθανές απειλές ασφάλειας.

Επιπλέον, το VLC δείχνει κατάλληλο σε διάφορες αλληλεπιδράσεις τύπου V2V, από τις αποφάσεις για αλλαγή λωρίδας σε έναν δρόμο και την καλύτερη αντίληψη του δρόμου, μέχρι την προηγμένη σήμανση κυκλοφορίας. Τα οχήματα που κάνουν χρήση της VLC τεχνολογίας, θα πρέπει να κινούνται με μειωμένη ταχύτητα.

Λόγω της αρχιτεκτονικής της τεχνολογίας υπάρχουν κάποιες προκλήσεις. Μερικά χαρακτηριστικά του VLC, όπως η απαραίτητη ύπαρξη επικοινωνίας οπτικού πεδίου, τα μικρού μήκους κύματα που χρησιμοποιεί, η ευαισθησία στις σκιάσεις σήματος και η ευαισθησία σε φυσικά φαινόμενα, είναι ικανά να προκαλέσουν αλλοίωση στην μεταφορά των δεδομένων μέσω VLC. Στην Εικόνα 2.13 απεικονίζεται η επικοινωνία με χρήση VLC [17].



Εικόνα 2.13 *VLC τεχνολογία [27]*

Πίνακας 2.1 *Σύγκριση των τεχνολογιών επικοινωνίας στα VANETs*

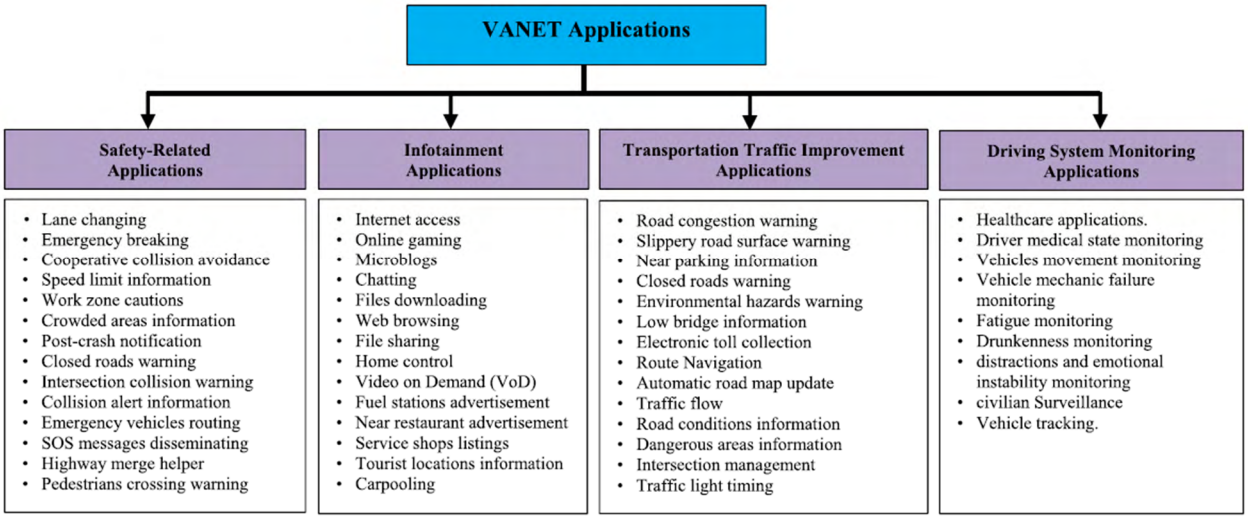
Συγκριτικός Πίνακας Τεχνολογιών Επικονωνίας σε Αδόμητα Οχηματικά Δίκτυα								
Τεχνολογία	**Εμβέλεια**	**Ρυθμός μετάδοσης**	**Κινητικότητα**	**Καθυστέρηση**	**Χαρακτηριστικά**	**Μηχανισμοί ασφάλειας**	**Βελτιώσεις**	**Σενάρια χρήσης (V2V,V2I,V2X)**
DSRC (Dedicated Short-Range Communications)	1km	3-27Mbps	Μέχρι 300km/h	5ms	1) Μικρή εμβέλεια. 2)Ειδικά σχεδιασμένο για χρήση σε αδόμητα οχηματικά δίκτυα. 3)Μικρή καθυστέρηση.	IEEE 1609.2	1) Σε επίπεδο εφαρμογής	V2V, V2I
Wi-Fi	100-300m	54Mbps	Μέχρι 250km/h	3-10ms	1) Μεγάλη διαθεσιμότητα. 2) Διαφορετικός ρυθμός μετάδοσης ανάλογα το standard. 3) Χρειάζεται υποδομή.	SSL/TLS	1) Σε φυσικό επίπεδο (PHY layer) 2) Σε επίπεδο MAC 3) Σε επίπεδο εφαρμογής	V2V, V2I

Συγκριτικός Πίνακας Τεχνολογιών Επικονωνίας σε Αδόμητα Οχηματικά Δίκτυα								
LTE/4G	5km	300Mbps	Μέχρι 200-300km/h	5ms(V2I) 100ms(V2V)	1) Μεγάλη κάλυψη 2) Μικρή καθυστέρηση. 3) Χρειάζεται σταθερή υποδομή	SSL/TLS Μηχανισμός αμοιβαίας ταυτοποίησης	1) Σε φυσικό επίπεδο (PHY layer) 2) Σε επίπεδο MAC	V2X
Infrared	1-100m	4Mbps	Μέχρι 70km/h	10ms	1) Αξιόπιστο 2) Εύκολα διαχειρίσιμο			V2V, V2I
Mmwave/5G	~1-300m	1-10Gbps	Μέχρι 500km/h	1-3ms	1) Μεγάλη συχνότητα 2) Μεγάλος ρυθμός εκπομπής 3) Μικρή εμβέλεια	SSL/TLS Μηχανισμός αμοιβαίας ταυτοποίησης	1) Σε φυσικό επίπεδο (PHY layer) 2) Σε επίπεδο MAC	V2X
WiMAX	~60km	70Mbps-100Mbps	Μέχρι 70km/h	50ms	1) Μεγάλη εμβέλεια 2) Μεγάλος ρυθμός μετάδοσης 3) Χρειάζεται σταθερή υποδομή	PKM (Privacy Key Management)	1) Σε επίπεδο MAC 2) Σε επίπεδο Network	V2I

Συγκριτικός Πίνακας Τεχνολογιών Επικονωνίας σε Αδόμητα Οχηματικά Δίκτυα								
Satellite	Global	100 Mbps	Μέχρι 120km/h	500-1000ms	1)Μικρό κόστος 2) Παγκόσμια κάλυψη 3)Πολύ μεγάλη καθυστέρηση			V2I
VLC (Visible Light Communication)	50m (V2I) 20m (V2V)	1-500Mbps	Χαμηλή ταχύτητα	1-3ms	1) Μεγάλος ρυθμός μετάδοσης 2) Μικρό κόστος 3) Χαμηλή κατανάλωση ενέργειας 4) Περιορισμένο οπτικό πεδίο			V2V,V2I
Bluetooth	~100m	1-4Mbps	Μέχρι 30km/h	5-15ms	1) Μικρή κατανάλωση ενέργειας 2) Μικρό κόστος 3) Μεγάλη συμβατότητα με συσκευές	SSP (Secure Simple Pairing)	1) Σε επίπεδο εφαρμογής 2) Σε επίπεδο MAC 3) Σε φυσικό επίπεδο (PHY layer)	V2V, V2I

2.5 Εφαρμογές στα αδόμητα οχηματικά δίκτυα

Τα τελευταία χρόνια, παρατηρείται αυξημένη ζήτηση για ενσωμάτωση των ευφυών συστημάτων μεταφορών (ITS) στις έξυπνες πόλεις που δημιουργούνται. Το γεγονός αυτό, έχει οδηγήσει τόσο την επιστημονική κοινότητα, όσο και τις βιομηχανίες να καινοτομούν και να σχεδιάζουν μια ευρεία γκάμα υπηρεσιών και εφαρμογών για αδόμητα οχηματικά δίκτυα. Το αποτέλεσμα της προόδου που έχει σημειωθεί στον τομέα αυτό, είναι η μεγάλη ποικιλία υπηρεσιών, που είναι ικανές να ανταποκριθούν στις απαιτήσεις των οδηγών, των ταξιδιωτών και του κρατικού μηχανισμού. Το σύνολο των υπηρεσιών αυτών είναι δυνατόν να κατηγοριοποιηθεί σε τέσσερις βασικές διακριτές κατηγορίες ανάλογα τη χρήση τους. Η πρώτη κατηγορία αφορά εφαρμογές και υπηρεσίες που είναι σχετικές με την ασφάλεια , η δεύτερη κατηγορία αφορά την ψυχαγωγία, η τρίτη κατηγορία αφορά τη βελτίωση της κυκλοφορίας στο οδικό δίκτυο και τέλος η τέταρτη κατά σειρά κατηγορία αφορά την παρακολούθηση των συστημάτων οδήγησης. Κάθε μια από αυτές τις κατηγορίες περιέχει μια πληθώρα εξειδικευμένων χρήσεων και πιθανών εφαρμογών. Στην Εικόνα 2.14 παρουσιάζεται ένα συγκεντρωτικό γράφημα των εφαρμογών κάθε κατηγορίας [17],[28].



Εικόνα 2.14 *Εφαρμογές στα VANETs [17]*

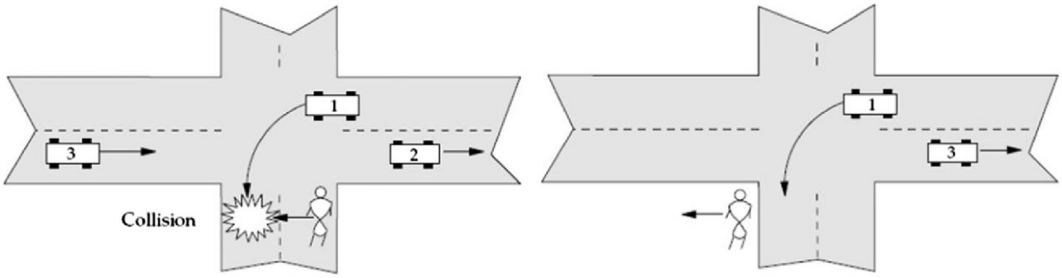
2.5.1 Εφαρμογές ασφάλειας

Η βασική κατηγορία εφαρμογών στα αδόμητα οχηματικά δίκτυα είναι οι εφαρμογές ασφάλειας, οι οποίες έχουν ως στόχο να μειώσουν την συχνότητα των οδικών ατυχημάτων. Αυτό είναι δυνατόν να επιτευχθεί, μέσω της άμεσης μεταφοράς δεδομένων, που αφορούν την ασφάλεια, επιτρέποντας έτσι στον οδηγό να λαμβάνει αποφάσεις προληπτικά με μεγαλύτερη ευκολία βάση της ειδοποίησης που έλαβε, συμβάλλοντας στην μείωση των ατυχημάτων. Οι εφαρμογές τέτοιου είδους διαχωρίζονται σε τρείς κατηγορίες: i) τις εφαρμογές που βοηθούν τον οδηγό κατά την διάρκεια της

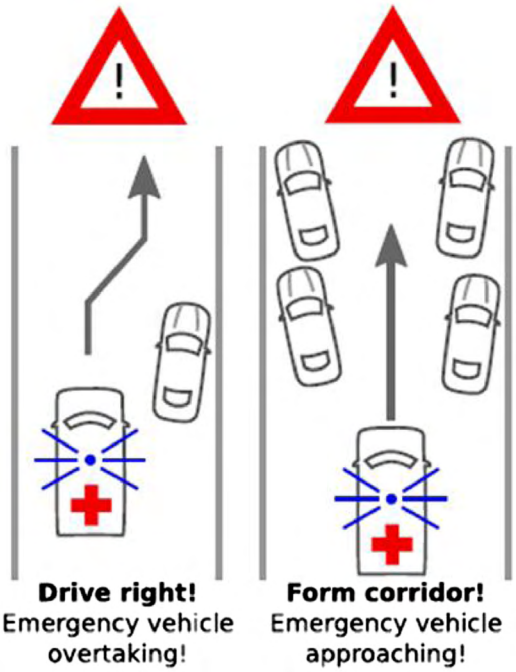
οδήγησης, ii) τις εφαρμογές παροχής πληροφοριών ασφάλειας και iii) τις εφαρμογές προειδοποίησης του οδηγού. Μια πολύ χρήσιμη υπηρεσία θεωρείται το σύστημα αποφυγής σύγκρουσης σε διασταυρώσεις, το οποίο έχει ως κύριο στόχο την αποφυγή κάποιας σύγκρουσης σε διασταυρώσεις του οδικού δικτύου. Μέσα σε ένα αδόμητο οχηματικό δίκτυο, όπου είναι εφικτές επικοινωνίες, όπως όχημα προς όχημα (V2V) και όχημα προς υποδομή (V2I), τα οχήματα μπορούν να ανταλλάσσουν δεδομένα και μεταξύ τους αλλά και με τη βοήθεια των παρόδιων μονάδων, οι οποίες αναμεταδίδουν την πληροφορία στα υπόλοιπα οχήματα με σκοπό την αποφυγή κάποιου ατυχήματος. Τα μηνύματα που ανταλλάσσονται, μπορούν να περιέχουν πληροφορίες που αφορούν τις διασταυρώσεις, όπως την κατάσταση στην οποία βρίσκονται οι φωτεινοί σηματοδότες εκείνη την στιγμή, την προτεραιότητα που έχει ο κάθε κόμβος, το μποτιλιάρισμα που μπορεί να παρουσιάζεται σε αυτό το σημείο, καθώς επίσης και τυχόν καιρικά φαινόμενα. Επίσης, μέσω αισθητήρων και καμερών, οι παρόδιες μονάδες είναι σε θέση να προειδοποιούν τα οχήματα για τυχόν παραβιάσεις του Κ.Ο.Κ, όπως παραβίαση ερυθρού σηματοδότη.

Αρκετές έρευνες προτείνουν την δημιουργία ενός συστήματος, με σκοπό την προστασία των πεζών από ατυχήματα σε διασταυρώσεις. Αυτό επιτυγχάνεται με την εγκατάσταση αισθητήρων στις διασταυρώσεις. Την ώρα που οι πεζοί περνούν τη διάβαση, ένα αυτόματο μήνυμα εκπέμπεται προς τα οχήματα, ενημερώνοντας τα για την διέλευση πεζών. Στην Εικόνα 2.15 παρουσιάζεται το σύστημα αυτό. Οι εφαρμογές ασφαλείας μπορούν να είναι χρήσιμες ακόμα και για τον κρατικό μηχανισμό, αφού σε καταστάσεις κινδύνου τα οχήματα, όπως τα πυροσβεστικά, τα ασθενοφόρα και τα περιπολικά μπορούν να βρουν την ταχύτερη διαδρομή μέχρι το σημείο του ατυχήματος, αφού πρώτα τα υπόλοιπα οχήματα, που βρίσκονται σε μικρή ακτίνα, έχουν αλλάξει πορεία ύστερα από μηνύματα ασφάλειας, που έλαβαν σχετικά με την πορεία και την ταχύτητα των οχημάτων έκτακτης ανάγκης. Στην Εικόνα 2.16 παρουσιάζεται μια τέτοια περίπτωση.

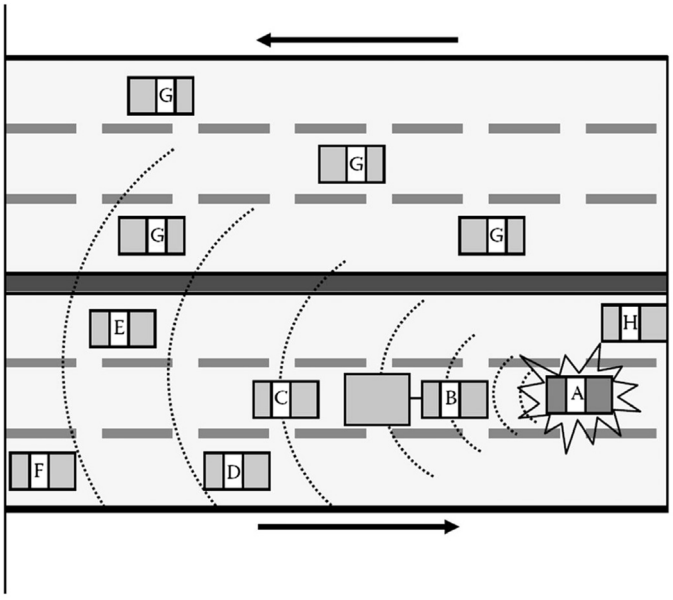
Σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, μηνύματα SOS ανταλλάσσονται από τις εφαρμογές ασφαλείας, τα οποία περιέχουν πληροφορίες σχετικά με την ακριβή τοποθεσία της καταστροφής. Με τον ίδιο τρόπο λειτουργούν και για τυχόν σταματημένα οχήματα επί της οδού, αποφεύγοντας έτσι την σύγκρουση. Επιπλέον, είναι δυνατόν οι οδηγοί να λαμβάνουν ειδοποιήσεις, όταν πλησιάζουν σε κάποιο νοσοκομείο ή σε κάποια ζώνη διέλευσης άγριων ζώων ή σε κάποιο σχολείο, ώστε να ελαττώνουν την ταχύτητα του οχήματος. Τέλος, οι εφαρμογές ασφαλείας είναι χρήσιμες ακόμα και σε καταστάσεις απότομου φρεναρίσματος του προπορευόμενου οχήματος, καθώς στέλνονται μηνύματα για το συμβάν, με αποτέλεσμα, ακόμα και αν οι οδηγοί των υπολοίπων οχημάτων δεν έχουν την ορατότητα να το διακρίνουν, να είναι ενημερωμένοι, ώστε να μειώσουν ταχύτητα και να αποφευχθεί κάποιο ατύχημα. Στην Εικόνα 2.17 παρουσιάζεται η περίπτωση του απότομου φρεναρίσματος [17],[28].



Εικόνα 2.15 *Σύστημα ειδοποίησης για διέλευση πεζών [28]*



Εικόνα 2.16 *Σύστημα ειδοποίησης για όχημα έκτακτης ανάγκης [28]*



Εικόνα 2.17 *Ειδοποίηση απότομου φρεναρίσματος [28]*

2.5.2 Εφαρμογές ψυχαγωγίας

Η κατηγορία αυτή εφαρμογών εξυπηρετεί τους οδηγούς και τους επιβάτες του οχήματος με την παροχή υπηρεσιών ψυχαγωγίας, όπως κοινή χρήση βίντεο μέσω του διαδικτύου, διαδικτυακά παιχνίδια, πρόσβαση στο διαδίκτυο και τηλεφωνία μέσω διαδικτύου (VoIP). Οι εφαρμογές αυτές σε πολλές περιπτώσεις απαιτούν μεγάλο εύρος ζώνης και ανοχή στις καθυστερήσεις. Τρεις νέες υποκατηγορίες μπορούν να περιέχονται στην κατηγορία των εφαρμογών ψυχαγωγίας και αυτές είναι: α) η κατηγορία ψυχαγωγικών εφαρμογών, β) η κατηγορία που αφορά το ηλεκτρονικό εμπόριο και γ) η κατηγορία που αφορά ανακοινώσεις της εκάστοτε πόλης.

Σε περίπτωση όπου τα γνωστά δίκτυα, όπως το Wi-Fi ή το WiMAX δεν είναι διαθέσιμα προς τους χρήστες, τότε τα αδόμητα οχηματικά δίκτυα είναι ικανά να παρέχουν δικτυακή πρόσβαση. Το ίδιο είναι εφικτό ακόμα και για τα οχήματα, όταν ένα όχημα είναι συνδεδεμένο σε αντίστοιχο δίκτυο, τότε μπορεί να προσφέρει πρόσβαση στο διαδίκτυο και σε ένα κοντινό του όχημα. Μέσα σε ένα αδόμητο οχηματικό δίκτυο χρήσιμες είναι επίσης και οι εφαρμογές διομότιμων χρηστών (peer-to-peer), όπως εφαρμογές άμεσης ανταλλαγής μηνυμάτων ή αρχείων και διαδικτυακής τηλεόρασης.

Επιπλέον, οι επιχειρήσεις μπορούν να εκμεταλλευτούν τις δυνατότητες που παρέχουν τα αδόμητα οχηματικά δίκτυα και να διαφημίσουν τα προϊόντα τους, όπως τα βενζινάδικα που μπορούν να διαφημίσουν την τιμή της βενζίνης ή μια επιχείρηση εστίασης να διαφημίσει τον τιμοκατάλογό της στα κοντινά οχήματα, με σκοπό να προσελκύσουν πελάτες. Άλλες χρήσεις των εφαρμογών τέτοιου είδους στα αδόμητα οχηματικά δίκτυα είναι η διευκόλυνση τουριστών στην εύρεση κοντινών καταστημάτων, αλλά και η εύρεση μεταφορικού μέσου, όπου με την V2V επικοινωνία είναι εφικτό τα οχήματα να ανταλλάξουν πληροφορίες σχετικά με τρόπους μετακίνησης, όπως η τεχνική της κοινής χρήσης του οχήματος από άτομα που έχουν τον ίδιο προορισμό (car-sharing). Συνεπώς, μειώνεται η χρήση οχημάτων στις πόλεις και η ρύπανση [17],[28].

2.5.3 Εφαρμογές βελτίωσης κυκλοφορίας

Οι εφαρμογές βελτίωσης κίνησης έχουν ως στόχο να βελτιστοποιήσουν την οδική κυκλοφορία και να μειώσουν τα ατυχήματα μέσω της σωστής διαχείρισης της συμφόρησης. Αυτές οι εφαρμογές παρέχουν στα οχήματα δεδομένα, που αφορούν την κυκλοφορία, επιτρέποντας έτσι στους οδηγούς να αποφύγουν σημεία με μεγάλη συμφόρηση, τα οποία πιθανόν να καθυστερήσουν τον οδηγό. Οι εφαρμογές αυτές μπορούν να χωριστούν σε τρεις κύριους τομείς: i) τον τομέα που αφορά τον συντονισμό των διασταυρώσεων, ii) τον τομέα που ρόλος του είναι η εποπτεία συμφόρησης και iii) τον τομέα που έχει ως στόχο να ενημερώσει τους οδηγούς για την κατάσταση των οδών.

Παρατηρείται σε οδικά δίκτυα ότι ένας σημαντικός αριθμός ατυχημάτων σημειώνεται σε σημεία διασταυρώσεων των οδών. Στα σημεία αυτά, οι φωτεινοί σηματοδότες λειτουργούν με τη χρήση χρονοδιακοπτών, κάτι που δεν θεωρείται χρήσιμο, όταν παρατηρείται μεγάλη συμφόρηση σε ορισμένα σημεία. Μια εφικτή λύση είναι η τοποθέτηση προσαρμοστικών φωτεινών σηματοδοτών, οι οποίοι μπορούν να δέχονται πληροφορίες σχετικά με την τρέχουσα κατάσταση του οδικού δικτύου μέσα από τα αδόμητα οχηματικά δίκτυα.

Μια ακόμη λύση στην βελτίωση της κυκλοφορίας στο οδικό δίκτυο είναι οι εφαρμογές διαχείρισης της συμφόρησης, οι οποίες είναι σχεδιασμένες να λαμβάνουν δεδομένα σχετικά με την κατάσταση των δρόμων ανά τακτά χρονικά διαστήματα και να ενημερώνουν για ταχύτερες διαδρομές τους οδηγούς, αποφεύγοντας έτσι τα κομμάτια αυτά, που παρατηρείται η συμφόρηση.

Επιπλέον, συμφόρηση δεν παρατηρείται μόνο μέσα στα κέντρα των πόλεων, αλλά και στα διόδια εθνικών οδών, όπου οι οδηγοί σταματούν, για να πληρώσουν, σχηματίζοντας μεγάλες ουρές. Για την μείωση της συμφόρησης στα σημεία αυτά, έχουν δημιουργηθεί εφαρμογές, μέσω των οποίων γίνεται ηλεκτρονική πληρωμή διοδίων, μειώνοντας έτσι τον χρόνο αναμονής των οχημάτων στην ουρά.

Τέλος, οι ψηφιακοί χάρτες, όπως το Google Maps, είναι ένα χρήσιμο εργαλείο, το οποίο μπορεί να μειώσει αισθητά την συμφόρηση, προτείνοντας βέλτιστες διαδρομές, αφού πρώτα έχει συγκεντρώσει στοιχεία σχετικά με συμβάντα στο οδικό δίκτυο, όπως κλειστοί δρόμοι και διαδηλώσεις. Έτσι, οι οδηγοί είναι σε θέση να αποφασίσουν ποια διαδρομή θέλουν να ακολουθήσουν [17],[28].

2.5.4 Εφαρμογές παρακολούθησης συστημάτων οδήγησης

Οι συγκεκριμένες εφαρμογές επικεντρώνονται στην παρακολούθηση της υγείας του οδηγού και στην κατάσταση, στην οποία βρίσκεται το όχημα. Αυτές οι εφαρμογές μπορούν να κατηγοριοποιηθούν σε: α) εφαρμογές παρακολούθησης υγείας του οδηγού, β) εφαρμογές παρακολούθησης αντανακλαστικών, γ) εφαρμογές παρακολούθησης της κίνησης του οχήματος και δ) εφαρμογές ελέγχου των εξαρτημάτων του οχήματος.

Οι εφαρμογές υγείας αναλαμβάνουν την παρακολούθηση της υγείας των οδηγών και μοιράζονται τις πληροφορίες αυτές με τα κοντινότερα ιατρικά κέντρα. Σε πολλές περιπτώσεις, οι οδηγοί, λόγω θεμάτων υγείας που αντιμετωπίζουν, είναι πιθανό να βρεθούν σε καταστάσεις, όπως για παράδειγμα λιποθυμίας, με αποτέλεσμα να προκληθεί κάποιο ατύχημα. Για να είναι σε θέση, λοιπόν, οι εφαρμογές αυτές να παρακολουθούν την υγεία του οδηγού, γίνεται χρήση ασύρματων αισθητήρων σώματος. Επομένως, σε περίπτωση που εντοπίσουν κάτι ασυνήθιστο, εκπέμπουν μηνύματα μέσω της μονάδας OBU, στα κοντινότερα ιατρικά κέντρα.

Επίσης, θέματα όπως η κόπωση, η μέθη και η συναισθηματική αστάθεια είναι παράγοντες, οι οποίοι επηρεάζουν σε μεγάλο βαθμό τα αντανακλαστικά, καθώς και την ικανότητα ενός οδηγού στη λήψη σωστών αποφάσεων. Για τον λόγο αυτό, οι εφαρμογές παρακολούθησης αντανακλαστικών, αποστέλλουν μηνύματα προειδοποίησης προς τα κοντινά οχήματα, όταν ανιχνεύσουν κάποια τέτοια κατάσταση. Σε περίπτωση μέθης, η εφαρμογή μπορεί να ειδοποιήσει το κοντινότερο αστυνομικό τμήμα, ώστε να ληφθούν τα κατάλληλα μέτρα.

Σημαντικό, επίσης, κομμάτι, αποτελεί και η παρακολούθηση των επιμέρους εξαρτημάτων του οχήματος, όπως τα φρένα, όπου μπορεί να βοηθήσει στην πρόληψη ατυχημάτων, που προκύπτουν από βλάβες. Οι ασύρματοι αισθητήρες, οι οποίοι βρίσκονται τοποθετημένοι στο όχημα, μπορούν να ειδοποιήσουν τον οδηγό για τυχόν βλάβη. Συνεπώς, οι εφαρμογές παρακολούθησης αυτών των εξαρτημάτων μπορούν είτε να υποδείξουν στον οδηγό το κοντινότερο σημείο για επισκευή της βλάβης είτε να ενημερώσουν τις υποδομές της πόλης σχετικά με την βλάβη, ώστε να παρθούν οι κατάλληλες αποφάσεις.

Τέλος, οι εφαρμογές παρακολούθησης κίνησης του οχήματος μπορούν να ωφελήσουν στην παρακολούθηση κλεμμένων οχημάτων ή οχημάτων που συνδέονται με εγκληματικές δραστηριότητες. Μέσω από έναν μοναδικό αριθμό (ID), που έχει η κάθε μονάδα OBU, και με τη βοήθεια του συστήματος GPS, η δράση των αστυνομικών αρχών διευκολύνεται σημαντικά, καθώς ο εντοπισμός γίνεται ευκολότερος [17],[28].

2.6 Ζητήματα ασφάλειας στα αδόμητα οχηματικά δίκτυα

Στη σύγχρονη ταχύτατα, αναπτυσσόμενη κοινωνία, υπάρχει όλο και μεγαλύτερο ενδιαφέρον προς τα αδόμητα οχηματικά δίκτυα, με αποτέλεσμα ο ρυθμός ενσωμάτωσής τους στις πόλεις να αυξάνεται ραγδαία. Τα αδόμητα οχηματικά δίκτυα, όπως έχει ήδη αναφερθεί έχουν ως στόχο, όχι μόνο την βελτίωση της ασφάλειας των οδηγών και των πεζών, αλλά και την αποδοτική διαχείριση της συμφόρησης, που παρατηρείται στα αστικά κέντρα. Για να επιτευχθούν οι στόχοι αυτοί, γίνεται χρήση διαφόρων εφαρμογών και λειτουργιών στα αδόμητα οχηματικά δίκτυα. Αντίστοιχα, οι εφαρμογές αυτές κάνουν χρήση πολλών τεχνολογιών, με σκοπό την ασύρματη επικοινωνία των συστατικών ενός VANET. Αυτό έχει ως απότοκο, να τις κάνει ευάλωτες σε έναν μεγάλο αριθμό επιθέσεων, λόγω των ευπαθειών που μπορεί να παρουσιάζει η κάθε τεχνολογία, με αποτέλεσμα να μην υπάρχει σωστή λειτουργία αυτών.

Εμβαθύνοντας περαιτέρω, θα αναφερθούμε αρχικά στις κατηγορίες επιτιθέμενων, οι οποίοι μπορούν να εκμεταλλευτούν τυχόν ζητήματα ασφαλείας, που παρουσιάζονται προς όφελος τους. Οι επιτιθέμενοι μπορούν να καταταχθούν σε μια από τις παρακάτω κατηγορίες ανάλογα την δράση τους [4],[29]:

- **Εσωτερικοί-Εξωτερικοί**: Στην κατηγορία αυτήν, τα άτομα, τα οποία είναι εξουσιοδοτημένα να έχουν πρόσβαση μέσα στο δίκτυο, ονομάζονται εσωτερικοί. Τα άτομα αυτά, λόγω της εξουσιοδότησης που έχουν, μπορεί να κατέχουν θέση ακόμα και διαχειριστή, πράγμα που τα κάνει ιδιαίτερα επικίνδυνα, αφού έχουν όλα τα δικαιώματα, που χρειάζεται ένας χρήστης, ώστε να εξαπολύσει κάποια επίθεση. Από την άλλη, έχουμε τα άτομα, τα οποία βρίσκονται εκτός τους δικτύου, όπου παρεισφρέουν στο δίκτυο, για να εξαπολύσουν μια επίθεση. Τα άτομα αυτά ονομάζονται εξωτερικοί επιτιθέμενοι και παρουσιάζουν περιορισμούς, ως προς τις δυνατότητες που έχουν για να πραγματοποιήσουν την επίθεση.

- **Κακόβουλοι-Λογικοί**: Οι κακόβουλοι επιτιθέμενοι, ως επί των πλείστων, δεν εξαπολύουν επιθέσεις, με σκοπό να επωφεληθούν οι ίδιοι. Κύριος στόχος τους είναι η δυσλειτουργία του δικτύου. Επομένως, μπορούν να προβούν σε διάφορες επιθέσεις, που στοχεύουν σε δυσλειτουργία ενός δικτύου. Οι λογικοί επιτιθέμενοι έχουν ως στόχο το προσωπικό κέρδος από τις επιθέσεις, που εξαπολύουν. Για τον λόγο αυτό, στοχεύουν σε συγκεκριμένους χρήστες μέσα σε ένα δίκτυο. Αυτό τους καθιστά ιδιαίτερα επικίνδυνους.

- **Ενεργοί-Παθητικοί**: Οι ενεργοί επιτιθέμενοι είναι σύνηθες να επιτίθενται, κατασκευάζοντας νέα κακόβουλα πακέτα, με σκοπό να βλάψουν τους υπόλοιπους κόμβους του δικτύου. Οι παθητικοί επιτιθέμενοι στις περισσότερες περιπτώσεις “κρυφακούν” (eavesdrop) σε ένα κανάλι επικοινωνίας, με σκοπό να συγκεντρώσουν χρήσιμες πληροφορίες για τους κόμβους του δικτύου. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για κάποια μελλοντική επίθεση.

- **Τοπικοί-Εκτεταμένοι**: Σε επιθέσεις, όπου το πεδίο δράσης του επιτιθέμενου περιορίζεται στο ίδιο δίκτυο, δηλαδή έχει αποκτήσει τον έλεγχο μελών του δικτύου, όπως κόμβοι και σταθμοί βάσης, ο επιτιθέμενος χαρακτηρίζεται ως τοπικός. Στην περίπτωση, όμως, που έχει αποκτήσει τον έλεγχο μελών ξεχωριστών δικτύων, τότε ο επιτιθέμενος ανήκει στους εκτεταμένους.

- **Ανεξάρτητοι-Συνεργαζόμενοι**: Πολλοί τύποι επιθέσεων μπορούν να εξαπολυθούν και από έναν μόνο επιτιθέμενο, χωρίς τη βοήθεια άλλων. Οι επιτιθέμενοι, οι οποίοι έχουν την ικανότητα να πραγματοποιούν επιθέσεις χωρίς τη συνεργασία με άλλους, ορίζονται ως ανεξάρτητοι. Σε αντίθετη περίπτωση, εάν μια ομάδα ατόμων θέλει να πραγματοποιήσει μια

DDoS, τότε πολλά διαφορετικά μέλη θα πρέπει να συνεργαστούν. Οι επιτιθέμενοι, οι οποίοι πρέπει να συνεργαστούν με άλλα άτομα, ώστε να φέρουν εις πέρας μια επίθεση, χαρακτηρίζονται ως συνεργαζόμενοι.

Παρακάτω, αναλύονται τα ζητήματα ασφάλειας, που παρατηρούνται, τόσο στην υποδομή ενός αδόμητου οχηματικού δικτύου, όσο και στους κόμβους αυτού. Στον Πίνακα 2.2 παρουσιάζονται: συγκεντρωτικά: α) τα ζητήματα ασφάλειας, β) πιθανοί τύποι επιθέσεων, γ) το κομμάτι που επηρεάζει η κάθε επίθεση, όσον αφορά την εμπιστευτικότητα, δ) την ακεραιότητα και την διαθεσιμότητα, καθώς και ε) μερικά CVEs που αφορούν κάθε επίθεση.

2.6.1 Επαλήθευση

Τα αδόμητα οχηματικά δίκτυα είναι ένας τύπος δικτύου, όπου βασίζεται σε μεγάλο βαθμό στην ανταλλαγή μηνυμάτων και πληροφοριών μεταξύ των μελών του. Για τον λόγο αυτό, ο αποστολέας και ο παραλήπτης θα πρέπει, πρώτα, να έχουν επαληθεύσει την ταυτότητα τους, για να υπάρχει εμπιστοσύνη μεταξύ των κόμβων. Ένα από τα βασικότερα ζητήματα ασφάλειας, που παρατηρούνται στα αδόμητα οχηματικά δίκτυα, είναι αυτό της επαλήθευσης. Ο επιτιθέμενος μπορεί να εκμεταλλευτεί ευπάθειες σε συστήματα επαλήθευσης και να αλλοιώσει είτε την ταυτότητα του (ID Authentication), δηλώνοντας ότι είναι κάποια άλλη οντότητα του δικτύου, είτε αλλοιώνοντας την ακριβή τοποθεσία του και δηλώνοντας κάποια άλλη (Location Authentication), είτε αλλοιώνοντας την ιδιότητα που έχει, είτε ως κόμβος είτε ως μέρος της υποδομής (Property Authentication). Ο επιτιθέμενος μπορεί να εξαπολύσει επιθέσεις, όπως GPS Spoofing, Impersonation attack, Sybil attack και Replay attack [4],[29].

2.6.2 Διαθεσιμότητα

Η διαθεσιμότητα παίζει πολύ σημαντικό ρόλο μέσα σε ένα αδόμητο οχηματικό δίκτυο, γιατί μέσω αυτής επιτυγχάνεται η σωστή λειτουργία του δικτύου και η αποστολή σημαντικών πληροφοριών, την ώρα που είναι αναγκαίες. Επειδή, λοιπόν, η διαθεσιμότητα του δικτύου έχει άμεσο αντίκτυπο στους ίδιους τους χρήστες, γίνεται συχνά στόχος κακόβουλων χρηστών. Ακολουθώντας, ειδικά σχεδιασμένες τεχνικές, οι επιτιθέμενοι μπορούν να εξαπολύσουν επιθέσεις, όπως DoS attack και Blackhole attack, με στόχο την αποσταθεροποίηση της διαθεσιμότητα του δικτύου και τη μη ομαλή λειτουργία αυτού [4],[29].

2.6.3 Εμπιστευτικότητα

Η εμπιστευτικότητα σε ένα αδόμητο οχηματικό δίκτυο είναι αναγκαία από τις εφαρμογές, οι οποίες παρέχουν υπηρεσίες στους χρήστες, όπως η πλοήγηση στο διαδίκτυο. Μέσω αυτής διασφαλίζεται ότι μόνο ο αποστολέας και ο παραλήπτης έχουν πρόσβαση στην πληροφορία, που διαμοιράζεται. Αυτό επιτυγχάνεται μέσω πρωτοκόλλων κρυπτογράφησης, όμως, σε περίπτωση που δεν υπάρχουν ισχυρά πρωτόκολλα κρυπτογράφησης, τότε παρουσιάζεται ζήτημα ασφάλειας, αφού οι επιτιθέμενοι μπορούν να το εκμεταλλευτούν και να πραγματοποιήσουν επιθέσεις, όπως Impersonation attack [4],[29].

2.6.4 Ευπάθειες επεξεργαστικής μονάδας

Ένα από τα βασικότερα μέρη του οχήματος, όσον αφορά τη διασύνδεση του με τα υπόλοιπα μέλη ενός αδόμητου οχηματικού δικτύου αλλά και την καθολική λειτουργία του μέσα σε αυτό, είναι η επεξεργαστική μονάδα. Η επεξεργαστική μονάδα αποτελείται από διάφορα επιμέρους κομμάτια, όπως CPU, μνήμες αποθήκευσης, αισθητήρες κ.α. Κάθε ένα από αυτά τα επιμέρους τμήματα της επεξεργαστικής μονάδας είναι πιθανόν να εμφανίζουν κενά ασφάλειας, κάτι που τα κάνει ευάλωτα σε επιθέσεις κακόβουλου κώδικα (malware attack). Για τον λόγο, αυτό οι ευπάθειες που μπορεί να παρουσιάζει η επεξεργαστική μονάδα, χαρακτηρίζονται ως σημαντικό ζήτημα ασφάλειας στα αδόμητα οχηματικά δίκτυα [30],[31].

2.6.5 Φυσική ασφάλεια οχήματος

Το οχήματα αποτελούν τα βασικά στοιχεία ενός αδόμητου οχηματικού δικτύου. Σε πολλές περιπτώσεις γίνονται στόχοι κακόβουλων ατόμων, με αποτέλεσμα η φυσική ασφάλεια των οχημάτων να αποτελεί ένα επιπλέον ζήτημα, όταν ο επιτιθέμενος παραβιάζοντας το όχημα μπορεί να έχει πρόσβαση στα συστήματα αυτού, όπως για παράδειγμα η επεξεργαστική μονάδα. Μέσω αυτής της μη εξουσιοδοτημένης πρόσβασης που αποκτά, είναι ικανός να τροποποιήσει συστήματα του οχήματος προς δικό του όφελος αλλά και να εξαπολύσει απευθείας κάποια επίθεση, χωρίς ο ιδιοκτήτης να το γνωρίζει [30],[31].

2.6.6 Ευπάθειες στους αισθητήρες του οχήματος

Τα σύγχρονα έξυπνα οχήματα βασίζονται σε μεγάλο βαθμό στους αισθητήρες, που βρίσκονται εγκατεστημένοι σε αυτά. Οι αισθητήρες αυτοί αποτελούν κομμάτια υλικού (Hardware), κάτι που τους καθιστά ευάλωτους σε πιθανές επιθέσεις, όπως Sensor Spoofing και Sensor Jamming. Για να επιτευχθούν οι επιθέσεις αυτές, ο επιτιθέμενος θα πρέπει να εκμεταλλευτεί κάποια ευπάθεια,

που συνήθως παρουσιάζουν τα κομμάτια υλικού. Επομένως, οι ευπάθειες, που μπορεί να παρουσιάσουν οι αισθητήρες του οχήματος, θεωρούνται ως ένα ζήτημα, που μπορεί να επηρεάσει την ασφάλεια [30].

2.6.7 Άπληστοι οδηγοί

Μέσα σε ένα αδόμητο οχηματικό δίκτυο υπάρχουν οδηγοί, οι οποίοι εκμεταλλεύονται κακόβουλα το δίκτυο προς όφελος τους, όπως για τη διευκόλυνσή τους σε περιπτώσεις συμφόρησης. Οι οδηγοί αυτοί ονομάζονται άπληστοι οδηγοί (Greedy Drivers) και συνήθως πραγματοποιούν επιθέσεις, οι οποίες είτε τροποποιούν τα μηνύματα που ανταλλάσσονται (message falsification attack) είτε καθυστερούν τη μετάδοση σημαντικών μηνυμάτων, όπως αυτά που στοχεύουν στην αποφυγή πιθανού κινδύνου (message delay attack). Το γεγονός αυτό μπορεί να επηρεάσει όχι μόνο τη συνολική ασφάλεια του δικτύου αλλά και την ασφάλεια του κάθε οδηγού. Ολοκληρώνοντας, συμπεραίνεται ότι οι άπληστοι οδηγοί αποτελούν ένα σοβαρό ζήτημα στα αδόμητα οχηματικά δίκτυα [29].

2.6.8 Ιδιωτικότητα

Για να υπάρχει σωστή λειτουργία σε ένα αδόμητο οχηματικό δίκτυο, θα πρέπει να διασφαλίζεται η ιδιωτικότητα του κάθε κόμβου, η οποία αποτελεί ένα πολύ σημαντικό παράγοντα των αδόμητων οχηματικών δικτύων. Σε περίπτωση παραβίασής της, ο επιτιθέμενος είναι σε θέση να υποκλέψει προσωπικά στοιχεία του ιδιοκτήτη του οχήματος αλλά και στοιχεία που αφορούν την τοποθεσία του. Εάν δεν χρησιμοποιηθούν ισχυροί μηχανισμοί προστασίας της ιδιωτικότητας, τότε υπάρχει μεγάλος κίνδυνος διαρροής ευαίσθητων πληροφοριών σε κακόβουλους χρήστες, οι οποίοι μπορούν να τις εκμεταλλευτούν και να πραγματοποιήσουν επιθέσεις, όπως Impersonation attack και repudiation attack [1],[29],[30],[32].

2.6.9 Κενά ασφάλειας σε μέρη της υποδομής

Όπως έχει ήδη αναφερθεί, τα αδόμητα οχηματικά δίκτυα δεν αποτελούνται μόνο από οχήματα αλλά ένα μέρος τους είναι και η σταθερή υποδομή, όπως οι RSU και οι σταθμοί βάσης. Τα μέρη αυτά της υποδομής βασίζονται σε ειδικά λογισμικά, ώστε να παρέχουν τις υπηρεσίες στο υπόλοιπο δίκτυο. Σε πολλές περιπτώσεις, τα λογισμικά αυτά παρουσιάζουν κενά ασφαλείας, τα οποία μέσω των ενημερώσεων ασφαλείας του κατασκευαστή επιδιορθώνονται. Όμως, στην περίπτωση όπου δεν έχει γίνει σωστή συντήρηση των παραπάνω στοιχείων του αδόμητου οχηματικού δικτύου, οι ενημερώσεις ασφαλείας είναι πολύ πιθανό να μην έχουν εγκατασταθεί,

καθιστώντας το αντίστοιχο μέρος της υποδομής ευάλωτο σε επιθέσεις κακόβουλου κώδικα (malware). Συνεπώς, τα κενά ασφαλείας που παρουσιάζονται σε μέρη της υποδομής, αποτελούν ένα σημαντικό ζήτημα ασφάλειας [33].

2.6.10 Ασφάλεια στην διαχείριση των κλειδιών

Η κρυπτογράφηση αποτελεί μια από τις πιο διαδεδομένες τεχνικές προστασίας των πληροφοριών. Για την κρυπτογράφηση, αλλά και για την αποκρυπτογράφηση των δεδομένων, είναι απαραίτητη η χρήση ειδικών κλειδιών. Μέσα σε ένα δίκτυο υπάρχουν μηχανισμοί, οι οποίοι φροντίζουν τη διαχείριση των κλειδιών αυτών. Σε περίπτωση μη ορθής προστασίας των κλειδιών κρυπτογράφησης, ο επιτιθέμενος έχει τη δυνατότητα να τα υποκλέψει και να τα χρησιμοποιήσει σε επιθέσεις τύπου MiTM (Man in The Middle), όπου θα μπορεί να αποκρυπτογραφήσει τα δεδομένα τα οποία έχει συλλέξει από την επικοινωνία των κόμβων, που παρείσφρησε. Αυτό καθιστά την ορθή προστασία των εν λόγω κλειδιών απαραίτητη για την ασφάλεια ενός αδόμητου οχηματικού δικτύου [29].

Πίνακας 2.2 Συγκεντρωτικός πίνακας ζητημάτων ασφάλειας στα VANETs

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
Ασφάλεια-οχήματα	**Επαλήθευση ταυτότητας** (Η διαδικασία κατά την οποία κάθε κόμβος επιβεβαιώνει την ταυτότητα του με διάφορους τρόπους όπως πιστοποιητικά και ψευδώνυμα.)	[29]	**GPS spoofing** (Ο επιτηθέμενος παράγει ψεύτικα σήματα με την τοποθεσία που επιθυμεί αυτός με αποτελέσμα να υπερκαλύψουν τα πραγματικά σήματα που χρειάζεται ο κόμβος. Ως αποτέλεσμα έχει την παρέκκλιση του χρήστη από τον αρχικό στόχο)	[29]	Confidentiality, Integrity, Availability	CVE-2012-6334	Low: 2.9	None	Partial	None
						CVE-2012-6335	Low: 3.3	None	Partial	None
						CVE-2012-6336	Low: 3.3	None	Partial	None
						CVE-2014-9969	High: 10.0	Complete	Complete	Complete
	Κρυπτογράφηση (Λόγω της χαμήλης υπολογιστικής ισχυής που έχουν οι μονάδες των κόμβων δεν είναι δυνατή η χρήση πολύ ισχυρών αλγορίθμων κρυπτογράφησης.)	[29],[31]	**Man in the middle** (Ο επιτηθέμενος μπαίνει αναμέσα στην επικοινωνία δυο κόμβων και είτε μπορεί να αποκρυπτογραφήσει τα δεδομένα που ανταλλάσονται είτε να τα τροποποίησει για δικό του όφελος. Ως αποτέλεσμα είναι είτε η παρακολούθηση είτε η πραγματοποίηση κάποιας απάτης.) **Replay attack** (Ο επιτηθέμενος υποκλέπτει μια μετάδοση δεδομένων και στην συνεχεία μεταδίδει το δικό του τροποποιημένο πακέτο στους κόμβους. Ως αποτελέσμα έχει την εγκρίση πρόσβασης σε οργανισμούς είτε δίκτυα τα οποία δεν είχε πρόσβαση πριν.) **Bruteforce** (Ο επιτηθέμενος προσπαθεί να παραβίασει τα στοιχεία σύνδεσης κάποιου χρήστη με την εξαντλητική χρήση κωδικών και ονόματος χρήστη. Ως αποτέλεσμα έχει την πρόσβαση στο σύστημα και την υποκλοπή δεδομένων.)	[29], [31]	Confidentiality, Integrity	CVE-1999-0667	High: 10.0	Complete	Complete	Complete
	Διαθεσιμότητα (Αφορά την διαθεσιμότητα των	[29]	**DOS attack** (Ο επιτηθέμενος στέλνει μεγαλό αριθμό πακέτων στον κόμβο, με αποτέλεσμα λόγω της μικρής	[29]	Availability	CVE-2017-15815	High: 10.0	Complete	Complete	Complete

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
	καναλιών επικονωνίας και του χώρου προσωρινής αποθήκευσης ώστε να υπάρχει ομαλή λειτουργία του δικτύου.)		επεξεργαστικής ισχύς των μονάδων του κόμβου να υπερχειλίζει ο χώρος αποθήκευσης. Το αποτέλεσμα είναι η δυσλειτουργία του κόμβου.)			CVE-2017-15822	High: 8.3	Complete	Complete	Complete
	Εμπιστευτικότητα (Λόγω του περιορισμένου χώρου αποθηκέυσης στην μονάδα του κόμβου, είναι δύσκολο να συγκρατήσει το μεγάλο μέγεθος μοναδικών ταυτοτήτων του κάθε κόμβου ώστε να τους αναγνωρίσει μελλοντικά.)	[29]	**Impersonation attack** (Ο επιτηθέμενος προσποιείται ότι είναι κάποιος άλλος από τους κόμβους με αποτέλεσμα να αποσπάσει ευαίσθητα στοιχεία.)	[29]	Confidendiality					
	Ευπάθειες επεξεργαστικής μονάδας κόμβου (Κενά ασφαλείας που παρουσιάζονται στα διάφορα εξαρτήματα της μονάδας του κόμβου.)	[29],[30]	**Malware** (Ο επιτηθέμενος εγκαθιστά το κακόβουλο λογισμικό στα συστήματα που παρουσιάζουν κάποιο κενό ασφαλείας με αποτέλεσμα είτε να υποκλέψει δεδομένα είτε να προκαλέσει κάποια βλάβη σε αυτά.)	[29],[30]	Confidentiality, Availability	CVE-2020-36244	High: 7.5	Complete	Partial	Partial
	Ασφάλεια στο όχημα (Οι επιβάτες είτε κάποιος οδηγός που έχει φυσική πρόσβαση στο όχημα μπορεί να τροποιήση το σύστημα προς δικό του όφελος.)	[30],[31]	**Message falsification** (Ο επιτηθέμενος τροποποιεί με τέτοιο τρόπο τα μηνύματα που πρόκειται να μεταδοθούν ώστε να αποκτήση χρήσιμες πληροφορίες από το θύμα ή να προκαλέσει κάποια ζημιά.)	[30]	Integrity					

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
	Ευπάθειες στους αισθήτηρες του οχήματος (Ευπάθειες που μπορεί να παρουσιάζονται στους αισθητήρες του κάθε οχήματος.)	[30]	**Sensor spoofing** (Ο επιτηθέμενος αποκτά πρόσβαση και τροποποιεί τα παραγόμενα δεδομένα των αισθητήρων με αποτέλεσμα να προκληθούν λαθός εκτιμήσεις και ίσως ατυχήματα.) **Sensor jamming** (Ο επιτηθέμενος παράγει πολλά σήματα τα οποία υπερχειλίζουν τον αισθητήρα με αποτέλεσμα την λάθος λειτουργία του και την εμφάνιση λάθος αποτελεσμάτων.)	[30]	Availability					

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
Ασφάλεια στην υποδομή	**Επαλήθευση ταυτότητας** (Η διαδικασία κατά την οποία κάθε κόμβος επιβεβαιώνει την ταυτότητα του με διάφορους τρόπους όπως πιστοποιητικά και ψευδώνυμα.)	[29],[1]	**Impersonation attack** (Ο επιτηθέμενος προσποιείται ότι είναι κάποιος άλλος από τους κόμβους με αποτέλεσμα να αποσπάσει ευαίσθητα στοιχεία.) **Sybil attack** (Ο επιτηθέμενος παράγει πολλαπλά μηνύματα τα οποία εμφανίζονται ως απεσταλμένα από πολλαπλές διαφορετικές πηγές με αποτέλεσμα το θύμα να θεωρήσει την πληροφορία του μηνύματος ορθή και έτσι να ενεργήσει με τον τρόπο τον οποίο θέλει ο επιτηθέμενος.)	[29],[1]	Confidentiality, Availability	CVE-2010-3869	Medium: 4.0	None	Partial	None
						CVE-2010-3868	Medium: 5.8	Partial	Partial	None
						CVE-2018-1000625	High: 10.0	Complete	Complete	Complete
	Άπληστοι οδηγοί (Οι οδηγοί οι οποίοι επιτήθενται στο δίκτυο για προσωπικό τους όφελος.)	[29],[2]	**Message falsification** (Ο επιτηθέμενος τροποποιεί με τέτοιο τρόπο τα μηνύματα που πρόκειται να μεταδοθούν ώστε να αποκτήση χρήσιμες πληροφορίες από το θύμα ή να προκαλέσει κάποια ζημιά.) **Message delay attack** (Τα μηνύματα μεγάλης σημασίας όπως αποφυγής κινδύνου μεταφέρονται με καθυστέρηση με αποτέλεσμα να υπάρξει κίνδυνος ατυχήματος.)	[29],[2]	Integrity					
	Τμηματοποίηση του δικτύου σε επιμέρους δίκτυα	[29]	**DOS attack** (Ο επιτηθέμενος στέλνει μεγαλό αριθμό πακέτων στον κόμβο, με	[29]	Availability	CVE-2017-15815	High: 10.0	Complete	Complete	Complete

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
	(Λόγω της μικρής εμβέλειας που έχουν οι κεραίες σε ένα οχηματικό δίκτυο, το δίκτυο τμηματοποιείται σε πολλά επιμέρους δίκτυα.)		αποτέλεσμα ο χώρος προσωρινής αποθήκευσης να γεμίσει και να απορρίψει τα σημαντικά πακέτα.) **Jamming attack** (Ο επιτηθέμενος παρεμβάλει και μπλοκάρει το σήμα προς τον κόμβο στόχο με αποτέλεσμα να μην είναι δυνατή η επικονωνία μεταξύ σταθμού και κόμβου.)			CVE-2017-15822	High: 8.3	Complete	Complete	Complete
	Ιδιωτικότητα (Να μην έχουν πρόσβαση στην τοποθεσία και ταυτότητα του χρήστη πέρα από τον ίδιο.)	[1],[30],[32], [29]	**Impersonation attack** (Ο επιτηθέμενος προσποιείται ότι είναι κάποιος άλλος από τους κόμβους με αποτέλεσμα να αποσπάσει ευαίσθητα στοιχεία.) **Repudiation attack** (Ο επιτηθέμενος προσποιούμενος κάποιον άλλον κόμβο μπορεί να διαφυγεί από παραβιάσεις, προστίματα κ.α)	[1],[30],[32], [29]	Confidentiality					
	Κενά ασφαλείας σε μέρη της υποδομής (Συσκεύες της υποδομής οι οποίες δεν έχουν εγκατεστημένες τις τελευταίες ενημερώσεις ασφάλειας.)	[1]	**Malware** (Ο επιτηθέμενος εγκαθιστά το κακόβουλο λογισμικό στα συστήματα που παρουσιάζουν κάποιο κενό ασφαλείας με αποτέλεσμα είτε να υποκλέψει δεδομένα είτε να προκαλέσει κάποια βλάβη σε αυτά.)	[1]	Confidentiality, Availability	CVE-2020-36244	High: 7.5	Complete	Partial	Partial

	Ζητήματα ασφαλείας	Βιβλιογραφία-Ασφάλεια	Τύποι επιθέσεων	Βιβλιογραφία-Επιθέσεις	CIA	CVE	CVSS	Confidentiality	Integrity	Availability
	Ασφάλεια στην διαχείριση των κλειδιών (Σε περίπτωση μη ορθής προστασίας των κλειδιών είτε ταυτότητας είτε κρυπτογράφησης υπάρχει κίνδυνος υποκλοπής δεδομένων.)	[29]	**Man in the middle** (Ο επιτηθέμενος μπαίνει αναμέσα στην επικοινωνία δυο κόμβων και είτε μπορεί να αποκρυπτογραφήσει τα δεδομένα που ανταλλάσονται είτε να τα τροποποίησει για δικό του όφελος. Ως αποτέλεσμα είναι είτε η παρακολούθηση είτε η πραγματοποίηση κάποιας απάτης.)	[29]	Confidentiality, Integrity	CVE-1999-0667	High: 10.0	Complete	Complete	Complete

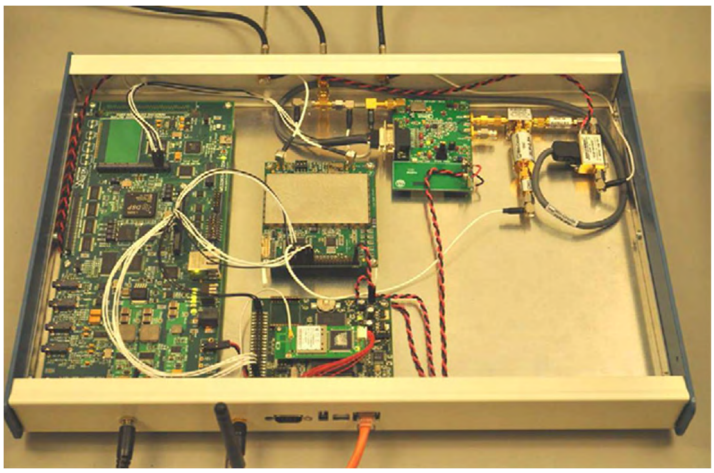
2.7 Επιθέσεις στα αδόμητα οχηματικά δίκτυα

Τα αδόμητα οχηματικά δίκτυα, λόγω της αρχιτεκτονικής τους αλλά και λόγω του τρόπου λειτουργίας τους, παρουσιάζουν ένα πλήθος ζητημάτων, που αφορούν την ασφάλεια του δικτύου και των κόμβων αυτού. Εκμεταλλευόμενοι τα ζητήματα αυτά, οι επιτιθέμενοι, έχουν τη δυνατότητα να οργανώσουν και να πραγματοποιήσουν μια γκάμα από επιθέσεις διαφορετικού τύπου, όπου η καθεμία έχει έναν συγκεκριμένο στόχο. Οι επιθέσεις αυτές μπορούν να χωριστούν σε κατηγορίες, ανάλογα με το αν επηρεάζουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (Integrity) και τη διαθεσιμότητα (availability) του αδόμητου οχηματικού δικτύου, όπως φαίνεται και στον Πίνακα 2. Παρακάτω, προβαίνουμε σε αναλυτική περιγραφή μερικών επιθέσεων, που παρατηρούνται στα αδόμητα οχηματικά δίκτυα.

2.7.1 GPS Spoofing

Οι εφαρμογές, που κάνουν χρήση των δεδομένων τοποθεσίας, πληθαίνουν διαρκώς. Οι εφαρμογές αυτές ποικίλουν, από εφαρμογές πλοήγησης μέχρι εφαρμογές ψυχαγωγίας, οι οποίες βασίζονται στην ακριβή τοποθεσία του χρήστη. Για τον λόγο, αυτό τα δεδομένα τοποθεσίας είναι πολύ σημαντικά και πρέπει να χαρακτηρίζονται από ακρίβεια και αξιοπιστία. Για τη συλλογή των δεδομένων τοποθεσίας γίνεται χρήση των παγκόσμιων δορυφορικών συστημάτων πλοήγησης.

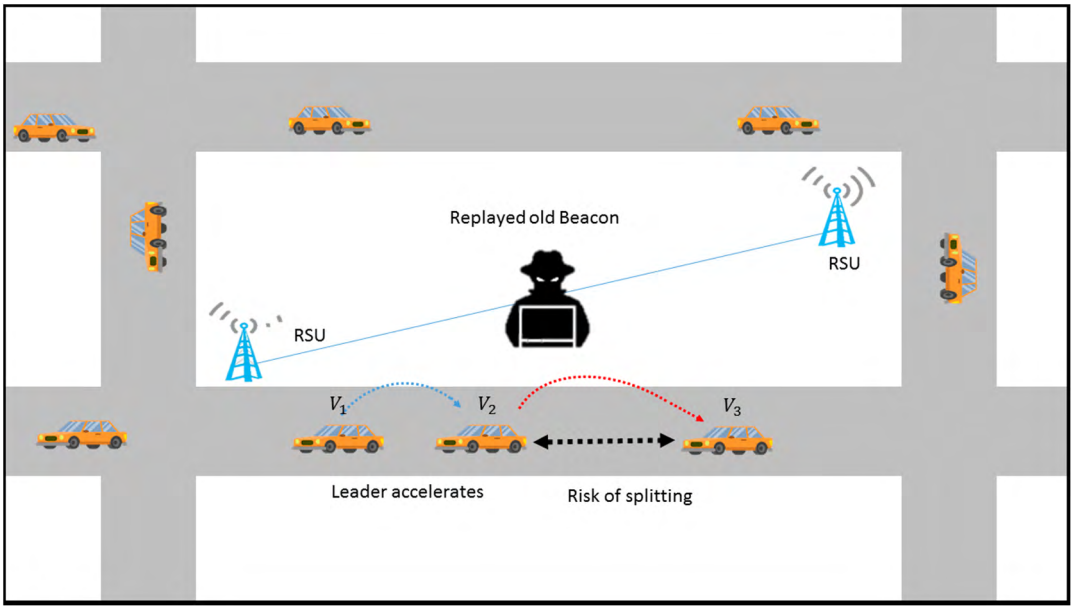
Στο πλαίσιο της επίθεσης GPS Spoofing, ο σκοπός του επιτιθέμενου είναι είτε η αλλοίωση της πραγματικής τοποθεσίας ενός κόμβου είτε η παραπλάνηση άλλων κόμβων σε σημείο, που εκείνος επιθυμεί. Κάθε όχημα και κάθε σύγχρονη συσκευή είναι εξοπλισμένα με έναν δέκτη GPS. Προκειμένου, λοιπόν, να επιτευχθεί η επίθεση είναι απαραίτητο ο επιτιθέμενος, με τη χρήση ενός ειδικά διαμορφωμένου πομπού (GPS Spoofer), να εκπέμψει σήματα εντοπισμού ισχυρότερα από αυτά του πραγματικού δορυφόρου, με αποτέλεσμα ο δέκτης να θεωρήσει τα κακόβουλα σήματα, ως τα πραγματικά δορυφορικά σήματα. Η πραγματοποίηση μιας τέτοιας επίθεσης γίνεται ευκολότερη, όταν υπάρχουν πλατφόρμες ανάπτυξης, όπως τα HackRF και bladeRF, τα οποία διευκολύνουν τον επιτιθέμενο στη δημιουργία ενός πομπού (GPS Spoofer). Ο μικρός βαθμός δυσκολίας, στην υλοποίηση της συγκεκριμένης επίθεσης, την καθιστά αρκετά επικίνδυνη. Στην Εικόνα 2.18 παρουσιάζεται ένα παράδειγμα ενός πομπού (GPS Spoofer) [4],[35].



Εικόνα 2.18 *GPS Spoofer [34]*

2.7.2 Replay attack

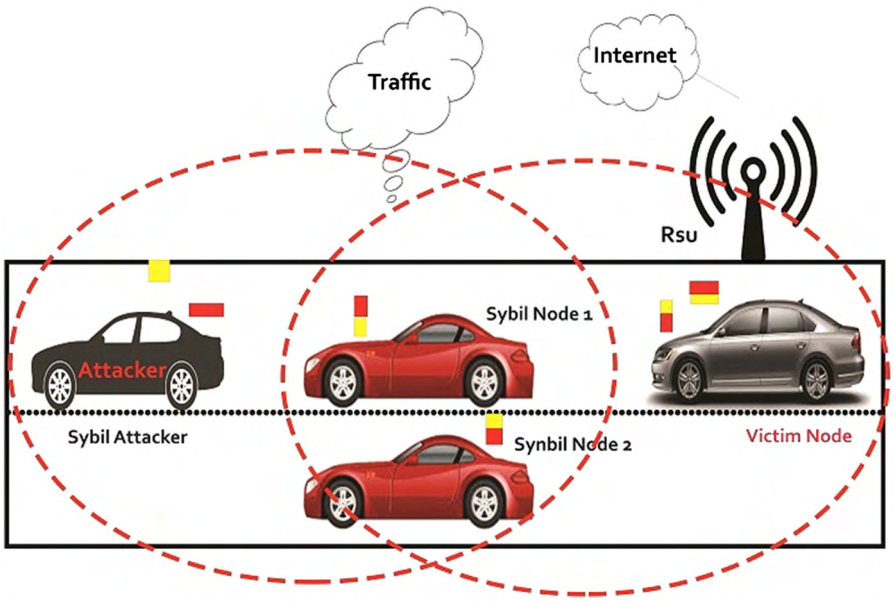
Μέσα σε ένα αδόμητο οχηματικό δίκτυο είναι πολύ σημαντική η ορθή αποστολή και λήψη των μηνυμάτων, τα οποία περιέχουν πληροφορίες μεγάλης αξίας. Η επίθεση επανάληψης των μηνυμάτων (Replay attack) θεωρείται ως μια από τις κλασικές επιθέσεις. Κατά την πραγματοποίηση αυτής, ο επιτιθέμενος μεταδίδει ξανά κάποιο μήνυμα, το οποίο έχει αποσταλεί προς τους παραλήπτες. Ο επιτιθέμενος έχει τη δυνατότητα να ενθυλακώσει το μήνυμα, που επιθυμεί, μέσα σε πακέτα του δικτύου, τα οποία έχουν ήδη ληφθεί και να τα μεταδώσει ξανά. Με τον τρόπο αυτό, είναι σε θέση να επαναλάβει την αποστολή πλαισίων-φάρων (Beacons) με σκοπό τον έλεγχο της τοποθεσίας και του πίνακα δρομολόγησης ενός κόμβου. Τέλος, η επίθεση αυτή μπορεί να υλοποιηθεί και από μη νόμιμους κόμβου του δικτύου σε αντίθεση με άλλες επιθέσεις. Στην Εικόνα 2.19 απεικονίζεται ένα παράδειγμα της επίθεσης [4],[6].



Εικόνα 2.19 *Replay attack [36]*

2.7.3 Sybil attack

Σε επιθέσεις τύπου Sybil, ο επιτιθέμενος κόμβος δημιουργεί πολλές ψεύτικες ταυτότητες ή έχει καταφέρει μέσω άλλων επιθέσεων να υποκλέψει ταυτότητες κόμβων του δικτύου και να τις χρησιμοποιήσει προς όφελός του. Άρα, ο κακόβουλος κόμβος γεμίζει το δίκτυο με κόμβους, οι οποίοι δεν υφίστανται στην πραγματικότητα αλλά απλά εμφανίζονται στο δίκτυο, λόγω των ψεύτικων ταυτοτήτων που έχει δημιουργήσει. Κατά την διάρκεια της επίθεσης αυτής, ο επιτιθέμενος φτάνει να έχει τον έλεγχο ενός μεγάλου αριθμού ψεύτικων κόμβων (Sybil 's), οι οποίοι διαμοιράζονται ψευδείς πληροφορίες με τους υπόλοιπους κόμβους. Η συγκεκριμένη επίθεση μπορεί να χαρακτηριστεί και ως επίθεση ψευδαίσθησης (illusion attack), καθώς οι μολυσμένοι κόμβοι μπορούν να μεταδώσουν ψευδή μηνύματα για κάποιο ατύχημα ή για κάποια επερχόμενη συμφόρηση, δημιουργώντας μια ψευδαίσθηση στο θύμα, με αποτέλεσμα τον έλεγχο της κυκλοφορίας στο οδικό δίκτυο. Επιπλέον, σε περιβάλλοντα και εφαρμογές, όπου οι κόμβοι καλούνται να συμμετάσχουν σε ψηφοφορίες εντός του δικτύου, ο επιτιθέμενος, μπορεί να χρησιμοποιήσει το αποτέλεσμα μιας τέτοιας ψηφοφορίας προς όφελός του. Συνεπώς, καταλήγουμε αβίαστα στο συμπέρασμα ότι ο βαθμός επικινδυνότητας μιας τέτοιας επίθεσης είναι μεγάλος. Στην Εικόνα 2.20 απεικονίζεται ένα σενάριο της Sybil attack [4],[6],[29],[30],[38].

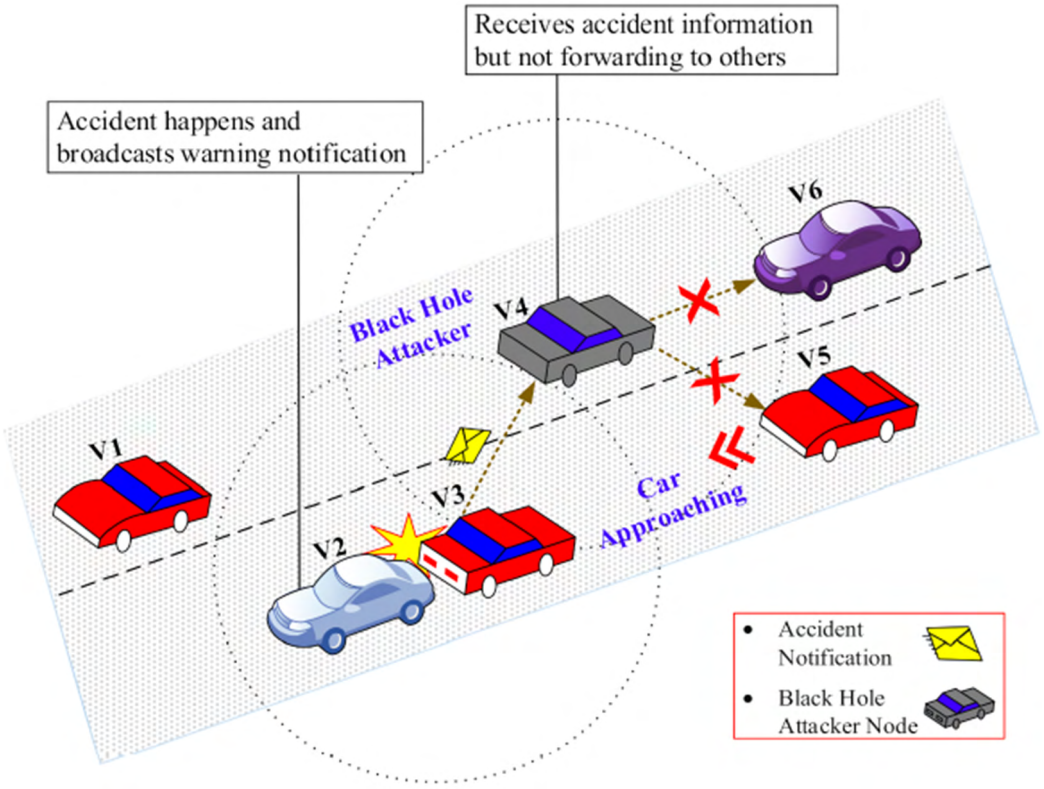


Εικόνα 2.20 *Sybil attack [37]*

2.7.4 Blackhole attack

Σε όλα τα αδόμητα, δίκτυα επομένως, και στα αδόμητα οχηματικά δίκτυα γίνεται επικοινωνία μεταξύ των κόμβων. Ο κάθε κόμβος μπορεί να μεταδώσει πακέτα προς έναν προορισμό και στη συνέχεια οι κόμβοι, που παρεμβάλλονται μέχρι τον τελικό προορισμό, να αναμεταδώσουν τα πακέτα

αυτά. Στην συγκεκριμένη επίθεση, ο επιτιθέμενος είναι νόμιμος χρήστης του δικτύου και, κατά την υλοποίηση της επίθεσης, λαμβάνει τα πακέτα, που προορίζονται για αυτόν. Όμως, δεν μεταδίδει τα πακέτα στον επόμενο κατά σειρά κόμβο, για τον οποίο προορίζονται. Αυτό έχει ως αποτέλεσμα, λόγω της αλλοίωσης που προκαλείται στους πίνακες δρομολόγησης των κόμβων του δικτύου, τα σημαντικά μηνύματα αποφυγής κινδύνου να μη φτάνουν στους τελικούς χρήστες, καθιστώντας την επίθεση αυτή εξαιρετικά επικίνδυνη για την λειτουργία του δικτύου και την ασφάλεια των οδηγών. Στην Εικόνα 2.21 απεικονίζεται ένα σενάριο της επίθεσης μαύρης τρύπας (Blackhole attack) [4],[6],[29].

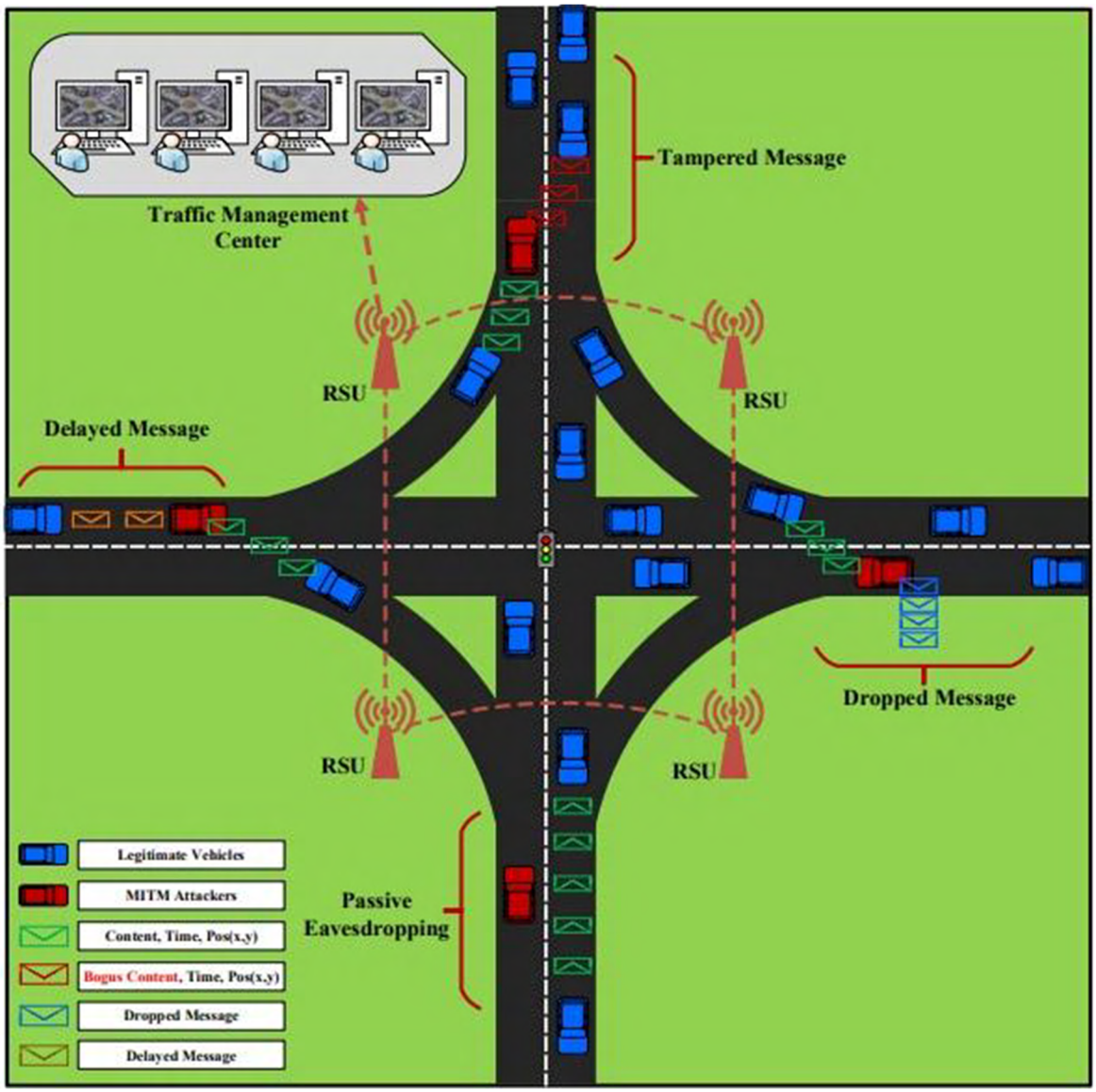


Εικόνα 2.21 *Blackhole attack [39]*

2.7.5 Man in The Middle attack

Στα αδόμητα οχηματικά δίκτυα οι κόμβοι μπορούν να εγκαθιδρύσουν ένα κανάλι επικοινωνίας για ανταλλαγή πληροφοριών με άλλους κόμβους εντός της εμβέλειάς τους και με παρόδιες μονάδες. Στις επιθέσεις τύπου Man in The Middle (MiTM), ο επιτιθέμενος καταφέρνει να παρεισφρήσει στο κανάλι επικοινωνίας και να τοποθετήσει τον εαυτό του ανάμεσα στον αποστολέα και τον παραλήπτη. Οι κόμβοι δεν αντιλαμβάνονται την παρουσία του κακόβουλου χρήστη και συνεχίζουν την ανταλλαγή μηνυμάτων, θεωρώντας ότι βρίσκονται σε άμεση επικοινωνία, όμως ο επιτιθέμενος ελέγχει την επικοινωνία. Ο ίδιος μπορεί να είναι παθητικός, όπου απλά παρακολουθεί το κανάλι και συλλέγει τις ευαίσθητες πληροφορίες προς όφελός του. Ωστόσο, μπορεί να είναι ενεργητικός, όπου στην περίπτωση αυτή τροποποιεί και αναμεταδίδει τα πακέτα, που συλλέγει, ή

εισάγει καθυστέρηση σε ένα πακέτο, ή απορρίπτει πακέτα. Η επίθεση αυτή έχει ως αποτέλεσμα, τη μη ορθή λειτουργία του δικτύου, καθώς και τη διαρροή ευαίσθητων δεδομένων. Στην Εικόνα 2.22 παρουσιάζεται ένα σενάριο επίθεσης MiTM [6],[41].

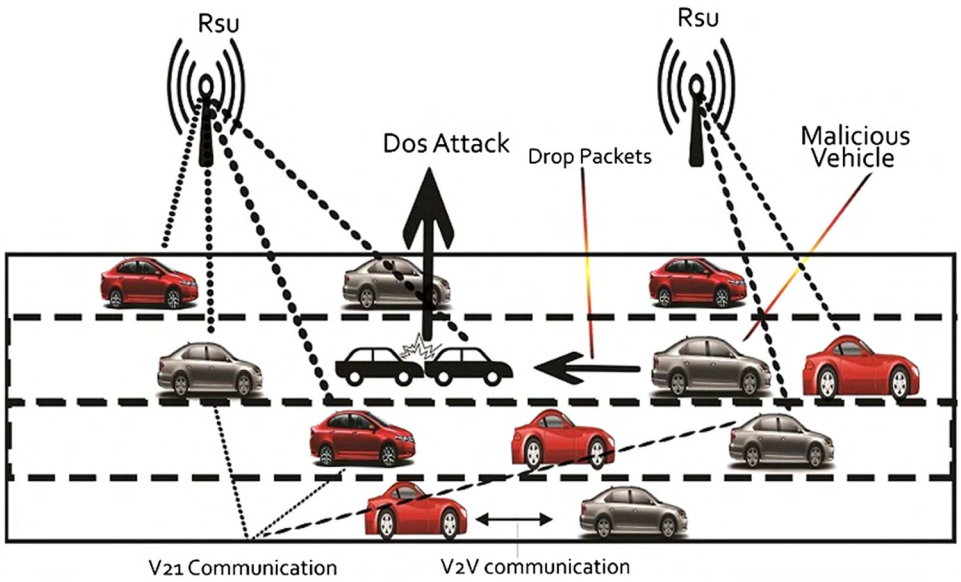


Εικόνα 2.22 *Man in The Middle attack [40]*

2.7.6 DoS attack

Μια από τις βασικότερες απαιτήσεις των αδόμητων οχηματικών δικτύων είναι η διαθεσιμότητα. Μέσω αυτής, επιτυγχάνεται η ασφάλεια τόσο των οδηγών, όσο και των κόμβων του δικτύου, μέσω της ανταλλαγής σημαντικών μηνυμάτων. Η ασφάλεια των οδηγών και των οχημάτων βρίσκεται πολλές φορές στο στόχαστρο των επιτιθέμενων, όπου με την πραγματοποίηση επιθέσεων τύπου DoS (Denial Of Service) έχουν ως στόχο να πλήξουν τη διαθεσιμότητα του δικτύου. Οι επιθέσεις τύπου DoS θεωρούνται από τις πιο διαδεδομένες και επικίνδυνες σε ένα αδόμητο οχηματικό δίκτυο.

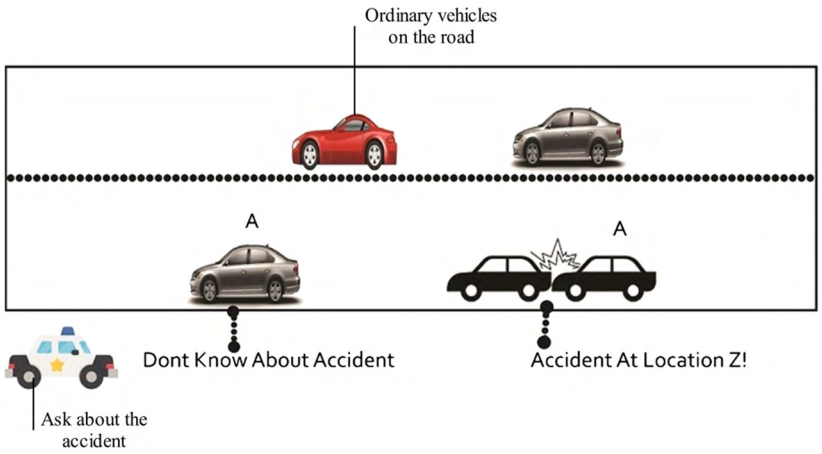
Ο επιτιθέμενος, ο οποίος μπορεί να είναι κάποια εσωτερική οντότητα του δικτύου ή κάποια εξωτερική, προσπαθεί να παρεμποδίσει τους χρήστες από το να χρησιμοποιήσουν υπηρεσίες του δικτύου. Είναι εφικτό να το επιτύχει με πολλαπλούς τρόπους, όπως για παράδειγμα, να κρατήσει απασχολημένο έναν κόμβο, αποστέλλοντάς του συνεχώς μεγάλο αριθμό επαναλαμβανόμενων μηνυμάτων, τα οποία ο κόμβος πρέπει να επεξεργαστεί. Με τον τρόπο αυτό, κρατά απασχολημένο τον κόμβο και δεν του επιτρέπει να κάνει χρήση κάποιας άλλης υπηρεσίας εντός του δικτύου. Στην Εικόνα 2.23 απεικονίζεται ένα σενάριο επίθεσης DoS [4],[6],[29].



Εικόνα 2.23 *DoS attack [37]*

2.7.7 Impersonation attack

Κάθε κόμβος, μέσα σε ένα αδόμητο οχηματικό δίκτυο, έχει μια ταυτότητα, χάρη στην οποία μπορεί να ξεχωρίζει σε σχέση με τους υπόλοιπους, όπως γίνεται και στην καθημερινότητα των ανθρώπων. Σε επιθέσεις, που αφορούν την ταυτότητα, όπως η επίθεση πλαστοπροσωπίας (Impersonation attack), ο επιτιθέμενος καταφέρνει να πείσει τους υπόλοιπους κόμβους σχετικά με την αυθεντικότητα της πηγής των μηνυμάτων. Κάθε κόμβος είναι συνδεδεμένος με κάποιο αναγνωριστικό μέσα στο δίκτυο, όπου σε περιπτώσεις ατυχημάτων είναι αναγκαία η χρήση του, με σκοπό να βρεθεί ο υπαίτιος. Στην επίθεση πλαστοπροσωπίας, ο επιτιθέμενος είναι ικανός να προβάλλει τον εαυτό του ως επαληθευμένο αποστολέα του μηνύματος. Στην συνέχεια, λαμβάνει το μήνυμα του αποστολέα και το παραμετροποιεί προς δικό του όφελος, προτού να το αποστείλει στους επιθυμητούς κόμβους. Στην Εικόνα 2.24 παρουσιάζεται ένα σενάριο επίθεσης πλαστοπροσωπίας [6],[29].



Εικόνα 2.24 *Impersonation attack [37]*

2.7.8 Malware

Οι επιθέσεις κακόβουλου λογισμικού (malware attacks) έχουν αυξηθεί τα τελευταία χρόνια, με αποτέλεσμα να αποτελούν κίνδυνο και για τα αδόμητα οχηματικά δίκτυα. Μια επίθεση malware μπορεί να αποτελείται από επιμέρους τμήματα, όπως ιούς (viruses), σκουλήκια (worms) και δούρειους ίππους (Trojans). Το malware είναι ικανό να εξαπλωθεί μέσα σε ένα αδόμητο οχηματικό δίκτυο, μέσω των διαφημίσεων που προβάλλουν οι παρόδιες μονάδες. Μια τέτοια πιθανή εξάπλωση θα μπορούσε να απειλήσει την ασφάλεια, την ιδιωτικότητα αλλά και τη διαθεσιμότητα του δικτύου. Οι παρόδιες μονάδες, όπως και οι επεξεργαστικές μονάδες, χρησιμοποιούν πακέτα λογισμικού, τα οποία πιθανόν να παρουσιάζουν κενά ασφάλειας, όπου κάποιος κακόβουλος χρήστης μπορεί να εκμεταλλευτεί, με σκοπό να εγκαταστήσει κάποιο κακόβουλο λογισμικό. Λόγω της αρχιτεκτονικής των συστατικών αυτών των αδόμητων οχηματικών δικτύων, δεν είναι εφικτή η εγκατάσταση λογισμικού προστασίας από malware (anti-malware), γεγονός που τα καθιστά αρκετά ευάλωτα. Το Emotet είναι ένα παράδειγμα malware, που μπορούμε να συναντήσουμε στα αδόμητα οχηματικά δίκτυα [42],[43],[44],[45].

2.7.9 Message Falsification attack

Πολλές εφαρμογές στα αδόμητα οχηματικά δίκτυα, όπως επίσης και η επικοινωνία σε αυτά, βασίζονται στην ανταλλαγή μηνυμάτων, που περιέχουν χρήσιμη πληροφορία ανάλογα με τον σκοπό τους. Στην επίθεση παραποίησης μηνυμάτων (Message Falsification attack), ο επιτιθέμενος τροποποιεί ένα συγκεκριμένο μέρος του μηνύματος προς όφελός του και στην συνέχεια το αναμεταδίδει στους υπόλοιπους κόμβους του δικτύου. Πιο συγκεκριμένα, ο επιτιθέμενος τροποποιεί τα μηνύματα, που έχει λάβει σχετικά με επερχόμενη συμφόρηση στο οδικό δίκτυο με τρόπο τέτοιο, ώστε το μήνυμα να υποδεικνύει ότι δεν υπάρχει επερχόμενη συμφόρηση. Αυτό έχει ως απόρροια,

τον έλεγχο της κυκλοφορίας ενός δικτύου και τη μη ορθή λειτουργία αυτού. Η επίθεση αυτή επηρεάζει την ακεραιότητα [4],[6].

2.7.10 Sensor Spoofing

Τα σύγχρονα οχήματα είναι εξοπλισμένα με σημαντικό αριθμό αισθητήρων, που ο καθένας επιτελεί μια ξεχωριστή λειτουργία. Οι αισθητήρες αυτοί, δέχονται και παράγουν δεδομένα, τα οποία είναι χρήσιμα για τα οχήματα και τους οδηγούς. Στο πλαίσιο της επίθεσης Sensor Spoofing, ο επιτιθέμενος μπορεί αφενός να τροποποιήσει τα δεδομένα, που παράγει ένας αισθητήρας δίνοντας λάθος πληροφορίες στα κοντινά του οχήματα, και αφετέρου να δημιουργήσει και να αποστείλει ο ίδιος ψευδείς πληροφορίες προς κάποιον αισθητήρα ενός κόμβου. Αυτό μπορεί να έχει ως αποτέλεσμα τη λήψη λάθος αποφάσεων από τους οδηγούς και την πιθανή πρόκληση κάποιου ατυχήματος [30].

2.7.11 Sensor Jamming

Οι αισθητήρες, λοιπόν, αποτελούν σημαντικό κομμάτι της ασφάλειας των οχημάτων στα σύγχρονα οδικά δίκτυα. Οι αισθητήρες βασίζονται σε μια κεραία, ώστε να λαμβάνουν τα σήματα σχετικά με διάφορα συμβάντα. Αφού λάβουν τα σήματα, θα πρέπει στην συνέχεια να τα επεξεργαστούν, ώστε να ενημερώσουν με κατάλληλο μήνυμα τον οδηγό. Σε μια επίθεση παρεμβολής του αισθητήρα (Sensor Jamming), ο επιτιθέμενος προσπαθεί να υπερχειλίσει τον δέκτη του αισθητήρα είτε με σήματα, τα οποία περιέχουν ψευδή πληροφορία, είτε με σήματα θορύβου, τα οποία μεταδίδει στον αισθητήρα με πολύ μεγάλη συχνότητα. Έτσι, ο αισθητήρας παραμένει απασχολημένος, με αποτέλεσμα να μην είναι σε θέση να δεχτεί σήματα πραγματικών γεγονότων, το οποίο είναι εξαιρετικά επικίνδυνο για την ασφάλεια των οχημάτων. Στην περίπτωση της μετάδοσης σημάτων με ψευδή πληροφορία, ο αισθητήρας παράγει λανθασμένες ειδοποιήσεις στον οδηγό, οδηγώντας τον σε λάθος αποφάσεις. Με την επίθεση αυτή, ο επιτιθέμενος στοχεύει να βλάψει τη διαθεσιμότητα και κατ' επέκταση την ασφάλεια του δικτύου [4],[6],[30].

2.7.12 Message Delay attack

Οι εφαρμογές ασφάλειας βασίζονται στην άμεση ανταλλαγή μηνυμάτων μεταξύ των κόμβων. Οι επιτιθέμενοι μπορούν να επηρεάσουν την ασφάλεια των οδηγών, πραγματοποιώντας μια επίθεση καθυστέρησης μηνυμάτων (Message Delay attack). Κατά την επίθεση αυτή, ο κακόβουλος κόμβος εισάγει μια καθυστέρηση στην προώθηση του πακέτου προς τον επόμενο, με αποτέλεσμα το πακέτο να φτάσει καθυστερημένα. Στην περίπτωση αυτή, εάν ένα πακέτο, το οποίο περιέχει πληροφορίες

σχετικά με κάποιο επερχόμενο κίνδυνο, καθυστερήσει να φτάσει στον παραλήπτη, υπάρχει μεγάλη πιθανότητα να προκληθεί κάποιο ατύχημα [29],[46].

2.7.13 Repudiation attack

Ο μηχανισμός μη αποκήρυξης είναι πολύ σημαντικός για την ασφάλεια ενός αδόμητου οχηματικού δικτύου, καθώς διασφαλίζει ότι ο αποστολέας και ο παραλήπτης ενός μηνύματος δεν μπορούν να αρνηθούν ότι απέστειλαν και παρέλαβαν κάποιο μήνυμα αντίστοιχα. Σε μια επίθεση αποκήρυξης, ο επιτιθέμενος αρνείται να συμμετάσχει σε οποιαδήποτε δραστηριότητα αφορά την αποστολή ή τη λήψη μηνυμάτων, σε περίπτωση αμφισβήτησης αυτού από τρίτους [4],[6],[29].

Κεφάλαιο 3: Εργαλεία και μέθοδοι

3.1 Προσομοιωτές κίνησης

Κατά την αναβάθμιση ενός αστικού κέντρου, ένα πολύ σημαντικό κομμάτι, το οποίο αναβαθμίζεται ή υλοποιείται από την αρχή, είναι το οδικό δίκτυο. Παράλληλα με τις μελέτες γίνεται χρήση των προσομοιωτών κίνησης. Με τη βοήθεια των προσομοιωτών κίνησης, οι πολιτικοί μηχανικοί έχουν μια πιο ρεαλιστική εικόνα, ως προς το ποια τμήματα του οδικού δικτύου είναι ωφέλιμα να κατασκευαστούν και ποια όχι.

Οι προσομοιωτές κίνησης είναι σε θέση να απεικονίσουν την κίνηση με βάση κάποια μοντέλα κίνησης, τα οποία οι συγκοινωνιολόγοι κατατάσσουν σε τρεις διακριτές κατηγορίες με γνώμονα τη ροή κίνησης, που εξετάζει το καθένα [47],[48]. Τα μοντέλα κίνησης είναι τα εξής:

- **Μακροσκοπικά (macroscopic)**: Τα μοντέλα αυτά μοντελοποιούν την κίνηση σε ευρεία κλίμακα, βασιζόμενα σε μαθηματικά μοντέλα. Απεικονίζουν τη ροή της κίνησης ως ένα υδάτινο ρεύμα. Λόγω της μη λεπτομερούς ανάλυσης της κίνησης, τα μοντέλα αυτά δεν έχουν μεγάλες απαιτήσεις σε υπολογιστικούς πόρους και χαρακτηρίζονται από ταχύτητα στην εκτέλεση, κάτι που τα καθιστά κατάλληλα για προσομοιώσεις σε οδούς ταχείας κυκλοφορίας. Τέλος, τα μοντέλα αυτά δεν εστιάζουν σε οχήματα μεμονωμένα αλλά σε ολόκληρα τμήματα του οδικού δικτύου.
- **Μικροσκοπικά (microscopic)**: Κατά τη δημιουργία ή τη μελέτη ενός αδόμητου οχηματικού δικτύου είναι πολύ σημαντική η επικοινωνία μεταξύ των οντοτήτων του, καθώς και η ακριβής θέση αυτών, ώστε να μπορεί να μοντελοποιηθεί. Τα μικροσκοπικά μοντέλα εστιάζουν στη μοντελοποίηση της κάθε οντότητας του δικτύου μεμονωμένα, παρέχοντας λεπτομερή ανάλυση. Για τον λόγο αυτό, έχουν χαρακτηριστεί ως τα καταλληλότερα για τη μοντελοποίηση αδόμητων οχηματικών δικτύων σε αστικά περιβάλλοντα. Όμως, λόγω του μεγάλου όγκου λεπτομερειών που παράγεται κατά την διάρκεια της ανάλυσης, οι απαιτήσεις τους σε φυσικούς πόρους κατά την προσομοίωση είναι αυξημένες, όπως και ο χρόνος εκτέλεσης.
- **Μεσοσκοπικά (mesoscopic)**: Τα χαρακτηριστικά τόσο των μακροσκοπικών, όσο και των μικροσκοπικών μοντέλων συνδυάζονται στα μεσοσκοπικά. Τα μεσοσκοπικά μοντέλα εστιάζουν λεπτομερώς στις οντότητες του δικτύου μεμονωμένα (πχ οχήματα), όπως ακριβώς και τα μικροσκοπικά, ενώ διαχειρίζονται τις διασυνδέσεις και τη συμπεριφορά των οντοτήτων αυτών με παρόμοιο τρόπο, όπως τα μακροσκοπικά μοντέλα. Επομένως, αναλύουν τη μέση ταχύτητα των οχημάτων συνολικά στο δίκτυο και όχι την αυξομείωση της ταχύτητας του οχήματος μεμονωμένα.

Υπάρχει μια ευρεία γκάμα λογισμικών προσομοίωσης κίνησης, τα οποία χρησιμοποιούνται και για τη μελέτη των αδόμητων οχηματικών δικτύων. Παρακάτω παρουσιάζονται μερικά από αυτά.

3.1.1 Simulation of Urban MObility (SUMO)

Το Γερμανικό Κέντρο Αεροναυπηγικής (German Aerospace Center) δημιούργησε το λογισμικό προσομοίωσης Simulation of Urban Mobility (SUMO) στις αρχές του 2001. Το συγκριμένο λογισμικό χαρακτηρίζεται ως ανοιχτού κώδικα. Θεωρείται κατάλληλο για την προσομοίωση μεγάλων οδικών δικτύων, αφού κάνει χρήση της μικροσκοπικής κλίμακας μοντελοποίησης. Τα τελευταία χρόνια και ύστερα από αρκετές αναβαθμίσεις, το SUMO παρέχει πλέον μια σουίτα λογισμικών προσομοίωσης κίνησης. Τα νεότερα εργαλεία του SUMO υποστηρίζουν περισσότερους τύπους εισόδου και μεγαλύτερη απόδοση. Επίσης, παρέχει μια ευρεία γκάμα από οντότητες, τις οποίες μπορεί να χρησιμοποιήσει ο χρήστης κατά τη δημιουργία ενός δικτύου, όπως για παράδειγμα οχήματα και σηματοδότες. Για τη δημιουργία και μελέτη ενός οδικού δικτύου το SUMO παρέχει δύο επιλογές: i) ο χρήστης μπορεί να δημιουργήσει ένα τυχαίο δίκτυο κάνοντας χρήση της εφαρμογής netgenerate, όπου παίρνει ως έξοδο το τυχαία παραγόμενο δίκτυο του SUMO, ii) ο χρήστης έχει τη δυνατότητα, σε περίπτωση που επιθυμεί να μελετήσει ένα πραγματικό οδικό δίκτυο, να κάνει χρήση του εργαλείου OpenStreetMaps και να παράγει το αντίστοιχο δίκτυο, όπου στη συνέχεια, με τη χρήση της εφαρμογής netconvert, μπορεί να διαμορφώσει το παραγόμενο αρχείο σε μορφή αναγνώσιμη από το SUMO [49],[50].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[3].

3.1.2 VANETMObiSim

Ένας ακόμα προσομοιωτής κίνησης είναι το VANETMObiSim. Το συγκεκριμένο εργαλείο κάνει χρήση της γλώσσας JAVA και θεωρείται ως μια επέκταση του CanuMobiSim. Το VANETMObiSim χρησιμοποιεί τόσο μακροσκοπικά, όσο και μικροσκοπικά μοντέλα κίνησης, γεγονός το οποίο βοηθά τον χρήστη στην απεικόνιση ενός πιο ρεαλιστικού περιβάλλοντος. Όπως και σε άλλους προσομοιωτές κίνησης, έτσι και στο εργαλείο αυτό ο χρήστης έχει τη δυνατότητα να παράγει τυχαίους χάρτες μέσα από αυτό, ή να εισάγει πραγματικούς χάρτες της επιλογής του. Στο VANETMObiSim η εισαγωγή χαρτών γίνεται μέσω του TIGER (Topologically Integrated Geographical Encoding and Referencing). Σε αυτήν την περίπτωση, η απεικόνιση γίνεται σε μακροσκοπικό επίπεδο. Όσον αφορά το μικροσκοπικό

[3] https://sumo.dlr.de/docs/index.html

επίπεδο απεικόνισης, το VANETMObiSim είναι ικανό για χρήση πολλαπλών μοντέλων κινητικότητας, όπως μοντέλα για διασταυρώσεις, αλλαγή λωρίδας και προσπέρασης. Όλα αυτά συντελούν στην πιο ρεαλιστική απεικόνιση της συμπεριφοράς των οχημάτων μέσα στο δίκτυο. Τέλος, στα πλεονεκτήματα του VANETMObiSim εντάσσεται και η δυνατότητα του για υποστήριξη προσομοιωτών δικτύου, όπως το ns-2, το GloMoSim και το QualNet [51].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[4].

3.1.3 STRAW

Το εργαλείο STRAW (Street Random Waypoint) ανήκει και αυτό στην οικογένεια των προσομοιωτών κίνησης. Μπορεί να χρησιμοποιηθεί για προσομοιώσεις που αφορούν μόνο πόλεις των Ηνωμένων Πολιτειών, γεγονός το οποίο περιορίζει τη χρήση του. Ένα ακόμα αρνητικό του εργαλείου είναι ότι η κίνηση των κόμβων περιορίζεται από τις οδούς, καθώς λειτουργεί με βάση τα αληθινά δεδομένα κυκλοφορίας για την εκάστοτε πόλη. Τέλος, το STRAW είναι σχεδιασμένο με τρόπο τέτοιο, ώστε να λειτουργεί με προσομοιωτές, όπως ο προσομοιωτής JIST-SWANS αλλά και ο ns-2 [48].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[5].

3.2 Προσομοιωτές δικτύου

Το σημαντικότερο στοιχείο σε ένα αδόμητο οχηματικό δίκτυο αποτελεί η διασύνδεση μεταξύ των οντοτήτων του. Για τη δημιουργία και μελέτη ενός αδόμητου οχηματικού δικτύου είναι απαραίτητη η χρήση προσομοιωτών δικτύου. Με τη χρήση των προσομοιωτών δικτύου, οι ερευνητές έχουν τη δυνατότητα να αναλύσουν τη δικτυακή συμπεριφορά κάθε κόμβου κάτω από διαφορετικές περιστάσεις. Η δημιουργία ενός δοκιμαστικού περιβάλλοντος απαιτεί μεγάλο εξοπλισμό, όπως υπολογιστές, δρομολογητές κ.α, καθώς επίσης και οικονομικούς πόρους. Για τον λόγο αυτό, η επιστημονική κοινότητα στρέφεται όλο ένα και περισσότερο σε λογισμικά προσομοίωσης δικτύου, τα οποία χαρακτηρίζονται από μικρό κόστος και μεγάλο πλήθος δυνατοτήτων. Σε περιβάλλοντα, όπως τα αδόμητα οχηματικά δίκτυα, οι προσομοιωτές δικτύου χρησιμοποιούνται για τη μελέτη της διασύνδεσης των οχημάτων μεταξύ τους ή των οχημάτων με άλλα μέρη της υποδομής. Στη συνέχεια, αναλύονται μερικά παραδείγματα προσομοιωτών κίνησης.

[4] https://sourceforge.net/projects/vanetmobisim/
[5] http://oldaqualab.cs.northwestern.edu/projects/144-straw-street-random-waypoint-vehicular-mobility-model-for-network-simulations-e-g-car-networks

3.2.1 Omnet++

Το εργαλείο Omnet++ έγινε διαθέσιμο στο ευρύ κοινό το 1997, έκτοτε αναβαθμίζεται διαρκώς μέχρι και σήμερα. Ο προσομοιωτής αυτός είναι βασισμένος στη γλώσσα προγραμματισμού C++ και χρησιμοποιείται στη μοντελοποίηση και οπτικοποίηση των διασυνδέσεων μέσα σε ένα δίκτυο. Το εργαλείο αυτό ξεχωρίζει από τα υπόλοιπα εργαλεία προσομοίωσης δικτύων καθώς: α) είναι ανοιχτού κώδικα, β) είναι συμβατό με λειτουργικά, όπως Windows, MacOS και Linux, γ) αναπτύσσεται διαρκώς, λόγω της μεγάλης κοινότητας, την οποία έχει. Το Omnet++ μπορεί να υποστηρίξει μια ευρεία γκάμα από πλαίσια (frameworks), όπως το πλαίσιο κινητικότητας (mobility framework) και το INET πλαίσιο.

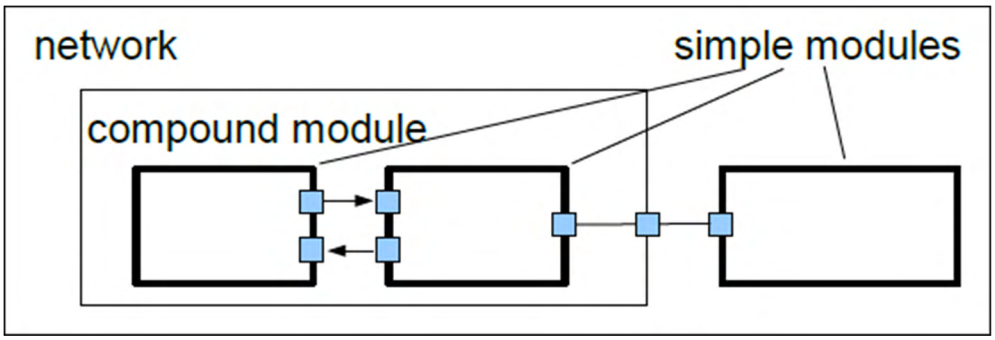
Λόγω της αρχιτεκτονικής του, ο προσομοιωτής αυτός θεωρείται κατάλληλος για την προσομοίωση μεγάλης κλίμακας δικτύων. Το κύριο χαρακτηριστικό του είναι η αρθρωτότητα. Όλα ξεκινούν από την απλή δομοστοιχεία (Simple Module), η οποία είναι γραμμένη σε γλώσσα C++. Κάθε δομοστοιχεία μπορεί να επιτελέσει μια λειτουργία, την οποία μπορεί να ορίσει ο χρήστης παραμετροποιώντας τον κώδικα της. Οι δομοστοιχείες, που επιτελούν παρεμφερείς λειτουργίες, μπορούν να λειτουργήσουν και ως μια σύνθετη δομοστοιχεία (compound module). Οι δομοστοιχείες ανταλλάσσουν δεδομένα μεταξύ τους μέσα από την πύλες (gates), τις οποίες διαθέτουν, όπου κάθε δομοστοιχεία έχει μια πύλη εισόδου και μία εξόδου, όπως φαίνεται στην Εικόνα 3.1.

Το Omnet++ παρέχει τη δυνατότητα στον χρήστη να ορίσει τις διασυνδέσεις μεταξύ των δομοστοιχειών, με τη χρήση της γλώσσας NED, η οποία χαρακτηρίζεται ως μια περιγραφική γλώσσα τοπολογίας. Μέσα από το περιβάλλον του εργαλείου, ο χρήστης μπορεί είτε να προγραμματίσει ο ίδιος τις διασυνδέσεις είτε να τις ορίσει με τη λειτουργία drag and drop.

Τέλος, ένα άλλο διακριτό χαρακτηριστικό του Omnet++ είναι οι δυνατότητες οπτικοποίησης που παρέχει, καθώς ενσωματώνει ολοκληρωμένο περιβάλλον ανάπτυξης (IDE), το οποίο είναι βασισμένο στο eclipse. Έτσι, διευκολύνει τους χρήστες στην αποσφαλμάτωση του κώδικα τους και στην καλύτερη κατανόηση πολύπλοκων δικτύων. Επομένως, το Omnet++ χαρακτηρίζεται ως κατάλληλο, για την προσομοίωση αδόμητων οχηματικών δικτύων [52],[53].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[6].

[6] https://omnetpp.org/documentation/



Εικόνα 3.1 *Δομή του omnet++ [52]*

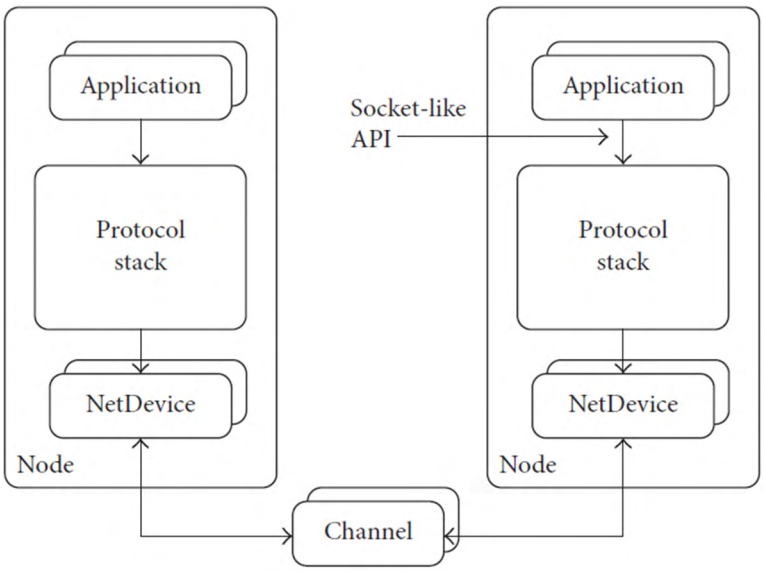
3.2.2 NS-3

Ο network simulator 3 (ns-3) κυκλοφόρησε το 2008 και αποτελεί έναν ακόμη προσομοιωτή δικτύων. Το εργαλείο ns-3 είναι ανοιχτού κώδικα και είναι αδειοδοτημένο κάτω από την GNU GPLv2 άδεια. Θεωρείται αρκετά διαδεδομένο στην ερευνητική κοινότητα, παρόλο που δεν παρέχει στον χρήστη γραφικό περιβάλλον, χαρακτηρίζεται όμως από ευκολία στη χρήση. Το ns-3 είναι σχεδιασμένο για περιβάλλοντα Linux, όμως υπάρχει η δυνατότητα χρήσης του και σε Windows περιβάλλοντα.

Η δημιουργία του έγινε με σκοπό να αντικαταστήσει τον προκάτοχό του (ns-2) και να ξεπεράσει τους περιορισμούς της επεκτασιμότητας και της υψηλής χρήσης μνήμης. Ένα από τα πλεονεκτήματα του ns-3 είναι η δυνατότητα ανάπτυξης πειραμάτων και σε γλώσσα Python, κάτι το οποίο δεν ήταν εφικτό στον ns-2 προσομοιωτή. Στην αρχιτεκτονική του συγκεκριμένου εργαλείου διακρίνονται τέσσερα βασικά συστατικά: α) οι κόμβοι, β) οι εφαρμογές , γ) οι δικτυακές συσκευές, δ) τα κανάλια επικοινωνίας και ε) οι βοηθοί τοπολογίας. Κάθε ένα από τα παραπάνω συστατικά έχει δημιουργηθεί με τη χρήση της γλώσσας C++. Επιπλέον, το ns-3 μπορεί να υποστηρίξει τη δημιουργία δικτύων, τα οποία είναι βασισμένα σε IP αλλά και τη δημιουργία δικτύων, τα οποία δε βασίζονται σε IP. Κυριότερα πρωτόκολλα που χρησιμοποιούνται είναι το Wi-Fi, WiMAX και LTE, καθώς επίσης και τα πρωτόκολλα δρομολόγησης AODV και OSLR. Τέλος, το ns-3 παράγει αρχεία καταγραφής είτε σε pcap μορφή είτε σε tracefile. Στην Εικόνα 3.2, παρουσιάζεται η λειτουργία του βασικού μοντέλου του ns-3 [54],[56].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[7].

[7] https://www.nsnam.org/documentation/



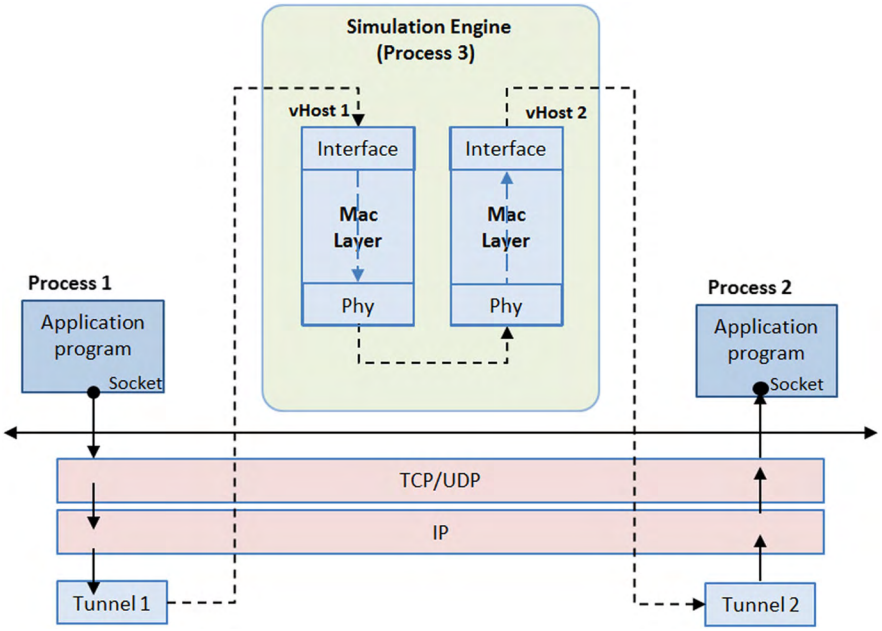
Εικόνα 3.2 *Αρχιτεκτονική βασικού μοντέλου ns-3 [55]*

3.2.3 EstiNet

Το εργαλείο EstiNet θεωρείται ως προσομοιωτής αλλά και ως εξομοιωτής δικτύων. Το EstiNet ανήκει στην κατηγορία των πληρωτέων εργαλείων και κάνει χρήση μιας πρωτοποριακής μεθόδου, η οποία ονομάζεται kernel re-entering. Η πρωτοποριακή αυτή μέθοδος χρησιμοποιεί δικτυακές διεπαφές τούνελ, ώστε να μπορεί να παρεμποδίζει τα πακέτα, τα οποία ανταλλάσσονται μεταξύ των εφαρμογών και να τα κατευθύνει προς το ίδιο το εργαλείο.

Όσον αφορά τη χρήση του για τον σχεδιασμό αλλά και την ανάλυση αδόμητων οχηματικών δικτύων, το EstiNet προσφέρει τη δυνατότητα εισαγωγής δομοστοιχείας (Module), ως πρόσθετο (add-on). Όπως και σε άλλα εργαλεία προσομοίωσης δικτύων, έτσι και στο EstiNet είναι δυνατή η δημιουργία οδικού δικτύου εξ αρχής, όπως επίσης και η εισαγωγή χάρτη της επιλογής του χρήστη. Το εργαλείο παρέχει έναν ενσωματωμένο προσομοιωτή κίνησης, ο οποίος έχει τη δυνατότητα για προσομοίωση σεναρίων: α) αλλαγής λωρίδας, β) προσπεράσματος και γ) σωστής συμπεριφοράς στους φωτεινούς σηματοδότες. Επιπλέον, υποστηρίζει βασικά πρωτόκολλα για τη δημιουργία αδόμητων οχηματικών δικτύων, όπως το IEEE 802.11p, IEEE 1609.3 και IEEE 1609.4.

Τέλος, στις δυνατότητες του εργαλείου προστίθεται η απεικόνιση τόσο επεξεργαστικών μονάδων, όσο και παρόδιων μονάδων, όπου ο χρήστης μπορεί να παραμετροποιήσει τις διασυνδέσεις μεταξύ των κόμβων, όπως εκείνος επιθυμεί. Στην εικόνα 3.3 παρουσιάζεται η αρχιτεκτονική του εργαλείου EstiNet [57],[58].



Εικόνα 3.3 *Αρχιτεκτονική απεικόνιση του εργαλείου EstiNet [57]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[8].

3.2.4 VANETsim

Το VANETsim είναι ένας προσομοιωτής, ο οποίος στη μελέτη των ζητημάτων ασφαλείας που παρατηρούνται στις οχηματικές επικοινωνίες, χαρακτηρίζεται από ευκολία στον χειρισμό αλλά μικρή φορητότητα, καθώς είναι διαθέσιμος μόνο για περιβάλλοντα Windows. Ο χρήστης έχει τη δυνατότητα να αναλύσει διάφορες πιθανές επιθέσεις σε επίπεδο εφαρμογής. Για τη δημιουργία των σεναρίων επίθεσης, το VANETsim χρησιμοποιεί τέσσερα βασικά μέρη του: α) τη γραφική διεπαφή (GUI), β) τον δημιουργό σεναρίων (scenario creator), γ) τον πυρήνα προσομοίωσης (simulation core) και δ) τη μηχανή επεξεργασίας (Post processing engine).

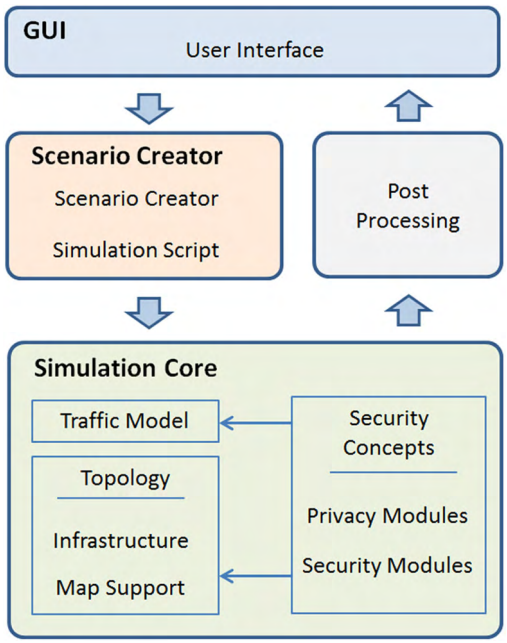
Σχετικά με τη δημιουργία των οδικών δικτύων, ο χρήστης έχει τη δυνατότητα, μέσω της γραφικής διεπαφής, να δημιουργήσει είτε το δικό του οδικό δίκτυο είτε να εισάγει κάποιο έτοιμο με τη χρήση του OpenStreetMaps. Επίσης, μπορεί να παραμετροποιήσει τους χάρτες, τους οποίους εισήγαγε και τους αποθηκεύσει σε μορφή XML.

Τα σενάρια δημιουργούνται με χρήση του δημιουργού σεναρίων και υπεύθυνος για την εκτέλεση τους είναι ο πυρήνας προσομοίωσης. Επιπλέον, υπάρχει η δυνατότητα δημιουργίας αρχείων καταγραφής (log files) μέσω της μηχανής επεξεργασίας.

Τέλος, καθώς η ανάπτυξη του VANETsim έχει σταματήσει, το εργαλείο έχει τη δυνατότητα να προσομοιώσει μόνο δύο ειδών μηνύματα: α) τα μηνύματα φάρου (beacons) και β) τα μηνύματα

[8] http://www.gordonsmart.com/ns/?page_id=21140

ειδικού σκοπού, όπως η έλευση κάποιου ασθενοφόρου. Το γεγονός αυτό, περιορίζει τις δυνατότητες του εργαλείου. Στην Εικόνα 3.4 απεικονίζεται η αρχιτεκτονική του VANETsim [57].



Εικόνα 3.4 *Αρχιτεκτονική απεικόνιση του προσομοιωτή VANETsim [57]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[9].

3.2.5 SNS

Ο SNS (Stage Network Simulator) είναι ένας προσομοιωτής δικτύου, ο οποίος είναι βασισμένος στο εργαλείο ns-2. Το εργαλείο αυτό εισάγει ένα νέο τρόπο προσομοίωσης, διαφορετικό από τους υπόλοιπους προσομοιωτές, καθώς αυτοί χρειάζονται μεγάλο αριθμό υπολογιστικών πόρων, ώστε να εκτελέσουν τους υπολογισμούς τους. Οι υπολογισμοί αυτοί πραγματοποιούνται σε μεμονωμένη εκτέλεση του εκάστοτε σεναρίου. Ο SNS, μέσω της προσωρινής αποθήκευσης και επαναχρησιμοποίησης, προσπαθεί να λύσει το πρόβλημα αυτό. Χωρίζοντας την εκτέλεση του σεναρίου σε φάσεις, έχει τη δυνατότητα μετά το πέρας κάποιας φάσης να απελευθερώσει τους πόρους, οι οποίοι ήταν δεσμευμένοι και να τους χρησιμοποιήσει σε νέα φάση. Με τη μέθοδο αυτή, είναι δυνατό να επιτύχει βελτίωση στην ταχύτητα εκτέλεσης των σεναρίων. Γεγονός, που το καθιστά κατάλληλο για τη δημιουργία μεγάλης κλίμακας, όπως τα αδόμητα οχηματικά δίκτυα [59],[60].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[10].

[9] https://svs.informatik.uni-hamburg.de/vanet/#
[10] https://eclipse.dev/mosaic/docs/simulators/network_simulator_sns/

3.2.6 JIST/SWANS

Το εργαλείο JIST/SWANS αποτελείται από δύο επιμέρους τμήματα. Το ένα τμήμα είναι ο προσομοιωτής διακριτών γεγονότων JIST. Το JIST δημιουργήθηκε με σκοπό την υλοποίηση προσομοιώσεων, όπου θα γίνεται χρήση τόσο παλαιών τεχνικών, όσο και προσομοιώσεων, που βασίζονται σε γλώσσες προγραμματισμού. Το εργαλείο αυτό λειτουργεί σε μια εικονική μηχανή (virtual machine) JAVA. Σε αντίθεση με άλλα εργαλεία, οι προσομοιώσεις δεν χρειάζεται να είναι σχεδιασμένες σε κάποια ειδική γλώσσα, που αφορά μόνο προσομοιώσεις. Το JIST παραμετροποιεί με τέτοιο τρόπο την εικονική μηχανή, ώστε να τη μετατρέψει σε περιβάλλον προσομοίωσης. Ο κώδικας προσομοίωσης είναι γραμμένος σε γλώσσα JAVA και μπορεί να τρέξει σε οποιαδήποτε εικονική μηχανή.

Όσον αφορά το SWANS, είναι προσομοιωτής δικτύων, ο οποίος έχει υλοποιηθεί πάνω στο περιβάλλον του JIST. Για τη δημιουργία του δικτύου κάνει χρήση διαφορετικών τμημάτων κώδικα και χαρακτηρίζεται ως κατάλληλο για τη δημιουργία και ανάλυση μεγάλης κλίμακας δικτύων.

Ο συνδυασμός των δυο αυτών τμημάτων επιτυγχάνει παρόμοιες λειτουργίες με εργαλεία, όπως το ns-2, με μικρότερη όμως κατανάλωση υπολογιστικών πόρων. Επιπλέον, επιτυγχάνει βελτίωση στον χρόνο εκτέλεσης της προσομοίωσης [59],[61].

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[11].

3.3 Συνδυαστικά περιβάλλοντα

Όπως είδαμε, για τη δημιουργία προσομοιώσεων αδόμητων οχηματικών δικτύων είναι απαραίτητη, σε πολλές περιπτώσεις, η χρήση διαφορετικών λογισμικών για τη μοντελοποίηση της κινητικότητας και του οδικού δικτύου. Για τον λόγο αυτό, δημιουργήθηκαν τα συνδυαστικά περιβάλλοντα ανάπτυξης, τα οποία συνδυάζουν τόσο τους προσομοιωτές κίνησης, όσο και τους προσομοιωτές δικτύων. Ο Πίνακας 3.1 αποτελεί έναν συγκεντρωτικό πίνακα με τους προσομοιωτές, που ερευνήσαμε (κίνησης, δικτύων, συνδυαστικά περιβάλλοντα) για τα αδόμητα οχηματικά δίκτυα. Στη συνέχεια, αναλύονται μερικά από τα συνδυαστικά περιβάλλοντα, που χρησιμοποιούνται για την προσομοίωση των αδόμητων οχηματικών δικτύων.

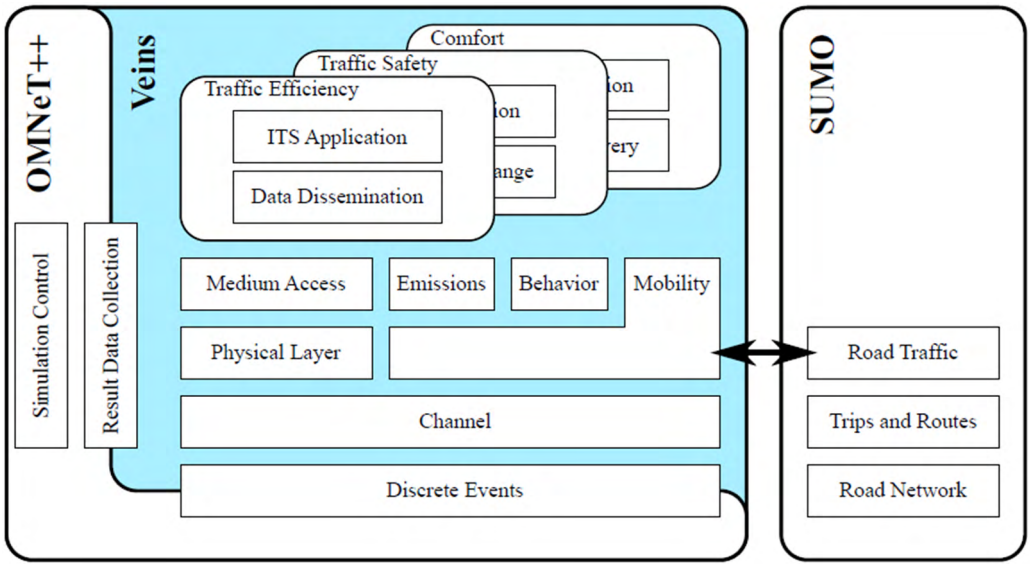
[11] http://jist.ece.cornell.edu/docs.html

3.3.1 VEINS (Vehicular In-Network Simulations)

Ένα από τα πιο δημοφιλή συνδυαστικά εργαλεία, για την προσομοίωση αδόμητων οχηματικών δικτύων, θεωρείται το εργαλείο Veins. Το Veins αποτελεί ένα ανοιχτού κώδικα πλαίσιο (framework), το οποίο βασίζεται σε δύο εργαλεία, τον προσομοιωτή δικτύου Omnet++ και τον προσομοιωτή κίνησης SUMO. Διακρίνεται από μεγάλη φορητότητα, καθώς μπορεί να τρέξει σε γνωστά περιβάλλοντα, όπως Windows, Linux και MacOS.

Το Veins κάνει χρήση του πρωτοκόλλου σύνδεσης TraCI (Traffic Control Interface) με τη βοήθεια του οποίου είναι δυνατή η παράλληλη εκτέλεση των προσομοιωτών κίνησης και δικτύου. Το εργαλείο αυτό, για κάθε ένα κόμβο της προσομοίωσης στο Omnet++, κάνει σύζευξη με την κίνηση, η οποία έχει οριστεί για τον συγκεκριμένο κόμβο, μέσω του SUMO. Μέσω του πρωτοκόλλου σύνδεσης είναι δυνατή η ανταλλαγή μηνυμάτων μεταξύ των προσομοιωτών.

Επιπλέον, το Veins έχει τη δυνατότητα να υποστηρίξει τη μοντελοποίηση πολλών διαφορετικών πρωτοκόλλων, όπως το IEEE 802.11p και το ETSI ITS-G5. Τέλος, στα αρνητικά του Veins επισημαίνεται ότι, για να μπορεί ο χρήστης να τρέξει τις προσομοιώσεις, τις οποίες δημιούργησε, θα πρέπει τόσο το εργαλείο Omnet++, όσο και το SUMO να λειτουργούν ορθά. Σε αντίθετη περίπτωση, η προσομοίωση είναι ανέφικτη. Στην Εικόνα 3.5 παρουσιάζεται η αρχιτεκτονική του εργαλείου Veins [57],[63].



Εικόνα 3.5 *Αρχιτεκτονική απεικόνιση του εργαλείου Veins [62]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[12].

[12] https://veins.car2x.org/documentation/

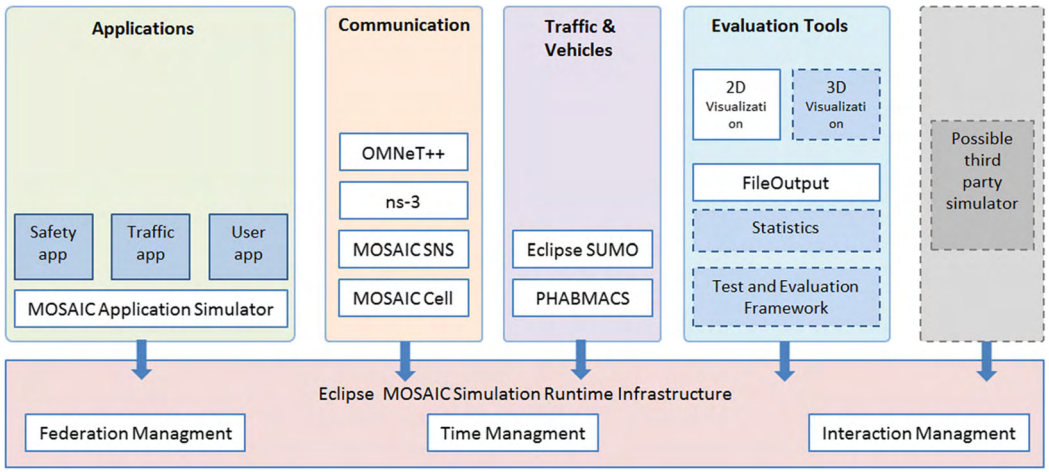
3.3.2 Eclipse MOSAIC

Ένα ακόμα συνδυαστικό περιβάλλον, αποτελεί το εργαλείο Eclipse MOSAIC, του οποίου η παλαιότερη ονομασία ήταν V2X Simulation Runtime Infrastructure (VSim-RTI). Το συγκεκριμένο εργαλείο αποτελεί ένα ανοιχτού κώδικα συνδυαστικό περιβάλλον, το οποίο χρησιμοποιείται στην προσομοίωση ετερογενών συστημάτων.

Είναι βασισμένο στο πρότυπο IEEE High Level Architecture (HLA) και είναι ικανό να παρέχει στον χρήστη τη δυνατότητα να συνδυάζει διαφορετικούς προσομοιωτές, τους οποίους μπορεί να αλλάζει, ώστε να αυξήσει τις δυνατότητες μοντελοποίησής του σεναρίου. Αυτήν τη στιγμή, το Eclipse MOSAIC μπορεί να υποστηρίξει προσομοιωτές δικτύου όπως: α) το Omnet++, β) το SNS και γ) το ns-3 και να υποστηρίξει προσομοιωτές κίνησης, όπως το SUMO και το PHABAMCS.

Ένα από τα βασικά χαρακτηριστικά του εργαλείου είναι η δυνατότητα ενσωμάτωσης προσομοιωτών της επιλογής του χρήστη. Για να επιτευχθεί αυτό, γίνεται χρήση τριών στοιχείων: i) του federation management, ii) του time management και iii) του interaction management. Κάθε ένα στοιχείο επιτελεί μια διαφορετική λειτουργία στο εργαλείο.

Τέλος, λόγω του τρόπου με τον οποίο είναι σχεδιασμένο το Eclipse MOSAIC, η απεικόνιση των δεδομένων της προσομοίωσης είναι εφικτό να πραγματοποιηθεί με πολλούς διαφορετικούς τρόπους και εργαλεία, όπως το WebSocket Visualizer και το PHABMap, καθιστώντας το χρήσιμο για την απεικόνιση αδόμητων οχηματικών δικτύων. Στην Εικόνα 3.6 απεικονίζεται η αρχιτεκτονική του Eclipse MOSAIC [57],[64],[65].



Εικόνα 3.6 *Αρχιτεκτονική απεικόνιση του εργαλείου Eclipse MOSAIC [57]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[13].

[13] https://eclipse.dev/mosaic/docs/

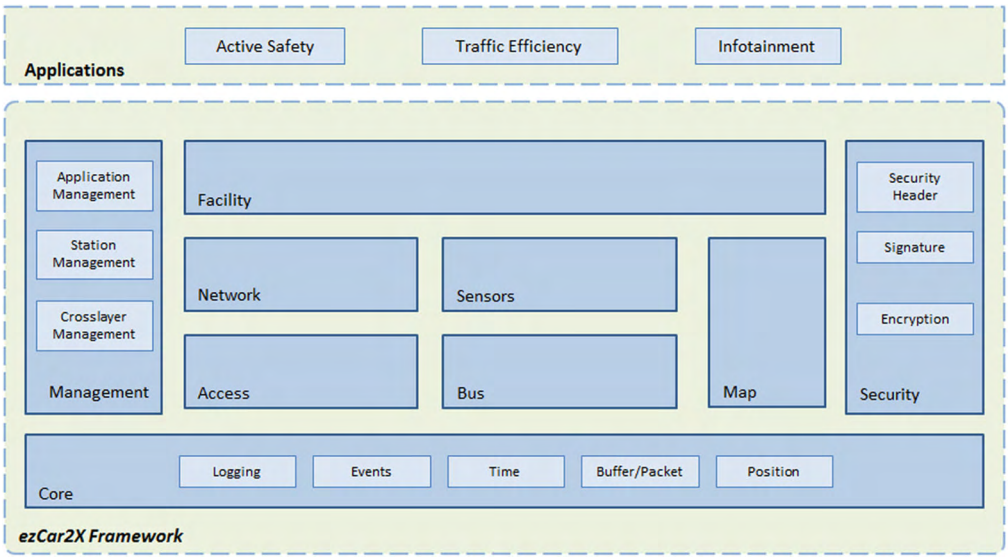
3.3.3 ezCar2X

Το ezCar2X αποτελεί ένα αρθρωτό πλαίσιο λογισμικού (modular software framework), το οποίο χρησιμοποιείται στην ανάπτυξη εφαρμογών ευφυών συστημάτων μεταφοράς αλλά και πρωτοκόλλων επικοινωνίας. Το εργαλείο αυτό είναι διαθέσιμο για πλατφόρμες Windows και Linux, και δε θεωρείται ανοιχτού κώδικα.

Όσον αφορά τη χρήση του, δίνει τη δυνατότητα στον χρήστη να προσομοιώσει σενάρια, που αφορούν την επικοινωνία του οχήματος με άλλες συσκευές στο δίκτυο (V2X). Είναι βασισμένο στην αντικειμενοστρέφια, καθώς για την υλοποίησή του έχει γίνει χρήση της γλώσσας C++, η οποία θεωρείται πως καταναλώνει μικρότερο αριθμό υπολογιστικών πόρων κατά την εκτέλεση της προσομοίωσης. Για τη δημιουργία και την εκτέλεση των προσομοιώσεων, το ezCar2X, κάνει χρήση του προσομοιωτή κίνησης SUMO και του προσομοιωτή δικτύου ns-3, καθώς υπάρχει συμβατότητα λόγω της αρχιτεκτονικής του εργαλείου. Επιπλέον, με τη χρήση του TraCI API είναι δυνατή η σύζευξη και άλλων προσομοιωτών δικτύου.

Σχετικά με την αρχιτεκτονική του στο ezCar2X, τα συστατικά του λειτουργούν ως διαμοιραζόμενες βιβλιοθήκες. Το περιβάλλον του ezCar2X είναι βασισμένο στα πρότυπα του ευρωπαϊκού ινστιτούτου επικοινωνιών (ETSI) για ευφυή συστήματα μεταφοράς (ITS). Έτσι, το εργαλείο αυτό αποτελείται από κάποιες βασικές δομοστοιχείες (modules), οι οποίες επιτελούν διαφορετικές λειτουργίες. Οι δομοστοιχείες αυτές είναι οι εξής: α) Core Module, β) Access Module, γ) Network Module, δ) Security Module, ε) Map Module.

Τέλος, το ezCar2X παρέχει τη δυνατότητα εισαγωγής χάρτη από το εργαλείο OpenStreetMaps. Στην Εικόνα 3.7 παρουσιάζεται η αρχιτεκτονική του εργαλείου [57],[66].



Εικόνα 3.7 *Αρχιτεκτονική απεικόνιση του εργαλείου ezCar2X [57]*

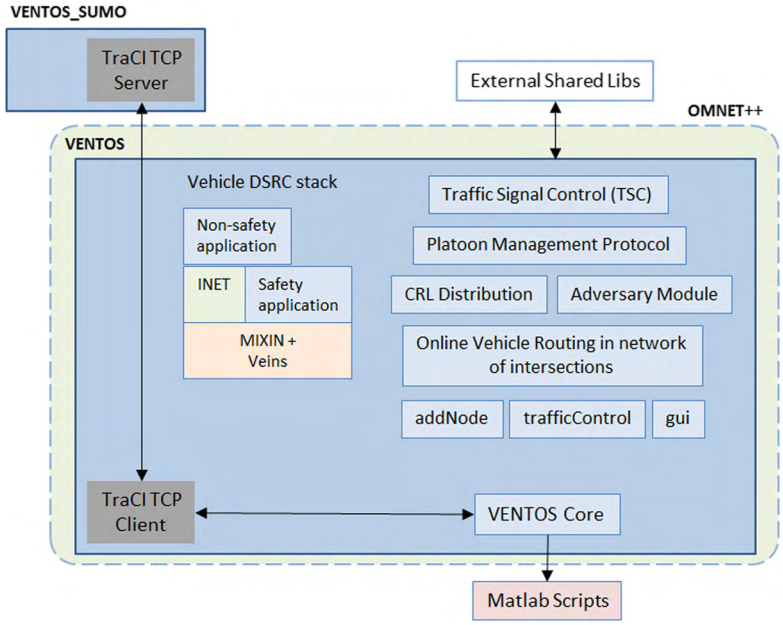
Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[14].

3.3.4 VENTOS

Το VENTOS είναι ένας προσομοιωτής ανοιχτού κώδικα, ο οποίος χρησιμοποιείται για τη δημιουργία και ανάλυση δικτυακών εφαρμογών. Χαρακτηρίζεται από μεγάλη φορητότητα, καθώς είναι συμβατό με περιβάλλοντα Linux, Windows και MacOS. Για την προσομοίωση των σεναρίων, το VENTOS κάνει χρήση του προσομοιωτή κίνησης SUMO και του προσομοιωτή δικτύου Omnet++. Επιπλέον, το εργαλείο δίνει τη δυνατότητα στον χρήστη να δημιουργήσει τις δικές του δομοστοιχείες (Modules) αλλά και να χρησιμοποιήσει τις ήδη υπάρχουσες, που διαθέτει. Έτσι, η προσομοίωση πολύπλοκων σεναρίων απλοποιείται.

Όσον αφορά την αρχιτεκτονική του VENTOS, διακρίνονται δύο βασικές δομοστοιχείες. Η πρώτη δομοστοιχεία αφορά την εισαγωγή νέου κόμβου και η δεύτερη τη διαχείριση της συμπεριφοράς των κόμβων μέσα στην προσομοίωση (αυξομείωση ταχύτητας, αλλαγή κατεύθυνσης κα). Επιπλέον, παρέχει τη δυνατότητα σύνδεσης με πραγματικές επεξεργαστικές και παρόδιες μονάδες, για πιο ρεαλιστικά αποτελέσματα στην προσομοίωση.

Τέλος, σημειώνεται ότι για να εκτελεστεί σωστά οποιαδήποτε προσομοίωση, τόσο το εργαλείο Omnet++, όσο και το SUMO, θα πρέπει να λειτουργούν ορθά. Σε αντίθετη περίπτωση, η προσομοίωση δεν επιστρέφει τα επιθυμητά αποτελέσματα. Στην Εικόνα 3.8 παρουσιάζεται η αρχιτεκτονική του περιβάλλοντος VENTOS [57],[67].



Εικόνα 3.8 *Αρχιτεκτονική απεικόνιση περιβάλλοντος VENTOS [57]*

[14] https://www.ezcar2x.fraunhofer.de/en/download.html

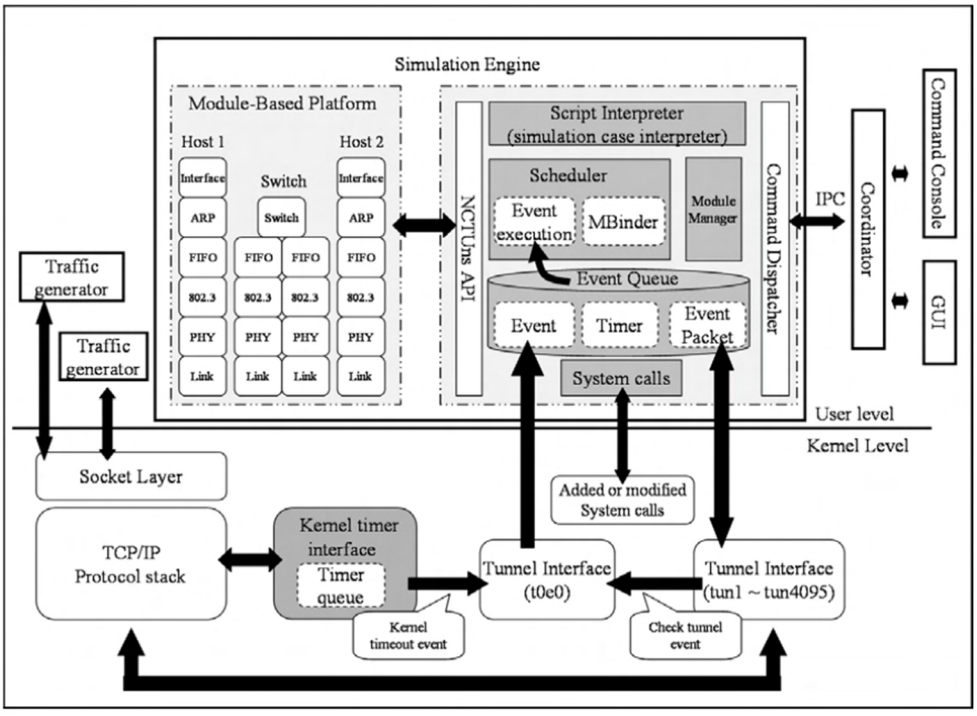
Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[15].

3.3.5 NCTUns

Το NCTUns (National Chiao Tung University network simulator) αποτελεί έναν προσομοιωτή, ο οποίος λειτουργεί ταυτόχρονα ως προσομοιωτής κίνησης αλλά και ως προσομοιωτής δικτύου. Κάνει χρήση της στοίβας πρωτοκόλλου Linux TCP/IP και είναι συμβατό με Linux Fedora. Το συγκεκριμένο εργαλείο είναι βασισμένο στη γλώσσα C++.

Σχετικά με την αρχιτεκτονική του, το NCTUns αποτελείται από εφτά βασικά στοιχεία, τα οποία είναι τα εξής: i) γραφική διεπαφή (GUI), ii) επιτελικός αποστολέας εργασίας (job dispatcher), iii) συντονιστής (coordinator), iv) μηχανή προσομοίωσης (simulation engine), v) πυρήνα Linux (Linux kernel), vi) εφαρμογές, vii) daemons. Κάθε ένα από αυτά τα στοιχεία επιτελεί σε μια ξεχωριστή λειτουργία του εργαλείου.

Τέλος, παρόλο που το NCTUns χαρακτηρίζεται από ακρίβεια, στις δικτυακές του προσομοιώσεις, ο βαθμός δυσκολίας στη χρήση του είναι υψηλός. Στην Εικόνα 3.9 απεικονίζεται η αρχιτεκτονική του εργαλείου NCTUns [68],[69].



Εικόνα 3.9 *Αρχιτεκτονική απεικόνιση του εργαλείου NCTUns [69]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[16].

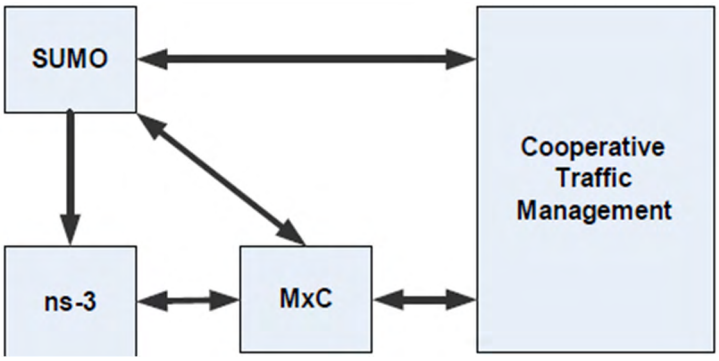
[15] http://maniam.github.io/VENTOS/
[16] https://github.com/jorgenio/nctuns/blob/master/NCTUns-6.0/README

3.3.6 iTETRIS

Ένα ακόμα συνδυαστικό περιβάλλον είναι το iTETRIS. Το εργαλείο αυτό είναι ανοιχτού κώδικα και δημιουργήθηκε με σκοπό να λύσει το πρόβλημα της προσομοίωσης μεγάλης κλίμακας δικτύων, που εστιάζουν στην αποδοτικότερη διαχείριση της κίνησης μέσω της χρήσης ευφυών συστημάτων μεταφοράς. Το περιβάλλον αυτό είναι διαθέσιμο μόνο σε λειτουργικά συστήματα, τα οποία είναι βασισμένα σε UNIX.

Για τη δημιουργία και προσομοίωση των σεναρίων, το iTETRIS κάνει χρήση του προσομοιωτή κίνησης SUMO και του προσομοιωτή δικτύου ns-3. Κατά την προσομοίωση, το κέντρο διαχείρισης κίνησης παίρνει τις αποφάσεις σχετικά με την ανακατεύθυνση της κίνησης και ενημερώνει τα οχήματα στο δίκτυο μέσω ανταλλαγής μηνυμάτων επικοινωνίας (MxC).

Το iTETRIS, λόγω της χρήσης του προσομοιωτή δικτύου ns-3, είναι ικανό να προσομοιώσει σενάριο, κάνοντας χρήση των τεχνολογιών IEEE 802.11p, UMTS και WiMAX. Τέλος, σημειώνεται ότι το εργαλείο δεν αναβαθμίζεται πλέον, κάτι που το καθιστά δύσκολο στη χρήση. Στην εικόνα 3.10 απεικονίζεται η αρχιτεκτονική του περιβάλλοντος iTETRIS [70].



Εικόνα 3.10 *Αρχιτεκτονική απεικόνιση συνδυαστικού περιβάλλοντος iTETRIS [70]*

Ενδεικτικές οδηγίες για την εγκατάσταση και χρήση του εργαλείου αντλήθηκαν από το διαδίκτυο[17].

[17] http://www.ict-itetris.eu/10-10-10-community/

Πίνακας 3.1 *Συγκεντρωτικός πίνακας εργαλείων*

	Veins (SUMO&Omnet++)	**NS-3&SUMO**	**Eclipse MOSAIC (SUMO&Omnet++ &NS3&SNS)**	**ezCar2X (Sumo & ns-3)**	**EstiNet**	**VENTOS (omnet++ &SUMO)**	**VANETsim**
Φορητότητα	✓	✓	✓	×	×	×	×
Opensource	✓	✓	✓	×	×	✓	✓
Freeware	✓	✓	✓	✓	×	✓	✓
Paid	×	×	?	×	✓	×	×
Ευκολία χρήσης	✓	×	×	×	✓	×	✓
Ευκολία εγκατάστασης	✓	×	✓	×	✓	×	✓
GUI	✓	×	×	×	✓	×	✓
Δυνατότητα παραμετροποίησης πρωτοκόλλων επικοινωνίας	✓	✓	✓	×	✓	×	×
Αρχεία καταγραφής	✓	✓	✓	×	✓	×	✓
Διαθέσιμα παραδείγματα	✓	✓	✓	✓	✓	✓	×
Περιορισμοί σχεδίασης	Δεν παρουσιάστηκε κάποιος περιορισμός	Δεν έχει μεγάλη κλιμακοθετησιμότητα δηλαδή δεν μπορεί να διαχειριστεί μεγαλό όγκο δεδομένων όσον αφορά το σεναρίο υλοποίησης.	Περιορισμοί στην σχεδίαση του φυσικού περιβάλλοντος.	×	Δεν είναι δυνατή η σχεδίαση μεγάλων περιβάλλοντων. Το όριο κόμβων είναι 15 και το χρονικό όριο 5 λεπτά.	Οι περιορισμοί αφορούν πολλά αρχεία πηγής τα οποία απαιτούν κάποιες διορθώσεις ώστε να μπορεί ο χρήστης να σχεδίασει κάτι. Αδύνατη η σχεδίαση μεγάλων έργων.	Δεν είναι δυνατή η σχεδίαση μεγάλων έργων. Δεν δυνατή η απεικόνιση πολλών κόμβων.

	Veins (SUMO&Omnet++)	**NS-3&SUMO**	**Eclipse MOSAIC (SUMO&Omnet++ &NS3&SNS)**	**ezCar2X (Sumo & ns-3)**	**EstiNet**	**VENTOS (omnet++ &SUMO)**	**VANETsim**
Δυνατότητες στην χρήση του εργαλείου	Πληθώρα σύγχρονων πακέτων για την προσομοίωση του δικτύου μας. Δυνατότητα αναδρομολόγησης των οχημάτων. Λεπτομερή μοντέλα IEEE 802.11p. IEEE 1609.4 DSRC/WAVE network layers	Μεγάλο πλήθος πακέτων για την προσομοίωση Σύγχρονα μοντέλα δρομολόγησης των κόμβων Δυνατότητα για παρακολούθηση των κόμβων Δυνατότητα δημιουργίας pcap αρχείων Δυνατότητα δημιουργίας γραφημάτων	Δυνατότητες στην δημιουργία προσομοιώσεων με την χρήση διαφορετικών προσομοιωτών κίνησης και δικτύων. Δυνατότητα δημιουργίας log files για διαφορετικές λειτουργίες της προσομοίωσης καθώς επίσης και csv αρχεία με το αποτέλεσμα της προσομοίωσης	×	Περιέχει πολλά πακέτα για προσομοιώσεις. Το κάθε τμήμα μπορεί να παραμετροποιηθεί μεχρί ενός σημείου.	Έχει δυνατότητα απεικόνισης αρκετών σεναρίων όσον αφορά τα οχήματα.	Δυνατή η σχεδίαση του χάρτη όπως επιθυμεί ο χρήστης. Μπορεί να γίνει τοποθέτηση φαναριών, χαλασμένων δρόμων κλπ σε οποίο σημείο επιθυμεί. Εισαγωγή χάρτη από openstreetmaps.

	Veins (SUMO&Omnet++)	**NS-3&SUMO**	**Eclipse MOSAIC (SUMO&Omnet++ &NS3&SNS)**	**ezCar2X (Sumo & ns-3)**	**EstiNet**	**VENTOS (omnet++ &SUMO)**	**VANETsim**
Περιορισμοί στην χρήση του εργαλείου	Δεν παρουσιάστηκε κάποιος περιορισμός	Δεν παρουσιάστηκε κάποιος περιορισμός	Το εργαλείο περιορίζει τον χρήστη σε βασικές λειτουργίες του εργαλείου διότι μερικές βρίσκονται στην πληρωτέα έκδοση όπως (3D απεικόνιση, Προσομοιωτής οχημάτων PHABMACS, αποτελέσματα στατιστικών)	×	Είναι αρκετά δύσκολη η χρήση χαρτών ορισμένων από τον χρήστη καθώς επίσης και η δημιουργία ενός αδόμητου οχηματικού δικτύου. Πολλές λειτουργίες δεν είναι διαθέσιμες στη δωρεάν έκδοση.	Πολλά πακέτα είναι μη ενημερωμένα.	Δεν δέχεται πολύ μεγάλους χάρτες. Ο αριθμός σεναρίων που αφορούν είτε ασφάλεια είτε άλλες λειτουργίες είναι περιορισμένος. Η παραμετροποίηση των κόμβων είτε άλλον στοιχειών της προσομοίωσης είναι περιορισμένη.
Χάρτες (real-world/User defined)	Πραγματικού κόσμου και ορισμένοι από τον χρήστη	Πραγματικού κόσμου και ορισμένοι από τον χρήστη	Πραγματικού κόσμου και ορισμένοι από τον χρήστη	×	Ορισμένοι από τον χρήστη	Πραγματικού κόσμου και ορισμένοι από τον χρήστη	Ορισμένοι από τον χρήστη
Macroscopic	✓	✓	✓	×	×	✓	×
Microscopic	✓	✓	✓	×	✓	✓	✓

	Veins (SUMO&Omnet++)	**NS-3&SUMO**	**Eclipse MOSAIC (SUMO&Omnet++ &NS3&SNS)**	**ezCar2X (Sumo & ns-3)**	**EstiNet**	**VENTOS (omnet++ &SUMO)**	**VANETsim**
Πλεονεκτήματα	Μεγάλη κοινότητα για υποστήριξη. Οι κόμβοι μπορούν να αλληλεπιδρούν ελεύθερα με τον προσομοιωτή κίνησης. Προσφέρει μια ολοκληρωμένη σειρά μοντέλων ειδικά για επικοινωνία μεταξύ οχημάτων που χρησιμεύουν ως δομοστοιχειωτό πλάισιο για προσομοίωση εφαρμογών. Θεωρείται ως μια λύση για την ενσωμάτωση των δυο εργαλείων σε ένα.	Μεγάλη ταχύτητα προσομοίωσης όσον αφορά μεγαλά έργα. Μεγάλη κοινότητα για υποστήριξη στο εργαλείο NS3 Δεν καταναλώνει μεγάλο πλήθος πόρων του συστήματος Χρησιμοποιεί python scripting για να την απλοποίηση μερικών εργασιών Έτοιμα παραδείγματα	Λόγω του τρόπου λειτουργίας ο χρήστης μπορεί να γράψει όπως αυτός επιθυμεί τον κώδικα της κάθε οντότητας για την προσομοίωση Υποστηρίζει 3 διαφορετικούς προσομοιωτές δικτύου (ns3,opnet++,sns) Κατανοητό documentation και παραδείγματα	×	Μεγάλη ταχύτητα στην εκτέλεση των έργων. Δεν καταναλώνει πόρους του συστήματος. Εύκολη διεπαφή χρήστη ως προς την χρήση. Δεν υπάρχει κοινότητα για υποστήριξη	Κάνει χρήση του Omnet++ που επιτρέπει την τροποποίηση του κώδικα σε προσομοίωση. Γίνεται χρήση του SUMO.	Έχει εύκολη στην χρήση διεπαφή χρήστη. Έχει εύκολη εγκατάσταση και δεν απαιτεί μεγαλό αριθμό πόρων του συστήματος. ίναι εύκολη και κατανοητή η απεικόνιση των συνδέσεων μεταξυ των κόμβων.

Μειονεκτήματα	Για μεγάλα περιβάλλοντα προσομοίωσης με πολλούς κόμβους καθυστερεί στην δημιουργία και αναπαραγωγή αυτών.	Δεν έχει μεγάλη κλιμακοθετησιμότητα δηλαδή δεν μπορεί να διαχειριστεί μεγαλό όγκο δεδομένων όσον αφορά το σεναρίο υλοποίησης. Έχει περιορισμένη δυνατότητα παρακολούθησης κόμβων σε σχέση με άλλα εργαλεία Όλες οι ενεργειες πραγματοποιούνται μέσω της γραμμής εντολών του linux.	Απαιτεί αρκετό χρόνο και μεγάλο υπόβαθρο για την εκμάθηση του Πολλές χρήσιμες λειτουργίες βρίσκονται στην πληρωτέα έκδοση Αρκετά δύσχρηστο λόγω του ότι η κάθε προσομοίωση αποτελείται από πολλά διαφορετικά αρχεία java τα οποία πρέπει να δημιουργήσει ο χρήστης από την αρχή Δεν υπάρχει μεγάλη κοινότητα για υποστήριξη	Δεν ήταν δυνατή η εγκατάσταση του εργαλείου δίοτι πολλά αρχεία πηγής λείπουν. Πολλά αρχεία που υπάρχουν στο repo του εργαλείου στο gitlab είναι ημιτελή με αποτέλεσμα να μην είναι δυνατή η εγκατάσταση του. Δεν υπάρχει κοινότητα για υποστήριξη του εργαλείου.	Η πληρωτέα έκδοση του είναι ακριβή. Στην δωρεάν έκδοση οι δυνατότητες είναι αρκετα περιορισμένες. Λειτουργεί μόνο σε fedora, επομένως είναι απαραίτητη η χρήση κάποιου εικονικού μηχανήματος. Δεν είναι δυνατή η παραμετροποίηση κώδικα σε κάποια προσομοίωση.	Αρκετά παλιό εργαλείο. Τα μέρη του είναι πλέον μη ενημερωμένα σε μεγάλο βαθμό. Δεν υπάρχει κοινότητα. Έχει σταματήσει η υποστήριξη του εργαλείου με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες. Είναι συμβατό μόνο με παλίες εκδόσεις των omnet++ και SUMO.	Το εργαλείο δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες. Δεν υπάρχει κοινότητα. Λειτουργεί με συγκεκριμένες εκδόσεις της Java μόνο. Δεν είναι δυνατή η επιλογή πρωτόκολλου επικονωνίας μεταξύ των κόμβων. Δεν είναι δυνατή η παραμετροποίηση του κώδικα των οντοτήτων.

	GROOVEnet (out-of-date)	**VNS (out-of-date)**	**NCTUns (out-of-date)**	**STRAW (out-of-date)**	**VanetMobiSim (out-of-date)**	**iTETRIS (out-of-date)**
Φορητότητα	×	×	×	×	×	×
Opensource	✓	✓	✓	✓	✓	✓
Freeware	✓	✓	✓	✓	✓	✓
Paid	×	×	×	×	×	×
Ευκολία χρήσης	×	×	×	×	×	×
Ευκολία εγκατάστασης	×	×	×	×	×	×
GUI	✓	✓	✓	✓	✓	✓
Δυνατότητα παραμετροποίησης πρωτοκόλλων επικοινωνίας	×	×	×	×	×	×
Αρχεία καταγραφής	×	×	×	×	×	×
Διαθέσιμα παραδείγματα	×	×	×	×	×	×
Περιορισμοί σχεδίασης	×	×	×	×	×	×

	GROOVEnet (out-of-date)	**VNS (out-of-date)**	**NCTUns (out-of-date)**	**STRAW (out-of-date)**	**VanetMobiSim (out-of-date)**	**iTETRIS (out-of-date)**
Δυνατότητες στην χρήση του εργαλείου	×	×	×	×	×	×
Περιορισμοί στην χρήση του εργαλείου	×	×	×	×	×	×
Χάρτες (real-world/User defined)	×	×	×	×	×	×
Macroscopic	×	×	×	×	×	×
Microscopic	×	×	×	×	×	×

	GROOVEnet (out-of-date)	**VNS (out-of-date)**	**NCTUns (out-of-date)**	**STRAW (out-of-date)**	**VanetMobiSim (out-of-date)**	**iTETRIS (out-of-date)**
Πλεονεκτήματα	×	×	×	×	×	×

	GROOVEnet (out-of-date)	**VNS (out-of-date)**	**NCTUns (out-of-date)**	**STRAW (out-of-date)**	**VanetMobiSim (out-of-date)**	**iTETRIS (out-of-date)**
Μειονεκτήματα	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.	Η εφαρμογή δεν υποστηρίζεται πλέον με αποτέλεσμα να υπάρχουν bugs, ασυμβατότητες με νεότερα λειτουργικά και μη ανανεωμένες βιβλιοθήκες.

Κεφάλαιο 4: Πειραματική προσέγγιση

Με σκοπό την περαιτέρω εμβάθυνση και κατανόηση της ασφάλειας των αδόμητων οχηματικών δικτύων προχωρήσαμε, στη συνέχεια της παρούσας διπλωματικής εργασίας, σε προσομοίωση ορισμένων σεναρίων επίθεσης, που είναι εφικτό, υπό συνθήκες, να πραγματοποιηθούν σε ένα αδόμητο οχηματικό δίκτυο. Στο κεφάλαιο αυτό, θα αναλυθεί ο τρόπος με τον οποίο εργαστήκαμε για την υλοποίηση του κάθε σεναρίου, καθώς επίσης και τα εργαλεία, τα οποία χρησιμοποιήθηκαν. Παρακάτω, παρουσιάζονται οι λεπτομέρειες υλοποίησης του κάθε σεναρίου ξεχωριστά.

4.1 Επιλογή πρώτου σεναρίου

Το πρώτο σενάριο επίθεσης, το οποίο υλοποιήσαμε, αποτελεί η επίθεση Sybil. Για την επιλογή της συγκεκριμένης επίθεσης έγινε έρευνα σχετικά με α) τα συστατικά του αδόμητου οχηματικού δικτύου, τα οποία επηρεάζει, β) την πιθανότητα πρόκλησής της, γ) τον βαθμό επικινδυνότητάς της και δ) τη δυνατότητα απεικόνισής της με τα υπάρχοντα εργαλεία προσομοίωσης.

Η επίθεση Sybil, όπως αναφέρεται και σε προηγούμενο κεφάλαιο, είναι μια από τις πιο γνωστές επιθέσεις στα αδόμητα οχηματικά δίκτυα. Ο επιτιθέμενος προσπαθεί είτε να παρακάμψει τα συστήματα ταυτοποίησης μέσω ευπαθειών, που παρατηρούνται σε αυτά, είτε να υποκλέψει ταυτότητες κόμβων του δικτύου, ώστε να τις εκμεταλλευτεί για μεταγενέστερη χρήση τους. Το παρών σενάριο χωρίζεται σε τρία επιμέρους στάδια. Στο πρώτο στάδιο θεωρούμε ότι ο επιτιθέμενος έχει τη δυνατότητα να εκμεταλλευτεί ευπάθειες του συστήματος διαχείρισης πιστοποιητικών και πιο συγκεκριμένα του πρωτοκόλλου SCEP. Εκμεταλλευόμενος την ευπάθεια, που αναφέρεται στο CVE-2010-3868 και στο CVE-2010-3869, ο επιτιθέμενος έχει τη δυνατότητα δημιουργίας μεγάλού αριθμού πιστοποιητικών με χρήση του ίδιου SCEP one time password (OTP), το οποίο έχει τη δυνατότητα να ανακτήσει με τη σάρωση του δικτύου, με το λογισμικό wireshark. Στη συνέχεια, και στο δεύτερο στάδιο ο επιτιθέμενος δημιουργεί τον μολυσμένο κόμβο στο δίκτυό μας. Στην προσομοίωσή μας έχουμε ορίσει έναν μολυσμένο κόμβο και δεκατέσσερα θύματα. Ο μολυσμένος κόμβος εδραιώνει την επικοινωνία με τους μη μολυσμένους κόμβους στο δίκτυο. Στο τρίτο και τελευταίο στάδιο, ο επιτιθέμενος αρχίζει να μεταδίδει ψεύδη μηνύματα ατυχήματος στους υπόλοιπους κόμβους του δικτύου, με αποτέλεσμα να αλλάξει την πορεία των οχημάτων και τελικώς να έχει τη δυνατότητα αλλοίωσης της κυκλοφορίας. Στον πίνακα 4.1 παρουσιάζονται τα συστατικά της επίθεσης, καθώς επίσης και τα αντίστοιχα CVEs, που αφορούν την επίθεση.

Πίνακας 4.1 Συγκεντρωτικός πίνακας στοιχείων επίθεσης

Επίθεση	Συστατικά επίθεσης	CVEs	CVSS Base Score
Sybil Attack	1) Ο επιτιθέμενος 2) Οι μολυσμένοι κόμβοι 3) Το πρωτόκολλο SCEP 4) Το σύστημα διαχείρισης πιστοποιητικών 5) Η τεχνολογία επικοινωνίας μεταξύ των κόμβων (DSRC)	CVE-2010-3869	Medium: 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)
		CVE-2010-3868	Medium: 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

4.1.1 Επιλογή εργαλείων για την προσομοίωση

Για την προσομοίωση του σεναρίου της επίθεσης Sybil έγινε λεπτομερής σύγκριση των εργαλείων, που αναλύθηκαν στο προηγούμενο κεφάλαιο. Καταλήξαμε στην επιλογή του συνδυαστικού περιβάλλοντος Veins 5.2, διότι είναι ικανό να συνδυάσει τον προσομοιωτή κίνησης SUMO, ώστε να έχουμε τη δυνατότητα για μελέτη πραγματικών οδικών δικτύων ορισμένα από τον χρήστη αλλά και τον προσομοιωτή δικτύων Omnet++, ο οποίος μάς δίνει τη δυνατότητα μελέτης περισσότερων τεχνολογιών επικοινωνίας. Επίσης, μέσω του γραφικού περιβάλλοντος, το οποίο παρέχεται στον χρήστη, είναι δυνατή η καλύτερη κατανόηση του σεναρίου μέσω της απεικόνισής του.

4.1.2 Προσομοίωση της κίνησης των οχημάτων

Η κίνηση των κόμβων μέσα στο οδικό δίκτυο αποτελεί ένα πολύ σημαντικό κομμάτι της προσομοίωσης. Στο σενάριό μας, επιλέξαμε τη χρήση του εργαλείου Simulation of Urban MObility (SUMO) (version 1.17.0) για την προσομοίωση της κίνησης. Το SUMO είναι ικανό να μοντελοποιήσει την κίνηση, κάνοντας χρήση του μικροσκοπικού μοντέλου κίνησης. Το εργαλείο παρέχει τη δυνατότητα απεικόνισης διαφορετικών τύπων οχημάτων. Επιπλέον, μέσω του γραφικού περιβάλλοντος, το οποίο παρέχεται στον χρήστη, διευκολύνει τη διαδικασία δημιουργίας του μοντέλου κινητικότητας. Σε συνδυασμό με το SUMO είναι δυνατή η χρήση του εργαλείου OpenStreetMaps, έτσι ώστε ο χρήστης να έχει τη δυνατότητα επιλογής της περιοχής, στην οποία θα υλοποιηθεί η προσομοίωση. Επίσης, μέσω του εργαλείου osmWebWizard, ο χρήστης μπορεί να ορίσει ο ίδιος τον αριθμό οχημάτων στην προσομοίωση, καθώς επίσης και τη διάρκεια αυτής. Επομένως, με βάση τα παραπάνω χαρακτηριστικά, το SUMO θεωρήθηκε κατάλληλο για την υλοποίηση του σεναρίου, που επιλέξαμε.

Η περιοχή, την οποία έχουμε επιλέξει, είναι η ευρωπαϊκή πόλη Erlangen. Η περιοχή αυτή θεωρήθηκε καταλληλότερη για το σενάριό μας διότι αποτελεί απεικόνιση ενός αστικού οδικού δικτύου μεσαίας κλίμακας, καθώς επίσης η διάταξη των στοιχείων του δικτύου (οδοί, διασταυρώσεις)

βοηθούν στην καλύτερη απεικόνιση και κατανόηση του δικτύου, επομένως και στην εξαγωγή ορθότερων συμπερασμάτων. Στην Εικόνα 4.1 παρουσιάζεται η περιοχή, την οποία επιλέξαμε, όπως αυτή απεικονίζεται στο γραφικό περιβάλλον του SUMO.

Για τη δημιουργία και προσομοίωση του αστικού δικτύου γίνεται η χρήση των παρακάτω αρχείων μορφής xml, τα οποία είναι δυνατόν να παραμετροποιηθούν είτε μέσα από το ίδιο το εργαλείο είτε με τη χρήση κάποιου εργαλείου με δυνατότητα παραμετροποίησης αρχείων τύπου xml.

- Το αρχείο **erlangen.net.xml** περιέχει το οδικό δίκτυο και τα συστατικά αυτού, όπως δρόμοι, λωρίδες, διασταυρώσεις, φωτεινοί σηματοδότες κλπ. Το συγκεκριμένο αρχείο παράγεται από το netconvert εργαλείο του sumo.
- Το αρχείο **erlangen.rou.xml** περιέχει τους τύπους οχημάτων της προσομοίωσης, καθώς επίσης και τη διαδρομή του κάθε οχήματος. Επιπλέον, ορίζονται δεδομένα του οχήματος. Μερικά από αυτά είναι η επιτάχυνση, ο ρυθμός μείωσης ταχύτητας και η τελική ταχύτητα. Στο σενάριό μας έχουμε παραμετροποιήσει τον κώδικα, όπως φαίνεται παρακάτω, ώστε να ορίσουμε τον αριθμό κόμβων σε δεκαπέντε.

```
<routes>
<vType id="vtype0" accel="2.6" decel="4.5" sigma="0.5" length="2.5" minGap="2.5"
maxSpeed="14" color="1,1,0"/>
<route id="route0" edges="-39539626 -5445204#2 -5445204#1 113939244#2 -126606716
23339459 30405358#1 85355912 85355911#0 85355911#1 30405356 5931612 30350450#0
30350450#1 30350450#2 4006702#0 4006702#1 4900043 4900041#1"/>
<flow id="flow0" type="vtype0" route="route0" begin="0" period="3" number="15"/>
</routes>
```

- Το αρχείο **erlangen.poly.xml** περιέχει τα σημεία ενδιαφέροντος (Points Of Interests), όπως κτήρια και μνημεία, τα οποία μπορούν να απεικονιστούν στην προσομοίωση.
- Το αρχείο **erlangen.sumo.cfg** περιέχει ρυθμίσεις, που αφορούν την προσομοίωση, όπως, ποια αρχεία θα τρέξουν. Στην περίπτωσή μας έχουν οριστεί τα παραπάνω αρχεία, που αναφέραμε, όπως φαίνεται στο παρακάτω κομμάτι κώδικα. Επιπλέον, ορίζεται: α) η διάρκεια της προσομοίωσης, β) οι ρυθμίσεις σχετικά με τα reports και γ) η επιλογή για ενεργοποίηση του γραφικού περιβάλλοντος.

```
<configuration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://sumo.dlr.de/xsd/sumoConfiguration.xsd">
   <input>
      <net-file value="erlangen.net.xml"/>
      <route-files value="erlangen.rou.xml"/>
      <additional-files value="erlangen.poly.xml"/>
   </input>
   <time>
      <begin value="0"/>
      <end value="1000"/>
      <step-length value="0.1"/>
   </time>
   <report>
      <xml-validation value="never"/>
      <xml-validation.net value="never"/>
      <no-step-log value="true"/>
   </report>
   <gui_only>
      <start value="true"/>
   </gui_only>
</configuration>
```

- Το αρχείο **erlangen.launchd.xml** περιέχει τις παρακάτω γραμμές κώδικα και μέσω αυτού πραγματοποιείται η εκκίνηση της προσομοίωσης

```
<launch>
   <copy file="erlangen.net.xml" />
   <copy file="erlangen.rou.xml" />
   <copy file="erlangen.poly.xml" />
   <copy file="erlangen.sumo.cfg" type="config" />
</launch>
```

Τέλος, θα πρέπει να εισάγουμε όλα τα παραπάνω αρχεία στο φάκελο της υλοποίησής μας (project), στο εργαλείο Veins.

Εικόνα 4.1 *Απεικόνιση ευρωπαϊκής πόλης Erlangen στο SUMO*

4.1.3 Δικτυακή προσομοίωση σεναρίου

Για τη σωστή μελέτη και την εξαγωγή συμπερασμάτων στο σενάριο, το οποίο έχουμε επιλέξει, είναι απαραίτητη μια ρεαλιστική απεικόνιση των διασυνδέσεων μεταξύ των συστατικών του σεναρίου. Η δικτυακή μας προσομοίωση πραγματοποιείται με τη χρήση του εργαλείου Omnet++ (version 5.7).

Το εργαλείο αυτό επιλέχθηκε, διότι παρέχει τη δυνατότητα στον χρήστη να προσομοιώσει σενάρια, που επιθυμεί με τη χρήση πληθώρας πρωτοκόλλων επικοινωνίας. Ένα επίσης πολύ σημαντικό πλεονέκτημα του εργαλείου αποτελεί η γραφική διεπαφή, μέσω της οποίας γίνεται ευκολότερη η απεικόνιση και κατανόηση των διασυνδέσεων. Επιπλέον, παρέχει πολλές δυνατότητες κατά τη διάρκεια της παραμετροποίησης του σεναρίου, καθιστώντας το αποτέλεσμα πιο ρεαλιστικό.

Στην προσομοίωση του σεναρίου, οι κόμβοι στο δίκτυο κάνουν χρήση του πρωτοκόλλου επικοινωνίας IEEE 802.11p (DSRC/WAVE), όπου ο προπορευόμενος κόμβος, ο οποίος είναι μολυσμένος, ξεκινάει τη μετάδοση μηνυμάτων για επερχόμενο ατύχημα στα οχήματα, που βρίσκονται εντός της εμβέλειας του. Οι κόμβοι στο δίκτυο είναι εξοπλισμένοι με κάρτες δικτύου, οι οποίες υποστηρίζουν το συγκεκριμένο πρωτόκολλο επικοινωνίας. Τέλος, το συγκεκριμένο σενάριο υλοποιήθηκε με τη χρήση του κώδικα **TraCIDemoRSU11p.cc**.

4.1.4 Παράμετροι σεναρίου

Για την υλοποίηση της προσομοίωσης της επίθεσης Sybil attack, χρησιμοποιήθηκαν οι παρακάτω παράμετροι:

Πρωτόκολλο επικοινωνίας	DSRC/WAVE
Αριθμός κόμβων	15
Ταχύτητα κόμβων	2.6 m/s
Κώδικας προσομοίωσης	TraCIDemoRSU11p.cc
Ρυθμός μετάδοσης δεδομένων	6 Mbps
Διάρκεια προσομοίωσης	300 Sec

4.2 Επιλογή δεύτερου σεναρίου

Για το δεύτερο σενάριο επίθεσης, έχουμε επιλέξει να προσομοιώσουμε μια επίθεση πλαστοπροσωπίας (impersonation attack), καθώς, ο συγκεκριμένος τύπος επίθεσης, θεωρείται εξαιρετικά επικίνδυνος για την ασφάλεια των οδηγών και του δικτύου, λόγω της ευκολίας στην υλοποίηση και του αντίκτυπου που έχει.

Στη συγκεκριμένη επίθεση, ο επιτιθέμενος καταφέρνει να πείσει τους υπόλοιπους κόμβους ότι τα μηνύματα, τα οποία μεταδίδει, προέρχονται από επαληθευμένο κόμβο του δικτύου. Για την προσομοίωσή μας, τα οχήματα επικοινωνούν μέσω του πρωτοκόλλου Wi-Fi και η ανταλλαγή μηνυμάτων γίνεται μέσω αλυσιδωτής επικοινωνίας (chain communication). Σε αρχικό στάδιο της επίθεσης, ο κακόβουλος χρήστης, αφού έχει σαρώσει πρώτα το δίκτυο με σκοπό να εντοπίσει το θύμα, θα πρέπει είτε να υποκλέψει στοιχεία της ταυτότητας του θύματος, ώστε να τα χρησιμοποιήσει για τη δημιουργία των ειδικά παραμετροποιημένων κακόβουλων πακέτων, είτε να αποκτήσει πρόσβαση διαχειριστή στο κεντρικό σύστημα του θύματος, απομακρυσμένα από όπου και θα στείλει τα κακόβουλα πακέτα προς τους υπόλοιπους κόμβους του δικτύου. Στην περίπτωσή μας ο επιτιθέμενος θεωρούμε ότι είναι ικανός να εκμεταλλευτεί τις δύο ευπάθειες της μονάδας Wi-Fi των κόμβων, όπως παρουσιάζονται στα CVE-2019-13581 και CVE-2019-13582. Ο επιτιθέμενος, μέσω ειδικά διαμορφωμένων Wi-Fi πακέτων, τα οποία αποστέλλει στο θύμα, καταφέρνει να εκτελέσει κακόβουλο κώδικα στη μονάδα Wi-Fi και μέσω αυτής να αποκτήσει δικαιώματα διαχειριστή και επομένως πρόσβαση στο κεντρικό σύστημα του κόμβου.

Στο δεύτερο στάδιο της επίθεσης, ο κακόβουλος χρήστης, αφού έχει αποκτήσει πρόσβαση στο κεντρικό σύστημα, χρησιμοποιεί τα στοιχεία ταυτότητας του κόμβου με τρόπο τέτοιο, ώστε οι υπόλοιποι κόμβοι να τον θεωρούν ως νόμιμο κόμβο του δικτύου. Ύστερα, ξεκινάει τη μετάδοση παραμετροποιημένων πακέτων για επερχόμενο ατύχημα στα οχήματα, που βρίσκονται πίσω του, με τα στοιχεία του θύματος.

Στο τρίτο στάδιο της επίθεσης, ο επιτιθέμενος, αφού έχει καταφέρει να πείσει τους κόμβους για την προέλευση των μηνυμάτων, επηρεάζει την κυκλοφορία, αφού οι κόμβοι αλλάζουν

κατεύθυνση, ώστε να αποφύγουν την επερχόμενη συμφόρηση λόγω του ψεύτικου ατυχήματος, το οποίο μετέδωσε ο κακόβουλος χρήστης. Στον Πίνακα 4.2 παρουσιάζονται τα συστατικά της επίθεσης, καθώς επίσης και τα αντίστοιχα CVEs, που αφορούν την επίθεση.

Πίνακας 4.2 *Συγκεντρωτικός πίνακας στοιχείων επίθεσης*

Επίθεση	Συστατικά επίθεσης	CVEs	CVSS Base Score
Impersonation attack	1) Ο επιτιθέμενος 2) Η μονάδα Wi-Fi 3) Το θύμα 4) Το πρωτόκολλο επικοινωνίας (Wi-Fi)	CVE-2019-13581	High: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
		CVE-2019-13582	High: 7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P)

4.2.1 Επιλογή εργαλείων για την προσομοίωση

Για να επιτύχουμε μια, όσο το δυνατόν, πιο ρεαλιστική και κατανοητή προσομοίωση του δεύτερου σεναρίου, επιλέξαμε την επίθεση πλαστοπροσωπίας. Πραγματοποιήθηκε εκ νέου σύγκριση των εργαλείων προσομοίωσης και αποφασίστηκε η χρήση του εργαλείου Veins 5.2, επομένως και των προσομοιωτών SUMO 1.17.0 και Omnet++ 5.7, λόγω του μεγάλου αριθμού δυνατοτήτων που παρέχουν στον χρήστη.

4.2.2 Προσομοίωση της κίνησης των οχημάτων

Για την υλοποίηση της επίθεσης πλαστοπροσωπίας, όπως έχουμε ήδη αναφέρει, έγινε χρήση του προσομοιωτή κίνηση SUMO 1.17.0. Σχετικά με το οδικό δίκτυο, στο οποίο πραγματοποιείται η επίθεση, αποφασίστηκε να διατηρηθεί η ίδια περιοχή Erlangen, καθώς αποτελεί καλύτερη λύση για την απεικόνιση και κατανόηση των αποτελεσμάτων της προσομοίωσης.

Όσον αφορά την κίνηση των κόμβων, αυτή παρουσιάζεται ως μια ροή. Οι κόμβοι ακολουθούν ο ένας τον άλλον με την ίδια σταθερή ταχύτητα. Για την καλύτερη απεικόνιση της επίθεσης, έχουμε παραμετροποιήσει τον κώδικα του αρχείου erlangen.rou.xml και έχουμε ορίσει τον αριθμό των κόμβων σε τέσσερις, όπως φαίνεται παρακάτω.

```
<routes>
<vType id="vtype0" accel="2.6" decel="4.5" sigma="0.5" length="2.5" minGap="2.5"
maxSpeed="14" color="1,1,0"/>
<route id="route0" edges="-39539626 -5445204#2 -5445204#1 113939244#2 -126606716
23339459 30405358#1 85355912 85355911#0 85355911#1 30405356 5931612 30350450#0
30350450#1 30350450#2 4006702#0 4006702#1 4900043 4900041#1"/>
<flow id="flow0" type="vtype0" route="route0" begin="0" period="3" number="4"/>
</routes>
```

4.2.3 Δικτυακή προσομοίωση σεναρίου

Στο σενάριο επίθεσης πλαστοπροσωπίας, το οποίο επιλέξαμε, οι κόμβοι επικοινωνούν μεταξύ τους με τη χρήση του πρωτοκόλλου Wi-Fi. Η δικτυακή προσομοίωση έγινε μέσω της χρήσης του εργαλείου Omnet++ 5.7, το οποίο επιλέχθηκε, καθώς είναι συμβατό με βιβλιοθήκες κατάλληλες για την προσομοίωση δικτυακών σεναρίων με χρήση Wi-Fi.

Οι κόμβοι της προσομοίωσης δημιουργούν μια αλυσιδωτή επικοινωνία (chain communication), όπου ο κάθε κόμβος αναμεταδίδει το μήνυμα ατυχήματος στον κόμβο, που ακολουθεί. Για την υλοποίηση της δικτυακής προσομοίωσης, παραμετροποιήθηκε ο κώδικας των αρχείων **VeinsInetSampleApplication.cc** και **VeinsInetApplicationBase.cc.**

4.2.4 Παράμετροι σεναρίου

Για την υλοποίηση της προσομοίωσης της επίθεσης πλαστοπροσωπίας, χρησιμοποιήθηκαν οι παρακάτω παράμετροι:

Πρωτόκολλο επικοινωνίας	Wi-Fi
Αριθμός κόμβων	4
Ταχύτητα κόμβων	2.6 m/s
Κώδικας προσομοίωσης	VeinsInetSampleApplication.cc/VeinsInetApplicationBase.cc
Ρυθμός μετάδοσης δεδομένων	12 Mbps
Διάρκεια προσομοίωσης	1000 Sec

4.3 Επιλογή τρίτου σεναρίου

Για το τρίτο και τελευταίο σενάριο επίθεσης, έχουμε επιλέξει να προσομοιώσουμε την επίθεση Blackhole, καθώς αποτελεί μια πολύ συχνή επίθεση στα αδόμητα οχηματικά δίκτυα και η υλοποίησή της οδηγεί σε αποσταθεροποίηση της κυκλοφορίας.

Στην επίθεση αυτή, ο επιτιθέμενος δημιουργεί ψεύτικους πίνακες δρομολόγησης, τους οποίους στη συνέχεια μεταδίδει στους γειτονικούς κόμβους, με σκοπό να τους πείσει ότι η βέλτιστη διαδρομή για τη μετάδοση του πακέτου τους, περνάει από τον ίδιο τον κόμβο. Στη συνέχεια, αφού έχει κερδίσει την εμπιστοσύνη των γειτονικών κόμβων, είτε αλλοιώνει το πακέτο, το οποίο δέχεται και το προωθεί, είτε δεν προωθεί το πακέτο (packet drop) στον επόμενο κατά σειρά κόμβο, οδηγώντας σε απώλεια πακέτων (packet loss), επομένως και κρίσιμων δεδομένων.

Κατά τη διάρκεια της επίθεσης, οι κόμβοι έχουν δημιουργήσει μια αλυσιδωτή επικοινωνία (chain communication) και χρησιμοποιούν την τεχνολογία Wi-Fi. Η υλοποίηση της επίθεσης χωρίζεται σε στάδια. Στο πρώτο στάδιο αυτής, ο επιτιθέμενος ερευνά για ευπάθειες, τις οποίες θα μπορούσε να εκμεταλλευτεί στο σύστημα του κόμβου, ώστε να αποκτήσει τη δυνατότητα εκτέλεσης κώδικα με δικαιώματα διαχειριστή. Στην περίπτωσή μας, θεωρούμε ότι ο επιτιθέμενος έχει αποκτήσει φυσική πρόσβαση στο όχημα, από το οποίο θα εξαπολύσει την επίθεση. Η ευπάθεια, την οποία και

εκμεταλλεύεται, όπως αναφέρεται και στο CVE-2018-9322, αφορά το σύστημα ψυχαγωγίας του κόμβου. Μέσω αυτής της ευπάθειας, ο επιτιθέμενος έχει τη δυνατότητα να παρακάμψει τους μηχανισμούς ασφαλείας για αναβαθμίσεις του σταθερολογισμικού (firmware) και έτσι να αποκτήσει τη δυνατότητα εκτέλεσης εντολών στο σύστημα με δικαιώματα διαχειριστή. Για να εκμεταλλευτεί τη συγκεκριμένη ευπάθεια, ο κακόβουλος χρήστης κάνει χρήση της USB διεπαφής ή της OBD-II διεπαφής του οχήματος.

Στο δεύτερο στάδιο της επίθεσης, και αφού ο κακόβουλος χρήστης έχει αποκτήσει τη δυνατότητα εκτέλεσης εντολών ως διαχειριστής, δημιουργεί ψεύτικους πίνακες δρομολόγησης, τους οποίους και διαφημίζει στους γειτονικούς κόμβους. Στο σενάριο μας ο κακόβουλος κόμβος είναι ο τρίτος κατά σειρά. Στη συνέχεια, ο προπορευόμενος κόμβος αποστέλλει μήνυμα ατυχήματος στον κόμβο, που τον ακολουθεί. Ο κόμβος αυτός με την σειρά του μεταδίδει το μήνυμα στον επόμενο κόμβο. Όμως, κατά το τρίτο στάδιο της επίθεσης, ο επιτιθέμενος δηλαδή ο τρίτος κατά σειρά κόμβος δε μεταδίδει το πακέτο (packet drop), με αποτέλεσμα ο τέταρτος κόμβος να μην ενημερωθεί για την κατάσταση των προπορευόμενων οχημάτων, με αποτέλεσμα να μην αλλάξει διαδρομή και να ακολουθήσει τη διαδρομή, που έχει πραγματοποιηθεί το ατύχημα.

Η επίθεση αυτή επηρεάζει την ομαλή λειτουργία του οδικού δικτύου και μπορεί να αποβεί μοιραία για την ασφάλεια των οδηγών, καθώς λόγω αυτής προκαλείται απώλεια πακέτων με χρήσιμες πληροφορίες, όπως στο παράδειγμά μας, όπου το ατύχημα του προπορευόμενου οχήματος πιθανόν να οδηγούσε σε νέα σύγκρουση των κόμβων, που θα ακολουθούσαν την ίδια διαδρομή. Στον Πίνακα 4.3 παρουσιάζονται τα συστατικά της επίθεσης, καθώς επίσης και το αντίστοιχο CVE που αφορά την επίθεση.

Πίνακας 4.3 *Συγκεντρωτικός πίνακας στοιχείων επίθεσης*

Επίθεση	Συστατικά επίθεσης	CVEs	CVSS Base Score
Blackhole attack	1) Ο επιτιθέμενος 2) Η μονάδα USB 3) Το σύστημα ψυχαγωγίας του κόμβου (infotainment) 4) Το πρωτόκολλο επικοινωνίας (Wi-Fi)	CVE-2018-9322	High: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

4.3.1 Επιλογή εργαλείων για την προσομοίωση

Στο πλαίσιο της τρίτης προσομοίωσης, έγινε χρήση του προσομοιωτή κίνησης SUMO 1.17.0 και του προσομοιωτή δικτύου Omnet++ 5.7 μέσω του εργαλείου Veins 5.2. Τα παραπάνω εργαλεία επιλέχθηκαν για την υλοποίηση και του τρίτου σεναρίου επίθεσης, καθώς ικανοποιούν τις απαιτήσεις, που υπάρχουν για την προσομοίωση.

4.3.2 Προσομοίωση της κίνησης των οχημάτων

Για την επιτυχή προσομοίωση της επίθεσης Blackhole, όσον αφορά το κομμάτι της προσομοίωσης της κίνησης έγινε εκ νέου χρήση του εργαλείου SUMO 1.17.0, διότι αποτελεί την βέλτιστη λύση βάση των δυνατοτήτων, τις οποίες παρέχει. Η περιοχή, στην οποία διαδραματίζεται το σενάριό μας, παραμένει η ευρωπαϊκή πόλη Erlangen, καθώς παρέχει καλύτερη οπτικοποίηση και κατανόηση του σεναρίου επίθεσης. Τέλος, όσον αφορά τις παραμέτρους της προσομοίωσης κίνησης όπως: α) ο αριθμός οχημάτων, β) η ταχύτητα τους, γ) η διαδρομή τους, δεν μεταβλήθηκαν.

4.3.3 Δικτυακή προσομοίωση σεναρίου

Για τη δικτυακή προσομοίωση της επίθεσης Blackhole επιλέχθηκε το εργαλείο Omnet++ 5.7, καθώς τα οχήματα στο σενάριό μας επικοινωνούν μεταξύ τους, κάνοντας χρήση του πρωτοκόλλου Wi-Fi. Όπως έχουμε ήδη αναφέρει, το συγκεκριμένο εργαλείο είναι συμβατό με αρκετές χρήσιμες βιβλιοθήκες, οι οποίες συντελούν στην υλοποίηση του σεναρίου. Επιπλέον, παρέχει τη δυνατότητα στον χρήστη να παραμετροποιήσει τον κώδικα της προσομοίωσης με τρόπο τέτοιο, ώστε ο επιλεγμένος κόμβος να μπορεί να απορρίπτει εισερχόμενα πακέτα (packet drop), γεγονός το οποίο συντελεί στην προσομοίωση της επίθεσης.

Κατά την δικτυακή προσομοίωση, οι κόμβοι δημιουργούν μια αλυσιδωτή επικοινωνία, κάνοντας χρήση της τεχνολογίας Wi-Fi. Ο προπορευόμενος κόμβος αποστέλλει το πρώτο μήνυμα ατυχήματος στον ακόλουθο κόμβο του, ο οποίος είναι και ο επιτιθέμενος κόμβος. Στη συνέχεια, ενώ ο δεύτερος κόμβος θα έπρεπε να προωθήσει το μήνυμα ατυχήματος στον τρίτο κατά σειρά κόμβο, αυτός απορρίπτει το πακέτο, με αποτέλεσμα το πακέτο να μη φτάσει στον τρίτο κόμβο. Για να επιτύχουμε μια τέτοια συμπεριφορά των κόμβων, παραμετροποιήσαμε κατάλληλα τον κώδικα των αρχείων **VeinsInetSampleApplication.cc** και **VeinsInetApplicationBase.cc.** Το αποτέλεσμα μιας τέτοιας συμπεριφοράς μέσα στο δίκτυο είναι η απώλεια πακέτων (packet loss) και επομένως η μη ορθή διάδοση χρήσιμων πληροφορίων για την ασφάλεια των οδηγών.

4.3.4 Παράμετροι σεναρίου

Για την υλοποίηση της προσομοίωσής του σεναρίου επίθεσης Blackhole, χρησιμοποιήθηκαν οι παρακάτω παράμετροι:

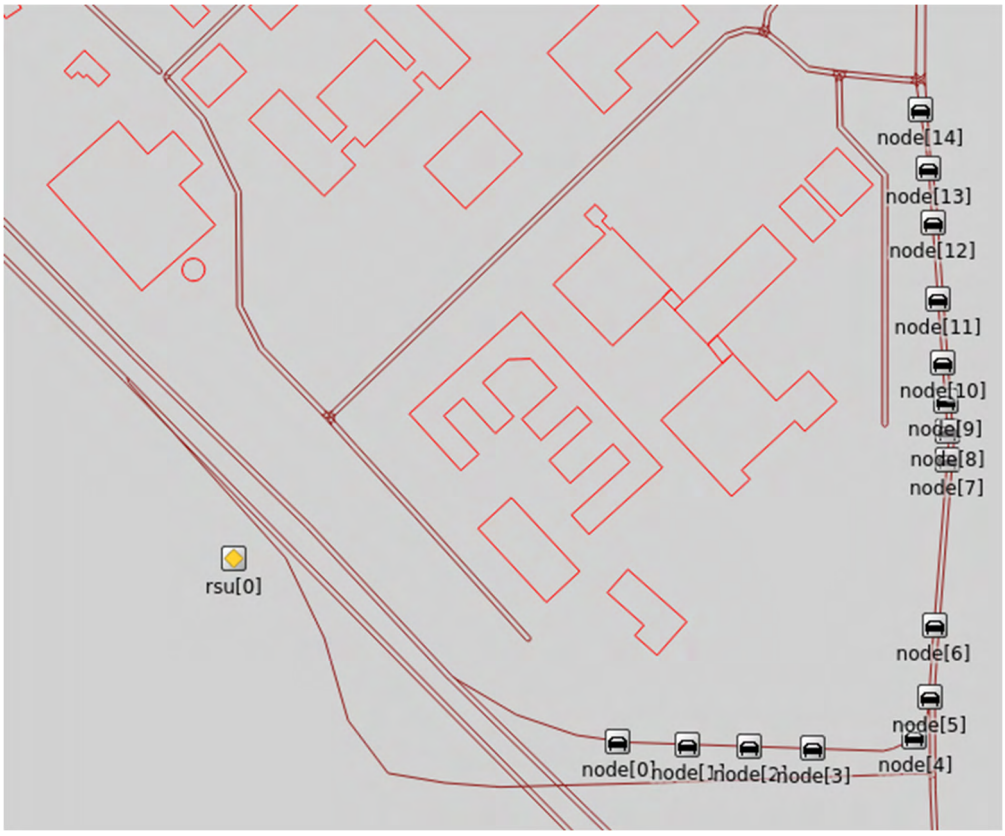
Πρωτόκολλο επικοινωνίας	Wi-Fi
Αριθμός κόμβων	4
Ταχύτητα κόμβων	2.6 m/s
Κώδικας προσομοίωσης	VeinsInetSampleApplication.cc/VeinsInetApplicationBase.cc
Ρυθμός μετάδοσης δεδομένων	12 Mbps
Διάρκεια προσομοίωσης	1000Sec

Κεφάλαιο 5: Αποτελέσματα προσομοίωσης

Στο παρόν κεφαλαίο, θα παρουσιαστούν τα αποτελέσματα από την κάθε επίθεση στο αδόμητο οχηματικό δίκτυο της πόλης Erlangen, την οποία επιλέξαμε να προσομοιώσουμε στο πλαίσιο αυτής της εργασίας. Τα αποτελέσματα της κάθε επίθεσης θα αναλυθούν ξεχωριστά για κάθε ένα σενάριο. Για την καλύτερη κατανόηση των αποτελεσμάτων του κάθε σεναρίου ξεχωριστά, θα γίνει χρήση στιγμιότυπων από το γραφικό περιβάλλον του εργαλείου Veins, το οποίο χρησιμοποιήθηκε για την υλοποίηση και των τριών σεναρίων.

5.1 Αποτελέσματα πρώτης προσομοίωσης

Για την πρώτη προσομοίωση επιλέξαμε την επίθεση Sybil attack, όπως έχουμε ήδη αναφέρει σε προηγούμενο κεφάλαιο. Στο σενάριο, το οποίο υλοποιήσαμε, ο προπορευόμενος κόμβος είναι ταυτόχρονα και ο μολυσμένος κόμβος του δικτύου, ο οποίος θα μεταδώσει το ψευδές μήνυμα ατυχήματος με σκοπό την αλλοίωση της κυκλοφοριακής ροής. Θεωρούμε ότι ο επιτιθέμενος έχει εκμεταλλευτεί την ευπάθεια του πρωτοκόλλου SCEP και έχει δημιουργήσει τον μολυσμένο κόμβο, ο οποίος απεικονίζεται στην προσομοίωση ως node[0]. Όπως παρατηρούμε στην Εικόνα 5.1, τα οχήματα κινούνται σε μια οδό του οδικού δικτύου σε μορφή ροής, μέχρι να φτάσουν στον τελικό τους προορισμό.

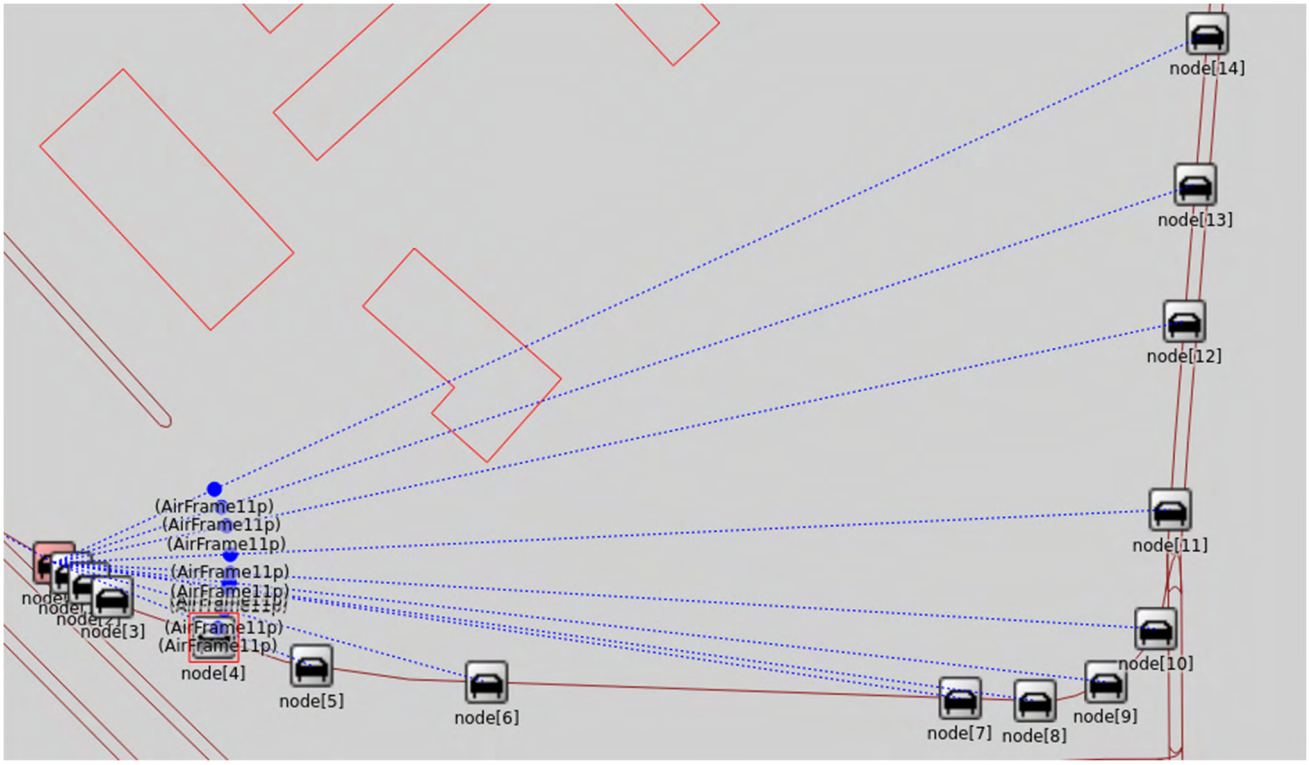


Εικόνα 5.1 *Απεικόνιση της κίνησης των οχημάτων μέσα στο δίκτυο*

Σε χρονικό σημείο της προσομοίωσης, το οποίο έχουμε ορίσει εμείς, ο κόμβος 0 (node [0]) γίνεται κόκκινος, όπως φαίνεται στην Εικόνα 5.2 και ξεκινάει τη μετάδοση μηνύματος ατυχήματος, με χρήση του πρωτοκόλλου DSRC/WAVE, προς τους κόμβους και τις παρόδιες μονάδες, που βρίσκονται στην εμβέλεια εκπομπής του, όπως φαίνεται στην Εικόνα 5.3.

Εικόνα 5.2 *Έναρξη μετάδοσης μηνύματος για ατύχημα*

Ο κάθε κόμβος με τη σειρά του αναμεταδίδει το μήνυμα αυτό στους πλησιέστερούς του κόμβους. Με μπλε κουκίδα (AirFrame11p) απεικονίζονται τα μηνύματα, που αποστέλλονται στους κόμβους.



Εικόνα 5.3 *Μετάδοση μηνύματος για ατύχημα με χρήση της τεχνολογίας DSRC/WAVE*

Αφού ολοκληρωθεί η μετάδοση των μηνυμάτων, παρατηρούμε ότι, ενώ όλα τα οχήματα της προσομοίωσης έπρεπε να ακολουθήσουν την ίδια διαδρομή, τα οχήματα node 12,13 και 14, τα οποία είχαν τη δυνατότητα αναστροφής, ακολούθησαν άλλη διαδρομή, ώστε να φτάσουν στον τελικό προορισμό τους, όπως μπορούμε να διακρίνουμε στην Εικόνα 5.4.

Εικόνα 5.4 *Απεικόνιση νέων διαδρομών ύστερα από την επίθεση*

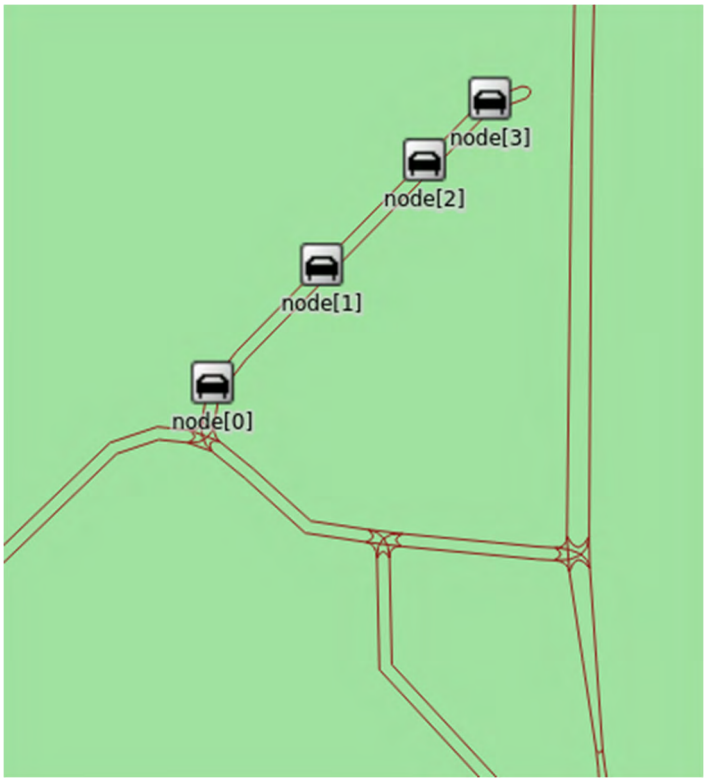
Αντίθετα, τα υπόλοιπα οχήματα παρέμειναν προσκολλημένα πίσω από τον μολυσμένο κόμβο έως ότου αυτό να αρχίσει να κινείται εκ νέου προς τον τελικό προορισμό, όπως φαίνεται στην Εικόνα 5.5.

Εικόνα 5.5 *Απεικόνιση κίνησης του επιτιθέμενου κόμβου προς τον τελικό προορισμό*

Τέλος, μέσω της προσομοίωσης αυτής, παρατηρούμε ότι με την υλοποίηση μιας τέτοια επίθεσης ο επιτιθέμενος μπορεί με ευκολία να προκαλέσει αλλοίωση της κυκλοφοριακής ροής, επομένως και συμφόρηση στο οδικό δίκτυο ακόμα και σε αδόμητα οχηματικά δίκτυα με μεγαλύτερο αριθμό κόμβων, μέσω της δημιουργίας περισσότερων μολυσμένων κόμβων.

5.2 Αποτελέσματα δεύτερης προσομοίωσης

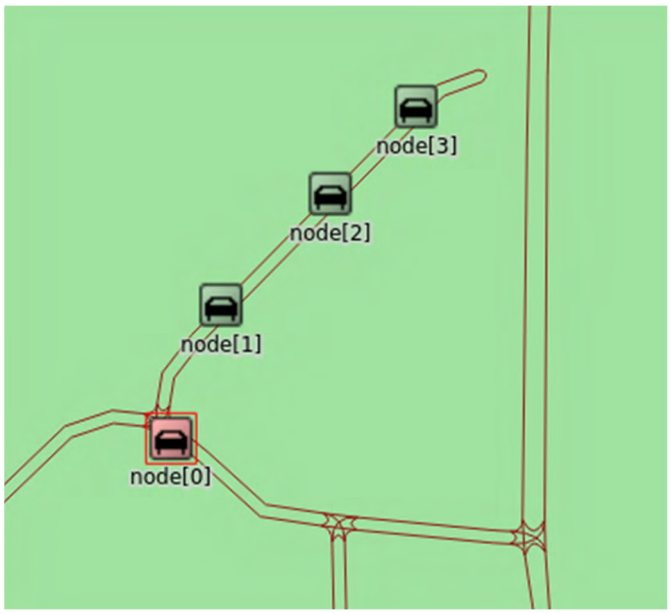
Για τη δεύτερη προσομοίωσή μας, επιλέξαμε να παρουσιάσουμε μια επίθεση πλαστοπροσωπίας (Impersonation attack). Στο σενάριο, το οποίο υλοποιήσαμε, θεωρούμε ότι ο επιτιθέμενος έχει εκτελέσει με επιτυχία το πρώτο στάδιο της επίθεσης, όπου θα πρέπει να έχει αποκτήσει πρόσβαση στα στοιχεία ταυτότητας του θύματος εκμεταλλευόμενος τις ευπάθειες, τις οποίες έχουμε ήδη παρουσιάσει. Στο γραφικό περιβάλλον του εργαλείου Veins τα οχήματα κινούνται κατά μήκος μιας οδού το ένα πίσω από το άλλο, με σκοπό να ακολουθήσουν τη διαδρομή, την οποία έχουμε εμείς ορίσει, μέσω του εργαλείου SUMO έως ότου φτάσουν στον τελικό τους προορισμό, όπως φαίνεται στην Εικόνα 5.6.



Εικόνα 5.6 *Απεικόνιση κίνησης οχημάτων*

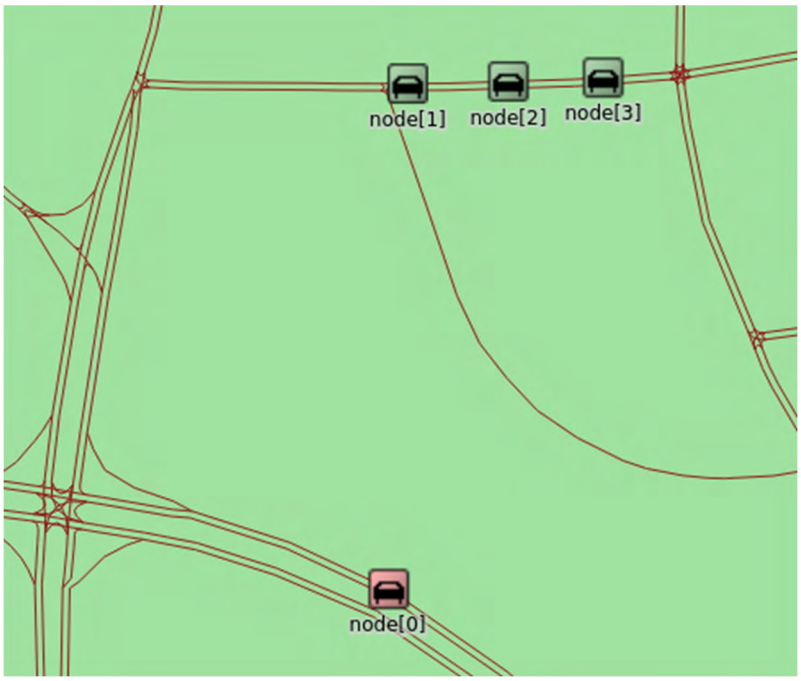
Για τη μετάδοση των μηνυμάτων εντός του δικτύου, οι κόμβοι κάνουν χρήση της τεχνολογίας Wi-FI και δημιουργούν μια αλυσιδωτή επικοινωνία. Κατά τη διάρκεια της προσομοίωσης, ο επιτιθέμενος κόμβος, ο οποίος απεικονίζεται ως node[0], ξεκινάει τη μετάδοση μηνυμάτων για ατύχημα, κάνοντας

χρήση των στοιχείων του θύματος. Όπως φαίνεται και στην Εικόνα 5.7, ο δεύτερος κόμβος δέχεται το μήνυμα, το οποίο με τη σειρά του προωθείται στον επόμενο κατά σειρά κόμβο. Η διαδικασία αυτή τερματίζεται, όταν το μήνυμα φτάσει στον τελευταίο κόμβο. Σημειώνεται ότι οι κόμβοι, οι οποίοι έχουν δεχτεί το μήνυμα, αποκτούν πράσινο χρώμα στην προσομοίωση.



Εικόνα 5.7 *Απεικόνιση οχημάτων τα οποία έχουν λάβει το μήνυμα ατυχήματος*

Αφού γίνει η μετάδοση του μηνύματος για το ατύχημα, παρατηρούμε ότι τα υπόλοιπα οχήματα παρακάμπτουν την αρχική τους διαδρομή και ακολουθούν νέα, όπως φαίνεται στην Εικόνα 5.8.

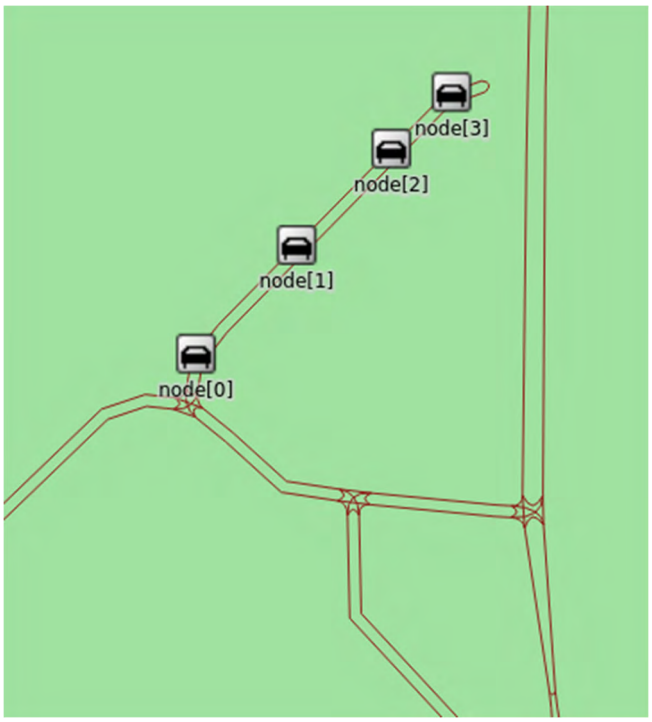


Εικόνα 5.8 *Απεικόνιση νέας διαδρομής οχημάτων ύστερα από την επίθεση*

Το αποτέλεσμα της προσομοίωσής μας είναι ότι ο επιτιθέμενος κόμβος κατάφερε να μεταβάλλει την κυκλοφορία με τέτοιον τρόπο, ώστε να παραμείνει ως μοναδικό όχημα στη συγκεκριμένη οδό, παραπλανώντας τους υπόλοιπους κόμβους, ώστε να αλλάξουν κατεύθυνση. Τέτοιου είδους επιθέσεις μπορούν να απαλλάξουν υπαίτιους κακόβουλων ενεργειών αλλά και να δημιουργήσουν κυκλοφοριακά προβλήματα εντός του οδικού δικτύου.

5.3 Αποτελέσματα τρίτης προσομοίωσης

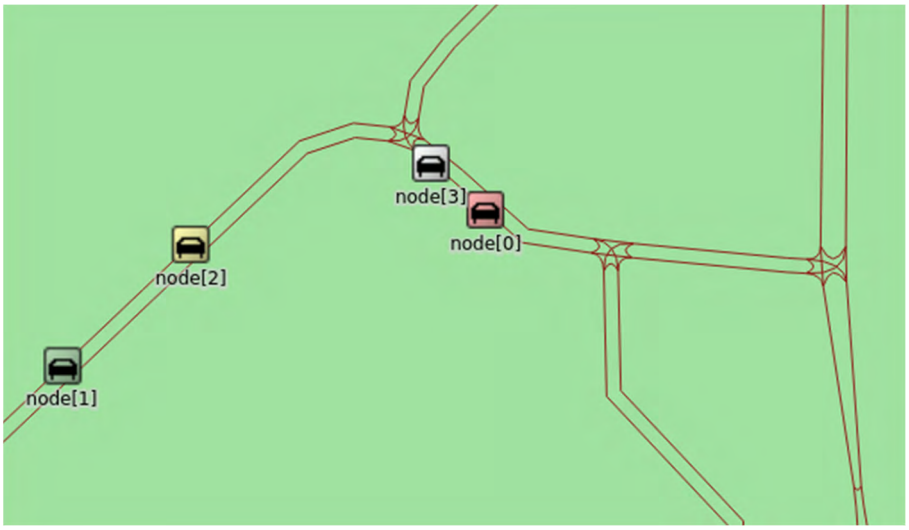
Για την τρίτη προσομοίωση, έχει επιλεχθεί η υλοποίηση της επίθεσης Blackhole. Στο πλαίσιο του σεναρίου αυτού, θεωρούμε ότι ο επιτιθέμενος έχει καταφέρει να εκμεταλλευτεί την ευπάθεια, που παρατηρείται στο σύστημα ψυχαγωγίας του κόμβου, την οποία έχουμε ήδη αναλύσει, ώστε να αποκτήσει πρόσβαση στο κεντρικό σύστημα με δικαιώματα διαχειριστή. Όπως μπορούμε να παρατηρήσουμε στην Εικόνα 5.9, τα οχήματα ακολουθούν κίνηση ροής μέχρι τον τελικό τους στόχο.



Εικόνα 5.9 *Απεικόνιση κίνησης οχημάτων*

Ο προπορευμένος κόμβος παρουσιάζει κάποιο ατύχημα, το οποίο και ξεκινάει να μεταδίδει προς τους ακόλουθους κόμβους, ώστε να αλλάξουν πορεία και να αποφύγουν τυχόν νέα σύγκρουση, ή συμφόρηση. Όμως, όταν ο τρίτος κόμβος, ο οποίος είναι και ο κακόβουλος, θα πρέπει να προωθήσει το μήνυμα στον ακόλουθό του, τότε αυτός απορρίπτει (packet drop) το πακέτο, με αποτέλεσμα να μην ενημερωθεί ο τέταρτος κόμβος. Η ενέργεια αυτή οδηγεί σε απώλεια πακέτων (packet loss), επομένως και χρήσιμων δεδομένων για τους οδηγούς. Σημειώνεται ότι ο κόμβος, ο οποίος έχει εμπλακεί σε ατύχημα, έχει χρώμα κόκκινο, ο κόμβος, που έλαβε το μήνυμα, έχει χρώμα πράσινο, ο

επιτιθέμενος κόμβος, που απέρριψε το πακέτο, έχει χρώμα κίτρινο και ο κόμβος, ο οποίος δεν έλαβε το μήνυμα απεικονίζεται με γκρι χρώμα. Τέλος, το αποτέλεσμα της προσομοίωσης αυτής, όπως απεικονίζεται και στην εικόνα 5.10, είναι ότι ο τέταρτος κόμβος της προσομοίωσης, ο οποίος δεν έλαβε το μήνυμα ατυχήματος, αδυνατεί να αλλάξει πορεία, σε αντίθεση με τους υπόλοιπους κόμβους, με αποτέλεσμα να ακολουθήσει τη διαδρομή, όπου υπάρχει συμφόρηση και να παραμείνει προσκολλημένος πίσω από τον κόμβο, ο οποίος είχε το ατύχημα, έως ότου αυτός να ξεκινήσει να κινείται εκ νέου προς τον τελικό προορισμό του.



Εικόνα 5.10 *Αποτέλεσμα επίθεσης Blackhole*

Κεφάλαιο 6: Επίλογος και μελλοντική εργασία

Στο πλαίσιο της παρούσας διπλωματικής εργασίας, πραγματοποιήθηκε έρευνα σχετικά με την ασφάλεια των αδόμητων οχηματικών δικτύων. Για την καλύτερη ανάλυση και απεικόνιση του θέματος, εστιάσαμε στη δημιουργία τριών διαφορετικών σεναρίων επίθεσης (Sybil attack, Impersonation attack, Blackhole attack), τα οποία προσομοιώσαμε με τη χρήση του συνδυαστικού εργαλείου Veins.

Κατά τη διάρκεια της έρευνάς μας, εξετάσαμε τις διαθέσιμες τεχνολογίες διασύνδεσης των κόμβων μέσα σε ένα αδόμητο οχηματικό δίκτυο, καθώς επίσης και τους διαθέσιμους προσομοιωτές για τη δημιουργία των σεναρίων επίθεσης σε ένα ελεγχόμενο περιβάλλον, με σκοπό την καλύτερη κατανόηση της σοβαρότητας των ζητημάτων ασφαλείας, που παρατηρούνται στα αδόμητα οχηματικά δίκτυα. Από την έρευνα, την οποία πραγματοποιήσαμε, προκύπτουν τα εξής συμπεράσματα:

- Τα αδόμητα οχηματικά δίκτυα αποτελούνται από συστατικά, τα οποία με την πάροδο του χρόνου ενσωματώνουν όλο ένα και πιο περίπλοκα συστήματα. Κατά καιρούς, λόγω και της πολυπλοκότητας, τα συστήματα αυτά παρουσιάζουν ευπάθειες, τις οποίες μπορούν κακόβουλοι χρήστες να εκμεταλλευτούν, ώστε να υλοποιήσουν μια σειρά από επιθέσεις. Οι επιθέσεις αυτές μπορεί να είναι είτε σε επίπεδο κόμβου είτε σε επίπεδο δικτύου, λόγω ευπάθειας σε κάποιο πρωτόκολλο επικοινωνίας.
- Από την προσομοίωση της επίθεσης Sybil συμπεραίνουμε ότι τα αδόμητα οχηματικά δίκτυα μπορούν να παρουσιάσουν προβλήματα εμπιστοσύνης μεταξύ των κόμβων, με αποτέλεσμα τη χειραγώγηση του δικτύου από κάποιον επιτιθέμενο και τη μη ορθή λειτουργία αυτού.
- Μέσω επιθέσεων πλαστοπροσωπίας (Impersonation attack), που μπορούν να υλοποιηθούν μέσα σε ένα αδόμητο οχηματικό δίκτυο, συμπεραίνουμε ότι οι επιτιθέμενοι έχουν τη δυνατότητα για εκτέλεση κακόβουλων ενεργειών, όπως ανακατεύθυνση της κυκλοφορίας στο οδικό δίκτυο, αποφεύγοντας την οποιαδήποτε ποινή.
- Μέσα από την προσομοίωση της επίθεσης Blackhole, παρατηρούμε ότι τα αδόμητα οχηματικά δίκτυα είναι ευάλωτα σε απώλεια πακέτων, γεγονός το οποίο επηρεάζει την ασφάλεια των οδηγών, καθώς δε δέχονται σημαντικές πληροφορίες, που αφορούν την ασφάλειά τους.

- Τα διαθέσιμα εργαλεία προσομοίωσης παρέχουν συγκεκριμένες δυνατότητες για προσομοίωση επιθέσεων στα αδόμητα οχηματικά δίκτυα, επομένως περιορίζουν τα όρια της έρευνας, όσον αφορά την ανάλυση περαιτέρω ευπαθειών.

Συμπερασματικά, μέσω της έρευνας που διεξήχθη, καταλήγουμε ότι η ασφάλεια στα αδόμητα οχηματικά δίκτυα είναι καίριας σημασίας, καθώς τα συγκεκριμένα δίκτυα και οι εφαρμογές αυτών έχουν τη δυνατότητα να ενισχύσουν την καθολική ασφάλεια των οδικών δικτύων και να βελτιώσουν την κυκλοφορία εντός των αστικών ιστών. Καθώς τα αδόμητα οχηματικά δίκτυα αποτελούν ένα διαρκώς εξελισσόμενο κλάδο, η ανάγκη για συνεχή έρευνα και βελτίωση της ασφάλειας αυτών είναι επιτακτική. Η παρούσα διπλωματική εργασία θα μπορούσε να χρησιμοποιηθεί ως εφαλτήριο για έρευνα νέων ευπαθειών στα αδόμητα οχηματικά δίκτυα, καθώς επίσης και μηχανισμούς αντιμετώπισης αυτών.

Σε μελλοντική ενασχόληση με την παρούσα εργασία, θα ήταν δυνατή η δημιουργία ενός πιο ρεαλιστικού μοντέλου προσομοίωσης. Για τη δημιουργία του νέου μοντέλου θα μπορούσε να γίνει χρήση τηλεκατευθυνόμενων οχημάτων (RC cars), τα οποία να ενσωματώνουν τα απαραίτητα χαρακτηριστικά, όπως δικτυακές διεπαφές, επεξεργαστικές μονάδες, μονάδα GPS και αισθητήρες. Τα συγκεκριμένα οχήματα θα ήταν εφικτό να χρησιμοποιούν τη γνωστή μονάδα Raspberry Pi, ως επεξεργαστική μονάδα. Μέσω της δημιουργίας της κατάλληλης διασύνδεσης για την επικοινωνία των οχημάτων, θα ήταν εφικτή η δοκιμή εκμετάλλευσης ευπαθειών, που αφορούν τεχνολογίες επικοινωνίας για την πραγματοποίηση επιθέσεων. Επιπλέον, θα ήταν εφικτό να πραγματοποιηθεί εκμετάλλευση ευπάθειας είτε στη μονάδα Raspberry Pi είτε στη μονάδα GPS και τους αισθητήρες. Μέσω των επιθέσεων αυτών, είναι δυνατή η ανάλυση της συμπεριφοράς του κάθε κόμβου σε αρκετά ρεαλιστικό περιβάλλον και η καλύτερη κατανόηση του αντίκτυπου, που θα μπορούσε να έχει η κάθε επίθεση σε πραγματικό περιβάλλον.

Βιβλιογραφία

1. Benarous, L., Batim, S. and Mellouk, A. (2022a) *Security in vehicular networks: Focus on location and Identity Privacy*. London: Wiley-ISTE.
2. Botkar, S.P. *et al.* (2021) *Vanet: Challenges and opportunities*. Boca Raton: CRC Press, Taylor et Francis Group.
3. Yoshizawa, T. *et al.* (2023) 'A survey of security and privacy issues in V2X Communication Systems', *ACM Computing Surveys*, 55(9), pp. 1–36. doi:10.1145/3558052.
4. Saggi, M.S.K. and Sandhu, R.K. (2014) *A Survey of Vehicular Ad Hoc network on Attacks & Security Threats in VANETs*, pp. 1–9.
5. Karne, Radhakrishna & Sreeja, T. (2021). REVIEW ON VANET ARCHITECTURE ANDAPPLICATIONS. 12. 1745-1749.
6. Sheikh, Liang and Wang (2019) 'A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)', *Sensors*, 19(16), p. 3589. doi:10.3390/s19163589.
7. Rawat, D.B. and Bajracharya, C. (2018) *Vehicular Cyber Physical Systems Adaptive Connectivity and security*. Cham: Springer International Publishing.
8. Tangade, S.S. and Manvi, S.S. (2013) 'A survey on attacks, security and Trust Management Solutions in VANETs', *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*[Preprint]. doi:10.1109/icccnt.2013.6726668.
9. Petrov, T. *et al.* (2021) 'A performance benchmark for dedicated short-range communications and LTE-based cellular-V2X in the context of vehicle-to-infrastructure communication and urban scenarios', *Sensors*, 21(15), p. 5095. doi:10.3390/s21155095.
10. El Zorkany, M., Yasser, A. and Galal, A.I. (2020) 'Vehicle to vehicle "V2V" communication: Scope, importance, challenges, research directions and future', *The Open Transportation Journal*, 14(1), pp. 86–98. doi:10.2174/1874447802014010086.
11. Abdessamed, D. and Samira, M. (2014) 'Target tracking in VANETs using V2I and V2V communication', *2014 International Conference on Advanced Networking Distributed Systems and Applications* [Preprint]. doi:10.1109/inds.2014.11.
12. Zhou, Li and Ding (2019) 'Practical v2i secure communication schemes for heterogeneous VANETs', *Applied Sciences*, 9(15), p. 3131. doi:10.3390/app9153131.
13. SERAJ, E. *et al.* (2021) *PLANNING V2X COMMUNICATION SYSTEM USING VANET ON OMNET++ SIMULATOR*[Preprint]. doi:10.21608/iugrc.2021.245415.
14. Bhover, Sushma.U., Tugashetti, A. and Rashinkar, P. (2017) 'V2X communication protocol in VANET for co-operative Intelligent Transportation System', *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* [Preprint]. doi:10.1109/icimia.2017.7975531.
15. Priyanka, j and M, R. (2023) *Signature based V2X communication and authentications using resourceful Signcryption and optimised ECC* [Preprint]. doi:10.21203/rs.3.rs-1397170/v1.
16. Alalewi, A., Dayoub, I. and Cherkaoui, S. (2021) 'On 5G-V2X use cases and enabling technologies: A comprehensive survey', *IEEE Access*, 9, pp. 107710–107737. doi:10.1109/access.2021.3100472.
17. N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong and K. H. Chong, "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions," in IEEE Access, vol. 10, pp. 86127-86180, 2022, doi: 10.1109/ACCESS.2022.3198656.
18. K, T. *et al.* (2015) 'A survey on Vanet Technologies', *International Journal of Computer Applications*, 121(18), pp. 1–9. doi:10.5120/21637-4965.
19. Moustafa, Hassnaa & Zhang, Yan. (2009). Vehicular Networks: Techniques, Standards, and Applications. 2.
20. Elsayed, M.M. *et al.* (2023) 'Vehicles Communications Handover in 5G: A survey', *ICT Express*, 9(3), pp. 366–378. doi:10.1016/j.icte.2022.01.005.

21. *5G spectrum and frequency bands: What they are and why they matter* (2023) *Verizon*. Available at: https://www.verizon.com/about/news/5g frequency-bands-explained (Accessed: 26 September 2023).
22. Simmons, A. (2022) *What's the difference between 4G LTE and 5G?*, *Dgtl Infra*. Available at: https://dgtlinfra.com/explaining-the-key-differences-between-4g-and-5g/ (Accessed: 26 September 2023).
23. Sahoo, P., Chiang, M.-J. and Wu, S.-L. (2014) 'SVANET: A smart vehicular ad hoc network for efficient data transmission with wireless sensors', *Sensors*, 14(12), pp. 22230–22260. doi:10.3390/s141222230.
24. Arena, F., Pau, G. and Severino, A. (2020) 'A review on IEEE 802.11p for Intelligent Transportation Systems', *Journal of Sensor and Actuator Networks*, 9(2), p. 22. doi:10.3390/jsan9020022.
25. Jiang, D. and Delgrossi, L. (2008) 'IEEE 802.11p: Towards an international standard for wireless access in Vehicular Environments', *VTC Spring 2008 - IEEE Vehicular Technology Conference* [Preprint]. doi:10.1109/vetecs.2008.458.
26. Wang, X. *et al.* (2019) 'Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions', *IEEE Communications Surveys & Tutorials*, 21(2), pp. 1314–1345. doi:10.1109/comst.2018.2882064.
27. Kelarestaghi, K.B., Foruhandeh, M., Heaslip, K.P., & Gerdes, R.M. (2019). Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures. ArXiv, abs/1903.01541.
28. Al-Sultan, S. *et al.* (2014) 'A comprehensive survey on Vehicular Ad Hoc Network', *Journal of Network and Computer Applications*, 37, pp. 380–392. doi:10.1016/j.jnca.2013.02.036.
29. Malhi, A.K., Batra, S. and Pannu, H.S. (2020) 'Security of vehicular ad-hoc networks: A comprehensive survey', *Computers & Security*, 89, p. 101664. doi:10.1016/j.cose.2019.101664.
30. Chowdhury, N. and Mackenzie, L.M. (2022) *Vehicular Communications for smart cars: Protocols, applications and security concerns*. Boca Raton: CRC Press, Taylor & Francis Group.
31. Hartenstein, H. and Laberteaux, K. (2010) *VANETs vehicular applications and inter networking technologies*. Chichester, West Sussex, U.K.: Wiley.
32. Campolo, C., Molinaro, A. and Scopigno, R. (2015) *Vehicular ad hoc networks standards, Solutions, and research*. Cham: Springer International Publishing.
33. I. Ali, Q. (2015) 'Security issues of Solar Energy Harvesting Road Side Unit (RSU)', *Iraqi Journal for Electrical And Electronic Engineering*, 11(1), pp. 18–31. doi:10.33762/eeej.2015.102711.
34. Shepard, D.P., Humphreys, T.E. and Fansler, A.A. (2012) 'Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks', *International Journal of Critical Infrastructure Protection*, 5(3–4), pp. 146–153. doi:10.1016/j.ijcip.2012.09.003.
35. Zeng, K.C. *et al.* (2017) 'A practical GPS location spoofing attack in Road Navigation Scenario', *Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications* [Preprint]. doi:10.1145/3032970.3032983.
36. Al-shareeda, M.A. *et al.* (2020) 'Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)', *2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP)* [Preprint]. doi:10.1109/icicsp50920.2020.9232047.
37. Arif, M. *et al.* (2019) 'A survey on security attacks in VANETs: Communication, applications and challenges', *Vehicular Communications*, 19, p. 100179. doi:10.1016/j.vehcom.2019.100179.
38. Azam, S. *et al.* (2022) 'Collaborative learning based Sybil Attack Detection in vehicular ad-hoc networks (VANETS)', *Sensors*, 22(18), p. 6934. doi:10.3390/s22186934.
39. Malik, A. *et al.* (2022) 'An efficient dynamic solution for the detection and prevention of Black Hole attack in Vanets', *Sensors*, 22(5), p. 1897. doi:10.3390/s22051897.
40. Ahmad, F. *et al.* (2018) 'Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies', *Sensors*, 18(11), p. 4040. doi:10.3390/s18114040.

41. Al-shareeda, M.A., Anbar, M., Manickam, S., *et al.* (2020) 'Review of Prevention Schemes for Man-in-the-middle (MITM) attack in vehicular ad hoc networks', *International Journal of Engineering and Management Research*, 10(3), pp. 153–158. doi:10.31033/ijemr.10.3.23.
42. Le, D. *et al.* (2021) 'A behavior-based malware spreading model for vehicle-to-vehicle communications in VANET Networks', *Electronics*, 10(19), p. 2403. doi:10.3390/electronics10192403.
43. Nikaein, N. *et al.* (2013) 'Application distribution model and related security attacks in VANET', *SPIE Proceedings*[Preprint]. doi:10.1117/12.2010545.
44. Zhang, T., Antunes, H. and Aggarwal, S. (2014) 'Defending connected vehicles against malware: Challenges and a solution framework', *IEEE Internet of Things Journal*, 1(1), pp. 10–21. doi:10.1109/jiot.2014.2302386.
45. Elkhail, A.A. *et al.* (2021) 'Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses', *IEEE Access*, 9, pp. 162401–162437. doi:10.1109/access.2021.3130495.
46. Prajapati, Nitesh & Grover, Jyoti & Gaur, Manoj. (2011). Implementation of Temporal Attacks in Vehicular Ad Hoc Networks. International Journal of Computer Applications. 975-8887.

47. Nguyen, J. *et al.* (2021) 'An overview of agent-based traffic simulators', *Transportation Research Interdisciplinary Perspectives*, 12, p. 100486. doi:10.1016/j.trip.2021.100486.
48. Martinez, F.J. *et al.* (2011) 'A survey and Comparative Study of simulators for vehicular ad hoc networks (VANETs)', *Wireless Communications and Mobile Computing*, 11(7), pp. 813–828. doi:10.1002/wcm.859.
49. Krajzewicz, Daniel & Erdmann, Jakob & Behrisch, Michael & Bieker-Walz, Laura. (2012). Recent Development and Applications of SUMO - Simulation of Urban MObility. International Journal On Advances in Systems and Measurements. 3&4.
50. Behrisch, Michael & Bieker-Walz, Laura & Erdmann, Jakob & Krajzewicz, Daniel. (2011). SUMO – Simulation of Urban MObility: An Overview. Proceedings of SIMUL. 2011.
51. Härri, J. *et al.* (2009) 'Vehicular mobility simulation with vanetmobisim', *SIMULATION*, 87(4), pp. 275–300. doi:10.1177/0037549709345997.
52. Varga, A. and Hornig, R. (2008) 'An overview of the omnet++ simulation environment', *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*[Preprint]. doi:10.4108/icst.simutools2008.3027.
53. Xiaodong Xian, Weiren Shi and He Huang (2008) 'Comparison of OMNET++ and other simulator for WSN Simulation', *2008 3rd IEEE Conference on Industrial Electronics and Applications* [Preprint]. doi:10.1109/iciea.2008.4582757.
54. Rampfl, S. (2013) Network Simulation and its Limitations [Preprint]. doi:10.2313/NET-2013-08-1_08.
55. Amewuda, A.B., Katsriku, F.A. and Abdulai, J.-D. (2018) 'Implementation and evaluation of WLAN 802.11ac for residential networks in NS-3', *Journal of Computer Networks and Communications*, 2018, pp. 1–10. doi:10.1155/2018/3518352.
56. Nsnam (no date) *About NS-3*, *ns*. Available at: https://www.nsnam.org/about/ (Accessed: 12 October 2023).
57. Weber, J.S., Neves, M. and Ferreto, T. (2021) 'VANET simulators: An updated review', *Journal of the Brazilian Computer Society*, 27(1). doi:10.1186/s13173-021 00113-x.
58. Shie-Yuan Wang, Chih-Liang Chou and Chun-Ming Yang (2013) 'EstiNet openflow network simulator and Emulator', *IEEE Communications Magazine*, 51(9), pp. 110 117. doi:10.1109/mcom.2013.6588659.
59. Martinez, F.J. *et al.* (2011) 'A survey and Comparative Study of simulators for vehicular *ad hoc* networks (VANETs)', *Wireless Communications and Mobile Computing*, 11(7), pp. 813–828. doi:10.1002/wcm.859.

60. *SNS A staged network simulator* (no date) *SNS: Staged Simulation in NS2*. Available at: https://www.cs.cornell.edu/people/egs/sns/ (Accessed: 12 October 2023).
61. Schoch, E. *et al.* (2008) 'Simulation of ad hoc networks: NS-2 compared to Jist/Swans', *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*[Preprint]. doi:10.4108/icst.simutools2008.3021.
62. Sommer, C. *et al.* (2019) 'Veins: The open source vehicular network simulation framework', *Recent Advances in Network Simulation*, pp. 215–252. doi:10.1007/978 3-030-12842-5_6.
63. Al-Shareeda, M.A. and Manickam, S. (2023) 'A systematic literature review on security of vehicular ad-hoc network (VANET) based on veins framework', *IEEE Access*, 11, pp. 46218–46228. doi:10.1109/access.2023.3274774.
64. Schrab, K. et al. (2023) 'Modeling an its management solution for mixed highway traffic with Eclipse Mosaic', IEEE Transactions on Intelligent Transportation Systems, 24(6), pp. 6575–6585. doi:10.1109/tits.2022.3204174.
65. Schünemann, B. (2011) 'V2X simulation runtime infrastructure vsimrti: An assessment tool to design Smart Traffic Management Systems', Computer Networks, 55(14), pp. 3189–3198. doi:10.1016/j.comnet.2011.05.005.
66. Roscher, K. et al. (no date) 'ezCar2X. Rapid-Prototyping of Communication Technologies and Cooperative ITS Applications on Real Targets and Inside Simulation Environments', ezCar2X: Rapid-Prototyping of Communication Technologies and Cooperative ITS Applications on Real Targets and Inside Simulation Environments [Preprint]. doi:10.24406/publica-fhg-385675.
67. Amoozadeh, M. et al. (2019) 'Ventos: Vehicular Network Open Simulator with hardware-in-the-loop support', Procedia Computer Science, 151, pp. 61–68. doi:10.1016/j.procs.2019.04.012.
68. Aljabry, I.A. and Al-Suhail, G.A. (2021) 'A survey on network simulators for vehicular ad-hoc networks (VANETS)', International Journal of Computer Applications, 174(11), pp. 1–9. doi:10.5120/ijca2021920979.
69. Wang, Shie-Yuan & Huang, Yu-Ming. (2012). NCTUns distributed network emulator. Internet Journal. 4.
70. Gozalvez, J. & TURKSMA, Siebe & LIN, Lan & Lazaro, Oscar & Cartolano, Fabio & Robert, Eric & Krajzewicz, Daniel & BAUZA, Ramon & Filali, Fethi & Röckl, Matthias & Leguay, Jeremie & MICHELACCI, Carlo & Vreeswijk, Jaap & MANEROS, Julen & GONZALEZ, Ainara & Lenardi, Massimiliano. (2009). iTETRIS: the Framework for Large-Scale Research on the Impact of Cooperative Wireless Vehicular Communications Systems in Traffic Efficiency.