ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

"ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δίκτυα Συνδεδεμένων Οχημάτων : Τρέχουσα Κατάσταση και Ανοιχτές Προκλήσεις

Παναγιώτης Α. Γεωργούλας

Επιβλέπων:
Δρ. Νικόλαος Πασσάς, Εργαστηριακό Διδακτικό Προσωπικό (ΕΔΙΠ)

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Δίκτυα Συνδεδεμένων Οχημάτων :
Τρέχουσα Κατάσταση και Ανοιχτές Προκλήσεις

Παναγιώτης Α. Γεωργούλας
Α.Μ.: ΙΟ1190014

Επιβλέπων:
Δρ. Νικόλαος Πασσάς, Εργαστηριακό Διδακτικό Προσωπικό (ΕΔΙΠ)

Εξεταστική Επιτροπή:
Δρ. Νικόλαος Πασσάς, (μέλος ΕΔΙΠ)
Δρ. Παντελής Μπαλαούρας, (μέλος ΕΔΙΠ)
Δρ. Σαράντης Πασκαλής, (μέλος ΕΔΙΠ)

Οκτώβριος 2022

ΠΕΡΙΛΗΨΗ

Η ολοένα αυξανόμενη παραγωγή οχημάτων σε όλο τον κόσμο και ταυτόχρονα η μεγαλύτερη ανάγκη για ασφάλεια αλλά και μείωση των εκπομπών άνθρακα που ορίζει μια σύγχρονη κοινωνία, έχουν οδηγήσει τη αυτοκινητοβιομηχανία σε νέες προκλήσεις για την δημιουργία ασφαλέστερων και φιλικότερων προς το περιβάλλον προτύπων για το σύστημα των οδικών μεταφορών. Αυτές οι προκλήσεις με την βοήθεια των ραγδαίως αναπτυσσόμενων νέων τεχνολογιών έχουν φέρει στην επιφάνεια τα λεγόμενα ασύρματα δίκτυα συνδεμένων οχημάτων και καινοτόμες υπηρεσίες όπως το Vehicle to Everything. Αυτές οι υπηρεσίες έχουν πολύ ψηλές απαιτήσεις και θέτουν αυστηρές προκλήσεις στο δίκτυο όπως η αξιοπιστία των υπηρεσιών, το latency και το mobility management καθώς μιλάμε για πολύ δυναμικά περιβάλλοντα. Η παρούσα διπλωματική εργασία εξηγεί τα ασύρματα δίκτυα συνδεδεμένων οχημάτων και αναλύει ξεχωριστά τις επικοινωνίες (ασύρματες και κυψελωτές) που χρησιμοποιούνται σε αυτά τα δίκτυα. Ακόμα εξετάζει υβριδικές μεθόδους ασύρματων και κυψελωτών τεχνολογιών για την αντιμετώπιση αρκετών ζητημάτων όπως το handover, ενώ το 5G υπόσχεται να δώσει λύσεις σε αρκετές προκλήσεις. Ακόμα γίνεται αναφορά στα δίκτυα οχημάτων αυτοματοποιημένης οδήγησης, τα αυτόνομα διασυνδεδεμένα οχήματα καθώς και στο fog computing για δίκτυα οχημάτων. Τέλος γίνεται μια εκτενής ανάλυση των απαιτήσεων - προκλήσεων ασφαλείας καθώς και πιθανών κακόβουλων επιθέσεων σε δίκτυα οχημάτων, ενώ παρουσιάζονται και τεχνικές για την διατήρηση της ιδιωτικότητας και της εμπιστευτικότητας για την διασφάλιση των επικοινωνιών.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Vehicular Ad-Hoc Networks

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: V2V, V2I, V2X, VANETs, LTE-A, 5G, DSRC, WAVE, VLC, ADVNETs, CAV, V2X SECURITY

ABSTRACT

The increasing production of vehicles around the world and at the same time the greater need for safety but also the reduction of carbon emissions defined by a modern society, has led the automotive industry to new challenges in order to create safer and more environmentally friendly standards for the road transport system. These challenges, with the help of rapidly evolving new technologies, have brought to the surface so-called wireless interconnected vehicle networks and innovative services such as Vehicle to Everything. These services have very high requirements and pose severe challenges to the network such as service reliability, latency and mobility management as we are talking about very dynamic environments. This dissertation explains the wireless networks of connected vehicles and analyzes separately the communications (wireless and cellular) used in these networks. It is also considering hybrid methods of wireless and cellular technologies to address several issues such as handover, while 5G promises to provide solutions to several challenges. Reference is also made to automated driving vehicle networks, autonomous interconnected vehicles as well as fog computing for vehicle networks. Finally, an extensive analysis is made of the requirements - security challenges as well as possible malicious attacks on vehicle networks. Techniques for maintaining privacy and confidentiality to secure communications are also presented.

SUBJECT AREA: Vehicular Ad-Hoc Networks

KEYWORDS: V2V, V2I, V2X, VANETs, LTE-A, 5G, DSRC, WAVE, VLC, ADVNETs, CAV, V2X SECURITY

Η παρούσα εργασία αφιερώνεται

στην οικογένειά μου

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της παρούσας μεταπτυχιακής διπλωματικής εργασίας, θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους όσους συνέβαλλαν για την επιτυχή ολοκλήρωσή της.

Ακόμα θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους τους καθηγητές του μεταπτυχιακού που εκτός από τις ακαδημαϊκές γνώσεις που μας προσφέρουν, μας διαμορφώνουν με το παράδειγμά τους και ως ανθρώπους. Ιδιαιτέρες ευχαριστίες θα ήθελα να εκφράσω στο επιβλέπων καθηγητή μου, κύριο Νίκο Πασσά ο οποίος εκτός από επιβλέπων αποτέλεσε και καθηγητής που με τον τρόπο διδασκαλίας του με έκανε να αγαπήσω τον κόσμο των κινητών και ασύρματων επικοινωνιών.

Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου για την συνεχή υποστήριξη που μου έδινε κατά την διάρκεια των μεταπτυχιακών μου σπουδών καθώς και τον αδερφό μου για την δύναμη που μου έδωσε σε μια πολύ δύσκολη περίοδο της ζωής του που συνέπεσε με αυτή του μεταπτυχιακού.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ 19

1 ΕΙΣΑΓΩΓΗ 21

1.1 Δίκτυα συνδεδεμένων οχημάτων 21

1.1.1 Vehicle to Vehicle (V2V) 22

1.1.2 Vehicle to Infrastructure (V2I) 23

1.1.3 Vehicle to Pedestrian (V2P) 24

1.1.4 Vehicle to Everything (V2X) 24

1.2 Οι τάσεις στις επικοινωνίες οχημάτων 25

1.2.1 Εφαρμογές ασφαλείας 26

1.2.2 Ασφάλεια σε V2V επικοινωνίες 28

1.3 Η αρχιτεκτονική του V2V 29

1.3.1 Sensors and collectors 29

1.3.2 Processor and decision-making 29

1.3.3 Storage repository 30

1.3.4 Global Positioning System (GPS) receiver 30

1.3.5 Communication radio 30

1.3.6 Driver-vehicle interface 30

1.3.7 Security 30

1.4 Η αρχιτεκτονική του V2I 31

2 VEHICULAR AD-HOC NETWORKS 32

2.1 Η αρχιτεκτονική των Vehicular ad-hoc Networks 32

2.2 Πρωτόκολλα δρομολόγησης 36

2.2.1 Unicast πρωτόκολλο δρομολόγησης 36

2.2.2 Multicast πρωτόκολλο δρομολόγησης 38

2.2.3 Broadcast πρωτόκολλο δρομολόγησης 38

2.3 Τα χαρακτηριστικά των VANETs 40

2.4 VANET εφαρμογές και οι απαιτήσεις του δικτύου τους 41

2.4.1 Εφαρμογές ασφαλείας και οι απαιτήσεις του δικτύου τους 42

2.4.2 Non-safety εφαρμογές 44

3 ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ 46

3.1 Dedicated Short-Range Communication (DSRC) 46

3.2 Wireless Access in Vehicular Environment (WAVE) 47

3.3 WiMAX 48

3.4 White-Fi 48

3.5 Visible Light Communication (VLC) 48

4 ΚΥΨΕΛΩΤΑ ΔΙΚΤΥΑ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ 50

4.1 LTE – 4G ... 50
4.1.1 Περιπτώσεις χρήσης και απαιτήσεις των υπηρεσιών για LTE - V2X ... 51
4.1.2 Τεχνικές προκλήσεις και κίνητρα για LTE - V2X ... 53
4.2 5G ... 54
4.2.1 Millimeter Wave ... 55
4.2.2 Massive MIMO ... 56
4.2.3 Software Defined Network (SDN) ... 57
4.2.4 Mobile Edge Computing (MEC) ... 58
4.2.5 Network Slicing ... 60
4.2.6 Fog Computing ... 61
5 ΕΤΕΡΟΓΕΝΗ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ ... 65
5.1 Υβριδικά DSRC-Cellular δίκτυα ... 66
5.1.1 Υβριδική αρχιτεκτονική ... 67
5.1.2 Διαχείριση της κινητικότητας ... 69
5.1.3 Στρατηγικές παράδοσης (handover) ... 69
5.1.4 Σχήματα επιλογής δικτύου ... 70
5.2 Dynamic Spectrum Sharing ... 72
6 AUTOMATED DRIVING VEHICULAR NETWORKS (ADVNETs) ... 73
6.1 Δομές επικοινωνίας ... 74
6.2 Τεχνολογίες που εφαρμόζονται στα ADVNETs ... 75
6.2.1 Infrared (IR) ... 75
6.2.2 Visible Light Communications για ADVNETs ... 76
6.3 Connected and Automated Vehicles (CAV) ... 77
7 SECURITY ΓΙΑ V2X ΕΠΙΚΟΙΝΩΝΙΕΣ ... 79
7.1 Προκλήσεις και απαιτήσεις ασφαλείας για V2X επικοινωνίες ... 79
7.2 Επιθέσεις σε V2X επικοινωνίες ... 81
7.2.1 Επιθέσεις βασισμένες στη συμπεριφορά ... 82
7.2.2 Επιθέσεις στο hardware (H/W) και το software (S/W) ... 84
7.2.3 Επιθέσεις στις υποδομές ... 84
7.2.4 Επιθέσεις στην ιδιωτικότητα ... 85
7.2.5 Επιθέσεις τροποποίησης των δεδομένων ... 86
7.3 Τεχνικές ασφαλείας για V2X επικοινωνίες ... 86
7.3.1 Κρυπτογραφία συμμετρικού κλειδιού ... 86
7.3.2 Διατήρηση της ιδιωτικότητας ... 87
7.3.3 Έλεγχος ταυτότητας ... 87
8 ΑΝΟΙΧΤΑ ΘΕΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ ... 89
8.1 Θέματα ασφαλείας ... 89
8.2 Θέματα παράδοσης και αδιάλειπτης συνδεσιμότητας ... 90
8.3 Μηχανική μάθηση για επικοινωνίες οχημάτων ... 91

8.4 MillimeterWave και μηχανική μάθηση 92
8.5 Διαχείριση μεγάλων δεδομένων 93
8.6 Vehicle-to-Grid (V2G) 93
8.7 Άλλα θέματα και προκλήσεις 94
9 ΣΥΜΠΕΡΑΣΜΑΤΑ 96
ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ 98
ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ 99
ΠΑΡΑΡΤΗΜΑ Ι 101
ΒΙΒΛΙΟΓΡΑΦΙΑ 105

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

Σχήμα 1.1 - Επικοινωνίες Vehicle to Everything. [18] 25
Σχήμα 1.2 - Αριθμός ατυχημάτων και οι συνέπειές τους ανα έτος. [68] 27
Σχήμα 1.3 - Αρχιτεκτονική εξαρτημάτων μιας OBU. [50] 29
Σχήμα 1.4 - Αρχιτεκτονική V2I. [22] 31
Σχήμα 2.1 - Η αρχιτεκτονική των επιπέδων για τα VANETs ανά περιοχή. [36] 35
Σχήμα 2.2 - Βασικές λειτουργίες κάθε τύπου επικοινωνίας σε οχήματα. [19] 36
Σχήμα 2.3 - Εφαρμογές διασυνδεδεμένων οχημάτων. 42
Σχήμα 2.4 - Τύποι Non-safety εφαρμογών. [8] 45
Σχήμα 3.1 - Κατανομή του DSRC φάσματος από το FCC. [25] 46
Σχήμα 3.2 - Multichannel λειτουργία για δίκτυα οχημάτων σύμφωνα με το Ευρωπαϊκό Πρότυπο. [25] 47
Σχήμα 4.1 - LTE Αρχιτεκτονική: δίκτυο πρόσβασης (eUTRAN) και δίκτυο κορμού (EPC). [40] 50
Σχήμα 4.2 - V2X εφαρμογές (V2V/V2P/V2I/V2N). [33] 52
Σχήμα 4.3 – Πιλοτικά σήματα (pilot signals) που αποστέλλονται σε έναν massive MIMO σταθμό βάσης. [71] 56
Σχήμα 4.4 - Μια τυπολογική αρχιτεκτονική του Software-defined για ετερογενή δίκτυα οχημάτων. [18] 58
Σχήμα 4.5 - Mobile edge computing για δίκτυα οχημάτων. [29] 59
Σχήμα 4.6 - Network slicing για επικοινωνίες οχημάτων. [29] 60
Σχήμα 4.7 - Network slicing (5G) για διάφορους τομείς και εφαρμογές, με διαφορετικές απαιτήσεις υπηρεσιών. [50] 61
Σχήμα 4.8 - Αρχιτεκτονική fog computing για δίκτυα οχημάτων. [50] 62
Σχήμα 4.9 - Αρχιτεκτονική fog network με επικοινωνίες V2V μεταξύ fog node και άλλων οχημάτων. [50] 63
Σχήμα 5.1 - Κόμβοι δικτύου σε υβριδική DSRC - cellular αρχιτεκτονική. [36] 67
Σχήμα 5.2 - Σχήμα δρομολόγησης βασισμένο σε clustering. [9] 68
Σχήμα 5.3 - Η λογική της επιλογής του δικτύου βασισμένη σε handover triggers. [36] .. 71
Σχήμα 6.1 - Εξαρτήματα ενός διασυνδεδεμένου και αυτοματοποιημένου οχήματος. [8] 77
Σχήμα 7.1 - Ταξινόμηση επιθέσεων για V2X επικοινωνίες. 82

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1.1 - Τρόποι επικοινωνίας συνδεδεμένων οχημάτων. [50].....21
Εικόνα 2.1 - Τομείς των VANETs. [19].....33
Εικόνα 2.2 - Αρχιτεκτονική C2C. [19].....34
Εικόνα 2.3 - Κατηγοριοποίηση των επικοινωνιών ενός VANET. [25].....35
Εικόνα 2.4 - Δρομολόγηση Unicast. [9] 37
Εικόνα 2.5 - Δρομολόγηση Multicast. [9] 38
Εικόνα 2.6 - Δρομολόγηση Broadcast. [9] 39
Εικόνα 2.7 - Κινητικότητα Οχημάτων. [20].....41
Εικόνα 2.8 - Εφαρμογές ασφαλείας βασισμένες σε V2V. [8] 42
Εικόνα 2.9 - Εφαρμογές ασφαλείας βασισμένες σε V2I/I2V. [8] 43
Εικόνα 2.10 - Non-safety εφαρμογές. [8] 44
Εικόνα 3.1 - Μετάδοση δεδομένων οδικής ασφάλειας με χρήση VLC. [72] 49
Εικόνα 4.1 - Τρόποι επικοινωνίας οχημάτων σε 5G περιβάλλον. [50].....54
Εικόνα 4.2 - Επικοινωνίες V2X με χρήση mmWave (πολλαπλοί mmWave πομποδέκτες αναπτύσσονται σε ένα όχημα για την ταυτόχρονη επικοινωνία V2V και V2I). [69] 55
Εικόνα 5.1 - V2X επικοινωνίες σε υβριδικό DSRC - cellular αστικό σενάριο. [36] 66
Εικόνα 6.1 - Απεικόνιση κανονικών και platoon-based ADVETs. [9] 73
Εικόνα 8.1 - OPGW αγωγός σε smart grid. [70] 94

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1.1 – Αριθμός ατυχημάτων και παθόντων για το 2019 και το 2020. [68].....27
Πίνακας 2.1 – Απαιτήσεις δικτύου για εφαρμογές που βασίζονται σε V2V. [50].....43
Πίνακας 4.1 – Παραδείγματα παραμέτρων για V2X υπηρεσίες. [39] 52
Πίνακας 5.1 – Οι κυριότερες ασύρματες τεχνολογίες για ετερογενείς επικοινωνίες οχημάτων. [40].....65

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία ασχολείται με το ευρύτερο τομέα των επικοινωνιών σε δίκτυα οχημάτων, τα λεγόμενα Vehicular ad-hoc Networks (VANETs). Το αντικείμενο της παρούσας εργασίας είναι μια εκτεταμένη και ταυτόχρονα στοχευμένη μελέτη των επικοινωνιών που χρησιμοποιούνται σε αυτά τα δίκτυα, από ασύρματες επικοινωνίες έως τα κυψελωτά δίκτυα, ο συνδυασμός αυτών, για τη λειτουργία ετερογενών δικτύων και η ασφάλεια αυτών των επικοινωνιών.

Η ερευνητική μεθοδολογία που ακολουθήθηκε για την εκπόνηση της εργασίας πραγματοποιήθηκε κυρίως σε βιβλιογραφικό αλλά και συγκριτικό επίπεδο. Αρχικά έγινε εκτεταμένη μελέτη συγγραμμάτων και δημοσιεύσεων από διεθνή επιστημονικά περιοδικά, συνέδρια, αποτελέσματα ερευνών από αξιόπιστες πηγές όπως διεθνείς οργανισμοί που καθορίζουν τα πρότυπα. Στη συνέχεια έγινε στοχευόμενη συλλογή πληροφοριών και ακολούθησε η ανάλυσή τους. Μετά την ανάλυση τα δεδομένα συγκρίθηκαν, ταξινομήθηκαν και αποτέλεσαν την δομή της παρούσας εργασίας. Τέλος διατυπώθηκαν προβληματισμοί, ανοιχτά προβλήματα, προτάσεις για μελλοντική έρευνα και συμπεράσματα.

Η δομή της εργασίας αποτελείτε από 9 κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στις επικοινωνίες των οχημάτων και δίνεται ιδιαίτερη σημασία στο να γίνουν από την αρχή ξεκάθαροι οι τρεις βασικοί πυλώνες στους οποίους γίνεται ο διαχωρισμός των επικοινωνιών σε δίκτυα οχημάτων. Αυτοί είναι το Vehicle to Vehicle (V2V), το Vehicle to Infrastructure (V2I) και το Vehicle to Pedestrian (V2P), με το σύνολο αυτών να ονομάζεται Vehicle to Everything (V2X). Στη συνέχεια γίνεται αναφορά στις τάσεις της εποχής που βρίσκονται αυτή τη στιγμή στο επίκεντρο των ερευνών για τις επικοινωνίες των οχημάτων και αυτές δεν μπορεί να είναι άλλες παρά το safety των επιβατών – οδηγών στα οχήματα και το security των επικοινωνιών καθαυτών. Ακόμα συνεχίζουμε με τις αρχιτεκτονικές απαιτήσεις που χρειάζεται να έχουν οι επικοινωνίες των οχημάτων και γίνεται στοχευμένη αναφορά στα δομικά στοιχεία που απαιτούνται για τη λειτουργία των δυο κυριότερων επικοινωνιών σε οχήματα, το V2V και το V2I. Στο επόμενο κεφάλαιο (2°) γίνεται περιγραφή και ανάλυση των VANETs με αυτό να περιλαμβάνει τις αρχιτεκτονικές του, τα χαρακτηριστικά του, τα πρωτόκολλα δρομολόγησης του, τις εφαρμογές του και τις απαιτήσεις του δικτύου που χρειάζονται σε αυτά τα δίκτυα. Τα επόμενα 3 κεφάλαια (3,4,5) συνεχίζουν με τις ασύρματες – κυψελωτές επικοινωνίες που χρησιμοποιούνται για τα οχήματα καθώς και τα ετερογενή ασύρματα δίκτυα οχημάτων. Το πρώτο από αυτά αναλύει τις τεχνολογίες DSRC, WAVE WiMAX, Wite-Fi και VLC. Το επόμενο κεφάλαιο αναλύει τις κυψελωτές τεχνολογίες LTE – 4G, 5G και πιο συγκεκριμένα το mmWave, το Massive MIMO, το SDN, το MEC, το Network Slicing και το vehicular fog computing το οποίο θα παίξει πολύ σημαντικό ρόλο στην ανάπτυξη των δικτύων με οχήματα στο μέλλον. Το τελευταίο κεφάλαιο εξ αυτών παρουσιάζει μια υβριδική DSRC – Cellular αρχιτεκτονική καθώς και στρατηγικές handover, σχήματα επιλογής δικτύου και mobility management. Στη συνέχεια στο κεφάλαιο 6 βλέπουμε τα Automate Driving Vehicular Networks (ADVNETs), τις τεχνολογίες που μπορούν να χρησιμοποιηθούν για αυτά καθώς και τα διασυνδεδεμένα

αυτόνομα οχήματα. Συνεχίζοντας στο 7^{ο} κεφάλαιο γίνεται μια εκτενής περιγραφή και ανάλυση των απαιτήσεων ασφαλείας, τις προκλήσεις καθώς και πιθανών κακόβουλων επιθέσεων σε δίκτυα οχημάτων. Ακόμα παρουσιάζονται τεχνικές για την διατήρηση της ιδιωτικότητας και της εμπιστευτικότητας για την διασφάλιση των επικοινωνιών. Τέλος στο 8^{ο} κεφάλαιο διατυπώνονται ανοιχτά προβλήματα και σκέψεις για μελλοντική έρευνα ενώ στο 9^{ο} και τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα της παρούσας εργασίας.

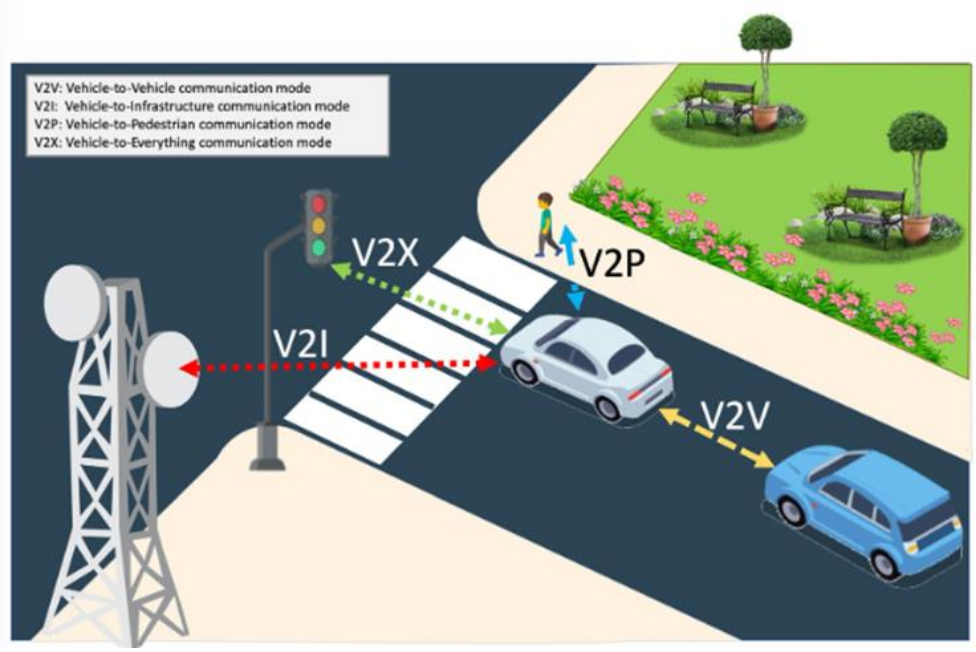
1 ΕΙΣΑΓΩΓΗ

Την τελευταία δεκαετία, ο τομέας της αυτοκινητοβιομηχανίας εξελίχθηκε δραστικά όσον αφορά τις τεχνολογίες υλικού (hardware) και λογισμικού (software) που ενσωματώθηκαν στα νέα οχήματα. Αυτή η συνεχής εξέλιξη ανοίγει νέες ευκαιρίες στην αγορά σε μια πληθώρα υπηρεσιών και εφαρμογών, οι οποίες, όταν συνδυάζονται με τις τεχνολογικές εξελίξεις σε διάφορους τομείς, καθιστούν την οδήγηση ασφαλέστερη και πιο άνετη. Η αυτοκινητοβιομηχανία έχει επενδύσει σημαντικούς πόρους (οικονομικούς και τεχνολογικούς) για την αυτοματοποίηση των οχημάτων και τη μετάβαση προς την ανάπτυξη αυτόνομων αυτοκινήτων. Οι κατασκευαστές οχημάτων όπως η Volvo αναπτύσσουν λύσεις για τη βελτίωση της ασφάλειας και της άνεσης, όπως το city safety technology που ενσωματώνει μια κάμερα και μια μονάδα GPS για την ανίχνευση της τοποθεσίας και της μετακίνηση αντικειμένων για τυχόν μελλοντικούς κινδύνους, συμβάλλοντας έτσι στη μείωση των ατυχημάτων στη Σουηδία έως και 45%.

Ωστόσο, η επιτυχία των νέων έξυπνων οχημάτων βασίζεται στην ενσωμάτωση τριών βασικών στοιχείων. Πρώτον, οι αισθητήρες του αυτοκινήτου να αλληλεπιδρούν πλήρως μεταξύ τους. Δεύτερον, συστήματα πληροφοριών που ενσωματώνουν χαρτογράφηση υψηλής ευκρίνειας με πλοήγηση υψηλής ακρίβειας, τεχνητή νοημοσύνη και ισχυρή επεξεργαστική ισχύ σημάτων. Τρίτον, μια τεχνολογία που διευκολύνει την επικοινωνία και τη συνεργασία μεταξύ των οχημάτων, γνωστή και ως δίκτυο συνδεδεμένων οχημάτων (connected vehicles network).

1.1 Δίκτυα συνδεδεμένων οχημάτων

Τα δίκτυα συνδεδεμένων οχημάτων ορίζουν διαφορετικούς τρόπους επικοινωνίας για την αυτοματοποίηση των μηνυμάτων. Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) και Vehicle-to-Everything (V2X).



Εικόνα 1.1 - Τρόποι επικοινωνίας συνδεδεμένων οχημάτων. [50]

1.1.1 Vehicle to Vehicle (V2V)

Οι V2V επικοινωνίες λειτουργούν χρησιμοποιώντας ασύρματα σήματα για την ανταλλαγή δεδομένων μεταξύ οχημάτων σχετικά με ατυχήματα, καιρικές συνθήκες καθώς και την κυκλοφορία. Η επικοινωνίες V2V θεωρούνται πιο αποτελεσματικές από τα τρέχον ενσωματωμένα συστήματα Original Equipment Manufacturer (OEM) που χρησιμοποιούν κυρίως αισθητήρες και κάμερες για να επιτρέπουν στο όχημα να βλέπει και να αναλύει τη γύρω περιοχή. Ενώ τα συστήματα αυτοματισμού είναι αρκετά πολύτιμα, οι αισθητήρες δεν είναι σε θέση να διαχειριστούν κρυμμένα αντικείμενα ή απότομες αλλαγές πορείας άλλων οχημάτων.

Οι V2V επικοινωνίες μπορούν να βοηθήσουν στη μείωση της κυκλοφοριακής συμφόρησης, να βελτιώσουν δραματικά την οδηγική εμπειρία, την ασφάλεια των επιβατών και των οδηγών. Εκτιμάται ότι οι επικοινωνίες V2V θα συνεχίσουν να αυξάνεται λόγω της εκθετικής αύξησης του αριθμού των οχημάτων στους δρόμους. Σήμερα, ο συνολικός αριθμός οχημάτων (αυτοκίνητα, φορτηγά και λεωφορεία) παγκοσμίως έχει αυξηθεί κατά πολύ, ήδη το 2016 είχαμε φτάσει τα 1,32 δισεκατομμύρια οχήματα. Ορισμένες προβλέψεις προβλέπουν ότι ο συνολικός αριθμός θα μπορούσε να φτάσει τα 2,8 δισεκατομμύρια οχήματα μέχρι το 2036. Αρκετοί παράγοντες παρακινούν την ανάπτυξη των επικοινωνιών V2V, συμπεριλαμβανομένης της αυξημένης ανησυχίας για την ασφάλεια, την ταχεία πρόοδος στις ασύρματες και κυψελωτές τεχνολογίες και την έντονη ζήτηση για καινοτομίες και τεχνολογικές βελτιώσεις.

Οι βασικοί παίκτες στην αγορά των V2V επικοινωνιών είναι οι BMW, Audi, Daimler AG, General Motors, Volvo Cars, Toyota, Volkswagen και η Delphi Automotive LLP. Η αγορά επικοινωνίας V2V είναι τμηματοποιημένη με βάση την τεχνολογία, τις συσκευές και τις εφαρμογές. Ο τομές των εφαρμογών εστιάζει σε συστήματα ελέγχου κυκλοφορίας, αποτελεσματικότητας της κυκλοφορίας, πληρωμής και άλλες εφαρμογές. Ο τομές των τεχνολογιών αξιοποιεί τις ασύρματες επικοινωνίες για την ανάπτυξη της αγοράς των V2X επικοινωνιών. Ο τελευταίος τομέας αναφέρεται σε συσκευές OEM, συσκευές μετά την πώληση ή συσκευές aftermarket και συσκευές που βασίζονται στην υποδομή. Ωστόσο, ορισμένοι από τους σημαντικότερους παράγοντες που εμποδίζουν την ανάπτυξη της αγοράς επικοινωνιών V2V είναι η έλλειψη προηγμένων προτύπων, οι ανησυχίες σχετικά με το απόρρητο των δεδομένων, η χρηματοδότηση και τα ζητήματα ασφάλειας. Για παράδειγμα, δεν είναι σαφές ποιος θα απορροφήσει το κόστος των απαιτούμενων συσκευών και την εγκατάστασή τους. Δεν είναι ακόμη σαφές εάν οι οδηγοί ή οι κρατικοί μηχανισμοί θα επιβαρυνθούν με το σχετικό κόστος.

Τα κύρια πλεονεκτήματα των V2V επικοινωνιών, περιλαμβάνουν τη βελτιωμένη οδική ασφάλεια, τη μείωση της κυκλοφοριακής συμφόρησης και την αποτελεσματική διαχείριση της ροής των οχημάτων στους δρόμους. Ωστόσο, το V2V έχει αρκετούς περιορισμούς, επειδή καθώς τα οχήματα γίνονται συστήματα εξαρτώμενα από την τεχνολογία πληροφοριών (IT), γίνονται ευάλωτα σε επιθέσεις καθώς και σε πρόσθετο κόστος που προκαλείται από την εγκατάσταση των συστημάτων V2V σε οχήματα.

1.1.2 Vehicle to Infrastructure (V2I)

Οι V2I επικοινωνίες είναι ένας από τους κύριους παράγοντες που αναμένεται να τροφοδοτήσει την ανάπτυξη του τομέα των επικοινωνιών για οχήματα και υποδομής. Η επαφή μεταξύ των οχημάτων και της οδικής υποδομής είναι μια ανταλλαγή πληροφοριών σχετικά με βασικά δεδομένα ασφάλειας και λειτουργίας. Οι V2I επικοινωνίες προσφέρουν εφαρμογές ασφαλείας που έχουν σχεδιαστεί για την αποφυγή ατυχημάτων και συγκρούσεων μεταξύ οχημάτων. Επίσης, η εισαγωγή της τεχνολογίας V2I θα βοηθήσει στην υποστήριξη της υποδομής και της ανάπτυξης οχημάτων. Η επικοινωνία μεταξύ οχημάτων και υποδομής είναι ένας νέος τρόπος για την ανάπτυξη των έξυπνων ταξιδιωτικών συστημάτων που παρέχων πληροφορίες σχετικά με την κυκλοφορία. Η επικοινωνία μεταξύ οχημάτων και υποδομής επιτρέπει την μετάδοση πληροφοριών από υπηρεσίες κοινής ωφελείας σχετικά με πληροφορίες κυκλοφορίας, οδικές πινακίδες και ατυχήματα. Επιπλέον, η σύνδεση οχημάτων με υποδομή παρέχει πολλά δεδομένα για πιθανή βελτιστοποίηση της διαδρομής του οχήματος.

Επιπλέον, οι V2I επικοινωνίες επιτρέπουν σε πολλά και διαφορετικά οχήματα να συνδεθούν με την οδική υποδομή (Road Side Unit) RSU και μέσο αυτής σε έναν σταθμό βάσης (Cellular Base Station) BS που επιτρέπει σε πολλά οχήματα να λειτουργούν στο ίδιο εύρος ζώνης. Η τεχνολογία επικοινωνίας μεταξύ οχημάτων και υποδομής επιτρέπει σε όλους τους servers να διατηρούν τα οχήματα στο δρόμο τους, να ρυθμίζουν την ταχύτητά τους και να ελέγχουν συνεχώς την τοποθεσία τους. Μέρος όλων των νέων τεχνολογιών σχετικά με την οδήγηση χωρίς οδηγό είναι το hardware και το software που χρησιμοποιούνται για την επικοινωνία του οχήματος με την υποδομή. Η ανάπτυξη της αυτόνομης οδήγησης είναι η κινητήρια δύναμη που συμβάλλει στην τεχνολογική και οικονομική ανάπτυξη στην αγορά των V2I επικοινωνιών. Οι κύριοι παράγοντες που οδηγούν στην υιοθέτηση των V2I τεχνολογιών παγκοσμίως είναι η βελτιστοποίηση της κινητικότητας των πεζών, των οχημάτων και οι μειωμένες εκπομπές λόγω καλύτερης διαχείρισης της κυκλοφορίας.

Ακόμα οι V2I επικοινωνίες αποτελούνται από προηγμένη τεχνολογία διασυνδεδεμένων οχημάτων που σε συνδυασμό με τη υποδομή μπορούν να δημιουργήσουν μια σύνδεση των οχημάτων προς ένα κέντρο ελέγχου κυκλοφορίας. Αυτό συμβάλλει σημαντικά στην ανάπτυξη της αγοράς μεταξύ οχημάτων και υποδομής. Η απουσία ωστόσο προτύπων στα κυψελωτά δίκτυα για τέτοιου είδους επικοινωνίες είναι ένας βασικός παράγοντας που εμποδίζει την ανάπτυξη της αγοράς επικοινωνιών μεταξύ οχημάτων και υποδομής. Η εφαρμογή των V2I τεχνολογιών σε αυτόνομα οχήματα θα προωθούσε την κίνηση των οχημάτων κάτω από οποιεσδήποτε καιρικές συνθήκες, κάτι που αποτελεί μια από τις τελευταίες εξελίξεις στη βιομηχανία αυτών των τεχνολογιών.

Επιπλέον, τα νέας γενιάς ασύρματα δίκτυα (5G), μπορούν να υποστηρίξουν τεχνολογίες όπως το Internet of Things, το Cloud Computing (CC) και το Edge Computing (EC). Το Internet of Things (IoT) είναι μια νέα εποχή υπολογιστών στον ψηφιακό κόσμο που σκοπεύει να δημιουργήσει έναν τεράστιο αριθμό έξυπνων συσκευών που μπορούν να υποστηρίξουν ένα ευρύ φάσμα εφαρμογών και υπηρεσιών. Αυτές οι συσκευές έχουν

περιορισμένους πόρους και οι υπηρεσίες που παρέχουν θα επιβάλλουν μοναδικά πλεονεκτήματα για την τεχνολογία V2I.

1.1.3 Vehicle to Pedestrian (V2P)

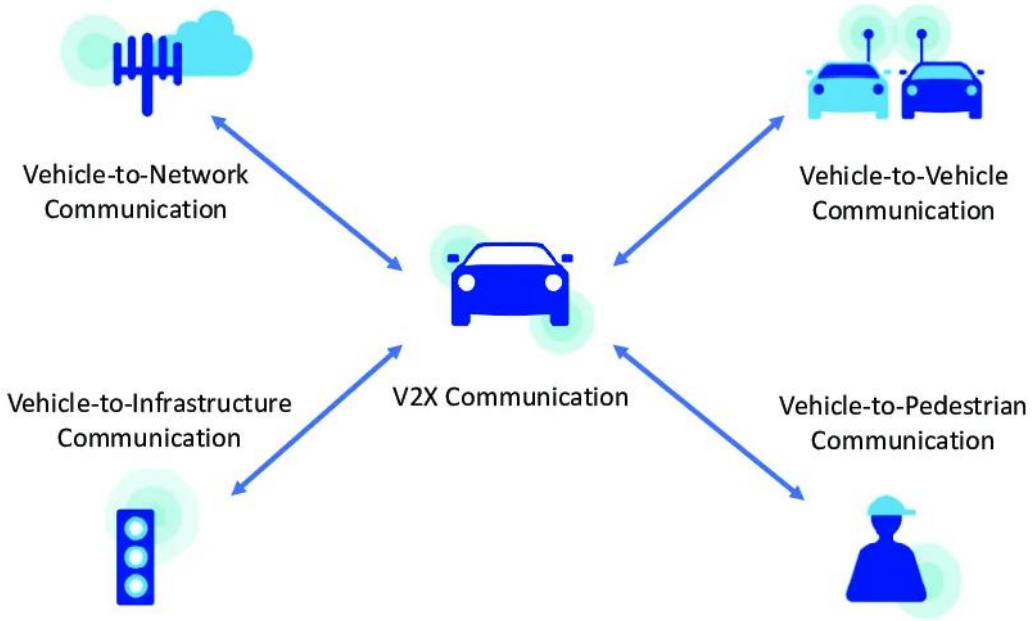
Οι V2P επικοινωνίες εστιάζουν στη δημιουργία ενός συστήματος μετάδοσης δεδομένων που ειδοποιεί τους οδηγούς για το πού βρίσκονται οι πεζοί. Το δίκτυο Vehicle to Pedestrian δημιουργεί άμεση επικοινωνία μεταξύ ενός οχήματος και του πεζού. Το πεδίο εφαρμογής του V2P μπορεί επίσης να ισχύει και για άλλους ευάλωτους χρήστες του δρόμου, όπως οι ποδηλάτες, οι επιβάτες που εισέρχονται ή εξέρχονται από τα μέσα μαζικής μεταφοράς, τα άτομα που χρησιμοποιούν αναπηρικό καροτσάκι καθώς και παιδιά σε καροτσάκι. Τα σήματα ξεκινούν να μεταδίδονται εάν κάποιος πεζός έχει εντοπιστεί κοντά στο αυτοκίνητο. Οι ειδοποιήσεις (alerts) προειδοποιούν τους οδηγούς για πεζούς που πλησιάζουν ή ειδοποιούν τους ίδιους τους πεζούς για το αυτοκίνητο. Χωρίς τις έξυπνες οδικές υποδομές (φανάρια, αισθητήρες, κάμερες), μια σταθερή σύνδεση V2P δεν μπορεί να επιτευχθεί.

Οι συνήθεις ειδοποιήσεις ή μηνύματα ασφαλείας από την οπτική γωνία των πεζών ενδέχεται να περιέχουν πλήρεις πληροφορίες για το όχημα. Ειδοποιεί τον πεζό (σε ένα smartphone) για την ταχύτητα, την τοποθεσία και την κατεύθυνση του αυτοκινήτου που πλησιάζει. Μπορεί επίσης να χρησιμοποιήσει αυτές τις πληροφορίες για τον εντοπισμό και την πρόβλεψη κατεύθυνσης ορισμένων οχημάτων σε μια δεδομένη στιγμή.

Εκτός από τη διασφάλιση της οδικής ασφάλειας, ο στόχος του V2P είναι να διευκολύνει την κινητικότητα στους δρόμους σε συνδυασμό με τις άλλες τεχνολογίες. Από τη μείωση της κυκλοφοριακής συμφόρησης μέχρι την εξάλειψη των πιθανών ατυχημάτων και συμβάντων σύγκρουσης.

1.1.4 Vehicle to Everything (V2X)

Το Vehicle to Everything (V2X) είναι ένα σύστημα επικοινωνιών όπου ένα όχημα ανταλλάσσει δεδομένα με οποιαδήποτε οντότητα που μπορεί να επηρεάσει το όχημα, όπως εξωτερικούς αισθητήρες, συσκευές και πεζούς εντός του περιβάλλοντός του, για να ενεργοποιήσει μια ποικιλία εφαρμογών ασφάλειας και ψυχαγωγίας μέσω ασύρματων επικοινωνιών. Επί της ουσίας συμπεριλαμβάνει όλες τις παραπάνω τεχνολογίες καθώς τα βασικά του στοιχεία είναι το V2V, το V2I και το V2P.



Σχήμα 1.1 - Επικοινωνίες Vehicle to Everything. [18]

Αν και η αγορά V2X βρίσκεται ακόμα στα πρώτα της στάδια, οι περισσότεροι κατασκευαστές έχουν αρχίσει να ενσωματώνουν την τεχνολογία και τα οχήματα συνδέονται όλο και περισσότερο με άλλα οχήματα και υποδομές γύρω τους. Τα οχήματα γίνονται επίσης έξυπνα και είναι εξοπλισμένα με συστήματα που απαιτούν λιγότερη ανθρώπινη συμμετοχή. Ως αποτέλεσμα, οι χρήστες επωφελούνται από ασφαλέστερα, πιο οικολογικά ταξίδια με μειωμένες εκπομπές άνθρακα, χάρη στο cruise control και τους αισθητήρες.

Ωστόσο, τα πλήρη πλεονεκτήματα των συστημάτων V2X θα απαιτήσουν χρόνο για να γίνουν αντιληπτά, επειδή, για να επικοινωνήσει ένα όχημα με μια οντότητα, αυτή η οντότητα πρέπει να είναι εξοπλισμένη με τεχνολογία V2X. Οι περισσότερες οντότητες όπως οι χώροι στάθμευσης, τα φανάρια και τα παραδοσιακά οχήματα δεν διαθέτουν συστήματα V2X, πράγμα που σημαίνει ότι δεν μπορούν να επικοινωνήσουν με τα οχήματα που ήδη χρησιμοποιούν το σύστημα.

Καθώς η αγορά V2X επεκτείνεται, τα οχήματα θα μπορούν να επικοινωνούν με άλλα οχήματα, συστήματα κυκλοφορίας και άλλους χρήστες του δρόμου, όπως οι ποδηλάτες εξοπλισμένοι με συστήματα V2X.

1.2 Οι τάσεις στις επικοινωνίες οχημάτων

Όπως αναφέραμε προηγουμένως, η επικοινωνία μεταξύ των οχημάτων είναι ένα κρίσιμο στοιχείο για τα δίκτυα οχημάτων, όπου τα οχήματα μπορούν να ανταλλάσσουν μηνύματα και πληροφορίες (όπως ταχύτητα, τοποθεσία, κατεύθυνση ταξιδιού, επιτάχυνση και ιστορικό διαδρομής) μεταξύ τους σχετικά με επικίνδυνες συνθήκες. Αυτά τα μηνύματα και οι ανταλλαγές πληροφοριών αναμένεται να βελτιώσουν την

αποτελεσματικότητα της κυκλοφορίας και την αποφυγή συγκρούσεων, γεγονός που με τη σειρά του θα βελτιώσει την οδική ασφάλεια και θα μειώσει την κυκλοφοριακή συμφόρηση.

Τα οχήματα εντός του ορίου που χρειάζεται για να επικοινωνήσουν, μπορούν να λάβουν πληροφορίες σχετικά με γεγονότα όπως ατυχήματα ή ξαφνικές στάσεις μπροστά και να στείλουν ένα σήμα στους οδηγούς που βρίσκονται εντός αυτού του εύρους, με τη μορφή ‘’alerts’’ ώστε να μπορούν να επιβραδύνουν όπως απαιτείται.

Για τις επικοινωνίες V2X, έχουν ανεπτύχθη αρκετοί αλγόριθμοι και μοντέλα για να βελτιώσουν την αποδοτικότητα των επικοινωνιών αυτών. Για παράδειγμα η σκίαση - shadowing (συμβαίνει όταν αντικείμενα εμποδίζουν τη διάδοσης μεταξύ του πομπού και του δέκτη) που προκαλείται από οχήματα, κτίρια ή άλλα αντικείμενα και μπορεί να βλάψει την απόδοση της μετάδοση, λόγω των διακυμάνσεων της ισχύος του σήματος, οδηγούν σε απώλεια μηνυμάτων. Έτσι μια μέθοδος μετάβασης – handover για τη βελτίωση της ανταλλαγής δεδομένων και της προειδοποίησης σύγκρουσης, είναι απαραίτητη. Αυτή η μέθοδος επιτρέπει και την επικοινωνία ετερογενών δικτύων κατά κύριο λόγο μεταξύ τεχνολογιών Wireless Fidelity (Wi-Fi), Dedicated Short Range Communications (DSRC) και κυψελωτών δικτύων (LTE – 5G) και φαίνεται ότι αυξάνει το εύρος επικοινωνίας σε V2V και V2I επικοινωνίες. Ωστόσο, λόγω της αύξησης του χρόνου που προκαλείται από τη μετάβαση μεταξύ των δικτύων, αυτή η μέθοδος δεν μπορεί να χρησιμοποιηθεί σε εφαρμογές που απαιτούν καθυστερήσεις επικοινωνίας μικρότερες από 200 ms.

Διάφοροι κατασκευαστές αυτοκινήτων εργάζονται σε συστήματα που επιτρέπουν την επικοινωνία μεταξύ των οχημάτων. Για παράδειγμα, η Volvo αναπτύσσει μια τεχνολογία διασύνδεσης των αυτοκινήτων της για ασφάλεια. Είναι ένα σύστημα βασισμένο σε cloud έτσι ώστε να ειδοποιεί άλλα κοντινά Volvo για ένα ατύχημα, και να βοηθήσει στην αποφυγή περαιτέρω ατυχημάτων.

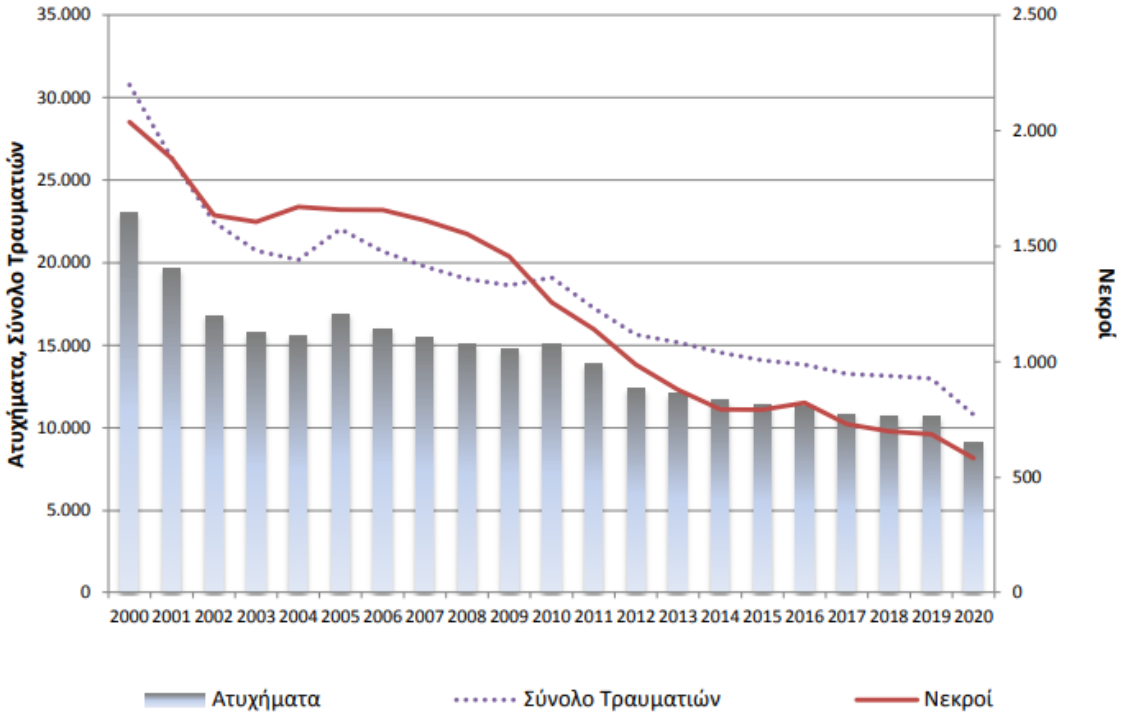
1.2.1 Εφαρμογές ασφαλείας

Σύμφωνα με τον Παγκόσμιο Οργανισμό Υγείας, περίπου 1,35 εκατομμύρια άνθρωποι πεθαίνουν κάθε χρόνο από τροχαία ατυχήματα και περίπου 50 εκατομμύρια τραυματίζονται ή μένουν ανάπηροι στον κόσμο. Μόνο στην Ελλάδα για το έτος 2019 είχαμε 10.712 τροχαία ατυχήματα ενώ για το έτος 2020 είχαμε 9.083. Περισσότεροι από 1.000 άνθρωποι πέθαναν σε τροχαία δυστυχήματα και 23.000 τραυματίστηκαν ή έμειναν ανάπηροι μόνο για τα έτη 2019-2020. Ο παρακάτω πίνακας παρουσιάζει αναλυτικά τον αριθμό των ατυχημάτων και των παθόντων στην Ελλάδα για τα έτη 2019-2020.

Πίνακας 1.1 – Αριθμός ατυχημάτων και παθόντων για το 2019 και το 2020. [68]

	2019	2020	Ετήσια Μεταβολή 2020/2019 (%)
Ατυχήματα	**10.712**	**9.083**	**-15,2**
εκ των οποίων, θανατηφόρα	656	552	-15,9
% θανατηφόρων ατυχημάτων	6,1	6,1	
Σύνολο παθόντων	**13.690**	**11.402**	**-16,7**
Νεκροί	688	584	-15,1
Σύνολο τραυματιών	13.002	10.818	-16,8
Βαριά τραυματίες	652	518	-20,6
Ελαφρά τραυματίες	12.350	10.300	-16,6

Ακόμα το παρακάτω σχήμα δείχνει τον αριθμό των τροχαίων ατυχημάτων και τις συνέπειές τους (θάνατοι και τραυματισμοί) στην Ελλάδα ανά έτος, και αναπτύχθηκε από την Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ).



Σχήμα 1.2 - Αριθμός ατυχημάτων και οι συνέπειές τους ανα έτος. [68]

Δεδομένης της ανάγκης για οδική ασφάλεια και της αύξησης του αριθμού των οχημάτων που υποστηρίζουν τεχνολογία V2X όπως οι BMW (Γερμανία), Audi (Γερμανία), Daimler (Γερμανία), General Motors (ΗΠΑ), Volvo (Σουηδία), Toyota Motor Corporation

(Ιαπωνία), Volkswagen (Γερμανία), Qualcomm (ΗΠΑ), AutoTalks (Ισραήλ) και Delphi Automotive (Ηνωμένο Βασίλειο), υπήρξε ένα αυξανόμενο ενδιαφέρον για την ανάπτυξη εφαρμογών V2X που μπορούν να βοηθήσουν στη μείωση των κινδύνων και της σοβαρότητας των τροχαίων ατυχημάτων. Αυτό οδηγεί σε βελτιωμένη ασφάλεια κατά την οδήγηση. Τέτοιες εφαρμογές περιλαμβάνουν ειδοποίηση έκτακτης ανάγκης, πέδηση έκτακτης ανάγκης, ειδοποιήσεις στο δρόμο, υποβοήθηση αλλαγής λωρίδας, προειδοποίηση στάσης και προειδοποίηση τυφλού σημείου. Η ασφάλεια είναι ένας κρίσιμος παράγοντας κατά το σχεδιασμό συστημάτων για οχήματα. Σε αυτό το πλαίσιο, αρκετές εργασίες έχουν επικεντρωθεί στον σχεδιασμό μηχανισμών και μεθόδων που βελτιώνουν την οδική ασφάλεια και συμβάλλουν στη μείωση του αριθμού των ατυχημάτων και των θανατηφόρων τροχαίων.

Ένα παράδειγμα τέτοιων εργασιών είναι δοκιμές χρησιμοποιώντας τους αισθητήρες του οχήματος και την επικοινωνία V2V για την ανίχνευση της διαμήκους και πλευρικής κίνησης του οχήματος, έτσι ώστε να διασφαλιστεί μια ασφαλής απόσταση μεταξύ των οχημάτων. Δύο σενάρια δοκιμής είναι: οδήγηση σε κυρτό δρόμο και ένας ελιγμός διπλής αλλαγής λωρίδας. Τα αποτελέσματα δείχνουν την αξιοπιστία του συστήματος στον προσδιορισμό της διαμήκους και πλευρικής κίνησης του οχήματος χρησιμοποιώντας V2V επικοινωνία και έναν ενσωματωμένο αισθητήρα millimeter wave.

1.2.2 Ασφάλεια σε V2V επικοινωνίες

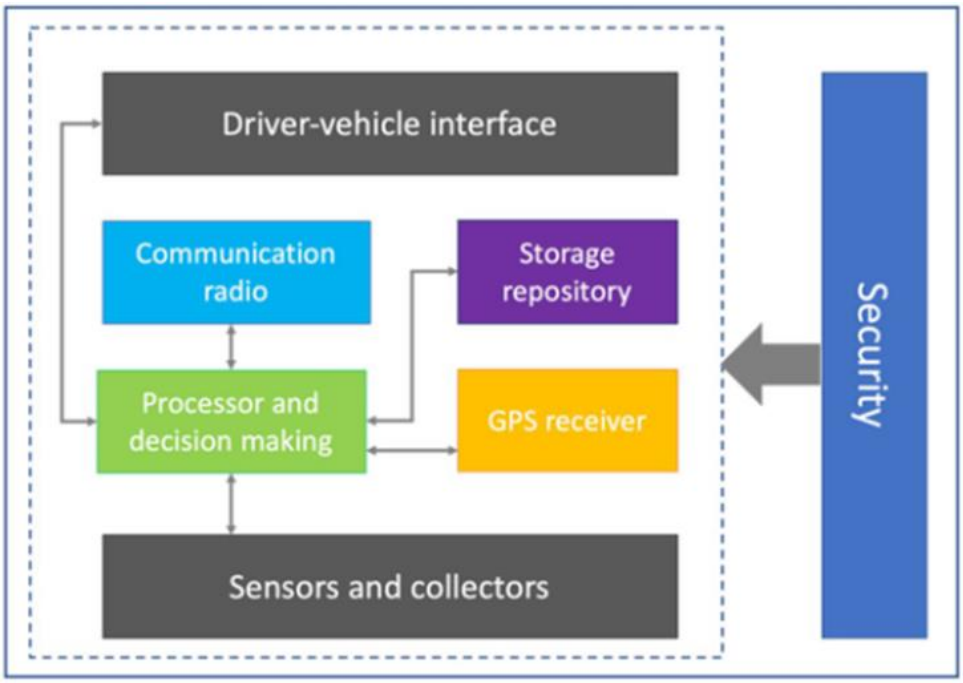
Μια σημαντική ανησυχία στο περιβάλλον V2X είναι ότι τα μηνύματα θα μπορούσαν να υποκλαπούν και να τροποποιηθούν πριν φτάσουν στον προορισμό τους ή να παρακολουθούνται οι δραστηριότητες του οδηγού, κάτι που επηρεάζει το απόρρητο του οδηγού και θέτει σε κίνδυνο την ασφάλεια του οχήματος. Σε ένα Vehicular Ad-Hoc Network – (VANET), είναι ζωτικής σημασίας η ασφάλεια των πληροφοριών επειδή είναι ένα περιβάλλον ασύρματης επικοινωνίας που είναι ανοιχτό σε διάφορους τύπους εξωτερικών απειλών. Η ανταλλαγή πληροφοριών γίνεται επίσης πιο δύσκολο να ασφαλιστεί λόγω της υψηλής κινητικότητας των οχημάτων και των ραγδαίων αλλαγών στην τοπολογία του δικτύου. Ορισμένες από τις απαιτήσεις ασφαλείας για το VANET περιλαμβάνουν τον έλεγχο ταυτότητας των χρηστών, τη διασφάλιση της ακεραιότητας των δεδομένων, την εμπιστευτικότητα, την επεκτασιμότητα, τη διατήρηση του απορρήτου και την προστασία των δεδομένων.

Ένα ασφαλές σύστημα V2X περιλαμβάνει τρία κύρια στοιχεία:

- διαπιστευτήρια ή πιστοποιητικά ασφαλείας
- έλεγχος ταυτότητας μέσω έγκυρων πιστοποιητικών
- ανταλλαγή νέων πιστοποιητικών για την ενεργοποίηση της κρυπτογραφημένης επικοινωνίας

1.3 Η αρχιτεκτονική του V2V

Το περιβάλλον V2V αποτελείται από οχήματα, το καθένα εξοπλισμένο με μια On-Board Unit (OBU). Αυτή η μονάδα μεταδίδει διαφορετικούς τύπους δεδομένων (όπως τη θέση, την ταχύτητα και την κατεύθυνση του οχήματος) και επίσης λαμβάνει παρόμοια δεδομένα από άλλα οχήματα. Το παρακάτω σχήμα απεικονίζει την εσωτερική αρχιτεκτονική από μια On-Board Unit.



Σχήμα 1.3 - Αρχιτεκτονική εξαρτημάτων μιας OBU. [50]

1.3.1 Sensors and collectors

Αυτές οι συσκευές συλλέγουν δεδομένα σχετικά με την ασφάλεια, τις πληροφορίες κυκλοφορίας και την ψυχαγωγία και συνδέονται απευθείας με τον επεξεργαστή και το στοιχείο της λήψης των αποφάσεων. Μέσα στο όχημα υπάρχουν δύο τύποι μετάδοσης δεδομένων. Ο πρώτος τύπος μετάδοσης δεδομένων είναι εντός του οχήματος, ο οποίος εστιάζει στη μετάδοση των δεδομένων από τους αισθητήρες σε μια κεντρική συσκευή μέσα στο όχημα. Ένα όχημα θα είναι εξοπλισμένα με περίπου 200 αισθητήρες κατανεμημένους μέσα σε αυτό. Ο δεύτερος τύπος μετάδοσης είναι μεταξύ οχημάτων και περιλαμβάνει ανταλλαγή δεδομένων σε πραγματικό χρόνο μεταξύ των οχημάτων. [50]

1.3.2 Processor and decision-making

Αυτός είναι ο πυρήνας του συστήματος και λαμβάνει το σύνολο των δεδομένων από διαφορετικές συσκευές, αναλύει τις πληροφορίες αυτών και φιλτράρει τα δεδομένα για να αποφύγει τη διάδοση άσχετων πληροφοριών. Στη συνέχεια, αυτές οι πληροφορίες

χρησιμοποιούνται για τη λήψη των καλύτερων αποφάσεων και τη μείωση της κυκλοφορίας στο δίκτυο. [50]

1.3.3 Storage repository

Αυτό το στοιχείο αποθηκεύει πληροφορίες σχετικά με τα προγράμματα οδήγησης και τις εφαρμογές, όπως πιστοποιητικά ασφαλείας, δεδομένα εφαρμογών και άλλες πληροφορίες. [50]

1.3.4 Global Positioning System (GPS) receiver

Αυτό το εξάρτημα παρέχει πληροφορίες όπως η τοποθεσία του οχήματος. Χρησιμοποιείται επίσης για τον συγχρονισμό της ώρας και των communication radio στις OBU κάθε οχήματος. [50]

1.3.5 Communication radio

Αυτό είναι το εξάρτημα που χρησιμοποιείται για την ανταλλαγή δεδομένων με άλλα οχήματα μέσω των κεραιών. Το συγκεκριμένο εξάρτημα πρέπει να λειτουργεί σε ετερογενές περιβάλλον επικοινωνίας, όπου πολλαπλές τεχνολογίες ασύρματης δικτύωσης συνεργάζονται μεταξύ τους για να παρέχουν την καλύτερη επιλογή επικοινωνίας με βάση διάφορες παραμέτρους όπως το επίπεδο QoS, τη συνάφεια πληροφοριών, την ασφάλεια και το απόρρητο. [50]

1.3.6 Driver-vehicle interface

Τα συστήματα επικοινωνίας V2V επικεντρώνονται σε δύο τύπους υπολογιστικών και επικοινωνιακών συστημάτων. Πρώτον, υπάρχουν συστήματα που βασίζονται σε πληροφορίες σχετικές με την οδήγηση (όπως πληροφορίες διαδρομής ή συνθήκες κυκλοφορίας) για να κάνουν την οδήγηση πιο ασφαλή και άνετη διαδικασία. Δεύτερον, υπάρχουν συστήματα που βασίζονται στον έλεγχο. Παρακολουθούν τις αλλαγές στις συνήθειες οδήγησης που μπορούν να επηρεάσουν την ρουτίνα και τις λειτουργίες (όπως διατήρηση λωρίδας κυκλοφορίας, αποφυγή σύγκρουσης και έλεγχος ταχύτητας) της οδηγικής συμπεριφοράς. Αυτή η διεπαφή είναι το στοιχείο το οποίο έρχεται σε άμεση επαφή με το οδηγό, επομένως είναι υπεύθυνο για την ειδοποίηση και την προειδοποίηση αυτού. [50]

1.3.7 Security

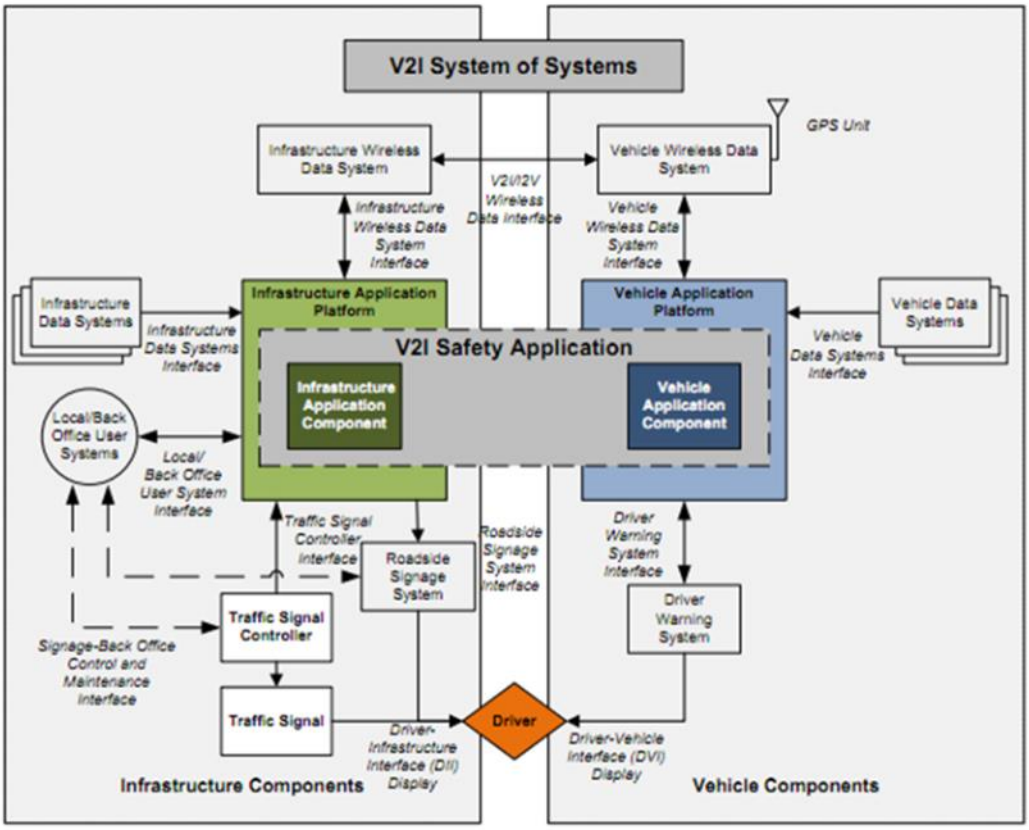
Η ασφάλεια είναι ένα κρίσιμο στοιχείο που υλοποιεί τις λειτουργίες και τους μηχανισμούς ασφαλείας που χρησιμοποιούνται από όλα τα στοιχεία του συστήματος και πρέπει να λαμβάνεται υπόψη σε επίπεδο συσκευής, δικτύου και εφαρμογής. [50]

1.4 Η αρχιτεκτονική του V2I

Η αρχιτεκτονική των V2I επικοινωνιών επικεντρώνεται σε κριτήρια απόδοσης του συστήματος. Η V2I αρχιτεκτονική βασίζεται σε δυο βασικά στοιχεία. Το πρώτο είναι τα εξαρτήματα και οι εφαρμογές της υποδομής (infastracture) και το δεύτερο είναι εξαρτήματα και οι εφαρμογές του οχήματος που βρίσκεται ενσωματωμένα σε αυτό. Αυτά τα στοιχεία συνδυάζονται και επεξεργάζονται τα δεδομένα του οχήματος και της υποδομής για να δώσουν στους οδηγούς μηνύματα και δεδομένα μέσω ασύρματης επικοινωνίας.

Στις εφαρμογές της υποδομής, ένας μηχανισμός υποστήριξης για τη μεταφορά των δεδομένων μεταξύ ετερογενών συστημάτων πρέπει να είναι διαθέσιμος. Ακόμα το Vehicle Appliance Framework παρέχει μια διεπαφή υποστήριξης για διαφορετικά συστήματα ειδοποιήσεων στο όχημα/οδηγό, σηματοδότησης και σήμανσης στον δρόμο.

Οι ειδοποιήσεις αποστέλλονται μέσω μηνυμάτων από τις εφαρμογές της υποδομής σε οχήματα που πλησιάζουν, στο τμήμα ευθύνης του κάθε RSU. Οι εφαρμογές του κάθε οχήματος αναμεταδίδουν τα μηνύματα σε μορφή ειδοποίησης (alerts) στον οδηγό για το συγκεκριμένο όχημα ή για παράπλευρα οχήματα έτσι ώστε ο οδηγός να αποφύγει τυχών συγκρούσεις. Η εφαρμογή συντονίζει την εμφάνιση των μηνυμάτων του οδηγού έτσι ώστε να είναι πιο έντονα αν ο οδηγός βρεθεί σε μια άμεση ανάγκη από ότι αν βρίσκεται σε διαδικασία αλλαγής λωρίδας κυκλοφορίας. [22]



Σχήμα 1.4 - Αρχιτεκτονική V2I. [22]

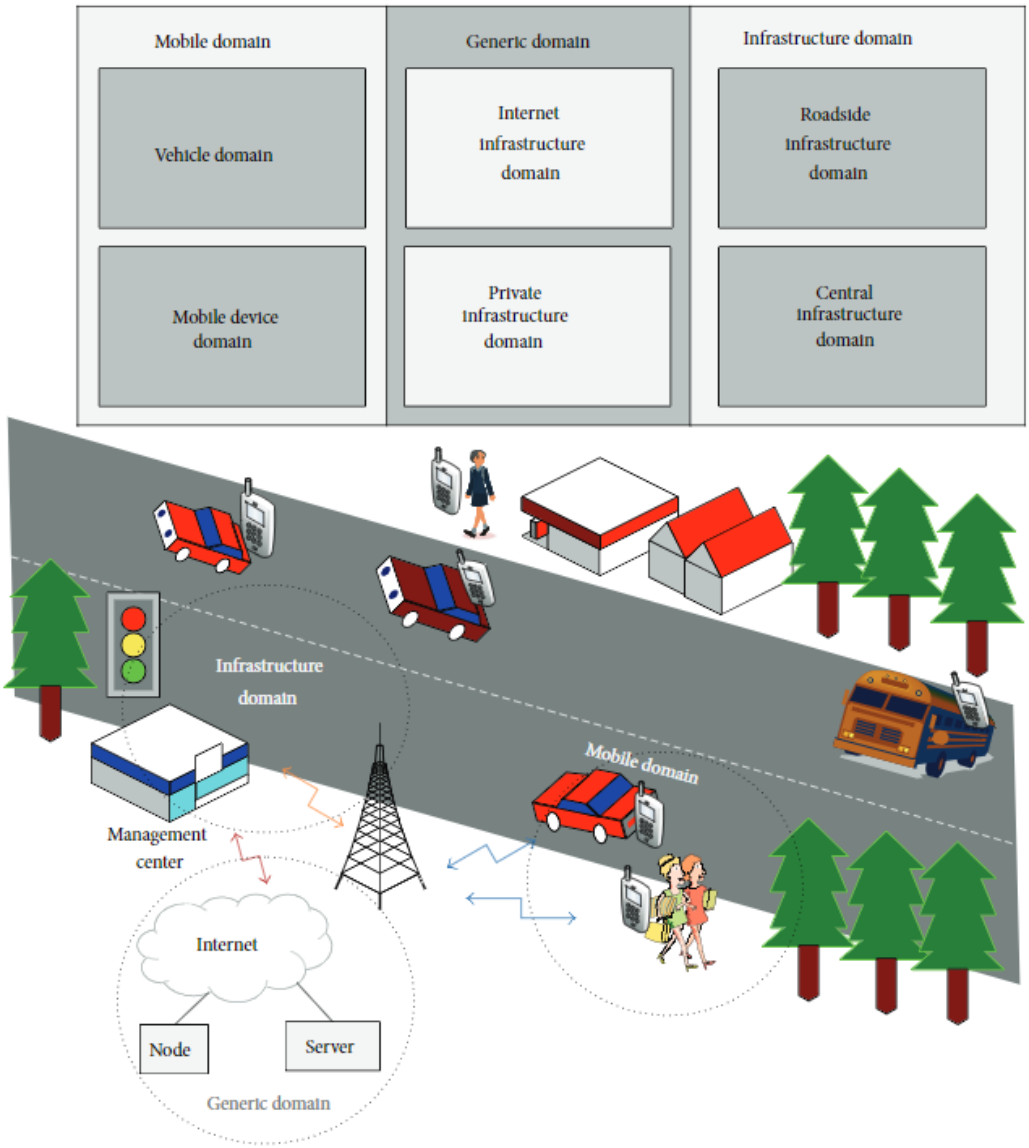
2 VEHICULAR AD-HOC NETWORKS

Πρόσφατα, με την μεγάλη άνθηση των τεχνολογιών πληροφορικής και επικοινωνιών (Information and Communication Technologies – ICT) και της ενσωμάτωσης των ασύρματων συσκευών στα σύγχρονα οχήματα μπορεί και γίνει πραγματικότητα το λεγόμενο Intelligent Transport System – ITS. Σκοπός του ITS είναι να βελτιώσει την οδική ασφάλεια και την αποτελεσματικότητα της κυκλοφορίας καθώς και να προσφέρει υπηρεσίες ενημέρωσης και ψυχαγωγίας (στο Παράρτημα Ι φαίνονται τα βασικά ITS projects για ΗΠΑ, Ιαπωνία και Ευρώπη). Η ITS τεχνολογία βασίζεται σε αυτοοργανωμένα ασύρματα δίκτυα γνωστά ως Vehicular ad-hoc Networks – VANETs. Σε αυτά τα κινητά και ασύρματα δίκτυα, τα οχήματα είναι αυτοοργανωμένα και επικοινωνούν μεταξύ τους χωρίς να απαιτείται καμία υποδομή ή κεντρική οντότητα συντονισμού. Τα οχήματα τα οποία κινούνται εντός του VANET ενδέχεται να παίζουν το ρόλο ενός σταθερού κόμβου στο δίκτυο που βασίζεται στην υποδομή. Μπορούν ακόμα να ανιχνεύουν, να συλλέγουν και να μεταδίδουν δεδομένα σε πραγματικό χρόνο σχετικά με την κυκλοφορία, τις συνθήκες οδήγησης και τους πιθανούς κινδύνους στους δρόμους. Στην πραγματικότητα, η διάδοση τέτοιων δεδομένων στο VANET θα ενίσχυε την οδική ασφάλεια και την οδηγική άνεση. Λόγω των χαρακτηριστικών των VANET, όπως η υψηλή κινητικότητα των οχημάτων, οι κατατμήσεις δικτύου και ο κατακερματισμός, οι πληροφορίες πρέπει να ανταλλάσσονται με αποτελεσματικό τρόπο για να αποφευχθεί ένα broadcasting storm.

2.1 Η αρχιτεκτονική των Vehicular ad-hoc Networks

Τα βασικά χαρακτηριστικά των VANETs μπορεί να διαφέρουν σύμφωνα με τον οργανισμό που τα τυποποιεί. Ακολουθώντας αρχικά την αμερικάνικη τυποποίηση IEEE και ISO μπορούμε να ξεχωρίσουμε τους εξής τρείς τομείς:

- *Mobile domain* - περιλαμβάνει όλους τους τύπους οχημάτων (π.χ. αυτοκίνητα, τρένα, λεωφορεία) καθώς και όλους τους τύπους φορητών συσκευών (π.χ. smartphone, laptop, smart watches).
- *Infrastructure domain* - ενσωματώνει τον τομέα της οδικής υποδομής (π.χ. φανάρια, κάμερες κ.λπ.) και τον τομέα της κεντρικής υποδομής (π.χ. Κέντρα Διαχείρισης Κυκλοφοριακής Κίνηση και Κέντρα Διαχείρισης Οχημάτων).
- *Generic domain* - περιλαμβάνει το Internet και τις Ιδιωτικές υποδομές.



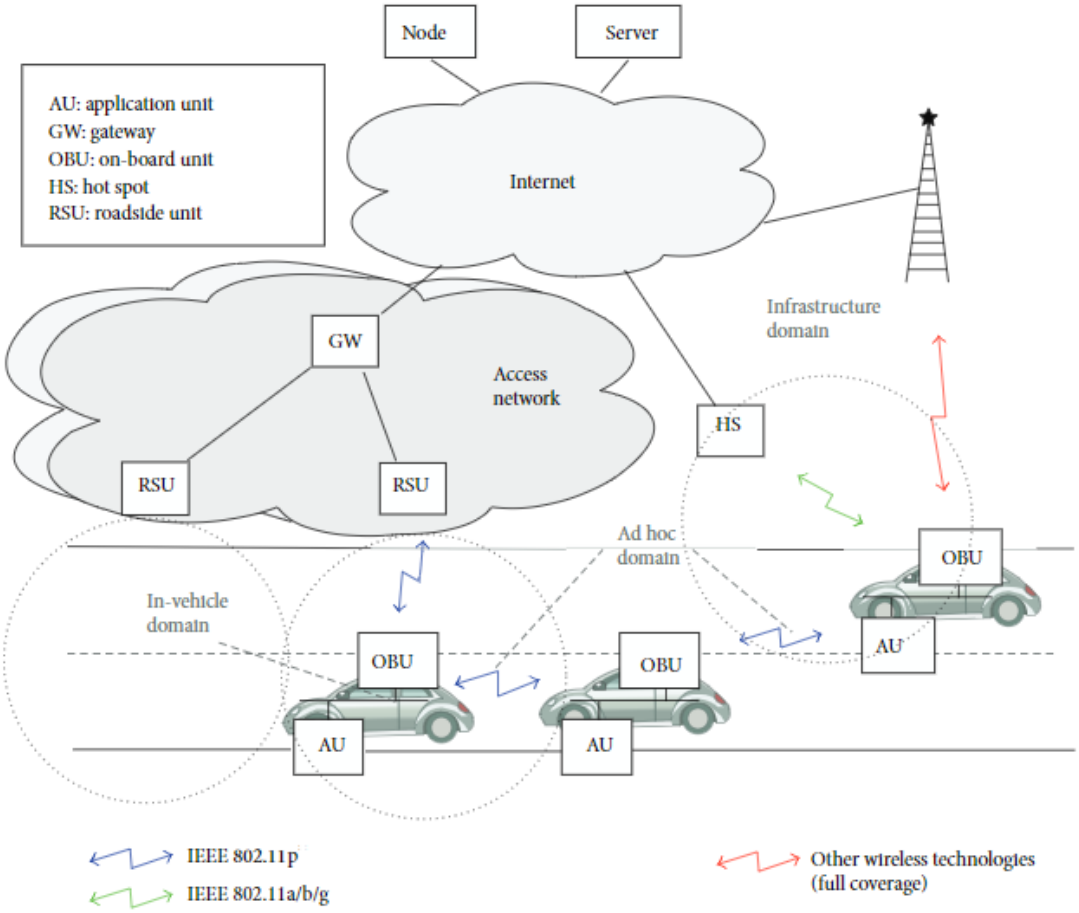
Εικόνα 2.1 - Τομείς των VANETs. [19]

Το ευρωπαϊκό πρότυπο αρχιτεκτονικής για τα VANET είναι λίγο διαφορετικό. Στην πραγματικότητα, βασίζεται στο σύστημα επικοινωνίας CAR-2-X. Όπως θα δούμε παρακάτω, η αρχιτεκτονική του συστήματος επικοινωνίας CAR-2-CAR, περιλαμβάνει τους ακόλουθους τρείς τομείς:

- *In-vehicle domain* - αποτελείται από μία ή πολλαπλά application units – AU και μία On-Board Unit - OBU. Μια AU είναι μια αποκλειστική συσκευή, η οποία μπορεί να είναι ενσωματωμένη εντός του οχήματος ή μια ξεχωριστή φορητή συσκευή όπως smartphone, φορητός υπολογιστής κ.λπ. Εκτελεί μία ή πολλές εφαρμογές που εκμεταλλεύονται τις δυνατότητες επικοινωνίας της OBU. Οι μονάδες AU και OBU συνδέονται μόνιμα μέσω ενσύρματης ή ασύρματης σύνδεσης.
- *Ad-hoc domain* - αποτελείται από οχήματα εξοπλισμένα με OBU και σταθερές μονάδες Road-Side Units - RSU που αναπτύσσονται σε συγκεκριμένες

τοποθεσίες κατά μήκος του δρόμου. Οι OBU μπορούν να επικοινωνούν μεταξύ τους και με άλλες, απευθείας ή μέσω multi-hop, χρησιμοποιώντας ασύρματες συσκευές επικοινωνίας μικρής εμβέλειας που επιτρέπουν ad-hoc επικοινωνίες μεταξύ οχημάτων. Το RSU είναι μια σταθερή συσκευή που μπορεί να συνδεθεί σε ένα δίκτυο υποδομής ή στο Διαδίκτυο. Μπορεί να στείλει, να λάβει ή να προωθήσει δεδομένα στον τομέα ad-hoc (δηλαδή, οχήματα εξοπλισμένα με OBU), γεγονός που επιτρέπει την επέκταση της κάλυψης του ad-hoc δικτύου. Μια OBU μπορεί να έχει πρόσβαση στο Διαδίκτυο μέσω μιας σύνδεσης με μια RSU, δημόσιων ή ιδιωτικών ασύρματων Hot Spots (HS) για επικοινωνία με κόμβους ή διακομιστές Διαδικτύου.

- *Infrastructure domain* - Η πρόσβαση αποτελείται από HS και RSU. Σε περίπτωση που ούτε τα RSU ούτε τα HS παρέχουν πρόσβαση στο Διαδίκτυο, οι OBU μπορούν να εκμεταλλευτούν κυψελωτά δίκτυα για παράδειγμα WiMax και 4G.

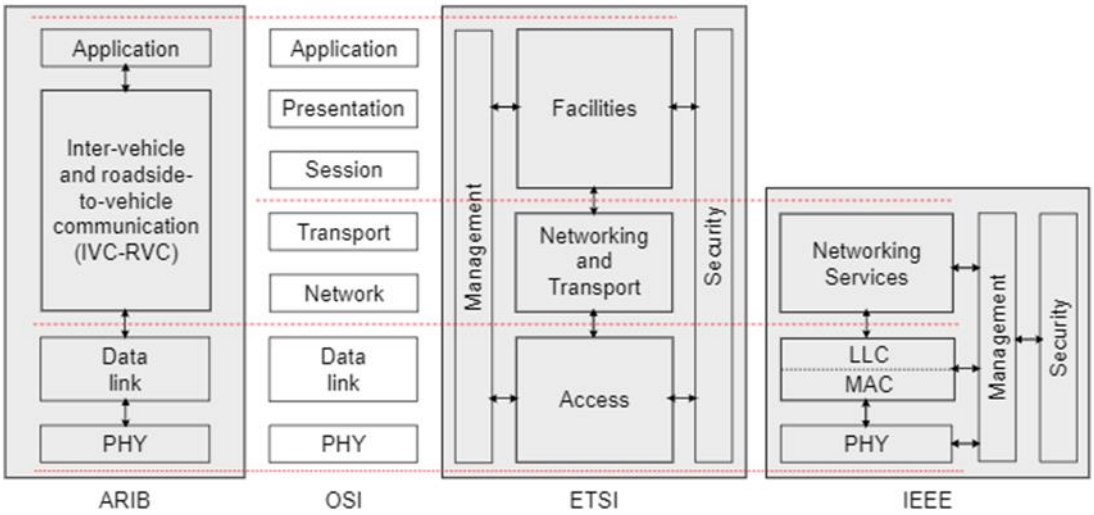


Εικόνα 2.2 - Αρχιτεκτονική C2C. [19]

Όσον αφορά την αρχιτεκτονική των στρωμάτων για τα VANET το γνωστό στους περισσότερους Open Systems Interconnection - OSI ομαδοποιεί παρόμοιες λειτουργίες επικοινωνίας σε ένα από τα επτά λογικά επίπεδα. Το επίπεδο session και το επίπεδο

presentation παραλείπονται και ένα νέο επίπεδο μπορεί να διαιρεθεί περαιτέρω σε υποστρώματα σε αυτήν την αρχιτεκτονική. [19]

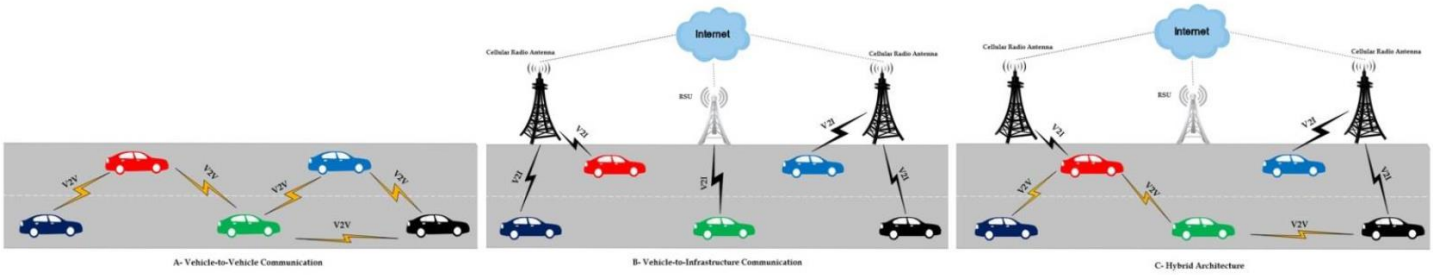
Γενικά, η αρχιτεκτονική των VANET μπορεί να διαφέρει από περιοχή σε περιοχή, και επομένως τα πρωτόκολλα και τα interfaces να είναι επίσης διαφορετικά μεταξύ τους. Παρακάτω μπορούμε να συγκρίνουμε τα layers του μοντέλου του OSI με τα IEEE (North America), ETSI (Europe), and ARIB (Japan). [36]



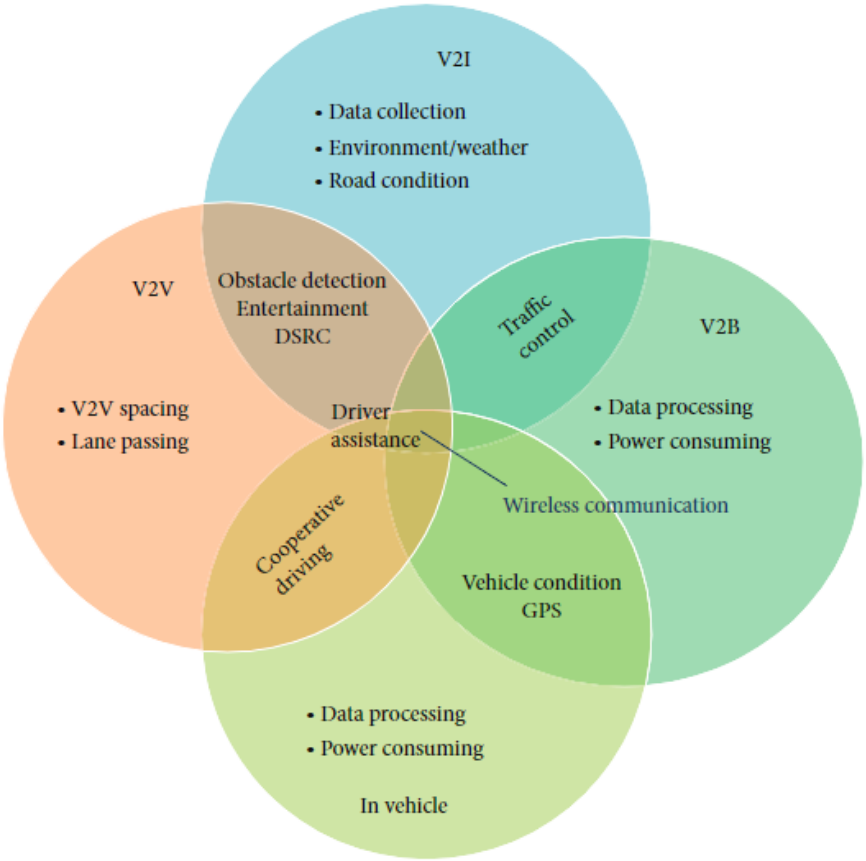
Σχήμα 2.1 - Η αρχιτεκτονική των επιπέδων για τα VANETs ανά περιοχή. [36]

Τέλος μπορούμε να κατηγοριοποιήσουμε τις επικοινωνίες ενός VANET ως εξής:

- *In-vehicle communication* - μεταξύ της OBU του οχήματος και των AU του.
- *Vehicle to vehicle* - ασύρματες επικοινωνίες μεταξύ των OBU των οχημάτων.
- *Vehicle to infrastructure* - αναφέρεται σε αμφίδρομες ασύρματες επικοινωνίες μεταξύ οχημάτων και RSU που με την σειρά του συνδέονται με την υποδομή.
- *Infrastructure to infrastructure* - επικοινωνίες μεταξύ των RSU για την επέκταση της κάλυψης του δικτύου.
- *Vehicle to broadband (cloud)* - επικοινωνίες μεταξύ οχημάτων και cloud μέσω ασύρματων ευρυζωνικών τεχνολογιών όπως το 4G/5G.



Εικόνα 2.3 - Κατηγοριοποίηση των επικοινωνιών ενός VANET. [25]



Σχήμα 2.2 - Βασικές λειτουργίες κάθε τύπου επικοινωνίας σε οχήματα. [19]

2.2 Πρωτόκολλα δρομολόγησης

Ένα πρωτόκολλο δρομολόγησης δημιουργεί μια διαδρομή – μονοπάτι μεταξύ μιας πηγής και ενός προορισμού (ή μιας ομάδας προορισμών), αποφασίζει να προωθήσει τις πληροφορίες και ενεργεί για τη διατήρηση της διαδρομής ή την ανάκτησή της από μια αποτυχία κατά την μετάδοση. Με βάση τις εφαρμοζόμενες στρατηγικές μετάδοσης στα VANETs, μπορούμε να ταξινομήσουμε τα πρωτόκολλα δρομολόγησης σε unicast, multicast και broadcast routing protocols. [9]

2.2.1 Unicast πρωτόκολλο δρομολόγησης

Αναφέρεται σε μετάδοση ένα προς ένα από μια οντότητα επικοινωνίας σε μία άλλη. Ο κύριος στόχος του unicast είναι η μετάδοση πακέτων από ένα όχημα πηγής σε ένα άλλο όχημα προορισμού μέσω ασύρματων επικοινωνιών single/multi-hop, είτε χρησιμοποιώντας έναν μηχανισμό "hop-by-hop" ή "store-and-forward". Η κύρια διαφορά μεταξύ αυτών των δύο μηχανισμών είναι εάν τα ενδιάμεσα οχήματα προωθούν τα ληφθέντα πακέτα αμέσως ή να τα κρατάνε έως ότου ένας αλγόριθμος δρομολόγησης λάβει μια απόφαση για την προώθησή τους. Τα πρωτόκολλα δρομολόγησης unicast μπορούν να εκτελεστούν με δύο τρόπους:

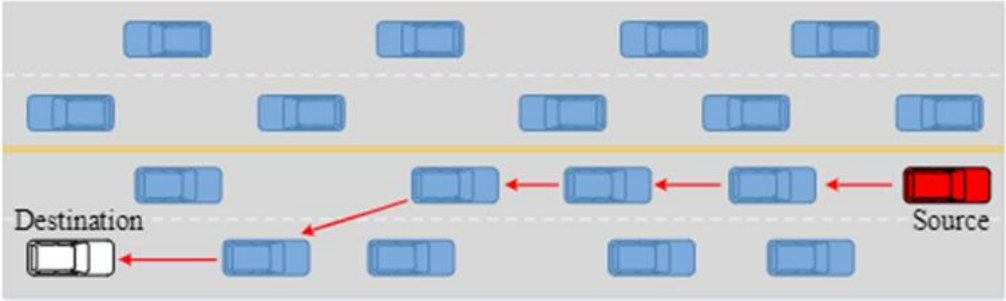
- Greedy
- Opportunistic

Στα greedy πρωτόκολλα δρομολόγησης, το όχημα που στέλνει το μήνυμα προωθεί πακέτα στους γείτονές του και στη συνέχεια τα ενδιάμεσα οχήματα προωθούν αυτά τα πακέτα στους πιο απομακρυσμένους γείτονές του έως ότου αυτά τα πακέτα παραληφθούν από το όχημα προορισμού. Δηλαδή, οι αποφάσεις προώθησης των πακέτων σχετικά με τη δρομολόγηση που βασίζεται σε greedy τεχνική λαμβάνονται με βάση τις γεωγραφικές θέσεις των οχημάτων. Τα πρωτόκολλα δρομολόγησης unicast που βασίζονται σε greedy λειτουργούν καλά σε απλά σενάρια επικοινωνίας όταν χρησιμοποιείται ο μηχανισμός "hop-by-hop", όπως για οχήματα σε δρόμους ευθείας κυκλοφορίας. Ωστόσο, για αστικές περιοχές που έχουν πολλές διασταυρώσεις, τα greedy πρωτόκολλα δρομολόγησης αποθήκευσης και προώθησης είναι πιο κατάλληλα για την υποστήριξη εφαρμογών που δεν είναι ευέλικτες ως προς τις καθυστερήσεις. Για παράδειγμα, εκμεταλλευόμενοι τη διαθεσιμότητα των πληροφοριών τις γύρω περιοχής, μπορούμε να μειώσουμε την καθυστέρηση επιλέγοντας την επόμενη μετάδοση με βάση τις πληροφορίες τοποθεσίας, την ταχύτητα, την κατεύθυνση, τη δυναμική πυκνότητα κυκλοφορίας και την απόσταση από τον προορισμό. [9]

Τα opportunistic πρωτόκολλα δρομολόγησης, υποστηρίζουν ασύρματα δίκτυα που λειτουργούν σε σενάρια με συχνές αποσυνδέσεις, όπως δίκτυα οχημάτων. Σε opportunistic πρωτόκολλα δρομολόγησης, τα πακέτα δεδομένων από την πηγή παραδίδονται στον προορισμό όπου:

- Τα ενδιάμεσα οχήματα θα πρέπει να έχουν τη δυνατότητα να αποθηκεύουν και να μεταφέρουν τα ληφθέντα πακέτα και να λειτουργούν με τρόπο «αποθήκευσης και προώθησης».
- Οι αποφάσεις προώθησης λαμβάνονται ανεξάρτητα για οχήματα σε διαφορετικές περιοχές, προκειμένου να παραδοθούν τα πακέτα με ελάχιστες ή καθόλου πληροφορίες σχετικά με την τοποθεσία του προορισμού.
- Πολλά αντίγραφα των πακέτων της πηγής μπορούν να μεταδοθούν παράλληλα για να αυξηθεί η πιθανότητα παράδοσης τουλάχιστον ενός αντιγράφου από το σύνολο των πακέτων.

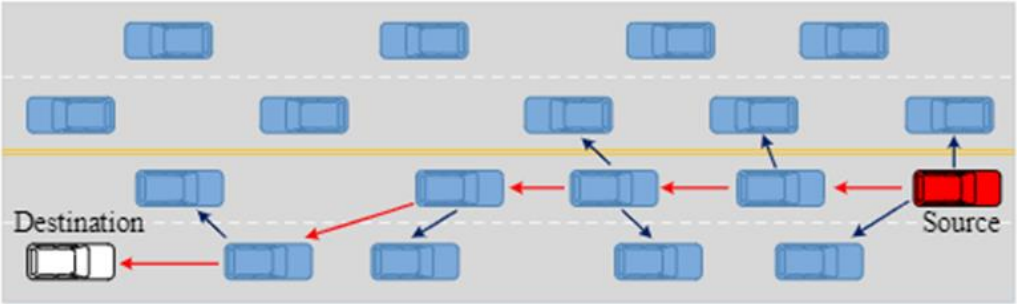
Οι κύριες προκλήσεις στο σχεδιασμό πρωτοκόλλων δρομολόγησης με unicast περιλαμβάνουν τον τρόπο μιας αποτελεσματικής κοινής χρήσης πληροφοριών, τη μείωση της καθυστέρησης, τις απώλειες των πακέτων καθώς και την αντιμετώπιση της σύγκρουσης των πακέτων κατά τη δρομολόγηση όταν υπάρχει μεγάλος αριθμός αιτημάτων. [9]



Εικόνα 2.4 - Δρομολόγηση Unicast. [9]

2.2.2 Multicast πρωτόκολλο δρομολόγησης

Είναι ένας τύπος ομαδικής επικοινωνίας one-to-many ή many-to-many όπου τα πακέτα της πηγής απευθύνονται σε μια ομάδα προορισμών ταυτόχρονα. Έχει αποδειχθεί ότι τα multicast πρωτόκολλα δρομολόγησης είναι απαραίτητα για τις αμφίδρομες επικοινωνίες μεταξύ μιας ομάδας οχημάτων σε ορισμένες καταστάσεις, όπως τυφλά σημεία, κυκλοφοριακή συμφόρηση και καταστροφές. Ένα από τα πιο κλασικά και οικεία πρωτόκολλα δρομολόγησης πολλαπλής εκπομπής είναι το geocast, το οποίο χρησιμοποιείτε για τα δίκτυα οχημάτων, όπου η ομάδα των προορισμών προσδιορίζεται με βάση της γεωγραφικής τους τοποθεσίας. Το πρωτόκολλο geocast μπορεί να βελτιωθεί λαμβάνοντας υπόψη περισσότερες και διαφορετικές πληροφορίες, όπως πληροφορίες κινητικότητας και σύνδεσης οχημάτων καθώς και κατεύθυνσης των οχημάτων. Ο κύριος στόχος είναι η αντιμετώπιση των προκλήσεων που προκαλούνται από τις αποσύνδεσης του δικτύου, την κινητικότητα και τα περιττά πακέτα, με απώτερο σκοπό να έχουμε αποτελεσματικότερα πρωτόκολλα πολλαπλής εκπομπής. Ένα άλλο σημαντικό ζήτημα στο σχεδιασμό πρωτοκόλλων δρομολόγησης πολλαπλής εκπομπής είναι η ασφάλεια, δηλαδή πρέπει να είμαστε σίγουροι ότι μόνο εξουσιοδοτημένα οχήματα μπορούν να εμπλέκονται στις σχετικές επικοινωνίες και να παρέχεται το απόρρητο των επικοινωνιών μεταξύ μιας εξουσιοδοτημένης ομάδας οχημάτων. Για την αντιμετώπιση αυτού του ζητήματος, έχουν προταθεί σχήματα διαχείρισης κλειδιών ομάδας τα οποία θα δούμε σε επόμενο κεφάλαιο. [9]



Εικόνα 2.5 - Δρομολόγηση Multicast. [9]

2.2.3 Broadcast πρωτόκολλο δρομολόγησης

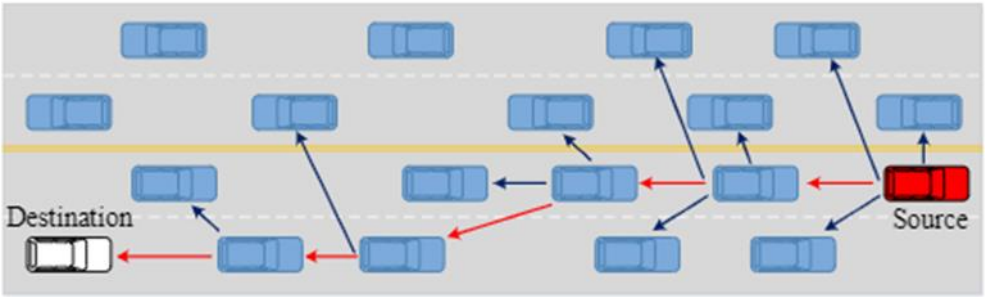
Χρησιμοποιεί μια μέθοδο επικοινωνίας one-to-all για να μεταφέρει ένα μήνυμα από μια πηγή σε πολλούς δέκτες ταυτόχρονα. Για δίκτυα οχημάτων, το broadcast είναι μια σημαντική μέθοδος δρομολόγησης, η οποία συνήθως χρησιμοποιείται για την επικοινωνία γειτονικών οχημάτων, τη διάδοση χρήσιμων πληροφοριών κυκλοφορίας σε άλλα οχήματα, την υποστήριξη εφαρμογών οδήγησης που σχετίζονται με την ασφάλεια και τη συνεργασία για τη διάδοση των παραπάνω πληροφοριών για μεθόδους unicast ή multicast. Η διαθεσιμότητα και η πρακτικότητα των broadcast μεταδόσεων σε δίκτυα οχημάτων είναι αναπόσπαστο στοιχείο για αυτά. Ωστόσο, δύο σημαντικά προβλήματα

πρέπει να ληφθούν υπόψη κατά το σχεδιασμό ενός τέτοιου πρωτοκόλλου για δίκτυα οχημάτων, ειδικά για δίκτυα οχημάτων που βασίζονται σε DSRC. Αυτά είναι το:

- καταιγίδα εκπομπής (broadcast storm)
- πρόβλημα αποσύνδεσης δικτύου (disconnected network problem)

Μια καταιγίδα εκπομπής εμφανίζεται συνήθως σε περιβάλλον επικοινωνίας με πολλά πακέτα εκπομπής δηλαδή υψηλή πυκνότητα οχημάτων. Αυτό συμβαίνει δηλαδή όταν πολλά οχήματα προσπαθούν να μεταδώσουν πακέτα ταυτόχρονα. Όταν εμφανίζεται μια καταιγίδα εκπομπής, η μετάδοση μεταξύ γειτονικών οχημάτων μπορεί να αντιμετωπίσει channel contentions και packets collisions. Υπάρχουν πολλές διάφορες τεχνικές για την αντιμετώπιση αυτού του ζητήματος σε δίκτυα οχημάτων. Ένα παράδειγμα είναι όταν ένα όχημα αναμεταδίδει τα λαμβανόμενα πακέτα εκπομπής με συγκεκριμένη πιθανότητα. Σε αυτή την τεχνική, η πιθανότητα αναμετάδοσης για κάθε όχημα εξαρτάται από την απόσταση μεταξύ αυτού και του αποστολέα, δηλ., απαιτούνται μόνο πληροφορίες GPS. Εκτός από τις πληροφορίες απόστασης, άλλες πληροφορίες έχουν επίσης χρησιμοποιηθεί για την επιλογή οχημάτων αναμετάδοσης, όπως πληροφορίες τοπολογίας και πληροφορίες χωρικής κατανομής. Επιπλέον, προηγμένες τεχνικές εφαρμόζονται στα πρόσφατα πρωτόκολλα εκπομπής, όπως η κωδικοποίηση δικτύου για τη μείωση του αριθμού των εκπομπών και επομένως τη μείωση των περιττών εκπομπών. [9]

Το πρόβλημα των αποσυνδέσεων του δικτύου είναι ένα άλλο σημαντικό πρόβλημα για κάθε τύπο δρομολόγησης στις επικοινωνίες οχημάτων. Παρόμοια με τα πρωτόκολλα δρομολόγησης unicast και multicast, η μέθοδος αποθήκευσης και προώθησης εφαρμόζεται συνήθως και στα broadcast πρωτόκολλα για την αντιμετώπιση του προβλήματος των αποσυνδέσεων του δικτύου. Για παράδειγμα, με την ενσωμάτωση της αναμετάδοσης και της αποθήκευσης - προώθησης, έχει προταθεί ένα κατανεμημένο πρωτόκολλο μετάδοσης πολλαπλών βημάτων (multihop broadcast protocol), το οποίο μπορεί να χειριστεί προβλήματα καταιγίδας αλλά και προβλήματα αποσυνδέσεων του δικτύου. Ακόμα μπορεί να λειτουργήσει σε διαφορετικά περιβάλλοντα κυκλοφορίας, συμπεριλαμβανομένων ακραίων σεναρίων με πυκνή ή αραιά κυκλοφορία οχημάτων. [9]



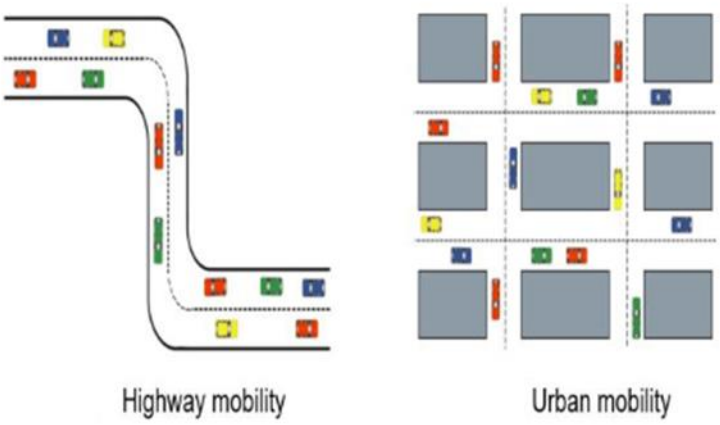
Εικόνα 2.6 - Δρομολόγηση Broadcast. [9]

2.3 Τα χαρακτηριστικά των VANETs

Τα VANETs είναι ένας ειδικός τύπος ad-hoc δικτύων που διακρίνονται από τα ακόλουθα χαρακτηριστικά: [20]

- *Mobility* - Τα VANET κατά κύριο λόγο αποτελούνται από σταθερά RSU στην άκρη του δρόμου και οχήματα τα οποία μετακινούνται διαρκώς. Οι ταχύτητες των οχημάτων μπορεί να διαφέρουν, από πολύ μεγάλες έως αρκετά χαμηλές, με αποτέλεσμα οι τεχνολογίες των επικοινωνιών σε τέτοια δίκτυα να άρχονται αντιμέτωπες με νέες προκλήσεις λόγω της δυναμικής κινητικότητας των οχημάτων. Για παράδειγμα σε περιοχές όπου επικρατεί μεγάλη κυκλοφοριακή συμφόρηση, τα οχήματα μένουν ακίνητα ή κινούνται πολύ αργά, με αποτέλεσμα να έχουν αρκετό χρόνο για την ανταλλαγή μηνυμάτων. Από την άλλη έχουν να αντιμετωπίσουν αρκετές προκλήσεις, όπως data collision, channel fading, απόρριψη μηνυμάτων και άλλα προβλήματα παρεμβολών λόγω της υψηλής πυκνότητάς τους. Ωστόσο σε περιοχές με πιο αραιή κυκλοφορία όπως αυτοκινητόδρομοι, οι ταχύτητες των οχημάτων είναι αρκετά μεγαλύτερες με αποτέλεσμα να οδηγούμαστε σε άλλες προκλήσεις ως προς τις επικοινωνίες. Κάποιες από αυτές μπορεί να είναι αστοχίες σύνδεσης, μικρό παράθυρο επικοινωνίας (μερικά δευτερόλεπτα), μεγάλη end to end καθυστέρηση κ.λπ.
- *Movement pattern* - Τα VANET δίκτυα οχημάτων διαφέρουν από αυτά των Mobile Ad-Hoc Networks (MANETs) λόγω της διαφορετικής κίνησης των κόμβων. Όσον αφορά αυτήν την κίνηση των κόμβων στα MANET γίνεται ελεύθερα και οπουδήποτε ανά πάσα στιγμή, αρκεί να βρίσκονται εντός του εύρους της κυψέλης που τους εξυπηρετεί. Από την άλλη στα VANET οι κόμβοι (οχήματα) ακολουθούν αναγκαστικά την τοπολογία των οδικών δικτύων εντός των γεωγραφικών περιοχών όπου κινούνται. Τα οχήματα σε VANET δίκτυα ακολουθούν τρείς τύπους τοπολογικών περιοχών: αστική περιοχή, αγροτική περιοχή και αυτοκινητόδρομοι. Όπως φαίνεται στην παρακάτω εικόνα οι αστικές περιοχές έχουν ένα πιο σύνθετο οδικό δίκτυο καθώς και πιο πυκνό όσον αφορά των αριθμό των οχημάτων σε σχέση με της αγροτικές περιοχές. Ακόμα τα αστικά κέντρα έχουν περισσότερα εμπόδια και φανάρια με αποτέλεσμα να χρειάζονται και περισσότερα RSU σε σχέση με τις αγροτικές περιοχές και τους αυτοκινητόδρομους. Τέλος η κίνηση των οχημάτων στους αυτοκινητόδρομους γίνεται προς μια συγκεκριμένη κατεύθυνση σε πολλαπλές λωρίδες. Έτσι από τα παραπάνω διαπιστώνουμε ότι τα τοπολογικά χαρακτηριστικά του οδικού δικτύου μεταφορών επηρεάζουν άμεσα την αποδοτικότητα και την αποτελεσματικότητα των επικοινωνιών σε δίκτυα οχημάτων.
- *Traffic density* - κυμαίνεται από πολύ υψηλή έως πολύ χαμηλή, ανάλογα με τη γεωγραφική περιοχή (δηλαδή, υψηλή κυκλοφορία στην αστική περιοχή και χαμηλή κυκλοφορία σε αγροτική περιοχή και αυτοκινητόδρομους) και τον παράγοντα χρόνο (δηλ. χαμηλή κυκλοφορία σε ώρες εκτός αιχμής και υψηλή κυκλοφορία σε ώρες αιχμής). Η πυκνότητα της κυκλοφορίας εγείρει κρίσιμες προκλήσεις που σχετίζονται με το σχεδιασμό αποτελεσματικών πρωτοκόλλων επικοινωνίας για τα VANET. Για παράδειγμα, σε αγροτικές περιοχές με πολύ χαμηλή κυκλοφορία, τα πρωτόκολλα διάδοσης δεδομένων πρέπει να

αντιμετωπίζουν το ζήτημα της αποσύνδεσης από το δίκτυο. Ωστόσο, θα πρέπει να χρησιμοποιηθούν προηγμένοι μηχανισμοί διάδοσης δεδομένων για να αποφευχθεί το γνωστό ζήτημα της καταιγίδας μετάδοσης (broadcast storm) σε περίπτωση πολύ υψηλής κυκλοφορίας, ειδικά σε αστικές περιοχές κατά τις ώρες αιχμής.

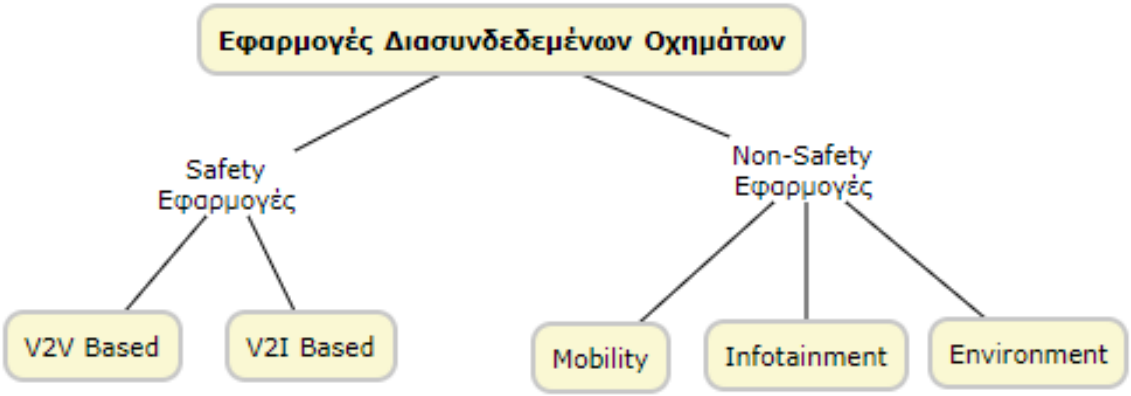


Εικόνα 2.7 - Κινητικότητα Οχημάτων. [20]

- *Heterogeneity* - Οι κόμβοι στα VANET έχουν διαφορετικά χαρακτηριστικά και δυνατότητες. Για παράδειγμα, τα οχήματα είναι κινούμενοι κόμβοι, οι οποίοι επικοινωνούν σε διαφορετικό εύρος ζώνης, έχουν διαφορικές δυνατότητες ανίχνευσης και έχουν εξ ορισμού διαφορετικές κατηγορίες όπως για παράδειγμα ιδιωτικά οχήματα, οχήματα εκτάκτου ανάγκης (αστυνομία, πυροσβεστική), οχήματα μεταφορών και συντήρησης κ.λπ.. Τα RSU από την άλλη, είναι σταθεροί κόμβοι τοποθετημένοι σε συγκεκριμένες τοποθεσίες και πλήρως εξοπλισμένοι με ad-hoc χαρακτηριστικά.

2.4 VANET εφαρμογές και οι απαιτήσεις του δικτύου τους

Βασική προϋπόθεση για αυτές τις επικοινωνίες είναι η ταχεία και αποτελεσματική ανταλλαγή σχετικών μηνυμάτων που βελτιώνουν την οδική ασφάλεια. Για να ικανοποιήσουμε αυτήν την απαίτηση, πρέπει να αντιμετωπίσουμε πολλές τεχνικές προκλήσεις, όπως η χαμηλή καθυστέρηση, ο εγγυημένος ρυθμός μετάδοσης δεδομένων και η υψηλή αξιοπιστία. Οι εφαρμογές VANET κατηγοριοποιούνται ως εφαρμογές ασφάλειας και μη. Οι non-safety εφαρμογές μπορεί να έχουν να κάνουν με την απόδοση της κυκλοφορίας, το infotainment και άλλα. Το παρακάτω σχήμα απεικονίζει την ταξινόμηση των εφαρμογών.



Σχήμα 2.3 - Εφαρμογές διασυνδεδεμένων οχημάτων.

2.4.1 Εφαρμογές ασφαλείας και οι απαιτήσεις του δικτύου τους

Παρακάτω φαίνονται κάποια σενάρια εφαρμογών ασφαλείας για V2V και V2I επικοινωνίες. Πιο συγκεκριμένα εφαρμογές που βασίζονται σε V2V επικοινωνίες μπορούμε να τις ξεχωρίσουμε από εξαιρετικά κρίσιμες εφαρμογές (όπως τα φώτα φρένων έκτακτου ανάγκης, εμπρόσθια σύγκρουση και η ανίχνευση ενδεχόμενης σύγκρουσης σε τυφλή διασταύρωση) έως άλλες που απαιτούν υψηλά επίπεδα ποιότητας υπηρεσίας (QoS) έως μη κρίσιμες εφαρμογές (όπως η υποβοήθηση στροφής προς τα αριστερά και παρκαρίσματος και η προειδοποίηση αλλαγής λωρίδας). [8]

Εικόνα 2.8 - Εφαρμογές ασφαλείας βασισμένες σε V2V. [8]

Εικόνα 2.9 - Εφαρμογές ασφαλείας βασισμένες σε V2I/I2V. [8]

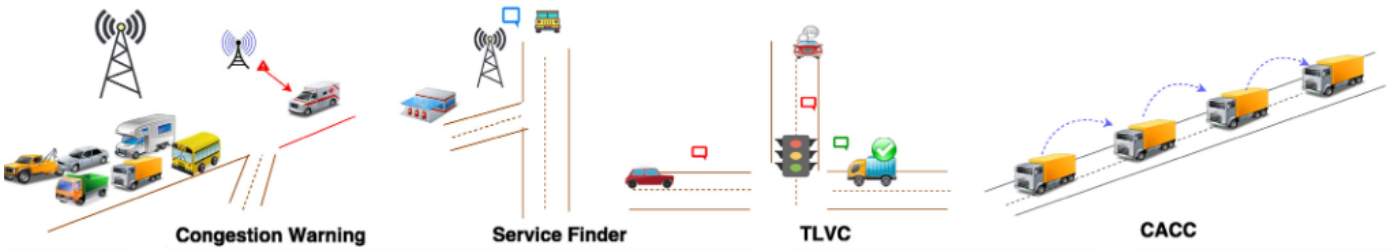
Στον παρακάτω πίνακα φαίνονται ορισμένες εφαρμογές για σενάρια V2V και οι απαιτήσεις του δικτύου τους. Όπως φαίνεται, οι απαιτήσεις καθυστέρησης είναι περίπου 100ms για τις περισσότερες εφαρμογές οδικής ασφάλειας, όταν λαμβάνουμε υπόψη ταχύτητες ταξιδιού μεγαλύτερες από 120 km/h και η περιοχή κάλυψης δεν είναι μεγαλύτερη από 300m, με ποσοστά αξιοπιστίας παράδοσης δεδομένων άνω του 99%. Τα δεδομένα σχετικά με τη θέση, την ταχύτητα, την επιτάχυνση και την κατεύθυνση ταξιδιού είναι θεμελιώδη για τις περισσότερες εφαρμογές. [50]

Πίνακας 2.1 – Απαιτήσεις δικτύου για εφαρμογές που βασίζονται σε V2V. [50]

Type	Application	Maximum latency (milliseconds)	Data transmitted	Range (meters)
Highly critical applications	Emergency brake lights	100	Position, car direction, velocity, acceleration	200
	Pre-crash sensing	20	Vehicle type, position, car direction, velocity, acceleration, yaw rate	50
	Blind intersection warning	100	Position, car direction, velocity	300
	Forward collision	100	Vehicle type, position, travel direction, velocity, acceleration, rotation angle	150
Non-critical applications	Left turn assist	100	Timing, position, direction	300
	Lane-change warning	100	Position, travel direction, velocity, acceleration, turn signal status	150
	Stop sign assist	100	Position, velocity, travel direction	300
	Roadside service finder	500	Position, velocity	300

2.4.2 Non-safety εφαρμογές

Εκτός από τις εφαρμογές ασφάλειας, τα δίκτυα οχημάτων επιτρέπουν την ενσωμάτωση πολλών άλλων υπηρεσιών που σχετίζονται με την κινητικότητα, το περιβάλλον, την ενημέρωση, την ψυχαγωγία, την κοινωνική δικτύωση οχημάτων, τη συντήρηση, τις πληρωμές κ.λπ. Συγκεντρώνουμε όλες αυτές τις υπηρεσίες στην κατηγορία των non-safety εφαρμογών. Η παρακάτω εικόνα απεικονίζει non-safety εφαρμογές. Το σενάριο αντιπροσωπεύει ένα σενάριο προειδοποίησης κυκλοφοριακής συμφόρησης με λειτουργία I2V. Το δεύτερο σενάριο είναι ένας ανιχνευτής οδικής υπηρεσίας. Για παράδειγμα, μια οδική μονάδα παρέχει πληροφορίες σε οχήματα υπό διέλευση μέσω περιοδικής μετάδοσης. Ας υποθέσουμε ότι ένα αυτοκίνητο βρίσκεται σε μια νέα τοποθεσία και χρειάζεται καύσιμα ή κάποιες επισκευές. Αυτή η εφαρμογή βοηθά τον οδηγό να βρει αυτές και τις σχετικές υπηρεσίες. Το επόμενο σενάριο απεικονίζει τη διαχείριση των σημάτων κυκλοφορίας και τη συμβουλή βέλτιστης ταχύτητας, η οποία βασίζεται στο Traffic-Light-To-Vehicle Communication (TLVC). Σε αυτή τη μέθοδο, ένας controller φωτεινών σηματοδοτών κάνει broadcast τις πληροφορίες προγραμματισμού των φαναριών σε κοντινά οχήματα με λειτουργία I2V. Οι οδηγοί αφού λάβουν αυτές τις πληροφορίες μπορούν να προσαρμόσουν την ταχύτητά τους έτσι ώστε να περάσουν το φανάρι όταν είναι πράσινο. Ολόκληρος αυτός ο μηχανισμός μπορεί να βοηθήσει στην αποφυγή απότομης ακινητοποίησης και πέδησης, στη μείωση της κατανάλωσης καυσίμου και των εκπομπών άνθρακα. Ο μηχανισμός Cooperative Adaptive Cruise Control (CACC) επιτρέπει στο όχημα να κυκλοφορούν σε platoon. Όπως φαίνεται στο τελευταίο σενάριο εάν τα οχήματα μπορούν να επικοινωνούν μεταξύ τους με λειτουργία V2V, οι οδηγοί μπορούν να ανταλλάσσουν πληροφορίες και να συνεργάζονται. Αυτή η επικοινωνία V2V μπορεί να κάνει τη συνολική κίνηση πολύ πιο ομαλή. Εάν υπάρχει ελεύθερη κίνηση στο δρόμο, η κατανάλωση καυσίμου και οι εκπομπές CO2 μπορούν να μειωθούν. Τα οχήματα κινούνται μαζί σε μια συμπαγή ομάδα (κοντά και με ασφάλεια) και αντιμετωπίζουν λιγότερη αντίσταση αέρα. [8]

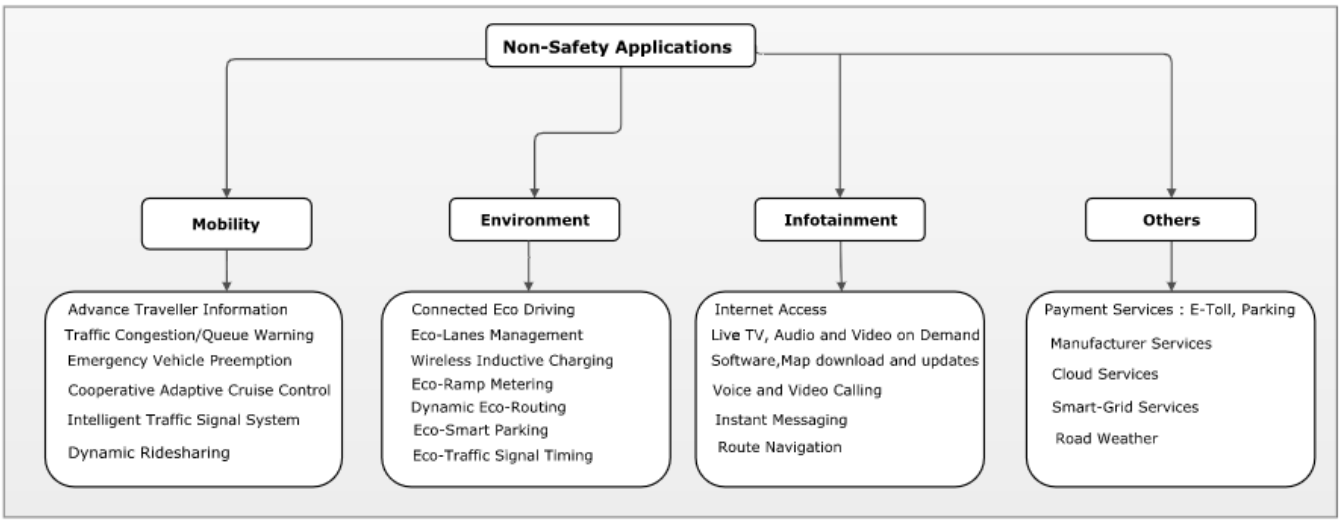


Εικόνα 2.10 - Non-safety εφαρμογές. [8]

Στις infotainment υπηρεσίες, ο οδηγός μπορεί να έχει πρόσβαση σε πολλές υπηρεσίες, όπως ήχος, βίντεο, ζωντανή τηλεόραση, ενημερώσεις λογισμικού, πλοήγηση, ανταλλαγή μηνυμάτων, κλήσεις και πολλά άλλα. Πολλές από αυτές τις εφαρμογές είναι παρόμοιες με τις εφαρμογές που χρησιμοποιούμε σε έξυπνα τηλέφωνα. Ωστόσο, το Quality of Service (QoS) και το Quality of Experience (QoE) είναι ένα ουσιαστικό ζήτημα

στην οδική επικοινωνία λόγω της υψηλής κινητικότητας και της δυναμικής τοπολογίας του δικτύου. [8]

Η επικοινωνία που απαιτείται για τις περισσότερες από τις non-safety εφαρμογές βασίζεται σε V2I ή I2V επικοινωνίες. Ωστόσο, υπάρχουν ορισμένες εφαρμογές σε αυτήν την κατηγορία, όπως το CACC που βασίζεται σε επικοινωνίες V2V. Οι εφαρμογές ασφαλείας έχουν μεγαλύτερη προτεραιότητα έναντι των non-safety εφαρμογών για πρόσβαση σε κανάλια επικοινωνίας. Διάφοροι τύποι non-safety εφαρμογών φαίνονται στο παρακάτω σχήμα. [8]



Σχήμα 2.4 - Τύποι Non-safety εφαρμογών. [8]

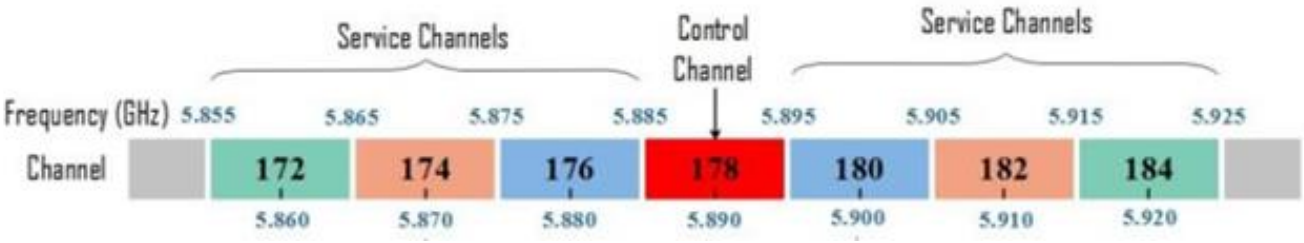
3 ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ

3.1 Dedicated Short-Range Communication (DSRC)

Το 1999, το United States Federal Communication Commission (FCC) διέθεσε 75 MHz για dedicated short-range communications (DSRC) στα 5,9 GHz μεταξύ 5.850-5.925 GHz για το ITS. Ομοίως, το 2008, το European Telecommunications Standards Institute (ETSI) διέθεσε 70 MHz φάσματος στη ζώνη των 5,8 GHz για εφαρμογές DSRC. Το DSRC ξεκίνησε το 2001 με την τυποποίηση ISO Communication Access for Land Mobiles (CALM) και ολοκληρώθηκε το 2010 με το IEEE 802.11p. Σήμερα, το DSRC χρησιμοποιείται αποκλειστικά για επικοινωνίες V2V και V2I.

Η τεχνολογία DSRC επιτρέπει την επικοινωνία υψηλής ταχύτητας μεταξύ οχημάτων και της υποδομής ή μεταξύ οχημάτων από 300m έως 1Km που είναι το εύρος επικοινωνίας της συγκεκριμένης τεχνολογίας. Επιπλέον, το σύστημα DSRC υποστηρίζει ταχύτητα οχήματος έως και 200 km/h. Αυτό το πρότυπο προσφέρει half duplex επικοινωνία και ταχύτητες μεταφοράς δεδομένων 6-27 Mbps. Επιπλέον, η FCC δεν χρεώνει για τη χρήση του φάσματος DSRC. Το DSRC υποστηρίζει την τεχνική OFDM (Orthogonal Frequency Division Multiplexing) για την πολυπλεξία των σημάτων.

Όπως φαίνεται στα σχήματα παρακάτω, το φάσμα του DSRC χωρίζεται σε επτά κανάλια ξεκινώντας από το κανάλι 172 έως το 184. Το φάσμα περιλαμβάνει μια κενή ζώνη προστασίας 5 MHz, ένα Control Channel 10 MHz (CCH) και 6 κανάλια των 10 MHz Service Channels (SCH). Το κανάλι 178 είναι το κανάλι ελέγχου (CCH), το οποίο χρησιμοποιείται αποκλειστικά για επικοινωνίες ασφαλείας. Επιπλέον, τα κανάλια 172 και 184 προορίζονται για εφαρμογές ασφαλείας και ειδική χρήση, ενώ τα άλλα κανάλια εξυπηρέτησης (SCH) έχουν χρήση για διάφορες εφαρμογές που είτε σχετίζονται με ασφάλεια είτε όχι. [25]

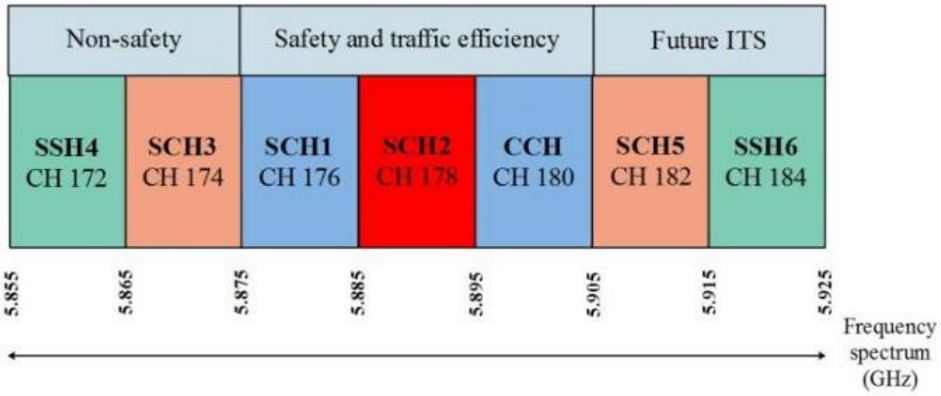


Σχήμα 3.1 - Κατανομή του DSRC φάσματος από το FCC. [25]

Σύμφωνα με το ETSI, ολόκληρο το φάσμα στο DSRC χωρίζεται σε χρονοθυρίδες των 50ms και τα μηνύματα έχουν δύο διαφορετικές προτεραιότητες:

- *Χαμηλή* - για μηνύματα δεδομένων που μεταδίδονται στα κανάλια SCH
- *Υψηλή* - για μηνύματα ασφάλειας ή ελέγχου που μεταδίδονται στο κανάλι CCH

Εάν το κανάλι CCH είναι ενεργό, όλοι οι κόμβοι είναι υποχρεωμένοι να σταματήσουν την επικοινωνία τους κατά τη διάρκεια του χρονικού πλαισίου CCH για τη λήψη και τη μετάδοση μηνυμάτων ασφαλείας στο κανάλι CCH.



Σχήμα 3.2 - Multichannel λειτουργία για δίκτυα οχημάτων σύμφωνα με το Ευρωπαϊκό Πρότυπο. [25]

3.2 Wireless Access in Vehicular Environment (WAVE)

Το Wireless Access for Vehicular Environments (WAVE) είναι επίσης γνωστό ως IEEE 802.11p WAVE. Είναι μια εγκεκριμένη τροποποίηση του προτύπου IEEE 802.11. Το WAVE απαιτείται για την υποστήριξη εφαρμογών ITS στις επικοινωνίες μικρής εμβέλειας.

Οι επικοινωνίες οχημάτων απαιτούν μεταφορά δεδομένων υψηλής ταχύτητας και γρήγορη επικοινωνία λόγω της υψηλής τοπολογικής τους αλλαγής και της υψηλής κινητικότητάς τους, με αποτέλεσμα να έχουμε μεγάλα overhead στο MAC επίπεδο. Για αυτό, η ομάδα εργασίας American Society for Testing and Materials (ASTM 2313) μετονόμασε το DSRC σε IEEE 802.11p WAVE όπου ενσωμάτωσε το φυσικό επίπεδο και το επίπεδο MAC. Το WAVE αποτελείται από τα Road Side Units (RSU) και On-Board Units (OBU). Οι ασύρματες επικοινωνίες μεταξύ OBU και RSU χρησιμοποιούν το WAVE Short Message Protocol (WSMP), το οποίο επιτρέπει την ανταλλαγή μηνυμάτων σε ένα περιβάλλον όπου απαιτούνται χαμηλές καθυστερήσεις. Το πρότυπο WAVE επιτρέπει ασύρματους ρυθμούς μετάδοσης δεδομένων από 6-27 Mbits/s για μικρές αποστάσεις έως 1 Km με καθυστέρηση 50–100 ms.

Στο WAVE, οι V2V και V2I επικοινωνίες χρησιμοποιούν το εύρος συχνοτήτων από 5.850-5.925 GHz και παρέχει στατιστικά στοιχεία για την κυκλοφορία σε πραγματικό χρόνο έτσι ώστε να βελτιώσει την απόδοση των VANETs. Το WAVE χρησιμοποιεί OFDM τεχνική για να χωρίσει τα σήματα σε narrow band κανάλια. Το WAVE είναι βασικό μέρος του DSRC. Ωστόσο, και οι δυο όροι χρησιμοποιούνται συνήθως αυθαίρετα. Σε ορισμένες περιπτώσεις, ο όρος DSRC χρησιμοποιείται ως γενικότερος όρος σε σύγκριση με το WAVE.

3.3 WiMAX

Η τεχνολογία WiMAX προτάθηκε για την υποστήριξη υψηλής ταχύτητας επικοινωνίας V2I δεδομένου ότι η απόδοση του 802.11p μπορεί να παρεμποδιστεί από συνθήκες μη οπτικής επαφής. Η έκδοση WiMAX IEEE 802.16m μπορεί να υποστηρίξει κινητικότητα έως και 350 km/h με αναμενόμενη καθυστέρηση παράδοσης μικρότερη από 30ms.

3.4 White-Fi

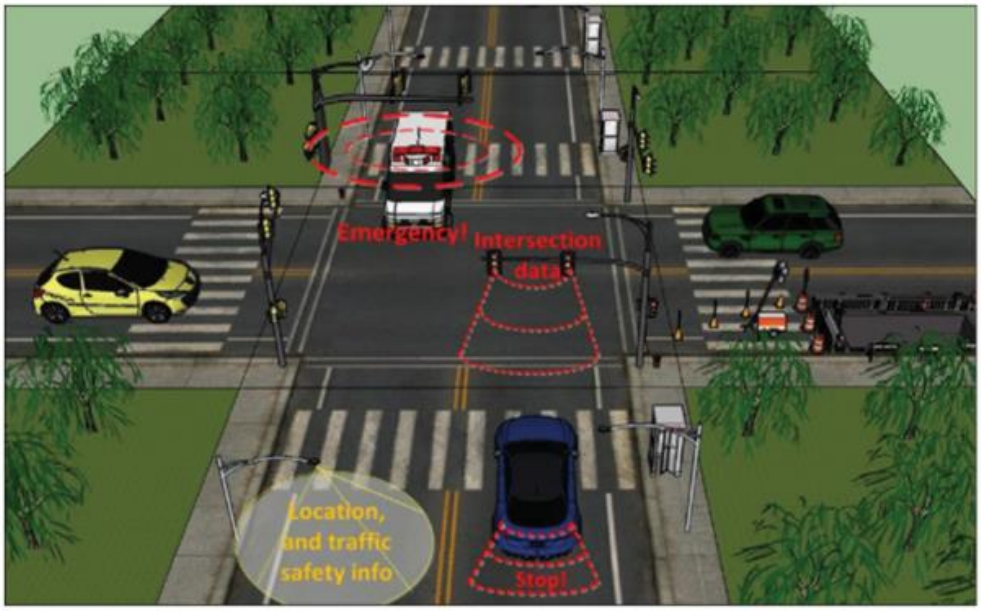
Είναι ένας όρος που επινοήθηκε από την FCC των Ηνωμένων Πολιτειών για να περιγράψει τις επικοινωνίες που επιτρέπουν στους μη αδειοδοτημένους χρήστες να έχουν πρόσβαση στο φάσμα της τηλεόρασης στις ζώνες VHF/UHF μεταξύ 54 και 790 MHz. Η πρόοδος της τεχνολογίας White-Fi έχει πυροδοτήσει πολλές νέες έρευνες σχετικά με τα δίκτυα οχημάτων, για την εξερεύνηση του μη αδειοδοτημένου φάσματος για να λυθεί το ζήτημα της σπανιότητας αυτού στα δίκτυα οχημάτων. Τα δίκτυα οχημάτων με δυνατότητα White-Fi μπορούν να βελτιώσουν την ικανότητα διάδοσης εκφορτώνοντας ένα τμήμα της κίνησης δεδομένων από τη ζώνη του DSRC ή τη ζώνη της κινητής τηλεφωνίας στη μπάντα της τηλεόρασης. Ακόμα, σε αντίθεση με την μπάντα των 2,4 GHz που χρησιμοποιείται από το Wi-Fi, το φάσμα της τηλεόρασης βρίσκεται σε χαμηλότερο εύρος συχνοτήτων και επιτρέπει στο σήμα να διεισδύει καλύτερα στους τοίχους και να ταξιδεύει μακρύτερα από το εύρος υψηλότερης συχνότητας. Έτσι, η τεχνολογία White-Fi μπορεί να παρέχει επικοινωνίες σχετικά μεγάλης εμβέλειας για τη βελτίωση της απόδοσης της μετάδοσης. Για παράδειγμα, η χρήση του White-Fi για διάδοση σε μεγάλες αποστάσεις με σκοπό την αποφυγή της μετάδοσης πολλαπλών πηδημάτων (multi-hop) μπορεί να μειώσει την καθυστέρηση μετάδοσης ορισμένων πληροφοριών που σχετίζονται με την ασφάλεια. Ωστόσο, οι επικοινωνίες οχημάτων με δυνατότητα White-Fi δημιουργούν πιθανές παρεμβολές στους χρήστες της τηλεόρασης, οι οποίες ενδέχεται να φέρουν περαιτέρω προκλήσεις για την προστασία των υπηρεσιών αυτής. Τέλος, λόγω του μη αδειοδοτημένου χαρακτηριστικού αυτής της μπάντας, επιτρέπεται η συνύπαρξη δικτύων οχημάτων και άλλων υφιστάμενων ασύρματων δικτύων. Έτσι οι χρήστες οχημάτων ενδέχεται να αντιμετωπίσουν παρεμβολές που προκαλούνται από άλλα δίκτυα και επομένως, να επηρεάσουν την ποιότητα των υπηρεσιών ορισμένων εφαρμογών σε οχήματα.

3.5 Visible Light Communication (VLC)

Το VLC επιτρέπει τη μετάδοση δεδομένων σε υψηλού ρυθμούς ταυτόχρονα με το φως. Στην πραγματικότητα, αρκεί η γρήγορη ενεργοποίηση και απενεργοποίηση της διόδου εκπομπής φωτός LED για τη μετάδοση ενός αόρατου σήματος στο ανθρώπινο μάτι και απολύτως ασφαλές για το ανθρώπινο σώμα, εκμεταλλευόμενο το ευρύ και ελεύθερο οπτικό φάσμα. Το VLC επομένως είναι κατάλληλο για μετάδοση μηνυμάτων. Τα οχήματα είναι ήδη εξοπλισμένα με φώτα LED που θα μπορούσαν εύκολα να χρησιμοποιηθούν για επικοινωνίες V2V χωρίς παρεμβολές από ηλεκτρομαγνητικές συσκευές και μικρότερες παρεμβολές από τους γείτονες χάρη στις περιορισμένες

δυνατότητες που έχει το φως στο να διαπερνά αντικείμενα. Εκτός από αυτά τα πλεονεκτήματα, πρέπει να σημειωθεί ότι το VLC είναι ευαίσθητο στο φως του περιβάλλοντος και στις καιρικές συνθήκες, καλύπτει περιορισμένες αποστάσεις και δεν διασχίζει εμπόδια.

Αυτό το είδος επικοινωνιών περιγράφεται από το πρότυπο IEEE 802.15.7, το οποίο ορίζει τα PHY και MAC επίπεδα για το φάσμα του ορατού φωτός και υποστηρίζει υπηρεσίες ήχου και εικόνας σε ορατές συνδέσεις. Στο φυσικό επίπεδο, οι διαθέσιμοι τρόποι λειτουργίας διαφέρουν ως προς τη διαμόρφωση και την κωδικοποίηση, επιτρέποντας ρυθμό μετάδοσης δεδομένων από 11,67 έως 96 Mb/s. Στο επίπεδο MAC, το πρότυπο IEEE 802.15.7 προβλέπει τη χρήση CSMA/CA. Κάθε κόμβος εκπέμπει μόνο εάν ο άλλος ανιχνεύεται ως αδρανές μετά από ένα τυχαίο χρονικό διάστημα και το μήνυμα θεωρείται ότι ελήφθη σωστά μόνο με τη λήψη της επιβεβαίωσης στον πομπό. Μια αναθεώρηση του προτύπου, ονομάζεται IEEE 802.15.7r1 και προβλέπει την καλύτερη αντιμετώπιση των επικοινωνιών στα οχήματα με χρήση VLC. Σε αυτή την περίπτωση, το πρότυπο λαμβάνει υπόψη τις απαιτήσεις των οχημάτων και στοχεύει να βελτιώσει την κινητικότητα, τους ρυθμούς μετάδοσης δεδομένων και τα πρωτόκολλα δικτύου.

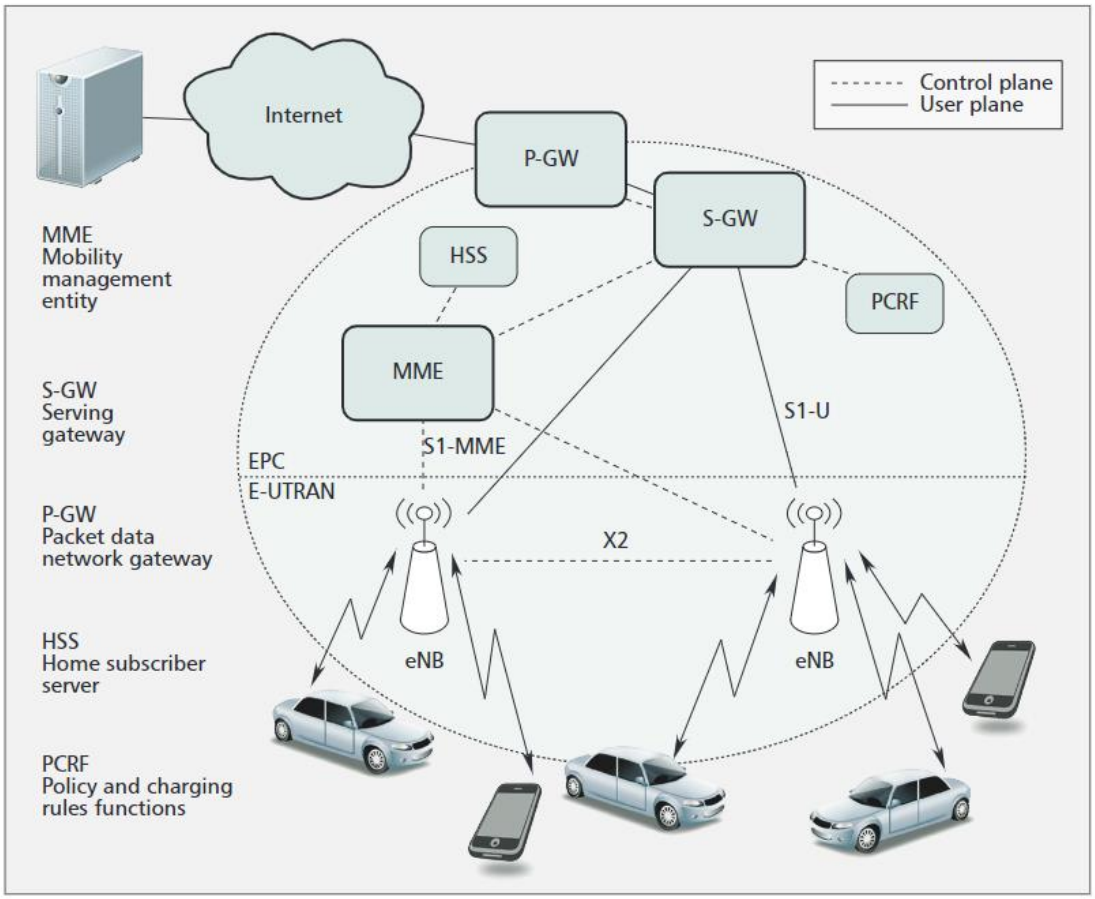


Εικόνα 3.1 - Μετάδοση δεδομένων οδικής ασφάλειας με χρήση VLC. [72]

4 ΚΥΨΕΛΩΤΑ ΔΙΚΤΥΑ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ

4.1 LTE – 4G

Το LTE αντιπροσωπεύει μια γενιά δικτύων κινητής τηλεφωνίας που ορίζονται από το Third Generation Partnership Project (3GPP). Το σύστημα LTE χαρακτηρίζεται από μια αρχιτεκτονική all IP. Οι μετάδοση των δεδομένων βασισμένη σε IP επιτρέπει μεγαλύτερη ανάπτυξη και επέκταση του δικτύου σε σχέση με τα προηγούμενα κυψελωτά δίκτυα. Χάρη στην απλοποιημένη αρχιτεκτονική του, το LTE μπορεί να παρέχει round-trip χρόνους μικρότερους των 10 ms και latency μικρότερο των 100 ms. Αυτό είναι ιδιαίτερα ωφέλιμο για εφαρμογές οχημάτων που είναι ευαίσθητες στις καθυστέρηση. Το δίκτυο πρόσβασης αποτελείται από eNodeB, τα οποία διαχειρίζονται radio resources και handovers ενώ το δίκτυο κορμού αποτελείται από τρεις κύριες μονάδες. Πρώτο το mobility management entity (MME), υπεύθυνο για διαδικασίες ελέγχου, όπως ο έλεγχος ταυτότητας (authentication), ασφάλειας (security), αποθήκευσης των χρηστών και πληροφοριών θέσης. Δεύτερο το S-GW, υπεύθυνο για τη δρομολόγηση, την προώθηση δεδομένων και της χρέωσης μέσω του policy and charging rules function (PCRF). Τέλος το P-GW, είναι η οντότητα που επιτρέπει την επικοινωνία μεταξύ IP και circuit-switched δικτύων.



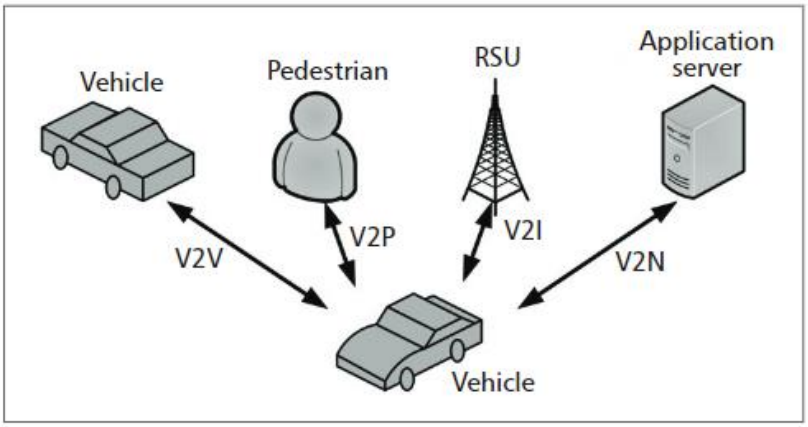
Σχήμα 4.1 - LTE Αρχιτεκτονική: δίκτυο πρόσβασης (eUTRAN) και δίκτυο κορμού (EPC). [40]

Το air interface του LTE είναι ευέλικτο και υποστηρίζει συστήματα όπως το time division duplexing (TDD), frequency division duplexing (FDD), και το half duplex FDD. Παρέχει επίσης πλάτος καναλιού από 1,4 έως 20 MHz. Όσον αφορά την τεχνολογία πρόσβασης, το orthogonal frequency division multiple access (OFDMA) χρησιμοποιείται στο downlink και το single carrier frequency division multiple access (SC-FDMA) για το uplink, παρέχοντας και τα δύο υψηλή ευελιξία. Η τεχνική multiple input multiple output (MIMO) βελτιώνει τη φασματική απόδοση ακόμη και σε UE τα οποία κινούνται με μεγάλη ταχύτητα, καθιστώντας το LTE ιδιαίτερα αποδοτικό σε απαιτητικά και δυναμικά περιβάλλοντα διάδοσης όπως αυτό των οχημάτων.

Τα radio resources διαχειρίζονται κεντρικά από ένα eNodeB σε επαναλαμβανόμενο χρονικό διάστημα μετάδοσης (διάρκειας 1 ms), με στόχο την επίτευξη συγκεκριμένων απαιτήσεων QoS. Βασικό ρόλο παίζει ο διαχειριστής πακέτων (packet scheduler) των eNodeB. Επιλέγει τη ροή κυκλοφορίας των πακέτων με βάση τις σχετικές απαιτήσεις QoS και αποφασίζει το κατάλληλο σχήμα διαμόρφωσης και κωδικοποίησης με βάση την ανατροφοδότηση των UE και την ποιότητα του καναλιού. [40]

4.1.1 Περιπτώσεις χρήσης και απαιτήσεις των υπηρεσιών για LTE - V2X

Όταν ο UE εκπέμπει εξυπηρετείται από το evolved Universal Mobile Telecommunications System Radio Access Network (E-UTRAN) το οποίο υποστηρίζει επικοινωνίες V2X. Αφού το UE που εκπέμπει έχει έγκυρο subscription και authorization, τα μηνύματα που περιέχουν πληροφορίες σχετικά με V2X εφαρμογές μπορούν να μεταδοθούν. Οι επικοινωνίες LTE V2X περιλαμβάνουν κυρίως επικοινωνίες V2V, V2I, V2N και V2P. Τα οχήματα που βρίσκονται σε κοντινή απόσταση μπορούν να ανταλλάσσουν πληροφορίες είτε απευθείας μεταξύ τους, είτε με τη βοήθεια υποδομών όπως τα evolved nodeB (eNB) ή τα RSU. Οι RSU κόμβοι μπορούν να ανταλλάσουν unicast (one-to-one connection μεταξύ client και server) πληροφορίες με οχήματα χρησιμοποιώντας εφαρμογές V2I. Επιπλέον, οι RSU κόμβοι μπορούν να μεταδίδουν broadcast πληροφορίες που σχετίζονται με ένα συμβάν έκτακτης ανάγκης ή πληροφορίες για την κατάσταση της κυκλοφορίας σε μια ομάδα χρηστών UE. Επίσης στις επικοινωνίες V2N και τα δύο μέρη, δηλαδή UE οχημάτων και το server application, υποστηρίζουν V2N εφαρμογές και επικοινωνούν μεταξύ τους με τη βοήθεια του LTE δικτύου. Επιπλέον, το evolved packet core (EPC) του LTE δικτύου μπορεί να συνδεθεί με έναν server του ITS για διάφορες υπηρεσίες οχημάτων. Τέλος το V2P υποστηρίζει την ανταλλαγή μηνυμάτων μεταξύ οχημάτων και πεζών. Αυτά τα μηνύματα μπορεί να μεταδίδονται από το UE του οχήματος στο UE των πεζών και το ανάποδο.



Σχήμα 4.2 - V2X εφαρμογές (V2V/V2P/V2I/V2N). [33]

Οι απαιτήσεις των υπηρεσιών V2X καθορίζονται από διάφορες εφαρμογές και σενάρια λειτουργίας. Για να καλύψει μια ποικιλία σεναρίων, η 3GPP ορίζει κάποιες παραμέτρους σε επίπεδο σύνδεσης και συστήματος για επικοινωνίες V2X. Αυτές οι παράμετροι ορίζονται βάση της ικανότητας ενός οχήματος να λαμβάνει τουλάχιστον ένα μήνυμα V2X μεταξύ δύο διαδοχικών μηνυμάτων V2X που αναφέρουν ένα επικείμενο συμβάν με πιθανότητα μεγαλύτερη από 95% σε περιπτώσεις που η ταχύτητα του οχήματος διαφέρει. Οι απαιτήσεις που σχετίζονται με την ασφάλεια υποστηρίζονται από authorization, integrity και privacy σύμφωνα με την 3GPP.

Ο παρακάτω πίνακας παρουσιάζει τις βασικές παραμέτρους απόδοσης με τις προτεινόμενες τιμές για τις 3GPP Release 14 V2X υπηρεσίες. Η παράμετρος *"effective distance"* είναι αρκετά μεγαλύτερη από το εύρος που απαιτείται για την υποστήριξη του χρόνου σύγκρουσης 4sec έτσι ώστε να δίνει αρκετό χρόνο στο οδηγό να ανταποκριθεί στη μέγιστη σχετική ταχύτητα *(relative speed).* Η παράμετρος *"minimum radio layer message reception reliability"* δηλώνει την πιθανότητα που έχει ο παραλήπτης να λάβει ένα μήνυμα V2X στην πραγματική απόσταση *(effective distance)* και εντός της μέγιστης ανεκτής καθυστέρησης *(maximum tolerable latency)*.

Πίνακας 4.1 – Παραδείγματα παραμέτρων για V2X υπηρεσίες. [39]

	Parameters				
Scenarios	Effective distance	Absolute speed of a UE	Relative speed between 2 UEs	Maximum tolerable latency	Minimum radio layer message reception reliability
#1 suburban/major road	200 m	50 km/h	100 km/h	100 ms	90%
#2 freeway/motorway	320 m	160 km/h	280 km/h	100 ms	80%
#3 autobahn	320 m	280 km/h	280 km/h	100 ms	80%
#4 NLOS/urban	150 m	50 km/h	100 km/h	100 ms	90%
#5 urban intersection	50 m	50 km/h	100 km/h	100 ms	95%
#6 campus/ shopping area	50 m	30 km/h	30 km/h	100 ms	90%
#7 imminent crash	20 m	80 km/h	160 km/h	20 ms	95%

4.1.2 Τεχνικές προκλήσεις και κίνητρα για LTE - V2X

Οι ανησυχίες σχετικά με τις καθαρά DSRC λύσεις επικοινωνίας V2X έχουν αυξήσει το ενδιαφέρον της ερευνητικής κοινότητας για τη διερεύνηση της ικανότητας των κυψελωτών τεχνολογιών να υποστηρίζουν αξιόπιστες επικοινωνίες V2X για διαφορετικές εφαρμογές. Υπάρχουν πολλοί παράγοντες οι οποίοι τραβούνε το ενδιαφέρον στα κυψελωτά δίκτυα. Ένας είναι η υψηλή χωρητικότητα που προσφέρει το LTE στο downlink και στο uplink, η οποία μπορεί να υποστηρίξει πολλά οχήματα ανά κυψέλη. Αυτές οι τιμές είναι υψηλότερες από του 802,11p, το οποίο προσφέρει ρυθμό μετάδοσης δεδομένων έως 27 Mb/s σε σχέση με το 1Gb/s του LTE-A. Ένας δεύτερος είναι η ευρεία κάλυψη που προσφέρει το LTE και μειώνει τη συχνότητα των handovers. Αυτό λύνει το πρόβλημα του 802.11p με την κακή, διακοπτόμενη και βραχέα συνδεσιμότητα και το LTE για επικοινωνίες V2I δίνει την λύση ακόμη και για κόμβους που κινούνται με υψηλές ταχύτητες. Η εκμετάλλευση της LTE υποδομής δίνει επίσης τη λύση για την επέκταση της συνδεσιμότητας του δικτύου σε εκείνα τα σημεία όπου οι άμεση επικοινωνία V2V δεν μπορεί να επιτευχθεί λόγω χαμηλής πυκνότητας αυτοκινήτων (ώρες αραιής κυκλοφορίας, αγροτικές περιοχές, κ.λπ.) ή δύσκολες συνθήκες διάδοσης (shadowing). Τέλος η ώριμη τεχνολογία του LTE διευκολύνει την υλοποίηση και επιταχύνει την ανάπτυξη των επικοινωνιών V2X.

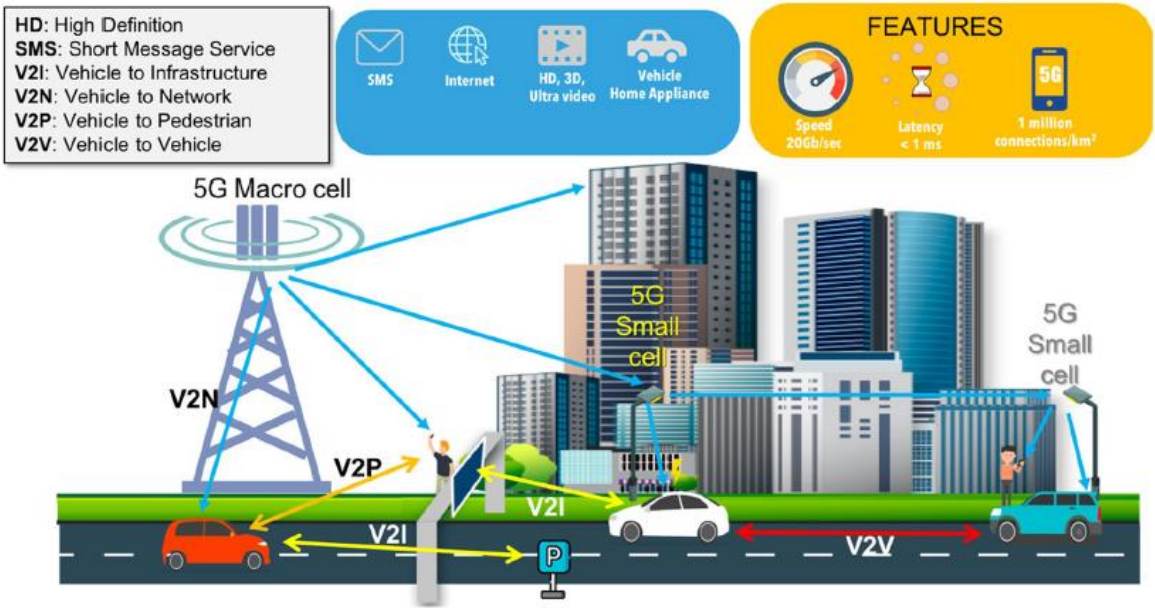
Παρά τα παραπάνω πλεονεκτήματα, υπάρχουν αρκετές προκλήσεις που περιορίζουν την ικανότητα των κυψελωτών δικτύων να υποστηρίξουν αξιόπιστες επικοινωνίες V2X. Λόγω της φύσης του κεντρικού ελέγχου των κυψελοειδών δικτύων, τα δεδομένα των οχημάτων πρέπει να περάσουν πρώτα από το σταθμό βάσης, περιορίζοντας έτσι τις επικοινωνίες V2V ειδικά για εφαρμογές ασφαλείας που έχουν πολύ αυστηρές απαιτήσεις καθυστέρησης. Σε λειτουργία unicast, ένα όχημα στέλνει το μήνυμα ασφαλείας του, στο σταθμό βάσης, ο οποίος με την σειρά του μεταδίδει το μήνυμα είτε σε κάθε όχημα εντός της κυψέλης είτε μόνο στα οχήματα που σχετίζονται με το συμβάν. Και στις δύο περιπτώσεις, το downlink κανάλι αποτελεί πρόβλημα ακόμη και όταν υπάρχει μικρός αριθμός οχημάτων στην κυψέλη. Οι διαθέσιμες δυνατότητες μετάδοσης broadcast και multicast υποστηρίζονται ήδη στα πρότυπα της 3GPP, δηλαδή το multimedia broadcast and multicast services (MBMS) και το evolved MBMS (eMBMS), στο δίκτυο κορμού και στο δίκτυο πρόσβασης. Προσφέρουν τη δυνατότητα αποστολής των δεδομένων σε ένα σύνολο χρηστών που είναι εγγεγραμμένοι στην προσφερόμενη υπηρεσία, αντί να αποστέλλονται σε κάθε κόμβο ξεχωριστά και αποτελούν πολλά υποσχόμενες λύσεις για τη μετάδοση μηνυμάτων ασφαλείας. Σε μια broadcast λειτουργία, ο σταθμός βάσης εκπέμπει ένα μήνυμα ασφαλείας σε όλα τα οχήματα εντός της κυψέλη του και εναπόκειται σε κάθε όχημα να καθορίσει τη συνάφεια του ληφθέντος μηνύματος ασφαλείας. Ως αποτέλεσμα, τα οχήματα λαμβάνουν πολλά άσχετα μηνύματα και διενεργούν περιττή επεξεργασία (καθώς ο αριθμός των οχημάτων σε ένα σταθμό βάσης είναι πολύ μεγαλύτερος από τον αριθμό των οχημάτων που έχουν συνάφειας με το μήνυμα ασφαλείας). Μια λύση σε αυτό το πρόβλημα είναι η χρήση του multicast, έτσι ώστε το μήνυμα να αποστέλλεται στα οχήματα που βρίσκονται στο ίδιο multicast group. Ωστόσο, αυτή η λύση μπορεί να είναι δαπανηρή όσον αφορά την καθυστέρηση και την επιβάρυνση του ελέγχου που σχετίζεται με τις διαδικασίες σύνδεσης και αποσύνδεσης του eMBMS, οι οποίες είναι απαραίτητες για τη δημιουργία

ενός multicast group. Αν και το broadcast/multicast μπορούν να μειώσουν το φορτίο του downlink. Το uplink ωστόσο γίνεται εμπόδιο σε καταστάσεις υψηλής πυκνότητας οχημάτων, οι uplink ζεύξεις επιτυγχάνονται πάντα χρησιμοποιώντας unicast. Επιπλέον ένας άλλος παράγοντας που επηρεάζει την καθυστέρηση στα κυψελωτά δίκτυα είναι η κατάσταση του τερματικού. Προκειμένου να εξοικονομηθούν πόροι, τα μη ενεργά τερματικά διατηρούνται σε κατάσταση αναμονής, αλλά οι ρυθμίσεις επανασύνδεσης που απαιτούνται για τη μετάβαση σε ενεργή λειτουργία πριν από την αποστολή δεδομένων μπορεί να καθυστερήσει περισσότερο από την απλή καθυστέρηση μετάδοσης. Τέλος, η αξιολόγηση της απόδοσης των αμιγώς κυψελοειδών δικτύων επικοινωνίας V2X πρέπει να λαμβάνει υπόψη την παραδοσιακή κίνηση, του δικτύου κινητής τηλεφωνίας (π.χ. φωνητικές κλήσεις), η οποία συνήθως αγνοείται.

4.2 5G

Ο οδικός χάρτης των επικοινωνιών στα οχήματα χαρακτηρίζεται από τις εξελίξεις ως προς το 5G, το οποίο αντιμετωπίζεται ως η μελλοντική τεχνολογία που θα καλύπτει – με τη ανάπτυξη των NR κόμβων - τρεις βασικές απαιτήσεις:

- *Peak Datarate* - μεγαλύτερο από 10 Gbps
- *Device Density* - μεγαλύτερο από 1 εκατομμύριο ανά km^2
- *Latency* - μικρότερο από 1 ms



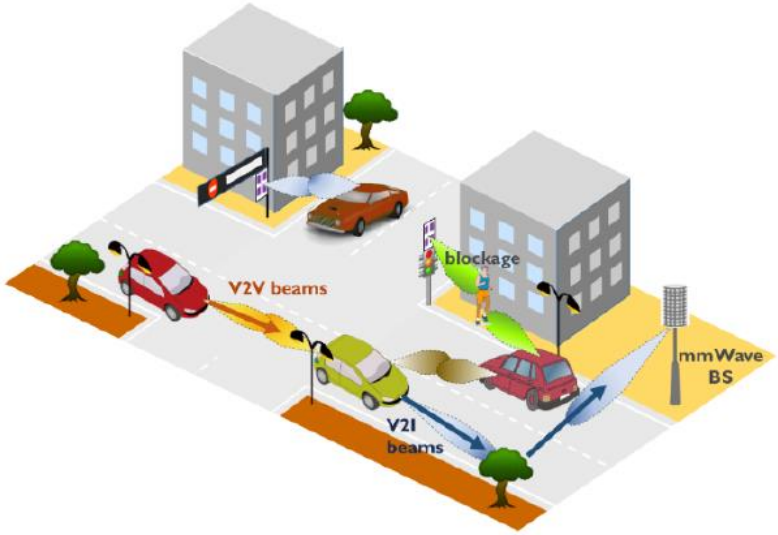
Εικόνα 4.1 - Τρόποι επικοινωνίας οχημάτων σε 5G περιβάλλον. [50]

Τα ασύρματα δίκτυα 5G θα ενσωματώνουν διάφορες αναδυόμενες τεχνολογίες όπως massive MIMO, device-to-device communications, multi radio access technology, full-duplex radios ,millimeter waves, cloud technologies και το SDN.

4.2.1 Millimeter Wave

Οι millimeter wave επικοινωνίες έχουν δημιουργηθεί για να παρέχουν συνδέσεις υψηλής ταχύτητας δεδομένων μεταξύ οχημάτων και roadside υποδομών για 5G V2X επικοινωνίες. Ωστόσο, το mmWave αντιμετωπίζει αρκετές προκλήσεις. Στο physical layer, το mmWave είναι ευάλωτο σε σκίαση (shadowing). Η σκίαση περιορίζει τις συνδέσεις από σημείο σε σημείο έως και μερικές εκατοντάδες μέτρα. Επιπλέον, ενδέχεται να προκύψουν ζητήματα καθυστέρησης, αξιοπιστίας και ασφάλειας κατά την μετάδοση mmWave συνδέσεων. Σε mmWave επικοινωνίες, μπορεί να υπάρξουν καθυστερήσεις κατά τη δημιουργία ενός κλειδιού στο φυσικό επίπεδο καθώς επίσης και κατά τη διάρκεια του beam search στην αρχική πρόσβαση. Επιπλέον, το mmWave αυξάνει το randomness και μπορεί να δημιουργήσει κλειδί με μικρότερη καθυστέρηση. Αυτή η γρήγορη παραγωγή κλειδιών περιπλέκει τη διαδικασία ανταλλαγείς πληροφοριών λόγω της δημιουργίας διαφορετικών κλειδιών σε δύο οχήματα που επικοινωνούν. Το broadcasting είναι ένα άλλο ζήτημα στις mmWave επικοινωνίες λόγω των beamforming επικοινωνιών. Στο mmWave, τα μηνύματα μεταδίδονται με beamforming προς μια συγκεκριμένη ομάδα χρηστών με αποτέλεσμα να δημιουργούνται προβλήματα κατά τη μετάδοση μηνυμάτων προς οχήματα που βρίσκονται σε γωνιακή κατεύθυνση σε σχέση με την κατεύθυνση εκπομπής. [16]

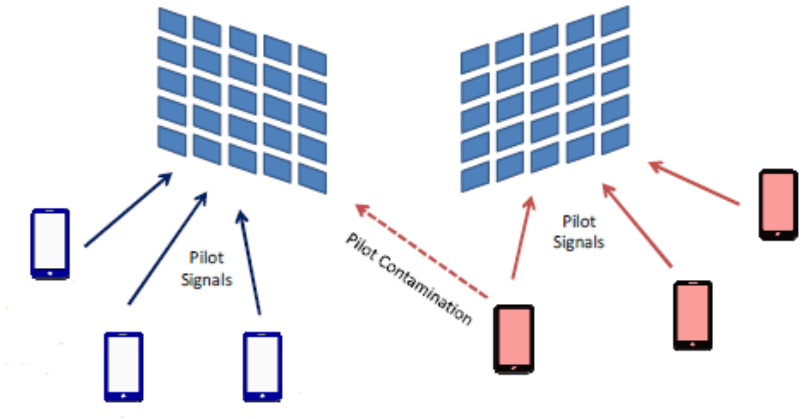
Μια λύση για τα παραπάνω προβλήματα θα ήταν μια τεχνική βελτίωσης βάσει της τοποθεσίας, όπως η επαναληπτική αναζήτηση, που μπορεί να χρησιμοποιηθεί για τη μείωση της καθυστέρησης που σχετίζεται με το beam search κατά την αρχική πρόσβαση σε επικοινωνίες mmWave. Το πρόβλημα που σχετίζεται με το broadcasting προς οχήματα που βρίσκονται σε γωνιακή κατεύθυνση μπορεί να λυθεί με τη χρήση πομποδέκτη εντός οχήματος που να συνδυάζει την επανεκπομπή των ίδιων πληροφοριών σε διαφορετική κατεύθυνση. Επιπλέον, η εξαιρετικά πυκνή ανάπτυξη σταθμών βάσης και RSU μπορεί να χρησιμοποιηθεί για την αντιμετώπιση του μικρού εύρους επικοινωνίας του mmWave.



Εικόνα 4.2 - Επικοινωνίες V2X με χρήση mmWave (πολλαπλοί mmWave πομποδέκτες αναπτύσσονται σε ένα όχημα για την ταυτόχρονη επικοινωνία V2V και V2I). [69]

4.2.2 Massive MIMO

Το Massive MIMO χρησιμοποιεί εκατοντάδες κεραίες στους σταθμούς βάσης και παρέχει υψηλό κέρδος όσον αφορά την φασματική απόδοση ενώ μπορεί να ικανοποιήσει τις κλιμακωτές απαιτήσεις των ασύρματων δικτύων επόμενης γενιάς. Σε επικοινωνίες V2X οι MIMO κεραίες έχουν δείξει ότι μπορούν να επιτύχουν υψηλούς ρυθμούς μετάδοσης δεδομένων έως και 40 Mbps. Ωστόσο, στο Massive MIMO, η διαθεσιμότητα για την κατάσταση του καναλιού είναι μία από τις πιο βασικές απαιτήσεις για την αποφυγή παρεμβολών μεταξύ των χρηστών έτσι ώστε να επιτευχθεί υψηλό κέρδος. Το SINR σε τέτοια συστήματα περιορίζεται πολύ από το pilot contamination, το οποίο είναι πιο έντονο σε καταστάσεις υψηλής κινητικότητας. Σε καταστάσεις υψηλής κινητικότητας, το pilot signal περιορίζεται λόγω του μικρού χρόνου αλλαγής μεταξύ των καναλιών και η απόδοση του δικτύου επηρεάζεται σημαντικά από τους περιορισμούς στο κανάλι το οποίο είναι βασικό ζήτημα σε ένα massive MIMO σύστημα. [16]



Σχήμα 4.3 – Πιλοτικά σήματα (pilot signals) που αποστέλλονται σε έναν massive MIMO σταθμό βάσης. [71]

Για την αντιμετώπιση του παραπάνω ζητήματος σχετικά με το massive MIMO στις επικοινωνίες οχημάτων έχει προταθεί ένα μοντέλο που αυξάνει τη συνολική απόδοση του δικτύου και έχει εφαρμογή σε διάφορα περιβάλλοντα επικοινωνιών όπως pico, micro και macro cell. Το μοντέλο βελτιστοποιεί τον σχεδιασμό των pilot signals στα συστήματα massive MIMO. Έτσι προτείνετε ένα σχήμα στο οποίο τα pilot signals επαναχρησιμοποιούνται μεταξύ των χρηστών για να μειώσουν το pilot overhead σε ένα σταθμό βάσης. Στο προτεινόμενο σχήμα, το pilot contamination λόγω της επαναχρησιμοποίησης του μειώνεται με τη βοήθεια ενός graph coloring αλγόριθμου. Επιπλέον, χρησιμοποιείτε ένας επαναληπτικός αλγόριθμος για τον έλεγχο της ισχύος και την ελαχιστοποίηση αυτής κατά την μετάδοσης δεδομένων. [16]

Λαμβάνοντας υπόψη τα παραπάνω συνιστάτε και η χρήση διαφορετικής διαμόρφωσης, σε διαφορετικές περιοχές, σύμφωνα με τις ιδιότητες του καναλιού έτσι ώστε να ενισχυθεί η απόδοση των συστημάτων MIMO. Έτσι προτείνεται η διαμόρφωση με QPSK σε περιοχές που το SINR είναι μικρό και το κανάλι δεν είναι καλό, ενώ αν το κανάλι είναι σε καλή κατάσταση μπορούμε να διαμορφώσουμε με 64-QAM. Στις περιοχές με μέτριες συνθήκες καναλιού, η χρήση ενός μείγματος και των δύο μαζί με διαμόρφωση 16-QAM είναι ιδανική έτσι ώστε να αυξηθεί το throughput.

4.2.3 Software Defined Network (SDN)

Το SDN έχει σχεδιαστεί ως μια νέα τεχνολογία που παρέχει ανθεκτικότητα στο δίκτυο και δυνατότητα προγραμματισμού της ροής σε δίκτυα 5G. Τα δίκτυα οχημάτων με δυνατότητα SDN αποτελούνται από macro και small cells, συμπεριλαμβανομένων σταθμών βάσης και access point. Στα δίκτυα οχημάτων SDN, ένας κεντρικός ελεγκτής με πρωτόκολλο OpenFlow ελέγχει τους σταθμούς βάσης, τα macro cells και τα access point. Επιπλέον, το SDN μεταφέρει τον έλεγχο από την υποδομή στο control layer έτσι ώστε να φιλοξενήσει διάφορες εφαρμογές και να παρέχει νέες λειτουργίες. Επιπλέον, ο controller του SDN είναι υπεύθυνος για τα δίκτυα πρόσβασης, συμπεριλαμβανομένου του authentication, του traffic management και άλλων ζητημάτων, ενώ οι σταθμοί βάσης αποτελούν το data plane του SDN και εφαρμόζουν τις πολιτικές που ορίζονται από τον controller. Έτσι, το SDN μπορεί να βοηθήσει στη μείωση του signaling overhead στα δίκτυα οχημάτων και να βελτιώσει την ποιότητα των επικοινωνιών.

Επιπλέον, το SDN μπορεί να χρησιμοποιηθεί για δια δικτύωση και εκμετάλλευση πόρων σε ετερογενή δίκτυα με ευέλικτο τρόπο. Επιπλέον, τα δίκτυα οχημάτων με δυνατότητα SDN μπορούν να αποτελούνται από cloud computing centers, SDN controllers και fog computing clusters. Σε τέτοια δίκτυα, οι SDN controllers μεταφέρουν τις πληροφορίες κατάστασης από τα fog clusters στα cloud centers. Αυτά τα fog computing clusters ή fog cells περιλαμβάνουν, RSUs, σταθμούς βάσης, χρήστες και οχήματα που βρίσκονται στην άκρη του 5G-SDN δικτύου. Τα fog cells που βασίζονται στο 5G-SDN μπορούν να χρησιμοποιούν multi-hop relays για να μειώσουν το handover μεταξύ RSUs και οχημάτων. Επιπλέον, παρέχουν υψηλότερο throughput από τα παραδοσιακά συστήματα.

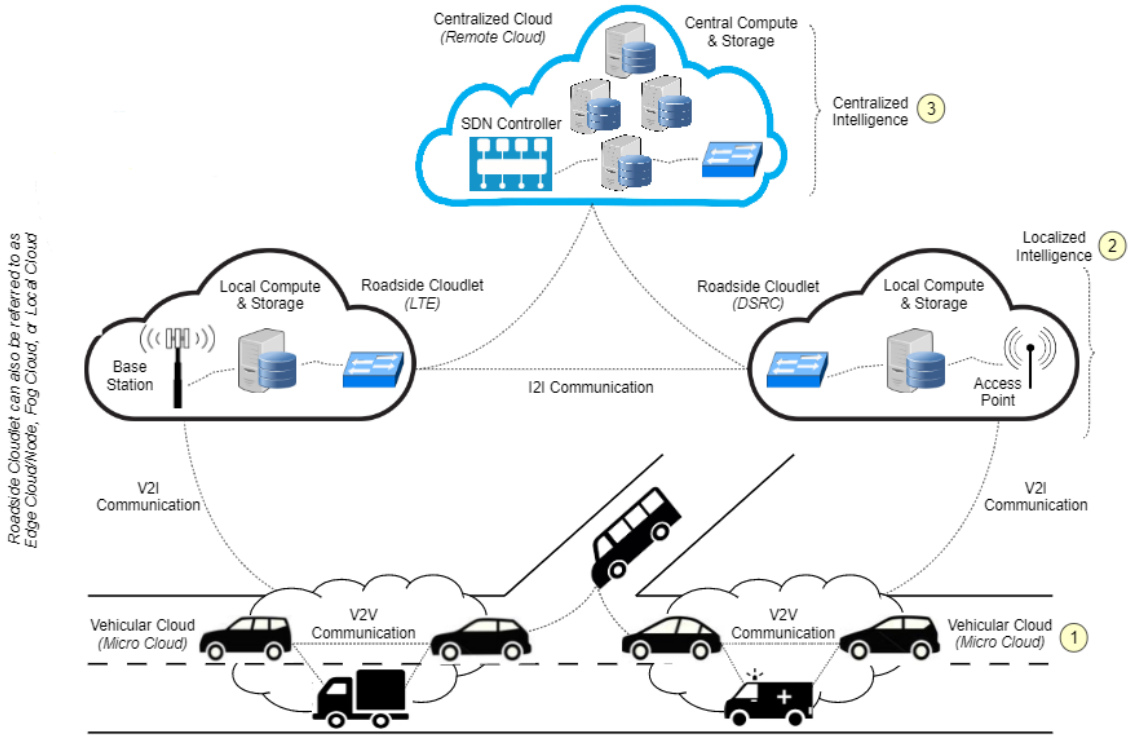
Ωστόσο, υπάρχουν αρκετές προκλήσεις για τα SDN δίκτυα οχημάτων με κάποιες από αυτές να είναι οι παρακάτω: [16]

- *Inter-Operation* - Τα δίκτυα οχημάτων 5G με δυνατότητες SDN μπορούν να χρησιμοποιηθούν για διαλειτουργικότητα μεταξύ διαφόρων τεχνολογιών. Ωστόσο, λόγω των διαφορετικών προτύπων επικοινωνίας και των link επικοινωνίας με διάφορα πρότυπα δικτύωσης, η διαλειτουργικότητα μπορεί να είναι περιορισμένη.
- *Network Management* - Στα δίκτυα SDN, υπάρχουν διαφορετικές προδιαγραφές software και hardware με διάφορες υπηρεσίες. Τέτοια δίκτυα είναι πιο πολύπλοκα στη διαχείριση.
- *QoS Provisioning* - Λόγω της δυναμικής τοπολογίας στα δίκτυα οχημάτων, η διαθεσιμότητα πόρων μπορεί να ποικίλλει. Επιπλέον, αυτό το πρόβλημα επιδεινώνεται λόγω της υψηλής ετερογένειας στα δίκτυα οχημάτων που βασίζονται στο SDN.

Ένα SDN δίκτυο ανοιχτού κώδικα είναι μια λύση για τη διαλειτουργικότητα και διαχείριση ενός ετερογενούς δικτύου. Το SDN αυτό αποτελείται από ένα API για το radio access που διαχωρίζει το user plane από το control plane. Το SDN υποστηρίζει ενεργό RAN slicing καθώς και load balancing και mobility management. Η πλατφόρμα

αυτή διαχειρίζεται ταυτόχρονα ετερογενή δίκτυα όπως δίκτυα κινητής τηλεφωνίας και Wi-Fi δίκτυα. [16]

Ακόμα προτείνεται το control plane να σχεδιαστεί αποτελεσματικά για την αντιμετώπιση θεμάτων που σχετίζονται με το SDN σε ετερογενή δίκτυα οχημάτων καθώς μπορεί να φέρει προβλήματα στις επικοινωνίες μεταξύ ελεγκτών και οχημάτων. Στο υβριδικό DSRC και κυψελωτό δίκτυο V2X, το SDN μπορεί να χρησιμοποιήσει και τα δύο, ad-hoc και κυψελωτό δίκτυο στη διαχείριση του δικτύου.



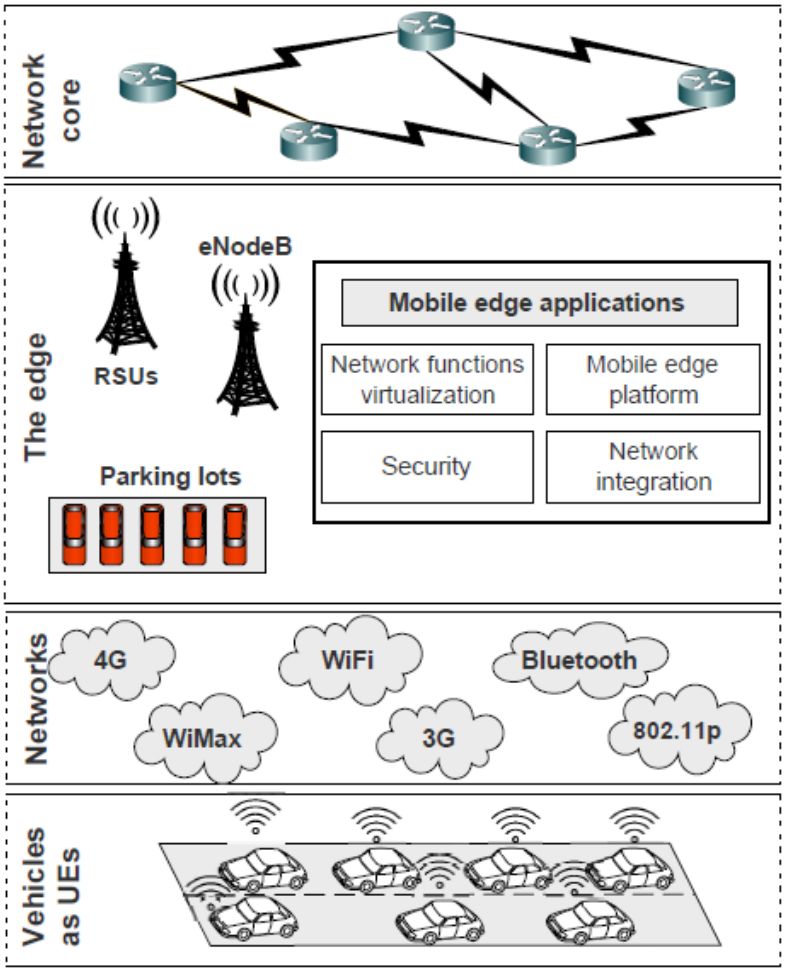
Σχήμα 4.4 - Μια τυπολογική αρχιτεκτονική του Software-defined για ετερογενή δίκτυα οχημάτων. [18]

4.2.4 Mobile Edge Computing (MEC)

Το mobile edge computing στα 5G δίκτυα επικοινωνίας για οχήματα έχει σχεδιαστεί έτσι ώστε να παρέχει χαμηλές καθυστερήσεις. Σε αυτά τα συστήματα, κάποιες βασικές λειτουργίες του δικτύου κορμού μεταφέρονται στο άκρο αυτού, δηλαδή πιο κοντά στον χρήστη. Το Network Function Virtualization (NFV) μπορεί να χρησιμοποιηθεί για το mobie edge computing για την παροχή διαφορετικών υπηρεσιών. Στο NFV, οι λειτουργίες του δικτύου κορμού τοποθετούνται στα eNB και στα RSU με δυνατότητες αποθήκευσης και επεξεργασίας. Επιπλέον, το mobile edge computing μπορεί να χρησιμοποιηθεί για την ενίσχυση του ελέγχου στα δίκτυα οχημάτων που βασίζονται στο 5G-SDN. Ακόμα, οι servers του mobile edge computing μπορούν να διαχειρίζονται ομάδες οχημάτων σε δίκτυα που βασίζονται επίσης στο 5G-SDN. Το control plane του

SDN και οι servers του mobile edge computing μπορούν να τοποθετηθούν στο ίδιο σημείο, έτσι ώστε οι servers του mobile edge computing να μπορούν να λειτουργούν ως τοπικοί ελεγκτές για τον εντοπισμό του control plane στα δίκτυα οχημάτων που βασίζονται στο 5G-SDN. Τέλος, η βελτίωση της διαχείρισης των δικτύων και πόρων αυτού με μια βιώσιμη ανάπτυξη είναι μερικά πλεονεκτήματα του mobile edge computing με SDN.

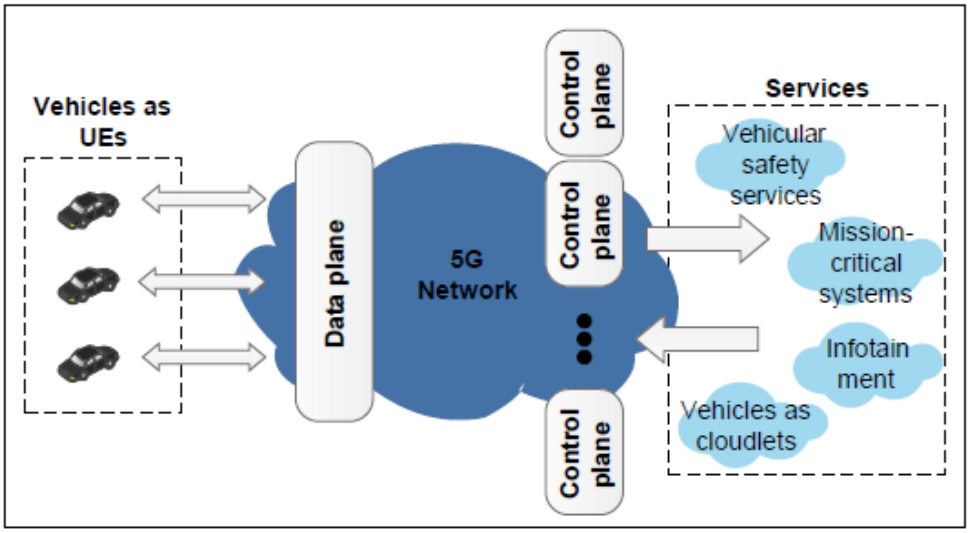
Υπάρχουν ωστόσο αρκετές προκλήσεις στα 5G δίκτυα οχημάτων με υποβοήθηση edge computing λόγω του τεράστιου όγκου δεδομένων, της δυναμικής αλλαγής στην τοπολογία και της άνισης κυκλοφοριακής κατανομής. Επιπλέον, η μεταφορά των λειτουργιών του δικτύου κορμού σε RSU και eNB θα αυξήσει πολύ το κόστος για την ανάπτυξη τέτοιων δικτύων. Επιπλέον, θα υπάρξει πρόβλημα σχετικά με την παροχή υψηλής υπολογιστικής ικανότητας και χωρητικότητας αποθήκευσης καθώς και ασφάλειας στα edge συστήματα. [16]



Σχήμα 4.5 - Mobile edge computing για δίκτυα οχημάτων. [29]

4.2.5 Network Slicing

Το network slicing είναι μέρος της λειτουργίας του δικτύου όπου σε διάφορα τμήματα του μπορεί να διαμορφώνει ‘’εικονικά’’ και ξεχωριστά τις παραμέτρους του έτσι ώστε να υποστηρίζει συγκεκριμένες λειτουργίες και απαιτήσεις. Μπορούν να λειτουργούν παράλληλα διαφορετικά slice του δικτύου για την παροχή υπηρεσιών σε πραγματικό χρόνο. Έτσι, το slicing του δικτύου στοχεύει στην απομόνωση των λειτουργιών και των πόρων του δικτύου από ένα ενιαίο δίκτυο υποδομής. Το slicing διαιρεί το δίκτυο χωρίζοντας το control plane σε πολλά επίπεδα και επηρεάζει πολλές λειτουργίες ελέγχου, όπως το authentication, το mobility και το session management. Επιπλέον, επηρεάζει τις λειτουργίες του user plane, όπως η δυνατότητα προγραμματισμού.



Σχήμα 4.6 - Network slicing για επικοινωνίες οχημάτων. [29]

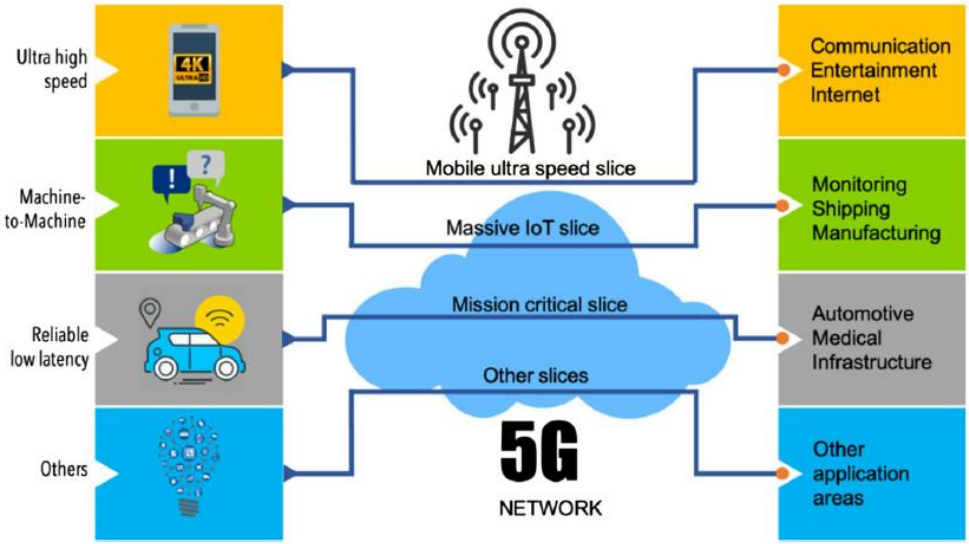
Διαφορετικά slice του δικτύου μπορούν να χρησιμοποιηθούν, για διάφορες εφαρμογές. Για παράδειγμα μπορούμε να χρησιμοποιήσουμε ένα slice του δικτύου για εφαρμογές που απαιτούνε ασφάλεια, για εφαρμογές που επαιτούνε χαμηλές καθυστερήσεις και εφαρμογές ενημέρωσης και ψυχαγωγίας που απαιτούσαν υψηλό bandwidth.

Ωστόσο, υπάρχουν αρκετές προκλήσεις για την χρήση του network slicing στα 5G δίκτυα οχημάτων. Κάποια από αυτά είναι:

- Το slice manager πρέπει να διαμορφώσει πολλαπλά slices ανά συσκευή ταυτόχρονα.
- Το network slicing εγκυμονεί κινδύνους ως προς την ασφάλεια καθώς ενδέχεται να απαιτούνται διαφορετικά επίπεδα ασφαλείας για διαφορετικά slice του δικτύου.
- Μια αμφίδρομη σχέση εμπιστοσύνης απαιτείται μεταξύ του slice manager και του παρόχου που ελέγχει την υποδομή.

Έτσι, για να είναι αποτελεσματικό το slicing του δικτύου, οι εφαρμογές των οχημάτων θα πρέπει να μετατρέπονται σε τεχνικές προδιαγραφές έτσι ώστε το slice manager να τις παίρνει και να διαμορφώνει πολλαπλά slice ανά εφαρμογή οχήματος. Επιπλέον, θα πρέπει να υπάρχει μια κατευθυντήρια γραμμή όπου θα καθορίζει εάν οι λειτουργίες του δικτύου θα πρέπει να είναι centralized ή sliced. [16]

Μια λύση για network slicing σε επικοινωνίες οχημάτων θα μπορούσε να είναι μια αρχιτεκτονική που θα υποστηρίζει συγκεκριμένες εφαρμογές σε οχήματα, διασφαλίζοντας παράλληλα quality of service. Στην αρχιτεκτονική αυτή, μπορούμε να εισάγουμε τρία slice. Το πρώτο slice θα μπορούσε να είναι ένα slice χαρτογράφησης υψηλής ευκρίνειας που χρησιμοποιείται για την πλοήγηση οχημάτων. Το δεύτερο slice να είναι ένα αρχείο κοινού ενδιαφέροντος για τη διαμοιρασμό δημοφιλούς περιεχομένου. Ενώ το τρίτο slice να είναι ένα slice μετάδοσης on demand για διαδραστικές συνεδρίες και φωνητικές κλήσεις σε πραγματικό χρόνο. Κάθε ένα από αυτά τα slices θα υποστηρίζει συγκεκριμένες εφαρμογές και θα εγγυάται quality of service σε δίκτυα οχημάτων.



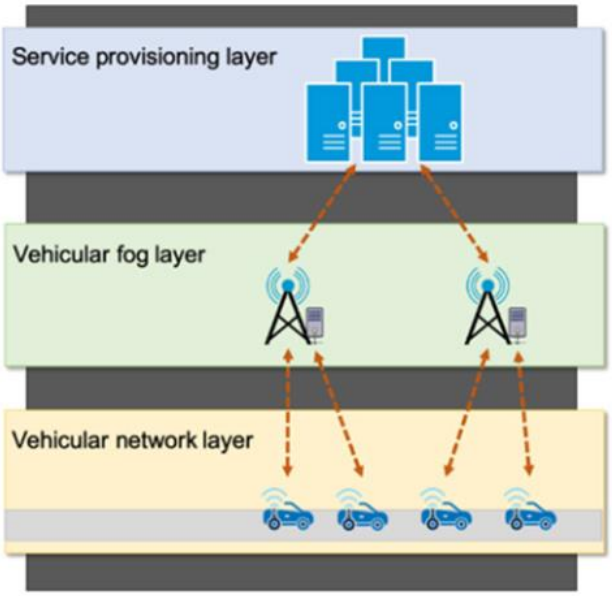
Σχήμα 4.7 - Network slicing (5G) για διάφορους τομείς και εφαρμογές, με διαφορετικές απαιτήσεις υπηρεσιών. [50]

4.2.6 Fog Computing

Ο αριθμός των συσκευών που είναι συνδεδεμένες στο Internet of Things και στο cloud για την αποθήκευση δεδομένων αυξάνεται εκθετικά τα τελευταία χρόνια σε πολλούς τομείς, όπως e-Health, Intelligent Transportation Systems και smart cities. Στα VANET, απαιτείται οι πόροι όπως οι υπολογιστές, η αποθήκευση και η δικτύωση να έχουν αρκετά υψηλές αποδόσεις. Έτσι τα τελευταία χρόνια έχουν προταθεί αρκετές λύσεις που βασίζονται στο cloud computing. Οι νέες απαιτήσεις οδήγησαν στην ενσωμάτωση τόσο των cloud computing τεχνολογιών όσο και των τεχνολογιών VANETs, γεγονός που

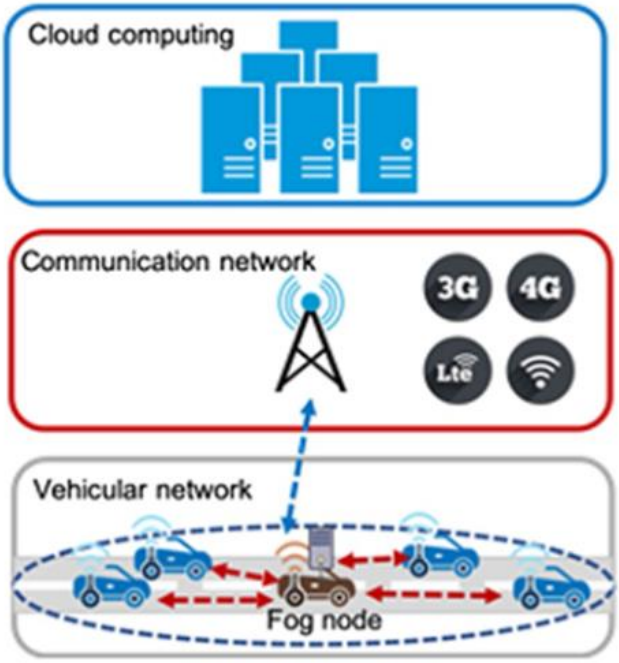
οδήγησε στην ιδέα του Vehicular Cloud Computing (VCC) που προσφέρει στους οδηγούς υπηρεσίες γνωστές ως pay as you go. Ωστόσο, οι λύσεις που βασίζονται στο cloud δεν είναι αρκετά βέλτιστες και αποτελεσματικές, επειδή δεν πληρούν όλες τις απαιτήσεις των VANET (ελάχιστες καθυστερήσεις, αδιάλειπτες υπηρεσίες και υψηλή ταχύτητα επεξεργασίας). Το cloud computing επιφέρει μεγάλες καθυστερήσεις όταν μεταφέρονται δεδομένα μεταξύ του οχήματος και του cloud. Σε αυτό το πλαίσιο, μια σημαντική πρόκληση για το VCC είναι η παροχή Quality of Service (QoS) για εκείνες τις εφαρμογές που χρειάζονται διαθέσιμους υπολογιστικούς και αποθηκευτικούς πόρους πιο κοντά στα οχήματα. Η εμφάνιση του fog computing υπόσχεται να λύσει ορισμένους από τους περιορισμούς της κεντρικής επεξεργασίας που χρησιμοποιείται από το cloud computing. Το fog computing επεκτείνει τις υπηρεσίες του cloud computing στην άκρη του δικτύου και βοηθά στην επεξεργασία των πληροφοριών για στην επίτευξη χαμηλής καθυστέρησης και γρήγορων αποκρίσεων. Το fog computing επιτρέπει σε μεγάλο αριθμό αποκεντρωμένων συσκευών να επικοινωνούν και να συνεργάζονται μεταξύ τους για την εκτέλεση εργασιών αποθήκευσης και επεξεργασίας χωρίς τη συμμετοχή τρίτων.

Όπως βλέπουμε στο παρακάτω σχήμα η αρχιτεκτονική του fog computing για οχήματα μπορεί να περιλαμβάνει πολλά επίπεδα. Το Vehicular Network Layer (VNL) εξετάζει οχήματα εξοπλισμένα με αισθητήρες, OBUs και δυνατότητες επικοινωνίας που τους επιτρέπουν να μοιράζονται πληροφορίες με άλλα οχήματα. Το Vehicular Fog Layer (VFL) διαθέτει μονάδες εξοπλισμένες με δυνατότητες επικοινωνίας, επεξεργασίας και αποθήκευσης. Αυτές οι μονάδες τοποθετούνται σε κρίσιμα σημεία (όπως διασταυρώσεις και χώροι στάθμευσης) για να παρέχουν επαρκή κάλυψη. Τέλος, το Service Provisioning Layer (SPL) παρέχει πρόσβαση σε διαφορετικές υπηρεσίες cloud (όπως υπηρεσίες πληροφοριών κυκλοφορίας, παρακολούθηση καιρού, πρόγνωση καιρού και υπηρεσίες ψυχαγωγίας) και μπορεί να επικοινωνεί με τους fog κόμβους οχημάτων και τους παρόχους υπηρεσιών. [50]



Σχήμα 4.8 - Αρχιτεκτονική fog computing για δίκτυα οχημάτων. [50]

Το παρακάτω σχήμα παρουσιάζει μια αρχιτεκτονική που απεικονίζει τις επικοινωνίες V2V σε περιβάλλον fog για οχήματα. Οι Fog Nodes V2V (V2V-FN) μπορούν να εφαρμοστούν σε ειδικά οχήματα (όπως αστυνομικά οχήματα, αστικές συγκοινωνίες και ταξί) με υψηλές δυνατότητες επικοινωνίας, αποθήκευσης και επεξεργαστικής ισχύς. Αυτά τα οχήματα θα μπορούν να προσφέρουν υπηρεσίες streaming, υπηρεσίες κυκλοφοριακής κατάστασης κ.λπ. Στο vehicular network επίπεδο, οι fog κόμβοι προσφέρουν υπηρεσίες επεξεργασίας, υπολογισμού και αποθήκευσης ενώ μπορούν να επικοινωνούν απευθείας με cloud servers μέσω δικτύων επικοινωνίας όπως Wi-Fi, 4G και 5G. Το fog δίκτυο οχημάτων εκμεταλλεύεται το cloud computing για να προσφέρει υπηρεσίες pay-as-you-go στους οδηγούς σε ένα VANET περιβάλλον. [50]



Σχήμα 4.9 - Αρχιτεκτονική fog network με επικοινωνίες V2V μεταξύ fog node και άλλων οχημάτων. [50]

Σε ένα fog περιβάλλον, δεν υπάρχει μοναδικός ορισμός για τον fog κόμβο. Οι fog κόμβοι ορίζονται ως οι βασικές μονάδες που χρησιμοποιούν δυνατότητες επεξεργασίας, όπως υπολογιστικούς servers. Θεωρούμε έναν fog κόμβο μια φυσική συσκευή που παρέχει πόρους για υπηρεσίες στην άκρη του δικτύου.

Θα μπορούσαμε ωστόσο να κατηγοριοποιούμε τους fog κόμβους με βάση τα χαρακτηριστικά και τις λειτουργίες τους:

- *Fog Nodes ως mini-clouds ("dumbs")* – περιλαμβάνουν edge συσκευές που αναμεταδίδουν δεδομένα.
- *Fog Nodes ως mini-clouds ("smarts")* – περιλαμβάνουν edge συσκευές με δυνατότητες υπολογισμού, αποθήκευσης και δικτύωσης που επιτρέπουν την προεπεξεργασία δεδομένων για μεταφορά στο mini-cloud εντός του fog κόμβου.

Σε ένα fog περιβάλλον που αποτελείται από fog κόμβους, η τοποθεσία επεξεργασίας των δεδομένων μιας εφαρμογής εξαρτάται από τις απαιτήσεις της, όπως η καθυστέρηση (latency), η ασφάλεια (security), η κινητικότητα (mobility) και η επεκτασιμότητα (scalability). Ένα άλλο βασικό στοιχείο στο περιβάλλον fog είναι οι θέσεις των κόμβων. Η θέση των κόμβων εξαρτάται από την αρχιτεκτονική που εμπλέκεται. Οι κόμβοι μπορούν να βρίσκονται κοντά σε ένα σταθμό βάσης BS ή μπορεί να είναι συσκευές ενός χρήστη όπου οι χρήστες μοιράζονται τους κόμβους. Κατά την εφαρμογή του σχεδίου με τους fog κόμβους σε ένα VANET, για τη λειτουργία V2I επικοινωνιών είναι αρκετά απλό να υπάρχουν κόμβοι fog κοντά ή πάνω σε RSUs έτσι ώστε να πετυχαίνεται κάλυψη σε μεγάλη περιοχή. Αλλά για τις επικοινωνίες V2V, πρέπει να αντιμετωπιστούν αρκετές προκλήσεις, όπως τα κριτήρια που χρησιμοποιούνται κατά την επιλογή ενός κόμβου και η χωρητικότητα αποθήκευσης του κόμβου. Καθώς τα δεδομένα που παράγονται από οχήματα είναι ευαίσθητα όσον αφορά το απόρρητο, χρειαζόμαστε αποτελεσματικούς μηχανισμούς διατήρησης της ιδιωτικότητας. Η χρήση των κόμβων σε ένα περιβάλλον επικοινωνίας V2V θα εξαρτηθεί επίσης από άλλους παράγοντες όπως ο αριθμός των εισερχόμενων αιτημάτων και η συχνότητα των αιτημάτων. [50]

5 ΕΤΕΡΟΓΕΝΗ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΕΣ ΟΧΗΜΑΤΩΝ

Τα ετερογενή δίκτυα χρησιμοποιούν διαφορετικές Radio Access Technologies (RAT) όπως δίκτυα Wi-Fi, WiMAX, 4G, 5G και διάφορες μορφές σταθμών βάσης. Ωστόσο, τα τελευταία χρόνια, η έρευνες έχουν επικεντρωθεί στα ετερογενή ασύρματα δίκτυα επικοινωνιών για οχήματα και κυρίως με χρήση του LTE. Η μελέτες κατά κύριο λόγο ρίχνουν το βάρος τους στην σύγκριση της LTE τεχνολογίας με το IEEE 802.11p/WAVE για να βρεθεί ποια τεχνολογία από τις δυο μπορεί να υποστηρίξει συνεργατικές εφαρμογές ασφάλειας για τα οχήματα. Το LTE προσφέρει μεγάλη χωρητικότητα δικτύου υποστηρίζει καλύτερα την κινητικότητα των χρηστών και έχει καλύτερη κάλυψη. Από την άλλη όμως το LTE υποφέρει από υψηλό latency και αυξάνει το φόρτο του δικτύου σε σύγκριση με το 802.11p. Ωστόσο, έχουν προταθεί υβριδικές προσεγγίσεις κατάλληλες για ετερογενή δίκτυα οχημάτων που συνδυάζουν τόσο το LTE όσο και το 802.11p.

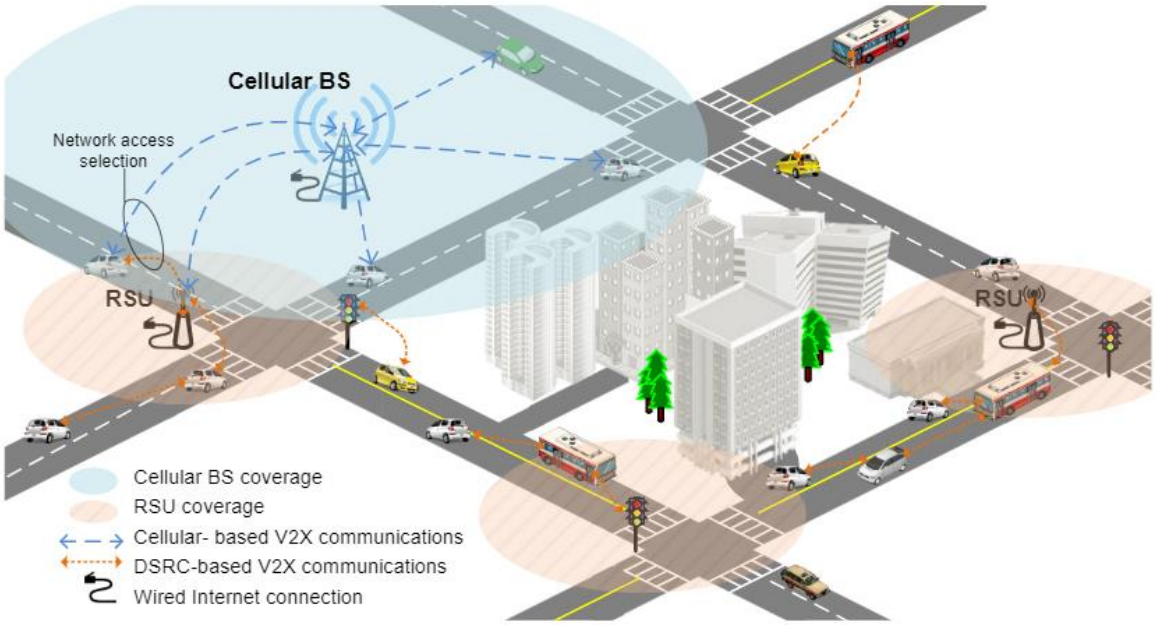
Επί του παρόντος, η έρευνα ασχολείται με τα ετερογενή ασύρματα δίκτυα επικοινωνιών για οχήματα. Ενδεικτικά μπορούμε να αναφέρουμε κάποιες προτάσεις όπως χρήση δορυφορικών επικοινωνιών σε δικτύου οχημάτων όπου το downlink γίνεται με την χρήση δορυφόρου ενώ το uplink με τη χρήση κυψελωτών δικτύων. Μια άλλη πρόταση μπορεί να είναι το LTE για επικοινωνίες V2I και το DSRC για επικοινωνίες V2V σαν μια από τις καλύτερες λύσεις για την υποστήριξη υπηρεσιών σε οχήματα. Δεδομένου ότι τα δίκτυα οχημάτων είναι εξαιρετικά δυναμικά λόγω των γρήγορων αλλαγών, οι περισσότερες από αυτές τις μελέτες δίνουν έμφαση στο κανάλι μετάδοσης, στο handover, στη διάδοση των δεδομένων και το mobility, ενώ άλλες επικεντρώνονται σε θέματα ασφάλειας. Ο παρακάτω πίνακας συνοψίζει τις κύριες ασύρματες τεχνολογίες για ετερογενή δίκτυα οχημάτων.

Πίνακας 5.1 – Οι κυριότερες ασύρματες τεχνολογίες για ετερογενείς επικοινωνίες οχημάτων. [40]

Feature	Wi-Fi	802.11p	UMTS	LTE	LTE-A
Channel width	20 MHz	10 MHz	5 MHz	1.4, 3, 5, 10, 15, 20 MHz	Up to 100 MHz
Frequency band(s)	2.4 GHz, 5.2 GHz	5.86–5.92 GHz	700–2600 MHz	700–2690 MHz	450 MHz–4.99 GHz
Bit rate	6-54 Mb/s	3–27 Mb/s	2 Mb/s	Up to 300 Mb/s	Up to 1 Gb/s
Range	Up to 100 m	Up to 1 km	Up to 10 km	Up to 30 km	Up to 30 km
Capacity	Medium	Medium	Low	High	Very High
Coverage	Intermittent	Intermittent	Ubiquitous	Ubiquitous	Ubiquitous
Mobility support	Low	Medium	High	Very high (up to 350 km/h)	Very high (up to 350 km/h)
QoS support	Enhanced Distributed Channel Access (EDCA)	Enhanced Distributed Channel Access (EDCA)	QoS classes and bearer selection	QCI and bearer selection	QCI and bearer selection
Broadcast/multicast support	Native broadcast	Native broadcast	Through MBMS	Through eMBMS	Through eMBMS
V2I support	Yes	Yes	Yes	Yes	Yes
V2V support	Native (ad hoc)	Native (ad hoc)	No	No	Potentially, through D2D
Market penetration	High	Low	High	Potentially high	Potentially high

5.1 Υβριδικά DSRC-Cellular δίκτυα

Για τις επικοινωνίες οχημάτων έχουν προταθεί υβριδικές λύσεις που εκμεταλλεύονται τα οφέλη τόσο της DSRC όσο και των κυψελωτών δικτύων, όπως φαίνεται στο παρακάτω σχήμα.



Εικόνα 5.1 - V2X επικοινωνίες σε υβριδικό DSRC - cellular αστικό σενάριο. [36]

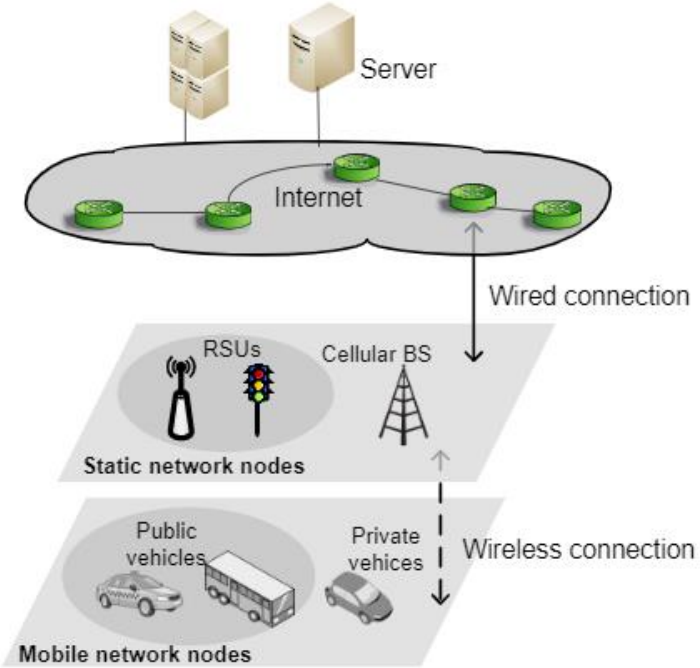
Τα οφέλη από τη χρήση των δύο τεχνολογιών είναι τα ακόλουθα καθώς ένα κυψελωτό δίκτυο μπορεί να λειτουργήσει ως:

- Backup ασφαλείας όταν τα δεδομένα του οχήματος σε V2V επικοινωνίες χαθούν ή δεν καταφέρουν να παραδοθούν σε ένα αραιό δίκτυο.
- ένα δίκτυο πρόσβασης στο internet
- ένα δίκτυο κορμού για μηνύματα ελέγχου

Για παράδειγμα, τα περισσότερα πρωτόκολλα ad-hoc routing που προτείνονται για DSRC, βασίζονται στη συλλογή πληροφοριών οχήματος (π.χ. πληροφορίες τοποθεσίας GPS, κατάσταση της κυκλοφορίας οχημάτων κ.λπ.) για τη βελτίωση της απόδοσής τους. Όταν αυτές οι πληροφορίες είναι σπάνιες ή δεν μπορούν να φτάσουν σε κόμβους/αναμεταδότες, π.χ. λόγω κατακερματισμού του δικτύου, τα πρωτόκολλα δρομολόγησης ad-hoc δεν μπορούν να λειτουργήσουν. Σε αυτήν την περίπτωση, τα κυψελωτά δίκτυα μπορούν να χρησιμοποιηθούν για να γεφυρώσουν το κενό του κατακερματισμένου τμήματος του δικτύου ή μπορούν να βασιστούν πλήρως σε αυτά. Επίσης, οι ολοένα αναπτυσσόμενοι σταθμοί βάσης σε αστικές πόλεις, αυτοκινητόδρομους και αγροτικές περιοχές παρέχουν μια βάση για πρόσβαση στο internet εντός του οχήματος, υποστηρίζοντας διάφορες εφαρμογές ψυχαγωγίας. Εκτός από τη βελτίωση που μπορεί να προσφέρει ένα κυψελωτό δίκτυο στις επικοινωνίες V2X, ένα μέρος από το φάσμα του DSRC μπορεί να αξιοποιηθεί ευκαιριακά από τα κυψελωτά δίκτυα όταν οι απαιτήσεις της κινητής τηλεφωνίας κορυφώνεται και η κίνηση των V2X δεδομένων πέφτει κατακόρυφα. [36]

5.1.1 Υβριδική αρχιτεκτονική

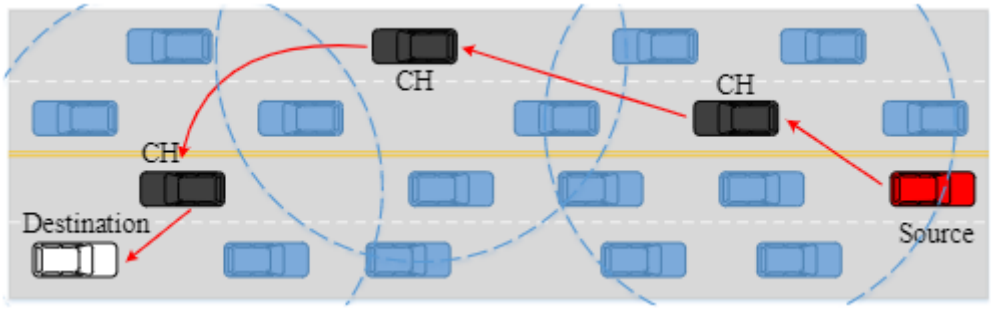
Σε ένα υβριδικό κυψελωτό/DSRC δίκτυο, οι κόμβοι είναι είτε στατικοί, δηλαδή, σταθμοί βάσης και RSU είτε κινητοί δηλαδή οχήματα. Τους στατικούς και τους κινητούς κόμβους μπορούμε εννοιολογικά να τους κατατάξουμε σε hierarchical ή flat αρχιτεκτονική. Στην hierarchical αρχιτεκτονική, η χρήση της κυψελωτής/DSRC τεχνολογίας για επικοινωνίες V2X περιορίζεται σε κόμβους δικτύου που ανήκουν σε συγκεκριμένα hierarchical levels. Για παράδειγμα, τα δημόσια οχήματα, όπως τα λεωφορεία και τα ταξί, μπορεί να ανήκουν σε ένα συγκεκριμένο ιεραρχικό επίπεδο, ενώ τα υπόλοιπα ιδιωτικά οχήματα μπορεί να τοποθετούνται σε χαμηλότερο επίπεδο της ιεραρχίας. Σε αυτήν την υβριδική αρχιτεκτονική δύο επιπέδων, ένα δημόσιο όχημα είναι εξοπλισμένο με δύο διεπαφές. Μία για πρόσβαση στο κυψελωτό δίκτυο και η άλλη για να επικοινωνεί με άλλα ιδιωτικά οχήματα (σε χαμηλότερο ιεραρχικό επίπεδο) μέσω της τεχνολογίας DSRC. Ένα τέτοιο κυψελωτό/DSRC δίκτυο έχει μια fixed hierarchical αρχιτεκτονική, αφού οι κόμβοι που ανήκουν σε κάθε επίπεδο της ιεραρχίας είναι προεπιλεγμένοι και δεν αλλάζουν με το χρόνο. Από την άλλη πλευρά, σε μια δυναμική ιεραρχία, οι κόμβοι δεν διαφοροποιούνται αρχικά με βάση τον τύπο τους και θεωρούνται ομοιογενείς. Στη συνέχεια, κατά τη λειτουργία του δικτύου, τα ιεραρχικά επίπεδα δημιουργούνται δυναμικά και ενημερώνονται με βάση τις διακυμάνσεις στην τοπολογία του δικτύου, όπως η αλλαγή της κυκλοφορίας κ.λπ.



Σχήμα 5.1 - Κόμβοι δικτύου σε υβριδική DSRC - cellular αρχιτεκτονική. [36]

Ένας τρόπος για να επιτευχθεί μια δυναμική ιεραρχία είναι χρησιμοποιώντας ένα σχήμα clustering των κόμβων, το οποίο ομαδοποιεί τους κοντινούς κόμβους σε ένα σύνολο που ονομάζεται cluster. Κάθε cluster έχει cluster head (CH) που είναι υπεύθυνο για τη διατήρηση του cluster και τη διαχείριση των πόρων του δικτύου του. Οι υπόλοιποι κόμβοι ονομάζονται cluster members (CM) και ένα CM μπορεί να ανήκει σε πολλαπλά

clusters. Το CH μπορεί να επιλέξει μερικά από τα CM του ως gateway κόμβους που διευκολύνουν τις inter-cluster επικοινωνίες μεταξύ γειτονικών clusters. Σε μια τέτοια αρχιτεκτονική, τα CH και τα gateways δημιουργούν μια δυναμική ιεραρχία που μπορεί να χρησιμοποιηθεί για τη μετάδοση πληροφοριών προς/από το κυψελωτό δίκτυο. Για παράδειγμα, ένας CH μπορεί να κατεβάσει δημοφιλές περιεχόμενο βίντεο από τους σταθμούς βάσης και να το μεταδώσει με χρήση DSRC στα CM του. Επιπλέον, τα CH και τα gateways μπορούν να συγκεντρώνουν πληροφορίες που συλλέγονται από τα CM τους πριν τις μεταδώσουν στους σταθμούς βάσης, μειώνοντας έτσι το φορτίο κίνησης δεδομένων V2X στο κυψελωτό δίκτυο. Ενώ μια fixed ιεραρχία παρέχει μια απλή και αμετάβλητη στο χρόνο αρχιτεκτονική, δεν είναι ευέλικτη και στιβαρή στη δυναμική του δικτύου (π.χ. αποσυνδέσεις και κατακερματισμός) και μερικές φορές είναι δύσκολο να εφαρμοστεί, σαν μια αρχιτεκτονική που βασίζεται σε δημόσια όχηματα αλλά βρίσκεται σε αστικό περιβάλλον όπου τα δημόσια οχήματα είναι αραιά. Από την άλλη πλευρά, μια δυναμική ιεραρχία που βασίζεται σε clusters έχει ευελιξία στις παραλλαγές του δικτύου, αλλά ο σχηματισμός και η διατήρηση των cluster κόμβων απαιτεί συνεχή ανταλλαγή μηνυμάτων, η οποία μπορεί να αυξηθεί σημαντικά σε ένα δυναμικό δίκτυο οχημάτων. Επομένως, ο τρόπος σχηματισμού σταθερών clusters που διαρκούν για μεγάλο χρονικό διάστημα είναι ένα σημαντικό ζήτημα που πρέπει να ληφθεί υπόψη κατά την υιοθέτηση ενός κυψελωτού δικτύου DSRC που βασίζεται σε clusters.



Σχήμα 5.2 - Σχήμα δρομολόγησης βασισμένο σε clustering. [9]

Σε αντίθεση την hierarchical αρχιτεκτονική, σε ένα flat κυψελωτό/DSRC δίκτυο, η χρήση κυψελών ή τεχνολογίας DSRC δεν περιορίζεται σε μια συγκεκριμένη ομάδα κόμβων. Εναλλακτικά, η επιλογή της τεχνολογίας που θα χρησιμοποιηθεί για τις επικοινωνίες V2X θα πρέπει να βασίζεται στον τύπο των δεδομένων που μεταδίδονται ή σε ορισμένες μετρήσεις απόδοσης, οι οποίες αντικατοπτρίζουν το QoS, στον φόρτο κίνησης των δεδομένων ή την κάλυψη δικτύου. Για παράδειγμα, η μετάδοση των πακέτων ελέγχου μπορεί να περιορίζεται στο κυψελωτό δίκτυο ενώ η προώθηση των δεδομένων σχετικά με την κίνηση να επιτυγχάνεται με χρήση DSRC. Όταν η τεχνολογία που θα χρησιμοποιηθεί επιλέγεται με βάση τις μετρήσεις απόδοσης, οι κόμβοι θα πρέπει να λαμβάνουν updates τόσο για το DSRC όσο και για το κυψελωτό δίκτυο (π.χ. διαθέσιμο bandwidth και connectivity) και η απόφαση να βασίζεται στα κριτήρια του δικτύου. [36]

5.1.2 Διαχείριση της κινητικότητας

Η διαχείριση της κινητικότητας είναι ένα σημαντικό ζήτημα στο σχεδιασμό υβριδικών DSRC/κυψελωτών δικτύων για επικοινωνίες V2X. Σε αντίθεση με τα παραδοσιακά ad-hoc δίκτυα κινητής τηλεφωνίας, η υψηλή κινητικότητα κόμβων σε δίκτυα οχημάτων μπορεί να προκαλέσει συχνές αλλαγές στην τοπολογία του δικτύου και κατακερματισμό. Επίσης, οι αστικοί δρόμοι και οι αυτοκινητόδρομοι είναι πολύ ευαίσθητοι στις διακυμάνσεις της πυκνότητας των οχημάτων κατά τη διάρκεια της ημέρας. Επιπλέον, σε μια αστική περιοχή με πολλά κτίρια και ψηλούς πύργους, οι επικοινωνίες V2X μπορούν να έχουν διακοπτόμενη συνδεσιμότητα λόγω εξασθένισης και σκίασης. Επιπλέον, οι υψηλές ταχύτητες των οχημάτων, σε αυτοκινητόδρομους, μπορούν να προκαλέσουν χωροχρονικές διακυμάνσεις στην τοπολογία του δικτύου, οι οποίες επηρεάζουν άμεσα την απόδοση του δικτύου. Για παράδειγμα, σε μια cluster υβριδική κυψελωτή/DSRC αρχιτεκτονική, η κινητικότητα του οχήματος μπορεί να επηρεάσει σημαντικά τη σταθερότητα των cluster κόμβων λόγω της επίδρασής της στη ένωση και τη διάσπαση των clusters, προκαλώντας στον έλεγχο των clusters υψηλό overhead. Ως αποτέλεσμα, η κινητικότητα των οχημάτων επιφέρει τεχνικές δυσκολίες στη διατήρηση των V2V και V2I συνδέσεων. Ως εκ τούτου, καθώς τα οχήματα μετακινούνται εντός και εκτός των περιοχών κάλυψης άλλων οχημάτων, RSU και σταθμών βάσης αλλάζει και το point of attachmen (PoA). Έτσι η διαχείριση κινητικότητας των οχημάτων στοχεύει στο να παρέχει απρόσκοπτη επικοινωνία μέσω αποτελεσματικών στρατηγικών παράδοσης (handover strategies) και σχημάτων επιλογής δικτύου (network selection schemes) .

5.1.3 Στρατηγικές παράδοσης (handover)

Δεδομένου ότι τα οχήματα είναι πάντα σε κίνηση, το handover μεταξύ οχημάτων και υποδομής στις V2I επικοινωνίες είναι αναγκαίο. Υπάρχουν λοιπόν δυο στρατηγικές παράδοσης – handovers:

- *Horizontal Handover* – όταν ένα session μετάδοσης δεδομένων μεταφέρεται από ένα PoA σε ένα άλλο, αλλά στο ίδιο δίκτυο (χρησιμοποιώντας την ίδια τεχνολογία πρόσβασης).
- *Vertical Handover* – όταν ένα session μετάδοσης δεδομένων μεταφέρεται από ένα PoA σε ένα άλλο, αλλά σε διαφορετικό δίκτυο (χρησιμοποιόντας διαφορετικής τεχνολογίας πρόσβασης).

Για παράδειγμα, ένα horizontal handover απαιτείται για τη μεταφορά Video Streaming session ενός οχήματος από ένα RSU σε ένα άλλο RSU καθώς το όχημα κινείται εντός της περιοχής κάλυψής του. Από την άλλη πλευρά, ένα vertical handover απαιτείται για τη μεταφορά Video Streaming session από μια RSU σε ένα σταθμό βάσης. Δεδομένου ότι διαφορετικές τεχνολογίες πρόσβασης έχουν διαφορετικά χαρακτηριστικά (π.χ frequency band, διαθέσιμο bandwidth, διαμόρφωση και coding schemes), το vertical handover έχει μια πιο απαιτητική διαδικασία σε σύγκριση με το horizontal handover. Ο βασικός πυλώνας για την συνεργασία κυψελωτών/DSRC δικτύων βασίζεται σε μια σωστή handover στρατηγική που διαχειρίζεται αποτελεσματικά τις συνεχής αλλαγές των μεταδόσεων από τη μία τεχνολογία πρόσβασης στην άλλη με όσο το δυνατόν

χαμηλότερη απώλεια πακέτων και handover latency. Κάποιοι από τους λόγους για handover είναι οι παρακάτω:

- Αποσυνδέσεις λόγω μετακίνησης των κόμβων έξω από το εύρος επικοινωνίας
- Υποβάθμιση της ποιότητας του σήματος λόγω της κινητικότητας, της εξασθένισης του καναλιού ή των παρεμβολών.
- Διαθεσιμότητα πολλών δικτύων στον ίδιο χρόνο – χώρο, καθιστώντας κάποια δίκτυα πιο ελκυστικά σε σχέση με άλλα όσον αφορά το κόστος χρέωσης ή το διαθέσιμο bandwidth (π.χ. στις επικαλυπτόμενες περιοχές κάλυψης των σταθμών βάσης και RSUs).

Ωστόσο, για επικοινωνίες V2X που δεν περιλαμβάνουν πρόσβαση στο internet, όπως το broadcast μηνυμάτων ασφαλείας V2V ή η διανομή περιεχομένου σε V2I, μια λύση για τη διαχείρισης της κινητικότητας θα πρέπει να λαμβάνει υπόψη τη μεταφορά των δεδομένων μεταξύ διαφορετικών τεχνολογιών πρόσβασης και διαφορετικών τύπων επικοινωνιών (V2V/V2I). Για παράδειγμα, η μετάδοση μηνυμάτων ασφαλείας από οχήματα και RSU μπορεί να εναλλάσσεται μεταξύ εκπομπών που βασίζονται σε DSRC και eMBMS, με τρόπο που εγγυάται την αξιόπιστη και έγκαιρη παράδοση κάθε μηνύματος ασφαλείας σε όλους τους κόμβους.

5.1.4 Σχήματα επιλογής δικτύου

Γενικά, υπάρχουν διάφοροι παράγοντες που μπορούν να πυροδοτήσουν ένα handover. Η επιλογή του δικτύου (network selection) είναι η διαδικασία λήψης της απόφασης για handover. Ένα handover μπορεί να είναι user centric ή network centric.

Το user centric handover περιλαμβάνει:

- *Οικονομικό κόστος* – οι υπηρεσίες κινητής τηλεφωνίας επί του παρόντος είναι διαθέσιμες στους χρήστες με τέλη συνδρομής (δηλ. προγράμματα δεδομένων), ενώ τα δίκτυα που βασίζονται σε DSRC είναι πιθανό να είναι δωρεάν, ειδικά για εφαρμογές που σχετίζονται με την ασφάλεια.
- *Παροχή QoS* – το QoS του χρήστη βασίζεται σε μετρήσεις όπως το end to end delay, η απώλεια πακέτων, το throughput και άλλες απαιτήσεις για συγκεκριμένες εφαρμογές, όπως η ποιότητα του βίντεο σε video streaming και online gaming.

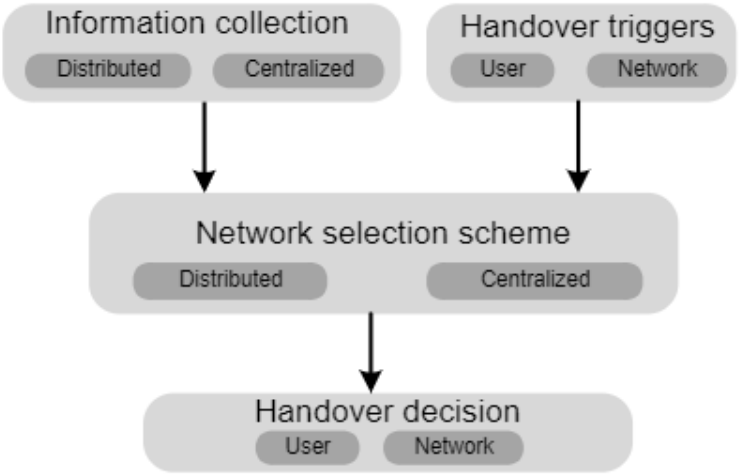
Το network centric handover περιλαμβάνει:

- *Data traffic priority* – η κίνηση των δεδομένων των οχημάτων χωρίζεται σε κατηγορίες διαφορετικών προτεραιοτήτων.
- *Load balancing* – μεταξύ σταθμών βάσης και RSU ανάλογα με τις δυνατότητές τους.
- *Fairness quarantees* – για διαφορετικούς χρήστες.
- *Network throughput maximization* – είναι ο κύριος λόγος που μπορεί να ενεργοποιηθεί ένα handover καθώς μεγιστοποιεί την ισχύ του δικτύου για να

υποστηρίξει τις απαιτήσεις των χρηστών όσον αφορά το διαθέσιμο bandwidth και το απαιτούμενο latency.

Το network selection scheme μπορεί να χρησιμοποιήσει user centric, network centric ή έναν συνδυασμό και τον δυο handovers για να ορίσει ένα αλγόριθμο που θα αποφασίζει εάν θα πρέπει να γίνει ή όχι ένα handover. Θα πρέπει να σημειωθεί ότι απαιτείται μια χαρτογράφηση QoS μεταξύ διαφορετικών τεχνολογιών πρόσβασης. Για παράδειγμα, οι προτεραιότητες των μηνυμάτων για τα οχήματα που ορίζονται στο πρότυπο IEEE1609.4 θα πρέπει να αντιστοιχιστούν στα πρότυπα της κυψελωτής τεχνολογίας για να διατηρηθεί το αναμενόμενο επίπεδο παροχής QoS. [36]

Οι πληροφορίες των user και network centric πρέπει να συλλέγονται και να παρέχονται ως είσοδος για το network selection scheme προκειμένου να αποφασιστεί εάν θα πρέπει να ξεκινήσει ή όχι ένα handover. Τα user και network centric δηλαδή είναι απλά μετρήσεις που οδηγούν στην απόφαση για το αν θα γίνει handover. Η διαδικασία συλλογής των πληροφοριών που σχετίζονται με το handover μπορεί να είναι distributed ή centralized. Στην distributed προσέγγιση, κάθε κόμβος μπορεί να βασιστεί στις received signal strength (RSS) πληροφορίες από διαφορετικά δίκτυα εντός της εμβέλειάς του ως δείκτη για την ικανότητα των δικτύων να υποστηρίξουν τις απαιτήσεις τους για QoS. Από την άλλη πλευρά, στην centralized προσέγγιση, μια οντότητα του δικτύου μπορεί να είναι υπεύθυνη για τη συλλογή και την επεξεργασία πληροφοριών που σχετίζονται με το handover, για παράδειγμα, συλλέγοντας πληροφορίες οχημάτων και μεταφορτώνοντάς τες σε ένα cloud ή έναν κεντρικό ελεγκτή μέσω των σταθμών βάσης ή των RSU. [36]



Σχήμα 5.3 - Η λογική της επιλογής του δικτύου βασισμένη σε handover triggers. [36]

Τα network selection schemes μπορεί να είναι είτε distributed είτε centralized με βάση τον τύπο του αλγορίθμου που εκτελείτε. Για παράδειγμα, στις distributed προσεγγίσεις κάθε όχημα επιλέγει το δικό του δίκτυό με βάση τις τοπικές πληροφορίες, ανεξάρτητα από άλλα οχήματα. Από την άλλη πλευρά, μια centralized προσέγγιση όπως ένα κινητό τηλέφωνο, AR, CH, RSU, BS ή cloud μπορεί να επιλέξει το βέλτιστο δίκτυο βάσει μιας προκαθορισμένης συνάρτησης. Μια τέτοια συνάρτηση μπορεί να ενσωματώνει

διαφορετικούς κανόνες για handover, όπως network load balancing, απαιτήσεις QoS ή διαθέσιμο data rate ανά όχημα και τεχνολογία πρόσβασης. [36]

Μια πλήρως distributed επιλογή δικτύου που βασίζεται σε τοπικές πληροφορίες μπορεί να υποφέρει από κακά handovers λόγω περιορισμένων ή ανακριβών τοπικών πληροφοριών σε ορισμένα οχήματα ως αποτέλεσμα της προσπάθειας κάθε οχήματος να βελτιστοποιήσει τη δική του απόδοση. Από την άλλη πλευρά, ένας κεντρικός controller με καθολικές πληροφορίες μπορεί να εκτελέσει μια πρώιμη πρόβλεψη για το χρόνο που ένα όχημα θα χρειαστεί να κάνει handover. Παρόλο που η συλλογή πληροφοριών για handover και η επιλογή δικτύου μπορεί να είναι centralized, η απόφαση για handover μπορεί να αφεθεί αποκλειστικά στους κόμβους. Αυτή η προσέγγιση δίνει σε κάθε κόμβο την ελευθερία λήψης αποφάσεων έναντι αποσυνδέσεων από τον κεντρικό ελεγκτή που εκτελεί το selection scheme. Σε περίπτωση αποσύνδεσης, ένας κόμβος μπορεί να αποφασίσει να ξεκινήσει ένα handover βάσει τοπικών πληροφοριών (π.χ. RSS από γειτονικές RSU/BS). [36]

5.2 Dynamic Spectrum Sharing

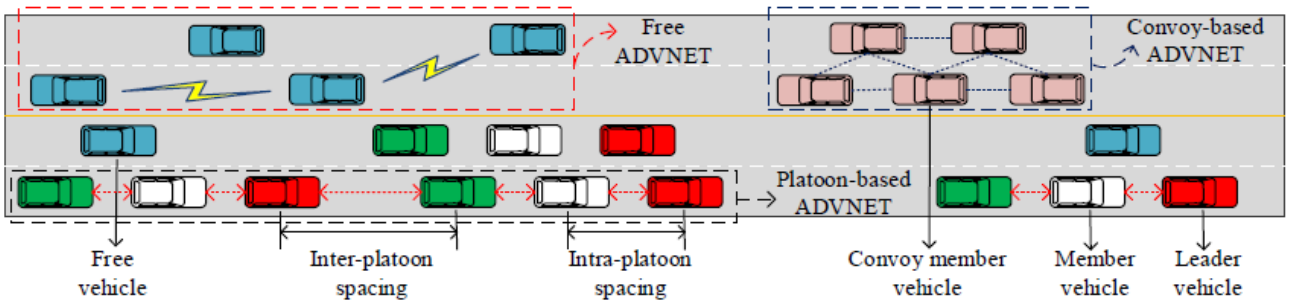
Το αδειοδοτημένο και μη αδειοδοτημένο φάσμα, όπως το κυψελωτό φάσμα, το DSRC και το mmWave μπορούν να συνυπάρχουν δυναμικά για να παρέχουν υψηλής ποιότητας υπηρεσίες στα δίκτυα οχημάτων. Η multi-radio τεχνολογία μπορεί να χρησιμοποιηθεί για το δυναμικό διαμοιρασμό του φάσματος και τη βελτιστοποίηση των πόρων αυτού. Ωστόσο, η υψηλή κινητικότητα των οχημάτων περιορίζει τη διαθεσιμότητα των πόρων και η απόδοση μειώνεται σημαντικά λόγω της ετερογένειας. Έτσι, οι χρήστες πρέπει να συνεργάζονται μεταξύ τους και να μοιράζονται δυναμικά διαφορετικούς πόρους για να βελτιώνουν τη χρήση του φάσματος.

Σε δίκτυο οχημάτων όπου συνυπάρχουν χρήστες κυψελωτού και DSRC στο μη αδειοδοτημένο φάσμα μπορεί να χρησιμοποιηθεί για την υποστήριξη υπηρεσιών V2X. Επιπλέον, οι χρήστες του κυψελωτού δικτύου και οι χρήστες του DSRC μοιράζονται το φάσμα με βάση το energy-sensing. Η συγκεκριμένη μέθοδος επιτρέπει στους χρήστες του κυψελοτού δικτύου και του DSRC να συνυπάρχουν στο ίδιο μη αδειοδοτημένο φάσμα χωρίς data collision κατά τη μετάδοση δεδομένων. [16]

6 AUTOMATED DRIVING VEHICULAR NETWORKS (ADVNETs)

Τα αυτόνομα οχήματα ανοίγουν την πόρτα για την διαχείριση ενός στόλου οχημάτων και την συντονισμένη οδήγηση. Σύμφωνα με τη στρατηγική διαχείρισης της κυκλοφορίας που εφαρμόζεται στα ADVNET, μπορούμε να ταξινομήσουμε τα ADVNET σε: free ADVNET, σε convoy-based ADVNET και platoon-based ADVNET, όπως φαίνεται στο παρακάτω σχήμα. Στα ελεύθερα ADVNET, τα AV κινούνται ανεξάρτητα, υπό τον έλεγχο των αυτοματοποιημένων συστημάτων αυτόματου πιλότου. Στα ADVNET που βασίζονται σε convoy, τα AV που κινούνται σε πολλές λωρίδες και με την ίδια κατεύθυνση ομαδοποιούνται σε ένα convoy, όπου οι πλευρικοί και διαμήκεις έλεγχοι διεξάγονται από όλα τα AV του convoy για να διατηρηθεί η προκαθορισμένη απόσταση μεταξύ των οχημάτων και κατ' επέκταση η ταχύτητά τους. Ένα convoy μπορεί να θεωρηθεί ως επέκταση του platoon. Στα ADVNET που βασίζονται σε platoon, ο κεντρικός έλεγχος γίνεται από το πρώτο όχημα της διμοιρίας και τα AV κινούνται συνεργατικά με την ίδια σταθερή ταχύτητα και διατηρούν μια σταθερή απόσταση μεταξύ των οχημάτων το ένα με το άλλο. Η στρατηγική διαχείρισης που βασίζεται σε platoon μπορεί όχι μόνο να μειώσει την κατανάλωση ενέργειας και τις εκπομπές καυσαερίων ελαχιστοποιώντας την αντίσταση του αέρα των AV, αλλά και να αυξήσει την ασφάλεια οδήγησης με τη συνεργατική οδήγηση μεταξύ των οχημάτων.

Επιπρόσθετα η δομή που βασίζεται σε platoon μπορεί επίσης να εφαρμοστεί στα Manual Driving Vehicular Networks (MDVNET), όπου χειροκίνητα τα οχήματα μπορεί να σχηματίσουν αυθόρμητα ένα platoon, δηλαδή, το ένα όχημα ακολουθεί το άλλο για εύκολη οδήγηση. Ωστόσο, δεδομένου ότι η πιθανότητα πολλά οχήματα χειροκίνητα να κινούνται αυθόρμητα σε platoon είναι πολύ μικρή, οι υπάρχουσες τεχνικές που βασίζονται σε platoon σε MDVNET βασίζονται σε ομάδες, όπου το πρώτο όχημα, δηλ. το κορυφαίο όχημα , ενεργεί ως CH, και τα άλλα, δηλ. οχήματα μέλη, είναι CM.



Εικόνα 6.1 - Απεικόνιση κανονικών και platoon-based ADVETs. [9]

Σε αντίθεση με τα MDVNET τα ADVNET πρέπει να ακολουθούν υψηλότερες απαιτήσεις καθώς οι επιπτώσεις της υψηλής κινητικότητας και του περίπλοκου περιβάλλοντος επικοινωνίας είναι πιο σημαντικές καθώς:

- Οι κόμβοι στα ADVNET, δηλ., τα AV, είναι self-driving χωρίς ανθρώπινες ενέργειες και παρεμβάσεις και έχουν πιο αυστηρούς περιορισμούς καθυστέρησης και υψηλότερες απαιτήσεις ως προς την παράδοσης των πακέτων για την εξασφάλιση της ασφάλειας των AV.
- Απαιτούνται περισσότεροι τύποι πληροφοριών που σχετίζονται με την ασφάλεια των AV, με αποτέλεσμα να προκαλείται μεγαλύτερη φόρτωση δεδομένων στο δίκτυο των ADVNET.
- Τέλος η διαχείριση και η κατανομή των υπολογιστικών πόρων είναι πιο περίπλοκη, καθώς οι πληροφορίες που βασίζονται στους αισθητήρες αλλά και στις επικοινωνίες θα πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία για τα AV.

6.1 Δομές επικοινωνίας

Οι επικοινωνίες οι οποίες χρησιμοποιούνται είναι διαφορετικές ανάλογα με τον τύπο του ADVNET που θα χρησιμοποιηθεί και των τύπο των πληροφοριών που θέλουμε να μεταδώσουμε. Διαφορετικές δομές επικοινωνίας έχουν σχεδιαστεί για διαφορετικούς τύπους ADVNET.

Σε free ADVNET, χρησιμοποιούνται κατά κύριο λόγο οι V2V επικοινωνίες που βασίζονται σε broadcast, δηλαδή κάθε AV εκπέμπει τις πληροφορίες του στα γειτονικά οχήματα. Για παράδειγμα, μπορούμε να χρησιμοποιήσουμε έναν αλγόριθμο αποφυγής συγκρούσεων σε διασταυρώσεις, όπου ένα AV εκπέμπει πληροφορίες σχετικά με τη σύγκρουση σε άλλα AV εντός του εύρους επικοινωνίας του μόλις κινηθεί σε μια κρίσιμη περιοχή, αποφεύγοντας έτσι την ατελείωτη αναμονή στις διασταυρώσεις. Μια άλλη δομή επικοινωνίας είναι η V2I για σενάρια που βασίζονται στην υποδομή, όπου οι υποδομές χρησιμοποιούνται για τη συλλογή και τη μετάδοση πληροφοριών από ή προς τα AV. [9]

Το convoy ADVNET εισήχθη για να υποστηρίξει τη συνεργατική οδήγηση μεταξύ AV σε πολλαπλές λωρίδες. Τουλάχιστον δύο είδη επικοινωνίας χρησιμοποιούνται στα ADVNET που βασίζονται σε convoy. Αυτές είναι οι επικοινωνίες V2V που βασίζεται σε broadcasting για την ανταλλαγή πληροφοριών και τη βελτίωση των συνεργατικών ελιγμών και οι επικοινωνίες V2I για τη βελτίωση της αποτελεσματικότητας της διαχείρισης της κυκλοφορίας. [9]

Για τα ADVNET που βασίζονται σε platoon, εκτός από τη διασφάλιση της ασφαλούς οδήγησης για κάθε AV, μια άλλη σημαντική πρόκληση είναι η διατήρηση της σταθερότητας του platoon, δηλαδή η διασφάλιση ότι τα σφάλματα απόστασης μεταξύ και εντός αυτού (inter και intra platoon) δεν αυξάνονται από το ένα AV στο άλλο και από το ένα platoon στο άλλο. Οι πληροφορίες ταχύτητας και επιτάχυνσης του οχήματος που ηγείτο και των προηγούμενων οχημάτων πρέπει να κοινοποιούνται σε όλα τα οχήματα

μέλη και στο επόμενο όχημα, αντίστοιχα, για τη διατήρηση της σταθερότητας του platoon. Έτσι, οι περισσότερες δομές επικοινωνίες που χρησιμοποιούνται σε platoon ADVNET βασίζονται σε:

- *Intra-platoon communication structure* – χρησιμοποιείται για την ανταλλαγή πληροφοριών μεταξύ AV εντός του ίδιου platoon, μπορεί περαιτέρω να ταξινομηθεί σε τρεις δομές επικοινωνίας.
    - Από αρχηγό σε μέλος (ή από μέλος σε αρχηγό) για κοινή χρήση πληροφοριών μεταξύ του οχήματος που ηγείτο και ενός οχήματος μέλους.
    - Μεταξύ δύο γειτονικών οχημάτων για κοινή χρήση πληροφοριών ταχύτητας και επιτάχυνσης.
    - Multicasting communication για τη βελτίωση της αποτελεσματικότητας των επικοινωνιών σε ένα platoon.

- *Inter-platoon communication structure* – έχει σχεδιαστεί για την ανταλλαγή πληροφοριών μεταξύ AV μέσα σε διαφορετικά platoon, όπως η ανταλλαγή πληροφοριών σύγκρουσης από ένα platoon σε ένα επερχόμενο platoon.

Παρόμοια με τα free ADVNET, η υποδομή παίζει τον ρόλο του ελέγχου στα περισσότερα ADVNET που βασίζονται σε platoon. Ως εκ τούτου, η υποδομή συνήθως αναμεταδίδει πληροφορίες στα AV. [9]

6.2 Τεχνολογίες που εφαρμόζονται στα ADVNETs

Αρκετές τεχνολογίες επικοινωνίας εφαρμόζονται στα ADVNET, συμπεριλαμβανομένων εκείνων που έχουν εφαρμοστεί ευρέως στα MDVNET, π.χ., DSRC, cellular, Wi-Fi και άλλες τεχνολογίες επικοινωνίας μικρής εμβέλειας, όπως infrared και VLC. Μεταξύ αυτών, οι περισσότερες από τις επικοινωνίες μεγάλης εμβέλειας στα ADVNET συνήθως υποστηρίζονται από το DSRC και από τις τεχνολογίες κινητής τηλεφωνίας. Δεδομένου λοιπόν αυτού και ότι το DSRC, οι κυψελωτές επικοινωνίες και το Wi-Fi έχουν αναφερθεί σε προηγούμενα κεφάλαια, θα επικεντρωθούμε στις υπέρυθρες (infrared) και το VLC τα οποία έχουν προταθεί κυρίως για ADVNET, ακόμη και αν μπορούν να χρησιμοποιηθούν και για MDVNET. [9]

6.2.1 Infrared (IR)

Είναι μια από τις πρώτες τεχνολογίες που χρησιμοποιεί φως αόρατο στον άνθρωπο, δηλαδή υπέρυθρο φως, για να επιτρέψει τις ασύρματες επικοινωνίες σε ένα πεδίο με οπτική επαφή (line-of-sight - LOS). Λαμβάνοντας υπόψη ότι οι δρόμοι είναι συνήθως σε ευθεία γραμμή, η επικοινωνία μεταξύ των AV μπορεί να επιτευχθεί με ένα φθηνό υπέρυθρο λέιζερ. Επιπλέον, το μήκος κύματος των υπέρυθρων επικοινωνιών είναι πολύ μικρότερο από άλλες ασύρματες επικοινωνίες, ενώ έχει δυνατότητες για μετάδοση δεδομένων 1Gbps. Επομένως, είναι μια καλή λύση για κοινή χρήση δεδομένων μεγάλου όγκου, όπως πληροφορίες ψυχαγωγίας πολυμέσων μεταξύ AV. Οι υπέρυθρες μπορούν

να χρησιμοποιηθούν για τη μέτρηση της απόστασης εντός platoon για να βοηθήσουν τον έλεγχο της απόστασης μεταξύ των οχημάτων. Ωστόσο, οι υπέρυθρες επικοινωνίες μπορούν να χρησιμοποιηθούν μόνο σε ορισμένες περιπτώσεις, όπως για την επικοινωνία δύο γειτονικών ADVNET που βασίζονται σε platoon, καθώς το υπέρυθρο φως μπορεί να μεταφέρει σε αποστάσεις μικρότερες των 10 μέτρων και δεν διαπερνά εμπόδια. Επιπλέον, οι καιρικές συνθήκες είναι μια άλλη πρόκληση για τις υπέρυθρες επικοινωνίες. Έτσι, προκειμένου να αξιοποιηθούν τα πλεονεκτήματα κατά την αντιμετώπιση σχετικών προκλήσεων, οι υπέρυθρες επικοινωνίες συνδυάζονται πάντα με άλλες τεχνολογίες επικοινωνίας, όπως το DSRC, για την υποστήριξη των εφαρμογών των AV. [9]

6.2.2 Visible Light Communications για ADVNETs

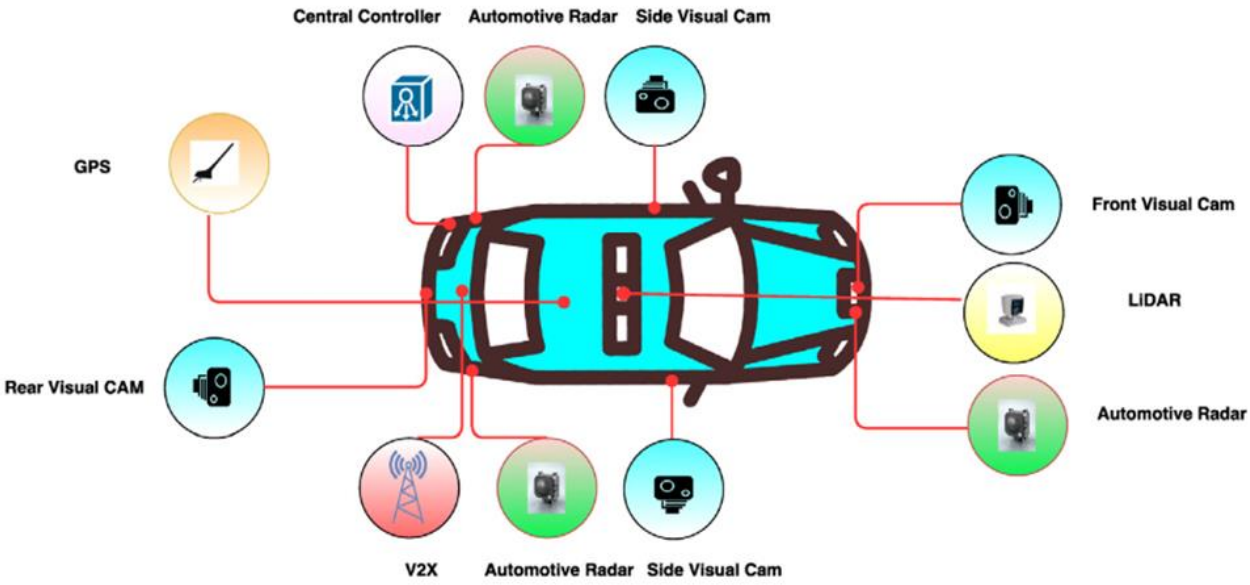
Είναι ένα είδος επικοινωνίας που μεταδίδεται μέσω του ορατού φωτός. Σε σύγκριση με άλλου είδους ασύρματων επικοινωνιών, το VLC έχει τα ακόλουθα σημαντικά πλεονεκτήματα:

- Λειτουργεί σε bandwidth των 360 Terahertz που δεν χρειάζεται άδεια και ανήκει στο φάσμα του ορατού φωτός το οποίο μπορεί να αξιοποιηθεί για ασύρματες επικοινωνίες, αποφεύγοντας παράλληλα παρεμβολές από τα RF σήματα. Ως εκ τούτου, μπορεί να χρησιμοποιήσει το ελεύθερο φάσμα για να υποστηρίξει παράλληλα τη συνεχώς αυξανόμενη ζήτηση των δεδομένων κινητής τηλεφωνίας. Για παράδειγμα, το VLC χρησιμοποιούνται για τη δημιουργία αντιγράφων ασφαλείας των επικοινωνιών DSRC για τη μείωση της απώλειας πακέτων που προκύπτει από συμφόρηση σε σενάρια υψηλής πυκνότητας οχημάτων σε MDVNET.
- Το VLC μπορεί να επιτύχει πολύ υψηλές ταχύτητες μετάδοσης δεδομένων περίπου 100 Mbps στο πρότυπο IEEE 802.15.7.
- Το VLC έχει την δυνατότητα μετάδοσης δεδομένων με χαμηλές ταχύτητες από 1000 έως και 2000 μέτρα. Τυπικά όμως μπορεί να υποστηρίξει δίκτυα οχημάτων με μια εμβέλεια της τάξεις των 50 με 100 μέτρων. Επιπλέον, ένα σημαντικό πλεονέκτημα είναι η αξιοποίηση της υπάρχουσας υποδομής φωτισμού για την υποστήριξη των VLC επικοινωνιών καθώς μπορεί να αναπτυχθεί εύκολα και φθηνά.

Τα παραπάνω πλεονεκτήματα και οι ιδιαιτερότητες του VLC το κάνουν να ταιριάζει καλύτερα στα ADVNET. Για παράδειγμα, η ανταλλαγή πληροφοριών μεταξύ των μελών ενός platoon και η υποστήριξη του ελέγχου ενός platoon. Παρόμοια με τις υπέρυθρες επικοινωνίες, τα σήματα VLC δεν μπορούν να διαπεράσουν τα περισσότερα εμπόδια. Επομένως, μπορούν να χρησιμοποιηθούν μόνο για επικοινωνίες μεταξύ δύο οχημάτων με LOS. Θα πρέπει ωστόσο να σημειωθεί ότι οι τεχνολογίες IR και VLC δεν μπορούν να χρησιμοποιηθούν μόνο για την υποστήριξη επικοινωνιών σε ADVNET αλλά και σε MDVNET. Για παράδειγμα, το IR έχει χρησιμοποιηθεί σε εφαρμογές διοδίων. [9]

6.3 Connected and Automated Vehicles (CAV)

Τα πλήρως αυτοματοποιημένα οχήματα που δοκιμάστηκαν από την Google και την Tesla ως αυτοκίνητα χωρίς οδηγό βασίζονται αποκλειστικά σε δεδομένα που συλλέγονται από τους αισθητήρες τους. Τα ανεπεξέργαστα και ανιχνευόμενα δεδομένα όλων των τομέων υποβάλλονται σε επεξεργασία από τον κεντρικό ελεγκτή, τα αποτελέσματα του οποίου επιτρέπουν στα οχήματα να λάβουν τις δικές τους αποφάσεις οδήγησης. Δεδομένου ότι δεν βασίζονται σε δεδομένα άλλου οχήματος, μπορούν να δουν μέχρι μια ορισμένη απόσταση. Αυτά τα οχήματα είναι αυτοματοποιημένα, αλλά δεν είναι συνδεδεμένα σε κάποιο δίκτυο και έχουν περιορισμένες δυνατότητες ανίχνευσης. Οι Radio Access Technologies μπορούν να επιτρέψουν στα αυτοματοποιημένα οχήματα να επικοινωνήσουν με το δίκτυο οχημάτων και να τους επιτρέψουν να δουν πέρα από τις ικανότητες ανίχνευσής τους σε διάφορες κατευθύνσεις, αξιοποιώντας τα δεδομένα ανίχνευσης ή επεξεργασίας άλλων οχημάτων. Τα αυτοματοποιημένα οχήματα με ενσωμάτωση σε δίκτυα V2X αναφέρονται ως Connected and Automated Vehicles (CAV). Για να αντεπεξέλθουν σε περίπλοκες και διαφορετικές οδικές συνθήκες και να παρέχουν καλύτερη ασφάλεια από ότι σήμερα, τα πλήρως αυτοματοποιημένα οχήματα πρέπει να συνεργάζονται και να βασίζονται σε δεδομένα άλλον CAV. Οι βασικές τεχνολογίες των CAV είναι τα Light Detection and Radars (LiDAR), τα RADAR, οι οπτικές κάμερες, οι εκτιμητές θέσης υψηλής ακρίβειας και οι τεχνολογίες V2X και φαίνονται στο παρακάτω σχήμα. Ο συνδυασμός συνδεσιμότητας και αυτοματισμού μπορεί να βελτιώσει τα επίπεδα ασφάλειας, τον συντονισμό της κυκλοφορίας, την άνεση και την απόδοση σχετικά με την κατανάλωση των καυσίμων. [8]



Σχήμα 6.1 - Εξαρτήματα ενός διασυνδεδεμένου και αυτοματοποιημένου οχήματος. [8]

Ο ρυθμός παραγωγής δεδομένων των αισθητήρων ενός αυτόνομου οχήματος είναι σε TeraByte ανά ώρα οδήγησης. Οι Radio Access Technologies όπως το DSRC, το VLC και το LTE-A (Release 13/14) που υποστηρίζουν ρυθμούς μετάδοσης δεδομένων σε Mbps δεν μπορούν να υποστηρίξουν τον απαιτούμενο ρυθμό μετάδοσης δεδομένων σε Gbps που απαιτούνται για αυτόνομα συνδεδεμένα οχήματα σε V2X δίκτυα. Για παράδειγμα, η ανταλλαγή ασυμπίεστων και ανεπεξέργαστων εικόνων των καμερών θα πρέπει να υποστηρίζεται από μια απόδοση της τάξης των 100-700 Mbps. Ομοίως, σε περίπτωση λήψης χαρτών υψηλής ανάλυσης σε πραγματικό χρόνο από διακομιστή χαρτών, η καθυστέρηση και η απόδοση είναι κρίσιμοι παράγοντες. Έτσι, τα RATs για CAV θα πρέπει να έχουν δυνατότητες που να παρέχουν τις πληροφορίες ή τα δεδομένα με υψηλή ταχύτητα και με αξιόπιστο τρόπο και εντός του καθορισμένου χρονικού ορίου. Αν και οι τεχνικές απαιτήσεις των εφαρμογών CAV δεν έχουν ακόμη καθοριστεί, τα RATs πρέπει να παρέχουν χαμηλές καθυστέρησης, υψηλές αποδόσεις δεδομένων (σε Gbps), υψηλή αξιοπιστία και με υψηλή κινητικότητα. Αυτές οι απαιτήσεις είναι υποχρεωτικές για την ανταλλαγή ανεπεξέργαστων δεδομένων από αισθητήρες και επεξεργασμένων δεδομένων μεταξύ CAV. Αυτές οι επικοινωνίες όχι μόνο επιτρέπουν την ανταλλαγή δεδομένων, αλλά επεκτείνουν και την ικανότητα λήψης καλύτερων αποφάσεων για ασφάλεια. Το mmWave σε εξαιρετικά υψηλές συχνότητες (Extremely High Frequency – EHF) μπορεί να είναι μια από τις λύσεις για επικοινωνία μεταξύ CAV και CAV με την υποδομή και γενικότερα μία από τις μελλοντικές λύσεις για την τεχνολογία των αυτόνομων διασυνδεδεμένων οχημάτων. [8]

7 SECURITY ΓΙΑ V2X ΕΠΙΚΟΙΝΩΝΙΕΣ

7.1 Προκλήσεις και απαιτήσεις ασφαλείας για V2X επικοινωνίες

Το V2X χρησιμοποιείται ευρέως για πολλές εφαρμογές στην επικοινωνία οχημάτων. Αυτές οι εφαρμογές επιβάλλουν διαφορετικές απαιτήσεις ασφαλείας. Παρακάτω θα δούμε τις κύριες προκλήσεις και απαιτήσεις ασφαλείας για τις V2X επικοινωνίες.

Μια από αυτές είναι η δυναμική τοπολογία του δικτύου. Λόγω της υψηλής κινητικότητας στο V2X προκύπτει μια σημαντική πρόκληση που είναι δύσκολο να αντιμετωπιστεί, ιδιαίτερα όσον αφορά τα πλαίσια ασφαλείας. Τα οχήματα σε γενικές γραμμές κινούνται με μεγάλη ταχύτητα, κάνοντας έτσι συνδέσεις για μικρές χρονικές περιόδους. Έτσι, η προσαρμογή των χαρακτηριστικών ασφαλείας με την ποιότητα της επικοινωνίας που επηρεάζεται από τα οχήματα υψηλής ταχύτητας γίνεται ένα δύσκολο έργο.

Η τεχνολογία V2X περιλαμβάνει ένα δίκτυο οχημάτων μεγάλης κλίμακας παγκοσμίως γεγονότος που επιφέρει προβλήματα επεκτασιμότητας του δικτύου. Η διαχείριση του ελέγχου ενός μεγάλου δικτύου μαζί με τα θέματα ασφάλειας όπως η ανταλλαγή πιστοποιητικών κ.λπ. είναι αρκετά απαιτητική διαδικασία. Οι τεχνικές ασφαλείας που χρειάζονται προγενέστερες πληροφορίες σχετικά με οχήματα/κόμβους που συμμετέχουν, δεν είναι κατάλληλες για δίκτυα οχημάτων. [60]

Ακόμα η ετερογένεια των δικτύων, προκύπτει από την υλοποίηση διαφορετικών δικτύων στην υποδομή ανά τον κόσμο. Ως εκ τούτου, οι κατασκευαστές οχημάτων θα εφαρμόσουν τεχνικές με βάση τις πολιτικές ασφάλειας και απορρήτου της αντίστοιχης χώρας. Έτσι, είναι προφανές ότι ο συγχρονισμός μεταξύ των ειδικών χαρακτηριστικών ασφαλείας που υιοθετούνται από διαφορετικούς κατασκευαστές για V2X τεχνολογίας είναι δύσκολο να επιτευχθεί.

Ένα ακόμα ζήτημα είναι η καθυστέρηση στις επικοινωνίες V2X η οποία μπορεί να οφείλεται σε διάφορα ζητήματα, όπως για παράδειγμα, ποιες πληροφορίες συλλέγονται, ποια δεδομένα πρέπει να υποβληθούν σε επεξεργασία, τι πρέπει να μεταδοθεί και να ληφθεί. Επομένως, όλοι οι παράγοντες που σχετίζονται με το latency θα πρέπει να αντιμετωπιστούν έτσι ώστε οι κρίσιμες καταστάσεις ασφάλειας να αντιμετωπίζονται σε πραγματικό χρόνο.

Ένα V2X δίκτυο επικοινωνίας θα πρέπει να μπορεί να ιεραρχεί τα δεδομένα που λαμβάνονται από εκατοντάδες κόμβους. Η επεξεργασία των δεδομένων θα πρέπει να λαμβάνει υπόψη τις τεχνικές προτεραιοτήτων, προσωρινής αποθήκευσης και ουράς για τη διασφάλιση μιας αποτελεσματικής σύνδεσης. Τα δεδομένα που λαμβάνονται από κρίσιμους τομείς για την ασφάλεια πρέπει να αντιμετωπίζονται με ύψιστη προτεραιότητα, ώστε να αποφεύγονται προβλήματα στη λειτουργία του δικτύου.

Οι επικοινωνίες οχημάτων στο μέλλον θα πρέπει να υποστηρίζουν εφαρμογές διαφόρων ειδών και συναφών υπηρεσιών. Για την ενεργοποίηση αυτών των υπηρεσιών, τα οχήματα θα πρέπει να μεταδίδουν κρίσιμα δεδομένα, όπως για

παράδειγμα, η ταυτότητα του οχήματος, που απαιτεί μέγιστη ασφάλεια για να γίνει αποδεχτεί από το υπόλοιπο τηλεπικοινωνιακό σύστημα.

Οι επιθέσεις σε V2X επικοινωνίες κατηγοριοποιούνται σε δύο τύπους:

- Attacks on the System
- Attacks on the User

Παραδείγματα επιθέσεων στον χρήστη μπορούν να επιφέρουν κυκλοφοριακή συμφόρηση, ατυχήματα ή μείωση της εμπιστοσύνης του χρήστη στο σύστημα λόγω αναξιόπιστων μηνυμάτων. Οι επιθέσεις στο σύστημα αποτελούνται από παρακολούθηση της τοποθεσίας για συγκεκριμένα οχήματα ή τη δημιουργία ψευδών αναφορών από ένα όχημα.

Η διασφάλιση λοιπόν της εμπιστοσύνης των χρηστών είναι μια σημαντική πρόκληση που πρέπει να ξεπεραστεί. Είναι αλήθεια ότι η αγορά δεν επιθυμεί οχήματα που είναι επιρρεπή σε ζητήματα απορρήτου ή που παραβιάζουν τους κανόνες κυκλοφορίας. Αποτελεσματικά μέτρα για την προστασία του απορρήτου των χρηστών είναι ο συνδυασμός του ITS με λύσεις που βασίζονται σε public key infrastructure (PKI). Υπάρχουν και τεχνικές που εξαρτώνται από τις ομαδικές υπογραφές (signatures), όπου τα οχήματα που βρίσκονται σε κοντινή απόσταση ομαδοποιούνται μαζί. Έτσι, στην ομαδοποίηση, δημιουργείται μία υπογραφή, με αποτέλεσμα την προστασία της ανωνυμίας (anonymity) και της ιδιωτικής (privacy) των μελών της ομάδας. Ωστόσο, σε ρεαλιστικές συνθήκες, οι προτεινόμενες λύσεις μπορεί να μην είναι αρκετά καλές. [60]

Οι οντότητες που εμπλέκονται στις V2X επικοινωνίες είναι ευάλωτες σε επιθέσεις καθώς δεν παύουν να είναι ασύρματα δίκτυα. Ένα παράδειγμα επίθεσης μπορεί να είναι ένα όχημα να προκαλεί ψευδείς ειδοποιήσεις κινδύνου λόγω επίθεσης στο σύστημά του. Οι ψευδείς ειδοποιήσεις επηρεάζουν όλα τα γύρω οχήματα, την υποδομή και άλλα. Ομοίως, τα μεταδιδόμενα μηνύματα μπορούν να παραποιηθούν για παραπλάνηση και άλλων οχημάτων στο δίκτυο. Αυτά τα παραδείγματα δείχνουν τη σημασία των απαιτήσεων ασφαλείας στις V2X επικοινωνίες για δίκτυα οχημάτων. Λαμβάνοντας υπόψη το μεγάλο εύρος επικοινωνιών που αντιστοιχεί στις V2X επικοινωνίες, είναι προφανές ότι η έκθεση σε επιθέσεις σε αυτά τα δίκτυα είναι πολύ μεγάλη. Η κύριες προκλήσεις αφορούν τον σχεδιασμό ασφαλών πρωτοκόλλων για σωστούς μηχανισμούς ανίχνευσης και άμυνας έναντι επιθέσεων.

Για να αυξηθεί η εμπιστοσύνη των χρηστών, όσον αφορά τις δυνατότητες του V2X, υπάρχει ανάγκη ανάπτυξης αξιόπιστων συστημάτων. Αυτά τα συστήματα πρέπει να ανταποκρίνονται στις ανάγκες των χρηστών με σεβασμό στην ασφάλεια (security), το απόρρητο (privacy), την αξιοπιστία (reliability) και την ακεραιότητα (integrity). Το πρώτο σημαντικό βήμα για την επίτευξη της αξιοπιστίας είναι η σωστή αποτύπωση των απαιτήσεων ασφαλείας. Οι απαιτήσεις ασφαλείας ποικίλλουν ανάλογα με το είδος της επίθεσης. Παρακάτω λοιπόν φαίνονται οι V2X απαιτήσεις ασφαλείας: [60]

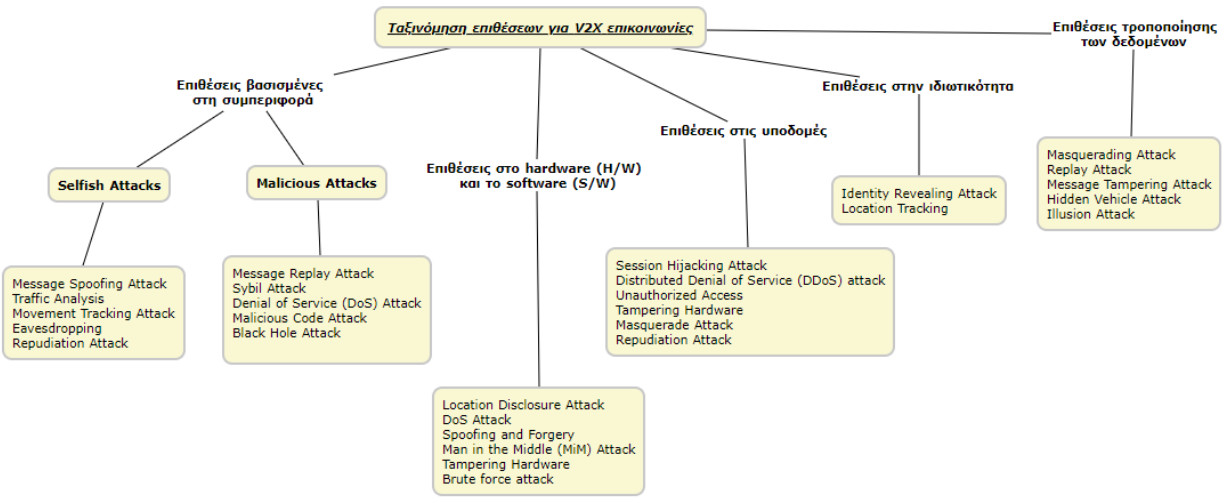
- *Authentication* – εξασφαλίζουμε ότι ένας παραλήπτης έχει παραλάβει ένα μήνυμα από έμπιστο αποστολέα.
- *Integrity* – η ακεραιότητα των πληροφοριών διατηρείται όταν το περιεχόμενο των μηνυμάτων δεν τροποποιηθεί και δεν εκτεθεί σε διαφθορές, ζημιές, καταστροφές, ή άλλες διαταραχές της αυθεντικής του κατάστασης κατά τη μετάδοσή του.
- *Access Control* – εξουσιοδοτεί ένα κόμβο για την εκτέλεση ενεργειών σε δίκτυο που του επιτρέπετε. Χρησιμεύει για την παροχή πρόσβασης σε συγκεκριμένες υπηρεσίες.
- *Confidentiality* – η εμπιστευτικότητα διασφαλίζει την απόκρυψη του περιεχομένου των μηνυμάτων από μη εξουσιοδοτημένη πρόσβαση (άτομο ή σύστημα).
- *Availability* – η διαθεσιμότητα των πληροφοριών λαμβάνει χώρα όταν οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στην πληροφορία χωρίς παρεμβολές ή παρεμποδίσεις.
- *Privacy and Anonymity* – οι επικοινωνίες V2X θα πρέπει να προβλέπουν την προστασία του απορρήτου των χρηστών τους. Τα προσωπικά - ιδιωτικά στοιχεία των χρηστών δεν πρέπει να αποκαλύπτονται. Επομένως, το απόρρητο αναφέρεται στην απόκρυψη πληροφοριών και δεδομένων, ενώ η ανωνυμία θεωρείται ως υποσύνολο του απορρήτου στα δίκτυα οχημάτων.

Οι απαιτήσεις ασφαλείας που απαιτούνται από την 3GPP είναι authentication και authorization, confidentiality και integrity, replay protection και privacy. Το authentication μεταξύ των UE χρησιμοποιεί λύσης ασφαλείας που βασίζονται σε identity ή certificate. Για authentication, πρέπει να χρησιμοποιείται public key cryptography και πιστοποιητικά (certificates). Η μεταφορά δεδομένων μεταξύ των UE και της V2X υποδομής εξαρτάται από το Generic Authentication Architecture (GAA). Το απόρρητο μπορεί να επιτευχθεί με τη χρήση είτε του Pseudonymous Mobile Subscriber ID (PMSI) είτε κρυπτογραφώντας το International Mobile Subscriber Identity (IMSI). Για το Machine Type Communication (MTC), εισήχθησαν βελτιστοποιήσεις στην Έκδοση 10 και πρόσθετες προδιαγραφές προστέθηκαν με την πάροδο των ετών με την ονομασία Cellular IoT στην 3GPP. Τα χαρακτηριστικά του MTC όπως το Power Saving Mode (PSM), το Service Exposure, η παρακολούθηση συσκευών, και οι ομαδικές επικοινωνίες τεκμηριώνονται στο έγγραφο της 3GPP TS 23.682. [60]

7.2 Επιθέσεις σε V2X επικοινωνίες

Στο παρακάτω σχήμα γίνεται μια αναπαράσταση για την ταξινόμηση των επιθέσεων σε V2X δίκτυα σύμφωνα με πέντε κατηγορίες: [60]

- Επιθέσεις βασισμένες στη συμπεριφορά
- Επιθέσεις στο hardware (H/W) και το software (S/W)
- Επιθέσεις στις υποδομές
- Επιθέσεις στην ιδιωτικότητα
- Επιθέσεις τροποποίησης των δεδομένων



Σχήμα 7.1 - Ταξινόμηση επιθέσεων για V2X επικοινωνίες.

7.2.1 Επιθέσεις βασισμένες στη συμπεριφορά

Αυτές οι επιθέσεις βασίζονται στα πρότυπα συμπεριφοράς των χρηστών. Ο στόχος αυτού του τύπου των επιθέσεων είναι να επηρεάσει τη συμπεριφορά των κόμβων. Οι επιθέσεις που βασίζονται σε πρότυπα συμπεριφοράς χωρίζονται σε δύο τύπους: [60]

- Selfish attacks
- Malicious attacks

Selfish attacks

Αυτές οι επιθέσεις αποτελούν μια «εγωιστική» συμπεριφορά όπου οι κόμβοι ενδέχεται να μην προωθούν πακέτα ή να μην εκτελούν λειτουργίες επαλήθευσης. Παραδείγματα τέτοιων επιθέσεων σε V2X επικοινωνίες δίνονται παρακάτω.

Message spoofing attack

Ο attacker σε επιθέσεις πλαστογράφησης παρέχει εσφαλμένες πληροφορίες τοποθεσίας στα οχήματα του δικτύου. Αξίζει να σημειωθεί ότι οι πληροφορίες θέσης του οχήματος πρέπει να είναι ακριβείς στα δίκτυα οχημάτων. Οι ψευδείς πληροφορίες σχετικά με τη θέση του οχήματος μπορεί να οδηγήσουν σε καταστάσεις που είναι επιζήμιες σε τέτοια περιβάλλοντα.

Traffic analysis/movement tracking attack

Σε περιβάλλον οχημάτων, η ανάλυση της κυκλοφορίας ή η επιθέσεις παρακολούθησης της κίνησης αποτελεί απειλή για το απόρρητο των χρηστών καθώς και το απόρρητο των μεταδιδόμενων μηνυμάτων. Είναι μια παθητικής μορφή επίθεση, όπου ο εισβολέας «ακούει» μέσω ενός δικτύου και στη συνέχεια αναλύει τα δεδομένα που συλλέγονται

κατά τη διάρκεια της περιόδου ακρόασης. Τα αποτελέσματα της ανάλυσης δεδομένων χρησιμοποιούνται από τους εισβολείς για περεταίρω επιθέσεις στο μέλλον.

Eavesdropping

Αυτή είναι μια παθητικής μορφή επίθεση, όπου ο εισβολέας ακούει μόνο το μέσο επικοινωνίας χωρίς το θύμα να το γνωρίζει. Σε αυτήν την επίθεση διακυβεύεται η εμπιστευτικότητα των μεταδιδόμενων μηνυμάτων. Αυτή η επίθεση διευκολύνει τη συλλογή ορισμένων χρήσιμων πληροφοριών που μπορεί να βοηθήσουν στην παρακολούθηση του οχήματος.

Repudiation

Αυτή η επίθεση έχει ως αποτέλεσμα την απώλεια tracking events όταν ένας κόμβος αρνείται οποιαδήποτε επικοινωνία.

Malicious attacks

Εδώ, οι εισβολείς δημιουργούν κακόβουλες δραστηριότητες στο δίκτυο, όπως modification και message replays. Οι υπάρχουσες κακόβουλες επιθέσεις σε V2X δίκτυα περιγράφονται παρακάτω. [60]

Message replay attack

Αυτή η επίθεση είναι σχεδόν κοινή σε όλους τους τύπους δικτύων. Σε αυτήν την επίθεση, ένα ήδη σταλμένο πακέτο μηνυμάτων αναπαράγεται σε τακτά χρονικά διαστήματα από τον εισβολέα. Ένα παράδειγμα μπορεί να είναι η επανάληψη των πλαισίων beacon από τον εισβολέα για τον εντοπισμό της θέσης των οχημάτων.

Sybil attack

Σε αυτή την επίθεση, ο εισβολέας δημιουργεί πολλά οχήματα στο δρόμο με την ίδια ταυτότητα. Έτσι τα άλλα οχήματα στο δρόμο εξαπατούνται και έτσι καταλήγουν να στέλνουν μηνύματα σε ψεύτικους παραλήπτες.

Denial of Service (DoS) attack

Οι επιθέσεις DoS περιλαμβάνουν μια ομάδα επιθέσεων που στοχεύουν τη διαθεσιμότητα του δικτύου. Αυτές οι επιθέσεις ενδέχεται να επηρεάσουν σοβαρά την απόδοση των εφαρμογών στα δίκτυα οχημάτων. Οι επιτιθέμενοι αυτού του τύπου μπορεί να είναι είτε εσωτερικοί είτε εξωτερικοί. Ο πρωταρχικός στόχος των εισβολέων έγκειται στη διακοπή της επικοινωνίας καθώς και στην παρενόχληση των υπηρεσιών έτσι ώστε να μην είναι διαθέσιμες σε νόμιμους χρήστες. Ένα παράδειγμα επίθεσης DoS είναι η επίθεση flooding, όπου ο εισβολέας πλημμυρίζει σκόπιμα το κανάλι ελέγχου με μεγάλο όγκο μηνυμάτων. Έτσι, οι OBU και τα RSU δεν είναι σε θέση να χειριστούν τόσο τεράστιο όγκο μηνυμάτων, με αποτέλεσμα διαταραχές στο δικτύου.

Malicious code attack

Σε αυτόν τον τύπο επίθεσης, τα κακόβουλα οχήματα μεταδίδουν πληροφορίες με τη μορφή κώδικα, όπως ιούς, με στόχο την επίθεση στο σύστημα του οχήματος ή στους σταθμούς βάσης. Οι κακόβουλοι κώδικες έχουν επίσης τη δυνατότητα να καταστρέφουν εφαρμογές στα οχήματα και να παρεμποδίζουν τις υπηρεσίες των οχημάτων.

Black hole attack

Σε αυτόν τον τύπο επίθεσης, ο εισβολέας λαμβάνει πακέτα από τα δίκτυα αλλά αρνείται τη συμμετοχή στη δρομολόγηση των λαμβανόμενων δεδομένων. Αυτό προκαλεί την άκαιρη ενημέρωση των πινάκων δρομολόγησης. Επομένως, οι νόμιμοι χρήστες εμποδίζονται στο να λάβουν σημαντικές πληροφορίες. Γενικά ο εισβολέας δηλώνει ότι είναι μέρος του δικτύου, ενώ στην πραγματικότητα δεν είναι.

7.2.2 Επιθέσεις στο hardware (H/W) και το software (S/W)

Αυτή η ενότητα ασχολείται με επιθέσεις που είναι επικίνδυνες όσον αφορά το hardware και το software των διαφορετικών μονάδων ελέγχου στα όχημα.

Man in the Middle (MiM) attack

Αυτή η επίθεση μπορεί να επιτευχθεί σε διαφορετικά περιβάλλοντα (V2V/V2I/V2X) στο δίκτυα οχημάτων. Δηλαδή ο εισβολέας μπορεί να τοποθετηθεί μεταξύ δύο επικοινωνούντων κόμβων, μεταξύ αποστολέα και παραλήπτη. Επίσης, ο εισβολέας αναλαμβάνει τον έλεγχο στην επικοινωνία των δύο οχημάτων που επικοινωνούν. Η επίθεση MiM παραβιάζει ζητήματα ακεραιότητας, αυθεντικότητας στα δίκτυα οχημάτων.

Brute force attack

Αυτός ο τύπος επίθεσης είναι δύσκολο να εκτελεστεί σε δίκτυα οχημάτων, λόγω σύντομων χρόνων σύνδεσης ωστόσο μπορεί να επηρεάσει τέτοια δίκτυα. Για παράδειγμα, η επίθεση μπορεί να λάβει χώρα στην προσπάθεια ταυτοποίησης του οχήματος στο δίκτυο μέσω μιας συγκεκριμένης διαδικασίας αναζήτησης. Η εμπιστευτικότητα των μηνυμάτων και οι διαδικασίες επαλήθευσης ταυτότητας ενδέχεται να παρεμποδιστούν από την πραγματοποίηση τέτοιων επιθέσεων.

7.2.3 Επιθέσεις στις υποδομές

Αυτές οι επιθέσεις αποτελούν κίνδυνο για διάφορες υποδομές που σχετίζονται με τη λειτουργία των τεχνολογιών V2X. Παραδείγματα τέτοιων επιθέσεων είναι η μη εξουσιοδοτημένη πρόσβαση.

Session hijacking attack

Στην αρχή κάθε νέου session, πραγματοποιείται έλεγχος ταυτότητας, έτσι ο επιτιθέμενος ελέγχει το session μεταξύ κόμβων.

Distributed Denial of Service (DDoS) attack

Η επίθεση DDoS είναι ένας τύπος επίθεσης DoS. Στην επίθεση DDoS, ένας κύριος εισβολέας ενεργεί ως διαχειριστής επίθεσης μαζί με άλλους εισβολείς. Οι επιθέσεις DDoS προκαλούν κυρίως διαταραχές στο δίκτυο πλημμυρίζοντάς το με μηνύματα.

Unauthorized access

Σε αυτές τις επιθέσεις, γίνεται βίαιη επίθεση στην πρόσβαση των υπηρεσιών του δικτύου από κακόβουλες οντότητες χωρίς να έχουν το δικαίωμα. Αυτή η επίθεση οδηγεί τελικά σε ατυχήματα, ζημιές ή κατασκοπεία ευαίσθητων δεδομένων.

Tampering hardware

Αυτή η επίθεση είναι αποτέλεσμα ορισμένων κακόβουλων υπαλλήλων της αυτοκινητοβιομηχανίας, οι οποίοι, κατά τη διάρκεια της συντήρησης, προσπαθούν να παραβιάσουν το hardware. Ο στόχος αυτής της επίθεσης είναι είτε να αποκτήσει πρόσβαση είτε να τροποποιήσει κάποια δεδομένα στο όχημα.

Masquerade attack

Ο εισβολέας χρησιμοποιεί μια έγκυρη ταυτότητα για να κρυφτεί. Προσπαθεί να δημιουργήσει black hole ή να παράξει μη έγκυρα μηνύματα που φαίνεται να λαμβάνονται από αυθεντικούς κόμβους. Ένας εισβολέας μπορεί να παρουσιαστεί ως όχημα έκτακτης ανάγκης και να αναγκάσει άλλα οχήματα στο δρόμο να αλλάξουν λωρίδα ή να μειώσουν την ταχύτητά τους.

7.2.4 Επιθέσεις στην ιδιωτικότητα

Αυτές οι επιθέσεις παραβιάζουν το απόρρητο των οδηγών, των οχημάτων και των χρηστών στα δίκτυα οχημάτων. Παραδείγματα τέτοιων επιθέσεων απορρήτου σε V2X δίκτυα μπορεί να είναι επίθεση αποκάλυψης της ταυτότητας και εντοπισμού της τοποθεσίας.

Identity revealing attack

Σε αυτήν την επίθεση, η ταυτότητα του χρήστη ενός οχήματος παραβιάζεται με αποτέλεσμα τα προσωπικά στοιχεία του ιδιοκτήτη να εκτεθούν, γεγονός που μπορεί να επιφέρει περεταίρω συνέπειες στο μέλλον.

Location tracking

Αυτός ο τύπος επίθεσης παρακολουθεί τη θέση ενός οχήματος καθώς και τη διαδρομή που ακολουθεί το όχημα για μια συγκεκριμένη χρονική περίοδο.

7.2.5 Επιθέσεις τροποποίησης των δεδομένων

Αυτές οι επιθέσεις αλλάζουν ή τροποποιούν τα δεδομένα κατά τη μετάδοση. Επομένως, η ακεραιότητα των δεδομένων τίθεται σε κίνδυνο. Αν και αυτός ο τύπος επίθεσης προσβάλει επικοινωνίες V2I και V2V, είναι πιο διαδεδομένο να συμβεί σε V2I επικοινωνίες. Παραδείγματα επιθέσεων σχετικά με την παραβίαση της εμπιστευτικότητας των δεδομένων σε δίκτυα οχημάτων είναι masquerading attack, replay attack, message tampering attack, hidden vehicle attack και illusion attack.

Message tampering attack

Αυτή η επίθεση έχει ως αποτέλεσμα την τροποποίηση, την αλλαγή, τη διαγραφή ή την ανακατασκευή δεδομένων που υπάρχουν ήδη. Ο εισβολέας ξεκινά αυτήν την επίθεση τροποποιώντας ή ανακατασκευάζοντας ένα συγκεκριμένο μέρος του μηνύματος για να επιτύχει τις κακόβουλες προθέσεις του.

Hidden vehicle attack

Σε αυτό το είδος επίθεσης, δημιουργούνται ψευδείς alarm θέσης από κρυφά οχήματα που οδηγούν σε ατυχήματα. Το GPS δεν λειτουργεί και, ως εκ τούτου, οδηγούμαστε στην εξαπάτηση των πληροφοριών του GSP που είναι επίσης γνωστό ως GPS spoofing.

Illusion attack

Αυτή η επίθεση επηρεάζει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων στις επικοινωνίες οχημάτων καθώς δημιουργούνται ψευδή δεδομένα από τους εισβολείς. Τα ψευδή δεδομένα που δημιουργούνται από τους εισβολείς έχουν πρόσβαση στο δίκτυο και βασίζονται στην αλληλεπίδραση με τους οδηγούς για τη λήψη μη θεμιτών αποφάσεων. Ο εισβολέας συνδέεται στο δίκτυο, με αποτέλεσμα να δυσκολεύεται ο εντοπισμός του.

7.3 Τεχνικές ασφαλείας για V2X επικοινωνίες

7.3.1 Κρυπτογραφία συμμετρικού κλειδιού

Η συμμετρική κρυπτογραφία θεωρείται λιγότερο ευέλικτη σε σύγκριση με την ασύμμετρη όσον αφορά τις δυνατότητες για τον έλεγχο ταυτότητας. Όμως, όσον αφορά τα overhead υπολογισμού και επικοινωνιών, η κρυπτογραφία συμμετρικού κλειδιού θεωρείται εξαιρετικά αποτελεσματική. Η κρυπτογραφία συμμετρικού κλειδιού χρησιμοποιεί έναν Hash Message Authentication Code (HMAC) για σκοπούς ελέγχου ταυτότητας. Το μήνυμα με ένα μυστικό κλειδί γίνονται hash από αυτόν που υπογράφει το συνολικό μήνυμα. Το μυστικό κλειδί πρέπει να είναι γνωστό σε αυτών που δέχεται το μήνυμα για την επαλήθευση του MAC, ακολουθώντας την ίδια διαδικασία ανάποδα. Επομένως, κάθε κόμβος που διαθέτει μυστικό κλειδί είναι ικανός να παράγει και να επαληθεύει MAC. Η κρυπτογραφία συμμετρικού κλειδιού σε V2X επικοινωνίες παρέχει

το πλεονέκτημα της σύντομης παραγωγής και επαλήθευσης μηνυμάτων, με το ελάχιστο overhead ασφαλείας. Ένα παράδειγμα μπορεί να είναι κάθε OBU να διαθέτει ένα μυστικό κλειδί που θα είναι προεγκατεστημένο στο όχημα ή να έχει ένα σύνολο κοινόχρηστων μυστικών κλειδιών. Ένα άλλο παράδειγμα είναι, οι RSU να αναλαμβάνουν την ευθύνη για την επαλήθευση της γνησιότητας των μηνυμάτων που λαμβάνονται από τα οχήματα. Μετά την επαλήθευση, τα RSU στέλνουν πίσω ειδοποιήσεις στα αντίστοιχα οχήματα ότι το μήνυμα που έλαβαν είναι γνήσιο. Με την ανίχνευση ενός RSU, τα οχήματα ξεκινούν τη σύνδεση με το συγκεκριμένο RSU. Αυτό ακολουθεί μια διαδικασία αμοιβαίας επαλήθευσης ταυτότητας με το όχημα και το RSU εγκαθιστά ένα κοινό μυστικό κλειδί με το όχημα. Τα RSU διαμοιράζονται με τα οχήματα ένα ID (pseudo - ID) που βοηθά το RSU να αναγνωρίσει το όχημα που έστειλε το μήνυμα και να επαληθεύσει τον έλεγχο ταυτότητας του μηνύματος. Κάθε όχημα παράγει ένα HMAC με τη βοήθεια συμμετρικού κλειδιού. Στη συνέχεια, το όχημα εκπέμπει το μήνυμα, το οποίο υπογράφεται με συμμετρικό HMAC. Το μήνυμα εκπομπής που λαμβάνεται από άλλα οχήματα επαληθεύεται χρησιμοποιώντας την επαλήθευση ελέγχου ταυτότητας μέσο του RSU. Το RSU έχει τη δυνατότητα ελέγχου ταυτότητας του μηνύματος καθώς διαθέτει τα κλειδιά κρυπτογράφησης HMAC που διαμοιράζονται τα άλλα οχήματα. [60]

7.3.2 Διατήρηση της ιδιωτικότητας

Μια άλλη τεχνική που χρησιμοποιείται για την ασφάλεια των επικοινωνιών στα οχήματα είναι η διατήρηση της ιδιωτικότητας. Αυτή η τεχνική περιλαμβάνει τη διατήρηση της ιδιωτικότητας τόσο του οδηγού όσο και του οχήματος. Ένα παράδειγμα είναι η ανάπτυξη ενός μηχανισμού άμυνας που βασίζεται σε ψευδώνυμα, για τη διασφάλιση του απορρήτου του χρήστη και της ιχνηλάτησεις του οχήματος. Ο αμυντικός μηχανισμός για την διατήρησης της ιδιωτικότητας βασίζεται στον έλεγχο ταυτότητας με χρήση ψευδωνύμου. Η διατήρηση του απορρήτου με βάση το ψευδώνυμο αποτελείται από δύο βήματα: δημιουργία ψευδωνύμου και έλεγχος ταυτότητας ψευδωνύμου. Ο έλεγχος ταυτότητας ψευδώνυμου αφορά ουσιαστικά τη διαφύλαξη του απορρήτου. Ένα όχημα χρειάζεται να ενημερώνει τα διαπιστευτήριά του αρκετά συχνά για τη διατήρηση του απορρήτου. Τα ψευδώνυμα παρέχουν την απόκρυψη της πραγματικής ταυτότητας των οχημάτων, έτσι ώστε τα γειτονικά οχήματα και τα RSU να μην μπορούν να αποκρυπτογραφήσουν τον αποστολέα ενός συγκεκριμένου μηνύματος. Έτσι οι στόχοι ασφάλειας του απορρήτου, της ιχνηλάτησεις, μαζί με την αποτελεσματική επικοινωνία ικανοποιούνται από αυτή την τεχνική. [60]

7.3.3 Έλεγχος ταυτότητας

Οι μέθοδοι ελέγχου ταυτότητας των μηνυμάτων για την ασφάλεια των επικοινωνιών V2X περιλαμβάνουν διάφορες τεχνικές, όπως η χρήση υπογραφών προσανατολισμένων σε ομάδες, πρωτόκολλα ελέγχου ταυτότητας και άλλα. Ένα παράδειγμα είναι μια αποκεντρωμένη τεχνική ελέγχου ταυτότητας, όπου κάθε RSU είναι υπεύθυνο για τη διατήρηση και τη διαχείριση των οχημάτων εντός του εύρους του ως

ομάδα. Τα οχήματα που εντάσσονται στην ομάδα, μεταδίδουν μηνύματα από όχημα σε όχημα ανώνυμα. Τα μηνύματα V2V επαληθεύονται άμεσα από τα οχήματα της ίδιας ομάδας αλλά και από άλλες γειτονικές ομάδες. Παρέμβαση τρίτου εισάγεται εάν εντοπιστεί ψευδές μήνυμα. Σε αυτήν την περίπτωση, τα οχήματα ζητούν από το RSU να στείλει ένα μυστικό κλειδί μέλους χωρίς να το γνωρίζουν άλλα οχήματα. Το RSU με την σειρά του μεταδίδει κρυφά το μυστικό κλειδί μέλους στα οχήματα της ομάδας. Στη συνέχεια, τα οχήματα μπορούν να στέλνουν μηνύματα ανώνυμα ως μέλη της ομάδας. Τα μέλη της ομάδας έχουν τη δυνατότητα να υπογράψουν εκ μέρους της ομάδας με τη βοήθεια ομαδικών υπογραφών. Η υπογραφή επαληθεύεται από κάθε μέλος της ομάδας, με τη βοήθεια του δημόσιου κλειδιού της ομάδας. Όμως η ταυτότητα του υπογράφοντος δεν αποκαλύπτεται σε κανέναν εκτός από τον manager της ομάδας. Τα περισσότερα μηνύματα ωστόσο δεν χρειάζεται να προωθηθούν, καθώς αφορούν γενικές πληροφορίες για την κατάσταση οδήγησης. Τα οχήματα στέλνουν μόνο σημαντικά μηνύματα αφού τα υπογράψουν. Στη συνέχεια, τα μηνύματα προωθούνται σε άλλα οχήματα εντός της περιοχής κάλυψης του συγκεκριμένου οχήματος και στους γείτονές του. Το σύστημα είναι ισχυρό καθώς, εάν συμβεί κάποια βλάβη σε RSU, επηρεάζονται μόνο τα οχήματα που καλύπτονται από την περιοχή των συγκεκριμένων RSU. [60]

8 ΑΝΟΙΧΤΑ ΘΕΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΗ ΕΡΕΥΝΑ

Σε αυτό το κεφάλαιο παρουσιάζονται κάποια ανοιχτά ζητήματα, ερευνητικές προκλήσεις καθώς και μελλοντικές κατευθύνσεις έρευνας για δίκτυα οχημάτων. Η αντιμετώπιση αυτών των ζητημάτων είναι σημαντική για επιτυχημένες και αποτελεσματικές επικοινωνίες σε δίκτυα οχημάτων και θα αποτελέσουν σημείο ερευνητικού ενδιαφέροντος τα απόμενα χρόνια.

8.1 Θέματα ασφαλείας

Μια σειρά από τομείς που σχετίζονται με τα δίκτυα οχημάτων και έχουν ιδιαίτερο χαρακτηριστικό την ασφάλεια εμφανίζονται παρακάτω ως μελλοντικές κατευθύνσεις έρευνας.

Ασφάλεια και διαλειτουργικότητα συσκευών

Ένας σωστός συγχρονισμός μεταξύ των διαφορετικών προδιαγραφών που έχουν αναπτυχθεί από τους διάφορους κατασκευαστές αυτοκινήτων για τη διασφάλιση της διαλειτουργικότητας των συσκευών είναι απαραίτητος. Για την διασφάλιση της ασφάλειας και της διαλειτουργικότητας των συσκευών προτείνεται η δημιουργία κοινοπραξιών στον χώρο της αυτοκινητοβιομηχανίας οι οποίες να έχουν στόχο την ανάπτυξη κοινών τεχνικών προδιαγραφών. Με τον τρόπο αυτό θα αυξηθεί η διαλειτουργικότητα και η ασφάλεια των οχημάτων ανεξαρτήτου της χώρας που κινούνται. Ακόμα η δημιουργία κοινών προτύπων μέσω των κοινοπραξιών θα βοηθήσει και στην μείωση του κόστους των οχημάτων καθώς οι δοκιμές προτύπων θα είναι κοινές από τα περισσότερα μέλη της βιομηχανίας.

Πολιτικές ασφαλείας

Ένα πολύ σημαντικό ζήτημα είναι οι πολιτικές που ορίζουν βασικούς κανόνες για την υποστήριξη των μονάδων που επηρεάζουν την ασφάλεια των οχημάτων. Για παράδειγμα πρέπει να υπάρχουν ελάχιστες απαιτήσεις ασφαλείας για τις DSRC μονάδες. Έτσι προτείνεται ο καθορισμός συγκεκριμένων συνθηκών υπό τις οποίες ανακαλείται μια μονάδα DSRC και πώς γίνεται η επανεγκατάσταση μετά την ανάκληση της. Αυτές οι πολιτικές ασφαλείας θα πρέπει να περιλαμβάνουν περιορισμένη χρήση των εκπομπών των μονάδων ασφαλείας για απροσδιόριστους λόγους και την εκπλήρωση ελάχιστων απαιτήσεων ασφαλείας.

Προστασία κλειδιών

Η αυτοκινητοβιομηχανία έχει προσπαθήσει να λύσει το θέμα της προστασίας των κλειδιών ασφαλείας με μια τελική οντότητα εντός του οχήματος. Η προστασία και η αξιοπιστία της τελικής οντότητας καθώς και των κλειδιών που χρειάζονται για την υπογραφή διατηρείται με χρήση ασφαλούς εκκίνησης του οχήματος, ασφαλών ενημερώσεων και αυτοελέγχων. Αυτό το θέμα αποκτά μεγαλύτερη σημασία με την

ολοένα και μεγαλύτερη ανάπτυξη των τεχνολογιών για τα συνδεδεμένα οχήματα. Λαμβάνοντας υπόψη τα παραπάνω και κυρίως την προστασία της τελικής οντότητας εντός του οχήματος προτείνεται η χρήση κάποιου κωδικού ασφαλείας ή βιομετρικού χαρακτηριστικού για την επιβεβαίωση ότι ο οδηγός είναι εξουσιοδοτημένος. Έτσι αν ο χρήστης δεν έχει την απαραίτητη εξουσιοδότηση δεν θα μπορεί το όχημα να συμμετέχει στο δίκτυο συνδεδεμένων οχημάτων. Εδώ πρέπει να σημειωθεί ότι η πιστοποίηση όσο και η αξία του κάθε χαρακτηριστικού ασφαλείας κρίνονται με βάση το Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών των ΗΠΑ (US Federal Information Processing Standard) για την επίτευξη του καλύτερου αποτελέσματος.

Ασφάλεια των δεδομένων

Η αύξηση του αριθμού των αυτοκινήτων που συνδέονται ασύρματα στα δίκτυα συνδεδεμένων οχημάτων, ανοίγει ένα νέο κεφάλαιο σχετικά με την πρόσβαση των χάκερ για κακόβουλες ενέργειες στα δεδομένα των αυτοκινήτων. Επομένως, για τη διασφάλιση της ασφάλειας των δεδομένων σε οχήματα, θα πρέπει να είναι ικανά να αντιμετωπίζουν διάφορες επιθέσεις. Μια λύση που προτείνεται είναι πλήρη ενσωμάτωση των πρωτοκόλλων ασφαλείας των ασυρμάτων δικτύων στα δίκτυα των οχημάτων και η χρήση credential για την είσοδο στα συστήματα του οχήματος. Ωστόσο προβλέπεται ότι ο αριθμός των συνδεδεμένων αυτοκινήτων θα φτάσει τα 240 εκατομμύρια παγκοσμίως με αποτέλεσμα η απουσία ενός καθολικού προτύπου για την ασφάλεια των συνδεδεμένων οχημάτων μπορεί να περιπλέξει την ανάπτυξη χαρακτηριστικών ασφαλείας στο μέλλον έτσι θα ήταν πάλι βολικό η δημιουργία κοινοπραξιών.

8.2 Θέματα παράδοσης και αδιάλειπτης συνδεσιμότητας

Το ITS είναι πλέον αναπόσπαστο κομμάτι των έξυπνων πόλεων. Για την παροχή αξιόπιστων υπηρεσιών ITS χρειαζόμαστε μια αδιάλειπτη συνδεσιμότητα με χαμηλές καθυστερήσεις, υψηλό throughput και υψηλή απόδοση στην παράδοση των πακέτων. Τα οχήματα πρέπει να έχουν τη δυνατότητα να εκτελούν εφαρμογές και να χρησιμοποιούν υπηρεσίες συνεχόμενα. Η παροχή μια αξιόπιστης συνδεσιμότητας σε ένα δίκτυο οχημάτων με γρήγορες τοπολογικές αλλαγές, ποικίλες ταχύτητες οχημάτων, μεταβλητή πυκνότητα είναι μεγάλες προκλήσεις και οι επικοινωνίες V2V και V2I υποφέρουν από τις υψηλές απώλειες πακέτων, τις υψηλές καθυστερήσεις και το χαμηλό throughput. Ένα βασικό ερώτημα λοιπόν που προκύπτει είναι πως θα μπορέσουμε να έχουμε οχήματα με συνεχή συνδεσιμότητα και υποστήριξη Quality of Service.

Η πρώτη προσέγγιση είναι η ανάπτυξη RSU για την εξασφάλιση μιας αδιάλειπτης συνδεσιμότητας. Ωστόσο η ανάπτυξη μεγάλου αριθμού RSU δεν είναι τόσο συμφέρουσα προσέγγιση λόγω του υψηλού κόστους κατασκευής και συντήρησης. Ακόμα η ανάπτυξη πολλών RSU μπορεί να προκαλέσει παρεμβολές. Επομένως, αυτή η προσέγγιση πρέπει να διερευνηθεί στο άμεσο μέλλον έτσι ώστε να είμαστε σίγουροι για τον αν πρόκειται για μια συμφέρουσα ή όχι λύση.

Μια δεύτερη προσέγγιση στην οποία έχουμε ήδη αναφερθεί είναι η συνεχείς πρόσβαση των οχημάτων σε οποιοδήποτε δίκτυο (ετερογενείς δίκτυα). Για να γίνει αυτό πρέπει να γίνουν τα εξής:

- Να εξοπλιστούν οι OBU των οχημάτων με πολλαπλές κάρτες διεπαφής δικτύου για να παρέχεται σύνδεση με τις διαθέσιμες τεχνολογίες ασύρματης πρόσβασης, όπως το IEEE 802.11p, το LTE-A και το 5G.
- Τα ετερογενή δίκτυα οχημάτων θα πρέπει να μπορούν να συνδυάζουν τεχνολογίες όπως το IEEE 802.11p και των δικτύων κινητής τηλεφωνίας χρησιμοποιώντας διάφορες μεθόδους για την παροχή συνδέσεων οπουδήποτε στο δίκτυο.
- Θα πρέπει να υλοποιηθούν ασφαλείς και αδιάλειπτες επιλογές συνδεσιμότητας με γρήγορη παράδοση (horizontal και vertical handover σε ετερογενή δίκτυα).

Όσον αφορά την παράδοση σε δίκτυα οχημάτων, λόγω της γρήγορης και μεγάλης κινητικότητα τους, τα οχήματα μπορούν να κάνουν πολύ συχνά handover μεταξύ διαφορετικών δικτύων. Είναι επιθυμητό λοιπόν ένα όχημα να παραμένει πάντα συνδεδεμένο με το καταλληλότερο σύστημα. Οι παραδοσιακοί μηχανισμοί handover για κυψελωτά δίκτυα δεν είναι κατάλληλοι για τα ετερογενή δίκτυα οχημάτων καθώς το handover των οχημάτων είναι πιο συχνό από τους χρήστες κινητής τηλεφωνίας. Η υλοποίηση μιας παράδοσης περιλαμβάνει τρία στάδια, την έναρξη της παράδοσης, την απόφαση της παράδοσης και την εκτέλεση της παράδοσης. Η επιλογή των κατάλληλων μετρήσεων και μεθόδων για την απόφαση της παράδοσης σε ένα δίκτυο οχημάτων είναι ένας σημαντικός τομέας έρευνας. Ο κύριος στόχος της παράδοσης είναι η διατήρηση της συνδεσιμότητας, η διατήρηση του QoS και ο περιορισμός των περιττών μεταβιβάσεων. Επομένως, η απόφαση για handover εξαρτάται, από διάφορες μετρήσεις όπως η κατάσταση του καναλιού, το φορτίο του δικτύου, το SINR, η τοποθεσία και η ισχύς του λαμβανόμενου σήματος. Δεδομένου ότι το handover παίζει ζωτικό ρόλο στις επικοινωνίες των οχημάτων, θεωρείτε πολύ σημαντικό για το μέλλον των επικοινωνιών σε οχήματα να βρεθούν πιο γρήγοροι και αξιόπιστοι μηχανισμοί παράδοσης για ετερογενή περιβάλλοντα. Το αν η παραδοσιακή προσέγγιση μπορεί να εφαρμοστεί στο δίκτυο οχημάτων ή όχι και ο τρόπος εφαρμογής των αποφάσεων παράδοσης στο ετερογενές δίκτυο οχημάτων παραμένει ένα ανοιχτό ερευνητικό πρόβλημα. Έτσι αυτό το θέμα παραμένει σίγουρα στο επίκεντρο τις έρευνας για τα επόμενα χρόνια καθώς μπορεί να συνδυαστεί με το machine learning για καλύτερα αποτελέσματα.

8.3 Μηχανική μάθηση για επικοινωνίες οχημάτων

Οι πρόσφατες εξελίξεις στην τεχνητή νοημοσύνη έχουν θεωρηθεί ως η κύρια δύναμη πίσω από τις τάσεις για την εξέλιξη της αυτόνομης οδήγησης και των αναδυόμενων ADVNET. Η τεχνητή νοημοσύνη έχει μελετηθεί ευρέως για έξυπνες μεταφορές. Η μηχανική μάθηση, ειδικότερα, έχει προταθεί γενικά για ασύρματα δίκτυα [76] και για την αντιμετώπιση των ειδικών απαιτήσεων των επικοινωνιών σε οχήματα [75]. Για παράδειγμα, μια μέθοδος βασισμένη σε deep learning μπορεί να συλλέγει πληροφορίες

ροής κυκλοφορίας από πολλές πηγές δεδομένων και από μια μεγάλη ποικιλία έξυπνων εφαρμογών που σχετίζονται με τις μεταφορές [74]. Ακόμα υπάρχουν προσεγγίσεις βαθιάς ενισχυτικής μάθησης (deep reinforcement learning) για δυναμική κεντρικοποιημένη ενορχήστρωση (dynamic centralized orchestration) δικτύων, caching, computing για δίκτυα οχημάτων, [75] ενώ έχει αναπτυχθεί και ένα σχήμα διαχείρισης πόρων των οχημάτων, που βασίζεται επίσης στη βαθιά ενισχυτική μάθηση [76]. Επιπλέον, έχει επινοηθεί μια στρατηγική vertical handoff βασισμένη σε Q-learning για ετερογενή δίκτυα οχημάτων, [77] η οποία διασφαλίζει απρόσκοπτη διαχείριση της κινητικότητας χωρίς προηγούμενη γνώση στην handoff συμπεριφορά του δικτύου.

Παρά τις πολύ μεγάλες δυνατότητες εφαρμογής της μηχανικής μάθησης σε δίκτυα οχημάτων, εξακολουθούν να υπάρχουν αρκετές προκλήσεις. Για παράδειγμα, τα δίκτυα οχημάτων παρουσιάζουν σημαντικές διαφορές σε σχέση με τις εφαρμογές που χρησιμοποιείται παραδοσιακά η μηχανική μάθηση όπως computer vision και speech recognition, τοπολογίες δικτύου, traffic flow κ.λπ.. Ο τρόπος αποτελεσματικής εκμάθησης και πρόβλεψης τέτοιων δυναμικών περιβαλλόντων όπως αυτό τον οχημάτων για την επίτευξη αξιόπιστων επικοινωνιών εξακολουθεί να είναι ένα ανοιχτό ζήτημα. Επιπλέον, τα δεδομένα δημιουργούνται και αποθηκεύονται φυσικά σε πολλές διαφορετικές οντότητες στα δίκτυα οχημάτων, π.χ. οχήματα, RSUs και remote clouds. Είναι ιδιαίτερα ενδιαφέρον να διερευνηθεί εάν οι παραδοσιακοί κεντρικοποιημένοι αλγόριθμοι μηχανικής μάθησης μπορούν να προσαρμοστούν ώστε να λειτουργούν αποτελεσματικά σε κατανεμημένα δίκτυα. Ειδικότερα, πρέπει να ληφθούν υπόψη τα έξοδα που προκύπτουν από την ανταλλαγή και τη συλλογή πληροφοριών για τη λήψη ευφυών αποφάσεων σε δίκτυα οχημάτων με δυνατότητα εκμάθησης. Ένα άλλο σημαντικό στοιχείο είναι ότι οι περισσότεροι σύγχρονοι αλγόριθμοι μηχανικής μάθησης με τεχνολογίες τελευταίας γενιάς και ειδικότερα η βαθιά μάθηση, περιλαμβάνουν έντονη χρήση εγκαταστάσεων με υπολογιστές υψηλής απόδοσης, όπως μονάδες επεξεργασίας γραφικών (GPU). Τέτοια ισχυρή υπολογιστική ισχύς δεν μπορεί να είναι διαθέσιμη σε οχήματα, έτσι ισχυροί remote servers θα είναι μάλλον περιορισμένοι. Από τα παραπάνω μπορούμε να βγάλουμε το συμπέρασμα ότι απαιτείται ειδική μεταχείριση για την μείωση της πολυπλοκότητας των αλγορίθμων μάθησης έτσι ώστε να είναι εφαρμόσιμοι σε δίκτυα οχημάτων. Μια πρόταση που θα μπορούσε να διερευνηθεί εκτενέστερα στο μέλλον είναι το αν θα μπορούσαν να λειτουργήσουμε τους αλγόριθμους μηχανικής μάθησης σε κατανεμημένα δίκτυα με την περεταίρω ανάπτυξη του edge computing και του fog computing.

8.4 MillimeterWave και μηχανική μάθηση

Οι mmWave επικοινωνίες παρέχουν υψηλό ρυθμό μετάδοσης δεδομένων σε επικοινωνίες V2X που βασίζονται στο 5G και είναι μια από τις καλύτερες λύσεις για επικοινωνίες οχημάτων αυτή τη στιγμή. Το beamforming όμως παραμένει ακόμα ένα από τα προβλήματα στις mmWave επικοινωνίες για V2X δίκτυα. Το contextual online learning [73] είναι μια πολλά υποσχόμενη λύση. Οι συγγραφείς προτείνουν [73] μια τεχνική γρήγορης μηχανικής μάθησης (fast machine learning - FML), η οποία είναι χαμηλής πολυπλοκότητας και περιέχει ένα αλγόριθμο online μάθησης για τους

mmWave σταθμούς βάσης. Ο αλγόριθμος αυτός επιτρέπει στους mmWava σταθμούς βάσης να μαθαίνουν αυτόματα από προηγούμενες αποφάσεις και συναφείς πληροφορίες. Το FML μπορεί και λαμβάνει υπόψη διάφορα beems με την πάροδο του χρόνου καθώς επίσης και πληροφορίες όπως η κατεύθυνση του οχήματος. Αυτός ο αλγόριθμος online μάθησης μπορεί να εντοπίζει συγκρούσεις δεδομένων για κάθε όχημα καθώς λαμβάνει το σύνολο των δεδομένων από αυτά. Επιπλέον παρέχει αυτόματα μεγαλύτερη κάλυψη σε περιοχές με μεγάλη κίνηση καθώς μεγιστοποιεί την χωρητικότητα του συστήματος.

Ωστόσο, το contextual online learning απαιτεί τεράστιο όγκο περιοδικών δεδομένων λόγω των συναφών πληροφοριών που συλλέγει καθώς και των πληροφοριών τοποθεσίας. Για αυτό το λόγο μελλοντικές έρευνες θα πρέπει να αντιμετωπίσουν τις προκλήσεις που σχετίζονται με τη συλλογή δεδομένων και τοποθεσίας για το contextual online learning σε mmWave επικοινωνίες.

8.5 Διαχείριση μεγάλων δεδομένων

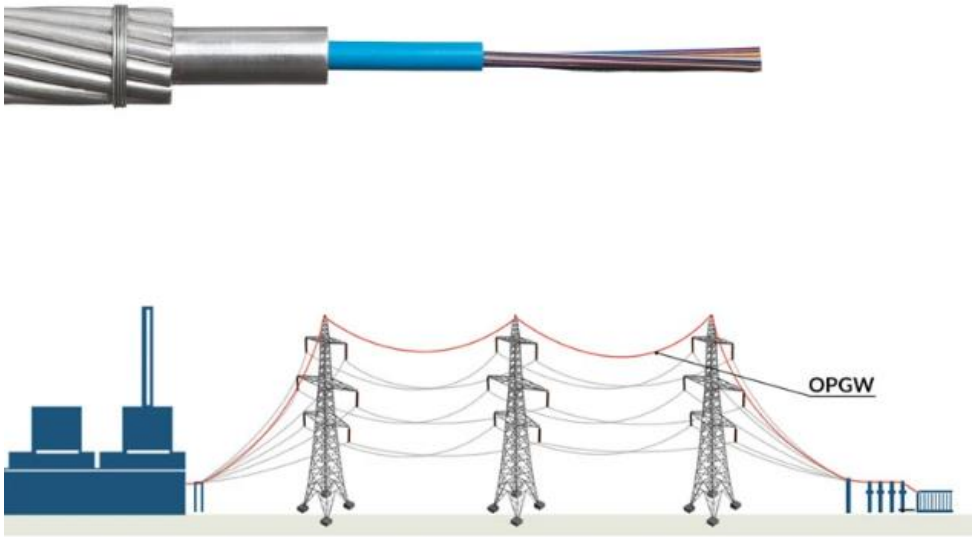
Με εκατομμύρια οχήματα στους δρόμους, ένας τεράστιος όγκος δεδομένων παράγεται από διαφορετικούς συμμετέχοντες στο δίκτυο. Αυτά τα δεδομένα πρέπει να διαχειρίζονται και να συγκεντρώνονται για να μειωθεί η κατανάλωση bandwidth και η μνήμη. Λόγω των ετερογενών χαρακτηριστικών του περιβάλλοντος, τίθενται προκλήσεις ως προς τη διαχείριση των δεδομένων.

Η διαχείριση αυτού του δυναμικού όγκου δεδομένων περιλαμβάνει διάφορες διαδικασίες από τη συλλογή, τη συγκέντρωση, την επικύρωση έως και την μετάδοσή τους. Πράγματι, είναι μια πρόκληση που απαιτεί το σχεδιασμό και την ανάπτυξη έξυπνων πρωτοκόλλων δρομολόγησης, για τη δημιουργία αποτελεσματικής επικοινωνίας και τη βελτίωση της μετάδοσης των δεδομένων μεταξύ των οχημάτων. Απαιτούνται προηγμένες τεχνικές επεξεργασίας και εξόρυξης δεδομένων για τη συλλογή, τη συγκέντρωση, την επεξεργασία και την ανάλυση των δεδομένων σε ετερογενή δίκτυα οχημάτων. Μια πρόταση για περεταίρω έρευνα είναι το cloud computing το οποίο μπορεί να παρέχει ένα αποτελεσματικότερο τρόπο εκμετάλλευσης των πόρων υπολογισμού και αποθήκευσης σε δίκτυα οχημάτων.

8.6 Vehicle-to-Grid (V2G)

Τα smart grids και τα ηλεκτρικά οχήματα Electric Vehicles (EV) κερδίζουν ολοένα και περισσότερο έδαφος τόσο στον ακαδημαϊκό όσο και στον βιομηχανικό τομέα. Υπάρχουν πολλά οφέλη από τη χρήση ηλεκτρικών οχημάτων, όπως, χαμηλότερες εκπομπές άνθρακα μέσω της «πράσινης» επιλογής, μικρότερο κόστος με την ολοένα και μεγαλύτερη διάδοσής τους στο ευρύτερο κοινό και αύξηση της γενικότερης ενεργειακής απόδοσης. Αυτό φαίνεται να το ακολουθεί και η βιομηχανία όπως η Volvo της οποίας ολόκληρη η σειρά οχημάτων που θα κυκλοφορήσει το 2023 θα είναι εξ ολοκλήρου ηλεκτρική. Ως εκ τούτου, η διασύνδεση των οχημάτων στα συστήματα

ηλεκτρικής ενέργειας τόσο για την φόρτισή τους όσο και για την ενσωμάτωση επικοινωνιών πάνω σε αυτά είναι ένα ζήτημα το οποίο έχει να προσφέρει πολλή έρευνα τα απόμενα χρόνια. Μια πολύ ενδιαφέρουσα ερευνητική πρόταση θα μπορούσε να είναι η ταυτόχρονη ανάπτυξη των έξυπνων δικτύων ηλεκτρικής ενέργειας με ενσωματωμένες επικοινωνίες. Τι εννοούμε με αυτό, τα έξυπνα δίκτυα ηλεκτρικής ενέργειας μπορούν να φέρουν αγωγούς όπως ο Optical Ground Wire (OPGW) ο οποίος μπορεί να εξυπηρετήσει δυο σκοπούς. Ένας είναι η μεταφορά δεδομένων μέσο των οπτικών ινών στο εσωτερικό αυτού και δεύτερο να γειώσει τους πυλώνες σε περίπτωση κεραυνού. Θα μπορούσαμε λοιπόν κατά την ανάπτυξη αυτών των δικτύων να ενσωματώναμε RSU επάνω στους πυλώνες ηλεκτρικής ενέργειας. Με τον τρόπο αυτό θα μπορούσαμε να χρησιμοποιήσουμε την οπτική ίνα σαν το core δίκτυο των επικοινωνιών για οχήματα και να αναπτύξουμε ένα δίκτυο με RSU κατά μήκος μεγάλων αυτοκινητόδρομων όπου γίνεται συνήθως η μεταφορά της ηλεκτρικής ενέργειας. Με τον τρόπο αυτό μπορούμε να έχουμε ταυτόχρονα μεταφορά ηλεκτρικής ενέργειας, δίκτυο κορμού με οπτικές ίνες και ανάπτυξη RSU είτε σε σταθμούς φόρτισης οχημάτων είτε επάνω στους πυλώνες. Παρακάτω φαίνεται ένα παράδειγμα OPGW αγωγού σε δίκτυο ηλεκτρικής ενέργειας. Τέλος με την παραπάνω πρόταση μπορούμε να μειώσουμε κατά πολύ το κόστος κατασκευής δικτύων για οχήματα καθώς μπορούμε να εκμεταλλευτούμε αλλά και να αναβαθμίσουμε την υπάρχουσα υποδομή ηλεκτρικής ενέργειας και τις ανερχόμενες κατασκευές σταθμών φόρτισης για ηλεκτρικά οχήματα στους αυτοκινητόδρομους.



Εικόνα 8.1 - OPGW αγωγός σε smart grid. [70]

8.7 Άλλα θέματα και προκλήσεις

Λόγω της τεχνολογίας του self-driving, τα ADVNET μπορεί να θεωρηθούν ως ένας συνδυασμός του cloud computing και του Internet of things (IoT). Το cloud computing παρέχει υπηρεσίες χαρτών (π.χ. χάρτες υψηλής ευκρίνειας) και πληροφορίες σχετικά με τις συνθήκες του δρόμου στα AV για την υποστήριξη μιας ασφαλούς πλοήγησης. Από

την άλλη, οι παράμετροι που διαμορφώνονται σε πραγματικό χρόνο (π.χ. κατεύθυνση, ταχύτητα και επιτάχυνση) των AV προσδιορίζονται με βάση τους αισθητήρες - δυναμικές πληροφορίες γύρω από το δρόμο - του οχήματος και τις πληροφορίες που μεταδίδονται από άλλα οχήματα. Για την ανάπτυξη αυτών των δικτύων και γενικότερα των δικτύων με οχήματα έχει δοθεί μεγάλη βάση στην mmWave τεχνολογία λόγω των πολύ υψηλών συχνοτήτων για την επικοινωνία αυτόνομων οχημάτων.

Υπάρχουν ωστόσο ορισμένα ζητήματα που πρέπει να ληφθούν υπόψη. Οι τεχνολογίες mmWave και VLC έχουν θεωρηθεί ότι υποστηρίζουν δίκτυα οχημάτων, ωστόσο ο τρόπος αντιμετώπισης των πιθανών ζητημάτων που προκαλούνται από την υψηλή κινητικότητα των οχημάτων και τις δύσκολες καιρικές συνθήκες χρειάζεται περαιτέρω διερεύνηση και δοκιμή. Επιπλέον, σε ετερογενή δίκτυα οχημάτων με μία ή και δύο τεχνολογίες επικοινωνίας, η εύρεση ενός κριτηρίου για την επιλογή δικτύου δεν είναι εύκολη δουλειά. Ακόμα, για να επιτευχθεί αποτελεσματικά μια συνεργατική ανταλλαγή δεδομένων για οδήγηση, η διαχείριση των πληροφοριών και ο συνεργατικός έλεγχος θα πρέπει να λαμβάνονται υπόψη σε παγκόσμιο επίπεδο, γεγονός που οδηγεί σε περίπλοκο ζήτημα κατανομής των πόρων, ειδικά σε σενάρια με ετερογενείς απαιτήσεις. Τέλος, με την αύξηση των οχημάτων και της ζήτησης δεδομένων κινητής τηλεφωνίας, ο περιορισμός των πόρων (συμπεριλαμβανομένων των πόρων επικοινωνίας, computing και αποθήκευσης) είναι ένα κρίσιμο ζήτημα. Εκτός από τη διασύνδεση δύο τεχνολογιών επικοινωνίας, μπορεί να συμβάλει και μια τρίτη τεχνολογία επικοινωνίας, πράγμα που καθιστά την κατανομή των πόρων ακόμα πιο περίπλοκη.

9 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το DSRC έκανε την πρώτη εμφάνιση του στις εφαρμογές επικοινωνίας οχημάτων το 1999 από το FCC. Ακόμα και σήμερα με πάνω από 20 χρόνια διαδρομής παραμένει ένα από τα βασικά πρωτόκολλα επικοινωνίας για οχήματα που είναι πολύ αποτελεσματικά για εφαρμογές μικρής εμβέλειας (300m). Για να μελετήσουμε και να κατανοήσουμε τις βασικές τεχνολογίες των V2X επικοινωνιών δόθηκε ιδιαίτερη σημασία και στα σύγχρονα κυψελωτά δίκτυα. Τόσο τα ασύρματα όσο και τα κυψελωτά δίκτυα έχουν τα δικά τους οφέλη και αδυναμίες. Έτσι από την πλευρά τους οι cellular τεχνολογίες είναι πιο κατάλληλες για εφαρμογές όπως ο έλεγχος της κυκλοφορίας και οι εφαρμογές infotainment τα οποία απαιτούν μεγαλύτερες περιοχές κάλυψης.

Όσον αφορά τα κλασικά δίκτυα ad-hoc για οχήματα (VANETs) μπορούν να ανταπεξέλθουν για τις επικοινωνίες από όχημα σε όχημα (V2V) και από όχημα σε υποδομή (V2I) αλλά έχουν αρκετά προβλήματα. Κάποια από αυτά είναι το χαμηλό εύρος ζώνης, οι καθυστερήσεις από άκρο σε άκρο και τα μη ισορροπημένα traffic flows λόγο την δυναμικής κινητικότητας. Αυτά τα προβλήματα μπορούν να ξεπεραστούν με μια υβριδική DSRC-cellular αρχιτεκτονική, την οποία μελετήσαμε, έτσι ώστε να έχουμε πιο αποδοτικά δίκτυα οχημάτων τα οποία διασφαλίζουν αυστηρότερες απαιτήσεις για κρίσιμες εφαρμογές ασφαλείας. Η 5G τεχνολογία με την σειρά της έχει παίξει πολύ σημαντικό ρόλο για την ανάπτυξη αυτών των δικτύων καθώς παρέχει εξαιρετικά χαμηλές καθυστερήσεις, υψηλούς ρυθμούς μετάδοσης δεδομένων και μικρές απώλειες πακέτων. Τα παραπάνω πλεονεκτήματα ικανοποιούν πολλές εφαρμογές ασφαλείας για VANETs οι οποίες έχουν αυστηρές απαιτήσεις. Ωστόσο οι προκλήσεις στα ετερογενή δίκτυα παραμένουν μεγάλες. Μπορεί το 5G να έχει κατακλίσει την αγορά των συμβατικών τηλεπικοινωνιών και το DSRC να υποστηρίζεται από όλα τα σύγχρονα οχήματα αλλά η συνύπαρξη των δυο τεχνολογιών και η διαλειτουργικότητα είναι ένα ζήτημα που επιφέρει πολλή έρευνα ακόμα καθώς όπως είπαμε τα δίκτυα οχημάτων είναι πολύ απαιτητικά λόγω της πολύ δυναμικής τους κατάστασης.

Επιπλέον οι εφαρμογές ασφαλείας στοχεύουν στην βελτιστοποίηση της οδικής ασφάλειας καθώς και μια αποτελεσματικότερη διαχείριση της κυκλοφορίας στέλνοντας προειδοποιητικά μηνύματα στους οδηγούς είτε μέσω της υποδομής είτε μέσω της ανταλλαγής μηνυμάτων από άλλα διασυνδεδεμένα οχήματα. Αυτά τα μηνύματα ωστόσο λειτουργούν σαν υποστήριξη για την απόφαση που θα πάρει ο οδηγός. Δεδομένου ότι αυτά τα μηνύματα ασφαλείας μπορούν να επηρεάσουν την απόφαση του οδηγού και ότι μεταδίδονται σε ένα περιβάλλον ανοιχτής πρόσβασης, είναι πολύ σημαντικό να διασφαλιστεί ότι προέρχονται από ένα νόμιμο χρήστη (όχημα ή υποδομή) και το περιεχόμενο αυτού πρέπει να επαληθεύεται έγκαιρα από τα οχήματα που το λαμβάνουν. Η παροχή αυτών των απαιτήσεων ασφαλείας για εφαρμογές οχημάτων βασίζεται κυρίως σε μεθόδους κρυπτογράφησης. Ωστόσο τα χαρακτηριστικά των επικοινωνιών σε δίκτυα οχημάτων είναι πολύ απαιτητικά και οι αποδώσεις των εφαρμογών ασφαλείας επιφέρουν ακόμα μεγαλύτερες προκλήσεις στις τεχνικές κρυπτογράφησης.

Το Internet of Things (IoT) εισχωρεί όλο και περισσότερο στην ζωή μας με ολοένα και περισσότερους τομείς να γίνονται κρίσιμοι για τις σύγχρονες τεχνολογίες. Ένας από αυτούς τους τομείς είναι και το Intelligent Transport System – ITS, με τις V2X τεχνολογίες να είναι οι πιο κρίσιμες για την ασφάλεια και την διαχείριση της κυκλοφορίας σε μια αυτοματοποιημένη ITS διαδικασία καθώς μπορεί να παίξει καθοριστικό ρόλο στην μείωση των ατυχημάτων στους δόμους. Οι δρόμοι στο άμεσο μέλλον πρόκειται να γίνουν πολύ πιο έξυπνοι και ασφαλέστεροι καθώς τομείς του IoT όπως το smart city's, τα αυτόνομα οχήματα και οι επικοινωνίες αυτών μελετούνται εδώ και χρόνια και έχουν ήδη αρχίσει να κάνουν την εμφάνισή τους. Τα πρώτα αυτόνομα οχήματα έχουν γίνει εδώ και καιρό πραγματικότητα από κάποιες μεγάλες εταιρίες όπως η Google και η Tesla. Είναι λοιπόν καιρός για την αυτοκινητοβιομηχανία εκτός από ασφαλή οχήματα, που έχει ρίξει το βάρος της τα τελευταία χρόνια, να αναπτύξει και πιο αυτοματοποιημένα οχήματα τα οποία με τις διαδικασίες που θα έχουν ενσωματωμένες θα είναι ασφαλέστερα για όλους και όχι μόνο για τους επιβάτες. Για να μπορέσει ωστόσο η βιομηχανία να είναι δελεαστική στο ευρύ κοινό θα πρέπει να υποστηρίζονται για τους επιβάτες περισσότερες εφαρμογές ψυχαγωγίας και infotainment οι οποίες να δίνονται δωρεάν και όχι συνδρομητικά στους καταναλωτές. Αυτός είναι ίσως ένας τρόπος για να γίνει η αγορά πιο δελεαστική για τον μέσο καταναλωτή καθώς τα πρώτα οχήματα που θα κυκλοφορούν δεν θα έχουν σίγουρα ένα χαμηλό κόστος αγοράς. Εδώ ωστόσο προκύπτει ένα ερώτημα το οποίο σχετίζεται με το πως θα παρέχονται οι υπηρεσίες ασφαλείας στο κοινό και ποιος θα επωμίζεται το κόστος των επικοινωνιών αυτών. Το πιο πιθανό είναι να έχουμε ένα σύστημα που θα λειτουργεί παρόμοια με αυτό το κλασικών κινητών επικοινωνιών με παρόχους και συνδρομητές. Καλό θα ήταν ωστόσο κάποιες βασικές εφαρμογές ασφαλείας να δίνονται εντελώς δωρεάν στο ευρύ κοινό.

Τέλος, όσον αφορά την παρούσα διπλωματική εργασία έχει αναπτύξει τις κυριότερες τεχνολογικές τάσεις επικοινωνιών για τα δίκτυα οχημάτων και έχει επισημάνει τις βασικότερες τεχνικές προκλήσεις και ευκαιρίες που θα έρθουν στο προσκήνιο τα επόμενα χρόνια με την ανάπτυξη του 5G, του cloud computing, του machine learning και των μεγάλων δεδομένων. Εν κατακλείδι σε αυτή την εργασία γίνεται μια πλήρης και σύγχρονη ανασκόπηση στα δίκτυα και τις επικοινωνίες των οχημάτων καθώς επίσης προωθεί την τεχνολογική πρόοδο, την ανάπτυξη και δίνει ερεθίσματα με προτάσεις για μελλοντική έρευνα των τεχνολογιών αυτών.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	***Ελληνικός Όρος***
Handover	Παράδοση
Latency	Καθυστέρηση
Mobility Management	Διαχείριση κινητικότητας
Pilot Signals	Πιλοτικά σήματα
Access Point	Ασύρματο σημείο πρόσβασης
Base Station	Σταθμός βάσης
Network Selection Schemes	Σχήματα επιλογής δικτύου
Routing Protocols	Πρωτόκολλα δρομολόγησης
User Equipment	Εξοπλισμός του χρήστη (όχημα ή κινητό)
Cellular Network	Κυψελωτό δίκτυο
Wireless Access	Ασύρματη Πρόσβαση

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

3GPP	Third-Generation Partnership Project
IEEE	Institute of Electrical and Electronics Engineers
DSRC	Dedicated Short Range Communications
GPS	Global Positioning System
LOS	Line of Sight
NLOS	Non Line of Sight
LTE	Long-Term Evolution
NHTSA	U.S. National Highway Traffic Safety Administration
OEM	Original Equipment Manufacturer
OBU	On-Board Unit
OFDM	Orthogonal Frequency Division Multiplexing
QoS	Quality of Service
RSU	Road Side Unit
SDN	Software Defined Network
MEC	Mobile Edge Computing
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VANET	Vehicular Ad hoc NETwork
VCC	Vehicular Cloud Communication
VFL	Vehicular Fog Layer

WAVE	Wireless Access in Vehicular Environments
Wi-Fi	Wireless Fidelity
MDVNETs	Manual Driving Vehicular Networks
ADVNETs	Automated Driving Vehicular Networks
AVs	Autonomous Vehicles
CAV	Connected-and-Automated Vehicles
VLC	Visible Light Communication
MIMO	Multiple Input and Multiple Output
eMBMS	Evolved Multimedia Broadcast and Multicast Services
MME	Mobility Management Entity
NR	New Radio
S-GW	Service Gateway
P-GW	Packet Gateway
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
UE	User Equipment
eNB	e NodeB
MAC	Media Access Control
Infotainment	Information and entertainment

ΠΑΡΑΡΤΗΜΑ Ι

US ITS Projects	Start-End	Goal
PATH (California Partners for Advanced Transit and Highways)	1986-Ongoing	The first several years of PATH research are divided into three primary categories: Navigation,automation and road electrification. Later in 2005–2006, PATH had been reorganized into four programmatic areas to align with Caltrans interests: traffic operations, transit operations, transportation safety and policy and behavior. Transportation Safety Research, Traffic Operations, Sustainability, Modal Applications, Integrated Corridor Management, Automated and Connected Vehicles and Berkeley Deep Drive are the main research domains of PATH. Starting in Summer 2015. California PATH plans a new initiative on advanced computer vision and machine learning for autonomous transportation.
Vehicle Safety Communications (VSC)	2002-2004	Eight high potential benefit safety application scenarios are selected: 1) Traffic Signal Violation Warning 2) Curve Speed Warning 3) Emergency Electronic Brake Lights 4) Cooperative Forward Collision Warning 5) Intersection Collision Warning 6) Left Turn Assistant 7) Lane Change Warning 8) Stop Sign Movement Assistance. DSRC has been proposed as a potential catalyst for a number of vehicle safety applications.
IntelliDrive(sm)/VII (Vehicle Infrastructure Integration)	2004-2009	Verify and enhance WAVE/IEEE 1609 features. Vehicle to Vehicle communication for Safety Applications. Vehicle to Infrastructure for Safety, Mobility and Environment.
CICAS (Cooperative Intersection Collision Avoidance Systems)	2004-2009	Develop and demonstrate cooperative intersection collision avoidance systems for both violations and gaps; to warn drivers about likely violations of traffic control devices and to help them maneuver through cross traffic and inform other drivers (i.e., potential victims) about impending violations as well as identify pedestrians and cyclists within an intersection.
Vehicle Safety Communications Applications	2006-2009	Implementation and testing of vehicle safety system using Dedicated Short Range Communications (DSRC) at 5.9 GHz and vehicle positioning.Explore possible improvements in this autonomous vehicle-based safety systems that can facilitate new communications-based safety applications.
SafeTrip21 (Safe and Efficient Travel through Innovation and Partnership for the 21st century)	2008-Ongoing	In order to accelerate the deployment of near-market-ready ITS technologies capable of delivering safety and mobility benefits, numerous operational tests and demonstration have been carried out. Demonstration is about, How better use of information, navigation, communications, technologies and protocols can make a measurable impact. For example, How it can reduce vehicle crashes and traffic congestion, enhance transit use and ride sharing, promote motor freight efficiency and safety, allow convenient electronic payment options, moderate environmental impacts and reduce unnecessary motor fuel consumption in both urban and rural settings.
Vehicle-to-Vehicle (V2V) Communications for Safety	2009-Ongoing	Facilitates the deployment of the Vehicle-to-Vehicle communication-based safety systems that should enhance safety across the vehicle fleet within the USA. Enabling each vehicle on the roadway to communicate with each other. Based on the set of data collected and the communications, a new generation of active safety applications and systems needs to be implemented.

Βασικά ITS Projects για τις ΗΠΑ [8]

Japanese ITS projects	Start-End	Goals
Electronic Toll Collection Systems	1993-Ongoing	Use of Identical OBU for all ETC operations and provided by different road operators. The system uses DSRC (ARIB STD-T75) communication for transmitting data at high-speed and in a robust manner. Uniform transponder and payment card are used on any toll network. Broaden serviceability to all types of vehicles. Both the Prepayment and post-payment charge offers are provided.
VICS (Vehicle Information and Communication System)	1996-Ongoing	Aim is to provide real-time road traffic information about congestion and regulation to the drivers. Processed Information in the form of text or graphic from the VICS center, is delivered via three communication and broadcasting media: FM Multiplex broadcasting, Radio wave beacon and Infrared beacon.
Advanced Safety Vehicle (ASV) Phase-vise ASV-1:1991-95 ASV-2:1996-00 ASV3: 2001-05 ASV4:2006-10 ASV5:2010-15	1991-Ongoing	Methods and devices which provide increased traffic safety and make the vehicles more friendly to humans (V2I/I2V and V2V communication). Active safety(preventive): OBU observes sensor data about the traffic situation and driving conditions, makes decisions and supports the driver or even takes control of the vehicle to prevent an accident. Both 5.8 GHz DSRC and 700 MHz ITS communications in V2V communications are used to send alerts or warning to the drivers about potential collisions with other drivers.
Smartway	2004-2007	To build a road system with communication infrastructure (RSUs) using DSRC 5.8 GHz for exchanging information among cars, drivers, pedestrians and users in I2V mode.
DSSS (Driving Safety Support Systems)	2006-ongoing	To prevent traffic accidents at intersections by issuing visual and audible warnings. DSSS alerts drivers based on information collected from various roadside sensors (detects cars, motorcycles, and pedestrians that are not in the driver's sight), road configuration, traffic signal and regulations. Road-to-vehicle cooperative system on local roads (Vehicle-Infrastructure communication based on the IR light beacon).
ITS-Safety 2010	2008-2011	To achieve the required applications of vehicle-infrastructure cooperative systems by March 2011.
ITS Spot	2009-Ongoing	To Provide three basic services: i) Dynamic Route Guidance ii) Assisting Safety Driving ii) ETC and in addition to these some additional services including internet access. ITS Spots installed mainly on expressways and services are provided via 5.8 GHz DSRC.

Βασικά ITS Projects για την Ιαπωνία [8]

European ITS projects	Start-End	Goals
COMeSafety (Communications for eSafety)	2006-2009	Have an eSafety Forum for all issues related to V2V and V2I communications as a basis for cooperative intelligent road transport systems. Coordination and consolidation of research results and their implementation. Support to worldwide harmonization. Support to frequency and spectrum allocation.
COOPERS (CO-OPerative SystEms for Intelligent Road Safety)	2006-2010	Improve road safety by using direct and latest traffic information communication between infrastructure and motorized vehicles on a section of motorway.
CVIS (Cooperative Vehicle-Infrastructure Systems)	2006-2010	To Design develop and test new technologies so that vehicles can communicate with each other and with the nearby RSUs.
SEVECOM (Secure Vehicular Communication)	2006-2008	To define a stable and future-proof solution to the security issues associated with vehicular communication and inter vehicle communication. To Identify all possible threats and specify an architecture and security mechanisms. Define cryptographic primitives which can cover specific operational environment.
SAFESPOT	2006-2010	Prevention of road accidents via a safety margin assistant. Detect potentially dangerous situations in advance and sensitize drivers to the surroundings in space and time. V2V and V2I communications are used for making safety information available to the drivers. Improving safety information in its the precision, reliability and quality.
NoW (Network on Wheels)	2004-2008	Developing a vehicular communication system based on Adhoc and WLAN technology for car-to-car and car-to-infrastructure communication. This vehicular communication must be used primarily for road safety and infotainment applications. Two main technologies used: WLAN (IEEE 802.11) and GPS-based positioning.
AIDE (Adaptive Integrated Driver-vEhicle interface)	2004-2008	Generate knowledge and develop methodologies for man-machine interface technologies necessary for the safe and efficient integration of ADAS, MS and nomadic devices into the driving environment.
APROSYS (Advanced Protection Systems)	2004-2009	Development and introduction of critical technologies to improve passive safety for all European road users in all types of accidents and emergencies.

Βασικά ITS Projects για την Ευρώπη [8]

European ITS projects	Start-End Years	Goals
PREDRIVE C2X (Preparation for driving implementation and evaluation of C2X communication technology)	2008-2010	Develop an integrated simulation model for cooperative systems that provides a holistic approach to estimating expected benefits in terms of safety, efficiency, and environment. Broad dissemination activities planned to communicate the public about the benefits of vehicle technology in cooperative systems and to reach out to all relevant European stakeholders.
GeoNET	2008-2010	Implementation and formal testing of a networking mechanism as a single software module to be incorporated into Cooperative Systems. Allow transparent IP connectivity between a vehicle and the road side infrastructure, even in cases when delivery is multi-hopped or cached along the way. Use of geographic addressing and the routing mechanism to distribute the packets to nodes within a selected destination area.
iTETRIS	2008-2011	Development of a large-scale and long-term simulation tool for the evaluation of cooperative traffic management applications. The simulator couples traffic and network simulation in a closed-loop for detailed analyses of the effects and performance evaluation of cooperative applications on traffic flow, travel time, emissions, etc.
ROSATTE (Road safety attributes exchange infrastructure in Europe)	2008-2010	Establishment of an efficient and assured quality data supply chain from public authorities to commercial map providers for safety-related road content.
PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)	2011-2015	Bring secure, privacy-protected V2X communication closer to reality by providing field testing to a security and privacy subsystem. Provide comprehensive protection to in-vehicle sensors, onboard network and V2V/V2I communication, and the receiving applications.
PRECIOSA (Privacy enabled capability in co-operative systems and safety applications)	2008-2010	Demonstration of co-operative system s compliance with future privacy regulations. It is done using a sample application that can be endowed with technologies for proper privacy protection of location related data. Define an evaluation approach to co-operative systems in terms of communication and data storage privacy. Define a privacy aware architecture for co-operative systems, involving appropriate trust models and ontologies, and a privacy verifiable architecture for V2V and V2I. Define and validate guidelines for privacy aware co-operative systems. Investigate the key challenges for privacy.
DRIVE C2X	2011-2014	Create a harmonized testing environment in Europe for cooperative systems through Field Operational Tests (FOTs). Coordinate the tests carried out in parallel throughout the DRIVE C2X community. Evaluate cooperative systems. Promote cooperative driving.
COLOMBO (Cooperative Self-Organizing System for low Carbon Mobility at low Penetration Rates)	2012-2015	Reduce congestion and its impact on everyday life in urban environments. The development of smarter urban transport systems, with the aim of disseminating good practices towards more efficient urban transport. Bring together technologies, methods and combine well-established modeling tools such as vehicular pollutant emissions (PHEM), traffic simulation (SUMO) and vehicular communication (iTETRIS and ns-3).

Βασικά ITS Projects για την Ευρώπη [8]

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] H. Zhou, W. Xu, J. Chen, and W. Wang, “Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities,” *Proceedings of the IEEE*, vol. 108, no. 2, pp. 308–323, Feb. 2020.

[2] N. Gaouar and M. Lehsaini, “Toward vehicular cloud/fog communication: A survey on data dissemination in vehicular ad hoc networks using vehicular cloud/fog computing,” *International Journal of Communication Systems*, vol. 34, no. 13, Sep. 2021.

[3] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, “Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[4] Arnav ThakurandReza Malekian, Senior Member, IEEE “Fog Computing for Detecting Vehicular Congestion”.

[5] K. Kai, W. Cong, and L. Tao, “Fog computing for vehicular Ad-hoc networks: Paradigms, scenarios, and issues,” *Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, Apr. 2016.

[6] IEEE ITSS and Institute of Electrical and Electronics Engineers, *Proceedings, 2017 IEEE International Conference on Service Operations and Logistics, and Informatics : September 18-20, 2017, Bari, Italy.*

[7] G. Naik, B. Choudhury, and J. M. Park, “IEEE 802.11bd 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications,” *IEEE Access*, vol. 7, pp. 70169–70184, 2019.

[8] P. K. Singh, S. K. Nandi, and S. Nandi, “A tutorial survey on vehicular communication state of the art, and future research directions,” *Vehicular Communications*, vol. 18, Aug. 2019.

[9] H. Peng, L. Liang, X. Shen, and G. Y. Li, “Vehicular communications: A network layer perspective,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064–1078, Feb. 2019.

[10] “MillimeterWave Vehicular Communication to Support Massive Automoive Sensing”, 18 May 2016.

[11] K. Z. Ghafoor *et al.*, “Millimeter-Wave Communication for Internet of Vehicles: Status, Challenges and Perspectives.”

[12] S. A. Busari, K. M. S. Huq, S. Mumtaz, L. Dai, and J. Rodriguez, “Millimeter-Wave Massive MIMO Communication for Future Wireless Systems: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 20, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 836–869, Apr. 01, 2018.

[13] T. W. C. Brown, D. A. Humphreys, M. Hudlicka, and T. H. Loh, “Prediction of SINR using BER and EVM for Massive MIMO Applications.”

[14] B. M. Masini, A. Bazzi, and A. Zanella, “A survey on the roadmap to mandate on board connectivity and enable V2V-based vehicular sensor networks,” *Sensors (Switzerland)*, vol. 18, no. 7, Jul. 2018.

[15] S. Kumar Gupta, Y. Khan, and D. T. Ngo, “An LTE-Direct-Based Communication System for Safety Services in Vehicular Networks.” .

[16] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, “Challenges and Solutions for Cellular Based V2X Communications,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 222–255, Jan. 2021.

[17] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, “DSRC versus 4G-LTE for connected vehicle applications: A study on field experiments of vehicular communication performance,” *Journal of Advanced Transportation*, vol. 2017, Jan. 2017.

[18] A. Mahmood, W. E. Zhang, and Q. Z. Sheng, “Software-defined heterogeneous vehicular networking: The architectural design and open challenges,” *Future Internet*, vol. 11, no. 3, 2019.

[19] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, “Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends,” *International Journal of Distributed Sensor Networks*, vol. 2015. Hindawi Publishing Corporation, 2015.

[20] T. Yeferny and S. Hamad, “Vehicular Ad-hoc Networks: Architecture, Applications and Challenges,” 2020.

[21] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, “Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network - Performance evaluation,” *Transportation Research Part C: Emerging Technologies*, vol. 68, pp. 168–184, Jul. 2016.

[22] D. Kanthavel, S. K. B. Sangeetha, and K. P. Keerthana, “An empirical study of vehicle to infrastructure communications - An intense learning of smart infrastructure for safety and mobility,” *International Journal of Intelligent Networks*, vol. 2, pp. 77–82, 2021.

[23] M. Muhammad and G. A. Safdar, “5G-based V2V broadcast communications: A security perspective,” *Array*, vol. 11, p. 100084, Sep. 2021.

[24] A. M. Little, “Hybrid vehicular communications based on V2V-V2I protocol switching,” 2011.

[25] A. Zekri and W. Jia, “Heterogeneous vehicular communications: A comprehensive study,” *Ad Hoc Networks*, vol. 75–76. Elsevier B.V., pp. 52–79, Jun. 01, 2018.

[26] Leonardo Gomes Baltar, Markus Mueck, Dario Sabella ‘’ Heterogeneous Vehicular Communications – Multi-Standard Solutions to Enable Interoperability’’ *2018 IEEE Conference on Standards for Communications and Networking.*

[27] P. Dong, T. Zheng, S. Yu, H. Zhang, and X. Yan, “Enhancing vehicular communication using 5g-enabled smart collaborative networking,” *IEEE Wireless Communications*, vol. 24, no. 6, pp. 72–79, Dec. 2017.

[28] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, “5G mmwave positioning for vehicular networks,” *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, Dec. 2017.

[29] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, “5G for Vehicular Communications,” *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[30] L. Wang, T. Han, Q. Li, J. Yan, X. Liu, and D. Deng, “Cell-less communications in 5g vehicular networks based on vehicle-installed access points,” *IEEE Wireless Communications*, vol. 24, no. 6, pp. 64–71, Dec. 2017.

[31] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, “Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2377–2396, Oct. 2015.

[32] G. Karagiannis *et al.*, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4. pp. 584–616, Dec. 2011.

[33] Shao-hui Sun, Jin-ling hu, ying peng, Xue-Ming pan, li Zhao, and Jia-yi fang “Support for vehicle-to-everything services based on LTE”, June 2016.

[34] Panos Papadimitratos, Arnaud de La Fortelle, Knut Evenssen, Roberto Brignolo and Stefano Cosenza, “Vehicular communication systems - Enabling technologies, applications, and future outlook on intelligent transportation”, November 2009.

[35] K. A. Hafeez, L. Zhao, B. Ma, and J. W. Mark, “Performance analysis and enhancement of the DSRC for VANET’s safety applications,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3069–3083, 2013.

[36] K. Abboud, H. A. Omar, and W. Zhuang, “Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[37] TSGS, “TS 122 185 - V14.3.0 - LTE; Service requirements for V2X services (3GPP TS 22.185 version 14.3.0 Release 14),” 2017.

[38] Z. H. Mir and F. Filali, “LTE and IEEE 802.11p for vehicular networking: a performance evaluation,” 2014.

[39] Hanbyul Seo, Ki-Dong Lee, Shinpei Yasukawa, Ying Peng, and Philippe Sartori “LTE evolutionfor vehicle-to-everything services”, June 2016.

[40] Giuseppe Araniti, Claudia Campolo, Massimo Condoluci, Antonio Iera, and Antonella Molinaro, “LTE for vehicular networking - A survey”, May 2013.

[41] I. A. Abbasi and A. S. Khan, “A review of vehicle to vehicle communication protocols for VANETs in the urban environment,” *Future Internet*, vol. 10, no. 2. MDPI AG, Jan. 31, 2018.

[42] C. Weiß, “V2X communication in Europe - From research projects towards standardization and field testing of vehicle communication technology,” *Computer Networks*, vol. 55, no. 14, pp. 3103–3119, Oct. 2011.

[43] I. Takai, T. Harada, M. Andoh, K. Yasutomi, K. Kagawa, and S. Kawahito, “Optical vehicle-to-vehicle communication system using LED transmitter and camera receiver,” *IEEE Photonics Journal*, vol. 6, no. 5, Oct. 2014.

[44] X. Zhao, S. Jing, F. Hui, R. Liu, and A. J. Khattak, “DSRC-based rear-end collision warning system – An error-component safety distance model and field test,” *Transportation Research Part C: Emerging Technologies*, vol. 107, pp. 92–104, Oct. 2019.

[45] R. A. Dziyauddin *et al.*, “Computation offloading and content caching and delivery in Vehicular Edge Network: A survey,” *Computer Networks*, vol. 197. Elsevier B.V., Oct. 09, 2021.

[46] G. S. Taki, ‘’ Li-Fi based Intelligent Speed Assistance’’ *2019 3rd International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) : August 29-31, 2019.*

[47] Y. Li, “Anti-fatigue and collision avoidance systems for intelligent vehicles with ultrasonic and Li-Fi sensors,” in *2020 3rd IEEE International Conference on Information Communication and Signal Processing, ICICSP 2020*, Sep. 2020, pp. 203–209.

[48] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular Ad Hoc network,” *Journal of Network and Computer Applications*, vol. 37, no. 1. Academic Press, pp. 380–392, 2014.

[49] J. Karedal *et al.*, “A geometry-based stochastic MIMO model for vehicle-to-vehicle communications,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3646–3657, Jul. 2009.

[50] S. Zeadally, J. Guerrero, and J. Contreras, “A tutorial survey on vehicle-to-vehicle communications,” *Telecommunication Systems*, vol. 73, no. 3, pp. 469–489, Mar. 2020.

[51] L. Liang, H. Peng, G. Y. Li, and X. Shen, “Vehicular communications: A physical layer perspective,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10647–10659, Dec. 2017.

[52] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): Status, results, and challenges,” *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, Aug. 2012.

[53] I. Sen and D. W. Matolak, “Vehicle-vehicle channel models for the 5-GHz band,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 9, no. 2, pp. 235–245, Jun. 2008.

[54] Albert Demba, Dietmar P. F. Möller ‘’Vehicle-to-Vehicle Communication Technology’’ *2018 IEEE International Conference on Electro/Information Technology (EIT) : 3-5 May 2018.*

[55] C. M. Huang, M. S. Chiang, D. T. Dao, W. L. Su, S. Xu, and H. Zhou, “V2V Data Offloading for Cellular Network Based on the Software Defined Network (SDN) Inside Mobile Edge Computing (MEC) Architecture,” *IEEE Access*, vol. 6, pp. 17741–17755, Mar. 2018.

[56] J. Janai, F. Güney, A. Behl, and A. Geiger, “Computer Vision for Autonomous Vehicles: Problems, Datasets and State of the Art,” *Foundations and Trends® in Computer Graphics and Vision*, vol. 12, no. 1–3, pp. 1–308, 2020.

[57] P. Mangesh Kale, “Vehicle To Vehicle Communication for Crash Avoidance System.”

[58] Daniel Jiang, Luca Delgrossi ‘’IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments’’ *2008 IEEE 67th Vehicular Technology Conference-spring : Marina Bay, Singapore, 11-14 May 2008*.

[59] Arcade NSHIMIYIMANA, Deepak Agrawal, Wasim Arif, ‘’Comprehensive Survey of V2V Communication for 4G Mobile and Wireless Technology’’ *23-25 March 2016.*

[60] A. Ghosal and M. Conti, “Security issues and challenges in V2X: A Survey,” *Computer Networks*, vol. 169, Mar. 2020.

[61] F. Li and Y. Wang, “Routing in vehicular ad hoc networks: A survey,” in *IEEE Vehicular Technology Magazine*, 2007, vol. 2, no. 2, pp. 12–22.

[62] A. F. Molisch and C. F. Mecklenbräuker, “INTRODUCTION VEHICULAR WIRELESS NETWORKS A SURVEY ON VEHICLE-TO-VEHICLE PROPAGATION CHANNELS,” 2009.

[63] Shivaji Kulkarni, Amogh Darekar Suhas Shirol ‘’Proposed Framework for V2V Communication using Li-Fi Technology’’ *December 2017*.

[64] P. Krishnan, “Design of Collision Detection System for Smart Car Using Li-Fi and Ultrasonic Sensor,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11420–11426, Dec. 2018.

[65] Ø. Risan and E. Peytchev, “A Vehicle-to-Vehicle Communication Protocol for Collaborative Identification of Urban Traffic Conditions,” 2010.

[66] H. Hartenstein, “INTRODUCTION TOPICS IN AD HOC AND SENSOR NETWORKS A Tutorial Survey on Vehicular Ad Hoc Networks,” 2008.

[67] Wei, S., Zou, Y., Zhang, X., Zhang, T., & Li, X. An integrated longitudinal and lateral vehicle following control system with radar and vehicle-to-vehicle communication. IEEE Transactions on Vehicular Technology, 2019.

[68] Ελληνική Στατιστική Αρχή ''Οδικά τροχαία ατυχήματα'' 30 Μαρτίου 2022 https://www.statistics.gr/el/statistics/-/publication/SDT04/-

[69] Junil Choi, Vutha Va, Nuria Gonzalez-Prelcic, Robert Daniels, Chandra R. Bhat, and Robert W. Heath Jr, ''Millimeter Wave Vehicular Communication to Support Massive Automotive Sensing'', Sep. 2016.

[70] https://dosensecable.com/cable/OPGW/OPGW.html

[71] Tim W. C. Brown, David A. Humphreys, Martin Hudlicka, Tian H. Loh,''Prediction of SINR using BER and EVM for Massive MIMO Applications'', Sep. 2018.

[72] Alin-Mihai Cailean, Mihai Dimian, ''Impact of IEEE 802.15.7 Standard on Visible Light Communications Usage in Automotive Applications'', IEEE Communications Magazine, April 2017.

[73] G. H. Sim, S. Klos, A. Asadi, A. Klein, and M. Hollick, “An online context aware machine learning algorithm for 5G mmWave vehicular communications,” IEEE/ACM Trans. Netw., vol. 26, no. 6, pp. 2487–2500, Dec. 2018.

[74] Y. Lv, Y. Duan, W. Kang, Z. Li, and F. Wang, “Traffic flow prediction with big data: A deep learning approach,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 865–873, Apr. 2015.

[75] T. He, N. Zhao, and H. Yin, “Integrated networking, caching and computing for connected vehicles: A deep reinforcement learning approach,” IEEE Trans. Veh. Technol., to appear.

[76] H. Ye and G. Y. Li, “Deep reinforcement learning for resource allocation in V2V communications,” in Proc. IEEE ICC, May 2018.

[77] Y. Xu, L. Li, B.-H. Soong, and C. Li, “Fuzzy Q-learning based vertical handoff control for vehicular heterogeneous wireless network,” in Proc. IEEE ICC, Jun. 2014, pp. 5653–5658.