



**ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ**

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

**ΔΙΑΣΥΝΔΕΔΕΜΕΝΑ ΑΥΤΟΚΙΝΗΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ
ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

**ΚΥΡΙΑΖΗ ΜΠΟΥΣΙΟΥ
ΟΔΥΣΣΕΑ ΚΟΥΜΟΥΤΣΑΚΟΥ**

Επιβλέπων : Διαμαντοπούλου Βασιλική (Επίκουρη Καθηγήτρια)

Μέλη εξεταστικής επιτροπής: Καρύδα Μαρία (Καθηγήτρια)
Κοκολάκης Σπυρίδων (Καθηγητής)

Διπλωματική εργασία υποβληθείσα στο Τμήμα Μηχανικών πληροφοριακών και επικοινωνιακών συστημάτων ως μέρος των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στα Πληροφοριακά και Επικοινωνιακά Συστήματα.

Καρλάβασι Σάμου, Φεβρουάριος, 2024



UNIVERSITY OF THE AEGEAN
ENGINEERING SCHOOL

DEPARTMENT OF INFORMATION AND COMMUNICATION SYSTEMS ENGINEERING

MASTER PROGRAMME IN INFORMATION AND COMMUNICATION SYSTEMS

Connected vehicles and privacy protection.

Master Thesis

Of

Kyriazis Bousios
Odysseas Koumoutsakos

Supervisor professor: Diamantopoulou Vasiliki (Assistant Professor)

Members of the examination committee: Karyda Maria (Professor)
Kokolakis Spyridon (Professor)

Master Thesis submitted to the Department of Information and Communication Systems Engineering of the University of the Aegean in partial fulfillment of the requirements for the degree of Master of information and communication systems.

Karlovasi Samos, February 2024

Στις οικογένειές μας

Ευχαριστίες

“Σα βγεις στον πηγαιμό για την Ιθάκη, να εύχεται να είναι μακρύς ο δρόμος, γεμάτος περιπέτειες, γεμάτος γνώσεις...

Ένα ακόμη κεφάλαιο μιας υπέροχης διατίας με όμορφες αναμνήσεις, απόκτηση ζητούμενων γνώσεων, καθώς και πολλών ωρών δουλειάς φτάνει στο τέλος του.

Θα ήθελα να ευχαριστήσω την καθηγήτρια μου, κυρία Διαμαντοπούλου Βασιλική για την αποδοχή της να συνεργαστεί μαζί μας. Επιπροσθέτως θα ήθελα να εκφράσω τις ευχαριστίες μου στην καθηγήτρια κυρία Μαρία Καρύδα, καθώς και στον καθηγητή κύριο Σπυρίδων Κοκολάκη, για όλες τις γνώσεις που μου μεταλαμπάδευσαν καθ’ όλη τη διάρκεια των σπουδών μου.

Επιπλέον θα ήθελα να ευχαριστήσω τον αδερφικό μου φίλο, συμφοιτητή και συνεργάτη αυτής της διπλωματικής εργασίας κύριο Οδυσσέα-Παναγιώτη Κουμουτσάκο, για την συνεργασία του και την συμβολή του στην περάτωση αυτής.

Θερμά ευχαριστώ στους γονείς μου Θανάση και Φωτεινή, καθώς και τον αδερφό μου Βασίλη, για την ανεκτίμητη συναισθηματική και οικονομική τους στήριξη, την ευκαιρία που μου έδωσαν για να σπουδάσω, καθώς και για την εμπιστοσύνη τους σε εμένα όλα αυτά τα χρόνια των προπτυχιακών και μεταπτυχιακών σπουδών μου. Χωρίς εκείνους δεν θα μπορούσα να είμαι ο άνθρωπος που είμαι σήμερα.”

Last but not least, θα ήθελα να ευχαριστήσω θερμά την κοπέλα μου Κατερίνα, για την πολύτιμη στήριξή της αυτά τα 2 χρόνια. Οι συμβουλές της, καθώς και η διακριτική της παρουσία στο πλευρό μου ήταν καταλυτικά συστατικά στην ολοκλήρωση αυτής της εργασίας.”

Με εκτίμηση και σεβασμό

-Κυριαζής Μπούσιος

Πάει και αυτό...

Ένα υπέροχο κεφάλαιο κλείνει προσθέτοντας ένα λιθαράκι ακόμη στον γνωστικό μου ορίζοντα. Θα ήθελα να ευχαριστήσω θερμά την καθηγήτρια μου κυρία Διαμαντοπούλου Βασιλική για την αποδοχή της να συνεργαστεί μαζί μας.

Ευχαριστώ επιπλέον θερμά τον παλιό καλό μου φίλο, συμφοιτητή και συνεργάτη σε αυτή την εργασία κύριο Κυριαζή Μπούσιο, για την συνεργασία του και τη συμβολή του στην περάτωση της εργασίας αυτής.

Τελειώνοντας ένα μεγάλο ευχαριστώ στους γονείς μου, τους αφανείς ήρωες αυτής της ιστορίας που με στήριζαν, με στηρίζουν και θα συνεχίσουν να με στηρίζουν με ότι μπορούν.

Με εκτίμηση και σεβασμό

-Οδυσσέας Κουμουτσάκος

© 2024

των

Κυριαζή Μπούσιου και Οδυσσέα Κουμουτσάκου

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1: ΤΑ ΣΤΑΔΙΑ ΕΞΕΛΙΞΗΣ ΤΟΥ ΑΥΤΟΚΙΝΗΤΟΥ	1
1.1 Γνωρίζοντας το αυτοκίνητο	1
1.1.1 Ιστορική αναδρομή του αυτοκινήτου	1
1.1.2 Εξέλιξη του αυτοκινήτου	2
1.1.3 Το αυτοκίνητο σήμερα	2
1.1.4 Τα νέα smart cars είναι ακόμα ένας κλάδος του λεγόμενου Internet of Things (IoT)	2
1.1.5 Κατανόηση Ευρωπαϊκού πλαισίου και προστασία της ιδιωτικότητας	3
1.2 Σκοπός της διπλωματικής εργασίας	3
1.3 Δομή της διπλωματικής εργασίας	3
ΚΕΦΑΛΑΙΟ 2: Το εσωτερικό των διασυνδεδεμένων αυτοκινήτων	5
2.1 Τι είναι το VANET (Vehicular Ad Hoc Network)	5
2.2 Η αρχιτεκτονική των σύγχρονων αυτοκινήτων	6
2.2.1 Βασικός εξοπλισμός ενός διασυνδεδεμένου οχήματος	6
2.3.1 Στοιχεία ενός διασυνδεδεμένου οχήματος	9
2.3.1.1 Οθόνη αφής με υψηλή ανάλυση	9
2.3.1.1.1 Συναγερμός αντικλεπτικής προστασίας	10
2.3.1.1.2 Αισθητήρες παρακολούθησης	11
2.3.1.1.3 Συστήματα αυτόνομης οδήγησης	11
2.3.1.1.4 Συστήματα ενεργειακής απόδοσης	12
ΚΕΦΑΛΑΙΟ 3: Εσωτερική και εξωτερική δικτύωση των διασυνδεδεμένων οχημάτων	
3.1 Εσωτερική δικτύωση	13
3.1.1 Οι ενσύρματες συνδέσεις	13
3.1.1.1 Ανάλυση του CAN	13
3.1.1.2 Ιστορία του CAN	14
3.1.1.3 Οφέλη CAN	14

3.1.1.4 Εκπομπή επικοινωνίας	14
3.1.1.5 Προτεραιότητα	15
3.1.1.6 Λειτουργία επικοινωνίας CAN	16
3.1.1.7 ISO 11898	17
3.1.1.8 Ο διάυλος CAN Bus και οι εφαρμογές του	17
3.1.2 Ασύρματες συνδέσεις (Wireless Connections)	18
3.1.2.1 Wi-Fi (Wireless-Fidelity)	18
3.1.2.2 Bluetooth	18
3.1.2.3 Cellular Networks (3G,4G,5G)	19
3.1.2.4 Near Field Communication (NFC)	20
3.1.2.5 Vehicle to Everything (V2X) Communication	20
3.1.2.6 GPS (Global Positioning System)	21
3.1.2.7 Dedicated Short Range Communication (DSRC)	21
3.2 Πληροφορίες συστήματος υπολογιστή για υπηρεσίες συνδεδεμένου αυτοκινήτου	23
3.3 Οδική βοήθεια	24
3.3.1. Επιπρόσθετη οδική βοήθεια	24
ΚΕΦΑΛΑΙΟ 4: Πλεονεκτήματα και μειονεκτήματα των διασυνδεδεμένων οχημάτων	25
4.1 Πλεονεκτήματα	25
4.2 Μειονεκτήματα	26
4.3 Μεταβατικό στάδιο	27
ΚΕΦΑΛΑΙΟ 5: Ιδιωτικότητα και προσωπικά δεδομένα	28
5.1 Εισαγωγή	28
5.2 Προσωπικά δεδομένα και ιδιωτικότητα	29
5.3 Ιδιωτικότητα στα VANET	30
5.3.1 Τι δεδομένα συλλέγονται από τα διασυνδεδεμένα αυτοκίνητα	30
5.3.2 Τα προσωπικά δεδομένα στο έλεος των αυτοκινητοβιομηχανιών	31
5.4 Προστασία της ιδιωτικότητας στα διασυνδεδεμένα αυτοκίνητα	36

5.4.1 Πρότυπο IEEE 1609.2	33
5.4.2 Μηχανισμοί ενδυνάμωσης ασφάλειας	33
5.4.2.1 ARAN	33
5.4.2.2 SEAD	34
5.4.2.3 SAODV Protocol	34
5.4.2.4 ASAODV	35
5.4.2.5 One Time cookie	35
5.4.3 Ενημέρωση του καταναλωτή από τις εταιρίες διασυνδεδεμένων οχημάτων ως προς την ιδιωτικότητα του	36
ΚΕΦΑΛΑΙΟ 6: ΑΠΕΙΛΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΑ VANET	38
6.1 Εισαγωγή	38
6.1.1 Απειλή της ιδιωτικότητας του χρήστη δια μέσω συσκευών του οχήματος ή διαφόρων εφαρμογών	39
6.1.2 Παραβίαση της ιδιωτικότητας του χρήστη από επιθέσεις στα δίκτυα των διασυνδεδεμένων οχημάτων	41
6.1.2.1 Eaves dropping	42
6.3.2.2 Masquerading Assault	43
6.1.2.3 GPS Spoofing Assault	44
6.1.2.4 Brute Force Assault	45
ΚΕΦΑΛΑΙΟ 7: Συμπεράσματα	46
ΒΙΒΛΙΟΓΡΑΦΙΑ	48

Λίστα Σχημάτων

- Σχήμα 1: Modeling tools to evaluate the performance of wireless multi-hop networks. Σελίδα 5
- Σχήμα 2: Ένα σύστημα υποστήριξης οδηγού με επίγνωση του περιβάλλοντος για έξυπνα αυτοκίνητα που βασίζονται σε VANET. Σελίδα 6
- Σχήμα 3: Το εσωτερικό των διασυνδεδεμένων αυτοκινήτων. Σελίδα 7
- Σχήμα 4: Οθόνη αφής υψηλής ανάλυσης ενός διασυνδεδεμένου οχήματος Renault Clio. Σελίδα 9
- Σχήμα 5: Οθόνη αφής υψηλής ανάλυσης μιας Mercedes A-180. Σελίδα 10
- Σχήμα 6: Κάμερα παρακολούθησης σε ένα διασυνδεδεμένο όχημα Tesla. Σελίδα 10
- Σχήμα 7: Mercedes A-200 η αυτόματη λειτουργία παρκαρίσματος. Σελίδα 10
- Σχήμα 8: Τα οφέλη του CAN: Σελίδα 15
- Σχήμα 9: Ασύρματες επικοινωνίες ενός διασυνδεδεμένου οχήματος. Σελίδα 22
- Σχήμα 10: Ανάλυση των επικοινωνιών των διασυνδεδεμένων οχημάτων σε μια έξυπνη πόλη. σελίδα 23
- Σχήμα 11: Eaves dropping assault. Σελίδα 42
- Σχήμα 12: Masquerading assault Σελίδα 43
- Σχήμα 13: GPS Spoofing assault. Σελίδα 42

Ακρωνύμια

ECU	<i>Electronic Control Unit</i>
GPS	<i>Global Positioning System</i>
SUV	<i>Sports Utility Vehicle</i>
ABS	<i>Anti-Lock Breaking System</i>
EBD	<i>Electronic Brake Pressure Distribution</i>
IoT	<i>Internet Of Things</i>
VANET	<i>Vehicular Ad Hoc Network</i>
ASR	<i>Anti-Slip Regulation</i>
ESP	<i>Electronic Stability Program</i>
ADAS	<i>Advanced Driver Assistant System</i>
SAE	<i>Society Of Automotive Engineers</i>
EA	<i>Enhanced Autopilot</i>
KH/H	<i>Kilometer Per Hour</i>
ΗΠΑ	<i>Ηνωμένες Πολιτείες της Αμερικής</i>
V2V	<i>Vehicle To Vehicle</i>
V2X	<i>Vehicle To Everything</i>
V2I	<i>Vehicle To Infrastructure</i>
CAN	<i>Controller Area Network</i>
LabVIEW	<i>Laboratory Virtual Instrument Engineering Workbench</i>
RPM	<i>Revolutions Per Minute</i>
CSMA	<i>Carrier Sense Multiple Access</i>
ISO	<i>International Organization for Standardization</i>
P2P	<i>Peer-to-Peer</i>

Wi-Fi	<i>Wireless Fidelity</i>
3G,4G,5G	<i>The 3rd,4th,5th Generation mobile network</i>
OTA updates	<i>Over The Air updates</i>
NFC	<i>Near Field Communication</i>
V2N	<i>Vehicle To Network</i>
V2P	<i>Vehicle to Pedestrian</i>
POI	<i>Point Of Interest</i>
DSRC	<i>Dedicated Short Range Communications</i>
ACEA	<i>The European Automobile Manufacturers' Association</i>
EE	<i>Ευρωπαϊκή Ένωση</i>
Covid19	<i>Corona Virus Disease 2019</i>
ΙΧ	<i>Ιδιωτικής Χρήσης όχημα</i>
ΦΠΑ	<i>Φόρος Προστιθέμενης Αξίας</i>
ΟΗΕ	<i>Οργανισμός Ηνωμένων Εθνών</i>
PCLOB	<i>Privacy and Civil Liberties Oversight Board</i>
ΕΣΑΒ	<i>Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου</i>
ΓΚΠΔ	<i>Γενικός Κανονισμός για την Προστασία των Δεδομένων</i>
ΕΟΧ	<i>Ευρωπαϊκός Οικονομικός Χώρος</i>
GDPR	<i>General Data Protection Regulation</i>
SCCs	<i>Standard Contractual Clauses</i>
BCRs	<i>Binding Corporate Rules</i>
PII	<i>Personal Identifiable Information</i>
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
MITM	<i>Man In The Middle</i>

<i>DDOS</i>	<i>Distributed Denial-of-Service</i>
<i>UDP</i>	<i>User Datagram Protocol</i>
<i>CPU</i>	<i>Central Processing Unit</i>
<i>HTTP</i>	<i>Hypertext Transfer Protocol</i>
<i>ARAN</i>	<i>Authenticated Routing for Ad Hoc Networks Protocol</i>
<i>SEAD</i>	<i>Source Location Privacy-Aware Energy-Efficient Adaptive Clustering Protocol</i>
<i>WSNs</i>	<i>Wireless Sensor Networks</i>
<i>SAODV</i>	<i>Secure Ad Hoc On-Demand Distance Vector</i>
<i>AODV</i>	<i>Ad Hoc On-Demand Distance Vector</i>
<i>ECDSA</i>	<i>Elliptic Curve Digital Signature Algorithm</i>
<i>H/Y</i>	<i>Ηλεκτρονικός Υπολογιστής</i>

Περίληψη

Τα διασυνδεδεμένα αυτοκίνητα (Connected Vehicles), γίνονται ολοένα και πιο διαδεδομένα παγκοσμίως. Για την ακρίβεια η συντριπτική πλειοψηφία των καινούργιων οχημάτων ακολουθούν πιστά την εξέλιξη της τεχνολογίας, η οποία έχει φέρει επαναστατικές μεθόδους οδικής ασφάλειας καθώς και πληθώρα νέων επιλογών (οδηγικών και διασκέδασης) στους οδηγούς αυτών. Σχετικά με την οδική συμπεριφορά των νέων οχημάτων, μια πληθώρα αισθητήρων που παρακολουθούν διαφορετικές πτυχές του οχήματος, στέλνουν ειδικευμένες πληροφορίες στον οδηγό μέσω των πλέον ηλεκτρονικών πινάκων του αυτοκινήτου, αλλά επιπλέον δίνουν ακόμα περισσότερες πληροφορίες στο κομμάτι του ηλεκτρονικού ελέγχου του οχήματος ECU (Electronic Control Unit).

Τα νέα οχήματα επίσης, είναι διαρκώς συνδεδεμένα με το διαδίκτυο και με αυτό τον τρόπο επιτρέπουν στους οδηγούς να έχουν τον έλεγχο και την γενικότερη κατάσταση (κλειδωμένο/ξεκλειδωτό) του οχήματος, καθώς επίσης και την ακριβή τοποθεσία αυτού. Το όχημα επίσης καθώς είναι συνδεδεμένο στο διαδίκτυο μπορεί να λάβει ενημερώσεις λογισμικού από την ίδια την αυτοκινητοβιομηχανία που το κατασκεύασε, όπως επίσης να «επικοινωνεί και να αλληλεπιδρά» με τρίτες μορφές ασύρματων συνδεδεμένων συσκευών (δορυφόρους, GPS).

Παρά τον ενθουσιασμό που δημιουργείται με τις πολλαπλές νέες δυνατότητες των συνδεδεμένων αυτοκινήτων, δημιουργούνται αντιστοίχως και εύλογες απορίες και φόβοι για την αξιοπιστία της ασφάλειας των δικτύων με τα οποία το όχημα αλληλεπιδρά. Ίσως μια κακόβουλη επίθεση στα δίκτυα επικοινωνίας των αυτοκινήτων να δημιουργήσουν τροχαία ατυχήματα σε περίπτωση παράκαμψης των πρωτοκόλλων ασφαλείας. Επιπροσθέτως η σημαντικότερη ίσως ανησυχία είναι για την διαχείριση των δεδομένων που συλλέγονται με την βοήθεια αυτών των ηλεκτρονικών συστημάτων. Πως μπορούμε να εξασφαλίσουμε πως αυτά που ακούνε και βλέπουν τα ηλεκτρονικά συστήματα των οχημάτων δεν θα διαρρεύσουν εσκεμμένα προς τρίτους, προκειμένου οι αυτοκινητοβιομηχανίες να μεγαλώσουν ακόμη περισσότερο τα κέρδη τους, πουλώντας ουσιαστικά τα προσωπικά δεδομένα των καταναλωτών.

Στην παρακάτω εργασία θα παρατεθούν ένας προς ένας ο τρόπος λειτουργίας αυτών των συστημάτων ο οποίος είναι αξιοσημείωτος. Θα παρατεθούν όμως και οι φόβοι για την παραβίαση της ιδιωτικότητας των οδηγών και των μελών που χρησιμοποιούν τα συνδεδεμένα αυτοκίνητα.

Κλείνοντας θα τεθούν επί τάπητος περισσότερα από ένα παραδείγματα παραβίασης ιδιωτικότητας για την καλύτερη κατανόηση των κινδύνων που ελλοχεύουν από τις ενέργειες αυτές.

Λέξεις Κλειδιά: *Ηλεκτρονικός Έλεγχος οχήματος, αισθητήρες, Οδική Ασφάλεια, GPS, προσωπικά δεδομένα καταναλωτών, Πρωτόκολλα ασφαλείας, Παραβίαση ιδιωτικότητας*

Abstract

Connected vehicles are becoming more and more widespread worldwide. Most of the new manufactured vehicles are following the evolution of technology, which has already delivered revolutionary methods of road safety, as well as many choices for entertainment purposes for the passengers of a connected vehicle. Regarding the road safety measures of the new vehicles, quite a lot of sensors are managing to obtain data from different information sources of the vehicle, and they present them via electronic indicators to the driver. Sensors also provide relevant information at the electronic control unit of the vehicle (ECU).

The new connected vehicles are always connected to the internet and with this way, they are letting their drivers to know the current situation of the vehicle as well as the status of it (whether if it is locked or unlocked) and regarding its position via GPS signal. The connected vehicle can also obtain software updated from the manufacturer company anytime and to communicate with third party's items such as satellites for GPS signal.

Despite the enthusiasm that it is created for this whole new framework and for the new capabilities of the vehicles, several concerns and fears are unlocked regarding the reliability of the security of the networks that these cars are interacting with. Probably a malicious attack and a security breach at the communication networks of the connected cars could possibly create several traffic incidents and accidents. Furthermore, the main concern is the personal information data management which is gathered from these smart electronic systems. The question is "How can we be sure that the recording data will not leak out deliberately or not", so the manufacturing company gains even more profit from customers by selling their personal data to third parties.

At the below master's thesis, we will try to evaluate and present the mode of operation for these systems in the connected vehicles framework which is remarkable. We will also present and evaluate more than one example of security privacy breach, for a better understanding of the dangers which arise from these actions.

Keywords: *ECU (Electronic Control Unit), Sensors, Road Safety, GPS, Personal data of customers, Security of Networks, Security breach*

1

Τα στάδια εξέλιξης του αυτοκινήτου

1.1 Γνωρίζοντας το αυτοκίνητο

Με τον όρο αυτοκίνητο, ονομάζουμε το τετράτροχο επιβατικό όχημα, με κινητήρα εσωτερικής καύσης (μέχρι το έτος 2020), αλλά και με ηλεκτρικό/υβριδικό κινητήρα στο έτος 2024. Θεωρείται ακόμα και στις μέρες μας ως το χρησιμότερο και πιο διαδεδομένο μεταφορικό μέσο του κόσμου. Περισσότερες από 60 διαφορετικές αυτοκινητοβιομηχανίες έχουν αναπτυχθεί παγκοσμίως λανσάροντας αρκετούς διαφορετικούς τύπους αυτοκινήτων όπως SUV, Sedan, Coupe, Jeep κ.α. [1]

Το έτος 2022, ξοδεύτηκαν σχεδόν 2 τρισεκατομμύρια Αμερικανικά δολάρια μόνο για τις πρώτες 20 αυτοκινητοβιομηχανίες συνολικά παγκοσμίως, για πωλήσεις επιβατικών και επαγγελματικών αυτοκινήτων. Αυτό το νούμερο είναι κατά 12% υψηλότερο σε σχέση με το 2021. Την μερίδα του λέοντος την είχε η Toyota με συνολικά 10,48 εκατομμύρια πωλήσεις παγκοσμίως, που ισοδυναμεί με το 8% της παγκόσμιας αγοράς. [2]

1.1.1 Ιστορική αναδρομή του αυτοκινήτου

Το έτος 1886 ο Γερμανός εφευρέτης Karl Benz αποκτώντας το δίπλωμα ευρεσιτεχνίας (Benz Motorwagen) ουσιαστικά φέρνει στην αγορά το αυτοκίνητο όπως το γνωρίζουμε σήμερα. Έπειτα, τα αμέσως επόμενα χρόνια, την σκυτάλη παίρνουν οι Αμερικανοί και πιο συγκεκριμένα η αυτοκινητοβιομηχανία της Ford. Με το πρώτο μοντέλο της (Model T) σαρώνει την αμερικανική αγορά και φέρνει την πρώτη επανάσταση στο χώρο των μεταφορών και της αυτοκίνησης. Από τότε ως τώρα πληθώρα πραγμάτων και τεχνολογιών έχουν ενσωματωθεί στα σύγχρονα αυτοκίνητα.[3]

1.1.2 Εξέλιξη του αυτοκινήτου

Όπως προαναφέρθηκε το πρώτο αυτοκίνητο κατασκευάστηκε με κινητήρα εσωτερικής καύσης. Με την πάροδο των χρόνων και την βοήθεια της τεχνολογίας όμως, τα αυτοκίνητα εξελίχθηκαν και πλέον διακρίνεται ορατά η μετάβαση στο υβριδικό και ηλεκτρικό αυτοκίνητο. [4]

Η εξέλιξη των αυτοκινήτων περιλαμβάνει επίσης τη βελτίωση της ασφάλειας, τη μείωση της ρύπανσης, την εφευρετικότητα στα συστήματα πέδησης και οδήγησης (ABS- EBD).

Παρατηρείται ότι πλέον τα αυτοκίνητα έχουν αναβαθμιστεί τεχνολογικά με αποτέλεσμα να συνδυάζουν άνεση και ασφάλεια, ενώ συνεχίζουν να εξελίσσονται ακόμη περισσότερο με προσθήκη αυτόνομης οδήγησης (Eyes on the road) και πληθώρα καινοτόμων λειτουργιών.

1.1.3 Το αυτοκίνητο σήμερα

Το αυτοκίνητο σήμερα έχει μετασχηματιστεί σε όλα τα επίπεδα σε σχέση με τον προκάτοχό του. Ξεκινώντας από την συνδεσιμότητα, τα καινούργια αυτοκίνητα είναι πλέον συνδεδεμένα στο διαδίκτυο. Το διαδίκτυο των πραγμάτων (IoT), επιτρέπει την επικοινωνία τους με άλλες συσκευές, με διάφορα συστήματα πλοήγησης καθώς και με νέες υποδομές και έξυπνα συστήματα προηγμένων πόλεων. Έπειτα με την άνοδο της τεχνολογίας, γίνεται μετάβαση στην αυτόνομη οδήγηση. Υπάρχει τεράστια βελτίωση στο τομέα αυτό, Για παράδειγμα υπάρχουν αυτοκίνητα όπως το Model x της Tesla, για τα οποία οι κατασκευαστές τους υποστηρίζουν ότι ο αυτόματος πιλότος μπορεί να αναλάβει εξ' ολοκλήρου την μετάβαση από ένα σημείο σε ένα άλλο χωρίς τον παραμικρό κίνδυνο ατυχήματος. Επιπροσθέτως, η βιωσιμότητα χρησιμοποιώντας ανακυκλωμένα υλικά, έχει ξεκινήσει να λαμβάνει χώρα όλο και περισσότερο. Οι εταιρείες αυτοκινήτων επικεντρώνονται όλο και περισσότερο στη μείωση των ρύπων (Αποτυπώματα του άνθρακα) και την δημιουργία όλο και πιο βιώσιμων μοντέλων με χρήση ανακυκλώσιμων υλικών και άλλων πρακτικών. Για το τέλος μένει η ασφάλεια. Έχουν γίνει συντονισμένες προσπάθειες με διάφορα τεχνολογικά συστήματα όπως το ABC, EBD, Hill Stop, τα οποία βοηθούν τους οδηγούς στην πρόληψη ατυχημάτων. Επιπλέον οι διάφοροι αισθητήρες παρακολουθούν την οδική συμπεριφορά και ενεργοποιούν αυτόματα συστήματα αποφυγής σύγκρουσης σε περίπτωση που χρειαστεί. [5]

1.1.4 Τα νέα διασυνδεδεμένα αυτοκίνητα είναι ακόμα ένας κλάδος του λεγόμενου *Internet of Things (IoT)*

Τα διασυνδεδεμένα αυτοκίνητα, είναι ακόμη ένα παρακλάδι του διαδικτύου των πραγμάτων (Internet of Things). Σαν ορισμό του διαδικτύου των πραγμάτων μπορούμε να ορίσουμε ως: Ένα παγκόσμιο δίκτυο διαφόρων φυσικών αντικειμένων (ηλεκτρικών και μη) τα οποία αλληλεπιδρούν σε ένα περιβάλλον δικτύου, και μπορούν να επικοινωνήσουν μεταξύ τους, αλλά και με άλλες συσκευές (H/Y, κινητό τηλέφωνο, τάμπλετ). Το κάθε αντικείμενο διαθέτει μια μοναδική Mac address, και αισθητήρες που διοχετεύουν διάφορες πληροφορίες σε διάφορες εφαρμογές που παρουσιάζουν στον χρήστη όλες τις σημαντικές πληροφορίες που χρειάζεται να μάθει. Η επανάσταση του IoT έχει εισέλθει σε όλες τις οικιακές ηλεκτρικές συσκευές (πχ κουζίνα, κλιματιστικό, ψυγείο), στην υγεία (διάφορα smart watches που παρακολουθούν τους σφυγμούς

και το επίπεδο οξυγόνου στο αίμα ενός ασθενή), όπως επίσης και στα αυτοκίνητα με λειτουργίες που θα εξεταστούν παρακάτω. [6]

1.1.5 Κατανόηση Ευρωπαϊκού νομικού πλαισίου και προστασία της ιδιωτικότητας

Η άνεση και η καινοτομία που μας προσφέρει η ανάπτυξη της τεχνολογίας, μέσω του IoT, καθώς και η αυξανόμενη χρήση του διαδικτύου έχει διάφορους κινδύνους. Η παραβίαση από τρίτους της ασφάλειας του δικτύου, και η πρόσβαση σε ιδιωτικά δεδομένα, είναι ο μεγαλύτερος φόβος των χρηστών. Υπάρχει όμως και η κακοπροαίρετη διαχείριση των προσωπικών δεδομένων από τους ίδιους τους κατασκευαστές αυτοκινήτων, με την αθέμιτη καταγραφή προσωπικών δεδομένων, και διανομή τους σε τρίτους. Για τα παραπάνω, υπάρχει η προστατευτική ομπρέλα της νομοθετικής εξουσίας κάθε κράτους, αλλά και το Ευρωπαϊκό νομικό πλαίσιο για την προστασία της ιδιωτικότητας και της ασφάλειας των ανθρώπων. [7]

1.2 Σκοπός της διπλωματικής εργασίας

Σε αυτή τη διπλωματική εργασία θα γίνει ανάλυση του πως η σύνδεση των αυτοκινήτων μπορεί να προσφέρει πλεονεκτήματα στην οδική ασφάλεια, την άνεση και την ευχρηστία, καθώς επίσης και στην ανάλυση των προκλήσεων που σχετίζονται με την ιδιωτικότητα. Θα γίνει εκτενής αναφορά σε ζητήματα όπως η συλλογή και η διαχείριση δεδομένων, η προστασία από κυβερνοεγκλήματα και οι νομοθετικοί περιορισμοί.

Το διαδίκτυο των πραγμάτων επεκτείνεται, με την συνδρομή διαφόρων εργαλείων που πλέον έχουν εγκατασταθεί στο αυτοκίνητο (Αισθητήρες), όπως επίσης και με τη βοήθεια διάφορων εφαρμογών (Apple Play, Android auto) οι οποίες ουσιαστικά κάνουν το Smartphone ένα με το αυτοκίνητό. Η συνάρτηση αυτή οδηγεί στη σιγουριά ότι οι αυτοκινητοβιομηχανίες θα προσφέρουν στο άμεσο μέλλον σχεδόν μηδαμινές πιθανότητες ατυχημάτων στην ασφαλτο. Οι διάφορες τεχνολογίες που θα αναλυθούν μια προς μια στα επόμενα κεφάλαια, έχουν ξεκινήσει να βοηθούν τον οδηγό σε πολλά σημεία της οδικής συμπεριφοράς. Ο απόλυτος στόχος είναι μελλοντικά να αναλάβουν τον έλεγχο της οδήγησης (Σαν αυτόματος πιλότος αεροπλάνου) με σκοπό τον μηδενισμό τροχαίων ατυχημάτων. Ωστόσο η τεχνολογία δεν έχει μείνει στο κομμάτι της συλλογής δεδομένων αποκλειστικά για την οδική συμπεριφορά. Πλέον τα διασυνδεδεμένα αυτοκίνητα, σαν άλλος ηλεκτρονικός υπολογιστής, προσφέρουν πληθώρα άλλων δυνατοτήτων στους επιβάτες. Η διασκέδαση και η πλοήγηση είναι μερικές από αυτές τις δυνατότητες.

1.3 Δομή της διπλωματικής εργασίας

Στη παρακάτω μεταπτυχιακή διπλωματική εργασία, θα γίνει προσπάθεια επεξήγησης των χαρακτηριστικών των διασυνδεδεμένων αυτοκινήτων, σε ταυτόχρονη αντιπαραβολή σχετικών παραδειγμάτων για την ευκολότερη κατανόηση από τον αναγνώστη. Στο δεύτερο μέρος αυτής θα γίνει εκτενής επεξήγηση στο τι είναι η ιδιωτικότητα και στο πως μπορεί να παραβιαστούν τα προσωπικά δεδομένα των οδηγών αυτών των αυτοκινήτων. Πιο συγκεκριμένα, στο δεύτερο

κεφάλαιο θα αναλυθεί σε πρώτη φάση τι είναι το ασύρματο δίκτυο πολλαπλών διαδρομών , Vehicular ad hoc network εν συντομία (VANET). Στο τρίτο κεφάλαιο θα γίνει αναφορά στις τεχνολογίες επικοινωνίας των έξυπνων αυτοκινήτων. Πρώτα στο εσωτερικό του με το πρωτόκολλο CAN, και έπειτα στις επιμέρους ασύρματες τεχνολογίες όπως Bluetooth και NFC. Έπειτα στο τέταρτο κεφάλαιο, γίνεται μια αναφορά στα πλεονεκτήματα των τεχνολογιών των διασυνδεδεμένων οχημάτων, αλλά και στα διάφορα μειονεκτήματα αυτών. Συνεχίζοντας στο πέμπτο κεφάλαιο, θα γίνει αναφορά στην ιδιωτικότητα αλλά και στα προσωπικά δεδομένα. Επιπροσθέτως στο κεφάλαιο 6, θα γίνει αναφορά στις ευπάθειες του δικτύου VANET, στο προφίλ των επιτιθέμενων σε αυτό χρηστών, αλλά επίσης και στις τεχνικές που χρησιμοποιούν. Εκτενής αναφορά θα γίνει επίσης σε διάφορα πρωτόκολλα προστασίας της ιδιωτικότητας.

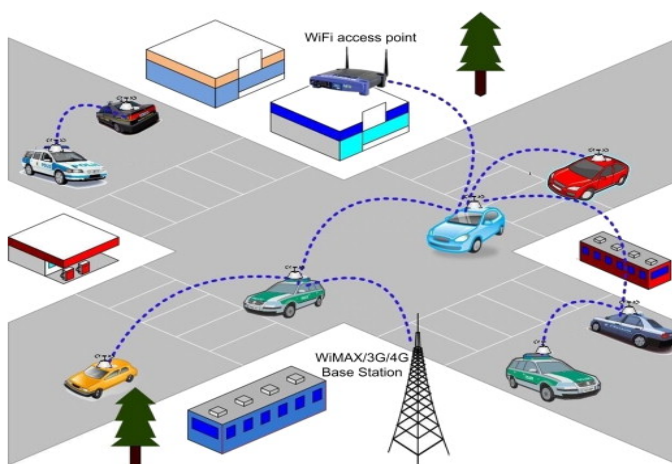
2

Το εσωτερικό των διασυνδεδεμένων αυτοκινήτων (Connected Vehicles interior)

2.1 Τι είναι το VANET (Vehicular ad hoc network)

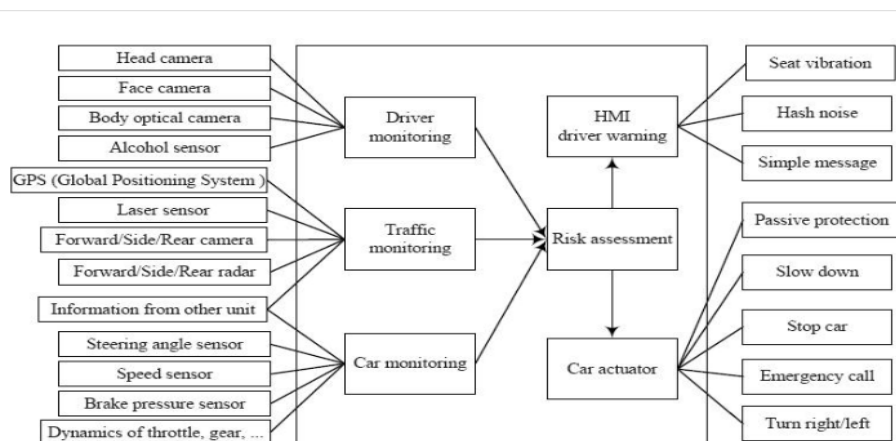
Το VANET είναι μια ειδική περίπτωση ασύρματου δικτύου πολλαπλών διαδρομών, το οποίο έχει τον περιορισμό των γρήγορων αλλαγών τοπολογίας λόγω της μεγάλης κινητικότητας των κόμβων. Με την αύξηση του αριθμού των οχημάτων που είναι εξοπλισμένα με τεχνολογίες πληροφορικής και ασύρματες συσκευές επικοινωνίας, η επικοινωνία μεταξύ οχημάτων γίνεται ένα πολλά υποσχόμενο πεδίο έρευνας, τυποποίησης και ανάπτυξης. Τα VANET επιτρέπουν ένα ευρύ φάσμα εφαρμογών, όπως η πρόληψη συγκρούσεων, η ασφάλεια, η διέλευση τυφλών, ο δυναμικός προγραμματισμός διαδρομών, η παρακολούθηση της κατάστασης της κυκλοφορίας σε πραγματικό χρόνο κ.λπ. Μια άλλη σημαντική εφαρμογή για τα VANETs είναι η παροχή συνδεσιμότητας στο Διαδίκτυο σε κόμβους οχημάτων. [8]

Σχήμα 1: Στο δίπλα σχήμα παρατηρούμε ένα σχετικό παράδειγμα του VANET.



2.2 Η αρχιτεκτονική των σύγχρονων αυτοκινήτων

Ένα διασυνδεδεμένο αυτοκίνητο είναι μια ολοκληρωμένη ενσωμάτωση πολλών διαφορετικών αισθητήρων και μονάδων ελέγχου. Ένα διασυνδεδεμένο αυτοκίνητο μπορεί να παρακολουθεί το περιβάλλον οδήγησης, να αξιολογεί πιθανούς κινδύνους και να λαμβάνει τα κατάλληλα μέτρα για να αποφύγει ή να μειώσει τον κίνδυνο. Η γενική αρχιτεκτονική ενός έξυπνου αυτοκινήτου παρουσιάζεται στο παρακάτω σχήμα. [9]



General architecture of a smart car.

Σχήμα 2: Ένα σύστημα υποστήριξης οδηγού με επίγνωση του περιβάλλοντος για έξυπνα αυτοκίνητα που βασίζονται σε VANET

Η αρχιτεκτονική του διασυνδεδεμένου αυτοκινήτου αντικατοπτρίζει τον τρόπο με τον οποίο η τεχνολογία ενσωματώνεται στα οχήματα για να προσφέρει προηγμένες λειτουργίες, ασφάλεια, ενημέρωση και ενεργειακή απόδοση. Η ανάπτυξη των έξυπνων αυτοκινήτων βασίζεται σε πληθώρα τεχνολογιών, περιλαμβανομένων αισθητήρων, επεξεργαστών, λογισμικού και επικοινωνιακών συστημάτων.

2.3 Βασικός εξοπλισμός ενός διασυνδεδεμένου οχήματος

Τα πλήρως αυτοματοποιημένα διασυνδεδεμένα οχήματα κατά μεγάλη πιθανότητα δεν θα είναι διαθέσιμα για κυκλοφορία για τουλάχιστον 10 χρόνια ακόμη. Αυτά τα οχήματα είναι αλήθεια ότι αντιπροσωπεύουν το μέλλον της αυτοματοποιημένης οδήγησης. Το διασυνδεδεμένο όχημα είναι αυτόνομο και ο ανθρώπινος παράγοντας (οδηγός) θα ήταν επιθυμητό να μην παίρνει εξολοκλήρου τον έλεγχο του οχήματος για όλη τη διάρκεια της διαδρομής που θα έχει ορίσει πριν την έναρξη της. Επιπλέον, το επιθυμητό και αναμενόμενο χαρακτηριστικό των οχημάτων αυτών, είναι ότι το κάθε αυτόνομο διασυνδεδεμένο όχημα, θα πρέπει να περιέχει τουλάχιστον βασικά χαρακτηριστικά που προσφέρονται σε προσφορές αυτοκινήτων μεσαίας κατηγορίας που πωλούνται σήμερα και στις ίδιες

τιμές με τα σημερινά αυτοκίνητα, ώστε να υπάρξουν και οι κατάλληλες προϋποθέσεις για να αγοραστεί από τους μέσους (σε οικονομική δυνατότητα) καταναλωτές.

Μια καινοτομία των διασυνδεδεμένων οχημάτων θα είναι και οι περιστρεφόμενες θέσεις στο εσωτερικό τους. Όπως αναφέρθηκε παραπάνω, το ζητούμενο είναι ο οδηγός να μην ασκεί καμία επιρροή στη πορεία του διασυνδεδεμένου οχήματος. Επομένως δίνεται η δυνατότητα ο οδηγός να αλληλεπιδρά με ασφάλεια με τους υπόλοιπους επιβάτες του οχήματος. Γι αυτό το σκοπό οι μπροστινές θέσεις του οδηγού και του συνοδηγού θα μπορούν να περιστρέφονται και πριν την εκκίνηση αλλά και κατά τη διάρκεια της πορείας του οχήματος προς το μέρος των πίσω θέσεων. [10]



Σχήμα 3: Το εσωτερικό ενός διασυνδεδεμένου αυτοκινήτου

Με την λειτουργία της αυτόνομης οδήγησης του οχήματος, ο οδηγός και οι επιβάτες των οχημάτων αυτών έχουν τις παρακάτω δυνατότητες :

- Δυνατότητα ξεκούρασης και ύπνου. Οι επιβάτες του οχήματος συμπεριλαμβανομένου και του οδηγού αυτού, θα μπορούν να ξεκουράζονται και ακόμη να κοιμούνται καθώς η λειτουργία αυτόνομης οδήγησης εξασφαλίζει τη δυνατότητα ασφαλούς οδήγησης χωρίς την επίβλεψη του ανθρωπίνου παράγοντα.
- Δυνατότητα παροχής γεύματος. Ο οδηγός θα μπορεί να καταναλώσει το γεύμα του χωρίς να ανησυχεί για την οδηγική συμπεριφορά του αυτοκινήτου.
- Δυνατότητες διασκέδασης. Ο οδηγός θα μπορεί να παρακολουθεί για παράδειγμα ένα τηλεοπτικό σόου της αρεσκείας του στην βασική οθόνη του οχήματος χωρίς να ανησυχεί για την οδηγική συμπεριφορά του αυτοκινήτου.

Οι κύριες συνιστώσες της αρχιτεκτονικής ενός έξυπνου αυτοκινήτου περιλαμβάνουν:

- **Αισθητήρες:**

Τα έξυπνα αυτοκίνητα είναι εξοπλισμένα με διάφορους τύπους αισθητήρων για την συλλογή δεδομένων από το περιβάλλον. Αισθητήρες όπως ραντάρ, κάμερες, λέιζερ, αισθητήρες υπερήχων και αισθητήρες θερμοκρασίας βοηθούν στην παρακολούθηση του οχήματος και του περιβάλλοντος του.

- **Επεξεργαστές και λογισμικό:**

Προηγμένοι επεξεργαστές, όπως οι ενσωματωμένοι υπολογιστές, επιτρέπουν την ανάλυση των δεδομένων που συλλέγονται από τους αισθητήρες. Το λογισμικό ελέγχου οχήματος διαχειρίζεται την εκτέλεση διαφόρων λειτουργιών, όπως η αυτόνομη οδήγηση, η παρακολούθηση της κίνησης και η ανταπόκριση σε αισθητήρες ασφαλείας.

- **Συστήματα Επικοινωνίας:**

Η αρχιτεκτονική περιλαμβάνει συστήματα επικοινωνίας που επιτρέπουν τη σύνδεση του αυτοκινήτου με άλλα οχήματα, τον οδηγό, τον χρήστη και το διαδίκτυο. Αυτή η συνδεσιμότητα επιτρέπει τη μεταφορά δεδομένων, ενημερώσεις λογισμικού και αλληλεπίδραση με άλλες ψηφιακές πλατφόρμες.

- **Αυτόνομη Οδήγηση:**

Οι σύγχρονες αρχιτεκτονικές επιτρέπουν την υλοποίηση συστημάτων αυτόνομης οδήγησης. Αυτά τα συστήματα βασίζονται σε αισθητήρες και επεξεργαστές για την παρακολούθηση του περιβάλλοντος και την αυτόνομη λήψη αποφάσεων για την κατεύθυνση και την ταχύτητα.

- **Συστήματα Ασφαλείας:**

Προηγμένα συστήματα ασφαλείας όπως τα εξελιγμένα συστήματα φρεναρίσματος, ηλεκτρονικά συστήματα ελέγχου πρόσφυσης, και αυτόνομα συστήματα αποφυγής σύγκρουσης βελτιώνουν την ασφάλεια του οχήματος.

- **Ενημέρωση και Ψυχαγωγία:**

Ενσωματωμένα συστήματα ενημέρωσης και ψυχαγωγίας προσφέρουν στους επιβάτες πληροφορίες, ψυχαγωγία και συνδεσιμότητα με φορητές συσκευές.

Η εξέλιξη στην αρχιτεκτονική των έξυπνων αυτοκινήτων επικεντρώνεται στη βελτίωση της ασφάλειας, της ενεργειακής απόδοσης και της ολοκληρωμένης εμπειρίας του οδηγού και των επιβατών. Καθώς η τεχνολογία συνεχίζει να προχωρά, αναμένεται ότι τα έξυπνα αυτοκίνητα θα εξελίσσονται και θα ενσωματώνουν νέες καινοτομίες για τη μετέπειτα εξέλιξη της αυτοκινητοβιομηχανίας. [11]



Σχήμα 4:

Στο σχήμα αριστερά παρατηρούμε την οθόνη 9.1 ιντσών ενός Renault Clio, η οποία παρέχει πληθώρα παροχών ενημέρωσης και ψυχαγωγίας για τους επιβάτες του αυτοκινήτου. [12]

2.3.1 Στοιχεία ενός διασυνδεδεμένου αυτοκινήτου

Τα διασυνδεδεμένα αυτοκίνητα συνδυάζουν πολλά προηγμένα στοιχεία και τεχνολογίες προκειμένου να προσφέρουν εξειδικευμένες λειτουργίες και βελτιωμένη εμπειρία οδήγησης. Ανάλογα με το μοντέλο και την εταιρεία κατασκευής, τα στοιχεία ενός έξυπνου αυτοκινήτου μπορεί να διαφέρουν.

2.3.1.1 Οθόνη αφής με υψηλή ανάλυση.

Η οθόνη αφής ίσως είναι το πιο διακριτό και διάσημο στοιχείο των σύγχρονων αυτοκινήτων. Βάση της οθόνης αυτής πραγματοποιείται η μεγαλύτερη αλληλεπίδραση μεταξύ χρήστη και αυτοκινήτου. Η οθόνη περιέχει όλες τις παρακάτω λειτουργίες:

- i. Ραδιόφωνο
- ii. Ρύθμιση θερμοκρασίας του κλιματισμού
- iii. Διαχείριση τηλεφωνικών κλήσεων σε περίπτωση σύνδεσης του κινητού τηλεφώνου με το αυτοκίνητο
- iv. Αντικατοπτρισμός της οθόνης του κινητού τηλεφώνου (Mirroring)
- v. Διαχείριση ασύρματης συνδεσιμότητας συσκευών με χρήση της τεχνολογίας Bluetooth. (Tablet)
- vi. Παρακολούθηση του ενσωματωμένου συστήματος πλοήγησης (GPS)
- vii. Αλληλεπίδραση χρήστη με διάφορες εφαρμογές ψυχαγωγίας
- viii. Παρακολούθηση συστημάτων ασφαλείας. [13]



Σχήμα 5: Στη δίπλα εικόνα παρατηρούμε την οθόνη αφής υψηλής ανάλυσης μιας Mercedes A-180. Παρατηρούμε προσεκτικά επίσης ότι η επιφάνεια των οργάνων μέτρησης (Cadran), έχει αντικατασταθεί και αυτή από οθόνη υψηλής ευκρίνειας.

[14]

2.3.1.1.1 Συναγερμός αντικλεπτικής προστασίας.

Ένα όχημα, δεν κινδυνεύει μόνο από τον παράγοντα ενός τροχαίου ατυχήματος. Οι κλοπές έχουν αυξηθεί κατακόρυφα καθώς το αυτοκίνητο ήταν, είναι και θα είναι πάντα ένα αγαθό ακριβό και απαραίτητο για την ανθρώπινη διαβίωση. Η αύξηση των τεχνολογιών του, έχουν οδηγήσει και στην αύξηση των τιμών πώλησης των επιβατικών οχημάτων. [15]



Σχήμα 6: Στην παραπάνω εικόνα διακρίνουμε την σχετική κάμερα παρακολούθησης σε ένα διασυνδεδεμένο όχημα Tesla Model X.

2.3.1.1.2 Αισθητήρες παρακολούθησης.

Στα τεχνικά «αόρατα» μέρη του αυτοκινήτου ένα ευρύ φάσμα αισθητήρων δίνει τα απαραίτητα δεδομένα στον οδηγό για την αναγνώριση οδικών σημάτων, διελεύσεις πεζών, αλλαγή λωρίδας αλλά και για την αυτόνομη λειτουργία του διασυνδεδεμένου οχήματος όπου αυτό είναι δυνατό. Αυτές οι λειτουργίες είναι οι κατεξοχήν δυναμικές λειτουργίες ενός σύγχρονου smart car.

2.3.1.1.3 Συστήματα Αυτόνομης Οδήγησης:

Ο απώτερος στόχος των μηχανικών αυτοκινήτων, είναι μελλοντικά η αυτόματη οδήγηση του οχήματος, κάτι σαν τον σημερινό αυτόματο πιλότο του αεροπλάνου. Αυτό σύμφωνα με τους μηχανικούς της Tesla Motorworks έχει καταστεί ήδη μερικώς εφικτό σε επίπεδο οδήγησης. Πιο συγκεκριμένα, ο αυτόματος πιλότος της Tesla, είναι ένα προηγμένο σύστημα υποβοήθησης οδηγού, το ονομαζόμενο ADAS (Advanced driver assistance system) που αναπτύχθηκε και ισοδυναμεί με μερική αυτοματοποίηση οδήγησης του οχήματος (αυτοματισμός επιπέδου 2, όπως ορίζεται από τη Society of Automotive Engineers εν συντομία SAE). Η Tesla παρέχει "Βασικό αυτόματο πιλότο" σε όλα τα οχήματα της, ο οποίος περιλαμβάνει κεντράρισμα λωρίδας και cruise control με επίγνωση της κυκλοφορίας. Οι ιδιοκτήτες μπορούν να αγοράσουν μια αναβάθμιση σε "Enhanced Autopilot" (EA) που προσθέτει ημιαυτόνομη πλοήγηση σε δρόμους περιορισμένης πρόσβασης, αυτόματη στάθμευση και τη δυνατότητα κλήσης του αυτοκινήτου από γκαράζ ή θέση στάθμευσης προς το μέρος του ιδιοκτήτη. Ωστόσο, υπάρχουν αρκετές καταγγελίες για σωρεία ατυχημάτων που έχουν προκληθεί από αυτού του τύπου την οδήγηση. Θα υπάρξει εκτενέστερη ανάλυση σε επόμενο κεφάλαιο. Μια πιο πρώιμη μορφή αυτόματης οδήγησης, έστω και αρκετά βραχυπρόθεσμης, είναι το αυτόματο παρκάρισμα του αυτοκινήτου. Αρκετοί κατασκευαστές αυτοκινήτων έχουν προσθέσει αυτή την λειτουργία κυρίως σε οχήματα πολυτελείας. [16]



Σχήμα 7: Στη δίπλα εικόνα φαίνεται σε μια Mercedes A-200 η αυτόματη λειτουργία παρκκαρίσματος (Active Parking Assistant). [17]

2.3.1.1.4 Συστήματα Ενεργειακής Απόδοσης

Μια ακόμα σημαντική πτυχή των διασυνδεδεμένων οχημάτων, είναι και η τεχνολογία των συστημάτων ενεργειακής απόδοσης. Η περιβαλλοντική καταστροφή που έχει συντελεστεί κατά την διάρκεια των τελευταίων 50 χρόνων είναι σημαντική, και τα αυτοκίνητα με κινητήρες εσωτερικής καύσης (Βενζινοκινητήρες και πετρελαιοκινητήρες) έχουν σημαντικότατο μερίδιο για αυτή. Οι ιδιοκτήτες σε συνεργασία με τους μηχανικούς και τους περιβαλλοντολόγους των σύγχρονων αυτοκινητοβιομηχανιών, δε θα μπορούσαν να μην ευαισθητοποιηθούν και να πραγματοποιήσουν τεχνολογικά άλματα για την διαχείριση αυτού του καίριου ζητήματος. Οι υβριδικοί και οι ηλεκτρικοί κινητήρες των αυτοκινήτων, σε συνδυασμό με διάφορες τεχνολογίες μείωσης της κατανάλωσης καυσίμων σε βενζινοκινητήρες και πετρελαιοκινητήρες έχουν συνθέσει ένα νέο τοπίο στην ενεργειακή απόδοση των σύγχρονων διασυνδεδεμένων αυτοκινήτων. Η τεχνολογία start stop των απλών συμβατικών κινητήρων, είναι μια χαρακτηριστική τεχνολογία για εξοικονόμηση καυσίμου. Πιο συγκεκριμένα σε πείραμα που πραγματοποιήθηκε στις ΗΠΑ το 2022, η τεχνολογία start stop δοκιμάστηκε με τα εξής αποτελέσματα:

Δύο αυτοκίνητα που διέθεταν το σύστημα αυτό, οδηγήθηκαν σε μια διαδρομή 80 μιλίων που περιελάμβανε πολλές στάσεις, μια φορά με το σύστημα ενεργοποιημένο και μια άλλη φορά απενεργοποιημένο. Και τα δύο αυτοκίνητα έκαιγαν λιγότερα καύσιμα με την τεχνολογία ενεργοποιημένη και βελτίωσαν τη διανυθείσα χιλιομετρική τους απόσταση. Τα τεχνικά συμπεράσματα είναι τα παρακάτω:

Παρατηρήθηκε μείωση κατανάλωσης καυσίμου από 3% έως και 12% με το κλείσιμο του οχήματος όταν σταματούσε. [18]

3

Εσωτερική και εξωτερική δικτύωση των διασυνδεδεμένων οχημάτων.

3.1 Εσωτερική δικτύωση

Τα διασυνδεδεμένα αυτοκίνητα χρησιμοποιούν διάφορες τεχνικές επικοινωνίας για να επικοινωνήσουν εσωτερικά και εξωτερικά. Πιο συγκεκριμένα, παρατηρούνται εξίσου ασύρματες (Wireless Connections) αλλά και ενσύρματες συνδέσεις (Wired Connections) εντός του οχήματος.

3.1.1 Οι ενσύρματες συνδέσεις.

Η πρώτη ενσύρματη σύνδεση που θα αναλύσω είναι το πρωτόκολλο CAN (Controller Area Network). Το CAN είναι ένα σειριακό πρωτόκολλο επικοινωνίας το οποίο υποστηρίζει πολύ αποτελεσματικά τον έλεγχο πολλών συσκευών σε πραγματικό χρόνο. Φτάνοντας στο σήμερα, όλα τα καινούρια επιβατικά αυτοκίνητα διαθέτουν δίκτυα τύπου CAN. Ακόμα λόγω της επιτυχίας του CAN στην αυτοκινητοβιομηχανία σήμερα χρησιμοποιείται και από άλλους τύπους μεταφορικών μέσων όπως αεροπλάνα, πλοία, τρένα, διαστημόπλοια, καθώς επίσης στην βιομηχανία και στα ιατρικά μηχανήματα. [19]

3.1.1.1 Ανάλυση του CAN

Ένας δίαυλος δικτύου ελεγκτή περιοχής (CAN), είναι ένα σύστημα σειριακού διαύλου υψηλής ακεραιότητας για τη δικτύωση έξυπνων συσκευών. Οι δίαυλοι και οι συσκευές CAN είναι κοινά εξαρτήματα σε συστήματα αυτοκινήτων. Χρησιμοποιώντας μια συσκευή διασύνδεσης, υπάρχει δυνατότητα χρήσης του LabVIEW (To Laboratory Virtual Instrument Engineering Workbench είναι μια πλατφόρμα σχεδιασμού συστήματος και ένα περιβάλλον ανάπτυξης για μια οπτική

γλώσσα προγραμματισμού που αναπτύχθηκε από την National Instruments) για επικοινωνία με ένα δίκτυο. [20]

3.1.1.2 Ιστορία CAN

Το CAN εμφανίστηκε σαν ιδέα το 1983 και παρουσιάστηκε το 1986 στο συνέδριο της Society of Automotive Engineer (SAE) στο Detroit του Michigan, από την εταιρεία Robert Bosch GmbH. Στο παρελθόν, οι κατασκευαστές αυτοκινήτων συνέδεαν ηλεκτρονικές συσκευές σε οχήματα χρησιμοποιώντας συστήματα καλωδίωσης από σημείο σε σημείο. Οι κατασκευαστές άρχισαν να χρησιμοποιούν όλο και περισσότερα ηλεκτρονικά αντικείμενα στα οχήματα, με αποτέλεσμα να δημιουργούνται ογκώδεις μιάντες καλωδίων που ήταν βαριές και ακριβές. Στη συνέχεια αντικατέστησαν την αποκλειστική καλωδίωση με δίκτυα εντός του οχήματος, γεγονός που μείωσε το κόστος, την πολυπλοκότητα και το βάρος της καλωδίωσης. Το CAN, ένα σύστημα σειριακού διαύλου υψηλής ακεραιότητας για τη δικτύωση έξυπνων συσκευών, εμφανίστηκε ως το τυπικό δίκτυο επικοινωνίας εντός του οχήματος. Η αυτοκινητοβιομηχανία υιοθέτησε γρήγορα το CAN και, το 1993, έγινε το διεθνές πρότυπο γνωστό ως ISO 11898. Από το 1994, αρκετά πρωτόκολλα υψηλότερου επιπέδου έχουν τυποποιηθεί στο CAN, όπως το CANopen και το DeviceNet. Άλλες αγορές έχουν υιοθετήσει ευρέως αυτά τα πρόσθετα πρωτόκολλα, τα οποία αποτελούν πλέον πρότυπα για τις βιομηχανικές επικοινωνίες. Το πρωτόκολλο CAN bus αναπτύχθηκε από την Bosch σαν ένα σύστημα αναμετάδοσης μηνυμάτων που καθορίζετε από το πολύ 1 megabit το δευτερόλεπτο (bps). Δυστυχώς το CAN δεν μπορεί στείλει μεγάλα πακέτα δεδομένων από κόμβο σε κόμβο (από A σε B) μέσα από ένα δίκτυο bus όπως τα παραδοσιακά πρωτόκολλα USB ή Ethernet. Στο δίκτυο CAN πολλά μικρά μηνύματα από αισθητήρες όπως η θερμοκρασία ή οι στροφές (RPM=Revolutions Per Minute) μεταδίδονται σε ολόκληρο το δίκτυο, που παρέχει με συνέπεια δεδομένα σε κάθε κόμβο του συστήματος. [21]

3.1.1.3 Οφέλη CAN

Δίνεται η δυνατότητα στον κατασκευαστή να συμπεριλάβει στην άτρακτο του αυτοκινήτου ένα δίκτυο χαμηλού κόστους. Το CAN παρέχει ένα φθηνό, ανθεκτικό δίκτυο που βοηθά πολλές συσκευές να επικοινωνούν μεταξύ τους. Ένα πλεονέκτημα αυτού είναι ότι οι ηλεκτρονικές μονάδες ελέγχου ECU(Electronic Control Unit) μπορούν να έχουν μια ενιαία διασύνδεση αντί για αναλογικές και ψηφιακές εισόδους σε κάθε συσκευή του συστήματος. Αυτό μειώνει το συνολικό κόστος και το βάρος στα αυτοκίνητα. Επιπλέον, το πρωτόκολλο αυτό κατασκευάστηκε με προδιαγραφές υψηλής ανοσίας σε ηλεκτρικές παρεμβολές, την δυνατότητα της αυτοδιάγνωσης και της επισκευής των σφαλμάτων δεδομένων. Αυτά τα χαρακτηριστικά οδήγησαν το πρωτόκολλο CAN στην δημοτικότητα σε μια ποικιλία βιομηχανικών εφαρμογών συμπεριλαμβανομένων των κτιριακών αυτοματισμών της ιατρικής και γενικά της βιομηχανοποίησης. [22]

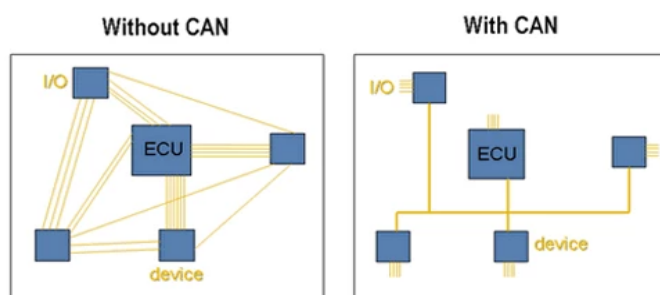
3.1.1.4 Εκπομπή Επικοινωνίας

Κάθε μία από τις συσκευές του δικτύου διαθέτει ένα τσιπ ελεγκτή CAN και επομένως ονομάζεται και ως «έξυπνη». Όλες οι συσκευές στο δίκτυο βλέπουν όλα τα μεταδιδόμενα μηνύματα. Κάθε συσκευή μπορεί να αποφασίσει εάν ένα μήνυμα είναι σχετικό ή αν πρέπει να φιλτραριστεί. Αυτή η δομή επιτρέπει τροποποιήσεις σε δίκτυα με ελάχιστο αντίκτυπο. Πρόσθετοι κόμβοι που δεν

εκπέμπουν μπορούν να προστεθούν χωρίς τροποποίηση στο δίκτυο. Το πρωτόκολλο επικοινωνίας CAN είναι ένα πρωτόκολλο με νοητικές αισθήσεις, με πολλαπλή πρόσβαση, με ανίχνευση σύγκρουσης και διαιτησία σχετικά με την προτεραιότητα των μηνυμάτων (CSMA / CD + AMP). Το CSMA (Carrier Sense Multiple Access), σημαίνει ότι κάθε κόμβος σε ένα δίαυλο πρέπει να περιμένει για μια προκαθορισμένη περίοδο αδράνειας πριν επιχειρήσει να στείλει ένα μήνυμα. Το αναγνωριστικό υψηλότερης προτεραιότητας κερδίζει πάντοτε πρόσβαση στο δίαυλο. Μέχρι και το τελευταίο bit υψηλής λογικής το αναγνωριστικό συνεχίζει να εκπέμπει επειδή είναι η υψηλότερης προτεραιότητας. Σε κάθε κόμβο του διαύλου παίρνει μέρος στο γράψιμο κάθε bit και ένας διαιτητικός κόμβος ξέρει εάν θα τοποθετήσει το υψηλής λογικής bit στο δίαυλο. Το πρότυπο ISO-11898: 2003, με το τυπικό αναγνωριστικό 11-bit, προβλέπει ρυθμούς μετάδοσης από 125 Kbps έως 1 Mbps. Το πρότυπο τροποποιήθηκε αργότερα με το “εκτεταμένο” αναγνωριστικό 29-bit. Το πρότυπο 11-bit αναγνωριστικό πεδίο παρέχει για 211, ή 2048 διαφορετικά αναγνωριστικά μηνύματος, ενώ το διευρυμένο αναγνωριστικό 29-bit παρέχει για 229, ή 537 εκατομμύρια αναγνωριστικά. [23]

3.1.1.5 Προτεραιότητα

Κάθε μήνυμα έχει μια προτεραιότητα, οπότε αν δύο κόμβοι προσπαθήσουν να στείλουν μηνύματα ταυτόχρονα, αυτός με την υψηλότερη προτεραιότητα μεταδίδεται και αυτός με τη χαμηλότερη προτεραιότητα αναβάλλεται. Αυτή η διαιτησία δεν είναι καταστροφική και έχει ως αποτέλεσμα τη μη διακοπή μετάδοσης του μηνύματος υψηλότερης προτεραιότητας. Αυτό επιτρέπει επίσης στα δίκτυα να πληρούν ντετερμινιστικούς χρονικούς περιορισμούς.



Σχήμα 8: Στο δίπλα σχήμα παρατηρούνται τα οφέλη του CAN. [24]

Η πρόσβαση στο δίαυλο bus γίνεται όταν υπάρξει κάποιο συμβάν δηλαδή ένα σήμα από κάποιον αισθητήρα και πραγματοποιείτε τυχαία. Εάν δυο κόμβοι προσπαθήσουν να καταλάβουν ταυτόχρονα το δίαυλο η πρόσβαση υλοποιείτε με μία μη καταστρεπτική διαδικασία για το σήμα μέσω μιας διαιτητικής διαδικασίας. Μη καταστροφική σημαίνει ότι στον κόμβο μετά από μια επιτυχημένη διαιτησία την συνεχίζει σε όλους τους κόμβους με το μήνυμα να συνεχίζεται χωρίς να καταστρέφεται από έναν άλλο κόμβο. Εδώ είναι πολύ σημαντικό να αναφερθεί ότι στα μηνύματα του διαδίκτυου συστήματος το υψηλής λογικής ψηφίο πάει με το λογικό “1” και το χαμηλής λογικής ψηφίο πάει με το λογικό “0” αλλά στο πρωτόκολλο CAN δεν είναι έτσι. Στο πρωτόκολλο CAN το ψηφίο “0” θεωρείτε το ψηφίο προτεραιότητας άρα και ψηφίο υψηλής λογικής. Η κατανομή της προτεραιότητας των μηνυμάτων είναι ένα από τα χαρακτηριστικά που κάνει το CAN ιδιαίτερα ελκυστικό για χρήση μέσα σε περιβάλλον ελέγχου σε πραγματικό χρόνο. Όσο χαμηλότερος είναι λοιπόν ο αριθμός αναγνωριστικού του δυαδικού μηνύματος τόσο

μεγαλύτερη είναι η προτεραιότητα του. Ένα αναγνωριστικό που αποτελείται εξ ολοκλήρου από μηδενικά είναι μήνυμα υψηλότερης προτεραιότητας σε ένα δίκτυο διότι κρατάει κατειλημμένο τον κυρίαρχο δίαυλο για περισσότερο χρόνο. Επομένως εάν δυο κόμβοι αρχίσουν να μεταδίδουν ταυτόχρονα ο κόμβος που στέλνει ένα τελευταίο bit αναγνώρισης ως ‘0’ (κυρίαρχο bit) ενώ οι άλλοι κόμβοι στέλνουν ‘1’ (υπολειπόμενο bit) ο πρώτος κυριαρχεί και κρατά των έλεγχο του διαύλου και συνεχίζει μέχρι να ολοκληρώσει το μήνυμά του. Στο δίκτυο του CAN bus πάντα ένα κυρίαρχο κομμάτι ‘0’ αντικαθιστά ένα υπολειπόμενο κομμάτι ‘1’ στο δίαυλο. Σημαντικό είναι ότι ένας κόμβος μετάδοσης παρακολουθεί συνεχώς κάθε κομμάτι της δικής του μετάδοσης. Έτσι το παρακάτω σχήμα δείχνει την διαδικασία διαιτησίας CAN που χειρίζεται ένας ελεγκτής CAN. Επειδή κάθε κόμβος παρακολουθεί συνεχώς τις δικές του μεταδόσεις, καθώς το υπολειπόμενο bit του κόμβου B αντικαθίσταται από το κυρίαρχο bit υψηλής λογικής του κόμβου C, το B ανιχνεύει ότι η κατάσταση του διαύλου δεν ταιριάζει με το bit που μεταδίδει. Επομένως, ο κόμβος B σταματά τη μετάδοση ενώ ο κόμβος C συνεχίζει με το μήνυμά του. Μια άλλη προσπάθεια μετάδοσης του μηνύματος γίνεται από τον κόμβο B μόλις απελευθερωθεί ο δίαυλος από τον κόμβο C. Αυτή η λειτουργία είναι μέρος της φυσικής σηματοδότησης του ISO 11898, το οποίο σημαίνει ότι περιέχεται εξ ολοκλήρου στον ελεγκτή CAN και είναι απολύτως διαφανής στον χρήστη του CAN.

3.1.1.6 Λειτουργία επικοινωνίας CAN

Όπως αναφέρθηκε προηγουμένως, το CAN είναι ένα δίκτυο peer-to-peer *. Αυτό σημαίνει ότι δεν υπάρχει κύριος που να ελέγχει πότε μεμονωμένοι κόμβοι έχουν πρόσβαση σε δεδομένα ανάγνωσης και εγγραφής στο δίαυλο. Όταν ένας κόμβος είναι έτοιμος να μεταδώσει δεδομένα, ελέγχει αν ο δίαυλος είναι απασχολημένος και, στη συνέχεια, απλώς γράφει ένα πλαίσιο στο δίκτυο. Τα πλαίσια που μεταδίδονται δεν περιέχουν διευθύνσεις ούτε του κόμβου μετάδοσης ούτε οποιουδήποτε από τους προβλεπόμενους κόμβους λήψης. Αντίθετα, ένα αναγνωριστικό διαιτησίας που είναι μοναδικό σε όλο το δίκτυο επισημαίνει το πλαίσιο. Όλοι οι κόμβοι στο δίκτυο λαμβάνουν το πλαίσιο και, ανάλογα με το αναγνωριστικό διαιτησίας αυτού του μεταδιδόμενου πλαισίου, κάθε κόμβος στο δίκτυο αποφασίζει εάν θα αποδεχτεί το πλαίσιο. Εάν πολλοί κόμβοι προσπαθήσουν να μεταδώσουν ένα μήνυμα στον δίαυλο ταυτόχρονα, ο κόμβος με την υψηλότερη προτεραιότητα (χαμηλότερο αναγνωριστικό διαιτησίας) αποκτά αυτόματα πρόσβαση στο δίαυλο. Οι κόμβοι χαμηλότερης προτεραιότητας πρέπει να περιμένουν μέχρι να γίνει διαθέσιμος ο δίαυλος προτού προσπαθήσουν ξανά να εκπέμψουν. Η κατανομή της προτεραιότητας των μηνυμάτων εξαρτάται από τον σχεδιαστή του σήματος, αλλά οι βιομηχανικές ομάδες συμφωνούν αμοιβαία σχετικά με την σημασία ορισμένων μηνυμάτων, δηλαδή το πόσο σημαντικό είναι ένα μήνυμα. Για παράδειγμα ένας κατασκευαστής κινητήρων μπορεί να καθορίσει αυτό το μήνυμα 0010 είναι ένα σήμα αναμετάδοσης ρεύματος περιέλιξης από κινητήρα σε δίκτυο CAN ενώ το 0011 είναι το ταχύμετρο. Επειδή το 0010 έχει το χαμηλότερο δυαδικό αναγνωριστικό, μηνύματα όπως αυτό, έχουν πάντα υψηλότερη προτεραιότητα στον δίαυλο από εκείνα που σχετίζονται με τις μετρήσεις του ταχύμετρου (0011).

*Ένα δίκτυο υπολογιστών peer-to-peer (ή P2P, ελληνικά: ομότιμο δίκτυο) είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. [25]

3.1.1.7 ISO 11898

Το ISO 11898 ορίζει κάποιες προδιαγραφές όπως για υψηλές ταχύτητες δίνονται για μέγιστη ταχύτητα σηματοδότησης το 1 Mbps με μήκος διαύλου 40 m και μέγιστο αριθμό κόμβων τους 30. Συνιστάτε επίσης, χωρίς να προσδιορίζεται επακριβώς το μήκος στελέχους στα 0,3 m. Το καλώδιο έχει καθοριστεί να είναι θωρακισμένο ή αθωράκιστο με συνεστραμμένη σύζευξη με χαρακτηριστική αντίσταση (Z_0) τα 120 Ω. Το πρότυπο ISO 11898 ορίζει μια ενιαία γραμμή καλωδίωσης συνεστραμμένου ζεύγους ως τοπολογία δικτύου, όπου φαίνεται και στο παρακάτω σχήμα όπου τερματίζονται τα δυο άκρα σε μια αντίσταση 120 Ω, οι οποίες ταιριάζουν με την χαρακτηριστική σύνθετη αντίσταση της γραμμής για την αποφυγή ανακλάσεων του σήματος. Σύμφωνα με το πρότυπο ISO 11898, πρέπει να αποφευχθεί η τοποθέτηση της RL σε ένα κόμβο διότι οι γραμμές των διαύλων χάνουν το τερματικό τους εάν ο κόμβος αποσυνδεθεί από το δίαυλο. [26]

3.1.1.8 Ο Δίαυλος CAN Bus και οι εφαρμογές του.

Το πρότυπο CAN ορίζει ένα δίκτυο επικοινωνίας που συνδέει όλους τους κόμβους επάνω στο δίαυλο και τους επιτρέπει να μιλάνε μεταξύ τους. Μπορεί να είναι κάποιος κεντρικός κόμβος ελέγχου ή και μη, όπου μπορεί να προστεθεί ανά πάσα στιγμή στο δίαυλο ακόμα και αν το δίκτυο είναι απασχολημένο (hot – plugging). Οι κόμβοι του, θεωρητικά θα μπορούσαν να στείλουν μηνύματα από την τεχνολογία της έξυπνης αποστολής του ελεγκτή του κινητήρα. Μια πραγματική εφαρμογή μπορεί να περιλαμβάνει έναν αισθητήρα θερμοκρασίας που στέλνει μηνύματα ενημέρωσης της θερμοκρασίας έτσι ώστε αυτό να χρησιμοποιηθεί για την ρύθμιση της ταχύτητας του κινητήρα ενός ανεμιστήρα. Εάν ένας κόμβος με αισθητήρα πίεσης θέλει να στείλει ένα μήνυμα ταυτόχρονα, η διαιτησία διασφαλίζει ότι το μήνυμα αποστέλλεται. [27]

Σχετικά με τις εφαρμογές του CAN Bus

Τα συστήματα διαύλου CAN χρησιμοποιούνται επίσης ως συστήματα επικοινωνίας πολλαπλών μικροελεγκτών ως ανοικτά συστήματα επικοινωνιών για ευφυείς συσκευές. Για παράδειγμα, το σειριακό σύστημα διαύλου CAN, που αναπτύχθηκε αρχικά για χρήση σε αυτοκίνητα, χρησιμοποιείται ολοένα και περισσότερο στη βιομηχανία και σε άλλα συστήματα αυτοματισμού. Αυτό οφείλεται στο γεγονός ότι οι απαιτήσεις για τα βιομηχανικά συστήματα είναι παρόμοια με εκείνα για τα δίκτυα επιβατικών αυτοκινήτων, κυρίως όσον αφορά το κόστος εγκατάστασης και συντήρησης, την αξιοπιστία, τη διαθεσιμότητα, την ευρωστία και την ικανότητα να λειτουργούν σε ένα δύσκολο ηλεκτρικό περιβάλλον, υψηλά επίπεδα απόδοσης σε πραγματικό χρόνο και ευκολία χρήσης. Για παράδειγμα, στον τομέα της ιατρικής μηχανικής ορισμένοι χρήστες επέλεξαν το CAN επειδή πρέπει να πληρούν ιδιαίτερα αυστηρές απαιτήσεις ασφαλείας. Παρόμοιος αντιμετωπίζουν προβλήματα κατασκευαστές μηχανημάτων, ρομπότ και συστημάτων μεταφοράς, που πρέπει να πληρούν πολύ υψηλές επιχειρησιακές απαιτήσεις. Με το πέρασμα των χρόνων λοιπόν το CAN έχει γίνει ένα από τα ισχυρότερα πρωτόκολλα στη αυτοκινητοβιομηχανία αν όχι το ισχυρότερο. Έτσι σήμερα έχει αναπτυχθεί αρκετά και περιλαμβάνει πρωτόκολλα υψηλότερου επιπέδου (CAN Open) καθώς επίσης μπορεί να συνδυαστεί με άλλα πρωτόκολλα όπως το LINBus. Το μέλλον λοιπόν του CANBus φαίνεται να είναι λαμπρό καθώς η τεχνολογία αναπτύσσεται συνεχώς με αποτέλεσμα το κόστος να μικραίνει και τα συστήματα αυτά να μπορούν να μπαίνουν ολοένα και σε πιο πολλές εφαρμογές με την αξιοπιστία να φτάνει ολοένα σε μεγαλύτερα επίπεδα. [28]

3.1.2 Ασύρματες συνδέσεις (*Wireless Connections*).

Οι ασύρματες συνδέσεις στα διασυνδεδεμένα αυτοκίνητα παίζουν σημαντικό ρόλο στην επικοινωνία του οχήματος με άλλες συσκευές, υποδομές και υπηρεσίες. Αυτές οι συνδέσεις επιτρέπουν τη μεταφορά δεδομένων, την ανταλλαγή πληροφοριών και τη λειτουργία ποικίλων εξυπηρετήσεων. Οι βασικές ασύρματες συνδέσεις σε διασυνδεδεμένα αυτοκίνητα είναι οι εξής:

3.1.2.1 *Wi-Fi (Wireless Fidelity)*

Τα διασυνδεδεμένα αυτοκίνητα μπορούν να είναι εξοπλισμένα με σύστημα Wi-Fi για ασύρματη σύνδεση στο διαδίκτυο. Αυτό επιτρέπει στους επιβάτες να συνδέονται με το διαδίκτυο για ψυχαγωγία, εργασία, ή άλλες δραστηριότητες. Η τεχνολογία Wi-Fi χρησιμοποιείται εκτενώς στα διασυνδεδεμένα αυτοκίνητα για διάφορους σκοπούς. Ορισμένες από τις κύριες χρήσεις περιλαμβάνουν:

- ✓ **Σύνδεση με το Ίντερνετ:** Τα διασυνδεδεμένα αυτοκίνητα μπορούν να είναι εξοπλισμένα με Wi-Fi για τη σύνδεσή τους σε δίκτυα Wi-Fi στο σπίτι, σε επιχειρήσεις ή σε δημόσια μέρη. Αυτή η σύνδεση επιτρέπει τη λήψη ενημερώσεων λογισμικού, την αναβάθμιση χαρτών και την πρόσβαση σε online υπηρεσίες.
- ✓ **Σύνδεση με άλλες συσκευές:** Το Wi-Fi επιτρέπει τη σύνδεση του αυτοκινήτου με άλλες συσκευές, όπως κινητά τηλέφωνα, tablet, κλπ. Αυτό μπορεί να διευκολύνει τη μεταφορά αρχείων, τη χρήση εφαρμογών και άλλες δραστηριότητες.
- ✓ **Συνδεσιμότητα με εξωτερικά συστήματα:** Το Wi-Fi χρησιμοποιείται για τη σύνδεση με εξωτερικά συστήματα όπως κάμερες, συστήματα ασφαλείας, και άλλα έξυπνα συστήματα που μπορεί να είναι ενσωματωμένα στο αυτοκίνητο.
- ✓ **Ασύρματη σύνδεση με ήχο και εικόνα:** Το Wi-Fi χρησιμοποιείται για τη σύνδεση με συστήματα ψυχαγωγίας στο αυτοκίνητο. Αυτό μπορεί να περιλαμβάνει τη μετάδοση μουσικής, βίντεο ή ακόμα και τη σύνδεση με streaming υπηρεσίες.
- ✓ **Ενημέρωση σε πραγματικό χρόνο:** Η σύνδεση Wi-Fi επιτρέπει τη λήψη ενημερώσεων και πληροφοριών σε πραγματικό χρόνο, όπως κίνηση, καιρό και άλλες πληροφορίες που μπορούν να είναι χρήσιμες για τον οδηγό. [29]

3.1.2.2 *Bluetooth*

Η τεχνολογία Bluetooth χρησιμοποιείται για ασύρματη επικοινωνία μεταξύ του διασυνδεδεμένου αυτοκινήτου και άλλων συσκευών, όπως κινητά τηλέφωνα, ηχοσυστήματα, smartwatches κ.ά. Η σύνδεση Bluetooth επιτρέπει τη μετάδοση αρχείων, τη χρήση χειριστηρίων από άλλες συσκευές, και την παροχή υπηρεσιών όπως το hands-free. Η τεχνολογία Bluetooth είναι ευρέως χρησιμοποιούμενη στα διασυνδεδεμένα αυτοκίνητα για διάφορες λειτουργίες που βελτιώνουν τη συνδεσιμότητα, την ευκολία χρήσης και την ασφάλεια. Ορισμένες κύριες χρήσεις του Bluetooth σε διασυνδεδεμένα αυτοκίνητα περιλαμβάνουν:

- ✓ **Σύνδεση κινητού τηλεφώνου:** Η κύρια χρήση του Bluetooth στα αυτοκίνητα είναι για τη σύνδεση με το κινητό τηλέφωνο. Αυτό επιτρέπει στον οδηγό να απαντά κλήσεις, να καλεί, και να ακούει μουσική χωρίς την ανάγκη χρήσης καλωδίων.

- ✓ **Ασύρματη μετάδοση ήχου:** Το Bluetooth χρησιμοποιείται για την ασύρματη μετάδοση ήχου από το κινητό τηλέφωνο στον ήχο του αυτοκινήτου. Αυτό επιτρέπει στους επιβάτες να απολαμβάνουν τη μουσική τους, να ακούν podcast, κλπ., χωρίς να απαιτείται σύνδεση με καλώδια.
- ✓ **Σύνδεση με άλλες συσκευές:** Το Bluetooth επιτρέπει στο αυτοκίνητο να συνδεθεί με άλλες συσκευές, όπως ασύρματα ακουστικά, έξυπνα ρολόγια, φορητές συσκευές κλπ.
- ✓ **Σύνδεση με συσκευές ενημέρωσης κίνησης:** Σε ορισμένα αυτοκίνητα, το Bluetooth χρησιμοποιείται για τη σύνδεση με συσκευές πλοήγησης και υπηρεσίες ενημέρωσης κίνησης.
- ✓ **Έλεγχος κλιματισμού και άλλων λειτουργιών:** Σε ορισμένα αυτοκίνητα, το Bluetooth μπορεί να χρησιμοποιηθεί για τον ασύρματο έλεγχο του συστήματος κλιματισμού και άλλων λειτουργιών. [30]

3.1.2.3 Cellular Networks (3G, 4G, 5G)

Η σύνδεση με κυψελικά δίκτυα (κινητής τηλεφωνίας) επιτρέπει στα διασυνδεδεμένα αυτοκίνητα να επικοινωνούν με το διαδίκτυο και άλλες υπηρεσίες. Η σύνδεση με κυψελιδικά δίκτυα χρησιμοποιείται για υπηρεσίες όπως η αναβάθμιση λογισμικού, η πλοήγηση σε πραγματικό χρόνο, και άλλες online υπηρεσίες. Οι κυψέλες κινητής τηλεφωνίας (Cellular Networks) όπως τα 3G, 4G και 5G παίζουν σημαντικό ρόλο στην συνδεσιμότητα των διασυνδεδεμένων αυτοκινήτων. Η χρήση των κινητών δικτύων στα διασυνδεδεμένα αυτοκίνητα παρέχει γρήγορη και αξιόπιστη ασύρματη σύνδεση, επιτρέποντας διάφορες λειτουργίες και υπηρεσίες. Ορισμένες κύριες εφαρμογές περιλαμβάνουν:

- ✓ **Συνδεσιμότητα στο διαδίκτυο:** Η τεχνολογία κινητής τηλεφωνίας επιτρέπει στα διασυνδεδεμένα αυτοκίνητα να συνδέονται στο διαδίκτυο μέσω των κινητών δικτύων 3G, 4G ή 5G. Αυτό επιτρέπει τη λήψη ενημερώσεων λογισμικού, την αναβάθμιση χαρτών, και την πρόσβαση σε online υπηρεσίες.
- ✓ **Υπηρεσίες πλοήγησης σε πραγματικό χρόνο:** Η σύνδεση με κινητά δίκτυα επιτρέπει τη λήψη πληροφοριών πορείας και υπηρεσιών πλοήγησης σε πραγματικό χρόνο, χρησιμοποιώντας την τεχνολογία GPS.
- ✓ **Ενημερώσεις κίνησης:** Τα διασυνδεδεμένα αυτοκίνητα μπορούν να λαμβάνουν ενημερώσεις σχετικά με την κίνηση σε πραγματικό χρόνο, προσφέροντας εναλλακτικές διαδρομές για την αποφυγή της κίνησης.
- ✓ **Επικοινωνία με τον κατασκευαστή:** Τα αυτοκίνητα μπορούν να στέλνουν δεδομένα σχετικά με την κατάστασή τους στον κατασκευαστή για παρακολούθηση της απόδοσης και προληπτική συντήρηση.
- ✓ **Κοινοποίηση δεδομένων με άλλα οχήματα (V2V):** Η τεχνολογία Cellular V2V (Vehicle-to-Vehicle) επιτρέπει στα αυτοκίνητα να επικοινωνούν αμοιβαία, ανταλλάσσοντας πληροφορίες σχετικές με την κυκλοφορία και την ασφάλεια.
- ✓ **Αναβάθμιση λογισμικού αυτοκινήτου (OTA Updates):** Η τεχνολογία 4G και 5G επιτρέπει την ασύρματη αναβάθμιση του λογισμικού του αυτοκινήτου μέσω του αέρα (Over-the-Air Updates), εξασφαλίζοντας ότι το αυτοκίνητο είναι πάντα ενημερωμένο με τις τελευταίες εκδόσεις λογισμικού και επιδιορθώσεις ασφαλείας. [31]

3.1.2.4 Near Field Communication (NFC)

Η τεχνολογία NFC επιτρέπει την ασύρματη επικοινωνία σε κοντινές αποστάσεις και χρησιμοποιείται για γρήγορη και ασύρματη σύνδεση με άλλες συσκευές, όπως κινητά τηλέφωνα ή άλλα smart devices. Η τεχνολογία Near Field Communication (NFC) είναι μια μορφή ασύρματης επικοινωνίας που επιτρέπει τη μετάδοση δεδομένων από μικρές αποστάσεις, συνήθως μέχρι και μερικά εκατοστά. Στα έξυπνα αυτοκίνητα, η τεχνολογία NFC χρησιμοποιείται για διάφορες εφαρμογές. Ορισμένες κύριες χρήσεις περιλαμβάνουν:

- ✓ **Ασύρματη κλειδούμενη πρόσβαση (Car Key):** Το NFC χρησιμοποιείται για την ασύρματη κλειδούμενη πρόσβαση στο αυτοκίνητο. Ο οδηγός μπορεί να χρησιμοποιήσει ένα smartphone ή μια κάρτα με NFC για να ξεκλειδώσει και να εκκινήσει το όχημα.
- ✓ **Ενσωματωμένες εφαρμογές οδήγησης:** Το NFC μπορεί να χρησιμοποιηθεί για την ενεργοποίηση ενσωματωμένων εφαρμογών οδήγησης. Για παράδειγμα, ο οδηγός μπορεί να κρατά ένα smartphone με ενσωματωμένο NFC κοντά σε έναν αναγνώστη στο αυτοκίνητο για να ξεκλειδώσει προσαρμοσμένες ρυθμίσεις οδήγησης.
- ✓ **Εύκολη πρόσβαση σε πληροφορίες οχήματος:** Οι κάτοχοι αυτοκινήτων μπορούν να χρησιμοποιούν συσκευές με NFC για να αποκτήσουν γρήγορη πρόσβαση σε πληροφορίες σχετικά με το όχημά τους, όπως τεχνικά χαρακτηριστικά, ιστορικό συντήρησης και άλλα.
- ✓ **Συνδεσιμότητα με άλλες συσκευές:** Το NFC επιτρέπει την εύκολη σύνδεση με άλλες συσκευές, όπως smartphones, χωρίς την ανάγκη για περίπλοκες διαδικασίες σύζευξης.
- ✓ **Ανταλλαγή πληροφοριών με άλλα οχήματα (V2V):** Η τεχνολογία NFC μπορεί να χρησιμοποιηθεί για την ανταλλαγή βασικών πληροφοριών με άλλα οχήματα κατά τη διάρκεια της οδήγησης. [32]

3.1.2.5 Vehicle-to-Everything (V2X) Communication

Η τεχνολογία V2X επιτρέπει στα οχήματα να επικοινωνούν μεταξύ τους (V2V= Vehicle to Vehicle), με την υποδομή οδικής κυκλοφορίας (V2I=Vehicle to Infrastructure), με πεζούς (V2P=Vehicle to Pedestrian) και με το δίκτυο (V2N=Vehicle to Network). Αυτές οι ασύρματες συνδέσεις συνεισφέρουν στη δημιουργία διασυνδεδεμένων αυτοκινήτων με εξελιγμένες λειτουργίες, όπως αυτόνομη οδήγηση, σύνδεση με το διαδίκτυο, και ασύρματη επικοινωνία με άλλες συσκευές. Οι τεχνολογίες V2X επιτρέπουν την ανταλλαγή πληροφοριών μεταξύ των διάφορων στοιχείων στο οδικό περιβάλλον, προσφέροντας πολλαπλά οφέλη όσον αφορά την ασφάλεια, την απόδοση και την άνεση. Ορισμένες χρήσεις της τεχνολογίας V2X στα διασυνδεδεμένα αυτοκίνητα περιλαμβάνουν:

- ✓ **Ασφάλεια οδικής κυκλοφορίας (V2V):** Τα οχήματα μπορούν να επικοινωνούν μεταξύ τους για την ανταλλαγή πληροφοριών σχετικά με την κίνηση, την αποφυγή ατυχημάτων και την βελτίωση της γενικής ασφάλειας.
- ✓ **Βελτίωση ροής κυκλοφορίας (V2I):** Τα οχήματα μπορούν να επικοινωνούν με την υποδομή των οδών, όπως τα φανάρια κυκλοφορίας, για τη βελτίωση της ροής της κυκλοφορίας.

- ✓ **Προειδοποιήσεις πεζών (V2P):** Τα οχήματα μπορούν να ανιχνεύουν πεζούς με τη χρήση τεχνολογίας V2P και να προειδοποιούν τον οδηγό για τον κίνδυνο.
- ✓ **Συνεργασία με κοινόχρηστα οχήματα (V2V):** Κοινόχρηστα οχήματα, όπως αυτόνομα ή ρομποτικά οχήματα, μπορούν να επικοινωνούν με τα υπόλοιπα οχήματα στο οδικό δίκτυο.
- ✓ **Διαχείριση πάρκινγκ (V2I):** Η τεχνολογία V2I μπορεί να χρησιμοποιηθεί για την αποφυγή της κυκλοφορίας στις περιοχές πάρκινγκ, παρέχοντας πληροφορίες σχετικά με τη διαθεσιμότητα χώρων στάθμευσης. [33]

3.1.2.6 GPS (Global Positioning System)

Χρησιμοποιείται για την καθορισμό της θέσης του οχήματος. Το Global Positioning System (GPS) είναι μια τεχνολογία που χρησιμοποιείται ευρέως στα έξυπνα αυτοκίνητα για την καθοδήγηση, την πλοήγηση και άλλες σχετικές λειτουργίες. Το GPS είναι ένα παγκόσμιο σύστημα που αποτελείται από δορυφόρους που παρέχουν πληροφορίες σχετικά με τη θέση και τον χρόνο. Οι κύριες χρήσεις του GPS στα διασυνδεδεμένα αυτοκίνητα περιλαμβάνουν:

- ✓ **Πλοήγηση:** Η πλοήγηση GPS είναι μια κύρια χρήση στα διασυνδεδεμένα αυτοκίνητα. Τα συστήματα GPS παρέχουν ακριβείς πληροφορίες σχετικά με τη θέση του οχήματος και τις οδηγίες για τον προορισμό του. Αυτό βοηθά τους οδηγούς να επιλέγουν την καλύτερη διαδρομή, να αποφεύγουν την κίνηση και να φτάνουν αποτελεσματικά στον προορισμό τους.
- ✓ **Παροχή ενημερώσεων κίνησης:** Τα συστήματα GPS συνήθως ενσωματώνουν πληροφορίες για την κίνηση, επιτρέποντας στους οδηγούς να λαμβάνουν ενημερώσεις για την κατάσταση της κίνησης στη διαδρομή τους.
- ✓ **Αναζήτηση κοντινών σημείων (POI):** Τα GPS επιτρέπουν στους οδηγούς να βρίσκουν κοντινά σημεία ενδιαφέροντος, όπως βενζινάδικα, εστιατόρια, τράπεζες και άλλα.
- ✓ **Ασφάλεια και παρακολούθηση:** Οι συσκευές GPS μπορούν να χρησιμοποιηθούν για την παρακολούθηση της θέσης του οχήματος για λόγους ασφάλειας, όπως σε περιπτώσεις κλοπής.
- ✓ **Ασφαλή οδήγηση:** Ορισμένα συστήματα GPS παρέχουν ειδοποιήσεις για περιοχές όπου ισχύει χαμηλό όριο ταχύτητας ή για περιοχές με υψηλό κίνδυνο.
- ✓ **Παροχή καταγραφής διαδρομών:** Ορισμένα έξυπνα αυτοκίνητα χρησιμοποιούν την τεχνολογία GPS για την καταγραφή και ανάλυση των διαδρομών του οχήματος, προσφέροντας χρήσιμα στοιχεία σχετικά με την οδηγική συμπεριφορά και την κατανάλωση καυσίμου. [34]

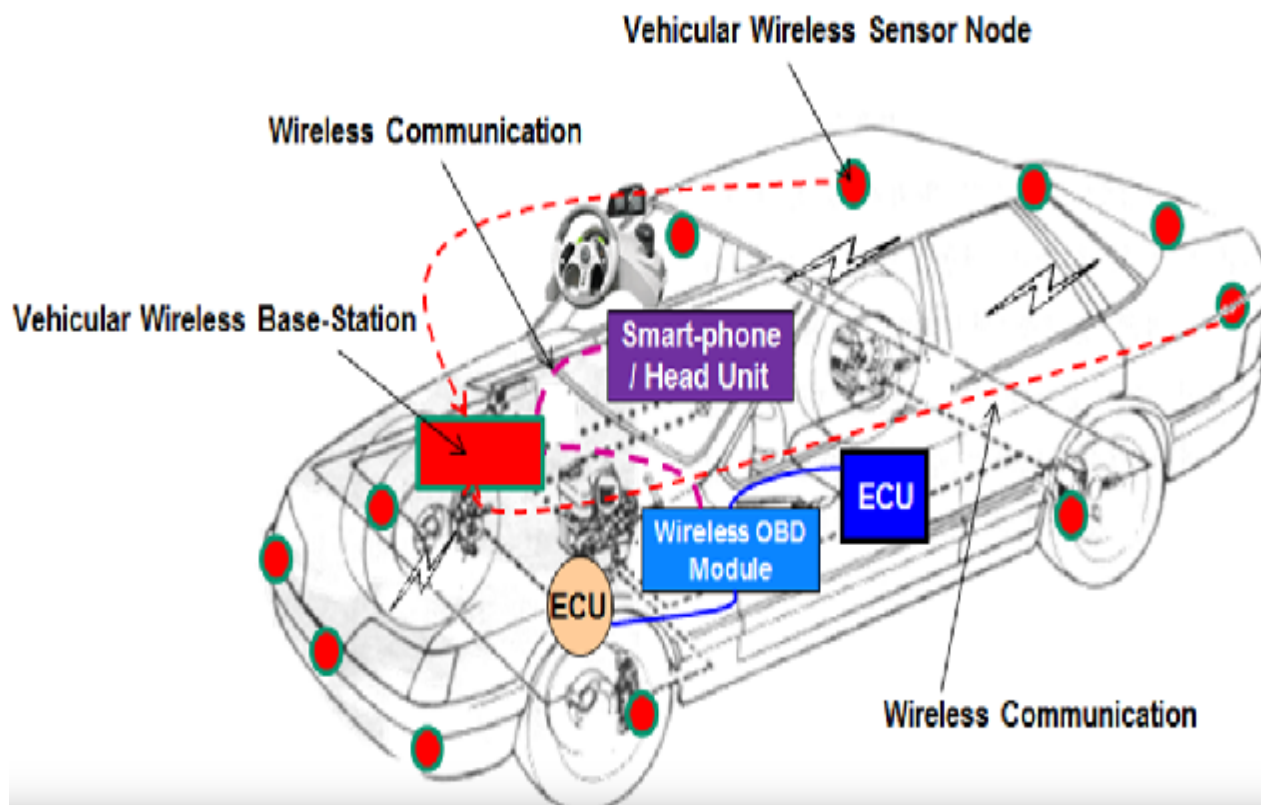
3.1.2.7 Dedicated Short-Range Communications (DSRC). Εξωτερικές διασυνδέσεις ενός διασυνδεδεμένου οχήματος.

Η τεχνολογία Dedicated Short-Range Communications (DSRC) αναφέρεται σε ένα είδος ασύρματης επικοινωνίας με κοντινό εύρος, η οποία έχει σχεδιαστεί ειδικά για εφαρμογές σε οχήματα και υποδομές οδικών. Η χρήση της τεχνολογίας DSRC στα διασυνδεδεμένα αυτοκίνητα παρέχει δυνατότητες επικοινωνίας μεταξύ οχημάτων (V2V) και οχημάτων προς υποδομές (V2I). Ορισμένες εφαρμογές της τεχνολογίας DSRC περιλαμβάνουν:

- ✓ **Ασφάλεια οδικής κυκλοφορίας (V2V):** Η DSRC επιτρέπει στα οχήματα να ανταλλάσσουν πληροφορίες σχετικά με τη θέση, την ταχύτητα και άλλες παραμέτρους, βελτιώνοντας έτσι την ασφάλεια στο οδικό δίκτυο.
- ✓ **Κίνηση μελλοντικών οχημάτων (V2V):** Η επικοινωνία μεταξύ των οχημάτων μπορεί να χρησιμοποιηθεί για τον συντονισμό και τον έλεγχο των κινήσεων, ιδίως σε συνθήκες κυκλοφοριακής συμφόρησης.
- ✓ **Ενημερώσεις για κινδύνους ή ατυχήματα (V2V):** Η DSRC μπορεί να χρησιμοποιηθεί για την ανταλλαγή ενημερώσεων σχετικά με κινδύνους, ατυχήματα ή άλλα σημαντικά γεγονότα στο οδικό δίκτυο.
- ✓ **Σηματοδότης επικοινωνίας (V2I):** Η DSRC επιτρέπει την επικοινωνία με υποδομές οδικών, όπως σήματα κυκλοφορίας και άλλες εγκαταστάσεις, βοηθώντας στην βελτίωση της ροής της κυκλοφορίας.
- ✓ **Προειδοποιήσεις πεζών (V2P):** Η DSRC μπορεί να χρησιμοποιηθεί για την ενημέρωση των οδηγών σχετικά με την παρουσία πεζών σε κοντινή απόσταση.

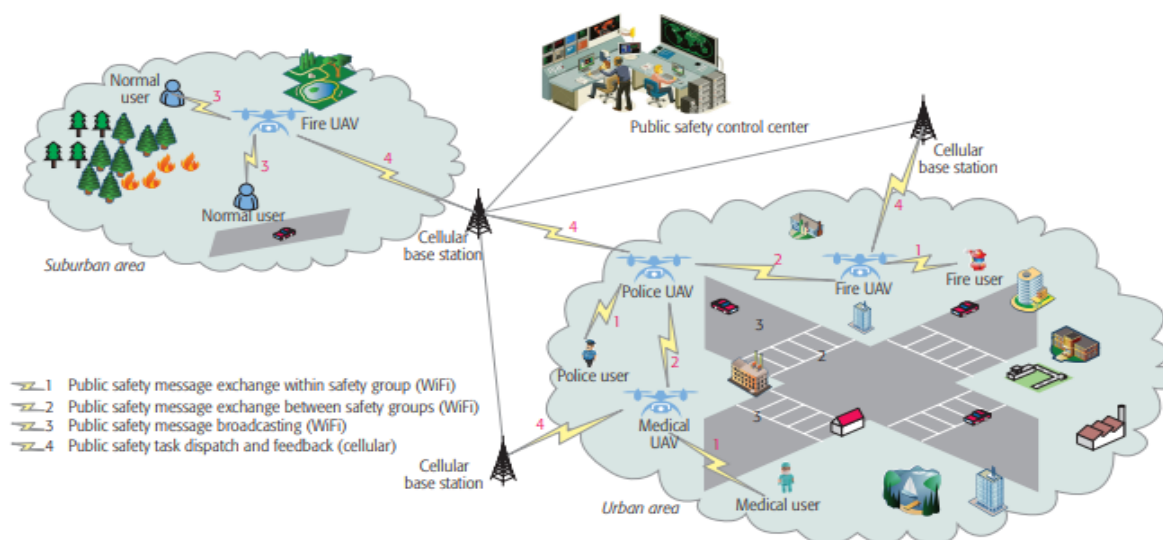
Η τεχνολογία DSRC συμβάλλει στη δημιουργία ενός ευφυούς οδικού δικτύου, όπου τα οχήματα και οι υποδομές μπορούν να επικοινωνούν μεταξύ τους για βελτίωση της ασφάλειας, της ροής της κυκλοφορίας και της επίδοσης του οδικού δικτύου. [35]

Σχήμα 9: Στην παρακάτω εικόνα διακρίνουμε αναλυτικά τις ασύρματες επικοινωνίες ενός διασυνδεδεμένου οχήματος. [36]



3.2 Πληροφορίες συστήματος υπολογιστή για υπηρεσίες συνδεδεμένου αυτοκινήτου

Στο επιστημονικό άρθρο “ComProSe Shaping Future Public Safety Communities with ProSe-Based UAVs” των Zhenhui Yuan, Jie Jin, Jing Chen, Lingling Sun, and Gabriel-Miro Muntean γίνεται αναφορά στο πως επιτυγχάνεται η επικοινωνία των διαφόρων συνδεδεμένων οχημάτων μεταξύ τους (επίγειων και εναέριων), με την βοήθεια διαφόρων κεραιών (Cellular Base stations) για την σωστή πρόληψη αλλά και έγκαιρη αντιμετώπιση διαφόρων κινδύνων. Κατά τον ίδιο ακριβώς θα γίνεται η επικοινωνία των διασυνδεδεμένων οχημάτων σε μια έξυπνη πόλη. Το συνδεδεμένο όχημα, θα λογίζεται πλέον ως η κυρίαρχη μηχανή που αποτελεί κομμάτι μιας έξυπνης πόλης. Αυτό θα γίνεται καθώς τα ιδιωτικά ΙΧ οχήματα αποτελούν το 80% των οχημάτων που κινούνται στους δρόμους της πόλης. Η μεταφορά πληροφοριών που θα συλλέγονται σε ζωντανό χρόνο πχ από το ελικόπτερο της αστυνομίας που θα περιπολεί πάνω από το κέντρο της πόλης, στα οχήματα που κινούνται προς αυτό, για την αποφυγή χρήσης συγκεκριμένων δρόμων (λόγω μιας πιθανής πορείας για παράδειγμα) είναι το απόλυτο ζητούμενο και ο σκοπός της τεχνολογίας αυτής. Οι διάφορες κεραίες που θα εγκατασταθούν σε συγκεκριμένα σημεία των έξυπνων πόλεων, θα έχουν εκτός από τον ρόλο του αναμεταδότη, ρόλο και διαιτητή ώστε να φιλτράρουν την πληθώρα δεδομένων που θα δέχονται και θα μεταδίδουν. Σκοπός και απόλυτη προτεραιότητα αυτής της τεχνολογίας, είναι η μετάδοση των δεδομένων υψηλότερης σημαντικότητας (πχ διακομιδή ασθενών με ασθενοφόρο) για την εύρεση βέλτιστης διαδρομής για αποφυγή κίνησης. [37]



Σχήμα 10: Ανάλυση των επικοινωνιών των διασυνδεδεμένων οχημάτων σε μια έξυπνη πόλη [37]

3.3 Οδική βοήθεια

Τα νέα οχήματα έχουν συγκεκριμένο σύστημα ενημέρωσης των αρμοδίων αρχών σε περίπτωση ατυχήματος στο δρόμο. Η τεχνολογία αυτή αναπτύχθηκε πρώτα στα smart phones. Πλέον σε περίπτωση τροχαίου ατυχήματος, το συνδεδεμένο όχημα που βρίσκεται σε ασύρματη συνδεσιμότητα με το κινητό του οδηγού ειδοποιεί αυτόματα συγκεκριμένους αριθμούς που έχει προσθέσει ο κάθε οδηγός σε περίπτωση ατυχήματος. Θα θεωρηθεί μεγάλη πρόοδος εάν η τεχνολογία αυτή εντοπίζει το στίγμα του αυτοκινήτου που μπορεί να βρίσκεται σε διαφορετική χώρα από την χώρα που έχει αγοραστεί, και να στέλνει στους αντίστοιχους αριθμούς ανάγκης (πχ ΕΛ.ΑΣ , Ε.Κ.Α.Β.) αν αυτό χρειαστεί. Για παράδειγμα, στα κινητά τηλέφωνα που έχουν αγοραστεί από τις ΗΠΑ ο αριθμός έκτακτης ανάγκης είναι καθορισμένος στο 911, όμως σε περίπτωση που ο κάτοχος του κινητού τηλεφώνου βρίσκεται πχ στην Ελλάδα για δουλειά ή διακοπές ο αριθμός αυτός δεν αλλάζει αυτόματα στο 100, που είναι ο αντίστοιχος αριθμός της ΕΛ.ΑΣ. .

3.3.1 Επιπρόσθετη οδική βοήθεια

Σε περίπτωση σημαντικής βλάβης του οχήματος ικανής να το καθλώσει στον δρόμο, υπάρχει στο συνδεδεμένο όχημα επιλογή άμεσης επικοινωνίας με την ασφαλιστική εταιρία, προκειμένου να σταλεί ειδική βοήθεια (γερανός) ώστε το όχημα να μετακινηθεί με ασφάλεια στο κοντινότερο συνεργείο. Αυτό λύνει τα χέρια του οδηγού, ο οποίος δεν θα χάσει χρόνο μέχρι να βρει τα κατάλληλα τηλέφωνα επικοινωνίας.

- Πλησιέστερο πρατήριο καυσίμων: Σε μια έξυπνη πόλη, το διασυνδεδεμένο όχημα θα έχει πρόσβαση σε μια βάση δεδομένων η οποία θα παρέχει πληροφορίες σχετικά με τις απαραίτητες δομές που θα βρίσκονται εγγύτερα του οχήματος. Ένα καλό παράδειγμα είναι τα πρατήρια καυσίμων. Είναι απαραίτητο τα συγκεκριμένα πρατήρια να είναι μέρος αυτής της βάσης, ώστε να ειδοποιείται ο οδηγός του διασυνδεδεμένου αυτοκινήτου σχετικά με την απόσταση του επόμενου πρατηρίου από τη θέση του, καθώς και του ωραρίου που αυτό λειτουργεί, καθώς και των έξτρα παροχών που αυτό διαθέτει (πχ εστιατόριο, πλύσιμο αυτοκινήτου).

4

Πλεονεκτήματα και μειονεκτήματα των διασυνδεδεμένων αυτοκινήτων

4.1 Πλεονεκτήματα

Τα έξυπνα οχήματα, προσφέρουν πολλά πλεονεκτήματα που μπορούν να επηρεάσουν θετικά την κινητικότητα, την ασφάλεια και την ευφυΐα στον τομέα των μεταφορών. Αναλυτικά, ορισμένα από τα πλεονεκτήματα αυτών των οχημάτων περιλαμβάνουν:

- **Την ασφάλεια**: Μειωμένος αριθμός τροχαίων ατυχημάτων λόγω ανθρώπινων λαθών. Υιοθέτηση προηγμένων συστημάτων ασφαλείας, όπως αισθητήρες, κάμερες και ραντάρ, που ελαχιστοποιούν τους κινδύνους συγκρούσεων.
- **Την βελτιωμένη κυκλοφοριακή ροή**: Ενσωμάτωση των πρωτοκόλλων τεχνολογίας επικοινωνίας Vehicle-to-vehicle μεταξύ οχημάτων (V2V) και με το πρωτόκολλο Vehicle-to-infrastructure (V2I), βελτιώνοντας την ροή της κυκλοφορίας και μειώνοντας τη συμφόρηση.
- **Την ενίσχυση της ενεργειακής απόδοσης**: Βελτιστοποίηση της οδήγησης για βέλτιστη κατανάλωση καυσίμου και μείωση της ρύπανσης.
- **Την εξοικονόμηση χρόνου**: Η δυνατότητα για τους επιβάτες να αφήσουν προσωρινά τον έλεγχο του οχήματος, επιτρέποντας τους να ασχοληθούν με άλλες δραστηριότητες κατά τη διάρκεια του ταξιδιού.
- **Την πρόσβαση για ευπαθείς ομάδες**: Προσφέρουν τη δυνατότητα στα άτομα με περιορισμένη κινητικότητα ή άλλες αναπηρίες να έχουν πρόσβαση σε αυτοκίνητα, ανεξαρτήτως ικανοτήτων οδήγησης.

- **Συμμόρφωση στα περιβαλλοντικά πρότυπα:** Μείωση της κυκλοφοριακής συμφόρησης και βελτιωμένη οδήγηση συνεισφέρουν στη μείωση των εκπομπών και στη συμμόρφωση προς περιβαλλοντικά πρότυπα.
- **Εξέλιξη της υποδομής:** Απαιτείται εξέλιξη της υποδομής (οδική, επικοινωνιακή) για να υποστηρίξει την ασφαλή λειτουργία των έξυπνων οχημάτων. Η βελτιστοποίηση των δρόμων, των οδικών σημάτων και άλλων σχετικών υποδομών, κρίνεται αναγκαία προκειμένου να εισαχθούν τα smart cars στην κυκλοφορία.

Εύκολα μπορεί να αντιληφθεί κάποιος ότι η οδήγηση τα αμέσως επόμενα χρόνια θα γίνει πιο εύκολη, πιο προσιτή, αλλά και αρκετά πιο οικολογική. Η πληθώρα πλεονεκτημάτων έχει καταστήσει τα smart cars ως ίσως την πιο υποσχόμενη τεχνολογική ανάπτυξη. Υπάρχουν όμως και μειονεκτήματα τα οποία χρίζουν προσοχής.

4.2 Μειονεκτήματα

Παρά τα πολλά πλεονεκτήματα, τα έξυπνα οχήματα επίσης αντιμετωπίζουν ορισμένα και σημαντικά μειονεκτήματα και προκλήσεις. Αναλυτικά, ορισμένα από τα μειονεκτήματα αυτών των οχημάτων περιλαμβάνουν:

- **Το κόστος υλοποίησης:** Η ενσωμάτωση προηγμένων τεχνολογιών, όπως οι αισθητήρες, το λογισμικό και η υποδομή της επικοινωνίας, απαιτούν υψηλό κόστος προσαρμογής και αναβάθμισης. Αυτό αντικατοπτρίζεται στην τιμή ενός smart car, η οποία προς το παρόν κρίνεται απαγορευτική για ένα νοικοκυριό. Επιπλέον κρίνεται αναγκαίο να υπάρξει αναβάθμιση των μαθημάτων οδήγησης καθώς οι οδηγοί αναμένεται να αντιμετωπίσουν μια αρκετά διαφορετική εμπειρία οδήγησης.
- **Την ύπαρξη φόβου για τυχών ανακρίβεια της τεχνολογίας:** Οι αισθητήρες και οι τεχνολογίες αναγνώρισης είναι ακόμα υπό ανάπτυξη και μπορεί να υπάρξουν καταστάσεις όπου η τεχνολογία δεν λειτουργεί απολύτως σωστά.
- **Την ανθρώπινη δυσπιστία:** Ορισμένοι οδηγοί μπορεί να προτιμούν τον έλεγχο του οχήματος και να αντιμετωπίζουν ανησυχίες όσον αφορά την ασφάλεια και τον έλεγχο της κίνησης του αυτοκινήτου τους, εάν οι ίδιοι δεν έχουν τον απόλυτο έλεγχο.
- **Τον φόβο της κυβερνοασφάλειας:** Η σύνδεση των οχημάτων στο διαδίκτυο και η χρήση λογισμικού καθιστούν τα έξυπνα οχήματα ευαίσθητα στην κυβερνοασφάλεια, με δυνητικούς κινδύνους για κακόβουλες επιθέσεις τρίτων χρηστών.
- **Την υποδομή και την συμβατότητα:** Η αποτελεσματική λειτουργία των έξυπνων οχημάτων απαιτεί την ανάπτυξη συμβατών υποδομών, όπως επικοινωνιακά δίκτυα και υποστηρικτική υποδομή στους δρόμους. Γίνεται κατανοητό ότι κράτη με δυσχερή οικονομική θέση θα αργήσουν πολύ να συμμορφωθούν στις απαραίτητες για τα smart cars υποδομές.
- **Την ανεπάρκεια κανονιστικού πλαισίου:** Η έλλειψη ομοιογενούς νομοθετικού πλαισίου για την λειτουργία αυτοκινήτων χωρίς οδηγό μπορεί να προκαλέσει νομικές ανασφάλειες.
- **Τις κοινωνικές και τις ηθικές προκλήσεις:** Αντιμετώπιση ηθικών διλημμάτων, όπως η απόφαση του οχήματος σε περίπτωση αναπόφευκτης σύγκρουσης. (Θα αναλυθεί εκτενέστερα σε επόμενο κεφάλαιο.)

- **Την δυσκολία συντήρησης:** Η συντήρηση και επισκευή προηγμένων τεχνολογιών μπορεί να απαιτεί εξειδικευμένες γνώσεις και εξοπλισμό. Αυτό απαιτεί την επανεκπαίδευση όλων σχεδόν των μηχανικών αυτοκινήτων, και την εκτόξευση του κόστους συντήρησης των αυτοκινήτων.

Είναι σημαντικό να σημειωθεί ότι πολλά από αυτά τα μειονεκτήματα είναι πιθανόν να ξεπεραστούν σχετικά γρήγορα καθώς η τεχνολογία εξελίσσεται. Υπάρχουν όμως και αρκετά, τα οποία θα χρειαστεί αρκετό χρονικό διάστημα για να μελετηθούν καλύτερα. Επιπροσθέτως θα πρέπει η νομοθεσία του κάθε κράτους, να διευκολύνει την υιοθέτηση των έξυπνων οχημάτων, πράγμα το οποίο είναι αρκετά σύνθετο και αμφίβολο ότι θα πραγματοποιηθεί. [38] [39]

4.3 Μεταβατικό στάδιο

Όπως αναλύθηκε εκτενώς στα προηγούμενα κεφάλαια, η προμήθεια νέων έξυπνων οχημάτων θα βοηθήσει πολύ στο σύνολο της οδικής συμπεριφοράς. Αναλύθηκαν τα πλεονεκτήματα και τα μειονεκτήματα αυτών, καθώς και τα προβλήματα και οι δυσκολίες ενσωμάτωσης τους στους δρόμους της Ελλάδας. Οι απεριόριστες νέες δυνατότητες που δίνονται στον οδηγό, θα τον βοηθήσουν στο να απολαύσει μια νέα εμπειρία οδήγησης. Η αυξανόμενη «ψηφιοποίηση» της οδήγησης περνά σε άλλο τεχνολογικό επίπεδο, και οι οδηγοί θα πρέπει να αποδεχτούν ότι πλέον θα πρέπει να «παραχωρήσουν» αρκετές λειτουργίες αυτής, σε διάφορους αλγορίθμους οι οποίοι πλέον σταδιακά, θα εισάγουν τον «αυτόματο πιλότο» στην οδήγηση. Η ιδιωτικότητα ωστόσο δύναται να δοκιμαστεί. Στα αμέσως επόμενα κεφάλαια, θα γίνει εις βάθος ανάλυση σχετικά με την ασφάλεια και την ιδιωτικότητα σχετικά με τις νέες τεχνολογίες των έξυπνων οχημάτων.

5

Ιδιωτικότητα και προσωπικά δεδομένα

5.1 Εισαγωγή

Όπως προαναφέρεται στα προηγούμενα κεφάλαια το IoT μετέτρεψε τα αυτοκίνητα σε τροχοφόρους υπολογιστές. Σαν υπολογιστές, επεξεργάζονται ένα μεγάλο πλήθος δεδομένων . Μέρος των δεδομένων που επεξεργάζονται τα διασυνδεδεμένα αυτοκίνητα αφορούν τα προσωπικά δεδομένα του οδηγού, με αποτέλεσμα να υπάρχει κίνδυνος για την προστασία των προσωπικών δεδομένων των οδηγών-χρηστών που εμπλέκονται σε ένα VANET .

Αυτό γεννά ερωτηματικά όπως

- α) Τι είδους προσωπικά δεδομένα διαχειρίζονται τα έξυπνα αυτοκίνητα και γιατί;
- β) Απειλείται η ιδιωτικότητα του χρήστη στο δίκτυο των έξυπνων αυτοκινήτων;
- γ) Πόσο καλά προστατευμένη είναι η ιδιωτικότητα του χρήστη;

Στο κεφάλαιο αυτό θα εξεταστούν ένα προς ένα τα παραπάνω ερωτήματα, και θα αναλυθούν κάποιες έννοιες ώστε να μπορεί να γίνει κατανοητή η σημαντικότητα της προστασίας της ιδιωτικότητας στον κόσμο των διασυνδεδεμένων αυτοκινήτων.

5.2 Προσωπικά δεδομένα και Ιδιωτικότητα

Προσωπικά Δεδομένα: Τα προσωπικά δεδομένα αποτελούν πληροφορίες που αναφέρονται σε άτομο που βρίσκεται εν ζωή και του προσδίδουν μια ταυτότητα . Τέτοια δεδομένα είναι

1. Το όνομα και το επώνυμο
2. Το φύλο
3. Η ηλικία και η ημερομηνία γέννησης
4. Η διεύθυνση κατοικίας
5. Η ηλεκτρονική του διεύθυνση (email)
6. Ο αναγνωριστικός αριθμός ταυτότητας (ΑΔΤ)
7. Τα δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
8. Ο τηλεφωνικός του αριθμός [47]

Ιδιωτικότητα: Η ιδιωτικότητα είναι το δικαίωμα ενός ατόμου ή μιας ομάδας να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς θα διαβιβάζονται σε άλλους. Είναι το δικαίωμα της προστασίας της προσωπικότητας και του ιδιωτικού βίου, που ορίζεται ως το δικαίωμα του ατόμου «να μην ενοχλείται από άλλους και να αφήνεται μόνο στην ηρεμία του». [40][47]

Ιδιωτικότητα στο διαδίκτυο: Η ανησυχία για την προστασία του ιδιωτικού απορρήτου έχει διατυπωθεί από την απαρχή της κοινής χρήσης ηλεκτρονικών υπολογιστών Η ιδιωτικότητα στο διαδίκτυο περιλαμβάνει το δικαίωμα ή την εντολή προστασίας προσωπικών δεδομένων όσον αφορά την αποθήκευση, την επεξεργασία, την παροχή και την προβολή πληροφοριών σε τρίτους. [41][47]

Προστασία της ιδιωτικότητας: Η προστασία της ιδιωτικότητας σχετίζεται με την προστασία ενός ιδιώτη από τις αδικαιολόγητες παρεμβάσεις των προσωπικών δεδομένων και την παροχή πληροφοριών που παραβιάζουν την σωματική, την ηθική και την νομική ελευθερία του. Δηλαδή τα προσωπικά στοιχεία ενός προσώπου ή ομάδας ατόμων, που μπορούν να συγκεντρωθούν, να αποθηκευτούν, να υποστούν επεξεργασία ή να διαδοθούν επιλεκτικά, πρέπει να προστατεύονται από μη εξουσιοδοτημένη προσπέλαση, υποκλοπή ή παραποίηση. [42][47]

5.3 *Ιδιωτικότητα στα Vehicular Ad Hoc Network (VANET)*

Η εποχή που το αυτοκίνητο απλά μετέφερε κάποιον στον επιθυμητό προορισμό έχει περάσει προ πολλού. Η πρόοδος της τεχνολογίας συνδυάζοντας το αυτοκίνητο και τον ηλεκτρονικό υπολογιστή, δημιούργησε το έξυπνο αυτοκίνητο. Πλέον πρόκειται για ένα αυτοκίνητο - υπολογιστή, το οποίο συλλέγει και κοινοποιεί συνεχώς δεδομένα χάρη στους αισθητήρες του και τα συστήματα πλοήγησης που διαθέτει, ανεξάρτητα εάν βρίσκεται σε κίνηση ή όχι.

5.3.1 *Τι δεδομένα συλλέγονται από τα διασυνδεδεμένα αυτοκίνητα*

Τα διασυνδεδεμένα αυτοκίνητα διαχειρίζονται πληθώρα δεδομένων διαμέσου του VANET όπως προαναφέρθηκε με σκοπό την καλύτερη οδηγική εμπειρία του οδηγού και την ασφάλεια του στην ασφάλτο. Κάποια από αυτά όμως είναι προσωπικά δεδομένα του οδηγού.

Πιο αναλυτικά:

1. Μέσω πλατφορμών για διασυνδεδεμένα οχήματα που απαιτεί εγγραφή χρήστη, ο οδηγός καταχωρεί στοιχεία όπως τηλέφωνο επικοινωνίας, ηλεκτρονική διεύθυνση, διεύθυνση κατοικίας, φορολογικά στοιχεία και στοιχεία κάρτας. Ακόμα καταχωρούνται τα στοιχεία του ίδιου του αυτοκινήτου.
2. Επίσης μέσω GPS εφαρμογών καταχωρείται η τοποθεσία του αυτοκινήτου ανά πασα στιγμή και αυτό με σκοπό είτε να εντοπίσει το πλησιέστερο παρκινγκ σε σχέση με τη θέση του, είτε να βρει τη συντομότερη διαδρομή. Γνωστοποιείται δηλαδή η θέση ενός συνδεδεμένου οχήματος ανά πάσα στιγμή στον αντίστοιχο διαχειριστή του συστήματος γεωεντοπισμού του οχήματος.
3. Κάμερες καταγράφουν το εσωτερικό του αυτοκινήτου αλλά και έξω από αυτό.
4. Μικρόφωνα βοηθούν επίσης στην ενδοεπικοινωνία των οδηγών, όπως για παράδειγμα η αποθήκευση φωνής για την ταυτοποίηση του εκάστοτε οδηγού. Ο σκοπός είναι να υπάρχει η δυνατότητα να μπορούν να δοθούν ορισμένες εντολές στο όχημα χωρίς ο οδηγός να πρέπει να χρησιμοποιήσει τα χέρια του εφόσον οδηγεί. Αυτές οι εντολές, είναι γενικά ακουστικές εντολές του οδηγού προς το όχημα, οι οποίες γίνονται δια της ομιλίας προκειμένου να μην διαταραχτεί η οδηγική συμπεριφορά.
5. Επιπροσθέτως, υπάρχουν συστήματα καταγραφής της δραστηριότητας του οδηγού, δηλαδή για παράδειγμα με τι ταχύτητα οδηγεί το όχημα του, ή πόσο συχνά ανανεώνει τα καύσιμα του οχήματος. Γενικότερα ο σκοπός είναι να παρατηρηθεί πόσο ακολουθείται ο κώδικας καλής οδικής συμπεριφοράς. Κατά αυτό τον τρόπο, δημιουργείται το προφίλ του οδηγού, και γίνεται κατανοητό, εάν ο οδηγός διαθέτει την απαραίτητη επάρκεια ώστε να κριθεί ικανός για οδήγηση ή μη.
6. Ακόμα κάποιες εφαρμογές διασυνδεδεμένων αυτοκινήτων ζητούν το ιατρικό προφίλ του οδηγού. Για παράδειγμα μέσω της αντίστοιχης εφαρμογής, εάν έχει γίνει γνωστοποίηση σε αυτή ότι ο οδηγός έχει προβλήματα υγείας και πρέπει να λάβει την απαραίτητη ιατρική

αγωγή (φάρμακο) εν ώρα οδήγησης, το όχημα θα μπορεί να ειδοποιήσει τον οδηγό για να σταματήσει.

7. Τέλος το νομικό προφίλ του οδηγού αποτελεί επίσης σημαντική πληροφορία για μερικές αυτοκινητοβιομηχανίες που παράγουν διασυνδεδεμένα οχήματα.

Όπως γίνεται αντιληπτό ένας οδηγός ενός διασυνδεδεμένου αυτοκινήτου, βρίσκεται διαρκώς υπό “παρακολούθηση” από αυτό. Μπορούμε να ισχυριστούμε ότι σταδιακά ο απώτερος σκοπός είναι ο οδηγός να “απομακρύνεται” από το τιμόνι. Επιπλέον ξεκινά να χάνεται η ανεξαρτησία του μέσα στο όχημα όπως γίνεται μέχρι στιγμής με τα συμβατικά οχήματα. Καταλήγουμε στο γεγονός, ότι οι αυτοκινητοβιομηχανίες γίνονται ένας μεγάλος αποδέκτης και διαχειριστής πληθώρας ευαίσθητων προσωπικών δεδομένων. [43][45][46][51][34]

5.3.2 Τα προσωπικά δεδομένα είναι αφημένα στο έλεος των αυτοκινητοβιομηχανιών

Προκειμένου, να λειτουργήσει η εν λόγω τεχνολογία των διασυνδεδεμένων αυτοκινήτων, θα πρέπει να συγκεντρώνει πλήθος δεδομένων, όπως η ακριβής τοποθεσία του οχήματος, ο χρόνος του πιθανού ατυχήματος, ο αριθμός των επιβατών του οχήματος, ο τύπος του οχήματος, και τέλος ο τύπος του καυσίμου που το όχημα χρησιμοποιεί για να κινείται. Όλα τα παραπάνω είναι αναμενόμενο να προσελκύσουν το ενδιαφέρον πολλών επιχειρήσεων με αποτέλεσμα να ανοίγει ο «ασκός του Αιόλου» για το που αρχίζει και που τελειώνει η προστασία της ιδιωτικής ζωής ενός ατόμου. Είναι εμφανές πλέον πως τα σύγχρονα αυτοκίνητα βαθμολογούνται κάτω από τη βάση στην προστασία της ιδιωτικότητας. Οι περισσότερες αυτοκινητοβιομηχανίες παραδέχονται ότι μπορεί να πωλούν τα προσωπικά δεδομένα των οδηγών σε τρίτους, αποκαλύπτει νέα έρευνα. Τα αυτοκίνητα είχαν τη χαμηλότερη βαθμολογία για θέματα ιδιωτικότητας μεταξύ 12 προϊόντων που έχει εξετάσει το ίδρυμα Mozilla από το 2017, όπως ρολόγια παρακολούθησης αθλητικών επιδόσεων, έξυπνα ηχεία και άλλες συνδεδεμένες συσκευές. Από τις 25 μάρκες αυτοκινήτων που εξετάστηκαν, οι οποίες επιλέχθηκαν με βάση τη δημοτικότητά τους στην Ευρώπη και τη Βόρεια Αμερική, καμία δεν βρέθηκε να πληροί τις προδιαγραφές του ιδρύματος. Συγκριτικά, το αντίστοιχο ποσοστό για τις εφαρμογές ψυχικής υγείας είναι 37%. Οι 19 από τις 25 αυτοκινητοβιομηχανίες δηλώνουν στην πολιτική ιδιωτικότητας ότι τα δεδομένα μπορεί να πωληθούν σε άλλες εταιρείες. Οι μισές δηλώνουν ότι θα παρέδιδαν τις πληροφορίες στην κυβέρνηση ή την αστυνομία με ένα απλό αίτημα, αντί με δικαστική εντολή. Αξιοσημείωτο επίσης να αναφερθεί είναι το γεγονός ότι μόνο δύο εταιρείες, η Renault και η Dacia, δίνουν στους οδηγούς τη δυνατότητα να ζητούν τη διαγραφή των δεδομένων τους. Παρόλο που οι κατασκευαστές μπορεί να πωλούν τα δεδομένα σε τρίτους, συχνά αρνούνται να τα διαβιβάσουν σε ανεξάρτητα συνεργεία για την επισκευή των οχημάτων. Το 2020, το 52% των Αμερικανών που συμμετείχαν σε δημοσκόπηση της Pew Research δήλωσε ότι επέλεξε να μην αγοράσει κάποιο προϊόν ή υπηρεσία λόγω ανησυχίας για τη συλλογή προσωπικών δεδομένων. Η ιαπωνική Nissan παραδέχτηκε ότι συλλέγει «ευαίσθητες προσωπικές πληροφορίες», όπως ο αριθμός πινακίδας, η φυλή, ο σεξουαλικός προσανατολισμός και δείκτες υγείας. Επιπλέον, η εταιρεία παραδέχεται ότι

μπορεί να πουλά «προφίλ» των οδηγών που «αντανακλούν τις προτιμήσεις του καταναλωτή, τα χαρακτηριστικά του, τις ψυχολογικές τάσεις, τις προδιαθέσεις, τη συμπεριφορά, τις απόψεις, τη νοημοσύνη, τις ικανότητες και τις δεξιότητές τους». Ήταν μία από τις έξι εταιρείες που παραδέχονται ότι συλλέγουν «γενετικές πληροφορίες» ή «γενετικά χαρακτηριστικά». Η Nissan ανέφερε ακόμα ότι συλλέγει δεδομένα «σεξουαλικής συμπεριφοράς», χωρίς να εξηγήσει το πώς. Ιδιαίτερα χαμηλή ήταν η βαθμολογία της Tesla. Αν ο οδηγός ζητήσει την εξαίρεσή του από τη συλλογή δεδομένων, η εταιρεία λέει πως ενδέχεται να μην μπορεί να τον ενημερώσει άμεσα για προβλήματα που θα μπορούσαν να οδηγήσουν σε «μειωμένη λειτουργικότητα, σοβαρή ζημιά ή αδυναμία λειτουργίας». Μια έκθεση του Ιδρύματος Mozilla, ενός μη κερδοσκοπικού οργανισμού τεχνολογικής έρευνας και υπεράσπισης, διαπίστωσε ότι οι πολιτικές απορρήτου των αυτοκινητοβιομηχανιών είναι εξαιρετικά χαλαρές. Η μελέτη προσδιόρισε τα αυτοκίνητα ως τη «χειρότερη κατηγορία προϊόντων για την προστασία της ιδιωτικής ζωής που έχουμε εξετάσει ποτέ». Ο αμερικανός γερουσιαστής ΕντΜάρκι έγραψε μια επιστολή στις αυτοκινητοβιομηχανίες των ΗΠΑ στις 30 Νοεμβρίου 2023, θέτοντας μια μεγάλη σειρά ερωτήσεων σχετικά με τις πρακτικές δεδομένων τους. Τα σημερινά έξυπνα αυτοκίνητα παρουσιάζουν στους οδηγούς μια αντιστάθμιση μεταξύ άνεσης και ιδιωτικότητας, υποθέτοντας ότι οι οδηγοί έχουν τη δυνατότητα να βελτιώσουν το απόρρητο των δεδομένων των αυτοκινήτων τους. Οι ιδιοκτήτες συχνά δεν έχουν λόγο στο πώς μπορεί να χρησιμοποιηθούν τα δεδομένα τους, διαπιστώνει η έκθεση του ιδρύματος, το οποίο προωθεί τεχνολογίες ανοιχτού κώδικα και αναπτύσσει το browserFirefox. Οι αγοραστές «δεν έχουν και πολλές επιλογές», εκτός αν αγοράσουν κάποιο μεταχειρισμένο παλιό μοντέλο. [44][45]

5.4 Προστασία της ιδιωτικότητας στα διασυνδεδεμένα αυτοκίνητα

Τα διασυνδεδεμένα αυτοκίνητα λόγω του όγκου δεδομένων που πρέπει να συλλέγουν δεν προωθούν ως πρώτη προτεραιότητα την προστασία της ιδιωτικότητας του οδηγού-χρήστη, οι κατασκευάστριες όμως εταιρείες είναι υποχρεωμένες για τον παραπάνω λόγο ,το ότι δηλαδή περνούν από τα «χεριά τους» ή μάλλον από τα οχήματα τους προσωπικά δεδομένα χρηστών, να τηρούν κάποια μετρά προστασίας της ιδιωτικότητας τους οδηγού χρήστη . Τέτοια μετρά μπορεί να είναι η χρήση ισχυρών μηχανισμών αυθεντικοποίησης (ψευδώνυμο), η κρυπτογράφηση των δεδομένων (VPNσύνδεση), η προστασία από επιθέσεις παρακολούθηση των κόμβων. Στις παρακάτω παραγράφους θα αναλυθούν μηχανισμοί και μέθοδοι προστασίας της ιδιωτικότητας του οδηγού-χρήστη .[52]

5.4.1 Πρότυπο IEEE 1609.2

Το πρότυπο IEEE 1609.2 αφορά την ασφάλεια και την προστασία της ιδιωτικότητας στις επικοινωνίες των ασύρματων δικτύων αυτοκινήτων, συμπεριλαμβανομένων των Vehicular Ad-Hoc Networks (VANETs). Το πρότυπο αυτό προσδιορίζει τα προφίλ ασφαλείας και απορρήτου που πρέπει να χρησιμοποιούν οι εφαρμογές επικοινωνίας μεταξύ οχημάτων (V2V), καθώς και μεταξύ οχημάτων και υποδομής (V2I). Το πρότυπο 1609.2 είναι αυτό που εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων. Με τη βοήθεια του προτύπου αυτού, ο οδηγός ορίζει ασφαλείς μορφές μηνυμάτων διαχείρισης και εφαρμογών και την επεξεργασία αυτών με σκοπό την προστασία των δεδομένων από υποκλοπές, πλαστογράφηση ή άλλους τύπους παραποίησης της πληροφορίας. [64]

5.4.2 Μηχανισμοί ενδυνάμωσης ασφαλείας VANET δικτύου

Στο υποκεφάλαιο αυτό θα αναλυθούν ορισμένες τεχνικές που χρησιμοποιούνται σε δίκτυα για διασυνδεδεμένα αυτοκίνητα και διασφαλίζουν την ιδιωτικότητα του οδηγού- χρήστη.

5.4.2.1 Authenticated Routing for Ad Hoc Networks Protocol (ARAN)

Το πρωτόκολλο δρομολόγησης ARAN βασίζεται στο AODV. Στο ARAN, υπάρχει μια αρχή που ονομάζεται αρχή πιστοποιητικών (CA) και είναι υπεύθυνη για την αποστολή ενός υπογεγραμμένου πιστοποιητικού στους κόμβους, μόλις λάβει ένα αίτημα πιστοποίησης. Οι τεχνικές ασύμμετρης κρυπτογράφησης χρησιμοποιούνται για την επαλήθευση της αυθεντικότητας της ανίχνευσης ασφαλούς διαδρομής και οι χρονικές ετικέτες χρησιμοποιούνται για την εκκαθάριση της διαδρομής .

Το ARAN έχει ουσιαστικά πέντε βήματα:

1. Πιστοποίηση
2. Αυθεντική εύρεση διαδρομής
3. Ρύθμιση αυθεντικής διαδρομής
4. Συντήρηση διαδρομής
5. Ανάκληση κλειδιού

Στη διαδρομή ARAN, η διαδικασία ελέγχου ταυτότητας πραγματοποιείται σε κάθε βήμα προσθέτοντας το σύμβολο και το πιστοποιητικό κάθε μεσαίου κόμβου, έτσι αυτό το πρωτόκολλο λύνει το πρόβλημα πλαστοπροσωπίας.[65][58]

5.4.2.2 *Secure and Efficient Ad Hoc Distance Vector Protocol (Sead)*

Το πρωτόκολλο SEAD (Source Location Privacy-Aware Energy-Efficient Adaptive Clustering Protocol) είναι ένα πρωτόκολλο που αναπτύχθηκε για ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks - WSNs). Το SEAD σχεδιάστηκε για να διαχειρίζεται την ενέργεια και να προστατεύει το απόρρητο της τοποθεσίας του πηγαίου κόμβου.

Ορισμένα από τα βασικά χαρακτηριστικά του SEAD είναι :

- **Να μπορεί να χρησιμοποιεί συγκεντρωτική δομή:** όπου οι αισθητήρες ομαδοποιούνται σε clusters και επιλέγεται ένας clusterhead για την επικοινωνία με τον sink (τον συγκεντρωτικό κόμβο).
- **Να μπορεί να προστατεύει το απόρρητο της τοποθεσίας του πηγαίου κόμβου:** Οι επικεφαλές κάθε cluster δρουν ως οι ενδιάμεσοι κόμβοι για τη μεταφορά των δεδομένων, προστατεύοντας έτσι την τοποθεσία του πηγαίου κόμβου.
- **Να μπορεί να σχεδιάζει μια προσαρμοστική επιλογή του επικεφαλές κόμβου σε κάθε γύρο επικοινωνίας:** με σκοπό την ισορροπία του φόρτου εργασίας και την εξοικονόμηση ενέργειας.
- **Οι ενδιάμεσοι κόμβοι σε κάθε cluster είναι υπεύθυνοι για την επεξεργασία και την προώθηση των δεδομένων:** με σκοπό τη μείωση της κατανάλωσης ενέργειας των αισθητήρων.

Το SEAD ανήκει στην κατηγορία των πρωτοκόλλων που εστιάζουν στην εξοικονόμηση ενέργειας και την επιλογή επικεφαλές κόμβων με γνώμονα την προστασία της απόρρητης τοποθεσίας σε ασύρματα δίκτυα αισθητήρων.[58][76]

5.4.2.3 *SAODV protocol*

Το SAODV (Secure Ad-Hoc On-Demand Distance Vector) είναι μια εξέλιξη του AODV (Ad-Hoc On-Demand Distance Vector) πρωτοκόλλου δρομολόγησης για ασύρματα ανοικτά δίκτυα (Ad-Hoc Networks) που έχει σχεδιαστεί για να παρέχει πρόσθετα επίπεδα ασφάλειας.

Οι βασικές αρχές του SAODV παραμένουν παρόμοιες με αυτές του AODV, αλλά περιλαμβάνει μέτρα ασφαλείας για την προστασία του δικτύου από διάφορες απειλές και επιθέσεις. Αυτά τα μέτρα περιλαμβάνουν κυρίως τη χρήση κρυπτογραφίας, πιστοποίησης, και μέτρων αντιμετώπισης επιθέσεων.

Κάποια χαρακτηριστικά του SAODV είναι:

- Το SAODV χρησιμοποιεί μηχανισμούς αυθεντικοποίησης για να επιβεβαιώσει την ταυτότητα των συμμετεχόντων στο δίκτυο.
- Το SAODV χρησιμοποιεί πρωτόκολλα κρυπτογράφησης για την προστασία των επικοινωνιών.
- Το SAODV περιλαμβάνει μέτρα αντιμετώπισης επιθέσεων, όπως ανίχνευση και αντιμετώπιση κακόβουλων ενεργειών.
- Η διαδρομή προς έναν προορισμό διακυβεύεται μόνο όταν υπάρχει ανάγκη για αυτήν, μειώνοντας τον υπολογιστικό φόρτο και το εύρος ζώνης.

Το SAODV συνήθως χρησιμοποιείται σε περιβάλλοντα όπου η ασφάλεια των επικοινωνιών είναι κρίσιμη, όπως σε στρατιωτικές εφαρμογές, αισθητήρια δίκτυα (VANET) και άλλα ευαίσθητα περιβάλλοντα. [67]

5.4.2.4 A-SAODV protocol

Το A-SAODV (Authentication-based Secure Ad Hoc On-Demand Distance Vector) είναι ένα επιπρόσθετο πρωτόκολλο ασφαλείας που βασίζεται στο AODV (Ad Hoc On-Demand Distance Vector). Το A-SAODV σχεδιάστηκε για να παρέχει πρόσθετα επίπεδα ασφαλείας στο AODV, ειδικά στον τομέα της αυθεντικοποίησης.

Κάποια από τα οφέλη του A-SAODV ως προς ένα ασφαλέστερο Ad-Hoc δίκτυο είναι να:

- Χρησιμοποιεί μηχανισμούς αυθεντικοποίησης για την επιβεβαίωση της ταυτότητας των συμμετεχόντων στο δίκτυο.
- Εφαρμόζει κρυπτογραφία για την ασφαλή μεταφορά δεδομένων, όπως στο SAODV.
- Επεκτείνεται, επιτρέποντας την ενσωμάτωση περισσότερων ασφαλιστικών μηχανισμών.
- Περιλαμβάνει μέτρα αντιμετώπισης επιθέσεων, παρόμοια με το SAODV.

Το A-SAODV αποτελεί ένα επιπρόσθετο επίπεδο ασφαλείας για την εξασφάλιση των επικοινωνιών σε ασύρματα ανοικτά δίκτυα, όπως τα ασύρματα δίκτυα αισθητήρων και τα ασύρματα δίκτυα αυτοκινήτων (VANETs).[73]

5.4.2.5 One-TimeCookie

Το "One-TimeCookie" αναφέρεται σε ένα είδος cookie που χρησιμοποιείται στο πλαίσιο των διαδικτυακών συστημάτων αυθεντικοποίησης και ασφαλείας. Τα cookies είναι μικρά κομμάτια

δεδομένων που αποθηκεύονται στον υπολογιστή του χρήστη και συνήθως χρησιμοποιούνται για την αποθήκευση πληροφοριών σχετικά με τη σύνδεση του χρήστη, τις προτιμήσεις του, αλλά και για άλλα σχετικά δεδομένα. Το One-Time Cookie, όπως υποδηλώνει το όνομά του, είναι ένα cookie που έχει περιορισμένη διάρκεια ζωής και μπορεί να χρησιμοποιηθεί μόνο μία φορά. Συνήθως, αυτό το είδος cookie δημιουργείται κατά τη διάρκεια μιας συγκεκριμένης συνεδρίας σύνδεσης ή για ένα συγκεκριμένο αίτημα και στη συνέχεια ακυρώνεται ή λήγει μετά από τη χρήση του. Ο λόγος για τη χρήση ενός One-Time Cookie μπορεί να είναι η αύξηση της ασφάλειας. Διότι, αν ένα τέτοιο cookie χρησιμοποιηθεί μόνο μια φορά, μειώνεται η πιθανότητα για επίθεση με βάση τα cookies (cookie-based attacks), όπως το session hijacking, καθώς το cookie αυτό δεν θα έχει επαναχρησιμοποιηθεί σε μελλοντικές συνεδρίες.[66]

5.4.3 Ενημέρωση του καταναλωτή από τις εταιρείες διασυνδεδεμένων οχημάτων ως προς την ιδιωτικότητα του

Η πρόληψη είναι το καλύτερο μέτρο άμυνας στις πιο πολλές περιπτώσεις, έτσι και στην περίπτωση της προστασίας της ιδιωτικότητας του οδηγού-χρήστη όσον αφορά τα διασυνδεδεμένα οχήματα. Στην δεδομένη κατάσταση που βρίσκεται η τεχνολογία των διασυνδεδεμένων οχημάτων υπάρχουν κενά ως προς την ιδιωτικότητα του χρήστη. Φυσικά με την βοήθεια της τεχνολογίας οι εταιρείες τρέχουν να τα καλύψουν και να κερδίσουν την εμπιστοσύνη του καταναλωτή ως προς αυτό το ζήτημα. Οι αυτοκινητοβιομηχανίες δεν έχουν σκοπό να βλάψουν να τον καταναλωτή ούτε έχουν πρόθεση να παραβιάσουν την προσωπική του ζωή, όμως χρειάζονται τα δεδομένα του, ακόμα και τα προσωπικά, για να του παρέχουν ανέσεις εφόσον επένδυσε στο προϊόν τους, ένα διασυνδεδεμένο όχημα δηλαδή. Άρα η εταιρεία πρέπει να ενημερώνει τον ενδιαφερόμενο οδηγό-χρήστη ως προς την επιλογή του αυτή χωρίς βεβαία να τον απωθεί. Πρέπει όμως να γνωρίζει τους κινδύνους στην καινούργια αυτή τεχνολογία και να μη το παίρνει απήφιστα ότι άπλα είναι ένα όχημα. Αυτό το όχημα έχει την δυνατότητα να τον καταγράφει 24 ώρες αν χρειαστεί και πρέπει να το γνωρίζει. Επίσης πρέπει να είναι ικανός να αναγνωρίσει τις παροχές ασφαλείας των εφαρμογών της εταιρείας που θα του παρέχει το διασυνδεδεμένο όχημα.

Για παράδειγμα, σε μια εταιρεία Α που στην εφαρμογή της άπλα κάνει εγγραφή μόνο με ένα όνομα χρήστη, και σε μια άλλη εταιρεία Β που στην εφαρμογή της θέλει όνομα χρήστη και έναν ισχυρό κωδικό, ο καταναλωτής και μέλλον οδηγός-χρήστης πρέπει να γνωρίζει το ότι η ιδιωτικότητα του θα είναι καλύτερα προστατευμένα στην εταιρεία Β. Μπορούμε να υποθέσουμε, ότι τα διασυνδεδεμένα οχήματα απευθύνονται σε νεότερες γενιές που είναι ικανές να ενημερωθούν σχετικά και να μπορούν να κρίνουν ανάλογα. Από εκεί και πέρα η προστασία της ιδιωτικότητας του χρήστη, αποτελεί ένα συμβόλαιο εμπιστοσύνης μεταξύ καταναλωτή και αυτοκινητοβιομηχανίας. Η εταιρεία ενημέρωσε τον καταναλωτή, και εκείνος το αποδέχτηκε, ότι κάποια από τα προσωπικά του δεδομένα θα ζητηθούν ή θα χρησιμοποιηθούν από το όχημα για τις ανέσεις και τους λογούς που επέλεξε ένα τέτοιο όχημα. Συμπερασματικά η ενημέρωση του χρήστη προστατεύει προληπτικά από παραβίαση της ιδιωτικότητας άτομα που δεν είναι τόσο

εξοικειωμένα με την τεχνολογία αυτή και μπορεί να προβούν σε λάθη ως προς την προσωπική τους ζωή. Οι ερευνητές εργάζονται για την ανάπτυξη εργαλείων ανάλυσης δεδομένων που προστατεύουν καλύτερα το απόρρητο και σημειώνουν πρόοδο όσον αφορά την εξάλειψη της αντιστάθμισης. Έρευνα με επικεφαλής τον Έρβιν Μούρ, διδακτορικό φοιτητή στο εργαστήριο Βιωσιμότητας, Βελτιστοποίησης και Μάθησης για Ανεξάρτητα Δίκτυα του Διεθνούς Πανεπιστημίου της Φλόριντα, που δημοσιεύτηκε στο IEEE Internet of Things Journal, διερεύνησε την ιδέα της χρήσης ομοσπονδιακής μηχανικής μάθησης που βασίζεται σε blockchain για τη βελτίωση του απορρήτου και της ασφάλειας των χρηστών και των ευαίσθητων δεδομένων τους. Η τεχνική θα μπορούσε να χρησιμοποιηθεί για την προστασία των δεδομένων των οδηγών. Υπάρχουν και άλλες τεχνικές για τη διατήρηση του απορρήτου, όπως η συσκοτίση τοποθεσίας, η οποία αλλάζει τα δεδομένα τοποθεσίας του χρήστη για να αποτρέψει την αποκάλυψη της τοποθεσίας του. Ενώ εξακολουθεί να υπάρχει αντιστάθμιση μεταξύ του απορρήτου των χρηστών και της ποιότητας της υπηρεσίας, οι τεχνικές ανάλυσης δεδομένων διατήρησης του απορρήτου, θα μπορούσαν να ανοίξουν τον δρόμο για τη χρήση δεδομένων χωρίς διαρροή προσωπικών στοιχείων αναγνώρισης οδηγών και επιβατών. Με αυτόν τον τρόπο, οι οδηγοί θα μπορούσαν να επωφεληθούν από ένα ευρύ φάσμα υπηρεσιών και χαρακτηριστικών των σύγχρονων αυτοκινήτων, χωρίς να πληρώσουν το υψηλό κόστος της χαμένης ιδιωτικότητας.[51]

6

Απειλή της Ιδιωτικότητας στα VANET

6.1 Εισαγωγή

Η συνδεσιμότητα των αυτοκινήτων με τη βοήθεια των VANET με άλλα οχήματα και με τον έξω κόσμο έχει και υπέρ και κατά. Αφενός μπορεί ο οδηγός να δέχεται πληροφορίες σε πραγματικό χρόνο π.χ. για τον καιρό ή την κίνηση, όμως υπάρχει ο κίνδυνος ευαίσθητα προσωπικά δεδομένα όπως οι προορισμοί του στο σύστημα πλοήγησης να πέσουν σε χέρια τρίτων. Τα Vehicular Ad-Hoc δίκτυα είναι ασύρματα δίκτυα που δημιουργούνται ευέλικτα και αυτόνομα, χωρίς την ανάγκη υποδομής όπως ασύρματοι σταθμοί ή βάσεις. Η ιδιωτικότητα του οδηγού-χρήστη σε ένα διασυνδεδεμένο όχημα μπορεί να πληχτεί άμεσα ή έμμεσα όπως θα αναλυθεί παρακάτω.

6.1.1 Απειλή της ιδιωτικότητας του χρήστη δια μέσω συσκευών του οχήματος ή διαφόρων εφαρμογών.

Η ιδιωτικότητα του οδηγού χρήστη στα διασυνδεδεμένα αυτοκίνητα, πραγματοποιείται με την βοήθεια των οπτικοακουστικών μέσων του οχήματος ή δια μέσω εφαρμογών που διαθέτουν τα διασυνδεδεμένα οχήματα. Γίνεται κατανοητό ότι το ίδιο το όχημα γίνεται ένα ανοιχτό παράθυρο της ιδιωτικής ζωής κάποιου προς όφελος άλλων. Παρακάτω αναλύονται μερικές τέτοιες περιπτώσεις και τα μέσα του οχήματος που μπορεί να προκαλέσουν τέτοια διαρροή δεδομένων .

1. Καταγραφή από εσωτερικές κάμερες επιβατών στο όχημα

Σε προηγούμενα κεφάλαια αναφέρθηκε ότι τα διασυνδεδεμένα αυτοκίνητα διαθέτουν κάμερες στο εσωτερικό τους με σκοπό να καταγράφουν τον οδηγό αλλά και την πορεία του αυτοκινήτου. Επιπροσθέτως οι κάμερες στο εσωτερικό του διασυνδεδεμένου οχήματος καταγράφουν και για λόγους ασφαλείας (καταγραφή έκνομης πράξης εις βάρος του οχήματος) και ειδοποιούν τον οδηγό μέσω των αντίστοιχων καταλλήλων εφαρμογών. Αυτό έχει όμως και το τίμημα του, καθώς η κάμερα αυτή μπορεί να καταγράψει πέρα από τον οδηγό συνεπιβάτες εν αγνοία τους. Η καταγραφή αυτή φυσικά παραβιάζει την ιδιωτικότητα, καθώς τα φυσιογνωμικά χαρακτηριστικά κάποιου βρίσκονται καταγεγραμμένα από την κάμερα του οχήματος χωρίς ο ίδιος να το γνωρίζει . [75]

2. Καταγραφή από εξωτερικές κάμερες του διασυνδεδεμένου οχήματος

Όπως αναφέρθηκε πριν λίγο, δημιουργούνται εύλογες απορίες και προβληματισμοί σχετικά με το πόσο νόμιμο και ασφαλές, για την προστασία της ιδιωτικότητας, είναι το γεγονός ότι οι εξωτερικές κάμερες μπορούν κάλλιστα να καταγράψουν πρόσωπα τυχαίων περαστικών σε ανύποπτη χρονική στιγμή, χωρίς την συγκατάθεση τους. Οι κάμερες που διαθέτουν τα διασυνδεδεμένα αυτοκίνητα είναι υψηλής ανάλυσης και καταγράφουν για μεγάλα χρονικά διαστήματα τον εξωτερικό χώρο γύρω από το διασυνδεδεμένο όχημα. Αυτές οι κάμερες μετατρέπουν το διασυνδεδεμένο όχημα σε ένα τέλειο εποπτικό μέσο, καθώς κανένας δεν μπορεί να υποψιαστεί ότι ένα όχημα καταγράφει τα πάντα γύρω του . Σε πρώτο βαθμό είναι οι πινακίδες άλλων αυτοκινήτων καθώς επίσης και τα πρόσωπα τυχαίων πολιτών. Η συγκεκριμένη δυνατότητα των διασυνδεδεμένων αυτοκινήτων, μπορεί εκτός από τα χαρακτηριστικά που αναφέρθηκαν παραπάνω, να δώσει επίσης πληροφορίες σε μια μεγάλη βάση δεδομένων, με άγνωστους αποδέκτες, για την ακριβή ώρα και τοποθεσία που καταγράφηκε από την αντίστοιχη κάμερα η διέλευση ενός τυχαίου οχήματος ή ενός

πεζού. Σε αυτό το σημείο είναι προφανές και σωστό να αναφερθεί, ότι παραβιάζεται η ιδιωτικότητα του ατόμου από τα μέσα (κάμερες) που διαθέτουν τα διασυνδεδεμένα αυτοκίνητα.[75]

3. Καταγραφή φωνής επιβατών μέσα στο όχημα από το μικρόφωνο του οχήματος

Τα διασυνδεδεμένα αυτοκίνητα διαθέτουν επίσης μικρόφωνα στο εσωτερικό τους. Αυτό είναι μέσο το οποίο μπορεί να καταγράψει την ομιλία όχι μόνο του οδηγού-χρήστη αλλά και άλλων συνεπιβατών του οχήματος. Με την χρήση ενός απλού παραδείγματος, είναι βέβαιο ότι δεν μπορεί να καταρριφθεί ο ισχυρισμός «ότι η ιδιωτικότητα ενός επιβάτη οχήματος σε ένα διασυνδεδεμένο όχημα (ταξί) είναι αμφίβολο να μην έχει παραβιαστεί εάν εκείνος ομιλεί στο τηλέφωνο για κάποιο προσωπικό ζήτημα που έχει». Γίνεται εύκολα κατανοητό ότι εάν το μικρόφωνο είναι ανοιχτό για κάποιο λόγο, ή ενεργοποιείται αυτόματα όταν ανιχνεύσει ομιλία θα καταγράψει λέξεις κλειδιά του επιβάτη, ή ακόμη και το σύνολο της συνομιλίας του. Βεβαιώνεται έτσι ότι το μικρόφωνο μπορεί να χρησιμοποιηθεί ως μέσο παραβίασης της ιδιωτικότητας του ατόμου. [74]

4. Καταγραφή τοποθεσίας και διαδρομής του οδηγού

Τα διασυνδεδεμένα οχήματα διαθέτουν επίσης σύστημα εντοπισμού θέσης (GPS). Γίνεται κατανοητό ότι το όχημα, παρέχει ανά πάσα στιγμή την τοποθεσία του, στις διαφορές οδικές δομές αλλά και σε άλλα διασυνδεδεμένα οχήματα. Η δυνατότητα αυτή αν και έχει πολλά θετικά για το όχημα αλλά και για τον οδηγό του, μπορεί να χαρακτηριστεί αρνητικό ως προς την ιδιωτικότητα του οδηγού. Αυτός ο ισχυρισμός μπορεί να ευσταθεί, επειδή η θέση του οδηγού-χρήστη μπορεί να γνωστοποιηθεί σε τρίτους κατά λάθος, ή και ηθελημένα. Χαρακτηριστικό παράδειγμα που δημιουργείται, είναι ότι η θέση του οχήματος γίνεται γνωστή ακόμα και για μια συγκεκριμένη διαδρομή που ακολουθεί ο οδηγός-χρήστης (όπως για τη δουλειά του ή να πάρει το παιδί του από το σχολείο). Είναι αρκετά προβληματικό, ότι ο χειριστής ενός τρίτου οχήματος, μπορεί ανά πάσα στιγμή να μπορεί να γνωρίζει την τοποθεσία καθώς και την ταυτότητα (Αριθμός κυκλοφορίας οχήματος) ενός άλλου οχήματος, που κινείται σε κοντινή απόσταση από αυτόν. Η δυνατότητα αυτή γίνεται με την βοήθεια ενός επίγειου σταθμού ο οποίος θα «μεταδίδει» πληροφορίες από το ένα όχημα στο άλλο. Είναι εύκολα κατανοητό ότι αυτό το γεγονός, πέρα του ότι παραβιάζει την ιδιωτικότητα του οποιουδήποτε οδηγού διασυνδεδεμένου οχήματος, μπορεί επιπλέον

να τον εκθέτει και σε πιθανό κίνδυνο. Ακόμα εφαρμογές GPS σε κινητά για διασυνδεδεμένα οχήματα μπορούν να εντοπίσουν άλλα οχήματα αντίστοιχης τεχνολογίας πολύ εύκολα . [34]

5. Εγγραφή σε μη ασφαλείς εφαρμογές για διασυνδεδεμένα αυτοκίνητα που ζητούν προσωπικά δεδομένα χρήστη

Ένα επιπλέον αντικείμενο για μελέτη είναι ο ισχυρισμός, ότι ένας επιπλέον κίνδυνος άμεσης παραβίασης της ιδιωτικότητας του οδηγού-χρήστη πραγματοποιείται με την βοήθεια των διαφόρων εφαρμογών διαφόρων εταιρειών για διασυνδεδεμένα αυτοκίνητα, που δεν πληρούν στο έπακρο τους κανονισμούς ασφαλείας του χρήστη. Η τήρηση της πολιτικής ασφαλείας διασύνδεσης χρήστη σε όλες τις εφαρμογές, πρέπει να είναι απαραίτητη και αδιαπραγμάτευτη. Με την βοήθεια αυτής της πολιτικής, τα προσωπικά δεδομένα του οδηγού-χρήστη, κατά την εγγραφή του σε αυτές, θα προστατεύονται από το νομικό πλαίσιο της εκάστοτε χώρας. Σε περίπτωση παράβασης αυτών των κανονισμών, ο οδηγός-χρήστης πιθανόν μη γνωρίζοντας και ο ίδιος τον κίνδυνο , παραθέτει προσωπικά δεδομένα , όπως αριθμό κάρτας τραπέζης , προσωπικά στοιχεία διπλώματος οδήγησης, τόπο μόνιμης κατοικίας, καθώς και άλλα ευαίσθητα προσωπικά δεδομένα σε μια εφαρμογή που μπορεί να τα επεξεργαστεί και να τα εκθέσει σε κίνδυνο . Μπορεί για παράδειγμα η εφαρμογή να μην κρύβει τον αριθμό οχήματος από άλλους χρήστες, ή ακόμη να μην αποκρύπτει τα ευαίσθητα προσωπικά στοιχεία του ίδιου του οδηγού (όπως οδó μόνιμης κατοικίας και μέρος που μπορεί να παρκάρει το όχημα του) . [46]

6.1.2 Παραβίαση της ιδιωτικότητας του χρήστη από επιθέσεις στα δίκτυα των διασυνδεδεμένων οχημάτων.

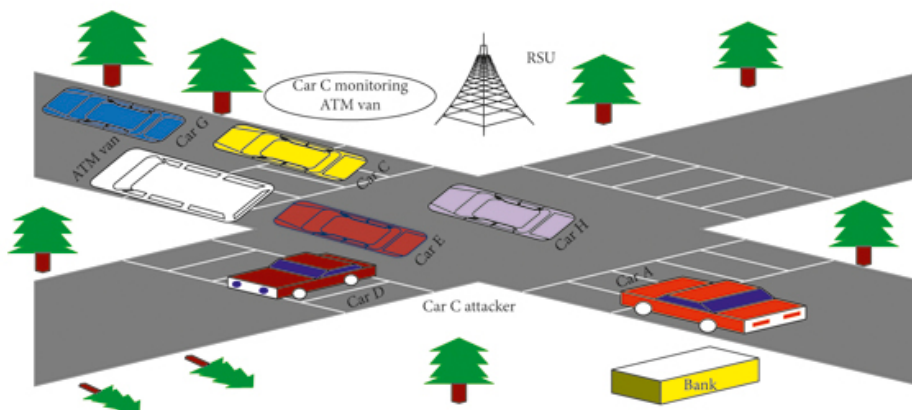
Η ιδιωτικότητα του οδηγού – χρήστη μπορεί να παραβιαστεί ορισμένες φορές από κακόβουλους τρίτους χρήστες. Οι χρήστες αυτοί ασκώντας συγκεκριμένες επιθέσεις, όπως θα αναλυθούν παρακάτω, παραβιάζουν την ασφάλεια ενός δικτύου που επικοινωνούν διασυνδεδεμένα οχήματα και μπορούν να εκμαιεύσουν προσωπικές πληροφορίες του οδηγού χρήστη.

Επιγραμματικά είναι:

- Eaves dropping attack
- Masquera ding attack
- GPS Spoofing attack
- Brute Force attack

6.1.2.1 Eaves dropping (Ακρόαση)

Η επίθεση Eaves dropping (ακρόαση) αναφέρεται στη μη εξουσιοδοτημένη παρακολούθηση ή ακρόαση των επικοινωνιών μεταξύ δύο ή περισσότερων οντοτήτων, συνήθως μέσω δικτύων επικοινωνίας. Ο ισχυρισμός αυτός μπορεί να γίνει με διάφορους τρόπους, στοχεύοντας στην παρακολούθηση πληροφοριών χωρίς τη συγκατάθεση των εμπλεκόμενων μερών. Ανάλογα με το περιβάλλον και τη μέθοδο, μπορεί να λέγεται επίσης "sniffing" ή "interception". **Οι επιθέσεις ακρόασης μπορούν να προκαλέσουν τη διαρροή ευαίσθητων πληροφοριών και να θέσουν σε κίνδυνο την ιδιωτικότητα και την ασφάλεια.** Ο κακόβουλος χρήστης μπορεί να παραβιάσει τις κάμερες ή το μικρόφωνο σε αυτή την επίθεση και να κλέψει προσωπικές πληροφορίες των επιβατών παραβιάζοντας έτσι και την ιδιωτικότητά τους. [59]

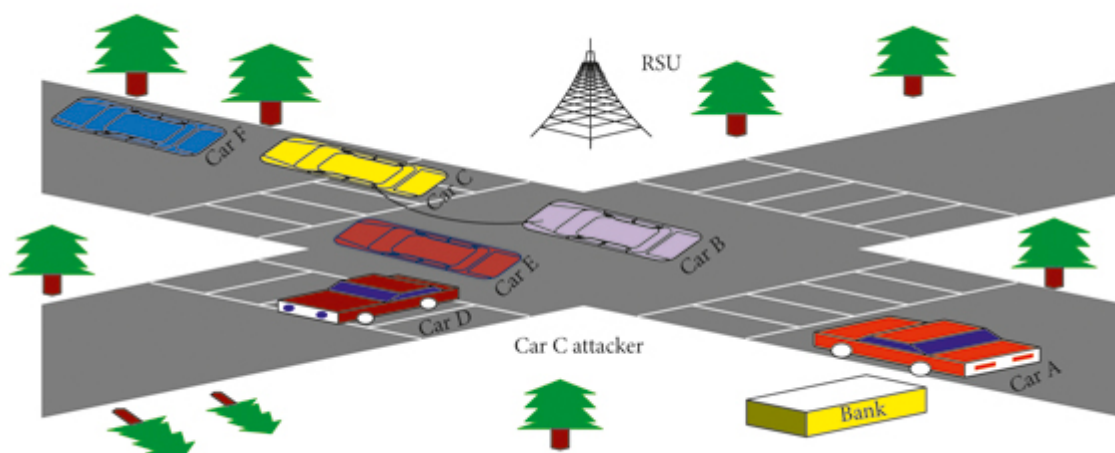


Σχήμα 11: Eaves dropping assault

6.1.2.2 Masquerading Assault

Ο όρος "Masquerading Assault" αναφέρεται σε μια μορφή επίθεσης όπου ο επιτιθέμενος προσποιείται ότι είναι κάποιος άλλος, συνήθως προσποιούμενος την ταυτότητα ενός εγκυροποιημένου χρήστη, συσκευής ή συστήματος. Αυτή η τεχνική είναι γνωστή και ως "masquerade attack" και είναι μια μορφή απάτης ή ανακοπής ασφάλειας.

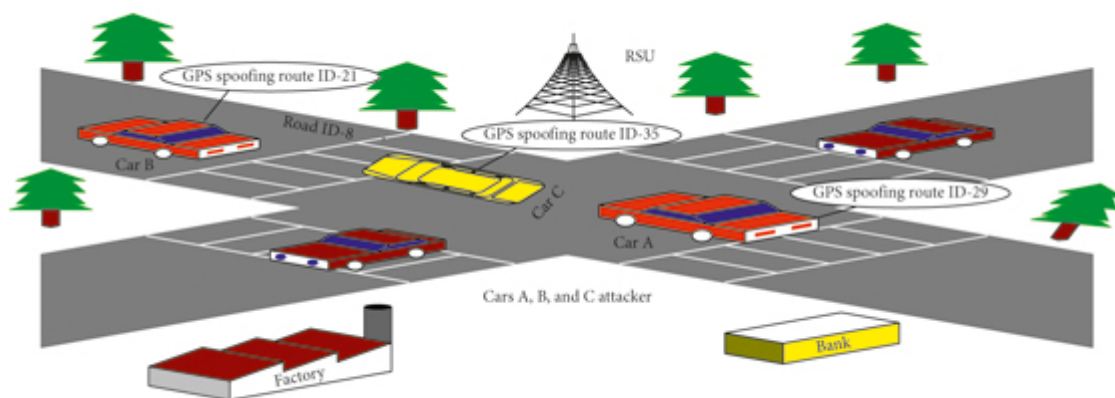
Κατά τη διάρκεια μιας επίθεσης masquerading, ο επιτιθέμενος εκμεταλλεύεται πληροφορίες ή διαπιστευτήρια που ανήκουν σε έναν εγκυροποιημένο χρήστη ή σύστημα για να έχει πρόσβαση σε πληροφορίες ή πόρους που δεν έχει αρμοδιότητα να αποκτήσει. **Αυτή η τακτική μπορεί να χρησιμοποιηθεί για την εξόρυξη ευαίσθητων δεδομένων, την παραβίαση της εμπιστευτικότητας ή ακόμη και για την εκτέλεση κακόβουλου λογισμικού.** [61]



Σχήμα 12: Masquerading assault

6.1.2.3 Global Positioning System Spoofing Assault

Η επίθεση στο σύστημα παραποίησης του συστήματος παγκόσμιου εντοπισμού (Global Positioning System - GPS Spoofing) αναφέρεται στην τεχνική κατά την οποία ο επιτιθέμενος παραποιεί τις πληροφορίες του GPS προκειμένου να παρέχει παραπλανητικές ή παραποιημένες πληροφορίες για τη θέση ενός δέκτη GPS. Αυτό μπορεί να οδηγήσει σε ποικίλες επιπτώσεις, καθώς οι χρήστες ή οι συσκευές που εξαρτώνται από τις ακριβείς πληροφορίες του GPS μπορεί να παραπλανηθούν ως προς την πραγματική τους θέση. **Μια τέτοια επίθεση μπορεί να επηρεάσει την ασφάλεια και την αποτελεσματικότητα των μεταφορών ή να παραπλανήσει ως προς την πραγματική της θέση κάποιο όχημα.** [62]



Σχήμα 13: GPS spoofing assault.

6.1.2.4 Brute Force Assault

Η επίθεση "Brute Force" (βίαιη επίθεση) αναφέρεται σε μια μέθοδο όπου ο επιτιθέμενος προσπαθεί να ανακαλύψει και να υποκλέψει τα σωστά διαπιστευτήρια (όπως όνομα χρήστη και κωδικό πρόσβασης) ενός συστήματος δοκιμάζοντας όλες τις πιθανές συνδυασμούς. Στην ουσία, πρόκειται για μια αναζήτηση "βίας" με όλες τις πιθανές προσπάθειες για να εντοπίσει τα σωστά διαπιστευτήρια.

Συγκεκριμένα, στην επίθεση Brute Force καταχωρίζονται διαφορετικές προσπάθειες για είσοδο στο σύστημα, συνήθως με τη δοκιμή όλων των πιθανών κωδικών πρόσβασης. Αυτή η μέθοδος μπορεί να είναι αποτελεσματική εάν οι κωδικοί πρόσβασης είναι αδύναμοι ή εύκολοι να υποκλαπούν. Έχοντας έτσι τα διαπιστευτήρια του οδηγού ένας κακόβουλος χρήστης αποκτά κατ' επέκταση πρόσβαση σε ευαίσθητες πληροφορίες του οδηγού.[63]

7

Συμπεράσματα

Συμπερασματικά, στη παραπάνω μεταπτυχιακή διπλωματική εργασία αναφέρθηκαν διεξοδικά τα επιμέρους τμήματα ενός διασυνδεδεμένου αυτοκινήτου, τα καινοτόμα ηλεκτρονικά και μη συστήματα που έχει, καθώς και το κόστος και τα πλεονεκτήματα, αλλά και τα μειονεκτήματα αυτού. Στο δεύτερο μισό έγινε εκτενής ανάλυση της προστασίας της ιδιωτικότητας αλλά και των κινδύνων υποκλοπής προσωπικών δεδομένων. Ο κίνδυνος διαρροής προσωπικών δεδομένων, ηθελημένα ή μη, αποτελεί κορυφαία πρόκληση για όλους τους ανθρώπους, που στο άμεσο ή στο μακρινό μέλλον, θα γίνουν κάτοχοι ενός ή περισσότερων διασυνδεδεμένων αυτοκινήτων.

Τα διασυνδεδεμένα αυτοκίνητα, είναι δεδομένο ότι θα γίνουν αναπόσπαστο κομμάτι της ζωής μας. Θα ήταν μη συνετό, οι οδηγοί να μη δεχτούν την ασύγκριτα ασφαλέστερη οδηγική εμπειρία που θα τους παρέχεται. Αλλά όχι μόνο οι οδηγοί (απλοί ή επαγγελματίες), αλλά και οι πεζοί οι οποίοι με τα νέα συστήματα ασφαλείας που παρέχονται, θα αισθάνονται σίγουρα αρκετά ασφαλέστεροι.

Καλό θα ήταν οι αυτοκινητοβιομηχανίες, να διαφυλάξουν τα προσωπικά δικαιώματα των πελατών τους σαν κόρη οφθαλμού. Γι αυτό το λόγο, στις ανεπτυγμένες κοινωνίες όπως αυτές των Ηνωμένων Πολιτειών της Αμερικής αλλά και της Ευρωπαϊκής Ένωσης, ήδη έχουν γίνει μεγάλες κινήσεις προστασίας αυτών, από τις εκάστοτε δικαστικές εξουσίες, ακόμη και αν οι ίδιοι συναινέσουν στην επεξεργασία αυτών άθελά τους.

Η προστασία της ιδιωτικότητας, όπως αναλύθηκε παραπάνω, θα αποτελέσει ένα δυνατό τεστ για όλους μας. Είναι αλήθεια ότι μπορούμε να ισχυριστούμε πως η ανάπτυξη της τεχνολογίας σίγουρα δεν χρησιμοποιείται με καλή βούληση σε όλους τους τομείς. Ο κάθε ανθρώπινος νους θα εκλάβει σίγουρα διαφορετικά αυτόν τον ισχυρισμό, άλλος θα πιστέψει ότι ίσως είναι καλό να «θυσιάσει» μικρό κομμάτι από την προστασία της ιδιωτικότητας του για να απολαύσει τις ανέσεις και την ασφάλεια στον δρόμο που θα του παρέχει ένα τέτοιο όχημα, και άλλος θα μείνει πολύ επιφυλακτικός για το μέλλον που προμηνύεται τουλάχιστον απρόβλεπτο. Η ανθρωπότητα θα

πρέπει να αποφασίσει για το εάν όντως μπορεί να τα καταφέρει και να μείνει έντιμη πρωτίστως ως προς τον εαυτό της.

Κλείνοντας, είναι εύκολα αντιληπτό ότι ο λόγος των τεχνολογικών θαυμάτων, αλλά και ο λόγος της σωστής και συνετής εκμετάλλευσης αυτών, έχουν έναν κοινό παρονομαστή, τον άνθρωπο. Εκείνος εσχάτως θα ορίσει, το πώς θα κινηθεί σε αυτή τη κρίσιμη καμπή της ιστορίας του, αξιολογώντας όλες τις αποφάσεις που έχει λάβει καθ' όλη τη διάρκεια της ύπαρξής του.

8

Βιβλιογραφία

- [1] Ben Aris, (December 15, 2022), Only 11 foreign car brands left in Russia out of 60 before the war.
- [2] Mathilde Carlier, (June 8, 2023), Toyota's retail vehicle sales from 2017 to 2022.
- [3] The first automobile 1885–1886. By Mercedes-Benz group.
- [4] Michael J. Coren, (January 30, 2024), Plug-in hybrids vs. electric cars: We did the math on which is better for you (The Washington Post).
- [5] Autopilot Features , by Tesla.com.
- [6] Stephen Gossett, Jessica Powers (January 12, 2024), Automotive IoT: A Brief Overview of the Connected Car.
- [7] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications Version 2.0, Adopted on (9 March 2021).
- [8] Hakim Badis, Abderrezak Rachedi, (2015), Modeling tools to evaluate the performance of wireless multi-hop networks.
- [9] Ihn-Han Bae, Stephan Olariu, (06 December 2010), A Tolerant Context-Aware Driver Assistance System for VANETs Based Smart Cars.
- [10] Felix Roeckle, Raphael Hahn, Sebastian Stegmueller, Florian Herrmann, (Features of future autonomous cars: beyond interior design A global survey on user preferences)
- [11] Keith Barry, (January 5, 2023), New Car Features We Love and Some We don't.
- [12] Vijay Pattni, (28 Jan 2019), Look at the size of the brand-new Renault Clio's screen.
- [13] Anshul Saxena, (25 September, 2023), Everything You Need to Know About In-Vehicle Infotainment Systems.
- [14] Paul Horrell, 923 Mar 2023), Mercedes-Benz A-Class review.

- [15] Alex Guberman, (24 July 2019), Purpose of Internal Camera in Tesla Model 3 Revealed
- [16] What is ADAS?, <https://www.synopsys.com/automotive/what-is-adas.html>
- [17] How To: Mercedes-Benz PARKTRONIC with Active Parking Assist, <https://www.waltersmercedesbenzofriverside.com/videos/how-to-mercedes-benz-parktronic-with-active-parking-assist/#:~:text=Your%20Mercedes%2DBenz%20will%20control,put%20the%20car%20in%20park.>
- [18] Jeff Wagner (18 October, 2022), Is stop-start technology really beneficial for your vehicle?
- [19] Karim Nice, How Wires, Fuses, and Connectors Work
- [20] Wèi Zhī, (28 October 2019), Car CAN protocol analysis tool usage
- [21] David Bortolami, (28 September 2020), CAN-Bus: Introduction and History
- [22] EMQ Technologies Inc, (1 June, 2023), CAN Bus: How It Works, Advantages, and Disadvantages
- [23] Advanced Industrial Control Technology, 2010, Carrier Sense Multiple Access
- [24] Emerson team (24 May 2023), Controller Area Network (CAN) Overview
- [25] Basecoin team, (18 May 2021), Τι είναι ένα δίκτυο Peer-to-Peer (P2P) και πώς λειτουργεί;
- [26] <https://www.iso.org/obp/ui/en/#iso:std:iso:11898:-2:ed-2:v1:en>
- [27] Bayerische Motoren Werke (BMW). Δίαυλος CAN. Το Δίκτυο δεδομένων χρησιμοποιεί μονή γραμμή δεδομένων.
- [28] Nikhil Agnihotri, What are top applications of CAN protocol?
- [29] Beverly Braga, (11 September 2020), What New Cars Have Wi-Fi?
- [30] Elizabeth Blackstock, (11 January, 2022), Bluetooth in Cars: How Does It Work?
- [31] Kersten Heineke, Alexandre Ménard, Freddie Södergren and Martin Wrulich (27 June 2019), Development in the mobility technology ecosystem—how can 5G help?
- [32] Andrew J. Hawkins, (11 December, 2023), If you want to use a digital key to drive your car, look for this logo
- [33] Jacob Biba, Jessica Powers (29 March 2023), What Is Vehicle-to-Everything (V2X) Technology?
- [34] Kailash Vaviya, Jenn Peters, (4 October 2023), What Cars Have GPS Tracking Built-in: Everything You Need To Know
- [35] Stan Weiss, (8 September 2022), Connected Vehicles and Tolling's Frequency Future: DSRC
- [36] D. Yun, Seung-Ju Lee, Do Hyun Kim, (October 2014), A study on the vehicular wireless base-station for in-vehicle wireless sensor network system

- [37] Zhenhui Yuan, Jie Jin, Jing Chen, Lingling Sun, Gabriel-Miro Muntean, (December 2017), ComProSe Shaping Future Public Safety Communities with ProSe-Based UAVs
- [38] T. Schmidt, R. Philipsen, P. Themann, M. Ziefle, (22 June 2016), Public perception of V2X-technology - evaluation of general advantages, disadvantages and reasons for data sharing with connected vehicles
- [39] Alberto Bocca, Donkyu Baek, (4 July 2019), Automated Driving Systems: Key Advantages, Limitations and Risks
- [40] <https://el.wikipedia.org/wiki/%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1>
- [41] https://el.wikipedia.org/wiki/%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1_%CF%83%CF%84%CE%BF_%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF
- [42] https://el.wikipedia.org/wiki/%CE%93%CE%B5%CE%BD%CE%B9%CE%BA%CF%8C%CF%82_%CE%9A%CE%B1%CE%BD%CE%BF%CE%BD%CE%B9%CF%83%CE%BC%CF%8C%CF%82_%CE%B3%CE%B9%CE%B1_%CF%84%CE%B7%CE%BD_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1_%CF%84%CF%89%CE%BD_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD
- [43] <https://www.lifo.gr/now/tech-science/exypna-aytokinita-poso-asfali-einai-ta-prosopika-dedomena-odigoy-kai-epibatou>
- [44] <https://underwriter.gr/%CF%80%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC-%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1-%CF%83%CF%84%CE%B1-%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B1-%CE%B1%CF%85%CF%84%CE%BF%CE%BA%CE%AF/>
- [45] <https://www.in.gr/2023/09/06/in-science/technology/aytokinito-ta-prosopika-dedomena-pou-syllegontai-einai-proion-gia-poulima/>
- [46] https://www.gocar.gr/news/feed/29102,Poia_dedomena_moirazontai_ta_exypna_ayto.html
- [47] https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page0a_gr/page0a_gr?OpenDocument&ExpandSection=2
- [48] <https://techmonitor.ai/technology/cybersecurity/vehicle-cybersecurity-enisa>
- [49] <https://www.hindawi.com/journals/scn/2021/9997771/>
- [50] <https://www.geeksforgeeks.org/wormhole-attack-in-wireless-sensor-networks/>
- [51] <https://www.sofokleousin.gr/ta-eksypna-aytokinita-mas-kratoun-asfaleis-i-eisvalloun-stin-idio>
- [52] <https://www.sciencedirect.com/science/article/abs/pii/S1570870503000192>

- [53] <https://www.scirp.org/journal/paperinformation?paperid=97285>
- [54] Taskeen Zaidi Syed.Faisal, July 2019 , An Overview: Various Attacks in VANET
- [55] Rupali Sharma , 2016 , Gray-hole Attack in Mobile Ad-hoc Networks : A Survey
- [56] Yih-Chun Hu, Adrian Perrig, and David B. Johnson , February 2006 , Wormhole Attacks in Wireless Networks
- [57] Mohammed Ali Hezam Al Junaid , Syed A. A, Mohd Nazri Mohd Warip, Ku Nurul Fazira Ku Azir , Nurul Hidayah Romli , 2017 , Classification of Security Attacks in VANET: A Review of Requirements and Perspectives
- [58] Mohsen Imani , Mahdi Taheri , M.Naderi , December 2010 , Security enhanced routing protocol for ad hoc networks
- [59] [What Are Eavesdropping Attacks? | Fortinet](#)
- [60] [Node impersonation attack: \(a\) the Invisible Node attack. The malicious... | Download Scientific Diagram \(researchgate.net\)](#)
- [61] [What is a Masquerade Attack? - Definition from Techopedia](#)
- [62] [What Is GPS Spoofing and How Do You Defend Against It? | Okta](#)
- [63] [What is a Brute Force Attack? | Definition, Types & How It Works \(fortinet.com\)](#)
- [64] William Whyte , 06 Dec 2026 , IEEE 1609.2 and Connected Vehicle Security: Standards Making in a Pocket Universe
- [65] [aran_jsac05.pdf \(ucsb.edu\)](#)
- [66] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad and Patrick Traynor , One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens
- [67] Manel Guerrero-Zapata , June 2002 , Secure Ad hoc On-Demand Distance Vector Routing
- [68] [Elliptic Curve Digital Signature Algorithm - Wikipedia](#)
- [69] [Blockchain - Elliptic Curve Digital Signature Algorithm \(ECDSA\) - GeeksforGeeks](#)
- [70] [A deep learning-based general robust method for network reconfiguration in three-phase unbalanced active distribution networks - ScienceDirect](#)
- [71] [Towards holistic secure networking in connected vehicles through securing CAN-bus communication and firmware-over-the-air updating - ScienceDirect](#)
- [72] Zeyu Lei, Yuhong Nan, Yanick Fratantonio, and Antonio Bianchi , On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices
- [73] Preeti Sachan & Pabitra Mohan Khilar , Authenticated Routing for Ad-Hoc On-Demand Distance Vector Routing Protocol

[74] <https://www.mdpi.com/2079-9292/11/5/766>

[75] SIVA R. K. NARLA , JULY 2013 , The Evolution of Connected Vehicle Technology: From Smart Drivers to Smart Cars to... Self-Driving Cars

[76] [SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks - ScienceDirect](#)

