ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«INTELLIGENT TRANSPORTATION SYSTEMS AND GDPR CHALLENGES»

Διπλωματική Εργασία

του

Ντελιάκη Γεώργιου

Θεσσαλονίκη, Μάρτιος 2024

«INTELLIGENT TRANSPORTATION SYSTEMS AND GDPR CHALLENGES»

Ντελιάκης Γιώργος

Πτυχίο Τμήματος Τηλεπληροφορικής και Διοίκησης, ΤΕΙ Ηπείρου, Σχολή Διοίκησης και Οικονομίας, 2008

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2024

Κωνσταντίνος Ψάννης Στυλιανός Ξυνόγαλος Μιχαήλ Μαντάς

Ντελιάκης Γιώργος

Περίληψη

Το Διαδίκτυο των Πραγμάτων (IoT), τα ασύρματα δίκτυα 5ης γενιάς, τα μαζικά δεδομένα, το blockchain, η τεχνητή νοημοσύνη και το cloud computing παρουσιάζουν τεράστια επίδραση στην εξέλιξη του τομέα των μεταφορών. Οι προκλήσεις που φέρνουν οι τεχνολογίες αυτές στον κλάδο είναι πολλές και σημαντικές.

Οι εφαρμογές IoT έχουν εφαρμογή σε αρκετούς τομείς των έξυπνων μεταφορών όπως η έξυπνη κυκλοφορία, η έξυπνη στάθμευση και η έξυπνη κινητικότητα. Οι εφαρμογές αυτές μπορούν να δώσουν στους οδηγούς αποτελεσματικές ιδέες διαδρομών, γρήγορες κρατήσεις στάθμευσης, οικονομικό φωτισμό δρόμου, τηλεματική για τις δημόσιες συγκοινωνίες, αποφυγή ατυχημάτων και αυτόνομη οδήγηση χρησιμοποιώντας αισθητήρες ενσωματωμένους σε αυτοκίνητα ή κινητές συσκευές και συσκευές που αναπτύσσονται στην πόλη. Ο σχεδιασμός και ο προγραμματισμός έξυπνων μεταφορών, οι έξυπνες κοινότητες, οι έξυπνες πόλεις, τα έξυπνα συστήματα ελέγχου και άλλοι τομείς που έχουν ενσωματωθεί στο οικοσύστημα του IoT, χρησιμοποιούν τεχνικές ανάλυσης μαζικών δεδομένων, τεχνολογία ιδιαίτερα κρίσιμη για την ανάπτυξη ευφυών συστημάτων μεταφορών καθώς επιτρέπουν την αποτελεσματική διαχείριση όλων των δεδομένων που απαιτούνται για την ανάπτυξη νέων τρόπων παροχής ασφαλέστερων, καθαρότερων και αποδοτικότερων μεταφορών. Η έλευση του 5G έχει τη δυνατότητα να παρέχει αξιόπιστη πρόσβαση σε Internet υψηλής ταχύτητας στα μέσα μαζικής μεταφοράς, να συλλέγει και να αναλύει δεδομένα σε πραγματικό χρόνο από συνδεδεμένα αυτοκίνητα, υποδομές και συσκευές για να βοηθήσει στη λήψη επιχειρησιακών αποφάσεων.

Το blockchain φαίνεται να είναι η τεχνολογία που μπορεί να δώσει αξιόπιστες λύσεις στη διαχείριση δεδομένων για έξυπνες και ασφαλείς μεταφορές. Οι τεχνολογίες κατανεμημένου καθολικού όπως το blockchain έχουν τη δυνατότητα να προστατεύσουν τα δεδομένα κίνησης και θέσης του ατόμου και να προστατεύσουν το απόρρητό τους. Η θέσπιση και διευθέτηση των αρχών και των κανονισμών που υποδηλώνουν με ποιον τρόπο πρέπει να αναπτυχθεί, να εφαρμοστεί η τεχνητή νοημοσύνη είναι γνωστό ότι έχουν κρίσιμα αποτελέσματα που μπορούν να απειλήσουν την ασφάλεια των ανθρώπων, π.χ. αυτόνομα οχήματα. Το νομικό πλαίσιο που θα διέπει τη λειτουργία συσκευών τεχνητής νοημοσύνης στα ITS είναι μια από τις μεγαλύτερες προκλήσεις για την προστασία της ιδιωτικής ζωής των μετακινούμενων, της διαφάνειας και της λογοδοσίας. Η διαχείριση των δεδομένων στα ITS είναι ζωτικής σημασίας γιατί είναι το κλειδί όχι μόνο για την εφαρμογή τεχνολογιών, αλλά και για την αξιολόγηση του κοινωνικού τους αντικτύπου, ακόμη και για τη θέσπιση πολιτικών.

Ο GDPR είναι η εξέχουσα νομοθεσία σχετικά με την προστασία των δεδομένων εντός της ΕΕ, θέτοντας επίσης ένα παγκόσμιο πρότυπο, καθώς αντιπροσωπεύει τη ραχοκοκαλιά της μελλοντικής ψηφιακής οικονομίας της ΕΕ. Η διαχείριση και η προστασία των δεδομένων βρίσκεται στο επίκεντρο αυτής της πρόκλησης.

Λέξεις κλειδιά: Ευφυή Συστήματα Μεταφορών, Τεχνητή Νοημοσύνη, ΓΚΠΔ, Μαζικά Δεδομένα, 5G, IoT, Αυτόνομα Οχήματα, Blockchain, Προσωπικά Δεδομένα, Privacy, Τηλεπικοινωνίες, GDPR, Ασφάλεια Δεδομένων

Abstract

The Internet of Things (IoT), 5G wireless networks, big data, blockchain, artificial intelligence and cloud computing have a huge impact on the evolution of the transport sector. The challenges these technologies bring to the industry are many and significant.

IoT applications have application in several areas of smart transport such as smart traffic, smart parking and smart mobility. These applications can give drivers effective route concepts, fast parking reservations, economical street lighting, telematics for public transport, accident avoidance and autonomous driving using sensors embedded in cars or mobile devices and devices deployed in the city. Smart transport planning and planning, smart communities, smart cities, intelligent control systems and other sectors integrated into the IoT ecosystem, use big data analytics techniques, technology particularly critical for the development of intelligent transport systems as they enable the efficient management of all data needed to develop new ways of providing safer ones, cleaner and more efficient transport. The advent of 5G has the potential to provide reliable, high-speed Internet access on public transportation, collect and analyze real-time data from connected cars, infrastructure, and devices to aid in making operational decisions.

Blockchain seems to be the technology that can give reliable solutions in data management for smart and secure transfers. Distributed ledger technologies like blockchain have the potential to protect an individual's movement and location data and protect their privacy. Establishing and arranging the principles and regulations that indicate how AI should be developed, applied is known to have critical effects that can threaten people's safety, e.g. autonomous vehicles. The legal framework governing the operation of AI devices in ITS is one of the biggest challenges for mobile privacy, transparency and accountability.

Data management in ITS is crucial because it is key not only to implement technologies, but also to assess their social impact and even establish policies.

GDPR is the preeminent data protection legislation within the EU, also setting a global standard as it represents the backbone of the EU's future digital economy. Data management and protection is at the heart of this challenge.

Keywords: Intelligent Transport Systems, Artificial Intelligence, GDPR, Big Data, 5G, IoT, Autonomous Vehicles, Blockchain, Personal Data, Privacy, Telecommunications, GDPR, Dara Security

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών του Πανεπιστημίου Μακεδονίας και του Δημοκριτείου Πανεπιστημίου Θράκης, με τίτλο «Δίκαιο και Πληροφορική». Ο συνδυασμός δύο διαφορετικών επιστημονικών πεδίων και το ενδιαφέρον μου για τις επιπτώσεις της διαχείρισης των προσωπικών δεδομένων στο διαδίκτυο, ήταν οι δύο βασικοί παράγοντες που με ώθησαν να επιλέξω το συγκεκριμένο μεταπτυχιακό. Οι προσδοκίες εκπληρώθηκαν καθώς το πρόγραμμα απαρτίζεται από υψηλού επιπέδου Διδακτικό προσωπικό και η οργάνωση – δομή των μαθημάτων μας ήταν στοχευμένη και ουσιαστική. Για αυτόν τον λόγο θα ήθελα να συγχαρώ την κα. Ευγενία Αλεξανδροπούλου-Αιγυπτιάδου, υπό τη Διεύθυνση της οποίας διεξάγεται το παρόν πρόγραμμα. Επίσης, θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Ψάννη Κωνσταντίνο, ο οποίος ως επιβλέπων καθηγητής, με καθοδήγησε για την εκπόνηση της παρούσας εργασίας, δείχνοντας μου εμπιστοσύνη και προσφέροντας μου την κατάλληλη καθοδήγηση. Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, η οποία με στηρίζει σε κάθε μου απόφαση και είναι πάντα δίπλα μου.

Περιεχόμενα

1 Εισαγωγή

Τα έξυπνα συστήματα μεταφορών έχουν σχεδιαστεί για να ανταποκρίνονται καλύτερα και να προσαρμόζονται καλύτερα στις μεταβαλλόμενες συνθήκες κυκλοφορίας, κάτι που καθίσταται δυνατό με την ανάπτυξη νέων τεχνολογιών, όπως το Διαδίκτυο των πραγμάτων (IoT), το υπολογιστικό νέφος και η ανάλυση μαζικών δεδομένων. Όπου, η συλλογή και ανάλυση δεδομένων σε πραγματικό χρόνο που καθίσταται δυνατή από αυτές τις τεχνολογίες μπορεί να χρησιμοποιηθεί για την ενίσχυση της ροής της κυκλοφορίας, τη μείωση της συμφόρησης και την ενίσχυση της ασφάλειας. Επίσης, η επιθυμία να αυξηθεί η αποδοτικότητα των μεταφορών, να μειωθεί η συμφόρηση και να βελτιωθεί η ασφάλεια έχει προωθήσει την πρόοδο των ευφυών συστημάτων μεταφορών (ITS) και των οδικών μονάδων (RSU) από συμβατικά σε έξυπνα συστήματα μεταφορών. Η μετάβαση σε έξυπνα συστήματα μεταφορών υπόσχεται σημαντικά τη βελτίωση της αποδοτικότητας, της ασφάλειας, της ευφυΐας, της αξιοπιστίας και της βιωσιμότητας των συστημάτων μεταφορών.

Η αυτοκινητοβιομηχανία βρίσκεται σε μια πορεία όπου τα οχήματα αποκτούν συνεχώς μεγαλύτερη επίγνωση του περιβάλλοντός τους λόγω της προσθήκης διαφόρων τύπων ενσωματωμένων αισθητήρων. Ταυτόχρονα, αυξάνεται ο όγκος της αυτοματοποίησης των οχημάτων, ο οποίος, με κάποια ενδιάμεσα βήματα, θα κορυφωθεί με την πλήρως αυτοματοποιημένη οδήγηση χωρίς ανθρώπινη παρέμβαση. Κατά μήκος αυτής της διαδρομής, αυξάνεται ο αριθμός των αλληλεπιδράσεων, τόσο μεταξύ των οχημάτων όσο και μεταξύ των οχημάτων και άλλων χρηστών του οδικού δικτύου, με μια ολοένα και πιο έξυπνη οδική υποδομή. Ως επακόλουθο, η σημασία και η εξάρτηση από ικανά συστήματα επικοινωνίας για την επικοινωνία οχήματος με οτιδήποτε (V2X) γίνεται βασικό πλεονέκτημα που θα βελτιώσει την απόδοση της αυτοματοποιημένης οδήγησης και περαιτέρω αύξηση της οδικής ασφάλειας με συνδυασμό τεχνολογιών που βασίζονται σε αισθητήρες. Από την άλλη, η βιομηχανία κινητών επικοινωνιών έχει συνδέσει περισσότερους από 5 δισεκατομμύρια ανθρώπους τα τελευταία 25 χρόνια και τα κινητά τηλέφωνα έχουν γίνει μέρος της καθημερινής μας ζωής. Το επόμενο βήμα στην ασύρματη συνδεσιμότητα είναι η σύνδεση όλων των ειδών συσκευών, με συνολικά 28 δισεκατομμύρια συνδεδεμένες συσκευές να έχουν προβλεφθεί έως το 2021.

Αυτές οι τεχνολογίες διαδραματίζουν επίσης ζωτικό ρόλο σε ένα σύγχρονο σύστημα μεταφορών. Τα οχήματα με εξελιγμένα συστήματα πρόληψης ατυχήματος, όπως τα συστήματα προειδοποίησης σύγκρουσης (collision warning systems, CWS) ή το σύστημα υποβοήθησης διατήρησης λωρίδας (lane-keeping assistance, LKA), είναι πλέον διαθέσιμα στην αγορά. Το επόμενο στάδιο για τη μείωση των τροχαίων ατυχημάτων είναι ο έγκαιρος προγραμματισμός για τέτοια αυτοκίνητα ώστε να ελαχιστοποιηθούν οι συγκρούσεις, βελτιώνοντας παράλληλα τη ροή της κυκλοφορίας. Για την αποτελεσματική διαχείριση των κυκλοφοριακών προβλημάτων, απαιτούνται επικοινωνίες μεταξύ οχημάτων και υποδομών (V2I).

2 Τεχνολογίες Ευφυών Συστημάτων Μεταφορών

2.1 IOT & ITS

Τις τελευταίες δεκαετίες, έχουμε βιώσει την κυριαρχία νέων τύπων επικοινωνίας μεταξύ ανθρώπων και πραγμάτων και μεταξύ των ίδιων των πραγμάτων που οδηγούν στην εμφάνιση ενός νέου παραδείγματος που ονομάζεται Διαδίκτυο των Πραγμάτων. Το παράδειγμα του IoT έχει αποδείξει τις δυνατότητές του να αναδιαμορφώσει το μέλλον της επικοινωνίας στο Διαδίκτυο, φέρνοντας τεράστιες βελτιώσεις και ριζικό μετασχηματισμό στις ανθρώπινες ζωές. Αποτελείται από ένα πλήθος τεχνολογιών αιχμής στον τομέα των πληροφοριών και των επικοινωνιών που γεφυρώνουν τον φυσικό κόσμο (π.χ. οχήματα και έξυπνες συσκευές) με τον ψηφιακό κόσμο για να σχηματίσουν ένα νέο ευφυές σύστημα.

Τον περασμένο αιώνα σημειώθηκαν σημαντικές βελτιώσεις στην ποιότητα ζωής, ιδίως όσον αφορά την πρόσβαση στις υπηρεσίες. Ωστόσο, οι διαχειριστές, οι αρχιτέκτονες και οι πολεοδόμοι αντιμετώπισαν σημαντικό πρόβλημα λόγω της εντατικής βιομηχανίας και του αυξανόμενου πληθυσμού στις μητροπολιτικές περιοχές. Κατά την τελευταία δεκαετία, το Διαδίκτυο των Πραγμάτων (IoT) και οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) είχαν τεράστιο αντίκτυπο στον τρόπο με τον οποίο οι επιχειρήσεις προσεγγίζουν την καινοτομία και στον τρόπο με τον οποίο δημιουργούν και εκμεταλλεύονται ευκαιρίες στις καθημερινές τους δραστηριότητες. Αυτά επιδεινώθηκαν στις έξυπνες πόλεις, όπου ο σκοπός του Διαδικτύου των Πραγμάτων είναι να αξιοποιήσει τις ΤΠΕ για να επιτρέψει υπηρεσίες προστιθέμενης αξίας για τους πολίτες, παρέχοντας παράλληλα στις επιχειρήσεις περισσότερες ευκαιρίες να καινοτομήσουν ενσωματώνοντας τεχνολογία αιχμής. Μια πτυχή της έξυπνης πόλης είναι οι έξυπνες μεταφορές. Οι μεταφορές έχουν γίνει η δεύτερη μεγαλύτερη πηγή εκπομπών άνθρακα λόγω της χαμηλής αποδοτικότητάς τους. Έχει αντίκτυπο όχι μόνο στις έξυπνες μεταφορές αλλά και στο περιβάλλον. Ως αποτέλεσμα, η βελτίωση της αποδοτικότητας των μεταφορών είναι ζωτικής σημασίας για τις έξυπνες μεταφορές και τις έξυπνες πόλεις. Αν και οι μεταφορές έχουν βελτιώσει σημαντικά τη ζωή μας, πολλές σημαντικές προκλήσεις παραμένουν άλυτες, συμπεριλαμβανομένων των αυτοκινητιστικών συγκρούσεων και της έντονης κυκλοφοριακής συμφόρησης ιδιαίτερα στα μεγάλα αστικά κέντρα.

Οι πρόσφατες εξελίξεις στην ασύρματη δικτύωση αισθητήρων, το cloud computing, τα μεγάλα δεδομένα και το IoT δημιουργούν μια νέα γενιά έξυπνων εφαρμογών μεταφοράς. Το IoT αποτελείται από ένα δίκτυο φυσικών αντικειμένων με δυνατότητα web, ενσωματωμένα με αισθητήρες, επεξεργαστές, και υλικό επικοινωνίας που αποκτούν δεδομένα από το περιβάλλον τους. Αυτές οι συσκευές αποτελούν διάχυτες πλατφόρμες παρακολούθησης που επιτρέπουν τη μαζική συλλογή και ανταλλαγή δεδομένων σε πραγματικό χρόνο, χτίζοντας έτσι τα θεμέλια των έξυπνων συστημάτων μεταφορών.

Οι εφαρμογές IoT έχουν εξελιχθεί σε διάφορα μέρη των έξυπνων μεταφορών. Παραδείγματα είναι η έξυπνη κυκλοφορία, η έξυπνη στάθμευση και η έξυπνη κινητικότητα. Αυτές οι εξελίξεις καθιστούν τις έξυπνες μεταφορές εφικτές για να δώσουν στους οδηγούς αποτελεσματικές ιδέες διαδρομών, γρήγορες κρατήσεις

στάθμευσης, οικονομικό φωτισμό δρόμου, τηλεματική για τις δημόσιες συγκοινωνίες, αποφυγή ατυχημάτων και αυτόνομη οδήγηση χρησιμοποιώντας αισθητήρες ενσωματωμένους σε αυτοκίνητα ή κινητές συσκευές και συσκευές που αναπτύσσονται στην πόλη .

Οι εφαρμογές έχουν γίνει πιο έξυπνες καθώς το Διαδίκτυο των Πραγμάτων έχει αυξηθεί σε όγκο και οι συνδεδεμένες συσκευές χρησιμοποιούνται σε όλο και περισσότερες υποδομές των σύγχρονων πόλεων. Οι προσεγγίσεις μηχανικής μάθησης (ML) χρησιμοποιούνται για τη βελτίωση της νοημοσύνης και των δυνατοτήτων μιας εφαρμογής καθώς ο όγκος των διαθέσιμων δεδομένων επεκτείνεται. Καθώς ο παγκόσμιος πληθυσμός αυξάνεται, αυξάνεται και ο αριθμός των οχημάτων στο δρόμο, αυξάνοντας τα ζητήματα διαχείρισης της κυκλοφορίας, και ιδιαίτερα αυτά των δημόσιων συγκοινωνιών. Επιπλέον, αυξάνεται η συχνότητα των ατυχημάτων και άλλων προβλημάτων που σχετίζονται με την κυκλοφορία. Το Σύστημα Ευφυών Μεταφορών (ITS) ξεπερνά τα περισσότερα από αυτά τα προβλήματα συγχωνεύοντας τις υπάρχουσες τεχνολογίες με τις υφιστάμενες υποδομές. Με την εξέλιξη της κινητής τεχνολογίας και της πανταχού παρουσίας του κυψελοειδούς δικτύου με τα συγκριτικά οφέλη που προσφέρουν τα δίκτυα 5ης γενιάς, η παρακολούθηση οχημάτων σε πραγματικό χρόνο για αποτελεσματική διαχείριση των μεταφορών είναι πλέον λειτουργική.

Είναι επιτακτική ανάγκη να χρησιμοποιηθούν περισσότερο οι υποδομές του IoT και να ενσωματωθούν απρόσκοπτα οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) για τη δημιουργία ενός βιώσιμου, έξυπνου συστήματος μεταφορών. Η υλοποίηση και εφαρμογή προηγμένων επικοινωνιακών, ηλεκτρονικών και υπολογιστικών δυνατοτήτων επιτρέπει τη μεταφορά πληροφοριών, τον έλεγχο της ροής της κυκλοφορίας και τη διαχείριση των δικτύων μεταφορών. Τέσσερις βασικές έννοιες, η βιωσιμότητα, η ενσωμάτωση, η ασφάλεια και η αποκριτικότητα, έχουν προτεραιότητα κατά την υιοθέτηση και εφαρμογή αναδυόμενων τεχνολογιών στα συστήματα μεταφορών. Οι αρχές αυτές θα είναι ζωτικής σημασίας για την επίτευξη των κύριων στόχων των έξυπνων μεταφορών, οι οποίοι είναι η πρόσβαση και η κινητικότητα, η περιβαλλοντική βιωσιμότητα και η οικονομική ανάπτυξη[1].

Οι αναδυόμενες τεχνολογίες θα επιτρέψουν τη βιωσιμότητα των υποδομών μεταφορών. Με την εφαρμογή νέων τεχνικών συλλογής, επεξεργασίας και διάδοσης πληροφοριών με βάση τις συνθήκες κυκλοφορίας, θα ενθαρρύνουν την αποτελεσματική χρήση των υφιστάμενων υποδομών μεταφορών για τη ρύθμιση, τον έλεγχο και τη διαχείριση της κυκλοφορίας των οχημάτων. Αυτό θα βελτιώσει τη διαχείριση της συμφόρησης και θα μειώσει τις επιπτώσεις της.

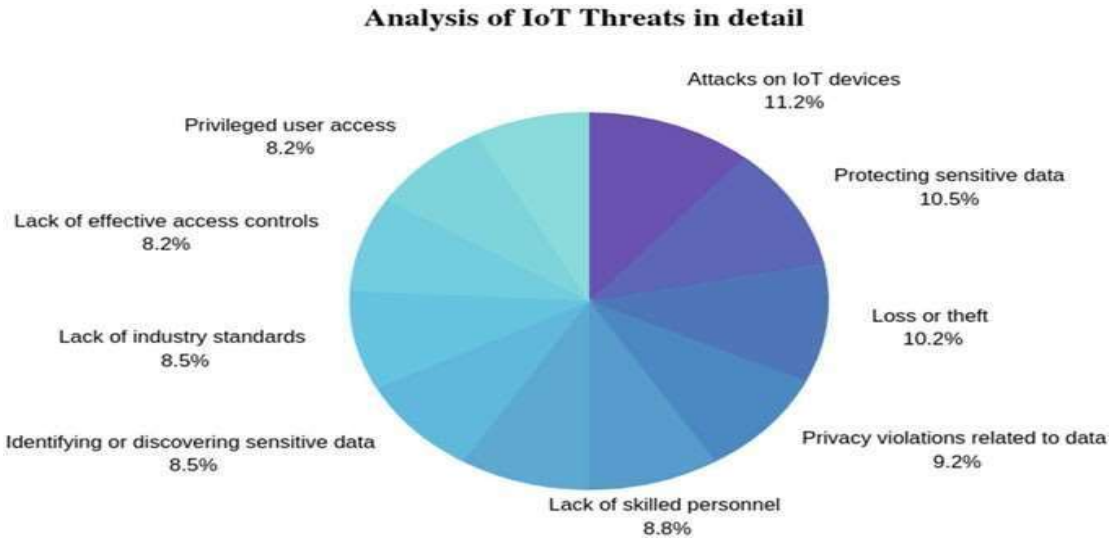
Το IoT είναι η τεχνική ραχοκοκαλιά των έξυπνων πόλεων σε τόσο σε επίπεδο υποδομών αλλά και των τεχνολογιών που θα διέπουν την λειτουργία των υποδομών αυτών, στο φυσικό και στο ψηφιακό κόσμο. Το IoT παρέχει τη δυνατότητα απομακρυσμένης παρακολούθησης, διαχείρισης και ελέγχου συσκευών, καθώς και δημιουργίας νέων πληροφοριών και αξιοποιήσιμων πληροφοριών από τεράστιες ροές δεδομένων σε πραγματικό χρόνο δίνοντας τη δυνατότητα σε ένα αντικείμενο να ακούει, να βλέπει, να ακούει, να ερμηνεύει και να επικοινωνεί ταυτόχρονα.

[1] Guerrero-Ibanez, J.A.; Zeadally, S.; Contreras-Castillo, J. Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wirel. Commun. 2015, 22, 122–128.

2.2 IOT και ασφάλεια δεδομένων στα ITS

Η υποδομή των έξυπνων πόλεων βελτιώνεται σε συνεχή ρυθμό λόγω των αυξανόμενων πλεονεκτημάτων που παρέχουν οι συνδεδεμένες συσκευές μέσω δικτύων, τα οποία επιτρέπουν τη σύνδεση των ανθρώπων και των συσκευών με τα δικά τους πλεονεκτήματα και μειονεκτήματα. Όπως ήδη αναφέρθηκε, οι συσκευές IoT έχουν αποδείξει τα οφέλη τους μέσα από τις αυξανόμενες απαιτήσεις τους και τις έξυπνες εφαρμογές τους σε διάφορους τομείς, από τα σπίτια έως τα γραφεία, την κυκλοφορία έως την υγεία, καλύπτοντας κάθε πτυχή της ζωής του ατόμου. Παράγοντες όπως η έλλειψη επαρκών πληροφοριών για την αίτηση συγκατάθεσης ιδιωτικών πληροφοριών και η έλλειψη δομών ασφαλείας στις συσκευές μπορούν να οδηγήσουν σε ζητήματα απειλών στην ασφάλεια δεδομένων, όπως η κατάχρηση δεδομένων, η άρνηση υπηρεσίας (DoS) και οι επιθέσεις man-in-the-middle.

Το μη ασφαλές λογισμικό των συσκευών IoT αυξάνει την πιθανότητα επιθέσεων στον κυβερνοχώρο σε αυτές τις συσκευές. Τα δεδομένα που λαμβάνονται από διάφορους αισθητήρες και συσκευές είναι σε διαφορετικές μορφές και πρέπει να υπάρχει μια τυποποιημένη πολιτική και πρωτόκολλο επικοινωνίας για τη διαλειτουργικότητα τους στο οικοσύστημα ασφάλειας. Η εύκολη πρόσβαση στα διαθέσιμα δεδομένα, σε συνδυασμό με πρόσθετες πληροφορίες μέσω των μέσων κοινωνικής δικτύωσης και των συσκευών IoT, μπορεί να οδηγήσει στην αποκάλυψη ιδιωτικών πληροφοριών. Η έλλειψη αυτοσχέδιων πολιτικών απορρήτου σύμφωνα με τις αυξανόμενες τάσεις στον κλάδο σχετικά με τον έλεγχο πρόσβασης, τη χρήση δεδομένων και την έκταση της χρήσης δεδομένων, συχνά προσελκύει εισβολείς για να διεισδύσουν εύκολα στα συστήματα. Κάθε πληροφορία που μπορεί να αποκαλύψει τα δεδομένα ταυτότητας οποιουδήποτε ατόμου, όταν ταυτοποιείται, πρέπει να προστατεύεται και να κρυπτογραφείται.



Εικόνα 1: Κατηγορία απειλών συσκευών IoT. Πηγή: Data Source International Data Corporation (2019)

Με τη γρήγορη και ενεργή ανάπτυξη του IoT, δεν αποτελεί έκπληξη η σημαντική αύξηση των επιθέσεων ασφαλείας που στοχεύουν συστήματα IoT. Γενικά, οι έξυπνες συσκευές IoT (π.χ. φορητές οθόνες υγείας, συνδεδεμένες συσκευές και οχήματα) φέρουν ευαίσθητες πληροφορίες. Έτσι, οποιεσδήποτε επιθέσεις στην ακεραιότητα, τη

διαθεσιμότητα ή την εμπιστευτικότητα των δεδομένων μπορούν να έχουν σοβαρό αντίκτυπο (π.χ. οικονομικές / ανθρώπινες απώλειες) στα θύματα αυτών των επιθέσεων. Οι επιτιθέμενοι μπορούν αρχικά να στοχεύσουν τεχνολογίες IoT (π.χ. αισθητήρες), ενσωματωμένες στο σύστημα (π.χ. ITS), με στόχο να υπονομεύσουν ολόκληρο το σύστημα. Η ασφάλεια αποτελεί κύριο μέλημα κάθε συστήματος, ωστόσο καθίσταται πιο κρίσιμη όταν εμπλέκονται ανθρώπινες ζωές, όπως στην περίπτωση των ITS. Λόγω της υψηλής προσβασιμότητας, της πολυπλοκότητας και της αλληλεξάρτησης των τεχνολογιών επικοινωνίας στα ITS, η πιθανότητα παραβιάσεων της ασφάλειας είναι υψηλή. Η ικανότητα εκτέλεσης επιτυχημένων επιθέσεων μπορεί να προκαλέσει σοβαρή ζημιά στο ITS.

Οι λειτουργίες των ITS ελέγχονται εξ ολοκλήρου από το ενσωματωμένο λογισμικό στο όχημα χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτό επιτρέπει στους επιτιθέμενους να ελέγχουν το όχημα εάν καταφέρουν να διεισδύσουν στο σύστημα ελάχιστα. Ως εκ τούτου, η κατανόηση των μοντέλων επίθεσης είναι ένα βήμα προς το σχεδιασμό αποτελεσματικών σχεδίων για την πρόβλεψη της συμπεριφοράς των επιτιθέμενων και την αντιμετώπιση των κακόβουλων δραστηριοτήτων τους.

Τα σύγχρονα συστήματα μεταφορών εξελίσσονται συνεχώς, αποφέροντας οφέλη βασιζόμενα στο «Intelligence» και τα πολλαπλά επίπεδα αυτονομίας. Καθώς τα συστήματα γίνονται πιο ανοιχτά και η τεχνολογία πιο περίπλοκη, οι επιθέσεις στην ασφάλεια, το απόρρητο και την εμπιστοσύνη γίνονται πιο εξελιγμένες. Ωστόσο, μερικές μελέτες έχουν επικεντρωθεί στην πληθώρα των ζητημάτων ασφάλειας στα ITS και τον μετριασμό τους.

Το Ευρωπαϊκό Συμβούλιο Ασφάλειας των Μεταφορών (European Transport Safety Council - ETSC) αναφέρει[2] ότι τα ITS επικεντρώνονται στην ανάπτυξη ψηφιακών τεχνολογιών (π.χ. ηλεκτρονικές μονάδες ελέγχου (Electronic Control Units - ECU), αισθητήρες κ.α.) για την προώθηση του «Intelligence» στα συστατικά στοιχεία των ITS. Παράλληλα, τα Συνεργατικά Έξυπνα Συστήματα Μεταφορών (C-ITS) επικεντρώνονται στην ανάπτυξη πρωτοκόλλων επικοινωνίας για την υποστήριξη αλληλεπιδράσεων μεταξύ των συνιστωσών ITS. Έτσι, ο στόχος του C-ITS είναι να επιτρέψει εφαρμογές που μπορούν να βελτιώσουν τη συνολική απόδοση των δικτύων οχημάτων. Προκειμένου να επιτευχθούν υψηλότερα επίπεδα διασυνδεσιμότητας μεταξύ των διαφόρων συνιστωσών ITS, τα οχήματα εξοπλίζονται με μια ποικιλία τεχνολογιών πληροφόρησης και επικοινωνίας. Αυτές περιλαμβάνουν τεχνολογίες ασύρματης επικοινωνίας, όπως Bluetooth, Wi-Fi, δορυφορικά συστήματα, 3G / 4G και πιο πρόσφατα, την 5η γενιά (5G). Ωστόσο, η χρήση τέτοιων στοιχείων για τεράστια συλλογή και διάδοση δεδομένων συνοδεύεται από ένα σύνολο προκλήσεων, ιδίως σε θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής. Τα σύγχρονα δίκτυα οχημάτων είναι ευάλωτα σε ένα ευρύ φάσμα απειλών για την ασφάλεια. Ένας εισβολέας μπορεί να εκμεταλλευτεί την έκθεση του συστήματος για να αποκτήσει πρόσβαση σε οχήματα και τελικά να τα ελέγξει. Αυτό μπορεί να οδηγήσει σε επικίνδυνες καταστάσεις οδήγησης προκαλώντας απειλητικές για τη ζωή συγκρούσεις.

Η ικανότητα εκτέλεσης μιας επιτυχημένης επίθεσης απαιτεί σε βάθος γνώση του στοχευμένου συστήματος. Το πρώτο βήμα για έναν εισβολέα θα ήταν να αξιολογήσει

[2] Brieng: Cooperative Intelligent Transport Systems (C-ITS), Eur. Transp. Saf. Council (ETSC), Brussels, Belgium, Nov. 2017 https://etsc.eu/wp-content/uploads/ETSC-Briefing-on-Cooperative-Intelligent-Transport-Systems-C-ITS.pdf

τις επιφάνειες επίθεσης για να αποκτήσει πρόσβαση και να παραδώσει κακόβουλη είσοδο στο σύστημα. Στη συνέχεια, ο εισβολέας πρέπει να αναζητήσει εκμεταλλεύσιμες ευπάθειες για τον έλεγχο του εξωτερικού και εσωτερικού δικτύου οχημάτων. Κατά συνέπεια, πρέπει να διασφαλίζεται η ασφάλεια για την καθιέρωση αξιόπιστων επικοινωνιών μεταξύ των διαφόρων συνιστωσών ITS.

Αναλύοντας τα πιθανά χαρακτηριστικά επίθεσης (π.χ. τη μέθοδο επίθεσης και το πεδίο επίθεσης) και τις αλληλεπιδράσεις των επιτιθέμενων με το σύστημα που δέχεται επίθεση (π.χ. ιδιότητα μέλους και κίνητρο), κατηγοριοποιούμε τους επιτιθέμενους σε διάφορες κατηγορίες.

Ενεργητικοί - Παθητικοί: Οι ενεργοί επιτιθέμενοι παράγουν πολλαπλά πακέτα για να μεταδοθούν σε άλλους κόμβους προκαλώντας επιβλαβείς επιπτώσεις στο δίκτυο. Γενικά, αυτοί οι επιτιθέμενοι έχουν την άδεια να λειτουργούν εντός του δικτύου. Οι παθητικοί επιτιθέμενοι έχουν τα αντίθετα χαρακτηριστικά συγκριτικά με τους ενεργητικούς. Προσπαθούν να παρακολουθούν σιωπηλά και να παρακολουθούν την κίνηση του δικτύου για να εξαγάγουν χρήσιμες πληροφορίες που μπορούν να χρησιμοποιηθούν για την προετοιμασία μελλοντικών επιθέσεων.

Εξωτερικοί - Εσωτερικοί: Οι εξωτερικοί επιτιθέμενοι διαπράττουν τις επιθέσεις τους εκτός του δικτύου. δεν είναι εξουσιοδοτημένοι να λειτουργούν στο δίκτυο. Γενικά, είναι περιορισμένοι όσον αφορά τις επιθέσεις που μπορούν να ξεκινήσουν. Πρέπει να παρακάμψουν με επιτυχία τις άμυνες του συστήματος, όπως τα τείχη προστασίας για να μπορούν να λειτουργούν μέσα στο δίκτυο. Αντίθετα, οι εσωτερικοί επιτιθέμενοι είναι κυρίως νόμιμα μέλη ή μέρος του δικτύου.

Τοπικοί - Εκτεταμένοι: Οι τοπικοί επιτιθέμενοι λειτουργούν εντός περιορισμένου πεδίου, στοχεύοντας μόνο κοντινά οχήματα ή RSU. Οι εκτεταμένοι επιτιθέμενοι επεκτείνουν το εύρος των επιθέσεών τους που μπορεί να εκτελεστεί από οπουδήποτε μέσω του internet.

Κακόβουλοι - Ορθολογικοί: Ο κύριος στόχος των κακόβουλων εισβολέων είναι να προκαλέσουν διακοπή και ζημιά στο δίκτυο χωρίς να εξετάσουν τις συνέπειες. Αυτού του είδους οι επιτιθέμενοι συνήθως δεν αναζητούν προσωπικά οφέλη από τις επιθέσεις τους. Από την άλλη πλευρά, οι ορθολογικοί επιτιθέμενοι μπορεί να είναι πιο επικίνδυνοι ξεκινώντας τις επιθέσεις τους με στόχο συγκεκριμένα θύματα για να προσελκύσουν την προσοχή και επίσης να μεγιστοποιήσουν τα οφέλη τους.

2.3 IoT & GDPR

Σύμφωνα με τις κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29, το IoT περιλαμβάνει εκτεταμένη επεξεργασία τεράστιου όγκου δεδομένων που συλλέγονται σε αναγνωρίσιμα φυσικά πρόσωπα μέσω αισθητήρων και επεξεργάζεται αυτά τα δεδομένα για την ανάλυση του περιβάλλοντος ή της συμπεριφοράς του ατόμου[3]. Αυτή η επεμβατική κατάρτιση προφίλ φυσικών προσώπων εντός του περιβάλλοντος του IoT αποσκοπεί στην παροχή εξατομικευμένων υπηρεσιών και εμπειριών στα πρόσωπα αυτά. Επιπλέον, πολλοί ενδιαφερόμενοι εμπλέκονται στην επεξεργασία αυτών των ογκωδών προσωπικών δεδομένων, συμπεριλαμβανομένων κατασκευαστών συσκευών - που μερικές φορές λειτουργούν επίσης ως πλατφόρμες δεδομένων, συλλέκτες

[3]https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

δεδομένων ή μεσίτες - προγραμματιστές εφαρμογών, κοινωνικές πλατφόρμες, ιδιοκτήτες συσκευών ή ενοικιαστές.

Τα σημαντικότερα ζητήματα μεταξύ του IoT και του GDPR αφορούν τη διαφάνεια, τη συγκατάθεση, την ιδιωτικότητα, τις διακρίσεις, και τις πολύπλοκες συμβατικές σχέσεις. Το IoT χαρακτηρίζεται από τη χρήση τεχνολογιών αναγνώρισης για τη συνεχή σύνδεση δεδομένων από τις συσκευές των ατόμων με τις μοναδικές τους ταυτότητες, εκτός από τη σύνδεση δεδομένων μεταξύ συσκευών και υπηρεσιών για την παροχή εξατομικευμένων υπηρεσιών. Τα φυσικά πρόσωπα ενδέχεται να μην ενημερώνονται σχετικά με αυτή τη συνεχή ταυτοποίηση και σύνδεση δεδομένων, όπως συμβαίνει δεδομένου ότι είναι δύσκολο να ληφθεί ρητή συγκατάθεση από το υποκείμενο των δεδομένων για κάθε συσκευή IoT συνδεδεμένη στο περιβάλλον IoT. Πέραν του ότι δεν γνωρίζουν τον τρόπο συλλογής, κοινοποίησης και περαιτέρω επεξεργασίας των προσωπικών τους δεδομένων από συσκευές του Διαδικτύου των πραγμάτων, τα υποκείμενα των δεδομένων ενδέχεται να μην ενημερώνονται σχετικά με πολλά ενδιαφερόμενα μέρη και τρίτους που εμπλέκονται στην επεξεργασία των προσωπικών τους δεδομένων και τους αποδέκτες στους οποίους μπορούν να κοινοποιηθούν δεδομένα προσωπικού χαρακτήρα. Αυτό το περίπλοκο σενάριο καθιστά δυσχερή για τους υπευθύνους επεξεργασίας τη συμμόρφωση με τις υποχρεώσεις που πρέπει να τηρούνται δυνάμει του ΓΚΠΔ όσον αφορά την ενημέρωση των υποκειμένων των δεδομένων σχετικά με τη συλλογή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, ενώ ενδέχεται να μην υπάρχει διαφάνεια όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, η οποία μπορεί να πραγματοποιείται μεταξύ των συσκευών του διαδικτύου των πραγμάτων ή των εμπλεκόμενων ενδιαφερόμενων μερών και αποδεκτών. Κατά συνέπεια, τα πρόσωπα στα οποία αναφέρονται τα δεδομένα δεν είναι σε θέση να δώσουν ελεύθερα τη «συγκεκριμένη, εν πλήρει επιγνώσει και σαφή» συγκατάθεσή τους «με δήλωση ή με σαφή θετική ενέργεια» δηλώνοντας τη συγκατάθεσή τους για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν γεγονός που καθιστά την επεξεργασία παράνομη των δεδομένων.

Το IoT χαρακτηρίζεται από τη συλλογή ογκωδών προσωπικών δεδομένων, η οποία πιθανότατα αποτελείται από περισσότερες πληροφορίες από ό, τι είναι απαραίτητο, από τα υποκείμενα των δεδομένων ή τους αισθητήρες σε συσκευές IoT με αυτοματοποιημένη επεμβατική παρακολούθηση της συμπεριφοράς των υποκειμένων των δεδομένων. Επιπλέον, οι υπεύθυνοι επεξεργασίας μπορούν να συνάγουν συμπεράσματα σχετικά με το υποκείμενο των δεδομένων τα οποία δεν σχετίζονται με τον σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα και τα οποία δεν γνωρίζει το υποκείμενο των δεδομένων. Ομοίως, τα τρίτα μέρη που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορούν να χρησιμοποιήσουν τα δεδομένα για άλλους σκοπούς τους οποίους δεν γνωρίζει το υποκείμενο των δεδομένων. Αυτό δεν συνάδει με την αρχή της ελαχιστοποίησης των δεδομένων του GDPR, η οποία ορίζει ότι τα δεδομένα πρέπει να είναι συναφή και να περιορίζονται σε ό, τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους συλλέγονται. Εάν οι ελεγκτές ελαχιστοποιήσουν την ποσότητα των προσωπικών δεδομένων που συλλέγονται από συσκευές IoT, θα συμμορφώνονται με τον GDPR, αλλά οι υπηρεσίες IoT δεν θα λειτουργούν σωστά, πράγμα που σημαίνει ότι το επιχειρηματικό μοντέλο για τη χρήση υπηρεσιών IoT δεν επαρκεί πλέον εάν ελαχιστοποιηθεί η συλλογή προσωπικών δεδομένων. Επιπλέον, η εξαγωγή συμπερασμάτων για σκοπούς άλλους από τον επιδιωκόμενο σκοπό συλλογής δεδομένων και χωρίς τη συγκατάθεση του υποκειμένου

των δεδομένων έρχεται σε σύγκρουση με την αρχή περιορισμού του σκοπού του GDPR.

Το IoT χαρακτηρίζεται επίσης από την εφαρμογή ανάλυσης μεγάλων δεδομένων και σύνθετων αλγορίθμων για την εξαγωγή επεμβατικών συμπερασμάτων προφίλ σχετικά με το υποκείμενο των δεδομένων, συνδέοντας σύνολα δεδομένων IoT ή συνδυάζοντας σύνολα δεδομένων που μοιράζονται τρίτα μέρη. Στην περίπτωση αυτή, οι υπεύθυνοι επεξεργασίας ενδέχεται να εισβάλουν στην ιδιωτική ζωή του υποκειμένου των δεδομένων συνδυάζοντας πολλαπλές κατηγορίες δεδομένων εν αγνοία του προσώπου στο οποίο αναφέρονται τα δεδομένα. Επιπλέον, τα συμπεράσματα που συνάγονται από το IoT για σκοπούς εξατομίκευσης ενδέχεται να οδηγήσουν σε δυσμενή μεταχείριση του υποκειμένου των δεδομένων. Εάν τα υποκείμενα των δεδομένων δεν γνωρίζουν την επεμβατική κατάρτιση προφίλ από τον υπεύθυνο επεξεργασίας και τρίτους, δεν θα μπορούν να ασκήσουν το δικαίωμά τους να μην υπόκεινται σε απόφαση βασιζόμενη αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία έχει νομικές και σημαντικές επιπτώσεις σε αυτά. Περαιτέρω συμπεράσματα τρίτων χωρίς ενημέρωση του υποκειμένου των δεδομένων θα προσκρούουν στο δικαίωμά τους, δυνάμει του ΓΚΠΔ, να ενημερώνονται σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, και σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται. Επιπλέον, η παροχή ουσιαστικών πληροφοριών σχετικά με τη λογική της ανάλυσης μαζικών δεδομένων και των πολύπλοκων αλγορίθμων στα υποκείμενα των δεδομένων για τη συμμόρφωση με τον ΓΚΠΔ ενδέχεται να μην αποτελεί απλή υποχρέωση εκπλήρωσης για τον υπεύθυνο επεξεργασίας. Επιπλέον, η εξατομίκευση που προκύπτει από συμπεράσματα δημιουργίας προφίλ IoT που οδηγούν σε διακριτική μεταχείριση του υποκειμένου των δεδομένων μπορεί να έρχεται σε σύγκρουση με την αρχή της δικαιοσύνης του GDPR.

Γενικά, προκειμένου να αυξηθεί η αποτελεσματικότητα της επικοινωνίας και της χρήσης των δεδομένων, το σύστημα IoT υιοθετεί συνήθως αυτόματη λειτουργία λήψης αποφάσεων που προσφέρει ευκολία στους χειριστές, αλλά μειώνει σχετικά τον βαθμό προσωπικού ελέγχου των δικών τους δεδομένων.

Για παράδειγμα, όταν τα άτομα χρησιμοποιούν δεδομένα όπως η διαχείριση αποθήκευσης τροφίμων οικιακών ψυγείων, οι ρυθμίσεις θερμοκρασίας κλιματισμού, τα αρχεία οδήγησης ή τα τέλη διοδίων, αυτά τα προσωπικά δεδομένα που συγκεντρώνονται από διαφορετικά συστήματα, είναι δυνατόν να δημιουργηθεί μια σχεδόν πλήρης εικόνα της ζωής αυτού του ατόμου με βάση αυτό. Εάν τα δεδομένα είναι ανεξέλεγκτα ή χρησιμοποιούνται καταχρηστικά, θα οδηγήσει σε αδικαιολόγητη παρέμβαση ή παραβίαση της ιδιωτικής ζωής.

Στην πραγματικότητα, εάν ξεκινήσουμε από την προστασία των προσωπικών δεδομένων, πρέπει να προσπαθήσουμε να διασφαλίσουμε ότι τα άτομα έχουν ανεξάρτητο έλεγχο των δεδομένων τους για τη συλλογή και τη χρήση προσωπικών δεδομένων, ώστε να αποφευχθεί η παραβίαση των δικαιωμάτων της προσωπικότητάς τους. Ταυτόχρονα, η χρήση μεμονωμένων δεδομένων πρέπει επίσης να περιορίζεται σε εύλογο εύρος. Κατά τη συλλογή ευαίσθητων προσωπικών δεδομένων χρηστών ή καταναλωτών, εκτός από τη ρητή συγκατάθεσή τους, τα δεδομένα θα πρέπει να προστατεύονται αποτελεσματικά.

Το δικαίωμα στην προστασία της ιδιωτικής ζωής των πληροφοριών αφορά τον αυτοέλεγχο των προσωπικών πληροφοριών. Ο στόχος είναι να διασφαλιστεί ότι τα άτομα έχουν την αυτονομία να καθορίσουν εάν θέλουν να αποκαλύψουν τις προσωπικές τους πληροφορίες και, εάν ναι, σε ποιο βαθμό, πότε, πώς και σε ποιον θα κοινοποιηθούν. Είναι επίσης σημαντικό να διασφαλίζεται το δικαίωμα των πολιτών να κατανοούν και να διαχειρίζονται τη χρήση των προσωπικών τους δεδομένων, συμπεριλαμβανομένης της δυνατότητας διόρθωσης τυχόν ανακριβειών στις πληροφορίες τους.

2.4 ITS & Έξυπνες Πόλεις

Πολλές αναπτυσσόμενες χώρες, επενδύουν ένα τεράστιο χρηματικό ποσό για να μετατρέψουν τις παλιές υπάρχουσες πόλεις τους σε σύγχρονες έξυπνες πόλεις. Ένα έξυπνο σύστημα μεταφορών αποτελεί αναπόσπαστο μέρος αυτού του σχεδιασμού. Η πρόοδος στο Διαδίκτυο των Πραγμάτων (IoT) και στις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ) διαδραματίζει κρίσιμο ρόλο στην ανάπτυξη έξυπνων πόλεων. Η έννοια της έξυπνης πόλης συνδυάζει ΤΠΕ και IoT για να βελτιώσει την αποτελεσματικότητα των υπηρεσιών πόλης, ενώ παράλληλα τις συνδέει με τους κατοίκους. Διευκολύνει την επικοινωνία μεταξύ του απασχολούμενου εργατικού δυναμικού στην έξυπνη πόλη, του κοινού που αλληλοεπιδρά με το IoT περιβάλλον, καθώς και τις ίδιες τις υποδομές, προκειμένου να παρακολουθούνται οι πόλεις για την επίτευξη των στόχων που έχουν θέσει στην ποιότητα και τη διαδραστικότητα των υπηρεσιών που προσφέρονται με τη βοήθεια του IoT.

Η στάθμευση οχημάτων είναι επίσης ένα ακόμη σημαντικό πρόβλημα που θα κληθούν να αντιμετωπίσουν πολλές έξυπνες πόλεις. Επειδή οι περισσότερες σημερινές έξυπνες πόλεις εκσυγχρονίστηκαν μέσα από το μοντέλο των παραδοσιακών πόλεων, είναι σύνηθες να έχουν περιορισμένη διαθεσιμότητα οδικού δικτύου και να μην μπορούν να χειριστούν τον τεράστιο αριθμό οχημάτων. Ως αποτέλεσμα, η εύρεση μιας θέσης στάθμευσης την κατάλληλη στιγμή και στη σωστή τοποθεσία έχει γίνει δυσεπίλυτο πρόβλημα για τους ανθρώπους παγκοσμίως. Ωστόσο, η εύρεση του σωστού μέρους για τη στάθμευση των οχημάτων μπορεί επίσης να οδηγήσει σε σπατάλη χρόνου και περισσότερη κατανάλωση ρυπογόνων καυσίμων. Η εκ των προτέρων ενημέρωση σχετικά με τη διαθεσιμότητα της πληρότητας στάθμευσης και τους βέλτιστους διαθέσιμους τρόπους μετακίνησης προς το σημείο, διαδραματίζει κρίσιμο ρόλο στη διασφάλιση ότι οι μετακινούμενοι θα έχουν ένα ασφαλές και άνετο ταξίδι. Διευκολύνει επίσης τη διαχείριση του κέρδους των υπηρεσιών για τους παρόχους χώρων στάθμευσης ενώ ταυτόχρονα βοηθά στον αποτελεσματικό έλεγχο της ρύπανσης στις έξυπνες πόλεις ρυθμίζοντας την κυκλοφοριακή συμφόρηση μειώνοντας το χρόνο των μετακινήσεων.

Ο σχεδιασμός και ο προγραμματισμός έξυπνων μεταφορών, οι έξυπνες κοινότητες, οι έξυπνες πόλεις, τα έξυπνα συστήματα ελέγχου και άλλοι τομείς που έχουν ενσωματωθεί στο οικοσύστημα του IoT, χρησιμοποιούν τεχνικές ανάλυσης μαζικών δεδομένων. Ένα μοντέλο για την αξιολόγηση των δεδομένων μεταφοράς είναι η χρήση πλαισίου ανοιχτού κώδικα για αρχιτεκτονικές μεγάλων δεδομένων το οποίο προτείνεται για το χειρισμό δεδομένων μεταφοράς σε πραγματικό χρόνο. Κάθε πλαίσιο περιέχει ένα εκτεταμένο οικοσύστημα τεχνολογιών ανοιχτού κώδικα που προετοιμάζει, επεξεργάζεται, διαχειρίζεται και αναλύει σύνολα μαζικών δεδομένων. Η προτεινόμενη υλοποίηση δοκιμάζεται χρησιμοποιώντας δεδομένα μεταφοράς από διάφορες αξιόπιστες πηγές που επεξεργάζονται μεγάλους όγκους δεδομένων και διανέμοντας τα

σε πραγματικό χρόνο στους πολίτες το συντομότερο δυνατό. Η επικοινωνία μεταξύ οχημάτων και η επικοινωνία μεταξύ οχημάτων και υποδομών διαδραματίζουν σημαντικό ρόλο στις έξυπνες μεταφορές. Αυτές οι τεχνικές δημιουργούν τα βασικά θεμέλια για αυτόνομα οχήματα για μελλοντικές έξυπνες πόλεις.

Ένα αποκεντρωμένο σύστημα διαχείρισης δεδομένων για έξυπνες και ασφαλείς μεταφορές είναι σχεδιασμένο για την αντιμετώπιση του προβλήματος ευπάθειας των δεδομένων, αξιοποιώντας το blockchain και το Διαδίκτυο των Πραγμάτων σε ένα βιώσιμο πλαίσιο έξυπνης πόλης. Τα ηλεκτρικά οχήματα (EVs) προβλέπεται να χρησιμοποιηθούν ευρέως σε προσωπικούς, επιχειρηματικούς και δημόσιους στόλους σε αστικές πόλεις στο μέλλον. Η δημοτικότητα των ηλεκτρικών οχημάτων θα επηρεάσει σημαντικά τη μακροπρόθεσμη βιωσιμότητα και την οικονομική ευημερία της των σύγχρονων αστικών κέντρων.

Οι έξυπνες πόλεις πρέπει να έχουν τρία βασικά χαρακτηριστικά που μπορεί να παρέχει το IoT: Ευφυΐα, Διασύνδεση/Διαλειτουργικότητα και Ενοργάνιση των διασυνδεδεμένων συσκευών (Intelligence, Interconnection and Instrumentation). Το IoT ως τεχνολογία θα συμπληρώσει την εξέλιξη των ITS έχοντας ως πλεονέκτημα την επικοινωνία μεταξύ συσκευών όπως hardware με τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (RFID), συσκευές που με τεχνολογία αισθητήρων, συστήματα εντοπισμού θέσης και αναδυόμενες τεχνολογίες για τη συλλογή πληροφοριών σχετικά με τις κυκλοφοριακές συνθήκες, τα ατυχήματα στις μεταφορές, τις επισκευές δρόμων ή τη διαθεσιμότητα για χώρους προσωρινής τοποθέτησης ιδιόκτητων οχημάτων. Το IoT, όταν είναι πλήρως λειτουργικό και ικανό να αξιοποιήσει τις δυνατότητές του, θα είναι ο συνδετικός κρίκος όλου του οικοσυστήματος των έξυπνων μεταφορών με επίκεντρο την τεχνητή νοημοσύνη, συμπεριλαμβανομένων των CAVs, PAVS και όλων των τρόπων λειτουργίας που λειτουργούν με MaaS γενικά, συμπεριλαμβανομένων των μετακινούμενων που δεν χρησιμοποιούν κανενός τύπου όχημα.

Τα αυτοοδηγούμενα αυτοκίνητα ή τα αυτόνομα οχήματα αποτελούν επίσης μέρος αυτού του σύγχρονου μοντέλου μεταφορών. Το Διαδίκτυο των Πραγμάτων (IoT), η Τεχνολογία Πληροφοριών και Επικοινωνιών (ΤΠΕ), το Παγκόσμιο Συστήμα Εντοπισμού Θέσης (GPS) συμβάλλουν όλα στην ανάπτυξη αυτής της τεχνολογίας αυτόνομων οχημάτων. Οι εξελίξεις σε αυτούς τους τομείς καθιστούν τους ελιγμούς του αυτόνομου οχήματος ευκολότερους και ακριβέστερους. Η υιοθέτηση ηλεκτρικών οχημάτων και η μετατροπή των υπαρχόντων βενζινοκίνητων οχημάτων σε ηλεκτρικά οχήματα διαδραματίζουν επίσης κρίσιμο ρόλο στο μελλοντικό σύστημα μεταφορών. Οι έξυπνες πόλεις έπρεπε επίσης να σχεδιάσουν ανάλογα και να κάνουν τις κατάλληλες ρυθμίσεις για τη βιωσιμότητα αυτού του νέου μοντέλου μεταφορών όπως για παράδειγμα με την πρόβλεψη δημιουργία σταθμών για τη φόρτιση ηλεκτρικών οχημάτων.

2.5 Τεχνολογίες Επικοινωνίας Οχημάτων V2V, V2X, V2I, V2P, V2N

Οι περιπτώσεις χρήσης επικοινωνίας οχημάτων ταξινομούνται σε τέσσερις κατηγορίες: Το V2X αναφέρεται σε επικοινωνίες οχήματος προς όχημα (V2V), οχήματος προς υποδομή (V2I), οχήματος προς πεζό (V2P) και οχήματος προς δίκτυο (V2N). Οι επικοινωνίες V2V και V2P πραγματοποιούνται κυρίως μεταξύ αυτοκινήτων ή οχημάτων και ανεπαρκώς προστατευόμενων χρηστών του οδικού δικτύου (π.χ. πεζών και ποδηλάτων) για τη μετάδοση πληροφοριών θέσης, ταχύτητας και κατεύθυνσης για την αποτροπή ατυχημάτων.

Το V2P (Vehicle-to-Pedestrian) αναφέρεται στην άμεση επικοινωνία μεταξύ ενός οχήματος και μιας ή περισσότερων ευάλωτων ομάδων μεταφοράς. Οι ευάλωτες ομάδες μεταφορών καλύπτουν ένα ευρύ φάσμα χρηστών του οδικού δικτύου, όπως γυναίκες με παιδικά καροτσάκια, παιδιά που πηγαίνουν στο σχολείο, επιβάτες που επιβιβάζονται και αποβιβάζονται από οχήματα, ποδηλάτες κ.λπ. Μέσω της επικοινωνίας V2P, οι οδηγοί και οι ευάλωτοι χρήστες της κυκλοφορίας μπορούν να ανιχνεύουν και να ειδοποιούν ο ένας τον άλλον με όφελος την αποτροπή πιθανών συγκρούσεων και σοβαρών ατυχημάτων.

Το V2N (Vehicle-to-Network) αναφέρεται στη σύνδεση μεταξύ οχημάτων και πλατφορμών cloud μέσω του δικτύου πρόσβασης και του κεντρικού δικτύου. Η πλατφόρμα cloud αλληλεπιδρά με το όχημα, αποθηκεύει και επεξεργάζεται τα ληφθέντα δεδομένα και παρέχει διάφορες υπηρεσίες εφαρμογών για το όχημα.

Η άμεση σύνδεση μεταξύ αυτοκινήτων και οδικών υποδομών, όπως οι οδικές μονάδες (RSU), αποτελεί μέρος του V2I. Το RSU λειτουργεί ως κόμβος προώθησης για τη διεύρυνση του εύρους των επικοινωνιών που λαμβάνονται από ένα όχημα. Η μετάδοση V2N πραγματοποιείται μεταξύ ενός οχήματος και ενός διακομιστή εφαρμογών V2X, επιτρέποντας υπηρεσίες όπως ψυχαγωγία, ροή, βίντεο και σύνδεση για δυναμική διαχείριση διαδρομής. Η χρήση ασύρματου δικτύου, η άμεση επικοινωνία μεταξύ δύο αυτοκινήτων ή μεταξύ οχήματος και παρόδιας υποδομής μπορεί να αυξήσει την ασφάλεια και την κινητικότητα των οδηγών. Οι εφαρμογές περιλαμβάνουν συνεργατική βοήθεια οδήγησης, αποκεντρωμένα οχήματα ανίχνευσης και επικοινωνίες χρηστών και πληροφοριών. Για παράδειγμα, με την τεχνολογία αυτή, τα αυτοκίνητα μπορούν να εκπέμπουν προειδοποίηση σε άλλα οχήματα για την αποτροπή ατυχημάτων κατά την αλλαγή λωρίδας. Η επικοινωνία οχημάτων, η οποία συνδέει αυτοκίνητα, οδικές μονάδες και πεζούς, είναι μια ζωτικής σημασίας τεχνολογία στο Ευφυές Σύστημα Μεταφορών (ITS).

Οι επικοινωνίες οχήματος προς οτιδήποτε (V2X) ασχολούνται με την ανταλλαγή πληροφοριών μεταξύ ενός οχήματος και πολλών τμημάτων του ευφυούς συστήματος μεταφορών (ITS), όπως άλλα αυτοκίνητα, πεζοί, πύλες Διαδικτύου και υποδομές μεταφορών (όπως φανάρια και πινακίδες). Η τεχνολογία έχει τη δυνατότητα να επιτρέψει ένα ευρύ φάσμα μοναδικών εφαρμογών σε τομείς όπως η οδική ασφάλεια, η ψυχαγωγία των επιβατών, οι υπηρεσίες κατασκευαστών αυτοκινήτων και η αποδοτικότητα της κυκλοφορίας των οχημάτων. Οι επικοινωνίες V2X βασίζονται πλέον σε μία από τις δύο βασικές τεχνολογίες: τις αποκλειστικές επικοινωνίες μικρής εμβέλειας (DSRC) και τα κυψελοειδή δίκτυα. Ωστόσο, δεν προβλέπεται ότι μια ενιαία τεχνολογία θα είναι σε θέση να χειριστεί ένα τόσο ευρύ φάσμα προβλεπόμενων εφαρμογών V2X για σημαντικό αριθμό αυτοκινήτων στο εγγύς μέλλον. Ως αποτέλεσμα, συνιστάται η διαλειτουργικότητα μεταξύ DSRC και τεχνολογιών κυψελοειδούς δικτύου για αποτελεσματικές επικοινωνίες V2X.

Στην εποχή των προηγμένων δικτύων 5^{ης} γενιάς και πέραν αυτών, η επικοινωνία οχημάτων όχι μόνο αξιοποιεί τα πλεονεκτήματα του μεγάλου εύρους ζώνης, της χαμηλής καθυστέρησης και της υψηλής αξιοπιστίας, αλλά περιλαμβάνει επίσης πολλές προηγμένες τεχνολογίες, όπως το edge computing και ο τεμαχισμός δικτύου. Οι υπηρεσίες cloud διανέμονται σε πλατφόρμες edge computing μέσω slice δικτύου, γεγονός που όχι μόνο διασφαλίζει την ασφάλεια των δεδομένων αλλά και μειώνει την καθυστέρηση επεξεργασίας δεδομένων.

Η εμφάνιση του Mobile Edge Computing (MEC) επιτρέπει στους χειριστές και σε τρίτους να αναπτύσσουν υπηρεσίες κοντά στους χρήστες, γεγονός που μειώνει αποτελεσματικά τον λανθάνοντα χρόνο και βελτιώνει την αποδοτικότητα των υπηρεσιών. Το 2014, το ETSI (Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων) ίδρυσε το Mobile Edge Computing Industry Specification Group για την τυποποίηση του MEC[4]. Σε σύγκριση με το cloud computing, το MEC επιλύει προβλήματα όπως η μεγάλη καθυστέρηση, η υπερφόρτωση του συστήματος λόγω του τεράστιου όγκου δεδομένων και μπορεί να υποστηρίξει καλύτερα υπηρεσίες με υψηλές απαιτήσεις σε πραγματικό χρόνο. Ωστόσο, το V2X πρέπει να υποστηρίζει μεγάλο αριθμό κόμβων V2X, συμπεριλαμβανομένων οχημάτων, πεζών και υποδομών. Ως εκ τούτου, οι απαιτήσεις μετάδοσης δεδομένων των κόμβων αυξάνουν σημαντικά το φορτίο του δικτύου και θέτουν υψηλότερες απαιτήσεις για εύρος ζώνης και καθυστέρηση επικοινωνίας.

2.6 Επικοινωνία οχήματος με όχημα (V2V)

Το V2V (Vehicle-to-Vehicle) αναφέρεται στην ανταλλαγή δεδομένων και πληροφοριών μεταξύ οχημάτων. Το όχημα μπορεί να κρίνει τις συνθήκες του δρόμου ανταλλάσσοντας πληροφορίες τοποθεσίας και ταχύτητας με κοντινά οχήματα σε πραγματικό χρόνο. Επιπλέον, μπορεί να δημιουργηθεί ένα διαδραστικό δίκτυο μεταξύ οχημάτων για την ανταλλαγή πληροφοριών φωνής, κειμένου και βίντεο.

Η επικοινωνία μεταξύ οχημάτων δίνει τη δυνατότητα ανταλλαγής δεδομένων σε πραγματικό χρόνο, όπως η τρέχουσα ταχύτητα του, ο προορισμός και η πορεία που πρόκειται να ακολουθήσει το κάθε όχημα. Για την επίτευξη του στόχου είναι απαραίτητο να είναι εγκατεστημένα τα κατάλληλα εργαλεία λογισμικού που θα διαχειρίζονται την ανταλλαγή των δεδομένων, διασφαλίζοντας ότι θα παραμένουν ασφαλή από πιθανές απειλές. Ο οδηγός ειδοποιείται με μηνύματα για τον απαραίτητο έλεγχο της κίνησης του οχήματος μεταφέροντας πληροφορίες σχετικές με την κυκλοφορία, τις καιρικές συνθήκες, τις ενδεχόμενες απειλές για την αποφυγή ατυχημάτων. Με τη βοήθεια της επικοινωνίας μεταξύ οχημάτων και των αισθητήρων που είναι τοποθετημένοι σε διάφορα σημεία του οδικού δικτύου, επιτυγχάνεται η ελαχιστοποίηση των τροχαίων ατυχημάτων και ενισχύεται η οδική ασφάλεια.

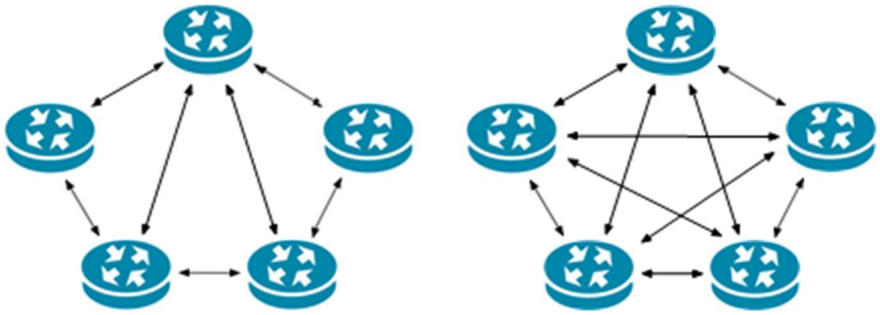
Ο ρόλος του IoT είναι ο συντονισμός των διαφόρων συσκευών και η σύνδεση τους με αισθητήρες μέσω ασύρματης σύνδεσης δικτύου. Η έξυπνη πόλη, που χρησιμοποιεί εργαλεία IoT έχει διάφορα οφέλη, όπως ο προσανατολισμός προς τον χρήστη χρησιμοποιώντας δεδομένα που συλλέγονται από αισθητήρες, όπως ο αισθητήρας μέτρησης του ποσοστού του αλκοόλ, ο μετατροπέας μέτρησης κραδασμών, το επιταχυνσιόμετρο, τα οποία συνδέονται με συσκευές IoT για την πρόληψη ατυχημάτων στον αυτοκινητόδρομο. Για παράδειγμα η διαδικασία που ακολουθείται κατά την αλλαγή λωρίδας σε ένα αυτόνομο όχημα για την αποφυγή μίας σύγκρουσης, είναι η μετακίνηση του σε άλλη λωρίδα όταν είναι διαθέσιμες οι απαιτούμενες αποστάσεις μεταξύ του οχήματος που πραγματοποιεί την αλλαγή και του γύρω περιβάλλοντος του, λαμβάνοντας υπόψη τα δεδομένα που αλλάζουν δυναμικά καθ΄ όλη τη διάρκεια της διαδικασίας ώστε να αποφευχθεί η σύγκρουση.

[4] https://www.etsi.org/newsroom/news/852-2014-12-news-new-etsi-mobile-edge-computing-industry-specification-group-starts-work

Η εξοικονόμηση καυσίμων αποτελεί κρίσιμο παράγοντα λόγω της αύξησης των τιμών των ορυκτών καυσίμων και των εκπομπών αερίων του θερμοκηπίου. Οι αισθητήρες που ανταλλάσσουν δεδομένα επικοινωνίας μεταξύ οχημάτων, παρέχουν πληροφορίες που βοηθούν στην εξοικονόμηση καυσίμου όπως για παράδειγμα αναλύοντας γεωλογικά δεδομένα, όπως η ταχύτητα του ανέμου, η κλίση του δρόμου που βοηθούν στη δυναμική λήψη αποφάσεων. Οι αισθητήρες των οχημάτων επίσης ανταλλάσσουν δεδομένα με τις υποδομές που υποστηρίζουν ένα ITS, για να γνωρίζει τις τρέχουσες κυκλοφοριακές συνθήκες και να προσαρμόζει τις πιθανές διαδρομές των οχημάτων με γνώμονα τη μείωση του ενεργειακού κόστους.

Η βιώσιμη ανάπτυξη είναι ο κύριος στόχος των σύγχρονων τεχνολογιών και το έργο της έξυπνης πόλης δημιουργεί έναν τρόπο για τους ανθρώπους να βελτιώνουν τη ποιότητα της ζωής τους στο διαθέσιμο αστικό περιβάλλον. Η εξισορρόπηση των πόρων στις ψηφιακές πόλεις ενισχύεται από τον κατάλληλο χειρισμό όλων των διαθέσιμων δεδομένων που έχουν συλλεχθεί. Οι δημόσιες συγκοινωνίες ειδικότερα είναι βιώσιμες για όλη τη κοινωνία αντλώντας παραδείγματα από τις ποικίλες εφαρμογές που παρέχει ένα ολοκληρωμένο ITS, όπως η μείωση της χρονικής καθυστέρησης των μέσων μαζικής μεταφοράς λόγω της κυκλοφοριακής συμφόρησης. Έτσι με αυτό το τρόπο αυξάνεται η εμπιστοσύνη των μετακινούμενων που χρησιμοποιούν τα δημόσια οχήματα για τις συνήθεις μετακινήσεις τους με αποτέλεσμα σταδιακά όλο και περισσότερος πληθυσμός να επιλέγει τις δημόσιες συγκοινωνίες από τα ιδιόκτητα οχήματα.

Η τεχνολογία V2V αποτελείται από ασύρματες μεταδόσεις δεδομένων μεταξύ μηχανοκίνητων οχημάτων. Πρωταρχικός στόχος είναι η πρόληψη πιθανών ατυχημάτων, επιτρέποντας στα διερχόμενα οχήματα να διαβιβάζουν δεδομένα σχετικά με τη θέση και την ταχύτητά τους εντός ενός ad hoc δικτύου πλέγματος. Το τελευταίο χρησιμοποιεί ένα αποκεντρωμένο σύστημα σύνδεσης, το οποίο μπορεί να παρέχει είτε μια πλήρως συνδεδεμένη τοπολογία πλέγματος είτε μια μερικώς συνδεδεμένη τοπολογία πλέγματος.



Εικόνα 2 Μερικώς συνδεδεμένη τοπολογία & Πλήρως συνδεδεμένη τοπολογία πλέγματος

Στην πρώτη περίπτωση, κάθε κόμβος συνδέεται απευθείας με άλλους στο δίκτυο. Στη δεύτερη περίπτωση, ορισμένοι κόμβοι μπορούν να συνδεθούν με όλους τους άλλους, ενώ οι υπόλοιποι συνδέονται μόνο με εκείνους με τους οποίους ανταλλάσσουν συχνά τα περισσότερα δεδομένα. Με την εκμετάλλευση αυτής της τοπολογίας δικτύου, οι κόμβοι ενός δικτύου πλέγματος μπορούν να ανταλλάσσουν μηνύματα και πληροφορίες

με γειτονικούς κόμβους στους οποίους συνδέονται απευθείας ή μπορούν να επιλέξουν μία από τις διαφορετικές διαθέσιμες διαδρομές για να φτάσουν στον προορισμό. Σε περίπτωση διακοπής ή προσωρινής δυσλειτουργίας ενός κόμβου, οι διαδρομές υπολογίζονται εκ νέου για να φτάσουν σε όλους τους προορισμούς.

Σήμερα με την υπάρχουσα τεχνολογία η ασφάλεια εξαρτάται εξ ολοκλήρου από τη λειτουργικότητα των αισθητήρων, των καμερών και των ραντάρ του οχήματος. Το σύστημα αντιδρά σε τυχόν επικίνδυνες καταστάσεις με βάση συγκεκριμένες παραμέτρους που ανιχνεύονται από αυτές τις συσκευές που έχουν εγκατασταθεί στο όχημα. Συνήθως, οι κύριες εξεταζόμενες παράμετροι είναι η ταχύτητα, η απόσταση από ένα εμπόδιο ή η παρουσία ενός οχήματος σε τυφλό σημείο. Ωστόσο, αν και οι χρησιμοποιούμενες τεχνολογίες είναι όλο και πιο αξιόπιστες, τα σφάλματα υπολογισμού δεν πρέπει να υποτιμώνται. Αντίθετα, τα πρωτόκολλα επικοινωνίας V2V θα βελτιώσουν την απόδοση στον τομέα της ασφάλειας, καθώς, όταν όλα τα οχήματα αλληλεπιδρούν μεταξύ τους, αυτό θα βοηθήσει το αυτοκίνητο που κινδυνεύει να αναλάβει μια πιο αποτελεσματική επιλογή για την επίλυση του προβλήματος. Επομένως, ο πρωταρχικός σκοπός κάθε κόμβου που αποτελεί μέρος του δικτύου πλέγματος θα είναι η συλλογή δεδομένων για την εγγύηση της ασφάλειας για τον εαυτό του και των γύρων του.

Τα νέα ευφυή συστήματα μεταφορών (ITS) θα χρησιμοποιούν δεδομένα από την επικοινωνία V2V για την ενίσχυση της διαχείρισης της κυκλοφορίας, επιτρέποντας στα οχήματα να επικοινωνούν επίσης με οδικές υποδομές, όπως φώτα ή πινακίδες. Οι τεχνολογίες αυτές θα μπορούσαν να καταστούν υποχρεωτικές στο όχι και τόσο μακρινό μέλλον και να συμβάλουν στην κατασκευή πιο αξιόπιστων αυτόνομων οχημάτων στους αυτοκινητόδρομους. Ωστόσο, η εφαρμογή των επικοινωνιών V2V και ενός ευφυούς συστήματος μεταφορών παρουσιάζει τρία κύρια εμπόδια: την ανάγκη να συμφωνήσουν οι κατασκευαστές αυτοκινήτων με τους κανόνες ασφάλειας και λειτουργίας· την εγγύηση της ιδιωτικής ζωής και της εμπιστευτικότητας των δεδομένων που διαβιβάζονται σε ραδιοτηλεοπτική μετάδοση και πολλαπλή μετάδοση· την αναγκαία χρηματοδότηση για την ανάπτυξη και τη διάδοση όλων των τεχνολογιών.

2.7 Επικοινωνία οχήματος προς Υποδομή (V2I)

Το V2I (Vehicle-to-Infrastructure) αναφέρεται στην επικοινωνία μεταξύ ευφυών οχημάτων και υποδομών, όπως RSU, φανάρια και κάμερες. Αφενός, οι παρόδιες υποδομές μπορούν να παρακολουθούν τις οδικές συνθήκες και να λαμβάνουν σχετικές πληροφορίες για οχήματα από κοντινές περιοχές. Από την άλλη, η οδική υποδομή δημοσιεύει πληροφορίες σε πραγματικό χρόνο για να καθοδηγήσει τα οχήματα να επιλέξουν τη βέλτιστη διαδρομή. Ως εκ τούτου, το V2I χρησιμοποιείται ευρέως στην παρακολούθηση και διαχείριση οχημάτων, υπηρεσίες κυκλοφορίας σε πραγματικό χρόνο.

Μια οδική μονάδα (RSU) αποτελεί ουσιαστικό στοιχείο των συνδεδεμένων οχημάτων και των ευφυών συστημάτων μεταφορών (ITS). Οι RSU τοποθετούνται συχνά σε διασταυρώσεις ή στις πλευρές των οδών. Ο κύριος στόχος μιας RSU είναι να καταστήσει δυνατή την επικοινωνία των οχημάτων μεταξύ τους και με τη γύρω υποδομή. Χρησιμοποιούνται για τη διαχείριση της κυκλοφορίας, τις εφαρμογές ασφάλειας, τον συντονισμό των σημάτων κυκλοφορίας, την παρακολούθηση των

υποδομών, τις υπηρεσίες έκτακτης ανάγκης, τις υπηρεσίες πληροφοριών κυκλοφορίας, την περιβαλλοντική παρακολούθηση και την οδική διαφήμιση. Οι RSU συλλέγουν, επεξεργάζονται και μεταδίδουν δεδομένα από οχήματα, επιτρέποντας καλύτερη διαχείριση της κυκλοφορίας, ασφάλεια και συνολική αποδοτικότητα των μεταφορών.

Οι RSU μπορούν να μεταδώσουν πληροφορίες σχετικά με την ασφάλεια σε κοντινά οχήματα, να βελτιστοποιήσουν το χρονισμό των σημάτων κυκλοφορίας και να παρέχουν ενημερώσεις και προτάσεις διαδρομής σε πραγματικό χρόνο. Τα RSU προσφέρουν επίσης περιβαλλοντική παρακολούθηση μέσω αισθητήρων, επιτρέποντας τον περιβαλλοντικό σχεδιασμό και διαχείριση. Συνοπτικά, τα RSU αποτελούν βασικά συστατικά των έξυπνων και συνδεδεμένων συστημάτων μεταφορών, με στόχο τη βελτίωση της οδικής ασφάλειας και τη μείωση της κυκλοφοριακής συμφόρησης.

Επιπλέον, η επικοινωνία V2I μπορεί να χρησιμοποιηθεί για την ανταλλαγή δεδομένων ταχύτητας, γωνίας κατεύθυνσης, θέσης, κατεύθυνσης ή κατάστασης πέδησης με άλλα γύρω οχήματα, όπου τα οχήματα λήψης θα συγκεντρώνουν αυτά τα μηνύματα και θα λαμβάνουν έξυπνες αποφάσεις χρησιμοποιώντας ενσωματωμένες εφαρμογές που θα προειδοποιούν τους οδηγούς για ατυχήματα, υπερβολική ταχύτητα, καθυστέρηση στη ροή της κυκλοφορίας, επικίνδυνη οδήγηση ή τυφλά σημεία στο οδικό δίκτυο.

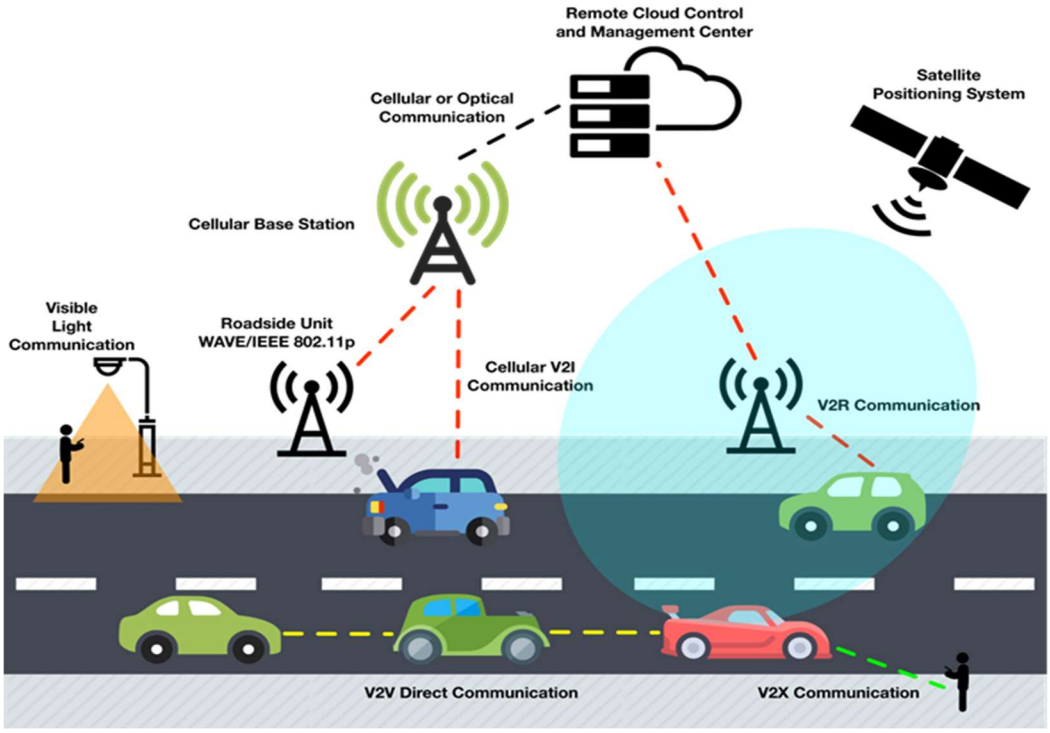
Μια έξυπνη πόλη χρησιμοποιεί πολλές ηλεκτρονικές συσκευές και αισθητήρες για τη συλλογή πληροφοριών από διάφορους κόμβους. Το σύστημα μεταφορών μπορεί να επικοινωνήσει με διαφόρων ειδών υποδομές που είναι διαθέσιμες στο έργο της ψηφιακής πόλης. Ο κοινωνικός μετασχηματισμός πραγματοποιείται μέσω του έργου έξυπνης πόλης και της λειτουργίας ασύρματης τεχνολογίας κινητών τηλεπικοινωνιών πέμπτης γενιάς 5G. Η εφαρμογή του δικτύου 5G εξαρτάται από τα χαρακτηριστικά του πληθυσμού και τον οικονομικό πλούτο της χώρας καθώς αποτελεί μια ιδιαίτερα δαπανηρή επένδυση. Ο τομέας της αυτοκινητοβιομηχανίας κινείται επίσης προς την κατεύθυνση της χρησιμοποίησης τεχνολογιών που σχετίζονται με έξυπνα συστήματα μεταφοράς, με τα σύγχρονα συνδεδεμένα οχήματα να λαμβάνουν και να μεταδίδουν πληροφορίες από το περιβάλλον τους στοχεύοντας στη βέλτιστη λειτουργία όπως η ευκολότερη πρόσβαση για ένα όχημα διάσωσης ή ασθενοφόρο που έχει τις απαραίτητες πληροφορίες. Η κυκλοφοριακή συμφόρηση, η ρύπανση, η ορθή εκμετάλλευση των υποδομών, η ζήτηση ενέργειας μειώνονται και η κινητικότητα και η ασφάλεια αυξάνονται από τις σύγχρονες καινοτομίες στα συνδεδεμένα οχήματα. Η ανταλλαγή δεδομένων μεταξύ οχημάτων ή μεταξύ οχημάτων και υποδομών είναι ουσιαστικής σημασίας σε έργα έξυπνης διαχείρισης δεδομένων και ο λόγος της προόδου είναι οι σύγχρονες τεχνολογίες επικοινωνιών όπως το 4G και το 5G που επιτρέπουν στα οχήματα χωρίς οδηγό να συνδέονται με χιλιάδες κόμβους δικτύου, γειτονικά αυτοκίνητα και ηλεκτρονικές συσκευές στην άκρη του δρόμου.

Σε αντίθεση με το μοντέλο επικοινωνίας V2V, το οποίο επιτρέπει την ανταλλαγή πληροφοριών μόνο μεταξύ οχημάτων, το V2I επιτρέπει στα διερχόμενα οχήματα να διασυνδέονται με το οδικό σύστημα. Αυτά τα στοιχεία περιλαμβάνουν αναγνώστες RFID, φανάρια, κάμερες, δείκτες λωρίδας, λάμπες φωτισμού, σήμανση και παρκόμετρα. Συνήθως, οι επικοινωνίες V2I είναι ασύρματες, αμφίδρομες και παρόμοιες με τις V2V, χρησιμοποιώντας αποκλειστικές συχνότητες επικοινωνίας μικρής εμβέλειας (Dedicated Short-Range Communication, DSRC) για τη μεταφορά

δεδομένων. Οι πληροφορίες αυτές αποστέλλονται από τα στοιχεία της υποδομής στο όχημα, ή αντιστρόφως, μέσω ενός ad hoc δικτύου. Στο ITS, οι αισθητήρες V2I μπορούν να αποκτήσουν δεδομένα υποδομής και να παρέχουν στους ταξιδιώτες συμβουλές σε πραγματικό χρόνο, στέλνοντας πληροφορίες σχετικά με τις οδικές συνθήκες, την κυκλοφοριακή συμφόρηση, τα ατυχήματα στο οδόστρωμα, την παρουσία εργοταξίων και τη διαθεσιμότητα θέσεων στάθμευσης. Ομοίως, τα συστήματα εποπτείας και διαχείρισης της κυκλοφορίας μπορούν να χρησιμοποιήσουν τα δεδομένα που συλλέγονται από την υποδομή και τα οχήματα για να ορίσουν μεταβλητά όρια ταχύτητας για να επιτύχουν εξοικονόμηση καυσίμου και να διευκολύνουν τις ροές κυκλοφορίας. Το υλικό, το λογισμικό και το firmware που καθιστούν την επικοινωνία μεταξύ οχημάτων και υποδομών εφαρμόσιμη, αποτελούν θεμελιώδες σημείο εκκίνησης για την ανάπτυξη αυτόνομων αυτοκινήτων.

2.8 Επικοινωνία οχήματος προς Όλα (V2X)

Τα μοντέλα επικοινωνίας V2V και V2I που αναφέρονται παραπάνω ολοκληρώνονται στο V2X, το οποίο αντιπροσωπεύει μια γενίκευση. Το τελευταίο συνίσταται στη μεταφορά δεδομένων από ένα όχημα σε οποιαδήποτε οντότητα που μπορεί να την επηρεάσει, ή το αντίστροφο, και ενσωματώνει άλλους πιο συγκεκριμένους τύπους επικοινωνίας, όπως όχημα προς πεζό (V2P), όχημα προς οντότητα στην άκρη του δρόμου (V2R) και όχημα προς συσκευή (V2D).



Εικόνα 3 Επικοινωνίες V2V, V2I & V2X

Σύμφωνα με την έκθεση για την παγκόσμια κατάσταση της οδικής ασφάλειας, υπάρχουν περίπου 1,25 εκατομμύρια άνθρωποι χάνουν τη ζωή τους εξαιτίας τροχαίων

ατυχημάτων κάθε χρόνο σε όλο τον κόσμο. Σχεδόν τα μισά από τα θύματα αναγνωρίστηκαν ως πεζοί, ποδηλάτες και μοτοσικλετιστές, οι οποίοι ορίζονται συλλογικά ως Ευάλωτοι Χρήστες του Οδικού Δικτύου (Vulnerable Road Users, VRU). Είναι χρήσιμο να σημειωθεί ότι τα ελαττώματα στο σχεδιασμό του δρόμου και η έλλειψη κατάλληλων διαχωρισμάτων για κάθε κατηγορία μετακινούμενου από την κυκλοφορία, επηρεάζουν σημαντικά τη δημιουργία ενός μη ασφαλούς περιβάλλοντος για τους οδηγούς και τους πεζούς. Ένα άλλο ζήτημα που δεν πρέπει να υποτιμάται, ειδικά στα αστικά κέντρα, είναι η απόσπαση της προσοχής των πεζών, που προκαλείται από τη χρήση των ακουστικών και των smartphones τους, που συχνά αντιμετωπίζονται ενώ περπατούν στο δρόμο. Ως εκ τούτου, είναι απαραίτητο να αναπτυχθεί ένα σύστημα προειδοποίησης και για τους πεζούς.

Ένας από τους κύριους σκοπούς της τεχνολογίας V2X είναι ακριβώς η υποστήριξη των πιθανών και αποτελεσματικών μηχανισμών επικοινωνίας μεταξύ οχημάτων και πεζών με στόχο τον περιορισμό των ατυχημάτων, μερικές φορές θανατηφόρων. Πρόσφατα, προς αυτή την κατεύθυνση, αναπτύχθηκε το Pedestrian Collision Warning (PCW), το οποίο μπορεί να εξασκήσει ασύρματες μονάδες που περιλαμβάνονται σε κινητά τηλέφωνα, όπως Wi-Fi, Bluetooth και Επικοινωνία Κοντινού Πεδίου (NFC).

Η τεχνολογία Vehicle-to-Everything ή Vehicle-to-X (V2X) επιτρέπει στα AV να επικοινωνούν με το περιβάλλον τους και κάνει την οδήγηση ασφαλέστερη και αποδοτικότερη για όλους. Η τεχνολογία V2X αποτελείται από V2V (όχημα προς όχημα), V2I (όχημα προς υποδομή), V2P (όχημα προς πεζό) και V2N (όχημα προς δίκτυο). Το V2V αναφέρεται στην άμεση επικοινωνία μεταξύ οχημάτων, το V2I είναι η σύνδεση μεταξύ οχημάτων και υποδομών, το V2P είναι η αμοιβαία επικοινωνία μεταξύ οχημάτων και πεζών ή άλλων ευάλωτων χρηστών του οδικού δικτύου όπως οι ποδηλάτες και το V2N συνδέει τα οχήματα στο Διαδίκτυο. Τα ad-hoc δίκτυα οχημάτων (VANETs), τα οποία αποτελούν ειδική κατηγορία κινητών ad hoc δικτύων (MANETs), αποτελούν τομέα σημαντικού ενδιαφέροντος των επικοινωνιών V2X. Το VANET είναι ένας συνδυασμός ασύρματου ad-hoc δικτύου και κυψελοειδούς τεχνολογίας που αποδίδει ένα ευφυές σύστημα μεταφορών (ITS) μεταξύ οχήματος προς όχημα και οχήματος προς οδικές μονάδες (RSU)[5]. Χρησιμοποιεί αποκλειστικές επικοινωνίες μικρής εμβέλειας (DSRC) που βασίζονται στο πρότυπο IEEE 802.11p για ασύρματη πρόσβαση σε περιβάλλοντα οχημάτων. Η τεχνολογία DSRC υποστηρίζει μια σύντομη ανταλλαγή πληροφοριών μεταξύ συσκευών που χρησιμοποιούν αποκλειστικές επικοινωνίες μικρής εμβέλειας (DSRC), όπως On-Board Units (OBUs) εξοπλισμένες στο εσωτερικό του οχήματος, RSU και κινητές συσκευές που μεταφέρονται από πεζούς. Η RSU επικοινωνεί με διακομιστές τοποθεσίας μέσω ενσύρματου/ασύρματου δικτύου για την παρακολούθηση πληροφοριών σε όλα τα οχήματα. Η υποδομή υπηρεσιών μιας RSU περιλαμβάνει το σύστημα διαχείρισης της κυκλοφορίας, την υποδομή δημόσιου κλειδιού και το κέντρο διαχείρισης της RSU[6].

Το δίκτυο κινητής τηλεφωνίας είναι μια άλλη δομή επικοινωνίας που απαιτείται για το V2X. Τον Ιούνιο του 2017, ο οργανισμός κινητής βιομηχανίας 3GPP[7] τυποποίησε ένα

[5] P. Mutalik and V. C. Patil, "A survey on vehicular ad-hoc network [VANET's] protocols for improving safety in urban cities," in Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon), Aug. 2017, pp. 840–845.

[6] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," Comput. Secur., vol. 103, Apr. 2021, Art. no. 102150.

[7] 3GPP. (2017). Release 14. [Online]. Available: https://www. 3gpp.org/release-14

σύνολο τεχνολογιών, γνωστό ως Cellular Vehicle-to-Everything (C-V2X), ειδικά σχεδιασμένο για να επιτρέπει την επικοινωνία μεταξύ AV και οδικής υποδομής.

Το Cellular Vehicle-to-Everything (C-V2X) είναι μια τεχνολογία ασύρματης επικοινωνίας που επιτρέπει στα οχήματα να επικοινωνούν μεταξύ τους, με πεζούς και με τη γύρω υποδομή χρησιμοποιώντας το κυψελοειδές δίκτυο. Το C-V2X έχει σχεδιαστεί για να βελτιώνει την οδική ασφάλεια, να μειώνει την κυκλοφοριακή συμφόρηση και να ενισχύει την αποτελεσματικότητα του συστήματος μεταφορών.

Βασισμένο σε δίκτυα LTE, το C-V2X παρέχει μία λύση για ολοκληρωμένη άμεση επικοινωνία (V2V, V2I και V2P) με επικοινωνία δικτύου (V2N) αξιοποιώντας την υπάρχουσα υποδομή κυψελοειδούς δικτύου. Το C-V2X μπορεί να υποστηρίξει ένα ευρύτερο φάσμα δυνατοτήτων από προηγούμενες αποκλειστικές λύσεις συνδεσιμότητας οχημάτων που βασίζονται στο 802.11p. Υποστηρίζει μεταδόσεις μικρής και μεγάλης εμβέλειας και επιτρέπει εξαιρετικά αξιόπιστη επικοινωνία σε πραγματικό χρόνο σε υψηλές ταχύτητες και σε κυκλοφορία υψηλής πυκνότητας. Στη λειτουργία επικοινωνίας V2V, V2I και V2P, το C-V2X λειτουργεί στη ζώνη συχνοτήτων των 5,9 GHz και λειτουργεί ανεξάρτητα από τα κυψελοειδή δίκτυα. Χρησιμοποιεί το GNSS ως κύρια πηγή συγχρονισμού χρόνου σε σενάρια εκτός κάλυψης. Στη λειτουργία επικοινωνίας δικτύου, το C-V2X χρησιμοποιεί το συμβατικό δίκτυο κινητής τηλεφωνίας για να επιτρέψει στο όχημα να λαμβάνει πληροφορίες σχετικά με τις οδικές συνθήκες και την κυκλοφορία στην περιοχή. Πρόσφατα, η 3GPP άρχισε να βελτιώνει το C-V2X με διάφορους τρόπους προς τις προδιαγραφές 5G New Radio (NR) V2X στην έκδοση 16[8] και μετά.

Το C-V2X μπορεί να ενισχύσει τις δυνατότητες λήψης αποφάσεων των αυτόνομων οχημάτων, να ενσωματωθεί με έξυπνα συστήματα μεταφορών, έξυπνες υποδομές και άλλες λύσεις αστικής κινητικότητας για να επιτρέψει την απρόσκοπτη επικοινωνία και συντονισμό. Αυτή η ενσωμάτωση μπορεί να βελτιώσει τη διαχείριση της κυκλοφορίας, τις δημόσιες συγκοινωνίες, την αντιμετώπιση καταστάσεων έκτακτης ανάγκης και τη συνολική ποιότητα ζωής στις πόλεις.

Έχει πραγματοποιηθεί εκτενής έρευνα από τη βιομηχανία και άλλους φορείς για την διάδοση των δυνατοτήτων επικοινωνίας οχημάτων και των υποδομών μεταφορών. Σύμφωνα με το 3GPP, καθορίζονται τέσσερις κατηγορίες περιπτώσεων χρήσης επικοινωνίας οχημάτων: Επικοινωνία Οχημάτων προς οχήματα (V2V), Επικοινωνία Οχημάτων προς Υποδομή (V2I), Επικοινωνία Οχημάτων προς Πεζούς (V2P) και Επικοινωνία Οχημάτων προς Δίκτυο (V2N), το σύνολο των παραπάνω συνηθίζεται να αναφέρεται ως V2X δηλαδή επικοινωνία οχημάτων με τα πάντα. Οι επικοινωνίες V2V και V2P εστιάζουν ουσιαστικά στην αλληλεπίδραση μεταξύ οχημάτων ή μεταξύ οχημάτων και ευάλωτων χρηστών του οδικού δικτύου, όπως πεζοί ή ποδηλάτες, προκειμένου να παρέχουν πληροφορίες σχετικά με την θέση, την ταχύτητα και άλλες αναγκαίες πληροφορίες για την αποφυγή ατυχημάτων. Το V2I αναφέρεται στην άμεση επικοινωνία μεταξύ οχημάτων και των υποδομών του οδικού δικτύου, όπως οι μονάδες εδάφους (RSU). Οι RSU χρησιμοποιούνται για τη μετάδοση μηνυμάτων και τη διεύρυνση του εύρους επικοινωνίας των οχημάτων, ενεργώντας ως κόμβοι προώθησης. Η μετάδοση V2N διευκολύνει την επικοινωνία μεταξύ ενός οχήματος και ενός διακομιστή εφαρμογών V2X, υποστηρίζοντας υπηρεσίες όπως το streaming για ψυχαγωγία και η συνδεσιμότητα για δυναμική διαχείριση διαδρομών.

[8] 3GPP. (2020). Release 16. [Online]. Available: https://www. 3gpp.org/release-16

Για να καταστεί δυνατή η ασύρματη επικοινωνία μεταξύ οχημάτων (V2V) και Οχήματος προς υποδομή(V2I) (γνωστή ως «V2X»), υπάρχουν μέχρι στιγμής δύο κύριες μέθοδοι επικοινωνίας V2X: Dedicated Short-Range Communication (DSRC) και η κυψελοειδής επικοινωνία οχημάτων. Το DSRC παρέχει εύρος επικοινωνίας από 100 έως 1000 m, με ρυθμό επικοινωνίας δεδομένων περίπου 27 Mbps. Το DSRC απαιτεί χαμηλό λανθάνοντα χρόνο και υψηλό ρυθμό δεδομένων για την υποστήριξη της επικοινωνίας εξ αποστάσεως. Στο ITS, το DSRC βασίζεται στο επίπεδο πρόσβασης όπως περιγράφεται στο πρότυπο IEEE 802.11P. Η κατανομή φάσματος για το DSRC είναι από 5,85 GHz έως 5,925 GHz, όπως καθορίζεται από την Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) των Ηνωμένων Πολιτειών (ΗΠΑ) και την Ευρωπαϊκή Επιτροπή Ηλεκτρονικών Επικοινωνιών (ECC). Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) και το ETSI κατακερμάτισαν τη ζώνη DSRC σε επτά διαφορετικά κανάλια 10 MHz το καθένα. Μεταξύ των επτά καναλιών, υπάρχει ένα κανάλι ελέγχου και έξι κανάλια εξυπηρέτησης. Τα κανάλια εξυπηρέτησης χρησιμοποιούνται για τη μετάδοση δεδομένων, ενώ το κανάλι ελέγχου χρησιμοποιείται για τη ρύθμιση των υπηρεσιών και των εφαρμογών που επιδιώκονται στα κανάλια εξυπηρέτησης.

Η επικοινωνία που βασίζεται σε DSRC / WAVE είναι πιο αξιόπιστη όταν το μήνυμα πρέπει να παραδοθεί σε κοντινή απόσταση με αυστηρές απαιτήσεις καθυστέρησης και αυστηρά πρωτόκολλα ασφαλείας. Αντίθετα , τα κυψελοειδή δίκτυα παρέχουν υψηλό εύρος ζώνης δικτύου. Επιπλέον, τα κυψελοειδή δίκτυα αυξάνουν επίσης το εύρος μετάδοσης των κόμβων VANET. Το DSRC αδυνατεί να υποστηρίξει μεγάλο εύρος ζώνης και εύρος μετάδοσης, ενώ τα κυψελοειδή δίκτυα (3G, LTE και LTE- A) υποφέρουν από υψηλό λανθάνοντα χρόνο που αποτελεί πρόκληση για εφαρμογές ασφάλειας και πραγματικού χρόνου όπως η επικοινωνία σε αυτόνομα αυτοκίνητα.

Από την άλλη, το 3GPP συνεχίζει να αναπτύσσει κυψελοειδείς επικοινωνίες οχημάτων, γνωστές και ως Cellular Vehicle-to-Everything (C-V2X), με στόχο τη λειτουργία κυψελοειδών δικτύων όπως το Long Term Evolution (LTE) και το 5G New Radio (5G NR) που μπορούν να προσφέρουν υπηρεσίες υψηλού ρυθμού δεδομένων και ευρεία κάλυψη. Και οι δύο τεχνολογίες V2X έχουν τα δικά τους πλεονεκτήματα και περιορισμούς όταν χρησιμοποιούνται σε περιβάλλον οχημάτων. Ως αποτέλεσμα, έχει προταθεί η ενσωμάτωσή τους σε ετερογενή δίκτυα οχημάτων για την εκμετάλλευση των μοναδικών πλεονεκτημάτων τους, αντιμετωπίζοντας παράλληλα τα μεμονωμένα μειονεκτήματά τους.

Τα διαθέσιμα πρότυπα για το VANET (IEEE 802.11p /DSRC) έχουν εγγενείς ελλείψεις όσον αφορά την αναποτελεσματική χρήση της ζώνης 5,9 GHz, τη μικρή εμβέλεια επικοινωνίας, την επιβάρυνση/καθυστέρηση λόγω κεντρικής ασφάλειας και αναποτελεσματικών πρωτοκόλλων εκπομπής και αναγνώρισης. Οι επικοινωνίες συσκευής προς συσκευή (D2D) και τα δίκτυα 5G, αντιμετωπίζουν αυτές τις ελλείψεις. Το D2D επιτρέπει την άμεση ανακάλυψη υπηρεσιών και επικοινωνίας μεταξύ των χρηστών που βρίσκονται σε κοντινή απόσταση. Μέχρι στιγμής, μπορεί να επιτρέψει άμεσες επικοινωνίες V2V και V2I χωρίς να διασχίσει την κυψελοειδή υποδομή και την παραδοσιακή κυψελοειδή (δηλ. Uplink/downlink) επικοινωνία. Ως εκ τούτου, η μετάδοση οχημάτων που βασίζεται σε D2D μπορεί να είναι χρήσιμη σε εφαρμογές οχημάτων κρίσιμης σημασίας, επειδή μπορεί να επιτύχει υψηλή φασματική απόδοση, υψηλό ρυθμό δεδομένων, χαμηλή ισχύ μετάδοσης και χαμηλό λανθάνοντα χρόνο.

Η συνεχής πρόοδος στον τομέα της πληροφορικής και των ασύρματων επικοινωνιών έχουν δώσει κίνητρα και πολλές νέες δυνατότητες που δεν υπήρχαν στο παρελθόν, ώστε οι αυτοκινητοβιομηχανίες να οραματίζονται την κατασκευή αυτόνομων οχημάτων. Τα οχήματα αυτά, γνωστά ως αυτόνομα οχήματα (Autonomous Vehicles, AVs), διαθέτουν ενσωματωμένους αισθητήρες με κύριο χαρακτηριστικό την αποτύπωση του περιβάλλον τους για πλοήγηση, ενώ αντικαθιστούν τον ανθρώπινο παράγοντα σε όλες τις λειτουργιές του οχήματος για την οδήγηση του. Οι προβλέψεις εκτιμούν ότι οι πωλήσεις των AVs θα υπερβούν τα 33 εκατομμύρια ετησίως έως το 2040, καθορίζοντας το ποσοστό της αυτόνομης κινητικότητας σε περισσότερο από το 26% των πωλήσεων νέων αυτοκινήτων[9].

2.9 Internet of Vehicles (IoV)

Το IoV είναι ένα κατανεμημένο δίκτυο που υποστηρίζει τη χρήση δεδομένων που δημιουργούνται από συνδεδεμένα αυτοκίνητα και ad hoc δίκτυα οχημάτων (VANET)[10]. Το IoV επιτρέπει την επικοινωνία μεταξύ διαφορετικών αισθητήρων και ECU μέσα στο όχημα για την παροχή αυτόνομης οδήγησης, πληροφοριών, και υπηρεσιών ψυχαγωγίας.

Το Internet of Vehicles (IoV) είναι μια αναπτυσσόμενη τεχνολογία από την εφεύρεση των έξυπνων οχημάτων που περιέχουν συνδεδεμένους αισθητήρες και ηλεκτρονικές μονάδες ελέγχου (ECU). Αυτές οι συσκευές ενισχύουν τον πολυαναμενόμενο στόχο της αυτόνομης οδήγησης. Ταυτόχρονα, η ασύρματη επικοινωνία έχει ανοίξει το δρόμο για ταχύτερη μεταφορά δεδομένων, μεγαλύτερη αξιοπιστία, χαμηλότερη καθυστέρηση και διαθεσιμότητα. Αυτές οι βελτιώσεις στην ασύρματη επικοινωνία υιοθετούνται από διαφορετικά πρωτόκολλα και εφαρμογές στο IoV. Σε γενικές γραμμές, το IoV είναι η συγχώνευση των Vehicular Ad Hoc Networks (VANET) με το Internet of Things (IoT)[11]. Σήμερα, τα συνδεδεμένα οχήματα αξιοποιούν το IoT για να συνδεθούν σε δίκτυα και να επωφεληθούν από πληροφορίες κυκλοφορίας σε πραγματικό χρόνο και πλοήγηση. Σύμφωνα με την Gartner, το 5G IoT θα είναι η πρωτοποριακή τεχνολογία επικοινωνίας για συνδεδεμένα αυτοκίνητα. Η Gartner δηλώνει επίσης ότι μέχρι το 2030, ένα μεγάλο ποσοστό των ευκαιριών της αγοράς για το 5G IoT θα αφιερωθεί στην αυτοκινητοβιομηχανία, καθώς τα συνδεδεμένα αυτοκίνητα θα καταλαμβάνουν περίπου το 53% των συνολικών σημείων πρόσβασης 5G IoT[12].

Το IoV υποστηρίζει πέντε τύπους επικοινωνίας δικτύου:

Συστήματα εντός του οχήματος που παρακολουθούν την εσωτερική απόδοση του οχήματος μέσω εποχούμενων μονάδων (OBU).

Συστήματα οχήματος προς όχημα (V2V) που υποστηρίζουν την ασύρματη ανταλλαγή πληροφοριών σχετικά με την ταχύτητα και τη θέση των γύρω οχημάτων.

---

[9] IHS Markit—Autonomous Vehicle Sales to Surpass 33 Million Annually in 2040, Enabling New Autonomous Mobility in More Than 26% of New Car Sales. 2018. Available online: https://ihsmarkit.com/research-analysis/autonomous-vehicle-sales-to- surpass-33-million-annually-in-2040-enabling-new-autonomous-mobility-in-more-than-26-percent-of-new-car-sales.html.

[10] http://www.eitc.org/research-opportunities/new-media-and-new-digital-economy/future-data-center-and-networking-architecture/the-internet-of-vehicles/the-internet-of-vehicles

[11] A. Dureja, S. Sangwan, A review: Efficient transportation—Future aspects of IoV, Evolving Technologies for Computing, Communication and Smart World (2021) 97–108.

[12] https://www.gartner.com/en/newsroom/press-releases/2019-10-17-gartner-predicts-outdoor-surveillance-cameras-will-be

Συστήματα οχήματος προς υποδομή (V2I) που υποστηρίζουν την ασύρματη ανταλλαγή πληροφοριών μεταξύ ενός οχήματος και υποστηρικτικών οδικών μονάδων (RSU).

Συστήματα Vehicle to Cloud (V2C) που επιτρέπουν στο όχημα να έχει πρόσβαση σε πρόσθετες πληροφορίες από το διαδίκτυο μέσω διεπαφών προγράμματος εφαρμογών (API).

Συστήματα οχήματος προς πεζό (V2P) που υποστηρίζουν την ευαισθητοποίηση για τους ευάλωτους χρήστες του οδικού δικτύου, όπως οι πεζοί και οι ποδηλάτες.

Στο πλαίσιο του 5G και των ευφυών συστημάτων μεταφορών (ITS), οι πέντε τύποι δικτύων που αναφέρονται παραπάνω αναφέρονται μερικές φορές ως επικοινωνία οχήματος προς όλα (V2X).

Το IoV εκμεταλλεύεται πολλές τεχνολογίες δικτύωσης για να παρέχει συνδεσιμότητα μεταξύ διαφόρων μονάδων μέσα στο όχημα, καθώς και επικοινωνία μεταξύ διαφορετικών οδικών οντοτήτων (π.χ. άλλα οχήματα και οδικές υποδομές) για να επωφεληθεί από την έξυπνη ανταλλαγή δεδομένων και την απόκτηση έτσι κρίσιμων πληροφοριών. Ωστόσο, η συνδεσιμότητα μέσω του δικτύου ενέχει πάντα τους κινδύνους της, ειδικά επειδή το δίκτυο IoV περιέχει αρκετούς αισθητήρες και επεξεργαστές IoT. Επιπλέον, η συνεχής επικοινωνία μεταξύ οδικών φορέων παράλληλα με το δίκτυο, καθιστά το IoV ανοιχτό στόχο για εισβολείς. Η ασφάλεια του IoV είναι ένα σοβαρό ζήτημα, καθώς μπορεί να προκαλέσει ανθρώπινο θάνατο εάν εσφαλμένες πληροφορίες παρεμβαίνουν στη λήψη αποφάσεων των οχημάτων. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τα τρωτά σημεία στην επικοινωνία δικτύωσης και να εκτελέσουν κακόβουλες δραστηριότητες, όπως η ανάληψη του ελέγχου του αυτοκινήτου, η μετάδοση παραπλανητικών πληροφοριών στο δίκτυο ή άλλες επιθέσεις που μπορούν να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος του οχήματος, καθώς και την αυθεντικότητα των χρηστών. Για παράδειγμα, μια επίθεση που πραγματοποιήθηκε από μια ομάδα χάκερ ήταν σε θέση να ξεγελάσει το λογισμικό αυτόνομης οδήγησης Autopilot της Tesla ώστε να παρεκκλίνει σε μια λωρίδα κυκλοφορίας στο αντίθετο ρεύμα κυκλοφορίας[13]. Επιπλέον, η αυτόνομη οδήγηση παρέχει έναν τεράστιο όγκο δεδομένων, τα οποία χρησιμοποιούνται για εφαρμογές με δυνατότητα τεχνητής νοημοσύνης (AI) και σκοπούς εξόρυξης δεδομένων. Το απόρρητο των δεδομένων των χρηστών θα μπορούσε να τεθεί σε κίνδυνο λόγω της ευαισθησίας των δεδομένων που μοιράζονται μεταξύ των χρηστών.

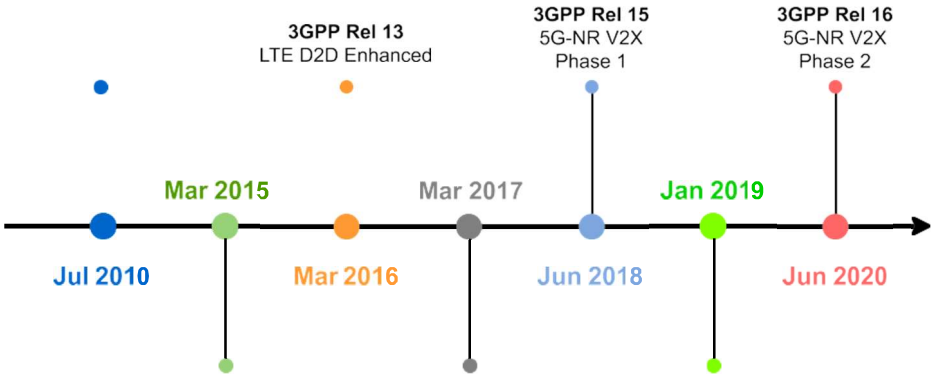
2.10 Περιπτώσεις Χρήσης 5G-V2X

Η τεχνολογία 5G αντανακλά τις προσδοκίες για την υλοποίηση των AV καθώς η επικοινωνία χιλιάδων αυτοκινήτων ταυτόχρονα μπορεί να υλοποιηθεί με τον διαμοιρασμό δεδομένων σε πραγματικό χρόνο από τους εγκατεστημένους αισθητήρες που είναι διασκορπισμένοι σε σημεία του οδικού δικτύου και διάφορες άλλες συσκευές. Η εξυπηρέτηση των τεράστιων αναγκών για το πλήθος των διασυνδεδεμένων συσκευών υλοποιείται με την υπηρεσία Massive Machine-Type Communications (mMTC), η οποία έχει σχεδιαστεί για τον σκοπό αυτό.

Η έκδοση 3GPP 12 ήταν το πρώτο πρότυπο που εισήγαγε άμεσες επικοινωνίες συσκευής προς συσκευή (D2D) χρησιμοποιώντας κυψελοειδείς τεχνολογίες για υπηρεσίες εγγύτητας (proximity services - ProSe). Το LTE V2X αναπτύχθηκε υπό την έκδοση 14 και ενισχύθηκε περαιτέρω στην έκδοση 15 (γνωστό ως LTE-eV2X) με

[13] https://www.cnbc.com/2019/04/03/chinese-hackers-tricked-teslas-autopilot-into-switching-lanes.html

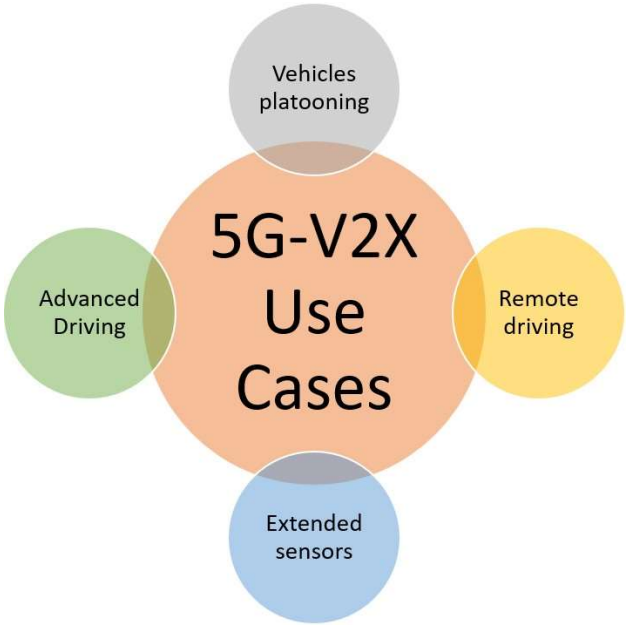
κύρια χαρακτηριστικά την υψηλότερη αξιοπιστία χαμηλού λανθάνοντος χρόνου και τους υψηλότερους ρυθμούς μετάδοσης δεδομένων. Η τεχνολογία 5G New Radio (5G NR) V2X κυκλοφόρησε επίσης στην έκδοση 15, που ανακοινώθηκε το 2019, για την υποστήριξη προηγμένων υπηρεσιών V2X, όπως η φάλαγγα οχημάτων, προηγμένη υποβοήθηση οδηγού και η δυνατότητα απομακρυσμένης οδήγησης. Στην έκδοση 16, το 3GPP ανακοίνωσε τη δεύτερη φάση του 5G NR, η οποία σκοπεύει να βελτιώσει την εξαιρετικά αξιόπιστη επικοινωνία χαμηλού λανθάνοντος χρόνου (URLLC).



Εικόνα 4: Εξέλιξη των επικοινωνιών V2X μέχρι 2020

Το 3GPP[14] καθορίζει τις απαιτήσεις απόδοσης για βελτιωμένα σενάρια V2X με βάση διαφορετικά επίπεδα αυτοματισμού οχημάτων. Μερικές από αυτές τις προηγμένες εφαρμογές περιλαμβάνουν το vehicle platooning, remote driving, advanced driving και extended sensors.

[14] Το 3rd Generation Partnership Project (3GPP) ενώνει επτά οργανισμούς ανάπτυξης τηλεπικοινωνιακών προτύπων (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), γνωστούς ως «Organizational Partners» παρέχοντας στα μέλη τους ένα σταθερό περιβάλλον για την παραγωγή των Αναφορών και των Προδιαγραφών που ορίζει τις τεχνολογίες 3GPP. https://www.3gpp.org/about-us/introducing-3gpp



Εικόνα 5: Περιπτώσεις χρήσης V2X λαμβάνοντας υπόψη διαφορετικά επίπεδα αυτοματισμού οχημάτων

2.11 Διμοιρία Οχημάτων (Vehicle Platooning)

Η πλοήγηση οχημάτων σε ευθυγράμμιση διατηρώντας μικρές αποστάσεις μεταξύ τους στους αυτοκινητόδρομους ονομάζεται φάλαγγα οχημάτων. Το όχημα στο μπροστινό μέρος της φάλαγγας ελέγχει την ταχύτητα, στη συνέχεια, τα ακόλουθα οχήματα δημιουργούν μια ευθεία γραμμή πίσω από το πρώτο όχημα και οδηγούν μόνα τους με ασφάλεια σε κοντινή απόσταση στον αυτοκινητόδρομο. Το platooning παρέχει την δυνατότητα σχηματισμού μιας συντονισμένης ομάδας οχημάτων με κύριο χαρακτηριστικό την διατήρηση μικρών αποστάσεων μεταξύ των οχημάτων, δημιουργώντας με αυτόν το τρόπο περισσότερο διαθέσιμο χώρο στο οδικό δίκτυο, καλύτερη διαχείριση των καυσίμων με οφέλη για το περιβάλλον. Παράλληλα η μείωση της απόσπασης των οδηγών από άλλες δραστηριότητες επιτυγχάνει την μείωση των τροχαίων ατυχημάτων. Όλα τα οχήματα της διμοιρίας ανταλλάσσουν περιοδικά πληροφορίες με το προπορευόμενο όχημα και εκτελούν τις απαιτούμενες ενέργειες που απαιτούνται για τη διατήρηση του σωστού σχηματισμού. Όλα τα οχήματα σε μια διμοιρία έχουν τη δυνατότητα να μπορούν να κινούνται αυτόνομα. Για την σωστή λειτουργία του vehicle platooning πρέπει να υποστηρίζονται αξιόπιστες επικοινωνίες V2V:

Είσοδος και έξοδος από τη διμοιρία: Κάθε όχημα θα μπορεί να ενταχθεί ή να αποχωρήσει από μια διμοιρία ανά πάσα στιγμή, ενώ η διμοιρία είναι ενεργή, υποστηρίζοντας πληροφόρηση με μηνύματα/σήματα για την ολοκλήρωση της ενέργειας ενσωμάτωσης ή αποχώρησης από τη διμοιρία.

Ενημέρωση και ειδοποίηση: Όλα τα οχήματα σε διμοιρία είναι ενημερωμένα ανά πάσα στιγμή για τον σχηματισμό της. Αυτό διευκολύνει την ομαλή λειτουργία της ένταξης ή της αποχώρησης από μια διμοιρία, καθώς το όχημα που επιθυμεί να ενταχθεί στη διμοιρία θα μπορεί να το κάνει χωρίς να την διαταράσσει.

Μηνύματα διαχείρισης: Επιτρέπει τη λειτουργία οχημάτων σε σταθερή κατάσταση σε μια διμοιρία με την ανταλλαγή μηνυμάτων διαχείρισης, συμπεριλαμβανομένης της επιτάχυνσης, του φρεναρίσματος, της επιλογής διαδρομής, της αλλαγής του προπορευόμενου οχήματος κ.λπ.

Βασικό στοιχείο για την ομαλή και απρόσκοπτη λειτουργία της διμοιρίας οχημάτων είναι η ανταλλαγή των πληροφοριών ανάμεσα στη διμοιρία να έχει κύρια χαρακτηριστικά την αξιοπιστία και την ασφάλεια, ώστε να μπορεί να υποστηρίξει την εκτέλεση των διαδρομών σε υψηλές ταχύτητες διατηρώντας μικρές αποστάσεις μεταξύ των οχημάτων της διμοιρίας.

Η εφαρμογή αυτή παρέχει πολλά πλεονεκτήματα ανάμεσα στα οποία είναι η βελτιωμένη διαχείριση της κυκλοφορίας, υψηλότερη χωρητικότητα για οχήματα στο οδικό δίκτυο, οδήγηση χωρίς συγκρούσεις και καλύτερη οικονομία καυσίμων. Οι επιβαίνοντες, χωρίς να απαιτείται δικιά τους παρέμβαση για την πορεία του οχήματος μπορούν να κάνουν άλλες εργασίες, αυξάνοντας την παραγωγικότητα τους όπου το επιθυμούν. Για τα οχήματα της φάλαγγας υποστηρίζεται συνεχής ενημέρωση με ανταλλαγή δεδομένων σε πραγματικό χρόνο με τα κοντινά οχήματα που αποτελούν κομμάτι της, δηλαδή έχουμε μια εφαρμογή επικοινωνίας μεταξύ οχημάτων (V2V). Τα σήματα επιτάχυνσης, πλοήγησης, δρομολόγησης, αλλαγής οχήματος κεφαλής της διμοιρίας και πέδησης μεταδίδονται στο όχημα για να διασφαλιστεί η ασφάλεια του οχήματος.

2.12 Απομακρυσμένη οδήγηση (remote driving)

Η απομακρυσμένη οδήγηση επιτρέπει σε έναν ανθρώπινο χειριστή ή απομακρυσμένο οδηγό να ελέγχει εξ αποστάσεως ένα όχημα μέσω επικοινωνίας V2N χρησιμοποιώντας μια εφαρμογή που βασίζεται στο cloud[15]. Διάφορα σενάρια μπορεί να χρησιμοποιούν την απομακρυσμένη οδήγηση ως εξής:

Η απομακρυσμένη οδήγηση μπορεί να βοηθήσει σε ειδικές περιπτώσεις που απαιτούν από το όχημα να ζητήσει από έναν απομακρυσμένο οδηγό βοήθεια μέσω τηλεχειρισμού, όπως σε ιδιαίτερα κακές καιρικές συνθήκες ή πρωτόγνωρες καταστάσεις στις οποίες ο φυσικός οδηγός του οχήματος δεν είναι σε θέση να λάβει ένα ασφαλές σχέδιο δράσης ή δεν ξέρει πώς να προχωρήσει στις ενέργειες που απαιτούνται.

Οι νέοι, οι ηλικιωμένοι και άλλοι που δεν έχουν άδεια ή δεν είναι ικανοί να οδηγήσουν θα μπορούσαν να επωφεληθούν από την απομακρυσμένη οδήγηση. Επιπλέον, η μετακίνηση φορτηγών από τη μία τοποθεσία στην άλλη, η παράδοση ενοικιαζόμενων αυτοκινήτων σε πελάτες και η παροχή υπηρεσιών ταξί με τηλεκατευθυνόμενο αυτοκίνητο είναι παραδείγματα καταστάσεων όπου οι ιδιοκτήτες στόλων ή μεμονωμένων οχημάτων μπορούν να τα ελέγχουν εξ αποστάσεως.

Τα μέσα μαζικής μεταφοράς που βασίζονται στο cloud είναι τα πλέον κατάλληλα για υπηρεσίες με προκαθορισμένες διαδρομές και στάσεις. Η απομακρυσμένη οδήγηση έχει τη δυνατότητα να μειώσει το κόστος της πλήρως αυτόνομης οδήγησης για συγκεκριμένες περιπτώσεις χρήσης λόγω των χαμηλότερων τεχνικών απαιτήσεων (π.χ.

[15] Gohar, A., & Lee, S. (2020). A cost efficient multi remote driver selection for remote operated vehicles. Computer Networks, 168, 107029. doi: 10.1016/j.comnet.2019.107029

λιγότεροι αισθητήρες εντός του οχήματος και λιγότερες απαιτήσεις υπολογισμού για εξελιγμένους αλγόριθμους).

2.13 Wi-Fi/ Ασύρματο δίκτυο αισθητήρων (WSN) - Διασκορπισμένοι αισθητήρες (extended sensors)

Οι έξυπνες πόλεις χρησιμοποιούν όλο και περισσότερο συνδέσεις Wi-Fi για τη σύνδεση διαφόρων πόρων. Λόγω του περιορισμένου εύρους ζώνης, η δικτύωση Wi-Fi χρησιμοποιείται συνήθως σε έξυπνα συστήματα μεταφοράς για τη σύνδεση αυτοκινήτων, φαναριών και φανοστάτη. Οι ερευνητικοί οργανισμοί προτείνουν συμπληρωματικές λύσεις χαμηλού κόστους, επειδή ο οδικός ηλεκτρικός εξοπλισμός για την υποστήριξη των VANET είναι δαπανηρός. Ένα ασύρματο δίκτυο αισθητήρων (WSN) είναι μία από τις ολοκληρωμένες λύσεις. Οι ασύρματοι κόμβοι δικτύου αισθητήρων τροφοδοτούνται συχνά από τεχνολογίες συλλογής, επικοινωνίας και επεξεργασίας χαμηλού κόστους, που τροφοδοτούνται με μπαταρία. Αυτοί οι κόμβοι χαμηλής κατανάλωσης ενέργειας μπορεί συχνά να λειτουργούν για αρκετά χρόνια σε ένα ζευγάρι μπαταριών AA, μειώνοντας τις απαιτήσεις συντήρησης. Λόγω της χαμηλής κατανάλωσης ενέργειας και του χαμηλού κόστους, ένας μεγάλος αριθμός WSN στην άκρη του δρόμου μπορεί να είναι στρατηγικά τοποθετημένα για να βοηθήσουν την τεχνολογία επικοινωνίας των οχημάτων.

Οι εκτεταμένοι αισθητήρες χρησιμοποιούνται από τα οχήματα για την κάλυψη αναγκών που σχετίζονται με πληροφορίες σχετικά με την θέση αντικειμένων που βρίσκονται σε κοντινή απόσταση, αυτό επιτυγχάνεται με την ανταλλαγή επεξεργασμένων, ή μη, δεδομένων μεταξύ των αισθητήρων. Η ανταλλαγή των διάφορων δεδομένων που απαιτούνται περιλαμβάνει διακομιστές οχημάτων, RSU, χρήστες του οδικού δικτύου και εφαρμογές επικοινωνίας οχημάτων V2X. Τα δεδομένα αυτά που ανταλλάσσουν τα οχήματα με το περιβάλλον τους τα επεξεργάζονται και στη συνέχεια τα μεταδίδουν σε άλλα οχήματα που βρίσκονται σε κοντινή απόσταση συμβάλλοντας με αυτόν τον τρόπο στη δημιουργία μιας ευρύτερης εικόνας για το συγκοινωνιακό περιβάλλον. Οι αισθητήρες για τον σκοπό αυτό μπορούν να συλλέξουν και να διαμοιράσουν μεταξύ των οχημάτων δεδομένα όπως μια φωτογραφία ενός αντικειμένου μέχρι και υλικό από κινούμενες εικόνες (βίντεο) σε πραγματικό χρόνο.

Η συλλογή και ο διαμοιρασμός των δεδομένων από τους αισθητήρες από διάφορες πηγές συμβάλει σημαντικά στη δημιουργία ασφαλούς περιβάλλοντος για την κίνηση των οχημάτων και των πεζών, προλαμβάνοντας μη επιθυμητά συμβάντα. Οι εκτεταμένοι αισθητήρες είναι απαραίτητο στοιχείο για την υλοποίηση της αυτόνομης και της συνεργατικής οδήγησης στα ITS.

Μία περίπτωση ανταλλαγής σημαντικών πληροφοριών μεταξύ των οχημάτων είναι για την προειδοποίηση καταστάσεων μη οπτικής επαφής (Non line of sight - NLOS). Σε αυτές τις περιπτώσεις οι αισθητήρες μπορούν να ενημερώσουν για την διέλευση των οχημάτων από διασταυρώσεις ή για την κατάσταση του οδικού δικτύου λόγω δύσκολων καιρικών συνθηκών που επικρατούν σε μια περιοχή που πρόκειται να διέλθει το όχημα.

2.14 Προηγμένη - αυτόνομη οδήγηση

Τα αυτόνομα οχήματα οραματίστηκαν για πρώτη φορά στις αρχές του 19ου αιώνα (Pendleton et al., 2017). Οι ΗΠΑ, η Γερμανία, η Γαλλία και η Ιαπωνία είχαν προγράμματα έρευνας και ανάπτυξης από το 1964 έως τις αρχές της δεκαετίας του 2000 για την ανάπτυξη αυτόνομων διμοιριών λεωφορείων και φορτηγών, ευφυών

συστημάτων οχημάτων και επεξεργαστών σκηνής οδήγησης οχημάτων που βασίζονται σε βίντεο (Shladover, 2018). Κατασκευαστές αυτοκινήτων όπως η Volvo χρησιμοποιούν τεχνολογία αυτόνομης οδήγησης από το 2006 και εισήγαγαν ένα πλήρως αυτόνομο αυτοκίνητο δοκιμών (επίπεδα SAE 1 και 2) στο δίκτυο οδικών μεταφορών το 2017 (Shladover, 2018). Το 2009, η Google και άλλες εταιρείες τεχνολογίας ανέπτυξαν ένα αυτόνομο όχημα στα επίπεδα SAE 1 και 2. Μέχρι τα τέλη του 2020, η WAYMO, θυγατρική της Alphabet Inc., είχε κάνει το ντεμπούτο των εμπορικών πρωτοτύπων AV, τα οποία είχαν διανύσει πάνω από 3 εκατομμύρια μίλια σε τέσσερις πολιτείες των ΗΠΑ. Από το 2014, η TESLA, έχει κατασκευάσει ηλεκτρικά οχήματα με ικανότητα λειτουργίας χωρίς οδηγό του 90% του χρόνου λειτουργίας χωρίς ανθρώπινη παρέμβαση (Shladover, 2018).

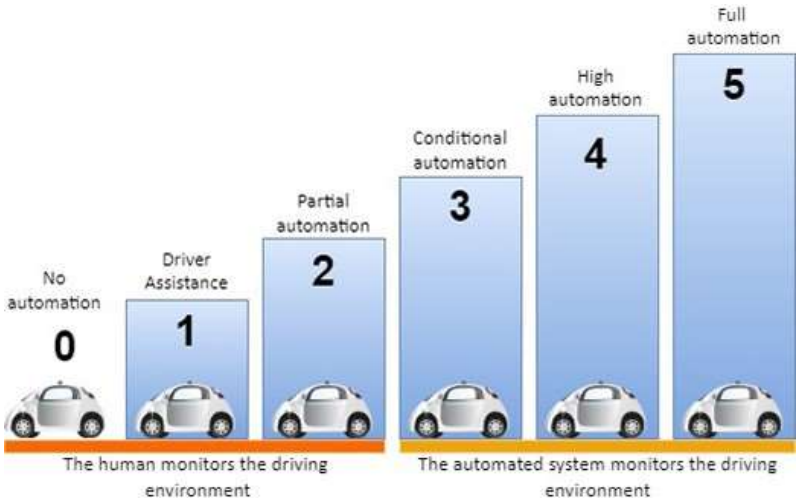
Η οδήγηση ενός οχήματος στο δρόμο απαιτεί βασικές λειτουργίες όπως ο εντοπισμός, η αντίληψη, ο σχεδιασμός, ο έλεγχος και η διαχείριση (Coppola and Morisio, 2016). Η απόκτηση πληροφοριών σχετικά με το άμεσο περιβάλλον οδήγησης ενός AV είναι σημαντική για τον εντοπισμό και την αντίληψη. Η διαθεσιμότητα όλων αυτών των λειτουργιών σε ένα όχημα είναι αυτό που κάνει ένα όχημα αυτόνομο. Ας υποθέσουμε ότι οποιαδήποτε αυτόνομα οχήματα πρέπει να επικοινωνούν με διάφορους τύπους υποδομών για να αποκτήσουν πληροφορίες σχετικά με το περιβάλλον οδήγησής τους ή να διαπραγματευτούν τους ελιγμούς οδήγησής τους. Στην περίπτωση αυτή, αναφέρεται ως συνδεδεμένο αυτόνομο όχημα (CAV) (Shladover, 2018). Ωστόσο, όταν οποιοδήποτε όχημα που οδηγείται από τον άνθρωπο, είτε χειροκίνητο είτε αυτοματοποιημένο, πρέπει να επικοινωνήσει με διαφορετικούς τύπους υποδομών για να κατέχει πληροφορίες, είναι γνωστό ως συνδεδεμένο όχημα (CV) (Coppola and Morisio, 2016). Ως εκ τούτου, η τεχνολογία CV είναι συμπληρωματική στην εφαρμογή αυτόνομων οχημάτων σε κάποιο βαθμό (Shladover, 2018), παρόλο που η συνδεσιμότητα δεν αποτελεί υποχρεωτικό χαρακτηριστικό ενός αυτόνομου οχήματος (Hendrickson et al., 2014).

Η ημιαυτόματη ή πλήρως αυτοματοποιημένη οδήγηση, γίνεται εφικτή με την προηγμένη οδήγηση. Κάθε όχημα, ή RSU, μοιράζεται δεδομένα από τοπικούς αισθητήρες με κοντινά οχήματα, επιτρέποντάς τους να συντονίζουν τις διαδρομές οδήγησης. Τα πλεονεκτήματα της προηγμένης οδήγησης περιλαμβάνουν ασφαλέστερες μετακινήσεις, λιγότερες συγκρούσεις και αυξημένη αποδοτικότητα της κυκλοφορίας.

5G-V2X Use Case	Minimum–Maximum Range (m)	Maximum Latency (ms)	Data Rate (Mbps)	Packet Reliability (%)
Vehicles platooning	80–350	10–500	50–65	90–99.99
Remote driving	-	5	1–25	99.999
Extended sensors	50–1000	3–100	10–1000	90–99.999
Advanced Driving	360–700	3–100	10–50	90–99.999

Εικόνα 6: Σύνοψη των απαιτήσεων για προηγμένες περιπτώσεις χρήσης 5G-V2X σύμφωνα με το 3GPP (ETSI TS 122 186 V16.2.0 (2020-11).

Ο όρος αυτόνομη χρησιμοποιείται συνήθως εναλλακτικά με την αυτόνομη οδήγηση. Ωστόσο, υπάρχει μια μικρή διαφορά μεταξύ των δύο όρων. Με βάση τους ορισμούς της Society of Automotive Engineers (SAE) για τα επίπεδα αυτοματισμού για οχήματα[16], οι οποίοι έχουν υιοθετηθεί από το Υπουργείο Μεταφορών των ΗΠΑ (συγκεκριμένα από την Εθνική Υπηρεσία Οδικής Ασφάλειας (NHTSA), υπάρχουν 6 επίπεδα αυτοματισμού που κυμαίνονται από το επίπεδο 0 (χωρίς αυτοματοποίηση) έως το επίπεδο 5 (πλήρης αυτοματοποίηση), κάθε επίπεδο με αυξανόμενη ποσότητα αυτοματισμού και φθίνουσα συμμετοχή του οδηγού. Από τα επίπεδα 0 έως 2, ένας άνθρωπος οδηγός παρακολουθεί το περιβάλλον οδήγησης, ενώ από τα επίπεδα 3 έως 5, ένα αυτοματοποιημένο σύστημα οδήγησης (ADS) παρακολουθεί το περιβάλλον οδήγησης και ο άνθρωπος δεν εμπλέκεται πλήρως. Έτσι, με βάση τους ορισμούς του SAE, ένα αυτόνομο όχημα στα επίπεδα 4 και 5 είναι αυτοοδηγούμενο, αλλά ένα αυτοοδηγούμενο όχημα στο επίπεδο 3 δεν είναι αυτόνομο καθώς είναι περιορισμένο στο περιβάλλον λειτουργίας και απαιτεί τη συμμετοχή ενός ανθρώπου οδηγού που μπορεί να αναλάβει τον έλεγχο όταν χρειάζεται. Από το επίπεδο 3 και μετά, το όχημα πρέπει να είναι εφοδιασμένο με αυξημένο αριθμό αισθητήρων και συσκευών επικοινωνίας ώστε να έχει "αυτογνωσία". Στην πραγματικότητα, τα πλήρως αυτόνομα οχήματα εξακολουθούν να μην είναι διαθέσιμα για το ευρύ κοινό εκτός από ειδικά δοκιμαστικά προγράμματα (π.χ. αυτοοδηγούμενα αυτοκίνητα Google και Tesla).



Εικόνα 7: Επίπεδα αυτοματισμού οδήγησης.

Το Υπουργείο Μεταφορών των ΗΠΑ κυκλοφόρησε το «Διασφαλίζοντας την αμερικανική ηγεσία στις τεχνολογίες αυτοματοποιημένων οχημάτων: Αυτοματοποιημένα οχήματα 4.0 (AV 4.0)» τον Ιανουάριο του 2021, το AV 4.0 θεσπίζει ομοσπονδιακές αρχές για την ανάπτυξη και την ενσωμάτωση αυτοματοποιημένων οχημάτων, που αποτελούνται από τρεις βασικούς τομείς εστίασης: Προτεραιότητα στην ασφάλεια και την προστασία, προώθηση της καινοτομίας και διασφάλιση συνεπούς ρυθμιστικής προσέγγισης.

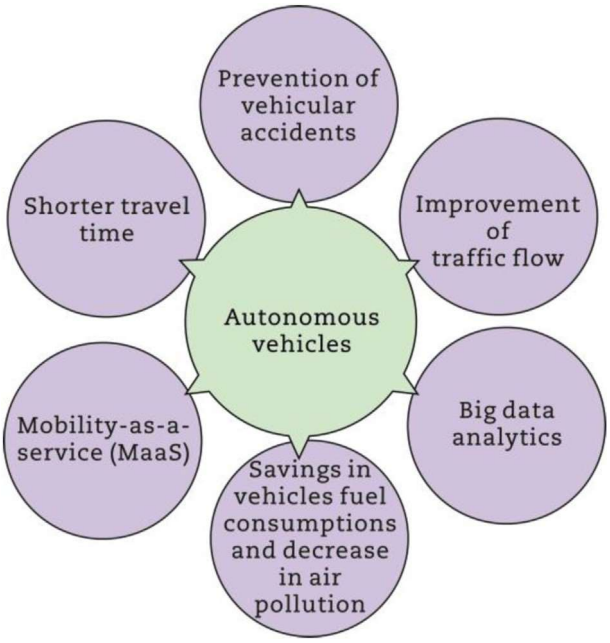
[16] https://www.sae.org/standards/content/j3016_202104/

2.15 Αυτόνομα οχήματα για τις έξυπνες πόλεις

Τα τελευταία χρόνια, το έργο έξυπνης πόλης έχει εφαρμοστεί σε αστικές περιοχές για να βελτιώσει τις σύγχρονες ανάγκες που προκύπτουν συνεχώς στις ζωές των ανθρώπων, υιοθετώντας προηγμένες τεχνολογίες. Οι άνθρωποι ενδιαφέρονται να αξιοποιήσουν τις σύγχρονες καινοτομίες που προσφέρει η συνδεσιμότητα δικτύων ειδικότερα με την έλευση του 5G, καινοτομίες όπως η διαχείριση απορριμμάτων, οι μεταφορές, η παρακολούθηση διαφόρων λειτουργιών της πόλης, η ασφάλεια, η διαχείριση νερού και τα αυτόνομα οχήματα. Ειδικά στον τομέα της αυτοκινητοβιομηχανίας, οι τρεις σύγχρονες τάσεις που απασχολούν τον τεχνολογικό κόσμο, τα ηλεκτρικά οχήματα, τα συνδεδεμένα οχήματα και τα αυτόνομα οχήματα φέρνουν επανάσταση στον συγκεκριμένο τομέα. Το ηλεκτρικό όχημα δίνει τη δυνατότητα για ένα περιβάλλον χωρίς ρύπανση μέσα στην αστική περιοχή, παρέχει ασφαλή οδήγηση ελαχιστοποιώντας τις πιθανότητες σύγκρουσης και ελέγχει την απερίσκεπτη οδήγηση των οδηγών καθώς τα περισσότερα ατυχήματα οφείλονται σε ανθρώπινο λάθος. Το συνδεδεμένο όχημα διαθέτει σύνδεση στο διαδίκτυο που λαμβάνει πληροφορίες σε πραγματικό χρόνο σχετικά με την κυκλοφορία της πόλης και δυναμικές δυνατότητες πλοήγησης στο ITS περιβάλλον, λαμβάνοντας υπόψη δεδομένα που αποθηκεύονται και επεξεργάζονται στο cloud. Αυτά τα οφέλη έρχονται με την εγκατάσταση έξυπνων συσκευών και αισθητήρων σε όλη την πόλη μαζί με την ασύρματη σύνδεση υψηλής ταχύτητας στο Διαδίκτυο και στη συνέχεια οι σύγχρονες αυτές καινοτομίες μπορούν να χρησιμοποιηθούν από τους ανθρώπους.

Η κυκλοφορία στην πόλη μπορεί να ελεγχθεί αποτελεσματικά με τη βοήθεια των πληροφοριών που ανταλλάσσονται μεταξύ των οχημάτων και των εγκατεστημένων συσκευών, λαμβάνοντας δυναμικές αποφάσεις στη διαχείριση της κυκλοφορίας, σε πραγματικό χρόνο. Για ένα αποτελεσματικό και καθολικό σύστημα διαχείρισης κυκλοφορίας, ο σχεδιασμός της έξυπνης πόλης απαιτεί την ύπαρξη και διαλειτουργικότητα διαφορετικών τεχνολογιών, όπως τεχνολογία αυτόνομης οδήγησης, επικοινωνία μεταξύ οχημάτων (V2V), επικοινωνία μεταξύ οχημάτων και υποδομών (V2I) και έξυπνο σύστημα στάθμευσης.

Με την εφαρμογή οχημάτων χωρίς οδηγό σε έξυπνες πόλεις, οι άνθρωποι μπορούν να αποκομίσουν πολλά οφέλη. Τα τροχαία ατυχήματα και το κόστος μεταφοράς μειώνονται πλήρως ενώ η κυκλοφοριακή συμφόρηση αντιμετωπίζεται αποτελεσματικά. Η βέλτιστη ταχύτητα οδήγησης μέσα στην πόλη μπορεί να εφαρμοστεί χωρίς παρεκκλίσεις και οι διαθέσιμες θέσεις στάθμευσης δίνονται ως πληροφορίες σε πραγματικό χρόνο μέσα στο όχημα του μετακινούμενου, οπότε μειώνεται ο χρόνος αναζήτησης του χώρου στάθμευσης. Έτσι, η οικονομία καυσίμου βελτιώνεται μειώνοντας τις περιττές αναζητήσεις χώρων στάθμευσης και την κυκλοφορία στην πόλη, και έτσι, οι εκπομπές ρυπογόνων αερίων που ενισχύουν το φαινόμενο του θερμοκηπίου μπορούν να μειωθούν σημαντικά.



Εικόνα 8: Οφέλη Αυτόνομων Οχημάτων

Παρά την πρόοδο της τεχνολογίας και το ενδιαφέρον του κοινού και των επιχειρήσεων, η βιομηχανία αυτόνομων οχημάτων εξακολουθεί να αντιμετωπίζει πολλές προκλήσεις, πρωταρχική από τις οποίες είναι η ασφάλεια. Αν και με κάποια πρόοδο στην ασφάλεια, ο κανονισμός που θα μπορούσε να επιβάλει τις απαιτήσεις ασφαλείας απουσιάζει σε μεγάλο βαθμό και εξακολουθεί να είναι ασαφές πώς οι τοπικές αρχές θα διαχειριστούν τους νόμους και τους κανονισμούς που διέπουν τη χρήση αυτόνομων οχημάτων.

Μια άλλη πρόκληση με την τεχνολογία είναι να προσπαθήσουμε να κατανοήσουμε τον τομέα στον οποίο τα AV μπορούν να είναι πιο χρήσιμα. Ένας βιομηχανικός τομέας που φωνάζει για αυτόνομα οχήματα είναι ο τομέας των φορτηγών, ο οποίος υποφέρει από εκτεταμένη έλλειψη οδηγών.

Η πρώτη σημαντική πρόκληση που πρέπει να αντιμετωπιστεί για την εισαγωγή των αυτόνομων οχημάτων στην πραγματικότητα είναι η δημιουργία κατάλληλης τεχνολογίας αυτόνομης οδήγησης. Ωστόσο, παρά τις τεράστιες τεχνολογικές εξελίξεις που έχουν γίνει όσον αφορά την τεχνολογία αυτόνομης οδήγησης, οι περισσότεροι κατασκευαστές AV εξακολουθούν να αγωνίζονται με θέματα ασφάλειας όταν πρόκειται για το άμεσο περιβάλλον οδήγησης. Οι αλγόριθμοι τεχνητής νοημοσύνης που εφαρμόζονται για τον προσδιορισμό του άμεσου περιβάλλοντος οδήγησης ενός οχήματος δεν είναι αρκετά ισχυροί όσον αφορά την αποδοτικότητα και την αποτελεσματικότητα στη λειτουργία σε ασταθή αστικά περιβάλλοντα οδήγησης και επίσης αυτές οι τεχνολογίες αγωνίζονται σε ασταθείς καιρικές συνθήκες όπως τυφώνες, τυφώνες και έντονες χιονοπτώσεις (Bezerra and Gomes, 2015). Τέλος, όταν πρόκειται για επικοινωνίες μεταξύ αυτόνομων οχημάτων, δεν πρέπει να υπάρχει διακοπή στην

επικοινωνία, επειδή τέτοιες βλάβες μπορούν να οδηγήσουν σε απρόβλεπτες καταστροφικές συνέπειες.

2.16 Συνδεδεμένα και Αυτόνομα Οχήματα

Το αυτοκίνητο έχει αλλάξει το φυσικό περιβάλλον της γης περισσότερο από οποιαδήποτε άλλη εφεύρεση στην ιστορία της ανθρωπότητας, αναδιαμορφώνοντας πόλεις και οικονομίες. Τα συνδεδεμένα αυτόνομα οχήματα (CAVs) είναι οι φυσικοί διάδοχοι των συμβατικών αυτοκινήτων με δυνατότητες όπως η αυτόνομη οδήγηση και η λήψη αποφάσεων χωρίς την ανθρώπινη παρέμβαση. Για την επίτευξη της αυτόνομης λειτουργίας των οχημάτων απαιτούνται λειτουργίες συνδεσιμότητας που τα καθιστούν ενεργά, συνεργάσιμα, συνεχώς ενημερωμένα με νέα δεδομένα και συντονισμένα, με το IoT περιβάλλον τους. Οι CAVs θα μεταμορφώσουν τις υπηρεσίες κινητικότητας, τα δίκτυα μεταφορών και τις οδικές υποδομές, μεταβιβάζοντας τον έλεγχο του οχήματος και τις ευθύνες οδήγησης από ανθρώπους σε μηχανές με τεράστιες δυνατότητες τεχνητής νοημοσύνης και ασύρματης συνδεσιμότητας. Τα CAVs προβλέπεται να είναι το επόμενο πρότυπο κινητικότητας, μεταμορφώνοντας τα αυτοκίνητα και την ανάπτυξη των πόλεων στο σύνολό τους μέσω της χρήσης της τεχνητής νοημοσύνης από αυτό που θεωρούνται σήμερα.

Τα CAVs σκοπεύουν να δημιουργήσουν πολλά οφέλη, όπως η δημιουργία περισσότερου ελεύθερου χρόνου (δεδομένου ότι ο μέσος οδηγός ξοδεύει το ισοδύναμο έξι εβδομάδων οδήγησης ετησίως), ενίσχυση της ασφάλειας των μεταφορών και της πρόληψης ατυχημάτων, βελτίωση της προσβασιμότητας, της άνεσης και της εμπειρίας οδήγησης εντός του οχήματος, διευκόλυνση των υπευθύνων χάραξης πολιτικής να δώσουν προτεραιότητα σε επιχειρηματικά μοντέλα κοινής χρήσης αυτοκινήτων και συνεπιβατισμού, μείωση της κυκλοφοριακής συμφόρησης, της υποβάθμισης του περιβάλλοντος, της ατμοσφαιρικής ρύπανσης, της ηχορύπανσης και του κοινωνικού αποκλεισμού για όσους δεν μπορούν προς το παρόν να οδηγήσουν. Ταυτόχρονα όμως υπάρχουν επίσης ορισμένες ανησυχίες, σχετικά με την αυξημένη ευπάθεια σε hacking, ελαττώματα λογισμικού και υλικού, απώλεια ιδιωτικότητας και εκμετάλλευση ταξιδιωτικών δεδομένων, προκλήσεις κατανομής ευθυνών, αυξημένη χρήση αυτοκινήτου από περισσότερους πληθυσμούς μη κατειλημμένα οχήματα, αυξημένα ποσοστά ατυχημάτων κα. Υπάρχουν 10 τομείς προτεραιότητας για την πολιτική και τον σχεδιασμό των CAVs που πρέπει να αντιμετωπιστούν για μια ομαλή μετάβαση: τεχνολογία, νομοθεσία, ζητήματα ηθικής κρίσης και απασχόλησης, οδικές υποδομές και χρήσεις γης, η ενσωμάτωση των CAVs στους χρήστες, η ασφάλεια των μεταφορών, η ασφάλεια στον κυβερνοχώρο και η προστασία της ιδιωτικότητας, τα επιχειρηματικά μοντέλα, η διαχείριση της κυκλοφοριακής συμφόρησης σύμφωνα με τις ανάγκες των μετακινούμενων και τέλος η αποδοχή, η εμπιστοσύνη και η προετοιμασία των χρηστών.

2.17 Συνδεδεμένα και Αυτόνομα Οχήματα στην Ελλάδα

Η Ελλάδα αποτελεί μια ενδιαφέρουσα περίπτωση, καθώς πριν από το 2019 ήταν μία από τις μόλις δύο χώρες της ΕΕ που έλαβαν πρόστιμο από την Ευρωπαϊκή Επιτροπή, επειδή δεν ενσωμάτωσαν πλήρως τον GDPR στην εθνική νομοθεσία τους. Ένα παράδειγμα αυτού είναι η Υπουργική Απόφαση 50308/7695 (ΦΕΚ 1837/26.08.2015) για τη λειτουργία ενός αυτόνομου αστικού λεωφορείου στο Δήμο Τρικκαίων εντός του CityMobil2. Σύμφωνα με αυτήν την απόφαση, ο υπεύθυνος ή ο χειριστής του αυτόνομου οχήματος θεωρείται οδηγός σύμφωνα με την εθνική νομοθεσία περί οδήγησης, και υπόκειται σε όλες τις διοικητικές, ποινικές και νομικές ευθύνες.

Εντούτοις, η εθνική νομοθεσία δεν είχε προσαρμοστεί τότε για να επιτρέπει την επιβολή προστίμων σε αντίστοιχες τοπικές ή εθνικές αρχές σε περιπτώσεις παραβιάσεων προσωπικών δεδομένων.

Παρόλο που η Ελλάδα δεν έχει παραδοσιακή αυτοκινητοβιομηχανία, η Tesla ίδρυσε μια μικρή ερευνητική μονάδα στην Ελλάδα το 2019. Η Uber προσφέρει ορισμένες υπηρεσίες στην Αθήνα, παρά τις διαμάχες που συνεχίζονται. Εκτός αυτού, υπάρχουν και άλλοι νέοι πάροχοι υπηρεσιών κινητικότητας, καθώς και μια σειρά εταιρειών ITS (Έξυπνα Συστήματα Μεταφοράς), που περιλαμβάνουν επιχειρήσεις e-scooter που ξεκίνησαν στη Θεσσαλονίκη τον Δεκέμβριο του 2018.

2.18 Ασφάλεια στον κυβερνοχώρο και CAV

Τα CAVs είναι σήμερα πολύπλοκα συστήματα πληροφορικής, αναπόσπαστο μέρος του οικοσυστήματος Internet of Things (IoT), το οποίο αποτελείται από διαφορετικά στοιχεία δικτύωσης και πληροφοριών, λογισμικού και υλικού. Αυτά τα στοιχεία επικοινωνούν μεταξύ τους, καθώς και εξωτερικές πηγές για την υποστήριξη των βασικών λειτουργιών αυτόνομης οδήγησης και των υπηρεσιών ψυχαγωγίας που προσφέρονται σε οδηγούς και επιβάτες. Για παράδειγμα, τα εξαρτήματα λογισμικού σε ένα CAV (συνήθως ενσωματωμένα στη μονάδα ελέγχου κινητήρα - ECU ή στις μονάδες ελέγχου μετάδοσης - TCU) μπορεί να είναι υπεύθυνα για τον έλεγχο της ισχύος, του κινητήρα, του πλαισίου (υποβοήθηση λωρίδας) και του αμαξώματος (π.χ. κλειδαριές) του οχήματος, όπως καθώς και για την επικοινωνία με εξωτερικά δίκτυα (Global Positioning System – GPS, τηλεπικοινωνιακοί φορείς, edge computing, όχημα προς όχημα – V2V – επικοινωνία), για υπηρεσίες ψυχαγωγίας (video streaming, gaming κ.λπ.) καθώς και για την ηλεκτρονική παρακολούθηση, διάγνωση και αναφορά οχημάτων στους κατασκευαστές αυτοκινήτων.

Καθώς ωριμάζουν οι τεχνολογίες πληροφοριών και δικτύωσης που σχετίζονται με τις CAV, αναδύονται πολλαπλές απειλές και κίνδυνοι που αφορούν την ασφάλεια των συστημάτων, καθώς και το απόρρητο των πληροφοριών που συλλέγονται και ανταλλάσσονται μεταξύ ανθρώπων και οχημάτων ή μεταξύ οχημάτων και οχημάτων. Τα συστήματα πληροφοριών και επικοινωνιών μεταξύ οχημάτων και δικτυακής υποδομής έχουν τη δυνατότητα απομακρυσμένης επίθεσης και πρόσβασης από κακόβουλους χρήστες.

Η έκθεση του ENISA[17] [Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), 2017] παρέχει ταξινόμηση των διαφόρων απειλών που μπορούν να επηρεάσουν την ασφάλεια και την ανθεκτικότητα μιας CAV. Σύμφωνα με την έκθεση, οι ακόλουθες απειλές εντοπίζονται με βάση τη μονάδα λογισμικού του οχήματος που επηρεάζεται:

Φυσικές απειλές, όπως έγχυση σφάλματος, δυσλειτουργία, πρόσβαση σε θύρες υλικού: Αυτή η απειλή μπορεί συνήθως να συνίσταται σε παραβίαση των ECU ή των TCU (για ανάκτηση κλειδιών ή πρόσβαση σε φυσικές διεπαφές εντοπισμού σφαλμάτων), χρήση ηλεκτρομαγνητικών εκπομπών της συσκευής ή χρήση ισχύος για διαρροή πληροφοριών (πλευρικό κανάλι) μπορούν να αλλάξουν τη συμπεριφορά της συσκευής και τελικά να αποκτήσουν πρόσβαση τρίτοι σε προστατευμένα δεδομένα (σφάλμα, έγχυση σφάλματος).

Ακούσιες αστοχίες και δυσλειτουργίες λογισμικού: Περιλαμβάνει κυρίως απειλές για τη συνέπεια και την ορθή λειτουργία των συστημάτων λογισμικού σε ένα CAV,

[17] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

όπως σφάλματα διαχείρισης σε υπηρεσίες πληροφοριών παρασκηνίου ή σφάλματα και διαρροή δεδομένων που προορίζονται για διαγνωστικούς σκοπούς. Μπορεί επίσης να περιλαμβάνει εσφαλμένη χρήση ή διαχείριση συσκευών και συστημάτων, χρήση πληροφοριών από αναξιόπιστες πηγές, ακούσια αλλαγή δεδομένων σε ένα σύστημα πληροφοριών ή, τέλος, ανεπαρκή σχεδιασμό, συντήρηση και ανάπτυξη μονάδων λογισμικού σε CAV.

Απώλεια και διακοπή επικοινωνίας: Η πιο κοινή απειλή σχετίζεται με τη διακοπή του δικτύου, είτε λόγω βλαβών δικτύου είτε λόγω κακής κάλυψης. Ειδικά στα αρχικά στάδια των δικτύων 5G, η κάλυψη θα περιοριστεί σε ορισμένες τοποθεσίες και οι εφαρμογές που είναι κρίσιμες για τον λανθάνοντα χρόνο πιθανότατα θα υποφέρουν από κακή συνδεσιμότητα ή τυφλά σημεία στα οδικά δίκτυα. Για παράδειγμα, μια διακοπή δικτύου μπορεί να οδηγήσει σε άρνηση υπηρεσίας για ευαίσθητες λειτουργίες, όπως επιδιορθώσεις over-the-air για κρίσιμα σφάλματα ή ευπάθειες. Γενικότερα, κάθε σχεδιασμός που βασίζεται υπερβολικά στη συνδεσιμότητα εκθέτει το όχημα σε πιθανά προβλήματα σε περίπτωση διακοπής λειτουργίας. Τα οχήματα θα πρέπει να σχεδιάζονται έτσι ώστε να προσφέρουν έναν υλοποιήσιμο υποβαθμισμένο τρόπο λειτουργίας σε περίπτωση διακοπής λειτουργίας.

Απώλεια ή διαρροή ευαίσθητων δεδομένων: Η διαχείριση των πληροφοριών που ανταλλάσσονται από τις CAV γίνεται σε περιβάλλοντα ιδιωτικού cloud, τα οποία διαχειρίζονται είτε πάροχοι τηλεπικοινωνιών είτε κατασκευαστές οχημάτων. Οι συνήθεις απειλές που σχετίζονται με τη διακυβέρνηση των δεδομένων που συλλέγονται σε CAV περιλαμβάνουν την απώλεια ευαίσθητων δεδομένων (π.χ. τοποθεσίες GPS , διεθνείς ταυτότητες συνδρομητών κινητής τηλεφωνίας κ.α.) λόγω επιθέσεων ή σφαλμάτων κατά την αποθήκευση από τρίτους παρόχους υπηρεσιών cloud. Ευαίσθητα δεδομένα ενδέχεται να χαθούν ή να παραβιαστούν λόγω φυσικών ζημιών σε περιπτώσεις τροχαίου ατυχήματος ή κλοπής ή ακόμη και μη κρυπτογραφημένα ιδιωτικά ή ευαίσθητα δεδομένα (όπως πληροφορίες πληρωμής, συνήθειες οδήγησης κ.λπ.) ενδέχεται να διαρρεύσουν όταν το όχημα πωληθεί σε άλλο χρήστη.

Υποκλοπή / Hacking και Phishing: Συνήθως, αυτοί οι τύποι απειλών περιλαμβάνουν επιθέσεις man-in-the-middle/session hijacking . Ένα μεγάλο σύνολο εφαρμογών ψυχαγωγίας σε CAV σημαίνει ότι, δεδομένης της κακής προστασίας της συνεδρίας, π.χ. η εφαρμογή επικοινωνεί μέσω μη κρυπτογραφημένων δικτύων 4G / 5G ή WIFI, υπάρχουν πολλά κίνητρα για έναν εισβολέα να πλαστοπροσωπήσει έναν απομακρυσμένο χρήστη, π.χ. με το ηλεκτρονικό ψάρεμα της ταυτότητας ενός CAV ή ενός χρήστη στο κατάστημα εφαρμογών που μπορεί να οδηγήσει σε οικονομική κατάχρηση.

Κακόβουλη δραστηριότητα/κατάχρηση: Τέλος, η κακόβουλη δραστηριότητα ή κατάχρηση ενός λογισμικού που λειτουργεί σε ένα CAV μπορεί να οδηγήσει σε άρνηση υπηρεσίας (DoS) ή χειραγώγηση των μονάδων υλικού και λογισμικού. Ένα DoS μπορεί να οδηγήσει σε μια μορφή διακοπής του δικτύου (π.χ. απώλεια συνδεσιμότητας δικτύου) αλλά και να προκαλέσει σφάλματα σε μια ECU μέσω κακόβουλου φορτίου. Ο πιθανός αντίκτυπος μιας τέτοιας επίθεσης μπορεί να οδηγήσει σε απροσδόκητες συμπεριφορές. Για παράδειγμα, αλλάζοντας το υλικολογισμικό ενός εξαρτήματος ή αλλάζοντας με άλλο τρόπο τα δεδομένα διαμόρφωσής του, ένας κακόβουλος χρήστης μπορεί να πάρει τον έλεγχο μιας ECU ή τον έλεγχο ενός οχήματος στέλνοντας εντολές που σχετίζονται με την οδήγηση (τιμόνι, φρενάρισμα κ.λπ.). Ένας κακόβουλος χρήστης μπορεί επίσης να προσπαθήσει να αλλάξει την ταυτότητα του

οχήματος, δηλαδή τον τρόπο με τον οποίο επικοινωνεί με τα άλλα οχήματα ή τα συστήματα παρασκηνίου, προκειμένου να πραγματοποιήσει απάτη στα συστήματα διοδίων ή για εγκληματικούς σκοπούς. Η ενσωμάτωση των οικοσυστημάτων ψυχαγωγίας και κινητής τηλεφωνίας μπορεί να προκαλέσει αύξηση του δυνητικού κακόβουλου λογισμικού που εισάγει ο χρήστης. Δεδομένου ότι, τα περισσότερα ECU προσφέρουν λειτουργικό σύστημα που βασίζεται σε Linux ή Android, αυτό σημαίνει ότι οι επιτιθέμενοι μπορούν να ανακυκλώσουν γνωστές διαδρομές επίθεσης.

2.19 Προστασία προσωπικών δεδομένων στα αυτόνομα οχήματα

Τα αυτόνομα οχήματα από τη φύση τους θα παράγουν, θα συλλέγουν, θα επεξεργάζονται και θα αποθηκεύουν τεράστιο όγκο δεδομένων που μπορούν να προσδιορίσουν, με υψηλό βαθμό βεβαιότητας, τον ιδιοκτήτη ή τον επιβάτη του οχήματος, τις δραστηριότητές τους, την τοποθεσία, την κατεύθυνση του ταξιδιού και το ιστορικό ταξιδιού. Τα δεδομένα αυτά θα έχουν μεγάλη αξία για τους χάκερ, τους διαφημιστές, τις ασφαλιστικές εταιρείες και πολλούς άλλους παρόχους υπηρεσιών ή προϊόντων, μια κατάσταση που δημιουργεί διάφορους φόβους για την ασφάλεια και την προστασία της ιδιωτικής ζωής, όχι μόνο λόγω του τεράστιου όγκου δεδομένων που συλλέγονται και αποθηκεύονται, είτε στο ίδιο το όχημα είτε αποστέλλονται στο υπολογιστικό νέφος, αλλά και επειδή παραμένει ασαφές σε ποιον ανήκουν τα παραγόμενα δεδομένα και εάν πραγματοποιούνται περαιτέρω μεταδόσεις[18].

1) Location Trailing Attacks: Αυτή η παθητική επίθεση αποτελεί κρίσιμη απειλή για την ιδιωτικότητα των χρηστών καθώς και για την πιστότητα των μεταδιδόμενων μηνυμάτων, καθώς οι επιτιθέμενοι μπορούν να αποκτήσουν ιδιωτικά και ευαίσθητα δεδομένα του ιδιοκτήτη και των επιβατών μέσω της τοποθεσίας και της παρακολούθησης των δραστηριοτήτων AV καθώς και του αρχείου οδήγησης. Για παράδειγμα, η διαπίστωση ότι ο χρήστης επισκέφθηκε ένα ATM ή/και ψώνισε σε ένα ακριβό κατάστημα παρέχει τη δυνατότητα στοχευμένης κλοπής. Επιπλέον, με τη βοήθεια πληροφοριών τοποθεσίας, οι επιτιθέμενοι μπορούν να σκιαγραφήσουν το προφίλ, να προβλέψουν και ενδεχομένως να χειραγωγήσουν τη συμπεριφορά των χρηστών AV[19].

2) Επιθέσεις υποκλοπής (Eavesdropping Attacks): Αυτός ο τύπος επίθεσης, γνωστός και ως sniffing ή snooping attack, περιλαμβάνει την υποκλοπή ή/και κλοπή ευαίσθητων πληροφοριών που μεταδίδονται μέσω ενός καναλιού επικοινωνίας (π.χ. ταυτότητα AV, τρέχουσα θέση AV, ταχύτητα, λαμβάνοντας υπόψη τις μη ασφαλείς επικοινωνίες και τα μη κρυπτογραφημένα πρωτότυπα στα δίκτυα AV [δίκτυα εντός οχήματος και εξωτερικά δίκτυα. Οι κλεμμένες πληροφορίες μπορούν να βοηθήσουν στην πρόσβαση σε άλλες πληροφορίες στο δίκτυο και να ξεκινήσουν περαιτέρω επιθέσεις, όπως επιθέσεις βάσει ταυτότητας. Η υποκλοπή είναι επίσης μια παθητική επίθεση, και ως εκ τούτου είναι δύσκολο να εντοπιστεί, ειδικά στην ασύρματη επικοινωνία εκπομπής[20].

3) Επιθέσεις ανάλυσης κυκλοφορίας (Traffic Analysis Attacks): Παρόμοια με τις επιθέσεις υποκλοπής, ο σκοπός των επιθέσεων ανάλυσης κυκλοφορίας είναι η παθητική συλλογή πολύτιμων δεδομένων σχετικά με το θύμα-στόχο (π.χ.

[18] H. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," Energies, vol. 11, no. 5, p. 1062, Apr. 2018.
[19] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022.
[20] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," Ad Hoc Netw., vol. 90, Jul. 2019, Art. no. 101823

αναγνωριστικό AV, τοποθεσία AV, διαδρομή που διανύθηκε κ.λπ.), αλλά χωρίς να διακυβεύονται τα πραγματικά δεδομένα. Αυτά τα δεδομένα μπορούν να αναλυθούν περαιτέρω για την εκτέλεση περαιτέρω επιθέσεων εναντίον του θύματος-στόχου, όπως παρεμβολές, υποκλοπές, εντοπισμός τοποθεσίας και επιθέσεις Sybil. Αυτή η επίθεση αποτελεί απειλή υψηλού επιπέδου για το απόρρητο των χρηστών και στην εμπιστευτικότητα των δεδομένων κατά την επικοινωνία οχημάτων, καθώς αποσκοπεί στην αποκωδικοποίηση της ανωνυμίας των επικοινωνιών μεταξύ οχημάτων (V2V) και με τις RSU (V2I)[21].

4) Home Attacks: Πρόκειται για μια νέα κατηγορία επιθέσεων κατά της ιδιωτικής ζωής και του απορρήτου των δεδομένων, όπου οι επιτιθέμενοι παραβιάζουν τον έλεγχο του οχήματος από άλλο χρήστη στο δίκτυο, μέσω της σύνδεσης στο Διαδίκτυο και αποκτούν μη εξουσιοδοτημένη πρόσβαση σε σημαντικές πληροφορίες σχετικά με το όχημα (π.χ. την τοποθεσία του, την ταυτότητα του ιδιοκτήτη κ.λπ.). Στη χειρότερη περίπτωση, οι επιτιθέμενοι μπορούν να αποκτήσουν τον πλήρη έλεγχο του οχήματος και να το χρησιμοποιήσουν για να εκτελέσουν τις κακόβουλες λειτουργίες τους, όπως η μετάδοση λανθασμένων μηνυμάτων, η κλοπή πολύτιμων και ευαίσθητων δεδομένων, η αλλαγή της συμπεριφοράς των αισθητήρων ή η έναρξη περαιτέρω επιθέσεων που μπορούν να επηρεάσουν ολόκληρο το δίκτυο[22].

2.20 GDPR και αυτόνομα οχήματα

Ο GDPR είναι η εξέχουσα νομοθεσία σχετικά με την προστασία των δεδομένων εντός της ΕΕ, θέτοντας επίσης ένα παγκόσμιο πρότυπο, καθώς αντιπροσωπεύει τη ραχοκοκαλιά της μελλοντικής ψηφιακής οικονομίας της ΕΕ. Πράγματι, ο GDPR αντικαθιστά την προηγούμενη οδηγία 95/46 / ΕΚ για την προστασία των δεδομένων , εισάγοντας αρκετές κρίσιμες βελτιώσεις, ξαναγράφοντας προηγούμενες θεμελιώδεις αρχές και συμπληρώνοντάς τις με την απαίτηση λογοδοσίας (άρθρο 5, παράγραφος 2), η οποία γίνεται ο ακρογωνιαίος λίθος της συμμόρφωσης με τον GDPR. Επιπλέον, επιβάλλει νέες υποχρεώσεις στον υπεύθυνο επεξεργασίας, όπως η γνωστοποίηση «παραβίασης δεδομένων» (άρθρα 33 και 34) και η εκτίμηση αντικτύπου δεδομένων (άρθρο 35), ενώ εισάγει νέους ρόλους ως εκτελών την επεξεργασία δεδομένων (άρθρο 28) και υπευθύνου προστασίας δεδομένων (άρθρα 37-39). Τρίτον, αυξάνει τα δικαιώματα του υποκειμένου των δεδομένων δημιουργώντας νέα προνόμια, συμπεριλαμβανομένου του «δικαιώματος στη λήθη» (άρθρο 17). Τέλος, αναδιοργανώνει το θεσμικό δίκτυο ευρωπαϊκών και εθνικών αρχών (Κεφάλαιο IV), ενώ επανασχεδιάζει τα κριτήρια ανάθεσης και αξιολόγησης ευθυνών σε περίπτωση παράβασης (Κεφάλαιο VII). Εν ολίγοις, ο GDPR ανοίγει το δρόμο για ένα προηγμένο νομικό πλαίσιο στην προστασία των προσωπικών δεδομένων, θέτοντας μια διεθνή πρότυπη έννοια της διακυβέρνησης δεδομένων.

Μέσα σε αυτό το ταχέως μεταβαλλόμενο πλαίσιο, η συλλογή και επεξεργασία δεδομένων μέσω οπτικοακουστικών μέσων εγείρει πολλαπλά νομικά ζητήματα ανάλογα με το ισχύον πλαίσιο διαχείρισης πληροφοριών, ανεξάρτητα από το αν πραγματοποιείται εντός ελεγχόμενου περιβάλλοντος, ή εντός δημόσιου χώρου.

[21] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, "Security and privacy challenges in vehicular ad hoc networks," in Connected Vehicles Internet Things. Cham, Switzerland: Springer, 2020, pp. 223–251.

[22] I. A. Sumra et al., "Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET)," in Proc. 3rd Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT), Oct. 2011, pp. 1–8.

Στην πρώτη περίπτωση, μπορεί να παρατηρηθεί ότι η βασική αρχή είναι η εμπιστευτικότητα, η οποία ισχύει για κάθε τύπο δεδομένων. Μεταξύ αυτών, μια ειδική κατηγορία αντιπροσωπεύεται από «προσωπικά δεδομένα», τα οποία σχετίζονται με αναγνωρισμένα - ή αναγνωρίσιμα - φυσικά άτομα. Παρά το γεγονός ότι ορισμένα δικαιώματα παρέχονται στους οδηγούς, τους επιβάτες ή τους πεζούς ως «υποκείμενα δεδομένων» (άρθρο 4 παράγραφος 1 του GDPR), κατ 'αρχήν η κυριότητα αυτών των δεδομένων ανήκει αποκλειστικά σε εκείνους που τελικά τα ελέγχουν και έτσι ορίζονται ως «Εκτελών την επεξεργασία» (άρθρο 4 παράγραφος 7 GDPR). Σύμφωνα με τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2015/962, πρέπει να χορηγείται «προσβασιμότητα, ανταλλαγή και περαιτέρω χρήση» ειδικών ειδών δεδομένων, ιδίως «στατικών δεδομένων σχετικά με το οδικό δίκτυο» (άρθρο 4), «δυναμικών δεδομένων σχετικά με το οδικό δίκτυο» (άρθρο 5) και «δεδομένων κίνησης» (άρθρο 6). Επιπλέον, ένας κανονισμός της ΕΕ καθορίζει το τεχνολογικό πρότυπο που πρέπει να υιοθετηθεί για τη μετάδοση δεδομένων, το οποίο είναι επί του παρόντος το DATEX II. Ο βασικός σκοπός αυτών των διατάξεων είναι φυσικά η οδική ασφάλεια, η οποία αποτελεί πρωταρχικό στόχο σε εθνικό (π.χ. Σουηδία, Ηνωμένο Βασίλειο) ή διεθνώς (π.χ. ΕΕ).

Στη δεύτερη περίπτωση, τα δεδομένα είναι ζωτικής σημασίας για την ανάπτυξη AV. Όπως είναι εύκολα κατανοητό λόγω των τεράστιων επενδύσεων που πραγματοποιούνται για το σχεδιασμό, την κατασκευή και τη συντήρηση οχημάτων, συσκευών επί του οχήματος και υποδομών, η αξία των αντίστοιχων ευρημάτων επιτυγχάνει έναν στρατηγικό στόχο όχι μόνο όσον αφορά τα καθαρά ερευνητικά αποτελέσματα, αλλά και τη βιομηχανική παραγωγή και ακόμη και τις γεωπολιτικές στρατηγικές ανάγκες. Αφενός, μπορεί να δοθεί προτεραιότητα στο γενικό συμφέρον της κοινοποίησης των τελικών αποτελεσμάτων της δημόσιας χρηματοδότησης ή, τουλάχιστον, να επιτραπεί στα ενδιαφερόμενα μέρη να επωφεληθούν έμμεσα από αυτά. Από την άλλη, υπάρχει δικαιολογημένη προσδοκία αναλογικού οφέλους από όσους συμβάλλουν στα αρχικά στάδια τέτοιων προσπαθειών και επενδύσεων.

Η διαχείριση και η προστασία των δεδομένων βρίσκεται στο επίκεντρο αυτής της πρόκλησης, δεδομένου ότι οι επενδυτές θα δικαιούνται χωρίς εξαιρέσεις να χορηγούν οποιαδήποτε «προσβασιμότητα, ανταλλαγή και περαιτέρω χρήση» - ή αλλιώς - στο ευρύ κοινό ή σε τρίτους.

Δεδομένου του τεράστιου όγκου δεδομένων που θα παράγονται καθημερινά από AV, είναι κρίσιμο να διατυπωθούν κανονισμοί με επίκεντρο την προστασία των προσωπικών δεδομένων. Επιπλέον, είναι σημαντικό να προωθηθεί η διακρατική συνεργασία όσον αφορά τη διαχείριση δεδομένων όχι μόνο στην ΕΕ, όπου πολλά κράτη μέλη είναι στενά διασυνδεδεμένα, π.χ. μέσω ενός χώρου χωρίς σύνορα (χώρος Σένγκεν), αλλά και διεθνώς μεταξύ χωρών και ηπείρων. Λόγω των υφιστάμενων παγκόσμιων αλυσίδων εφοδιασμού της κατασκευής οχημάτων και δεδομένου ότι οι κατασκευαστές οχημάτων δηλώνουν ήδη στους Όρους και Προϋποθέσεις πώλησης ότι όλα τα δεδομένα που παράγονται από οχήματα ανήκουν σε αυτούς, είναι προφανές ότι αυτό είναι ένα πεδίο διεθνούς ενδιαφέροντος τόσο για τους επαγγελματίες όσο και για τους υπεύθυνους χάραξης πολιτικής.

2.21 Τεχνολογίες Υλοποίησης ITS και Προβληματισμοί

Προς το παρόν έχουν εγκατασταθεί διάφορες λύσεις στα αυτοκίνητα που διατίθενται σήμερα στην αγορά, όπως αισθητήρες κατά της σύγκρουσης, ευφυή συστήματα πλοήγησης, συστήματα ειδοποίησης οδηγού, συστήματα υποβοηθούμενης στάθμευσης, και η αυτόνομη οδήγηση. Ωστόσο, κάθε εταιρεία χρησιμοποιεί ιδιόκτητες

τεχνολογίες που δεν είναι σε θέση να αλληλεπιδρούν και να συνεργάζονται με τον εξοπλισμό που εγκαθίσταται σε οχήματα που κατασκευάζονται από άλλους κατασκευαστές. Ακριβώς για αυτούς τους λόγους, είναι απαραίτητο να δημιουργηθεί ένα τυποποιημένο σύστημα που μπορεί να προσφέρει διαλειτουργικότητα σε όλο τον κόσμο, παρέχοντας μια εύκολη και αποτελεσματική ενοποίηση μεταξύ όλων αυτών των υπηρεσιών και εφαρμογών στην αγορά.

Οι νέες τεχνολογίες ITS θα πρέπει να ενσωματωθούν ακόμη πιο αποτελεσματικά στα υφιστάμενα δίκτυα κινητής τηλεφωνίας, που θα αναπτυχθούν τα επόμενα χρόνια, προκειμένου να εφαρμοστεί οριστικά το λεγόμενο IoT, υποστηρίζοντας νέες υπηρεσίες που βασίζονται στο υπολογιστικό νέφος και σε Software Defined Networks (SDN), δημιουργώντας έτσι όλο και πιο εξελιγμένες λύσεις. Η υιοθέτηση αυτών των δικτύων σε εφαρμογές ITS είναι απαραίτητη για την εξεύρεση μιας καθολικής και βιώσιμης εφαρμογής. Επιπλέον, η χρήση των κοινωνικών δικτύων και η εφαρμογή στρατηγικών crowdsourcing θα μπορούσαν επίσης να αποτελέσουν πολύτιμη υποστήριξη για τη διαχείριση των πόρων στις εφαρμογές ITS.

Σύμφωνα με τον παρακάτω πίνακα τα πλεονεκτήματα και τα μειονεκτήματα που θα πρέπει να αντιμετωπιστούν για την ευρεία διάδοση των επικοινωνιών οχημάτων θέτουν τις προκλήσεις για την υλοποίηση και τον στρατηγικό σχεδιασμό που απαιτείται σε ένα ευρύ επιστημονικό φάσμα από όλους τους εμπλεκόμενους.

Feature	Advantages	Downsides
Maintenance of road surface and signs	- Improvement of ITS systems performance	- Economic costs
Technological infrastructure	- Full operation of V2V, V2I, and V2X communications	- Complexity of large-scale implementation - Standardization
Big Data management	- Economic returns for possible private investors - More information thanks to analysis	- Ensure data privacy
Integration between ITS systems and technological infrastructure	- Improved performance in system operation - Development of possible new future applications	- Complexity of large-scale implementation - Standardization - Economic costs

Εικόνα 9 Πλεονεκτήματα και μειονεκτήματα στην υλοποίηση ITS

Ένα θεμελιώδες χαρακτηριστικό θα είναι η συντήρηση του οδοστρώματος και των πινακίδων που θα έχουν ως αποτέλεσμα την καλύτερη εφαρμογή των λειτουργιών των συστημάτων ITS. Στην περίπτωση αυτή, το κύριο εμπόδιο είναι το οικονομικό κόστος, δεδομένου ότι μόνο ένα μικρό μέρος της παγκόσμιας οδικής υποδομής, επί του παρόντος, θα μπορούσε να είναι έτοιμο για επικοινωνίες V2X και απαιτούνται σημαντικοί οικονομικοί πόροι για τη βελτίωση του οδικού δικτύου. Ένας άλλος στόχος που θα επιτευχθεί θα είναι η βελτίωση της τεχνολογικής υποδομής που θα περιλαμβάνει την πλήρη και συνολική λειτουργία των επικοινωνιών V2V, V2I και V2X. Ωστόσο, η δυσκολία που πρέπει να αντιμετωπιστεί δεν οφείλεται μόνο στη

δυνητικά δύσκολη εφαρμογή σε μεγάλη κλίμακα, αλλά και στην έλλειψη ενός κοινού προτύπου που θα χρησιμοποιείται παγκοσμίως. Η αποτελεσματική διαχείριση και ανάλυση των μαζικών δεδομένων θα αποτελέσει σίγουρα μια πολύ κερδοφόρα ευκαιρία, καθώς θα μπορούσε να συνεπάγεται όχι μόνο οικονομική απόδοση για πιθανούς ιδιώτες επενδυτές, αλλά και την ανάκτηση λεπτομερέστερων πληροφοριών χάρη σε προηγμένα εργαλεία ανάλυσης. Ωστόσο, όλα αυτά θα πρέπει να εγγυηθούν το απόρρητο των δεδομένων. Τέλος, είναι προφανές ότι η ολοκλήρωση και η συνέργεια μεταξύ των συστημάτων ITS και της τεχνολογικής υποδομής θα αποφέρει πλεονεκτήματα όσον αφορά τη βελτίωση των επιδόσεων στη λειτουργία των συστημάτων μεταφορών και την ανάπτυξη πιθανών νέων καινοτόμων εφαρμογών.

2.22 VANETs & Ασφάλεια

Με σκοπό την ανταλλαγή κρίσιμων πληροφοριών οδήγησης, έχουν δημιουργηθεί δίκτυα ad hoc οχημάτων (VANETs).

Το VANET είναι μια ειδική κατηγορία κινητού δικτύου Ad-Hoc (MANET). Το δίκτυο αυτό μπορεί να οριστεί ως ένα αυτόνομο σύστημα κόμβων ή κινητών σταθμών (MS) διασυνδεδεμένων με ασύρματες συνδέσεις. Οι συσκευές και οι κινητοί σταθμοί (MS) αντιπροσωπεύονται από κόμβους στο δίκτυο. Συνδέοντας ασύρματα όλους αυτούς τους κόμβους, δημιουργείται ένα προσωρινό δίκτυο. Κάθε ασύρματος κόμβος μπορεί να λειτουργήσει ως πομπός, δέκτης ή δρομολογητής. Τα οχήματα ως κόμβοι επικοινωνίας μπορούν να κινηθούν ανά πάσα στιγμή και προς οποιαδήποτε κατεύθυνση, επομένως η κινητικότητα των κόμβων είναι το κύριο πλεονέκτημα σε αυτά τα δίκτυα.

Η κύρια διαφορά του VANET σε σύγκριση με το MANET είναι η δυναμική μεταβλητή τοπολογία του δικτύου. Οι κόμβοι ως αυτοκίνητα μπορούν ελεύθερα να συνδεθούν ή να αποσυνδεθούν από την τοπολογία του δικτύου. Βασικά είναι τεχνολογία WLAN με αυθόρμητη δημιουργία σύνδεσης. Αυτό επιτρέπει τη δημιουργία προσωρινής σύνδεσης δικτύου για κόμβους. Στην περίπτωση των οδικών μεταφορών, κάθε όχημα μπορεί να γίνει φορέας πληροφοριών και, ανάλογα με την ταχύτητα του οχήματος, μπορεί να αποτελέσει γέφυρα μεταξύ διαφορετικών τοπολογιών.

Στην τεχνολογία VANET χρησιμοποιούνται τρία κύρια στοιχεία επικοινωνίας:

Εποχούμενη μονάδα (On-Board Unit - OBU) - Αυτή η μονάδα βρίσκεται σε οχήματα και αποτελείται από διεπαφή χρήστη, κύρια μονάδα ελέγχου, ειδική διεπαφή για σύνδεση με δεύτερη OBU και μνήμη για ανάγνωση / εγγραφή των πληροφοριών που λαμβάνονται.

Μονάδα εφαρμογής (Application Unit - AU) – Η AU είναι μια συσκευή που βρίσκεται στο όχημα. Αυτή η μονάδα χρησιμοποιεί επιτρεπόμενες εφαρμογές που καθορίζονται από τον πάροχο που χρησιμοποιεί τις δυνατότητες επικοινωνίας της εποχούμενης μονάδας. Είναι μια συσκευή με δυνατότητα εκτεταμένης χρήσης, μπορεί να παρέχει την ασφάλεια των εφαρμογών, αλλά μπορεί επίσης να παρέχει μια εφαρμογή για πρόσβαση στο Internet. Ένα βασικό χαρακτηριστικό είναι η σύνδεση μεταξύ της AU και της OBU χρησιμοποιώντας μια ενσύρματη ή ασύρματη λύση, η οποία τους επιτρέπει να βρίσκονται φυσικά στο ίδιο στοιχείο. Η AU επικοινωνεί με το δίκτυο μέσω της εποχούμενης μονάδας, η οποία φροντίζει για τις λειτουργίες δικτύου και κινητής τηλεφωνίας

Road Side Unit (RSU) - Είναι μια συσκευή που βρίσκεται δίπλα στους δρόμους ή σε ορισμένα συγκεκριμένα σημεία, όπως σταυροδρόμια, αυτοκινητόδρομους ή χώρους στάθμευσης. Αυτή η μονάδα χρησιμοποιείται για την παροχή σύνδεσης στο διαδίκτυο, την επανάληψη της επικοινωνίας μεταξύ της OBU και για την προειδοποίηση σημαντικών σημείων όπου πρέπει να αυξηθεί η προσοχή.

Τα δίκτυα VANET λειτουργούν στις ζώνες συχνοτήτων των αποκλειστικών επικοινωνιών μικρής εμβέλειας (DSRC) με πρότυπα ασύρματης πρόσβασης σε περιβάλλοντα οχημάτων (WAVE). Η ασύρματη πρόσβαση σε περιβάλλοντα οχημάτων διαφέρει σημαντικά από το Wi-Fi. Τα πρότυπα DSRC / WAVE γίνονται το κύριο κλειδί που χρησιμοποιείται στο ευφυές σύστημα μεταφορών (ITS).

Στην τεχνολογία VANET είναι διαθέσιμοι πολλοί τύποι συνδέσεων επικοινωνίας. Αυτές οι επικοινωνίες χωρίζονται ανάλογα με τη διαδρομή δεδομένων:

• Εσωτερική επικοινωνία οχημάτων - Αυτή είναι μια επικοινωνία μόνο μέσα στα εξαρτήματα του αυτοκινήτου.

• Επικοινωνία μεταξύ οχημάτων (V2V) - Σε αυτή την επικοινωνία, υπάρχει άμεση ανταλλαγή δεδομένων μεταξύ μεμονωμένων κόμβων (οχημάτων) στο δίκτυο. Ωστόσο, είναι το πιο σημαντικό κανάλι επικοινωνίας της υποδομής VANET και με την ανταλλαγή αυτών των δεδομένων, παρέχει τις περισσότερες πληροφορίες για τον οδηγό.

• Όχημα προς οδική υποδομή V2I - Είναι μια επικοινωνία όπου το όχημα και ένα σταθερό σημείο της υποδομής δικτύου επικοινωνούν μεταξύ τους.

• Όχημα σε όλα V2X - Είναι η πιο σημαντική επικοινωνία όσον αφορά την ανάπτυξη του IoT.

• Όχημα σε VANET cloud V2C - Με αυτήν την επικοινωνία, τα οχήματα μπορούν να επικοινωνούν με την υπηρεσία cloud VANET. Αυτή η λειτουργία μεσολαβεί σε διάφορους τύπους υπηρεσιών που εφαρμόζονται στα οχήματα. Η κύρια υπηρεσία είναι να καταστεί διαθέσιμη η πρόσβαση στο κοινό υπολογιστικό νέφος σε συστήματα οχημάτων.

Τα χαρακτηριστικά της τεχνολογίας συνδεδεμένων αυτοκινήτων που απολαμβάνουν οι καταναλωτές είναι πολυάριθμα. Ωστόσο, αυτά τα χαρακτηριστικά εκθέτουν το VANET σε πρωτοφανείς απειλές ασφαλείας που κυμαίνονται από τυπικές επιθέσεις δικτύου έως εξελιγμένο κακόβουλο λογισμικό και hacking. Εκτός από αυτές τις συνέπειες, η εμπορευματοποίηση της τεχνολογίας συνδεδεμένων αυτοκινήτων παρεμποδίζεται επίσης, τουλάχιστον εν μέρει, από τα ζητήματα ασφάλειας που αντιμετωπίζει αυτή η τεχνολογία. Είναι επίσης σημαντικό να αναφερθεί ότι υπάρχουν κυρίως δύο τύποι επικοινωνιών που εμπλέκονται στο VANET, η επικοινωνία μεταξύ οχημάτων όπου οι κόμβοι οχημάτων συνδέονται με άλλες οντότητες και η επικοινωνία εντός του οχήματος όπου διαφορετικά εξαρτήματα του αυτοκινήτου συνδέονται μέσω δικτύου και στο Διαδίκτυο. Αυτοί οι τύποι επικοινωνιών αυξάνουν τον κίνδυνο επιθέσεων απομακρυσμένης πρόσβασης και χειρισμού δεδομένων σε εφαρμογές VANET. Σε αυτό το πλαίσιο, το γεγονός ότι το σημερινό VANET χρησιμοποιεί την υπάρχουσα υποδομή δικτύωσης, το οποίο είναι επιρρεπές σε πληθώρα επιθέσεων, θέτει ερωτηματικά για την προσαρμογή του τόσο στους καταναλωτές όσο και στη βιομηχανία.

Η προστασία της ιδιωτικής ζωής σημαίνει ότι τα άτομα έχουν το δικαίωμα να ελέγχουν πλήρως τις πληροφορίες για τον εαυτό τους και να αποφασίζουν τις λεπτομέρειες των

πληροφοριών που κοινοποιούνται με άλλους. Η προστασία της ιδιωτικότητας των οχημάτων θα πρέπει να λαμβάνεται σοβαρά υπόψη εκτός από τα αναδυόμενα ζητήματα ασφάλειας. Ο ανώνυμος έλεγχος ταυτότητας είναι μια κοινή μέθοδος για τη διατήρηση του απορρήτου των οχημάτων στα VANETs. Η ανωνυμία είναι η κατάσταση της μη αναγνώρισης μέσα σε ένα σύνολο θεμάτων, η οποία μπορεί να παρέχεται με ψευδώνυμα. Ένα ψηφιακό ψευδώνυμο είναι μια συμβολοσειρά bit που χρησιμοποιείται ως μοναδικό αναγνωριστικό για έλεγχο ταυτότητας χωρίς καμία προσωπική αναγνωρίσιμη πληροφορία. Επομένως, ένα ψευδώνυμο επιτρέπει τον έλεγχο ταυτότητας μιας συγκεκριμένης οντότητας χωρίς να γνωρίζει την πραγματική της ταυτότητα. Με βάση τους χρησιμοποιούμενους κρυπτογραφικούς μηχανισμούς, τα ανώνυμα συστήματα ελέγχου ταυτότητας μπορούν να χωριστούν σε πέντε κατηγορίες:

Συστήματα βασισμένα στη συμμετρική κρυπτογραφία

Η συμμετρική κρυπτογραφία έχει υψηλή υπολογιστική απόδοση και χαμηλότερη επιβάρυνση επικοινωνίας που χρησιμοποιεί κωδικό εξουσιοδότησης μηνυμάτων (MAC) για τον έλεγχο ταυτότητας μηνυμάτων. Ο αποστολέας δημιουργεί το MAC για κάθε μήνυμα χρησιμοποιώντας το κοινόχρηστο μυστικό κλειδί. Όλοι οι κόμβοι σε ένα σύνολο ανωνυμίας χρησιμοποιώντας το ίδιο μυστικό κλειδί και μπορούν να επαληθεύσουν το MAC που συνδέεται με το μήνυμα.

Συστήματα βασισμένα σε υποδομές δημόσιου κλειδιού

Τα οχήματα είναι εξοπλισμένα με ζεύγη δημόσιων / ιδιωτικών κλειδιών για ψευδώνυμη επικοινωνία. Τα πιστοποιητικά δημόσιου κλειδιού χρησιμοποιούνται στην υποδομή δημόσιου κλειδιού (PKI) ως ασφαλής και αξιόπιστη μέθοδος για τον έλεγχο ταυτότητας ενός οχήματος, η οποία περιέχει το κλειδί δημοσίευσης ενός οχήματος και την ψηφιακή υπογραφή μιας αρχής πιστοποίησης (CA) για έλεγχο ταυτότητας.

Συστήματα που βασίζονται σε υπογραφή βάσει ταυτότητας

Η υπογραφή βάσει ταυτότητας (IBS) χρησιμοποιεί το αναγνωριστικό του κόμβου ως δημόσιο κλειδί και υπογράφει μηνύματα με το ιδιωτικό κλειδί που δημιουργείται από το αναγνωριστικό. Το αναγνωριστικό του αποστολέα είναι επαρκές για την επαλήθευση της υπογραφής χωρίς την ανάγκη πρόσθετων πιστοποιητικών ή ρητών δημόσιων κλειδιών.

Συστήματα βασισμένα σε υπογραφή χωρίς πιστοποιητικά

Στην κρυπτογραφία χωρίς πιστοποιητικό, το κέντρο δημιουργίας κλειδιών (KGC) λειτουργεί ως ημι-αξιόπιστο τρίτο μέρος που είναι υπεύθυνο για την παροχή στον χρήστη ενός μερικού ιδιωτικού κλειδιού DIDi που υπολογίζεται από την ταυτότητα του χρήστη IDi . Στη συνέχεια, ο χρήστης δημιουργεί το πραγματικό ιδιωτικό κλειδί με μια μυστική τιμή και το μερικό ιδιωτικό κλειδί που παρέχεται από το KGC. Σε αντίθεση με την κρυπτογράφηση που βασίζεται σε αναγνωριστικό, το KGC δεν μπορεί να αποκτήσει πρόσβαση σε αυτό το ιδιωτικό κλειδί. Στη συνέχεια, ο χρήστης χρησιμοποιεί τις δημόσιες παραμέτρους και τη μυστική τιμή για να δημιουργήσει το δημόσιο κλειδί PKIDi.

Συστήματα με βάση την υπογραφή ομάδας

Το απόρρητο των οχημάτων διατηρείται σε συστήματα που υποστηρίζουν ομαδική υπογραφή, επιτρέποντας στα έγκυρα μέλη της ομάδας να υπογράφουν μηνύματα ανώνυμα εκ μέρους της ομάδας. Μόνο ο διαχειριστής ομάδας έχει τη δυνατότητα να προσδιορίσει ποιος είναι ο πραγματικός αποστολέας. Το κύριο μειονέκτημα της

ομαδικής υπογραφής είναι ότι είναι συνήθως χρονοβόρα η επαλήθευση της υπογραφής, η οποία δεν είναι κατάλληλη για αυστηρές εφαρμογές σε VANETs.

Με την εκρηκτική αύξηση του μεγέθους και της πολυπλοκότητας του VANET, γίνεται όλο και πιο δύσκολη η διαχείριση τέτοιων δικτύων. Ως εκ τούτου, η ανάγκη μετάβασης σε πιο εξελιγμένες λύσεις που προωθούν την αυτονομία για τη λήψη αποφάσεων με τη χρήση τεχνητής νοημοσύνης (AI). Η μηχανική μάθηση (ML), ως υποσύνολο της τεχνητής νοημοσύνης, διαδραματίζει ηγετικό ρόλο στη δημιουργία συστημάτων επόμενης γενιάς. Με την εφαρμογή προσεγγίσεων ML στα ITS, μπορεί να επιτευχθεί σημαντική βελτίωση κάνοντας τις αμυντικές στρατηγικές (π.χ. ανίχνευση εισβολής, software και ανίχνευση κακόβουλου λογισμικού) πιο έξυπνες, προσαρμοστικές και εξαιρετικά αποτελεσματικές.

Αν και, το VANET κερδίζει δημοτικότητα, υποφέρει από πολλές προκλήσεις σχεδιασμού και ανάπτυξης λόγω της δυναμικής φύσης του.

Το VANET πρέπει να είναι αρκετά ασφαλές ώστε να αντιστέκεται σε επιθέσεις και να διασφαλίζει τον στόχο των υπηρεσιών ασφαλείας, όπως ο έλεγχος ταυτότητας, η διαθεσιμότητα, η εμπιστευτικότητα, η ακεραιότητα και η μη αποκήρυξη. Η προστασία της ιδιωτικής ζωής είναι επίσης μια σημαντική ανησυχία όπου η ταυτότητα και η τοποθεσία του οχήματος (οδηγού) θα πρέπει να είναι γνωστές μόνο στην αυθεντική οντότητα.

Διαχείριση εμπιστοσύνης για VANET:

Μοντέλο μηχανισμού εμπιστοσύνης: Λόγω της περιορισμένης χωρητικότητας των οχημάτων, τυπικές τεχνολογίες που απαιτούν πολύ υψηλότερους υπολογιστικούς πόρους, όπως ανίχνευση εισβολής, κρυπτογράφηση κωδικού πρόσβασης και τεχνολογία αποκρυπτογράφησης δεν ισχύουν. Εναλλακτικά, ο σκοπός του μηχανισμού εμπιστοσύνης είναι να αξιολογήσει το επίπεδο εμπιστοσύνης των οχημάτων, με βάση το ιστορικό αλληλεπίδρασής τους. Χρησιμοποιώντας αυτό ως καθοδήγηση αξιολόγησης, είναι σε θέση να εγκαταλείψει κακόβουλα οχήματα και να ενθαρρύνει αξιόπιστα οχήματα για αλληλεπίδραση δεδομένων. Εν αναμονή του πεδίου εφαρμογής του μοντέλου εμπιστοσύνης, εισάγονται οι ακόλουθες τρεις κατηγορίες:

Μοντέλο εμπιστοσύνης βάσει οντότητας: Η βιβλιογραφία που βασίζεται σε μοντέλο εμπιστοσύνης βάσει οντότητας αξιολογεί κυρίως την αξιοπιστία των οχημάτων. Εδώ, η άμεση εμπιστοσύνη και η έμμεση εμπιστοσύνη σύστασης εφαρμόζονται από κοινού, για τον εντοπισμό μη αξιόπιστων ή κακόβουλων οχημάτων. Σε προτεινομένη λύση των Tan et al. εφαρμόστηκε η θεωρία γραφημάτων για να αξιολογηθεί ή αξιοπιστία δρομολόγησης των οχημάτων με βάση το ρυθμό μετάδοσης πακέτων και τη μέση καθυστέρηση. Επίσης ένα προτεινόμενο μοντέλο Xiao et al. εμπιστοσύνης βασισμένο στην ιστορική αλληλεπίδραση μεταξύ των οχημάτων χρησιμοποιείται περαιτέρω για την κατασκευή ενός σχετικά σταθερού γραφήματος σύνδεσης εμπιστοσύνης.

Μοντέλο εμπιστοσύνης βάσει δεδομένων: Το μοντέλο εμπιστοσύνης βάσει δεδομένων στοχεύει στην αξιολόγηση της αξιοπιστίας του επιπέδου δεδομένων. Εδώ, αυτό το μοντέλο εμπιστοσύνης απαιτεί τη συλλογή δεδομένων από διάφορες πηγές, συμπεριλαμβανομένων των ίδιων των οχημάτων, των κοντινών οχημάτων τους και των RSU. Οι Huang et al. πρότειναν έναν νέο μηχανισμό ψηφοφορίας βασισμένο στη σχέση απόστασης μεταξύ του οχήματος και του αναφερόμενου γεγονότος. Εδώ, το όχημα αποφασίζει εάν θα αποδεχθεί τα ληφθέντα δεδομένα συμβάντος ανάλογα με το αποτέλεσμα της ψηφοφορίας, όπου μια μεγαλύτερη απόσταση από το γεγονός συνεπάγεται υψηλότερο βάρος ψήφου.

Συνδυασμένο μοντέλο εμπιστοσύνης: Το συνδυασμένο μοντέλο αξιοπιστίας από προεπιλογή, εκμεταλλεύεται και τους δύο τύπους μοντέλων εμπιστοσύνης. Δεν αξιολογεί μόνο τον βαθμό εμπιστοσύνης των οχημάτων, αλλά υπολογίζει επίσης την αξιοπιστία των δεδομένων. Εγγενώς, το κίνητρο του συνδυασμένου μοντέλου εμπιστοσύνης είναι ότι, η εμπιστοσύνη των οχημάτων επηρεάζει την αξιοπιστία των δεδομένων λόγω του αντίκτυπου της συμπεριφοράς αλληλεπίδρασης, ενώ η εμπιστοσύνη των δεδομένων, με τη σειρά της, αντικατοπτρίζει την αξιοπιστία των οχημάτων λόγω της διαδρομής προώθησης που θα διασχίσουν τα δεδομένα.

3 5G Technologies & ITS

3.1 Ανασκόπηση στην Εξέλιξη των Τηλεπικοινωνιών

Κάθε 10 χρόνια περίπου εμφανίζεται μια νέα γενιά ασύρματης τεχνολογίας κινητών τηλεπικοινωνιών .

Η πρώτη γενιά (1G) εισήχθη στις αρχές της δεκαετίας του 1980. Χαρακτηρίστηκε από τις δυνατότητες μετάδοσης φωνής χρησιμοποιώντας αναλογική τεχνολογία, χωρίς να υποστηρίζεται υπηρεσία δεδομένων για τη μετατροπή της φωνής σε ψηφιακά σήματα, έχοντας μέτρια ποιότητα ήχου. Οι συχνότητες λειτουργίας ήταν ~ 800 - 900 MHz και η χωρητικότητα του καναλιού περιορίστηκε στα 30 KHz. Είχε περιορισμένη χωρητικότητα, κακή λήψη, χαμηλή απόδοση μπαταρίας και παρεμβολές θορύβου περιβάλλοντος.

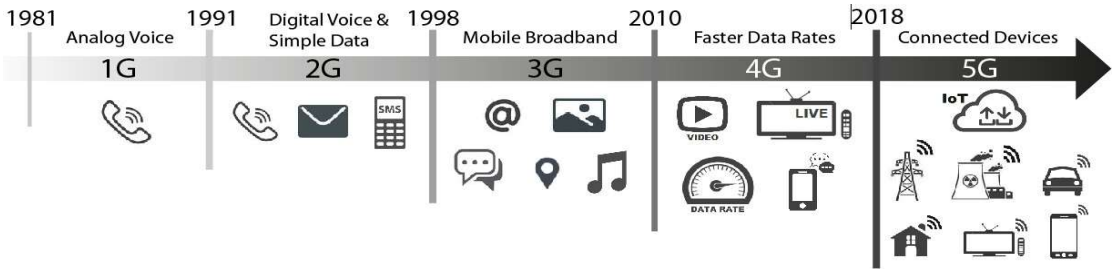
Η ψηφιακή τεχνολογία εισήχθη κατά τη διάρκεια της δεύτερης γενιάς (2G) στα τέλη της δεκαετίας του 1990, βελτιώνοντας την ποιότητα της φωνής και αυξάνοντας τη χωρητικότητα του ρυθμού δεδομένων. Κατά τη διάρκεια αυτής της δεύτερης γενιάς, το (GSM) ήταν ένα ψηφιακό πρότυπο που υποστήριζε διάφορες υπηρεσίες όπως: Υπηρεσία σύντομων μηνυμάτων (SMS) και Υπηρεσία μηνυμάτων πολυμέσων (MMS). Η πρόοδος στην τεχνολογία GSM είναι το GPRS που είναι επίσης γνωστό ως 2.5G, στο οποίο η ταχύτητα δεδομένων βελτιώθηκε έως και 150 Kbps. Οι παρεμβολές θορύβου και η ποιότητα της φωνής βελτιώθηκαν ενώ η ψηφιακή κρυπτογράφηση εισήχθη για πρώτη φορά στο 2G για την ασφαλή μετάδοση δεδομένων.

Η τρίτη γενιά (3G) εμφανίστηκε στα τέλη της δεκαετίας του 2000. Έφερε τα πρώτα πραγματικά ασύρματα δεδομένα, δίνοντας στους χρήστες ευρεία πρόσβαση στο διαδίκτυο μέσω κινητών συσκευών. Χαρακτηριστικό της τεχνολογίας 3G ήταν ο υψηλός ρυθμός μετάδοσης δεδομένων, με τον οποίο βελτιώθηκε ριζικά η ταχύτητα από 144 Kbps σε 2Mbps, επιτρέποντας την ανάπτυξη προηγμένων εφαρμογών πολυμέσων. Επιπλέον, οι νέες ζώνες συχνοτήτων και οι πληροφορίες τοποθεσίας επέτρεψαν τη λειτουργία εφαρμογών που δεν ήταν προηγουμένως διαθέσιμες σε κινητές συσκευές, όπως η γρήγορη περιήγηση στο διαδίκτυο, η πρόσβαση στο ηλεκτρονικό ταχυδρομείο, υπηρεσίες streaming, διενέργεια τηλεδιασκέψεων κ.α. Σημαντικό μειονέκτημα της τρίτης γενιάς είναι η αυξημένη κατανάλωση ενέργειας η οποία μειώνει τη διάρκεια ζωής της μπαταρίας των συσκευών.

Η τέταρτη γενιά (4G) που βασίζεται εξ ολοκλήρου στο πρωτόκολλο Internet (IP), παρουσιάστηκε το 2010 και χρησιμοποιείται ευρέως μέχρι και σήμερα. Κύρια πλεονεκτήματα της τεχνολογίας 4G είναι η υψηλότερη ασφάλεια, υπηρεσίες χαμηλότερου κόστους, πολυμέσων και Διαδικτύου μέσω IP, με αρκετά υψηλότερους ρυθμούς δεδομένων σε σύγκριση με τις προηγούμενες γενιές. Στα δίκτυα 4ης γενιάς

όλο το δίκτυο IP χρησιμοποιείται ως τύπος μεταγωγής και το κεντρικό δίκτυο είναι το διαδίκτυο (συγκριτικά με το δίκτυο πακέτων που χρησιμοποιεί το 3G και το PSTN που χρησιμοποιεί το 2G). Συγκεκριμένα, το 4G υποστηρίζει χωρητικότητα έως και 40 MHz με μέγιστη ταχύτητα τα 100 Mbps, προσφέρει ασύρματη ευρυζωνική σύνδεση υψηλής ταχύτητας, ξεκλειδώνοντας τις δυνατότητες των κινητών υπηρεσιών βίντεο και cloud, όπως online βιντεοπαιχνίδια, ζωντανή μετάδοση εικόνας υψηλής ποιότητας, κ.α.

Σήμερα βρισκόμαστε στο ξεκίνημα μιας νέας εποχής με την πέμπτη γενιά 5G ασύρματης τεχνολογίας κινητών τηλεπικοινωνιών, η οποία είναι ήδη λειτουργική και έχει φέρει δυνατότητες δικτύου και υπηρεσιών που δεν ήταν διαθέσιμες προηγουμένως ή δεν μπορούσαν να λειτουργήσουν αξιόπιστα. Τα δίκτυα 5ης γενιάς υποστηρίζουν αμφίδρομα μεγάλο εύρος ζώνης με ρυθμούς δεδομένων >1.0 Gbps με προτεινόμενο φάσμα 3 έως 300GHz με βελτιωμένη ενεργειακή απόδοση για τις διασυνδεδεμένες συσκευές. Τα δίκτυα πέμπτης γενιάς θα αποτελέσουν το όχημα για ένα πραγματικό διαδίκτυο των πραγμάτων, στοχεύοντας στην επέκταση της έννοιας του διαδικτύου, επιτρέποντας την εύκολη αλληλεπίδραση με μια μεγάλη ποικιλία συσκευών, όπως οικιακές συσκευές, κάμερες παρακολούθησης, φωτεινοί σηματοδότες, οχήματα. Ειδικότερα η κατηγορία οχήματα περιλαμβάνει αναδυόμενες έννοιες όπως αυτόνομα οχήματα, δίκτυα οχημάτων, διαχείριση κυκλοφορίας, έλεγχος κυκλοφοριακής συμφόρησης, βιώσιμη κινητικότητα, τα οποία υπάγονται στα Ευφυή Συστήματα Μεταφορών (ITS). Σημαντικά ζητήματα που προκύπτουν στην εφαρμογή του 5G είναι η υποδομή, που καθορίζει το κόστος και η ασφάλεια και προστασία της ιδιωτικής ζωής των χρηστών.



Σχήμα 1: Evolution of Mobile Communication, from 1G to 5G

Η καινοτομία σε όλους τους τομείς, συμπεριλαμβανομένης της κατασκευής, των δεξιοτήτων οδήγησης και της ασφάλειας, είναι γνωστή στην αυτοκινητοβιομηχανία. Ως αποτέλεσμα, όλες οι μεγάλες μάρκες στοχεύουν στην κατασκευή εξυπνότερων και καλύτερα συνδεδεμένων οχημάτων, τα οποία αναμενόταν να φτάσουν τα 250 εκατομμύρια έως το 2020[23].

Το 5G αποτελεί καταλύτη και επιταχυντή για τα κοινωνικά οφέλη των συνδεδεμένων, κοινόχρηστων και ηλεκτρικών οχημάτων και στο μέλλον θα καταστεί ένας από τους κεντρικούς πυλώνες στην ανάπτυξη αυτόνομων οχημάτων. Εκτιμάται ότι μέχρι το 2035, η τεχνολογία 5G θα αποφέρει περισσότερα από 2,4 τρισεκατομμύρια δολάρια σε

[23] Gartner Research—Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities. 2015. Available online: https://www.gartner.com/en/newsroom/press-releases/2015-01-26-gartner-says-by-2020-a-quarter-billion-connected-vehicles-will-enable-new-in-vehicle-services-and-automated-driving- capabilities.

οικονομική παραγωγή στον ευρύτερο τομέα της αυτοκινητοβιομηχανίας, που είναι σχεδόν το 20% του αναμενόμενου παγκόσμιου αντίκτυπου του 5G.

3.2 Μοντέλα Επικοινωνιών για Οχήματα

Οι τεχνολογίες Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) και Vehicle-to-Everything (V2X) προσπαθούν να δώσουν μοντέλα επικοινωνίας που μπορούν να χρησιμοποιηθούν από οχήματα σε διαφορετικά περιβάλλοντα εφαρμογής. Η υποδομή που προκύπτει είναι ένα ad-hoc δίκτυο πλέγματος του οποίου οι κόμβοι δεν είναι μόνο οχήματα αλλά και όλες οι κινητές συσκευές εξοπλισμένες με ασύρματες μονάδες. Η αλληλεπίδραση μεταξύ των πολλαπλών συνδεδεμένων οντοτήτων συνίσταται στην ανταλλαγή πληροφοριών μέσω της υιοθέτησης κατάλληλων πρωτοκόλλων επικοινωνίας.

Ωστόσο, τα συστήματα αυτά πρέπει να είναι σε θέση να συνεργάζονται, για παράδειγμα, επιτρέποντας την αμφίδρομη επικοινωνία μεταξύ των οχημάτων. Η αλληλεπίδραση μεταξύ των διαφόρων εμπλεκόμενων οντοτήτων απαιτεί την ανταλλαγή πληροφοριών για τη χρήση κατάλληλων πρωτοκόλλων επικοινωνίας, όπως τα πρότυπα IEEE 802.11p και LTE-V2V, τα οποία έχουν σχεδιαστεί για την υποστήριξη ασύρματης μετάδοσης δεδομένων μεταξύ των οχημάτων. Αναλυτικότερα, το πρότυπο IEEE 802.11p είναι μια εγκεκριμένη τροποποίηση του προτύπου IEEE 802.11 για την προσθήκη ασύρματης πρόσβασης σε περιβάλλοντα οχημάτων (WAVE)[24], ένα σύστημα επικοινωνίας οχημάτων που υποστηρίζει εφαρμογές Intelligent Transportation Systems (ITS). Αυτό περιλαμβάνει την ανταλλαγή δεδομένων υψηλής ταχύτητας μεταξύ οχημάτων (V2V), μεταξύ των οχημάτων και της οδικής υποδομής (V2I), τη λεγόμενη επικοινωνία οχημάτων προς όλα(V2X), στην αδειοδοτημένη ζώνη ITS των 5,9 GHz (5,85–5,925 GHz). με τον συντονισμό και τη συνεργασία μεταξύ οχημάτων και υποδομών. Το πρότυπο IEEE 802.11p παρέχει ρυθμό δεδομένων που κυμαίνεται από 6 Mbps έως 27 Mbps σε μικρή απόσταση ραδιοφωνικής μετάδοσης, περίπου 300 m.

Ο κύριος στόχος όλων των αναφερόμενων προτύπων είναι η μείωση των χρόνων σύνδεσης και η επέκταση του εύρους μετάδοσης, επιτρέποντας τη σωστή λειτουργία σε συνθήκες υψηλής κινητικότητας και πυκνότητας οχημάτων με πρωταρχικό σκοπό αυτών των τεχνολογιών να είναι η βελτίωση της οδικής ασφάλειας, προσπαθώντας να αποτρέψουν τυχόν επικίνδυνες καταστάσεις. Σε αυτό το πλαίσιο, οι τεχνολογίες V2V (Όχημα προς Όχημα), V2I (Όχημα προς Υποδομή) και V2X (Όχημα προς Όλα) σκοπεύουν να παρέχουν μοντέλα επικοινωνίας που μπορούν να χρησιμοποιούνται από οχήματα σε διαφορετικά πλαίσια εφαρμογής. Η υποδομή που προκύπτει είναι ένα ad-hoc δίκτυο πλέγματος του οποίου οι κόμβοι δεν είναι μόνο οχήματα, αλλά όλες οι κινητές συσκευές εξοπλισμένες με ασύρματη μονάδα.

3.3 Συνεργατικά Ευφυή Συστήματα Μεταφορών (C-ITS)

Τα Συνεργατικά Ευφυή Συστήματα Μεταφορών (C-ITS) έχουν φέρει μια τεχνολογική επανάσταση, ειδικά για τα επίγεια τροχήλατα οχήματα, όσον αφορά την οδική ασφάλεια, την αποτελεσματικότητα της κυκλοφορίας, καθώς και την εμπειρία των οδηγών και των επιβατών. Μέχρι στιγμής, αυτές οι εξελίξεις επικεντρώθηκαν σε

[24] Wireless Access in Vehicular Environments

παραδοσιακά μέσα μεταφοράς, αφήνοντας στην άκρη τη νέα γενιά προσωπικών οχημάτων όπως τα ποδήλατα τις μοτοσικλέτες, συσκευές προσωπικής κινητικότητας όπως τα segways ή τα ηλεκτρικά σκούτερ. Η ανάπτυξη ενός τέτοιου οικοσυστήματος θα χρειαστεί τη συνδρομή νέων αναπτυσσόμενων τεχνολογιών όπως τα δίκτυα 5ής γενιάς (5G networks), και Internet of Things (IOT).

3.4 Ευφυή Συστήματα Μεταφορών και 5G

Σε αναπτυγμένες οικονομίες ανά την υφήλιο, ο κλάδος των μεταφορών αντιστοιχεί περίπου στο 6% έως 12% του Ακαθάριστου Εγχώριου Προϊόντος (ΑΕΠ)[25]. Το 2010, περίπου ένα δισεκατομμύριο οχήματα είχαν παραχθεί, και έως το 2030, προβλέπεται ότι αυτός ο αριθμός θα διπλασιαστεί, δημιουργώντας συνθήκες συμφόρησης στο δίκτυο των μεταφορών με αποτέλεσμα ο ρυθμός των περίπου 1,3 εκατομμυρίων θανάτων ετησίως από τροχαία ατυχήματα να προβλέπεται να φθάσει σε 1,8 εκατομμύρια έως το 2030.

Ο πυρήνας των Ευφυών Συστημάτων Μεταφορών (ITS) είναι η αντιμετώπιση των προκλήσεων στον τομέα των μεταφορών. Τα ITS στοχεύουν στην παροχή καινοτόμων υπηρεσιών, με την χρήση των αναδυόμενων τεχνολογιών, που σχετίζονται με τις διάφορες μορφές μεταφοράς και την δυναμική διαχείριση της κυκλοφορίας. Συνεπώς, τα ITS διαθέτουν ένα ευρύ φάσμα λειτουργιών που σχετίζονται με κρίσιμους τομείς του κλάδου των μεταφορών όπως είναι η ασφάλεια, η βιώσιμη κινητικότητα, η κυκλοφοριακή συμφόρηση, και το ενεργειακό αποτύπωμα του κλάδου στο περιβάλλον με την μείωση της κατανάλωσης ενέργειας.

Το 5G προβλέπεται να συνδέσει μεμονωμένα οχήματα αναπτύσσοντας συνεργατικά ευφυή συστήματα μεταφορών (C-ITS). Το C-ITS με την υποστήριξη δικτύων 5ης γενιάς μπορούν να μετατρέψουν τις πόλεις σε έξυπνες και να προσκομίσουν στα αυτοματοποιημένα συστήματα μεταφορών μεγαλύτερη ασφάλεια και αποδοτικότητα από τα υφιστάμενα δίκτυα μεταφορών. Αυτό συμβάλλει επίσης στην αντιμετώπιση θεμελιωδών προβλημάτων στον κλάδο των μεταφορών που συναντιούνται στους μεγάλους αστικούς ιστούς, όπως της κυκλοφοριακής συμφόρησης, της επιβάρυνσης του περιβάλλοντος με ρύπους και των τροχαίων ατυχημάτων. Με ένα ολοκληρωμένο σύστημα διαχείρισης που αξιοποιεί δεδομένα που έχουν συλλεγεί και αξιοποιηθεί από συνδεδεμένα οχήματα, υποδομές του οδικού δικτύου και διασυνδεδεμένες συσκευές, μπορεί να βοηθήσει στη λήψη ορθότερων παρεμβάσεων για την βελτιστοποίηση της κυκλοφορίας των οχημάτων, την διαχείριση καυσίμου και χρόνου, κ.λπ. Οι πρώτες δοκιμές με τα C-ITS οδήγησαν σε αύξηση της αποτελεσματικότητας του φόρτου εργασίας κατά 20% και μείωση των ατυχημάτων μαζί με την κυκλοφοριακή συμφόρηση κατά 15%[26].

Το 2017, η Alibaba Cloud κυκλοφόρησε το "Urban Brain 1.0". Στο σύστημα 1.0, ο εγκέφαλος της πόλης μπορεί να ελέγξει τα φώτα σηματοδότησης και τις κάμερες, μέσω του μηχανισμού αυτόματης αναγνώρισης του συστήματος, μέσω της πλατφόρμας βελτιστοποίησης ελέγχου φωτός σήματος Internet + που βασίζεται σε AI, έτσι ώστε να ενημερώνει τους διαχειριστές της κυκλοφορίας για την κατάσταση της πόλης με την έξυπνη αποστολή πληροφοριών. Μετά από περισσότερο από ένα χρόνο εφαρμογής, τα δεδομένα πιλοτικού πειράματος της Alibaba στην περιοχή Xiaoshan του Hangzhou με

[25] Rodrigue, J.-P. (2016). The Geography of Transport Systems (4th ed.). Routledge. https://doi.org/10.4324/9781315618159

[26] Alibaba Cloud: 'City Brain' Lowers Traffic Congestion Rate by 15% in Sichuan Province. Available online: https://equalocean. com/news/2020082614640

τη χρήση τεχνητής νοημοσύνης για τον εντοπισμό σφαλμάτων στα φανάρια δείχνουν ότι η ταχύτητα των οχημάτων έχει αυξηθεί κατά περίπου 11%. Επωφελούμενη από τον «αστικό εγκέφαλο», η αποδοτικότητα της κυκλοφορίας του Hangzhou συνέχισε να βελτιώνεται, πέφτοντας από την 5η πιο συμφορημένη πόλη της χώρας στην 50η θέση. Από τότε, Alibaba Cloud ET City Brain έχει προσγειωθεί διαδοχικά σε 11 πόλεις, συμπεριλαμβανομένων των Hangzhou, Quzhou, Wuzhen, Suzhou, Chongqing, Macau και Kuala Lumpur. Το 2018, η Alibaba Cloud κυκλοφόρησε το Hangzhou "Urban Brain 2.0". Το "Urban Brain 2.0" καλύπτει συνολικά 420 τετραγωνικά χιλιόμετρα στην κύρια αστική περιοχή του Hangzhou, Yuhang District και Xiaoshan District.

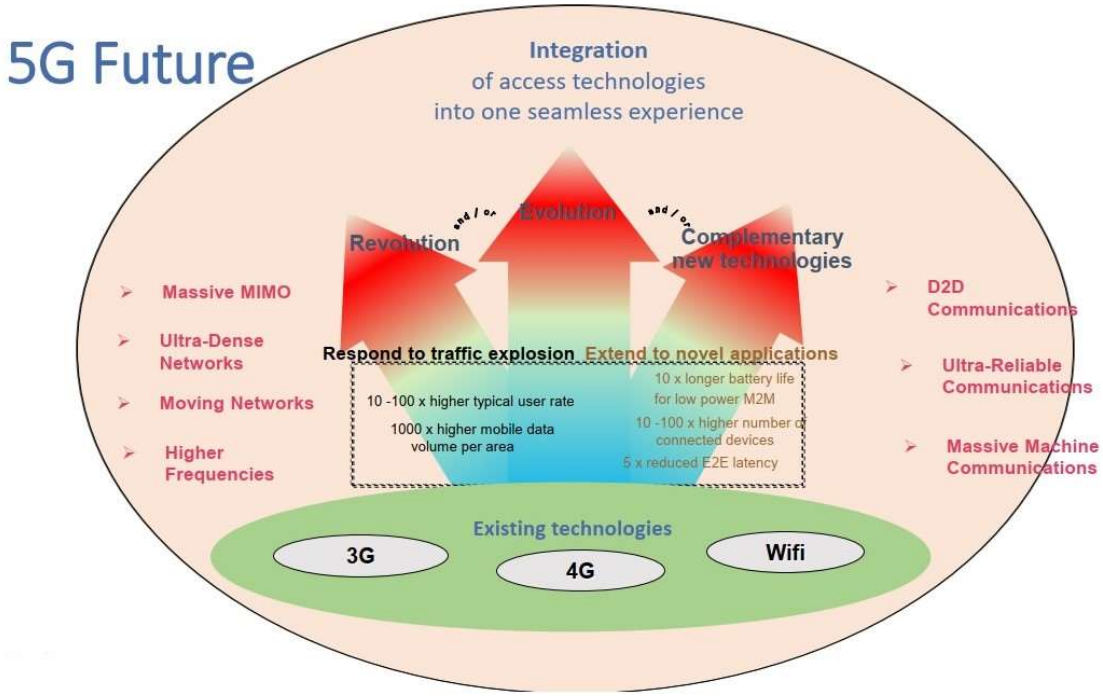
3.5 Η σημασία του 5G στα C-ITS

Με την συνεχόμενη αύξηση των διασυνδέσεων ανθρώπων και πραγμάτων, η κυκλοφορία δεδομένων έχει αυξηθεί δραματικά, ασκώντας πίεση στη σημερινή γενιά ασύρματων κινητών επικοινωνιών. Ως αποτέλεσμα της μεγάλης ανάπτυξης του αριθμού των συνδεδεμένων συσκευών, της κίνησης δεδομένων κινητής τηλεφωνίας και των ορίων των τεχνολογιών 4G, οι επιχειρήσεις και οι ακαδημαϊκοί επικεντρώνουν τις προσπάθειές τους στον καθορισμό των προτύπων για την πέμπτη γενιά (5G) της ασύρματης κινητής επικοινωνίας.

Η κυψελοειδής συνδεσιμότητα είναι απαραίτητη στο έξυπνο σύστημα μεταφορών. Το 5G προσανατολίζεται στη σύνδεση μεμονωμένων αυτοκινήτων μέσω της ανάπτυξης συνεργατικών ευφυών συστημάτων μεταφορών (C-ITS). Το 5G μπορεί να βοηθήσει τις πόλεις να γίνουν πιο έξυπνες, καθιστώντας τα αυτοματοποιημένα συστήματα μεταφορών ασφαλέστερα και αποδοτικότερα από τα υπάρχοντα δίκτυα μεταφορών. Αυτό βοηθά επίσης το σύστημα δημόσιων μεταφορών να αντιμετωπίσει σημαντικά προβλήματα μεταφορών, όπως η κυκλοφοριακή συμφόρηση, η ρύπανση και τα ατυχήματα. Το 5G έχει τη δυνατότητα να ξεπεράσει αυτές τις δυσκολίες δημιουργώντας ένα πραγματικά έξυπνο σύστημα μεταφορών με πρόσβαση σε Internet υψηλής ταχύτητας στα μέσα μαζικής μεταφοράς έχει τη δυνατότητα να συλλέγει και να αναλύει δεδομένα σε πραγματικό χρόνο από συνδεδεμένα αυτοκίνητα, υποδομές και συσκευές για να βοηθήσει στη λήψη επιχειρησιακών αποφάσεων, στη βελτιωμένη πλοήγηση, στη βελτιστοποίηση των πόρων καυσίμων και χρόνου και ούτω καθεξής.

Για να υιοθετηθεί σε μεγάλη κλίμακα, το C-ITS θα πρέπει να διευκολύνει την προσθήκη και τη διαχείριση ενός μεγάλου εύρους ετερογενών συσκευών, να επιτρέπει τη μεταφορά δεδομένων με υψηλό ρυθμό και να παρέχει απόκριση σε πραγματικό χρόνο. Για το λόγο αυτό η σημασία του 5G στη υλοποίηση του C-ITS κρίνεται απαραίτητη, καθώς μόνο στα δίκτυα πέμπτης γενιάς μπορούμε να μιλάμε για απόκριση σε πραγματικό χρόνο και τη μεταφορά δεδομένων με υψηλό ρυθμό.

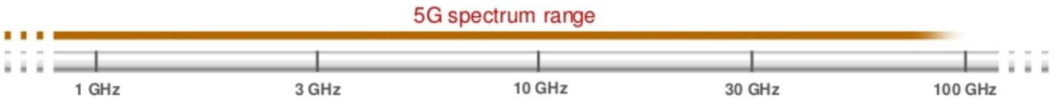
Η πέμπτη γενιά (5G) έχει αναπτυχθεί για την υποστήριξη τριών διαφορετικών υπηρεσιών, την ενισχυμένη ευρυζωνική σύνδεση (eMBB: enhanced mobile broadband), μαζική επικοινωνία συσκευών (mMTC: Massive Machine-type) και την εξαιρετικά αξιόπιστη επικοινωνία χαμηλού λανθάνοντος χρόνου (URLLC: Ultra-reliable and Low Latency). Οι δύο τελευταίες αποτελούν βασικές προϋποθέσεις για τη λειτουργία του Internet of Things (IoT). Σε σχέση με το 4G θα παρέχουν ταχύτατους χρόνους μετάδοσης στοιχείο απαραίτητο για την αξιοπιστίας του V2X και τη δυνατότητα σε ένα τεράστιο αριθμό συσκευών να μεταδίδουν δεδομένα με χαμηλό όγκο, λιγότερη ευαισθησία στην καθυστέρηση και χαμηλή κατανάλωση ενέργειας.



Εικόνα 10: Μελλοντικές τεχνολογίες με τα δίκτυα 5ης γενιάς, Πηγή: Teodor Iliev, New capabilities of 5G network for connected vehicles - the way to totally connected world

Μέχρι στιγμής, τα περισσότερα κινητά συστήματα έχουν αναπτυχθεί μέσα σε ένα ικανοποιητικό φάσμα, λίγο κάτω από 1GHz και λίγο πιο πάνω από 2GHz, με αποτέλεσμα να εκμεταλλεύονται ζώνες των 900MHz, 1800MHz, 1900MHz και 2100MHz. Οι συχνότητες σε αυτό το εύρος διαδίδονται καλά, σε λογικές αποστάσεις και μέσα από τοίχους και άλλα εμπόδια, και τα μήκη κύματος είναι έτσι διαμορφωμένα ώστε οι κεραίες να μπορούν να φτιάχνονται με διαστάσεις που να ταιριάζουν μέσα σε μια κανονική κινητή συσκευή. Αντίθετα, οι υψηλότερες συχνότητες διαδίδονται λιγότερα καλά και οι χαμηλότερες συχνότητες απαιτούν μεγαλύτερες κεραίες. Καθώς υπάρχει ανάγκη για μεγαλύτερη χωρητικότητα, τα δίκτυα κινητής τηλεφωνίας μπορούν να ωφεληθούν από την απελευθέρωση περισσότερους φάσματος εντός των αναφερθέντων συχνοτήτων. Συνεπώς, είναι πιθανό, οι τρείς ευρείς κατηγορίες φάσματος που θα χρησιμοποιηθούν στα 5G δίκτυα να είναι οι εξής:

1. Χαμηλές συχνότητες, κάτω από 1GHz για κάλυψη αγροτικών περιοχών και κάλυψη εντός κτηρίων.
2. Βασικές συχνότητες, από περίπου 1GHzέως 6GHz, για γενική κάλυψη και χωρητικότητα, με τις υψηλές συχνότητες να χρησιμοποιούνται για την χωρητικότητα των hot-spots.
3. Υψηλές συχνότητες, από 6GHz έως δεκάδες GHz, για υψηλή χωρητικότητα σε περιοχές πυκνής χρήσης, όπως για παράδειγμα σε πανεπιστημιουπόλεις και μέσων μαζικής μεταφοράς.



Εικόνα2. Φάσμα5G

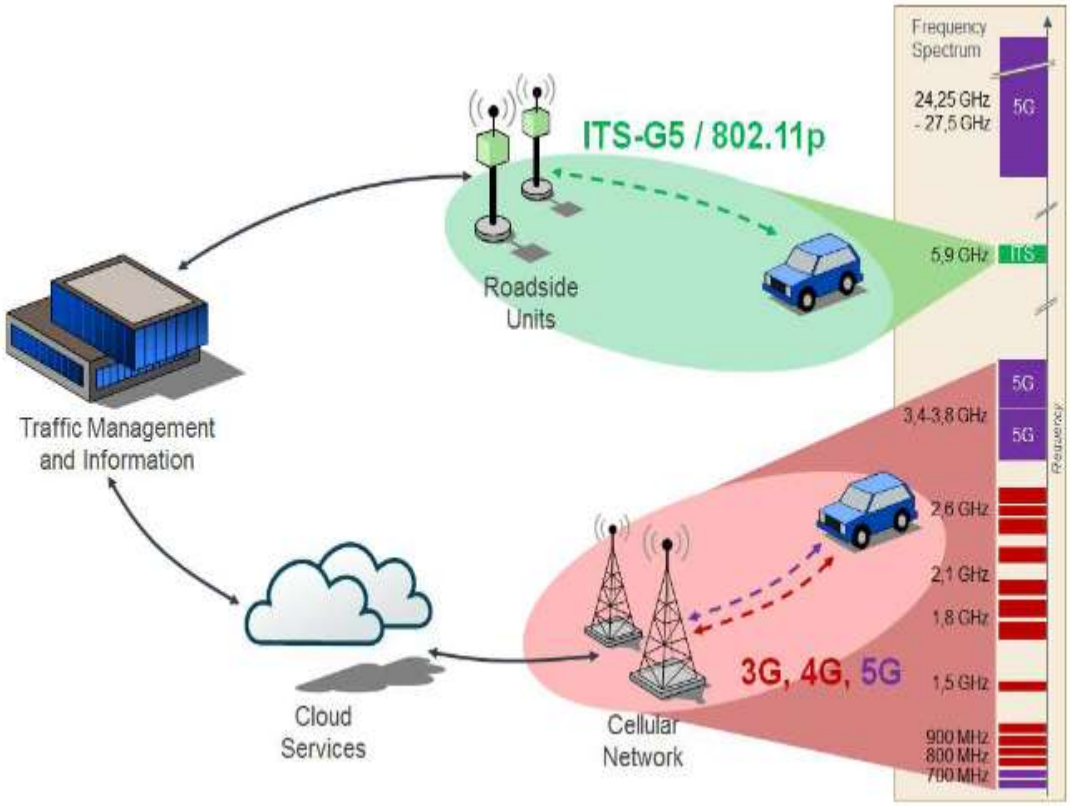
(πηγή: "5G Concept Ericsson, EAB-14:068423")

3.6 Συνεργατικά Ευφυή Συστήματα Μεταφορών στην Ευρώπη

Το 2008, η Ευρώπη όρισε με την απόφαση (2008/671/ΕΚ)[27] τα 30MhZ στη ζώνη των 5,9 GHz για την αύξηση της οδικής ασφάλειας και αποδοτικότητας, με τη διαθέσιμη ζώνη συχνοτήτων να έχει χωριστεί σε κανάλια επικοινωνίας 10 MHz, όπου το κανάλι ελέγχου (CCH) μεταξύ 5.895 και 5.905 GHz θα μεταφέρει δεδομένα κυκλοφορίας για αύξηση της ασφάλειας.

Ωστόσο, η συνεχής εξέλιξη των συστημάτων μεταφορών και ο αυξανόμενος αριθμός υπηρεσιών ασφάλειας που παρέχουν απαιτούν πρόσθετους πόρους φάσματος. Η νέα απόφαση (2020/1426)[28] η οποία καταργεί την (2008/671/ΕΚ) διπλασιάζει το επίπεδο του διαθέσιμου φάσματος στα 60MHz. Η κατανομή περισσότερου ραδιοφάσματος για τις μεταφορές θα υποστηρίξει την ανάπτυξη πλήρους κλίμακας συνδεδεμένων και αυτοματοποιημένων μεταφορών διευκολύνοντας την ανταλλαγή πληροφοριών σε πραγματικό χρόνο μεταξύ οχημάτων και οδικών υποδομών. Αυτό το φάσμα θα χρησιμοποιείται αποκλειστικά για την άμεση επικοινωνία, V2V και V2I.

[27] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32008D0671&from=EN
[28] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32020D1426&from=en



Εικόνα 11 Τρέχουσα κατανομή ζωνών συχνοτήτων που είναι διαθέσιμες για υπηρεσίες C-ITS. Πηγή: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/C-Roads_Position_paper_on_59GHz_final.pdf

Για την επίτευξη της διαλειτουργικότητας της επικοινωνίας μεταξύ των εφαρμογών διαφορετικών κατασκευαστών, η τυποποίηση διαδραματίζει σημαντικό ρόλο. Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) έχει αναπτύξει για τα ITS πρότυπα για την υποστήριξη εφαρμογών C-ITS από την πρώτη μέρα, εστιάζοντας σε πρωτόκολλα που υποστηρίζουν εφαρμογές για τα οχήματα. Πρωτόκολλα που υποστηρίζουν εφαρμογές που εκτελούνται σε έξυπνες υποδομές, όπως οι φωτεινοί σηματοδότες, έχουν αναπτυχθεί από την Ευρωπαϊκή Επιτροπή Τυποποίησης (CEN) TC 278.

Η τυποποίηση αποτελεί τη βάση για την ανάπτυξη το V2X θα αξιοποιηθεί μόνο εάν δημιουργηθεί ένα διαλειτουργικό σύστημα, πάνω στο οποίο κατασκευαστές αρχικού εξοπλισμού (OEM) θα σχεδιάζουν τις συσκευές τους, οι οποίες θα επικοινωνούν με τις υποδομές.

Καθώς ο πληθυσμός στις αστικές περιοχές συνεχίζει να αυξάνεται, οι ηλεκτρονικές υπηρεσίες στα μέσα μεταφοράς γίνονται ολοένα και πιο επιτακτικές. Η αξιοπιστία των συστημάτων είναι καίριας σημασίας για την εμπιστοσύνη των πολιτών σε ένα οικοσύστημα (Smart transportation) που θα διασυνδέει τους ίδιους, με εφαρμογές αστικής κινητικότητας. Στα συνεργατικά μοντέλα ευφυών συστημάτων μεταφορών (C-ITS), τα οχήματα είναι σε θέση να επικοινωνούν μεταξύ τους (Vehicle-to-Vehicle, V2V) αλλά και με τις υποδομές στο περιβάλλον τους (Vehicle-to-Infrastructure, V2I). Οι καινοτόμες εξελίξεις στον κλάδο των τηλεπικοινωνιών με τα νέα δίκτυα 5ης γενιάς (5G) διαθέτουν τα απαραίτητα χαρακτηριστικά για την εφαρμογή των παραπάνω

καινοτόμων τεχνολογιών. Ωστόσο, είναι γεγονός ότι αυτές οι εξελίξεις έχουν αφιερωθεί στα παραδοσιακά οχήματα, αγνοώντας επομένως τις προαναφερθείσες αναδυόμενες επιλογές προσωπικής κινητικότητας που μεταμορφώνουν το τοπίο των αστικών σεναρίων. Πολλοί πολίτες χρησιμοποιούν επί του παρόντος προσωπικά οχήματα όπως ποδήλατα, σκούτερ ή ηλεκτρικές μοτοσικλέτες, λόγω των ελκυστικών οικολογικών χαρακτηριστικών τους και της προώθησης βιώσιμου και υγιούς τρόπου ζωής.

3.7 Θέματα ασφαλείας στα δίκτυα 5G και προκλήσεις V2X - 5G

Η εισαγωγή υπηρεσιών και συσκευών πρόκειται να επηρεάσει την ασφάλεια στο περιβάλλον 5G και να εγείρει ζητήματα ιδιωτικότητας.

Τα τεχνολογικά μέτρα ασφαλείας, όπως ρυθμίζονται στον ΓΚΠΔ, περιλαμβάνουν την ψευδωνυμοποίηση, την ανωνυμοποίηση, και ταυτόχρονα τη μέθοδο κρυπτογράφησης. Οι αρχές της προστασίας δεδομένων του ΓΚΠΔ δεν εφαρμόζονται σε ανώνυμα δεδομένα, τα οποία δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Όσον αφορά τα ψευδωνυμοποιημένα δεδομένα, είναι ασφαλή εάν δεν μπορούν να αποδοθούν σε φυσικό πρόσωπο.

Τα δίκτυα 5G απαιτούν ολοκληρωμένα μέτρα για την εκπλήρωση των απαιτήσεων του GDPR, τα πρότυπα 3GPP 5G ορίζουν ότι τα αναγνωριστικά χρήστη κρυπτογραφούνται ασύρματα και πραγματοποιείται κρυπτογράφηση και προστασία ακεραιότητας από άκρη σε άκρη (end to end) στον δίαυλο μετάδοσης με στόχο τη διασφάλιση δεδομένων προσωπικού χαρακτήρα από τυχαία, μη εξουσιοδοτημένη ή παράνομη πρόσβαση, χρήση, τροποποίηση, αποκάλυψη, απώλεια, καταστροφή ή φθορά.

Οι απαιτήσεις ασφάλειας και απορρήτου της ομάδας εργασίας 3GPP SA314 στην τελευταία έκδοση (18)[29] 3GPP TS 33.501 για 5G είναι:

α) Εμπιστευτικότητα δεδομένων χρήστη και δεδομένων μετάδοσης,

β) Ακεραιότητα δεδομένων χρήστη και δεδομένων μετάδοσης,

γ) ασφαλής αποθήκευση και επεξεργασία των διαπιστευτηρίων συνδρομής και

δ) απόρρητο συνδρομητή

τα παραπάνω χαρακτηριστικά ασφαλείας δεν θα ενεργοποιηθούν όλα από προεπιλογή στον εξοπλισμό δικτύου, καθώς ορισμένα από αυτά είναι προαιρετικά για εφαρμογή για τους προμηθευτές ή για χρήση από τους επιχειρηματίες. Ως εκ τούτου, η αποτελεσματικότητα αυτών των χαρακτηριστικών ασφαλείας εξαρτάται από τον τρόπο με τον οποίο οι φορείς εκμετάλλευσης επιβάλλουν και διαχειρίζονται τα δίκτυά τους. Το Ευρωπαϊκό Συμβούλιο αναγνώρισε την ανάγκη θέσπισης ισχυρών κοινών προτύπων και μέτρων ασφαλείας, με έμφαση στην προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό, λαμβάνοντας υπόψη τα διεθνή πρότυπα για το 5G[30].

Παρά τη μεγάλη επιτυχία του 5G-V2X στην ανάπτυξη της επόμενης γενιάς ευφυών δικτύων οχημάτων μέσω της ενσωμάτωσης λογισμικών και μεθόδων απεικόνισης των λειτουργιών του δικτύου, η ασφάλεια της συνολικής αρχιτεκτονικής εξακολουθεί να

29 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

30 Council of the European Union, Brussels, Belgium. (Dec. 3, 2019). Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G-Council Conclusions (14517/19). [Online]. Available: https://www.consilium. europa.eu/en/press/press-releases/2019/12/03/significance-and-security- risks-of-5g-technology-council-adopts-conclusions/

είναι αμφισβητήσιμη. Αυτή η παραδοχή μπορεί να επηρεάσει αρνητικά την ασφάλεια του δικτύου και ανοίγει πόρτες για διάφορες νέες προκλήσεις για την ασφάλεια πλατφορμών 5G-V2X που διαχειρίζονται εικονικούς πόρους και τις σχέσεις τους με το επίπεδο εφαρμογής για ένα πλήρως αξιόπιστο σύστημα. Σύμφωνα με τους Hussain και Zeadally[31], η ασφάλεια είναι μία από τις κρίσιμες προκλήσεις που χρειάζονται περαιτέρω διερεύνηση για να διασφαλιστεί η απρόσκοπτη ενσωμάτωση της τεχνολογίας 5G με το VANET. Στο πλαίσιο του 5G, τεχνολογίες όπως το SDN και η εικονικοποίηση δικτύου (network virtualization) έχουν επεκτείνει το φάσμα των τρωτών σημείων ασφαλείας. Από τη μία πλευρά, το VANET που βασίζεται στο SDN έχει σχεδιαστεί χωρίς να θεωρείται η ασφάλεια ως κορυφαία προτεραιότητα. Συγκεκριμένα, οι ελεγκτές SDN μπορούν να στοχοποιηθούν από διάφορες επιθέσεις. Η ευελιξία που παρέχεται από τις διεπαφές προγραμματισμού εφαρμογών (API) μεταξύ διαφορετικών επιπέδων μπορεί επίσης να αξιοποιηθεί για την παραγωγή καταστροφικού malware για να πάρει τον έλεγχο ολόκληρου του συστήματος.

3.8 Προκλήσεις στο Πεδίο της Ασφάλειας και Λειτουργίας για τα C-ITS

Η ασφάλεια είναι ένας κρίσιμος παράγοντας επιτυχίας για την υιοθέτηση του C-ITS. Αυτό έχει ωθήσει αρκετές προσπάθειες τόσο από τη βιομηχανία όσο και από τον ακαδημαϊκό χώρο για να επιτρέψουν και να βελτιώσουν την ασφάλεια εντός του τομέα C-ITS. Οι οργανισμοί τυποποίησης, όπως το Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών (ETSI), έχουν καθορίσει κατευθυντήριες γραμμές για το σχεδιασμό και την ανάπτυξη ασφαλών υπηρεσιών για το C-ITS. Συγκεκριμένα, το ETSI έχει εντοπίσει βασικές ασφαλείς λειτουργίες που πρέπει να παρέχονται από το C-ITS, συμπεριλαμβανομένης της αναγνώρισης (identification), του ελέγχου ταυτότητας (authentication), της εξουσιοδότησης (authorization) και της εγγραφής – συνδρομής (enrolment).

Δυναμική: Τα C-ITS είναι πολύπλοκα και δυναμικά συστήματα στα οποία συνδέεται ένας αυξανόμενος αριθμός οντοτήτων (π.χ. οχήματα, RSU) και στα οποία η τοπολογία του δικτύου και η συνδεσιμότητα αλλάζουν συνεχώς με την πάροδο του χρόνου.

Διαχείριση: Η δυναμικότητα του οικοσυστήματος C-ITS μπορεί επίσης να επηρεάσει αποτελεσματικά το policy management (διαχείριση πολιτικών και διαδικασιών). Σε τέτοια συστήματα, οι διαθέσιμες πληροφορίες μιας οντότητας μπορούν να αποθηκευτούν και να διαχειριστούν από διαφορετικούς παρόχους που αλληλεπιδρούν μεταξύ τους. Επομένως, ένα πλαίσιο εξουσιοδότησης θα πρέπει να μπορεί να υποστηρίζει τη διαχείριση των πολιτικών ελέγχου πρόσβασης για συσκευές και πληροφορίες σε πολλούς παρόχους.

Αυτοματισμός: Ένα κύριο χαρακτηριστικό του C-ITS είναι η συνεργασία, η οποία επιτυγχάνεται μέσω αλληλεπιδράσεων μεταξύ οντοτήτων που εμπλέκονται στο C-ITS (π.χ. οχήματα, RSUs). Αυτές οι αλληλεπιδράσεις περιλαμβάνουν την ανταλλαγή κρίσιμων πληροφοριών ασφάλειας σε πραγματικό χρόνο.

Απόδοση: Το C-ITS είναι συστήματα στα οποία η καθυστέρηση είναι κρίσιμη και μπορεί να έχει σοβαρές συνέπειες που μπορεί να οδηγήσουν ακόμη και σε απώλεια ανθρώπινης ζωής. Επομένως, οι υπηρεσίες που αναπτύσσονται εντός του C-ITS δεν

[31] R. Hussain, F. Hussain, and S. Zeadally, ``Integration of VANET and 5G security: A review of design and implementation issues," Future Gener. Comput. Syst., vol. 101, pp. 843-864, Dec. 2019.3112-201812-I

πρέπει να περιέχουν καθυστέρηση τόσο από άποψη υπολογισμού όσο και από άποψη επικοινωνίας μεταξύ των οντοτήτων.

Αξιοπιστία: Ο κρίσιμος χαρακτήρας του C-ITS θέτει επίσης υψηλές απαιτήσεις για συνέχεια του επιχειρησιακού έργου, ακόμη και σε περιπτώσεις βλάβης του συστήματος. Από την άλλη πλευρά, οι εξαιρετικά ευαίσθητες πληροφορίες που συλλέγονται και ανταλλάσσονται εντός του C-ITS απαιτούν προστασία και η αποκάλυψή τους σε μη εξουσιοδοτημένα μέρη πρέπει να αποφευχθεί.

3.9 Mobility-as-a-Service (Η κινητικότητα ως υπηρεσία)

Το Mobility-as-a-Service (MaaS) ως ολοκληρωμένη έννοια λειτουργική και αξιόπιστη, βρίσκεται στα αρχικά στάδια της ανάπτυξης, περισσότερο ως φιλοσοφία παρά ως εφαρμογή πλήρους κλίμακας, ωστόσο είναι ιδιαίτερα δημοφιλής λόγω των αποτελεσμάτων που μπορούν να επιτευχθούν στο τοπίο της βιώσιμης κινητικότητας, ιδιαίτερα στα μεγάλα αστικά κέντρα. Στόχος του MaaS στο μέλλον είναι η προσφορά ψηφιακών πακέτων εξατομικευμένης πολυτροπικής κινητικότητας που θα αντικαταστήσουν τα ιδιόκτητα οχήματα μέσω της χρήσης μιας έξυπνης διαδικτυακής πλατφόρμας, ικανής να παρέχει ολοκληρωμένο σχεδιασμό ταξιδιού, κρατήσεις, έξυπνα εισιτήρια και πραγματικές υπηρεσίες πληροφόρησης. Εάν το MaaS εδραιωθεί ως πραγματικό υποκατάστατο της ιδιωτικής ιδιοκτησίας αυτοκινήτων και μετατρέψει τη χρήση του αυτοκινήτου σε υπηρεσία που παρέχεται αυστηρά, ανάλογα με τις ανάγκες των μετακινουμένων, έχει τη δυνατότητα να μειώσει δραματικά τον αριθμό των αυτοκινήτων στους δρόμους και έτσι να μειώσει σημαντικά τις καθυστερήσεις στις μετακινήσεις, την ατμοσφαιρική ρύπανση, την ηχορύπανση, την κατανάλωση ενέργειας και τον κοινωνικό αποκλεισμό που συνδέεται με τις μεταφορές. Το MaaS θα παρέχει συγκριτικά οφέλη σε σχέση με την υπάρχουσα κατάσταση όπως η ασφάλεια των μεταφορών η πρόληψη ατυχημάτων, η υγεία και την ευημερία, η κοινωνική συνοχή, η προσβασιμότητα και οι δαπάνες των ανθρώπων.

3.10 Ο Τεμαχισμός του Δικτύου στο 5G (Network Slicing)

Η επόμενη γενιά επικοινωνιών οχημάτων είναι επιτακτική ώστε να υποστηριχθεί η υψηλή ετερογένεια των στοιχείων του δικτύου και προκειμένου να ικανοποιηθεί η ανάγκη για ασφαλέστερες και άνετες κυκλοφοριακές συνθήκες. Στην πραγματικότητα, με την παραδοσιακή αρχιτεκτονική του δικτύου όπου κάθε υλικό (hardware) προορίζεται αποκλειστικά για κάθε υπηρεσία, θα ήταν εξαιρετικά δύσκολο να εξασφαλιστούν οι αυστηρές απαιτήσεις μεταφοράς υπηρεσιών. Σε αυτό το πλαίσιο, η έννοια των τομέων δικτύου έχει αναδειχθεί ως μια νέα τεχνολογία που στοχεύει σε διαφορετικά πρότυπα τυποποίησης, συμπεριλαμβανομένου του 3rd Generation Partnership Project (3GPP) Έκδοση 16[32], το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI)[33] και το ITU-T (ITU Telecommunication Standardization Sector)[34].

Η τεχνολογία 5G εισάγει τον τεμαχισμό δικτύου, ο οποίος χωρίζει τα παραδοσιακά συστήματα δικτύου με κακή επεκτασιμότητα και ευελιξία σε ανεξάρτητες λειτουργίες

[32] 3GPP. (2020). Release 16. pp. 36. [Online]. Available: https://www.3gpp.org/release-16
[33] ETSI GR NGP 011 V1.1.1: Next Generation Protocols (NGP); E2E Network Slicing Reference Framework and Information Model, ETSI, Sophia Antipolis, France, 2018, pp. 132.
[34] I. T. S. Sector. (2018). Y.3112: Framework for the Support of Network Slicing in the IMT-2020 Network. [Online]. Available: https://www.itu.int/rec/T-REC-Y.

δικτύου και στη συνέχεια τα συνδέει ουσιαστικά σε λογικά δίκτυα με συγκεκριμένες δυνατότητες υπηρεσιών. Ως εκ τούτου, ο τεμαχισμός δικτύου μπορεί να παρέχει ευέλικτα λειτουργίες δικτύου και πόρους σύμφωνα με τις απαιτήσεις διαφορετικών υπηρεσιών. Στις εφαρμογές V2X, υπάρχουν πολλά σενάρια εφαρμογών με διαφορετικές απαιτήσεις για την απόδοση του δικτύου, όπως λανθάνων χρόνος, εύρος ζώνης, ασφάλεια και αξιοπιστία. Η εισαγωγή της τεχνολογίας τεμαχισμού δικτύου μπορεί να παρέχει ευέλικτες υπηρεσίες προσαρμογής από άκρο σε άκρο με μεγάλο εύρος ζώνης, υψηλή αξιοπιστία και χαμηλή καθυστέρηση για υπηρεσίες V2X σε διαφορετικά σενάρια εφαρμογών.

Η δυνατότητα τεμαχισμού του δικτύου είναι ένα βασικό χαρακτηριστικό του 5G. Το Network Slicing δίνει τη δυνατότητα στους παρόχους υπηρεσιών να δημιουργήσουν μια ποικιλία αρχιτεκτονικών τμημάτων δικτύου που παρέχουν απόδοση για τις συνδέσεις τους ή την παράδοση πακέτων προτεραιότητας από συγκεκριμένους τύπους συσκευών ή εφαρμογών. Η έννοια του τεμαχισμού δικτύου έχει αναπτυχθεί για να αντιμετωπίσει τις ποικίλες απαιτήσεις υπηρεσιών των κάθετων βιομηχανιών.

Μέσω του τεμαχισμού δικτύου, η φυσική υποδομή δικτύου μπορεί να χωριστεί σε πολλαπλά εικονικά δίκτυα, επιτρέποντας στους φορείς εκμετάλλευσης να παρέχουν συγκεκριμένους τύπους υποστήριξης για συγκεκριμένες ομάδες χρηστών. Για παράδειγμα, η επικοινωνία μεταξύ οχημάτων απαιτεί υψηλή κινητικότητα και χαμηλό εύρος ζώνης, ενώ η κινητή ευρυζωνική σύνδεση σε σταθερή θέση απαιτεί υψηλό εύρος ζώνης αλλά χαμηλή κινητικότητα. Ο τεμαχισμός δικτύου μπορεί να βοηθήσει τους χειριστές να εκχωρήσουν διαφορετικούς πόρους για διαφορετικές ανάγκες. Μια άλλη σημαντική πτυχή είναι η πολυσυνδεσιμότητα, η οποία μπορεί να υποστηρίξει διαφορετικούς τύπους πρόσβασης από ασύρματες έως βασικές υπηρεσίες από το ίδιο δίκτυο, συμπεριλαμβανομένων των 5G, LTE, Wi-Fi και ακόμη και σταθερής πρόσβασης. Ο τεμαχισμός δικτύου και οι πολλαπλές συνδέσεις διασφαλίζουν ότι το 5G γίνεται μια ενιαία υποδομή δικτύου που μπορεί να καλύψει τις ανάγκες πολλαπλών υπηρεσιών.

Ένα slice είναι μια συλλογή λογικά προσαρμοσμένων λειτουργιών δικτύου που υποστηρίζουν τις απαιτήσεις υπηρεσιών επικοινωνίας συγκεκριμένων περιπτώσεων χρήσης ή επιχειρηματικών μοντέλων.

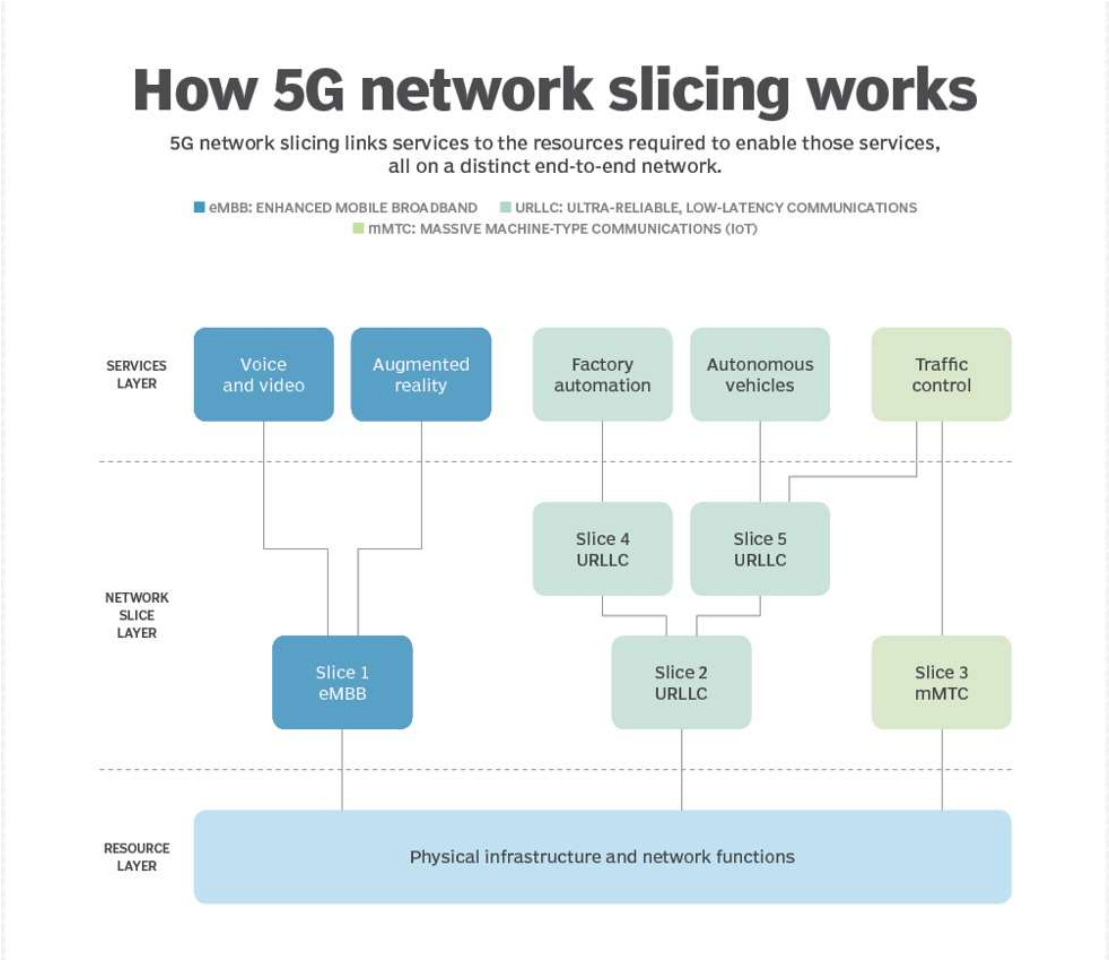
Ένας χειριστής δικτύου 5G μπορεί να τεμαχίσει ένα μεμονωμένο δίκτυο ή να συνδυάσει τη χωρητικότητα πολλαπλών δικτύων και να τεμαχίσει τους συγκεντρωμένους πόρους. Αυτό επιτρέπει στους χειριστές δικτύων 5G να επιλέξουν τα χαρακτηριστικά που χρειάζονται για να υποστηρίξουν τα επίπεδα απόδοσης φάσματος, χωρητικότητας κίνησης και πυκνότητας σύνδεσης, δηλαδή πόσες συσκευές μπορούν να συνδεθούν από έναν δεδομένο χώρο.

Οι τύποι υπηρεσιών 5G που χρησιμοποιούν το Network Slicing περιλαμβάνουν τα ακόλουθα:

Το Enhanced Mobile Broadband, ή eMBB, το οποίο παρέχει πρόσβαση σε δεδομένα κινητής τηλεφωνίας με έναν από τους τρεις τρόπους: σε χρήστες που είναι κατανεμημένοι με μεγάλη πυκνότητα, σε χρήστες που βρίσκονται σε κατάσταση υψηλής κινητικότητας και σε χρήστες που είναι κατανεμημένοι σε μεγάλες περιοχές.

Οι υπηρεσίες Massive Machine-Type Communications, ή mMTC, έχουν δημιουργηθεί για να εξυπηρετούν τεράστιους αριθμούς συσκευών σε μια μικρή περιοχή με στόχο την παραγωγή μικρού όγκου δεδομένων.

Την εξαιρετικά αξιόπιστη επικοινωνία χαμηλού λανθάνοντος χρόνου (URLLC: Ultra-reliable and Low Latency), για την παροχή ασφαλών επικοινωνιών με λανθάνοντες χρόνους 1 χιλιοστού του δευτερολέπτου (ms) και υψηλή αξιοπιστία με χαμηλή ή ακόμα και μηδενική απώλεια πακέτων.



Εικόνα 12 Παράδειγμα τεμαχισμού υπηρεσιών 5G, Πηγή: https://www.techtarget.com/whatis/definition/network-slicing

3.11 Ενσωματωμένα Κινούμενα Δίκτυα

Με το 5G και την εξέλιξή του, οι χρήστες θα αναμένουν ότι η συνδεδεμένη κοινωνία θα είναι διαθέσιμη χωρίς περιορισμούς και οι χρήστες θα χρησιμοποιούν υπηρεσίες περιορισμού εύρους ζώνης, όπως εφαρμογές επαυξημένης πραγματικότητας και virtual office όταν βρίσκονται εν κινήσει. Στο πλαίσιο αυτό, τα μελλοντικά οχήματα και συστήματα μεταφοράς μπορούν να διαδραματίσουν σημαντικό ρόλο στα ασύρματα δίκτυα, παρέχοντας πρόσθετες δυνατότητες επικοινωνίας και αποτελώντας αναπόσπαστο μέρος της υποδομής επικοινωνίας για τη βελτίωση της χωρητικότητας και της κάλυψης των κινητών δικτύων που βασίζονται στους φορείς εκμετάλλευσης.

Δηλαδή, για την αποτελεσματική εξυπηρέτηση των χρηστών οχημάτων, μια πολλά υποσχόμενη λύση είναι η ανάπτυξη κινούμενων σταθμών βάσης στα οχήματα για τη δημιουργία κινούμενων δικτύων.

Εικόνα 13: Απεικόνιση Κινούμενων Δικτύων

Ένας από τους σκοπούς των κινούμενων σταθμών βάσης είναι η αποτελεσματική εξυπηρέτηση των χρηστών εντός του οχήματος, η οποία γίνεται όλο και πιο απαιτητική για υπηρεσίες υψηλού ρυθμού δεδομένων και χαμηλού λανθάνοντος χρόνου.

Τα ενσωματωμένα κινούμενα δίκτυα μπορούν επίσης να επιτρέψουν υπερευαίσθητες συνδέσεις επικοινωνίας για τη μεταφορά μηνυμάτων ITS μεταξύ οχημάτων και κινητών συσκευών των λεγόμενων ευάλωτων χρηστών του οδικού δικτύου, όπως πεζοί, ποδηλάτες, παιδιά που παίζουν στους δρόμους, κατοικίδια ζώα κ.α., που δεν είναι εξοπλισμένα με αισθητήρες` επικοινωνιών για ITS.

3.12 Επιπτώσεις & Μετασχηματισμός στην Οικονομία και την Βιωσιμότητα με τα ITS

Όσον αφορά τη βιωσιμότητα, τα ITS θα έχουν ως αποτέλεσμα τη βελτιστοποίηση των συστημάτων μεταφορών που μειώνουν το χάσιμο χρόνου βελτιστοποιώντας τις διαδρομές, μειώνοντας τη συμφόρηση, τη ρύπανση, τις περιβαλλοντικές επιπτώσεις και βελτιώνοντας την απόδοση των οχημάτων και των οδηγών.

Για τις μεσαίες και μεγάλες πόλεις σε όλο τον κόσμο, οι προκλήσεις της κλιματικής αλλαγής, της αύξησης του πληθυσμού, της δημογραφικής αλλαγής, της αστικοποίησης και της εξάντλησης των πόρων προκαλούν μεγάλη ανησυχία για την επιβίωση, την ανάπτυξη και τη βιωσιμότητα. Σημαντικό μέρος αυτών των ανησυχιών είναι η υποβάθμιση της ποιότητας του περιβάλλοντος, τα προβλήματα της αλλαγής του κλίματος και οι απώλειες βιοποικιλότητας, η κατανάλωση ανανεώσιμων φυσικών

πόρων ταχύτερα από το ρυθμό ανανέωσης, η έκλυση επικίνδυνων αερίων και αερίων του φαινομένου του θερμοκηπίου, εν ολίγοις, προβλήματα που απειλούν την οικολογική και φυσική ισορροπία και υπερθέρμανση του πλανήτη. Η Deloitte (2022) προσδιορίζει πέντε τάσεις που αντιμετωπίζουν τις προκλήσεις που αντιμετωπίζει ο τομέας των μεταφορών ως εξής:

1) Δημιουργία βιώσιμων μηχανισμών χρηματοδότησης για τις μεταφορές,

2) Εξεύρεση λύσεων στο πρόβλημα των Ηλεκτρικών Οχημάτων (EV) και των υποδομών φόρτισης,

3) Εκσυγχρονισμός των συστημάτων μεταφορών με δίκαιο και χωρίς αποκλεισμούς τρόπο,

4) Ενίσχυση της ανθεκτικότητας των δικτύων μεταφορών,

5) Επιτάχυνση της ψηφιακής και τεχνολογικής καινοτομίας (Deloitte, 2022).

Η Ευρωπαϊκή Επιτροπή δημοσίευσε επίσης στις 14 Δεκεμβρίου 2021 πρόταση για μια νέα δέσμη νομοθετικών μέτρων με τίτλο Αποδοτική και πράσινη κινητικότητα, η οποία αποτελεί μέρος της Ευρωπαϊκής Πράσινης Συμφωνίας και αφορά ειδικά τον τομέα των μεταφορών. Η δέσμη αυτή αποσκοπεί στην επίτευξη του στόχου της Ευρωπαϊκής Πράσινης Συμφωνίας για μείωση των εκπομπών από τον τομέα των μεταφορών κατά 90 % μέσω της αύξησης της συνδεσιμότητας στον τομέα των μεταφορών, της στροφής των μεταφορών προς τις σιδηροδρομικές και τις εσωτερικές πλωτές μεταφορές, της βελτίωσης της αποδοτικότητας των πολυτροπικών μεταφορών, της εισαγωγής νέων σημείων φόρτισης, της εισαγωγής νέων ψηφιακών τεχνολογιών, της απόδοσης μεγαλύτερης προτεραιότητας στη βιώσιμη αστική κινητικότητα. Στη νέα νομοθετική πρόταση, η οποία αποτελείται από τέσσερις προτάσεις συνολικά, η Επιτροπή παρουσίασε νέο σχέδιο νομοθεσίας στους τομείς των διευρωπαϊκών δικτύων μεταφορών (ΔΕΔ-Μ) και των ευφυών συστημάτων μεταφορών (ITS), προκειμένου να καταστεί ο ευρωπαϊκός τομέας μεταφορών πιο πράσινος και πιο έξυπνος. Ταυτόχρονα, η Επιτροπή προτείνει νέα νομοθεσία για την τροποποίηση της νομοθεσίας για τα ευφυή συστήματα μεταφορών (ITS) Επίσημη Εφημερίδα της ΕΕ (2010), η οποία ισχύει από το 2010. Η πρόταση αποσκοπεί στην παροχή ταχύτερων έξυπνων υπηρεσιών, στη διάθεση ορισμένων δεδομένων σχετικά με την κυκλοφορία, το οδικό δίκτυο και τις μετακινήσεις σε ψηφιακή μορφή σε ολόκληρο το δίκτυο ΔΕΔ-Μ και στην προώθηση της αυτοματοποίησης των μεταφορών.

Στη Γερμανία τα αυτοματοποιημένα οχήματα θα μπορούσαν να αποτρέψουν περισσότερες από 30.000 συγκρούσεις ή το 70% των οπίσθιων συγκρούσεων έως το 2025, ή 450 εκατομμύρια ευρώ σε εξοικονόμηση κόστους επισκευής και σύγκρουσης, όπως υπολογίστηκε από τον προμηθευτή αυτοκινήτων Bosch[35]. Επιπλέον, τα αυτοματοποιημένα συστήματα οδήγησης έχουν τη δυνατότητα να εξοικονομήσουν στους Γερμανούς μετακινούμενους έως και 95 ώρες ετησίως το οποίο θα εξοικονομήσει 400.000 τόνους CO2 έως το 2025. Ομοίως, η Bosch εκτιμά ότι μέχρι το 2025, τα αυτοματοποιημένα οχήματα στις Ηνωμένες Πολιτείες (ΗΠΑ) κάθε χρόνο μπορούν να σώσουν 4000 ζωές και να αποτρέψουν περισσότερες από 210.000 συγκρούσεις. Αυτή η βελτίωση της ασφάλειας θα μεταφραζόταν σε 3,6 δισεκατομμύρια δολάρια σε εξοικονόμηση κόστους επισκευής για τους πολίτες και τις ασφαλιστικές εταιρείες των ΗΠΑ. Η Εθνική Υπηρεσία Οδικής Ασφάλειας των ΗΠΑ

[35] Fischer, A. My Car, My Hero: What the Connected Vehicle Will Be Capable of Doing on the Streets of the Future. 2017. https://www.automotiveworld.com/news-releases/car-hero-connected-vehicle-will-capable-streets-future/

εκτιμά ότι ο συνδυασμένος αντίκτυπος των τεχνολογιών V2X θα μπορούσε να μετριάσει τη σοβαρότητα έως και 80% των συγκρούσεων πολλαπλών οχημάτων και το 70% των συγκρούσεων με εμπορικά φορτηγά[36].

Η κυκλοφοριακή συμφόρηση εκτιμάται ότι κοστίζει το 1% του ΑΕΠ της ΕΕ, που ισούται με 100 δισεκατομμύρια ευρώ κάθε χρόνο[37]. Ένα παράδειγμα είναι η σημερινή λειτουργία των φωτεινών σηματοδοτών οι οποίοι είναι προγραμματισμένοι να παραμένουν πράσινοι ή κόκκινοι για σταθερά διαστήματα, ανεξάρτητα από το πόση ροή κυκλοφορίας προέρχεται από κάθε κατεύθυνση και εκτιμάται ότι προκαλούν στις διασταυρώσεις έως και το 45% της κυκλοφοριακής συμφόρησης[38].

Η ευρύτερη χρήση ηλεκτρικής ενέργειας στις μεταφορές μπορεί να μειώσει σημαντικά τις εκπομπές του τομέα, ιδίως σε χώρες με υψηλά επίπεδα ανανεώσιμων πηγών παραγωγής ηλεκτρικής ενέργειας. Οι βασικές ευκαιρίες για τις ανανεώσιμες πηγές ενέργειας στον τομέα των μεταφορών περιλαμβάνουν τη χρήση βιοκαυσίμων αναμεμειγμένων με συμβατικά καύσιμα, υποδομές που λειτουργούν με βιομεθάνιο, ηλεκτρικά οχήματα με συσσωρευτή και υβριδικά οχήματα με ρευματολήπτη, καθώς και την ευρεία χρήση ηλεκτρικής ενέργειας στους τρόπους μεταφοράς, συμπεριλαμβανομένης της χρήσης ανανεώσιμου υδρογόνου και ηλεκτρικών καυσίμων.

4 Μαζικά Δεδομένα

4.1 Big Data and Privacy

Ο όρος «μαζικά δεδομένα» είναι ένας ευρύτατα χρησιμοποιούμενος όρος ο οποίος μπορεί να αναφέρεται σε διάφορες έννοιες, ανάλογα με το εκάστοτε πλαίσιο. Εμπερικλείει συνήθως την έννοια «της αυξανόμενης τεχνολογικής ικανότητας συλλογής, επεξεργασίας και εξαγωγής νέων και προγνωστικών γνώσεων από μεγάλο όγκο και ποικιλομορφία δεδομένων με υψηλή ταχύτητα»[39]

Ένας άλλος ορισμός από την Gartner[40] τα ερμηνεύει ως εξής: «Τα Big Data είναι υψηλού όγκου, υψηλής ταχύτητας ή υψηλής ποικιλίας στοιχεία που απαιτούν αποδοτικές και καινοτόμες μορφές επεξεργασίας πληροφοριών που επιτρέπουν την ενίσχυση της κατανόησης, την λήψη αποφάσεων και την αυτοματοποίηση των διαδικασιών»

[36] ITSA. Transportation Safety Spectrum V2X Letter to Senate Communications Technology Innovation and the Internet Subcom- mittee. 2020.https://itsa.org/wp-content/uploads/2020/07/Transportation-Safety-Spectrum-V2X-Letter-to-Senate-Communications-Technology-Innovation-and-the-Internet-Subcommittee-072220.pdf

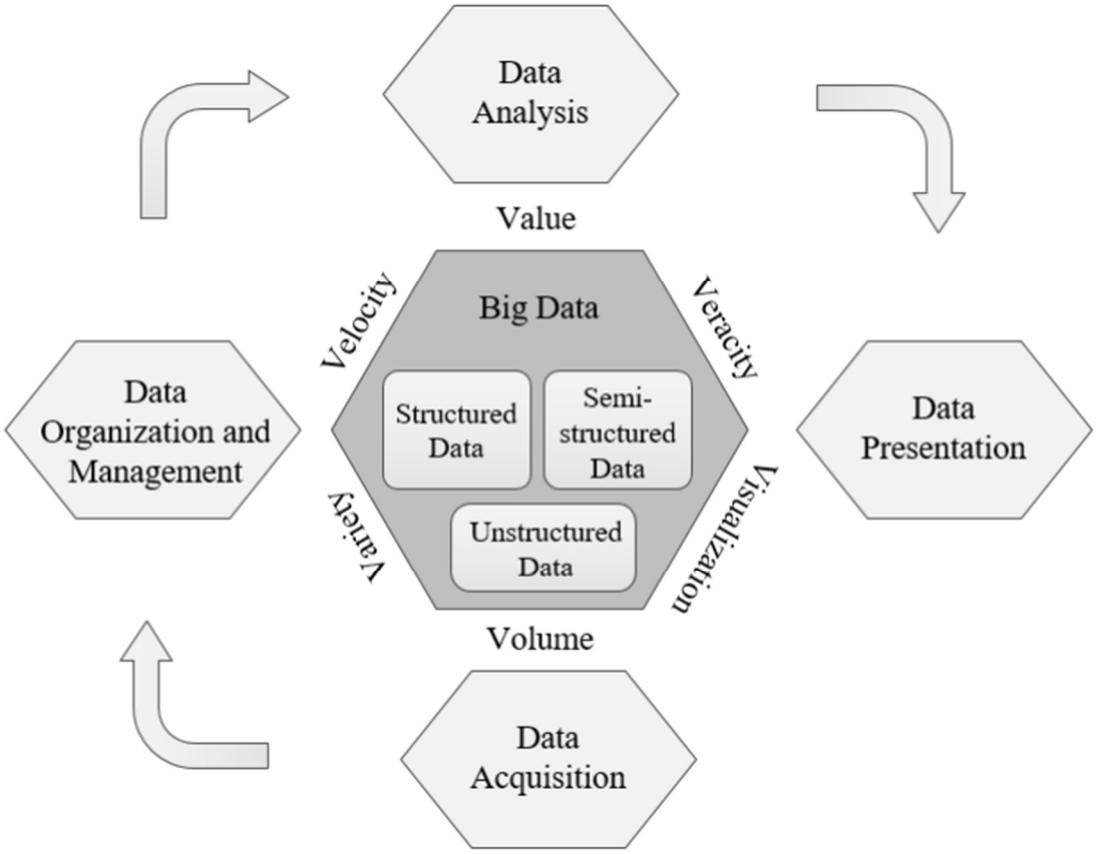
[37] European Mobility Week 2016 «Smart and sustainable mobility – an investment for Europe»: https://mobilityweek.eu/fileadmin/user_upload/materials/participation_resources/2016/Thematic_Guidelines_2016.pdf

[38] F. Knobloch and N. Braunschweig, "A Traffic-Aware Moving Light System Featuring Optimal Energy Efficiency," in IEEE Sensors Journal, vol. 17, no. 23, pp. 7731-7740, 1 Dec.1, 2017, doi: 10.1109/JSEN.2017.2669398.

[39] Εγχειρίδιο Οργανισμού Θεμελιωδών Δικαιωμάτων της ΕΕ (FRA)

[40] Gartner, είναι μια παγκόσμια εταιρεία έρευνας και παροχής συμβουλών που παρέχει πληροφορίες, συμβουλές και εργαλεία για τους ηγέτες στον τομέα της πληροφορικής, της χρηματοδότησης, του ανθρώπινου δυναμικού, της εξυπηρέτησης πελατών και της υποστήριξης, των επικοινωνιών, νομικών συμβουλών, μάρκετινγκ, πωλήσεις και λειτουργίες αλυσίδας εφοδιασμού https://www.gartner.com/en/information-technology/glossary/big-data

Λόγω της πολυπλοκότητας των μεγάλων δεδομένων και των μεγάλων προοπτικών εφαρμογής τους, ή τεχνολογία των μαζικών δεδομένων περιέχει ερευνητικά προβλήματα που πρέπει να επισημανθούν. Επομένως, μια σύντομη εισαγωγή στην επεξεργασία μεγάλων δεδομένων και στα κύρια χαρακτηριστικά τους αποτυπώνεται ως εξής.



Εικόνα 14: Κύρια χαρακτηριστικά και διεργασίες των Big Data (Πηγή: Junkuo Cao Mingcai Lin Xiaojin Ma, A Survey of Big Data for IoT in Cloud Computing, International Journal of Computer Science, Volume 47, Issue 3: September 2020)

Σε αντίθεση με τα παραδοσιακά δεδομένα, τα μεγάλα δεδομένα όχι μόνο έχουν τεράστιο όγκο δεδομένων, αλλά έχουν επίσης πιο περίπλοκες πηγές και δομές. Για να αντικατοπτρίζουν καλύτερα τον ορισμό των μεγάλων δεδομένων, πολλοί επιστήμονες και ειδικοί ορίζουν τα μεγάλα δεδομένα με τα ακόλουθα κύρια χαρακτηριστικά[41]:

Volume (όγκος), αναφέρεται στον μεγάλο όγκο των δεδομένων που δημιουργούνται κάθε δευτερόλεπτο.

Velocity (ταχύτητα): αναφέρεται στη ταχύτητα με την οποία τα δεδομένα δημιουργούνται και διακινούνται.

Variety (ποικιλία): αναφέρεται στους διαφορετικούς τύπους δεδομένων που μπορούν να χρησιμοποιηθούν.

[41] https://www.cscjournals.org/manuscript/Journals/IJCSS/Volume14/Issue5/IJCSS-1591.pdf

Veracity (ορθότητα): αναφέρεται στην αξιοπιστία όλων των δεδομένων που συλλέγονται.

Value (αξία): είναι ίσως το πιο σημαντικό από τα πέντε, καθώς αναφέρεται στην ανάγκη μετατροπής των δεδομένων, μέσα από την επεξεργασία, την ανάλυση, σε αξία για μια επιχείρηση ή έναν οργανισμό

Visualization (απεικόνιση): αφορά τη προβολή και επικοινωνία μεγάλων δεδομένων, αποτελεσματικά σε διαφορετικά περιβάλλοντα.

Η διαδικασία ακολουθεί μια αλληλουχία καταστάσεων που ξεκινάει από την συλλογή των μαζικών δεδομένων και καταλήγει στην ορθή παρουσίαση τους.

4.2 Δεδομένα Προσωπικού Χαρακτήρα και Κριτήρια Ταυτοποίησης στα Μαζικά Δεδομένα

Ως επεξεργασία δεδομένων νοούνται οι πράξεις ή τα σύνολα πράξεων που εκτελούνται σε δεδομένα προσωπικού χαρακτήρα ή σύνολα δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένο ή μη αυτοματοποιημένο τρόπο (άρθρο 4 παράγραφος 2 του ΓΚΠΔ). Ταυτόχρονα, είναι προφανές ότι δεν υπάρχει επεξεργασία δεδομένων εάν οι πράξεις συλλογής, καταγραφής, οργάνωσης, παραγγελίας κ.λπ. δεδομένων εκτελούνται σε πληροφορίες που δεν επιτρέπουν την άμεση ή έμμεση ταυτοποίηση ενός φυσικού προσώπου. Αυτό υποδεικνύεται από την αιτιολογική σκέψη 26 του ΓΚΠΔ, σύμφωνα με την οποία οι αρχές της προστασίας των δεδομένων δεν θα πρέπει να εφαρμόζονται σε ανώνυμες πληροφορίες ή σε ανώνυμα δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένης της επεξεργασίας για στατιστικούς ή επιστημονικούς σκοπούς. Η θέση αυτή απορρέει επίσης έμμεσα από το άρθρο 5 παράγραφος 1 στοιχείο β) του GDPR (αρχή περιορισμού του σκοπού), σύμφωνα με το οποίο η συλλογή και καταγραφή δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται για ρητό και νόμιμο σκοπό. Το κλειδί για τον προσδιορισμό του γεγονότος της επεξεργασίας είναι η πρόθεση με την οποία μια δεδομένη οντότητα περιήλθε στην κατοχή προσωπικών δεδομένων (σκοπός επεξεργασίας).

Προκειμένου να προσδιοριστεί πότε οι πληροφορίες που υποβάλλονται σε επεξεργασία σε σύνολα μαζικών δεδομένων θα πρέπει να θεωρούνται προσωπικά δεδομένα, θα πρέπει να υπενθυμίσουμε την έννοια των προσωπικών δεδομένων, η οποία σύμφωνα με το άρθρο 4 παράγραφος 1 του GDPR σημαίνει «κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (...) το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου». Ταυτόχρονα, ο ΓΚΠΔ διευκρινίζει ότι τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, όπως διευθύνσεις πρωτοκόλλου διαδικτύου ή αναγνωριστικά cookie, που δημιουργούνται από συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα, ή άλλα αναγνωριστικά, όπως ετικέτες RFID.

Σύμφωνα με το προαναφερθέν άρθρο 4 παράγραφος 1 του GDPR, τα προσωπικά δεδομένα περιλαμβάνουν όχι μόνο τις πληροφορίες που καθιστούν δυνατή την ταυτοποίηση ενός ατόμου, αλλά και εκείνες που επιτρέπουν τον έμμεσο προσδιορισμό της ταυτότητας, ιδίως εκείνες που προσδιορίζουν ένα άτομο άμεσα ή έμμεσα μόνο όταν συνδυάζονται με άλλα δεδομένα, π.χ. πληροφορίες σχετικά με την οικογενειακή

κατάσταση, το ιατρικό ιστορικό, την οικονομική κατάσταση ή την εκπαίδευση. Στην πράξη, η επισήμανση κριτηρίων που επιτρέπουν την έμμεση ταυτοποίηση είναι ιδιαίτερα δύσκολη.

Το πρόβλημα με τον καθορισμό των κριτηρίων έμμεσου προσδιορισμού επιλύθηκε εν μέρει με την αιτιολογική σκέψη 26 του ΓΚΠΔ, οι οποίες συμπληρώνουν το άρθρο 4 του ΓΚΠΔ. Για να διαπιστωθεί κατά πόσον είναι ευλόγως πιθανό να χρησιμοποιηθούν μέσα για την ταυτοποίηση του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως το κόστος και ο χρόνος που απαιτείται για την ταυτοποίηση, καθώς και η τεχνολογία που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και οι τεχνολογικές εξελίξεις. Στην περίπτωση της επεξεργασίας μαζικών δεδομένων, όλοι οι προαναφερθέντες παράγοντες μπορούν να αλλάξουν, ιδίως όταν μια τέτοια διαδικασία είναι πολύπλοκη και μακροχρόνια. Όπως είναι αναμενόμενο, αυτό ενέχει τον κίνδυνο να αυξηθεί δυναμικά η δυνατότητα ταυτοποίησης συγκεκριμένων προσώπων γιατί όσο μεγαλύτερο είναι το σύνολο δεδομένων, τόσο μεγαλύτερος είναι ο κίνδυνος.

4.3 Προκλήσεις για την Τεχνολογία Μαζικών Δεδομένων

Ο τεράστιος όγκος δεδομένων θέτει πολλές προκλήσεις όταν έρχεται στο προσκήνιο, ενώ ορισμένα δεδομένα θα μπορούσαν να αποθηκευτούν σε παραδοσιακές βάσεις δεδομένων, άλλες πηγές δεδομένων που δεν βρίσκονται σε δομημένη μορφή, όπως βίντεο και εικόνες, δεν θα μπορούσαν να τα αξιοποιήσουν. Αν και αυτά τα δεδομένα μπορούν να διαχειριστούν αποτελεσματικά μεμονωμένα, προκύπτουν πολλά ζητήματα κατά την ενσωμάτωση πολλών δεδομένων από διάφορες πηγές.

Οι μεγαλύτερες προκλήσεις είναι οι ακόλουθες.

Τα δεδομένα είναι ετερογενή στη φύση τους, καθώς τα δεδομένα προέρχονται από πολλαπλές πηγές πρέπει να είναι δομημένα πριν από την εκτέλεση της ανάλυσης και της περεταίρω επεξεργασίας τους.

Μερικές φορές τα δεδομένα μπορεί να είναι ελλιπή, γεγονός που μπορεί να δημιουργήσει πρόβλημα όταν λαμβάνονται για ανάλυση, στην περίπτωση αυτή πρέπει να εισαχθούν μηδενικές (null) τιμές στη θέση των τιμών που λείπουν, έτσι ώστε να μην επηρεάζουν τα υπόλοιπα δεδομένα και να έρχεται το επιθυμητό αποτέλεσμα.

Η διαχείριση του τεράστιου όγκου δεδομένων είναι το μεγαλύτερο ζήτημα στην εποχή των μεγάλων δεδομένων. Όσο περισσότερα δεδομένα χρησιμοποιούνται τόσο μεγαλύτερος είναι ο χρόνος επεξεργασίας που απαιτείται.

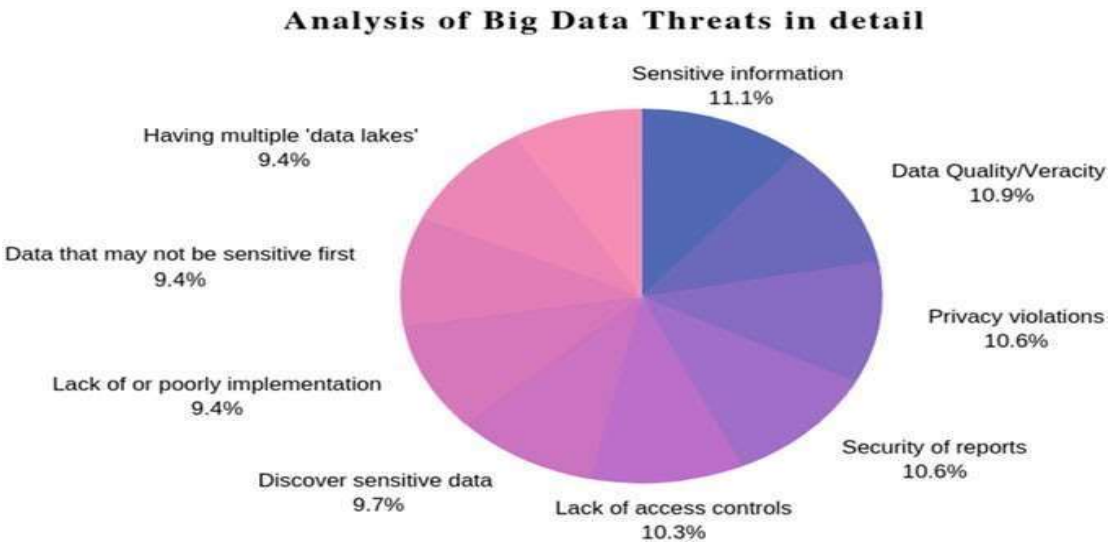
Το ζήτημα της ταχύτητας των μεγάλων δεδομένων και η επεξεργασία τους σε πραγματικό χρόνο θέτει την πρόκληση για την απρόσκοπτη ροή των δεδομένων για τα δίκτυα.

Η συλλογή δεδομένων και η μετατροπή τους σε μαζικά δεδομένα που θα μπορούν να επεξεργαστούν, θα πρέπει να γίνεται με τέτοιο τρόπο ώστε να μπορούν να επεκταθούν, όταν τα δεδομένα αυξάνονται εκθετικά. Τα δεδομένα δεν πρέπει μόνο να είναι επεκτάσιμα, αλλά και αξιόπιστα.

Το απόρρητο των δεδομένων είναι μια μεγάλη πρόκληση, λαμβάνοντας υπόψη την συνεχή αύξηση των δεδομένων που θα μπορούσαν να παραβιάσουν με ποικίλους τρόπους την ιδιωτική ζωή των χρηστών. Θα πρέπει να θεσπιστεί μηχανισμός ελέγχου σε διάφορα στάδια του κύκλου ζωής των μαζικών δεδομένων και να περιοριστεί ο διαμοιρασμός τους σε σκοπούς διαφορετικούς για τους οποίους συλλέγονται. Ακόμη

και όταν τα δεδομένα πρόκειται να δοθούν για ανάλυση, προτεραιότητα του υπεύθυνου επεξεργασίας αλλά και η εκ του σχεδιασμού φιλοσοφία των πληροφοριακών συστημάτων που τα διαχειρίζονται, είναι η προστασία των ευαίσθητων πληροφορίων που μπορούν να εκμεταλλευτούν μη αξιόπιστες πηγές.

Οι συσκευές IoT δημιουργούν μεγάλες ποσότητες δεδομένων που πρέπει να υποβληθούν σε επεξεργασία και ανάλυση προκειμένου να χρησιμοποιηθούν για την παροχή δημόσιων υπηρεσιών και τη βελτίωση της διαχείρισης. Τα μαζικά δεδομένα χρησιμεύουν επίσης για πρωτοβουλίες ανοιχτών δεδομένων προς όφελος της ανθρωπότητας και ενός καλύτερου μέλλοντος. Επειδή τα πλαίσια επεξεργασίας μεγάλων δεδομένων δεν χρησιμοποιούν SQL, δεν παρέχουν τους περιορισμούς ασφαλείας, όπως κρυπτογράφηση των κωδικών πρόσβασης και των προσωπικών πληροφοριών πριν τη μεταφορά μεταξύ των συστημάτων και είναι επιρρεπή σε επιθέσεις. Οι τεχνικές ανωνυμοποίησης δεδομένων συνήθως δεν εφαρμόζονται πριν από την ανάλυση, η οποία μπορεί να οδηγήσει σε αποκάλυψη προσωπικών πληροφοριών μετά την επεξεργασία των δεδομένων.



Εικόνα 15: Κατηγορίες απειλών μαζικών δεδομένων. Πηγή: Data Source International Data Corporation (2019)

Προκλήσεις στο επίπεδο πηγών δεδομένων: Όσον αφορά τις αρχές προστασίας της ιδιωτικής ζωής, τόσο η συγκατάθεση όσο και η αρχή του περιορισμού του σκοπού πρέπει να λαμβάνονται υπόψη πριν από την έναρξη της φάσης συλλογής. Κάθε υποκείμενο δεδομένων έχει το δικαίωμα να γνωρίζει τους λόγους πίσω από τη συλλογή κάθε δεδομένων από τις πηγές. Ως εκ τούτου, ζητείται από το υποκείμενο των δεδομένων να ορίσει τις προτιμήσεις του σχετικά με τη συχνότητα συλλογής, τον βαθμό λεπτομέρειας των δεδομένων και το σύνολο των πληροφοριών που επιτρέπει να αποκαλύψει σε εφαρμογές τρίτων. Η διατήρηση της ιδιωτικής ζωής στο επίπεδο προέλευσης είναι απαραίτητη και μπορεί να επηρεάσει ολόκληρο τον κύκλο ζωής των δεδομένων. Κάποιος μπορεί να δει ότι η αρχή της «ελαχιστοποίησης δεδομένων» και των Big Data είναι εκ πρώτης όψεως αντιφατική και πολύ προκλητική, επειδή οι αντιληπτές ευκαιρίες στα Big Data παρέχουν κίνητρα για τη συλλογή όσο το δυνατόν περισσότερων δεδομένων και τη διατήρηση αυτών των δεδομένων όσο το δυνατόν περισσότερο για ακόμη άγνωστους μελλοντικούς σκοπούς.

Προκλήσεις στο επίπεδο συλλογής δεδομένων: Οι εφαρμογές Big Data συνήθως τείνουν να συλλέγουν δεδομένα από διαφορετικές πηγές και χωρίς προσεκτική επαλήθευση της συνάφειας ή της ακρίβειας των δεδομένων που συλλέγονται με αυτόν τον τρόπο. Αυτό μπορεί να παρέχει ψευδή αποτελέσματα ανάλυσης και να επηρεάσει την αξιοπιστία των δεδομένων. Για παράδειγμα, στον τομέα της ηλεκτρονικής υγείας, εσφαλμένα δεδομένα σχετικά με την υγεία ή το περιβάλλον του ασθενούς μπορούν να οδηγήσουν σε εσφαλμένη διάγνωση που θέτει σε κίνδυνο τη ζωή του υποκειμένου των δεδομένων. Είναι σημαντικό να διασφαλιστεί ότι τα δεδομένα δεν τροποποιούνται κατά τη φάση μετάδοσης και εντοπίζονται κακόβουλες οντότητες που προσπαθούν να εισάγουν δεδομένα προκειμένου να δημιουργήσουν συμφόρηση στο δίκτυο ή να επηρεάσουν τα αποτελέσματα της ανάλυσης.

Προκλήσεις στα επίπεδα επεξεργασίας και αποθήκευσης δεδομένων: Τα δεδομένα αποθηκεύονται και υποβάλλονται σε επεξεργασία για την παροχή προηγμένων και υπολογισμένων πληροφοριών για το επίπεδο υπηρεσιών. Ωστόσο, τα προσωπικά δεδομένα θα πρέπει να αποθηκεύονται για σαφώς καθορισμένη χρονική διάρκεια (περιορισμός αποθήκευσης). Επομένως, απαιτείται περιορισμός διατήρησης και αποκάλυψης δεδομένων σε αυτό το στάδιο. Κατά συνέπεια, πρέπει να αναπτυχθούν οι απαραίτητοι μηχανισμοί για την καταστροφή δεδομένων όταν λήξει η προθεσμία διατήρησης. Επιπλέον, πολλά δεδομένα συλλέγονται για μη καθορισμένους σκοπούς, κυρίως για την ανάλυση μεγάλων δεδομένων. Ωστόσο, η ωμή δήλωση ότι τα δεδομένα συλλέγονται για οποιαδήποτε πιθανή ανάλυση δεν είναι επαρκώς αποδεκτός σκοπός. Η αρχή του περιορισμού της αποθήκευσης μπορεί να υπονομεύσει την ικανότητα πρόβλεψης, η οποία είναι μία από τις ευκαιρίες που καθίστανται δυνατές από την ανάλυση Big Data. Πράγματι, εάν η ανάλυση Big Data επιτρέπει την προβλεψιμότητα, είναι ακριβώς επειδή οι αλγόριθμοι μπορούν να συγκρίνουν τα τρέχοντα δεδομένα με τα αποθηκευμένα δεδομένα του παρελθόντος, προκειμένου να καθορίσουν τι πρόκειται να συμβεί στο μέλλον.

Ένα άλλο δύσκολο ζήτημα για την εξασφάλιση ενός συστήματος Big Data είναι η ανταλλαγή δεδομένων. Για παράδειγμα, τα δεδομένα οδικής κυκλοφορίας μπορούν να συλλεχθούν από κάμερες χωρίς χρήση ή smartphones ταξιδιωτών και GPS με τρόπο πληθοπορισμού. Κατά τη διάρκεια του παγκόσμιου οδικού σχεδιασμού, είναι δύσκολο να καθοριστεί η πολιτική πρόσβασης και να καταστεί δυνατή η κοινή χρήση δεδομένων διατήρησης της ιδιωτικής ζωής μεταξύ των εμπλεκόμενων εφαρμογών και υπηρεσιών. Ως εκ τούτου, η αποθήκευση και η ανταλλαγή μαζικών δεδομένων απαιτούν την ανάπτυξη κατάλληλων τεχνικών προκειμένου να γίνεται σεβαστή η συγκατάθεση και η ιδιωτικότητα του χρήστη, παρέχοντας παράλληλα καινοτόμο αναλυτική επεξεργασία για διαφορετικούς σκοπούς. Μόλις μια εφαρμογή Big Data επιλύσει όλες τις προηγούμενες προκλήσεις για το επίπεδο επεξεργασίας και αποθήκευσης, ένας ελεγκτής πρέπει να το αποδείξει. Εδώ έρχεται ο ρόλος της διαφάνειας και της λογοδοσίας. Ο υπεύθυνος επεξεργασίας πρέπει να παρέχει όλες τις πληροφορίες για τα επεξεργασμένα δεδομένα, παρέχοντας πού αποθηκεύονται τα δεδομένα και πώς χειρίζονται ή υποβάλλονται σε επεξεργασία. Αυτή η εργασία μπορεί να είναι εύκολη για κλασικές εφαρμογές. Αλλά στο πλαίσιο των Big Data, είναι ένα δύσκολο έργο. Η επεξεργασία μεγάλων δεδομένων είναι πολύπλοκη και με διαφορετικούς σκοπούς και εντατική επεξεργασία και κάποιο χρονικό διάστημα με αδιαφανείς διαδικασίες επεξεργασίας. Η δημιουργία, η διαφάνεια και η παρακολούθηση της χρήσης και αποθήκευσης δεδομένων είναι πολύ δύσκολη.

Προκλήσεις στα επίπεδα διανομής και υπηρεσιών: Οι εφαρμογές τρίτων έχουν πρόσβαση στα αναλυτικά αποτελέσματα που υπολογίζονται από δεδομένα πολιτών. Οι

κοινοποιούμενες πληροφορίες, ακόμη και ανώνυμες, ενδέχεται να αποκαλύψουν προσωπικά δεδομένα. Είναι σημαντικό η κοινή χρήση δεδομένων να ελέγχεται όσον αφορά τη συγκατάθεση των πολιτών. Η πρόκληση υπάρχει όταν υπάρχει μεγάλος αριθμός και ποικιλία εφαρμογών που χρησιμοποιούν προσωπικά δεδομένα και επικοινωνούν από πηγές δεδομένων σε επίπεδα επεξεργασίας. Στην περίπτωση αυτή, η παρακολούθηση της πρόσβασης σε δεδομένα και η κοινοποίηση παραβίασης δεδομένων καθίσταται δύσκολη. Επίσης, στο πλαίσιο της ανάλυσης μεγάλων δεδομένων, η επεξεργασία μπορεί να είναι αδιαφανής, ενώ τα άτομα (υποκείμενο των δεδομένων) πρέπει να λαμβάνουν σαφείς πληροφορίες σχετικά με τα δεδομένα που υποβάλλονται σε επεξεργασία. Πρέπει να είναι καλύτερα ενημερωμένοι σχετικά με το πώς και για ποιους σκοπούς χρησιμοποιούνται οι πληροφορίες τους και, σε ορισμένες περιπτώσεις, απαιτούν τη λογική που χρησιμοποιείται στους αλγορίθμους για τον προσδιορισμό των υποθέσεων και των προβλέψεων σχετικά με αυτούς.

Από την παραπάνω περιγραφή, οι βασικές αρχές του GDPR φαίνεται, ως επί το πλείστον, να έρχονται σε αντίθεση με ορισμένα από τα βασικά χαρακτηριστικά της εφαρμογής μεγάλων δεδομένων και της ανάλυσης μεγάλων δεδομένων. Ωστόσο, η επανεξέταση ορισμένων δραστηριοτήτων επεξεργασίας και των εξελίξεων ΤΠ μπορεί να συμβάλει στον σεβασμό της ιδιωτικής ζωής. Η αντιμετώπιση των αρχών του GDPR απαιτεί μια συντονισμένη στρατηγική που περιλαμβάνει διαφορετικές οργανωτικές οντότητες, συμπεριλαμβανομένων των νομικών, ανθρώπινων πόρων, ασφάλειας πληροφορικής και άλλων. Ο GDPR περιλαμβάνει βασικές απαιτήσεις που επηρεάζουν άμεσα τον τρόπο με τον οποίο οι οργανισμοί εφαρμόζουν την ασφάλεια IT. Επειδή το GDPR αφορά περισσότερο τις διαδικασίες ασφαλείας και τη διαχείριση του κινδύνου, κανένα προϊόν δεν θα λύσει όλα τα προβλήματα απορρήτου. Αυτό που χρειάζεται είναι να διασφαλιστεί ότι οι λύσεις συνεργάζονται για να είναι πραγματικά συμβατές με τον GDPR.

4.4 Big Transport Data (BTD)

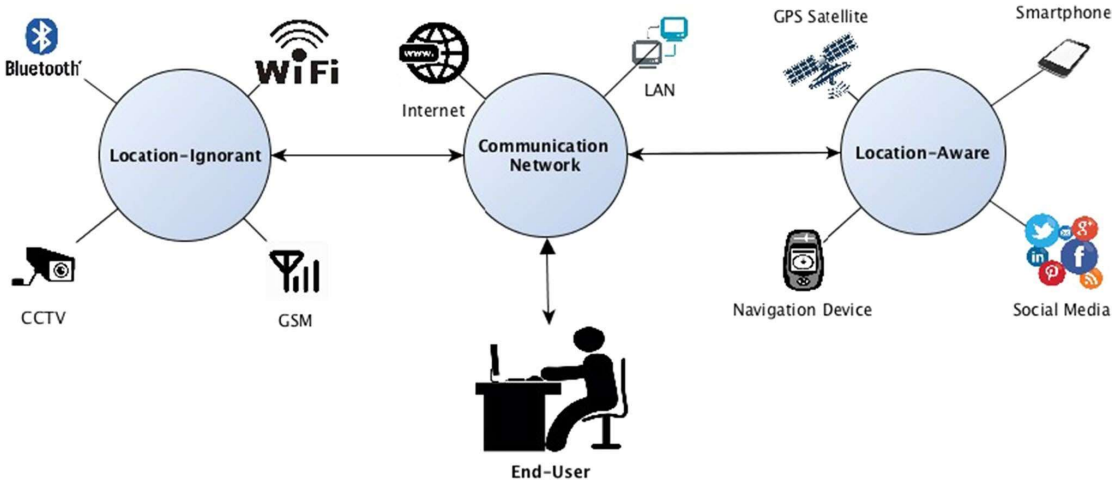
Χαρακτηρίζουμε τα Big Transport Data (BTD) απλά ως Big Data, αλλά με ισχυρές εφαρμογές στα συστήματα μεταφορών. Δηλαδή, δεδομένα που θα μπορούσαν να χρησιμοποιηθούν σε περιοχές που εμπίπτουν στην παραδοσιακή αρμοδιότητα του σχεδιασμού, του προγραμματισμού και των λειτουργιών των μεταφορών, όπως η πρόβλεψη της ζήτησης ταξιδιών, ο προγραμματισμός υποδομών, ο προγραμματισμός του δικτύου διαμετακόμισης, η βελτιστοποίηση της λειτουργίας κ.λπ.

Το BTD προέρχεται από το συνδυασμό τριών τύπων τεχνολογιών. Ξεκινάμε με δύο ευρείες κατηγορίες συσκευών που συλλέγουν BTD. Συσκευές με άγνοια τοποθεσίας και επίγνωση τοποθεσίας.

Οι συσκευές που αγνοούν την τοποθεσία είναι σε θέση να ανιχνεύσουν την παρουσία άλλων συσκευών, αν και δεν γνωρίζουν ρητά τις δικές τους τοποθεσίες. Αυτές περιλαμβάνουν τεχνολογίες όπως το Bluetooth, το Wi-Fi, Παγκόσμιο σύστημα για κινητά (GSM) και κλειστού κυκλώματος τηλεόρασης (CCTV).

Οι δεύτερες είναι συσκευές που μπορούν να προσδιορίσουν τη δική τους τοποθεσία, δηλαδή έχουν επίγνωση τοποθεσίας. Αυτές οι συσκευές συνήθως αντλούν τις θέσεις τους με βάση τη θέση άλλων συσκευών, όπως δρομολογητές Wi-Fi, πύργοι GSM ή satellites μέρος διαφόρων δορυφόρων πλοήγησης συστήματα, όπως το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS). Περιλαμβάνουν μονάδες GPS, πλοηγούς GPS και το πιο σημαντικό Smartphones.

Ενώ οι συσκευές που συλλέγουν δεδομένα είναι ζωτικής σημασίας για τη δυνατότητα χρήσης BTD, οι δυνατότητές τους μπορούν να αξιοποιηθούν μόνο εάν οι συσκευές είναι συνδεδεμένες σε δίκτυο επικοινωνιών, όπως το Διαδίκτυο, ιδιωτικά τοπικά δίκτυα (LAN) ή δίκτυα ευρείας περιοχής (WAN). Τα δίκτυα αυτά επιτρέπουν τη μεταφορά δεδομένων από συσκευές συλλογής σε συστήματα αποθήκευσης βάσεων δεδομένων από όπου θα έχουν πρόσβαση για επεξεργασία και ανάλυση από τους τελικούς χρήστες.



Σχήμα 1 Οικοσύστημα μεγάλων δεομένων μεταφοράς

4.5 Μαζικά Δεδομένα για τις Μεταφορές και την Κινητικότητα

Ερμηνεύοντας από τη σκοπιά των μεταφορών, τα Big Data μπορούν να θεωρηθούν ως ένα χαρτοφυλάκιο τεχνολογιών που επιτρέπουν την αποτελεσματική διαχείριση (αποθήκευση, επεξεργασία και πρόσβαση) όλων των δεδομένων που απαιτούνται για την ανάπτυξη νέων τρόπων παροχής ασφαλέστερων, καθαρότερων και αποδοτικότερων μεταφορών, καθώς και για τους χρήστες να εξατομικεύουν και να προσαρμόζουν την εμπειρία μεταφοράς τους. Με άλλα λόγια, τα Big Data είναι σε θέση να εκμεταλλευτούν πληροφορίες και να λύσουν προβλήματα μεταφοράς σε πρωτοφανείς κλίμακες. Αυτή η τεχνολογική εξέλιξη άνοιξε το δρόμο για ευκαιρίες για νέα μοντέλα μεταφοράς, υπηρεσίες και εφαρμογές που παρέμειναν ανεξερεύνητες, κυρίως λόγω της ανάγκης για νέα δεδομένα που δεν είχαν συλλεχθεί ούτε υποβληθεί σε επεξεργασία μέχρι σήμερα., Υπάρχουν δύο κύριοι παράγοντες που παρακινούν την υιοθέτηση του παραδείγματος των Μαζικών Δεδομένων στους τομείς των μεταφορών και της κινητικότητας. Το πρώτο σχετίζεται με την αστικοποίηση και τις έξυπνες πόλεις, οι οποίες έχουν θέσει ένα πλούσιο υπόστρωμα νέων πηγών Big Data. Η δεύτερη κινητήρια δύναμη είναι η έλευση και η προοδευτική ωριμότητα των καινοτόμων τεχνολογιών πληροφοριών και επικοινωνιών, όπως οι κινητές επικοινωνίες υψηλής ταχύτητας (5G), οι τεχνολογίες υπολογιστικού νέφους (cloud computing) και το Διαδίκτυο των Πραγμάτων (IoT), οι οποίες επέτρεψαν νέες μεθόδους επεξεργασίας και αξιοποίησης των μαζικών δεδομένων. Στις έξυπνες πόλεις, ο σχεδιασμός και η ανάπτυξη ευφυών συστημάτων κινητικότητας αποτελεί δύσκολη απαίτηση, δεδομένης της συνύπαρξης και της ποικιλομορφίας σταδιακά περισσότερων μέσων μεταφοράς και προτύπων κινητικότητας στις αστικές περιοχές. Ο Διαμοιρασμός σημαντικών πληροφοριών σχετικά με τον τρόπο με τον οποίο οι άνθρωποι μετακινούνται εντός και

εκτός αστικού περιβάλλοντος, για την επίλυση κινητικών προβλημάτων από την οπτική γωνία της κοινωνίας στο σύνολό της θα απαιτήσει αναμφίβολα οι μεταφορές να λειτουργούν με βιώσιμο τρόπο για λόγους ασφάλειας, πρακτικότητας και συνοχής. Για τον σκοπό αυτό, ο γενικός στόχος που επιδιώκουν οι τεχνολογίες για τη βελτίωση της κινητικότητας στις έξυπνες πόλεις είναι η επίτευξη καλύτερης ολοκλήρωσης και διαχείρισης των αστικών μεταφορών, καθώς και η ανάπτυξη ευφυών συστημάτων για απρόσκοπτη πολυτροπική κινητικότητα. Από την άποψη αυτή, η έννοια της Έξυπνης Κινητικότητας αναφέρεται στη βελτιστοποίηση των υπηρεσιών μεταφορών αντιμετωπίζοντας προβλήματα κρίσιμων δεδομένων, όπως η ελαχιστοποίηση της κυκλοφοριακής συμφόρησης και η εκτίμηση των περιβαλλοντικών επιπτώσεων των αποφάσεων που λαμβάνονται. Τα προβλήματα αυτά έχουν εντείνει την εστίαση της έρευνας σε νέους φιλικούς προς το περιβάλλον τρόπους μεταφοράς (π.χ. ποδήλατα, ηλεκτρικά οχήματα) που έχουν λιγότερες επιπτώσεις στο περιβάλλον, με έμφαση στον τρόπο διατήρησης των παλαιών μέσων μεταφοράς και άλλων υπηρεσιών κινητικότητας καθώς οι υπάρχουσες υποδομές βασίζονται σε διαφορετικά μοντέλα μεταφορών.

Επί του παρόντος, αυτά τα ευφυή συστήματα μεταφορών κινούνται και εξελίσσονται προς την απρόσκοπτη ενσωμάτωση μιας ευρείας ποικιλίας ετερογενών τεχνολογιών που μπορούν να συλλέξουν τεράστιες ποσότητες δεδομένων, να τα επεξεργαστούν και να λάβουν τα κατάλληλα μέτρα με βάση τα δεδομένα, όλα σε πραγματικό χρόνο. Λόγω αυτής της εξέλιξης, υπάρχει σημαντικός αντίκτυπος στην επιρροή που μπορεί να έχει η συμπεριφορά ενός οχήματος ή οδηγού για να προσφέρει πολλά οφέλη, όπως η πρόληψη τροχαίων ατυχημάτων, η μείωση του άγχους του οδηγού, η μείωση της κυκλοφοριακής συμφόρησης και πολλά άλλα, τα οποία μπορούν να βοηθήσουν στη ρύθμιση της ροής της κυκλοφορίας σε όλη την πόλη και να αυξήσουν τη ροή πληροφοριών σε περίπτωση έκτακτης ανάγκης.

4.6 Big data and Privacy by design

Στην περίπτωση των μαζικών δεδομένων, λόγω του μεγέθους και της ποικιλίας των δεδομένων που υποβάλλονται σε επεξεργασία, ακόμη και σε σχεδόν πραγματικό χρόνο, παρουσιάζονται πολλές προκλήσεις στον σχεδιασμό και εφαρμογής ενός νομικού πλαισίου που θα ανταποκρίνεται στις αυξημένες απαιτήσεις ασφάλειας και ιδιωτικότητας. Η πρόκληση στο πεδίο των μαζικών δεδομένων εμφανίζεται στο γεγονός ότι αντιβαίνει με την αρχή της ελαχιστοποίησης των δεδομένων[42] όπως αυτή ορίζεται από τον ΓΚΠΔ. Παράλληλα ο στρατηγικός σχεδιασμός 8 σημείων για την «εκ του σχεδιασμού προστασία της ιδιωτικότητας» στις τεχνολογίες πληροφοριών και συστημάτων (βλ. εικόνα 1) από τον ENISA[43], για την ενσωμάτωση κανόνων ασφάλειας στη προστασία της ιδιωτικότητας που πρέπει να τηρείται, ορίζει ως προϋπόθεση και αυτός την ελαχιστοποίηση των δεδομένων. Επιπλέον το άρθρο 25 παράγραφος 2 του ΓΚΠΔ, απαριθμεί τις διαστάσεις της υποχρέωσης ελαχιστοποίησης δεδομένων για την προεπιλεγμένη επεξεργασία, αναφέροντας ότι η υποχρέωση ισχύει για την ποσότητα των προσωπικών δεδομένων που συλλέγονται, την έκταση της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητα τους στα πλαίσια των αρχών της προστασίας δεδομένων από τον σχεδιασμό και εξ' ορισμού που ορίζονται στο άρθρο. Με άλλα λόγια, εάν ορισμένες κατηγορίες προσωπικών δεδομένων είναι περιττές ή εάν δεν απαιτούνται λεπτομερή δεδομένα για τον σκοπό της επεξεργασίας, τότε δεν θα συλλέγονται.

[42] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 5, στοιχείο γ.
[43] Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών.

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Εικόνα 16: Privacy by design strategies, Source: Privacy by design in Big Data, ENISA 2015

Επιπλέον, η συγχώνευση πληροφοριών από διαφορετικές πηγές είναι επίσης ουσιαστικό μέρος της ανάλυσης μαζικών δεδομένων, σε αντίθεση με τη κατανεμημένη επεξεργασία προσωπικών δεδομένων (Separate by design) που ορίζεται στον σχεδιασμό. Επίσης, η δυνατότητα εξαγωγής συμπερασμάτων και αποκρυπτογράφησης των ατόμων από τα συσχετισμένα σύνολα δεδομένων έρχεται σε αντίθεση με την ίδια την ιδέα της απόκρυψης των δεδομένων (Hide by design). Μπορεί επίσης να υποστηριχθεί ότι ακόμη και οι ίδιοι οι υπεύθυνοι επεξεργασίας δεδομένων δεν είναι αρκετά σίγουροι για τους όρους με τους οποίους έχει διαμορφωθεί το αρχικό σύνολο δεδομένων τους, λόγω της διασύνδεσης και επεξεργασίας δεδομένων από διαφορετικές πηγές άντλησης.

Σύμφωνα με τον ΓΚΠΔ[44], «Προκειμένου να είναι σε θέση να αποδείξει τη συμμόρφωση με τον παρόντα κανονισμό, ο υπεύθυνος επεξεργασίας θα πρέπει να υιοθετήσει εσωτερικές πολιτικές και να εφαρμόσει μέτρα που ανταποκρίνονται ιδίως στις αρχές της προστασίας δεδομένων από τον σχεδιασμό και εξ' ορισμού (privacy by design and by default). Τέτοια μέτρα θα μπορούσαν να συνίστανται, μεταξύ άλλων, στην ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ψευδωνυμοποίηση προσωπικών δεδομένων και τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία προσωπικών δεδομένων.

[44] Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 78

5 Τεχνητή Νοημοσύνη και Νομικοί Κανόνες

5.1 Εισαγωγή

Η τεχνητή νοημοσύνη (AI) είναι ένας κλάδος της επιστήμης των υπολογιστών που έχει φέρει επανάσταση στον τρόπο με τον οποίο οι άνθρωποι εκτελούν καθημερινές εργασίες χρησιμοποιώντας μηχανές με ελάχιστη ανθρώπινη παρέμβαση για την προώθηση αυτοματοποιημένης και έξυπνης συμπεριφοράς. Η μηχανική μάθηση (ML) και η βαθιά μάθηση (DL) είναι ταχέως εξελισσόμενα υποπεδία της τεχνητής νοημοσύνης που επιτυγχάνουν εξαιρετικά επίπεδα απόδοσης όταν μαθαίνουν να επιλύουν σταδιακά σύνθετα υπολογιστικά προβλήματα που βασίζονται σε δεδομένα ή χωρίς δεδομένα, καθιστώντας τα κρίσιμα για τη μελλοντική ανάπτυξη του ανθρώπινου πολιτισμού. Η πολυπλοκότητα των λύσεων τεχνητής νοημοσύνης έχει προχωρήσει πρόσφατα σε σημείο που δεν απαιτείται ανθρώπινη παρέμβαση στην ανάπτυξη τους. Ως αποτέλεσμα, ο χρήστης μπορεί να λάβει τεκμηριωμένη απόφαση με δυνητικά εκτεταμένες συνέπειες και να αποφύγει δαπανηρά λάθη. Τέτοιες εξηγήσεις βελτιώνουν τα μοντέλα τεχνητής νοημοσύνης, αυξάνουν την εμπιστοσύνη στο σύστημα και βοηθούν στον εντοπισμό σφαλμάτων και ζητημάτων απόδοσης.

Τα τελευταία χρόνια, η πληθώρα ιδιωτικών και δημόσιων ιδρυμάτων, εταιρειών και οργανισμών έχουν αφιερώσει πολλές προσπάθειες για τη θέσπιση και τη διευθέτηση των αρχών και των κανονισμών που υποδηλώνουν με ποιον τρόπο πρέπει να αναπτυχθεί, να εφαρμοστεί η τεχνητή νοημοσύνη στον κόσμο μας. Αυτοί οι κανονισμοί αναγνωρίζονται ευρέως ως αρχές AI, οι οποίες προτείνονται για την επίλυση των ζητημάτων που σχετίζονται με πιθανούς κινδύνους AI σε άτομα, οργανισμούς και τη συνολική δημόσια κοινότητα. Όλες αυτές οι προσπάθειες επιδιώκουν να καταστήσουν την ανάπτυξη της τεχνητής νοημοσύνης πιο υπεύθυνη στην πράξη.

Από τη σκοπιά του ανθρωποκεντρικού τρόπου λήψης αποφάσεων, οι τυπικοί αλγόριθμοι AI αφήνουν ένα ουσιαστικό ερώτημα αναπάντητο: με ποιον τρόπο οι υπεύθυνοι λήψης αποφάσεων μπορούν να εμπιστευτούν τα αποτελέσματα των αλγορίθμων AI και να δικαιολογήσουν τη χρήση τους; Η επίτευξη εμπιστοσύνης και η ανακάλυψη της επικύρωσης δύσκολα μπορεί να επιτευχθεί εάν ο άνθρωπος δεν είναι σε θέση να αποκτήσει πρόσβαση σε μια λογική εξήγηση για τους εσωτερικούς υπολογισμούς που οδηγούν τις αποφάσεις AI.

Ορισμένες εφαρμογές τεχνητής νοημοσύνης είναι γνωστό ότι έχουν κρίσιμα αποτελέσματα που μπορούν να απειλήσουν την ασφάλεια των ανθρώπων, π.χ. αυτοοδηγούμενα οχήματα, ιατρική διάγνωση βάσει δεδομένων, εκτίμηση ασφαλιστικού κινδύνου κ.λπ. Σε όλες αυτές τις περιπτώσεις, η εσφαλμένη παραγωγή αλγορίθμων μπορεί να οδηγήσει σε επιζήμιο αποτέλεσμα, το οποίο έχει δημιουργήσει την ανάγκη να διασφαλιστεί ότι οι αποφάσεις δεν λαμβάνονται αποκλειστικά με βάση τον χειρισμό δεδομένων.

Δυστυχώς, η πλειοψηφία των αλγορίθμων ML και DL έχουν χαρακτηριστεί ως «μαύρα κουτιά» από ακαδημαϊκούς επειδή η δομική τους κατασκευή είναι πολύπλοκη και είναι δύσκολο να εξηγηθούν και να δικαιολογηθούν στους ανθρώπους. Μια τέτοια αδιαφάνεια έχει δημιουργήσει την ανάγκη για εξηγήσιμους αλγόριθμους AI (XAI), η οποία υποκινείται κυρίως από τρεις παραμέτρους: 1) την ανάγκη καινοτομίας και δημιουργίας όσο το δυνατόν διάφανων αλγορίθμων μάθησης. 2) την ανάγκη για μεθόδους που επιτρέπουν στα ανθρώπινα άτομα να αλληλεπιδρούν και να συνεργάζονται μαζί τους. και 3) την ανάγκη για πίστη καθώς και αξιοπιστία στη λήψη αποφάσεων για την τεχνητή νοημοσύνη. Τα συστήματα τεχνητής νοημοσύνης που

βασίζονται σε δεδομένα θα πρέπει να λογοδοτούν, καθώς η λογοδοσία θεωρείται ότι θα καταστεί επίσημη απαίτηση πολύ σύντομα. Το άρθρο 22 του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ) ορίζει τα δικαιώματα και τις υποχρεώσεις που συνδέονται με τη χρήση της αυτοματοποιημένης λήψης αποφάσεων. Αποτελεί παράδειγμα του «δικαιώματος εξήγησης» παρέχοντας στα άτομα το δικαίωμα να λάβουν μια εξήγηση για τα αποτελέσματα που παράγονται αυτόματα από μια λύση τεχνητής νοημοσύνης, καθώς και να αμφισβητήσουν και να προκαλέσουν μια σχετική αναφορά, ιδιαίτερα όταν μπορεί να επηρεάσει δυσμενώς έναν άνθρωπο νομικά, οικονομικά, φυσιολογικά ή διανοητικά. Με την έγκριση του άρθρου GDPR, το Ευρωπαϊκό Κοινοβούλιο έσπευσε να διευθετήσει το δίλημμα που σχετίζεται με τη διάδοση δυνητικά παράλογων συμπερασμάτων στην κοινότητα, τα οποία ένας υπολογιστικός αλγόριθμος θα μπορούσε να έχει καταφέρει να μάθει από ακατάλληλα και παραπλανητικά δεδομένα[45].

Ο τομέας της τεχνητής νοημοσύνης συνεχίζει να φέρνει επανάσταση στον κόσμο μας και να προσαρμόζει τη μεθοδολογία με την οποία ενεργεί και συμπεριφέρεται ο ψηφιακός κόσμος. Αυτή η ταχεία ανάπτυξη στην τεχνητή νοημοσύνη προσφέρει στον ακαδημαϊκό χώρο και τη βιομηχανία μια μεγάλη ποικιλία τεχνικών, καθεμία προσαρμοσμένη για την αντιμετώπιση ενός συγκεκριμένου φάσματος προβλημάτων. Σε αυτό το πλαίσιο, η μηχανική μάθηση παρουσιάστηκε ως ένα υποπεδίο της τεχνητής νοημοσύνης που μπορεί να επιτρέψει το σχεδιασμό αυτοματοποιημένων αποφάσεων και αναλυτικών λύσεων εκπαιδεύοντας ευφυείς αλγόριθμους για την εκμάθηση εγγενών μοτίβων από δεδομένα. Ωστόσο, με την εμφάνιση των μεγάλων δεδομένων, η ML καθίσταται ανίκανη να αποκτήσει διορατικές αναλύσεις λόγω της πολυπλοκότητας και της υψηλής διάστασης των δεδομένων. Ως θεραπεία, η βαθιά μάθηση έχει εξελιχθεί ως κλάδος της ML που ενδιαφέρεται για την ανάπτυξη διαφορετικών κατηγοριών σύνθετων και βαθιών νευρωνικών δικτύων (NN) για την ανίχνευση και την εκμάθηση εγγενών αναπαραστάσεων από τέτοια δεδομένα μεγάλου μεγέθους. Δυστυχώς, με την αυξημένη πολυπλοκότητα των λύσεων DL να κυριαρχούν στην πλειοψηφία των εφαρμογών της επιστήμης των υπολογιστών, αποδείχθηκαν αδιαφανείς και αδύνατο να κατανοηθούν από τους ανθρώπινους ενδιαφερόμενους ή ακόμα και τους ειδικούς του τομέα. Αυτό με τη σειρά του εγείρει πολλά ερωτήματα σχετικά με τη δικαιοσύνη, τη λογοδοσία, την εμπιστοσύνη και την ευθύνη.

Η εξήγηση του τρόπου λειτουργίας των αλγορίθμων ML/DL είναι το μέρος της διαφάνειας για τη συλλογιστική σχετικά με τα αποτελέσματα και τις αποφάσεις τους, η οποία μπορεί να εξηγήσει τη συμπεριφορά τους με τρόπους κατανοητούς από τον άνθρωπο μέσω της ανάπτυξης ερμηνεύσιμων μοντέλων, μεθόδων και διεπαφών. Αρκετές μέθοδοι XAI αντιμετωπίζουν το ζήτημα της έλλειψης διαφάνειας και ερμηνευσιμότητας στους αλγόριθμους τεχνητής νοημοσύνης μαύρου κουτιού. Αυτό οφείλεται στην περίπλοκη εσωτερική δομή των μοντέλων και στην έλλειψη προσφοράς ερμηνευσιμότητας ώστε να μπορούν να υποστηριχθούν υψηλές επιδόσεις στα μοντέλα AI. Η εξέταση της αδιαφανούς φύσης των πολύπλοκων μοντέλων έχει εμποδίσει τις μελλοντικές εφαρμογές τους στη δημιουργία κρίσιμων αποφάσεων, όπως ο βιομηχανικός έλεγχος και τα αυτόνομα αυτοκίνητα, τα οποία μπορούν να θέσουν σε κίνδυνο τη ζωή και την υγεία των ανθρώπων.

[45] Sina Mohseni, Niloofar Zarei, and Eric D. Ragan. 2021. A Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems. ACM Trans. Interact. Intell. Syst. 11, 3–4 (2021), 1–45. 10.1145/3387166.

5.2 Η Επεξηγηματική Τεχνητή Νοημοσύνη (eXplainable Artificial Intelligence, XAI)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ (GDPR) στα άρθρα 13, 14 και 22 τονίζει το δικαίωμα του ανθρώπου οι μηχανικές αποφάσεις, να γίνονται αντιληπτές και ερμηνεύσιμες. Για παράδειγμα η απόρριψη ενός βιογραφικού από ένα σύστημα ΤΝ, να δίνει τη δυνατότητα στον ενδιαφερόμενο να αναζητήσει τους λόγους που απορρίφθηκε σε περίπτωση που αμφισβητηθεί η ορθότητα της απόφασης. Η Επεξηγηματική ΤΝ (eXplainable Artificial Intelligence, XAI) έχει αναπτυχθεί ως υποπεδίο της ΤΝ, με στόχο την παρουσίαση πολύπλοκων συστημάτων ΤΝ στους ανθρώπους με δομημένο και κατανοητό τρόπο[46]. Η προσέγγιση που θα αυξήσει την εμπιστοσύνη και την διαφάνεια πολλών αξιόπιστων αυτόνομων συστημάτων διακρίνεται σε δύο στάδια. Στο πρώτο στάδιο κατά την δημιουργία αποφάσεων, ένα κριτήριο που θα λαμβάνεται πάντα υπόψη είναι η κατανόηση των αποφάσεων αυτών από τον άνθρωπο, το γενικό αυτό πλαίσιο συχνά ονομάζεται ερμηνευσιμότητα. Στο δεύτερο στάδιο θα ακολουθεί η ρητή αιτιολόγηση των αποφάσεων στους ανθρώπους, το οποίο ονομάζεται επεξήγηση[47].

Η XAI έχει γενικά πολύ μικρή ικανότητα πρόβλεψης ή είναι άκαμπτη και υπολογιστικά δύσκολη να εφαρμοστεί, παρά το γεγονός ότι έχει προβλέψεις που είναι εύκολο να κατανοηθούν και να εξηγηθούν. Η απόδοση των αλγορίθμων XAI μπορεί αναπόφευκτα να επιδεινωθεί με τη μέθοδο εξηγησιμότητας, με άλλα λόγια, η απόδοση υποφέρει καθώς οι μέθοδοι εξήγησης γίνονται πιο περίπλοκες ενώ ταυτόχρονα η μικρής κλίμακας τυποποίηση των συσκευών IoT θέτει αυστηρούς περιορισμούς στην πολυπλοκότητα της λύσης XAI.

Με την αλματώδη πρόοδο και την αλλαγή συσχετίσεων στον ψηφιακό κόσμο, τα συστήματα και το λογισμικό είναι συνήθως επιρρεπή σε ένα ευρύ φάσμα απειλών για την ασφάλεια και επιθέσεων στον κυβερνοχώρο. Οι αλγόριθμοι AI έχουν αποδειχθεί ως καλύτερη λύση για την ανίχνευση αυτών των κυβερνοεπιθέσεων. Ωστόσο, σχεδόν όλες οι λύσεις ασφάλειας που βασίζονται σε AI δίνουν αποφάσεις Black-Box που μπορεί να είναι ανερμήνευτες ακόμη και για ειδικούς ασφαλείας. Ως εκ τούτου, η πρόοδος προς την εξήγηση λύσεων ασφάλειας αναμένεται ως μια πολλά υποσχόμενη κατεύθυνση για τη βελτίωση της ασφάλειας των δημόσιων και ιδιωτικών συστημάτων.

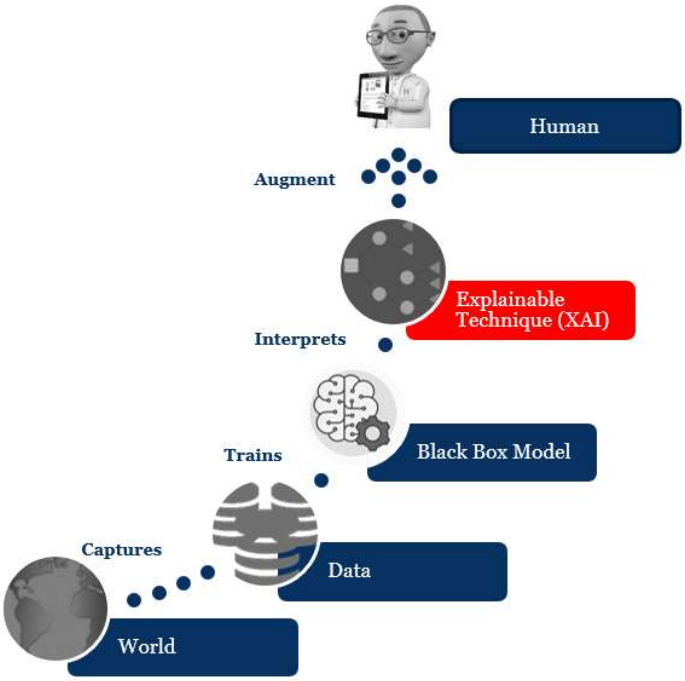
Ο ψηφιακός κόσμος είναι γνωστό ότι περιέχει μεγάλο όγκο δεδομένων σε πολλαπλές τοποθεσίες κάτι που προκαλεί ανησυχίες για την προστασία της ιδιωτικής ζωής κατά την αποθήκευση ή τη μετάδοση των δεδομένων αυτών. Αυτό καθίσταται ιδιαίτερα κρίσιμο όταν οι αλγόριθμοι τεχνητής νοημοσύνης ασχολούνται με ιδιωτικά δεδομένα, καθώς πρέπει να αντιμετωπιστούν τα δικαιώματα προστασίας της ιδιωτικής ζωής των ανθρώπων. Δεδομένου ότι οι αλγόριθμοι XAI έχουν σχεδιαστεί για να είναι ερμηνεύσιμοι για τον άνθρωπο δημιουργεί σοβαρές ανησυχίες σχετικά με τους συμβιβασμούς απορρήτου-εξηγησιμότητας καθώς είναι κρίσιμο να υπάρχει επιβεβαίωση ότι οι αλγόριθμοι XAI δεν απειλούν το απόρρητο των δεδομένων κατά τη διάρκεια της εξέλιξης τους ή κατά τη διάρκεια της εξαγωγής συμπερασμάτων.

[46] W. Samek et al. (Eds.): Explainable AI, LNAI 11700, pp. 5–7, 2019.
https://doi.org/10.1007/978-3-030-28954-6_8

[47] Miller T (2019). Explanation in artificial intelligence: Insights from the social sciences. Artificial Intelligence, Vol.267 1-38
https://doi.org/10.1016/j.artint.2018.07.007

5.3 Το Μοντέλο του «Μαύρου Κουτιού» (AI Black Box)

Με την ολοένα και αυξανόμενη εξέλιξη των νευρωνικών δικτύων Βαθιάς Μάθησης που χρησιμοποιούν συστήματα ΤΝ, η δυσκολία που διακρίνεται εντοπίζεται στην ύπαρξη διαφάνειας και επεξήγησης των εξαγόμενων αποτελεσμάτων. Η αδυναμία κατανόησης πλήρως της διαδικασίας λήψης αποφάσεων ή των αποτελεσμάτων, ορίζεται ως ένα μοντέλο ΤΝ «Μαύρου Κουτιού» (AI Black Box), καθώς για κάθε απόφαση που παίρνει ένα νευρωνικό δίκτυο Βαθιάς Μάθησης, συνεργάζονται χιλιάδες ή εκατοντάδες χιλιάδες νευρώνες. Ένας αλγόριθμος AI ανακηρύσσεται Black-Box εάν και μόνο εάν η κατασκευή, οι εσωτερικές λειτουργίες, η λογική και οι παράμετροί του είναι απρόσιτες για τον άνθρωπο και ως εκ τούτου είναι αδιαφανείς. Έτσι, το αδιαφανές AI μπορεί να δηλωθεί ως συνώνυμο με το Black-Box AI και οι δύο όροι μπορούν να χρησιμοποιηθούν εναλλακτικά. Με την προϋπόθεση ύπαρξης αλγορίθμου AI "Black-Box", η πρόκληση στην εξήγηση του μοντέλου Black-Box έγκειται στην προσφορά ενός εξηγήσιμου μοντέλου που μπορεί να προσομοιώσει τη συμπεριφορά του μαύρου κουτιού και επίσης να παραμείνει κατανοητό στους ανθρώπους. Συγκεκριμένα, το εξηγήσιμο μοντέλο που μοιάζει με το μαύρο κουτί πρέπει να είναι γενικά κατανοητό. Συνέπεια αυτής της πολυπλοκότητας είναι η δυσκολία κατάρτισης νομοθετικού πλαισίου για συστήματα ΤΝ και ιδίως για τα εξελιγμένα αυτόματα συστήματα, όπου η αδυναμία ερμηνείας δόλου και αιτιώδους συνάφειας, στοιχείων απαραίτητων για την διερεύνηση μιας αδικοπραξίας απαντάται σχεδόν σε κάθε πεδίο του δικαίου[48].



XAI – Black Box Model Πηγή: *https://www.linkedin.com/pulse/holy-grail-ai-enterprise-explainable-xai-saurabh-kaushik*

[48] Yavar Bathaee Harvard Journal of Law & Technology Vol 31, Number 2 Spring 2018

5.4 Σύσταση Νομικής Προσωπικότητας για προϊόντα ΤΝ (Ρομπότ)

Καθώς τα ρομπότ γίνονται πιο εξελιγμένα και ανεξάρτητα, υπάρχει μια αυξανόμενη ανάγκη για τους ανθρώπους να κατανοήσουν τι κάνουν και πως σκέφτονται. Επειδή τα ρομπότ μπαίνουν με την πρόοδο της τεχνολογίας ολοένα και περισσότερο σε καταστάσεις που η αλληλεπίδραση με ανθρώπους στον φυσικό κόσμο είναι πιο συχνή, γίνεται όλο και πιο ζωτικής σημασίας για τους ανθρώπους να διατηρούν ένα λογικό επίπεδο εμπιστοσύνης στα ρομπότ. Η ικανότητα εξήγησης της γνώσης και του σκεπτικού πίσω από τις αποφάσεις, όπως στις ανθρώπινες σχέσεις, ενισχύει σημαντικά την εμπιστοσύνη αναπτύσσοντας την κατανόηση του γιατί ελήφθη μια απόφαση και κατά συνέπεια προσφέρει μια εικόνα για μελλοντικές αποφάσεις.

Στο ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 201749 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)) στη παράγραφο 59 (στ) αναφέρεται το εξής:

Τη δημιουργία μακροπρόθεσμα ενός ειδικού νομικού καθεστώτος για τα ρομπότ, ώστε τουλάχιστον τα πιο εξελιγμένα, αυτόνομα ρομπότ να αναγνωρίζονται ως ηλεκτρονικά πρόσωπα με υποχρέωση επανόρθωσης τυχόν ζημίας που προκαλούν, και ενδεχομένως εφαρμογή της ηλεκτρονικής αυτής προσωπικότητας σε περιπτώσεις στις οποίες τα ρομπότ λαμβάνουν αυτόνομα αποφάσεις ή έρχονται με άλλον τρόπο σε ανεξάρτητη διάδραση με τρίτα μέρη.

Με τον όρο Ρομποτική εννοούμε την «δράση της ΤΝ στον φυσικό κόσμο». Μερικά παραδείγματα αποτελούν τα αυτόνομα αυτοκίνητα, ΣμηΕΑ (Συστήματα μη Επανδρωμένων Αεροσκαφών), ρομποτικές σκούπες κ.α.[50]

Σήμερα, σχεδόν όλα τα θέματα που σχετίζονται με τη ρύθμιση της ευθύνης των μη επανδρωμένων οχημάτων σχετίζονται με τον τομέα της ασφάλισης, αλλά αυτό δεν παρέχει ενιαία ρύθμιση της ευθύνης σε σχέση με τα θύματα τροχαίων ατυχημάτων, δεδομένου ότι η ευθύνη του οδηγού δεν ρυθμίζεται με τον ίδιο τρόπο σε διαφορετικές χώρες.

Εάν εξετάσουμε τα ζητήματα ασφάλισης αυτοκινήτων σε σχέση με το δίκαιο της ΕΕ, τότε πρέπει να πούμε ότι περιέχει μόνο δύο σημαντικά σημεία: τα οχήματα πρέπει να ασφαλίζονται με ασφάλιση αυτοκινήτου και τα θύματα μπορούν να εγείρουν αξιώσεις απευθείας στον ασφαλιστή. Ωστόσο, ο ασφαλιστικός κίνδυνος αξιολογείται διαφορετικά στα διάφορα κράτη μέλη (Evas, 2018). Επιπλέον, η υποχρεωτική ασφάλιση δεν οδηγεί από μόνη της σε ένα σύστημα χωρίς υπαιτιότητα, αλλά αντικαθιστά μόνο τον ασφαλισμένο με τον ασφαλιστή σε περίπτωση αδικοπραξίας (Patti, 2019). Επιπλέον, οι οδηγοί αυτοοδηγούμενων οχημάτων μπορούν να πέσουν θύματα ατυχήματος στο οποίο εμπλέκεται το δικό τους αυτοκίνητο, το οποίο υπερβαίνει πλήρως τους υφιστάμενους κανόνες. Όσο πιο αυτόνομο γίνεται το σύστημα, τόσο λιγότερο ο οδηγός μπορεί να θεωρηθεί υπεύθυνος για τυχόν ατυχήματα (Marchant et al, 2012).

[49] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52017IP0051&from=EN
[50] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341

5.5 Αιτιολογική έκθεση JURI για την έκθεση (2015/2103(INL))

Η Επιτροπή Νομικών Θεμάτων του Ευρωπαϊκού Κοινοβουλίου (JURI) Στην αιτιολογική της έκθεση [51] η επιτροπή επισημαίνει :

Η επιτροπή JURI πιστεύει ότι οι κίνδυνοι που απορρέουν από τις νέες αυτές αλληλεπιδράσεις πρέπει να αντιμετωπιστούν εγκαίρως και να διασφαλιστεί ότι εφαρμόζεται μια δέσμη βασικών θεμελιωδών αξιών σε κάθε στάδιο επαφής μεταξύ ρομπότ, τεχνητής νοημοσύνης και ανθρώπων. Κατά την διαδικασία αυτή πρέπει να δοθεί ιδιαίτερη έμφαση στην ασφάλεια, ιδιωτικότητα, ακεραιότητα, αξιοπρέπεια και αυτονομία των ανθρώπων.

Άλλες σημαντικές πτυχές που αποτελούν αντικείμενο αυτού του ψηφίσματος είναι: τυποποίηση, δικαιώματα πνευματικής ιδιοκτησίας, κυριότητα δεδομένων, εργασία και ευθύνη.

5.6 Ηθική και Τεχνητή Νοημοσύνη

Οι κατευθυντήριες γραμμές δεοντολογίας[52] για αξιόπιστη τεχνητή νοημοσύνη, σύμφωνα με την ομάδα εμπειρογνωμόνων υψηλού επιπέδου της Ευρωπαϊκής Επιτροπής για την τεχνητή νοημοσύνη, βασίζονται στην ανθρωποκεντρική και αξιόπιστη τεχνητή νοημοσύνη. Ο Χάρτης των Θεμελιωδών Δικαιωμάτων[53] και ο ΓΚΠΔ της Ευρωπαϊκής Ένωσης επισημαίνουν ρητά ότι ο σεβασμός της ανθρώπινης αξιοπρέπειας αποτελεί ύψιστη προτεραιότητα. Τα συστήματα τεχνητής νοημοσύνης θα πρέπει να σχεδιάζονται και να αναπτύσσονται κατά τρόπο ώστε να μην υπονομεύουν ή να βλάπτουν τους ανθρώπους. Λαμβάνοντας υπόψη τον ΓΚΠΔ (άρθρο 25) για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού, τόσο κατά τον καθορισμό των μέσων επεξεργασίας όσο και κατά τη στιγμή της ίδιας της επεξεργασίας, πρέπει να ληφθούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Τα μέτρα αυτά αποσκοπούν στην αποτελεσματική εφαρμογή των αρχών προστασίας των δεδομένων και στην ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία, προκειμένου να πληρούνται οι απαιτήσεις της από τον ΓΚΠΔ και την προστασία των δικαιωμάτων του υποκειμένου των δεδομένων.

Σύμφωνα με τις κατευθυντήριες γραμμές δεοντολογίας, η δυνατότητα επεξήγησης αποτελεί προϋπόθεση για την επίτευξη συναίνεσης, κατόπιν ενημέρωσης, από άτομα που αλληλεπιδρούν με συστήματα τεχνητής νοημοσύνης. Προκειμένου να διασφαλιστεί η επίτευξη της αρχής της επεξηγησιμότητας και της πρόληψης βλάβης, θα πρέπει να επιδιωχθεί η απαίτηση συναίνεσης μετά από ενημέρωση.

5.7 AI και GDPR

Η σύγκρουση μεταξύ AI και GDPR εκδηλώνεται στην αυτονομία των συστημάτων AI, οδηγώντας σε ζητήματα συμμόρφωσης με την αρχή λογοδοσίας του GDPR. Αυτό εγείρει το ερώτημα: «Μπορεί ένα σύστημα ΤΝ να συνάπτει συμφωνίες επεξεργασίας δεδομένων και να αλληλεπιδρά με ιδιώτες και υπευθύνους επεξεργασίας δεδομένων χωρίς παρέμβαση του κατόχου του και ο ιδιοκτήτης εξακολουθεί να είναι υπεύθυνος για τις αποφάσεις που λαμβάνει και τις ενέργειες στις οποίες προβαίνει το σύστημα

[51] https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EL.html#title9

[52] https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf

[53] Charter of Fundamental Rights of the European Union, OJ C 326, Standard 26.10.2012, European Union, 2012, pp. 391–407.

ΤΝ;». Δεν είναι σαφές αν τα συστήματα ΤΝ θεωρούνται υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία. Τα συστήματα ΤΝ ενδέχεται να συνάγουν παράλογα συμπεράσματα και αποφάσεις και να προβαίνουν σε επιβλαβείς ενέργειες, οι οποίες ενδέχεται να έχουν επιβλαβείς επιπτώσεις στην ανθρώπινη ζωή, καθώς και να οδηγούν σε άδικες και μη εφέσιμες αποφάσεις των νομικών αρχών όσον αφορά τις κυρώσεις.

Τα συστήματα τεχνητής νοημοσύνης, είτε βασίζονται σε θεωρητικές είτε σε εμπειρικές βάσεις, χαρακτηρίζονται ως πολυεπίπεδα συστήματα με πολύπλοκους αλγορίθμους και λογικές ML που χρησιμοποιούνται για την αυτοματοποίηση της επεξεργασίας προσωπικών δεδομένων και της λήψης αποφάσεων. Έτσι, καθίσταται δύσκολο να εξηγηθούν τα συμπεράσματα, οι αποφάσεις και οι ενέργειες αυτών των συστημάτων. Η δυσκολία εξήγησης της λογικής επεξεργασίας δεδομένων και λήψης αποφάσεων των συστημάτων ΤΝ εγείρει ζητήματα διαφάνειας, συμμόρφωσης όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει του ΓΚΠΔ. Ο ΓΚΠΔ απαιτεί από τους υπευθύνους επεξεργασίας να παρέχουν στο υποκείμενο των δεδομένων πληροφορίες σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, προκειμένου να διασφαλίζεται η δίκαιη και διαφανής επεξεργασία. Το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης σε αυτές τις πληροφορίες και σε περαιτέρω σημαντικές πληροφορίες σχετικά με τη λογική που διέπει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, καθώς και τις σημαντικές και αναμενόμενες συνέπειες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων. Τούτο μπορεί να εγείρει ανησυχίες όσον αφορά το δικαίωμα του υποκειμένου των δεδομένων να μην υπόκειται σε απόφαση βασιζόμενη αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία το επηρεάζει σημαντικά.

Παρόλο που ο ΓΚΠΔ δεν απαιτεί ρητά από τους υπευθύνους επεξεργασίας να διασφαλίζουν την πολιτική απορρήτου, οι υποχρεώσεις που επιβάλλονται στους υπευθύνους επεξεργασίας να παρέχουν στα υποκείμενα των δεδομένων πληροφορίες σχετικά με την επεξεργασία των προσωπικών τους δεδομένων απαιτούν έμμεσα από αυτούς να δημιουργήσουν μία. Επιπλέον, μια καλά σχεδιασμένη πολιτική προστασίας της ιδιωτικής ζωής πρέπει να είναι πλήρης, συμπεριλαμβανομένων όλων των πληροφοριών που απαιτούνται σε σαφή γλώσσα σχετικά με τη θεμιτή και παράνομη επεξεργασία, ώστε τα υποκείμενα των δεδομένων να μπορούν να κατανοούν όλες τις πτυχές της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν και να ασκούν τα δικαιώματά τους βάσει του ΓΚΠΔ. Επομένως, η ισχύς των αλγορίθμων AI και ML μπορεί να βοηθήσει τους υπευθύνους επεξεργασίας να προβούν σε αυτοματοποιημένη νομική ανάλυση των πολιτικών προστασίας της ιδιωτικής ζωής των διαδικτυακών πλατφορμών και υπηρεσιών τους και να βελτιώσουν τις πολιτικές αυτές προκειμένου να συμμορφωθούν με τις υποχρεώσεις πληροφόρησης που υπέχουν δυνάμει του ΓΚΠΔ. Επιπλέον, η πλειονότητα των πολιτικών προστασίας της ιδιωτικής ζωής είναι μακροσκελείς και δυσνόητες για τα υποκείμενα των δεδομένων, με αποτέλεσμα να δυσχεραίνεται η ενημέρωσή τους σχετικά με τις δραστηριότητες επεξεργασίας που ενδέχεται να λαμβάνουν χώρα επί των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, ώστε να μπορούν να λαμβάνουν τεκμηριωμένες αποφάσεις όσον αφορά την παροχή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Οι αλγόριθμοι ML μπορούν να χρησιμοποιηθούν για την αυτόματη σύνοψη των πολιτικών απορρήτου των ελεγκτών, ώστε να μπορούν τα υποκείμενα των δεδομένων να ασκούν τα δικαιώματά τους να ενημερώνονται σχετικά με τις δραστηριότητες επεξεργασίας δεδομένων βάσει του GDPR και, ως εκ τούτου, να

λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την αποκάλυψη των προσωπικών τους δεδομένων.

Η τροφοδότηση των αλγορίθμων μπορεί να παρέχει μια μεροληπτική αναπαράσταση της πραγματικότητας, η οποία έρχεται σε σύγκρουση με την αρχή της δικαιοσύνης της επεξεργασίας προσωπικών δεδομένων βάσει του GDPR. Αυτό εκδηλώνεται με την αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ που δίνει έμφαση σε φυλετικά, πολιτικά, θρησκευτικά δεδομένα, δεδομένα υγείας ή σεξουαλικά δεδομένα στο μοντέλο κατάρτισης δεδομένων και μπορεί να οδηγήσει σε διακριτική μεταχείριση των υποκειμένων των δεδομένων.

Η χρήση αλγορίθμων ML εγείρει ζητήματα συμμόρφωσης με την αρχή περιορισμού του σκοπού του GDPR, η οποία ορίζει ότι τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο με αυτούς τους σκοπούς.

Οι αλγόριθμοι μπορούν να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για άλλους διφορούμενους σκοπούς από εκείνους για τους οποίους συλλέχθηκαν αρχικά τα δεδομένα και να παράγουν νέους τύπους δεδομένων· επομένως, ο σκοπός για τον οποίο θα χρησιμοποιηθούν τα δεδομένα παραμένει ασαφής για τα υποκείμενα των δεδομένων.

Οι αλγόριθμοι ML τείνουν να συλλέγουν και να επεξεργάζονται μεγάλα προσωπικά δεδομένα και να τα επαναπροσδιορίζουν, σε σύγκρουση με την αρχή ελαχιστοποίησης δεδομένων του GDPR, η οποία απαιτεί τα προσωπικά δεδομένα να είναι επαρκή, συναφή και να περιορίζονται σε ό, τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Επιπλέον, η επεξεργασία και η αναπροσαρμογή της χρήσης μαζικών δεδομένων προσωπικού χαρακτήρα καθιστά δύσκολη την απόκτηση «ενημερωμένης και σαφούς» συγκατάθεσης από τα υποκείμενα των δεδομένων «με δήλωση ή με σαφή θετική ενέργεια», όπως απαιτείται από τον ΓΚΠΔ.

5.8 Αξιολόγηση Θεμάτων Ασφάλειας στα Ευφυή Συστήματα Μεταφορών

Σύμφωνα με Τεχνική Έκθεση του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων το 2010 (ETSI TR 102 893 V1.1.1)[54] στο πλαίσιο μιας ανάλυσης απειλών, ευπάθειας και κινδύνων (Threat, Vulnerability and Risk Analysis, TVRA) με τις ραδιοεπικοινωνίες να διενεργούνται στο φάσμα των 5,9 GHz σε ένα ευφυές σύστημα μεταφορών, όπως αυτή επικαιροποιήθηκε το 2017 (ETSI TR 102 893 V1.2.1)[55], καταδεικνύονται 5 στόχοι -πυλώνες που πρέπει να επιτευχθούν γύρω από την ασφάλεια στα Ευφυή Συστήματα Μεταφορών και αυτά είναι: η Εμπιστοσύνη (Confidentiality), η Ακεραιότητα (Integrity), η Διαθεσιμότητα (Availability), η Λογοδοσία (Accountability) και η Αυθεντικότητα (Authenticity).

Εμπιστοσύνη

[54] ETSI TR 102 893 V1.1.1: Technical Report, Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (2010)

[55] ETSI TR 102 893 V1.2.1: Technical Report, Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (2017) https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/tr_102893v010201p.pdf

Τα δεδομένα που ανταλλάσσονται μεταξύ χρηστών ITS πρέπει να είναι μη προσβάσιμα από μη εξουσιοδοτημένα άτομα. Οι πληροφορίες θα πρέπει να κρυπτογραφούνται, και να υπάρχει αμφίδρομη επαλήθευση της ταυτότητας του παραλήπτη και του αποστολέα, ενώ ταυτόχρονα θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, το ίδιο ισχύει και για τις πληροφορίες που διατηρούνται εντός των ITS-S. Τα ITS, θα πρέπει εκ του σχεδιασμού να επιτρέπουν μόνο σε εξουσιοδοτημένες εφαρμογές ITS να έχουν πρόσβαση σε πληροφορίες παραμέτρων ασφαλείας και μόνο εξουσιοδοτημένοι χρήστες ITS πρέπει να επιτρέπεται να έχουν πρόσβαση σε περιορισμένες πληροφορίες. Δεν θα πρέπει να είναι δυνατό για ένα μη εξουσιοδοτημένο μέρος να συμπεράνει την τοποθεσία ή την ταυτότητα των τελικών χρηστών ITS αλλά ούτε και τη διαδρομή που ακολουθούν με τα οχήματα τους, αναλύοντας την διαδρομή των δεδομένων που αποστέλλονται από και προς το όχημα χρηστών ITS. Οι πληροφορίες διαχείρισης που αποστέλλονται από ή προς ένα ITS-S και οι πληροφορίες διαχείρισης που φυλάσσονται σε ένα ITS-S, θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση. Οι απειλές για την αξιοπιστία των πληροφοριών περιλαμβάνουν την παράνομη συλλογή δεδομένων και τη συλλογή πληροφοριών τοποθεσίας. Ταυτόχρονα, ο εισβολέας μπορεί να κατασκευάσει ένα προφίλ ITS παρατηρώντας ποιες υπηρεσίες χρησιμοποιούνται τακτικά, πότε και πού.

Ακεραιότητα

Τα δεδομένα που φυλάσσονται στα ITS, πρέπει να προστατεύονται από μη εξουσιοδοτημένη διαγραφή και τροποποίηση. Μόνο εξουσιοδοτημένοι χρήστες και εφαρμογές ITS πρέπει να επιτρέπεται να τροποποιούν ή να διαγράφουν δεδομένα και επιπλέον κατά τη μετάδοση πληροφορίων απαιτείται προστασία στη χειραγώγηση και στη κακόβουλη τροποποίηση τους. Πρέπει να υπάρχει πρόβλεψη για την προστασία των πληροφοριών διαχείρισης που αποστέλλονται προς ή από ένα ITS-S στη χειραγώγηση ή την τροποποίηση των δεδομένων ενώ ταυτόχρονα οι πληροφορίες διαχείρισης που φυλάσσονται σε ένα ITS-S, θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση και διαγραφή. Οι απειλές για την ακεραιότητα των ITS συνίστανται στην απώλεια, τη διαφθορά και τη χειραγώγηση των πληροφοριών. Η μη εξουσιοδοτημένη πρόσβαση σε περιορισμένες πληροφορίες είναι δυνατή με τη χρήση κακόβουλου λογισμικού που εγκαθίσταται στο σταθμό ITS.

Διαθεσιμότητα

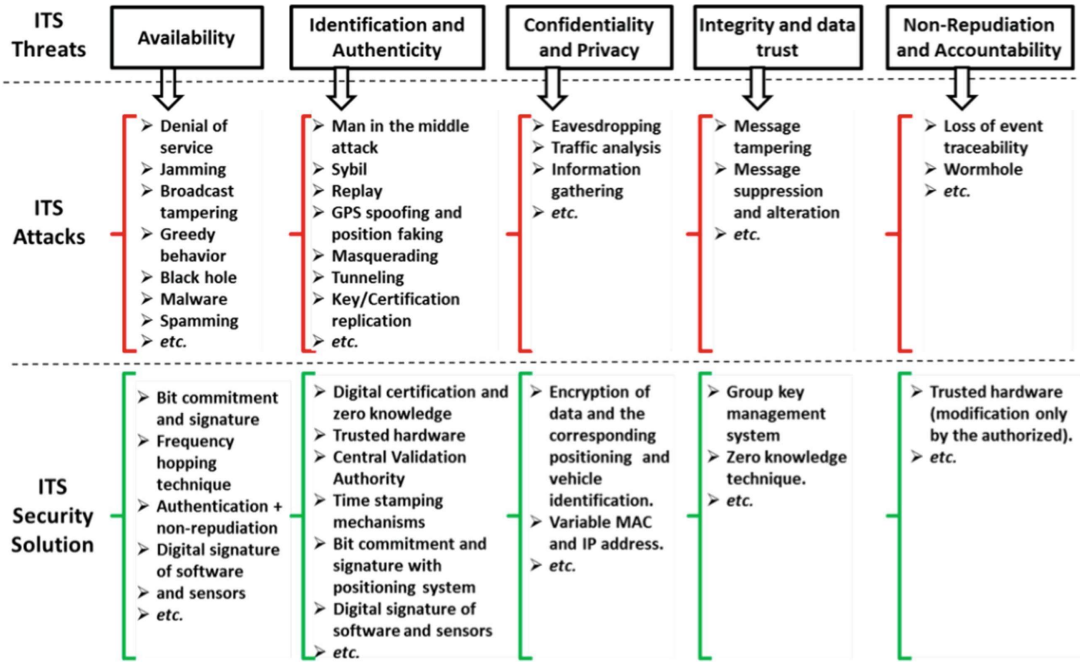
Για τη διαθεσιμότητα, δηλαδή την άμεση και απρόσκοπτη πρόσβαση στη λειτουργία των υπηρεσιών ITS από εξουσιοδοτημένους χρήστες, δεν θα πρέπει υπάρχουν εμπόδια από κακόβουλη δραστηριότητα εντός του περιβάλλοντος ITS. Οι απειλές για τη διαθεσιμότητα των συστημάτων ITS συνίστανται σε επιθέσεις άρνησης υπηρεσιών (DoS) και πραγματοποιούνται με τη χρήση κακόβουλου λογισμικού και μηνυμάτων spam μεγάλου όγκου. Τέτοιες επιθέσεις μπορεί να έχουν ως αποτέλεσμα ο σταθμός ITS να μην έχει τη δυνατότητα να λαμβάνει ή να αναμεταδίδει πληροφορίες.

Λογοδοσία

Στόχος της λογοδοσίας θα πρέπει να είναι η δυνατότητα ελέγχου όλων των αλλαγών σε εφαρμογές και παραμέτρους ασφαλείας (ενημερώσεις, προσθήκες και διαγραφές). Η έλλειψη λογοδοσίας μπορεί να προέλθει από απώλεια κρίσιμων πληροφοριών μέσω μη εξουσιοδοτημένης πρόσβασης ή και απώλειας ιχνηλασιμότητας συμβάντων. Η λύση στο πρόβλημα της λογοδοσίας είναι η χρήση αξιόπιστου λογισμικού που θα μπορεί να τροποποιηθεί μόνο από εξουσιοδοτημένους χρήστες.

Αυθεντικότητα

Τέλος ο στόχος της αυθεντικότητας επέρχεται όταν είναι αδύνατο για έναν μη εξουσιοδοτημένο χρήστη να παρουσιάζεται ως ITS-S όταν επικοινωνεί με άλλο ITS-S. Επίσης δεν θα πρέπει να είναι δυνατό για ένα ITS-S να λαμβάνει και να επεξεργάζεται πληροφορίες διαχείρισης και διαμόρφωσης από μη εξουσιοδοτημένο χρήστη. Η αυθεντικότητα είναι σημαντικό πρόβλημα ασφαλείας στα ITS, καθώς όλοι οι σταθμοί ITS έχουν τη δυνατότητα λήψης και αποστολής όλων των τύπων μηνυμάτων. Η διασφάλιση της αυθεντικότητας των πληροφοριών που επεξεργάζονται και λαμβάνονται από τα ITS περιλαμβάνει: προστασία του σταθμού ITS από επίθεση, έκθεση λανθασμένων σημάτων GNSS[56] και προστασία από λανθασμένα μηνύματα μετάδοσης.

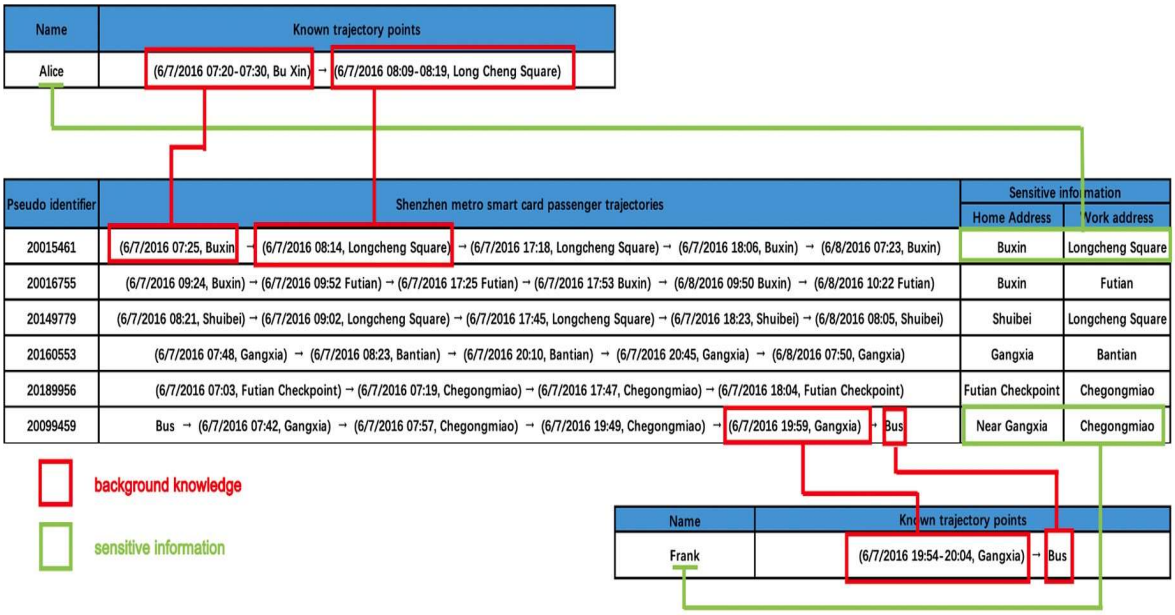


Εικόνα 17: Απειλές, Επιθέσεις και Λύσεις Ασφάλειας στα ITS

5.9 Παραβιάσεις της Ιδιωτικότητας με τα Δεδομένα Κίνησης και Θέσης των Επιβατών

Οι παραβιάσεις προσωπικών δεδομένων συμβαίνουν όταν οι χρήστες αναγνωρίζονται εκ νέου από ανώνυμα δεδομένα, καθώς έχει αποδειχθεί κατά το παρελθόν, ότι η αφαίρεση προσωπικών πληροφοριών και η ανωνυμοποίηση των δεδομένων δεν προστατεύει αποτελεσματικά την ιδιωτική ζωή.

[56] Global Navigation Satellite System (GNSS) refers to a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. The receivers then use this data to determine location https://www.euspa.europa.eu/european-space/eu-space-programme/what-gnss



Εικόνα 18. *Παραδείγματα επιθέσεων γνώσης υποβάθρου.*

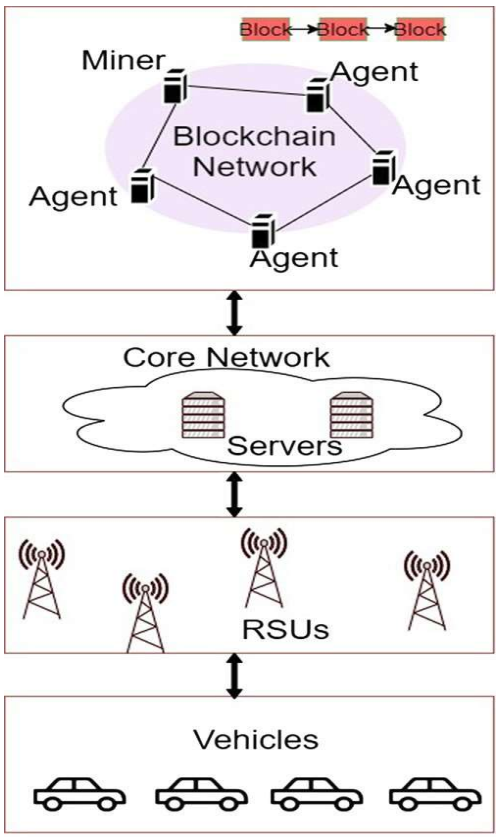
Η κόκκινη γραμμή στην Εικόνα 15 αντιπροσωπεύει τη βασική γνώση που ανήκει στον εισβολέα. Η πράσινη γραμμή αντιπροσωπεύει τις ευαίσθητες πληροφορίες που μπορεί να αποκτήσει ένας εισβολέας. Εάν ένας εισβολέας έχει ήδη γνωρίσει ότι η Alice έχει ταξιδέψει στον σταθμό "Bu Xin" εκείνη την ημέρα, γύρω στις 7:20 π.μ. - 7:30 π.μ. (δηλαδή με ακρίβεια 10 λεπτών) και στο "Long Cheng Κέντρο" σταθμός (την ίδια ημέρα) γύρω στις 8:09 π.μ. -8:19 π.μ., η μοναδική ταυτότητα της Alice μπορεί εύκολα να βρεθεί 20015461 καθώς είναι η μόνη επιβάτης με αυτά τα δύο ταξιδιωτικά αρχεία στο σύνολο δεδομένων. Με αυτές τις πληροφορίες, οι επιτιθέμενοι μπορούν να ανακαλύψουν όλα τα ιστορικά αρχεία ταξιδιού για την Alice και να τα χρησιμοποιήσουν για να συμπεράνουν ευαίσθητες προσωπικές πληροφορίες.

Οι περισσότερες επιθέσεις εναντίον δεδομένων τροχιάς (κίνησης και θέσης) ανήκουν στην κατηγορία των επιθέσεων γνώσης υποβάθρου (επίσης γνωστές ως record linkage attacks, Fung et al. 2010). Οι επιθέσεις γνώσης στο παρασκήνιο στοχεύουν στη χαρτογράφηση των εγγραφών σε ένα σύνολο δεδομένων κίνησης και θέσης που βασίζεται στις πληροφορίες που αποκτήθηκαν από τον εισβολέα. Οι πληροφορίες μπορεί να περιλαμβάνουν προσωπικές ταξιδιωτικές συνήθειες ή ευαίσθητες μεμονωμένες πληροφορίες, όπως τοποθεσία εργασίας και διεύθυνση κατοικίας. Αυτές οι πληροφορίες μπορούν εύκολα να συλλεχθούν με πολλούς τρόπους.

Μια επιτυχημένη επίθεση επιτρέπει στον εισβολέα να δημιουργήσει μια σύνδεση με εγγραφές σε ένα σύνολο δεδομένων, γεγονός που οδηγεί σε διαρροές απορρήτου, όταν οι εγγραφές περιλαμβάνουν ευαίσθητες πληροφορίες. Μέσω αυτών των συνδέσεων καταγραφής, μπορεί κανείς να αναλύσει την τοποθεσία εργασίας ενός ταξιδιώτη, τη διεύθυνση κατοικίας, το μοτίβο δραστηριότητας και άλλες ευαίσθητες πληροφορίες, με βάση τα δεδομένα κίνησης και θέσης του επιβάτη.

5.10 Blockchain & VANET

Το blockchain είναι μια τεχνολογία κατανεμημένου καθολικού (DLT) που εισήχθη από τον Satoshi Nakamoto για να υποστηρίξει το Bitcoin[57]. Χρησιμοποιεί τις έννοιες της κρυπτογραφίας, της θεωρίας παιγνίων, των κατανεμημένων συστημάτων και των τεχνολογιών επικοινωνίας. Το blockchain μπορεί να χρησιμοποιηθεί για την επίλυση αναδυόμενων ζητημάτων με τη διάδοση πληροφοριών και διαφορετικές προσεγγίσεις ασφάλειας στο VANET. Πρόκειται για μια αποκεντρωμένη και κατανεμημένη υπολογιστική τεχνολογία που παρέχει ιδιωτικότητα και ασφάλεια σε δίκτυα Peer-to-Peer (P2P).



Εικόνα 19: Αρχιτεκτονική VANET που βασίζεται σε blockchain.
Πηγή: https://www.sciencedirect.com/science/article/pii/S2214209622000055

Το πλαίσιο αποτελείται από τέσσερα επίπεδα. Το πρώτο επίπεδο περιλαμβάνει οχήματα, ενώ τα RSU αποτελούν μέρος του δεύτερου στρώματος. Το κεντρικό δίκτυο, το οποίο περιλαμβάνει διακομιστές έκδοσης πιστοποιητικών (Certificate Authority – CA), διακομιστές αποθήκευσης δεδομένων και άλλους διακομιστές με υψηλές δυνατότητες επεξεργασίας, χωρητικότητας αποθήκευσης και διαθεσιμότητα ενέργειας, είναι το τρίτο επίπεδο. Όλα τα δεδομένα αποθηκεύονται και υποβάλλονται σε επεξεργασία εντός του κεντρικού δικτύου. Τα δεδομένα που αποθηκεύονται στο κεντρικό δίκτυο κρυπτογραφούνται για λόγους ασφάλειας δεδομένων. Για να δημιουργήσει ένα δίκτυο blockchain, το τέταρτο επίπεδο χρησιμοποιεί μια ιδιωτική αλυσίδα μπλοκ δεδομένων εκτός από τη λειτουργικότητα επαλήθευσης και προώθησης

[57] https://en.wikipedia.org/wiki/Satoshi_Nakamoto

δεδομένων. Το δίκτυο blockchain αποθηκεύει τις τιμές κατακερματισμού κάθε δεδομένων στο κεντρικό δίκτυο. Αυτό διασφαλίζει ότι τα δεδομένα δεν παραβιάζονται ή αλλοιώνονται από εχθρικούς επιτιθέμενους. Επειδή εάν ενημερωθούν τα δεδομένα, η τιμή κατακερματισμού θα αλλάξει επίσης. Επιπλέον, η αποθήκευση των τιμών κατακερματισμού μπορεί να μειώσει σημαντικά τους πόρους αποθήκευσης του δικτύου blockchain, επιδεικνύοντας παράλληλα τον χρόνο αντίδρασης του συστήματος. Αποτελείται επίσης από διάφορες συναρτήσεις συναίνεσης και δομές ανταμοιβής. Διάφορα σενάρια, αλγόριθμοι και έξυπνα συμβόλαια ενσωματώνονται σε αυτό το επίπεδο. Τα έξυπνα συμβόλαια είναι συμβόλαια με προκαθορισμένους κανόνες και ρήτρες που μπορούν να εκτελεστούν αυτεπαγγέλτως. Τα έξυπνα συμβόλαια είναι πλήρως γραμμένα σε κώδικα και μόλις εκπληρωθεί η προϋπόθεση ενεργοποίησης, εκτελούνται αμέσως χωρίς την ανάγκη ανθρώπινης αλληλεπίδρασης. Στο δίκτυο blockchain, ο κόμβος πράκτορα είναι ένας κόμβος που συμμετέχει στο δίκτυο. Για να διατηρηθεί η ακρίβεια των συναλλαγών του δικτύου blockchain, κάθε κόμβος πράκτορα συμμετέχει στη συναίνεση και διατηρεί αντίγραφο ασφαλείας των δεδομένων του δικτύου. Ο κόμβος εξόρυξης είναι ένας συγκεκριμένος κόμβος πράκτορα που είναι υπεύθυνος για την επεξεργασία νέων μπλοκ blockchain και τη σύνταξη επικυρωμένων δεδομένων σε αυτά. Στη συνέχεια, όλοι οι κόμβοι πρακτόρων ανανεώνουν τα αντίγραφα ασφαλείας των δεδομένων τους στο δίκτυο blockchain. Δεν συμβάλλει μόνο στη συναίνεση του δικτύου blockchain, αλλά μπορεί επίσης να εξορύξει και να επικυρώσει νέα μπλοκ.

Στο στάδιο του σχεδιασμού λύσεων ασφαλείας για περιβάλλον VANET πρέπει να υπολογιστούν ορισμένοι σημαντικοί παράμετροι:

1. Αποκεντρωμένη συναίνεση: Στο VANET, κάθε κόμβος έχει μόνο μερικές πληροφορίες σχετικά με το περιβάλλον του. Είναι δύσκολο να επιτευχθεί συναίνεση σε ένα τόσο περίπλοκο περιβάλλον VANET.

2. Καθυστέρηση συναίνεσης: Οι περισσότερες από τις εφαρμογές VANET έχουν απαιτήσεις ευαισθησίας καθυστέρησης που έχουν μικρές έως μεσαίες αποστάσεις διάδοσης. Ελάχιστος χρόνος επικοινωνίας αναμένεται για εφαρμογές έκτακτης ανάγκης και ασφάλειας στο VANET, έτσι ώστε να αποφεύγονται ανεπιθύμητες καταστάσεις. Η τεχνολογία blockchain απαιτεί ορισμένο χρόνο πριν από την επίτευξη συναίνεσης στο VANET με δυνατότητα blockchain. Ως εκ τούτου, είναι πολύ σημαντικό να έχει σχεδιαστεί ένας αξιόπιστος και ελαφρύς αλγόριθμος συναίνεσης για το VANET.

3. Κινητικότητα: Στο VANET, τα ημιαυτόνομα οχήματα που ελέγχονται από τον οδηγό και τα αυτόνομα οχήματα είναι αντικείμενα υψηλής κινητικότητας που κινούνται στους δρόμους. Λόγω της υψηλής κινητικότητας των οχημάτων, είναι εξαιρετικά δύσκολο να δημιουργηθεί αξιόπιστη επικοινωνία παρά το γεγονός ότι υπάρχουν επαρκείς επικοινωνιακές και υπολογιστικές δυνατότητες. Η σύνδεση μεταξύ κινούμενων οχημάτων είναι παροδική. Επομένως, ο αλγόριθμος συναίνεσης δεν πρέπει να αποδοκιμάζει τη συνέπεια του συστήματος blockchain.

4. Πολλαπλασιασμός μπλοκ: Προκειμένου να επιτευχθεί συμφωνία, το blockchain απαιτεί τη διάδοση των μπλοκ σε ολόκληρο το δίκτυο. Θα πρέπει να υπάρχει αποτελεσματική διάδοση των μπλοκ λαμβάνοντας υπόψη τα χαρακτηριστικά του VANET για να εξασφαλιστεί η κατανομή των καθολικών σε όλους τους κόμβους.

5. Απαιτήσεις αποθήκευσης: Απαιτείται η ύπαρξη δυνατότητας αποθήκευση μεγάλου όγκου δεδομένων και ανταλλαγή δεδομένων μεγάλης κλίμακας για βελτιώσεις στα

συστήματα επικοινωνίας οχημάτων. Τα δεδομένα που παράγονται από τα οχήματα γίνονται όλο και πιο πολύπλοκα, ασκώντας πρόσθετη πίεση στη μετάδοση δεδομένων. Τα οχήματα δεν μπορούν να ανταποκριθούν σε αυτά τα πρότυπα λόγω περιορισμένων πόρων. Το cloud computing είναι ένα χαρακτηριστικό παράδειγμα που προσφέρει υποδομή για αλληλεπιδράσεις μεταξύ οχημάτων, RSU και άλλες οντότητες. Ωστόσο, τα δεδομένα κίνησης έχουν μεγαλύτερη σημασία σε τοπικό επίπεδο και έχουν χωρικό πεδίο εφαρμογής, γεγονός που απαιτεί χαμηλό λανθάνοντα χρόνο και επίγνωση τοποθεσίας. Το Edge computing είναι μια πολλά υποσχόμενη ιδέα που ενσωματώνει τεράστια αποθήκευση δεδομένων, υπολογισμό και κοινή χρήση πληροφοριών σε κοντινά οχήματα χρησιμοποιώντας υποδομές αιχμής δικτύου όπως RSU. Το vehicle fog computing επεκτείνει την έννοια της υπολογιστικής ομίχλης στα παραδοσιακά δίκτυα οχημάτων, επιτρέποντας την περαιτέρω βελτίωση των ευαίσθητων στις καθυστερήσεις εφαρμογών.

6. Πολυπλοκότητα: Στο VANET, συνυπάρχουν διάφορες ασύρματες τεχνολογίες. Η αποκλειστική επικοινωνία μικρής εμβέλειας (DSRC) χρησιμοποιείται για επικοινωνία V2V και V2I και οι RSU συνδέονται μεταξύ τους χρησιμοποιώντας επικοινωνία LTE/4G/5G. Εκτός από αυτό, τα οχήματα αλλάζουν τις τοπολογίες του δικτύου τους ενώ κινούνται. Υπάρχει ακραίος αντίκτυπος της πολυπλοκότητας των δικτύων στο σενάριο VANET. Ως εκ τούτου, είναι σημαντικό να σχεδιαστεί ένας ελαφρύς αλγόριθμος συναίνεσης.

7. Επεκτασιμότητα: Λόγω της περιορισμένης φύσης των δικτύων οχημάτων, το κόστος δημιουργίας ενός παραδοσιακού δημόσιου blockchain είναι ακριβό. Η επικοινωνία μεταξύ των κόμβων δικτύου είναι παροδική. Επιπλέον, η επεκτασιμότητα είναι ένα σημαντικό ζήτημα που πρέπει να αντιμετωπιστεί στα δημόσια συστήματα blockchain.

8. Απόδοση συναλλαγών: Ο αριθμός των συναλλαγών που αποθηκεύονται σε μια αλυσίδα μπλοκ ανά δευτερόλεπτο είναι γνωστός ως ρυθμός συναλλαγών. Λόγω της πολυπλοκότητας του μηχανισμού συναίνεσης, τα δίκτυα blockchain που βασίζονται στο Bitcoin μπορούν να φιλοξενήσουν επτά συναλλαγές ανά δευτερόλεπτο και να έχουν χρονική καθυστέρηση έως και μία ώρα. Ως αποτέλεσμα, πιστεύεται ότι οι παραδοσιακές δημόσιες λύσεις που βασίζονται σε blockchain είναι ακατάλληλες για εφαρμογές δικτύου οχημάτων σε πραγματικές συνθήκες.

5.11 Η Σημασία του Blockchain για τη Προστασία της Ιδιωτικότητας στα ITS

Το 2016 το δίκτυο μεταφορών του Σαν Φρανσίσκο παραβιάστηκε με αποτέλεσμα να δώσει τη δυνατότητα ελεύθερης πρόσβασης στους μετακινούμενους για δύο ημέρες.[58] Κατά τη διάρκεια του ίδιου έτους, διέρρευσαν πληροφορίες για 57 εκατομμύρια πελάτες και οδηγούς της Uber.[59]

Οι τεχνολογίες κατανεμημένου καθολικού όπως το blockchain έχουν τη δυνατότητα να προστατεύσουν τα δεδομένα κίνησης και θέσης του ατόμου και να προστατεύσουν το

[58] Sovrin Foundation, 2018. Sovrin: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust. Technical Report January. Sovrin Foundation.
Stewart, J., 2016. Sf's transit hack could've been way worse–and cities must prepare. Wired URL https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare.

[59] Wong, J.C., 2017. Uber concealed massive hack that exposed data of 57m users and drivers. The Guardian URL https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

απόρρητό τους. Η τεχνολογία είναι δύσκολο να παραβιαστεί και η ανταλλαγή δεδομένων είναι ασφαλής για όλα τα μέρη, συμπεριλαμβανομένων των ατόμων που δημιούργησαν τα δεδομένα. Μια αλυσίδα μπλοκ είναι μια κατανεμημένη βάση δεδομένων, δομή δεδομένων ή κοινόχρηστο καθολικό που διατηρεί μια λίστα εγγραφών συναλλαγών, η οποία δεν μπορεί να τροποποιηθεί εκτός εάν επιτευχθεί συναίνεση στο δίκτυο χρησιμοποιώντας έναν αλγόριθμο.[60] Μερικοί από τους πιο συνηθισμένους αλγόριθμους στις δημόσιες αλυσίδες μπλοκ είναι η απόδειξη της εργασίας που χρησιμοποιείται από το Bitcoin και το proof-of-stake που χρησιμοποιείται από το Peercoin.

Ο μηχανισμός blockchain παρέχει τα ακόλουθα χαρακτηριστικά[61]:

Αμετάβλητο: Το αμετάβλητο είναι το βασικό χαρακτηριστικό του μηχανισμού blockchain. Στον μηχανισμό blockchain, ένα μπλοκ συνδέεται με το προηγούμενο μπλοκ χρησιμοποιώντας την τιμή κατακερματισμού του προηγούμενου μπλοκ. Ως εκ τούτου, τα μπλοκ έχουν γίνει αμετάβλητα στο σύστημα που βασίζεται σε blockchain.

Κατανεμημένη φύση: Η τεχνολογία blockchain λειτουργεί σε κατανεμημένο χαρακτήρα. Στο σύστημα που βασίζεται σε blockchain, όλοι οι κόμβοι έχουν το ίδιο και ένα ενημερωμένο αντίγραφο του blockchain.

Ανωνυμία: Στο blockchain, κάθε κόμβος δικτύου συνδέεται με την ανώνυμη διεύθυνση (τυχαία τιμή κατακερματισμού του δημόσιου κλειδιού). Επομένως, οι κόμβοι μπορούν να είναι ανώνυμοι όταν ανταλλάσσουν πόρους με τους άλλους κόμβους του δικτύου.

Περιβάλλον εμπιστοσύνης: Λόγω της κατανεμημένης φύσης, ο μηχανισμός blockchain αποτρέπει το σύστημα από το πρόβλημα SPoF (single-point-of-failure). Παρέχει εμπιστοσύνη μεταξύ των διασυνδεμένων κόμβων που είναι κατανεμημένοι σε όλο το δίκτυο και δημιουργεί ένα περιβάλλον εμπιστοσύνης σε όλο το δίκτυο blockchain.

Διαφάνεια: Τα μπλοκ (ή δεδομένα) στον μηχανισμό blockchain είναι απολύτως διαφανή, καθώς κάθε μεμονωμένος κόμβος αποθηκεύει το πανομοιότυπο και ενημερωμένο αντίγραφο του blockchain και είναι απολύτως διαφανές σε κάθε συνδεδεμένο κόμβο στο δίκτυο.

Απόρρητο: Σε έναν μηχανισμό blockchain, κάθε χρήστης συμμετέχει στο δίκτυο και οι προσωπικές πληροφορίες του χρήστη είναι εντελώς ανώνυμες. Αυτό σημαίνει ότι οι χρήστες στο δίκτυο δεν μπορούν να προβλέψουν τις προσωπικές πληροφορίες άλλων χρηστών, καθώς περιλαμβάνει κρυπτογραφημένα δεδομένα για τη διατήρηση της ταυτότητας του χρήστη.

Έξυπνα συμβόλαια: Αντί να χρησιμοποιεί τη νομική γλώσσα, χρησιμοποιεί τη γλώσσα του υπολογιστή για τη σύνταξη των συμβάσεων. Όταν πληρούνται οι προκαθορισμένες συνθήκες, ο υπολογιστής εκτελεί αυτόματα ψηφιακές συμβάσεις. Ως αποτέλεσμα, μειώνει το κόστος υπογραφής της σύμβασης και την εποπτεία της.

---

[60] Hawaii International Conference on System Sciences (HICSS-50), pp. 1543–1552.
Kim, H.M., Laskowski, M., 2018. Toward an ontology-driven blockchain design for supply-chain provenance. Intell. Syst. Account. Finance Manage. 25, 18–27.
https://doi.org/10.1002/isaf.1424.

[61] A. A. Monrat, O. Schelén and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

Αυτονομία: Το blockchain χρησιμοποιεί συναινετικά πρωτόκολλα για την προσθήκη και αποθήκευση οποιουδήποτε μπλοκ στο αποκεντρωμένο δίκτυό του. Αυτά τα πρωτόκολλα είναι ανοιχτά και διαφανή που επιτρέπουν στους κόμβους να ανταλλάσσουν με ασφάλεια πληροφορίες.

Χρονολογική & χρονική σήμανση: Τα μπλοκ δεδομένων έχουν χρονική σήμανση και το τρέχον μπλοκ συνδέεται με το προηγούμενο. Οι κρυπτογραφικά ασφαλείς συναρτήσεις κατακερματισμού χρησιμοποιούνται για αυτό. Ως αποτέλεσμα, εάν ένας εισβολέας καταφέρει να μετριάσει οποιοδήποτε μπλοκ, όλα τα διάδοχα μπλοκ ακολουθούμενα από το μετριασμένο μπλοκ ακυρώνονται.

Αυτοματοποίηση ανταλλαγών: Γράφοντας τα έξυπνα συμβόλαια, η ανταλλαγή πόρων μεταξύ των κόμβων δικτύου blockchain μπορεί να αυτοματοποιηθεί. Ως εκ τούτου, διάφορες υπηρεσίες χρησιμοποιούνται αυτόματα στο δίκτυο χωρίς ανθρώπινη παρέμβαση.

Για τη διατήρηση της ιδιωτικής ζωής του ατόμου έχουν χρησιμοποιηθεί τεχνικές όπως, η λειτουργία κατακερματισμού[62] για την ανωνυμοποίηση των δεδομένων των χρηστών, και τεχνικές κρυπτογράφησης δημόσιου και ιδιωτικού κλειδιού για την ασφάλεια δεδομένων και επικοινωνιών. Ωστόσο, οι ερευνητές και οι τεχνολόγοι διαπίστωσαν ότι το blockchain μπορεί να είναι μια πιθανή λύση στο πρόβλημα της ιδιωτικής ζωής , απομονώνοντας κρίσιμες πληροφορίες και καθιστώντας τα άτομα μοναδικούς ιδιοκτήτες και ελεγκτές των δεδομένων τους.

Το Blockchain μετατρέπει τη κλασική κεντρική προσέγγιση σε ένα πλήρως αποκεντρωμένο δίκτυο κόμβων. Βασίζεται σε μια συγχρονισμένη τεχνολογία κατανεμημένου καθολικού (DLT), η οποία λειτουργεί ως αποκεντρωμένη βάση δεδομένων, διατηρώντας τις πληροφορίες που αναπαράγονται και μοιράζονται μεταξύ πολλαπλών κόμβων, κατανεμημένες σε απομακρυσμένες τοποθεσίες. Το Blockchain προσφέρει πολλά πλεονεκτήματα που περιλαμβάνουν την απόδειξη , τη λογοδοσία, την ιχνηλασιμότητα και τη διαφάνεια των συναλλαγών που αποθηκεύονται στο καθολικό.

Η εποχή των μεγάλων δεδομένων υπονομεύει το απόρρητο του χρήστη σε πολλά ψηφιακά σενάρια. Μεγάλα τρίτα μέρη επωφελούνται από τη διαχείριση των δεδομένων των χρηστών τους, συλλέγοντας, αναλύοντας, συσχετίζοντας και ελέγχοντας τεράστιες ποσότητες προσωπικών δεδομένων. Αυτοί οι οργανισμοί και οι υπηρεσίες τους υπόκεινται σε παραβιάσεις ασφάλειας και κατάχρηση δεδομένων χρηστών, γεγονός που μπορεί να θέσει σε κίνδυνο το απόρρητο των χρηστών. Οι συναλλαγές στην αλυσίδα μπλοκ δεν είναι απρόσβλητες από αυτά τα ζητήματα απορρήτου. Εκτός αυτού, τα άτομα έχουν λίγες επιλογές για τον έλεγχο των προσωπικών τους δεδομένων και της ιδιωτικής τους ζωής μέσω των διαδικτυακών συναλλαγών τους, συμπεριλαμβανομένου του πώς, πότε, πού, από ποιον και ποιες συγκεκριμένες προσωπικές πληροφορίες αποκαλύπτονται σε κάθε συγκεκριμένη συναλλαγή. Αυτό το πρόβλημα εντείνεται στο blockchain, καθώς τα ιδιωτικά δεδομένα που περιλαμβάνονται στο καθολικό είναι αμετάβλητα και τα δικαιώματα του χρήστη να ελέγχει και να διορθώνει προσωπικές πληροφορίες μειώνονται.

---

[62] Hashing: "κρυπτογραφική συνάρτηση κατακερματισμού". Ένας κατακερματισμός είναι μια μαθηματική συνάρτηση: της δίνετε μια τιμή εισόδου και η συνάρτηση σκέφτεται για λίγο και μετά εκπέμπει μια τιμή εξόδου. και η ίδια είσοδος δίνει πάντα την ίδια έξοδο. Αυτό που κάνει έναν κατακερματισμό ξεχωριστό είναι ότι είναι τόσο απρόβλεπτο όσο μπορεί να είναι μια μαθηματική συνάρτηση.https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous

Για να διασφαλιστεί η εμπιστευτικότητα των δεδομένων που διατηρούνται στην αλυσίδα μπλοκ, τα δεδομένα πρέπει να κρυπτογραφηθούν. Επιπλέον, η προστασία της ιδιωτικής ζωής περιλαμβάνει το δικαίωμα διαγραφής, ωστόσο, η αλυσίδα μπλοκ είναι αμετάβλητη, γεγονός που αποτελεί σημαντική πρόκληση. Από αυτή την άποψη, τα κατακερματισμένα προσωπικά δεδομένα παρέχουν ψευδώνυμο αλλά όχι ανωνυμία. Ομοίως, τα κρυπτογραφημένα προσωπικά δεδομένα θεωρούνται ψευδώνυμα (δηλαδή όχι ανώνυμα). Επιπλέον, τα ψηφιακά αναγνωριστικά μπορούν να θεωρηθούν δεδομένα προσωπικού χαρακτήρα και δεν θα πρέπει να εγγράφονται στο καθολικό, ή τουλάχιστον, θα πρέπει να υπάρχει διαφορετική προέλευση του ψηφιακού αναγνωριστικού για κάθε αλληλεπίδραση.

Το Blockchain μπορεί να φέρει επανάσταση στον κλάδο των μεταφορών παρέχοντας μέσω της τεχνολογίας αυτής καλύτερη και ασφαλέστερη λειτουργία των ITS διατηρώντας σε υψηλό επίπεδο υπηρεσίες προς τους μετακινούμενους, όπως για παράδειγμα οι λεπτομέρειες σχετικά με τη θέση οχημάτων δημόσιων συγκοινωνιών σε μια πόλη και πληροφορίες σχετικά με τη διαθεσιμότητα θέσεων σε ένα συγκεκριμένο όχημα.

Το Blockchain είναι επομένως ένα συνεργατικό οικοσύστημα που δημιουργεί εμπιστοσύνη μεταξύ όλων των εμπλεκόμενων μερών. Είναι μια τεχνολογία που προσφέρει αποκεντρωμένη και κατανεμημένη βάση δεδομένων μαζί με κρυπτογραφική ασφάλεια για την κοινή χρήση πληροφοριών με ασφαλή τρόπο. Μπορούμε να συμπεράνουμε ότι το blockchain αντιμετωπίζει τις προκλήσεις της αστικοποίησης εξασφαλίζοντας καλύτερη εφαρμογή του πλαισίου των ITS.

Η διατήρηση της ιδιωτικής ζωής των έξυπνων κόμβων που εμπλέκονται στο σύστημα VANET είναι υψίστης σημασίας. Τα ευφυή οχήματα παράγουν τεράστιο όγκο δεδομένων, συμπεριλαμβανομένων σημαντικών πληροφοριών όπως τροχαία ατυχήματα, περιβαλλοντικοί κίνδυνοι κ.λπ. Ο εισβολέας ξεκινά τις επιθέσεις, με στόχο να μάθει την πραγματική ταυτότητα του κόμβου. Μόλις αποκαλυφθεί η πραγματική ταυτότητα του κόμβου, είναι πολύ εύκολο για τον εισβολέα να εισέλθει και να προξενήσει ζημιά στη λειτουργία του συστήματος. Επομένως, είναι σημαντικό να διατηρηθεί η ταυτότητα του κόμβου με μεγάλη ασφάλεια. Το υπάρχον παραδοσιακό σύστημα υιοθέτησε διάφορες μεθόδους και τεχνικές για την επίτευξη της ιδιωτικής ζωής του χρήστη. Η εγγενής ιδιότητα του blockchain επιτυγχάνει εύκολα την ψευδωνυμία των κόμβων. Ως αποτέλεσμα, η πραγματική ταυτότητα των κόμβων δεν αποκαλύπτεται ποτέ.

Το Blockchain, ως δομή λογισμικού δεδομένων, πρέπει να συμμορφώνεται με τους ισχύοντες νόμους σχετικά με το απόρρητο των δεδομένων, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων. Ο GDPR θέτει αυστηρά ότι κάθε χρήστης που μοιράζεται τα δεδομένα του σε μια δημόσια πλατφόρμα πρέπει να έχει το δικαίωμα διόρθωσης και της λήθης. Δεδομένου ότι το blockchain είναι ένα αμετάβλητο και κατανεμημένο καθολικό, δεν συμμορφώνεται με αυτόν τον κανονισμό. Λόγω της κατανεμημένης αρχιτεκτονικής του, στην περίπτωση που ένας χρήστης επιθυμεί να εγκαταλείψει ένα δίκτυο blockchain, εάν το δικαίωμα στη λήθη πρέπει να εφαρμοστεί σύμφωνα με το GDPR, αυτό θα κοστίσει πολύ σε υπολογιστική ισχύ και θα απαιτήσει την εκ νέου εξόρυξη όλων των προηγούμενων μπλοκ της αλυσίδας και αυτή η διαδικασία είναι υπολογιστικά αδύνατη.

Το χαρακτηριστικό διαφάνειας της αλυσίδας συστοιχιών την καθιστά συμβατή με τον ΓΚΠΔ εκδηλώνει το ελέγξιμο κατανεμημένο καθολικό δεδομένων συναλλαγών και ιστορικού που μοιράζεται μεταξύ όλων των συμμετεχόντων στην αλυσίδα συστοιχιών

(δηλ. φυσικών προσώπων ή άλλου φορέα που έχει αρμοδιότητες υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία ή και των δύο) με εύκολο στην πρόσβαση τρόπο. Τούτο καθιστά την αλυσίδα συστοιχιών συμβατή με την αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας του ΓΚΠΔ, όπου η διαφάνεια απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση για τη διασφάλιση της δικαιοσύνης και της διαφάνειας. Η διαφάνεια της αλυσίδας συστοιχιών βελτιώνει τη λογοδοσία παρακολουθώντας όλες τις συναλλαγές, γεγονός που καθιστά δυνατή τη συμμόρφωση με την αρχή της λογοδοσίας βάσει του ΓΚΠΔ.

Η τεχνολογία πίσω από το blockchain παρέχει σημαντική - αν και όχι απόλυτη - εμπιστοσύνη, ανωνυμία και αμετάβλητο των αρχείων δεδομένων. Οι συμμετέχοντες στις συναλλαγές blockchain δεν χρειάζεται να γνωρίζουν ή να εμπιστεύονται ο ένας τον άλλον για να εισέλθουν σε μια συναλλαγή. Αντ 'αυτού, οι συμμετέχοντες βασίζονται στην κρυπτογράφηση και το αμετάβλητο των μπλοκ για την προστασία των δεδομένων τους από κινδύνους απορρήτου και αντισυμβαλλομένου. Συγκεκριμένα, τα δεδομένα εντός των μπλοκ είναι προσβάσιμα μόνο σε όσους διαθέτουν κρυπτογραφικά κλειδιά και, στην περίπτωση της αλυσίδας συστοιχιών χωρίς άδεια, το αμετάβλητο των δεδομένων προστατεύεται από το γεγονός ότι η συναίνεση όλων των συμμετεχόντων είναι απαραίτητη όχι μόνο για την προσθήκη νέων μπλοκ στην αλυσίδα, αλλά και για την αφαίρεσή τους. Από την άποψη της προστασίας της ιδιωτικής ζωής, η ίδια η δομή της αλυσίδας συστοιχιών επιβάλλει την προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό και, εν μέρει, της ιδιωτικής ζωής εξ ορισμού.

5.12 Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και η αλυσίδα συστοιχιών

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (Data Protection Impact Assessment - DPIA) είναι μια άσκηση, όπως αναφέρει το άρθρο 35 του GDPR, «μια εκτίμηση του αντίκτυπου των προβλεπόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα». Οι υπεύθυνοι επεξεργασίας δεδομένων αναμένεται να διενεργήσουν ΕΑΠΔ (Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων) εάν η επεξεργασία δεδομένων θα πραγματοποιηθεί με τη χρήση νέων τεχνολογιών και είναι πιθανό να δημιουργήσει υψηλούς κινδύνους για την ιδιωτική ζωή των φυσικών υποκειμένων. Η ΕΑΠΔ είναι υποχρεωτική εάν οι προσωπικές πτυχές των δεδομένων πρόκειται να χρησιμοποιηθούν για τη λήψη αποφάσεων στο πλαίσιο αυτοματοποιημένης διαδικασίας. Γενικά, η ΕΑΠΔ θα πρέπει να περιλαμβάνει συστηματική περιγραφή του σκοπού και των διαδικασιών επεξεργασίας δεδομένων, αξιολόγηση των κινδύνων για την προστασία της ιδιωτικής ζωής, πληροφορίες σχετικά με την αναγκαιότητα και την αναλογικότητα των πράξεων επεξεργασίας σε σχέση με τον σκοπό της επεξεργασίας και μέτρα που εφαρμόζονται για τη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ και τη μείωση των κινδύνων για την ιδιωτική ζωή των υποκειμένων των δεδομένων και τρίτων.

Η εφαρμογή του κειμένου των απαιτήσεων DPIA του GDPR στην αλυσίδα μπλοκ παράγει τις ακόλουθες συνέπειες και θέτει πολλά ερωτήματα για τους χρήστες του δικτύου blockchain και τους υπεύθυνους επεξεργασίας δεδομένων.

Πρώτον, επειδή υπάρχει ήδη εδώ και δύο δεκαετίες, το blockchain δεν είναι μια εντελώς νέα τεχνολογία. Παρ 'όλα αυτά, το blockchain είναι μια μορφή αυτοματισμού και υπάρχει μια ποικιλία από μη δοκιμασμένους τρόπους χρήσης του blockchain.

Επειδή η αυτοματοποίηση της επεξεργασίας δεδομένων με μη δοκιμασμένους τρόπους μπορεί να δημιουργήσει απρόβλεπτες δυσμενείς συνέπειες για την προστασία της ιδιωτικής ζωής, από τη σκοπιά του GDPR, το blockchain αποτελεί μια νέα τεχνολογία. Ως εκ τούτου, οι οντότητες που χρησιμοποιούν τεχνολογία blockchain για τον χειρισμό δεδομένων φυσικών υποκειμένων θα πρέπει να διενεργούν ΕΑΠΔ πριν από τη δημιουργία του δικτύου blockchain, εάν τα δεδομένα που υποβάλλονται σε επεξεργασία αφορούν δεδομένα προσωπικού χαρακτήρα φυσικών υποκειμένων. Εάν το σύστημα επεξεργασίας θεωρείται απίθανο να δημιουργήσει αυξημένους κινδύνους για την ιδιωτική ζωή των φυσικών υποκειμένων, η διενέργεια ΕΑΠΔ μπορεί κάλλιστα να είναι περιττή.

Δεύτερον, τόσο οι υπεύθυνοι επεξεργασίας δεδομένων όσο και τα φυσικά υποκείμενα θα μπορούσαν να αμφισβητήσουν τη χρησιμότητα της συμμετοχής στην ΕΑΠΔ, για τους ακόλουθους λόγους. Η σιωπηρή παραδοχή στην οποία βασίζεται η ΕΑΠΔ είναι ότι όσοι διενεργούν την ΕΑΠΔ μπορούν να προβλέψουν τους περισσότερους κινδύνους για την προστασία της ιδιωτικής ζωής με κάποιο βαθμό βεβαιότητας κατά τον χρόνο διενέργειας της ΕΑΠΔ. Τα φυσικά υποκείμενα των οποίων διακυβεύονται τα δικαιώματα προστασίας της ιδιωτικής ζωής θα μπορούσαν να υποστηρίξουν ότι η εν λόγω αξιολόγηση των κινδύνων για την προστασία της ιδιωτικής ζωής αφήνει τον προσδιορισμό της σοβαρότητας των παρόντων και μελλοντικών κινδύνων για την προστασία της ιδιωτικής ζωής στα χέρια εκείνων που εκτελούν την ΕΑΠΔ. Με τη σειρά τους, οι διενεργούντες την ΕΑΠΔ θα μπορούσαν να διαμαρτυρηθούν ότι η περιοδική ή συνεχής διενέργεια ΕΑΠΔ είναι μια δαπανηρή, τυπολατρική και επικίνδυνη άσκηση αξιολόγησης των κινδύνων για την προστασία της ιδιωτικής ζωής σε ένα περιβάλλον «πειραματικού» που δεν αντικατοπτρίζει πραγματικές καταστάσεις και κινδύνους για την ιδιωτική ζωή.

5.13 Μοναδικοί και από κοινού υπεύθυνοι επεξεργασίας δεδομένων και εκτελούντες την επεξεργασία δεδομένων στο blockchain

Εάν η φιλοσοφία του blockchain είναι η αποδιαμεσολάβηση, η φιλοσοφία πίσω από το GDPR θα μπορούσε να ονομαστεί «εκ νέου διαμεσολάβηση». Αυτό οφείλεται στο γεγονός ότι η προστασία των δικαιωμάτων των υποκειμένων των δεδομένων στο πλαίσιο του GDPR θα μπορούσε να θεωρηθεί ότι βασίζεται στις δραστηριότητες δύο ειδών διαμεσολαβητών δεδομένων: των μοναδικών και από κοινού υπευθύνων επεξεργασίας δεδομένων και των επεξεργαστών δεδομένων.

Ο GDPR ορίζει ως «υπεύθυνο επεξεργασίας δεδομένων» ένα φυσικό ή νομικό πρόσωπο ή δημόσια οντότητα που, μόνη ή από κοινού με άλλους υπεύθυνους επεξεργασίας δεδομένων, καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Τα κύρια καθήκοντα των μοναδικών ή περισσότερων (από κοινού) υπευθύνων επεξεργασίας δεδομένων περιλαμβάνουν την εκτίμηση των κινδύνων απορρήτου και την εφαρμογή αναλογικών τεχνικών και οργανωτικών μέτρων που διασφαλίζουν τα δικαιώματα των υποκειμένων των δεδομένων που απαριθμούνται στον GDPR. Εάν οι από κοινού υπεύθυνοι επεξεργασίας καθορίζουν συλλογικά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων, θα πρέπει να καθορίζουν τους ρόλους και τις αρμοδιότητές τους έναντι των υποκειμένων των δεδομένων με σαφήνεια και εκ των προτέρων. Εάν οι από κοινού υπεύθυνοι επεξεργασίας δεν δημιουργήσουν σύστημα κατανομής ρόλων και αρμοδιοτήτων, κάθε από κοινού υπεύθυνος επεξεργασίας καθίσταται υπεύθυνος για το σύνολο της ζημίας στα δικαιώματα προστασίας της ιδιωτικής ζωής του υποκειμένου των δεδομένων.

Στη συνέχεια στη γραμμή των διαμεσολαβητών δεδομένων είναι ο επεξεργαστής δεδομένων, τον οποίο ο GDPR περιγράφει ως φυσική ή νομική οντότητα που επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας δεδομένων. Η σχέση μεταξύ του υπευθύνου επεξεργασίας δεδομένων και του εκτελούντος την επεξεργασία είναι συμβατική και σε μεγάλο βαθμό ιεραρχική. Για παράδειγμα, μεταξύ πολλών άλλων υποχρεώσεων, ο εκτελών την επεξεργασία αναμένεται να συμμορφώνεται με τις τεκμηριωμένες οδηγίες του υπευθύνου επεξεργασίας, να διατηρεί τα δικαιώματα απορρήτου των υποκειμένων των δεδομένων καθ' όλη τη διάρκεια της διαδικασίας επεξεργασίας δεδομένων και να ελέγχει τους υπεργολάβους επεξεργασίας.

Οι εθνικές ρυθμιστικές αρχές προστασίας δεδομένων έχουν προτείνει ότι ο εντοπισμός των ελεγκτών δεδομένων και των επεξεργαστών στο blockchain θα μπορούσε να γίνει ταξινομώντας εκείνους που γράφουν στο blockchain ως ελεγκτές δεδομένων, ενώ ταυτόχρονα αντιμετωπίζουν εκείνους που επικυρώνουν καταχωρήσεις blockchain ως επεξεργαστές δεδομένων. Η εφαρμογή της λύσεως αυτής θα μπορούσε να είναι σχετικά απλή σε ορισμένες περιπτώσεις. Ωστόσο, προκύπτουν επιπλοκές όταν πρόκειται για τύπους blockchain στους οποίους η ίδια οντότητα είναι ταυτόχρονα ο υπεύθυνος επεξεργασίας δεδομένων και ο επεξεργαστής. Στις περιπτώσεις αυτές, κατά τον ΓΚΠΔ, ο εκτελών την επεξεργασία θα μπορούσε να εξομοιωθεί με υπεύθυνο επεξεργασίας, διότι, στην περίπτωση αυτή, ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται από τον εκτελούντα την επεξεργασία.

Εάν, ωστόσο, το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία συγχωνευθούν σε ένα μόνο πρόσωπο ή οντότητα, η διατήρηση της διάκρισης μεταξύ αυτών των τριών ρόλων θα μπορούσε να είναι άχρηστη. Αυτό αποκαλύπτει την έκταση - και τον εκτεταμένο αντίκτυπο - των φιλοσοφικών διαφορών μεταξύ του blockchain και του GDPR. Καθώς τα όρια μεταξύ των προσώπων που ο GDPR αντιμετωπίζει ως υποκείμενο δεδομένων, ελεγκτή και επεξεργαστή θολώνουν, η αποκέντρωση και η αποδιαμεσολάβηση χρησιμοποιώντας το blockchain είναι πιο ολοκληρωμένα. Το συμπέρασμα είναι ότι όσο περισσότερο το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας και η επεξεργασία ή η συγχώνευση σε ένα άτομο, τόσο μεγαλύτερη κυριαρχία έχει το υποκείμενο των δεδομένων στην ιδιωτική του ζωή. Ταυτόχρονα, η ρύθμιση και η ευθύνη για παραβιάσεις της ιδιωτικής ζωής καθίσταται εξαιρετικά δύσκολο – αν όχι αδύνατο – να εφαρμοστεί.

Χωρίς την απασχόληση μεσαζόντων και τη δημιουργία ενός κεντρικού συστήματος για τη διαδικασία προστασίας δεδομένων, οι ρυθμιστικές αρχές δεν έχουν την ικανότητα να ασχολούνται άμεσα με μυριάδες μεμονωμένα υποκείμενα δεδομένων. Ο κόσμος της πλήρους κυριαρχίας των υποκειμένων των δεδομένων επί της ιδιωτικής ζωής μπορεί να είναι ένας κόσμος χωρίς αποτελεσματική ευθύνη για παραβιάσεις της ιδιωτικής ζωής.

5.14 Διόρθωση και το δικαίωμα στη λήθη στο Blockchain

Η υπόσχεση του σχεδόν αμετάβλητου των δεδομένων που καταγράφονται στο blockchain είναι ένας από τους βασικούς λόγους για την προσέλκυση του blockchain σε πολλούς χρήστες. Ωστόσο, το δικαίωμα διόρθωσης και το δικαίωμα διαγραφής δεδομένων (δηλαδή το δικαίωμα στη λήθη) συγκαταλέγονται μεταξύ των σημαντικότερων δικαιωμάτων των υποκειμένων των δεδομένων που κατοχυρώνονται στον ΓΚΠΔ. Το δικαίωμα διόρθωσης σημαίνει ότι ο υπεύθυνος επεξεργασίας δεδομένων οφείλει στο υποκείμενο των δεδομένων να διορθώσει ανακριβή δεδομένα

προσωπικού χαρακτήρα και ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας να συμπληρώσει τυχόν ελλιπή δεδομένα προσωπικού χαρακτήρα. Το δικαίωμα στη λήθη συνεπάγεται ότι, σε ορισμένες περιπτώσεις, το υποκείμενο των δεδομένων μπορεί να ζητήσει την πλήρη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν από τον υπεύθυνο της επεξεργασίας. Το αμετάβλητο των δεδομένων που καταγράφονται στην αλυσίδα μπλοκ και το δικαίωμα διόρθωσης και διαγραφής του ΓΚΠΔ αναφέρθηκαν συχνά ως βασικές ασυμβατότητες μεταξύ της αλυσίδας μπλοκ και του ΓΚΠΔ. Ωστόσο, τεχνικοί και νομικοί λόγοι υποδηλώνουν ότι αυτές οι ασυμφωνίες δεν είναι τόσο ανυπέρβλητες όσο φαίνονται. Πρώτον, ούτε καν το blockchain χωρίς άδεια - αυτό στο οποίο η διαγραφή δεδομένων που καταγράφονται στα μπλοκ πρέπει να εγκριθεί από όλους τους συμμετέχοντες στο blockchain - δεν είναι απολύτως αμετάβλητο. Επιπλέον, άλλα είδη αλυσίδας συστοιχιών (blockchain), όπως η ιδιωτική αλυσίδα συστοιχιών (blockchain), είναι ειδικά διαρθρωμένα κατά τρόπον ώστε να μην είναι πλήρως αμετάβλητα. Δεύτερον, ο ΓΚΠΔ δεν περιέχει ακριβή ορισμό του πότε μπορεί να θεωρηθεί ότι τα δεδομένα έχουν διαγραφεί πλήρως. Το ζήτημα αυτό είναι σημαντικό, δεδομένου ότι πολλές τεχνικές διαγραφής δεδομένων αφήνουν τη δυνατότητα ανάκτησης δεδομένων και, ως εκ τούτου, τη δυνατότητα κατάχρησης.

Επιπλέον, υπάρχει μια σύγκρουση που προκύπτει μεταξύ των εννοιών της ιδιωτικής ζωής και της διαφάνειας. Οι αλυσίδες μπλοκ ενισχύουν τη διαφάνεια επιτρέποντας σε όλα τα εμπλεκόμενα μέρη να έχουν πρόσβαση στο ιστορικό συναλλαγών. Ωστόσο, η επιβολή του δικαιώματος διαγραφής δεδομένων ενδέχεται να έρχεται σε αντίθεση με αυτόν τον ανοικτό χαρακτήρα, καθώς η αφαίρεση πληροφοριών θα δημιουργούσε κενά στο αρχείο συναλλαγών. Είναι ζωτικής σημασίας να εξεταστεί η διασταύρωση της τεχνολογίας και του δικαίου. Η επιβολή του δικαιώματος στη λήθη περιλαμβάνει την πλοήγηση σε μια σχέση μεταξύ διαδικασιών και νομικών περιορισμών, η οποία καθίσταται ιδιαίτερα δύσκολη σε ένα αποκεντρωμένο σύστημα blockchain που λειτουργεί διασυνοριακά. Αυτές οι προκλήσεις υπογραμμίζουν τις περιπλοκές που συνεπάγεται η ενσωμάτωση του δικαιώματος στη λήθη στην τεχνολογία.

5.15 Διαφάνεια και ιδιωτικότητα μεταξύ blockchain και GDPR

Το ζήτημα της εξισορρόπησης της διαφάνειας και της ιδιωτικής ζωής στο πλαίσιο της τεχνολογίας έχει γίνει ανησυχητικό. Διεξάγεται εκτεταμένη έρευνα για να βρεθεί η ισορροπία που υποστηρίζει την ακεραιότητα των δικτύων blockchain, διασφαλίζοντας παράλληλα τα δικαιώματα απορρήτου των δεδομένων των χρηστών. Η διαφάνεια είναι ένα χαρακτηριστικό του blockchain χάρη στο κατανεμημένο και αμετάβλητο καθολικό του. Αυτή η πτυχή το καθιστά ελκυστικό ως εργαλείο για την οικοδόμηση εμπιστοσύνης, καθώς ενισχύει τη λογοδοσία και μειώνει την εξάρτηση από μεσάζοντες για την επαλήθευση των συναλλαγών. Ο αντίκτυπος αυτού του ανοίγματος εκτείνεται σε όλους τους κλάδους, συμπεριλαμβανομένων των τραπεζών και της διαχείρισης της εφοδιαστικής αλυσίδας. Ωστόσο, με την αύξηση των παραβιάσεων δεδομένων, των περιστατικών κλοπής ταυτότητας και των παραβιάσεων της ιδιωτικής ζωής, καθίσταται ολοένα και πιο σημαντικό να επιτευχθεί ισορροπία μεταξύ του ανοικτού χαρακτήρα και της προστασίας των δεδομένων. Ένα σημαντικό νομοθετικό πλαίσιο σε αυτή τη συζήτηση είναι ο GDPR που αναγνωρίζει τη διασφάλιση των προσωπικών δεδομένων των φυσικών προσώπων ως δικαίωμα. Ο κανονισμός αυτός εισάγει την έννοια της «προστασίας δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού», δίνοντας έμφαση στην ενσωμάτωση των ζητημάτων απορρήτου των δεδομένων στις πτυχές των συστημάτων, όπως τα δίκτυα blockchain. Η εύρεση ενός τρόπου ενσωμάτωσης του

blockchain χωρίς να διακυβεύονται τα χαρακτηριστικά του αποτελεί πρόκληση που οδηγεί σε καινοτόμες λύσεις. Η σύγκρουση μεταξύ της διαφάνειας των blockchains και των κανονισμών απορρήτου του GDPR πυροδότησε την ανάπτυξη τεχνικών όπως οι αποδείξεις μηδενικής γνώσης. Οι αποδείξεις μηδενικής γνώσης είναι τεχνικές που επιτρέπουν σε ένα μέρος (γνωστό ως δοκιμαστής) να αποδείξει την αλήθεια μιας δήλωσης, σε ένα άλλο μέρος (αναφέρεται ως επαληθευτής) χωρίς να αποκαλύπτει πληροφορίες σχετικά με την ίδια τη δήλωση. Αυτά τα αποδεικτικά στοιχεία παίζουν ρόλο, σε περιβάλλοντα, επιτρέποντας την επικύρωση συναλλαγών χωρίς αποκάλυψη ευαίσθητων δεδομένων, διασφαλίζοντας έτσι τόσο τη διαφάνεια των συναλλαγών όσο και το απόρρητο των χρηστών. Με αυτή την προσέγγιση, οι συμμετέχοντες μπορούν να επαληθεύουν με ασφάλεια τις συναλλαγές, διασφαλίζοντας παράλληλα την εμπιστευτικότητα των δεδομένων τους. Επιπλέον, υπάρχει αυξανόμενο ενδιαφέρον για τη χρήση αποθήκευσης δεδομένων εκτός αλυσίδας ως λύση. Η αποθήκευση εκτός αλυσίδας περιλαμβάνει την αποθήκευση πληροφοριών εκτός της αλυσίδας μπλοκ, διατηρώντας μόνο κρυπτογραφικούς κατακερματισμούς ή δείκτες στα δεδομένα της αλυσίδας. Αυτή η προσέγγιση επιτρέπει τη διαγραφή δεδομένων συμβατή με το GDPR, διατηρώντας παράλληλα την ακεραιότητα της αλυσίδας μπλοκ.

Επιπλέον, οι ερευνητές έχουν υποστηρίξει την αποθήκευση δεδομένων εκτός αλυσίδας, όπου τα κρυπτογραφημένα προσωπικά δεδομένα αποθηκεύονται ξεχωριστά από το blockchain διασφαλίζοντας τη συμμόρφωση με τις οδηγίες GDPR, για τη διαχείριση δεδομένων (Shahaab et al., 2023)

Τεχνικές όπως οι αποδείξεις μηδενικής γνώσης, η αποθήκευση δεδομένων εκτός αλυσίδας και τα αδειοδοτημένα μοντέλα blockchain μπορούν να χρησιμεύσουν για την επίτευξη ισορροπίας από αυτή την άποψη. Μια διεξοδική εξέταση αυτών των προσεγγίσεων που καθοδηγείται από ερευνητικές γνώσεις και νομικές εκτιμήσεις είναι ζωτικής σημασίας για την απελευθέρωση των δυνατοτήτων της τεχνολογίας blockchain, διασφαλίζοντας παράλληλα τα δικαιώματα απορρήτου των χρηστών (Stopar et al., 2019).

5.16 Προστασία της Ιδιωτικότητας στην εποχή του GDPR

Η επεξεργασία δεδομένων, ιδίως τα δεδομένα προσωπικού χαρακτήρα, τα νέα εργαλεία ΤΠ και η ψηφιακή αγορά έχουν αυξήσει την ανάγκη για καλύτερη προστασία της ιδιωτικής ζωής των νέων ψηφιακών προϊόντων και υπηρεσιών. Η λύση καθορίζεται σε μια νέα μεταρρύθμιση του πλαισίου της ΕΕ για την προστασία των προσωπικών δεδομένων, η οποία αλλάζει τους τρόπους με τους οποίους τα προσωπικά δεδομένα διαχειρίζονται και εφαρμόζονται ταυτόχρονα σε όλους τους οργανισμούς που διαθέτουν προσωπικά δεδομένα πολιτών της ΕΕ. Ο Γενικός Κανονισμός της ΕΕ για την προστασία δεδομένων 2016/679 έχει τεθεί σε ισχύ από τις 25 Μαΐου 2018. Ο GDPR έχει αλλάξει σημαντικά τους κανόνες που ορίζουν τα προσωπικά δεδομένα, εισάγοντας νέες έννοιες και συμμόρφωση, σχεδιασμό, εφαρμογή, συμμόρφωση συντήρησης και αξιολόγηση κινδύνου. Η βασική προϋπόθεση της ανάπτυξης της σύγχρονης ψηφιακής οικονομίας βασίζεται στην επιτάχυνση της ανάπτυξης των τεχνολογιών πληροφοριών και επικοινωνιών, ανταποκρινόμενη παράλληλα στις νέες προκλήσεις και απειλές για την ιδιωτική ζωή και την προστασία των δεδομένων προσωπικού χαρακτήρα. Όλο και περισσότερες προσωπικές πληροφορίες είναι online, είτε πρόκειται για ηλεκτρονικές τραπεζικές συναλλαγές, αγορές, κοινωνικά δίκτυα ή ηλεκτρονικές επιστροφές φόρου. Τα άτομα έχουν δικαίωμα στην προστασία και αποθήκευση των προσωπικών τους δεδομένων.

Σε σύγκριση με τον προηγούμενο κανονισμό (οδηγία για την προστασία των δεδομένων), η σημασία της εφαρμογής των αρχών είναι πιο έντονη, οι ορισμοί είναι σαφέστεροι και ταυτόχρονα επεκτείνονται από ορισμένες, σύγχρονες αρχές προστασίας προσωπικών δεδομένων. Σε αντίθεση με την προηγούμενη οδηγία, όπου οι αρχές αφορούσαν πρωτίστως την ποιότητα των δεδομένων, ο κανονισμός συνδέει τις αρχές με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι αρχές του κανονισμού, οι οποίες καλύπτονται επίσης από τον προηγούμενο κανονισμό, είναι οι εξής: η αρχή της νομιμότητας, της θεμιτής επεξεργασίας και της διαφάνειας, η αρχή του περιορισμού του σκοπού, η αρχή της ελάχιστης επεξεργασίας δεδομένων, η αρχή της ακρίβειας, η αρχή του περιορισμού της αποθήκευσης δεδομένων. Ωστόσο, η αρχή της ακεραιότητας και της εμπιστευτικότητας αποτελεί αναπόσπαστο μέρος του Κανονισμού και καλύπτει την προστασία των δεδομένων με τεχνικά και οργανωτικά μέτρα, ενημερώνοντας την εποπτική αρχή και τα πρόσωπα στα οποία ανήκουν τα δεδομένα σε περίπτωση παραβίασης δεδομένων. Ωστόσο, ίσως η πιο σημαντική αρχή είναι η αρχή της ευθύνης, η οποία εισάγει την υποχρέωση του φορέα εκμετάλλευσης να αποδείξει ότι συμμορφώνεται με όλες τις αρχές. Η προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί θεμελιώδες δικαίωμα κάθε ατόμου στην ΕΕ. Η έναρξη ισχύος του κανονισμού 2016/679 επιτρέπει τον έλεγχο των δεδομένων προσωπικού χαρακτήρα και τη βελτίωση της ασφάλειας στο διαδίκτυο και σε άλλες βάσεις δεδομένων.

Όσον αφορά την κατάρτιση προφίλ και την αυτοματοποιημένη λήψη αποφάσεων, ο ΓΚΠΔ έχει θεσπίσει ειδικούς κανόνες: το άρθρο 22 παράγραφος 1 ορίζει ότι το υποκείμενο των δεδομένων «έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, η οποία παράγει έννομα αποτελέσματα που το αφορούν». Όπως υπογραμμίζεται στις κατευθυντήριες γραμμές της Ομάδας Εργασίας του άρθρου 29[63], η τεχνολογική πρόοδος και οι δυνατότητες της ανάλυσης μαζικών δεδομένων, της τεχνητής νοημοσύνης και της μηχανικής μάθησης έχουν καταστήσει ευκολότερη τη δημιουργία προφίλ και τη λήψη αυτοματοποιημένων αποφάσεων, με πιθανές σημαντικές επιπτώσεις στα ατομικά δικαιώματα και ελευθερίες. Το συγκεκριμένο άρθρο προβλέπει, με τις εξαιρέσεις[64] που διατυπώνονται στον ΓΚΠΔ, γενική απαγόρευση της πλήρως αυτοματοποιημένης λήψης αποφάσεων.

Στο δίκαιο του Συμβουλίου της Ευρώπης η Εκσυγχρονισμένη Σύμβαση 108[65] παρέχει νέα δικαιώματα στο υποκείμενο των δεδομένων προκειμένου να πραγματοποιείται πιο αποτελεσματικά ο έλεγχος στα προσωπικά του δεδομένα στην εποχή των μαζικών δεδομένων.

Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή και συναφή και να περιορίζονται στα αναγκαία για τους σκοπούς της επεξεργασίας τους. Ωστόσο, το επιχειρηματικό μοντέλο των μαζικών δεδομένων ενδέχεται να είναι το άκρως αντίθετο της ελαχιστοποίησης των δεδομένων, διότι απαιτεί ολοένα και περισσότερα δεδομένα, και μάλιστα συχνά για απροσδιόριστους σκοπούς.

---

[63] Ομάδα εργασίας του άρθρου 29, Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, WP 251, 3 Οκτωβρίου 2017, σ. 9.

[64] Οι υπεύθυνοι επεξεργασίας δεδομένων δύνανται να απαλλάσσονται από την εν λόγω απαγόρευση μόνο σε τρεις συγκεκριμένες περιπτώσεις: όταν η απόφαση: 1) είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, 2) επιτρέπεται από το δίκαιο της ΕΕ ή το δίκαιο κράτους μέλους ή 3) βασίζεται σε ρητή συγκατάθεση.

[65] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018PC0451&from=en

Με την έλλειψη μέτρων αντιμετώπισης κινδύνων οι κοινωνίες μένουν εκτεθειμένες σε περιστατικά ασφαλείας, όπως το «φαινόμενο μαύρου κύκνου[66]» , που ταλαντεύεται μεταξύ περιπτώσεων χαμηλής επικινδυνότητας (δίνοντας την εντύπωση ότι δεν υπάρχει πραγματικός κίνδυνος) αλλά και συμβάντων μείζονος σημασίας, με τεράστιο αντίκτυπο στην ιδιωτικότητα των ατόμων. Η ενσωμάτωση τεχνολογιών βελτίωσης της ιδιωτικής ζωής, όπως η σωστή τεχνική ανωνυμοποίησης και κρυπτογράφησης, στο σχεδιασμό αναλυτικών στοιχείων αποτελεί αναπόσπαστο μέρος της αποφυγής παραβιάσεων προσωπικών δεδομένων και της ανοικοδόμησης της εμπιστοσύνης μεταξύ χρηστών και παρόχων υπηρεσιών.

Οι προκλήσεις της ιδιωτικής ζωής πρέπει, επομένως, να θεωρηθούν ως ευκαιρίες που εάν αντιμετωπιστούν κατάλληλα μπορούν να οικοδομήσουν εμπιστοσύνη στο μεγάλο οικοσύστημα δεδομένων, προς όφελος τόσο των χρηστών όσο και της βιομηχανίας μαζικών δεδομένων.

ο Γενικός Κανονισμός για την Προστασία Δεδομένων επιβάλλει στον υπεύθυνο επεξεργασίας την υποχρέωση να παρέχει στο υποκείμενο των δεδομένων σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται στο πλαίσιο της αυτοματοποιημένης λήψης αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ[67].

Η ψευδωνυμοποίηση αποτελεί μία από τις εγγυήσεις που μπορούν να παρέχουν προστασία έναντι της κατάχρησης μαζικών δεδομένων και προσωπικών πληροφοριών. Εάν τα δεδομένα προσωπικού χαρακτήρα έχουν πράγματι ανωνυμοποιηθεί, δηλαδή δεν υπάρχουν πληροφορίες που να αφήνουν ίχνη τα οποία τα συνδέουν με το υποκείμενο των δεδομένων, οι περιπτώσεις αυτές δεν εμπίπτουν στο πεδίο εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων.

Η επεξηγηματική έκθεση του πρωτοκόλλου για την τροποποίηση της σύμβασης (ETS No. 108), η οποία ήταν σε ισχύ από το 1985, για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα[68] αναφέρει (άρθρο 8) ότι ο υπεύθυνος επεξεργασίας υποχρεούται να ενεργεί με διαφάνεια κατά την επεξεργασία δεδομένων και ότι οι πληροφορίες που παρουσιάζονται στο υποκείμενο των δεδομένων θα πρέπει να είναι εύκολα προσβάσιμες, ευανάγνωστες και κατανοητές. Για την ενημέρωση των ατόμων που τα προσωπικά τους δεδομένα έχουν υποβληθεί σε επεξεργασία ο υπεύθυνος επεξεργασίας μπορεί να χρησιμοποιήσει κάθε πρόσφορο μέσο για τα ενημερώσει.

Σύμφωνα με την αρχή του περιορισμού της αποθήκευσης, η οποία προβλέπεται τόσο στον ΓΚΠΔ όσο και στην Εκσυγχρονισμένη Σύμβαση 108, τα δεδομένα πρέπει να διατηρούνται «υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Επομένως, τα δεδομένα θα πρέπει να διαγραφούν ή να ανωνυμοποιηθούν εάν ο υπεύθυνος επεξεργασίας επιθυμεί να τα αποθηκεύσει όταν δεν είναι πλέον αναγκαία και δεν εξυπηρετούν πλέον τον αρχικό σκοπό τους.

[66] black swan effect: γεγονότα υψηλού αντίκτυπου που φαίνονται απίθανα και απρόβλεπτα, αλλά, εκ των υστέρων, είναι εξηγήσιμα.
[67] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο στ
[68] https://rm.coe.int/cets-223-explanatory-report-to-the-%20protocol-amending-the-convention-fo/16808ac91a

Η διαδικασία ανωνυμοποίησης των δεδομένων σημαίνει ότι όλα τα αναγνωριστικά στοιχεία απαλείφονται από ένα σύνολο δεδομένων προσωπικού χαρακτήρα έτσι ώστε το υποκείμενο των δεδομένων να μην είναι πλέον ταυτοποιήσιμο[69].

Αντίστοιχα στο ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 14ης Μαρτίου 2017 (2016/2225(INI)) υπογραμμίζεται ότι ο αυτοσκοπός των μαζικών δεδομένων πρέπει να είναι η επίτευξη συγκρίσιμων συσχετισμών με όσο το δυνατόν λιγότερα δεδομένα προσωπικού χαρακτήρα. Επισημαίνεται επίσης πως η εφαρμογή της ψευδωνυμοποίησης, της ανωνυμοποίησης ή της κρυπτογράφησης σε δεδομένα προσωπικού χαρακτήρα μπορεί να μειώσει τους κινδύνους για όσους αποτελούν υποκείμενα των δεδομένων, όταν τα δεδομένα προσωπικού χαρακτήρα χρησιμοποιούνται σε εφαρμογές μαζικών δεδομένων.

5.17 Ο ρόλος των Δεδομένων στα ITS και ο GDPR

Τα δεδομένα θα μπορούσαν να θεωρηθούν ως το νόμισμα του 21ου αιώνα (Floridi, 2014), στις μεταφορές τα δεδομένα είναι εξίσου ζωτικής σημασίας με τα οχήματα και τις υποδομές για την απρόσκοπτη λειτουργία προηγμένων συστημάτων. Μπορεί να υποστηριχθεί ότι καθώς η έννοια της μεταφοράς, που αρχικά συνδεόταν με τη φυσική μετακίνηση επιβατών και εμπορευμάτων, μετατρέπεται σε μια πιο εξελιγμένη, χωρίς αποκλεισμούς και άυλη έννοια, εστιασμένη στο λογισμικό.

Η διακυβέρνηση των δεδομένων στα ITS και ιδίως των συνδεδεμένων αυτόνομων οχημάτων είναι ζωτικής σημασίας, δεδομένου ότι τα δεδομένα είναι το κλειδί όχι μόνο για την εφαρμογή τεχνολογιών, αλλά και για την αξιολόγηση του κοινωνικού τους αντικτύπου, ακόμη και για τη θέσπιση πολιτικών.

Ο GDPR είναι η εξέχουσα νομοθεσία σχετικά με την προστασία των δεδομένων εντός της ΕΕ, θέτοντας επίσης ένα παγκόσμιο πρότυπο, καθώς αντιπροσωπεύει τη ραχοκοκαλιά της μελλοντικής ψηφιακής οικονομίας της ΕΕ. Πράγματι, ο GDPR αντικαθιστά την προηγούμενη οδηγία 95/46/ΕΚ για την προστασία των δεδομένων, εισάγοντας αρκετές κρίσιμες βελτιώσεις, ξαναγράφοντας προηγούμενες θεμελιώδεις αρχές και συμπληρώνοντάς τις με την απαίτηση λογοδοσίας (άρθρο 5, παράγραφος 2), η οποία αποτελεί τον ακρογωνιαίο λίθο της συμμόρφωσης με τον GDPR. Επιπλέον, επιβάλλει νέες υποχρεώσεις στον Υπεύθυνο Επεξεργασίας, όπως η γνωστοποίηση «Παραβίασης Δεδομένων» (άρθρα 33 και 34) και η Εκτίμηση Αντικτύπου Δεδομένων (άρθρο 35), ενώ εισάγει νέους ρόλους ως Εκτελών την Επεξεργασία Δεδομένων (άρθρο 28) και του Υπεύθυνου Προστασίας Δεδομένων (άρθρα 37–39). Τρίτον, αυξάνει τα δικαιώματα του υποκειμένου των δεδομένων δημιουργώντας νέα προνόμια, συμπεριλαμβανομένου του «δικαιώματος στη λήθη» (άρθρο 17). Εν ολίγοις, ο GDPR ανοίγει το δρόμο για ένα προηγμένο νομικό πλαίσιο στην προστασία των προσωπικών δεδομένων, θέτοντας μια διεθνή πρότυπη έννοια της διακυβέρνησης δεδομένων.

Μέσα σε αυτό το ταχέως μεταβαλλόμενο πλαίσιο, η συλλογή και επεξεργασία δεδομένων στα αυτόνομα οχήματα εγείρει πολλαπλά νομικά ζητήματα ανάλογα με το ισχύον πλαίσιο διαχείρισης πληροφοριών, ανεξάρτητα για ποιο λόγο πραγματοποιείται.

Παρά το γεγονός ότι ορισμένα δικαιώματα παρέχονται σε οδηγούς, επιβάτες ή πεζούς ως «υποκείμενα δεδομένων» (άρθρο 4 παράγραφος 1 του GDPR), κατ' αρχήν η κυριότητα αυτών των δεδομένων ανήκει αποκλειστικά σε εκείνους που τελικά τα

[69] Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 26

ελέγχουν και ορίζονται ως «Εκτελών την επεξεργασία» (άρθρο 4 παράγραφος 7 GDPR). Σύμφωνα με τον κατ' εξουσιοδότηση κανονισμό (ΕΕ) 2015/962[70] , πρέπει να χορηγείται «προσβασιμότητα, ανταλλαγή και περαιτέρω χρήση» ειδικών ειδών δεδομένων, ιδίως «στατικών δεδομένων σχετικά με το οδικό δίκτυο» (άρθρο 4), «δυναμικών δεδομένων σχετικά με το οδικό δίκτυο» (άρθρο 5) και «δεδομένων κίνησης» (άρθρο 6). Επιπλέον, ένας κανονισμός της ΕΕ καθορίζει το τεχνολογικό πρότυπο που πρέπει να υιοθετηθεί για τη μετάδοση δεδομένων, το οποίο είναι επί του παρόντος το DATEX II[71].

Τα δεδομένα είναι ζωτικής σημασίας για την ανάπτυξη στα αυτόνομα οχήματα. Λόγω των τεράστιων επενδύσεων που έγιναν για το σχεδιασμό, την κατασκευή και τη συντήρηση οχημάτων, συσκευών επί του οχήματος και υποδομών, η αξία των αντίστοιχων ευρημάτων επιτυγχάνει έναν στρατηγικό στόχο όχι μόνο όσον αφορά τα καθαρά ερευνητικά αποτελέσματα, αλλά και τη βιομηχανική παραγωγή και ακόμη και τις γεωπολιτικές στρατηγικές ανάγκες.

Ωστόσο, δεδομένου του τεράστιου όγκου δεδομένων που θα παράγονται καθημερινά από τα AV, είναι κρίσιμο να διατυπωθούν τέτοιοι κανονισμοί. Επιπλέον, είναι σημαντικό να προωθηθεί η διακρατική συνεργασία όσον αφορά τη διαχείριση δεδομένων όχι μόνο στην ΕΕ, όπου πολλά κράτη μέλη είναι στενά διασυνδεδεμένα, αλλά και διεθνώς μεταξύ χωρών και ηπείρων. Είναι προφανές ότι αυτό είναι ένα πεδίο διεθνούς ενδιαφέροντος τόσο για τους επαγγελματίες όσο και για τους υπεύθυνους χάραξης πολιτικής.

5.18 ETC (Electronic Toll Collection) & ζητήματα GDPR

Τα ευφυή συστήματα μεταφορών (ITS) έχουν σχεδιαστεί για την αντιμετώπιση διαφόρων ζητημάτων όπως η συμφόρηση, η ρύπανση και τα ατυχήματα λόγω της σημαντικής αύξησης της κυκλοφορίας οχημάτων, των δημόσιων συγκοινωνιών, κ.λπ.. Η ροή δεδομένων ITS περιλαμβάνει τρεις κύριες συνιστώσες: συλλογή δεδομένων, ανάλυση δεδομένων και διάδοση δεδομένων. Η συνιστώσα συλλογής δεδομένων συγκεντρώνει πληροφορίες όπως ο χρόνος, η τοποθεσία, η ροή της κυκλοφορίας, η κατανάλωση καυσίμων κ.λπ. Αργότερα, τέτοια δεδομένα μπορούν να αναλυθούν για διάφορες εφαρμογές: ηλεκτρονική είσπραξη διοδίων (ETC), συλλογή στατιστικών κυκλοφορίας, οδική ασφάλεια, αυτοματοποιημένη επιβολή του νόμου για την κυκλοφορία κ.α. Τα συστήματα ETC αποσκοπούν στη βελτίωση των διοδίων μέσω της αυτόματης είσπραξης διοδίων, χωρίς επιβράδυνση των οχημάτων, σε αντίθεση με ένα χειροκίνητο σύστημα είσπραξης διοδίων που επιβραδύνει δραστικά τα οχήματα, προκαλώντας έτσι καθυστερήσεις και συμφόρηση. Αναμένεται ότι η παγκόσμια αγορά ηλεκτρονικής είσπραξης διοδίων, μεταξύ 2019 και 2030, θα έχει σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) 8,3%, φθάνοντας περίπου τα 18,5 δισεκατομμύρια δολάρια ΗΠΑ έως το 2030[72].

Για τη δημιουργία ενός ηλεκτρονικού συστήματος συλλογής διοδίων, χρησιμοποιούνται συνήθως 2 τύποι τεχνολογιών.

• Αποκλειστικές επικοινωνίες μικρής εμβέλειας (DSRC): Το DSRC χρησιμοποιείται ευρέως και εμπίπτει στην εμβέλεια ραδιοσυχνοτήτων ή μικροκυμάτων του

[70] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015R0962&from=EN
[71] https://datex2.eu/
[72] "Projections for the global electronic toll collection market size between 2019 and 2030," https://www.statista.com/statistics/1254629/global-electronic-toll-collection-market-forecast/, accessed: 2021-12-20.

ηλεκτρομαγνητικού φάσματος. Σε αυτή την τεχνολογία, οι κεραίες εγκαθίστανται στις γερανογέφυρες διοδίων που επικοινωνούν με τοποθετημένους αναμεταδότες ή ετικέτες στα οχήματα καθώς περνούν. Σκιαγραφούμε εν συντομία τις αλληλεπιδράσεις μεταξύ των συστατικών ως εξής. Ένας οδηγός υποβάλλει την ταυτότητά του, όπως ένα διαβατήριο, στο TSP (Toll service provider) και λαμβάνει ταυτότητα. Όταν ένα όχημα περνά από μια γέφυρα διοδίων, η εποχούμενη μονάδα (OBU), που βρίσκεται μέσα στο όχημα, επικοινωνεί με την RSU για να υπολογίσει το συνολικό τέλος διοδίων. Το RSU, από καιρό σε καιρό, στέλνει τις πληροφορίες του στο TSP για ενημέρωση. Τέλος, το TSP εκδίδει τιμολόγιο για τον οδηγό στο τέλος της περιόδου χρέωσης και, κατά συνέπεια, ο οδηγός καταβάλλει το συνολικό τέλος διοδίων, το οποίο οφείλει στον TSP.

Εικόνα 20: Στοιχεία συστήματος ETC βασιζόμενου σε DSRC

• Παγκόσμιο δορυφορικό σύστημα πλοήγησης (GNSS - Global navigation satellite system): Το εποχούμενο όχημα, με τη βοήθεια του Παγκόσμιου Συστήματος Εντοπισμού Θέσης (GPS), λαμβάνει τη θέση του οχήματος από τον δορυφόρο GPS και αποθηκεύει δεδομένα που σχετίζονται με την διαδρομή του οχήματος σε συνάρτηση με το κόστος των διοδίων σύμφωνα με την τιμολογιακή πολιτική του παρόχου. Για την επικοινωνία με τον πάροχο, χρησιμοποιούνται από κοινού το GNSS και το παγκόσμιο σύστημα κινητής επικοινωνίας (GSM). Σε αυτά τα συστήματα, οι ιδιωτικές τοποθεσίες αποθηκεύονται συνήθως στην εποχούμενη μονάδα και ο πάροχος δεν γνωρίζει τις θέσεις των οδηγών σε αντίθεση με τα συστήματα που βασίζονται σε DSRC όπου η RSU και ο πάροχος έχουν πρόσβαση στις ανώνυμες τοποθεσίες οδηγών

Εικόνα 21: Συστατικά στοιχεία συστήματος ETC που βασίζεται σε GNSS

Οι πάροχοι υπηρεσιών διοδίων (TSP) αποθηκεύουν διάφορες πληροφορίες, συμπεριλαμβανομένων των ωρών, των τοποθεσιών και των ταυτοτήτων των οχημάτων, για τη χρέωση των οδηγών. Οι αποθηκευμένες πληροφορίες θα μπορούσαν να προκαλέσουν προβλήματα απορρήτου στα συστήματα ETC, παραβιάζοντας τα άρθρα 1 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) της ΕΕ. Μία από τις βασικές ανησυχίες είναι ότι ο πάροχος μπορεί να χρησιμοποιήσει τα δεδομένα των οδηγών για να μάθει τα μοτίβα κίνησής τους, συμπεριλαμβανομένου του τόπου όπου πηγαίνουν για δουλειά ή αναψυχή, δημιουργώντας ατομικά προφίλ για τον καθένα. Η πρακτική αυτή θα έθετε σε κίνδυνο την αρχή που ονομάζεται «περιορισμός σκοπού» που αναφέρεται στον ΓΚΠΔ (άρθρο 5 του ΓΚΠΔ). Ένα άλλο πιθανό ζήτημα είναι ότι τρίτα μέρη, όπως ασφαλιστικές εταιρείες, μπορεί να βρουν τα δεδομένα εμπορικά πολύτιμα και να επιθυμούν να τα χρησιμοποιήσουν. Σε μια τέτοια περίπτωση, η χρήση των δεδομένων των οδηγών από τρίτους θα πρέπει να υπόκειται στη συγκατάθεση τους, όπως ορίζεται στον GDPR (άρθρο 7 GDPR). Η ασφάλεια των δεδομένων είναι μια άλλη πτυχή των ζητημάτων προστασίας της ιδιωτικής ζωής στα συστήματα ETC και αφορά τη διασφάλιση της ασφάλειας των πληροφοριών από εξωτερική πρόσβαση και εσωτερική διαρροή. Εάν τα μέτρα ασφαλείας δεν ληφθούν επαρκώς υπόψη, οι εξωτερικές οντότητες θα μπορούσαν να μάθουν για τα δεδομένα που μεταδίδονται μέσω του δικτύου ή οι εσωτερικοί υπάλληλοι θα μπορούσαν να συναγάγουν πληροφορίες που δεν πρέπει. Αυτό αντίκειται στην αρχή του ΓΚΠΔ, σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια των δεδομένων προσωπικού χαρακτήρα καταλλήλως (άρθρο 5 του ΓΚΠΔ).

5.19 Εργαλεία & πλαίσια συμμόρφωσης με τον ΓΚΠΔ

Η συμμόρφωση με τον GDPR αντιμετωπίζεται επί του παρόντος σε πολλά έργα της ΕΕ, όπως στα BPR4GDPR[73], DEFeND[74], SMOOTH[75], PDP4E[76], PAPAYA[77] και PoSeID-on[78]. Τα έργα αυτά αντιμετωπίζουν την έλλειψη συγκεκριμένων, λειτουργικών λύσεων που ανταποκρίνονται σε προκλήσεις και νομικές καινοτομίες που θέτει ο ΓΚΠΔ, παρέχοντας συστηματικές μεθόδους, λεπτομερείς τεχνικές και εργαλεία λογισμικού. Στη βιβλιογραφία επίσης είναι διαθέσιμα προτεινόμενα πλαίσια μοντέλων και εργαλείων απορρήτου για το GDPR τα οποία καλύπτουν εν μέρει τις αρχές και τα άρθρα του GDPR.

Ο στόχος του BPR4GDPR (Business Process Re-engineering and functional toolkit for GDPR compliance) είναι να παρέχει ένα ολιστικό πλαίσιο ικανό να υποστηρίξει διαδικασίες συμβατές με το GDPR από άκρο σε άκρο εντός και μεταξύ οργανισμών με δυνατότητα ΤΠΕ σε διάφορες κλίμακες. Οι προτεινόμενες λύσεις είναι πολύ γενικές και στοχεύουν στην κάλυψη ολόκληρου του κύκλου ζωής της διαδικασίας, από τον αρχικό προσδιορισμό ή τις προδιαγραφές της έως τη θέσπιση και την εκτέλεσή της.

Το DEFeND2 είναι το πλαίσιο διακυβέρνησης δεδομένων που έχει σχεδιαστεί για να βοηθήσει τους οργανισμούς να εφαρμόσουν το GDPR. . Ειδικότερα, η τεχνική εστίαση του έργου είναι στην παροχή της νέας πλατφόρμας Data Privacy Governance for Supporting GDPR (DEFeND), η οποία υποστηρίζει τη διακυβέρνηση απορρήτου με επίκεντρο τον οργανισμό και αντιμετωπίζει τις προκλήσεις που αντιμετωπίζουν οι οργανισμοί κατά τη συμμόρφωσή τους με τον GDPR.

Το έργο θα επιτύχει το στόχο του εισάγοντας ένα νέο παράδειγμα, το οποίο ονομάζουμε Model-Driven Privacy Governance (MDPG). Ένα τέτοιο παράδειγμα επιτρέπει τη δημιουργία (από ένα αφηρημένο έως ένα συγκεκριμένο επίπεδο) και την ανάλυση μοντέλων που σχετίζονται με την προστασία της ιδιωτικής ζωής ακολουθώντας μια προσέγγιση προστασίας της ιδιωτικής ζωής βάσει σχεδιασμού που εκτείνεται σε δύο επίπεδα, το επίπεδο σχεδιασμού και το επιχειρησιακό επίπεδο, και σε τρεις τομείς διαχείρισης, δηλαδή το πεδίο εφαρμογής δεδομένων, τη διαδικασία δεδομένων και την παραβίαση δεδομένων.

Το privacyTracker[79], ένα εργαλείο συμβατό με το GDPR που καλύπτει την εντοπισημότητα και τη διαφάνεια των δεδομένων. Εφαρμόζουν ορισμένα δικαιώματα GDPR, όπως η φορητότητα δεδομένων και το δικαίωμα διαγραφής. Ένα πλαίσιο privacyTracker είναι μια προσέγγιση που εξουσιοδοτεί τους καταναλωτές με κατάλληλους ελέγχους να εντοπίζουν την αποκάλυψη δεδομένων όπως συλλέγονται από εταιρείες και να αξιολογούν την ακεραιότητα αυτών των δεδομένων πολλαπλών

[73] bpr4gdpr. The business process re-engineering and functional toolkit for gdpr compliance project. 2021, Online; https://www.bpr4gdpr.eu/. [Accessed 15 January 2021].
[74] DEFeND. The Defend project. 2021, Online; https://www.defendproject.eu/. [Accessed 15 January 2021].
[75] SMOOTH. The Smooth platform. 2021, Online; https://smoothplatform.eu/. [Accessed 15 January 2021].
[76] PDP4E. The pdp4e project. 2021, Online; https://www.pdp4e-project.eu/. [Accessed 15 January 2021].
[77] PAPAYA. The papaya project. 2021, Online; https://www.papaya-project.eu/. [Accessed 15 January 2021].
[78] PoSeID-on. The PoSeID-on project. 2021, Online; https://www.poseidon-h2020.eu/. [Accessed 15 January 2021].
[79] Gjermundrød H, Dionysiou I, Costa K. PrivacyTracker: a privacy-by-design GDPR compliant framework with verifiable data traceability controls. In: International conference on web engineering. Springer; 2016, p. 3–15.

χειρισμών. Αυτό επιτυγχάνεται με την κατασκευή μιας δενδροειδούς δομής δεδομένων όλων των οντοτήτων που έλαβαν την ψηφιακή εγγραφή, διατηρώντας παράλληλα αναφορές που επιτρέπουν τη διέλευση του δέντρου από οποιονδήποτε κόμβο, τόσο με τρόπο από πάνω προς τα κάτω όσο και από κάτω προς τα πάνω.

Για τη λογοδοσία του GDPR στα συστήματα IoT, προτείνεται ένα μοντέλο IoT Databox[80] που παρέχει τους μηχανισμούς για την οικοδόμηση σχέσεων εμπιστοσύνης IoT. Το IoT Databox είναι μια λύση αιχμής που εφαρμόζει τη σύσταση τοπικού ελέγχου και συγκεντρώνει προσωπικά δεδομένα σε μια δικτυωμένη συσκευή που βρίσκεται στο σπίτι. Πληροί την απαίτηση εξωτερικής λογοδοσίας αναδεικνύοντας τις αλληλεπιδράσεις μεταξύ συνδεδεμένων συσκευών και επεξεργαστών δεδομένων

Το TagUBig - Taming Your Big Data[81] , ένα πλαίσιο για τον έλεγχο και τη βελτίωση της διαφάνειας, του απορρήτου, της διαθεσιμότητας και της χρηστικότητας όταν οι χρήστες αλληλεπιδρούν με εφαρμογές. Το πλαίσιο περιλαμβάνει στοιχεία που μπορούν να αντιμετωπίσουν ορισμένες από τις βασικές προκλήσεις του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

Για το σύστημα IoT, το ADvoCATE[82] είναι μια λύση με επίκεντρο τον χρήστη που επιτρέπει στα υποκείμενα των δεδομένων να ελέγχουν εύκολα τις συναινέσεις σχετικά με την πρόσβαση στα προσωπικά τους δεδομένα στο οικοσύστημα IoT και να ασκούν τα δικαιώματά τους που ορίζονται από τον GDPR. Βοηθά επίσης τους Υπευθύνους Επεξεργασίας και Επεξεργασίας Δεδομένων να πληρούν τις απαιτήσεις του GDPR. Μια υποδομή blockchain διασφαλίζει την ακεραιότητα των συναινέσεις επεξεργασίας προσωπικών δεδομένων, ενώ η ποιότητά τους αξιολογείται από μια υπηρεσία πληροφοριών.

Όπως μπορούμε να δούμε, πολλά έργα βλέπουν το φως στον τομέα του GDPR. Τα έργα αυτά έχουν διαφορετικούς στόχους και διαφορετικά πεδία. Δεδομένου ότι δεν είναι ακόμη εφικτό να αντιμετωπιστούν όλα τα ζητήματα, κάθε έργο έχει το δικό του κοινό-στόχο ή / και επικεντρώνεται σε ορισμένες συγκεκριμένες πτυχές του GDPR. Παρόλο που οι εργασίες διεξάγονται, αρκετές άλλες πτυχές του GDPR παραμένουν ανοικτές, όπως ο περιορισμός του σκοπού, η ελαχιστοποίηση των δεδομένων και ο περιορισμός της αποθήκευσης.

5.20 Σύνοψη και Συμπεράσματα

Σε αυτή τη Διπλωματική εργασία έγινε μια εις βάθος βιβλιογραφική έρευνα των έξυπνων συστημάτων μεταφορών και των εφαρμογών τους, εξετάζοντας τις κύριες τεχνολογίες που χρησιμοποιούνται σήμερα για την ανάπτυξη τους. Πραγματοποιήθηκε ανάλυση των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται από αυτά τα έξυπνα συστήματα μεταφορών για τη διασφάλιση της λειτουργικότητας και για τη βελτίωση των ζητημάτων των συστημάτων μεταφοράς. Εξηγούνται επίσης οι βασικές τεχνολογίες ασύρματων επικοινωνιών, όπως η επικοινωνία μεταξύ οχημάτων και οχημάτων με άλλες συσκευές.

[80] Crabtree A, Lodge T, Colley J, Greenhalgh C, Glover K, Haddadi H, et al. Building accountability into the Internet of Things: the IoT Databox model. J Reliab Intell Environ 2018;4(1):39–55.
[81] Ferreira A, Muchagata J. Tagubig-taming your big data. In: 2018 international carnahan conference on security technology. IEEE; 2018, p. 1–5.
[82] Rantos K, Drosatos G, Demertzis K, Ilioudis C, Papanikolaou A, Kritsas A. ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology. In: International conference on security for information technology and communications. Springer; 2018, p. 300–13.

Ένας στόχος που πρέπει να επιτευχθεί θα είναι η βελτίωση της τεχνολογικής υποδομής που θα περιλαμβάνει την πλήρη και συνολική λειτουργία των επικοινωνιών V2V, V2I και V2X. Ωστόσο, η δυσκολία που πρέπει να αντιμετωπιστεί δεν οφείλεται μόνο στη δυνητικά δύσκολη εφαρμογή σε μεγάλη κλίμακα, αλλά και στην έλλειψη ενός κοινού προτύπου που θα χρησιμοποιείται παγκοσμίως.

Οι αναδυόμενες τεχνολογίες όπως το Διαδίκτυο των Πραγμάτων, οι 5G Τεχνολογίες, το Blockchain, τα Μαζικά Δεδομένα, η Τεχνητή Νοημοσύνη είναι αναπόσπαστα κομμάτια του παζλ που πρέπει να συντεθεί για την εξέλιξη των Έξυπνων Πόλεων και των Ευφυών Συστημάτων Μεταφορών ως κομμάτι τους. Η ιδιαίτερη περίπτωση των ευφυών μεταφορών, όπου τα οχήματα θεωρούνται ευφυείς κινητές συσκευές ικανές να συνδεθούν στο δίκτυο για να μοιράζονται πληροφορίες σχετικά με το περιβάλλον τους, είναι ένας στόχος που απαιτεί προσεκτικό και έξυπνο σχεδιασμό για την διαλειτουργικότητα των εφαρμογών και την ασφαλή λειτουργία τους. Η βελτιστοποίηση των συστημάτων μεταφορών θα έχει ως αποτέλεσμα τη μείωση των περιβαλλοντικών επιπτώσεων και της εξοικονόμησης ενέργειας, ζητημάτων ιδιαίτερα κρίσιμα για το μέλλον.

Παρά τα μεγάλα πλεονεκτήματα που δείχνουν την έλευση της εποχής του 5G και του IoT, εξακολουθούν να υπάρχουν προβλήματα που πρέπει να αντιμετωπιστούν στον τεχνολογικό τομέα όπως η επίλυση των προβλημάτων κάλυψης και εύρους ζώνης.

Το 5G υπόσχεται να αλλάξει το πεδίο της ασύρματης επικοινωνίας με υψηλότερους ρυθμούς δεδομένων για τη μεταφορά των δεδομένων από την πηγή στον προορισμό σε πραγματικό χρόνο. Θα προσφέρει επίσης δυνατότητες AI και απαράμιλλη ταχύτητα με καλύτερη απόδοση μαζί με τη διάρκεια ζωής της μπαταρίας των συσκευών.

Η ανάπτυξη του IoT μπορεί να αποφέρει πολλά οφέλη στην προσωπική ζωή των ανθρώπων, μπορεί όμως να συλλέγει και να προσδιορίζει αυτόματα πληροφορίες και προτιμήσεις υποκειμένων, γεγονός που μπορεί να προκαλέσει βλάβη στην ασφάλεια και την ιδιωτικότητα των προσωπικών πληροφοριών τους.

Η τεχνολογία των Μαζικών Δεδομένων, θα αντιμετωπίσει προκλήσεις στην εφαρμογή και την ανάλυση των δεδομένων αυτών λόγω των χαρακτηριστικών τους όπως είναι ο όγκος και η ετερογένεια τους. Το απόρρητο είναι ίσως η πιο αυστηρή απαίτηση ασφαλείας που υπαγορεύεται από τις εφαρμογές μεταφοράς που αξιοποιούν τα Μαζικά Δεδομένα λόγω των προσωπικών γεωγραφικών δεδομένων και του περιεχομένου που μοιράζονται οι χρήστες μέσω των συσκευών και των υπολογιστών τους. Για το λόγο αυτό, ο κλάδος των μεταφορών εξακολουθεί να αντιμετωπίζει ανεπίλυτες προκλήσεις όσον αφορά τη συλλογή προσωπικών δεδομένων. Οι παραβιάσεις ασφαλείας και τα κενά καλύπτουν από την κλοπή ταυτότητας έως την ανεπιθύμητη παρακολούθηση τοποθεσίας και την υπερβολική αποθήκευση ιχνών δεδομένων.

Η έννοια της προστασίας της ιδιωτικής ζωής από το σχεδιασμό δίνει έμφαση στην αντιμετώπιση της προστασίας των δεδομένων των σχετικών συστημάτων όχι μόνο κατά τη διάρκεια του πλήρους κύκλου ζωής κάθε συστήματος, αλλά και σε όλες τις φάσεις σχεδιασμού και προγραμματισμού. Πολλά υποσχόμενοι τεχνικοί τομείς προς αυτή την κατεύθυνση περιλαμβάνουν τις πρόσφατα προτεινόμενες προσεγγίσεις που βασίζονται σε blockchain.

Παρά τα σημαντικά πλεονεκτήματα που αναλύθηκαν για τα χαρακτηριστικά τεχνικών κρυπτογράφησης-απορρήτου, οι τρέχουσες λύσεις blockchain εξακολουθούν να απέχουν πολύ για να αντιμετωπίσουν αυτές τις προκλήσεις απορρήτου με ολιστικό τρόπο. Αυτή η κατάσταση υπονομεύει τα δικαιώματα του χρήστη, όπως το δικαίωμα

να γίνει ανώνυμος σε ορισμένες περιπτώσεις, το δικαίωμα διαγραφής δεδομένων ή ανάκλησης συγκατάθεσης, μειώνοντας έτσι την υλοποίηση ενός μοντέλου πραγματικής διατήρησης της ιδιωτικής ζωής.

Ο GDPR και το blockchain θα μπορούσε να ειπωθεί ότι έχουν την ίδια αποστολή: να αυξήσουν την αίσθηση της ιδιωτικής ζωής και της αυτονομίας των ατόμων. Ωστόσο, οι μέθοδοι που χρησιμοποιούνται για την εκπλήρωση αυτής της αποστολής – η εκ νέου διαμεσολάβηση και η σχετική συγκέντρωση στην περίπτωση του GDPR, η αποδιαμεσολάβηση και η αποκέντρωση στην περίπτωση του blockchain – διαφέρουν σημαντικά και μπορεί επίσης να έρθουν σε άμεση σύγκρουση μεταξύ τους.

Ένα μεγάλο ζήτημα που αναδεικνύεται στον κλάδο της Τεχνητής Νοημοσύνης, μέσα από τη βιβλιογραφική έρευνα που πραγματοποιήθηκε, είναι να εξισορροπηθεί η καινοτομία με τα ατομικά δικαιώματα και τις κοινωνικές αξίες, διασφαλίζοντας την υιοθέτηση κανόνων και αρχών προστασίας προσωπικών δεδομένων που ορίζει ο Κανονισμός GDPR. Για να επιτευχθεί αυτό τα υποκείμενα των δεδομένων θα πρέπει να έχουν την δυνατότητα να ασκούν τα δικαιώματά τους να ενημερώνονται σχετικά την επεξεργασία των δεδομένων που τους αφορούν. Είναι κρίσιμο να εστιάσουν οι πολιτικές των κρατών σε μια υπεύθυνη, διαφανή και αξιόπιστη τεχνητή νοημοσύνη ώστε να μπορούν να εξηγηθούν τα συμπεράσματα, οι αποφάσεις και οι ενέργειες αυτών των συστημάτων. Όσο πλησιάζουμε περισσότερο στην πλήρως αυτόνομη οδήγηση, τα ευφυή συστήματα μεταφορών θα έρχονται ολοένα και περισσότερο αντιμέτωπα με τις παραπάνω προκλήσεις.

6 Βιβλιογραφία

Adavoudi Jolfaei, Amirhosein & Boualouache, Abdelwahab & Rupp, Andy & Schiffner, Stefan & Engel, Thomas. (2023). A Survey on Privacy-Preserving Electronic Toll Collection Schemes for Intelligent Transportation Systems. PP. 1. 10.1109/TITS.2023.3266828.

Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies. doi:10.1002/ett.3677

Ali QE, Ahmad N, Malik AH, Ali G, Rehman WU. Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy. Applied Sciences. 2018; 8(10):1964. https://doi.org/10.3390/app8101964

Arena F, Pau G. An Overview of Vehicular Communications. Future Internet. 2019; 11(2):27. https://doi.org/10.3390/fi11020027

Badu-Marfo, G., Farooq, B., & Patterson, Z. (2019). A Perspective on the Challenges and Opportunities for Privacy-Aware Big Transportation Data. Journal of Big Data Analytics in Transportation. doi:10.1007/s42421-019-00001-z

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for Blockchain: review and challenges. IEEE Access, 1–1. doi:10.1109/access.2019.2950872

Costantini, F., Thomopoulos, N., Steibel, F., Curl, A., Lugano, G., & Kováčiková, T. (2020). Autonomous vehicles in a GDPR era: An international comparison. Advances in Transport Policy and Planning. doi:10.1016/bs.atpp.2020.02.005

de Carvalho RM, Del Prete C, Martin YS, Rivero RMA, Önen M, Schiavo FP, et al. Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. SN Comput Sci 2020;1(4):1–16.

El-Gazzar, Rania & Stendal, Karen. (2020). Examining How GDPR Challenges Emerging Technologies. 10. 237-275. 10.5325/jinfopoli.10.2020.0237.

Fadhil, Mohammed & Ali, Qutaiba. (2023). Advancements in Intelligent Transportation Systems (ITS) and Roadside Unit (RSU) Design: A Comprehensive Review. International Journal of Advanced Natural Sciences and Engineering Researches. 7. 209-221. 10.59287/ijanser.1534.

F. Raviglione, S. Zocca, A. Minetto, M. Malinverno, C. Casetti, C.F. Chiasserini, F. Dovis, From collaborative awareness to collaborative information enhancement in vehicular networks, Vehicular Communications, Volume 36, 2022, 100497, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2022.100497

Fallgren, M., Dillinger, M., Alonso-Zarat, J., Boban, M., Abbas, T., Manolakis, K., … Vilalta, R. (2018). Fifth-Generation Technologies for the Connected Car: Capable Systems for Vehicle-to-Anything Communications. IEEE Vehicular Technology Magazine, 1–1. doi:10.1109/mvt.2018.2848400

Fantin Irudaya Raj, E., Appadurai, M. (2022). Internet of Things-Based Smart Transportation System for Smart Cities. In: Mukherjee, S., Muppalaneni, N.B., Bhattacharya, S., Pradhan, A.K. (eds) Intelligent Systems for Social Good. Advanced

Technologies and Societal Change. Springer, Singapore. https://doi.org/10.1007/978-981-19-0770-8_4

Ferreira A, Muchagata J. Tagubig-taming your big data. In: 2018 international carnahan conference on security technology. IEEE; 2018, p. 1–5.

G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis and S. Shiaeles, "Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 4, pp. 3614-3637, April 2023, doi: 10.1109/TITS.2023.3236274.

Gjermundrød H, Dionysiou I, Costa K. PrivacyTracker: a privacy-by-design GDPR compliant framework with verifiable data traceability controls. In: International conference on web engineering. Springer; 2016, p. 3–15.

Gopalakrishnan, K., Prentkovskis, O., Jackiva, I., & Junevičius, R. (Eds.). (2020). TRANSBALTICA XI: Transportation Science and Technology. Lecture Notes in Intelligent Transportation and Infrastructure. doi:10.1007/978-3-030-38666-5

Gohar A, Nencioni G. The Role of 5G Technologies in a Smart City: The Case for Intelligent Transportation System. Sustainability. 2021 13(9):5188. https://doi.org/10.3390/su13095188

Guevara, L., & Auat Cheein, F. (2020). The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. Sustainability, 12(16), 6469. doi:10.3390/su12166469

Hamideh Taslimasa, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Pulei Xiong, Suprio Ray, Ali A. Ghorbani, Security issues in Internet of Vehicles (IoV): A comprehensive survey, Internet of Things, Volume 22, 2023, 100809, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100809.

Hahn, D. A., Munir, A., & Behzadan, V. (2019). Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. IEEE Intelligent Transportation Systems Magazine, 1–1. doi:10.1109/mits.2019.2898973

Huang Z, Ruj S, Cavenaghi MA, Stojmenovic M, Nayak A. A social net- work approach to trust management in VANETs. Peer-to-Peer Netw Appl 2014;7(3):229–42.

Huimin Chen, Jiajia Liu, Jiadai Wang, Yijie Xun, Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasures, Vehicular Communications, Volume 39, 2023, 100548, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2022.100548.

Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems. doi:10.1016/j.future.2019.07.006

Ildar Begishev, Diana Bersei, Lyudmila Sherbakova, Ruslan Zhirov, Olga Kolesnikova, Problems of legal regulation of unmanned vehicles, Transportation Research Procedia, Volume 63, 2022, Pages 1321-1327, ISSN 2352-1465, https://doi.org/10.1016/j.trpro.2022.06.142.

Ing. Boris Cucor, Outlines of Vehicular Ad-Hoc networks, Transportation Research Procedia, Volume 55, 2021, Pages 1312-1319, ISSN 2352-1465, https://doi.org/10.1016/j.trpro.2021.07.115.

Isaac Oyeyemi Olayode, Bo Du, Alessandro Severino, Tiziana Campisi, Frimpong Justice Alex, Systematic literature review on the applications, impacts, and public perceptions of autonomous vehicles in road transportation system, Journal of Traffic and Transportation Engineering (English Edition), Volume 10, Issue 6, 2023, Pages 1037-1060, ISSN 2095-7564, https://doi.org/10.1016/j.jtte.2023.07.006.

I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3453-3495, 4th Quart., 2018.

J. Petit and S. E. Shladover, Potential cyberattacks on automated vehicles, IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546-556, Apr. 2015.

Jusic, Asim. (2022). Privacy between Regulation and Technology: GDPR and the Blockchain. 1. 47-59.

Jyoti Grover, Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review, Vehicular Communications, Volume 34, 2022, 100458, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2022.100458.

Katrakazas, C., Theofilatos, A., Papastefanatos, G., Härri, J., & Antoniou, C. (2020). Cyber security and its impact on CAV safety: Overview, policy needs and challenges. Advances in Transport Policy and Planning. doi:10.1016/bs.atpp.2020.05.001

L. Liang, H. Ye, and G. Y. Li, Toward intelligent vehicular networks: A machine learning framework," IEEE Internet Things J., vol. 6, no. 1, pp. 124-135, Feb. 2019.

Liang Qiao, Yujie Li, Dongliang Chen, Seiichi Serikawa, Mohsen Guizani, Zhihan Lv, A survey on 5G/6G, AI, and Robotics, Computers and Electrical Engineering, Volume 95, 2021, 107372, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2021.107372.

Lamssaggad, A., Benamar, N., Hafid, A. S., & Msahli, M. (2021). A Survey on the Current Security Landscape of Intelligent Transportation Systems. IEEE Access, 9, 9180–9208. doi:10.1109/access.2021.3050038

Li, Y., Yang, D., & Hu, X. (2020). A differential privacy-based privacy-preserving data publishing algorithm for transit smart card data. Transportation Research Part C: Emerging Technologies, 115, 102634. doi:10.1016/j.trc.2020.102634

Lu, Z., Qu, G., & Liu, Z. (2018). A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. IEEE Transactions on Intelligent Transportation Systems, 1–17. doi:10.1109/tits.2018.2818888

Mouna Rhahla, Sahar Allegue, Takoua Abdellatif, Guidelines for GDPR compliance in Big Data systems, Journal of Information Security and Applications, Volume 61, 2021, 102896, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2021.102896.

Milossi, M., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2021). AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach. IEEE Access, 9, 58455–58466. doi:10.1109/access.2021.3072782

Muthuramalingam, S., Bharathi, A., Rakesh kumar, S., Gayathri, N., Sathiyaraj, R., & Balamurugan, B. (2018). IoT Based Intelligent Transportation System (IoT-ITS) for Global Perspective: A Case Study. Internet of Things and Big Data Analytics for Smart Generation, 279–300. doi:10.1007/978-3-030-04203-5_13

Nikitas, A., Michalakopoulou, K., Njoya, E. T., & Karampatzakis, D. (2020). Artificial Intelligence, Transport and the Smart City: Definitions and Dimensions of a New Mobility Era. Sustainability, 12(7), 2789. doi:10.3390/su12072789

Oladimeji D, Gupta K, Kose NA, Gundogan K, Ge L, Liang F. Smart Transportation: An Overview of Technologies and Applications. Sensors. 2023; 23(8):3880. https://doi.org/10.3390/s23083880

Rantos K, Drosatos G, Demertzis K, Ilioudis C, Papanikolaou A, Kritsas A. ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology. In: International conference on security for information technology and communications. Springer; 2018, p. 300–13.

Rizou, S., Alexandropoulou-Egyptiadou, E., & Psannis, K. E. (2020). GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, 8, 108052–108061. doi:10.1109/access.2020.3000662

Sanjeev Kumar Dwivedi, Ruhul Amin, Ashok Kumar Das, Mark T. Leung, Kim-Kwang Raymond Choo, Satyanarayana Vollala, Blockchain-based vehicular ad-hoc networks: A comprehensive survey, Ad Hoc Networks, Volume 137, 2022, 102980, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2022.102980.

Siwicki, Maciej. (2023). Big Data Profiling and Predictive Analytics from the Perspective of GDPR. Studia Iuridica Lublinensia. 32. 249-266. 10.17951/sil.2023.32.2.249-266.

Sjoberg, K., Andres, P., Buburuzan, T., & Brakemeier, A. (2017). Cooperative Intelligent Transport Systems in Europe: Current Deployment Status and Outlook. IEEE Vehicular Technology Magazine, 12(2), 89–97. doi:10.1109/mvt.2017.2670018

Spalevic, Zaklina & Vićentijević, Kosana. (2022). GDPR and challenges of personal data protection. The European Journal of Applied Economics. 19. 55-65. 10.5937/EJAE19-36596.

Sung, Chun-Hsien & Lu, Ming-Chin. (2023). Protection of personal privacy under the development of the Internet of Things. Wireless Networks. 1-14. 10.1007/s11276-023-03569-1.

Surguli, Mohammed. (2023). How to deal with data privacy requirements in blockchain?.

Talih, Özgür & Çelikok, Kaan. (2023). Intelligent Transportation Systems and Policies in the World and in Türkiye: Assessment from A Sustainable Transportation Perspective Dünyada ve Türkiye'de Akıllı Ulaşım Sistemleri ve Politikaları: Sürdürülebilir Ulaşım Açısından Bir Değerlendirme. Süleyman Demirel Üniversitesi Vizyoner Dergisi. 14. 254-279. 10.21076/vizyoner.1281444.

Tan S, Li X, Dong Q. A trust management system for securing data plane of ad-hoc networks. IEEE Trans Veh Technol 2015;65(9):7579–92.

Telang, S., Chel, A., Nemade, A., Kaushik, G. (2021). Intelligent Transport System for a Smart City. In: Tamane, S.C., Dey, N., Hassanien, AE. (eds) Security and Privacy Applications for Smart City Development. Studies in Systems, Decision and Control, vol 308. Springer, Cham. https://doi.org/10.1007/978-3-030-53149-2_9

Torre-Bastida, A. I., Del Ser, J., Laña, I., Ilardia, M., Bilbao, M. N., & Campos-Cordobés, S. (2018). Big Data for transportation and mobility: recent advances, trends and challenges. IET Intelligent Transport Systems. doi:10.1049/iet-its.2018.5188

Ud Din Arshad, Q. K., Kashif, A. U., & Quershi, I. M. (2019). A Review on the Evolution of Cellular Technologies. 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST). doi:10.1109/ibcast.2019.8667173

Weiping Ding, Mohamed Abdel-Basset, Hossam Hawash, Ahmed M. Ali, Explainability of artificial intelligence methods, applications and challenges: A comprehensive survey, Information Sciences, Volume 615, 2022, Pages 238-292, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2022.10.013.

Xiao Y, Liu Y. BayesTrust and Vehicle Rank: Constructing an implicit Web of trust in VANET. IEEE Trans Veh Technol 2019;68(3):2850–64.

Yue Cao, Sifan Li, Chenchen Lv, Di Wang, Hongjian Sun, Jing Jiang, Fanlin Meng, Lexi Xu, Xinzhou Cheng, Towards cyber security for low-carbon transportation: Overview, challenges and future directions, Renewable and Sustainable Energy Reviews, Volume 183, 2023, 113401, ISSN 1364-0321, https://doi.org/10.1016/j.rser.2023.113401.

Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (Big Data Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.