Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

«Ασφάλεια Ψηφιακών Συστημάτων»

Μεταπτυχιακή Διπλωματική Εργασία με θέμα:

«Ζητήματα ασφάλειας και ιδιωτικότητας σε περιβάλλοντα έξυπνων μεταφορών»

Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης

Στοιχεία φοιτητή

Ανδρέας Μενεγάτος ΜΤΕ 1920

Πειραιάς,
Ιούλιος 2021

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να ευχαριστήσω από καρδιάς τον επιβλέποντα καθηγητή μου κο. Στέφανο Γκρίτζαλη για την αμέριστη βοήθειά του, την άψογη καθοδήγησή του και την υποστήριξή που μου παρείχε κατά τη διάρκεια συγγραφής της παρούσας Διπλωματικής εργασίας. Τις θερμές μου ευχαριστίες θα ήθελα να εκφράσω εξίσου και στα υπόλοιπα δύο μέλη της Τριμελούς Εξεταστικής Επιτροπής καθηγητές κο. Κωνσταντίνο Λαμπρινουδάκη και κο Χρήστο Ξενάκη καθώς και στο λοιπό διδακτικό προσωπικό του ΠΜΣ καθηγήτρια κα. Λίλιαν Μήτρου και επίκουρο καθηγητή κο. Χριστόφορο Νταντογιάν για το σύνολο των πολύτιμων γνώσεων και των υπόλοιπων ανεκτίμητων εφοδίων που προσέφεραν απλόχερα σε εμένα και τους συμφοιτητές μου.

Επιπλέον, θα ήθελα να εκφράσω τη βαθιά μου ευγνωμοσύνη στους γονείς μου και τον αδερφό μου για την στήριξή τους καθ' όλη τη διάρκεια των μεταπτυχιακών μου σπουδών. Τέλος, θα ήθελα να ευχαριστήσω τους συμφοιτητές και τις συμφοιτήτριές μου για το σύνολο των στιγμών που βιώσαμε μαζί αυτό το ενάμισι έτος σπουδών σε αυτές τις πρωτόγνωρες συνθήκες υπό τη σκιά της πανδημίας του κορωνοϊού.

Πίνακας περιεχομένων

ΠΕΡΙΛΗΨΗ

Τα ***Έξυπνα Συστήματα Μεταφορών*** (ITS) αποσκοπούν στην ενίσχυση της αποδοτικότητας των υπαρχόντων συστημάτων μεταφορών μέσω της ενσωμάτωσης ποικίλων τύπων τεχνολογιών (π.χ. συστήματα αισθητήρων, ελέγχου, ανάλυσης και μετάδοσης πληροφοριών) που επιτρέπουν τη βελτίωση της κινητικότητας, τη δραστική μείωση του περιβαλλοντικού αποτυπώματος καθώς και τη μεγιστοποίηση των οφελών προς το επιβατικό κοινό. Η τοπολογία δικτύου στην οποία βασίζονται τα ITS, τα αδόμητα ασύρματα δίκτυα οχημάτων (VANETs), συνιστά ένα εξαιρετικά περίπλοκο, ετερογενές και ευμετάβλητο περιβάλλον το οποίο παρέχει στα οχήματα τη δυνατότητα να επικοινωνούν μεταξύ τους διαμοιραζόμενα πολύτιμες πληροφορίες σχετικά με τις εκάστοτε οδικές και κυκλοφοριακές συνθήκες. Αν και οι δυνατότητες διασύνδεσης που προσφέρουν τα VANETs βελτιώνουν σημαντικά τη συνολική ασφάλεια στον τομέα των καθημερινών μετακινήσεων, η 'ανοιχτή' φύση τους εγείρει πολλαπλά ζητήματα ασφάλειας και ιδιωτικότητας που συσχετίζονται με στόχους όπως η εμπιστευτικότητα, η διαθεσιμότητα, η ακεραιότητα, η αυθεντικοποίηση η μη αποποίηση, η ιδιωτικότητα της τοποθεσίας, η ιδιωτικότητα της ταυτότητας, η ανωνυμία και η μη-συνδεσιμότητα.

Στο πλαίσιο αυτό, καθώς ολοένα και περισσότερα αυτόνομα οχήματα βγαίνουν στο προσκήνιο, ο τομέας των μεταφορών αλλάζει άρδην μορφή. Με την απαίτηση για διασυνδεσιμότητα να αυξάνεται διαρκώς και με δεδομένο ότι τα νέας γενιάς αυτόνομα οχήματα ενσωματώνουν ένα εύρος τεχνικών μηχανικής μάθησης και συστημάτων τεχνητής νοημοσύνης στη λειτουργία τους, εμφανίζεται ένα νέο φάσμα απειλών οι οποίες συχνά εκδηλώνονται με τη μορφή κακόβουλων επιθέσεων. Οι επιθέσεις αυτές μπορεί να επιφέρουν οικονομικές απώλειες, τροχαία ατυχήματα, αποκάλυψη ευαίσθητων και άλλων τύπων προσωπικών δεδομένων, ακόμα και να θέσουν σε κίνδυνο τη ζωή των χρηστών. Επομένως, είναι αναγκαία η εφαρμογή κατάλληλων μέτρων ασφαλείας για τον μετριασμό των επιπτώσεων των κινδύνων, ειδικά καθώς αυτές οι επιθέσεις απειλούν την ασφάλεια, την ασφάλεια και ακόμη και την ιδιωτικότητα των επιβατών οχημάτων και των άλλων χρηστών του δρόμου, μαζί με τους πεζούς.

Στην παρούσα εργασία αρχικά περιγράφουμε με συνοπτικό τρόπο την αρχιτεκτονική των έξυπνων συστημάτων μεταφορών αναφέροντας τα πρότυπα που διέπουν τη λειτουργία τους. Ακολούθως προβαίνουμε σε ενδελεχή ανάλυση των ζητημάτων ασφάλειας και ιδιωτικότητας που ανακύπτουν σε αυτά προτείνοντας συγχρόνως πιθανές τεχνικές-αντίμετρα για τον περιορισμό των διαφόρων τύπων κινδύνων που «γεννώνται» από αυτά. Τέλος, εξετάζουμε ως μελέτη περίπτωσης την χρήση διασυνδεδεμένων οχημάτων αυτοματοποιημένης οδήγησης αξιολογώντας το επίπεδο ασφάλειας και ιδιωτικότητας που παρέχουν.

ABSTRACT

Intelligent transport systems (ITS) encompass several types of sensing, analysis, control, and communications technologies to enhance safety, mobility, comfort, and efficiency of the transportation sector. In detail, various applications are contained which process and share information to alleviate congestion, improve traffic management, reduce the environmental footprint, and maximize the benefits of transportation to commercial users as well as the public in general.

The underlying technology, vehicular ad-hoc networks (VANETs), constitute a highly complex, heterogeneous, and volatile environment that allows vehicles to communicate with each other providing them the opportunity of sharing valuable information regarding the road and traffic conditions to enhance overall safety. Nevertheless, the open nature of ITS induces a vast amount of security and privacy challenges that pertain to security and privacy objectives such as confidentiality, authentication, integrity, non-repudiation, location privacy, identity privacy, anonymity, unlinkability, certificate revocation, and certificate resolution.

The automotive industry undergoes a paradigm shift as connected and autonomous vehicles gradually emerge. With the demand for connectivity in the automotive sector constantly increasing, a vast amount of novel cybersecurity risks and threats arise that need to be managed. In this context, the emergence of semi-autonomous and autonomous cars, which use advanced machine learning and artificial intelligence techniques widens the attack surface. Attacks targeting autonomous cars may result in financial losses, road accidents, disclosure of sensitive and other types of personal data, and even jeopardize road users' safety. Thus, appropriate security measures should be implemented to mitigate the potential risks, especially as these attacks threaten the security, safety and even the privacy of vehicle passengers and the rest of the road users, along with the pedestrians.

In this dissertation we provide a brief description of the architecture of ITS indicating the standards that govern their operation. Afterwards, we conduct a thorough analysis of security and privacy issues that arise in ITS environments proposing efficient countermeasures to mitigate the different types of emerging security and privacy risks. Finally, a case study is entailed referring to the security and privacy challenges linked to the field of interconnected autonomous vehicles.

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

Οι **έξυπνες πόλεις**[1] (smart cities) αποτελούν μια ανερχόμενη τάση στην οποία στρέφεται ένας διαρκώς αυξανόμενος αριθμός πόλεων σε παγκόσμια κλίμακα προκειμένου οι πολίτες τους να δρέψουν τα σημαντικά οφέλη που τους παρέχονται σε κοινωνικό, πολιτισμικό και περιβαλλοντικό επίπεδο. Στο πλαίσιο αυτό, οι τεχνολογίες πληροφορικής και επικοινωνιών (ICT) διαδραματίζουν καταλυτικό ρόλο καθώς με την ανάπτυξη λύσεων λογισμικού υποβοηθούν τις πόλεις στην προσπάθειά τους να γίνουν περισσότερο αποδοτικές μέσω της αυτοματοποίησης των διεργασιών τους. Οι δύο (2) βασικότεροι παράγοντες που συμβάλλουν καθοριστικά στην επίτευξη αυτού του στόχου είναι αφενός οι διατεθείσες τεχνολογικές λύσεις και αφετέρου οι ίδιοι οι πολίτες. Η αρμονική συνύπαρξη και αλληλεπίδραση αυτών των δύο παραγόντων προσδίδει αναρίθμητα πλεονεκτήματα στους πολίτες των πόλεων βελτιστοποιώντας τη διαδικασία χρήσης των πόρων (resource optimization). Η *βιώσιμη αστική κινητικότητα* (smart urban mobility) αποτελεί μια πτυχή των έξυπνων πόλεων η οποία βασίζεται στην ενσωμάτωση έξυπνων συστημάτων μεταφορών (ITS) για τον περιορισμό των επιπέδων ρύπανσης, τη μείωση των φαινομένων κυκλοφοριακής συμφόρησης και την προστασία της ζωής των πεζών και των οδηγών. Η σημασιολογική αναπαράσταση του όρου 'έξυπνο' που χρησιμοποιείται ως προσδιορισμός των συστημάτων μεταφορών συνίσταται στην ενσωμάτωση κάθε τεχνολογικής καινοτομίας που αλλάζει ριζικά την μέχρι πρότινος 'φύση' των μέσων μεταφοράς (από βενζινοκίνητα και πετρελαιοκίνητα οχήματα σε οικολογικά, από την αποκλειστική κατοχή στον διαμοιρασμό οχημάτων) καθιστώντας τα περισσότερο βιώσιμα. Η βιωσιμότητα οδηγεί με τη σειρά της σε αύξηση της αποδοτικότητας του συστήματος μεταφορών των αστικών ιστών. Δεδομένου ότι η συγκεκριμένη διαδικασία συσχετίζεται de facto με ανθρώπινες υπάρξεις – εν προκειμένω πολίτες - η ενεργή εμπλοκή των τελευταίων αποτελεί προαπαιτούμενο για την ορθή εφαρμογή βιώσιμων λύσεων που θα συμβάλλουν στη βελτίωση των συνθηκών διαβίωσής τους. Κατ' αυτόν τον τρόπο το Διαδίκτυο των πραγμάτων (IoT) και το Διαδίκτυο των οχημάτων (IoV) πρόκειται να διαδραματίσουν κυρίαρχο ρόλο στην εξέλιξη του πεδίου της βιώσιμης κινητικότητας, με τις απαιτήσεις της ασφάλειας και της ιδιωτικότητας να αποτελούν παραμέτρους μείζονος σημασίας που πρέπει να ληφθούν υπόψη κατά τη διαδικασία διασύνδεσης των αντικειμένων.

Τα **Έξυπνα Συστήματα Μεταφορών** μεταβάλλουν τον τρόπο λειτουργίας των παραδοσιακών συστημάτων μεταφορών δημιουργώντας μια αποτελεσματικότερη, ασφαλέστερη και πιο ευχάριστη εμπειρία για το σύνολο του επιβατικού κοινού που τα χρησιμοποιεί. Για το λόγο αυτό, ένας διαρκώς αυξανόμενος αριθμός ιδιωτικών και δημόσιων φορέων πόλεων αναλαμβάνουν πρωτοβουλίες για την ανάπτυξη και

[1] Σύμφωνα με τους (Caragliu, Del Bo, & Nijkamp, 2011) «*μια πόλη χαρακτηρίζεται ως έξυπνη όταν οι επενδύσεις σε ανθρώπινο και κοινωνικό κεφάλαιο καθώς και σε παραδοσιακές (συστήματα μεταφορών) και σύγχρονες (ICT) ψηφιακές υποδομές επικοινωνίας εντείνουν τη βιώσιμη οικονομική ανάπτυξη και παρέχουν μια υψηλή ποιότητα ζωής στους κατοικούντες σε αυτή, με μια συνετή διαχείριση των φυσικών πόρων, μέσω συμμετοχικής διακυβέρνησης*».

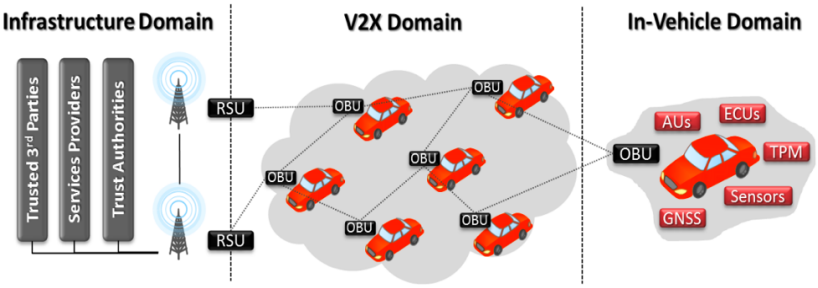
υποστήριξη των συστημάτων αυτών (IBM, 2017). Με τους αλγορίθμους πρόβλεψης κυκλοφοριακών συνθηκών (*prediction traffic algorithms*) να ενσωματώνουν διαρκώς στη λειτουργία τους μεθόδους που προάγουν το στοιχείο της καινοτομίας, καθώς επίσης και με την εισαγωγή αυτόνομων και ημιαυτόνομων οχημάτων για τη βελτίωση των συνθηκών ασφάλειας στο κυκλοφοριακό τοπίο, είναι εμφανές ότι το πεδίο των μεταφορών αναμένεται να αλλάξει άρδην εικόνα. Εκτός των ανωτέρω, υφίσταται ραγδαία ανάπτυξη και στα συστήματα πληροφόρησης και διασκέδασης (*infotainment systems*) των οχημάτων με την διαρκή ενσωμάτωση και εξέλιξη νέων τεχνολογικών εφαρμογών όπως συστήματα πλοήγησης, συσκευές που παρέχουν δυνατότητα διασύνδεσης μέσω Bluetooth, εφαρμογών σύνταξης και αποστολής μηνυμάτων κειμένων (SMS, e-mails) καθώς και εφαρμογών που επιτρέπουν τη διενέργεια τηλεφωνικών κλήσεων. Η ενσωμάτωση τεχνολογικών εφαρμογών στα συστήματα μεταφορών προσδίδει σε αυτά νέα χαρακτηριστικά που βελτιώνουν τόσο την εκτέλεση εργασιών σε ένα περιβάλλον το οποίο χαρακτηρίζεται από διαρκή κινητικότητα, όσο και τη διαδικασία μετακινήσεων αυτή καθαυτή, με την προσθήκη των χαρακτηριστικών της άνεσης και της κάλυψης μεγαλύτερων αποστάσεων. Ωστόσο, η εν λόγω ανάπτυξη έχει και το «κόστος» της. Συγκεκριμένα, δεδομένου ότι η ικανοποίηση της απαίτησης της διασυνδεσιμότητας στα ITS προϋποθέτει την ενσωμάτωση πλήθους κινητών συσκευών και εφαρμογών, η πιθανότητα εισαγωγής στο σύστημα συσκευών οι οποίες δεν διαθέτουν ένα επαρκές επίπεδο ασφάλειας αυξάνεται. Επομένως, παρέχεται η δυνατότητα σε κακόβουλους χρήστες- «επιτιθέμενους» να θέσουν σε κίνδυνο κρίσιμες παραμέτρους ενός συστήματος μεταφορών προξενώντας σοβαρές βλάβες στη λειτουργία του όπως για παράδειγμα καταστροφές στην υποδομή, καθυστερήσεις σε αποστολές οχημάτων έκτακτης ανάγκης ή αποκάλυψη δεδομένων προσωπικού χαρακτήρα. Εξαιτίας της αυξημένης πιθανότητας εκδήλωσης κινδύνων ασφάλειας και ιδιωτικότητας στο περιβάλλον των μεταφορών, έχει αναπτυχθεί μια πλειάδα μεθοδολογιών ανάλυσης και διαχείρισης κινδύνων προκειμένου να καθίσταται δυνατή η έγκαιρη αποτίμηση των επιπτώσεων των κινδύνων και να σχεδιάζονται και να υλοποιούνται τα απαιτούμενα μέτρα ασφάλειας το συντομότερο δυνατόν. Ωστόσο, πολλά από τα μοντέλα αυτά εξακολουθούν μέχρι και σήμερα να παρουσιάζουν σοβαρές αδυναμίες και έτσι απαιτούν ενδελεχή διερεύνηση πριν την εφαρμογή τους. Συνεπώς, καθίσταται αναγκαία η δημιουργία ενός ολιστικού πλαισίου ασφάλειας και ιδιωτικότητας για περιβάλλοντα έξυπνων μεταφορών προκειμένου να διασφαλιστούν η ασφάλεια και η ιδιωτικότητα των επιβατών σε παγκόσμια κλίμακα.

2. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ITS ΚΑΙ ΣΥΝΑΦΕΙΣ ΕΦΑΡΜΟΓΕΣ

Καθώς η τεχνολογία στα πεδία των κινητών και ασύρματων επικοινωνιών και στα συστήματα απομακρυσμένης παρακολούθησης μέσω αισθητήρων εξελίσσεται, τα έξυπνα συστήματα μεταφορών αποτελούν μια ανερχόμενη τεχνολογία η οποία θα επιτρέψει την ανάπτυξη ποικίλων εφαρμογών σχετικές με την οδική ασφάλεια και τη διαχείριση κυκλοφορίας. Σε αυτήν την ενότητα παρέχουμε μια υψηλού επιπέδου αρχιτεκτονική για τα ITS, εστιάζοντας στα χαρακτηριστικά τους, τα ζητήματα ασφάλειας και ιδιωτικότητας που ανακύπτουν σε αυτά καθώς και εφαρμογές που ανήκουν στο συγκεκριμένο πεδίο.

2.1. Μοντέλο αρχιτεκτονικής έξυπνων συστημάτων μεταφορών

Αν επιχειρήσουμε να προβούμε σε μια υψηλού επιπέδου περιγραφή του βασικού μοντέλου αρχιτεκτονικής των ITS, θα διακρίναμε τρία (3) βασικά πεδία (Εικόνα 1): το πεδίο εντός του οχήματος (in-vehicle domain), το πεδίο επικοινωνίας με τα υπόλοιπα οχήματα (V2X domain) και τέλος το πεδίο επικοινωνίας με την υποδομή του δικτύου (infrastructure domain).

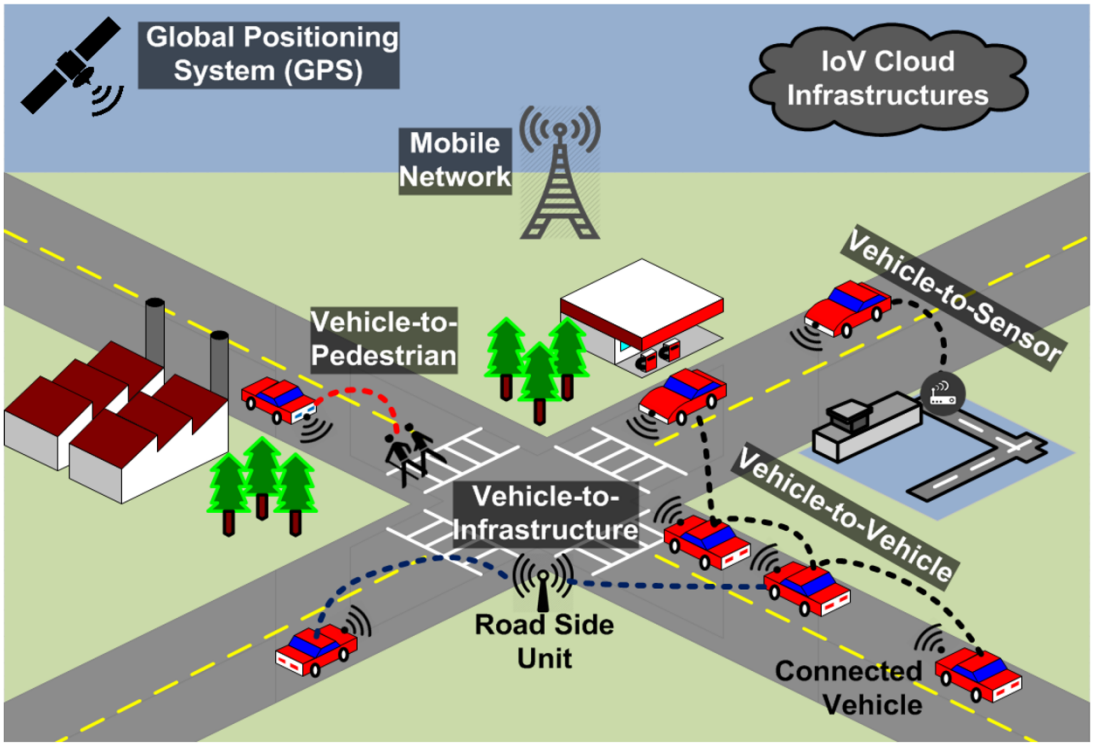


***Εικόνα 1**: Σχηματική αναπαράσταση ενός ITS σε υψηλό επίπεδο (Hamida, Noura, & Znaidi, 2015)*

Το πεδίο εντός του οχήματος συντίθεται από ένα όχημα το οποίο είναι εξοπλισμένο με ηλεκτρονικές μονάδες ελέγχου (**ECUs**), εποχούμενες στο όχημα μονάδες επεξεργασίας (**OBUs**), μια μονάδα αξιόπιστης πλατφόρμας (**TPM**) και μια μονάδα εφαρμογής (**AU**). Οι ECUs συλλέγουν δεδομένα σχετικά με τη κίνηση του οχήματος (π.χ. δεδομένα τοποθεσίας, ταχύτητας, διαστάσεις αυτοκινήτου, σειριακός αριθμός οχήματος), το περιβάλλον με το οποίο το όχημα βρίσκεται σε αλληλεπίδραση (π.χ αριθμός γειτονικών οχημάτων, κυκλοφοριακές συνθήκες) και ελέγχου της λειτουργικότητάς του. Η επικοινωνία των ECUs επιτυγχάνεται με την ανταλλαγή δεδομένων μέσω των OBUs και των AUs συνθέτοντας με αυτόν τον τρόπο ένα δίκτυο εντός του χώρου του οχήματος το οποίο στην ξενόγλωσση βιβλιογραφία συναντάται ως "*on-board network*". Η AU είναι υπεύθυνη για την εκτέλεση μιας ή περισσότερων εφαρμογών οι οποίες προσφέρονται από παρόχους απομακρυσμένων υπηρεσιών (**RSPs**) και επικοινωνεί με άλλες γειτονικές οντότητες του ITS χρησιμοποιώντας της δυνατότητες επικοινωνίας που παρέχει η OBU. Κάθε διασυνδεδεμένο όχημα

εξοπλίζεται επίσης με ένα TPM προκειμένου η επικοινωνία να καταστεί ασφαλής και αποτελεσματική περιλαμβάνοντας ένα σύνολο μηχανισμών ασφαλείας απαραίτητων για την προφύλαξη του πλήθους των διαφορετικών κλειδιών κρυπτογράφησης που απαιτούνται για τη διασφάλιση της απαίτησης της εμπιστευτικότητας και των πιστοποιητικών που χρησιμοποιούνται για σκοπούς αυθεντικοποίησης. Τέλος, χρησιμοποιούνται συστήματα δορυφορικού γεωεοντοπισμού για την παροχή δεδομένων τοποθεσίας υψηλής ακρίβειας.

Ο τύπος επικοινωνιών V2X (ή τομέας ad hoc) αποτελείται από τις OBUs κάθε οχήματος και τις μονάδες επικοινωνίας που βρίσκονται παραπλεύρως των δρόμων κυκλοφορίας (RSUs). Όπως φαίνεται στην Εικόνα 2, οι πληροφορίες που συλλέγονται στις OBUs των οχημάτων, ανταλλάσσονται σε πραγματικό χρόνο με τις υπόλοιπες γειτονικές ενσωματωμένες μονάδες επεξεργασίας και τις RSUs χρησιμοποιώντας ποικίλες τεχνολογίες επικοινωνίας οχημάτων (V2X), μεταξύ των οποίων είναι οι εξής: (i) επικοινωνίες από όχημα-σε-όχημα που αναπτύσσονται μεταξύ γειτονικών οχημάτων (ή OBUs) χρησιμοποιώντας τεχνολογίες επικοινωνιών μικρής εμβέλειας (DSRC) (ii) επικοινωνίες οχήματος-προς-υποδομή (V2I) που αναπτύσσονται μεταξύ των παρακείμενων OBUs και RSUs και αντίστροφα και (iii) επικοινωνία οχήματος με πεζούς (V2P) που αναπτύσσονται μεταξύ των OBUs / RSUs και των διερχόμενων πεζών.



***Εικόνα 2**: V2X τύποι επικοινωνιών (Hamida, Noura, & Znaidi, 2015)*

2.2. Χαρακτηριστικά στοιχεία των ITS

Παρόλο που τα ITS αναμένεται να αποτελέσουν κυρίαρχη τεχνολογία στο άμεσο μέλλον, εξακολουθούν να υφίστανται πολλαπλά ζητήματα ασφάλειας τα οποία θα πρέπει να διευθετηθούν προκειμένου να αναπτυχθούν αποτελεσματικά και πάνω απ' όλα ασφαλή ITS. Ειδικότερα, ήδη από την φάση του σχεδιασμού, θα πρέπει να ληφθούν υπόψη διάφορα χαρακτηριστικά στοιχεία των ITS όπως είναι τα εξής:

- **Υψηλές επιδόσεις:** Οι σταθμοί ITS (δηλαδή οι RSUs και οι OBUs) παρουσιάζουν υψηλά επίπεδα ισχύος σε θέματα παροχής υπηρεσιών εντοπισμού θέσης, αποθήκευσης και ρυθμού μετάδοσης δεδομένων.

- **Υψηλή κινητικότητα:** Τα ITS περιλαμβάνουν έναν τεράστιο αριθμό από κόμβους που μετακινούνται διαρκώς, με διαφορετικές ταχύτητες και σε διαφορετικές κατευθύνσεις, καθιστώντας έτσι την πρόβλεψη της θέσης του εκάστοτε κόμβου εξαιρετικά δύσκολη υπόθεση.

- **Υψηλή μεταβλητότητα στην τοπολογία του δικτύου:** Ανάλογα με τις θέσεις τους και τις ταχύτητές τους, οι σταθμοί των ITS μπορούν να ενταχθούν στο δίκτυο ή να το εγκαταλείψουν σε εξαιρετικά μικρό χρονικό διάστημα. Η προκύπτουσα τοπολογία δικτύου παρουσιάζει επομένως υψηλή μεταβλητότητα.

- **«Ευαισθησία» ως προς τον χρόνο:** Οι πληροφορίες ασφαλείας πρέπει να παραδίδονται στους κόμβους των ITS σε πολύ μικρό χρονικό διάστημα καθιστώντας έτσι την καθυστέρηση έναν από τους πιο σημαντικούς περιορισμούς ποιότητας υπηρεσίας (QoS) για αυτά τα είδη δικτύων.

- **Επαρκής ενέργεια:** Σε αντίθεση με τα ασύρματα δίκτυα αισθητήρων (WSN), όπου οι κόμβοι διαθέτουν περιορισμένους πόρους και μικρή διάρκεια ζωής μπαταρίας, οι οντότητες των ITS θεωρούνται συσκευές 'πλούσιες' σε πόρους (πχ αποθηκευτικός χώρος, υπολογιστική ισχύς). Το γεγονός αυτό επιτρέπει την εφαρμογή σύνθετων αλγορίθμων για την επίτευξη υψηλότερης απόδοσης σε περιβάλλοντα έξυπνων οχημάτων (Cheng, Shan, & Zhuang, 2011).

- **Καλό επίπεδο φυσικής προστασίας:** Κάθε οντότητα ενός ITS, διαθέτει μεθόδους για να διασφαλίσει την προστασία της σε φυσικό επίπεδο.

- **Χωρίς περιορισμό στο μεγέθος δικτύου:** Τα ITS μπορούν να χρησιμοποιηθούν εξίσου αποτελεσματικά τόσο σε γεωγραφικές περιοχές μικρής έκτασης όσο και σε αστικούς ιστούς ή ακόμα και σε διακρατικό επίπεδο.

- **Ασύρματες επικοινωνίες:** Οι οντότητες των ITS επικοινωνούν μεταξύ τους ανταλλάσσοντας πληροφορίες μέσω ασύρματων ζεύξεων. Ως εκ τούτου, συγκεκριμένα μέτρα ασφαλείας και πρωτόκολλα πρέπει να χρησιμοποιηθούν προκειμένου να διασφαλιστεί η ασφάλεια της επικοινωνίας.

- **Ετερογενείς τεχνολογίες επικοινωνίας V2X:** Τα οχήματα εκμεταλλεύονται διαφορετικούς τύπους τρόπων επικοινωνίας, όπως V2V, point-to-point V2I, V2I μικρής / μεγάλης εμβέλειας κ.λπ. Επιπλέον, τα συνδεδεμένα οχήματα υποστηρίζουν ένα ευρύ φάσμα τεχνολογιών επικοινωνίας, όπως IEEE 802.11p, Wi-Fi, Bluetooth, 5G / LTE κλπ.

- **Ετερογενή περιβάλλοντα:** Τα οχήματα λειτουργούν σε διάφορα περιβάλλοντα χαμηλής και υψηλής πυκνότητας δικτύου.

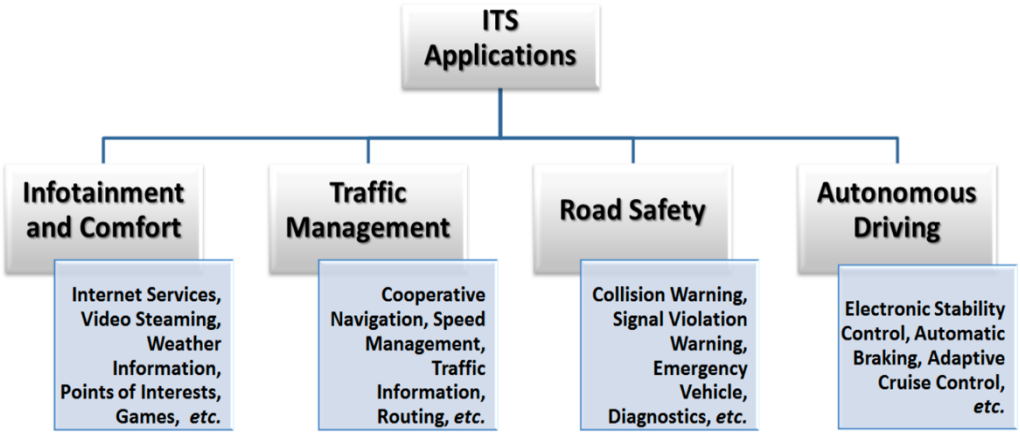
- **Ασφάλεια και ιδιωτικότητα:** Η ασφάλεια και η ιδιωτικότητα αποτελούν απαιτήσεις ύψιστης σημασίας στα ITS. Στα περισσότερα σενάρια, οι εισβολείς στοχεύουν τις διαδικασίες αυθεντικοποίησης, τους μηχανισμούς ακεραιότητας και τη διαθεσιμότητα του δικτύου. Σε αυτό το πλαίσιο, τα πρωτόκολλα ασφαλείας που εφαρμόζονται πρέπει να επιβαρύνουν όσο το δυνατόν λιγότερο την εκτέλεση των διαδικασιών επικοινωνίας που λαμβάνουν χώρα σε ένα ITS λόγω των χρονικών περιορισμών που τίθενται για την ανταλλαγή γρήγορων και ασφαλών πληροφοριών.

Παρατηρώντας με προσοχή τα παραπάνω χαρακτηριστικά διακρίνουμε ότι ορισμένες από τις προκλήσεις που έχουμε να αντιμετωπίσουμε στα ITS είναι αντιφατικές μεταξύ τους. Για παράδειγμα, ενώ οι επικοινωνίες στα δίκτυα οχημάτων πρέπει να είναι όσο το δυνατόν περισσότερο αποδοτικές ως προς τον χρόνο, οι επιπρόσθετες πράξεις επεξεργασίας και οι πολλαπλές κεφαλίδες που ενθυλακώνονται στα μηνύματα που ανταλλάσσονται και είναι απαραίτητες για να διασφαλίσουν την ασφάλεια και την ιδιωτικότητα των επικοινωνιών αυτών επιβαρύνουν το δίκτυο. Συμπερασματικά, είναι απαραίτητο να επιτευχθεί η βέλτιστη ισορροπία ανάμεσα σε αυτές τις αντικρουόμενες απαιτήσεις ώστε να πληρούνται τα κριτήρια QoS που αφορούν την ασφάλεια του δικτύου των ITS.

2.3. Εφαρμογές ITS

Οι εφαρμογές ITS εκμεταλλεύονται δεδομένα που συλλέγονται από οχήματα για τη βελτίωση της λειτουργίας των οχημάτων, την τόνωση του αισθήματος ασφάλειας και άνεσης των οδηγών καθώς και για τον εξορθολογισμό της χρήσης δημόσιων υποδομών. Όπως φαίνεται στην Εικόνα 3, οι εφαρμογές ITS μπορούν να κατηγοριοποιηθούν σε τέσσερις κύριες κατηγορίες: (i) ψυχαγωγίας και άνεσης (ii) διαχείρισης της κυκλοφορίας (iii) οδικής ασφάλειας και (iv) εφαρμογές που χρησιμοποιούνται για την οδήγηση αυτόνομων οχημάτων. Το υπόλοιπο αυτής της ενότητας παρέχει μια υψηλού επιπέδου περιγραφή των τριών κατηγοριών εφαρμογών

ITS σε υψηλό επίπεδο. Η τελευταία κατηγορία εξετάζεται ενδελεχώς στη μελέτη περίπτωσης που παραθέτουμε στο Κεφάλαιο 5.

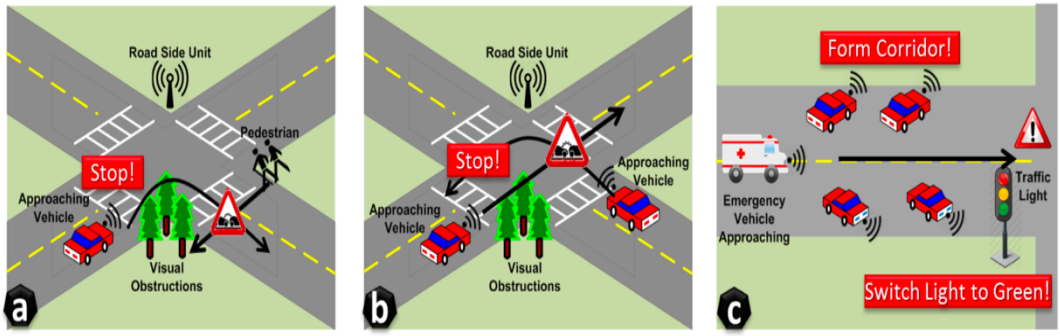


Εικόνα 3: *Κατηγοριοποίηση εφαρμογών που χρησιμοποιούνται στα ITS (Hamida, Noura, & Znaidi, 2015)*

2.3.1. Εφαρμογές διασφάλισης ασφάλειας στο οδικό δίκτυο

Οι εφαρμογές που χρησιμοποιούνται για σκοπούς οδικής ασφάλειας χρησιμοποιούν ασύρματες επικοινωνίες V2X που αναπτύσσονται μεταξύ γειτονικών οντοτήτων που συνθέτουν ένα οικοσύστημα ITS (π.χ. οχήματα, οδικές υποδομές κ.λπ.) στοχεύοντας στη μείωση των τροχαίων ατυχημάτων και στην προστασία των οδηγών και των πεζών από ποικίλους κινδύνους που ταλανίζουν ένα οδικό δίκτυο. Για το σκοπό αυτό, κάθε οντότητα ITS μεταδίδει περιοδικά μηνύματα ασφαλείας παρέχοντας στις γειτνιάζουσες οντότητές της πληροφορίες σχετικά με τις συνθήκες του περιβάλλοντος στο οποίο βρίσκεται καθώς και δεδομένα θέσης. Επιπλέον, κάθε οντότητα ITS μπορεί, παρουσία συγκεκριμένων συμβάντων έκτακτης ανάγκης (π.χ. ατυχήματα, δεδομένα που υποδηλώνουν κακή κατάσταση του οδικού δικτύου), να μεταδώσει μηνύματα γνωστοποίησης της θέσης της σε κοντινά της οχήματα χρησιμοποιώντας επικοινωνίες πολλαπλών αναπηδήσεων (multi-hop). Θα πρέπει να σημειωθεί ότι η κρίσιμη καθυστέρηση (ή καθυστέρηση επικοινωνίας από άκρο σε άκρο) αντιπροσωπεύει μία από τις κρισιμότερες παραμέτρους που λαμβάνονται υπόψη κατά το σχεδιασμό των εφαρμογών οδικής ασφάλειας. Συνήθως, η καθυστέρηση αυτή δεν πρέπει να υπερβαίνει τα εκατό χιλιοστά του δευτερολέπτου (100ms) .

Τρία (3) τυπικά παραδείγματα ανακυπτουσών εφαρμογών οδικής ασφάλειας ITS αποτυπώνονται στην παρακάτω εικόνα:



***Εικόνα 4**: Παραδείγματα εφαρμογών οδικής ασφάλειας: (a) Σύστημα προειδοποίησης διέλευσης πεζών; (b) left turn driver assistance και (c) καταφθάνον όχημα έκτακτης ανάγκης (Hamida, Noura, & Znaidi, 2015)*

Το πρώτο παράδειγμα αναφέρεται στις εφαρμογές ειδοποίησης των οδηγών σε περιπτώσεις διέλευσης πεζών (Εικόνα 4α). Προκειμένου να καθίσταται δυνατή η αναγνώριση ανθρώπινης παρουσίας οι αισθητήρες τοποθετούνται κατά μήκος των πεζοδρομίων και τα ληφθέντα αισθητηριακά δεδομένα συλλέγονται και υπόκεινται σε επεξεργασία από τις ηλεκτρονικές μονάδες που βρίσκονται παρακείμενες στο δρόμο (RSUs). Με αυτόν τον τρόπο, οι RSUs δύνανται να ανιχνεύσουν ή /και να προβλέψουν την πιθανότητα ατυχημάτων και να ειδοποιήσουν τα διερχόμενα οχήματα.

Το δεύτερο παράδειγμα αποτελούν οι εφαρμογές υποβοήθησης των οδηγών σε περιπτώσεις διασταυρώσεων, όπως φαίνεται στην Εικόνα 4β. Σε αυτό το σενάριο, δύο οχήματα ενδέχεται να πλησιάσουν μια διασταύρωση χωρίς να αντιλαμβάνεται το ένα την παρουσία του άλλου λόγω της ύπαρξης οπτικών εμποδίων (π.χ. παρουσία δέντρων, κτιρίων κλπ). Συνεπώς, ο στόχος μιας τέτοιας εφαρμογής είναι να βοηθήσει τους οδηγούς των οχημάτων να διασχίσουν με ασφάλεια τις διασταυρώσεις ακόμα και στις πιο σύνθετες περιπτώσεις που τα οχήματά τους πρόκειται να πραγματοποιήσουν αριστερόστροφη ή δεξιόστροφη κίνηση. Για το σκοπό αυτό, οι RSUs συλλέγουν πληροφορίες από τις OBUs των οχημάτων ή/και από τους προηγμένους αισθητήρες που βρίσκονται κατά μήκος του αυτοκινητόδρομου ούτως ώστε να ανιχνεύσουν την εμφάνιση ενός τέτοιου συμβάντος και να παράσχουν εγκαίρως τις απαιτούμενες συστάσεις στους εμπλεκόμενους οδηγούς.

Τέλος, ως τρίτη περίπτωση, υπάρχουν οι εφαρμογές προειδοποίησης για διέλευση οχημάτων έκτακτης ανάγκης, όπως φαίνεται στην Εικόνα 4γ, στις οποίες ένα καταφθάνον όχημα έκτακτης ανάγκης (π.χ. ασθενοφόρο, περιπολικό ή πυροσβεστικό όχημα) ζητά -με την αποστολή κατάλληλων μηνυμάτων ασφάλειας (safety messages)- από τα γειτονικά του οχήματα να σχηματίσουν ένα ‘διάδρομο’ (corridor) ώστε να περάσει από εκεί για να επιτελέσει γρηγορότερα την αποστολή του. Το όχημα έκτακτης ανάγκης έχει επιπλέον τη δυνατότητα να επικοινωνήσει με τις παρακείμενες ηλεκτρονικές μονάδες του οδικού δικτύου (RSUs) ώστε να θέσει τη λειτουργία των φαναριών σε πράσινο, ελαχιστοποιώντας έτσι ακόμα περισσότερο τον χρόνο απόκρισης σε συμβάντα έκτακτης ανάγκης.

Άλλα παραδείγματα εφαρμογών οδικής ασφάλειας περιλαμβάνουν τη χρήση ηλεκτρονικών φώτων για πεδήσεις έκτακτης ανάγκης, ενδείξεις παρουσίας στατικού οχήματος, προειδοποιήσεις για εκτέλεση οδικών έργων, εφαρμογές αποφυγής συγκρούσεων σε διασταυρώσεις και συστήματα προειδοποίησης αλλαγής λωρίδας.

2.3.2. Εφαρμογές διαχείρισης κυκλοφορίας (Traffic Management Applications)

Οι εφαρμογές που έχουν ως κύρια λειτουργία τη διαχείριση της κυκλοφορίας σε ένα οδικό δίκτυο αντιπροσωπεύουν μια δεύτερη μεγάλη κατηγορία εφαρμογών σε περιβάλλοντα ITS, αποσκοπώντας στη βελτίωση της διαδικασίας διαχείρισης και συντονισμού των ροών κυκλοφορίας και στην παροχή υπηρεσιών πλοήγησης συνεργατικής φύσεως (*cooperation navigation services*) στους οδηγούς. Αυτές οι εφαρμογές βασίζονται στη συλλογή και ανάλυση των ανταλλασσόμενων μηνυμάτων μεταξύ των οντοτήτων που συμμετέχουν σε ένα ITS προκειμένου να δημιουργηθούν βάσεις δεδομένων με δεδομένα κίνησης σε μορφή χαρτών. Τα δεδομένα κίνησης συλλέγονται γενικά από τις RSUs ή/και από διαφόρων τύπων αισθητήρες που βρίσκονται κατά μήκος των δρόμων και μεταδίδονται ασύρματα σε απομακρυσμένα κέντρα δεδομένων (*remote trusted data centers*) για περαιτέρω ανάλυση και επεξεργασία δεδομένων. Τα δεδομένα που συλλέγονται περιλαμβάνουν πληροφορίες σχετικές με το περιβάλλον και δεδομένα τοποθεσίας που σχετίζονται με τα οχήματα, τους οδηγούς και οδικά συμβάντα. Αφού τα συλλεχθέντα δεδομένα υποβληθούν σε επεξεργασία και μετασχηματιστούν σε σημαντικές πληροφορίες, παραδίδονται στους οδηγούς μέσω παρόχων υπηρεσιών (*service providers*) προσφέροντάς τους χρήσιμες ενημερώσεις για τρέχουσες και προβλεπόμενες περιοχές με συμφόρηση, προτεινόμενα δρομολόγια, οδηγίες πλοήγησης, ειδοποιήσεις ορίου ταχύτητας κλπ. Επιπροσθέτως, οι συγκεκριμένες εφαρμογές διαχείρισης της κίνησης μπορούν -υπό προϋποθέσεις- να επιτρέψουν στις αρχές να πραγματοποιήσουν προηγμένη χωροχρονική ανάλυση δεδομένων κίνησης, δημιουργώντας για παράδειγμα έναν πίνακα αφετηριών-προορισμών (O-D matrix) των διερχόμενων οχημάτων. Ο πίνακας αυτός διατηρεί αποθηκευμένα γεωγραφικά δεδομένα με στοιχεία αφετηρίας-προορισμού ταξιδιών στοχεύοντας στην εκτίμηση του όγκου κυκλοφορίας μεταξύ διαφορετικών τοποθεσιών αφετηριών και προορισμών (π.χ. συνοικίες, πόλεις κλπ.) προκειμένου να βελτιστοποιηθεί η χρήση και ο σχεδιασμός μελλοντικών οδικών και κτιριακών υποδομών. Είναι προφανές ωστόσο ότι μια τέτοια δομή δεδομένων θα πρέπει να υπόκειται σε όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα ασφάλειας για την προστασία των δεδομένων που διατηρούνται σε αυτήν, διαφορετικά εγείρονται σοβαρά ζητήματα ιδιωτικότητας.

Όπως φαίνεται στον Πίνακα 1, οι εφαρμογές αυτού του είδους βασίζονται στην μετάδοση μηνυμάτων ασφαλείας και V2X επικοινωνιών ανά τακτά χρονικά διαστήματα, των οποίων η κρίσιμη καθυστέρηση δεν πρέπει συνήθως να υπερβαίνει τα διακόσια χιλιοστά του δευτερολέπτου (200 ms). Άλλα παραδείγματα εφαρμογών διαχείρισης της κυκλοφορίας περιλαμβάνουν: ειδοποιήσεις ορίου ταχύτητας βάσει των τοπικών κανονιστικών ρυθμίσεων, προτεινόμενη ταχύτητα εναλλαγής πράσινου

φωτός, ηλεκτρονική συλλογή διοδίων και διαχείριση οχημάτων που κινούνται σε αυτοκινητοδρόμους.

***Πίνακας 1**: Τεχνικά χαρακτηριστικά εφαρμογών ITS. (Hamida, Noura, & Znaidi, 2015)*

Applications	Use Cases	Communication Modes	Radio Coverage	TX Frequency	Critical Latency
Active road safety	Intersection collision warning, Lane change assistance, etc.	Broadcasting , Cooperative messaging, etc.	From 300m to 20Km	10Hz	$\leq$ 100ms
Traffic Efficiency and Management	Regulatory speed limit notification	Periodic / permanent message broadcast	From 300m to 5Km	1-10Hz	-
	Green light optimal speed advisory			10Hz	$\leq$ 100ms
Cooperative Navigation	Electronic toll collection	Internet vehicle and unicast full duplex session	From 0m to 1Km	1Hz	$\leq 200ms$
	Adaptive cruise control, Vehicle highway automatic system	Cooperation awareness		2Hz	$\leq 100ms$
Global Internet Services	Insurance and financial services, Fleet management, etc.	Access to Internet	From 0m to full range	1Hz	$\leq 500ms$
Cooperative Local Services	Point of interest notifications	Periodic / permanent message broadcast	From 0m to full range	1Hz	$\leq 500ms$
	Electronic commerce	Full duplex communications			
	Media downloading	Access to Internet			

2.3.3. Infotainment and Comfort Applications

Οι εφαρμογές ψυχαγωγίας και διασκέδασης (*infotainment and comfort applications*) στοχεύουν στην ενίσχυση της οδηγικής εμπειρίας παρέχοντας στους οδηγούς διάφορες υπηρεσίες προστιθέμενης αξίας. Αυτές οι υπηρεσίες προσφέρονται γενικά από αξιόπιστους παρόχους υπηρεσιών, όπου οι αντίστοιχες εφαρμογές και υπηρεσίες λαμβάνονται και εγκαθίστανται στις application units (AUs). Οι AUs επικοινωνούν με τα απομακρυσμένα κέντρα δεδομένων των παρόχων υπηρεσιών μέσω των OBU τους, χρησιμοποιώντας διαφορετικά είδη πρωτοκόλλων επικοινωνίας τύπου V2I (π.χ. 4G /LTE, 5G). Ένα τυπικό παράδειγμα τέτοιου τύπου επικοινωνίας αποτελούν οι εφαρμογές απομακρυσμένου διαγνωστικού ελέγχου και συντήρησης οχήματος στην οποία οι πάροχοι υπηρεσιών συλλέγουν, κατά την κίνηση του οχήματος (‘on-the-fly’), πληροφορίες από τους αισθητήρες που βρίσκονται εντός του οχήματος και αποστέλλουν στους οδηγούς πληροφορίες σχετικά με ανιχνευθέντα ζητήματα ασφαλείας καθώς και για να τους υπενθυμίσουν προγραμματισμένες συντηρήσεις του αυτοκινήτου. Ένα άλλο παράδειγμα που ανήκει σε αυτήν την κατηγορία είναι η παροχή στους επιβαίνοντες του οχήματος της δυνατότητας σύνδεσης στο Διαδίκτυο. Η δυνατότητα αυτή αποτελεί προαπαιτούμενο για την προσφορά ενός εύρους υπηρεσιών άνεσης, όπως είναι τα διαδικτυακά παιχνίδια, η προβολή βίντεο, πλοήγηση στα social media ή πληροφορίες για τον καιρό. Οι εφαρμογές αυτές βασίζονται κυρίως σε επικοινωνίες V2I (όχημα προς υποδομή), των οποίων η καθυστέρηση δεν πρέπει συνήθως να υπερβαίνει τα πεντακόσια χιλιοστά του δευτερολέπτου (500 ms).

3. ΠΡΟΤΥΠΑ ΕΞΥΠΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΦΟΡΩΝ (ITS Standards)

Η ανάπτυξη των δραστηριοτήτων έρευνας και προτυποποίησης για ευφυή συστήματα μεταφορών ξεκίνησε πριν από περίπου μια δεκαετία περιλαμβάνοντας διάφορα διεπιστημονικά πεδία όπως τη μοντελοποίηση ραδιοφωνικών καναλιών, τα πρωτόκολλα που χρησιμοποιούνται στις ζεύξεις δεδομένων, τις ασύρματες επικοινωνίες, τα πρωτόκολλα επιπέδου δικτύωσης, την ασφάλεια και την ιδιωτικότητα των μεταδιδόμενων δεδομένων καθώς και διάφορες υπηρεσίες εντοπισμού. Σε αυτή η ενότητα θα αναφερθούμε εν συντομία στις πιο διαδεδομένες διαδικασίες προτυποποίησης στα ITS καθώς και στην «ομπρέλα» των τεχνολογιών που περιλαμβάνονται σε αυτές.

3.1. Πρότυπα που χρησιμοποιούνται στα ITS

Η αυξανόμενη ζήτηση για «έξυπνες» εφαρμογές συστημάτων μεταφοράς οδήγησε το 2004 στη δημιουργία της ομάδας εργασιών IEEE 802.11p. Η σύσταση της συγκεκριμένης ομάδας επέφερε μια σειρά βελτιώσεων στο πρότυπο IEEE 802.11 που χρησιμοποιείται στο πεδίο της υποστήριξης της ασύρματης πρόσβασης σε περιβάλλοντα οχημάτων (*WAVE*). Το παραχθέν πρότυπο IEEE 802.11p δημοσιεύθηκε το 2010 (Σχέδιο v11) και χρησιμοποιεί το φάσμα συχνοτήτων στη ζώνη των 5,9 GHz για να επιτρέψει τις επικοινωνίες V2V που αναπτύσσονται ανάμεσα στα εν κινήσει οχήματα καθώς και τις επικοινωνίες V2I που αναπτύσσονται μεταξύ των οχημάτων και των RSUs. Πρέπει να σημειωθεί ότι το πρότυπο IEEE 802.11p ορίζει μόνο τις προδιαγραφές για τα στρώματα φυσικού επιπέδου (physical layer) και επιπέδου ελέγχου πρόσβασης στο μέσο (MAC layer), όπως φαίνεται στον Πίνακα 2.

Πίνακας 2: Τεχνικά χαρακτηριστικά των δημοφιλέστερων τύπων οχηματικών τεχνολογιών επικοινωνιών (MAC/PHY). *(Hamida, Noura, & Znaidi, 2015)*

Characteristics	Vehicular Communication Technologies		
	802.11p (WAVE)	802.11 a/b/g/n (Wi-Fi)	Cellular (3G, LTE)
Mode of operation	*Ad hoc*, Infrastructure	*Ad hoc*, Infrastructure	Infrastructure
Communication type	V2V, V2I	V2I	V2I
Bit rate	Up to 27 Mbps	Up to 54 Mbps	Up to 2 Mbps
Communication range	Up to 1000 m	Up to 100 m	Up to 15,000 m
Support for mobility	High	Low	High
Frequency bands	5, 86 to 5.92 GHz	[2.4, 5.2] GHz	[800, 900, 1800, 1900] MHz
Channel bandwidth	[10, 20] MHz	1 to 40 MHz	25 MHz (GSM), 60 MHz (UMTS[1])
Related standards	IEEE, ISO, ETSI	IEEE	ETSI, 3GPP[2]

Στο πρότυπο IEEE 802.11p το φυσικό επίπεδο (PHY layer) βασίζεται στο σχήμα ορθογωνικής πολυπλεξίας διαίρεσης συχνότητας (OFDM) με εύρος ζώνης καναλιού τα 10 MHz, την υποστήριξη για διάφορους ρυθμούς δεδομένων (από 3 έως 27 Mbps) και μέγιστο εύρος επικοινωνίας 1 km. Στο ίδιο πρότυπο το επίπεδο ελέγχου πρόσβασης στο μέσο (MAC layer) βασίζεται σε μια βελτιωμένη έκδοση του αλγόριθμου **λειτουργίας κατανεμημένου συντονισμού** (*DCF*) που χρησιμοποιείται ήδη στην υπάρχουσα οικογένεια προτύπων IEEE 802.11 (Rezgui, Cherkaoui, & Chakroun , 2011). Η βελτιωμένη μορφή του αλγορίθμου αυτού είναι γνωστή στη βιβλιογραφία ως **αλγόριθμος ενισχυμένης πρόσβασης κατανεμημένου καναλιού** (*EDCA*). Βασικό στοιχείο του συγκεκριμένου αλγορίθμου αποτελεί η χρήση της έννοιας της **ποιότητας υπηρεσίας** (QoS) ως κριτήριο για την διασφάλιση υψηλής προτεραιοποίησης σε μηνύματα τα οποία δεν θα πρέπει να υπόκεινται σε χρονική καθυστέρηση, όπως είναι τα μηνύματα ασφαλείας που ανταλλάσσονται σε ένα περιβάλλον ITS. Το QoS επιτυγχάνεται μέσω του ορισμού διαφόρων επιπέδων ελέγχου πρόσβασης (AC layers) με βάση τα κριτήρια προτεραιοποίησης που έχουν τεθεί, π.χ. την καλύτερη δυνατή κίνηση, ειδοποιήσεις ασφαλείας / έκτακτης ανάγκης ή οπτικοακουστικά δεδομένα. Το 2016, δημιουργήθηκε η ομάδα εργασίας IEEE 1609 για να ορίσει επιπρόσθετα υψηλότερα επίπεδα από τα υπάρχοντα (πάνω από τα επίπεδα IEEE 802.11p PHY / MAC) συμπληρώνοντας έτσι τα χαρακτηριστικά του προτύπου IEEE 802.11p. Η προκύπτουσα οικογένεια προτύπων IEEE 1609 περιλαμβάνει τα εξής πρότυπα:

(i) IEEE 1609.1 για τη βελτίωση της διαδικασίας διαχείρισης πόρων

(ii) IEEE 1609.2 (IEEE Standards Association, 2016) για την ενεργοποίηση υπηρεσιών ασφαλείας

(iii) IEEE 1609.3 για την παροχή υπηρεσιών δρομολόγησης και την αντιμετώπιση ζητημάτων που ανακύπτουν σε αυτές τις υπηρεσίες

(iv) IEEE 1609.4 (IEEE Standards Association, 2016) για υποστήριξη πολυκαναλικών λειτουργιών (multichannel operations)

(v) IEEE 1609.5 για τη διαχείριση των διαφορετικών επιπέδων (layers management)

(vi) IEEE 1609.11 για OTA ανταλλαγή δεδομένων ηλεκτρονικών πληρωμών ανάμεσα στις οντότητες του ITS.

Ο συνδυασμός των προτύπων IEEE 802.11p και IEEE 1609 είναι γενικά γνωστός βιβλιογραφία ως **ασύρματη πρόσβαση σε περιβάλλοντα οχημάτων** (**WAVE**).

Παρόμοιες δραστηριότητες τυποποίησης έχουν λάβει χώρα και στον ευρωπαϊκό χώρο στο πλαίσιο της ομάδας εργασίας του Ευρωπαϊκού Ινστιτούτου Προτύπων Τηλεπικοινωνιών (ETSI) για ITS. Το πρότυπο (ETSI TS 102 636-3 V1.1.1, 2010) ορίζει μια αρχιτεκτονική αναφοράς για συνεργατικού τύπου επικοινωνίες ανάμεσα στα οχήματα, στην οποία συμπεριλαμβάνονται έξι (6) κύρια επίπεδα:

(i) το **επίπεδο εφαρμογής** (*application layer*) που υποστηρίζει λειτουργίες που επιτρέπουν τη διαχείριση εφαρμογών ITS (π.χ. προτεραιοποίηση, κατηγοριοποίηση)

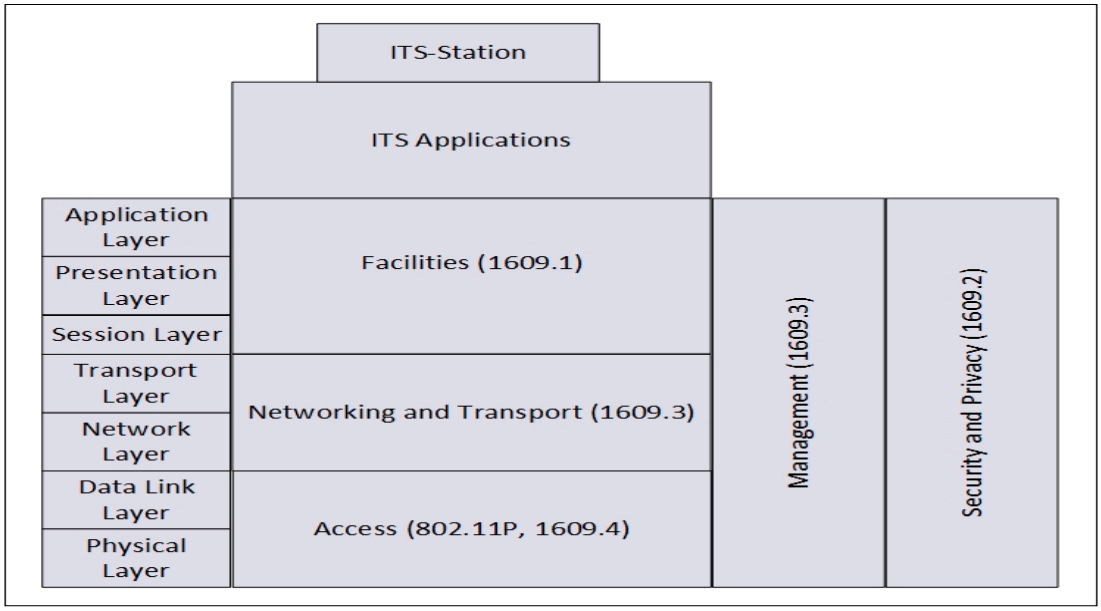
(ii) το **επίπεδο παροχής διευκολύνσεων** (*facilities layer*) στο οποίο υποστηρίζονται σύνοδοι (sessions) καθώς και διάφορες υπηρεσίες παρουσίασης των δεδομένων (data presentation)

(iii) το **επίπεδο δικτύωσης και μεταφοράς** (*networking and transportation layer*), το οποίο υποστηρίζει διάφορα δικτυακά πρωτόκολλα όπως το GeoNetworking και το IPv6 καθώς και πρωτόκολλα μεταφοράς (πχ TCP, UDP)

(iv) το **επίπεδο ελέγχου πρόσβασης στο μέσο** (*medium access control layer*) το οποίο υποστηρίζει διαφόρων τύπων τεχνολογίες επικοινωνίας (π.χ. IEEE 802.11p, Wi-Fi, 3G, LTE κλπ.), όπως φαίνεται στον Πίνακα 2

(v) την **οντότητα διαχείρισης** (*management entity)* η οποία είναι υπεύθυνη για τη διαχείριση των λειτουργιών του συνόλου των επιπέδων αρχιτεκτονικής ITS και

(vi) την **οντότητα ασφάλειας** (*security entity*) η οποία προσφέρει ποικίλες υπηρεσίες ασφαλείας.

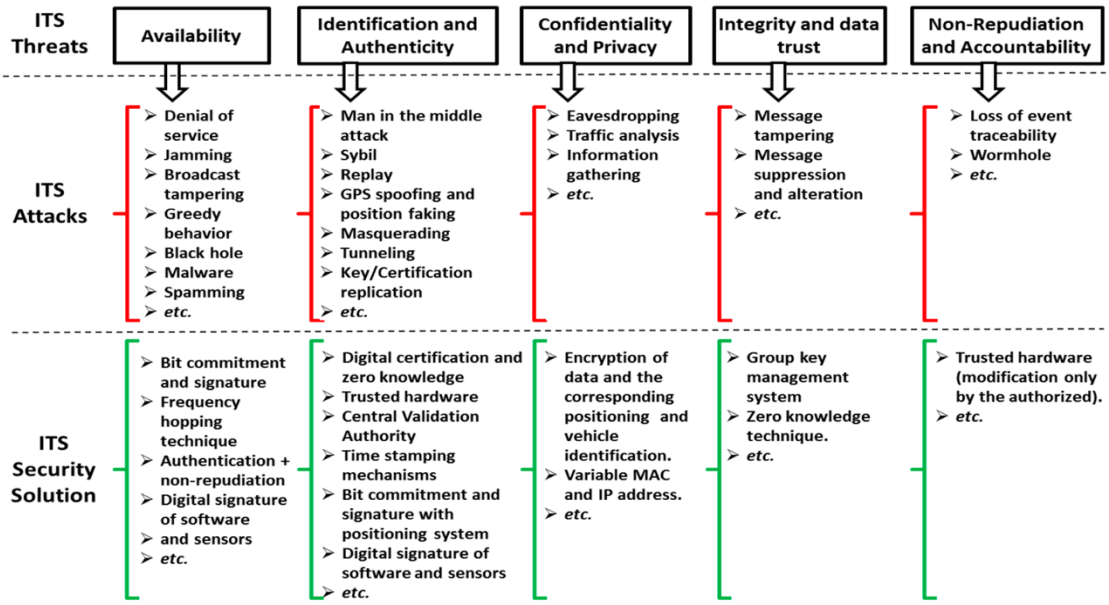


Εικόνα 5: *Πρότυπα τύπου WAVE για την αρχιτεκτονική επικοινωνιακής διαστρωμάτωσης (Ali, Ahmad, Malik, Ali, & Rehman, 2018)*

4. ΑΝΑΛΥΣΗ ΚΑΙ ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΑΠΕΙΛΩΝ ITS

Την τελευταία δεκαετία αναπτύσσεται όλο και περισσότερο ο τομέας της ερευνητικής ενασχόλησης της ακαδημαϊκής κοινότητας με τα έξυπνα συστήματα μεταφορών. Ένας από τους κυριότερους λόγους για τους οποίους συμβαίνει αυτό είναι διότι τα διάφορα ζητήματα ασφάλειας και ιδιωτικότητας που ανακύπτουν στα ITS δυσχεραίνουν τη διαδικασία αποδοχής των συστημάτων αυτών από το κοινωνικό σύνολο, καθώς θίγεται η εμπιστοσύνη του τελευταίου σε αυτά. Όπως έχουμε ήδη αναφέρει, πρωταρχικός στόχος των ITS αποτελεί η βελτίωση της ασφάλειας των επιβαινόντων στα οχήματα καθώς και η αποδοτική διαχείριση των κυκλοφοριακών ροών. Ωστόσο, δεδομένου ότι οι συγκεκριμένες έξυπνες λύσεις προβαίνουν σε εκτεταμένη χρήση τεχνολογιών ασύρματων επικοινωνιών, καθίστανται αυτομάτως ευάλωτες σε ένα πλήθος διαφορετικών απειλών που μπορεί να προξενήσουν δυσάρεστες επιπτώσεις στη λειτουργία τους. Όπως φαίνεται στην Εικόνα 6 οι κυριότεροι τύποι απειλών και επιθέσεων στα περιβάλλοντα έξυπνων συστημάτων μεταφορών συσχετίζονται με τις βασικότερες απαιτήσεις ασφάλειας: την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα, την αυθεντικοποίηση, την μη-αποποίηση, τη λογοδοσία καθώς και την ιδιωτικότητα.

Σε αυτήν την ενότητα θα αναφερθούμε ενδελεχώς στους κυριότερους κινδύνους ασφάλειας και ιδιωτικότητας στα ITS. Αρχικά, θα εξετάσουμε τις εμπλεκόμενες οντότητες ενός ITS εστιάζοντας την προσοχή μας στους κυριότερους τύπους επιτιθέμενων στα συστήματα αυτά. Κατόπιν θα προσδιορίσουμε επακριβώς τις απαιτήσεις ασφάλειας που συνδέονται με τα ITS περιβάλλοντα. Τέλος, θα προβούμε σε ανάλυση και κατηγοριοποίηση των βασικότερων τύπων επιθέσεων μαζί με τα αντίμετρα που θα πρέπει να ληφθούν για την αντιμετώπισή τους.



***Εικόνα 6**: Ενδεικτικές απειλές, επιθέσεις και μέτρα αντιμετώπισης που ανακύπτουν σε περιβάλλοντα ITS (Hamida, Noura, & Znaidi, 2015)*

4.1. Εμπλεκόμενες οντότητες στα ITS

Εξετάζοντας τα ITS υπό το πρίσμα της ασφάλειας διακρίνουμε τις εξής εμπλεκόμενες οντότητες:

- **Οι οδηγοί**: Οι οδηγοί αποτελούν το κρισιμότερο στοιχείο των ITS, δεδομένου ότι είναι αυτοί που καλούνται να λάβουν τις κρίσιμες αποφάσεις όταν λάβει χώρα κάποιο συμβάν στο οδικό δίκτυο και μπορούν να αλληλεπιδράσουν με τα συστήματα υποβοήθησης οδήγησης για να διασφαλίσουν την ασφάλειά τους.

- **Η εποχούμενη μονάδα (OBU)**: Η OBU αποτελεί μία συσκευή, η οποία ενσωματώνεται στο όχημα, προκειμένου να διενεργηθεί ανταλλαγή πληροφοριών με κάποια RSU ή με τις OBU άλλων οχημάτων. Αποτελείται από έναν επεξεργαστή εντολών και περιλαμβάνει μια μνήμη ανάγνωσης/εγγραφής, η οποία χρησιμοποιείται για την αποθήκευση και την ανάκτηση πληροφοριών. Επιπροσθέτως, περιλαμβάνει ένα περιβάλλον διεπαφής χρήστη, μία διεπαφή για τη σύνδεση με άλλες OBU και μία συσκευή δικτύου για ασύρματη επικοινωνία μικρής εμβέλειας, βασισμένη στο πρότυπο IEEE 802.11p. Σε γενικές γραμμές, οι βασικές λειτουργίες μιας συσκευής OBU είναι η παροχή́ δυνατότητας ασύρματης επικοινωνίας, η δρομολόγηση πληροφοριών, η αξιόπιστη μεταφορά́ μηνυμάτων και η ασφάλεια των δεδομένων.

- **Η μονάδα παραπλεύρως του δρόμου (RSU)**: Η RSU είναι μία μονάδα η οποία είναι τοποθετημένη παραπλεύρως ή κατά μήκος του δρόμου σε συγκεκριμένες, ειδικές θέσεις όπως σε κόμβους. Στον εξοπλισμό της συμπεριλαμβάνεται μία συσκευή δικτύου, προκειμένου να καταστεί εφικτή η επικοινωνία εντός μικρής εμβέλειας, σύμφωνα με το πρότυπο IEEE 802.11p. Επιπλέον, είναι πιθανό να περιλαμβάνει και άλλες δικτυακές συσκευές, προκειμένου να υποστηριχθεί επικοινωνία εντός του δικτύου υποδομής. Οι βασικές λειτουργίες και διαδικασίες μιας RSU είναι η επέκταση της εμβέλειας επικοινωνίας του αδόμητου (ad-hoc) δικτύου, μέσω της αναδιανομής πληροφοριών ανάμεσα στις OBUs και της επαναποστολής αυτών σε άλλες RSU, η εκτέλεση εφαρμογών ασφάλειας μέσω της προειδοποίησης οχημάτων για ενδεχόμενα συμβάντα στο δρόμο με την αποστολή των απαιτούμενων πληροφοριών σε αυτά καθώς και η παροχή σύνδεσης στο διαδίκτυο στις OBUs των οχημάτων.

- **Έμπιστες τρίτες οντότητες (TTP)**: Οι έμπιστες τρίτες οντότητες είναι υπεύθυνες για τη διαχείριση των πιστοποιητικών ασφαλείας, καθώς και για τα διάφορα ζεύγη ιδιωτικών/δημόσιων κλειδιών που χρησιμοποιούνται από ένα οικοσύστημα έξυπνων συστημάτων μεταφορών. Παραδείγματα τέτοιων οντοτήτων αποτελούν οι ρυθμιστικοί φορείς μεταφορών και οι κατασκευαστές οχημάτων.

- **Οι επιτιθέμενοι:** Οι επιτιθέμενοι προσπαθούν να παραβιάσουν την ασφάλεια των ITS χρησιμοποιώντας ποικιλία τεχνικών. Αυτοί οι εισβολείς μπορούν να ταξινομηθούν σε διαφορετικές κατηγορίες, όπως θα δούμε στην επόμενη ενότητα.

4.2. Προφίλ επιτιθέμενων σε ITS

Οι επιτιθέμενοι κατατάσσονται γενικά σε τρεις αμοιβαία αποκλειόμενες κατηγορίες προφίλ, οι οποίες είναι οι ακόλουθες:

- **Ενεργή/Παθητική διαδικτυακή συμπεριφορά:** Οι επιτιθέμενοι με ενεργή διαδικτυακή συμπεριφορά προβαίνουν σε κακόβουλες ενέργειες όπως είναι η μετάδοση κακόβουλων πακέτων με σκοπό να βλάψουν άλλους κόμβους του δικτύου. Η δημοφιλέστερη τακτική που ακολουθούν οι εισβολείς που ανήκουν σε αυτήν την κατηγορία είναι να επινοούν στρατηγικές παράκαμψης του υποσυστήματος εξουσιοδότησης ενός πληροφοριακού συστήματος αποσκοπώντας στην απόκτηση δικαιωμάτων υπερχρήστη(superuser) που θα τους επιτρέψουν να εκτελέσουν με επιτυχία το πλήρες φάσμα των κακόβουλων ενεργειών τους. Αντίθετα, οι επιτιθέμενοι που παρουσιάζουν παθητική συμπεριφορά περιορίζονται στην απλή παρακολούθηση των επικοινωνιών που αναπτύσσονται μεταξύ των κόμβων ενός δικτύου, προκειμένου να εξαγάγουν χρήσιμες πληροφορίες από αυτές. Αν και η τελευταία κατηγορία επιτιθέμενων δεν μπορούν να προκαλέσουν άμεση βλάβη στο δίκτυο όπως οι επιτιθέμενοι της προηγούμενης κατηγορίας, εντούτοις οι πληροφορίες που συγκεντρώνουν μπορούν να χρησιμοποιηθούν για μελλοντικές επιθέσεις.

- **Εξωτερικοί-Εσωτερικοί επιτιθέμενοι**: Οι εξωτερικοί επιτιθέμενοι αποτελούν άτομα τα οποία δεν υπόκεινται σε έλεγχο ταυτοποίησης και εξουσιοδότησης στοχεύοντας κυρίως την εμπιστευτικότητα και τη διαθεσιμότητα ενός ITS. Αντίθετα, οι εσωτερικοί επιτιθέμενοι αποτελούν εξουσιοδοτημένους χρήστες του ITS γεγονός που τους επιτρέπει να διαπράξουν σχεδόν κάθε είδους επίθεση.

- **Κακόβουλοι- 'λογικοί' επιτιθέμενοι:** Οι κακόβουλοι εισβολείς δεν έχουν συγκεκριμένους στόχους και ο κύριος στόχος τους είναι να καταστρέψουν το δίκτυο, για παράδειγμα με τη μετάδοση ψευδών πληροφοριών σε οχήματα μιας συγκεκριμένης γεωγραφικής περιοχής. Αντίθετα, οι «λογικοί» επιτιθέμενοι έχουν πάντα έναν συγκεκριμένο στόχο στο μυαλό τους γεγονός που τους καθιστά πολύ επικίνδυνους λόγω της απρόβλεπτης φύσης τους.

4.3. Απαιτήσεις ασφάλειας σε περιβάλλοντα έξυπνων μεταφορών

Για να διασφαλιστεί η ασφάλεια των V2X επικοινωνιών πρέπει να ληφθεί υπόψη ένα σύνολο διαφορετικών απαιτήσεων ασφάλειας. Συγκεκριμένα, ο σχεδιασμός εφαρμογών ITS απαιτεί ιδιαίτερη προσοχή και χαρακτηρίζεται από συγκεκριμένες προκλήσεις και απαιτήσεις:

- **Αυθεντικοποίηση (*authentication*)**: Πρόκειται για μια από τις σημαντικότερες απαιτήσεις ασφάλειας. Στα πλαίσια ενός ITS μπορεί να κατατμηθεί σε τρεις υποπεριπτώσεις: (i) έλεγχος ταυτότητας οχήματος για την αποτροπή επιθέσεων τύπου Sybil και την απόρριψη κακόβουλων οντοτήτων από το σύστημα (ii) έλεγχος ταυτότητας των αποστολέων των μηνυμάτων για να διασφαλιστεί ότι τα μηνύματα συντάχθηκαν από εξουσιοδοτημένους χρήστες του ITS και (iii) χρήση δεδομένων τοποθεσίας προκειμένου να διασφαλιστεί η ακεραιότητα και η συνάφεια των ληφθέντων πληροφοριών.

- **Ακεραιότητα δεδομένων (data integrity)**: Οι οντότητες που απαρτίζουν ένα ITS (π.χ. OBUs, RSUs) θα πρέπει να μπορούν να επαληθεύουν και να επικυρώνουν την ακεραιότητα των ληφθέντων μηνυμάτων, προκειμένου να αποτρέπεται οποιαδήποτε μη εξουσιοδοτημένη ή κακόβουλη τροποποίηση, χειραγώγηση ή διαγραφή κατά τη μετάδοση.

- **Ιδιωτικότητα και ανωνυμία *(privacy and anonymity)***: Σε ένα ITS τα δεδομένα ταυτοποίησης των οδηγών και των οχημάτων δεν πρέπει να εξάγονται εύκολα από τη μελέτη της ροής των μηνυμάτων που ανταλλάσσουν μεταξύ τους. Για να επιτευχθεί αυτός ο σκοπός πρέπει να περιφρουρηθεί το δικαίωμα του οδηγού να γνωρίζει ανά πάσα στιγμή την ταυτότητα των προσώπων που εμπλέκονται στη διαδικασία χρησιμοποίησης των προσωπικών του δεδομένων.

- **Διαθεσιμότητα (*availability*)**: Τα ανταλλασσόμενα μηνύματα θα πρέπει να διατίθενται στις εμπλεκόμενες οντότητες σε πραγματικό χρόνο, απαιτώντας έτσι την εφαρμογή αλγορίθμων χαμηλής επιβάρυνσης για την επεξεργασία τους όπως και τη χρήση «ελαφρών» μεθόδων κρυπτογράφησης (lightweight cryptography techniques).

- **Ιχνηλασιμότητα και ανάκληση (*traceability and revocation*)**: Σε περιπτώσεις στις οποίες μια έμπιστη τρίτη οντότητα (TTP) επιφορτίζεται με τον εποπτικό έλεγχο ενός ITS, θα πρέπει να της παρέχεται η δυνατότητα παρακολούθησης της συμπεριφοράς του συνόλου των εμπλεκόμενων οντοτήτων, ούτως ώστε να εντοπίζει εγκαίρως κακόβουλες οντότητες που προβαίνουν σε κατάχρηση του ITS. Για να διαχειριστεί επιτυχώς τέτοιου είδους περιστατικά, η εποπτική αρχή (TA) θα πρέπει πρωτίστως να μπορεί να προβαίνει σε ενέργειες που κυμαίνονται από την ανάκτηση των δεδομένων που αφορούν το «κακόβουλο» όχημα στην αποκάλυψη της ταυτότητας του κατόχου του. Επιπλέον, σε

περιπτώσεις στις οποίες η «συμπεριφορά» του κακόβουλου οχήματος εγκυμονεί σοβαρούς κινδύνους για την εύρυθμη λειτουργία και ασφάλεια του ITS, η εποπτική αρχή θα πρέπει να «αποβάλλει» το όχημα αυτό από το δίκτυο, προσαρτώντας τα στοιχεία του σε μια λίστα ανάκλησης (revocation list).

- **Εξουσιοδότηση (*authorization*):** Για την ικανοποίηση της εν λόγω απαίτησης είναι αναγκαίος ο ορισμός μηχανισμών ελέγχου πρόσβασης (access control) για τις διάφορες οντότητες ενός ITS. Πρέπει να επιβληθούν συγκεκριμένοι κανόνες για την αποδοχή ή την άρνηση πρόσβασης κατά τη χρήση συγκεκριμένων υπηρεσιών ή δεδομένων από κάποια οντότητα ITS.

- **Μη αποποίηση (*non-repudiation*):** Κάθε οντότητα ITS θα πρέπει να συσχετίζεται μοναδικά με ένα σύνολο πληροφοριών που την αφορούν προκειμένου να διασφαλίζεται η αυθεντικότητα των αποσταλμένων δεδομένων.

- **Ανθεκτικότητα (*resilience*) έναντι εξωτερικών επιθέσεων**: Οι οντότητες ενός ITS πρέπει να διαθέτουν ισχυρά μέσα για την προστασία τους έναντι μιας πλειάδας επιθέσεων. Στην κατεύθυνση αυτή, μια από τις κρισιμότερες απαιτήσεις που τίθεται είναι η ελαχιστοποίηση των ευπαθειών και λογικών ελαττωμάτων.

- **Εμπιστευτικότητα δεδομένων (*data confidentiality*)**: Τα μηνύματα που ανταλλάσσονται σε ένα έξυπνο περιβάλλον μεταφορών θα πρέπει διαθέτουν μέτρα και τεχνικές ασφάλειας για την προστασία του περιεχομένου τους (π.χ. κρυπτογράφηση) ούτως ώστε να αποφεύγεται η αποκάλυψη πληροφοριών "ευαίσθητης" φύσεως σε κακόβουλους κόμβους ή μη εξουσιοδοτημένα μέρη.

4.4 Κατηγοριοποίηση επιθέσεων ασφάλειας σε περιβάλλοντα έξυπνων μεταφορών

Τα περιβάλλοντα έξυπνων μεταφορών καθίστανται ευάλωτα σε μια πλειάδα διαφορετικών απειλών και επιθέσεων. Η πιο απλή κατηγοριοποίηση περιλαμβάνει την ένταξή τους στις κατηγορίες των απειλών ενεργητικής και παθητικής φύσεως. Οι πρώτες επιφέρουν σοβαρές επιπτώσεις στους πόρους και στη λειτουργικότητα των δικτύων με τη χρήση διαφόρων τεχνικών που θα εξετάσουμε διεξοδικά παρακάτω. Οι δεύτερες, στις οποίες επίσης θα αναφερθούμε διεξοδικά στις ενότητες που ακολουθούν, πλήττουν την εμπιστευτικότητα (*confidentiality*) και την ιδιωτικότητα (*privacy*) του δικτύου. Στην *Εικόνα 7* αποτυπώνονται τα κυριότερα είδη απειλών σε συνάρτηση με τις απαιτήσεις ασφάλειας τις οποίες πλήττουν κατά περίπτωση. Η προσέγγιση που θα ακολουθήσουμε στη συνέχεια για την κατηγοριοποίηση των κυριότερων τύπων επιθέσεων συσχετίζεται με τις υπάρχουσες κρυπτογραφικές μεθόδους που χρησιμοποιούνται ως μέτρα ασφαλείας για καθεμιά από αυτές. Η επιλογή μας αυτή

στηρίζεται στο γεγονός ότι η κρυπτογραφία διαδραματίζει σημαίνοντα ρόλο στην παροχή ενός ολιστικού πλαισίου για την προστασία των απαιτήσεων ασφαλείας [2]. Παρακάτω προβαίνουμε σε αναλυτική περιγραφή των επιθέσεων και των μέτρων ασφαλείας που χρησιμοποιούνται για να προστατευτεί το σύστημα από αυτές.

Compromised Security Services / Attacks	Availability	Authentication	Non-Repudiation	Integrity	Privacy	Confidentiality
Denial of service attacks (DoS)	✓					
Jamming attack	✓					
Sybil attack	✓	✓				
Variants of DoS (greedy, Black hole, gray hole, sink hole Wormhole, malware, masquerading Spamming, tunneling)	✓	✓	✓	✓	✓	
Loss of event traceability			✓			
Illusion		✓		✓		
Replay		✓		✓		
Key and/or certificate replication		✓				✓
GPS spoofing/position faking		✓			✓	
Message tampering/ suppression/fabrication/alteration	✓		✓	✓		
Broadcast tampering				✓		
Node impersonation		✓	✓	✓		
Brute force						✓
Eavesdropping						✓
Traffic analysis					✓	✓
Tracking/social engineering					✓	
Timing attack	✓					
Man in the middle attack		✓	✓	✓		

Εικόνα 7: *Συσχέτιση επιπτώσεων διαφορετικών τύπων επιθέσεων με τις κυριότερες απαιτήσεις ασφάλειας (Hamida, Noura, & Znaidi, 2015)*

4.4.1 Επιθέσεις στη διαθεσιμότητα και αντίμετρα

Η διαθεσιμότητα αποτελεί μια πολύ σημαντική απαίτηση για τα έξυπνα συστήματα μεταφορών διότι διασφαλίζει την ασφάλεια των οχημάτων και των οδηγών ενός δικτύου. Ο πιο γνωστός και, συγχρόνως, ο πιο επικίνδυνος τύπος επιθέσεων που στοχεύουν τη διαθεσιμότητα ενός ITS είναι οι επιθέσεις άρνησης υπηρεσιών (*DoS attacks*) εξαιτίας των σοβαρότατων επιπτώσεών τους στους πόρους του δικτύου. Οι συγκεκριμένες επιθέσεις διεξάγονται είτε από εσωτερικές είτε από εξωτερικές κακόβουλες οντότητες και αποσκοπούν στην παρεμπόδιση των χρηστών του συστήματος να χρησιμοποιήσουν τις υπηρεσίες και τους πόρους του δικτύου. Μια αρκετά διαδεδομένη παραλλαγή των DoS επιθέσεων αποτελούν οι **κατανεμημένες επιθέσεις άρνησης υπηρεσιών** (*DDoS*) το βασικό μοντέλο των οποίων συνίσταται σε

[2] Ενδεικτικοί μηχανισμοί ασφαλείας αποτελούν οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης, μηχανισμοί για την δημιουργία ασφαλών κλειδιών μαζί με τα πρωτόκολλα για τη διαχείριση και διανομή τους, συναρτήσεις κατακερματισμού, ψηφιακές υπογραφές.

έναν κόμβο με συντονιστικό ρόλο που έχει κατορθώσει να θέσει υπό τον έλεγχό του ένα σύνολο άλλων κόμβων (τις περισσότερες φορές χωρίς τη θέλησή τους) και τους ενορχηστρώνει για να διεξάγουν με επιτυχία την σχεδιαζόμενη επίθεση. Ακολούθως παρατίθενται μια λίστα με τις συνηθέστερες επιθέσεις τύπου DoS και DDoS συνοδευόμενες από τα αντίστοιχα μέτρα που χρησιμοποιούνται για την αντιμετώπισή τους.

- **Jamming attacks**: Ο συγκεκριμένος τύπος επίθεσης διεξάγεται στο φυσικό επίπεδο και αποσκοπεί στην διακοπή λειτουργίας του διαύλου επικοινωνίας μέσω της μετάδοσης σημάτων θορύβου υψηλής συχνότητας ούτως ώστε να επιτύχουν υψηλό επίπεδο παρεμβολής. Έτσι, μειώνεται ο δείκτης SNR[3] καθιστώντας τα οχήματα ανίκανα να επικοινωνήσουν μεταξύ τους και με άλλες οντότητες του συστήματος (π.χ. RSUs). Οι επιπτώσεις των συγκεκριμένων επιθέσεων μπορούν να αντιμετωπιστούν τυχαιοποιώντας τον μηχανισμό FHHS[4] του προτύπου OFDM χρησιμοποιώντας αποτελεσματικούς αλγορίθμους ψευδωανωνυμοποίησης.

- **Flooding attacks**: Το σενάριο επίθεσης στη συγκεκριμένη περίπτωση συνίσταται στην υπερφόρτωση του δικτύου μέσω της αποστολής ενός πολύ μεγάλου αριθμού μηνυμάτων με μηδενική αξία όσον αφορά το περιεχόμενό τους που αποστέλλονται από κακόβουλες οντότητες. Μια πιθανή επίπτωση των συγκεκριμένων επιθέσεων είναι η εμφάνιση ατυχημάτων σε περιπτώσεις που μηνύματα ασφάλειας υψηλής κρισιμότητας αδυνατούν να αποσταλούν στους νόμιμους παραλήπτες τους.

- **Sybil attacks:** Ο κυριότερος στόχος των συγκεκριμένων επιθέσεων είναι η δημιουργία σύγχυσης στο δίκτυο μέσω της εκπομπής 'ψευδών' ταυτοτήτων από κακόβουλους κόμβους. Οι αυθεντικοί κόμβοι εξαπατώνται θεωρώντας ότι τα κακόβουλα μηνύματα προέρχονται από τα οχήματα του συστήματος των οποίων τις ταυτότητες έχουν υποκλέψει και εκπέμπουν οι επιτιθέμενοι για να αποκρύψουν την πραγματική τους ταυτότητα. Η 'παραδοσιακή' μέθοδος προστασίας από τέτοιου είδους επιθέσεις είναι η προσθήκη στο δίκτυο μιας έμπιστης τρίτης οντότητας (TTP) η οποία θα είναι επιφορτισμένη με καθήκοντα αυθεντικοποίησης των κόμβων ενός συστήματος οποιαδήποτε χρονική στιγμή. Η διαδικασία αυθεντικοποίησης μπορεί να πραγματοποιείται είτε με άμεσο είτε με έμμεσο τρόπο. Στην πρώτη περίπτωση εγκαθιδρύεται ένα κανάλι

[3] **Signal-to-Noise Ratio** (SNR): Αποτελεί τον λόγο της ισχύος ενός σήματος προς την ισχύ θορύβου του εξωτερικού περιβάλλοντος. Εκφράζεται σε decibel και αποτελεί έναν από τους σημαντικότερους δείκτες που σχετίζονται με την ποιότητα υπηρεσιών ενός τηλεπικοινωνιακού δικτύου.

[4] **Frequency Hopping Spread Spectrum** (FHSS): Αποτελεί μια μέθοδο μετάδοσης ραδιοσημάτων που χαρακτηρίζεται από γρήγορες εναλλαγές της συχνότητας φορέα μεταξύ πολλών διακριτών συχνοτήτων που καταλαμβάνουν μια μεγάλη ζώνη φάσματος. Οι εναλλαγές ελέγχονται από έναν κωδικό γνωστό τόσο στον πομπό όσο και στον δέκτη.

επικοινωνίας ανάμεσα στην TTP και την προς αυθεντικοποίηση οντότητα ενώ, στη δεύτερη περίπτωση, εκτός από την TTP καθήκοντα αυθεντικοποίησης μπορούν να αναλάβουν και υφιστάμενοι κόμβοι του συστήματος. Ένα επιπρόσθετο επίπεδο προστασίας της διαδικασίας αυθεντικοποίησης επιτυγχάνεται με την χρήση πρωτοκόλλων οριοθέτησης απόστασης[5] (*distance bounding protocols*) ανάμεσα στον επαληθευτή ταυτότητας και τον προς αυθεντικοποίηση κόμβο όπως επίσης και με τη χρήση τεχνικών αυθεντικοποίησης της γεωγραφικής θέσης ενός κόμβου (*secure location verification*). Ως εναλλακτική προσέγγιση για την αντιμετώπιση των επιθέσεων αυτής της κατηγορίας προτείνεται η χρήση αποκεντρωμένων μοντέλων που εκμεταλλεύονται τα πλεονεκτήματα της τεχνολογίας «αλυσίδας μπλοκ» (*blockchain*) ώστε να παράσχουν απρόσκοπτα υπηρεσίες αυθεντικοποίησης στα οχήματα-κόμβους ενός VANET. Για παράδειγμα, ένα τέτοιου είδους μοντέλο έχει προταθεί από τους (Azees, Vijayakumar, Jeatha, Marimuthu, & Subaja-Christo, 2021). Το μοντέλο αυτό βασίζεται στην τεχνολογία blockchain για την διατήρηση των ιδιαίτερων χαρακτηριστικών κάθε οχήματος καθώς και των πληροφοριών που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών του VANET με κατανεμημένο τρόπο σε ένα διαμοιραζόμενο μητρώο πληροφοριών (*ledger*). Κατ' αυτόν τον τρόπο επιτυγχάνεται ο έλεγχος και η επαλήθευση της ταυτότητας κάθε χρήστη του VANET επιτυγχάνεται μέσω μιας διαδικασίας επίτευξης συμφωνίας (consensus) ανάμεσα στους κόμβους, χωρίς τη διαμεσολάβηση κάποιας ΤΑ.

- **Επιθέσεις κακόβουλου λογισμικού (malware attacks)**: Οι επιθέσεις κακόβουλου λογισμικού συντίθενται από ιούς (viruses), σκουλήκια (worms) και δούρειους ίππους (trojans) που μπορούν να επηρεάσουν το δίκτυο των οχημάτων, καθώς και συστατικά στοιχεία λογισμικού των OBU και RSU. Τέτοιου είδους επιθέσεις επιφέρουν σοβαρότατες επιπτώσεις όσον αφορά τη λειτουργικότητα των ITS, ωστόσο οι επιπτώσεις αυτές μπορούν να μετριαστούν με τη χρήση λογισμικού προστασίας από ιούς και κακόβουλο λογισμικό (antivirus). Ωστόσο, το σύγχρονο πολυμορφικό κακόβουλο λογισμικό μπορεί να μεταβάλλει τα χαρακτηριστικά του κατά τη φάση αναπαραγωγής, καθιστώντας έτσι το έργο της ανίχνευσής του πολύ δύσκολο. Το πιο διαδεδομένο κρυπτογραφικό αντίμετρο που χρησιμοποιείται στη συγκεκριμένη περίπτωση είναι η εφαρμογή τεχνικών αυθεντικοποίησης στις εκάστοτε ενημερώσεις λογισμικού (π.χ. χρήση ψηφιακής υπογραφής) ούτως ώστε να επαληθεύεται η εγκυρότητα των αποστολέων τους (π.χ. OEMs) πριν από την εγκατάστασή τους στις ECUs και τις OBUs.

[5] Τα **πρωτόκολλα οριοθέτησης απόστασης** αποτελούν κρυπτογραφικά πρωτόκολλα που επιτρέπουν στον επαληθευτή ταυτοτήτων (verifier) να θέτει ένα ανώτατο όριο όσον αφορά τη φυσική απόσταση που τον χωρίζει από μια προς αυθεντικοποίηση οντότητα (prover). Τα πρωτόκολλα αυτά έχουν ευρεία χρήση π.χ. σε περιπτώσεις ταυτοποίησης φυσικών προσώπων στην είσοδο ενός κτιρίου δεν είναι λογικό το μηχάνημα που χρησιμοποιείται για τον έλεγχο πρόσβασης να βρίσκεται περισσότερο από λίγα μέτρα μακριά από το προς αυθεντικοποίηση πρόσωπο.

- **Επιθέσεις ανεπιθύμητης αλληλογραφίας (spam attacks)**: Οι επιθέσεις ανεπιθύμητης αλληλογραφίας αποσκοπούν κυρίως στην κατανάλωση του εύρους ζώνης (bandwidth) του δικτύου και στην εισαγωγή υψηλών χρόνων καθυστέρησης στη διαδικασία μετάδοσης των πακέτων στο δίκτυο, μέσω της αποστολής πολύ μεγάλου αριθμού μηνυμάτων ανεπιθύμητης αλληλογραφίας (π.χ. διαφημιστικά μηνύματα) σε μια ομάδα χρηστών. Θα πρέπει να σημειωθεί ότι η διαδικασία ελέγχου αυτού του τύπου μηνυμάτων παρουσιάζει μεγάλες δυσκολίες, κυρίως εξαιτίας της έλλειψης κεντρικής υποδομής.

- **Black hole attacks**: Υφίστανται σε οποιοδήποτε τύπο ad hoc δικτύου, συμπεριλαμβανομένου των ITS. Στην πραγματικότητα, μια μαύρη τρύπα δημιουργείται μέσα στο δίκτυο όταν οι κακόβουλοι κόμβοι αποτυγχάνουν ή αρνούνται να διαδώσουν μηνύματα που παραλαμβάνουν παρόλο που έχουν δηλώσει διαθέσιμοι για συμμετοχή στις διάφορες διαδικασίες επικοινωνίας. Αυτό το είδος επίθεσης είναι πολύ επικίνδυνο για πολλές εφαρμογές ITS, ειδικά για εφαρμογές οδικής ασφάλειας που είναι ευαίσθητες σε χρονική καθυστέρηση.

- **Gray hole attacks:** Αποτελούν παραλλαγή των black hole επιθέσεων και συνίσταται στην απόρριψη πακέτων δεδομένων που σχετίζονται με συγκεκριμένες εφαρμογές ITS κατά τη διαδικασία δρομολόγησης.

- **Sinkhole attacks**: Μπορούν να χρησιμοποιηθούν για την προετοιμασία διεξαγωγής άλλων τύπων επιθέσεων, όπως των blackhole και των greyhole attacks. Σε αυτήν την επίθεση, τα πακέτα των γειτονικών κόμβων μεταδίδονται μέσω κακόβουλων κόμβων, οι οποίοι μπορούν να οδηγήσουν στην απόρριψη ή την τροποποίηση των ληφθέντων πακέτων προτού τα επαναμεταδώσουν. .

- **Worm hole attacks:** Αποτελούν έναν τύπο DoS επιθέσεων που απαιτούν τη συμμετοχή τουλάχιστον δύο κόμβων "A" και "B" που βρίσκονται σε μεγάλη γεωγραφική απόσταση μεταξύ τους. Ο "A" αποστέλλει στον "B" ένα συγκεκριμένο μήνυμα που ενημερώνει τους γειτονικούς κόμβους του "B" ότι ο "A" είναι ο γείτονάς τους. Αυτή η επίθεση επιτρέπει σε δύο ή περισσότερους κόμβους οι οποίοι υπό κανονικές συνθήκες δεν βρίσκονται σε γειτονική απόσταση να ανταλλάσσουν πακέτα ελέγχου μεταξύ τους και να δημιουργούν διαύλους επικοινωνίας από το μηδέν.

- **Tunneling attacks:** Ανήκουν στην ίδια συνομοταξία με τις worm hole attacks με τη μικρή διαφορά ότι χρησιμοποιούν το ίδιο δίκτυο για τη δημιουργία ιδιωτικής σύνδεσης. Στοχεύουν στη σύνδεση δύο απομακρυσμένων περιοχών του δικτύου οχημάτων χρησιμοποιώντας ένα πρόσθετο κανάλι επικοινωνίας, όπως ένα tunnel. Έτσι, τα θύματα δύο απομακρυσμένων περιοχών του δικτύου μπορούν να επικοινωνούν ωσάν να ήταν γείτονες.

Οι κρυπτογραφικές λύσεις γενικά δεν είναι αποτελεσματικές για την αντιμετώπιση των επιθέσεων που πλήττουν τη διαθεσιμότητα ωστόσο, όπως αποτυπώνεται και στην Εικόνα 5, υπάρχουν ορισμένες κρυπτογραφικές μέθοδοι, όπως οι αλγόριθμοι ψηφιακής υπογραφήw, οι οποίες μπορεί να αναχαιτίσουν τις επιπτώσεις τους.

4.4.2 Επιθέσεις στην αυθεντικοποίηση και αντίμετρα

Η αυθεντικοποίηση αποτελεί κρίσιμης σημασίας απαίτηση για τα ITS διότι διασφαλίζει την προστασία των νόμιμων κόμβων του συστήματος από μια πλειάδα επιθέσεων όπως black hole attacks, spoofing και replay attacks. Η ψηφιακή υπογραφή αποτελεί την πιο διαδεδομένη κρυπτογραφική μέθοδο για την εγγύηση της αυθεντικοποίησης των οντοτήτων του συστήματος, δίνοντας τη δυνατότητα στους παραλήπτες των μηνυμάτων να επιβεβαιώνουν την ταυτότητα των αποστολέων τους. Η έννοια της αυθεντικοποίησης συνίσταται στο γεγονός ότι μόνο οι αυθεντικοποιημένοι κόμβοι μπορούν να προσπελάσουν τους πόρους του δικτύου και να χρησιμοποιήσουν τις υπηρεσίες του. Οποιαδήποτε ευπάθεια στη διαδικασία της αυθεντικοποίησης μπορεί να αποβεί μοιραία για τη συνολική λειτουργικότητα του δικτύου. Παρακάτω παραθέτουμε τις κυριότερες κατηγορίες απειλών-επιθέσεων που στοχεύουν την συγκεκριμένη απαίτηση ασφαλείας:

- **Επιθέσεις ψευδεπίγραφων οντοτήτων (Falsified entitites attack)**: Ο επιτιθέμενος αποκτά ένα έγκυρο αναγνωριστικό και υποδύεται έναν άλλο νόμιμο κόμβο του δικτύου παραβιάζοντας έτσι τη διαδικασία ελέγχου ταυτότητας. Κάθε οντότητα ITS συνδέεται με ένα αναγνωριστικό δικτύου, το οποίο επιτρέπει τη διάκρισή της από τις υπόλοιπες οντότητες του συστήματος. Για παράδειγμα, μπορούν να αναπτυχθούν πλαστά σημεία πρόσβασης (rogue AP) κατά μήκος των δρόμων ώστε, μιμούμενα νόμιμες RSU, να ξεκινήσουν επιθέσεις εναντίον των συνδεδεμένων χρηστών και οχημάτων. Αυτή η επίθεση μπορεί να αποφευχθεί με την εφαρμογή κατάλληλων μηχανισμών ελέγχου ταυτότητας, για παράδειγμα με τη χρήση κρυπτογραφικών υποδομών δημόσιου κλειδιού, όπου κάθε οντότητα ITS συσχετίζεται με ένα έγκυρο πιστοποιητικό, το οποίο και υπογράφεται από την εποπτική αρχή του ITS.

- **Επιθέσεις αντιγραφής κρυπτογραφικών στοιχείων (cryptographic replication attacks)**: Σε αυτό το είδος επίθεσης, ο επιτιθέμενος αντιγράφει υπάρχοντα κλειδιά ή/και πιστοποιητικά εμποδίζοντας τις εποπτικές αρχές να αναγνωρίσουν ένα όχημα, ειδικά σε περιπτώσεις διενέξεων. Το πρώτο αντίμετρο που χρησιμοποιείται για τέτοιου είδους επιθέσεις είναι η χρήση έγκυρων κλειδιών μιας χρήσης. Μια άλλη λύση αποτελεί η, σε πραγματικό χρόνο, επαλήθευση της εγκυρότητας του πιστοποιητικού μιας οντότητας μέσω της εξέτασης μιας λίστας ανάκλησης πιστοποιητικών (CRL). Ωστόσο, στα ITS, η τελευταία λύση βρίθει ζητημάτων δεδομένου ότι τίθεται η ισχυρή απαίτηση της ύπαρξης εμπιστοσύνης μεταξύ των διαφόρων αρχών πιστοποίησης.

- **Επιθέσεις εξαπάτησης συστημάτων δορυφορικού γεωεντοπισμού με ψευδή δεδομένα τοποθεσίας (GNSS spoofing and injection attacks)**: Στα ITS, τα δεδομένα τοποθεσίας είναι ζωτικής σημασίας και πρέπει να χαρακτηρίζονται από ακρίβεια και αξιοπιστία. Τα κυριότερα τεχνολογικά μέσα που χρησιμοποιούνται για τη συλλογή των δεδομένων αυτών είναι τα παγκόσμια δορυφορικά συστήματα πλοήγησης (GNSS). Σε αυτό το πλαίσιο, οι επιθέσεις αυτού του τύπου πλήττουν κυρίως τα συνεργατικού τύπου δίκτυα οχημάτων και συνίσταται στην παροχή ψευδών πληροφοριών θέσης ενός οχήματος στα γειτονικά του οχήματα. Δεδομένου ότι κάθε όχημα είναι εξοπλισμένο με έναν δέκτη GPS, προκειμένου οι επιθέσεις αυτές να καταλήξουν σε επιτυχές αποτέλεσμα απαιτούν τη χρήση ενός πομπού που εκπέμπει σήματα εντοπισμού ισχυρότερα από τα αντίστοιχα των πραγματικών δορυφόρων GPS. Οι επιθέσεις αυτές αντιμετωπίζονται με τη χρήση πρωτοκόλλων 'δέσμευσης' bit (McGill University, 1997) και τη χρήση σχημάτων ψηφιακών υπογραφών ούτως ώστε τα συστήματα που χρησιμοποιούνται για τον προσδιορισμό της γεωγραφικής θέσης κάθε οχήματος να χρησιμοποιούν μόνο αυθεντικά (*γνήσια*) δεδομένα τοποθεσίας.

- **Χρονικές επιθέσεις (Timing attacks)**: Σε εφαρμογές που παρέχουν υπηρεσίες ασφάλειας στα ITS, η έγκαιρη παράδοση / λήψη μηνυμάτων ασφαλείας είναι πρωταρχικής σημασίας για τη διασφάλιση της ασφάλειας των οδηγών και των επιβατών. Η βασική ιδέα στην οποία βασίζονται οι επιθέσεις αυτές είναι η καθυστέρηση της μετάδοσης των μηνυμάτων αυτών ώστε να μην επιτευχθούν οι απαιτήσεις ασφάλειας που έχουν τεθεί. Ένα ενδεχόμενο σενάριο επίθεσης αυτής της κατηγορίας μπορεί να επιτευχθεί εξαναγκάζοντας νόμιμες οντότητες ITS να παρεμβάλλουν στη διαδικασία μετάδοσης των μηνυμάτων τους κακόβουλους κόμβους εισάγοντας έτσι σοβαρές καθυστερήσεις στη διαδικασία λήψης των μηνυμάτων από τις υπόλοιπες οντότητες. Το συνηθέστερο μέτρο αντιμετώπισης είναι η προσάρτηση χρονικής σήμανσης (timestamping) στα πακέτα που δεν πρέπει να υπόκεινται σε χρονικές καθυστερήσεις με αναπόφευκτη συνέπεια όμως τη χρήση πιο περίπλοκων μηχανισμών χρονικού συγχρονισμού (και άρα την αύξηση της πολυπλοκότητας).

4.4.3 Επιθέσεις στην ακεραιότητα και αντίμετρα

Ο κύριος στόχος της προστασίας της ακεραιότητας είναι να διασφαλιστεί ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται δεν μεταβάλλεται από κακόβουλους χρήστες κατά τη διαδικασία μετάδοσής τους. Ειδικότερα, στην απαίτηση της ακεραιότητας περιλαμβάνονται μηχανισμοί προστασίας από καταστροφή, μη εξουσιοδοτημένη δημιουργία και αλλοίωση των δεδομένων. Υπάρχουν ποικίλλες τεχνικές που μπορούν να χρησιμοποιηθούν για να πλήξουν την απαίτηση της ακεραιότητας, οπότε είναι προφανές ότι απαιτείται η παρουσία κατάλληλων μέτρων αντιμετώπισης αυτών. Η πιο διαδεδομένη λύση που χρησιμοποιείται ως αντίμετρο για

τη διασφάλιση της ακεραιότητας συνίσταται στην προσάρτηση μιας υπογραφής (signature) σε κάθε ανταλλαχθέν μήνυμα. Ωστόσο, αυτό το είδος προστασίας δεν μπορεί να εφαρμοστεί σε περιπτώσεις όπου υφίσταται μια διαδικασία συλλογής των δεδομένων (data aggregation). Ένας εξουσιοδοτημένος κόμβος του συστήματος μπορεί να είναι ευάλωτος τόσο σε εξωτερικές όσο και σε εσωτερικές επιθέσεις. Πολύ συχνά, οι επιπτώσεις που επιφέρει μια εξωτερική επίθεση είναι λιγότερες από επιπτώσεις που μπορεί να επιφέρει μια εσωτερική επίθεση. Στο πλαίσιο αυτό, οι κρυπτογραφικές συναρτήσεις κατακερματισμού αποτελούν την κύρια κρυπτογραφική μέθοδο για την αντιμετώπιση ζητημάτων ακεραιότητας. Στη συνέχεια, περιγράφονται εν συντομία αρκετά παραδείγματα επιθέσεων ακεραιότητας με τα αντίστοιχα αντίμετρά τους.

- **Επιθέσεις πλαστοπροσωπίας (masquerading attacks)**: Ο επιτιθέμενος προσαρτά στο όχημά του μια έγκυρη ταυτότητα (γνωστή και ως *μάσκα*) προκειμένου να εμφανίζεται στο δίκτυο ως αυθεντικοποιημένος κόμβος. Στη συνέχεια παράγει πλαστά μηνύματα τα οποία μεταδίδει σε γειτονικά οχήματα για την επίτευξη συγκεκριμένων στόχων, όπως την επιβράδυνση της ταχύτητάς τους. Σε ένα άλλο σενάριο επίθεσης ο κακόβουλος κόμβος αποκτά την ταυτότητα ενός οχήματος έκτακτης ανάγκης προκειμένου να εξαπατήσει τα υπόλοιπα οχήματα και να αποκτήσει προτεραιότητα έναντι αυτών. Ως λύση αντιμετώπισης τέτοιου είδους περιστατικών, προτείνεται η χρήση μιας λίστας ανάκλησης πιστοποιητικών στην οποία αποθηκεύεται το σύνολο ταυτοτήτων των οχημάτων τα οποία αποδεδειγμένα έχουν αναπτύξει στο παρελθόν κακόβουλη συμπεριφορά και η οποία διανέμεται σε όλους τους κόμβους του ITS δικτύου. Αν και η λύση αυτή μειώνει σημαντικά τις επιπτώσεις των επιθέσεων αυτής της κατηγορίας για να είναι αποτελεσματική απαιτεί την εφαρμογή μιας τεχνικής εντοπισμού κακόβουλων κόμβων.

- **Επιθέσεις αναπαραγωγής δεδομένων (data playback attacks)**: Αυτή η επίθεση συνίσταται στην επαναμετάδοση ενός μηνύματος αποσκοπώντας πιθανώς στην εκπομπή διαφορετικής θέσης για ένα όχημα από αυτήν στην οποία βρίσκεται πραγματικά ή στην τροποποίηση των εγγραφών που περιλαμβάνονται στους πίνακες δρομολόγησης για τα οχήματα-κόμβους του συστήματος. Η ανθεκτικότητα του συστήματος στο συγκεκριμένο είδος επίθεσης μπορεί να διασφαλιστεί μέσω της ενσωμάτωσης στις OBUs και τις RSUs κρυφής μνήμης (cache memory). Με τον τρόπο αυτό καθίσταται δυνατή η σύγκριση προσφάτως ληφθέντων μηνυμάτων με παλαιότερα ώστε να απορρίπτονται ενδεχόμενα διπλότυπα μηνύματα (π.χ. με χρήση αριθμών ακολουθίας ή πληροφοριών χρονικής σήμανσης). Επιπλέον, προκειμένου να κατοχυρωθεί ότι κάθε μήνυμα επεξεργάζεται μόνο μία φορά, μπορούν να χρησιμοποιηθούν tokens που εξασφαλίζουν μονοσήμαντη συσχέτιση με μια σύνοδο επικοινωνίας (session) δύο νόμιμων οντοτήτων και τυχαίων αριθμών μιας χρήσεως που χρησιμοποιούνται ευρέως σε κρυπτογραφικά σχήματα (nonces).

- **Επιθέσεις τροποποίησης δεδομένων (data alteration attacks)**: Αυτό το είδος επίθεσης στοχεύει στην παραβίαση της ακεραιότητας των ανταλλασσόμενων μηνυμάτων τροποποιώντας, διαγράφοντας ή δημιουργώντας εκ νέου το περιεχόμενό τους. Γενικά, ο εισβολέας παραποιεί τα ληφθέντα μηνύματα για την εξυπηρέτηση ιδίων σκοπών. Για παράδειγμα, σε ένα περιβάλλον έξυπνων μεταφορών, μια τέτοια επίθεση μπορεί να είναι η (ψευδής) σήμανση μιας διαδρομής ως κυκλοφοριακά επιβαρυμένης αποσκοπώντας στην εξαπάτηση των διερχόμενων οδηγών. Μια άλλη επικίνδυνη απειλή συνίσταται στην έγχυση στο δίκτυο ψευδών μηνυμάτων ασφαλείας, επηρεάζοντας έτσι την ασφάλεια των οδηγών και των οχημάτων τους. Ποικίλλες τεχνικές μπορούν να χρησιμοποιηθούν για την προστασία από απειλές αυτού του είδους, όπως οι υποδομές δημόσιου κλειδιού για δίκτυα οχημάτων (VPKI) ή η χρήση zero-knowledge τεχνικών για την διεκπεραίωση της διαδικασίας ελέγχου ταυτότητας μεταξύ των οχημάτων και για την ψηφιακή υπογραφή μηνυμάτων ITS. Μια άλλη αποτελεσματική μέθοδος συνίσταται στη δημιουργία ομαδικών επικοινωνιών όπου η διαχείριση των κλειδιών γίνεται από ένα σύστημα διαχείρισης κλειδιών ομάδας (GKM). Αυτό σημαίνει ότι ένας εισβολέας δεν θα πρέπει να είναι σε θέση να επικοινωνεί με τα μέλη της ομάδας.

- **Επιθέσεις «δηλητηρίασης» βάσης δεδομένων χαρτών (map database poisoning attack)**: Βάσει των ανταλλασσόμενων μηνυμάτων (π.χ. μηνύματα ασφαλείας μετάδοσης), κάθε OBU ενός κόμβου δημιουργεί και διατηρεί σε τοπικό επίπεδο μια βάση με δεδομένα που απεικονίζονται σε χάρτες για την παρακολούθηση των γειτονικών οχημάτων, την ενημέρωση για ενδεχόμενα ανακύπτοντα γεγονότα (π.χ. απεργίες, βλάβες στο δίκτυο) και για την προβολή διαφόρων σημείων ενδιαφέροντος (φαρμακεία, εστιατόρια, αρχαιολογικοί χώροι κτλ). Το σενάριο επίθεσης εν προκειμένω συνίσταται στην αποστολή κακόβουλων μηνυμάτων για να πληγεί η ακρίβεια των δεδομένων που διατηρούνται στις εν λόγω βάσεις δεδομένων επηρεάζοντας, ακολούθως, την ασφάλεια των χρηστών του ITS. Το κύριο αντίμετρο αποτελεί η επαλήθευση των ψηφιακών υπογραφών των ληφθέντων μηνυμάτων και ο εντοπισμός και η καταχώριση των στοιχείων των κόμβων που εμφανίζουν κακόβουλη συμπεριφορά σε κάποια λίστα αποκλεισμού (blacklist).

- **Επιθέσεις παραποίησης δεδομένων (data tampering attacks)**: Αυτή η επίθεση μπορεί να πραγματοποιηθεί από έναν εξουσιοδοτημένο χρήστη του συστήματος διαταράσσοντας την εύρυθμη λειτουργία αυτού και οδηγώντας σε επικίνδυνες καταστάσεις όπως την εμφάνιση ατυχημάτων. Το σενάριο επίθεσης στην περίπτωση αυτή συνίσταται στην απόκρυψη των πραγματικών μηνυμάτων ασφαλείας και την αντικατάστασή τους από ψευδή μηνύματα τα οποία στη συνέχεια διαχέονται στο δίκτυο. Το κύριο αντίμετρο είναι η ψηφιακή υπογραφή των μεταδιδόμενων μηνυμάτων ώστε να καθίσταται δυνατή η επαλήθευση της αυθεντικότητάς τους. Επιπλέον είναι αναγκαίος ένας μηχανισμός μη-

αποποίησης για τον εντοπισμό της ταυτότητας του επιτιθέμενου, η οποία θα πρέπει να προστεθεί στα CRL .

- **Επιθέσεις τύπου Man-in-the-middle**: Όπως υποδηλώνεται και στο όνομα ο επιτιθέμενος τοποθετεί τον εαυτό του στο τμήμα της επικοινωνίας που βρίσκεται μεταξύ του πομπού και του δέκτη. Στα ITS περιβάλλοντα, ο εισβολέας μπορεί να έχει τη μορφή μιας OBU ή μιας RSU η οποία τοποθετείται μεταξύ δύο οχημάτων που επικοινωνούν. Ο επιτιθέμενος ελέγχει την επικοινωνία μεταξύ των δύο επικοινωνουσών οντοτήτων την ίδια στιγμή που οι ίδιες αγνοούν την παρουσία του και θεωρούν ότι βρίσκονται σε άμεση επικοινωνία μεταξύ τους. Το αντίμετρο στην περίπτωση αυτή είναι η χρήση ψηφιακών πιστοποιητικών ώστε να είναι δυνατός ο έλεγχος της ταυτότητας των νόμιμων χρηστών.

4.4.4 Επιθέσεις στην εμπιστευτικότητα και αντίμετρα

Η εμπιστευτικότητα των μηνυμάτων τίθεται ως απαίτηση από ορισμένες εφαρμογές όπως αυτές που παρέχουν στους χρήστες υπηρεσίες πλοήγησης στον παγκόσμιο ιστό και επιτυγχάνεται με την κρυπτογράφηση των μηνυμάτων που μεταδίδονται μεταξύ των οχημάτων και των RSUs. Ωστόσο, όταν τα ανταλλασσόμενα μηνύματα δεν περιέχουν ευαίσθητες η διασφάλιση του απορρήτου του περιεχομένου τους δεν είναι αναγκαία. Πολλές επιθέσεις μπορούν να επηρεάσουν το δίκτυο εφόσον απουσιάζουν μηχανισμοί προστασίας της εμπιστευτικότητας. Μερικές από τις επιθέσεις αυτές είναι οι εξής:

- **Επιθέσεις υποκλοπής (eavesdropping attacks)**: Μια επίθεση υποκλοπής επηρεάζει μόνο την εμπιστευτικότητα του δικτύου και όχι τους πόρους και τη διαθεσιμότητά του. Αυτό το είδος επίθεσης επιτρέπει στον επιτιθέμενο να εξαγάγει πληροφορίες «ευαίσθητου» περιεχομένου από τα μεταδιδόμενα πακέτα όπως πληροφορίες θέσης των οχημάτων. Για την παροχή προστασίας ενάντια σε αυτό το είδος επίθεσης, όλα τα δεδομένα που είναι ζωτικής σημασίας για το σύστημα πρέπει να κρυπτογραφούνται έτσι ώστε να διασφαλίζεται το απόρρητο των επικοινωνιών των εμπλεκόμενων οντοτήτων.

- **Επιθέσεις υποκλοπής δεδομένων (data interception attacks)**: Αυτή η επίθεση επηρεάζει εκτός από την εμπιστευτικότητα των δεδομένων και την ιδιωτικότητα των χρηστών. Συνίσταται στην παθητική παρακολούθηση του δικτύου για συγκεκριμένη χρονική διάρκεια και ακολούθως στην ανάλυση των δεδομένων κίνησης που έχουν συλλεχθεί για την εξαγωγή του μέγιστου όγκου χρήσιμων πληροφοριών. Ως αντίμετρο μπορεί να χρησιμοποιηθεί το ίδιο με αυτό των επιθέσεων υποκλοπής.

- **Επιθέσεις εξαντλητικής αναζήτησης (brute force attacks)**: Οι επιθέσεις εξαντλητικής αναζήτησης στοχεύουν στην παραβίαση της εμπιστευτικότητας των μεταδιδόμενων δεδομένων και στην καταστρατήγηση της διαδικασίας της αυθεντικοποίησης των οχημάτων-χρηστών του συστήματος. Για παράδειγμα, η επίθεση αυτή μπορεί να αποκαλύψει το αναγνωριστικό δικτύου του οχήματος χρησιμοποιώντας διάφορες μεθόδους εξαντλητικής αναζήτησής του από κάποιο λεξικό όρων (dictionary attacks). Ωστόσο, λόγω της δυναμικής φύσης του ITS δικτύου, ο χρόνος επικοινωνίας μεταξύ των οντοτήτων είναι σχετικά σύντομος και, ως εκ τούτου, η συγκεκριμένη επίθεση δεν είναι εύκολο να πραγματοποιηθεί, καθώς είναι χρονοβόρα και κοστοβόρα στους πόρους. Επιπλέον, η διεξαγωγή της συγκεκριμένης επίθεσης καθίσταται δυσκολότερη εφόσον γίνεται χρήση ισχυρότερων αλγορίθμων κρυπτογράφησης και αντιστοίχως ισχυρών αλγορίθμων δημιουργίας κλειδιών.

4.5. Ζητήματα ιδιωτικότητας στα έξυπνα συστήματα μεταφορών

Ένα από τα θεμελιώδη ανθρώπινα δικαιώματα που χρήζουν διαφύλαξης σε μια κοινωνία είναι, εκτός από την ασφάλεια, το δικαίωμα των πολιτών της στην ιδιωτικότητα. Ήδη από το 1890 οι Αμερικανοί δικαστές Warren και Brandeis συνηγόρησαν υπέρ του δικαιώματος κάθε ατόμου σε μια «*ανενόχλητη ιδιωτική ζωή*» (Brandeis & Warren, 1890). Ειδική μνεία για την ιδιωτικότητα γίνεται και στο άρθρο 12 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου όπου αναφέρονται τα εξής: «*Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους*» (UN General Assembly, 1948)

Η ιδιωτικότητα αποτελεί κρίσιμη απαίτηση για τα ITS. Σε αυτήν την ενότητα, ορίζουμε ζητήματα ιδιωτικότητας που ανακύπτουν σε τρεις (3) θεματικές περιοχές: απόρρητο ταυτότητας (identity privacy), απόρρητο συμπεριφοράς (behavior privacy) και απόρρητο τοποθεσίας (location privacy).

4.5.1 Ιδιωτικότητα ταυτότητας (Identity privacy)

Όταν αναφερόμαστε σε ιδιωτικότητα ταυτότητας στα περιβάλλοντα έξυπνων μεταφορών εννοούμε την προστασία της πραγματικής ταυτότητας (ονοματεπώνυμο, αριθμός άδειας οδήγησης οδηγού, αριθμός κυκλοφορίας του αυτοκινήτου) των διαφόρων οντοτήτων που συνυπάρχουν στο πλαίσιο ενός συστήματος μεταφορών (οδηγοί, ταξιδιώτες, επιβάτες, πεζοί). Ένα από τα πιο διαδεδομένα τεχνολογικά μέσα που χρησιμοποιούνται για τον σκοπό αυτό αποτελεί η χρήση ψευδωνύμων, γνωστών και ως ψευδο-αναγνωριστικών, τα οποία αντικαθιστούν τα πραγματικά στοιχεία της ταυτότητας κάθε οντότητας κατά τη διαδικασία συσχέτισης αυτής με το όχημά της. Τα ψευδώνυμα έχουν τη δυνατότητα να προστατεύουν μηνύματα που φέρουν κρίσιμες

πληροφορίες ασφαλείας, όπως η θέση του οχήματος ή η ταυτότητα του αποστολέα τους. Ωστόσο, έχει αποδειχθεί ότι όταν τα οχήματα εφαρμόζουν απλές υλοποιήσεις σχημάτων παραγωγής και χρήσης ψευδωνύμων για την προστασία της ταυτότητας τους παραμένει εφικτή η παρακολούθησή τους από κακόβουλες οντότητες (Wiedersheim, Ma, Kargl, & Papadimitratos, 2010). Για την αντιμετώπιση περιστατικών αυτού του είδους είναι απαραίτητη η συμμόρφωση με καλές πρακτικές αναφορικά με τον τρόπο και τον χρονικό διάστημα αλλαγής του ψευδωνύμου ενός οχήματος.

Μια εναλλακτική μέθοδος που χρησιμοποιείται αντί της χρήσης ψευδώνυμων για την προστασία της ταυτότητας ενός χρήστη είναι η χρήση διαπιστευτηρίων βάσει συγκεκριμένων χαρακτηριστικών (attribute-based credentials). Η τεχνική αυτή επιτρέπει στους χρήστες να αυθεντικοποιούνται σε επαληθευτές-επικυρωτές ταυτότητας παρέχοντας κάθε φορά μόνο εκείνα τα χαρακτηριστικά από τα διαπιστευτήριά τους που σχετίζονται με τον εκάστοτε επαληθευτή (Camenisch, Lehmann, Neven, & Rial, 2014). Ωστόσο, η συγκεκριμένη μέθοδος ταυτοποίησης παρουσιάζει υψηλές απαιτήσεις σε πόρους προϋποθέτοντας επίσης τη δημιουργία διαμοιραζόμενων μυστικών/χαρακτηριστικών για το σύνολο των επιθυμητών υπηρεσιών. Συνεπώς, υφίσταται ένα είδος αντιστάθμισης (tradeoff) μεταξύ της προστασίας της ιδιωτικότητας των συμμετεχόντων σε ένα ITS και της απαίτησης μη αποποίησης (non-repudiation), η οποία είναι απαραίτητη για να είναι εφικτός ο προσδιορισμός των χρηστών του συστήματος σε περιπτώσεις που ενέχουν καθεστώς απόδοσης ευθυνών (π.χ. τροχαία ατυχήματα).

4.5.2 Ιδιωτικότητα συμπεριφοράς (Behaviour privacy)

Δεδομένης της αφθονίας των προσωπικών πληροφοριών ποικίλης φύσεως που χρησιμοποιούνται σε ένα οικοσύστημα μεταφορών (από οικονομικά δεδομένα και πληροφορίες τοποθεσίας έως και τα μοτίβα συμπεριφοράς που αναπτύσσουν οι χρήστες του συστήματος) είναι ευνόητο ότι η απαίτηση της ιδιωτικότητας όσον αφορά τη συμπεριφορά των χρηστών τίθεται σε κίνδυνο. Σύμφωνα με τους (Finn, Wright, & Friedewald, 2013) στα πλαίσια των έξυπνων συστημάτων μεταφορών, η ιδιωτικότητα συμπεριφοράς αναφέρεται στην ιδιωτικότητα των δεδομένων που περιγράφουν διάφορες πτυχές της προσωπικότητας μιας ομάδας ή μεμονωμένων ατόμων και τις ενέργειές στις οποίες αυτοί προβαίνουν εντός του ITS. Για να προφυλάσσει ένα σύστημα την ιδιωτικότητα της συμπεριφοράς, πρέπει να έχει τη δυνατότητα να ανωνυμοποιεί και να προστατεύει τα δεδομένα των χρηστών που συλλέγονται από ανεπιθύμητη χρήση ή αποκάλυψη, καθώς και να αποκρύπτει μοτίβα συμπεριφοράς των χρηστών του ITS.

Η προστασία της ιδιωτικότητας των ενεργειών στις οποίες προβαίνουν οι χρήστες εντός του ITS είναι απαραίτητη για να αποτρέψει τους επίδοξους επιτιθέμενους από απόπειρες παρακολούθησης και εξαγωγής συμπερασμάτων για συγκεκριμένα άτομα μέσα στο σύστημα. Καθώς το ITS καταγράφει πληροφορίες σχετικές με τις αγαπημένες διαδρομές των χρηστών προκειμένου να προσδώσει στις

μετακινήσεις τους τα θεμιτά στοιχεία της ασφάλειας και της αποτελεσματικότητας, καταγράφονται επίσης τα μοτίβα κίνησης αυτών. Όπως γίνεται αντιληπτό, από την ανάλυση του τελευταίου είδους πληροφοριών ένας επίδοξος επιτιθέμενος μπορεί να εξαγάγει χρήσιμα συμπεράσματα σχετικά με τη συμπεριφορά κάθε χρήστη. Για παράδειγμα, από την ανάλυση δεδομένων τοποθεσίας χρηστών όπως το ιστορικό των αφετηριών και των προορισμών στους οποίους έχει μεταβεί με το όχημά του μπορεί ένας επιτιθέμενος να προσδιορίσει τον τόπο διαμονής ή το χώρο εργασίας ενός χρήστη.

Μια πιο μοντέρνα προσέγγιση που μπορεί να χρησιμοποιηθεί για τη διαφύλαξη της ιδιωτικότητας των χρηστών ενός ITS είναι η προστασία της ιδιωτικότητας με χρήση μηχανισμών "διαφορικού απορρήτου" (differential privacy). Η συγκεκριμένη προσέγγιση αποτελεί ένα είδος ανωνυμοποίησης στο οποίο διαφοροποιούνται με τυχαίο τρόπο κάποια από τα αναγνωριστικά στοιχεία ταυτότητας των υποκειμένων των δεδομένων που μπορεί να βρίσκονται αποθηκευμένα σε μια βάση δεδομένων. Έτσι, ενώ μπορεί να συσχετίζονται λανθασμένες πληροφορίες με μεμονωμένα υποκείμενα, το συνολικό αποτέλεσμα που προκύπτει από την εκτέλεση ενός δεδομένου αλγορίθμου πάνω στα δεδομένα αυτά παραμένει το ίδιο αυτό που παράγεται όταν ο αλγόριθμος εφαρμόζεται στα πραγματικά δεδομένα. Την τεχνική αυτή χρησιμοποιούν πολλές μεγάλες εταιρίες όπως η Google (Newman, 2019), η Apple (Differential Privacy Team, Apple, n.d.) και η Uber (Greenberg, 2017). Ωστόσο, η διαφορική ιδιωτικότητα αντιμετωπίζει σοβαρά ζητήματα ιδίως όταν χρησιμοποιούνται δεδομένα με αναδρομικό τρόπο ή δεδομένα χρονοσειρών (Kargl, Friedman, & Boreli, 2013).

4.5.3 Ιδιωτικότητα τοποθεσίας (Location privacy)

Χρησιμοποιώντας τον ορισμό των (Finn, Wright, & Friedewald, 2013) η ιδιωτικότητα της τοποθεσίας στο πλαίσιο των έξυπνων συστημάτων μεταφορών θα μπορούσε να περιγραφεί ως το δικαίωμα ενός χρήστη να ταξιδεύει ή να μετακινείται εντός του συστήματος χωρίς να ανησυχεί ότι τα δεδομένα τοποθεσίας του θα κοινοποιηθούν σε τρίτους χωρίς ο ίδιος να το γνωρίζει και να έχει συγκατατεθεί ρητά για αυτό. Ενώ οι πληροφορίες τοποθεσίας είναι επωφελείς για τα ITS προκειμένου να παράσχουν στους χρήστες τους χρήσιμες υπηρεσίες που βασίζονται στην τοποθεσία τους (π.χ. προβολή κοντινών εστιατορίων, φαρμακείων ή χώρων διασκέδασης), τέτοιου είδους πληροφορίες μπορούν επιπροσθέτως να χρησιμοποιηθούν για να προσβάλλουν την ιδιωτικότητα των ατόμων. Χρησιμοποιώντας αυτές τις πληροφορίες τοποθεσίας, κακόβουλα άτομα μπορούν να πραγματοποιήσουν επιθέσεις στοχεύοντας μεμονωμένους χρήστες του συστήματος. Είναι εξαιρετικά δύσκολο για συστήματα πλοήγησης που βασίζονται σε τεχνολογίες γεωγραφικού εντοπισμού (GPS) να παρέχουν απρόσκοπτα τις υπηρεσίες τους διατηρώντας παράλληλα την ιδιωτικότητα των δεδομένων τοποθεσίας των χρηστών. Ωστόσο, είναι επιβεβλημένη η εξεύρεση της κατάλληλης ισορροπίας μεταξύ της παροχής ωφέλιμων υπηρεσιών υψηλής γεωγραφικής ακρίβειας στους χρήστες και την προάσπιση του δικαιώματός τους στην ιδιωτικότητα της τοποθεσίας τους. Σύμφωνα με τους (Yigitoglu, Damiani, Abul, & Silvestri, 2012) η απόκρυψη τοποθεσίας (location obfuscation) αποτελεί μια

διαδεδομένη τεχνική που χρησιμοποιείται για τη διαφύλαξη της ιδιωτικότητας της τοποθεσίας του χρήστη κατά τη χρήση υπηρεσιών που βασίζονται σε δεδομένα τοποθεσίας. Αυτό επιτυγχάνεται με την ελαφρά τροποποίηση ή γενικοποίηση[6] της τοποθεσίας του χρήστη ούτως ώστε να αποφευχθεί η αποκάλυψη της πραγματικής θέσης του.

4.5.4 Κατηγοριοποίηση μηχανισμών ιδιωτικότητας στα ITS

Στα ITS, η αυθεντικότητα της επικοινωνίας διασφαλίζεται μέσω των στοιχείων ταυτότητας των εξουσιοδοτημένων χρηστών του συστήματος. Απαιτούνται όμως τεχνικές διαφύλαξης της ιδιωτικότητας των χρηστών, προκειμένου να διασφαλιστεί ότι οι προσωπικές τους πληροφορίες δεν θα αποκαλυφθούν σε τρίτους. Οι ψηφιακές υπογραφές (digital signatures) δεν αποτελούν κατάλληλες λύσεις για την επίτευξη του στόχου αυτού, διότι αφενός δεν προασπίζουν την ανωνυμία των χρηστών που τις χρησιμοποιούν[7] και αφετέρου δεν πληρούν την απαίτηση της μη-συνδεσιμότητας (unlikability) μεταξύ αυτών και των εκδοθουσών υπογραφών[8]. Ωστόσο, το γεγονός ότι δεν μπορούν να πλαστογραφηθούν (unforgeability) εγγυώνται ότι η υπογράφουσα οντότητα αποτελεί τον αποστολέα του υπογεγραμμένου εγγράφου. Προκειμένου να επιτευχθούν τόσο η αυθεντικότητα όσο και η ιδιωτικότητα των χρηστών είναι απαραίτητη η αποσύνδεση της διαδικασίας δημόσιας επαλήθευσης της ταυτότητας ενός υπογράφοντα χρήστη από τις πληροφορίες που τον προσδιορίζουν μοναδικά.

Οι κυριότερες τεχνικές που χρησιμοποιούνται στην κατεύθυνση αυτή είναι η προστασία της ιδιωτικότητας με χρήση μεθόδων που βασίζονται στην ανωνυμία, η προστασία της ιδιωτικότητας με χρήση κρυπτογραφικών μεθόδων και η προστασία της ιδιωτικότητας με χρήση μεθόδων που βασίζονται σε μεθόδους διατάραξης (perturbation).

Οι (Qiu, Wu, & Chen, 2015) επεσήμαναν ποικίλλες τεχνικές (π.χ. T-closeness, L-diversity, and K-anonymity) που στηρίζουν τη λειτουργία τους στη διασφάλιση του χαρακτηριστικού της ανωνυμίας προκειμένου να προστατέψουν την ιδιωτικότητα των χρηστών. Θα πρέπει βέβαια να σημειωθεί ότι η ασφάλεια των τεχνικών αυτών μπορεί να επηρεαστεί με χρήση μεθόδων ανάλυσης ροών δεδομένων (data traffic analysis).

---

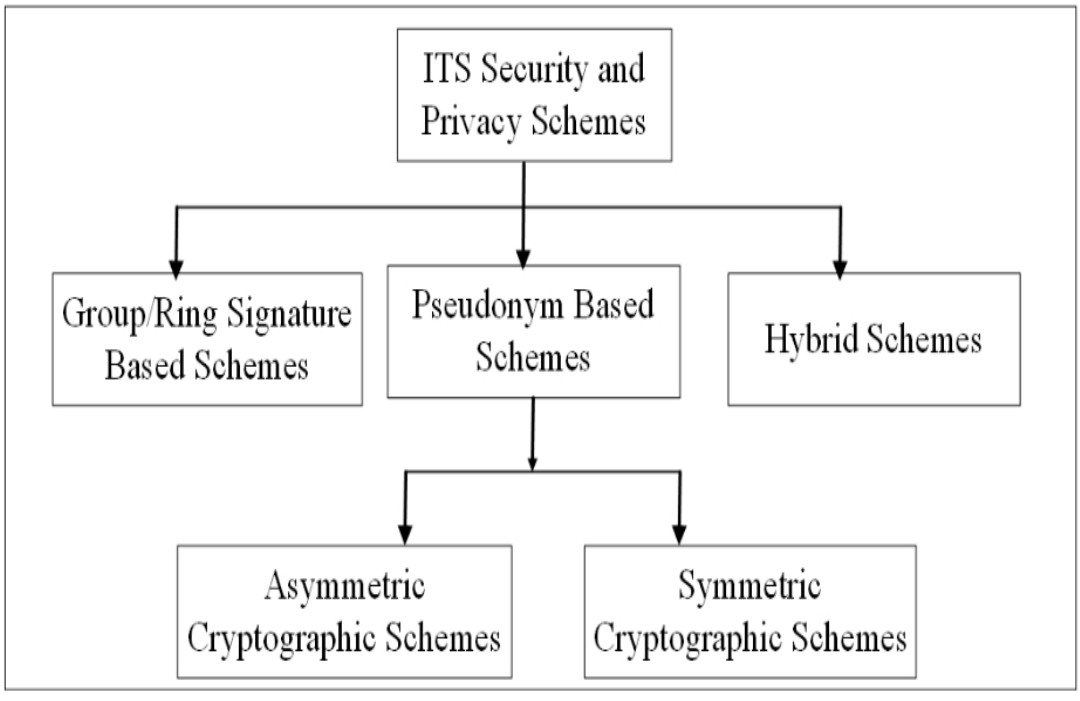
[6] Η γενικοποίηση (generalization) αποτελεί μια τεχνική ανωνυμοποίησης που αποσκοπεί στην απόκρυψη της ταυτότητας των μεμονωμένων ατόμων μέσω της ένταξής τους σε μια μεγαλύτερη ομάδα με άτομα που εμφανίζουν παρόμοια χαρακτηριστικά-αναγνωριστικά ταυτότητας (π.χ. αντικατάσταση του Τ.Κ μιας συγκεκριμένης συνοικίας με τον Τ.Κ. μιας ολόκληρης πόλης).

[7] Μια ψηφιακή υπογραφή (s) που εκδίδεται από κάποιον χρήστη (u) που διαθέτει ψηφιακό πιστοποιητικό (digital certificate) αποκαλύπτει την ταυτότητα του υπογράφοντος σε όλους τους πιθανούς επαληθευτές.

[8] Αυτό συμβαίνει διότι πολλαπλές ψηφιακές υπογραφές (s_1, ..., s_n) επί των αντίστοιχων μηνυμάτων (m_1, ..., m_n) που δημιουργούνται από τον ίδιο υπογράφοντα σε διαφορετικά περιβάλλοντα μπορούν να συσχετιστούν με αυτόν αποκαλύπτοντας περισσότερες πληροφορίες που τον αφορούν (οι οποίες μπορούν στη συνέχεια να χρησιμοποιηθούν με κακόβουλο τρόπο π.χ. για σκοπούς κατάρτισης προφίλ).

Όσον αφορά τις κρυπτογραφικές μεθόδους προστασίας (π.χ. πρωτόκολλα μηδενικής γνώσης, διαμοιρασμός μυστικής ποσότητας, ομομορφική κρυπτογράφηση) διασφαλίζουν μεν την εμπιστευτικότητα των προσωπικών πληροφοριών των χρηστών τους χωρίς όμως να εγγυώνται και το απόρρητο της τοποθεσίας των οχημάτων τους. Ομοίως, η προστασία της ιδιωτικότητας με χρήση μεθόδων διατάραξης - όπως ο διαμοιρασμός πληροφοριών ή η παραμετροποίηση των πληροφοριών κάθε χρήστη βάσει των ενδιαφερόντων του- επιτυγχάνεται μεταβάλλοντας την ακολουθία των αποσταλμένων πληροφοριών. Ωστόσο με τη χρήση perturbation τεχνικών η κρίσιμη δυνατότητα της ανάκλησης στα ITS περιβάλλοντα δεν μπορεί να επιτευχθεί αποδοτικά από άποψη χρόνου. Ως εκ τούτου, η απαίτηση της προστασίας της ιδιωτικότητας δεν εξυπηρετείται σε ITS περιβάλλοντα από τεχνικές διατάραξης.

Προκειμένου να δημιουργηθεί ένα πλήρως αξιόπιστο σύστημα για την προστασία της ιδιωτικότητας πρέπει να ληφθούν υπόψη οι απαιτήσεις εμπιστευτικότητας, ακεραιότητας, αυθεντικοποίησης και μη αποποίησης. Λαμβάνοντας υπόψη τα προαναφερθέντα χαρακτηριστικά, αρκετοί ερευνητές έχουν καταβάλει κάθε δυνατή προσπάθεια για την ενσωμάτωσή αυτών στο σχεδιασμό των συστημάτων ασφαλείας για ITS. Στα πλαίσια της παρούσας εργασίας, όπως φαίνεται και στην Εικόνα 8, θα εξετάσουμε τις εξής κατηγορίες-σχήματα ιδιωτικότητας: (i) σχήματα βάσει ομάδων / δακτυλίων, (ii) σχήματα ψευδώνυμων και (iii) υβριδικά σχήματα. Η αξιολόγηση των συστημάτων ασφάλειας και ιδιωτικότητας στα ITS, αποτιμάται με βάση τα εξής κριτήρια: (i) επεκτασιμότητα, (ii) ασφάλεια / ιδιωτικότητα, (iii) υπολογιστικό κόστος, (iv) χρονική καθυστέρηση και (v) συνολική επιβάρυνση (κόστη) από τις διαδικασίες επικοινωνίας.



***Εικόνα 8**: Κατηγοριοποίηση σχημάτων ιδιωτικότητας στα ITS (Ali, Ahmad, Malik, Ali, & Rehman, 2018)*

4.5.4.1 Σχηματα ιδιωτικοτητας βασισμενα σε ομαδικες ψηφιακες υπογραφες (Group/Ring signature-based privacy schemes)

Το μοντέλο αρχιτεκτονικής σε ένα σχήμα ομαδικής υπογραφής αποτελείται από μια οντότητα που έχει τον ρόλο του διαχειριστή της ομάδας (*group manager*) και τα μέλη αυτής. Ο διαχειριστής της ομάδας είναι υπεύθυνος για τη δημιουργία της και έχει ως καθήκοντα την αποδοχή και -σε ορισμένα σχήματα- την ανάκληση των μελών της. Κατά τη διαδικασία δημιουργίας της, ο διαχειριστής επιλέγει το δικό του μυστικό κλειδί καθορίζοντας παράλληλα τις παραμέτρους που θα πρέπει να περιέχει το ομαδικό δημόσιο κλειδί (*group public key*). Αφού ολοκληρωθεί η διαδικασία καθορισμού των παραμέτρων, ο διαχειριστής μπορεί να χρησιμοποιήσει το μυστικό του κλειδί για να εκδώσει πιστοποιητικά μέλους (*group membership certificates*) κατά το στάδιο της αποδοχής των υποψηφίων μελών της ομάδας. Επομένως, κάθε μέλος της ομάδας διαθέτει το δικό του πιστοποιητικό μέλους (Chaum & Van Heyst, 1991) το οποίο συγχρόνως αποτελεί το ιδιωτικό του κλειδί του στην υπογραφή που εκδίδει εκ μέρους ολόκληρης της ομάδας. Αυτή η ομαδική υπογραφή μπορεί στη συνέχεια να επαληθευτεί από οποιονδήποτε χρησιμοποιώντας το δημόσιο ομαδικό κλειδί. Κατ' αυτόν τον τρόπο παρέχεται ανωνυμία στον πραγματικό υπογράφοντα δίχως να αποκαλύπτονται προσωπικές πληροφορίες που δυνητικά θα μπορούσαν να συνδυαστούν μεταξύ τους προκειμένου να συνδεθούν τελικά με έναν χρήστη[9]. Ωστόσο, προκειμένου να διασφαλιστεί η απαίτηση της λογοδοσίας, είναι απαραίτητη η ύπαρξη μιας έμπιστης οντότητας, η οποία θα μπορεί ανά πάσα στιγμή να συσχετίζει την ομαδική υπογραφή με την πραγματική ταυτότητα του υπογράφοντος. Στα περισσότερα σχήματα ομαδικών υπογραφών τον ρόλο αυτό κατέχει ο διαχειριστής της ομάδας ο οποίος προσδιορίζει την πραγματική ταυτότητα των χρηστών-μελών που υπογράφουν ένα μήνυμα χρησιμοποιώντας τις πληροφορίες που συνελέχθησαν κατά το στάδιο αποδοχής τους ως μέλη της ομάδας.

Μια από τις πλέον διαδεδομένες τεχνικές που χρησιμοποιείται στα ITS περιβάλλοντα και βασίζεται στη λογική της ομαδικής υπογραφής έχει προταθεί από τους (Zhu, Jiang, Wang, & Li, 2014) οι οποίοι εισηγήθηκαν τη χρήση ασύμμετρης κρυπτογραφίας για τη διασφάλιση της ιδιωτικότητας των χρηστών.

Επιπλέον, οι (Zhang, Wu, Solanas, & Domingo-Ferrer, 2010) περιγράφουν ένα αποκεντρωμένο μοντέλο για την δημιουργία ομαδικής ψηφιακής υπογραφής των μελών της ομάδας. Στο μοντέλο αυτό, η RSU ενεργεί ως διαχειριστής μιας ομάδας οχημάτων. Ωστόσο, η συγκεκριμένη προσέγγιση καθίσταται ευάλωτη σε side-channel επιθέσεις.

[9] Επομένως πληρείται και η απαίτηση της μη-συνδεσιμότητας (unlinkability).

Οι (Huang, Yeh, & Chien, 2011) περιέγραψαν ένα σχήμα το οποίο στηρίζεται σε τεχνικές ελλειπτικών καμπυλών από το πεδίο της κρυπτογραφίας με στόχο την ταυτοποίηση ομάδων οχημάτων και παράλληλη μείωση του κόστους αυθεντικοποίησης που προκύπτει από τις χρησιμοποιούμενες ψηφιακές υπογραφές. Ωστόσο και η τεχνική αυτή καθίσταται επιρρεπής σε επιθέσεις τύπου άρνησης υπηρεσιών (DoS).

Στοχεύοντας στην όσο το δυνατόν μεγαλύτερη μείωση του υπολογιστικού χρόνου που δαπανάται κατά τον έλεγχο εγκυρότητας των υπογραφών μιας ομάδας οχημάτων μέσω των RSUs, οι (Zhang, Lin, Lu, Ho, & Shen , 2008) παρουσίασαν μια τεχνική στην οποία γίνεται χρήση ψευδώνυμων προκειμένου να επιτευχθεί η ανωνυμία των χρηστών. Εξαιτίας ωστόσο του γεγονότος ότι οι RSUs βρίσκονται εξ ορισμού σε μη φυλασσόμενο περιβάλλον είναι εύλογο να υποθέσουμε ότι καθίστανται ευάλωτες σε φυσικές επιθέσεις από κακόβουλες οντότητες. Επιπλέον, όπως και στα προηγούμενα σχήματα, έτσι και εδώ εμφανίζεται η απειλή των επιθέσεων τύπου DoS, αφού είναι εξαιρετικά εύκολη η έγχυση πλαστών μηνυμάτων στο δίκτυο .

Ομοίως, ο μηχανισμός που παρουσιάζεται από τους (Horng, et al., 2013), παρέχει έναν πολύ ισχυρό μηχανισμό ελέγχου της αυθεντικότητας των μηνυμάτων επιτυγχάνοντας συγχρόνως μικρότερα κόστη επιβάρυνσης κατά τις διαδικασίες αποστολής μηνυμάτων (message overheads) . Ωστόσο, ο μηχανισμός είναι επιρρεπής σε επιθέσεις τύπου Sybil καθώς και σε επιθέσεις επαναπροώθησης μηνυμάτων (replay attacks).

Οι (Hao, Cheng, Zhou, & Song, 2011) πρότειναν το συνεργατικού τύπου πρωτόκολλο ελέγχου ταυτότητας μηνυμάτων (CMAP). Το CMAP μειώνει τα διάφορα είδη κόστους (υπολογιστικά, μετάδοσης), χωρίς ωστόσο να πληροί την ιδιότητα της μη αποποίησης. Επιπλέον, με το CMAP οι διάφορες ομάδες οχημάτων μπορούν να επαληθεύσουν μόνο την αυθεντικότητα των μηνυμάτων, ενώ άλλα οχήματα απλώς αποδέχονται άκριτα τα μηνύματα από μια ομάδα επαλήθευσης της εγκυρότητάς τους. Ωστόσο, εάν η ταυτότητα οποιουδήποτε μέλους της ομάδας επαλήθευσης υποκλαπεί, τίθεται αυτομάτως σε κίνδυνο η εν συνόλω ασφάλεια του ITS.

Για τη μείωση του υπολογιστικού κόστους καθώς και των επιβαρύνσεων που συνάγονται από τα διάφορα είδη επικοινωνίας που αναπτύσσονται στα διάφορα σχήματα ομαδικών υπογραφών, οι (Lin & Li, 2013) παρουσίασαν μια προσέγγιση ομαδικής αυθεντικοποίησης οχημάτων. Με αυτήν την τεχνική, μειώθηκε σημαντικά τόσο το υπολογιστικό κόστος όσο και το κόστος μετάδοσης, ωστόσο για άλλη μια φορά υπάρχει ο κίνδυνος που προκύπτει από επιθέσεις τύπου DoS.

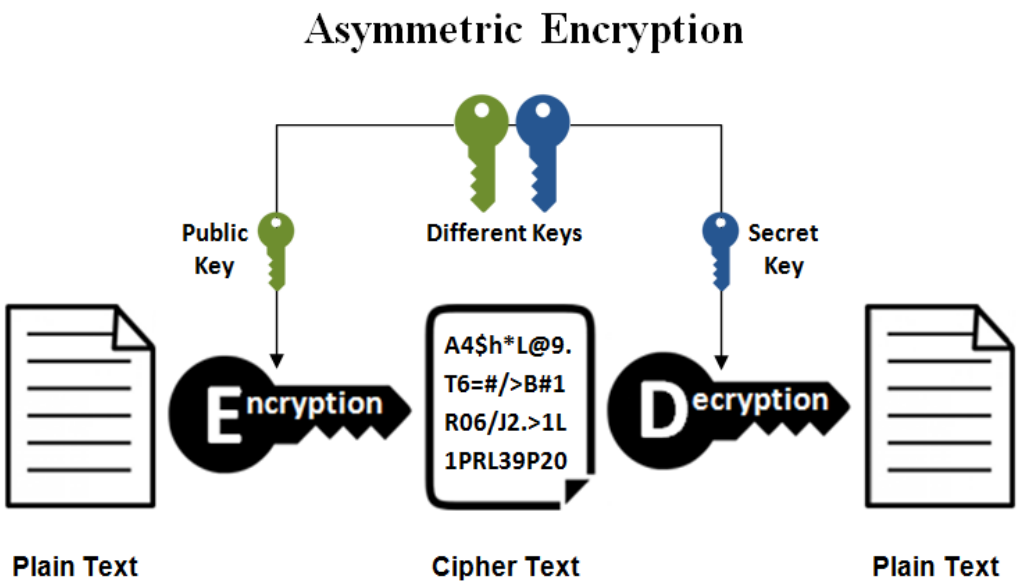
Συνοψίζοντας, γίνεται αντιληπτό ότι ορισμένα σχήματα δημιουργίας ομαδικών υπογραφών χαρακτηρίζονται μεν από επαρκές επίπεδο ασφάλειας αλλά με υψηλό

υπολογιστικό κόστος, ενώ σε άλλα η υπολογιστική επιβάρυνση μπορεί να είναι μεν χαμηλή, ωστόσο εξίσου χαμηλό είναι και το επίπεδο ασφάλειας.

4.5.4.2 Σχηματα ιδιωτικοτητας με χρηση ψευδωνυμων (Pseudonym-based privacy schemes)

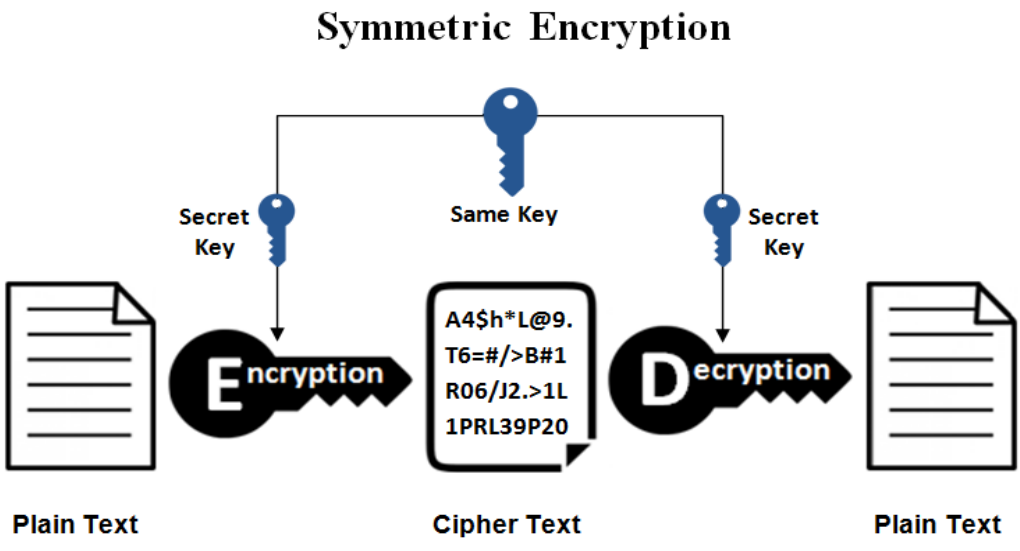
Όπως προκύπτει και από την ονομασία τους, τα εν λόγω σχήματα αντικαθιστούν την πραγματική ταυτότητα κάθε οχήματος-κόμβου με ένα ψευδώνυμο (pseudonym) προκειμένου να παράσχουν ανωνυμία. Τα σχήματα που βασίζονται σε ψευδώνυμα κατηγοριοποιούνται σε ασύμμετρα κρυπτογραφικά σχήματα και σε συμμετρικά κρυπτογραφικά σχήματα. Για τη διασφάλιση της αξιοπιστίας στους διάφορους τύπους επικοινωνιών που αναπτύσσονται μεταξύ των οχημάτων και των διακομιστών ενός έξυπνου συστήματος μεταφορών, είναι αναγκαία η ενσωμάτωση κατάλληλων μηχανισμών επαλήθευσης της ταυτότητας των οντοτήτων και της ακεραιότητας των μηνυμάτων που ανταλλάσσουν μεταξύ τους. Υπάρχουν διάφορα κρυπτογραφικά πρωτόκολλα που μπορούν να χρησιμοποιηθούν για την επίτευξη των δύο προαναφερθέντων στόχων στα ITS περιβάλλοντα. Συνοπτικά, τα πρωτόκολλα αυτά περιλαμβάνουν κρυπτογραφικές τεχνικές δημόσιου κλειδιού (ασύμμετρης κρυπτογραφίας) και κρυπτογραφικές τεχνικές ιδιωτικού κλειδιού (συμμετρικής κρυπτογραφίας).

- **Τεχνικές κρυπτογράφησης με χρήση δημόσιων κλειδιών**: Όπως φαίνεται στην Εικόνα 9, χρησιμοποιούνται δύο τύποι κλειδιών, ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι γνωστό σε όλους τους εμπλεκόμενους και χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων. Ομοίως, το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση και είναι γνωστό μόνο στον παραλήπτη του μηνύματος. Τα ζεύγη κλειδιών στα ITS περιβάλλοντα δημιουργούνται από κάποια αναγνωρισμένη αρχή έκδοσης πιστοποιητικών (CA). Συγκεκριμένα, η CA εκδίδει πιστοποιητικά σε οχήματα για να διασφαλίσει την αξιόπιστη επικοινωνία μεταξύ τους. Η CA μπορεί να δημιουργήσει μια λίστα ανάκλησης πιστοποιητικών εάν οποιοδήποτε όχημα παραβιάζει τους κανόνες της (π.χ. λήξη πιστοποιητικού, ενδεχόμενη συμμετοχή του οχήματος σε κακόβουλες δραστηριότητες, αποκάλυψη κλειδιών κτλ.). Η CRL περιλαμβάνει πληροφορίες σχετικά με τα ανακληθέντα πιστοποιητικά.



Εικόνα 9: Σχήμα ασύμμετρης κρυπτογραφίας

- **Τεχνικές συμμετρικής κρυπτογραφίας** : Όπως φαίνεται και στην Εικόνα 10, οι τεχνικές αυτές χρησιμοποιούν το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση το οποίο μοιράζεται μεταξύ των δύο επικοινωνούντων κόμβων-οχημάτων. Ωστόσο, οι συγκεκριμένες τεχνικές μπορούν να διασφαλίσουν μόνο την εμπιστευτικότητα των δεδομένων και όχι την ιδιωτικότητα ή τη διαδικασία ανάκλησης των ταυτοτήτων των κακόβουλων χρηστών του ITS.



Εικόνα 10: Σχήμα συμμετρικής κρυπτογραφίας

4.5.4.2.1 Public Key/Asymmetric-based Pseudonym Schemes

Σε συστήματα ασύμμετρης κρυπτογράφησης χρησιμοποιείται η λεγόμενη "υποδομή δημόσιου κλειδιού" (PKI). Ένα σχήμα παραγωγής ψευδώνυμων που υλοποιείται σε περιβάλλοντα ασύμμετρης κρυπτογράφησης προτάθηκε από τους (Raya & Hubaux, 2007). Στο σχήμα αυτό γίνεται χρήση πολλών νεοπαραχθέντων ασύμμετρων κλειδιών, ούτως ώστε τα οχήματα που αποστέλλουν μηνύματα που περιέχουν κρίσιμες πληροφορίες ασφαλείας να μην μπορούν να ταυτοποιηθούν. Ωστόσο, η συγκεκριμένη προσέγγιση αφενός απαιτεί μεγάλο αποθηκευτικό χώρο για την αποθήκευση του μεγάλου πλήθους των ασύμμετρων κλειδιών και αφετέρου διαθέτει υψηλό υπολογιστικό κόστος επειδή προϋποθέτει τον τακτικό έλεγχο καταχωρίσεων σε λίστες ανάκλησης πιστοποιητικών.

Οι (Karagiannis, et al., 2011) ανέπτυξαν μια τεχνική που ονομάζεται Expedite Message Authentication Protocol (EMAP) η οποία χρησιμοποιεί συναρτήσεις κατακερματισμού (hash functions) σε συνδυασμό με PKI για να μειώσει το χρονικό διάστημα που απαιτεί η διαδικασία ελέγχου των καταχωρήσεων σε CRLs. Ωστόσο, η επιβάρυνση που προξενείται από τις διάφορες διαδικασίες επικοινωνίας κυμαίνεται σε υψηλά επίπεδα διότι μαζί με τις CRLs ανταλλάσσονται επίσης οι συνόψεις των μηνυμάτων. Στο σχήμα που παρουσίασαν οι (Manvi, Kakkasageri, & Adiga, 2009) χρησιμοποιούνται κρυπτογραφικές τεχνικές ελλειπτικών καμπυλών για να μειώσουν τα κόστη επικοινωνίας και υπολογισμού. Ωστόσο, η προστασία της ταυτότητας του οχήματος-αποστολέα των μηνυμάτων κρίσιμων πληροφοριών κυμαίνεται σε πολύ χαμηλά επίπεδα.

Η κρυπτογραφία ελλειπτικών καμπυλών αποτελεί έναν εναλλακτικό τύπο ασύμμετρης κρυπτογράφησης (Menouar, Filali, & Abu-Dayya, 2013). Στη συγκεκριμένη περίπτωση, η χρήση μόνο της υπογραφής ενός από τους χρήστες στα παραχθέντα από αυτόν μηνύματα δεν αρκούν για να διασφαλίσουν την αυθεντικότητα των μηνυμάτων. Για το λόγο αυτό τα μηνύματα επισυνάπτονται σε ψηφιακά πιστοποιητικά. Θα πρέπει να σημειωθεί ότι η ταχύτητα κίνησης των οχημάτων επηρεάζουν το χρόνο μετάδοσης των οχημάτων όπως και το υπολογιστικό κόστος στις περιπτώσεις που γίνεται χρήση τεχνικών ελλειπτικών καμπυλών.

4.5.4.2.2. Σχηματα ψευδωνυμων που βασιζονται σε τεχνικες συμμετρικης κρυπτογραφιας (Symmetric Cryptographic-Based Pseudonym Schemes/Symmetric Encryption)

Η συμμετρική κρυπτογράφηση είναι πιο αποτελεσματική από την ασύμμετρη κρυπτογράφηση από άποψη υπολογιστικής πολυπλοκότητας. Τα συμμετρικά κρυπτοσυστήματα ωστόσο δεν πληρούν την ιδιότητα της μη αποποίησης. Οι (Schaub, Kargl, Ma, & Weber, 2010) παρουσίασαν ένα συμμετρικό κρυπτοσύστημα στο οποίο το καθήκον της ταυτοποίησης ενός χρήστη δεν ανατίθεται σε κάποια TTP, αλλά το σύνολο των πληροφοριών που μπορεί να συσχετιστούν με έναν χρήστη ενσωματώνεται απευθείας σε ψευδώνυμα. Τα τελευταία μπορούν να αποκαλυφθούν μόνο κατόπιν

συνεργασίας πολλών χρηστών. Σε αυτό το σχήμα, η CA και η οντότητα που επιφορτίζεται με την ευθύνη της παραγωγής ψευδωνύμων μπορούν να κρυπτογραφήσουν τις πληροφορίες που είναι απαραίτητες για τη διαδικασία σύνδεσης ενός ψευδωνύμου με έναν χρήστη του συστήματος. Ωστόσο, η ενσωμάτωση των πληροφοριών αυτών με άμεσο τρόπο στα πιστοποιητικά ψευδωνύμων μπορεί να θέσει σε κίνδυνο την ιδιωτικότητα των οχημάτων, με το σχήμα αυτό να καθίσταται ευάλωτο σε επιθέσεις αναμετάδοσης, Sybil και side-channel attacks.

Το σχήμα που προτάθηκε από τον (Rhim, 2012) χρησιμοποιεί κρυπτογράφηση δημόσιου κλειδιού. Το σχήμα υπολογίζει συνόψεις μηνυμάτων (message digests) τις οποίες αποστέλλει μαζί με τα παραχθέντα μηνύματα ασφαλείας προς επιβεβαίωση της ακεραιότητάς τους. Στην πλευρά του αποδέκτη υπολογίζονται οι κατακερματισμοί των μηνυμάτων και μετά συγκρίνονται με τις ληφθείσες συνόψεις μηνυμάτων για να επαληθευτεί η ακεραιότητά τους. Ωστόσο, η εν λόγω προσέγγιση είναι επιρρεπής σε επιθέσεις τύπου DoS, Sybil και side-channel. Οι (Carianha, Barreto, & Lima, 2011) ανέπτυξαν μια μεθοδολογία για τη βελτίωση του απορρήτου της γεωγραφικής θέσης του οχήματος σε μικτές ζώνες που ονομάζονται περιοχές ανωνυμοποίησης και στις οποίες γίνεται χρήση του πρωτοκόλλου κρυπτογράφησης μικτών ζωνών (CMAX). Το ιδιωτικό κλειδί που ανατίθεται από την RSU σε ένα όχημα χρησιμοποιείται για την κρυπτογράφηση των πληροφοριών που αποτυπώνουν την κατάστασή του (προσανατολισμός, θέση, ταχύτητα). Σύμφωνα με το πρωτόκολλο CMAX, η RSU αναθέτει ιδιωτικά κλειδιά μόνο σε εξουσιοδοτημένα οχήματα που εισέρχονται στη μικτή ζώνη. Το ιδιωτικό κλειδί στη συνέχεια χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων ασφαλείας και των μηνυμάτων γνωστοποίησης παρουσίας. Ειδικότερα, το ιδιωτικό κλειδί του αποστολέα θα χρησιμοποιηθεί για την κρυπτογράφηση των πληροφοριών που συνδέονται με την τρέχουσα κατάσταση του συστήματος. Ακολούθως, η RSU αποκρυπτογραφεί τα μηνύματα χρησιμοποιώντας το ιδιωτικό κλειδί του οχήματος-παραλήπτη και τα προωθεί στα γειτονικά στο όχημα-αποστολέα οχήματα-παραλήπτες. Ωστόσο, η προσέγγιση είναι επιρρεπής σε replay και side-channel attacks.

Οι ερευνητές (Wang, Liu, Zhu, Xu, & Wang, 2016) επιχείρησαν να προστατεύσουν την ιδιωτικότητα των οχημάτων χρησιμοποιώντας ένα μοντέλο με τρεις (3) κύριες οντότητες: την οντότητα διαχείρισης κλειδιών (KMC), την RSU και τα οχήματα που κινούνται εντός συγκεκριμένης ακτίνας από την RSU. Η KMC είναι υπεύθυνη για την εγγραφή των οχημάτων και των RSUs στο ITS καθώς και για την επίτευξη της απαίτησης της ιχνηλασιμότητας (traceability) των οχημάτων. Προκειμένου να ασκήσει με επιτυχία τα καθήκοντά της η KMC διατηρεί όλες τις πληροφορίες που συνδέονται με τα οχήματα του συστήματος όπως τα στοιχεία τον ιδιοκτητών τους, την ημερομηνία εγγραφής τους στο σύστημα καθώς και τον σειριακό αριθμό (VIN) που συσχετίζεται μοναδικά με καθένα από αυτά . Η RSU είναι υπεύθυνη για την προώθηση μηνυμάτων και την διανομή νέων (ενημερωμένων) κρυπτογραφικών κλειδιών στα οχήματα που κινούνται σε απόσταση από 1 έως 3 km από αυτήν. Όσον αφορά τα οχήματα αυτά διαθέτουν ενσωματωμένη OBU η οποία χρησιμοποιείται στα

διάφορα είδη επικοινωνιών τους καθώς και μια συσκευή ανθεκτική σε επιθέσεις τροποποίησης του περιεχομένου της (TPD). Η τελευταία έχει σχεδιαστεί για την αποθήκευση των διαφόρων ειδών κρυπτογραφημένων πληροφοριών παρέχοντας ταυτόχρονα ένα ασφαλές περιβάλλον για το σύνολο των κρυπτογραφικών διεργασιών που χρησιμοποιούνται για την ασφάλεια του συστήματος. Για την προστασία της ιδιωτικότητας χρησιμοποιούνται αυτο-δημιουργούμενα ψευδώνυμα (self-generated pseudonyms). Ωστόσο, όπως προκύπτει από την περιγραφή του, το συγκεκριμένο μοντέλο πάσχει από αστοχία μοναδικού σημείου (SPOF). Αυτό σημαίνει ότι προσωρινή ή μόνιμη διακοπή λειτουργίας της KMC μπορεί να οδηγήσει το σύστημα σε πλήρη κατάρρευση δεδομένου ότι η συγκεκριμένη οντότητα έχει στην αποκλειστική κατοχή της όλων των απαραίτητων -για τη λειτουργία του συστήματος- πληροφοριών. Το σχήμα καθίσταται επιπλέον ευάλωτο σε επιθέσεις έγχυσης ψευδών δεδομένων, έγχυσης κακόβουλου κώδικα, side-channel επιθέσεις και επιθέσεις τύπου Sybil.

Ένα άλλο σχήμα που βασίζει τη λειτουργία του σε ψευδώνυμα και χρησιμοποιεί τεχνικές συμμετρικής κρυπτογραφίας προτάθηκε από τους (Chim, Yiu, Hui, & Li, 2009). Στο σχήμα αυτό χρησιμοποιούνται RSUs για έλεγχο της ακεραιότητας των μηνυμάτων είναι όμως επιρρεπές σε επιθέσεις πλευρικού καναλιού (side-channel attacks).

Οι (Jahanian, Amin, & Jahangir, 2015) παρουσίασαν ένα χρονικά αποδοτικό σχήμα αυθεντικοποίησης που βασίζεται σε ακολουθίες χαρακτήρων (TESLA). Το TESLA αποτελεί μια τεχνική συμμετρικής κρυπτογραφίας στην οποία, αφού παραχθεί μια MAC ετικέτα με χρήση του διαμοιραζόμενου μυστικού κλειδιού, προσαρτάται στο μήνυμα που φέρει κρίσιμες πληροφορίες ασφαλείας. Ακολούθως αυτή η ετικέτα επαληθεύεται μέσω του διαμοιραζόμενου μυστικού κλειδιού. Η συγκεκριμένη προσέγγιση είναι ευάλωτη σε replay και side-channel attacks.

Μια βελτιωμένη μορφή του κρυπτοσυστήματος TESLA προτάθηκε από τους (Studer, Bai, Bellur, & Perrig, 2009). Το νέο κρυπτοσύστημα, που ονομάστηκε TESLA++, αποτελεί μια εξαιρετικά ενδιαφέρουσα παραλλαγή του προηγούμενου ενσωματώνοντας επιπλέον στη λειτουργία του αλγορίθμους ψηφιακών υπογραφών που χρησιμοποιούν για τη λειτουργία τους τεχνολογία ελλειπτικών καμπυλών (ECDSA). Στο συγκεκριμένο συμμετρικό σύστημα ένα όχημα πρέπει να παράξει και συγχρόνως να ελέγξει την ακεραιότητα πολυάριθμων μηνυμάτων σε ελάχιστο χρονικό διάστημα προκειμένου να επιβιώσει μέσα στο ITS. Το γεγονός αυτό βέβαια αυξάνει κατακόρυφα το υπολογιστικό κόστος δεδομένου ότι εκτός από την εκτέλεση των δραστηριοτήτων των αλγορίθμων TESLA και ECDSA απαιτείται και ο υπολογισμός ενός μεγάλου συνόλου κωδικών αυθεντικοποίησης μηνυμάτων (MACs).

4.5.4.3. Υβριδικα Σχηματα ιδιωτικοτητας (Hybrid Privacy Schemes)

Τα υβριδικά σχήματα ιδιωτικότητας αποτελούν συνδυασμό των σχημάτων ομαδικών υπογραφών και των σχημάτων ψευδωνύμων που εξετάσαμε στα προηγούμενα κεφάλαια. Οι (Calandriello, Papadimitratos, Hubaux, & Lioy, 2007), παρουσίασαν μια υβριδική τεχνική η οποία συνδυάζει σχήματα ιδιωτικότητας με βάση τα ψευδώνυμα και την ομαδική υπογραφή για να παραγάγει αυτοδημιουργούμενα (self-generated) ψευδώνυμα. Παρόλο που η τεχνική αυτή εμφανίζει πολύ χαμηλό υπολογιστικό κόστος, ανακύπτει το ζήτημα της διατήρησης της -συνήθως- κολοσσιαίου μεγέθους λίστας ανάκλησης πιστοποιητικών και του χρονικού καταμερισμού κατά την διανομή αυτής στα διάφορα οχήματα. Επιπλέον, τα αυτοδημιουργούμενα πιστοποιητικά ευνοούν την εκδήλωση σε αυτά επιθέσεων τύπου Sybil.

Οι (Bhavesh, Maity, & Hansdah, 2013) πρότειναν το υβριδικό μοντέλο αυθεντικοποίησης με πολλαπλά επίπεδα ανωνυμίας. Το μοντέλο αυτό μειώνει μεν το υπολογιστικό κόστος και τα κόστη μετάδοσης που επιφέρουν οι διάφοροι τύποι επικοινωνιών ωστόσο καθίσταται ευάλωτο σε περιστατικά αποκάλυψης ταυτότητας χρηστών, επιθέσεις αναμετάδοσης και επιθέσεις άρνησης υπηρεσιών. Συνεπώς, το μοντέλο αυτό παρέχει χαμηλό επίπεδο ασφάλειας και δεν διασφαλίζει την ανωνυμία των χρηστών.

Τέλος, υπάρχει και η υβριδική προσέγγιση των (Wagan, Mughal, & Hasbullah, 2010) στην οποία ο αρχηγός μιας ομάδας οχημάτων επιλέγεται με κριτήριο το αν κινείται στην ίδια κατεύθυνση με τα οχήματα της ομάδας του. Ωστόσο, τα κριτήρια βάσει των οποίων επιλέγεται ο αρχηγός της ομάδας δεν έχουν αναλυθεί διεξοδικά. Επιπροσθέτως, υπάρχουν πιθανότητες εμφάνισης κακόβουλων ενεργειών αφού δεν έχει αναφερθεί κατάλληλος μηχανισμός ανάκλησης ταυτότητας σε οχήματα που εμφανίζουν κακόβουλη συμπεριφορά. Όσον αφορά την χρονική απόκριση το μοντέλο παρουσιάζει υψηλές καθυστερήσεις εξαιτίας των ποικίλλων διεργασιών παραγωγής κρυπτογραφικών κλειδιών, τυχαίων αριθμών και πράξεων κατακερματισμού που λαμβάνουν χώρα συγχρόνως με τις διαδικασίες ελέγχου εγκυρότητας των συνόψεων. Συμπερασματικά το μοντέλο αυτό παρέχει χαμηλό επίπεδο ασφάλειας, εμφανίζοντας επιπλέον χαμηλή επεκτασιμότητα, υψηλά υπολογιστικά κόστη και υψηλά επίπεδα χρονικής καθυστέρησης (latency).

5. CASE STUDY: ΟΧΗΜΑΤΑ ΠΛΗΡΟΥΣ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗΣ ΟΔΗΓΗΣΗΣ

Ο τομέας της αυτοκινητοβιομηχανίας στρέφεται ολοένα και περισσότερο στην παραγωγή διασυνδεδεμένων και αυτόνομων οχημάτων. Τα έξυπνα αυτοκίνητα που διατίθενται στην παρούσα φάση στην αγορά είναι εξοπλισμένα με συστήματα που παρέχουν περιορισμένες δυνατότητες διασύνδεσης καθώς και τις λεγόμενες υπηρεσίες «προστιθέμενης αξίας» προκειμένου να βελτιώσουν αφενός την ασφάλεια των αυτοκινήτων και αφετέρου την εμπειρία των επιβαινόντων σε αυτά. Στο προσεχές διάστημα, οι δυνατότητες διασύνδεσης των έξυπνων αυτοκινήτων αναμένεται να επεκταθούν καθιστώντας τα έξυπνα αυτοκίνητα ικανά να διασυνδέονται με άλλους τύπους οχημάτων, πεζούς και τις περιβάλλουσες υποδομές μέσω των επικοινωνιών V2X (European Commision, 2018). Επιπλέον αρχίζουν να βγαίνουν στο προσκήνιο ημιαυτόνομα και πλήρως αυτόνομα αυτοκίνητα (δηλαδή οχήματα που κατατάσσονται στα επίπεδα 4 και 5 της αυτονομίας όπως ορίζονται στο (SAE Mobilus, 2021), τα οποία χρησιμοποιούν προηγμένες τεχνικές μηχανικής μάθησης (ML) και τεχνητής νοημοσύνης (AI). Κατασκευαστές αυτοκινήτων, προμηθευτές συστημάτων, φορείς εκμετάλλευσης οδικών δικτύων και άλλοι πάροχοι υπηρεσιών μεταφορών διεξάγουν ήδη εποπτευόμενες δοκιμές σε αυτόνομα οχήματα έχοντας ως δικλείδα ασφαλείας έναν οδηγό που βρίσκεται πάντα σε επιφυλακή ώστε αναλάβει τον έλεγχο του αυτοκινήτου εφόσον απαιτηθεί.

Τα τελευταία χρόνια, υπάρχει ένα διαρκώς αυξανόμενο ενδιαφέρον για αυτόνομα αυτοκίνητα τόσο από την πλευρά των τελικών χρηστών όσο και από την αντίστοιχη των κατασκευαστών με την παραγωγή τους να γνωρίζει ανοδική τάση στην αγορά αυτοκινήτων (European Commision, 2017). Βάσει των στοιχείων μελέτης (World Economic Forum, 2015) στην οποία ερωτήθηκαν περισσότεροι από 5.500 κάτοικοι πόλεων σε παγκόσμιο επίπεδο, το 58% των ερωτηθέντων δήλωσαν πρόθυμοι να επιβιβαστούν σε ένα όχημα χωρίς οδηγό. Τα ποσοστά αποδοχής της νέας τεχνολογίας των πλήρως αυτοματοποιημένων οχημάτων είναι υψηλότερα σε αναδυόμενες αγορές όπως η Κίνα (75%) και η Ινδία (85%) από ό,τι σε ευρωπαϊκές χώρες όπως το Ηνωμένο Βασίλειο (49%) και η Γερμανία (44%). Βέβαια, η ευρωπαϊκή οικονομία αναμένεται σε κάθε περίπτωση να επωφεληθεί από την νέα τεχνολογική τάση των αυτόνομων οχημάτων (European Commision, 2018), δεδομένου ότι το 23% της παγκόσμιας παραγωγής μηχανοκίνητων οχημάτων γίνεται εντός της ΕΕ. Επιπλέον, εξαιτίας του γεγονότος ότι σχεδόν το 72% των χερσαίων μεταφορών πραγματοποιείται οδικώς στον ευρωπαϊκό χώρο η εμπιστοσύνη προς τους κατασκευαστές αυθεντικών εξοπλισμών (OEM) βρίσκεται σε εξαιρετικά υψηλά επίπεδα. Παρ' όλα αυτά, αν και οι αισιόδοξες προβλέψεις αναφέρουν ότι τα πλήρως αυτοματοποιημένα οχήματα θα μπορούσαν να αναπτυχθούν ευρέως έως το 2030 (Arbib & Seba, 2017), ο επιστημονικός κόσμος του χώρου αυτού διατηρεί τις επιφυλάξεις του υπογραμμίζοντας ότι απαιτείται περαιτέρω έρευνα για τη δημιουργία ενός πλήρως αυτόνομου οχήματος, κυρίως αναφορικά με τους τομείς της τεχνητής νοημοσύνης και της κυβερνοασφάλειας (The Canadian Press, 2017).

Η κυβερνοασφάλεια αποτελεί έναν παράγοντα με καταλυτικό ρόλο στην εξέλιξη των έξυπνων αυτοκινήτων. Τα τελευταία χρόνια έχουν δημοσιευτεί αρκετές ερευνητικές μελέτες που αναφέρονται σε επιθέσεις που στοχεύουν έξυπνα αυτοκίνητα. Μία από τις πιο γνωστές είναι η εξ αποστάσεως επίθεση με στόχο ένα έξυπνο όχημα της εταιρείας Jeep (Drozhzhin, 2015) κατά την οποία οι ερευνητές C.Miller και C.Valasek αφού απέκτησαν τον απομακρυσμένο έλεγχο του οχήματος το οδήγησαν εκτός δρόμου. Η επιτυχία της συγκεκριμένης επίθεσης είχε ως αποτέλεσμα την άμεση ανάκληση 1,4 εκατομμυρίων οχημάτων της συγκεκριμένης εταιρείας. Επιπλέον, πρόσφατα ερευνητές του εργαστηρίου ασφάλειας της κινεζικής εταιρείας *Tencent* κατάφεραν, εκμεταλλευόμενοι συγκεκριμένες ευπάθειες σε διαγνωστικές υπηρεσίες της νέας σειράς οχημάτων της Mercedes-Benz, να αποκτήσουν (δια ζώσης και εξ αποστάσεως) τον έλεγχο του συστήματος ψυχαγωγίας (infotainment system) MBUX[10] δίνοντάς τους τη δυνατότητα να εκτελέσουν με μη εξουσιοδοτημένο τρόπο ενέργειες όπως την αλλαγή φωτισμού στο εσωτερικό του οχήματος ή το άνοιγμα της ηλιοροφής (Tencent Security Keen Lab, 2021). Σε συνέχεια των προηγούμενων επιθέσεων, ερευνητές της αγγλικής εταιρείας Pen Test Partners LLP κατόρθωσαν να θέσουν υπό τον έλεγχό τους έξυπνα οχήματα μέσω του συστήματος συναγερμού τους, προβαίνοντας σε ενέργειες όπως την ενεργοποίηση ή την απενεργοποίηση του συστήματος ακινητοποίησης (immobilizer) του οχήματος ή τη διακοπή της λειτουργίας του κινητήρα (Grustniy, 2019). Στο πλαίσιο της παροχής ενός περιβάλλοντος για την αποτίμηση του επιπέδου της ασφάλειας των τεχνολογικών εφαρμογών που περιλαμβάνονται σε ένα όχημα, κυκλοφόρησε πρόσφατα μια πλατφόρμα ανοιχτού κώδικα που ονομάζεται **PASTA** (Toyama, Yoshida, Oguma, & Matsumoto, 2018). Η εν λόγω πλατφόρμα προσομοιώνει εξ αποστάσεως λειτουργίες του οχήματος που σχετίζονται με το σύστημα μετάδοσης, το σύστημα πέδησης, τα παράθυρα και άλλα είδη λειτουργιών ώστε ο κάτοχος του οχήματος να ενημερωθεί αναφορικά με τα χαρακτηριστικά των ηλεκτρονικών επικοινωνιών, τις ανακύπτουσες ευπάθειες καθώς και πειραματικά σενάρια επιθέσεων. Ωστόσο, η συγκεκριμένη πλατφόρμα μπορεί επίσης να χρησιμοποιηθεί και από επίδοξους επιτιθέμενους, διευκολύνοντας τους στην προσπάθεια εκτέλεσης μη εξουσιοδοτημένων ενεργειών στο όχημα.

Με την απαίτηση της διασυνδεσιμότητας των έξυπνων αυτοκινήτων διαρκώς να ισχυροποιείται και την παράλληλη εμφάνιση ημιαυτόνομων και αυτόνομων οχημάτων, προκύπτουν νέες προκλήσεις, κίνδυνοι και απειλές για την κυβερνοασφάλεια. Για παράδειγμα, έχουν αναφερθεί εξ αποστάσεως επιθέσεις στις κάμερες και στα συστήματα LiDAR των οχημάτων (Petit, Stottelaar, & Feiri, 2015) οι οποίες οδηγούν σε φαινόμενα δυσλειτουργίας των αισθητήρων, άλλοτε εμφανίζοντας αντικείμενα του πραγματικού κόσμου σε σημεία ευρύτερα από αυτά στα οποία βρίσκονται στην πραγματικότητα και άλλοτε κατασκευάζοντας εξ ολοκλήρου τα δικά

[10] Το Mercedes-Benz User Experience (MBUX) infotainment system αποτελεί το σύστημα παροχής υπηρεσιών ψυχαγωγίας και διασκέδασης στα οχήματα της αυτοκινητοβιομηχανίας Mercedes-Benz. Η Mercedes-Benz ενσωμάτωσε για πρώτη φορά το MBUX στη σειρά A-Class το 2018. Σήμερα, διατίθεται σε όλη την νέα γενιά έξυπνων οχημάτων της όπως την E-Class, την GLE, την GLS, την EQC.

τους αντικείμενα. Εκτός όμως από τα σενάρια κακόβουλων δράσεων σε αισθητήρες, υπάρχουν και άλλες μέθοδοι επίθεσης, όπως η εξαπάτηση των συστημάτων γεωεντοπισμού που χρησιμοποιούν συστήματα δορυφορικών επικοινωνιών (GNSS) (Zeng, et al., 2018) και η εξαπάτηση συστημάτων που βασίζονται σε AI όπως συνέβη στην περίπτωση ενός αυτοοδηγούμενου οχήματος σχεδιάζοντας έναν κύκλο κιμωλίας γύρω από αυτό (ENISA, 2019). Οι επιθέσεις που στοχεύουν έξυπνα αυτοκίνητα μπορεί δυνητικά να επιφέρουν ακινητοποίηση των οχημάτων, τροχαία ατυχήματα, οικονομικές απώλειες, αποκάλυψη ευαίσθητων ή / και προσωπικών δεδομένων, ακόμα και να θέσουν σε κίνδυνο της ασφάλεια των χρηστών του δρόμου. Επομένως, επιβάλλεται η εφαρμογή κατάλληλων μέτρων ασφαλείας για τον μετριασμό των κινδύνων, ειδικά με δεδομένο ότι οι συγκεκριμένες επιθέσεις απειλούν την ασφάλεια και την ιδιωτικότητα τόσο των επιβαινόντων στο όχημα όσο και των υπόλοιπων χρηστών του δρόμου, συμπεριλαμβανομένων των πεζών.

5.1 Κατηγορίες αισθητήρων που χρησιμοποιούνται στα αυτόνομα οχήματα

Όπως ακριβώς οι άνθρωποι, αφού επεξεργαστούν τα ερεθίσματα τα οποία έχουν λάβει από το περιβάλλον τους μέσω των αισθητηριακών τους οργάνων, εκδηλώνουν συγκεκριμένες συμπεριφορές έτσι και τα οχήματα αυτοματοποιημένης οδήγησης χρησιμοποιούν ποικίλους αισθητήρες εντός και εκτός του οχήματος για να λαμβάνουν δεδομένα από το περιβάλλον τους τα οποία στη συνέχεια τροφοδοτούν στα σύνθετα συστήματα επεξεργασίας πληροφοριών που χρησιμοποιούν τεχνικές τεχνητής νοημοσύνης προκειμένου να τα επεξεργαστούν και να δώσουν το έναυσμα για την εκτέλεση συγκεκριμένων ενεργειών.

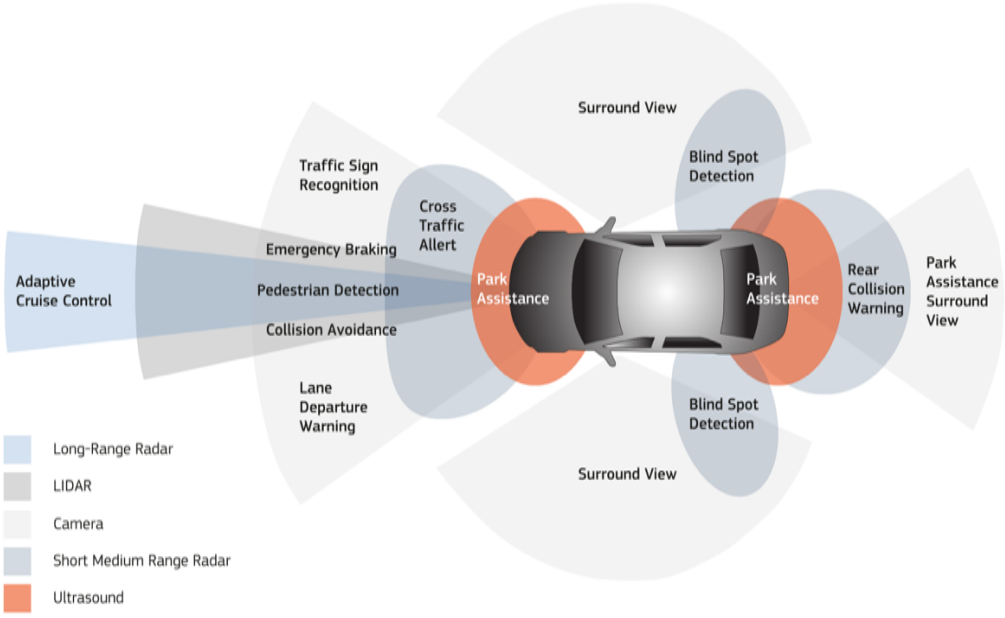
Οι αισθητήρες, λοιπόν, αποτελούν την πρωταρχική πηγή εισροής πληροφοριών στα συστήματα τεχνητής νοημοσύνης των οχημάτων αυτοματοποιημένης οδήγησης. Ταξινομούνται γενικά σε τρεις (3) κατηγορίες:

- **Εξωτερικοί αισθητήρες:** Αποσκοπούν στην αναγνώριση των περιβαλλοντικών συνθηκών του οχήματος. Τυπικά παραδείγματα αισθητήρων που ανήκουν σε αυτήν την κατηγορία και συνδέονται άμεσα με τη διαδικασία οδήγησης αποτελούν οι κάμερες και οι αισθητήρες αναγνώρισης του περιβάλλοντος μέσω διάχυσης του φωτός (LiDARs). Άλλοι αισθητήρες οι οποίοι βρίσκονται μεν σε διαρκή αλληλεπίδραση με το περιβάλλον του οχήματος αλλά δεν εμπλέκονται ειδικά με τη διαδικασία οδήγησης αποτελούν οι αισθητήρες GNSS, οι IMUs, συσκευές ραντάρ και οι αισθητήρες υπέρηχων (ultrasonic sensors).

- **Εσωτερικοί αισθητήρες:** Είναι οι παραδοσιακές συσκευές ελέγχου που βρίσκονται στο εσωτερικό του οχήματος και οι οποίες αποτυπώνουν σε ψηφιακή μορφή (μέσω οθονών) τα αποτελέσματα αναλογικών μετρητών όπως το στροφόμετρο ή το ταχύμετρο.

- **Άλλοι αισθητήρες:** Χρησιμοποιούνται κυρίως για τα διάφορα είδη ψηφιακών επικοινωνιών που αναπτύσσονται μεταξύ του οχήματος και των υπολοίπων οχημάτων (V2V) καθώς και των ηλεκτρονικών συσκευών που βρίσκονται παρακείμενες στο οδικό δίκτυο (V2I).

Στην Εικόνα 11 παρατίθενται οι θέσεις στις οποίες βρίσκονται τοποθετημένοι οι αισθητήρες σε ένα όχημα μαζί με τις κυριότερες λειτουργίες τις οποίες εξυπηρετούν. Το ποιοί τύποι αισθητήρων θα συμπεριληφθούν στα οχήματα κάθε αυτοκινητοβιομηχανίας εξαρτάται από την στρατηγική ανάπτυξης λογισμικού που χρησιμοποιεί η καθεμία. Σε κάθε περίπτωση, μια από τις προσφιλέστερες τακτικές που ακολουθούνται είναι η διαδικασία συγχώνευσης πολλαπλών τύπων δεδομένων (data fusion) που συλλέγονται από τα διαφορετικά είδη αισθητήρων ούτως ώστε το σύνολο των συλλεχθέντων δεδομένων (π.χ. δισδιάστατες ή τρισδιάστατες εικόνες) να ομογενοποιηθούν προτού τροφοδοτηθούν στα υποσυστήματα επεξεργασίας του οχήματος.



Εικόνα 11: *Θέση αισθητήρων στο όχημα και κύριες λειτουργίες αυτών (ENISA, 2021)*

Όπως γίνεται αντιληπτό, από τα παραπάνω είδη αισθητήρων, οι κάμερες και οι αισθητήρες αναγνώρισης του περιβάλλοντος μέσω διάχυσης του φωτός (LiDAR sensors) αποτελούν τις πιο διαδεδομένες πηγές εισόδων δεδομένων για τα οχήματα αυτοματοποιημένης οδήγησης.

Οι **κάμερες** (*cameras*) τροφοδοτούν τα συστήματα επεξεργασίας πληροφοριών του οχήματος με μια ακολουθία από δισδιάστατα σημεία (*pix*els) που περιέχουν κωδικοποιημένη χρωματική πληροφορία. Αυτά τα σημεία, σε πρώτη φάση, συνθέτουν εικόνες οι οποίες απεικονίζουν σε δισδιάστατη μορφή τον πραγματικό, τρισδιάστατο

κόσμο. Στη συνέχεια, αυτές οι εικόνες συνδυάζονται μεταξύ τους και προβαλλόμενες σε υψηλή ταχύτητα δημιουργούν μια αλληλουχία που προσδίδει στο ανθρώπινο μάτι την ψευδαίσθηση της κίνησης. Κατ' αυτόν τον τρόπο, τα τρισδιάστατα (3D) αντικείμενα του πραγματικού περιβάλλοντος αναπαρίστανται τελικά από τις ψηφιακές κάμερες από δισδιάστατες ακολουθίες κινούμενων εικόνων (video feeds).

Οι **αισθητήρες αναγνώρισης του περιβάλλοντος μέσω τεχνολογιών διάχυσης του φωτός** (*LiDAR sensors*) εκπέμπουν ακτίνες λέιζερ στο περιβάλλον του οχήματος δημιουργώντας έναν χάρτη χρωματικού βάθους (depth map) που προκύπτει από την ανάλυση του φάσματος του ανακλώμενου -στα διάφορα αντικείμενα του περιβάλλοντος- σήματος. Κατόπιν, ο χάρτης αυτός υπόκειται σε περαιτέρω επεξεργασία ούτως ώστε να δημιουργηθεί τελικά μια τρισδιάστατη αναπαράσταση των στοιχείων του εξωτερικού περιβάλλοντος.

Στην δεύτερη εικόνα (στα δεξιά) απεικονίζεται ένας πίνακας που παραθέτει τα θετικά και αρνητικά στοιχεία κάθε αισθητήρα. Έτσι, εξετάζοντας τα χαρακτηριστικά των προαναφερθέντων αισθητήρων, διαπιστώνουμε ότι οι ψηφιακές κάμερες πλεονεκτούν έναντι των LiDAR αισθητήρων όσον αφορά την αναγνώριση στοιχείων του οδικού δικτύου (π.χ. πινακίδες οδικής σήμανσης, φωτεινοί σηματοδότες, φώτα οχημάτων) χάρη στην ικανότητά τους να διακρίνουν ποικίλες χρωματικές αποχρώσεις. Υστερούν ωστόσο από αυτούς στο γεγονός ότι η ικανότητα αναγνώρισής τους επηρεάζεται σημαντικά από συγκεκριμένες κλιματολογικές συνθήκες (βροχή, ομίχλη, ξαφνικές μεταβολές στον ηλιακό φωτισμό).

	Sensor Type	Range	Pros	Cons
Exteroceptive (sensors that perceive environment)	LiDAR	Up to 200 meters	High precision High accuracy Wide Field of View	High cost No colour information Worsen aerodynamics (usually mounted on the roof)
	Cameras	Up to 100 meters	Can see colours and textures Low cost High availability	Sensitive to low intensity light Heavily affected by adverse weather conditions Inaccurate range estimation
	Radar	5 meters – 200 meters	Robust to environmental conditions Cheaper than LiDAR Mature and readily available Capable of determining relative motion of objects Fast detection response	Noisy response for metallic objects Not suitable for static objects Poor lateral resolution
	Sound microphone	Several hundreds of meters	Allows to hear environmental sounds.	Limited to audio signals.
	Ultrasonic sensors	Up to 2 meters	Robust to adverse weather conditions Proven track of reliability Most accurate sensor for close proximity Inexpensive	Only suitable for very short range Low resolution Not suitable for high speeds Heavily affected by changes in environmental conditions (temperature, humidity)
Proprioceptive (sensors that measure values within the system)	GNSS		High accuracy. Relatively inexpensive. Widespread deployment High-integrity and high-precision positioning capabilities	GNSS signals do not penetrate buildings such as multi-story car parks or inside tunnels, Issues of reflectivity and satellite visibility in built-up urban areas. Vulnerability to intentional and unintentional signal interferences.
	IMU	Within the vehicle	Needs no connection to or knowledge of the external world 6 degrees of freedom Used in sensor fusion with other localization techniques Inexpensive	Accuracy is dependent on calibration of accelerometer and three axis rate sensor. Around 30cm accuracy, so needs to be used in combination with other sensors
	Encoders (position, velocity, etc.)	Within the vehicle	Gives an accurate state of the vehicle Low cost. Easy to install.	Limited accuracy.

Εικόνα 12: *Σύγκριση στοιχείων αισθητήρων οχημάτων αυτοματοποιημένης οδήγησης (ENISA, 2021)*

5.2 AI και αυτόνομα οχήματα

Τα τελευταία χρόνια, υπάρχει μια διαρκώς αυξανόμενη τάση ενσωμάτωσης οχημάτων αυτοματοποιημένης οδήγησης στη διαδικασία παραγωγής των αυτοκινητοβιομηχανιών, η οποία μπορεί να θεωρηθεί ως μια μορφή αναγνώρισης των πολλαπλών οφελών που αποκομίζουν οι πολίτες των σύγχρονων κοινωνιών από αυτά. Ωστόσο, το στοιχείο της καινοτομίας που στα συγκεκριμένα "περιβάλλοντα" εδράζεται στην αυτοματοποιημένη λειτουργία των εν λόγω οχημάτων -μέσω της πλήρους απεμπλοκής του ανθρώπινου παράγοντα από τη διαδικασία της οδήγησης- δημιουργεί στους χρήστες τους εύλογους προβληματισμούς. Είναι χαρακτηριστικό ότι στην ετήσια έρευνα για τα αυτοματοποιημένα οχήματα που διεξήγαγε το 2021 η Αμερικανική Ένωση Αυτοκινήτου (AAA), διαπιστώθηκε ότι μόνο ένα ποσοστό της τάξης του 14% των Αμερικανών οδηγών θα εμπιστευόταν την οδήγηση σε ένα αυτοοδηγούμενο όχημα (Edmonds, 2021). Το περιεχόμενο των προβληματισμών συναρτάται με το ερώτημα του κατά πόσο η διαδικασία κίνησης των οχημάτων αυτού του τύπου είναι "ασφαλής", δίχως δηλαδή να τίθεται σε άμεσο κίνδυνο η ασφάλεια των επιβαινόντων σε αυτά.

Οριοθετώντας την απάντηση για το συγκεκριμένο ερώτημα, θα πρέπει αρχικά να εκλάβουμε ως δεδομένο ότι οι τεχνικές μηχανικής μάθησης (ML), που αποτελούν τον πυρήνα των διαφορετικών συστημάτων που έχουν αναπτυχθεί στα οχήματα αυτοματοποιημένης οδήγησης για να υποκαταστήσουν διάφορες πτυχές της ανθρώπινης οδηγικής συμπεριφοράς, περιλαμβάνουν ένα σύνολο ευπαθειών οι οποίες δύνανται να αποτελέσουν αντικείμενα εκμετάλλευσης από μια πλειάδα απειλών θέτοντας σε κίνδυνο την λειτουργία των οχημάτων και άρα την ζωή των επιβαινόντων σε αυτά. Στο πλαίσιο αυτό κρίνεται απαραίτητη η κατανόηση των διαφορετικών μηχανισμών τεχνητής νοημοσύνης που χρησιμοποιούνται στα οχήματα αυτοματοποιημένης οδήγησης ώστε να διασφαλίζουμε ότι εφαρμόζονται τα κατάλληλα μέτρα ασφάλειας για τον περιορισμό των επιπτώσεων των κινδύνων υψηλής επικινδυνότητας που εμφανίζονται στα περιβάλλοντα αυτά. Σε τελική ανάλυση θα αποφανθούμε σχετικά με το κατά πόσο είναι συμφέρουσα η εισαγωγή της τεχνολογίας των οχημάτων αυτοματοποιημένης οδήγησης στο οικοσύστημα των "παραδοσιακών" μεταφορών. Η αποτίμηση του οφέλους που αποκομίζουμε από την εισαγωγή της καινοτομίας (στην προκειμένη περίπτωση των οχημάτων αυτοματοποιημένης οδήγησης στο αστικό οδικό δίκτυο) εκτιμάται με βάση του κατά πόσο τα οφέλη αυτά υπερτερούν των ανακυπτόντων περιστατικών ασφάλειας.

Η κυβερνοασφάλεια στο πεδίο των οχημάτων αυτοματοποιημένης οδήγησης ταυτίζεται σε μεγάλο βαθμό με την προστασία της ασφάλειας των ψηφιακών συστημάτων. Το γεγονός αυτό φαντάζει απολύτως λογικό αν αναλογιστούμε ότι η διαδικασία ελέγχου της λειτουργίας των οχημάτων νέας γενιάς υλοποιείται, σχεδόν στο σύνολό της, από ηλεκτρονικά συστήματα τα οποία όμως, όπως έχουμε επισημάνει, καθίστανται ευάλωτα τόσο σε φυσικές όσο και σε εξ αποστάσεως επιθέσεις. Επειδή το εύρος των συγκεκριμένων απειλών είναι ιδιαιτέρως μεγάλο, γίνεται αντιληπτό ότι επιβάλλεται να προβούμε σε μερική οριοθέτηση αυτών. Έτσι, στο πλαίσιο της τρέχουσας θεματικής ενότητας, θα εστιάσουμε την προσοχή μας στο υποσύνολο των κινδύνων που σχετίζονται αποκλειστικά με τα υποσυστήματα των αυτόνομων οχημάτων που χρησιμοποιούν αλγοριθμικές τεχνικές από το πεδίο της τεχνητής νοημοσύνης. Τα συστήματα αυτά προσομοιώνουν ποικίλα σενάρια που λαμβάνουν χώρα κατά τη λειτουργία ενός οχήματος και τα οποία μέχρι πρότινος διευθετούνταν μέσω ανθρώπινης παρέμβασης π.χ. αντίληψη των περιβαλλοντικών συνθηκών, εκδήλωση ενεργειών στη βάση μιας αυτοματοποιημένης διαδικασίας λήψης αποφάσεων.

Όπως γίνεται αντιληπτό, τα εν λόγω συστήματα διαφοροποιούνται εκ φύσεως από τις "παραδοσιακές" μορφές λογισμικού. Πράγματι, στον "πυρήνα" των τεχνικών μηχανικής μάθησης που χρησιμοποιούνται από τα συστήματα αυτά βρίσκεται ένα σύνολο κανόνων το οποίο συνήθως αναπαρίσταται "αυστηρά" βάσει ενός μαθηματικού μοντέλου. Το γεγονός ότι η λειτουργία των μηχανισμών αυτών στηρίζεται, κατά κύριο λόγο, σε μεθόδους στατιστικής ανάλυσης που εφαρμόζονται σε σύνολα δεδομένων κολοσσιαίου μεγέθους, αφενός αυξάνει το επίπεδο αυτοματοποίησης σε πολύ υψηλά επίπεδα (καθιστώντας εφικτή ακόμα και την αυτοματοποίηση σύνθετων γνωστικών

διεργασιών), αφετέρου, ωστόσο, αποτελεί πρόσφορο έδαφος για κακόβουλους χρήστες οι οποίοι εκμεταλλεύονται το οποιοδήποτε κενό ασφάλειας για ιδίους σκοπούς. Συνεπώς, η διασφάλιση της ασφάλειας σε συστήματα αυτής της συνομοταξίας, προϋποθέτει την αναγνώριση και αντιμετώπιση των διαφορετικών τύπων κινδύνων που εκδηλώνονται αποκλειστικά σε περιβάλλοντα της τεχνητής νοημοσύνης ήδη από τη φάση του σχεδιασμού των συστημάτων αυτών (security by design) καθώς επίσης και την υψηλότερη προτεραιοποίησή τους συγκριτικά με τα υπόλοιπα είδη κινδύνων.

5.2.1 Κυριότερες λειτουργίες αυτοματοποιημένης οδήγησης

Για να κατανοήσουμε πλήρως τα ζητήματα ασφάλειας τα οποία ανακύπτουν στα υποσυστήματα τεχνητής νοημοσύνης ενός οχήματος πλήρους αυτοματοποιημένης οδήγησης θα εμβαθύνουμε στους μηχανισμούς τεχνολογίας που χρησιμοποιούνται από αυτά για τη λειτουργία τους. Η αυτοματοποιημένη οδήγηση αποτελεί μια πολυσχιδή διαδικασία η οποία συνίσταται σε μια πλειάδα λειτουργιών υψηλού επιπέδου. Οι λειτουργίες αυτές φαίνονται, σε πρώτη ανάγνωση, να υποβοηθούν τον οδηγό κατά τον χειρισμό του οχήματος (μέσω της εκπομπής προειδοποιητικών μηνυμάτων ή της ανάληψης του ελέγχου του οχήματος σε πολύ συγκεκριμένες περιπτώσεις) και όχι να τον αντικαθιστούν. Ωστόσο, καθώς η διαδικασία της μαζικής κατασκευής αυτόνομων οχημάτων ωριμάζει, οι εν λόγω διαδικασίες θα πάψουν να έχουν βοηθητικό χαρακτήρα και θα αποτελέσουν κυρίαρχα τμήματα της αυτοματοποιημένης οδηγικής διαδικασίας στην οποία ο στόχος της πλήρους απεμπλοκής του ανθρώπινου παράγοντα από αυτήν θα έχει πια επιτευχθεί. Ορισμένες από τις προαναφερθείσες διαδικασίες είναι οι ακόλουθες:

- **Adaptive Cruise Control (αυτόματος πιλότος):** Το βασικότερο χαρακτηριστικό της συγκεκριμένης λειτουργίας είναι η προσαρμογή της ταχύτητας του οχήματος μέσω της, κατά περίπτωση, επιτάχυνσης ή επιβράδυνσης αυτού ούτως ώστε να διατηρείται μια ασφαλής απόσταση από τα προπορευόμενα οχήματα.

- **Automatic parking assistance (σύστημα υποβοήθησης στάθμευσης):** Η συγκεκριμένη λειτουργία αυτοματοποιεί τη διαδικασία της στάθμευσης λαμβάνοντας υπόψιν παραμέτρους όπως η οδική σήμανση, το περιβάλλον του οχήματος και ο διαθέσιμος χώρος της θέσης.

- **Automotive navigation (αυτόματη πλοήγηση):** Το κυριότερο μέλημα της συγκεκριμένης λειτουργίας είναι η παροχή κατευθύνσεων για την επιτυχή άφιξη του οχήματος σε μια τοποθεσία-προορισμό. Στο πλαίσιο αυτό γίνεται προφανώς χρήση δεδομένων τοποθεσίας.

- **Blind spot/cross traffic/ lane change assistance (σύστημα υποβοήθησης αλλαγής λωρίδας):** Βασικός στόχος αυτής της λειτουργίας αποτελεί ο έγκαιρος εντοπισμός οχημάτων και πεζών που βρίσκονται γύρω από το όχημα όταν αυτό στρίβει σε μια διασταύρωση ή αλλάζει λωρίδα. Η επιτυχία στην εκτέλεση της εν λόγω λειτουργίας έγκειται στη χρήση αισθητήρων που βρίσκονται σε διάφορα σημεία του οχήματος.

- **Collision avoidance system (αυατήματα αποφυγής συγκρούσεων):** Αποσκοπεί στην αναγνώριση καταστάσεων που δύνανται να οδηγήσουν σε συγκρούσεις και την έγκαιρη αντιμετώπιση αυτών μέσω της παρακολούθησης και της κατά περίπτωση ελάττωσης αυτής όταν οι συνθήκες το απαιτούν.

- **Automated lane keeping systems (συστήματα διατήρησης λωρίδας):** Διατηρούν το όχημα ευθυγραμμισμένο εντός της λωρίδας στην οποία κινείται. Για να επιτύχουν τον στόχο τους τα συστήματα αυτά πρέπει αρχικά να είναι σε θέση να διακρίνουν εκείνα τα τμήματα του οδικού δικτύου τα οποία σχετίζονται άμεσα με τη διαδικασία της οδήγησης (π.χ. οδοί, αυτοκινητόδρομοι) από αυτά που δεν συνδέονται με αυτήν (π.χ. πεζοδρόμια). Στον "πυρήνα" της λειτουργικότητάς τους βρίσκεται η ικανότητά τους να αναγνωρίζουν τις γραμμές που σηματοδοτούν τα όρια της κάθε λωρίδας στο οδόστρωμα (και ιδιαίτερα αυτής στην οποία κινείται το όχημα σε μια δεδομένη χρονική στιγμή), καθώς και αυτές που υποδηλώνουν κατεύθυνση των κυκλοφοριακών ροών ή έχουν κάποιο άλλο εννοιολογικό περιεχόμενο συναφές όμως με τη διεργασία χειρισμού του οχήματος (π.χ. γραμμή υποχρεωτικής ακινητοποίησης οχήματος-stop line). Η ικανότητά τους αυτή πηγάζει από την χρήση αλγορίθμων επεξεργασίας δυσδιάστατων ή τρισδιάστατων εικόνων (Bar Hillel, Lerner, Levi, & Raz, 2014) που λαμβάνουν από τους αισθητήρες καταγραφής εικόνας του οχήματος συνδυαζόμενες -σχεδόν πάντα- με πραγματικούς οδικούς χάρτες. Τέλος, μέσω της χρήσης πολύπλοκων μηχανισμών μηχανικής μάθησης, να μπορούν να διακρίνουν επικίνδυνες μεταβολές στην παρατηρηθείσα «συμπεριφορά» του οχήματος αναλαμβάνοντας τον έλεγχο χειρισμού του όποτε αυτό κρίνεται επιβεβλημένο.

- **Traffic sign recognition (αναγνώριση οδικής σήμανσης)**: Ο βασικός στόχος της συγκεκριμένης λειτουργίας έγκειται στην αναγνώριση των πινακίδων οδικής σήμανσης που παρέχουν οδηγίες για την ασφαλή κίνηση του οχήματος. Αναγκαία συνθήκη για την επίτευξη αυτού του στόχου είναι η ικανότητα των αισθητήρων καμερών που βρίσκονται τοποθετημένοι στο όχημα να αναγνωρίζουν αντικείμενα βάσει πολλαπλών χαρακτηριστικών τους όπως το σχήμα, το χρώμα, τα απεικονισθέντα σύμβολα και τυχόν αναγραφόμενο κείμενο.

- **Αναγνώριση περιβαλλοντικών ήχων:** Συνίσταται στην δυνατότητα αναγνώρισης και ερμηνείας των περιβαλλοντικών ήχων που συσχετίζονται με τη διαδικασία οδήγησης. Ενδεικτικά παραδείγματα ήχων που ανήκουν σε αυτή τη συνομοταξία αποτελούν ο ήχος της κόρνας ενός οχήματος ή των σειρήνων οχημάτων έκτακτης ανάγκης. Είναι προφανές ότι η επιτυχής αναγνώριση τέτοιου είδους ηχητικών σημάτων ακόμα και σε περιβάλλοντα που χαρακτηρίζονται από υψηλό "θόρυβο" αποτελούν το κλειδί για την επιτυχή εκτέλεση της συγκεκριμένης λειτουργίας.

5.2.2 Κατηγορίες AI συστημάτων λογισμικού στα αυτόνομα οχήματα

Όσοι από εμάς έχουμε αποκτήσει άδεια οδήγησης γνωρίζουμε ότι η διαδικασία χειρισμού ενός οχήματος προϋποθέτει σύνθετες ικανότητες λήψης αποφάσεων προκειμένου να αντιμετωπιστούν απρόσμενες και εν δυνάμει επικίνδυνες ανακύπτουσες καταστάσεις. Στα περιβάλλοντα της αυτοματοποιημένης οδήγησης όλο αυτό το φάσμα των απαιτούμενων σύνθετων δεξιοτήτων επιτυγχάνεται μέσω των ενσωματωμένων στο όχημα συστημάτων λογισμικού τεχνητής νοημοσύνης. Τα συστήματα αυτά επεξεργάζονται τα δεδομένα που συλλέγονται από τους αισθητήρες και τα ερμηνεύουν ώστε να επιλέξουν την κατάλληλη ανά περίπτωση ενέργεια (ή σειρά ενεργειών). Στο πλαίσιο αυτό αναγνωρίζουμε τρία (3) αλληλοσυνδεόμενα υποσυστήματα:

- **Υποσύστημα αντίληψης** (*Perception module*): Προβαίνει σε εξαγωγή γνώσης σχετικά με το περιβάλλον του οχήματος αυτοματοποιημένης οδήγησης από την επεξεργασία των πολυειδών δεδομένων που συλλέγονται από τους αισθητήρες του οχήματος. Αποσκοπεί στη δημιουργία ενός μοντέλου που θα αναπαριστά την κατάσταση του περιβάλλοντος που περιβάλλει το όχημα και θα αναπροσαρμόζεται καθώς το περιβάλλον μεταβάλλεται. Η διαδικασία δημιουργίας ενός τέτοιου μοντέλου απαιτεί την αναγνώριση, ανά τακτά χρονικά διαστήματα, των διαφορετικών τύπων οχημάτων που κινούνται πέριξ του οχήματος αυτοματοποιημένης οδήγησης (άλλα αυτοκίνητα, φορτηγά, δίκυκλα οχήματα) και τις θέσεις τους, των 'συστατικών' στοιχείων της υποδομής του οδικού δικτύου (πινακίδες οδικής σήμανσης, φωτεινοί σηματοδότες, λωρίδες κυκλοφορίας), τυχόν διερχόμενων πεζών, ενώ, σε κάθε περίπτωση, καταγράφεται η θέση και ο προσανατολισμός του οχήματος αναφορικά με τις αντίστοιχες θέσεις των υπόλοιπων οχημάτων στο οδικό δίκτυο.

- **Υποσύστημα σχεδιασμού ενεργειών** (*Planning module*): Έχει ως κύρια λειτουργία τον καθορισμό της βέλτιστης διαδρομής που θα πρέπει να ακολουθήσει το όχημα προκειμένου να μεταβεί από την αρχική τοποθεσία (αφετηρία) στην επιθυμητή τοποθεσία (προορισμό) λαμβάνοντας υπόψη τυχόν περιορισμούς (γειτονικά κινούμενα οχήματα, εμπόδια στον δρόμο,

συμμόρφωση με τις διατάξεις του κώδικα οδικής κυκλοφορίας και τυχόν τοπικούς περιορισμούς π.χ. στην ταχύτητα) με τους οποίους το όχημα θα πρέπει να εναρμονιστεί.

- **Υποσύστημα ελέγχου** (*Control modu*le): Επιβλέπει την σωστή εκτέλεση της ακολουθίας των ενεργειών που παράγονται από το υποσύστημα σχεδιασμού ενεργειών από τους ενεργοποιητές (σύστημα αυξομείωσης ταχύτητας, σύστημα φώτων, σύστημα χειρισμού οχήματος κτλ) του οχήματος.

Η μηχανική μάθηση (ML) χρησιμοποιείται κατά κόρον σε διεργασίες που σχετίζονται με το υποσύστημα αντίληψης και ιδιαίτερα στη διεργασία δημιουργίας μιας πιστής αναπαράστασης του εξωτερικού περιβάλλοντος, με την χρήση της μάλιστα να ενισχύεται χάρη στη ραγδαία ανάπτυξη που γνωρίζει τα τελευταία χρόνια ο συναφής κλάδος της **μηχανικής όρασης** (computer vision)[11]. Επομένως, δεν προξενεί έκπληξη το γεγονός ότι οι εταιρείες προσφάτως επενδύουν σημαντικά ποσά στη δημιουργία κατάλληλων υποδομών για την επεξεργασία των -κολοσσιαίου μεγέθους- συνόλων δεδομένων που συλλέγουν από πραγματικές καταστάσεις οδήγησης, καθώς και στην πρόσληψη υψηλά καταρτισμένων ατόμων στο αντικείμενο της μηχανικής όρασης για την ανάπτυξη ενός μοντέλου που θα διεκπεραιώνει το σύνολο των σχετικών διεργασιών. Αντίθετα, η χρήση της μηχανικής μάθησης στους τομείς του σχεδιασμού και του ελέγχου βρίσκεται ακόμα σε νηπιακό στάδιο, παρόλο που και σε αυτές τις περιπτώσεις ανακύπτουν εξίσου μεγάλες επενδύσεις από εταιρείες του χώρου. Σε αυτό το πλαίσιο, αξιοποιούνται στο έπακρο τεχνικές μοντελοποίησης συμπεριφορών προκειμένου να αναπτυχθούν πολιτικές στη διαδικασία της οδήγησης που θα προσαρμόζουν τη συμπεριφορά του οχήματος βάσει των εκάστοτε περιβαλλοντικών συνθηκών. Όπως γίνεται αντιληπτό, τα προβλήματα αυτών των κατηγοριών διαφέρουν από τα αντίστοιχα προβλήματα αντίληψης όντας ένας από τους πιο καινοτόμους τομείς έρευνας στην ακαδημαϊκή κοινότητα.

Τα υπάρχοντα συστήματα επιτυγχάνουν ήδη πολύ υψηλές επιδόσεις σε ένα ευρύ φάσμα συνθηκών, παρά ταύτα η ικανότητα γενίκευσής τους (generalization property) περιορίζεται σημαντικά εξαιτίας της ακραίας πολυπλοκότητας και της ποικιλομορφίας που παρουσιάζει ο φυσικός κόσμος. Συνεπώς, μια κρίσιμη πρόκληση που συνδέεται με τα συστήματα μηχανικής μάθησης και χρήζει άμεσης επίλυσης, είναι ο σωστός χειρισμός περιπτώσεων που δεν έχουν ληφθεί υπόψη στο στάδιο του σχεδιασμού, και ειδικότερα στο σύνολο των δεδομένων εκπαίδευσης. Η διασφάλιση ότι, ένα σύστημα τεχνητής νοημοσύνης θα εξακολουθεί να παράγει τα "σωστά" αποτελέσματα ακόμα και υπό απροσδιόριστες συνθήκες, αποτελεί έργο πραγματικά κρίσιμης σημασίας αλλά, παράλληλα, και εξέχουσας δυσκολίας. Αυτό συμβαίνει διότι, ενδεχόμενη

[11] Η **μηχανική όραση** (computer vision) αποτελεί ένα διεπιστημονικό πεδίο, που βρίσκεται στην τομή των πεδίων της μηχανικής μάθησης, της ρομποτικής και της επεξεργασίας σήματος, αποσκοπώντας στην εξαγωγή πληροφοριών από ψηφιακές εικόνες και βίντεο. Περιλαμβάνει όλες τις φάσεις της επεξεργαστικής διαδικασίας δεδομένων εισόδου από την απόκτηση, την επεξεργασία και την ανάλυση τους, έως την παρουσίαση της εξαγόμενης γνώσης ως αριθμητική ή συμβολική πληροφορία.

αδυναμία αυτής της διασφάλισης, μπορεί να οδηγήσει σε επικίνδυνες καταστάσεις, όπως την αγνόηση ενός σημείου στάσης επειδή μπορεί να είναι μερικώς καλυμμένο από χιόνι, ή την ακινητοποίηση του οχήματος εξαιτίας ενός τμήματος θάμνου που μπορεί να εξέχει ελαφρώς από την πλευρά του δρόμου.

5.3 Προστασία δεδομένων σε περιβάλλοντα διασυνδεδεμένων οχημάτων

Το 2016 η Διεθνής Ομοσπονδία Αυτοκινητοβιομηχανιών (FIA) διεξήγαγε μια καμπάνια με την ονομασία (My Car My Data, 2016) για να βολιδοσκοπήσει τις απόψεις των Ευρωπαίων πολιτών στο θέμα των διασυνδεδεμένων οχημάτων. Παρά το γεγονός ότι τα αποτελέσματα κατέδειξαν τον υψηλό δείκτη ενδιαφέροντος των Ευρωπαίων οδηγών όσον αφορά την καινοτομία της διασυνδεσιμότητας προέκυψε επίσης ισχυρός προβληματισμός αναφορικά με το κατά πόσο -πρωτίστως- οι αυτοκινητοβιομηχανίες αλλά και οποιοσδήποτε άλλος εμπλεκόμενος πρόκειται να συμμορφωθεί με το νομοθετικό πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα που παράγονται στα περιβάλλοντα των έξυπνων οχημάτων. Είναι προφανές ότι, για να διασφαλιστεί η προστασία της ιδιωτικότητας αλλά και να τονωθεί η εμπιστοσύνη των χρηστών στο ITS, κάθε ένας από τους εμπλεκόμενους οφείλει να ενσωματώνει την απαίτηση της προστασίας των προσωπικών δεδομένων ήδη από τη φάση του σχεδιασμού του προϊόντος ή της υπηρεσίας που παρέχει (data protection by design) (PrivazyPlan, 2018).

Το πεδίο των διασυνδεδεμένων οχημάτων[12] (connected cars) βρίσκεται στο επίκεντρο των νομοθετικών φορέων την τελευταία δεκαετία γνωρίζοντας σημαντική εξέλιξη τα τελευταία δύο (2) χρόνια. Διάφορες νομοθετικές πρωτοβουλίες έχουν εκδοθεί κατά καιρούς τόσο σε εθνικό όσο και σε διεθνές επίπεδο για την ασφάλεια και την ιδιωτικότητα των συνδεδεμένων οχημάτων συμπληρώνοντας το υφιστάμενο θεσμικό πλαίσιο προστασίας των δεδομένων και της ιδιωτικότητας. Στην επόμενη ενότητα θα παρουσιάσουμε συνοπτικά στις κυριότερες από αυτές.

5.3.1 Πρωτοβουλίες για την προστασία των δεδομένων σε ευρωπαϊκό και σε εθνικό επίπεδο

Τον Ιανουάριο του 2017 ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) δημοσίευσε μια μελέτη με θέμα την κυβερνοασφάλεια στα έξυπνα αυτοκίνητα (ENISA, 2017). Στη μελέτη αυτή κατέγραψαν τα στοιχεία του οχήματος που χρήζουν προστασίας (assets) μαζί με τις αντίστοιχες απειλές (threats), τους κινδύνους (risks) και πιθανά μέτρα αντιμετώπισης αυτών (mitigation measures). Τον Αύγουστο του 2017 ο Βρετανικός φορέας διασυνδεδεμένων και αυτόνομων οχημάτων (CCAV) εξέδωσε ένα έγγραφο που περιελάμβανε ένα σύνολο κατευθυντήριων

[12] Οχήματα εξοπλισμένα στο εσωτερικό τους με πολλές ηλεκτρονικές μονάδες ελέγχου (ECUs) που διασυνδέονται μεταξύ τους μέσω ενός δικτύου, καθώς και των υποδομών που τους επιτρέπουν να διαμοιράζονται πληροφορίες με άλλες συσκευές που βρίσκονται τόσο εντός όσο και εκτός του οχήματος.

οδηγιών για την κυβερνοασφάλεια των διασυνδεδεμένων και αυτόνομων οχημάτων (Department for Transport, Centre for the Protection of National Infrastructure, and Centre for Connected and Autonomous Vehicles, 2017) .Τον Σεπτέμβριο του ίδιου έτους η 39η Οικουμενική Συνέλευση για την Προστασία Δεδομένων που διεξήχθη στο Χονγκ Κονγκ εξέδωσε ένα ψήφισμα για τα διασυνδεδεμένα οχήματα (Global Privacy Assembly, 2017). Το 2017 αποτέλεσε γενικά ένα έτος-ορόσημο για το θεσμικό και κανονιστικό πλαίσιο ασφάλειας των διασυνδεδεμένων οχημάτων αφού τον Οκτώβριο του ίδιου έτους η (Article 29 Data Protection Working Party, 2017)[13] αποδέχθηκε επίσης ένα νομοθέτημα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στα έξυπνα συστήματα μεταφορών συνεργατικής φύσεως (C-ITS). Επιπλέον, τον ίδιο μήνα, η γαλλική αρχή προστασίας δεδομένων προσωπικού χαρακτήρα (CNIL) εξέδωσε ένα έγγραφο συμμόρφωσης (CNIL, 2017) για τα διασυνδεδεμένα αυτοκίνητα, προκειμένου να βοηθήσει τους εμπλεκόμενους φορείς στην εξεύρεση κατάλληλων στρατηγικών για την ενσωμάτωση διαδικασιών προστασίας δεδομένων ήδη από το σχεδιασμό (data protection by design) των προϊόντων τους και εξ ορισμού (data protection by default). Με αυτόν τον τρόπο διασφαλίζεται το δικαίωμα των υποκειμένων των δεδομένων στην άσκηση αποτελεσματικού ελέγχου στα δεδομένα τους.

Τον Απρίλιο του επόμενου έτους (2018) η Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις Τηλεπικοινωνίες[14] σε συνεδρίασή της στη Βουδαπέστη αποδέχθηκε ένα έγγραφο εργασίας για τα διασυνδεδεμένα οχήματα. Η 31η Μαρτίου 2018 αποτέλεσε ημερομηνία-σταθμό για τον τομέα της διασυνδεσιμότητας των οχημάτων στον ευρωπαϊκό χώρο διότι από την ημέρα αυτή έγινε υποχρεωτική η ενσωμάτωση της ηλεκτρονικής υπηρεσίας e-Call[15] σε όλα τα νεοκατασκευασθέντα επιβατηγά οχήματα τύπου M_1 και N_1. Θα πρέπει να σημειωθεί ότι η Ομάδα Εργασίας του Άρθρου 29 είχε προβεί ήδη από το 2006 σε μελέτη των ζητημάτων ιδιωτικότητας και προστασίας των προσωπικών δεδομένων για το σύστημα eCall εκδίδοντας σχετικό έγγραφο εργασίας (Article 29 Working Party, 2006).

[13] Η ομάδα εργασίας του άρθρου 29 είναι η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ).

[14] Η Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις Τηλεπικοινωνίες (IWGDPT) ιδρύθηκε το 1983 με πρωτοβουλία ορισμένων εθνικών αρχών προστασίας δεδομένων ανά τον κόσμο. Τα μέλη της ομάδας δεν περιορίζονται μόνο στις εθνικές αρχές προστασίας δεδομένων, αλλά περιλαμβάνουν επίσης εκπροσώπους του ιδιωτικού τομέα και ΜΚΟ. Τα τελευταία χρόνια, η IWGDPT έχει επικεντρωθεί σε θέματα προστασίας προσωπικών δεδομένων και ιδιωτικότητας σε ICT..

[15] Η υπηρεσία *eCall* ("112") αποσκοπεί στη διευκόλυνση της παροχής άμεσης βοήθειας σε αυτοκινητιστές που εμπλέκονται σε τροχαίο ατύχημα εντός της επικράτειας των κρατών-μελών της Ευρωπαϊκής Ένωσης.

5.3.2 Εφαρμοστέο νομοθετικό πλαίσιο

Εντός της ΕΕ, το εφαρμοστέο δίκαιο για οποιαδήποτε πράξη επεξεργασίας λαμβάνει χώρα σε περιβάλλοντα διασυνδεδεμένων οχημάτων και περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων είναι ο ΓΚΠΔ. Επιπροσθέτως του ΓΚΠΔ, η οδηγία 2002/58/ΕΚ -όπως αναθεωρήθηκε από την 2009/136/ ΕΚ (εφεξής: "οδηγία e-Privacy")- καθορίζει ένα συγκεκριμένο πλαίσιο για όλους τους φορείς που επιθυμούν να αποθηκεύσουν ή να αποκτήσουν πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε τερματικό εξοπλισμό[16] συνδρομητή ή χρήστη συστήματος που κινείται εντός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).

Όπως περιγράφεται από το ΕΣΠΔ[17] στην παράγραφο 40 της 5/2019 γνωμοδότησής του (EDPB, 2019) σχετικά με την αλληλεπίδραση μεταξύ της οδηγίας e-Privacy και του ΓΚΠΔ, στο άρθρο 5 της οδηγίας e-Privacy προβλέπεται ότι, κατά κανόνα και με την επιφύλαξη ορισμένων εξαιρέσεων[18], απαιτείται προηγούμενη συγκατάθεση για την αποθήκευση πληροφοριών ή την απόκτηση πρόσβασης σε πληροφορίες που έχουν ήδη αποθηκευτεί στο τερματικό εξοπλισμό συνδρομητή ή χρήστη. Εφόσον το σύνολο ή τμήμα των πληροφοριών που αποθηκεύονται στη συσκευή του τελικού χρήστη αποτελούν δεδομένα προσωπικού χαρακτήρα, το άρθρο 5 §3 της οδηγίας υπερισχύει του άρθρου 6 του ΓΚΠΔ όσον αφορά τις δραστηριότητες αποθήκευσης ή απόκτησης πρόσβασης σε αυτές τις πληροφορίες. Ωστόσο, για οποιαδήποτε πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα προκύψει μετά τις προαναφερθείσες διαδικασίες επεξεργασίας, συμπεριλαμβανομένης της επεξεργασίας προσωπικών δεδομένων που αποκτώνται προσπελάζοντας πληροφορίες στον τερματικό εξοπλισμό, απαιτείται να υπάρχει νομική βάση σύμφωνα με το άρθρο

[16] Η έννοια του «τερματικού εξοπλισμού» οριοθετείται στην οδηγία 2008/63 / CE13. Συγκεκριμένα στο άρθρο 1 της οδηγίας ο τερματικός εξοπλισμός ορίζεται ως (α) « *ο εξοπλισμός που συνδέεται άμεσα ή έμμεσα με τη διεπαφή ενός δημόσιου τηλεπικοινωνιακού δικτύου που είναι υπεύθυνη για την αποστολή, επεξεργασία ή λήψη πληροφοριών. Σε κάθε περίπτωση (άμεση ή έμμεση), η σύνδεση μπορεί να γίνει μέσω σύρματος, οπτικών ινών ή ηλεκτρομαγνητικά. Μια σύνδεση θεωρείται έμμεση εάν μεταξύ του τερματικής συσκευής και της διεπαφής του δικτύου παρεμβάλλεται επιπρόσθετο είδος εξοπλισμού* (β) *«ο εξοπλισμός δορυφορικών επίγειων σταθμών*». Συνεπώς, υπό την προϋπόθεση ότι πληρούνται τα προαναφερθέντα κριτήρια, το διασυνδεδεμένο όχημα και τα διαφορετικά είδη συσκευών που συνδέονται εντός αυτού θα πρέπει επίσης να θεωρούνται ως «τερματικός εξοπλισμός» (πχ ένας υπολογιστής ή ένα smartphone) και οι διατάξεις του άρθρου 5(3) της οδηγίας e-Privacy εφαρμόζεται όπου απαιτείται.

[17] Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) είναι ένας ανεξάρτητος ευρωπαϊκός οργανισμός, ο οποίος συμβάλλει στη συνεκτική εφαρμογή των κανόνων προστασίας δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση και προάγει τη συνεργασία μεταξύ των αρχών προστασίας δεδομένων της ΕΕ. Το ΕΣΠΔ απαρτίζεται από εκπροσώπους των εθνικών αρχών προστασίας δεδομένων και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ). Το ΕΣΠΔ συστάθηκε με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) και έχει την έδρα του στις Βρυξέλλες.

[18] Το άρθρο 5 §3 της οδηγίας e-Privacy επιτρέπει την αποσύνδεση της απαίτησης για συγκατάθεση από τις δραστηριότητες αποθήκευσης πληροφοριών ή πρόσβασης σε πληροφορίες που είναι ήδη αποθηκευμένες σε τερματικό εξοπλισμό χρήστη όταν (1) γίνονται με αποκλειστικό σκοπό τη διεξαγωγή επικοινωνίας μέσω ενός δικτύου ηλεκτρονικών επικοινωνιών ή (2) είναι απολύτως απαραίτητες προκειμένου να επιτευχθεί η παροχή στο χρήστη μιας υπηρεσίας που ο ίδιος ζήτησε με ρητό τρόπο.

6 του ΓΚΠΔ αλλιώς στερείται νομιμότητας -σύμφωνα και με την παράγραφο 41 του (EDPB, 2019).

Εφόσον ο υπεύθυνος επεξεργασίας υποχρεούται, βάσει του άρθρου 5 §3 της οδηγίας e-Privacy, να ενημερώνει το υποκείμενο των δεδομένων κατά τη διαδικασία λήψης της συγκατάθεσης του για το σύνολο των σκοπών επεξεργασίας που συνδέονται με κάθε πράξη επεξεργασίας -συμπεριλαμβανομένης οποιασδήποτε πράξης επεξεργασίας προκύπτει σε μεταγενέστερο χρόνο με την προϋπόθεση βέβαια ότι πληρείται η συνθήκη περί συμβατότητας των σκοπών- η συγκατάθεση συνιστά συνήθως επαρκή νομική βάση (σύμφωνα και με το άρθρο 6 του ΓΚΠΔ). Συνεπώς, η συγκατάθεση αποτελεί την συνηθέστερη νομική βάση που χρησιμοποιείται τόσο για τις διαδικασίες αποθήκευσης ή/και πρόσβασης σε πληροφορίες που είναι ήδη αποθηκευμένες σε τερματική συσκευή φυσικού προσώπου όσο και για την επακόλουθη επεξεργασία των προσωπικών δεδομένων[19]. Σε κάθε περίπτωση, οι υπεύθυνοι επεξεργασίας πρέπει, κατά τον προσδιορισμό της κατάλληλης νόμιμης βάσης για κάθε είδος πράξης επεξεργασίας στην οποία προβαίνουν, να λαμβάνουν υπόψη τον αντίκτυπο που έχει η εκάστοτε πράξη στα δικαιώματα και τις θεμελιώδεις ελευθερίες των υποκειμένων των δεδομένων. Κατ' αυτόν τον τρόπο αποδεικνύουν τη συμμόρφωσή τους με την αρχή της αντικειμενικότητας (*fairness principle*) όπως επιτάσσει το άρθρο 5 του ΓΚΠΔ και έχει γνωμοδοτήσει σχετικά το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB, 2019).

5.3.3. Κίνδυνοι ιδιωτικότητας και προστασίας δεδομένων

Η Ομάδα Εργασίας του Άρθρου 29 έχει επισημάνει ήδη από το 2014 σε έγγραφό της (Article 29 Data Protection Working Party, 2014) αρκετά ζητήματα ιδιωτικότητας που σχετίζονται με το Διαδίκτυο των Πραγμάτων (IoT) και που μπορούν επίσης να ανακύψουν και στα περιβάλλοντα των διασυνδεδεμένων οχημάτων. Ιδιαίτερα τα ζητήματα που σχετίζονται με την ασφάλεια πληροφοριών και τις διαδικασίες ελέγχου αυτής αποκτούν νέο νόημα στο πλαίσιο των διασυνδεδεμένων οχημάτων. Αυτό συμβαίνει διότι σε ένα περιβάλλον που μέχρι πρότινος θεωρείτο απομονωμένο και προστατευμένο από εξωτερικές παρεμβολές πλέον εξαιτίας της διασυνδεσιμότητας εμφανίζονται ποικίλοι κίνδυνοι που σχετίζονται με την οδική ασφάλεια και οι οποίοι δυνητικά θέτουν σε κίνδυνο τη σωματική ακεραιότητα των ατόμων (π.χ. οδηγού, πεζού).

[19] Η συναίνεση βάσει του άρθρου 5 § 3 της οδηγίας 'e-Privacy' και η συναίνεση που απαιτείται ως νομική βάση για την επεξεργασία δεδομένων βάσει του άρθρου 6 του ΓΚΠΔ για τον ίδιο ρητά διατυπωμένο σκοπό επεξεργασίας μπορούν να συλλεχθούν ταυτόχρονα (για παράδειγμα, τσεκάροντας σε μια φόρμα ένα πεδίο που υποδεικνύει με σαφήνεια σε τι ακριβώς συναινεί το υποκείμενο των δεδομένων).

5.3.3.1 Έλλειψη ενημερωσης χρηστων των οχηματων

Οι οδηγοί και οι επιβάτες των οχημάτων ενδέχεται να μην είναι πάντοτε πλήρως ενημερωμένοι για τις διαδικασίες επεξεργασίας δεδομένων που εκτελούνται εντός ή μέσω του διασυνδεδεμένου οχήματος. Αυτή η πληροφόρηση -η οποία ενδέχεται να παρέχεται με χρονική καθυστέρηση- μπορεί να διατίθεται μόνο στον ιδιοκτήτη του οχήματος, ο οποίος όμως ως οντότητα δεν ταυτίζεται πάντοτε με τον οδηγό. Επομένως, υφίσταται ο κίνδυνος παροχής στους χρήστες των οχημάτων ανεπαρκών μέσων για την άσκηση των νόμιμων διαδικασιών ελέγχου στα προσωπικά τους δεδομένα ούτως ώστε να προστατεύσουν το δικαίωμά τους στην ιδιωτικότητα. Ο κίνδυνος αυτός κρίνεται ιδιαίτερα σοβαρός, ειδικά αν ληφθεί υπόψη ότι, κατά τη διάρκεια του χρόνου ζωής τους, τα οχήματα μπορεί να ανήκουν σε περισσότερους από έναν ιδιοκτήτη είτε λόγω πώλησης είτε λόγω εκμίσθωσής τους σε τρίτους.

Στην κατεύθυνση της μη ενημέρωσης των εμπλεκομένων μερών για τις πράξεις επεξεργασίας που εκτελούνται εντός του οχήματος συμβάλλει και το γεγονός ότι τα μέσα επικοινωνίας του οχήματος ενδέχεται να εκκινούν τη λειτουργία τους είτε με αυτόματο τρόπο είτε από προεπιλογή. Με δεδομένη την απουσία αποτελεσματικών μηχανισμών παρακολούθησης των διεργασιών αλληλεπίδρασης που οχήματος με τον -συνδεδεμένο σε αυτό- εξοπλισμό του, ο έλεγχος της ροής των δεδομένων από τον χρήστη αποτελεί εξαιρετικά δύσκολο έργο. Το έργο γίνεται δυσχερέστερο υπό το πρίσμα της παροχής στο υποκείμενο των δεδομένων μηχανισμών ελέγχου για την αποτροπή της χρήσης των δεδομένων που συνδέονται με αυτό σε μεταγενέστερες πράξεις επεξεργασίας για σκοπούς ασύμβατους με τον αρχικό σκοπό για τον οποίο έχει ήδη συγκατατεθεί[20].

5.3.3.2 Ποιοτητα της συγκαταθεσης των εμπλεκομενων μερων

Όταν η νομική βάση στην οποία στηρίζεται μια πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι η λήψη συναίνεσης από το υποκείμενο των δεδομένων, πρέπει να διασφαλιστεί ότι πληρούνται όλα τα απαραίτητα χαρακτηριστικά που προσδίδουν εγκυρότητα στη συγκατάθεση. Σύμφωνα με το άρθρο 7 του ΓΚΠΔ (Regulation (EU) 2016/679, 2018) προκειμένου μια συγκατάθεση να θεωρηθεί έγκυρη πρέπει να είναι ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει του υποκειμένου των δεδομένων. Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να προσέξουν ιδιαιτέρως τα μέσα που θα χρησιμοποιήσουν για την απόκτηση έγκυρης συγκατάθεσης από διαφορετικούς συμμετέχοντες, όπως ιδιοκτήτες ή χρήστες οχημάτων. Στις περιπτώσεις αυτές η συγκατάθεση πρέπει να παρέχεται χωριστά, για συγκεκριμένους σκοπούς και δεν πρέπει να θεωρείται προαπαιτούμενο για τη σύναψη του συμβολαίου αγοράς ή της εκμίσθωσης ενός νέου αυτοκινήτου. Τέλος, η συγκατάθεση πρέπει να μπορεί να ανακληθεί όσο εύκολα παρέχεται.

[20] Το φαινόμενο αυτό, που είναι γνωστό στη βιβλιογραφία ως *function creep*, καθιστά την μεταγενέστερη επεξεργασία έκνομη διότι στερείται νόμιμης βάσης βάσει του άρθρου 6 του ΓΚΠΔ.

Οι ίδιες ακριβώς προϋποθέσεις με αυτές που αναφέραμε προηγουμένως ισχύουν στις περιπτώσεις όπου η συγκατάθεση απορρέει ως απαίτηση συμμόρφωσης με την οδηγία e-Privacy όπως εάν υπάρχει αποθήκευση πληροφοριών ή προσπελάζονται πληροφορίες που έχουν ήδη αποθηκευτεί στο όχημα. Συνεπώς και η συναίνεση που παρέχεται σε αυτό το πλαίσιο πρέπει να προσεγγιστεί υπό το πρίσμα του ΓΚΠΔ προκειμένου να αξιολογηθεί η εγκυρότητά της.

Σε πολλές περιπτώσεις, ο χρήστης ενδέχεται να μην είναι ενήμερος για τις πράξεις επεξεργασίας προσωπικών δεδομένων που πραγματοποιούνται στο όχημά του. Αυτή η έλλειψη πληροφόρησης αποτελεί τροχοπέδη για την απόδειξη της εγκυρότητας μιας συγκατάθεσης καθώς, βάσει του ΓΚΠΔ, η συγκατάθεση επιβάλλεται να παραχωρείται εν πλήρει επιγνώσει. Σε τέτοιες περιπτώσεις, δεν μπορεί να γίνει επίκληση της συγκατάθεσης ως νομική βάση για την επεξεργασία των δεδομένων.

Τέλος, όταν η οδηγία e-Privacy δεν απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων, ο υπεύθυνος επεξεργασίας είναι αρμόδιος να επιλέξει τη νομική βάση που θεωρεί ανά περίπτωση καταλληλότερη για την εκάστοτε πράξη επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

5.3.3.3. Περαιτερω επεξεργασια προσωπικων δεδομενων

Όταν η νομική βάση στην οποία στηρίζεται η συλλογή των δεδομένων είναι η λήψη συγκατάθεσης όπως απαιτείται από το άρθρο 5 §3 της οδηγίας e-Privacy ή σε περιπτώσεις που η συλλογή εμπίπτει σε μία από τις δύο εξαιρέσεις του άρθρου και στη συνέχεια η πράξη επεξεργασίας εκτελείται σύμφωνα με το άρθρο 6 του ΓΚΠΔ, η μεταγενέστερη επεξεργασία των συλλεχθέντων δεδομένων θεωρείται νόμιμη μόνο εάν ο υπεύθυνος επεξεργασίας ζητήσει εκ νέου συγκατάθεση για τον νέο σκοπό επεξεργασίας ή εάν μπορεί να αποδείξει ότι η επεξεργασία είναι απαραίτητη προκειμένου ο υπεύθυνος να συμμορφωθεί με τους περιορισμούς που αναφέρονται στο άρθρο 23 §1 του ΓΚΠΔ (EDPB, 2020).

Η αρχική συγκατάθεση δεν νομιμοποιεί σε καμία περίπτωση μεταγενέστερη πράξη επεξεργασίας, καθώς η συγκατάθεση πρέπει να δίνεται κατόπιν πλήρους ενημέρωσης του υποκειμένου (informed consent) και να είναι συγκεκριμένη (explicit) προκειμένου να θεωρηθεί έγκυρη όπως αποτυπώνεται και στις ενότητες 3.2 και 3.3 σχετικής γνωμοδότησης του ΕΣΠΔ (EDPB, 2020). Για παράδειγμα, τα δεδομένα τηλεμετρίας (telemetry data), τα οποία συλλέγονται κατά τη χρήση του οχήματος για λόγους συντήρησης, δεν πρέπει να διαβιβάζονται σε ασφαλιστικές εταιρείες χωρίς να έχει δοθεί προηγουμένως η συγκατάθεση του οδηγού ή των χρηστών του οχήματος για την εκτέλεση της συγκεκριμένης πράξης επεξεργασίας με σκοπό τη δημιουργία προφίλ οδηγικής συμπεριφοράς. Η επεξεργασία αυτή επιτρέπει, για παράδειγμα, την προσφορά εξατομικευμένων ασφαλιστηρίων συμβολαίων στους οδηγούς στα οποία η

τιμή των ασφαλίστρων καθορίζεται βάσει της οδηγικής συμπεριφοράς τους (*σ.σ.: με αυτόν τον τρόπο ένας προσεκτικός οδηγός δυνητικά πληρώνει φθηνότερα ασφάλιστρα*).

Επιπλέον, τα δεδομένα που συλλέγονται από διασυνδεδεμένα οχήματα μπορούν να υποβάλλονται σε επεξεργασία από τις αρχές επιβολής του νόμου για τον εντοπισμό περιπτώσεων υπέρβασης του ορίου ταχύτητας ή άλλων παραβάσεων, εφόσον βέβαια πληρούνται οι ειδικοί όροι επεξεργασίας όπως αναφέρονται στο άρθρο 9 της οδηγίας 2016/680 (Directive (EU) 2016/680, 2018). Σε αυτήν την περίπτωση, τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται μπορούν υπό προϋποθέσεις να θεωρηθούν ως σχετιζόμενα με ποινικές καταδίκες και αδικήματα όπως αυτά περιγράφονται στο άρθρο 10 του ΓΚΠΔ. Οι κατασκευαστές μπορούν να παράσχουν στις αρχές επιβολής του νόμου τέτοιες κατηγορίες δεδομένων εφόσον πληρούνται οι ειδικοί όροι για μια τέτοιου είδους επεξεργασία. Το ΕΣΠΔ επισημαίνει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα με μοναδικό σκοπό την ικανοποίηση αιτημάτων που υποβάλλουν οι αρχές επιβολής του νόμου δεν αποτελεί συγκεκριμένο, ρητό και νόμιμο σκοπό κατά την έννοια του άρθρου 5 §1 στοιχείο β' του ΓΚΠΔ. Όταν οι αρχές επιβολής του νόμου έχουν την κατάλληλη εξουσιοδότηση από τον νόμο, τότε μπορεί να θεωρηθούν τρίτα μέρη όπως αυτά ορίζονται στο άρθρο 4 §10 του ΓΚΠΔ. Στην περίπτωση αυτή, οι κατασκευαστές θα έχουν το δικαίωμα να τους παρέχουν όσα δεδομένα έχουν στη διάθεσή τους υπό την προϋπόθεση βέβαια ότι συμμορφώνονται κάθε φορά με το ισχύον νομικό και κανονιστικό πλαίσιο κάθε κράτους-μέλους.

5.3.3.4 Υπερβαλλουσα συλλογη δεδομενων

Με το πλήθος των αισθητήρων που χρησιμοποιείται στα διασυνδεδεμένα οχήματα να αυξάνεται διαρκώς, αυξάνεται εξίσου ο κίνδυνος υπερβάλλουσας συλλογής δεδομένων εν συγκρίσει με αυτά που είναι απολύτως απαραίτητα για την επίτευξη του επιδιωκόμενου σκοπού. Επιπλέον, καθώς στα διασυνδεδεμένα οχήματα ενσωματώνονται ολοένα και περισσότερα συστήματα που χρησιμοποιούν αλγόριθμους μηχανικής μάθησης για τη λειτουργία τους γιγαντώνεται και ο απαιτούμενος αριθμός των δεδομένων που συλλέγονται για μεγάλο χρονικό διάστημα.

5.3.3.5 ανεπαρκεις μηχανισμοι διασφαλισης ασφαλειας προσωπικων δεδομενων

Η ποικιλία των λειτουργιών, των υπηρεσιών και των διεπαφών (π.χ. USB, RFID, Wi-Fi, Bluetooth) που παρέχονται από τα διασυνδεδεμένα οχήματα μοιραία συντελεί στην αύξηση των πιθανών 'τρωτών' σημείων μέσω των οποίων θα μπορούσε να διακυβευτεί η ασφάλεια των προσωπικών δεδομένων των χρηστών. Σε αντίθεση με τις περισσότερες IoT συσκευές, τα διασυνδεδεμένα οχήματα αποτελούν υψηλής κρισιμότητας συστήματα όπου ένα ενδεχόμενο περιστατικό παραβίασης ασφάλειας μπορεί να θέσει σε άμεσο κίνδυνο τη ζωή των χρηστών του οχήματος και των ανθρώπων γύρω του. Είναι λοιπόν αναγκαία η ανάπτυξη κατάλληλων μηχανισμών για

την προστασία του οχήματος από κυβερνοεπιθέσεις που μπορεί να εκμεταλλευτούν τις ευπάθειες των διασυνδεδεμένων οχημάτων.

Επιπλέον, τα προσωπικά δεδομένα που είναι αποθηκευμένα στα οχήματα αλλά και σε περιβάλλοντα εκτός των οχημάτων (π.χ. υποδομές υπολογιστικού νέφους) πρέπει να προστατεύονται επαρκώς έναντι μη εξουσιοδοτημένης πρόσβασης. Για παράδειγμα, κατά τον διαγνωστικό έλεγχο ενός οχήματος, ο εξουσιοδοτημένος τεχνικός είναι απαραίτητο να αποκτήσει πρόσβαση σε ορισμένα από τα διαγνωστικά δεδομένα του οχήματος. Εάν ωστόσο δεν εφαρμόζονται κατάλληλες δικλείδες ασφαλείας (π.χ. μηχανισμοί ελέγχου προσπέλασης) ο τεχνικός μπορεί να επιχειρήσει (με σημαντικές πιθανότητες επιτυχίας) να αποκτήσει πρόσβαση στο σύνολο των δεδομένων που είναι αποθηκευμένα στο όχημα.

5.3.4 Προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού

Λαμβάνοντας υπόψη τον όγκο και την ποικιλομορφία των προσωπικών δεδομένων που παράγονται από τα διασυνδεδεμένα οχήματα, το ΕΣΠΔ επισημαίνει ότι οι υπεύθυνοι επεξεργασίας δεδομένων οφείλουν να διασφαλίζουν ότι οι τεχνολογικές εφαρμογές που αναπτύσσονται στο πλαίσιο των διασυνδεδεμένων οχημάτων έχουν παραμετροποιηθεί ώστε να σέβονται την ιδιωτικότητα των χρηστών εφαρμόζοντας τις απαιτήσεις προστασίας δεδομένων από τον σχεδιασμό και εξ ορισμού όπως επιτάσσει το άρθρο 25 του ΓΚΠΔ. Οι τεχνολογίες πρέπει να σχεδιαστούν στη βάση της αρχής ελαχιστοποίησης των δεδομένων που συγκεντρώνονται κατά τη διαδικασία της συλλογής (collection limitation), να παρέχουν από προεπιλογή επιλογές προσανατολισμένες στην προστασία της ιδιωτικότητας του υποκειμένου (privacy by default) και να διασφαλίζουν ότι τα υποκείμενα των δεδομένων είναι καλά ενημερωμένα και έχουν την δυνατότητα να τροποποιούν με ευκολία τις παραμετροποιήσεις που σχετίζονται με τα προσωπικά τους δεδομένα.

Ορισμένες γενικές πρακτικές, που περιγράφονται παρακάτω, μπορούν επίσης να βοηθήσουν στην άμβλυνση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνδέονται με συνδεδεμένα οχήματα (EDPB, 2021).

5.3.4.1 Επεξεργασια προσωπικων δεδομενων σε τοπικο επιπεδο

Όλοι οι τύποι εμπλεκομένων με τα διασυνδεδεμένα οχήματα θα πρέπει να περιορίζουν, όσο το δυνατόν περισσότερο, διαδικασίες που χρησιμοποιούν προσωπικά δεδομένα για τη λειτουργία τους ή διαδικασίες μεταφοράς προσωπικών δεδομένων εκτός του οχήματος. Ωστόσο, εξαιτίας της φύσης τους τα διασυνδεδεμένα οχήματα καθίστανται ευάλωτα σε επιθέσεις που στοχεύουν τις διεργασίες τοπικής αποθήκευσης προσωπικών δεδομένων ή επιφέρουν αποκάλυψη σε δεδομένα προσωπικού χαρακτήρα

που έχουν αποθηκευτεί τοπικά σε τμήματα του οχήματος τα οποία μετέπειτα πωλούνται. Επομένως, θα πρέπει να εφαρμοστούν τα κατάλληλα μέτρα ασφάλειας για να διασφαλιστεί ότι ο χρήστης διατηρεί τον αποκλειστικό και πλήρη έλεγχο των προσωπικών του δεδομένων. Η τακτική αυτή είναι απόλυτα εναρμονισμένη με την θεμελιώδη απαίτηση της προστασίας της ιδιωτικότητας των χρηστών «εκ του σχεδιασμού» απαγορεύοντας οποιασδήποτε μορφής επεξεργασία δεδομένων από εμπλεκόμενους φορείς χωρίς να έχει ενημερωθεί προηγουμένως το υποκείμενο των δεδομένων. Επιτρέπει επίσης την επεξεργασία "ευαίσθητων" δεδομένων, όπως βιομετρικών δεδομένων ή δεδομένων που σχετίζονται με εγκλήματα ή με άλλες παραβάσεις, καθώς και δεδομένων τοποθεσίας. Τέλος, παρουσιάζει λιγότερους κινδύνους για την κυβερνοασφάλεια με μικρότερη χρονική καθυστέρηση, γεγονός που την καθιστούν ιδανική για μια πλειάδα αυτοματοποιημένων λειτουργιών υποβοήθησης της διαδικασίας οδήγησης όπως:

- **Εφαρμογές οικολογικής οδήγησης** που επεξεργάζονται δεδομένα που παράγονται εντός του οχήματος προκειμένου να εμφανίζουν συμβουλές εξοικονόμησης καυσίμου σε πραγματικό χρόνο στην οθόνη του οχήματος

- **Εφαρμογές που περιλαμβάνουν μεταφορά προσωπικών δεδομένων** σε μια συσκευή που βρίσκεται υπό τον πλήρη έλεγχο του χρήστη όπως για παράδειγμα ένα smartphone, χωρίς τα δεδομένα του οχήματος να διαβιβάζονται σε τρίτους (παρόχους εφαρμογών, κατασκευαστές οχημάτων). Χαρακτηριστικό παράδειγμα αποτελεί η δυνατότητα σύζευξης ενός smartphone με την ηλεκτρονική κονσόλα του αυτοκινήτου για διαμοιρασμό της οθόνης ή την χρήση των συστημάτων πολυμέσων του οχήματος ή του μικροφώνου (για τηλεφωνικές κλήσεις). Όλες αυτές οι δυνατότητες βέβαια θα πρέπει να παρέχονται στο βαθμό που τα δεδομένα που συλλέγονται παραμένουν πάντοτε υπό τον απόλυτο έλεγχο του υποκειμένου των δεδομένων και χρησιμοποιούνται αποκλειστικά για την παροχή της υπηρεσίας που έχει ζητήσει

- **Εφαρμογές που βελτιώνουν την ασφάλεια εντός του οχήματος**, όπως αυτές που παρέχουν ηχητικές ειδοποιήσεις ή απτικές ανατροφοδοτήσεις (π.χ. δονήσεις του τιμονιού όταν ένας οδηγός προσπερνά ένα άλλο όχημα χωρίς φλας ή ξεφεύγει από τις λευκές γραμμές που οριοθετούν μια λωρίδα στην επιφάνεια του οδοστρώματος). Τέλος, στην κατηγορία αυτή ανήκει και η παροχή ειδοποιήσεων σχετικά με την κατάσταση του οχήματος (π.χ., μια ειδοποίηση σχετικά με τη φθορά που επηρεάζει τα τακάκια φρένων)

- **Εφαρμογές σχετικές με τις λειτουργίες ξεκλειδώματος**, **εκκίνησης** ή **ενεργοποίησης συγκεκριμένων λειτουργιών του οχήματος** χρησιμοποιώντας τα βιομετρικά δεδομένα του οδηγού που είναι αποθηκευμένα εντός του (αναπαραστάσεις προσώπου ή φωνής, δακτυλικά αποτυπώματα)

Εφαρμογές όπως οι παραπάνω περιλαμβάνουν επεξεργασία που πραγματοποιείται για την εκτέλεση καθαρά προσωπικών δραστηριοτήτων από φυσικό πρόσωπο (δηλαδή, χωρίς τη μεταφορά προσωπικών δεδομένων σε υπεύθυνο επεξεργασίας δεδομένων ή εκτελούντα την επεξεργασία). Επομένως, σύμφωνα με το άρθρο 2 §2 του ΓΚΠΔ, αυτές οι εφαρμογές **δεν** εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

Ωστόσο, αν και ο ΓΚΠΔ δεν εφαρμόζεται στις περιπτώσεις επεξεργασίας προσωπικών δεδομένων από φυσικό πρόσωπο στο πλαίσιο άσκησης προσωπικών του δραστηριοτήτων, δεν παύει να ισχύει για όλους τους υπεύθυνους ή εκτελούντες την επεξεργασία, οι οποίοι παρέχουν τα μέσα για την επεξεργασία προσωπικών δεδομένων σύμφωνα με την αιτιολογική σκέψη 18 του ΓΚΠΔ. Ως εκ τούτου, όταν οι εμπλεκόμενοι φορείς ενεργούν ως υπεύθυνοι επεξεργασίας δεδομένων ή εκτελούντες την επεξεργασία πρέπει να αναπτύσσουν εντός του αυτοκινήτου εφαρμογές υψηλού επιπέδου ασφάλειας όντας συγχρόνως εναρμονισμένοι με την αρχή προστασίας του ιδιωτικού απορρήτου ήδη από τη φάση του σχεδιασμού όπως και της προστασίας των δεδομένων εξ ορισμού. Σύμφωνα με την αιτιολογική σκέψη 78 του ΓΚΠΔ, «*Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων*». Στην κατεύθυνση αυτή, το ΕΣΠΔ συνιστά την ανάπτυξη μιας ασφαλούς πλατφόρμας εφαρμογών εντός του αυτοκινήτου ή οποία θα διαχωρίζεται σε φυσικό επίπεδο από το σύνολο των λειτουργιών του οχήματος που σχετίζονται με την ασφάλειά του (safety functions).

Οι χρήστες του οχήματος θα πρέπει να έχουν πάντοτε την επιλογή άσκησης ελέγχου στις διαδικασίες συλλογής και επεξεργασίας των δεδομένων τους. Στο πλαίσιο αυτό:

- Οι πληροφορίες που αφορούν την επεξεργασία πρέπει να παρέχονται στη γλώσσα του οδηγού (εγχειρίδιο, ρυθμίσεις κλπ).

- Το ΕΣΠΔ επισημαίνει ότι μόνο δεδομένα που είναι απολύτως απαραίτητα για τη λειτουργία του οχήματος μπορούν να υπόκεινται σε πράξεις επεξεργασίας από προεπιλογή. Σε όλες τις υπόλοιπες περιπτώσεις, τα υποκείμενα των δεδομένων θα πρέπει να έχουν τη δυνατότητα να αποδέχονται ή να απορρίπτουν τις πράξεις επεξεργασίας ανά επιδιωκόμενο σκοπό όπως επίσης και να διαγράφουν τα σχετικά δεδομένα εκτός και αν ο σκοπός και η νομική βάση στην οποία στηρίζεται η επεξεργασία εμπίπτει στις εξαιρέσεις που ορίζονται στην παράγραφο 3 του άρθρου 17 του (Regulation (EU) 2016/679, 2018).

- Τα δεδομένα δεν πρέπει γενικά να διαβιβάζονται σε τρίτους

- Τα δεδομένα πρέπει να διατηρούνται μόνο για όσο διάστημα απαιτείται για την παροχή της υπηρεσίας εκτός αν ορίζεται διαφορετικά από το ευρωπαϊκό δίκαιο ή το δίκαιο του κράτους-μέλους (data retention)

- Τα υποκείμενα των δεδομένων θα πρέπει να δύνανται να διαγράφουν με μόνιμο τρόπο τυχόν υπολειπόμενα προσωπικά δεδομένα πριν από την πώληση των οχημάτων τους

- Τα υποκείμενα των δεδομένων θα πρέπει, όπου είναι εφικτό, να έχουν άμεση πρόσβαση στα δεδομένα που δημιουργούνται από αυτές τις εφαρμογές (δικαίωμα ενημέρωσης)

Τέλος, παρά το γεγονός ότι μπορεί να μην είναι πάντα εφικτή η επεξεργασία δεδομένων σε τοπικό επίπεδο, το μοντέλο της «υβριδικής επεξεργασίας» μπορεί συχνά να τεθεί σε εφαρμογή. Για παράδειγμα, όταν χρησιμοποιείται το μοντέλο της ασφάλισης που βασίζεται στην οδηγική συμπεριφορά, τα προσωπικά δεδομένα που συνδέονται με τα συμπεριφορικά χαρακτηριστικά του οδηγού (όπως η δύναμη που ασκεί στον ποδομοχλό πέδησης ή η χιλιομετρική απόσταση που καλύπτει) είτε υπόκεινται σε επεξεργασίας εντός του οχήματος είτε επεξεργάζονται από κάποιον τρίτο φορέα-εκτελούντα την υπηρεσία (ενδεχομένως κάποιον πάροχο υπηρεσιών τηλεμετρίας) που ενεργεί για λογαριασμό της ασφαλιστικής εταιρείας η οποία εν προκειμένω εκτελεί χρέη υπεύθυνου επεξεργασίας. Με αυτόν τον τρόπο, η ασφαλιστική εταιρεία δεν αποκτά ποτέ η ίδια πρόσβαση στα πρωτογενή συμπεριφορικά δεδομένα, αλλά μόνο στα μετασχηματισμένα δεδομένα που της παράσχει ο εκτελών την επεξεργασία. Με αυτόν τον τρόπο διασφαλίζεται εξ ορισμού η συμμόρφωση με την αρχή της ελαχιστοποίησης των δεδομένων.

5.3.4.2 Ανωνυμοποιηση και ψευδωνυμοποιηση

Εάν πρόκειται να εκτελεστεί διαβίβαση προσωπικών δεδομένων εκτός του οχήματος, τα δεδομένα αυτά θα πρέπει πρώτα να ανωνυμοποιηθούν ή να ψευδωνυμοιηθούν πριν από τη μετάδοσή τους. Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα (όπως ονοματεπώνυμο, ημερομηνία γέννησης, ΑΜΚΑ) από αποθηκευμένα δεδομένα, έτσι ώστε να μην είναι πλέον δυνατόν τα δεδομένα αυτά να συσχετιστούν με το υποκείμενο των δεδομένων το οποίο αφορούν. Βάσει της αιτιολογικής σκέψης 26 (PrivazyPlan, 2021), ο ΓΚΠΔ δεν εφαρμόζεται σε τέτοιας μορφής πληροφορίες (ανωνυμοποιημένες) αφού είναι αδύνατο τα δεδομένα αυτά να συνδεθούν με κάποιο ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ως εκ τούτου, η ανωνυμοποίηση μπορεί να θεωρηθεί ως μια στρατηγική επιλογή ενός υπεύθυνου επεξεργασίας για την κατά κάποιο τρόπο «αποδέσμευσή» του από τις διατάξεις του ΓΚΠΔ και από το αντίστοιχο νομοθετικό

καθεστώς που προδιαγράφεται. Αν και τα πλεονεκτήματα από μια τέτοια επιλογή μπορεί να είναι πολλαπλά[21] το γεγονός ότι η ανωνυμοποίηση αποτελεί μη αναστρέψιμη διαδικασία που καταργεί την ικανότητα αναγνώρισης των υποκειμένων των δεδομένων, μπορεί να έχει ως αποτέλεσμα την υποβάθμιση της χρησιμότητας και χρηστικότητας των ανωνυμοποιημένων δεδομένων και σε πολλές περιπτώσεις να τα καταστήσει μη εκμεταλλεύσιμα για σκοπούς επεξεργασίας.

Το 2014 η Ομάδα Εργασίας του Άρθρου 29 ανέλυσε την αποτελεσματικότητα των -μέχρι τότε- υφισταμένων τεχνικών ανωνυμοποίησης (Article 29 Data Protection Working Party, 2014) για την προστασία των δεδομένων και εξέδωσε συστάσεις για τη διαχείριση αυτών των τεχνικών, λαμβάνοντας υπόψη τον υπολειπόμενο κίνδυνο (residual risk) που προκύπτει κατά την ταυτοποίηση των υποκείμενων των δεδομένων σε καθεμία από αυτές τις τεχνικές. Παράλληλα, στο ίδιο κείμενό αναλύεται εκτενώς και η τεχνική της ψευδωνυμοποίησης και αποσαφηνίζονται ορισμένες παρανοήσεις αναφορικά με τις διαφορές μεταξύ της ψευδωνυμοποίησης και της ανωνυμοποίησης.

Στο άρθρο 4 § 5 του ΓΚΠΔ η ψευδωνυμοποίηση ορίζεται ως: «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο*». Στο άρθρο 25 του ΓΚΠΔ η ψευδωνυμοποίηση θεωρείται και ως μέθοδος που διασφαλίζει την τήρηση της αρχής της ελαχιστοποίησης των δεδομένων (data minimization): «*ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων*». Αντίστοιχη διατύπωση συναντάται και στο άρθρο 89 του κανονισμού. Οι τεχνικές ψευδωνυμοποίησης (ENISA, 2021) μπορούν να εκληφθούν ως εναλλακτική λύση της κρυπτογράφησης, ιδιαίτερα όσον αφορά το θέμα της «χρηστικότητας» των δεδομένων, επιτρέποντας την αντικατάσταση μόνο των προσωπικών αναγνωριστικών (personal identifiers) από τα δεδομένα, έτσι ώστε αυτά να περιέχουν μόνο ψευδή αναγνωριστικά. Τα δεδομένα δεν δύνανται να αποδοθούν σε κάποιο υποκείμενο, και ταυτόχρονα δεν περιορίζεται η ευκολία της επεξεργασίας τους. Ωστόσο, τα ψευδωνυμοποιημένα δεδομένα ενέχουν τον κίνδυνο ταυτοποίησης του υποκειμένου σε περιπτώσεις που ένας τρίτος κατορθώσει να αποκαλύψει τον μηχανισμό ψευδωνυμοποίησης, ή συνδέσει με άλλο τρόπο το ψευδοανωνυμοποιημένο σύνολο δεδομένων με τα υποκείμενα. Για τον λόγο αυτόν ο ΓΚΠΔ θέτει ως απαίτηση οι «*πρόσθετες πληροφορίες*» που χρησιμοποιούνται για την υλοποίηση της ψευδωνυμοποίησης να διατηρούνται σε ξεχωριστή τοποθεσία, και να «*υπόκεινται σε κατάλληλα τεχνικά και οργανωτικά μέτρα*»,

[21] Μεταξύ αυτών η διευκόλυνση της διεθνούς διακίνησης των ανωνυμοποιημένων δεδομένων όπως και η άρση των περιορισμών σχετικά με τον χρόνο διατήρησης των δεδομένων στη διάθεση του υπεύθυνου επεξεργασίας.

προκειμένου να καταστεί δυνατή η διασφάλιση και προστασία των προσωπικών δεδομένων των υποκειμένων. Θα πρέπει εδώ να σημειωθεί ότι τα ψευδωνυμοποιημένα δεδομένα προσωπικού χαρακτήρα εξακολουθούν να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και, ως εκ τούτου, εμπίπτουν στις διατάξεις και στους περιορισμούς που θέτει ο ΓΚΠΔ.

5.3.4.3 Μελετη εκτιμησης αντικτυπου

Δοθέντων του πλήθους και του ευαίσθητου περιεχομένου των προσωπικών δεδομένων που μπορούν να δημιουργηθούν μέσω των διασυνδεδεμένων οχημάτων η επεξεργασία -σύμφωνα και με το άρθρο 35 §1 του (Regulation (EU) 2016/679, 2018)- οδηγεί συχνά σε υψηλό κίνδυνο για τα θεμελιώδη δικαιώματα και τις ελευθερίες των χρηστών του εκάστοτε οχήματος (ιδιαίτερα σε περιπτώσεις που αυτή διενεργείται εκτός του οχήματος) . Όποτε συμβαίνει αυτό, οι εμπλεκόμενοι φορείς καλούνται να διενεργήσουν μια μελέτη εκτίμησης αντικτύπου (DPIA) όσον αφορά την προστασία των προσωπικών δεδομένων των υποκειμένων για να προσδιορίσουν και να μετριάσουν τις επιπτώσεις των κινδύνων που περιγράφονται εκτενώς στα άρθρα 35 και 36 του ΓΚΠΔ. Ακόμη και στις περιπτώσεις όπου δεν απαιτείται DPIA, είναι εξαιρετικά καλή πρακτική η διεξαγωγή της το συντομότερο δυνατό (από τη φάση του σχεδιασμού) καθώς με αυτόν τον τρόπο όλοι οι εμπλεκόμενοι των διασυνδεδεμένων οχημάτων (κατασκευαστές, πάροχοι υπηρεσιών) που δρουν ως υπεύθυνοι επεξεργασίας θα είναι ενήμεροι για το σύνολο των κινδύνων ιδιωτικότητας που αντιμετωπίζουν τα συστήματά τους πριν από την ανάπτυξη ή την υιοθέτηση νέων τεχνολογικών εφαρμογών. Οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να προχωρήσουν σε δημοσίευση των αποτελεσμάτων της διενεργηθείσας DPIA (ή τμημάτων αυτής), παρόλο που αυτό δεν είναι υποχρεωτικό από τον ΓΚΠΔ, προκειμένου να ενισχύσουν την εμπιστοσύνη των υποκειμένων στις διαδικασίες επεξεργασίας και να αποδείξουν τη συμμόρφωσή τους με τις απαιτήσεις της διαφάνειας και της λογοδοσίας (Article 29 Data Protection Working Party, 2017). Τέλος, βάσει του ΓΚΠΔ, μη εκτέλεση μιας DPIA όταν αυτή επιβάλλεται από την διενεργηθείσα πράξη επεξεργασίας (άρθρο 35 §1,§3,§4), ή η εκτέλεση μιας DPIA με εσφαλμένο τρόπο (άρθρο 35 § 2, §7-9)), ή η μη συνδρομή της αρμόδιας εποπτικής αρχής όπου αυτή απαιτείται (άρθρο 36 §3 στοιχείο ε’), μπορεί να επιφέρει διοικητικό πρόστιμο έως δέκα εκατομμύρια (10,000,000) ευρώ, ή στην περίπτωση επιχείρησης, έως και 2% στον συνολικό ετήσιο κύκλο εργασιών του προηγούμενου οικονομικού έτους, όποιο από τα δύο είναι υψηλότερο.

5.3.4.4 Διαφανης ενημερωση και προϋποθεσεις για την ασκηση των δικαιωματων του υποκειμενου των δεδομενων

Πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το υποκείμενο των δεδομένων ενημερώνεται για την ταυτότητα του υπευθύνου επεξεργασίας δεδομένων, τον σκοπό της επεξεργασίας, τους παραλήπτες των δεδομένων, την χρονική περίοδο για την οποία τα δεδομένα θα πρέπει να αποθηκευτούν καθώς και τα δικαιώματά του σύμφωνα με την αρχή της διαφάνειας (transparency principle) για την

οποία γίνεται ειδική μνεία στην αιτιολογική σκέψη 58 του ΓΚΠΔ (PrivazyPlan, 2021). Επομένως, όσοι εμπλεκόμενοι με τα διασυνδεδεμένα οχήματα ασκούν καθήκοντα υπεύθυνου επεξεργασίας θα πρέπει να παρέχουν στο υποκείμενο τις ακόλουθες πληροφορίες, διατυπωμένες με σαφήνεια, απλότητα και εύκολα προσβάσιμη μορφή:

- Τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων

- Τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα προσωπικά δεδομένα καθώς και τη νομική βάση για την επεξεργασία

- Τη ρητή παράθεση των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας δεδομένων ή ένα τρίτο μέρος, όταν αυτά τα νόμιμα συμφέροντα αποτελούν τη νομική βάση για επεξεργασία

- Τους αποδέκτες ή τις κατηγορίες αποδεκτών των προσωπικών δεδομένων (εφόσον υπάρχουν)

- Το χρονικό διάστημα για το οποίο θα διατηρηθούν αποθηκευμένα τα προσωπικά δεδομένα, ή εάν αυτό είναι αδύνατο, τα κριτήρια που χρησιμοποιήθηκαν για να προσδιοριστεί το διάστημα αυτό

- Την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος εναντίωσης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων

- Την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης ανά πάσα στιγμή χωρίς να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της

- Όποτε απαιτείται το γεγονός ότι ο υπεύθυνος επεξεργασίας προτίθεται να μεταφέρει προσωπικά δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό καθώς και τα μέτρα ασφάλειας που θα που χρησιμοποιούνται για τη μεταφορά τους

- Κατά πόσο η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση ή απαίτηση για τη σύναψη σύμβασης, καθώς και κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών

- Η ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ που παράγει νομικά αποτελέσματα σχετικά με το

υποκείμενο των δεδομένων ή παρομοίως επηρεάζει σημαντικά το υποκείμενο των δεδομένων, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων. Αυτό θα μπορούσε να ισχύει ιδιαίτερα σε σχέση με την παροχή ασφάλισης βάσει χρήσης σε ιδιώτες

- Το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή

- Πληροφορίες για περαιτέρω επεξεργασία

- Σε περίπτωση από κοινού ελέγχου δεδομένων, σαφείς και πλήρεις πληροφορίες σχετικά με τις ευθύνες κάθε υπεύθυνου επεξεργασίας δεδομένων

Σε ορισμένες περιπτώσεις, τα προσωπικά δεδομένα δεν συλλέγονται απευθείας από το άτομο με το οποίο σχετίζονται. Για παράδειγμα, ένας κατασκευαστής οχημάτων και εξοπλισμού μπορεί να βασιστεί σε έναν αντιπρόσωπο για να συλλέξει πληροφορίες σχετικά με τον ιδιοκτήτη του οχήματος, προκειμένου να προσφέρει μια υπηρεσία οδικής βοήθειας. Όταν τα δεδομένα δεν έχουν συλλεχθεί με άμεσο τρόπο, ο κατασκευαστής οχημάτων και εξοπλισμού, ο πάροχος υπηρεσιών ή οποιοσδήποτε άλλος εμπλεκόμενος σε ένα περιβάλλον διασυνδεδεμένων οχημάτων δρα ως υπεύθυνος επεξεργασίας δεδομένων, εκτός από τις προαναφερθείσες πληροφορίες, αναφέρει επίσης τις κατηγορίες των προσωπικών δεδομένων, την πηγή από την οποία προέρχονται τα προσωπικά δεδομένα και, κατά περίπτωση, εάν αυτά τα δεδομένα προέρχονταν από δημόσια προσβάσιμες πηγές. Αυτές οι πληροφορίες πρέπει να παρέχονται από τον υπεύθυνο επεξεργασίας εντός εύλογου χρονικού διαστήματος μετά τη λήψη των δεδομένων και το αργότερο κατά την πρώτη από τις ακόλουθες ημερομηνίες σύμφωνα με το άρθρο 14 §3 του ΓΚΠΔ:

(i) ένα (1) μήνα μετά τη λήψη των δεδομένων, λαμβανομένων υπόψη των ειδικών περιστάσεων υπό τις οποίες υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα,

(ii) κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων,

(iii) εάν αυτά τα δεδομένα πρόκειται να διαβιβαστούν σε τρίτους, πριν από τη διαβίβαση των δεδομένων.

Οι πληροφορίες που απευθύνονται στα υποκείμενα των δεδομένων μπορούν να παρέχονται σε επίπεδα ανάλογα με την σπουδαιότητα του περιεχομένου τους. Για παράδειγμα, θα μπορούσαν να οριστούν δύο (2) επίπεδα πληροφοριών με το πρώτο επίπεδο να περιλαμβάνει τις πιο σημαντικές για τα υποκείμενα των δεδομένων και το δεύτερο πληροφορίες που πιθανώς να είναι σημαντικές αλλά σε μεταγενέστερο στάδιο. Οι κυριότερες πληροφορίες του πρώτου επιπέδου περιλαμβάνουν, εκτός από την

ταυτότητα του υπευθύνου επεξεργασίας δεδομένων, τον σκοπό της επεξεργασίας και την περιγραφή των δικαιωμάτων του υποκειμένου των δεδομένων, καθώς και τυχόν πρόσθετες πληροφορίες σχετικά με τις πράξεις επεξεργασίας που ενέχουν υψηλό κίνδυνο στα θεμελιώδη δικαιώματα και τις ελευθερίες τους. Στα περιβάλλοντα των διασυνδεδεμένων οχημάτων το ΕΣΠΔ επιτάσσει να ενημερώνεται το υποκείμενο των δεδομένων για όλους τους αποδέκτες πληροφοριών πρώτου επιπέδου. Σύμφωνα με τις κατευθυντήριες οδηγίες που έχει εκδώσει η (Article 29 Data Protection Working Party, 2018) για τη διασφάλιση της διαφάνειας κατά την επεξεργασία, οι υπεύθυνοι επεξεργασίας θα πρέπει να γνωστοποιούν στα υποκείμενα των δεδομένων πληροφορίες των αποδεκτών των προσωπικών τους δεδομένων. Αυτό μπορεί να επιτευχθεί με την κατονομασία του συνόλου των αποδεκτών, έτσι ώστε τα υποκείμενα των δεδομένων να γνωρίζουν με ακρίβεια ποιοι χρησιμοποιούν τα προσωπικά τους δεδομένα. Εάν, ωστόσο, οι υπεύθυνοι επεξεργασίας δεν μπορούν να γνωστοποιήσουν στα υποκείμενα τα πλήρη στοιχεία των αποδεκτών, οι πληροφορίες που θα παράσχουν θα πρέπει να είναι όσο το δυνατόν πιο συγκεκριμένες, αναφέροντας τον τύπο του εκάστοτε αποδέκτη, τον τομέα δραστηριοποίησής του καθώς και την τοποθεσία του.

5.4 Κυβερνοασφάλεια συστημάτων τεχνητής νοημοσύνης που χρησιμοποιούνται στα οχήματα αυτοματοποιημένης οδήγησης

Η ραγδαία ανάπτυξη οχημάτων αυτοματοποιημένης οδήγησης και οι συνακόλουθες απαιτήσεις λειτουργικότητας και διασυνδεσιμότητας αυξάνουν την πιθανότητα εκδήλωσης επιθέσεων κυβερνοασφάλειας. Οι κίνδυνοι κυβερνοασφάλειας στα οχήματα αυτοματοποιημένης οδήγησης έχουν άμεση επίπτωση στην ασφάλεια των επιβατών, των πεζών, των υπόλοιπων οχημάτων και των αντίστοιχων υποδομών τους. Σε αυτό το κεφάλαιο θα επικεντρωθούμε στην παράθεση των ευπαθειών και των ζητημάτων ασφάλειας στα συστήματα τεχνητής νοημοσύνης που χρησιμοποιούνται από τα οχήματα αυτοματοποιημένης οδήγησης.

Οι απειλές που σχετίζονται με τα AI συστήματα διακρίνονται γενικά σε σκόπιμες (intentional) και μη σκόπιμες (non-intentional). Οι σκόπιμες απειλές περιλαμβάνουν την εκμετάλλευση από κακόβουλες οντότητες ευπαθειών που ελλοχεύουν σε τεχνικές μηχανικής μάθησης και μοντέλα τεχνικής νοημοσύνης αποσκοπώντας στην πρόκληση ζημιών (φυσικών ή μη) στα συστήματα αυτά. Η αυξανόμενη χρήση AI συστημάτων κυρίως για την αυτοματοποίηση της διαδικασίας λήψης αποφάσεων σε μια πλειάδα διαφορετικών τομέων καθιστά τα ψηφιακά συστήματα ευάλωτα σε ένα σύνολο κυβερνοεπιθέσεων η επιτυχής εκδήλωση των οποίων μπορεί να επιφέρει σοβαρές επιπτώσεις στη λειτουργία του συστήματος. Στο σημείο αυτό θα πρέπει να σημειώσουμε ότι οι μέθοδοι τεχνητής νοημοσύνης δεν αποτελούν κατ' ανάγκη τμήμα μόνο των διαφόρων μηχανισμών άμυνας των συστημάτων από τις κυβερνοεπιθέσεις. Αντιθέτως, μπορεί να αποτελέσουν εξαιρετικά χρήσιμο εργαλείο στα χέρια των επιτιθέμενων για την αυτοματοποίηση τμημάτων των

επιθέσεών τους επιτρέποντάς τους να ασκήσουν τις επιθέσεις τους με μεγαλύτερη ταχύτητα, μικρότερο κόστος και υψηλότερη ακρίβεια.

Οι μη σκόπιμες απειλές προκύπτουν ακούσια στα πλαίσια της χρήσης ενός συστήματος από εξουσιοδοτημένους χρήστες. Εκδηλώνονται με τη μορφή ξαφνικής καταστροφής ή διακοπής λειτουργίας ή κάποια άλλη μορφή και προκύπτουν είτε από κακό σχεδιασμό του συστήματος είτε από εγγενείς αδυναμίες στα χρησιμοποιούμενα μοντέλα τεχνητής νοημοσύνης και στις διάφορες τεχνικές μηχανικής μάθησης. Μια από τις αδυναμίες αυτές είναι η έλλειψη αμεροληψίας στις αποφάσεις που λαμβάνουν τα συστήματα αυτά εξαιτίας της διάδοσης μεροληψίας από τα δεδομένα εισόδου στα μοντέλα και τα αποτελέσματα αυτών. Επιπλέον εμφανίζεται συχνά αδιαφάνεια στη διαδικασίας λήψης αποφάσεων λόγω της σύνθετης δομής του εκάστοτε χρησιμοποιούμενου μοντέλου και των πολύπλοκων μαθηματικών λειτουργιών που αυτό περιλαμβάνει όπως και ανασφάλεια εξαιτίας της 'κακής' αναπαράστασης κρίσιμων λειτουργιών του συστήματος ή την ανάκυψη καταστάσεων που στις οποίες το μοντέλο δεν έχει εκπαιδευθεί από τα δεδομένα εκπαίδευσης που του τροφοδοτήθηκαν κατά τη φάση ανάπτυξής του.

5.4.1 Περιπτώσεις AI φυσικών επιθέσεων ενάντια στα αυτόνομα οχήματα

Τα τελευταία χρόνια έχουν αναφερθεί ποικίλλες περιπτώσεις φυσικών επιθέσεων έναντι των συστημάτων τεχνητής νοημοσύνης των ημιαυτόνομων οχημάτων. Μια από τις πιο διαδεδομένες επιθέσεις αυτού του είδους συναντάται στη διεθνή βιβλιογραφία με το ακρωνύμιο **DARTS** (Sitawarin, Bhagoji, Mosenia, Chiang, & Mittal, 2018). Οι επιθέσεις αυτές στοχεύουν το υποσύστημα αντίληψης ενός αυτόνομου οχήματος και ειδικότερα τις λειτουργίες αναγνώρισης των οδικών σημάτων από τα αυτόνομα οχήματα. Η συγκεκριμένη τεχνική ενισχύει τις επιθέσεις διατάραξης[22] επιτρέποντας στα αποτελέσματα τους να αποκτήσουν εκτυπώσιμη μορφή. Οι (Morgulis, Kreines, Mendelowitz, & Weisglass, 2019) απέδειξαν ότι εάν οι εικόνες που προκύψουν από τις επιθέσεις αυτές αναπαρασταθούν σε έντυπη μορφή προσομοιάζοντας πινακίδες οδικής σήμανσης τότε μπορούν να 'ξεγελάσουν' το σύστημα ταξινόμησης εικόνων ενός αυτόνομου οχήματος. Συγκεκριμένα, στα πλαίσια των εν λόγω ερευνών, τόσο οι πλαστογραφημένες (spoofed) όσο και οι αυθεντικές πινακίδες οδικής σήμανσης τοποθετήθηκαν στον περιβάλλοντα χώρο ενός αυτόνομου οχήματος. Τα αποτελέσματα έδειξαν ότι και τα δύο είδη πινακίδων έγιναν αντιληπτά και αποτέλεσαν αντικείμενο επεξεργασίας από το υποσύστημα αντίληψης του οχήματος με τις αλλοιωμένες εικόνες μάλιστα όχι μόνο να ταξινομούνται με εσφαλμένο τρόπο, αλλά να προκαλούν και κάποιες απροσδόκητες συμπεριφορές του οχήματος.

[22] Οι επιθέσεις διατάραξης (perturbation attacks) περιλαμβάνουν οποιαδήποτε ενέργεια τροποποιεί ελαφρώς το περιεχόμενο μιας εικόνας διατηρώντας όμως παράλληλα την αρχική της σημασιολογία, εξαπατώντας με αυτόν τον τρόπο το εκάστοτε χρησιμοποιούμενο μοντέλο μηχανικής εκμάθησης.

Στο ίδιο πλαίσιο, η ομάδα ερευνητών για προηγμένες απειλές της εταιρείας McAfee (McAfee ATR team) μελέτησε πώς τα AI συστήματα των οχημάτων αυτοματοποιημένης οδήγησης μπορούν να εξαπατηθούν από μια σειρά γνωστών στην ερευνητική κοινότητα τεχνικών όπως οι τεχνικές αντιπαραθετικής μηχανικής μάθησης (adversarial ML)[23]. Έτσι, οι (Povolny & Trivedy, 2020) σχεδίασαν ένα σενάριο επίθεσης για τα αυτοκίνητα της εταιρείας Tesla βάσει του οποίου παραποίησαν την ένδειξη των 35 mph μιας υπάρχουσας πινακίδας που υποδείκνυε το ανώτατο επιτρεπόμενο όριο ταχύτητας της περιοχής χρησιμοποιώντας μαύρη ταινία για να επιμηκύνουν ελαφρώς τη μεσαία γραμμή του αριθμητικού ψηφίου "3". Παρά την απλοϊκή της μορφή η επίθεση πέτυχε καθώς το υποσύστημα αντίληψης εικόνων του αυτοκινήτου εξέλαβε την αριθμητική τιμή των ‘35’ mph ως ‘85’ mph αναπτύσσοντας με αυτόν τον τρόπο ταχύτητα κατά πολύ μεγαλύτερη (137 km / h) από το επιτρεπόμενο στην περιοχή όριο ταχύτητας (περίπου 56 km/h).

Επιπλέον σε μια άλλη έρευνα η οποία είχε ως πεδίο εφαρμογής το ευρέως χρησιμοποιούμενο σύστημα υποβοήθησης οδήγησης (ADAS) MobilBeye, οι ερευνητές (Nassi, Ben-Netanel, Elovici, & Nassi, 2019) τοποθέτησαν στο οδικό δίκτυο πλαστές εικόνες σημάτων οδικής κυκλοφορίας προκειμένου να εκτιμήσουν κατά πόσο ενδεχόμενες περιβαλλοντικές μεταβολές (π.χ. αλλαγές στο χρώμα και το σχήμα ενός σήματος, την ταχύτητα προβολής εικόνων και τις συνθήκες περιβαλλοντικού φωτισμού) μπορούν δυνητικά να αποτελέσουν κρίσιμο παράγοντα επιτυχίας μιας επίθεσης. Για την διεξαγωγή των πειραμάτων, χρησιμοποίησαν ένα drone που μετέφερε έναν φορητό προβολέα, ο οποίος φώτιζε το εκάστοτε πλαστό οδικό σήμα. Τα πειράματά τους απέδειξαν ότι ήταν εφικτή η εξαπάτηση του Mobileye, κατά τέτοιο τρόπο ώστε να ερμηνεύει το προβαλλόμενο πλαστό σήμα κυκλοφορίας ως αυθεντικό σήμα κυκλοφορίας.

Η ερευνητική ομάδα (Tencent Keen Security Lab, 2019) πραγματοποίησε μια ολοκληρωμένη μελέτη βασισμένη σε τεχνικές αντίστροφης μηχανικής (reverse engineering) για την εύρεση ζητημάτων ασφαλείας σε ένα αυτοκίνητο Tesla. Ορισμένες από τις σοβαρότερες αδυναμίες που αναδείχθηκαν αφορούσαν τα συστήματα αντίληψης του οχήματος. Μεταξύ άλλων κατόρθωσαν να ενεργοποιήσουν τους υαλοκαθαριστήρες εκπέμποντας σήματα θορύβου σε μια ηλεκτρονική οθόνη που ήταν τοποθετημένη μπροστά από το όχημα, ξεγελώντας έτσι τον οπτικό αισθητήρα του συστήματος. Επικεντρώθηκαν επίσης στο σύστημα αναγνώρισης λωρίδων όπου αποδείχθηκε ότι με την εφαρμογή τεχνικών μείωσης της ευκρίνειας (blur) σε μια λωρίδα κυκλοφορίας το σύστημα αντίληψης του αυτοκινήτου ενδέχεται να μην δύναται να την εντοπίσει. Επίσης ένα άλλο συμπέρασμα στο οποίο κατέληξαν οι ερευνητές (παρόλο που ακόμα δεν έχει επιβεβαιωθεί επισήμως σε πραγματικές συνθήκες οδήγησης) είναι ότι το σύστημα αντίληψης του οχήματος μπορεί να χειραγωγηθεί και

[23] Η αντιπαραθετική μηχανική μάθηση αποτελεί μια τεχνική που χρησιμοποιείται στον τομέα της μηχανικής μάθησης για τον εντοπισμό δεδομένων εισόδου που μπορούν δυνητικά να ‘ξεγελάσουν’ ένα μοντέλο.

να συνθέσει μη υπαρκτές λωρίδες κυκλοφορίας εφόσον τοποθετηθούν αυτοκόλλητα σε κατάλληλα σημεία του δρόμου. Σε αυτήν την περίπτωση, ένας άνθρωπος οδηγός πιθανότατα θα είχε αντιληφθεί την απόπειρα εξαπάτησης και θα βασιζόταν στην κοινή λογική για να αντιδράσει σωστά.

Τέλος, οι (Chernikova, Oprea, Nita-Rotaru, & Kim, 2019) σε πρόσφατη έρευνά τους απέδειξαν ότι τα συστήματα του οχήματος τα οποία επιφορτίζονται με την ευθύνη της εκτίμησης της κατεύθυνσης στην οποία στρίβει το τιμόνι ενός αυτόνομου αυτοκινήτου σε μια δεδομένη χρονική καθίστανται ευάλωτα σε επιθέσεις που εξαπατούν το μοντέλο μηχανικής μάθησης κατά τη διαδικασία τροφοδότησής του με δεδομένα σε πραγματικό χρόνο[24]. Οι επιθέσεις αυτές είναι γνωστές στη βιβλιογραφία ως '*evasion attacks*' (Towards data science, 2019).

5.4.2. Σενάρια AI επιθέσεων στα αυτόνομα οχήματα

Τα τελευταία χρόνια το ενδιαφέρον της ερευνητικής κοινότητας για τον εντοπισμό ζητημάτων ασφάλειας σε συστήματα τεχνητής νοημοσύνης αυτόνομων οχημάτων διαρκώς αυξάνεται. Στο πλαίσιο αυτό περιγράφονται με λεπτομέρεια πιθανές επιπτώσεις τόσο στη λειτουργία του οχήματος όσο και σε σχετιζόμενες με αυτό υποδομές προτείνοντας παράλληλα ενδεικτικές τεχνικές μετριασμού των επιπτώσεων αυτών. Συγκεκριμένα, έχουν προσδιοριστεί διάφορες κατηγορίες απειλών που σχετίζονται με τους διαφορετικούς αισθητήρες, τους μηχανισμούς ελέγχου και τους μηχανισμούς επικοινωνιών. Εκτός από τις ευπάθειες που αφορούν ειδικά τα συστήματα ML και στις οποίες αναφερθήκαμε στην προηγούμενη ενότητα, ζητήματα ασφάλειας που σχετίζονται με την τεχνητή νοημοσύνη εκμεταλλεύονται επίσης τις πιο διαδεδομένες ευπάθειες σε επίπεδο υλικού και λογισμικού των ψηφιακών συστημάτων, επεκτείνοντας παράλληλα το πεδίο των επιθέσεων. Μερικά από αυτά τα θέματα ασφάλειας είναι τα ακόλουθα:

- **'Τύφλωση' ή θόλωση των αισθητήρων (sensor jamming)**: Η λειτουργία των αισθητήρων του οχήματος διακόπτεται ή μπλοκάρεται προσωρινά. Με αυτόν τον τρόπο, ο εισβολέας μπορεί να χειραγωγήσει το AI μοντέλο, να τροφοδοτήσει τον αλγόριθμο με λανθασμένα δεδομένα ή να παρέχει σκόπιμα ελλιπή δεδομένα ώστε να μειώσει την αποτελεσματικότητα της αυτοματοποιημένης λήψης αποφάσεων.

- **Επιθέσεις άρνησης υπηρεσιών (DoS/DDoS attacks)**: Στόχος των συγκεκριμένων επιθέσεων αποτελεί η διακοπή του συνόλου των επικοινωνιών που διατίθενται στο όχημα αυτοματοποιημένης οδήγησης καθιστώντας το ουσιαστικά 'τυφλό' ως προς το περιβάλλον του. Προφανώς πλήττουν την

[24] Η φάση αυτή αποτελεί την δεύτερη στον κύκλο ζωής ενός ML μοντέλου μετά από αυτήν τις εκπαίδευσης του μοντέλου (ML training phase) και συνίσταται στη πρόσδοση δυνατοτήτων συμπερασματολογίας στο μοντέλο (ML inference).

απαίτηση της διαθεσιμότητας στο όχημα παρεμποδίζοντας τις λειτουργίες που καθιστούν δυνατή την αυτόνομη οδήγηση.

- **Χειραγώγηση επικοινωνιών οχημάτων (Manipulating vehicle communications)**: Οι συγκεκριμένες επιθέσεις παρουσιάζουν σοβαρές επιπτώσεις στις λειτουργίες που επιτρέπουν την αυτόνομη οδήγηση επιτρέποντας στον επιτιθέμενο άλλοτε να τροποποιήσει το περιεχόμενο των μηνυμάτων που αποστέλλει το όχημα προς το περιβάλλον του (άλλα οχήματα ή σχετιζόμενες υποδομές) και άλλοτε το αντίστροφο (να τον εξαναγκάσει δηλαδή σε λανθασμένη ερμηνεία των πακέτων μηνυμάτων που προέρχονται από την οδική υποδομή).

- **Αποκάλυψη πληροφοριών (Information disclosure)**: Δεδομένης της αφθονίας (προσωπικών και ευαίσθητων) πληροφοριών που αποθηκεύονται και χρησιμοποιούνται από τα οχήματα ώστε να καταστεί εφικτή η αυτόνομη οδήγηση συμπεριλαμβανομένων κρίσιμων δεδομένων που αφορούν τα συστατικά στοιχεία (υποσυστήματα) του συστήματος τεχνητής νοημοσύνης, προκύπτει ένα ιδιαίτερο όφελος για επίδοξους επιτιθέμενους να αποκτήσουν πρόσβαση σε αυτούς τους τύπους πληροφοριών και να προξενήσουν φαινόμενα διαρροής του περιεχομένου του.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στα πλαίσια της παρούσας εργασίας, αναφερθήκαμε εκτενώς σε ζητήματα ασφάλειας και ιδιωτικότητας που ανακύπτουν σε περιβάλλοντα έξυπνων μεταφορών (ITS). Σε πρώτη φάση (Κεφάλαιο 2) επικεντρωθήκαμε στα αδόμητα ασύρματα δίκτυα οχημάτων (VANETs). Έτσι προβήκαμε σε μια υψηλού επιπέδου περιγραφή του βασικού μοντέλου αρχιτεκτονικής τους αναγνωρίζοντας τα δομικά στοιχεία που συνθέτουν το δίκτυο (AU, OBU, RSU, TPM). Δεδομένου ότι τα VANETs διαθέτουν εξαιρετικά ισχυρές δυνατότητες επεξεργασίας, δύνανται να παρέχουν στους χρήστες τους ένα ευρύ φάσμα υπηρεσιών διασυνδεσιμότητας και εφαρμογών. Οι υπηρεσίες διασυνδεσιμότητας καθιστούν δυνατή την ανταλλαγή πληροφοριών εντός του δικτύου σε τρείς (3) άξονες: ανάμεσα στα οχήματα (V2V), μεταξύ των οχημάτων και της περιβάλλουσας υποδομής του οδικού δικτύου (V2I) καθώς και μεταξύ των οχημάτων και των διερχόμενων πεζών (V2P). Οι εφαρμογές που χρησιμοποιούνται στα οχηματικά περιβάλλοντα επεξεργάζονται δεδομένα που συλλέγονται από τους αισθητήρες των οχημάτων και των περιβάλλουσων υποδομών αποσκοπώντας στη βελτίωση της λειτουργίας των οχημάτων, την ενίσχυση του αισθήματος ασφάλειας και άνεσης των οδηγών καθώς και στον εξορθολογισμό της χρήσης δημόσιων υποδομών από το επιβατικό κοινό. Προκειμένου να διασφαλιστεί ότι οι εν λόγω εφαρμογές προσφέρουν ένα επαρκές επίπεδο ασφάλειας στους χρήστες τους είναι απαραίτητο να πληρούν τις απαιτούμενες QoS απαιτήσεις (εμβέλεια, ραδιοκυματική συχνότητα, αποδεκτή χρονική καθυστέρηση). Στο Κεφάλαιο 3 της εργασίας μας εξετάσαμε και παραθέσαμε το σύνολο των χαρακτηριστικών προτύπων που σχετίζονται με τα VANETs. Συγκεκριμένα εξετάσαμε την οικογένεια προτύπων IEEE 802.11p και (IEEE Standards Association, 2016), καθώς και το πρότυπο (ETSI TS 102 636-3 V1.1.1, 2010)) που προδιαγράφουν τα τεχνικά χαρακτηριστικά των τριών τύπων τομέων επικοινωνίας (ccommunication domains) που αναφέραμε ότι λαμβάνουν χώρα εντός ενός VANET.

Στο Κεφάλαιο 4 υπεισήλθαμε στον ‘πυρήνα’ της εργασίας μας. Αφού κατονομάσαμε τις εμπλεκόμενες με το ITS οντότητες και περιγράψαμε τους διαφορετικούς τύπους των επιτιθέμενων, προσδιορίσαμε το σύνολο των απαιτήσεων ασφάλειας και ιδιωτικότητας που σχετίζονται με το έξυπνο σύστημα μεταφορών (π.χ. εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, μη-αποποίηση, ιδιωτικότητα, ιχνηλασιμότητα, ανθεκτικότητα). Στη συνέχεια διαπιστώσαμε ότι, εξαιτίας του γεγονότος ότι τα ITS είναι “ανοικτά” περιβάλλοντα, καθίστανται ευάλωτα σε ένα σύνολο διαφορετικών απειλών που εκδηλώνονται υπό τη μορφή επιθέσεων και πλήττουν καθεμιά από τις απαιτήσεις αυτές (π.χ. επιθέσεις τύπου DoS, Sybil, flooding, GNSS spoofing κτλ). Έτσι, αναφέραμε ενδεικτικούς μηχανισμούς ασφαλείας για την αντιμετώπιση καθεμιάς από αυτές τις απειλές. Ωστόσο, όπως είναι φυσικό, επειδή απόλυτη ασφάλεια δεν υφίσταται, τα αντίμετρα που προτείναμε απλώς μετριάζουν τις επιπτώσεις ή εμποδίζουν την εμφάνιση των ανακυπτόντων κινδύνων ασφάλειας. Όσον αφορά τους κινδύνους ιδιωτικότητας που πλήττουν τα ITS περιβάλλοντα προβήκαμε

σε ενδελεχή ανάλυση και αξιολόγηση ποικίλλων συστημάτων προστασίας της ιδιωτικότητας που έχουν προταθεί στη διεθνή βιβλιογραφία. Τα συστήματα αυτά κατηγοριοποιούνται ως εξής: (i) συστήματα ιδιωτικότητας που χρησιμοποιούν ομαδικές ψηφιακές υπογραφές, (ii) συστήματα ιδιωτικότητας που χρησιμοποιούν ψευδώνυμα και (iii) υβριδικά σχήματα ιδιωτικότητας. Η αξιολόγησή μας βασίστηκε στα ακόλουθα κριτήρια: (i) επεκτασιμότητα, (ii) παρεχόμενο επίπεδο ιδιωτικότητας, (iii) υπολογιστικό κόστος, (iv) χρονική καθυστέρηση και (v) συνολική επιβάρυνση (κόστη) από τις διαδικασίες επικοινωνίας. Από την αξιολόγησή μας καταλήξαμε στο συμπέρασμα ότι ενώ ορισμένες από τις προσεγγίσεις παρέχουν ένα καλό επίπεδο ασφάλειας και προστασίας της ιδιωτικότητας εντούτοις δεν προσφέρουν επεκτασιμότητα και επιπλέον χαρακτηρίζονται από υψηλό υπολογιστικό κόστος, ενώ όσες προσεγγίσεις υπερτερούν στα δύο τελευταία κριτήρια δεν προσφέρουν επαρκές επίπεδο ασφάλειας.

Τέλος, στο Κεφάλαιο 5, παραθέσαμε μια μελέτη περίπτωσης που αφορά τα διασυνδεδεμένα οχήματα πλήρους αυτοματοποιημένης οδήγησης. Ειδικότερα, περιγράψαμε τα δομικά στοιχεία ενός αυτόνομου οχήματος κάνοντας ιδιαίτερη μνεία στα χαρακτηριστικά των διαφορετικών τύπων αισθητήρων που χρησιμοποιούνται από τα οχήματα για την επιτυχή εκτέλεση των λειτουργιών τους. Κατόπιν αναδείξαμε τον κυρίαρχο ρόλο που πρόκειται να διαδραματίσει η επιστήμη της τεχνητής νοημοσύνης στο χώρο της αυτοματοποιημένης οδήγησης. Στο πλαίσιο αυτό, επισημάναμε τις κυριότερες λειτουργίες και τα υποσυστήματα ενός αυτοματοποιημένου οχήματος που στηρίζουν τη λειτουργία τους σε τεχνικές μηχανικής μάθησης παρέχοντας στους χρήστες τους βελτιωμένη οδηγική εμπειρία και ενίσχυση της ασφάλειάς τους. Ωστόσο, παρά τις φιλότιμες προσπάθειες των εμπλεκομένων, η εναρμόνιση της τεχνητής νοημοσύνης με τον χώρο των αυτοκινητοβιομηχανιών βρίσκεται ακόμα σε πρώιμο στάδιο. Αυτό έχει ως αποτέλεσμα τα AI-συστήματα των αυτοματοποιημένων οχημάτων να βρίσκονται στο επίκεντρο κακόβουλων χρηστών με ποικίλες περιπτώσεις φυσικών και άλλων τύπων επιθέσεων να έχουν αναφερθεί το τελευταίο διάστημα. Κλείνοντας, επιχειρήσαμε να αποτιμήσουμε την ιδιωτικότητα σε περιβάλλοντα διασυνδεδεμένων οχημάτων. Για το σκοπό αυτό, αφού αναφερθήκαμε σε πρωτοβουλίες που λήφθηκαν για την προστασία των δεδομένων σε ευρωπαϊκό και σε εθνικό επίπεδο, εξετάσαμε το υφιστάμενο κανονιστικό και ρυθμιστικό πλαίσιο που διέπει τη λειτουργία των οχηματικών περιβαλλόντων (ΓΚΠΔ, Κοινοτική οδηγία 'e-Privacy', γνωμοδοτήσεις της Ομάδας Εργασίας του Άρθρου 29- νυν Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων). Από τη μελέτη του νομοθετικού πλαισίου προέκυψε ότι υπάρχουν ποικίλοι κίνδυνοι (τους οποίους αναλύουμε διεξοδικά στην ενότητα 5.3.3) που πλήττουν την ιδιωτικότητα των χρηστών στα περιβάλλοντα αυτά οι οποίοι θα πρέπει να αντιμετωπιστούν με την χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων (π.χ. ανωνυμοποίηση, ψευδωνυμοποίηση, κρυπτογράφηση) -τα οποία αναφέρουμε αναλυτικά στην ενότητα 5.3.4- προκειμένου να διασφαλιστεί η προστασία της ιδιωτικότητας εξ ορισμού και από το σχεδιασμό όπως επιτάσσει ο ΓΚΠΔ στο άρθρο 25 και στην Αιτιολογική Σκέψη 78 (Regulation (EU) 2016/679, 2018).

7. ΒΙΒΛΙΟΓΡΑΦΙΑ

Ali, Q., Ahmad, N., Malik, A., Ali, G., & Rehman, W. (2018, October 17). Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy. *Applied Sciences, 8*(10), 1964.

Arbib, J., & Seba, T. (2017, May). *Rethinking Transportation 2020-2030 – The disruption of Transportation and the Collapse of the Internal-Combustion Vehicle and Oil Industries.* Ανάκτηση July 2021, από RethinkX: https://static1.squarespace.com/static/585c3439be65942f022bbf9b/t/591a2e4be6f2e1c13df930c5/1494888038959/Rethink%20X+Report_051517.pdf

Article 29 Data Protection Working Party. (2014, April 10). *Opinion 05/2014 on Anonymisation Techniques.* Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Data Protection Working Party. (2014, September 16). *Opinion 8/2014 on the Recent Developments on the Internet of Things.* Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Article 29 Data Protection Working Party. (2017, October 4). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679.* Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/newsroom/article29/items/611236

Article 29 Data Protection Working Party. (2017, October 4). *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).* Ανάκτηση July 2021, από European Commission: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888

Article 29 Data Protection Working Party. (2018, April 11). *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)* . Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/newsroom/article29/items/622227

Article 29 Working Party. (2006, September 26). *Working document on data protection and privacy implications in eCall initiative.* Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf

Azees, M., Vijayakumar, P., Jeatha, D., Marimuthu, K., & Subaja-Christo, M. (2021, February 18). BBAAS: Blockchain-Based Anonymous Authentication Scheme for Providing Secure Communication in VANETs. *Security and Communication Networks*, 11.

Bar Hillel, A., Lerner, R., Levi, D., & Raz, G. (2014). Recent progress in road and lane detection: a survey. *Machine Vision and Applications, 25*(3), 727-745.

Bhavesh, N., Maity, S., & Hansdah, R. (2013). A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs. *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (σσ. 462-469). Barcelona: IEEE.

Brandeis, L., & Warren, S. (1890, December 15). *The Right to privacy.* Ανάκτηση Ιούλιος 2021, από Harvard lab Review: https://archive.org/details/jstor-1321160/page/n1/mode/2up

Calandriello, G., Papadimitratos, P., Hubaux, J., & Lioy, A. (2007). Efficient and robust pseudonymous authentication in VANET. *4th ACM International Workshop on Vehicular ad hoc Networks*, (σσ. 19-28). Montreal.

Camenisch, J., Lehmann, A., Neven, G., & Rial, A. (2014). Privacy- Preserving Auditing for Attribute-Based Credentials. *European Symposium on Research in Computer Security (ESORICS)*, (σσ. 109-127).

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011, August). Smart Cities in Europe. *Journal of Urban Technology, 18*(2), 65-82.

Carianha, A., Barreto, L., & Lima, G. (2011). Improving location privacy in mix-zones for VANETs. *IEEE 30th International Performance Computing and Communications Conference (IPCCC)* (σσ. 1-6). Orlando, FL: IEEE.

Chaum, D., & Van Heyst, E. (1991). Group Signatures. *LNCS*(547), 257-265.

Cheng, H., Shan, H., & Zhuang, W. (2011). Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mechanical Systems and Signal Processing*, 2020-2038.

Chernikova, A., Oprea, A., Nita-Rotaru, C., & Kim, B. (2019, April 15). *Are Self-Driving Cars Secure? Evasion Attacks Against Deep Neural Networks for Steering Angle Prediction.* Ανάκτηση July 2021, από arXiv: https://arxiv.org/pdf/1904.07370v1.pdf

Chim, T., Yiu, S., Hui, L., & Li, V. (2009). Security and privacy issues for inter-vehicle communications in VANETs. *6th Annual IEEE Communications Society Conference on Sensor, Mesh and ad hoc Communications and Networks Workshops (SECON Workshops' 09*, (σσ. 1-3). Rome.

CNIL. (2017, October). *Connected Vehicles and personal Data.* Ανάκτηση July 2021, από CNIL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

Department for Transport, Centre for the Protection of National Infrastructure, and Centre for Connected and Autonomous Vehicles. (2017, August 6). *Principles of cyber security for connected and automated vehicles.* Ανάκτηση July 2021, από GOV.UK: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

Differential Privacy Team, Apple. (χ.χ.). *Learning with Privacy at Scale*. Ανάκτηση από Apple Inc.: https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf

Directive (EU) 2016/680. (2018, May 6). *The Data Protection Law Enforcement Directive.* Ανάκτηση July 2021, από European Commission: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&rid=1

Drozhzhin, A. (2015, August 6). *Black Hat USA 2015: The full story of how that Jeep was hacked.* Ανάκτηση July 2021, από Kaspersky daily: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

Edmonds, E. (2021, February 25). *AAA: Today's Vehicle Technology Must Walk So Self-Driving Cars Can Run*. Ανάκτηση Ιούλιος 2021, από AAA Newsroom: https://newsroom.aaa.com/2021/02/aaa-todays-vehicle-technology-must-walk-so-self-driving-cars-can-run/

EDPB. (2019, March 12). *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.* Ανάκτηση July 2021, από EDPB: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

EDPB. (2019, October 16). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects.* Ανάκτηση July 2021, από EDPB: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en

EDPB. (2020, May 4). *Guidelines 05/2020 on consent under Regulation 2016/679 (v1.1).* Ανάκτηση July 2021, από EDPB: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EDPB. (2020, December 15). *Guidelines 10/2020 on restrictions under Article 23 GDPR.* Ανάκτηση July 2021, από EDPB: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202010_article23_en.pdf

EDPB. (2021, March 9). *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications.* Ανάκτηση July 2021, από EDPB: https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

ENISA. (2017, January 13). *Cyber Security and Resilience of smart cars.* Ανάκτηση July 2021, από European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/

ENISA. (2019, November 25). *Good practices for security of Smart Cars.* Ανάκτηση July 2021, από European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/smart-cars

ENISA. (2021, February 11). *Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving.* Ανάκτηση July 2021, από European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving

ENISA. (2021, January 28). *Data Pseudonymisation: Advanced Techniques and Use Cases* . Ανάκτηση από European Union Agency for Cybersecurity: https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

ETSI TS 102 636-3 V1.1.1. (2010, 3). *ntelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architecture*. Ανάκτηση από ITS: https://www.etsi.org/deliver/etsi_ts/102600_102699/10263603/01.01.01_60/ts_10263603v010101p.pdf

European Commision. (2017, January). *Autonomous cars.* Ανάκτηση July 2021, από Autonomous cars: a big opportunity for European industry: https://ati.ec.europa.eu/reports/technology-watch/autonomous-cars

European Commision. (2018, May 17). *n the road to automated mobility: An EU strategy for mobility of the future.* Ανάκτηση July 2021, από Mobility and Transport: https://ec.europa.eu/transport/sites/default/files/3rd-mobility-pack/com20180283_en.pdf

Finn, R., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. Στο S. Gutwirth, R. Leenes, P. De Hert, & Y. Poullet, *European Data Protection: Coming of Age* (σσ. 3-32). Springer.

Global Privacy Assembly. (2017, September 25-29). *Resolution on Data Protection in Automated and Connected Vehicles*. Ανάκτηση July 2021, από 39th International Conference of Data Protection and Privacy Commissioners: https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

Greenberg, A. (2017, 07 13). *Uber's New Tool Lets Its Staff Know Less About You*. Ανάκτηση από Wired: https://www.wired.com/story/uber-privacy-elastic-sensitivity/

Grustniy, L. (2019, March 18). *Hacking smart car alarm systems.* Ανάκτηση July 2021, από Kaspersky daily: https://www.kaspersky.com/blog/hacking-smart-car-alarm-systems/26014/

Hamida, E., Noura, H., & Znaidi, W. (2015, July 6). Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics, 4*(3), 380-423.

Hao, Y., Cheng, Y., Zhou, C., & Song, W. (2011). A distributed key management framework with cooperative message authentication in VANETs. *IEEE Journal on Selected Areas in Communications*(29), 616-629.

Horng, S., Tzeng, S., Pan, Y., Fan, P., Wang , X., Li, T., & Khan, M. (2013). b-specs+: Batch verification for secure pseudonymous authentication in VANET. *IEEE Transactions on Information Forensics and Security*(8), 1860-1875.

Huang, J., Yeh, L., & Chien, H. (2011). Abaka: An anonymous batch authenticatedand key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technologies*(60), 248-262.

IBM. (2017). *Smarter Cities.* Ανάκτηση από New cognitive approaches to long-standing challenges: https://www.ibm.com/smarterplanet/us/en/smarter_cities/solutions/infrastructure_solutions

IEEE Standards Association. (2016, March 3). *IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages*. Ανάκτηση από IEEE : https://standards.ieee.org/standard/1609_2-2016.html

IEEE Standards Association. (2016, March 21). *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation*. Ανάκτηση από https://standards.ieee.org/standard/1609_4-2016.html

Jahanian, M., Amin, F., & Jahangir, A. (2015). Analysis of TESLA protocol in vehicular ad hoc networks using timed colored petri nets. *IEEE 6th International Conference on Information and Communication Systems (ICICS)*, (σσ. 222-227). Amman.

Karagiannis, G., Altintas, O., Ekici, E., Hejjenk, G., Jarupan, B., Lin, K., & Weil, T. (2011). A Survey on Tutorial on Requirements, Architectures, Challenges, Standards and Solutions. *IEEE Communications Surveys and Tutorials*(13), 584-616.

Kargl, F., Friedman, A., & Boreli, R. (2013). Differential Privacy in Intelligent Transportation Systems . *6th ACM Conference on Security and Privacy in Wireless and Mobile Networks(WiSec 2013)* (σσ. 107-112). Budapest, Hungary: ACM.

Lin, X., & Li, X. (2013). chieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technologies*(62), 3339-3348.

Manvi, S., Kakkasageri, M., & Adiga, D. (2009). Message authentication in vehicular ad hoc networks: ECDSA based approach. *2009 IEEE International Conference on Future Computer and Communication (ICFCC 2009)*, (σσ. 16-20). Kuala Lumpur, Malaysia.

McGill University. (1997, August 26). *Bit Commitment Protocol Over a Noisy Channel.* Ανάκτηση Ιούλιος 2021, από McGill University: https://www.cs.mcgill.ca/~crepeau/CRYPTO/BCDemo/BCprotocol.html

Menouar, H., Filali, F., & Abu-Dayya, A. (2013). Experimental evaluation of 5.9 GHz link asymmetry using standards-compliant implementation. *21st IEEE International Conference on Network Protocols (ICNP)*, (σσ. 1-6). Goettingen.

Morgulis, N., Kreines, A., Mendelowitz, S., & Weisglass, Y. (2019, June 30). *Fooling a Real Car with Adversarial Traffic Signs.* Ανάκτηση July 2021, από arXiv: https://arxiv.org/abs/1907.00374

My Car My Data. (2016). *What European think about connected cars.* Ανάκτηση July 2021, από Federation Internationale de l' automobile (FIA): https://mycarmydata.eu/docs/FIA_survey_2016.pdf

Nassi, D., Ben-Netanel, R., Elovici, Y., & Nassi, B. (2019, June 24). *MobilBye: Attacking ADAS with Camera Spoofing.* Ανάκτηση July 2021, από arXiv: https://arxiv.org/abs/1906.09765

Newman, L. H. (2019, May 09). *Google Wants to Help Tech Companies Know Less About You*. Ανάκτηση July 2021, από Wired: https://www.wired.com/story/google-differential-privacy-open-source/

Petit, J., Stottelaar, B., & Feiri, M. (2015). *Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.* Ανάκτηση July 2021, από Semantic Scholar: https://www.semanticscholar.org/paper/Remote-Attacks-on-Automated-Vehicles-Sensors-%3A-on-Petit-Stottelaar/e06fef73f5bad0489bb033f490d41a046f61878a?p2df

Povolny, S., & Trivedy, S. (2020, February 19). *Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles.* Ανάκτηση July 2021, από McAfee: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/

PrivazyPlan. (2018). *Recital 78, EU GDPR*. (N. Vollmer, Παραγωγός, & SecureDataService) Ανάκτηση July 2021, από Privazyplan: https://gdpr-text.com/el/read/recital-78/

PrivazyPlan. (2021, July 2). *Recital 26 EU GDPR.* Ανάκτηση July 2021, από PrivazyPlan: https://www.privacy-regulation.eu/en/recital-26-GDPR.htm

PrivazyPlan. (2021, July 2). *Recital 58 EU GDPR.* Ανάκτηση July 2021, από PrivazyPlan: https://www.privacy-regulation.eu/en/recital-58-GDPR.htm

Qiu, F., Wu, F., & Chen, G. (2015, June). Privacy and Quality Preserving Multimedia Data Aggregation for Participatory Sensing Systems. *IEEE Transactions on Mobile Computing, 14*(6), 1287-1300.

Raya, M., & Hubaux, J. (2007). Securing vehicular ad hoc networks. *Computer Security*, 39-68.

Regulation (EU) 2016/679. (2018, May 25). *The General Data Protection Regulation (GDPR).* Ανάκτηση July 2021, από European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Rezgui, J., Cherkaoui, S., & Chakroun , O. (2011). Deterministic access for DSRC/802.11p vehicular safety communication. *7th International Wireless Communications and Mobile Computing Conference (IWCMC)*, (σσ. 595-600). Istanbul.

Rhim, W. (2012). *A Study on MAC-based Efficient Message Authentication Scheme for VANET.* Seoul: Hanyang University.

SAE Mobilus. (2021, April 30). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.* Ανάκτηση July 2021, από J3016_202104: https://www.sae.org/standards/content/j3016_202104/

Schaub, F., Kargl, F., Ma, Z., & Weber, M. (2010). V-tokens for conditional pseudonymity in VANETs. *Wireless Communications and Networking Conference (WCNC)* (σσ. 1-6). Sydney, Australia: IEEE.

Sitawarin, C., Bhagoji, A., Mosenia, A., Chiang, M., & Mittal, P. (2018, May 31). *DARTS: Deceiving Autonomous Cars with Toxic Signs.* Ανάκτηση July 2021, από arXiv.org: https://arxiv.org/abs/1802.06430.

Studer, A., Bai, F., Bellur, B., & Perrig, A. (2009). Flexible,extensible,and efficient VANET authentication. *Journal of Communications and Networks*(11), 574-588.

Tencent Keen Security Lab. (2019, March 29). *Tencent Keen Security Lab: Experimental Security Research of Tesla Autopilot.* Ανάκτηση July 2021, από Keen Security Lab blog: https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/

Tencent Security Keen Lab. (2021, May 12). *Tencent Security Keen Lab: Experimental Security Assessment of Mercedes-Benz Cars.* Ανάκτηση July 2021, από Keen Security Lab Blog: https://keenlab.tencent.com/en/2021/05/12/Tencent-Security-Keen-Lab-Experimental-Security-Assessment-on-Mercedes-Benz-Cars/

The Canadian Press. (2017, October 10). *Self-driving Ubers could still be many years away, says research head.* Ανάκτηση July 2021, από National Post: https://nationalpost.com/pmn/news-pmn/canada-news-pmn/self-driving-ubers-could-still-be-many-years-away-says-research-head?r

Towards data science. (2019, July 15). *Evasion attacks on Machine Learning (or "Adversarial Examples").* Ανάκτηση Ιούλιος 2021, από towards data science: https://towardsdatascience.com/evasion-attacks-on-machine-learning-or-adversarial-examples-12f2283e06a1

Toyama, T., Yoshida, T., Oguma, H., & Matsumoto, T. (2018, December 3-6). *PASTA: Portable Security Testbed with Adaptability.* Ανάκτηση July 2021, από Black Hat: Europe 2018: https://pdfs.semanticscholar.org/2147/c30d34b4f1598bc35a34c02b6c4521983e6a.pdf

UN General Assembly. (1948, December 10). *OHCHR.* Ανάκτηση από The Universal Declaration of Human Rights (UDHR): https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=grk

Wagan, A., Mughal, B., & Hasbullah, H. (2010). VANET security framework for trusted grouping using TPM hardware. *IEEE Second International Conference on Communication Software and Networks (ICCSN'10)*, (σσ. 309-312). Singapore.

Wang, M., Liu, D., Zhu, L., Xu, Y., & Wang, F. (2016). LESPP: Lightweight and Efficient Strong Privacy Preserving authentication scheme for secure VANET communication. *Computing*(98), 685-708.

Wiedersheim, Z., Ma, Z., Kargl, F., & Papadimitratos, P. (2010). Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough. *Wireless On-demand Network Systems and Services (WONS)* (σσ. 176-183). IEEE.

World Economic Forum. (2015, November 24). *Self-Driving Vehicles in Urban Context.* Ανάκτηση July 2021, από weforum: http://www3.weforum.org/docs/WEF_Press%20release.pdf

Yigitoglu, E., Damiani, M., Abul, O., & Silvestri, C. (2012). Privacy Preserving Sharing of Sensitive Semantic Locations under road-network constraints. *13th International Conference on Mobile Data Management* (σσ. 186-195). Bengaluru: IEEE.

Zeng, K., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., . . . Yang, Y. (2018). *All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems.* Ανάκτηση July 2021, από Semantics Scholar: https://www.semanticscholar.org/paper/All-Your-GPS-Are-Belong-To-Us%3A-Towards-Stealthy-of-Zeng-Liu/840b98aee781aff66c82eafc560c109a35cbc589

Zhang, C., Lin, X., Lu, R., Ho, P., & Shen , X. (2008). An efficient message authentication scheme for vehicular communications. *IEEE Transactions on Vehicular Technologies*(57), 3357-3368.

Zhang, L., Wu, Q., Solanas, A., & Domingo-Ferrer, J. (2010). A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions On Vehicular Technology, 59*(4), 1606-1617.

Zhu, X., Jiang, S., Wang, L., & Li, H. (2014). Efficient Privacy-preserving authentication for vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*(63), 907-919.

ΠΑΡΑΡΤΗΜΑ

Α.ΠΙΝΑΚΑΣ ΑΡΚΤΙΚΟΛΕΞΩΝ

AAA	American Automobile Association
ACC	Adaptive Cruise Control
ADAS	Advanced Driver-Assistance Systems
AI	Artificial Intelligence
ALKS	Automated Lane Keeping System
AU	Application Unit
C-ITS	Cooperative Intelligent Transport Systems
CA	Certification Authority
CCAV	Center for Connected and Autonomous Vehicles
CMAP	Cooperative Message Authentication Protocol
CMAX	Cryptographic Mix Zone Protocol
CNIL	(French) National Commission on Informatics and Liberty
CRL	Certificate Revocation List
DARTS	Deceiving Autonomous caRs with Toxic Signs
DCF	Distributed Coordination Function
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPIA	Data Protection Impact Assessment
DSRC	Dedicated Short Range Communication
ECC	Elliptic-Curve Cryptography
ECDSA	Elliptic-Curve Digital Signature Algorithm
ECU	Electronic Control Unit
EDCA	Enhanced Distributed Channel Access
EDPB	European Data Protection Board
EMAP	Expedite Message Authentication Protocol
ETSI	European Telecommunications Standards Institute
FHHS	Frequency Hopping Spread Spectrum
GDPR	General Data Protection Unit
GKM	Group Key Manager
GNSS	Global Navigation Satellite System
GPS	Global Positioning System

ICT	Information and Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IoV	Internet of Vehicles
IPv6	Internet Protocol version 6
ITS	Intelligent Transport Systems
IWGDPT	International Working Group on Data Protection in Communications
KMC	Key Management Center
LiDAR	Light Detection And Ranging
LTE	Long Term Evolution
MAC	Message Authentication Code
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OTA (update)	Over The Air (update)
PASTA	Portable Automotive Security Testbed with Adaptability
PKI	Public Key Infrastructure
QoS	Quality of Service
RSP	Remote Service Provider
RSU	Road-Side Unit
SNR	Signal-to-Noise Ratio
SPOF	Single Point of Failure
TA	Trust Authority
TCP	Transmission Control Protocol
TESLA	Time-Efficient Stream Authentication
TPD	Tamper-Proof Device
TPM	Trusted Platform Module
TTP	Trusted Third Party
UDP	User Datagram Protocol
V2I	Vehicle-To-Infrastructure
V2P	Vehicle-To-Pedestrian
V2V	Vehicle-To-Vehicle
V2X	Vehicle-To-Everything
VANET	Vehicular Ad-hoc NETworks
VPKI	Vehicular Public Key Infrastructure

WAVE	Wireless Access in Vehicular Environment
WSN	Wireless Sensor Networks

Β. ΠΙΝΑΚΑΣ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΑΓΓΛΙΚΩΝ ΟΡΩΝ ΣΤΗΝ ΕΛΛΗΝΙΚΗ

AAA	Αμερικανική Ένωση Αυτοκινήτου
ACC	Σύστημα αυτόματου πιλότου
ADAS	Προηγμένο Σύστημα Υποβοήθησης Οδήγησης
AI	Τεχνητή νοημοσύνη
ALKS	Σύστημα υποβοήθησης διατήρησης λωρίδας
AU	Μονάδα εφαρμογής
C-ITS	Συνεργαζόμενα Έξυπνα Συστήματα Μεταφορών
CA	Αρχή Έκδοσης Πιστοποιητικών
CCAV	Βρετανικός φορέας για τα διασυνδεδεμένα και αυτόνομα οχήματα
CMAP	Συνεργατικό πρωτόκολλο αυθεντικοποίησης μηνυμάτων
CMAX	Κρυπτογραφικό πρωτόκολλο μικτών ζωνών
CNIL	Γαλλική αρχή προστασίας προσωπικών δεδομένων
CRL	Λίστα ανάκλησης πιστοποιητικών
DARTS	Εξαπάτηση αυτόνομων οχημάτων με χρήση πινακίδων οδικής σήμανσης
DCF	Συνάρτηση Κατανεμημένου Συντονισμού
DDoS	Κατανεμημένες επιθέσεις άρνησης υπηρεσιών
DoS	Επιθέσεις άρνησης υπηρεσιών
DPIA	Μελέτη Εκτίμησης Αντικτύπου
DSRC	Ασύρματες επικοινωνίες μικρής εμβέλειας
ECC	Κρυπτογραφία ελλειπτικών καμπυλών
ECDSA	Αλγόριθμος Ψηφιακής Υπογραφής με χρήση Ελλειπτικών καμπυλών
ECU	Ηλεκτρονική μονάδα ελέγχου οχημάτων
EDCA	Ενισχυμένη Κατανεμημένη Πρόσβαση Καναλιού

EDPB	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)
EMAP	Πρωτόκολλο αυθεντικοποίησης μηνυμάτων
ETSI	Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών προτύπων
FHHS	Διασπορά Φάσματος με Εναλλαγή Συχνοτήτων
GDPR	Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)
GKM	Διαχειρίστρια Οντότητα Ομαδικών Κρυπτογραφικών Κλειδιών
GNSS	Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης
GPS	Παγκόσμιο Σύστημα Στιγματοθέτησης
ICT	Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ)
IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών
IoT	Διαδίκτυο των Πραγμάτων
IoV	Διαδίκτυο των Οχημάτων
IPv6	Πρωτόκολλο Διαδικτύου (έκδοση 6)
ITS	Έξυπνα Συστήματα Μεταφορών
IWGDPT	Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις Τηλεπικοινωνίες
KMC	Οντότητα Διαχείρισης Κλειδιών
LiDAR	Αναγνώριση και φασματική απεικόνιση φωτός
LTE	Εξέλιξη στο Διηνεκές
MAC	Κωδικός Αυθεντικοποίησης Μηνύματος
OBU	Εποχούμενη μονάδα
OEM	Κατασκευαστές Πρωτότυπου Εξοπλισμού
OFDM	Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας
OSI	Διασύνδεση Ανοικτών Συστημάτων
OTA (update)	Ασύρματη ενημέρωση λογισμικού
PASTA	Φορητή Πλατφόρμα Ασφάλειας Οχημάτων
PKI	Υποδομή Δημόσιου Κλειδιού
QoS	Ποιότητα Υπηρεσιών
RSP	Πάροχος Απομακρυσμένων Υπηρεσιών
RSU	Μονάδα παραπλεύρως του δρόμου

SNR	Λόγος Σήματος προς Θόρυβο
SPOF	Μοναδικό Σημείο Αστοχίας
TA	Αρχή Εμπιστοσύνης
TCP	Πρωτόκολλο Ελέγχου Μετάδοσης
TESLA	Χρονικά Αποδοτικός Έλεγχος Αυθεντικότητας μεμονωμένων χαρακτήρων μηνυμάτων
TPD	Απαραβίαστη Συσκευή
TPM	Μονάδα αξιόπιστης πλατφόρμας
TTP	Έμπιστη Τρίτη Οντότητα
UDP	Πρωτόκολλο Δεδομενογράμματος Χρήστη
V2I	Επικοινωνία οχήματος-προς-υποδομή
V2P	Επικοινωνία οχήματος με πεζό
V2V	Επικοινωνία οχήματος-προς-όχημα
V2X	Επικοινωνία οχήματος με όλα (εμπεριέχει τις επικοινωνίες V2V, V2I, V2P)
VANET	Αδόμητα Ασύρματα Δίκτυα Οχημάτων
VPKI	Υποδομή Δημοσίου Κλειδιού σε Περιβάλλοντα Οχημάτων
WAVE	Ασύρματη Πρόσβαση σε Περιβάλλοντα Οχημάτων
WSN	Δίκτυα ασύρματων αισθητήρων

Γ. ΠΙΝΑΚΑΣ ΑΝΤΙΣΤΟΙΧΙΣΗΣ ΕΛΛΗΝΙΚΩΝ ΟΡΩΝ ΣΤΗΝ ΑΓΓΛΙΚΗ

Αδόμητα Ασύρματα Δίκτυα Οχημάτων	VANET
Αλγόριθμος Ψηφιακής Υπογραφής με χρήση Ελλειπτικών καμπυλών	ECDSA
Αμερικανική Ένωση Αυτοκινήτου	AAA
Αναγνώριση και φασματική απεικόνιση φωτός	LiDAR
Απαραβίαστη Συσκευή	TPD
Αρχή Έκδοσης Πιστοποιητικών	CA
Αρχή Εμπιστοσύνης	TA
Ασύρματες επικοινωνίες μικρής εμβέλειας	DSRC
Ασύρματη ενημέρωση λογισμικού	OTA (update)
Ασύρματη Πρόσβαση σε Περιβάλλοντα Οχημάτων	WAVE
Βρετανικός φορέας για τα διασυνδεδεμένα και αυτόνομα οχήματα	CCAV
Γαλλική αρχή προστασίας προσωπικών δεδομένων	CNIL
Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)	GDPR
Διαδίκτυο των Οχημάτων	IoV
Διαδίκτυο των Πραγμάτων	IoT
Διασπορά Φάσματος με Εναλλαγή Συχνοτήτων	FHHS
Διασύνδεση Ανοικτών Συστημάτων	OSI
Διαχειρίστρια Οντότητα Ομαδικών Κρυπτογραφικών Κλειδιών	GKM
Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις Τηλεπικοινωνίες	IWGDPT
Δίκτυα ασύρματων αισθητήρων	WSN
Έλεγχος πρόσβασης στο μέσο	MAC
Έμπιστη Τρίτη Οντότητα	TTP
Ενισχυμένη Κατανεμημένη Πρόσβαση Καναλιού	EDCA
Εξαπάτηση αυτόνομων οχημάτων με χρήση πινακίδων οδικής σήμανσης	DARTS
Εξέλιξη στο Διηνεκές	LTE
Έξυπνα Συστήματα Μεταφορών	ITS
Επιθέσεις άρνησης υπηρεσιών	DoS
Επικοινωνία οχήματος με όλα (εμπεριέχει τις επικοινωνίες V2V, V2I, V2P)	V2X
Επικοινωνία οχήματος με πεζό	V2P
Επικοινωνία οχήματος-προς-όχημα	V2V
Επικοινωνία οχήματος-προς-υποδομή	V2I
Εποχούμενη μονάδα	OBU

Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών προτύπων	ETSI
Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ)	EDPB
Ηλεκτρονική μονάδα ελέγχου οχημάτων	ECU
Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών	IEEE
Κατανεμημένες επιθέσεις άρνησης υπηρεσιών	DDoS
Κατασκευαστές Πρωτότυπου Εξοπλισμού	OEM
Κρυπτογραφία ελλειπτικών καμπυλών	ECC
Κρυπτογραφικό πρωτόκολλο μικτών ζωνών	CMAX
Λίστα ανάκλησης πιστοποιητικών	CRL
Λόγος Σήματος προς Θόρυβο	SNR
Μελέτη Εκτίμησης Αντικτύπου	DPIA
Μονάδα αξιόπιστης πλατφόρμας	TPM
Μονάδα εφαρμογής	AU
Μονάδα παραπλεύρως του δρόμου	RSU
Μοναδικό Σημείο Αστοχίας	SPOF
Οντότητα Διαχείρισης Κλειδιών	KMC
Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας	OFDM
Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης	GNSS
Παγκόσμιο Σύστημα Στιγματοθέτησης	GPS
Πάροχος Απομακρυσμένων Υπηρεσιών	RSP
Ποιότητα Υπηρεσιών	QoS
Προηγμένο Σύστημα Υποβοήθησης Οδήγησης	ADAS
Πρωτόκολλο αυθεντικοποίησης μηνυμάτων	EMAP
Πρωτόκολλο Δεδομενογράμματος Χρήστη	UDP
Πρωτόκολλο Διαδικτύου (έκδοση 6)	IPv6
Πρωτόκολλο Ελέγχου Μετάδοσης	TCP
Συνάρτηση Κατανεμημένου Συντονισμού	DCF
Συνεργαζόμενα Έξυπνα Συστήματα Μεταφορών	C-ITS
Συνεργατικό πρωτόκολλο αυθεντικοποίησης μηνυμάτων	CMAP
Σύστημα αυτόματου πιλότου	ACC
Σύστημα υποβοήθησης διατήρησης λωρίδας	ALKS
Τεχνητή νοημοσύνη	AI
Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ)	ICT
Υποδομή Δημόσιου Κλειδιού	PKI
Υποδομή Δημοσίου Κλειδιού σε Περιβάλλοντα Οχημάτων	VPKI

Φορητή Πλατφόρμα Ασφάλειας Οχημάτων	PASTA
Χρονικά Αποδοτικός Έλεγχος Αυθεντικότητας μεμονωμένων χαρακτήρων μηνυμάτων	TESLA