ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΔΠΜΣ Πληροφοριακά Συστήματα

UNIVERSITY OF MACEDONIA

Master Information Systems

Ασφάλεια, Επιθέσεις και Αντίμετρα στα Vehicular Area Networks

Security, Attacks and Countermeasures in Vehicular Area Networks

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ
Καθηγητής Αναστάσιος Α. Οικονομίδης
http://conta.uom.gr

Μέλη ομάδας
Κουζνός Βασίλειος (mis16047)
Κουζνός Χρήστος (mis16048)

Θεσσαλονίκη 16/05/2016

Πίνακας περιεχομένων

Περίληψη

Τα Vehicular Ad Hoc Networks (VANETs) είναι η νέα υποσχόμενη τεχνολογία που παρέχει σε οδηγούς και επιβάτες των οχημάτων πληθώρα εφαρμογών για την άμεση ενημέρωση και ασφάλεια τους εν κινήσει.

Αποτελούν μια τεχνολογία ασύρματου δικτύου για μετάδοση πληροφορίας μεταξύ οχημάτων, βασιζόμενη στα πρότυπα των Mobile Ad Hoc Networks (MANETs). Είναι κύριο κομμάτι των Intelligent Transportation Systems (ITS) (συστήματα που επιτρέπουν στους οδηγούς να χρησιμοποιούν καινοτόμες εφαρμογές στα μέσα μεταφοράς για οδική ασφάλεια και όχι μόνο).

Παρόλο που οι κατασκευαστές (vendors) προχώρησαν σε αρκετές μελέτες για την ανάπτυξη – υλοποίηση τους, ακόμα δεν έχουν φτάσει στο επιθυμητό επίπεδο όσον αφορά το θέμα της ασφαλής μετάδοσης των πληροφοριών.

Στην παρούσα εργασία γίνεται μια αναφορά σε τεχνικές προκλήσεις και θέματα ασφαλείας, ενδεχόμενους κινδύνους και πιθανές επιθέσεις που καλείται να ξεπεράσει το VANET καθώς και προτεινόμενες λύσεις και αντίμετρα για την αντιμετώπιση τους .

Abstract

The Vehicular Ad Hoc Networks (VANETs) is a promising technology which provides drivers and passengers with numerous applications for immediate notification and security while on the move.

It's a wireless technology for transmitting information between vehicles, based on Mobile Ad Hoc Networks (MANETs) standards. It is a major part of Intelligent Transportation Systems (ITS) (systems that allow drivers to use innovative applications on the means of transport for road safety and more).

Although vendors proceeded in several studies for their development and implementation, they still haven't reached the desired level on the issue of secure transmission of information.

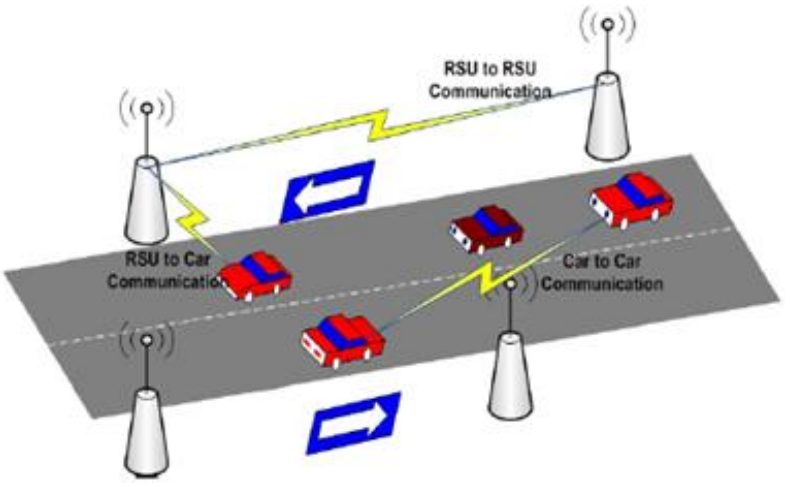
In this study there is a reference to technical challenges and security issues, potential risks and possible attacks VANETs are called to overcome, as well as proposed solutions and countermeasures to address them

Παρουσίαση θέματος/προβλήματος

Σύμφωνα με πρόσφατες πανεπιστημιακές μελέτες πάνω από 1,25 εκατομμύρια άνθρωποι χάνουν την ζωή τους και πάνω από 40 εκατομμύρια (World health organization, 2016) τραυματίζονται σε τροχαία ατυχήματα κάθε χρόνο.

Με βάση τα παραπάνω νούμερα , αλλά και σε συνδυασμό με την ραγδαία χρήση των αυτοκινήτων στην καθημερινότητα μας , την αύξηση της κίνησης στους δρόμους καθώς και την αυξανόμενη κατανάλωση καυσίμων, η διαχείριση - βελτιστοποίηση του κυκλοφοριακού συστήματος μέσω της επικοινωνίας μεταξύ των οχημάτων αποτελεί ένα βασικό αντικείμενο μελέτης. Η επικοινωνία μεταξύ οχημάτων και η ανταλλαγή πληροφοριών που κρίνονται απαραίτητες από τους εκάστοτε οδηγούς και επιβάτες μπορεί να φανεί χρήσιμη για το προγραμματισμό του ταξιδιού αλλά και για την ασφαλή οδήγηση.

Τα VANETs δημιουργούν μια ad hoc σύνδεση μεταξύ των αυτοκινήτων και κεντρικών σημείων, που επιτρέπει την άμεση διακίνηση της πληροφορίας σε ελάχιστο χρονικό διάστημα και με μεγάλα ποσοστά ακριβείας, χαρακτηριστικά που θα μελετηθούν εκτενέστερα στην συνέχεια.



Εικόνα 1. Δείγμα τοπολογίας δικτύου VANET

Η βασική προσπάθεια όλων των ενεργειών και των διαδικασιών της επικοινωνίας VANET, είναι να επιτευχθούν τέσσερις βασικοί στόχοι:

1. Η αυθεντικότητα της πληροφορίας που απεστάλει (information authenticity),
2. Η εγκυρότητα του αποστολέα και της πληροφορίας (message integrity και source authentication),
3. Η διασφάλιση της απόκρυψης της ταυτότητας του αποστολέα (privacy)
4. Η αδιάκοπη λειτουργία του συστήματος.

Κάθε επιτυχημένη επίθεση στο VANET δίκτυο μπορεί να σημαίνει απώλεια κάποιας ζωής ή οικονομική απώλεια για αυτό το λόγο η ασφάλεια των δεδομένων είναι ένα κρίσιμο κομμάτι της λειτουργίας ενός VANET δικτύου.
Σε αυτήν την εργασία θα γίνει παρακάτω αναφορά στις προκλήσεις που δέχεται ένα VANET δίκτυο, τις κύριες επιθέσεις και τις λύσεις που προτείνονται για την αποφυγή τους.

Κεφάλαιο 1

Η αρχιτεκτονική και εφαρμογή των δικτύων VANET.

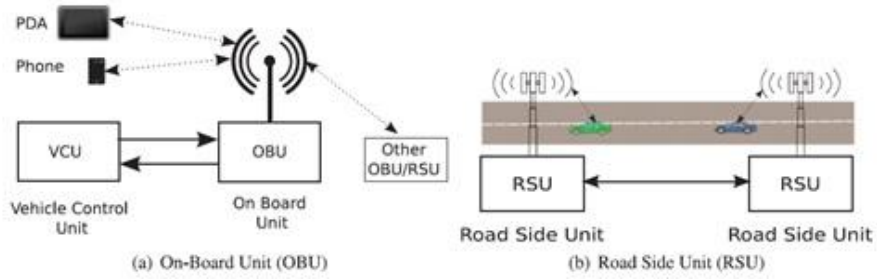
1.1 Τύποι επικοινωνίας VANET

Υπάρχουν δυο τύποι επικοινωνίας VANET.

- Ο πρώτος είναι μια ασύρματη επικοινωνία μεταξύ των οχημάτων (vehicle to vehicle) χωρίς να μεσολαβεί επιπλέον τεχνική υποδομή.
- Ο δεύτερος είναι η επικοινωνία μέσω ενός ή περισσοτέρων κεντρικών σημείων διάδοσης και μετάδοσης πληροφοριών και αντίστοιχων μέσων αποστολής, κεραίες, κατά μήκος των δρόμων, τα λεγόμενα RSU (Road Side Unit) τα οποία κατά κύριο λόγο είναι συνδεδεμένα με το internet.

1.2 Αρχιτεκτονική και τρόπος επικοινωνίας

Κάθε όχημα είναι εξοπλισμένο με δυο μονάδες, την OBU (On Board Unit) και την AU (Application Unit). Η μονάδα OBU είναι η τεχνολογική υποδομή που υλοποιεί την επικοινωνία μεταξύ των οχημάτων και εκείνη στην οποία βασίζεται η AU για να εκτελέσει τις εκάστοτε εφαρμογές, ώστε να μετατρέψει το κάθε όχημα σε επικοινωνιακό μέσο για την μετάδοση της πληροφορίας.
Στα VANET δίκτυα συνδέονται σύμφωνα με πρόσφατες μελέτες περί τα 750 εκατομμύρια οχήματα σε όλο τον κόσμο και επιτρέπουν την απευθείας επικοινωνία μεταξύ των οχημάτων (Vehicle-to-Vehicle V2V)μέσω σημάτων DSRC στην μπάντα των 5.9GHz (M.Raya, D.Jungels, P.Papadimitratos, I.Aad, JP.Hubaux, 2006) και στην απόσταση του ενός χιλιομέτρου, πέρα αυτής της απόστασης παρεμβάλλονται οι υποδομές RSU που συνήθως είναι εγκατεστημένες στους παράδρομους και επιτρέπουν την επικοινωνία του οχήματος και ενός δικτύου VANET (Vehicle –to-Infrastructure) όπως και με τα άλλα, τα πιο απομακρυσμένα. Κάθε όχημα χρησιμοποιεί την OBU συσκευή του για να συνδεθεί μέσω DSRC σήματος και RSU με τα άλλα δίκτυα αλλά διαθέτει και την TPD (Tamper Proof Device) συσκευή που έχει αποθηκευμένες πληροφορίες για το όχημα εν κινήσει, την ταχύτητα, την διαδρομή, όπως και πληροφορίες του οχήματος (πινακίδες, αριθμό πλαισίου) αλλά και πληροφορία του ίδιο του οδηγού , όπως ταυτότητα, άδεια οδήγησης.



Εικόνα 2. Μονάδα OBU και RSU

1.3 Χαρακτηριστικά γνωρίσματα ενός VANET δικτύου.

- **Αυξημένη κινητικότητα (High Mobility)** : Το οχήματα κινούνται με γρήγορες ταχύτητες ιδιαίτερα σε αυτοκινητόδρομους ταχείας διέλευσης. Αυτό το χαρακτηριστικό δυσκολεύει το σύστημα να υπολογίσει τη ακριβή θέση του οχήματος, αλλά και να διασφαλίσει στο ακέραιο την ιδιωτικότητα του, καθώς τα περισσότερα οχήματα συναντιούνται ή έρχονται κοντά μόνο για ελάχιστα δεύτερα και υπάρχει μεγάλη πιθανότητα να μην ξανασυναντηθούν μελλοντικά. Το πρόβλημα αυτό, απασχολεί τους εμπλεκόμενους χωρίς να έχει βρεθεί κάποια ουσιαστική λύση. (H.Moustafa, Zhang, 2009)

- **Συνεχής αλλαγή της τοπολογίας του δικτύου** : Η ταχύτητα του οχήματος παίζει ρόλο και σε αυτόν τον τομέα καθώς με την κίνηση του το όχημα διανύει μεγάλες αποστάσεις σε σύντομο χρονικό διάστημα και μεταπηδά από την μια τοπολογία δικτύου ad-hoc σε άλλη.
- **Δίκτυο χωρίς γεωγραφικά όρια** : Ανεξάρτητα από την ύπαρξη Ad-hoc συνδέσεων ανα ένα χιλιόμετρο όλα τα RSU επικοινωνούν μεταξύ τους και σε συνδυασμό προσφέρουν σύνδεση στο internet.
- **Συχνή ανταλλαγή πληροφοριών** : Διαρκής ανταλλαγή πληροφορίας και μεταξύ των οχημάτων και μέσω RSU με δυνατότητα αποστολής-παραλαβής μεγάλου όγκου πληροφορίας (H.Moustafa, Zhang, 2009).
- **Ο παράγοντας χρόνος** : Η πληροφορία σε ένα δίκτυο VANET πρέπει να μεταφέρεται όσο το δυνατό ταχύτερα ώστε όταν παραδοθεί στον οδηγό-επιβάτη του οχήματος να του δώσει τον απαραίτητο χρόνο να αντιδράσει ή να αποφασίσει (H.Moustafa, Zhang, 2009).
- **Σύστημα χωρίς ενεργειακούς περιορισμούς** : Τα VANET δίκτυα δεν έχουν περιορισμούς σε τροφοδοσία και κατανάλωση ενέργειας και αυτό το χαρακτηριστικό επιτρέπει την εφαρμογή πολύπλοκών εφαρμογών κρυπτογράφησης δεδομένων όπως RSA και ECDSA.

1.4 Εφαρμογές και χρήση των δικτύων VANET

Τα δίκτυα VANET βρίσκουν εφαρμογή σε εμπορικές εφαρμογές (applications) οι οποίες χωρίζονται σε δυο κύριες κατηγορίες.

1. **Εφαρμογές σχετικές με την ασφάλεια (Safety Related Applications)**
    1. Αποφυγή σύγκρουσης : Σύμφωνα με μελέτες το 60% των ατυχημάτων μπορεί να αποφευχθεί αν οι οδηγοί λάβουν ένα προειδοποιητικό μήνυμα μισό δευτερόλεπτο πριν την σύγκρουση.
    2. Υποστηρικτική οδήγηση : Οι οδηγοί μπορούν να λάβουν προειδοποιητικά μηνύματα για την ταχύτητα με την οποία προτείνεται να οδηγούν σε μια απότομη στροφή ή ακόμα και για το αν έχουν μπει στο αντίθετο ρεύμα κυκλοφορίας.
    3. Πρόβλεψη της κίνησης : Μπορεί να προβλεφθεί η κατάσταση σε ένα δρόμο με την αποστολή ενός μηνύματος προς όλους σχετικά με την κίνηση, πιθανό ατύχημα ή κάτι άλλο που θα προειδοποιήσει τους υπόλοιπους οδηγούς και εκείνοι είτε θα αλλάξουν διαδρομή ή θα επαναπρογραμματίσουν τις υποχρεώσεις και το ταξίδι τους.
2. **Εφαρμογές που αφορούν τον οδηγό – καταναλωτή (User Based Applications)**
    1. Εφαρμογές μεταξύ χρηστών : Εφαρμογές που παρέχουν τη δυνατότητα για ανταλλαγή μηνυμάτων και αρχείων-τραγουδιών, ταινιών μεταξύ των αυτοκινήτων του ίδιου ή και γειτονικού δικτύου.
    2. Σύνδεση στο διαδίκτυο : Το VANET δίκτυο παρέχει συνεχή σύνδεση στο διαδίκτυο.
    3. Υπόλοιπες υπηρεσίες : Υπηρεσίες όπως αυτόματη πληρωμή διοδίων, εντοπισμό σταθμού καυσίμων, χώρων εστίασης, ειδοποίηση για προσφορές σε γειτονικά εμπορικά καταστήματα και πολλά επιπρόσθετα.

1.5 Οικονομικές, τεχνικές και κοινωνικές προκλήσεις

Παρά το μεγάλο εύρος που μπορούν να βρουν εφαρμογή τα δίκτυα VANETs έχουν να αντιμετωπίσουν αρκετές προκλήσεις σε τεχνολογικό, κοινωνικό και οικονομικό επίπεδο, αναλυτικότερα:

Σε τεχνικό επίπεδο, η συντήρηση και συχνή αναπροσαρμογή του δικτύου είναι ένας από τους κρίσιμους παράγοντες που πρέπει οι κατασκευαστές και πάροχοι να έχουν στο μυαλό τους γιατί η εναλλαγή φόρτου του δικτύου σε διάφορες χρονικές περιόδους της μέρας αλλά και μεταξύ αραιοκατοικημένων – πυκνοκατοικημένων περιοχών, σε συνδυασμό με την αυξημένη κινητικότητα των οχημάτων και τον σύντομο χρόνο που παραμένουν σε επικοινωνία, δημιουργούν ιδιαίτερες δύσκολες συνθήκες για εύκολη αναδιάρθρωση του δικτύου. Επιπρόσθετα η εξέλιξη της χρήσης διευθύνσεων MAC των συσκευών μέσω πρωτοκόλλων IEEE 802.11 με την υιοθέτηση CSMA τεχνικών για την αποφυγή φόρτου του δικτύου είναι μια τεχνική που ακόμη εξελίσσεται. Σε κοινωνικό και οικονομικό επίπεδο είναι δύσκολο οι κατασκευαστές να δημιουργήσουν ένα σύστημα που θα διαβιβάζει το σήμα της παραβίασης σε έναν καταναλωτή που μπορεί να το απορρίψει ή να θεωρήσει ότι παρακολουθείται, για να επιτύχει αυτό πρέπει να βρεθεί ένα κίνητρο ώστε να γίνει δελεαστικό.

Κεφάλαιο 2

Η Ασφάλεια στα δίκτυα VANET

2.1 Θέματα ασφαλείας

Από όλες τις προκλήσεις η ασφάλεια του δικτύου είχε την λιγότερη προσοχή των κατασκευαστών μέχρι σήμερα. Η πληροφορία που μεταδίδεται είναι κρίσιμη για την ασφάλεια του οδηγού και των επιβατών για αυτόν τον λόγο πρέπει να υπάρχει μέριμνα για προστασία από επιθέσεις (attacks). Η αποφυγή παραποίησης των δεδομένων από attackers, η αξιοπιστία των δεδομένων που αποστέλλουν τα οχήματα για την κίνηση και την κατάσταση στους δρόμους, ο σωστός χρόνος αποστολής - λήψης της πληροφορίας, η κινητικότητα των οχημάτων, το μέγεθος του δικτύου και τέλος η γεωγραφική κάλυψη του σήματος είναι μερικοί από τους προβληματισμούς που απασχολούν τους κατασκευαστές (www.car-2-car.org, 2007).

2.2 Προκλήσεις σε θέματα ασφαλείας

Μερικές από τις προκλήσεις που καλείται να αντιμετωπίσει ένα VANET δίκτυο αφορούν την αρχιτεκτονική, τα πρωτόκολλα ασφαλείας, τους αλγόριθμους κρυπτογράφησης και πολλούς άλλους παράγοντες, παρακάτω θα δούμε αναλυτικά μερικούς (Ram Shringar Raw, Manish Kumar, Nanhay Singh, 2013).

Πραγματικός χρόνος αποστολής: Ο χρόνος είναι κρίσιμος παράγοντας για την ορθή και αποτελεσματική λειτουργία ενός VANET δικτύου επειδή ένα μήνυμα που περιέχει την πληροφορία που θα βοηθήσει τον οδηγό έχει ένα ελάχιστο περιθώριο καθυστέρησης περί τα 100ms. Αυτός είναι ο πραγματικός χρονικός περιορισμός που όμως για να επιτευχθεί χρειάζεται ένας γρήγορος αλγόριθμος κρυπτογράφησης μέσα στον οποίο θα εμπεριέχεται και ο έλεγχος της ορθότητας του περιεχομένου του (Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, 2015).

Η αξιοπιστία των δεδομένων : Ακόμη και αν ένα όχημα ή κόμβος ανήκει στο δίκτυο μπορεί να γίνει μέσο ή η αιτία για να προκληθούν προβλήματα και ατυχήματα. Ένας μηχανισμός που μπορεί να βοηθήσει ώστε να αποφευχθούν τέτοιου είδους φαινόμενα είναι ο συσχετισμός των δεδομένων που λαμβάνονται από τα διάφορα μέσα.

Μικρή ανοχή σε λάθη : Ενώ κάποια πρωτόκολλα επικοινωνίας έχουν σχεδιαστεί να δουλεύουν με βάση κάποιο ποσοστό πιθανοτήτων στο δίκτυο VANET δεν υπάρχει περιθώριο λαθους. Τα δεδομένα και η πληροφορία είναι ζωτικά κρίσιμη για τον άνθρωπο και ο παραμικρός λάθος υπολογισμός ενός αλγορίθμου μπορεί να προκαλέσει μεγάλο κίνδυνο (Ram Shringar Raw, Manish Kumar, Nanhay Singh, 2013).

Κρυπτογράφηση : Η επικοινωνία σε ένα δίκτυο VANET είναι κρυπτογραφημένη, με χρήση ίδιων ή διαφορετικών κλειδιών (ανάλογα με τον κατασκευαστή - τεχνολογία) μπορεί να γίνει η κρυπτογράφηση των δεδομένων στην αποστολή και η αποκρυπτογράφηση τους κατά την λήψη. Ένας κατασκευαστής μπορεί να σχεδιάζει δικά του κλειδιά κρυπτογράφησης ή μπορεί να χρησιμοποιεί «δημόσια κλειδιά» αρκεί και στις δυο περιπτώσεις να καλύπτουν κάποια πιστοποιητικά (CA). Η διαδικασία της ανταλλαγής κλειδιών μεταξύ των OBUs είναι μια πρόκληση από μόνη της για τους κατασκευαστές σε ότι αφορά το σχεδιασμό πρωτοκόλλων ασφαλείας (Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, 2015).

Κίνητρα για την χρήση τους : Στόχος ενός κατασκευαστή είναι να υλοποιήσει μια εφαρμογή που θα αρέσει στο χρήστη-καταναλωτή και θα την χρησιμοποιεί. Ένας χρήστης όμως παρουσιάζεται δύσπιστος όταν καλείται να υιοθετήσει στην καθημερινότητα του μια εφαρμογή που ελέγχει και ενημερώνει για την τυχόν παραβίαση κάποιου κανόνα του Κώδικα Οδικής Κυκλοφορίας (ΚΟΚ). Η πρόκληση στην συγκεκριμένη περίπτωση έγκειται στο τρόπο που θα γίνουν πιο αρεστά τέτοια συστήματα και θα πείσουν χρήστες, κατασκευαστές και την πολιτεία να τα εισάγουν στην παραγωγή και χρήση (Ram Shringar Raw, Manish Kumar, Nanhay Singh, 2013).

Η αυξημένη κινητικότητα των οχημάτων : Η υπολογιστική ισχύς αλλά και οι ενεργειακές ανάγκες ενός VANET δικτύου είναι παρόμοιες με εκείνες του ενσύρματου δικτύου αλλά η επεξεργασία και αποστολή του ίδιου μεγέθους πληροφορίας πρέπει να γίνει σε ταχύτερο χρονικό διάστημα. Για το λόγο αυτό οι κατασκευαστές προσπαθούν με τεχνικές να μειώσουν τον χρόνο εκτέλεσης των υπολογισμών, δυο από τις οποίες είναι οι κάτωθι (Verma, K., H. Hasbullah, A. Kumar, 2013).

- **Μείωση της πολυπλοκότητας των αλγορίθμων ασφαλείας**. Αρκετά πρωτόκολλα κρυπτογράφησης (SSL/TLS, DTLS) χρησιμοποιούν τεχνολογία RSA, η οποία βασίζεται σε ένα δημόσιο κλειδί κρυπτογράφησης και χρησιμοποιεί μια τεχνική αρκετά χρονοβόρα. Η εναλλαγή σε κάποιου άλλου είδους κρυπτογράφησης, όπως AES, Elliptic curve cryptosystems και lattice based cryptosystems προτείνεται για την εξάλειψη τέτοιων δυσκολιών.
- **Επιλογή πρωτοκόλλου μετάδοσης.** Για την ασφαλή μετάδοση μέσω IP, η τεχνολογία DTLS προτείνεται της TLS καθώς υποστηρίζει επικοινωνία σε επίπεδο μειωμένης έντασης σήματος. Η τεχνολογία IPSec είναι μια λύση που επίσης προτείνεται ωστόσο είναι αποδοτική σε περιπτώσεις που δεν υπάρχει υψηλή κινητικότητα των οχημάτων.

2.3 Απαιτήσεις ασφαλείας

Διαπίστευση : Διασφάλιση ότι το μήνυμα που παράγεται προέρχεται από αξιόπιστο χρήστη καθώς στο VANET το όχημα – χρήστης αντιδρούν ανάλογα με το περιεχόμενο της πληροφορίας που απεστάλει από κάποιο άλλο όχημα και για αυτό οι διαπιστεύσεις πρέπει να έχουν μια ηλεκτρονική υπογραφή πιστοποίησης που θα χρειάζεται ένα «κλειδί» για την κωδικοποίηση – αποκωδικοποίηση του μηνύματος [5].

Διαθεσιμότητα πληροφορίας : Η πληροφορία πρέπει να είναι διαθέσιμη μόνο σε όλους τους νόμιμους χρήστες του δικτύου. Καθώς μπορεί να προκληθούν DoS attacks (ένα είδος που θα αναλυθεί εκτενέστερα παρακάτω) και μπορεί να οδηγήσουν σε κατάρρευση του δικτύου και διακοπή της ροής της πληροφορίας. Με αποτέλεσμα το σύστημα να προσπαθήσει να ανακτήσει πλήρως την πληροφορία με το να παίρνει τα κομμάτια που έχουν παραληφθεί και να προσπαθεί να αναδημιουργήσει το μήνυμα. Επίσης μια απειροελάχιστη καθυστέρηση στην μετάδοση της πληροφορίας μπορεί να την καταστήσει αχρείαστη (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014).

Μη Απάρνηση αποστολής δεδομένων : Δηλαδή ένας κόμβος δεν έχει το δικαίωμα να αρνηθεί από έναν χρήστη την δυνατότητα του να μην στείλει την πληροφορία – μήνυμα. Επίσης η πληροφορία του κάθε οχήματος (διαδρομή, ταχύτητα, παραβάσεις) αποθηκεύεται στο TPD και οι αρχές έχουν το δικαίωμα με χρήση συγκεκριμένων προγραμμάτων να ανακτήσουν τυχόν πληροφορίες χρήσιμες για αυτούς ώστε να ασκήσουν τυχόν ποινικές διώξεις (Verma, K., H. Hasbullah, A. Kumar, 2013).

Ιδιωτικότητα : Η διασφάλιση της ιδιωτικότητας των πληροφοριών ενός πιστοποιημένου κόμβου σε σύγκριση με έναν άλλον άγνωστο. Το χαρακτηριστικό της ιδιωτικότητας είναι αυτό που προστατεύει το δίκτυο από επιθέσεις που προκαλούν καθυστερήσεις στην διάδοση των μηνυμάτων. Η χρήση προσωρινών «κλειδιών» που θα λήγουν μετά την χρήση τους είναι μια προτεινόμενη για την λύση (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014).

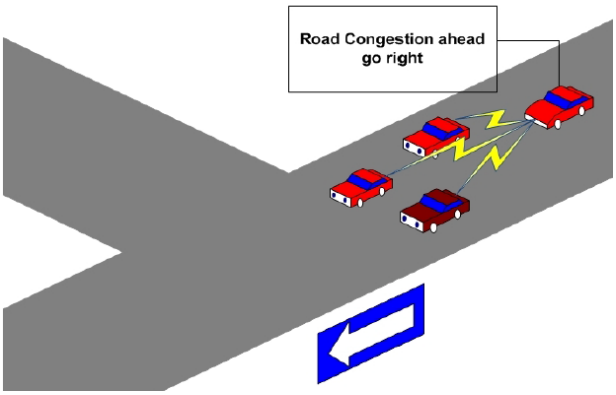
Κεφάλαιο 3

Οι επιθέσεις στα δίκτυα VANET

3.1 Τύποι επιτιθέμενων (Attackers)

Η διασφάλιση της προστασίας απέναντι σε επιθέσεις μπορεί να επιτευχθεί με τον εντοπισμό των της ταυτότητας, φύσης και του εύρους της ζημιάς που μπορεί να προκαλέσουν οι attackers. Παρακάτω περιγράφονται μερικοί τύποι.

- **Insider/Outsider** : Insiders ορίζονται ως εκείνοι που έχουν τα απαραίτητα διαπιστευτήρια και είναι μέλη ενός δικτύου, ενώ Outsiders ορίζονται ως εκείνοι που προσπαθούν να εισβάλουν και να διεισδύσουν στο δίκτυο. Χαρακτηριστικό παράδειγμα ενός insider attacker μπορεί να είναι ένας Selfish driver. Στην περίπτωση αυτή, ένας οδηγός προσπαθεί να χρησιμοποιήσει τα χαρακτηριστικά και τις δυνατότητες του δικτύου για το δικό του όφελος ανεξαρτήτως των συνεπειών που προκαλεί στο VANET δίκτυο. Όπως αναφέρθηκε και παραπάνω όλα τα οχήματα βασίζονται σε μια πολιτική εμπιστοσύνης μεταξύ των και ακολουθούν τους κανόνες των πρωτοκόλλων επικοινωνίας που επιτρέπουν τη διάδοση μηνυμάτων μεταξύ των. Επομένως, ένας οδηγός μπορεί να αποστείλει ένα μήνυμα για ένα ανύπαρκτο μποτιλιάρισμα ενός συγκεκριμένου δρόμου και να καλεί τους οδηγούς να αλλάξουν διαδρομή, με στόχο να χρησιμοποιήσει το δρόμο ελεύθερα για την δική του διευκόλυνση (Maxim Raya, 2005).



Εικόνα 3. Παραπληροφόρηση γειτονικών οχημάτων από attacker

- **Malicious/Rational** : Αποτελεί την διάκριση των attacker σε αυτούς που έχουν προσωπικό όφελος (Rational)και μη (Malicious). Στο παραπάνω παράδειγμα του *Selfish driver* μπορούμε να πούμε με σιγουριά σε πια κατηγορία ανήκει.

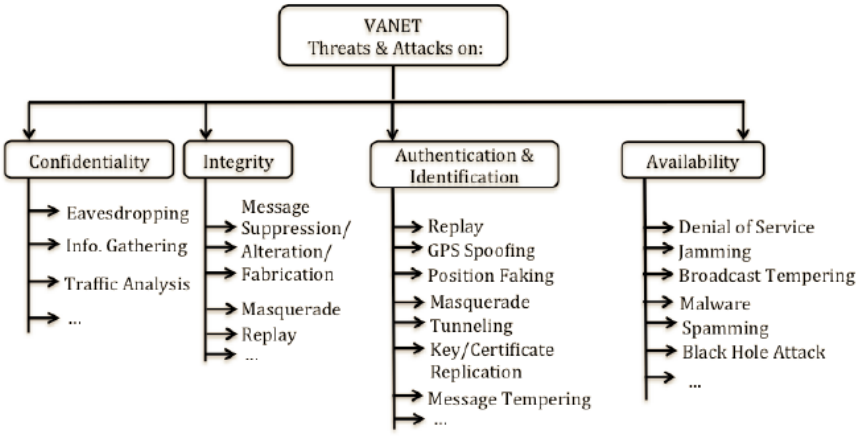
- **Active/Passive** : Οι ενεργητικοί (Active) attackers είναι εκείνοι που παράγουν παραπλανητικό σήμα μέσα στο δίκτυο. Ενώ οι παθητικοί (Passive) απλά παρατηρούν και μελετούν τα δεδομένα που κυκλοφορούν μέσα στο δίκτυο (M.Raya, D.Jungels, P.Papadimitratos, I.Aad, JP.Hubaux, 2006).

3.2 Κατηγορίες επιθέσεων

Τα VANET δίκτυα είναι εκτεθειμένα σε πολλούς κινδύνους και επιθέσεις. Από την στιγμή που ένα VANET δίκτυο είναι ενεργειακά αυτόνομο, η συσκευή OBU που είναι εφοδιασμένο δεν έχει πρόβλημα πρόβλημα με την διάρκεια της μπαταρίας όπως συμβαίνει στα κινητά τηλέφωνα και τις λοιπές έξυπνες συσκευές. Για τον

παραπάνω λόγο ένα OBU μπορεί να είναι εξοπλισμένο με όλα εκείνα τα ηλεκτρονικά κυκλώματα και επεξεργαστές για να εκτελεί πολύπλοκους και χρονοβόρους υπολογισμούς – αλγόριθμους. Ασφαλώς και αποτελεί ένα πλεονέκτημα έναντι των άλλων συσκευών, αλλά έχει και το μειονέκτημα ότι προκαλεί επιθέσεις που δεν παρατηρούνται σε απλά ad-hoc δίκτυα. Οι κατηγορίες των επιθέσεων (attacks) που ένα VANET είναι εκτεθειμένο βασίζονται κυρίως στο αντικείμενο – χαρακτηριστικό που προσπαθεί ένας attacker να εκθέσει σε κίνδυνο (Maxim Raya, 2005).

Οι κυριότερες μπορούν να είναι η ιδιωτικότητα, αξιοπιστία και η διαθεσιμότητα του δικτύου όπως και η ευθύνη μετάδοσης του σήματος και η πιστοποίηση της αυθεντικότητας του. Οι στόχοι των attackers περιγράφονται παραστατικά στο παραπάνω διάγραμμα (Mohamed Nidhal Mejri, Jalel BenOthman, Mohamed Hamdi, 2014).

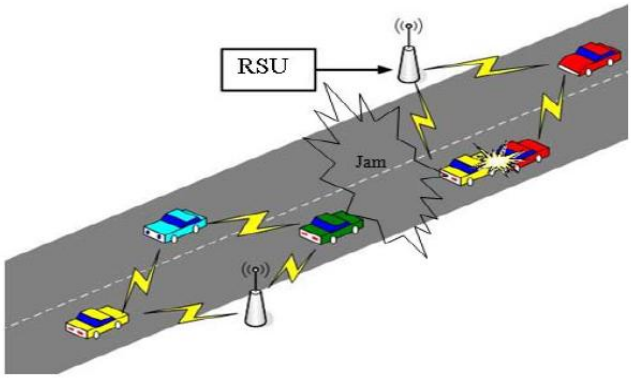


Εικόνα 4. Είδη επιθέσεων και που βρίσκουν αντίκτυπο

Οι σημαντικότεροι από τους κινδύνους – επιθέσεις μπορούν να περιγράφονται στην συνέχεια.

Denial of Service (DoS) : Αποτελούν τις πιο σύνηθες επιθέσεις και δεν επιτρέπουν το νόμιμο χρήστη να χρησιμοποιήσει τις υπηρεσίες ενός κόμβου (Mohamed Nidhal Mejri, Jalel BenOthman, Mohamed Hamdi, 2014). Αναλυτικότερα, η επίθεση αυτή συντελείται όταν οι attackers παίρνουν τον έλεγχο των πόρων ενός οχήματος ή προκαλούν ένα jam στο δίκτυο με σκοπό να μην επιτραπεί η λήψη της πληροφορίας στο όχημα, αυξάνοντας παράλληλα τον κίνδυνο για την ασφάλεια του οδηγού και επιβατών των οχημάτων που βασίζονται στα δεδομένα της εκάστοτε εφαρμογής – application που μπορεί να επηρεαστεί. Αν το attack προκαλείται από μια ομάδα attackers ονομάζεται Distributed DoS attack (Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, 2015).

Ένα παράδειγμα τέτοιας επίθεσης είναι, όταν ένας attacker θέλει να δημιουργήσει μια καραμπόλα σε έναν αυτοκινητόδρομο. Προκαλεί, με λάθος πληροφορίες στα αντίστοιχα applications, ένα ατύχημα και παράλληλα εμποδίζει την μετάδοση της προειδοποίησης στα οχήματα που ακολουθούν, έτσι προκαλείται συνωστισμός στο οδικό δίκτυο(jamming) (Mohamed Nidhal Mejri, Jalel BenOthman, Mohamed Hamdi, 2014).

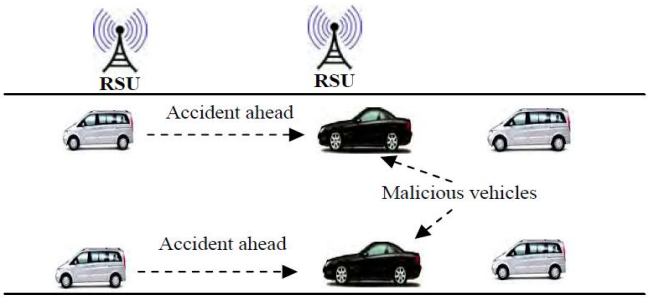


Εικόνα 5. Παράδειγμα DoS Attack

Επιπλέον, υπάρχει και ο κίνδυνος του SYN Flooding. Ένας μηχανισμός που πλήθος από αιτήματα συγχρονισμού (SYN) αποστέλλονται στον κόμβο ξεγελώντας τον με την χρήση ψεύτικης διεύθυνσης αποστολέα, έτσι ο κόμβος απαντάει με ένα SYN-ACK σε λανθασμένες διευθύνσεις του αποστολέα και περιμένει να λάβει πίσω το αντίστοιχο ACK πακέτο, αλλά μάταια. Με αποτέλεσμα να παραμένουν σε εκκρεμότητα δυο μισές συνδέσεις και ουσιαστικά τα πραγματικά αιτήματα των χρηστών να χάνονται (Verma, K., H. Hasbullah, A. Kumar, 2013).

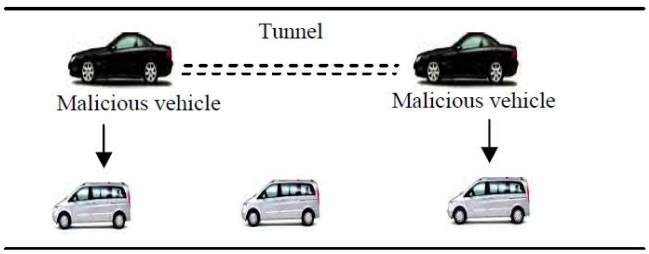
Routing attack : Επιθέσεις που εκμεταλλεύονται τα τρωτά σημεία ασφαλείας του δικτύου σε επίπεδο πρωτοκόλλου δρομολόγησης της πληροφορίας. Σε αυτές τις περιπτώσεις είτε διαγράφει τα πακέτα της πληροφορίας είτε διακόπτει την μετάδοση των δεδομένων στο δίκτυο (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014). Κατηγορίες αυτής της επίθεσης είναι :

- **Black Hole Attack**: Σε αυτήν την κατηγορία, οι attackers προσελκύουν τα nodes για να στέλνουν τις πληροφορίες τους μέσω αυτών. έτσι όταν τα δεδομένα αντί να προωθηθούν μέσω των attackers εκείνα διαγράφονται και χάνονται (Verma, K., H. Hasbullah, A. Kumar, 2013).



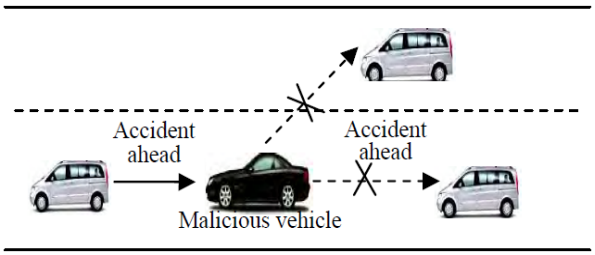
Εικόνα 6. Black Hole Attack

- **Wormhole Attack**: Σε αυτού του τύπου επίθεση, ο attacker λαμβάνει τα δεδομένα και τα ξαναρίχνει στο δίκτυο από άλλο σημείο. Αυτή η σύνδεση για επανεισαγωγή της πληροφορίας ονομάζεται wormhole. Και ο επιτιθέμενος μπορεί να στείλει μια πληροφορία πιο γρήγορα από ότι κανονικά και χωρίς να υπάρχει περιορισμός στην τοπολογία του δικτύου (ασύρματη ή ενσύρματη) (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014).



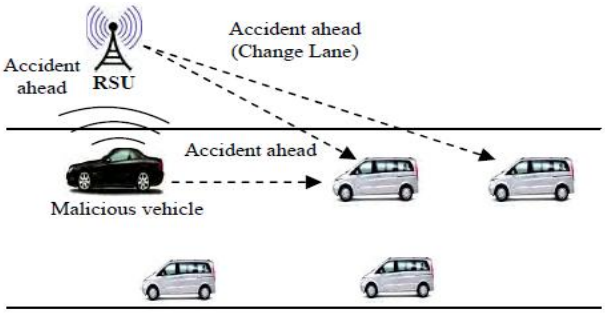
Εικόνα 7.1 Wormhole Attack

- **Sinkhole Attack**: Μια παραλλαγή του Black hole attack μόνο που στη συγκεκριμένη περίπτωση η διαγραφή της πληροφορίας είναι στοχευόμενη. Δηλαδή μπορεί να διαγραφούν πακέτα που αφορούν συγκεκριμένη πληροφορία.



Εικόνα 7.2 Sinkhole Attack

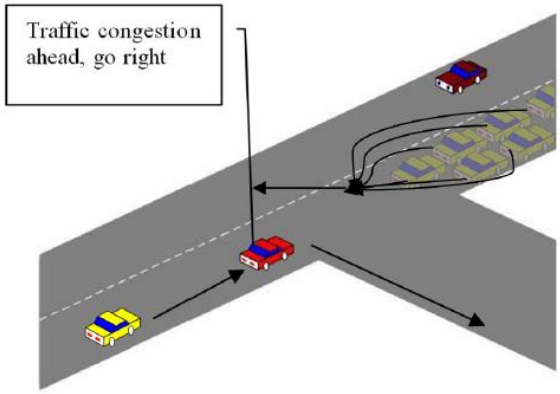
- **Illusion Attack**: Μια προσπάθεια του attacker να διαδώσει λανθασμένες πληροφορίες στα οχήματα και να αλλάξει την οδηγική του συμπεριφορά και τις αποφάσεις που πρέπει να πάρει, με αποτέλεσμα να προκαλούνται ατυχήματα και κυκλοφοριακά προβλήματα (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014).



Εικόνα 8. Illusion Attack

- **Sybil Attack** : Ο attacker δημιουργεί ένα μεγάλο αριθμό από ψεύτικα οχήματα με σκοπό να γεμίσει το VANET δίκτυο με αναληθείς πληροφορίες και να βλάψει τα νόμιμα οχήματα. Επηρεάζεται σημαντικά η απόδοση του δικτύου που καλείται να εξυπηρετήσει πολλά ανύπαρκτα οχήματα και γεμίζει το δίκτυο με ψευδή πληροφορίες και συντεταγμένες που προοδευτικά προκαλούν άλλου τύπου attacks (DoS Attack) (M.Raya, D.Jungels, P.Papadimitratos, I.Aad, JP.Hubaux, 2006).

Impersonate Attack : Σε αυτού του τύπου τις επιθέσεις ο attacker υποδύεται κάποιον ή κάποιους άλλους νόμιμους χρήστες για να κάνει χρήση δεδομένων που δεν έχει πρόσβαση είτε για να προκαλέσει προβλήματα στην λειτουργία του δικτύου. Η επίθεση αυτή μπορεί να γίνει μονό από ενεργούς insiders ή outsiders attackers και μπορεί να επηρεάσει την επικοινωνία σε διάφορα επίπεδα, όπως δικτύου, εφαρμογής ή και μετάδοσης της πληροφορίας. Μπορεί να εφαρμοστεί με δυο τρόπους, με το να υποδύεται ότι είναι κάποιος άλλος και να στέλνει μηνύματα με άλλη ταυτότητα (False attribute possession) ή με Sybil, δηλαδή να μπορεί να ξεγελάσει το σύστημα και να φαίνεται σαν πολλά οχήματα μαζί, έτσι αναφορές περί μποτιλιαρίσματος μπορεί να εμφανιστούν στους λοιπούς οδηγούς και να τους αναγκάσουν να αλλάξουν διαδρομή χωρίς να υπάρχει λόγος (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014).



Εικόνα 9. Παράδειγμα Sybil Attack

Session hijacking : Ο έλεγχος των διαπιστεύσεων για την έναρξη της μετάδοσης της πληροφορίας και σύνδεση στο δίκτυο γίνεται στην αρχή της σύνδεσης. Η επίθεση μπορεί να πραγματοποιηθεί εφόσον υλοποιηθεί η σύνδεση και οι attackers μπορούν να έχουν τον έλεγχο της σύνδεσης μεταξύ των κόμβων.

Eavesdropping : Μια ακόμη συνήθης επίθεση σε επίπεδο δικτύου και από παθητικούς attackers, που έχει ως μόνο στόχο να αποκτήσει ο attacker πρόσβαση σε προσωπικά – απόρρητα δεδομένα.

Message Suppression Attack : Ένας attacker αποκόπτει συγκεκριμένα πακέτα από το δίκτυο ή τα RSUs, πακέτα που μπορεί να περιέχουν πολύ κρίσιμη πληροφορία και τα έχει στην κατοχή του για δική του χρήση. Ένα πιθανό παράδειγμα χρήσης μπορεί να είναι έναντι των ασφαλιστικών εταιρειών ώστε να γίνει απόκρυψη της συμμετοχής του οδηγού – οχήματος σε ένα ατύχημα ή η αποκοπή ενός ειδοποιητικού μηνύματος και επαναχρησιμοποίηση του σε άλλο χρονικό διάστημα που δεν είναι απαραίτητο (Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, 2015).

Attacks on Network Layer (Routing Attacks)	Impact/Effect	Security Requirements
Denial of Service (DoS) Attack	Reduce the performance & efficiency of the network	Availability
Black Hole Attack	Cause data packets to be lost & misuse or discard the traffic	Availability
Wormhole Attack	Prevent the discovery of valid routes & cause data packets to be lost	Authentication & Confidentiality
Sinkhole Attack	Make the network complicated, either by modifying the data packets or by drooping them.	Availability
Illusion Attack	Cause car accidents, traffic jams & reduce the performance of the network in terms of bandwidth utilization	Authentication
Sybil Attack	Take over the control of whole network & inject false information in it like traffic congestion, accident etc	Authentication

Εικόνα 10. Attacks, αντίκτυπο στις επιδόσεις του δικτύου

Κεφάλαιο 4

Αντιμετώπιση των επιθέσεων στα δίκτυα VANET

4.1 Αλγόριθμοι και μηχανισμοί αντιμετώπισης επιθέσεων – Αντίμετρα

Για την ασφάλεια των VANET δικτύων έχουν προταθεί αρκετές λύσεις και έχουν γίνει αρκετές σχετικές μελέτες που έχουν ως αντικείμενο να αντιμετωπιστούν οι παραπάνω κίνδυνοι. Παρακάτω θα αναφερθούν οι προτεινόμενες λύσεις αλλά και θα παραταθεί σχετική αναφορά για το τι επιθέσεις προσπαθούν να εξαλείψουν.

4.1.1 Αντίμετρα επιθέσεων DoS Attack

Ένα σύστημα προ-πιστοποίησης (L. He, W.T. Zhu. Mitigating, 2012) είναι μια προσέγγιση πολύ αποτελεσματική και ισχυρή, διότι μπορεί να μετριάσει αποτελεσματικά τέτοιες επιθέσεις. Το σύστημα αυτό παρέχει μια διαδικασία προ-ελέγχου ταυτότητας πριν από τη διαδικασία επαλήθευσης της υπογραφής και εφόσον επιτευχθεί το πρώτο βήμα συνεχίζει στο δεύτερο διαφορετικά απορρίπτεται.

Ο αλγόριθμός APDA (Attacked Packet Detection Algorithm) (S.RoselinMary, M. Maheshwari, M. Thamaraiselvan, 2013) που εντοπίζει επιθέσεις DoS πριν από τον έλεγχο και χρησιμοποιείται για την ανίχνευση των μη έγκυρων αιτημάτων. Τα οχήματα στέλνουν μηνύματα σε RSU μέσω του μηχανισμού APDA. Αποθηκεύονται οι πληροφορίες των οχημάτων στα RSUs όπως και η θέση των οχημάτων. Αν το πακέτο δεδομένων είναι τύπου attack, παρακολουθείτε, αλλιώς όχι. Το πλεονέκτημα αυτής της προσέγγισης είναι ότι ελαχιστοποιεί την επιβάρυνση καθυστέρηση για την επεξεργασία και ενισχύει την ασφάλεια στην VANET.

Η τεχνική ADRIANE που αντιμετωπίζει τα Dos Attacks βασιζόμενη σε έλεγχο της διαδρομής με συμμετρική κρυπτογράφηση. Σε αυτή την περίπτωση ο αποστολέας και ο παραλήπτης χρησιμοποιούν δυο κλειδιά κρυπτογράφησης, ένα από την πηγή προς τον προορισμό και ένα από τον προορισμό προς την πηγή χαρακτηριζόμενα από ένα MAC αριθμό, όπου βάση των οποίων γίνεται και ο έλεγχος αυθεντικότητας (Mohan Li, 2014).

4.1.2 Αντίμετρα επιθέσεων Routing attack

4.1.2.1 Αντιμετώπιση των Black Hole attacks

Το πρωτόκολλο DPRAODV (Detection, Prevention & Reactive AODV) (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014) εντοπίζει τον attacker και τον απομονώνει εμποδίζοντας τον να προωθήσει κακόβουλα πακέτα. Μόλις εντοπιστεί ένα ALARM πακέτο αποστέλλεται στα υπόλοιπα οχήματα εμπεριέχοντας το ID του attacker και με αυτόν τον τρόπο ενημερώνονται ώστε να μην εκτελούν την μετάδοση των πακέτων πληροφορίας που προέρχονται από αυτό (S.RoselinMary, M. Maheshwari, M. Thamaraiselvan, 2013).

4.1.2.2 Αντιμετώπιση των Wormhole attacks

Η τεχνική HEAP (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014), που βασίζεται στο πρωτόκολλο AODV και πιστοποιεί τα πακέτα δεδομένων με την χρήση αλγορίθμου για κάθε hop. Ο εντοπισμός του attacker γίνεται με βάση τα γεωγραφικά κριτήρια και η πληροφορία διατηρείται για συγκεκριμένες αποστάσεις. Τα πλεονεκτήματα είναι η ασφάλεια και η μη χρήση επιπλέον εξοπλισμού.

4.1.2.3 Αντιμετώπιση των Sinkhole attacks

Το μοντέλο IDS (Intrusion Detection System) επιτρέπει τον εντοπισμό των Sinkhole attacks. Αποτελείται από IDS clients που λειτουργούν σε κάθε κόμβο του δικτύου και είναι υπεύθυνοι για την μεταξύ τους επικοινωνία. Οι λειτουργίες που εκτελεί ένας IDS client είναι η ανίχνευση εισβολέων, παρακολούθηση του δικτύου, αποφάσεις για δράσεις και αποτελείται από τεχνικά εξαρτήματα που εκτελούν τις παραπάνω δράσεις. Το μοντέλο όμως είναι πολύ δύσκολο να εφαρμοστεί σε ρεαλιστικό περιβάλλον (Al-Sakib Khan Pathan, 2013).

4.1.2.4 Αντιμετώπιση των Illusion attacks

Το μοντέλο PVN (Plausibility Validation Network) ελέγχει αν το μήνυμα που προέρχεται από τον αισθητήρα είναι έγκυρο ή όχι. Ο έλεγχος που πραγματοποιεί στο κάθε μήνυμα χωρίζεται σε 2 μέρη, αρχικά ξεχωρίζει αν προέρχεται από κεραία ή αισθητήρα και έπειτα γίνεται έλεγχος βάση μιας βάσης δεδομένων για το συμβάν. Μόνο αν περάσει και τους δυο ελέγχους θεωρείται έγκυρο, διαφορετικά διαγράφεται αυτόματα. Το μοντέλο απαιτεί τον αποτελεσματικό έλεγχο των μηνυμάτων που λαμβάνονται (S.RoselinMary, M. Maheshwari, M. Thamaraiselvan, 2013).

4.1.2.5 Αντιμετώπιση των Sybil attacks

Timestamp: Για τον εντοπισμό Sybil attack προτείνεται η προσέγγιση σήμανσης χρόνου (timestamp) (Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, 2014) βασιζόμενη στην υποστήριξη της μονάδας RSU. Σύμφωνα με αυτό το σκεπτικό είναι ελάχιστες οι φορές που δυο οχήματα περνούν ταυτόχρονα από μια συστοιχία RSUs και επομένως όταν τα μηνύματα που αποστέλλονται έχουν το ίδιο timestamp από το RSU τότε λογίζονται ως Sybil attack από ένα όχημα. Η προσέγγιση είναι απλή, αποτελεσματική και χωρίς επιπλέον κόστος καθώς δεν απαιτείται καν κρυπτογράφηση, παρόλαυτα μειονεκτεί στο ότι δεν μπορεί να καλύψει την περίπτωση που δυο οχήματα έρχονται από αντίθετες κατευθύνσεις.

4.1.3 Αντίμετρα επιθέσεων Session hijacking attack

Session timestamp: (Al-Sakib Khan Pathan, 2013) Αντίμετρο για την επίθεση Session hijacking, είναι η χρήση session σήμανσης χρόνου (session timestamp), συγκρίνοντας δηλαδή την παρούσα χρονική στιγμή που περιέχεται στο μήνυμα που λαμβάνουμε. Εφόσον η σήμανση χρόνου είναι πολύ μεγαλύτερη από την τρέχουσα ώρα, το μήνυμα κρίνεται ως ύποπτο και απορρίπτεται.

4.1.4 Αντίμετρα επιθέσεων Impersonation attack

Content Fragile Watermarking: Ως αντίμετρο για την επίθεση impersonation, είναι η δημιουργία ασφαλούς σύνδεσης με Key Factors (BUCK) Filter, που ανιχνεύει επιθέσεις πλαστοπροσωπίας μεταδίδοντας beacons και εντοπίζοντας την ακριβή θέση του οχήματος που στέλνει το μήνυμα. Μόλις ανιχνευτεί ο ελαττωματικός κόμβος ανιχνευτεί, μέσω των μηνυμάτων που περιέχουν Content Fragile Watermarking απομονώνεται από το περιβάλλον επικοινωνίας. Το προτεινόμενο σύστημα έχει αναλυθεί χρησιμοποιώντας τις μετρήσεις Beaconing Overhead, Node Load, Routing Stretch, CDF και Delay(Simranpreet Singh Chhatwal, Manmohan Sharma, 2015) .

4.1.5 Άλλα αντίμετρα επιθέσεων σε δίκτυα VANET

Secure and Efficient Ad hoc Distance Vector (SEAD) : Το πρωτόκολλο δρομολόγησης προτάθηκε [1] για να αντιμετωπιστούν οι πολλαπλές και ασυντόνιστες επιθέσεις που επηρεάζουν την λειτουργία των κόμβων. Βασιζόμενη στη Destination sequenced Distance Vector (DSDV[2]) δρομολόγηση. Το SEAD προστατεύει τον κόμβο που έχει την χαμηλότερη υπολογιστική ισχύ από άποψη υποδομής και ουσιαστικά είναι τρωτό σημείο

[1] http://www.netsec.ethz.ch/publications/papers/sead-journal.pdf

[2] DSDV : Μια τεχνική που υλοποιήθηκε το 1994 για την αποφυγή προβλημάτων επαναδρομολόγησης. Με την προσθήκη ενός μοναδικού αριθμού συχνότητας ώστε να εφαρμόζονται σωστά οι ενημερώσεις.

για κάθε attacker, όπως και από DoS attacks που έχουν σαν στόχο την υπερβολική χρήση του εύρους ζώνης του δικτύου (Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, 2015).

Secure Message Transmission (SMT) : Το πρωτόκολλο SMT εφαρμόζεται κυρίως στις άκρες του δικτύου και απαιτεί μια σχέση ασφαλείας μεταξύ της πηγής και του προορισμού, ωστόσο δεν απαιτεί εφαρμογή κρυπτογράφηση στους ενδιάμεσους κόμβους ενός δικτύου. Η πηγή αρχικά εντοπίζει όλες τις διαθέσιμες διαδρομές μέσω πρωτοκόλλου εντοπισμού διαδρομής και καθορίζει τα Active Path Sets (APS) που θα χρησιμοποιηθούν για την επικοινωνία, έπειτα διαχωρίζει κάθε μήνυμα που θέλει να αποστείλει σε μικρά κομμάτια τα κρυπτογραφεί και τα αποστέλλει μέσα από τις διαφορετικές διαδρομές που καθόρισε στο προηγούμενο βήμα. Κάθε κομμάτι έχει και ένα μοναδικό αριθμό MAC (Message Authentication Code) που χρησιμοποιείται για τον έλεγχο της ακεραιότητας και της πιστοποίησης της έγκυρης πηγής από όπου προέρχεται. Ο προορισμός στέλνει μια απάντηση σχετικά με την παράδοση ή μη των πακέτων και έτσι η πηγή αξιολογεί το εκάστοτε APS.

Authenticated Routing for Ad hoc network (ARAN) : Αποτελεί την πρόταση υλοποίησης ενός πρωτοκόλλου δρομολόγησης για ad hoc δίκτυα βασισμένο σε πιστοποιητικά ασφαλείας (Ms. Divyalakshmi Dinesh, Prof. Manjusha Deshmukh, 2014). Χρησιμοποιείται η τεχνική του δημοσίου κλειδιού κρυπτογράφησης της πληροφορίας και ενός κεντρικού υπολογιστή που το διαχειρίζεται και το αποστέλλει σε όλους τους κόμβους του δικτύου. Η πηγή της πληροφορίας αποστέλλει ένα Route Discovery Packet (RDP) στους γειτονικούς κόμβους για τον εντοπισμό των διαδρομών τα οποία και μαρκάρει με ένα αριθμό που τα χαρακτηρίζει. Η διαδρομή της πληροφορίας που μεταδίδεται από κόμβο σε κόμβο καταγράφεται και μεταφέρει το πιστοποιητικό και την ψηφιακή υπογραφή της. Όταν η πληροφορία φτάσει στον προορισμό, και μόνο τότε, στέλνεται ένα μήνυμα απόκρισης περί επιτυχημένης μετάδοσης της στο κόμβο από όπου προήλθε (Mohan Li, 2014). Ταυτόχρονα με τον εντοπισμό της σύντομης διαδρομής κάθε κόμβος επισυνάπτει το πιστοποιητικό του στο κομμάτι της πληροφορίας που μεταδίδεται. Το ARAN απαιτεί κάθε κόμβος να διαθέτει ένα πίνακα routing για κάθε κόμβο στο δίκτυο. Αν για κάποιο χρονικό διάστημα δεν μεταφέρονται δεδομένα από ένα κόμβο αυτόματα γίνεται ανενεργός στον πίνακα. Ωστόσο όταν μελλοντικά γίνει τελικά χρήση του και εντοπιστεί ότι βρίσκεται σε ανενεργή κατάσταση ένα μήνυμα λάθους (ERR) παράγεται για να ενημερωθούν οι γειτονικοί κόμβοι, η ίδια διαδικασία ακολουθείται σε περίπτωση που η σύνδεση είναι κατεστραμμένη ή έχει μεταφερθεί ένας κόμβος αλλού.

Non-Disclosure Method : Είναι μια τεχνική που επιτρέπει την προστασία του εντοπισμού της θέσης – τοποθεσίας. Στην προκειμένη περίπτωση η μετάδοση του μηνύματος γίνεται χωρίς να συμπεριλαμβάνεται η πληροφορία της τοποθεσίας με την χρήση Security Agents όπου χρησιμοποιούν ασύμμετρη κρυπτογράφηση. Η πληροφορία μεταδίδεται μέσω των SAs και όπου και εισάγεται το κλειδί κρυπτογράφησης του εκάστοτε agent, έτσι υπάρχει η δυνατότητα ιχνυλασιμότητας της μετάδοσης που όμως είναι πρόκληση και για τους attackers. Για αυτόν τον λόγο γίνεται μια χρήση τεχνικής μεταβλητών που έχουν ως στόχο να τους μπερδέψουν (Ms. Divyalakshmi Dinesh, Prof. Manjusha Deshmukh, 2014).

Στον παρακάτω πίνακα παρατίθενται συγκεντρωτικά οι εφαρμογές των παραπάνω λύσεων

Solution	Attacks Covered	Technology used	Security requirements
ARAN	1. Replay Attack 2. Impersonation 3. False Warning	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

Εικόνα 11 Πίνακας αντιμέτρων(καλύψεις, τεχνολογία) σε επιθέσεις στα δίκτυα VANET

Συμπεράσματα

Σήμερα, τα δίκτυα των οχημάτων αναπτύσσονται και βελτιώνονται. Πολλές νέες εφαρμογές χρησιμοποιούν αυτό το νέο είδος δικτύου επικοινωνίας. Ωστόσο, επειδή οι εν λόγω εφαρμογές έχουν επιπτώσεις στην ασφάλεια της οδικής κυκλοφορίας, πρέπει να επιτευχθεί η όσο το δυνατό ασφαλέστερη ανταλλαγή πληροφοριών.

Νέοι μηχανισμοί πρέπει να αναπτυχθούν για να ανταποκριθούν στα εν γενή χαρακτηριστικά των εν λόγω δικτύων (ταχύτητα των node's, αποκεντρωμένες υποδομές, κλπ).

Σε αυτήν την εργασία, έχουμε παρουσιάσει μια επισκόπηση των τρεχόντων ζητημάτων ασφαλείας πάνω στα VANETs, με έμφαση στην επικοινωνία της οδικής ασφάλειας. Επιπλέον, έχουμε εντοπίσει τις απαιτήσεις ασφαλείας που υπάρχουν σε κάθε χαρακτηριστικό των δικτύων VANET, καθώς και ότι εκτός από τις τυπικές ανάγκες ασφαλείας (π.χ. εμπιστευτικότητα), υπάρχουν και άλλες ιδαίτερες ανάγκες (π.χ. διασφάλιση της εμπιστοσύνης αναφερθεί σε δεδομένα). Επίσης, έχουμε προσδιορίσει διάφορες επιθέσεις που μπορούν να εκτελεστούν σε αυτά τα δίκτυα και τέλος, έχουμε περιγράψει και αναλύσει τους κύριους προτεινόμενους μηχανισμούς για την επίτευξη των στόχων της ασφάλειας.

Η ιδιωτικότητα και η ασφάλεια αποτελούν απαραίτητο θέμα προσοχής στα δίκτυα VANET, τα οποία είναι εκτεθειμένα σε πολλούς κινδύνους. Ενώ για κάποια είδη επιθέσεων όπως DoS,Routing και Session highjacking έχουν αναπτυχθεί σύγχρονοι μέθοδοι αντιμετώπισης τους. Οι αλγόριθμοι και τα αντίμετρα που έχουν σχεδιαστεί για επιθέσεις όπως Eavesdropping, Message Suppression και άλλες, δεν έχουν φτάσει σε ικανοποιητικό επίπεδο ώστε να εξασφαλίζουν την ασφάλεια και την εύρυθμη λειτουργία των δικτύων VANET. Οι επιθέσεις στο προσεχές μέλλον είναι πιθανόν να αυξηθούν, λόγω του ότι αναπτύσσονται όλο και περισσότερες εφαρμογές βασιζόμενες στα ασύρματα δίκτυα. Από την άποψη αυτή η διαθεσιμότητα του δικτύου εκτίθεται σε πολλούς τύπους επιθέσεων.

Η ασφάλεια στα δίκτυα VANET είναι ένας αναδυόμενος τομέας στον οποίο πολλές μελλοντικές έρευνες μπορούν να προκύψουν. Παρά το γεγονός ότι έχουν προταθεί αρκετοί μηχανισμοί, ορισμένα θέματα πρέπει ακόμη να αντιμετωπιστούν (π.χ. προβλήματα προστασίας της ιδιωτικής ζωής).

Επιπλέον, καθώς τα διάφορα VANET πρωτόκολλα, οι μηχανισμοί και οι εφαρμογές τους βασίζονται σε διαφορετικές αρχιτεκτονικές και παραδοχές, ένα κοινό πλαίσιο αξιολόγησης είναι απαραίτητο για να μετρηθεί και να συγκριθεί η συνεισφορά τους στην ασφάλεια των δικτύων VANET από τις επιθέσεις.

Σήμερα, οι μελέτες για τον σχεδιασμό και κατασκευή δικτύων VANET γίνονται βασιζόμενες στα αποτελέσματα εργαστηριακών προσομοιώσεων, κάτι που δεν καλύπτει όλο το φάσμα κινδύνων και επιθέσεων που καλούνται να αντιμετωπίσουν τα συστήματα σε πραγματικές συνθήκες. Τα αποτελέσματα της προσομοίωσης προσφέρονται συχνά για να αξιολογήθούν οι τρέχουσες προτάσεις. Ωστόσο, ένα κοινό σενάριο για την αξιολόγηση εναλλακτικών λύσεων δεν υπάρχει.

Τέλος, η προσπάθεια ανάπτυξης νέων αντιμέτρων από μεγάλες αυτοκινητοβιομηχανίες, κρατικούς φορείς, όπως το υπουργείο μεταφορών ΗΠΑ (US DoT) και εταιρείες πληροφορικής, όπως IBM, εστιάζεται στην εξέλιξη των πρωτοκόλλων κρυπτογράφησης που πιθανόν μελλοντικά να αποτελέσει και το κατάλληλο αντίμετρο για τα περισσότερα είδη προκλήσεων.

Βιβλιογραφία

[1]: World health organization. (2016). Road traffic injuries. Ανάκτηση από http://www.who.int/mediacentre/factsheets/fs358/en/

[2]: M Raya, D Jungels, P Papadimitratos, I Aad, JP Hubaux (2006).Certificate Revocation in Vehicular Networks. Laboratory for computer Communications and Applications (LCA).School of Computer and Communication Sciences.

[3]: Moustafa,H., Zhang,Y.(2009) .Vehicular networks: Techniques, Standards, and Applications. CRC Press.

[4]: Maxim Raya. (2005). The Security of Vehicular Ad Hoc Networks. SASN'05 Verginia USA. p. 11-21.

[5]: Ram Shringar Raw, Manish Kumar, Nanhay Singh. (2013). International Journal of Network Security & it's Applications (IJNSA). Vol.5, No.5.

[6]: Mohan Li. (2014). Security in Vanets. Ανάκτηση από http://www.cse.wustl.edu/~jain/cse57114/ftp/vanet_security/index.html

[7]: Mohamed Nidhal Mejri, Jalel BenOthman, Mohamed Hamdi. (2014). Survey on VANET security challenges and possible cryptographic solution . Vehicular Communications.

[8]: Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit .(2014). An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs). International Journal of Computer Science Engineering (IJCSE).

[9]: Verma, K., H. Hasbullah, and A. Kumar.(2013). An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. in Advance Computing Conference (IACC). 2013 IEEE 3rd International. 2013: IEEE.

[10]: He, L. and W.T. Zhu. Mitigating. (2012). DoS attacks against signature-based authentication in VANETs. Computer Science and Automation Engineering (CSAE). 2012 IEEE International Conference on 2012: IEEE.

[11]: RoselinMary, S., M. Maheshwari, and M. Thamaraiselvan. (2013). Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA) in Information Communication and Embedded Systems (ICICES). 2013 International Conference on.

[12]: Al-Sakib Khan Pathan (2013). Security of Self-Organizing Networks: MANET, WSN, WMN, VANET. CRC Press.

[13]: Simranpreet Singh Chhatwal, Manmohan Sharma . (2015). Detection of impersonation attack in VANETs using BUCK Filter and VANET Content Fragile Watermarking (VCFW). Computer Communication and Informatics (ICCCI), 2015 International Conference on. IEEE.

[14]: Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane.(2015). SEAD: A simple and eficient adaptive data dissemination protocol in vehicular ad-hoc networks. Wireless Net-works. Ανάκτηση από https://hal.inria.fr/hal-01242289/file/winet.pdf

[15]: Ms. Divyalakshmi Dinesh, Prof. Manjusha Deshmukh. (2014). International Journal of Engineering Technology, Management and Applied Sciences. Ανάκτηση από http://www.ijetmas.com

[16]: Car-2-car. (2007). Simulation Workshops. Ανάκτηση από https://www.car-2-car.org/index.php?id=104