Σχολή Τεχνολογίας

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

"MSc in Modern Communication Systems and the Internet of Things"

«Μελέτη Επιπτώσεων και Εντοπισμού των Επιθέσεων Άρνησης Υπηρεσίας (DoS) σε Συστήματα Αυτόνομων Οχημάτων (CAV) υπό Συνθήκες Κυκλοφοριακής Συμφόρησης»

Ζήσης – Ραφαήλ Τζοάννος του Σωτηρίου

ΛΑΡΙΣΑ, Ιούνιος 2025

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΣΥΓΧΡΟΝΑ ΣΥΣΤΗΜΑΤΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

«Master of Science in Modern Communication Systems and the Internet of Things»

«Study of Effects and Detection of Denial of Service (DoS) Attacks in CAV under Traffic Congestion Conditions»

Διπλωματική Εργασία

που υποβλήθηκε στο Τμήμα Ψηφιακών Συστημάτων του

Πανεπιστημίου Θεσσαλίας

ως μέρος των απαιτήσεων για την απόκτηση

Διπλώματος Μεταπτυχιακών Σπουδών στα Σύγχρονα Συστήματα Επικοινωνιών και Διαδίκτυο των Πραγμάτων από τον

Ζήση – Ραφαήλ Τζοάννο του Σωτηρίου

Δήλωση Αυθεντικότητας, ζητήματα Copyright

«Ο μεταπτυχιακός φοιτητής που εκπόνησε την παρούσα διπλωματική εργασία φέρει ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στη βάση των εξής παραγόντων: του σκοπού και χαρακτήρα της χρήσης (μη-εμπορικός, μη-κερδοσκοπικός, αλλά εκπαιδευτικός-ερευνητικός), της φύσης του υλικού που χρησιμοποιεί (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες κ.λπ.), του ποσοστού και της σημαντικότητας του τμήματος που χρησιμοποιεί σε σχέση με το όλο κείμενο υπό copyright, και των πιθανών συνεπειών της χρήσης αυτής στην αγορά ή την γενικότερη αξία του υπό copyright κειμένου».

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Η παρούσα διπλωματική εργασία εγκρίθηκε ομόφωνα από την τριμελή εξεταστική επιτροπή η οποία ορίστηκε από την Συνέλευση του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Θεσσαλίας, σύμφωνα με το νόμο και τον εγκεκριμένο Οδηγό Σπουδών του ΠΜΣ «Σύγχρονα Συστήματα Επικοινωνιών και Διαδίκτυο των Πραγμάτων».

Τα μέλη της Επιτροπής ήταν:

Επιβλέπων	**Δρ. Δημήτριος Κοσμάνος** Επιστημονικός Συνεργάτης, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Δρ. Κωνσταντίνος Χαϊκάλης** Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Δρ. Γεώργιος Καρέτσος** Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Θεσσαλίας, δεν υποδηλώνει αποδοχή των απόψεων του συγγραφέα.

Ημερομηνία έγκρισης: 27-06-2025

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Περίληψη

Το διαδίκτυο των πραγμάτων (IoT) είναι μία τεχνολογία που χρησιμοποιείται από πολύ μεγάλο αριθμό χρηστών τα τελευταία χρόνια, διότι διευκολύνει την χρήση συνδεδεμένων συσκευών στο διαδίκτυο σε πολλούς τομείς ένας εκ των οποίων είναι τα οχήματα. Το διαδίκτυο των οχημάτων (IoV) είναι μία τεχνολογία η οποία αναπτύσσεται ραγδαία. Πολλές εταιρίες επενδύουν αρκετά εκατομμύρια στον τομέα αυτό με σκοπό την δημιουργία αυτόνομων οχημάτων. Τα Connected and Autonomous Vehicles (CAV) χρησιμοποιούνται στις υπηρεσίες έξυπνων μεταφορών και προσφέρουν πολλά οφέλη τόσο στην κοινωνία όσο και στο περιβάλλον. Η μεγάλη εξέλιξη των αυτόνομων οχημάτων δημιουργεί ευπάθειες στα συστήματα ασφαλείας μέσω των οποίων μπορούν να πραγματοποιηθούν επιθέσεις με σκοπό να πλήξουν τόσο τα οχήματα όσο και τους επιβαίνοντες σε αυτά. Εξαιτίας αυτών των επιθέσεων δημιουργείται η ανάγκη για την λήψη μέτρων προστασίας καθώς και για την εύρεση αντιμέτρων με σκοπό την αποφυγή των επιθέσεων.

Η παρούσα διπλωματική εργασία αναφέρεται στην ασφάλεια των συστημάτων IoV, στις επιθέσεις καθώς και στις μεθόδους προστασίας των συστημάτων CAV και των ad-hoc δικτύων οχημάτων (VANET). Επίσης, παρουσιάζεται μία εις βάθος ανάλυση του αντίκτυπου των επιθέσεων spoofing υπό ρεαλιστικές συνθήκες οδήγησης που μπορεί να προκαλέσουν κυκλοφοριακή συμφόρηση και πιθανό ανεπιθύμητο ατύχημα καθώς και ένα πρώιμο σύστημα εντοπισμού των επιθέσεων με χρήση του φίλτρου Kalman. Η εργασία αυτή πραγματεύεται σενάρια προσομοίωσης που λαμβάνουν υπόψη ένα σύνολο παραμέτρων πολλαπλών επιπέδων, όπως ο λόγος παράδοσης πακέτων (PDR), η επιτάχυνση και η ταχύτητα. Αυτές οι παράμετροι μπορούν να καθορίσουν την ακεραιότητα των ανταλλασσόμενων wave short messages (WSM) και συγκεντρώνονται σε μια κεντρική αξιόπιστη αρχή (CTA) για περαιτέρω ανάλυση. Τέλος, γίνεται υπολογισμός της τιμής του συντελεστή διακύμανσης (CoV), και παρατηρείται αύξηση της απόλυτης τιμής του υπό συνθήκες επίθεσης spoofing.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Abstract

The Internet of Things (IoT) is a technology that has been used by a very large number of users in recent years because it facilitates the use of internet-connected devices in many areas, one of which is vehicles. The Internet of Vehicles (IoV) is a rapidly developing technology. A lot of companies are investing several million in this field to create autonomous vehicles. Connected and Autonomous Vehicles (CAV) are used in smart transport services and offer benefits to both society and the environment. The development of autonomous vehicles creates vulnerabilities in security systems through which attacks can be conducted to harm both the vehicles and their occupants. Because of these attacks, there is a need to take protective measures as well as to find countermeasures to avoid them.

This MSc thesis addresses the security of IoV systems, attacks as well as protection methods of CAV systems and vehicular ad-hoc networks (VANETs). It also presents an in-depth analysis of the impact of spoofing attacks, under realistic road conditions, which may cause some traffic congestion and a potential unwanted accident as well as an early attack detection system using the Kalman filter. This work has to do with simulation scenarios that take into consideration a set of cross-layer parameters, such as packet delivery ratio (PDR), acceleration and speed. These parameters can determine the integrity of the exchanged wave short messages (WSMs) and are aggregated in a central trusted authority (CTA) for further analysis. Finally, coefficient of variation (CoV) is estimated, showing a significant increase in spoofing attack scenario.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου στον Δρ. Κοσμάνο Δημήτριο, επιβλέποντα της διπλωματικής μου εργασίας, για την καθοδήγηση και την βοήθεια που μου παρείχε. Επίσης, θεωρώ υποχρέωση μου να ευχαριστήσω τον επίκουρο καθηγητή Δρ. Ξενάκη Απόστολο και τον αναπληρωτή καθηγητή Δρ. Χαϊκάλη Κωνσταντίνο για την πολύτιμη βοήθεια που μου προσέφεραν. Τέλος, ευχαριστώ τους γονείς μου Τζοάννο Σωτήριο και Παπαδημητρίου Χρυσούλα – Αποστολία για την υλική και ηθική υποστήριξη που μου παρείχαν κατά την εκπόνηση της διπλωματικής μου εργασίας αλλά και καθ' όλη την διάρκεια των σπουδών μου.

Ζήσης – Ραφαήλ Τζοάννος

20/6/2025

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Περιεχόμενα

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

1 Εισαγωγή

Τις τελευταίες δεκαετίες παρατηρείται αλματώδης άνοδος της τεχνολογίας. Αυτό έχει ως αποτέλεσμα διαφορετικές συσκευές που χρησιμοποιούνται στην καθημερινή μας ζωή να συνδέονται στο διαδίκτυο, να επικοινωνούν και να ανταλλάσσουν μηνύματα μεταξύ τους. Αυτό ονομάζεται Internet of Things (IoT) και περιγράφει φυσικά αντικείμενα ή ομάδες τέτοιων αντικειμένων με αισθητήρες, ικανότητα επεξεργασίας, λογισμικό και άλλες τεχνολογίες που συνδέονται και ανταλλάσσουν μηνύματα με άλλες συσκευές και συστήματα μέσω του διαδικτύου ή άλλων δικτύων επικοινωνιών. Ο όρος IoT εμφανίστηκε το 1999 όταν ο Kevin Ashton από το MIT το χρησιμοποίησε σε μια παρουσίαση του.

Το IoT είναι μία κορυφαία τεχνολογία που βρίσκεται σε συνεχή ανάπτυξη και επέκταση και περιλαμβάνει νέες βελτιωμένες συσκευές και υπηρεσίες. Αυτή η επέκταση το έχει καθιστά πολύ δημοφιλές και του δίνει την δυνατότητα να εφαρμόζεται σε διάφορους τομείς της έρευνας. Ένας τέτοιος τομέας είναι το ad hoc δίκτυο οχημάτων (VANET) που με την πάροδο του χρόνου εξελίχθηκε στο διαδίκτυο των οχημάτων (IoV). Χαρακτηριστικό παράδειγμα του IoT είναι η έννοια του έξυπνου σπιτιού που συμπεριλαμβάνει συσκευές όπως φωτιστικά, θερμοστάτες, συστήματα οικιακής ασφάλειας που υποστηρίζουν ένα ή περισσότερα οικοσυστήματα και μπορεί να ελεγχθεί μέσω συσκευών όπως τα έξυπνα κινητά τηλέφωνα και τα έξυπνα ηχεία. (P.A. Laplante κ.α., 2018; Sharma κ.α., 2018)

Το IoV είναι ένα δίκτυο οχημάτων που έχει ως σκοπό τη συλλογή δεδομένων χρησιμοποιώντας τους αισθητήρες που υπάρχουν στα οχήματα ή τις οδικές μονάδες όπως μονάδες GPS, LIDAR, αισθητήρες εικόνας κ.α. Αφενός, τα δεδομένα που συλλέγονται από τα οχήματα περιλαμβάνουν διάφορες παραμέτρους όπως την ταχύτητα ενός οχήματος, τη θέση του και την κατεύθυνση κίνησης του. Αφετέρου τα δεδομένα που συλλέγονται από τις οδικές μονάδες μπορούν να περιλαμβάνουν συνολικές πληροφορίες κυκλοφορίας. Όλα αυτά τα δεδομένα που συλλέγονται υποβάλλονται σε επεξεργασία με σκοπό την παροχή καλύτερης ταξιδιωτικής εμπειρίας, τη βελτίωση της οδηγικής ασφάλειας και την καλύτερη αντιμετώπιση των ατυχημάτων.

Χαρακτηριστική εφαρμογή του IoV αποτελούν οι οδικές μονάδες (RSU) που τοποθετούνται κοντά στις διαβάσεις και μπορούν να ανιχνεύσουν την συμφόρηση των οχημάτων χρησιμοποιώντας είτε κάμερα είτε αισθητήρες που τοποθετούνται στους δρόμους.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Τα συγκεκριμένα δεδομένα μπορούν να χρησιμοποιηθούν μαζί με άλλα δεδομένα που έχουν συλλεγεί από άλλες διαβάσεις για να παρέχουν μια ολοκληρωμένη εικόνα της κυκλοφορίας σε μία περιοχή. Μία άλλη εφαρμογή του IoV που έχει ως σκοπό την ασφάλεια είναι το σύστημα ενημέρωσης και ψυχαγωγίας που εφοδιάζονται τα οχήματα της εταιρείας Subaru. Αυτό το σύστημα είναι σε θέση να αντιλαμβάνεται την κούραση του οδηγού και να ηχεί κάποιο μήνυμα με σκοπό ο οδηγός να σταματήσει για να ξεκουραστεί. Ακόμη οι τεχνολογίες του IoV κυριαρχούν στα συστήματα των έξυπνων πόλεων και στα αυτοκίνητα χωρίς οδηγό. (Khelifi κ.α., 2019; Takahashi, 2020; Nanda κ.α., 2019)

Η ραγδαία εξέλιξη της τεχνολογίας στον τομέα του IoV έχει δημιουργήσει την ανάγκη για διαρκή και αυξημένη ασφάλεια των συστημάτων. Αυτό συμβαίνει, διότι η παραβίαση αυτών των συστημάτων θα επιφέρει επιπτώσεις τόσο στα δεδομένα των χρηστών όσο πιθανόν και στην σωματική τους ασφάλεια. Η ανάπτυξη των αυτόνομων οχημάτων (CAV) είναι απαραίτητη για την ασφαλή επικοινωνία μεταξύ των οχημάτων προκειμένου να διασφαλιστεί η αξιοπιστία και η ασφάλεια. Τα CAV εκπέμπουν περιοδικά πληροφορίες κυκλοφορίας στα γειτονικά τους οχήματα μέσω βασικών μηνυμάτων ασφαλείας (BSM). Οι πληροφορίες που εκπέμπονται είναι η ταχύτητα, η τοποθεσία του οχήματος, το id του κ.α. Στη συνέχεια μία εφαρμογή ασφαλείας χειρίζεται αυτές τις πληροφορίες και παράγει διάφορες ειδοποιήσεις στους οδηγούς. Τέτοιες είναι οι ειδοποιήσεις αποφυγής σύγκρουσης, αλλαγής λωρίδας κυκλοφορίας κ.α. (Nahri κ.α., 2018; Tzoannos κ.α., 2024)

Επομένως, διασφαλίζεται ότι οι κρίσιμες πληροφορίες φτάνουν με τη συντομότερη δυνατή καθυστέρηση σε κάθε όχημα μέσω των μηνυμάτων BSM. Αυτές οι πληροφορίες συνήθως ανταλλάσσονται μέσω της τεχνολογίας Cooperative Adaptive Cruise Control (CACC), που αποτελεί μία βελτίωση του Adaptive Cruise Control (ACC) και βασίζεται σε αισθητήρες επιτρέποντας στα οχήματα να κινούνται σε σταθερό σχηματισμό platoon. Η ασύρματη επικοινωνία μεταξύ των V2V επιτυγχάνεται μέσω της τεχνολογίας Dedicated Short-Range Communication (DSRC) η οποία χρησιμοποιείται ευρέως για την επικοινωνία μεταξύ των οχημάτων και των RSU. Ωστόσο πρόσφατα εισήχθη και το πρότυπο του Cellular-V2X (CV2X) το οποίο χρησιμοποιεί τεχνολογία κινητής τηλεφωνίας για να διευκολύνει την επικοινωνία των οχημάτων ειδικά σε μεγαλύτερες αποστάσεις. (Kosmanos κ.α., 2020; Kosmanos κ.α., 2019)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Τα αυτόνομα οχήματα είναι ευάλωτα σε διάφορες μορφές κυβερνοεπιθέσεων. Γι' αυτό το λόγο τα μηνύματα που ανταλλάσσονται μέσω του διαδικτύου θα πρέπει να επαληθεύονται και να επικυρώνονται για την ορθότητά τους. Χρησιμοποιούνται διάφορες μέθοδοι κρυπτογράφησης για τον έλεγχο ταυτότητας των μηνυμάτων BSM, ωστόσο αυτές οι τεχνικές αποτρέπουν αποτελεσματικά τις εξωτερικές επιθέσεις αλλά όχι και τις εσωτερικές επιθέσεις όπου διαπιστευμένοι κόμβοι στέλνουν πλαστές πληροφορίες είτε εκούσια είτε ακούσια. Τέτοιες επιθέσεις είναι οι επιθέσεις άρνησης υπηρεσίας DoS. Ο εντοπισμός ενός μέλους του platoon αποφασίζεται με τη χρήση του GPS. Αυτό είναι ευάλωτο σε επιθέσεις jamming & spoofing. Τα ήδη υπάρχοντα GPS δεν έχουν την δυνατότητα ανίχνευσης και αντιμετώπισης τέτοιων επιθέσεων λόγω της έλλειψης μηχανισμών κρυπτογράφησης και ελέγχου ταυτότητας. (Nahri κ.α., 2018; Wang κ.α., 2022)

Η παρούσα διπλωματική εργασία αναφέρεται στην ασφάλεια των συστημάτων IoV, στις επιθέσεις καθώς και στις μεθόδους προστασίας των συστημάτων CAV και των ad-hoc δικτύων οχημάτων (VANET). Επίσης παρουσιάζεται μία εις βάθος ανάλυση του αντίκτυπου των επιθέσεων spoofing υπό ρεαλιστικές συνθήκες οδήγησης που μπορεί να προκαλέσουν κυκλοφοριακή συμφόρηση και πιθανό ανεπιθύμητο ατύχημα καθώς και ένα πρώιμο σύστημα εντοπισμού των επιθέσεων με χρήση του φίλτρου Kalman. Στην εργασία διερευνώνται τα αποτελέσματα των επιθέσεων spoofing σε μία σειρά από οχήματα CAV η οποία δημιουργείται με ad-hoc τρόπο, έχοντας κάποιες ελάχιστες εγγυήσεις ασφαλείας όπως ελάχιστη απόσταση μεταξύ των οχημάτων ίση με 2,5m.κ.α. Ακόμη γίνεται υπολογισμός της τιμής του CoV και παρατηρείται αύξηση της απόλυτης τιμής του υπό συνθήκες spoofing. Τέλος, ερευνώνται διάφορες cross-layer παράμετροι όπως το PDR κ.α. Για την επίτευξη των προσομοιώσεων χρησιμοποιούνται τα λογισμικά OMNeT++ 5.6.2, INET 3.6, Veins 5.0 και SUMO 1.9.2.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

2 Κατηγοριοποίηση επιθέσεων και μέθοδοι προστασίας στα CAV και στο VANET

Τα Connected and Autonomous Vehicles (CAV) είναι ένα είδος αυτοκινήτου που είναι εξοπλισμένο με πληθώρα τεχνολογιών όπως αισθητήρες, ρομποτική και πολύπλοκο λογισμικό. Τα οχήματα αυτά εκτελούν διάφορες λειτουργίες όπως επικοινωνία Vehicle to Everything (V2X) και μετάδοση δεδομένων In Vehicle Network (IVN) μέσω ασύρματης τεχνολογίας. Το IVN είναι ο θεμέλιος λίθος των CAV για τον υπολογισμό των δεδομένων και για την επικοινωνία μεταξύ των διαφορετικών αισθητήρων και των μηχανικών εξαρτημάτων σε ένα όχημα. Αυτό χρησιμοποιεί το πρωτόκολλο CAN για αποτελεσματικό ρυθμό μετάδοσης των δεδομένων και την τοπολογία διαύλου για την σύνδεση των Electric Control Units (ECU). Τα CAV ή αλλιώς τα αυτοκίνητα χωρίς οδηγό είναι μια καινούργια τεχνολογία η οποία εντάσσεται στο ευφυές σύστημα μεταφοράς (ITS). (Masood M., Saeed Z. & Khan M. U., 2023; Limbasiya κ.α., 2022)

Το Vehicular Ad-hoc Network (VANET) είναι ένας τύπος δικτύου που δημιουργήθηκε χρησιμοποιώντας τις αρχές των Mobile Ad-hoc Networks (MANETs), έχοντας μία πλήρως αυτό-οργανωμένη διαμόρφωση. Το δίκτυο αυτό έγινε γνωστό το 2001 στις εφαρμογές ad-hoc κινητής επικοινωνίας και δικτύωσης car-to-car, δημιουργώντας δίκτυα με σκοπό την ανταλλαγή πληροφοριών μεταξύ των οχημάτων. Γνωστές εφαρμογές του δικτύου VANET αποτελούν η αποτελεσματική διαχείριση της κυκλοφορίας, η παρακολούθηση της οδικής συμπεριφοράς και η προσφορά ασφάλειας και άνεσης στους οδηγούς. Τα VANET αναφέρονται ως έξυπνα δίκτυα μεταφορών (ITS) και αποτελούν τον προπομπό του διαδικτύου των οχημάτων (IoV). (C.K. Toh, 2008; Talib κ.α., 2018)

2.1 Είδη επιθέσεων στα συστήματα CAV

Τα συστήματα CAV είναι ένα επίκαιρο θέμα έρευνας τόσο στον ακαδημαϊκό χώρο όσο και στον βιομηχανικό τομέα. Η ανάπτυξη τους υπόσχεται βελτίωση της κυκλοφορίας, ελαχιστοποίηση των τροχαίων ατυχημάτων και διευκόλυνση της βιώσιμης μεταφοράς. (Sun κ.α., 2022) Τα CAV είναι υποχρεωτικό να συνδέονται με άλλες οντότητες για την

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ορθή λειτουργία τους. Η σύνδεση αυτή όμως τα κάνει ευάλωτα σε διάφορες επιθέσεις. Υπάρχουν δύο είδη επιθέσεων οι παθητικές και οι ενεργές.

1. *Παθητικές επιθέσεις*: Όταν συμβαίνει μία παθητική επίθεση είναι πολύ δύσκολο να εντοπιστεί. Αυτό γίνεται, διότι ο εισβολέας δεν μπορεί να αλλάξει το περιεχόμενο των δεδομένων του μηνύματος. Επίσης, ο αποστολέας και ο παραλήπτης δεν γνωρίζουν ότι παρεμβάλει κάποιος κακόβουλος στην μεταξύ τους επικοινωνία. Οι επιθέσεις αυτές έχουν ως σκοπό την παρακολούθηση της κυκλοφορίας των δεδομένων.
    - *Υποκλοπή*: Οι επιθέσεις υποκλοπής (Eavesdropping) έχουν ως σκοπό την κλοπή των μηνυμάτων από το κανάλι επικοινωνίας V2X. Πιθανές ευπάθειες του διαύλου CAN έχουν ως αποτέλεσμα οι εισβολείς να αποκτούν πρόσβαση στο δίκτυο του οχήματος και να παρακολουθούν την μετάδοση των μηνυμάτων. Το γεγονός ότι τα οχήματα CAV επικοινωνούν με διάφορους άλλους όπως πεζούς, υποδομές κ.α. κάνει τις επιθέσεις υποκλοπής μείζονος σημασίας, διότι οι κακόβουλοι μπορούν να παρακολουθούν ιδιωτικές πληροφορίες. Αυτές οι πληροφορίες μπορεί να κοινοποιηθούν σε εταιρείες διαφόρων συμφερόντων με σκοπό να πλήξουν τους χειριστές των οχημάτων. Οι επιθέσεις αυτές είναι γνωστές και ως επιθέσεις sniffing ή snooping.
    - *Ανάλυση κυκλοφορίας δεδομένων:* Επειδή οι επιθέσεις υποκλοπής μπορούν να αποφευχθούν με τη χρήση κρυπτογραφημένων μηνυμάτων, οι κακόβουλοι χρησιμοποιούν τεχνικές ανάλυσης της κυκλοφορίας των δεδομένων για να αντλήσουν πληροφορίες μέσω της κίνησης αυτών. Τέτοιες πληροφορίες είναι η διάρκεια, ο χρόνος, η συχνότητα των μηνυμάτων αλλά και η παρουσία ή μη του οδηγού. Οι κακόβουλοι μέσα από αυτά τα δεδομένα μπορούν να εξάγουν πληροφορίες για την καθημερινότητα των χρηστών των CAV.
2. *Ενεργές επιθέσεις:* Σε αυτό το είδος επιθέσεων οι κακόβουλοι εισχωρούν στο δίκτυο επικοινωνίας και μπορούν να αλλάξουν τα περιεχόμενα των μηνυμάτων ή να παράγουν νέα πακέτα δεδομένων. Οι επιθέσεις αυτές είναι σοβαρότερες από τις παθητικές στα συστήματα των CAV, διότι η αλλαγή των μηνυμάτων μπορεί να προκαλέσει βλάβη στο ίδιο το όχημα αλλά και τραυματισμό των επιβαινόντων.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

- *Επιθέσεις DoS και DDoS:* Μία επίθεση άρνησης υπηρεσίας (DoS) συμβαίνει όταν μία υπηρεσία είναι μη διαθέσιμη για κάποιο χρονικό διάστημα λόγω υπερφόρτωσης της χωρητικότητας ή εξάντλησης των πόρων του δικτύου. Αυτή η επίθεση είναι σοβαρή, διότι μπορεί να καταστρέψει ολόκληρο το δίκτυο των οχημάτων κάνοντας τις υποδομές και τις υπηρεσίες μη διαθέσιμες για τους χρήστες. Σε μία επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS), οι κακόβουλοι χρησιμοποιούν μεγαλύτερο αριθμό παραβιασμένων συστημάτων για να επιτεθούν. Αυτό κάνει δύσκολο τον εντοπισμό και την άμυνα κατά της επίθεσης. Οι επιτιθέμενοι δεν έχουν ως σκοπό την υποκλοπή των πληροφοριών αλλά να καταστήσουν το δίκτυο μη διαθέσιμο. Λόγω του αντίκτυπου που έχει ένα μη διαθέσιμο δίκτυο στους χρήστες, αυτή η επίθεση είναι η πιο διαδεδομένη μεταξύ των υπολοίπων.

Υπάρχουν διάφορες επιθέσεις οι οποίες ως αποτέλεσμα προκαλούν άρνηση υπηρεσίας. Οι πιο σημαντικές είναι οι ακόλουθες:

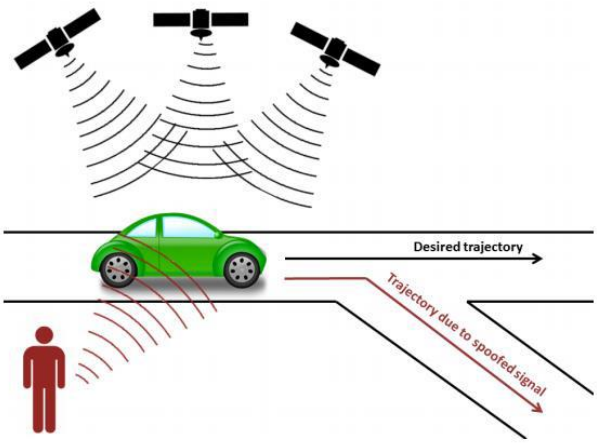
  - *Επίθεση Μπλοκάρισμα:* Η επίθεση μπλοκάρισμα (Jamming) είναι ένα από τα μέσα που χρησιμοποιούν οι κακόβουλοι για να παραβιάσουν τα δίκτυα οχημάτων. Η επίθεση αυτή κατατάσσεται στις επιθέσεις DoS, διότι οι επιτιθέμενοι προκαλούν άρνηση υπηρεσιών στα εξουσιοδοτημένα συστήματα κατακλύζοντάς τα με κίνηση δεδομένων και διατηρώντας απασχολημένο το μέσο επικοινωνίας. Τέτοιες επιθέσεις γίνονται συνήθως σε αισθητήρες όπως το GPS, ο Lidar και η κάμερα προκαλώντας παρεμβολές.
  - *Επίθεση Man-In-The-Middle:* Η επίθεση MITM αποσκοπεί στην παραβίαση και στην υποκλοπή των επικοινωνιών μεταξύ δύο μερών του δικτύου. Αυτή είναι μια επικίνδυνη επίθεση στο δίκτυο, διότι ο επιτιθέμενος παρακολουθεί κρυφά, καταγράφει και ελέγχει την επικοινωνία μεταξύ των συστημάτων.

- *Επιθέσεις Spoofing*: Με τον όρο επιθέσεις πλαστογράφησης εννοούμε την εισβολή ενός μη εξουσιοδοτημένου ατόμου στο δίκτυο του οχήματος και την παρουσίαση του ως εξουσιοδοτημένου. Ο εισβολέας εκπέμπει ψευδή μηνύματα και έχει ως σκοπό τη λήψη λάθος αποφάσεων από τα συστήματα του CAV. Παράδειγμα αποτελεί το ατύχημα που θα συμβεί εάν το CAV πιστεύει, λόγω ψευδούς μηνύματος που έχει λάβει, πως δεν υπάρχει κάποιο εμπόδιο στην πορεία του ενώ υπάρχει. Ακόμη, οι εισβολείς μπορούν να κατευθύνουν πολλά αυτοκίνητα μαζί

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

προς μία κατεύθυνση δημιουργώντας κυκλοφοριακή συμφόρηση. Κατά τη διάρκεια τέτοιων επιθέσεων οι κακόβουλοι μπορούν να τροποποιήσουν, να καθυστερήσουν και να απορρίψουν μηνύματα ή δεδομένα μεταξύ των CAV προκαλώντας μη επιθυμητές καταστάσεις στη λειτουργία του platoon οχημάτων.

Μια χαρακτηριστική εφαρμογή αυτής της επίθεσης είναι το *GPS Spoofing*. Τα CAV βασίζονται σε μεγάλο βαθμό στο GPS το οποίο παρέχει πληροφορίες τοποθεσίας και ώρας. Αυτό αποτελεί τη βάση πολλών κύριων διεργασιών όπως τα βασικά μηνύματα ασφαλείας και οι χρονικές σημάνσεις των μηνυμάτων. Με αυτή την επίθεση ο κακόβουλος εξαπατά τον χρήστη μέσω της μετάδοσης σημάτων που έχουν τα ίδια χαρακτηριστικά με εκείνα των νόμιμων δορυφορικών σημάτων GPS. Η ισχύς του ψευδούς σήματος είναι υψηλότερη από το πραγματικό σήμα GPS και ως εκ τούτου το όχημα αγνοεί το πραγματικό σήμα οδηγώντας το σε λάθος πορεία καθώς είναι προγραμματισμένο να ακολουθεί το ισχυρότερο σήμα GPS. (Kamal κ.α., 2021) Η επίθεση αυτή απεικονίζεται στην Εικόνα 1. Σύμφωνα με έρευνες τα συστήματα πλοήγησης των Tesla Model S και Model 3 είναι ευάλωτα σε επιθέσεις. Οι ερευνητές απέδειξαν ότι μπορούν να εκτελεστούν επιθέσεις GPS Spoofing στο GPS των οχημάτων Tesla ασύρματα.



Εικόνα 1: Απεικόνιση επίθεσης GPS Spoofing [17]

Μία άλλη μορφή επίθεσης των συστημάτων CAV αποτελούν οι επιθέσεις μέσω του διαύλου CAN. Το Controller Area Network (CAN) είναι ένα απλό και ισχυρό πρωτόκολλο σειριακής επικοινωνίας που έχει σχεδιαστεί για την αυτοκινητοβιομηχανία και μπορεί να εφαρμοστεί με επιτυχία σε συστήματα πραγματικού χρόνου. Το πρωτόκολλο αυτό επιτρέπει την επικοινωνία μεταξύ διαφορετικών αισθητήρων και ενεργοποιητών.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Γι’ αυτό χρησιμοποιείται από τις μεγαλύτερες αυτοκινητοβιομηχανίες όπως η General Motors, η Volkswagen κ.α. Στα σύγχρονα οχήματα εκατοντάδες μονάδες ECU είναι ενσωματωμένες για τον έλεγχο των διάφορων λειτουργιών των οχημάτων. Αυτές οι μονάδες ECU συνδέονται και επικοινωνούν μέσω του διαύλου CAN.

Ο δίαυλος CAN κατέχει σημαντικό ρόλο στην αυτόνομη οδήγηση, διότι μέσω αυτού γίνεται ο έλεγχος, η διάγνωση και μεταφέρονται τα διαφορετικά σήματα μεταξύ των ECU. Ο δίαυλος CAN όντας ο κεντρικός δίαυλος εντός του οχήματος γίνεται στόχος των hackers. Παραβιάζοντας κανείς τον δίαυλο CAN μπορεί να αποκτήσει πρόσβαση στις ECU και να απειληθεί τόσο η ασφάλεια του οχήματος όσο και των επιβαινόντων. Οι επιθέσεις στον δίαυλο CAN ταυτίζονται με αυτές των οχημάτων CAV, καθώς αυτό αποτελεί μέρος του αυτόνομου οχήματος. Ωστόσο, υπάρχουν τρεις κύριες κατηγορίες επιθέσεων του διαύλου CAN:

1. *Επιθέσεις στις ECU*
2. *Επιθέσεις στο IVN*
3. *Επιθέσεις σχετικά με το κλειδί του αυτοκινήτου*

Δύο χαρακτηριστικές επιθέσεις στον διαύλου CAN είναι οι εξής:

- *Τροποποίηση μηνυμάτων:* Σε επιθέσεις τροποποίησης μηνυμάτων οι κακόβουλοι εισάγουν ψευδή μηνύματα στο δίκτυο IVN μέσω της θύρας (On-Board Diagnostic) OBD-II ή άλλου συστήματος τηλεματικής. Το πρωτόκολλο CAN δεν διαθέτει κάποιο μηχανισμό ελέγχου ταυτότητας των μηνυμάτων και ως εκ τούτου μπορεί να δεχθεί επίθεση από κακόβουλους. Ακόμη, η τροποποίηση μηνυμάτων περιλαμβάνει την καθυστέρηση ενός μηνύματος, την αναδιάταξη ή διαγραφή ορισμένων πακέτων του μηνύματος ή την εισαγωγή νέων. Παράδειγμα αποτελεί η καθυστέρηση του μηνύματος για έκτακτο φρενάρισμα το οποίο μπορεί να προκαλέσει σοβαρό ατύχημα.
- *Επιθέσεις επανάληψης:* Αυτές οι επιθέσεις συμβαίνουν όταν κάποιος κακόβουλος υποκλέπτει τα δεδομένα της επικοινωνίας του καναλιού, τα καταγράφει και τα αναμεταδίδει. Ενώ ο αποστολέας και ο παραλήπτης είναι πιστοποιημένοι δεν γνωρίζουν πως κάποιος έχει εισχωρήσει ανάμεσα τους και παρεμποδίζει τα μηνύματα. Τέτοιες χρησιμοποιούνται στις επιθέσεις σχετικά με το κλειδί του αυτοκινήτου. (Kamal κ.α., 2021; Khattak Z., Smith B. & Fontaine M., 2021; Sun X., Yu R. & Zhang P., 2022; Masood M., Saeed Z. & Khan M. U., 2023; Limbasiya κ.α., 2022, Tzoannos, 2023)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

2.2 Μορφές επιθέσεων στο δίκτυο VANET

Το ad-hoc δίκτυο οχημάτων VANET είναι ένα αυτό-οργανωμένο δίκτυο που δημιουργήθηκε για να παρέχει ασύρματη επικοινωνία μεταξύ οχημάτων, στα οποία οι πληροφορίες διαδραματίζουν σημαντικό ρόλο σε θέματα όπως η ανίχνευση σύγκρουσης, η εκ νέου δρομολόγηση, η παρακολούθηση κυκλοφορίας κ.α. Οι κύριες προκλήσεις που αντιμετωπίζει το VANET είναι η ασφάλεια και το απόρρητο των πληροφοριών που οδηγούν σε ποικίλες επιθέσεις. Σε αυτό μπορούν να πραγματοποιηθούν πολυάριθμοι τύποι επιθέσεων με την επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) να είναι μία από τις πιο κοινές και επικίνδυνες. Οι επιθέσεις αυτές έχουν ως αποτέλεσμα την έλλειψη διαθεσιμότητας πληροφοριών για την επικοινωνία των οχημάτων. Αναπτύχθηκαν πολλές μέθοδοι για την αντιμετώπιση του DDoS ωστόσο η αποτελεσματικότητα των περισσότερων ήταν περιορισμένη σε κάποιο βαθμό και οι εισβολείς εκμεταλλεύτηκαν αυτές τις αδυναμίες για να πραγματοποιήσουν επιθέσεις στο δίκτυο. (Krishna K. & Reddy K., 2023)

2.2.1 Είδη επιθέσεων

Το δίκτυο VANET χρησιμοποιεί πληθώρα νέων τεχνολογιών καθώς και διάφορους τρόπους επικοινωνίας μεταξύ των οχημάτων γεγονός που δημιουργεί ευπάθειες τις οποίες μπορούν να εκμεταλλευτούν διάφοροι κακόβουλοι. Τρεις κύριες κατηγορίες επιθέσεων είναι:

1. *Επιθέσεις στο δίκτυο οχημάτων (VANET):* Όταν ένα όχημα ή μία υποδομή συνδέεται στο δίκτυο VANET επιτρέπεται η μεταξύ τους επικοινωνία προσφέροντας τους πολλές δυνατότητες. Τέτοιες είναι οι πληροφορίες σχετικά με την κίνηση, την κατάσταση του δρόμου καθώς και τη θέση των οχημάτων και των πεζών με σκοπό την αποφυγή των ατυχημάτων και της κυκλοφοριακής συμφόρησης. Εφόσον στο δίκτυο VANET δεν παρέχεται κεντρική διαχείριση, διάφορα πρωτόκολλα ασφαλείας τα οποία απαιτούν κεντρικό trusted third party (TTP) ή απαιτούν διαρκή συνδεσιμότητα όπως η υποδομή δημοσίου κλειδιού (PKI) δεν μπορούν να χρησιμοποιηθούν δημιουργώντας ευπάθειες.

   Η ασφάλεια του δικτύου μπορεί να γίνει στόχος επιθέσεων όπως οι επιθέσεις κωδικού πρόσβασης ή οι επιθέσεις κλειδιού. Μία άλλη επίθεση είναι η υποκλοπή δεδομένων κατά την διάρκεια της ασύρματης σύνδεσης, μέσω της οποίας δίνεται πρόσβαση στους εισβολείς στα ιδιωτικά δεδομένα του οχήματος όπως είναι η τοποθεσία. Άλλη μια επίθεση είναι η επίθεση Sybil όπου ένα κακόβουλο όχημα

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

εκπέμπει διάφορα μηνύματα χρησιμοποιώντας πλαστά διαπιστευτήρια. Άλλες επιθέσεις στις οποίες είναι ευάλωτο το δίκτυο VANET είναι οι επιθέσεις black-hole, οι επιθέσεις wormhole και οι επιθέσεις DoS τόσο σε μεμονωμένα οχήματα όσο και σε ομάδες οχημάτων. Επιπλέον καθώς οι ασύρματες επικοινωνίες γίνονται με την χρήση των πρωτοκόλλων Wi-Fi, Bluetooth, GSM, τα οχήματα μπορεί να γίνουν στόχοι επιθέσεων λόγω των ευπαθειών των πρωτοκόλλων.

2. *Επιθέσεις στους αισθητήρες:* Τα οχήματα και κυρίως τα αυτόνομα οχήματα εξοπλίζονται με πληθώρα αισθητήρων οι οποίοι είναι υπεύθυνοι για διάφορες διεργασίες. Τέτοιες είναι ο έλεγχος της απόστασης μεταξύ των οχημάτων, οι οδικές συνθήκες, η ανίχνευση καπνού ή φωτιάς, το σύστημα επιτάχυνσης – επιβράδυνσης του οχήματος καθώς και η ανίχνευση εμποδίων. Οι αισθητήρες αποτελούν σημαντικό στοιχείο των αυτόνομων οχημάτων καθώς παρέχουν πληροφορίες με σκοπό την ασφαλή οδήγηση. Επίθεση σε αυτούς συνεπάγεται αλλοίωση των δεδομένων γεγονός που μπορεί να οδηγήσει στην πρόκληση ατυχημάτων και στον τραυματισμό των επιβαινόντων στο όχημα. Παράδειγμα αποτελεί η απενεργοποίηση του συστήματος πέδησης ή του τιμονιού ενός αυτόνομου οχήματος από κάποιον κακόβουλο. Άλλες μορφές επιθέσεων στους αισθητήρες είναι:
    - οι επιθέσεις Jamming στον αισθητήρα Lidar
    - οι επιθέσεις αλλοίωσης της ποιότητας της κάμερας
    - οι επιθέσεις Spoofing στο σήμα του GPS ή του Lidar κ.α.

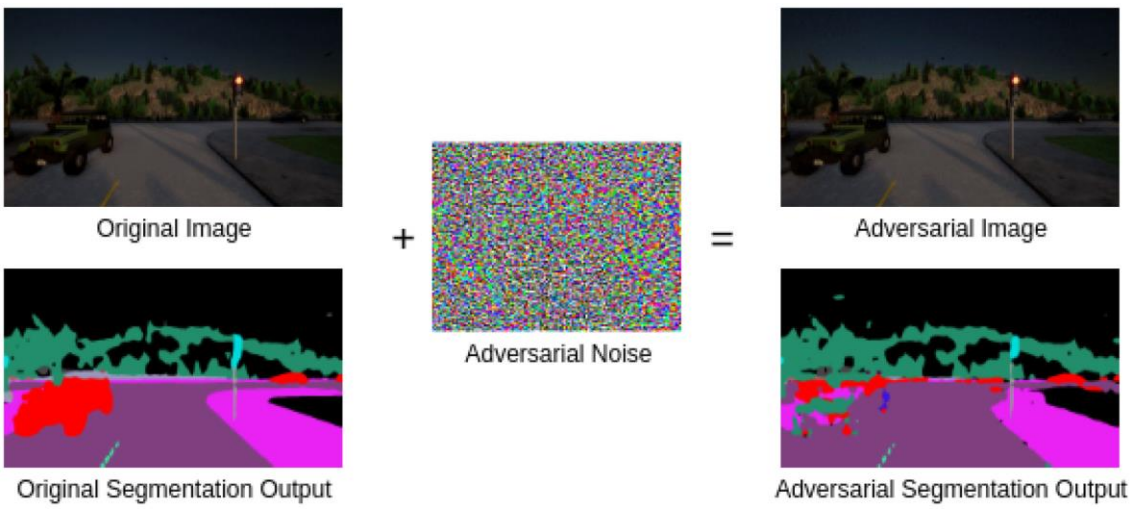
   Όλες αυτές οι επιθέσεις επηρεάζουν άμεσα την λειτουργία του οχήματος καθώς τα δεδομένα που παρέχονται σε αυτό έχουν αλλοιωθεί και οι αποφάσεις που λαμβάνει θα είναι λανθασμένες.
3. *Επίθεση στο Hardware:* Εκτός από τις επιθέσεις που διεξάγονται από κακόβουλους οι οποίοι βρίσκονται μακριά από το όχημα και αποσκοπούν στην αλλοίωση των δεδομένων των αισθητήρων ή στην υποκλοπή των δεδομένων, υπάρχουν και επιθέσεις που διεξάγονται από άτομα που έχουν πρόσβαση στο όχημα. Τέτοιοι είναι οι μηχανικοί που επισκευάζουν τα οχήματα. Αυτοί αποκτώντας πρόσβαση στο υλικό των αυτόνομων οχημάτων μπορεί να εκμεταλλευτούν τα δεδομένα των αισθητήρων και να προκαλέσουν βλάβη στα συστήματα επικοινωνίας. Αυτοί μπορούν ακόμη να εισάγουν ιούς ή κακόβουλο λογισμικό στο framework του οχήματος. Αυτό μπορεί να συμβεί ενημερώνοντας το firmware της μονάδας ECU με προσαρμοσμένες βιβλιοθήκες που έχουν ως σκοπό την πρόκληση των κακόβουλων λειτουργιών στο όχημα. (Talib κ.α., 2018; Kloukiniotis κ.α., 2022)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

2.2.2 Επιθέσεις Adversarial Attack σε αυτόνομα οχήματα

Μία επιπλέον σημαντική μορφή επιθέσεων στα αυτόνομα οχήματα είναι οι επιθέσεις Adversarial Attack. Οι επιθέσεις αυτές περιλαμβάνουν μικρές διαταραχές οι οποίες δεν γίνονται αντιληπτές από το ανθρώπινο μάτι αλλά μολύνουν τις εικόνες που καταγράφει το όχημα με σκοπό την πρόκληση λάθος αποφάσεων. Αυτό συμβαίνει διότι οι μολυσμένες εικόνες παραπλανούν τα μοντέλα βαθιάς μάθησης, τα οποία χρησιμοποιούν τις εικόνες που συλλέγονται από τους αισθητήρες του οχήματος ώστε να λάβουν τις απαραίτητες αποφάσεις. Υπάρχουν δύο τύποι τέτοιων επιθέσεων. Αυτές είναι οι evasion και poisoning attacks.

Στις επιθέσεις evasion παραποιούνται τα δεδομένα ελέγχου με σκοπό την εσφαλμένη ταξινόμηση τους. Οι επιθέσεις αυτές πραγματοποιούνται στο μοντέλο της μηχανικής μάθησης κατά την διάρκεια της εξαγωγής των συμπερασμάτων. Κατά την επίθεση σχεδιάζονται δεδομένα εισόδου με συγκεκριμένες ιδιότητες μη αντιληπτές από τον άνθρωπο οι οποίες μπορούν να χειραγωγήσουν το μοντέλο στόχου με αποτέλεσμα να παραχθούν λανθασμένες αποφάσεις. Στις επιθέσεις poisoning παραποιούνται τα δεδομένα εκπαίδευσης με σκοπό να επηρεαστεί το επίπεδο αντίληψης του μοντέλου και να προκληθεί άρνηση εξυπηρέτησης. Κάποιοι τρόποι χειραγώγησης του μοντέλου στόχου είναι η καταστροφή της λογικής του, ο χειρισμός και η μόλυνση των δεδομένων του κ.α. Ένα χαρακτηριστικό παράδειγμα επιθέσεων Adversarial Attack απεικονίζεται στην Εικόνα 2 η οποία δείχνει την εξαφάνιση ενός μέρος του οχήματος από τον αισθητήρα της κάμερας μετά από επίθεση. (Kloukiniotis κ.α., 2022; Amirkhani κ.α., 2022)



Εικόνα 2: Προσομοίωση επίθεσης Adversarial Attack [11]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

2.2.3 Τύποι επιθέσεων στην ανίχνευση αντικειμένων

Η ανίχνευση αντικειμένων είναι μία από τις πιο σημαντικές εφαρμογές βαθιάς μάθησης. Οι τεχνικές ανίχνευσης αντικειμένων γίνονται συχνά στόχοι επιθέσεων Adversarial Attack χάνοντας έτσι την αξιοπιστία και την αποτελεσματικότητα τους. Δύο κύριες μορφές επιθέσεων Adversarial Attack που έχουν ως σκοπό την παραπλάνηση των τεχνικών της μηχανικής μάθησης είναι οι στοχευμένες και οι μη στοχευμένες επιθέσεις. Οι μη στοχευμένες επιθέσεις θέλουν να εξαπατήσουν ένα μοντέλο ανίχνευσης αντικειμένων και δεν δίνουν σημασία στην τελική ετικέτα ή στις παραπλανητικές ετικέτες. Σε αυτές τις επιθέσεις τα αντικείμενα λαμβάνουν λανθασμένες ετικέτες. Από την άλλη, οι στοχευμένες επιθέσεις έχουν ως στόχο την εξαπάτηση του μοντέλου ώστε να ορίζει συγκεκριμένες ετικέτες στα αντικείμενα. Αυτές οι επιθέσεις πραγματοποιούνται για μία συγκεκριμένη κατηγορία αντικειμένων. Επίσης, στην ανίχνευση αντικειμένων πραγματοποιούνται και επιθέσεις μαύρου και λευκού κουτιού. Τέλος, υπάρχουν διάφορες μορφές επιθέσεων κατά της ανίχνευσης των αντικειμένων σε αυτόνομα οχήματα. Τέτοιες είναι οι *Επιθέσεις Targeted Objectness Gradient (TOG),* οι *επιθέσεις evaporate*, οι *επιθέσεις DeepFool* κ.α. (Amirkhani κ.α., 2022)

2.3 Τρόποι προστασίας κακόβουλων επιθέσεων

2.3.1 Στα συστήματα CAV

Τα οχήματα CAV αποτελούνται από πολλές διαφορετικές τεχνολογίες με τις οποίες πρέπει να επικοινωνούν. Αυτό τα καθιστά ευάλωτα σε κακόβουλες επιθέσεις. Σύμφωνα με έρευνα, το 2019 μόνο το 38% των επιθέσεων ήταν για ερευνητικούς σκοπούς. Το 57% των επιθέσεων πραγματοποιήθηκαν από κακόβουλους με σκοπό να πλήξουν το όχημα και να υποκλέψουν τις προσωπικές πληροφορίες των χρηστών του. Για την αντιμετώπιση των επιθέσεων αλλά και για την καλύτερη θωράκιση των οχημάτων παρουσιάζονται ορισμένα αντίμετρα.

1. *Κρυπτογράφηση:* Μία λύση αποτελεί η κρυπτογράφηση των μηνυμάτων. Είναι πολύ σημαντικό να έχουν πρόσβαση στα μηνύματα μόνο οι νόμιμοι χρήστες. Αυτό επιτυγχάνεται με ένα καλό σύστημα κρυπτογράφησης – αποκρυπτογράφησης. Μέσω της κρυπτογράφησης προστατεύονται τα μηνύματα και η επικοινωνία γίνεται πιο ασφαλής. Αυτή η τεχνική είναι πολύ σημαντική για τα σύγχρονα οχήματα επειδή διασφαλίζει την ασφάλεια και την ακεραιότητα των δεδομένων. Άρα,

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

η επικοινωνία πρέπει να είναι επαρκώς κρυπτογραφημένη και η διεύθυνση IP των τηλεματικών συσκευών να μην αποκαλύπτεται σε εξωτερικές συσκευές.

2. *Απομόνωση απειλών:* Η διασύνδεση του εσωτερικού δικτύου των οχημάτων με τον εξωτερικό κόσμο είναι ένα σύνηθες σημείο επίθεσης. Η θύρα OBD και το σύστημα τηλεματικής αποτελούν τις διεπαφές σύνδεσης του CAV με τις εξωτερικές συσκευές. Η θύρα OBD χρησιμοποιείται για διαγνωστικούς σκοπούς. Από την άλλη το σύστημα τηλεματικής συλλέγει πληροφορίες για την τοποθεσία του οχήματος, την δραστηριότητα του οδηγού κ.α. τις οποίες στέλνει στους διακομιστές χρησιμοποιώντας το δίκτυο κινητής τηλεφωνίας. Η απομόνωση της θύρας OBD από το εσωτερικό δίκτυο είναι δύσκολη καθώς χρησιμοποιείται για τον εντοπισμό των βλαβών του οχήματος αλλά και για την ενημέρωση του υλικολογισμικού. Εγκαθιστώντας έναν ανιχνευτή σε αυτήν τη θύρα θα εντοπιστεί εάν γίνει προσπάθεια αποστολής μολυσμένων δεδομένων προς το εσωτερικό δίκτυο του οχήματος κατά την διαδικασία εύρεσης βλαβών.
3. *Εγκατάσταση πυλών:* Οι πύλες (gateways) είναι αναπόσπαστο μέρος των δικτύων επικοινωνίας των οχημάτων. Αυτό συμβαίνει, διότι οι ECU επικοινωνούν μεταξύ τους μέσω πυλών. Οι πύλες λειτουργούν ως μεταφραστές μεταξύ των κόμβων που χρησιμοποιούν διαφορετικά πρωτόκολλα και των διάφορων μορφών data frame. Παράδειγμα αποτελεί όταν μία χαμηλής ταχύτητας ECU θέλει να στείλει μήνυμα σε μία ECU υψηλής ταχύτητας. Τότε οι πύλες προσαρμόζουν το baud rate με σκοπό την συμβατότητα μεταξύ του αποστολέα και του παραλήπτη. Παρόλο που οι πύλες χρησιμοποιούνται αρκετά χρόνια στα δίκτυα οχημάτων οι σύγχρονες πύλες είναι αρκετά πολύπλοκες λόγω των αυξημένων μονάδων ECU των οχημάτων.
4. *Σύστημα ανίχνευσης εισβολής:* Το σύστημα Intrusion Detection System (IDS) έχει σχεδιαστεί για το δίκτυο CAN. Αυτό χρησιμοποιεί τις γνωστές επιθέσεις όπως η επίθεση DoS για να αναγνωρίσει τυχόν επιθέσεις στο όχημα. Όμως με τη χρήση αυτού του συστήματος αυξάνεται πολύ η πολυπλοκότητα. Άλλες τεχνικές για τον ίδιο σκοπό είναι η βαθιά μάθηση, τα συστήματα ανίχνευσης ανωμαλιών κ.α. Επομένως, οι σχεδιαστές των αυτόνομων οχημάτων πρέπει να τοποθετήσουν συστήματα προστασίας από εισβολές στα δίκτυα οχημάτων με σκοπό τον εντοπισμό των εισβολέων και την αναφορά τους. Ο Πίνακας 1 παρουσιάζει τις διάφορες μορφές επιθέσεων καθώς και τα προτεινόμενα αντίμετρα. (Kim κ.α., 2021; Masood M., Saeed Z. & Khan M. U., 2023, Tzoannos, 2023)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Πίνακας 1: Μορφές επιθέσεων και προτεινόμενα αντίμετρα [17, 22]

Type of Attacks	Proposed Countermeasures
Eavesdropping	Authentication, Encryption, Cryptography
Traffic Analysis	Intrusion Detection System (IDS), Encryption
Spoofing	Authentication, IDS
GPS Spoofing	Bias Estimation Range Check, Velocity Consistency Check, Global Navigation Satellite System Augmentation
Replay Attacks	Gateway installation, Encryption
Masquerades	Authentication, Gateways, Encryption
Message Modification	Authentications, Encryption
Denial-of-Service Attack	Gateways installation, IDS, Encryption, Authentication

Τέλος, για τον εντοπισμό των επιθέσεων GPS Spoofing χρησιμοποιούνται τα δεδομένα εισόδου και εφαρμόζονται κατάλληλοι αλγόριθμοι ώστε να παραχθούν λύσεις μετριασμού των επιθέσεων. Μία από τις λύσεις της βιβλιογραφίας χρησιμοποιεί δεδομένα από πολλαπλούς αισθητήρες όπως το επιταχυνσιόμετρο, το γυροσκόπιο, η πυξίδα κ.α. για τον υπολογισμό μίας παράλληλης ροής των εκτιμώμενων τοποθεσιών του οχήματος χωρίς τη χρήση του GPS αλλά μίας μεθόδου που βασίζεται στο Bayesian filtering. Έτσι, μέσω της σύγκρισης της εκτιμώμενης θέσης του οχήματος και της ένδειξης του GPS γίνεται ο εντοπισμός των πιθανών επιθέσεων. Μία άλλη λύση είναι ένας συνεργατικός αμυντικός μηχανισμός έναντι των GPS Spoofing επιθέσεων που βασίζεται στην πολλαπλή συγκέντρωση πληροφοριών μεταξύ των οχημάτων ενός δικτύου και περιλαμβάνει μετρήσεις όπως οι σχετικές αποστάσεις, οι σχετικές γωνίες και οι σχετικές αζιμουθιακές γωνίες των οχημάτων για τον υπολογισμό της θέσης. Ακόμη, γίνονται προσπάθειες και για την εύρεση νέων αλγορίθμων εντοπισμού και αντιμετώπισης τέτοιων επιθέσεων. (Kamal κ.α., 2021)

2.3.2 Στο δίκτυο VANET

Το δίκτυο VANET μπορεί να δεχθεί πολλές μορφές επιθέσεων. Γι' αυτό το λόγο έχουν αναπτυχθεί αρκετοί τρόποι αντιμετώπισης των επιθέσεων. Ένας από αυτούς είναι η χρήση διάφορων αλγορίθμων κρυπτογράφησης όπως η υποδομή δημοσίου κλειδιού οχημάτων (VPKI). Σύμφωνα με αυτόν τον αλγόριθμο το όχημα αποστολέας πρέπει να κρυπτογραφήσει με το ιδιωτικό κλειδί το μήνυμα. Το όχημα παραλήπτης θα αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί. Έτσι, πιστοποιείται η αυθεντικότητα του απεσταλμένου μηνύματος. Άλλοι αλγόριθμοι κρυπτογράφησης που μπορούν να χρησιμοποιηθούν είναι η συμμετρική κρυπτογράφηση, η υβριδική κρυπτογράφηση και η

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

μέθοδος ομαδικού κλειδιού στην οποία χρησιμοποιείται ένα προσωρινό κλειδί για κάθε session. Το κλειδί αυτό προκύπτει από το κύριο κλειδί.

Ένας άλλος τρόπος είναι η ανίχνευση κακόβουλου λογισμικού. Αυτό μπορεί να γίνει είτε με βάση την υπογραφή, όπου αναλύοντας το κακόβουλο λογισμικό παράγεται μία υπογραφή η οποία χρησιμοποιείται για τον μετέπειτα εντοπισμό του, είτε με βάση την συμπεριφορά όπου παρατηρώντας την συμπεριφορά του συστήματος οι αλγόριθμοι μπορούν να εντοπίσουν την μη φυσιολογική συμπεριφορά που προκαλείται λόγω της επίθεσης. Το κακόβουλο λογισμικό μπορεί να εντοπιστεί και με την χρήση υπηρεσιών cloud. Μέσω του cloud εντοπίζεται το κακόβουλο λογισμικό, γίνεται ανάλυση του και τα αποτελέσματα παρέχονται στο όχημα. Αυτό χρησιμοποιείται κυρίως για να μειωθεί ο φόρτος εργασίας από τις μονάδες RSU. Τέτοιου είδους αλγόριθμοι χρησιμοποιούνται συχνά στους τομείς της μηχανικής μάθησης και της εξόρυξης δεδομένων.

Υπάρχουν πολλοί ακόμη τρόποι προστασίας από τις επιθέσεις στο δίκτυο VANET. Ένας από αυτούς είναι το πρωτόκολλο κατά των επιθέσεων replay. Σε αυτό το πρωτόκολλο το μήνυμα που λαμβάνεται, στέλνεται στην RSU για έλεγχο ορθότητας και για τον εντοπισμό του κακόβουλου αποστολέα. Μία άλλη μέθοδος είναι η μέθοδος Robust για επιθέσεις Sybil (RobSAD). Σε αυτή αναγνωρίζονται οι κόμβοι Sybil μέσω της ολόιδιας οδηγικής συμπεριφοράς, καθώς δύο ή περισσότερα άτομα δεν μπορούν να έχουν ολόιδια οδηγική συμπεριφορά. Παρόλο που υπάρχουν όλοι αυτοί οι τρόποι προστασίας οι επιθέσεις εξακολουθούν να υφίστανται και γι’ αυτό είναι αναγκαίο να συνεχιστεί η έρευνα ώστε να βρεθούν και νέοι τρόποι προστασίας. (Talib κ.α., 2018)

Επιπλέον, μία πολύ συχνή μορφή επίθεσης των αυτόνομων οχημάτων αποτελούν οι επιθέσεις Adversarial Attack. Λόγω αυτού έχουν ανακαλυφθεί διάφοροι μηχανισμοί άμυνας. Τρεις κύριοι μηχανισμοί είναι οι εξής:

1. *Τροποποίηση δεδομένων:* Η μέθοδος αυτή αποτελείται από τρία είδη τροποποίησης τα οποία αφορούν είτε τα δεδομένα εκπαίδευσης είτε τα χαρακτηριστικά τους.
    a. *Feature Denoising*
    b. *Input Transformation*
    c. *Adversarial Training*
2. *Προσθήκη μοντέλου:* Η μέθοδος αυτή στοχεύει στην αύξηση των μοντέλων ώστε το μοντέλο στόχος να είναι πιο ανθεκτικό στις adversarial επιθέσεις. Αυτό επιτυγχάνεται με δύο τρόπους:

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

a. *Ανίχνευση Adversarial*
b. *Αλγόριθμοι συνόλου*

3. *Τροποποίηση μοντέλου:* Η μέθοδος αυτή αποτελείται από τεχνικές που τροποποιούν είτε τις παραμέτρους είτε τα χαρακτηριστικά κάθε μοντέλου.
    a. *Gradient Hiding*
    b. *Defensive Distillation*
    c. *Network Verification* (Kloukiniotis κ.α., 2022)

Άλλη μία σημαντική μορφή επιθέσεων στα αυτόνομα οχήματα είναι οι επιθέσεις στην ανίχνευση αντικειμένων. Για την αντιμετώπιση αυτών των επιθέσεων, πολλοί επιστήμονες ασχολούνται ερευνητικά με το θέμα και προτείνουν διάφορους τρόπους αντιμετώπισης. Ένας τέτοιος τρόπος είναι η εκπαίδευση με στοιχεία επιθέσεων. Στόχος αυτού είναι η χρήση των εικόνων που έχουν υποστεί διαταραχές για την εκπαίδευση του δικτύου. Σύμφωνα με τους Zhang et al. η μέθοδος αυτή επέφερε θετικά αποτελέσματα σε όλα τα σύνολα δεδομένων που χρησιμοποίησαν.

Ένας άλλος τρόπος αντιμετώπισης είναι η συμπίεση JPG. Με την χρήση αυτής της μεθόδου φαίνεται πως μειώνοντας τα δεδομένα των εικόνων, δηλαδή συμπιέζοντας τες, μειώνονται οι επιθέσεις. Αυτό συμβαίνει διότι εξαλείφεται η ικανότητα ανίχνευσης των μοντέλων DNN από τους επιτιθέμενους. Σύμφωνα με τους Amirkhami et al. οι περισσότερες εικόνες στα σύνολα δεδομένων βρίσκονται σε μορφή JPG. Έτσι, συμπιέζοντας τες και διενεργώντας επιθέσεις της μορφής FGSM απέδειξαν ότι η τεχνική της συμπίεσης απέτρεψε σημαντικά την απώλεια της ακρίβειας ταξινόμησης. Ωστόσο, η υπερβολική συμπίεση των εικόνων μειώνει την απόδοση των νευρωνικών δικτύων. (Amirkhami κ.α., 2022)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

3 Μελέτη επιπτώσεων Spoofing επιθέσεων παρουσία ενός Spoofer

Τα Connected and Autonomous Vehicles είναι εξοπλισμένα με τεχνολογίες αιχμής όπως κάμερες, αισθητήρες και άλλες έξυπνες συσκευές για παρακολούθηση, μετάδοση και λήψη πληροφοριών. Αυτά αποθηκεύουν προσωπικά δεδομένα όπως μηνύματα, οικονομικές πληροφορίες κ.α. Γι' αυτό το λόγο διάφοροι κακόβουλοι προσπαθούν να αποκτήσουν απομακρυσμένη πρόσβαση στις αποθηκευμένες πληροφορίες και να τις κλέψουν. Τα CAV είναι ευάλωτα σε διάφορους τύπους κυβερνοεπιθέσεων. Μία από τις πιο σημαντικές κατηγορίες είναι οι επιθέσεις DoS. Υποκατηγορία αυτών των επιθέσεων αποτελούν οι επιθέσεις πλαστογράφησης (Spoofing). Το συγκεκριμένο κεφάλαιο παρουσιάζει μια σε βάθος ανάλυση του αντίκτυπου των επιθέσεων spoofing υπό ρεαλιστικές κυκλοφοριακές συνθήκες που μπορεί να προκαλέσει κυκλοφοριακή συμφόρηση και πιθανό ανεπιθύμητο ατύχημα.

3.1 Τοπολογία

Το κεφάλαιο αυτό προσομοιώνει ένα πραγματικό μοντέλο κυκλοφορίας, σε συνθήκες κίνησης μιας σχετικά μικρής πόλης, όπως το Erlangen, στη Γερμανία. Για το λόγο αυτό, υποθέτουμε ότι κάθε νέο όχημα προστίθεται με σχετικά γρήγορο ρυθμό, εντός του περιβάλλοντος προσομοίωσης, ο οποίος είναι R = 1/3 vehicle/sec. Τα οχήματα ξεκινούν τη διαδρομή τους από το πανεπιστήμιο της πόλης και κατευθύνονται προς τον ίδιο τελικό προορισμό, όπως φαίνεται στην Εικόνα 3. Αυτά αποτελούν μια διμοιρία (platoon) οχημάτων, για την οποία υποθέτουμε ότι το μοντέλο κίνησης είναι το γνωστό μοντέλο Gipps. Αυτό ακολουθεί το πρότυπο του collision-free car-following μοντέλου (Sun κ.α., 2022).

Στο πλαίσιο του μοντέλου Gipps, η ασφαλής ταχύτητα (safe speed) αναφέρεται στη μέγιστη ταχύτητα που μπορεί να αναπτύξει ένα όχημα ανά πάσα στιγμή διασφαλίζοντας ότι μπορεί να σταματήσει με ασφάλεια πριν φτάσει στο προπορευόμενο όχημα (Gipps, 1981; Treiber & Kesting, 2013). Σε αυτήν την ταχύτητα λαμβάνεται υπόψη ο χρόνος αντίδρασης του οδηγού, οι δυνατότητες επιβράδυνσης τόσο του προπορευόμενου όσο και του επόμενου οχήματος αλλά και η τρέχουσα ταχύτητα και θέση των οχημάτων. Η

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ασφαλής ταχύτητα στο μοντέλο Gipps επηρεάζεται από παραμέτρους όπως η μέγιστη επιτάχυνση, ο χρόνος αντίδρασης, η επιθυμητή ταχύτητα και ελάχιστη απόσταση μεταξύ των οχημάτων.

Εικόνα 3: Η διαδρομή των οχημάτων από την αφετηρία έως τον προορισμό [29]

Οι τιμές για αυτές τις παραμέτρους επιλέχθηκαν με βάση το γεγονός ότι η κυκλοφορία γίνεται σε αστικό περιβάλλον, όπου υπάρχουν συχνές στάσεις, διασταυρώσεις και πεζοί. Ο Πίνακας 2 παρουσιάζει όλες αυτές τις παραμέτρους. Συγκεκριμένα, η ελάχιστη απόσταση ορίζεται περίπου από 2,0 έως 5,0 m για αστικά περιβάλλοντα. Επομένως, επιλέγουμε τη μέση τιμή περίπου 2,5 m. Η απόσταση ασφαλείας στο μοντέλο Gipps είναι η ελάχιστη απόσταση που πρέπει να τηρείται μεταξύ ενός οχήματος και του προπορευόμενου οχήματος ώστε να αποτραπεί μια σύγκρουση. Σε αυτό λαμβάνονται υπόψη οι τρέχουσες ταχύτητες και οι δυνατότητες επιβράδυνσης των οχημάτων. Αυτή η απόσταση διασφαλίζει ότι εάν το προπορευόμενο όχημα επιβραδύνει ξαφνικά, το επόμενο όχημα μπορεί να σταματήσει εγκαίρως ώστε να αποφευχθεί μια σύγκρουση. Σύμφωνα με τα παραπάνω, ένα όχημα πρέπει να κινείται με ταχύτητα περίπου 40–50 km/h, έτσι ώστε να διατηρείται συνεχώς μια ελάχιστη απόσταση ασφαλείας περίπου 30–50 m, ακόμη και αν το προπορευόμενο όχημα σταματήσει απότομα λόγω ενός απροσδόκητου γεγονότος που μπορεί να συμβεί στο δρόμο.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Πίνακας 2: Παράμετροι προσομοίωσης [29]

Evaluation Parameters in Veins Simulator	Normal Scenario	Spoofing Attack Scenario
Number of Lanes	one per direction	one per direction
Row	1	1
RSU	1	1
Total Simulation Time	120 s	120 s
Duration of Attack	0 s	110 s
Range of Vehicles (vehicles/km)	10, 15, 20, 25	10, 15, 20, 25
Desired Speed	50 m/s	50 m/s
Maximum Acceleration	6.0 m/s^2	6.0 m/s^2
Maximum Deceleration	7.5 m/s^2	7.5 m/s^2
Reaction Time	1.0 to 1.5 s	1.0 to 1.5 s
Vehicle Length	2	2
Minimum Gap	2.5 m	2.5 m
Victim	0	1 (Node 1)
Spoofing Attackers	0	1

Όλα τα μέλη της διμοιρίας είναι εξοπλισμένα με ραντάρ τα οποία έχουν κατεύθυνση προς τα εμπρός και προς τα πίσω ώστε να εντοπίζουν τα εμπόδια που υπάρχουν γύρω τους. Όλα τα οχήματα της διμοιρίας στέλνουν περιοδικά WSM μηνύματα, με την μέθοδο unicast στα υπόλοιπα οχήματα, τα οποία περιέχουν πληροφορίες που σχετίζονται με την κίνηση όπως η θέση, η ταχύτητα, η επιτάχυνση κ.α. Επίσης, στην περιοχή υπάρχει ένα RSU που αναμεταδίδει τα μηνύματα WSM που ανταλλάσσονται. Ωστόσο, εάν τα πρώτα οχήματα της διμοιρίας εντοπίσουν οποιαδήποτε κυκλοφοριακή διαταραχή, δηλαδή ατύχημα μεταξύ οχημάτων ή ατυχήματα μεταξύ οχημάτων και πεζών, ενδέχεται να αλλάξουν τη διαδρομή τους, σε πραγματικό χρόνο, προκειμένου να φτάσουν στον προορισμό τους πιο γρήγορα. Έτσι, για να διασφαλιστεί η ασφάλεια στο δρόμο που κινούνται τα αυτόνομα οχήματα πρέπει να χρησιμοποιηθούν λύσεις σχετικά με τους αισθητήρες για τον υπολογισμό της θέσης των οχημάτων βασιζόμενοι σε ασύρματες τεχνολογίες V2V. Για το σκοπό αυτό, σε αυτές τις τεχνολογίες, είναι πολύ σημαντικό τα δεδομένα που ανταλλάσσονται να προστατεύονται και να διασφαλίζεται η ακεραιότητά τους. (Tzoannos κ.α., 2024)

3.2 Επιθέσεις Spoofing

Σε αυτό το κεφάλαιο παρουσιάζονται διάφορα σενάρια για την αξιολόγηση του αντίκτυπου μιας σημαντικής επίθεσης DoS, όπως είναι η επίθεση spoofing, υπό ρεαλιστικές συνθήκες κυκλοφορίας και για τη διαμόρφωση κατάλληλων στρατηγικών μετριασμού αυτών των επιθέσεων. Μια αντιπροσωπευτική κατηγορία επιθέσεων spoofing σε μία διμοιρία

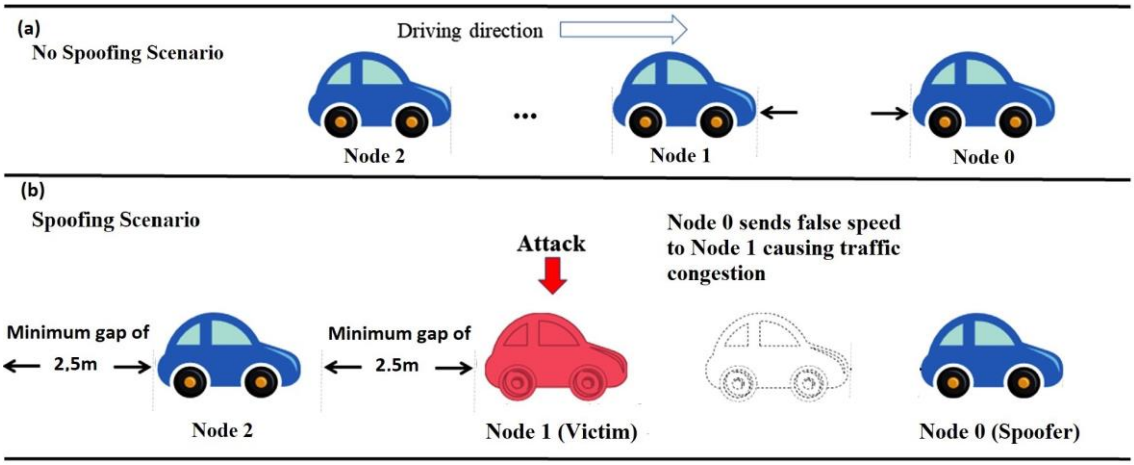
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

οχημάτων αποτελούν οι επιθέσεις που προκαλούνται από μη μέλη της διμοιρίας. Σύμφωνα με πρόσφατη βιβλιογραφία, προτείνονται λύσεις σχετικά με τα πρωτόκολλα ασφαλούς διαχείρισης στην προσθήκη νέων οχημάτων σε μία διμοιρία. Επομένως, οποιαδήποτε εξωτερική επικοινωνία με τα μέλη της διμοιρίας φιλτράρεται, ενώ εξετάζεται και η ασφάλεια της εσωτερικής τους επικοινωνίας. (Kloukiniotis κ.α., 2022). Όπως προαναφέρθηκε, στα σενάρια αυτού του κεφαλαίου, η διμοιρία οχημάτων δημιουργείται με adhoc τρόπο, σε συνθήκες πραγματικού χρόνου, με βάση χαρακτηριστικά της κίνησης των οχημάτων όπως εάν κινούνται στον ίδιο δρόμο με την ίδια ταχύτητα κ.α. Επιπλέον υποθέτουμε ότι ένας κόμβος εντός της διμοιρίας μπορεί να λειτουργεί ως επιτιθέμενος είτε λόγω επηρεασμού του από κακόβουλα λογισμικά είτε διότι ενεργεί για προσωπικό συμφέρον. Αυτό επιτυγχάνεται μέσω της διάδοσης παραπλανητικών δεδομένων π.χ. τροποποιημένων WSM μηνυμάτων σε άλλα μέλη της διμοιρίας. Τα οχήματα αντιλαμβάνονται αυτές τις πληροφορίες ως ακριβείς και δέχονται επίθεση.

Στα σενάρια προσομοίωσης, όλα τα οχήματα έχουν εγκατεστημένη μια κάρτα δικτύου χρησιμοποιώντας το πρότυπο IEEE 802.11p, το οποίο υποστηρίζει την ασύρματη πρόσβαση σε περιβάλλοντα οχημάτων (WAVE) (IEEE, 2019). Το πρότυπο αυτό αξιοποιεί τη συχνότητα 5,9 GHz για να διευκολύνει την επικοινωνία μεταξύ όλων των κινούμενων οχημάτων (V2V) εντός του διαθέσιμου εύρους επικοινωνίας, την επικοινωνία Vehicle to Infrastructure (V2I) καθώς και την επικοινωνία μεταξύ των οχημάτων και της RSU. Συγκεκριμένα, το σενάριο της επίθεσης spoofing προϋποθέτει ότι η διμοιρία των οχημάτων κινείται γύρω από την πόλη Erlangen, στις καθορισμένες διαδρομές, σύμφωνα με την Εικόνα 3.

Ξεκινώντας από το 10ο δευτερόλεπτο της προσομοίωσης, το πρώτο όχημα της διμοιρίας (Node 0: spoofer–επιτιθέμενος) αρχίζει να παραποιεί τις παραμέτρους ενός WSM μηνύματος, ιδίως της ταχύτητας, εκχωρώντας μια τυχαία τιμή που προκύπτει από μια ομοιόμορφη κατανομή, εντός του εύρους των (0,1, 0,9). Παρά τις αλλαγές, αυτό το όχημα συνεχίζει κατά μήκος της σχεδιασμένης διαδρομής του χωρίς καμία απόκλιση. Στη συνέχεια, ο Node 1 (victim–θύμα), μόλις λάβει αυτό το μήνυμα, ρυθμίζει την ταχύτητά του σε μια τιμή που προέρχεται από ομοιόμορφη κατανομή με τιμές στο σύνολο (0,1, 0,9). Αυτό δημιουργεί κυκλοφοριακή συμφόρηση, με τα μέλη της διμοιρίας που ακολουθούν να σχηματίζουν μια ουρά στην ελάχιστη απόσταση των 2,5 m, όπως φαίνεται στην Εικόνα 4.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

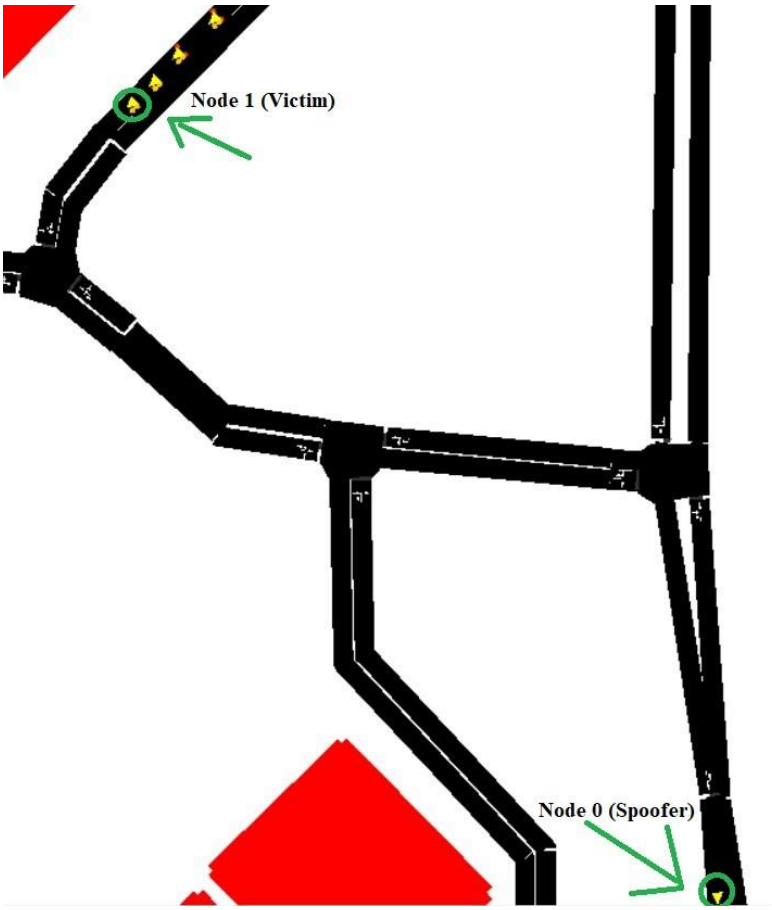


Εικόνα 4: (α): Η διμοιρία των οχημάτων υπό κανονικές συνθήκες,
(β): η διμοιρία των οχημάτων υπό επίθεση spoofing [29]

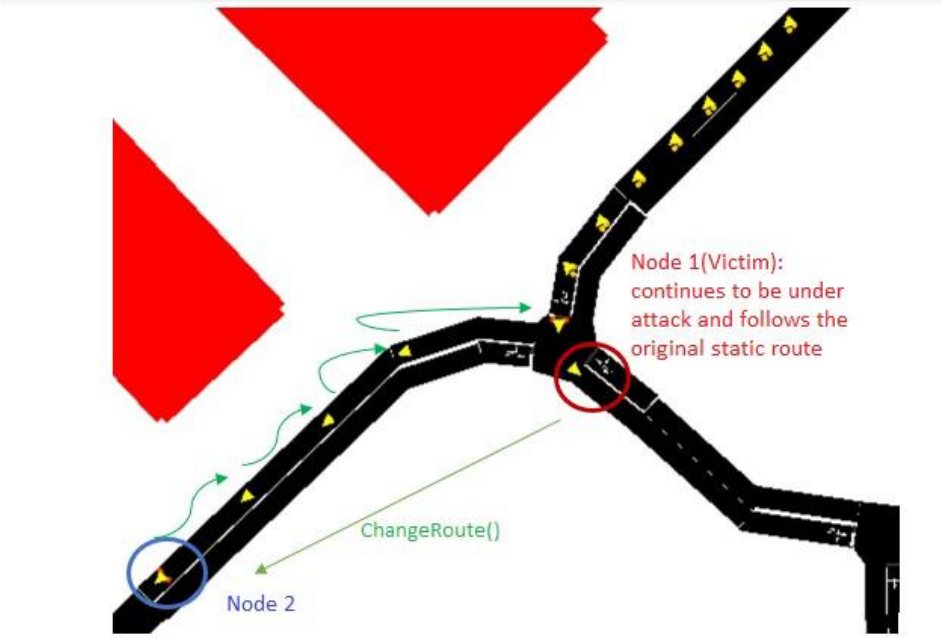
Αυτό συμβαίνει διότι, κατά τη διάρκεια της επίθεσης, τα οχήματα κινούνται σε δρόμο διπλής κατεύθυνσης με μία λωρίδα κυκλοφορίας ανά κατεύθυνση. Επομένως, τα οχήματα που ακολουθούν δεν μπορούν να προσπεράσουν τον Node 1 (θύμα). Γύρω στο 85ο δευτερόλεπτο της προσομοίωσης, η διμοιρία οχημάτων φτάνει σε μία διασταύρωση. Αυτό σημαίνει ότι η διάρκεια της επίθεσης spoofing είναι περίπου 75 δευτερόλεπτα. Υποθέτουμε ότι κάθε κόμβος της διμοιρίας εκτελεί ένα εξαιρετικά προστατευμένο κομμάτι κώδικα, σύμφωνα με το οποίο εάν ένα όχημα παραμείνει σταματημένο για ένα εύλογο διάστημα 10 δευτερολέπτων, θα ειδοποιήσει τα ακόλουθα οχήματα ώστε να αλλάξουν πορεία με σκοπό να φτάσουν στον προορισμό τους.

Στη συνέχεια, τα οχήματα που ακολουθούν μετά από τον κόμβο θύμα αποσπώνται από τη διμοιρία, αν έχουν την επιλογή, ώστε να «ξεπεράσουν» το εμπόδιο του Node 1 και να συνεχίσουν ανεμπόδιστα τη διαδρομή τους. Η περιγραφή αυτής της επίθεσης απεικονίζεται από την Εικόνα 5 και την Εικόνα 6. Όπως ήδη αναφέρθηκε, κατά την κίνηση της διμοιρίας, τα οχήματα ανταλλάσσουν WSM μηνύματα που περιέχουν διάφορες πληροφορίες, για την ταχύτητά τους, την επιτάχυνσή τους και την θέση τους. Σύμφωνα με τις τιμές των WSM μηνυμάτων, εξάγουμε έναν αριθμό μετρήσεων για να εξετάσουμε τις συνέπειες της επίθεσης spoofing. Αυτές αναφέρονται στη συνολική απόσταση που διανύθηκε, στο ποσοστό PDR των WSM μηνυμάτων για κάθε όχημα, καθώς και στον χρόνο καθυστέρησης των οχημάτων που παραμένουν στην ουρά λόγω της επίθεσης. (Tzoannos κ.α., 2024)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Εικόνα 5: Οι κόμβοι δημιουργούν μία ουρά οχημάτων με σχεδόν μηδενική ταχύτητα λόγω της επίθεσης spoofing ενώ ο Node 0 (Spoofer) συνεχίζει κανονικά τη διαδρομή του [29]



Εικόνα 6: Στην διασταύρωση τα οχήματα από το Node 2 και μετά διαχωρίζονται δυναμικά από την επιρροή του Node 1 και συνεχίζουν την πορεία τους σε εναλλακτική διαδρομή. Με πράσινο χρώμα φαίνεται η ειδοποίηση των κόμβων για το “ChangeRoute()” [29]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

3.3 Αξιολόγηση απόδοσης μοντέλου

Για την αξιολόγηση της απόδοσης του μοντέλου επίθεσης spoofing, γίνεται χρήση των λογισμικών OMNeT++ 5.6.2, INET 3.6, Veins 4.7 και SUMO 0.30.0 (C. Sommer, R. German & F. Dressler, 2011). Σε αυτό το μοντέλο προσομοιώνουμε και συγκρίνουμε δύο σενάρια. Το πρώτο το ονομάζουμε Κανονικό Σενάριο (Normal Scenario), όπου τα οχήματα κινούνται υπό κανονικές συνθήκες στους δρόμους της πόλης, χωρίς την παρουσία κάποιου επιτιθέμενου. Στο δεύτερο σενάριο, το οποίο ονομάζεται Spoofing Attack Scenario, γίνεται μία επίθεση πλαστογράφησης (Spoofing) με διαφορετικές τυχαίες αλλά διακριτές τιμές οχημάτων σε μία αστική περιοχή. Οι τιμές αυτές είναι n = 10, 15, 20, 25. Ο Πίνακας 2 περιγράφει όλες τις παραμέτρους της προσομοίωσης που εφαρμόστηκαν για την πραγματοποίηση της επίθεσης Spoofing.

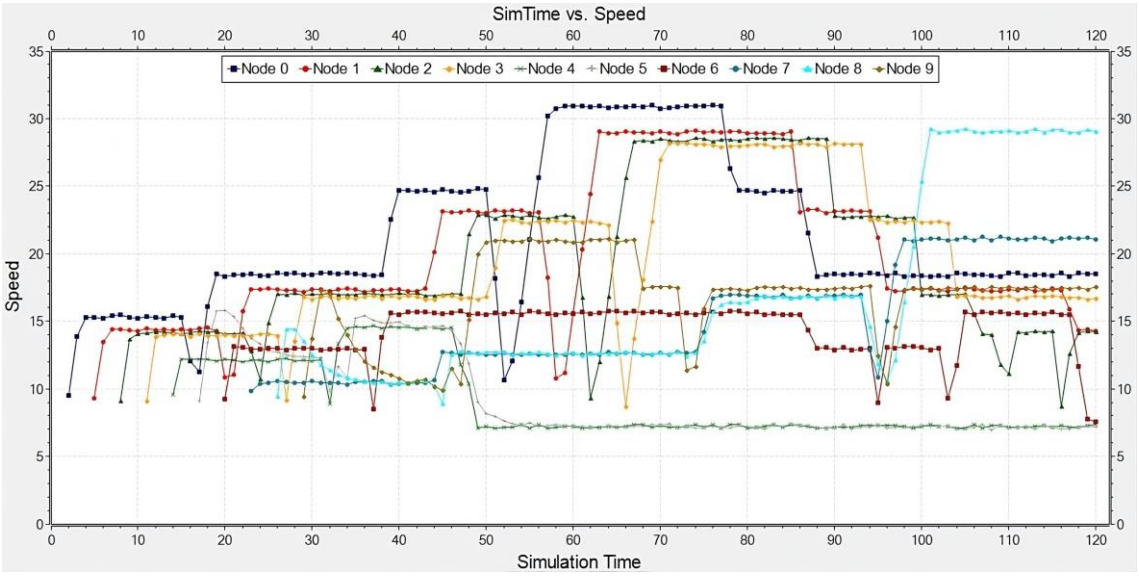
Τα αποτελέσματα της επίθεσης πλαστογράφησης στην κίνηση της διμοιρίας παρουσιάζονται από τα παρακάτω πειράματα. Σε αυτά η ταχύτητα και η επιτάχυνση συγκρίνονται για τα δύο όρια της τιμής n των οχημάτων, δηλαδή για 10 και για 25 vehicles/km. Η Εικόνα 7, η Εικόνα 8, η Εικόνα 9 και η Εικόνα 10 παρουσιάζουν την ταχύτητα και την επιτάχυνση για μια διμοιρία οχημάτων μεγέθους 10. Ενώ, η Εικόνα 11, η Εικόνα 12, η Εικόνα 13 και η Εικόνα 14 παρουσιάζουν την ταχύτητα και την επιτάχυνση για μια διμοιρία οχημάτων μεγέθους 25.

Η πλειονότητα των δημοσιευμένων ερευνητικών εργασιών χρησιμοποιεί μετρικές για την μεταβλητότητα της οδήγησης ως κυρίαρχο μέτρο ασφάλειας για την αξιολόγηση της διακύμανσης της συμπεριφοράς των CAV (Wang et al., 2015). Όλες οι παραλλαγές στην συμπεριφορά των CAV, όπως οι απότομες διακυμάνσεις στους παράγοντες κίνησης π.χ. η επιτάχυνση, η επιβράδυνση και η ταχύτητα, εκφράζονται μέσω της μεταβλητότητας (volatility). Ο όρος volatility εκφράζει την ισορροπία μεταξύ των κινδύνων ασφαλείας και της μειωμένης άνεσης. Ως εκ τούτου, η μέτρηση της μεταβλητότητας είναι ένας δείκτης για μία μελλοντική σύγκρουση. Η μέτρηση της μεταβλητότητας σύμφωνα με τους Khattak et al. περιγράφεται από την εξίσωση CoV, η οποία δίνεται από τον λόγο της τυπικής απόκλισης του διανύσματος της ταχύτητας ή της επιτάχυνσης προς το μέσο όρο του ίδιου διανύσματος. Αυτό φαίνεται στην Εξίσωση 1, όπου η τυπική απόκλιση αντιπροσωπεύεται από S.D και ο μέσος όρος της ταχύτητας και της επιτάχυνσης-επιβράδυνσης αντιπροσωπεύεται από $\hat{y}$.

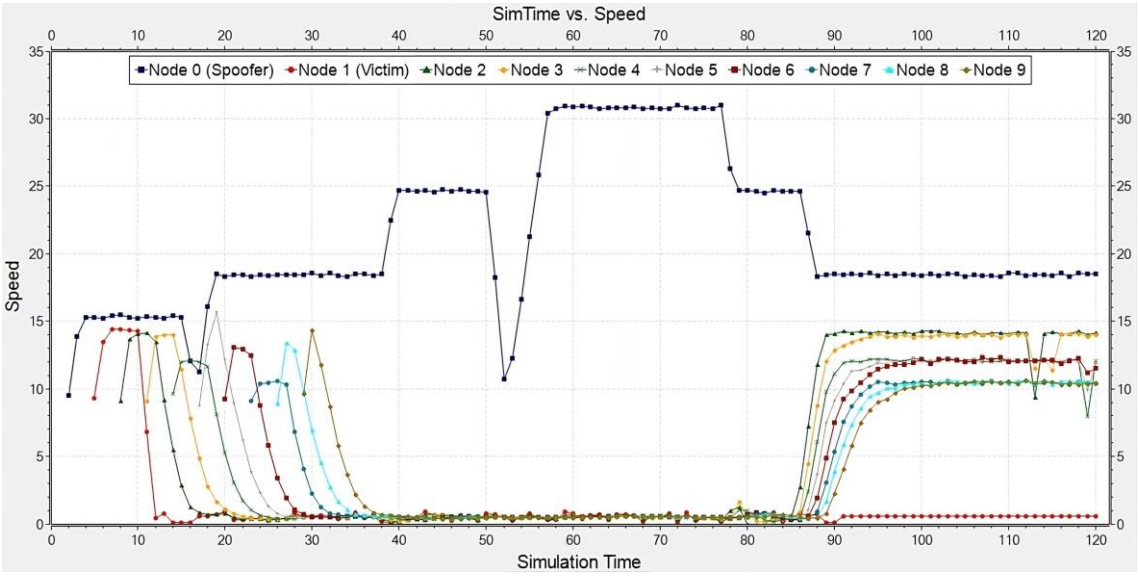
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Εξίσωση 1: Ορισμός του Coefficient of Variation (CoV)

$$CoV = \frac{S.D}{\hat{y}}$$

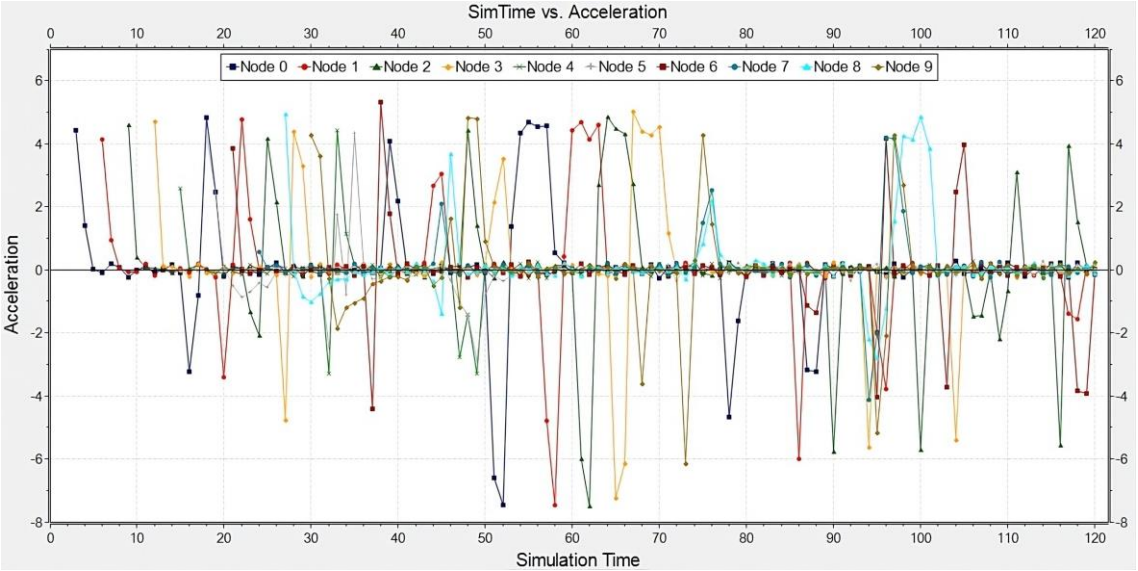


Εικόνα 7: Η ταχύτητα των οχημάτων του platoon για 10 vehicles/km στο κανονικό σενάριο [29]

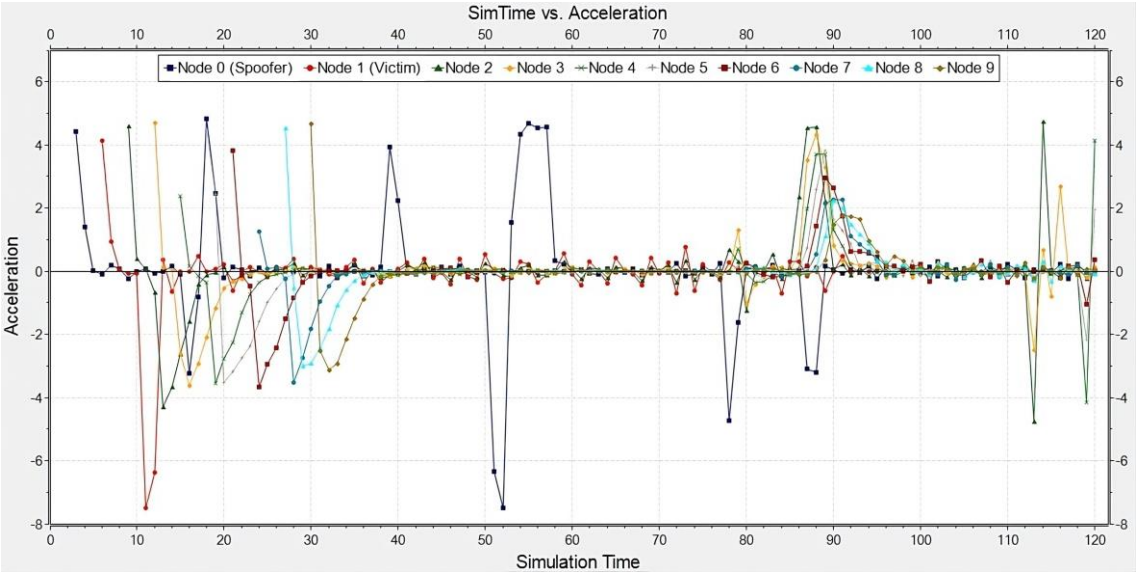


Εικόνα 8: Η ταχύτητα των οχημάτων του platoon για 10 vehicles/km στο σενάριο επίθεσης Spoofing [29]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

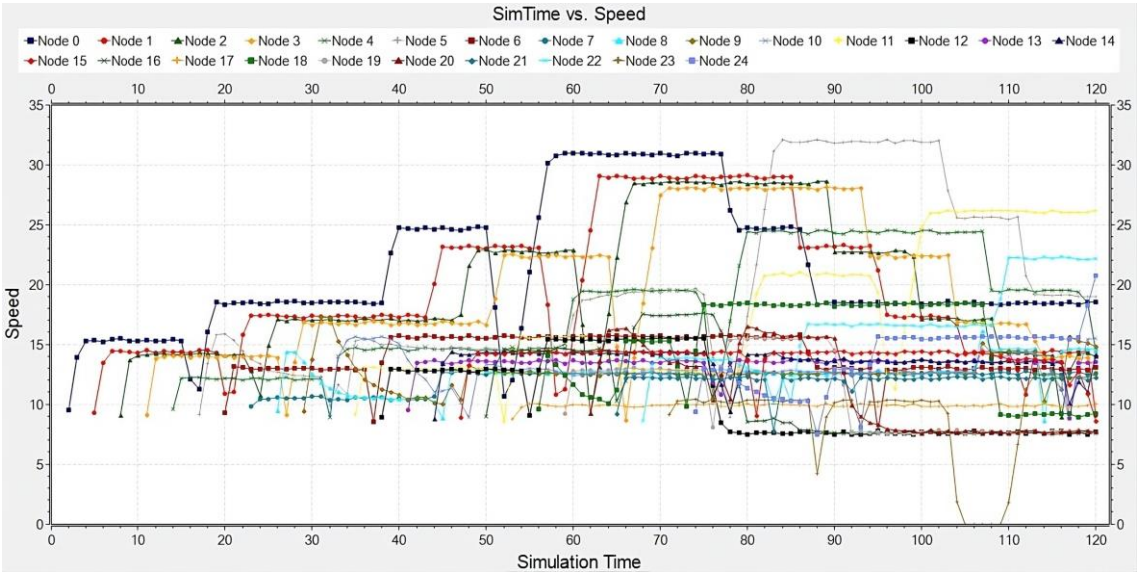


Εικόνα 9: Η επιτάχυνση των οχημάτων του platoon για 10 vehicles/km στο κανονικό σενάριο [29]

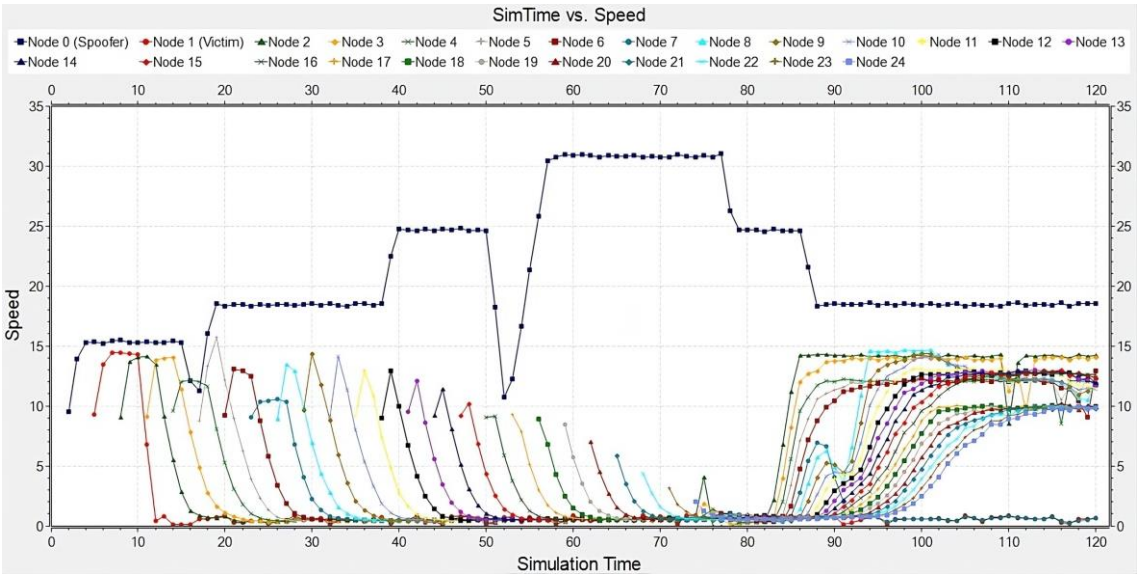


Εικόνα 10: Η επιτάχυνση των οχημάτων του platoon για 10 vehicles/km στο σενάριο επίθεσης Spoofing [29]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

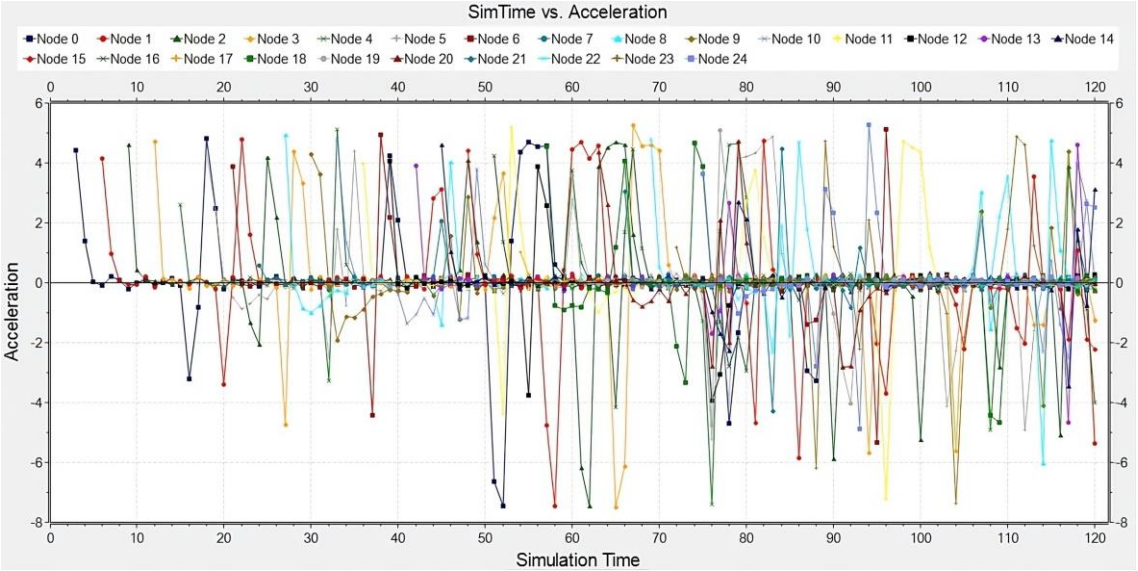


Εικόνα 11: Η ταχύτητα των οχημάτων του platoon για 25 vehicles/km στο κανονικό σενάριο [29]

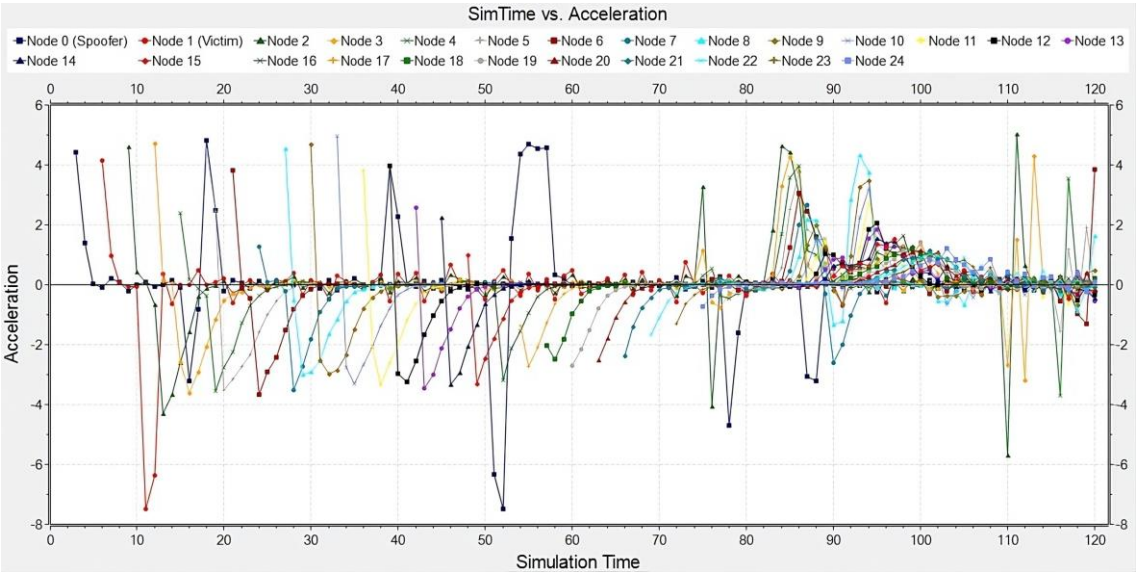


Εικόνα 12: Η ταχύτητα των οχημάτων του platoon για 25 vehicles/km στο σενάριο επίθεσης Spoofing [29]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Εικόνα 13: Η επιτάχυνση των οχημάτων του platoon για 25 vehicles/km στο κανονικό σενάριο [29]



Εικόνα 14: Η επιτάχυνση των οχημάτων του platoon για 25 vehicles/km στο σενάριο επίθεσης Spoofing [29]

Ακόμη, διεξήχθη στατιστική ανάλυση των παραπάνω αποτελεσμάτων, για 120 sec. όσο και ο συνολικός χρόνος των παρατηρήσεων. Δηλαδή, λήφθηκε μία τιμή για κάθε 1sec. από τα συνολικά 120 sec. του χρόνου προσομοίωσης. Μέσω αυτής της ανάλυσης παρατηρούνται οι τιμές της εξίσωσης CoV για την επιτάχυνση στο εύρος τιμών οχημάτων 10, 15, 20, 25 vehicles/km. Αυτό περιγράφει ο Πίνακας 3. Ενώ ο Πίνακας 4 δείχνει τις τιμές CoV για την ταχύτητα εντός του ίδιου εύρους οχημάτων/χλμ. Το βασικό συμπέρασμα που εξάγεται όσον αφορά τη μέτρηση που βασίζεται στη μεταβλητότητα είναι ότι, υπό την επίθεση πλαστογράφησης, η CoV της ταχύτητας αυξάνεται κατά περίπου 12,1%,

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

καθώς και η απόλυτη τιμή της επιτάχυνσης CoV, αλλά σε μικρότερη έκταση. Αυτό οφείλεται στο γεγονός ότι, κατά τη διάρκεια της επίθεσης πλαστογράφησης, το όχημα-θύμα και όσα βρίσκονται πίσω από αυτό επιβραδύνουν απότομα, με αποτέλεσμα να έχουν αρνητική μέση τιμή επιτάχυνσης και οι διακυμάνσεις στις τιμές επιβράδυνσης να είναι σημαντικά υψηλότερες σε σύγκριση με τις τιμές επιτάχυνσης. Αυτό υποδηλώνει επίσης αυξημένο κίνδυνο συγκρούσεων στο πίσω μέρος της διμοιρίας. Τέλος, για το εύρος οχημάτων, οι συντελεστές παραμένουν σταθεροί, γεγονός που οφείλεται στο ότι το εύρος είναι αρκετά περιορισμένο.

Πίνακας 3: Τιμές CoV για την επιτάχυνση [29]

Kind of Attack	Density of 10 vehicles/km	Density of 15 vehicles/km	Density of 20 vehicles/km	Density of 25 vehicles/km
Normal Scenario	664.9341	678.5202	679.1850	679.1850
Spoofing Attack Scenario	−682.9962	−678.0775	−680.5207	−694.6582

Πίνακας 4: Τιμές CoV για την ταχύτητα [29]

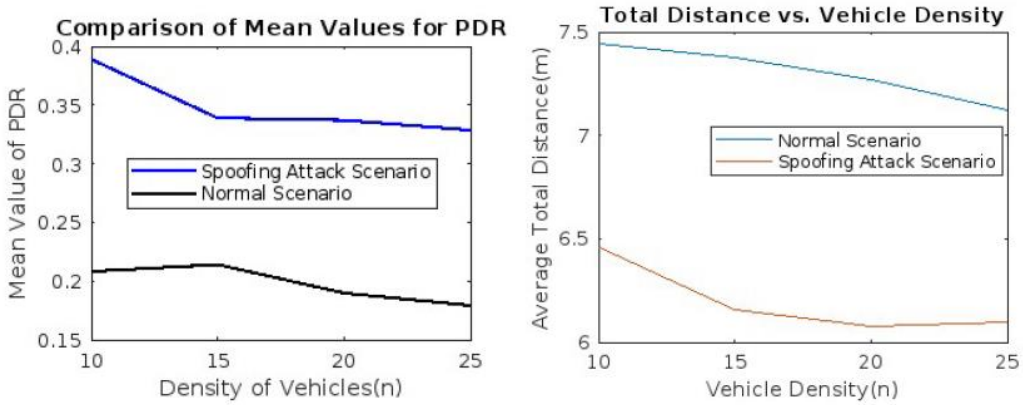
Kind of Attack	Density of 10 vehicles/km	Density of 15 vehicles/km	Density of 20 vehicles/km	Density of 25 vehicles/km
Normal Scenario	23.4126	23.5272	23.5172	23.5172
Spoofing Attack Scenario	190.6639	191.2707	190.8419	190.8157

Η Εικόνα 15 απεικονίζει τη σύγκριση της μέσης τιμής του PDR για όλα τα οχήματα που υπάρχουν στην περιοχή, στο εύρος τιμών που ορίζει ο Πίνακας 2. Δείχνει επίσης τη μέση συνολική απόσταση που διανύει κάθε όχημα κατά τη διάρκεια της προσομοίωσης σε λογαριθμική κλίμακα, επειδή η διαφορά μεταξύ του κανονικού σεναρίου και του σεναρίου επίθεσης είναι αρκετά μεγάλη. Παρατηρείται ότι τόσο η κατανομή του PDR όσο και η κατανομή της συνολικής απόστασης προσεγγίζουν μια εκθετική κατανομή με πολύ μικρή παράμετρο. Ομοίως, οι κατανομές των ίδιων παραμέτρων για την περίπτωση της επίθεσης πλαστογράφησης προσεγγίζουν τη συνάρτηση αθροιστικής κατανομής (CDF) μιας εκθετικής κατανομής με πολύ μικρή παράμετρο. Επομένως, η επίθεση πλαστογράφησης έχει ως αποτέλεσμα όλα τα οχήματα να ταξιδεύουν μικρότερες αποστάσεις από αυτές που θα διένυαν κανονικά στο ίδιο χρονικό διάστημα, ενώ ταυτόχρονα επηρεάζεται σημαντικά το μέσο ασύρματης μετάδοσης, αυξάνοντας τον αριθμό των πακέτων που μεταδίδουν τα οχήματα.

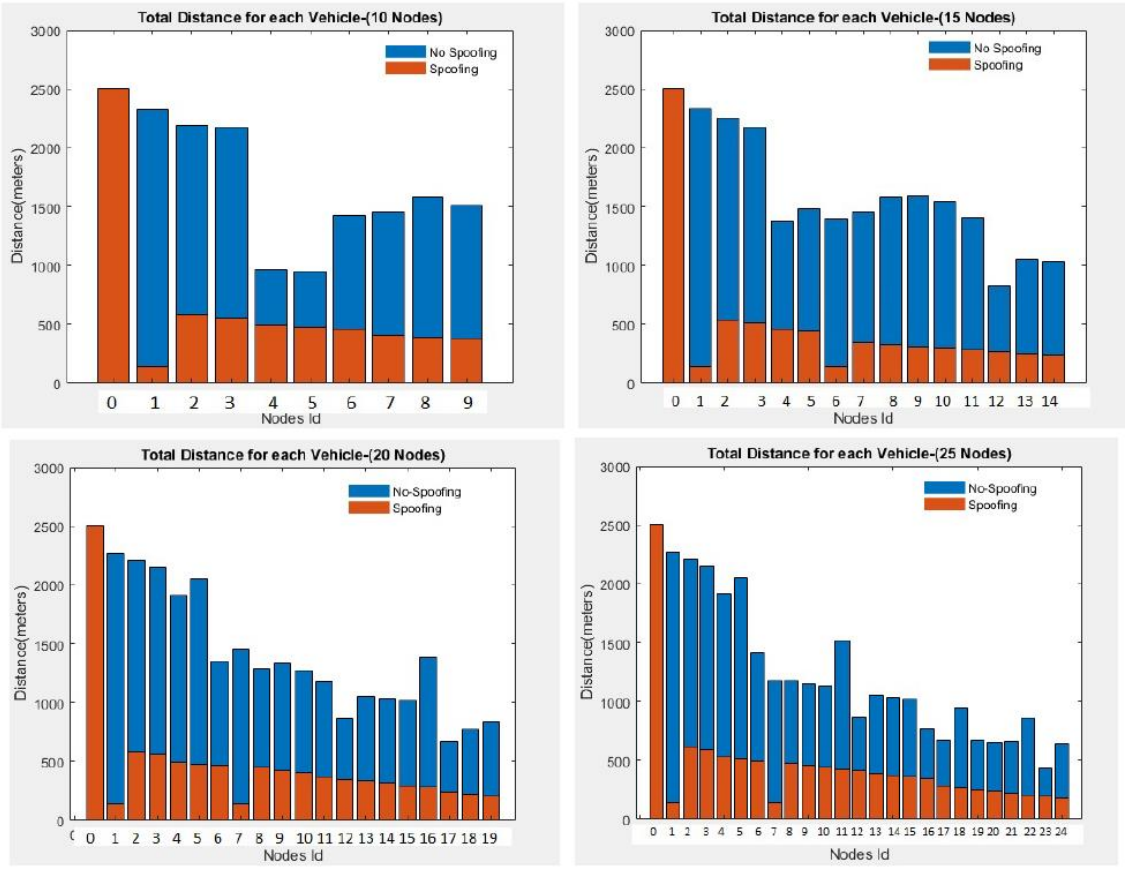
Η Εικόνα 16 απεικονίζει τη συνολική διανυθείσα απόσταση για όλους τους κόμβους με τιμές (n = 10, 15, 20, 25 vehicles/km) σε ένα εύρος από 10 έως 25 οχήματα. Σε αυτή τη σειρά σχημάτων, τα κύρια συμπεράσματα είναι πανομοιότυπα με αυτά που παρουσιάζονται στην Εικόνα 15. Αυτό που είναι ξεκάθαρο είναι ότι η επίθεση spoofing επηρεάζει μόνο τον κόμβο θύματος (Node 1), αναγκάζοντας τον να κινείται με ελάχιστη ταχύτητα

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

για όλη την υπόλοιπη προσομοίωση με τις επιπτώσεις στα ακόλουθα οχήματα να είναι σημαντικές αλλά όχι τόσο μεγάλες. Τέλος, για τις διάφορες τιμές οχημάτων (Vehicle Density), δεν παρατηρείται σημαντική αύξηση της διανυθείσας απόστασης. (Tzoannos κ.α., 2024)



Εικόνα 15: Μέση τιμή του PDR και μέση συνολική διανυθείσα απόσταση για τις διάφορες τιμές οχημάτων [29]



Εικόνα 16: Γραφήματα για την συνολική διανυθείσα απόσταση για όλους τους κόμβους σε όλα τα σενάρια προσομοίωσης [29]

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

3.3.1 Ψευδοκώδικας για το ChangeRoute

Η υποενότητα αυτή παρουσιάζει σε μορφή ψευδοκώδικα την λειτουργία του ChangeRoute. Δηλαδή της διαδικασίας που ακολουθείται όταν ένα όχημα ειδοποιείται ότι στο δρόμο που κινείται υπάρχει ένα εμπόδιο ή έχει συμβεί ένα ατύχημα. Επίσης παρουσιάζεται και η αντίδραση του κόμβου – οχήματος μέσω της αλλαγής διαδρομής. Ακολουθεί ο Πίνακας 5 με επεξήγηση των όρων που χρησιμοποιούνται στον ψευδοκώδικα.

```
INITIALIZE simulation environment
FOR each vehicle:
    Register the vehicle's TraCI handle (traciVehicle)
    Initialize default route

WHEN simulation starts:
    Wait for simulation time to progress

MAIN EVENT LOOP or OMNeT++ handleMessage()
    IF event is vehicle movement or timer tick:
        FOR each vehicle:
            GET current edge ID using traciVehicle->getRoadId()
            GET vehicle position using traciVehicle->getPosition()

            IF vehicle receives alert (e.g., accident ahead)
               AND vehicle is on a route that passes the danger zone
               THEN
                     Find a new edge or alternative path
                     CALL traciVehicle->changeRoute(newEdgeID, simTime())
CONTINUE simulation
```

Πίνακας 5: Επεξήγηση όρων ψευδοκώδικα

Term / Function	Explanation
`TraCI (Traffic Control Interface)`	A runtime API that connects OMNeT++ with SUMO, allowing OMNeT++ to control and monitor traffic simulation in real time.
`traciVehicle`	A TraCI-controlled vehicle object, provides access to the vehicle in SUMO.
`getRoadId()`	Returns the ID of the current **edge** (road segment) the vehicle is on.
`getPosition()`	Returns the current (x, y) coordinates of the vehicle in the SUMO network.
`changeRoute(newEdgeID, simTime())`	Changes the vehicle's route to start with `newEdgeID` at the given simulation time.
`newEdgeID`	The ID of a new edge (road segment) used to reroute the vehicle.
`simTime()`	Gets the current OMNeT++ simulation time, used to time the rerouting.
`handleMessage()`	Main OMNeT++ function called when messages/events are received.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

4 Μελέτη επιπτώσεων Spoofing επιθέσεων παρουσία άνω του ενός Spoofer

Τα Connected and Autonomous Vehicles λόγω της εξελιγμένης τεχνολογίας που διαθέτουν γίνονται στόχοι διάφορων κακόβουλων επιθέσεων. Μία σοβαρή μορφή επίθεσης αποτελούν οι επιθέσεις DoS, υποκατηγορία των οποίων είναι οι επιθέσεις Spoofing. Σε αυτή την κατηγορία, οι επιθέσεις μπορούν να πραγματοποιηθούν είτε από έναν επιτιθέμενο (spoofer) είτε από περισσότερους επιτιθέμενους σε μορφή ενός κατανεμημένου συστήματος. Το παρών κεφάλαιο αποτελεί επέκταση του προηγούμενου κεφαλαίου με την διαφορά ότι στο συγκεκριμένο πραγματοποιούνται επιθέσεις από περισσότερους του ενός spoofer.

4.1 Τοπολογία

Το κεφάλαιο αυτό προσομοιώνει ένα πραγματικό μοντέλο κυκλοφορίας, σε συνθήκες κίνησης μιας σχετικά μικρής πόλης, όπως το Erlangen, στη Γερμανία. Υποθέτουμε ότι κάθε νέο όχημα προστίθεται με σχετικά γρήγορο ρυθμό, εντός του περιβάλλοντος προσομοίωσης, ο οποίος είναι R = 1/3 vehicle/sec. Τα οχήματα ξεκινούν τη διαδρομή τους από το πανεπιστήμιο της πόλης και κατευθύνονται προς τον ίδιο τελικό προορισμό, όπως φαίνεται στην Εικόνα 3. Αυτά αποτελούν μια διμοιρία (platoon) οχημάτων, για την οποία υποθέτουμε ότι το μοντέλο κίνησης είναι το γνωστό μοντέλο Gipps. Αυτό ακολουθεί το πρότυπο του collision-free car-following μοντέλου (Sun κ.α., 2022). Η ασφαλής ταχύτητα στο μοντέλο Gipps επηρεάζεται από παραμέτρους όπως η μέγιστη επιτάχυνση, ο χρόνος αντίδρασης, η επιθυμητή ταχύτητα και ελάχιστη απόσταση μεταξύ των οχημάτων.

Οι τιμές για αυτές τις παραμέτρους επιλέχθηκαν με βάση το γεγονός ότι η κυκλοφορία γίνεται σε αστικό περιβάλλον, όπου υπάρχουν συχνές στάσεις, διασταυρώσεις και πεζοί. Ο Πίνακας 6 παρουσιάζει όλες αυτές τις παραμέτρους. Συγκεκριμένα, η ελάχιστη απόσταση ορίζεται περίπου από 2,0 έως 5,0 m για αστικά περιβάλλοντα. Επομένως, επιλέγουμε τη μέση τιμή περίπου 2,5 m. Η απόσταση ασφαλείας στο μοντέλο Gipps είναι η

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ελάχιστη απόσταση που πρέπει να τηρείται μεταξύ ενός οχήματος και του προπορευόμενου οχήματος ώστε να αποτραπεί μια σύγκρουση. Έτσι, ένα όχημα πρέπει να κινείται με ταχύτητα περίπου 40–50 km/h, ούτως ώστε να διατηρείται συνεχώς μια ελάχιστη απόσταση ασφαλείας περίπου 30–50 m, ακόμη και αν το προπορευόμενο όχημα σταματήσει απότομα λόγω ενός απροσδόκητου γεγονότος που μπορεί να συμβεί στο δρόμο.

Πίνακας 6: Παράμετροι προσομοίωσης

Evaluation Parameters in Veins Simulator	Normal Scenario	Spoofing Attack Scenario
Number of Lanes	one per direction	one per direction
Row	1	1
RSU	1	1
Total Simulation Time	150 s	150 s
Duration of Attack	0 s	110 s
Range of Vehicles (vehicles/km)	10, 15, 20, 25	10, 15, 20, 25
Desired Speed	50 m/s	50 m/s
Maximum Acceleration	6.0 m/s^2	6.0 m/s^2
Maximum Deceleration	7.5 m/s^2	7.5 m/s^2
Reaction Time	1.0 to 1.5 s	1.0 to 1.5 s
Vehicle Length	2	2
Minimum Gap	2.5 m	2.5 m
Victim	0	3 (Node 1, Node 13, Node 21)
Spoofing Attackers	0	3

Όλα τα οχήματα της διμοιρίας στέλνουν περιοδικά WSM μηνύματα, με την μέθοδο unicast στα υπόλοιπα οχήματα, τα οποία περιέχουν πληροφορίες που σχετίζονται με την κίνηση όπως η θέση, η ταχύτητα, η επιτάχυνση κ.α. Επίσης, στην περιοχή υπάρχει ένα RSU που αναμεταδίδει τα μηνύματα WSM που ανταλλάσσονται. Ωστόσο, εάν τα οχήματα της διμοιρίας εντοπίσουν οποιαδήποτε κυκλοφοριακή διαταραχή, δηλαδή ατύχημα μεταξύ οχημάτων ή ατυχήματα μεταξύ οχημάτων και πεζών, ενδέχεται να αλλάξουν τη διαδρομή τους, σε πραγματικό χρόνο, προκειμένου να φτάσουν στον προορισμό τους πιο γρήγορα. Ακόμη, σύμφωνα με τις παραμέτρους προσομοίωσης η μέγιστη επιτάχυνση ορίζεται σε 6,0 m/s^2, η μέγιστη επιβράδυνση σε 7,5 m/s^2, η επιθυμητή ταχύτητα είναι 50 m/s ενώ ο χρόνος αντίδρασης ορίζεται σε 1,0 έως 1,5 sec. Τέλος, σε σύγκριση με το προηγούμενο κεφάλαιο, οι spoofers έχουν αυξηθεί από έναν σε τρεις και ο συνολικός χρόνος προσομοίωσης έχει αυξηθεί από 120 sec. σε 150 sec.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

4.2 Επιθέσεις Spoofing

Σε αυτό το κεφάλαιο παρουσιάζονται διάφορα σενάρια για την αξιολόγηση του αντίκτυπου μιας σημαντικής επίθεσης DoS, όπως είναι η επίθεση spoofing, υπό ρεαλιστικές συνθήκες κυκλοφορίας και για τη διαμόρφωση κατάλληλων στρατηγικών μετριασμού αυτών των επιθέσεων. Στα σενάρια αυτού του κεφαλαίου, η διμοιρία οχημάτων δημιουργείται με ad-hoc τρόπο, σε συνθήκες πραγματικού χρόνου, με βάση χαρακτηριστικά της κίνησης των οχημάτων όπως εάν κινούνται στον ίδιο δρόμο με την ίδια ταχύτητα κ.α. Επιπλέον υποθέτουμε ότι ένας ή περισσότεροι κόμβοι εντός της διμοιρίας μπορεί να λειτουργούν ως επιτιθέμενοι είτε λόγω επηρεασμού τους από κακόβουλα λογισμικά είτε διότι ενεργούν για προσωπικό συμφέρον. Αυτό επιτυγχάνεται μέσω της διάδοσης παραπλανητικών δεδομένων π.χ. τροποποιημένων WSM μηνυμάτων σε άλλα μέλη της διμοιρίας. Τα οχήματα αντιλαμβάνονται αυτές τις πληροφορίες ως ακριβείς και δέχονται επίθεση. Το σενάριο της επίθεσης προϋποθέτει ότι η διμοιρία των οχημάτων κινείται γύρω από την πόλη Erlangen, στις καθορισμένες διαδρομές, σύμφωνα με την Εικόνα 3.

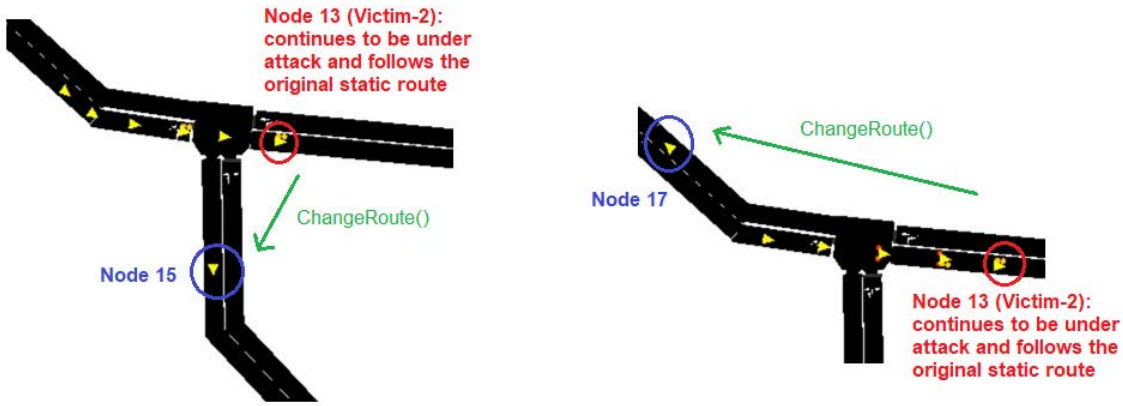
Ξεκινώντας από το 10ο δευτερόλεπτο της προσομοίωσης, το πρώτο όχημα της διμοιρίας (Node 0: spoofer 1–επιτιθέμενος 1) αρχίζει να παραποιεί τις παραμέτρους ενός WSM μηνύματος, ιδίως της ταχύτητας, εκχωρώντας μια τυχαία τιμή που προκύπτει από μια ομοιόμορφη κατανομή, εντός του εύρους των (0,1, 0,9). Παρά τις αλλαγές, αυτό το όχημα συνεχίζει κατά μήκος της σχεδιασμένης διαδρομής του χωρίς καμία απόκλιση. Στη συνέχεια, ο Node 1 (victim 1–θύμα 1), μόλις λάβει αυτό το μήνυμα, ρυθμίζει την ταχύτητά του σε μια τιμή που προέρχεται από ομοιόμορφη κατανομή με τιμές στο σύνολο (0,1, 0,9). Αυτό δημιουργεί κυκλοφοριακή συμφόρηση, με τα μέλη της διμοιρίας που ακολουθούν να σχηματίζουν μια ουρά στην ελάχιστη απόσταση των 2,5 m, όπως φαίνεται στην Εικόνα 4.

Αυτό συμβαίνει διότι, κατά τη διάρκεια της επίθεσης, τα οχήματα κινούνται σε δρόμο διπλής κατεύθυνσης με μία λωρίδα κυκλοφορίας ανά κατεύθυνση. Επομένως, τα οχήματα που ακολουθούν δεν μπορούν να προσπεράσουν τον Node 1 (θύμα 1). Γύρω στο 85ο δευτερόλεπτο της προσομοίωσης, η διμοιρία οχημάτων φτάνει σε μία διασταύρωση. Αυτό σημαίνει ότι η διάρκεια της πρώτης επίθεσης spoofing είναι περίπου 75 δευτερόλεπτα. Υποθέτουμε ότι κάθε κόμβος της διμοιρίας εκτελεί ένα εξαιρετικά προστατευμένο κομμάτι κώδικα, σύμφωνα με το οποίο εάν ένα όχημα παραμείνει σταματημένο για ένα εύλογο διάστημα 10 δευτερολέπτων, θα ειδοποιήσει τα ακόλουθα οχήματα ώστε να αλλάξουν πορεία με σκοπό να φτάσουν στον προορισμό τους.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Στη συνέχεια, κάποια από τα οχήματα που ακολουθούν μετά από τον κόμβο θύμα-1 αποσπώνται από τη διμοιρία, αν έχουν την επιλογή, ώστε να «ξεπεράσουν» το εμπόδιο του Node 1 και να συνεχίσουν ανεμπόδιστα τη διαδρομή τους. Στις προσομοιώσεις του συγκεκριμένου κεφαλαίου κατά το 85ο δευτερόλεπτο σταματάει η επίδραση του Spoofer 1 στο Victim-1 (Node 1) και αυτό συνεχίζει κανονικά την προκαθορισμένη του διαδρομή. Ένας αριθμός κόμβων αποσπάστηκε από την διμοιρία κατά την διάρκεια της επίθεσης, όταν είχε την επιλογή. Οι υπόλοιποι κόμβοι συνεχίζουν κανονικά την πορεία τους πίσω από το Node 1 το οποίο δεν αποτελεί πλέον θύμα.

Κατά το 100ο δευτερόλεπτο της προσομοίωσης το 13ο όχημα (Node 12: spoofer 2–επιτιθέμενος 2) αρχίζει να παραποιεί τις παραμέτρους ενός νέου WSM μηνύματος και να αναμεταδίδει ψευδείς πληροφορίες όπως ο Node 0 νωρίτερα. Ο Node 13 (victim 2–θύμα 2), μόλις λάβει τα νέα WSM μηνύματα ρυθμίζει την ταχύτητα του σε μία τιμή που προέρχεται από ομοιόμορφη κατανομή με τιμές στο σύνολο (0,1, 0,9). Αυτό δημιουργεί κυκλοφοριακή συμφόρηση με τα μέλη της διμοιρίας που ακολουθούν να σχηματίζουν μία ουρά από αυτοκίνητα στην ελάχιστη επιθυμητή απόσταση των 2,5 m. Όπως φαίνεται και από την Εικόνα 17 τα οχήματα που ακολουθούν τον Node 13 (θύμα-2) όταν έχουν την ευκαιρία, αλλάζουν την προκαθορισμένη διαδρομή τους για να αποφύγουν τον κόμβο θύμα και να συνεχίσουν κανονικά την πορεία τους. Αυτή η επίθεση spoofing συνεχίζεται έως το 120ο δευτερόλεπτο. Αυτό σημαίνει πως η διάρκεια της δεύτερης επίθεσης spoofing είναι περίπου 20 δευτερόλεπτα.



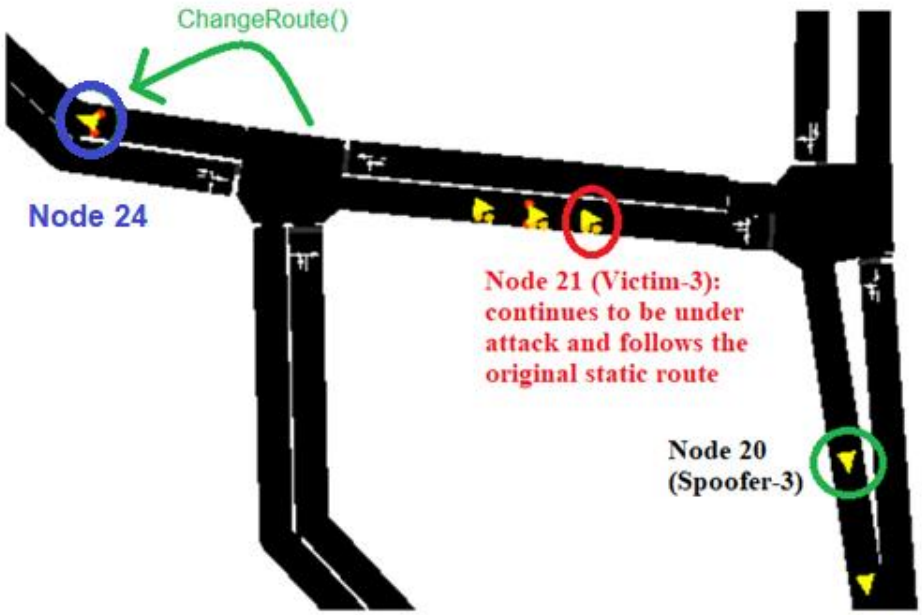
Εικόνα 17: Στιγμιότυπα κατά την διάρκεια της 2ης επίθεσης

Στη συνέχεια τα οχήματα συνεχίζουν κανονικά την πορεία τους έως το 125ο δευτερόλεπτο όπου το 21ο όχημα της διμοιρίας (Node 20: spoofer 3–επιτιθέμενος 3) αρχίζει

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

να παραποιεί τις παραμέτρους ενός νέου WSM μηνύματος, ιδίως της ταχύτητας, εκχωρώντας μια τυχαία τιμή που προκύπτει από μια ομοιόμορφη κατανομή, εντός του εύρους των (0,1, 0,9) ενώ αυτό το όχημα συνεχίζει κατά μήκος της σχεδιασμένης διαδρομής του χωρίς καμία απόκλιση. Ο Node 21 (victim 3–θύμα 3) που ακολουθεί, λαμβάνοντας το νέο μήνυμα ρυθμίζει την ταχύτητα του σε μία τιμή που προέρχεται από ομοιόμορφη κατανομή με τιμή στο σύνολο (0,1, 0,9) όπως συμβαίνει και με τους προηγούμενους κόμβους θύματα. Σύμφωνα με την Εικόνα 18 όταν δοθεί η ευκαιρία στα οχήματα που ακολουθούν τον κόμβο θύμα 3 όπως μία διασταύρωση, αυτά αλλάζουν την προσχεδιασμένη διαδρομή τους ώστε να συνεχίσουν την πορεία τους χωρίς καθυστερήσεις. Η τρίτη επίθεση spoofing συνεχίζεται έως το 140^{o} δευτερόλεπτο και διαρκεί 15 δευτερόλεπτα.

Όπως ήδη αναφέρθηκε, κατά την κίνηση της διμοιρίας, τα οχήματα ανταλλάσσουν WSM μηνύματα που περιέχουν διάφορες πληροφορίες, για την ταχύτητά τους, την επιτάχυνσή τους και την θέση τους. Σύμφωνα με αυτές τις τιμές των WSM μηνυμάτων, εξάγουμε έναν αριθμό μετρήσεων για να εξετάσουμε τις συνέπειες της επίθεσης spoofing. Αυτές αναφέρονται στη συνολική απόσταση που διανύθηκε, στο ποσοστό PDR των WSM μηνυμάτων για κάθε όχημα, καθώς και στον χρόνο καθυστέρησης των οχημάτων που παραμένουν στην ουρά λόγω της επίθεσης. Σκοπός των επιθέσεων αυτού του κεφαλαίου αποτελεί η διερεύνηση των επιπτώσεων και η ανάλυση των αποτελεσμάτων των πολλαπλών επιθέσεων spoofing σε μία διμοιρία οχημάτων και η σύγκρισή τους με αυτά του προηγούμενου κεφαλαίου.



Εικόνα 18: Στιγμιότυπο κατά την διάρκεια της 3ης επίθεσης

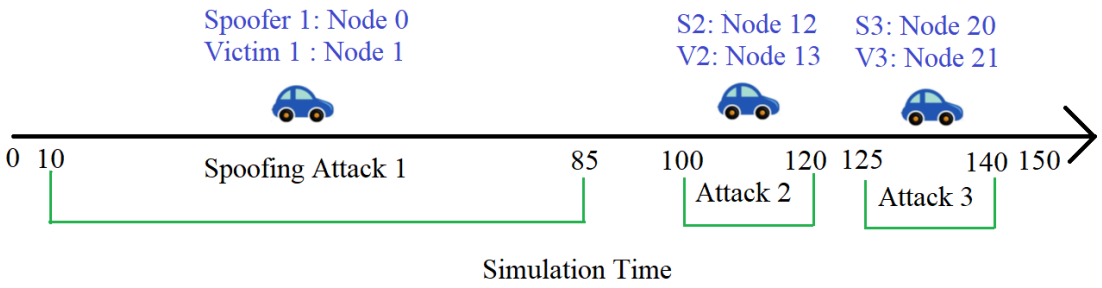
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

4.3 Αξιολόγηση απόδοσης μοντέλου

Για την αξιολόγηση της απόδοσης του μοντέλου επίθεσης spoofing, γίνεται χρήση των λογισμικών OMNeT++ 5.6.2, INET 3.6, Veins 4.7 και SUMO 0.30.0. Σε αυτό το μοντέλο προσομοιώνουμε και συγκρίνουμε δύο σενάρια. Το πρώτο το ονομάζουμε Κανονικό Σενάριο (Normal Scenario), όπου τα οχήματα κινούνται υπό κανονικές συνθήκες στους δρόμους της πόλης, χωρίς την παρουσία κάποιου επιτιθέμενου. Στο δεύτερο σενάριο, το οποίο ονομάζεται Spoofing Attack Scenario, γίνονται επιθέσεις πλαστογράφησης (Spoofing) με διαφορετικές τυχαίες αλλά διακριτές τιμές οχημάτων σε μία αστική περιοχή. Οι τιμές αυτές είναι n = 10, 15, 20, 25. Ο Πίνακας 6 περιγράφει όλες τις παραμέτρους της προσομοίωσης που εφαρμόστηκαν για την πραγματοποίηση των επιθέσεων.

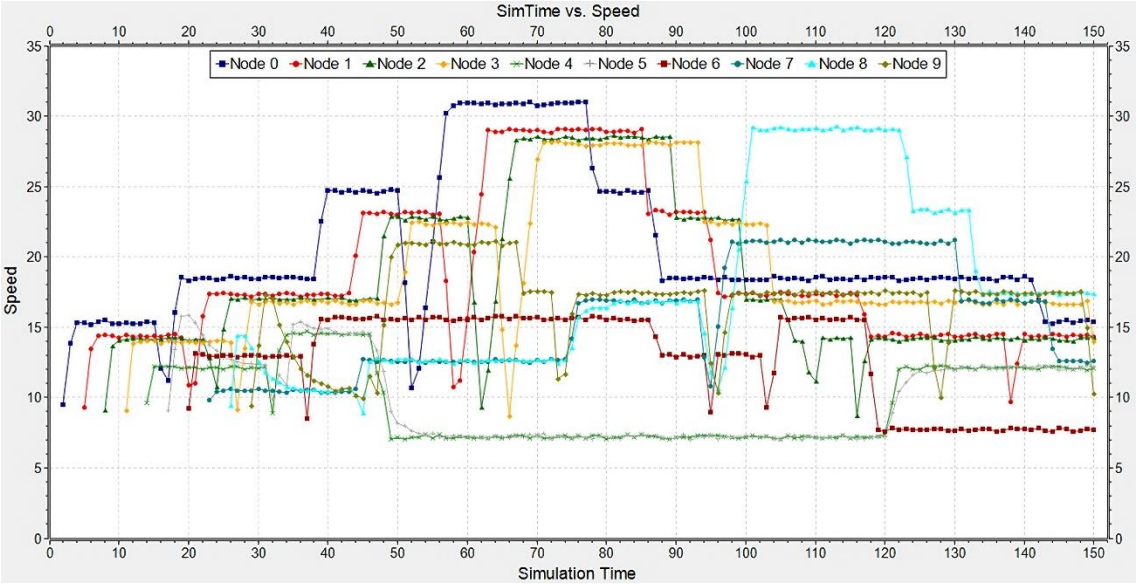
Τα αποτελέσματα της επίθεσης πλαστογράφησης στην κίνηση της διμοιρίας παρουσιάζονται από τα παρακάτω πειράματα. Σε αυτά η ταχύτητα και η επιτάχυνση συγκρίνονται για τα δύο όρια της τιμής n των οχημάτων, δηλαδή για 10 και για 25 αλλά και για μία ενδιάμεση τιμή 20 vehicles/km. Η Εικόνα 20, η Εικόνα 21, η Εικόνα 22 και η Εικόνα 23 παρουσιάζουν την ταχύτητα και την επιτάχυνση για μια διμοιρία οχημάτων μεγέθους 10. Η Εικόνα 24, η Εικόνα 25, η Εικόνα 26 και η Εικόνα 27 παρουσιάζουν την ταχύτητα και την επιτάχυνση για μια διμοιρία οχημάτων μεγέθους 20. Ενώ, η Εικόνα 28, η Εικόνα 29, η Εικόνα 30 και η Εικόνα 31 παρουσιάζουν την ταχύτητα και την επιτάχυνση για μια διμοιρία οχημάτων μεγέθους 25. Μέσα από αυτές τις εικόνες παρουσιάζεται η επίδραση των επιθέσεων τόσο στην ταχύτητα όσο και στην επιτάχυνση των οχημάτων.

Το μοντέλο συστήματος αυτού του κεφαλαίου αποτελείται από ένα κατανεμημένο σύστημα πιο πολύπλοκο σε σχέση με αυτό του προηγούμενου κεφαλαίου, διότι περιλαμβάνει τρεις επιτιθέμενους που συνεργάζονται για να επιτεθούν σε διαφορετικά χρονικά διαστήματα. Λόγω αυτού γίνεται δυσκολότερη η ανίχνευση των επιθέσεων. Αυτό παρατηρείται τόσο από τα γραφήματα ταχύτητας και επιτάχυνσης που ακολουθούν όσο και από αυτά της συνολικής διανυθείσας απόστασης. Η Εικόνα 19 περιγράφει το μοντέλο.

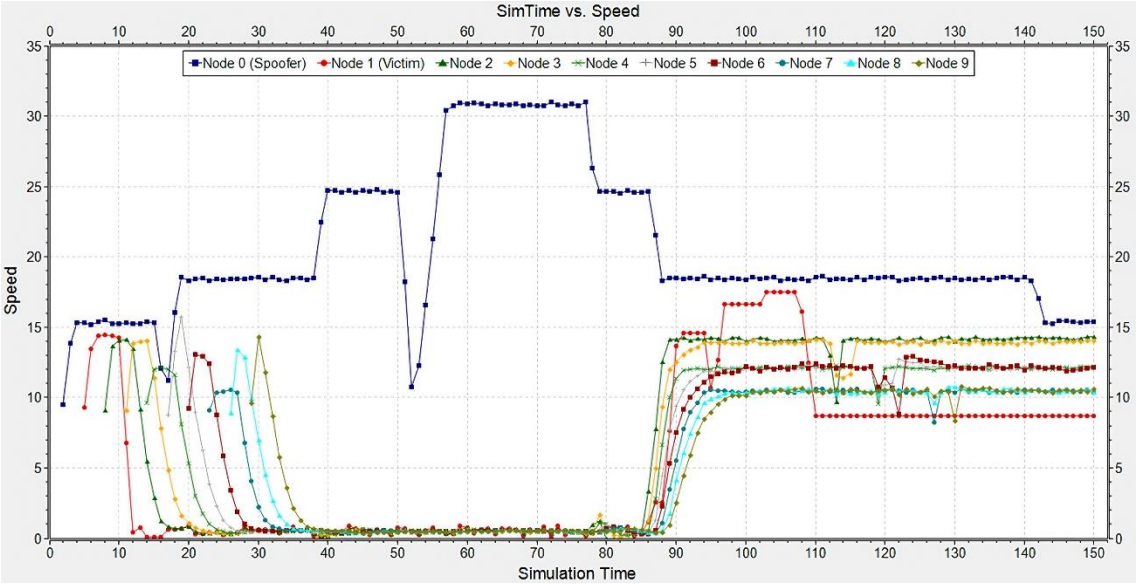


Εικόνα 19: Μοντέλο Συστήματος

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

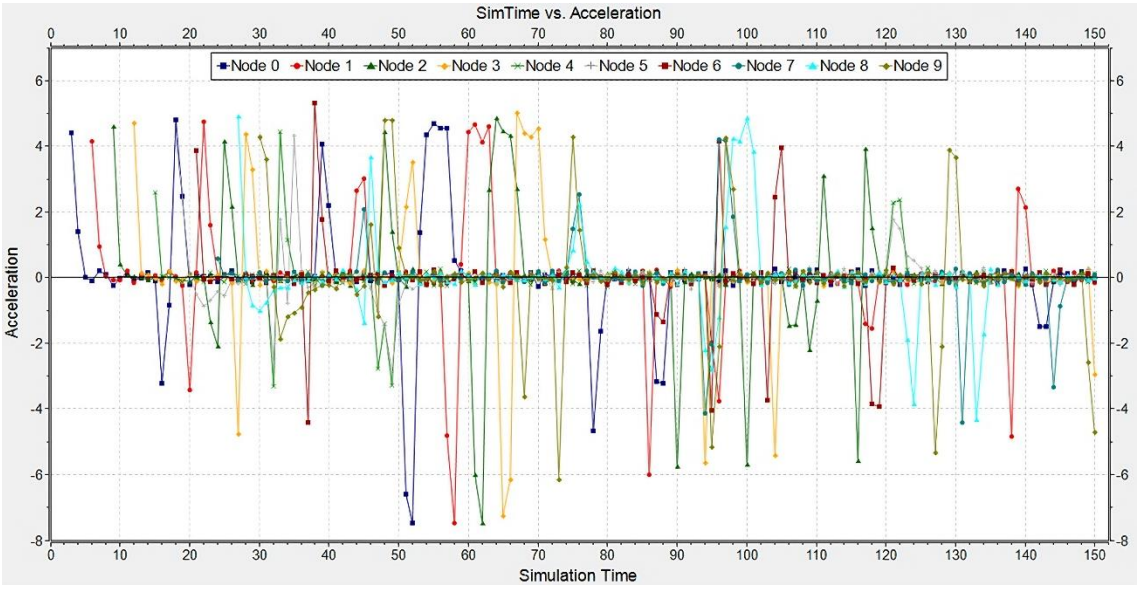


Εικόνα 20: Η ταχύτητα των οχημάτων του platoon για 10 vehicles/km στο κανονικό σενάριο

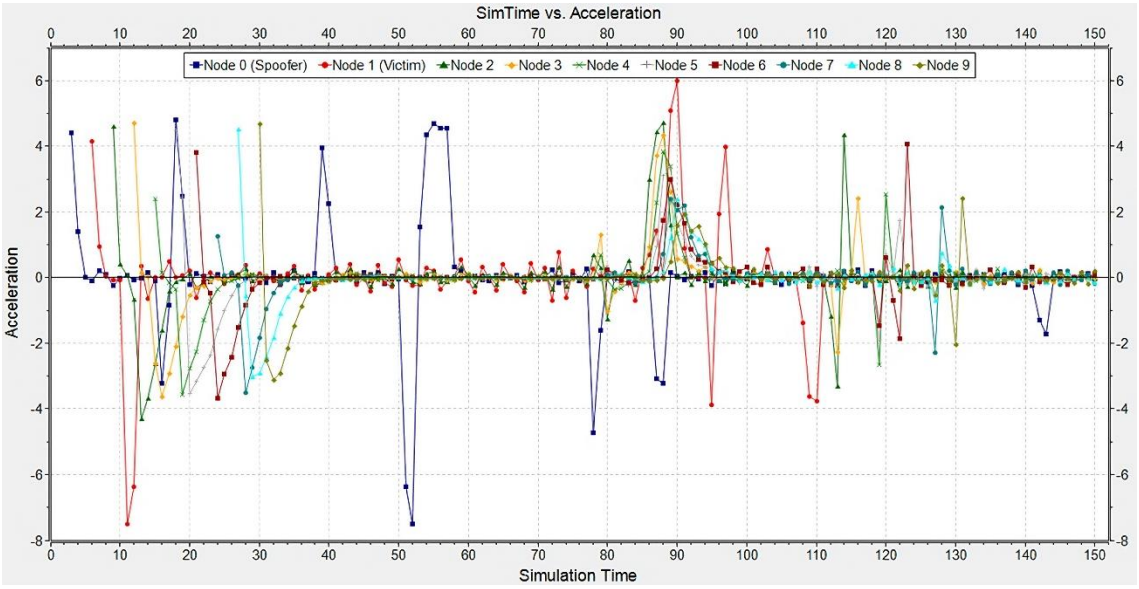


Εικόνα 21: Η ταχύτητα των οχημάτων του platoon για 10 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

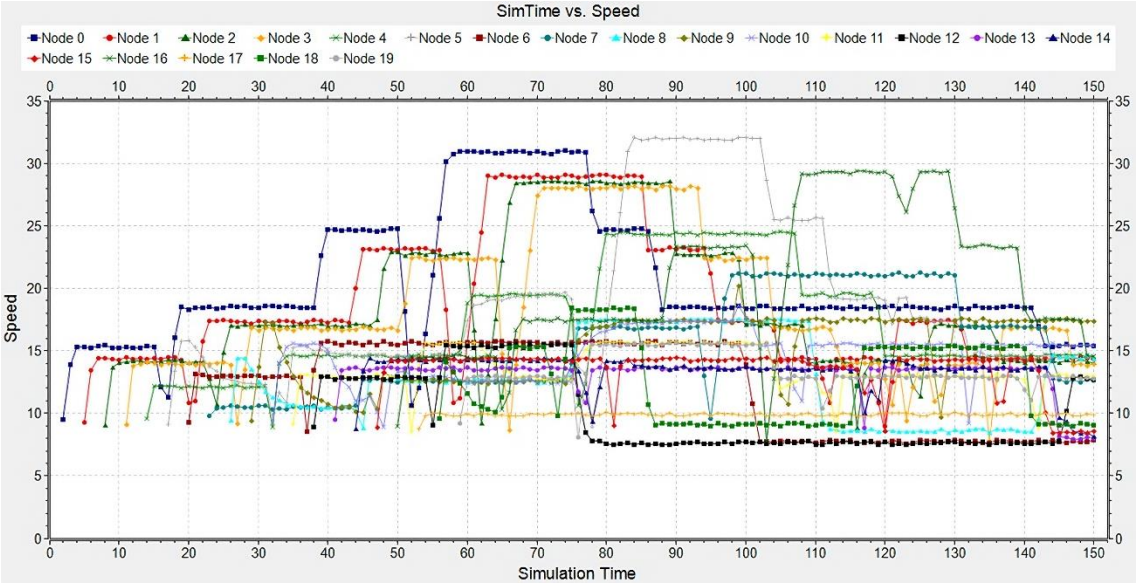


Εικόνα 22: Η επιτάχυνση των οχημάτων του platoon για 10 vehicles/km στο κανονικό σενάριο

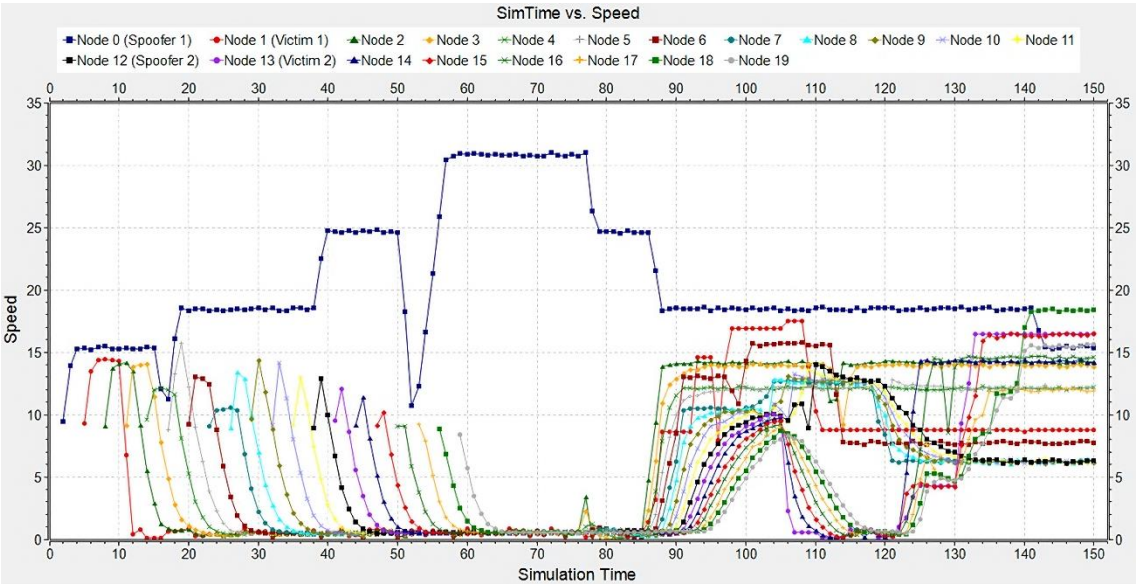


Εικόνα 23: Η επιτάχυνση των οχημάτων του platoon για 10 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

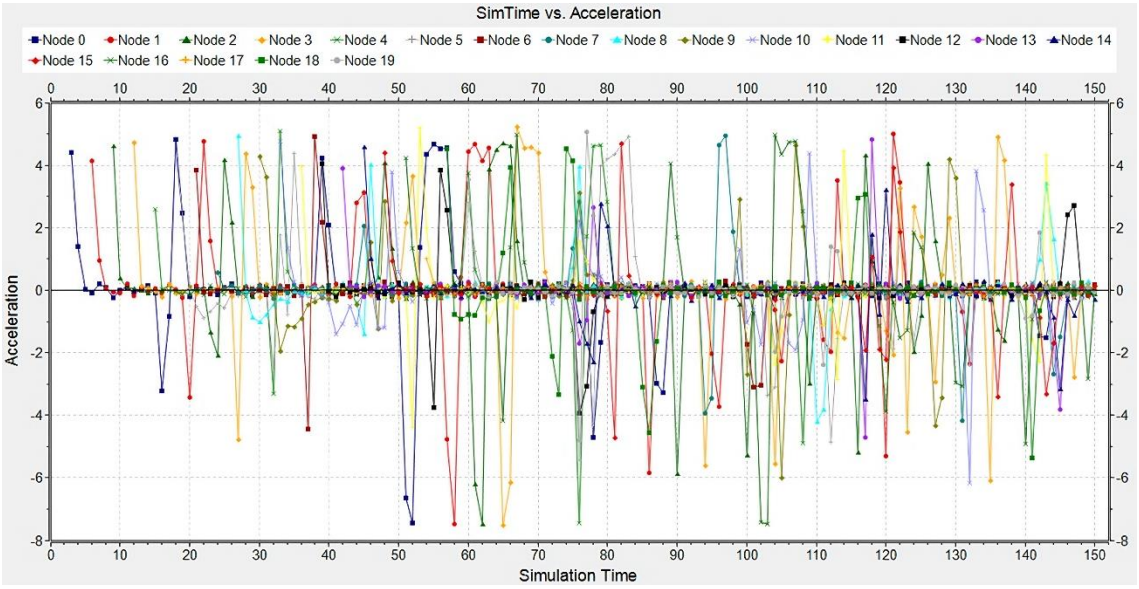


Εικόνα 24: Η ταχύτητα των οχημάτων του platoon για 20 vehicles/km στο κανονικό σενάριο

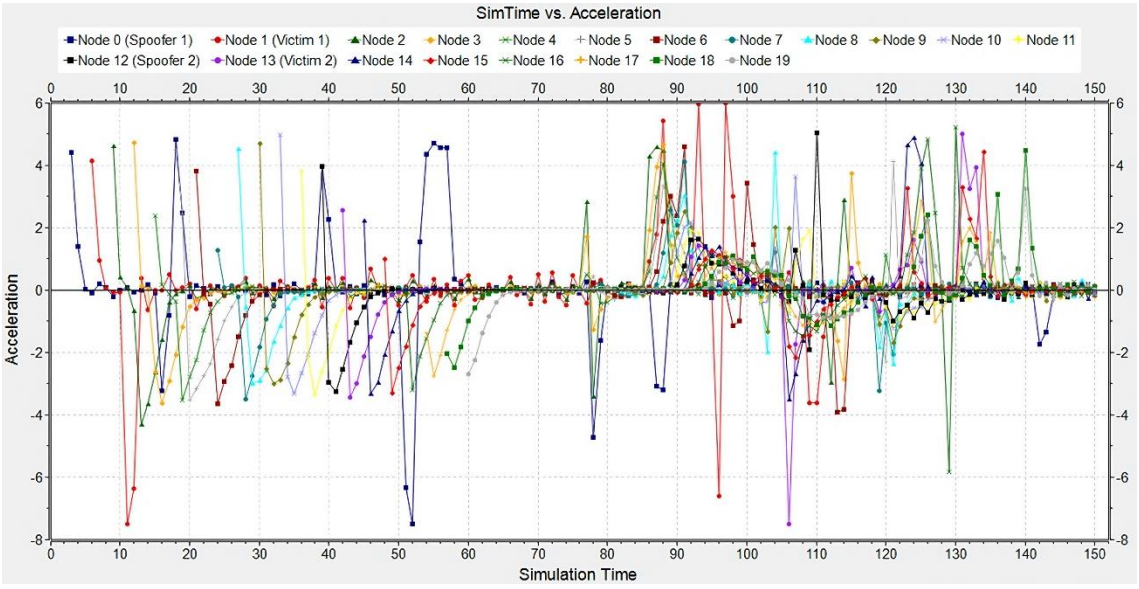


Εικόνα 25: Η ταχύτητα των οχημάτων του platoon για 20 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

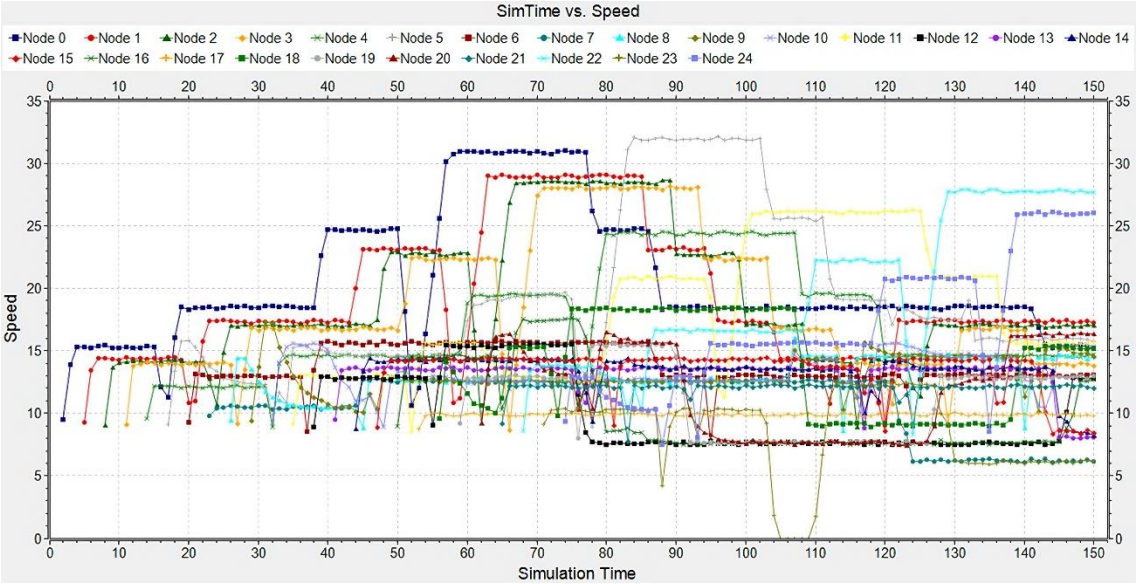


Εικόνα 26: Η επιτάχυνση των οχημάτων του platoon για 20 vehicles/km στο κανονικό σενάριο

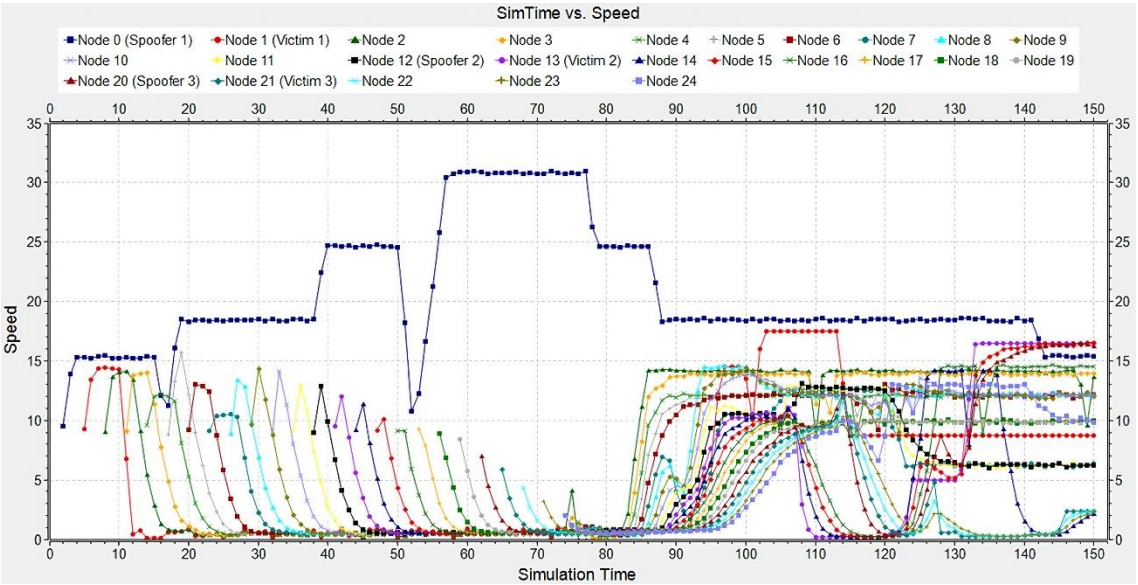


Εικόνα 27: Η επιτάχυνση των οχημάτων του platoon για 20 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

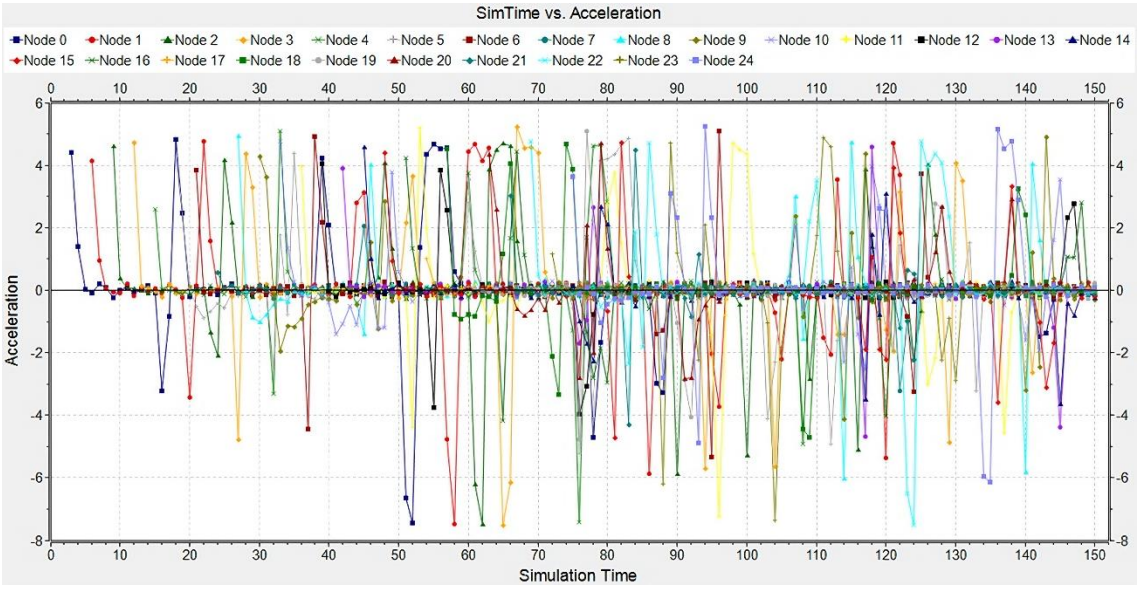


Εικόνα 28: Η ταχύτητα των οχημάτων του platoon για 25 vehicles/km στο κανονικό σενάριο

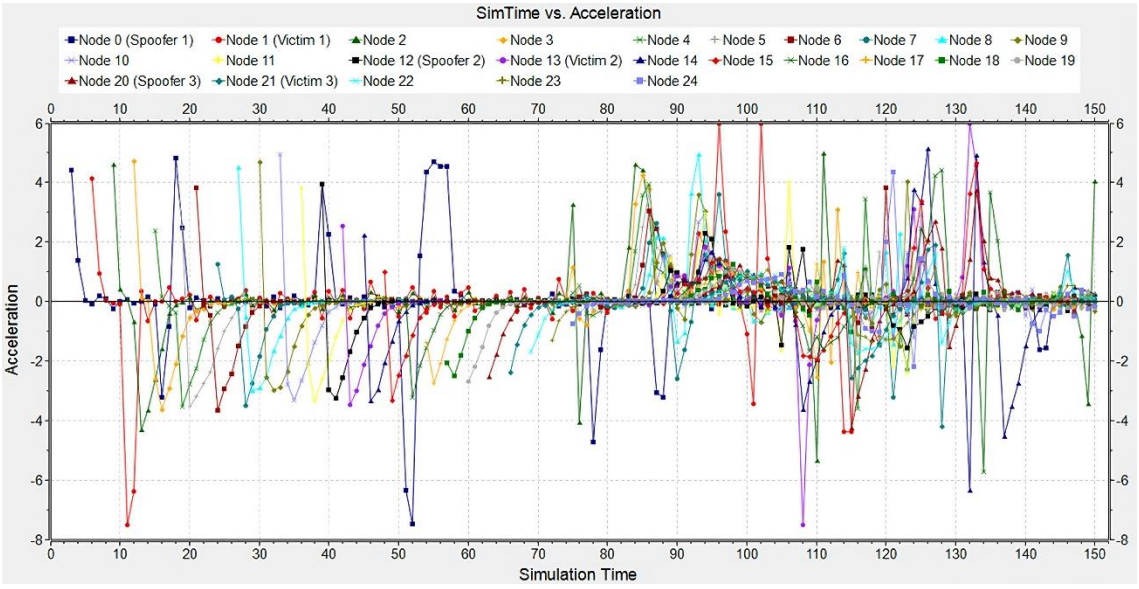


Εικόνα 29: Η ταχύτητα των οχημάτων του platoon για 25 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Εικόνα 30: Η επιτάχυνση των οχημάτων του platoon για 25 vehicles/km στο κανονικό σενάριο



Εικόνα 31: Η επιτάχυνση των οχημάτων του platoon για 25 vehicles/km στο σενάριο επίθεσης Spoofing

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Επίσης, διεξήχθη στατιστική ανάλυση των παραπάνω αποτελεσμάτων, για 150 sec. όσο και ο συνολικός χρόνος των παρατηρήσεων. Δηλαδή, λήφθηκε μία τιμή για κάθε 1sec. από τα συνολικά 150 sec. του χρόνου προσομοίωσης. Μέσω αυτής της ανάλυσης παρατηρούνται οι τιμές τόσο για το PDR όσο και για την συνολική διανυθείσα απόσταση.

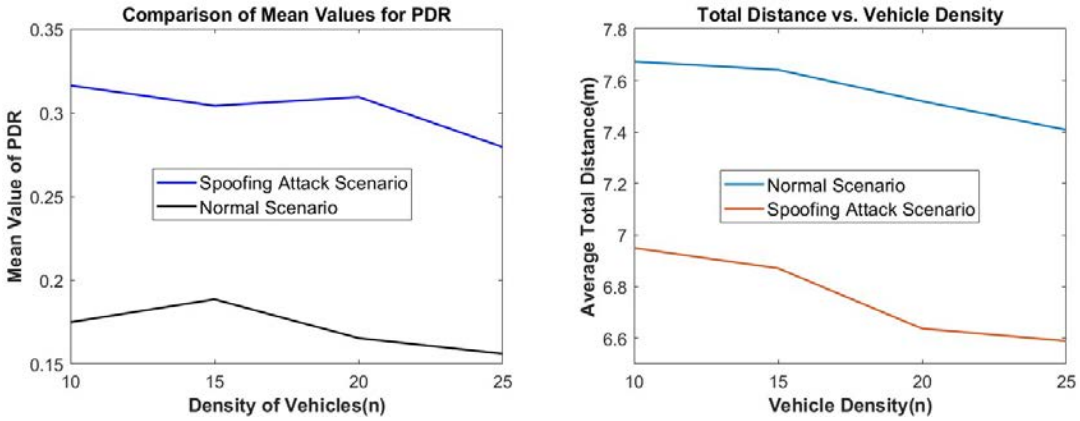
Η Εικόνα 32 απεικονίζει τη σύγκριση της μέσης τιμής του PDR για όλα τα οχήματα που υπάρχουν στην περιοχή, στο εύρος τιμών που ορίζει ο Πίνακας 6. Δείχνει επίσης τη μέση συνολική απόσταση που διανύει κάθε όχημα κατά τη διάρκεια της προσομοίωσης σε λογαριθμική κλίμακα, επειδή η διαφορά μεταξύ του κανονικού σεναρίου και του σεναρίου επίθεσης είναι αρκετά μεγάλη. Παρατηρείται ότι τόσο η κατανομή του PDR όσο και η κατανομή της συνολικής απόστασης προσεγγίζουν μια εκθετική κατανομή με πολύ μικρή παράμετρο. Ομοίως, οι κατανομές των ίδιων παραμέτρων για την περίπτωση της επίθεσης πλαστογράφησης προσεγγίζουν τη συνάρτηση αθροιστικής κατανομής (CDF) μιας εκθετικής κατανομής με πολύ μικρή παράμετρο. Επομένως, η επίθεση πλαστογράφησης έχει ως αποτέλεσμα όλα τα οχήματα να ταξιδεύουν μικρότερες αποστάσεις από αυτές που θα διένυαν κανονικά στο ίδιο χρονικό διάστημα, ενώ ταυτόχρονα επηρεάζεται σημαντικά το μέσο ασύρματης μετάδοσης, αυξάνοντας τον αριθμό των πακέτων που μεταδίδουν τα οχήματα. Ακόμη, σε σύγκριση με την Εικόνα 15 του προηγούμενου κεφαλαίου φαίνεται πως η συνολική διανυθείσα απόσταση έχει αυξηθεί λόγω του περισσότερου χρόνου προσομοίωσης, ενώ η διαφορά του PDR μεταξύ του κανονικού σεναρίου και του σεναρίου επίθεσης παραμένει σχετικά σταθερή.

Η Εικόνα 33 απεικονίζει τη συνολική διανυθείσα απόσταση για όλους τους κόμβους με τιμές (n = 10, 15, 20, 25 vehicles/km) σε ένα εύρος από 10 έως 25 οχήματα. Σε αυτή τη σειρά σχημάτων, τα κύρια συμπεράσματα είναι πανομοιότυπα με αυτά που παρουσιάζονται στην Εικόνα 32. Αυτό που είναι ξεκάθαρο είναι ότι η επίθεση spoofing επηρεάζει τους κόμβους θύματα (Node 1, Node 13, Node 21), αναγκάζοντας τους να κινούνται με ελάχιστη ταχύτητα κατά την διάρκεια της επίθεσης αλλά και τους αμέσως επόμενους κόμβους αυτών. Οι επιπτώσεις στα υπόλοιπα οχήματα είναι σημαντικές αλλά όχι τόσο μεγάλες. Για τις διάφορες τιμές οχημάτων (Vehicle Density), δεν παρατηρείται σημαντική αύξηση της διανυθείσας απόστασης.

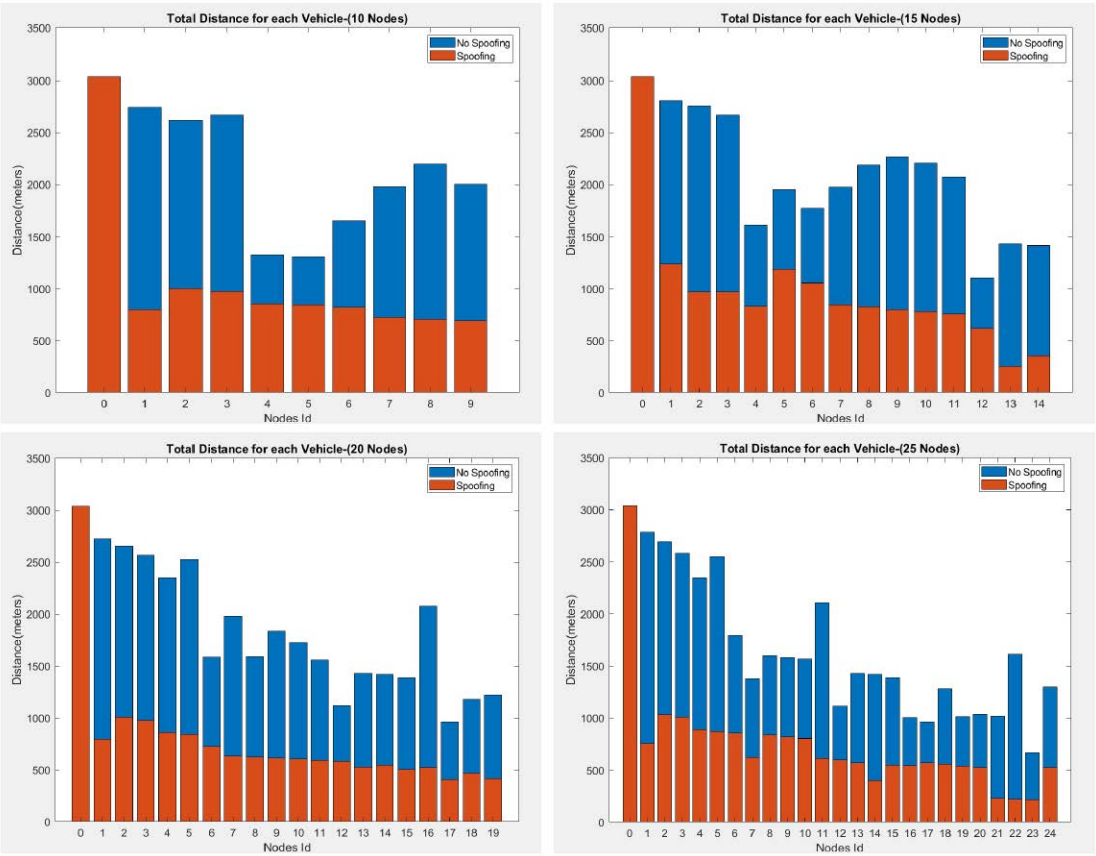
Αυτή η συμπεριφορά παρατηρείται διότι, στις επιθέσεις αυτού του κεφαλαίου παρόλο που υπάρχουν περισσότεροι επιτιθέμενοι, αυτοί επιτίθονται σε διαφορετικά – μικρότερα χρονικά διαστήματα αλλά και σε λιγότερα οχήματα καθώς επηρεάζονται μόνο τα οχήματα που τους ακολουθούν. Ενώ στο προηγούμενο κεφάλαιο υπήρχε ένας επιτιθέμενος

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

με μεγαλύτερη χρονική διάρκεια επίθεσης, επηρεάζοντας περισσότερους κόμβους. Περίπτωση προς μελλοντική έρευνα αποτελεί η από κοινού επίθεση όλων των επιτιθέμενων στα ίδια οχήματα και η ανάλυση των επιπτώσεων της σε αυτά. Παρόμοιο συμπέρασμα μπορεί να εξαχθεί και για το PDR διότι, όσο περισσότερα οχήματα επηρεάζονται από τις επιθέσεις τόσο περισσότερα μηνύματα ανταλλάσσονται.



Εικόνα 32: Μέση τιμή του PDR και μέση συνολική διανυθείσα απόσταση για τις διάφορες τιμές οχημάτων



Εικόνα 33: Γραφήματα για την συνολική διανυθείσα απόσταση για όλους τους κόμβους σε όλα τα σενάρια προσομοίωσης

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Ο Πίνακας 7 παρουσιάζει τις τιμές που χρησιμοποιήθηκαν για να δημιουργηθεί η Εικόνα 15 και η Εικόνα 32. Οι τιμές περιγράφουν τη σύγκριση της συνολικής διανυθείσας απόστασης σε σχέση με το πλήθος των οχημάτων για το κανονικό σενάριο και για το σενάριο επίθεσης Spoofing τόσο για το κεφάλαιο 3 όσο και για το κεφάλαιο 4. Μεταξύ των τιμών των δύο κεφαλαίων παρατηρούνται μικρές διαφορές οι οποίες δικαιολογούνται από το διαφορετικό συνολικό χρόνο προσομοίωσης των σεναρίων.

Πίνακας 7: Σύγκριση μεταξύ των τιμών του Total Distance vs Vehicle Density των κεφαλαίων 3 και 4

Vehicle Density (veh/km)	Chapter 3		Chapter 4	
	Normal Scenario	Spoofing Scenario	Normal Scenario	Spoofing Scenario
10	7.4427	6.4612	7.6743	6.9505
15	7.3771	6.1569	7.6421	6.8712
20	7.2661	6.1391	7.5198	6.6371
25	7.1207	6.0938	7.4087	6.5889

Συμπερασματικά, συγκρίνοντας τα αποτελέσματα των κεφαλαίων 3 και 4 παρατηρείται πως υπάρχουν ομοιότητες αλλά και διαφορές. Αρχικά, εμφανίζουν παρόμοιες συμπεριφορές στο PDR και στο Total Distance. Ωστόσο, φαίνεται πως με την προσθήκη περισσότερων επιτιθέμενων επηρεάζονται όλοι οι κόμβοι της διμοιρίας ακόμη και αυτοί που βρίσκονται στο τέλος της. Παράδειγμα αποτελούν οι κόμβοι 17 – 19 και οι κόμβοι 22 – 24 που εμφανίζουν μεγαλύτερη διαφορά μεταξύ των αποστάσεων που διένυσαν κατά την διάρκεια των επιθέσεων. Ακόμη μία σημαντική παρατήρηση που εξάγεται από τα αποτελέσματα και κυρίως από τα γραφήματα ταχύτητας και επιτάχυνσης είναι πως όσο περισσότεροι επιτιθέμενοι υπάρχουν, τόσο πιο δύσκολη γίνεται η ανίχνευση (detection) των επιθέσεων. Αυτό συμβαίνει διότι στα γραφήματα υπάρχουν πολύ περισσότερες πληροφορίες, γεγονός που προκαλεί σύγχυση στα συστήματα ανίχνευσης επιθέσεων.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

5 Εντοπισμός επιθέσεων με χρήση του φίλτρου Kalman

Τα τελευταία χρόνια οι επιθέσεις spoofing έχουν αναδειχθεί ως μία από τις ισχυρότερες επιθέσεις ενάντια σε συστήματα όπως το GPS κ.α. Το συγκεκριμένο κεφάλαιο αναφέρεται στον εντοπισμό των επιθέσεων spoofing που αναλύθηκαν στα προηγούμενα κεφάλαια. Το φίλτρο Kalman αποτελεί ένα ελαφρύ και αποδοτικό εργαλείο, ιδανικό για ανίχνευση επιθέσεων σε πραγματικό χρόνο, και λειτουργεί ως θεμέλιο για την ανάπτυξη ενός μελλοντικού, πιο εξελιγμένου συστήματος, το οποίο θα ενσωματώνει προηγμένους αλγορίθμους μηχανικής μάθησης ώστε να εντοπίζει και να αντιμετωπίζει τις επιθέσεις πιο ολοκληρωμένα. Το φίλτρο που χρησιμοποιείται για τον εντοπισμό των επιθέσεων είναι πολύ γνωστό και βρίσκει εφαρμογή στην επεξεργασία σήματος, στα οικονομικά κ.α.

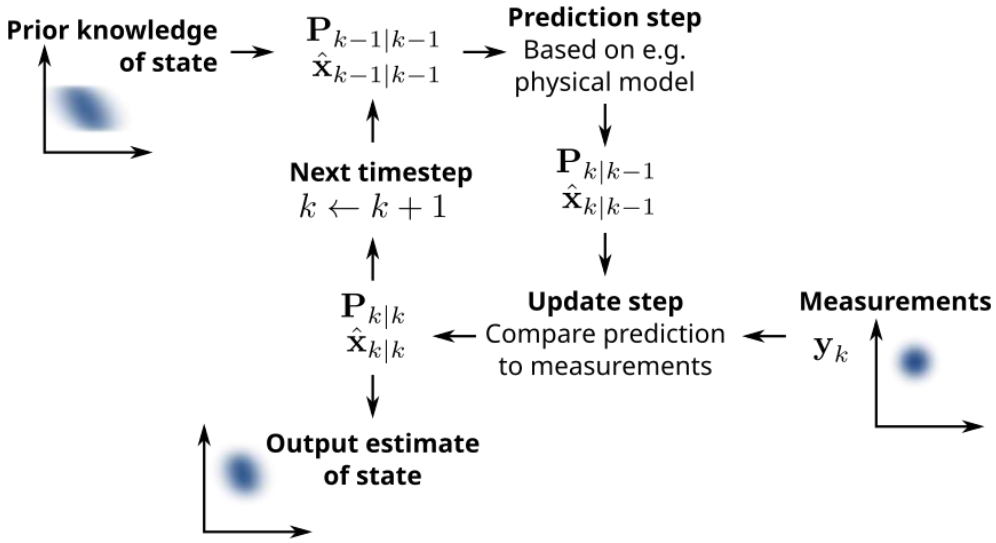
5.1 Παρουσίαση των λειτουργιών και των εφαρμογών του φίλτρου

Το φίλτρο Kalman αποτελεί μία μέθοδο εκτίμησης κατάστασης, η οποία βασίζεται σε μετρήσεις που συλλέγονται διαχρονικά από πηγές όπως τα συστήματα παγκόσμιου εντοπισμού θέσης (GNSS – Global Navigation Satellite Systems) και τα μηνύματα ασφαλείας (WSM – Wave Short Messages) που ανταλλάσσονται μέσω της τεχνολογίας ασύρματης επικοινωνίας μικρής εμβέλειας (DSRC – Dedicated Short-Range Communications). Λαμβάνει υπόψη την παρουσία στοχαστικού θορύβου και σφαλμάτων στις μετρήσεις, με στόχο την ακριβέστερη πρόβλεψη της πραγματικής κατάστασης ενός δυναμικού συστήματος. Το φίλτρο φέρει το όνομα του Ούγγρου Rudolf E. Kálmán που το εφηύρε. Αυτό χρησιμοποιείται ευρέως σε εφαρμογές όπως η πλοήγηση, η καθοδήγηση, ο έλεγχος οχημάτων κ.α. των οποίων η θέση μεταβάλλεται δυναμικά.

Η λειτουργία του αλγορίθμου αποτελείται από δύο στάδια. Το πρώτο στάδιο είναι η πρόβλεψη. Σε αυτό το στάδιο το φίλτρο παράγει εκτιμήσεις για τις μεταβλητές της τρέχουσας κατάστασης και υπολογίζει την επόμενη κατάσταση με βάση το μαθηματικό μοντέλο του συστήματος. Το δεύτερο στάδιο είναι η διόρθωση. Σε αυτό το στάδιο γίνεται

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ενσωμάτωση των νέων μετρήσεων με σκοπό την βελτίωση της πρόβλεψης. Ο αλγόριθμος είναι αναδρομικός και μπορεί να λειτουργεί σε πραγματικό χρόνο χρησιμοποιώντας μόνο τις τρέχουσες μετρήσεις εισόδου, την προηγούμενη κατάσταση που υπολογίστηκε και τον πίνακα αβεβαιότητας, δηλαδή τον θόρυβο που προστέθηκε στις μετρήσεις. Η Εικόνα 34 αναπαριστά μία γενική μορφή της λειτουργίας του φίλτρου.



Εικόνα 34: Περιγραφή λειτουργιών φίλτρου Kalman
[https://en.wikipedia.org/wiki/Kalman_filter]

Για την βέλτιστη λειτουργία του φίλτρου γίνεται η υπόθεση ότι ο θόρυβος των δεδομένων ακολουθεί την κανονική κατανομή Gauss. Ασχέτως, αυτής της υπόθεσης το φίλτρο Kalman αποτελεί την καλύτερη επιλογή όσον αφορά στην εκτίμηση γραμμικών συστημάτων λόγω του ελάχιστου μέσου τετραγωνικού σφάλματος. Ακόμη, έχουν αναπτυχθεί επεκτάσεις και γενικεύσεις της μεθόδου όπως το εκτεταμένο φίλτρο Kalman κ.α. τα οποία λειτουργούν σε μη γραμμικά συστήματα. Το φίλτρο Kalman χρησιμοποιεί το δυναμικό μοντέλο ενός συστήματος, τα γνωστά δεδομένα ελέγχου αυτού και πολλαπλές διαδοχικές μετρήσεις για να σχηματίσει μια εκτίμηση των μεταβαλλόμενων μεγεθών του συστήματος. Αυτό είναι καλύτερο από την εκτίμηση με μόνο μία μέτρηση. Το φίλτρο αυτό, είναι ένας αλγόριθμος που συγχωνεύει τις μετρήσεις από αισθητήρες και την μέχρι τώρα εκτίμηση της κατάστασης του δυναμικού συστήματος.

Τα δεδομένα θορύβου, στις εξισώσεις που περιγράφουν την εξέλιξη του συστήματος και οι εξωτερικοί παράγοντες που δεν λαμβάνονται υπόψη, περιορίζουν το πόσο καλά προσδιορίζεται η κατάσταση του συστήματος. Το φίλτρο Kalman αντιμετωπίζει αποτελεσματικά την αβεβαιότητα που οφείλεται στα δεδομένα θορύβου και τους τυχαίους εξωτερικούς παράγοντες. Παράγει, επίσης, μια εκτίμηση της κατάστασής του ως μέσο όρο

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

της προβλεπόμενης κατάστασης του συστήματος και της νέας μέτρησης χρησιμοποιώντας έναν σταθμισμένο μέσο όρο. Τα βάρη που χρησιμοποιούνται υπολογίζονται από τη διακύμανση. Το αποτέλεσμα του σταθμισμένου μέσου όρου είναι μια νέα εκτίμηση κατάστασης που βρίσκεται μεταξύ της προβλεπόμενης και της μετρούμενης κατάστασης, έχοντας καλύτερη εκτιμώμενη αβεβαιότητα από οποιαδήποτε από τις δύο μεμονωμένες. Αυτή η διαδικασία επαναλαμβάνεται σε κάθε χρονικό βήμα, με τη νέα εκτίμηση και τη διακύμανσή της να επηρεάζουν την πρόβλεψη που χρησιμοποιείται στην επόμενη επανάληψη. Αυτό σημαίνει ότι το φίλτρο Kalman λειτουργεί αναδρομικά και απαιτεί μόνο την τελευταία "καλύτερη εκτίμηση" της κατάστασης ενός συστήματος για τον υπολογισμό της νέας κατάστασης.

Συνήθως, η απόκριση του φίλτρου μετριέται με βάση το κέρδος του. Το κέρδος Kalman είναι το βάρος που δίνεται στις μετρήσεις και στην εκτίμηση της τρέχουσας κατάστασης και μπορεί να "ρυθμιστεί" για να επιτευχθεί μια συγκεκριμένη απόδοση. Με υψηλό κέρδος, το φίλτρο δίνει μεγαλύτερο βάρος στις πιο πρόσφατες μετρήσεις και έτσι προσαρμόζεται σε αυτές με μεγαλύτερη απόκριση. Με χαμηλό κέρδος, το φίλτρο προσαρμόζεται στις προβλέψεις του μοντέλου πιο προσεκτικά. Στα άκρα, ένα υψηλό κέρδος (κοντά στο ένα) θα οδηγήσει σε μια πιο σπασμωδική εκτιμώμενη τροχιά, ενώ ένα χαμηλό κέρδος (κοντά στο μηδέν) θα εξομαλύνει τον θόρυβο αλλά θα μειώσει την απόκριση.

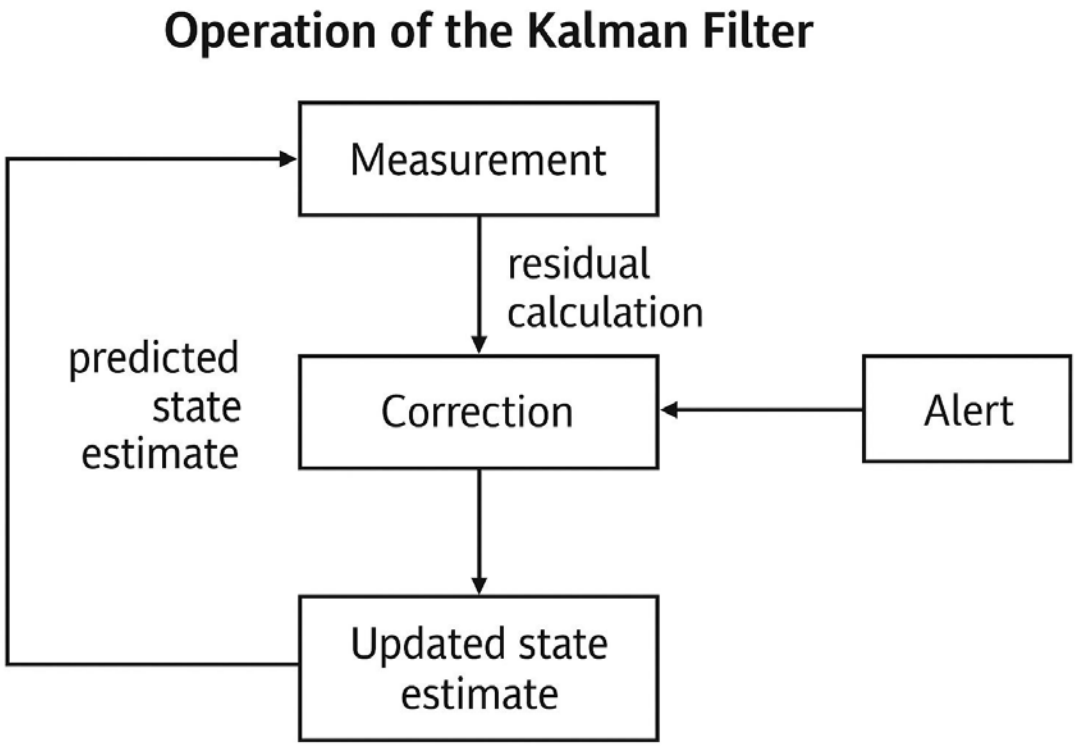
Κατά την εκτέλεση των πραγματικών υπολογισμών για το φίλτρο, η εκτίμηση κατάστασης και οι διακυμάνσεις κωδικοποιούνται σε πίνακες λόγω των πολλαπλών διαστάσεων που εμπλέκονται σε ένα μόνο σύνολο υπολογισμών. Αυτό επιτρέπει την αναπαράσταση γραμμικών σχέσεων μεταξύ διαφορετικών μεταβλητών κατάστασης όπως η ταχύτητα και η επιτάχυνση σε οποιοδήποτε από τα μοντέλα μετάβασης ή τις διακυμάνσεις. Η Εικόνα 35 παρουσιάζει τις αρχές του φίλτρου σε μορφή διαγράμματος και πως ακριβώς έχει τροποποιηθεί σε αυτό το κεφάλαιο, έτσι ώστε να μπορεί να χρησιμοποιηθεί για τον εντοπισμό των επιθέσεων spoofing.

Η επιλογή του φίλτρου Kalman δεν έγινε τυχαία. Αυτό επιλέχθηκε διότι είναι πιο γρήγορο σε σχέση με τα υπόλοιπα φίλτρα ή και αλγορίθμους μηχανικής μάθησης. Επίσης, δεν χρειάζεται πολλά δεδομένα για να εκπαιδεύσει (training) το μοντέλο του ώστε να παραχθούν τα αποτελέσματα. Το φίλτρο λειτουργεί γνωρίζοντας μόνο την προηγούμενη κατάσταση του συστήματος, γεγονός που ενισχύει την ταχύτητά του. Ακόμη το φίλτρο Kalman χρησιμοποιείται από πολλούς ερευνητές για τον εντοπισμό των επιθέ-

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

σεων. Παράδειγμα αποτελούν οι Dabaghi Daryan et al. οι οποίοι ενσωματώνουν ένα φίλτρο Kalman στο tracking loop του GNSS σήματος, επιτυγχάνοντας ποσοστά μετριασμού των επιθέσεων έως και 97%. Ωστόσο, παρόλα τα πλεονεκτήματα που έχει το συγκεκριμένο φίλτρο υπάρχουν και μερικοί περιορισμοί όπως η τοπική εκτίμηση χωρίς τον εντοπισμό του spoofer κατά την οποία εντοπίζεται η επίθεση αλλά όχι ο επιτιθέμενος κ.α.

Ο τρόπος χρήσης του φίλτρου σε αυτό το κεφάλαιο διαφέρει από πολλές ερευνητικές εργασίες λόγω της μη ύπαρξης στατικού αλλά δυναμικού threshold. Αυτό βοηθάει πολύ στην καλύτερη ανίχνευση των επιθέσεων αλλά και στην αποφυγή ψευδών θετικών (false positive) αποτελεσμάτων. Ιδιαίτερα, σε περιβάλλοντα όπως αυτόνομα οχήματα ή IoT συσκευές, όπου ο εντοπισμός των επιθέσεων πρέπει να γίνεται σε πραγματικό χρόνο και η υπολογιστική ισχύς είναι περιορισμένη, το φίλτρο προσφέρει «ελαφριά» και αποδοτική πρόβλεψη, επιτρέποντας την άμεση ενεργοποίηση ειδοποιήσεων όταν οι μετρήσεις ξεφεύγουν σημαντικά από τις προβλέψεις του μοντέλου. (Dabaghi Daryan, N., Tohidi, S., & Mosavi, 2024; Jin, X. κ.α., 2024; Greg Welch & Gary Bishop, 2006; Kalman, R., 1960; Uhlmann J. & Julier S.J., 2022).



Εικόνα 35: Λειτουργία του φίλτρου Kalman

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

5.2 Μοντέλο συστήματος

Για τον εντοπισμό των επιθέσεων με την χρήση του φίλτρου Kalman εισάγονται τα δεδομένα της ταχύτητας του spoofing scenario του 3ου κεφαλαίου, δηλαδή ύπαρξη ενός επιτιθέμενου, για N=20 κόμβοι. Τα δεδομένα υπόκεινται σε κατάλληλη προεπεξεργασία (π.χ. εξομάλυνση, αναδιάταξη σε διανυσματική μορφή), ώστε να είναι συμβατά με τη μαθηματική αναπαράσταση που απαιτεί το φίλτρο Kalman, και στη συνέχεια εισάγονται για ανάλυση. Ακολουθούν αναλυτικά οι εξισώσεις και οι επεξηγήσεις αυτών για την λειτουργία του φίλτρου καθώς και τα στάδια που υλοποιούνται για το prediction και το update.

1. **State Representation**

$$\text{Εξίσωση κατάστασης:} \quad x_k = \mathrm{A} \cdot x_{k-1} + w_{k-1} \quad (1)$$

$$\text{Εξίσωση μέτρησης:} \quad z_k = \mathrm{H} \cdot x_k + v_k \quad (2)$$

Όπου:

$x_k = state\ vector\ at\ time\ k$

$z_k = observed\ measurement\ (spoofed\ speed)$

$w_{k-1} \sim N(0, Q) = process\ noise\ (Gaussian)$

$v_k \sim N(0, R) = measurement\ noise\ (Gaussian)$

2. **Διάνυσμα κατάστασης:**

$$x_k = \begin{bmatrix} u_k \\ a_k \end{bmatrix} \quad (3)$$

Όπου:

$u_k = ταχύτητα$

$a_k = επιτάχυνση$

3. **Πίνακες:**

$$State\ Transition\ Matrix: \quad A = \begin{bmatrix} 1 & \Delta_t \\ 0 & 1 \end{bmatrix} \quad (4)$$

Ο πίνακας A ονομάζεται πίνακας μετάβασης κατάστασης. Συγκεκριμένα, περιγράφει πως η τρέχουσα κατάσταση $x_{\kappa-1}$ εξελίσσεται στο επόμενο χρονικό βήμα x_κ χωρίς είσοδο

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ελέγχου. Πολλαπλασιάζοντας αυτόν τον πίνακα με το διάνυσμα κατάστασης προκύπτει η νέα ταχύτητα:

$$u_k = u_{k-1} + \Delta t \cdot a_{k-1}$$

Θεωρείται ότι η επιτάχυνση παραμένει σταθερή $\alpha_k = \alpha_{k-1}$, γεγονός που μας οδηγεί στην γραμμική κινηματική εξίσωση:

$$u = u_0 + t \cdot a$$

Ο πίνακας μοντελοποιεί την κίνηση υποθέτοντας σταθερή επιτάχυνση σε ένα χρονικό βήμα $\Delta_t = 1s$

$$Observation\ Matrix: \quad H = [1 \quad 0] \quad (5)$$

Ο πίνακας Η ονομάζεται πίνακας παρατήρησης. Προβάλλει την κατάσταση στο χώρο των μετρήσεων. Δηλώνει ότι μετριέται μόνο η ταχύτητα u_k και όχι η επιτάχυνση. Δηλαδή, $z_k = u_k + \theta\acute{o}\rho\upsilon\beta o\varsigma$.

$$Process\ Noise\ Covariance: \quad Q = 0.1 \cdot I_2 \quad (6)$$

Εισάγει αβεβαιότητα σχετικά με το πόσο εμπιστευόμαστε το μοντέλο διαδικασίας.

$$Measurement\ Noise\ Covariance: \ R = 5 \quad (7)$$

Ορίζει πόσος θόρυβος αναμένεται στις παρατηρούμενες μετρήσεις.

4. Αλγόριθμος φίλτρου Kalman:

Prediction Step:

$$x_{k|k-1} = A \cdot x_{k-1|k-1} \quad (8)$$

$$P_{k|k-1} = A \cdot P_{k-1|k-1} \cdot A^T + Q \quad (9)$$

Update Step:

$$y_k = z_k - H \cdot x_{k|k-1} \quad (Innovation/Residual) \ (10)$$

$$S_k = H \cdot P_{k|k-1} \cdot H^T + R \quad (Innovation\ Covariance) \ (11)$$

$$K_k = P_{k|k-1} \cdot H^T \cdot S_k^{-1} \quad (Kalman\ Gain) \ (12)$$

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

$$x_{k|k} = x_{k|k-1} + K_k + y_k \quad (13)$$

$$P_{k|k} = (I - K_k \cdot H) \cdot P_{k|k-1} \quad (14)$$

5. Residuals and Spoof Detection

Το residual $|y_k|$, το οποίο ονομάζεται επίσης και «καινοτομία» μας δείχνει την απόκλιση της μέτρησης από την εκτίμηση της προηγούμενης κατάστασης και χρησιμοποιείται σε αυτή την τροποποιημένη έκδοση του φίλτρου για την ανίχνευση πιθανής επίθεσης.

$$Residual_k = |z_k - H \cdot \hat{x}_{k|k-1}| \quad (15)$$

Το threshold χρησιμοποιείται για την ανίχνευση

$$Threshold = \mu + 3\sigma \quad (16)$$

Όπου:

$\mu = το\ μέσο\ των\ residuals$

$\sigma = η\ τυπική\ απόκλιση\ των\ residuals$

6. Εάν το residual υπερβαίνει το threshold, ενεργοποιείται ένα alert:

$$Alert_k = \begin{cases} 1, Residual_k > Threshold \\ 0, \quad αλλιώς \end{cases} \quad (17)$$

Τέλος, στο μοντέλο μέτρησης, χρησιμοποιείται η ταχύτητα που στέλνουν σε μορφή WSM τα γειτονικά όχήματα ως μέτρηση με την προσθήκη κάποιου θορύβου λόγω της ασύρματης μετάδοσης. Ακολουθεί ο Πίνακας 8 με τις επεξηγήσεις των συμβόλων:

Πίνακας 8: Επεξηγήσεις συμβόλων αλγορίθμου

Symbol	Meaning
x	State estimate (speed & acceleration)
P	Estimate covariance
z	Measurement (spoofed speed)
y	Residual (innovation)
K	Kalman gain
A	State transition model
H	Observation model
Q	Process noise covariance
R	Measurement noise covariance

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

5.3 Εύρεση Δυναμικού Threshold για Εντοπισμό Επιθέσεων

Σε αυτή την υποενότητα εστιάζουμε λίγο περισσότερο στα στάδια υλοποίησης 4 και 6 του φίλτρου Kalman της ενότητας 5.2, στα οποία υλοποιείται η εύρεση ενός δυναμικού κατωφλίου για τον εντοπισμό των επιθέσεων. Αυτό το δυναμικό κατώφλι (residual threshold) στο πλαίσιο ανίχνευσης spoofing επιθέσεων με χρήση του φίλτρου Kalman ορίζεται με τρόπο ώστε να προσαρμόζεται στατιστικά στις συνθήκες κάθε κόμβου. Συγκεκριμένα, το φίλτρο Kalman παράγει σε κάθε χρονική στιγμή μια εκτίμηση της ταχύτητας, με βάση το μαθηματικό μοντέλο της κίνησης και τα δεδομένα που έχουν προηγηθεί. Η διαφορά μεταξύ της προβλεπόμενης τιμής και της πραγματικής μέτρησης αποτελεί την καινοτομία ή αλλιώς το residual. Η ποσότητα αυτή δείχνει πόσο «μακριά» βρίσκεται μια μέτρηση από αυτό που αναμενόταν σύμφωνα με το μοντέλο.

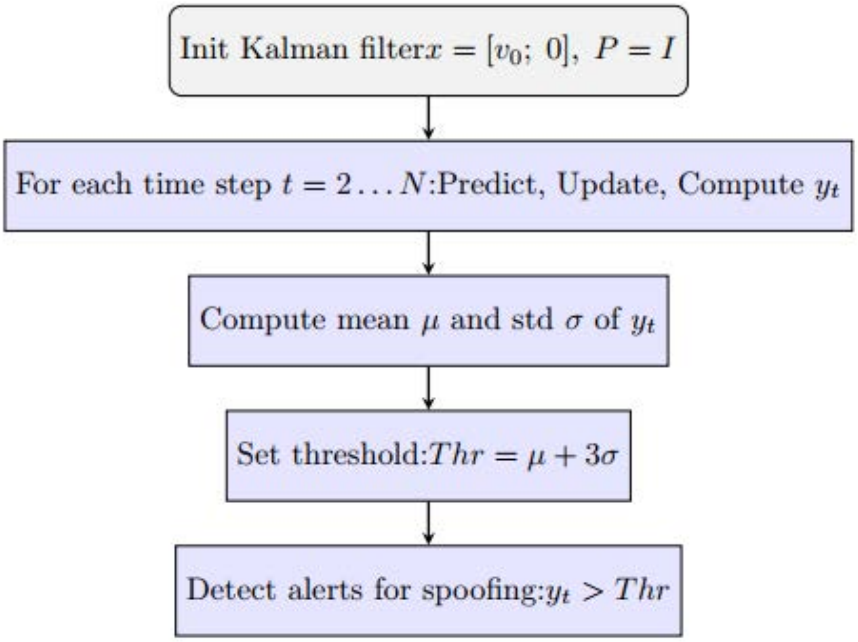
Αφού υπολογιστεί το residual για όλα τα χρονικά βήματα ενός κόμβου, υπολογίζεται η μέση τιμή και η τυπική απόκλισή του. Με βάση αυτά τα δύο στατιστικά, ορίζεται ένα κατώφλι ως το άθροισμα της μέσης τιμής με τρεις φορές την τυπική απόκλιση. Πρόκειται δηλαδή για ένα στατιστικό όριο που καλύπτει περίπου το 99,7% των τιμών αν ο θόρυβος ακολουθεί κανονική κατανομή. Επομένως, εάν κάποιο residual ξεπεράσει αυτό το κατώφλι, θεωρείται εξαιρετικά απίθανο να οφείλεται σε φυσιολογική διακύμανση του συστήματος, και καταγράφεται ως πιθανό spoofing συμβάν. Το κατώφλι αυτό χαρακτηρίζεται ως δυναμικό γιατί επανυπολογίζεται για κάθε κόμβο με βάση τα δικά του residuals, και προσαρμόζεται στις εκάστοτε συνθήκες της μέτρησης και του σεναρίου.

Η παραπάνω προσέγγιση διαφοροποιείται σημαντικά από την κλασική χρήση του φίλτρου Kalman με σταθερό κατώφλι, το οποίο προκύπτει θεωρητικά από την κατανομή του θορύβου και εφαρμόζεται με τη μορφή ελέγχου αξιοπιστίας τύπου x^2. Στην περίπτωση αυτή, το κατώφλι είναι ίδιο για όλους τους κόμβους και δεν προσαρμόζεται στη μεταβαλλόμενη φύση των δεδομένων ή των αισθητήρων. Αντίθετα, η δυναμική προσέγγιση επιτρέπει σε κάθε κόμβο να «εκπαιδευτεί» στα δικά του χαρακτηριστικά θορύβου και να θέτει πιο ρεαλιστικά και εξατομικευμένα όρια για την ανίχνευση επιθέσεων. Με αυτόν τον τρόπο, αυξάνεται η ευαισθησία του συστήματος στα πραγματικά spoofing σήματα και μειώνονται οι ψευδείς συναγερμοί που συχνά προκύπτουν από σταθερά και γενικευμένα όρια.

Η υλοποίηση του δυναμικού κατωφλίου επιτυγχάνεται χωρίς να απαιτείται πρόσθετη πολυπλοκότητα, καθώς τα στατιστικά στοιχεία εξάγονται απευθείας από τα residuals που

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

ήδη υπολογίζονται στο πλαίσιο του φίλτρου. Συνολικά, η τεχνική αυτή ενσωματώνει μια απλή αλλά αποτελεσματική μορφή στατιστικής νοημοσύνης στο σύστημα, βελτιώνοντας την προσαρμοστικότητα και την ακρίβεια της ανίχνευσης επιθέσεων spoofing στα συστήματα CAV. Η αναπαράσταση της παραπάνω διαδικασία φαίνεται στο παρακάτω διάγραμμα ροής της Εικόνα 36.



Εικόνα 36: Διάγραμμα ροής δυναμικού threshold

5.4 Αποτελέσματα

Αυτή η υποενότητα εστιάζει στα αποτελέσματα του αλγορίθμου του φίλτρου Kalman. Τα αποτελέσματα παρουσιάζονται ως γραφήματα

1) **ταχύτητας,** περιέχοντας την ταχύτητα υπό κανονικές συνθήκες, υπό συνθήκες επίθεσης spoofing και την πρόβλεψη του φίλτρου,

2) **residual**, δηλαδή της καινοτομίας του φίλτρου που περιγράφει την διαφορά μεταξύ της τιμής της μέτρησης και της τιμής της πρόβλεψης. Σε αυτό το γράφημα φαίνεται με κόκκινο χρώμα το δυναμικό threshold πάνω από το οποίο ανιχνεύεται η επίθεση.

3) **alerts,** τα οποία περιγράφουν τις ειδοποιήσεις του αποτελέσματος του φίλτρου όταν εντοπίζονται οι επιθέσεις.

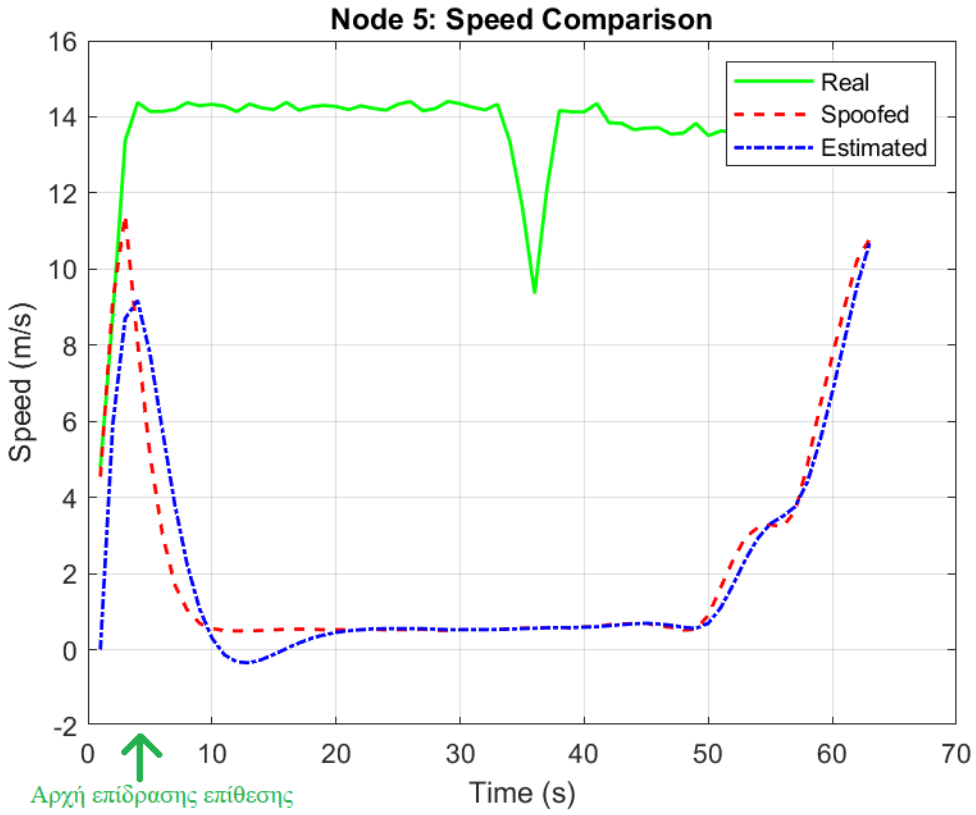
Η Εικόνα 37, η Εικόνα 38 και η Εικόνα 39 αναφέρονται στα αποτελέσματα του φίλτρου για το Node 5. Με βάση τα γραφήματα φαίνεται πως το estimation του μοντέλου σε

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

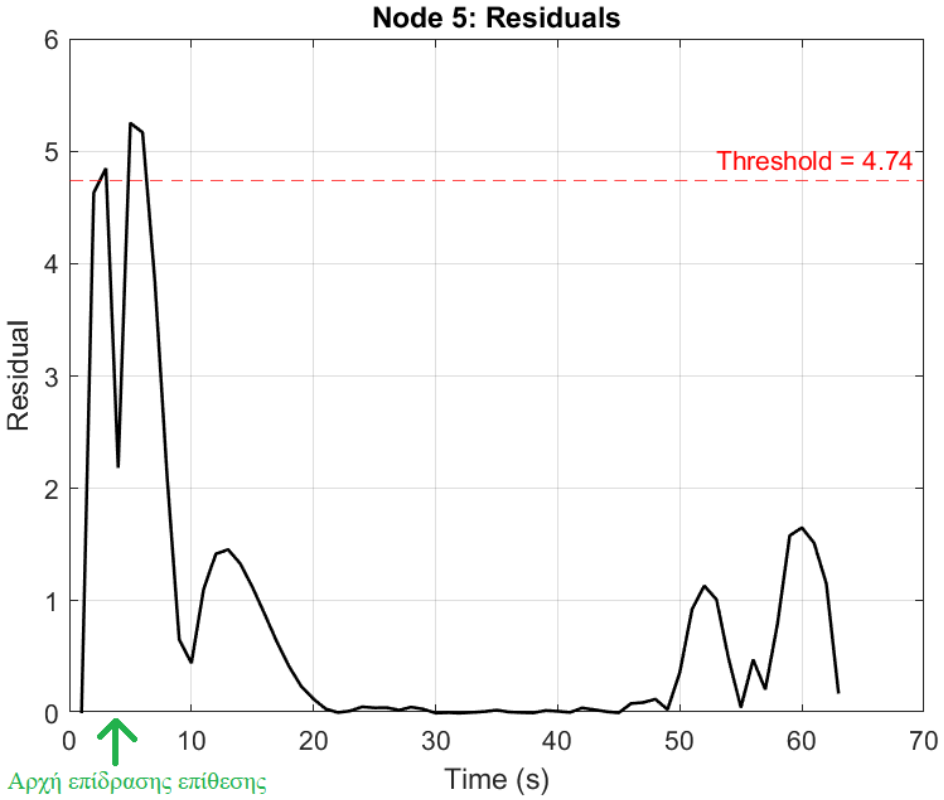
αυτό το σύστημα δεν λειτουργεί υποδειγματικά, εξαιτίας του γεγονότος ότι το correction βασίζεται στις προηγούμενες (prior) εκτιμήσεις οι οποίες έχουν αλλοιωθεί από τον spoofer. Ωστόσο, τα residuals και τα alerts δείχνουν πως εντοπίζεται η αρχή της επίδρασης της επίθεσης και στο σωστό χρόνο. Ο χρόνος σε αυτά τα γραφήματα αρχίζει από την στιγμή που το όχημα εισάγεται στην διμοιρία (platoon). Δηλαδή σε σύγκριση με τα γραφήματα των προηγούμενων κεφαλαίων ο Node 5 επηρεάζεται από την επίθεση περίπου 5 δευτερόλεπτα μετά την είσοδο του στη διμοιρία. Αυτό αποδεικνύεται από τα παρακάτω γραφήματα και κυρίως από τα alerts. Επομένως, για τα δεδομένα που χρησιμοποιήσαμε, το φίλτρο έχει σχεδόν 100% detection accuracy. Στα γραφήματα απεικονίζεται ενδεικτικά μόνο ο Node 5 καθώς οι υπόλοιποι κόμβοι παρουσιάζουν παρόμοια συμπεριφορά.

Ο προτεινόμενος αλγόριθμος του φίλτρου Kalman επιτυγχάνει την ανίχνευση επιθέσεων spoofing βασισμένος στα residuals, ωστόσο εντοπίζει κυρίως το χρονικό σημείο έναρξης της επίθεσης και όχι όλο το χρονικό διάστημα διάρκειάς της. Ως μελλοντική εργασία και στο πλαίσιο ενός πιο εξελιγμένου συστήματος, είναι αναγκαίο να ενσωματωθούν διάφορες τεχνικές μία εκ των οποίων είναι η ήπια εξασθένηση της μέτρησης (soft measurement weakening). Αυτή η τεχνική παρουσιάζεται αναλυτικά στην ερευνητική εργασία των Jin et al. Οι ερευνητές αναφέρουν ότι όταν μια μέτρηση θεωρείται ύποπτη, αντί να απορρίπτεται πλήρως από το φίλτρο, μειώνεται σταδιακά η επιρροή της στη διαδικασία ενημέρωσης κατάστασης μέσω δυναμικής προσαρμογής του Kalman gain. Έτσι, το σύστημα παραμένει ευαίσθητο σε αλλαγές και εξακολουθεί να παρακολουθεί τις αποκλίσεις σε βάθος χρόνου, βελτιώνοντας την ικανότητα του φίλτρου να παρακολουθεί τη διάρκεια ολόκληρης της επίθεσης (Jin κ.α., 2024). Τέλος, υπάρχουν και άλλες παρόμοιες τεχνικές οι οποίες εξελίσσονται από πολλούς ερευνητές και θα προσφέρουν μεγαλύτερη ακρίβεια και μετριασμό των επιθέσεων. Έτσι, με αυτόν τον τρόπο θα ενισχυθεί η ασφάλεια των αυτόνομων οχημάτων, θα μειωθούν οι επιθέσεις και τα οχήματα θα γίνουν ασφαλέστερα για τους χρήστες τους.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

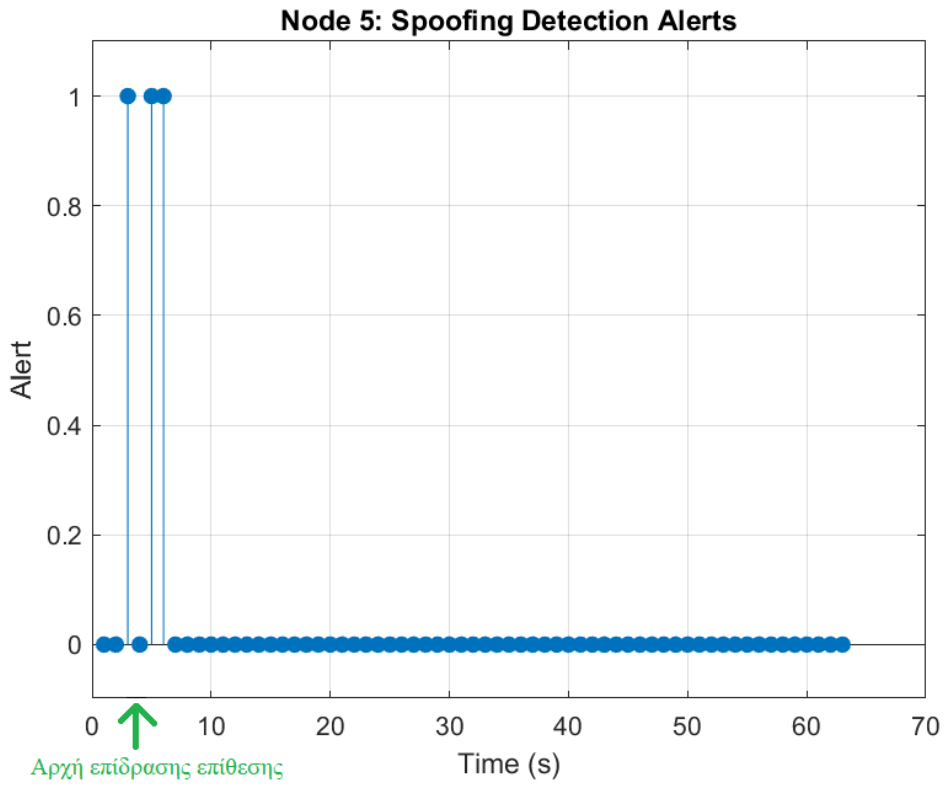


Εικόνα 37: Σύγκριση ταχυτήτων για το Node 5



Εικόνα 38: Residual φίλτρου Kalman για το Node 5

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Εικόνα 39: Alerts του φίλτρου Kalman για το Node 5

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

6 Συμπεράσματα

Με την ταχεία ανάπτυξη των τεχνολογιών και της έρευνας στην επιστήμη και τη μηχανική, η κυκλοφορία πλήρως αυτόνομων οχημάτων κοντεύει να αποτελεί μέρος της καθημερινότητάς μας. Τα CAV βοηθούν στη μείωση των τροχαίων ατυχημάτων, στη βελτίωση της ποιότητας ζωής και στην προώθηση της αποτελεσματικότητας των συστημάτων μεταφοράς. Ωστόσο, υπάρχουν διάφορες προκλήσεις όσον αφορά την ασφάλεια και την ιδιωτικότητα στο περιβάλλον των CAV. Η παρούσα διπλωματική εργασία αναφέρθηκε τόσο στις κυβερνοεπιθέσεις των αυτόνομων οχημάτων όσο και στην μελέτη των επιπτώσεων τους. Το 2ο κεφάλαιο της διπλωματικής εργασίας εστίασε στην ανάλυση των διάφορων μορφών επιθέσεων και στην παρουσίαση προτεινόμενων αντίμετρων για τα συστήματα CAV και το δίκτυο VANET. Για την συγγραφή του χρησιμοποιήθηκαν άρθρα από επιστημονικά περιοδικά και βιβλία πληρώντας κάποια κριτήρια ένταξης. Τέτοια κριτήρια ήταν η συνάφεια με το θέμα της διπλωματικής, η ημερομηνία συγγραφής τους να είναι η τελευταία πενταετία, να είναι δημοσιευμένα από έγκριτους εκδοτικούς οίκους κ.α.

Στη συνέχεια διεξήχθη μία μελέτη επιπτώσεων και εντοπισμού των επιθέσεων άρνησης υπηρεσίας (DoS) στα CAV. Η προσέγγιση αυτή χρησιμοποιεί ένα πραγματικό σενάριο προσομοίωσης κυκλοφορίας μέσω διάφορων εργαλείων όπως το OMNeT++, το INET, το VEINS και το SUMO. Αναπτύχθηκε ένα ισχυρό πλαίσιο προσομοίωσης για ένα δίκτυο οχημάτων σε πραγματικό χρόνο που αποτελείται από έναν αριθμό οχημάτων και μια RSU. Αυτό το πλαίσιο προσομοίωσης αντιμετωπίζει επιδέξια την πολυπλοκότητα των VANET, ιδίως στις επικοινωνίες οχήματος προς όχημα, και διερευνά τα τρωτά σημεία που μπορεί να έχουν τα συνδεδεμένα οχήματα σε επιθέσεις DoS από κακόβουλους χρήστες. Τα ευρήματα καταδεικνύουν σημαντική αύξηση της απόστασης οδήγησης υπό την επίδραση μιας επίθεσης spoofing, ενώ ταυτόχρονα, μια διερεύνηση άλλων επιπέδων της στοίβας δικτύου (π.χ. PDR) δείχνει επίσης πιθανές αδυναμίες απέναντι σε μια επίθεση spoofing, καθώς αυξάνονται αρκετά τα WSM μηνύματα που ανταλλάσσονται. Αυτό είναι ένα στοιχείο που μπορεί να βοηθήσει στην ευκολότερη αναγνώριση ενός εισβολέα σε ένα μελλοντικό σύστημα ανίχνευσης. Ακόμη, στο 5ο κεφάλαιο αναλύθηκε ένα πρώιμο σύστημα εντοπισμού των επιθέσεων με χρήση του φίλτρου Kalman.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Συνοψίζοντας, σε σύγκριση με την τρέχουσα βιβλιογραφία, παρατηρείται ότι δεν υπάρχει αντίστοιχη εργασία με ένα ρεαλιστικό πλαίσιο προσομοίωσης όπως αυτό που προτείνεται σε αυτήν την εργασία που να λαμβάνει υπόψη τις πραγματικές συνθήκες κυκλοφορίας. Επίσης, οι τιμές της συνάρτησης μεταβλητότητας CoV δεν είναι εντελώς κοντά στο μηδέν, λόγω απρόβλεπτων καταστάσεων. Σε αντίθεση με τις ερευνητικές εργασίες των Khattak et.al. και των Krishna K. & Reddy K. οι οποίες ακολουθούν μια θεωρητική προσέγγιση. Όταν υλοποιείται μια επίθεση DoS, η μεταβλητότητα της ταχύτητας και της επιτάχυνσης παρουσιάζει μια μικρή αύξηση, οδηγώντας σε μεγαλύτερες τιμές CoV.

Αυτή η διπλωματική εργασία αντιπροσωπεύει μια πρώιμη έκδοση ενός μελλοντικού ολιστικού μοντέλου που, εκτός από την υλοποίηση επιθέσεων DoS, θα περιέχει επίσης ένα σύστημα ανίχνευσης επιτιθέμενων σε πραγματικό χρόνο χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης. Οι υλοποιημένες επιθέσεις θα δοκιμαστούν, ακόμη με στοχαστικά μοντέλα εισόδου όπως ο ρυθμός άφιξης των οχημάτων, θα διερευνηθούν μέθοδοι για την επαλήθευση της ταυτότητας των μελών μιας διμοιρίας οχημάτων με παθητικές μεθόδους εκτίμησης παραμέτρων σε φυσικό επίπεδο όπως η σχετική ταχύτητα, ώστε τα οχήματα να μπορούν να κάνουν διασταύρωση με τις πληροφορίες που ανταλλάσσονται μέσω των μηνυμάτων. Απώτερος σκοπός είναι οι μελλοντικές μέθοδοι ανίχνευσης να βασίζονται σε τεχνικές Τεχνητής Νοημοσύνης. Τέλος, πολλοί ερευνητές αλλά και πολλές αυτοκινητοβιομηχανίες πραγματοποιούν έρευνες για την αντιμετώπιση των επιθέσεων, την μείωση των ευπαθειών και την εξέλιξη τόσο των αυτόνομων οχημάτων όσο και των δυνατοτήτων του δικτύου VANET. Μέσα από όλα αυτά μπορεί να δημιουργηθεί ένας νέος δρόμος για την κυβερνοασφάλεια των CAV.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Βιβλιογραφία

[1] A. Amirkhani, M.P. Karimi, A. Banitalebi-Dehkordi, "A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles", Springer-Verlag, 2022

[2] N. Dabaghi Daryan, S. Tohidi, & M. R. Mosavi, "Intelligent mitigation of GPS spoofing using the Kalman filter in the tracking loop based on multi-correlator", Survey Review, 2024.

[3] P.G. Gipps, "A behavioural car-following model for computer simulation.", Transp. Res. Part B Methodol. 1981

[4] IEEE. "IEEE Draft Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Enhancements for Positioning", IEEE: Piscataway, 2019.

[5] X .Jin, X. Zhang, S. Li, S. Zheng, "Detection of slowly varying spoofing using weighted Kalman gain in GNSS/INS tightly coupled systems", GPS Solut, 2024.

[6] R. Kalman, "A New Approach to Linear Filtering and Prediction Problems", ASME Journal of Basic Engineering, 1960.

[7] M. Kamal, A. Barua, C. Vitale, C. Laoudias and G. Ellinas, "GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles," IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021

[8] Z. H. Khattak, B. L. Smith, M. D. Fontaine, "Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes", Accident Analysis & Prevention, 2021

[9] A. Khelifi, M. A. Talib, D. Nouichi, M.S. Eltawil, "Toward an Efficient Deployment of Open-Source Software in the Internet of Vehicles Field" Arabian Journal for Science and Engineering, 2019

[10] K. Kim, J.S. Kim, S. Jeong, J.H. Park, H.K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense", Elsevier Ltd., 2021

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

[11] A. Kloukiniotis, A. Papandreou, A. Lalos, P. Kapsalas, D.-V. Nguyen, K. Moustakas, "Countering Adversarial Attacks on Autonomous Vehicles Using Denoising Techniques: A Review", IEEE Journal of Intelligent Transportation Systems, 2022

[12] D. Kosmanos, A.Pappas, L. Maglaras, S. Moschoyiannis, F.J. Aparicio-Navarro, A.Argyriou, H Janicke, "A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles." Array, 2020

[13] D. Kosmanos, A. Pappas, F.J. Aparicio-Navarro, L. Maglaras, H. Janicke, E. Boiten A. Argyriou, "Intrusion Detection System for Platooning Connected Autonomous Vehicles. " 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2019

[14] I. Koukoutsis, "Εξομοίωση με το software VEINS και ανάλυση αποτελεσμάτων", Bachelor Thesis, University of Thessaly, 2022

[15] P.A. Laplante, M. Kassab, NL. Laplante, JM. Voas, "Building Caring Healthcare Systems in the Internet of Things", IEEE Syst J., 2018

[16] T. Limbasiya, K.Z. Teng, S. Chattopadhyay, J. Zhou, "A Systematic Survey of Attack Detection and Prevention in Connected and Autonomous Vehicles", Elsevier, 2022

[17] M. Masood, Z. Saeed, M.U. Khan, "A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs)", Journal on Advanced Research in Electrical Engineering (JAREE), 2023

[18] M. Nahri, A. Boulmakoul, L. Karim, A. Lbath, "IoV distributed architecture for real-time traffic data analytics", Elsevier, 2018

[19] A. Nanda, D. Puthal, J.J.P.C. Rodrigues, S.A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions", IEEE Wireless Communications, 2019

[20] N. Sharma, N. Chauhan, N. Chand, "Security challenges in Internet of Vehicles (IoV) environment", First International Conference on Secure Cyber Computing and Communication (ICSCCC), 2018

[21] C. Sommer, R. German, F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis", IEEE Trans. Mob. Comput. 2011.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

[22] X. Sun, F. R. Yu and P. Zhang, "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)," IEEE Transactions on Intelligent Transportation Systems, 2022

[23] Z. Sun, R. Liu, H. Hu, D. Liy, Z. Yan, "Cyberattacks on connected automated vehicles: A traffic impact analysis", IET Intelligent Transport Systems, 2022

[24] D. Takahashi, "Subaru Legacy 2020 review: Sensors that detect a drowsy or distracted driver", venturebeat.com, 2020

[25] M.A. Talib, S. Abbas, Q. Nasir, M.F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security", International Journal of Distributed Sensor Networks, 2018

[26] C.K. Toh, "Research Challenges in Intelligent Transportation Networks", Nanyang Technological University, 2008

[27] M. Treiber, A. Kesting, "Chapter 16: Calibration and Validation" In Traffic Flow Dynamics: Data, Models and Simulation, Springer, 2013

[28] Z.-R. Tzoannos, "Security Challenges and Attacks Classifications in Autonomous Vehicles and IoV Systems ", Bachelor Thesis, University of Thessaly, 2023

[29] Z.-R. Tzoannos, D. Kosmanos, A. Xenakis, C. Chaikalis, "The Impact of Spoofing Attacks in Connected Autonomous Vehicles under Traffic Congestion Conditions." Telecom, 2024

[30] J. Uhlmann, S.J. Julier, "Gaussianity and the Kalman Filter: A Simple Yet Complicated Relationship", Jou. Cie. Ing., 2022.

[31] K. Vamshi Krishna, K. Ganesh Reddy, "Classification of Distributed Denial of Service Attacks in VANET: A Survey", Wireless Pers Commun, 2023

[32] X. Wang, A.J. Khattak, J. Liu, G. Masghati-Amoli, S. Son, "What is the level of volatility in instantaneous driving decisions? " Transp. Res. Part C Emerg. Technol. 2015

[33] Z. Wang, H. Wei, J. Wang, X. Zeng, Y. Chang, "Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey", Sustainability, 2022

[34] G. Welch, G. Bishop, "An Introduction to the Kalman Filter", 2006, https://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Δημοσίευση

Το 3ο κεφάλαιο της παρούσας διπλωματικής εργασίας έχει δημοσιευθεί στο επιστημονικό περιοδικό Telecom του εκδοτικού οίκου MDPI.

Tzoannos, Z.-R.; Kosmanos, D.; Xenakis, A.; Chaikalis, C. The Impact of Spoofing Attacks in Connected Autonomous Vehicles under Traffic Congestion Conditions. *Telecom* **2024**, *5*, 747-759. https://doi.org/10.3390/telecom5030037

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Παράρτημα

Στο παράρτημα αυτό παρατίθεται ο οδηγός εγκατάστασης των λογισμικών που χρησιμοποιούνται για τα σενάρια προσομοίωσης των επιθέσεων Spoofing.

Το Veins μπορεί να τρέξει σε Linux, Mac OS X και Windows περιβάλλοντα. Προτιμάται όμως το Linux λόγω των εκτεταμένων δυνατοτήτων debugging που προσφέρει. Για να κατασκευαστεί σε Linux χρειάζεται πρώτα να εγκατασταθούν κάποια πακέτα με την παρακάτω εντολή στο τερματικό :

```
sudo apt-get install build-essential gcc g++ bison flex perl tcl-dev tk-dev
blt libxml2-dev zlib1g-dev default-jre doxygen graphviz libwebkitgtk-1.0-0
openmpi-bin libopenmpi-dev libpcap-dev autoconf automake libtool libproj-dev
libgdal1-dev libfox-1.6-dev libgdal-dev libxerces-c-dev qt4-dev-tools
```

Στο Mac OS X θα χρειαστεί να εγκατασταθούν τα αντίστοιχα πακέτα μέσω Macports τρέχοντας την εντολή στο τερματικό :

```
sudo port install bison zlib tk blt libxml2 libtool xercesc3 proj gdal fox
```

Η εγκατάσταση που επιλέχθηκε ήταν στα Windows.

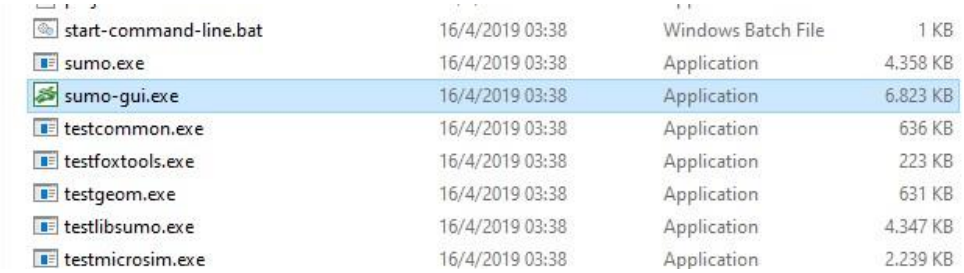
Υποθέτοντας ότι το home directory είναι το C:\Users\user και το απαραίτητο software θα εγκατασταθεί στον φάκελο C:\Users\user\src (ο οποίος έχει δημιουργηθεί) τα βήματα είναι τα εξής.

Βήμα πρώτο

Κατεβάζετε το Sumo 1.9.2 και κάνετε αποσυμπίεση στον φάκελο C:\Users\user\src\sumo-1.9.2 στον οποίο μέσα θα βρείτε το αρχείο C:\Users\user\src\sumo-1.9.2\bin\sumogui.exe.

Εδώ ας σημειωθεί ότι οι συντομότερες εκδόσεις του Sumo προϋποθέτουν να είναι εγκατεστημένο το Microsoft Visual C++ 2010 Redistributable Package (x86).

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

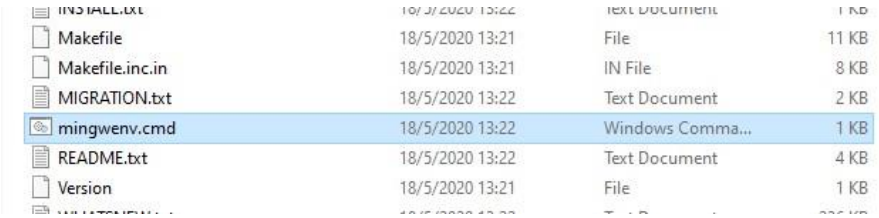


Προσοχή πρέπει να δοθεί και στην έκδοση του Sumo, πρέπει να χρησιμοποιηθεί η συγκεκριμένη έκδοση για το Veins-5.0.

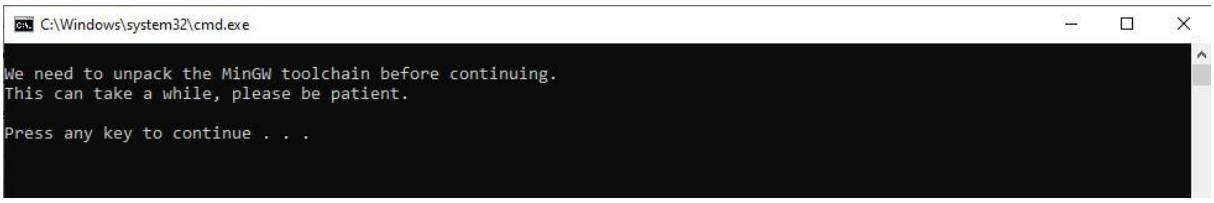
Βήμα δεύτερο

Κατεβάζετε το OMNeT++ 5.6.2 for Windows και το κάνετε αποσυμπίεση στον φάκελο C:\Users\user\src\omnetpp-5.6.2.. Σημείωση ότι πρέπει να μην υπάρχουν κενά στο όνομα του φακέλου. Μέσα στον φάκελο θα πρέπει να βρείτε το Script :

```
C:\Users\user\src\omnetpp-5.6.2\mingwenv.cmd
```



Τρέχοντάς το βλέπετε ένα περιβάλλον MinGW το οποίο μοιάζει με το terminal του Linux.



Για να κάνετε Build το OmneT++ 5.6.2 θα πρέπει να γράψετε την εντολή :

```
./configure
```

Και μετά την εντολή :

```
make
```

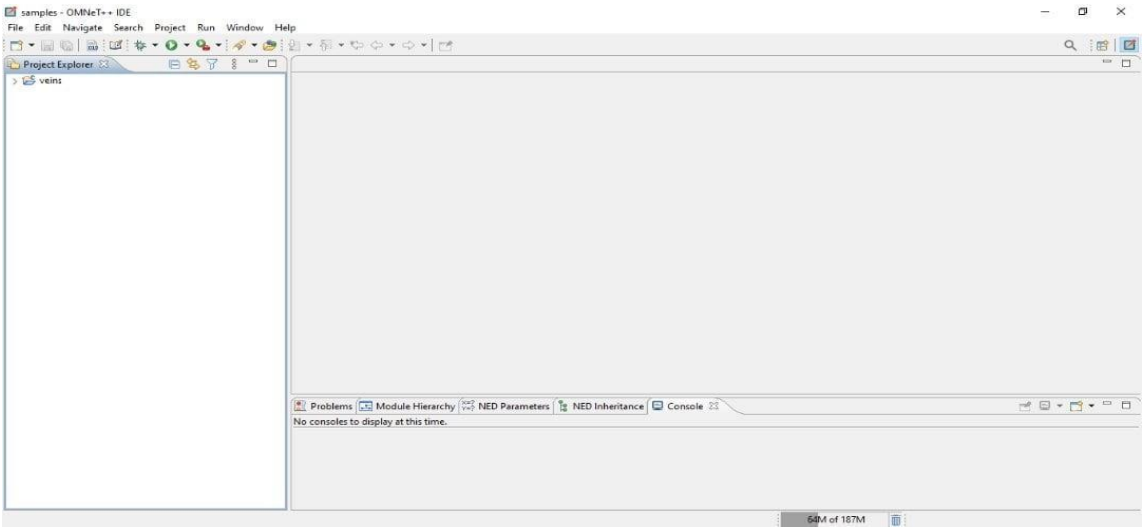
για να ξεκινήσει η διαδικασία της εγκατάστασης η οποία θα διαρκέσει μερικά λεπτά. Όταν ολοκληρωθεί και όλα έχουν πάει καλά το αποτέλεσμα θα είναι το

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

/c/Users/user/src/omnetpp-5.6.2/bin/omnetpp. Για να τρέξετε το OMNeT πληκτρολογήστε την εντολή :

```
omnetpp
```

Αυτό θα ανοίξει το OMNeT++ IDE. Όλα αυτά υπό την προϋπόθεση ότι έχει επιλεχθεί το C:\ Users\user\src\omnetpp-5.6.2\samples ως workspace.

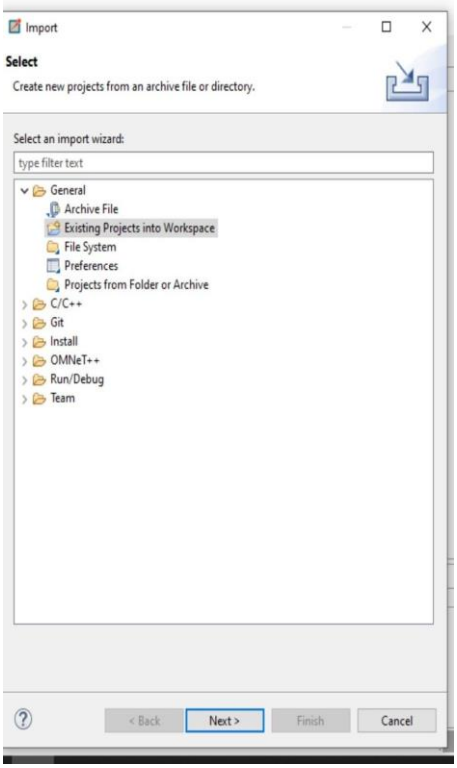


Εικόνα 40: Περιβάλλον OMNeT++.

Βήμα τρίτο

Κατεβάστε και το Veins 5.0 και αποσυμπιέστε στον φάκελο C:\Users\user\src\veins-5.0. Εισάγετε το project στο OMNeT++ IDE workspace πατώντας File > Import > General: Existing Projects into Workspace και επιλέξτε τον φάκελο που κάνατε αποσυμπίεση το Framework

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Κάντε build το project επιλέγοντας Project > Build All στο περιβάλλον του OMNeT++5.6.2. Αφού δημιουργηθεί το project είστε έτοιμοι να τρέξετε την πρώτη IVC προσομοίωση.

Βήμα τέταρτο

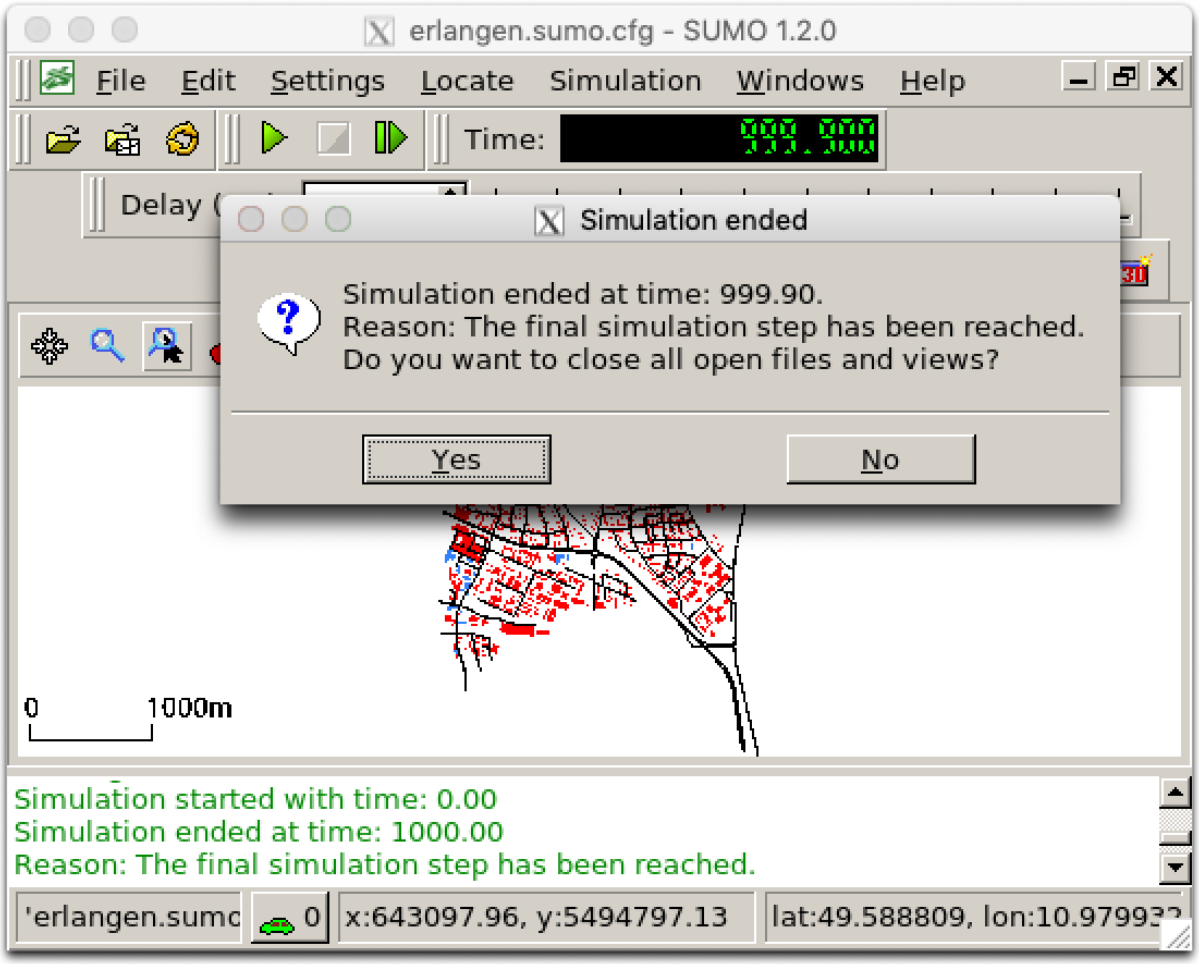
Σιγουρευτείτε ότι το Sumo λειτουργεί πηγαίνοντας στο τερματικό MinGW του OMNeT++ αλλάξτε το τρέχον directory σε /c/Users/user/src/veins-5.0/examples/veins/ χρησιμοποιώντας της εξής εντολή: cd ../veins-5.0/examples/veins. Έπειτα τρέξτε αυτήν την εντολή για να ξεκινήσει το Sumo.

```
/c/Users/user/src/sumo-1.9.2/bin/sumo.exe -c erlangen.sumo.cfg
```

Στην συνέχεια θα πρέπει να δείτε μια γραμμή που λέει "Loading configuration... done.", στην συνέχεια μετά από λίγο δεν θα εμφανιστεί κάτι άλλο στην γραμμή εντολών.

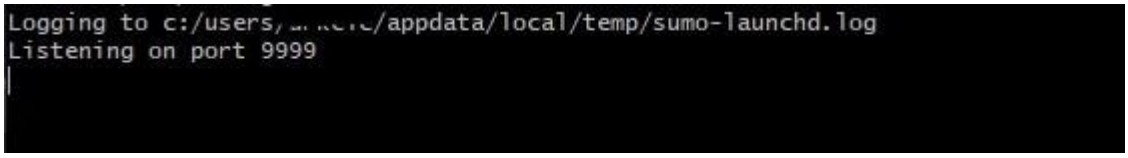
Εάν εγκαταστήσατε σε άλλο path το Sumo, να θυμάστε ποια εντολή χρησιμοποιήσατε αντί του /c/Users/user/src/sumo-1.9.2/bin/sumo.exe. Θα χρειαστεί να προσθέσετε αυτήν την εντολή στην -c επιλογή του sumo-launchd.py του επόμενου βήματος.

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250



Τελευταίο βήμα είναι να τρέξετε το σενάριο του Veins. Αρχικά ανοίγετε το OMNeT++ και στην συνέχεια πληκτρολογείτε την παρακάτω εντολή στην γραμμή εντολών (python script).

```
/c/Users/user/src/veins-5.0/sumo-launchd.py -vv -c /c/Users/user/src/sumo-1.9.2/bin/sumo.exe
```

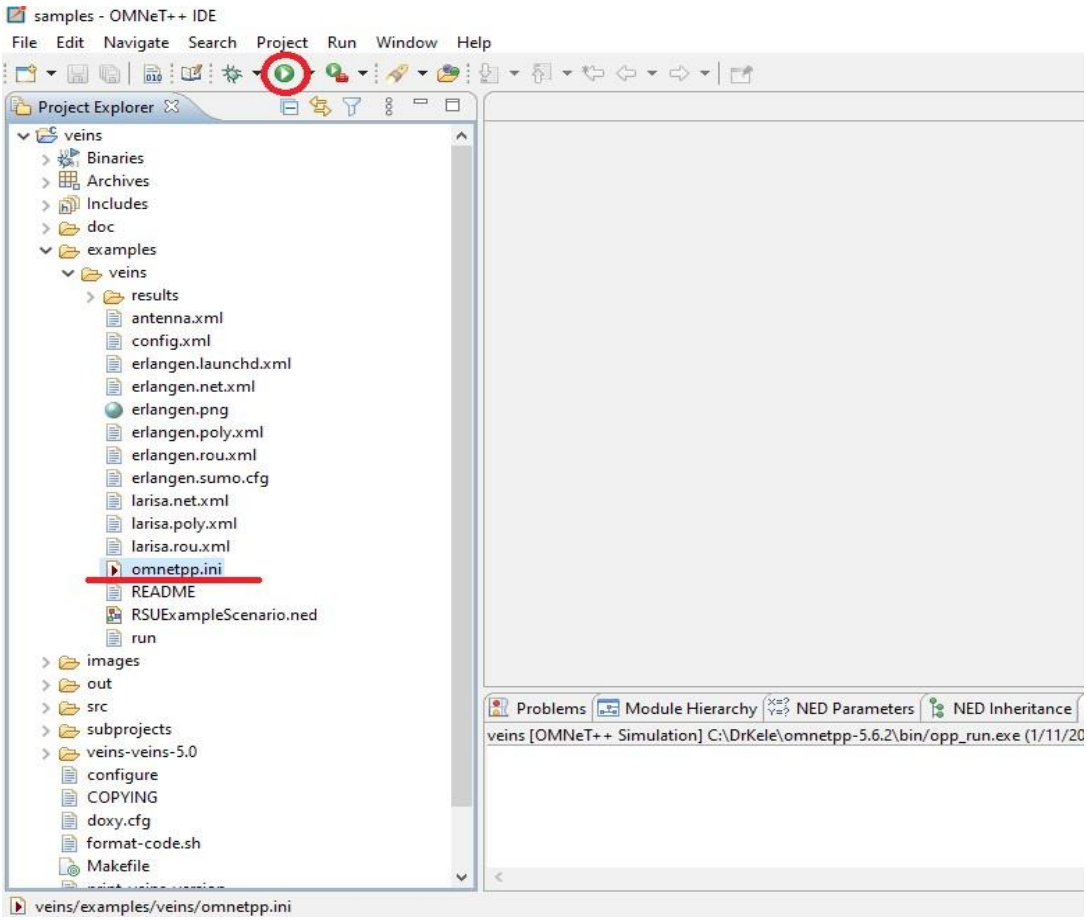


Εικόνα 41: Μετά την ενεργοποίηση του script

Αυτό το script θα δώσει την εντολή να ξεκινήσουν TCP συνδέσεις μεταξύ του OMNeT++ και του Sumo, δημιουργώντας ένα νέο αντίγραφο της προσομοίωσης Sumo για κάθε προσομοίωση που συνδέεται με το OMNeT++. Μόλις ενεργοποιήσετε το Script, αφήστε ανοιχτό το τερματικό και συνεχίστε στο OMNeT++ IDE.

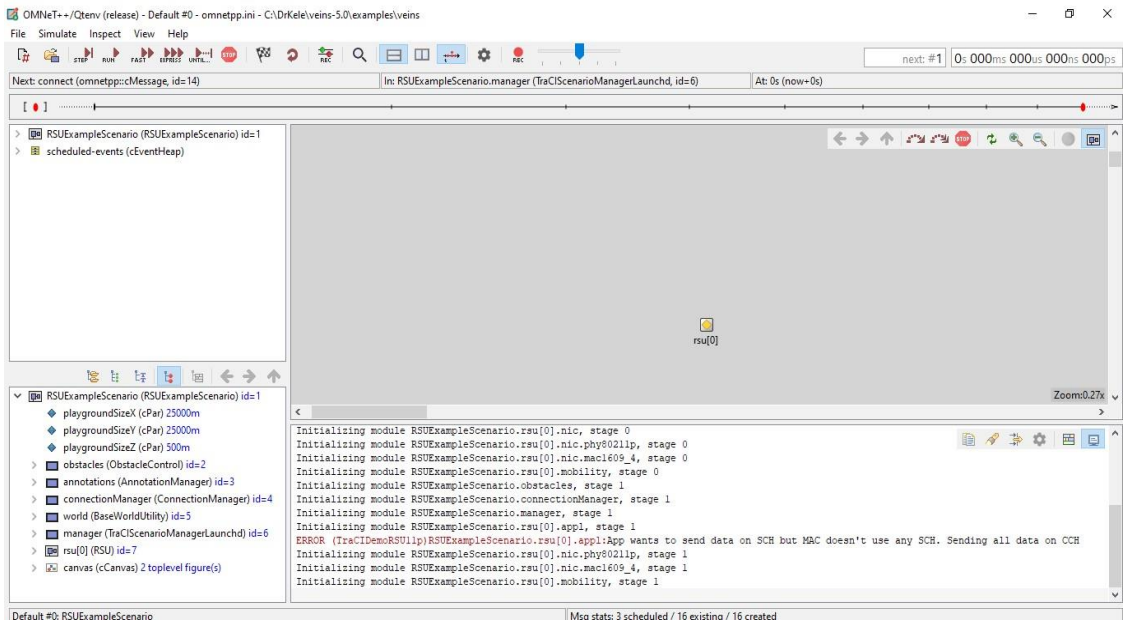
Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Στο IDE τρέξτε το σενάριο του Veins κάνοντας δεξί κλικ στο εξής path veins-5.0/examples/veins/omnetpp.ini στο παράθυρο αριστερά. Στην συνέχεια επιλέγετε Run As > OMNeT++ simulation. Μην ξεχάσετε να δώσετε πρόσβαση στο Sumo σε οποιοδήποτε Firewall χρησιμοποιείτε. Παρομοίως με το προηγούμενο παράδειγμα, αυτό πρέπει να δημιουργήσει και να ανοίξει ένα δεύτερο παράθυρο. Στην συνέχεια μπορείτε να ξανά τρέξετε την προσομοίωση πατώντας το πράσινο “play” button στο OMNeT++ IDE.



Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

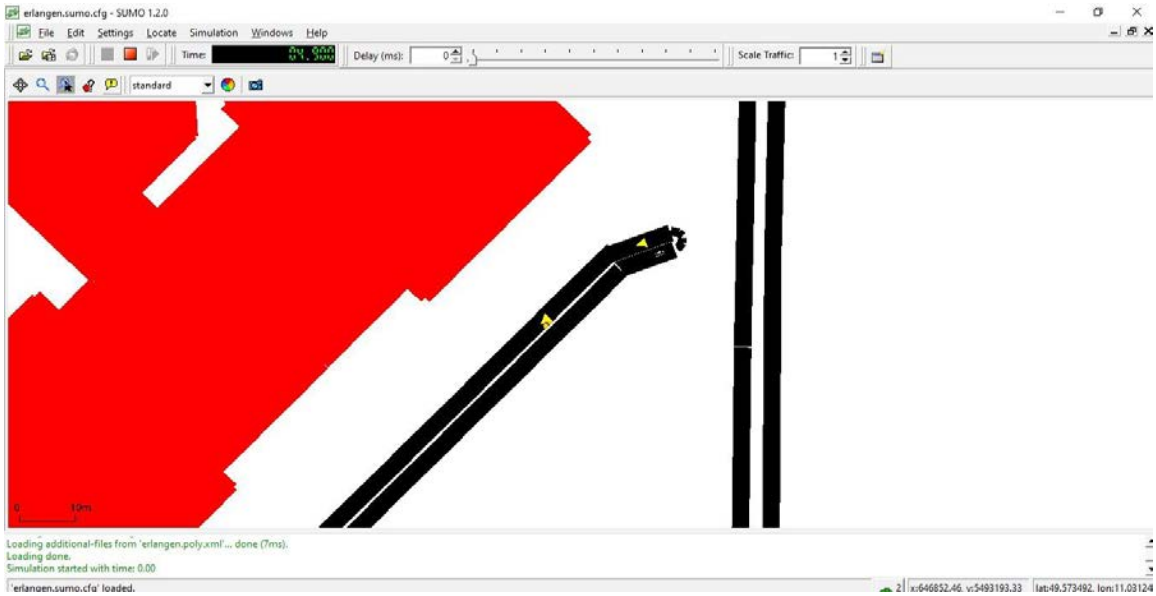
Στην Εικόνα 42 διακρίνεται με κόκκινο σημάδι το play button και το σενάριο προς υλοποίηση.



Εικόνα 42: Περιβάλλον OMNET++

Σε αυτήν την εικόνα παρουσιάζεται το παράθυρο που ανοίγει όταν πατήσετε το play button. Αν μέχρι εδώ όλα πήγαν σωστά θα πρέπει να ανοίξει η προσομοίωση στο sumo μόλις πατήσετε το Run. Εκεί θα δείτε έναν χάρτη (erlangen) και μια σειρά οχημάτων να εκτελούν ένα σενάριο στο οποίο θα γίνεται ένα ατύχημα.

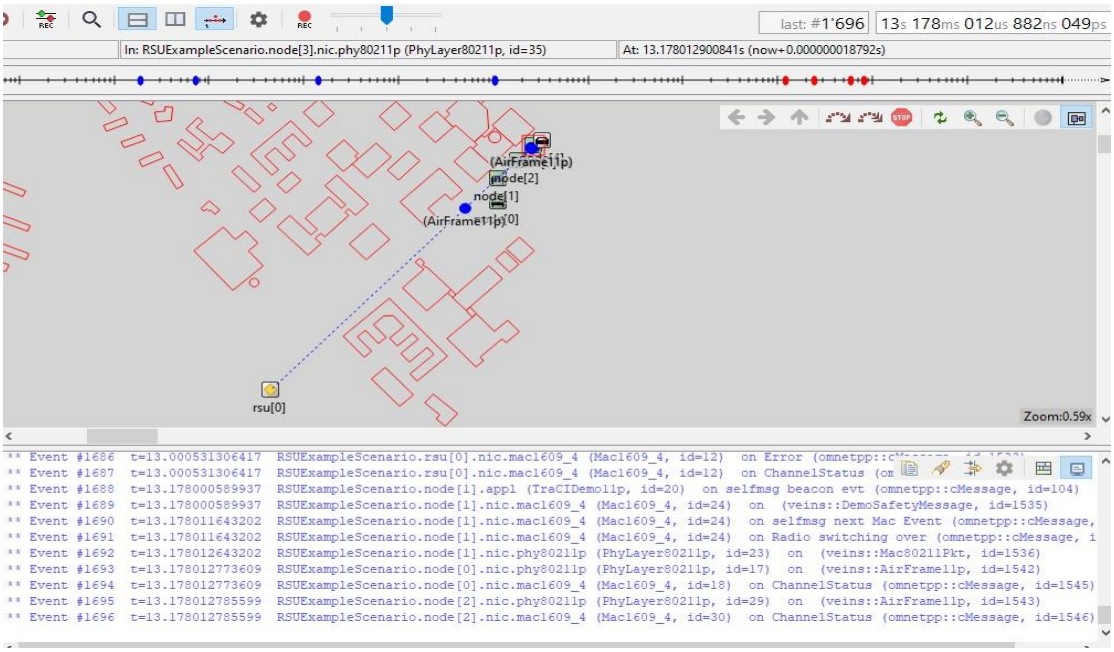
Στην Εικόνα 43 φαίνεται το σημείο εκκίνησης των οχημάτων που συμμετέχουν στο σενάριο.



Εικόνα 43: Αναδυόμενο παράθυρο Sumo

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250

Στην Εικόνα 44 φαίνονται τα οχήματα και τα μηνύματα που ανταλλάσσουν μεταξύ τους (OMNeT++ IDE).



Εικόνα 44: Ανταλλαγή μηνυμάτων μεταξύ των οχημάτων στο περιβάλλον OMNeT ++

Επίσης μπορείτε να τρέξετε το σενάριο σε debug mode. Αυτό μπορείτε να το κάνετε επιλέγοντας debug as αντί του Run as όταν τρέχετε την προσομοίωση κάνοντας δεξί κλικ στο omnetpp.ini. Κάνοντας το θα δείτε πολλές πληροφορίες στο τερματικό, ωστόσο η προσομοίωση θα εκτελεσθεί με χαμηλότερη ταχύτητα. Αν ενδιαφέρεστε να δείτε τον πηγαίο κώδικα της εφαρμογής που εκτελείται στα προσομοιωμένα οχήματα, ελέγξτε το αρχείο omnetpp.ini και θα δείτε ότι είναι TraCIDemo11p. Ο κώδικας του βρίσκεται στο αρχείο src/veins/modules/application/traci/TraCIDemo11p.cc. Μπορείτε να δείτε την μέθοδο handlePositionUpdate η οποία καθορίζει πως αντιδρά ένα όχημα όταν λαμβάνεται ένα position update από το Sumo, ελέγχοντας αν έμεινε ακίνητο για αρκετή ώρα και στέλνει broadcast μηνύματα στα υπόλοιπα οχήματα με σκοπό να ειδοποιήσει για πιθανή εμπλοκή στον τρέχοντα δρόμο τους. Μπορείτε επίσης να δείτε την μέθοδο αρχικοποίησης η οποία ορίζει sentMessage = false για αυτό το όχημα κατά την εκκίνηση της εφαρμογής.

Η μέθοδος onWSM καθορίζει την αντίδραση που υπάρχει στα δεδομένα που λαμβάνονται καλώντας την changeroute για να αποφύγει τον δρόμο για τον οποίο δέχθηκε πληροφορίες και αν η sentMessage είναι ακόμα false προγραμματίζει μια υπενθύμιση να στείλει ξανά το μήνυμα σε δύο δευτερόλεπτα και θέτοντας το sentMessage flag. Η handleSelfMsg καθορίζει τον τρόπο που αντιδρά σε τέτοιου είδους υπενθυμίσεις. Καλώντας την sendDown να στείλει το broadcast. (Koukoutsis, 2022)

Institutional Repository - Library & Information Centre - University of Thessaly
06/09/2026 19:56:21 EEST - 216.73.216.250