2020

A novel intrusion detection system against spoofing attacks in connected electric vehicles

Dimitrios Kosmanos

Apostolos Pappas

Leandros Maglaras

Sotiris Moschoyinnais

Francisco J. Aparicio-Navarro

See next page for additional authors

10.1016/j.array.2019.100013

Kosmanos, D., Pappas, A., Maglaras, L., Moschoyiannis, S., Aparicio-Navarro, F. J., Argyriou, A., & Janicke, H. (2020). A novel intrusion detection system against spoofing attacks in connected electric vehicles. *Array, 5*, article 100013. https://doi.org/10.1016/j.array.2019.100013

Array 5 (2020) 100013

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/journals/array/2590-0056/open-access-journal

A novel Intrusion Detection System against spoofing attacks in connected Electric Vehicles

Dimitrios Kosmanos [a], Apostolos Pappas [a], Leandros Maglaras [b,*], Sotiris Moschoyiannis [c], Francisco J. Aparicio-Navarro [b], Antonios Argyriou [a], Helge Janicke [d]

[a] Department of Electrical and Computer Engineering, University of Thessaly, Volos, Greece
[b] Faculty of Computing, Engineering and Media, De Montfort University, Leicester, UK
[c] Department of Computer Science, University of Surrey, GU2 7XH, UK
[d] Cyber Security Cooperative Research Centre, and Edith Cowan University, Australia

ARTICLE INFO

Index Terms:
Connected vehicles
Cyber security
Electric vehicles
Intrusion detection systems
Spoofing attack

ABSTRACT

The Electric Vehicles (EVs) market has seen rapid growth recently despite the anxiety about driving range. Recent proposals have explored charging EVs on the move, using dynamic wireless charging that enables power exchange between the vehicle and the grid while the vehicle is moving. Specifically, part of the literature focuses on the intelligent routing of EVs in need of charging. Inter-Vehicle communications (IVC) play an integral role in intelligent routing of EVs around a static charging station or dynamic charging on the road network. However, IVC is vulnerable to a variety of cyber attacks such as spoofing. In this paper, a probabilistic cross-layer Intrusion Detection System (IDS), based on Machine Learning (ML) techniques, is introduced. The proposed IDS is capable of detecting spoofing attacks with more than 90% accuracy. The IDS uses a new metric, Position Verification using Relative Speed (PVRS), which seems to have a significant effect in classification results. PVRS compares the distance between two communicating nodes that is observed by On-Board Units (OBU) and their estimated distance using the relative speed value that is calculated using interchanged signals in the Physical (PHY) layer.

1. Introduction

Two of the main prohibiting factors for the adoption of the Electric Vehicles (EVs) across Europe are the driving range (i.e. the distance the vehicle can cover before it needs to recharge), and the lack of supporting charging infrastructure. One solution to these pivotal factors would be the implementation of stochastic optimisation techniques for the charging procedure of EVs [1]. However, this research area has specific limitations regarding the optimal placement of charging stations in a city, queue stability issues, especially when few charging stations must facilitate a large number of requests, among others. Furthermore, the deployment of charging infrastructure requires changes to the existing civil infrastructure, which are costly and take a long time to implement. To overcome these prohibiting factors, it is important that novel and cost-effective approaches to help in the adoption of EVs are proposed.

A novel solution initially proposed in Refs. [2,3] to increase the driving range of EVs is the use of city buses as energy sources on the move. The EVs can make efficient use of Mobile Energy Disseminators (MED), which operate as mobile charging stations, and Static Charging Stations (SCS) [2]. The role of a MED can be taken over by city buses that follow a predefined route across the city. Inner-city busses repeatedly move along a predefined route. An EV can establish a communication with a MED and approach it at a specific location along the predefined route to complete the charging process. The proposed method exploits Inter-Vehicle Communication (IVC) in order to eco-route EVs. This innovative approach drives the investigation towards integrated solutions that allow EVs to charge while moving through the city, without the need for a significant change in the existing road infrastructure.

Dynamic Wireless Charging (DWC) is a technology with great potential, but further R&D may still be required towards its applicability. A number of companies are actively developing DWC solutions, both in the research and testing phases [4–7]. In Ref. [8] the authors have proposed an intelligent routing technique that can be used to implement a dynamic charging model on existing road infrastructures. The proposed system for Dynamic Wireless Charging is based mainly on wireless Vehicle-to-Vehicle (V2V) communications and uses a route optimisation solution. The usage of wireless communication among EVs and MED coordinates the real-time booking procedure for either the SCS or the

* Corresponding author.
E-mail address: leandros.maglaras@dmu.ac.uk (L. Maglaras).

https://doi.org/10.1016/j.array.2019.100013
Received 23 October 2019; Received in revised form 25 November 2019; Accepted 26 November 2019
Available online 2 December 2019

MED, optimizing waiting times. Specifically, nodes that enter the system broadcast periodically beacon messages, known as Cooperative Awareness Message (CAM), to inform of their presence. Every beacon message contains a Node Identifier, GPS coordinates, GPS speed, current Timestamp and MAC address of the EV. These messages are transmitted several times per second using Dedicated Short Range Communication (DSRC) and Wireless Access in Vehicular Environments (WAVE) technology, based on the IEEE 802.11p standard. However, these messages are vulnerable to a wide range of cyber threats, such as eavesdropping, spoofing and modification attacks.

In particular, a spoofing attack against the communication between EVs could allow an attacker to modify the charging process (e.g. changing the order of charging) either on a MED or on a SCS for its benefit, affecting legitimate EVs. A spoofing attack is one of the most dangerous attacks for route optimisation systems. This type of attack allows an attacker to spoofs its real geographical position in the information sent within CAM messages, making other nodes believe that the vehicle is in another position [9]. This way an attacker can benefit against competing EVs, since the charging sequence is based on navigation decisions. Every EV has a table that contains the locations and the node identifiers of every other EV in its vicinity. The information about the location of every vehicle is extracted from their GPS system and sent to its neighbors through CAM messages. An attacker can create an illusion that he is present at a specific location by altering the location table of the GPS System or by generating and sending stronger fake location signals to its GPS receiver. The presence of an Intrusion Detection System (IDS) capable of detecting GPS falsification is essential in such a system. Moreover, the spoofing attack disrupts the legitimate communication between two nodes, causing similar effects to those of a Denial of Service (DoS) attack. At the same time it is more difficult to be detected since it requires only a very small number of malicious packets to be produced. The proposed IDS uses an additional metric from the Physical (PHY) layer: the estimated relative speed along with the GPS parameters are making it more efficient in detecting such attacks.

Motivation: The main motivation of this paper is to investigate how the presence of a spoofing attacker as an inner node of the system affects the total travel time that must be optimized in Ref. [8]. Specific examples are described in which the presence of an attacker can violate the right order for the charging of EVs using the MED or the SCS. These examples are not unique, however they are highly probable and can incur a significant increase in the total travel time. This indicates that more advanced attacks, possibly involving numerous coordinated attackers, can impact and degrade the operation of the system. However, the detailed analysis of coordinated attack models is out of scope of this paper. Here, we show that a probabilistic IDS is appropriate in order to detect and mitigate the presence of at least one attacker.

Concluding, an IDS based on Machine Learning (ML) is developed in order to detect spoofing attackers. Based on the outcomes of the IDS, attackers are excluded from the Dynamic Wireless Charging mechanism. Another contribution of the article is the introduction of a novel metric that is used as a separate feature for the ML algorithms. This metric named Position Verification using Relative Speed (PVRS) is based on the relative speed Δu which is estimated through interchanged signals in the PHY layer. PVRS compares the distance between two communicating nodes through their on-board Units (OBU) and the estimated distance that is calculated using the Δu value. The effect of the proposed PVRS metric in the performance of the probabilistic IDS was an increase of 6% in accuracy. Therefore, PVRS is an appropriate metric especially for the detection of a spoofing attack. This is the first proposed ML IDS in the literature that can effectively detect a spoofing attacker in a realistic application, alleviating also its effects. The detection engine of the proposed IDS is based on several ML algorithms, such as Random Forest (RF) and k-Nearest Neighbour (k-NN), using metrics in a cross-layer approach. Both supervised learning techniques are very popular, with the k-NN being robust against noisy training data like the ones obtained from a real-life urban environment and RF being one of the most accurate algorithms, reducing the chance of over-fitting. The outcomes of both supervised ML approaches are correlated using data fusion techniques in order to improve the overall performance of the IDS.

The rest of this paper is organised as follows. Section 2 provides an overview of related work in the domain of spoofing attack detection. Section 3 describes the topology and the types of the implemented attacks. Section 4 describes the proposed probabilistic IDS and the newly introduced PVRS metric. Section 5 presents the experimental evaluation setup, the impact of the implemented attack in V2V communication and the proposed system for Dynamic Wireless Charging. It also includes the experimental results of the probabilistic IDS. Section 6 contains a discussion of recent authentication and key-distribution techniques that are used in VANETs in order to strengthen and secure the communication process. Finally, Section 7 summarises our findings and concludes our work.

2. Related work

The literature in the area of spoofing attacks in VANETs is divided in two distinctive areas of interest. Firstly, techniques that use metrics from the Application layer (APP), e.g. speed-deviation, such as Acceptance Range Threshold (ART) [10]. Speed Deviation Verification at consecutive time intervals has been also used for the verification of each vehicle location. However, this metric is vulnerable against GPS spoofing attacks. Swaszek et al. [11] consider the use of range-only information to detect Global Navigation Satellite System (GNSS) spoofing of a platoon of vehicles equipped with inter-vehicle communications. This paper considers the use of short range only information communicated amongst a platoon of vehicles to detect GNSS spoofing. So the ability to detect spoofing depends largely on the relative platoon geometry and the direction of spoofing. These methods are mainly based on upper layer metrics, the honesty of nearby vehicles and the traffic density of spoofing attackers. However, there is a scarce number of proposed detection systems that use a cross-layer approach.

Secondly, there is a specific area in which the publications also use metrics from the PHY layer, such as the Received Signal Strength (RSS), and metrics from the Application (APP) layer, such as speed-deviation of nodes [12]. In various publications, the strength distribution analysis is used to detect Sybil or Spoofing attacks [13]. The proposed is a cooperative detection method, in which multiple neighbouring nodes cooperate to measure the signal strength distribution of a suspicious node and verify its physical position. However, the simulation results of [13] indicate that given the unstable nature of radio propagation, this basic cooperative method can only afford quite limited accuracy. To solve this limited accuracy of the proposed model due to propagation delay or packet losses, especially in VANETs, the concept of Presence Evidence System (PES) is proposed in order to be ensured that nodes in the opposite traffic are physical nodes and we can have them as the trusty sources of signal strength measurements. However, the ability to detect spoofing depends largely on this assumption that the opposite traffic is trusty sources. The authors in Ref. [14] propose a solution to correct the wrong position given by the fake GPS. The correction is based on a validation process by comparing the given position to an Roadside Unit (RSU) using the wireless Vehicle-to-Infrastructure communication (V2I). However, the wireless communication between the transmitter and the RSU can be impaired by fast fading characteristics such as shadowing from buildings or other obstacles that exist in VANETs. Therefore, a realistic IDS for a VANET must take into account parameters from the PHY or MAC layer that indicate the communication problem. Moreover, it is obvious that the proposed IDS is based on V2V communication only and can be applied to a VANET without any extra infrastructure such as RSUs.

Existing literature [13,14] uses RSUs as verifying base stations, with publicly known true locations. The RSUs located in the transmission range of the vehicles are used to verify the real received position from satellite against the spoofed GPS transmitter. However, it is not clear

explained how these RSU stations can be assumed as non-malicious. A variety of approaches have been proposed in the literature to recognize spoofing. Of interest here are methods which compare Global Navigation Satellite System (GNSS) information to measurements available from other, non-GNSS sensors [11]. In Ref. [15] Carson and Bevly discussed the use of range and bearing information with GPS positions to detect spoofing for a platoon of vehicles. They assumed the availability of Relative Position Vectors (RPVs) between pairs of vehicles from the radar sensor. To detect spoofing of a single vehicle they compared these RPVs to the corresponding GPS difference vector, declaring spoofing if the difference was too great. Their focus was on a pair of vehicles only. All the above mentioned techniques use the IVC for the interchange of ranging information between nodes to detect anomalies that indicate spoofing of the GPS positions. However, the wireless V2I communication confronts the wireless interference from the entire location as well the fading characteristics.

Last, extensive works present applications of spatial processing methods for GPS spoofing detection and mitigation that use either Phase Delay Measurements [16] or the Angle of Arrival (AoA) estimation [17] from the PHY layer to verify the message originator. From an attacker perspective, an illegitimate node may intentionally falsify information to achieve a certain goal that might be rational in some scenarios. A drawback of using metrics from the PHY layer is the incorrect GPS spoofing detection (e.g. false alarms) that may occur in situations where multiple correct satellite signals are received from similar directions and phase delay differences are below a predefined threshold.

All the above publications do not use ML approaches for detecting spoofing attacks. On the other hand, several articles such as [18,19] introduce the Received Signal Strength Indicator (RSSI)-based schemes for detecting spoofing attacks in Wireless Sensor Networks (WSNs) using ML techniques without using a cross-layer architecture. based on detailed analytical models for the mobile radio channel, the proposed algorithm combines two classifiers to process and analyze the instant samples of received signal strength to detect attacks. The algorithm is optimized for scenarios where the legitimate node and the attacking node are at the same distance or at a very close distance from each other in relation to a landmark, which is the worst case scenario. A novel cross-layer IDS is presented in Ref. [20] with high accuracy results. However, this IDS has only been tested only in a platoon of vehicles application. Last, in Ref. [21] an IDS is proposed based on a deep convolutional neural network (DCNN) to protect the controller area network (CAN) bus of the vehicle. The DCNN learns the network traffic patterns and detects malicious traffic without hand-designed features. The experimental results demonstrate that the proposed IDS has significantly low false negative rates and error rates when compared to the conventional machine-learning algorithms, increasing also the complexity of the system.

In contrast to all the aforementioned works for the detection of a spoofing attack using position verification techniques that is observed by the GPS. We use an additional prototype metric named PVRS that compares the distance traveled and is observed by the On-Board Units (OBU) sensors with the estimated traveled distance using the **relative speed (Δu)** metric between the sender and the receiver [22,23]. The novelty of the Δu metric is that it can be estimated by the wireless channel of the PHY layer using the effect of the Doppler phenomenon without extra sensors or infrastructure. This estimated metric can be combined with social mobility patterns constructing the PVRS metric. Relative speed as a metric can be combined with other metrics from the APP and the PHY layer leading to a cross-layer detection approach. From the PHY layer different metrics such as the RSSI, the Signal to Interference and Noise Ratio (SINR) and Packet Delivery Ratio (PDR) for the effective detection of a spoofing attack are used.

3. System model

3.1. System description and topology

Two different charging systems are compared: one that uses a Static Charging Station (SCS) only, and one that combines a SCS and a Mobile Energy Disseminators (MED). We use different initial energy conditions for all the EVs of the simulation. Our intelligent route search method takes into account the waiting time either for the MED-EV appointment or for the waiting time at the queue of an SCS, in the presence of a spoofing attacker among the inner nodes of the system. It is shown that the proposed method decreases significantly the waiting time for the charging procedure and the charging time that is needed for an EV, because the EV continues to charge along its route.

However, the presence of a spoofer in the system can either cause the starvation of specific EVs for a long time interval or cause the rerouting of the EVs for charging, which results in a significant increase in the overall travel time. At initialisation, the system model is populated with a number of EVs (50–200). From this point onwards, every node broadcasts, at a time interval of $\delta(t) = 0.1$ seconds, a CAM message to inform either the SCS or the MED of its presence. All EVs are informed of the waiting time either by the SCS or by the MED. This comes as a response through the periodical communication with MEDs or SCS using the CAM messages. Based on this information, an EV can choose either the SCS or the MED for its charging needs whilst selecting the best route from its starting point to its final destination.

For our simulated scenario, we use 3 inner nodes - vehicles of a charging system. The 2 first vehicles represent the pair Attacker-Receiver. The third vehicle is a legitimate vehicle, the Victim, whose identity is spoofed by the attacker. The nodes that enter the system broadcast periodically beacon messages, to inform of their presence and update the MED and the SCS with information about their current location. This beacon message contains a Node Identifier; the GPS coordinates; the GPS speed; the current Timestamp and the MAC address. In Fig. 1 the attacker (EV A) initially intercepts the Node Identifier (ID) of EV I, when the EV I broadcasts the CAM to inform about its presence. Then, the attacker immediately spoofs the ID of EV I to transmit CAMs with false GPS location coordinates earlier than the legitimate CAMs sent by the EV I. This means that most of the legitimate CAMs sent by the EV I are lost or delayed due to the MAC backoff procedure. After that, the receiving MED would be misdirected to an incorrect location, different from the one agreed with EV I, interfering with the charging process.

The above scenario is not the only one that may occur. For example, a spoofing attacker may launch a spoofing attack not only for their own benefit. The attacker may aim to disrupt the operation of the system as a form of Denial of Service (DoS) by virtue of the V2V communication problem between EV I and EV B (see Section 3.2). In any case, the developed IDS would need to distinguish between both legitimate CAMs sent by EV I, and spoofed CAMs sent by EV A, both transmitted with the ID of EV I.

It is well known that for broadcasting a packet in the 802.11p protocol, relay nodes may be involved in routing this packet to its final

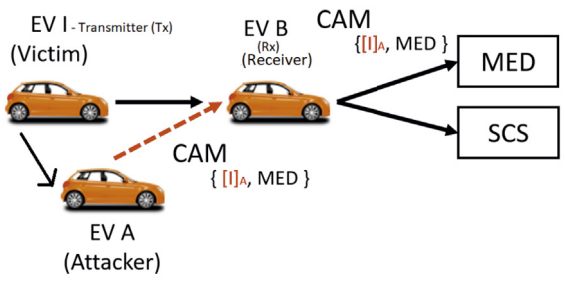


Fig. 1. Topology. Beacon routing from EV A to the MED or the SCS. IDS placement at the EV B.

destination. The localisation of the proposed IDS is decided to be one step before the SCS or the MED as can be seen in Fig. 1, which is located at the transmission range (1000 m) of both the SCS and the MED. This role of relay node has the EV B in which located the IDS and re-transmit a packet from the EV I (which is the victim) either the EV A (which is the attacker) until the destination which is either the MED or the SCS.

A specific example of the Dynamic Wireless Charging System that is susceptible to a spoofing attack is described in Fig. 2. Firstly, Fig. 2a shows the attacker that is randomly selected from one of the inner nodes of the system. The attacker can either be located on a road which is in a vertical position to the road the EV I is located on, or on the same road and hence following the EV I. We investigate the case that the attacker is initially located on a vertical road in relation to EV I, since the results are similar in both cases.

Next, EV A intercepts the ID of EV I. As a consequence of the spoofing attack, EV I loses its turn for charging (see Fig. 2b 2c). From this situation the attacker EV A has benefited since it is that vehicle that ends up following the MED for charging (see Fig. 2d). So, the victim can charge only after the termination of the spoofing attack, greatly increasing its waiting time for charging.

The blocking of the EV I must be detected by the proposed IDS to maintain satisfactory levels for the overall travel time of the Dynamic Wireless Charging System. A long term mitigation strategy could involve the localisation of the attacker EV A and its exclusion by the charging process.

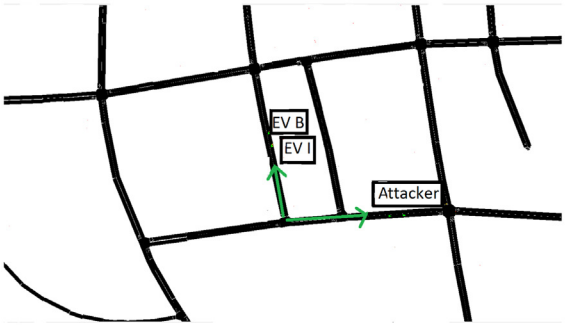
3.2. Spoofing attack in V2V communication

All EVs in the proposed charging system periodically broadcast CAMs, known as beacon messages, in order to inform neighbouring vehicles of their presence. Each CAM comprises several fields such as Vehicle Identifier (ID), Time instance, the MAC address and current vehicle GPS location and speed.

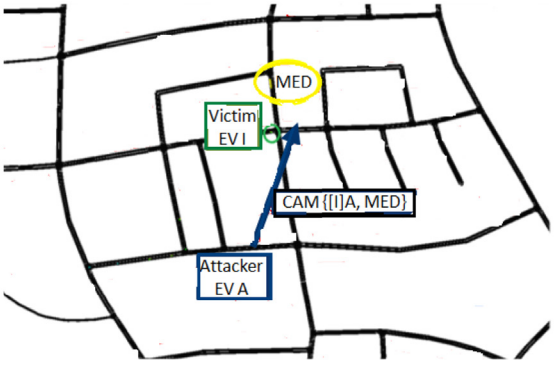
Safety applications are very challenging for the design of a MAC protocol in VANETs due to their low latency (less than 100 ms) and high reliability requirements. However, the performance of the 802.11p MAC protocol is highly affected by some key parameters, such as the packet size of safety related message, the message generation function, the vehicle density, the communication range, etc. Some of these parameters are not set properly in recent proposed evaluations. Furthermore, as stated in Ref. [24], there is significant concern if BSMs (Basic Safety Messages) are constrained to be sent on the central control channel (CCH) during the 50 ms CCH interval. This is because there could be hundreds of devices in a given area and the collision rate could be very high.

According to the IEEE 1609.4 coordination scheme, the channel time is divided into synchronization intervals with a fixed length of 100 ms, consisting of 50 ms (including 4 ms guard interval) alternating between CCH and service channels (SCH). All vehicles stay in the control channel during the CCH 50 ms period and switch to one of the six service channels during the SCH 50 ms period. However, the ID and the MAC address of the sender in the WAVE Service Advertisement (WSA) frame [25] can be modified by a spoofer. In addition, this spoofing attack can increase the collision probability which has a negative effect on the performance of the IEEE 802.11p MAC protocol, specifically in safety applications using the above mentioned CCH intervals [26]. This situation arises if a node stays in the CCH channel for a time interval longer than 50 ms. Other factors need to be also defined, such as the number of vehicles than can be accommodated in VANET safety applications with these specific CCH intervals. The implications of the implemented spoofing attack are presented in more detail in Section 5.2. .

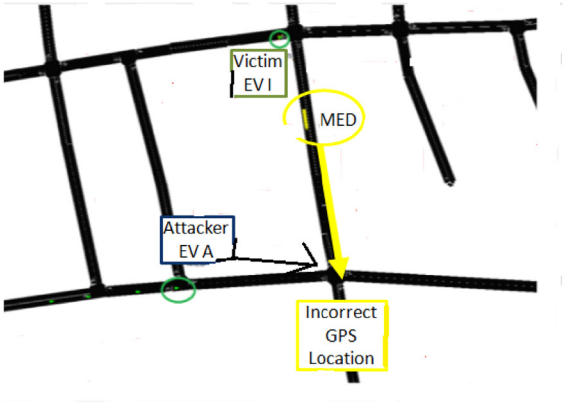
For the simulated attack scenario, initially, the EV I and EV B vehicles have a wireless connection established using the IEEE 802.11p MAC protocol. The attacker EV A approaches the EV I and EV B vehicles. When



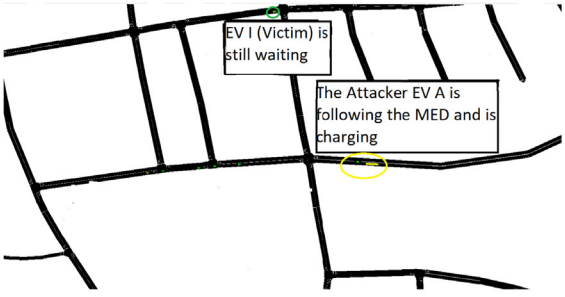
(a) The attacker is initially located in a vertical road in relation to the EV I and intercepts the ID of EV I and continues its route



(b) The attacker spoofs the ID of EV I



(c) The MED passes the EV I and leads to incorrect GPS location



(d) The attacker EV A benefits from the spoofing attack and books the MED for charging

Fig. 2. Spoofing Attack effects on MEDs.

the EV A approaches the EV B in a distance within the transmission range of 1000*m*, the attacker intercepts the ID and MAC address of EV I from the broadcasting CAMs and starts its spoofing attack. During the spoofing attack, EV A also broadcasts a CAM message every 0.1 s, using the ID of EV I, in order to inform the EV B about an incorrect GPS location and speed value. Since the attacker replicates the ID and MAC address of EV I, during the spoofing attack, there would be WSA frames showing discrepancies between the identity and the physical characteristic of the frames.

The routing flow that is selected in the transport layer is based on the incorrect spoofed MAC address of the transmitter EV I. This results in frame losses in the PHY layer due to path losses and fast fading factors, or due to the strict delay constraints of the backoff procedure in the MAC layer. Hence, many CAMs sent by EV I are lost in the MAC layer and are never acknowledged by the client, which increases the Packet Error Rate (PER) and also decreases the throughput. So it is clear that the spoofing attack affects the communication channel. This attack can be also used as an another kind of a DoS attack. The designed IDS aims to detect these discrepancies in the communication channel.

As discussed earlier, the attacker exploits these fields to transmit false GPS location coordinates within the CAMs, which misdirects the EV I to an incorrect location. As a consequence the observed RSSI values of the wireless communication between *Transmitter- EV I* (*Tx*) and *Receiver- EV B* (*Rx*) to move to a different level, indicating the spoofing attack.

Fig. 3 shows a comparison between the RSSI values obtained at the receiver that corresponds to different distances between the *Transmitter* and *Receiver* vehicles during the first two stages of the simulation (i.e., the initial period of normal traffic and the spoofing attack). The initial period of normal traffic is between the time interval (10–70 s), while the spoofing attack is conducted in the time interval between (70–85 s). When the position of the transmitter, which is the spoofer during the spoofing attack, is quite different from the legitimate vehicle's position, the level of the RSSI values change significantly as can be seen in Fig. 3. This can indicate the spoofing attack, but also shows that the RSSI maybe is a crucial metric for the detection of a spoofing attack in a cross-layer ML approach.

4. The probabilistic IDS

4.1. Supervised ML techniques

The *k*-NN is a simple Machine Learning (ML) technique for pattern recognition, based on feature similarity [27]. When we say a technique is non-parametric, it means that it does not make any assumptions on the underlying data distribution. Therefore, *k*-NN could and probably should be one of the first choices for a classification study when there is little or no prior knowledge about the distribution of the data points. *k*-NN is also a *lazy* algorithm (as opposed to an *eager* algorithm). What this means is that it does not use the training data points to do any generalisation. In other words, there is no explicit training phase or it is very minimal. In other words, the training phase is pretty fast. So, the *k*-NN algorithm is also useful for non-linear data, which is the case for the data we use for training in this study.

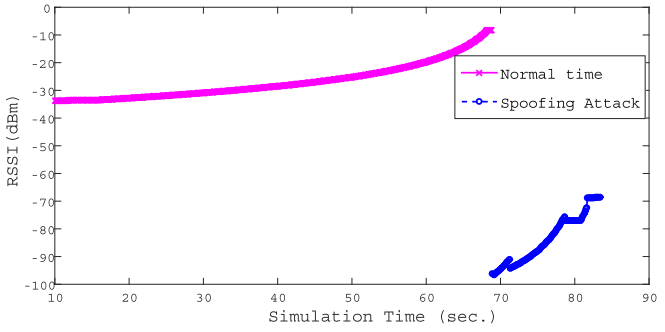


Fig. 3. Different RSSI levels during the normal operation and spoofing attack.

The *Random Forest* (RF) is a supervised learning algorithm, based on decision tree models that split a subset of features at training time and output the class that has the majority votes of the classes of the individual trees [28]. This supervised learning algorithm is preferred over others for the following reasons. Firstly, it can be used for both classification and regression tasks, providing high accuracy. Secondly, if there are more trees, it does not allow overfitting trees in the model. It has the power to handle a large data set with higher dimensionality. Lastly, the RF classifier can handle missing values while maintaining the accuracy of a large proportion of data.

Each of the classification algorithms is able to generate accurate results when implemented independently. However, the combined use of these algorithms may help improve the overall performance of an IDS [29]. Different methodologies were evaluated to assess whether the classification results could be improved, for instance, by applying data fusion techniques.

Ensemble learning has been used to combine the outputs from different classification techniques. Ensemble learning is the process in which multiple classifiers are strategically selected and combined in order to solve a particular computational intelligence problem. Ensemble learning is primarily used to improve the classification performance of a model. One of the most commonly used ensemble learning algorithms is known as Bagging [30]. In this algorithm, bootstrapped replicas of the training data for each classifier (RF, *k*-NN) are used. During the last step of Bagging, the majority voting combination rule is used. Since the intended output of the IDS is a probabilistic IDS, the conditional probabilities are estimated for each classifier in the presented IDS using the Bayesian rule as a data fusion technique.

4.2. Position verification metric and localisation of the attacker

The presented IDS uses cross-layer metrics for training from both the PHY and APP layers. From the PHY layer we extract the RSSI, the SINR and the PDR. From the APP layer we extract the relative speed (Δu) and the GPS coordinates, each one used for the generation of the Position Verification using Relative Speed (PVRS) metric. We must also compare the GPS location observed by the On-Board Unit (OBU) with the estimated location using the relative speed metric. This procedure results in a new novel metric called PVRS. All these metrics, listed in Table 1, are used in a cross-layer approach to improve the detection accuracy of the IDS. Furthermore, for the training-testing procedure of the proposed IDS, the data have been divided into 70% for training and 30% for testing.

The relative speed (Δu), introduced in Ref. [23], indicates the relative speed between an attacker EV A and the receiver EV B:

$$\Delta u_A = |\vec{u}_A - \vec{u}_B| \tag{1}$$

where $\vec{u}_A$, $\vec{u}_B$ are the speed of the attacker and the receiver, respectively. The metric Δu can be effectively estimated by the RF signals' interchange in the PHY layer. The novelty of this metric is that it can be estimated by the physical properties of the wireless channel, using the effect of the Doppler phenomenon [22].

To create the proposed PVRS metric we must make some fundamental assumptions. Specifically, we assume as reliable the communication between the *Tx-Rx* at the initial time instant and an initial distance *dx*

Table 1
Metrics that are jointly processed by the classification algorithms.

ID	Model Feature	Short Description
1	*PVRS*	Position Verification using estimated Δu
2	RSSI	Signal Strength Indicator (dBm)
3	SINR	Signal Quantity Indicator (dB)
4	PDR	Packet Delivery Ratio

between the two nodes. From this time onward the difference $\Delta(x)$ between distance $d_x(t-1)$ between *Tx-Rx* at the time $t-1$ and distance $d_x(t)$ after a verifying time interval of $\delta(t) = 0.1$ is used as verification distance. This relative movement $\Delta(x)$ of the transmitter-receiver pair is calculated by their OBUs, according to the transmitter-receiver GPS coordinates in two dimensions with respect to the traffic ahead.

This mobility pattern can be justified by the social mobility patterns that are introduced in Ref. [31] for clustering needs. So we can compare the distance $\Delta(x)$ observed by the OBU with the estimated distance $\Delta(x)_{est}$ using the estimated relative speed value Δu between *Tx-Rx*. This estimated distance is in essence a relative mobility parameter k_{ijx} between the nodes *i-j*, which is a parameter indicating whether the force among the nodes is positive or negative (acceleration or deceleration). This value depends on whether the vehicles are approaching or moving away along the corresponding axis.

$$\Delta(x)_{est} = \frac{\Delta u}{\delta(t)}\delta(t)^2 \tag{2}$$

where the $k_{TxRx} = \frac{\Delta u}{\delta(t)}$ is the rate of change of speed (acceleration or the deceleration value) indicating the ratio of divergence or convergence among moving nodes *Tx-Rx* at the duration $\delta(t) = 0.1s$. Comparing the estimated distance $\Delta(x)_{est}$ with the distance $\Delta(x)$ that is observed by OBU, we can get the proposed metric PVRS.

It can be seen that the Algorithm 1 for the generation of the PVRS metric is based on position verification. The algorithm firstly examines if the *Tx* and *Rx* vehicles approach each other or move away from each other. This is determined by the sign of the *ddu* value, which is the difference between the previous relative speed value at the time instant $t-1$ and the current relative speed value at the time instant *t*.

Afterwards, if the difference between the $\Delta(x)_{est}$ and $\Delta(x)$ values is in the range of an apriori average spoofing deviation value (r = 10 m), this indicates the normal operation of the system although we note this value is a quite small threshold for the detection of a spoofing attack. So, we can set the PVRS value equal to the previous value in Algorithm 1. Otherwise, there is a quite large deviation between the estimated distance and the distance observed by the GPS. In that case, the PVRS value will be increased by one indicating the start of a spoofing attack. The PVRS value will change again at the end of the spoofing attack, because the legitimate transmitter is located in a different position to the spoofer.

Using this approach, a continuous line can be constructed which will join the points that indicate either the normal behavior or the spoofing attack as a form of linear interpolation technique [32]. The spoofing deviation value is an average error which is added in the difference in distance between a claimed position and the real physical position.

This algorithm for the PVRS metric which is based on the position verification is presented in Algorithm 1. Therefore, the entire area is then partitioned into small areas (called subnetworks) that can be investigated in isolation for the detection of a spoofing attacker. A subnetwork can be assumed an ellipse whose foci are the Tx and Rx vehicles. This ensures that all objects whose sum of distances from Tx and to Rx (i.e., from Tx to object and from object to Rx) is less than 1000 m, (this is the maximum communicating distance for 802.11p) are accounted for.

Algorithm 1 PVRS Algorithm

M = number of observations at consecutive time instants
$r = 10m$
$t = 0$
$PVRS \leftarrow matrix(nrow = M, ncol = 1)$
$\Delta(x) \leftarrow matrix(nrow = M, ncol = 1)$ maxtrix of OBU's observations
$\Delta u \leftarrow matrix(nrow = M, ncol = 1)$ maxtrix of estimated relative speed
$t++$
while $(t <= M)$ **do**
  $ddu(t) = \Delta u_{est}(t-1) - \Delta u_{est}(t)$
  if $ddu(t) > 0$ **then**
    $\Delta(x)_{est}(t) \leftarrow \Delta(x)_{est}(t-1) - \frac{ddu(t)}{\delta(t)}\delta(t)^2$

(*continued on next column*)

(*continued*)

Algorithm 1 PVRS Algorithm

    if $\Delta(x)_{est}(t) - r <= \Delta(x)$ **then**
      $PVRS(t) \leftarrow PVRS(t-1)$
    else
      $PVRS(t) \leftarrow PVRS(t-1) + 1$
    end if
  else
    $\Delta(x)_{est}(t) \leftarrow \Delta(x)_{est}(t-1) + \frac{ddu(t)}{\delta(t)}\delta(t)^2$
    if$\Delta(x)_{est}(t) + r >= \Delta(x)$**then**
      $PVRS(t) \leftarrow PVRS(t-1)$
    else
      $PVRS(t) \leftarrow PVRS(t-1) + 1$
    end if
  end if
end while
  return*PVRS*

An example in Fig. 4 indicates the different values that get the PVRS metric for a spoofing or a normal traffic during a time interval. Every change in the value of the PVRS metric indicates the end or the start of a spoofing attack.

After the detection of the spoofing attack the node that launches this type of attack must be localised and excluded from the system. Given the initial distance $d_x(t=0)$ between *Tx-Rx* as reference distance and the estimated distance $\Delta(x)_{est}$ after the specific time interval that is estimated in Algorithm 1, we can estimate the accurate location of the attacker. We have already mentioned that the transmitter's GPS coordinates are known to the *Rx*. This technique for the localisation of the attacker can be seen as being similar to the one proposed in Ref. [19] where the spatial correlation of the received RSSI inherited from wireless nodes can be used for determining the true location. Both techniques use the values of the wireless communication in the physical layer of the 802.11p protocol for the localisation. Either the estimated relative speed value Δu that is estimated through the physical layer or the RSSI value at the *Rx*.

5. Experimental evaluation

To evaluate the effect of a spoofing attack on the Dynamic Wireless Charging of EVs, our experimental evaluation has been conducted using simulations in the city of Erlangen, as shown in Fig. 5. We used the Simulation of Urban Mobility (SUMO) and the OMNET++/VEINS [33]. SUMO is adopted as our traffic simulator and OMNET++ is used to simulate the wireless communication. Furthermore, the GEMV (a geometry-based efficient propagation model for V2V) [34] tool was integrated into the VEINS network simulator for a more realistic simulation of the PHY layer. For describing the modeled area GEMV uses the outlines of vehicles, buildings and foliage. Based on the outlines of the objects, it forms R-trees. R-tree is a tree data structure in which objects in the field are bound by rectangles and are hierarchically structured based

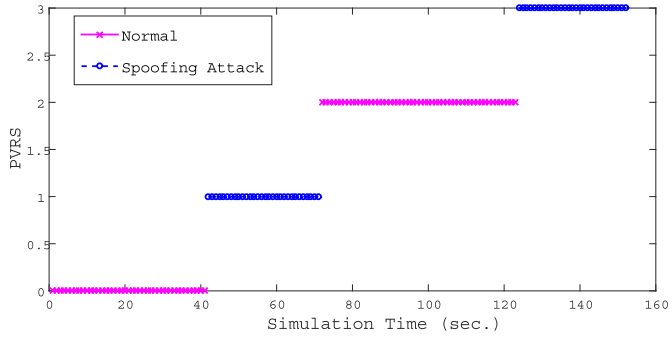


Fig. 4. Different PVRS value levels during the normal operation and spoofing attack.

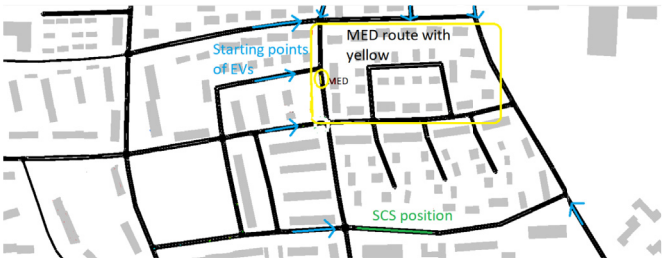


Fig. 5. Section of the Erlangen city map used to conduct the simulations. The MED route is marked in yellow. The position of the SCS is marked in green. The arrows in cyan point at the journey starting points of the EVs. The buildings are represented for the Non-Line of Sight (NLOS) links to be considered in the V2V communication.

on their location in space. Hence, GEMV employs a simple geometry-based small-scale signal variation model and calculates the additional stochastic signal variation and the number of diffracted and reflected rays based on the information about the surrounding objects. GEMV was configured and modified to be portable to the VEINS simulator and incorporated into this. Last, to setup and test our classification algorithms for the spoofing attacks detection on the previously obtained data, we chose to use the programming language R [35].

5.1. Evaluation setup

As can be seen in Fig. 5, a bus which follows a specific route acts as MED. The route followed by the MED is represented in yellow. Furthermore, an SCS is found at a fixed location at the road side of the corresponding city district. All the parametric side roads of the area in which the SCS and MED charging models are located are used as starting points (s^k) for the Dynamic Wireless Charging System with the same probability. The point at which the EVs are introduced in SCS or MED system is shown in Fig. 5 with $(m_b, s_b$ respectively).

There are between 50 and 200 EVs in the simulated environment. Additionally, each EV k entering the simulation has starting energy charge (ϵ_s^k) defined according to a uniform distribution with values between 1 and 6 kWh. 60% of the EVs need recharging and are considered as anxious drivers (i.e the starting energy charge is smaller than the energy required to complete its travel).

The only communication paths available are via the ad-hoc network and there is no other communication infrastructure. All the above parameters and the selected evaluated area were chosen in way that does not favour any charging method (MED or SCS). The power of the antenna is $Ptx = 18dBm$ and the communication frequency f is $5.9Ghz$. In our simulations, we use a minimum sensitivity (Pth) of $-69dBm$ to $-85dB$, which gives a transmission range of about 1000 m, as can be seen in Table 2. As a result of the above transmission range, there is no communication with a few EVs. So, a number of EVs are excluded from the charging procedure because of the communication lost between EVs. This happens when the SINR threshold is below 10 dB due to attenuation that is caused by the building obstacles of the city.

After 60 s of normal operation of the proposed Dynamic Wireless

Table 2
Evaluation parameters.

Independent parameters	Range of values
Number of vehicles	50–200
Initial Energy (ϵ_s^k)	1-6 kWh
P_{tx}	18dBm
f	5.9Ghz
Packet length	750 bits
Packet Header length	256 bits
Minimum sensitivity (P_{th})	−69dBm to −85dB
Transmission range	1000 meters

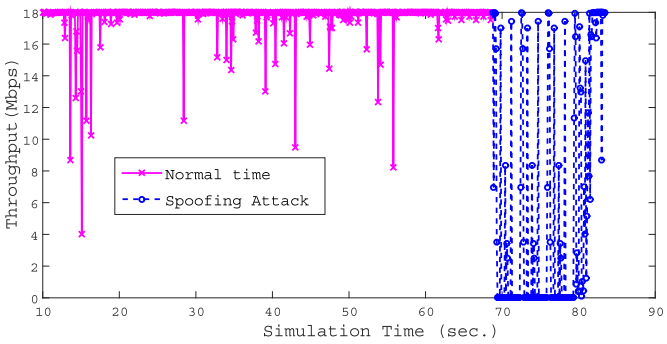


Fig. 6. Throughput (Mbps) of the communication between the *Tx* and *Rx* vehicles during the experimental simulation. The normal communication without attack in *pink* and spoofing attack in *blue*.

Charging a spoofing attacker node is inserted in the systems and conducts a spoofing attacks with duration about 25 s. The overall simulation utilizes a set of 1000 observations equally split into the two implemented scenarios examined (normal operation and spoofing attack). To avoid overfitting[1] only 30% of the total number of the observations are used for training while the remaining 70% for testing.

5.2. Effect of spoofing attack in the V2V MAC layer

In order to show the effect of the spoofing attack on the communication between the Transmitter (*Tx*) and Receiver (*Rx*) vehicles, the throughput has been plotted in Fig. 6. The Y-axis represents the throughput in Mbps, whereas the X-axis represents the time in seconds. The normal (i.e., without attack) communication between the *Tx* - *Rx* vehicles is represented in *pink* and the spoofing attack is represented in *blue*. The effective packets interchange without interfering the attacker between the *Tx* and *Rx* vehicles is the time interval between 0 and 60 s. The spoofing attack is launched during the time interval 60–85 s.

As can be seen in Fig. 6, the average throughput for the normal communication is 18 Mbps, approximately. When the spoofing attack is launched, the average throughput drops to 8 Mbps. This change in the throughput clearly shows that the modification of the GPS coordinates and speed values within the CAM messages has a clear effect upon the communication between the connected vehicles.

Focusing on the effect of the spoofing attack on the IEEE 802.11p MAC layer, the IEEE 802.11p protocol employs Hybrid Coordination Function (HCF) contention-based channel access Enhanced Distributed Channel Access (EDCA) as the MAC method. This is an enhanced version of the Distributed Coordination Function (DCF) of the IEEE 802.11 protocol. The EDCA uses Carrier Sense Multiple Access with collision avoidance (CSMA/CA). In the EDCA scheme, a node willing to transmit will sense the medium, and if the medium is idle for greater than or equal to an Arbitration Inter-Frame Space [Access Class] (AIFS[AC]) period, the node starts transmitting directly. If the channel becomes busy during the AIFS[AC], the node will defer the transmission by selecting a random backoff time. The spoofing attack of node EV A has as effect when the legitimate EV I wants to transmit and find the channel busy initiating the backoff procedure. In Fig. 7, the *busy time* for every MAC transmission every Time Step (in total 200 Time Steps) from the victim node EV I to the receiver EV B is shown. From the results in Fig. 7, the effect of the spoofing attack in MAC layer is evident. Without the spoofing attack, the maximum busy time value reaches only 3.8 ms, whereas the maximum busy time reaches about 8.5 ms when the spoofing attack is conducted, increasing substantially the probability of collisions.

Fig. 8 shows the average MAC delay T_{MAC} for different density of

[1] Overfitting occurs when the classifier tends to memorize the training set and thus generalize poorly when facing previously unseen data.

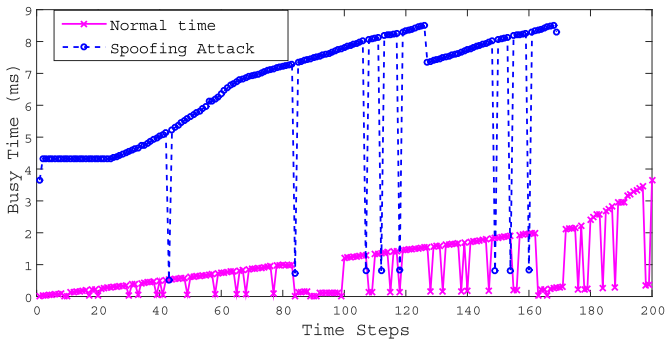


Fig. 7. Busy Time (ms) of the communication between EV I and EV B vehicles during the experimental simulation. The normal communication without attack in *pink* and has a duration of 200 Time Steps (20 s), whereas the spoofing attack in *blue* has a duration of 170 Time Steps (17 s).

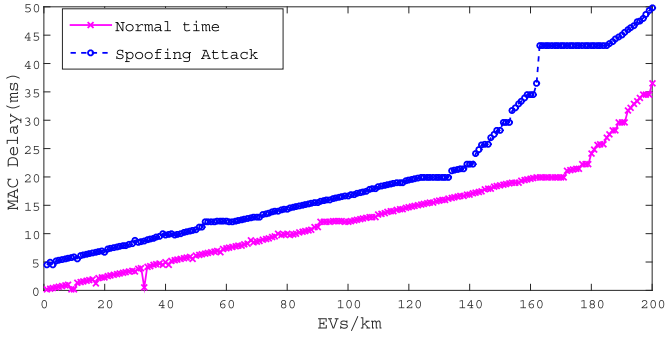


Fig. 8. MAC Layer Delay T_{MAC} (ms) of the communication between EV I and EV B vehicles during the experimental simulation using a range of 200$EVs/\ km$. The normal communication without attack in *pink*. While the spoofing attack in *blue*.

vehicles with the standard central control channel (CCH) interval setting of 50 ms. The T_{MAC} is the time delay that occurs at the MAC layer since the safety message arrived to MAC layer until the message is finally sent out. The end-to-end delay T_{E2E} depends mostly on T_{MAC} and the propagation delay. This work only focuses on T_{MAC} increase caused by spoofing attacks. As it can be seen in Fig. 7, the T_{MAC} increase is directly proportional to the density of vehicles. An increase in the number of vehicles, as well as a decrease of the CCH interval will cause more contention and more backoff time. Hence, the MAC delay T_{MAC} is mostly driven by the backoff time.

Moreover, the MAC delay is always less than 100 ms in all the simulated scenarios. It indicates that IEEE 802.11p MAC protocol can satisfy the latency requirement (i.e. less than 100 ms) in VANET safety applications [26]. It can be observed in Fig. 8 that, with the presence of spoofing attack in Dynamic Wireless Charging System, the T_{MAC} delay reaches over 45 ms with a traffic density of 200 EVs per kilometer (EVs/km) in need of charging in the area. This value of MAC delay is very close to the CCH interval, which is 50 ms. As a result, it becomes difficult for EV I to have access to one of the six service channels (SCH) channels. This combination of the MAC delay with the traffic density can be assumed as a marginal threshold for the proposed dynamic charging system. This is because if the T_{MAC} delay exceeds the 50 ms (CCH interval) the established wireless connection using the IEEE 802.11p MAC protocol between two EVs in fact will be questionable due to the collision probability increase.

5.3. Effect of spoofing attack on the overall travel time

This section compares two different charging system scenarios, with and without a spoofing attack. The first charging system scenario contains only an SCS, and the second scenario contains both an SCS and a MED. In the two scenarios with a spoofing attack, the malicious node replicates the identity of the EV A ($ID = 40$). Fig. 9 represents average travel times for a total number of 100 EVs in the system. It is obvious from the results that the insertion of the spoofing node with $ID = 40$ causes a significant increase in average travel time. The routing optimisation [8] which is applied to the Dynamic Wireless System is negatively affected. The optimum EVs charging order is altered, which causes an increase in the average travel time value of the system.

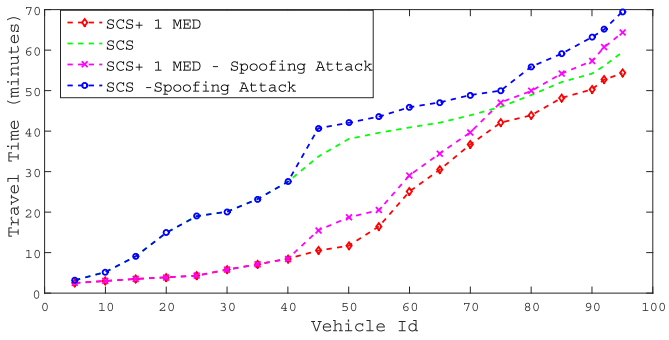


Fig. 9. Average Travel Time comparison between the two different charging system scenarios, with and without a spoofing attack.

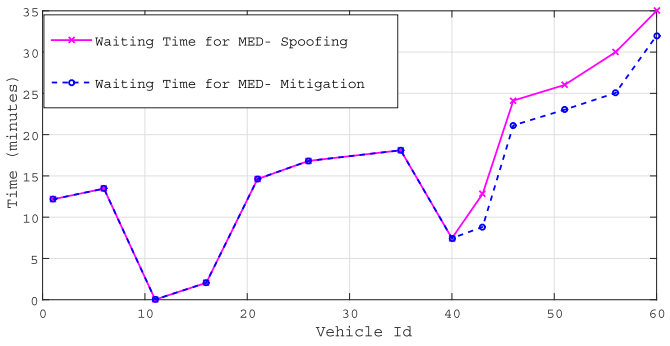
Focusing specifically on the system that uses only an SCS, the difference of the average overall travel time with and without the presence of spoofing attack is about 5min, which increases the average total travel time by 10%. This increase is even more noticeable in the scenario with an SCS and a MED. In this case, travel time difference with and without the presence of spoofing attack is about 8min, increasing the average total travel time by 13%. The travel time difference is slightly higher in this second scenario because the MED, which is a mobile node, contributes with additional propagation delay in the V2V communication. This is also caused by the spoofing attack.

Additionally, Fig. 10a compares the average waiting time of each EV at the point that it is planned to meet and follow the MED when the spoofing attack is conducted with the average waiting time of each EV after the mitigation of the spoofing attack. It can be seen that the spoofing attack increases the waiting time by 10%. Similarly, Fig. 10b compares the average queue time in the SCS when a spoofing attacker enters the system and the average queue time after the exclusion of this node from the charging process after the mitigation of the spoofing attack. The effect of the attack is clearly shown with the high difference between the two values. The queue time increases about 30% after the EV with $ID = 40$ launches the spoofing attack. This is due to the re-ordering of the dynamic charging process after the presence of the spoofing attacker. Hence, this delays the overall dynamic charging process. As a consequence, most EVs would select the SCS for charging, which in turn increases significantly the queue time.

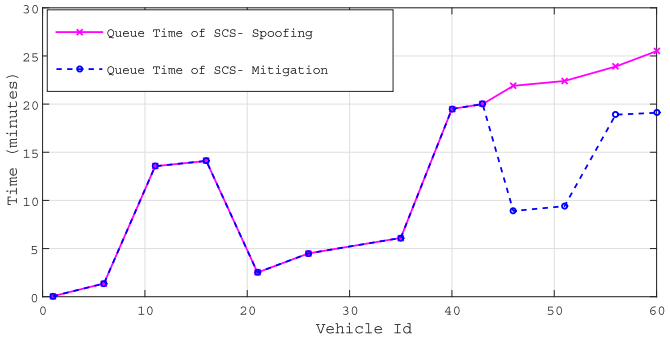
Finally, it is also noticeable that, with the presence of a spoofing attacker in the system, the average waiting time increases with the same rate as the average queue time. This finding also verifies that the spoofing attack violates the right order of charging process having as consequence the increase of the waiting time for the proposed charging system (SCS + MED), as the number of EVs is increased. Therefore, this balances the performance of the two charging system scenarios (i.e. SCS and SCS + MED). On the contrary, after the mitigation of the spoofing attacker, as the simulation time increases, the waiting time for MED and the queue time for SCS both increase and decreases irregularly. This happens because there are two choices for charging of EVs (MED or SCS) that are quickly interchanged.

5.4. IDS performance

We evaluated the performance of our attack detector by using a detection rate and receiver operating characteristic (ROC) curve, which



(a)



(b)

Fig. 10. Average Waiting Time for MED, Queue Time of SCS with the presence of spoofer and after the mitigation procedure; (a) Average Waiting Time for MED with the presence of spoofer attacker vs Average Waiting Time for MED after the mitigation with excluding the EV with $ID = 40$ from the charging process; (b) Queue Time of SCS with the presence of spoofer attacker vs Queue Time of SCS after the mitigation with excluding the EV with $ID = 40$ from the charging process.

is a probability curve since the proposed system is probabilistic. Another evaluation metric used is the area under curve (AUC) which represents the degree or measure of separability between classes. Thus, the higher AUC score, the better our model can distinguish between classes. The last metric that we use for the evaluation of the proposed cross-layer IDS is the accuracy. Informally, accuracy is the fraction of predictions our model got right in the total of predictions.

In order to evaluate the adaptability of the presented IDS in detecting a spoofing attack in a Dynamic Wireless Charging System, additional experiments have been conducted. These experiments combine the implemented spoofing attack with the normal operation of Dynamic Wireless Charging System as two separates classes. Our proposed IDS, using the *k*-NN and RF algorithms, was trained and tested on both the absence and presence of the PVRS feature. The presence of the PVRS feature in our data set played a major role in detecting the attack, since both *k*-NN and RF algorithms achieved high, and equal, accuracy scores of 91.3%. Although the accuracy of each model is the same, they produce very different AUC scores. The RF algorithm excels, having a score of 0.986 as can be seen in Fig. 12, while the *k*-NN algorithm has an AUC score of 0.935. On the other hand, the absence of the PVRS feature impacts our results negatively. The accuracy of both the *k*-NN and RF algorithms drops to 84.9% and 85.6% respectively. The AUC score drops slightly (0.956) for the Random Forest in comparison to the higher drop (0.839) noticed in the *k*-NN algorithm. This is shown in Fig. 11.

It can be seen from the previous experiments that most of the discrepancies between the two ML algorithms used for the classification results are observed when the PVRS is not used for training and testing. So, a data fusion method for our Dynamic Wireless Charging System could be used in this case. The Data Fusion approach combines the outcome of the two supervised ML classifiers. As observed in Fig. 13, the

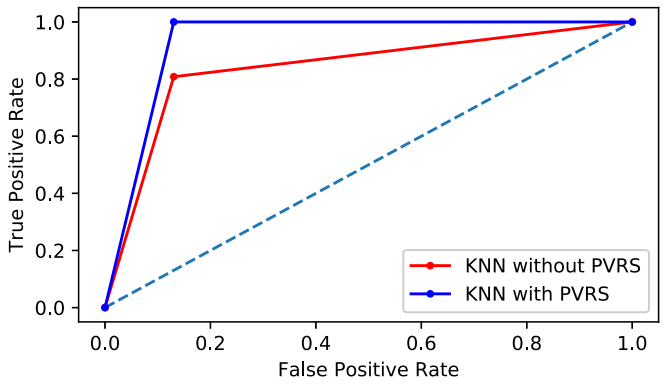


Fig. 11. Spoofing Attack Detection: ROC curve for cross-layer approach using the *k*-NN algorithm.

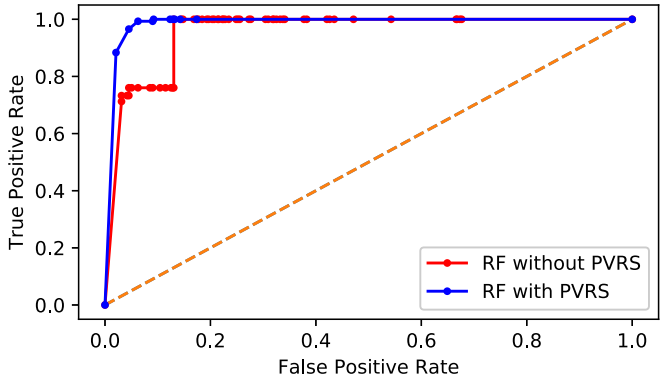


Fig. 12. : Spoofing Attack Detection: ROC curve for cross-layer approach using the RF algorithm.

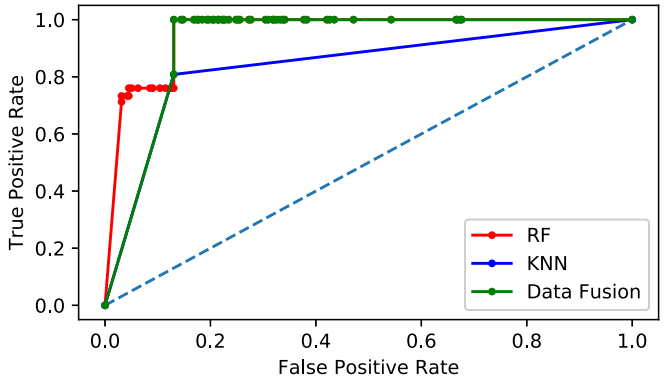


Fig. 13. Spoofing Attack Detection: ROC curves for cross-layer approach using the Data Fusion between two supervised ML algorithms.

data fusion method combines the two algorithms and actually produces a better result.

Last, in Table 3 we summarize the classification accuracy, exploiting the usage of the proposed PVRS metric as an extra feature for training and testing or not using both the *k*-NN and *k*-NN algorithm. Comparing the accuracy results with the usage of the PVRS metric with those without the

Table 3
Classification accuracy percentages exploiting the usage of the PVRS metric or not.

	k-NN	RF
PVRS metric	91.3%	91.3%
without PVRS metric	84.9%	85.6%

usage of PVRS metric we can observe an 6.4% accuracy increase for the *k*-NN algorithm and a corresponding 5.7% accuracy increase for the RF algorithm.

6. Discussion

Today security and anonymity in group communications play even more vital role due to the increased level of threats that appear on a daily basis. A strong difference is that now the new generation networks possess highly dynamic characteristics through information exchange among automated vehicles. Moreover, when specific time critical applications are running on top of communication between cars, as the dynamic charging framework described in this article, security is even more important. Authentication and key-distribution methods can be used in order to strengthen and secure the communication process amongst the various entities of the system. Many research works that can provide security and privacy in VANETs have been proposed during the last years. Authors in Ref. [36] proposed the use of anonymous certificates and a modification of Public Key Infrastructure (PKI) for the provision of authentication and integrity. The OBUs which are on board the vehicles are equipped with a large number of public and private key pairs that can use for communicating with neighbouring cars. Authors in Ref. [37] came out with an anonymous authentication scheme in order to make a VANET robust to several attacks, including an impersonation attack. Finally authors in Ref. [38] present a detailed analysis of privacy preservation methods for ad hoc social networks, including VANETs. As future work we plan to combine the proposed IDS with a Key Distribution System that would increase the security without increasing computational cost thus demanding central entities, such as RSUs to act as central authorities.

7. Conclusions

In this paper, an Intrusion Detection System (IDS) based on supervised Machine Learning (ML) algorithms was developed to detect spoofing attackers and exclude them from the proposed system for Dynamic Wireless Charging with Mobile Energy Disseminators (MEDs), as a mitigation approach. Specific showcases of the proposed Dynamic Wireless Charging with MEDs are investigated with the presence of an inner node of the system as a spoofing attacker. These cases show that the average total time is increased by about 13% in the system (SCS + MED), because of the re-ordering of the charging process Dynamic Wireless Charging System with MEDs. This re-ordering of the charging process with MEDs increases the requests for charging with SCS, and results in an increase of the average queue time in SCS by about 30%. While the increase of the average waiting time for MED due to the spoofing attack is at about 10%.

The above results point to the need of a probabilistic IDS to detect and mitigate the spoofing attacker. The proposed cross-layer IDS achieves a good accuracy at about 91% using either the *k*-NN or the RF algorithm. Moreover, a new metric Position Verification using Relative Speed (PVRS) is proposed that compares the distance between two communicated nodes that is observed by on-board Units (OBU) and the estimated distance that is estimated using the Δu value estimated by the interchanged signals in the PHY layer. The effect of this new PVRS metric in the performance of the proposed probabilistic IDS has proved to be an increase in accuracy by about 6%, using both supervised ML algorithms. Furthermore, due to the discrepancies that occurred in the classification performance of the two ML algorithms without using the PVRS metric, a data fusion method between these algorithms (k-NN, RF) has proved to have clearly superior performance compared with each individual ML algorithm.

Lastly, this paper has demonstrated the communication problem that is provoked on Dynamic Wireless Charging System with MEDs with an attacker, and can be considered as a trigger for more complex attacks with more attackers.

Author contribution

All authors contributed equally to this manuscript.

Declaration of competing interest

The authors declare no conflict of interest.

8 Acknowledgements

We thankfully acknowledge the support of the CONCORDIA H2020 (GA no. 830927) EU project, and the EPSRC IAA project AGELink (EP/R511791/1).

References

[1] Chrysanidis G, Kosmanos D, Argyriou A, Maglaras L. Stochastic optimization of electric vehicle charging stations. *IEEE Smart World Congress (SWC)*; 2019.
[2] Maglaras L, Topalis FV, Maglaras AL. Cooperative approaches for dymanic wireless charging of electric vehicles in a smart city. In: Energy conference (ENERGYCON), 2014 IEEE international. IEEE; 2014.
[3] Maglaras L, Jiang J, Maglaras A, Topalis F, Moschoyiannis S. Dynamic wireless charging of electric vehicles on the move with mobile energy disseminators. Int'l J Adv Comput Sci Appl 2015;6:239–51.
[4] Luke H, Ben W, Bani A, Denis N. Potential of wireless power transfer for dynamic charging of electric vehicles. In: IET intelligent transport systems, vol. 13. IET; 2019. p. 3–12.
[5] Graeme D. https://www.qualcomm.com/news/onq/2017/05/18/wireless-dynamic-ev-charging-evolution-qualcomm-halo; 2017.
[6] Maglaras L. How to charge your electric car 'on the fly'. www.brinknews.com/how-to-charge-your-electric-car-on-the-fly/; 2017.
[7] Yamauchi M. https://www.pluglesspower.com/gen2-tech-specs/; 2019.
[8] Kosmanos D, Maglaras L, Mavrovouniotis M, Moschoyiannis S, Argyriou A, Maglaras A, Janicke H. Route optimization of electric vehicles based on dynamic wireless charging. IEEE Access 2018;vol. 6. 42 551 – 42 565.
[9] Sparsh S, Ajay K. A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud. In: Vehicular communications, vol. 12. Elsevier; 2018. p. 138–64.
[10] van der Heijden RW, Al-Momani A, Kargl F, Abu-Sharkh OMF. Enhanced position verification for VANETs using subjective logic. In: IEEE 84th vehicular technology conference. VTC-Fall; 2016.
[11] Swaszek PF, Hartnett RJ, Seals KC. Using range information to detect spoofing in platoons of vehicles. In: 30th international technical meeting of the satellite. Division of The Institute of Navigation (ION GNSS); 2017. p. 2838–53.
[12] Grover J, Prajapati NK, Laxmi V, Gaur MS. Machine learning approach for multiple misbehavior detection in vanet. In: International conference on advances in computing and communications, vol. 192. SpringerLink; 2011. p. 644–53.
[13] Yu B, Xu C-Z, Xiao B. Detecting sybil attacks in VANETs. In: Journal of parallel and distributed computing, vol. 73. Elsevier; 2013. p. 746–56.
[14] Anouar B, Mohammed B, Abderrahim G, Mohammed B. Vehicular navigation spoofing detection based on V2I calibration. In: 4th IEEE international colloquium on information science and technology (CiSt); 2016.
[15] Carson N, Bevly D. A robust method for spoofing prevention and position recovery in attacks against networked gps receivers. In: Proceedings of the 2015 international technical meeting of the institute of navigation. Dana Point, California: ION; 2015. p. 623–32.
[16] Magiera J, Katulski R. Detection and mitigation of GPS spoofing based on antenna array processing. In: Journal of applied research and technology, vol. 13. ScienceDirect; 2015. p. 45–57.
[17] Abdelaziz A, Burton R, Koksal CE. Message authentication and secret key agreement in VANETs via angle of arrival. In: 2016 IEEE vehicular networking conference (VNC); 2016.
[18] de Lima Pinto EM, Lachowski R, Pellenz ME, Penna MC, Souza RD. A machine learning approach for detecting spoofing attacks in wireless sensor networks. In: 32nd IEEE international conference on advanced information networking and applications. AINA); 2018.
[19] Chen Y, Yang J, Trappe W, Martin RP. Detecting and localizing identity-based attacks in wireless and sensor networks. In: IEEE transactions on vehicular technology, vol. 59; 2010. p. 2418–34.
[20] Kosmanos D, Pappas A, Francisco LM, Aparicio Navarro J, Janicke H, Boiten E, Argyriou A. Intrusion detection system for platooning connected autonomous vehicles. In: SEEDA-CECNSM conference; 2019.
[21] Hyun Min S, Jiyoung W, Huy K. In-vehicle network intrusion detection using deep convolutional neural network. In: Vehicular communications. Elsevier; 2019.
[22] Kosmanos D, Argyriou A, Maglaras L. Estimating the relative speed of RF jammers in VANETs. Secur Commun Netw November 2019;2019.
[23] Karagiannis D, Argyriou A. Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning. Veh Commun July 2018;13:56–63.
[24] Kenney JB. Dedicated short-range communications (dsrc) standards in the United States. In: Proc. IEEE, vol. 99. IEEE; 2013. p. 1162–82. no. 7.

[25] Campolo C, Cozzetti HA, Molinaro A, Scopigno R. Augmenting vehicle-to-roadside connectivity in multi-channel vehicular ad hoc networks. In: Journal of network and computer applications, vol. 36. Elsevier; 2013. p. 1275–86. no. 5.
[26] Lusheng M, Karim D, Barend VW, Jacobus, Yskandar H. Performance evaluation of ieee 802.11p mac protocol in vanets safety applications. In: 2013 IEEE wireless communications and networking conference (WCNC). IEEE; 2013.
[27] Sutton O. Introduction to k nearest neighbour classification and condensed nearest neighbour data reduction. In: University lectures. *University of Leicester*; 2012.
[28] Liaw A, Wiener M, et al. Classification and regression by random forest. In: R news. vol. 2; 2002. p. 18–22. no. 3.
[29] Aparicio-Navarro FJ, Kyriakopoulos KG, Parish DJ. A multi-layer data fusion system for wi-fi attack detection using automatic belief assignment. In: World congress on internet security. WorldCIS; 2012. p. 45–50.
[30] Gaikwad DP, Thool RC. Intrusion detection system using bagging ensemble method of machine learning. In: IEEE international conference on computing communication control and automation; 2015.
[31] Maglaras LA, Al-Bayatti AH, He Y, Wagner I, Janicke H. Social internet of vehicles for smart cities. J Sens Actuator Netw 2016;5(1):3.
[32] Bayen AM, Siauw T. Interpolation. An Introduction to MATLAB Programming and Numerical Methods for Engineers, 2015, https://www.sciencedirect.com/topics/engineering/linear-interpolation; 2015.
[33] Sommer C, German R, Dressler F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Trans Mob Comput 2015;10(1):3–15.
[34] Boban M, Barros J, Tonguz OK. Geometry-based Vehicle-to-Vehicle channel modeling for large-scale simulation. IEEE Trans Veh Technol 2016;63:4146–64.
[35] What is r?. https://www.r-project.org/about.html; 2017.
[36] Raya M, Hubaux J-P. Securing vehicular ad hoc networks. J Comput Secur 2007; 15(1):39–68.
[37] Bayat M, Barmshoory M, Rahimi M, Aref MR. A secure authentication scheme for vanets with batch verification. Wirel Netw 2015;21(5):1733–43.
[38] Ferrag MA, Maglaras L, Ahmim A. Privacy-preserving schemes for ad hoc social networks: a survey. IEEE Commun Surve Tutorials 2017;19(4):3015–45.