The Impact of Malicious Nodes Positioning on Vehicular Alert Messaging System

Wafa Ben Jaballah[a,*], Mauro Conti[b], Mohamed Mosbah[c], Claudio E. Palazzi[b]

[a] *Orange Labs, Paris, France*
[b] *Department of Mathematics, University of Padua, Italy*
[c] *LaBRI, Bordeaux INP, University of Bordeaux, CNRS, UMR 5800, France*

Abstract

ICT components of vehicular and transportation systems have a crucial role in ensuring passengers' safety, particularly in the scenario of vehicular networks. Hence, security concerns should not be overlooked, since a malicious vehicle might inject false information into the intervehicle wireless links, leading to life and money losses. This is even more critical when considering applications specifically aimed at improving people's safety, such as accident warning systems. To assess the scenario of such type of applications in a vehicular network, we have performed a thorough evaluation of accident warning systems under a position cheating attack. As one of the main contributions of this paper, we determine the impact of a different number of malicious vehicles on delaying the alert warning messages. In particular, we study the impact of the position of malicious vehicles on delaying alert messages. We identify the most effective strategies that could be used by malicious vehicles in order to maximize the delay of the alert message, and thus strengthen the impact of the attacker. Finally, we pinpoint that even with a small number of malicious vehicles, the positioning cheating attack can significantly increase the delay of the alert message when compared to a scenario without attack.

Keywords: Vehicular Safety, Alert Messaging Warning, Position Cheating Attack.

1. Introduction

Nowadays, the common goal of major projects on transportation and vehicular systems is to improve the safety of passengers through intervehicle communication technology [1, 2, 3, 4, 5, 6, 7, 8]. This kind of applications requires vehicles' position awareness, in order to react in real time for safety critical tasks. For instance, when an accident happens, involved vehicles can alert all the approaching vehicles by sending a short-range alert message. The alert message is then reforwarded throughout the platoon of vehicles that are traveling toward the accident. Vehicles, on receiving such alert message, can change direction or stop to avoid being involved in the pileup. Therefore, minimizing the broadcast of delivery time of the alert message is one of the main challenges for intervehicular communication. Recent research has demonstrated that the broadcast time is strictly

*Corresponding Author

Email addresses: wafa.benjaballah@orange.com (Wafa Ben Jaballah), conti@math.unipd.it (Mauro Conti), mosbah@labri.fr (Mohamed Mosbah), cpalazzi@math.unipd.it (Claudio E. Palazzi)

related to the number of message relays (hops) and the network congestion [1, 5, 6, 9, 10, 11]; and the whole process requires an accurate information on vehicles' position.

When a vehicle disseminates a wrong position it influences the broadcast of alert message, either by delaying its transmission or interrupting its forwarding. In this case, when an accident happens, the alert message will be delayed and thus the broadcast information will be no longer crucial for these vehicles. Thus, the position cheating attack could lead to life and money losses. As an example, the position cheating attack could be leveraged by terrorists in order to kill or injure people.

Efforts have been made by both industrial and academic communities to provide secure positioning solutions, to verify and detect vehicles cheating about their positions [2, 3, 9, 12]. These solutions are not completely effective [12, 20] and come with a cost in terms of implementation, deployment, energy and bandwidth occupation. In order to improve their effectiveness and reduce the required overhead, we need to thoroughly understand the impact of such attacks depending on the number and placement of the malicious vehicles. In essence, the following question seems to be unanswered: *How the number and the positioning of malicious vehicles affect the system performance?* Moreover, there is a real concern for vehicles cheating about their positions as in [24, 25].

In this paper, we analyze position cheating attacks on vehicular safety applications. In particular, we consider applications that maximize the speed of propagation of alert warning messages, and study the impact of the position cheating attack on the performance of the vehicular system. The results show that the performance of an alert broadcast algorithm under this attack depends not only on the number of malicious vehicles, but also on their position in the platoon. From our results, we can determine a way to strengthen the capabilities of an attacker even when employing few malicious vehicles.

The remaining part of the paper is organized as follows. The next section overviews related work regarding position cheating dissemination in vehicular communications, and possible countermeasures. Section III points out the case study for vehicular safety applications. In Section IV, we present the particular problem of position cheating attack and thus the motivation for a closer look into these scenarios. In Section V, we analyze the impact of positioning malicious vehicles, and we present the simulation results of the analyzed scenarios. Finally, Section VI concludes the paper.

2. Related Work

Manufacturers are about to make a cutting-edge step in terms of vehicular technologies, by letting vehicles communicate with each other. In this way, vehicles will dramatically increase their environment awareness, thereby increasing safety and optimizing traffic [1, 2, 4, 9, 13, 14, 15]. However, different vehicular applications have specific requirements and characteristics. For instance, vehicular safety applications require position awareness from vehicles, in order to react in real time for safety critical tasks. This information will help the vehicle to brake fast, based on a warning message received from another vehicle. Also, a vehicle could be able to indicate an accident's location as well as to determine whether it should react to a received message. For example, when a vehicle has already passed the location of an accident, the broadcast information is no longer crucial for it.

In this section, we briefly review the different algorithms for vehicular communications that aim to disseminate broadcast message as fast as possible. Various proposed algorithms in the literature

require vehicles to know and share their positions. One class of solutions proposes high throughput dissemination schemes based on formation of a multi-hop backbone network [21, 22, 27, 28, 29]. In [21], the authors analyze a networking protocol when used to broadcast message flows generated by a road side unit along a linear road, forming a vehicular network structure. In this scheme, they require to elect nodes that act as relay nodes for a period of time based on the proximity of such nodes to targeted optimal positions. Their scheme aims to attain a high end-to-end throughput rate, while at the same time assuring low-packet delivery delay and discard ratios. This class of solutions requires an election process without nodes cheating about their position. In particular, a malicious relay node could cheat about its location claiming to be farther than it actually is. Moreover, a malicious vehicle could induce a denial of service attack by relaying a high throughput data packets, thus inducing a delay of message propagation.

A second class of solutions includes the transmission of an alert message without requiring a backbone structure [9, 11, 31, 32]. In [9], the authors propose the Fast Multi-hop Broadcast Algorithm (FMBA). FMBA aims at reducing the number of hops traversed by a message, in order to minimize its propagation delay. Vehicles in a car platoon dynamically estimate their transmission range, and exploit this information to efficiently propagate a broadcast message via multi-hop communication, but with as few transmissions as possible. In essence, the farthest vehicle in the transmission range of a message sender (or forwarder) will be statistically privileged in becoming the next (and only) forwarder. In [11], the authors have improved the fast broadcast algorithm using heterogeneous transmission range. In fact, unlike [9], the authors select the forwarder of the message as the vehicle whose transmission spans farther. As previously demonstrated by the authors in [9, 11, 31, 32], both protocols FMBA and the one in [11] are in the same class of solutions for fast message propagation. All these algorithms require that the location information should be correct, in order to benefit from the vehicular communications. However, a malicious vehicle could disseminate false position information and thus try to delay the propagation of the alert messages. Clearly, the position cheating attack has an impact on this category of solutions. In [11], a malicious vehicle could cheat on the farthest span, thus delaying the propagation of messages. Therefore, the capability to verify and detect position cheating attacks is a crucial topic that deserves investigation [12]. The position cheating attack has an impact on vehicular multi-hop communication protocols using either low message rate [9, 11] or high throughput capacity rate for the message dissemination [21, 22].

Another important thread of related work regards the position cheating attack in vehicular networks. In [16], the authors highlight the problem of position cheating; then, they propose an approach for secure positioning. The technique takes the basics of positioning systems in order to verify the vehicle positions. The main idea is to use the radio signal strength or time flight in order to detect whether a vehicle is cheating about its location. In [17], the authors present the position cheating attack as a dreadful attack. They focus on a technique in which a base station builds a trustworthy network. This technique uses the notion of "Verifiable Multilateration". The approach works as follows. Each base station evaluates the time between sending a challenge to a destination node and the arrival time of the reply. A malicious vehicle is not able to reduce the value (in the reply), however it might enlarge the distance to one base station and then delay the answer. This attack could be detected by a misleading multilateration when collecting all distance measurements. For the sake of completeness, the position cheating attack has been already investigated in other scenarios such as cognitive radio networks [23, 33, 36, 37], wireless sensor networks [34], and location-based social network services [35]. The majority of the proposed

location estimation and positioning techniques are highly vulnerable to position cheating attacks. Two serious threats to cognitive radio networks are the tracking of the position of a cognitive radio user without authorization and adversarial attacks. Estimating the location of a wireless device is a well studied problem. However, localizing primary user transmitters in the context of dynamic spectrum access is not trivial.

Although the literature carries a multitude of secure positioning protocols in vehicular communications addressing a number of countermeasures [2, 3, 12, 16, 17, 18, 19, 20, 26], there is no thorough study that investigates how number and position of malicious vehicles affect the system performance.

3. Case Study: Fast Multi-Hop Broadcast Algorithm (FMBA)

Vehicular safety applications require direct vehicle to vehicle communications due to specific requirements as the highly dynamic topology, and the stringent delay requirements. Different algorithms for fast broadcast have been proposed for vehicular safety [5, 9, 11]. The majority of these algorithms require information dissemination (e.g., current transmission range, current position, and timestamp), and run a forwarder selection algorithm.

For the sake of clarity, in the following, we focus on the Fast Multi-hop Broadcast Algorithm (FMBA) as a representative vehicular safety algorithm. Indeed, the analysis of the position cheating attack for FMBA can be adapted also to other solutions that aim to fast propagate a broadcast message, as in [11].

We assume that each vehicle knows its own location, for instance, using GPS which is widely present in nowadays cars and that provides accurate information about time and position. We also suppose there are N vehicles arranged in the platoon. A platoon can be looked at as a collection of vehicles connected by an ad hoc network and engaged in following each other longitudinally. In Table 1, we present the notation used in this paper.

Symbol	**Definition**
$CMBR$	Current Maximum Back Range
$LMBR$	Latest-Turn Maximum Back Range
TR	Actual Transmission range
$MaxRange$	How far the transmission is expected (according to the outcome of the protocol) to go backward before the signal becomes too weak to be intelligible
d	Distance between two vehicles
CW	Contention Window
$CWMax$	Maximum Contention Window
$CWMin$	Minimum Contention Window
$Hello$	Hello message transmitted by a vehicle in the estimation phase to update the transmission range
P_X	Position of Vehicle X

Table 1: Notation.

The aim of FMBA is to reduce the time required by a message to propagate from the source to the farthest vehicle in a certain area of interest [9]. To achieve this goal, FMBA exploits a distributed mechanism for the estimation of the transmission range of vehicles. These transmission

range estimations are obtained by exchanging *Hello* messages among the vehicles and are then used to reduce the number of hops an alert message has to traverse to cover a certain area of interest. This behavior leads to a decrease in the number of transmissions, as well as in the time required by a broadcast message to reach all the cars following the sender within a certain distance. FMBA is composed by two phases: the estimation phase and the broadcast phase. The former is continuously active and is meant to provide each vehicle with an up-to-date estimation of its transmission range. The latter is performed only when a message has to be broadcast to all vehicles in the sender's area of interest. To forward a packet, each receiver has to compute its waiting time before attempting to forward the message. This waiting time is expressed through a Contention Window (CW) computed using the following equation (1):

$$CW = \left| \frac{(MaxRange - d)}{MaxRange} \times (CWMax - CWMin) + CWMin \right|. \quad (1)$$

When a car has to send or forward a broadcast message, it computes the $MaxRange$ value as the maximum between the $LMBR$ and $CMBR$ values and includes it in the broadcast message. The value d is the distance between the receiver and the sender of the message. To avoid unnecessary transmissions, all vehicles between the original sender and the current forwarder abort their attempt to forward the message; whereas all vehicles behind the current forwarder compute a new CW for the next hop.

In Figure 1, we illustrate the CW computed by different vehicles through Equation 1. The farther a vehicle is from the source of a broadcast message, the smaller its CW results. The waiting time is a value computed randomly within CW. Therefore, in the considered example in Figure 1, D has the highest probability to become the next forwarder, as its waiting time is randomly chosen within the smallest CW among those assigned by FMBA to A, B, C, and D.

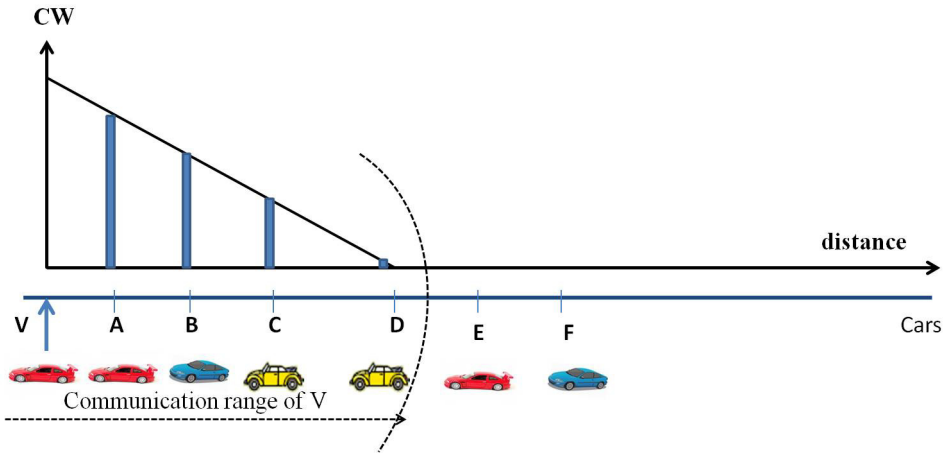


Figure 1: Contention window versus distance.

4. Position-Cheating Attack

The goal of a malicious vehicle cheating about its position is to induce a delay, by increasing the CW of honest vehicles. In this section, we analyze the impact of the position cheating attack on FMBA-like algorithms. The position cheating attack does not target only FMBA protocols, but

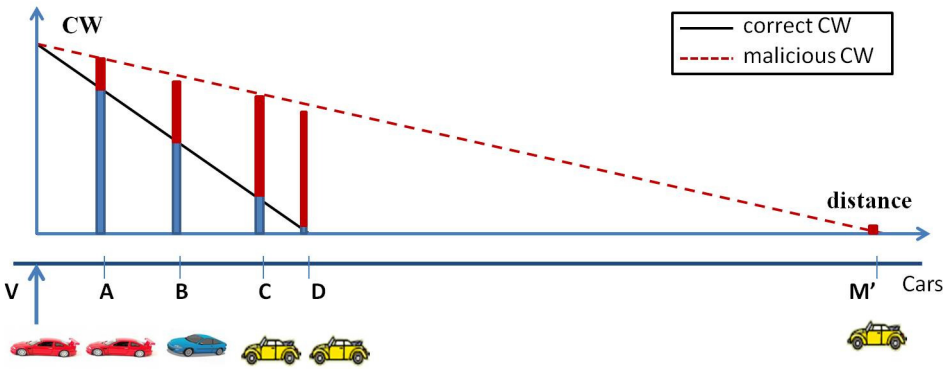


Figure 2: Impact of distance cheating on the contention period.

also the same class of protocols aiming to increase the speed of propagation of alert messages as in [5, 11]. Let us consider the scenario where a malicious vehicle could announce in a *Hello* message a false position being more distant than the real one. Then, honest nodes eventually receiving an alert broadcast message will compute unnecessarily large CWs, thus slowing down the forwarding process. For ease of presentation, Figure 2 depicts the impact of this attack presenting the CWs of some vehicles, depending on their distance from the original sender/forwarder (vehicle V) of the alert message.

In particular, as the CW of each vehicle is computed through Equation 1, without any malicious vehicle the CW function should vary as shown by the continuous line in the Figure 2. Instead, if during the estimation phase, a malicious vehicle within transmission range of V sent a *Hello* message to declare a fake position (corresponding to the one of M' in Figure 2), the transmission range estimation of vehicle V would be wrongly computed as the distance from V to M', instead of from V to D. This leads vehicles A, B, C and D to overestimate their CWs as they will consider the minimum CW in position M', as shown by the dotted line in Figure 2.

Algorithm 1 illustrates the pseudo-code for the position cheating attack as executed by a malicious vehicle M. In particular, the executing node M cheats about its claimed position (Algorithm 1, line 2). Then, M broadcasts its *Hello* message (Algorithm 1, line 3) indicating its claimed position. In our protocol, one malicious vehicle needs to send one *Hello* message in order to execute the attack, thus involving a very limited overhead and complexity.

Algorithm 1: Position-Cheating attack

1 Input: *real_position*: (Real position of M);
claimed_position: (Claimed position of M);
vehicle_ID: ID of the vehicle M;
drm: declared max range of M;
Hello msg: *Hello* message generated by M;
2 $claimed\_position > real\_position$;
3 $M \rightarrow *$: Hello msg = $< vehicle\_ID, claimed\_position, drm >$;

5. Position cheating impact: Performance Evaluation

In this section, we study the performance of the FMBA algorithm without attack, and under the position cheating attack, varying number and position of the attackers. We use for our experiments the well known NS-2 simulator (version ns-2.29). In particular, for the sake of fairness, our experiments are based on the same version of NS-2 employed in the paper proposing FMBA [10], also including the same two-ray ground reflection model to represent the wireless channel on a highway with multiple lanes [30]. In our simulations, vehicles have the same distance between each other and travel at the same speed. We used the same value of parameters as FMBA protocol, with choosing a 4 Km as area of interest. We summarize the configuration parameters in Table 2.

Parameter	**Value**
Hello Message Size	50 B
Broadcast Message Size	200 B
Idle Time Duration	100 ms
Time Slot	200 μs
$CWMin$	32 slots
$CWMax$	1024 slots
Vehicle Speed	$70 - 140$ km/h
Simulation Time	40 s
Area of Interest	4 Km
Number of Simulations	200

Table 2: Configuration parameters.

5.1. Simulation Environment

In order to evaluate the delay perceived by the vehicles, we used a discrete propagation of delay in terms of number of waited slots. This allows us to be independent from the specific wireless technology adopted (e.g., should we consider the time slots of an IEEE 802.11$b/g/p$) and maintain the generality of the results. Then, the actual propagation time is simply proportional to the number of slots and to the slot duration for the considered wireless technology [9, 10]. However, we configured NS-2 to simulate the IEEE 802.11p. The transmission range is computed based on the NS-2 two-ray ground model, including the interference between vehicles and channel errors. This is a scenario inspired by the general literature in the field [30]. We are interested in evaluating two metrics: i) The number of slots is the total number of slots perceived by all the forwarders of the message cumulatively, (each vehicle that receives the alert message will compute a waiting time before attempting to forward the message); and ii) the computed estimated transmission range by vehicles when receiving a *Hello* message, (the vehicle updates its estimated transmission range, either backward or forward, depending on the direction of the message). We evaluate thoroughly the performance of the original FMBA, FMBA with four different attacks, and with different number of malicious vehicles. In particular, the four attacks we considered are as follows: i) "FMBA, Attack #1" represents a malicious vehicle executing a position cheating attack where the claimed position is its real position + 1.5 TR, (TR is the transmission range); ii) "FMBA, Attack #2" represents that a malicious vehicle claims a position that represents its real position + 3 TR; iii) "FMBA, Attack #3" indicates the scenario where a malicious vehicle cheats about its position, and claims a position that is the sum of its real position plus a random value between 0 and 6 TR; iv) "FMBA, Attack #4" refers to a malicious vehicle claiming a position that is the sum

of its real position + 5 TR. We considered an extensive set of scenarios, and for each of them we run 200 simulations averaging their outcomes. For each scenario, we use two transmission ranges TR=300m and TR=1000m. We choose 300m and 1000m as transmission range, since these values come straightforward from the IEEE 802.11p draft, which indicates them as the boundaries for a highway scenario [38].

Before the forwarding process, every vehicle in the platoon computes a random waiting time within the CW. CW is initially set to $CWMin$, and follows a general backoff mechanism. Using the backoff mechanism, every vehicle doubles its value every time a transmission attempt results in a collision and decreases linearly with every successful transmission. The first vehicle in the platoon generates an alert message and forwards it after 37s of simulation. In particular, a $Hello$ message is transmitted every 100ms to feed the transmission range of the vehicles. In our simulations, we consider different number of malicious vehicles sending $Hello$ messages cheating about their position, thus impacting on the transmission range estimation of some vehicles. An alert message is then transmitted. This allows us to evaluate the impact of false position information. In order to understand the impact of the number of malicious vehicles, we choose different percentages of malicious vehicles varying from 1% to 50%. Later, we evaluate the impact of the position of one malicious vehicle in order to understand its impact on the message propagation. Then, in order to have a general overview, we investigate on scenarios with three malicious vehicles.

5.2. Impact of the number of malicious vehicles

In FMBA, information dissemination about vehicles' positions is fundamental. Hence, vehicles cheating about their position can have a severe impact regarding the performance of the algorithm. In the following, we assess the impact of the position cheating attack on delaying the alert message.

Let us consider the following scenario where we evaluate different percentages of malicious vehicles and their impact on degrading the performance of the vehicular system. The simulation results of the considered scenario are presented in Figure 3. This figure shows the average number of slots for different percentages of malicious vehicles. Where not differently stated, the vehicle density is 25 cars per km, and the platoon length is 4Km. In the x-axis, the percentage of malicious vehicles in the platoon varies from 1% to 50%. This figure presents two interesting outcomes. First, we notice that there is a linear increase of the number of slots, when the percentage of malicious vehicles is between 1% and 5% (with an increase of 200 slots in average). When the percentage of malicious vehicles is higher than 6%, the number of slots increases with less than 100 slots until reaching 10% of malicious vehicles. Second, when the percentage of malicious vehicles is more than 20%, there is a very slight increase (roughly the same number of slots) for all values of 20%, 30%, 40%, and 50%. It is worth noting that after a certain percentage of malicious vehicles, the impact of the attack does not differ much.

For a given number of malicious vehicles, we are motivated to study the positions that could be taken by a smart attacker that aims to degrade the performances of FMBA, in terms of estimated transmission range of vehicles and average number of slots waited before attempting to forward a message. To this aim, we elaborate the following scenario, where we consider vehicles' dispersion on the road (uniform and random distribution) in order to analyze the number of slots and the estimated transmission range. From this scenario, we could be able to analyze how the number of malicious vehicles has an impact on the alert warning system.

Figure 4(a), Figure 4(b), and Figure 4(c) represent the computed estimated transmission range for different vehicles in the platoon, with evaluating the following protocols: i) FMBA without attack; ii) FMBA where one malicious vehicle executes the position cheating attack, within the

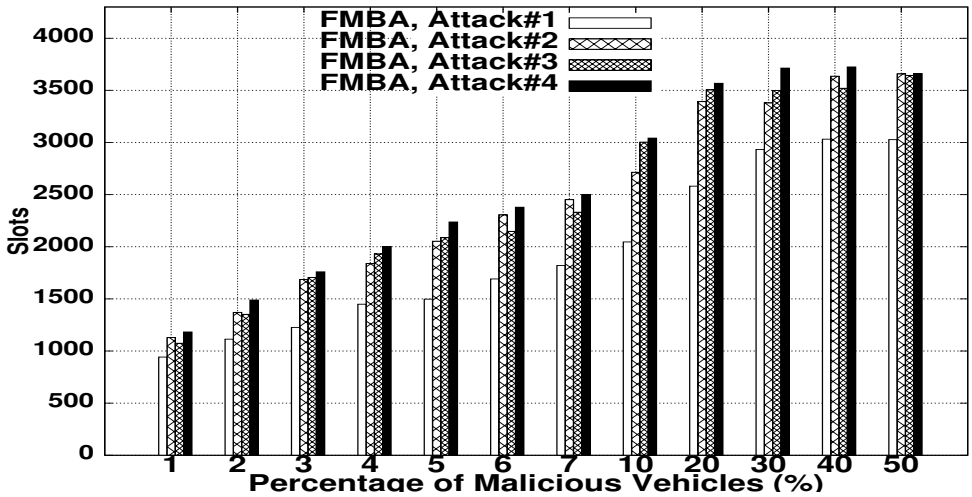


Figure 3: Average number of slots: Random malicious vehicles, TR=300m,

first hop of the source of the alert message; iii) FMBA where one malicious vehicle placed at the second hop; iv) FMBA where one malicious vehicle is at random position; v) FMBA where three malicious vehicles claim random false positions; vi) FMBA where three malicious vehicles are uniformly distributed (fixed distance from each others); vii) FMBA where three malicious vehicles are distributed in a smart way (alternative hops, i.e., at one hop we place a malicious vehicle, at the next forwarding hop, there is no malicious vehicle); viii) FMBA where seven malicious vehicles claim random positions; and ix) FMBA where seven malicious vehicles are uniformly distributed. In order to understand the behavior of the position cheating attack on the different scenarios, we evaluated the performances of the protocols under different vehicle density: 100 cars per km (Figure 4(a)); 50 cars per km (Figure 4(b)); and 25 cars per km (Figure 4(c))). For the sake of clarity, and due to space limit, we consider here the attack where the position cheating attack is the real position + 5 TR (corresponds to Attack #4) where an adversary claims a higher position; while other attacks have similar behavior.

It is interesting to note that from the different figures (Figure 4(a), Figure 4(b), and Figure 4(c)), the scenario executing the algorithm FMBA with 7 malicious vehicles with uniform distribution leads vehicles to compute higher values of the estimated transmission range. For instance, vehicles compute more than 1500m as transmission range, compared to the other algorithms having 1, 3 or 7 malicious vehicles randomly distributed. The lowest values correspond to the vehicles not affected by the attack.

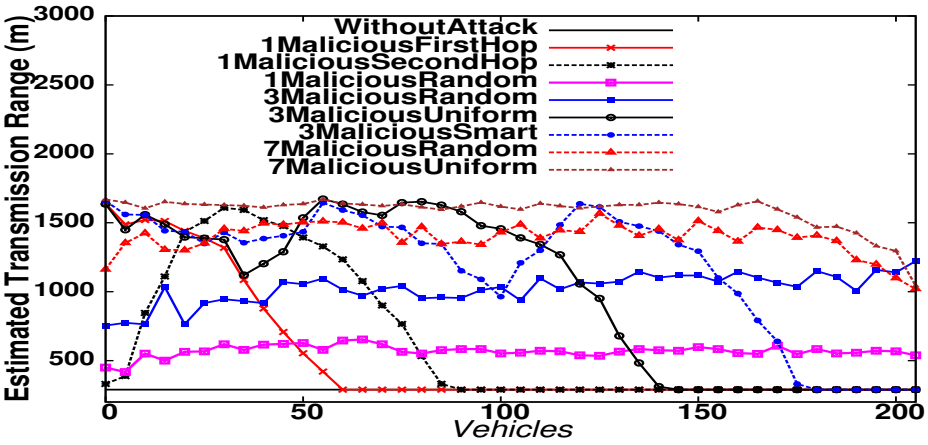
Moreover, when considering three vehicles, we notice that the smart and the uniform distributions of vehicles achieve a higher computation of the estimated transmission range compared to the random distribution of three malicious vehicles. For instance, in Figure 4(a), the computed estimated transmission range when executing the position cheating attack, with a smart distribution of 3 malicious vehicles affects more than 150 honest vehicles with a wrong estimated transmission of 1400m in average.

Another interesting point shown by Figure 4 is that the smart distribution affects a large number of vehicles compared to the uniform distribution. For instance, the smart distribution of malicious vehicles increases the number of affected vehicles in the platoon, i.e., more than 85

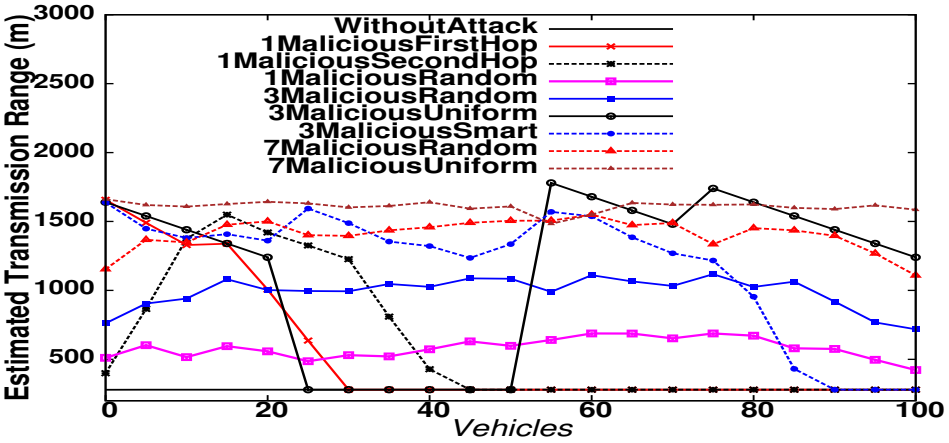
vehicles in Figure 4(b). In this case, the scenario of 3 malicious vehicles with a smart distribution achieves roughly the same performance than the scenario with 7 malicious vehicles with a uniform distribution. The attacker can achieve the same performance with small number of malicious vehicles placed along the road.

Let us consider the following scenario where one malicious vehicle is positioned within the transmission range of the first sender of the alert message. Hence, the malicious vehicle affects the estimated transmission range of the first 30 vehicles in the platoon (Figure 4(b)). However, when the malicious vehicle is positioned randomly within the second hop, it affects the first 40 vehicles with different values of the estimated transmission ranges. Moreover, with a malicious vehicle placed randomly in the platoon, it affects the estimated transmission range of all the vehicles, but with lower values (between $400m$ and $750m$).

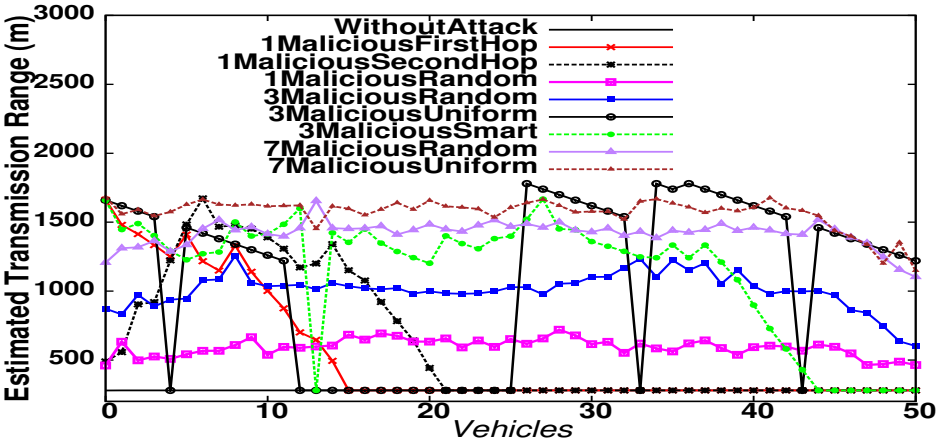
From the obtained results, it is clear that just 3 malicious nodes along our considered car platoon are already capable of significantly impact on the performance of the system. We are motivated to study the behavior of the malicious vehicles in the following scenarios: i) one malicious vehicle in the platoon; ii) two malicious vehicles in the platoon; and iii) three malicious vehicles executing a position cheating attack. For each scenario, we vary the positions of the malicious vehicles, and we are interested in evaluating two metrics: 1) the average number of slots waited before attempting to forward a message; and 2) the estimated transmission range of vehicles. From these scenarios, we draw the best positions that could be taken by malicious vehicles in order to successfully increase the propagation delay of alert message.



(a) Density=100 cars per km.



(b) Density=50 cars per km.



(c) Density=25 cars per km.

Figure 4: Estimated transmission range: TR=300m.

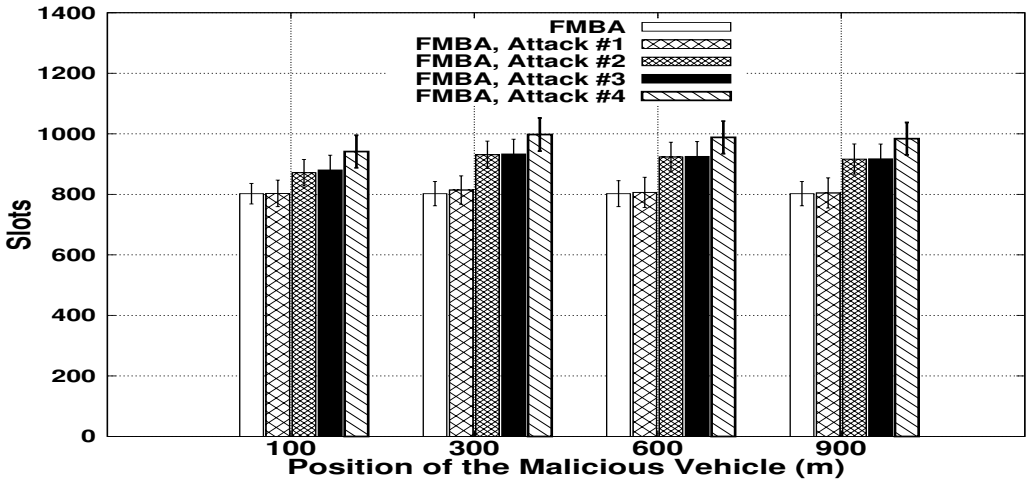


Figure 5: Average number of slots: TR=300m, density=25 cars per km.

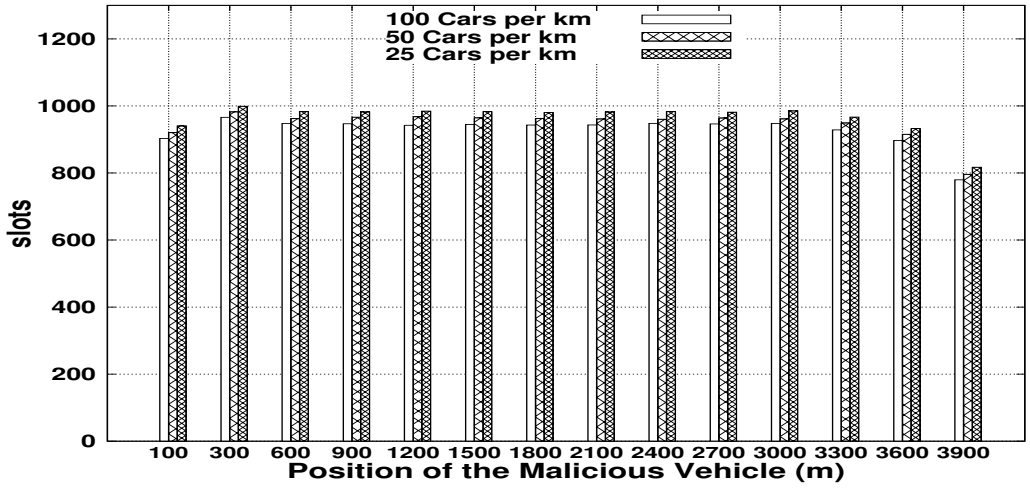
5.3. Impact of the position of one malicious vehicle

In this section, we consider one malicious vehicle with different positions in the platoon and we evaluate the total average number of slots waited before attempting to forward a message. Figure 5 represents the average number of slots required to propagate a message under TR=300m. It is clear that the original protocol FMBA without attack has to wait for a small number of slots (802 slots) compared to the other protocols. Moreover, a malicious vehicle executing "FMBA, Attack #4" increases the transmission delay of the alert warning message (approximately 980 slots in average for a malicious vehicle at 900m).

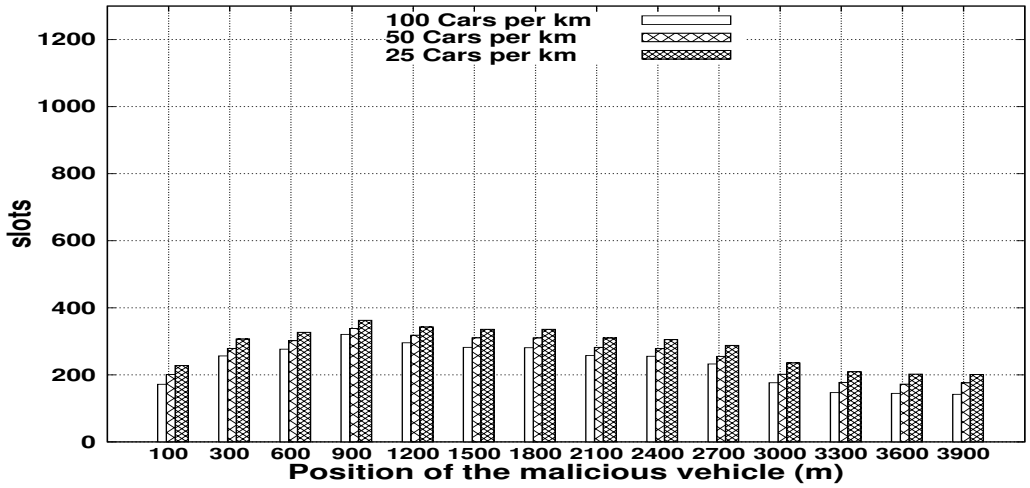
An interesting outcome from Figure 5 is that positioning the malicious vehicle at the end of the transmission range of the source of the alert message generates the highest increase of the vehicles' CW and slots, compared to the other possible positions. For instance, when the malicious vehicle is at 300m (which is close to the transmission range of the source), the algorithm "FMBA, Attack #4" increases the contention period (which is expressed in terms of number of slots waited before forwarding the alert message), and it has 995 slots. Furthermore, it is worth noting that when the malicious vehicle is at 100m from the first transmitter of the message, the contention period increases by a small number of slots, and the total average number of slots is 956, compared to the number of slots performed where the malicious vehicle is at 300m, or 600m, and 900m for the algorithms "FMBA, Attack #2", "FMBA, Attack #3", and "FMBA, Attack #4". The decrease of the number of slots waiten by vehicles at the position 100m could be explained by two facts: i) there is a small number of vehicles affected by the attack, and ii) the forwarders of the alert message compute low values of transmission ranges.

Let us focus now on the following scenario where we vary the position of the malicious vehicle in the platoon, for different transmission ranges and with different vehicle densities. The results of experiments are shown in Figure 6. In particular, in Figure 6(a), we represent the average number of slots for a TR=300m, evaluating FMBA under Attack #4, for different vehicle densities. The x-axis represents the positions taken by one malicious vehicle. When the malicious vehicle is at 100m, the total average number of slots taken by the alert warning message is 936 slots (for vehicle density of 25 cars per km). When the malicious vehicle is at 300m, the number of slots is on

average 995. Hence, there is an increase of the number of slots, since it affects more vehicles beyond the message source and first forwarder of the alert message. When we place the malicious vehicle between the positions $600m$ and $3300m$, the number of slots is roughly around 980 slots (for vehicle density of 25 cars per km). When we place the malicious vehicle at $3600m$ and $3900m$, then the average number of slots decreases. When the malicious vehicle is at $3600m$, then the number of slots is in average 930 slots. In case the malicious vehicle is at $3900m$, then the number of slots is around 817 slots, with a density of 25 cars per km. An explanation to the decrease of the number of slots by a malicious vehicle placed at $3900m$ is that, apart from the low number of affected vehicles, this will not impact on the estimated transmission range of the last forwarders of the message. The same trends are present in the charts representing the average number of slots with a TR=$1000m$ (we refer the reader to Figure 6(b)).



(a) TR=300m



(b) TR=1000m

Figure 6: Average number of slots: One malicious vehicle.

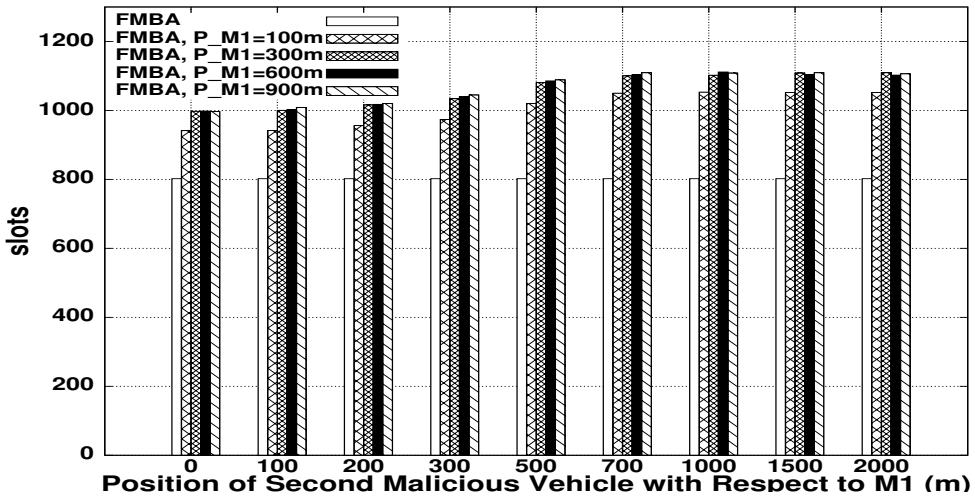


Figure 7: Average number of slots: Two malicious vehicles, TR=300m.

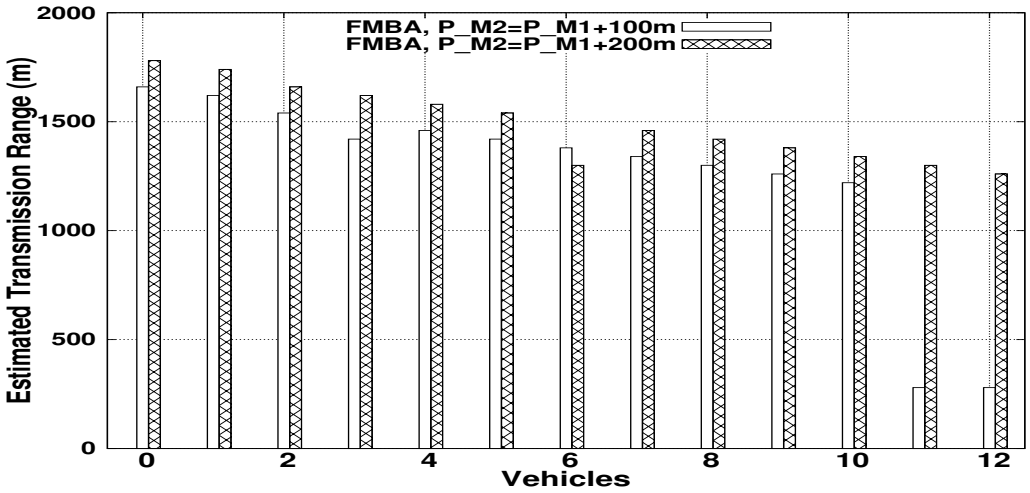
5.4. Impact of the position of two malicious vehicles

Let us now consider the scenario in which there are two malicious vehicles, $M1$ and $M2$, in the platoon. Our aim here is to evaluate the impact of both attackers. Our approach consists on varying the positions of the two vehicles on the road. To this aim, in this experiment, we vary the positions of $M1$: 100m, 300m, 600m, and 900m from the source of a message. The malicious vehicle $M2$ is placed on the following distances with respect to the position of $M1$ (P_M1): 100m, 200m, 300m, 500m, 700m, 1000m, 1500m, and 2000m.

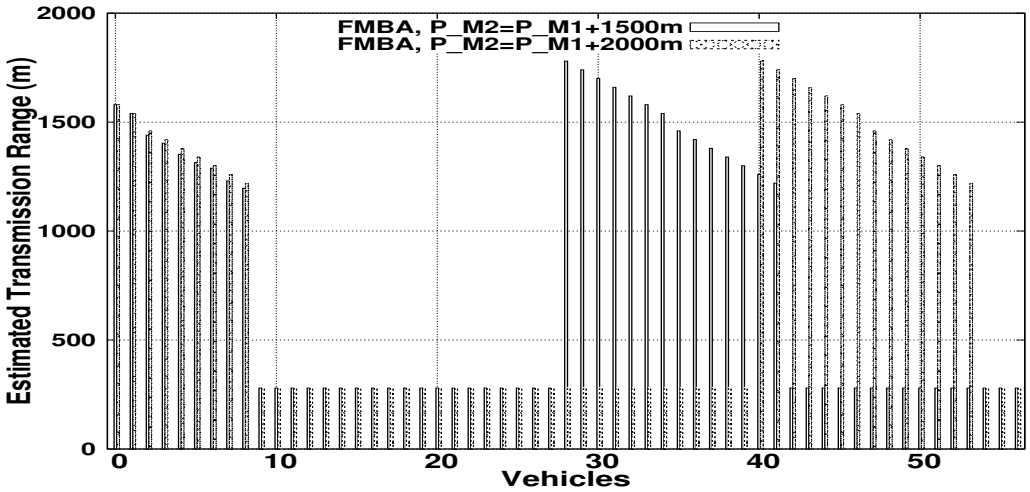
Our goal is to determine, given the position of $M1$, how the position of $M2$ further impacts on transmission delays. In Figure 7, we represent the average number of slots with varying the positions of two malicious vehicles in the platoon. It is interesting to note that having a second malicious vehicle with a distance of 100m from the first malicious vehicle increases slightly the average number of slots (more than 10 slots). When we place the second malicious vehicle at 200m from the first one, the number of slots experienced by all the evaluated algorithms increases. When the second malicious vehicle is at 300m from the first malicious vehicle, the average number of slots is increased. Another interesting outcome from Figure 7 is that a malicious vehicle at 700m increases largely the number of slots waited before attempting to forward the message for more than 100 slots. As an explanation, consider that when a second malicious vehicle is at 700m from the first one, then the total area of influence of the two is larger than when considering two vehicles at 100m and 300m. Thus, the region of the affected vehicles (potential forwarders of the message) has higher transmission range values than the configuration with the second malicious node at 100m, 300m, and 500m, respectively, from the first one. When placing the second malicious vehicle between 700m and 1500m, the average number of slots is roughly the same.

An important question entails deriving the number of affected vehicles by the attack, as well as the computed estimated transmission range. In Figure 8, we present the estimated transmission range of the affected vehicles. In the x-axis, we represent the vehicles affected by the attack.

In fact, we are interested in evaluating the following algorithms (with different parameters of the attack): "$FMBA$, P_M2=P_M1+100m", "$FMBA$, P_M2=P_M1+200m" (see Figure 8(a)). For the sake of clarity, we represent only the vehicles that are affected by the position cheating



(a) P_M2=P_M1+100m, P_M2=P_M1+200m



(b) P_M2=P_M1+1500m, P_M2=P_M1+2000m

Figure 8: Estimated transmission range: Two malicious vehicles, P_M1=100m, TR=300m.

attack. From Figure 8(a), we notice that having a second malicious vehicle executing the algorithm "$FMBA$, P_M2=P_M1+100m" affects the computation of the transmission range of 12 vehicles in the platoon, with a wrong value between 1250m and 1700m.

In Figure 8(b), we present the impact of a second malicious vehicle when P_M2=P_M1+1500m, and P_M2=P_M1+2000m, respectively. An interesting outcome from this chart is that the number of affected vehicles wrongly computing their transmission range is roughly the same for all the evaluated scenarios. Furthermore, the value of the computed transmission range for all the affected vehicles is in average between 1200m and 1750m. We also provide the scenario where the first malicious vehicle is very far from the source of the alert message. Figure 9 reports the estimated transmission range for the vehicles affected by the position cheating attack, where

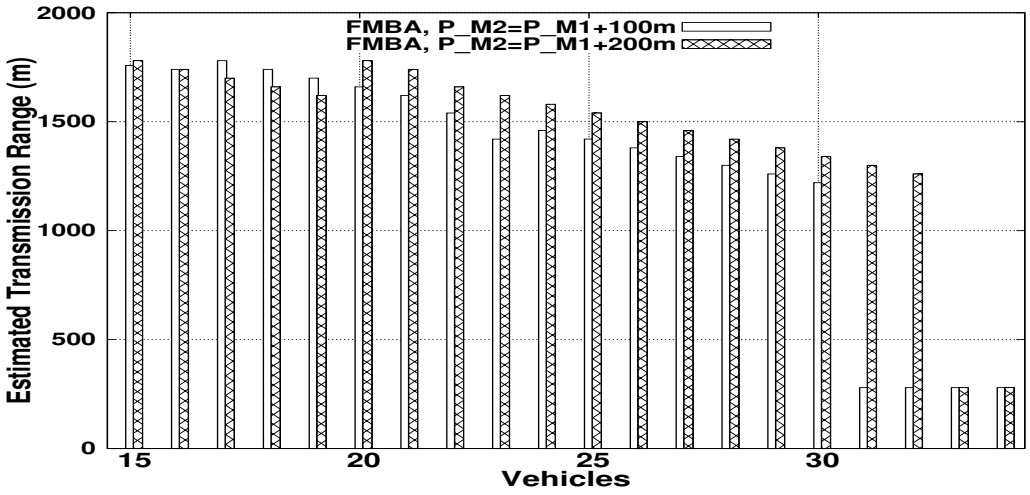


Figure 9: Estimated transmission range: P_M1=900m.

P_M2=P_M1+100m, P_M2=P_M1+200m. It is interesting to notice that there is a slight difference in terms of the estimated transmission range for the malicious vehicle that executes the attack when having P_M2=P_M1+100m (the position of $M2$ is about 100m far from $M1$), and P_M2=P_M1+200m. Furthermore, the number of vehicles wrongly computing their transmission range is roughly the same. Having a second malicious vehicle at less than 200m from the first one does not have a significant impact (20 slots of increment) compared to having just one malicious vehicle in the platoon, placed at P_M1=900m. As it is evident only vehicles from 15 to 32 vehicles are affected by the attack; however other vehicles are not affected.

5.5. Impact of the position of three malicious vehicles

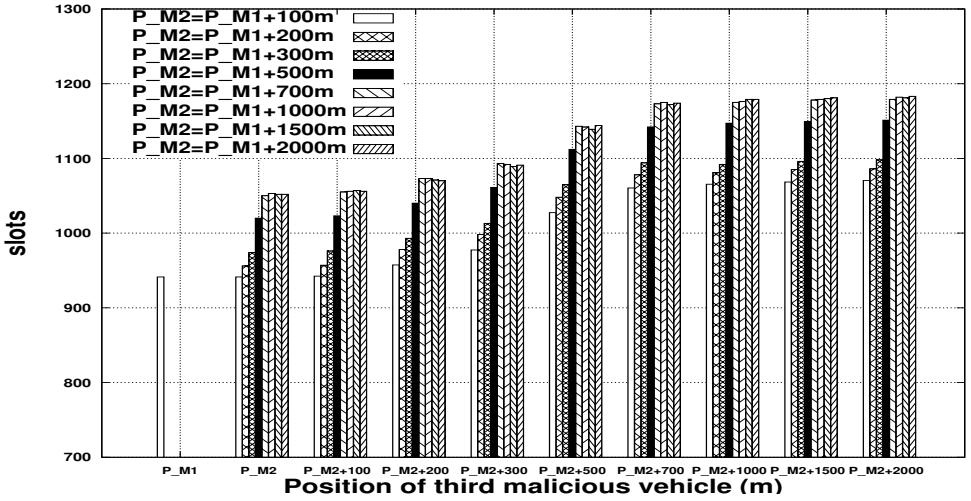
In this section, we are interested in evaluating the impact of three malicious vehicles in the platoon. Our question entails the placement of a third malicious vehicle in the platoon to increase the number of slots waited before attempting to forward a message. In order to analyze the delay incurred by an alert message, we considered scenarios with variable positions of the three malicious vehicles. In fact, we vary the positions of the malicious vehicle $M2$ with respect to $M1$. In the same way, we vary also the position of the third malicious vehicle $M3$ with respect to $M2$.

Let us focus on Figure 10, where we present the average number of slots when having one malicious vehicle at 100m from the source of the alert message and varying the position of the two malicious vehicles. For the sake of clarity, when there is no third malicious vehicle, we just present in the x-axis the position of the second malicious vehicle $M2$. Moreover, when only one malicious vehicle is active, we present in the x-axis the position of $M1$. We consider the scenario where the malicious vehicle $M2$ is at 100m from the first malicious vehicle $M1$. From this figure, we observe three interesting outcomes. First, to a very slight increase of the distance between malicious vehicles also corresponds a slight increase of the number of slots, and we have a reduced precision of the transmission range estimation (this would very slighty increase the number of slots of more than 20 slots). As a confirmation, when $M3$ is at 100m from the second malicious vehicle $M2$, the number of slots increases of more than 20 slots; this number increases very slightly when distance between $M2$ and $M3$ is 200m, and 300m. Similar, the estimated transmission range for all

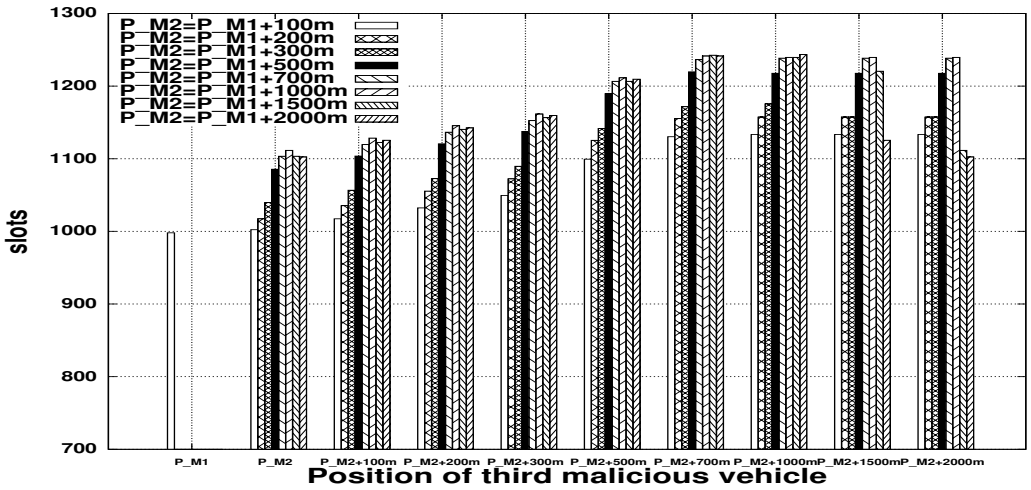
the evaluated protocols increase when the distance between malicious vehicles varies from $100m$, to $300m$. The number of vehicles and the forwarders affected by the position cheating of the three malicious vehicles is small. The second interesting point depicted in Figure 10(a) is that, when the distance between $M2$ and $M3$ is higher than $300m$, we have an increase in the total number of slots. This is due to the fact that, when the transmission ranges of malicious vehicles overlap, so do their area of influence, thus diminishing the total area (and the number of vehicles in it) affected by the attack. This is different when compared to the case where the malicious vehicles are distant from each other more than $300m$. Similar trends are present in the outcomes of the different protocols when P_M1=$300m$, and P_M1=$600m$.

Let us focus on the impact of the attack when a malicious vehicle $M1$ is placed at $900m$ from the source of the message and we vary the positions of $M2$ and $M3$. An interesting point is that the impact of the attacker decreases when the second malicious vehicle is at P_M2=$P\_M1 + 1000m$, P_M2=$P\_M1 + 1500m$, and P_M2=$P\_M1 + 2000m$.

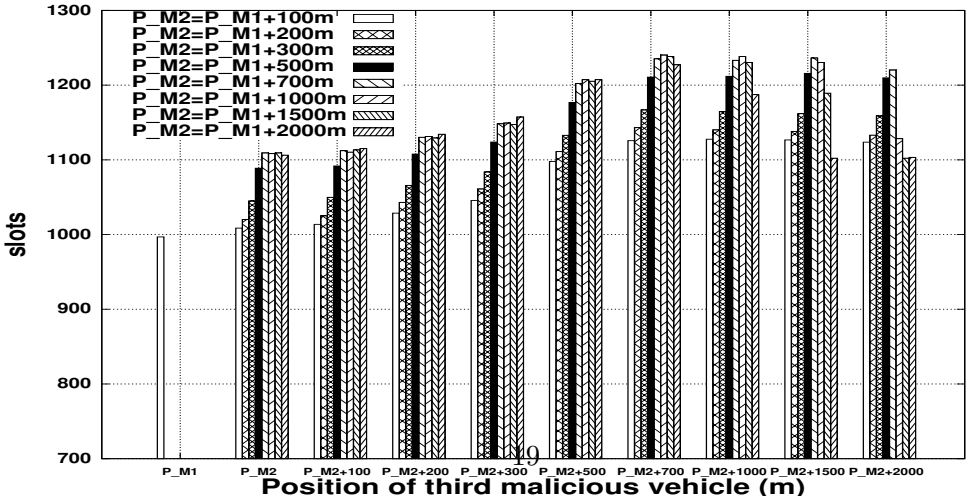
In Figure 11, we present the estimated transmission range computed by the vehicles when $P\_M1 = 900m$, $P\_M2 = P\_M1 + 2000m$, and varying the position of $M3$, using the following positions $P\_M3 = P\_M2 + 700m$, $P\_M3 = P\_M2 + 1000m$, $P\_M3 = P\_M2 + 1500m$, and $P\_M3 = P\_M2 + 2000m$. The x-axis represents the numbered, sequential position of each vehicle in the platoon. An interesting outcome is that having more than $1000m$ of distance between the second and the third vehicle does not impact on the computation of the vehicles' estimated transmission range (for $P\_M3 = P\_M2 + 1000m$, it affects the estimated transmission range only for eight vehicles at the end of the platoon). This has consequences on decreasing the delay of the alert message for $P\_M3 = P\_M2 + 1000m$, $P\_M3 = P\_M2 + 1500m$, $P\_M3 = P\_M2 + 2000m$. In this case, having three malicious vehicles that have the following positions $P\_M3 = P\_M2$+$1000m$, $P\_M3 = P\_M2 + 1500m$, $P\_M3 = P\_M2 + 2000m$, leads to the same performances as there are only two malicious vehicles in the platoon $M1$ and $M2$, in a way that $M1$ and $M2$ are placed in the following positions $P\_M2 = P\_M1 + 500m$, $P\_M2 = P\_M1 + 700m$, $P\_M2 = P\_M1 + 1000m$, $P\_M2 = P\_M1 + 1500m$, and $P\_M2 = P\_M1 + 2000m$. The worst-case scenario from a malicious vehicle point of view is when the total number of slots decreases. We refer the reader to Figure 10(c), where the number of slots achieved by the algorithm when placing P_M2=P_M1+$2000m$, and P_M3=P_M2+$2000m$ decreases of more than 120 slots compared to placing the malicious vehicle at P_M3=P_M2+$700m$.



(a) P_M1=100m

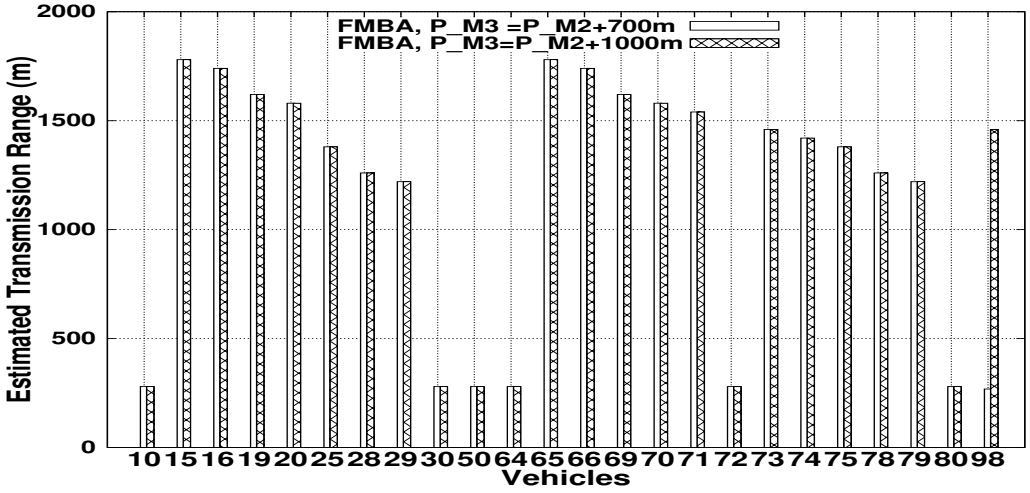


(b) P_M1=600m

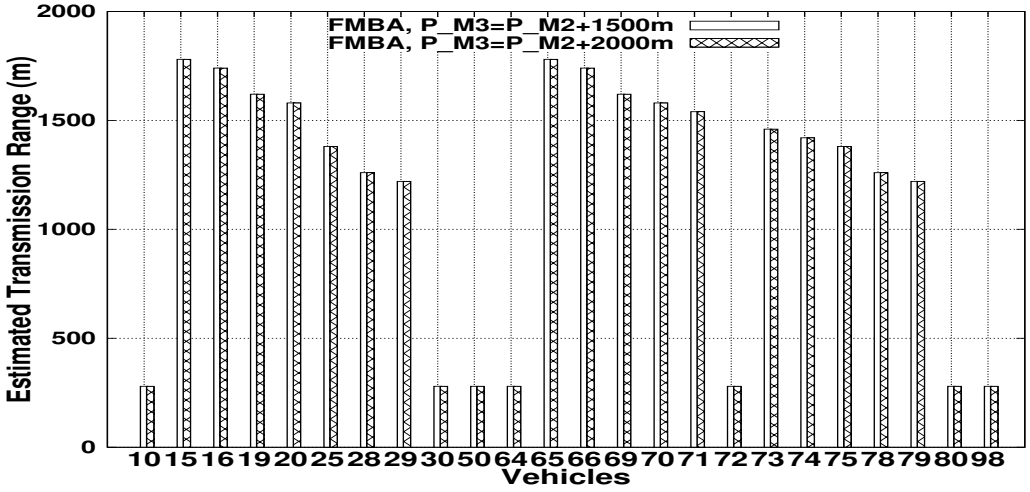


(c) P_M1=900m

Figure 10: Average number of slots: Fixing $M1$, varying $M2$ and $M3$.



(a) P_M3=$P\_M2 + 700m$, P_M3=$P\_M1 + 1000m$



(b) P_M3=$P\_M2 + 1500m$, P_M3=$P\_M2 + 2000m$

Figure 11: Estimated transmission range: Three malicious vehicles, TR=300m, P_M1=900m, P_M2=P_M1 + 2000m, Attack #4.

5.6. Lessons learned

In summary, from the simulations that we executed, we are now able to conjecture how many vehicles could execute the position cheating attack. We have found that the number of malicious vehicles that lead to the worse case scenario is bounded by the $number\ of\ hops\ /\ 2$. This is obvious since a malicious vehicle affects in average two hops (backward, and frontward) vehicles, and this is the best way to cover the whole platoon with decreasing the number of vehicles. Moreover, a uniform distribution (where each vehicle is within a fixed distance one from each other) of malicious vehicles is more effective compared to the random distribution (vehicles are randomly placed in the car platoon without a fixed distance from each other).

Positions of the malicious vehicles in the vehicles' platoon play a crucial role in determining some parameters such as the number of affected vehicles, the number of slots and the computed estimated transmission range. In our study, we concentrate on scenarios simulating different positions of malicious vehicles to understand their impact. In real world scenarios, the attackers could be the drivers of the malicious vehicles. In this case, these malicious drivers could position their vehicles with respect to the others.

In this work, we presented a more effective way of positioning malicious vehicles compared to a scenario where they are placed randomly, in order to deduce the best positions that degrade the performance of the system. Having only one malicious vehicle, the most effective position is at the end of the transmission range of the source of the message. Considering two malicious vehicles, the variation is quite visible when placing the malicious vehicle at more than $2TR$ from the other malicious vehicle (TR is the transmission range of the malicious vehicle). However, placing a malicious vehicle in a position farther than the length of area of interest-$2TR$ will reduce the impact of the added malicious vehicle. Furthermore, adding a malicious vehicle in a position farther than the length of area of interest-TR, has no impact on increasing the delay.

All those scenarios where adding another malicious vehicle does not have an impact on increasing the number of slots could be described by the following features. First, there is an overlapping area between the transmission ranges affected by the malicious vehicles. Second, the number of affected vehicles decreases. Third, the number of affected vehicles are at the end of the platoon (affecting only the last hops), and thus the estimated transmission ranges of all the forwarders of the alert message are not affected.

Through this study, we evaluate the impact of malicious nodes positioning on a vehicular alert messaging system. Hence, our results also demonstrate that security cannot be overlooked when creating an alert messaging system; rather, it should be taken into careful consideration since the beginning of the design process.

6. Conclusion

Due to the safety and the vital role of vehicular and transportation systems, security concerns should not be overlooked. In particular, in this paper, we addressed the problem of vehicles cheating about their positions, and hence degrading the performance of the vehicular safety system. We pinpointed that there was still a need to understand the impact of such attacks on the resources of the adversary, particularly in terms of the number of malicious vehicles and the way the adversary places them. We filled this gap by studying carefully the impact of the number of malicious vehicles as well as their positioning on the area of interest. Furthermore, we have shown that both the number of malicious vehicles and their careful distribution significantly contribute to the impact of the attack.

7. Acknowledgments

Mauro Conti is supported by a Marie Curie Fellowship funded by the European Commission (agreement PCIG11-GA-2012-321980). This work is also partially supported by the EU TagItSmart! Project (agreement H2020-ICT30-2015-688061), the EU-India REACH Project (agreement ICI+/2014/342-896), the Italian MIUR-PRIN TENACE Project (agreement 20103P34XC), and by the Project Tackling Mobile Malware with Innovative Machine Learning Techniques funded by the University of Padua.
This study has been carried out with financial support from the French State, managed by the French National Research Agency (ANR) in the frame of the Investments for the future Programme IdEx Bordeaux (ANR-10-IDEX-03-02).

References

[1] A. Broggi, P. Cerri, S. Ghidoni, P. Grisleri, and H. G. Jung, "A New Approach to Urban Pedestrian Detection for Automatic Braking," *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 4, pp. 594–605, 2009.

[2] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "Fast and Secure Multi-hop Broadcast Solutions for Inter-Vehicular Communication", *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 433-450, 2014.

[3] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "A secure alert messaging system for safe driving", *Elsevier Computer Communications*, vol. 46, pp. 29-42, 2014.

[4] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.

[5] M. Di Felice, A. Ghandour, H. Hartail, and L. Bononi, "Enhancing the performance of safety applications in IEEE 802.11p/WAVE Vehicular Networks," *IEEE WOWMOM*, San Francisco, CA, USA, pp. 1-9, 2012.

[6] G. Marfia, M. Roccetti, A. Amoroso, and G. Pau, "Safe Driving in LA: Report from the Greatest Intervehicular Accident Detection Test Ever," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, 2013.

[7] F. Qu , F.-Y. Wang and L. Yang, "Intelligent transportation spaces: Vehicles, traffic, communications, and beyond," *IEEE Commun. Mag.*, vol. 48, no. 11, pp. 136–142, 2010.

[8] T.-S. Dao , K. Y. K. Leung , C. M. Clark and J. P. Huissoon, "Markov-based lane positioning using intervehicle communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 8, no. 4, pp. 641-650, 2007.

[9] C. E. Palazzi, S. Ferretti, M. Roccetti, G. Pau, and M. Gerla, "How Do You Quickly Choreograph Inter-Vehicular Communications? A Fast Vehicle-to-Vehicle Multi-Hop Broadcast Algorithm, Explained," *IEEE CCNC*, Las Vegas, NV, USA, 2007.

[10] C. E. Palazzi, M. Roccetti, and S. Ferretti, "An Intervehicular Communication Architecture for Safety and Entertainment," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, pp. 90–99, 2010.

[11] A. Amoroso, M. Ciaschini, and M. Roccetti, "The farther relay and oracle for VANET. preliminary results," in *IEEE WICON*, Hawaii, USA, pp. 1-7, 2008.

[12] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "On the Performance of Secure Vehicular Communication Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 898–912, 2011.

[13] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security Challenges in Vehicular Cloud Computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 284–294, 2013.

[14] V. Daza, J. Domingo-Ferrer, F. Seb, A. Viejo, "Trustworthy Privacy-Preserving Car-Generated Announcements in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1876–1886, 2009.

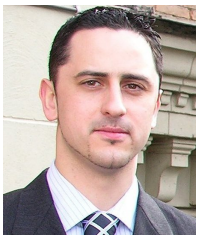
[15] C. Busold, A. Taha, C. Wachsmann, A. Dmitrienko, H. Seudie, M. Sobhani, A.-R. Sadeghi, "Smart keys for cyber-cars: secure smartphone-based NFC-enabled car immobilizer," *CODASPY*, San Antonio, TX, USA, pp. 233–242, 2013.

[16] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," *ACM VANET Workshop*, Los Angeles, CA, USA, 2006.

[17] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," *IEEE INFOCOM*, Barcelona, Spain, pp. 1-10, 2006.

[18] M. E. Mahmoud and X. S. Shen, "An Integrated Stimulation and Punishment mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3947–3962, 2011.
[19] G. Yan, S. Olariu, J. Wang, S. Arif, "Towards Providing Scalable and Robust Privacy in Vehicular Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1896-1906, 2014.
[20] J. Han, Y. -H. Lin, A. Perrig, F. Bai, "MVSec: secure and easy-to-use pairing of mobile devices with vehicles," *ACM WISEC*, Oxford, United Kingdom, pp. 51-56, 2014.
[21] F. Cuomo, I. Rubin, A. Baiocchi, P. Salvo, "Enhanced VANET Broadcast Throughput Capacity via a Dynamic Backbone Architecture," *Elsevier Ad hoc networks*, pp. 42-59, 2014.
[22] P. Salvo, F. Cuomo, A. Baiocchi, I. Rubin, "Investigating VANET dissemination protocols performance under high throughput conditions," *Vehicular communication*, vol. 2, no.4, pp. 185-194, 2015.
[23] A. Fragkiadakis, E. Tragos, I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 428-445, 2013.
[24] http://www.washingtonpost.com/cars/breaking-fca-recalls-14-million-chrysler-dodge-jeep-ram-vehicles-over-hacking-concerns/2015/07/24/e1773530-3232-11e5-a879-213078d03dd3_story.html.
[25] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/?mbid=social fb/.
[26] S. Dietzel, R. W. van der Heijden, H. Decke, F. Kargl,"A flexible, subjective logic-based framework for misbehavior detection in V2V networks", *IEEE WoWMoM*, Sydney, Australia, pp. 1-6, 2014.
[27] M. Fazio, C. E. Palazzi, S. Das, M. Gerla,"Facilitating real-time applications in VANETs through fast address auto-configuration", *IEEE CCNC*, Las Vegas, NV, USA, 2007.
[28] M. Fazio, C. E. Palazzi, S. Das, M. Gerla,"Automatic IP address configuration in VANETs", *ACM MobiCom/VANET*, Marina del Rey, Los Angeles, CA, USA, 2006.
[29] M. Di Felice, L. Bedogni, L. Bononi,"Dynamic backbone for fast information delivery in vehicular ad hoc networks: an evaluation study", *ACM PE-WASUN 2011*, Miami Beach, FL, USA, 2011.
[30] S. Martnez, C. T. Calafate, J. C. Cano, P. Manzoni,"DTN Protocols for Vehicular Networks: an Application Oriented Overview", *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 868-887, 2015.
[31] M. Roccetti, G. Marfia, A. Amoroso,"An optimal 1D vehicular accident warning algorithm for realistic scenarios", *IEEE ISCC*, Riccione, Italy, pp. 145-150, 2010.
[32] A. Amoroso, G. Marfia, M. Roccetti, "Going realistic and optimal: A distributed multi-hop broadcast algorithm for vehicular safety", *Computer Networks*, vol.55, no. 10, pp. 2504-2519, 2011.
[33] H. Celebi, H. Arslan, "Enabling location and environment awareness in cognitive radios", *Computer Communications*, vol. 31, no. 6, pp. 1114-1125, 2008.
[34] S. Capkun, J. P. . Hubeaux, "Secure positioning of wireless devices with application to sensor networks", *IEEE INFOCOM*, Miami, Florida, USA, pp. 1917-1928, 2005.
[35] W. He, X. Liu, M. Ren, "Location cheating: A security challenge to location-based social network services", *IEEE ICDCS*, Minneapolis, Minnesota, USA, pp. 740-749, 2011.
[36] R. Chen, J. M. Park and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25-37, 2008.
[37] Z. Jin, S. Anandd, KP. Subbalakshmi "Detecting primary user emulation attacks in dynamic spectrum access networks", *IEEE ICC*, Dresden, Germany, pp. 1-5, 2009.
[38] *Dedicated Short Range Communications (DSRC) Home. [Online]. Available: http://www.its.dot.gov/DSRC/.*

Wafa Ben Jaballah is a Post-Doc Researcher at Orange Labs, Paris, France. In 2014, she received her Ph.D. degree from the University of Bordeaux. She was a Post-Doc Researcher at the University of Bordeaux, France in 2014. In 2013, she was an Assistant Researcher at the Institut Polytechnique de Bordeaux. Her main research interest is in the area of network security, and web security. She has been a Visiting Researcher at University of Padua (2012, 2013, 2014, and 2015).



Mauro Conti is an Associate Professor at the University of Padua, Italy. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined the University of Padua, where he became Associate Professor in 2015. He has been Visiting Researcher at GMU (2008), UCLA (2010), UCI (2012, 2013, and 2014), and TU Darmstadt (2013). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013). His main research interest is in the area of security and privacy. In this area, he published more than 100 papers in topmost international peer-reviewed journals and conference. He is Associate Editor for several journals, including IEEE Communications Surveys & Tutorials. He was Program Chair for TRUST 2015, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Mohamed Mosbah received his Ph.D. degree from the University of Bordeaux 1, France, in 1993. He was an associate professor between 1994 and 2002. He is a full professor in computer science since 2003 at Polytechnic Institute of Bordeaux, France. His research interests include distributed algorithms and systems, formal models, security, and ad hoc and sensor networks. He participated to several national and European research projects, including collaborations with industry. He wrote more than 60 research papers published in international journals and conference proceedings. He is involved in various technical program committees and organisations of many international conferences.

Claudio E. Palazzi is an Associate Professor in Computer Science of the Department of Mathematics, University of Padua, Italy. He received his M.S. degree in Computer Science from UCLA in 2005, his Ph.D. degree in Computer Science from University of Bologna in 2006, and his Ph.D. degree in Computer Science from UCLA in 2007. From 2007 to 2010 he was an Assistant Professor at the Department of Pure and Applied Mathematics of the University of Padua. His research is primarily focused on protocol design and analysis for wired/wireless networks, with emphasis on network-centric multimedia entertainment and vehicular networks. On these topics, he is active in various technical program committees in prominent international conferences and is co-author of more than 130 papers, published in international conference proceedings, books, and journals. He is Associate Editor for several journals, including Elsevier Computer Networks.