# Impact of Security Threats in Vehicular Alert Messaging Systems

Wafa Ben Jaballah*, Mauro Conti†, Mohamed Mosbah*, Claudio E. Palazzi†
*University of Bordeaux, LaBRI, CNRS, France, Email: wafa.benjaballah@labri.fr, mosbah@labri.fr
†University of Padua, Italy, Email: conti@math.unipd.it, cpalazzi@math.unipd.it

***Abstract*—Automotive industry is about to make a cutting-edge step in terms of vehicular technologies by letting vehicles communicate with each other and create an Internet of Things composed by vehicles, i.e., an Internet of Vehicles (IoV). In this context, information dissemination is very useful in order to support safe critical tasks and to ensure reliability of the vehicular system. However, the industrial community focused more on safe driving and left security as an afterthought, leading to the design of insecure vehicular and transportation systems.**

**In this paper, we address potential security threats for vehicular safety applications. In particular, we focus on a representative vehicular alert messaging system, and we point out two security threats. The first threat concerns relay broadcast message attack that forces the honest nodes to not collaborate in forwarding the message. The second threat focuses on interrupting the message relaying to degrade the network performance. Finally, we run a thorough set of simulations to assess the impact of the proposed attacks to vehicular alert messaging systems.**

## I. Introduction

The Internet of Things (IoT) paradigm has gained attention in the academia and industry due to its abilitiy to form communications between things and people, and between things themselves [1]. Given the importance of vehicles, various initiatives propose to create safer and more efficient driving conditions [2]–[4]. Inter-Vehicular Communications (IVC) plays a vital role in this effort, enabling a variety of applications for safety, traffic efficiency, driver assistance, and infotainment. This rich set of applications is confirmed by automobile manufactorers and telecommunication companies, that have been motivated to equip every vehicle with related novel technology. This technology allows drivers and passengers from different vehicles to communicate with each other thus creating an Internet of Vehicles (IoV) to improve and enrich the driving experience. For instance, information about traffic and road conditions, as well as emergency breaking and other unexpected actions, can be exchanged among vehicles. Alert messaging is one of the most important applications among those thought to be supported by vehicular communication. Its main purpose is to broadcast an alert message generated by a vehicle acting abnormally (e.g., involved in an accident) to all following vehicles, so as to let them react as quickly as possible. Clearly, the propagation speed of the message is crucial; to this aim, the message is broadcast among vehicles, also resorting to multihop relaying.

Even though many alert message applications have been devised to quickly broadcast the alert message [2]–[4], it is crucial for such data exchange to be resilient to security attacks. These unique features of vehicular communications are a double-edged sword as they offer a large set of tools and services for drivers, as well as a set of possible attacks. The security threats could make antisocial and criminal behaviors easier, in ways that would actually jeopardize the benefits of the deployment of vehicular systems [5], [6]. Indeed, various successful attacks have been found in vehicular and transportation systems such as malware infection affecting the braking and engine systems, and relay attacks to passive keyless entry and start systems [5]–[7]. In [8], we introduced a position cheating attack that could be leveraged by an attacker to delay the transmission of an alert message. The majority of all these security vulnerabilities come from the poor design and implementations of the vehicular system.

*Contribution.* In this paper, we raise two security threats for alert messaging system that are able to jeopardize the effectiveness of the vehicular communications. Furthermore, we assess thoroughly the impact of both attacks on a representative vehicular safety algorithm, the Fast Multi-Hop Broadcast Algorithm (FMBA) [2].

*Organization.* This paper is organized as follows. The next section reviews main work on ensuring safe driving as well as analyzing security vulnerabilities in vehicular systems. Section III presents the notation and model assumptions. In Section IV, we focus on FMBA, a representative algorithm for vehicular safety. We present the relay broadcast message attack in Section V. In Section VI, we introduce the forwarding interrupting attack. We evaluate the performances of FMBA, and FMBA under the two attacks in Section VII. Finally, in Section VIII conclusions are drawn.

## II. Related Work

The past decade has witnessed a growing interest of IVC and its panoply of potential applications [2], [4]. Two research threads have been recently emerged in parallel [2], [8]. One research thread concerns providing safer vehicle

[1] 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). Mauro Conti is supported by a Marie Curie Fellowship funded by the European Commission under the agreement No. PCIG11-GA-2012-321980. This work is also partially supported by the TENACE PRIN Project 20103P34XC funded by the Italian MIUR, and by the Project "Tackling Mobile Malware with Innovative Machine Learning Techniques" funded by the University of Padua.

conditions [4]. The second thread focuses on analyzing security vulnerabilities in vehicular and transportation systems [6], [8]. In the following, we present the major techniques and approaches for enabling vehicular safety. IVC enables a vehicle to communicate with other vehicles, both directly and in a multi-hop fashion. Minimizing the broadcast delivery time is one of the main challenges for IVC. The broadcast time is strictly related to both the number of relays of the messages (hops) and the network congestion [2], [4]. In order to minimize the number of hops that a message experiences during its propagation over the network, the approach in [9] assigns different contention windows to each vehicle receiving the message. The contention windows of the vehicles are inversely proportional to the distance from the previous sender. Each of these vehicles randomly selects a waiting time within its contention window before forwarding the message. In this kind of approaches a unique, constant and well-known transmission range for all vehicles is assumed; unfortunately, this assumption is not realistic.

With FMBA, vehicles in the platoon dynamically estimate their transmission range and exploit this information to efficiently propagate a broadcast message with as few transmissions as possible [2]. 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 [4], the authors have enhanced the fast broadcast algorithm using heterogeneous transmission range, selecting the forwarder of the message as the vehicle whose transmission spans farther.

An emergent research area focuses on security of vehicular communications [6], [8], [10], [11]. In [5], the authors identify the problem of malware that can infect vehicles in a variety of ways and can cause severe consequences in the braking system. In order to defend against malware attacks, the same authors propose an approach that takes into account the specific constraints of vehicular systems, and implement a cloud-assisted vehicle malware defense framework. In [6], the authors evaluate the security issues on a modern automobile and demonstrate the vulnerability of the vehicular system. The attacker could completely ignore the driver's input including disabling the brakes, stopping the engine, etc. In [10], the authors discuss the security threats related to the integration of smartphones into automotive systems and applications, particularly considering the access control systems (doors and immobilizer) to unlock a vehicle. The authors propose a security architecture that aims to protect the electronic access tokens on the smartphone and provides advanced features such as context-aware access policies, remote issuing and revocation of access rights as well as their delegation to other users. In [7], the authors detect a relay attack in passive keyless entry and start systems in vehicles. In fact, the attacker could relay messages between the key and the other devices.

Some works focus on analyzing security vulnerabilities of message exchange in vehicular systems [8], [12]. In [8], we analyze security threats to state of the art IVC based safety applications also discussing countermeasures for these threats. We hence propose a solution which is both fast and secure in broadcasting safety related messages: Fast and Secure Multi-hop Broadcast Algorithm (FS-MBA). Considering secure broadcasting, the authors of [12] propose two broadcast authentication schemes, fast authentication and selective authentication as two countermeasures to signature flooding. Fast authentication mechanism secures periodic beacon messages. Selective authentication secures multi-hop applications in which a bogus signature may spread out and impact a significant number of vehicles.

It is clear that the road to a successful deployment of a vehicular system has to go also through vulnerability analysis. Along this line, we raise in this paper novel security threats for vehicular communications and we study their impact on a vehicular safety application.

## III. Notation and Model Assumptions

In this section, we present the notation (summarized in Table I) and assumptions used in this paper.

| **Symbol** | **Definition** |
|---|---|
| $CMBR$ | Current Maximum Back Range |
| $LMBR$ | Latest-Turn Maximum Back Range |
| $MaxRange$ | How far the transmission is expected 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 |

TABLE I
Notation

We have made the following assumptions about the general model we are considering:

- At most one malicious vehicle is in the network.
- The hearing communication range is symmetric; if a vehicle $V$ hears a vehicle $P$, then $P$ can hear $V$ as well.
- A vehicle $V$ does not know its transmission range.
- Each vehicle knows its own location, e.g., through GPS.
- The network is loosely time synchronized through GPS.

In the literature, there is a rich set of tools and algorithms for providing vehicular safety. For the sake of clarity, we choose FMBA [2] as a representative example of solutions aimed at ensuring fast propagation of alert messages.

## IV. Fast Multi-hop Broadcast Algorithm: FMBA

The aim of the Fast Multi-Hop Broadcast Algorithm (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 [2]. To achieve this goal, FMBA exploits a distributed mechanism for the estimation of the communication range of vehicles. These communication range estimations are obtained by exchanging a number of $Hello$ 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 leads to a decrease in the number of transmissions as well as the time required by a broadcast message to reach all the vehicles 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. Instead, the latter one is performed only when a message has to be broadcast to all vehicles in the sender's area of interest. In order 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 as:

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

When a car has to send or forward a broadcast message, it computes the $MaxRange$ value in the broadcast message as the maximum between $LMBR$ and $CMBR$ values. 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 based on last forward parameters to participate in the election for the next forwarder [2], [3].

## V. Relay broadcast message attack

In this section, we present the relay broadcast message attack which aims at jeopardizing the collaboration among honest nodes in forwarding alert messages. In particular, the adversary repeats the transmission of the same message, enforcing other vehicles not to forward packets. In this scenario, we consider an honest node which broadcasts a message to all the receivers in its transmission range. We suppose that the adversary intercepts the broadcast message and rebroadcasts it without waiting. First, we remark that all the nodes that receive this same broadcast message from the front will restart their broadcast procedure, which is precisely what the attacker is trying to accomplish, the attacker pushes them to restart the broadcast procedure (see Section IV). Second, all the nodes that receive this message from back, stop trying to forward this message. In fact, according to the FMBA, the message has been already propagated over the considered vehicles, and these vehicles will exit the forwarding procedure. The adversary could repeat broadcasting the same message, pushing the nodes to not forward the packet, by just restarting at each time the broadcast process.

In more details, let us consider the following scenario where vehicles $A$ (at position 0 $m$), $B$ at position 400 $m$, $C$ at position 500 $m$, $D$ at position 700 $m$, $E$ at position 800 $m$, $M$ at position 1300 $m$ , and $F$ at position 1400 $m$. The honest car ($C$) forwards its messages. In this attack scenario, we suppose that the vehicle ($M$) is malicious and does not wait for the expiration of its time interval; it sends the message immediately. When receiving the message, vehicles which are behind $M$ (e.g., car $F$) restart the broadcast process, whereas nodes which are in front of $M$ (e.g., cars $D$ and $E$) will exit the forwarding process. This attack could be executed by a malicious vehicle $M$ following different strategies. As a first strategy, $M$ does not modify the message but just broadcasts it. In this case, vehicles that are behind $M$ restart the forwarding process, thus wasting time. Vehicles that are in front of $M$ exit the forwarding process (according to the correct process of FMBA algorithm). Hence, no vehicle is able to forward the broadcast message if the adversary repeats every message sent by the source (or the forwarder). As a second strategy $M$ could modify the broadcast message and then forwards it with a high $MaxRange$ to generate slow forwarding hops with vehicles employing uncessarily high CWs. As a third strategy, malicious vehicle $M$ forwards the message with a low $MaxRange$ in order to increase the probability that more than one vehicle simultaneously attempt to forward the message, thus resulting in transmission collisions and delay.

The behaviour of the malicious vehicle running the relay broadcast attack is described in Algorithm 1. In fact, a source $S$ broadcasts a message (line 2) and the malicious vehicle $M$ retransmits it without waiting (line 4). Without attack, all the receivers of the message should wait for a random waiting time within the contention window (as confirmed by the forwarding process of FMBA). When executing the relay broadcast message attack, a malicious vehicle $M$ does not need to wait for the waiting time. Hence, it forwards immediately the broadcast message and tries to rebroadcast it. The impact of the attack leads the potential receivers of the message, that are behind the malicious vehicle, waste time by restarting the forwarding process. Vehicles that are in front of the malicious vehicle will exit the forwarding process as the message was already sent. The result of this malicious behaviour could lead not to forward the broadcast message if the adversary repeats the same message, or it could increase the delay of the broadcast message transmission.

**Algorithm 1**: Relay broadcast message attack

```
1 Input S: the sender of the message;
  $broadcast$ msg: the broadcast message of $S$;
2 $S \rightarrow$*: $broadcast$ msg;
3 $M$ intercepts the $broadcast$ msg and does not wait for the expiration
  of its waiting time;
4 $M \rightarrow$ *: $broadcast$ msg;
```

## VI. Forwarding Interrupting attack

The goal of this attack is to degrade the network performance by impeding alert message relaying. In this attack, the forwarder vehicle is malicious and tries to broadcast a message frontward but not backward. To do so, the malicious node has to be located at the very end of the transmission range and be endowed with a directional antenna. The attack can be easier to be performed if the malicious vehicle is endowed with a very sensitive receiving antenna (more sensitive than standard antennas installed in vehicles); this way, the malicious vehicle can be loosely located farther than the regular transmission range thus being sure to be the farthest vehicle receiving the message. By forwarding the alert message only frontward, vehicles in front of the malicious node will abort their forwarding procedure, as the message has already been sent farther than their position. On the other hand, vehicles behind the malicious node will simply not receive any message. Let us consider the attack scenario. An honest vehicle $C$ broadcasts a message, whereas the forwarder vehicle is $M$, which maliciously forwards the message only frontward. Vehicles ($D$, $E$, and $F$) that are in front of $M$ will hence exit the forwarding process and the forwarded message will never be propagated toward following cars. Furthermore, $n$ malicious nodes might collaborate to block the transmission of messages in different zones.

Algorithm 2 presents the execution of a forwarding interrupting attack by a malicious vehicle $M$. The aim of the malicious vehicle is to stop the propagation of the alert message in the network. In fact, without attack, the alert message broadcast by the sender $S$ is propagated to the end of the platoon (Algorithm 2, line 2). When executing the forwarding interrupting attack, the malicious vehicle intercepts the broadcast message and transmits it to the vehicles in front of it (Algorithm 2, line 4). This attack disrupts the packet transmission process and blocks the transmission of the broadcast message.

**Algorithm 2**: Forwarding interrupting attack

```
1 Input: $broadcast$ msg : the broadcast message;
  $A$: the sender of the broadcast message;
2 $A \rightarrow *$: $broadcast$ msg;
3 // M is the forwarder of the message;
4 $M \rightarrow$ front vehicles of $M$: $broadcast$ msg;
```

## VII. Performance Evaluation

We carried out an extensive experimental study to test FMBA under the two different attacks we discussed in this paper (the relay broadcast message attack, and the forwarding interrupting attack). The main tool utilized for our experiments is the well known NS-2 simulator (version ns-2.29). We use the wireless model two-ray ground reflection, the type of road is highway with multiple lanes, and vehicle's speed is between $70 - 140$ $km/h$. The contention window parameters are $CWMin$ = 32 slots, and $CWMax$ = 1024 slots. The duration of a time slot is 200 $\mu$s, and the idle time before $Hello$ message generation is 100 $ms$. For the protocol FMBA, the application message size is 200 $B$, and $Hello$ message size is 50 $B$. If no alert message happens, there is a transmission of $Hello$ messages.

### A. Simulation Environment

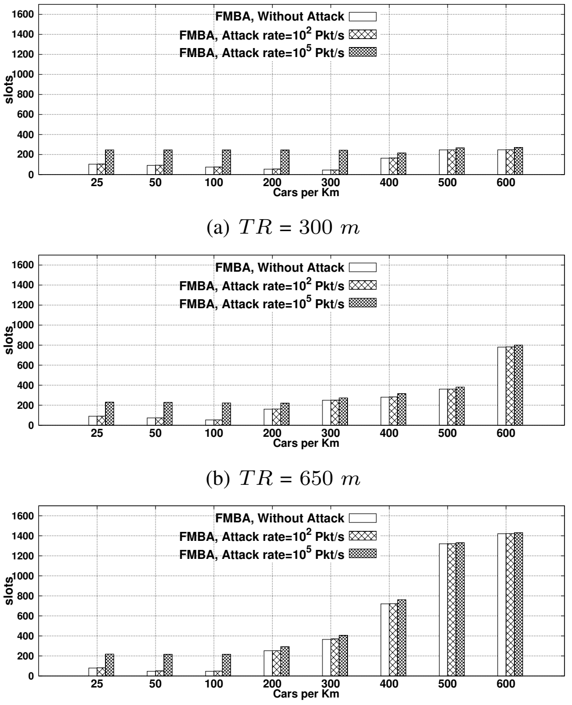
We implemented and evaluated the performances of three protocols: the original FMBA, FMBA with relay broadcast message attack, and FMBA with interrupting forwarding message attack. We simulated an extensive set of scenarios. For each scenario, we used three different transmission ranges $TR$ = 300 $m$, $TR$ = 650 $m$, and $TR$ = 1000 $m$ to show how our systems scale. In FMBA, every vehicle in the platoon computes a random waiting time within the contention window before forwarding the message. The adopted contention window is initially set to $CWMin$ and follows a general backoff mechanism by which its value doubles every time a transmission attempt results in a collision and decreases linearly with every successful transmission. We let the simulation run for 37 $s$, after which the first vehicle in the platoon generates an alert message. We compare the various schemes, we analyze their abilitiy in quickly forwarding the messages to all interested vehicles: FMBA, FMBA with attacks. For each attack, we are interested in evaluating some performance metrics. In particular, we focus on the average number of slots waited before transmitting a message, and the percentage of message propagation. The alert message has to be propagated from a certain vehicle to all following vehicles in an area of interest of $7 \times TR$. We choose $7 \times TR$ as there is no point in transmitting an instantaneous alarm farther. However, we could set a larger (or smaller) area of interest if it is more appropriate. The number of vehicles per $Km$ of (multi-lane) road varies from 25 to 600.

### B. Relay broadcast message attack

In this attack scenario, the malicious node does not wait for the expiration of its time interval, it broadcasts the message, and keeps sending the same message. The aim of the attacker is either to block the message transmission, and then not allow the forwarding of the alert message, or to delay the message transmission. In order to evaluate this attack, we consider two simulated scenarios both using FMBA and a single attacker, one with an attack rate of $10^2$ packets/$s$ and another with an attack rebroadcast rate of $10^5$ packets/$s$.

*a) Total number of slots waited:* Figure 1 reports the average number of slots required to broadcast a message. In the $x$-axis, we present the vehicles' density, and in the $y$-axis, we present the number of slots. We evaluated our scenarios using three transmission ranges $TR$ = 300 $m$, $TR$ = 650 $m$, and $TR$ = 1000 $m$. Let us consider Figure 1(a) that represents the average number of slots with using a factual transmission range $TR$ = 300 $m$. As expected, with a higher rebroadcast rate, the number of slots increases compared to a low attack rate. For example, with a vehicle's density = 100 cars per km, when the malicious vehicle rebroadcasts the message with an attack rate = $10^5$ packets/$s$, then the average number of slots waited by message forwarders is more than 200 slots; however FMBA with attack rate = $10^2$ packets/$s$ achieves less than 100 slots. An explanation to the increase of the number of slots for an attack rate = $10^5$ packets/$s$ could be the fact that the attacker delays the transmission of the alert message and keeps sending the same message. In fact, vehicles that are in front of the malicious node will exit the forwarding process, whereas the vehicles that are on the back of the malicious node will restart the broadcast process, thus this will increase the delay of the message transmission. The relay broadcast message attack could lead to the increase of the number of slots waited by all the forwarders of the message. In the same chart, it is clear that FMBA without attack and "FMBA, Attack rate = $10^2$ packets/$s$" has roughly the same performances. Actually, with low broadcast rate, the performances of the algorithm without attack and with attack are roughly the same. This demonstrated that before resending the same message by the malicious vehicle, another vehicle in the platoon is able to forward the broadcast message.

Another important point is that all the evaluated scenarios ($TR$ = 650 $m$ and $TR$ = 1000 $m$) have roughly the same trends (Figure 1(b), and Figure 1(c)). Then, we can confirm that increasing the rebroadcast rate of the alert message would delay the transmission of the packet, and even lead to postpone the alert message propagation (the warning message did not reach the last vehicle in the platoon). When the rebroadcast rate is for instance $10^5$ packets/$s$, the number of slots increases. From Figure 1(a), we see also that for a low vehicle density (for example 25 vehicles per km), the number of slots affected by the attack is higher compared to the number of slots induced by a malicious node with higher vehicle density. This could be explained by the fact that with more vehicles, there is a higher probability that the message propagates till reaching the end of the platoon. For instance, when a broadcast message is disseminated, the vehicles that receive this message will try to compute their waiting time (through the contention window) before attempting to forward the message. As the vehicle density increases, the waiting time of many vehicles will result roughly very close to each other. Thus, before the malicious vehicle attempts to rebroadcast the message, there could be another vehicle that forwards the message before receiving the same alert message.



(a) $TR$ = 300 $m$

(b) $TR$ = 650 $m$

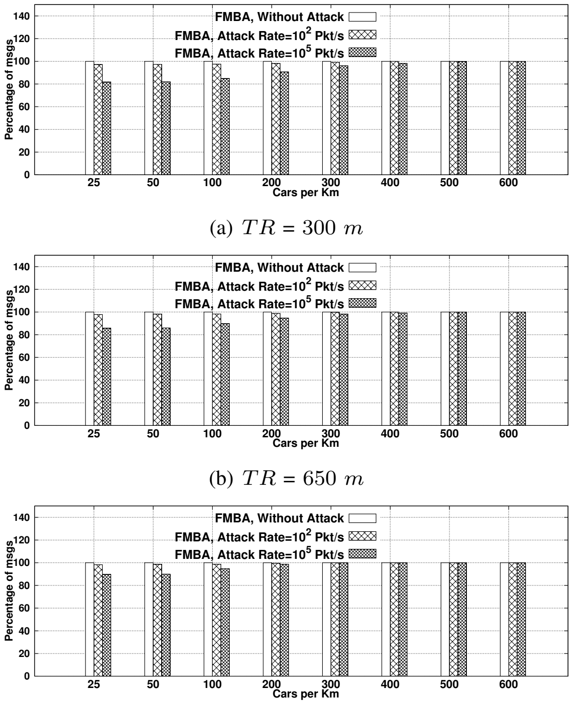
(c) $TR$ = 1000 $m$

Fig. 1. FMBA under the relay broadcast message attack: Average number of slots required to propagate a message to the end of the platoon.

*b) Percentage of Message Propagation:* In the following, we focus on computing the percentage of message propagation till the end of the platoon of the different algorithms: FMBA, and FMBA under the relay broadcast message attack. In Figure 2, we report the percentage of message propagation of FMBA, and FMBA under the relay broadcast message attack. In the $x$-axis, we present the density of vehicles, and in the $y$-axis, we present the percentage of message propagation. We evaluate FMBA under two different rebroadcast rates, $10^2$ packets per second, and $10^5$ packets per second. An interesting outcome from Figure 2(a) is that the percentage of message propagation increases when the rebroadcast rate decreases. For example, when vehicle density = 100 vehicles per km, and the rebroadcast rate = $10^5$ packets/$s$, then the percentage of message propagation is less than $85\%$; however with having a rebroadcast rate = $10^2$ packets/$s$, the percentage of message propagation is higher than $92\%$. We notice also that, with higher vehicle density, the percentage of message propagation for all the schemes under different transmission ranges increases. For instance, when the vehicle density is $400$ cars per km, the message propagation is more than $92\%$ for all the schemes. This could be explained by the fact that there is a higher probability to find a forwarder of a message when the vehicle density is high. For instance, with $TR$ = 300 $m$, and with a vehicle density of 25 cars per $km$, the message propagation is approximately $80\%$ for a rebroadcast rate $10^5$ packets/$s$. Another interesting point from Figure 2 is that, with a low transmission range ($TR$ = 300 $m$), the percentage of message propagation is lower compared to the protocols using a transmission range $TR$ = 650 $m$, or $TR$ = 1000 $m$. For instance, with a density of 25 vehicles per $km$, the percentage of message propagation is about $81\%$ ($89\%$), for $TR$ = 300 $m$ ($TR$ = 1000 $m$) respectively. This could be explained by the fact that having higher transmission range increases the probability to have a fast forwarder of the alert message.

## C. Forwarding interrupting attack

In order to evaluate the performances of FMBA under the forwarding interrupting attack, we consider two scenarios. In the first scenario, the malicious node is placed randomly under the transmission range of the source of the alert message. In the second scenario, the malicious node is placed at the end of the transmission range. In these scenarios, we evaluate the percentage of messages that propagate till the end of the car platoon. We note that in the second scenario, the forwarder selection is the same as with the original FMBA; however, the first forwarder of the message behaves maliciously and runs the forwarding interrupting attack. In Figure 3, we report the percentage of messages that traversed the whole car platoon with or without attack. In the $x$-axis, we report the vehicle's density, and in the $y$-axis we present the percentage of messages traversing the whole car platoon. From Figure 3, we notice that the percentage of message propagation is high. For instance, for a density of 25 cars per $km$, the percentage of message propagation is more than $80\%$ for FMBA under transmission ranges ($TR$ = 300 $m$, $TR$ = 650 $m$,



(a) $TR$ = 300 $m$

(b) $TR$ = 650 $m$

(c) $TR$ = 1000 $m$

Fig. 2. FMBA under the relay broadcast message attack: Percentage of message propagation.

and $TR$ = 1000 $m$). In fact, when the density of vehicles increases, there is a high probability that the message reaches the end of the platoon. This could be explained by the fact that increasing the vehicle's density also raises the probability that some vehicle will forward the message.

Let us consider the scenario where the malicious vehicle is at the end of the transmission range and forwards the message. In Figure 4, we report the percentage of message propagating till the end of the platoon, when the malicious vehicle is the forwarder of the message. From Figure 4, we notice that the attacker has a different percentage of success in blocking the alert message transmission. For instance, the percentage of messages, propagating till the end of the platoon, under the attack is approximately 23$\%$ with a $TR$ = 300 $m$ and a density of 25 cars per km. This confirms our findings that when an attacker is the last forwarder within the transmission range of the sender, then it has a higher possibility to block the transmission of the packet. Having a density of 300 vehicles per $km$, the percentage of propagation is more than 90$\%$ with $TR$ = 300 $m$ and about 100$\%$ with $TR$ = 1000 $m$.

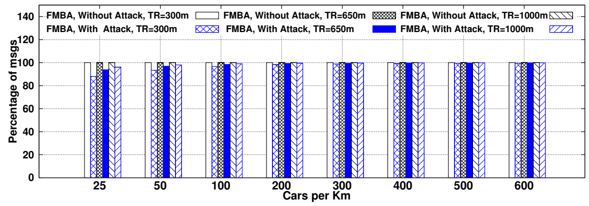


Fig. 3. FMBA under the forwarding interrupting attack with random position of the malicious node: Percentage of message propagation.

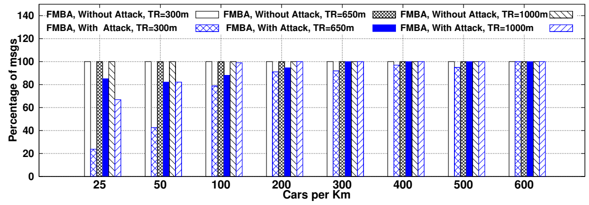


Fig. 4. FMBA under forwarding interrupting attack with a position of last forwarder of malicious node: Percentage of message propagation.

## VIII. Conclusion

In this paper, we analyse two novel security threats for vehicular communications: the relay broadcast message attack, and the forwarding interrupting attack. These two attacks have an impact either on delaying the alert message transmission, or interrupting the forwarding of the alert message. We implemented and tested our attacks on an alert message application based on the state of the art Fast Multi-Hop Broadcast Algorithm (FMBA). Our simulation results confirm that the considered attacks have a significant impact on the performances of FMBA. As a future work, we will focus on evaluating the impact of asymmetric communications, as well as the impact of practical real constraints.

## References

[1] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] C. E. Palazzi, M. Roccetti, and S. Ferretti, "An Intervehicular Communication Architecture for Safety and Entertainment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 90–99, 2010.

[3] 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," in *CCNC*, Jan 2007, pp. 960–964.

[4] A. Amoroso, M. Ciaschini, and M. Roccetti, "The Farther Relay and Oracle for VANET. Preliminary Results," in *WICON*, 2008, pp. 1–7.

[5] T. Zhang, H. Antunes, and S. Aggarwal, "Defending Connected Vehicles Against Malware: Challenges and a Solution Framework," *IEEE Internet of Things*, vol. 1, no. 1, pp. 10–21, Feb 2014.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *IEEE S&P*, May 2010, pp. 447–462.

[7] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," in *NDSS*, 2011, pp. 1–15.

[8] W. B. Jaballah, M. Conti, M. Mosbah, and C. E. Palazzi, "Fast and Secure Multihop Broadcast Solutions for Intervehicular Communication," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 1–18, 2014.

[9] E. Fasolo, R. Furiato, and A. Zanella, "Smart Broadcast Algorithm for Inter Vehicular Communication," in *IEEE WPMC*, 2005, pp. 1–6.

[10] C. Busold, A. Taha, C. Wachsmann, A. Dmitrienko, H. Seudié, M. Sobhani, and A.-R. Sadeghi, "Smart Keys for Cyber-cars: Secure Smartphone-based NFC-enabled Car Immobilizer," in *ACM CODASPY*, 2013, pp. 233–242.

[11] V. N. Lolla, L. K. Law, S. V. Krishnamurthy, C. Ravishankar, and D. Manjunath, "Detecting MAC Layer Back-off Timer Violations in Mobile Ad Hoc Networks," in *ICDCS*, 2006, pp. 63–74.

[12] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. lyer, "Flooding-resilient Broadcast Authentication for VANETs," in *ICMCN*, 2011, pp. 193–204.