Performance Impact Analysis of Security Attacks on Cross-Layer Routing Protocols in Vehicular Ad hoc Networks

Sihem Baccari, Haifa Touati, Mohamed Hadded, Paul Mühlethaler

Performance Impact Analysis of Security Attacks on Cross-Layer Routing Protocols in Vehicular Ad hoc Networks

Sihem Baccari
Unité de Recherche
Hatem Bettahar, IResCoMath
Gabes, Tunisie
sihembaccari51@gmail.com

Haifa Touati
Unité de Recherche
Hatem Bettahar, IResCoMath
Gabes, Tunisie
haifa.touati@cristal.rnu.tn

Mohamed Hadded
Institut VEDECOM
23 bis Allée des Marronniers,
78000 Versailles, France
mohamed.elhadad@vedecom.fr

Paul Muhlethaler
INRIA Paris
2 Rue Simone IFF,
75012 Paris, France
paul.muhlethaler@inria.fr

***Abstract*—Recently, several cross-layer protocols have been designed for vehicular networks to optimize data dissemination by ensuring internal communications between routing and MAC layers. In this context, a cross-layer protocol, called TDMA-aware Routing Protocol for Multi-hop communications (TRPM), was proposed in order to efficiently select a relay node based on time slot scheduling information obtained from the MAC layer. However, due to the constant evolution of cyber-attacks on the routing and MAC layers, data dissemination in vehicular networks is vulnerable to several types of attack. In this paper, we identify the different attack models that can disrupt the cross-layer operation of the TRPM protocol and assess their impact on performance through simulation. Several new vulnerabilities related to the MAC slot scheduling process are identified. Exploiting of these vulnerabilities would lead to severe channel capacity wastage where up to half of the free slots could not be reserved.**

***Index Terms*—VANET, Security, Cross-layer routing, Black-hole attack, Gray-hole attack, MAC attacks.**

I. Introduction and Motivation

Given the increasingly high accident rate on the roads, one of the major aims of Intelligent Transportation System (ITS) project which is to improve road safety. In this perspective Vehicular Ad hoc NETworks (VANETs) have been proposed to allow vehicles to communicate and exchange information describing road conditions in order to minimize accidents and improve the driving quality. VANET were officially launched with the IEEE 802.11p [1] standard, which gave rise to a new communication paradigm allowing vehicles to exchange different types of information, notably messages for signaling accidents or congestion on the road. VANETs also offer the possibility of providing so-called infotainment services to improve passenger comfort. In summary, VANETs applications can broadly be divided into three categories: safety services, traffic management and user-oriented services [2].

Taking into consideration the specific characteristics of VANETs, particularly the high mobility of vehicles that leads to rapid changes in the network topology, any routing protocol must react quickly to convey information, especially safety messages. Hence, since the launch of VANETs, several works on data routing have been conducted in order to optimize the packets dissemination in terms of end-to-end delay and packet delivery ratio. Some of these proposals [8], [9] are based on geographic position like GPSR, some are based on topology like AODV. But they are all linked only to the network layer without considering parameters of other layers. This traditional architecture cannot often support the specific needs of a vehicular network, essentially the very dynamic change in topology, but above all it does not guarantee QoS since the IEEE 802.11p standard is a contention-based MAC method, hence it cannot ensure an efficient broadcast with bounded access delays. The cross-layer concept represents a promising solution to overcome the limits of a classical routing based on a single layer and to ensure a better selection of the forwarding candidate. The TRPM protocol [3], [6] was designed as a cross-layer approach based on data exchange between routing and MAC layers. The slot scheduling is based on a completely distributed TDMA scheduling scheme called DTMAC [4], which requires confirmation of the reservation from all the neighbors, otherwise the reservation will be considered to have failed. The choice of an efficient relay node in the routing process is based on distance information and the waiting time calculated through the DTMAC scheduling.

However, with the remarkable increase in security threats, securing the data dissemination process against attacks is therefore primordial, since fake messages from attackers may cause a disruption in the road and therefore can directly affect people's life. Thus, studying the impact of attacks on data routing is extremely necessary, before forming a security solution, to find out how much it can be affected. Moreover, several works have been carried out in this context, for instance, in [5] Jose Grimaldo et al studied the impact of the black hole attack on the performance of the AODV, OLSR, DSR, and DSDV protocols in terms of Packet Delivery Ratio (PDR), Network load overhead and End to End Delay (EED) using a Panama City realistic urban scenario. In [7], Abdulaziz Alshammari et al presented a performance study of the AODV protocol in the presence of malicious nodes using a real time vehicular traffic simulation in the Greater Detroit area. The results showed a remarkable decrease in the performance in

terms of throughput, PDR and EED.
In this direction, this paper is going to outline the potential threats, that could affect the TRPM protocol. New vulnerabilities, that do not exist in the literature, have been identified in this work. These vulnerabilities result from the use of TDMA slot scheduling information in the TRPM forwarding decision and target the availability by disrupting the slot reservation process. Furthermore, many attacks threaten the data routing process of the TRPM protocol, the most important of them is the black-hole attack, in which a malicious node could delay, modify or drop all packets supposed to be forwarded. In a second step of this work, we assess the impact of those attacks on the TRPM protocol in terms of packet delivery ratio, end-to-end delay and channel usage ratio. The remainder of this paper is structured as follows: Section II summarizes the principle of the TRPM routing protocol. Section III describes security vulnerabilities that can affect data dissemination using TRPM protocol. In Section IV, we present the simulation results and the performance impact analysis. Finally, conclusion and future work are reported in Section V.

II. TDMA-aware Routing Protocol for Multi-hop Communications in Vehicular Ad Hoc Networks (TRPM)

In this section, we briefly describe the cross-layer TRPM protocol. The forwarding decisions in TRPM are based on nodes positions and slot scheduling information coming from the MAC layer, which operates under the DTMAC protocol. In the following, we firstly present the MAC layer protocol: DTMAC. Then we describe the TRPM forwarding algorithm principle.

A. Distributed TDMA-based MAC (DTMAC) Protocol

In [4], Mohamed et al. proposed a distributed and location-based TDMA-based MAC protocol called DTMAC in order to avoid collisions, caused by the hidden node problem and to provide a reliable broadcast service with bounded access delay using the vehicle location and slot reuse concept. DTMAC is based on the hypothesis that the road is divided into small areas of length equal to R, where R is the communication range. The time is partitioned into frames, each frame being partitioned into three equal sets of time slots S_0, S_1 and S_2. Each frame contains a fixed number of slots equal to T and each time slot has a fixed time duration. For collision-free scheduling, each packet transmitted by any vehicle must contain an additional information item called *Frame Information (FI)*. As shown in Figure 1, the FI consists of a set of *ID Fields (IDFs)* of size equal to the number of time slots per frame. Each IDF is mainly composed of three fields describing the state of each slot time, free or occupied, through the $SLT-STS$ field. It also allows to provide the address of the vehicle that uses the slot through the $VC-ID$ field and the type of packet transmitted through the $PKT-TYP$ field. At the end of the frame, any vehicle can determine the sets of busy and free slots. If vehicle x wishes to reserve a time slot, it must listen to the channel during the set S_j of time

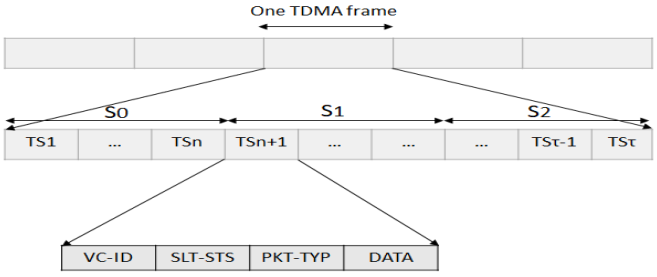

Fig. 1. Frame Information (FI) structure.

slots reserved for the area i in which it is traveling where $j = (i + 2)\ mod\ 3$. After identifying the free time slots, vehicle x randomly selects one of the free slots (say slot k) and updates its *Frame Information* locally. Thereafter, x broadcasts during slot k its FI to all its neighbors. It considers that its reservation has been successful if all the neighbors report in their FI that slot k is used by vehicle x.

B. TRPM Packet Forwarding Algorithm

TRPM routing protocol [3] is based on a cross layer architecture which relies on close communication with the MAC layer to improve transfer decisions. Thus, the forwarding relay selection algorithm takes into account on the destination vehicle's position and the slot scheduling information obtained from the MAC layer, using the DTMAC protocol.
In fact, each data transmitter uses the slot scheduling information to determine the optimal set of next hops, situated in the next or previous adjacent areas, closest geographically to the destination by observing, respectively, the set of time slots $S_{(i+2)\ \%\ 3}$ or $S_{(i+1)\ \%\ 3}$ where i represents the area of the transmitting vehicle. More precisely, when a packet is received, the vehicle looks among its neighbors for a relay node that optimizes the value of a normalized weight function WHS calculated as follows:

$$WHS_{i,j} = \alpha * \frac{\Delta t_{i,j}}{\tau} - (1 - \alpha) * \frac{d_{i,j}}{R}$$

Where:

- T represents the number of slots per frame.
- j is one of the neighbor candidates to be the next relay.
- $\Delta t_{i,j}$ represents the difference between the emission slot of vehicle i and that of vehicle j.
- $d_{i,j}$ represents the distance between the source and the destination vehicle.
- R represents the communication range.

By extracting the area ID of the transmitter vehicle contained in the received message, vehicle j can determine the appropriate set of potential relays. Then it will use the weight function WHS to select a forwarding vehicle in the next area. Finally, the node with the minimum WHS value will be selected as the best relay node.

III. Security Vulnerabilities

Data routing is the key mechanism for any type of network. Indeed, it is thanks to the means of selecting the best next hops provided by the routing protocols that data dissemination is improved. However, in a less centralized vehicular environment, vehicles move freely in a fully distributed network, and the lack of centralized control and defense mechanisms make it vulnerable to multiple routing attacks. In this context, an absence of adequate security measures, can degrade the network performance in terms of Packet Delivery Ratio (PDR), End-to-End Delay (EED), availability, etc.

Furthermore, since packet dissemination is a key service to guarantee the proper functioning of the network, this makes it an ideal target for attackers. Attackers could disable or intercept the path between the source and the destination, or even completely cut it, where information could be manipulated, modified or even lost. In this case, the effect of VANET is reversed, and it becomes a danger to passenger safety and may cause accidents.

Whatever the performances provided, any routing algorithm remains very vulnerable to security attacks. This is particularly the case when malicious nodes are present since there is a high probability that the intermediate nodes launch attacks either passive, by intercepting the transmitted data, or actively, by confusing the network with concrete attacks, like the removing, the modification or the late arrival of packets. This represents a serious problem which must be taken into account to improve the quality of services provided and mostly to ensure the availability of the network. In this context, we will study, in this section, the various threats that can target the security of the TRPM protocol. These attacks are mainly classified into two levels: (i) Network level attacks and (ii) MAC layer attacks.

A. Network Layer Attacks

Unlike traditional networks, VANET is an open environment with no fixed infrastructure, which makes network security very difficult to achieve. Some serious security vulnerabilities related to the network layer are briefly described in this section.

1) Black-Hole Attack: This attack is one of the most common types of attacks in ad hoc networks, it is an active internal attack on availability. In this attack, the malicious node presents itself as an authentic relay point that can deliver the packet correctly. As shown in Figure 2, once it receives packets, the node that is supposed to relay the packets, rejects them and thus opens the way to a denial of service attack. As a result, the impact of a black-hole attack is very severe, especially that the nature of this attack makes it difficult to detect or to prevent.

2) Gray-Hole Attack: This is a category of a black-hole attack in that the malicious node deletes packets but, in this case, this is done in a partial or a selective way. In fact, the malicious node can switch between two modes: either it remains in normal mode as a harmless node or it switches to the attack mode. Here, as shown in Figure 3, attackers rely

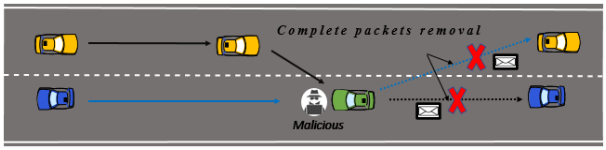

Fig. 2. Black-hole attack principle.

on a selective packet dropping method that determines how they operate during the forwarding process, for example by eliminating all packets to a particular destination, a partial dropping based on random selection method, at every time period or after a certain number of packets. Gray-hole attack detection are harder to detect than black-hole attacks, since due to the selective transfer, some traffic still flows across the network.

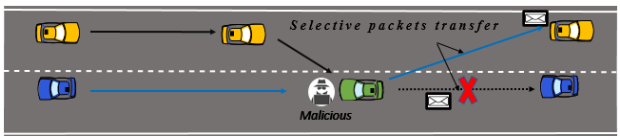

Fig. 3. Gray-hole attack principle.

3) Packet Transfer Delay: Central to VANET networks is their ability to report road problems, attackers will, of course, seek to undermine this function by launching timing attacks in which a malicious node delays the forwarding of a packet by adding an additional duration to render the message useless. VANET security applications are critical and very time-sensitive, in fact, a delay of just a few seconds can have extremely serious consequences, thus it is very important to detect and prevent these types of attack.

B. Medium Access Control (MAC) Layer Attacks

In this paper, we identify several new vulnerabilities that result from the use of the DTMAC slot scheduling information to make next hop selection decision in TRPM. The details of each identified attack are described in this section.

1) Channel Access Deny Attack: As we already detailed in Section II, during the reservation process (see Figure 4), when a vehicle wants to acquire a slot time, it must wait for confirmation from all its neighbors to be able to say that its request has been successful. In other words, all its neighbors must indicate in their FIs that the slot is being used by this vehicle. Here, the attacker could intervene to prevent the process by indicating in its FI that the slot is not reserved by this vehicle. The purpose of the attacker here is to disrupt the slot reservation process and to block access. This security breach could lead to serious problems such as a denial of service by preventing vehicles from acquiring time slots even to send security messages.

2) Slot Reservation Attack: by using the scheduling algorithm linked to DTMAC, only one slot per frame is authorized to be reserved by the same vehicle. However it is possible that a selfish vehicle requests several slots during the same frame.

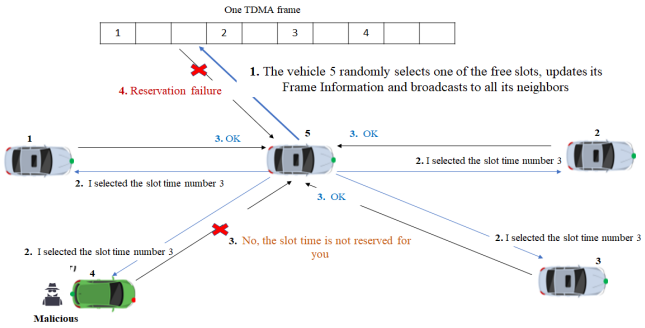

Fig. 4. Example of denial of access attack

3) Frame Information Poisoning: *Frame Information* is exchanged in clear with no guarantee of the integrity of its content. Thus, it is very easy therefore to falsify it. For example, a malicious node can falsify the state of a free slot through indicating it as occupied to prevent vehicles from acquiring it

4) Malicious MAC Behavior: this attack is a form of selfishness and anarchism in which a vehicle seizes another slot, different to its reserved one, to send its data.

5) Identity Spoofing: during this attack, a malicious vehicle creates several fake identities and then uses them in the *Frame Information* in order to achieve malicious objectives. An example could be, the use of several false identities to acquire several time slots during the same frame. Subsequently with these several identities, this attacker can create illusions of events that don't really exist.

To study the security level of the TRPM routing protocol, we injected the previously detailed attacks and analyse their impact. The simulation results are detailed in Section IV.

IV. Simulation Results and Analysis of Impact Performance

A. Simulation Setup

In order to evaluate the impact of the different attacks detailed in the previous section, we developed several attack models by injecting malicious behavior for a varying number of vehicles in the network. Three attacks are evaluated in this study:

i Black-hole attack in which malicious nodes remove or delay each packet received,

ii Gray-hole attack in which the removal or the delaying of packets is linked to a random selection function.

iii MAC level attack in which we simulate denial of access attacks.

We simulated these attacks models using the NS2 simulator. Moreover, we have used the same traffic scenarios used in [10] generated with SUMO (Simulation of Urban MObility) [11]. In all the scenarios, multi-hop unicast data packets are periodically sent from a source vehicle to a single destination through several relay nodes. The simulation parameters used in these simulations are summarized in Table I. For each attack, three scenarios are studied: (i) low density scenario where only 43 vehicles are moving in the highway, (ii) medium density with 128 vehicles and (iii) high density scenario with 256 vehicles in the network. To evaluate the performance of the TRPM protocol under the attack scenarios, we used the following metrics: The *Packet Delivery Ratio (PDR)*, *End-to-End Delay (EED)* and the *Average number of reserved slots*. The evaluation metrics are defined as follows:

TABLE I
SIMULATION PARAMETERS

Highway length	$3Km$
Vehicle speed	$120km/h$
Transmission range	$310m$
Slots/frame	100
Slot duration	$0.001s$
Simulation time	$120s$
Vehicles Density	43, 128, 256
Ratio of malicious nodes	1%, 10% ..., 30% of nodes

- Packet Delivery Ratio is defined as the ratio of total number of packets received to the total number of packets sent from the source vehicle to the destination during the simulation.
- End-to-End delay defined as the average time required to deliver all the packets sent from the source to the destination vehicle.
- Average number of reserved slots is computed as the average slots occupied per frame during the total number of frames.

B. Black-Hole Attack Impact Analysis

In the simulations we compared the performance of the TRPM protocol with and without Black-hole attack in the low, medium and high density scenarios. We computed its PDR and EED by evaluating the effect of increasing the ratio of malicious vehicles.

We, firstly, evaluate the impact of the attack in terms of PDR. As shown in Figure 5, TRPM in its normal state, i.e. without attacks, provides a very strong capacity for delivering packets that is always close to the ideal rate, i.e. 100%. Whether in the low, the medium or the high density network, TRPM without attacks achieves an average PDR of 95%. However, this capacity is very sensitive to Black-hole attacks, and a very remarkable decrease in the rate of delivered packets is observed especially when the number of black-hole attackers nodes in the network increases. For instance, in the low density scenario, when 30% of nodes work as attackers, only 13% of the data packets are successfully delivered. Moreover, we observe that the impact of the Black-hole attack on the PDR increases when the vehicle density decreases. For example, when 30% of the nodes are malicious, the Black-hole attack decreases the PDR in the high density case to about 36%, whereas in the the low density case, the PDR falls to 13%. This can be explained by the fact that the number of relay nodes in a dense network is lower than that in a low density network, since TRPM chooses the farthest node as a forwarder. Hence, the probability to have an attacker in the path between

the source and the destination is higher when the number of forwarders increases, i.e. in the low density scenario. We also

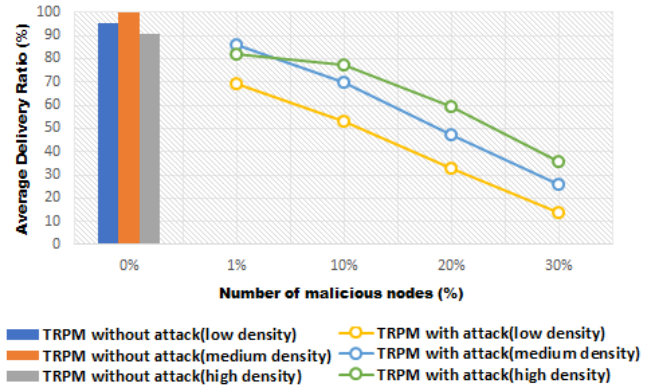

Fig. 5. Black-hole attack : The average Packet Delivery Ratio vs number of Black-hole attacker nodes

evaluate the impact of Black-hole attack on TRPM's EED, which is really one of the serious constraints for security applications in VANETs as they are sensitive to delay. In this scenario, Black-hole attacker nodes delay each received packet before relaying it to introduce an "artificial" forwarding delay. The results plotted in Figure 6 clearly illustrate the effect of the packet transfer delay attack on the EED. For instance, in the low density scenario and when 30% of the vehicles perform Black-hole attack by delaying packet forwarding, the resulting EED is 25 times greater than when TRPM is used without attack. In fact, the presence of Black-hole attackers on the highway increases the EED up to $1.8s$. This value represents a very long delay that is never suitable for several VANET security applications where the EED must not exceed a strict threshold. In fact, in order to guarantee the effectiveness of alert messages, for example in the case of a wrong way driver warning or an approaching emergency vehicle warning, the EED must not surpass a maximum of $1s$, according to [12]. Even, in the presence of a low ratio of attackers, namely 1%, the EED, in a high density network, increases from $55,57ms$ to $250,78ms$. Hence, even with only one malicious vehicle in the network, the EED is about 5 times greater, which clearly indicates the extent to which this protocol can be affected by such attacks.

C. Gray-Hole Attack Impact Analysis

In this section, we analyze the performance of TRPM under Gray-hole attack. In the same way as before, we evaluated its PDR and EED while increasing the ratio of malicious vehicles and varying the network density. Similarly to the Black-hole attack, as shown in Figure 7, the PDR of TRPM decreases in the presence of Gray-hole attackers but less sharply than Black-hole effect, due to the random selective transfer method.For instance, in the case of low density with 30% malicious nodes, the PDR does not exceed 47%, which means that more than half of the packets are lost due to the attack. The same for the medium density case with 30% of attackers

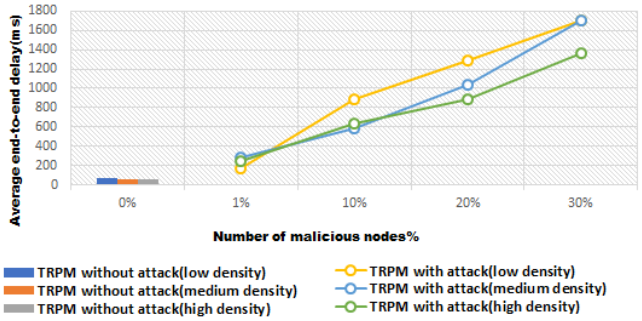

Fig. 6. Black-hole attack: Average End-to-End Delay vs number of Black-hole attacker nodes

nodes, we notice a decrease in the packet delivery rate for around 43% compared to the case without attack and less pointedly in the case of high density, where it drops to 52%. To study the EED metric, we simulated several scenarios that

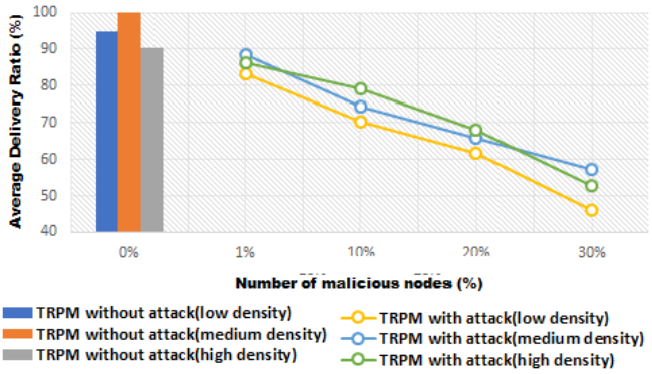

Fig. 7. Gray-hole attack: The average Packet Delivery Ratio vs number of Gray-hole attacker nodes

involve packet forwarding delay during a random period under the Gray-hole attack. Results plotted in Figure 8, confirm that the EED experiences irregular growth but slightly lower than the case of Black-hole attack. It is worth mentioning that, in a medium density network, with 20% of nodes as attackers, the EED is around 12 times greater than in the case of the TRPM without attack. These observations also show the negative impact that these attacks can have on the EED which, we recall, must not exceed a certain scale in order to guarantee timely safety packets delivery. Therefore, it is essential to enhance the TRPM protocol by introducing robust detection and prevention techniques to secure data routing against these types of attack.

D. Channel Access Deny Attack Impact Analysis

In this subsection, we evaluate the impact of the MAC level attacks, that we identified in Section III.B, on the performance of the TRPM protocol. More precisely, we simulated denial of access attack in which a malicious vehicle firstly launches a *Frame Information* poisoning attack by falsifying its FI and then it will broadcast it to its neighbor which results in an

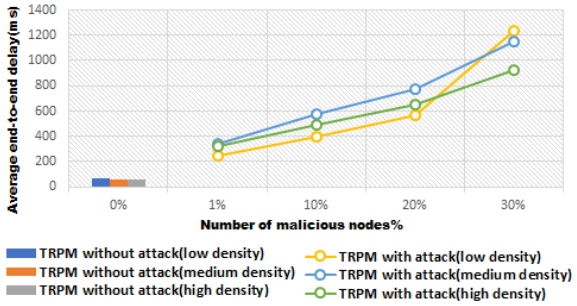

Fig. 8. Gray-hole attack: Average End-to-End Delay vs number of gray-hole attacker nodes

access attack by preventing the reservation. To further show the effect of this attack, we launched it during 30 frames in which a malicious vehicle tries to disrupt the reservation process of about 20% of the vehicles in the network. The results are evaluated according to the average number of slots occupied per frame during the total number of frames. At first glance and based on Figure 9, we can directly observe that the number of reserved slots clearly declines. For instance, in the case of low density, the access attack results in the wastage of 47% of the slots during frame number 30, which means that almost half of the slots that should be used can not be reserved, even though they are free, and therefore about half of the overall channel capacity is wasted due to this MAC attack. From there, we can clearly deduce the gravity of this attack and its impact on the slot scheduling mechanism.

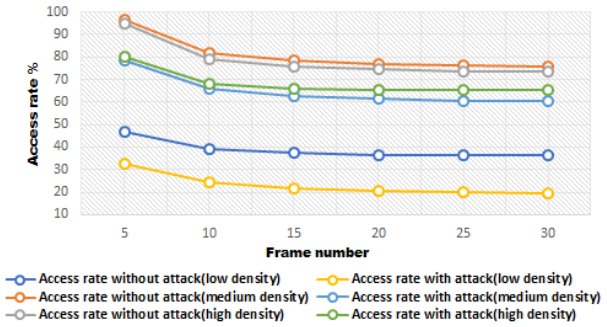

Fig. 9. MAC level Attack: Channel access rate vs frame number.

V. Conclusion

The highly dynamic nature of vehicular networks not only makes their configuration and set up difficult, but also makes them very vulnerable to attack, especially with the absence of a central control. Therefore, in order to make VANETs more secure, it is essential to study and assess the impact that attacks can have on data dissemination in these networks. In this paper we have identified the most serious attack models and have used simulation to assess their impact on the TRPM cross-layer protocol. We have identified several previously undocumented vulnerabilities which threaten the time slots scheduling process of TRPM. In addition, we have demonstrated through different attack models, the extent of the damage that these vulnerabilities can lead on the performance of the TRPM protocol. The simulation results show the severity of these attacks, on the performance of TRPM in terms of Packet Delivery Ratio, which drastically decreases to 13% under the effect of Black-hole attack. The End-to-End Delay evaluation reveals the presence of Black-hole and Gray-hole attackers in the network increases the transmission delay up to $1.8s$ which exceeds the acceptable threshold for a number of delay-sensitive VANET applications. Finally, exploiting the slot scheduling vulnerability that we identified reveals that up to 47% of free slots could not be reserved due to MAC attack which means that $1/2$ of channel capacity is wasted.
In future work, we will exploit the results of this investigation, to develop a solution for detecting and preventing attacks threatening the TRPM protocol. Mainly we will focus on the new identified MAC level attacks to provide a solution against these types of malicious behavior.

References

[1] 802.11p, IEEE standard for information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 11 : Wireless LAN medium access control (MAC) and physical layer (PHY) and physical layer (PHY) specifications amendment 6, 2010.

[2] M. Hadded, P. Muhlethaler, A. Laouiti, R. Zagrouba, and L. A. Saidane, "Tdma-based mac protocols for vehicular ad hoc networks a survey, qualitative analysis and open research issues", IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2461-2492, Jun. 2015.

[3] M. Hadded, A. Laouiti, P. Muhlethaler, and L. A. Saidane, "TDMA aware Routing Protocol for Multi-hop Communications in Vehicular Ad Hoc Networks", IEEE WCNC, San Francisco, USA, March 2017.

[4] M. Hadded, A. Laouiti, P. Muhlethaler, and L. A. Saidane, "An infrastructure-free slot assignment algorithm for reliable broadcast of periodic messages in vehicular ad hoc networks", VTC-Fall, Montreal, Canada, Sep. 2016.

[5] J. Grimaldo and R. Martí, "Performance comparison of routing protocols in VANETs under black hole attack in Panama City", CONIELECOMP, pp. 126-132, Cholula, 2018.

[6] M. Hadded, P. Muhlethaler, and A. Laouiti, "Performance evaluation of a TDMA-based multi-hop communication scheme for reliable delivery of warning messages in vehicular networks", in Proc. Wireless Commun. Mobile Comput. Conf. (IWCMC), 2017, pp. 1029-1034.

[7] Alshammari, A., Zohdy, M.A., Debnath, D. and Corser, G, "Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area", Journal of Information Security, vol. 11, pp. 71-80, 2020.

[8] A. Aboud, H. Touati. "Geographic Interest Forwarding in NDN-Based Wireless sensor Networks", in Proceedings of the 13th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA),Agadir, Morocco, 2016, pp. 1-8.

[9] Aboud, A., Touati, H. and Hnich, B., "Efficient forwarding strategy in a NDN-based Internet of Things", Cluster Computing, vol. 22, pp. 805-818, 2019.

[10] M. Hadded, P. Muhlethaler, A. Laouiti, and L. Saidane, "A Novel Angle-based Clustering Algorithm for Vehicular Ad Hoc Networks", Singapore:Springer, 2017, pp. 27–38

[11] F. Karnadi, Z. Mo, and K. chan Lan, "Rapid generation of realistic mobility models for VANET", in IEEE WCNC, Hong Kong, China, Mar. 2007, pp. 2506-2511.

[12] S. Ucar, S. C. Ergen and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination", in IEEE Transactions on Vehicular Technology, vol. 65, no. 4, pp. 2621-2636, April 2016.