# Impact Analysis of Greedy Behavior Attacks in Vehicular Ad hoc Networks

Tayssir Ismail, Haifa Touati, Nasreddine Hajlaoui, Mohamed Hadded, Paul Mühlethaler, Samia Bouzefrane, Leila Azouz Saidane

# Impact Analysis of Greedy Behavior Attacks in Vehicular Ad hoc Networks

Tayssir Ismail
*CRISTAL Lab,*
*National School of Computer Science,*
*University of Manouba, Tunisia*
taissirism88@gmail.com

Haifa Touati
*Hatem Bettaher IResCoMath Research Lab,*
*University of Gabes, Tunisia*
haifa.touati@cristal.rnu.tn

Nasreddine Hajlaoui
*Hatem Bettaher IResCoMath Research Lab,*
*University of Gabes, Tunisia*
hajlaoui.ing@gmail.com

Mohamed Hadded
*IRT SYSTEMX*
*2 Bd Thomas Gobert,*
*91120 Palaiseau, France*
mohamed.elhadad@irt-systemx.fr

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

Samia Bouzefrane
*CEDRIC Lab,*
*Conservatoire National des Arts et Metiers,*
*Paris (France)*
samia.bouzefrane@cnam.fr

Leila Azouz Saidane
*CRISTAL Lab,*
*National School of Computer Science,*
*University of Manouba, Tunisia*
leila.saidane@ensi.rnu.tn

***Abstract*—Vehicular Ad hoc Networks (VANETs), while promising new approaches to improving road safety, must be protected from a variety of threats. Greedy behavior attacks at the level of the Medium Access (MAC) Layer can have devastating effects on the performance of a VANET. This kind of attack has been extensively studied in contention-based MAC protocols. Hence, in this work, we focus on studying the impact of such an attack on a contention-free MAC protocol called Distributed TDMA-based MAC Protocol *DTMAC*. We identify new vulnerabilities related to the MAC slot scheduling process that can affect the slot reservation process on the DTMAC protocol and we use simulations to evaluate their impact on network performance. Exploitation of these vulnerabilities would result in a severe waste of channel capacity where up to a third of the free slots could not be reserved in the presence of an attacker. Moreover, multiple attackers could cripple the channel and none could acquire a time slot.**

***Index Terms*—VANET - Security - DTMAC - MAC attacks - Greedy behavior attack**

## I. Introduction and Motivation

In recent years, Intelligent Transportation Systems (ITS) [1] have gained increasing interest as a promising research area in academia. Vehicular ad hoc networks (VANETs) [2] are the most important component of ITS as they enable a fast and efficient network deployment in a wide variety of scenarios without a fixed network infrastructure. In a VANET, vehicles cooperate to collect and share information with each other, with the road infrastructure, and with other vulnerable road users. Indeed, vehicle-to-vehicle communications have the potential to make a significant contribution to overall traffic control by exchanging safety messages, accident warning messages and information on traffic conditions. They can therefore play an important role in managing complex issues such as accident rates, environmental pollution, etc.

In general, VANET interactions carry sensitive information, making them highly susceptible to any attack that could seriously impact the performance of these systems. Security is a major concern in any system, and becomes even more critical when human lives are at stake, as it is the case in VANETs. The communication protocols in the different layers of a VANET can be subject to manipulation by selfish nodes. For example, the MAC protocol and the routing protocol were designed on the assumption that all participating nodes would obey the given specifications [13]. However, nodes may deviate from the protocol specifications in order to achieve a given goal, to the detriment of honest participants. A greedy node may, for instance, disobey the wireless channel access rules in order to obtain higher throughput than other nodes. In such a case, the misbehaving node will degrade the overall performance of the network for the other users. In order to carry out a successful attack, extensive knowledge of the targeted system is required. The first step for a greedy attacker would be to assess the attack surface to access the system. Next, the attacker must look for exploitable vulnerabilities to control the external and internal vehicular network. Therefore, VANETs must ensure a certain minimal level of security and guarantee performance to establish reliable communications between the various components and achieve the full potential of their interactions.

The greedy behavior attack has been widely investigated in Vehicular Ad hoc Networks [3], [4], [5] due to its impact on network performance. Several studies have been carried out in this context, for instance, in [3], [4], Mejri et al. combine both linear regression and watchdog concepts to detect greedy nodes in VANETs at the 802.11 MAC layer. This solution relies on the presence of correlation between the different nodes' access times to the channel. Linear regression makes it possible to distinguish between a VANET under attack and a safe one. To identify the greedy nodes, a watchdog tool supervises three predefined connection parameters: the duration between two successive transmissions, the transmission time and the connection attempts of a node. The existence

of an attack is confirmed if the three defined metrics exceed the normal threshold. In [5], a game theory framework is implemented to solve the greedy behavior problem in the IEEE 802.11 CSMA/CA protocol in VANETs. Two collaboration-based tit-for-tat (TFT) strategies are proposed: Group Reputation and Cooperative Detection. Both strategies are effective in improving the decision to detect misbehavior and hence enforce MAC layer cooperation in VANETs. In the group reputation strategy, a reputation is aggregated from the node's neighbours, while in the cooperative detection strategy, a cooperative detection mechanism is proposed. These strategies are (1) resistant to ambiguous control caused by collisions and (2) able to force greedy nodes to cooperate due to the threat of retaliation. However, the majority of work carried out thus far has addressed the greedy behavior attack in 802.11 MAC protocols. Few studies in the literature identify attacks that target TDMA-based protocols like [6] and [7].

This paper discusses the potential threats that could affect the DTMAC protocol. Additional vulnerabilities, which have not been covered in the literature in the TDMA context, are identified in this study. These vulnerabilities occur as a result of using TDMA slot scheduling information in the DTMAC slot reservation process. The most important of these vulnerabilities is the neighbor reservation cancellation attack, in which a greedy node could cancel the reservations of all or a percentage of its neighbors. In a second step of this work, we evaluate the impact of these attacks on the DTMAC protocol in terms of access ratio per frame and access collision ratio.

The rest of this paper is structured as follows: Section II summarizes the principle of the DTMAC protocol. Section III describes the greedy behavior attack. In Section IV, we present the simulation results and performance impact analysis. Finally, the conclusion and future work are presented in Section V.

## II. Distributed TDMA-based MAC (DTMAC) Protocol

In this section, we briefly describe the MAC layer protocol DTMAC [8], a TDMA-based protocol that aims to avoid collisions caused by the hidden node problem and to ensure fairness and minimize interference between vehicles. The DTMAC protocol has been used in the cross-layer TRPM protocol [6] as the MAC layer protocol responsible for slot scheduling.

DTMAC is a distributed location-based TDMA-based MAC protocol for VANETs that exploits the linear feature of VANET topologies. In the DTMAC protocol, the road is divided into $N$ small fixed areas, denoted by $x_i$, $i$ = 1,..., $N$. All of these areas are equal in length to $R$, where $R$ is the communication range of the vehicles. Area identification can be easily found through maps and GPS devices. The time slots of the single TDMA frame are split into three sets, $S_0$, $S_1$, and $S_2$, assigned to vehicles in three adjacent zones: $x_i$, $x_{i+1}$, and $x_{i+2}$, respectively. Each frame comprises a constant number of time slots, denoted $\tau$, and each time slot has a fixed duration, denoted $s$. Each vehicle can detect the start time of each frame as well as the start time of a time slot.

To prevent collisions on the transmission channel, specific information, called *Frame Information* ($FI$), is added to each transmitted packet. Each time slot is dynamically reserved by the active vehicles (specifically those whose communication device is transmitting) for collision-free transmission of safety or other control messages. The $FI$, as shown in Figure 1, consists of a set of ID Fields ($IDFs$) equal in size to the number of time slots per frame, $\tau$. Each $IDF$ is composed of three fields: VC ID, SLT STS, and PKT TYP which respectively describe the $ID$ of the vehicle accessing the corresponding slot, the status of each slot, indicating whether the slot is *idle*, *busy* or in *collision*, and the type of packet transmitted by the vehicle. By exchanging messages between neighboring vehicles, they inform each other about the time slot assignment.

The DTMAC slot scheduling mechanism uses vehicle location and the concept of slot reuse to ensure that vehicles in adjacent zones have a collision-free schedule. Each active vehicle in the network must be assigned a fixed time slot in the frame for safety messages or other control packets. It is assumed that a vehicle's slot cannot be used by neighboring vehicles in the same or adjacent zones, otherwise collisions will occur. For example, if an active vehicle $v$ wants to reserve a time slot, it must determine the set of available time slots and then attempt to select one at random. It is considered that $v$ has successfully reserved a time slot only if all of its neighbors record that vehicle $v$ is using the corresponding time slot and as long as it is in the same area, it will continue to reuse it. Each vehicle $v$ that needs to reserve a time slot, will follow the same slot reservation mechanism.

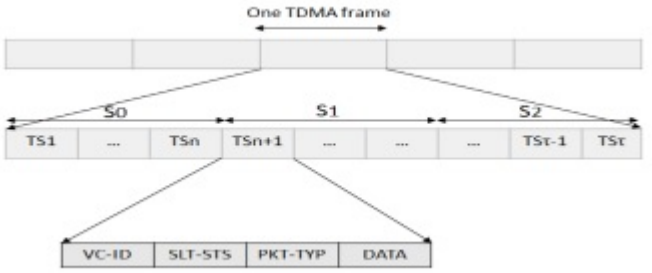



Fig. 1: Frame Information (FI) structure [9]

## III. Greedy Behavior Attacks

MAC layer misbehavior is achieved when a selfish user or attacker is able to change MAC layer parameters. A selfish user can employ different schemes to manipulate MAC layer rules. In the IEEE 802.11 protocol, a greedy user can implement a variety of strategies to maximize its access to the medium.

In the TDMA MAC protocol, a greedy user can manipulate the number of slots that it reserves; it can cancel its neighbors'

reservations and always reserve the first free slot for itself so as to have quick access to the channel.

In this paper, we identify some greedy vulnerabilities that result from the use of DTMAC slot scheduling information. These vulnerabilities are principally related to the reservation process. Details of each attack are described in this section.

### A. Cancelling neighbors' reservations

As described in Section II, during the reservation process, if a vehicle wants to acquire a time slot, it must wait for confirmation from all its neighbors before it can know that its request has been successfully completed. This implies that all its neighbors must indicate in their FIs that the slot is used by this vehicle. Here, the attacker could interfere to prevent the process by indicating in its FI that the time slot is not reserved by this vehicle. The attacker's goal here is to disrupt the slot reservation process. This security vulnerability could lead to serious consequences such as a denial of service by preventing vehicles from acquiring slots or even from sending safety messages.

In a greedy attack, to cancel its neighbors' reservations, the greedy node will scan its current zone and cancel the reservations of its neighbors by indicating in its FI that the allocated time slots are *idle*, as shown in Figure 2.

### B. Multi access attack

Using the scheduling algorithm linked to DTMAC, only one slot per frame is allowed to be reserved by a single vehicle. However, it is possible for a greedy vehicle to access more than one slot during a single frame, as illustrated in Figure 3. In this case, a greedy node will try to act like any legitimate node in the network and will attempt to acquire a time slot. Once this step has been completed, the attacker will look for any available time slots in its region. Then it will force its ID to all unreserved slots, as shown in Figure 3, in any frame as long as the attacker remains in the network. This attack is less serious than the first one in terms of affecting the reservation process since once a vehicle has successfully reserved a slot time e.g. vehicle 2 and vehicle 5, the attacker could not cancel it. However once the attacker succeeds in forcing its ID to all the free slots in its region, the vehicles that want to reserve a time slot will try to proceed with the normal reservation process of DTMAC, i.e. randomly choosing a free slot from those available, updating their FI and informing their neighbors by sending their FI. However, in the case of such an attack, no slots will be available and the reservation will fail, as shown in Figure 3a.

## 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 have developed several attack models by injecting greedy nodes for a variable number of vehicles in the network.

We simulated these attack models using the NS2 [10] simulator. The same traffic scenarios as those used in [11], generated with SUMO [12] (Simulation of Urban MObility), were considered. The simulation parameters used in these simulations are summed up in Table I . For each attack, three scenarios are investigated:

1) Low-density scenario where only 44 vehicles are travelling on the highway
2) Medium density with 128 vehicles
3) High-density scenario with 256 vehicles in the network.

TABLE I: SIMULATION PARAMETERS

| | |
|---|---|
| Highway length | 2km |
| Vehicle speed | 120 km |
| Transmission range | 300 m |
| Slots/frame | 100 |
| Slots duration | 0.001 s |
| Simulation time | 120 s |
| Vehicles Density | 44, 128, 256 |
| Ratio of malicious nodes | 1%, 10% ..., 30% of nodes |

To evaluate the performance of the DTMAC protocol in the attack scenarios, we used the following metrics: *(i)* Average access ratio *(ii)* Access ratio and *(iii)* Access collision.

The evaluation metrics are defined as follows:

- Average access ratio: is computed as the average number of slots occupied per frame during the total number of frames.
- Access ratio: is the ratio of vehicles that managed to reserve time slots per frame.
- Access collision : is defined as the number of access collisions per frame.

### B. Neighbors reservations cancellation Impact Analysis

In the simulations, we compared the performance of the DTMAC protocol with and without a greedy behavior attack in the low, medium and high density scenarios. We computed its access ratio by evaluating the effect of:

- Scenario 1: Fixing one attacker and increasing the ratio of victim vehicles.
- Scenario 2: Increasing the number of attackers in the network.

*1) Scenario 1: One greedy attacker in the network:* We initially evaluate the impact of the attack in terms of the average access ratio. We first assess the impact of having one greedy attacker in the network. As shown in Figures 4, 5 and 6, an attacker randomly chooses a percentage (either 10%, 30% or 100%) of its neighbors to cancel their reservations. DTMAC in its unaltered state, i.e. without attacks, has a very high average access ratio that is always close to the ideal rate, i.e. 100%. Regardless of network density, attack-free DTMAC achieves the highest average access ratio for any given simulation time. However, the average access ratio is very sensitive to greedy behavior attacks, and a very significant decrease in the percentage of successfully reserved slots is observed, especially as the number of victim nodes in the network increases. As an illustration, in the low density

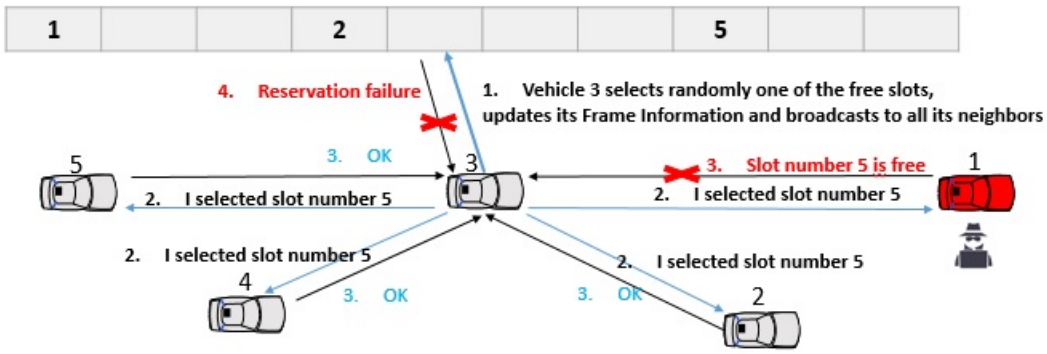
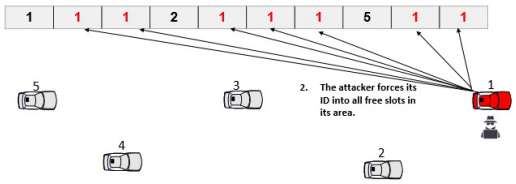
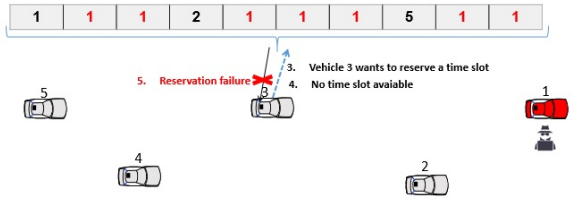



Fig. 2: Illustration of neighbor reservation cancellation attack




(a) The attacker forces its ID into all free slots in its area




(b) Reservation failure

Fig. 3: Illustration of multi access attack

scenario, when 10% of the neighbors, randomly selected from the set of the attacker neighbors, are the victims of an attacker with greedy behavior, the average access rate is reduced to approximately 90%. Furthermore, we observe almost the same impact of the greedy behavior attack on the access ratio when the density of vehicles increases. Their average access ratio is in the order of 90%. When the number of victim nodes of a greedy attacker is increased to 30% of its neighbors, the average access ratio reaches 45%. This is clearly seen in the medium and especially the high density scenario, as the number of nodes is greater than the number of slots per frame. The average access ratio drops to about 80% in medium and high densities, if the greedy attacker cancels the reservations of all its neighbors. In the low density case, the average access ratio falls to almost 65%. This drop in the low density scenario is due to the fact that only 44 nodes are active in the network and consequently the attacker's neighbors represent a significant number of them. This can be explained by the fact that the cancellation of the neighbors' reservation will lead the victim nodes to retry the reservation in subsequent frames, which in turn will increase the access collision rate and decrease the number of successfully reserved slots and consequently lower the overall access ratio in the network.

*2) Scenario 2: Multiple greedy attackers in the network:* We also evaluated the impact of cancelling neighbours' reservations on DTMAC's average access ratio while increasing the number of attackers in the network. To achieve a more

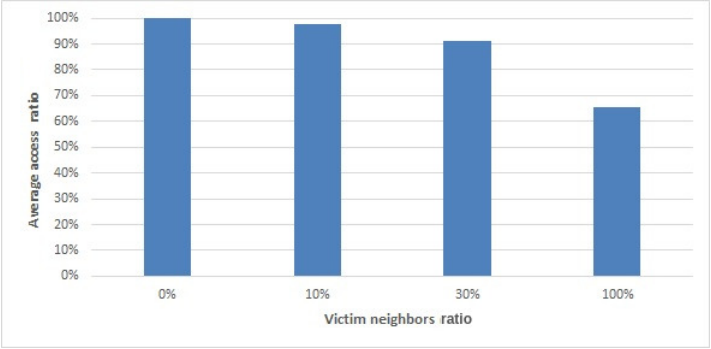



Fig. 4: Scenario 1: Average access ratio vs victim neighbors for low density scenario

accurate impact, we chose attackers belonging to different areas. Figures 7, 8 and 9 illustrate the impact of injecting more than one greedy attacker into the network for the three densities. For instance, in the low density scenario, when two attackers are present in the network, the resulting average access ratio is 50% of the average access ratio when DTMAC is not under attack. If the number of attackers reaches three, the average access ratio drops to almost 10%. The more the number of attackers increases, the more the network is paralyzed and no vehicle is able to reserve a slot. The same impact is observed in the medium density scenario, with more than three attackers where the reservations in the network do

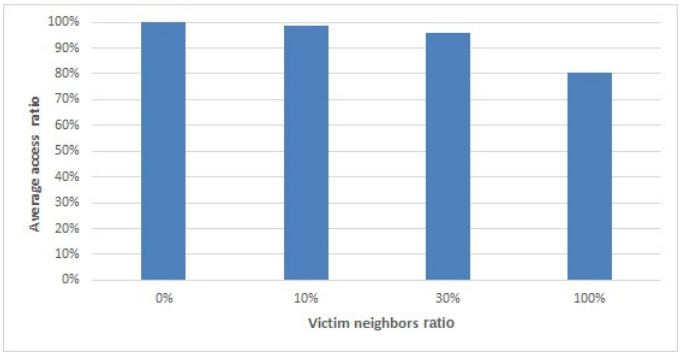



Fig. 5: Scenario 1: Average access ratio vs victim neighbors for medium density scenario

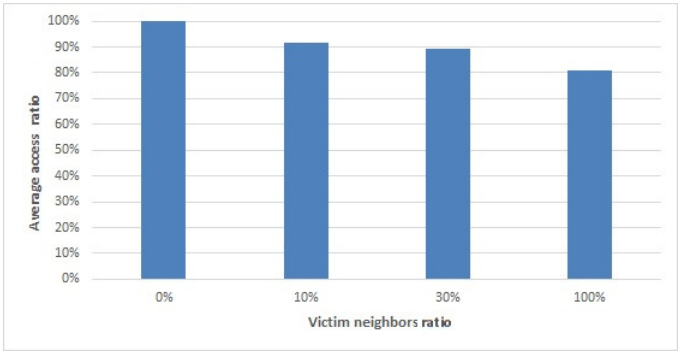



Fig. 6: Scenario 1: Average access ratio vs victim neighbors for high density scenario

not exceed 10% of the total reservations made in DTMAC without attackers. For the high density scenario, 70% of successful slot reservations are lost when three attackers are present in the network. Six attackers succeed in reducing the average access ratio to 20% of the total average access ratio and 80% of channel capacity is wasted. For a greater number of attackers in the network, the average access ratio is almost 0%, implying that the slot reservation process is no longer possible.

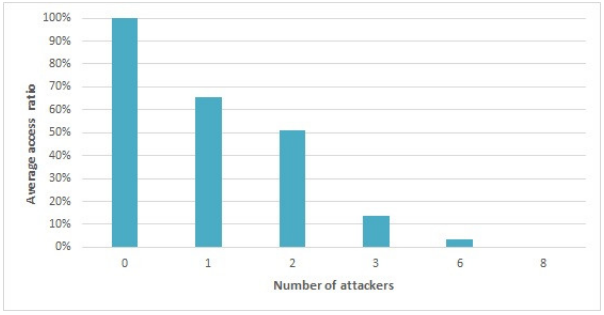



Fig. 7: Scenario 2: Average access ratio vs number of attackers for low density scenario

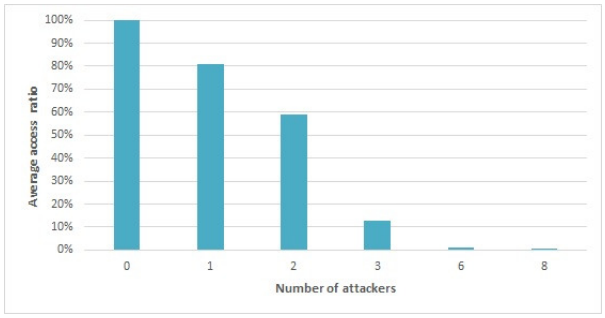



Fig. 8: Scenario 2: Average access ratio vs number of attackers for medium density scenario

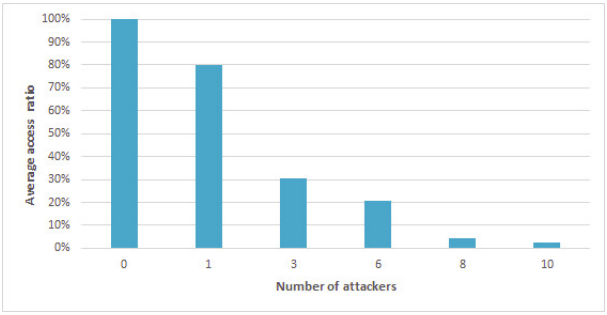



Fig. 9: Scenario 2: Average access ratio vs number of attackers for high density scenario

### C. *Multi-access attack Impact Analysis*

In this section, we analyze the performance of DTMAC under multi-access attack. In the same way as before, we evaluated the access ratio per frame. The impact of this kind of attack is made clear only if the number of active vehicles is greater than the number of available time slots. For this reason, we have discarded the low and medium scenarios and focus on the high density scenario because it shows the impact of this attack.

As explained in Section III.B, the reservation process is not disrupted if a vehicle (other than the attacker) has managed to acquire a time slot. For this reason, in order to show the impact of this attack, we consider the first frames to evaluate the effect on the access ratio. As shown in Figure 10, the number of reserved slots decreases by up to 50% during the first 20 frames. This means that half of the channel capacity is lost in the presence of a greedy vehicle that performs a multi access attack.

This attack is also evaluated in terms of access collisions as illustrated in Figure 11. The choice of this evaluation metric is due to the increase in the number of global access collisions, which is multiplied by 1.5 compared to the number of global access collisions for DTMAC without an attack. Between frame 2 and frame 10, we notice that the collision access ratio is unstable. Both cases are found, the collision access ratio in the scenario with an attack is sometimes on top and in others the scenario without an attack is in excess. From frame 11,

the impact of this attack is clear, since the scenario with an attack generates more collisions than the scenario without an attack. This implies that the attacker manages to prevent other vehicles from obtaining their reservation even though the slot times are not reserved.

To summarize, the presence of a single attacker in the network increases the overall number of access collisions by 1.5 compared to normal, implying that not all of the channel capacity is used and a significant percentage of it is lost. This increase will block a significant number of vehicles in the network from reserving a slot time, leading to a delay in reporting a potentially urgent event such as an accident. This will induce a loss of efficiency and usefulness of the network resources.

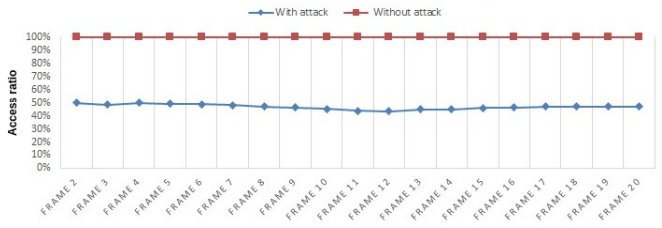



Fig. 10: Access ratio for multi access attack

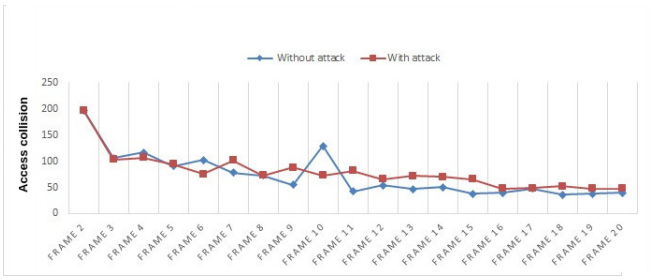



Fig. 11: Access collision for multi access attack

## V. Conclusion

VANETs are continuously evolving, bringing benefits that can improve road safety at multiple levels. However, they are very vulnerable to attacks. Therefore, it is important to study the impact of attacks on channel access in these networks. In this paper, we focus on the greedy behavior attack on the DTMAC protocol. Based on the characteristics of such an attack and the protocol itself, we identify undocumented greedy behavior that can disrupt the slot reservation process in DTMAC and then evaluate its impact by means of simulation. The slot scheduling vulnerability was exploited through two newly identified attacks: the neighbor reservation cancellation attack and the multi-access attack. The former was tested under two scenarios: the first with a single attacker in the network, while varying the percentage of affected neighbors, and the second with multiple attackers in the network. The results reveal that when the number of attacked neighbors increases, about $30\%$ of the free slots cannot be reserved, which means that a third of the channel capacity is wasted. The multiple attacker scenario shows that the network can be paralyzed and no vehicle can acquire a free slot. $8$ is the average number of attackers that would need to be present to successfully carry out this task. The multi-access attack reveals that $50\%$ of the free slots are wasted and unreserved if a greedy attacker forces its ID into all the free slots in its neighborhood. Another metric, the access collision ratio, is evaluated in this scenario, showing how the number of collisions increases in the presence of an attacker.

In future work, we will exploit the results of this investigation to develop a solution for detecting and preventing greedy behavior attacks that threaten the DTMAC protocol, focusing mainly on the new attacks identified at the MAC level.

## References


[1] Lamssaggad, Ayyoub, Nabil Benamar, Abdelhakim Senhaji Hafid, and Mounira Msahli. "A Survey on the Current Security Landscape of Intelligent Transportation Systems." IEEE Access 9 (2021): 9180-9208.

[2] Rasheed, Asim, Saira Gillani, Sana Ajmal, and Amir Qayyum. "Vehicular ad hoc network (VANET): A survey, challenges, and applications." In Vehicular Ad-Hoc Networks for Smart Cities, pp. 39-51. Springer, Singapore, 2017.

[3] Mejri, Mohamed Nidhal, and Jalel Ben-Othman. "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks." In 2014 IEEE Global Communications Conference, pp. 5032-5037. IEEE, 2014.

[4] Mejri, Mohamed Nidhal, and Jalel Ben-Othman. "GDVAN: a new greedy behavior attack detection algorithm for VANETs." IEEE Transactions on Mobile Computing 16, no. 3 (2016): 759-771.

[5] Al-Terri, Doaa, Hadi Otrok, Hassan Barada, Mahmoud Al-Qutayri, and Yousof Al Hammadi. "Cooperative based tit-for-tat strategies to retaliate against greedy behavior in VANETs." Computer Communications 104 (2017): 108-118.

[6] Baccari, Sihem, Haifa Touati, Mohamed Hadded, and Paul Muhlethaler. "Performance Impact Analysis of Security Attacks on Cross-Layer Routing Protocols in Vehicular Ad hoc Networks." In SoftCom 2020. 2020.

[7] Baccari, Sihem, Mohamed Hadded, Haifa Touati, and Paul Muhlethaler. "A secure trust-aware cross-layer routing protocol for Vehicular Ad hoc Networks." Journal of Cyber Security and Mobility (2020).

[8] Hadded, Mohamed, Paul Muhlethaler, and Anis Laouiti. "Performance evaluation of a TDMA-based multi-hop communication scheme for reliable delivery of warning messages in vehicular networks." In 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1029-1034. IEEE, 2017.

[9] Hadded, Mohamed, Anis Laouiti, Paul Muhlethaler, and Leila Azouz Saidane. "An infrastructure-free slot assignment algorithm for reliable broadcast of periodic messages in vehicular ad hoc networks." In 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), pp. 1-7. IEEE, 2016.

[10] Issariyakul, Teerawat, and Ekram Hossain. "Introduction to network simulator 2 (NS2)." In Introduction to network simulator NS2, pp. 1-18. Springer, Boston, MA, 2009.

[11] Hadded, Mohamed, Paul Muhlethaler, Anis Laouiti, and Leila Azzouz Saidane. "A novel angle-based clustering algorithm for vehicular ad hoc networks." In Vehicular Ad-Hoc Networks for Smart Cities, pp. 27-38. Springer, Singapore, 2017.

[12] Karnadi, Feliz Kristianto, Zhi Hai Mo, and Kun-chan Lan. "Rapid generation of realistic mobility models for VANET." In 2007 IEEE wireless communications and networking conference, pp. 2506-2511. IEEE, 2007.

[13] A. Rebei, M. Hadded, H. Touati, F. Boukhalfa and P. Muhlethaler, *"MAC-aware Routing Protocols for Vehicular Ad Hoc Networks: A Survey,"* 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Hvar, Croatia, 2020, pp. 1-6, doi: 10.23919/SoftCOM50211.2020.9238249.