A secure trust-aware cross-layer routing protocol for Vehicular Ad hoc Networks

Sihem Baccari, Mohamed Hadded, Haifa Touati, Paul Mühlethaler

A secure trust-aware cross-layer routing protocol for Vehicular Ad hoc Networks

Sihem Baccari[1], Mohamed Hadded[2], Haifa Touati[3], Paul Muhlethaler[4]
[1]Hatem Bettahar IResCoMath Research Unit, Tunisia,
sihembaccari51@gmail.com
[2]Institut VEDECOM, 23 bis Allee des Marronnie, 78000 Versailles, France
mohamed.elhadad@vedecom.fr
[3]Hatem Bettahar IResCoMath Research Unit, Tunisia
haifa.touati@cristal.rnu.tn
[4]INRIA Paris, 2 Rue Simone IFF, 75012 Paris, France,
paul.muhlethaler@inria.fr

Abstract

VANETs currently represent one of the most prominent solutions that aim to reduce the number of road accident victims and congestion problems while improving the quality of driving. VANETs form a very dynamic open network in which vehicles exchange information and warnings about road situations and other traffic information through several routing protocols, without any intermediate control. However, the absence of a central control makes such a network vulnerable to several types of attack, not only from the outside but also, and mostly, from the interior. This makes their detection by classical security techniques more difficult and requires the development of new techniques to control the information circulating in the network. In this context, a proposed routing protocol called TDMA-aware Routing Protocol for Multi hop communication in Vehicular networks, is vulnerable to security threats, such as Black Hole and Gray Hole attacks, as well as MAC attacks such as Denial of Service (DoS), which lead to a considerable deterioration in the network's performance in terms of packet delivery ratio, end-to-end delays, channel access rate, etc. To mitigate the effect of those attacks, we propose a trust-based model in which each node will establish a trust relationship with its neighbors based on their behaviors during the channel access and packet forwarding process. The simulation results show a significant decrease in the effect of attacks on the performance of the TRPM protocol.

VANET, Cross-layer routing, Security, Trust, Black Hole attack, Gray Hole attack, MAC attacks

1 Introduction and motivation

Road accidents are continuing to escalate in an alarming way, and claim thousands of lives each year. In an attempt to find solutions, on-going research focuses on designing efficient Intelligent Transportation Systems (ITS), the most prominent result being Vehicular Ad-hoc NETworks known as VANETs. A VANET is a kind of Mobile Ad-hoc NETwork in which each vehicle is equipped with a wireless device that allows it to communicate and exchange traffic information with other vehicles on the road in order to avoid many problems, particularly accidents and congestion problems. VANET applications are numerous and can be classified into three categories according to their QoS requirements: safety services (which require a high commitment to the QoS requirements as such services are very sensitive to time and data loss), and then the traffic management and user-oriented services which are less QoS-sensitive [2].

Since the launch of VANETs, a number of standardization efforts have been made. The current IEEE 802.11p [1] standard provides a priority-based access scheme using a contention-based channel access method [6] that by no means guarantees a successful channel access within the desired timeframe, thus making it unsuitable for the requirements of real-time applications. For this reason, researchers have directed their attention towards contention-free MAC techniques, which rely on the use of a predetermined schedule to reduce the access delay.

Time Division Multiple Access (TDMA) is one of the most favored contention-free MAC techniques that can offer equal access to the channel by dividing the time into several slots. Many TDMA-based MAC protocols have been proposed for VANETs. In addition, several TDMA-aware routing protocols have been proposed in order to optimize the selection of the next relay node. In this context, a TDMA aware Routing Protocol for Multi-hop communications called TRPM [3], [5] was designed to allow vehicles to exchange safety messages over long distances. The TRPM relay node selection is achieved by combining the distance with the waiting time between the source slot and that of the candidate node obtained from the slot scheduling information coming from a completely distributed TDMA scheduling scheme called DTMAC [4].

Although the promising benefits of VANET applications can result in greatly reducing the number of road fatalities and enhancing passenger comfort, the exchange of information in this network represents a key and a vital service, particularly for safety applications, and this makes it an ideal target for attackers aiming to disrupt the functioning of the network. Due to the specific characteristics of VANETS, notably the high mobility of nodes, surveillance of the network is more difficult. Consequently, TRPM, like any other routing protocol in a perfectly unstable environment, is always vulnerable to several types of attacks that can threaten the availability of information, such as Black Hole and Gray Hole attacks, as well as denial of access attacks.

Conventional security techniques such as authentication and signature are efficient against external attacks, but using these methods in the context of real-time security applications, not only leads to additional processing time that can impact reception delays but also does not allow internal trust between

vehicles to be maintained. Hence, trust-based models represent a complementary solution to overcome this problem by providing an efficient, fast and light control. Current solutions, however, do not cover all potential problems, as they were designed for specific contexts and security issues. Hence, it is essential to design a comprehensive security solution allowing vehicles to monitor each other's behavior, so as to be able to detect and eliminate malicious nodes. In this paper, we propose a trust-based detection mechanism against TRPM protocol misbehavior. Our mechanism focuses mainly on detecting and mitigating the effect of packet removal caused by black and gray hole attacks and new access attacks linked to the use of the DTMAC protocol.

The rest of this paper is structured as follows: in Section 2 we present some existing techniques for the detection and elimination of attacks. Section 3 summarizes the principle of the TRPM routing protocol. Section 4 describes security vulnerabilities that can affect data dissemination using the TRPM protocol. In Section 5, we detail the proposed solutions to mitigate these attacks and to build a trust-aware and robust cross-layer routing protocol. In Section 6, we present the simulation results and the performance impact analysis. Finally, the conclusion and future work are discussed in Section 7.

2 Related work

Several studies have been described in the literature in order to secure routing protocols using trust-based approaches, For instance:

Tripathi Sharma proposed in [11], a trust model allowing the detection and elimination of rogue nodes in a VANET. In this model, an observer node, with a higher trust value, evaluates the behavior of other nodes in the network. A node is considered to be trustworthy if it participates correctly in the forwarding process, otherwise it will be blacklisted by the observer node. For each new node in the network, an observer node that is geographically close and moving in the same direction is assigned in order to monitor the behavior of this node for as long a period as possible. Thus, the trust value, which is presented by a binary value to reduce network overload, can be calculated directly based on the percentage of packets deleted or modified in relation to the total number of packets received by this vehicle, or indirectly based on recommendations from neighboring nodes. After detecting a malicious node, all the vehicles will be notified so that they can update their trust information.

In [12], Shashi Gurung et al. proposed an approach called MBDP-AODV to mitigate the effect of a full packet removal attack on the AODV protocol based on a dynamic threshold value of the destination sequence number. In this work the authors firstly studied the possible behavior of nodes in the network in order to identify any potential threats, particularly a Black Hole attack. For each new communication, the source node calculates the mean for the destination sequence number, using the number of reply packets, then it calculates the

standard deviation of the destination sequence number that will be considered as the threshold value. A malicious vehicle is detected when the threshold value is greater than the average, in this case if the destination sequence number is greater than the threshold and the number of hops is equal to 1 then the source node blacklists the next hop and broadcasts an alert to notify the other nodes. When the number of hops is greater than 1, a special message containing the suspected sequence number will be sent from the source node to the next hop which will repeat the same steps until reaching the malicious node.

In [13], Biswaraj Sen et al. proposed a trust model in order to evaluate the trustworthiness of nodes in a distributed environment. In their proposal, each node is equipped with an intrusion detection module to monitor its neighboring nodes by collecting information about their behavior during the packet forwarding process. Each node updates the trust values of its neighbors based mainly on 3 factors: the belief factor, which is linked to positive events, the disbelief factor, which takes into account negative events and the uncertainty factor which is initially set at 1. An anomaly is detected when the disbelief factor exceeds a certain threshold. In order to differentiate between network congestion and a routing attack, the node calculates the PFP (Packet Forward Percentage) of the suspect node. If a node is identified as malicious, it will be excluded from the routing process.

The authors in [14], present a trust-based distribution technique for detecting and preventing Gray-hole malicious behavior in VANETs. Their method includes two modules: the first module deals with the detection of attacks based on nodes' locations and relative speed. The authors define two threshold values for the distance and the relative speed in order to distinguish between a link failure event and a node's malicious behavior. The second module is responsible for preventing malicious nodes from participating in the routing process by using a Multi-Criteria Decision Making (MCDM) method called TOPSIS in order to select the most trustworthy path.

In [15], a trust and delay aware routing in VANETs is proposed for V2V and V2I communications. In the first step, the source vehicle calculates its neighbors' degrees of confidence, based on some collected knowledge, in order to determine all the trustworthy paths. Then for each path, the source vehicle calculates its Message Reachable Time (MRT). Finally, the path with the maximum trust, i.e. having the minimum MRT, will be selected as an optimal path to forward the message.

In conclusion, despite the surge in VANET security research, the proposed methods still have a number of shortcomings and limitations, making them inappropriate for use in the context of the TRPM protocol. In short, these solutions have the following major drawbacks:

- Generally speaking, many of these solutions, like [11], [13], [14] and [15], are dedicated to a specific context and do not address all the security

issues and threats. Therefore, these methods are efficient only against a few specific malicious behaviors.

- The majority of these studies deal only with routing level attacks, however the MAC layer is no less important than the network/routing layer and it can also be threatened.

- Some research like [12] suggests solutions to prevent attacks that rely on a centralized control scheme, however the TRPM protocol is designed for completely decentralized environments where each node works separately, which makes this solution impractical.

These limitations motivated us to propose a new Trust-based misbehavior detection scheme to deal with potential cyber attacks that can threaten the TRPM protocol. Moreover, in this work we deal with a variety of attacks that can threaten both the MAC and routing layers. We evaluate some existing attacks, like Black and Gray Hole attacks and, in addition, we present and evaluate new attacks that threaten the MAC layer.

3 Background

In this section, we give an overview of the TRPM routing protocol. We firstly summarize the DTMAC slot scheduling principle, followed by a description of the TRPM forwarding algorithm. Before presenting these protocols and our security solution, we introduce the notations adopted in this paper in Table 1.

3.1 Distributed TDMA-based MAC (DTMAC) protocol

In order to reduce the risk of collisions and provide an efficient broadcast service with a bounded access delay, the Distributed based TDMA-based MAC (DTMAC) protocol was proposed, by Mohamed et al. in [4], giving rise to a new contention-free channel access technique that exploits the slot reuse concept and the vehicles' position. To achieve these goals, as illustrated in Figure 1, the road is divided into small areas numbered from x_1 to x_n of length equal to the vehicle's communication range. Furthermore, the channel time is divided into frames where each frame, in turn, is partitioned into three equal sets of time slots: S_0, S_1 and S_2 and each time slot is of a fixed duration.

To avoid collision, some additional information called Frame Information (FI) must be included in each packet transmitted by any vehicle. With a size equal to the number of time slots per frame. As shown in Figure 2, the FI is a set of ID (IDF) fields in which each IDF is mainly composed of a field called $VC-ID$ containing the MAC address of the vehicle that is using the slot, a field called $SLT-STS$ shows whether the slot is free or busy and a field called $PKT-TYP$ describes the type of packet transmitted (periodic information or an event-driven safety message).

Table 1: Notations.

Notation	Meaning
x_v	the area number v.
i	the vehicle number i.
A_i	The set of vehicles that are moving in the adjacent right-hand area.
B_i	The set of vehicles that are moving in the adjacent left-hand area.
S_k	the set of time slots number k.
$WHS_{i,j}$	the weight value of neighboring vehicle j calculated by the vehicle i.
τ	represents the total number of slots per frame.
$\Delta t_{i,j}$	represents the difference between the slot of the transmitting vehicle i and that of the candidate vehicle j.
$d_{i,j}$	represents the distance between two vehicles i and j.
R	is the vehicle's communication range.
α	is a weighted value set to 0.4
$frwd_i$	potential forwarder for the source vehicle i

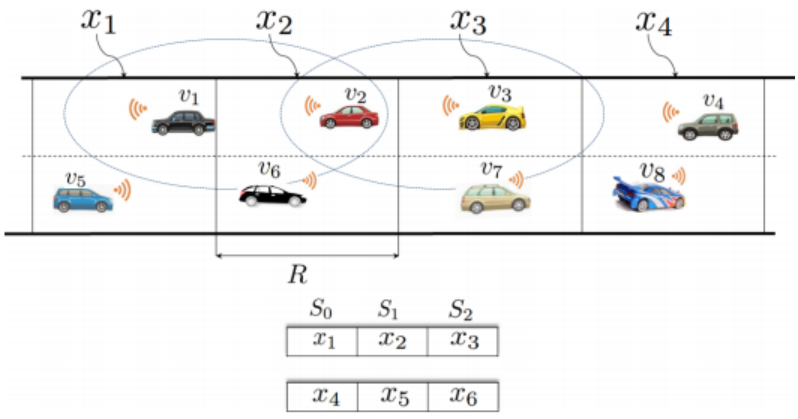

Figure 1: TDMA slots scheduling principle

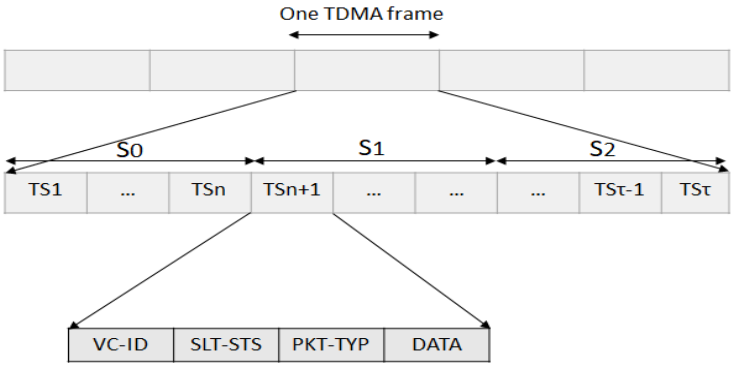

Figure 2: Frame Information (FI) structure.

Each vehicle that wishes to reserve a time slot, should listen to the channel during the set S_k of time slots reserved for zone x_v in which it is moving where $k = (v + 2) mod\ 3$. Then, it must wait until the end of the frame to determine the sets of occupied and free slots. After identifying the free time slots, the vehicle randomly selects one of them and locally updates its Frame Information to broadcast it during the chosen slot to all its neighbors. The reservation is considered successful if all the neighbors have indicated in their FIs that the slot is indeed reserved for this vehicle.

3.2 TRPM Packet forwarding algorithm

The TRPM cross-layer architecture [3] is based on a close communication between the MAC and network layers. Thus, the routing decisions are made by considering the destination vehicle's position and the scheduling information, coming from the MAC layer as a result of using the DTMAC protocol. At first, the source vehicle (say i) groups its neighbors into two sets, A_i and B_i, based on scheduling information from its Frame Information. A_i represents the set of vehicles that are moving in the adjacent right-hand area, belonging to the set of slots $S_{(k+1)} mod\ 3$ where k represents the set of time slots to which the source i belongs. Similarly, B_i represents the set of vehicles that are moving in the adjacent left-hand area, belonging to the set of slots $S_{(k+2)} mod\ 3$.

Then, depending on the destination's location, vehicle i can determine the optimal set of next hops that are geographically closest to the destination. In other words, vehicle i will select a relay node from set B_i when the destination vehicle is moving in front of it. If, on the other hand, the destination vehicle is moving behind it, set A_i is the most appropriate. In the next step, vehicle i selects among the vehicles of the chosen set 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 j is one of the neighbors of vehicle i. Finally, the candidate vehicle that minimizes the waiting time and allows long distance transmission, in other words which has the minimum WHS value, will be selected as the next hop. These steps are repeated until the destination is reached.

4 Security vulnerabilities

VANETs offer great potential to reduce road problems and protect human lives. However, the very dynamic nature of vehicular networks leads to completely unstable environments that are difficult to control. In fact, the short connections, the easy and frequent disconnection of nodes and the lack of centralized control of arrivals and departures can lead to a number of security problems and potentially dangerous situations. These specific characteristics of VANETs encourage more attackers and facilitate the spread of their malicious behavior in the network.

The distributed environment will increase the probability of attacks and make the networks less secure and open to threat. These attacks may generally take one of two forms: either by intercepting personal information and secret data passively in order to gain information about passengers' private lives or by injecting effective behavior which leads to a deviation from the normal state of the network towards a chaotic state, for example creating the illusion of an accident and a road jam in order to disrupt road traffic. Moreover, the use of the TRPM protocol in the context of VANETs, will add other security threats given that this cross-layer approach is dedicated essentially to the exchange of security messages which require a very high level of guarantee of delay and reliability and there can be little doubt that this feature will attract more attention from attackers to launch attacks that threaten data availability and integrity.

Table 2 summarizes the most serious security vulnerabilities that may affect TRPM cross-layer operations. In particular, we have identified two categories of attacks, of which network level attacks represent the most severe common threats like the problem of complete or partial loss of packets, caused by Black Hole and Gray Hole attacking nodes which remove, respectively, in a complete or selective manner the packets supposed to be transmitted during the forwarding process. We also identified the problem of delayed packet reception which represents one of the biggest challenges for real-time security applications since a simple delay can lead to very hazardous consequences, such as in the case of an accident alert delayed by a malicious node to create a malfunction on the road. Moreover, we have identified a new category of attacks that can threaten channel access. In fact, the use of the time slot scheduling information obtained from the MAC layer in the next hop selection process reveals several anomalies and security vulnerabilities, in particular the possibility of exploiting the nature of the DTMAC protocol to disrupt the reservation process and prevent vehicles from exchanging information. Several other possible violations and abuses could constitute a serious threat, such as exceeding the number of slots allowed to be reserved in the same frame, inserting fake Frame Information for malicious purposes, etc.

We start by simulating the previously mentioned attacks in order to assess the extent of the damage that they cause. Then, we propose a security solution to mitigate their effects. Details are given in Section 5.

Table 2: Summary of major security threats

	Layer	Attack on	Active Passive	Attack description
Black Hole	Routing	Availability	Active	A malicious node drops all packets passed through it and that are supposed to be redirected.
Gray Hole	Routing	Availability	Active	Based on a selection function, a node partially drops packets supposed to be transmitted.
Packet transfer Delay	Routing	Availability	Active	The addition of an artificial period of time to postpone the transfer of the packet which generates a reception a delay.
Channel access deny	MAC	Availability Integrity	Active	An attacker node can prevent other vehicles from accessing the channel by falsifying its FI.
Identify spoofing	MAC	Authentication	Active	A vehicle creates a fake identity to use it then maliciously in the frame information.
Slot reservation attack	MAC	Authentication	Active	A selfish node violates the DTMAC protocol rules by requesting several slots during the same frame.
Frame information poisoning	MAC	Integrity	Active	Since FI is exchanged in the clear, a malicious node can falsify its content to adapt it according to its malicious goals.
Slot greedy attack	MAC	Authentication	Active	A malicious node seizes the slot of another vehicle to send its data.

5 The proposed Trust-aware cross-layer routing protocol

Achieving efficient secure communication remains one of the most important challenges in vehicular networks. Despite the progress that has been made in developing solutions and research in this domain, attackers continue to develop their attack methods and exploit any loophole that enables them to achieve their goals. Hence, it is essential to continue to study the nature and impact of possible attacks in order to ensure and maintain security in VANETs. The current IEEE 802.11p standard provides an asymmetric Public Key Infrastructure using an Elliptic Curve Digital Signature (PKI/ECDSA) as a default security mechanism [1]. However, PKI and signatures are not sufficient to ensure security in VANETs because sometimes even authenticated vehicles can provoke malicious behavior. Therefore, a trust-based solution is required to detect misbehaving or malicious vehicles (e.g. vehicles that do not forward the messages or vehicles that disturb/damage the channel access process), even if they initially begin as legitimate nodes.

In the following section we introduce a new solution, called Trust-based TRPM, to detect and eliminate routing and access attacks in the routing process. The overall architecture of the proposed solution and the description of its different blocks and mechanisms, are detailed in the following sub-sections.

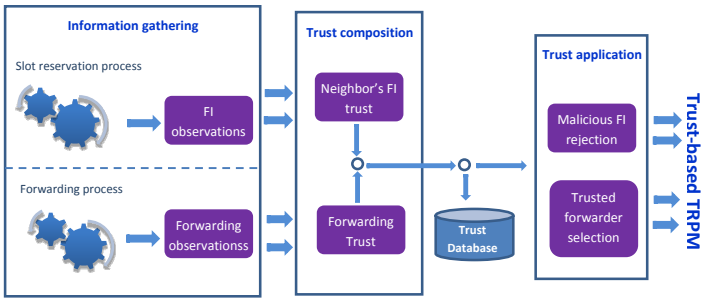

Figure 3: General Architecture of the proposed Trust-aware cross-layer routing protocol

5.1 General architecture of the proposed Trust-based TRPM

The trust architecture that we propose to secure TRPM and its components is described in Figure 3. The trust model is mainly composed of three modules: Information gathering, Trust composition and Trust application.

Our trust architecture is based on direct observation in which the trust related information received directly from one-hop neighbors is collected in the information gathering module. The trust related information is collected regarding the vehicles' behavior at the MAC and routing layers. Thus, the trust computation is calculated in the two following cases:

- Channel access mode: is the case where FI is exchanged between vehicles within one-hop to schedule the channel access.
- Routing mode: Where the vehicle acts as a relay node to forward packets on behalf of other vehicles until the packet is received by the destination node.

Each vehicle analyzes the exchanged data in order to check whether the security requirements are respected or not. These results will be used by the Trust composition module to provide periodically a set of trust levels that will be used by the Trust application module to make a decision. The trust metric calculated at each layer has a certain threshold, and when it is exceeded, the vehicle concerned is considered to be malicious.

5.2 Information Gathering

To enhance security in the network and avoid packet removal caused by routing and channel access attackers, we propose that each node continuously analyses the behavior of its neighbors.

During the forwarding process, each vehicle takes into account the number of positive and negative events. In other words, it monitors the number of packets received and correctly forwarded without modification, and the number of negative events is calculated by considering the number of packets dropped by each node. Thus, as shown in Figure 4, each vehicle conserves the collected data and locally controls its neighbors by updating these values at each transmission.

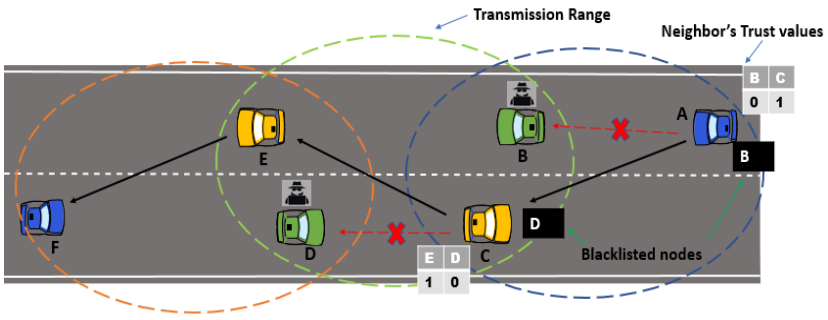

Figure 4: Black and Gray hole attack detection principle

During the slot reservation process, each vehicle observes the behaviors of its neighbors by analyzing the FI that is exchanged within its communication

range. As mentioned above, each vehicle that wishes to acquire a slot time must wait for a reservation confirmation from each of its neighbors. Figure 5 depicts a scenario where vehicle A is legitimately trying to access the channel and vehicle B is malicious and trying to deny access by broadcasting fake FI indicating that the slot is not reserved for vehicle A. This MAC layer misbehavior can be considered as a denial of service (DoS) attack, through modifications in the frame information. To deal with this problem, we propose a behavior control mechanism based on the marking of nodes. In our model, each node locally controls the behaviors of its neighbors at the MAC layer by checking the FI that they broadcast

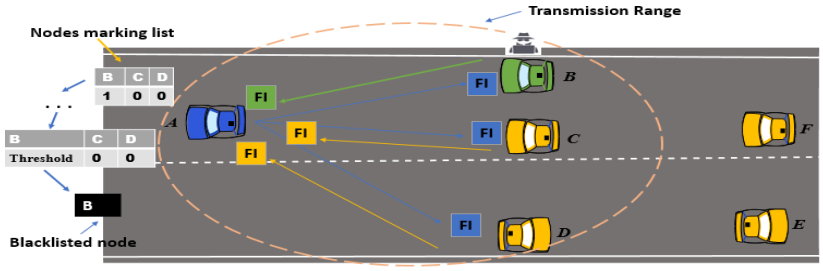

Figure 5: MAC attack detection principle

5.3 Trust composition

This module is in charge of measuring the trust level for each neighbor, especially the Neighbor's FI Trust (NFT) and the Forwarding Trust (FT). To compose the Forwarding Trust value, all the vehicles start with an initial trust value and then with each new transmission the source vehicle updates these values by checking, for each forwarder vehicle, whether it has correctly transferred the packet or not. Thus, if a forwarder node has a number of negative events that is always greater than the positive events, then an anomaly is detected. More clearly, to detect malicious nodes at the routing layer, the sender node uses the FT value, which is calculated as follows:

$$FT_{node} = \frac{\sum Forwarded - packets_{node}}{\sum Received - packets_{node}} \quad (1)$$

Using the FT value, each node classifies its neighbors into two types: malicious nodes and trustworthy nodes, based on a pre-defined threshold value. We set different thresholds to differentiate between Black Hole and Gray Hole attackers. The overall routing attack mitigation process is summarized in Algorithm 1.

To compose the Neighbor's FI Trust level, each vehicle locally controls its neighbors by checking their exchanged FIs. If one of the neighbors, say B, broadcasts fake FI , the requesting vehicle, A, will decrease B's NFT level and will mark it as suspect. For each new request, the source vehicle A, updates its

marking list. As long as the NFT value remains greater than a threshold value, node B is still considered trustworthy. However, when the threshold value is reached, the neighboring vehicle B will be considered as a DoS attacker.

5.4 Trust database

In Trust-TRPM, each vehicle maintains a Trust database for all the vehicles within its communication range. The trust database contains a Trust Value Table (TVT) and a Malicious Vehicles Table (MVT). Each vehicle can identify and isolate malicious vehicles among all its neighboring nodes based on the MVT information, which can protect the radio channel from any potential damage caused by malicious vehicles. A vehicle declares its neighbor as being a malicious node if the corresponding trust value falls below a trust threshold. As mentioned in the algorithm above , all vehicles having a Trust value below the threshold must demonstrate a good behavior to increase their Trust values.

5.5 Trust application

As shown in the algorithm below, which describes the overall forwarding process scheme in our solution, once a vehicle has been detected as a malicious forwarder, by exceeding a given threshold, it will be eliminated from the forwarding process. Thus, the sender node selects, from the sets A_i or B_i, only the nodes that can be considered as trustworthy due to their high Trust value, i.e. their FT is always below the threshold value. Similarly, if a node is considered as a channel access attacker, then it will be blacklisted and isolated from the reservation process. Its FIs will be considered as bogus messages and will be ignored. Finally, isolating the malicious vehicles in Trust-based TRPM is accomplished by considering only the slot reservation requests of vehicles that have Trust values greater than the trust threshold.

6 Simulation results

6.1 Simulation setup

To evaluate the performance of our proposed mechanism, we firstly developed and simulated several attack models by injecting malicious behavior for a varying number of vehicles in order to show the effect of such attacks, in the absence of control, on the performance of TRPM. Then, we simulated our solution in the presence of several attacker nodes. Three types of attacks are implemented and evaluated in this study:

i Black Hole attacks in which malicious nodes remove each packet received.

ii Gray Hole attacks in which the removal of packets is linked to a random selection function.

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

Algorithm 1: The overall trust-based forwarding process

Result: Lists of trustworthy and blacklisted forwarders
initialization;
/* Trust Application: Prevention of malicious nodes */
if dst.zone-number < src.zone-number **then**
  $frwd_i = \{j \in A_i | (WHS_i, j = min(WHS_i, l \forall l \in A_i) and (Is\_in\_BlackList(j) == False))\}$;
else
  $frwd_i = \{j \in B_i | (WHS_i, j = min(WHS_i, l \forall l \in B_i) and (Is\_in\_BlackList(j) == False))\}$
if $frwd_i \geq 0$ **then**
  $send\_msg(msg.src, msg.dst, msg.frwdi)$;
  /* Information Gathering*/
  if $frwd_i$ has received the msg **then**
    received_packet$[frwd_i]$++;
  if $frwd_i$ has correctly forwarded the msg **then**
    forwarded_packet$[frwd_i]$++;
  /* Trust Composition: Forwarding Trust calculation according to eq. 1 */
  Update_FT_value($frwd_i$);
  /* Trust Application: Detection of malicious node*/
  if $FT \leq$ threshold **then**
    Add_in_Black_List($frwd_i$);
  else
    if $frwd_i \in Black\_List$ **then**
      Remove_from_Black_List($frwd_i$);
else
  queue_message(msg);
  go_to 1 ;

For the simulation, we used realistic VANET scenarios generated by exporting from OpenStreetMap (OSM) a metropolitan area of a map of San Jose (California) 3000m x 100m in size and then edited it using Java OpenStreetMap Editor (JOSM). The vehicular traffic scenarios and the simulation of the area with road traffic were produced by MOVE and SUMO [9]. The parameters of each vehicle flow include the maximum number of vehicles, the starting route and destination of the flow, the start and end time of the flow and a random speed for each vehicle of between 120 km/h and 150 km/h. Then, the generated traces were used in the ns2.35 simulator [8]. Furthermore, 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 3.

Table 3: 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
Ratio of malicious nodes	1%, 10% ..., 30% of nodes

For the datasets used to evaluate our solution, we kept the same data used in [4] by varying the density of vehicles in the network. In the proposed trust based solution, all the vehicles start at the initialization step of the network with an initial trust value equal to 0. We assigned this value in the assumption that all the vehicles initially are unknown vehicles and only at the channel access phase and through data exchange will it be discovered whether they are trustworthy or not. In this study, we injected the MAC and routing attack models studied above into the network and we varied the percentage of malicious nodes from 0% to 30%.

For each simulation, two scenarios, with different densities, were studied by varying the number of vehicles moving on the highway from 43 to 128. To evaluate the performance of the TRPM protocol, we used the following metrics: The Packet Delivery Ratio (PDR) and the channel access rate. The evaluation metrics are defined as follows:

- 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.
- Channel access rate refers to the rate of vehicles successfully accessing the channel.

For each metric and for each scenario, we ran 10 simulations with different distributions of malicious nodes. We calculated the average result with a confidence interval of 95%.

6.2 Performance analysis of Trust-based TRPM in the face of Black and Gray Hole attacks

In this section, we evaluate the performance of our solution for the mitigation of the effect of Black and Gray Hole attacks in terms of PDR (Packet Delivery Ratio). For this purpose, we compared the results of the proposed Trust-based TRPM with those of the original TRPM under the effect of routing attacks, by varying the number of attackers in the network from 1% to 30% of the total number of nodes.

We start with the evaluation of our mechanism against the Black Hole attack. The results, given in Figures 6 and 8, show a very remarkable deterioration in the performance of the TRPM routing protocol caused by the effect of the Black Hole attackers. For instance, in the case of a network composed of 43 vehicles where 30% of the nodes are malicious, the PDR of the TRPM protocol decreases severely to only 13%. The effect of such an attack is even remarkable in the case of a density equal to 128: when 20% of the nodes are working as malicious, TRPM achieves only 47% of PDR. On the other hand, the TRPM protocol, in a normal state without attacks, achieves very high performance in terms of PDR: close overall to 100%, according to [3]. In fact, the absence of monitoring in a fully distributed environment further facilitates the propagation of this type of malicious behavior in the network.

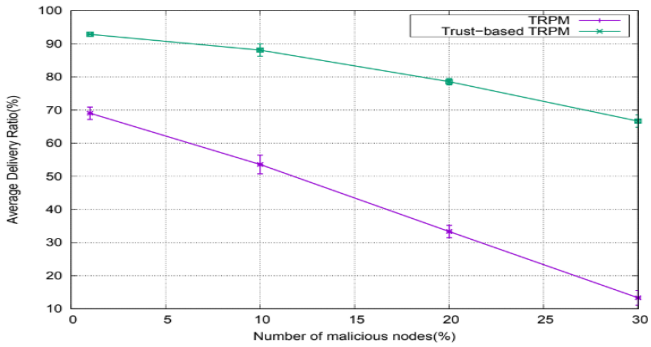

Figure 6: Black Hole attacks:Average delivery ratio vs Number of malicious nodes in the case of 43 vehicles

By comparing these results with the performance of the proposed Trust-based TRPM , we can clearly notice the improvement in the PDR. Thus, our solution significantly reduces the rate of lost packets. For instance, a PDR optimization of over 50% is achieved in the case of low density when 30% of the nodes are attackers. Moreover, the PDR rate exceeds 74% in the case of 128 vehicles when

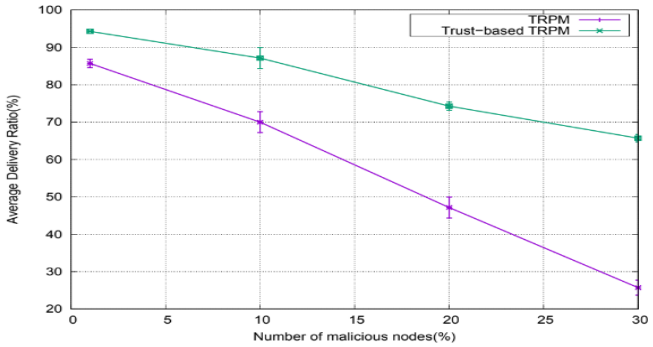

Figure 7: Black Hole attacks:Average delivery ratio vs Number of malicious nodes in the case of 128 vehicles

20% of nodes are malicious. When the number of attackers in the network is low, Trust-based TRPM achieves high rates of the PDR, citing as an example, that the PDR value reaches 94% in the case of 128 vehicles with 1% of attackers.

We also compared the performance of Trust-based TRPM with that of the original TRPM in the presence of Gray Hole attackers. As for the case of the Black Hole attack, the packet delivery rate is considerably affected by this attack. Thus, we can notice, in Figures 8 and 9, the decrease in the performance of TRPM although it is less severe than in the case of Black Hole attacks since the deletion of the packets under a Gray Hole attack is linked to a random selection function. For example, the delivery rate does not exceed 46% in the case of low density with 30% of the nodes as attackers. Even for the case of 128 vehicles, the PDR does not exceed 57%.

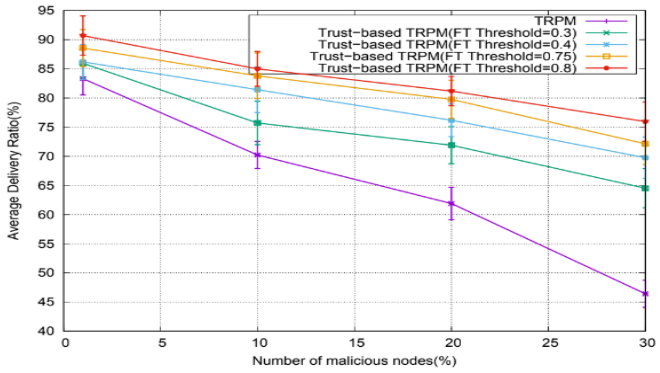

Figure 8: Gray Hole attacks:Average delivery ratio vs Number of malicious nodes in the case of 43 vehicles

Unlike a Black Hole attacker, the behavior of a Gray Hole attacker is com-

pletely unstable. This makes its detection more difficult as it can participate correctly in the forwarding process for an unbounded duration and then it can suddenly switch to being malicious and start to disrupt the network. To remedy this problem, we run the simulations with several FT threshold values in order to determine the most suitable threshold value.

In Figures 8 and 9, we see a clear improvement with the first threshold value and by further increasing this value, the performance of the Trust-based TRPM, in terms of PDR, begins to increase considerably compared to that of TRPM. For example, in the case of low density with 30% of nodes operating as attackers, using a threshold value set to 0.75, improves the PDR to 72% against a value that does not exceed 46% for the original TRPM. Moreover, with 128 vehicles, our proposed mechanism allows the Trust-based TRPM to deliver considerably improved values compared to the original TRPM. For instance, using a threshold value =0.8, Trust-based TRPM achieves a PDR value of 85% when 20% of nodes are behaving maliciously.

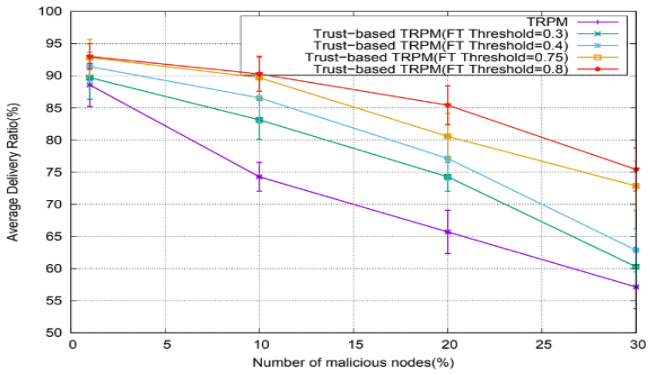

Figure 9: Gray Hole attacks:Average delivery ratio vs Number of malicious nodes in the case of 128 vehicles

6.3 Performance analysis of Trust-based TRPM under MAC attacks

In this section, we evaluate the performance of our solution against denial of access attacks. To clearly show the effectiveness of our mechanism, we compare the access rate in the case without attacks, with attacks in the presence of our solution. In the first scenario, for 30 frames we simulated an attacking vehicle that is attempting to disrupt the reservation of all its neighbors. Then, we simulated the same scenario in the presence of the node behavior control provided by our proposed technique.

As shown in Figures 10 and 11, we clearly see a deterioration in the rate of vehicles successfully accessing the channel. In fact, the nature of the DTMAC protocol and its reservation method makes launching and propagating attacks

very fast and difficult to detect. We can already clearly observe, whatever the vehicle density, that more than 50% of the access rate of the DTMAC protocol has been lost compared to that in the case without attack, which presents constant high performance with a very low collision rate close generally to 0% as an advantage of using this contention-free technique [4]. Moreover, the impact of this attack not only prevents vehicles from gaining slots, but also leads to a waste of the overall capacity of the channel since the attacked slots cannot be reserved, even if they are free.

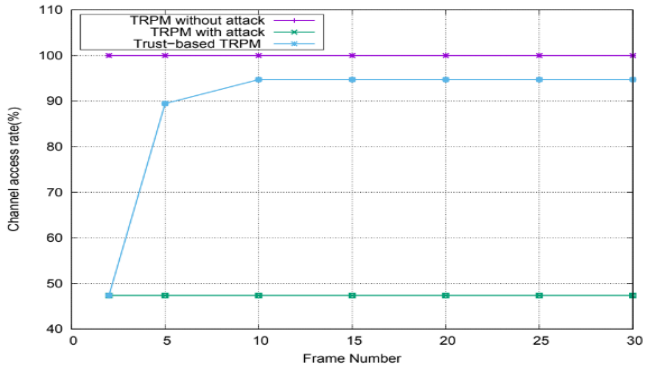

Figure 10: Channel access rate vs frame number in the case of 43 vehicles

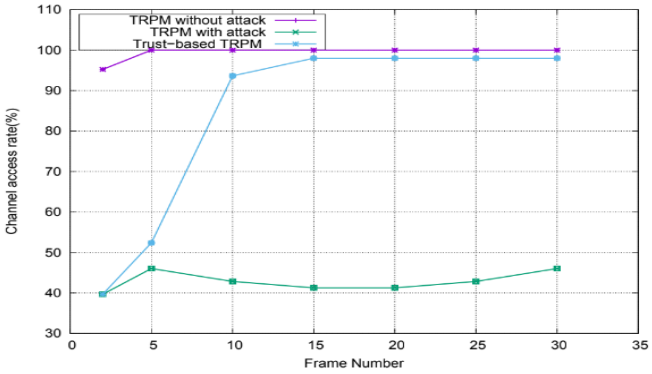

Figure 11: Channel access rate vs frame number in the case of 128 vehicles

On the other hand, the use of our proposed behavior control mechanism led to a very significant reduction in the severity of this attack and a return to a stable channel access with a small decrease, which is explained by the fact that once the attacker has been detected, it will be prevented from accessing the channel, even if it has a slot. As soon as the nodes begin detecting and eliminating the malicious node, the overall access rate to the channel will be

positively influenced and fewer and fewer vehicles will be affected. For instance, in the case of low density our proposed solution provided a performance very comparable to that of the normal state without any attack, where the access rate was optimized by more than 43% starting from frame 5. By increasing the vehicle density towards 128, Trust-based TRPM shows an improvement in performance of more than 51% starting from frame 10. To sum up, our proposed mechanism clearly reduces the effect of the access attack and prevents attackers from having a detrimental effect on network performance

7 Conclusion

VANET technology is a very promising solution to maintain road safety while providing greater comfort for passengers, and its effective deployment requires studying all the associated pressures and constraints, particularly the security of shared information, which plays a fundamental role in such networks.

In this paper, we have proposed a trust model for securing VANETs against Black-hole, Gray-hole and MAC attacks within the TRPM cross-layer routing protocol. The proposed solution, called Trust-based TRPM, has proven to have considerable capacity in detecting and eliminating malicious nodes that attempt to disrupt normal network operation. Moreover, Trust-based TRPM is a very fast technique which does not require much computing time as each node is responsible for its safety, thereby avoiding the need to load the network. Simulation results illustrate the effectiveness of the proposed trust-based approach to detect and isolate misbehaving nodes. In summary, we have demonstrated that our solution improves the PDR and channel access rate when different ratios of malicious nodes are present in the network.

Our present solution is intended for detecting some sets of malicious behavior. In future work we aim to improve and expand our mechanism to include other types of attacks and malicious activities. In particular we will focus on the detection of packet transfer delay attacks, which threaten the reception delays and represent one of the major constraints for real-time security applications.

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*, 17(4): 2461-2492, 2015.

[3] M. Hadded, A. Laouiti, P. Muhlethaler, and L. A. Saidan. TDMA aware Routing Protocol for Multi-hop Communications in Vehicular Ad Hoc Networks. *IEEE Wireless Communications and Networking Conference (WCNC)*, 1-6, San Francisco, USA, 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. *IEEE 84th Vehicular Technology Conference (VTC-Fall)*, 1-7, Montreal, Canada, 2016.

[5] 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. *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 1029-1034, 2017.

[6] R. Uzcategui and G. Acosta-Marum. Wave: A tutorial. *IEEE Communications Magazine*, 47(5):126–133, May 2009.

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

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

[9] F. Karnadi, Z. Mo, and K. chan Lan. Rapid generation of realistic mobility models for VANET. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2506-2511, Hong Kong, China, 2007.

[10] S. Ucar, S. C. Ergen and O. Ozkasap. Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination. *IEEE Transactions on Vehicular Technology*, 65(4):2621-2636, 2016.

[11] K.N. Tripathi and S.C. Sharma. A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS). *International Journal of System Assurance Engineering and Management*, 11(2):426–440, 2020. .

[12] S. Gurung and S. Chauhan. A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wireless Networks24*, 2957–2971, 2017

[13] B. Sen, M. G. Meitei, K. Sharma, M. K. Ghose, and S. Sinha. Mitigating black hole attacks in MANETs using a trust-based threshold mechanism. *International Journal of Applied Engineering Research*, 13(7):5458-5463, 2018

[14] A. K. Ahmed, M. N. Abdulwahed and B. Farzaneh. A distributed trust mechanism for malicious behaviors in VANETs. *Indonesian Journal of Electrical Engineering and Computer Science*, 19(3):1147-1155, 2020.

[15] M. J. Sataraddi and M. S. Kakkasageri. Trust and Delay based Routing for VANETs. *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 1-6, GOA, India, 2019.