Security Improvements for Connected Vehicles Position-Based Routing

Andrey Silva[1], Lucas Silva[1], Aurenice Oliveira[2] and Aldebaro Klautau[1]

[1]Institute of Technology, Federal University of Pará, Belém, Pará, 66075-110, Brazil
[2]Department of Electrical and Computer Engineering, Michigan Technological University,
Houghton, MI 49931-1295, USA

Abstract: The constant growing on the number of vehicles is increasing the complexity of traffic in urban and highway environments. It is paramount to improve traffic management to guarantee better road usage and people's safety. Through efficient communications, Vehicular Ad hoc Networks (VANETs) can provide enough information for traffic safety initiatives, daily traffic data processing, and entertainment information. However, VANETs are vulnerable to malicious nodes applying different types of network attacks, where an attacker can, for instance, forge its position to receive the data packet and drop the message. This can lead vehicles and authorities to make incorrect assumptions and decisions, which can result in dangerous situations. Therefore, any data dissemination protocol designed for VANET should consider security issues when selecting the next-hop forwarding node. In this paper, we propose a security scheme designed for position-based routing algorithms, which analyzes nodes position, transmission range, and hello packet interval. The scheme deals with malicious nodes performing network attacks, faking their positions forcing packets to be dropped. We used the Simulation of Urban MObility (SUMO) and Network Simulator-version 3 (NS-3) to compare our proposed scheme integrated with two well-known position-based algorithms. The results were collected in an urban Manhattan grid environment varying the number of nodes, the number of malicious nodes, as well as the number of source-destination pairs. The results show that the proposed security scheme can successfully improve the packet delivery ratio while maintaining low average end-to-end delay of the algorithms.

Keywords: Security, GPSR, routing, VANETs, SUMO, NS-3.

1. Introduction

Vehicular Ad Hoc Network (VANET) is an emerging network technology that provides communication for vehicles to have Internet connectivity, and to access safety as well as entertainment applications. VANET is a particular case of Mobile Ad Hoc Network (MANET) and is a key component of intelligent transportation systems (ITS). The development of ITS systems has accelerated the advancement of new technologies to improve road safety enhancement, and traffic management efficiency [1].

In VANET, vehicles are equipped with various sensors to obtain information regarding traffic, road conditions, neighbor's vehicles status (speed, brake, etc.), and positioning through global positioning system (GPS) receivers. This information can be wirelessly broadcasted to neighboring vehicles to prevent congestion and imminent accidents [2]. Vehicles can use different types of applications through vehicle-to-everything (V2X) communications. The term V2X includes all types of communications from a vehicle to any entity, for instance, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [3].

The data collected via V2X communications is useful to provide real time information services related to road safety such as collision warning, road congestion, traffic light status, and sudden braking or lane changing of nearby vehicles [4]. The information exchanged among vehicles through V2X communications is performed either with dedicated short-range communication (DSRC) standard (IEEE 802.11p) or cellular vehicle-to-everything (C-V2X) wireless communication [5]. A typical VANET architecture is shown in Fig. 1. The system is composed of a roadside unit (RSU), an LTE-based infrastructure, vehicles equipped with on board unit (OBU) enabling vehicle-to-UAV (V2U) and vehicle-to-pedestrian (V2P) communications, as well as Internet access.

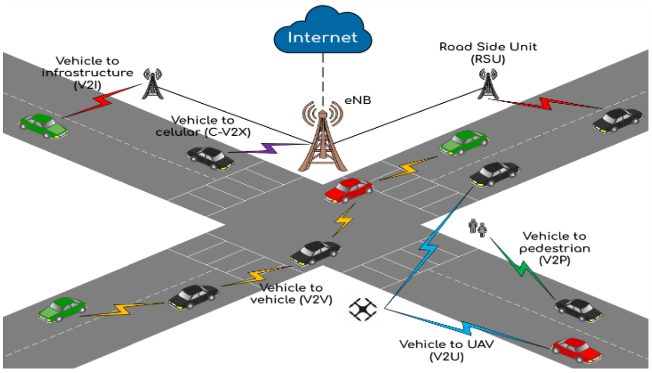
Internet
Vehicle to infrastructure (V2I)
Road Side Unit (RSU)
eNB
Vehicle to celular (C-V2X)
Vehicle to pedestrian (V2P)
Vehicle to vehicle (V2V)
Vehicle to UAV (V2U)

Figure 1. VANET typical structure.

Cyber security plays a significant role in VANETs since a successful network attack by a malicious vehicle can produce serious consequences such as car accidents or traffic congestion. Due to the large number of vehicles and the rapid changes in the network topology, it is extremely important to ensure that the messages transmitted among vehicles will be efficiently delivered [6]. Such concern is because VANETs operate on a wireless network, which allows cyber security attacks from any node located in any direction [7]. Thus, designing efficient security schemes to deal with the network security and privacy issues as well as improving the network against malicious nodes is a challenging task. These challenges (network security issues in general, not only for position-based algorithms) propelled researchers to try diverse strategies to minimize (or eliminate) the effects of these attacks.

Sathish et al. [8] presented a strategy to reduce the impact of the black hole attacks. In their scheme, a fake RREQ (Route Request) packet is broadcasted with a non-existing destination address. Any node that responds to this RREQ is inserted into a list of black holes. In the proposed solution, a cooperative black hole is a node that has a next-hop node listed as a black hole.

Dong et al. [9] proposed DoS attack detection over Software Defined Network (SDN). It uses data sets for flow assessment purposes as well as detecting the attacker based on traces. A sequential probability test is also used to measure the frequency of the *False/True* error rate. The results show performance in terms of accuracy as well as the ability to detect threats across multiple flows.

Bruno et al. [10] proposed the use of an anonymous authentication and Sybil attack detecting protocol for the VANETs called ASAP-V (Authentication and Sybil Attack detection Protocol for VANETs). Their simulation results indicated that the ASAP-V is quite robust against Sybil attacks, having a detection time shorter than the average compared to state of the art. The authentication procedure in the protocol depends on providing position privacy for users, through a multiple pseudonym system, while the Group Signature System is used for the non-repudiation process. Also, the proposed protocol used the anonymity set theory to provide privacy to users and to detect and prevent Sybil attacks.

In Singh et al. [11], the authors proposed the use of the machine learning techniques Support Vector Machines (SVM) and Logistic Regression in the VeReMi database to analyze secure messages and detect false position information that is transmitted by malicious nodes. In Ali et al. [12] an Intrusion Detection System (IDS) using Support Vector Machines (SVM) and Feed Forward Neural Networks (FFNN) is proposed to detect rushing and greyhole attacks.

In Waraich et al. [13], an algorithm is proposed to prevent DoS attack based on the use of a Quick Response Table (QRT). In the proposed method, when a packet is dropped on a route, its drop count is incremented and, after reaching a limit value, the path is isolated from the network. Thus, using QRT, routes and nodes that are considered suspicious are ignored for routing.

Lachdhaf et al. [14] proposed a strategy to detect and prevent isolated and cooperative black hole attacks using the AODV routing protocol. In the presented method, the Cyclic Redundancy Check 32 bits (CRC-32) is used to store the address of the destination in the RREQ message. When an intermediate node receives the RREQ, an RREP (Route Reply) is only sent after the destination's address is configured and verified with the address stored in the CRC-32. Thus, if the address transmitted by the RREP is not as expected, communication with that node is rejected.

Terri et al. [15] proposed two collaborative-based approaches, Cooperative Detection (CD) and Group Reputation (GR). These techniques can detect malicious nodes in the MAC layer of the VANET network. Both approaches performed better than the available methods for detecting Distributed Denial of Service (DDOS) attacks. However, for the detection of wormhole and grey hole attacks, the approaches have not achieved significant performance.

A large quantity of position-based routing protocols proposed for VANETs do not consider security issues to select the next-hop forwarding node, such as [16], [17], [18], [19]. Examples of these issues are discussed in the next section. On the other hand, the protocols taking cyber security issues into consideration use cooperative or very sophisticated methods to detect malicious activities in the network. Our proposed method uses a scheme designed for position-based routing algorithms that constantly analyzes the position, transmission range, and hello packet interval of the neighbors' nodes and checks if those information's are characteristics of a malicious node, in case positive, that node is added to a blacklist. With that, the goal is to improve the forwarding strategy algorithm to detect and avoid malicious nodes that are faking their positions to force packets to be dropped. Moreover, by checking the timestamp information of the neighbors' nodes, our proposed scheme can avoid sending data to a node that is not closer to the sender anymore.

To evaluate the performance of the proposed method, we conducted simulations considering interactive entertainment applications as the type of service of our investigation. Hence, as also observed in [20], the data does not need to be disseminated among all the vehicles in the network. Therefore, the desirable properties of the routing protocol should be unicast routing, which motivates us to use unicast routing protocol to forward the data. We chose the Geographic Perimeter Stateless Routing (GPSR) [21] as a baseline algorithm, which is a widely adopted position-based unicast routing protocol for VANETs [22]. In addition, we also used our previous work, which presented a novel routing protocol known as Path Aware GPSR (PA-GPSR) [18].

We analyzed the performance metrics such as packet delivery rate and end-to-end delay in scenarios under network attacks (position faking and black hole). The results demonstrate that our proposed scheme can significantly improve the packet delivery ratio for both algorithms with a slight increase in the end-to-end delay, which is expected. This can be explained by the fact that for UDP applications, the packet delay is just considered when packets are delivered. Thus, in our scheme, some packets are taking long routes to avoid the malicious nodes, which increases the end-to-end delay, while in the traditional algorithms (without the security feature), the packets are being captured by the malicious nodes and dropped. The main contributions of this manuscript are listed below:

- We developed a simulation-based model to evaluate the impact of network attacks under different numbers of attackers.
- We successfully proposed a new method to deal with position faking and black hole attacks in VANETs position-based routing protocols.
- The proposed algorithm can help the vehicle itself to identify attackers acting as malicious nodes without the need of nodes cooperation or any extra sophisticated method to exchange this information, such as Software Defined Network (SDN).
- There are several network attack strategies in the VANET literature. However, it is challenging to find the source code for them. Therefore, we provided our source code as open source available to help other researchers to reproduce our findings. The source code can be found at *https://github.com/CSVNetLab/VanetSecurity*.

This paper is organized as follows: In Section II, we present a brief literature review of the main malicious attacks in VANETs. In Section III, we present our cyber security method to improve the position-based routing protocols against position faking and black hole attacks. We then describe simulation settings and the performance results in Section IV. Finally, in Section V, we present additional discussions and conclusions.

2. Security Attacks in VANET

There are several types of security attacks on the network layer in VANETs, which can be characterized by interrupting communication between network nodes and modifying geographic positioning information. They are also responsible for discarding, changing information, or causing a delay in sending data packets. Moreover, these attacks can generate replicas of messages, which are distributed over the network, prompting an overhead [23]. The following describes some of the security attacks at the network layer in VANETs.

2.1. Black Hole Attack

In a black hole attack, a malicious node presents itself as the closest to the destination or the best path to be taken, thus redirecting the traffic of the packages to itself [7]. When the packets arrive at the malicious node, they are discarded or forwarded to a different node away from the destination. This process occurs without informing the source node, as shown in Fig. 2.

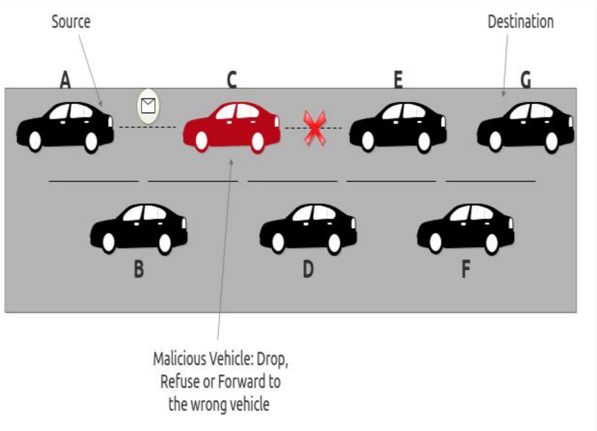
Source
Destination
A
C
E
G
B
D
F
Malicious Vehicle: Drop, Refuse or Forward to the wrong vehicle

Figure 2. Black hole attack.

This type of attack, although frequent, still presents significant challenges to be detected since the malicious node also behaves as a regular node at certain times [24].

2.2. Wormhole Attack

It is one of the variants of the black hole attack [24]. In a wormhole attack, two malicious nodes positioned in different regions of the network form a communication tunnel between them. When one of the nodes receives a packet, it will send it through the "tunnel" to the node on the other side of the network, thus the nodes end up knowing the information carried at different points, as illustrated in Fig. 3. With this knowledge it is possible to control the data traffic on the network allowing more aggressive attacks to be executed such as packet replicas, generating an overhead [25], [26]. The wormhole attack is quite complex to be detected, as it usually does not affect the normal performance of the network.

2.3. Position Faking

Position falsification is one of the most significant problems in VANETs, especially in position-based routing, since all reliable routing of data packets depends on vehicle location information stored in a table with vehicle identification and their respective geographic location [7], [24]. Despite the high degree of importance of this information, attacks of this type can be very frequent, as the malicious node can easily change the information in the table. Fig. 4 shows an example of how this attack occurs: node A needs to forward packets to node H and, according to its neighbors' table, the fastest way is to forward the packet through node B. However, node B is a malicious node that is faking its position (node b is the position where node B is faking to be) acting as it is closer to node H, where its real position is given by B, instead of b. When packets are redirected to node B (since based on its faked position node B is the closest node to the destination), it ends up dropping the packets.

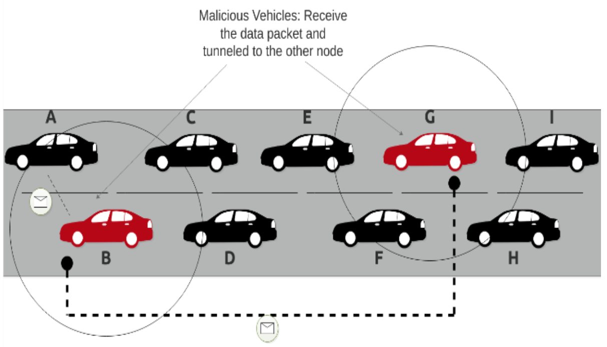
Malicious Vehicles: Receive the data packet and tunneled to the other node
A
C
E
G
I
B
D
F
H

Figure 3. Wormhole attack.

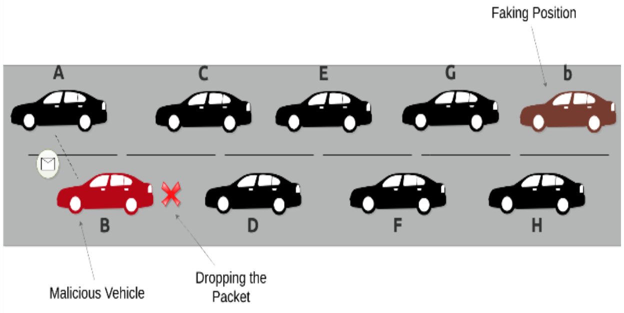

Figure 4. Position faking attack.

2.4. GPS Spoofing

Like position faking attack, GPS spoofing has been studied extensively, as it is vital to ensure the reliability of geographic positioning information [27]. In this fake GPS position attack, a malicious vehicle provides fake GPS information to other vehicles within its range different from that offered by the real GPS satellite and is obtained by a GPS simulator. The other vehicles in the range will then follow the signal provided by the simulator, since it is stronger than the signal provided by the satellite [7]. In this way, all location information within that area is controlled by the attacker, allowing a wider range of attacks to be carried out. The GPS counterfeit attack can be used most effectively in areas where there is a low reception of satellite signals, such as tunnels and urban roads surrounded by trees.

2.5. Denial of Service (DoS) Attack

The main purpose of the Denial of Service (DoS) attack is to prevent authorized nodes from using network services and resources [7]. In this type of attack, the attacker can act both inside the network and outside. In an internal attack, the malicious node can block routes after sending false communications to its neighbors or forge periodic messages to neighboring nodes, to keep them occupied in such a way that they are unable to access other network services. In an external attack, the malicious node repeatedly disseminates communications within the network, but with false identities, consuming bandwidth and preventing the use of resources by authorized nodes [28].

2.6. Sybil Attack

In this type of attack, the malicious vehicle sends several messages to its neighbors; however, each message has a different identification, thus creating the illusion that there are more vehicles than the reality, thus forcing the victim to take another route [24], [25], [29]. Fig. 5 shows an example of how this attack occurs: malicious node A sends several messages with different identifications to node D, creating the illusion of congestion and thus forcing node D to take another route.

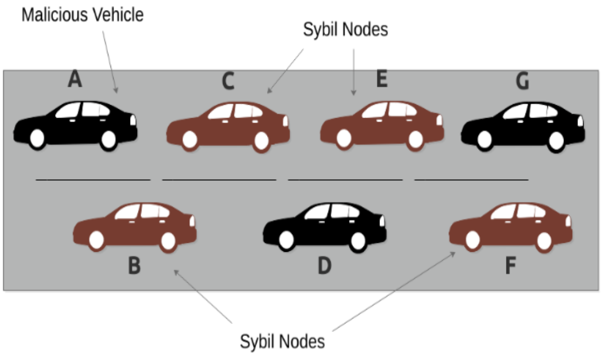

Figure 5. Sybil attack.

2.7. Man-In-The-Middle Attack

Man-in-the-middle is a severe attack, as it can compromise all the authenticity of the information, manipulating messages that are carried over the network [30]. The term ‘‘Man-in-the-middle” is derived from basketball, in which one player in the middle tries to intercept the ball while two other players try to pass. This attack can occur in two ways, passive and active. In a passive attack, the malicious vehicle can spy on the communication channel between two authorized vehicles on the network. In an active attack, the malicious vehicle can discard, delay, or change the contents of the data packet, changing the location of the source/destination node and the content of the message [2], [31]. Many VANETs attacks are variants of the Man-in-the-middle attack, such as the black hole, or the DoS attack.

3. Proposed Cyber Robust Security Scheme

The Cyber Robust (CR) scheme that we are proposing is a V2V security feature for position-based routing protocols (currently designed only to urban scenarios) that aims to reduce the impacts of the network attacks (faking position and black hole), discussed in Section II, by using a particular form of greedy forwarding. Our goal is to improve the greedy forwarding strategy of the GPSR-based algorithms (in this case, the GPSR and PA-GPSR) by introducing a security feature that uses a Neighbors' Trust List (NTL). The forwarding algorithm can check if the neighbor node is malicious by comparing the neighbor node position and the current node transmission range. If the algorithm detects that a node is malicious, it will be added to the list.

3.1. Neighbor's Trust List

All vehicles periodically transmit a hello packet to one hop neighbors and this information is stored in the Neighbors' Table (NT). With this information, the transmitting node can compare its transmission range and the neighbors position stored in the NT to identify malicious activity. Moreover, the transmitting node uses the timestamp information obtained from NT to avoid nodes with stolen position information, which contributes to select nodes that are not in the current node transmission range anymore. Each entry in the NTL has the identification (IP address) of the malicious nodes.

3.2. Network Attack and Prevention Example

Fig. 6 illustrates how the attack is performed and how the algorithm reacts to prevent data packets to be delivered to a malicious node. The node *A* is sending data to node *H* using the greedy forwarding strategy. In the first moment, the malicious node *M* is acting as a normal node, passively waiting for data packets to any destination to start faking its position. In the second moment, node *Z* also wants to send data to node *H*, then node Z sends the data to node *X*. Out of the two neighbors that lie within the communication range of node *X*, the malicious node *M* is the closest to the destination *H* and is the best option for receiving the packets. Therefore, node *X* sends the packets to node *M* according to the greedy forwarding algorithm. After receiving the packets, node *M* drops the packet and collects the destination node position. In the third moment, node *M* uses the position of the destination node *H* to fake its position in the hello packet to a position (*M′*) closer to the destination, deceiving neighbors' nodes since now the node seems to be closer to the destination. Node *D* now is also sending data packets to node *M*, since node *M* is ‘‘closer” to *H* than node *E*. In the fourth moment, nodes *X* and *D* using the security algorithm detailed in Algorithm 1, which detects that node *M* is faking its position, since the faked position *M′* of node *M* is totally out of range of node *D* and *X*. In this case, both nodes insert node *M* in the NTL and now both are avoiding sending data to *M*.

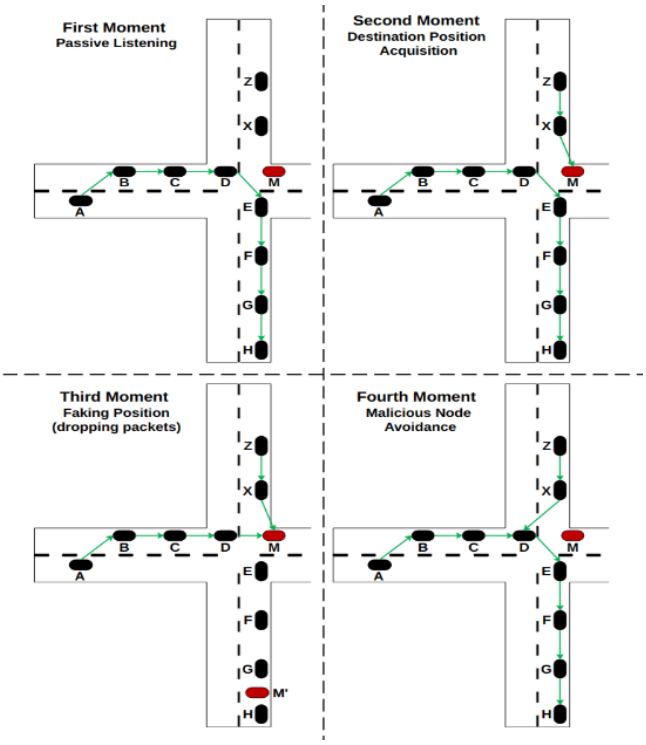

Figure 6. Malicious attack behavior and security prevention.

3.3. Stolen Information Avoidance

Another feature of our proposed CR scheme is to avoid sending data to any node that does not send any hello packet in the last communication period. This period is calculated as:

$$P = H + J \tag{1}$$

where ***H*** is the hello interval and ***J*** is a guard time (half of ***H***). This feature reduces the packet drop by preventing data to be sent to nodes that probably are not in the transmission range anymore. This situation occurs because the refresh rate of the NT is naturally bigger than the hello interval, which can lead to a situation where there is stolen neighbors' information at the NT.

3.4. Proposed Algorithm

Our cyber robust (CR) proposed security scheme is shown in detail in Algorithm 1, where *R* is the node receiving a packet, *N* is the set of one-hop neighbors of *R*, *n* is a node of the set *N*, and *D* is the destination node.

Algorithm 1 Proposed Security Algorithm

```
$Tr$ = get_transmission_range ();
$H$ = get_hello_interval ();
$J$ = get_jitter_interval ();
$I$ = get_refresh_interval ();
$S$ = get_average_speed ();
$T$ = get_current_time ();
At_Forwarding_Data_Packet

if $n \in N$ && Distance ($n$, $D$) $\leq$ Distance ($R$, $D$) then
    $n\_addr$ =from_NT_get_neighbor_node_addr ();
    $n\_time$ =from_NT_get_neighbor_node_timestamp ();
    if isMalicious ($n\_addr$) == false then
        if distance ($n$, $R$) > $Tr$ && distance ($n$,$R$) <= ($Tr$+($I$*$S$)) && ($T$-$n\_time$) >= ($H$+$J$) then
            continue;
        if distance ($n$, $R$) >($Tr$+($I$*$S$)) then
            malicious_list_add($n\_addr$);
            continue;
        end if
        No malicious node detected, proceeding to the forwarding algorithm;
    end if
  end if
end if
```

3.5. Time Complexity Analysis

Assuming that the number of neighbors' nodes is n, when the packet is forwarded using any form of greedy forwarding, the current node needs to calculate and compare the distances of the nodes to find the neighbor node with the shortest distance as the next hop node. Thus, for each node, the time complexity of greedy forwarding is $O(n)$. The proposed CR scheme (applied to CR-GPSR and CR-PAGPSR) adds an extra loop for each greedy forwarding step by searching for a malicious node in the NTL, in this way, the time complexity of the CR is also $O(n)$. Then, since the greedy forwarding has the computational complexity of $O(n)$, and CR performs twice the number of lookups (because of the extra table), the time complexity of an algorithm using greedy forwarding and the CR feature is $O(2n)$ which is the same as $O(n)$. Therefore, we can conclude that the CR feature does not affect the time complexity of the algorithms based on greedy forwarding, such as the PA-GPSR, and GPSR [18], [21].

4. Results and Discussion

The simulation of vehicles was conducted in an area of 1100m^2 with 9 intersections and 12 two-way streets, as shown in Fig. 7. The initial position of vehicles was randomly distributed and the movement of vehicles on the roads was based on the Car-following model (Krauss model) restricted along the street. The vehicle's speed does not exceed 15 m/s. To simulate a sparse urban network, we used 50, 70, 90 and 110 nodes. The number of malicious nodes was set to 10 and 20. The hello packet interval was set to 1 second. Each vehicle has a communication range set to 250 meters (approximately). The IEEE 802.11p standard was used to model MAC layer and two-ray ground radio propagation model was used to compute the wireless channel fading characteristics. We considered the data traffic to be Constant Bit Rate (CBR) for each node pair (source-destination) to generate packets of fixed size (512 Bytes). To evaluate the impact of the existing traffic in the network, we adopted two values of CBR connections (15 and 20) for each scenario varying the numbers of nodes. Random source-destination pairs were selected for each group of simulations. In this way, to perform the result for 15 CBR connections, we randomly selected 15 pairs and used the same pairs for all the sets of simulation runs. Moreover, the position of the nodes was available through a precise location service. Therefore, we assume there was no error in the location information. The total time for each simulation was configured to 200 seconds. All the results shown in this manuscript represent an average of 30 simulation runs and a 95% confidence interval. These parameters were selected based on the previous studies [18], [19], [32], [33], [34], [35], [36], [37].

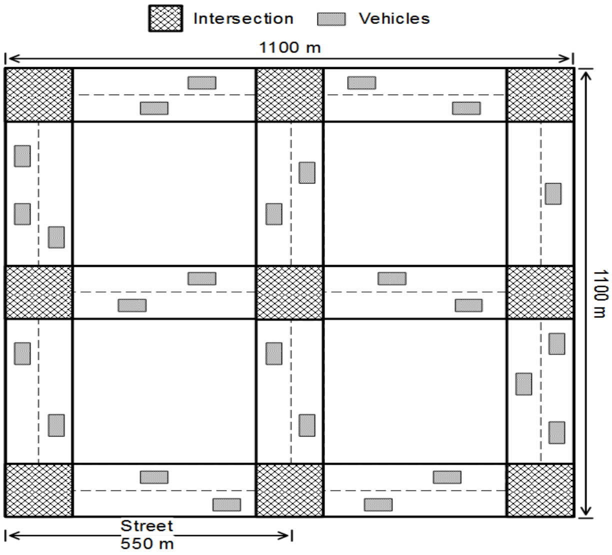

Figure 7. Scenario with 9 intersections and 12 streets.

The performance metrics used in our simulations are defined as follows:

- **Packet delivery rate (PDR)**: Represents the ratio of the total received packets at destination R_{dest} to the total number of packets sent from the source node T_{source}.

$$PDR\ (\%) = \frac{R_{dest}}{T_{source}} \times 100 \qquad (2)$$

- **End-to-end delay**: The average value of all successfully received packets delay D_n.

$$Delay = \frac{\sum_{n=1}^{N} Dn}{N} \qquad (3)$$

4.1. Packet Delivery Ratio

We first study the PDR of routing cyber robust (CR) security schemes (CR-GPSR and CR-PAGPSR) against their traditional schemes (GPSR and PA-GPSR) with scenarios varying the number of vehicles and malicious nodes. Fig. 8-11 represent the packet delivery ratio for different numbers of vehicles (nodes), malicious nodes and CBR connections. For all different CBR cases, in general, the average packet delivery ratio when the number of vehicles increase tends to be higher (with some exceptions), since the network connectivity also increases, which reduces the probability of encountering a network partition and gives more options for the algorithms when selecting different nodes to forward. High percentages of PDR mean that the network is delivering more packets, e.g., in the context of routing protocol, the algorithms are leading packets through good routes.

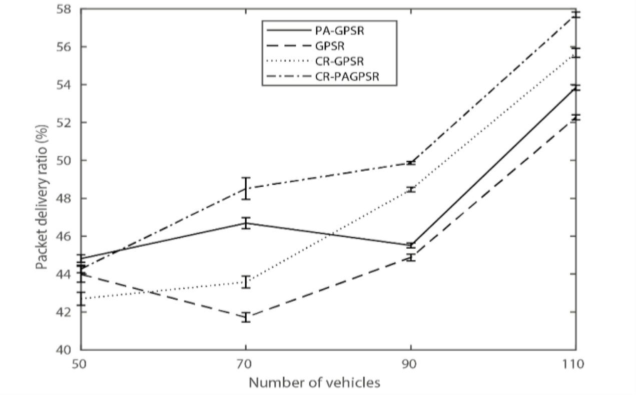

Figure 8. PDR for 15 CBR connections and 10 malicious nodes.

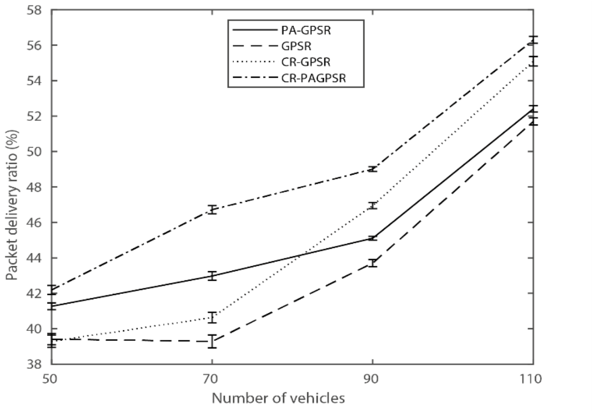

Figure 9. PDR for 20 CBR connections and 10 malicious nodes.

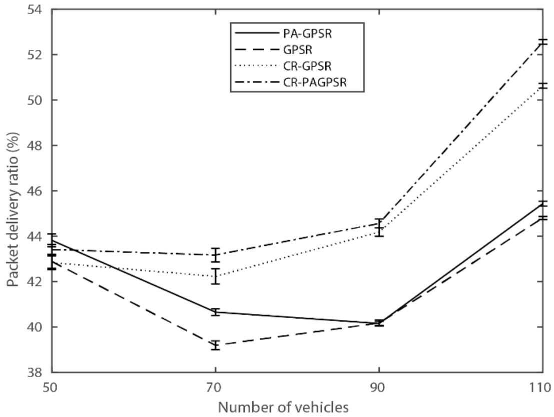

Figure 10. PDR for 15 CBR connections and 20 malicious nodes.

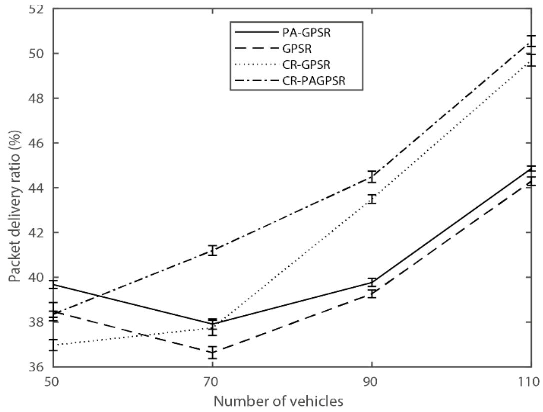

Figure 11. PDR for 20 CBR connections and 20 malicious nodes.

Overall, as shown in Fig. 8-11, when the security improvement is used in the scenario with 10 malicious nodes and 15 CBR connections, the CR-GPSR and CR-PAGPSR can increase the PDR by about 4% and 5%, respectively, on average as compared to their conventional routing schemes. In Fig. 9, in the scenario with 10 malicious nodes and 20 CBR connections, the CR-GPSR and CR-PAGPSR can increase the PDR by about 4% and 6.5%, respectively. In Fig. 10, in the scenario with 20 malicious nodes and 15 CBR connections, the CR-GPSR and CR-PAGPSR can increase the PDR by about 7% and 7.5%, respectively. In Fig. 11, in the scenario with 20 malicious nodes and 20 CBR connections, the CR-GPSR and CR-PAGPSR can increase the PDR by about 5.5% and 7%, respectively.

In general, the algorithms with the security improvement (CR-GPSR and CR-PAGPSR) have better performance of avoiding malicious nodes when compared with their traditional approaches. The only cases where performance degradation occurs are in scenarios where the number of vehicles is equal to 50 (except for the scenario with 20 CBR connections and 10 malicious nodes). In these cases, the CR-GPSR and CR-PAGPSR present a small performance degradation. It shows that the security improvement is not well suitable for highly sparse networks (e.g., networks with a small number of nodes). Moreover, the bad performance of the algorithm in this scenario (50 nodes) is caused by the ratio of the number of non-malicious and malicious nodes for 10 and 20 malicious nodes scenarios are 20% and 40%, respectively. These high ratios may cause bad route selection or even force the packet to be dropped. It is important to notice that the application used in this work is sending only 5 packets per second. We are confident that the improvement in the PDR would be better by using a higher bit rate application with smaller packet interval. The next section presents how the security improvement affects the end-to-end delay performance of the selected algorithms in the same scenarios.

4.2. End-to-end Delay

Fig. 12-15 illustrate the average end-to-end delay for the four scenarios varying the number of CBR connections, malicious nodes, and the number of vehicles. Analyzing the results, it can be highlighted that the algorithms with the proposed security feature (CR-GPSR and CR-PAGPSR) achieves a

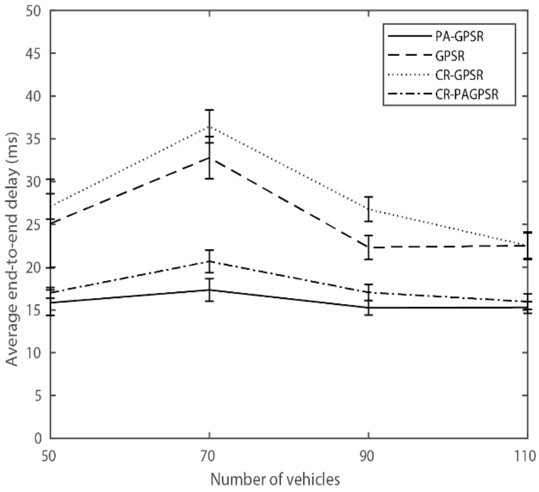

Figure 12. End-to-end delay for 15 CBR connections and 10 malicious nodes.

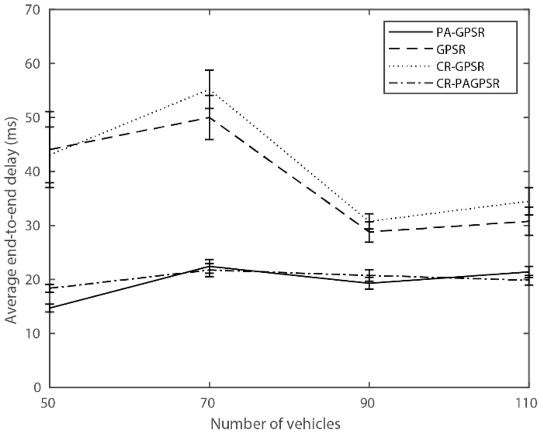

Figure 13. End-to-end delay for 20 CBR connections and 10 malicious nodes.

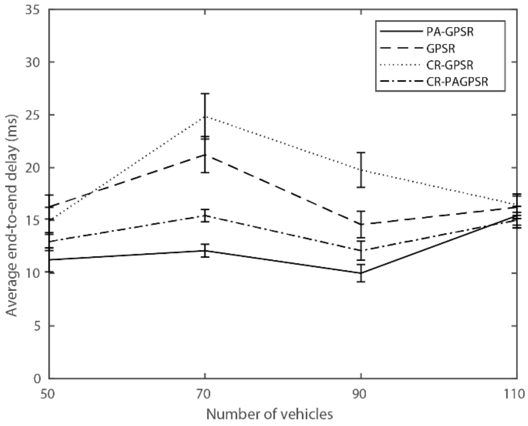

Figure 14. End-to-end delay for 15 CBR connections and 20 malicious nodes.

higher end-to-end delay in comparison with their traditional versions (GPSR and PA-GPSR) in the four scenarios evaluated. This can be explained by the fact that the application is UDP-based. A user datagram protocol (UDP) splits a message into packets (datagram) to be forwarded by the nodes in the network. In this case, the delay is only taken in account when the packet arrives. The security improved versions are delivering more packets (as shown in Fig. 8-11) by avoiding some routes when detect malicious nodes in the way, causing packets to be delivered through a long path (e.g., packets that have higher delay). On the other hand, the traditional GPSR and PA-GPSR would have lost the packet to the malicious node.

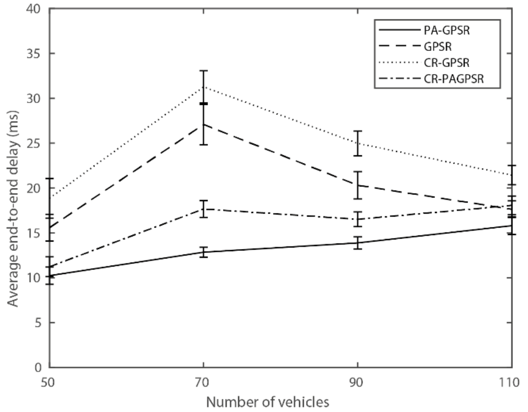

Figure 15. End-to-end delay for 20 CBR connections and 20 malicious nodes.

Analyzing the results in Fig. 12 we can observe that the difference between the average end-to-end delay of PA-GPSR and CR-PAGPSR is about 2ms, and about 3ms between GPSR and CR-GPSR. In Fig. 13, PA-GPSR and CR-PAGPSR have almost the same delay values (the difference between them is less than 1ms), and the differences between GPSR and CR-GPSR is about 2ms. These small differences are obtained in the scenario with 10 malicious nodes, which cause less impact in the end-to-end delay, since few packets are lost. The delay difference is higher when the scenario based on 20 malicious nodes is considered. Analyzing the results in Fig. 14 and Fig. 15, the difference between the average end-to-end delay of PA-GPSR and CR-PAGPSR are about 2ms and 3ms, respectively, and the difference between GPSR and CR-GPSR are 3ms and 5ms, respectively. Based on this, it can be noticed that the increased value in the delay is also influenced by the number of CBR connections. When the number of CBR connections increases, the delay difference is also increased.

5. Conclusions

The focus of this work was to increase the robustness of the well-known V2V position-based routing protocol GPSR and its variant PA-GPSR against malicious activity due to their inability to handle and detect network attacks. We have proposed a Cyber Robust (CR) feature that uses the transmission range, hello packet interval, position information shared regularly among neighbors' nodes, and a special list called Neighbors Trust List (NTL) to detect attempts of malicious attacks. We conducted a comparative performance study of the traditional GPSR and PA-GPSR against their CR versions using the NS-3 network simulation in a Manhattan grid scenario. The node's mobility was generated by SUMO and imported to NS-3. We quantitatively analyzed the PDR gains and end-to-end delay of the algorithms in different scenarios, varying the number of CBR connections and malicious nodes. Extensive simulations showed that the PDR of the algorithms with the CR feature outperform their traditional versions (with no increase of computational complexity). The algorithms with the CR feature showed a slight increase for the end-to-end delay when compared to their traditional versions, since the algorithms with the CR feature could take long routes to avoid malicious nodes. On the other hand, the traditional GPSR and PA-GPSR would have lost the packet for the malicious attack. To facilitate the reproduction of our results, we provided an open-source implementation of our framework at github.com/CSVNetLab/VanetSecurity. For future implementation, we plan to compare our CR scheme against position-based routing algorithms under a real scenario using the OpenStreetMap tool to select areas of real cities. Besides, we also plan to use higher bit rate entertainment applications.

References

[1] H. Xu, M. Zeng, W. Hu, J. Wang, "Authentication-based vehicle-to-vehicle secure communication for VANETs." Mobile Information Systems, vol. 19, 2019.

[2] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies." Sensors 18, no. 11, 2018.

[3] J. M. Lozano Domínguez, T. J. Mateo Sanguino, "Review on V2X, I2X, and P2X communications and their applications: A comprehensive analysis over time." Sensors 19, no. 12, 2019.

[4] X. Cheng, C. Chen, W. Zhang, Y. Yang "5G-enabled cooperative intelligent vehicular (5GenCIV) framework: When benz meets marconi." IEEE Intelligent Systems, no. 32, pp. 53–59, 2017.

[5] L. Nkenyereye, L. Nkenyereye, S. Islam, Y.-H. Choi, M. Bilal, J.-W.Jang, "Software-defined network-based vehicular networks: A position paper on their modeling and implementation." Sensors 19, no. 17, 2019.

[6] M. S. Sheikh, J. Liang, "A comprehensive survey on VANET security services in traffic management system." Wireless Communications and Mobile Computing, vol. 19, 2019.

[7] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges." Vehicular Communications, vol. 19, 2019.

[8] M. Sathish, K. Arumugam, S. N. Pari, V. Harikrishnan, "Detection of single and collaborative black hole attack in MANET." In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), India, pp. 2040–2044, 2016.

[9] P. Dong, X. Du, H. Zhang, T. Xu, "A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows." In 2016 IEEE International Conference on Communications (ICC), Malaysia, pp. 1–6, 2016.

[10] T. B. M. de Sales, A. Perkusich, L. M. de Sales, H. O. de Almeida, G. Soares, M. de Sales, "ASAP-V: A privacy-preserving authentication and sybil detection protocol for VANETs." Information Sciences, vol. 372, pp. 208–224, 2016.

[11] P. K. Singh, S. Gupta, R. Vashistha, S. K. Nandi, S. Nandi, "Machine learning based approach to detect position falsification attack in VANETs." In: International Conference on Security & Privacy, Singapore, pp. 166–178, 2019.

[12] K. M. Ali Alheeti, A. Gruebler, K. McDonald-Maier, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks." Computers, vol. 5, no. 3, pp. 1-16, 2016.

[13] P. S. Waraich, N. Batra, "Prevention of denial-of-service attack over vehicle ad hoc networks using quick response table." In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), India, pp. 586–591, 2017.

[14] S. Lachdhaf, M. Mazouzi, M. Abid, "Detection and prevention of black hole attack in VANET using secured AODV routing protocol." In: International Conference on Networks & Communications (NetCom 2017), Dubai, pp. 25–36, 2017.

[15] D. Al-Terri, H. Otrok, H. Barada, M. Al-Qutayri, Y. Al Hammadi, "Co-operative based tit-for-tat strategies to retaliate against greedy behavior in VANETs." Computer Communications, vol. 104, pp 108–118, 2017.

[16] X. Bao, H. Li, G. Zhao, L. Chang, J. Zhou, Y. Li, "Efficient clustering V2V routing based on PSO in VANETs." Measurement, vol. 152, 2020.

[17] J. Wu, M. Fang, H. Li, X. Li, "RSU-assisted traffic-aware routing based on reinforcement learning for urban VANETs." IEEE Access, vol. 8, pp. 5733–5748, 2020.

[18] A. Silva, N. Reza, A. Oliveira, "Improvement and performance evaluation of GPSR-based routing techniques for vehicular ad hoc networks." IEEE Access, vol. 7, pp. 21722–21733, 2019.

[19] A. Silva, K. M. N. Reza, A. Oliveira, "An adaptive GPSR routing protocol for VANETs." In 2018 15th International Symposium on Wireless Communication Systems (ISWCS), Portugal, pp. 1–6, 2018.

[20] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, A. A. Loureiro, "Data communication in VANETs: Protocols, applications and challenges." Ad Hoc Networks, vol. 44, pp. 90–103, 2016.

[21] B. Karp, H.-T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks." In: Proceedings of the 6th annual international conference on Mobile computing and networking, USA, pp. 243–254, 2000.

[22] A. N. Vigilia, J. S. Suseela, "Survey on unicast, multicast and broadcast routing techniques in vehicular ad-hoc networks–present and future." British Journal of Mathematics & Computer Science, vol. 13, pp. 1–26, 2016.

[23] J. Vasu, G. Tejpal, S. Sharma, "Review on various routing attacks in vehicular ad hoc networks." International Journal of Computer Applications, vol. 167, no. 1, 2017.

[24] V. H. La, A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey." International Journal on ad hoc Networking Systems, vol. 4, no. 2, pp. 1-20, 2014.''

[25] M. A. H. Al Junaid, A. Syed, M. N. M. Warip, K. N. F. K. Azir, N. H. Romli, "Classification of security attacks in VANET: a review of requirements and perspectives." MATEC Web of Conferences, vol. 150, 2018.

[26] R. Mishra, A. Singh, R. Kumar, "VANET security: Issues, challenges and solutions." In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), India, pp. 1050–1055, 2016.

[27] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, B. Eiss-feller, "Emerging attacks on VANET security based on GPS time spoofing." In 2015 IEEE Conference on Communications and Network Security (CNS), Italy, pp. 344–352, 2015.

[28] N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study." International Journal of Security and Its Applications, vol. 10, no. 5, pp. 261–274, 2016.

[29] D. Kushwaha, P. K. Shukla, R. Baraskar, "A survey on sybil attacks in vehicular ad-hoc network." International Journal of Computer Applications, vol. 98, no. 15, 2014.

[30] K. Stepién, A. Poniszewska-Maranda, "Security measures in the vehicular ad-hoc networks–man in the middle attack." In: International Conference on Mobile Web and Intelligent Information Systems, Turkey, pp.136–147, 2019.

[31] T. Zaidi, S. Faisal, "An overview: Various attacks in VANET." In: 20184th International Conference on Computing Communication and Automation (ICCCA), India, pp. 1–6, 2018.

[32] X. Zhang, X. Cao, L. Yan, D. Sung, "A street-centric opportunistic routing protocol based on link correlation for urban VANETs." IEEE Transactions on Mobile Computing, vol. 15, no. 7, pp. 1586-1599, 2016.

[33] X. M. Zhang, K. H. Chen, X. L. Cao, D. K. Sung, "A street-centric routing protocol based on micro topology in vehicular ad hoc networks." IEEE Transactions on Vehicular Technology, vol. 65, no. 7, pp. 5680–5694, 2016.

[34] N. Li, J.-F. Martíınez-Ortega, V. H. Díaz, J. A. S. Fernandez, "Probability Prediction-based reliable and efficient opportunistic routing algorithm for VANETs." IEEE/ACM Transactions on Networking (TON), vol. 26, no. 4, pp. 1933–1947, 2018.

[35] X. Yang, M. Li, Z. Qian, T. Di, "Improvement of GPSR protocol in vehicular ad hoc network." IEEE Access, vol. 6, pp. 39515-39524, 2018.

[36] A. Silva, N. Reza, A. Oliveira, A. Klautau, "A reduced beacon routing protocol for inter-vehicle communications." XXXVII Brazilian Symposium of Telecommunications and Signal Processing (SBrT), Brazil, pp. 905-910, 2019.

[37] Drishya, S. R., S. Renukadevi, and V. Vaidehi. "A Stable Clustering Scheme with Node Prediction in MANET." International Journal of Communication Networks and Information Security (IJCNIS), vol. 13, no. 1, 2021.