Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks

Nizar Alsharif, Albert Wasef, and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada
Email: {nshalari,awasef,xshen}@brcr.uwaterloo.ca

Abstract—In this paper, we investigate the effects of routing loop, sinkhole, and wormhole attacks on the position-based routing (PBR) in vehicular ad hoc networks (VANETs). We also introduce a new attack termed wormhole-aided sybil attack on PBR. Our study indicates that the wormhole-aided sybil attack has the worst impact on the packet delivery in PBR. To ensure the reliability of PBR in VANETs, we propose a set of plausibility checks that can mitigate the impact of these PBR attacks. The proposed plausibility checks do not require adding extra hardware to the vehicles. In addition, they can adapt to different road characteristics and traffic conditions. Simulation results are given to demonstrate that the proposed plausibility checks are able to efficiently mitigate the impact of the previously mentioned PBR attacks.

I. INTRODUCTION

VANET is one of the promising technologies that will provide a wide range of safety and comfort applications for travelers along roads. VANETs enable (V2X) communications where vehicles equipped with on-board units (OBUs) can communicate with other vehicles and roadside units (RSUs) installed along roads. VANET applications can be classified according to the encountered number of hops in vehicular communications to one-hop and multi-hop applications.

Routing is one of the vital mechanisms for achieving reliable multi-hop applications in VANETs. Unfortunately, the highly dynamic VANET topology poses many challenges for designing an efficient routing scheme for VANETs. Vehicular communication projects such as CarTalk2000 [1] and NoW [2] have considered position-based routing (PBR) [3] to cope with the challenging VANET network characteristics. PBR requires each vehicle to periodically broadcast its geographic location in a beacon packet. Fortunately, this requirement can be easily achieved in VANETs as each vehicle is equipped with (Global Positioning Service) GPS receiver used to determine its location. Based on the received packets from the neighboring vehicles, each vehicle maintains a list of the geographic locations of its neighboring vehicles. In case of forwarding a packet, a vehicle selects the next hop vehicle based on its routing table and the forwarding strategy in the employed PBR scheme. In PBR, the route of the packets from a source to a destination does not depend on predetermined forwarders but rather the forwarders can be different for different packets along the same route between the source and destination. Consequently, PBR can adapt to the highly dynamic VANET topology. Studies show that PBR performs well in urban and highway scenarios [4].

Without secure PBR, an attacker can severely disrupt the network operation by launching a number of serious attacks such as impersonation attack, packet modification attack, sybil attacks, sinkhole attack, routing loop attack, and wormhole attack. The attackers can be generally classified into outsiders who are illegitimate entities that do not have any security materials such as authentic certificates, secret keys, etc., and insiders who are legitimate authentic users behaving maliciously. The attacks on PBR can be classified as follows: (1) Attacks detectable by the traditional security mechanisms such as impersonation attack and packet modification attack. Whether launched by outsider attackers or insider attackers, this type of attacks can be easily detected by any security mechanism providing the primary secure routing requirement which are entity authentication, message integrity, and end-to-end non-repudiation. It is widely acceptable that Public Key Infrastructure (PKI) will be the basic building block of any VANET security mechanism [5]-[8]. In PKI, each entity has time-limited authentic certificate(s), and it signs every outgoing message. Authentic certificates are used to achieve entity authentication. Since certificates cannot be forged, impersonation attacks are almost impossible. Any packet modification attempt renders the signature attached to a message invalid, and the message will be eventually dropped; (2) Attacks undetectable by the traditional security mechanisms such as routing loop, sinkhole, wormhole, and sybil attacks. These attacks are usually launched by insider malicious nodes which have authentic security credentials, e.g., secret keys, certificates, etc. Hence, it is difficult to detect these attacks using the traditional security mechanisms.

Our contributions in this paper are as follows: (1) We investigate the effects of the undetectable attacks on the PBR performance. To the best of our knowledge, this is the first work to investigate the effect of these attacks in the VANET context; (2) We introduce a new PBR attack termed wormhole-aided sybil attack; (3) We propose a set of plausibility checks that can adapt to road characteristics and traffic conditions to mitigate the effects of this type of attacks; and (4) We verify the reliability of the proposed plausibility checks through simulations which show that the proposed plausibility checks can efficiently mitigate the effects of this type of attacks.

The remainder of the paper is organized as follows. Section II investigates the impact of the PBR attacks on the network performance and introduces the wormhole-aided sybil attack. In section III, we present the proposed plausibility checks and their implementation requirements. Performance evaluation is given in section IV. The related work is discussed in section V. Section VI concludes the paper.

II. IMPACT OF PBR ATTACKS ON THE PBR PERFORMANCE

In this section, we conduct simulations to investigate the effects of the undetectable attacks on the PBR performance. The metric of interest is the Packet Delivery Ratio (PDR) which is defined as the ratio of the number of transmitted packets to the
number of received packets. We adopt the Greedy Perimeter Stateless Routing (GPSR) scheme [9] as an instance of PBR. In GPSR, the default packet forwarding strategy is the greedy strategy, where the sender selects the closest vehicle to the destination as the next hop. If the sender cannot find a forwarder based on the greedy strategy, it forwards the packet around the perimeter of the region containing itself and the destination.

Table I shows the employed parameters in the conducted simulations. In these simulations, we consider a bidirectional roads in a Manhattan city street scenario, and random distribution of the vehicles in the simulation area. According to its location, each vehicle moves following the lane direction with fixed speed of 60 km/h. Upon reaching an intersection, vehicles make a turn with probability 50% or keep moving in the same direction. Vehicles reached the end of the simulation area start entering the area from the opposite side. Every 300 msec, each vehicle sends a beaconing message indicating its position. Every 500 msec, 5 random source vehicles and 5 random destination vehicles are selected. Packets are routed from the sources to the destination using the GPSR protocol. For accuracy, every simulation result is averaged over 10 simulation repetitions.

A. Impact of Routing Loop Attacks

In routing loop attack, an internal attacker receives a message, updates it, and sends it back to one of the previous forwarders (or the source) even if there is a better node in its routing table that is available to be the next forwarder according to the routing strategy. The aim of this attack is to delay or prevent the delivery of a message. In this simulation, an attacker ignores the routing strategy and sends the packet back to its sender. Fig. 1 shows the resulting PDR vs. the vehicles density when 0%, 5%, 15%, and 30% of the vehicles are malicious, i.e., they are launching the routing loop attack. It can be seen from Fig. 1 that the PDR increases with the vehicles density. Also, the PDR decreases as the number of malicious vehicles increases as more packets are trapped in routing loops and they cannot reach their destinations.

B. Impact of Sinkhole Attacks

In a sinkhole attack, an internal attacker convinces other nodes to be their next hop forwarder by announcing a different location in its beacon messages; it then drops any received message in a selfish behavior. The impact of sinkhole attacks on the network performance includes both poisoning the routing tables of the attacker’s neighbors and dropping their packets. A sinkhole attacker can be rational or irrational according to its motive. Rational sinkhole attackers aim to grab other node packets to analyze them. For example, an attacker will claim a location close to an automatic payment unit in order to extract important payment information. On the other hand, irrational sinkhole attackers aim to disturb the network operation. Two simulations were designed to evaluate the impact of sinkhole attacks. In the first simulation, each attacker claims random locations in its beacon messages and drops any received message. In the second simulation, the attacker claims a plausible location located on the road map and within its transmission range. The claimed location is designed to be ahead of the real attacker’s location by the value $C_r/2$ in its movement direction, where $C_r$ is the nominal communication range of a vehicle in VANET. This attack is referred to as smart sinkhole attack. Fig. 2 and Fig. 3 respectively show the PDR when simple sinkhole and smart sinkhole attack are launched. It can be seen that the simple sinkhole attack affects the PDR of the network more than the smart sinkhole attack. By claiming farther distances, the simple sinkhole attackers are able to convince more nodes to be their next hop; the smart sinkhole attackers limit their location options in order to be plausible. From Figs 1-2, it can be seen that the simple sinkhole attack has more impact on the PDR compared with the routing loop attack.

C. Impact of Wormhole Attack

In a wormhole attack, two or more attackers are connected via a private high speed link and they resend messages heard in one terminal into the other terminal(s). Replaying authentic beacons from different locations enables attackers to dominate the routing paths. Wormhole attackers connect the network via
their private connection, which may improve the network’s performance as if road-side infrastructure has been used for delivering the packets from one location to another. The attackers aim to dominate the connection so they can eavesdrop or partition the network. Fig. 4 shows the effect of wormhole attack on the network’s PDR. In this simulation scenario, the attackers replay all the packets, whether beacon or data packets, from one location to another. As it can be seen from the figure, the network’s PDR is improved since the attackers improve the network connectivity by relaying the packets from one location to another.

D. Wormhole-Aided Sybil Attack and Its Impact

In traditional sybil attack, an attacker claims to be multiple vehicles by broadcasting multiple identities for itself. Then the attacker disseminates faked geographic positions corresponding to the claimed vehicles to subvert the routing paths of the neighboring vehicles. As mentioned previously, it is widely acceptable that PKI will be used to secure VANETs, where each vehicle has an authentic time-limited certificate(s). A time-limited certificate can only be used during its validity period. When a vehicle receives a message, it first checks the validity period of the sender’s certificate. If it is invalid, it immediately drops the message. Consequently, it is impossible to launch the traditional sybil attack when PKI is used in securing VANET.

Now, we introduce a new form of sybil attack termed wormhole-aided sybil attack. In this attack, a wormhole attack is launched between two attackers. Each attacker captures only the beacon messages broadcast in its area and forward them to the other attacker. Then, each attacker replays the received beacon messages in its area. The vehicles receiving the replayed beacons will accept them because these beacons are generated from authentic vehicles during the validity period of their certificates. Thus, each attacker appears as multiple vehicles which causes severe disruption to the routing decisions of its neighboring vehicles. Fig. 5 shows the network’s PDR under this attack. It can be seen that this attack has a severe impact on the network’s PDR even if the number of malicious nodes is only 5%. Also, for the cases when the malicious nodes are 15% and 30% of the total number of nodes, the PDR is almost less than 30%. The reason for the severe impact of this attack on the network’s PDR is that replaying beacons form one location to another contaminates the routing tables of the nodes in the area where the replaying is taking place, which results in selecting forwarders that do not exist in the transmission range of the transmitting node. It can be seen from Figs. 1-5 that the wormhole-aided sybil attack has the worst impact on the network performance compared with other attacks under consideration.

III. THE PROPOSED PLAUSIBILITY CHECKS AND THEIR IMPLEMENTATION REQUIREMENTS

In this section, we propose plausibility checks (PC) and their implementation requirements to mitigate the effects of the aforementioned attacks on the network performance.

A. Plausibility Checks

The plausibility checks ensure that the received message follows some logical rules as follows.

1) Spatial Checks:

a) Communication range: Each recipient (forwarder or destination) of a message must make sure that they fall within the sender’s communication range by ensuring that \( l_r - l_s \leq C_r \), where \( l_r \) and \( l_s \) are the locations of the receiver and the sender, respectively, and \( C_r \) is the nominal communication range of the vehicles in VANETs.

b) Speed and density: Greenshields’ speed-density relation [10] states that

\[
v(k) = v_f - \frac{v_f k}{k_j}
\]

(1)
where \( v_f \) is the free flow speed (i.e., the maximum speed), \( k_j \) is the jam density (i.e., the maximum allowed density). We adopt Greenshields’ relation to check that the speed of the transmitting vehicle and the density of the neighboring vehicles are plausible as follows: When a vehicle receives a message, it calculates the number of its neighboring vehicles from its routing table and calculates the density of the neighboring vehicles. Then, it uses eq. (1) to calculate the plausible average speed of its neighboring vehicles as a function of the neighboring vehicles’ density. After that, it ensures that \( v_s \leq v(k) \pm \Delta \), where \( v_s \) is the speed of the sender, and \( \Delta \) is a speed margin factor to accommodate for the speed variations. Intuitively, \( v(k) \) should be always a positive value. A negative value for \( v(k) \) implies that the density \( k \) exceeded the maximum allowed density \( k_j \), which could imply a sybil attack.

c) Moved distance: The receiver of a message can check the plausibility of the moved distance by the transmitter with respect to the last known position of the transmitter by ensuring that \( l_{s2} - l_{s1} \leq (t_{s2} - t_{s1}) \cdot v(k) \), where \( l_{s2} \) is the location of the sender included in the received message, \( t_{s2} \) is the timestamp included in the received message, and \( l_{s1} \) is the location of the sender at time \( t_{s1} \) in the routing table (i.e., the location of the sender received from the beacon messages).

d) Map location: Taking the advantage that each vehicle is equipped with a GPS receiver, the receiver of a message must ensure that the location of the sender of the message does not lie on an impossible location, e.g., house, river, etc.

2) Temporal Checks: Each beacon and data packet includes a timestamp of the sending time. Upon receiving a packet or a beacon, each vehicle checks that \( t_r - t_s \leq \Delta_t \) where \( t_r \) is the receiving time, and \( \Delta_t \) is the maximum plausible time for transmission and processing.

3) Strategy Checks: In PBR, different protocols have different forwarding strategies. When a vehicle receives a packet to be forwarded, it should check if it falls into a feasible forwarding region with respect to the destinations position and the forwarding strategy.

4) Overhearing Checks: When a node sends a packet to be forwarded, it expects to hear the packet being forwarded. If the packet was not transmitted, it re-transmits the packet to the next node in the routing metric, and avoids selecting the node that does not forward the packet as a forwarder for a period of time.

5) Content Checks: Checking message contents in terms of duplicated or expired content will effectively preserve the network resources. For example, if a node \( x \) forwards a packet to node \( y \) at time \( t_1 \) and it received the same packet again at time \( t_2 \), node \( x \) excludes node \( y \) from its routing table for a period of time and forwards the packet to the next node in its routing table. In addition, monitoring the contents in term of message generating rate helps in bandwidth preserving. For example, sending beacons or location inquiries at a considerable high rate should be ignored and reported.

B. Implementation Requirements

Since the plausibility checks are logical rules, there is no need for adding any extra hardware to the vehicles. All the required information to deploy the plausibility checks can be obtained autonomously by the vehicles except for the nominal communication range of a vehicle \( C_r \), the free flow speed \( v_f \), and the jam density \( k_j \). The nominal communication range \( C_r \) changes from one area to another depending on the number of obstructions in the area that may limit the transmission range of the vehicles. For example, the nominal communication range of a vehicle will change from rural to urban areas. Similarly, the jam density \( k_j \) and the free flow speed \( v_f \) change from one area to another depending on the number of lanes on the road. We propose to divide the coverage area of a VANET service provider to smaller areas each with its specific \( C_r \), \( v_f \), and \( k_j \) and upload this information in each vehicle during the initial registration with the VANET service provider. In this way, the plausibility checks can adapt to different road characteristics. In addition, using Greenshields’s formula makes the speed check adaptive to the real time traffic density.

IV. Performance Evaluation of PBR Employing Plausibility Checks

In this section, we evaluate the performance of the PBR employing the plausibility checks (PBR-PC) by conducting the same simulation scenarios performed in section II using the same simulation parameters. We set the overhearing period in the overhearing check to \( 600 \) ms. It should be noted that we excluded the wormhole attack from the performance evaluation as it improves the network performance as previously discussed.

Figs. 6-9 show the effect of the routing loop, simple sinkhole, smart sinkhole, and wormhole-aided sybil attacks on the performance of the GPSR (as an instance of PBR) employing plausibility check (GPSR-PC), respectively. It can be seen that PBR-PC can maintain the network PDR to at least 90% for vehicles density greater than 50 vehicle/Km\(^2\) in all scenarios.

The strategy and content checks are designed to detect the routing loop attacks. The spatial and the overhearing checks can efficiently detect the simple and smart sinkhole attacks. Also, the spatial, temporal, content, and strategy checks can thwart the wormhole-aided sybil attack.

From Figs. 6-9 and the previous discussion, the PBR employing plausibility checks can efficiently mitigate the effects of the routing loop, sinkhole, and wormhole-aided sybil attacks and maintain the network performance to comparable levels with the attack-free scenario (i.e., the 0% malicious nodes in the...
V. Related Work

Only few works have addressed the problem of detecting falsified positions in VANET. Golle et al. [11] proposed a technique for detecting and correcting malicious data. The main idea is that each vehicle, based on its sensors capabilities, could maintain a model for the network status which can be used to detect falsified data. It is shown that this technique can work efficiently when additional hardware, such as using sensors, cameras, etc., are used to obtain accurate information about the vehicles positions. The work in [12] requires installing additional radar on each vehicle, which is used as the vehicle’s virtual eye to verify the locations of the neighboring vehicles. Leinmüller et al. [13] proposed using hard thresholds to detect falsified positions. This work does not require additional hardware in the vehicles. However, it lacks the adaptability to different road characteristics and traffic conditions. Sybil attack in VANET is discussed in [14] and [15] based on the difficulty of deploying PKI in VANETs, which may not be true especially with the well-known security and privacy requirements in VANETs. Different from the above works, our work studies the impact of PBR attack on the network performance and it can hinder most the undetectable attacks by traditional security schemes. In addition, our approach can adapt to different road characteristics and real time traffic conditions.

VI. Conclusion

In this paper, we have investigated the effect of routing loop, sinkhole, wormhole, and wormhole-aided sybil attacks on the performance of PBR in VANETs, where we have shown that the wormhole-aided sybil attack has the worst impact on the network performance. In addition, we have proposed a set of plausibility checks that can adapt to different road characteristics and traffic conditions. Employing the proposed plausibility checks with PBR can not only efficiently mitigate the effects of these attacks, but also maintain the network performance at high level. Our future work will focus on cooperative misbehavior detection to thwart the effect of these attacks.

REFERENCES


Fig. 9. The impact of wormhole-aided sybil attack on GPSR-PC figures.


Fig. 9. The impact of wormhole-aided sybil attack on GPSR-PC