CSIT (September 2013) 1(3):261–279
DOI 10.1007/s40012-013-0025-1

ORIGINAL RESEARCH

Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks

Jyoti Grover · Vijay Laxmi · Manoj Singh Gaur

Received: 3 June 2013 / Accepted: 16 August 2013 / Published online: 24 September 2013

Abstract Vehicular ad hoc networks (VANETs) are vulnerable to message forging attacks, where an attacker creates a new message or replays/modifies an existing message. Forging of message can be carried out by attacker directly or indirectly through another vehicle. In VANETs, each vehicle periodically broadcasts short packets (beacons) with its identifier, time and current geographical position. In a position forging attack, an attacker broadcasts timely coordinated traffic warning messages with forged positions, producing illusion of an accident/traffic jam or an emergency braking. In this manner, VANET performance degrades in terms of channel utilization. It also severely impact the performance of security algorithms. In this paper, our focus is on the design and implementation of various forms of position forging attacks. We have presented detection approaches for these attacks. Unlike existing detection approaches, our methods are not based on the concept of estimating the position of senders. We have analyzed the impact of forged position information on average vehicle speed, number of collisions and percentage of delivered packets. Effectiveness of detection methods for various attack scenarios is compared. Instead, it works on the pattern of position information broadcast in consecutive packets. Simulation results demonstrates the effectiveness and adaptability of our proposed approach for VANETs.

J. Grover (✉) · V. Laxmi · M. S. Gaur
Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan, India
e-mail: jyoti.grover@gmail.com

V. Laxmi
e-mail: vlgaur@gmail.com

M. S. Gaur
e-mail: gaurms@gmail.com

Keywords Vehicular ad hoc networks · Position forging · Path forging · Attack · Security · Simulation

1 Introduction

The goal of vehicular Ad Hoc networks (VANETs) is to improve vehicle passenger safety by means of inter-vehicular communication. For example, in case of an accident, VANET communication can be used to warn other vehicles approaching the site. VANET employs two types of communication devices (1) on-board units (OBUs) and (2) road side units (RSUs). An OBU is installed in a vehicle and RSUs are placed on roadside. VANET offers two types of communication—vehicle to vehicle (V2V) and vehicle to RSU (V2R).

Information security is an essential requirement for the effectiveness of inter-vehicle communication. VANETs are vulnerable to many security threats and attacks. Various types of attacks in VANET are presented in [1, 2]. Malicious nodes take the advantage of wireless communication environment to implement the position and identity (ID) spoofing attacks. In this attack, the attacker masquerades as another by spoofing ID and position of some other node and thereby gains an illegitimate advantage. As all the communication is conducted over the shared broadcast channel and periodical exchange of beacon packets, attacker can claim multiple identities without being detected. VANET introduces challenges for efficient trust and ID management due to absence of a centralized authority [3, 4]. Vehicles are assumed to be cooperative and relay packets to others, but malicious nodes may not comply with this protocol.

VANET supports two types of applications—event-driven and cooperative awareness applications. In event-driven

applications, nodes send messages about the occurrence of certain events, such as, warning about dangerous road conditions or post-crash warnings. Cooperative awareness applications determine a dangerous situation based upon messages received from neighboring nodes. These applications are also called position related applications as they are dependent on accurate position information. Examples of these applications include traffic condition reports, collision avoidance, emergency alert and cooperative driving. If position information is incorrect, these applications may not work as expected.

A malicious node creates multiple virtual identities and associates forged positions with them. It sends wrong messages using these identities and positions, thereby creating an illusion of a non-existent event. Malicious nodes could harm VANET applications by causing misbehavior [1, 5] such as:

- Drop packets: An attacker may drop all the warning packets during an accident.
- Insert fake information or modify existing packets: An attacker may create an illusion of a traffic jam before selecting an alternate route to his advantage.
- Replay packets: An attacker may pretend to be at a fake position to create the illusion of an actual vehicle.

A collision warning message application is shown in Fig. 1. Whenever a vehicle detects any relevant event (e.g. car accident, traffic jam, emergency braking etc.), it broadcasts a warning message to nearby vehicles to inform the drivers.

A malicious vehicle can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions. For example, a malicious node can misuse safety related applications to clear the path for an aggressive driver by convincing other vehicles to slow down or speed up on the road. The malicious vehicle forges its ID (in some cases, it creates multiple virtual identities) and position information for its non-detection.

An attacker may decrease VANET performance by manipulating VANET topology. A safety message contains basic information such as sender-ID, time, position, speed and warning message as shown in Fig. 2. Beacon packets are broadcast periodically in VANET. The difference between beacon packets and safety packets is that the warning field is absent in the former.

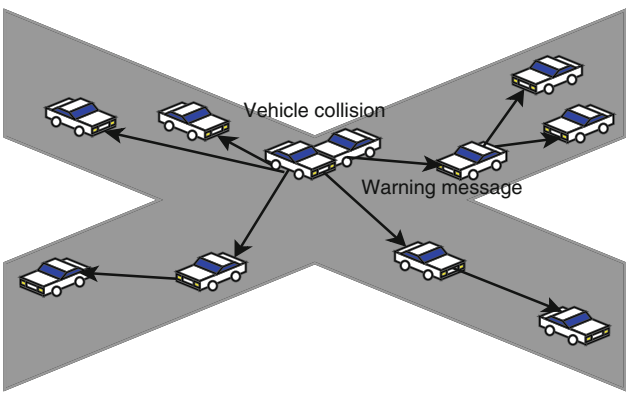

Fig. 1 An example of collision warning message in VANET

In VANET, it is assumed that each entity (RSU and OBU) is bound to a unique ID. Also, each entity is bounded by position i.e two entities can not be at the same position at any time instant. Safety packets (see Fig. 2) include position and timestamp of the last relaying node along with the originating node's position and timestamp. Safety packets may need to propagate across multiple hops. In this paper, the term node is used for vehicles as well as for RSUs. A received safety message is discarded if the difference between its timestamp and the receiver timestamp is larger than the sum of propagation and processing delays for one hop transmission. Moreover, a message is discarded by the receiver if the coordinates of the sender are outside its maximum wireless communication range. This validation is applied on a per-hop manner only. These condition checks are known as plausibility validation checks.

Since the sender ID and position play a special role in any traffic safety message, they require more attention. An attacker node can forge this information for launching attacks in the network. This information serves as the basis for attack detection also. For example, if a node broadcasts packets from random positions with uncoordinated time, it can be detected competently.

Specifically, the contributions of our paper are:

- Modeling and simulation of different forms of position forging attacks.
- Design, simulation and evaluation of detection approaches for these attacks.
- Analysis and comparison of these detection approaches.

We discuss in detail the various position forging attacks in VANET and attacker behaviors that pose high risks to the system. To the best of our knowledge, we are the first to address the modeling of different forms of position forging attacks in VANET. We also propose the detection mechanisms for these attacks. In general, a driver's behavior depends on the traffic warning messages that it receives. Vehicles that receive incorrect traffic information change their behavior accordingly. Previous detection approaches estimate the position of sender using RSS values of received beacon packets. On the other hand, our proposed approach checks for inconsistency of position information

Sender–ID	Timestamp	Position	Speed	Warning

Fig. 2 Safety message format

in consecutive beacon packets in order to detect position forging attacks. We measure the speed inconsistency and thereby vehicle presence time in RSU range in order to detect position forging attacks using single ID. Position forging attack with multiple fake identities (combination of ID and position forging attack) is detected by measuring the similarity in neighborhood information of nodes within the vicinity of attacker (that has created fake identities)

To present our contributions, the rest of the paper is organized as follows. Section 2 discusses related work of several attacks on inter-vehicle communication system and their detection approaches. Section 3 describes VANET model and vulnerabilities in VANET. Various forms of position forging attacks are presented in Sect. 4. In Sect. 5, we discuss impact of position forging attacks on VANET performance. Sections 6, 7 and 8 describe the detection methods for these attacks. Section 9 presents capabilities and limitations of our position forging detection mechanisms. Finally, Section 10 concludes the paper.

2 Related work

Aijaz et al. [1] present various types of attacks on an inter-vehicle communication system. They analyze how an attacker can manipulate the input of an OBU and sensor readings. The authors propose plausibility checks using constant system examinations.

Raya and Leinmuller [2, 6] discuss a number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and security problems. For example, malicious vehicles can convince other vehicles to slow down or speed up on the road for their own benefit. However, the authors do not analyze implementation issues and solutions to address such security threats.

Security research on position based attack in VANET is still in its infancy. Position verification is the only method to detect position based attacks in VANET. Most of the security solutions on position security are designed for position-based routing [7, 8]. A framework to detect nodes cheating their position in greedy perimeter stateless routing is presented in [9]. They estimate the claimed position of nodes by assuming different number of sensors. These sensors work autonomously on every node or require cooperation among neighboring nodes. Consistency of position data is inspected and verified by change in movement and density of vehicles [10]. This verification process is based upon the trust value generated by neighboring vehicles. They also perform map based verification. They show that cooperative sensors efficiently detect position faking nodes in a scenario where attacker passes all autonomous sensor based verifications such as acceptance and mobility range checks. However, position verification using cooperative sensors leads to communication overhead and increase in false positive rate (FPR). Whereas, our proposed approach uses the features of VANET i.e. presence of RSUs at certain locations and traffic pattern of vehicles (movement of vehicles on the road only). In our proposed approach, each beacon packet with incorrect position information is not discarded as it may lead to computational overhead. In some cases, where an attacker sends the message with fake position for short duration of time, it would not adversely effect the performance of VANET applications. In addition to it, we also have designed an approach to detect combination of position and ID forging attacks.

Sastry et al. [11] propose an approach based on the verification of a node residing within a defined region. This solution uses the functionality of special nodes at specific locations and defines an acceptable distance for each verifier. In this approach, whenever a node n sends a beacon packet containing its position, verifier sends a *challenge* via radio device. After receiving the *challenge*, the node n has to answer via ultrasound. If the answer reaches at verifier in the previously calculated time, n is approved to be within the region. This approach is not appropriate for highly mobile networks such as VANETs.

Vora et al. [12] present a position verification scheme based on logic reception of beacon packets. In this approach, verifier nodes are divided in acceptors and rejectors. The acceptor nodes are distributed over the region which is to be verified. Acceptor nodes are covered with the rejector nodes in the form of ring. If a node `n` sends a beacon packet, verifier receiving the packet decides whether the position of the beacon packet is acceptable. If the beacon packet is first received by a rejector, it signifies that node n does not reside within the region.

Yan et al. [13] have proposed a position verification approach by assuming that GPS device and radar is installed on each node. GPS position claimed by neighboring nodes (via beacon packets) is matched with the estimated position by radar at receiver end. In this way, local security i.e. position security of vehicles within the vicinity is obtained. System security is achieved by extending the local security through remote position verification. They also address three security aspects of position security in VANET [14]. Position information availability is enhanced by selecting stable routing paths in geographic routing protocols. They also preserve position confidentiality by encryption/decryption and access control mechanisms.

Hubaux et al. [15] propose verifiable multilateration approach for position verification. In this approach, four base stations are involved. Each base station measures the time between sending the `test` packet and arrival of `reply` packet. A malicious node might introduce some delay while sending the `reply` packet. This delay can be discovered using multilateration during measurements of four distance w.r.t. four base stations. This approach can

become efficient by using synchronization among base stations. The only problem with this approach is the uniform placement of four base stations in VANET scenario. High mobility of vehicles is also a serious issue in proper implementation of this approach in VANET.

Hesiri et al. [16] propose a position and velocity verification scheme for one hop neighbors. They simulate the proposed scheme in various vehicular mobility environments including rural, urban and manhattan. They evaluate the proposed scheme for both position and velocity verifications with automotive grade differential global positioning system (GPS). They introduce the errors in position and speed intentionally and evaluate results for rural, urban and Manhattan scenarios.

Golle et al. [17] propose an approach for detecting and correcting malicious data in VANET. In this approach, every vehicle builds a VANET model in which specific rules and statistical properties of VANET environment are implemented and stored. However, the authors have not presented and validated any experimental results. Their VANET model does not provide concrete means to detect misbehavior, detection is sketched through examples and computational aspects of the scheme are not investigated in detail. All in all, their VANET model is not flexible and is not able to switch to new network scenario.

Now we present the analysis of work related to ID spoofing attacks, since we have also implemented combination of ID and position spoofing attacks in this paper. In this attack, a malicious node spoofs the ID of other node (apart from using incorrect position) and use this ID to propagate wrong information in the network. Xiao et al. [18] illustrate a localized and distributed scheme to detect Sybil (ID spoofing) attack in VANETs. The approach takes advantage of VANET traffic patterns and road side base stations. They introduce a basic signal strength based position verification scheme. However, this scheme proves to be inaccurate for spoofing attacks. They have enhanced the accuracy of position verification approach by observing the signal strength distribution over a period of time.

Shaohe et al. [19] discuss a cooperative RSS based Sybil attack detection for static sensor networks, where all nodes (normal and malicious) have fixed transmission power. Each node overhears packets and computes the distance to other nodes using received signal strength. Each node creates a group of neighboring nodes using similarity of received signal strength (RSS) values and periodically broadcasts the group result. Identities with similar RSS values are then grouped into suspect group. A similar RSS based approach for Sybil attack detection in wireless sensor networks is also described by Demirbas et al. in [20].

An approach to detect Sybil attack in a static wireless sensor networks is proposed in [21] where information about neighboring nodes is used to detect Sybil attacks. However, it is not feasible to directly apply this scheme to detect attacks in VANET scenario because of its unique features such as high mobility of vehicles and frequent network fragmentation.

Bouassida et al. [22] use variations in received signal strength for detection of Sybil nodes in VANET. They successively measure the received signal strength variations to obtain an estimate of relative node localization. This localization gives an indication on the coherence of received signal strengths i.e. how much two nodes can be distinguished from each other. They assume that all the beacon messages are sent with the same signal strength which is not a realistic assumption.

In the approach discussed in [23, 24], RSUs are the only components that issue certificates to all vehicles passing across them. It is very rare to have two vehicles passing by multiple RSUs at exactly the same time due to the difference of moving dynamics of multiple vehicles. In this case, two messages will be treated as being issued from the same vehicle if they have a similar timestamp series issued by RSUs.

Mauro et al. [25] address node capture attack in mobile ad hoc networks (MANETs). They propose that mobile networks can leverage mobility and local cooperation to detect node capture attacks. They developed a protocol to increase the level of cooperation among nodes.

Nai-Wei et al. [26] present an Illusion attack in VANET. In this attack, a malicious node creates a particular traffic situation and sends fraud traffic warning messages to other nodes for convincing them that a traffic event has occurred. To detect and defend against such illusions, they introduce the plausibility validation network model in their paper. However, they have not implemented this attack and its defense approach in any simulator.

Roadside attacker behavior is discussed in detail by Leinmuller et al. in [27]. This paper provides an overview of various position forging attacks. They identify attacks for different VANET applications. They conclude that single position forging is the best choice for event-driven applications. From an attacker's point of view, forging of multiple vehicle movement path proves prominent for cooperative awareness applications. The authors have proposed solution [28, 29] to defend roadside attackers. They have used the feature "static position" of roadside attacker. Their approach is based on the constitution of trust relations for vehicles that have been neighbors for a certain time. Roadside attackers can not achieve certain trust level because of insufficient evidence of their movement pattern. We have implemented position forging attacks from a different perspective. We use the vehicles as attackers, whereas in their work, a roadside unit is considered as an attacker which is unrealistic in VANET environment. Additionally, we propose detection mechanisms for these attacks in our proposed work. Our

detection mechanism is based on the speed and presence time verification by RSUs for all the passing-by vehicles. We also measure the similarity in neighborhood information of nodes in the vicinity of fake nodes created by an attacker.

In our previous work, we have introduced variants of position forging attacks and their impact on VANET performance. Proposed work is an extended version of our [30] previous work.

3 VANET model and vulnerabilities

In this section, we discuss VANET components, the underlying communication system and vulnerabilities of a safety communication system.

3.1 System model

VANET consists of two basic components—RSU and OBU. A RSU is a stationary unit while OBUs are installed in vehicles, therefore these are mobile units. Each node in VANET consists of an event data recorder (EDR), GPS receiver, computing platform [15]. In proposed detection method, EDR is required to store the information of events received from nearby nodes. Computing platform is used for processing data and making decisions based on traffic messages received from neighboring nodes. There is a well defined hierarchy of central authorities (CA) responsible for managing vehicles identities registered in its respective geographic region. In our case, RSUs are assumed as lowest level CA that directly connects with vehicles on road. RSUs are connected with predecessor CAs using wired link. ID authentication infrastructure [15] such as electronic license plate is implemented for the whole network. V2V communication is used for disseminating safety and warning messages in the network. V2R communication is used to provide specific facilities, e.g. Internet access and special service request.

VANET can be modeled using graph notations. The graph $G = (V, E)$ consists of set of nodes in the Euclidean plane and a set of edges $E \subseteq \{V \times V\}$. Nodes represent vehicles or RSUs and edges represent communication links between the nodes. All vehicles are equipped with same wireless transceivers. An edge (v_i, v_j) exist between nodes v_i and v_j, if the Euclidean distance between nodes v_i and v_j is less than or equal to their transmission range.

$$E = \{(v_i, v_j) \mid (POS_i - POS_j) \leq TR\}$$

where POS_i and POS_j are the X–Y positions of nodes i and j and TR is transmission range of the node. This equation results in an undirected graph that may be connected or disconnected depending upon the distance between nodes.

$$(POS_i - POS_j) = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}$$

If the distance between two vehicles is more than TR i.e. at multi-hop distance, they exchange messages through intermediate vehicles.

We consider a widely used radio propagation model—`shadowing model` [31] using signal attenuation. It considers the multipath propagation effects of the real world communication system and may depict physical scenario better than 'Two-ray ground reflection' and 'free space model'. The exact value of signal attenuation is not known and receiver can not calculate the distance from sender accurately. Shadowing model is comprised of two parts:

- *Path loss model* this uses d_0 as a reference position and d is the position where the signal strength is measured, i.e. position of RSU. Received power $P_r(d)$ is calculated relative to $P_r(d_0)$.

$$\frac{P_r(d)}{P_r(d_0)} = \left(\frac{d}{d_0}\right)^{\beta}$$

- *Relation of received power and distance* this part considers the deviations of received power at a certain distance. It is a `log` normal random variable i.e measured in decibels (dB) of Gaussian distribution. The complete shadowing model is represented as:

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{dB} = -10\beta log\left(\frac{d}{d_0}\right) + X_{dB}$$

where d_0 is a reference position. In our case, the reference position is the position of RSU involved in the detection process. X_{dB} is a Gaussian random variable with zero mean and standard deviation σ S_{dB}. Path-loss exponent ($\beta = 2$ for free space propagation). We have taken $\beta = 5$ to model presence of vehicles and buildings that shall result in faster decrease of average received power as a distance becomes larger.

3.2 IEEE 802.11p protocol

IEEE 802.11p [32] is an amendment of 802.11a standard, specifically for wireless access in vehicular environments. It is used to improve the performance of CSMA/CA based networks in vehicular environments. It defines enhancements to 802.11a that are required to support intelligent transportation system (ITS) applications. It also uses MAC amendment 802.11e for QoS support. It allows data exchange between high speed vehicles and also between vehicles and RSUs in the licensed ITS band of 5.9 GHz (5.85–5.925 GHz). It deals with data link and physical layers of the OSI model. It is used as the groundwork for dedicated short range communications (DSRC), a U.S.

Department of Transportation project based on the ISO Communications. Vehicle-based communication network is used in applications such as toll collection, vehicle safety services and commerce transactions via vehicles.

DSRC protocol provides transmission ranges of 250–1000 m, with data rates in 6–27 Mbps range in VANET. In an 802.11p network, synchronization depends on global time reference, such as coordinated universal time. This can be provided by a global navigation satellite systems such as GPS or Galileo.

3.3 Vulnerabilities

In VANET, each vehicle publicly receives available safety messages. VANET safety communication system differs from the usual approach in information systems that restrict access. VANET vulnerabilities originate from its open nature explained as follows:

- Openness of wireless communication channel: Each node is free to access the communication channel. It is not protected against any physical disturbance.
- Unencrypted exchange of information: As safety messages are meant for all the nodes in VANET, these are sent in plaintext form. It is ensured that everyone understand the safety message broadcast in VANET. Likewise, each node is free to send messages with any content.

4 Position forging attacks

In this section, we discuss various forms of position forging attacks. The attacker may use one or multiple IDs to launch an attack while modifying its positions or fabricating a new position to give illusion of presence of a different vehicle, the attacker has to ensure that attack is not detected. The attacker attempts to forge positions derived from its own and/or its neighboring nodes' position. An attacker can also use positions of multiple nodes at different time intervals. Digital maps provide another method of deriving node positions. An attacker can select any arbitrary position on the road. In all forms of position forging attacks, the attacker uses positions on the road to evade attack detection process.

Due to the shared nature of wireless medium, malicious nodes can collect ID information through passive overhearing and utilize the ID information to launch ID based spoofing attacks in VANET. An ID forging attack is an impersonation or spoofing attack where an attacker illegitimately fabricates multiple identities or spoofs the identities of other nodes and hence, creates an illusion of multiple nodes. All the fake identities created by an attacker simultaneously participate in the network [33, 34] in order to disrupt the VANET applications. ID based spoofing attack is a serious attack in VANET because it can promote a series of traffic injection attacks.

If an attacker implements a combination of ID and position forging attacks, multiple virtual identities are created for position forging. It makes other vehicles believe that there are more nodes in the network than the actual count. This gives the impression of a state of congestion and may lead to all vehicles slowing down their speed, thereby leading to real congestion.

4.1 Forging random positions using single ID (FRPSI)

In this position forging attack, an attacker creates one virtual ID for sending any message. The attacker uses this virtual node for sending the same safety message but using random positions. It is the simplest form of position forging attack in VANET. The attacker broadcasts same fake message of a non-existent event in the network from a sequence of arbitrary positions.

This attack is shown in Fig. 3. Numbers *1,2,…,5* represent time instances at which an attacker node *M* pretends to be *M′* and broadcast messages using forged positions. Node positions connected with solid lines represent the actual path movement at different time intervals. Node positions connected with dotted lines represent the sequence of forged positions used by attacker. This notation shall be used for all forms of position forging attacks. There are two variants of this attack.

- Case 1. The attacker forges an event by broadcasting a fake message, using position information within its vicinity, as shown in Fig. 3. The broadcast position is within the range of attacker's actual position.
- Case 2. Attacker may use positions outside its vicinity but within the road boundary for forging an event, as shown in Fig. 4.

In this attack, there may be inconsistency in subsequent positions used by attacker. These attacks are easy to detect as observers can infer the same ID broadcasting a message

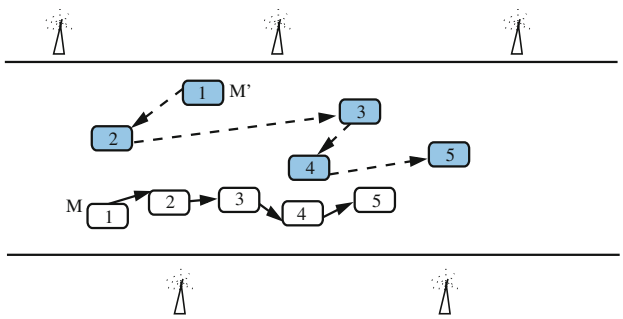

Fig. 3 Sequence of forged positions used by a an attacker node *M* pretending as node *M′*

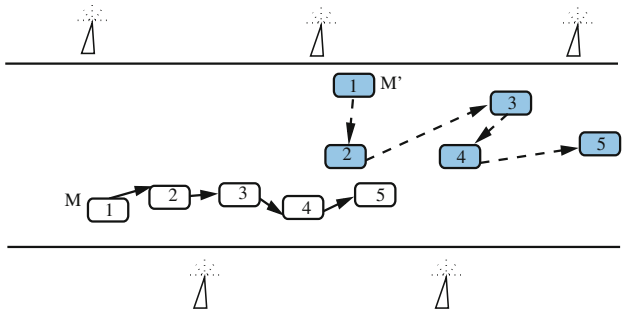

Fig. 4 Sequence of forged positions (outside the vicinity of an attacker node *M*) by using ID *M′*

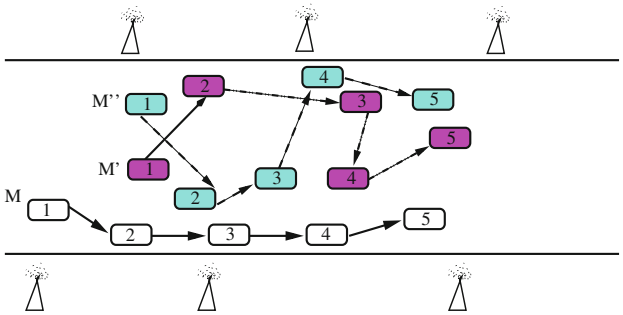

Fig. 5 Attacker M broadcast message by using random sequence of positions and two different identities *M′* and *M″*

from random positions. This leads to inconsistency in positions of subsequent packets.

4.2 Forging random positions using multiple IDs (FRPMI)

An attacker broadcasts fake messages using multiple fake identities from random positions at any instant of time. An attacker creates an illusion of some warning or safety event by spoofing the identities of other nodes or fabricating identities and then using these simultaneously in the network. The attacker associates random positions with each fabricated node at different time intervals. This attack can be launched easily. However, the major concern is choosing the appropriate IDs and node positions. The attacker needs to consider that no two fabricated nodes broadcast the same position at any time. Attacker's effort is proportional to the number of identities used by it. A sample random position forging attack using two IDs is shown in Fig. 5.

4.3 Forging path using single ID (FPSI)

In a path-forging attack, the attacker creates one virtual ID to broadcast fake messages using a consistent sequence of forged positions. This attack is intelligent and difficult to detect. The attacker wants to create an illusion that the node is moving normally on a pre-defined path. A sample for this attack is shown in Fig. 6. This attack is considered successful when the traffic situation does not change. Inconsistent movement paths may be detected based on changes in traffic patterns.

While forging a position, the attacker tries to keep a forged position within its communication range, to make the detection process difficult. All nodes within the transmission range of attacker consider it to be a genuine node.

4.4 Forging path using multiple IDs (FPMI)

In this attack, an attacker creates multiple virtual identities that participate simultaneously in the network, with a

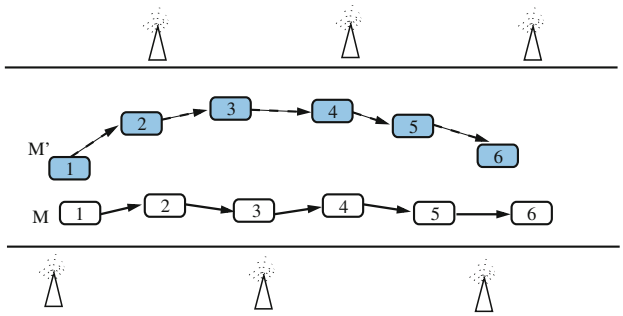

Fig. 6 Sequence of positions on one forged path by an attacker *M* pretending as *M′*

sequence of positions on the pre-defined path. Simultaneous multiple path forging attacks are carried out in this case. The attacker takes care that same positions are not used by more than one node at any time. This attack is shown in Fig. 7. The effort required to implement this attack increases linearly with the number of paths to be forged. The attacker forges the whole traffic situation by simulating positions and movement of other vehicles.

This type of attacker possesses the highest possibility of clearing position and speed consistency checks, as it is very careful about the construction of forged paths. Also, all the forged paths may not be detected at the same time.

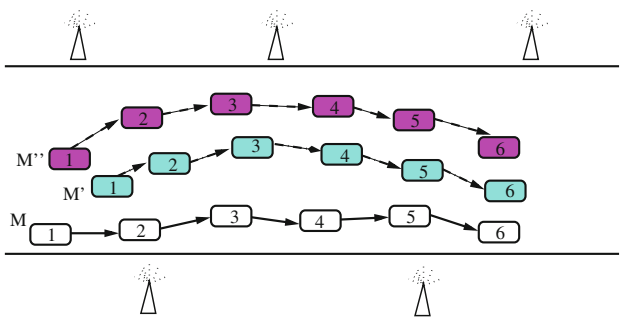

Fig. 7 Two forged paths using two IDs *M′* and *M″*

5 Impact of position forging attacks on VANET performance

In this section, we discuss the attacker model, the underlying experimental setup and impact of position forging attacks on VANET performance.

5.1 Attacker model for position forging attacks

Various position forging attacks are implemented according to the position forging behavior deployed. Attacker model for various position forging attacks is provided in Algorithm 1.

Algorithm 1 Attacker model for position forging attacks

V = Set of vehicles
A = Set of attackers and $A < V$
$N_{virtual}$ = Number of virtual identities created by attacker
$POS_{(X,Y)}$ = Set of valid (X, Y) positions on all road segments
$POS_{k,t} = (X, Y)$ position of k^{th} vehicle at time t
T_{range} = Transmission range of attacker
POS_{rand} = Random position in T_{range}
$Attacker_i = i^{th}$ attacker, $i \in \{1, \cdots, A\}$
Δ = A set of virtual nodes associated with all attackers
t_s = Start time of attack
t_f = End time of attack
for $i = 1$ to A do
  for $k = 1$ to Δ do
    Assign identity from set $N_{virtual}$
    $POS_{rand} \in POS_{(X,Y)}$
    if FRPSI | FRPMI then
      $POS_{rand} \in POS_{(X,Y)}$
      $POS_{k,t_s} = POS_{rand}$
    else
      repeat
        η = neighbour(k)
        $POS_{k,t_s} = POS_{\eta,t_s} \pm \epsilon$
      until $POS_{k,t_s} \notin POS_{(X,Y)}$
    end if
  end for
end for
for $i = 1$ to A do
  for $t_0 = t_s$ to t_f do
    for $k = 1$ to Δ do
      POS_{k,t_0} as per attack mode
      $PATH_k = \{POS_{k,t_s}, \cdots, POS_{k,t_f}\}$
    end for
  end for
end for

In a FRPSI attack, $N_{virtual}$ equals one and *PATH* contains random positions on the road structure. All considered positions are according to the format of two-dimensional coordinate system.

In a FRPMI attack, the value of $N_{virtual}$ is greater than one and multiple *PATH*s are associated with these virtual identities containing random positions. Hence, the number of *PATH* required and $N_{virtual}$ are same. The attacker considers all road boundaries in the simulation area while using any random position.

In a FPSI attack (path forging with single ID), $N_{virtual}$ equals one and *PATH* contains only one sequence of positions derived by knowing its own and neighboring node's positions for sending a beacon packet. In a FPMI attack (path forging with multiple IDs), multiple identities are associated with an attacker. The value of $N_{virtual}$ is greater than one and each ID simultaneously performs path forging with an additional constraint that no two virtual identities are at the same position at any given time interval.

Apart from forging positions, the attacker node may block the packet forwarding process, a usual norm in VANET. Each honest node forwards the received safety message to its neighboring nodes, whereas, a malicious node captures these messages to send its own messages with different identities. The BLOCK FORWARDING PROCESS is defined in Algorithm 2.

Algorithm 2 Attacker node block the forwarding process

V = Set of vehicles
A = Set of attackers
P = Set of received packets
$L = V - A$, Set of legitimate vehicles
$FORWARD(P)$: Function for forwarding the packets
$BLOCK(P)$: Function for blocking the packets
for $i = 1$ to V do
  for $j = 1$ to P do
    if $i \in A$ then
      $BLOCK(P)$
    else
      $FORWARD(P)$
    end if
  end for
end for

5.2 Experimental setup

To evaluate various position forging attacks, we implement them in NCTUns-5.0 simulator [35]. This simulator supports various parameters including topology (road network), communication and network protocol, vehicular traffic, feedback loop and propagation models.

In our experiments, we simulate a two-directional 10 km long highway with multi-lanes in each direction. The average speed range of vehicles is set between 30 and 150 km/h, number of nodes is 150 and the transmission range is 250 m. Each simulation case has a variable number of position forging attackers, as well as a variable number of identities used by these attackers. The duration of each simulation is 1,000 s and each simulation is repeated 10–15 times with a different seed to achieve a higher confidence level. The simulation results shown in graphs are calculated by averaging the results of individual experiments. We use the 802.11p wireless communication protocol in our simulation scenario. In our simulation we do not model GPS anaccuracies primarily because there is no inbuilt support of GPS in NCTUns-5.0.

5.3 Performance evaluation metrics

The simulation results are evaluated using the following parameters :

- Number of packet collisions: The hidden terminal problem is the main cause of collisions in a wireless network. Broadcast messages can not use the request to send/clear to send exchange because it floods the network with traffic. If multiple nodes transmit at the same time, a collision occurs on this shared communication channel. We count the number of such collisions in our network scenario. In presence of attack, owing to participation of virtual identities should increase number of collisions as well.
- Average vehicle speed: We calculate the average speed of all vehicles involved in the simulation. The impact of variable number of position forging attackers on the average speed of all vehicles is determined.
- Packets delivered: It is defined as ratio of the packets received to packets transmitted in the network. We measure the percentage of delivered packets.

We consider “congestion avoidance application” in order to evaluate the impact of these position forging attacks on VANET performance. Whenever a vehicle observes an accident on the road, it broadcasts this warning message to all the vehicles in its vicinity. Therefore no explicit knowledge of underlying routing protocol is required to implement congestion avoidance application.

5.4 Impact of position forging attacks

We evaluate the difference between two cases of position forging attackers in terms of percentage of delivered packets. In the first case, position forging attackers, broadcast fake packets with forged positions. In the second case, a position forging attacker blocks the forwarding process. The difference between these two types of attackers in terms of percentage of delivered packets is shown in Fig. 8.

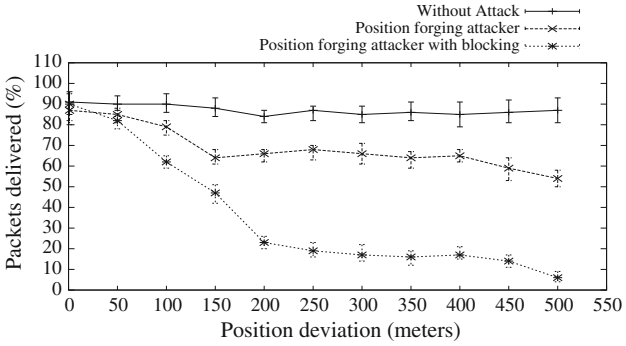

Fig. 8 Impact of position forging attacker on percentage of delivered packets

The percentage of delivered packets is measured w.r.t. position deviation, is the difference between the actual and forged position of an attacker for broadcasting packets. It is observed that there is a reduction of up to 50 % in delivered packets in case the position forging attacker blocks the forwarding process, as compared to a basic form of position forging attack. We observe greater reduction in delivered packets in cases where the position deviation is more than 250 m. This is because the communication range is 250 m in our case. Therefore, our approach do not consider the packets received from nodes outside the reception range (250 m).

If there is no attacker in our simulation environment, we observe that the number of packet collisions are approximately 5 %. Figure 9a shows the impact of random position forging attack (with a variable number of identities used by these attackers) on the number of packet collisions in our scenario. As the number of attackers increases, the number of packet collisions increases proportionally. This is because of the fact that virtual identities generated by attacker has to participate in the network simultaneously to broadcast beacon packets in the network. Therefore, the total number of packets generated in the network increases. The same communication channel is shared among all nodes, resulting in an increase in number of packet collisions. Similar results are observed for path forging attackers in Fig. 9b.

From Fig. 9, we observe that the percentage of packet collision increases as the number of identities spoofed by the attacker increases. We also observe that collisions do not increase proportionally when the number of identities spoofed by attacker is greater than two. It’s possible that same set of IDs are used from the list of available virtual ID pool. It is observed that in case of 500 m communication range, approximately 80 % packets are collided which

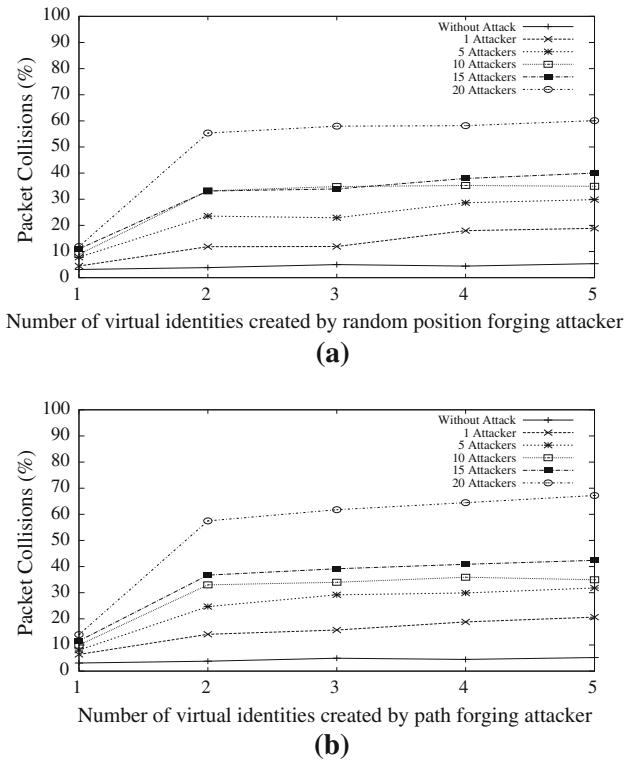

Fig. 9 Impact of random position forging and path forging attacker on number of packet collisions. **a** Impact of random position forging attacker on number of packet collisions, **b** impact of path forging attacker on number of packet collisions

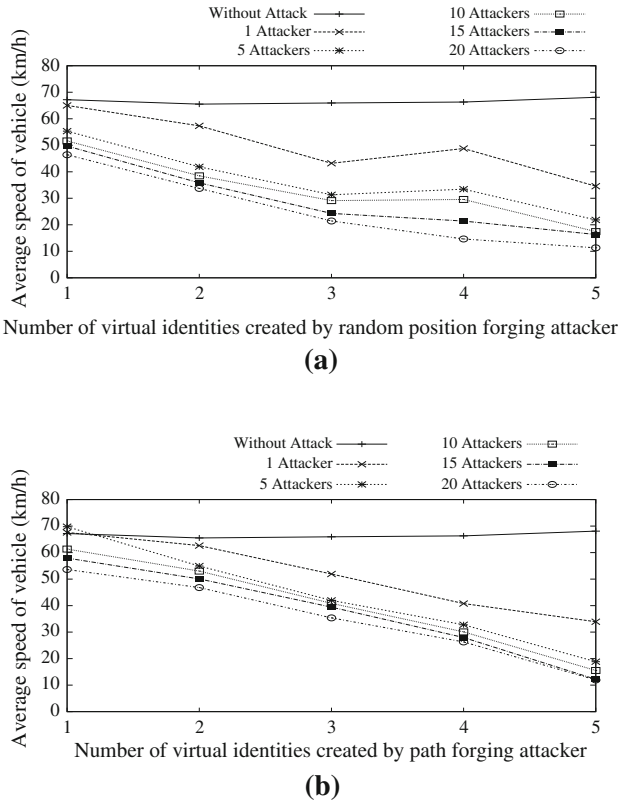

Fig. 10 Impact of random position forging and path forging attacker on average speed of vehicles. **a** Impact of random position forging attacker on average speed of vehicles, **b** impact of path forging attacker on average speed of vehicles

is quite higher as compared to 250 m communication range.

It is observed that the number of packet collisions is approximately same for random position forging attacker and path forging attacker. This is because the same number of identities are used by attackers in both cases.

Figure 10a illustrates the impact of random position forging attackers on average vehicle speed in VANET. A larger number of attackers decreases the average vehicle speed. All nodes, receiving the same message from a significantly large number of nodes, slow down their speed due to the illusion of a congestion on a nearby road.

In Fig. 10b, the average vehicle speed is evaluated based on different number of path forging attackers. These attackers broadcast the same packet using a consistent sequence of positions in such a way that receivers consider it a genuine message. Due to this typical nature of the attacker, it leads to an illusion of increased number of vehicles around receiving nodes, as compared to the scenario that involves random position forging attackers. It decreases the average speed of vehicles to 20 km/h which can cause real congestion.

The difference in reduction of average vehicle speed between graphs 10a and b is due to the nature of attacker broadcasting the beacon packets periodically. Path forging attack attempts to present a consistent path to evade detection. So speed changes are abrupt as may not be in random position forging. So average speed in random position forging is less as compared to random position forging attack.

6 Proposed detection methodology for FRPSI attack

This detection approach is based on acceptance range and speed verification. It is applicable for detection of FRPSI attacks, where an attacker forges random positions using a single ID. In this case, inconsistency in position and speed (broadcast in consecutive beacon packets) helps in detecting the attack. Proposed approach is based on the assumption that RSUs are deployed in the network. The solution does not require the presence of multiple RSUs within the range of vehicle. At a given time a vehicle is required to be in range of atleast one RSU. In a transmission range of r, distance between two RSUs cannot exceed $2r$. Each RSU stores beacon packets received from passing vehicles for a significant period of time and periodically exchanges this information with other RSUs. It performs the following two verifications for validating the existence of a misbehaving vehicle.

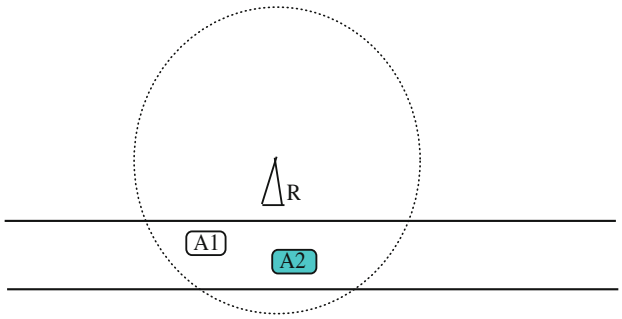

Fig. 11 A1 is actual position of node A and A2 is its forged position. Acceptance range of RSU R is same for this node at two positions

- Acceptance range verification: This is done by checking that receiver position P_r is within acceptance range (AR) of sender position P_s.

  $$| P_r - P_s | \leq AR$$

  All messages received from nodes, that claim to be at a distance larger than AR are ignored. In our experiments, we consider two cases: $AR = 250$ m and $AR = 500$ m. If the forged position is within the acceptance range of receivers, this verification method validates the received message and it is not discarded as shown in Fig. 11.
- Speed verification: For the attack scenario, where an attacker forges the position within the boundary of acceptance range of RSU, acceptance range verification shall always pass. So speed verification is required. Each RSU calculates the speed of passing-by vehicles depending upon the position information broadcast in subsequent packets of these vehicles using following equation.

  $$V_s = \frac{\sqrt{(X_{t_{i+1}} - X_{t_i})^2 + (Y_{t_{i+1}} - Y_{t_i})^2}}{t_{i+1} - t_i}$$

  Here, we consider a two-dimensional coordinate system. X_{t_i+1} and X_{t_i} are the X-positions of a node at time interval t_{i+1} and t_i respectively. Similar notations are used for Y-positions. V_s refers to the vehicle speed. Speed of a vehicle should be within the limits defined by road authorities. Speed verification is done using the following equation.

  $$V_s \geq 0$$
  $$V_s \leq V_{max} + \Delta$$

  V_{max} is the maximum speed allowed on the road. Δ is the speed tolerance error. If the calculated speed exceeds V_{max}, the node is considered as suspicious and put under scrutiny.

The verification methods defined above are integrated for detection of FRPSI attack. If there is an inconsistency in position and speed of consecutive beacon packets received from a vehicle, it is suspected as malicious. It is assumed that RSUs perform the consistency checks and RSU being more resourceful, computation time required is reduced. All RSUs exchange their observations periodically. If an inconsistency is measured by more than one RSU for an extended time duration, messages received from suspected vehicles are discarded. Consider an example consisting of three vehicles (V_1, V_2, $V3$), Table 1 depicts position and speed consistency verification for these three vehicles at different time intervals. In this table, duration of time interval is taken as 1 min. However, in simulation, duration of each time interval is 1 second. This verification is performed by each RSU in VANET.

Here, we define a threshold γ to discriminate speed change as rapid or gradual. The value of γ is chosen as 10 km/h. If change in vehicle speed at two consecutive time intervals is greater than γ, it signifies the rapid change in speed, otherwise speed change is gradual.

$$\text{if}(V_s^{t_n} - V_s^{t_{n+1}}) > \gamma$$

Rapid change in speed

else

Gradual change in speed

In this Table, Vehicle V2 shows rapid change in positions and calculated speed as change in speed from 94 to

Table 1 An example of position and speed consistency check performed by a RSU

Vehicle-ID		t_0	t_1	t_2	t_3	t_4
V1	X–Y position	(951, 720)	(1897, 786)	(2809, 786)	(3795, 812)	(4698, 845)
	Speed (km/h)	54	57	55	59	54
V2	X–Y position	(846, 678)	(2419, 712)	(426, 5112)	(3075, 2134)	(2131, 789)
	Speed (km/h)	70	94	289	239	98
V3	X–Y position	(811, 768)	(2194, 794)	(3643, 743)	(3732, 763)	(3676, 886)
	Speed (km/h)	78	83	87	79	88

V2 fails speed consistency check

Table 2 An example of time duration consistency measurement based on speed verification performed by each RSU

Time		*V*1	*V*2	*V*3
T_0	Speed (km/h)	50	65	39
	RSU-ID	1	2	4
T_1	Speed (km/h)	51	64	40
	RSU-ID	1	2	4
T_2	Speed (km/h)	50	64	45
	RSU-ID	1	2	5
T_3	Speed (km/h)	52	63	47
	RSU-ID	1	2	5
T_4	Speed (km/h)	51	65	45
	RSU-ID	3	2	7
T_5	Speed (km/h)	52	64	44
	RSU-ID	3	2	7

289 km/h is observed at the difference of one time interval. As evident from the table, other vehicles are showing a gradual change in positions and speed. This indicates the presence of a malicious node in the network.

6.1 Assumptions for detection

To implement our proposed approach for detection, we make the following assumptions.

- All nodes are equipped with same wireless communication equipment necessary for establishment of VANETs.
- Majority of vehicles (about 85 %) are honest.
- A road map is available with all RSUs and they are aware of valid road positions and their neighboring RSUs.
- RSUs are deployed in the network at regular intervals.
- All RSUs are trusted and their functionality is correct.
- RSUs have predefined communication between them and it does not create any overhead for proposed approach.

6.2 Simulation result of FRPSI attack detection approach

Experimental setup and simulation parameters are same as described in Sect. 5.2 We consider two transmission ranges—250 and 500 m. We use the following notations—(a) TR: transmission range and (b) O_T: observation period. These notations are used throughout this paper. TR is the transmission range of sender and O_T is the length of maximum consecutive time intervals for which RSU make a record of passing by vehicles and after O_T. RSUs exchange their observations with neighboring RSUs. The simulation results are evaluated using metrics like detection rate (*DR*) and *FPR*. These metrics are computed using true positive (*TP*), true negative (*TN*), false positive (*FP*) and false negative (*FN*). *TP* indicates the number of correctly identified malicious nodes, *TN* is the number of correctly classified legitimate nodes, *FP* is the number of legitimate nodes incorrectly classified as malicious and *FN* is the number of malicious nodes classified as legitimate. The performance of any detection scheme is measured by checking its *DR* and *FPR*.

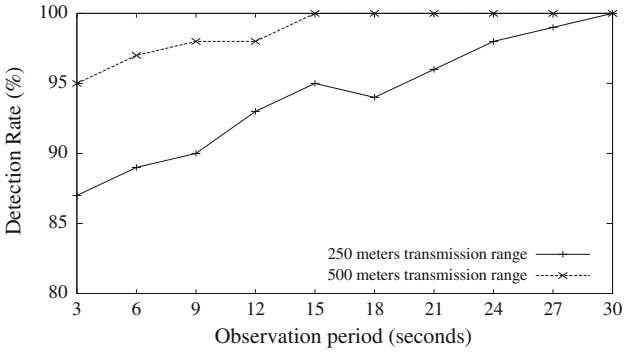

Fig. 12 Impact of observation time and transmission range on DR

- Detection rate (DR)

$$DR = \frac{TP}{TP + FN}$$

- False positive rate (FPR)

$$FPR = \frac{FP}{FP + TN}$$

These evaluation parameters are common for all detection techniques proposed in this paper. Figure 12 illustrates the impact of TR and O_T on DR of this approach. It is observed that O_T required for 100 % detection of attack in case of 250 and 500 m TR is 15 and 30 s respectively. More number of nodes can be observed by an observer RSU during the same time period with a 500 m TR as compared to 250 m TR.

Impact of TR and O_T on FPR can be seen in Fig. 13. High TR of nodes decreases the FPR and provides more accuracy. Longer O_T also helps in decreasing the number of FPs and provides more accuracy. These two factors are collectively used to derive accurate results of our proposed detection approach.

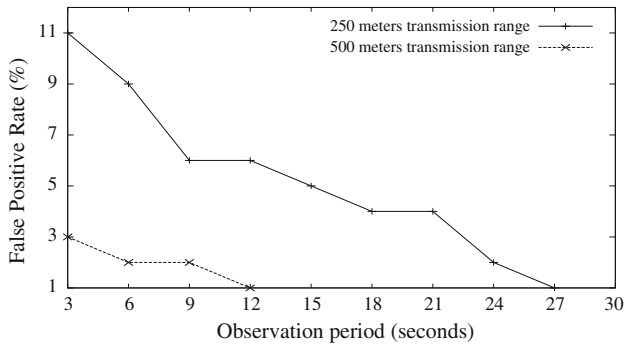

Fig. 13 Impact of observation time and transmission range on FPR

7 Proposed detection approach for FRPMI and FPMI attacks

This approach is lightweight as it does not use the support of RSUs to detect FRPMI and FPMI attacks, rather only neighboring vehicles are responsible for detection of attacks. Our proposed approach is suitable to detect a combination of ID and position forging attacks. In proposed approach, we exploit the basic features of ID spoofing attacker "using forged identities simultaneously" to differentiate malicious nodes from legitimate nodes. Proposed approach follows the basic assumption that two legitimate vehicles cannot have exactly same set of neighboring nodes for reasonably long duration of time except in the case of high vehicle density. All the fake identities created by FRPMI or FPMI attacker are bound to same physical device and share same set of neighboring nodes at same time instant. Experiment results show the effectiveness of proposed approach to locate the attack with different number of network parameters.

In proposed approach, each vehicle participates in detection by making a group of neighboring nodes at fixed intervals of time. Nodes with similar neighborhood are analyzed rather than the investigation of physical parameters of each node independently. All the nodes in vicinity (communication range) form a group of neighboring nodes by periodic exchange of beacon packets. As all the fake identities originated by an attacker node share the same physical device (malicious node), their neighbors share same set of communication neighbors depending upon the transmission power used by these fake identities to broadcast beacon packets. Proposed detection approach is able to determine all the fake identities launched by same malicious node. The basic requirement for detection of FRPMI and FPMI attacks is the presence of some neighboring nodes. This is a reasonable assumption as target of FRPMI and FPMI attacks is to influence the decision of neighboring nodes. If there are no neighbors of a node, attacker would fail to achieve its target. A basic procedure of detection approach using neighboring information is presented in Algorithm 3.

Algorithm 3 FRPMI and FPMI attacks detection using neighboring information

$\mathcal{V} = \{V_1, V_2 \cdots V_n\}$, Set of n vehicles on road
A = Set of Sybil attackers
T = Duration of simulation time
N_j^t = Neighbors of node V_j at t time interval
$Timer_n = 0$ // Time instance for measuring the duration of similarity in neighboring nodes
σ = Threshold (time duration during which normal nodes may have same set of neighbors)
$C_{j,k}^t$ = Set of common neighbors of node V_j and V_k at t time interval
M_j^t = Set of nodes V_j present in the minimum transmission range of fake node list
for $t = 1$ to T do
  for $j = 1$ to n do
    createNeighborList(N_j^t) // Communication neighbors
  end for
end for
for $t = 1$ to T do
  for $j = 1$ to n do
    for $t = j + 1$ to N_j^t do
      $C_{j,k}^t = N_j^t \cap N_k^t$
      if $C_{j,k}^t = \phi$ then
        Malicious node forges neighboring list
        break
      end if
      $M_j^t = M_j^t \cap C_{j,k}^t$
    end for
  end for
  $Timer_j = Timer_j + 1$
  for $j = 1$ to n do
    if $(Timer_j > \sigma)\&\&(M_j^t \neq \phi)$ then
      $M_j^t \in$ Malicious-group
      break
    else
      $M_j^t \in$ Legitimate-nodes
      continue
    end if
  end for
end for

7.1 Detection steps

Overall FRPMI and FPMI attacks detection approach includes four phases:

- Periodic exchange of beacon packets: In first phase, each vehicle V_j on the road periodically broadcasts and receives beacon messages from neighboring nodes. Beacon messages are broadcast by all the nodes in VANET to announce their presence as it is a usual norm of VANET. Though information of neighboring nodes can be collected by overhearing process, but we

use the fundamental characteristics of periodic communication of nodes in VANET. Each time, a node broadcasts beacon message, it attaches its neighbor list in the beacon packet. A beacon packet contains sender ID, its geographical position and time of sending the packet.

- Group construction of neighboring nodes: When a vehicle collects enough beacon messages from neighboring vehicles, it make a record of neighboring nodes N_i^t in the form of groups at regular intervals of time.
- Exchange groups with other nodes in vicinity: After significant duration of time (depending upon the density and speed of vehicles), these nodes exchange their neighboring nodes record with other nodes in vicinity.
- Identify the vehicles comprising similar neighboring nodes: After receiving the groups of neighboring nodes, each node V_j matches its neighbor table with the neighboring node V_k table $N_j^t \cap N_k^t$. If any two neighbors do not find any common neighbor, our algorithm assumes the forging of neighboring table by sender node. On the other hand, if it finds that some neighboring nodes have the same set of nodes in neighbor table for duration greater than threshold (σ), these nodes are put under malicious-group category. In this manner, proposed approach attempts to detect all the fake identities originated from an attacker.

7.2 Experimental setup and simulation results for proposed detection methodology

In this section, we discuss experimental setup and simulation results of proposed approach.

(1) Experimental setup: Vehicular traffic simulator [36] is used to evaluate the proposed detection approach. It contains 24 h car traffic trace file on the real road maps of Switzerland for 2,60,000 vehicles in an area of around 250 × 260 km^2. These traces describe the individual movement of cars through a queue-based model determined from real data. A multi-agent microscopic traffic simulator (MMTS) [36] is used to obtain these traces. This simulator is capable of simulating public and private traffic over real road maps of Switzerland with high level of realism. Mobility of vehicles is modeled by MMTS using the behavior of people living in the area within a period of 24 h. This trace file contains the position and speed of all the vehicles at discrete time interval of 1 s. We evaluate our detection approach using 10,000 nodes in 634 km road segment area obtained from these realistic traces.

(2) Simulation results: We derive a threshold value (σ) in realistic scenario for different transmission range of vehicles by performing series of experiments. σ is a maximum time period during which normal vehicles may stay together in the transmission range of each other, i.e able to correctly differentiate the legitimate and malicious nodes. Value of σ is 44 s for 250 m transmission range and 80 s for 500 m transmission range. We repeated our experiments by varying the value of σ. Use of proper threshold can improve the efficiency of proposed approach as well as reduce the probability of false detections, such as FPs and FNs.

Selecting a proper value of σ is an important issue of proposed approach to obtain high DR and acceptable error rate. Selection of σ is a trade off between DR and error rate. Improper value of σ would incur overheads on the network system. These overheads depend upon the specific VANET application. We have found that although smaller values of σ gives more accuracy in terms of *DR*, but it produces more *FPR*.

DR is evaluated for both the transmission ranges i.e. 250 and 500 m. Figure 14 is procured using 44 s threshold value for 250 m transmission range and 80 s threshold for 500 m transmission range. These figures also consider the variations in number of virtual identities bounded with attacker node. Figure 14 shows the DR of Sybil attack considering transmission range of 250 and 500 m. We also consider the different number of Sybil attackers and identities bounded with these attackers. Average DR is 94 %, as can be seen in Fig. 14b when the transmission range of vehicles is 250 m. DR increases in 500 m transmission range. 98 % detection accuracy is observed in this case. We also observe that DR increases with increase in number of virtual identities created by position forging attacker.

We have evaluated FPR to analyze the proposed approach. Figure 15 signifies the FPR percentage for 250 and 500 m transmission range. FPR rate for 500 m transmission range is quite less (refer Fig. 15b) as compared to 250 m transmission range as shown in Fig. 15a. The reason behind this output is the presence of more neighboring nodes in 500 m transmission range. It is also observed that FPR rate decreases with increase in number of virtual identities created by position forging attacker.

Our proposed approach can work perfectly with dynamic transmission range of vehicles. Artimy [37] has presented a dynamic transmission range assignment algorithm that procure variable transmission range based on the density, connectivity of vehicles and traffic conditions on the road. Proposed approach is able to detect FRPMI and FPMI attacks even if transmission range of fake nodes created by attacker is different. Our approach can easily comply with dynamic traffic scenario i.e. if the frequency

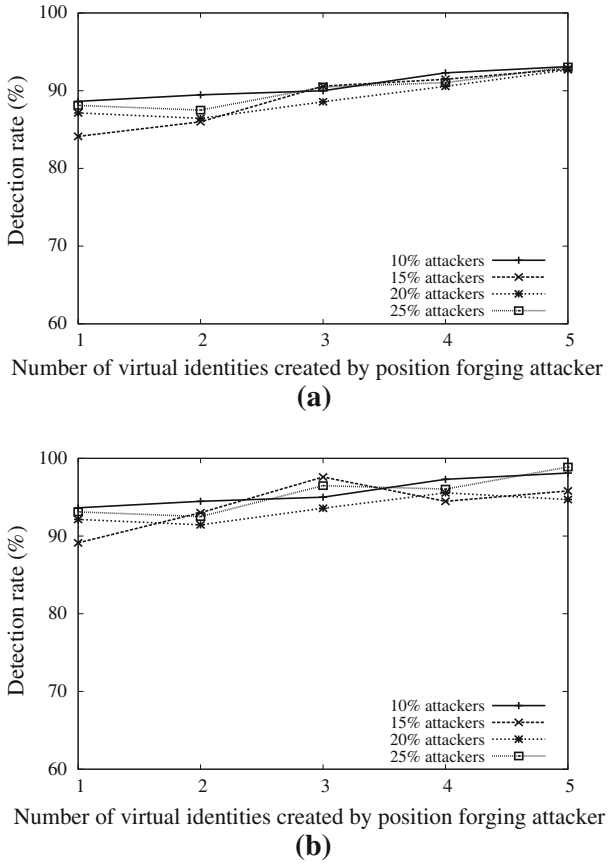

Fig. 14 Impact of number of FRPMI and FPMI attackers (with varying number of virtual identities) on percentage DR with transmission range of 250 and 500 m. **a** Impact of different number of FRPMI and FPMI attackers on DR with 250 m transmission range,**b** impact of different number of FRPMI and FPMI attackers on DR with 500 m transmission range

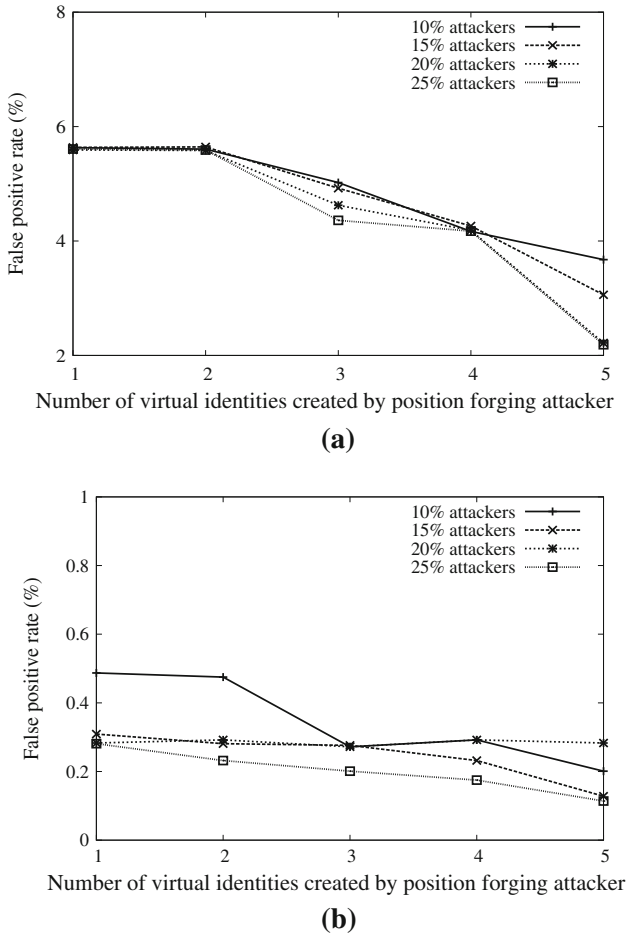

Fig. 15 Impact of number of FRPMI and FPMI attackers (with varying number of virtual identities) on percentage FPR with transmission range of 250 and 500 m. **a** Impact of different number of FRPMI and FPMI attackers on FPR with 250 m transmission range,**b** impact of different number of FRPMI and FPMI attackers on FPR with 500 m transmission range

of beacon packets is adjusted according to the environment conditions. As average number of neighboring nodes would increase with increased transmission power of sender, more computations would be required for computing the neighboring nodes. Our proposed approach is based on the similarity in neighboring nodes of all the nodes in vicinity for significant duration of time. There will not be any effect of modification in transmission range as well as updating the groups of neighboring nodes on detection accuracy of Sybil attack using proposed detection approach. In fixed transmission range, frequency of group formation of neighboring nodes depends upon the vehicle mobility. Number of groups formed, i.e. connectivity of vehicles is proportional to transmission range and speed of vehicles. An attacker may spoof transmitting power and while broadcasting the beacon packet, it increase/decrease the transmitting power. Groups of neighboring nodes vary dynamically depending upon the variations in transmission power of nodes, but it does not effect the performance of proposed approach. There would be some some neighbors which observe all the fake identities created by an attacker for longer period of time depending upon the dynamic transmission power of nodes.

8 Proposed detection methodology for FPSI attack

Like the detection methodology described for FRPSI attacks, FPSI attack detection approach uses acceptance range and speed verification. Another check (Time spent in a cell) is required for verification of time duration during which an attacker remains within the acceptance range of observer i.e. RSU.

Figure 16 illustrates the duration of time ($t_3 - t_0$) spent by vehicle V in the acceptance range of RSU. Time spent in a cell is dependent on the speed of vehicle passing across

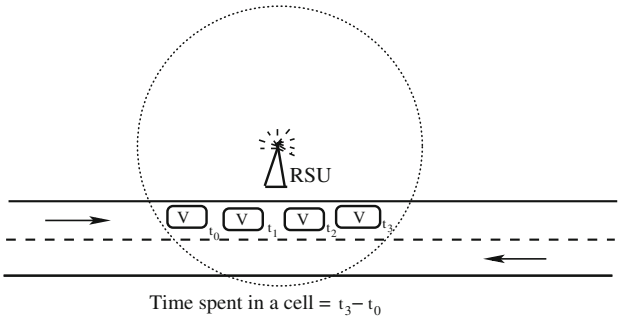

Fig. 16 Duration of time vehicle V stays within the acceptance range of RSU

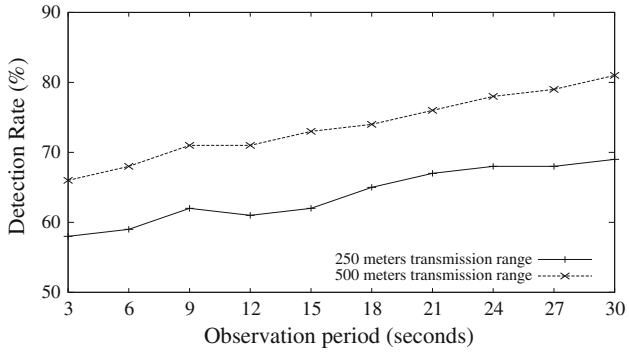

Fig. 17 Impact of observation time and transmission range on DR

the RSU. These three verifications are integrated for validation of such an attack.

We put the functionality of verification at RSU end only as they are assumed to be trusted and minimal computations are required to detect such attacks. It is assumed that each RSU knows the boundary positions of the road segment.

Also, each RSU is aware of the reception range within the road segment. If a RSU observes any inconsistency in calculated speed for consecutively received beacon packets from a passing by vehicle, this vehicle is put under scrutiny. All RSUs exchange their observations periodically. If an inconsistency is measured by multiple RSUs for a significant long period of time, these vehicles are identified as illegitimate. Messages sent by these vehicles would be discarded. In order to avoid redundancy, we are not describing the acceptance range and speed verification in this section (refer to Sect. 6).

8.1 Variants of FPSI attack

We consider three variants of FPSI attack as shown in Table 2.

- Type 1: This refers to the scenario where a vehicle proves itself to be mobile by sending beacon packets from consistent sequences of positions on road. If the observing RSU observes the existence of this vehicle in its communication range for a significantly long time period, this implies that either the vehicle is moving slowly or it is at a fixed position. Vehicle *V*2 in this table represents this form of path forging attack. In this case, the calculated speed from consecutive beacon packets from V2 shows its average speed 64km/h, but the vehicle stays it is staying in the acceptance range of observer for a long duration of time. In this example, the duration of time interval is 3 s and acceptance range of each observer is 500 m.
- Type 2: This refers to the scenario where FPSI attacker broadcasts beacons with positions of opposite direction than the actual direction of movement. As transmission power is limited, illusion of a virtual vehicle moving in opposite direction can be sustained only for limited time interval by attacker. Vehicle *V*3 represents this type of behavior in the Table I. In this case, the calculated average speed of *V*3 is 40 km/h. However, it crosses the observer RSUs very quickly. It implies the forged movement in a reverse direction when compared to its actual movement.
- Type 3: This refers to the scenario where an attacker forges positions near its real positions, such an attack has negligible impact on the VANET performance. Position verification is a suitable solution for detection of this form of attack. According to our survey, no solution is appropriate for accurate verification of positions.

8.2 Simulation results

The experimental setup and simulation parameters are same as described in Sects. 5.2 and 6.2. We consider two TR cases: 250 and 500 m. The relationship between O_T and DR based on TR is illustrated in Fig. 17. The graph depicts results for a scenario which involves 30 attackers out of 150 vehicles. Equal proportion of three variants of attackers i.e. 10 attackers of each case are used. Our approach shows a maximum DR of 81 % with O_T of 30 s for the 500 m TR case.

Impact of TR and O_T on FPR is depicted in Fig. 18. A FPR of 11 % is achieved using 30 s O_T for case where TR equals 500 m. This is due to the equal proportion of Type 3 attackers. The proposed method is not effective for detection of Type 3 attacks.

9 Discussion

In this section, we discuss the capabilities and limitations of proposed detection strategies for various forms of

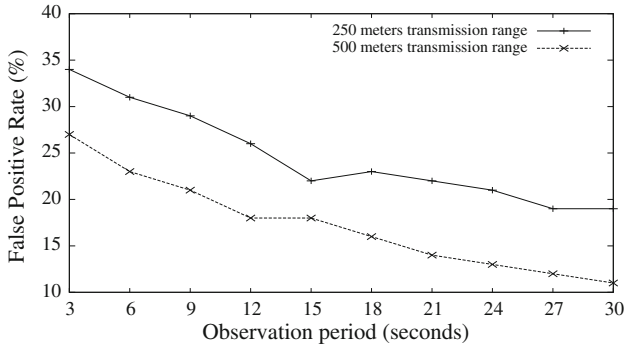

Fig. 18 Impact of observation time and transmission range on FPR

position forging attacks. FRPSI and FPSI attacks are position forging attacks and the other two attacks (FRPMI and FPMI) are a combination of position and ID forging attacks. The detection strategy for FRPSI attack is simple as it does not require any communication between the vehicles. It also works reliably for sparse networks and does not get affected by message loss. However, this detection approach is unable to detect an attack where a node broadcasts fake position that shows gradual change.

The detection method designed for FRPMI and FPMI attacks is same because attackers forge identities in addition to spoofing position. This method is based on similarity in neighboring nodes of neighbors of fake identities created by FRPSI and FPSI attacker. If this similarity is measured for a significantly long period of time, these nodes are considered as malicious nodes. This solution is lightweight and efficient as it is not dependent on position verification. This approach gives good results even in the case when an attacker is spoofing the transmitting power. Malicious nodes may increase/decrease RF (radio frequency) power. As attacker node could be interested in penetrating our detection system, so it can spoof power for broadcasting beacon packets. Decreasing power means that attacker is not able to spread impact of attack at intended position (range). Increasing power means that attacker can still be heard by its neighbors and detected. spoofed transmission power, therefore, does not affect our detection performance.

The FPSI attack detection approach is somewhat similar to the detection method for FRPSI attack with the exception of an extra check `Time spent in a cell` that is required for its detection. This detection approach is not suitable when actual and forged positions are close to each other for a reasonably long period of time. It shows good results when forged positions are in reverse direction as compared to actual positions. The proposed approach gives better results if a vehicle pretends to be moving with high speed but its time of contact is greater than the threshold according to calculated speed. In terms of the DR, we have analyzed that detection approach defined for FRPMI and FPMI attacks is more efficient as compared to detection methods for FRPSI and FPSI attacks. This may be because of the fact that number of honest nodes at any given time are likely to be more than RSUs in the neighborhood of malicious vehicle.

Proposed approach is not able to detect position forging attacks in some scenarios. For example, when a vehicle takes a U-turn. In this case, observers (RSU or neighboring vehicles) may consider the vehicles moving in backward direction as attacker vehicles. In this situation, attacker vehicle may propagate false location information by measuring the distance from observer and tuning the transmission power accordingly. In another example, when a vehicle is moving on a flyover with loops. Actual distance might be different from the Euclidean distance in this case. This is an open problem for consistency based solutions.

Another problem occurs when some vehicles are moving in a group. In this scenario, one vehicle might aid the other by sending wrong alert packets. For example, if two vehicles V_1 and V_2 move together as a group. V_1 has to take right turn and V_2 is supposed to go left. V_1 takes right turn as per its requirement but V_2 pretends as V_1 by sending an alert packet "*Congestion on right road*" and take the left turn as described. Vehicles behind V_2 notice the alert and also receive the subsequent beacon packets from V_2, thereby conclude that alert sent by V_2 is correct. This type of misbehavior of V_2 is undetected and V_1 might take benefit of moving on congestion free road. Our future work includes to address these issues.

10 Conclusion

In this paper, we present various position forging attacks in VANETs involving attacker(s) that sends forged traffic warning messages to create an illusion of occurrence of a non-existing event. The attacker performs this attack by using virtual identities and faked positions. In order to avoid unforeseen traffic events, the nodes receiving these fraud messages change their driving behavior. We investigate the impact of various positions forging attacks on average vehicle speed, percentage of delivered packets and channel utilization in terms of number of collisions in VANETs. We observe that by creating virtual congestion, the attacker becomes successful in causing real congestion by slowing down the vehicles.

We have proposed and implemented detection approaches for all types of position forging attacks. Our detection approaches use VANET functionality, such as placement of RSUs (in the form of traffic and road lights) and high mobility of vehicles. Previous solutions in literature used for detection of position forging attackers are based upon

position verification and require specialized hardware such as radar. Unlike these approaches, our technique does not require any special hardware as position information in beacon packets generated by various vehicles is collected for a duration either by RSU or neighboring nodes and analyzed for suspicious activity. All our detection approaches are able to detect position forging nodes for simulation data as well as real traffic data for FPMI and FRPMI.

In future work, we would like to design a framework that integrate these detection approaches so that any type of position and ID forging attack can be detected dynamically. Also we would like to consider a scenario where a small fraction of RSUs are compromised in our future work. We also would like to consider the GPS inaccuracies in order to evaluate the proposed techniques.

References

1. Aijaz A, Bochow B, Dtzer F, Festag A, Gerlach M, Kroh R, Leinmller T (2006) Attacks on inter vehicle communication systems—an analysis. In: Proceedings of WIT, pp 189–194
2. Raya M, Hubaux JP (2007) Securing vehicular ad hoc networks. J Comput Secur 15(1):39–68
3. Plossl K, Nowey T, Mletzko C (2006) Towards a security architecture for vehicular ad hoc networks. In: The first international conference on availability, reliability and security, 2006 (ARES 2006), p 8
4. Douceur JR (2002) The Sybil attack. In: IPTPS '01: revised papers from the first international workshop on peer-to-peer systems. Springer, London, pp 251–260
5. Raya M, Papadimitratos P, Hubaux J-P (2006) Securing vehicular communications. IEEE Wirel Commun Mag 13(5):8–15 (Special issue on inter-vehicular communications)
6. Leinmuller T, Schoch E, Maihofer C (2007) Security requirements and solution concepts in vehicular ad hoc networks. In: Proceedings of the fourth annual conference on wireless on demand network systems and services (WONS 2007),pp 84–91
7. Leinmller T, Schoch E, Kargl F, Maihfer C (2010) Decentralized position verification in geographic ad hoc routing. Secur Commun Netw 3(4):289–302
8. Leinmüller T, Maihöfer C, Schoch E, Kargl F (2006) Improved security in geographic ad hoc routing through autonomous position verification. In: VANET '06: proceedings of the 3rd international workshop on vehicular ad hoc networks. ACM, New York, NY, pp 57–66
9. Karp B, Kung HT (2000) GPSR: greedy perimeter stateless routing for wireless networks. In: Proceedings of the 6th annual international conference on mobile computing and networking, ACM, pp 243–254
10. Leinmuller T, Schoch E, Kargl F (2006) Position verification approaches for vehicular ad hoc networks. IEEE Wirel Commun 13(5):16–21
11. Sastry N, Shankar U, Wagner D (2003) Secure verification of location claims. In: Proceedings of the 2nd ACM workshop on wireless security, pp 1–10
12. Vora A, Nesterenko M (2006) Secure location verification using radio broadcast. IEEE Trans Depend Secur Comput 3(4):377–385
13. Yan G, Olariu S, Weigle Michele C (2008) Providing VANET security through active position detection. Comput Commun 31(12):2883–2897
14. Yan G, Olariu S, Weigle Michele C (2008) Providing location security in vehicular ad hoc networks. IEEE Wirel Commun 16(6):48–55
15. Hubaux J-P, Čapkun S, Luo J (2004) The security and privacy of smart vehicles. IEEE Secur Priv 2(3):49–55
16. Hesiri Weerasinghe D, Tackett R, Fu H (2010) Verifying position and velocity for vehicular ad-hoc networks. Secur Commun Netw 4(7):785-791
17. Golle P, Greene D, Staddon J (2004) Detecting and correcting malicious data in VANETs. In: VANET '04: proceedings of the 1st ACM international workshop on vehicular ad hoc networks, pp 29–37
18. Xiao B, Yu B, Gao C (2006) Detection and localization of Sybil nodes in VANETs. In: DIWANS '06: proceedings of the 2006 workshop on dependability issues in wireless ad hoc networks and sensor networks. ACM, New York, NY, pp 1–8
19. Lv S, Wang X, Zhao X, Zhou X (2008) Detecting the Sybil attack cooperatively in wireless sensor networks. In: CIS '08: proceedings of the 2008 international conference on computational intelligence and security. IEEE Computer Society, Washington, DC, USA, pp 442–446
20. Demirbas M, Song Y (2006) An RSSI-based scheme for Sybil attack detection in wireless sensor networks. In: WOWMOM '06: proceedings of the 2006 international symposium on world of wireless, mobile and multimedia networks. IEEE Computer Society, Washington, DC, USA, pp 564–570
21. Ssu KF, Wang WT, Chang WC (2009) Detecting Sybil attacks in wireless sensor networks using neighboring information. Comput Netw 53(18):3042–3056
22. Salah Bouassida M, Guette G, Shawky M, Ducourthial B (2009) Sybil nodes detection based on received signal strength variations within VANET. Int J Netw Secur 9(1):22–33
23. Chen C, Wang X, Han W, Zang B (2009) A robust detection of the Sybil attack in urban VANETs. In: ICDCS workshops, IEEE Computer Society, pp 270–276
24. Park S, Aslam B, Zou C, Turgut D (2009) Defense against Sybil attack in vehicular ad hoc network based on roadside units support. In: Proceedings of military communications conference (MILCOM'09), IEEE Computer Society, pp 1–7
25. Conti M, Di Pietro R, Mancini Luigi V, Mei A (2009) Mobility and cooperation to Thwart node capture attacks in MANETs. J Wirel Commun Netw. doi:10.1155/2009/945943
26. Lo N-W, Tsai H-C (2007) Illusion attack on VANET applications—a message plausibility problem. In: 2007 IEEE Globecom Workshops, pp 1–8
27. Leinmuller T, Schmidt RK, Schoch E, Held A, Schafer G (2008) Modeling roadside attacker behavior in VANETs. In: 2008 IEEE GLOBECOM workshops, pp 1–10
28. Leinmuller T, Robert KS, Albert H (2010) Cooperative position verification—defending against roadside attackers 2.0. In: 17th ITS world congress, Busan
29. Robert KS, Leinmuller T, Albert H (2009) Defending against roadside attackers. In: 16th ITS world congress on intelligent transport systems, Stockholm
30. Grover J, Gaur MS, Laxmi V (2011) Position forging attacks in vehicular ad hoc networks: implementation, impact and detection. In: Proceedings of the 7th international wireless communications and mobile computing conference (IWCMC–2011), IEEE, Istanbul, pp 701–706
31. Rappaport TS (1996) Wireless communications, principles and practice. Prentice Hall, London

32. Jiang D, Delgrossi L (2008) IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In: Vehicular technology conference, 2008, IEEE, pp 2036–2040
33. Grover J, Kumar D, Sargurunathan M, Gaur MS, Laxmi V (2010) Performance evaluation and detection of Sybil attacks in vehicular ad-hoc networks. Recent trends in network security and applications, communications in computer and information science. Springer, Berlin, pp 473–482
34. Grover J, Gaur MS, Laxmi V (2010) A novel defense mechanism against Sybil attacks in VANET. In: Proceedings of the 3rd international conference on security of information and networks, ACM, pp 249–255
35. Wang SY, Lin CC (2008) NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In: 2nd IEEE international symposium on wireless vehicular communications, pp 1–2
36. Naumov V, Baumann R, Gross T (2006) An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. In: Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, ACM, pp 108–119
37. Artimy M (2007) Local density estimation and dynamic transmission range assignment in vehicular ad hoc networks. IEEE Trans Intell Transp Syst 8(3):400–412