Position Forging Attacks in Vehicular Ad Hoc Networks: Implementation, Impact and Detection

Jyoti Grover[1], Manoj Singh Gaur[2], Vijay Laxmi[3]
Department of Computer Engineering
Malaviya National Institute of Technology
Jaipur-302017, Rajasthan, India
{jyoti.grover[1]|gaurms[2]|vlgaur[3]}@gmail.com

***Abstract*—Vehicular Ad Hoc Network (VANET) applications operate on the principle of periodic exchange of messages between nodes. However, a malicious node can create multiple virtual identities for transmitting fake messages using different forged positions. This creates an illusion of a non-existent event. In VANET, each vehicle periodically broadcasts its identity (ID), time and current geographic position in beacon packets. Node position and time are important factors for modeling an attack as well as for its detection. In this paper, we introduce new variants of (a) Position forging attacks and (b) Combination of position and ID forging attacks. We also propose an implementation of these attacks, their impact on the performance of VANET and description of detection methodology. In a position forging attack, an attacker broadcasts timely coordinated wrong traffic warning messages with forged positions, producing an illusion of a car accident, a traffic jam or an emergency braking. This degrades the performance of VANET in terms of channel utilization. It also has a severe impact on the performance of security algorithms. We analyze the impact of forged position information on average vehicle speed, percentage of delivered packets and number of collisions.**

***Index Terms*—VANET, Position Forging, Identity Forging, Attack, Performance, Simulation**

I. Introduction

The objective of Vehicular Ad Hoc Networks (VANETs) is to improve vehicle passenger safety by means of inter-vehicle communication. For example, in case of an accident, VANET communication can be used to warn other vehicles approaching the site. VANET is basically used for providing two types of applications – Event-Driven and Cooperative Awareness applications. In Event-Driven applications, nodes send messages about the occurrence of certain events. Cooperative awareness applications determine dangerous situations based upon messages received from neighboring nodes. Both of these applications are dependent on accurate position information. Falsified position information can be generated by inaccurate Geographical Position System (GPS) or intentionally by an attacker to disturb the whole safety system. A malicious node creates multiple virtual identities and associates forged positions with them.

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 to its destination by convincing other vehicles to slow down or speed up on the road. The malicious vehicle forges its identity (sometimes creates multiple virtual identities) and position information to escape its detection.

In this paper, we discuss in detail the various position forging attacks in VANET and attacker behavior that pose high risks to the system. In general, drivers' behavior depends on traffic warning messages they receive. An attacker can degrade VANET performance by manipulating the topology. Beacon packets are periodically broadcast and they contain some basic information like Sender-ID, time, position and speed. Since the sender identity 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 of attack detection as well. We also evaluate the impact of these attacks on VANET performance and outline of proposed detection methodologies for these attacks.

The rest of the paper is organized as follows. Section II discusses related work of several attacks on inter-vehicle communication system and their detection approaches. Section III describes VANET model, communication model used in VANET. Various forms of position forging attacks are presented in Section IV. Impact of attacks, attacker model, experimental setup and simulation results are discussed in Section V. Section VI overviews the detection process of these attacks. Concluding remarks with future work are covered in Section VII.

II. 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 proposed plausibility checks using constant system examinations. However, this paper does not discuss how to apply plausibility checks in detail.

Raya and Hubaux [2] discuss number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and security problems. Golle *et al* [3] 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.

978-1-4577-9538-2/11/$26.00 ©2011 IEEE

Raya *et al* [4], [5] have formulated a misbehavior detection system to exclude malicious vehicles from the communication system. It is based on its deviation of attacker node from normal behavior. A basic position verification approach is proposed by Leinmuller *et al* [6], [7] to evaluate the cooperation of vehicles regarding geographic routing in VANETs. Consistency of position data is inspected i.e change in movement and density of vehicles and map based verification. Yan *et al* [8], [9] have also proposed a position verification approach. In their work, it is assumed that GPS devices are installed in each node. GPS position claimed by sender are matched with the estimated position by radar at receiver end.

Xiao *et al* [10] have proposed 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. The detection approach uses statistical analysis of signal strength distribution.

Shaohe *et al* [11] have proposed a cooperative RSS based Sybil attack detection for static sensor networks where all nodes have fixed transmission power; either it is honest or malicious. Each node overhears packets and computes the distance to other nodes using received signal strength. Each node creates group of neighboring nodes by similarity in RSS value and periodically broadcasts the group result. Identities with similar RSS values are grouped into a suspect group.

In our previous work [12], we have surveyed the Sybil attack in VANET and analyzed the features of existing detection approaches. We have performed the implementation of Sybil attack in VANET scenario and proposed distributed detection methodology in [13]. We have proposed two detection approaches for Sybil attack detection in [14] and [15].

Nai-Wei *et al* [16] presented 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. Plausibility validation network model is introduced in this paper to detect and defend against illusion attack.

Roadside attacker behavior is discussed in detail by Leinmuller *et al* in [17]. This paper provides an overview of various position forging attacks. They have left the detection mechanism for various position forging attacks as future work. In our paper, we are implementing position forging attacks but from a different perspective. We are using vehicles as attackers whereas in their work, roadside unit is considered as an attacker, which is not practical in case of path forging attacks. Also, we propose detection mechanisms for these attacks in this paper.

III. System Model

In this section, we present a brief description of the VANET and associated communication model.

A. VANET model

VANET consists of two basic components: (1) Road Side Unit (RSU) and (2) On Board Unit (OBU). RSU is a fixed unit while OBUs are installed in vehicles and are moving. Each node in VANET consists of an EDR (Event Data Recorder), GPS (Global Positioning System) receiver, computing platform and a radar. A hierarchy of central authorities (CA) is responsible for managing of vehicles identities registered in its respective geographic region. At the data link layer, dedicated short range communication (DSRC) protocol [18], currently being standardized as IEEE 802.11p is used. It provides transmission range between 250 to 1000m, with data rates in the 6-27Mbps range.

B. Communication Model

In VANETs, both RSUs and vehicles participate in communication. VANET offers three types of communication: (1) In-Vehicle (IV) (2) Vehicle to Vehicle (V2V) and (3) Vehicle to Road side unit (V2R). In-vehicle communication facilitates information to exchange between different components of a vehicle. V2V allows communication between vehicles. It is used for disseminating safety and warning messages in the network. V2V can be categorized into two types depending upon the relative position of sender and receiver: single-hop and multi-hop. Safety messages are sent by local broadcast of vehicles i.e. using single-hop V2V communication. Multi-hop V2V communication is usually exploited for sending non-safety messages. V2R allows communication between the vehicles and RSUs. It is used to provide facilities e.g Internet access and special service request.

IV. Different forms of position forging attacks

An attacker may use one or multiple identities (IDs) to launch a position forging attack. An attacker can forge positions using various methods. Positions can be selected or guessed by knowing its own and neighboring nodes' positions. Attacker can spoof the positions of other nodes and uses them at different time intervals. Digital maps provide another method of deriving node positions. If an attacker implements a combination of Position and ID forging attack, multiple virtual identities are used simultaneously for position forging. This 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.

A. FRPSI (Forging Random Positions using Single ID):

In this position forging attack, an attacker forges its identity for sending any message. The attacker uses this forged identity for sending the same safety message but from random positions.

This attack is shown in Figure 1. Numbers $1, 2, ...5$ represent time instances at which an attacker node M 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 forged identity of an attacker. This notation is applicable for all forms of position forging attacks. The purpose of this type of attack is to simply broadcast same event information from different positions.

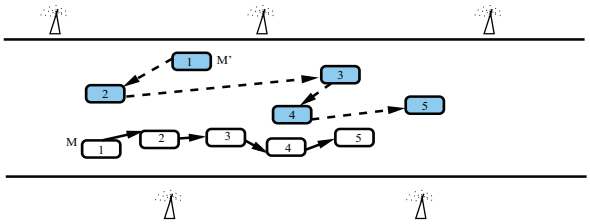

Fig. 1. Sequence of forged positions used by a an attacker node M pretending as node M'

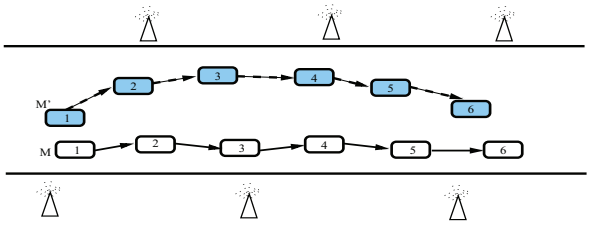

Fig. 3. Sequence of positions on one forged path by an attacker M pretending as M'

B. FRPMI (Forging Random Positions using Multiple IDs):

An attacker broadcasts fake messages using multiple fake identities from random positions at the same time. To create an illusion of some warning or safety event, an attacker spoofs the identities of other nodes or fabricates identities and uses them simultaneously in the network. The attacker associates random positions with each fabricated node at each time interval.

In this attack, the major concern is to choose the appropriate IDs and node positions. The attacker has to consider that no two fabricated nodes broadcast same position at same time. Attacker's effort is proportional to the number of identities used by the attacker. A sample *FRPMI* attack using 2 IDs is shown in Figure 2.

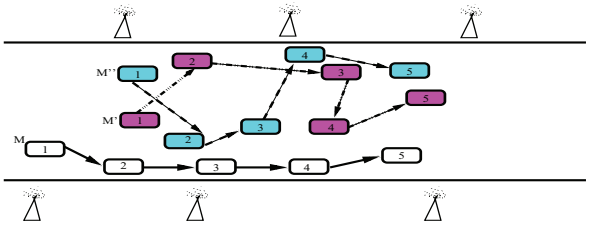

Fig. 2. Attacker M broadcast message by using random sequence of positions and two different identities M' and M''

C. FPSI (Forging Path using Single ID):

In a path-forging attack, the attacker forges its identity to broadcast fake messages using a forged consistent sequence of positions. This attack is intelligent and difficult to detect. The motive of the attacker is to create an illusion that the node is moving normally on a pre-defined path. A sample for this attack is shown in Figure 3. This attack is successful when the traffic situation does not change. Inconsistent movement paths may be detected based on changes in traffic pattern.

D. FPMI (Forging Path using Multiple IDs):

In this attack, an attacker creates multiple virtual identities that participate simultaneously in the network with a 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 the same time. This attack is shown in Figure 4. The attacker may forge the whole traffic situation by simulating a majority of vehicles i.e. their positions as well as movement. This type of attacker possesses the highest possibility of passing position and speed consistency checks as it is more careful about the construction of forged paths.

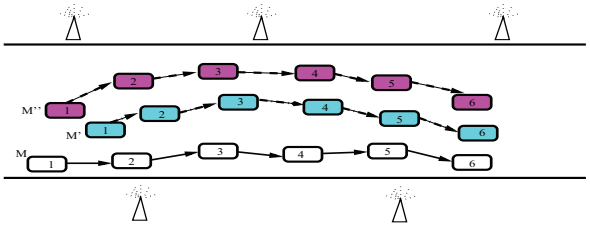

Fig. 4. Two forged paths using two IDs M' and M''

V. Impact of Position forging attacks on VANET performance

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

A. Attacker Model for position forging attacks

Various position forging attackers are implemented according to their behavior of forging. Attacker model for position forging attacks is provided in Algorithm 1.

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 $PATH$ are associated with these virtual identities containing random positions. Hence, number of $PATH$ required and $N_{virtual}$ are same. Multiple copies of application programs required for sending beacon packets are associated with attacker node in this case. The attacker considers all road boundaries in the simulation area while using any random position.

In a *FPSI* attack, $N_{virtual}$ equals one and $PATH$ contains a sequence of positions derived by knowing its own and neighboring node's positions for sending a beacon packet.

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
T_{range} = Transmission range of attacker
POS_{rand} = Random position in T_{range}
$Attacker_i$ = i^{th} attacker, $i \in [1, \cdots, A]$
Δ = 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 $N_{virtual}$
    $POS_{rand} \in POS_{(X,Y)}$
    $POS_{(x,y),k,t_s} = POS_{(x,y),i,t_s} + POS_{rand}$
  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**
      $POS_{(x,y),k,t_0}$ as per attack mode
      $PATH_k = POS_{(x,y),k,t_s}, \cdots, POS_{(x,y),k,t_f}$
    end for
  end for
end for

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

In a *FPMI* attack, multiple identities are associated with the attacker. Value of $N_{virtual}$ is greater than one and each identity simultaneously performs path forging. We take into account a special consideration that no two virtual identities are at the same position at any given time interval.

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

B. Experimental Setup and Simulation Results

To evaluate various position forging attacks, we implement them in NCTUns 5.0 simulator [19]. This simulator provides multiple simulation parameters including topology (road network), communication and network protocol, vehicular traffic, feedback loop and several others. We applied a widely used radio propagation model – `shadowing model` to consider the multipath propagation effects of the real world communication system.

In our experiments, we simulated a two-direction 10km highway with multi-lanes in each direction. The average speed range of vehicles is set between 30–180 Km/h, number of nodes is 150 and transmission range is 250 meters. Each simulation case has a variable number of position forging attackers, as well as variable number of identities used by these attackers. Duration of each simulation is 1000 seconds and each simulation is repeated 10-15 times with a different seed value to achieve a higher confidence level. 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.

C. Impact of Position Forging Attacks

The simulation results are evaluated using the following parameters :

- **Number of Packet Collisions:** Hidden terminal problem is the main cause of collisions in a wireless network. If multiple nodes transmit at the same time, a collision occurs at this shared communication channel. We count the number of collisions in our network scenario.
- **Average Vehicle Speed:** We calculate the average speed of all vehicles involved in the simulation.
- **Packets delivered:** It is defined as number of the packets received over number of packets transmitted in the network.

We measure the difference between two cases of position forging attackers in terms of percentage of delivered packets. In the first case, there are position forging attackers that are broadcasting fake packets with forged positions. The second case considers a position forging attacker that blocks the forwarding process. The impact of these two types of attackers on percentage of delivered packets is shown in Figure 5.

The percentage of delivered packets is measured w.r.t. position deviation. Position deviation is the difference between the actual position of attacker and position forged by it for broadcasting packets. It is observed the reduction of 50% delivered packets in position forging attacker blocking the forwarding process as compared to basic form of position forging attack. We observe greater reduction in delivered packets in cases where position deviation is more than 250 meters. If there is no attacker in our simulation environment, we observe that number of packet collisions are approximately 5%.

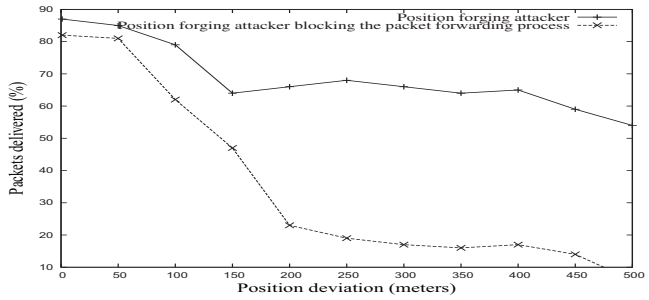

Fig. 5. Impact of position forging attacker on percentage of delivered packets

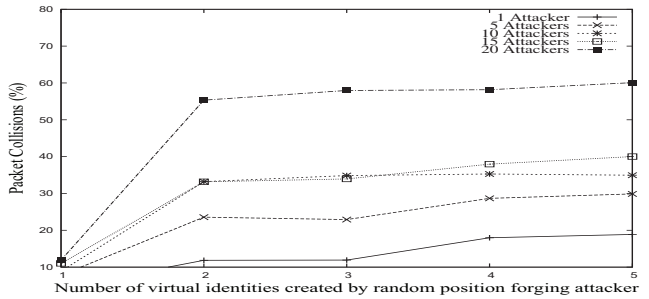

Fig. 6. Impact of random position forging attacker on number of packet collisions

Figure 6 shows the impact of random position forging attack (with a variable number of identities used by these attackers) on number of packet collisions in our scenario. As the number of attackers increase, number of packet collisions increases proportionally. Similar results can be seen for path forging attackers from Figure 7.

We measure the number of packet collisions by considering two parameters used for implementation of attackers: (1) Number of attackers and (2) Number of virtual identities created by attacker. We consider various cases of attackers by varying the number of attackers and virtual identities used by it.

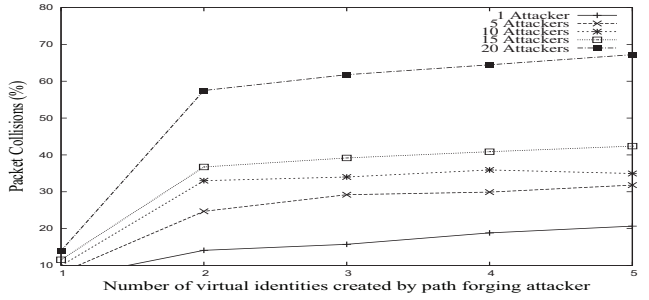

Fig. 7. Impact of path forging attacker on number of packet collisions

It is observed that the number of packet collisions in a path forging attack is approximately within the same range as that of random position forging attack. This is due to the same number of identities being used by attackers in both cases. All identities used by attackers participate simultaneously in the network for broadcasting packets. This increases the total number of packets generated in the network. Since the same communication channel is shared among all nodes, therefore the number of packet collisions also increases.

Figure 8 illustrates the impact of random position forging attackers on average vehicle speed in VANET. 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.

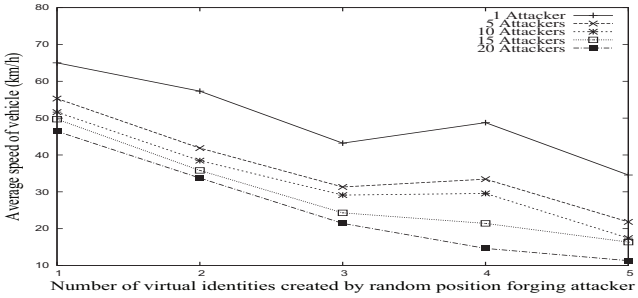

Fig. 8. Impact of random position forging attacker on average speed of vehicles

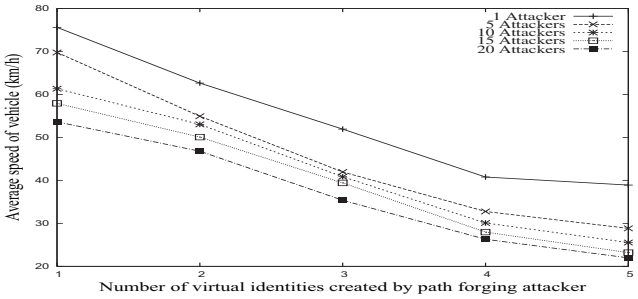

Fig. 9. Impact of path forging attacker on average speed of vehicles

In Figure 9, the average vehicle speed is evaluated based on different number of path forging attackers. Path forging attackers broadcast the same packet using a consistent sequence of positions in such a way that receivers consider it as genuine messages. Due to this typical nature of attacker, there is an illusion of more 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 20Km/h which can cause real congestion.

VI. Proposed Detection Methodology

Due to lack of space, we present a brief outline of detection approaches for above-defined attacks. Detection process of *FRPSI* attack constitutes the verification of acceptance range and speed of vehicles. It is assumed that RSUs perform the verification process so that computation time required for verification can be minimized. Each RSU calculates the speed depending upon the position information broadcast in subsequent beacon packets of a passing–by vehicle. If there is an inconsistency in position and the speed of consecutive packets received from a vehicle, it is suspected as being malicious. All RSUs exchange their observations periodically. If an inconsistency is measured by more than one RSU for an extended time duration, the suspected vehicles are discarded.

Detection approach for *FPSI* attack also uses acceptance range and speed verification. Another check (`Time spent in a cell`) is required for verification of the time duration during which an attacker remains within the cell (acceptance range of observer i.e. RSU). These three verifications are integrated for validation of this form of attack. Indiscriminate behavior of this form of attack requires application of this extra check. *FPSI* attack passes acceptance range and speed verification but `time spent in a cell` check strengthen the validation of attack.

Other proposed approach is applicable for detection of *FRPMI* and *FPMI* attacks. These attacks are a combination of ID and position forging attacks and use multiple identities simultaneously. It is based on the similarity of received signal strength (RSS). This method makes use of VANET properties such as the predefined mobility pattern of nodes and placement of some fixed units on roadside. Each vehicle in VANET periodically broadcasts a beacon packet. All receivers store the RSS value of beacons and group these sender IDs with similar RSS values. All RSUs exchange similar RSS value groups after a fixed interval of time. If some members of a group stored in one RSU match with another RSU group during an incremental time interval, this implies the existence of attack. Nodes having similar RSS values over a significant period of time are considered to have the same physical trajectory. This scenario is possible only for virtual nodes created by attacker.

VII. Conclusion and Future Work

In this paper, we elaborate various new forms of position forging attacks in VANET where an attacker sends forged traffic warning messages to create an illusion of occurrence of a non-existing event. The attacker perform this function by using virtual identities and faked positions. In order to avoid false traffic events, the nodes receiving these fraud messages change their driver behavior accordingly. We investigated the impact of various positions forging attacks on the average speed of vehicles, percentage of delivered packets and channel utilization in terms of number of collisions in VANET. We observed that by creating virtual congestion, the attacker becomes successful in leading to real congestion by slowing down the vehicles. We also briefly discussed our work in progress for detection of these attacks.

References

[1] Amer Aijaz, Bernd Bochow, Florian Dtzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmller. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Proceedings of WIT*, pages 189–194, 2006.

[2] M. Raya and J.P. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[3] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and Correcting Malicious Data in VANETs. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37, New York, NY, USA, 2004. ACM.

[4] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.P. Hubaux. Eviction of Misbehaving and Faulty nodes in Vehicular Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks*, 25(8):1557–1568, 2007.

[5] Tyler Moore, Jolyon Clulow, Panos Papadimitratos, Ross Anderson, and Jean pierre Hubaux. Fast Exclusion of Errant Devices from Vehicular Networks. In *Sensor and Ad Hoc Communications and Networks*, pages 135–143. IEEE, 2008.

[6] T. Leinmuller, E. Schoch, and F. Kargl. POSITION VERIFICATION APPROACHES FOR VEHICULAR AD HOC NETWORKS. *Wireless Communications, IEEE*, 13(5):16–21, october 2006.

[7] T. Leinmller, E. Schoch, F. Kargl, and C. Maihfer. Influence of falsified position data on geographic ad-hoc routing. In *2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2005)*, pages 102–112, 2005.

[8] Gongjun Yan, Stephan Olariu, and Michele C. Weigle. Providing VANET Security Through Active Position Detection. *Comput. Commun.*, 31(12):2883–2897, 2008.

[9] Gongjun Yan, S. Olariu, and M. Weigle. Providing location security in vehicular Ad Hoc networks. *Wireless Communications*, 16(6):48–55, December 2009.

[10] Bin Xiao, Bo Yu, and Chuanshan Gao. 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*, pages 1–8, New York, NY, USA, 2006. ACM.

[11] Shaohe Lv, Xiaodong Wang, Xin Zhao, and Xingming Zhou. Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks. In *CIS '08: Proceedings of the 2008 International Conference on Computational Intelligence and Security*, pages 442–446, Washington, DC, USA, 2008. IEEE Computer Society.

[12] Jyoti Grover, M.S. Gaur, and Vijay Laxmi. Sybil Attacks in VANET: Detection and Prevention. In Al-Sakib Khan Pathan, editor, *Security of Self-Organizing Networks MANET, WSN, WMN, VANET*, pages 269–294. Auerbach Publications, 2011.

[13] Jyoti Grover, Deepak Kumar, M. Sargurunathan, M.S. Gaur, and Vijay Laxmi. Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks. In *Recent Trends in Network Security and Applications*, Communications in Computer and Information Science, pages 473–482. Springer Berlin Heidelberg, 2010.

[14] Jyoti Grover, M.S. Gaur, and Vijay Laxmi. A Novel Defense Mechanism against Sybil Attacks in VANET. In *Proceedings of the 3rd international conference on Security of information and networks*, SIN '10, pages 249–255, New York, NY, USA, 2010. ACM.

[15] Jyoti Grover, M.S. Gaur, Nitesh Prajapati, and Vijay Laxmi. RSS-based Sybil Attack Detection in VANETs. In *Proceedings of the international conference TENCON2010*, pages 2278–2283. IEEE, 2010.

[16] Nai-Wei Lo and Hsiao-Chien Tsai. Illusion Attack on VANET Applications - A Message Plausibility Problem. In *Globecom Workshops, 2007 IEEE*, pages 1–8, 2007.

[17] T. Leinmuller, R.K. Schmidt, E. Schoch, A. Held, and G. Schafer. Modeling Roadside Attacker Behavior in VANETs. In *GLOBECOM Workshops, 2008 IEEE*, pages 1–10, nov. 2008.

[18] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040, 2008.

[19] S.Y. Wang and C.C. Lin. 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*, September 2008.