International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:11, No:6, 2017

Imposter Detection Based on Location in Vehicular Ad-Hoc Network

Sanjoy Das, Akash Arya, Rishi Pal Singh

***Abstract*—**Vehicular Ad hoc Network is basically the solution of several problems associated while vehicles are plying on the road. In this paper, we have focused on the detection of imposter node while it has stolen the ID's of the authenticated vehicle in the network. The purpose is to harm the network through imposter messages. Here, we have proposed a protocol namely Imposter Detection based on Location (IDBL), which will store the location coordinate of the each vehicle as the key of the authenticity of the message so that imposter node can be detected. The imposter nodes send messages from a stolen ID and show that it is from an authentic node ID. So, to detect this anomaly, the first location is checked and observed different from original vehicle location. This node is known as imposter node. We have implemented the algorithm through JAVA and tested various types of node distribution and observed the detection probability of imposter node.

***Keywords*—**Authentication, detection, IDBL protocol, imposter node, node detection.

I. Introduction

THE intelligent transportation system always helps human being for safer travel and as well as economic development globally. Heavy road traffic is one of the major problems faced worldwide. Thus to deal with traffic situation, safety etc. on road in transportation system there is a new innovation called VANET which has brought a revolutionary change in the transport system.

VANET (Vehicular Ad-hoc Network) is a sub-category of MANET (Mobile Ad-hoc Network). The communication is established through wireless medium among Vehicles to Roadside Units (RSUs) and Vehicle-to-Vehicle. The VANET primarily focuses on safety concern and improved traffic condition by establishing an environment that promotes inter-vehicular communications (V2V) and vehicles to Infrastructure (V2I) communications regarding road related concern such as accidents, road traffic routing etc. [1]. Each node within the VANET networks is equipped with wireless devices for information exchange. The VANET plays a vital role in improving the situation of traffic related issues, finding correct route, know traffic situation in advance. This needs the prior knowledge of the situation around the vehicles.

A VANET is a self-organized network that can be formed by connecting vehicles, aiming to improve the security and privacy and traffic control with internet access by the drivers.

Sanjoy Das, Associate Professor, is with the School of Computing Science and Engineering, Galgotias University, India (e-mail: sdas.jnu@gmail.com).
Akash Arya is with the Galgotias University, (e-mail:akash4arya5@gmail.com).
Rishi Pal Singh is with the Guru Jambheshwar University of Science and Technology, Hisar, India (e-mail:pal_rishi@yahoo.com)

A simple scenario of VANET is shown in Fig. 1. The world health organization data show that nearly 1.2 million people are killed every year due to road accidents [4]. So with the help of this application, we are able to reduce the road accidents and save human lives. For establishing a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax) [1]. The dedicated short range communication is operating on 5.9 GHz and it uses IEEE 802.11 access methods for communication. The DSRC creates a new kind of communication application which increases overall security, privacy, efficiency or safety of the transportation system [2]. ITS is the future of transportation system. VANETs are a temporary network with no fixed infrastructure, no wired communication between vehicles. It is a collection of multiple nodes and nodes have a duty to forward the message, maintain a routing table and secure their resource from imposter attackers. It is used for the short time communication. In VANET, vehicles may establish communication via vehicle-to-vehicle (V2V) or Vehicle-to-Infrastructure (V2I). There are many challenging issues as authentication of any new vehicles, how to detect any imposter vehicles, how to establish secure communication among the vehicles etc. [8]. In this network, message received from another vehicle should be authenticated because some of the vehicles may misbehave in the network and may create a congestion or may possible broadcast false information for their own advantages over the other vehicles. In this paper, we have developed a protocol known as IDBL. It helps to authenticate and detection of imposters in the network. This technique establishes a secure communication among vehicles.

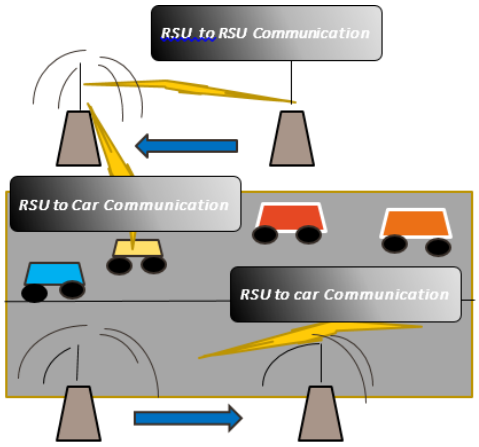

Fig. 1 Simple scenario of VANET

The paper is organized as follows: Section II discusses related work done by researchers and academicians. In Section III, IDBL is discussed. Section IV discusses the simulation environments and the result analysis. Finally, we have concluded the paper with future direction for further research in Section V.

II. Related Work

In order to suggest the proposed work, a lot of papers have been considered and their works have been studied carefully. In [5], authors have suggested a mechanism to determine the traffic on the road. The prime focus of the paper is to handle congestion over the network and to find the appropriate mechanism to improve the traffic flow but the solution is expensive in nature. Also, there are no means to impose any penalty for a malicious node. Data-centric techniques are considered in [3]. In this paper, the focus is set on the data which are transferred over the VANET. The data-centric technique prevents transfer of the same data again and again in the network and expensive in nature. In [6], security issues are considered. In VANET, communication follows wireless medium and due to this, it is always vulnerable to attackers. The most lethal attack considered is DDoS, where network is not available to the legitimate users as and when required. In this paper, how to stop a DDOS is well discussed but nothing addressed on permanent blockage of nodes causing the problems [7].

Newsome et al. [9] study the threat posed by the Sybil attack in wireless sensor networks and propose new types of defenses known as Position verification. In this approach, the network each node position is verified first. Secondly, it checks identities of each node. If messages are coming from the same location it is assumed that it comes from the same node [9]. Through their analysis, it is shown that position verification can be used to prevent Sybil attacks in VANETs. Position verification is a well-known problem in ad hoc networks [10]. The certificate revocation leads to a creation of certificate revocation list [20]. The CRL is issued by a trusted authority and updated after each revocation [11]. When the message is authenticated by PKI system, firstly it verifies the revocation status of the sender's certificate. This is done by using the CRL which is followed by the verification of sender's certificates. Finally, sender's signature verifies on the received message [11], [20]. In [12], to protect the privacy of user identity and location, KI scheme is used. It uses anonymous public keys resulting in storage problems as they make use of a large number of keys and certification. In [13], authors have described various security attacks and their effects. An attacker with multiple fake ID's try to mislead another node that multiple neighbours exist and communication between all fake nodes is fully controlled by the imposter attacker [14], [15]. The global observer thus accesses the route of the target vehicle. To launch this kind of attack, the attacker may make use of the RSU [16], [19]. The attack type is passive aimed at collecting the target nodes ID and location. This is done by sending imposter code to the neighbour of the target node which in turn discloses target vehicle's ID and location and hence, its privacy is lost [17], [19]. To execute such attacks, the nature of the attacker may be outsider or insider or an authentic user. In such attacks, wrong information is distributed over the network to affect the decisions of other vehicles, hence enforcing it to decide a wrong path [18], [19].

III. Methodology

Security is one of the major concerns for any researcher as any point of weakness could lead to hazardous conditions in the era of cyber threats. To establish secure communication between any two vehicles is a major concern. The ongoing message exchange in wireless medium can easily be listened by imposter node. There are various types of attack where there is a case of the message being hacked with various kinds of intentions. Due to the openness of the network in VANETs, the attack by imposter node becomes easy. It is difficult to detect because the network is open. This attack becomes potential threat for information exchanged in the network. This can be misused the information security and property safety of users. Therefore, how to accurately the new accessing node and how to detect imposter node are becoming an immediate research problem.

In this methodology we have considered an identity threat scenario. In this scenario, the identity of node is stolen and with the help of stolen ID, it tries capture the network by sending imposter messages. Thus, we have used a technique to use the location information of the node as the key to authenticate the message.

We proposed a detection technique protocol based on the location of nodes, that is "Imposter Detection Based on Location" (IDBL). We assume that all the scenario is stationary. This scenario works on traffic signal points. This technique helps in detecting the imposter node within VANET by using location verification.

In this technique, we have designed a network topology with few authenticated nodes. Existed vehicles are able to communicate each other. In this stage, every node knows its neighbour nodes' ID's and locations. In our simulation, we considered that each node has a unique location and one location cannot be the same for two nodes. The imposter node is attacking the network to break the security and privacy, before that, ID of an authenticated node is stolen for communication. In our method, we have detected the imposter node attack which tries to make an identity attack. Once identity of a node is stolen, that particular node immediately starts sending messages in the network. Thus to check the authenticity of a sender, the location information of node is used. The message contains the location information. Here, the location information considered as the key for the authenticity of the message. The received message can be authenticated if and only if messages are received from ID and location of node; otherwise detected as an imposter node.

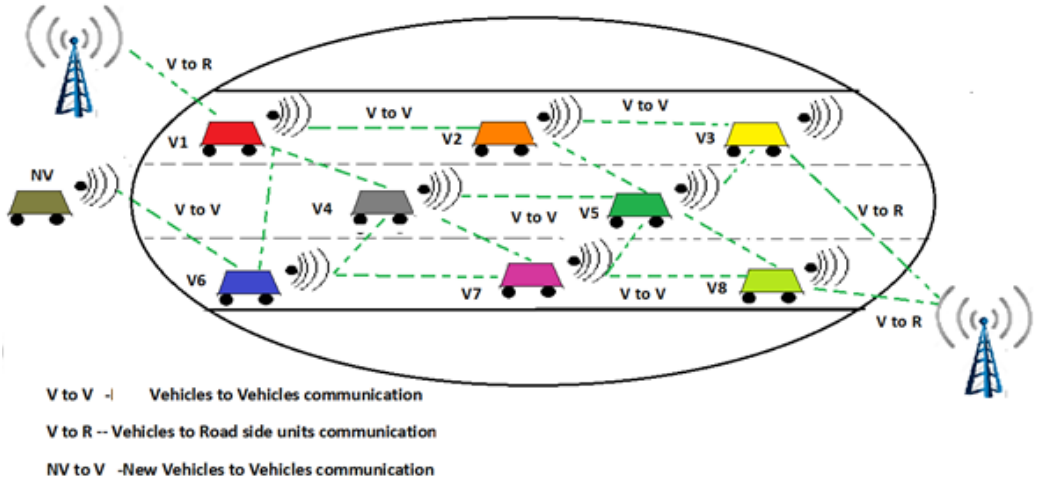

Fig. 2 Various Communication used in VANET

In the system model scenario, there is a network in which some authenticate nodes are communicating among themselves. Imposter nodes are attacking in the network and try to make identity attack and want to send the message to existing network. The authenticate nodes participate in communication once they are able to detect the imposter node, otherwise not.

Algorithm: IDBL protocol

Start
Imposter node attacks the node in the network
Imposter node access ID
for every accessed ID
for every Request
if (location present in buffer) // location present in the authenticate node
{
imposter node +=1; // Imposter node increase
}
else
{
authenticate node+=1; // authenticate node increase
}
end
detection percentage = (imposter nodes/total nodes) *100.

IV. Simulation and Results Analysis

We have simulated and implemented the algorithm for Imposter node detection through JAVA programming. The simulation focused on the detection of the imposter node and increasing the performance of the network. Considered simulation parameters are shown in Table I.

Fig. 3 shows snapshot of simulation environment where only blue coloured authenticate nodes are deployed. Every node has its own (X, Y) position or a unique location. Here, we may randomly choose any source node and it can communicate with the rest of nodes. Fig. 3 shows deployment of 10 true nodes in the network.

TABLE I
Simulation Parameters

Parameters	Values
Number of Node	10,20, 30
Node Deployment	Random
Number of Imposter node	10, 20, 30, 40, 50
Simulation Area	1000*1000
Simulation tools	NetBeans IDE J2SE

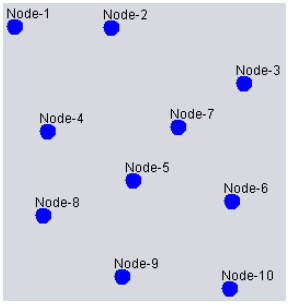

Fig. 3 Snapshot of Node deployment (Only Authenticated Node)

Fig. 4 shows the snapshot of imposter node and true node deployment. The nodes marked as red are imposter nodes. Firstly imposter node wants to break the security and privacy of the network. The existing nodes' ID's are randomly stolen by imposter node. Further they participate in the communication in the network. We have detected the imposter nodes through our simulation. The detection is fully based on the location. The detection of a number of imposter nodes may be increased if we increase the number of the authenticate nodes participating in the communication.

We have tested and investigated our method of imposter node detection with various cases of simulation.

Case-1: We fixed true node as node 10. We have gradually increased the number of imposter node and observed the detection of imposter node in various simulation runs. The result is presented in Table II as well as in Fig. 5.

In Fig. 5, we have shown the detection percentage of imposter node with respect to true node 10. From the result, it

is clearly visible that after the 15 imposter node as the number increases the detection percentage is also increasing. We have investigated our methodology for 30 imposter nodes.

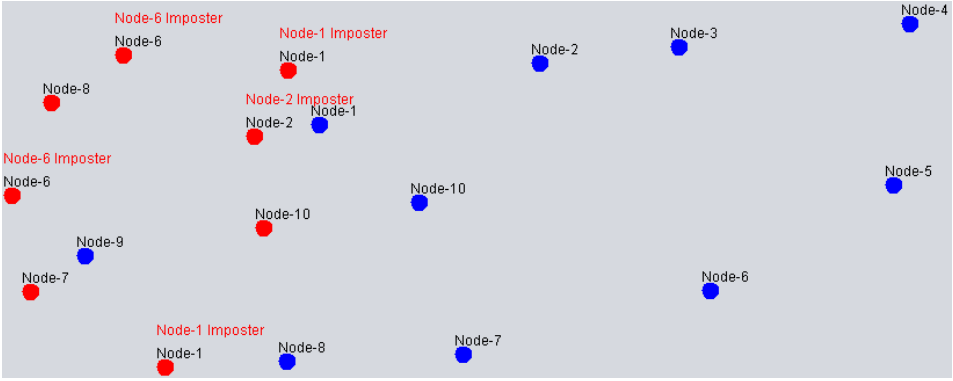

Fig. 4 Node deployment (Authenticated and Imposter Node)

TABLE II
IMPOSTER NODE DETECTION (WHEN TRUE NODE IS 10)

Number of Imposter Node	Number of detected Imposter Node	% of detection
5	3	60
10	5	50
15	7	46.60
20	15	50
25	23	60
30	23	76.66

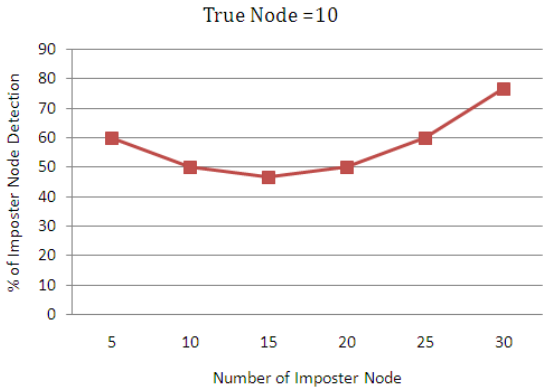

Fig. 5 Detection of imposter node in Case-1

Case-2: We fixed true node as node 20. We have gradually increased the number of imposter node and observed the detection of imposter node in various simulation runs. The result is presented in Table III as well as in Fig. 5.

TABLE III
IMPOSTER NODE DETECTION (TRUE NODE 20)

Number of Imposter Node	Number of detected Imposter Node	% of detection
5	2	40
10	4	40
15	7	46.66
20	10	50
25	16	64
30	22	73.33

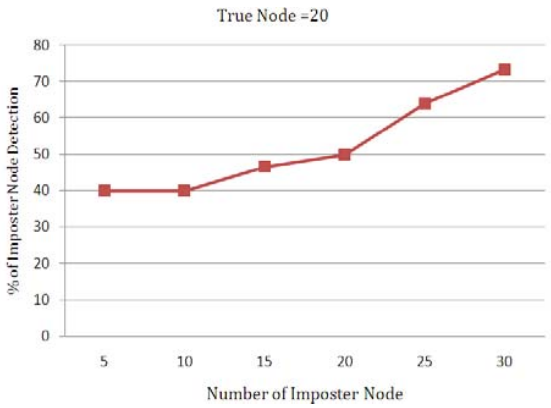

Fig. 6 Detection of imposter node in Case-2

In Fig. 6, we have shown the detection percentage of imposter node with respect to true node 20. From the result, it is clearly visible that after the 10 imposter node, as the number increases the detection percentage is also increasing. As we increase the network size and increase the source node communication, the percentage of detection of imposter nodes increases. We have investigated our methodology for 30 imposter node.

Through simulation it is observed that, in this protocol, if we fixed the number of imposter node and network size and increase iteration of attack on the network then it may be possible that it can detect more and more imposter nodes. As we know that here attacks are happening randomly, the detection of all imposter is not possible with few iteration. Otherwise much more iteration is needed to detect. There is a possibility that maximum number of imposters may be detected within few simulation iteration in random attack scenario. To investigate we have tested the same with 10 imposter and true node 10. The results are presented in Table IV and Fig. 7.

TABLE IV
IMPOSTER NODE DETECTION IN DIFFERENT ITERATION (TRUE AND IMPOSTER NODE 10)

Number of iteration	% of detection
1	50
2	60
3	60
4	90
5	60
6	50
7	70
8	60
9	80
10	80

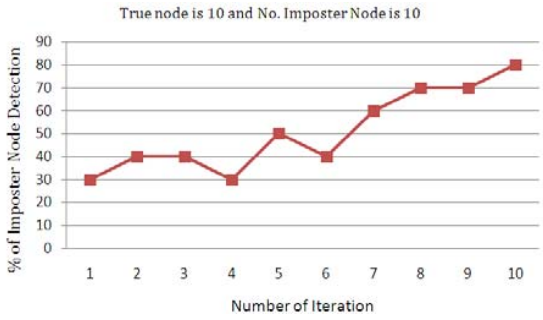

Fig. 7 Detection of imposter node percentage

V. CONCLUSION AND FUTURE DIRECTION

The position based algorithm for both ad-hoc and wireless sensor networks works in both dynamic and static scenario. In a decentralized environment of VANET, it really becomes a tough task to communicate between nodes. Due to dynamic topology of the networks, nodal communication, and efficient routing is a different task. This paper is mainly focused on an improving the network performance and increasing the detection of imposter by introducing this protocol. It is efficient in improving the performance the security and privacy of the network. Java technology is used here in implementing the protocol. On the basis of our research and analysis of simulation results, we draw the conclusion that this work is better in the present scenario. Our technique allows detecting the maximum number of imposters in the network. Hence, the protocol improves the performance of the networks in terms of probability of detection of imposters.

This work can be extended in future by considering a more dynamic traffic scenario. We can also consider the timestamp of the last message as the key to authenticate the next message from the same node. There are various many ways to make the VANET environment more secure and fruitful.

REFERENCES

[1] S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004.
[2] Moustafa, H., Zhang, Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).
[3] Yaseer Toor et al., "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, vol 10, No 3, pp. 74-88, 3rd quarter 2008.
[4] Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006;http://www.crhc.uiuc.edu/~yihchun/
[5] D. Sutariya, "Data Dissemination Techniques in Vehicular Ad Hoc Network," International Journal of Computer Applications, Volume 8– No.10, PP.35-39, October 2010.
[6] V. H. La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey," International Journal on Ad Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.
[7] A. Pathre, C. Agrawal, and A. Jain, "Identification of Malicious Vehicle in Vanet Environment from Ddos Attack," J. Glob. Res. Comput. Sci., vol. 4, no. 6, pp. 1– 5, 2013.
[8] U. Khan, S. Agrawal, and S. Silakari, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks," Procedia Comput. Sci, ICICT, Elsevier. vol. 46, 2014, pp. 965–972, 2015
[9] J. Newsome, E. Shi, D. Song and A. Perrig. The Sybil Attack in Sensor Networks: Analysis and Defenses. In Proc. of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004).
[10] Hussain R, Son J, Oh H. Anti Sybil: Standing against Sybil attacks in privacy preserved VANETs. In: International Conference on Connected Vehicles and Expo, IEEE; 2012. p. 108-113.
[11] C. Selva Lakshmi et al "Secured Multi Message authentication protocol for Vehicular Communication," International Journal of Advanced Research in computer and communication Engineering. vol-2, Issue 12, December 2013
[12] C. Zhang et al., "An efficient message authentication scheme for vehicular communication," IEEE Trans. Vehicular Technology, vol. 57, no. 6, pp-3357-3368, Nov. 2008.
[13] Dilendrashukla, Akash Vaibhav, Sanjoy das, Prashant Johri, "Security and attack analysis in VANET- A survey," to be published in the preceding of IEEE International conference on computing communication and automation (ICCCA 2016). 29-30 April 2016.
[14] R. K. Schmidt et al., "Exploration of Adaptive Beaconing for Efficient Intervehicle Safety Communication," In IEEE Network, vol. 24, Issues.1, pp. 14-19, Feb. 2010.
[15] Chen, Y., Jian, W.,& Jiang, W.(2009) "An improved AOMDV routing protocol for V2V communication," In IEEE intelligent vehicles symposium (IV"09, June 2009, pp. 1115-1120), 2009
[16] Tong Zhou et al., "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE Journal on selected areas in communications, Vol. 29, Issues. 3, pp. 582-594, March 2011.
[17] Manik Lal Das et al., "A novel remote user authentication scheme using bilinear pairings," In the proceeding of Elsevier computer and society, Vol. 25, Issues.3, pp. 184-189, 2006
[18] Ajay Rawati, Santosh Sharma and Rama Susil, "VANET: Security Attacks On Its Possible Solutions," Journal of Information and Operations Management, Vol. 3, Issue.1, pp.301-304, 2012
[19] Tyagi, Pand Dembla, D., "Investigating the security threats in Vehicular ad hoc Networks (VANETs): Towards security engineering for safer on-road transportation," International Conference on Advances in Computing, Communications and Informatics, pp. 2084 – 2090, Sept. 2014.
[20] Akash Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, Prashant Johri, "Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey", International Journal of Wireless and Microwave Technologies (IJWMT), Vol.7, No.3, pp.36-48, 2017.DOI: 10.5815/ijwmt.2017.03.04