International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Detecting Sybil Attacks using Proofs of Work and Location in VANETs

*[1]G Divya Vani, [2]Madapuri Rajeshwari, [3]Andhrapu Sindhuja
[1]Assistant Professor, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, India
[2,3] Students, Department of CSE, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:

Accepted: 20 April 2023
Published: 07 May 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
34-38

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) are gaining rapid momentum with the increasing number of vehicles on the road. VANETs are ad-hoc networks where vehicles exchange information about the traffic, road conditions to each other or to the road-side infrastructures. VANETs are characterized by high mobility and dynamic topology changes due to the high-speed vehicles in the network. These characteristics pose security challenges as vehicles can be conceded. It is critical to address security for the sake of protecting private data of vehicle and to avoid flooding of false data which defeats the purpose of VANETs. Sybil attack is one of the attacks where a vehicle fakes multiple vehicle identity to compromise the whole network. In this work, a direct trust manager is introduced which derives the trust value of each of its neighbor nodes at a regular interval of time. If the trust value is deviated, it confirms sybil attack. The proposed system is compared with the existing system to prove improved sybil attack detection ratio, thus providing better security. NS2 environment is used to prove the simulation results. The experimental results show that the attack detection ratio of SAD-V-DTC is 5 times better than that of the existing system. The packet delivery ratio shows an improvement of 27.27% while the false positive shows a good increase of 65.80% than the existing system.

Keywords: VANET, Sybil Attack, RSA Algorithm, Location Certificate, Direct Trust Calculation, AODV, NS2.

I. INTRODUCTION

VANETs offer communication among the moving vehicles and fixed infrastructure unit with the purpose of promoting comfort, safety, and efficiency. The decentralized nature and wireless communication medium bring numerous security threats to vehicular networks. Sybil attack is a serious threat in VANET where the malicious vehicle spoofs multiple identities in order to counterfeit the events for enhancing

driving experience personally. Sybil attack is difficult to identify as sybil nodes behave to be legitimate nodes and the attack is not visible until it becomes apparent to other vehicles. The Sybil attacker takes acquisition of the entire VANET operations and inserts false-hearted event information which results in erroneous decisions in vehicles. For instance, the VANET system produces a traffic event report based on information collected from numerous vehicles. Here, the traffic event report is deviated from the realistic situation when some of the vehicles are Sybil. Consequently, the Sybil attacker uses it for his own benefit and creates data inconsistency in the network. Location-based Sybil attack detection mechanism utilizes the motion pattern of vehicles in which the vehicles cannot fake other vehicles under different RSUs for attack detection. However, an ingenious attacker may compromise the RSUs for legitimate trajectories and also reinforce the attack level. Hence, it is crucial to detect the Sybil attack without revealing the location privacy and real identity without compromising both vehicles and RSUs. In order to improve attack detection and routing performance," Sybil Attack Detection in Vehicular Ad-hoc Networks using Direct Trust Calculation" (SAD-V-DTC) is proposed. The main objective of SAD-V-DTC is to improve attack detection ratio and increase packet delivery ratio. In this work, a direct trust manager is introduced which derives the trust value of each of its neighbor nodes at a regular interval of time. If the trust value is deviated, it confirms sybil attack. To further mitigate sybil attack, the sybil nodes are stored in blacklist. When a source node wants to communicate to another node, it checks the blacklist and bypasses the sybil route to reach the target node. By following this method, sybil node is detected quickly and malicious nodes are made aware to all the neighboring nodes in the network.

II. RELATED WORK

One of the most important characteristics of security is authentication. Every node has unique identity in the network. Sybil attack is an attack which compromises on authenticity of a node. An attacker fakes multiple identity of a legitimate node or even fake nodes for his personal benefit. The attacker misuses the identities to transmit false messages in the network or may limit the resources leading to DoS attack. This is a dangerous attack as it leads to other form of attacks as well like DoS, impersonation attack, bogus attack, etc. Different works are carried out in order to prevent or detect sybil attack in VANETs. Few of the works are discussed next. In order to preserve the privacy of vehicles like unique identity, location, driver details etc., pseudonyms are created. The pseudonyms are used in the message exchange rather than the original identity. However, the pseudonyms too can be compromised leading to sybil attack. In [3], the trusting authority distributes multiple pseudonyms for same vehicle to RSU. These multiple pseudonyms are hashed to a common value. Whenever the RSU encounters a vehicle with a pseudonym that does not belong to the pool of pseudonyms with a common hash value, it identifies that node as the attacker. It is important to note that this method works well as long as the RSU is not compromised. If RSU is compromised, then all the pseudonyms are comprised as sybil attack cannot be prevented. In [4], another sybil detection method is proposed by using footprint (locations traversed) of the vehicles as the main baseline. When a vehicle encounters RSU, it authorizes itself with proof of location at that particular time. The next RSU it encounters concatenated the proof of location at that point of time. This consecutive series of location information is called the trajectory of the vehicle. The RSU signs anonymously, thus preserving the privacy of RSU with respect to location and identity. This ensures that the RSU cannot be compromised. Another rule incorporated is temporarily linkable, which means that two messages are valid if they are generated by the same RSU within a given period of time. If the messages cross the given time period, they become invalid. When a vehicle wants to communicate information to RSU or another vehicle, the RSU checks

the trajectory and confirms it with other consecutive neighboring RSUs. If trajectory is found, it is a valid node, else it is a Sybil node and is removed from the network. In [5], a hybrid scheme is proposed which combines P2DAP [3] and footprint [4]. P2DAP performs better than footprint with the increase in number of vehicles while the footprint outperforms P2DAP when the speed of vehicles increases. Hybrid scheme was introduced with the intent of higher performance and higher detection rate. It works by applying footprint when the vehicle speed increased (if speed exceeds 40km/hr.) and applying P2DAP when the number of vehicles is more. In [6], a detection system for Sybil attack using each RSUs neighboring list, called IOAC (Infrastructure Observation-based Affinity Computation) is proposed. It uses fake IDs instantaneously to distinguish malicious nodes from legitimate nodes. This system is built on two evidences that observing two neighborhood RSUs identities at the same time tells that they are related, while observing two identities of two different neighborhood RSUs with no interconnected zone of communication range concurrently states that the two identities are not related. With this knowledge, IDs that are strongly involved to each other are found thus they might belong to the identical vehicle. In [7], an active algorithm for detecting sybil attack is proposed. After receiving a message from a suspicious node, the distance between the host node and the suspicious node is calculated, using the GPS coordinates. The transmission power to be used for the detection packet is calculated. Host node sends the detection packet. If detection packet does not cause a delay, then this node is labeled as sybil else new transmission power is calculated which excludes doubting node. If detection packet does not cause a delay, then this node is labeled as honest else it is a sybil node. In [8], a method for detecting sybil attack is proposed based on similarity measuring of RSSI time series. A vehicle sends the basic information on control channel periodically. Neighboring nodes will determine received signal strength indication value for each received packet. Each vehicle monitors the control channel and records all the latest messages within the observation time. For each packet, voiceprint stores the ID and received signal strength indication and for each received ID it generates RSSI time series. Each two RSSI time series is compared and distance is measured. If the distance between the nodes are closer to zero the it is marked as sybil nodes.

III. PROPOSED SYSTEM

In this work, the new scheme had been proposed which will be based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network. The Sybil attack can harm the network throughput and delay. The throughput of the network can be reduced because network resources get wasted. The delay can be raised because packets are routed to wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

1. The speed of the mobile nodes are fixed on the defined roads
2. The RSU's are responsible to maintain the information about all vehicles
3. The mobile nodes have to present its neighbour node information to RSU's
4. The RSU's can maintain the neighbour node information about all the nodes

The malicious vehicles can change its identity every time and send hello messages to RSU's for network join. The vehicles which are on the network can register itself with the server. In the registered information the unique vehicle number and its identification number will be defined. This registered information can be available on all RSU's. When any join the network, is have to send hello message to RSU and then RSU ask nodes for their identification number. When the identification number will be successfully verified the RSU gather all the information about neighbouring or adjacent nodes of the registered nodes. The RSU will also define the speed limit of the vehicle on the road

for which it is registered. When any malicious node can send hello message to RSU, the RSU will register the malicious node but when RSU checks the adjacent node and that are different from the legitimate node. The malicious node can be detected from the network. To verify the detection process, the RSU's will flood the monitor mode messages in the network , and adjacent nodes of the malicious nodes can start monitoring the malicious nodes and detect that it is the malicious nodes.

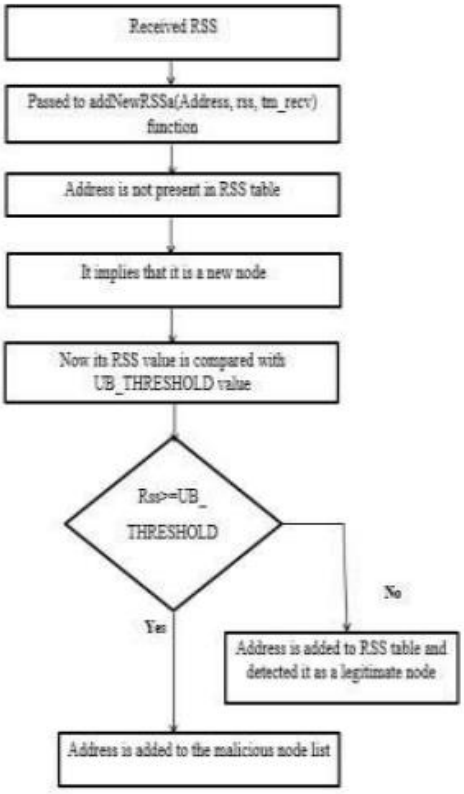

Fig.1.Overall flow graph of RSS

IV. RESULTS

To analyze the performance metrics in Network Simulator (NS2.35) of various true positive rate and false positive rate with different kinds of speed and density in the networks. The UB–THRESHOLD be around RSS value (in Watts) of some scenarios when a transmitter is stirring with 10 m/s speed; lower speeds thresholds will increase detection accuracy. The TIME–THRESHOLD is the typical (maximum) time in which a node should listen from another node, otherwise that identity will be measured as out of range or previous identity of a whitewasher. Shorter time intervals will rise identity revalidations in the network; while lengthy intervals will increase table sizes in network nodes. The LIST–SIZE is the maximum RSS records reserved for an identity or address.

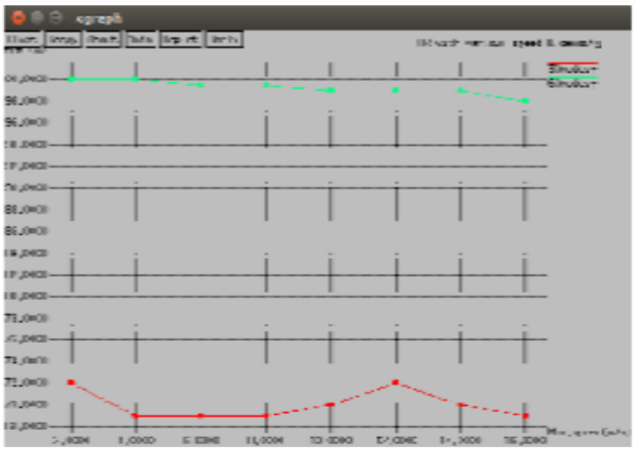

Figure 2 shows the true positive rate and maximum speed of the networks is high in nodes 60 and the true positive rate is less in nodes 30

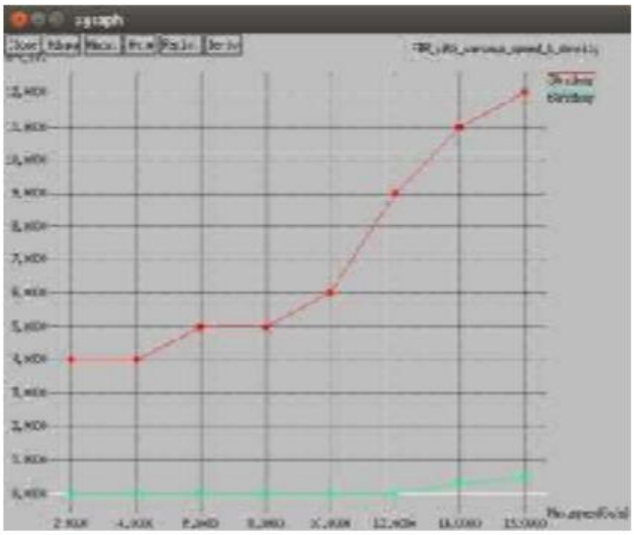

Fig.3. False Positive Rate

V. CONCLUSION AND FUTURE WORK

The vehicular adhoc network is the self configuring type of network in which vehicles can move freely on the roads. The vehicular adhoc network is the decentralized type of network in which vehicles can

join or leave the network when they want. Due to such type of network nature many malicious nodes may join the networks which are responsible to trigger various type of security attacks. The Sybil attack is most common type of attack in which malicious nodes can change its identification time to time. In this work, it is been concluded that Sybil attack reduced network performance in terms of throughput, delay and packeltoss. In this work, technique will be proposed which will be based on network information and monitor mode technique. The simulation is performed in NS2 and it has been analyzed that proposed technique will detect malicious nodes from the network in minimum amount of time. In future proposed technique will be applied for the detection of wormhole attack in the network.

VI. REFERENCES

[1]. Hugo Conceicao “Large-Scale Simulation of V2V Environments", SAC’08 March 16-20, 2008, Fortaleza,Cear´ a, Brazil, pp 28-33

[2]. Stephan Olariu"An Architecture for Traffic Incident Detection ", MoMM2009, December 14–16, 2009, Kuala Lumpur, Malaysia.

[3]. Jeong-Ah Jang "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-ofSightand/or Traffic-Violation-Prone Environment", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, pp 1-11

[4]. Maxim and jean-Pierre Hubaux “The security of vehicular ad hoc networks”,ACM,2005

[5]. SumaiyaIqbal"Vehicular Communication: Protocol Design, Testbed Implementation and Performance Analysis", IWCMC’09, June 21-24, 2009, Leipzig, Germany, pp 410-415 A. AHMAD "Hybrid Multi-Channel Multi-hop MAC in VANETs ", MoMM2010, 8–10 November, 2010, Paris, France, pp 353-357

[6]. Rakesh Kumar, Mayank India “ A Comparative Study of Various Routing Protocols in VANET, 2012 pp 1-12

[7]. JosianeNzouonta et al “ Routing on City Roads using Real-Time Vehicular Traffic information 2008, p-18.

[8]. Y. Yao et al., "Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs," 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, Denver, CO, 2017, pp. 591-602.

[9]. J. Jenefa, E. A. Mary Anita,” Secure Vehicular Communication Using ID Based Signature Scheme,” Springer Science+Business Media, 2017.

[10]. T. M. de Sales, H. O. Almeida, A. Perkusich, L. de Sales and M. de Sales, "A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks," 2014 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, 2014, pp. 426-427.

Cite this article as :

G Divya Vani, Madapuri Rajeshwari, Andhrapu Sindhuja, "Detecting Sybil Attacks using Proofs of Work and Location in VANETs", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 10 Issue 3, pp. 34-38, May-June 2023.

Journal URL : https://ijsrset.com/IJSRSET2310310