International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 9, pp: 520-526www.ijaem.net ISSN: 2395-5252

Sybil Attack Detection Technique for Vehicular Ad Hoc Networks

RandeepKaur, Er. Yadvinder Singh
Department of Computer Science and Engineering
BhaiGurdas Institute of Engineering & Technology, Sangrur, Punjab, India

Date of Submission: 15-11-2020 Date of Acceptance: 28-11-2020

ABSTRACT: The vehicular adhoc networks are the self configuring and de-centralized type of network in which no central controller is present. The vehicle nodes have high mobility due to which path establishment from source to destination is the major issue in the network.This forces the vehicle to choose another path and leave the road which is a benefit for the attacker. In the recent times, various technique has been proposed for the detection of malicious nodes from the network. The proposed technique is based on promiscuous mode and distance based technique. The simulation is been performed in Ns2 and results shows that purposed technique shows good results in terms of various parameters.

Keywords:VANET, Sybil, Distance Method,Beacon

I. INTRODUCTION

The VANET is generated when a group of vehicles such as mobiles or stationary vehicles were interconnected using a wireless network. The major significant aspect of VANETs is to give the comfort and safety to the drivers that are present in the vehicular scenarios. The vehicular ad-hoc networks are regarded as an infrastructure for an intelligent transportation system due to increasing number of vehicles that are autonomous. In a smart city, the VANETs comprise in every activity in which Internet connectivity is utilized.The processing and wireless communication is obtained for which this network has potentiality [1]. Various opportunities are provided using this network for robust applications. Vehicles and road safety, traffic competence, optimization of vehicular traffic and ITs are comprised in these applications. The data is shared among the vehicles in the vehicular ad-hoc networks to offer the security and ease to the drivers.In general, the implementation of Vehicle-to-road infrastructure and Vehicle-to-broadband cloud performs through wireless technology that is known as DSRC. This technology is carried out for recognizing and creating communication by means of speedy moving objects in limited physical range by an individual. The data information is transferred easily in this technology in actual manner [2]. The voice, image are comprised in this information. The connection is established among the vehicles and the frameworks are supported in organic way with the help of Dedicated Short-range Communication. There are various advantages of this technology. For instance, this technology is helpful for reducing congestion and accidents as result, the traffic condition is enhanced. Various amenities are provided using connection that is available between vehicles and the supporting framework. The reporting of traffic information, support while driving and timely warning that ensures the driving safety are comprised in these amenities.The networks are left vulnerable to Sybil attack after utilizing the wireless mode of communication. The occurrence of Sybil attack in vehicular networks is found when a number of identities are obtained by the malicious vehicle or road-side units. A Sybil attacker applies different fake identity on multiple messages that are sent to other vehicles in queue. In this way, the confusion is made among another vehicle that is available in same track.

The two basic kinds of nodes are:

- Malicious node: Nodes that prank the identities of other nodes.
- Sybil node: The malicious node that produces the additional identities to the attack is called Sybil attack. The actually existing node ($S \subset N$) and outside the network node ($S \not\subset N$) are the two kinds of Sybil nodes in which N is used to illustrate the set of all vehicles and the collection of Sybil nodes is characterized by S [3].

The mode of shared wireless communication is utilized to transmit the messages. As a result, the additional identities are stolen and fabricated by Sybil attacker so as the attack is launched.There are some network services that are affected by Sybil node. These services include routing, congestion in network and allocation of resources. Due to this, the performance as well as service excellence of the networks is reduced. The effect Sybil attack can observe on some protocols and applications in VANETs. These affects are describes as:

- In generating routes, its appearance is noticed on several places that causes disturbance in multipath or geographic routing algorithms of route generation. The head selection mechanism is disturbed by it in the routing protocols that are based on cluster.
- The essential information is collected and determined for several applications with the help of voting system. The results that achieve from voting are changed by Sybil nodes while recognizing the node's behavior and verifying the position of vehicles [15].
- The fake IDs are executed by the attacker after provocation of malicious behavior with spreading actions.
- The numerous IDs are employed to control the internet polls and prepare a result in the favor of it.
- There are numerous IDs as a result the allocation of resources is affected by Sybil node and the unfair share of resources is acquired.
- There is a reduction in the trust of authorize node because of Sybil attack.

II. LITERATURE REVIEW

Anu S Lal, et.al (2015) analyzed that two main concerns of Vehicular Ad-hoc Networks were security and privacy. The majority of privacy preserving schemes had prone to Sybil attack as many identities were created by a malicious user for simulating numerous vehicles. The enhancement of the scheme CP ^{2} DAP was suggested in this paper [16]. The central authority and a set of fixed nodes that were known as RSUs were collaborated in this scheme for detecting the Sybil attacks. In the modification, the collaborative scheme based on the region authority was suggested for Sybil attacks detection. The bloom filter had employed for the prevention from further attacks of malicious vehicles. In this scheme, there was not any necessity to reveal the identification of any vehicle to detect the Sybil attack. Thus the privacy was protected.

MandeepKaurSaggi, et.al (2015) suggested a new method for Sybil attack detection and isolation on vehicles that provided the network capability [17]. This method had two phases. The nodes were registered after the recognition of their credentials by road-side units, in the first phase. The second phase had started when they were succeeded in verification. The identification was assigned to the vehicles in second phase. The road-side units defined the threshold speed limit to the information that was collected from the neighboring nodes. It had been verified by the RSU that the threshold value was exceed the speed limit. The Sybil attack produced manifold identities that damaged the network. The wrong information was overflow by misusing these identities on the network. It was observed in the simulation outcomes that the probability for detection had maximized and the percentage of Sybil attack had diminished using the suggested method.

Shikha Sharma, et.al (2016) analyzed that the Sybil attack was an encounter that was utilized to contaminate the personality of an attacker into multiple incognito personalities [18]. The route of network was constructed by it. The timestamp approach had introduced for Sybil attack that was in associated system, the network that was self-correlated and the cordial network system. The evaluation of various methods was done so as the Sybil attack was mitigated. The timestamp approach had suggested for detecting and preventing the Sybil attack. The results achieved from this approach had compared with the EBRS Approach. The suggested approach outperformed to earlier approach.

SupinderKaur, et.al (2016) examined that Vehicular Ad-hoc Networks were self configuring networks in which vehicles and roadside structure elements were gathered together [19]. These roadside structured elements had connected with each other and there was not any infrastructure, information of current traffic situation to sending and receiving needed. To communicate among mobile vehicles, these elements were utilized. The attacks, authentication and so on were few security concerns that had included in it. Several attacks that had set off in VANET as well as the Sybil attack along with its impacts on the networks had described in this paper.

HarvinderKaur, et.al (2016) studied that privacy and security were two main concerns in vehicular ad hoc networks [20]. The more time was taken for the authentication as the environment in VANETs was very powerful. A number of techniques were inclined towards the Sybil attacks simultaneously to preserve the privacy. This paper suggested a lightweight authentication technique. A secure communication system had described using this scheme in vehicles, RSUs and vehicles to other vehicles. In the vehicular ad hoc networks, the privacy as well as verification of anonymous legitimate nodes was required the most. However, there were many scheme related to privacy preservation that were aware of Sybil attacks. It was very challengeable to prevent and detect the Sybil attacks within the privacy-friendly environment of vehicular network. This technique carried out the timestamps scheme. In crowded traffic areas, the minimum computing rate was evaluated during authentication. The actual status of vehicle was not to be disclosed to protect the vehicles' privacy.

Hamid Hamed, et.al (2018) recommended a novel RSU support based method to detect the Sybil attacks and the attackers in VANETs [21]. The two vehicles were passed simultaneously by multiple roadside units was regarded as a rare coincidence. Two IDs were examined in the locality of different Road-side units. It was observed in the examination that these identities were belonged to various vehicles. It was confirmed using these two facts whether the Sybil attack was executed or not. The routine communications were carried out amongst the nodes and Road-side units in the suggested method for detecting the attackers. It had observed in the outcomes of simulation that the suggested method acquired better performance concerning detection rate and false positive rate than the existing schemes. Two IDs were examined in the locality of different Road-side units. It was observed in the examination that these identities were belonged to various vehicles.

KhaledRabieh, et.al (2015) suggested that a cross-layer scheme in which Sybil vehicles were recognized with Road Side Units [22]. This technique had determined the locations of vehicles as Sybil vehicles were present at the location that they claimed. The directional antenna was employed for sending the claimed location of vehicle by a challenge packet. The challenge was received and the response was sent back when the vehicle was present at the location that was expected. If there was any suspicion of Sybil attack, the packets were sent rather than sending the challenge packets every time so as the overhead was diminished. Various Sybil attack methods were described. The maximum detection rate had achieved in the results from this suggested technique and only low possibility of false alarm had achieved using this technique. The suitable communication and computation overhead was needed for this technique.

Mohamed Khalil, et.al (2018) analyzed that the subset of MANETs was the Vehicular Ad-hoc Networks [23]. The capability of inter-communication among vehicles was described by arranging these networks as they ensured the security. The services for people during the driving had been provided by these networks. The VANET had utilized to represent the various attacks such as Sybil attacks, ID disclosure and spoofing. A new technique was suggested in this paper to deal with the Sybil attack. The encryption of symmetric key was carried out in this suggested protocol technique. The RSUs and vehicles on the road were also validated in this technique that ensured that one identity was not manipulated by one malicious inside the network. The managers for RSUs or CA were not required in this protocol. The least messages were exchanged with Road Side Units to create effectiveness of the suggested technique.

III. RESEARCH METHODOLOGY

The vehicular ad hoc network is dynamic type of network in which malicious nodes can enter or leave the network according to their requirements. The mobility of the vehicular ad hoc network is very high due to which nodes change its location frequently. The research work is based on the detection and isolation of Sybil attack from vehicular ad hoc network. The proposed methodology is based on the two step verification. In the first step, the vehicle which is creating intrusion is marked and in the second step actual malicious node gets detected from the network. In the proposed scheme, the road side units flood the beacon frames in the network. When the beacon frames get flooded into the network, every vehicle node which is present in the network needs to reply back with its identification id. The road side units calculate distance to vehicle node based on the formula given in equation 1

Distance =Speed * Time ------- (1)

In the equation 1, the signal propagation time is fixed and time is the delay time in the network. The time is calculated when beacon packet sent in the network and when vehicle send reply to road side unit. When the Sybil attack is triggered in the network, two vehicle nodes have same identification number and due to which road side units calculate two distances of single node which represents intrusion in the network.

In the second step, malicious node gets identified from the network using promiscuous mode technique. Every wireless device have two mode which are operating mode and promiscuous mode. In the promiscuous mode node watch activity of its adjacent node and in the operating mode node access internet services. The nodes change its mode to promiscuous mode and watch which node changed its identification recently. The node which changes its identification recently will be marked as malicious node from the network.

Proposed Algorithm

Initialization

1. V= Network, S=Source, D=Destination, n=node id

Location and Path update

1. Calculate Range=$\sqrt{2\text{hr}}$
2. Calculate Location=$\sqrt{(\text{x}1 - \text{z})^2 + (\text{y}1 - \text{y})^2}$
3. Distance =Speed * Time
4. If Location similar and range high accepted

Define Zone Z

Malicious Node Detection

Mark Intrusion

Change network operation to promiscuous mode

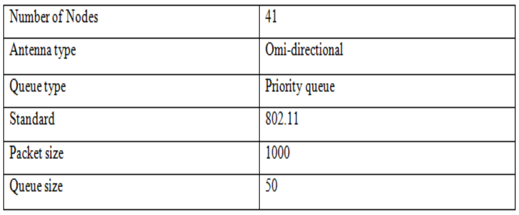
Node which change its identification recently is marked as malicious

S transmit data to D from established path

IV. RESULT AND DISCUSSION

NS2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic

Table 1: Simulation Parameters



Number of Nodes	41
Antenna type	Omi-directional
Queue type	Priority queue
Standard	802.11
Packet size	1000
Queue size	50

There are a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. In this thesis, we follow the general ideas described in RFC 2501, and we use four quantitative metrics. The packet delivery ratio and average end-to-end delay are most important for best-effort traffic. The other two qualitative metrics used in this thesis are and throughput.

- **Throughput**

The throughput is defined as the fraction of all the received data packets at the destinations over the number of data packets sent by the sources. This is an important metric in networks. If the application uses TCP as the layer 2 protocol, high packet loss at the intermediate nodes will result in retransmissions by the sources that will result in network congestion.

$$\text{Throughput} = \frac{\text{Total data packets recieved}}{\text{Total data packets sent}}$$

- **Average End-to-End Delay**

End-to-end delay includes all possible delays in the network caused by route discovery latency, retransmission by the intermediate nodes, processing delay, queuing delay, and propagation delay. To average the end-to-end delay we add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets. This metric is important in delay sensitive applications such as video and voice transmission.

$$\text{Average End to end delay} = \sum \frac{(\text{time received} - \text{time sent})}{\text{total data packets received}}$$

- **Overhead**

Ad hoc networks are designed to be scalable. As the network grows, various routing protocols perform differently. The amount of routing traffic increases as the network grows. An important measure of the scalability of the protocol, and thus the network, is its routing overhead. It is defined as the total number of routing packets transmitted over the network, expressed in bits per second or packets per second. The causes of routing overhead are network congestion and route error packets.

- **Packet loss**

The packetloss is the parameter which counts the number of packets which get lost in the network.

$$\text{Packet loss} = \text{number of packewts sent} - \text{number of packets recieved}$$

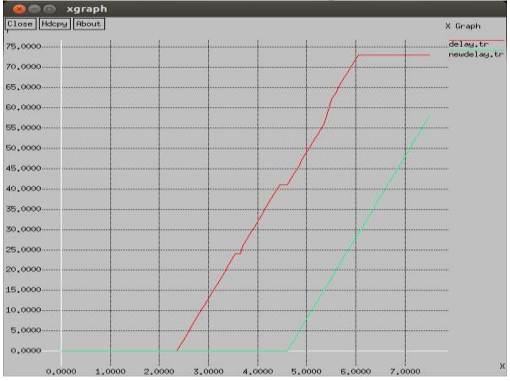


Fig 1: Delay Comparison

As shown in figure 14, the delay of the proposed and existing technique is compared and it is been analyzed delay of the proposed technique is reduced isolation of Sybil attack in the network

Table 2: Delay Analysis

Time	Proposed Technique	Existing technique
4.5 second	6 packets	46 packets
6 seconds	25 packets	70 packets
7 seconds	58 packets	75 packets

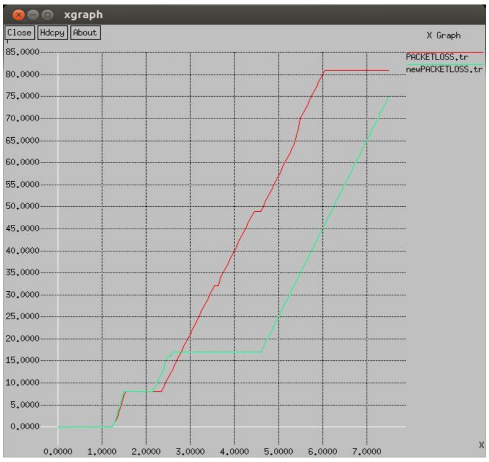


Fig 2: Packetloss comparison

As shown in figure 2, the packetloss of the proposed and existing technique is compared and it is been analyzed that network packetloss is reduced when Sybil attack is isolated from the network

Table 2:Packet loss Analysis

Time	Proposed Technique	Existing technique
4.5 second	16 packets	45 packets
6 seconds	45 packets	70 packets
7 seconds	65 packets	85 Packets

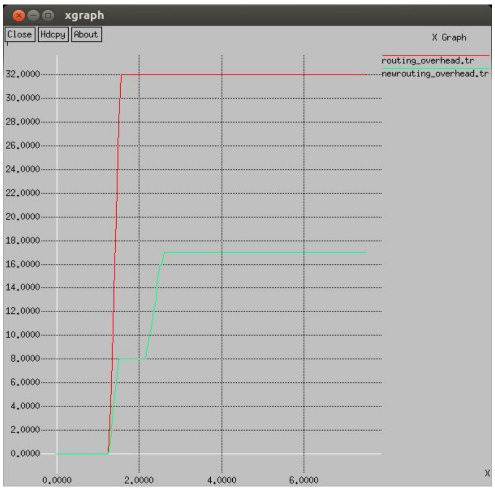


Fig 3: Routing overhead

As shown in figure 3, the routing overhead is the parameter which measures the extra number of packets which are transmitted in the network. The routing overhead in the network is reduced when attack is detected and isolated from the network

Table 3: Routing Analysis

Time	Proposed Technique	Existing technique
4.5 second	16 packets	30 packets
6 seconds	17 packets	32 packets
7 seconds	18 packets	32 Packets

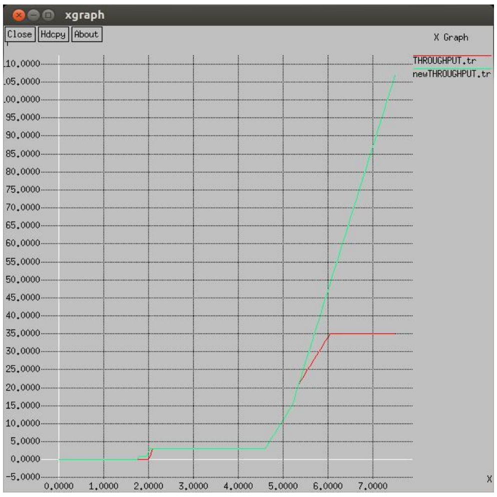


Fig 4: Throughput Comparision

As shown in figure 4, the throughput of the proposed and existing technique is compared and it is been analyzed that after the malicious node isolation the network throughput is increased at steady rate

Table 4: Throughput Analysis

Time	Proposed Technique	Existing technique
4.5 second	25 packets	20 packets
6 seconds	55 packets	35 packets
7 seconds	37 packets	105 Packets

V. CONCLUSION

In this work, it is been concluded that broadcasting is the technique which is applied to select efficient path from source to destination. Due to decentralized nature of the network, some time malicious nodes join the networks which are responsible to trigger various type of active and passive attacks. This work is based on to detect malicious nodes from the network which are responsible to trigger sybil attack in the network. The simulation of the proposed technique is been done in Ns2 and results shows that performance is increased in the network

REFERENCES

[1]. SabihurRehman, M. Arif Khan, Tanveer A. Zia, LihongZheng, “Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges”, Journal of Wireless Networking and Communications, volume 3, issue 3, pp 29-38

[2]. M.NewlinRajkumar, M.Nithya, P.HemaLatha, “Overview of VANET with its Features and Security Attacks”, 2016, International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 01

[3]. Deeksha, Ajay Kumar, Manu Bansal, “A Review on VANET Security Attacks and Their Countermeasure”, 2017, Proceedings of the 4th International Conference on “Signal Processing, Computing and Control

[4]. Irshad Ahmed Abbasi, and Adnan Shahid Khan, “A Review of Vehicle to Vehicle Communication Protocols for VANETs in the Urban Environment”, 2018, Future Internet

[5]. Marvy B. Mansour, CherifSalama, Hoda K. Mohamed and Sherif A. Hammad, “VANET SECURITY AND PRIVACY – AN OVERVIEW”, 2018, International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.2

[6]. Mohammed Ali Hezam Al Junaid1, Syed A. A1, MohdNazriMohd Warip1, Ku NurulFazira Ku Azir1, NurulHidayahRomli, “Classification of Security Attacks in VANET: A Review of Requirements and Perspectives”, 2018, MATEC Web of Conferences

[7]. Ram Shringar Raw, Manish Kumar, Nanhay Singh, “SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET”, 2013, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5

[8]. F. Sabahi, “Impact of Threats on Vehicular Adhoc Network Security”, 2012, International Journal of Computer Theory and Engineering, Vol. 4, No. 5

[9]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, “Security Analysis of Vehicular Ad Hoc Networks (VANET)”, 2010, Second International Conference on Network Applications, Protocols and Services

[10]. Mina Rahbari and Mohammad Ali JabreilJamali, “EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET”, 2011, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6

[11]. Amit A. Mane, “Sybil attack in VANET”, 2016, International Journal of Computational Engineering Research (IJCER), Volume 06, Issue 12

[12]. K.Selvakumar, S.Naveen Kumar, “Security Issues and ANALYSING Sybil Attack Detection in VANET”, 2019, International Journal of Recent Technology and Engineering (IJRTE), Volume-7 Issue-5

[13]. HarsimratKaur, PreetiBansal, “Efficient Detection & Prevention of Sybil Attack in VANET”, 2015, International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9

[14]. MukulSaini, Kaushal Kumar2 and Kumar VaibhavBhatnagar, “Efficient and Feasible Methods to Detect Sybil Attack in VANET”, 2013, International Journal of Engineering Research and Technology, Volume 6, Number 4, pp. 431-440

[15]. Zaid A. Abdulkader, Azizol Abdullah, MohdTaufik Abdullah, Zuriati Ahmad Zukarnain, “A Survey on Sybil Attack Detection in Vehicular Ad hoc Networks (VANET)”, 2018, Journal of Computers Vol. 29 No. 2, pp. 1-6

[16]. Anu S Lal, Reena Nair, “Region authority based collaborative scheme to detect Sybil

attacks in VANET", 2015, International Conference on Control Communication & Computing India (ICCC)

[17]. MandeepKaurSaggi, RanjeetKaur, "Isolation of Sybil attack in VANET using neighboring information", 2015, IEEE International Advance Computing Conference (IACC)

[18]. Shikha Sharma, Shivani Sharma, "A defensive timestamp approach to detect and mitigate the Sybil attack in vanet", 2016, 2nd International Conference on Contemporary Computing and Informatics (IC3I)

[19]. SupinderKaur, Anil Kumar, "Techniques to isolate sybil attack in VANET-A review", 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)

[20]. HarvinderKaur, MandeepDevgan, Parminder Singh, "Sybil attack in VANET", 2016, 3rd International Conference on Computing for Sustainable Global Development (INDIACom)

[21]. Hamid Hamed, AlirezaKeshavarz-Haddad, ShapourGolbaharHaghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support", 2018, Electrical Engineering (ICEE), Iranian Conference on

[22]. KhaledRabieh, Mohamed M. E. A. Mahmoud, Terry N. Guo, Mohamed Younis, "Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs", 2015, IEEE International Conference on Communications (ICC)

[23]. Mohamed Khalil, Marianne A. Azer, "Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks", 2018, Wireless Days (WD)