ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

Prevention of Sybil attack in vehicular ad hoc networks using active route timeout approach

Preeti rawat[1] Shikha Gupta[2]
M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India[1] Assit. Prof., Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India [2]

ABSTRACT

Nowadays VANET is most popular topic for the researchers and technological industries whosoever is having potential in improving the traffic safety and increasing efficiency, because a large number of accidents are taking place every year. Security is a major issue in Ad-hoc networks, as high mobility of nodes creates difficulty in security of networks. Vehicular ad-hoc networks uses wireless communication links to communicate with each other. VANET makes many things easier for users and decreases the number of accidents, helps in knowing the route situation; on the above VANET has many safety and non safety applications. There are many attacks which affect VANET but Sybil attack is one of the most serious types. It is a threat to these networks due to need of a distinctive, individual and persistent identity per node plus absence of central identity management. A Sybil attacker can affect to the ad hoc networks in many ways. This paper present active route timeout concept to detect performance improvement of AODV routing protocol for Vehicular Ad hoc Network. AODV protocol is simulated using OPNET Modeller v14.5 with varying number of mobile nodes.
Keywords*:* VANET, Active Route Timeout, AODV.

I. INTRODUCTION

In an ad hoc network, there is no fixed infrastructure such as base stations or moving vehicles. Moving vehicles are considered as nodes that are within each other's radio range and they can communicate directly via wireless links, while those that are far away are depending upon other nodes to relay messages as routers. High node mobility in an vehicular ad hoc network causes frequent changes of the network topology. VANET is designed for Vehicular to vehicular (V2V) and Vehicular to Infrastructure (V2I) and vehicular to roadside units (V2R) communication [7]. Security in VANETs is important, because the message sent by one vehicle might have important consequences such as accident prevention. AODV (Reactive ad hoc network routing protocol) attempt to minimize the route discovery overhead by caching the route information for some period of time after a connection expires. How long each node should keep this route information is set a priority, and usually arbitrarily.

This paper is divided in VI sections; section II describes Sybil attacks in VANET, section III describes Literature review, section IV gave proposed work, section V is description of simulation parameters, section VI shows results and the last section VII conclusion.

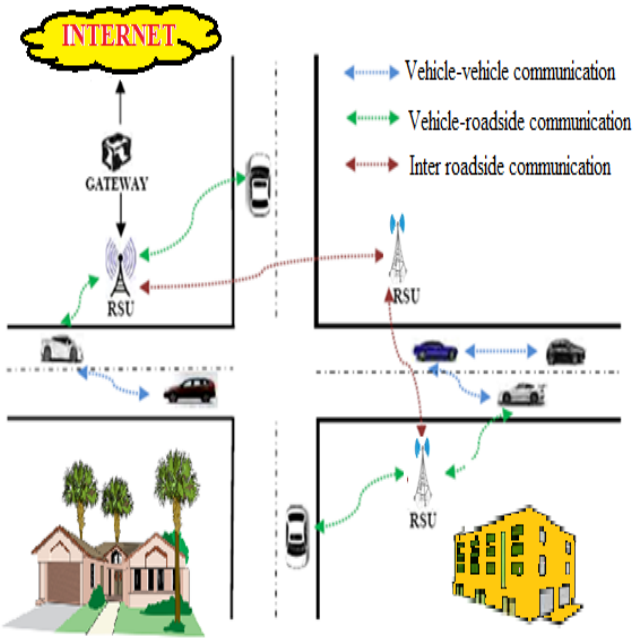

Fig 1: Architecture of VANET

This architecture of VANET, describes that vehicles are considered as nodes which can move freely with high mobility within a network and stay connected, even if they are at high speed. Each vehicle can communicate with other vehicle via DSRC (Dedicated Short Range Communication).

VANET has many applications divided into two parts Safety and Non-Safety applications [10]. These applications include distribution of multimedia information and traffic control. When VANET is used in traffic control, it helps in avoiding accidents by sharing information about the situation of road, such as road congestion and traffic accidents Therefore, it manages city traffic, reduce number of accidents by informing the users about it and improve safety with high efficiency and high mobility[4]. Due to high mobility topology tends to change frequently. It can also helps to share some information between vehicles,

such as weather forecast, petrol pumps, and restaurant addresses, music or video download services. It also allows a lot of value added services like automated toll payment, location based services like finding closest restaurant, travel lodge, fuel station.

II. SYBIL ATTACK

In this attack, a node sends multiple messages to alternative nodes and every message contains a special fake identity. The main goal of the attacker is to produce illusion to alternative nodes by sending wrong messages and to confuse alternative nodes on the road to change their way and go away from the road for the advantages or benefit of the attacker. This attack is very dangerous in routing because a node can claim to be in several positions at the same time. There are some of the criteria which should be followed for ensuring security in ad- hoc networks:
Availability: All the services should function well and should be available to each and every node.
Confidentiality: Some data is only be used by Authorized users.
Integrity: data received and sent will be same.
Non repudiation: sender and receiver can't deny of sending and receiving data.
Authentication: each and every node in the network must be real.

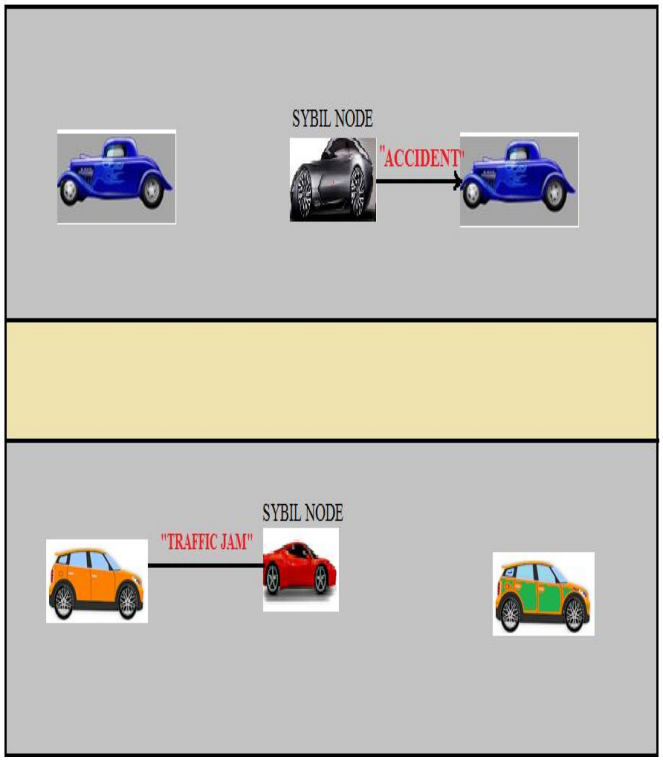

Fig 2: SYBIL ATTACK

III. LITERATURE REVIEW

AUTHOR	DESCRIPTION
Sohail et al [18]	The author proposed a lightweight scheme to identify the Sybil nodes by deprived of using centralized trusted third party or any extra hardware, such as a geographical positioning system or directional antennae.
E.A. Mary [6]	This author proposed a certification based localized authentication scheme for the prevention of VANET from Sybil identities
Wenyu et al[16]	The author proposed a model which is called a two-class undirected assorted association stochastic block models to discover opponent's Sybil identities within the network. The model make differences between the Sybil identities.
Kuo-Feng et al [7]	The author developed a scheme in which verification of node identities is done through analysing the information of neighbouring node each node in order to protect WSNs against such Sybil attack.
Arpita M.bhise[8]	The author presents an Improved Genetic Based Routing Protocol for VANETs, using spanning tree and routing tree. The main goal of this author is to decrease the delay from source to destination node by using genetic algorithm.
Wagan, A. A., et al.[19]	The author Presented a hardware based security framework that uses both standard asymmetric PKI and symmetric cryptography for faster and secure safety message exchange.
Anuradha Singh et al[4]	The author overview of the vehicular ad hoc networks, its standards, applications, security issues and the existing VANET routing protocols.
liang xiao et al.;[9]	The author proposed a mechanism to detect the Sybil nodes in WSN using the concept of channel based mechanism. The performance of Sybil detector is measured by field measurements and propagation modeling software.

IV. Proposed work

In our proposed algorithm we show the effect of different parameters on energy consumption through routing QoS. First we take an example of Active route time out, Hello Interval and Time-To-Live. The constant value is used to modify the values of the parameters. First of all Set Active Route time as any value X, Hello Interval as any value Y and TTL as any value T and calculate the results of Quality of service(Q) and routing results for that value X, Y and T. After taking the previous value suppose a constant value is added in the value of Active Route Timeout and Hello Interval so that the value becomes X' and Y'. Then again the simulation takes place in different scenarios and calculates the result of QoS(Q') for X', Y' and T. Compare both the results of QoS i.e. Q and Q'. If Q' is better than Q then the optimized value of Active Route Timeout(X') and Hello Interval(Y') is obtained. If not, then the optimized value of Active Route Timeout and Hello Interval is X and Y. Now, add a constant value to TTL and apply it on better results of QoS (either Q or Q') to obtain a new QoS(Q''). Compare it with previously obtained improved QoS. If better results are obtained, then optimized value of TTL is taken as T' else it is T.
Below is given the flowchart of proposed algorithm:

Step 1: Start and take active route timeout=X and hello interval=Y.
Step 2: SET X'=X+x and Y'=Y+y .
Step 3: Run and analyze the results.
Step 4: Calculate QoS of VANET of X and Y for Q.
Step 5: Run and analyze results.
Step 6: After comparison if Q' is better than Q then replace the values.
Step 7: If results are not improved go to step 2, otherwise
Step 8: End

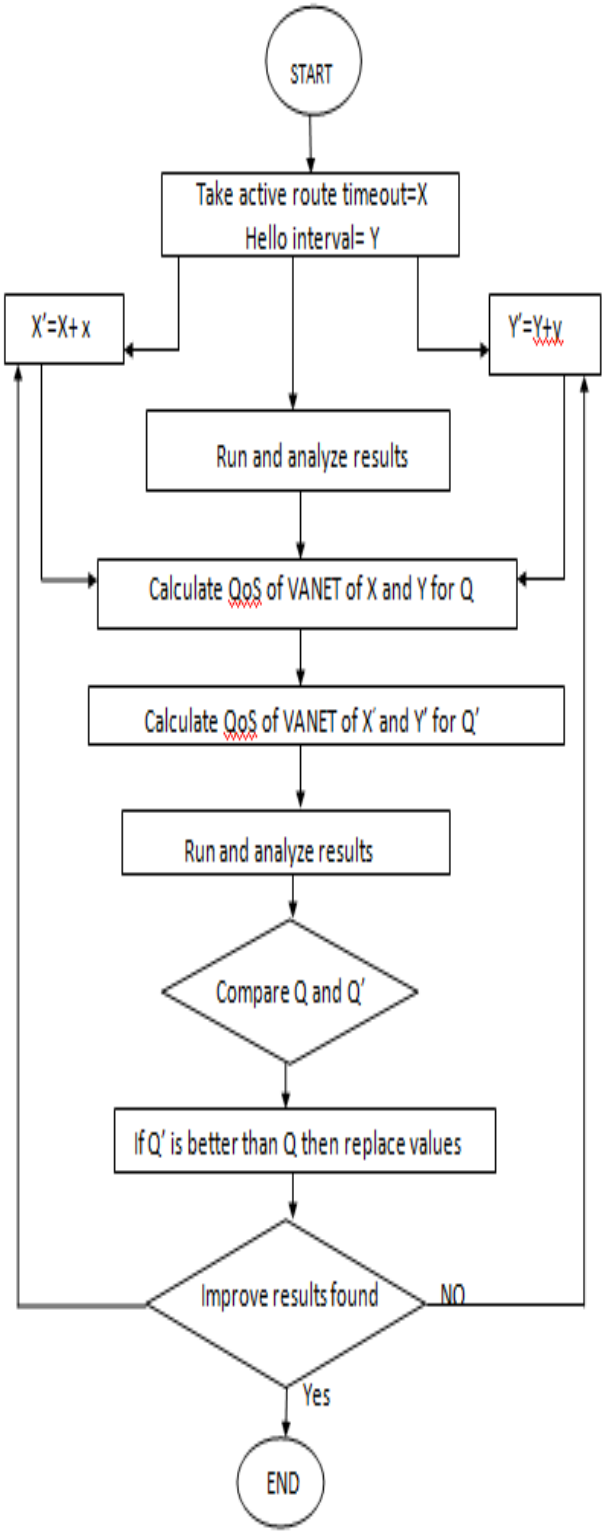

Fig 3: flowchart of proposed algorithm

V. SIMULATION PARAMETERS

Simulation Parameters	
Examined Protocols	AODV
Number of Nodes	150, 200
Types of Nodes	Mobile
Simulation Area	1500*1500 meters
Simulation Time	1200 seconds
Mobility	10 m/s
Pause Time	100 seconds
Performance Parameters	Throughput, Delay
Traffic type	FTP
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Wireless LAN MAC Address	Auto Assigned
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	256
Packet-Reception Threshold	95
Long Retry Limit	4
Max Receive Lifetime(seconds)	0.5
Buffer Size(bits)	256000

VI. RESULTS

Scenario 1 represents the mitigation of Sybil attack and implementation of the proposed method, scenario 2 represents the network that is under the Sybil attack and Scenario3, represents the scenario with no malicious event and normal network state.

Throughput: Throughput can be defined as the ratio of the total amount of data reaches a destination from the source. The time it takes by the destination to receive the last message is called as throughput. It can express as bytes or bits per seconds (byte/sec or bit/sec). There are some factors that affect the throughput such as; changes in topology, availability of limited bandwidth, unreliable communication between nodes and limited energy.

There are two main scenarios in which the first scenario comprises of 150 mobile nodes and the latter holds 200 mobile nodes. In each scenario, we performed two simulations of a regular network operation in VANET and a VANET a Sybil attack to be precise.

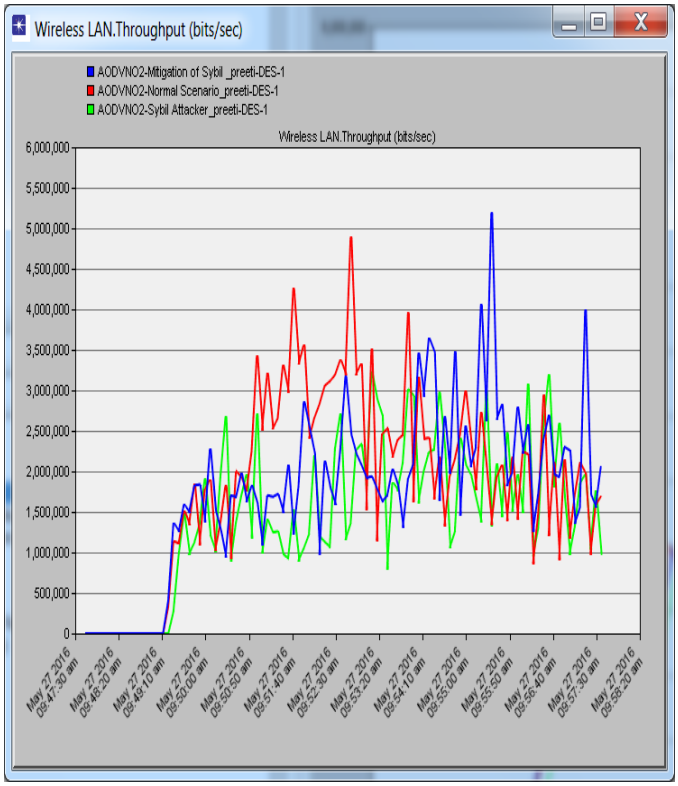

Fig 4: **Throughput of all three scenarios at 150 nodes**

In figure the graph represents the throughput in bits per seconds. The x-axis denotes the simulation time in minutes and the y-axis denotes throughput in bits per seconds. It can be clearly seen, that the Sybil attack decreases the overall network throughput in comparison to the normal network state.

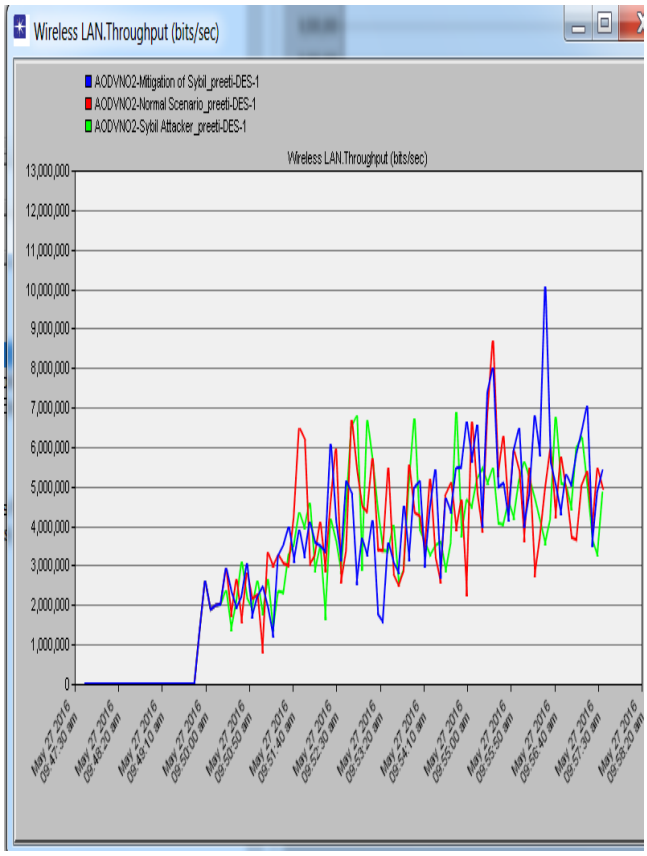

Fig 4: **Throughput of all three scenarios at 200 nodes**

VII. CONCLUSION

VANETs is quiet not secure as well as prone to various attacks. One of the major attacks in VANET is Sybil attack which makes multiple identities to confuse other nodes and reduce the trust of legal nodes in the network. So there is requirement of a secured protocol which can be capable to rapidly organize and also use dynamic routing mechanism. Peer-to-peer systems play an ever-increasingly significant role of our daily life. Since, most of the network systems are susceptible to Sybil attacks. For designing more effective and practical Sybil defenses, we uses active route timeout concept to detect performance improvement of AODV routing protocol for Vehicular Ad hoc Network. AODV protocol is simulated using OPNET Modeller v14.5 with varying number of mobile nodes.

REFERENCES

[1] Preeti Rawat1, Shikha Sharma2,;" Review on Sybil Attack in Vehicular Ad Hoc Network", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 4, April 2016.

[2] Er.Sushil Lekhi1,Gurjeet Kaur2;" A Novel Hybrid Approach of Neural Network and AOTDV for the Detection of Sybil Attack in Ad-hoc Network", International Journal of Computer Science and Communication Engineering Volume 4 issue 2(September 2015 issue)

[3] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.

[4] Anuradha Singh1, Mintu Singhz," Comprehensive Review on Vehicular Ad hoc Network ", International Journal of Advanced Research in Computer and communication Engineering Vol. 4, Issue 4, April 2015

[5] Sangeeta Bhatti," A Novel Algorithmic Approach for Detection of Sybil Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 5, Issue 5, May 2015

[6] E.A. Mary, "Sybil Secure Architecture for Multicast Routing Protocols for MANETs" CCIS 190, pp. 111–118, Springer-Verlag 2011.

[7] Kuo-Feng Ssu, Wei-Tong Wang and Wen-Chung Chang "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information,", Elsevier 2009.

[8] Arpita M.Bhise et al.," Review on detection and mitigation of Sybil attack in the network", international conference on information security and privacy (ICISP), 11-12 December 2015

[9] Liang xiao, Larry J.greenstein, Narayan B. madayam, Wade trappe, Channel based detection of Sybil attacks in wireless networks, IEEE Transaction on Information Forensics And Security,sep 2009,vol 4.p.492-503

[10] Adnan Nadeem and Michael P. Howarth,``A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, pp.1-19, 2012.

[11] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE, 2010 ,, Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks", IEEE Transactions ON Vehicular Technology, VOL. 59, NO. 5.

[12] J. Wang, G. Yang, Y. Sun, and S.Chen, "Sybil attack detection based on RSSI for wireless sensor network," WiCom '07: International Conference on Wireless Communications, Networking and Mobile Computing, September 2007, pp. 2684-2687, 21-25

[13] L. Shaohe, W. F. Xiaodong, Z. Xin, and Z. Xingming,"Detecting the Sybil Attack Cooperatively in Wireless sensor Networks," in International Conference on Computational Intelligence and Security, CIS '08. Vol.1 2008, pp.442-446

[14] D. Murat, and S. Youngwhan, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. Nternational Symposium, 2006, pp.259-268

[15] Mukul Saini1, Kaushal Kumar2 and Kumar Vaibhav Bhatnagar3; "Efficient and Feasible Methods to Detect Sybil Attack in VANET", nternational Journal of Engineering Research and Technology, Volume 6, Number 4 (2013), pp. 431-440

[16] Wenyu Zang "Detecting Sybil Nodes in Anonymous Communication Systems," International Conference on Information Technology and Quantitative Management, Elsevier 2013.

[17] Kuo-Feng Ssu, Wei-Tong Wang and Wen-Chung Chang "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information,", Elsevier 2009.

[18] Sohail et al," Lightweight Sybil Attack Detection in MANETs" IEEE SYSTEMS JOURNA 2012.

[19] Wagan, "VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination"International Symposium in Information Technology (IT Sim), 2010, pp. 607 – 611.