International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Threshold Technique for Isolation of Grayhole Attack in Vehicular Adhoc Network

Komalpreet Kaur[1], Rupinder Kaur[2], Gautam Kaushal[3]
[1,2,3]*Department of E.C.E, Punjabi University Patiala*

Abstract: ***The vehicular adhoc network is the decentralized type of network in which mobile nodes can communicate with each other. The vehicle nodes are highly mobile nodes which can change its location at the steady rate. Due to self configuring nature of the network malicious nodes join the networks which are responsible to trigger various types of active and passive attacks in the network. The grayhole attack is the active type of attack in which malicious node select the nodes which will be controlled by the malicious node. The selected nodes are responsible to flood the victim node with the rough data packets. In this work, threshold based technique is been proposed in which network which is sending data above the threshold value will be responsible to trigger grayhole attack in the network. The proposed technique is been implemented in NS2 and it is been analyzed that proposed technique is performed well in terms of throughput, delay and packetloss.***
Keywords: Active and Passive Attack, AODV, Grayhole

I. INTRODUCTION

The VANETs have proved to be beneficial due to their easy configuration as well as quick deployment. For asking any kind of help from other vehicles, a vehicle can send messages to other vehicles and can also inform the concerned authorities regarding problems they are facing on that road. For offering convenience and providing road safety VANETs are used in almost all areas. It is however, to be made sure that there are no invalid messages being sent across the network and the network is not being utilized in a malicious way. There is a possible situation to be present within the network in which the vehicles whose permanent identity is known can travel with low fuel reserve and ask for help. The identity is however is known to the attacker, it can monitor the communication and will also try to extract information from the vulnerable vehicle present. It will follow the vehicle until it runs out of fuel and then attack it to steal the important information [1]. Further, without contacting the authorities, the vehicle could be used in wrong manner. There can be a solution to this in which the permanent identity of the vehicle can be known only to its authorized personnel and hidden from all other vehicles. The major privacy issues within VANETs involve the information as well as the communication privacy. It is easy for the malicious node to eavesdrop on the traffic of network if the information of the vehicle's location is disclosed within the network. It can also trace the details of the other vehicles present within the same location. There are various privacy enhancement techniques proposed to solve such issues. The VANETs have some special characteristics as compared to the MANETs. These characteristics are listed below [2]

The VANETs are large-scale networks in which thousands of vehicles are deployed. There are a large number of nodes present within the network such that each vehicle can be registered within the network.

The mobility of the vehicles can be affected by the configuration of the road, the traffic laws as well as the speed limits. The behavior as well as interaction amongst the drivers is the reasons which affect the mobility of the vehicle. It is very complex to provide simulation in the vehicle traffic. It is thus a very tough task to simulate the vehicle traffic and provides the study for applications in the transportation engineering.

As compared to the typical mobile devices which are involved in MANETs, more resources are to be accessed by vehicles in the case of VANETs. There are large batteries, antennas, as well as the processing power provided here. So it is not necessary to provide resource conservations measures here.

There are vehicles as well as road-side infrastructure units (RSUs) present in the VANETs. The vehicles are able to communicate with each other as well as with the RSUs using VANETs. The RSUs are referred to as the fixed entities as well as the mobile entities are the vehicles. There can be one-hop communication amongst vehicles in VANETs or multi-hop in which the vehicles can act as routers and retransmit the messages. So, here the vehicles can communicate directly with each other of can pass messages amongst a series of vehicles. The nature of the message is an important factor which determines the type of communication. The one-hop communication can be provided if the vehicles wish to communicate on individual basis. If the vehicle requires a certificate authority (CA) to travel along with it, a message is broadcasted and [assed across the network. This stops once the RSU is reached and this type of communication is known as multi-hop type of communication [3].

The information related to link is used within the network for transferring the packets from source to destination in the case of topology based routing protocols. There are three broader classifications of these protocols [4].

A. Proactive routing
B. Reactive routing
C. Hybrid routing

The overhead which is created by the proactive routing protocols is overcome by the on-demand or reactive routing protocols. Only the routes which are currently active are maintained here using this type of protocol. The nodes which are currently being utilized for sending the packets from the source to destination are only highlighted here for route discovery and maintenance. By sending the RREQ (Route Request) from one node to establish the route for sending data at particular destination is done through route discovery. The node waits for RREP (Route Reply) once the RREQ is sent. If any RREP is not received within certain duration, it is assumed by the source node that the route is either unavailable or has expired. If the RREP is received at certain destination, the unicasting method is utilized for forwarding the information for ensuring that the route is present for communication. There are two categories for classification of reactive routing protocols. They are source routing and the hop-by-hop routing. In the case of source routing, the data packets hold the complete route information from source to destination. The information is taken from the data packet and stored in the header by each node while forwarding them to other intermediate nodes within the network. Thus, for sending a packet to certain destination, there is no need to update the complete routing information by each intermediate node. This type of routing is not suitable for the large scale networks which include numerous nodes which have dynamic natures such as VANETs. There might be chances of route failure due to the large number of nodes present within the network. There might also be chances of network overhead and increment in the route information present in the header of each node due to the increment in the number of intermediate nodes. As compared to the on-demand source routing technique, the hop-by-hop reactive routing method is advantageous. This is due to the fact that there is a next hop and a destination address present for each data packet here. Thus, for sending the data packet to certain destination, the intermediate nodes involve the routing table information.

II. LITERATURE REVIEW

Xia Shen, et.al, author surveys a collection of representative congestion control approaches for the IEEE 802.11p vehicular network. Assist, a novel distributed multi-priority congestion control method is proposed to maximize the transmission open doors for the highest priority traffics while keeping the collision probability at a low level [6]. Open issues for the future work on the congestion control approach design are drawn in this paper. The remaining challenges in the surveyed congestion control approaches are then concluded, which essentially focus on the traffic priority and congestion measurement consideration.

Dong Nguyen, et.al, approaches to reliably transmit information over an error-prone network utilize either forward error correction (FEC) or retransmission techniques. In this paper, some network coding schemes are proposed to reduce the number of broadcast transmissions from one sender to multiple receivers [7]. The principle idea is to allow the sender to combine and retransmit the lost packets absolutely so that with one transmission, multiple receivers can recover their own particular lost packets.

Alok Nandan, proposed which utilizes a gossip mechanism that leverages the inherent broadcast nature of the wireless medium, and a piece-selection strategy that considers in decisions to exchange pieces [8]. Through simulation it is seen that gossip incorporates location-awareness into peer selection, while bringing about low messaging overhead, and consequently enhancing the swarming protocol performance. An analytical model is built to portray the performance of SPAWN. It is seen that as more peers participate in the protocol, the performance improves.

Xiang Cheng, et.al, author address key issue on the design of deterministic simulation models is the means by which to properly design accurate and efficient parameter computation methods. The examination of V2V deterministic SoS channel simulators first concentrated on the design of parameter computation methods under isotropic scattering environments. Another parameter computation method, named as IMMEA, for deterministic SoS simulation models has been proposed under the condition of non-isotropic scattering MIMO V2V Rayleigh fading channels [9]. The proposed IMMEA is the first parameter computation method that can meet the accuracy-efficiency design criteria for all non-isotropic scattering MIMO V2V scenarios. Numerical results have shown that compared with existing MMEAs, the IMMEA gives a similar efficiency, while it offers better approximations to the STCF of the reference model

Christina Fragouli, et.al address problem of broadcasting in an ad hoc wireless network is considered, where all nodes of the network are sources that need to transmit information to every single other node. Our figure of legitimacy is energy efficiency, a critical design parameter for wireless networks since it specifically influences battery life and along these lines network lifetime. It

is demonstrated that applying ideas from network coding allows acknowledging critical benefits in terms of energy efficiency for the problem of broadcasting, and proposing exceptionally simple algorithms that allow understanding these benefits in practice.

III. PROPOSED METHODOLOGY

The grayhole is the active type of attack which is possible in the vehicular adhoc network. In the grayhole attack the malicious node is present in the network which drop data packets and forward some packets in the network. The technique is been proposed which detect and isolate malicious nodes from the network which are responsible to trigger grayhole attack in the network. The proposed technique is based on the threshold technique. In the proposed technique, the network throughput is defined, when the malicious start dropping the packets throughput will be reduced to steady rate. When the network throughput reduced to threshold value, the traffic analyze module get activated and it will analyze the node which drop packets. In the traffic analyzer module the watchdog technique is applied to watch adjacent node in the network. To isolate the malicious node in the network, technique of multipath routing is applied in the network

A. Proposed Algorithm

1) Input : Deploy network with finite number of vehicle node

2*) Output :* Detection of malicious nodes

a) Deploy vehicular adhoc network with the finite number of vehicle nodes

B. Establish route ()

1) Source send route request packets in the network

2) The nodes which are adjacent to destination will respond back with the route reply packets

3) The best path from source to destination will be selected on the basis of hop count and sequence number

C. Detection of malicious node()

1) Analyze the network throughput

2) if (network throughput reached to threshold

3) . Traffic analyze module get activates

4) Each node watch its adjacent node and node which drop packets is detected as malicious node

5) Else

6) source keep on sending data to destination

D. Apply multipath routing when step 3.2 get true

1) End

IV. RESULTS AND DISCUSSION

The proposed algorithm is implemented in NS2 to detect malicious nodes from the network. The malicious nodes are responsible to trigger grayhole attack in the network. When grayhole attack get triggered performance of the network will be reduced at steady rate. The proposed technique is applied for the detection of malicious nodes. The performance of proposed technique is tested in terms of throughput and packetloss

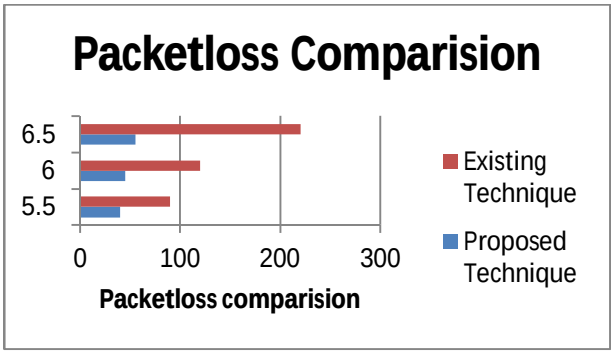

Fig 1: Packetloss Comparison

As shown in figure 1, the packetloss of proposed algorithm and existing algorithm is compared. It is been analyzed that due to isolation of grayhole attack in the network throughput will be increased at steady rate

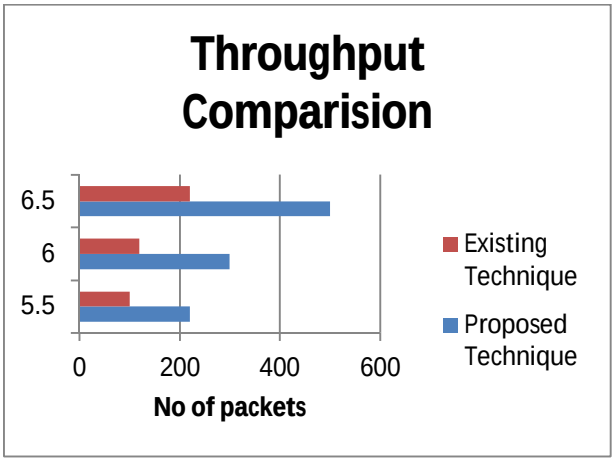

Fig 2: Throughput Comparison

As shown in the figure 2, the network throughput is compared and it is been analyzed that after the isolation of malicious nodes in the network throughput will be increased at steady rate

V. CONCLUSION

In this paper, it is been concluded that grayhole attack is the active type of attack in which malicious node flood the victim node with the rough data packets. The malicious node joins the network because the vehicular adhoc network is the decentralized type of network. In this work, threshold based technique is proposed in which node which is sending data above the assigned value will be marked as malicious which is sending rough data packets. The node which is sending the control packets above the assigned value will be detected as malicious nodes. The proposed technique performs well in terms of various parameters.

VI. ACKNOWLEDGMENT

I would like to Thanks my guide Er. Rupinder kaur for the continuous assist me for my M.tech study and related research, for her support, and extensive knowledge. Her guidance helped me all the time of research and writing for this paper.

REFERENCES

[1] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, “Co-operative downloading in vehicular ad-hoc wireless networks,” 2005, IEEE WONS 2005, pp. 32–41, St. Moritz, Switzerland
[2] M. Li, Z. Yang and W. Lou, “CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding,” 2011, IEEE J. Sel. Areas Commun., vol. 29, no. 1, pp. 223-235
[3] A. Duel-Hallen, “Fading Channel Prediction for Mobile Radio Adaptive Transmission Systems,” 2007, IEEE, vol. 95, no. 12, pp. 2299-2313
[4] S Michael, M Imad,” Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET”, 2013, IEEE Trans Mobile Computer 12(4), 722–734
[5] Xia Shen, Xiang Cheng, Rongqing Zhang, and Bingli Jiao,” Distributed Congestion Control Approaches for the IEEE 802.11p Vehicular Networks”, 2013, IEEE Intelligent transportation systems magazine
[6] Dong Nguyen, Tuan Tran, Thinh Nguyen, and Bella Bose,” Wireless Broadcast Using Network Coding”, 2009, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Vol. 58, No. 2
[7] Alok Nandan, Shirshanka Das, Giovanni Pau, Mario Gerla and M.Y. Sanadidi,” Co-operative Downloading in Vehicular Ad-hoc Wireless Networks”, 2005, IEEE
[8] Xiang Cheng, Qi Yao, Cheng-Xiang Wang, Bo Ai, Gordon L. Stuber, Dongfeng Yuan, and Bing-Li Jiao,” An Improved Parameter Computation Method for a MIMO V2V Rayleigh Fading Channel Simulator Under Non-Isotropic Scattering Environments”, 2013, IEEE COMMUNICATIONS LETTERS, Vol. 17, No. 2
[9] Christina Fragouli, Jörg Widmer, and Jean-Yves Le Boudec,” Efficient Broadcasting Using Network Coding”, 2008, IEEE/ACM TRANSACTIONS ON NETWORKING, Vol. 16, No. 2
[10] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala,“Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs”, INFOCOMP Journal of Computer Science, vol. 11 no. 1, March 2012, pp. 1-12.
[11] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, ” A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks”, Second International Conference on Advanced Computing & Communication Technologies, Apr. 2012 .

[12] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal, "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs", International Conference on System Engineering and Technology, September 11-12, 2012
[13] Hichem Sedjelmaci and Sidi Mohammed Senouci." A new intrusion detection framework for vehicular networks" In IEEE International Conference on Communications (ICC), 2014, pages 538–543, June 2014.