Advances and Applications in Mathematical Sciences
Volume 19, Issue 6, April 2020, Pages 481-494

A NOVEL TECHNIQUE TO DETECT THE ISOLATION OF GRAYHOLE ATTACK IN VANET

RITIKA SAINI[1], SUSHIL LEKHI[2] and ANUJ GUPTA[3]

[1,2]Rayat Institute of Engineering and Information Technology
Railmajra, Ropar, Punjab, India

[2]Department of Computer Science and Engineering
CGC-College of Engineering
Landran, Mohali, Punjab, India
E-mail: ritikasaini514@yahoo.in
lekhi.engg@gmail.com
anuj.coecse@cgc.edu.in

Abstract

With the help of road side unit vehicles communicate among themselves. This technique termed as VANET. This network helps us to improve the safety and efficiency of the occupants during travelling in vehicles. The basic idea of this technique is to send information about the traffic information to the road side unit or other vehicles. These vehicles get safe from attacks and misuse of their private data. The objective of this paper to secure the communication among the vehicles and the road side unit. In this technique the communication mainly dependant on the safety of the road such as vehicles tracking, emergency situations and message monitoring. There are various attacks like Sybil and Grayhole attack are vulnerable to VANET. To protect from these attacks our technique provide malicious node identification mechanism that help us to provide better facility to send data to vehicles safely. To avoid these types of attacks, our propose technique include feature like key management system to prevent the communication among the vehicles. Our proposed system mostly focus on Bandwidth, packet loss and packet delivery ratio.

Introduction

Those who knows the domain well and those who are undergoing rapid changes they did not distance themselves from transportation. The network

2010 Mathematics Subject Classification: 90B18.

Keywords: VANET (Vehicular ad hoc network), MANET (Mobile ad hoc network), RSU (Road side unit), Access Point, OBU (On-board units).

Received 31 October 2019; Accepted 18 December 2019

that communicates between vehicles plying on the road called VANET. Vehicle communication can be improved by inter vehicular communication. VANET includes the below mentioned communications:

- Inter-Vehicular Communication
- Vehicle-to-RSU Communication
- Inter-RSU Communication

The means of challenges in Vanet is how to contest with the high mobility of vehicles due to their changing speed. The focus of VANETs is to fulfill user's requirements on the road and make their journey safe and comfortable.

1. Characteristics

There are some special characteristics present in VANETs. These are listed below:

1. High mobility
2. Dynamic type of topology
3. The Frequent disconnections
4. Availability of the transmission medium
5. Limited bandwidth

2. Various Attacks in VANET

Denial of Service attack. This attack occurs when attacker controls all the benefits of the vehicle and stop communication network between vehicles. So attacker causes problems in communication of vehicle to send their message to the destination. Attacker may pose a risk to the driver, the driver may have to rely on incorrect information, due to this wrong information any major accident or disaster can also occur.

Message Suppression Attack. An Attacker drops the packets and can keep the data so that it can be used later on and send the wrong information. Attacker keep the information because the correct information about the accident not reached to the destination.

Fabrication Attack. An Attacker can send wrong information and can also claim that the information that is coming is from wrong sender.

Alteration Attack. in this the attacker can change the information such that if there is heavy traffic on the road, but attacker will tell road is empty.

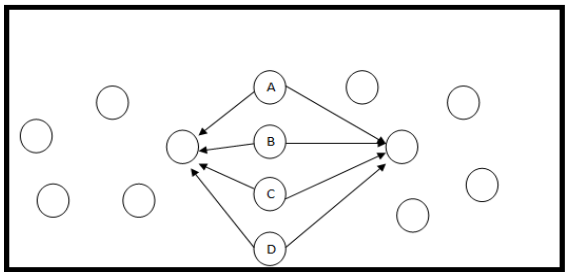
Replay Attack. In this attack the attacker re-sends old data to take advantages of attack situations.

Black hole Attack: in this network attacker stop sending data to other users due to the entry of unwanted malicious nodes in the network.

Grey hole Attack: in this attacker drops the 50% information and change the remaining 50% information and send the wrong information on the network.

Sybil Attack: in this attacker shows the wrong vehicles and also shows there are more than 100 vehicles on the road so that the driver change their lanes.

Grey hole Attack: in this attacker drops the 50% information and change the remaining 50% information and send the wrong information on the network.



In this figure: *A*, *B*, *C*, *D* nodes are malicious nodes which create fake or similar identity in the network and collapse the network. Grey hole attack is a critical attack. In this type of attack attackers generate multiple messages from different ids to other vehicles. Other vehicles are thinking in this way that messages are coming from different vehicles with different ids, so there is condition of jam occurs. In this way attacker produce illusion of other vehicle and force them to choose another path and leave the road for the benefit of the attacker. Overall it is concluded that Sybil attack is performed or launched by sending multiple messages from different ids.

3. Algorithms and Examples

Identification of Grayhole attack

A Grayhole attack is basically the extension of black hole attack. In this, the source and monitoring systems are handled using partial forwarding. The selective data packet dropping method is presented as a normal node and this node participates in communication. A node that can behave in a complete normal manner and switch to behaving like gray hole which is actually an attacker, is known as gray hole node [4]. This gray hole node will behave completely normal and so it is difficult to identify the attacker. The routing table which contains the information of the next hop node is updated for each node. A specific route is to chosen by the node is the source node needs to route a packet to the destination node. The routing table is used to check if the route selected by the source node is available or not. A broadcasting Route Request (RREQ) message is sent to the neighbour of the node if it initiates a route discovery process. The intermediate nodes, after receiving the message, update the routing tables for reverse route to the source. When the RREQ query reaches top the destination node or any other node that has a route to the destination, a route reply message is sent back to the source node. There are two phases of the grayhole attack:

Phase 1: The AODV protocol is exploited by the malicious node. This is done to show that it has a valid route to the destination node which intends to interrupt the packets available in the spurious route.

Phase 2: In this phase, the malicious node drops the interrupted packets on the hold of certain probability. The packet selection is done on the base of this probabilistic method. The behaviour of the attacker node changes instantly which results in either transferring or dropping the packets. The malicious node creates an illusion of genuine nodes by forwarding some packets. This creates a level of difficulty of detect the attacks in the network.

Proposed Algorithm

Input: vehicles, RSU, malicious vehicle

Output: Malicious vehicle

Apply information gathering process

{

1. Node send its credentials to road side units

2 If (Matched= true)

3. Assign identification

4. Else

5. Send not verified message

6. }

7. }

If (Network throughput = reduced)

1. Send ICMP messages in the network

2. Node receive the message go to monitor node

3. If (Node drop packets = true)

4. Node = Malicious node

5. Else

6. Node = Legitimate node

7. }

End

Isolation Mechanism

Security in vehicular network [1] plays a major role in an ad-hoc network to provide safe and secure communication. The security goals are authentication, integrity, robustness, confidentiality, non-reputation and anonymity. In protection mechanism, we focus on securing the VANETs from several critical attacks such as Black hole attack, Wormhole attack and Sybil attacks. To provide data confidentiality, encryption is only used for allowing honest users for reading and processing the data which are transmitted. Asymmetric algorithms such as Elliptical Curve Cryptographic algorithm are mostly preferred for packet transmission in the network; it generates private key and public key, which has higher security according. According to key base certification [7], DMV sector generates asymmetric keys for vehicles in

the networks that distribute them when keys are generated. The DMV sector does a key management process which avoids the attacks in the network, by having the key table. This key table contains RSS values, MAC address and logical address and their private keys of every vehicle. During Vehicle-to Vehicle Communication and Vehicle-to-Infrastructure in the network, keys are verified.

If any vehicle enters in a VANET, it must register in a DMV sector and it gets an asymmetric key for secure communication in the network. DMV sector maintains a key management process, by recollecting all keys from every vehicle in the network and updates the new key for every vehicle at every slot K. In our routing mechanism, any vehicle suspect any malicious node in the Pseudo code: Isolation Mechanism

Input: Message (M)

Output: Providing secure communication

Begin

Step 1: $\text{Veh}_i \rightarrow$ DMV

Step 2: Key_i Generation

Step 3: Distribute $\text{Key}_i$to all Veh_i

Step 4: $Veh_1 \rightarrow M$

Step 5: $M \rightarrow (\text{Request})\, Veh_2$

Step 6: $Veh_2 \rightarrow (\text{Request})\, RSU$

Step 7: $RSU \rightarrow (\text{Request})\, DMV$

Step 8: $DMV \rightarrow (\text{Reply})\, RSU$

Step 9: $RSU \rightarrow (\text{Reply})\, Veh_2$

Step 10: if (Reply is Valid)

Else

Veh_2cancels it Reply

Step 11: RSU generates A to Veh_i and RSU_i

//////Revocation process

Step 12: DMV recollects Key_i

Step 13: if (Key table)

Generates new Key_i

Update Key_i

Distribute Key_i

Else

Cancel authentication to

$A \rightarrow \text{RSU}_i$

Generates new Key_i

Update Key_i

Distribute Key_i

End

Network, it moves a warning message to other vehicles and again an warning signal is generated by the RSU to other RSUs. Here revocation process takes place, any malicious user have valid key, then DMV sector cancels the valid key and announces to RSU. Then every vehicle in the network cancels their connection to the specific vehicle.

If any vehicle suspects the malicious behaviour of node (i.e. malicious behaving node (Sender node) sends message to another vehicle (Receiver Node)), then it sends a message to RSU followed by DMV sector. DMV sector check the keys of the malicious node, if it is valid node, it sends a message to RSU and RSU forwards message to receiver node. Then it can continue it communication else an invalid message is received to the receiver node. Figure 4.2 describes the pseudo code for protection mechanism. Key_i is the private keys for every vehicle, Veh_i represents the vehicles, M is the

Message from sender Veh_1, Req represents the request message from Veh_1, to RSU and to DMV and Rep is the reply message from DMV to RSU and to Veh_1. A is the alarm signal that generated when malicious user communicates with other vehicle.

Figure 7 describes the protection mechanism in our paper. In this diagram, a malicious node sends a message to normal node. Here normal node needs to check the sender is normal node or malicious node, so it sends a message to RSU, RSU sends a message by checking in the DMV Sector whether it is a valid node or invalid node. If normal node receives valid message then it continues its communication else it cancels its communication with malicious node. Then RSU sends warning signal to all vehicles and to all RSU in the network.

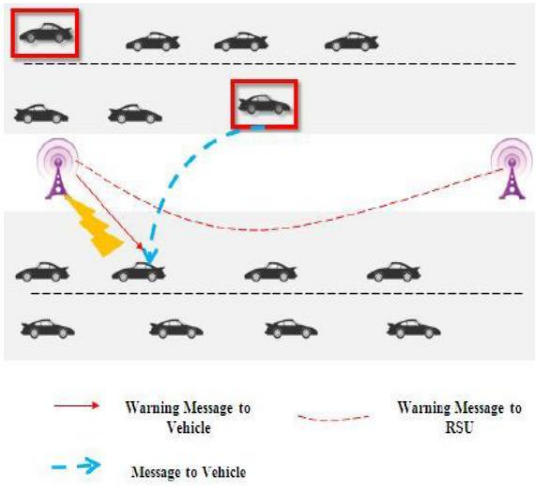


Figure 7. Isolation mechanism.

As per the security requirements and the topology we defined the output parameters will be defined.

NS2- It is a distinct event scheduler used to simulate wired and wireless network. It provides notable hold up to simulate bunch of vehicular protocols [2] like TCP, FTP and DSR etc. It uses TCL as its scripting language to measure and analyse performance of developed model. It run on "real time environment". NS stands for network simulator which is primarily UNIX

based it follows two groups that are event based and time based simulator. It provides collaborative environment which is responsible for freely distributed, more confidence in results. Different varieties of simulations are being done by NS like text based and animation based. Main scenario of NS is to interpret and work with a famous network simulator. For getting a better perceiving of the networking effectiveness.

Screenshots

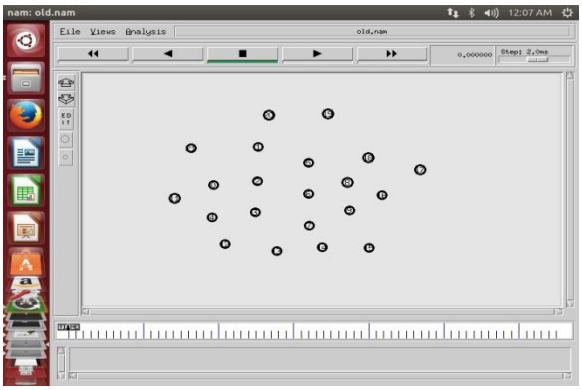


Figure 8. Network Deployment.

As shown in figure 8, a fixed area is used for the placement of the "wireless adhoc network" which is responsible for the free movement of nodes from one location to another.

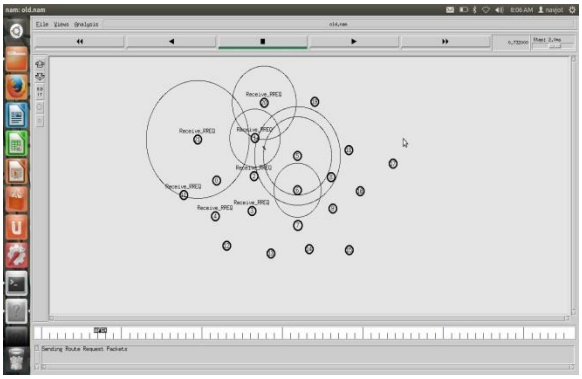


Figure 9. Establishing the path.

As shown in figure 9, Due to the decentralized nature of the network "nodes" can change their position freely.

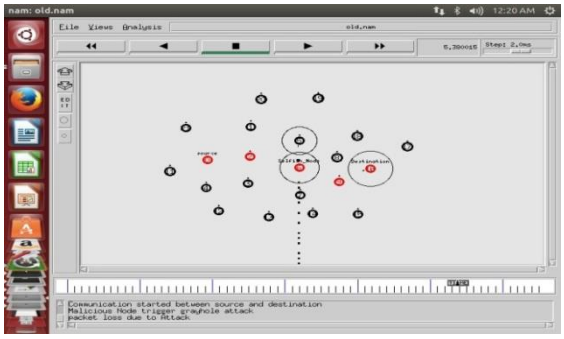


Figure 10. Triggering of attack.

As shown in figure 10, while making the paths in between the "source and the destination nodes" the best path is being selected. The Gray hole attack will be triggered once the malicious node then it will leaves the path and this result in inclining the delay between the s and the *d*.

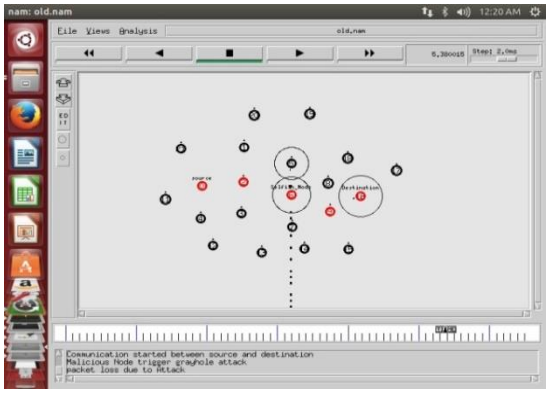


Figure 11. Detecting the malicious node.

As shown in the figure 11, the nodes which go the monitor mode will start sensing its adjacent node and node which detect the malicious node will send reply to the source about the malicious node and source will isolate that node.

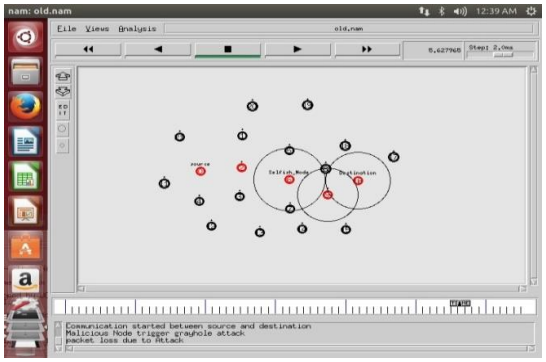


Figure 12. Isolation of malicious node.

As shown in figure 12, the malicious node will be detected by the node which go the monitor mode and analyze the behavior of the node. The source will isolate the malicious node and change the path for the data transmission.

Bandwidth consumption: It is the bandwidth consumed by the vehicles at different velocities. As the no of vehicle increases the consumption also increases [10].

Table: 1. Bandwidth used.

Average Velocity	Bandwidth (First)	Bandwidth (Second)	Bandwidth (Proposed)
3	15	20	15
6	28	25	24
9	55	30	28

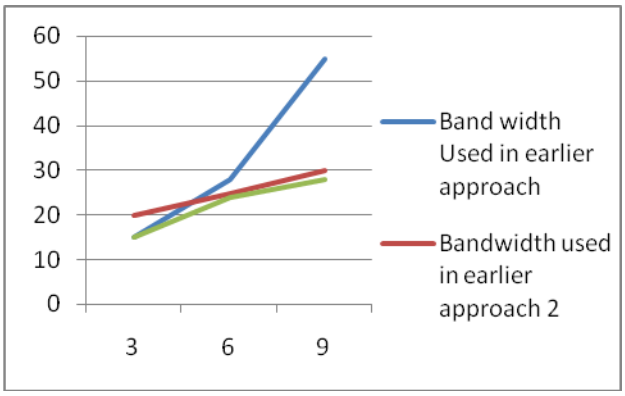


Figure 13. Bandwidth used by different approaches.

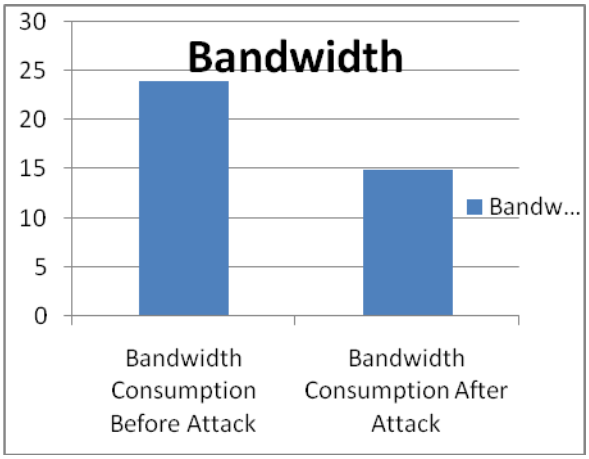


Figure 14. Graphical Representation of Bandwidth.

Future Scope and Conclusion

Ad-hoc network like VANET which provides links between two vehicles. It has capacity to enhance higher links and security measures. VANET has many problems in terms of security. There are various forms of attacks in VANET such as Sybil attack, Wormhole attack and Black hole attack. To identify these forms of attacks we proposed a "Malicious Node Identification Routing and Protection Mechanism for VANET against Various Attacks"which comprise AODV protocol. This Routing mechanism includes three different scenarios for identifies these attacks in the network. For prevent the networks from various attacks, we introduce a Protection Mechanism that uses an asymmetric algorithm and it allows a key management based on key revocation process in the network.

Our routing mechanism provides best results in terms of Packet loss, Packet Delivery ratio (PDR), Bandwidth, etc. In our future work, we enhance our routing process that identify and save VANET from more endangered attacks like gray hole attack, Sybil attack etc.

- The proposed algorithm is the secure algorithm which isolate malicious nodes from the network. The proposed secure algorithm can be compared with the other secure algorithm to analyze its reliability.

- The proposed algorithm is the improvement in AODV protocol to

improve security of VANET. The proposed Technique can also be tested on other routing protocols.

- In future, algorithm can be proposed which can also isolate Sybil attack using trusted and un-trusted authorities technique.

References

[1] Bharati Mishra, Saroj Kumar Panigrahy, Tarini Charan Tripathy, Debasish Jena and Sanjay Kumar Jena, A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation, Information and Communication Technologies (WICT), (2011), 880-885.

[2] Adil Mudasir Mala and Ravi kantsahu, Security Attack with an Effective Solution for DOS attack in VANET, International Journal of Computer Applications (0975-8887), 66(22), March 2013.

[3] H. Noori and B. B. Olyaei, A novel study on beaconing for VANET-based vehicle to vehicle communication: Probability of beacon delivery in realistic large-scale urban area using 802.11p International Conference on Smart Communications in Network Technologies (SaCoNeT), 2013, pp. 1-6.

[4] M. Garai and N. Boudriga, A novel architecture for QoS provision on VANET 10th International Conference on High Capacity Optical Networks and Enabling Technologies (HONET-CNS), 2013, pp. 25-31.

[5] G. El Mouna Zhioua, Jun Zhang, H. Labiod and N. Tabbane, VOPP: A VANET offloading potential prediction model Wireless Communications and Networking Conference (WCNC), 2014, pp. 2408-2413.

[6] Yiliang Liu, Liangmin Wang and Hsiao-Hwa Chen, Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks, IEEE Transactions on Vehicular Technology, (2014).

[7] Parul Tyagi and Deepak Dembla, A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs), International Journal of Computer Applications (0975-8887) 91(7), April 2014.

[8] Prakash Tripathi and Kanojia Sindhuben Babulal, Security In Vehicular Ad-Hoc Network, International Journal Of Scientific & Technology Research Volume 3, Issue 11, November 2014, ISSN 2277-8616.

[9] Y. Bevish Jinila and K. Komathy, An Efficient Authentication Scheme for Vanet Using Cha Cheon's ID Based Signatures, Research papers computer science, Volume : 4,Issue : 6, June 2014 ,ISSN - 2249-555X

[10] L. A. Vinh Hoa and Ana Cavalli, Security Attacks and Solutions In Vehicular Ad Hoc Networks: A Survey, International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[11] Jason J. Haas and Yih-Chun Hu, University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A, Real-World VANET Security Protocol Performance, p1-7,2014.

[12] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET VT-2014-00658. DOI 10.1109/TVT.2015.2406877, IEEE (2015)

[13] Ahmad, Hybrid Multi-Channel Multi-hop MAC in VANETs, MoMM2010, 8-10 November, Paris, France, pp 353-357, 2015.

[14] M. Raya and J. Hubaux, Security of Ad Hoc and Sensor Networks, SASN '05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2015.

[15] M. Raya, J. Pierre and Hubaux, Securing vehicular ad hoc Networks, Journal of Computer Security, vol. 15, pp: 39-68, jan 2015.