Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.8 No.S1, 2019, pp.7-9

DOI: https://doi.org/10.51983/ajcst-2019.8.S1.2015

Detecting and Preventing a Black Hole Attack in VANET

V. Sasirekha[1] and S. Nithyadevi[2]
[1&2]Assistant Professor in Computer Science,
[1]J.K.K.Nataraja College of Arts & Science, Namakkal, Tamil Nadu, India
[2]Anbu Arts and Science College, Namakkal, Tamil Nadu, India
E-Mail: sasirekhailangkumaran@gmail.com, nithyamca81@gmail.com
(Received 10 November 2018; Revised 13 December 2018; Accepted 8 January 2019; Available online 15 January 2019)

***Abstract* - In recent years, Vehicular Adhoc Network is one of fastest ongoing emerging field in the networking industry. But it faces lot of challenges today. Security is the major concern in the VANET. Now a day's hacking is the hobby of the programmers. Lots of applications were developed for security attack. VANET is a dynamic network, it require secure communication. The VANET is vulnerable to various types of attacks. In this paper we have focused on black hole attack. The Black hole attack may interrupt the packets and insert the false information in the packets and sends to the other vehicle. The receiver of the vehicles is directly affected. Here we developed a mechanism with AODV protocol called blackhole attack detection and prevention which is mainly focused on vehicles sequence number. The source vehicles sequence number compared with the destination vehicles sequence number. If it is larger than the destination vehicle then the vehicle is marked as malicious vehicle. And this vehicles information is send to the Road Side Unit(RSU). The Road Side Unit analyzes the malicious vehicle and blocks the vehicle.**
***Keywords:* RSU, AODV, VANET**

I. INTRODUCTION

VANET is the special class of Mobile Adhoc Network. It considered Moving cars as node. The Vehicle can communicates with each other through Intelligent Transport System (ITS) it enable real life application. Every vehicle contain Onboard Unit (OBU).A typical OBU can equipped with GPS or other short range communication module like Dedicated Short Range Communication(DSRC). There are three types of communications in the VANET. Vehicle to Vehicle Communication (V2V), Vehicle to Infrastructure Communication (V2I), Vehicle to Road Side Unit Communication (V2R). VANET faces different security attacks.

A. Security Requirements

Security is a major problem to be identified and rectified to overcome the vulnerability and various types of attacks.The following requirements are confirmed to the security.

B. Authentication

A vehicle in theVANET should acknowledge only theauthenticated messages. Every message from the sender must be authenticated to ensure the security and also to overcome the various attacks.

1. *Data Consistency:* The messages in VANET consist of time, location and vehicle information. These are very important to manage secure communication.
2. *Confidentiality:* In VANET messages werekept in very confidentiality. No one should not decrypt and broadcast the other vehicle information.
3. *Data Integrity:* Data integrity tells that the securecommunications have to ensure that the messages are not corrupted and not modified by the attackers.
4. *Availability:* Even the attacker attacks the network the VANET is available to the applications of vehicular systems.
5. *Privacy:* VANET ensure that the information of the vehicle is not accessible by the others. It will be maintained by securely.

C. Black Hole Attack

Now a day's route discovery is a very easiest process. Most of the new vehicle comes with the facility to mapping to discover route. While driving us often see the google map to find the route. If our vehicle is compromised then we cannot get the reliable route. In the Blackhole attack the malicious node advertise the message itself by sending the route request and reply messages.The attacker node uses routing protocol to broadcasts the packet with shortest route to the destination. The attacker node always available to reply the route request messages and thus intercept the packet. Any vehicle wants to send the message in the network it first send the route discovery message to its neighboring nodes. At that time the Blackhole attacker node waits to receive other vehicles route discovery messages, once it received then the malicious node send back to the false route reply message with modified sequence number. After receiving the false message, the vehicle sends the message to the malicious node. The entiremessage sendsthe vehicle through the malicious node will be dropped.

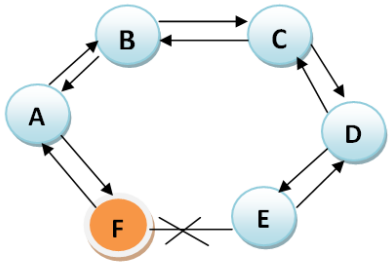

Fig. 1 Black Hole Attack

Fig. 1 shows the Blackhole attack. The Label A,B,C,D,E,F are considered as the vehicles in the VANET. The vehicle F is the attacker node or malicious vehicle. Here Vehicle "A" wants to send the data packet to vehicle "E" for that vehicle "E" wants to initiate the Route Discovery Request message. As soon as Route Discovery Message delivered in the network the malicious vehicle send the Route Reply Message with the shortest path to the destination. i.e. vehicle "F" is the shortest route to the Vehicle "A". Now the vehicle "E" sends all the messages through the vehicle "C". All the messages received from vehicle "E" will be dropped.

II. RELATED WORK

VANET is the emerging field of the network industry. Security problem is the major challenges. Many researchers were proposed theirs results and solutions regarding the security attack. In this paper we have described some of them as follows.

Rand S Majeed *et al.,* [1] eliminate the Blackhole attack with single and multipleattacks effect. Total number of dropped packets was measured and improves the performance of AODV under the single attacker.

VimalBibhu *et al.,* [2] analyzed the performance of the network with the effect of Blackhole attack. They analysed the attacks with parameters like end-to-end delay, throughput, network load etc., the author did the evaluation using OLSR and AODV protocols. The author produced the result is AODV is more vulnerable than OLSR.

III. PROPOSED APPROACH

Here the Black hole attack prevention and detection mechanisms used with the AODV protocol.This mechanism mainly focused on Sequence Number. It is named as SN_AODV. From which source vehicle receive the Route Reply Message with highest Sequence Number then it will considered as malicious vehicle that is going to produce the blackhole attack.

A. Pseudo code

The Blackhole prevention method is used to protect the network.This mechanism takes the Route discovery Message. We had taken some notation as follows.

SN_ID - Source Node Identification, DN_ID – Destination Node Identification, MN_ID - Malicious Node Identification, SN_SEQ – Source Node Sequence Number, DN_SEQ – Destination Node Sequence Number, RT – Route Table, RDREQ - Route Discovery Request, RREP – Route Reply, BROD_ID – Broadcast Identification.

Step 1: Source Node Broadcast the Route Discovery Message.

SN->RDREQ[SN_ID,DN_ID, SN_SEQ, BROD_ID]

*Step 2:*Neighbour vehicles send the Route Reply Message.
SN<- RREP[ND_ID, SN_ID, DN_SEQ, HOP_COUNT, LIFETIME]

*Step 3:*Route Discovery Node will store all the incoming Route Reply Message in the Routing Table. And create Trusted Route List Trusted_Route_List[SN_ID, DN_ID, SN_SEQ, DN_SEQ, HOP_COUNT]

Step 4: Compare the Destination Sequence Number with the Source Sequence Number. If it is Larger than the Source Sequence Number then the vehicle is marked as a Malicious Vehicle.

```
If( DN_SEQ > SN_SEQ)
{
SN_ID = MN; // Marking as a Malicious Node
Update Trusted_Route_List( )
{
Trusted_Route_List->REMOVE(SN_ID)  // Remove Malicious Node
Malicious_Route_List ->ADD(SN_ID)
}
```

Step 5: After generating Trusted and Malicious Route List, every node will send the Malicious route to RSU. RSU broadcast the malicious node identity to all its neighbour vehicles and block the vehicle.

IV. SIMULATION AND DISCUSSION

TABLE I SIMULATION PARAMETERS

Simulation Parameters Examined with the Simulation Time 1000 seconds and Area 2000*2000 meter	
No of Vehicles	100
Type of Vehicle	Car
Type of packet Send	UDP
Pass Time	10 minutes
Maximum Speed	10/20/30 minutes
Transmission of OBU	100m
Transmission of RSU	250m
Routing Protocol	AODV
Simulator	NS 2.35
Traffic Model	CBR
Mobility Model	Random Waypoint Model

In this mechanism we had taken 100 vehicles to run the simulation with different network parameters which is given in the Table I. We first run the simulation without any malicious vehicle and calculated number of packets dropped. After that marked a vehicle as a malicious and run the simulation for checking the effect of malicious vehicle and we analyzed the number of packets dropped in Table II. The packet drop percentage was reduced.

TABLE II PACKET LOSS ANALYSIS

Scenario	No of Pack. Sent %	No of Pack. Rec.%	Packet Loss Before Prevent %	Packet Loss After Prevention %
Scenario-1	80.32	20.59	90.2358	15.5567
Scenario-2	96.58	18.43	89.7459	12.6790
Scenario-3	92.28	21.75	94.6782	14.6953
Average	90.39	20.256	91.5533	14.3103

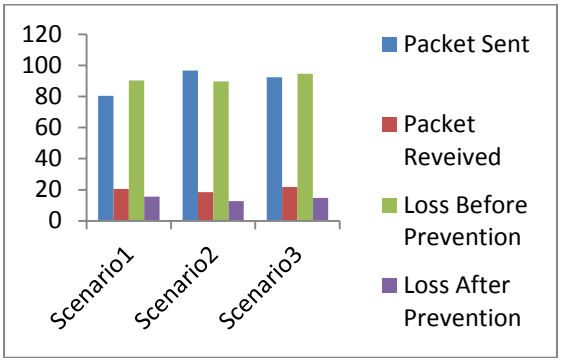

Fig.2 Packet Loss Analysis with Graph Representation

V. CONCLUSION

In this paper we proposed a novel approach to detect and prevent the Blackhole attack in the VANET. We have implemented a mechanism which was based on the vehicles sequence number. This mechanism decreases the packet loss because this method detects the malicious vehicle and eliminate the blackhole attack. And also prevent the blackhole attack by generating the malicious vehicle list which is send to the RSU. The RSU block the vehicle communication. In future, we have to identify different approaches to eliminate the blackhole attack for better results with the traffic scenario.

REFERENCES

[1] Vimal Kumar and Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network,"*in* Procedia Computer Science Vol. 48, pp. 472 – 479, *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014)* , Elsevier, 2015.

[2] Saurabh Gupta, SubratKar and S.Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocol for Wireless Network" in *International Conference on Computer & Communication Technology (ICCCT)-2011, IEEE*,1386-611, 2011

[3] VimalBibhu, Kumar Rosan, "Performance Analysis of Blackhole Attack inVANET", *I. J. Computer Network and Information Security*,Vol. 11, pp. 47-54, October. 2012.

[4] Al-Shurman, M. Yoo and S. Park, "Black hole attack in Mobile Ad Hoc Networks", *ACM Southeast Regional Conference*, pp. 96-97, 2004.

[5] Rand S Majeed, and Mohammed abdala,"Blackhole Attack effect Elimination in VANET Networks using IDA-AODV, RAODV and AntNet Algorithm",*Journal of Telecommunication*, Vol. 36, No. 1, February 2017.

[6] Abdul Kalam, KunnelAboobaker, and Dr. Stephen Wolthusen"Performance analysis of Authentication Protocols in Vehicular Ad Hoc Networks (VANET)", Department of Mathematics, Royal Holloway, University of London, UK, 2009.

[7] Pradeep Kumar Sharma, ShivlalMewada and Pratiksha Nigam, "Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network", International Journal of Scientific Research in Network Security and Communication, Vol.1, No. 4, pp.8-11, 2013.

[8] D. Patel and K. Chawda, "Blackhole and grayhole attacks in MANET,"*International Conference on Information Communication and Embedded Systems* (ICICES2014), Chennai, pp.1-6, 2014.

[9] Umesh Kumar Singh, JalajPatidar and Kailash Chandra Phuleriya, "On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, No. 1, pp.11-15, 2015.

[10] Bala, Anu; Bansal, M.; Singh, J, "Performance Analysis of MANET under Blackhole Attack," in Networks and Communications, 2009. *NETCOM '09. First International Conference on IEEE*, pp. 141-145, 27-29, Dec. 2009.