Mitigation of Black Hole Attack in VANETs

Pooja Nayak, Mrs. Manasa S
Department of Information Science and Engineering, NMAMIT, Nitte, Udupi, Karnataka, India

Abstract - VANETs or Vehicular Ad hoc Networks, a type of wireless ad-hoc networks, where vehicles are interlinked by wireless networks which continuously stores, forwards and shares data between the domains of vehicles. These types of networks are being increasingly used to improve the safety of transportation. Since the information transmission between the vehicular domains are through open access or wireless environment, security of the network is considerable important. Moreover, many possible attacks such as Sybil attack, Node impersonation attack, Denial of Service (DOS), Black hole attack, Distributed Denial of Service (DDOS) attack, Gray hole attack and other attacks have been recorded in the literature. This research is conducted on one of the most prominent and also the most difficult to detect and prevent the attack namely, the black hole attack. The typical nature of this attack is to drop packets by targeting routing protocols based on network destination. Ad-hoc On Demand Distance Vector (AODV), which is much prone to black hole attack, is researched further. In this paper several simulations under different scenarios are carried out to observe the effect of the attack on the AODV routing protocol. And in this work we have also tried to overcome the network from black hole attack by using some of the security techniques called SHA-1 and MD5

Keywords: VANET, Black hole Attack, AODV.

I. INTRODUCTION

In By looking into the importance of internet and rapid improvements in the wireless technologies, a new expectation of a Wi-Fi environment is emerging rapidly. This leads to the development of Vehicular Ad-hoc Networks (VANETs) [1]. These networks works on the basis of co-operation, here communication is done in either within the single hop or multi hop fashion and the trust among the nodes are maintained so that these nodes can help other nodes for data transmission. VANET helps to guide both safety, and non-safety applications. Security is the main aspect of VANET [2]. But due to high mobility vehicular communication is critically insecure to various threats so security is an important aspect for the deployment of VANET. One of the most important attack is the Denial of Service (DOS) and the most crucial attack under this category is black hole attack. The performance of the network is degraded due to this attack [3]. Black hole attack aims at dropping the packets. This attack is also referred as Packet drop attack [4].

II. RELATED WORK

In this section author should discuss about related research has been done in the same domain or related domains with the name of the researcher and should be mentioned in the references. In [5], authors have done the simulation of routing protocol AODV which generates real world mobility model for VANETs. The tools used for this purpose is MOVE (Mobility Model Generator for Vehicular Networks) along with NS2 and SUMO (Simulation of Urban Mobility). In [6], authors have presented some of security criteria to measure security which includes non-repudiation, confidentiality, availability, authentication, integrity and access control. In [7], authors presented various attacks like Sybil attack, node impersonation attack, black hole attack, worm hole attack, DoS attack, DDoS attack, the author also mentioned some solution to prevent such attacks. In [8], author has given the solution to overcome the problem of worm hole attack detection. For this the author has used a special packet called Decision Packet. In [9], author proposed a method called Protection node based strategy to remove the effect of DDoS or DoS attack in VANETs. In [10], authors measured the network performance using AODV protocol by the effect of black hole attack. The proposed process uses the AODV encryption-decryption for detecting the black hole attack.

The literature review indicates that simulation analysis for AODV particularly for VANETs are scarce, and most of the researches are concentrated on Simulation analysis for AODV on MANETs. The present research focused on study of various attacks possible over VANETs and is directed towards finding impact of black hole attack on AODV specific to VANETs by simulation of different scenarios such as throughput, packet delivery ratio, and total energy consumed by using simulation tools.

III. PROBLEM IDENTIFICATION AND IMPLEMENTATION

Malicious node waits for the source node to send RREQ message to the destination once it intrudes the Ad hoc network [11]. Soon after receiving RREQ message by the malicious node it replies with RREP with highest sequence number to the source node before other node send RREP. Now source node will receive RREP message with the highest sequence number from the malicious node and source starts establishing connection to the black hole node by checking its routing table.

At the sender side:
Step 1: Enter the input plaintext

IV = 'key'
Plaintext = input_string

Step 2: IV and plaintext is hashed by using SHA-1 algorithm

MD5_key = hash (IV, plaintext)

Step 3: Plaintext is encrypted by using encryption algorithm

Encrypted_msg = encryption_algorithm (MD5_key, plaintext)

Step 4: Appending the encrypted message to the packet and forwarding it to receiver

Packet_append (Encrypted_msg)
Send (Packet)

At the receiver side:

Step 1: Packet is decapsulated to get encrypted message

IV = 'key'
Encrypted_msg = packet_decapsulate (packet)

Step 2: IV and Plaintext is hashed by using SHA-1 algorithm to get MD5_key

MD5_key = hash (IV, Plaintext)

Step 3: Message is decrypted by using decrypted by using decryption algorithm

Plaintext=decryption_algorithm
(MD5_key, Encrypted_msg)

Step 4: Display the Plaintext

Display (Plaintext)

IV. SIMULATION AND RESULTS

Simulation is done using NS2 along with the SUMO and MOVE tools to produce realistic mobility model. Vehicular Ad hoc network is created using SUMO and MOVE tool which is built on the top of SUMO and facilitates real world mobility models for VANET simulations. Mobility trace file is the output of MOVE that contains information about realistic vehicle movements which can be used in NS2. Due to its flexibility and modular nature it is widely used to specify network protocol and simulating their behaviors. NS2 mainly uses two languages; they are object oriented tool command language and C++. Simulation parameters are shown in table1.

TABLE 1. SIMULATION PARAMETERS

Parameter	Values
No. of nodes	25
Simulation Area	1000*1000
Simulation Time	100 sec
Mobility model	Two Ray Ground
Traffic	cbr
Mac	802.11
Protocol	AODV

In this work we have used NS2.35 tool for the purpose of simulation, and here without any modification we have implemented AODV and later recompiled NS2.35 with the changes of black hole attack. In black hole implementation we have taken 20% of the nodes as black hole nodes. Simulation metrics are the inputs and outputs which are observed in terms of throughput, total energy consumption and packet delivery ratio.

Throughput:

Fig 4.1 and Fig 4.2 shows variation of throughput with number of nodes. Throughput is measured in its/sec. In Fig 4.1 indicates black hole attack in the network without adding any security algorithm and it shows less performance as compared to AODV without any attack. Fig 4.2 a security algorithm is introduced to measure the performance and it shows superior performance than Blackhole attack without security algorithm.

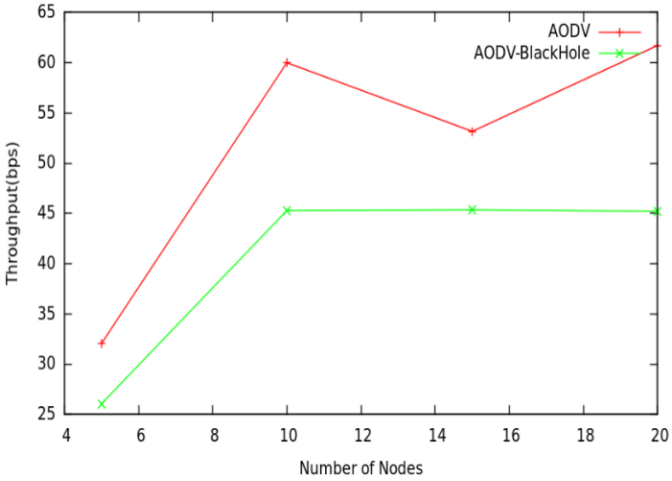

Fig. 4.1 Throughput for no of nodes without security algorithm

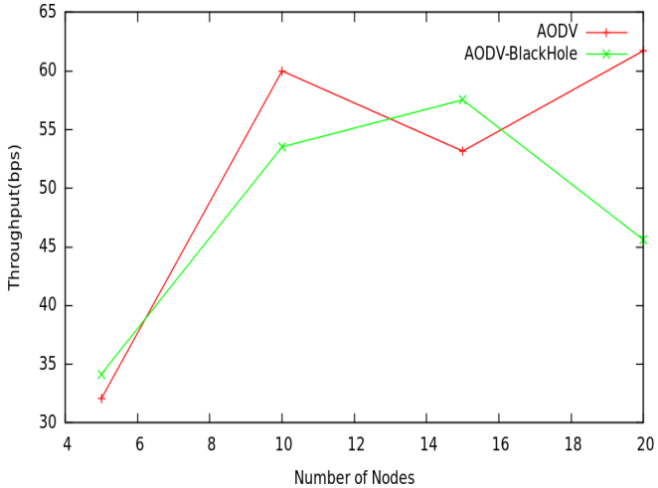

Fig. 4.2 Throughput for no of nodes with security algorithm

End to end Delay

Fig 4.3 and Fig 4.4 indicates variation of end to end delay with number of nodes. In Fig 4.3 shows variation of end to end delay with black hole attack in the network without adding any security algorithms. Fig 4.4 security algorithm is added to measure the performance. With security algorithm shows more end to end delay as compared to without security algorithm.

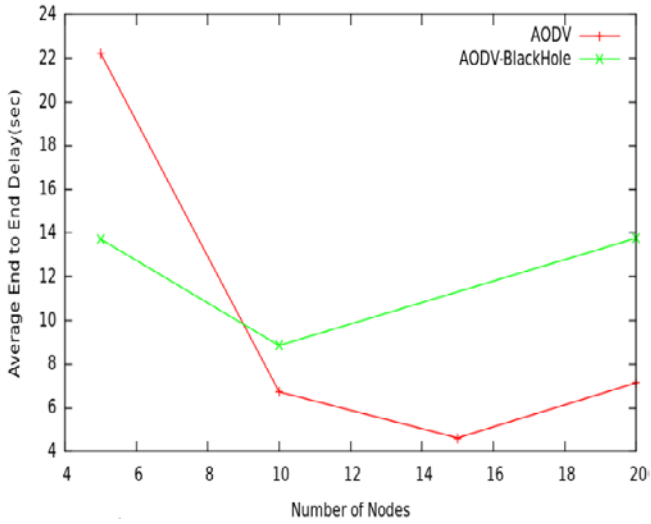

Fig. 4.3 End to end delay for no of nodes without security algorithm

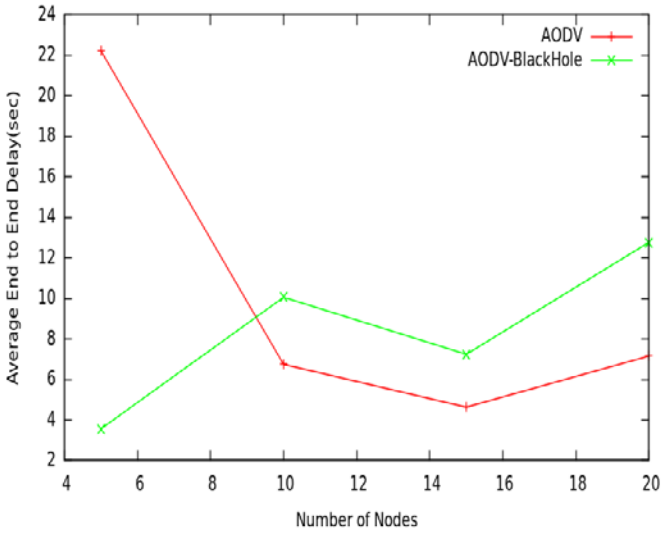

Fig. 4.4 End to end delay for no of nodes with security algorithm

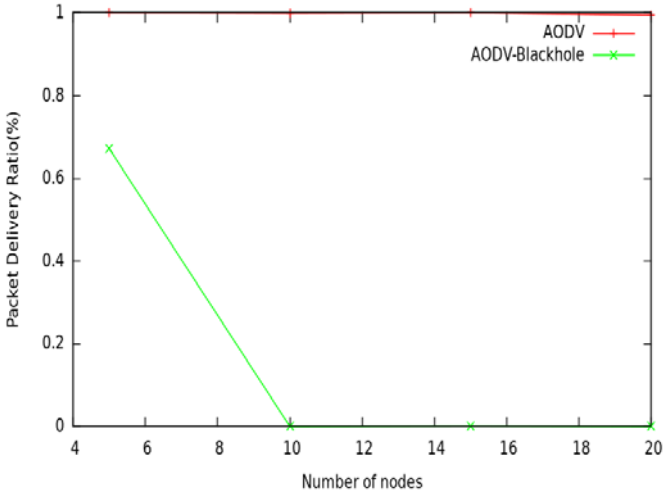

Fig.4.5 Packet delivery ratio for number of nodes with and without security algorithm

Packet Delivery Ratio

Packet Delivery Ratio measures the effectiveness, reliability, and efficiency of routing protocol. Fig.3 shows packet delivery ratio for number of nodes. Graph for both detection and prevention in case of PDR remains same, because as the number of attackers is same in both the cases.

V. CONCLUSION

Using NS2.35 impact of black hole attack is observed for AODV, by varying the number of nodes for different scenarios. The comparison is done on the basis of average throughput, packet delivery ratio, total amount of energy consumed. And we found that a black hole node degrades the network performance in VANETs. So to overcome from this attack we have used security Algorithms. And we got better performance for throughput. This can be extended to study and analysis of other attacks. These results can be used to develop protocol which is secure against the black hole attack.

REFERENCES

[1] Ankit kumar and Madhavi Sinha, “Overview on Vehicular Ad Hoc Network and its Security Issues”, International conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2014.

[2] Haiyun Luo, Fan Ye, SongwuLu, Lixia Zhang, “Security in mobile ad hoc networks challenges and solutions”, Volume-II, Issues-1, PP:38-47, IEEE 2014.

[3] Ankit D Patel, Mr. Kartik Chawda, “Blackhole and Grayhole Attacks in MANET”, ICICES2014-S.A. Engineering College, Chennai, Tamil Nadu, India, PP: 1-6, IEEE 2014.

[4] Rutvij H Jhaveri, MR-AODV “A Solution to Mitigate Black hole and Gray hole Attack on AODV Based MANETs”, Third International Conference on Advanced Computing and communication Technologies, PP: 254-260, IEEE 2014.

[5] Tajinder Kaur and A.K Verma, “Simulation and Analysis of AODV routing protocol in VANETs”, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July-2014.

[6] Rashmi Raiya and Shubham Gandhi, “Survey of Various Security Technique in VANET”, International Journal of advanced Research in computer Science and Software Engineering, Volume-4, Issue-6, June-2014.

[7] Aman deep Kaur and Prakash Rao Ragini, “Study of various Attacks and impact of Gray hole Attack over Ad-Hoc On Demand (AODV) Routing Protocol in MANETs”, International Journal of Engineering Research and Technology(IJERT), Vol-3, Issue-5, May-2014.

[8] Harbir Kaur, Sanjay Batish and Arvind Kakaria, “An Approach to Detect the Worm hole Attack in Vehicular Ad hoc Networks”, International Journal of Smart Sensor and Ad hoc Networks (IJSSAN) ISSN NO-2248-9738, Vol-1, Issue-4, 2014.

[9] Pooja Bansal, Shabnam Sharma and Aditya Prakash, “A Novel Approach for Detection of Distributed Denial of Service attack in VANET”, International Journal of Computer Application (0975-8887), Volume 120-No. 5, June 2015.

[10] Samah Ahmed Senbel, Ahmed Ibrahim and Nagy E Zaki, “Solution to Black hole Attack in Ad hoc On Demand Distance Vector Routing Protocol”, Journal of Computer Science and Applications, Vol-3, No. 4, 90-93,2015.

[11] Sharndeep Kaur and Dr. Anuj Gupta, ”A Novel Technique to Detect and Prevent Black hole Attack in MANET”, International Journal of Innovative Research in Science, Engineering and Technology, Vol-4, Issue-6, June 2015.