Performance analysis of Black Hole Attack on Vanet's Reactive Routing Protocols

Sonia

CSE department

PEC University of Technology

Chandigarh

Padmavati

Assistant Professor,

PEC University of Technology

Chandigarh

ABSTRACT

Vehicle Ad-hoc Network is vulnerable to several attacks. One of the main attacks is the black hole attack which absorbs all the data packets in the network. In this paper, we have analyzed the performance of VANET in presence of black hole attack by using different routing protocols AODV, DSR and AOMDV. This paper analyzed that which protocol is more vulnerable to the black hole attack and how much is the impact of attack on these three protocols. The main parameters considered are throughput, end-to-end delay and scalability. These parameters are compared for each routing protocol both using with black hole attack and without black hole attack. Simulation shows that DSR has high performance in terms of throughput, delay and scalability. The simulation setup comprises of 20 Vehicular nodes moving with constant speed of 10 meter per second. Simulation is carried using Network Simulator (NS2) 2.35.

Keywords

VANET – Vehicle Ad-hoc Network, AODV – Ad Hoc On Demand Distance Vector Routing, DSR – Dynamic Source Routing, RREQ – Route Request, RREP – Route Reply, AOMDV – Ad Hoc On Demand Multipath Distance Vector Routing, black hole attack.

1. INTRODUCTION

VANET is a new form of MANET (Mobile Ad-hoc Network) which consists of number of vehicles with the capability of communicating with each other without a fixed infrastructure. So VANET has highly dynamic topology as compared to MANET [1]. The main challenges in maintaining a good connectivity are high vehicle mobility and variable traffic environment. Due to its open access medium, it is more prone to security attacks. The black hole attack is one of the major security threats in VANETs. In black hole attack, when there is any route request, one malicious node advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [2]. When the malicious node receives an RREQ message, immediately sends a false RREP message over its route, assigning high sequence no. before other nodes send a true one.

In the following, we first introduce some possible attacks in VANET including black hole attack in section 2. In section 3, we describe reactive routing protocols which include AODV, DSR and AOMDV. Section 4 describes the simulation setup and performance metrics. Further section 5 shows the results followed by conclusion and future work.

2. VANET ATTACKS

Attacks are broadly divided in to three groups i.e. attacks on availability, attacks on authentication and attacks on confidentiality which are explained as following.

2.1 Attacks on Availability

It is an attempt by the intruder to make a machine or network resource unavailable to its intended users. It is an effort to temporarily interrupt or suspend the services [3].

2.1.1 Denial of Service Attack (DOS)

In DOS, attacker prevents the legitimate user to accessing the networking services by jamming the network. Black hole attack is type of denial of service attack.

2.1.2 Distributed Denial of Service Attack (DDOS)

This attack is in distributed form as its name implies. In this, attacker uses different location for the attack. They may send messages at different time to different vehicles. This attack is more critical than DOS attack. Other availability attacks may be malware, spamming etc.

2.2 Attacks on Authentication

When an attacker obtains information from an authentication exchange and recovers data and legitimate user's authentication key is compromised [4].

2.2.1 Sybil Attack

In this attack, attacker provide illusion of vehicles by transmitting messages with different Id's to vehicles and vehicles feels that messages are coming from different vehicles and there will be jam further and they take their alternate routes.

2.2.2 Node Impersonation Attack

In VANET, vehicles have unique Id to communicate with other vehicles. In this attack, attacker can change his identity with the originator and can modify the contents of the message on behalf of actual originator.

2.2.3 Replay Attack

In this attack, previous messages are transmitted repeatedly at new connection. This attack is generated by authenticate or malicious user. The main objective of this attack is to mystify the authorities and prevent identification of vehicle in any accident [4].

2.3 Attacks on Confidentiality

The confidentiality attack attempts to gather private information by intercepting it over the wireless link. This attack is of two types i.e. passive and active attacks [2].

2.3.1 Passive Attacks

In which the attacker attack passively by intercepting the messages. Passive attacks do not affect the target and the target is unaware of the attacks e.g. eavesdropping.

2.3.2 Active Attacks

In this attack, attacker intercepts the messages and can modify or drop the message. Active attacks do affect the target and the target is aware of the attack. E.g. Spoofing, Fishing.

2.4 Black hole attack

This attack creates obstacles in a network communication by showing itself as a cooperative node in providing the shortest path. In actual, black hole node is virtual node which doesn't allow data packets to reach at destination so it provide false RREP to source node with highest sequence number and absorbs all the packets [1]. Black hole attack is of two types named as Single black hole attack and Collaborative black hole attack. In single black hole attack, all network traffic is redirected to single black hole node which is malicious node and drops all the packets. In collaborative black hole attack, there are many malicious nodes work together to redirect normal routing information towards them and fabricate that route according to them. Some researchers had work on black hole attack and provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem. So the black hole problem is still research area [5]. Figure 1 shows DSR nam file (dsrblackhole.nam) with black hole attack. It shows that if node 2 is black hole node, node 0 wants to send message to node 5 then node 2 will absorb the packets and don't allow packets to reach at node 5.

Figure 1: NAM of DSR with black hole(dsrblackhole.nam)

3. REACTIVE ROUTING PROTOCOLS

This type of protocol finds on demand path by flooding the network with Route Request Packet (RREQ). These protocols are also known as On Demand Routing Protocols.

3.1 AODV Routing Protocol

AODV is On Demand Routing Protocol. They are not maintained periodically but routing tables are created only when required. This adds advantage over Table Driven Routing protocols in which every node has to keep up to date routing tables. This Routing Protocol is used for finding a path to the destination in an ad-hoc network. AODV include three control messages RREQ (Route Request) and RREP (Route Reply) and RERR (Route Error) [6], [7]. When any node needs path for destination, RREQ is broadcast to all neighboring nodes. If any neighboring node has path, that node send RREP to source node otherwise forward RREQ to its neighboring nodes. on receiving RREP, source node send data packet to the node which has path for destination. The process continues until the packet is received by destination node. AODV provides unicast, multicast and broadcast communication [8].

3.2 DSR Routing Protocol

The Dynamic Source Routing (DSR) is a reactive routing protocol based on the concept of source routing [6]. Like AODV, DSR uses no periodic routing messages but for maintenance of route information it uses cache technology [9]. As it uses no periodic routing protocols, it reduces bandwidth overhead, maintains battery power and avoids large routing updates. DSR has two phases namely Route Discovery and Route Maintenance [14.] When a node wants to send a packet, it checks its route cache. If it has destination path, it forward the packet. Otherwise, the source node initiates a route discovery process by broadcasting RREQ. Neighboring node checks its route cache by receiving a route request. If the node doesn't have routing information for the RREQ, it appends its own address to the route field. Then, the request packet is forwarded to its neighbors. If the requested packet reaches to its destination, a route reply packet (RREP) is generated [15]. After route generated by destination, it comprises addresses of nodes that have been traversed by the route request packet. As DSR uses route cache mechanism it reduces route discovery control overheads[10].

3.3 AOMDV Routing Protocol

AOMDV is Ad Hoc on Demand Multipath Distance Vector Routing. AOMDV is multipath extension of AODV. This protocol is based on hop to hop routing but ensures loop freedom and disjointness of alternate paths [11]. The routing entries contain a list of the next-hops with their hop counts. All have the same sequence number. This helps in keeping track of a route [12]. The benefit of using AOMDV is that it allows in between nodes to reply to RREQs, while still selecting disjoint paths. But it has message overheads during route discovery since it is a multipath routing protocol, the destination replies to the multiple RREQs causes overhead.

4. SIMULATION TOOL AND SETUP

Simulation is performed using simulator NS2 2.35. It is popular simulator in the ad hoc networking community. NS2 advantage of using it over other simulator is that it is freely distributed, open source, flexibly configured [13]. At terminal, it produces NAM (Network Animator).

Table 1: Simulation Parameters

Simulator	NS-2(ver. 2.35)
Simulation time	100 sec
No. of nodes	8, 20
Routing Protocols	AODV, DSR and AOMDV
Traffic Model	CBR
Terrain Area	1000m x 1000m
No. of malicious node	1

The aim of paper is to determine which routing protocol is less vulnerable to black hole attack. Simulation is carried to compare for three routing protocols AODV, DSR and AOMDV. Each scenario has two simulations. In the first one every node is working in cooperation with each other to keep the network in communication. The second simulation has communication in presence of black hole attack.

4.1 Performance Metrics

Metrics selected to evaluate performance of routing protocols are throughput, end to end delay and scalability.

4.1.1 Throughput is the ratio of total no. of packets received to total no. of packets send by the sender. It is affected by topological changes, bandwidth and unreliable communication. Throughput is measured in terms of bits per second [5].

4.1.2 End to end delay is time elapsed for a packet to be transmitted from the source node to the destination node.

4.1.3 Scalability of network or process is defined as its ability to be enlarged with its growth. Scalability is compared for three routing protocols by increasing no. of VANET nodes.

5. RESULTS AND DISCUSSIONS

Comparison of three routing protocols AODV, DSR and AOMDV is carried out in VANET with black hole attack and aim of the paper is to analyze which protocol is more vulnerable to black hole attack. It is analyzed that all the three VANET protocol shows high performance without black hole attack than with black hole attack.

Figure 2: Throughput with and without black hole attack

As shown in Figure 2, DSR shows high throughput than AODV and AOMDV in both with and without black hole

attack. Each node spends maximum time on updating their routing tables in AODV and DSR is based on cache strategies due to which overhead reduces and maximum packets are sent from source to destination. At extreme time 100 seconds, the throughput of DSR is quiet higher which is constant and continuous from 20 seconds. If the no. of nodes is increased from 8 to 20 with black hole attack as shown in Figure 3, again DSR shows high throughput than AOMDV and AODV. Higher the throughput, higher is the rate of performance. So, there is good indication of performance for DSR. Finally the graph clearly depicts that AODV is quiet effective as compared to AOMDV.

Figure 3: Throughput with black hole attack having 20 nodes

As shown in Figure 4, it clearly demonstrates the various effects of delay as accordance to time as this delay indicates the better performance. As VANET has a feature of high mobility. The average packet delay increases with mobility for AOMDV and AODV but DSR has a lower delay than AODV and AOMDV at higher mobility values due to the way routes are detected in DSR. The route acquisition procedure in DSR allows more routes to be detected and cached than in AODV, which obtains a single route per RREQ. With DSR, packets wait less during route acquisition than with AODV. AOMDV delay is highest (effect of Black Hole increases the end to end delay) which is 5500. AODV delay is 5000 and it is continuously increasing which is quiet clear from the slant straight line graph. DSR delay is decreasing initially and finally from both points. So, these are data with the implementation of the Black Hole. In case of without black hole attack, Due to sharp increment from 20-100 seconds, AODV and AOMDV decrease so far. Finally at time 100 seconds, the delay of AOMDV is highest among three protocols used which is near about 4700. After that AODV which is near about 4800 and finally DSR having 4000. So with and without black hole attack DSR shows less delay than AODV and AOMDV.

Figure 4: End to end delay with and without black hole attack

If scalability is analyzed, then according to Figure 5, DSR shows less delay than AODV and AOMDV. AOMDV shows higher end to end delay. So overall, DSR shows better results than AODV and AOMDV.

Figure 5: End to end delay in black hole attack with 20 nodes

6. CONCLUSION AND FUTURE WORK

Security of VANET is very important feature for its deployment. This paper analyzed possible VANET security threats and mainly focuses on black hole attack. Many researchers provide mechanism for black hole detection and prevention but they are not applicable to the extent that we can say VANETs are secure from black hole attack. Comparison of reactive routing protocols AODV, DSR and AOMDV is carried out. After all experiments and simulation we conclude that DSR performance is better than AODV and AOMDV with and without black hole attack. In all scenarios, DSR outperforms in terms of throughput and delay as compared to AODV and AOMDV. Results shows that DSR is much scalable than other routing protocols. So we conclude that DSR is better routing protocol to be deployed in VANET,

Out of all three routing protocols, black hole node has high impact on AOMDV than AODV and DSR. We tried to analyze the impact of black hole attack in VANETs using AODV, DSR and AOMDV. Similarly other attacks like greyhole attack, jellyfish attack, and wormhole attack need to be study in VANET. Performance of other protocols GRP, TORA under these attacks in VANET can be taken as future work.

7. REFERENCES

- [1] C. Hernandez-Goya et al., "Cooperation Requirements for Packet Forwarding in Vehicular Ad-Hoc Networks (VANETs)", ACM International Conference On Computer Systems and Technologies, 2009, pp. 1-6.
- [2] Fan-Hsun Tseng, Li-Der Chou, and Han-Chieh Chao, "A Survey of black hole attacks in Wireless Mobile Ad Hoc Networks", SPRINGER Human-centric Computing and Information Sciences, 2011, 22 Nov. 2011, pp. 1-16.
- [3] Vimal Bibhu et al., "Performance Analysis of black hole attack in VANET", International Journal Of Computer Network and Information Security, Oct. 2012, pp. 47-54.
- [4] Ajay Rawat, Santosh Sharma, and Rama Sushil, "VANET: Security Attacks and its possible solution", Journal of Information and Operations Management, vol. 3, Issue 1, 2012, pp. 301-304.
- [5] Arti Sharma, Satendra Jain, "A Behavioral Study of AODV with and without black hole attack in MANET", IJMER International Journal of Modern Engineering Research (IJMER), vol. 1, Issue 2, pp. 391-395.
- [6] P. Manickam et al., "Performance Comparison of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networking (IJWMN), vol. 3, no. 1, Feb. 2011, pp. 98-106.
- [7] M.Geetha et al., "Performance Comparison and Analysis of AODV and DSDV Gateway Discovery Protocol in MANET", International Journal of Engineering Science and Technology, vol. 2(11), 2010, pp. 6521-6531.
- [8] Anuj K. Gupta, Dr. Harsh Sadawarti, and Dr. Anil K. Verma, "Performance analysis of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering and Technology, vol. 2, no. 2, April 2010, pp. 226-231.
- [9] Yih-Chun Hu and David B.Johnson, "Caching Strategies in On-Demand Routing Protocols for Wireless Ad hoc Networks", ACM 2000, pp. 1-12.
- [10] Rajeev K. Shakya, NS2 Guide, 2010; <http://home.iitk.ac.in/~rajeevs/research-ns2.html>
- [11] Mahesh K. Marina, Samir R. Das, "Ad Hoc On Demand Multipath Distance Vector Routing", Wireless Communication & Mobile Computing, 2006, pp. 969-980.
- [12] S. R. Biradar et al., "Performance Evaluation and Comparison of AODV and AOMDV", IJCSE, vol. 02, no. 02, 2010, pp. 373-377.
- [13] Sheenu Sharma, Roopam Gupta, "Simulation study of black hole attack in Mobile Ad Hoc Network", Journal of Engineering Science and Technology, vol. 4, no.2, 2009, pp. 243-250.

- [14] Uma Nagaraj, Dr. M. U. Kharat, Poonam Dhamal, “Study of Various Routing Protocols in VANET,” IJCST International Journal of Computer Science & Technology, vol. 2, Dec. 2011, pp. 45-52 .
- [15] Shaikhul Islam Chowdhury et. al., “Performance Evaluation of Reactive Routing Protocols in VANET,” IEEE, Oct. 2011, pp. 559-564.