International Journal of Science and Engineering Applications
Volume 8–Issue 07,258-260, 2019, ISSN:-2319–7560

Performance Analysis of Black Hole attack in MANET

Dr. Khin Khat Khat Kyaw
Associate Professor
Information Technology Department
West Yangon Technological University, Yangon,
Myanmar

Abstract: Due to the mobility and non-centralized management, Mobile adhoc Network (MANET) is broadly used in current communication system. The researchers have been proposed various MANET routing protocols in order to improve network reliability. However, most of the MANET routing protocols have lack of attack prevention. While the MANET communication system becomes larger, the various types of attacks appear in parallel. Therefore, performance analysis of attacks in routing protocols is one of the important issues in the case of MANET improvement. In this paper, two routing protocols, AODV and DSDV were tested with black hole attack. The performances of those two protocols were compared when they were attacked by malicious node.

Keywords: Black Hole attack, MANET, AODV, DSDV,NS2

1. INTRODUCTION

MANET allows devices to create a network on demand without prior configuration. Thus, nodes within a MANET are involved in routing and forwarding information between neighbors [1]. As shown in [1], the basic characteristics of MANET are network infrastructure, network topology, self-organization, limited resources and poor physical security. Consequently, the design of a routing protocol should be considered with the following issues: distributed network, dynamic topology, power awareness, addressing schemes, network size and security. In order to improve security goals, the routing protocols should be analyzed with various attacks.

2. Related Work

In [2],the authors defined that network overhead, processing time and energy consumption were the three security parameters in MANET. Security issues can be categorized into two types: security services and attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service. They discussed that the important security services were availability, authentication, confidentiality, data integrity and non-repudiation. Detecting and eliminating malicious nodes, is another aspect of the MANET security. Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows: black hole attack, worm hole attack, Byzantine attack, Snooping attack, Routing attack, Resource consumption attack, Session hijacking, Denial of service, Jamming attack, Impersonation Attack, Modification Attack, Fabrication Attack and Man-in-the-middle attack.

The detection system for black hole attack was proposed in [3]. To detect the black hole attack their proposed system checks the RREPs that come from multiple paths. As the black hole node immediately send RREP message to the source without checking its routing table, it is more likely that the first RREP comes from the black hole node. Then the solution will discard the first RREP packet using the route reply saving mechanism that come from malicious node and choose the second RREP packet. The authors used NS-2.35 for the simulation and compared the result of AODV and BDS solution under black hole attack. The BDS solution against Black hole node has high packet delivery ratio as compared to the AODV protocol under black hole attack.

In wormhole attack, an attacker creates a tunnel between two points in the network and creates direct connection between them as they are directly connected[4]. Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. This attack compromises the security of networks. A potential solution is to avoid wormhole attack is to integrate the prevention methods into intrusion detection system but it is difficult to isolate the attacker using only software based approach because the packets sent by the wormhole are similar to the packets sent by legitimate nodes. All the simulation work was performed in OPNET MODELER network simulator version 14.0. The effect of wormhole attack was analyzed by using parameter like number of hops, delay, retransmission attempt, and data dropped.

MANET often suffers security attacks more than wired networks because of its nature features such as dynamic topology and open medium[5]. Some these attacks are such as wormhole attacks, flooding attack, gray-hole attack, routing table overflow attack, Denial of Service (DoS) attack, selfish node misbehaving, impersonation attack, black hole attack, modification attack, etc. The warm hole attack creates a tunnel by attackers which placed themselves in the strategic position of the network; declare the tunnel as a shortest path of transmission in order to record the traffic or ongoing packets, also transfer usually the selective information to other location, and then retransfer them to the network. In black hole attack, when a malicious find out that neighbors initiate to send a RREP packet, it RREP the fake packet with highest value of sequence number and lowest hop count, order that it assumes that this malicious node has the best route to the destination. Thus, the source node discards all other RREPs; malicious node drops all the packets in other words, it stops forwarding packets to the right destination. In the flooding attack, the attacker set up path between network's nodes to disseminate its unpleasant packets and congest the network.

The authors implemented a cryptographic and trust based system to enhance the security of the Zone Routing Protocol

(ZRP) so that the communication between the source and the destination can be made secure along with the additional security of the intermediates nodes[6]. To prevent the Denial-of-Services (DoS) Attacks, keyed-Hash Message Authentication Code – Secure Hashing Algorithm 512 (HMAC-SHA512) is implemented. HMAC-SHA512 guarantees that the data packets are received by the destination only and in its original form but at the expense of the increased processing time at the source and the destination. The Trust Based system increases the Packet Delivery Fraction (PDF) but at the expense of the increased End to End Delay. The simulations further show that as the malicious nodes percentage goes past 30%, the performance of the system degrades considerably. Furthermore, the mobility plays an important role while analyzing the network. If the pause time is increased, the mobility decreases that leads to more stable networks.

In a wormhole attack two nodes are connected with one another with the help of a medium which is not available to normal nodes, with the help of this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot[7]. The authors have proposed an approach that will be using the information present in the routing table for the detection of the wormhole links. The approach has been applied to DSDV and the detection of self-sufficient wormhole nodes and attacks.

3. AODV and DSDV

Ad-hoc On-Demand Distance Vector Routing (AODV) protocol provides self-starting, dynamic, loops free, multihop routing[8]. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to the destinations that are not in active communication. New routes are created on demand. It means control packets are broadcast when needed and hence eliminate the need for periodic broadcast of routing updates. AODV protocol works in two phases a) route discovery process and b) route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path. RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for route freshness, loop prevention and faster convergence. Route maintenance is performed with two additional messages: Hello and RRER messages.

The idea of Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) protocol was introduced in 1994[9]. The design is to operate each Mobile Host as a specialized router, which periodically advertises its view of the interconnection topology with other Mobile Hosts within the network. Packets are transmitted between the stations of the network by using routing tables which are stored at each station of the network. Each routing table, at each of the stations, lists all available destinations, and the number of hops to each. Each route table entry is tagged with a sequence number which is originated by the destination station. To maintain the consistency of routing tables in a dynamically varying topology, each station periodically transmits updates, and transmits updates immediately when significant new information is available.

4. Black Hole Attack

Mobile Ad Hoc Network using the AODV protocol faces an attack named Blackhole attack where a malicious node or Blackhole node consumes the network traffic and drops all data packets[3]. When the source node(A) broadcasts the RREQ message for destination node(D) to establish a path for data transfer, the malicious node(B) immediately responds to source node(A) with a false RREP message showing that it has the highest sequence number of destination node(D), as if it is coming from Node (D). Node A assumes that Node D is behind Node B with 1 hop count and discards the newly received RREP packet come from Node C or E. Node A then starts to send out all data packet to the node B. Node A is trusting that these packets will reach Node D but Node B will drop all data packets. The malicious node or Black hole node takes all the routes coming up to itself. It stops forwarding any packet to any other nodes. The network operation is hampered as the black hole node B consumes the packets easily.

5. SIMULATION RESULTS

The Blackhole attack was implemented for AODV and DSDV protocols. Then the performance of attacks was examined by using NS2 simulator. In NS2,all routing protocols are implemented in the directory ”ns-2.35”.
In the file “aodv.h”, the malicious variable was added as *bool malicious*. Then “aodv.cc” was modified to declare malicious node as follows:

```
if(strncasecmp(argv[1], "hacker", 6) == 0) {
    malicious = true;
    return TCL_OK;
   }
```

Figure. 1 Malicious Node Declaration

For the malicious node, the packets are dropped out with the following code:

```
if(strncasecmp(argv[1], "hacker", 6) == 0) {
    malicious = true;
    return TCL_OK;
   }
```

Figure.2 Dropout Packets Creation

Next, the “tcl” file was implemented as shown in Table 1.

Table 1. Node Creation for Simulation

Total nodes	7
Source node	0
Destination node	3
Attacker node	5

Similarly in DSDV protocol, “dsdv.h” and “dsdv.cc” were also modified.
There were four “tcl” files for this simulation:”aodv with attack”,”aodv without attack”, “dsdv with attack” and “dsdv without attack”. The “tcl” files were compiled to get “trace” and “nam” files. According to trace files, the number of sent packets, the number of received packets, and the number of dropped packets were compared. The analysis results are shown in Table2 and Table3. Figure 3 shows the example of running “nam” file.

Table2. Simulation Results for AODV

	Sent	Received	Dropped out
Attack	1238	0	1238
No attack	1238	1238	0

Table 3. Simulation Results for DSDV

	Sent	Received	Dropped out
Attack	1319	1469	4064
No attack	1319	1462	4016

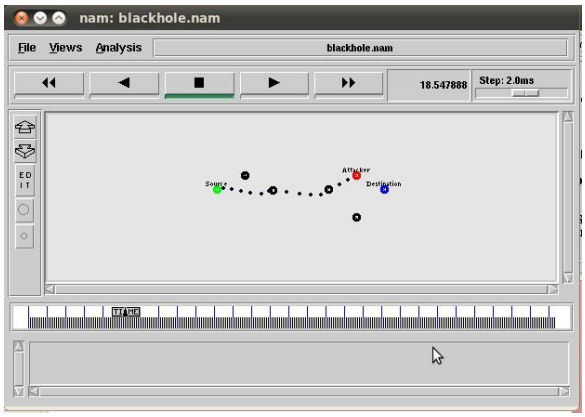

Figure 3. Simulation for Blackhole attack in AODV protocol

Under the Blackhole attack, AODV cannot work properly since all the packets are dropped out by the attacker. In DSDV protocol, the dropped out packets with Blackhole attack increase 25% more than the dropped out packets with no attack.

6. CONCLUSION

In MANET, most routing protocols do not include security issue. Therefore, analysis on attacks in MANET is an important research to improve mobile adhoc network communication. In this paper, the two routing protocols, AODV and DSDV, are analyzed with Blackhole attack. According to simulation results, Blackhole attack can drop out all the packets in AODV protocol. On the other hand, Blackhole attack can drop out 25% more than the dropped packets in normal case. The future work is to search how many percent of sent packets has been dropped by Blackhole attack in DSDV.

REFERENCES

[1] Ms. Rajni1 , Ms. Reena2. Review of MANETS Using Distributed Public-key Cryptography. International Journal of Computer Trends and Technology (IJCTT) – volume 10 number 3 – Apr 2014.

[2] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah. Security Challenges in mobile adhoc networks. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.

[3] Ashok Koujalagi. Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET.American Journal of Computer Science and Information Technology,ISSN 2349-3917, Vol.6 No.2:25, June 2018.

[4] Achint Gupta, Dr. Priyanka V J, Saurabh Upadhyay. Analysis of Wormhole Attack in AODV based MANET Using Opnet Simulator. International Journal of Computing, Communications and Networking, Vol.1, No.2, September-October 2012.

[5] Mahsa Gharehkoolchian. Improving Security Issues in MANET AODV Routing Protocol. https://www.researchgate.net/publication/285512741.

[6] Dilli Ravillaa, Chandra Shekar Reddy Putta. Enhancing the Security of MANETs Using Hash Algorithms. Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015).

[7] Zubair Ahmed Khan, M. Hasan Islam. Wormhole Attack: A new detection technique. https://www.researchgate.net/publication/261158779.

[8] Preeti Sachan and Pabitra Mohan Khilar. Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[9] Perkins C.E and Bhagwat P. Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV)for Mobile Computers. SIGCOMM ACM, 1994, pp. 234-245.