DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5054

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

COLLUSION BW HOLE ATTACK

Sunil Kumar Jangir
Department of Computer Science and Engineering,
JECRC University,Jaipur,
Rajasthan,India

Naveen Hemrajani
Department of Computer Science and Engineering,
JECRC University,Jaipur,
Rajasthan,India

Abstract- In this world of technology, it is important to provide security and to find the loopholes present in the network. There are two types of networks – wired network and wireless network. Wireless network is more vulnerable to attacks as compared to the wired networks as a number of nodes are never fixed in wireless network. Any node can come and join the network as well as any node can leave the network. This paper includes conclusions of some Denial of Service attacks and their effect on the MANETs, How they attack and which methodology they adopt. This paper mainly focuses on proposing a new attack which can cause severe harm to the network. This attack inhibits the strategy of two main attacks –BlackHole and Wormhole attack. This attack actually works in collaboration with some internal nodes which will work for a malicious node and will help that node in causing disruption to the network. In particular, this paper describes all the weak areas of a network that can be targeted by this new attack.

Keywords: MANET; DOS ;Security Attacks

1. INTRODUCTION

As already mentioned, this paper proposes a new attack, a type of a Denial of Service attack which can not only slow down the network but can also result in defaming as it is hard to find outthe actual intruder in the network. The name of this attack is Collusion BW Hole Attack .As in MANET, the communication starts when there is a node that has a data or a message packet that is to be sent to some other node. For the transmission of this packet the source node will choose a path which is both secure and less time consuming. For selection of this path the source node will look for the routing tables of other nodes and will find a suitable path to transmit the packet. Here, in Collusion BW attack, the intruder will take advantage of this demand of source node to hack the network and will eventually steal or drop the data. The intruder node will work with two or more internal nodes, who will form a tunnel and simultaneously send that data to the intruder node rather than sending it to the desired node. The whole methodology and strategy of this new proposed attack is described further in the paper. This paper includes only the description of this attack, the methodology that can be used by these intruding nodes and the weaknesses of a network that can be targeted by this attack.

2. MANET

Mobile Ad Hoc Network is a cluster of mobile nodeswhich can communicate with one another without a specified and predefined topology or central administration. MANETs are dynamic in nature, which means any node which wants to communicate can join the network and similarly any node can leave the network after the completion of its work at any time. It provides flexibility asthere is an absence of centralized system and it follows a decentralized system which means there are no server and client. Thus, it offers a peer-to-peer network in which any node can act as a host and as a router at the same time.[1] It is very easy to form a MANET network at cheap prices as it does not follow the predefined and centralized infrastructure, this property is the reason why MANET is widely used and becoming popular nowadays. But due to its flexible and dynamic nature, it is becoming vulnerable to many severe attacks. These attacks are mainly intended to steal the information that is transferred among communicating parties.[2,3]

As in MANET no restriction is applied on the nodes, any node can join the network, this can lead to severe consequences like eavesdropping, stealing of information, denial of services, response delay etc.

As compared to wired network A MANET is more prone to attacks due to the following factors:

• The Nodes have limited energy due to whichsecurity solutions that are complex cannot be used in MANET.

• Transmission of data packets and routing is done using wireless medium.Wireless medium being a shared network and generally unreliable and makes eavesdropping more likely. Even if we make the channel reliable, the communication might be unreliable due to the broadcasting nature of the MANETs.

•MANET does not have any central management point or node, which makes it hard to ensure that all the nodes that are taking part in the network are benign.

• Routing is very challenging because the network topology of network keeps on changing and the mobility of nodes plays a very important role in the network.[4-6]

3. AODV

An Ad hoc On-Demand Distance Vector routing protocol is tailored particularly for the mobile nodes, where the time span for the establishment of new network and the termination of previous one is not fixed. Thus, this protocol seeks to provide less processing time, memory consumption and network utilization as well as fast adaption to dynamic forming links. It works on destination sequence numbers and gives loop freedom[9][13-15]

3.1 Security Flaws in AODV

AODV is vulnerable to routing attacks due to lack of security features; some more secure protocols are generally

designedto provide the authentication,confidentiality, integrity and non-repudiation.AODV can easily be compromised by a malicious node to disrupt its routing. The misbehaviour of an inside attacking node is discussed in.
The actions that are performed by the inside attackers to disrupt the routing in AODV are
1) It may modify or forge the RREQ or RREP packets.
2) To work as a legitimate node it may spoof either the destination IP or the source IP and thus is able to receive or drop data packets.
3) To degrade the performance of the network and to increase the routing delayit may generates a fake RERR packet,
4) The attacker may send fake RREPs of highest sequence numbers (like Blackhole attack) to cause a DoS attack.
5) To deplete the node batteries, it may create the routing loops and launch sleep deprivation or resource consumption attacks.
6) To disrupt the normal routing behaviour it replays old routing messages or make a tunnel/wormhole.[7-13]

4. COLLUSION BW HOLE ATTACK

When an RREQ(Route request packet) is sent from a source node to other nodes in the network for the transmission of the package then the malicious node MN1 in the network may send Route Reply (RREP) with higher sequence number. As we know that the higher sequence number is replaced by the lower sequence number and allows the source node or other node to transmit the packet with the node with higher sequence number. Here the source node transmit the packet from the malicious node and the malicious node MN1 again send route request (RREQ) for the transmission of packet then again a malicious node MN2 send route reply with higher sequence number and the packet is again transmitted through the malicious node MN2. When a packet is transmitted to second malicious node MN2 in the network it tunnels the packet to the other malicious node MN3. When the packet is tunneled to the malicious node MN3 then usually broadcast of RREQ occurs but here in this attack case uni-cast occurs and the packet is dropped. This attack satisfies the vulnerability present in AODV so this attack is not possible to detect easily which are.

1) To modify or forge RREQ or RREP packets.
2) Source IP address or Spoof destination pose as the legitimate network node and thus drops or receive the data packets.
3) Make a tunnel/wormhole or replay old routing messagesto disrupt the normal routing behaviour.

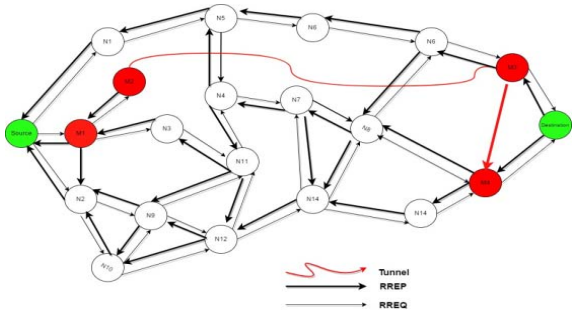

Figure 1: How a packet is dropped in Collusion BW Hole Attack

In AODV there is black hole and worm hole attack. In worm hole attack the attacking node capture the packet from one location and transmits that to the other node which is located at distant. A wormhole attack can be exploited very easily by attacker without compromising with the legitimate node and without having the knowledge of that. Whereas in black hole attack, when the source node attempts to send some data packets to a destination node, and starts the routing discovery process thena malicious node, MN1 shows that it has the route for the destination node every time it receives RREQ packets. Then it sends the response to source node at once. If the reply from a normal node for example (N1,N2,...,N14) etc. reaches the source node of the RREQ first, everything works well but when the packet is received by MN1 node then it makes the source node think that the routing discovery process is completed and ignores all other reply messages, and starts to send data packets. A forged routing has been created. As a result of which all the packets through MN1 are simply lost or consumed and never received by its desired destination.
Collusion BW Hole Attack is different from these attack because in this attack the packets are dropped once received by the malicious node where as in Collusion BW Hole Attack there is no packet drop by first malicious node and in worm hole attack after tunnelling the broadcast of packet occur while in Colliding Collusion BW hole attack uni cast occur and the packet is dropped by the malicious node but at the same time the RREP and RREQ route request and reply of the neighbour legitimate node are managed such a way that the dropped packet node(malicious node) can never be identified.

4.1 Symptoms of Attack

Hence we can make a conclusion that our attack Collusion BW Hole Attack is valid only when:
Case 1: The Malicious Node MN1 receives the packet from the source node by sending the higher sequence number of route reply RREP of the route request RREQ sent by the source node (Malicious Activity).
Case 2: After tunnelling when the malicious node MN3 receive the packet there must occur a unicast instead of broadcast and the packet is dropped after the tunnelling. It means here is forge that MN1 is going to drop the packet but from MN1 to MN3 they keep transmitting the packets among them self resulting in Spoofing of the destination and IP address to work as legitimate node.

4.2 Proposed Attack Model

N_L: Set of legitimate nodes.
N_M: Set of malicious nodes.
N: Total Number of nodes used i.e., NL □ N_M
B: Packet Drop By the Node

Collusion BW Hole Attack: An ordered set of attackers {MN1, MN2, MN3 ...},MN is the malicious node. MN1 is first malicious node that receives packet from the source by sending route reply of high sequence number to the source node and works as legitimate node
if A is any node such that A $\longrightarrow$B then A$\longrightarrow$ N_M must be true. As there can only be packet drop in the network only if

that node is a malicious node which means A must belong to malicious node A $\longrightarrow N_M$ (MN1, MN2, MN3...). Collusion BW Hole Attack is executed then N $\longrightarrow N_M$ which means that all the nodes taking part must me malicious node, and also $N_M N_L$ this happens when a route request of high sequence number Seq_no. to the source node when it sends the route request to the neighbouring node.

4.3 How Is It More Dangerous Than Other Attacks

The Collusion BW Hole Attack defined in this paper can result in more disastrous effects as it posses the pros of two types of attacks with diminished cons. The following key points describe its harmful consequences.

- In this attack two or morenodes will work in a collaboration to form a tunnel and the information they are stealing from the network will be sent to a node which is an intruder who wants to slow down the network. Now, identifying this third node which is not displaying any suspicious activity is a tough row to hoe.
- Secondly, the nodes which are working for the main intruder node will sometimes show their illegitimate nature and other times they will behave as normal genuine nodes. Thus, confusing the network handler and making it hard for him to be found at once.
- Third key factor in this attack is that even if the tunnel making nodes are identified by the network handler but still the identity of the main intruder node will be hidden as while being in the network the tunnel making node will never show any suspicious activity.
- The main intruder node is not bounded to be in the network, it may happen to be some external node which just wants to eavesdrop to the communication that is taking place between the nodes that are present in the network. Every algorithm can be applied to the nodes communicating in the network, but for outsiders it is impossible to predict which node is genuine.
- Also, if the main intruder node is disguising in the network, then it will properly hide its identity and won't display any suspicious activity. It will be completely dependent on the tunnel which is formed by the two disguised malicious nodes in the network.

Thus, these points' sums up the whole idea of Collusion BW Hole Attack and how it can be more harmful to a network then other Denial of Services attacks in MANETs like Blackhole attack, Wormhole Attack, etc. The tunnel formed in this attack plays a vital role in hiding the identity of the main intruder node.

5. SIMULATION & RESULTS

Table 1: Simulation Parameters

Parameter	Value
Simulator	NS3
Area	1000 x1000
Simulation time	500 sec
MAC	802.11
Application traffic	CBR
Routing protocols	AODV
No. of S-D pairs	8
Pause time	10 sec
No. of malicious nodes	2 – 10
Bandwidth	2 Mbps
Data payload	512Bytes/Packet
Maximum speed	10 – 50 m/s
No. of nodes	100

5.1 Effect of number of attackers in network

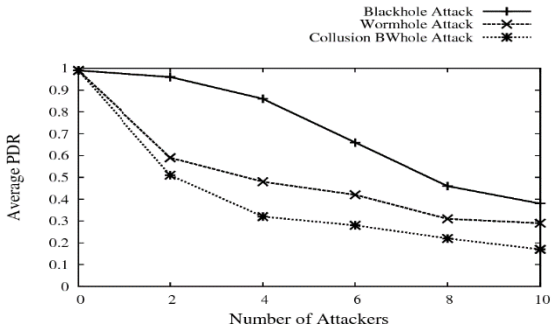

Figure 2 : Average PDR with increasing number of attackers.

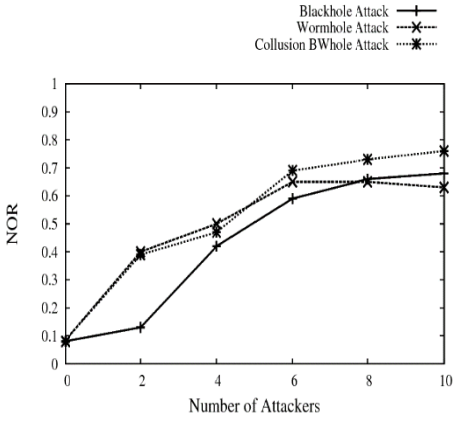

Figure 3: NOR with increasing number of attackers.

Since the ratio of source-destination pair is fixed while the effect of attackers on various network parameters increases due to the ever increasing number of attackers. As shown in figure the average End to End Delay increases as the number of attackers increases this is because the attackers either drop the packet or keep on rotating the packet in a single loop. Here Collusion BW hole Attacks have the highest Average ETE Delay as in this case the packet is tunnelled and rotated in its own loop for IP table updation so

that it works as a legitimate node and cannot be identified. Average PDR increases with increasing number of attackers as the packet starts dropping with increase in attacker effect. The effect of NOR increases with increase in the attacker as it broadcasts the messages used for route discovery which will be large in number and since the number of attacker increases the route will include various attacker node for the destination but in Collusion BW hole attack it will be maximum as no broadcast occur, here unicast occur so very less chance that the broadcast message is received by any legitimate node.

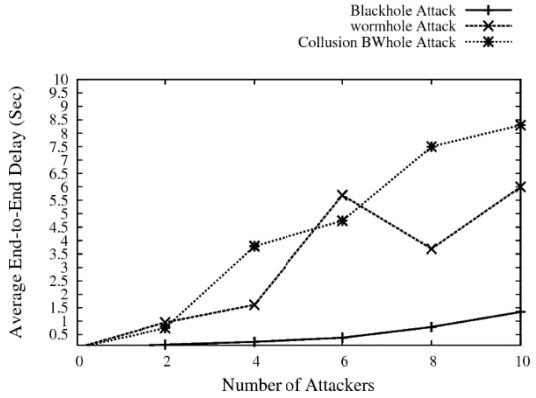

Figure 4 : Average ETE Delay with increasing number of attackers.

5.2 Effect of Network Size

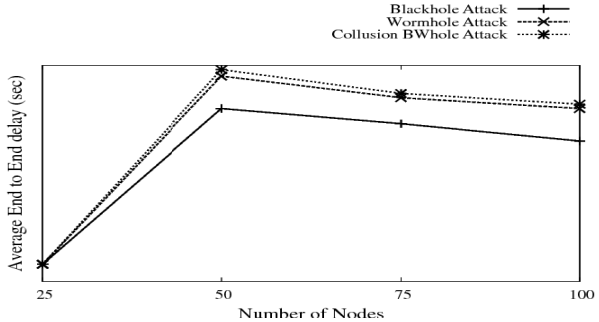

Figure 5 : Average ETE Delay with increase in network size

The effect of Attacker node is very less in low dense network and vice versa because of the lesser number of nodes, the probability that the attacker becomes a part of the discovery route is very less. The PDR decreases with an increase in the network size as the number of packets transmitted by the source will be always less than the packets that are received by the destination node. The packet drop increases as number of nodes increases so the PDR decreases the Collusion BW Hole attack has the minimum PDR in this case. Normalize Routing Overhead increases if number of nodes increases as with an increasing number of nodes the broadcast messages which are used for the route discovery also increases gradually so average End to End Delay also increases if the network size increases.

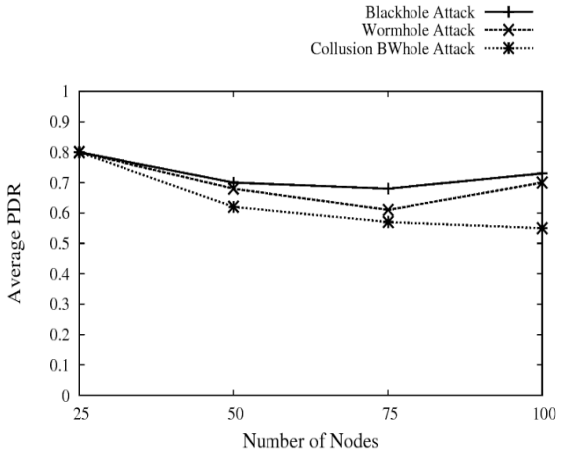

Figure 6 : Average PDR with increase in network size

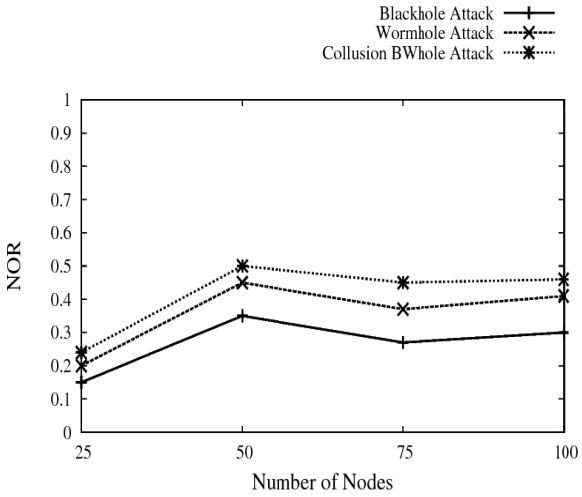

Figure 7 : NOR with increase in network size

6. CONCLUSION

As per the simulation result it can be concluded that in previously purposed attacks when a Malicious node receives a packet from the source node by generating the route reply of high sequence number and a large amount of route request is generated which increases the amount of traffic in the network which alarms the network that a packet has been hijacked by the attacker, also when a malicious node tunnel the packet to other malicious node then the broadcast occurs which helps in identification of the malicious node and the attack.

In our Collusion BW Hole Attack as each node sends the route reply to the source node so there is very less time gap between the reply of the Malicious node and the legitimate node and also the packet is not dropped by the malicious node at the beginning , after tunnelling of the packet to other malicious node the unicast occur which also keep the malicious node safe from being detected and the packet is dropped somewhere near the destination node which assures the network that the packet transmission was going in the legitimate route so no detection technique works to detect this attack.

7. REFERENCES

[1]. Pravin R Satav; Pradip M. Jawandhiya "Review on single-path multi-path routing protocol in manet: A study"International Conference onRecent Advances and Innovations in Engineering (ICRAIE) ,(2016)

[2]. Yuxia Bai; Yefa Mai; Nan Wang "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs"Wireless Telecommunications Symposium (WTS) ,(2017)

[3]. Mohd Imran; Mohammad Abdul Qadeer "Evaluation Study of Performance Comparison of Topology Based Routing Protocol, AODV and DSDV in MANET" International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE),(2016)

[4]. Sharma B.S., Chauhan N," Security issues and their solutions in MANET" International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), New Delhi, India(2015)

[5]. Salehi M. and Samavati H. , "Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks". Sixth International Conference on Next Generation Mobile Applications, Services and Technologies, 100(2011).

[6]. Mike Burmester; Breno de Medeiros "On the Security of Route Discovery in MANETs"IEEE Transactions on Mobile Computing, Volume: 8, Issue: 9 pp: 1180 - 1188, DOI: 10.1109/TMC.2009.13,(2009)

[7]. Kishor Jyoti Sarma; Rupam Sharma; Rajdeep Das "A survey of Black hole attack detection in Manet" International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),2014

[8]. Revathi B., D.Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET" International Journal of Computer Science and Management Research ,1(2) (2012).

[9]. Sunil J. Soni; Suketu D. Nayak "Enhancing security features & performance of AODV protocol under attack for MANET"International Conference on Intelligent Systems and Signal Processing (ISSP) , (2013)

[10]. 10.Nikam D.P,Raut V.,"Improooved MANET Security Using Elliptic Curve Cryptography and EAACK" International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur ,India(2015)

[11]. Kannhavong B. , Nakayama H. , Nemoto Y., Kato N. and Jamalipour, " A survey of routing attacks in mobile ad hoc networks". In Wireless Communications, IEEE 14 (5),85-91,(2007).

[12]. Gupta C.,Pathak P., "Movement based or neighbor based tehnique for preventing wormhole attack in MANET", In Symposium on Colossal Data Analysis and Networking (CDAN),(2016)

[13]. Khalili M., Taheri H., Vakilinia S., "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, 1(2011).

[14]. Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 1(22), 38-42.(2010)

[15]. Sharma, N. and Sharma, A. 2012 , "The Black-Hole Node Attack in MANET," Advanced Computing & Communication Technologies (ACCT), Second International Conference ,546,(2012)