International Conference on Emerging Trends in Engineering, Technology, Science and Management
IIMT College of Engineering, Greater Noida, India (ICETETSM-17)
12th April 2017, www.conferenceworld.in ISBN: 978-93-86171-38-2

A SURVEY OF SINGLE BLACK HOLE ATTACK AND COLLABORATIVE BLACK HOLE IN MANET

Shilpi Jain[1], Sudhanshu Ranjan Choudhary[2], Shubham[3]

[1]*Asst. Professor, Dronacharya Group of Institutions,Greater Noida*
[2,3] *B.Tech Student, Dronacharya Group of Institutions,Greater Noida*

ABSTRACT:

In the current study survey of black hole attack detection techniques in MOBILE Ad Hoc Network (MANET) are discussed with performance analysis. The aim of the paper is to find the gaps of the detection techniques of black hole attack in order to help the future researchers to propose a robust and feasible detection technique that will not only enhance the efficiency but also be easy to implement in MANET. The comparisons are done on the basis of different network parameters like throughput, packet drop ratio (PDR) ETC.

Keywords: Black hole attack, detection techniques, comparative analysis, MANET.

I. INTRODUCTION

A Mobile ad-hoc network (MANET) is a newest Research topic among researchers because it provide flexibility and infrastructure less network. MANET has some different characteristic like dynamic network topology, limited power and limited bandwidth for communication. The routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol, DSR both are of reactive routing protocol. AODV protocol is vulnerable by single Black Hole as well as collaborative Black Hole attack. A malicious node which act as a black hole advertise itself as having the shortest path to the destination node. In this paper we analyze in detail," Single Black Hole" and Collaborative Black Hole" types of attack. We also provide a detailed list of solutions which protect the black hole in MANET's

Ad hoc networks have a large number of potential areas. Military uses such as connecting soldiers or other military units to each other on the battlefield or creating sensory arrays with thousands of sensors are two typical examples [1]. Ad hoc networks is used in situations where creating the infrastructure would be impracticable. Wireless mobile ad hoc network is infra Structure less network which is composed of several movable user nodes. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or base Station in wireless networks. Instead, it seeks to set up routes on-demand. If a node wants to initiate communication with the

other node to which it has no route, the routing protocol will try to establish such a route by forwarding Packets. It Uses Three Type of Messages:

RREQ - A route request message is transmitted by a node requiring a route to a node. It is broadcasted. Every RREQ carries a time to live (TTL) value which initialized to that states for how many hops this message should be forwarded.

If TTL= Negative value, at the target node, it discard the packet.

If TTL= 0, at Target node then it accept the Packet

RREP - A route reply message is send back to originator of a RREQ as shown in figure 1 if the receiver is either the node using the requested address, or it has a valid route to the requested address.

RERR - RERR is a error message generated by a node if it will not receive proper packet. Nodes or when a link breakage in an active route is detected.

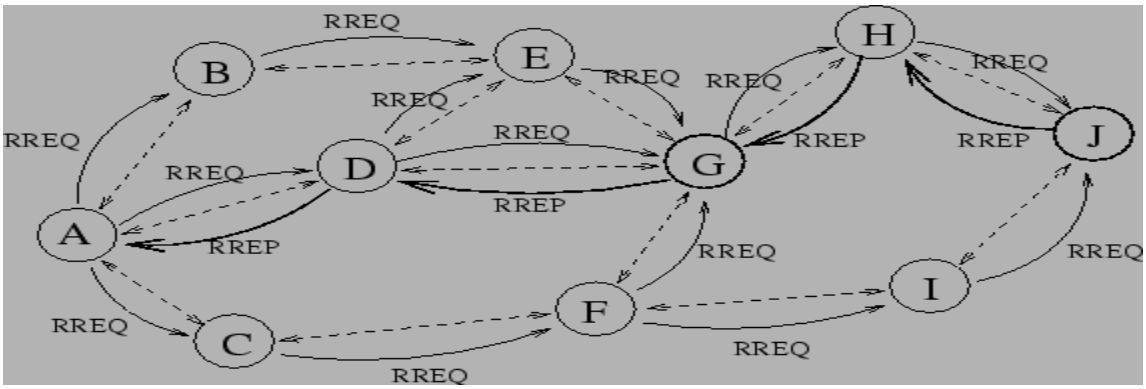

Figure.1: Architecture of AODV protocol

The security threats have been extensively discussed and investigated in the wired and wireless networks [2]. There are many security related issues which have been studied in recent years. For instance, snooping attacks, packet overflow on the network by intruder node, wormhole attacks, single black hole attacks [3], co-operative black hole attack, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks [4]. This paper will focus on single black hole attack and collaborative black hole attack scheme in MANET.

II. LITERATURE REVIEW

In the literature of black hole attack detection a number of attack detection techniques are evolved.

In [7] authors proposed DSA (Digital Signature Algorithm) based detection technique and Blowfish algorithm for encryption.

In [10] handshake mechanism is used where a periodic dynamic Id (value) is generated in a same group. Each node forwards data packet to its neighboring node after verifying dynamic value. Since the malicious node does not belong to the group, the dynamic value will not matched by malicious nodes.

In [11] one algorithm is proposed that after finding the route, the source node sends encrypted message to the cluster head

In [12] the proposed work not only detects the black hole nodes in case when the node is not idle but it can also detect the Black hole nodes in case when a node is idle as well.

In [13] Modify Zone Routing protocol are used. It first finds the neighbor nodes and update the entry in routing table. It calculate the trust value of a node accordingly it decide whether the received message is from the appropriate node or not.

In [16] proposed a DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of black hole by notifying other nodes in the network of the incident. It detects the black hole node on the basis of sequence number. If the RREP_Seq_no. finds more than the threshold value, the node announce as a malicious node.

In [17] proposed a new mechanism Cooperative Bait Detection Scheme (called the CBDS) for detecting mischievous nodes in MANETs under gray/collaborative blackhole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique.

III. BLACK HOLE ATTACK

The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs).It is occurred at routing layer in which data is change from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer [5]. Routing protocol whether we are using Active Routing Protocol or Proactive Routing Protocol is targeted by the attack. Black hole attack having great influencing attack on virtual mesh network [5]. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks.

In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorized node to sender node and then sender become confuse in two replies. On that way, Fault node become sender node and whole data received by it. In this, the data packets fully dropped by sender node.

Black hole attack will cause powerful effect to the performance of mesh networks. In previous research, the authors have carried out on black hole attack [6].

Single Black Hole: A single Black hole attack by sending falsie message to other node and it form a hole which have no idea of creating it. In figure 2. Shows the single black hole, node 8 act as a malicious node, which advertise itself

as having the shortest path to the destination node even if it does not have proper path to the node G (Destination Node).

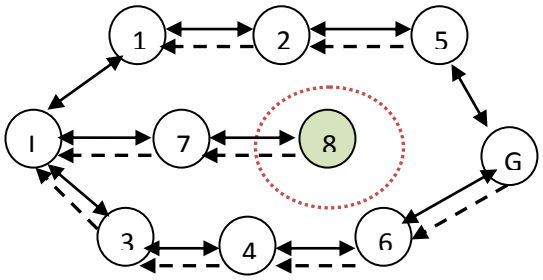

Figure 2. Single black hole attack

Schemes	Routing protocol	Simulator	Detection type	Publication year	Results	Defects
Security [7] Algorithm using blowfish and Digital Signature	AODV	NS-2.34	SINGLE	2016	Reduces the end to end delay. The throughput is improved by 80-85%	It Produce more Overhead
Using Intrusion Detection System[8]	AODV	NS-2	SINGLE	2016	Number of packets dropped is decreased by 75-80% than AODV	-
Restricted IP is used for detection in MANET [9]	AODV	OPNET Modeler	Single	2015	Throughput is improved by 92%	In cooperative, throughput decrease
Handshaking scheme [10]	AODV	NS-2	Single	2015	the number of packets dropped is decreased by	Use Handshake Protocol in static manner

Schemes	Routing protocol	Simulator	Detection type	Publication year	Results	Defects
					75-80% than AODV and throughput increased by 85 %	
Effective value based scheme in AODV [11]	AODV	MATLAB	Single	2014	scheme improves network throughput to about 82%, from 71% network throughput provided by AODV	if data packets are used instead of dummy packets to check the node's effective value more improved performance result.
It use Threshold value [12]	AODV	NS 2.34	Single	2013	Throughput increased by 75%	It Produce more Overhead
Trustworthy factor is attached with the node [13]	ZRP	NS2	Single	2012	Its works effectively and efficently	Few additional delay
Next Hop Information Scheme [14]	AODV	NS-2	Single detection	2010	The PDR is improved by 40-50% and the number of packets dropped is decreased by 75-80% than	Few additional delay

Schemes	Routing protocol	Simulator	Detection type	Publication year	Results	Defects
					AODV	
IDS based on ABM [15]	MAODV	NS-2	Single detection	2010	The packet loss rate can be decreased to 11.28% and 14.76%	Cooperative isolation the malicious node, but failed at collaborative black hole attacks
DPRAODV [16]	AODV	NS-2	Single detection	2009	The PDR is improved by 80-85% than AODV when under black hole attack	A little bit higher routing overhead and end-to-end delay than AODV

Table 1: Survey of different scheme of Single black hole attack in MANET

IV. COOPERATIVE BLACK HOLE

In AODV Routing Protocol, when Initiator node I wants to communicate with Goal node G, the initiator node I broadcast the RREQ packet (figure 2) to its entire neighboring node. The neighboring node updates their routing table if it found any new entry in the packet and check if it is a Goal node. If not, the neighboring node decrease the Time To Live Field(TTL) and floods the network with the RREQ to the Goal node G until it reaches node G or any other intermediate node which has a fresh sufficient path to G, as depicted by example in Figure 1. The goal node or intermediate node generates the Route Reply Message (RREP) in reverse direction as shown in figure: This is a normal working of any reactive routing protocol when network has no malicious node.

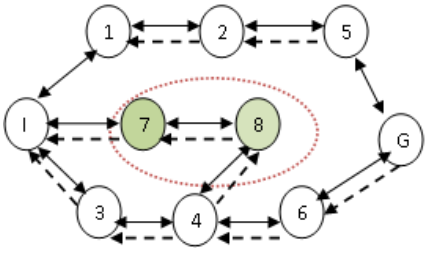

Figure 3 Cooperative Black hole

Schemes	Routing protocol	Simulator	Publication year	Results	Defects
cooperative bait detection scheme [17]	DSR	NS-2	2016	Even in the case where 40% of the total nodes in the network are malicious, the CBDS scheme still successfully detects those malicious nodes while keeping the packet delivery ratio above 90%	A higher control overhead than AODV
CROSS- CHECKING ALGORITHM[18]	AODV	NS-2	2015	Leads to maximum throughput.	The delay is increased.
It use Threshold value [12]	AODV	NS-2	2013	Throughput increased by 70% in case of cooperative	It Produce more Overhead
BDSR [19]	DSR	QualNET	2011	The PDR of BDSR is always higher than 90%	The overhead is minimal higher than DSR, but lower than WD approach
BBN and RIP [20]	AODV	-	2010	No simulation results	-
MAC and Hash-based PRF Scheme [21]	AODV	NS-2	2009	The PDR is higher than 90% when AODV is inaccessible 50%	The malicious node is able to forge a fake reply to dodge the detection scheme

Table2: Comparison of Collaborative Black Hole Attack Schemes

V. ANALYSIS AND DISCUSSION

In this paper we represent various detection schemes of both types of black hole attack. Table 1 and table 2 focus on the performance comparisons of the detection schemes. This information is very important and helpful for the future researchers in order to modify the existing scheme or to propose new detection techniques. The result analysis

of the detection techniques shows the performance on the basis of throughput and PDR which are two very crucial parameters in MANET. The tables also shows the drawbacks of the detection techniques which may be recovered in future by the researchers. Hence it will show the gaps of the techniques. From the tables one important inference can be drawn that in comparison to Single black hole attack, collaborative black hole attack decreases the throughput considerably.

VI CONCLUSION AND FUTURE SCOPE

In the current study we represent a detailed survey of various black hole attack detection techniques with their performance analysis and drawbacks. We observed that most of the detection techniques suffer from high overhead and hence become infeasible to be implemented. In future we can propose a robust black hole detection technique that will be lightweight as well as efficient in terms of throughput and PDR.

REFERENCES

1. Sonia, Padmavati, "Performance analysis of Black Hole Attack on Vanet's Reactive Routing Protocols", International Journal of Computer Applications (0975 – 8887) Volume 73– No.9, July 2013
2. Zou L, Chao H-C: Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 2011,25(3):29–34.doi:10.1109/MNET.2011.5772059 doi: 10.1109/MNET.2011.5772059MATHView ArticleGoogle Scholar
3. Raghvendra Prasad , Kuntal Barua," Implementation, Detection and Prevention of Black hole Attack for Mobile Ad-hoc Network Scenario using NS-2 ",International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
4. Meghna Chhabra1 , Brij Gupta1*, Ammar Almomani," A Novel Solution to Handle DDOS Attack in MANET "Journal of Information Security, 2013, 4, 165-179 Published Online July 2013 .
5. Rupinder Kaur,ParminderSingh :" Review of Black Hole and Gray Hole Attack", International journal of Multimedia and Its Applications(IJMA) Vol.6,No.6,December 2014.
6. D.Boneh,C.Gentry,B.Lynn,H.Shachem,"Aggregate and Verifiably Encrypted Signature from Bilineer Maps ",Advances in Cryptology-EUROCRYPT'03,LNCS 2656,Berlin,Spinger-Veralg,2003,pp.416- 432.
7. Gaurav Rathore " , Blackhole Attack in AODV Routing Protocol Using Security Algorithm in MANET",International Journal of Computer Applications(0975-8887) Volume 113-No.3,January 2016.
8. Nikita Patel,Jay amin, "Detection of Blackhole Attack Using Intrusion Detection System in AODV Based MANET.IJARIIEISSN(O)-2395-4396,VOL-2Issue-3 2016.
9. Hitender Gupta#1, Harsh Aggarwal ," Simulation to Detect and Removal of Black Hole in Manet" SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – EFES April 2015.

10. K.R.Viswa Jhananie1 , Dr.C.Chandrasekar," Detection and Removal of Blackhole Attack Using Handshake Mechanism in MANET and VANET "IOSR Journal of Mobile Computing & Application (IOSR-JMCA) e-ISSN: 2394-0050, P-ISSN: 2394-0042.Volume 2, Issue 1. (Mar. - Apr. 2015), PP 01-05.
11. Priyanka, Mukesh Dalal, "Security in MANET: Effective value Based Malicious Node Detection and Removal Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.
12. Neelam Khemariya, Ajay Khuntetha," An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013.
13. Himani Yadav and Rakesh Kumar," Identification and Removal of Black Hole Attack for Secure Communication in MANETs" , International Journal of Computer Science and Telecommunications Volume 3, Issue 9, September 2012.
14. Jaisankar N, Saravanan R, Swamy KD: A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26–27 March 2010 2010.
15. Su M-Y: Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications 2011,34(1):107–117. doi:10.1016/j.comcom.2010.08.007 doi:10.1016/j.comcom.2010.08.007 10.1016/j.comcom.2010.08.007.
16. Raj PN, Swadas PB: DPRAODV: A Dynamic Learning System AgainstBlackhole Attack in AODV based MANET.International Journal of Computer Science 2009, 2: 54–59. doi: abs/0909.2371 doi: abs/0909.2371.
17. Deepali Tambekar, Prof. H. V. Kumbhar," Prevention of Collaborative Attacks of Malicious Node in MANET Using CBDA Scheme", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 6, June 2016.
18. Garima Gupta1 and Atul Mishra," SIMULATION BASED STUDY OF COOPERATIVE BLACK HOLE ATTACK RESOLUTION USING CROSSCHECKING ALGORITHM", International Journal on AdHoc Networking Systems (IJANS) Vol. 5, No. 2, April 2015.
19. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L: Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13–16 Feb. 2011 2011.
20. Vishnu KA, Paul J: Detection and Removal of Cooperative Black/Gray hole attack in Mobile Ad Hoc Network International Journal of Computer Applications 2010,1(22):38–42. doi: 10.5120/445–679 doi: 10.5120/445-679View Article.
21. Min Z, Jiliu Z: Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. Paper presented at the International Symposium on Information Engineering and Electronic Commerce, Ternopil, Ukraine, 16–17 May 2009 2009