ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

Detection and Prevention of Cooperative Black Hole Attack in Mobile Adhoc Network :A Review

[1] Lakshmi Sabarinath,[2] Mary Anita E A
[1][2] Research Scholar, AMET University, Chennai
[1][2] Professor, S.A.Engineering College, Chennai

***Abstract* - MANETs (Mobile Adhoc Network) are distributed and self directed networks thatoperate without centralized access point and physical fixed infrastructure . Theyare more challenged and prone to attacks when compared to any other conservativenetwork. Black hole attack is one such attack that disrupts communication andreduces the performance of the network. Black hole detection systems aim atremoving this vulnerability. In this paper, we have discussed various techniques fordetection and prevention of cooperative Blackhole attack and provided acomprehensive survey on cooperative BlackHole attack.**

***Index Terms*-- MANET, Black hole, Security, Cooperative attack**

1.INTRODUCTION

A mobile ad hoc network (MANET) is a collection of self-organized nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. The mobile nodes are self-organized by storing the information about its neighbor node. Nodes can communicate only if they are within the radio signal. If the nodes are not within range they can communicate with the help of multi hop routing. Each node in the network behaves as a host or as a router or both in the same time. The size of the network is not limited. Each node in a MANET is limited to a certain power and bandwidth .The main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths. MANETs are more vulnerable to attack and security of communication in MANET is very important. The attacks against MANET are classified into two types: passive attack and active attack. A passive attack is one that does not disrupt the operation of the network. An active attack alters the operation of the network by modifying and interrupting data. Active attack can be further divided into external attacks and internal attacks. An external attack is one in which participating nodes are not part of the network. An internal attack is one in which compromised or malicious nodes are part of the network. MANETS have different types of security attacks such as black hole, grey hole, warm hole which disrupt the network.

A black hole attack is one in which a malicious node uses the routing protocol to advertise itself as having the shortest path to the destination node whose packets it wants to discard/replay packets. When an attacker receives RREQ packet, then it creates a reply where an extremely short route is advertised. If the malicious reply reaches the source node before the reply from a legitimate node, a forged route gets created. Once the attacker has been able to insert itself between source and destination node, it is able to do discard/replay packets passing between them. Black hole attack can be either internal or external.

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

External Black hole attack

External attacks physically stay outside of the network and deny access to control of internal malicious node and control it to attack other nodes in MANET.

Cooperative Blackhole attack

In co operative black hole attack the malicious nodes have an effect in a group. Many detection schemes are failed in discussing the cooperative black hole attack problems. Now recently, several cooperative detection schemes are proposed to detect and prevent the multiple black hole attack.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

Related Work

Various researchers have proposed different methods for detection and prevention of black hole attack in MANETS.

Data Routing Information Table

Sanjay Ramaswamy et. al [1] proposed a method to detect multiple black hole nodes cooperating as a group with slightly modified AODV protocol by using data routing information (DRI) and cross checking . It identifies multiple black hole attacks and discovers a secure path from source node to destination node by avoiding multiple black hole node attacking in cooperation.

Fidelity Table

Latha Tamilselvan et al [2] have proposed a solution for cooperative black hole attack by modifying the fidelity table. The sequence number and received time of the packet is stored in the fidelity table and is compared with the threshold value to find secure path from source to destination by ignoring multiple malicious. The black hole node is avoided by ALARM packets thereby improving the packet delivery ratio.

Distributed and Cooperative Mechanism

Chang Wu Yu et al [3] have proposed a solution against the black hole attack problem for ad hoc networks that works in a distributed manner. All mobile nodes cooperate together to analyze and detect possible multiple black hole nodes in a more reliable way .Simulation results show that this solution has higher black hole detection rate and achieves better packet delivery rate with much less overhead, especially when the network is busier. A constrained broadcasting algorithm has been proposed to effectively reduce the overhead.

Certificate Chaining

Certificate chaining method proposed by E.A.Mary Anita et al [4] provides a security mechanism for multicasting routing protocols by modifying the route discovery process. An enhanced certificate based authentication mechanism, where nodes authenticate each other by issuing certificates to neighboring nodes and generating public key without the need of any online centralized authority has been proposed

Anomaly Detection Method

Alem Y.F et.al [5] have proposed an Intrusion Detection system using Anomaly Detection (IDAD) technique to prevent multiple black nodes by. To discover secure path, IDAD collects the abnormal activities of the node. Audit data is then collected and the information about the node is sent to IDAD system to compare the activity of the nodes with previous information. If any node activity is suspicious, then IDAD system ignores the specific node from the network .To avoid false positive alarm this method checks multiple anomaly conditions.

Data Routing Information Table and Cross Checking using FREQ and FREP

Hesiri Weerasingh et al [6] have proposed a solution for avoiding cooperative black hole attack by Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) .This solution identifies multiple collaborative black hole nodes and finds the secure path from source node to destination node .Every node has to maintain an extra database to store the routing information .

Anti Black Hole Mechanism

Ming-Yang Su et al [7] have proposed a mechanism to detect and separate malicious nodes which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism). When the suspicious value of a node exceeds a threshold, a block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the malicious node. IDS nodes are specially located within each other transmission range, which is not always feasible in normal case.

Peak Value Method

Rutvij et al [8] proposed a method to avoid cooperative black hole attack by a factor called “peak value’. The PEAK is calculated by number of request and number of reply used every time . Malicious node is notified by other nodes in use of RREQ . Suspicious nodes are discovered by PEAK value resulting in better packet delivery ratio.

Boardcasting Method

Antony Devassy et. al. [9] have proposed a method for safe route from source to destination by IDCMN-ID broad casting method. In this method, the malicious nodes

are identified first using another black hole detection scheme, then the id of those malicious nodes is sent or broadcasted to the entire network. Therefore even if the malicious nodes take part in two or more routing paths, packets do not move towards malicious nodes because the entire network knows about the malicious

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

nodes. The main drawback of this solution is maintaining an extra database to store the table and limited bandwidth.

Modified Extended Data Routing Information Table

Vani et.al [11] proposed a modified AODV protocol for eliminate cooperative black hole and grey hole attacks in MANET by using modified extended data routing information (MEDRI) table. This solution shows increase in throughput and packet delivery ratio.

Neighbour Node Monitoring

Durgesh et al [12] proposed an approach using real time monitoring with promisuous mode to detect and avoid cooperative Black hole attack .The forward count and receive count are stored in every neigbour node table and is used to detect suspicious node .

Cross Checking Method

Gayathri Wahane et.al [13] proposed a solution based on cross checking with true link (timing based counter measure) and secure knowledge algorithm to detect Cooperative Black hole attack. This method exchanges information about the nodes in network layer and MAC and stores in DRI table thereby reducing false malicious detection. This method reduces routing overhead delay and maximizes through put.

Cooperative Bait Detection Scheme

Jian Ming Chang et al[14] proposed a scheme to detect multiple black hole attack by cooperative Bait detection scheme (CBDS) This method uses a reverse tracing technique to help in solving the issue .CBDS detects with the use of DSR , 2ack and best effort full tolerant routing (BFTR) protocols to show better performance in metrics.

Detection Of Multiple Black Hole Attack Algorithm

Arathy et al[15] proposed a algorithm detects single and multiple black hole nodes using an additional route with nonexistent target address, computes a threshold ADSN, creates a black hole list and invokes the proposed D-CBH algorithm. Using ADSN, black hole list and next hop information extracted from RREP, the D-CBH algorithm creates a list of collaborative black hole nodes.

Honeypot- Based Dynamic Anomaly Detection Using Cross-Layer Security

Usha et al[16] have proposed technique detects and isolates black hole attacks from the adhoc network. This technique implements cross layer isolation, which is responsible for separating the black hole nodes using the MAC and network layer features from the MANET.

Table 1.Comparison Of Various Schemes On Cooperative Black Hole Attack

Table 1.Comparison Of Various Schemes

S.No	Author	Method	Protocol	Results	Merits & Demerits
1.	S. Ramaswamy, H. Fu, M. Sreekantaradhya a at al .[1]	DRI TABLE and cross check	Modified AODV Protocol	Secure path from source to destination preventing multiple blackhole attack	Merits Minimum packet loss and better through put, PDR Demerits Delay in identifying blackhole can cause can cause packet losses Overhead of keeping DRI Table by all nodes
2.	Tamilselvan L, Sankaranarayanan V.[2]	Fidelity Table	Enhancement on AODV	Secure route is selected on the based of threshold value Malicious node is avoided by ALARM Packets	Merit Better packet delivery ratio
3.	Wu C, Wu TK, Cheng RH et.al.[3]	Distributed cooperative mechanism	AODV	This solution has higher black hole detection rate and achieves better packet delivery rate	Merits A constrained broadcasting algorithm to effectively reduce the overhead .
4.	Anita, E. M., & Vasudevan, V. (2010).	Certificate Chaining	Multicasting Protocol ODMRP	Large improvement in PDR and Throughput Difficult as it involves private Key generation and authentication	Merits Highly effective No packets loss Demerits Overhead in implementing private keys issuing and checking certificate makes it costly and difficult and causes delay of about 15 %
5.	Alem, Y. F., & Xuan, Z. C.[5] (2010, May)	Anomaly detection method	AODV	Each node data is collected previously and compared the activity Decrease the number of Packet to faster communication	Merits Reduce the number of routing packet in turn minimizes network overhead and facilitate faster communication Techniques check multiple anomaly conditions Demerits Neighbour nodes may give false information Cannot detect new type of attack
6.	Hesiri Weerasinghe . [6](2011)	DRI Table & Cross checking using FREQ and FREP	AODV	A higher through perform almost 50% than AODV	Demerits 5 to 8% more communication overhead of route request.
7.	Ming-Yang Su	Anti blackhole Mechanism	AODV	All IDS nodes performe ADM. Detected IDS to all nodes on the network	Demerits Special mechanism is needed to safe the IDS
8.	Rutvij H. Jhaveri ,et. al. (2012)	Peak value method	AODV	In this procedure peak value are allocated in memory	Merits Better result in Packet delivery ratio, end to end delay
9.	Devassy, A., & Jayanthi, K	MN-ID Broadcasting	Unicasting Protocols AODV DSR	Highly effective. No packet loss once MN-ID is detected	Merits Larger improvement is PDR, EED, Through put Easy to implement Demerits Need to be paired with an efficient BH detection scheme.

ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 6, June 2017

10.	Seryvuth Tan and Keecheon Kim	Secure route discovery	SR AODV	Novel approach is used to secure the routes to destination	Merits Increase in packet delivery ratio
11.	Vani A. Hiremani et.al.(2013)	ERDA Table	MODIFIED AODV	This technique is also capable for detection of nodes which are affected by non consecutive cooperative blackhole attack	Merits Increase in throughput and packet delivery ratio.
12.	Kshirsagar, Durgesh et. al.(2013)	Real Time of Monitoring	AODV	This method used promiscuous mode for monitoring purpose	Merits Mode is helped in identifying malicious node without false positive rate.
13.	Wahane, Gayatri et. al.	Cross checking with true link (timing based counter measurement (concept)	AODV	Presents good performance in terms of energy consumer and minimum packet loss. In enhances AODV Protocol to improve the network performance according to routing update conditions	Merits This solution routing overhead, delay and maximum throughput when number of nodes and pause time more.
14.	Jian-Ming Chang et. al.	Cooperative Bait Detection Scheme (CBSD)	DSR Protocol	The PDR of BDSR is always higher than 90%	Demerits The overhead is minimal higher than DSR. But lower than WD approach.
15.	Arathy et.al.(2016)	D-MBH algorithm	AODV Protocol	The proposed algorithm detect single and collaborative black holes with reduced computational and routing overhead	DEMERITS There is no considerable improvement in storage overhead.
16.	G.Usha et. al.(2016)	Honey pot based dynamic anomaly detection using cross layer security	AODV Protocol	In this technique end to end delay is very low.	MERITS The NRL is very low.The PDR is very minimum.

This technique is also capable for detection of nodes which are affected by non consecutive co-operative blackhole and grayhole attacks in MANET

I. CONCLUSION

.In the current era of wireless network, popularity of MANET is increasing at a veryfast pace with its wide range of multimedia applications running in aninfrastructure less environment .In this paper we have surveyed about variousexisting defense approaches to detection and prevention of cooperative black holeattack. Prevention from this attack is still an open challange problem. Further theresearchers can provide dynamic and realistic solutions to defend against thisattack

REFERENCES

1)S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard.Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003.

2)Tamilselvan L, Sankaranarayanan V. Prevention of black hole attack in MANET. Proceedings of IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications; 2007. p. 27–30

3)Wu C, Wu TK, Cheng RH, Chang SC. A distributed and cooperative black hole node detection and elimination mechanism for ad hoc network. Lecture Notes in Computer Science. 2007; 4819:538–49.

4)Anita, E. M., & Vasudevan, V. (2010), Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining, International Journal of Computer Applications, 1(12), 21-2.

5)Alem, Y. F., & Xuan, Z. C. (2010, May), Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection, Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 3, pp. V3-672). IEEE.

6)Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Elsevier, Computer Communications 34 (2011) 107–117.

7)Hesiri Weerasinghe , 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun. 24-28.

8)Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. 2012 Second International Conference on Advanced Computing & Communication Technologies. 2 (2), p535-540

9)Devassy, A., & Jayanthi, K., Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting(2012).

10)Seryvuth Tan and Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on

AODV-based MANETs"978-0-7695-5088-6/13 © 2013 IEEE.

11)Vani A. Hiremani, Manisha Madhukar Jadhao, "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET" IEEE 2013

12)Kshirsagar, Durgesh, and Abhijit Patil. "Blackhole attack detection and prevention by real time monitoring." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.

13)Wahane, Gayatri, Ashok M. Kanthe, and Dina Simunic. "Detection of cooperative black hole attack using crosschecking with truelink in MANET." Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on. IEEE, 2014.

14)Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks byMalicious Nodes in MANETs: A Cooperative BaitDetection Approach", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015

15)Arathy K Sa*, Sminesh C Na."A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET"", Elsevier, Computer Communications 34 (2016) 264–271.

16) G. Usha a , ∗, M. Rajesh Babu b , S. Saravana Kumar "Dynamic anomaly detection using cross layer security in MANET ",Elsevier, Computer Communications 34 (2016) 1-11.