International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Different Existing Technique for Detection of Black Hole Attack in MANETs

Heta Changela[1], Amit Lathigara[2]

[1]PG Scholar, Computer Engineering, School of engineering, RK University, Gujarat, India

[2]Head of Department-Computer Engineering, School of engineering, RK University, Gujarat, India

Abstract: ***Mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network. In which mobile devices are connected directly without wires. Communication will occur between nodes directly or through intermediate nodes. The node is acting as a host and router both; it will communicate with each other through multi-hops due to limited transmission ranges. MANETs vulnerable to various attacks including Black Hole attack .The black hole attack is present at network layer. Black hole is an attack in which malicious node incorrectly due itself as a valid node. It will receive the information and it will not forward the information to next nodes .This paper presents a review of various techniques used to detect and prevent the black hole attack in AODV routing protocol.***

Keywords: MANET, black hole attack, detection and prevention techniques, AODV

1. Introduction

The mobile ad hoc networks diverge from already present networks by the fact that they depend on no fixed infrastructure. MANETs contain of nodes that are moving casually with some speed. In the network, nodes can be either fixed or mobile. In MANETs, communication occurs between nodes directly or through intermediate nodes which act as routers. There are also many open issues about MANETs, like security problem, fixed transmission bandwidth, reliable data delivery, dynamic link establishment and etc.[3]

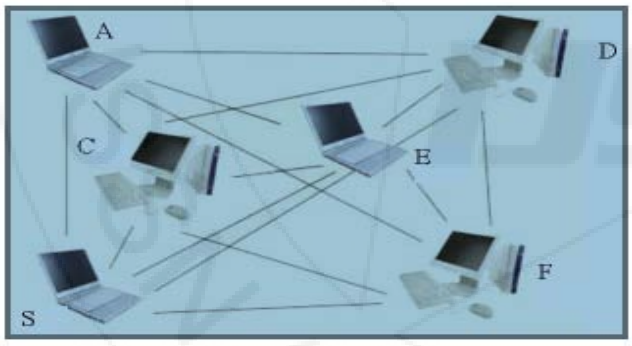

Figure 1: Mobile ad-hoc Network

Common attacks faced by networks include Black hole, gray hole and wormhole attacks, and IP spoofing. We focus on different types of black hole attacks in MANET which can be separated into single black hole attack and collaborative black hole attack. Black hole attack is behave like a malicious node in the network [13] and it compulsorily acquire that it has a shortest path to reach the destination. By accidentally nodes start sending data to the destination through the black hole and black hole will divert all traffic in the network to itself, and after that it will drop all packets. Hundreds of nodes might be required in a network and security measures undertaken must be efficient and cost effective for a vast network.Here we discuss all two type of black hole attack.

2. Black Hole Attack in MANET

Mobile ad hoc networks use distributed routing protocols, if malicious node presence in the network then it will interrupt the network. MANETS are vulnerable to various types of attacks. Based on different characteristics the attack on mobile ad hoc network is classified as passive and active attacks. One of the active attacks is Black hole attack. A black hole is a node that has some characteristics like that it always responds with a Route Reply (RREP) message to every RREQ, even though it does not have any route to the destination node.

In networking, black holes refer to places in the network where entering or leaving traffic is silently discarded, without updating the source that the data did not reach its planned receiver. [12] In black hole attack a malicious node can be detects the active route and notes the destination address or can be sends a route reply packet (RREP). In Black hole attack Hop count value is set to lowermost values and the sequence number is set to the uppermost value. Malicious node send RREP to the next node which is belongs to the active route. This can also be send directly data to source node if route is available. The RREP received by the next node to the malicious node will spread through the established inverse route to the data of source node. The fresh information received in the Route Reply and it will allow the source node to keep informed to its routing table. New route selected by source node for picking data. The malicious node will drop now all the data to which it belong in the route. [8]

There are two types of black hole attack in network. 1) Single Black hole attack 2) Collaborative Black hole attack. [9]

In single black hole attack, all network traffic is redirected to single black hole node which is malicious node and drops all the packets. A single black hole attack is easily happened in the mobile ad hoc networks. In collaborative black hole attack, there are many malicious nodes work together to redirect normal routing information to them and produce that route according to them.

Licensed Under Creative Commons Attribution CC BY

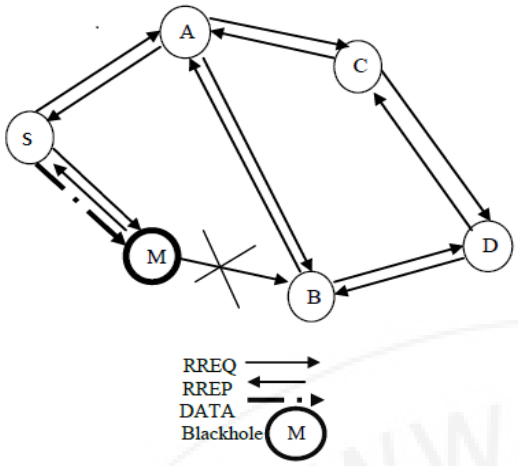

Figure 2: Blackhole attack In MANET

3. Ad-Hoc On Demand Distance Vector(AODV)

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol for wireless ad hoc networks. It is discovers a route to a destination only when it is required. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination to all mobile nodes work in support using the routing control messages. AODV has no security mechanisms, malicious nodes can perform many attacks by not execute as per the AODV rules. A malicious node (**M)** can carry out many attacks against AODV.[15] AODV route discovery, there are three important control messages specifically Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). Control messages can carry an important attribute called destination sequence number. The format of RREQ and RREP packet are given below table. [3]

RREQ field

Source_ add	Source_ Seq	Broadcast_ Id	Dst_ add	Dst_ Seq	Hop_ count

RREP field

Source_ Add	Dst_ add	Dst_ Seq	Hop_ count	Lifetime

A. Route Discovery Process

The Route Request (RREQ) reaches the destination or some transitional node, which has new route to destination and it will generate the reverse path automatically. The RREP message follows the reverse path.[14] The intermediate node can use its recorded to every route entry. Intermediate node will respond only if Route Request's Seq_num to destination is greater than the recorded value in intermediate node .RREP is also keep tracking all routing information and if a node receive more than one route reply it will update routing information to the table. It will accept Route Reply only it has more Seq_num to the previous Route Reply or same Seq_num with less hop count.[5] Source node starts sending data as it receive the Route Reply and after update routing information in table. If path breaks it will send Route Error message and route discovery is reinitiated at the source if required. [8]

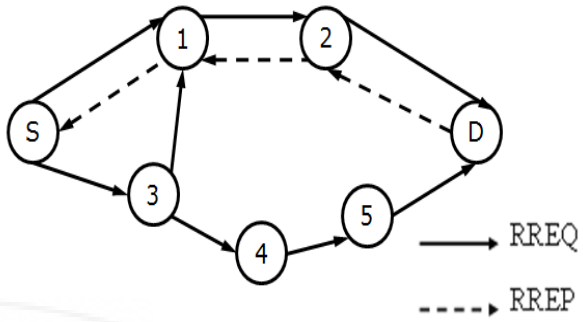

Figure 3: Route Discovery Process

Here in fig. source node and destination node are there S is a source node and D is a destination node. Source node wants to send data to destination node and it broadcast the RREQ to its neighbour node if neighbour node has path to destination then it will goes there else its further broadcast RREQ to its neighbour node. Destination node will send back RREP to source node via neighbour node and source node receive RREP and path will complete.

B. Route Maintenance

After the route discovery phase the source node gets the route to the destination and at the same time it is the responsibility of the source node to keep the maintenance.[14] Maintenance of the discovered/established route is necessary for two main advantages, first to achieve stability in the network and secondly to reduce the excessive overhead required in discovering new route.

4. Existing Technique for Black Hole Attack

A. Credit Based On AODV(CAODV)

Watchara and Sakuna [1] used that source node will broadcast RREQ to other nodes till a destination node or node which have a route to destination replies RREP back to source. The receiving node will assign a credit to the next hop node or who sent RREP. When a node in the path sends one packet, one credit is deducted from the next hop node. As soon as a destination node receives data packet, it will send Credit Acknowledge (CACK) and it will back to a source node. A node within a way back will increase credit of the next hop by 2 to indicate a higher trust level of the next hop. On the other hand, credit will be decreased if a node cannot receive CACK. The node will be untrusted and mark as a blacklist, when a credit reaches zero.

B. REAct: Resource-Efficient Accountability Scheme based on Random Audits

This scheme provides publicly confirmable evidence of node misbehaviour. REAct [2] constitutes of three phases: (i) Audit phase, (ii) Search phase and (iii) Identification phase. The goal of the audit phase is to verify that the audited node forwards packets to the destination. When a node is audited, it has to provide proof of the packets it forwards. The audit phase constitutes three steps: (a) sending of an audit request. (b) Building up behavioural proof and (c) then processing of this build up behavioural proof. The Search node identify misbehaving link in which packets are dropped. Communicating overhead reduces significantly with misbehaviour and compared with reputation-based and

Licensed Under Creative Commons Attribution CC BY

acknowledgment based schemes. It is ineffective in the collaborative black hole setting because other malicious node is able to handle a fake proof and send to the audit node. Second, the behavioural proof only records the information of transmission packets rather than the nodes.

C. Watchdog Mechanism

Watchdog Mechanism [3] is used, it keep track record of two table pending packet table and node rating table. In packet pending table contains unique packet id, address of next hop to which packet will forward, address of destination node and expiry date. In node rating table each node maintain rating of node, node address, packet which are dropped, packet which are forwarded, and last field is calculated if ratio of dropped packets and successfully forwarded packet is greater than a given threshold value then this node misbehave value is 1 which indicate the malicious node else misbehave value is 0.

D. Detection, Prevention and Reactive AODV (DPRAODV) Scheme

Detection, Prevention and Reactive AODV (DPRAODV) Scheme [6] said that a node who receives the RREP first it will compare and check the value of sequence number to its routing table this will perform in normal AODV. Node will accept RREP packet only if it has RREP_Seq_no greater than the one who present in routing table. One of the solutions is that to check to find whether the RREP_seq_no is higher than the given threshold value. If we talk about threshold value then it will update dynamically as in every time of interval. If node have the value of RREp_seq_no is greater than the given threshold value then the node is supposed to be malicious node and it will enter to the black list node. As node detected after it send new control packet called ALARM and it will send to its neighbour node. New node receives a RREP packet and threshold value will update in given time interval. ALARM packet which is control packet and it has information about black list node and every parameter has also so that every neighbouring node has information about black list node then RREP packet from that node is to be discarded. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV.

E. Time Based Threshold Detection Scheme

Time Based Threshold Detection Scheme [7] is used that we have to take care about checking whether there is large difference between the sequence number of source nodes or intermediate node who has sent back RREP or not. Route reply n Request reply table which is from the malicious node who has highest sequence number. If there is existing much more differences between source and destination sequence number, then the destination node is malicious node, then we could immediately eliminate that entry from the RR-Table**.** If the destination sequence number is larger than others, then this DNS from the malicious node. Node will send a RREQ to neighbour node and malicious node will also receive RREQ. Malicious node will sent fake RREP. In AODV, as the destination sequence number is high, the route node will be considered to be fresher and hence source node would start sending data packets to node route node. In our proposed algorithm, AODV before sending data packets firstly source node will check the difference between sequence numbers. If it is too larger, the node will be malicious one, and it will be isolated from the network.

F. Fuzzy Logic

IDS is used based on two factors packet loss rate and data rate. Fuzzy logic [4] is use these two factors to solve the problem. Definite conclusion based on ambiguous noisy or missing information. First we define the N number of nodes and set source and destination node and repeat step un till current node equal to destination node with using neighbor nodes and keep record of each neighbour node. Algorithm is on priority high priority node will take part in communication. Priority define by following step 1) packet loss is low and data rate is high set high priority 2) packet loss is medium and data rate is high set medium priority 3) Packet loss and data rate both low set low priority.

G. Redundant Route And Unique Sequence Number Scheme

First approach [10] is Sender node will utilize the authenticity of the RREP packet, any packet can arrive to many path. During this sender node will find safe path to destination. If sender find safe path to reach the destination after that buffered packet will be transmitted. More than one node have same shared node and based on that sender will find safe route and if no shared nodes then that will be wait for next RREQ. Second approach is unique sequence number is given to every packet. Two methods we have to keep track that one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node. These tables are updated when any packet arrived or transmitted. RREQ will broadcast to neighbour node and up to destination, then destination node will sent RREP and contain last packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and it will receives this RREQ, It will reply to the sender node with a RREP contains the last packet- sequence-numbers received from the source by this intermediate node.

H. Nital Mistry Et Al.'S Method

Nital Mistry et al. [11] add a new table Cmg_RREP_Tab, a new timer MOS_WAIT_TIME and a variable Mali_node to the original AODV routing protocol. The RREP_WAIT_TIME is a time period during the source node sends first RREP packet until receive the RREP control messages. MOS_WAIT_TIME is half the value of RREP_WAIT_TIME. The RREP packets are stored in Cmg_RREP_Tab. In additional function Pre_Receive Reply is executed. The source node analyze all the RREP packets stored in the Cmg_RREP_Tab table. RREP packet has a higher destination sequence number than the source sequence number, and the sender is suspected to be a malicious node. RREP packet with the highest destination sequence number is chosen in Cmg_RREP_Tab table. The simulation will be PDR of AODV drops by 81.812 % in presence of Black hole attack. The same increases by 81.811 % when our solution is used in presence of Black hole attack. At the same time, that the rise in End-to-End delay is 13.28%.

Licensed Under Creative Commons Attribution CC BY

5. Comparison of Single Black Hole Attack Detection Schemes

Schemes	*Routing Protocol*	*Simul-ator*	*Publication Year*	*Result*
Credit Based On AODV[1]	Credit based (CAODV)	NS-2	2012	In contrast with CAODV, we found the average throughput of the original AODV is decreased at about 40 percentages
REAct: Resource - Efficient Accountability Scheme based on Random Audits[2]	DSR	NS-2	2009	Communica-tion overhead grows up to three times larger compare to the single misbehaving node case
Watchdog Mechanism[3]	AODV	-	2012	Improve the data security in mobile ad-hoc network.
Detection,prevention and Reactive AODV(DPRAODV} scheme [6]	AODV	NS-2	2009	PDR of DPRAODV is improved by 80-85% than AODV under attack with Average-End-to-end delay same
Time-based Threshold Detection Scheme [7]	AODV	-	2012	Very less packet lost percentile in the proposed AODV as compared to the AODV.
Fuzzy Logic[4]	-	Global Sensor	2013	It implemented on packet loss and data rate at time of node communi-cation
Redundant Route and Unique Sequence Number Scheme[11]	AODV	NS-2	2004	Solution 1 has a longer delay and lower number of verified routes than Solution 2, but Solution 1 appears to be more secure than Solution 2
Nital Mistry et al.'s Method[13]	AODV	NS-2	2010	PDR of AODV drops by 81.812 % in presence of Black hole attack and rise in End-to-End delay is 13.28 %.

Table 1: Comparison of Single Black Hole Attack Detection Scheme

6. Conclusion

Black hole attack has very grave impact on protocol in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs. The detection of Black Holes in ad hoc networks is still considered to be a most challenging task. The different papers have given several applications for detection and prevention of black hole attacks in MANET. Each and every proposal has its own merits and demerits in their respected results. We can be concluded that Black Hole attacks affect network negatively with using existing technique we can reduce the effect of black hole attack. In Future we can make effective algorithm to reduce the effect of attack in MANET.

References

[1] Watchara Saetang and Sakuna Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks", 2012 *International Conference on Computer Networks and Communication Systems* (CNCS 2012).
[2] Kozma W,Lazos L,"REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits".Second *ACM Conference on Wireless Network Security*, Zurich, Switzerland, 16-18 March 2009.
[3] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black- Hole and Wormhole Attack in Routing Protocol AODV in MANET " , *International Journal of Computer Science, Engineering and Applications* (IJCSEA) Vol.2, No.1, February 2012.
[4] Sonal,Kiran Narang "Black Hole Attack Detection using Fuzzy Logic" 2013 *International Journal Of Science and Research*(IJSR),ISSN:2319-7064.
[5] Humaira Ehsan, Farrukh Aslam Khan "Malicious AODV Implementation and Analysis of Routing Attacks in MANETs" 2012 *IEEE* 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[6] Payal N. Raj, Prashant B. Swadas. "DPRAODV : A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet." *International Journal of Computer Science* Issues, Vol.2, 2009, pp 54-59.
[7] Tamilselven L and Sankaranarayanan, "Prevention of Black hole Attack in MANET" *International Conference on wireless Broadband and Ultra Wideband Communications*, 27-30 August 2007.
[8] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" *Computer Technology & Applications*,Vol 3 (4), 1395-1399 IJCTA July-August 2012.
[9] Ravinder Kaur, Jyoti Kalra "A Review Paper on Detection and Prevention of Black hole in MANET" *International Journal of Advanced Research in Computer Science & Software Engineering* Volume 4, Issue 6, June 2014.
[10] Al-Shurman M, Yoo S-M, Park S (2004) "Black Hole Attack in Mobile Ad Hoc Networks". Paper presented at the 42nd Annual *ACM Southeast Regional Conference* (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.
[11] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) "Improving AODV Protocol Against Blackhole Attacks" Paper presented at the *International MultiConference of Engineers & Computer Scientists*, Hong Kong, 17-19 March, 2010.
[12] Chander Diwaker, Sunita Choudhary " Detection Of Blackhole Attack In Dsr Based Manet" *International*

Licensed Under Creative Commons Attribution CC BY

Journal of Software & Web Sciences 4(2), March-May, 2013, pp. 130-133.

[13] Ms Monika Y. Dangore, Mr Santosh S. Sambare "Detecting And Overcoming Blackhole Attack In Aodv Protocol" 2013 *International Conference on Cloud & Ubiquitous Computing & Emerging Technologies.*

[14] Rashmi Ahlawat, Setu K Chaturvedi "A Survey on Black Hole Attacks and Comparative Analysis of Various IDS Schemes in MANET" *International Journal of Computer Applications* (0975 – 8887) Volume 80 – No1, October 2013.

[15] Mohamed A. Abdelshafy, Peter J. B. King "Analysis of Security Attacks on AODV Routing" 2013 *IEEE.*

Licensed Under Creative Commons Attribution CC BY