ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 8, August 2015

Detection and Prevention of Black Hole Attack with Modified DRI Table in Mobile Network

Neelam Peters[1], Aakanksha S. Choubey[2]

Shri Shankaracharya Technical Campus, Bhilai, India[1]

Assistant Professor, Computer Science, Shri Shankaracharya Technical Campus, Bhilai, India [2]

Abstract: Mobile ad-hoc network is an autonomous network that consists of nodes that communicate with one another with wireless channel. Mobile accidental networks (MANETs) are unit extensively utilized in military and civilian applications. MANET is employed in varied applications, like battlefield, business applications, and remote areas. One of the common attacks in MANETs is a part attack during which a malicious node incorrectly replies for any route requests while not having active route to fastened destination and drops all the receiving packets. If these malicious nodes work together as a bunch then the potential damage can be terribly serious. This kind of attack is named cooperative part attack Mobile. In this paper, we have concentrated on analysing the performance of one of the popular routing protocols for MANET AODV with Black hole AODV. Our theme relies on AODV protocol that is improved by deploying advanced DRI table with further parity. The simulation on NS2 shows effectiveness of our projected theme. Finally we eliminate the part attack and increase network performance by reducing the packet dropping quantitative relation in network. The detection of malicious node in accidental network continues to be thought of as a difficult task. Simulation shows that AODV with our mechanism gave relatively higher performance as compared to AODV.

Keywords: Mobile Ad hoc network, Black Hole Attack, IDSAODV, Network Simulator2.

I. INTRODUCTION

MANETs are composed of autonomous nodes that are self- managed with none infrastructure. They need several potential applications, particularly in military associate degree rescue operations like connecting troopers within the battle or establishing a brief network in situ of one that folded when a disaster like an earthquake. Each node act as router therefore security is the main challenge in a MANET. MANET routing protocols are primarily 3 sorts, they're Proactive or Table driven Reactive or On Demand, and hybrid routing protocol that is combination of proactive and reactive. AODV is on demand routing protocol that realizes the route on the premise of on demand. If an exceedingly node wish to send a packet it broadcast a route request message (RERQ). With the assistance of RERQ message AODV routing protocol produce the route. In this routing protocol once nodes are moving a similar method apply to search out new route. Security is the main challenge of Manet, because Manet is dynamic in nature. There are basically 2 forms of attacks in Manet. They're passive attack and active attack. A Passive attack doesn't disrupt the operation of the network. It simply snoop the info with none alert from the network and confidentiality of the info has been lost. It's terribly arduous to notice the passive attack within the network. The active attacks destroy the info and disrupt the operation of the network. Black hole attack is the example of active attack. Assailant uses the routing protocol to advertise itself as having the shortest path to the node whose packets desires to intercept. Associate degree assailant listen the requests for routes in an exceedingly flooding primarily based protocol. Once the assailant receives asking for route to the destination node, it creates a reply consisting of an especially short route. If the malicious reply reaches the initiating node before the reply from the particular node, a faux route gets created. Once the malicious device has been ready to insert itself between the communicating nodes, it's ready to do something with the packets passing between them. It will drop the packets between them to perform a denial-of-service attack. Part drawback in MANETS could be a serious security drawback to be resolved. During this drawback, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it desires to intercept. In flooding primarily based protocol, if the malicious reply reaches the requesting node before the reply from the particular node, a cast route has been created. This malicious node then will opt for whether or not to drop the packets to perform a denial-of-service attack or to use its place on the route because the beginning in an exceedingly man-in-the-middle attack.

In this paper we project a mechanism to spot multiple part nodes cooperating as a bunch in impromptu network. The projected mechanism work with slightly changed AODV protocol and build use of data routing information table(DIR) with parity bit additionally to cached and current routing table. We ascertain misbehaviour nodes in mobile impromptu atmosphere, and additionally realize secure route to the destination and enhance the performance of network by eliminating cooperative part attack.

The reminder of paper is organized as follows, section II describes related works, in section III AODV and behaviour of cooperative black hole attack is discussed, in section IV proposed mechanism is discussed for making

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 8, August 2015

MANET free from cooperative black hole attack and also theoretical analysis of the proposed scheme is covered in section IV, simulation and results is carried out in section V, and finally conclusion and future direction are given in section VI.

II. RELATED WORK

[14] Deng, Li and Agrawal have suggested a mechanism of defence against a black hole attack on AODV routing protocol. In their proposed scheme, when the Route Reply packet is received from one of the intermediate nodes, another Route Request is sent from the source node to the neighbour node of the intermediate node in the path. This is to check whether such a path really exists from the intermediate node to the destination node. While this scheme completely eliminates the black hole attack by a single attacker, it fails miserably in identifying a cooperative black hole attack involving multiple malicious nodes. [2] Watchdog and Path rate introduces the use of Data Routing Information DRI to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes. The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication. Mechanisms for securing the routing layer of a MANET by cryptographic techniques are proposed by Hu et al, Papadimitratos and Hass. [3] J. Sen. et al. have presented a scheme for detection of malicious packet dropping nodes in a MANET The mechanism is based on local misbehaviour detection and flooding of the detection information in a controlled manner in the network so that the malicious node is detected even if moves out a local neighbourhood. [4] In this work the authors discuss a protocol viz. DPRAODV to counter the Black hole attacks. DPRAODV checks to find whether the RREP_Seq_No is higher than the threshold value. In this protocol, the threshold value is dynamically updated at every time interval.

If the value of RREP_Seq_No found to be higher than the threshold value, the node is suspected to be malicious and is added to a list of blacklisted nodes. It also sends an ALARM packet to its neighbours with information about the blacklisted node. Thus, the neighbour nodes know that RREP packets from the malicious node are to be discarded. That is, if any node receives the RREP packet, looks over the list to check the source of the received message. If the reply is from the suspected node, the same is ignored. Thus, the protocol though successful, suffers from the overhead of updating threshold value at every time Interval and generation of the ALARM packets. The routing overhead, as a result is higher. [5] Nitalmistry has proposed an algorithm to counter black hole attack Against the AODV routing protocol, using cmg_Rrep table and Mos_wait time but this method cannot tackle the problem of cooperative black hole attack.

III.METHODOLOGY

Cooperative Black Hole Attack

A part attack is quite denial of service attack where a malicious node will attract all packets by incorrectly claiming a recent route to the destination so it absorbs them while not forwarding them to the destination. A part attack must have two phases. In the first phase the malicious node exploit the unplanned routing protocol as AODV to advertise itself as having a legitimate route to a destination node and in the second phase the assaulter node drops the intercepted packets without forwarding them.

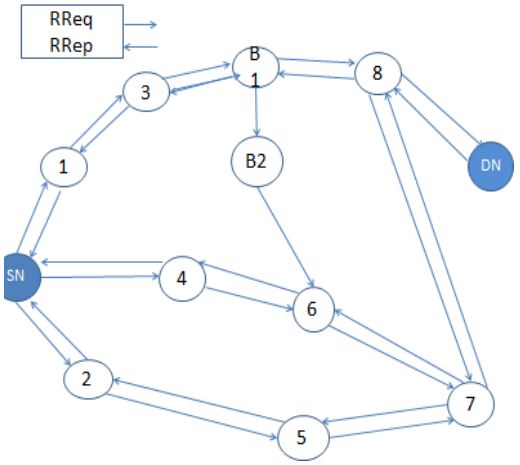

Fig. 1. RReq and RRep message under Black Hole Attack

In the projected answer we intend to modify the operating of supply node victimization further operate [1] as RREP_tab, a timer MOS_Wait_Time and a variable Mali node. We intend to additionally change DRI (data routing table) by adding 'check bit 'with it. The supply node settle for and store all RREPs within the freshly created table i.e. RREP_tab till the time ,MOS_Wait_Time that is 0.5 the worth of RREP_WAIT_TIME i.e. the time that supply node waits for RREP management messages before make RREQ management message. Our security mechanism include four security procedures

A) Neighbourhood information assortment and native malicious Node detection.

B) Finding trustworthy node to destination and complete elimination of cooperative region nodes.

C) Establishing secure path to destination.

D) World alarm arising and blacklisting malicious Nodes.

A. Neighborhood data collection and local malicious node detection

At this time every node store information the info the data} forwarding data regarding their neighbors in data routing information table (DRI) from [3].The DRI table for node' 6' in table one maintain routing data of its neighbor nodes B1,B2,5,5,8.An entry '1' for a node below column ' from' implies that node half dozen has forward knowledge packet coming back from that node Associate in Nursingd an entry '1' for a node below column 'through' implies that node half dozen has forward knowledge packet to it node .thus entry for node four shows that node '6' has not forward knowledge packet

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 8, August 2015

coming back from node '4' however node '6'has forward knowledge packet to node '4' when an exact threshold quantity (which rely on the quality of the network) every node determine its neighbor that doesn't act for the aim of knowledge communication

Local Anomaly Detection

The first security procedure is invoked by a node once it identifies a node that has not act for the aim of information communication, and treated such node because the suspicious nodes by examining its DRI table as mentioned higher than. The node that initiates the native anomaly detection procedure is termed as leader Node (IN) i.e.as shade given in [5]. The node that with success takes half in digital communication is thought as cooperative node (CN). The IN first chooses a Cooperative Node (CN) in its neighborhood supported its DRI records and broadcasts a RREQ message to its 1-hop neighbors requesting for a route to the CN. back to the current RREQ message the IN can receive variety of RREP messages from its neighboring nodes. it'll definitely receive a RREP message from the suspected Nodes (SNs). when receiving the RREP from the SNs the IN sends a groundwork packet to the CN through the SNs one by one to envision the complete SNs. IN send probe packet a minimum of double to every SNs. when the time to measure (TTL) worth of every probe packet is over, the IN enquires the CN whether or not it's received the probe packet. If the reply to the current question is affirmative, (i.e., the probe packet is received by the CN) then the IN updates its DRI table by creating AN entry '1' below the column 'Check Bit' against the node ID of the SNs. However, if the probe packet is found to not reached the CN, then IN build AN entry '0' below the column 'check bit'.When each node i.e. node 6 check its neighbor. 5,4,8 b1 b2 he find that node b1 ,b2 ,8 ,4 are suspected nodes and node 5 is trusted node for node 6 i.e. he securely route data from node 5 with both column filled with 1, 1.

TABLE I DRI ENTRY FOR NODE 6

Node id	Form	Through
B1	0	0
B2	0	0
5	1	1
4	0	1
8	0	1

In Fig. 1, node 6 acts as the IN and initiates the local Anomaly detection procedure for all SNs (First for node B1) and chooses Node 5 as the CN because Node 5 is the most reliable node for node 6 as both the entries under columns 'From' and 'Through' for Node 5 is '1'. Node 6 broadcasts a RREQ message to all its Neighbor nodes B1, B2, 4, 8, requesting them for a route to the CN, i.e., node 5 .in the example. After receiving a RREP From the nodes, IN sends a PROB PACKET 1 first from node b1 to Node 5 after TTL value OF FIRST PROB PACKET is over then IN enquires node 5 whether it has Received the probe packet. ,if node 5 has not received the probe packet, then node 6 send another PROB PACKET 1 to node 5 through node B1 again after TTL value it enquires node 5 whether he receive the packet from node 6 if PROB PACKET 1 is received by CN then IN node makes an entry '1' under the column 'Check Bit' in its DRI table corresponding to the row of node B1 otherwise filled it with entry ' 0' .Similarly IN check all other neighboring node to fill their corresponding 'check bit.

TABLE II MODIFIED DRI ENTRY FOR NODE 6

Node id	Form	Through	Check bit
B1	0	0	0
B2	0	0	0
5	1	1	1
4	1	1	1
8	1	1	1

From here node 6 verify b1, b2 as suspected node also reliable neighbors, 5, 4, 8.

B. Finding trusted node to destination and complete elimination of cooperative black hole

Now through AODV protocol the supply (SN) send route request (REQ) for the destination node (DN) currently the supply node (SN) can expect a time MOST_WAIT_TIME and to receive and store all route reply (RREP) returning from the destination node or from intermediate nodes and store all the request in its buffer in RREP_tab .now supply demand there DRI tables and store then in buffer alongside their 'check bits' currently the supply examine DRI table of all the nodes sequentially to search out the trusty nodes Example If source' SN' found 'RREP' comes from node eight,6, b1 b2 6 ,7 for reaching destination 'DN'

TABLE III RREP_tab

Node RREP to destination	B2	B1	8	6	7

Then supply demand their several DRI table with parity bit and realize one trusty node (CN) to destination With the assistance of parity bit .Now supply node send prob. packet a pair of through remaining suspected node thereto trusty node when TTL price OF initial PROB PACKET is over supply node Sn build enquiry to trust node (CN) whether or not he receive prob. packet 2. If packet not receive then supply node send another PROB PACKET a pair of to CN. if anyone of 2 PROB PACKET is received we tend to contemplate that node as associate other trusty node and supply node mark an entry underneath parity bit as '1'for that node however if the packet isn't received supply treat them as 'black hole node' and maintains the identity of such node as MALI_node, thus in future it will discard any management messages returning from that node.

C. Establish secure path to destination

The nodes whose bit is '1' is taken into account as sure node to the destination currently we tend to check the DRI entry of such nodes to seek out another sure node during this means a secure path is established from supply to destination by eliminating malicious nodes. Consistent with figure one secure path is S, 4, 6, 7, 8, DN.

D. Global alarm arising and blacklisting malicious node

The nodes that mark as '0 'under the column parity bit and that don't respond for chance packet is marked as part node. We tend to store identity of such malicious node as African country _node so in future we are able to discard

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 8, August 2015

any management message returning from that node and inform all the nodes within the network by generating alarm message to all or any the node within the network concerning malicious node .It conjointly ensures that the known malicious node is isolated so it cannot use any network resources.

IV. METHODOLOGY OF EVALUATION

We performed simulations in Network Simulator ns-2. We have studied Different network scenarios to back up the Defined model. Our Simulations run for 600 seconds. Nodes are placed on a flat plane of 1000m x 1000m. For radio propagation, the default Two Ray Ground model is used.802.11 is used as Media Access Control protocol. NodesMobilize to random points at random speed which is less than 10 meter per second and are assumed to be alwaysmoving. Movements are randomized by program and saved in a scenario file for each simulation. Constant bit rate (CBR) generator is used to generate packets. Data packet size is 512 bytes. The number of nodes is varied between 5, 25, and 50 nodes in which two of them are a resource saving node or a node which will perform black hole attack. Data transfer rate between nodes 512Kbps

TABLE IV SIMULATION PARAMETERS

Parameter	Value
Simulator	Ns-2
Simulation Time	600s
Number of nodes	5,25,50
Routing Protocol	AODV
Traffic Model	CBR
Pause time	2s
Mobility	Less than 10 m/s
Terrain area	1000m x 1000m
Transmission Range	512m
No. of malicious node	1

We can conclude that the packet delivery ratio is increased which means that the delivery ratio of eliminated black hole scenario goes up after detecting black hole. It goes around 85% in average when the black hole present the delivery ratio is under 60% It is observed from simulation that our proposed mechanism perform better result as compared to the normal AODV protocol under black hole attack

V. CONCLUSION AND FUTURE WORK

Black hole attack is one of the major security challenges for Manet's .We has proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to identify multiple black hole nodes cooperating with each other in a MANET; and Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also we showed that the effect of packet delivery ratio and Throughput with respect to the variable Node mobility. There is reduction in Packet Delivery Ratio and Throughput. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of malicious node in ad hoc networks is still considered to be a challenging task. Simulation show that AODV with our mechanism gave comparatively better performances as compared to AODV As a future scope of work, the proposed security mechanism may be extended to detect other malicious nodes as gray hole and Detection of wormhole attacks in MANETs.

REFERENCES

[1] NitalMistry, Devesh C Jinwala, Member, IAENG, MukeshZaveri, "Improving AODV Protocol against Black hole Attacks", Proceedings of the International Multi Conference of Engineers and Computer Scientists, 2010, vol. II, IMECS 2010, March 17-19, 2010, Hong Kong

[2] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dynamics Learning System Against Black hole Attack In Body Based Manet." In: International Journal of Computer Science Issues, vol.2, 2009, pp. 54-59

[3] HesiriWeerasinghe and Huirong Fu, Member of IEEE, "Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: "Simulation implementation and Evaluation, International Journal of Software Engineering and Its Application vol.2, No.3, 2008. Oakland University Rochester MI 48309 USA, June 2008, pp. 16-20.

[4] K.Vijaya"Secure 2Ack Routing Protocol in Mobile Ad Hoc Networks," TENCON 2008, IEEE Region 10 Conference, November 2008, pp. 1-7.

[5] Jay dip Sen., M.Girish Chandra Harihara S.G H.ReddyP. Balamuralidhar,"A Mechanism for Detection of Gray Hole Attack" in Mobile AdHoc Networks," Information, Communications & Signal Processing, 2007 6th International Conference on. ICICS 2007, pp1-5.

[6] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26

[7] J. Sen., M. Girish Chandra, P. Balamuralidhar, S.G. Harihara, and H. Reddy, "A distributed protocol for detection of packet dropping attack in mobile ad hoc networks", in Proceedings of IEEE International Conference on Telecommunications (ICT'07), May 2007, Penang, Malaysia.

[8] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method". International Journal of Network Security, vol.5, No.3, , Nov. 2007, PP.338– 346.

[9] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, March 2005, pp. 2137-2142.

[10] C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.

[11] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, 2003, pp. 570-575.

[12] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad-hoc networks," In Proceedings of the 8th

[13] Annual International Conference on Mobile Computing and Networking (MobiCom 2002), , ACM Atlanta, GA, September 2002, pp. 12-23. C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.

[14] P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks," In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.

[15] H. Deng, W. Li, and D.P. Agrawal, "Routing security in wireless Ad hoc networks," IEEE Communications Magazine, vol. 40, Issue: 10, October 2002, pp. . .70 - 75.

[16] Boston, Massachusetts, United States,2000, pp. 255-265 S. Marti, T. Guili, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In Proceedings of MOBICOM.