ISSN:0975-9646

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

Aakanksha Choubey[1], Neelam Peters[2]

Associate Professor, Computer Science and Engineering, Shree Shankaracharya Technical Campus, Bhilai, India [1]

Student (M. E CTA), Computer Science and Engineering, Shree Shankaracharya Technical Campus, Bhilai, India [2]

***Abstract*— Ad hoc Network may be a self-organized autonomous network that consists of mobile nodes that communicate with each other over wireless links .Wireless impromptu networks square measure not well protected against the attack of malicious nodes as a result of security vulnerabilities within the routing protocols. One of the common attacks in MANETs is that the part Attack, in which malicious node incorrectly claiming it to own the recent and shortest path to the destination and so drops all the receiving packets. If this malicious node work along as a gaggle then the damage are going to be terribly serious. This sort of attack is understood as Cooperative part attack. We have a tendency to plan a mechanism to mitigate single part attack likewise as cooperative black hole attack to get a secure route to the destination by avoiding attacks. During this paper we have a tendency to planned associate degree approach for better analysis and improve security of AODV that is one in all the popular routing protocols for Edouard Manet. Our theme is based on AODV protocol that is improved by deploying Advanced DRI table with extra parity. The Simulation on NS2 is meted out and also the planned theme has created results that demonstrate the effectiveness of the mechanism in detection and elimination of the attack and increasing network performance by reducing the packet dropping magnitude relation in network.**

***Keywords*— Mobile Ad hoc network, Black Hole Attack, IDSAODV, Packet Dropping Ratio, Network Simulator2.**

I. INTRODUCTION

A mobile accidental network (MANET) consists of variety of mobile nodes equipped with a transmitter and a receiver. A Mobile Ad-Hoc Networks could be an assortment of distributed nodes, that communicates over wireless network, There are range of vulnerability exist in Manet as lack of a fixed infrastructure, restricted information measure ,dynamic topology, resource constraints and particularly restricted battery life and memory usage etc. The communication is troublesome to organize because of frequent configuration changes. Routing and network management area unit done hand in glove by the nodes therefore forms multi hop design, wherever every node work as host likewise as router that forward packets for different nodes that will not be inside direct communication vary. As, router the node can notice the optimum path and manage the data delivery with the assistance of routing protocol theme there area unit many various routing protocols are devised for accidental networks and have principally classified into 3 categories like proactive (table driven) and reactive (On demand) and hybrid protocols. The proactive protocols maintain routing data regarding every node and data is updated throughout the network sporadically or once topology changes. Each node needs to store and exchange routing data with different nodes sporadically so as to own current routes to all destination i.e. destination sequence distance vector (DSDV) Protocol. In reactive or supply initiated on demand protocols, a node initiate a route discovery method throughout the network, only if it need to send packets thus don't sporadically update the routing data i.e. Ad hoc on demand distance vector (AODV)Dynamic supply Routing (DSR) etc. Hybrid protocol makes use of each reactive and proactive approaches i.e. Zone Routing Protocol (ZRP). during this paper we tend to specialise in AODV protocol which is one amongst the reactive routing protocols in MANETs. AODV is a gorgeous protocol for many researchers as a result of its effectively adaptive nature in extremely dynamic environment accidental On Demand Distance Vector (AODV) routing protocol is appropriate for each Unicast and Multicast routing. it's loop-free and self-starting protocol, builds routing methods between the nodes as long as demanded by the source nodes. Manet's area unit liable to varied styles of attack as well as passive attack as eavesdropping, and active attack as interfering, impersonation and denial of service attack. Denials of service (DOS) attacks that create network connectivity unprocurable to the supposed user of the network Black hole attack could be a reasonably active Denial of Service (DOS) attack. A part attack may be shaped either by a single malicious node or by many nodes in collusion. In black hole attack a malicious node tries to capture the trail toward itself by incorrectly claiming massive sequence range and smaller hop count to the destination and so drop all knowledge packet rather than forwarding to the destination .In cooperative part attack set of node is also compromised in such some way that it should not be attainable to detect their malicious behaviour such node will generate new fake routing messages and supply incorrect link state information and therefore increase packet dropping magnitude relation within the network. In this paper we've got planned a mechanism to spot multiple part nodes cooperating as a bunch in accidental network .the planned mechanism work with slightly modified AODV protocol and create use of the info routing information table (DRI) with 'check bit' additionally to cached and current routing table. We've got determine misbehaviour nodes in mobile accidental setting, and also find secure route to the destination. And enhance the performance of network by eliminating cooperative black hole attack. The reminder of paper II organized as follows section II described related works, in section III AODV and behaviour of cooperative black hole attack is discussed, section IV proposed

mechanism is discussed for making MANET free from cooperative black hole attack and also theoretical analysis of the proposed scheme is covered is 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

The authors discuss a protocol viz. DPRAODV to counter the Black hole attacks. DPRAODV checks to search out whether or not the RREP_Seq_No is over the brink worth. During this protocol, the brink worth is dynamically updated at when interval. If {the worth|the worth} of RREP_Seq_Nos found to be over the brink value, the node is suspected to be malicious and is side to a listing of blacklisted nodes. It conjointly sends associate degree ALARM packet to its neighbours with data regarding the blacklisted node. Thus, the neighbour nodes grasp those RREP packets from the malicious node area unit to be discarded. That is, if any node receives the RREP packet, appearance over the list to examine the supply of the received message. If the reply is from the suspected node, an equivalent is unnoticed. Thus, the protocol tho' productive, suffers from the overhead of change threshold worth at when Interval and generation of the ALARM packets. The routing overhead, as a result's higher. Researchers have projected varied techniques to stop region attack in mobile circumstantial network. Ramaswamy et al. [2] projected an answer to defensive against the cooperative region attacks. However no simulations or performance evaluations are done. Hesiri. Weerasinghe and, Huirong. Fu [3] introduces the utilization of information Routing data DRI to stay track of past routing expertise among mobile nodes within the network and crosschecking of RREP messages from intermediate nodes by supply nodes. The most downside of this method is that mobile nodes ought to maintain additional information of past routing experiences additionally to a routine work of maintaining their routing table. It's evident that maintaining past routing experiences wastes memory area furthermore as overwhelming a major quantity of interval that contributes to slow communication. Mechanisms for securing the routing layer of a Manet by cryptanalytic techniques square measure projected by Hu et al [4], Papadimitratos and Hass [5]. Deng, Li and Agrawal [6] have prompted a mechanism of defence against a region attack on AODV routing protocol. In their projected theme, once the Route Reply packet is received from one in every of the intermediate nodes, another Route Request is shipped from the supply node to the neighbour node of the intermediate node within the path. this is often to envision whether or not such a path very exists from the intermediate node to the destination node. Whereas this theme fully eliminates the region attack by one assailant, it fails miserably in distinctive a cooperative region attack involving multiple malicious nodes. Researchers have planned numerous techniques to stop part attack in mobile unintended network. Ramaswamy et al. [2] planned an answer to defensive against the cooperative part attacks. However no simulations or performance evaluations are done. Hesiri. Weerasinghe and, Huirong. Fu [3] introduces the utilization of information Routing info DRI to stay track of past routing expertise among mobile nodes within the network and crosschecking of RREP messages from intermediate nodes by supply nodes. The most disadvantage of this method is that mobile nodes ought to maintain an additional info of past routing experiences additionally to a routine work of maintaining their routing table. It's evident that maintaining past routing experiences wastes memory house in addition as intense a major quantity of interval that contributes to slow communication. Mechanisms for securing the routing layer of a Manet by cryptologic techniques area unit planned by Hu et al [4], Papadimitratos and Hass [5]. Deng, Li and Agrawal [6] have advised a mechanism of defence against a region attack on AODV routing protocol. In their projected theme, once the Route Reply packet is received from one in every of the intermediate nodes, another Route Request is shipped from the supply node to the neighbour node of the intermediate node within the path. This is often to see whether or not such a path extremely exists from the intermediate node to the destination node. Whereas this theme fully eliminates the region attack by one aggressor, it fails miserably in distinctive a cooperative region attack involving multiple malicious nodes.

III. Ad Hoc On-Demand Distance Vector Routing

The circumstantial On-demand Distance Vector Routing (AODV) protocol may be a reactive unicast routing protocol for mobile circumstantial networks. It operates in 2 phases specifically route discovery and route maintenance AODV uses route discovery by broadcasting RREQ to all or any its neighbouring nodes, Sequence numbers facilitate in avoiding the chance of forwarding an equivalent packet quite once. once a supply node needs a route to a destination, it broadcasts a route request (RREQ) packet across the network. These broadcasted RREQ packet is received by every node gift within the network throughout its travel every node will increase the hop count by one. If Associate in Nursing RREQ message with an equivalent RREQ ID is received, the node merely rejects the freshly received RREQs. Associate in Nursing RREQ arrives at a node that possesses a current route to the destination. If Associate in nursing intermediate node incorporates a route entry for the required destination, it determines whether or not the route is current by examination the destination sequence variety in its own route entry to the destination sequence variety within the RREQ. If the RREQ's sequence variety for the destination is bigger than that recorded by the intermediate node, then intermediate node should not use its recorded route to reply to the RREQ. Instead the intermediate node rebroadcasts the once the destination node or intermediate node that has contemporary enough route to the destination receive the RREQ message they produce Associate in Nursing RREP message and update their routing tables with accumulated hop count and therefore the sequence number of the destination node. Subsequently the RREP message is unicasted to the supply node. AODV Broadcasting a RREQ from supply node and procure a unicast RREP from destination node or intermediate node, Route maintenance is finished by suggests that of route error (RERR) packets. RERR (Route

Error) is initiated by the node upstream (closer to the source) of the break. it's propagated to any or all the affected destinations. RERR lists all the nodes laid low with the link failure once AN intermediate node detects a link failure (via a link-layer feedback,.), it generates a RERR packet. The RERR propagates towards all traffic sources having a route via the unsuccessful link, and erases all broken routes on the approach. A supply upon receiving the RERR initiates a brand new route discovery if it still desires the route. Aside from this route maintenance mechanism, AODV conjointly features a timer-based mechanism to purge stale routes. In AODV protocol, the routing table entry contains the

following fields:
Scientific discipline address,
destination sequence range,
next-hop scientific discipline address,
hop-count,
entry expiration time>

Cooperative Black Hole Attack

A region attack is quite denial of service attack wherever a malicious node will attract all packets by incorrectly claiming a recent route to the destination and so absorbs them while not forwarding them to the detonation. A region attack should faces within the 1st face the malicious node exploit the unexpected routing protocol as AODV to advertise itself as having a legitimate route to a destination node within the second face the assaulter node drops the intercepted packets while not forwarding them. Faux RREP messages from a malicious node contain the subsequent parameters:

A. most destination sequence range − to create the route up thus far.

B. Single hop-count − to create a route with the shortest path.

C. Life-long route − informs a route can exist as long because the network.

D. Destination IP address − address of the destination node derived from RREQ.

E. Time-stamp − the time the RREP was generated

In case of cooperative region multiple region node area unit act in coordination with one another the primary region node B1fordward all the information to its partners node B2 and B2drop them rather than forwarding to destination. As In fig one supply node Sn desires to speak with the destination node DN , the supply node Sn broadcast the RREQ packet., every neighbouring node update its routing table with Associate in Nursing entry for the supply node Associate in Nursingd checks if it's the destination node or whether it has current route to the destination node if associate intermediate node doesn't have this route to the destination node it updates the route request packet by increasing the hop count and floods the network with the route request to the destination node DN or the other intermediate node that has current route to DN. The destination Node DN or any intermediate node that has presently route to DN initiate a route reply within the reverse direction as shown in figure. The supply atomic number 50 sends packet to the node that response initial and discards others. In previous work author [14] propose answer to spot single part attack. however once multiple part nodes square measure acting in coordination with one another initial part B1 talk to its partner B2 as next hope, then as previous mechanism propose in [14], the supply atomic number 50 send more request (frq) to B2 through a distinct route (S, 4, 6, B2) aside from via B1.Node S raise B2 if he's having route to B1 and route to DN. as a result of B2 is co in operation with B1 its more reply is 'yes 'for each queries currently as per answer in [11] node S begin causing packet assumptive route (S,B1,B2) is secure however the packet square measure drop in node B1

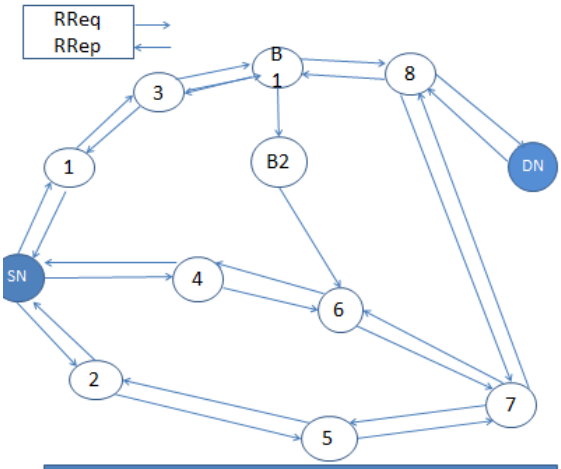

Fig.1Shows RReq and RRep message under Black Hole Attack

IV. PROPOSED MECHANISM

. The supply node settle for and store all RREPs within the fresh created table i.e. RREP_tab till the time ,MOS_Wait_Time that is [*fr1] the worth of RREP_WAIT_TIME i.e. the time that supply node waits for RREP management messages before create RREQ management message. Our security mechanism accommodates four security procedures

(A) Neighbourhood information assortment and native malicious Node detection.

(B) Finding trusty node to destination and complete Elimination of cooperative part nodes.

(C) Establishing secure path to destination.

(D) World alarm arising and blacklisting malicious Nodes.

A. Neighbourhood information assortment and native malicious Node detection.

At this time every node store {the information the info the data} forwarding data concerning their neighbours in data routing information table (DRI) from [3].The DRI table for node' 6' in table one maintain routing data of its neighbour nodes B1,B2,5,5,8.An entry '1' for a node below column ' from' implies that node six has forward information packet returning from that node associate degree an entry '1' for a node below column 'through' implies that node six has forward information packet to it node .thus entry for node four shows that node '6' has not forward information packet returning from node '4' however node '6'has forward information packet to node

'4' once a definite threshold interval (which depend upon the quality of the network) every node establish its neighbour that doesn't act for the aim of knowledge communication

Native Anomaly Detection

The first security procedure is invoked by a node once it identifies a node that has not act for the aim of knowledge communication, and treated such node because the suspicious nodes by examining its DRI table as mentioned on top of. 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 initial chooses a Cooperative Node (CN) in its neighbourhood supported its DRI records and broadcasts a RREQ message to its 1-hop neighbours requesting for a route to the CN. Back to the current RREQ message the IN can receive variety of RREP messages from its neighbouring nodes. it'll definitely receive a RREP message from the suspected Nodes (SNs). once receiving the RREP from the SNs the IN sends an exploration packet to the CN through the SNs one by one to envision the whole SNs. IN send probe packet a minimum of two occasions to every SNs. once the time to measure (TTL) price 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 associate degree 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 associate degree entry '0'below the column 'check bit'. once every node i.e. node six check its neighbour. 5,4,8 b1 b2 he notice that node b1 ,b2 ,8 ,4 ar suspected nodes and node five is trusty node for node six i.e. he firmly route information from node five with each column filing In Fig. 1, node six acts because the IN and initiates the native Anomaly detection procedure for all SNs (First for node B1) and chooses Node five because the CN as a result of Node five is that the most reliable node for node six as each the entries below columns 'From' and 'Through' for Node five is '1'. Node six broadcasts a RREQ message to any or allits Neighbour nodes B1, B2, 4, 8, requesting them for a route to the CN, i.e., node 5 .in the example. once receiving a RREP From the nodes, IN sends a PROB PACKET one initial from node b1 to Node five once TTL price OF initial PROB PACKET is over then IN enquires node five whether or not it's Received the probe packet. ,if node five has not received the probe packet, then node six send associate degree other PROB PACKET one to node five through node B1 once more once TTL price it enquires node five whether or not he receive the packet from node six if PROB PACKET one is received by CN then IN node makes an entry '1' below the column 'Check Bit' in its DRI table similar to the row of node B1 otherwise stuffed it with entry ' 0' .Similarly in restraint all different neighbouring node to fill their corresponding 'check bit. From here node six verify b1, b2 as suspected node conjointly reliable neighbours, 5, 4, 8.

B. Finding trusty node to destination and complete Elimination of cooperative part nodes.

Now through AODV protocol the supply (SN) send route request (REQ) for the destination node (DN)currently the supply node (SN) can watch for 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 at the side of their 'check bits' currently the supply examine DRI table of all the nodes consecutive to seek out the trusty nodes Example If source' SN' found 'RREP' comes from node eight,6, b1 b2 6 ,7 for reaching destination 'DN' Then supply demand their various DRI table with bit and notice one trusty node(CN) to destination With the assistance of bit .Now supply node send prob. packet a pair of through remaining suspected node to it trusty node once TTL price OF initial PROB PACKET is oversupply node metallic element 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 anybody of 2PROB PACKET is received we tend to take into account that node as associate degree other trusty node and supply node mark an entry below 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 trusty node to the destination currently we tend to check the DRI entry of such nodes to seek out another trusty node during this means a secure path is established from supply to destination by eliminating malicious nodes. per figure one secure path S, 4, 6, 7, 8, DN.

D. world alarm arising and blacklisting malicious node

The nodes that mark as '0 'under the column bit and that don't respond for likelihood packet is marked as part node. we tend to store identity of such malicious node as Republic of Mali _node so in future\rawer will discard any management message returning from that node and inform all the nodes within the network by generating alarm message to any or all 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. SIMULATION AND RESULTS

We performed simulations in Network machine ns-2. We've got studied completely different network eventualities to back up the outlined model. Our Simulations run 600 seconds. Nodes are placed on a flat plane of 1000m x 1000m. For radio propagation, the default 2 Ray Ground model is employed. 802.11 is employed as Media Access management protocol. Nodes mobilize to random points {at random|randomly|indiscriminately|haphazardly|willy-

nilly|arbitrarily|every that way} speed which is a smaller amount than ten meter per second and are assumed to be continually moving. Movements arrandomised by program and saved in a very situation file for every simulation. Constant bit rate (CBR) generator is employed to get packets. Information packet size is 512 bytes. User information Program protocol is employed in transport layer. the amount of nodes is varied between five, 25, and fifty nodes within which 2 of them are a resource saving node or a node which can perform part attack. Information transfer rate between nodes 512Kbps.

VI Conclusion And Future Work

Black hole attack is one in every of the key security challenges for MANETs .We have projected a possible answer for it within the AODV protocol. The projected answer will be applied to spot multiple part nodes cooperating with one another in a very MANET; and see secure methods from supply to destination by avoiding multiple part nodes acting in cooperation. Conjointly we tend to showed that the impact of packet delivery magnitude relation and outturn with regard to the variable node quality. There's reduction in Packet Delivery magnitude relation and outturn. In part attack all network traffics ar

Redirected to a selected node or from the malicious node inflicting serious injury to networks and nodes as shown within the results of the simulation. The detection of malicious node in unplanned networks remains thought-about to be a difficult

Task. Simulation show that AODV with our mechanism gave relatively higher performances as compared to AODV As a future scope of labour, the projected security mechanism could also be extended to notice different malicious nodes as grey hole and Detection of hollow attacks in MANETs.

References

[1] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri, "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] Hesiri Weerasinghe 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] Latha Tamilselvan 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] Latha Tamilselvan 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.

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

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

[11] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad-hoc networks," In Proceedings of the 8thAnnual International Conference on Mobile Computing and Networking (MobiCom 2002), , ACM Atlanta, GA, September 2002, pp. 12-23.