Preventing DSR routing protocol against Black Hole using Counting Method

Pooja Bavarva[1],Pratik Modi[2]

[1]*Department of Computer Engineering, LDRP-ITR, poojabavarva@gmail.com*
[2]*Departmen of Computer Engineering, LDRP-ITR, pratik1031@gmailcom*

Abstract-Ad-hoc networks are developing engineering, because of their spontaneous nature, are often made frail situations, which makes them helpless against attacks. These attacks are propelled by taking part malicious node against distinctive system administrations. Specially Dynamic Source Routing(DSR) is a comprehensively acknowledged system directing convention for Mobile Ad-hoc Network (MANET). Black Hole attack is one of the serious security dangers in ad-hoc systems which could be effortlessly utilized by misusing powerlessness of on-demand routing protocols such as DSR. In this paper we proposed a Counter calculation for distinguishing the malicious node in DSR protocol experiencing black hole attack. Subsequently we can show the huge change of packet delivery ratio (PDR) and average End-to-End delay.

Keywords -mobile ad hoc networks; routing protocols; black hole attack; DSR

I. INTRODUCTION

Wireless networking is a developing technology that permits users to get to data and services electronically, paying little heed to their geographic position. Wireless networks have ended up progressively well known in the registering business. The requisitions of the ah-hoc system are endless. Mobile Ad hoc system (MANET) is a self-composed system on the grounds that it is a base less characteristic of systems. MANET is an accumulation of nodes. Every node can join by wireless correspondence links, without any settled station for example, base station. In MANET every node can act as a router and network is attained in the structure of multihop chart between the node [1].

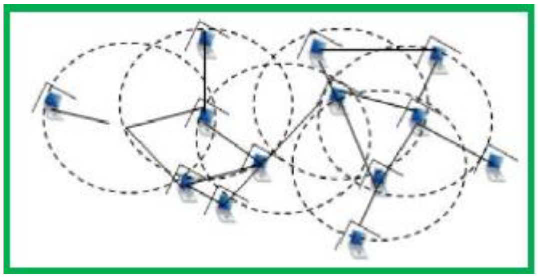

Fig. (a): Wireless Network Structures (Infrastructure less Networks)[1]

Because of the one of a kind attributes of MANET, creating an intrusion detection systems (IDS) in this system is challenging. There is no unified gateway device to screen the system activity. Since the medium is open, both honest to goodness and malicious nodes can get to it. In addition, there is no agreeable division between ordinary and unusual exercises in a mobile nature. Since nodes can move arbitrarily, false routing data can originate from a traded off node or a legitimate node that has old fashioned data. Black hole attack is a standout amongst the most widely recognized attack made against the reactive routing protocol in MANETs. The black hole attack includes malicious node(s) fabricating the hope-count, consequently claiming to have the most limited and freshest route to the destination. Various studies have attempted to devise successful discovery strategies for this attack. The point of this paper is to discover strategies against the black hole attack inside the extent of Dynamic Source Routing (DSR) protocol [1] [2].

II. Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) [3, 4] is a basic and effective directing convention composed detail for utilization in multi-hop wireless ad hoc mobile network. DSR is one of the essential routing protocol that are utilized for mobile ad hoc networks as much energy proficient routing protocols are planned focused around its component. It discovers the routes from source to destination just when the source launches route finding methodology. All parts of protocol work altogether on interest. This protocol likewise makes the network sorting toward oneself out and self arranging. Essentially the protocol is made out of two instruments, Route Discover and Route Maintenance and these two systems cooperate to permit nodes to run across and keep up the source route to any destination node.

- Route Discovery
- Route Maintenance

A) Route discovery

Route discovery is finished with two sub steps that is Route request and Route Reply.

B) Route request

The route discovery comes in play when a mobile node has some information/packet to send to any destination and it doesn't have any route to the destination in its route cache. At that point it launches route discovery by broadcasting a route request (RREQ) packet. This route request holds location of the destination, location of the source and a unique identification number that is produced by the source node just. Every node accepts the packet and checks whether the packet is implied for it or not. In the event that it is not the destination node then it essentially forward the packet to the outgoing links including its own address in the packet. To avoid copy route request which is created from the same source, a node just forwards the route request that has not yet been seen show up in the route request with the same identification number.

C) Route reply

When the packet reaches at the destination node or reaches at a node that holds in its route cache an unexpired route to the destination, then a route reply is created. Not just the packet holds all the location of the intermediate node it has run over however the sequences of hops are likewise stored in it. The Route reply is created by the destination setting the route record held in the route request into route reply. Throughout the route reply if the destination node has the route to the initiator in its route cache, It may utilize that route for route reply. Generally destination node may invert the route in the route record if the connection is symmetric. On the off chance that the symmetric connections are not supported then the node may launch its own particular route discovery piggybacking the route reply on the new route request. At the point when any intermediate node gets any route reply from destination node or any possible node then they add their route record and forwards to its neighbor nodes.

D) Route maintenance

Route maintenance is a methodology of recognizing connection whether it is reliable and equipped for convey packet on it or not. This methodology is executed by the utilization of route error packets and acknowledgements. At the point when the data link layer experiences a fatal transmission issue then a route error message is produced. Assume a packet is retransmitted (up to a most extreme number of attempts) by some hop the greatest number of times and number of receipt conformation in accepted, then this node gives back a packet error

message to the first sender of the packet, recognizing the connection over which the packet couldn't be sent. (Fig.b) shows, AODV routing protocol with RREQ
and RREP message [1].

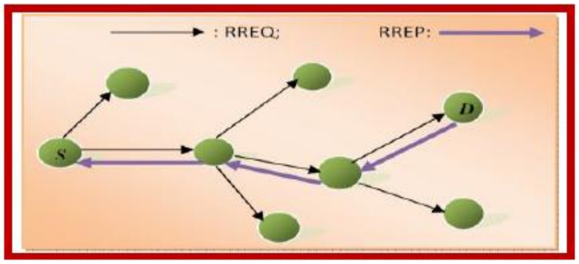

Fig. b: DSR routing protocol with RREQ and RREP message [5]

Figure (Fig.c) shows AODV routing protocol with RERR message [1].

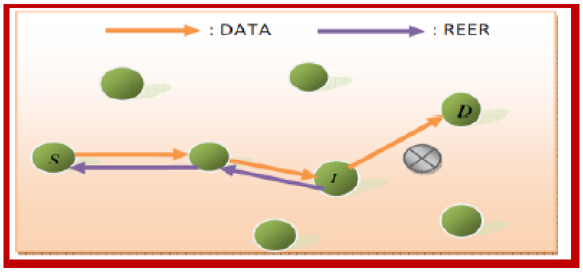

Fig. c: DSR routing protocol with RERR message [5]

III. Black Hole Attack

In a black hole attack, a malicious node sends fake routing data, asserting that it has an ideal route and reasons other good node to route information packets through the malicious one. For illustration, in DSR, the attacker can send a fake RREP (including a fake hop count that is manufactured to be equivalent or higher than the one held in the RREQ) to the source node, guaranteeing that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Along these lines, all traffic will be directed through the attacker, and therefore, the attacker can misuse or discard the traffic.

IV. Existing Work on Black Hole Attack

In [4] Intrusion Detection Systems (IDS) are one of the essential systems utilized to obstruct attacks against security dangers. Intrusion detection can delegated system based and host based. System built IDS introduced with respect to information fixation purposes of a system, for example, switches and routers. In the mobile ad hoc networks we have no central devices that monitors traffic flow so our proposed method intrusion detection using anomaly detection (IDAD) utilization host based IDS outline. IDAD accept each movement of a user or a framework might be observed and irregularity exercises of an intruder could be recognized from typical exercises. To discover a black hole IDAD needs to be given with a pre-collected set of anomaly exercises, called review information. When review information gathered and given to the IDAD framework, the IDAD framework is ready to compare each action and review information. On the off chance that any movement of a host out of the action recorded in the review information, the IDAD framework disconnects the specific node from the system. In this calculation they first broadcast RREQ for route discovery and after that get RREP and match the RREP with the review information on the off chance that they match save route to the route table and send the information generally dispose of the RREP and after that again attempt.

In [2] [8], the authors present the route confirmation request (CREQ) and route confirmation reply (CREP) to maintain a strategic distance from the black hole. In this approach, the intermediate node not just sends RREPS to the source node additionally sends CREQS to its next-hop node at the destination node. In the wake of accepting a CREQ, the next-hop node searches up its cache for a route to the source. In the event that it has the route, it sends the CREP to the source. After getting the CREP, the source node can confirm the validity of the route by analyzing the route in RREP and the one in CREP. In the event that both are matched, the source node judges that the route is right.

One weakness of this methodology is that it can't stay away from the black hole attack in which two consecutive node work in collusion, that is, when the following hop node is a colluding attacker sending CREPS that backing the erroneous path.

In [6] authors have specified the DSR protocol and Black hole attack in MANETs and proposed a practical answer for the black hole attacks that might be executed on the DSR protocol. The Proposed technique might be utilized to discover the secured routes and prevent the black hole nodes in the MANET. As future work, author aim to create reproductions to analyze the execution of the proposed result focused around the different security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility, expanding number of malicious node, expanding number of nodes and extent of the black hole nodes.

In [6], the authors proposed an answer that requires a source node to hold up until a RREP packet touches base from more than two nodes. After accepting numerous RREPs, the source node checks whether there is an shared node or not. On the off chance that there is, the source node judges that the route is safe. The fundamental disadvantage of this result is that it introduces time delay, in light of the fact that it must hold up until different RREPs arrive.

In [10], the authors analyzed the black hole attack and indicated that a malicious node must increment the destination sequence number sufficiently to convince the source node that the route gave is sufficiently enough. In view of this examination, the authors propose a measurable based anomaly identification methodology to locate the black hole attack, taking into account contrasts between the end grouping amounts of the gained RREPs.

The key advantage of this methodology is that it can recognize the attack requiring little to no effort without presenting additional routing traffic, and it doesn't require change of the current protocol. In any case, false positives are the principle detriment of this approach because of the way of inconsistency identification.

In [14], as indicated by author result, data about the following hop to destination should be included in the RREP packet when any intermediate node answers for RREQ. At that point the source node sends a further ask for (FREQ) to next hop of answered node and gets some information about the answered node furthermore route to the destination. By utilizing this system we can distinguish dependability of the answered node just if the following node is trusted. Be that as it may, this result can't prevent cooperative black hole attack on MANETs. For example, if the next hop also cooperative with the answered node, the answer for the FREQ will be essentially "yes" for both inquiries.

V. Proposed Algorithm

The result, which is proposed to keep the black hole attacks in the MANET. This result isessentially to change the working of the source node without substituting intermediate node and destination nodes by utilizing a system called Prior- Recieve-Reply.

In this method we can checking whether there is large difference between the hop count of source nodes or intermediate node who has sent back RREP or not. Typically, the first routes reply in the RR table which is from the malicious node with high destination sequence number. Now, we can compare the first destination hop count with the source hop count. If there is existing much more differences between source and destination hop count, then the destination node is malicious node, then we could immediately eliminate that entry from the RR-Table.

Algorithm:Prior_RecieveReply(RREP)Method

Case I: If source node is blackhole node.

Each intermediate node which receives route request from source node to find the destination will drop the control message and avoid the communication with malicious source node.

Case II: If destination node is blackhole node.

Each intermediate node which receives a control message from malicious destination node towards source node will drop the control message and avoid the communication with malicious node.

Case III: If intermediate node is blackhole node.

If neighbor of malicious node receives a message from malicious node will drop a control message instead of forwarding it.

In all above cases, proposed algorithm removes routing table entries having malicious node entries for all future communication as well.

The above algorithm is identified the malicious node and removed from the table. The routing table does not maintain the malicious node in the path. Moreover, in order to maintain freshness, the RR-Table is flushed once a route request is chosen from it. Thus, the operation of the proposed protocol is the same as that of the original DSR once the malicious node has been detected. The main benefits of proposed solution are:

(1)The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process. (2) With no delay the malicious node are easily identified.(3) No modification is made in other default operations of DSR Protocol (4) Better performance produced in little modification.

VI. Results

Performance comparison is made on the basis of above two metrics between existing DSR and proposed DSR.

Packet Delivery Ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Fig.4 shows that PDR of DSR is heavily affected by the malicious nodes where as the PDR of Proposed DSR are immune to it. According to our result, the proposed DSR is secure against black hole attacks.

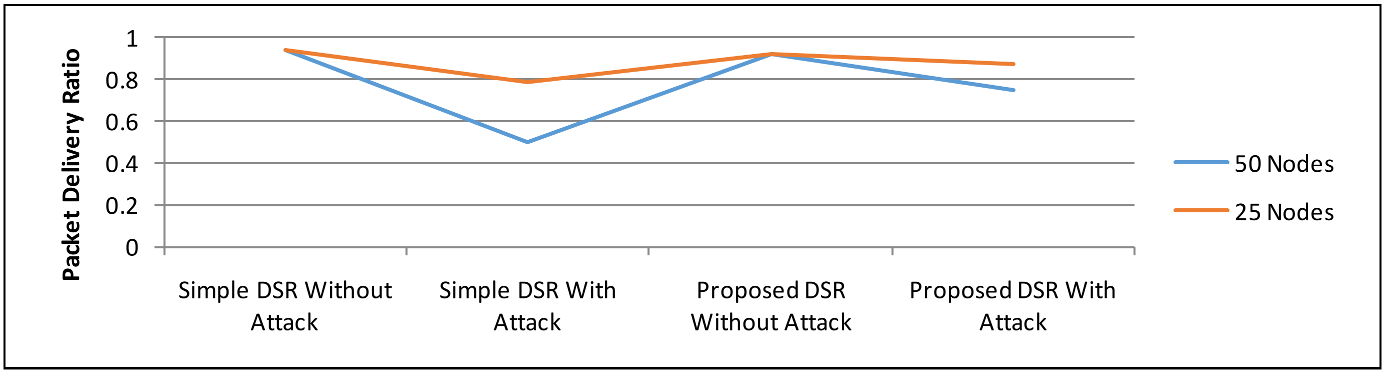

Fig d: Packet Delivery Ratio (PDR)

Average End-to-End Delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at the MAC layer, etc. It is measured in milliseconds. The Fig 5 shows that the significant improvement of modified DSR routing protocol.

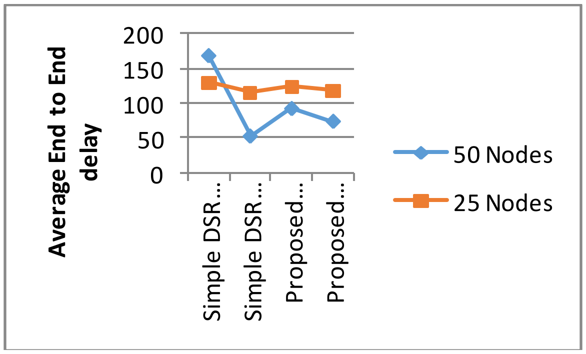

Fig. e: End-to-End Delay

VI. Conclusion

In this article we analyzed the security system with our proposed and modified DSR algorithm. This technique is very simple and efficient approach for defending the DSR protocol against Black Hole attacks. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET.
This method we have three cases:
Case I: If source node is blackhole node.

Each intermediate node which receives route request from source node to find the destination will drop the control message and avoid the communication with malicious source node.

Case II: If destination node is blackhole node.

Each intermediate node which receives a control message from malicious destination node towards source node will drop the control message and avoid the communication with malicious node.

Case III: If intermediate node is blackhole node.

If neighbor of malicious node receives a message from malicious node will drop a control message instead of forwarding it.

In all above cases, proposed algorithm removes routing table entries having malicious node entries for all future communication as well. This algorithm has achieved good improvement in PDR with admissible end-to-end delay. Furthermore, the proposed solution does not require any overhead on either the destination node or any intermediate node on DSR routing protocol.

REFERENCES

[1] Tamilarasan-Santhamurthy; “A Comparative Study of Multi-Hop wireless Ad-Hoc Network Routing Protocols in MANET”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011, PP: 176-184.ISSN(online):1694-0814.

[2]Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; “A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS”, IEEE Wireless Communications •October 2007.PP: 85-90.

[3]S.ciet al; “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks” IEEE Trans.Vehic Tech. vol: 55, No: 4, July2006, PP: 1302-1310.

[4]Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by Yibeltal Fantahum Alem & Zhao Hheng Xaun from Tainjin 300222, China 2010, IEEE.

[5]Neelam Khemariya, Ajay Khunteta, Krishna Kumar Joshi, “Detection and Prevention from Black Hole attack in AODV protocol for MANET” International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1179 ISSN 2229-5518

[6] An Adaptive Approach to Detecting Black Hole Attacks in Ad Hoc Network 2010 24th IEEE International Conference

[7] Modified AODV Protocol against Blackhole Attacks
in MANET by K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4,
K.Thilagam5, Lecturer, Dept. of Computer Applications, Karpagam
University, and Coimbatore. International Journal of Engineering and Technology Vol.2 (6), 2010.

[8] Seungjoon Lee, Bohyung Han, Minho Shin; “Robust Routing in Wireless Ad Hoc Networks” 2002, international Conference.

[9] Mohammad Al-Shurman and Seong-Moo Yoo,Seungjin Park “Black Hole Attack in Mobile Ad Hoc

[10] F.Shin, D.Jin, W.Liu, “Preventing Black Hole in DSR Based Wireless Ad Hoc Networks” Computer Science and its Applications, Lecture Notes in Electrical Engineering Volume 203, 2012, pp
953-969

[11] Weerasinghe.H. “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, IEEE Student Member

[12] Dokurer .S, Y. M. Erten , Can Erkin Acar “Performance analysis of ad-hoc networks under black hole attacks”, Turkey

[13] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”,IACC 258, North Dakota State University, Fargo

[14] Weerasinghe.H. “Preventing Cooperative BlackHole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation”, IEEE Student Member