A Novel Approach to Discover Black Hole and Worm Hole Attacks in MANETs

S.Kanishka, G.Karishma, M.Swetha, J.Keerthi lal
Final year Students, Department of Computer science and Application,
Vels University, Chennai

Abstract

Mobile Ad-hoc networks (MANET) are assemblies of self-organizing mobile nodes with energetic topologies and have no fixed organization. Because of their dynamic ad-hoc nature, in which indefinite device develops unprompted interactions among themselves, then networks are predominantly vulnerable to numerous security threats. Consequently it is proposed to enterprise and implement malicious node detection system to avoid black hole and worm hole attacks in MANETs. In this paper we use Cooperative bait detection scheme to perceive black hole attacks. To detect Worm hole attack as well we combined Performance Evaluation Multipath Algorithm in CBDS scheme. Worm hole attacks are distinguished using hop-count and time delay analysis from the viewpoint of users deprived of any superioratmosphere assumptions.

Keywords— *CBDS, DSR, Reverse Tracing, MANETs, Performance Evaluation Multipath algorithm.*

I. INTRODUCTION

Mobile Adhoc network is infrastructure less network that self-configured repeatedly by mobile nodes deprived of the help of any centralized management. In MANET nodes have special physiognomies that each node in MANET behaves like receiver and transmitter and allow collaborating with other nodes in its radio range. In order for a node to forward a packet to a node that is out of its radio range, the backing of other nodes in the network is needed; this is known as multi-hop communication. Consequently each node must act as both a host and a router at the equivalent time. The network topology normally deviations due to the mobility of mobile nodes in the network. In MANET each node can communicate with the help of its neighbour node that's derives in its radio range. Each node forwards their packet to their neighbour node towards end where path for transmitting message packet is advocated by routing protocol as shortest path. Every routing protocol essences over shortest path where some malicious node over network use this insatiability of routing protocol and present an illusion of shortest path among two end point of network and attack major traffic over the network.

In black hole attacks, a node transmits a wicked broadcast informing that it has the shortest path to the terminus, with the goal of stopping messages. Worm hole attack attract massage packet and play number of misbehave with that routing packet like perusing of confidential message, drop, corrupt and modification transmitted massage over network. In this paper, our focus is on perceiving black hole attacks and worm hole attack using a dynamic source routing (DSR) based routing technique. DSR is a Dynamic Source Routing protocol. It has two main processes: route discovery and route maintenance. To complete the route discovery phase, the source node broadcasts a Route REQuest (RREQ) packet finished the network. If an intermediate node has routing material to the destination in its route cache, it will reply with a RREP to the source node. When destination receives the RREQ, it can know each intermediary node's address amongst the route. The destination node relies on the collected steering information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the recognised route. DSR does not have any detection mechanism, but the source node can get all route information regarding the nodes on the route.

II. RELATED WORK

In Liu et al. proposed a 2ACK scheme for the recognition of routing misbehaviour in MANETs. In this scheme, two-hop heading packets are sent in the opposite direction of the routing path to specify that the data packets have been successfully received. A parameter acknowledgment ratio, that is Rack, is also used to regulator the ratio of the received data packets for which the acknowledgment is compulsory. This scheme belongs to the class of proactive schemes and, hence, produces additional routing upstairs regardless of the existence of malicious nodes. In Xue and Nahrstedt anticipated a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to display the quality of the routing path to be chosen by the destination node. If the performance of the path deviates from a predefined behaviour set for defining "good" routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route unearthing processes, which may lead to significant routing overhead.

In Hongsong et al. proposes an intrusion detection model to contest the black hole attack in AODV routing protocol. In this model, a security agent, recognised by a hardware thread in network processor uses corresponding multithreading architecture; try to detect two cases of figure of attack. Those exploiting AODV control messages RREQ (Route REQuest) and RREP (Route REPly). The agent monitors the RREQ-RREP messages at real-time and if any detection rule is desecrated, the black hole attack is detected and the malicious node is quarantined and recorded to a black list. This solution requires a special material for its implementation. It is enthusiastic to AODV protocol and it considers only control messages, nevertheless that black hole attack can target data messages. In the concept of leashes is introduced to detect worm hole attacks. A leash is any evidence added to a packet in order to restrict the distance that the packet is permitted to travel. A leash is associated with each hop. Thus, each communication of a packet requires a new leash. Two types of leashes are considered, explicitly geographical leashes and temporal leashes. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet.

A temporal leash offers an upper bound on the lifetime of a packet. As a result, the packet can only travel animperfect distance. A receiver of the container can use these leashes to check if the packet has travelled farther than the leash consents and if so Source node stochastically chooses an adjacent node with which to liaise, in the sense that the address of this node is used as bait destination address to bait malevolent nodes to send a reply RREP message. Malicious nodes are thereby sensed and prevented from participating in the routing operation, using a reverse drawing technique. In this setting, it is presumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. The modified CBDS scheme comprises four steps,

1) Theoriginal bait step
2) The initial reverse tracing step
3) Thecleaned to reactive defence step
4) Presentation evaluation multipath phase

A. Initial Bait Step:

The aim of the bait phase is to fascinate a malicious node to send a reply RREP by sending the bait RREQ*'* that it has used to promote itself as having the shortest path to the node that impedes the packets that were converted. The following method is considered to generate the destination address of the bait RREQ*'*. The source node selects an adjacent node. The bait phase is stimulated whenever the bait RREQ*'* is sent prior to seeking the initial routing path. The follow-up bait phase analysis measures are as follows. First, if the *nr* node had not thrown a can drop the packet. In Mahajan et al. proposed some proposals to perceive worm hole attacks like,

1) The abrupt diminution in the path lengths can be used as a possible symptom of the worm hole attack.
2) With the existing advertised path information, if the end-to-end path delay for a path cannot be clarified by the sum of hop delays of the hops present on its publicized path, reality of worm hole can be suspected.
3) Some of the paths may not follow the promoted false link, yet they may use some nodes elaborate in the worm hole attack. This will lead to an increase in hop delay due to worm hole traffic and subsequently an increase in end-to-end delay on the path. An unexpected increase in the end-to-end delay and the hop line up delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the occurrence of worm hole.

III. PROPOSED WORK

This paper offerings detection system called the cooperative bait detection scheme (CBDS), which aims at perceiving and preventing malicious nodes introduction black hole attacks in MANETs. In order to detect Worm hole attacks along with Black hole attacks in MANETs we incorporated Performance Evaluation Multipath Algorithm in CBDS scheme. Worm hole attacks are noticed using hop-count and time delay analysis from the viewpoint of users without any special atmosphere assumptions. In this system the black hole attack, then after the source node had sent out the RREQ', there would be other nodes' reply RREP in accumulation to that of the *nr* node. Consequently, the reverse tracing program in the next step would be initiated in order to detect this route.

If only the *nr* node had guided the reply RREP, it means that there was no other malicious node extant in the network and that the CBDS had commenced the DSR route discovery phase. Another, if *nr* was the malicious node of the black hole attack, then after the source node had sent the RREQ*'*, other nodes would have also sent reply RREPs. This would designate that malicious nodes happened in the reply route. In this case, the reverse tracing program in the next step would be originated to perceive this route. If *nr* calculatingly gave no reply RREP, it would be directly enumerated on the black hole list by the source node. If only the *nr* node had sent a reply RREP, it would mean that there was no other malicious node in the network, excluding the route that *nr* had provided; in this case, the route discovery phase of DSR will be started. The route that *nr* delivers will not be listed in the choices provided to the rout route unearthing phase.

B. Initial Reverse Tracing Step:

To perceive the behaviours of malicious nodes, the reverse tracing program is used finished

the route reply to the RREQ*'* message. The malicious node will reply with a false RREP if it has received the RREQ*'*. Then the reverse tracing process will be directed for nodes receiving the RREP, with the aim to deduce the dubious path information and the momentarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node instantaneously when these nodes send reply RREPs.

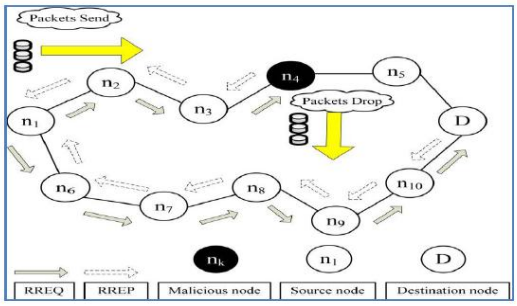

Fig. 1 Black Hole Attack-Node n4 Drops all the Data Packets.

C. Shifted to Reactive Defence Phase:

Subsequently the above, the DSR route finding process is stimulated. When the route is established and if at the destination it is found that the packet delivery ratio knowingly falls to the beginning, the discovery scheme would be generated again to detect for continuous maintenance and real-time reaction efficiency. The threshold is a fluctuating value in the range [85%, 95%] that can be familiarconferring to the current network efficiency. The initial threshold value is set to 90%. A dynamic threshold algorithm is calculated that controls the time when the packet delivery ratio cataracts under the same threshold. If the descending time is summarized, it means that the malicious nodes are still present in the network. In that case, the threshold should be adjusted upward. Then, the threshold will be lowered. It should be discerned that the CBDS offers the opportunity to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the important zone by simply observing at the malicious nodes reply to every RREP.

D. Performance Evaluation Multipath Phase:

In this Phase worm hole attacks are noticed without any extra hardware necessities. The basic idea behind this work is that the worm hole attack reduces the length of hops and the data transmission delay. First, we haphazardlyproduce a Number in between 0 to maximum number of nodes. Then we make the Node with same quantity as transmitter node. After this we produce the route from selected conveying node to any destination node with definite average route length. Then we send packet rendering to selected destination and start timer to count hops and delay. The process is frequent and the routes, their hops and delay are stored. Now if the hop count for a certain route decreases snappishly for average hop count then at least one node in the route must be attacker. Now we check the delay of all previous routes which involve any on node of the doubtful route. Now the node not encounter beforehand should be malicious let there are N such nodes. If N == 1 then it is the attacker else wait for future arrangements which show eccentricity and involve only one of N nodes. Nodes are black listed by the nodes hence they are not complicated in future routes. Whole process is recurring until we didn't get the computed goal. The goal can be to become complete list of malicious nodes.

IV. SIMULATION RESULTS

A simulation of above designated CBDS is developed for recognizing the black hole attack achieved by the malicious node. Simulation is obtained using Java and Net beans Technology. In these simulation scenario twenty nodes has been shaped. Each node has a communication range of 200.

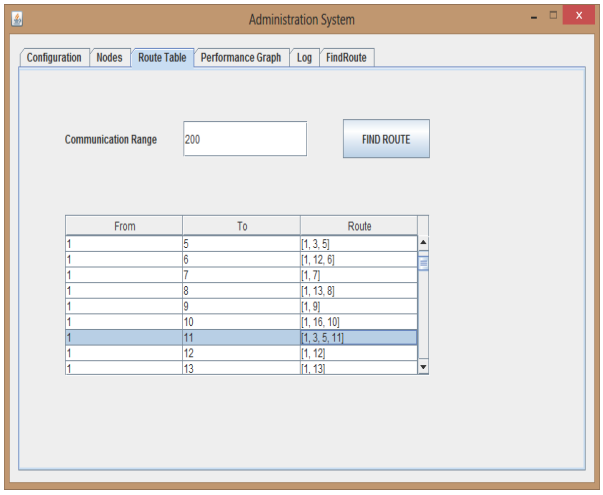

Fig 2. Configuration of Node

As shown dissimilar path from one to another node is calculated using DSR algorithm. Among the dissimilar path (1, 3, 5, and 11) has been preferred for our analysis. Consider node 0 as a source node and 11 as destination node. As source node 0 send data to the destination node 11, the intermediate nodes 5 and 3 advancing the data to the destination node as shown in Fig 5. Consider Node 7 as malicious node, which achieves the black hole attack. It publicizes as having shortest path to the destination, as a result it receives the data from source node 0 and does not forward to the destination node 11. The innovative path before attack is 1, 3,5,11. After the attack the path is 1, 7.

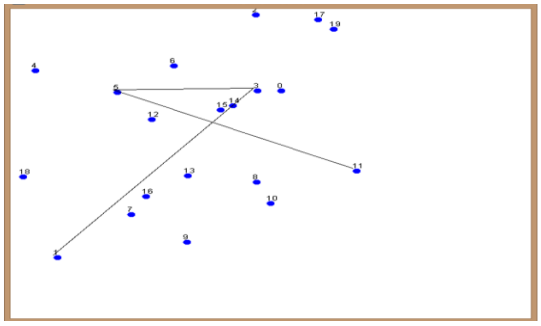

Fig.3 Data Transmission Between Nodes before Attack

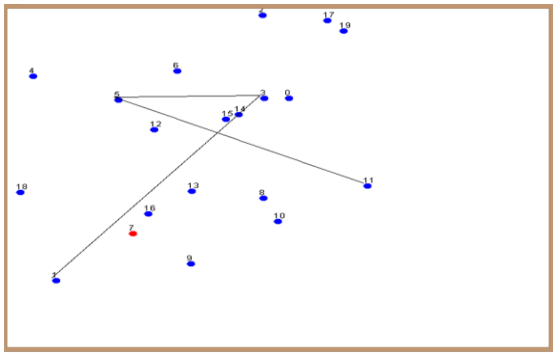

Fig. 4 Malicious Node (black hole) Detected After Attack using Reverse Tracing Program

V. CONCLUSIONS

In this paper, a new mechanism called the CBDS is used for sensing malicious nodes in MANETs under gray/collaborative black hole attacks. To this mechanism, presentation Evaluation Multipath Algorithmhas been added to perceive the worm hole attack in MANETs. As future work, we intend to explore the integration of the CBDS with other well-known message sanctuary schemes in order to concept a comprehensive secure routing framework to defend MANETs against miscreants. We also intend to use CBDS in other routing protocol like AODV.

REFERENCES

[1] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," in IEEE Wireless Communications, Oct. 2007, pp. 85–91.

[2] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[3] FayazAhamed P et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 71-79

[4] Yang H., Luo H., Ye F., Lu S. and Zhang L.: Security in mobile ad hoc networks: challenges and solutions, In IEEE Wireless Communications, vol. 11, no. 1, pp.38–47 (2004).

[5] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 Packet Leashes: A Defense against Worm hole Attacks in Wireless Networks, Twenty-Second Annual Joint Conference of IEEE Computer and Communications, Volume 3, pp. 1976-1986.

[6] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowl- edgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[7] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004.

[8] C. Hongsong, J. Zhenzhou, and H. Mingzeng, "A novel security agent scheme for aodv routing protocol based on thread state transition," Asia Journal of Information Technology, vol. 5, no. 1, pp. 54–60, 2006.

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 Packet Leashes: A Defense against Worm hole Attacks in Wireless Networks, Twenty-Second Annual Joint Conference of IEEE Computer and Communications, Volume 3, pp. 1976-1986.

[10] V. Mahajan, M. Natu, A. Sethi. ,Analysis of worm hole intrusion attacks in MANETS, IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.

[11] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, Preventing Worm hole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach, IEEE Communication Society, WCNC 2005