BLACK HOLE ATTACK COUNTERMEASURES IN MOBILE ADHOC NETWORKS

Opinder Singh[†], Dr. Jatinder Singh[‡], and Dr. Ravinder Singh[‡]

[†] *Research Scholar, IKG PTU, Kapurthala, Punjab.*
[‡]*IKG PTU, Kapurthala, Punjab.*
E-mail: [†]opindermca2008@gmail.com, [‡]bal_jatinder@rediffmail.com, [‡]dr.rs.global@gmail.com

ABSTRACT
A mobile adhoc network (MANET) is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces. In MANET every node can functions as transmitter, router and data sink. MANET has dynamic topology which allows nodes to join and leave the network at any point of time. MANET is more vulnerable due to its characteristics such as dynamic topology, distributed cooperation and open medium. Security issues in mobile adhoc networks are veiled by various techniques that were introduced in past decade. Due to decentralized nature of MANET, the security issues cultivate resulting in welcoming various lethal vulnerabilities. Out of all attacks in MANET, Black hole attacks are considered most challenging adversarial modules that tremendously affect the communication system in MANET. This paper presents survey of various security techniques used for mitigating Black hole attacks in MANET.

Keywords: Mobile ad hoc network (MANET), Security, vulnerabilities, Attacks, Black hole attack, Intrusion Detection Systems.

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e. routing functionality will be incorporated into mobile nodes. MANET is more vulnerable than wired network due to mobile nodes, threats from malicious nodes inside the network. Because of vulnerabilities, MANET is more prone to malicious attacks. MANET has following vulnerabilities [1, 2]:

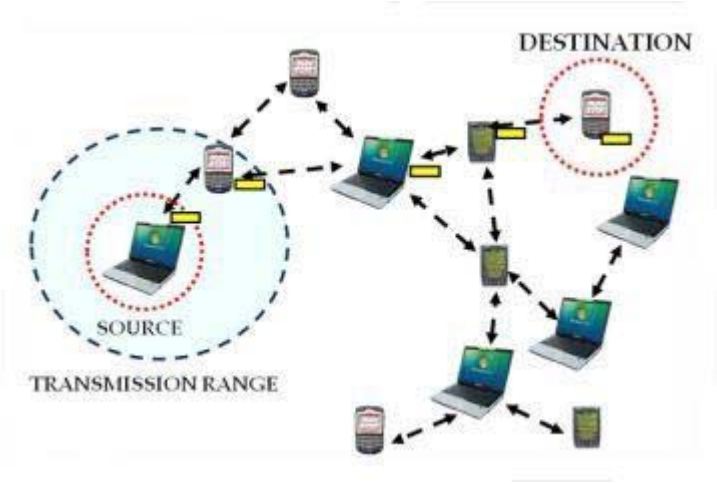


Fig.1. Mobile Ad hoc network.

- Lack of centralized node
- Scalability
- Limited power supply
- Adversary inside the Network
- Limited Resources
- Dynamic topology
- Bandwidth constraint
- No predefined Boundary

MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Various attacks on different layers of MANET are shown in the following figure.

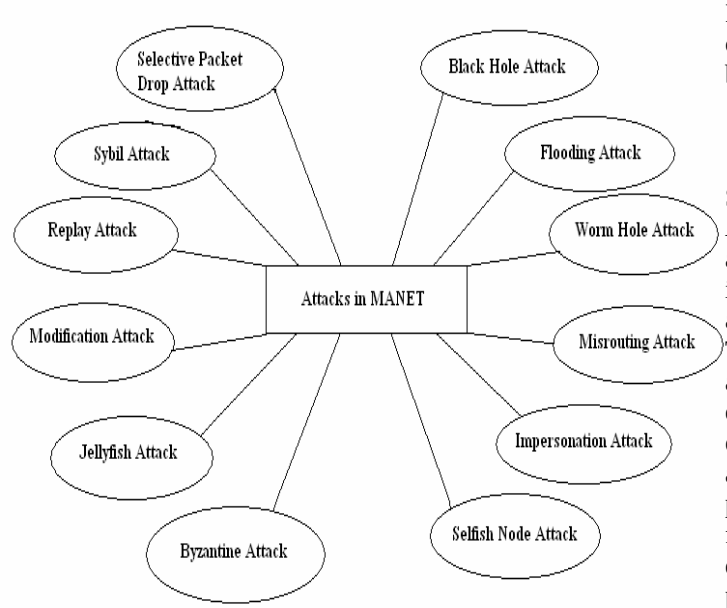
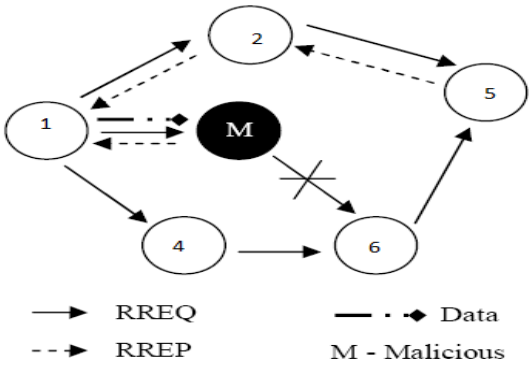


Fig.2. Different types of attacks in Mobile Ad hoc network.

II. BLACK HOLE ATTACK

In the following illustrated figure 2, imagine a malicious node M. When node 1 broadcasts a RREQ packet to nodes 2, 4 and M. All of these nodes receive this packet. Node M, being a malicious node, does not check up



F**ig.3.** Black Hole Attack

with its routing table for the requested route to node 5. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 1 Receives the RREP from M ahead of the RREP from 2 and 4. Node 1 assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node 1 sends data to M, it absorbs all the data and thus behaves like a Black hole [3].

III. BLACK HOLE ATTACK COUNTERMEASURES

In this section of the paper, we provides various countermeasures proposed in the literature to tackle with the black hole attack in mobile adhoc networks.

A. Fuzzy Logic

Sonal and Kiran Narang in their paper entitled "Black Hole Attack Detection using Fuzzy Logic" provides the solution against black hole attack by using fuzzy logic. This mechanism is responsible for identifying and mitigating the black hole node and provide solution to packet loss in mobile adhoc networks. Throughput is also increased by using this fuzzy based approach. The proposed algorithm provides efficiency against different parameters like end to end delay, energy consumption etc. The proposed algorithm provides the solution of packet loss and data rate against the black hole attack in network. The purposed work will firstly detect the black hole attack using the fuzzy logic. The fuzzy logic is implemented on packet loss and data rate at time of node communication. This algorithm provides the better solution [4].

B. Distributive Cooperative Mechanism

Chang Wu Yu, Wu T-K, Cheng RH and Shun chao chang in their paper entitled "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network " given a distributive cooperative mechanism for detecting black hole attack in MANETs. This mechanism consists of four steps (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. Simulation is done in NS-2 simulator. The Packet Delivery Ratio is improved by 64.14% to 92.93% when compared with AODV. Defect of this technique is a higher control overhead as compared to original AODV [5].

C. DRI Table Approach

H. Weerasinghe and Huirong Fu in their paper entitled "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation",

proposed a technique based on DRI table and cross checking scheme for detecting collaborative black hole attack in MANETs. In this mechanism AODV routing protocol is slightly modified by adding Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). In this technique if the source node (SN) does not have the route entry to the destination node, it will broadcast a RREQ message to discover a secure path to the destination node. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination node replies, all intermediate nodes update the routing entry for that destination. Source node also trusts on destination node and start to send data along the path that reply comes back. In this mechanism source node will also update the DRI table with all intermediate nodes between source and destination node. The algorithm is more efficient in terms of throughput, packet loss rate, end-to-end delay and control packet overhead as compared to AODV protocol [6,7].

D. Time Based Method

Tamilselven L and Sankaranarayanan in their paper entitled "Prevention of Black hole Attack in MANET" proposed a time based threshold mechanism for detecting and mitigating black hole attack in MANET. In this technique checking is performed to identify whether there is large difference between the sequence number of source nodes or intermediate node who has sent RREP or not. If there exists much more differences between source and destination sequence number, then it means the destination node is malicious node then that entry should be immediately eliminated from RR- Table. In this technique a node sends 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 time based mechanism for preventing black hole attack 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 [8].

E. Watchdog technique

Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre in their paper entitled "Black- Hole and Wormhole Attack in Routing Protocol AODV in MANET" proposed a Watchdog Mechanism for preventing from black hole and worm hole attacks in MANETs. This mechanism is used the concept of keeping track record of two table pending packet table and node rating table. Pending packet table is used to contain unique packet id, address of next hop to which packet will forward, address of destination node and expiry date and node rating table contains the record regarding 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 [9].

F. Strong node approach

Agrawal, P., Ghosh, R. K., and Das, S. K. in their paper entitled "Cooperative black and gray hole attacks in mobile ad hoc networks" give a strong node mechanism for detection and prevention of MANETs from black hole attack. Strong nodes are some special nodes which help the source and destination nodes to find out black hole attack in MANETs. These strong nodes are able to tuning its antenna to large ranges and short ranges. These strong nodes are responsible for end-to-end inspection and secure communication from source to destination nodes and can also recognize whether the data packets have reached the destination or not. If there is any differences occured in number of messages sent from source and reached at destination then strong nodes will inquire the nodes in their areas regarding to monitoring results of each node's performance. If the inspection results show misbehavior then protocol detects the black hole attack in the MANET. At the end this approach announces malicious node to the network by sending messages to all nodes. Advantage of this approach for mitigating black hole attack is that it decrease the no. of monitoring nodes in the network, only some nodes present in particular range are responsible for monitoring. Drawback of this approach is that as there is no fixed boundary for detection of malicious node in MANET, so some times this mechanism will not give the best results and another drawback is that difference between signal strength of strong and normal nodes make it unsuitable for MANET [10].

G. Abm (anti-blackhole mechanism)

Ming-Yang Su in their paper entitled "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" provides the anti black hole mechanism for mitigating black hole attack in MANET. In this approach different IDS nodes are used for performing ABM (Anti-Blackhole Mechanism). These nodes estimate the suspicious value of different nodes in the MANET based on the difference between RREQs and RREPs transmitted from the node. In this technique if an intermediate node never broadcasts a RREQ for a specific route and always forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node in the SN table exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network for isolating the suspicious node. Drawbacks of this technique is

that IDS nodes are specially located within each others transmission range, which is not always feasible in normal case [11].

IV. CONCLUSION AND FUTURE WORK

Due to continue growth of mobile adhoc networks, the need for more effective security mechanisms is also increasing. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of mobile adhoc networks. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have given number of techniques for detection of black hole attack. In this paper different countermeasures proposed for tackling with black hole attack are discussed. The state-of the-art routing methods of existing solutions are categorized and discussed. Novel, efficient, and robust techniques for dealing with black hole attack is still a great challenge and need of the time. This paper will benefit more researchers to realize the current status rapidly.

V. ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing opportunity to conduct this research work.

REFERENCES

[1] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", "International Journal of Multidisciplinary and Current Research", Volume 2, Jan-Feb, 2014, ISSN: 2321-3124.

[2] Jatinder Singh, Lakhwinder Kaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", "International Arab Journal of Information Technology", Volume 9, No. 3, May 2012 and ISSN: 1683-3198.

[3] P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", "IEEE International Conference on Trust, Security and Privacy in Computing and Communications", 2012.

[4] Sonal, Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic", "International Journal of Science and Research (IJSR)", Volume 2 Issue 8, August 2013, India Online ISSN: 2319-7064.

[5] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[6] Hesiri Weerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Intenation Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.

[7] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, " Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 2326 June 2003

[8] Tamilselven L and Sankaranarayanan, "Prevention of Black hole Attack in MANET" International Conference on wireless Broadband and Ultra Wideband Communications, 27-30 August 2007.

[9] 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.

[10] Agrawal, P., Ghosh, R. K., and Das, S. K. 2008. "Cooperative black and gray hole attacks in mobile ad hoc networks". In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 310-314.

[11] Ming-Yang Su," Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Elsevier, Computer Communications 34 (2011) 107–117

[12] Jaisankar N, Saravanan R, Swamy KD (2010) A Novel Security Approach for Detecting Black Hole Attack in MANET. Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010.

[13] Yang, H., Shu, J., Meng, X., and Lu, S. 2006. SCAN: "Self-organized network-layer security in mobile ad hoc networks", J. IEEE Selected Areas in Comm. Vol. 24, No. 2 (Feb. 2006), 261-273.

[14] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[15] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[16] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions", IEEE Wireless Communications. 11 (1), pp. 38-47, 2004.