International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
*International Conference "*INTELINC 18*", 12th & 13th October 2018*

Survey on black hole attack with Time period analysis in the AODV routing protocol in MANET

S.G.Rameshkumar[1], Dr.G.Mohan[2]
Assistant professor[1], Professor[2]
Department of Electrical Engineering, Faculty of Engineering and Technology, Annamalai University, Chidambaram[1,2]

Abstract: Malicious nodes attacks based loss of packets during the transmission is the vital problem in the mobile ad-hoc networks. Errors during the transmission, broken links, unidentified routes to the destination and malicious nodes attacks are the main reasons for loss of packets. Identify the specific reason of packet loss in the adhoc networks is the tedious task. Black hole attacks is the one of vital attack performed by the malicious node attacks to loss the packets in the network. Timeout period is one of the important technique to detect the malicious nodes that make black hole attack in the multihop network. This survey paper analyse the packet loss problem and black hole attack in the Ad-hoc distance vector routing protocol in the MANET.

Index Terms: Packet Loss, AODV, Timeout period, single black hole, cooperative black hole attack

I. INTRODUCTION

MANET is a multi-hop dynamic and transitory communication network of mobile nodes in the wireless network without any infrastructure. Multi-hop links helps to establish the communication between the nodes in the Ad-hoc networks based on routers and hosts. MANET helps to communicate in natural disaster zone, defence zone and mobile network[1].

In MANET, all the links established between the mobile nodes through wireless medium. The MANET faces various issues like security threats, finite bandwidth for transmission, dynamic establishment for links, abusive broad casting messages. There are many security threats like replication of packets, denial of service based attacks, overflow in the routing table, black hole attack, grey hole and also warm hole attacks [2].

Fig.1. Infrastructure of MANET

II. ROUTING PROTOCOL

Routing protocols are classified as proactive, reactive and hybrid.

The proactive routing protocols are table driven. Each node maintains their own routing table with neighbouring nodes and number of hops details. Every node periodically broadcast their routing information to its adjacent nodes. Destination sequenced distance vector routing and Optimized link state routing protocols are fall under proactive routing protocol category.

Adhoc on-demand distance vector and dynamic source routing protocols are fall under reactive routing protocol category. In AODV, each node maintains the next hop and routing path in its routing table. In DSR, each node

maintains their route cache from the source node to destination node. Routing path is recorded in the route cache.

The hybrid routing protocol combines the features of the proactive and reactive routing protocols. Temporally ordered routing algorithm and zone routing protocol are fall under the hybrid routing protocol category.

III. BLACK HOLE ATTACK

There are various types of attacks in MANET like black hole, gray hole, jelly fish, worm hole, blackmail, sybil, etc.,

Single / Cooperative black hole attacks are occurred based on the malicious nodes and it drops the received packets without forwarding [3].

In reactive routing protocols, at the time of route establishment, malicious node sends optimized paths to the node falsely. In the proactive routing protocols, malicious node sends the optimised paths as route update messages. Malicious node sends the shortest route information to the destination node and controls the packets which are passed between malicious nodes during the time of route request received from the destination node. It leads to the destination node is unreachable.

.

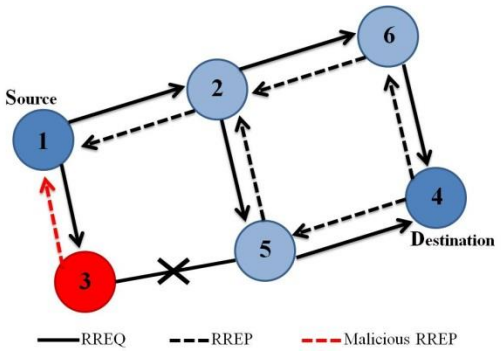

Fig. 2: Black Hole Attack

In the AODV protocol, the attacker node sends a fake route reply to the source node when it received a request for the route to the destination node and allows the source node to select the route which one have that attacker node is an intermediate node. It makes the attacker node to discard or misuse the route and also traffic.

In the cooperative black hole [4], more than one black hole nodes acted together and generate fake routes. The figure 3 shows the node 1, node 4 and node 4 are black hole nodes that are synchronized with each other.

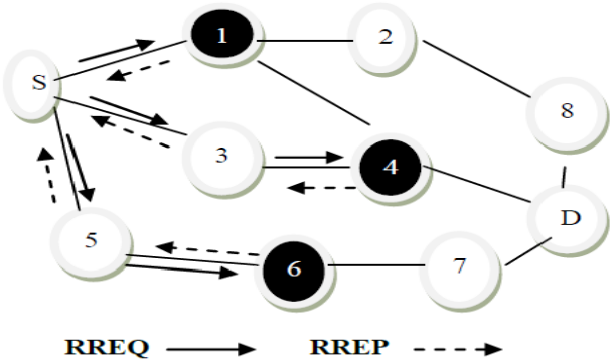

Fig.3. Cooperative black hole attack

IV. RELATED WORK

Bo Sun et al. [5] use the neighbourhood-based and routing recovery scheme in AODV. This detection scheme recognizes the black hole attack and protocol for the route recovery built the correct path. It helps to find out the nodes which are unavailable in the path and source node request the destination node to reconfigure the path. In this scheme, routing overhead is not increase but fails at the time of attackers collaborate to copy the fake reply packets.

Mohammad Al-Shurman et al [6] proposed redundant route method to avoid the black hole attacks. In this method, source node sent route request to the destination node and receives route replies to find the more than one route.

The unique sequence number scheme is also proposed by the author. In this solution, sequence numbers of the last packet sent and last packet received to every node to be recorded in two additional tables. At the time of packets received in the node or sent from the node, these two tables will be updated automatically. This two table value used to the sender to identify the node is malicious or normal.

Latha Tamilselvan et al [7] propose a time based threshold detection scheme with modified AODV routing protocol. The RimerExpiredTable is used to set the timer to collect the neighbouring node's request after receiving the first request. In the modified AODV, packet sequence number and its received time stored in the collect route reply table. Received time is used to find the timeout value and identify the route based on the threshold value. This proposed method produces high packet delivery ratio and fails in end to end delay at the time of malicious node is away from the source node.

Djamel Djenouri et al. propose random two hop ACK scheme to monitor and Bayesian detection scheme to detect the black hole attack and isolate the black hole attack nodes in MANET. The simulation results shows higher true detection rate than the existing watchdog approach [8].

William Kozma Jr. et al. propose a reactive misbehaviour detection scheme with audit phase, search phase and identification phase. In this scheme, destination node sends the feedback to the source node at the time of high packet drop ratio is recognized. After that, source node selects the audit node with bloom filter to generates a behavioural proof and identifies the malicious node. Binary search method used to find the malicious node with audit node's data. This detection scheme is automatically triggered at the time of performance is drop away between source and destination nodes [9].

N. Jaisankar et al. recommended a next hop information approach to detect the black hole attacks. It consists detection phase and reaction phase. In the detection phase, next hop information is appended to the RREP packet and updating the black identification table in all nodes. Route reply packet is scrutinized between the intermediate and destination nodes and identifies the black hole nodes. In the reaction phase, identified black hole node is separated from the route. Id of the separated black hole node is added in the remaining node's isolation table. In this next hop information approach, ratio of the packet delivery ratio is increased and ratio of packet drop is decreased [10].

Harsh Pratap Singh, Rashmi Singh [11] evaluates the internal and external clocks nodes to detect the black hole nodes. Threshold clock is used for this evaluation. Broadcast synchronization and relative distance are used to synchronize the clocks.

Sukla Banerjee [12] replaces the transmission of total data traffic with small blocks from the source to destination. Each small sized blocks are verified in both sides and identified the malicious nodes are found in the route. Before sending blocks, source sends the alert message about data block to the destination node. This strategy detects and removes the cooperative black and gray-hole attacks. More time required to convert the total traffic data into small data blocks.

Zhao Min and Zhou Jiliu [13] suggest a two techniques using hash-based authentication mechanism are message authentication code and the pseudo random function. First technique verifies and approves the messages and second one identifies the groups. Collaborative mistrustful nodes are identified and find the new routing path without cooperative black hole attacks.

Chang Wu Yu et al. [14] find and remove the collaborative black hole attacks using local data gathering, location detection of the nodes, cooperative black hole detection and global reply.

Chatzimisios et al. [15] proposed an analytical model using a Markov chain to compute and analyse the functions of packets such as the transmission delay of the packets, time and probability of the packet drops of the IEEE 802.11 protocol and also introduces packet limit and retry based performance analysis scheme.

VahidHeydari [16] introduces two analytical models to find the optimum timeout period for the malicious node detection in adhoc networks for DSR protocol. Queuing analysis is used to find the mean and maximum delay in

every hop and other analytical model is used to define the mean number of hops.

Tickoo and Sikdar [17] developed an analytical model for evaluating the queuing delays at nodes over a single hop in IEEE 802.11 MAC based wireless network. Their model can support arbitrary arrival patterns, packet size distributions and number of nodes. One key observation in their analysis is that the primary contributor to the delay is the channel access and reservation time associated with each packet transmission.

V. CONCLUSION AND FUTURE WORK

This study reveals that the black hole attack is the crucial threat and identifies the vulnerabilities in packet delivery, routing overhead and end-to-end delay. Various techniques and approaches are observed in this study to detect the single or cooperative black hole nodes. After studying all the approaches examines that the most of the approaches has low packet delivery ratio and also high overhead. In future work, develop such approach which can efficiently minimize all these constraints.

REFERENCES

[1] Burbank JL, Chimento PF, Haberman BK, Kasch WT, "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology". IEEE Communications Magazine archive. Volume 44 Issue 11, November 2006. Page 39-45

[2] Sarma N, Nandi S, "Service differentiation using priority-based MAC protocol in MANETs". International Journal of Internet Protocol Technology archive, Volume 5 Issue 3, September 2010, Pages 115-131

[3] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine,Volume: 40 , Issue: 10 , Oct 2002

[4] MamtaSengar, PawanPrakash Singh, Savita Shiwani3, "Detection of Black Hole Attack In MANET Using FBC Technique", International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 2, March – April 2013

[5] Sun B, Guan Y, Chen J, Pooch UW, "Detecting Black-hole Attack in Mobile Ad Hoc Networks", European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003

[6] Al-Shurman M, Yoo S-M, Park , "Black Hole Attack in Mobile Ad Hoc Networks", 42nd Annual ACM Southeast Regional Conference, 2-3 April 2004

[7] Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007

[8] Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6

[9] Kozma W, Lazos L, "REAct: Resource-Efficient Accountability for Node Misbehaviour in Ad Hoc Networks based on Random Audits", ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009

[10] Jaisankar N, Saravanan R, Swamy KD, "A Novel Security Approach for Detecting Black Hole Attack in MANET", International Conference on Recent Trends in Business Administration and Information Processing, India, 26-27 March 2010

[11] Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol", International Conference on Electronics and Communication Systems, 2014 , DOI: 10.1109/ECS.2014.6892653

[12] Sukla Banerjee "Detection/Removal of Cooperative Black & GrayHole Attack in MANETs" in proceedings of the World Congress on Engineering & Computer Science 2008.

[13] Min Z, Jiliu Z, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", International Symposium on Information Engineering and Electronic Commerce, DOI: 10.1109/IEEC.2009.12

[14] Yu CW, Wu T-K, Cheng RH, Chang SC, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in Knowledge Discovery and Data Mining pp 538-549

[15] P. Chatzimisios, A. C. Boucouvalas, V. Vitsas, "IEEE 802.11 packet delay—A finite retry limit analysis", GLOBECOM '03, pages 950–954, 2003.

[16] VahidHeydari, Seong-Moo Yoo, "Timeout Period Analysis to Detect Black Hole Attack in Multihop Wireless Ad Hoc Networks", International Journal of Wireless Information Networks 25(7):1-15 · September 2017

[17] O. Tickoo, B. Sikdar, "Queuing analysis and delay mitigation in IEEE 802.11 random access MAC based wireless networks", In Proceedings of INFOCOM, pages 1404–1413