www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9547-9551

A Review Paper on Collaborative Black Hole Attack in MANET

Barleen Shinh[1], Manwinder Singh[2]
Rayat Institute of Engineering and Information Technology
Rail Majra Distt. Nawanshar,
Punjab 143001

Abstract: Ad-hoc networks have become a new standard of wireless communication in infrastructure less environment. MANET is a Mobile Ad-hoc Network in which the nodes get connected with each other without an access point. Messages are exchanged and relayed between nodes. Routing algorithms are utilized for forwarding packets between indirect nodes i.e not in direct range with aid of intermediate nodes. They are spontaneous in nature and absence of centralized system makes them susceptible to various attacks. Black hole attack is one such attack in which a malicious node advertises itself as the best route to the destination node and hinders the normal services provided by the network.

Keywords: Mobile Ad Hoc network, Single Black hole attack, Collaborative Black Hole Attack

1. Introduction

A MANET consists of wireless hosts that can be arbitrarily deployed as a multi-hop packet radio network in absence of any infrastructure or centralized system. Some characteristics of MANETs are

unreliable wireless media links used for communication between nodes, dynamic network topologies, restraint battery, lifetime of the network, bandwidth and computation power of nodes [1]. MANETs are prone to various types of active and passive attacks. Active attacks are categorized into Interception, interruption, fabrication and modification attacks. A passive attacker does not interrupt with the operation of a routing protocol but puts efforts to gather the vital information from packets. MANET has proactive, reactive and hybrid routing protocols [2]. In proactive protocols the routes to all parts of the network or the destinations is determined at the starting time and a route update table is maintained periodically. Some popular protocols are Destination Sequence Distance Vector (DSDV) and Wireless Routing Protocol (WRP). In reactive protocols the route discovery process is carried out for establishing the routes as and when required. Mostly used protocols are Ad-hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) [3]. Hybrid protocols Employ a hierarchical strategy these protocols adhere to combination of properties of both proactive and reactive protocol. The most widely used protocols are Ad hoc on-demand distance vector (AODV) routing protocol and Dynamic

Source Routing Protocol (DSR). It is a source initiated on-demand routing protocol [4]. However, DSR is vulnerable to the well known black hole attack.

A. Black Hole Attack in MANET

MANETs are vulnerable to various attacks. General attack types are on the layers that function for the routing mechanism of the network. Attacks have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. In black hole attack a malicious node stops forwarding the data packets [5]. As a result, when the malicious node is selected as a route, it denies the communication to take place. In DSR the malicious node waits for the neighbors to initiate a RREQ packet as shown in figure 1. As the node A receives the RREQ packet from source node S, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node A. The malicious node takes all the routes towards itself. It does not allow forwarding of packets to the required node C as seen in the anywhere [6]. Thus the packets attracted by the black hole node will not reach the destination.

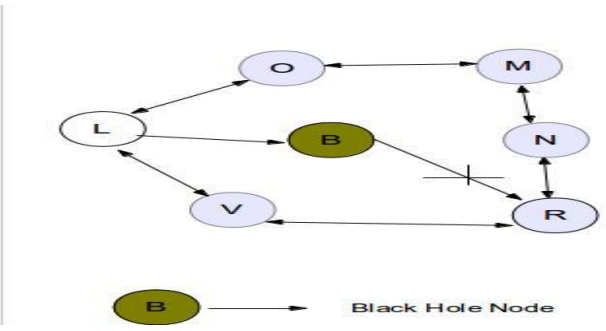
Figure 1 Black Hole Attack in MANET

2. Literature Review

[1] Dr. E. Karthikeyan et al, proposed a secured strategy of issuing a digital security certificate to nodes present in the network. The proposed method utilizes DSR protocol. It is an efficient method of detecting and eradicating black hole nodes or malicious in the MANET. By incorporating digital security certificate the memory overhead can be reduced. The certificate can be added to the routing table in routing cache of DSR. Frequent refreshment of routing cache drastically reduces the need of memory overhead.

[2] Shinni Mittal and Harish Taluja, had proposed solution that is an improvement of the ABDSR routing protocol, which can prevent co-operative black holes. We present a mechanism to identify multiple black holes cooperating with each other and a solution to discover a secure and optimum route avoiding cooperative black hole attack. In their approach all nodes participated in communication to fight against the Black hole attack is to make use of a "Reputation Table" where in every participating node will be assigned a reputation level that acts as a measure of trustworthiness. If the level falls below defined threshold or 0, it is considered to be a malicious node, termed as a Black hole and it is eliminated.

[3] Dr. A. Rajaram et al, proposed a solution Energy Based Routing Algorithm (EBRA) to



reduce the energy consumption of the node. The energy consumed takes in account three factors like mobility of the node, malicious behavior of the node. In ad hoc networks, node can move randomly. No infrastructure is required. While increasing the movement of the node, the node mobility increases which leads to higher energy consumption and therefore a threshold limit is added .

[4] Pradeep Kumar Sharma et al, proposed a centralized system with MANET then it prevent the attacks. It is a type of network where all users get connected to a main server which plys role of important agent for all transmissions and receptions. The server acts like a database for storing information about the users and all the communications occurring between the nodes. Instant message sending and receiving require main server-structure like these. Also called centralized server-structure. Black Hole attacks are more vulnerable than Gray Hole attacks because the packet drop ratio is high for Black Hole attacks compared to Gray Hole attacks, not only that the normalized routing load also increases in the presence of Black Hole attacks compared to Gray Hole attacks.

[5] S. P. Manikandan, R. Manimegalai, proposed a trust based routing mechanism called Trust Correlation Service to prevent black hole attack in Mobile ad hoc Networks (MANETs). The data collected by this mechanism is distributed among the nodes involved in the wireless network. Trust earned by a node and correlation score for different nodes is calculated before route establishment for transmission and reception of packets between source and destination. The trustworthiness of a node is computed based on factors like reputation of a node, its prevention against various attacks and unauthorized usage of resources. The correlation score for nodes is calculated based on the trust needed and total number of packets transmitted by source node and received by destination node.

[6] Chander Diwaker, Sunita Choudhary, proposed a technique of identifying and isolating black hole attack by eradicating the disadvantages of DBA-DSR algorithm. DBA-DSR is enhanced version of DSR protocol and detects malicious nodes with aid of fake Route request and Route Reply packet. This invites several disadvantages of this method, the main implies increased overhead packets due to sending of acknowledgement packets repeatedly to keep an eye on fake route reply packets generated from malicious nodes.

3. Conclusion and Future Scope

We conclude that multiple black hole attack is one of the devastating attack done on the network. Due to this attack packet loss may occur and delay increases. The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols. A study can be conducted on the relationship between the average detection delay and mobility of the nodes. More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained. A complete system can be designed to implement intruder identification. A complete approach can be developed that

considers more parameters such as the available queue length and the delay on a path during the route determination. In order to avoid traffic fluctuation, randomness can be introduced into route determination. A fast response mechanism (local repair) can be developed for reactive protocols to reduce packet drop due to route changes.

References

[1] Sevil Şen, John A. Clark, Juan E. Tapiador (2010), *"Security Threats in Mobile Ad Hoc Networks."* IEEE 2010.

[2] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer Richard, A. Kemmerer (2004), "AnIntrusion Detection Tool for AODV-based Ad hocWireless Networks" 2004.

[3] M.E.G, Moe, B.E. Helvik, S.J. Knapskog (2008), *"Trust Based Secure Mobile Ad-hoc Networks routing using HMMs"* Proceedings ACM Symposium on Qos and Security for Mobile Ad-hocNetwork, Vancouver, British Columbia, Canada, 27-28 October 2008, pp. 83-90. [3] Dokurer, S. Ert, Y.M, Acar, C.E (2007), *"Performance Analysis of Ad-Hoc Networks under Black Hole Attack."* Proceedings IEEE, pp. 148-153, 2007.

[4] Fei Wang, Yijun Mo, Benxiong Huang,"COSR: Cooperative on Demand Secure Route Protocol in
MANET", IEEE ISCIT, China, pp 890-893.

[5] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks," IEEE INFOCOM, San Francisco, CA, USA, Vol 3, pp 1987-1997.

[6] Chee wah Tan,"Enforcing cooperation in an adhoc Network using cost-credit based forwarding and Routing Approach", WCNC, IEEE, pp 2935-2939.

[7] Haiying Shen and Ze Li,"ARM: An Account-based Hierarchical Reputation Management System for Wireless Ad Hoc Networks ,The 28th International Conference on Distributed Computing Systems Workshops, IEEE, pp 370-375.

[8] A.V. Babu , Mukesh Kumar Singh "Node Isolation Probability of Wireless Adhoc Networks in Nagakami Fading Channel" International journal of computer networks and communications, Vol 2, pp 21-36.

[9] Qi He, Dapeng Wu, Pradeep Khosla,"SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", WCNC / IEEE Communications Society, Vol. 2, pp 825-830.

[10] D.Johnson,Y.Hu,D. Maltz,"The Dynamic Source Routing protocol (DSR) for Mobile Ad hoc
network", RFC 4728.

[11] S. Buchegger and J-Y. Le Boudec,"Performance Analysis of the CONFIDANT Protocol:Cooperation Of Nodes, Fairness In Dynamic Ad-hoc Networks", Proc. of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[12] Hameed Janzadeh, Kaveh Fayazbakhsh, bahador bakshi,"A secure credit-based cooperation stimulating mechanism for MANETs using hash chains", Future Generation Computer Systems -

Elsvier ,pp 926-934.

[13] Sonja Buchegger, Jean Yves Le Boundee, "Self - policing in Mobile Ad hoc Networks" In CRC

Press, Chapter Handbook on Mobile Computing.

[14] Rekha kaushik, Jyoti Singhai "Simulation Analysis of Node Misbehaviour in an Ad hoc

Network using NS2 " International journal of computer science and network security, Vol 8 , pp 179-182.