A SURVEY ON IMPROVING THE PERFORMANCE OF DSR PROTOCOL UNDER BLACKHOLE ATTACK IN MANET

G. Vennila* & D. Arivazhagan**
Department of Information Technology, AMET University, Chennai, Tamilnadu

Cite This Article: G. Vennila & D. Arivazhagan, "A Survey on Improving the Performance of DSR Protocol under Blackhole Attack in Manet", International Journal of Scientific Research and Modern Education, Volume 2, Issue 1, Page Number 175-177, 2017.

Abstract:

The Mobile Ad-hoc Network is a network in which the nodes can communicate with other nodes without infrastructure network. This network has exposed to handle different types of attacks. Black hole attack is one of the attack in which the node itself claim the fake RREP that has shortest distance to reach destination. In this way that the node drops the packets from sender and further, it will not forward the packets to any other node. Such type of node is known as malicious node. Most of the researchers are find feasible solution to improve the performance of routing protocol under this attack. This paper presents the analysis on improving the performance of DSR Protocol under black hole attack.

Key Words: MANET, Black Hole Attack, RREP & DSR

Introduction:

The Mobile Ad-hoc Network is an infrastructure-less network in which the nodes are moved anywhere in the network. Due to the dynamic nature, the networks are exposed to various kinds of attacks. One of the major kinds of attack is black hole attack. The malicious node makes use of fake RREP to drops the packet from the genuine node. There are two kinds of black hole attack: Single black hole attack and Co-operative black hole attack. In Single black hole attack, one node is work as a fake node that drops the packet and it is not forwarded to any other node in the network. In Co-operative black hole attack, more than one node together is work as fake nodes that drops the packets and not forwarded to any other node in the network. This paper analyze one of the routing attack known as black hole attack and also its focus to study the existing mechanism to detect , prevent the malicious attack and the analysis done by considering the following factors: Packet delivery ratio, Delay, Throughput. The paper is structured as follows section 2 describes the process of DSR Protocol, section 3 describes about black hole attack, section 4 explains various detection and prevention techniques of black hole attack.

DSR Protocol:

The DSR Protocol is an on-demand routing protocol used in MANET to maintains the routing information about each node present in the network. This Protocol has three mechanisms are Route Discovery, Route Reply and Data Transmission [11]. The process of DSR Protocol is depicted in Fig.1. If the source needs to send the packet to particular node, it establishes the path by route discovery mechanism. Then, the particular node is send Route reply to the source and the data is transferred from source to desired node in the given network.

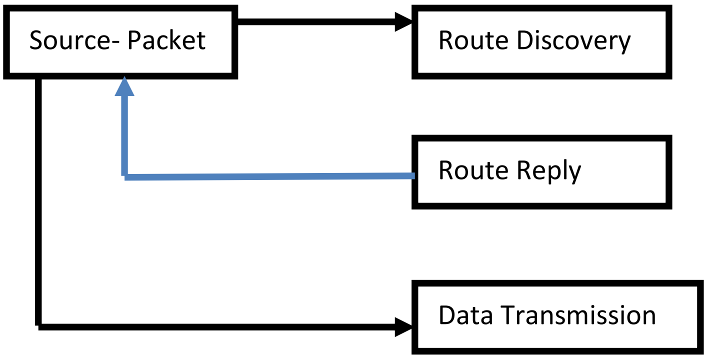

Figure 1: DSR Protocol Process

Black Hole Attack:

The black hole attack is a malicious attack use fake RREP to consumes the packet from source and drops to forward the packet to any other node. If the source node needs to send the packet to destination node, it sends RREQ to all the nodes (Node-A, Node-B and Malicious Node) in the network. Subsequently the malicious node sends RREP that has shortest path to reach destination to the source node. The source node gets the first RREP from the malicious node than the other nodes (Node- A, Node- B). Since the malicious node sets highest sequence number in RREP than the other nodes.

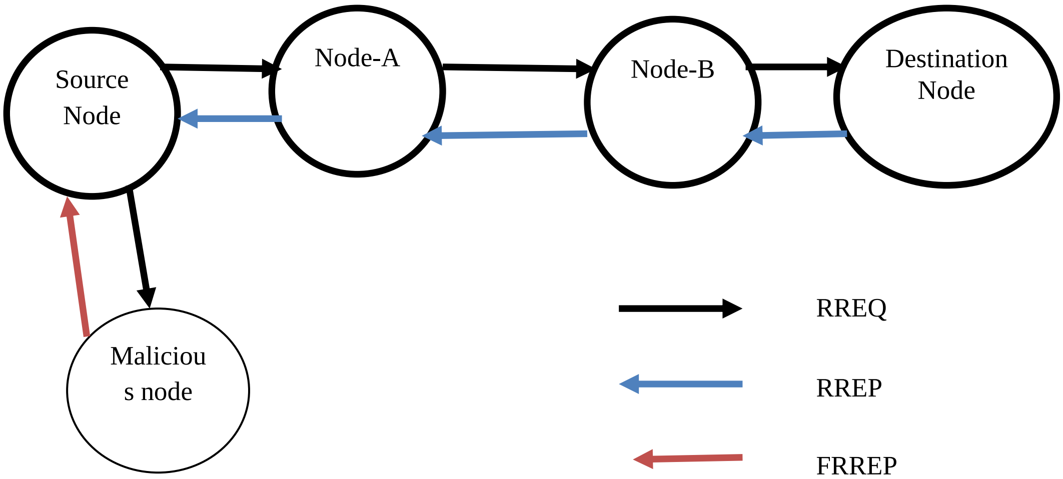

Figure 2: Black Hole Attack

Existing Detection & Prevention Techniques:

Most of the researchers have found a solution to the black hole attack in which some of the recent techniques are analyzed in this paper. These techniques can be classified as Credit based method, Reputation based method and acknowledgement based method [1].

Credit Based Method:

The credit based technique is to give incentive for nodes which truly perform networking functions. The payment system may be set up to achieve the same goal. The Nodes get paid for providing services to other nodes. When the node requests other nodes for packet forwarding, they use same payment system to send packet to other node. Credit based schemes have two models:

✓ The Packet Purse Model (PPM) and 2) The Packet Trade Model (PTM)[2]

Reputation Based Method:

This technique builds a metric for each node according to detect the black hole attack. The watchdog model was implemented in DSR protocol. It is only neighbor monitoring scheme to detect the malicious node. Pathrater describes a route without having malicious nodes or misbehaving nodes lying on the paths. This mechanism is satisfied for malicious nodes. The difficulty in watchdog model is not detect a black hole node in the presence of 1) Ambiguous collisions 2) Receiver collisions 3) Limited transmission power 4) False misbehavior 5) Partial dropping[3-5] use similar monitoring schemes but it propagates collected information to its nearby nodes and are exposed to false accusation attacks.

Acknowledgement Based Methods:

The Acknowledgment based methods ensures that the packet coming from destination or not. Liu et al [6] proposed 2ACK system where the nodes openly send acknowledgment to detect the node misbehavior. The major disadvantage in this 2ACK is that the acknowledgements overhead is increased and to reduce the same kind of problem, the improved 2ACK has been proposed by P. Samba Siva Rao et al [7], which depends on 2ACK and reduces the number of acknowledgments.

G. Vennila et al [8] proposed hash based technique to identify the selfish node in Mobile Ad-hoc Network. The proposed algorithm has four phases: Initialization phase, Hash generation at Destination, Hash generation at Source, Node Misbehavior Identification and Packet Forwarding phase. It uses the concept of hash function and implemented under the protocol DSR called as hash based DSR.

The hash based DSR gives better results compared with the original DSR. The results achieved from simulation testing implemented in MATLAB to study the effect of selfish nodes presents in the network and to evaluate the network performance in terms of throughput and delay. The result shows the better performance in terms of packet delivery ratio up to 70% and time delay has been reduced up to 80% compared to the existing Dynamic Source Routing (DSR) protocol

G. Vennila et al [9] proposed one cryptographic algorithm RSA and sequence number calculation to eliminate the black hole node. Initially, the two large prime numbers has been taken and calculate the d and e value. The RREQ is considered as M. The RREQ is encrypted at the sender side and it forwards the RREQ to the neighbor's node. If the node knows key value then the node can able to decrypt the RREQ and it generates RREP to the source. After receiving the RREP in source, it computes the threshold diff in which the RREP come from legitimate node or malicious node. Base on the threshold diff, it sends the packet from source to destination. If the difference of sequence value is below the threshold value, then the node is considered as legitimate node. Suppose, if the difference of Sequence number is greater than the threshold value, then the node is considered as malicious node.

Nitin Khanna et al [10] proposed one mechanism Trace route in which it sets a timer for Reverse trace. On receiving the Trace packet each intermediate hop forwards the trace and set the timer for Reverse trace. If the timer expires before the Reverse trace is received, then the node marks as Black hole node and send Reverse trace to source through previous nodes.

Trace route mechanism gets activated for the detection of source of Black hole attack and thus breaking the co-operation among them by marking one of the nodes involved in collaboration. The proposed solution shows higher control load for small values of parameters are mobility and node density. This is due to some fixed overhead caused due to enhancement in security of MANET and the use of Cryptography.

Conclusion:

The black hole attack is analyzed and its effects with Dynamic Source Routing Protocol. Further, its two type's single and co-operative black hole attacks are examined and also the existing detection, prevention techniques presented to improve the performance of black hole attack in Mobile Ad-hoc Network. In future, the efficient algorithm to be proposed to improve the performance of DSR protocol with the presence of more than one malicious node.

References:

1. Padiya S, Pandit R, Patel S. Survey of Innovated Techniques to Detect Selfish Nodes in MANET. International Journal of Computer Networking. 2013.
2. Koshti D, Kamoji S. Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks. IJSCE. 2011.
3. He Q, Wu D, Khosla P. Sori: A secure and objective reputation based incentive scheme for ad-hoc networks. WCNC; 2004. p. 825–30
4. Buchegger S, Boudec JL. Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks). Proceedings IEEE/ACM Workshop on (MobiHoc'02); 2002 Jun. p. 226–336.
5. Michiardi P, Molva R. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. CMS'02; 2002 Sep.
6. Liu K, Deng J, Varshney P, Balakrishnan K. An acknowledgment-based approach for the detection of routing misbehavior in manets. IEEE Transactions on Mobile Computing. 2006
7. Samba P, Aswini M, Kusuma T, Vasudha Y. Detection of Routing Misbehavior Nodes Using Improved 2-ACK in MANET'S (Simulation through NS-2). International Journal of Computer Science and Information Technologies. 2014; 5(2):1042–4.
8. G. Vennila, D. Arivazhagan, "Hash based Technique to Identify the Selfish Node in Mobile Ad-hoc Network", Indian Journal of Science and Technology, Vol 8(14), 70696, July 2015
9. G. Vennila, D. Arivazhagan, "Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm", International Journal of Engineering and Technology (IJET), Vol 6 No 5 Oct-Nov 2014.
10. Nitin Khanna, "Mitigation of Collaborative Blackhole Attack using Trace Route Mechanism with Enhancement in AODV Routing Protocol", International Journal of Future Generation Communication and Networking, Vol. 9, No. 1 (2016), pp. 157-166.
11. D. B. Jagannadha Rao, Karnam Sreenu, Parsi Kalpana, "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2012.