e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.529

Volume 9, Issue 3, March 2021

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A General Study of Black Hole Attack in MANET

Ashutosh Vashist
Research Scholar, PH.D (Computer Science),
Department of Computer Science.
School of Engg. & Tech.
Om sterling global University
Hisar (Haryana), India

Abstract: ***Mobile Ad hoc Network (MANET) is a type of wireless networks that provides numerous applications in different areas. Security of MANET had become one of the hottest topics in networks fields. The characteristics of the mobile ad hoc network (MANET), such as no need for infrastructure, high speed in setting up the network, and no need for centralized management, have led to the increased popularity and application of this network in various fields. Security is one of the essential aspects of MANETs. AODV is a reactive routing protocol that has no techniques to detect and neutralize the black-hole node in the network. In this paper we study the impact of presence of black hole node on MANET.***

Keywords: MANET ,BLACKHOLE, , Network, Security.

I. INTRODUCTION

Wireless communication network could be controlled by a central infrastructure that controls communication between nodes in the network, or it could be an infrastructure-less which is called Ad hoc Networks. Mobile Ad hoc Network (MANET) is an application of the Wireless Ad hoc Network (WANET) that connects mobile nodes to each other. In MANET, nodes do not rely on a central node to coordinate the communication or to carry data between them; instead of that, they work together to carry data between nodes that cannot reach each other directly. In other words, nodes may work as a bridge between the sender and the receiver node when sender and receiver are not in the same coverage. The mobility of the nodes leads to a dynamic changing in the network topology. MANET routing protocols are designed to be adaptive to any dynamic topology changes.[i] A MANET is a network without infrastructure and a self configured network of mobile devices that are connected wirelessly. Each device in a MANET has complete independence and freedom to move in any direction; therefore in many cases, the connection between each mobile device and other devices is changing. Without the need for a fixed communication infrastructure to create a dynamic network, the importance of MANETs in applications such as military battlefield communications, relief and emergency operations, environmental protection, taxi networks, and independent space communications is increasing. Growing demand for MANETs has raised many concerns about security issues, especially for sensitive security applications. Unlike wired networks, MANETs are inherently insecure due to shared wireless media and the lack of any central control. The unique characteristics of MANETs have created new challenges for security design.[ii]

II. RELATED WORK

In the proposed system depends on a special type of nodes that is called guard nodes, which help in detecting black-hole nodes in the network. Guard nodes are nodes that are in the promiscuous mode that check the behavior of other nodes in the network. Guard nodes contain tables that record the behavior of the nodes in the network. Each node has a trust value that is determined according to its behavior in the network, and it decreases when the node only sends RREP and does not send RREQ. If the trust value of a node decreases below the determined threshold, then it is blocked or isolated. Guard nodes broadcast an

alarm to all adjacent nodes when a black-hole node is detected. The limitations of this system are that it needs a special type of nodes (guard nodes) and a huge number of guard nodes to cover all the network; also this system has a high overhead because of having many tables.[iii]

In this attack [19-21] a malicious node may advertise a good path to a destination during routing process. The intention of the node may be to hinder the path finding process or interpret the packet being sent to destination. Alternatively black-hole scenario may be defined as the one in which the cannel properties tend to be asymmetric i.e. the signal strength in both direction may not be same. In this case a node which receives the data packet but does not forward it is termed as black hole.

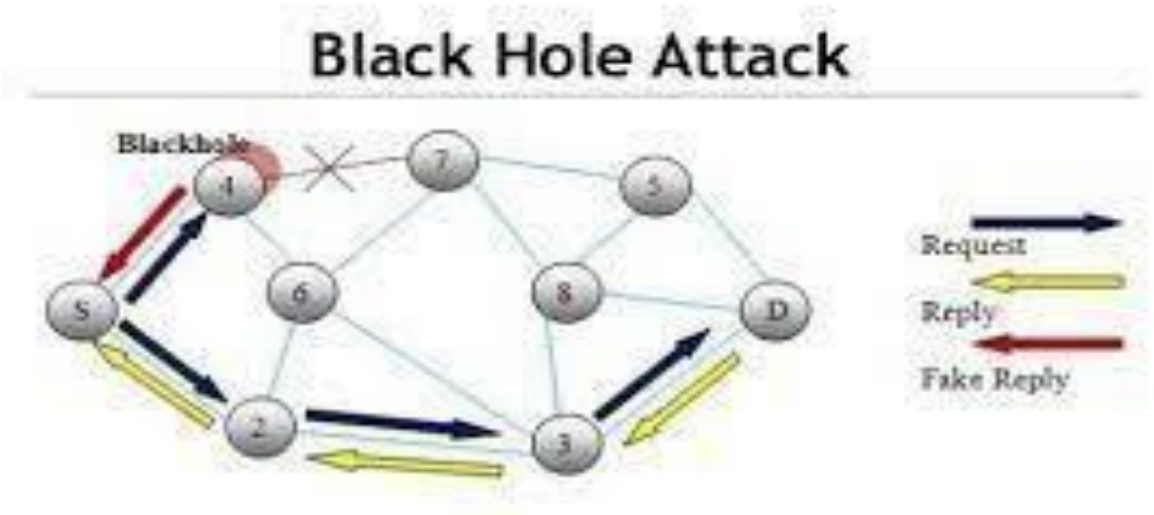
In either case the normal operation of the MANET is disrupted.[iv]

S. Dourker et al performed a performance analysis of ad hoc networks in the presence of the black hole nodes. In this they studied the effects of black hole attacks on the network performance. For this purpose the study was carried out on the packet loss with and without a black hole node using simulator NS-2. A solution was also proposed by them in order to minimize the effect of black hole attacks. This solution improved the network performance in the presence of a black hole by about 19%.[v]

Okoli Adaobi et al worked to find the impact of black hole attack on the performance of MANET and also found the impact of position of black hole node. According to them under the on-demand routing protocol, the closer a malicious node is to the source of traffic, the greater the extent of damage inflicted on the networks.[vi]

III. Black Hole

Blackhole Attack Overview AODV is not provided with protection mechanisms because the primary purpose of this protocol is to quickly deliver packets to the destination. This protocol assumes that all nodes in its network are normal nodes and not contain malicious nodes. These the main reasons which made the protocol vulnerable to many attacks for example (blackhole attack and warm hole attack). The blackhole attack is a type of denial of service attack where the malicious nodes send a fake reply to the source that contains it has a valid path and also the highest sequence number path to the destination.[vii] One of the main disadvantages of the black hole attack is to reduce network performance because it deletes the packets that are attached to it. In the black hole attack, if it found a single malicious node, it called a single blackhole attack. The presence of more than a malicious node in the AODV network called a collaborative black hole attack.[viii] In the blackhole attack, malicious nodes generate a fake RREP with a higher sequence number value, then send it to the nearest intermediate node and then forward it to the source nodes. The source will use the proposed path from the malicious node as the best and shortest path to the destination. When the data packet reaches the malicious node it drops and deletes it then does not reach it to the desired destination.



[ix]

IV. Simulation

For the purpose of simulation modification is done to the existing AODV routing protocol according to our proposed routing methodology and compared with the basic AODV routing protocol. The simulation carried out using the network simulator NS-2.35.

V. Conclusion

MANET networks are networks with a dynamic topology that comes with a lot of security and attacks issues. One of the major attacks is the Black Hole Attack that exploits the used routing protocol to harm the normal operations of the network. Every day a new detection and prevention schemes are being proposed by researchers over the world to overcome this problem. By detecting this attack or at least mitigate the negative effect of it, we will help in preserving good and secure networks for exchanging knowledge and experiences around the world.

References

[i] S. Mirza and S. Z. Bakshi, “Introduction to MANET,” International Research Journal of Engineering and Technology, vol. 5, no. 1, pp. 17–20, 2018.

[ii] F. R. Yu and H. Tang, “Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks,” Wireless Networks, vol. 16, no. 8, pp. 2169–2178, 2010

[iii] A. R. Rajeswari, K. Kulothungan, and A. Kannan, “GNBAODV: guard node based –aodv to mitigate black hole attack in MANET,” International Journal of Scientifc Research in Science, Engineering and Technology, vol. 2, no. 6, pp. 671–677, 2016.

[iv] Shailender Gupta, C. K. Nagpal and Charu Singla,"IMPACT OF SELFISH NODE CONCENTRATION IN MANETS",International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[v] S. Dokurer, Y. M. Ert , C. E. Acar,‖ Performance analysis of ad-hoc networks under black hole attacks‖, SoutheastCon, 2007. Proceedings. IEEE

[vi] Okoli Adaobi, Ejiro Igbesoko, Mona Ghassemian,‖ Evaluation of Security Problems and Intrusion Detection Systems for Routing Attacks in Wireless Self-Organised Networks‖, New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on 7-10 May 2012. [vii] M. Salehi, A. Boukerche and A. Darehshoorzadeh, “Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks,” Ad Hoc Networks, Vol.50, pp.88-101, 2016

[viii] S. Ali, “Enhanced Virtual Private Network Authenticated Ad Hoc on Demand Distance Vector Routing,” International Journal of Innovative Engineering and Management Research, Vol.7, Issue.12, pp.190-197, 2018

[ix] https://www.google.com/search?q=black+hole+in+manet&rlz=1C1VDKB_enIN987IN987&source=lnms&tbm=is ch&sa=X&ved

