INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue2)

Available online at www.ijariit.com

Review On Jelly Fish Detection and Prevention Schemes in MANETS

Sukhpal Kaur
Guru Kashi University, Bathinda, Punjab
sukhpal948@gmail.com

Dr. Rajinder Singh
Guru Kashi University, Bathinda, Punjab
rajneel2807@gmail.com

Abstract: The Mobile ad Hoc Networks work for number of applications in the present times. Some of the uses require quick transmission of the data from an emergency disaster prone area to the help centers. If the objective of least end to end delay between the transmissions is defeated for the delay sensitive applications, then it could lead to more harm. Jelly Fish attack is one such kind of many possible attacks leading to the delay in the transmission of the packets. This paper reflects the idea of jelly fish attack and various techniques concerning its identification and prevention.

Keywords: Mobile Ad Hoc Networks, Jelly Fish, End To End Delay.

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless frameworks. MANETs include mobile nodes that are allowed to move done in the network. Nodes are the gadgets that are mobile and that take an interest in the networks, for example, mobile telephone, portable PC, individual computerized help, MP3 player and PC. These nodes can go about as host/switch or both all the while. They can structure self-emphatic topologies depending upon their availability with each other in the framework. These nodes are able to arrange themselves and because of this interesting capacity, they can be conveyed earnestly without the need of any foundation. Web Engineering Task Force (IETF) has MANET working gathering (WG) that is given for creating IP routing conventions. Routing conventions is one of the testing and entrancing examination zones. Various routing traditions have been made for MANETs i.e. AODV, OLSR, DSR and so on.

The first step towards developing good security solutions is to understand possible form of attacks. Security of communication in MANET is critical for secure transmission of information. Due to the absence of any central co-ordination mechanism and the presence of shared wireless medium, MANET becomes more vulnerable to digital/cyber-attacks than wired network. The attacks could be classified on the groundwork of the origin of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This study describes the Jelly Fish attack in section II. The brief study about the past techniques for the prevention and detection of these attacks has been described in section III and the paper concludes with the conclusion in the section IV.

II. JELLY FISH ATTACK

Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network. Applications such as HTTP, FTP and video conferencing are provided by TCP and UDP. Jelly fish attack disturbs the performance of both protocols. It is same as black hole attack but the difference is that the black hole attacker node drops all the data packets but jelly fish attacker node produces delay during forwarding packets. Jelly fish attack is categorized as Jelly fish reorder attack, JF periodic dropping attack and JF delay variance attack. Jelly fish attacks are targeted against closed loop flows. TCP has well known vulnerabilities to delay, drop and mis-order the packets. Due to this node can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obey protocol rules; hence this attack is called as passive attack [8].

III. LITERATURE REVIEW

Mohammad et.al. [2012] proposed effect of JF Delay Variance attack on MANET using AODV as a routing protocol. Effect is calculated with respect to some network parameters like throughput, end- to- end delay etc. It is watched that MANET is flexible up to 10% of JellyFish (JF) attackers. They don't have any hard effect on the execution of network. For attackers over 10% and below 20% execution is influenced with a normal rate yet for 20% or over 20% execution of network turns out to be more regrettable MANETs are susceptible to different attacks. Out of which DoS are most perilous and exceptionally hard to recognize and defend. Jellyfish is another DoS attack sorted as JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack. In JF delay variance attack, a JF aggressor node interrupts into forwarding packets and delays information packets for some measure of time before forwarding. Because of this attack, top of the line to-end delay is presented in the network bringing about low execution (i.e. throughput) [1].

Amandeep Kaur et. al., [2013] concentrates on the impacts of jellyfish attack on MANET's routing protocols. Here four protocols AODV, DSR, TORA and GRP are utilized. Execution of the network has been evaluated in terms of Data dropped, Data dropped, Load, Retransmission attempts. [2].

Sanjay Kumar [2016] proposed an answer for the JellyFish delay variance attack in AODV protocol for MANETs. The JellyFish attack is a DOS attack that is difficult to recognize. It makes delay of information packets, before their transmission and gathering in the network. In this paper, they propose an answer for the JellyFish delay variance attack in specially appointed on AODV protocol for MANETs. [3].

Sakshi et. al., [2017] implemented Jellyfish DOS attack on AODV and proposed a JFDV identification calculation that investigates packet delaying trouble making of nodes and identifies various JFDV attacker nodes. It lessens normal end-to-end delay and builds throughput by re-routing information packets through backup route of action comprising of non-malicious nodes. The uses of the security strategies of wired networks, for example, get to control and verification have been unsatisfactory to remote networks because of the exceptional components of such networks, for example, dynamic evolving topology, no brought together control and so on. Thus, accomplishing security objectives for MANET has increased critical consideration of the scholarly community and research group as of late. Jellyfish attack is one of the genuine directing attacks among all the network layer attacks on MANET. [4].

Sapna et. al., [2015] modifies the current TCP and AODV network to deal with the jellyfish periodic dropping attack and the jellyfish delay variance attack. The proposed network adjusts the AODV routing protocol and TCP to deal with the jellyfish attack variations. The proposed network utilizes the E_TCP of the current network alongside the changed AODV routing to get the compelling outcomes. The proposed procedure utilizes the forwarding rate and the delay check to upgrade the execution of the protocol. The forwarding rate is determined by number of packets divided by number of packets sent. The node with forwarding rate under 0.70 i.e. 70% is disposed of and the coming packet transmission is utilized to figure the normal delay. The packet that doesn't achieve the goal of the normal delay time than the packet is disposed of**.** [5].

Hepikumar et. al., [2013] give review on jellyfish attack. Jellyfish attack is a kind of DOS (Denial of service) attack in which attackers or malicious nodes try to increase packet end-to-end delay and delay jitter. Before applying attack jellyfish attacker first gain access to the routing group in mobile ad hoc network. This can be possible by performing Rushing attack. According to change in number of senders, receivers and attack position scenarios will get change in jellyfish attack. As attacker get hold of forwarding packet, they start delaying or dropping data packets for certain amount of time before forwarding them normally [6].

Devesh Tedia, Umesh kumar [2016] explains various techniques developed to detect and prevent from jellyfish attack [7]. To design a security mechanism for MANET various attack variations as well as their characteristics must be known. This paper studies distinct kinds of attacks namely - Data traffic attacks, Jelly Fish Attacks, Jelly Fish Reorder Attack, Black Hole Attack, Gray Hole. The paper study mainly focuses on the jellyfish attack and its type.

CONCLUSION

This paper investigates various previous studies concerning the jelly fish attack in mobile ad hoc networks which produce unnecessary delay, and packet dropping. It can be analyzed from the various schemes presented that much of the work has been done to identify and protect from the delay variance attack. The authors in [4] has also worked upon the first variant, jellyfish delay variance attack. As a future work we would aim at detection and prevention of the kind of the jellyfish attack, i.e., jellyfish packet dropping attack.

REFERENCES

1. **Mohammad Wazid, Roshan Singh Sachan, R H Goudar,** "Measuring the Impact of Jelly Fish Attack on the Performance of Mobile Ad Hoc Networks using AODV Protocol" in ELSEVIER 2012.
2. **Amandeep Kaur, Deepinder Singh Wadhwa,** "Effects of Jelly Fish Attack on Mobile Ad-Hoc Network's Routing Protocols " in Amandeep Kaur et al Int. Journal of Engineering Research and Applications Sep-Oct 2013.
3. **Sanjay Kumar**, "Detection and Prevention of Jellyfish Attack in AODV Routing Protocol in MANET" in International Journal of Science Technology & Engineering December 2016.
4. **Sakshi sachdeva and parneet kaur,** "Detection and analysis of Jellyfish attack in MANETs" in IEEE 2017.

5. **Sapna Hans and Jitendra Kumar,** "Implementation of Secure AODV under Jelly Fish Attack" in International Journal of Engineering Sciences Paradigms and Researches June 2015.
6. **Mr. Hepikumar R. Khirasariya,** "Simulation study of jellyfish attack in MANET (mobile ad hoc network) using AODV routing protocol" in journal of information, knowledge and research in computer engineering 2013.
7. **Devesh Tedia, Umesh kumar,** " Various Attacks Including JellyFish Attack Along with Security Issues in MANET" in International Journal for Research in Applied Science & Engineering 2016.
8. **Mohammad Wazid, Vipin Kumar, RH Goudar,** "Comparative performance analysis of routing protocols in mobile ad-hoc network under Jelly fish attack", 2nd IEEE International Conference on parallel, distributed and grid computing, 2012.
9. **Nikolaos A. Pantazis, and Dimitrios D. Vergados**, "A Survey on Power Control Issues in Wireless Sensor Networks",IEEE Communications Surveys & Tutorials, VOLUME 9, NO.4, 2007,
10. **Rong Zheng and Robin Kravats**, "On Demand Power Management for Ad hoc Networks," Journal of Ad hoc Networks, Elsevier, Vol. 3, pp 51-68, 2005.
11. **Tanu Preet Singh, Neha, Vikrant Das, "**Multicast Routing Protocols in MANETS**",** in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 1, January 2012.
12. **C.E.Perkins**, "Ad Hoc Networking", Addison Wesley, 2001.

