Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 2052-2057
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.234

Study of Direct Trust-based Detection Algorithm for Prohibiting Jellyfish Attack in MANET

Shruti Thapar, Department of Electronics and Communication Engineering, Jaipur National University, Jaipur, Rajasthan
Sudhir Kumar Sharma, Department of Electronics and Communication Engineering, Jaipur National University, Jaipur, Rajasthan

Abstract-As the trend to using portable and mobile devices with time, MANET has become the important field due to its adaptability in various applications. There is a huge requirement for such kind of networks, which easily allow users to make or establish connection for communication in between. MANET earned its popularity by its various applications, quick and easy deployment in the network between the movable nodes. There is no need of infrastructural setup to create a mobile ad hoc network setup. In MANET, Mobile nodes will communicate through a wireless medium which makes this network highly vulnerable to much kind of harmful attacks present around. The most harmful attack among the list various attacks is jellyfish attack. In this research paper, we tried an approach which can able to detect and prevent jellyfish attack with increasing number of nodes.

Keywords: MANET, Jellyfish Attack, DTD, Mobile nodes, Routing Protocols, Performance Metrics.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) simply works without any access on mobile nodes using various wireless links with each and every node works randomly and can move anywhere around the network to maintain the link in between the nodes. due to its easy maintenance, they are popularly used in various applications such as disaster relief, emergency rescue operations, military services, vehicular networks (VANETs), office conferences, campus networks, robot networks etc. Security is the major aspect in any kind of network. In MANET, also due to its wireless and random network setup, safety and security is the major issue falls all around. To understand the hazardous activity of the network, it becomes important to get full information about the malicious content or attacker nodes present in the network. MANET get easily infected, as it has less centralized access, frequently changing topology, trustless environment and shortage of resources. No prior safety measures are there which can save MANET from harmful activity going inside the network, which makes it more prone towards attacks. Various kinds of attacks which can harm the MANET are wormhole attack, black hole attack, grayhole attack, flooding attack, denial of service (DoS), selfish node misbehaving, and impersonation attack etc. The attacker node can easily access the control of the network and target any of the layer stacks due to its wireless kind of nature. Malicious node can easily jam the network, disturb it through congestion, reorder the packet and change the routes of the networks, delays the packet etc. For secure and safe communication, network architecture is to be changed, to increase the efficiency of the networks affected by the attacks. Here, in this research paper, jellyfish attack is discussed in detail, and to prevent the mobile ad hoc network from this attack DTD scheme is applied around the network with TCP routing protocol to enhance the packet delivery ratio and decrease the delay rates caused by the attacking nodes. Still there is a need of vast and improved research work to be done on this topic as a lot of research work is already been done. The paper is organized as Section II describes an overview about jellyfish attack. Section III discusses related work. Section IV proposed methodology to remove Jellyfish attack from the network. Section V provides simulation results and Section VI gives conclusion to work done.

II. JELLYFISH ATTACKS

Routing protocols are brutally affected by Jellyfish attack and it is a very tough task to identify the jellyfish attacking node middle in the network. This will harm the data by reordering the packet sequence, dropping the packet or by delaying the packets which will increase the congestion in the network and goodput will be decreased. In this, the false node disturbs the normal call for protocol and introduces unwanted delays in the network. This attack is initiated from network itself and is so hard to detect. The attacker node first behaves like a trustworthy node but when any data packet reaches towards it, it will start delaying the packet more in the network or even reorder the sequence of the packet. It become mean and change their routing path explained in various versions of Jellyfish attack mentioned below. Types of Jellyfish Attacks are:

- **JF-Reorder Attack:** In Jellyfish Reorder attack, the false node will not follow the rule of FIFO I/P queue for data to proper route and creates reordering buffer size of k for random selection of packet before forwarding. Due to its reordering the packet in the network, TCP receives maximum duplicate ACK messages which will increase the congestion rate in the network. Due to increasing congestion rates network will have to suffer from unwanted delays and decreased throughput all around.
- **JF-Periodic Drop Attack:** In Jellyfish Periodic Drop attack, the false node randomly select and remove either a small piece of packets or remove the whole data packets for a small period of time. The time is decided by the attacking node only. This attacking node misuses the limits of TCP, that if acknowledgement (ACK) of any ongoing data packet has not been received before the expiration of Retransmission Timeout (RTO) value, then source node takes this timeout as that path which is increasing traffic in the network and will starts the slow phase and vice a versa. After that TCP connection is removed from the network. Due to this delay and goodput of the network will be affected very badly.
- **JF-Delay Variance Attack:** In Jellyfish Delay variance attack, the false node follows the rules of FIFO I/P queue to forward the data, but it will delay the packets before forwarding towards its destination. In Jellyfish delay variance attack, the false nodes will delay the packets and provides wrong information to TCP control at source node side to send traffic in bulk which will increase more collision and losses in the network. It becomes very difficult for TCP to manage the network traffic because there is no other option to detect the lost packets due to heavy network congestion. Therefore, it is hard to find and prevent the various versions of JF-Attacks in the network.

III. LITERATURE SURVEY

To control the malicious activities of the jellyfish attack present in the network, researchers find out a new way to protect the environment. Author [1] worked on authenticated routing based on attack injection and detection framework using genetic fuzzy logic rule based system (AR-AIDF-GFRS) for the removal of jellyfish attack in the network. In this fuzzy logic is been used in 4 different ways like, fuzzification, rule evaluation, aggregation of the rule outputs and defuzzification on the network. Author also compared the results with artificial ant colony based scheme. This scheme is been used with NS-2 simulator with AODV and DSR routing protocol for packet delivery ratio, throughput, delay, overhead and efficiency patterns. Using such scheme, author evaluated that packet delivery ratio and throughput level can be increased to great extent as compared to previous existing methods. This scheme can also be implementing on real time existing wireless networks for improved delivery ratio and throughput factors with less delay rates.

TCP and UDP are considered as one of the most effective transport layer protocols, which can able to transfer packets without any error or delay in it. But if TCP rates are degraded then it will directly affect the denial of service or jellyfish attack present in the network. This can delay, drop or reorder the packets of the network. In [2], author used friendship based jellyfish attack detection algorithm (FJADA) to minimize the activity of jellyfish attack in the manet. FJADA scheme uses direct trust based detection policy (DTD) in it. This scheme will control the packet collision, congestion and error spreading in the network. The proposed technique quickly and accurately controls the malicious activities of the attacker in the network. Author becomes successful to control the PDR, throughput rate, delay variance and detection rate of the false node in the network. This scheme is highly commendable to restrict the further damages in the network using MATLAB software with PETRI NET designs.

Previously, collaborative bait detection scheme were used to detect any kind of attack present in the network. This comes out to be a big failure to find the jellyfish attack in the network later. In particular research work [3], author used ant colony optimization based on clustering routing protocol. This work includes clustering of nodes and node's trust value to define the efficiency of the network. The exact trust value enables the trust tables of MANET to detect the jellyfish attack in the network. This research work comes out with efficient results by improving PDR rates and better aspects of secure communication in the network and it can also detect jellyfish attack in a very effective way.

To increase the network lifetime, author [10] used residual energy based reliable multicasting routing protocol. This scheme is introduced to increase the network lifetime, PDR and its forwarding rates in the network. As we know that multicasting of data packets may lead to increase the congestion and collision in the network. So, to improve such condition author used RERMR technique for network betterment using NS-2 simulator. The results came out with flying colors that RERMR gives high forwarding rates of the packets without any malicious content in it. Author compared the technique with previous techniques and find out that, this scheme is best to use for real life rescue operation or for military operations. But still if more improvement is made on such technique than network will become more prone to work with.

If attackers are detected timely then working on wireless systems becomes much easier. In [11], author used such intrusion detection scheme which work on trust management between all the nearby nodes. Based on the trust values nodes considered as trustworthy, risky or malicious nodes of the network. According to these three categories trustworthy nodes are recommended to rely on and it becomes easier to detect the malicious node from the network. Using MATLAB software author did its research part and conclude that the proposed scheme is actually gives the good results for detecting intrusion priory.

Author [12], worked on MANET and UAV network both with ODMRR routing protocol using Exacta cyber network simulator to detect the jellyfish attacking nodes of the network. This is the fresh approach used for multicasting routing protocol. Trust based policies are used to measure the trust values of the nodes. By this, selection of trustworthy nodes becomes easier to work on MANET and UAV both. This scheme needs much more improved patterns for further prospective but author finds the best and desired results using it.

IV. IMPLEMENTATION

Jellyfish attack detection

To detect and prevent from all the three variants of jellyfish attack present in the mobile ad hoc network, here we have adopted a light weight direct trust based detection (DTD) scheme or algorithm to make MANET an error free network. We have used TCP routing protocol to briefly examine the effectiveness and feasibility of our proposed scheme or methodology. In the method, each nodes of the network creates a trust table of its own and that's for suppose N being number of nodes in the network. Trust values are assigned to each and every node present in the network by the trust tables and only control messages can do any sort of changes in it. To reduce the congestion rates in the network only last updated things are conveyed by the control panel. Only by receiving the message form control panel, trust tables will add a new entry of the node or either updates their list of trust values for the existing nodes. Only a node can define as a JF node, when its trust valve is less than the minimum threshold value. Once attacking nodes is identified, it will be blacklisted from the trust table to maintain any route on. Neighboring nodes also broadcast this information through control panel in the network. Each blacklisted node has a timer fixed on it, after time expires that blacklisted node again work as a good node in the network. This is done to give another chance to false positive nodes, to work again in the network, but the same nodes gets three rejected or blacklisted then no more chances will be given to that particular node of the network. In our work, we have implemented a trust table at each and every node of the network built with proper information about the blacklisted nodes of the network. To analyze the scheme properly, few steps are taken to ensure that blacklisted nodes will not participate in the communication process. Nodes cannot send or receive messages through blacklisted nodes during routing process on any source to destination pair. If any node may receive the data packet through blacklisted node then it will ensure the route discovery for re routing the data packets. To describe the whole implementation on the network, a 16 node setup is been created and can be seen in the figure below. It can be observed through the diagram that all the blacklisted nodes are indicated properly.

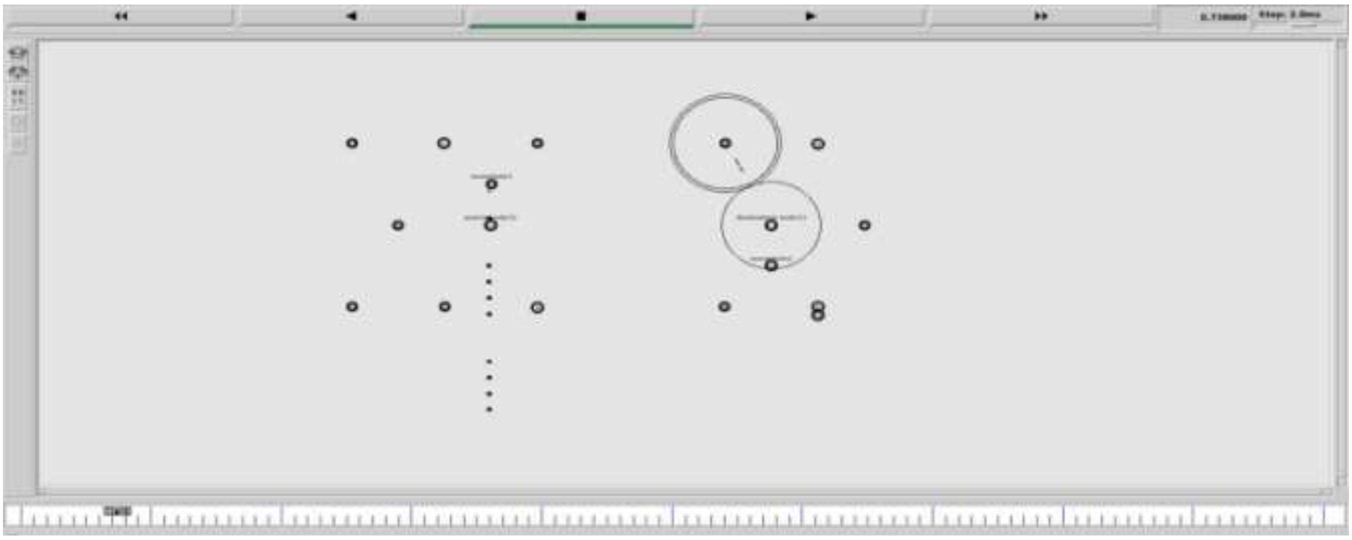

Figure 1: A 16 node network setup.

V. EXPERIMENTAL RESULTS

This simulated network is having 10 to 16 numbers of nodes with in the area of 700*700m^2. It uses the transmission range of 250 meters with random way point mobility model for the entire scenario. It has used the data size of 512 bytes. The simulation work is followed by analyzing the efficiency of the network by varying number of nodes in the presence of jellyfish attack with in the network. Packet delivery ratio and average end to end delay will be calculated as the performance metrics for the scenario generated. The number of packet being generated by the application and how many packets are received by the destination node will be analyzed as packet delivery rate of the network. Average end to end delay will be analyzed as how much time is taken by the data to travel between source node and destination node. It is analyzed by that time on which source initiates the data packet and destination node receives the packet. If the packet is taking more time, then delay will be introduced in the network by the selfish nodes. In this research we have evaluated direct trust based detection algorithm (DTD) to find jellyfish attack with the help of NS-2 Simulator. to increase the throughput rate of the network by finding and blacklisting the JF-node present in the network, is the prime motto of this research. Packet delivery ratio and average end to end delay can be seen in the below mentioned figures to analyze the efficiency of the proposed scheme. The results clearly depicts that by increasing number of nodes packet delivery rate is increasing and delay rates are decreasing. This is due to the fact that DTD scheme is reducing the effects of jellyfish attack in the network. Simultaneously, it is also capable to discover the entire false node present in the routing path and blacklisting them from the network. Due to this congestion in the network decreases and data packet rate on the destination node increases.

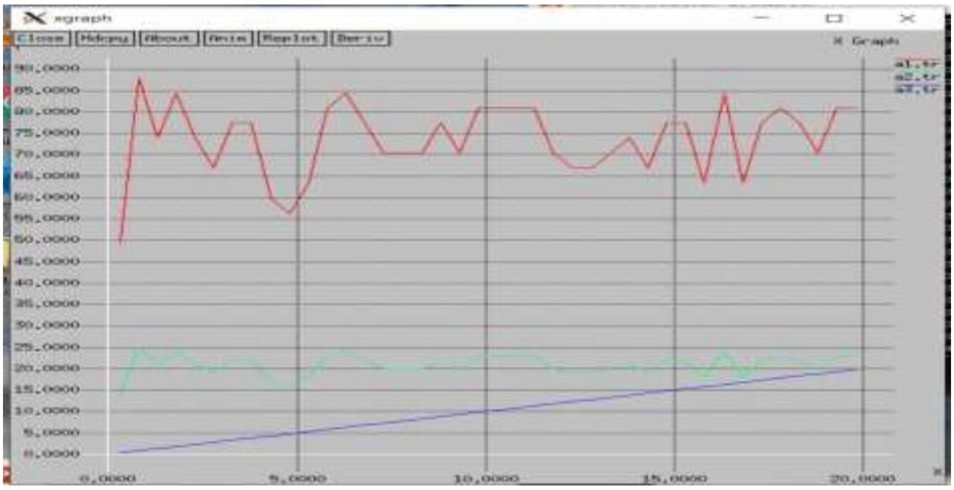

Figure 2: Packet Delivery Ratio with increasing number of nodes.

In figure, blue line shows the packet delivery rate with no malicious nodes present in the network, red line indicates packet delivery rate during the presence of attack and green line shows the packet transfer rate after the proposed method removes the false nodes from the network is shown in Figure 2. The end to end delay can be shown with and without detection of jellyfish attack is shown in Figure 3. It is concluded that the detection and prevention of jellyfish attack by the proposed algorithm decreases the end to end delay to a great extent. The throughput obtained in case of decreasing number of jellyfish attackers can be seen in Figure 4. It is observed that the proposed methodology enhances throughput of the system by eliminating malicious nodes.

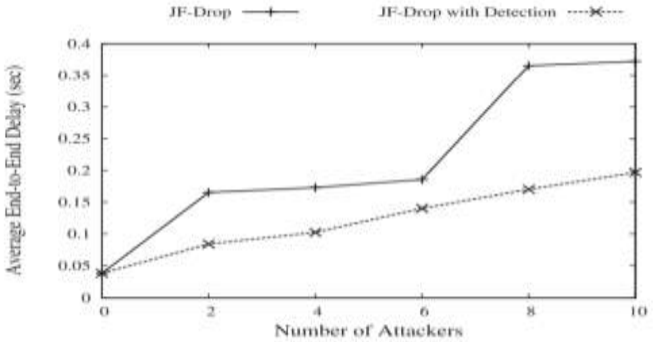

Figure 3: Average end to end delay with increasing number of JF attackers

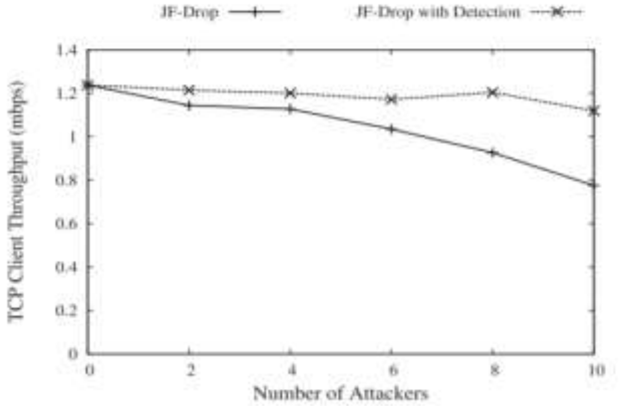

Figure 4: TCP throughput with increasing number of JF attackers

VI. CONCLUSION

In this research an integrated approach is presented to find and remove jellyfish attack from MANET. MANET being a infrastructure less wireless kind of characteristics make it vulnerable for almost all the attacks present around the network. Jellyfish is the most hazardous kind of attack. In literature survey, we have analyzed that many approaches are there to detect and prevent this malicious attack, but the research lacks in terms of algorithms that can prevent both of these simultaneously. A major reason behind this is that the prevention strategies for both of these attacks work on different parameters and network configuration. Our research algorithm is simulated on NS2 simulator and the performance is measured under 10-16 nodes through End to end delay and throughput. Thus, it is concluded that the proposed scheme is effective in detecting and preventing both the above cited attacks and works satisfactorily with increasing number of nodes.

REFERENCES

[1]. G. Suseendran, E. Chandrasekaran and Anand Nayyar," Defending Jellyfish Attack in Mobile Ad hoc Networks via Novel Fuzzy System Rule", Springer Nature Singapore Pte Ltd. 2019, V. E. Balas et al.

(eds.), Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing 839, https://doi.org/10.1007/978-981-13-1274-8 33.

[2]. Sunil Kumar, Kamlesh Dutta and Anjani Garg," FJADA: Friendship Based JellyFish Attack Detection Algorithm for Mobile Ad Hoc Networks", Springer Science+Business Media, LLC, part of Springer Nature 2018, Wireless Pers Communication, https://doi.org/10.1007/s11277-018-5797-z.

[3]. S. Satheeshkumar and N. Sengottaiyan," Defending against jellyfish attacks using cluster based routing protocol for secured data transmission in MANET", Springer Science Business Media, LLC 2017, Cluster Comput, DOI 10.1007/s10586-017-1202-z.

[4]. P Raghavendra Raju and Dr.K.C.Shet," A Cryptographic Hashing Solution for mitigating Persistent Packet Reordering Attack in Wireless Ad Hoc Networks", 2012 International Conference on Computing Sciences, 978-0-7695-4817-3/12, IEEE, DOI 10.1109/ICCS.2012.83.

[5]. Abdul Kayum Ali, Bobby Sharma and Usha Mary Sharma," Impact Analysis of JellyFish Attack in MANETs", ADBU-Journal of Engineering Technology, AJET, and ISSN: 2348-7305, Volume 4(1), 2016.

[6]. Devesh Tedia and Umesh kumar Lilhore," Various Attacks Including JellyFish Attack Along With Security Issues in Manet", IJRASET, Volume 4 Issue VII, July 2016, ISSN: 2321-9653.

[7]. Preety Dahiya and Miss Bhawana," Design and Implementation of NAODV_ETCP to Handle Jelly Fish Attack", International Journal of Engineering Trends and Technology (IJETT) – Volume 35 Number 7- May 2016, ISSN: 2231-5381 http://www.ijettjournal.org.

[8]. Sakshi Sachdeva and Parneet Kaur," Detection and Analysis of Jellyfish Attack in MANETs", ICICT-2016, doi: 10.1109/inventive.2016.7824793.

[9]. Girish Paliwal, Ankur Prakash Mudgal and Swapnesh Taterh," A Study on Various Attacks of TCP/IP and Security Challenges in MANET Layer Architecture", Springer India 2015 K.N. Das et al. (eds.), Proceedings of Fourth International Conference on Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing 336, DOI 10.1007/978-81-322-2220-0_16.

[10]. S. Gopinath and N. Nagarajan," Energy based reliable multicast routing protocol for packet forwarding in MANET", Journal of Applied Research and Technology, 13 (2015) 374-381, 1665-6423.

[11]. Syed Muhammad Sajjad, Safdar Hussain Bouk and Muhammad Yousaf," Neighbor Node Trust Based Intrusion Detection System for WSN", 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, EUSPN-2015, Procedia Computer Science 63 (2015) 183 – 188, doi: 10.1016/j.procs.2015.08.331.

[12]. Ashish Thomas, Vijay Kr. Sharma and Gaurav Singhal," Secure Link establishment method to prevent Jelly Fish Attack in MANET", 2015 International Conference on Computational Intelligence and Communication Networks, 978-1-5090-0076-0/15, 2015 IEEE, DOI 10.1109/CICN.2015.224.

[13]. Vijay Laxmi, Chhagan Lal, M.S. Gaur and Deepanshu Mehta," JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET", j ournal of information security and applications xxx (2014) 1e1 4, http://dx.doi.org/10.1016/j.jisa.2014.09.003, 2014 Elsevier.

[14]. Avani Sharma and Rajbir Kaur," Non-cryptographic Detection Approach and Countermeasure for JFDV Attack", SIN'14, September 09 - 11 2014, Glasgow, Scotland, Uk, Copyright 2014 ACM 978-1-4503-3033-6/14/09, http://dx.doi.org/10.1145/2659651.2659657.

[15]. Mousumi Sardar, Subhashis Banerjee, Kishore Majhi and Koushik Majumder," Trust Based Network Layer Attacks Prevention in MANET", Emerging Trends in Computing and Communication, Lecture Notes in Electrical Engineering 298, DOI: 10.1007/978-81-322-1817-3_21, Springer India 2014.

[16]. Manjot Kaur, Malti Sarangal and Anand Nayyar," Simulation of Jelly Fish Periodic Attack in Mobile Ad hoc Networks", International Journal of Computer Trends and Technology (IJCTT) – volume 15 number 1 – Sep 2014, ISSN: 2231-5381 http://www.ijcttjournal.org.

[17]. Vijay Laxmi, Deepanshu Mehta and M. S. Gaur," Impact Analysis of JellyFish Attack on TCP-based Mobile Ad-hoc Networks", SIN '13, November 26-28, 2013, Aksaray, Turkey,Copyright 2013 ACM 978-1-4503-2498-4/00/10, http://dx.doi.org/10.1145/2523514.2526999.

[18]. Fahad Samad, Qassem Abu Ahmed, Asadullah Shaikh and Abdul Aziz," JAM: Mitigating Jellyfish Attacks in Wireless Ad Hoc Networks", IMTIC 2012, CCIS 281, pp. 432–444, 2012, Springer-Verlag Berlin Heidelberg 2012.

[19]. K. Ganesh Reddy and P. Santhi Thilagam," Intrusion Detection Technique for Wormhole and Following Jellyfish and Byzantine Attacks in Wireless Mesh Network", ADCONS 2011, LNCS 7135, pp. 631–637, 2012, Springer-Verlag Berlin Heidelberg 2012.