Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444
Volume 4, Issue 3, March-2017

Jellyfish Attack Detection and Prevention in MANET: A Review

Patel Pooja B.
Department of Computer Engineering
Smt. S. R. Patel Engineering College,
Dabhi – Unjha, India

Patel Manish M.
Department of Computer Engineering
Smt. S. R. Patel Engineering College,
Dabhi – Unjha, India

Patel Megha B.
Department of Computer Engineering
Smt. S. R. Patel Engineering College,
Dabhi – Unjha, India

***Abstract*— Denial of Service (DoS) attack is one type of attacks in MANET, which detection and prevention is difficult. Jellyfish attack is DoS attack which further divided into three types like JF Reorder Attack, JF Periodic Dropping Attack and Jellyfish Delay Variance Attack. Jellyfish attack delay data packets for some amount of time means high end-to- end delay in the network and that reduce the performance of network. Jellyfish attack is difficult to detect as it obeys all the protocol rules. In this paper we discussed different techniques to detect and prevent jellyfish attack like cluster base and super cluster base technique, non-cryptography approach technique, Efficient Transmission Control Protocol to detect JFDV attack, Enhanced AODV Routing Protocols to detect JFDV attack, Mitigating Jellyfish Attack technique, Use displacement frequency and reorder density parameters to detect Jellyfish Reorder Attack.**

***Key words* — DoS Attack, Jellyfish Attack, MANET, Jellyfish Delay Variance Attack (JFDV)**

I. Introduction

In mobile ad hoc network mobile nodes are communicate with each other using wireless links and without any specified infrastructure or any centralized access point or base station. MANET is easily adaptable and self-configurable network so it is deploy quickly. MANET's node communicates with its limited range even though it works as host as well as router. The network in MANET is access by valid users as well as attacker because of MANET has no specified boundary or infrastructure. [1]

Characteristics of MANET likes lack of centralized authority, limited communication range, high power constraints, highly dynamic topology, inter node connected with mutual trust base that make them vulnerable to security attacks**.** [3]

Application of MANET: In robot networks, vehicular networks (VANETs), campus networks, home networking, indoor and outdoor conferences, emergency operations, rescue during natural calamities or tragedies, military services and disaster relief. [7]

Security issues: Outside attackers without trust relationship and inside attackers with trust relationship connected to the nodes which disrupt whole network. MANET is vulnerable from inside attackers because nodes communicate with each other on trust base and there is no centralized access point for monitoring them. [1]

II. JELLYFISH ATTACK IN MANET

Jellyfish attack is DoS attack which further divided into three types like JF Reorder Attack, JF Periodic Dropping Attack and Jellyfish Delay Variance Attack. In this kind of attack, the malicious node produces high end to end delay in the network and that reduce the performance of network. To prevent itself from detection and diagnosis, JF node remains active in both route discovery process and packet forwarding process. [3]

JF attack follows all the protocol rules so it detection is difficult. Jellyfish attack similar as blackhole attack but the difference is that the blackhole attacker node drops all the data packets and jellyfish attacker node produces high end to end delay during forwarding the data packets. [1]

Jellyfish attack targets closed loop flows because of that flow react by packet loss and delay. To make diagnosis in order, jellyfish attacks compliance both control plane and data plane. Jellyfish attack detection is very costly and time consuming.

Jellyfish attack Application: HTTP, file transfer, real time video etc. TCP connection has desynchronizes because data packet delay by Jellyfish attack which reduces network performance. [5]

TYPES OF JELLYFISH ATTACK

A. Jellyfish Reorder Attack:

Jellyfish (JF) node creates a reordering k size buffer instead of forwarding them in FIFO buffer. Duplicate acknowledgement is sent to the sender while packets arrive in re-order at the destination side. Without waiting for retransmission timeout, sender retransmits the data packets if three duplicate acknowledgements are received at the sender side. The packet has reached at destination side sender still believes that packet is lost. So sender retransmits the packet again and again that occur congestion in network. If the length of reordering is equal to or more than the threshold of duplicate acknowledgement then sender assumes that packets are lost. [8]

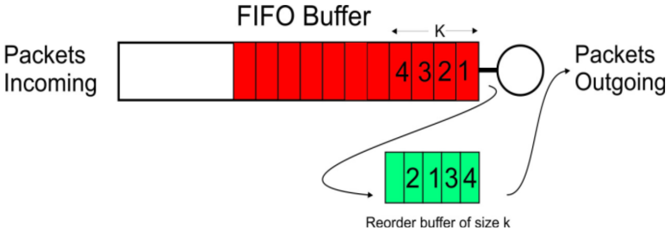

Figure 1: Jellyfish Reorder Attack [1]

B. *Jellyfish Periodic Dropping Attack:*

Due to congestion, TCP throughput will be reducing because node forces to drop packets periodically. JF node may either chose fraction for dropping the packets or may discard all the packets which are received for some particular amount of time e.g. dropping some milliseconds in every 1 second near the timeout scale. When the flow becomes stable attacker repeats their work of dropping the data packet so it reduce the performance of network. [1]

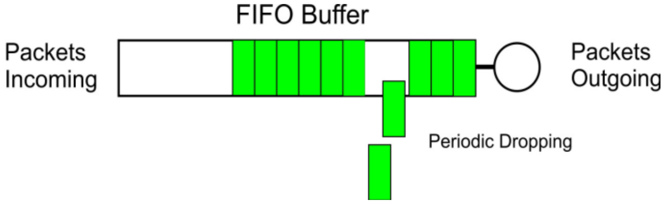

Figure 2: Periodic dropping attack [1]

C. *Jellyfish Delay Variance Attack:*

In JFDV attack, JF nodes are random delay between each data packets for some amount of time. This process force to send traffic bursts and eventually create more collisions in network. In TCP, if the acknowledgement of forwarding data packet is not received within round trip time (RTT) of data packet so accordingly that the value of RTO will be increase. [3]

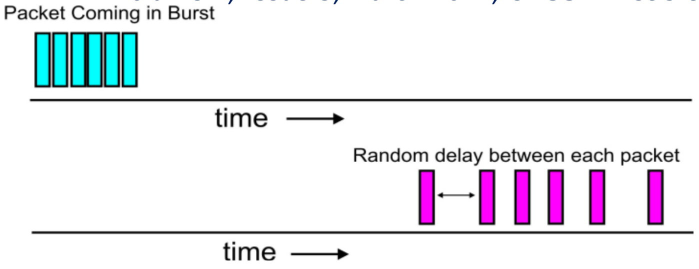

Figure 3: Delay Variance Attack [1]

Jellyfish delay variation leads the following situations in the network:

1. Jellyfish node increases re-transmission timeout (RTO) as compare to round trip time (RTT).
2. It increases collision and loss of packets due to data traffic burst.
3. Due to congestion delay available bandwidth is unutilized. [3]

III. LITERATURE REVIEW

- Cluster based and Super Cluster based intrusion detection and prevention techniques for JF Reorder Attack [2]

A. Cluster Based Intrusion Detection and Prevention Technique (CBIDPT)for JF Reorder Attack[2]

Multiple mobile nodes are connected to each other with limited communication range and it create cluster. A cluster head is elected by each mobile nodes of every cluster which are in range. [2]

Cluster head elects on the basis of following two consideration points:
1) Fairness: The probability of every node become a cluster head should be equal.
2) Efficiency: Efficient cluster head should be selected through some methods or techniques.

Cluster head has responsibility to detect the attacker node from different clusters. In CBIDPT, source node and intermediate nodes make entry into its FIFO buffer then it forward the data packet to the neighbor node. Source node and intermediate node sends same FIFO buffer to cluster head also. Cluster head compares its sequence numbers of FIFO buffer with sequence numbers of all intermediate nodes FIFO buffer. If any reordering is found in forwarding data packet, cluster head automatically omits that intruder node on the basis of their ID which is already stored in cluster head. Then cluster head searches for other optimum route which has not any type of intruder node. [2]

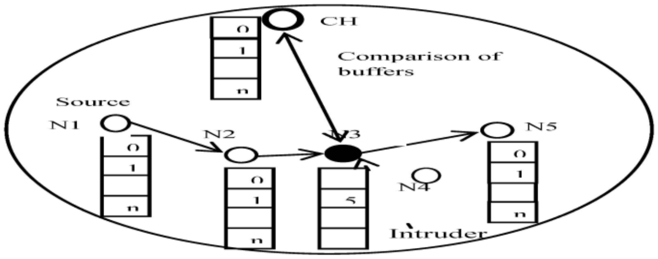

Figure 4: Intrusion Detection using CBIDPT [2]

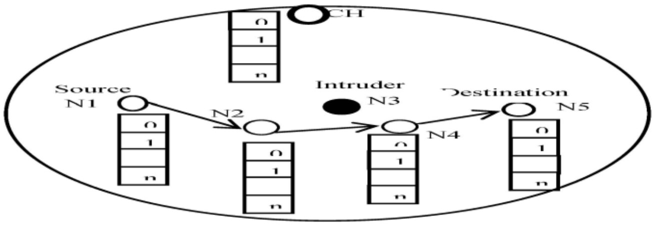

Figure 5: Normal flow after intrusion detection and prevention using CBIDPT [2]

B. Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT)for JF Reorder Attack [2]

Super Cluster is build by collecting multiple clusters. When cluster head (also an intermediate node) becomes intruder that time SCBIDPT is use. Super cluster head is the supreme authority to check misbehavior of different cluster heads. All work same in CBIDPT and SCBIDPT. But only super cluster head have authority to remove cluster head from the network when cluster head become intruder. [2]

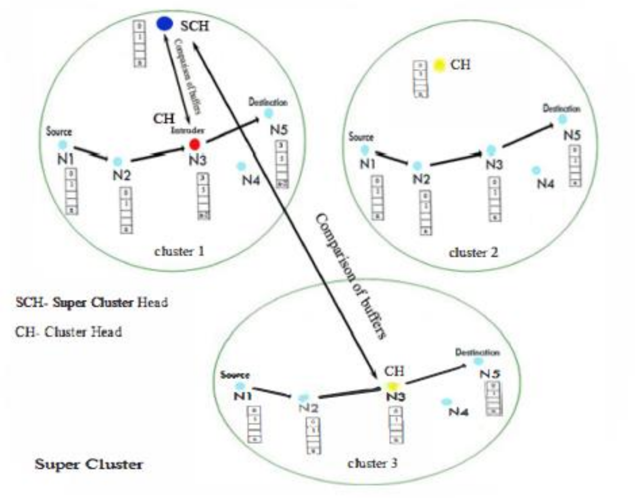

Figure 6: Intrusion Detection using SCBIDPT [2]

- Non-cryptography approach for detection and mitigation of JFDV Attack [3]

Non-cryptography approach is work basically on delay threshold time. Where delay threshold time defines as a time interval boundary of all enroute nodes of forwarding data packet. This approach has following two phases:

1. To analyze all data packets and check which particular data packet among them is delaying data packet at enroute nodes. Any misbehavior found during analysis, decides malicious (JF) node present in the routing path of data packet.
2. After detection of JF node presence it re-routing the forwarding data packet through alternate optimum routing path which having non-malicious nodes.

If difference between time of current forwarding data packet and their previous send data packet with delay threshold time is greater than JF attack is detected. For prevention of JF attack re-routing process is used.

- *Re-routing Process:* For example: Source node S send forwarding data packet to destination node D through the nodes 1, 2 and 3. In this process node No. 2 delay in forwarding data packet to its neighbor node 3 in process means that node No. 2 behaves as JF node. After detection of such JF node present in the process then node No. 1 searches other alternate node having non-malicious node for forwarding the data packet. [3]

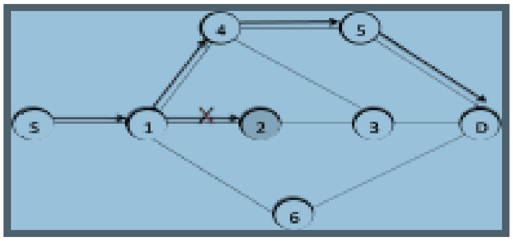

Figure 7: Re-Routing of data packet in OLSR [3]

- Efficient Transmission Control Protocol (E-TCP) [4]

Jellyfish delay variance attack delays the data packet during forwarding the data packets to the destination. Because of that packet ACK is also delayed and sender assumes that the packet has been lost. In this situation sender retransmits the same packet again and again that create congestion in the network. If cluster head time equal to intermediate node buffer entry time than efficient TCP otherwise not. [4]

E-TCP protocol prevents JFDV attack by disabling fast retransmission of malicious data packets and enabling selective ACK in order of send data packet. The network performance is improved by TCP protocol so it named as Efficient Transmission Control Protocol (E-TCP).

- Enhanced AODV routing protocols (EAODV) for detect JFDV attack [5]

Enhanced AODV (EAODV) routing protocol is detect the JF delay variance attack and also removes attacker node without its knowledge. After certain interval of time each node sends a normal broadcast packet in EAODV then check which node among its neighboring nodes is delaying the data packet by time more than the threshold time of network. For that it checks receive time and sending time difference greater then threshold JF node present otherwise not. In route discovery reply from JF node is discarded and choose alternate path.

- Mitigating Jellyfish Attack [7]

In modified TCP protocol output is very low or RTO value is high so it starts sending catalyst-helper packets (CHPs) with a constant ratio to check if congestion is still there or not. If no longer congestion in network, it avoids long waiting time and it allows observing nodes to detect misbehaviors of attacker node in the network. [7]

Furthermore, each flow have unique id number (*flow id*) while forwarding the data packets. Observing node has 3-tuple values (IP address, SEQ, flow id) for identify packets.

> ➢ *Detection Mechanism of JF Periodic Attack:* These detection mechanisms collect FORWARDED actions which named as evidences. The more evidences are collected through this mechanism then results of JF periodic attack detection is more accurate.[7]
>
> If the observed node o is non malicious then gap g is very small so it will not include drop intervals and the evidences will be distributed in whole interval. If node o is malicious then g will be high enough so it includes some pure drop intervals.

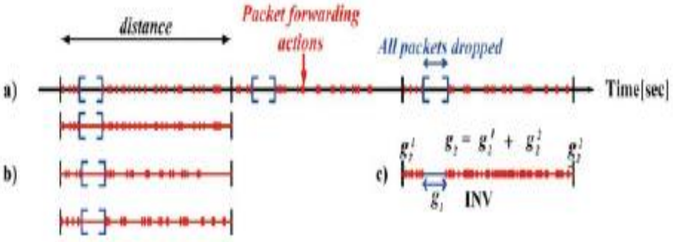

Figure 8: JF Periodic Attacks (Detection Mechanism) [7]

> ➢ *Detecting Jellyfish Reorder Attack:* Observing nodes comparing the SEQ numbers of all outgoing packets (of the same flow) for detection of packet reordering. If an observed node send packets SEQ numbers is lower than the sent packet SEQ number, it occur misbehavior. If misbehaviors occur for at least $T_{reorder}$ seconds, it detects JF reorder attack.
>
> If a sufferer flow result is very low then it sending CHPs and attacker is continuously reordering of packets. Thus the attack will be detected by one neighbor hop.

- Use using displacement frequency and reorder density parameters for detect Jellyfish Reorder Attack [8]

In this method, packet arrives at its destination it use assign value of packet which called as receive index (RI) and sequence number (S) respectively. For find reorder density (RD) use receive index (RI) and sequence number (S) of packet. [8]

Where Reorder Density (RD) is use to detect and capture the nature of reordering in a packet flow which is separate density function. Packet displacement frequency called as Frequency Density (FD).

For calculating metric **i.e.** ∑ **FD*RD** use the product of frequency density and reorder density of all the displacements and their summation. Displacement Frequency is the displacement of k with number of packets arriving this term is denoted by FD[k]. [8]

IV. CONCLUSION AND FUTURE SCOPE

In jellyfish attack, the malicious node produces delay before the transmission and reception of data packets in the network. Jellyfish attack delay data packets for some amount of time. So, result is high end-to- end delay in the network and that reduce the performance of network.

Here, we discussed detection and prevention techniques for jellyfish attack. We can detect jellyfish attack by all above techniques but we don’t know delay is occurring due to congestion or JF node. This problem is solve in future by considering parameter likes sending and receiving time of forwarding data packet compare with its threshold time of packet and load of network.

REFERENCES

[1] Vijay Laxmi, Deepanshu Mehta, M. S. Gaur, Parvez Faruki, Chhaganlal,” Impact Analysis of Jellyfish Attack on TCP-based Mobile Ad-hoc Networks”, © ACM 2013, pp.189-195

[2] Mohammad Wazid, Avita Katal, R H Goudar, “Cluster and Super Cluster Based Intrusion Detection and Prevention Techniques for Jellyfish Reorder Attack”, International Conference on Parallel, Distributed and Grid Computing © IEEE 2012, pp. 435-440

[3] Avani Sharma, Rajbir Kaur, “Non-cryptographic Detection Approach and Countermeasure for JFDV Attack”, © ACM 2014

[4] Mohammad Wazid, Avita Katal, Roshan Singh Sachan, R H Goudar,“ E-TCP for Efficient Performance of MANET under JF Delay Variance Attack ”,Conference on Information and Communication Technologies (ICT),© IEEE 2013, pp. 145-150

[5] Sakshi Garg, Satish Chand,” Enhanced AODV protocol for defense against Jellyfish Attack on MANETs ", © IEEE 2012, pp. 2279-2284

[6] Mohammad Wazid, Vipin Kumar, RH Goudar,” Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under Jellyfish Attack”, International Conference on Parallel, Distributed and Grid Computing , © IEEE 2012, pp. 147-152

[7] Fahad Samad, Qassem Abu Ahmed, Asadullah Shaikh, Abdul Aziz,” JAM: Mitigating Jellyfish Attacks in Wireless Ad Hoc Networks”, © Springer-Verlag Berlin Heidelberg 2012, pp. 432-444

[8] Simranpreet Kaur, Rupinderdeep Kaur, A.K. Verma, “Jellyfish attack in MANETs: A Review”, ©IEEE 2015, pp. 1-5

[9] Xin Yuan, Santosh Mahapatra, Wickus Nienaber, Scott Pakin, Michael Lang,” A New Routing Scheme for Jellyfish and its Performance with HPC Workloads”, © 2013 ACM

[10] B. B. Jayasingh, B. Swathi,” A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network”, © BIJIT Jan – June, 2010

[11] Hoang Lan Nguyen,Uyen Trang Nguyen,“Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks” ,International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL)© IEEE 2006

[12] Hoang Lan Nguyen, Uyen Trang Nguyen“A Study of Diffrenet Types of Attacks in Mobile Ad hoc Networks”, 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) ©IEEE 2012

[13] Meenakshi Patel,Sanjay Sharma ,“Detection of Malicious Attack in MANET” , © IEEE 2012

[14] Vijay Laxmi,Chhagan Lal,M.S. Gaur,Deepanshu Mehta,”Jellyfish attack:Analysis,detection and countermeasure in TCP-based MANET” ©Elsvier Ltd.-ScienceDirect 2014, pp. 1-14