International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 21, Issue 01) and (Publishing Month: June 2015)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Implementation of Secure AODV under Jelly Fish Attack

Sapna Hans[1] and Jitendra Kumar[2]

[1]Student, M. Tech. CSE,
Bahra Institute of Management and Technology, VPO Chidana, District Sonepat, Haryana (India)
sapna.hans09@gmail.com

[2]HOD, CSE Department,
Bahra Institute of Management and Technology, VPO Chidana, District Sonepat, Haryana (India)
jitendrakumar.03@gmail.com

Abstract

This paper modifies the existing TCP and AODV system to handle the jelly fish periodic dropping attack and the jelly fish delay variance attack. The proposed system modifies the AODV routing protocol and TCP to handle the jelly fish attack variants. The proposed system uses the E_TCP of the existing system along with the modified AODV routing to get the effective results. The proposed process uses the forwarding rate and the delay check to enhance the performance of the protocol. The forwarding rate is calculated by number of packet received divided by number of packet forwarded. The node with forwarding rate less than 0.70 i.e. 70% is discarded and the hello packet transmission is used to calculate the average delay within the path. If the packet doesn't reach the destination the average delay time than the packet is discarded and the route is marked as the congested route; where this threshold value i.e. constant value for any particular network. The other packet transmission doesn't prefer the route.

Keywords: *MANET, Jelly Fish Attack, AODV.*

I. Introduction

A mobile ad hoc network is a self-organizing system of mobile nodes that communicate with each other via wireless links with no fixed infrastructure or centralized administration such as base stations or access points. Nodes in a MANET operate both as hosts as well as routers to forward packets for each other in a multi-hop fashion. MANETs are suitable for applications in which no infrastructure exists such as military battlefield, emergency rescue, vehicular communications and mining operations. In these applications, communication and collaboration among a given group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and resources, since a single message can be delivered to multiple receivers simultaneously [1].

II. Attacks in MANET

A MANET provides network connectivity between mobile nodes over potentially wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network- layer protocols that extend the connectivity. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications.

Nodes in a MANET works together as hosts and routers to forward packets for each other in a multi-hop manner. MANETs are useful for various applications in which no infrastructure exists like vehicular communications, and mining operations [1].Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide security architecture to secure ad hoc networking. They found that numerous presently existing attacks have some common features and have been categorized into different attacks based on their minor differences. So hereby they are trying to categorize them into two broad categories: DATA traffic attacks and CONTROL traffic attacks. [2].

III. 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 [3].

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 nodes can change the sequence of the packets also drop some of the data packets. The jelly fish attacker nodes fully obeys protocol rules, hence this attack is called as passive attack [4].

IV. Proposed System

The proposed system modifies the existing system to handle the jelly fish periodic dropping attack and the jelly fish delay variance attack. The proposed system modifies the AODV routing protocol and TCP to handle the jelly fish attack variants. The proposed system uses the E_TCP of the existing system along with the modified AODV routing to get the effective results. The proposed process uses the forwarding rate and the delay check to enhance the performance of the protocol. The forwarding rate is calculated by number of packet received divided by number of packet forwarded. The node with forwarding rate less than 0.70 i.e. 70% is discarded and the hello packet transmission is used to calculate the average delay within the path. If the packet doesn’t reach to the destination within th+average delay time than the packet is discarded and the route is marked as the congested route; where th is threshold value i.e. constant value for any particular network. The other packet transmission doesn’t prefer the route.

This process can be easily understood by the following algorithm:

```
The Source S and the destination D
Transmit the hello packet n the network
Avdelay=Calculate the delay
Delay=0;
Current_node=S
While current_node~=D
    Broadcast the RREQ from current_node
    G=group of nodes at one hop distance from current_node
    For each node in G say n
        If forwarding ratio of node n<0.70
            Then discard the node
        End if
    End for
    Forward the data to any node in G
    Update current_node
    Delay=delay+current_delay
    If delay>avdelay+th
        Then discard the node(path)
        Current_node=S
    End if
End while
```

The proposed algorithm is an efficient algorithm i.e. used is capable to handle the jelly-fish attack.

V. Simulation Results

The implementation and result analysis of this algorithm is done by using the simulator NS2. The proposed technique is implemented in NS-2.35 Simulator in Linux environment. The tcl file is executed and it generates a .nam file which can be viewed in Network Animator tool of ns2 simulator.

Performance Metrics

Following are the metrics from which we calculate the performance of the network:

- **Throughput**

Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

- **Packet Delivery Ratio (PDR)**

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packet receive / ∑ Number of packet send

- **End-to-end Delay**

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

Table 1: Result Analysis of existing System

Number of nodes	PDR	E2e delay	Through Put
10	13.48	37.17	1.06
20	43.10	28.11	50.24
30	37.46	28.19	59.08

Table 2: Result Analysis of Proposed System

Number of nodes	PDR	E2e delay	Through put
10	49.87	14.15	1070.24
20	49.83	14.28	1074.66
30	49.79	13.85	1083.00

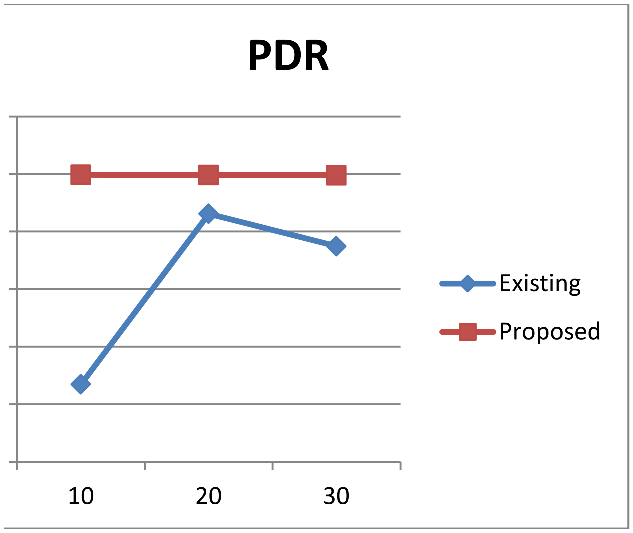

Figure 1: Comparison of PDR

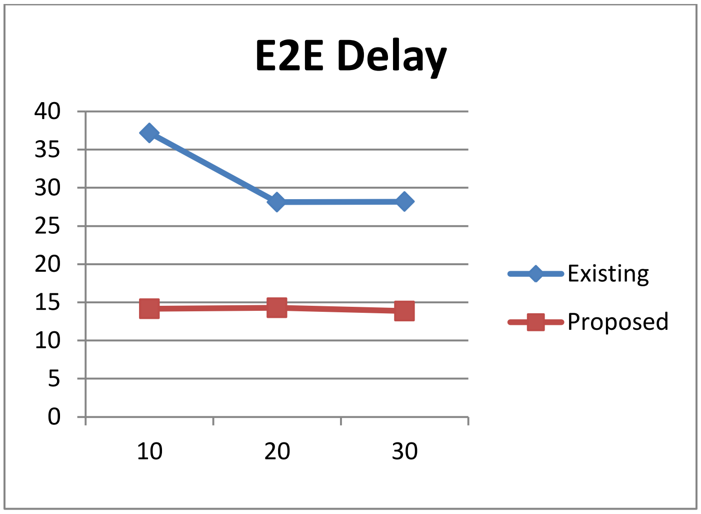

Figure 2: Comparison of E2EDelay

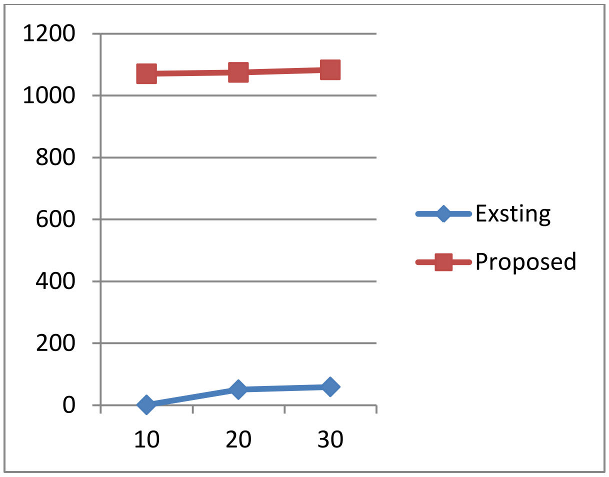

Figure 3 : Comparison of Through Put

VI. Conclusion

The paper shows that the performance of the proposed protocol is better than the existing protocol. The E2Edelay gets decreased and it results in enhanced throughput. The decreased delay and enhanced throughput confirms the better performance of the proposed protocol. The better performance is verified by the packet delivery ratio of the proposed protocol. The PDR of the proposed protocol is also better than the existing protocol.

References

[1] Nguyen, Hoang Lan, and Uyen Trang Nguyen. (2008),A Study Of Different Types Of Attacks On Multicast In Mobile Ad Hoc Networks., Ad Hoc Networks 6, no. 1.

[2] Bhattacharyya, Aniruddha, Arnab Banerjee, Dipayan Bose, Himadri Nath Saha, and Debika Bhattacharya. (2011) Different types of attacks in Mobile ADHOC Network., arXiv preprint arXiv:1111.4090.

[3] Amandeep Kaur et al (2013) Effects of Jelly Fish Attack on Mobile Ad-Hoc Network’s Routing Protocols, Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.1694-1700

[4] 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