Design and Implementation of NAODV_ETCP to Handle Jelly Fish Attack

Preety Dahiya[1], Miss Bhawana[2]
[1,2]*Department of Electronics and Communication Engineering ,R.N. College of Engineering And Management, Maharshi Dayanand University, Rohtak,Haryana*

Abstract--- *This paper modifies the existing TCP and AODV system to handle the jelly fish periodic dropping attack, the jellyfish packet reordering 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. In the E_TCP protocol the buffer stores the sequence number and the acknowledgement time while in the NAODV_ETCP protocol the fr(forwarding ratio) is also stored in buffer. This paper analyzes the performance using PDR, E2Edelay and the throughput on the various scenario attacked by different types of jellyfish attack. The result analysis shows that the performance of NAODV_ETCP is better than the ETCP protocol.*

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 [1]. Techniques for protecting the routing infrastructure in global Internet that have been proposed in recent years are not adequate for ad hoc network requirements. Ad hoc networks face threats that are not encountered in traditional network requirements. These unique threats induce types of network failure modes that cannot be handled by security services designed for the global internet infrastructure [2].

II. Literature Survey

Thomas D. Dyer at al. [3](2001) examined the performance of the TCP protocol for bulk data transfers in mobile ad hoc networks (MANETs). They vary the number of TCP connections and compare the performances of three recently proposed on-demand (AODV and DSR) and adaptive proactive (ADV) routing algorithms.

Latha Tamilselvan et al. [4](2007) discussed the routing security issues of MANETs. One type of attack, the black hole, which can easily be deployed against the MANET, is described and a feasible solution for it in the AODV protocol was proposed. One of the principal routing protocols used in Ad-Hoc networks was AODV (Ad-Hoc On demand Distance Vector) protocol.

Jatin D. Parmar et al,[5] (2010) introduced some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a big issue in MANETs as they were infrastructure-less and autonomous.

Mohammad Wazid et al. [6] (2013) said that the existence of JF attackers affects the performance of the network. E-TCP is a modified Transmission Control Protocol proposed. Under the application of E-TCP the network performs better reducing the congestion and improving the performance of the network.

III. Attacks in MANET

This assumption is unfortunately not true in a hostile environment. Because cooperation is assumed 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 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. 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. [7].

IV. 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 [8]. 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 [9].

V. Proposed System

The proposed system i.e. NAODV_ETCP modifies the existing system i.e. AODV_ETCP to handle the jelly fish periodic packet dropping attack, the jelly fish delay variance attack. The source node broadcast the RREQ message and the group of nodes at one hop distance receives the request. The nodes with forwarding ratio less than the threshold value gets discarded from the group. The forwarding ratio is calculated by number of packet received divided by number of packet forwarded. The node with forwarding rate less than 0.7 i.e.70% is discarded i.e. the threshold is 0.70. The remaining nodes of the group receive the packet and send the acknowledgment. The process continues until destination reached. If any node receive the acknowledgment from the destination but not from the neighbor node then the node discard the neighbor node. This process handles the packet dropping attack.

The whole process can be easily understood by the following algorithm:

1. The Source node say S and the destination node say D is selected.
2. The S node transmits the hello packet.
3. ad=the time taken by hello packet to reach the destination.
4. T=0
5. Select cur=S
6. First_t=0;
7. While cur~=D
8. Broadcast the RREQ from cur after reordering at cur.
9. G=Group of nodes at one hop distance from cur.
10. If first _t=0
11. First_t=1
12. else
13. If the cur receives the Ack from destination but not from neighbour
14. Then discard the neighbour node
15. End if
16. End if
17. For each node in G say Ni
18. If forwarding ratio of node Ni<0.70
19. Then discard the node
20. End if
21. Store the RREQ in the buffer of Ni.
22. Send Ack from each node Ni.
23. End for
24. Update cur.
25. t=t+current_time_taken
26. If t>ad+th
27. Then discard the path.
28. cur=S
29. End if
30. End while

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

VI. Simulation Result

Simulation can be defined as “Imitating or estimating how events might occur in a real situation”. It can involve complex mathematical modeling, role playing without the aid of technology, or combinations.

There are two languages used in NS-2; C++ and OTCL (an object oriented extension of Tool Command Language). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTCL script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTCL. The OTCL script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to

graphical software called Network Animation (NAM).

Parameter Analyzed

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.

Σ Number of packet receive / Σ 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.

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

Table 1: Performance Analysis under packet dropping attack at 30 nodes

Number Of nodes attack	PDR		E2E delay		Throughput	
	Existing	Proposed	Existing	Proposed	Existing	Proposed
0	37.46	49.79	28.19	13.85	59.08	1083.00
1	33.10	49.19	28.90	13.86	54.24	1082.00
2	30.56	49.14	28.75	13.86	52.75	1082.00
3	27.46	49.09	29.34	13.86	49.08	1082.00

Table 2: Performance Analysis under delay variance attack at 30 nodes

Number Of nodes attack	PDR		E2E delay		Throughput	
	Existing	Proposed	Existing	Proposed	Existing	Proposed
0	37.46	49.79	28.19	13.85	59.08	1083.0
1	36.36	49.69	31.90	13.86	44.24	1082.0
2	36.28	49.68	33.34	13.86	42.87	1082.0
3	36.16	49.67	35.24	13.86	40.18	1082.0

Table 3: Performance Analysis under packet reordering attack at 30 nodes

Number Of nodes attack	PDR		E2Edelay		Throughput	
	Existing	Proposed	Existing	Proposed	Existing	Proposed
0	37.46	49.79	28.19	13.85	59.08	1083.0
1	35.60	49.39	28.90	13.85	55.24	1083.0
2	34.79	49.30	28.66	13.86	52.34	1082.0
3	33.06	49.19	29.14	13.86	49.68	1082.0

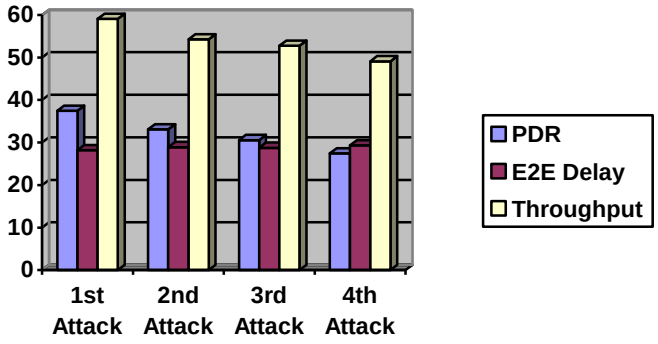

Figure 1: PDR Comparison

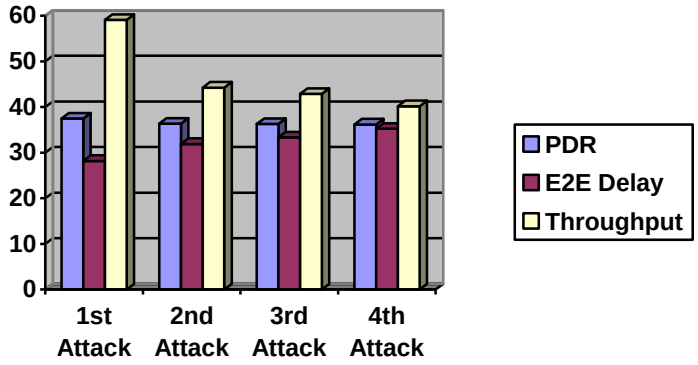

Figure 2: E2E Delay Comparison

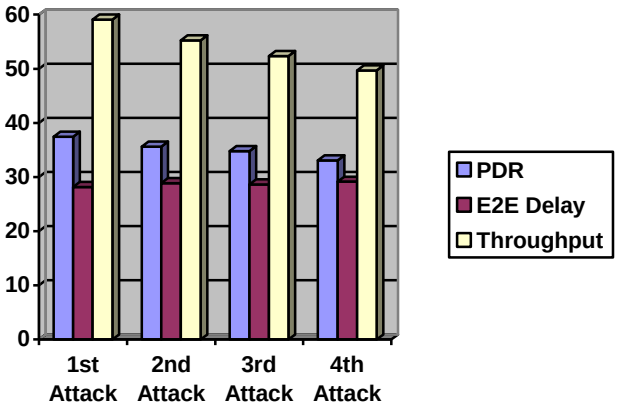

Figure 3: Throughput Comparison

VII. Conclusion and Future scope

This paper reviews various attacks in MANET. The main focus of the paper is on the jellyfish attack and its types. The paper also discusses various work done to detect and prevent the jellyfish attack MANET. In future, a technique can be developed to handle more than one jellyfish attack at one time.

VIII. Acknowledgment

We are thanking to our management for their continuing support and encouragement for completing this work and we are thanking our head of the department for his valuable suggestion.

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]Begum, Syed Atiya, L. Mohan, and B. Ranjitha.(2012), Techniques for Resilience of Denial of service Attacks in Mobile Ad Hoc Networks. Proceedings published by International Journal of Electronics Communication and Computer Engineering 3, no. 1.

[3] Dyer, Thomas D., and Rajendra V. Boppana.(2001), A comparison of TCP performance over three routing protocols for mobile ad hoc networks., In proceedings of the 2nd ACM international symposium on mobile ad hoc networking and computing, pp. 56-66. ACM.

[4] Tamilselvan, Latha, and V. Sankaranarayanan.(2007) Prevention of black hole attack in MANET. In Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on, pp.21-21. I EEE,

[5] Jhaveri, Rutvij H., Ashish D. Patel, Jatin D. Parmer, and Bhavin I. Shah.(2010) MANET routing protocols and wormhole attack against AODV. International Journal Of Computer Science And Network Security10, no. 4: 12-18.

[6] Wazid, Mohammad, Avita Katal, Roshan Singh Sachan, and R.H. Goudar.(2013) E-TCP for efficient performance of MANET under JF delay variance attack. In Information and Communication Technologies (ICT), 2013 IEEE Conference on, pp. 145-150 IEEE,

[7] Bhattacharyya, Aniruddha, Arnab Banerjee, Dipayan Bose, Himadri Nath Different types of attacks in Mobile ADHOC Network., arXiv preprint arXiv: 1111.4090.

[8]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

[9]Mr. Hepikumar R. Khirasariya,(NOV 12 TO OCT 13.), Simulation Study of Jelly Fish Attack In Manet (Mobile Ad Hoc Network) Using Aodv Routing Protocol, Journal Of Information, Knowledge And Research In Computer Engineering, ISSN: 0975-6760 VOLUME- 02,ISSUE-02|