SIMULATION STUDY OF JELLYFISH ATTACK IN MANET (mobile ad hoc network) USIND AODV ROUTING PROTOCOL

MR. HEPIKUMAR R. KHIRASARIYA

Master of Engineering [Computer Engineering Branch] Student,
V.V.P Engineering College, Rajkot.
Enrollment number:- 120470702001
Gujarat Technological University (GTU)

happyrk204@gmail.com

ABSTRACT: *Mobile ad hoc networks (MANETs) are highly vulnerable as there is no presence of trusted centralized authority and dynamic network topology. Multiple senders and receivers can act at a same time in MANET and communication is hop by hop through intermediate node. Due to such characteristics of MANET various kind of attacks are possible. Attack in MANET may be active or passive. 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 starts delaying or dropping data packets for certain amount of time before forwarding them normally.*

Keywords—Mobile ad hoc network (MANET), Jellyfish attack, Rushing attack, malicious node.

JIKRCE

I: INTRODUCTION

In mobile ad hoc network, there is no centralizing administration as there is absence of any base station or access point. Communication in mobile ad hoc networks takes place through wireless medium and varying infrastructure or topology also becomes reason for various kinds of attacks. Mobile ad hoc networks are used in various applications like military battlefield, emergency rescue, vehicular communications and mining operations. In mobile ad hoc network any nod may be sender or receiver or sometimes nodes have to perform duty of routers. As compare with wired network security issues are more in mobile ad hoc networks as there is lake of any centralized authority, dynamic network topology, low Bandwidth, and battery and memory constraints of mobile devices. There is also lake of trust relationships between mobile nodes in mobile ad hoc networks. In this paper, Simulation-based study of the effects of Jellyfish attack in mobile ad hoc networks is presented. I study how the number of attackers and their positions affect the performance of a connection in terms of packet delivery ratio, throughput, end-to-end delay, and delay jitter. In simulations, AODV (Ad hoc On-demand Distance Vector) routing protocol is used.

II: OVERVIEW OF AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol in mobile ad hoc networks (MANETs).In AODV, every node maintains a table, containing information about neighbors to which they will have to send the packets in order to reach to the destination. Sequence numbers, that is one of the key features of On-Demand Distance Vector, ensures the freshness of routes. When a node (source node) wants to send a packet to another node (destination node), the source node performs a Route Discovery by broadcasting a ROUTE REQUEST (RREQ) packet to the destination node, which is flooded throughout the network in a controlled manner.

Every node forwarding the RREQ message caches a route back to the Source node S. Routes is maintained by using ROUTE ERROR (RERR) message, which is sent to notify other nodes about a link breakage. HELLO messages are used by the nodes for detecting and monitoring links to their corresponding neighbors.[3]

III: RUSHING ATTACK:

In reactive routing protocols, which use duplicate suppression, rushing attack is quite possible. As shown in to the figure.1, consider node X as the source node and node Y as the destination node. M1 and M2 are the two neighboring nodes of destination node Y. In routing activity that uses reactive routing protocol Ad hoc on Demand Distance Vector (AODV).Source node X need to communicate to destination node Y. So, X will broadcasts route request (RREQ) packet. There are multiple paths available via which this RREQ packet reached to node Y. There are two neighboring nodes M1 and M2 passes this RREQ packet finally to the node Y. Now, if H is the malicious node also passes this packet via multiple paths through M1 and M2 speedily then other nodes. It means in all paths RREQ was forwarded through H or in other words H is able to rush its RREQ earlier to destination. Then other legitimate RREQ packets will be ignored as per the protocol rules. So, as a result source node X is unable to find legitimate route with less number of hops. Later on H may not forward the RREQ.

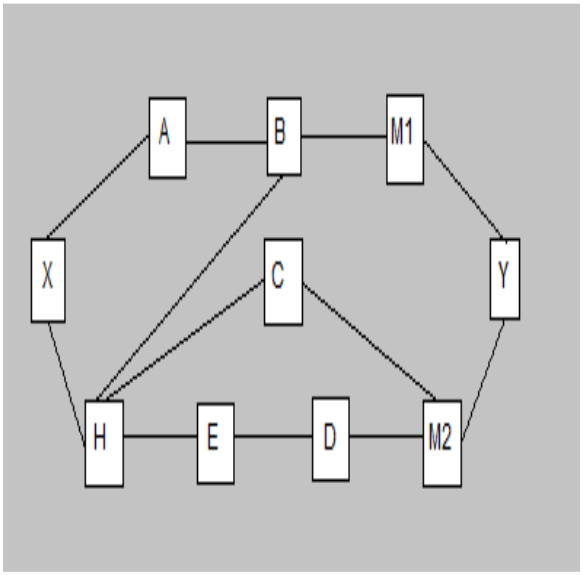

Fig.1 rushing attack scenario

IV: JELLY FISH ATTACK:

Jelly fish attacks are targeted against closed-loop flows. In jellyfish attack, attacker node or malicious node fully obeys protocol rules. So, it is a passive attack and difficult to detect. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. As shown in fig.2 jellyfish attack is further classified into three sub categories Jellyfish recorder attack, Jellyfish periodic dropping attack and Jellyfish Delay variance attack.[1]

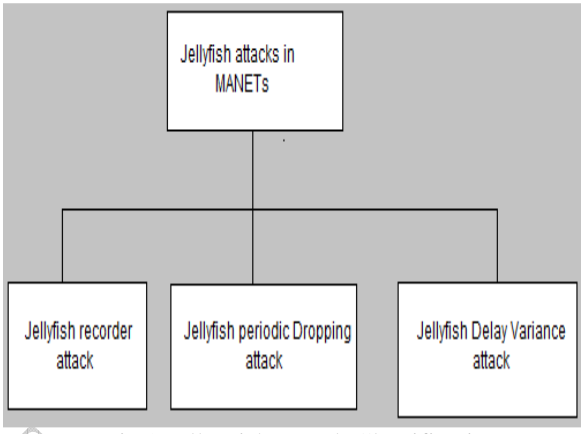

Fig 2 Jelly Fish Attack Classification

Jellyfish Reorder Attack

Jelly Fish Reorder attack is possible due to well known vulnerability of TCP. Jelly fish attacker uses this vulnerability to record packets. This is possible because of factors such as route changes or the use of multipath routing.[1]

Jellyfish Periodic Dropping Attack

Periodic dropping is possible because of sarcastically chosen period by the mischievous node. This kind of periodic dropping is possible at relay nodes. Suppose that congestion losses force a node to drop a% of packets. Now consider that the node drops a% of packets periodically then TCPs throughput may be reduced to near zero even for small values of a [1].

Jellyfish Delay Variance Attack

In this type of attack, the malicious node randomly delays packet without changing the order of the packets.[1]

In this set of experiments, a jellyfish attacker first needs to gain access to the routing paths. If successful, it then delays all data packets it receives for a random period of time ranging from zero to 10 seconds before forwarding them. Fig. 3 shows the average end-to-end delay and delay jitter of a

JKRCE

connection under various conditions as a function of the number of attackers.[2]

V: JELLYFISH ATTACK: Number of Flows

Figs. 3(a) and 3(b) show that the higher the number of attackers, the longer the EED and the larger delay jitter. The graphs also show that higher number of flows results in higher EED and delay jitter, as it creates a higher chance for jellyfish attackers to be in the routing paths. This explains that when there is only one flow in the network, it is harder for jellyfish attackers to locate the routing path and interfere with the data flow.[9]

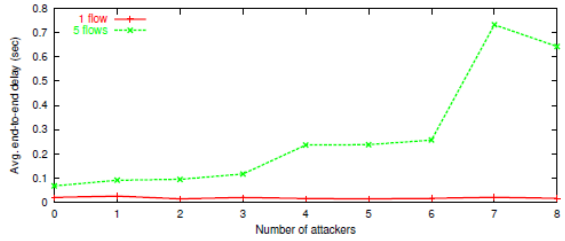

Fig 3(a)Number of flows: End-to-end delay

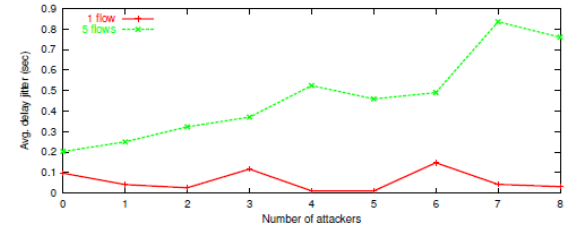

Fig 3(b) Number of flows: Delay jitter

VI: JELLYFISH ATTACK: Node Mobility

In general, the higher the mobility speeds, the higher the EED and delay jitter (Figs. 4(a) and 4(b)). However, there is one exception: the no-mobility case, which was expected to have the smallest EED and delay jitter, actually had higher EED and delay jitter than the 1 m/s case. It is because a slow mobility speed makes it a little harder for jellyfish attackers to invade into the routing paths. [9]

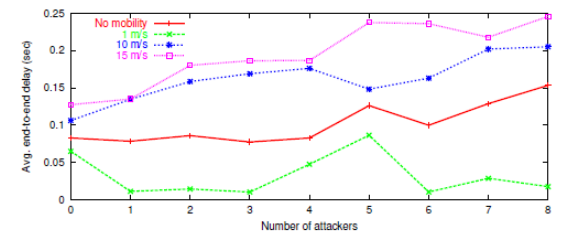

Fig 4(a) Node mobility: End-to-end delay

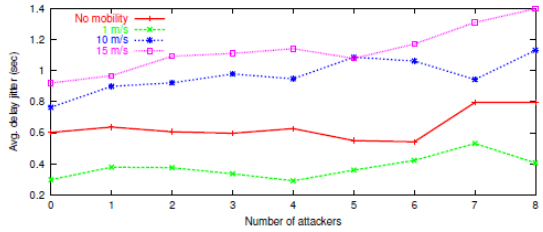

Fig 4(b) Node mobility: Delay jitter

VII: JELLYFISH ATTACK: Traffic Load

The EEDs and delay jitters for different traffic loads as a function of the number of attackers are shown in Figs. 5(a) and 5(b). As the numbers of attackers increases, the EEDs and delay jitters of all the traffic loads also increased. Moreover, the graphs show that with the same number of attackers, the higher the traffic load, the higher the EED and delay jitter. One of the reasons is due to higher transmission rate and more collisions in the network. Another reason is that with high traffic load, data packets arrive at a attacker node at a much higher rate. As a result, more data packets will be captured and delayed by the attacker, resulting in higher EED and delay jitter. [9]

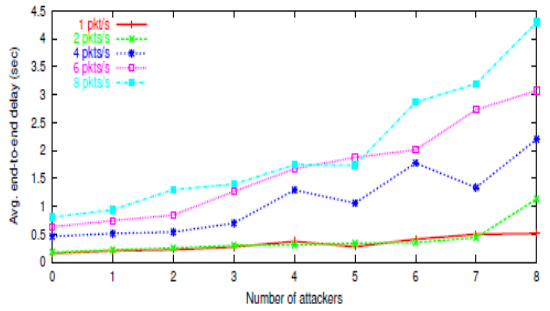

Fig 5(a) Traffic loads: End-to-end delay

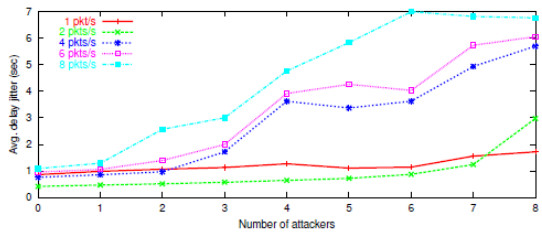

Fig 5(b) Traffic loads: Delay jitter

VIII: JELLYFISH ATTACK: Attack Positions

This experiment studies the effects of jellyfish attacks on the packet end-to-end delay and the delay jitter in the four cases near the senders, near

the receivers, around the network center, and uniformly distributed over the entire network area. Figs. 6(a) and 6(b) display the simulation results. The near-sender position was the most powerful attack location, causing the highest EED and delay jitter compared to other positions. [9]

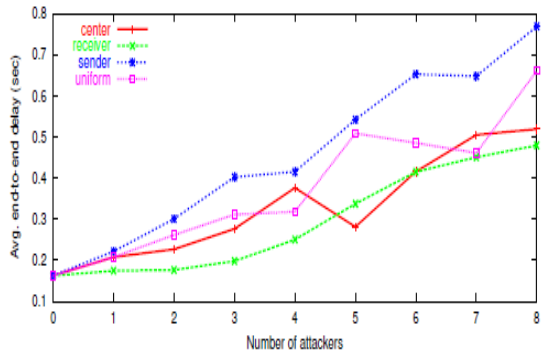

Fig 6(a) Attack positions: End-to-end delay

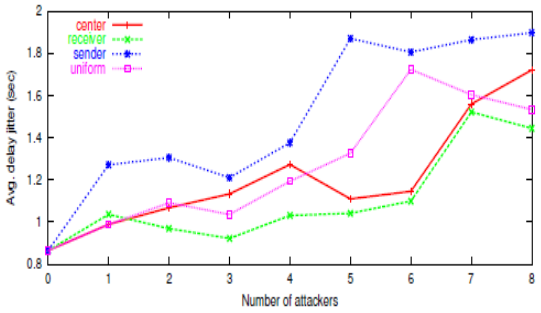

Fig 6(b) Attack positions: Delay jitter

VI: CONCLUSION

The performance of a connection in a MANET under Jellyfish attack depends heavily on many factors such as the number of flows, node mobility, traffic load, and the number of attackers as well as their positions. Our simulation results confirm an intuitive claim: the more attackers there are in the network, the more damage they inflict on a flow in terms of packet delivery ratio, or delay and delay jitter (jellyfish attack). Jellyfish attacks severely increase the packet end-to-end delay and delay jitter. In particular, a network with a high density of connections is easier for attackers to capture the routes and hence the data packets. On the other hand, mobile nodes may create extra difficulties for attackers to intrude into the routing paths, as the paths may change due to node mobility. But if the mobility is too high, then the network performance will suffer because of frequent link breaks. With respect to attack positions, areas near the senders are the most damaging positions.

8. REFERENCES

[1] Fei Xing, Wenye Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks" in proc. of IEEE MILCOM'06 conference on Military communications

[2] I. Aad, J.P. Hubaux and E.W. Knightly, Denial of Service Resilience in Ad Hoc Networks, in: Proceedings of ACM MobiCom 2004, Sep. 2004.

[3] C.E. Perkins, E.M. Royer and S.R. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, in: Proceedings of IEEE WMCSA '99, New Orleans, LA, Feb. 1999.

[4] B.Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, Mitigating Byzantine Attacks in Ad Hoc Wireless Networks, Technical Report, Mar. 2004.

[5] D.B. Johnson, D.A. Maltz, Y.C. Hu, and J.G. Jetcheva, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Kluwer Academic Publishers, Vol. 5, pp. 153-181, 1996.

[6] QualNet Simulator, http://www.qualnet.com

[7] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks, in: Proceedings of IEEE MILCOM '02, 2002.

[8] P. Ning and K. Sun, How toMisuse AODV: A Case Study of Insider Attacks AgainstMobile Ad-hoc Routing Protocols, in: Proceedings of the 4th Annual IEEE Information Assurance Workshop, West Point, Jun. 2003.

[9] *Hoang Lan Nguyen, Uyen Trang Nguyen.*a study of different types of attacks in MANET, 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)