International Journal of Electrical and Electronic Engineering & Telecommunications

ISSN 2319 – 2518 www.ijeetc.com
Vol. 4, No. 4, October 2015

Research Paper

IMPLEMENTATION OF DELAY VARIANCE ATTACK FOR AODV AND TORA USING VOICE TRAFFIC

Deepak Kumar[1]* and Harjinder Singh[1]

*Corresponding Author: Deepak Kumar, ✉ sunilkapoorldh@gmail.com

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without the aid of any established infrastructure or centralized administration. Every node is allowed to enter and leave the network freely, which along with nodes movement makes routing very difficult. Due to such characteristics of MANET various kind of attacks are possible. The main target of the paper is to analyze the impact of Delay Variance attack for AODV and TORA using Voice Traffic under MANET. Simulation is carried out by using OPNET modeler 14.0. Measurements of different parameters with complete analysis and comparison are presented.

Keywords: Delay variance attack, AODV, TORA MANET, Voice traffic

INTRODUCTION

Mobile Ad hoc Networks can be termed as a set of wireless mobile nodes forming a dynamic autonomous network. Each node in MANET serves as a router and a host, and is allowed to join and leave the network freely. Mobile Ad hoc networks can be frequently deployed in conferences, emergency situations and campuses for data sharing and real time applications (Anipakala Suresh, 2005). Scalability is one of the main issues in MANETs, as increase in the number of nodes along with high node mobility makes routing very difficult for a multi hop network. The MANETs are affected by different types of attacks, which include Packet dropping attack, Packet Modification attack, Sybil attack, Denial-of-Service attack, etc. The MANETs are more prone to Denial of-Service (DOS) attacks as compared to others. A Denial-of-Service attack is an attempt to make a machine or network resource unavailable to its intended and legitimate users. The DOS attacks can be done in different ways, which are consumption of computational resources, disruption of configuration information, disruption of state information and disruption of physical network components (Mehmud Abliz, 2011).

[1] Department of Electronics & Communication Engg., Punjabi University, Patiala.

Denial-of-Service attacks have been discussed that affect the working of a network and have disastrous results. Among these attacks, the Delay Variance Attack (JellyFish attack) is the worst type of Denial-of-Service attack because it is difficult to detect and hence difficult to remove from the network. It desynchronizes the TCP-connection by delaying the packet and hence reduces the performance of network (Sakshi Garg and Satish Chand, 2014).

The JellyFish (JF) attack can be easily carried out in MANET because the MANETs are infrastructure-less and there is no centralized administration on nodes present in the network (Mohammad *et al.*, 2012). A malicious node can enter the network easily and create the attack. This attack affects the functionality of TCP. Due to the fact that the TCP is reliable and waits for ACK before sending more packets, it becomes more susceptible to this attack. The JF delay variance attack delays the packet before forwarding it, so the TCP sends each packet again as it does not receive the ACK in time. This increases the congestion in network and reduces the throughput of the network. The JF attack being protocol-compliant is difficult to detect. In this paper, we propose an enhanced AODV protocol, which is able to detect the attacker node and remove it from the forwarding path created during the route discovery.

ROUTING PROTOCOL

Ad hoc nature, high node mobility and changing network sizes in MANETs make routing very difficult. Therefore it is important to determine a suitable routing protocol which can perform efficiently under the required conditions. Comparison of AODV and TORA is performed in this paper over different number of nodes, in order to determine that which routing protocol can perform efficiently, when we increase the number of nodes. Main contribution of this paper is to provide a simulated environment for the performance comparison of AODV and TORA and determine which protocol can perform better if we increase the number of nodes with TCP and UDP traffics.

Ad-Hoc on-Demand Distance Vector Routing (AODV)

AODV is a Reactive routing protocol. AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. Without source routing, AODV relies on routing table entries to propagate an RREP back to the source and, subsequently, to route data packets to the destination. AODV (Anisur Rahman and Alex Talevski, 2009) uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. An important feature of AODV is the maintenance of timer based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. A set of predecessor nodes is maintained for each routing table entry, indicating the set of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing

all routes using the broken link. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves.

Temporally-Ordered Routing Algorithm (TORA)

The TORA is a source initiated protocol and provides multiple routes for any desired source/destination pair (Chenna Reddy and Sekhar Reddy, 2006). The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. In order to accomplish that nodes maintain routing information about adjacent (one-hop) nodes. The protocol performs three basic functions: route creation, route maintenance, and route erasure.

SIMULATION ENVIRONMENT

The simulations are carried out using discrete event simulation software known as OPNET (Optimized Network Engineering Tool) Modeler version (Chenna Reddy and Sekhar Reddy, 2006). It is one of the most widely used commercial simulators based on Microsoft Windows platform and Linux Operating System.

To justify the proposed work, simulations for mobile ad hoc network under JF delay variance attack for two routing protocols, i.e., AODV and TORA has been performed in OPNET. In this paper, total eight simulation scenarios have been considered depending on the type of data flow (normal or under JF attack), type of routing protocol (AODV or OLSR) and number of MANET nodes (30 or 50 nodes). For example, one simulation scenario is MANET with 30 nodes is under JF attack and uses OLSR for routing. The nodes were randomly placed within certain gap from each other in campus environment. Voice traffic with low quality speech is generating in the network explicitly (i.e., user defined) via application configuration node.

Table 1: Parameters for the Simulation of Network

Parameters	**Values**
Simulator	Opnet Modeler 14.0
Area	10*10 KM
Network Size	30 Nodes and 50 Nodes
Traffic Type	Voice (Low quality Speech)
Encoder Scheme	G.723.1 5.3K
Mobility Model	Random waypoint
Voice Frame per Packet	1
Simulation Time	10 Minutes
Compression Delay (Sec)	1
Ad Hoc Routing Protocols	AODV and TORA
Buffer Size	256000
Forwarding Rate	300000 packet/sec for honest nodes 5000 packet/sec for JF nodes
Packet Size	1024
Short Retry Limit	7
Long Retry Limit	4
Type of Service	Best Effort
Transmit Power	0.020

RESULTS

Load

Figures 1 and 2 shows the load in MANET for 30 and 50 nodes. In case of AODV 30 nodes, normal flow network and jelly fish attack network produces the equal values at the peak. But in 50 node scenario, jelly fish scenario

Figure 1: Load (bits/sec) 30 Nodes (AODV)

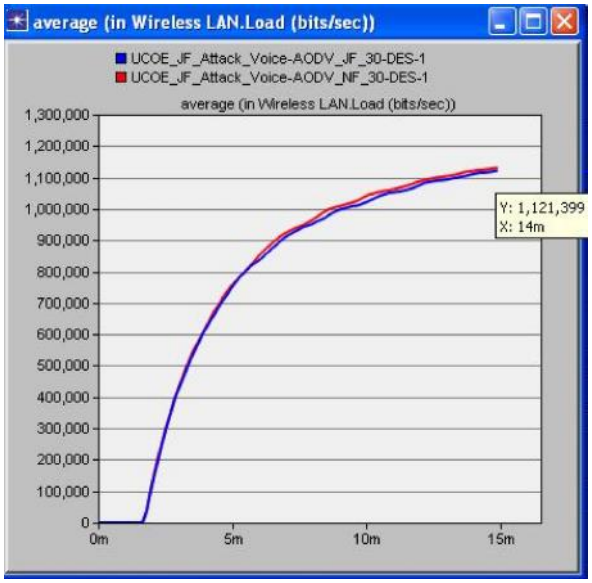


Figure 2: Load (bits/sec) 50 Nodes (AODV)

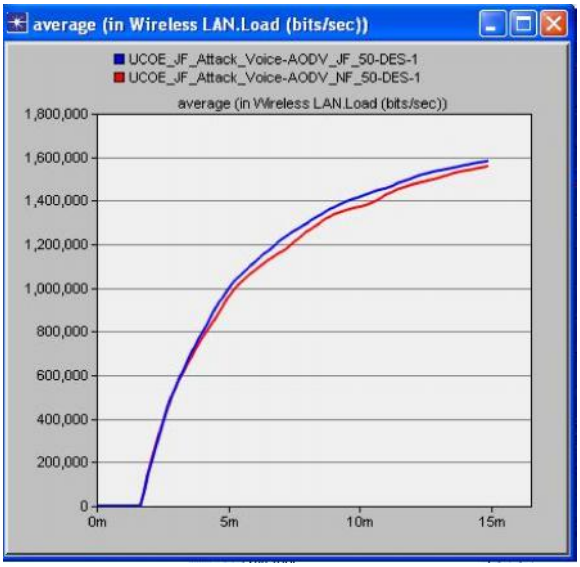


Figure 3: Load (bits/sec) 30 Nodes (TORA)

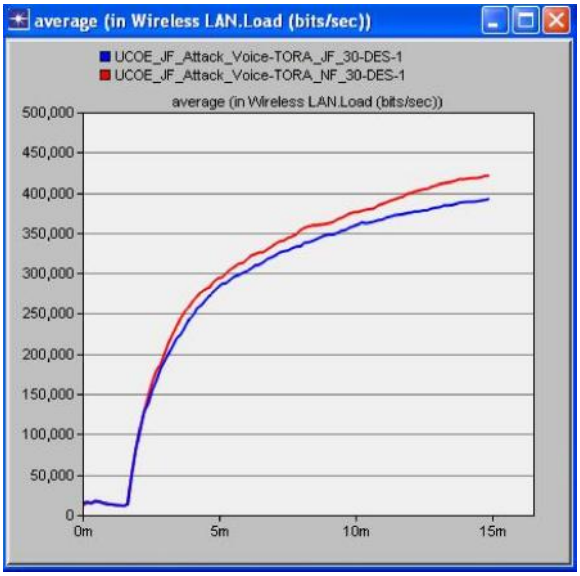
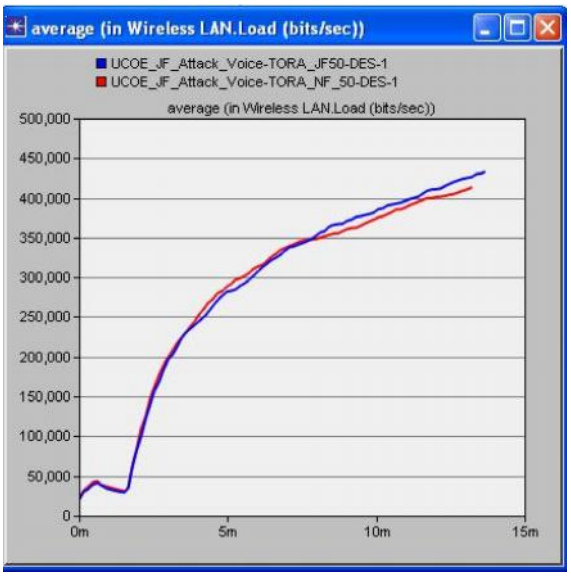


Figure 4: Load (bits/sec) 50 Nodes (TORA)



gives the highest value/load in the network, so we can define jelly fish nodes creates the high load in the high node density.

Figures 3 and 4 also shows the load for TORA, i.e., 30 and 50 nodes. According to Figures 3 and 4, TORA with Jelly Fish attack scenario produces the worst performance in both cases, means jelly fish also affect the network in the case of Load.

Delay

Figures 5 and 6 shows the wireless delay in MANET for 30 and 50 nodes. In case of

Figure 5: Delay (sec) 30 Nodes (AODV)

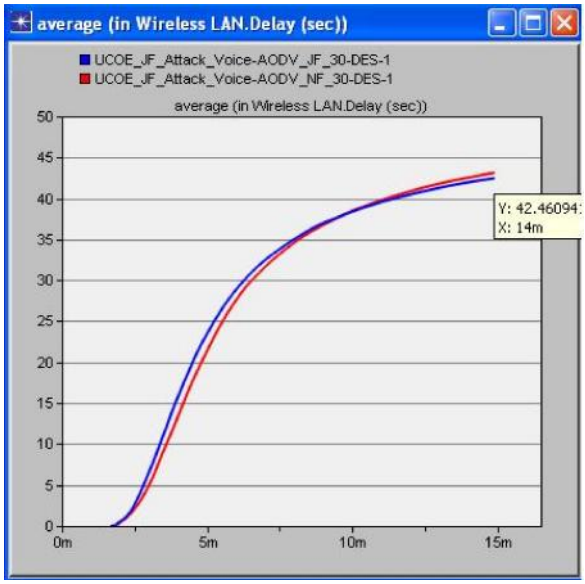
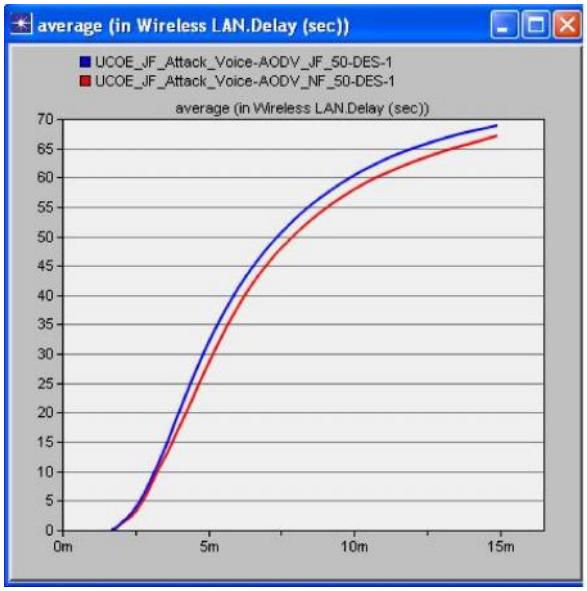


Figure 6: Delay (sec) 50 Nodes (AODV)



AODV 30 nodes, there is little bit difference in the values between normal flow network and jelly fish attack network. But in 50 node scenario, jelly fish scenario gives the highest value/delay in the network so we can define jelly fish nodes creates the high load in the high node density.

Figure 7: Delay (sec) 30 Nodes (TORA)

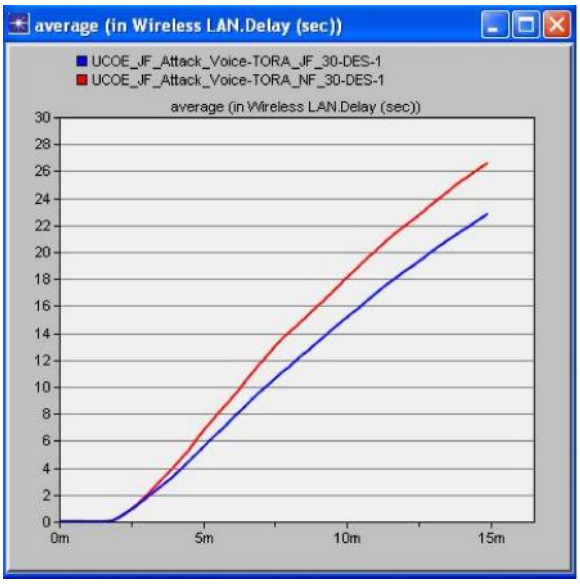
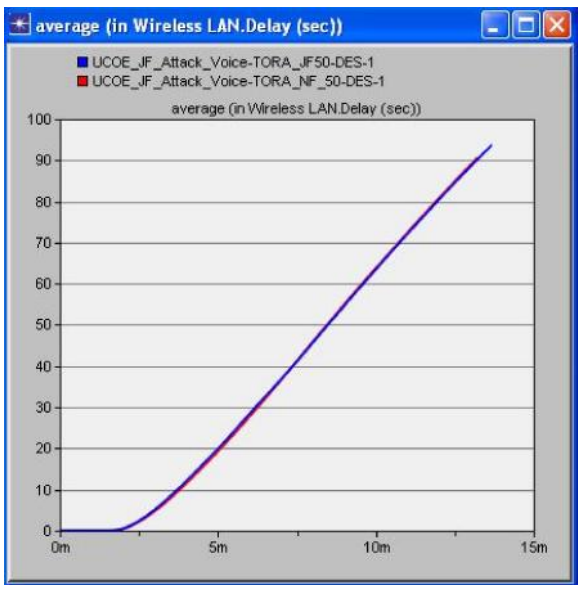


Figure 8: Delay (sec) 50 Nodes (TORA)



Figures 7 and 8 also shows the wireless delay for TORA, i.e., 30 and 50 nodes. According to fig 7, heavy delays in the normal flow but in case of 50 nodes, when nodes increases the delay also increases in the jelly fish scenario. It means high node scenario will affect the network.

Throughput

Figures 9 and 10 shows the throughput of the network for 30 and 50 nodes. In both cases AODV 30 and 50 nodes, normal flow network produces best performance. Jellyfish network has the worst performance. It degrades the throughput of the network.

Figure 9: Throughput (bits/sec) 30 Nodes (AODV)

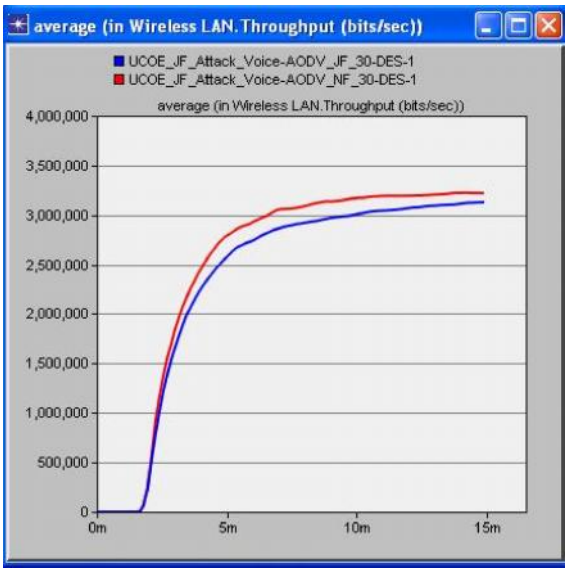


Figure 10: Throughput (bits/sec) 50 Nodes (AODV)

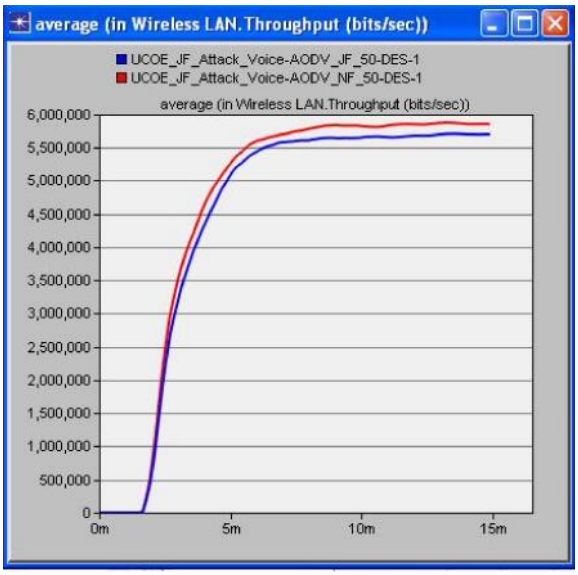


Figure 11: Throughput (bits/sec) 30 Nodes (TORA)

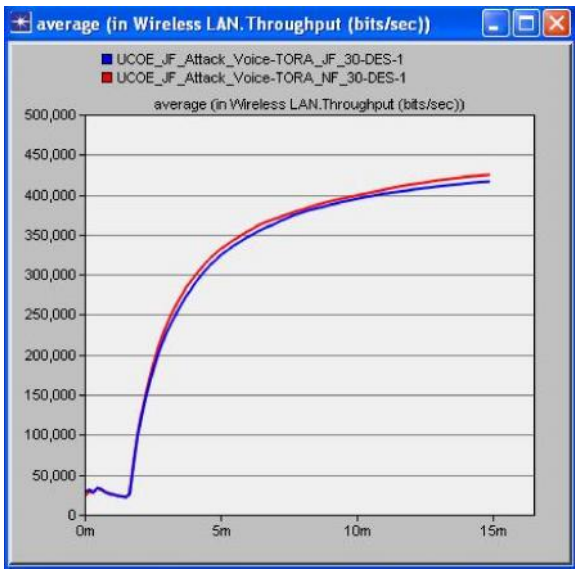
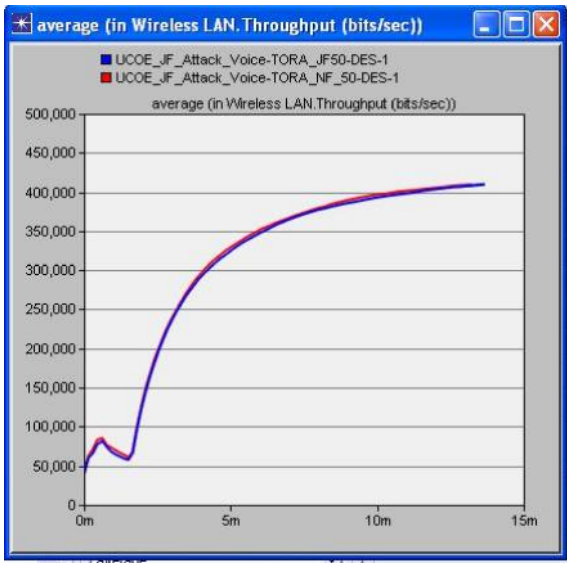


Figure 12: Throughput (bits/sec) 50 Nodes (TORA)



Figures 11 and 12 also shows the throughput of the network TORA, i.e., 30 and 50 nodes. According to Figure 7, normal flow

network has the good results but in case of 50 nodes, both scenarios have the equal results.

CONCLUSION

In this paper, we studied Jellyfish: delay variance attack that they are expected to forward, in a way that leads astray end-to-end congestion control protocols. This attack is protocol-compliant and yet has a devastating impact on the throughput of closed-loop flows, such as TCP flows and congestion-controlled UDP flows. It showed that, perhaps surprisingly, such attacks can actually increase the capacity of ad hoc networks as they will starve all multihop flows and provide all resources to one-hop flows that cannot be intercepted by Jellyfis. As such a partitioned system is clearly undesirable; we also consider fairness measures and the mean number of hops for a received packet, as critical performance measures for a system under attack. A well and good monitoring mechanism must be implemented in the MANET nodes in order to identify and isolate the selfish nodes from the network.

REFERENCES

1. Anipakala Suresh (2005), "Performance Analysis of Ad hoc On-Demand Distance Vector Routing", (AODV) Using OPENT Simulator, Communication Networks, April 11, University of Bremen, Bermen.
2. Chenna Reddy P and Sekhar Reddy P (2006), "Performance Analysis of Adhoc Routing Protocols", *IEEE*.
3. Kumar S and Sengupta J (2010), "AODV and OLSR Routing Protocols for Wireless Ad-hoc and Mesh Networks", 1st IEEE International Conference on Computer and Communication Technology (ICCCT), September 17-19, at MNNIT Allahabad.
4. Mehmud Abliz (2011), "Internet Denial-of-Service Attacks and Defense Mechanisms", No. TR-ll-178, March, Univ. Pittsburgh Tech. Rep, Pittsburgh, USA.
5. Md. Anisur Rahman and Alex Talevski (2009), "Performance Measurement of Various Routing Protocols in ad-Hoc Network", *IMECS*, March 18-20, Hong Kong.
6. Mohammad W, Vipin K and Goudar R H (2012), "Comparative Performance Analysis of Routing Protocols in Mobile Ad-Hoc Networks Under JellyFish Attack", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, India.
7. Sakshi Garg and Satish Chand (2014), "Enhanced AODV Protocol for Defence Against JellyFish Attack on MANETs", *IEEE*.