International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Analysis of AODV and TORA under DDoS Attack in MANETs

Sachin Garg

Punjabi University, Patiala, India

Abstract: ***Wireless networks are gaining popularity day by day, as users want wireless connectivity irrespective of their geographic position. There is an increasing threat of malicious nodes attacks on the Mobile Ad-hoc Networks (MANET). Distributed denial of service attack is one of the security threat in which is used to make the network resources unavailable. The distributed denial of service (DDoS) attack is launched from various attacking nodes, hence called DDoS. DDoS is an improved form of denial of service attack. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed. An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration. Two popular MANET routing protocols like Ad Hoc On-Demand Distance Vector Routing (AODV) and Temporally Ordered Routing Algorithm (TORA) have been implemented. The scope of this thesis is to study the effects of DDoS attack in MANET using both Ad-Hoc on Demand Distance Vector (AODV) and Temporally Ordered Routing Algorithm (TORA). Comparative analysis of DDoS attack for both protocols is taken into account. The impact of DDoS attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements were taken in the light of throughput, end-to-end delay, network load and various other parameters. In this project an attempt has been made to compare the performance of two prominent on-demand reactive routing protocols for mobile ad hoc networks: AODV and TORA, under the normal conditions and DDoS attack situations. The simulation model is created using the Network Simulator 2 (NS-2) with MANET essential configurations and compatible physical layer models are used to study the performance of the AODV and TORA. The On-demand protocol, AODV has performed better than the TORA protocol under the both conditions.. Although AODV and TORA share similar on-demand behavior, the differences in the protocol mechanics can lead to significant performance differentials. The performance differentials are analyzed using normal and attack situations.***

Keywords: Mobile ad-hoc networks, DDoS attack, AODV, TORA, Security

1. Introduction

Mobile Ad Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free to move in and out in a network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, DSR and TORA.

Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources[4].

2. Literature Survey

Tariq A. Alahdal et. al. have worked on performance of Standardized Routing Protocols in Ad-hoc Networks. In this paper, authors study and compare the performance of the

following routing protocols AODV, DSR, DSDV, RAODV, AOMDV, and TORA. The authors have proved that that AOMDV has better performance than AODV and RAODV on the basis of delay. P.Kuppusamy and Dr.K.Thirunavukkarasu have conducted a study and comparison of olsr, aodv and tora routing protocols in ad hoc networks. This research paper describes the characteristics of ad hoc routing protocols OLSR, AODV and TORA based on the performance metrics like packet delivery ratio, end–to–end delay, routing overload by increasing number of nodes in the network. This comparative study proves that AODV, TORA performs well in dense networks than OLSR in terms of packet delivery ratio. Lamyaa M.T. Harb et. al. have conducted a detailed performance analysis of mobile ad hoc networks under attack. The authors have discussed AODV, DSR, TORA and DSDV for MANETs. The authors have addressed the security concerns in MANET operations under the attack situations. Asma Tuteja et. al have performed a comparative performance analysis of dsdv, aodv and dsr routing protocols in manet using ns2. In this paper, authors have compared mobile ad-hoc network routing protocols DSDV, AODV and DSR. The performane of all of the three protocols is compared with teach other to fetch the best performing candidate. The performance analysis has been conuded on the basis of PDR, Throughput, Delay and Routing overhead as performance parameters. Samir R. Das et. al, have worked on the comparative performance evaluation of routing protocols for MANETs. Authors evaluate several routing protocols for mobile, wireless, ad hoc networks via packet level simulations. The protocol suite includes routing protocols specifically designed for ad hoc routing, as well as more traditional protocols, such as link state and distance vector used for dynamic networks. Performance is evaluated with respect to fraction of packets delivered, end-to-end delay and routing load for a given traffic and mobility model. It is observed that the new generation of on-demand routing protocols use a much lower routing load. However the traditional link state and distance vector protocols provide, in general, better packet delivery and delay performance. Gaurav Kumar Gupt and Mr. Jitendra Singh have presented a paper on DDoS Attack in mobile ad-hoc networks. In this paper authors has evaluated that How to thwart the DoS attacks differently and effectively and keep the vital security-sensitive ad hoc networks available for its intended use is essential.

3. Experimental Design

This research project analyzes the AODV and TORA under Denial of Service and Distributed Denial of Service attacks, which are reactive and hybrid routing protocols respectively in nature. These attacks can result as a long and unexpected service downtime which can affect the cellular networks and businesses at a large, can result in mass losses to the cellular network services companies. To avoid these situation the selection of the existing MANET protocols based on their security mechanism becomes extremely important. Also the existing popular routing protocol has to be improved periodically to avoid the future developments in the security attack mechanisms for MANETs. To make the selection and improvements in the existing protocols it is extremely important to analyze the performance of the existing MANET protocols. The popular MANET protocols in these days are AODV and TORA. In this research we will analyze the performance of these protocols under DoS and DDoS attacks. We will compare these protocols on the basis of **Load, Packet Loss, Delay, Throughput, Packet Delivery Ratio, etc**. These working scenarios has been simulated in NS2 using AODV protocol.

AODV shares DSR's on-demand characteristics in that it also discovers routes on an as needed basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each 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 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. 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.

4. Simulation Model

In the simulation, both AODV and TORA are at first simulated under the normal environment. All of the above mentioned parameters have been obtained from the simulations. AODV comes pre-configured in the Network Simulator 2, where TORA protocol required a patch before running its successfully.

Then both protocols, AODV and TORA have been tested under the distributor denial of service attack. When both protocols undergo the DDoS attack in the simulation, a lot of backend coding had to be written. The DDoS nodes had to be created using various network parameters. To generate the DDoS attack, the nodes has been configured in a way to transmit heavy data loads towards the targeted with tweaked IP headers. The IP headers carry the falsified payload in its header, which is responsible for the resource unavailability on the target node due to the high density of data being received. The latter mentioned parameters have been collected from all of the four simulation sub-sets, i.e. Normal AODV, Normal TORA, AODV under DDoS, TORA under DDoS, etc.

5. The Traffic And Mobility Models

Continuous bit rate (CBR) and Variable bit rate (VBR) traffic sources are used in this simulation. The source-destination pairs are spread randomly over the network. Only 512-byte to 1 Mb data packet rates are used in the current simulation. The number of source-destination pairs and the packet

The mobility model uses the *random waypoint* model in a rectangular field. The field configurations used is: 800 m x 800 m field with 11 nodes. Here, each packet starts its journey from a random location to a random destination with a randomly chosen speed (uniformly distributed between 0–

20 m/s). Once the destination is reached, another random destination is targeted after a pause. The pause time, which affects the relative speeds of the mobiles, is varied. Simulations are run for 10 simulated seconds. Identical mobility and traffic scenarios are used across protocols to gather fair results. The performance metrics chosen for the evaluation of Distributed Denial of Service attack are end-to-end delay, throughput and network load.

The first two metrics are the most important for best-effort traffic. The routing load metric evaluates the efficiency of the routing protocol. Note, however, that these metrics are not completely independent. For example, lower packet delivery fraction means that the delay metric is evaluated with fewer samples. In the conventional wisdom, the longer the path lengths, the higher the probability of a packet drops. Thus, with a lower delivery fraction, samples are usually

Simulation Results of AODV under Normal Circumstances

The AODV has been implemented under the normal conditions. Under the normal conditions, AODV is considered the best protocols among its real-time contenders. The AODV has been simulated with total 11 nodes. The nodes have been divided into four major parts: sender nodes, receiver nodes, end routing nodes, traversing nodes. There are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5.

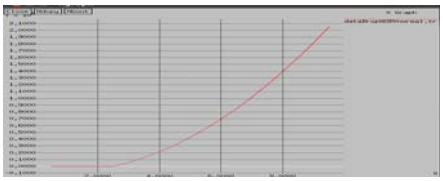

Figure 1: The graph of Data Drop.

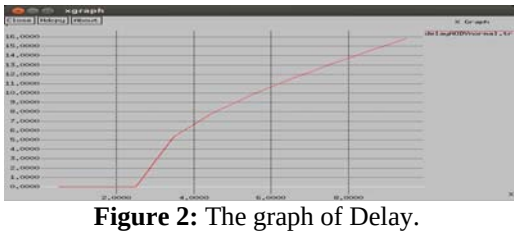

Figure 2: The graph of Delay.

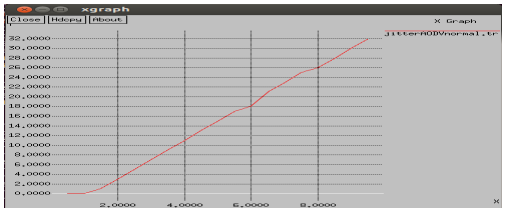

Figure 3: The graph of Jitter.

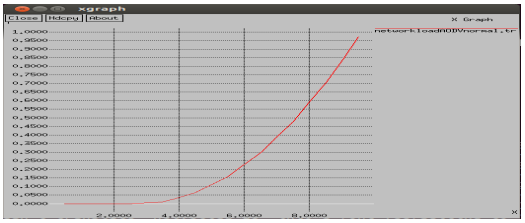

Figure 4: The graph of Network Load

All of the results displayed in this simulation scenario have been recorded on the node 5 from first path. Data drop rate (Figure 5.1) has shown a very good performance of the AODV protocol under MANETs. A minimal data drop rate (2 pps) has been observed in this simulation. Also, the results have shown that a minimum delay (Figure 5.2) has been recorded from the AODV MANET simulation under normal conditions. The maximum delay observed in the simulation touches maximum 16 milliseconds. In the figure 3 and 4, the jitter and network load has been recorded. A usual amount of jitter has been recorded in the AODV simulation under normal conditions. Also the recorded network load also posses the usual performance metric.

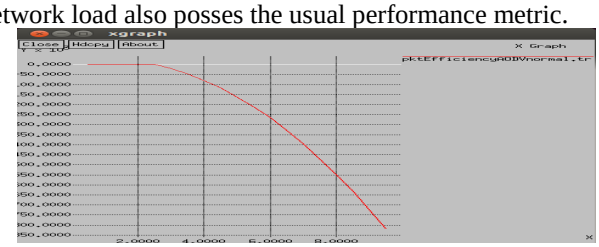

Figure 5: The graph of Packet Efficiency

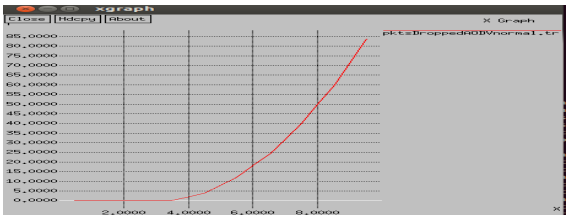

Figure 6: The graph of Packets Dropped

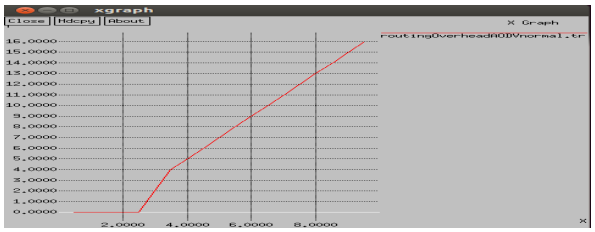

Figure 7: The graph of Routing Overhead

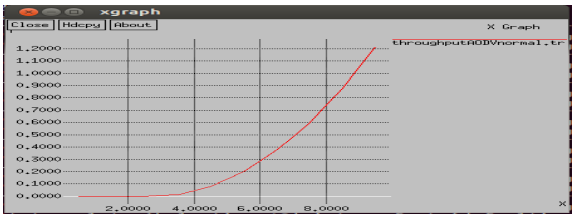

Figure 8: The graph of Throughput

The figure 5 and 6 shows the total number of packets dropped and number of packets sent per second respectively. The total number of packets dropped in the normal simulation of AODV has been observed around 85. Packets sent at the rate of almost 95 packets per second which is a

quite good rate. The latter two properties have shown the effectiveness of the AODV protocol in MANET under normal conditions. Routing overhead and throughput has been shown under the normal MANET over AODV protocol shown in the figure 7 and 8 respectively. The Routing overhead is pretty usual and also, the throughput is quite higher as per usual desired results.

Simulation Results of TORA under Normal Circumstances

The TORA has been implemented under the normal conditions. Under the normal conditions, TORA is considered the best protocols among its real-time contenders. The TORA has been simulated with total 11 nodes. The nodes have been divided into four major parts: sender nodes, receiver nodes, end routing nodes, traversing nodes. Similarly, there are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5.

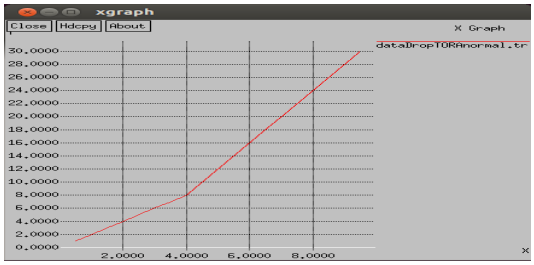

Figure 9: The graph of Data Drop

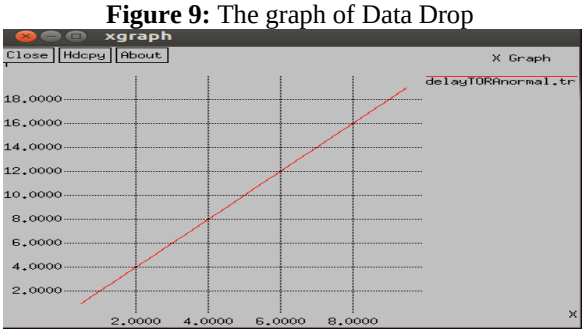

Figure 10: The graph of Delay

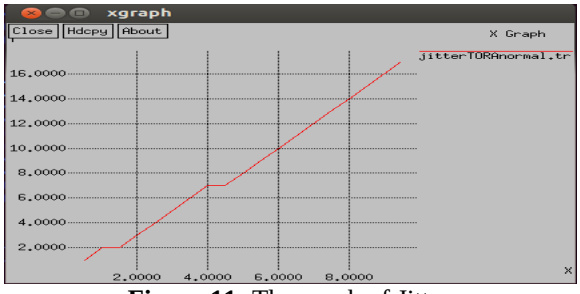

Figure 11: The graph of Jitter

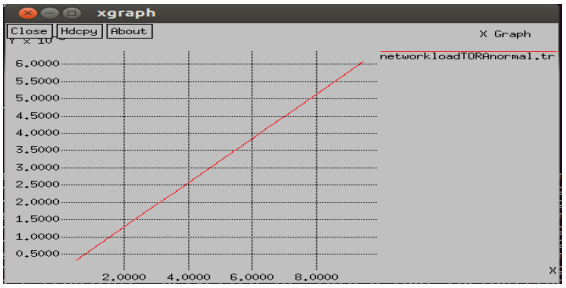

Figure 12: The graph of Network Load

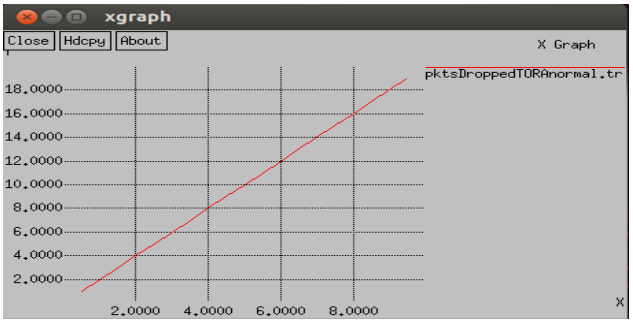

Figure 13: The graph of Packet Dropped

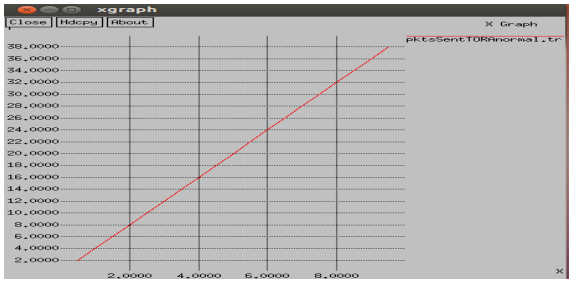

Figure 14: The graph of Packets Sent

Similarly, all of the results displayed in this simulation scenario have been recorded on the node 5 from first path. Data drop rate (Figure 5.1) has shown a very good performance of the TORA protocol under MANETs but It is slightly lower than AODV in MANETs. Little higher usual data drop rate (66 ppm) has been observed in this simulation which shows significantly higher than AODV. Also, the results have shown that an optimal delay of 38 milliseconds (Figure 5.2) has been recorded from the TORA in MANET simulation under normal conditions. The maximum delay observed in the simulation ranges between 2 and 38 milliseconds. In the figure 11 and 12, the jitter and network load has been recorded. A usual amount of jitter has been recorded in the TORA simulation under normal conditions. Also the recorded network load also posses the usual performance metric. But the network load and jitter are higher than the AODV under normal situations.

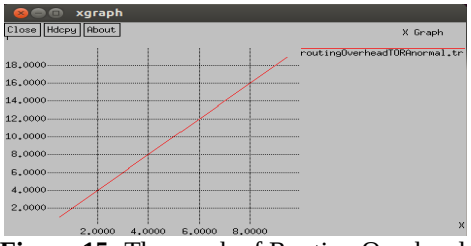

Figure 15: The graph of Routing Overhead

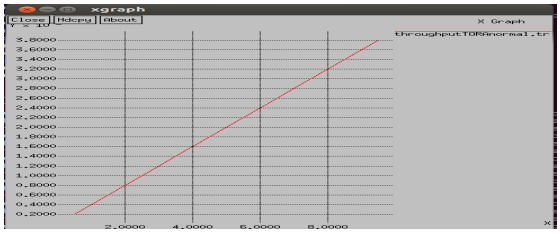

Figure 16: The graph of Throughput

The figure 13 and 14 shows the total number of packets dropped and number of packets sent per second respectively. The total number of packets dropped in the normal simulation of TORA has been observed around 19. Packets sent at the rate of almost 38 packets per second which is a quite good rate. The latter two properties have shown the effectiveness of the TORA protocol in MANET under normal conditions. Routing overhead and throughput has been shown under the normal MANET over TORA protocol shown in the figure 15 and 16 respectively. The Routing overhead is pretty usual and also, the throughput is quite higher as per usual desired results.

6. Simulation Results of AODV under DDoS Attack

Also, the AODV has been implemented under the DDoS attack. Under the distributed denial of service attack, AODV has been tested and compared with TORA as its real-time contender. Similarly, the AODV has been simulated with total 11 nodes. The nodes have been divided into four major parts: sender nodes, receiver nodes, end routing nodes, traversing nodes. There are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5. The nodes 7 and 8 are launching the distributed denial of service attack on the node 1. This move definitely decreases the performance of AODV. But in this simulation, we had to test the results of AODV and TORA under normal conditions and under DDoS attack.

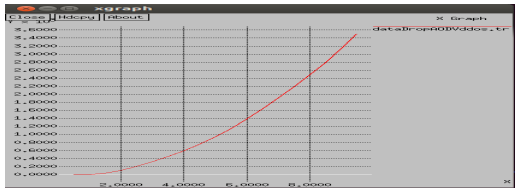

Figure 17: The graph of Data Drop

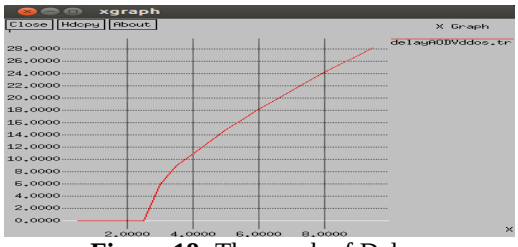

Figure 18: The graph of Delay

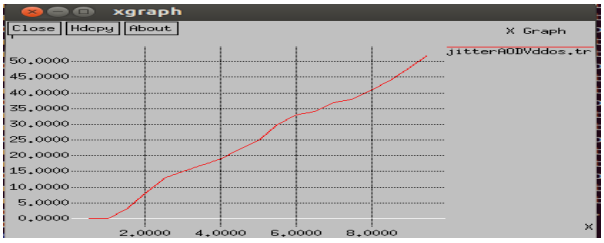

Figure 19: The graph of Jitter

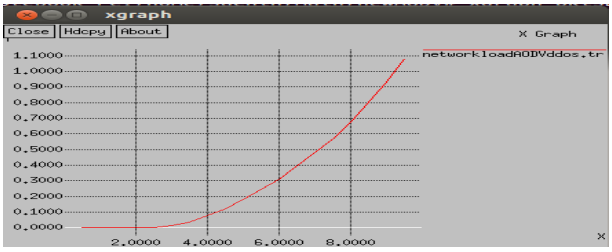

Figure 20: The graph of Network Load

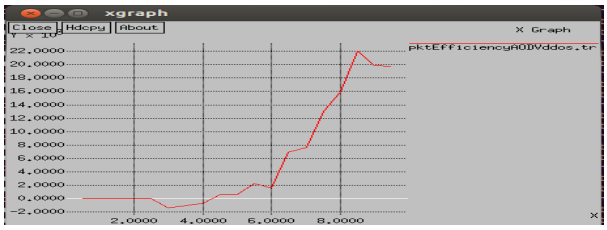

Figure 21 : The graph of Packet Efficiency

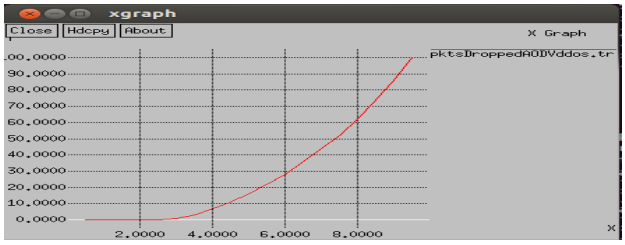

Figure 22: The graph of Packets Dropped

All of the results displayed in this simulation scenario have been recorded on the node 5 from first path. Data drop rate (Figure 5.1) has shown a very good performance of the AODV protocol under attack MANETs. A higher data drop rate (60 ppm) has been observed in this simulation with DDoS attack. Also, the results have shown that a higher delay of almost 29 milliseconds (Figure 5.2) has been recorded from the AODV MANET simulation under DDoS attack. The maximum delay observed in the simulation touches maximum 29 milliseconds and ranges between 0 to 29 milliseconds. In the figure 17 and 18, the jitter and network load has been recorded. A high jitter and high network load has been recorded in the AODV simulation under DDoS attack. Also the recorded network load and jitter shown a significant decrease in the performance of MANET with AODV.

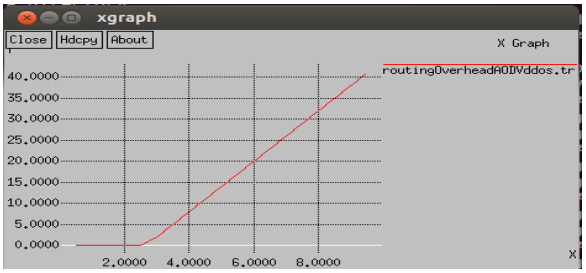

Figure 23: The graph of Routing Overhead

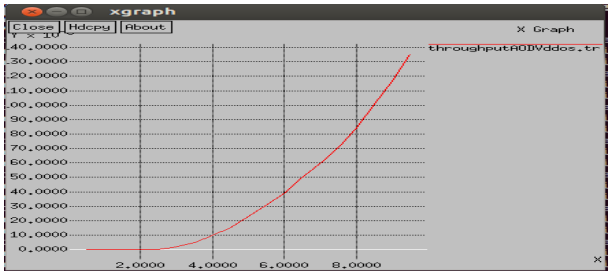

Figure 24: The graph of Throughput

The figure 21 and 22 shows the total number of packets dropped and number of packets sent per second respectively. The total number of packets dropped in the simulation with DDoS attack configured with AODV has been observed around 100. Packets sent at the rate of almost 105 packets per second which is due to the packet flooding done by the DDoS attacker in the MANET cluster in this simulation. The latter two properties have shown the effectiveness of the AODV protocol to handle the network under the DDoS attack in MANETs. Routing overhead and throughput has been shown under the DDoS attack MANET over AODV protocol shown in the figure 23 and 24 respectively. The Routing overhead is recorded at higher rate and also, the throughput is significantly higher than the usual and desired results recorded in the normal AODV or TORA simulations.

7. Simulation Results of TORA Under DDoS Attack

Also, the TORA protocol also has been implemented in NS2 under the DDoS attack. Under the distributed denial of service attack, TORA has been thoroughly tested and compared with TORA in normal conditions and AODV under DDoS attack as its real-time contender. TORA simulation is using the similar topology as the latter ones. Total 11 numbers of nodes has been simulated in the simulation. Each node functions according to following four categories: sender nodes, receiver nodes, end routing nodes, traversing nodes. There are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5. The nodes 7 and 8 are launching the distributed denial of service attack on the node 1. This is pretty sure that DDoS attack has a definite tendency towards a decrease in the performance of TORA. But in this simulation, we had to test the results of TORA under normal conditions and under DDoS attack with each other and with AODV under DDoS attack.

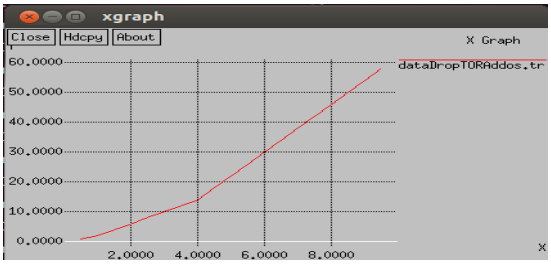

Figure 25: The graph of Data Drop

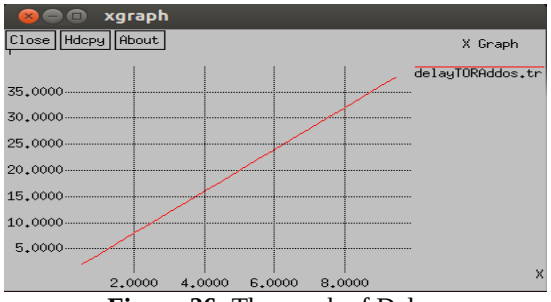

Figure 26: The graph of Delay

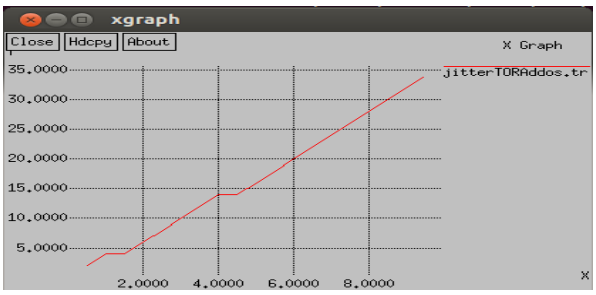

Figure 27: The graph of Jitter

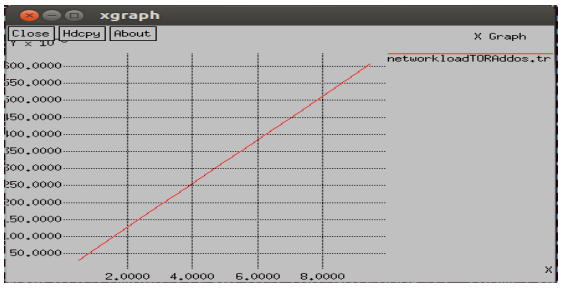

Figure 28: The graph of Network Load

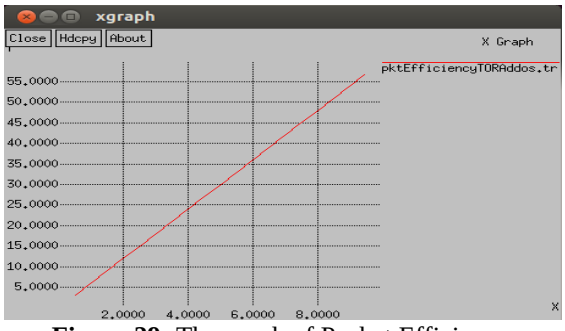

Figure 29: The graph of Packet Efficiency

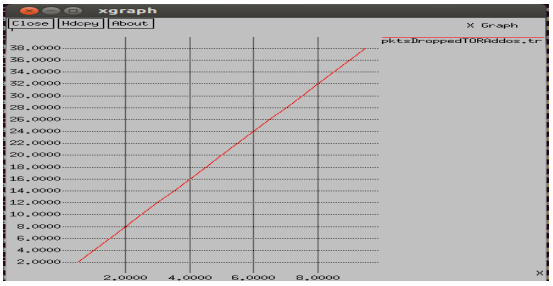

Figure 30: The graph of Packets Dropped

All of the results displayed in this simulation scenario have been recorded on the node 5 from first path. Data drop rate (Figure 25) has shown poor performance of the TORA protocol under attack situations in the MANETs. A higher data drop rate has been recorded in this simulation where TORA is under DDoS attack. Also, the results have shown that a higher delay of almost 70 milliseconds (Figure 5.2) has been recorded from the TORA MANET simulation under DDoS attack. The maximum delay observed in the simulation touches maximum 70 milliseconds and ranges between 3 to 70 milliseconds. In the figure 27 and 28, the jitter and network load has been recorded. A higher jitter and higher network load has been recorded in the TORA simulation under DDoS attack. Also the recorded network load and jitter shown a significant decrease in the performance of MANET with TORA. TORA performance on the basis of these four performance properties shows the poor performance in comparison with AODV under attack in MANETs.

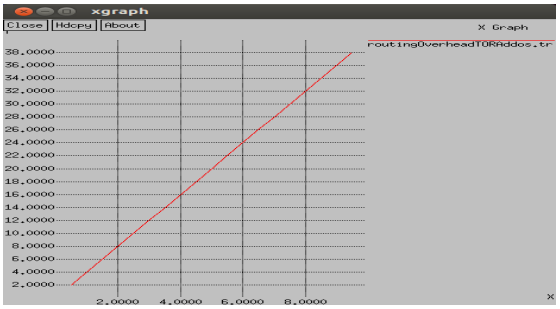

Figure 31: The graph of Routing Overhead

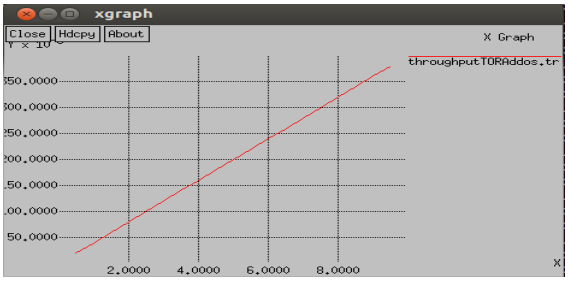

Figure 32: The graph of Throughput

The figure 29 and 30 shows the total number of packets dropped and number of packets sent per second respectively. The total number of packets dropped in the simulation with DDoS attack configured with TORA has been observed very high whereas, Packets sent at the rate of almost 21 packets per second which is very slow and reason behind it is the packet flooding done by the DDoS attacker in the MANET cluster in this simulation. The latter two properties have shown the effectiveness of the TORA protocol to handle the network under the DDoS attack in MANETs. Routing overhead and throughput has been shown under the DDoS attack MANET over TORA protocol shown in the figure 31 and 32 respectively. The Routing overhead is recorded at very higher rate and also, the throughput is pretty higher than the AODV under attack and TORA and AODV under normal situations results.

8. Conclusion

In this research, the performance evaluation survey has been performed on AODV and TORA protocols. Both of the protocols have been tested under the normal and attack situations in MANET environments using Network Simulator -2 (NS-2). The protocol performance has been evaluated on the basis of various parameters such as, delay, network load, packet drop rate, total no. of packets sent, throughput, etc.

Total 11 numbers of nodes has been simulated in the simulation. Each node functions according to following four categories: sender nodes, receiver nodes, end routing nodes, traversing nodes. There are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5. The nodes 7 and 8 are launching the distributed denial of service attack on the node 1. This is pretty sure that DDoS attack has a definite tendency towards a decrease in the performance of TORA. But in this simulation, we had to test the results of TORA under normal conditions and under DDoS attack with each other and with AODV under DDoS attack. All of the simulations have been simulated with total 11 nodes. The nodes have been divided into four major parts: sender nodes, receiver nodes, end routing nodes, traversing nodes. There are total two paths between the sender nodes and receiver nodes. First Path consisted of the end nodes 7 and 8, followed by end routing node 0, which is connected to other end node 5 via nodes 1 and 2 to reach node 6. Whereas, the second path consisted of everything similar expect the two nodes 1 and 2. Instead of nodes 1 and 2 there are nodes 3 and 4 traversing nodes have been used to connect end nodes 0 and 5. The observed results of both of the TORA simulation have shown that TORA under normal conditions has worked far better than TORA under DDoS attack. Similarly, AODV under normal conditions has performed way better than AODV under DDoS attack. When the results of AODV and TORA, both under normal situations have been compared, the AODV has been observed as the better candidate in comparison with TORA under the normal simulation. It means the AODV protocol is recommended for the MANETs, where the probability of attack is lesser or no attack. The AODV and TORA under DDoS attack results have shown that TORA is the poor performer than the AODV. The AODV is observed effective to handle the MANETs under situation of DDoS attack. In both scenarios, the AODV has been observed as the perfect candidate out of the two compared.

9. Future Work

In future, the new security mechanisms against DDoS, balckhole or other variant of DDoS (like selective jamming attack, packet dropping attack, etc.) AODV or TORA can proposed. Also, the best considered AODV protocol can be compared with the other candidate protocols used for MANET simulations. AODV or TORA, or both of them can be compared with more protocols or with each other under different conditions in MANETs or other environments.

References

[1] Tariq A. Alahdal, Saida Mohammad, “Performance of Standardized Routing Protocols in Ad-hoc Networks”, ICCEEE, vol. 1, pp. 23-28, IEEE, 2013.
[2] P.Kuppusamy, Dr.K.Thirunavukkarasu, ” A Study and Comparison of OLSR, AODV and TORA Routing Protocols in Ad Hoc Networks”, pp. 143-147, IEEE, 2011.
[3] Lamyaa M.T. Harb, Dr. M. Tantawy, Prof. Dr. M. Elsoudani, ”PERFORMANCE OF MOBILE AD HOC NETWORKS UNDER ATTACK”, pp. 1201-1206, IEEE 2013.
[4] Asma Tuteja et. al, “Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2”, ICACE, pp. 330-333, IEEE 2010.
[5] Samir R. Das et. al, “Comparative Performance Evaluation of Routing Protocols for Mobile, Ad hoc Networks”, ICCCN, pp. 153-161, IEEE, 1998.
[6] Jaya Jacob et. al, “ Performance Analysis and Enhancement of Routing Protocol in Manet”, vol. 2, issue 2, pp. 323-328, IJMER, 2012.
[7] Anuj K. Gupta, Dr. Harsh Sadawarti, “Performance analysis of AODV, DSR & TORA Routing Protocols”, IACSIT, vol. 2, no. 2, vol. 226-231, IJET, 2010.
[8] Anu Bala, Munish Bansal, Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, ICNC, vol. 1, pp. 141-145, IEEE 2009.
[9] Gaurav Kumar Gupt, Mr. Jitendra Singh, “Truth of D-DoS Attacks in MANET”, vol. 10, issue 15, GJCST 2010.