INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue4)

Available online at: www.Ijariit.com

A Survey over the Critical Performance Analytical Study of the MANET Routing Protocols (AODV & TORA)

Manju[1]
Research Scholar, DIET, Kharar
Mrs Maninder kaur[2]
Assistant Professor, DIET, Kharar

ABSTRACT—The mobile ad-hoc network (MANET) is the ad-hoc technology for the automatic connectivity of the nodes in the network cluster. The MANETs are considered as the infrastructure less technology, which uses the peer-to-peer connectivity mechanism for the establishment of the inter-links between the network nodes. The MANET data is propagated over the paths established through the routing algorithms. There are several routing algorithms, which are primarily segmented in the two major groups, reactive and proactive. The reactive networks are designed to query the path when it's required, whereas the proactive routing protocol constructs the pre-computed route based routing table, which is utilized to propagate the data over the pre-derived links/routes. In this paper, the major routing protocols have been evaluated for their performance under the distributed denial of service (DDoS) attacks. The advance on-demand distance vector (AODV) and temporally ordered routing algorithm (TORA) protocols, which are considered as one of the best protocols. This paper focuses upon the assessment of the best routing protocol under the DDoS attack over the MANETs. The security and vulnerability analysis of the routing protocols plays the vital role in the security enhancement of the aimed routing protocols. The security evaluation has been based upon the targeted protocols based upon the various factors.

KEYWORDS: Security Analysis, Vulnerability analysis, distributed denial of service (DDoS) attack, MANET Routing.

I. INTRODUCTION

Mobile spontaneous Networks are autonomous and sub-urbanized wireless systems. MANETs include mobile nodes that are liberated to move in and move into a network. Nodes are the systems or devices i.e. itinerant, laptop, personal digital help, MP3 player and private laptop that are collaborating within the network and are mobile. These nodes will act as host/router or each at a similar time. They 'll kind whimsical topologies looking on their property with one another within the network. These nodes have the flexibility to tack together themselves and since of their self configuration ability, they'll be deployed desperately while not the necessity of any infrastructure. Net Engineering Task Force (IETF) has painter social unit (WG) that's devoted for developing scientific discipline routing protocols. Routing protocols is one in all the difficult and attention-grabbing analysis areas. Several routing protocols are developed for MANETS, i.e. AODV, DSR and TORA.

Security in Mobile spontaneous Network is that the most significant concern for the essential practicality of network. The provision of network services, confidentiality and integrity of the information is achieved by reassuring that security problems are met. MANETs typically suffer from security attacks due to its options like open medium, dynamic its topology dynamically, lack of central watching and

management, cooperative algorithms and no clear defense mechanism. These factors have modified the battle field scenario for the MANETs against the protection threats. The MANETs works while not a centralized administration wherever the nodes communicate with one another on the idea of mutual trust. These characteristic makes MANETs additional at risk of be exploited by associate wrongdoer within the network. Wireless links additionally makes the MANETs additional vulnerable to attacks, that builds it easier for the wrongdoer to travel within the network and find access to the continuing communication. Mobile nodes gift within the variation of wireless link will catch and even participate within the network.

MANET should have a secure manner for transmission and communication and this can be a quite difficult and important issue as there has been increasing threats of attack on the Mobile Networks. Security is that the cry of the day. So as to supply secure communication and transmission, the engineers should perceive differing types of attacks and their effects on the MANETs. Hole attack, part attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (dos), ungenerous node misbehaving, impersonation attack are quite attacks that a painter will suffer from. A painter is additional hospitable these sorts of attacks as a result of communication relies on mutual trust between the nodes, there's no central purpose for network management, no authorization facility, smartly dynamic topology and restricted resources[4].

II. LITERATURE SURVEY

Tariq A. Alahdal et. Al. Have worked on performance of Standardized Routing Protocols in Ad-hoc Networks. Throughout this paper, authors study and compare the performance of the next routing protocols AODV, AOMDV, DSDV, DSR, RAODV and TORA. The authors have established that that AOMDV has higher performance than AODV and RAODV on the thought of delay. Lamyaa M.T. Harb et. Al. Have conducted a detailed performance analysis of mobile sudden networks vulnerable. The authors have mentioned AODV, DSR, TORA and DSDV for MANETs. The authors have addressed the security problems in painter operations beneath the attack things. P.Kuppusamy and Dr.K.Thirunavukkarasu have conducted a study and comparison of olsr, aodv and tora routing protocols in sudden networks. This analysis paper describes the characteristics of sudden routing protocols OLSR, AODV and TORA supported the performance metrics like packet delivery relation, end–to–end delay, routing overload by increasing sort of nodes among the network. This comparative study proves that AODV, TORA performs well in dense networks than OLSR in terms of packet delivery relation.

Samir R. Das et. Al, have worked on the comparative performance analysis of routing protocols for MANETs. Authors appraise several routing protocols for mobile, wireless, sudden networks via packet level simulations. The protocol suite includes routing protocols specifically designed for sudden routing, additionally as extra ancient protocols, resembling link state and distance vector used for dynamic networks. Asma Tuteja et. Al have performed a comparative performance analysis of dsdv, aodv and dsr routing protocols in painter using ns2. Throughout 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 different to fetch the only performing arts candidate. The performance analysis has been conuded on the thought of PDR, Throughput, Delay and Routing overhead as performance parameters. Gaurav Kumar Gupt and Jitendra Singh have given a paper on ddos Attack in mobile ad-hoc networks. Throughout this paper authors has evaluated that the thanks to thwart the dos attacks otherwise and effectively and keep the important security-sensitive sudden networks offered for its meant use is very important.

III. FINDINGS OF THE LITERATURE REVIEW

Previously the works done on MANETs targeted chiefly on completely different security threats and attacks akin to dos, ddos, and Impersonation, Wormhole, Sybil, and region attack. Among these attacks region attack concerned in Manet is evaluated supported reactive routing protocol like ad hoc On Demand Distance Vector (AODV) and TORA and its effects are careful by stating however this attack disrupt the performance of Manet. Little or no attention has been given to the very fact to check the impact of Denial of Service attack in Manet utilizing Reactive and Hybrid routing protocols and to check the vulnerability of each these protocols against the attack. There's a desire to handle these varieties of protocols below the attack, furthermore because the impacts of the attacks on the MANETs. This thesis analyzes Denial of Service attack in MANETs utilizing AODV and TORA that are considered reactive and hybrid routing protocols and considered secure & balanced in nature. This research analyzes the AODV and TORA below Denial of Service and Distributed Denial of Service attacks, that are reactive and hybrid routing protocols are balanced and flexible in nature. These attacks may result as a protracted and revolutionary service period of time which might have an effect on the cellular networks and businesses at an oversized segment, may result in mass losses to the cellular network services firms. To avoid these state of affairs the choice of the

prevailing Manet protocols supported their security mechanism becomes extraordinarily necessary. Additionally the present standard routing protocol needs to be improved sporadically to avoid the longer term developments within the security attack mechanisms for MANETs. To form the choice and enhancements within the existing protocols it's extraordinarily necessary to research the performance of the prevailing Manet protocols. The popular Manet protocols in the current development are known as the AODV and TORA. In the existing model's analysis we'll analyze the performance of those protocols below dos and ddos attacks. We'll compare these protocols on the concrete and fundamental parameters of Load, Packet Loss and Delay. These operating eventualities may be simulated in NS2.

IV. METHODOLOGY

This analysis can begin with literature survey of existing MANET standard routing protocol's behavior against Denial of Service attacks. Within the literature study, we are going to study the prevailing MANET routing algorithms like TORA and AODV. The detailed literature study can lead towards the discovery and implementation of the possible improvements over the pre-mentioned MANET routing protocols using the network simulation version 2 (NS-2). It additionally becomes quite vital to conduct a close literature review regarding the performance analyzing parameters. The proposed model simulations would be developed using the various domains of the NS2 simulator. The radical performance and have testing model would be produced and used to investigate the performance of the MANET routing protocol (TORA, AODV and DSR) beneath the Denial of Service attack.

V. COMPARATIVE STUDY

The comparative study between the two routing protocols for the Manets is based upon the performance analytical study of the AODV and TORA protocols. Variable bit rate (VBR) and Continuous bit rate (CBR) traffic sources has been utilized for the performance analytical model of the routing protocols in this simulation. The source-destination pairs are unfolded under the randomized paradigm over the network. Solely 512-byte to one Mb information packet rates are utilized in this simulation. The amount of source-destination pairs and therefore the packets are exchanged between the defined source and destination in the simulation model. The quality model uses the random waypoint model during a rectangular field. The sector or cluster configurations used is: 800 m x 800 m field with eleven nodes. Here, every packet starts its journey from a random location to a random destination with a every which way chosen speed (uniformly distributed between 0–20 m/s). Once the destination is reached, another random destination is targeted when a stoppage. The pause time, that affects the relative speeds of the mobiles, is varied. Simulations are endure ten simulated seconds. Identical quality and traffic situations are used across protocols to assemble genuine results.

VI. COMPARATIVE RESULTS

Also, the AODV has been enforced beneath the DDoS based flooding attacks. Beneath the distributed denial of service attack, AODV has been tested and compared with TORA as its period challenger. Similarly, the AODV has been simulated with total eleven nodes. The nodes are divided into four major parts: sender nodes, receiver nodes, finish routing nodes, traversing nodes. There are complete and total 2 multiple data propagation paths between the sender nodes and receiver nodes. Initial Path consisted of the tip nodes seven and eight, followed by finish routing node zero, that is connected to alternative finish node five via nodes one and a pair of to succeed in node half-dozen. Whereas, the second path consisted of everything similar expect the 2 nodes one and a pair of. Rather than nodes one and a pair of there are the nodes three and four traversing nodes are accustomed connect finish nodes zero and five. The nodes seven and eight area unit launching the distributed denial of service attack on the node one. This move undoubtedly decreases the performance of AODV. However during this simulation, we tend to had to check the results of AODV and TORA beneath traditional conditions and beneath DDoS based flooding attacks.

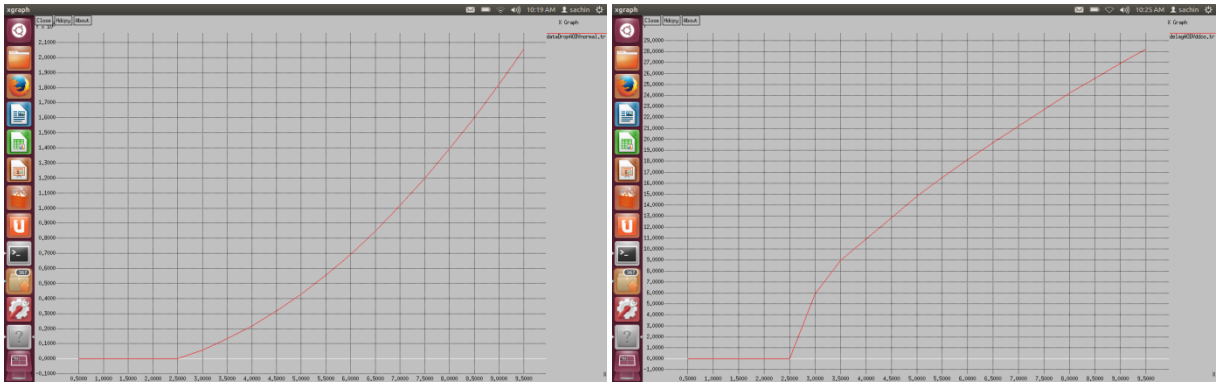

Figure 5.1 (a) and (b): Evaluation of the Data Drop (a) and Transmission Delay (b) under the AODV protocol over the MANETs

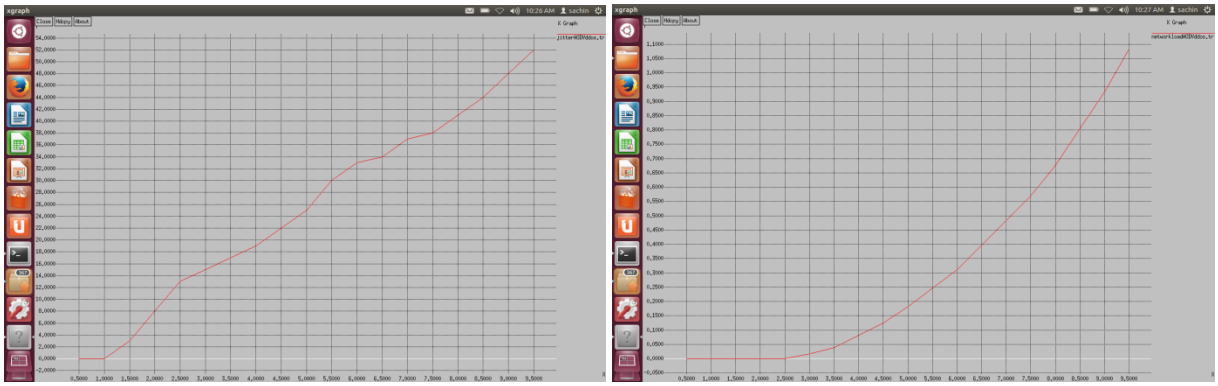

Figure 5.2 (a) and (b): Evaluation of the Jitter (a) and Network Load (b) under the AODV protocol over the MANETs

TORA simulation is exploring the similar topology because the latter ones. Total eleven numbers of nodes has been simulated within the simulation. Each and every node functions in the accordance with the following four categories: sender nodes, receiver nodes, terminal routing nodes, traversing nodes. There are total 2 ways between the sender nodes and receiver nodes. Initial Path consisted of the top nodes seven and eight, followed by finish routing node zero, that is connected to different finish node five via nodes one and a couple of to achieve node half-dozen. Whereas, the second path consisted of everything similar expect the 2 nodes one and a couple of. Rather than nodes one and a couple of there are nodes three and four traversing nodes are accustomed connect finish nodes zero and five. The nodes seven and eight are considered launching the distributed denial of service attack on the node one. This is often pretty certain that DDoS based flooding attack incorporates a definite tendency towards a decrease within the performance of TORA. However during this simulation, we tend to had to check the results of TORA below traditional conditions and below DDoS based flooding attack with one another and with AODV below DDoS based flooding attacks.

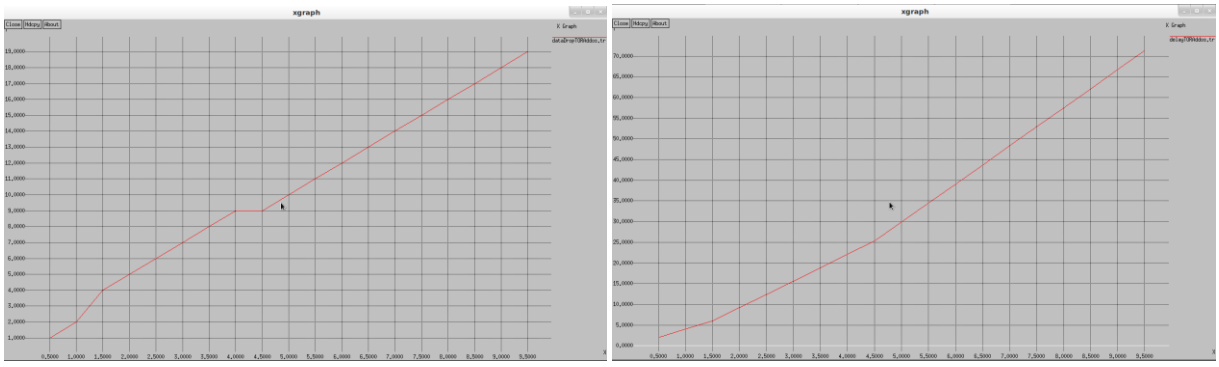

Figure 5.3 (a) and (b): Evaluation of the Data Drop (a) and Transmission Delay (b) under the AODV protocol over the MANETs

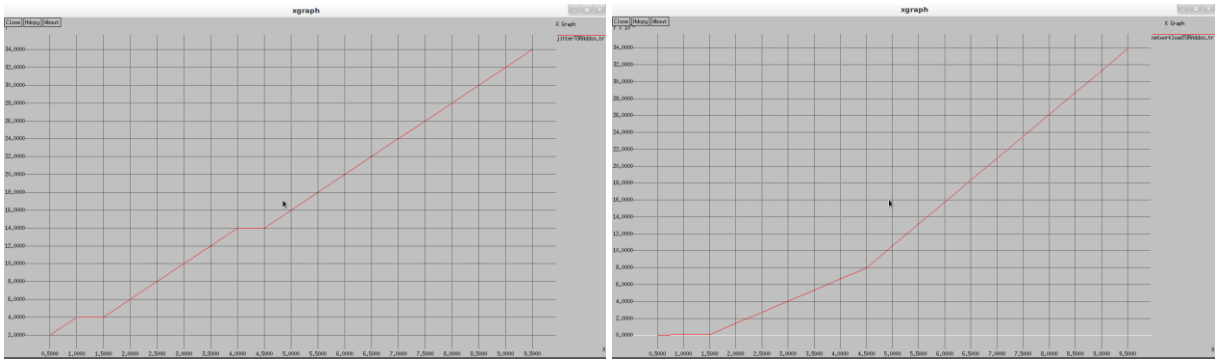

Figure 5.4 (a) and (b): Evaluation of the Jitter (a) and Network Load (b) under the AODV protocol over the MANETs

VII. CONCLUSION

The scope of this thesis is to check the results obtained from the DDoS based jamming attacks over the MANETs running over AODV and TORA protocols. The comparative study for the evaluation of DDoS has been individually studied over each of the routing in focus. The overall impact of the DDoS based service jamming attack on the MANET network is evaluated for the assessment and impact of the attack over the data propagation based performance parameters. The measurements have been taken within the computationally light-weighted turnout (throughput), transmission delay, overall jitter and network load. During this project an effort has been created to check the performance of 2 distinguished on-demand reactive routing protocols for mobile unexpected networks: AODV and TORA, underneath the traditional conditions and DDoS based service jamming attacks. The simulation model is formed by designing and utilizing the simulation model in the NS-2 simulator with all essential MANET parameters for performance study of the AODV and TORA protocols. The On-demand protocol, AODV has performed higher than the TORA protocol underneath all of the conditions. Though AODV and TORA share similar on-demand behavior, the variations within the protocol mechanics will cause important performance differentials. The performance differentials are analyzed victimization traditional and attack things. The AODV protocols have been found better than the TORA protocols under our performance analytical study of these two primary protocols.

REFERENCES

[1] Anu Bala, Munish Bansal, Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, ICNC, vol. 1, pp. 141-145, IEEE 2009.

[2] Anuj K. Gupta, Dr. Harsh Sadawarti, “Performance analysis of AODV, DSR & TORA Routing Protocols”, IACSIT, vol. 2, no. 2, vol. 226-231, IJET, 2010.

[3] Asma Tuteja et. al, “Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2”, ICACE, pp. 330-333, IEEE 2010.

[4] Gaurav Kumar Gupt, Mr. Jitendra Singh, “Truth of D-DoS Attacks in MANET”, vol. 10, issue 15, GJCST 2010.

[5] Jaya Jacob et. al, “ Performance Analysis and Enhancement of Routing Protocol in Manet”, vol. 2, issue 2, pp. 323-328, IJMER, 2012.

[6] Lamyaa M.T. Harb, Dr. M. Tantawy, Prof. Dr. M. Elsoudani, ”PERFORMANCE OF MOBILE AD HOC NETWORKS UNDER ATTACK”, pp. 1201-1206, IEEE 2013.

[7] 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.

[8] Samir R. Das et. al, “Comparative Performance Evaluation of Routing Protocols for Mobile, Ad hoc Networks”, ICCCN, pp. 153-161, IEEE, 1998.

[9] Tariq A. Alahdal, Saida Mohammad, “Performance of Standardized Routing Protocols in Ad-hoc Networks”, ICCEEE, vol. 1, pp. 23-28, IEEE, 2013.

