International Journal of Engineering & Technology, 4 (2) (2015) 390-398
www.sciencepubco.com/index.php/IJET

doi: 10.14419/ijet.v4i2.4609
Research Paper

MANETs performance analysis with dos attack at different routing protocols

Alaa Zain [1]*, Heba A. El-Khobby [2], Hatem M. Abd Elkader [3], Mustafa M. Abdelnaby [4]

[1] Dep. Electronics and communication Eng., E-JUST, Alexandria, Egypt
[2] Dep. of Electronics and Electrical communication Eng., Faculty of engineering, Tanta University, Tanta, Egypt
[3] Dept. of Information Systems, Information and Technology Institute, Menoufia University, Menoufia, Egypt
[4] Dep. of Electronics and Electrical communication Eng., Faculty of engineering, Tanta University, Tanta, Egypt
**Corresponding author E-mail: alaazain1986@gmail.com*

Abstract

A Mobile Ad-Hoc Networks (MANET) is widely used in many industrial and people's life applications, such as earth monitoring, natural disaster prevention, agriculture biomedical related applications, and many other areas. Security threat is one of the major aspects of MANET, as it is one of the basic requirements of wireless sensor network, yet this problem has not been sufficiently explored. The main purpose of this paper is to study different MANETs routing protocols with three scenarios of Denial of Service (DoS) attacks on network layer using proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocols like Ad hoc On-Demand Distance Vector (AODV), Hybrid routing protocols like Geographic Routing Protocol (GRP). Moreover, a comparative analysis of DoS attacks for throughput, Data loss, delay and network load is taken into account. The performance of MANET under the attack is studied to find out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The simulation is done using OPNET 17.

Keywords: *MANET; Routing Protocols; DoS Attacks; AODV; OLSR.*

1. Introduction

A MANET is exposed to various types of attacks, because they are decentralized and distributed in nature, communication takes place via multi-hop intermediate nodes low battery power supply, limited bandwidth support, operations using wireless communication, multi-hop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks [1]. Previously, the works done on security issues in MANET were based on reactive routing protocol like AODV. Different kinds of attacks types were studied, and their effects on the performance analysis of MANET [2]. Unlike traditional networks in MANET, routing functions are performed by dedicated nodes, and routing functions are carried out by all available nodes. Due to the nature of the network, the vulnerability of the links, the limited physical protection of each of the mobile nodes, the absence of certification authority and the lack of a centralized monitoring or management point make security goals difficult to achieve [3], [4]. DoS is produced by unexpected nodes failure or malicious action. This attack is a dangerous vulnerable to most networks. Sensor networks being very energy-sensitive and battery resource-limitation. Wood and Stankovic at explored various types of DoS attacks that may happen in every network layers of MANET [5]. The DoS attack tries to exhaust the resources available in the network, by sending extra unnecessary packets and so prevents network users from accessing services or use the resources to which they are deserved. DoS attack is not only for the attackers attempt to devastate, obstruct, or damage a network, but also for any event that diminishes a network's capability to provide a service [6-8]. In MANET, several types of DoS attacks might be carried out in different layers. At physical layer the DoS attacks could be jamming and tampering, at link layer collision, exhaustion, flooding, unfairness, at network layer, neglect and greed, misdirection, black holes, gray holes and at a transport layer, this attack could be performed by malicious flooding and de-synchronization. The paper is organized as follows. Section 2 presents the classification of MANETS routing protocols.

Section 3 explains different types of attacks on MANET. DoS attacks are reviewed in section 4 followed by other attacks on MANET in section 5, section 6, we create modeling of network on OPNET after that we explain the simulation setup in section VII. Results and statistics are shown in sections 7, Finally we draw conclusions about impact on DoS attacks on MANET at section 8.

2. Classification of MANETs routing protocols

Routing protocols in MANETs are classified into three different categories according to their functionality; reactive protocols, proactive protocols and hybrid protocols as shown in Fig.1. Reactive (on-demand) routing has the advantages that eliminate periodic updates and adaptive to network dynamics. Reactive routing protocols have the disadvantages that it is a high flood-search overhead with mobility, distributed traffic and high route acquisition latency. Reactive routing protocols are like Dynamic Source Routing (DSR) and AODV routing protocol. DSR has cooperative nodes; it is relatively small network diameter (5-10 hops), Detectable packet error and unidirectional or bidirectional link promiscuous mode. AODV routing protocol has the feature source floods route request in the network; reverse paths are formed when a node hears a route request.

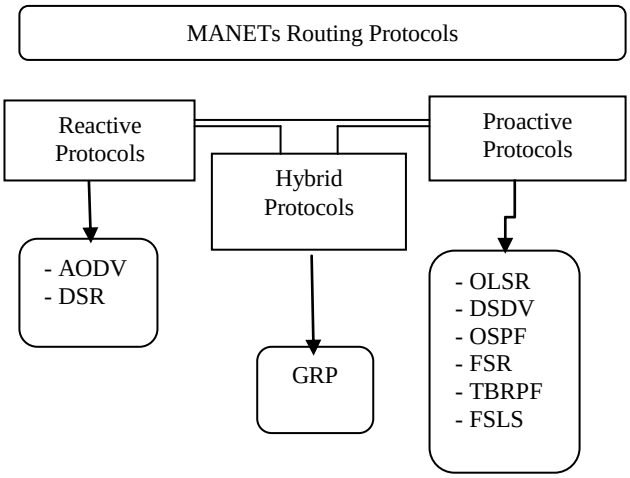

Fig. 1: Manets Routing Protocols

The first difference between AODV and DSR is that in DSR each packet carries full routing information, whereas in AODV the packets carry the destination address. This means that AODV has potentially less been routing overheads than DSR [9]. The second difference is that in AODV, the route replies to only carry the destination IP address and the sequence the route replies, whereas in DSR the route replies carry the address of every node along the route number [10].

Proactive routing protocols are traditional distributed shortest path protocols based on periodic updates and high routing overhead. Proactive Routing protocols are like: Link state Fish-Eye Routing, OLSR and table drive: Destination-Sequenced Distance Vector (DSDV).

Hybrid routing protocols are a new generation of protocol, which are both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form somesort of a backbone to reduce the route discovery overheads. The advantage of these protocols is that it has significantly reduced the amount of communication overhead when compared to be pure proactive protocols, and also it allows fast routing discovered which reduce the delays associated with reactive protocols such as DSR [11]. Hybrid routing protocols like Geographic Routing Protocol (GRP). GRP is a position based protocol routing protocol. In GRP, the Global Positioning System (GPS) has a function to locate the location of node to collects network information and thee quadrants optimize flooding. In this routing protocol source, node collects all the information about the route to the designation by sending a query to destination through the network.

3. Type of security attacks

3.1. External and internal attacks

External attacks in which the attacker from out the network aims to cause jamming, wrong routing information or disturb nodes from providing services. Internal attacks in which the attacker wants to access to the network and contribute in the network activities, either by some malicious activities to get the access to the network as a new node, or by using a current node as a basis to conduct its malicious behaviors.

3.2. Passive and active attacks

An active attack attempts to modify or destroy the data in the network. Active attacks can be internal or external attack. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. The internal attacks are more severe and hard to detect than external attacks because attacker is already part of the network. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted [12].

4. Denial of service (DoS)

DoS is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks. MANETs are very energy-sensitive and resource-limitation; they are very vulnerable to DoS attacks. Various DoS attacks are explored that may happen in every network layer of MANET [13]. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In MANETs, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious node.

5. Other attacks on MANET

5.1. Black hole attack

In this type of attack, a malicious node advertises itself as having the shortest path to the destination node. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created [14]. This malicious node then can choose whether to perform a DoS attack by dropping the packets or to use its place on the route as the first step in a man-in-the-middle attack.

5.2. Gray hole attack

In this kind of attack, the malicious node behaves normally in the beginning and reply true RREP messages to the nodes that started RREQ messages [15]. When it receives the packets, it starts dropping the packets and launch DoS attack. The gray hole attacks have deferent scenarios sometimes the attacker node drops the packets for a part of time after that switch to normal mode. This kind of act is difficult to be discovered in the network [16].

5.3. Wormhole attack

In this kind of attack, the attacker gets themselves in distinguished location in the network. They have the shortest path between the nodes. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network .When the attacker nodes create a direct link between each other in the network. This kind of attack scenario is known as out of band wormhole. The other type of wormhole attack is known as in band wormhole attack. In this type of attack, the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker [17].

5.4. Impersonation attack

In MANETs IP and MAC address uniquely identifies the host. These measurements are not enough to authenticate sender .In this attack, the malicious node hides its IP address and uses another IP address in the network; this is known as spoofing [18].

5.5. Routing table overflow attack

In this kind of attack, malicious node tries to create routes to nonexistent nodes to the authorized nodes present in the network. It can simply send excessive route advertisements to overflow the routing table. The goal is to have enough

routes so that creation of new routes is prevented. This attack is usually done against proactive protocols [4]. Proactive routing protocols updates route periodically before even they are required. This is one of the flaws that make proactive protocols vulnerable to the routing table attack [19].

5.6. Jelly fish attack

In this kind of attack, the malicious node produces delay before the transmission and reception of data packets in the network. 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. Jelly fish attack is kind of denial of service attacks, and it is passive attack [20].

5.7. Sleep deprivation torture attack

The nodes operating in MANETs have limited resources, i.e. battery life, the node remains active for transmitting packets during the communication. When communication cease these nodes go back to sleep mode in order to preserve their resources. In this kind of attack, the attacker uses this point of the nodes by making it busy, keeping it awake to drain all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily use the network [21].

5.8. Selfish node attack

In this kind of attack a malicious node doing a routing misbehavior in the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attacks aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attackers the malicious node can sometime drop the packets [22]. When the malicious node sees that the packets need a lot of resources, it is no longer interested in the packets it just simply drops the packets and does not forward it in the network.

6. Modeling of network

We created our network using blank scenario with startup wizard. We selected empty scenario topology and campus as our network scale. Size of the network scale is specified by selecting the X span and Y span in given units. We selected 1000 * 1000 meters as our network size and MANET model in the technologies. After this manual configuration various topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually.

7. Simulation setup

The simulation setup of four scenarios comprising of 16 mobile nodes moving at a constant speed of 10 m/sec as shown in Fig. 2. Total of nine scenarios have been developed, all of them with mobility of 10 m/s. Number of malicious nodes were varied, and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024). The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 m/sec and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only. Our goal was to determine the protocol which shows less vulnerability in case of denial of service attack. We choose AODV, DSR, GRP and OLSR routing protocol, which are reactive and proactive protocols respectively. In case AODV and OLSR, first scenario malicious node buffer size is lowered to a level which increased packet drop. Second scenario there is jamming attack net. The Third scenario is kind of spoofing reply where malicious node send true data but delayed or with a large amount. In fourth scenario we use malicious node broadcasting hello packets with more transmission power than a base station.

Table 1: MANET Traffic Model Parameters.

Number of Nodes	16
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load, packet dropped
Pause time	100 seconds
Mobility (m/s)	10 m/sec
Packet size (bits)	exponential(1024)
Power(W)	0.005
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000

8. Results and statistics

Three types of DOS attack scenarios, and global discrete event statistics (DES) are involved in OPNET 17 simulation. The deference between global and object statistics that global statistic is for entire network's collection of data. Where statistics object involves individual nodes statistics. After the selection of statistics and running the simulation, results are taken and analyzed. In our case, we have used global discrete event statistics (DES).

8.1. Result of the first scenario

The first scenario is a type of DOS on physical layer. Two nodes are malicious they dropped the packets so it is supposed to be type of node destructive attack.

8.1.1. Throughput

From Fig. 2, it is obvious that the throughput for OLSR is high compared to that of GRP. Here the malicious node dropped the data rather than forwarding it to the destination, thus effecting throughput. The same is observed in the case of AODV.

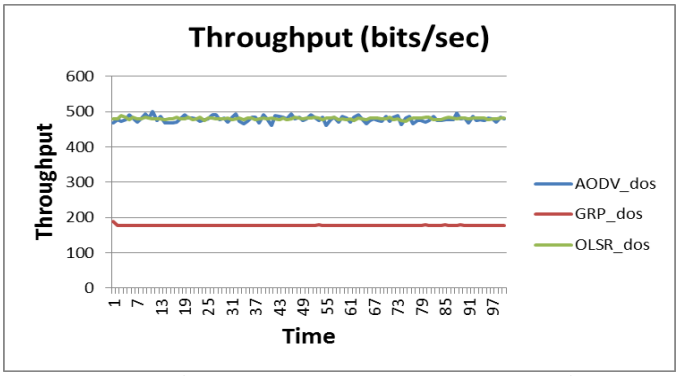

Fig. 2: Throughput of (AODV, GRP and OLSR) with Dos Attack for 16 Nodes.

8.1.2. The network load

The network load graph of OLSR and AODV with DOS attack and without presence of attack has been shown in the Figure 5. The network load of OLSR is much high as compare to AODV and DSR. In case of attack, OLSR has fewer network loads as compare to without attack. However, under attack, it cannot send its packet i.e. packet discarding leads to a reduction of network load. OLSR has a high network load in presence of two malicious nodes as compare to that of AODV. OLSR has a high network loads than AODV as shown in Fig. 4 because the routing protocols are able to adjust its changes in it during node restart and node pausing. This is different at different speeds, at high speeds the routing protocols take much more time for adjusting and afterward sending of traffic to the new routes.
From Fig. 6, it is obvious that the network load for OLSR is high compared to that of GRP. The same is observed in the case of AODV.

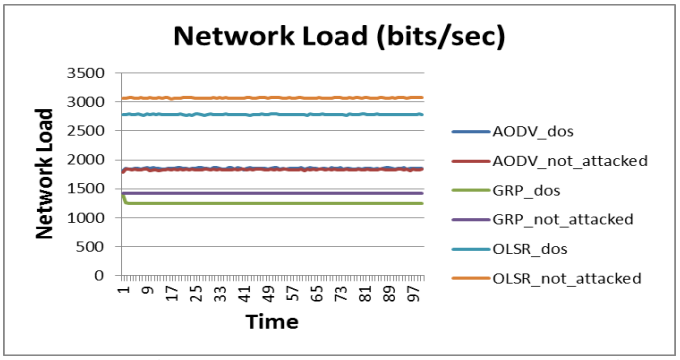

Fig. 3: Network Load of (AODV, GPR and OLSR) with and Without Attack for 16 Nodes.

8.1.3. Data loss

Data dropped in case of DOS attack and without attack depends on the protocol routing. From Fig. 4, it is obvious that the data dropped for OLSR is high compared to that of GRP. The same is observed in the case of AODV.

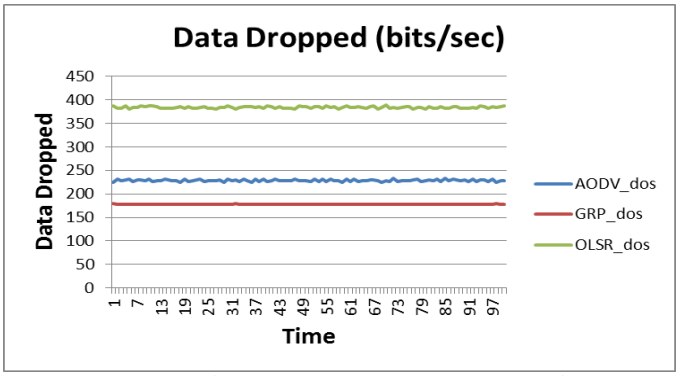

Fig. 4: Network Load of (AODV, GRP and OLSR) with Attack for 16 Nodes.

8.1.4. Packed end to end delay

Packed end to end delay in case of DOS attack and depends on the protocol routing. In Fig. 5, it is obvious that the network load for GRP is high compared to that of OLSR. The same is observed in the case of AODV.

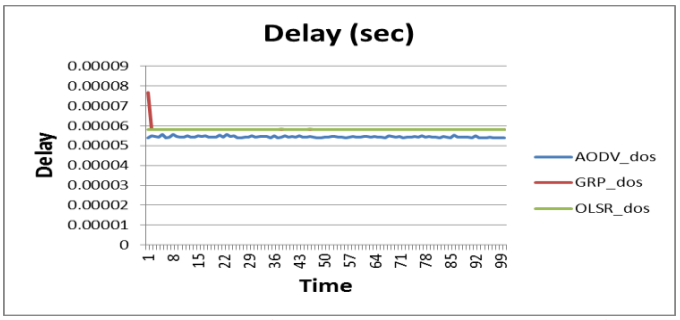

Fig. 5: Packet End-To-End Delay of AODV, GRP and OLSR with Attack for 16 Nodes.

8.2. Result of the second scenario

In the second scenario, there is jamming net consists of two malicious nodes so it is supposed to be kind of jamming attack. In jamming attack initially the malicious nodes keep monitoring wireless medium to determine the frequency that victim node is receiving a signal from sender. It then transmit signal on that frequency.

8.2.1. Throughput

From Fig. 6, it is obvious that the throughput for AODV is higher compared to that of GRP. The same is observed in the case of OLSR.

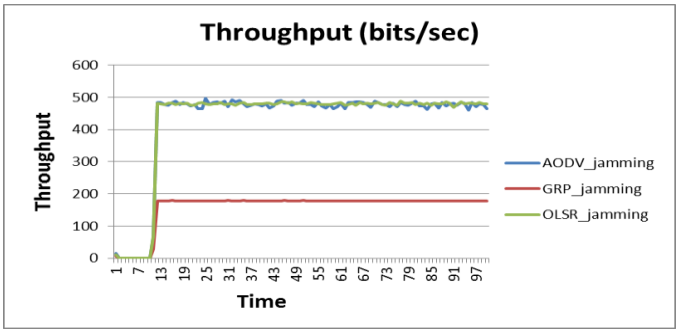

Fig. 6: Throughput of (AODV, GRP and OLSR) with DOS Attack for 16 Nodes.

8.2.2. Packed end to end delay

Packed end to end delay in case of jamming attack and without attack depends on the protocol routing. From Fig. 7, it is obvious that the packed end to end delay for OLSR is higher compared to that of GRP. The same is observed in the case of AODV.

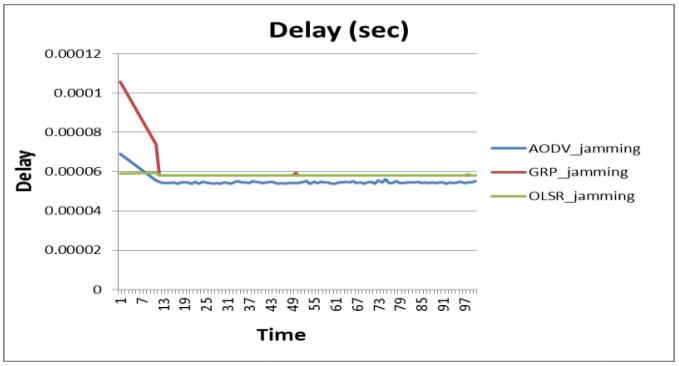

Fig. 7: Packet End-To-End Delay of AODV, GRP and OLSR with Attack for 16 Nodes.

8.2.3. The network load

The network load graph of OLSR, DSR and AODV with DOS attack and without attack has been shown in the Fig. 15. The network load of OLSR is much high as compared to AODV because under attack, node cannot send its packet, i.e. packet discarding leads to a reduction of network load. OLSR has a high network load in presence of two malicious nodes as compare to that of AODV and DSR. From Fig. 16, it is obvious that the network load for OLSR is higher compared to that of GRP. The same is observed in the case of AODV.

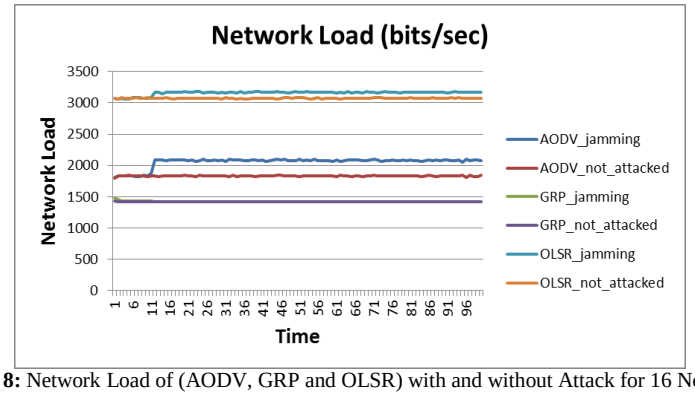

Fig. 8: Network Load of (AODV, GRP and OLSR) with and without Attack for 16 Nodes.

8.3. Result of the third scenario

In the third scenario, it is kind of spoofing replay it is a form of network attack in which a malicious node send true data but delayed or with a large amount. This is carried out either by one of the network nodes or by a new node adversary itself as normal nodes then send delayed data with a large amount.

8.3.1. Throughput

From Fig. 9, it is obvious that the throughput for AODV is higher compared to that of OLSR. The same is observed in the case of GRP.

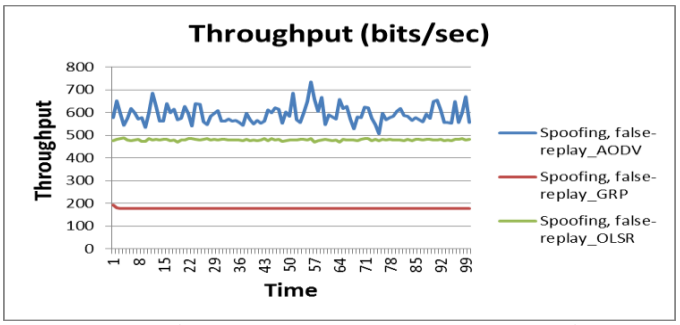

Fig. 9: Throughput of (AODV, GRP and OLSR) with DOS Attack for 16 Nodes.

8.3.2. Packed end to end delay

Packed end to end delay in case of spoofing attack and without attack depends on the protocol routing. In Fig. 10, it is obvious that the packed end to end delay for GRP is higher compared to that of OLSR. The same is observed in the case of AODV.

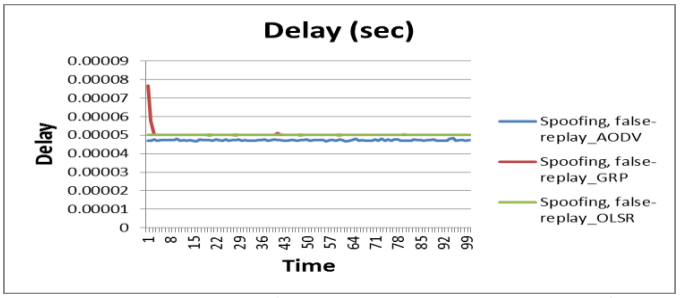

Fig. 10: Packet End-To-End Delay of AODV, GRP and OLSR with Attack for 16 Nodes.

8.3.3. The network load

The network load of OLSR, GRP and AODV with DOS attack and without attack has been shown in Fig. 11, it is obvious that the network load for OLSR is higher compared to that of GRP. The same is observed in the case of AODV.

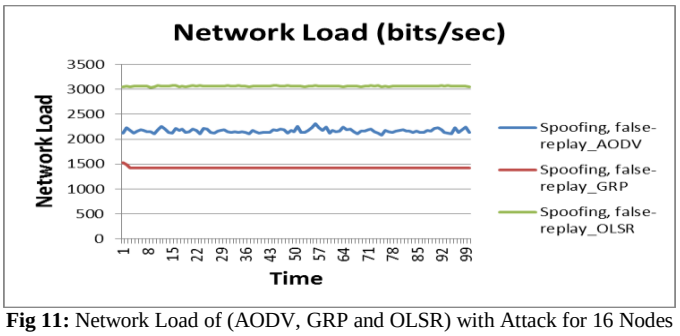

Fig 11: Network Load of (AODV, GRP and OLSR) with Attack for 16 Nodes

9. Conclusion

In our study, we analyzed that DOS attack with three different scenarios with respect to the performance parameters of end-to-end delay, throughput; packet dropped and network load. The intrusion has analyzed of three protocols OLSR, GRP and AODV, that have more severe effect when there is a higher number of malicious nodes and. The percentage of severances in delay under attack in case of OLSR is more than in case of AODV. In case of network load, however, there is effect on AODV by the malicious node is less as compare to OLSR. Based on our research and analysis of a simulation result we draw the conclusion that AODV is less vulnerable to denial of service attack than DSR, GRP and OLSR.

References

[1] Yang, Hao, et al. "Security in mobile ad hoc networks: challenges and solutions." Wireless Communications, IEEE 11.1 (2004): 38-47. http://dx.doi.org/10.1109/MWC.2004.1269716.

[2] Roopak, Monika, and B. Reddy. "Blackhole Attack Implementation in AODV Routing Protocol." International Journal of Scientific & Engineering Research4.5 (2013): 402-406.

[3] Begum, Syed Atiya, L. Mohan, and B. Ranjitha. "Techniques for resilience of denial of service attacks in mobile ad hoc networks." Proceedings published by International Journal of Electronics Communication and Computer Engineering3.1 (2012).

[4] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.

[5] A.D. Wood and J. Stankovic, "Denial of service in sensor network", IEEE Computer Magazine, vol. 5, no. 10, pp. 54-62J. Clerk, Oct. 2002.

[6] Von Mulert, Jan, Ian Welch, and Winston KG Seah. "Security threats and solutions in MANETs: A case study using AODV and SAODV." Journal of Network and Computer Applications 35.4 (2012): 1249-1259. http://dx.doi.org/10.1016/j.jnca.2012.01.019.

[7] Wu, B., Chen, J., Wu, J., Cardei, M. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. [book auth.] X. Shen, and D.-Z. Du (Eds.) Y. Xiao, Wireless/Mobile Network Security, Spinger, 2006.

[8] OPNET Technologies, www.opnet.com.

[9] Mohapatra, S., and P. Kanungo. "Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 Simulator." Procedia Engineering 30 (2012): 69-76. http://dx.doi.org/10.1016/j.proeng.2012.01.835.
[10] Khan, Shafiullah, Nabil Ali Alrajeh, and Kok-Keong Loo. "Secure route selection in wireless mesh networks." Computer Networks 56.2 (2012): 491-503. http://dx.doi.org/10.1016/j.comnet.2011.07.005.
[11] Remondo, David. "Wireless ad hoc networks: an overview." Network performance engineering. Springer Berlin Heidelberg, 2011. 746-766.
[12] Sari, Arif, and Beran Necat. "Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism." International Journal of Ad Hoc, Sensor and Ubiquiotus Computing 3 (2012): 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306.
[13] Gupta, Anurag, et al. "Improved AODV Performance in DOS and Black Hole Attack Environment." Computational Intelligence in Data Mining-Volume 2. Springer India, 2015. 541-549.
[14] Mandala, Satria, et al. "Quantifying the Severity of Blackhole Attack in Wireless Mobile Adhoc Networks." Security in Computing and Communications. Springer Berlin Heidelberg, 2014. 57-67. http://dx.doi.org/10.1007/978-3-662-44966-0_6.
[15] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1 (2011): 1-16. http://dx.doi.org/10.1186/2192-1962-1-4.
[16] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "A novel solution for grayhole attack in aodv based manets." Advances in Communication, Network, and Computing. Springer Berlin Heidelberg, 2012. 60-67. http://dx.doi.org/10.1007/978-3-642-35615-5_9.
[17] Singh, Rajinder, Parvinder Singh, and Manoj Duhan. "An effective implementation of security based algorithmic approach in mobile adhoc networks." Human-centric Computing and Information Sciences 4.1 (2014): 1-14. http://dx.doi.org/10.1186/s13673-014-0007-9.
[18] Waharte, Sonia, et al. "Routing protocols in wireless mesh networks: challenges and design considerations." Multimedia tools and Applications 29.3 (2006): 285-303. http://dx.doi.org/10.1007/s11042-006-0012-8.
[19] Aggarwal, Nitin, and Kanta Dhankhar. "Attacks on Mobile Adhoc Networks: A Survey." International Journal of Research in Advent Technology 2.5 (2014): 307-316.
[20] Sánchez-Casado, L., et al. "Defenses against Packet-Dropping Attacks in Wireless Multihop Ad Hoc networks." Security for Multihop Wireless Networks (2014): 377. http://dx.doi.org/10.1201/b16754-18.
[21] Vaithiyanathan, S.R. Gracelin, E.N. Elizabeth and S. Radha, 2010a. A novel method for detection and elimination of modification attack and TTL attack in NTP based routing algorithm. Proceedings of the International Conference on Recent Trends in Information, Telecommunication and Computing, Mar. 12-13, IEEE Xplore Press, Kochi, Kerala, pp: 60-64. ISBN: 978-1-4244-5956-8, DOI: 10.1109/ITC.2010.23. http://dx.doi.org/10.1109/ITC.2010.23.
[22] Patel, Meenakshi, and Sanjay Sharma. "Detection of malicious attack in manet a behavioral approach." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013. http://dx.doi.org/10.1109/iadcc.2013.651425.