Performance evaluation of MANET routing protocols under DDOS attacks

Khaled Ahmed Abood Omer
Computer Science and Engineering Department, Faculty of Engineering, University of Aden
E-mail: k_abood@hotmail.com
DOI: https://doi.org/10.47372/uajnas.2022.n2.a09

Abstract

Mobile ad-hoc networks (MANETs) consist of a set of communicating wireless mobile nodes or devices that could be deployed without the need for pre-established infrastructure for communication. Due to the insecure wireless communication medium and dynamic behavior of the nodes in MANETs, routing protocols are vulnerable to various security attacks, such as distributed denial of service (DDOS) attacks. DDOS attacks are used to temporarily disable network services by overloading the target system with huge traffic, such that it cannot respond to legitimate traffic. In this paper, we evaluate the performance of the Ad hoc on demand vector (AODV), Temporally ordered routing algorithm (TORA), Geographic routing protocol (GRP), and optimized link state routing (OLSR) routing protocols in MANETs under the DDOS attacks. These routing protocols are simulated using OPNET simulator to compare their performance using specific performance metrics on the network. The experimental results show that TORA protocol performs better than the AODV, OLSR, and GRP protocols under the DDOS attack.

Keywords: Routing protocols, MANET, security, DDOS attacks.

Introduction

Mobile ad-hoc networks (MANETs) consist of wireless mobile nodes that communicate with each other in the absence of a fixed infrastructure. In MANET, each node works as a router and a host. MANET is based on the cooperation among participating nodes and every node is willing to forward packets to make sure that packets are delivered from source to destination in a multi-hop route. Ad hoc networks are useful for the applications such as disaster recovery, automated battlefields, agriculture fields, security and vigilance, search and rescue, crowd control, conferences, meetings [2].

In MANETs, all networking functions, like routing and packet forwarding, are performed by the mobile nodes themselves in a self-organized manner. However, MANETs are exposed to vulnerabilities as a result of their basic features like no central network management, topology changes dynamically, and resource limitation. Due to the mobility and wireless media, MANETs are exposed to security risks, such as information disclosure, intrusion, or denial of service. Therefore, the security requirements in MANETs are much higher than those in wired networks [3, 9]. Among all network attacks, Denial of Service (DoS) and Distributed DoS (DDoS) attacks are serious threats to network functionality. MANETs are vulnerable to these attacks since existing MANET routing protocols, do not provide enough security defense capacity [15, 16].

A Denial of service (DOS) attack is a clear attempt to prevent the legitimate user from accessing services or network resources. DoS attacks can be initiated at any layer of the protocol stack causing physical jamming, disconnection, failure of routing, transport, and application protocols. This DOS attack is achieved by overloading the target system with many requests, such that it cannot respond to legitimate traffic. As a result, it makes the service unavailable for the legitimate user. The basic type of attack is the consumption of system resources like processor time and memory to disturb service to a specific system [16, 17].

Distributed Denial of Service (DDoS) attack attempts to consume the resources of the target node so that it cannot provide service or resources. The DDOS attacks become dangerous and hard to prevent since a group of attackers coordinate in DoS attack [18]. When a DDoS attack occurs in MANET, the attacker compromises some mobile nodes, which can follow different mobile patterns and have different speeds. Therefore, this attack gradually reduces the functionality as well as the overall performance of the MANET network.

In this work, the performance of four routing protocols in MANETs under the DDOS attack, was evaluated using OPNET simulator. The routing protocols are: Ad hoc on demand vector (AODV), Temporally ordered routing algorithm (TORA), Geographic routing protocol (GRP), and optimized link state routing (OLSR) routing protocols. the attack simulation model is to be used in simulating these routing protocols. Finally, we present the results of simulation experiments, carried out using the OPNET network simulator.

This paper is organized as follows: section 2 describes the related work about routing protocols and DDOS attacks, section 3 includes a simulation environment. section 4 describes results and discussions, Finally, section 5 includes the findings of the work.

Related work

Routing protocols used in MANETS are classified into three categories named as proactive, reactive, and hybrid routing protocols. Proactive or table-driven routing protocols are OLSR and GRP protocols. In these routing protocols, the routes to all the nodes are maintained in the routing table. Packets are sent over a predefined route specified in the routing table. A Reactive or on-demand routing protocol are such as AODV and TORA protocols. These routing protocols establish the routes on request for routing. A source node initiates the route discovery phase to find a new route whenever there are packets to be sent to a destination. The grouping of proactive and reactive approaches results in hybrid routing protocols such as Zone Routing Protocol (ZRP). The performance of these routing protocols was evaluated without consideration of any security attacks on MANET [2, 5, 8, 11]. In this paper, we consider AODV, TORA, OLSR, and GRP routing protocols for further investigation under DDOS security attacks.

1. Routing Protocols

AODV is a reactive routing protocol where routes are discovered only on demand when there is a need to send packets to a destination [13]. This protocol uses three types of messages - route request (RREQ), route reply (RREP), and route error (RERR). The routing table is used to store the information about the next hop to the destination and a sequence number received from the destination which indicates the received information is updated. The route discovery is achieved by broadcasting the RREQ message to the neighbors with the requested destination sequence number, which prevents the old information from being sent back to the request and also prevents looping problem. Passed nodes update their own routing table about the requested node. Therefore, the discovered route is recorded in the routing table of the intermediate nodes. The destination creates RREP message to be sent back to the source. The source starts sending the packets to the destination after receiving the RREP message. When the corresponding route breaks, then the RERR message is used to inform the neighbors.

TORA is adaptive and distributed routing protocol for mobile, multihop, wireless networks based on the concept of link reversal [12]. This protocol is a source-initiated on-demand routing protocol that finds multiple routes from a source node to a destination node. All Nodes maintain routing information about their immediate one-hop neighbors in the network. TORA uses control messages that are localized to a small set of nodes nearby a topological change. The protocol has three basic functions: Route creation, Route maintenance, and Route erasure. Nodes use a height metric to establish a directed acyclic graph (DAG) rooted at the destination during the route creation and route maintenance phases. Route maintenance is necessary when any of the links in DAG is broken.

OLSR is a proactive routing protocol, so the routes are available without delay when needed to send packets in the network [7]. OLSR uses Multipoint Relays (MPR) to reduce the overhead in the network. This protocol uses Hello message to discover the information about the link status and neighboring nodes in the network. Topology control (TC) message periodically broadcasts information about advertized neighbors including the MPR selector list. The Hello messages are sent only one hop away whereas the TC messages are broadcast to the entire network. Also Multiple Interface Declaration (MID) message is broadcast in the network only by MPRs to report to other hosts that the announcing host has multiple OLSR interface addresses. Also Host and Network Association (HNA) message provides the external routing information for routing to the external addresses.

GRP is a location-based routing protocol [10]. GRP is distance-based, greedy algorithm that uses the Global Positioning System (GPS) to mark the location of each node in the network. GRP selects the next hop on the path as a node geographically closest to destination. The network area is divided into square quadrants for routing so that every four quadrants of the lower level form a quadrant of a higher level. GRP maintains routing tables based on the geographical locations of the nodes in the network. Now, if the source and the destination nodes are located in the same quadrant, then the source sends a packet to its immediate neighbor closest to the destination. Similarly, the intermediate node forwards the packet to its immediate neighbor closest to the destination, until the packet arrives at the destination. If source and destination are located in different quadrants, then the source sends the packet to its immediate neighbor closest to the highest-level quadrant where the destination exists. As the packet crosses the quadrant boundaries, the location information about the destination becomes more precise and finally the packet arrives at the destination's quadrant and is routed to destination using precise location information.

2. Distributed Denial of Service (DDoS) Attacks

In the context of Information Security, availability means that information is readily accessible to authorized and legitimate users. Availability attacks, sometimes called denial of service (DoS) attacks, are more important in computer networks. A DoS attack occurs when an attacker (or a malicious node) attempts to entirely consume all available resources of the target node and, then, blocks all services to legitimate users by sending massive amounts of fake traffic to the victim. A DoS attack usually consumes bandwidth, memory, processor or CPU cycles, or any other resource that is necessary for normal operation. The victim will become overwhelmed by the overload of traffic and will not be able to respond to legitimate users [9, 16, 6].

In order for an attacker to overload a target node, the attacker must be able to generate more traffic than the victim or target node can handle. This is difficult to be achieved by using a single attacking node. To make this attack successful, the attacker will gather many attacking nodes to use in the denial of service attack. This attack is called Distributed Denial of Service (DDoS) [6].
In DDoS attack, the attacker uses a suitable attack to insert malicious or zombie software on a number of nodes distributed all over the network. This malicious software does not cause any harm to these nodes. Next, the attacker coordinates and triggers all the zombies to launch the attack on the victim node in the network [16, 14].

Zain et al [19] compared the performance of OLSR, AODV, DSR, and GRP MANETs routing protocols under DoS attacks on the network layer using OPNET simulator. Moreover, they simulated these routing protocols under DoS attacks for the delay throughput Data loss, and network load metrics. Based on their simulation results, they concluded that the AODV protocol is less vulnerable to DOS attack than DSR, GRP, and OLSR protocols.

Abdelhaq et al. [1] implemented DDoS Attack Simulation Model in Network Simulator 2 (NS-2) to examine the effect of DDoS Attack on Zone Routing Protocol (ZRP), AODV protocol, and Location-Aided Routing (LAR) protocol. The performance of three routing protocols was analyzed in terms of throughput and end-to-end latency metrics under DDOS attacks. They found that ZRP

performed better compared to AODV and LAR protocols in terms of throughput and end-to-end delay.

Alsaqour et al [4] studied the impact of resource consumption attacks on AODV and Dynamic Source Routing (DSR) routing protocols. They used the NS-2 simulator to find the most resistant routing protocol to such attacks. The experiment results showed that the DSR protocol is more sensitive to flooding attacks than the AODV protocol in terms of throughput, end-to-end delay, and energy consumption. The DSR has more throughput while AODV has a less end-to-end delay and less energy consumption than the DSR protocol, in all experiments, so the AODV is better than the DSR in facing this attack in MANET.

Stojanovic et al [18] studied the influence of mobility models, node speed, and attack duration on the MANET vulnerability under bandwidth DDoS attacks. They carried out the experiments on the AODV routing protocol using the network simulator NS-2. The Results of this study indicated that the MANET vulnerability to bandwidth DDoS attacks strongly depends on the mobility pattern and speed of the mobile nodes in the network.

Simulation Environment

In this paper, was evaluated the performance of MANET routing protocols, under a DDoS attack, The DDOS attacks are achieved by flooding the target node in the MANET network with a large number of junk packets. In the attack model used in this work, the attacker compromises several mobile nodes by installing malicious code into them using worms. However, the attacker could be an internal node or an external device. The compromised mobile nodes become zombies, which at the same time create rubbish packets and send them toward the target node. The Simulation parameters used in our experiments are shown in Table 1 below.

Table 1 Simulation Parameters

Network Parameters	Values
Number of Mobile Nodes	36
Simulation Time	1000 seconds
Simulation Area	1000 m x 1000 m
Routing Protocols	AODV, TORA, OLSR, GRP
Mobility Model	Random waypoint (speed 0-10m/s)
PHY Characteristic	PHY 802.11g

The attack simulation model is made of 36 nodes deployed in a 1000m x1000m network. There is only one target or victim node, 23 legitimate nodes, and 12 zombies with infected software during the DDOS attack period. Legitimate nodes packets inter-arrival time = 1.0 seconds, and Zombies packets inter-arrival time = 0.001 seconds. Further at the target node, the datagram forwarding rate of the IP processor (queue) is reduced to 2000 packets/sec to make the target slower, and the memory size of the IP processor (queue) is reduced to 8 MB to see the packets get dropped after the queue is filled up.

Two scenarios were implemented to measure the impact of DDOS attacks on the four routing protocols under investigation based on the attack simulation model. In the first scenario, the DDOS attack duration is 200 seconds, and in the second scenario, it is 400 seconds.

The simulation time for the attack simulation model is 1000 seconds with the starting time of packet generation at 100 seconds. The legitimate nodes send IP traffic to the target node from 101 seconds to the end of the simulation (1000 seconds) with an inter-arrival time of 1.0 seconds. Then the DDOS attack is triggered by the zombies for a duration of 200 seconds in the first scenario and 400 seconds in the second scenario starting at 301 seconds of the simulation time. In the first

scenario, the zombie nodes send IP traffic to the target node from 301 seconds to 500 seconds with an inter-arrival time of 0.001 seconds. Similarly, in the second scenario, the zombie nodes send IP traffic to the target node from 301 seconds to 700 seconds with an inter-arrival time of 0.001 seconds.

1. Performance metrics:

In this paper, we consider the following performance metrics to investigate the performance of the routing protocols under investigation:

Traffic drops (Packets /sec): The number of IP packets dropped by all nodes in the network due to insufficient space in the queue of the processor. A lower Traffic drop leads to better routing protocol performance. Therefore, this metric shows that the memory is consumed by the DDOS attacks.

End-to-end delay of MANET IP packets (seconds): the time passed between the creation of the packet at its source and its destruction at its destination for the entire network. A lower end-to-end delay leads to better routing protocol performance.

Data dropped (buffer overflow bits/sec): The total size of higher layer data packets dropped by all the WLAN MACs in the network due to insufficient higher layer data buffer space. A lower data drop leads to better routing protocol performance.

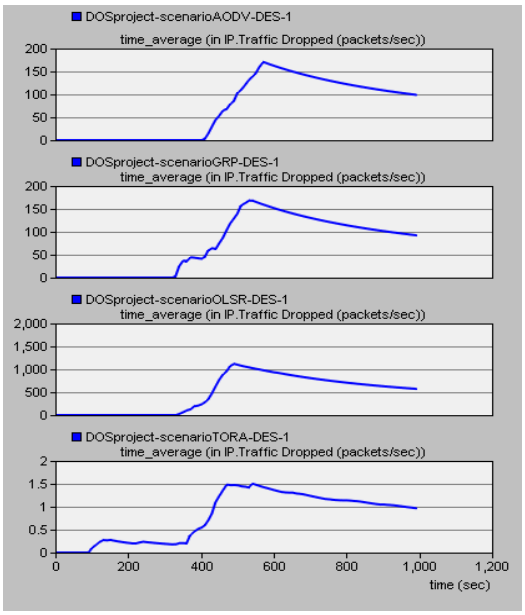
Processing delay experienced by an IP datagram: The delay from the time when the packet arrives at the IP layer to the time it is sent out from the IP layer. This delay includes: Queuing delay and Processing delay based on the processing speed/forwarding rate.

Processor or CPU Utilization (%): This statistic reports the utilization of the processor. The CPU is used to model the IP packet forwarding delays and application processing delays. It is important to know that the CPU utilization greater than 80% is considered alarming, and will increase waiting time at the node's queue. Therefore, this metric shows that the processor is consumed by the DDOS attacks.

Results and Discussion:

In this section, we illustrate and discuss the experimental results obtained by simulation of the four Routing protocols according to the attack model illustrated above.

Figure 1a and Figure 1b show that the IP traffic dropped increases within the DDOS attacks period in the network due to insufficient space in the central processor's queue. During DDoS attacks huge amount of traffic gets to the target node, and starts waiting for service in the queue of the target's IP processor, because the target's resources are fully utilized. Once the memory is filled up, any more incoming request traffic will get dropped at the target node. Therefore, the packets are dropped after some time of the attack and continued for some time after the attack stops. Further, the OLSR protocol has maximum traffic dropped and the TORA protocol has the minimum traffic dropped.



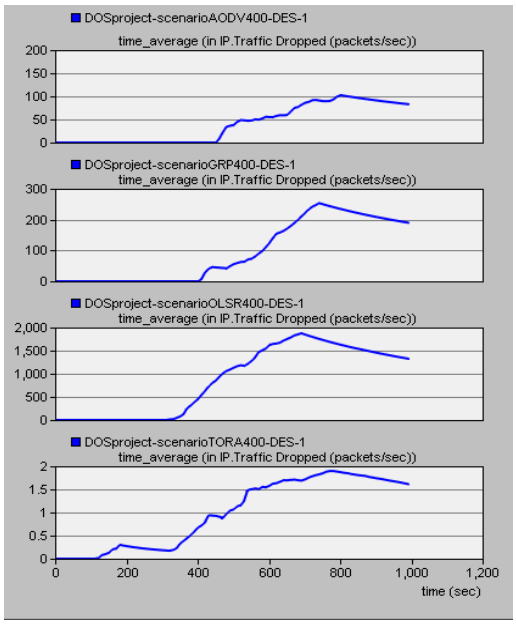
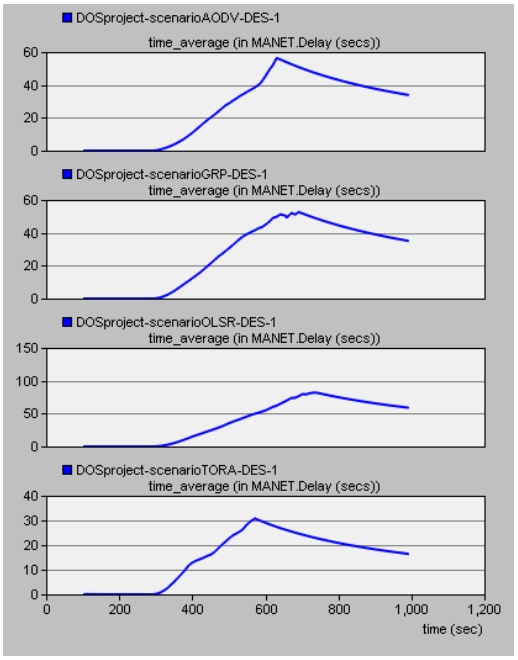


Fig. 1a IP traffic drop (packets/sec) (200 sec) Fig. 1b IP traffic drop (packets/sec) (400 sec)

Figure 2a and Figure 2b show that the End-to-End Delay increases within the DDOS attack period in the network. Further, the OLSR protocol has maximum delay and the TORA protocol has the minimum delay.



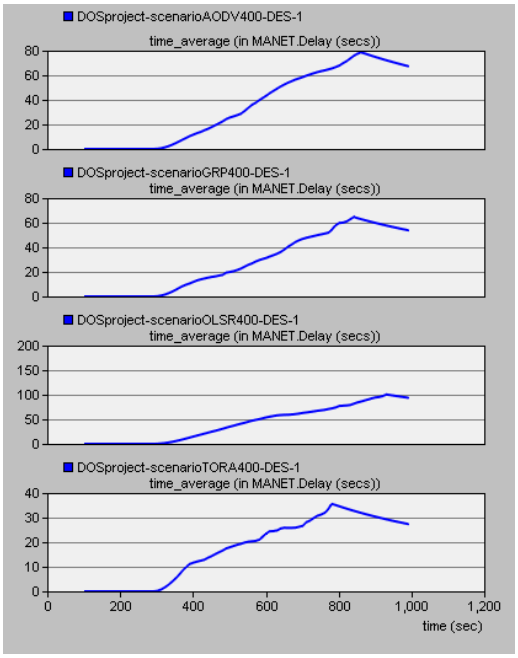


Fig. 2a End-to-End Delay (200 sec) Fig. 2b End-to-End Delay (400 sec)

Figure 3a and Figure 3b show that the wireless LAN data dropped increases within the DDOS attack period in the network due to buffer overflow. It is clear that when there are zombie nodes in the network, then the data dropped by all the routing protocols under consideration increases. Also,

the GRP protocol has a higher data dropped compared to the remaining protocols, and the TORA protocol has the minimum buffer overflow.

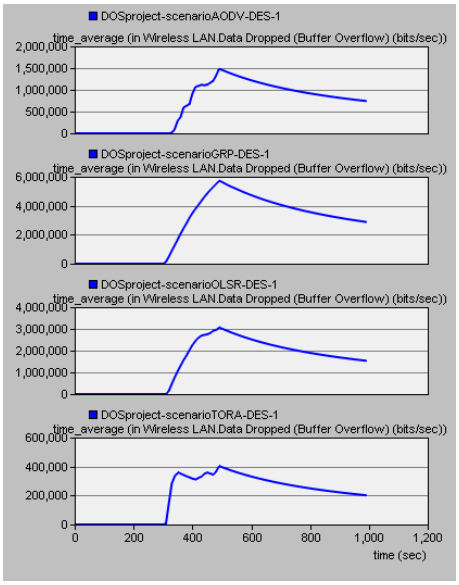


Fig. 3a wireless LAN data drop (bits/sec) (200 s)

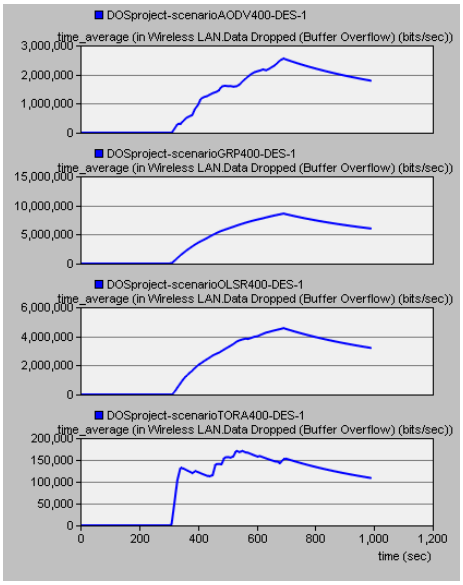


Fig. 3b wireless LAN data drop (bits/sec)(400 s)

Figure 4a and Figure 4b show the CPU utilization at the target node only. The figure shows that the CPU utilization increases within the DDOS attack period in the network due to the huge amount of traffic sent to the target node. It is clear that when zombie nodes are activated in the network, then the CPU utilization approaches 100% by all the routing protocols under consideration. The CPU utilization of the target remains 100% for some time even though the attack lasted only for about 200 seconds. This is because a huge amount of incoming traffic is waiting for service in the queue of the target's IP processor and it takes some time to deplete the fully consumed target node. Further, we see that the TORA protocol recovers from the attack very fast, compared to other protocols where the CPU utilization returns to its normal value before the attack.

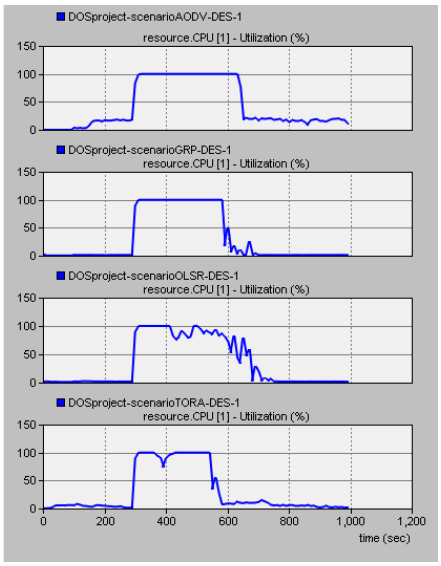


Fig. 4a CPU utilization at the target node (200 s)

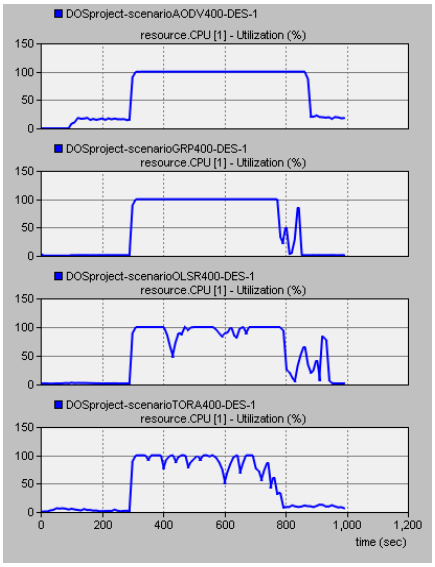


Fig. 4b CPU utilization at the target node (400 s)

Figure 5a and Figure 4b show the IP traffic dropped at the target node only. The figure shows that the traffic drop increases within the DDOS attack period for the routing protocols under consideration in the network. It is clear that, when zombie nodes are triggered in the network, then the traffic dropped increases in AODV, OLSR, and GRP routing protocols due to a large amount of traffic sent to the target node under attack. Further, we note that the TORA protocol has the minimum traffic dropped approaching zero packet, compared to the routing protocols under consideration in the network.

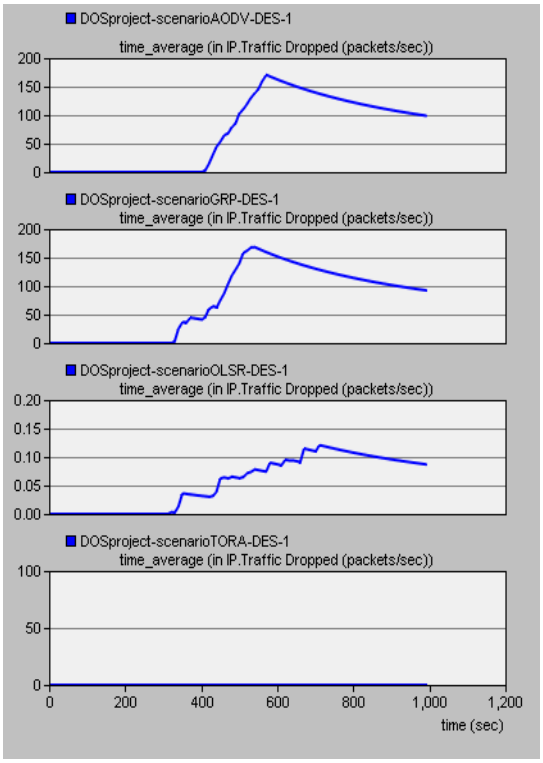


Fig. 5a IP traffic drop in the target node (200 sec)

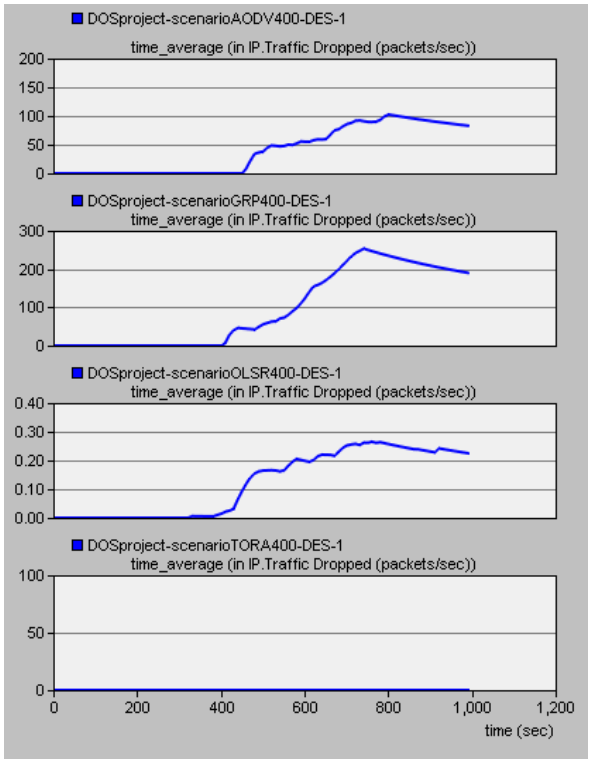


Fig. 5b IP traffic drop in the target node (400 sec)

Figure 6a and Figure 6b show the processing delay experienced by an IP datagram at the target node only. The figure shows that the processing delay increases during the duration of the DDOS attack for the routing protocols under consideration in the network. It is clear that, when zombie nodes are triggered in the network, then the processing delay increases in AODV, OLSR, and GRP routing protocols due to a large amount of traffic to be sent by the target node under attack. Further, we note that the TORA protocol has a minimum processing delay approaching zero seconds compared to the routing protocols under consideration in the network.

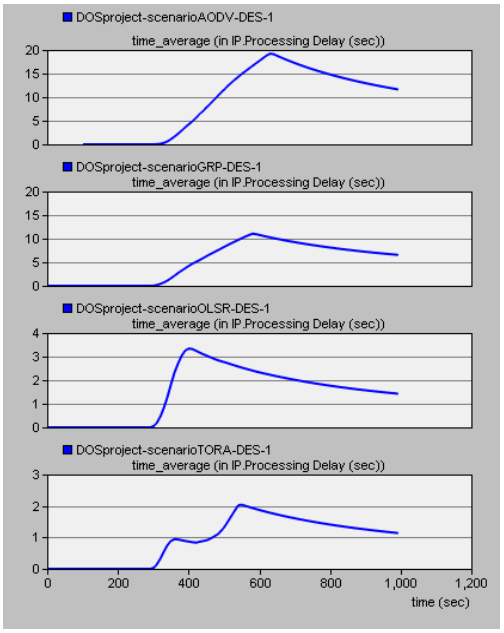


Fig. 6a processing delay at the target node

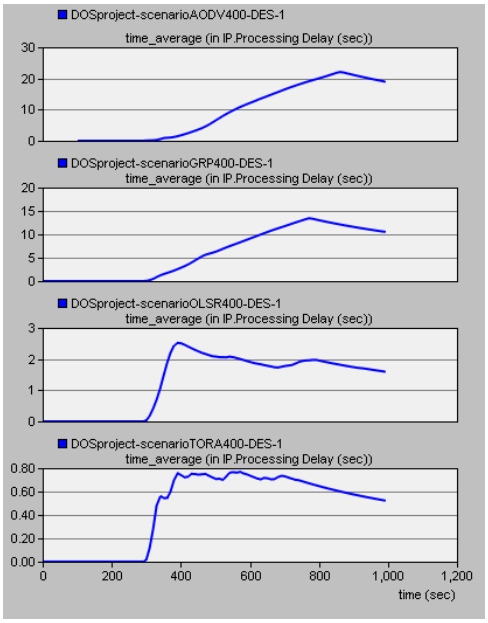


Fig. 6b processing delay at the target node

Conclusion

In this paper, we have compared the performance of AODV, TORA, OLSR, and GRP routing protocols under the attack of DDOS, using the OPNET simulator. This comparison is achieved by flooding the target node with a large number of packets in the MANET network according to the attack simulation model used.

The experimental results show that the performance of routing protocols under investigation is degraded under DDOS attacks in the MANET network. Further, the simulation results show that the TORA routing protocol outperforms the remaining routing protocols, and hence the TORA routing protocol is more resistant to the DDOS attack.

References

1. 1 Abdelhaq M., R. Alsaqour, M. Alaskar, F. Alotaibi, R. Almutlaq, B. Alghamdi, B. Alhammad, M. Sehaibani, D. Moyna, (2020), " The resistance of routing protocols against DDOS attack in MANET", International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 5, pp. 4844-4852
2. [2] Abolhasan M., T. Wysocki and E. Dutkiewicz, (2004), " A review of routing protocols for mobile ad hoc networks", Elsevier Journal of Ad Hoc Networks, Vol. 2, No. 1, pp. 1-22.
3. [3] Agrawal S., S. Jain, S. Sharma, (2011), "A Survey Of Routing Attacks And Security Measures In Mobile Ad-Hoc Networks", Journal Of Computing, Vol. 3, No. 1, pp. 41-48.
4. [4] Alsaqour R., M. Abdelhaq, N. Alghamdi, M. Alneami, T. Alrsheedi, S. aldghbasi, R. Almalki, and S. Alqahtani, (2021), " a simulation model for the effect of resource consumption attack over MANET", ARPN Journal of Engineering and Applied Sciences, Vol. 16, N. 13, pp. 1323-1330
5. [5] Aujla G. S., and S. S. Kang, (2013), "Comprehensive Evaluation of AODV, DSR, GRP, OLSR and TORA Routing Protocols with varying number of nodes and traffic applications over MANETs", IOSR Journal of Computer Engineering, Vol. 9, No. 3, pp. 54 -61.
6. [6] Chatam J. W., J. Rice, and J.A. Hamilton, (2004), "Using Simulation to Analyze Denial of Service Attacks", Applied Telecommunications Symposium, ASTC, Arlington, pp. 18-22.

7. [7] Clausen T. and P. Jacquet (2003), "Optimized Link State Routing Protocol (OLSR)." RFC 3626, IETF Network Working Group.
8. [8] Gupta A. K., H. Sadawarti, and A. K. Verma, (2010), "Performance analysis of AODV, DSR & TORA Routing Protocols", International Journal of Engineering and Technology, Vol.2, No. 2., pp. 226-231.
9. [9] Joshi P., (2011), "Security Issues in Routing Protocols in Manets at Network Layer," Procedia Computer Science, Vol. 3, pp. 954-960.
10. [10] Li Z. (2009), "Geographic Routing Protocol and Simulation", Proceedings of International Workshop on Computer Science and Engineering, pp. 404-407
11. [11] Manickam P. , T. Guru Baskar, M. Girija, and D. Manimegalai, (2011), "Performance Comparisons Of Routing Protocols In Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networks, Vol. 3, No. 1, pp. 98-106
12. [12] Park V. D. and M. S. Corson, (1997), "A highly adaptive distributed routing algorithm for mobile wireless networks", Proceedings of INFOCOM'97, vol. 3, pp. 1405-1413.
13. [13] Perkins C. and E Royer, (1999), "Ad Hoc On-Demand Distance Vector Routing," 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., pp 1-11.
14. [14] Pfleeger C. P. and S. L. Pfleeger, J. Margulies (2015), "Security in Computing", Pearson education 5th Edition, pp. 396-430.
15. [15] Raymond D. R. , S.F Midkiff, (2008), "Denial of Service in Wireless Networks: Attacks and Defences", IEEE CS: Security and Privacy, pp. 74-81.
16. [16] Saluja K. K. and P. Kakkar, (2012), "The DDOS Attacks In MANET- A Review", Journal Of Information Systems And Communication, Volume 3, Issue 1, pp. 310-314
17. [17] Specht S. M., R. Lee, (2004), "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," ISCA 17th International Conference on Parallel and Distributed Computing Systems, San Francisco, pp. 543-550.
18. [18] Stojanovic M., V. Acimovic-Raspopovic, V. Timcenko, (2012), "The Impact of Mobility Patterns on MANET Vulnerability to DDoS Attacks", Electronics And Electrical Engineering, No. 3(119), pp. 29-34.
19. [19] Zain A., H. A. El-Khobby, H. M. Abd Elkader, M. M. Abdelnaby, (2015), "MANETs performance analysis with DOD attack at different routing protocols", International Journal of Engineering & Technology Sciences, pp. 390-398.

تقييم الأداء لخوارزميات التوجيه في الشبكات المتنقلة تحت هجمات حجب الخدمة الموزعة

خالد أحمد عبود عمر
قسم علوم وهندسة الحاسب، كلية الهندسة، جامعة عدن
البريد الالكتروني: k_abood@hotmail.com
DOI: https://doi.org/10.47372/uajnas.2022.n2.a09

الملخص

تتكون الشبكات المتنقلة المخصصة (MANETs) من مجموعة من الأجهزة المحمولة اللاسلكية للاتصال التي يمكن نشرها دون الحاجة إلى بنية تحتية مسبقة للاتصال. نظرًا لوسط الاتصال اللاسلكي غير الآمن والسلوك الديناميكي للأجهزة في MANETs، فإن بروتوكولات التوجيه معرضة لهجمات أمنية مختلفة، مثل هجمات رفض الخدمة الموزعة (DDOS). تُستخدم هجمات DDOS لتعطيل خدمات الشبكة مؤقتًا عن طريق التحميل الزائد على النظام المستهدف بحزم بيانات ضخمة، بحيث لا يمكنها الاستجابة لحزم البيانات المشروعة.

في هذه الورقة، نقوم بتقييم أداء برتوكولات التوجيه الآتية: AODV، TORA، GRP، OLSR في MANETs تحت هجمات DDOS. تتم محاكاة بروتوكولات التوجيه هذه باستخدام محاكي OPNET لمقارنة أدائها باستخدام مقاييس أداء محددة على الشبكة. تظهر نتائج التجارب التي حصلنا عليها أن بروتوكول TORA يعمل بشكل أفضل من بروتوكولات التوجيه AODV و OLSR و GRP في ظل هجوم DDOS.

الكلمات المفتاحية: خوارزميات التوجيه، الشبكات المتنقلة، الامن، هجوم حجب الخدمة الموزعة.