International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 5, October 2020, pp. 4844~4852
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i5.pp4844-4852

The resistance of routing protocols against DDOS attack in MANET

Maha Abdelhaq[1], Raed Alsaqour[2], Mada Alaskar[3], Fayza Alotaibi[4], Rawan Almutlaq[5], Bushra Alghamdi[6], Bayan Alhammad[7], Malak Sehaibani[8], Donia Moyna[9]
[1,3,4,5,6,7,8,9]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia
[2]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Saudi Arabia

Article Info

Article history:

Received Dec 18, 2019
Revised Mar 22, 2020
Accepted Mar 30, 2020

Keywords:

AODV
DDoS attack
MANET
Routing
Simulation model

ABSTRACT

A Mobil Ad hoc Network (MANET) is a wireless multi-hop network with various mobile, self-organized and wireless infrastructure nodes. MANET characteristics such as openness restricted resources and decentralization impact node efficiency and made them easy to be affected by various security attacks, especially Distributed Denial of Service (DDoS) attacks. The goal of this research is to implement a simulation model called DDoS Attack Simulation Model (DDoSM) in Network Simulator 2(NS-2) and to examine the effect of DDoS Attack on various routing protocol types in MANET namely: Zone Routing Protocol (ZRP), Ad hoc On-Demand Distance Vector (AODV) protocol and Location-Aided Routing (LAR) protocol. The introduced model uses the NS-2 simulator to apply DDoS on the three chosen routing protocols. In terms of throughput and end-to-end latency under the consequences of the attack, the performance of three routings protocols was analyzed.

Corresponding Author:

Maha Abdelhaq,
Department of Information Technology,
College of Computer and Information Sciences,
Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia
Email: MSAbdelhaq@pnu.edu.sa, maha.ukm@gmail.com

1. INTRODUCTION

The Mobile Ad-hoc Network (MANET) is a series of mobile nodes that are distributed via wireless multi-hop technology [1]. Each node can act as a router on its own in an infrastructure-free way to provide the network functionality necessary [2, 3]. The MANET can be used in various fields, including military applications, sensor environments, rescue operations [4]. MANET has special features such as dynamic topology, which implies that nodes frequently change mobility, which compromises network security [5]. It is, therefore vulnerable to various attacks such as flooding attacks that deliberately send ample traffic packets to interrupt the efficiency of the network [6, 7].

Securing MANET is a critical research issue; it is vulnerable to many types of attacks and interferes with network security characteristics. One of the threatening attacks MANET is the Distributed Denial of Service (DDoS) attack [7-12]. The DDoS attacker has hundreds or thousands of useless packets flooding the victim's resources to make the network busy or out of service. This will reduce the capacity of the network and render it unable to perform its role. It thus becomes incapable of providing services to the legitimate nodes.

We deployed a DDoS network attack in the NS-2 simulator in this study, and it is called the distributed Denial of Service protocol (DDoSM). DDOSM uses the NS-2 traffic generator to produce

a stream of Constant Bit Rate (CBR) traffic, a feature that does not exist in actual networks but is used for simulation purposes of testing the most sensitive and efficient routing protocols under the attack effect without affecting network performance. The DDoSM model will be incorporated into three types of routing protocols: Zone Routing Protocol (ZRP) [13] which is a hybrid routing protocol, Ad-hoc On-Demand Distance Vector (AODV) [14] which is a reactive routing protocol, and Location-Aided Routing (LAR) [15] which is an aided routing protocol to geographic position. The DDoSM model performs flooding attacks on these routing protocols and then analyzes resistance to DDoS attack by each of these routing protocols and this can be useful for maintaining a MANET.

The remainder of the article is structured accordingly. We provide an overview of the research background and work related to it in Section 2. Section 3 introduces the theoretical simulation model, simulation environment and performance metric for the DDoS attack. Section 4 addresses the results and evaluations and we summarize our research and future work in Section 5.

2. BACKGROUND AND RELATED WORK

2.1. Mobile ad-hoc network (MANET)

MANET is a type of wireless network that does not have a central base station to spread nodes. As shown in Figure 1, When two nodes have to communicate with each other, they have to be within each other's range and have to rely on other nodes for communication. MANET is easily set up in locations that do not embrace the existence of wired networks for a short time span. It may be helpful in war or natural disaster situations. However, due to the lack of networks and cables, MANET has several advantageous benefits such as low budget and effortless operation, and because it has a quick implementation with setup for the same purpose. Because of its open nature, and no central supervision, MANET suffers from security threats.

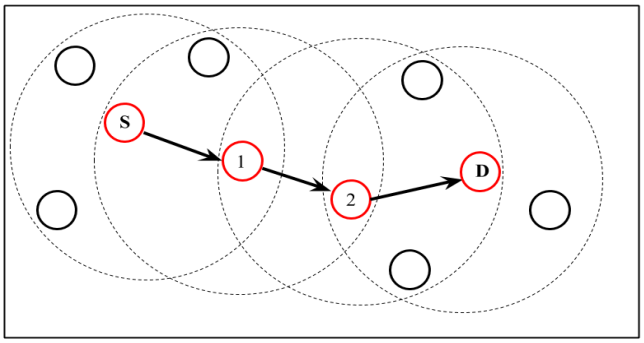

Figure 1. Mobile ad-hoc network

2.2. Routing in MANET

Routing is when each node has to find paths to transfer data packets between computing devices in the network. Routing in MANET is a major challenge because the topology is temporary and dynamic. This section reviews our study into the three chosen routing protocols.

2.2.1. Location-aided routing (LAR) protocol

LAR is one of the common routing protocols which seeks to reduce the overhead control message [15, 16]. In order to identify a potential target node location, LAR utilizes the Global Positioning System (GPS). LAR determines a portion of the network which is experiencing limited flooding on the basis of that knowledge. So, the amount of control messages passing through the network declines during the route discovery process. LAR assumes that the network nodes know their own location and the last known location of the destination node. On this basis, LAR links the search area of the route to the region in which the route to the destination node is located.

LAR adjusts the mechanism of path discovery so that only the nodes that are part of the search area will retransmit route request packets. When the route request packet reaches the intermediate node, the node first determines whether the request packet for the incoming route falls into the search zone specified. If not, the route data package should be transmitted, unless it is part of the search area. If not, the packet will be discarded.

As the Figure 2 shows, if nodes *I* and *K* receive a route request for destination node *D* from node *S*, the route request is sent because both *I* and *K* are within rectangular request range. The path request will be sent. By comparison, if the route request is received by the node *N*, the request is ignored because *N* is outside the rectangular route request zone.

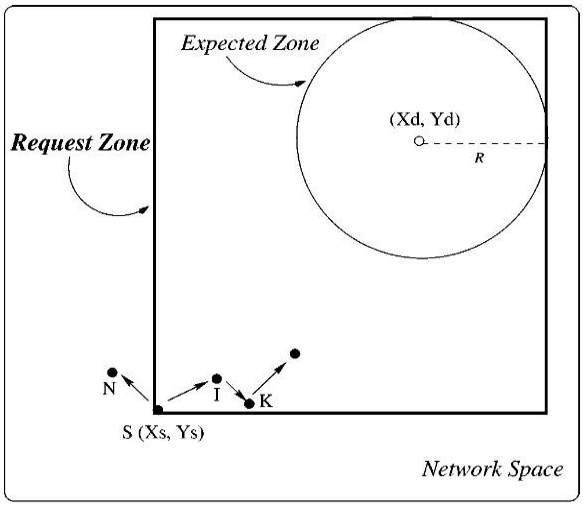

Figure 2. LAR routing protocol [15]

2.2.2. Ad-hoc on-demand distance vector (AODV) protocol

This work adopts the AODV routing protocol [17, 18]. AODV is a powerful, self-starting, large-scale routing protocol. Over many years it has been extensively studied and developed, there by confirming its robustness and advantages. As shown in Figure 3(a), AODV's route discovery process was accompanied by the source node transmits a route request (RREQ) packet to all MANET nodes.The RREQ packet contains information on routing, including the IP address of the originator, ID of transmission and sequence number of the recipient. Every intermediate node receives the RREQ packet and retains the reverse path towards the source node. The intermediate node verifies that an RREQ packet with the same IP address and transmitted ID has already been provided, and then decides whether an RREQ packet is to be refused or admitted.

This verification process helps prevent attacks from floods. The intermediate node will validate the destination sequence number contained in its routing list after processing the RREQ packet. The intermediate node uni-casts the Route Response (RREP) packet to the source node if the sequence number is greater than or equal to the one found in the RREQ packet. If there is no fresh-styled route to the destination node, the RREQ packet must retain its Navigation until the target node is reached, which actually uni-casts the RREP packet to the source node as shown in Figure 3(b).

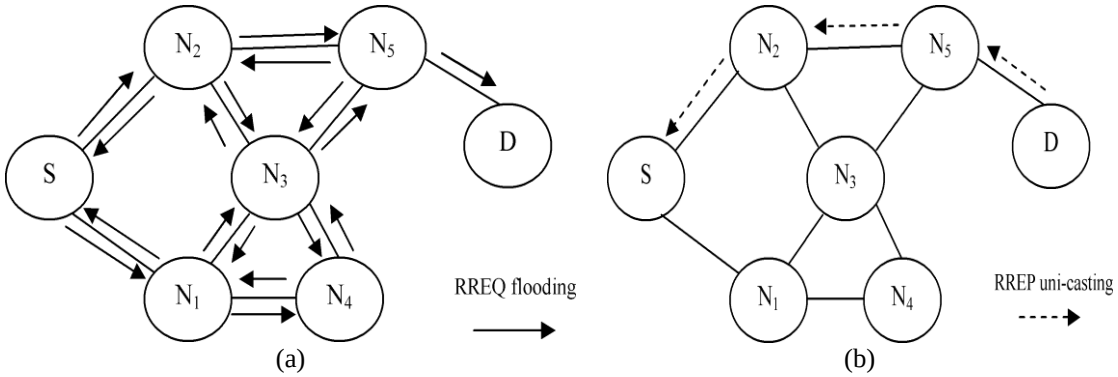

Figure 3. AODV routing protocol. S: source node, D: destination node, N1 to N5 intermediate nodes, (a) RREQ packet propagation, (b) Path of the RREP packet [19]

2.2.3. Zone routing protocol (ZRP)

ZRP is a hybrid routing protocol. The main idea of this hybrid protocol is to use both the proactive and reactive protocol routing mechanisms [20]. ZRP is based on the zone concept. A zone's nodes are broken down into outer nodes and inner nodes. Outer nodes are connected nodes directly, and the inner nodes are connected nodes indirectly. The routing zone is represented in hops with a radius ρ. If ρ=1 implies, the source only goes to its direct link nodes. If ρ=2 the source could go further.

Since most communication takes place in ZRP between the nodes near to each other, ZRP uses proactive protocols to discover the routing information within the zone. This is known as the IARP (Intra-Zone Routing Protocol). The reactive protocols are used to discover the routes between zones. This is named IERP (Interzone Routing Protocol) [21].

Consider the network found in Figure 4(a). The S node has a packet that must be sent to X. The scale of the zone is ρ = 2 radius. The node uses IARP's routing table to check if the destination lies within its zone. A route request is given using IERP because it is not identified. The message is transmitted to the outward nodes (the figure shows a gray color). Each check-in their routing table for the destination. Node *I* cannot find the destination in its routing table. It, therefore, broadcasts the message to its outward nodes, as shown in Figure 4(b) in gray color. The request is not passed back to the nodes *D*, *F* and *S* because of query control mechanisms.

Lastly, node *T* receives a request to locate the destination in its routing zone, as illustrated in Figure 4(c). Node *T* adds the path from node X itself to the route request. A route reply with the reversed direction is generated and returned to the source node. If there were many routes to the destination, several replies would be provided to the source.

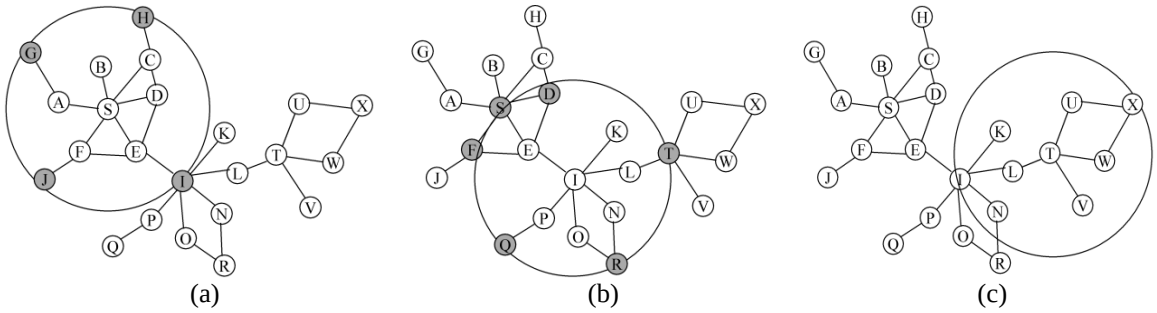

Figure 4. ZRP routing protocol, (a) routing zone of node S, (b) routing zone of node I, (c) routing zone of node T [13]

2.3. Related work

To our best knowledge, no one has conducted a comparative study of the three routing protocols chosen up to now: AODV, ZRP, and LAR under the DDoS attack [10]. In [22], the authors have examined the performance analysis of four AODV routing protocols, dynamic source routing (DSR), destination-sequenced distance-vector routing (DSDV), and the optimized link state routing protocol (OLSR). Then they concluded the implementation of these protocols under greyhole attacks [23] and blackhole attacks [24, 25] would suffer an efficiency degradation compared to normal situations.

In [26], the author presented a performance evaluation survey for the routing protocols AODV and temporary ordered routing algorithm (TORA) for various performance parameters under DDoS attack. The simulation had only been implemented for 11 nodes. The results of this experiment showed that AODV performs better than TORA.

In [2], the authors inspected the number of malicious nodes increases with various reactive routing protocols during the flood attack; the overall network performance decreases. During their work, the authors discussed many performance metrics such as the ratio of packet transmission, jitter, and throughput. The result was that AODV performs best under flood attack.

In [27], the authors evaluated the performance of AODV and secure ad-hoc on-demand vector routing (SAODV) under blackhole, greyhole, selfish and flooding routing protocols [28, 29]. They perceive that the SAODV, which is an AODV extension designed to achieve the security features in the routing messages, it has better performance under blackhole, greyhole and selfish attacks. In comparison, under the flooding attack, the AODV has superior efficiency. The author also found that the network's effect of flooding and blackhole attacks is greater than that of other attacks.

In [30], the author investigated the effect of the Resource Consumption Attack (RCA) on MANET performance, particularly the AODV protocol. This concentrated on how the number of attackers and their location would influence the packet delivery ratio and jitter delay. The results of the study may help other researchers propose solutions that could reduce the impact of RCA.

3. DDOS ATTACK SIMULATION MODEL (DDOSM)

Figure 5 demonstrates the architecture of DDoSM, the layout is extended to the three routing protocols of choice, namely ZRP, AODV, and LAR. When a regular link begins using CBR traffic, it sends out a stream of flooding packets to overload the destination. The study simulations were constructed using NS-2 to evaluate the effectiveness of the DDoS attack, and the simulation findings were collected from two experimental scenarios. The first scenario as shown in Figure 6 was applied by varying one factor which is the number of attackers (3, 6 and 9), all attackers have a radio range of 250 m. and the attackers were placed near the destination where they could exhaust their limited received window which in the worst case leads to resource consumption which helps to clarify the effect of flooding attack.

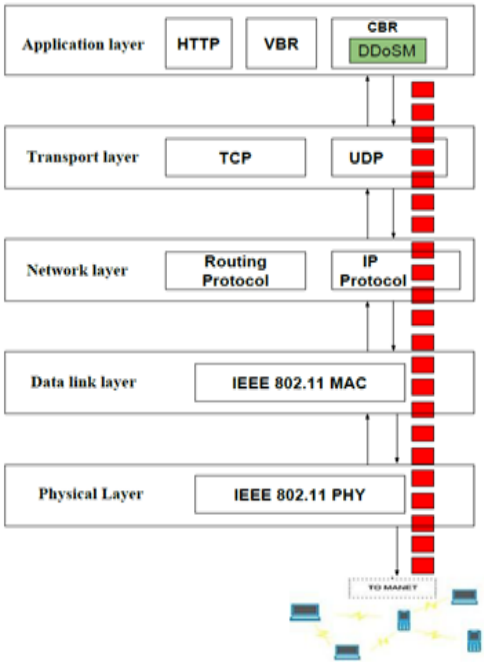

Figure 5. DDoSM system architecture

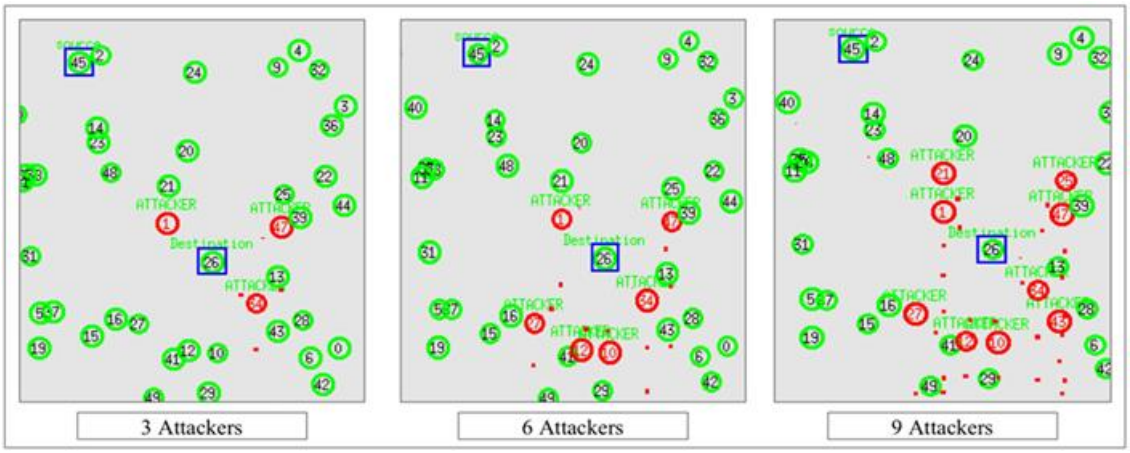

Figure 6. Network topology for scenario I

The second scenario as shown in Figure 7 carries out the results by varying the radio range (300, 350 and 400 m), whereas the number of attackers is 3. Using a traffic load of 2 packets/s, the CBR connection starts from 2 s until the simulation ends. The attackers target the CBR connection in both cases by using a flood rate equal to 50 packets/s and the size of the packets is 1000 bytes and the attacker begins simulation until the end at 30 s. The parameters of the simulation used in all scenarios are shown in Table 1.

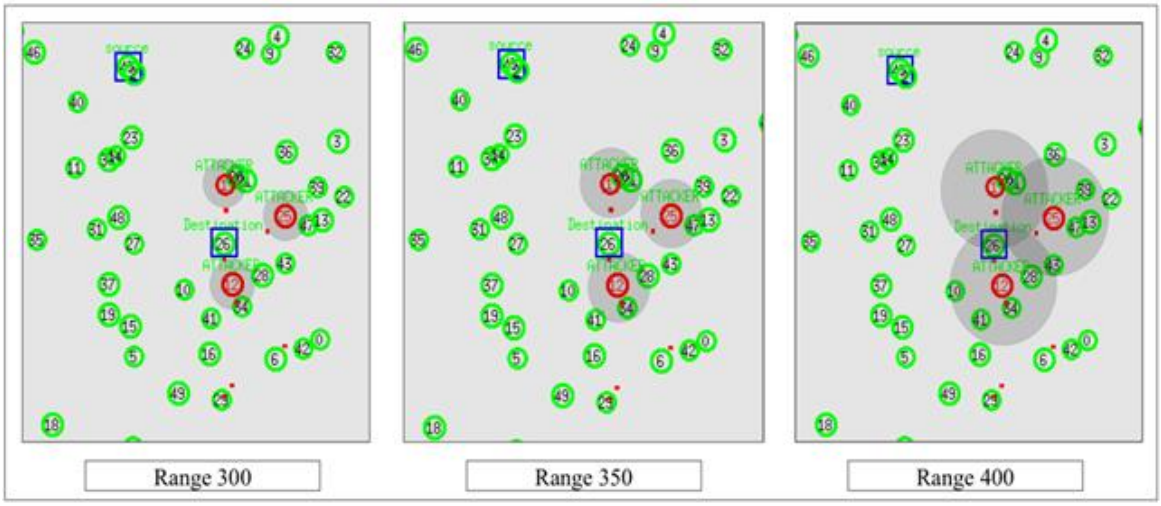

Figure 7. Network topology for scenario II

Table 1. Simulation parameters

Parameter	Value
Network area	1000m x 1000m
No. of nodes	50
Node speed	0 – 7 m/s
Bandwidth	11 mbps
Traffic Packet size	512 bytes
Packet rate	2 packets per second
Traffic type	CBR
Flood interval	0.02 s
Flood rate	50 packets per second
Mobility model	Random waypoint
Antenna model	Omnidirectional
Propagation model	Two-ray ground
Period of emulation	100 s

The research focused on each routing protocol; under the DDoS attack, two performance metrics were calculated.

a. Throughput

Throughput is the number of bits per unit of time at the destination. In each experimental outcome, this represents the sum of the destinations throughput values.

b. End-to-end delay

It is the time between the first bit of a packet being sent by the source and the end bit of the packet being sent by the destination side. In each experiment, the average time is recorded for the destination

4. RESULTS AND DISCUSSIONS

4.1. Experimental results for the scenario I

Flooding CBR traffic affects MANET, where overwhelmed traffic is sent to the destination, creates congestion in the usual route resulting in the data packet falling as a result, affecting the network performance metrics. The experimental results in Figure 8 demonstrate that the network throughput declines when there is an increased number of attackers. If put near the destination, DDoSM will create this difference under 3, 6, and 9 attackers. ZRP decreases network throughput by around 42.1 percent compared to the normal situation (zero attackers) when 3 attackers are added. In the case of LAR, it reduces network

throughput by 51.5 percent. AODV's efficiency is poorer than other protocols because it eliminates network communication by 57.4%. ZRP reduces network throughput by around 49.1 percent compared to the normal scenario (zero attackers) in the case of 6 attackers applied. In the case of LAR, it reduces network throughput by 56.3 percent. AODV's performance is lower than other protocols because it reduces network throughput by 61.7%. In the worst case of this experiment, as implemented by 9 attackers, ZRP reduces network throughput by about 57.1 percent compared to the normal (zero attackers) situation. In the case of LAR, it reduces network throughput by 62.8 percent. AODV's efficiency is poorer than other protocols because it eliminates network communication by 67.3%. As noted in Figure 8, the impact of the attack is directly proportional to the number of attackers, as a result, it is assumed that if the number of attackers reaches more than 10, the network could crash because of the number of attackers is 3, the performance in LAR and AODV dropped to half the normal scenario for each protocol and the performance of 9 attackers continues to decrease. Figure 9 shows the effects of the attack on the end-to-end delay compared to the number of attackers, AODV has the largest effect compared to other protocols where, in the case of 9 attackers, the delay increases by around 98.71% and in the case of LAR and ZRP, the delay increases by 97.1% and 96% respectively, resulting in ZRP outperforming other protocols in terms of end-to-end delay.

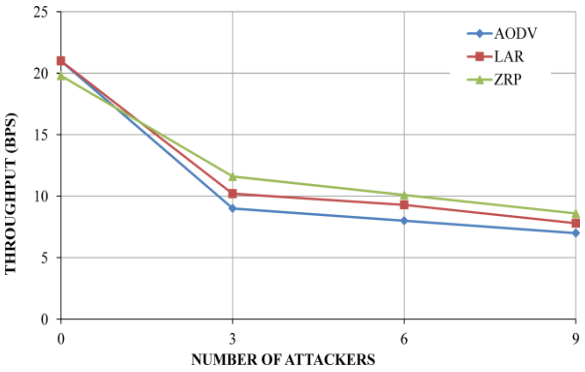

Figure 8. Throughput vs number of attackers

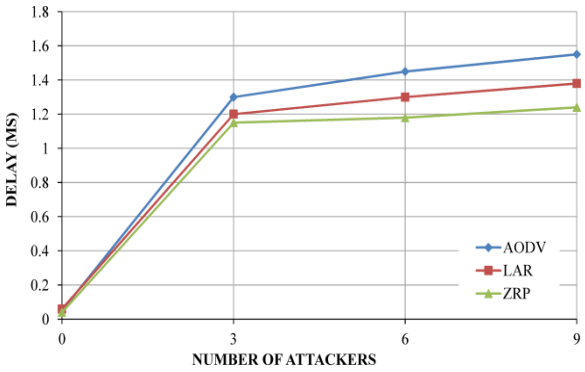

Figure 9. Delay vs number of attackers

4.2. Experimental results for scenario II

The simulation results of scenario II demonstrate the effect of varying the attacker's radio range under the performance metrics (throughput and end-to-end delay), the radio range specifies the maximum distance a node can send its data. Increasing the radio range leads to decreasing the network throughput and increasing the end-to-end delay. In scenario II, the number of attackers is 3 and the flooding rate is 50 packets/s. The focus was on varying the radio range and observing its impact on the three routing protocols, it can be seen from the Figure 10, ZRP shows a slight decrease in network throughput while LAR shows an average dropping in throughput, however, AODV shows the worst performance under all ranges. Figure 11 depicts the effect of different radio range on the end-to-end delay, AODV has the highest delay compared to other two protocols in all ranges, in contrast, ZRP has the minimum delay and better performance.

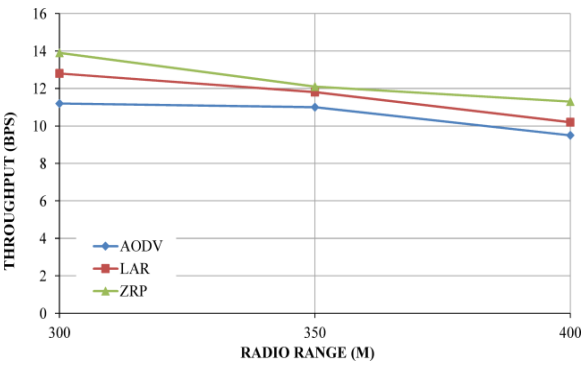

Figure 10. Throughput vs radio range

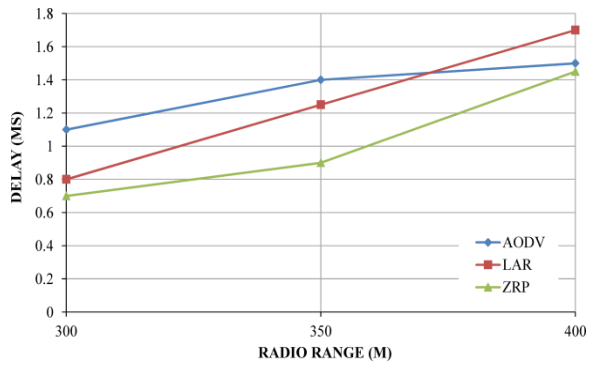

Figure 11. Delay vs radio range

5. CONCLUSION AND FUTURE WORK

This research analyzed three types of routing protocols in MANET and implemented a DDoSM using CBR traffic flooding. DDoS has been deployed using the NS2 emulator in the routing protocols AODV, ZRP and LAR. Additionally, the efficiency of routing protocols was analyzed using performance parameters of the throughput and end-to-end delay. Finally, the assessment and analysis effects of the protocols were presented. In both scenarios, ZRP worked best in terms of throughput and end-to-end delay and exhibited the most resistance behavior relative to the protocols AODV and LAR. For future work, we'll evaluate the performance of these protocols on other performance metrics, including jitter and overhead routing. We are now looking to do a realistic deployment.

ACKNOWLEDGEMENTS

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

REFERENCES

[1] R. Raju L. and C. R. K. Reddy, "Node activity based trust and reputation estimation approach for secure and QoS routing in MANET," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5340-5350, 2019.

[2] P. Kakkar and K. Saluja, "Performance investigations of reactive routing protocols under flooding attack in MANET," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 623-627, 2016.

[3] S. G. Datey and T. Ansari, "Mobile Ad-hoc networks its advantages and challenges," *International Journal of Electrical and Electronics Research*, vol. 3, no. 2, pp. 491-496, 2015.

[4] M. Yadav and N. Uparosiya, "Survey on MANET: Routing protocols, advantages, problems and security," *International Journal of Innovative Computer Science & Engineering*, vol. 1, no. 2, pp. 12-17, 2014.

[5] P. Nayak and B. Vathasavai, "Impact of random mobility models for reactive routing protocols over MANET," *International Journal of Simulation--Systems, Science & Technology*, vol. 17, pp. 13.1-13. 9, 2016.

[6] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wireless Networks*, vol. 25, pp. 1685-1695, 2019.

[7] S. Sarika, et al., "Security issues in mobile ad hoc networks," *Procedia Computer Science*, vol. 92, pp. 329-335, 2016.

[8] O. H. Younis, et al., "A Survey on Security Attacks/Defenses in Mobile Ad-hoc Networks," *Communication on Applied Electronics*, vol. 6, no. 10, pp. 1-9, 2017.

[9] L. Sergii, et al., "Detection of the botnets' low-rate DDoS attacks based on self-similarity," *International Journal of Electrical & Computer Engineering*, vol. 10, pp. 3651-3658, 2020.

[10] A. Saravanan, et al., "A new framework to alleviate DDoS vulnerabilities in cloud computing," *International Journal of Electrical & Computer Engineering*, vol. 9, no. 5, pp. 4163-4175, 2019.

[11] M. Narender and B. N. Yuvaraju, "Preemptive modelling towards classifying vulnerability of DDoS attack in SDN environment," *International Journal of Electrical & Computer Engineering*, vol. 10, no. 2, pp. 1599-1611, 2020.

[12] A. D. Basheer, et al., "SIEM-based detection and mitigation of IoT-botnet DDoS attacks," *International Journal of Electrical & Computer Engineering*, vol. 10, pp. 2182-2191, 2020.

[13] N. Beijar, "Zone routing protocol (ZRP)," Networking Laboratory, Helsinki University of Technology, Finland, pp. 1-12, 2002.

[14] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2070-1721, 2003.

[15] Y. B. Ko and N. H. Vaidya, "Location-Aided Routing (LAR) in mobile ad hoc networks," *Wireless networks*, vol. 6, pp. 307-321, 2000.

[16] M. F. Khan and I. Das, "An Investigation on Existing Protocols in MANET," in *Innovations in Computer Science and Engineering*, pp. 215-224, 2019.

[17] C. E. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *IETF MANET Internet Draft*, 2003.

[18] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications (WMCSA'99)*, New Orleans, LA, pp. 90-100, 1999.

[19] M. Abdelhaq, et al., "Securing mobile ad hoc networks using danger theory-based artificial immune algorithm," *PLoS ONE*, vol. 10, no. 5, p. e0120715, 2015.

[20] S. R. Malwe, et al., "Location and selective-bordercast based enhancement of zone routing protocol," in *2016 3rd International Conference on Recent Advances in Information Technology (RAIT)*, pp. 83-88, 2016.

[21] A. Kumar, et al., "Location-based routing protocols for wireless sensor networks: A survey," *Wireless Sensor Network*, vol. 9, no. 1, pp. 25-72, 2017.

[22] M. S. Khan, et al., "A comparative performance analysis of MANET routing protocols under security attacks," in *Mobile and Wireless Technology*, pp. 137-145, 2015.

[23] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks*, vol. 24, pp. 565-579, 2018.
[24] S. Prakash and A. Swaroop, "A brief survey of blackhole detection and avoidance for ZRP protocol in MANETs," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 651-654, 2016.
[25] L. A. K. Al Dulaimi, et al., "Black hole attack behavioral analysis general network scalability," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 2, pp. 677-682, 2019.
[26] S. Garg, "Performance analysis of AODV and TORA under DDoS attack in MANETs," *IJSR International Journal of Science and Research*, vol. 3, no. 10, pp. 297-304, 2014.
[27] M. A. Abdelshafy and P. J. B. King, "AODV and SAODV under attack: Performance comparison," in *International Conference on Ad-Hoc Networks and Wireless*, pp. 318-331, 2014.
[28] M. M. Ghonge, et al., "Selfish attack detection in mobile Ad hoc networks," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-4, 2017.
[29] K. A. P. Yamini, et al., "Handling Selfishness over Collaborative Mechanism in a Mobile Ad hoc Network," *Journal of Cyber Security and Mobility*, vol. 7, no. 1&2, pp. 39-52, 2018.
[30] M. Abdelhaq, et al., "The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing," *International Journal of Network Security*, vol. 16, pp. no. 4, pp. 399-404, 2014.