ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

# A SIMULATION MODEL FOR THE EFFECT OF RESOURCE CONSUMPTION ATTACK OVER MANET

Raed Alsaqour[1], Maha Abdelhaq[2], Njoud Alghamdi[2], Maram Alneami[2], Tahani Alrsheedi[2], Salma Aldghbasi[2], Rahaf Almalki[2] and Sarah Alqahtani[2]

[1]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

E-Mail: raed.ftsm@gmail.com

## ABSTRACT

Mobile Ad-Hoc Network (MANET) is an infrastructure-less network which has an ability to configure itself without any centralized management. The topology of MANET changes dynamically which make it open for new nodes to join it easily. The openness area of MANET makes it very vulnerable to different types of attacks. One of the most dangerous attacks is resource consumption attack (RCA). This type of attack, the attacker consumes the normal node energy by flooding it with bogus packets. Routing in MANET is susceptible to RCA and this is a crucial issue which deserves to be studied and solved. Therefore, the main objective of this paper is to study the impact of RCA on three routing protocols namely; Ad hoc On-Demand Distance Vector **(**AODV) and Dynamic Source Routing (DSR); as a try to find the most resistant routing protocol to such attack. The contribution of this paper is a new RCA model (RCAM) which applies RCA on the three chosen routing protocols using NS-2 simulator.

**Keywords:** mobile ad hoc network, routing protocols, AODV, DSR, resource consumption attack.

## INTRODUCTION

The Mobile Ad-Hoc Network (MANET) is a set of mobile wireless nodes that connect with each other through multi-hop routes without the assistance of any networks, such as base stations [1, 2]. MANET can be used in several areas such as military areas, sensor networks, rescue operations and conferences [3]. MANETs have access to information and resources regardless of their geographical location due to self-configuring networks, MANETs are independent of central network management.

In MANET, various types of protocols are implemented for routing. This protocols can be classified into reactive, proactive and hybrid protocols for routing [4, 5]. The objective of this paper is to study three routing protocols namely, Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) under the effect of resource consumption attack (RCA). To the best of our knowledge, no researcher has introduced such study until now. The contribution of this project is a new Resource Consumption Attack Model (RCAM) in which the attack is applied on MANET routing using network simulator-2 (NS-2). Specifically, RCAM has to be applied on AODV and DSR to test their resistance under attack.

The remainder of the paper is arranged accordingly as follows: In Section 2, we provide background and related work. Section 3 presents the RCA mechanism. Section 4 presents the simulation settings. In section 4, we explain the findings and discussions. Finally, the conclusions and possible guidelines for further work are presented in Section 5.

## BACKGROUND AND RELATED WORK

### Mobile Ad-Hoc Network (MANET)

The abbreviation MANET is for Mobile Ad Hoc Network. It can be defined as mobile networks and wireless machines nodes that are connected with each other (See Figure-1). Moreover, the nodes can be connected to one another through point-to-point access with an IP address. In addition, there is no central administration when these nodes forward packet between one another. This means that there is a weak security for MANET since there is a dynamic topology when nodes forward these packets to each other [6].

There are different reasons why MANET was developed. For instance, the MANET was first developed around 1991 in order to create communication networks in the battlefield. Therefore, with the advancement of technology in the current world, the emergence of small devices and the interest that people have in wireless technology, the MANETs are gaining efforts as a result of increase in the number of broad applications that comes with it. Also, the MANETs are gaining efforts since they can be provided anytime and everywhere with limited or without communication infrastructure (Khan, Olanrewaju, Anwar, Najeeb, & Yaacob, 2018). Furthermore, MANETs are gaining popularity because they are comfortable to use. Furthermore, the MANETs are classified as mobile ad hoc network and it can be applied in mobile networks by using a wireless link to organize an infrastructure network and has become comfortable to use. Example on this application; military sector, flood and earthquake (Rao & Siddhartha, 2019).

VOL. 16, NO. 13, JULY 2021 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences



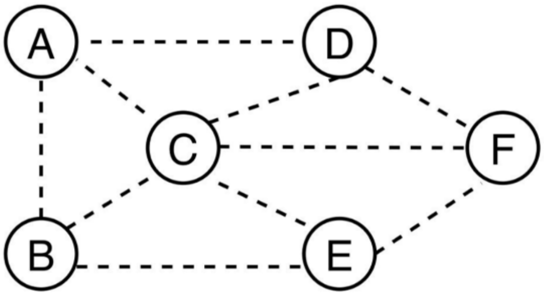


**Figure-1.** MANET Network Topology.

### Ad Hoc On-Demand Distance Vector (AODV)

AODV is a reactive protocol where a network builds routes at the beginning of the connection (Perkins & Royer, 1999; Sultan & Zaki, 2017). Especially for MANET, AODV was developed. It gets solely on-demand routes that transform it into a very beneficial and needed MANET algorithm. To identify and manage routes, AODV carries out two distinct operations: route discovery and maintenance. AODV uses two signals to monitor the path discovery and route maintenance process. Control messaging used by AODV include: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

The discovery of the route would rely on the RREQ and RREP. In routing table entries, the path information for the intermediate nodes is stored. The discovery process is shown in Figure-2. In Figure-2, the route discovery source is initiated by sending the RREQ message from source node S. In the Figure-3, as the RREQ is obtained by the destination or mid-node, the RREP will be sent to the source node and destination node sequence number is applied to the routing table. Afterward, the RREP message is unicasted to the source node. The route is configured when an RREP is sent to the source node. The message includes the full route to the destination and is stored with next-hop addresses. Maintenance of routes depends, however, on the RERR communication and can handle the dynamic MANET network topology. The RERR message also controls the routes by transmitting a warning of a link failure to the other nodes.

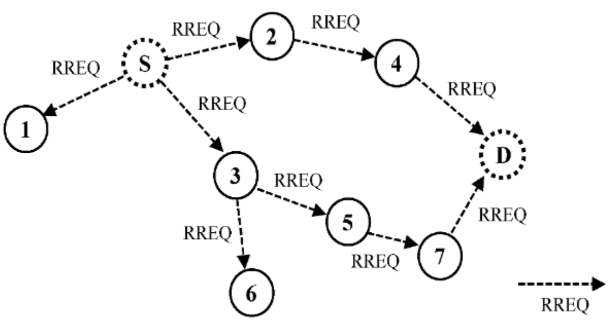


**Figure-2.** AODV broadcasts RREQ packet.

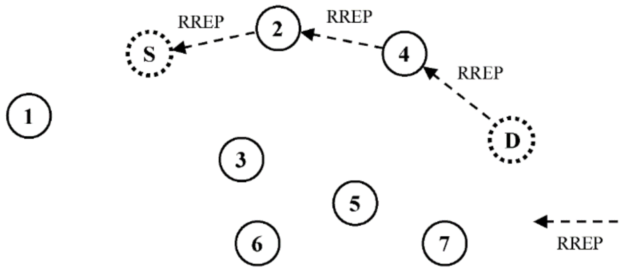


**Figure-3.** AODV replies RREP packet.

### Dynamic Source Routing (DSR)

As a protocol, DSR is made up of two primary tasks: Route Discovery and Route Management. If a network source wants to send a packet to a destination and does not have a path in its cache to the destination, it begins a route search process by sending the RREQ packet to the network. The RREQ package includes the address of the source node, the destination node, a unique sequence number, and an empty route log. The other nodes can validate their cache after receiving route requests. If the destination route is not available in the cache, the node can add its address to the record and re-broadcast the request. The node can add its data to the original packet data if it has a route to the destination, and send an RREP reply to the source. Figure-4 shows a basic DSR process.

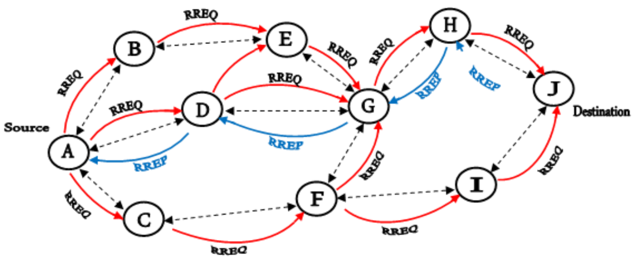


**Figure-4.** DSR routing protocols.

### RESOURCE CONSUMPTION ATTACK (RCA)

The RCA is aimed to disable network services to the user by sending more packet traffic on network to prevent users from accessing these services [7]. It is caused unavailable network and response time is high. This attack consume power and may prevent the service temporarily or permanently for the purposes of many of them exhausting the memory or the channel bandwidth [8]. RCA sends malware from many computers and different locations to the victim until the service or application is disrupted then they cannot find the client as shown in Figure-5. The attacks can access to these resources and take all available resources. This cause impact on network performance [9].

ARPN Journal of Engineering and Applied Sciences



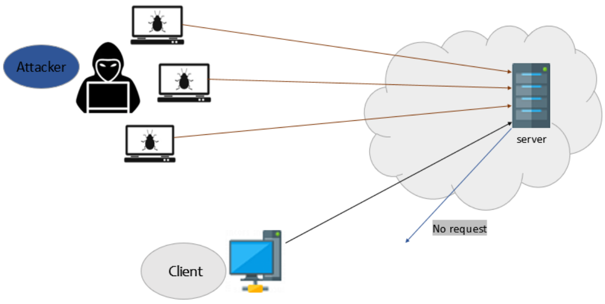


**Figure-5.** Resource Consumption Attack.

**RELATED WORK**

In [10], the authors evaluate and compare the performance of AODV, FSR, DSDV and DSR protocols using NS2 a wireless communication simulator[11]. Based on the efficiency parameters, which are throughput, packet delivery ratio and average end-to-end delay, they also reveal the simulation results. The observed findings revealed that the reactive type AODV algorithm performs better in terms of throughput and average end-to-end delay, whereas the reactive type DSR is marginally better in terms of packet delivery ratio among the routing algorithms.

In [12], the author studies and contrasts the efficiency of the AODV, DSR, DSDV, RAODV, AOMDV and TORA protocols. The focus was on TORA and AODV under Distributed Denial-of-Service (DDoS) attack on MANET [13, 14]. They compare these protocols based on load, packet loss, delay, throughput, and packet delivery ratio. The observed findings revealed that TORA performed much better under normal conditions than TORA under a DDoS attack. Similarly, AODV has done much better under regular circumstances.

In [15], the authors compared three MANET routing protocols, which are: DSDV, DSR and AODV using NS-2, they used three metrics to evaluate performance which are throughput, packet delivery ratio and jitter. Over all the parameters observed, the findings revealed that the AODV protocol outperformed the other two protocols when the network reaches 35 nodes, while the DSR in smaller networks is the better protocol.

In [16], the authors analyse the MrDR approach designed to detect DoS attacks in the MANET context and compare it with the current Trust Enhanced Anonymous On-Demand Routing Protocol (TEAP) method, which is also focused on the principle of trust. To evaluate the efficiency of the suggested approach to the TEAP approach, they used two metrics: packet delivery ratio and network overhead. The outcome shows the usefulness of the approach suggested as it provides improved network efficiency relative to TEAP.

In [17], The authors intend to compare multiple AODV, DSR and DSDV protocols to the simulator's influential measurements. In addition, they used three metrics: throughput, loss of packets and delay time. The outcome indicates that there is a minimum number of missing packets for DSR relative to DSDV and AODV.

Based on the summarized related work, as shown in Table-1, we introduced a comparative study of the three chosen routing protocols, which are: DSR and AODV under the impact of RCA. To the best of our knowledge, no researcher has introduced a new model for RCA on AODV and DSR to study their resistance against the attack.

**Table-1.** Related works comparison.

| Study | Our Study | [15] | [17] | [16] | [10] | [12] |
|---|---|---|---|---|---|---|
| Performance metrics VS Network metrics | throughput, E2E, energy consumed *VS* Number of attacks, radio range | throughput, packet delivery ratio, Jitter. *VS* nodes, simulation time, radio propagation model, MAC support | throughput, packet loss, E2E *VS* simulation time, packet size | PDR, the network overhead *VS* simulation time | throughput, PDR, E2E *VS* nodes, simulation time, MAC protocol, packet size, radio propagation model | load, packet loss, E2E, throughput, PDR *VS* Traffic, mobility model |

PDR: Packet Delivery Ratio, E2E: End to End delay

**SIMULATION ENVIRONMENT AND SETTINGS**

To determine the effect of a RCA attack, this research experiments were generated using NS-2. The experiments were conducted by varying the number of attackers by one variable (1, 2, 3 and 4). The attackers were positioned close to the destination, helping to illustrate the impact of the RCA attack. The total period simulated is 50.0s. The Constant Bit Rate (CBR) connection begins with a traffic load of 5 packets/s from 5.0s to the end of the simulation. The packets size is 512 bytes and the interval between packets sending is >0.2s. The attacker starts at beginning of simulation until the end. The mobility and radio propagation models used are, random waypoint and two-ray ground reflection models, respectively. Table-2 below illustrates the network settings that we used in our experiments.

VOL. 16, NO. 13, JULY 2021 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

**Table-2.** Simulation settings**.**

| Parameter | Value |
|---|---|
| Network area | 800m × 800m |
| Number of nodes | 20 |
| Nodes speed | 0 - 5 m/s |
| Bandwidth | 11 mbps |
| Traffic Packet size | 512 bytes |
| Packet rate | 5 packets per second |
| Traffic type | CBR |

In this research, we study the effect of RCA against the adhoc routing protocols using the performance metrics: throughput, end-to-end delay and energy consumption. We repeat each experiment 5 times and calculate the average of each our selected performance metrics.

**End-to-End (E2E) Delay**

The E2E delay refers to the average time consumed in one millisecond to transfer a data packet successfully from source to destination across your network [18]. It includes any delay, such as latency of route discovery buffering, media-control retransmission delay (MAC), lining at the queue of the interface, propagation delay and the time of transmission. The delay of E2E is calculated as follows:

$$\text{E2E delay} = \frac{\sum_{i=1}^{n}(R_i - S_i)}{n} \quad (1)$$

where $n$ is the amount of successfully transmitted data packets across the network, $i$ is the specific packet ID, $Ri$ is the time to receive a unique ID packet $i$ and $Si$ is the time it takes to deliver a unique ID packet $i$.

**Throughput**

The throughput parameter is the average of the effective data packets received over the entire duration of the simulation. This measures the efficiency and effectiveness of the routing protocol when processing data packets from the destinations [19]. Throughput estimated per second in kilobits (kbps). For measure the throughput the following formula is used:

$$\text{Throughput} = \sum \frac{\text{Total bytes received}}{\text{Stop time} - \text{Start time}} \quad (2)$$

**Energy Consumption**

Energy consumption is an obvious concern for ad hoc mobile wireless networks, since most mobile hosts run on minimal battery power. We calculate the total nodes' energy, and we can derive the total energy consumption.

**Experimental Cases**

Case-1 studies the effects of varying the number of attackers on throughput, end-to-end delay, and energy consumption on all studied protocols in MANET as shown in Figure-6, where the source node (1) and the attackers are located near-destination node (17).

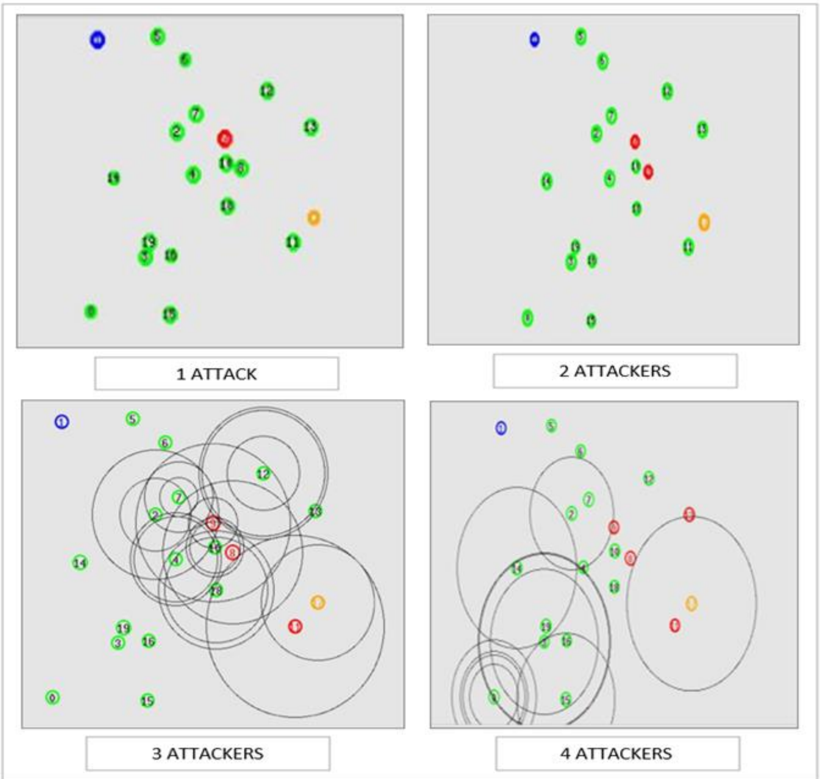


**Figure-6.** Case-1 with 1-4 attackers.

ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

Case-2 studies the effects of varying the attacker's radio range on throughput, end-to-end delay, and energy consumption on all studied protocols in MANET as shown in Figure-7, where the source node (1) and the attackers are located near-destination node (17) and we select constant number of attackers which is 4 attackers.

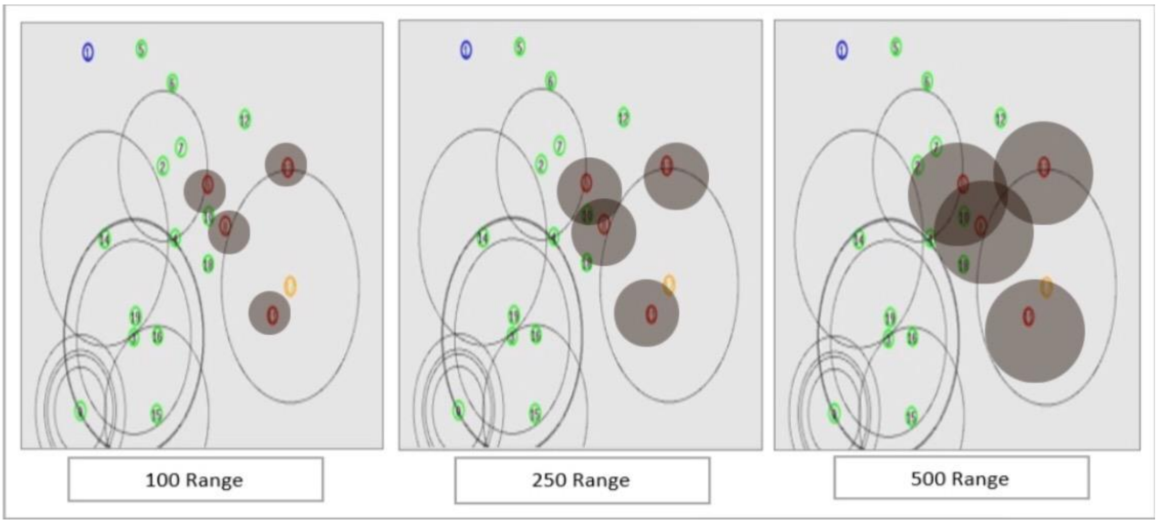


**Figure-7.** Case-2 with different radio ranges.

**RESULTS AND DISCUSSIONS**

Figures 8-10 show the effect of flooding CBR data packets on DSR and AODV protocols by increasing the flooder attackers' number; 1 attacker, 2 attackers, 3 attackers, and 4 attackers.

Figures 8-10 show that the increasing in the number of attacks on DSR reduces the throughput, increases the end-to-end delay, and increases the energy consumptions values. The experimental results in Figure-8 show that when the number of attackers increases, the network throughput decreases. The throughput value at 1 attacker is 507.5 kbps, at 2 attackers is 486.8 kbps, at 3 attackers is 355.6 kbps, and the final case which is 4 attackers is 280.5 kbps. The experimental results, in Figure-9, show also the effect of number of attackers in DSR end-to-end delay. When the number of attackers increases, the network end-to-end delay increases. The end-to-end delay value at 1 attacker is 0.7 ms, at 2 attackers is 1.4 ms, at 3 attackers is 2 ms, and the final case which is 4 attackers is 2.9 ms. In addition, the experimental results in Figure-10 show that when the number of attackers, the network total energy consumption increases. The energy consumption value at 1 attacker is 396 kj, at 2 attackers is 480 kj, at 3 attackers 590 kj, and the final case which is 4 attackers is 875 kj.

Figures 8-10 show that the increasing the number of attacks on AODV reduces the throughput, increases the end-to-end delay and increases the energy consumptions values.

The experimental results in Figure-8 show that when the number of attackers increases, the network throughput decreases. The throughput value at 1 attacker is 20.8 kbps, at 2 attackers is 20.4 kbps, at 3 attackers is 20.3 kbps, and the final case which is 4 attackers is 20.1 kbps. The experimental results in Figure-9 shows that when the number of attackers increases, the network end-to-end delay increases. The end-to-end delay value at 1 attacker is 0.035 ms, at 2 attackers is 0.045 ms, at 3 attackers is 0.051 ms, and the final case which is 4 attackers is 0.14 ms. Also, the experimental results in Figure-10 shows that when the number of attackers increases, the network total energy consumption increases. The energy consumption value at 1 attacker is 67 kj, at 2 attackers is 78 kj, at 3 attackers 87 kj, and the final case which is 4 attackers is 96 kj.

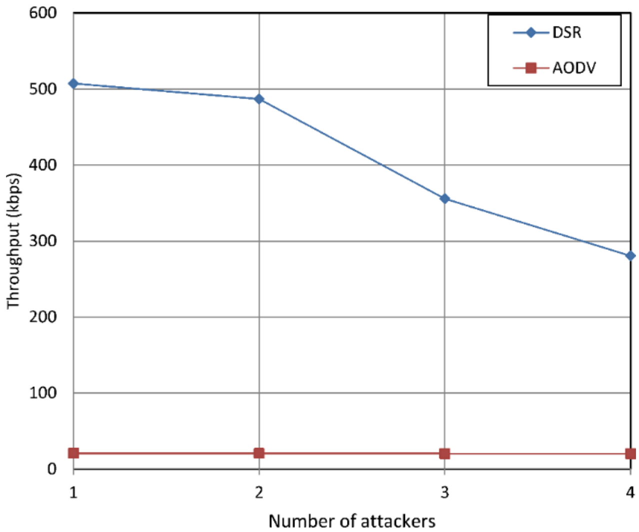


**Figure-8.** Throughput against the number of attackers.

VOL. 16, NO. 13, JULY 2021 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

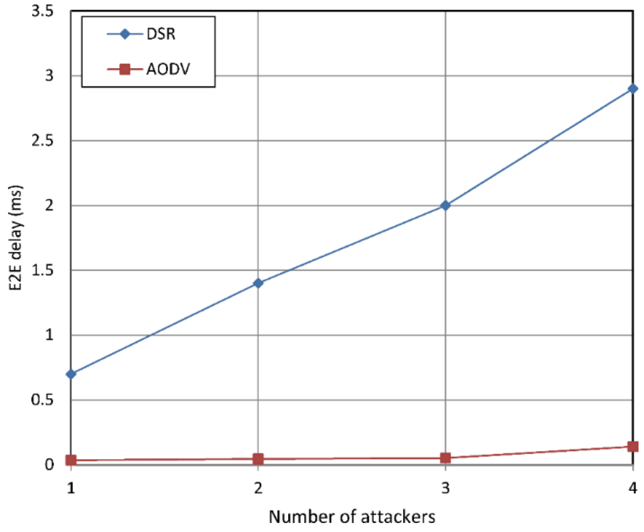


**Figure-9.** E2E delay against the number of attackers.

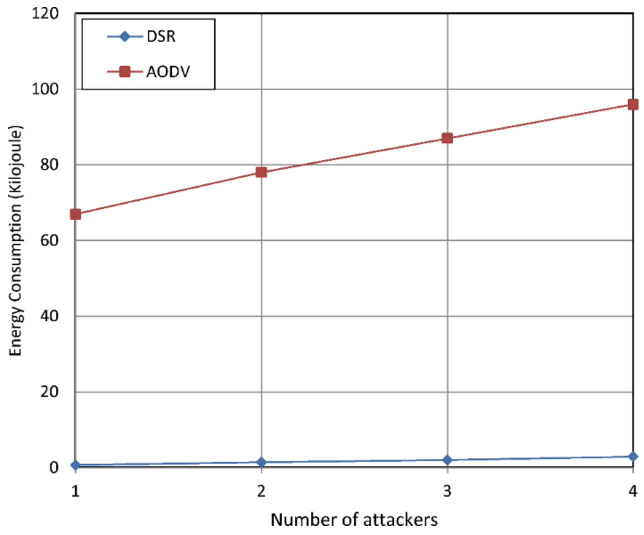


**Figure-10.** Energy consumption against the number of attackers.

Figures 11-13 show the effect of flooding CBR data packets on DSR and AODV protocols by changing the flooder attackers' radio range, which are 100 m, 250 m, and 500 m.

Figures 11-13 show that the increasing the radio range to different radio range on DSR decreases the throughput, increases the end-to-end delay, and increases the energy consumptions values. Figure-11 shows that when the radio range of attackers increases, the network throughput decreases. The throughput value at radio range 100 m is 350 kbps, at radio range 250 m is 300 kbps, and at radio range 500 m is 180 kbps. Figure-12 shows that when the radio range of attackers increases, the network end-to-end delay increases. The end-to-end delay value at radio range 100 m is 2.6 ms, at radio range 250 m is 3 ms, and at radio range 558.7 m is 4.2 ms. Finally, Figure-13 shows that when the radio range of attackers increases, the network total energy consumption increases. The energy consumption value at radio range 100 m is 820 kj, at radio range 250 m is 850 kj, and at radio range 500 m is 1050 kj.

Figures 11-13 show that the increasing the radio range to appropriate radio range on AODV decreases the throughput, increases the end-to-end delay, and increases the energy consumptions values.

Figure-11 show that when the radio range of attackers increases, throughput decreases. The throughput value at radio range 100 m is 20.8 kbps, at radio range 250 m is 18 kbps, and at radio range 558.7 m is 11.4 kbps. Figure-12 show that when the radio range of attackers increases, the network end-to-end delay increases. The end-to-end delay value at radio range 100 m is 0.12 ms, at radio range 250 m is 0.14 ms, and at radio range 558.7 m is 0.2 ms. Figure-13 show that when the radio range of attackers increases, the total energy consumption increases. The energy consumption value at radio range 100 m is 80 kj, at radio range 250 m is 110 kj, and at radio range 500 m is 180 kj.

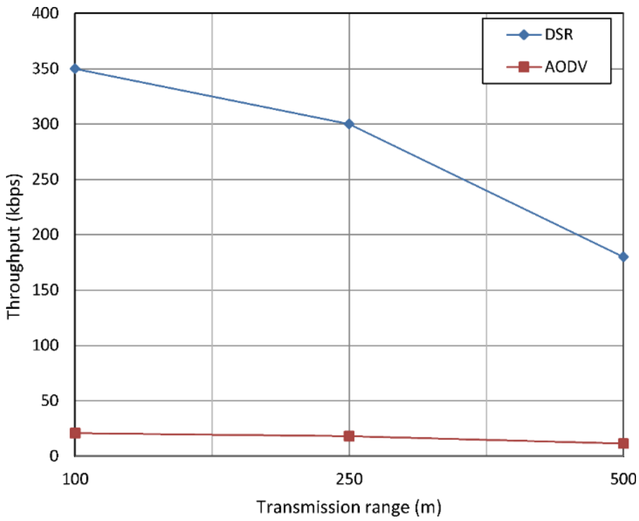


**Figure-11.** Throughput against the transmission range.

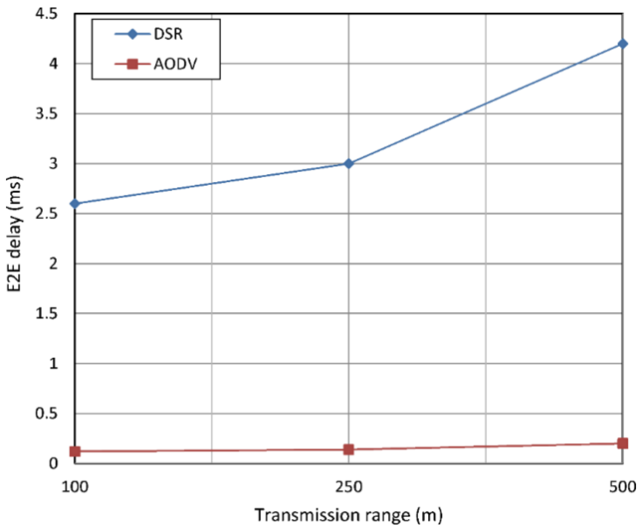


**Figure-12.** E2E delay against the transmission range.

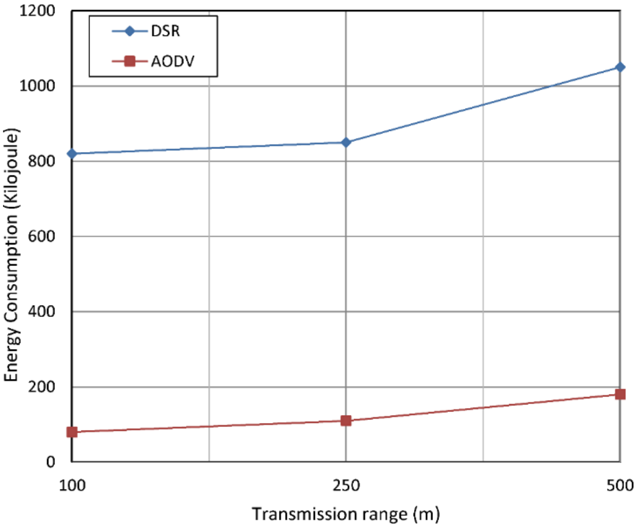


**Figure-13.** Energy consumption against the transmission range.

## CONCLUSIONS AND FUTURE WORK

In this paper, we studied two routing protocols categories in MANET; reactive and proactive routing protocols, and we introduced a RCA model that implemented on AODV and DSR routing protocols using NS-2 simulator. The main objective of our paper is experimenting the impact of RCA over MANET to determine the most resistant protocol against the attack. The experiment results show that the DSR protocol is more sensitive to flooding attack than the AODV protocol in the term of throughput, end-to-end delay, and energy consumption. The DSR has more throughput while AODV has less end-to-end delay and less energy consumption than the DSR protocol, in all experiments, so the AODV is the better than the DSR in facing RCA in MANET.

As future work, we will evaluate the performance of these protocols using other performance metrics such as jitter, routing overhead, compare between theses protocols by developing same flooding mechanism to get the most sensitive protocol between them. Also, as a future work, we will create a real experiment with real mobile devices operate MANET network with AODV and DSR protocols to transfer data and measure real power consumption in resource consumption attacks.

## ACKNOWLEDGEMENT

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] A. S. V. Rao and C. Siddhartha. 2019. "Two-Step Verification Technique for Isolation of Black hole Attack in MANETs. International Journal of Recent Technology and Engineering (IJRTE). 8: 491-495.

[2] A. Vijaya Krishna and S. Naseera. 2018. A comprehensive and proportional analysis of course-plotting algorithms in MANETs. ARPN Journal of Engineering and Applied Sciences. 13: 3770-3781.

[3] L. Raja and S. S. Baboo. 2014. An overview of MANET: Applications, attacks and challenges. International Journal of Computer Science and Mobile Computing, vol. 3, pp. 408-417, 2014.

[4] [4] I. Sumra, P. Sellappan, A. Abdullah and A. Ali. 2018. Security issues and challenges in Manet-Vanet-Fanet: A Survey. EAI Endorsed Transactions on Energy Web. Vol. 5.

[5] [5] M. Tariq, H. Fareed and R. Alsaqour. 2016. Performance analysis of reactive routing protocols in mobile ad hoc network using NS2. ARPN Journal of Engineering and Applied Sciences. 11: 4267-4271.

[6] H. Alani and R. Alsaqour. 2017. Routing discovery scheme for high mobility in MANET. ARPN Journal of Engineering and Applied Sciences. 12: 536-543.

[7] M. S. Abdelhaq, R. A. Alsaqour, M. Al-Hubaishi, T. Alahdal and M. Uddin. 2014. The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing. IJ Network Security. 16: 376-381.

[8] R. van Rijswijk-Deij, A. Sperotto and A. Pras. 2014. DNSSEC and its potential for DDoS attacks: a comprehensive measurement study. in Proceedings of the 2014 Conference on Internet Measurement Conference. pp. 449-460.

[9] A. Dhanapal and P. Nithyanandam. 2019. The Slow HTTP DDoS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. Scalable Computing: Practice and Experience. 20: 669-685.

[10] Y. Bai, Y. Mai and N. Wang. 2017. Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs. in 2017 Wireless Telecommunications Symposium (WTS), Chicago, IL. pp. 1-5.

[11] T. Issariyakul and E. Hossain. 2009. Introduction to network simulator 2 (NS2). in Introduction to network simulator NS2, 1st ed: Springer, Boston, MA. pp. 1-18.

[12] S. Garg. 2014. Performance analysis of AODV and TORA under DDoS attack in MANETs. IJSR

International journal of science and research. 3: 297-304.

[13] R. Singh and T. P. Sharma. 2019. Present Status of Distributed Denial of service (DDoS) attacks in internet world. International Journal of Mathematical, Engineering and Management Sciences. 4: 1008-1017.

[14] P. Oberoi, S. Mittal and R. K. Gujral. 2019. ADRCN: A framework to detect and mitigate malicious insider attacks in cloud-based environment on IaaS. International Journal of Mathematical, Engineering and Management Sciences. 4: 654-670.

[15] A. A. Ajibesin, M. M. Kah, A. T. Ishaq and C. A. Ajibesin. 2019. Performance Analysis of Topology and Destination Based Routing Protocols in Mobile Ad-Hoc Network Using NS2. in 2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT). pp. 1-6.

[16] A. Alsumayt, J. Haggerty and A. Lotfi. 2018. Evaluation of detection method to mitigate DoS attacks in MANETs. in 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). pp. 1-5.

[17] A. Sahoo, A. Shreya, C. S. Dash, I. Priyadarshini, S. Sobhanayak, S. S. Panda, *et al*. 2018. Performance Evaluation of AODV, DSDV and DSR Routing Protocol for Wireless Adhoc Network. in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN). pp. 348-351.

[18] D. Gao, H. Lin, Y. Liu and A. Jiang. 2016. Minimizing End-to-End Delay Routing Protocol for Rechargeable Wireless Sensor Networks. Adhoc & Sensor Wireless Networks. Vol. 34.

[19] N. Muthukumaran. 2017. Analyzing throughput of MANET with reduced packet loss. Wireless Personal Communications. 97: 565-578.