A Simulation Modeling for the Effect of Resource Consumption Attack over Mobile Ad Hoc Network

Raed Alsaqour[1], Maha Abdelhaq[2*], Njoud Alghamdi[3], Maram Alneami[4], Tahani Alrsheedi[5], Salma Aldghbasi[6], Rahaf Almalki[7], Sarah Alqahtani[8]

[*]{Corresponding Author: msabdelhaq@pnu.edu.sa }

[1]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia

[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia

Summary

Mobile Ad-hoc Network (MANET) is an infrastructure-less network that can configure itself without any centralized management. The topology of MANET changes dynamically which makes 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 the Resource Consumption Attack (RCA). In 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 that deserves to be studied and solved. Therefore, the main objective of this paper is to study the impact of RCA on two 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 two chosen routing protocols using the NS-2 simulator.

Keywords:

Mobile ad hoc network; Routing Protocols; AODV; DSR; Resource Consumption Attack.

1. Introduction

The Mobile Ad-Hoc Network (MANET) is a set of mobile wireless nodes that connect 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. These protocols can be classified into reactive, proactive and hybrid protocols for routing [4, 5]. The objective of this paper is to study two 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 a 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 related wok. Section 5 presents the simulation environment and settings. In section 6, we explain the results and discussion. Finally, the conclusions and possible guidelines for further work are presented in Section 7.

2. Background and Related Work

2.1 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 (See Fig. 1). Moreover, the nodes can be connected 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 weak security for MANET since there is a dynamic topology when nodes forward these packets to each other [6, 7].

There are different reasons why MANET was developed. For instance, the MANET was first developed around 1991 to create communication networks on 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 the increase in the number of broad applications that come with it. Also, the MANETs are gaining efforts since they can be provided anytime and everywhere with limited or without communication infrastructure [8]. Furthermore, MANETs

Manuscript received September 5, 2023
Manuscript revised September 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.9.14

are gaining popularity because they are comfortable to use. Furthermore, the MANETs are classified as mobile ad hoc networks and they can be applied in mobile networks by using a wireless link to organize an infrastructure network and has become comfortable to use. Examples of this application are; military sector, flood and earthquakes.

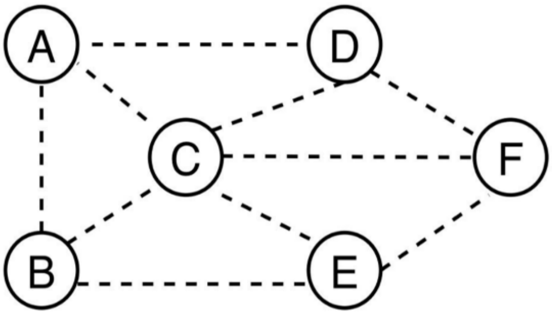

Fig. 1 MANET Network Topology

2.2 Ad Hoc On-Demand Distance Vector (AODV)

AODV is a reactive protocol where a network builds routes at the beginning of the connection [9, 10]. Especially for MANET, AODV was developed. It gets solely on-demand routes that transform it into a very beneficial and needed MANET algorithm [11]. 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 includes 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 Fig. 2. In Fig. 2, the route discovery source is initiated by sending the RREQ message from source node S. In Fig. 3, as the RREQ is obtained by the destination or mid-node, the RREP will be sent to the source node and the 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.

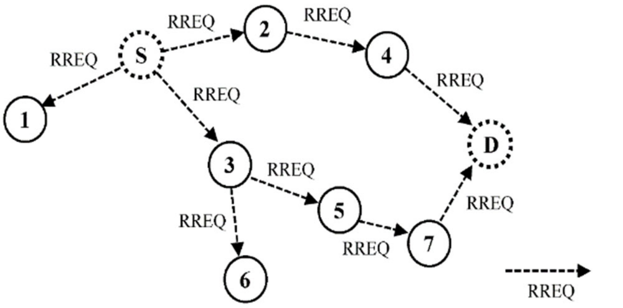

Fig. 2 AODV broadcasts RREQ packet

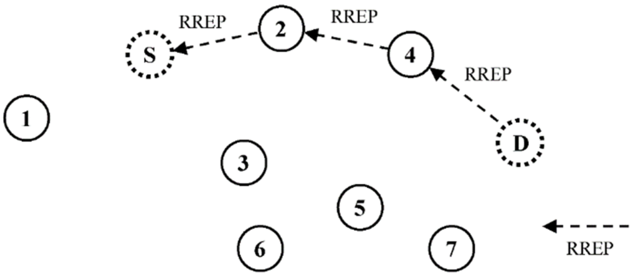

Fig. 3 AODV replies RREP packet

2.3 Dynamic Source Routing (DSR)

As a protocol, DSR is made up of two primary tasks: Route Discovery and Route Management [11]. 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. Fig. 4 shows a basic DSR process.

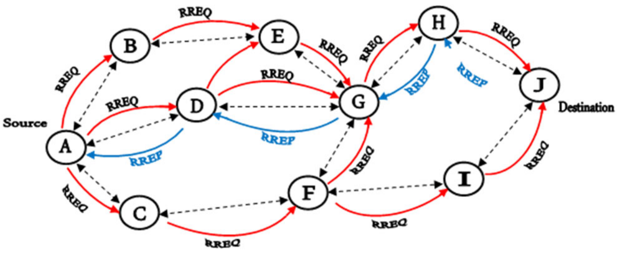

Fig. 4. DSR routing protocols

3. Resource Consumption Attack (RCA)

The RCA is aimed to disable network services to the user by sending more packets' traffic on the network to prevent users from accessing these services [12]. It is caused unavailable network and response time is high. This attack consumes power and may prevent the service temporarily or permanently for many of them exhausting the memory or the channel bandwidth [13]. 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 Fig. 5. The attacks can access these resources and take all available resources. This causes an impact on network performance [14].

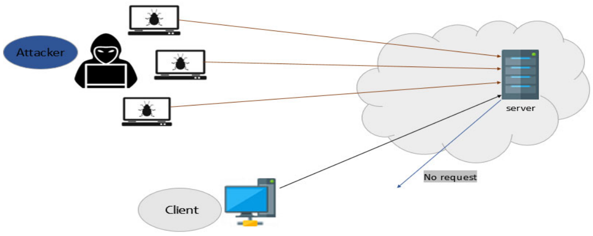

Fig. 5 Resource Consumption Attack

4. Related Work

In [15], the authors evaluate and compare the performance of AODV, FSR, DSDV and DSR protocols using NS2 a wireless communication simulator [16]. 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 [17], 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 [18, 19]. 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 [20], 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. Overall, 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 [21], the authors analyze 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 [22], 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 two 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 work comparison

Study	***Our Study***	***[20]***	***[22]***	***[21]***	***[15]***	***[17]***
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

5. Simulation Environment and Settings

To determine the effect of the RCA attack, these 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 the 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.

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
Channel	Channel/WirelessChannel
propType	Propagation/TwoRayGround
antType	Antenna/OmniAntenna
llType	LL
ifqType	Queue/DropTail/PriQueue
ifqType	CMUPriQueue
ifqLen	50
phyType	Phy/WirelessPhy
macType	Mac/802_11
adhocRouting	AODV or DSR
agentTrace	ON
routerTrace	ON
macTrace	ON
movementTrace	ON
Energymodel	EnergyModel
initialEnergy	100
rxPower	0.5
txPower	0.9
idlePower	0.45
sleepPower	0.05

5.1 Model Architecture

Fig. 6 shows the RCAM system architecture. The RCAM is placed within the network layer of the TCP/IP protocol stack. It is applied to the two chosen routing protocols namely; AODV and DSR. When IP protocol requests a route, the routing protocol starts to discover paths in this instance, RCAM starts a resource consumption attack to MANET by sending RREQ packets.

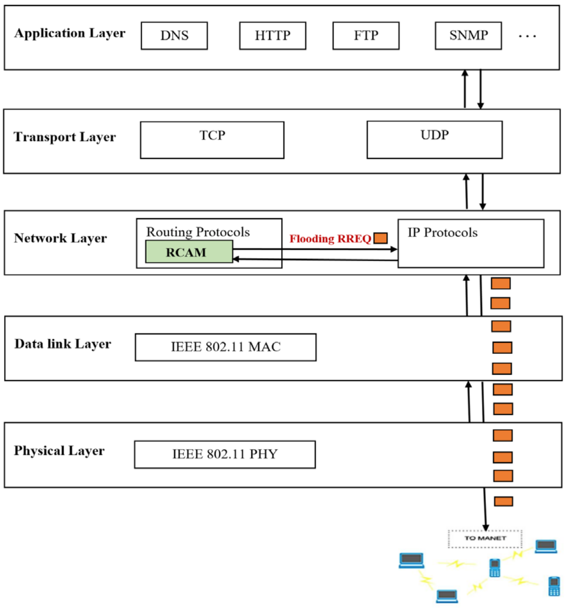

Fig. 6. RCAM System Architecture

5.2 Performance Metrics

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 of our selected performance metrics.

5.2.1 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 [23]. 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:

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

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.

5.2.2 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 [24]. Throughput estimated per second in kilobits (kbps). To measure the throughput the following formula is used:

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

5.2.3 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.

5.2.4 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 Fig. 7, where the source node (1) and the attackers are located near-destination node (17).

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 Fig. 8, where the source node (1) and the attackers are located near-destination node (17) and we select the constant number of attackers which is 4 attackers.

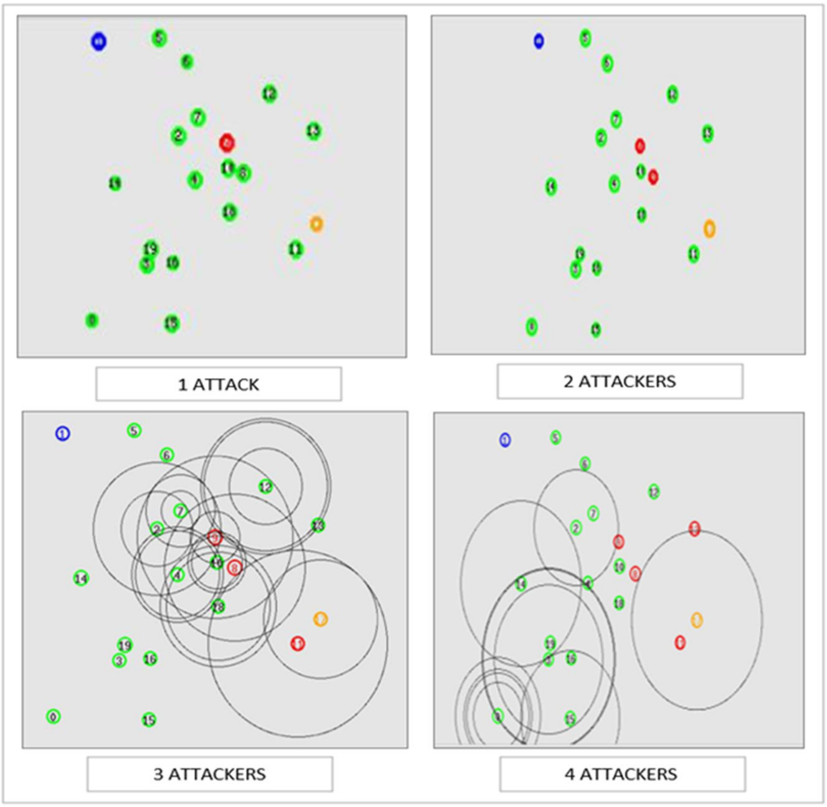

Fig. 7 Case-1; 1-4 Attackers

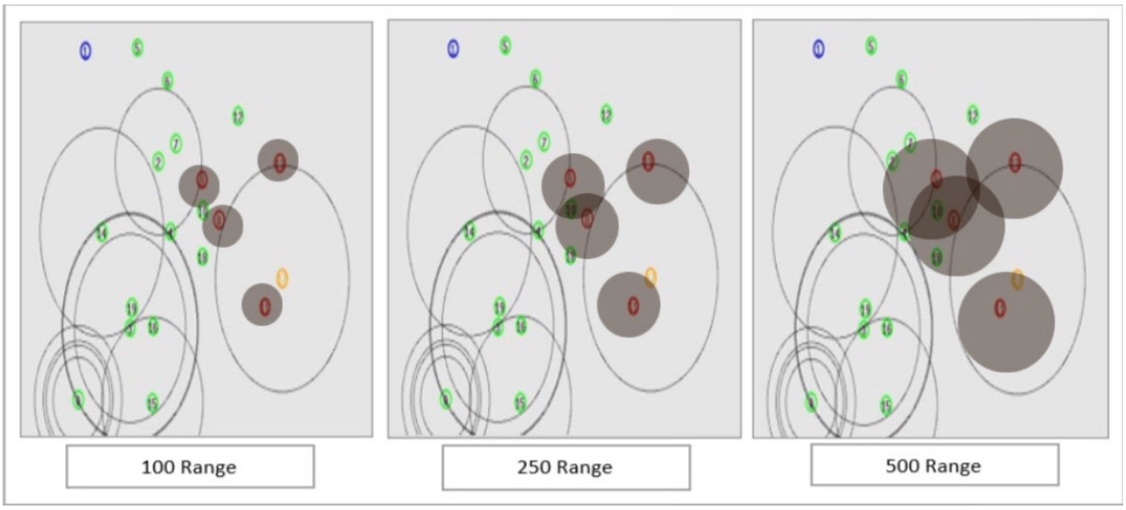

Fig. 8 Case-2; 100-500 meters radio ranges

6. Results and Discussion

Figs. 9-11 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. Figs. 9-11 show that the increase 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 Fig. 9 show that when the number of attackers increases, the network throughput decreases. For DSR, 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. For AODV, it is 20.8 kbps, 20.4 kbps, 20.3 kbps and 20 kbps respectively.

The experimental results, in Fig. 10, also show the effect of the number of attackers in DSR end-to-end delay. When the number of attackers increases, the network end-to-end delay increases. For DSR, 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. For AODV, it is 0.035 ms, 0.045 ms, 0.051 ms and 0.14 ms respectively.

Also, the experimental results in Fig. 11 show that when the number of attackers increases, the network total energy consumption increases. For AODV, 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. For AODV, it is 396 kJ, 480 kJ, 590 kJ and 875 kJ respectively.

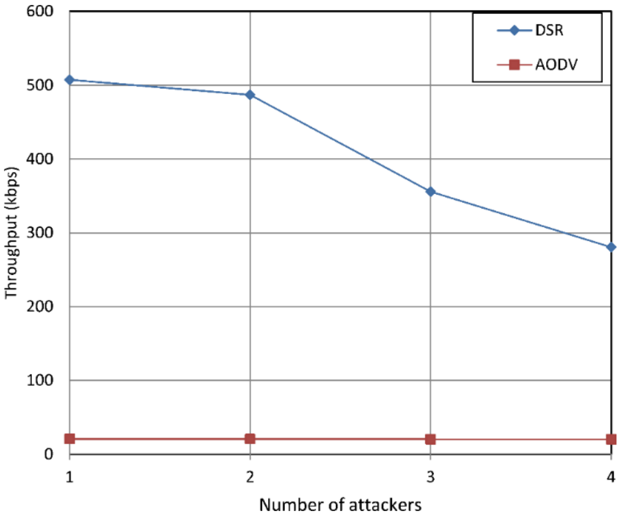

Fig. 9 Throughput against the number of attackers

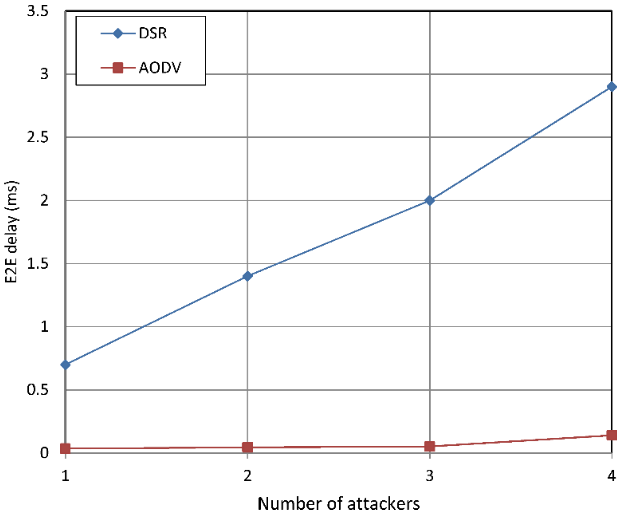

Fig. 10 E2E delay against the number of attackers

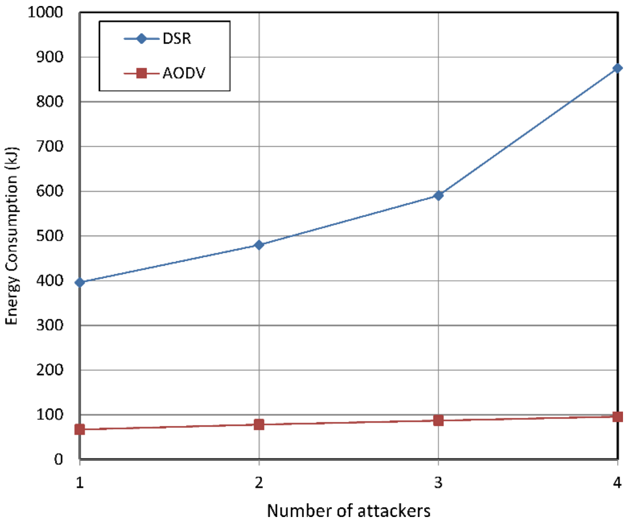

Fig. 11 Energy consumption against the number of attackers

Figs. 12-14 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. Figs. 12-14 show that increasing the radio range to the appropriate radio range on AODV decreases the throughput, increases the end-to-end delay, and increases the energy consumptions values. Figs. 12-14 show that 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.

Fig. 12 shows that when the radio range of attackers increases, the network throughput decreases. For DSR, 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. For AODV, it is 20.8 kbps, 18 kbps, 11.4 kbps respectively.

Fig. 13 shows that when the radio range of attackers increases, the network end-to-end delay increases. For DSR, 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 500 m is 4.2 ms. For AODV, it is 0.12 ms, 0.14 ms, 0.2 ms respectively.

Finally, Fig. 14 shows that when the radio range of attackers increases, the total energy consumption increases. For AODV, 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. For DSR, it is 820 kJ, 850 kJ and 1050 kJ respectively.

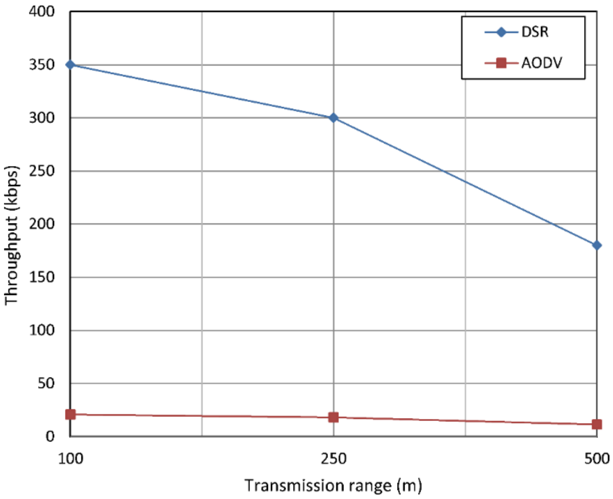

Fig. 12 Throughput against the transmission range

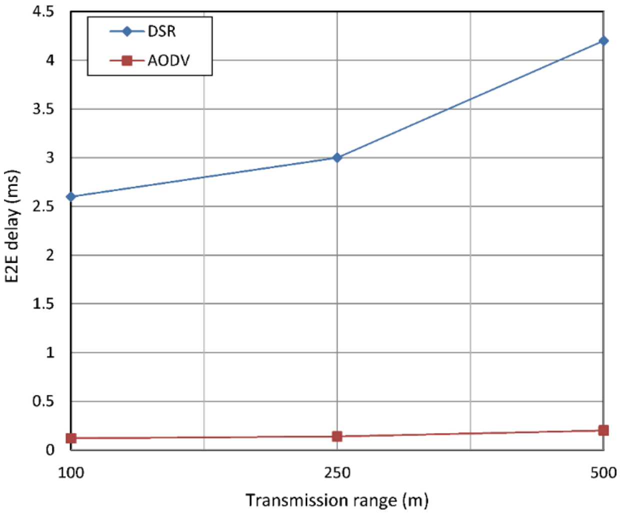

Fig. 13E2E delay against the transmission range

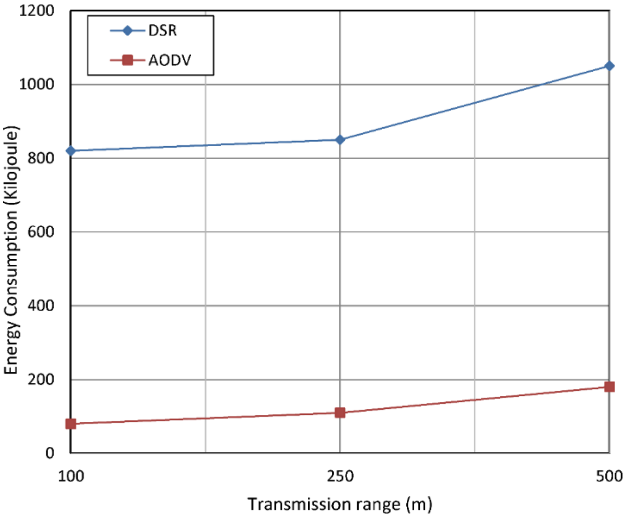

Fig. 14 Energy consumption against the transmission range

7. Conclusions and Future Work

In this paper, we studied two routing protocols categories in MANET; reactive and proactive routing protocols, and we introduced the RCA model that was implemented on AODV and DSR routing protocols using NS-2 simulator. The main objective of our paper is to experiment with 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 better than the DSR in facing RCA in MANET.

In future work, we will evaluate the performance of these protocols using other performance metrics such as jitter, routing overhead and compare these protocols by developing the same flooding mechanism to get the most sensitive protocol between them. Also, as 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 throughput, delay and energy consumption in resource consumption attacks.

Acknowledgments

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, "Two-Step Verification Technique for Isolation of Black hole Attack in MANETs," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 8, pp. 491-495, 2019.

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

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

[4] I. Sumra, P. Sellappan, A. Abdullah, and A. Ali, "Security issues and challenges in Manet-Vanet-Fanet: A Survey," *EAI Endorsed Transactions on Energy Web,* vol. 5, pp. 1-6, 2018.

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

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

[7] A. Al Sharah, M. Alhaj, and F. Al Naimat, "Trade-off between Energy Consumption and Transmission Rate in Mobile Ad-Hoc Network," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 12, pp. 245-252, 2121.

[8] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, A. R. Najeeb, and M. Yaacob, "A survey on MANETs: architecture, evolution, applications, security issues and solutions," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 12, pp. 832-842, 2018.

[9] E. M. Royer and C. E. Perkins, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA, pp. 90-100, 1999.

[10] M. T. Sultan and S. M. Zaki, "Evaluation of energy consumption of reactive and proactive routing protocols in MANET," *arXiv preprint arXiv:1706.06322,* 2017.

[11] S. M. Alkahtani and F. Alturki, "Performance Evaluation of Different Mobile Ad-hoc Network Routing Protocols in Difficult Situations," *(IJACSA) International Journal of Advanced Computer Science and Applications,* vol. 12, pp. 158-167, 2021.

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

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

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

[15] Y. Bai, Y. Mai, and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for

MANETs," in *2017 Wireless Telecommunications Symposium (WTS)*, Chicago, IL, 2017, pp. 1-5.

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

[17] S. Garg, "Performance analysis of AODV and TORA under DDoS attack in MANETs," *IJSR International journal of science and research,* vol. 3, pp. 297-304, 2014.

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

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

[20] A. A. Ajibesin, M. M. Kah, A. T. Ishaq, and C. A. Ajibesin, "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)*, 2019, pp. 1-6.

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

[22] A. Sahoo, A. Shreya, C. S. Dash, I. Priyadarshini, S. Sobhanayak, S. S. Panda*, et al.*, "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)*, 2018, pp. 348-351.

[23] D. Gao, H. Lin, Y. Liu, and A. Jiang, "Minimizing End-to-End Delay Routing Protocol for Rechargeable Wireless Sensor Networks," *Adhoc & Sensor Wireless Networks,* vol. 34, pp. 77-98, 2016.

[24] N. Muthukumaran, "Analyzing throughput of MANET with reduced packet loss," *Wireless Personal Communications,* vol. 97, pp. 565-578, 2017.