The Impact of Selfishness Attack on Mobile Ad Hoc Network

Maha Abdelhaq[*1], Raed Alsaqour[2], Noura Albrahim[1], Manar Alshehri[1], Maram Alshehri[1], Shehana Alserayee[1], Eatmad Almutairi[1], Farah Alnajjar[1]

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia.
[2]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, 93499 Riyadh, Saudi Arabia.

Abstract: Mobile Ad-Hoc Network (MANET) is an infrastructure-less network that has the ability to 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 selfishness attack. In this type of attack, each node tries to save its resources, behave selfishly or non-cooperatively by not forwarding packets that are generated by other nodes. Routing in MANET is susceptible to selfishness attack 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 selfishness attack on two routing protocols namely, Ad hoc On-Demand Distance Vector (AODV) and Destination Sequenced Distance Vector (DSDV), as a try to find the most resistant routing protocol to such attack. The contribution of this paper is a new Selfishness Attack Model (SAM) which applies selfishness attack on the two chosen routing protocols in the NS-2 simulator. According to the conducted simulation results, AODV shows higher performance than DSDV under the effect of selfishness attack.

***Keywords*:** mobile ad hoc network, routing protocols, AODV, DSDV, Selfishness attack.

1. Introduction

Mobile Ad-Hoc Network (MANET) is a set of mobile wireless nodes that communicate with each other, possibly via multi-hop paths, without any infrastructure like base stations [1, 2]. MANET can be used in several areas such as military areas, sensor networks, rescue operations and conferences [3]. Regardless of geographic location, due to self-configuring networks, MANETs are independent of central network administration offering access to information as well as services.

Specific routing protocol types are used in MANET. These can be categorized into reactive, constructive and hybrid routing protocols[4-6]. The objective of this paper is to study two routing protocols namely, Ad hoc On-Demand Distance Vector (AODV) and Destination Sequenced Distance Vector (DSDV) under the effect of selfishness attack [7]. To the best of our knowledge, no researcher has introduced such a study until now. The contribution of this paper is a new Selfishness Attack Model (SAM) in which the attack is applied to MANET routing using network simulator-2 (NS-2). Specifically, SAM has been applied on both AODV and DSDV to experiment with their resistance under a selfishness attack. The results gained in this paper shows the outperformance of AODV over DSDV.

The rest of this paper is organized as follows. In Section 2, we provide the background and related work. In Section 3, we present the proposed simulation settings. In Section 4, we explain the results and evaluations. Finally, the conclusion and possible directions for future work are in Section 5.

2. Background and related work

2.1. Mobile ad hoc network (MANET)

Mobile nodes in MANET are movable (dynamic) forming a temporary network. If the source and destination nodes are distant from each other (outside direct transmission range), they communicate using a sequence of intermediate nodes, which co-operate to forward the traffic to the destination. MANET is easy to set up in short intervals. This can be useful in natural disasters and wars. Furthermore, MANET has several beneficial advantages such as low budget and effortless installation due to the absence of infrastructure and wires, also for the same reason it has an easy deployment and configuration [8, 9].

2.2. Ad hoc On-Demand Distance Vector Routing (AODV) protocol

AODV is a reactive routing protocol where the network establishes routes at a communication startup [10]. AODV was designed specifically for MANET. It obtains the strictly on-demand routes which make it a very useful and desired MANET algorithm. AODV uses two distinct operations to find and maintain routes: the operation of the route discovery process and the operation of route maintenance. AODV uses two messages to monitor the route discovery process and the maintenance of the routes. AODV's control messages are: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

Route discovery relies on the RREQ and RREP. The intermediate node route information is stored in the entries of the routing table. The process for the route discovery is depicted in Fig. 1. In Fig. 1, The source initiates the discovery of the route by transmitting the RREQ message. In Fig. 2, when the destination or intermediate node has the path to the destination receives the RREQ, it sends the RREP to the source node and updates its routing table with the total hop count and the destination node sequence number. The RREP message is later unicasted to the source node. When the RREP is received by the source node, a path is then set. The message includes the full route to the destination, and the next-hop addresses to reach the destination are retained. Path management is therefore based on the RERR message and this

[*] *Corresponding Author*

can handle the topology of the complex network in MANETs. The RERR message also maintains the routes by transmitting an alert of a communication failure to the other nodes.

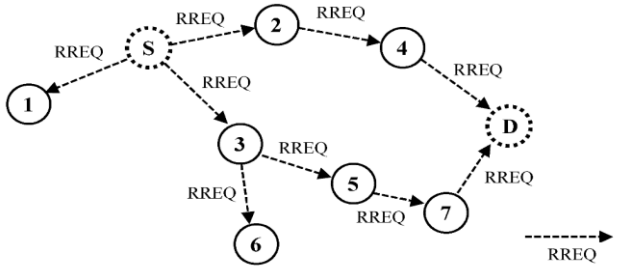

Figure 1. AODV broadcasts RREQ packet

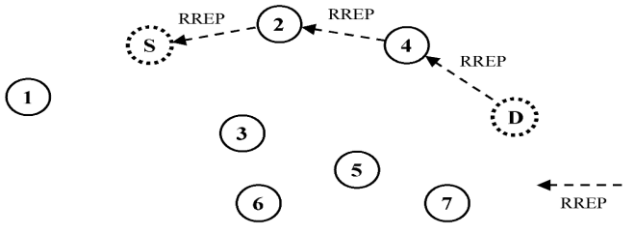

Figure 2. AODV replies RREP packet

2.3. Destination Sequenced Distance Vector (DSDV) protocol

Every node in DSDV has its own routing table. Every mobile node advertises its routing table to its current neighbors (e.g., by transmitting their entries). The entries in the routing table that change dynamically over time, so the routing information should be advertised to ensure that all other mobile nodes are always located by each node. Furthermore, every mobile node agrees on the request to relay data packets to other nodes. The mobile node raises its sequence number by 2 prior to each advertising of a new routing table [11]. The Fig. 3 is an illustration of DSDV routing protocol. In this illustration, a packet is sent (node 3 is not shown) from node 1 to node 3. The next hop for the packet from node 1 is node 4 (Fig. 3a). When node 4 receives the packet, it looks up its routing table to the destination address node 3 (Fig. 3b). Node 4 then transmits the packet as defined in the table to the next hop, in this case node 5 (Figure 3c). This process will be repeated as needed until the packet reaches destination node 3.

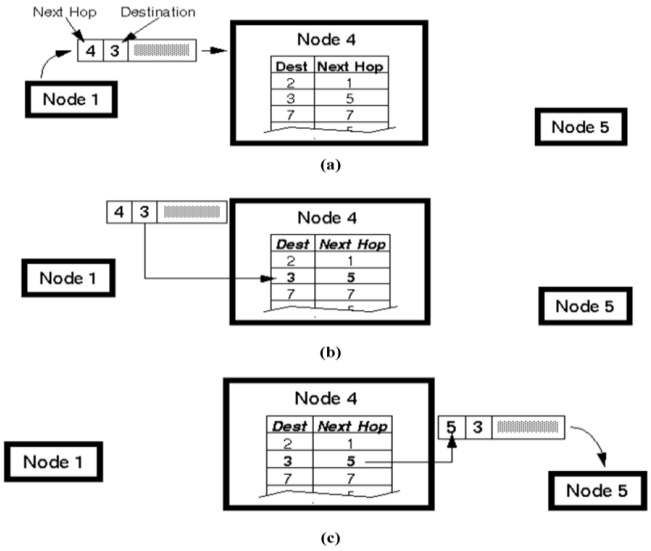

Figure 3. Routing procedure in DSDV [12]. (a) Node 1 transmits a packet to node 4 for forwarding, (b) Node 4 looks up the destination in its routing table, (c) Node 4 retransmits the packet to the next-hop

2.4. Selfishness Attack

In a selfishness attack, a malicious node preserves its resources; as the battery, by not engaging in the operations of the network. A selfish node affects network performance, like routing or data packets based on the routing protocol are not handled correctly. The selfish node usually drops all data and controls packets even if those packets are sent to it. If a selfish node needs to send data to another node, it will start to work as a standard AODV process. The node returns to its silent mode and selfish behavior after it finishes sending its data [13, 14].

The major problem of selfishness is of great interest because the nodes of a MANET are often powered by batteries and energy is a valuable resource [15]. In terms of consumed resources, the effect of this attack model is that these greedy nodes will save a significant portion of their battery life by ignoring huge data packets.

2.5. Related work

In [16], the authors studied and analyzed the performance of AODV in MANET, the malicious selfish node is introduced in the network to analyses the selfish node attack. Network parameters are evaluated and compared using a simulation tool. the selfish node does not forward the packets of other nodes and decreases the performance of the network and the author compares the packet delivery ratio and end-to-end delay with and without the presence of the selfish node in the network.

In [17], the authors studied and analyzed the performance of DSDV, AODV and Zone Routing Protocol (ZRP) under blackhole attack [18]. Blackhole attack is a kind of active attack that an attacker first introduces into the forwarding group and then, instead of forwarding the data packet to the correct destination, it simply drops all the packets it receives resulting in a weak packet delivery ratio that affects DSDV, AODV and ZRP performance.

In [19], the authors analyzed and compared the following AODV, Dynamic Source Routing (DSR), DSDV, Personalized Ad hoc On-Demand Distance Vector (RAODV), Ad Hoc On-Demand Multipath Distance Vector (AOMDV) and Temporally Ordered Routing Algorithm (TORA) routing protocols. The focus was on the TORA, AODV attack on MANET under the Distributed Denial-of-Service (DDoS). They evaluate these protocols based on the metrics of load, packet loss, delay, throughput, packet delivery ratio. The results found have shown that TORA has performed much better under normal conditions than TORA under DDoS attack. Likewise, AODV performed much better under normal conditions.

In [20], the authors examined and analyzed the performance of blackhole, gray hole, selfish and flooding attacks routing protocols for both AODV and Secure Ad-hoc On-demand Distance Vector Routing (SAODV). They concluded that the blackhole and flooding attacks have a dramatic impact on the network performance by using a fake RREP. On the other hand, SAODV's efficiency in the presence of blackhole, a gray whole, is better than AODV [21] and selfishness attacks because the routing packets are not forwarded by SAODV without maintaining authenticity and integrity.

3. Simulation settings and results

To determine the effectiveness of the selfishness attack, the research scenario was designed using NS-2 [22] and obtaining

the simulation experiment results. The experiments have been applied by varying one factor which is the number of attackers (2, 4, 6 and 8) the attackers were placed near the destination which helps clarify the effect of Selfishness attack. The Constant Bit Rate (CBR) connection [23] starts from 1.0s until the end of simulation using a traffic load of 2 packets/s the size of the packet is 512 bytes and the attacker starts at the 30s into simulation until the end. The mobility model and radio propagation model used are random waypoint and two-ray ground reflection models [24, 25], respectively.
Both the simulation parameters and their values are summarized in Table 1.

Table 1. Simulation parameters

Parameter	Value	Unit
Simulator	NS-2 (Version 2.34)	-
Number of runs	5	-
Channel type	Channel/Wireless channel	-
Radio-propagation model	Propagation/Two ray round wave	-
Network interface type	Phy/WirelessPhy	-
MAC Type	Mac /802.11	-
Interface queue Type	Queue/Drop Tail	-
Link Layer Type	LL	-
Antenna	Antenna/Omni Antenna	-
Simulation Area	1000 X 1000	m^2
Routing Protocols	AODV, DSDV	-
Mobility Model	Random Way Point	-
Source Type	CBR	-
Number of nodes	50	
Bandwidth	11	mbps
Packet rate	2 packet per second	
Node speed	0-7	m/s

In this paper, each result is collected from the average of 5 runs for the experiment in NS-2. For each routing protocol, two performance metrics have been calculated which are:

3.1. Average E2E delay

Average E2E delay refers to the average time, in second, consumed to successfully transmit a data packet across the network from source to destination. It encompasses all possible delays, namely, buffering during the latency of route discovery, retransmission delay at the media access control (MAC), queuing at the interface queue, the propagation delay, and the transmission time delay. The average E2E delay is computed with the following formula:

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

where n is the number of data packets which are transmitted successfully over the network, i is the unique packet identifier, R_i is the time needed to receive a packet that has a unique identifier i, and S_i is the time consumed in sending a packet with a unique identifier i.

3.2. Average Throughput (Avg-Throughput)

The average throughput metric is the average of received successful data packets to the total simulation time period. This determines the efficiency and quality of routing protocol when the destinations receive data packets. Avg-Throughput reflects the average of data packet throughput values over the 5 experiment cycles. The equation used to measure the throughput is as follows:

$$Throughput = \sum Packets\ received\ by\ destination \quad (2)$$

The network simulation topology used in the simulation experiments is as shown in Fig. 4. The source node is node number (41), the destination node is node number (42). All the selfishness attackers are located beside the destination node transmission range.

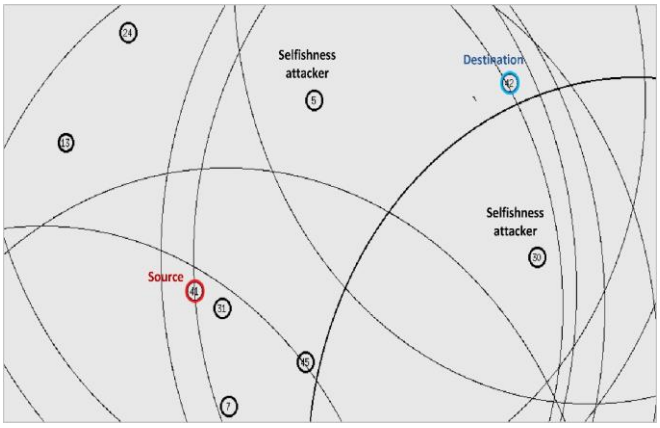

Figure 4. Network simulation topology

3.3. Evaluations

Figures. 5 and 6 show throughput and average E2E delay vary with the number of selfishness attackers in the AODV and DSDV protocols. Selfishness CBR traffic affects MANET, where there is overloaded traffic transmitted to the destination causes congestion in the targeted link, thereby leading to dropping data packet, as a result of selfishness impacts the network performance metrics.
The results of experiments show that AODV is better than DSDV. AODV has higher performance than DSDV, which has a high result of throughput and less end-to-end delay from DSDV. Results show that DSDV collapses to selfishness attacks. The results show that increases in the number of attacks on both protocols reduces the throughput and increase the end-to-end delay values.
The simulation results of throughput versus several attackers are shown in Fig. 5. The experimental results, in Fig. 5, prove that when the number of attackers increases as a result the network throughput decreases. when 2 attackers are applied, AODV throughput has been reduced by around 9.20% compared to the normal scenario (zero attackers). In the case of DSDV, its throughput has been reduced by 18.6%. DSDV has lower performance than AODV. In the case of 4 attackers applied, AODV throughput has been reduced by around 21.40% compared to the normal scenario (zero attackers). In the case of DSDV, its throughput has been reduced by 30.70% In the case of 6 attackers applied, AODV throughput has been reduced by around 29.80% compared to the normal scenario (zero attackers). In the case of DSDV, the throughput reduced by 41.30%. The worst-case of this simulation experiment is when 8 attackers applied, the throughput of AODV has been reduced by 37.50% compared to the normal scenario (zero attackers). In the case of DSDV, it has been reduced by 50%. AODV outperforms DSDV under the effect of all numbers of attackers.
Fig. 6 illustrates the impact of selfishness attack on the end-to-end delay versus the number of attackers, DSDV has the highest effect compared to AODV where in the case of 8 attackers the delay grows around 98.71%, as a result, AODV outperforms DSDV in terms of end-to-end delay.

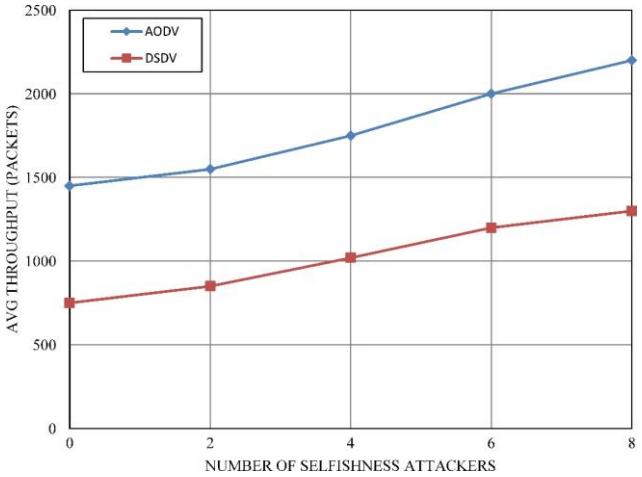

Figure 5. Average throughput vs the number of attackers

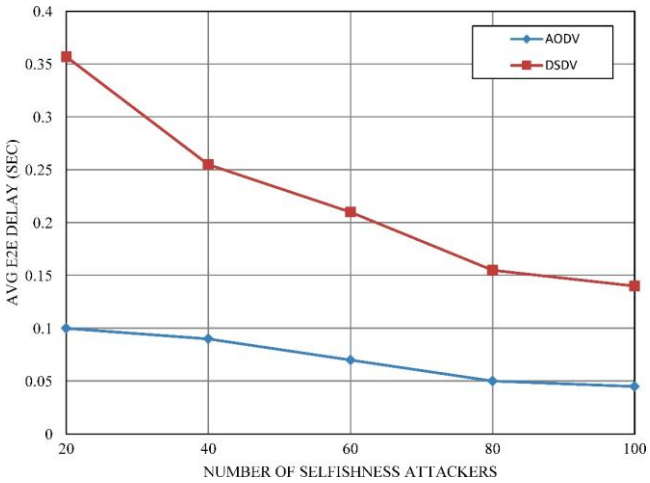

Figure 6. Average E2E delay vs the number of attackers

4. Conclusion and future work

This paper examined the performance of ADOV and DSDV routing protocols in the presence of the selfishness attack affects in those protocols. Average throughput and average end-to-end delay performance metrics were used to compare the performance of two protocols under selfishness attack. The results and their analysis has shown that AODV outperformed and more resistant to selfishness attack than DSDV in terms of throughput and end-to-end delay.

As future work, we will evaluate the performance of these protocols using other performance metrics such as jitter, routing overhead and we are looking for doing the real implementation.

5. Acknowledgment

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

Reference

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad hoc networks*, vol. 1, pp. 175-192, 2003.

[2] A. Shakir, R. Alsaqour, M. Abdelhaq, A. Alhussan, M. Othman, and A. Mahdi, "Novel Method of Improving Quality of Service for Voice over Internet Protocol Traffic in Mobile Ad Hoc Networks," *International Journal of Communication Networks and Information Security*, vol. 11, pp. 331-341, 2019.

[3] M. Yadav and N. Uparosiya, "Survey on MANET: Routing protocols, advantages, problems and security," *International Journal of Innovative Computer Science & Engineering*, vol. 1, pp. 12-17, 2014.

[4] V. Rajeshkumar and P. Sivakumar, "Comparative study of AODV, DSDV and DSR routing protocols in MANET using network simulator-2," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, pp. 2319-5940, 2013.

[5] H. Zafar, N. Alhamahmy, D. Harle, and I. Andonovic, "Survey of reactive and hybrid routing protocols for mobile ad hoc networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 3, pp. 193-216, 2011.

[6] 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)*, 2017, pp. 1-5.

[7] K. A. P. Yamini, S. Kannan, and A. Thangadurai, "Handling Selfishness over Collaborative Mechanism in a Mobile Ad hoc Network," *Journal of Cyber Security and Mobility*, vol. 7, pp. 39-52, 2018.

[8] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, *Ad hoc mobile wireless networks: principles, protocols, and applications*: CRC Press, 2016.

[9] R. C. Poonia and S. Gupta, "Highly Dynamic Networks: Current Trends and Research Challenges," *International Journal of Advanced Studies in Computers, Science and Engineering*, vol. 5, p. 1, 2016.

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

[11] A. A. Etorban, "The Design and Performance Evaluation of a Proactive Multipath Routing Protocol for Mobile Ad Hoc Networks," School of Mathematical and Computer Sciences, Heriot-Watt University, May 2012.

[12] B. C. Lesiuk, "Routing in Ad Hoc Networks of Mobile Hosts," ed. Victoria, BC, Canada http://www.ghost.lesiuk.org/AdoHoc/adhoc/#E18E2: Department of Mechanical Engineering University of Victoria, December 2, 1998.

[13] M. M. Ghonge, P. Jawandhiya, and V. Thakare, "Selfish attack detection in mobile Ad hoc networks," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2017, pp. 1-4.

[14] S. Buchegger and J.-Y. Le Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proceedings 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, 2002, pp. 403-410.

[15] P. Michiardi and R. Molva, "Prevention of denial of service attacks and selfishness in mobile ad hoc networks," in *in Mobile Ad Hoc Networks, Institut Eurecom Research Report RR-02-063*, 2002.

[16] S. Ruj, R. Sachdeva, and S. Govindram, "Analysis of Selfish Node Attack in AODV Routing Protocol using GLOMOSIM," *International Journal of Engineering Development and Research*, vol. 5, pp. 784-789, 2017.

[17] N. Arora, E. P. Vyas, and K. Arora, "Performance analysis of DSR, AODV and ZRP under black hole attack," *Int. J. Appl. Res. Eng. Sci*, vol. 1, pp. 1-6, 2014.

[18] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," *Wireless Networks*, vol. 22, pp. 1505-1511, 2016.

[19] 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.

[20] M. A. Abdelshafy and P. J. King, "AODV and SAODV under attack: Performance comparison," in *International Conference on Ad-Hoc Networks and Wireless*, 2014, pp. 318-331.

[21] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks*, vol. 24, pp. 565-579, 2018.
[22] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*: Springer, 2011.
[23] B. Paul, M. Ibrahim, M. Bikas, and A. Naser, "Experimental analysis of AODV & DSR over TCP & CBR connections with varying speed and node density in VANET," *arXiv preprint arXiv:1204.1206*, 2012.
[24] 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. 112-115, 2016.
[25] E. Zöchmann, K. Guan, and M. Rupp, "Two-ray models in mmWave communications," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2017, pp. 1-5.