Wireless Personal Communications (2019) 106:365–376
https://doi.org/10.1007/s11277-019-06166-8

Defending Against Flooding Attacks in Mobile Ad-Hoc Networks Based on Statistical Analysis

Payam Mohammadi[1] · **Ali Ghaffari**[2]

Published online: 5 April 2019

Abstract
Due to their specific structure and plenty of their utilization, mobile ad-hoc networks are vulnerable to various attacks. An attack which impacts on network layer is referred to as flooding attack. By transmitting several packets, this attack occupies the processor so that it cannot receive the remaining data and packets. Hence, it causes disruption and disorder in the network. In this paper, for preventing this problem, a method has been proposed based on DSR routing protocol which quickly identifies the flooding attack. Indeed, the proposed method not only identifies and detects the malicious nodes in comparison with valid and proper nodes but also imposes sufficient penalties and reconsiders it again. The method proposed in this paper is called defending against flooding attacks-dynamic source routing. At the outset, it detects misbehavior in the network; then, for discovering malicious nodes, it uses average packet transmission RREQ which measures average transmission route request (RREQ) packets. The results of simulating the proposed method in NS-2 environment indicated that it improved packet delivery rate and end-to-end delay.

Keywords Mobile ad-hoc networks (MANETs) · Flooding attack · Safe routing · Average packet transmission RREQ (APTR) · Dynamic source routing (DSR)

1 Introduction

No pre-fabricated infrastructures are used in MANETs. That is, infrastructures such as central station, router, switch or any other structures used in other networks are not utilized in MANETs. Rather, it is a number of wireless nodes which are connected to non-neighboring nodes means of establishing communications with neighboring nodes [1, 2]. WSNs and MANETs have recently attracted a lot of industrialists and researchers' attention. These networks have many applications as in battlefield, rescue operations, coverage of natural disasters such as earthquake, volcano, etc. [3–7]. MANETs are challenged by numerous problems regarding power consumption and safe communications. Due to the mobility of nodes, the power of nodes is supplied by battery. Hence, since nodes' power

✉ Ali Ghaffari
A.Ghaffari@iaut.ac.ir

[1] Department of Computer Engineering, Germi Branch, Islamic Azad University, Germi, Iran

[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

supply is limited, certain measures should be taken to save their power. Various attacks might impact on the resources of these networks. It should be noticed that MANET have certain unique features such as the followings: unreliability of wireless links, dynamically changing topology, lack of a certification authority, and the absence of a centralized monitoring or management point. Consequently, MANETs are troubled by different threats and attacks including flooding attack, impersonation attack, grey hole attack, black hole attack, denial of service (DoS) attack and selfish misbehaving [8–11].

Routing algorithms in MANETs demonstrate distributed and cooperative behavior which results in their vulnerability to DoS attacks. Also, RREQ flooding attack refers to a flooding-type DoS attack in the presence of AODV routing protocol where the attacking node broadcasts great masses of RREQ packets for establishing a route with the nonexistent or existent destination in the network [12]. In this attack, the attacking node acts like a normal nodes in every aspect except for flooding a large amount of malicious RREQ packets which exhausts and paralyzes network bandwidth and nodes' resources; also, battery power required for doing the measurement operations is depleted which interrupts the routing operation [13, 14]. This attack is illustrated in Fig. 1.

Based on the above-mentioned arguments, it should be maintained that flooding attacks in MANETs should be quickly identified because these attacks interrupt nodes' performance in the network. That is, in the presence of these attacks, the network will not be able to provide appropriate service.

In this paper, we proposed a method based on DSR routing protocol [15] for fast identification of flooding attack and for preventing the above-mentioned problem. The proposed method not only identifies and distinguishes malicious nodes from valid and normal nodes but also reconsiders them after imposing sufficient fines and penalty on them. The proposed method firstly detects misbehavior in the network. Then, for discovering malicious nodes, it uses APTR for measuring average route request packets. The results of simulating the proposed method in NS-2 revealed that it was able to improve the parameters of average packet delivery rate, end-to-end delay and throughput. The major contributions of the paper are as follows:

- Proposing a method for identifying and preventing route request flooding attacks in MANETs.
- Evaluating and validating the efficiency of the proposed method in NS-2 simulator at different simulation times.

The remaining parts of the paper are organized as follows: in Sect. 2, related works on the effect of flooding attacks on MANETs are briefly reviewed. In Sect. 3, the proposed

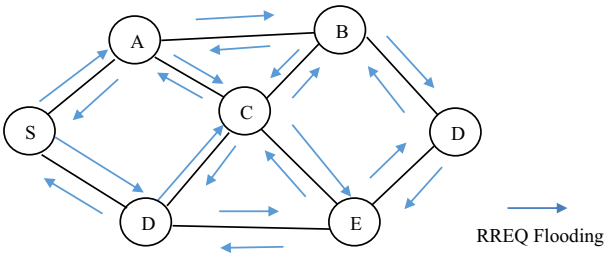

Fig. 1 An example of RREQ flooding attack in MANETs

mechanism is described. In Sect. 4, the simulation results on evaluating the proposed mechanism are given; finally, Sect. 5 draws the conclusion of the study and directions for further research.

2 Related Works

In this section, some studies conducted on discovering and preventing flooding attacks are reviewed.

A clustering behavior based on reputation was proposed in [16] for identifying flooding malicious nodes in military battlefield networks. Similar to battlefield condition, Group Mobility model was proposed. In fact, clustering nodes within clusters have several merits. The reputation of a node is measured at cluster heads. This method has double natures. Thus, it effectives sorts out false detection of genuine nodes as malicious ones. A new method known as mitigating flooding attack mechanism was introduced in [17] which is based on a dynamic threshold value and has three phases. It utilizes specific nodes called flooding-intrusion detection systems (F-IDS) which are applied in MANETs for detecting and preventing flooding attack. F-IDS nodes are set in promiscuous mode for monitoring nodes' behavior. A fuzzy logic-based flooding attack detection mechanism was proposed in [18]. In this method, there is a pre-defined threshold value in fuzzy decision component which is compared with calculated variety level for identifying the behavior of nodes. In case the calculated variety level is less than the pre-defined threshold value, it will announce that node as a malicious node. One demerit of this method is that it depends on a fixed threshold value which is not appropriate for mobile conditions which can result in false positive problems. A method for mitigating the impact of route request flooding attack was introduced in [19]. In this method, neighbor reply information of the specific node is distributed among its neighbors and reputation value is measured. In line with each node's reputation value, their neighboring nodes limit the request packet sent by the given node. It was assumed that while sending reply packet information through any misbehaving nodes, the node would maintain the integrity of reply packet. A method for detecting and preventing flooding attack called Balanced AODV (B-AODV) was proposed in [10]. This method presumes that all network nodes have normal behavior. Each node applies a balance index for accepting or rejecting RREQ packets. In case network nodes begin to behave normally and request too much route, they are identified as malicious nodes. B-AODV is characterized by these characteristics: (A). using adaptive threshold based on network conditions and nodes behavior (balance index), (B) not using additional routing packets for detecting malicious nodes, (C) independent detection and prevention operations on each node, (D) detecting and preventing operations in real time, (E) no need for promiscuous mode.

An RREQ Priority Assessment index method was proposed in [20] for mitigating the impact of the flooding attacks on AODV routing protocol by using two threshold values, i.e., Min_Threshold and Max_Theshold. Accordingly, priority of an RREQ originator is determined based on its flow rate through three levels: legal level, moderate level and the strongest level. When a node has legal priority, the router node holds packets and forwards them as per threshold policy of request rate limit. When a node has a moderate priority, the relay service will be carried out with downgrading/upgrading priority. When a given node has the strongest priority, the forwarding service will be rejected and its packets will ignored. The shortcoming of this method is that all nodes can operate in overhearing mode which lead to the waste of mobile nodes' energy.

3 The Proposed Method

The proposed method was designed based on the technique of suppressing neighbors which identifies malicious nodes throughout route construction stage. In case it detects a malicious node, it keeps it in the isolated condition for a while and investigates its behavior in the network so as to avoid flooding attack in the network layer. If the node is identified as a malicious node, it will remain in the detention list for the period of time. After the end of this time period, it will be considered again as a normal node in a specific part of the network. Before transmitting a data packet, each node investigates detention field list in the proposed DAFA-DSR. If the node is in the detention list, data packet will not be transmitted to it. Otherwise, the node will be regarded as a normal node and data packet will be transmitted to it.

The proposed method avoids the production of unnecessary RREQ packets and can detect attacks in which several fake RREQ packets with invalid IP addresses are sent to the target. For detecting these malicious nodes, there is a security module in each of the acknowledged nodes in the network which has two main parts: misbehavior detection system in the network and flooding detection system. The first part is used for maintaining network status. In case the number of route requests is more than threshold, it informs the nodes about the possibility of misbehavior and abnormal behavior in the network. Such a declaration indicates the presence of one or more RREQ flooding attacks in the network. Consequently, the second stage is executed. The responsibility of the second part is to discover the resources of misbehavior in the network which might be a single attack or shared flooding attacks. Such attacks might be detected through real-time tracking of different packets transmitted/received by the available nodes in the network. By default, DSR protocol uses an optional HELLO message for stabilizing connections among neighboring nodes. All nodes should stick observe all the defined mechanisms for preventing the production of fake route requests in the network.

3.1 Misbehavior Informing Stage in the Network

The informing stage is used for the optimal application of detecting nodes' misbehavior. This stage contributes to the production of active security solutions. As long as the network is in the safe condition, i.e. no flooding attack is reported, the detection system will be inactive until that time. For tracking network status, each node exchanges a HELLO message with its neighbors through a defined process. The proposed method adds a new field to the HELLO message which provides information about the produced or received RREQ packets. That is, as each node receives an RREQ message, it adds one unit to the number of its received messages (Received++). Also, by transmitting an RREQ message, the node adds one unit to the number of its transmitted messages (sent++). Using this field facilitates and guarantees the periodic tracking of the nodes' behavior to find whether they are parts of the flooding attack or not. Each node in the network should have the information of the HELLO message about the exchanged RREQ packets. Transmitting HELLO messages is not only aimed at maintaining and stabilizing connections among neighboring nodes but is also intended to investigate whether the network is safe from flooding attacks or not. Before transmitting HELLO message, nodes produce and receive information about RREQ messages.

When a HELLO message is received from a neighboring node, the node receiving the HELLO message marks that neighboring node as an active node. Then, the available information within the HELLO message is decoded. If the neighboring node is a new node, it produces a new input for registering that node's information in its table and writes the information of that node in the respective input. However, if the node is one of the previous neighbors, the inputs related to that node are updated. The node receiving HELLO message registers the input related to the neighboring node as the active node in the table and stores the information related to the exchanged RREQ packets.

The excessive increase in transmitting RREQ packets is considered as a flooding attack. Such abnormal changes is determined by the average transmission weight of the previous observations. If the average weight is greater than the threshold, a detection process should be set up by the attack detection system for identifying the resources of flooding attacks.

3.2 Flooding Attack Detection Mechanism

For implementing this stage of the proposed method, the available misbehaviors should be initially detected. The distinguishment of the two stages leads to the optimization of the respective operations for detecting malicious nodes. When the detection process is executed, each node in the network should carry out a search in the list of its neighbors so as to find a node which has produced more RREQ packets. For detecting the resources of flooding attacks, each node measures the number of produced RREQs. For doing so, an average weight formula was used in the proposed DAFA-DSR method. As mentioned earlier in the paper, APTR is a procedure for measuring average transmission of RREQ packets. The average transmission by the series data is used at certain times for smoothening short-term and long-term fluctuations. Based on these measurements, we can analyze our observations of the RREQ packets at specific time periods. For X series, APTR might be measured recursively.

$$APTR = \begin{cases} S_1 = X_1; & \text{for } t = 1 \\ S_t = \alpha \cdot X_t + (1 - \alpha) \cdot S_{t-1}; & \text{for } t > 1 \end{cases} \quad (1)$$

In this equation, α coefficient is a smoothening factor with a fixed value between 0 and 1. X_t refers to the RREQ value at t time period. S_t denotes an APTR value at each t time period. APTR can be executed with low α values for investigating network when it is affected by flooding attacks. Also, high α values can contribute to the analysis of the overall network observations and detect the attack resource. After the required information is obtained through HELLO messages, the number of transmitted RREQs is determined for each node. By receiving a HELLO message from each of its neighbors, a given node can measure APTR value for all of its neighboring nodes. A threshold is considered at each time for APTR. If APTR value of a node is greater than the threshold value, it reveals that the number of transmitted RREQ messages by this node is much higher than the expected threshold. Hence, such a node is regarded as a malicious node.

3.3 Adding Malicious Nodes to the Blocked List

When a node identifies a malicious node in its neighborhood, it adds that node to its blocked list. Accordingly, it rejects all the requests arrived from the malicious node until the specific Θ time has passed. Also, this node transmits an RRER message to its neighbors

so that they disconnect themselves from that malicious node and isolate it from the network until time Θ has passed.

3.4 Reconsideration of the Malicious Node

Each node keeps the blocked list field of a specific node for a certain time period (Θ = 4 * RTT). RTT denotes the average back and forth time of RREQ. After this time is finished, the invalid node is reconsidered as a valid node and it is investigated throughout the normal operations of the network. When that node is regarded as a valid or normal node, all the neighboring nodes update the DAFA-DSR inputs related to that particular node. If that node demonstrates malicious behavior, it will be included within the blocked list again. Accordingly, all the neighboring nodes make changes in DAFA-DSR. The stages of the proposed DAFA-DSR method are fully illustrated in the flowchart given in Fig. 2.

4 Evaluating the Efficiency of the Proposed Method

The proposed method was evaluated using NS-2 software. Values of the simulation parameters are given in Table 1.

The number of available nodes of the network in this scenario was 20 nodes and the number of malicious nodes was assumed to be 4. The dimensions of the simulation environment used in this scenario was 700 m × 700 m. Radio dissemination range for each node was 250 nodes. Its MAC layer protocol was IEEE 802.11. Also, there were two traffic flows in this simulation which send packets to the network with a fixed rate. In this scenario, simulations were carried out at the following times: 150, 300, 450, 600, and 750 s. These times were considered on both the attacked DSR routing protocol. Then, they were compared with the times on the proposed DAFA-DSR. Buffer size used in this scenario was 150 packets. The nodes in this scenario were placed at random positions.

4.1 Performance Metrics

The following evaluation criteria were used for evaluating the proposed method: number of lost packets, packet delivery ratio, end-to-end delay and throughput.

4.1.1 Average Packet Loss Rate (APLR)

Flooding attack results in an interruption in the normal routing process of the network. Also, it leads to the loss of many packets. That is, in MANETs and DSR routing protocol, the highest number of packet loss is related to flooding attacks. Equation (2) measures APLR.

$$APLR = \frac{1}{N}\left(\frac{\sum_{i=1}^{n} S_i - \sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} S_i}\right) \times 100\% \tag{2}$$

where N denotes the number of conducted experiments; S_i refers to the number of transmitted packets by node *i*; R_i indicates the number of received packets. Figure 3 shows that the proposed DAFA-DSR method was able to reduce the number of lost packets better than

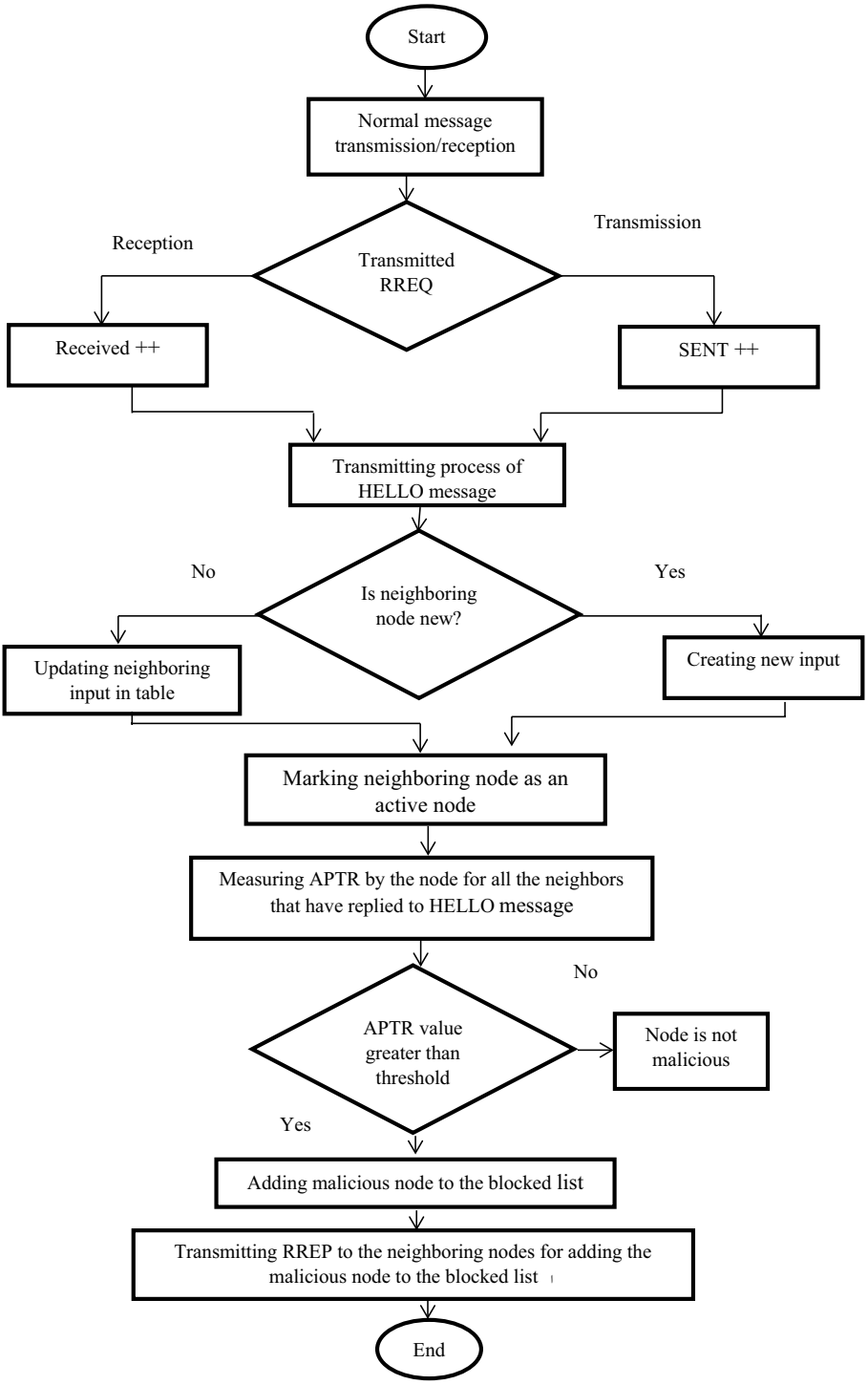

Fig. 2 Flowchart of the proposed DAFA-DSR method

Table 1 Simulation parameters

Parameter	Value
Environment	700 m × 700 m
Number of nodes	20
Routing protocol	DSR
Transmission range	250 m
Antenna type	Omni antenna
Simulation times	150, 300, 450, 600, 750
Mobility model	Random waypoint
Malicious nodes	4
MAC layer	IEEE 802.11
Flooding rate interval	0.01 s
Packet size	512 bytes
Traffic type	CBR (UDP)
Buffer size	150 packets
Placement position	Random

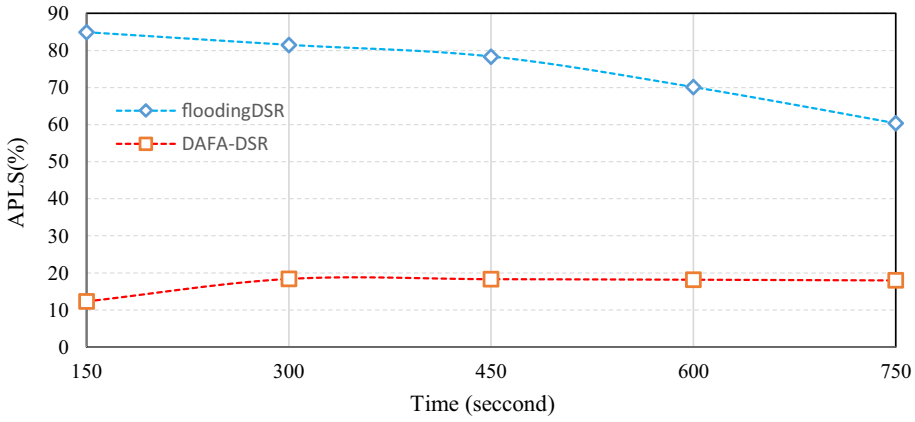

Fig. 3 Average packet loss rate (APLR)

DSR protocol under flooding attack at different times. The reason for a lower packet loss rate in the proposed DAFA-DSR method was that the proposed method was able to identify flooding attack early; hence, it prevents this attack which, consequently, enhances the efficiency of the proposed method.

4.2 Average Packet Delivery Rate (APDR)

The criterion of packet delivery rate is of high significance in MANETs. It is measured through Eq. (3):

$$APDR = \frac{1}{N}\left(\frac{\sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} S_i}\right) \times 100 \tag{3}$$

As shown in Fig. 4, the simulation was conducted on the proposed method with 20 nodes at different times, i.e. 150, 300, 450, 600 and 750 s. The results obtained from the simulations indicated that the proposed DAFA-DSR has a better performance than DSR protocol in terms of packet delivery rate. Consequently, it can be argued that these results demonstrate the higher efficiency of the proposed method because it can detect the flooding attack earlier and faster than DSR protocol. Hence, it prevents the occurrence of the attack. In the flooding attack, the transmission of numerous packets leads to the occupancy and busyness of the processor; in this way, it cannot receive the remaining data packets. Consequently, several packets are lost. In contrast, the proposed method detects the attack and lets more data packets be delivered to the destination.

4.3 End-to-End Delay

In MANETs, end-to-end delay indicates the time at which data packets are transmitted from the source to the destination throughout the network. Figure 5 illustrates the end-to-end delay for the proposed DAFA-DSR and compares it with DSR routing protocol in terms of end-to-end delay. It was found that the proposed DAFA-DSR has significantly lower end-to-end delay than DSR routing protocol. DAFA-DSR had better performance at different times which is regarded as another evidence for the higher efficiency of the proposed method. In other words, as discussed earlier, the proposed method detects and prevents flooding attack. In this way, the proposed method does not allow the attack to transmit additional destructive packets and waste the processor's time. Thus, in the proposed method, packets reach the destination early. Furthermore, it should be highlighted the proposed method does not constantly consider a node as malicious. Rather, it reconsiders and investigates the node after a certain time period. As a result, DAFA-DSR removes less nodes from the network and using more nodes in routing results in lower delay.

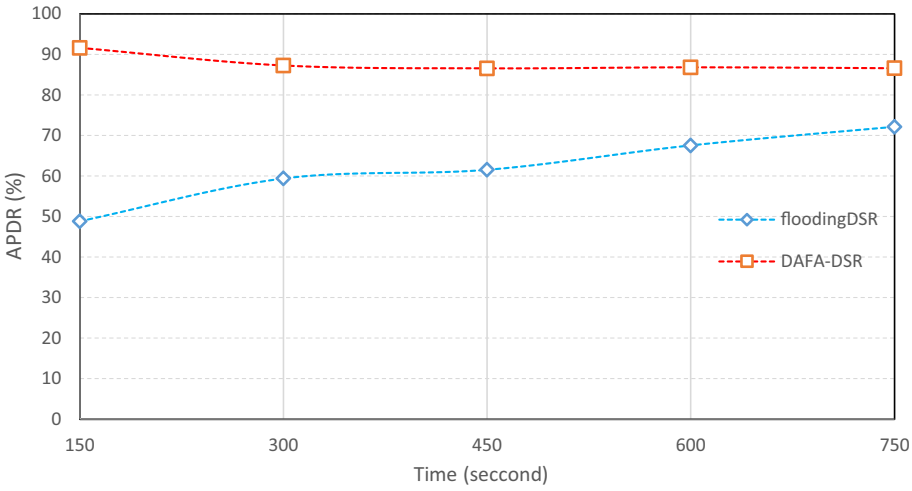

Fig. 4 Average packet delivery rate (APDR)

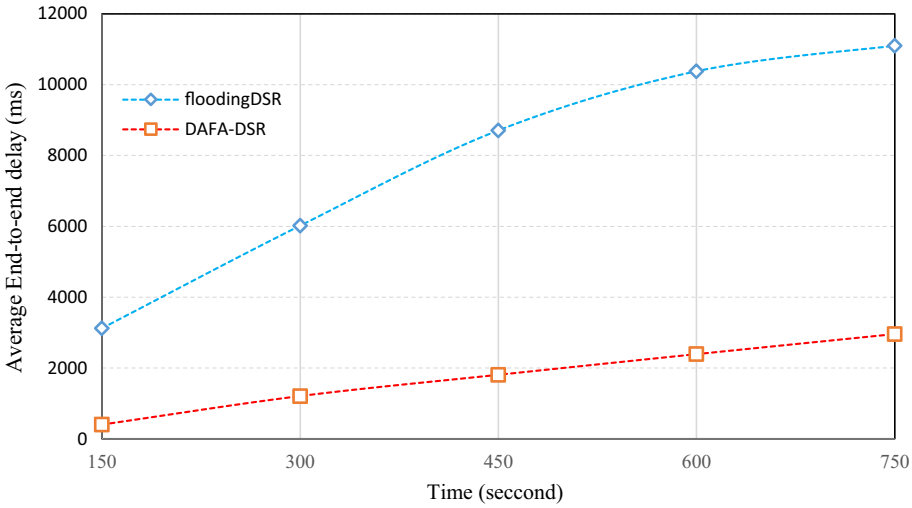

Fig. 5 Average end-to-end delay

4.4 Throughput

This criterion is obtained via dividing the amount of data received in the destination by the data arrival time in terms of Kbps. Throughput is measured through Eq. (4).

$$Average\ throughput = \frac{1}{N}\left(\frac{\sum_{i=1}^{n} R_i \times P_s}{t_p - t_s}\right) \times \frac{8}{1000} \tag{4}$$

In this equation, P_s denotes the size of transmitted packets; t_p refers to the stop time of the simulation and t_s indicates the starting time of the simulation. As depicted in Fig. 6, when

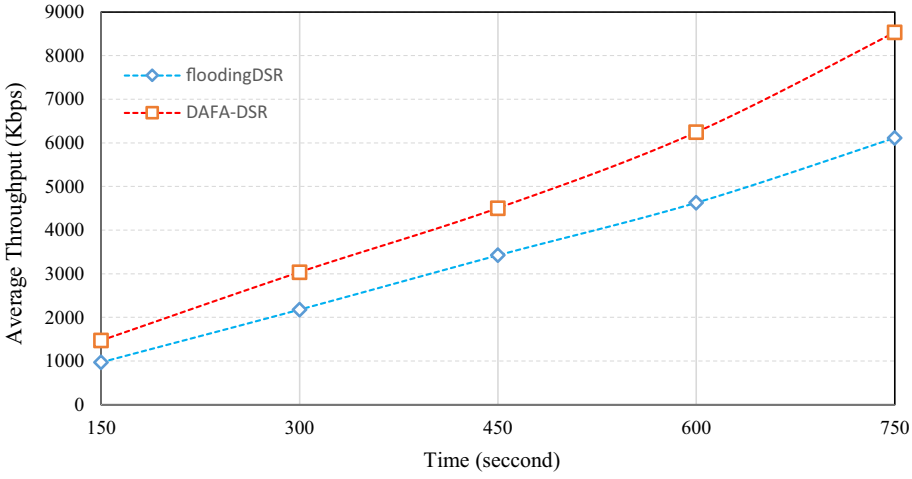

Fig. 6 Average throughput

compared with DSR, the proposed DAFA-DSR had better performance at different times. It can be argued that the proposed method was able to deliver more data packets to the destination at a certain time. Thus, it can be maintained that, at the same time unit, DAFA-DSR had higher throughput than the attacked DSR protocol.

5 Conclusion and Directions for Further Research

As mentioned earlier, the method proposed in this paper consisted of two main parts, i.e. misbehavior detection system in the network and flooding detection system. The first part was aimed at maintaining stability of the network status. In case the number of route requests exceeds the threshold, the nodes will be informed about abnormal behavior in the network. The second part of the proposed paper was aimed at discovering the resources of misbehavior in the network via APTR criterion. When a node is discovered as a malicious node, data packet will not be transmitted to that node and that node will be included in the detention list.

It can be concluded that the proposed DAFA-DSR could efficiently hardly attacks in the route detection stage and during data packet transmission stage. When compared with DSR protocol under the flooding attack, the proposed method is more efficient and effective. That is, DAFA-DSR can enhance the overall throughput of the network. Indeed, the major advantage of the proposed DAFA-DSR is that, after a logical penalty, the accused node can be reconsidered as a normal node in the network.

As a direction for further research, the proposed DAFA-DSR may be improved and optimized by using meta-heuristic algorithms such as artificial immune algorithms, bee colony, etc.

References

1. Ghaffari, A. (2017). Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms. *Wireless Networks, 23,* 703–714.
2. Asadi, E., & Ghaffari, A. (2016). A multicast routing protocol based on ODMRP with stable link in mobile ad hoc networks. *International Journal of Computer Science and Information Security, 14,* 68.
3. Ghaffari, A. (2015). Congestion control mechanisms in wireless sensor networks: A survey. *Journal of Network and Computer Applications, 52,* 101–115.
4. Azari, L., & Ghaffari, A. (2015). Proposing a novel method based on network-coding for optimizing error recovery in wireless sensor networks. *Indian Journal of Science and Technology, 8,* 859–867.
5. Mohammadi, R., & Ghaffari, A. (2015). Optimizing reliability through network coding in wireless multimedia sensor networks. *Indian Journal of Science and Technology, 8,* 834–841.
6. Ghaffari, A. (2014). Designing a wireless sensor network for ocean status notification system. *Indian Journal of Science and Technology, 7,* 809–814.
7. Chang, J.-M., Tsou, P.-C., Woungang, I., Chao, H.-C., & Lai, C.-F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Systems Journal, 9,* 65–75.
8. Guo, Y., Gordon, S., & Perreau, S. (2007). A flow based detection mechanism against flooding attacks in mobile ad hoc networks. In *Wireless communications and networking conference, 2007. WCNC 2007* (pp. 3105–3110). Washington: IEEE.
9. Verma, S. S., Patel, R., & Lenka, S. K. (2017). Analysing varying rate flood attack on real flow in MANET and solution proposal 'real flow dynamic queue'. *International Journal of Information and Communication Technology, 10,* 276–286.
10. Faghihniya, M. J., Hosseini, S. M., & Tahmasebi, M. (2016). Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network. *Wireless Networks, 23*(6), 1863–1874.
11. Sakiz, F., & Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks, 61,* 33–50.

12. Kumar, S., & Dutta, K. (2017). Direct trust-based security scheme for RREQ flooding attack in mobile ad hoc networks. *International Journal of Electronics, 104,* 1034–1049.
13. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60,* 19–31.
14. Yu, J., Kang, H., Park, D., Bang, H.-C., & Kang, D. W. (2013). An in-depth analysis on traffic flooding attacks detection and system using data mining techniques. *Journal of Systems Architecture, 59,* 1005–1012.
15. Hu, Y.-C., Johnson, D., & Maltz, D. (2004). The dynamic source routing protocol for mobile ad hoc networks (DSR). IETF Draft.
16. Kaur, T., Toor, A. S., & Saluja, K. K. (2014). Defending MANETs against flooding attacks for military applications under group mobility. In *2014 recent advances in engineering and computational sciences (RAECS), 2014* (pp. 1–6).
17. Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating route request flooding attack in MANET. *Wireless Networks, 24*(8), 2899–2914.
18. Chaudhary, A., Tiwari, V., & Kumar, A. (2014). A novel intrusion detection system for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks. In *Recent advances and innovations in engineering (ICRAIE), 2014* (pp. 1–4).
19. Choudhury, P., Nandi, S., Pal, A., & Debnath, N. C. (2012). Mitigating route request flooding attack in MANET using node reputation. In *2012 10th IEEE international conference on industrial informatics (INDIN)* (pp. 1010–1015).
20. Jiang, F.-C., Lin, C.-H., & Wu, H.-W. (2014). Lifetime elongation of ad hoc networks under flooding attack using power-saving technique. *Ad Hoc Networks, 21,* 84–96.

Payam Mohammadi received his BSc in computer software engineering from the Tehran science and culture University in 2013, TEHRAN, IRAN. He received MSc degree in computer software engineering from Islamic Azad University, GERMI branch, GERMI, IRAN in 2017. His research interests are mainly in the field of Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs) and networks security.

Ali Ghaffari received his B.Sc., M.Sc. and Ph.D. degrees in computer engineering from the University of Tehran and IAUT (Islamic Azad University), Tehran, Iran in 1994, 2002 and 2011 respectively. As an assistant professor of computer engineering at Islamic Azad University, Tabriz Branch, Iran, his research interests are mainly in the field of wired and wireless networks, Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), networks security and Quality of Service (QoS). He has published more than 60 international conference and reviewed journal papers.