Shahid Bahonar University of Kerman

Journal of Mahani Mathematical Research

Print ISSN: 2251-7952 Online ISSN: 2645-4505

DSNAODV: DETECTING SELFISH NODES BASED ON AD HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

M. Vanday Baseri ✉ and M. Kuchaki Rafsanjani

Dedicated to sincere professor Mashaallah Mashinchi

Article type: Research Article

(Received: 04 December 2021, Received in revised form: 06 May 2022)

(Accepted: 21 May 2022, Published Online: 09 June 2022)

Abstract. In mobile ad hoc networks (MANETs), innumerable intermediate nodes interchange information without the need for infrastructure. In these networks, nodes depend upon each other for routing and forwarding packets, and communication among them is very important. Forwarding packets consumes network bandwidth, local CPU time, memory, and energy. Therefore, some nodes might intend not to forward packets to save resources for their use that called selfish nodes. The destruction of basic action of the network can occur due to this selfish behavior of the node. So in this paper, we focused on dropper misbehavior for data packets and route request packets. For detecting this kind of nodes in this paper, we improved the ad hoc on-demand distance vector (AODV) routing protocol and proposed a new routing protocol for detecting selfish nodes. The performance analysis shows that the DSNAODV (Detecting Selfish Node based on Ad hoc On-demand Distance Vector routing protocol) protocol can improve the packet delivery ratio and use less energy compared to AODV and EBTS protocols.

Keywords: Mobile ad hoc networks (MANETs), Selfish nodes, Ad hoc on-demand distance vector (AODV), Consumption energy, Routing.
2020 MSC: 68M10, 68M12, 68M18.

1. Introduction

In mobile ad-hoc networks (MANETs), each node is free to move and connect with another over a wireless connection, without the requirement for a centralized controller or base station. Each node is responsible for forwarding the packets to its neighboring nodes [1]. Due to the lack of resources, some mobile nodes refuse to forward the packet to other nodes. This type of node is called a selfish node. This type of nodes in the route degrades the overall performance of the whole network. If every node of the network decides to act selfishly, then the entire network could be collapsed [2,3]. Briefly, misbehavior

✉ Vanday67@yahoo.com, ORCID: 0000-0003-2527-2072

DOI: 10.22103/jmmrc.2022.18621.1179
Publisher: Shahid Bahonar University of Kerman
How to cite: M. Vanday Baseri, M. Kuchaki Rafsanjani, *DSNAODV: Detecting Selfish Nodes based on Ad hoc On-demand Distance Vector routing protocol*, J. Mahani Math. Res. 2022; 11(3): 57-68.

in ad-hoc networks can be classified into two main groups, namely, selfish nodes and malicious nodes. These two types can damage MANET and cause two main attacks and can be difficult to detect. Selfish nodes can cause packet dropping attack, whereas malicious node causes the denial of service (DoS) attack [4]. Routing protocols in ad-hoc networks are grouped under three categories like proactive, reactive, and hybrid routing protocols. In a proactive routing protocol, the routing information in each node of the network is updated periodically whether the routing path is needed or not. DSDV and OLSR are examples of proactive routing protocols. Reactive routing protocol maintains routes only for data communication. This type of protocol helps to reduce routing overhead. Examples of reactive routing protocols are AODV, DSR, and TORA. Hybrid routing protocols combine the characteristics of proactive and reactive routing protocols [5]. The zone-based routing protocol (ZRP) is an example of a hybrid routing protocol. Ad-hoc on-demand distance vector (AODV) is one of the most popular on-demand routing protocols. The conventional AODV finds the shortest path between the source and destination nodes [6]. AODV is an example of a reactive protocol that we have improved in this paper. The rest of this paper is as follows; Section 2 describes selfish nodes and AODV protocol. In Section 3, we review the related works. In Section 4, we produce our proposed protocol (DSNAODV). Section 5 is simulation and results evaluation and finally in Section 6, we conclude the paper.

1.1. **Contributions of this paper.** Several techniques have been proposed to detect selfish nodes in mobile ad hoc networks. These techniques can be classified into four categories [7]: the reputation-based scheme, the credit-based scheme, the acknowledgment-based scheme, and the game-theoretic scheme. The proposed DSNAODV routing protocol can detect selfish nodes in MANETs. The DSNAODV is a reputation-based routing protocol in which each node monitors the behavior of neighboring nodes. This protocol consists of three basic steps. Initially, 3 parameters are calculated for each node by its neighbor: real energy, expected energy, and the rate of outgoing packets to incoming packets (Alpha). In the second step, the energy level is calculated. Finally, the values of the two parameters of energy-level and Alpha are compared with the threshold values and based on them, the selfishness of the node is decided. The advantages of our proposed protocol are as bellow:

- The main purpose of the DSNAODV protocol is to correctly identify selfish nodes in the MANETs.
- One of the important parameters in routing algorithms is packet delivery rate which has been improved by the proposed protocol.
- Energy consumption is of particular importance due to its limitations in MANETs. In the DSNAODV protocol, the amount of energy consumed in the routing and detection process is reduced.

2. Background

In this section, selfish nodes and AODV routing protocol have been described.

2.1. **Selfish nodes.** There are different kinds of selfish nodes behaviors in MANET and some of them are:

- In forwarding node selfish behavior, selfish nodes do not advertise available routes or do not forward route request packets (RREQ), so they do not participate correctly in the routing [8].
- In packet dropper misbehavior, when the data packets come to the selfish node for forwarding, it drops all of them. This is the most common misbehavior that we can see in different kinds of literature that have been studied. The watchdog mechanism is a solution to deal with this misbehavior [9].
- In partial dropping misbehavior, the selfish node drops packets at a lower rate than the watchdog's configured minimum misbehavior threshold, so it confuses the watchdog for detecting [10].
- In false misbehavior accusations misbehavior, a node may falsely report other innocent nodes in its neighborhood as misbehaving to avoid getting packets forward. Selfish nodes can also take advantage of imperfect monitoring mechanisms. When the miss detect ratio is high, a selfish node can always drop other nodes' packets, but still claim that it has been forwarded [11].
- By increasing hop counts, paths that include selfish nodes seem longer than they are, so it is another selfish behavior. In this case, the source nodes are more likely to choose other routes that appear to be shorter [12].

In this paper, we focused on dropper misbehavior for data packets and route request packets.

2.2. **Ad hoc On-demand Distance Vector (AODV) routing protocol.** AODV [6,13,14,15] is an example of a reactive routing protocol. It is jointly developed in the Nokia Research Centre of the University of California, Santa Barbara and the University of Cincinnati by Perkins and Das. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. It creates routes on an on-demand basis, so it minimizes the number of required broadcasts. So, AODV is the most efficient protocol in comparison to other routing protocols used in the MANET environment because it has low communication overhead, and also low memory and bandwidth consumption [7]. A source node initiates a route discovery phase to locate the other node because of sending a message, it does not already have a valid route to a destination node. It broadcasts a route request (RREQ) packet to its neighboring nodes, which then forward the request to their neighboring nodes, and so on until either the destination node or an intermediate node that has a fresh route to the destination node is found. The destination sequence numbers (DestSeqNum) are used by AODV to ensure the freshness of routes and to find the most recent path to the destination. If DestSeqNum of the current packet received by a node is greater than the last DestSeqNum stored at the node, its path information is updated. In summary, AODV has the following features [13]:

- Nodes store only the routes that are needed.
- The need for broadcast is minimized.
- Reduces memory requirement.
- Scalable to large populations of nodes.

3. Related works

In a MANET, some nodes have limited resources, especially the battery. Forwarding packets consume resources so some nodes are not willing to forward packets to others because of saving their resources and acts selfishly [16]. Some techniques have been proposed to deal with selfish nodes in MANET. Buttayan and Hubaux [15] have proposed a method that uses a virtual currency, called nuglet to detect selfish nodes. In this method, when a node forwards packets to another a nuglet counter increases. When a node wants to send its packets, if its credit is less than a predefined threshold, it is not allowed to send packets. In the reputation-based method, it detects a selfish node by using a reputation system that detects and rates a selfish node. When a node's reputation is good it participates in network activity otherwise it is marked as selfish. Michiardi and Molva [17] have proposed CORE, which uses the Watchdog mechanism to consider neighbors, and then detect and isolate selfish nodes. It calculates a reputation value for each node. Based on this reputation, nodes are allowed to participate in the network or are excluded. Cooperative nodes with low battery conditions would not be detected as misbehaving nodes right away because the node reputation is heavily weighted towards past reputation. However, only a positive indirect reputation is allowed in this system to avoid false accusation and denial of service attacks [4] [18]. A collaborative Watchdog algorithm is introduced in [19], a cooperative approach in which detection of selfish node relies on Watchdog mechanism and each node maintain a reputation table of nodes. Upon detection of selfish nodes, a collaborative node disseminates this information to other nodes. A node with a bad reputation is marked selfish cooperatively and isolated from the network. Vijayan et al. [20] have proposed an energy-based trust solution for detecting selfish nodes that in this paper, we named EBTS. They used fuzzy logic in evaluating trust for misbehavior detection of selfish nodes in MANET. In their proposed scheme, there are four steps supervisor, aggregator, trust calculator, disseminator. They used the solution to calculate the trust for every node in the MANET and to identify the selfish nodes taking energy utilization factor as the main factor in calculating trust. In [3] a new game-theoretic scheme has been proposed for selfish node detection in MANET. This scheme is based on a modified AODV routing protocol. In this method, in addition to identifying selfish nodes, the concept of the Least Total Cost Factor is used and in the process of transferring the packet, only the path with the lowest cost is chosen. The payoff matrix is used and it is shown that a node would benefit if only it was willing to cooperate. Otherwise, after crossing the predefined threshold limit, the node will be misbehaved or selfishly removed from the network.

Abirami and Sumithra [21] have proposed the neighbor credit value-based AODV (NCV- AODV). This model is designed to detect selfish nodes in the network that increases network security. This system is designed to rely on observing the behavior of neighboring nodes. If a node is identified as selfish, a fake packet will be sent to the suspicious node to ensure whether it is truly selfish or not. This method increases the overall performance significantly, but it fails as soon as the adjacent node tends to drop the packet of data for a real reason.

Mangayarkarasi and Manikandan [22] have proposed a cost-effective collaborative anomaly detection system for selfish nodes attacks in MANET. The system has an anomaly detection module that initially selects a set of monitoring nodes to run this module. If the source wants to be in contact with the destination, it relies on the monitoring nodes which collaboratively exchange the details. The features of each node are calculated from transmissions of the control packet and data packet. Based on the information collected, a fuzzy logic decision (FLD) is used to detect suspicious nodes. Since by exchanging common information of monitoring nodes, the suspicious node is confirmed, the chance of missed detection is minimized.

Ponnusamy et al. [23] have proposed selfish node removal using reputation model (SNRRM). In this model, the reputation-based mechanism is used to remove the selfish nodes from routing. The reputation for each node is calculated by two parameters of the current energy level and the relationship ratio of that node. The nodes of source and destination are S and D respectively, and the communication begins with the sending of the packet by the sender node. The transfer process is performed if both the S and D nodes are within the scope of the communication. The sender node calculates the reputation of the S and is updated if the system matches. If S and D are not within the scope of communication, S will send control packets to its neighbors and wait for answers. A node is known reputed if it replies to the S' message. Then check energy values of reputed nodes calculate the energy threshold and pick a higher residual energy node. Repeat the process till it reaches the 'D'.

4. Proposed protocol: DSNAODV

In this paper, we propose a new routing protocol for detecting selfish nodes and use the AODV routing protocol and improve it. The flowchart of the proposed protocol is shown on figure 1.

4.1. **Parameters description.** In the proposed protocol every node acts as a judge node and calculates energy-level and Alpha (This parameter is defined in the following text) for all of its neighbors and then makes a judgment about them. N is a number of the judge node's neighbors. Some main parameters are:

- Real energy

For energy, according to [24] we have four parameters:

- The initial energy (*initenergy*);
- The transmission power (*txpower*);
- Reception power (*rxower*);
- Remaining energy(*energy*).

At first, energy is equal to *initenergy.* When a node transmits or receives packets, its initenergy will be reduced. For calculating energy consumed during the transmission process (*txenergy*) and reception process (*rxenergy*) for one packet, we use the following equations:

$$txenergy = txpower * (packetsize/bandwidth); \tag{1}$$

$$rxenergy = rxpower * (packetsize/bandwidth). \tag{2}$$

When a node sends one packet, its neighbor that receives the packet calculates the remaining energy for that node as bellow:

$$energy = energy – txenergy. \tag{3}$$

When a node receives one packet its neighbor calculates the remaining energy for that node as bellow:

$$energy = energy – rxenergy. \tag{4}$$

- Alpha

For every node, we assign *inpC*, *inpD*, *outC*, *outD* that are the number of the input control packets, number of the input data packets, number of output control packets, number of the output data packets. When two nodes have a relation with each other, they update these counters in their neighboring table. For a normal node according to [4] we expect the value of *inpC*+*inpD* with *outC*+*outD* to be equal, but when a node is selfish this equation is not correct. We define alpha for every node that calculates by the node's direct neighbors (Eq. (5)):

$$Alpha = (outC + outD)/(inpC + inpD). \tag{5}$$

Alpha is the rate of outgoing packets to incoming packets, which if the value is equal to 1, indicates that all received packets have been sent. So, we conclude that the node behaved correctly; but if alpha is less than 1 it shows that the

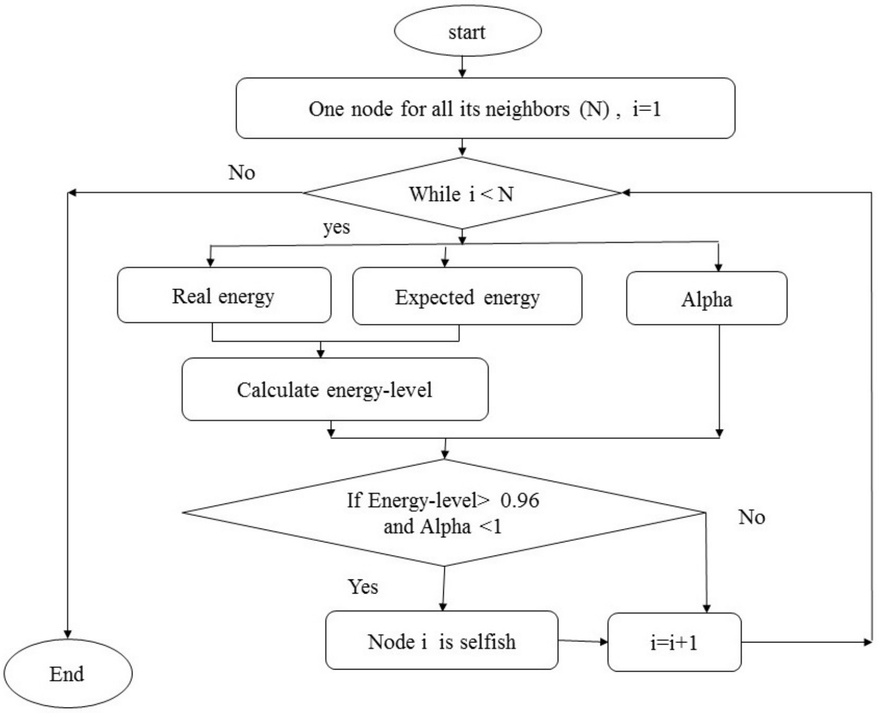

Figure 1. Flowchart of the DSNAODV protocol.

node didn't send all receiving packets and maybe it is selfish.

- Expected energy(E-expect)
After an interval time, every node calculates the expected energy for each of its direct neighbors as bellow:

$$E1 = rxenergy * (inpC + inpD); \tag{6}$$

$$E2 = txenergy * (outC + outD); \tag{7}$$

$$E\text{-}expect = initenergy - (E1 + E2). \tag{8}$$

- Energy-level
We define energy-level according to Eq. (9):

$$Energy\text{-}level = energy/E\text{-}expect. \tag{9}$$

Finally, based on experiments we assign a threshold for energy-level equal to 0.96. In our method for a node if $\alpha < 1$ and $energy\text{-}level > 0.96$, it is a selfish node otherwise it is a normal node.

The proposed protocol steps: Node A repeats the following steps for all its direct neighbors, such as node B.
Step 1: Gets real energy of B.
Step 2: Calculates the expected energy for B.
Step 3: Computes the Alpha value for B.
Step 4: Obtains energy-level for B, according to real energy values and expected energy.
Step 5: If the energy-level is less than 0.96 and Alpha is less than 1, node A concludes that node B is selfish else it is not.

5. **Simulation and results evaluation**

We used the MATLAB simulator and then compare our protocol with the AODV routing protocol and EBTS. The simulation parameters and their values are in Table 1:

Table 1. Simulation parameters.

Parameters	Values
Dimension	$500m * 500m$
Number of nodes	50
Packet size	512
bandwidth	$1.375 * 10^6$
rxpower	180
txpower	280
initenergy	20

We performed 10 runs when a different number of selfish nodes exists in MANET. The proposed protocol is analyzed by using packet delivery ratio, consumption energy, and detection rate criteria.

- Packet delivery ratio (PDR): PDR can be measured as the ratio of the number of packets delivered in total to the total number of packets sent from the source node to the destination node in the network [25].
- Consumption energy: Total energy that MANET consumes among simulations.
- Detection rate is defined as bellow [26]:

$$DR = Nsd/Nst \tag{10}$$

where N_{sd} is the number of selfish nodes detected by one or more normal nodes, N_{st} is the total number of selfish nodes. Figure 2 shows PDR as a function of a different number of selfish nodes. It can be observed from the diagram that when the number of selfish nodes is more than 9, our proposed protocol is much better than EBTS protocol. Our protocol and AODV have the same PDR, because we just detect selfish nodes, but don't remove them.

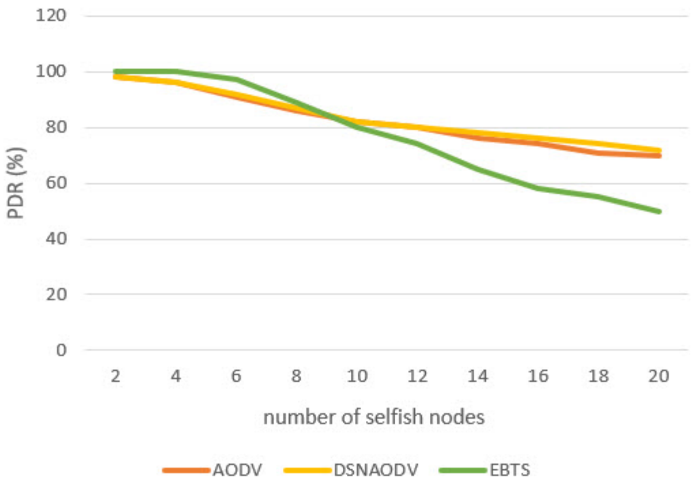

Figure 2. Packet delivery ratio (PDR) versus number of selfish nodes (MANET with 50 nodes).

The impact of selfish nodes on the consumption energy of MANET is shown on Figure 3. This figure shows that energy increases as time increases. DSNAODV uses a much less amount of energy in comparison with EBTS, but a little more than AODV; Because DSNAODV performs operations to detect selfish nodes relative to AODV, so this makes sense.

Finally, in Figure 4 detection rate of the DSNAODV protocol has been shown. In this figure, number of selfish nodes and all the nodes in MANET are variable. It can be seen that when the number of selfish nodes increase, the detection rate decrease. Also, when the number of all the nodes in MANET increases detection rate decreases.

6. Conclusion and future work

Mobile ad hoc network (MANET) has various characteristics like dynamic mobility, limited resources, self-configuration and it is the independent wireless network. The limited resources of the nodes in MANET without any centralized administration motivate nodes to behave selfishly to preserve their resources. So, we proposed a new routing protocol as DSNAODV that can detect these

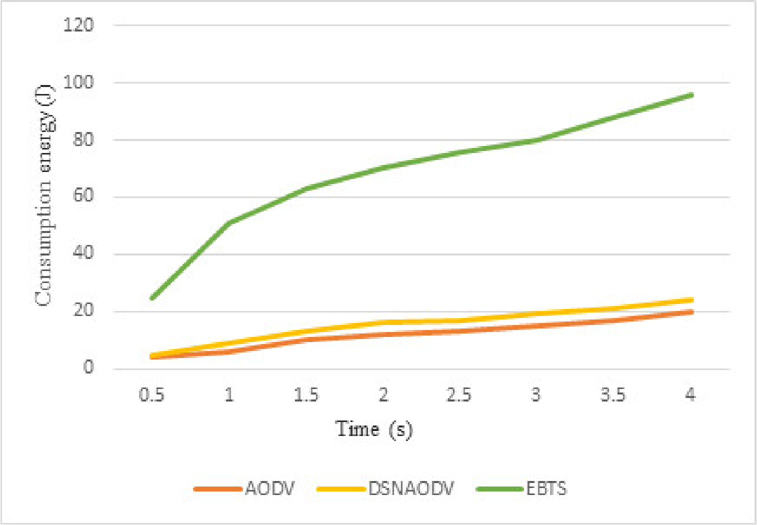

Figure 3. Consumption energy versus time (10 selfish nodes among 50 nodes of MANET).

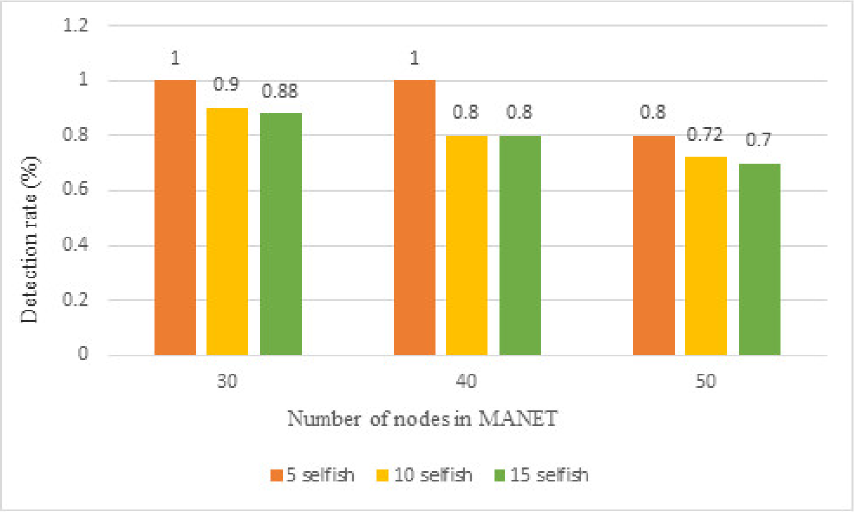

Figure 4. Detection rate versus number of nodes in MANET.

selfish nodes. The energy of node and the number of input and output packets were the two most important parameters in our protocol. The DSNAODV is a reputation-based routing protocol in which each node monitors the behavior of neighboring nodes. We presented simulation results and compared DSNAODV with EBTS and AODV and it was obvious that DSNAODV improved packet delivery ratio and energy consumption. Here we just detect selfish nodes. In the future, we are aiming to remove them from the network for increasing the lifetime of the network and its performance.

References

[1] S. J. Al-Shakarchi and R. Alubady, *A Survey of Selfish Nodes Detection in MANET: Solutions and Opportunities of Research*, Proceedings of the 1st IEEE Babylon International Conference on Information Technology and Science (BICITS)(2021),178-184.

[2] M. M. Musthafa, K. Vanitha, A.M.J.MD. Zubair Rahman, K. Anitha,*An Efficient Approach to Identify Selfish Node in MANET*, Proceedings of the International Conference on Computer Communication and Informatics (ICCCI)(2020).

[3] D. Das, K. Majumder, A. Dasgupta, *Selfish Node Detection and Low-Cost Data Transmission in MANET using Game Theory*, Procedia Computer Science vol.54 (2015) 92-101.

[4] T. Fahad, R. Askwith, *A Node Misbehavior Detection Mechanism for Mobile Ad-hoc Networks*, (2006).

[5] K. Santhi, B. Parvathavarthini, *Performance analysis of randomized rever ad hoc on-demand distance vector routing protocol in MANET*, Journal of Computer Science vol . 10, no. 11 (2014) 1850-1858.

[6] G. Ghalavand, A. Dana, A. Ghalavand and M. Rezahosieni, *Reliable routing algorithm based on fuzzy logic for Mobile Adhoc Network*, Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering(2010), V5-606-V5-609.

[7] M. Vanday. Baseri, H. Fatemidokht, *Survey of different techniques for detecting selfish nodes in MANETs*, Journal of Mahani Mathematical Research Center (JMMRC) vol. 11, no. 2 (2022) 45-59.

[8] A. Babakhouya, Y. Challal, and A. Bouabdallah, *A Simulation Analysis of Routing Misbehavior in Mobile Ad Hoc Networks*, Proceedings of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies (2008), 592-597.

[9] T. Fahad, D. Djenouri and R. Askwith, *On detecting packets droppers in MANET: A novel low-cost approach*, Proceedings of the Third International Symposium on Information Assurance and Security (2007), 56-64.

[10] D. Djenouri, N. Badache, Two Hops ack, *New approach for selfish nodes detection in mobile ad hoc networks*, Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, (2005), 288-294.

[11] W. Yu, K. J. Ray Liu, *Secure cooperation in autonomous mobile ad-hoc networks under noise and imperfect monitoring, a game-theoretic approach*, IEEE transactions on information forensics and security vol. 3, no. 2 (2008) 317-330.

[12] H. J. Kim, J. M. Peha, *Detecting selfish behavior in a cooperative commons*, Proceedings of the 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, (2008), 1-12.

[13] C. E. Perkins and E. M. Royer, *Ad-hoc on-demand distance vector routing*, Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, (1999), 90-100.

[14] A. N. Thakare, M.Y. Joshi, *Performance analysis of AODV & DSR routing protocol in mobile ad hoc networks, IJCA Special Issue on Mobile Ad-hoc Networks (2010) 211-218.*

[15] L. Buttyan and J.-P. Hubaux, Stimulating cooperation in self-organizing in mobile ad hoc networks, Mobile Networks and Applications vol. 8 (2003) 579-592.

[16] Y. Wang, M. Singhal, On improving the efficiency of truthful routing in MANETs with selfish nodes, Pervasive and Mobile Computing (2007) 537-559.

[17] P. Michiardi and R. Molva, Core, A Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks*, Proceedings of the Communication and Multimedia Security Conference (2002), 107-121.*

[18] T. Anantvalee and J. Wu, Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks*, Proceedings of the IEEE International Conference on Communications, (2007), 3383-3388.*

[19] E. H.Orallo, M. D. Serrat, J.C. Cano, C. T. Calafate, and P. Manzoni, Improving selfish node detection in MANETs using a collaborative watchdog, IEEE Communications Lettersvol. 16, no. 5 (2012) 642-645.

[20] R. Vijian, V. Mareeswari, and K.Ramakrishna, Energy-based trust solution for detecting selfish nodes in MANET using fozzy logic, International Journal of Research and Reviews in Computer Science(IJRRCS) vol. 2, no. 3 (2011) 647-652.

[21] K. Rama Abirami and M. G. Sumithra, Evaluation of neighbor credit value-based AODV routing algorithms for selfish node behavior detection, Cluster Computing vol. 22 (2018) 1–10.

[22] R. Mangayarkarasi and R. Manikandan, Cost effective collaborative anomaly detection system for selfish node attacks in MANET, Journal of Critical Reviews vol. 7, no. 13 (2020) 148-154.

[23] M. Ponnusamy, A. Senthilkumar, R. Manikandan, Detection of selfish nodes through reputation model in Mobile Ad hoc Network–MANET, Turkish Journal of Computer and Mathematics Education vol. 12, no. 9 (2021) 2404-2410.

[24] M.A. Gabri, L. I. Chunlin , Y.Zhiyong, A. H. Naji Hasan, and Z. Xiaoqing, Improved the energy of ad hoc on-demand distance vector routing protocol*, Proceedings of the International Conference on Future Computer Supported Education, (2012), 355 – 361.*

[25] M. Khaeel Ullah Khan and K.S. Rame, Effect on packet delivery ratio (PDR) throughput in wireless sensor networks due to black hole attack, International Journal of Innovative Technology and Exploring Engineering (IJITE) vol. 8, no. 12S (October 2019ar) 428-432.

[26] L. W. Wu and R.-F. Yu, A threshold-based method for selfish nodes detection in MANET*, Proceedings of the IEEE International Computer Symposium (ICS2010), (2010), 875-882.*

Mahboubeh Vanday Baseri
Orcid number: 0000-0003-2527-2072
Department of Computer Science
Shahid Bahonar University of Kerman
Kerman, Iran
Email address: Vanday67@yahoo.com

Marjan Kuchaki Rafsanjani
Orcid number: 0000-0002-3220-4839
Department of Computer Science
Shahid Bahonar University of Kerman
Kerman, Iran
Email address: Kuchaki@uk.ac.ir