Shahid Bahonar University of Kerman

Journal of Mahani Mathematical Research Center

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

SURVEY OF DIFFERENT TECHNIQUES FOR DETECTING SELFISH NODES IN MANETS

M. Vanday Baseri* and H. Fatemidokht

Article type: Research Article

(Received: 05 December 2021, Revised: 20 February 2022, Accepted: 26 February 2021)

(Available Online: 08 March 2022)

(Communicated by A. Borumand Saeid)

Abstract. In Mobile Ad-hoc Networks (MANETs), each node is free to move and connect over a wireless connection, without the requirement for a centralized controller or base station. These features make MANET useful and functional in a variety of areas, including tactical situations, sensor networks, and rescue operations. However, this type of network also has a range of issues such as security, Quality of Service, dynamic topology, scalability, the absence of central management, and energy consumption. In MANETs, some of the nodes do not take part in forwarding packets to other nodes to conserve their resources such as energy, bandwidth, and power. The nodes which act selfishly to conserve their resources are called selfish nodes. In recent years, mobile ad hoc networks have become a very popular research topic. In this paper, we classified techniques for detecting selfish nodes in 4 categories namely reputation-based scheme, credit-based scheme, acknowledgment-based scheme, and game-theoretic scheme. Then we mentioned different methods available for reducing the effect of selfish nodes in mobile ad hoc networks. Finally tables 1 and 2 show the comparison of techniques for detecting selfish nodes.

Keywords: Mobile Ad Hoc Network (MANETs), selfish nodes, Reputation-based scheme, Credit-based scheme, Acknowledgement-based scheme, Game-theoretic scheme.
2020 MSC: 68Mxx.

1. Introduction

The MANET is a dynamic topology network without infrastructure, and it consists of a group of mobile nodes whose communication takes place with no central administration. They move randomly and may act as sources, destinations, or intermediate routers to carry out the transmitting and receiving operations in the network [1]. If the source and the destination mobile hosts are not in the envelopment area, data packets are forwarded to the destination host through other nodes which exist between the two mobile hosts [2]. When a node does not want to forward the data in the network to preserve its resource is known as a selfish node. These types of nodes deny all the packets except

*Corresponding author, ORCID: 0000-0003-2527-2072
E-mail: Vanday67@yahoo.com

DOI: 10.22103/jmmrc.2022.18626.1180

How to cite: M. Vanday Baseri, H. Fatemidokht, *Survey of different techniques for detecting selfish nodes in MANETs*, J. Mahani Math. Res. Cent. 2022; 11(2): 45-59.

those which are destined to it. These nodes use the network and resources for their use and refuse to provide service back. Selfish nodes do not directly attack other nodes, but they simply do not want to use their energy, CPU, or bandwidth to redirect the data [3-5]. Generally, in MANET, all nodes can be divided into three types. They are [6]:

- Non-selfish nodes
- Fully selfish nodes
- Partially selfish nodes

Nodes that allocate their memory space completely for other nodes are called Non-selfish. Selfish nodes do not allocate their memory space for other nodes. Partially selfish nodes allocate a minimum portion of their memory space for other nodes and remain for the benefit of their node. Selfish nodes impress the performance of the network in terms of the partitioning of the network, lifetime of the network, decreased data access, increment rate of packet dropping, and throughput [7]. Ad hoc On-demand Distance Vector Routing (AODV) is the most efficient protocol in comparison to other routing protocols used in the MANET environment as it has low communication overhead due to which, it consumes low memory and bandwidth [3]. For the AODV routing protocol, the behavior of selfish node can be classified as follows [7]:

- Do not forward Route Request (RREQ) messages: When selfish nodes receive RREQ messages, they will not forward these messages and drop these to avoid being the route member for other nodes. Hence the transmission path must be built on more nodes because of avoiding forwarding any messages for others by selfish nodes.
- Do not send Hello messages: This kind of selfish node hides and avoids being included in the others' transmission path.
- Do not forward Data messages: For routing information, this kind of selfish node will forward the messages but it will not relay data messages and drop them. This misbehavior will impact the performance of MANET.
- Delayed forwarding RREQ messages: After this kind of selfish node receives an RREQ message, it will forward this message with a delay to avoid being the route member.
- Do not forward Route Reply (RREP) messages: Because the AODV routing protocol uses the RREP messages translated from the destination node by the intermediate nodes to the source node to establish a completed transmission path. The intermediate nodes will drop all RREP messages received by selfish nodes. The transmission path will not be established. Hence, the source node will persistently send RREQ messages to intend to establish the transmission path. Finally, the whole network will become disabled.

2. Classification of techniques for detecting selfish nodes

Several techniques have been proposed to detect selfish nodes in mobile ad hoc networks, as shown in Figure 1. These techniques can be classified into four categories: the reputation-based scheme, the credit-based scheme, the acknowledgment-based scheme, and the game-theoretic scheme.

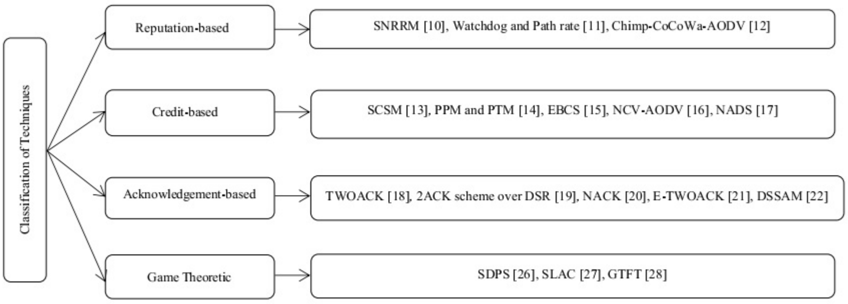
Classification of Techniques
Reputation-based
SNRRM [10], Watchdog and Path rate [11], Chimp-CoCoWa-AODV [12]
Credit-based
SCSM [13], PPM and PTM [14], EBCS [15], NCV-AODV [16], NADS [17]
Acknowledgement-based
TWOACK [18], 2ACK scheme over DSR [19], NACK [20], E-TWOACK [21], DSSAM [22]
Game Theoretic
SDPS [26], SLAC [27], GTFT [28]

Figure 1. Different Techniques for detecting selfish nodes.

2.1. **The Reputation-Based Scheme.** In a reputation-based scheme, nodes detect and declare the misbehavior of a doubtful node. When a declaration is heard, the misbehaving node will be disconnected from the network. In [8] is offered a scheme for mitigating routing misbehavior in MANET. It contains two major modules: watchdog and path rater. The watchdog module distinguishes misbehaving nodes and in the path rater module, the routing protocol avoids these nodes. Nodes use overhearing to confirm whether the next-hop node faithfully forwards the packets or not [8]. One of the main reasons for using reputation systems in a network is providing information to help assess whether an entity is trustworthy or not. This helps in the detection of selfish and malicious nodes. Another reason is to encourage entities to behave in a trustworthy manner, i.e. to encourage good behavior and to discourage untrustworthy entities from participating during communication [9].

2.1.1. *Selfish Node Removal using Reputation Model (SNRRM).* Ponnusamy et al. [10] have proposed Selfish Node Removal using Reputation Model (SNRRM). In their model, the node reputation is determined to remove the selfish nodes from routing. The reputation calculation of each node is done through the node's current energy level and its communication ratio. The source node 'S' is set and destination 'D' is set and the communication begins with the sender node. If both 'S' and 'D' fall under the communication range, the node checks only for 'S' reputation value, if matches, the transmission process is done and the updates the system. If both 'S' and 'D' do not fall under the communication range then 'S' sends control packets to its neighbors and waits for reply messages. Nodes that respond to the message of ‘S’ are considered as reputed nodes. 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’.

2.1.2. *Watchdog and Path rater.* Watchdog and path rater work with the DSR protocol. They operate at the node level of a MANET. The path rater chooses the most secure route to take when sending packets but the Watchdog detects misbehaving nodes. The Watchdog measures a neighboring node’s frequency of dropping or misrouting packets, or its frequency of invalid routing information advertisements. Watchdog maintains a buffer of recently sent packets and compares each overheard packet with the packets in the buffer to see if there is a match. If there is a match, the packet will remove from the buffer. If a packet has remained in the buffer for a long time, for the neighboring node a failure tally is incremented by the Watchdog. If the tally overpasses a predefined threshold, it sends a message to the sender node to be aware of the misbehaving node. Watchdog may not detect a misbehaving node because of ambiguous collisions, receiver collisions, limited transmission power, false behavior, collusion, and partial dropping. A node might be accused of being malicious for the same reasons. Path rater keeps track of the trustworthiness rating of every known node. It calculates path metrics by averaging the node ratings in the path to each known node. If there are multiple paths to the same receiver, then it chooses the path with the highest metric. Watchdog and path rater does not use encryption to protect data or nodes. They use behavior grading by monitoring downstream nodes but are vulnerable to numerous MANET behavior attacks. They do not use multipath routing [11].

2.1.3. *Chimp-CoCoWa-AODV.* Sherif and Salini [12] have presented a Chimp-CoCoWa-AODV protocol to detect and isolate the selfish nodes in MANET. In their method, at first, the selfish node is detected by the local watchdog in the Collaborative Contact-based Watchdog (CoCoWa). Watchdog is one of the best monitoring mechanisms in wireless ad-hoc networks to detect the misbehaving and selfish nodes in the networks. The transmitter and receiver are overheard by the watchdog in terms of calculating the ratio between transmitted packets and received packets to detect the anomalies. The performance of the local watchdog can be improved by the dissemination of information about the selfish node when contact occurs between pairs of nodes. The diffusion between a node pair is defined as a contact. The improved CoCoWa can quickly propagate the selfish node information and hence provides enhanced precision within less time. A node is noted as positive if the watchdog detects that node as a selfish node whereas it is noted as negative if the watchdog detects that node as a non-selfish node. The node transmits information about selfish behavior when in contact with other nodes through collaborative information transmission. Afterward, the selfish node is isolated from the packet transmission. Finally, AODV is integrated with the Chimp optimization algorithm for optimal path selection.

2.2. **The Credit-based scheme.** In a credit-based scheme, incentives are provided for nodes to encourage them to forward data packets. For this purpose, it uses virtual currency or payment systems. When nodes provide services to other nodes, they earn rewards. Similarly, a node must pay other nodes that forward packets sent by that node.

2.2.1. *Stimulating Cooperation in Self-Organizing MANET (SCSM).* Buttyan and Hubaux [13] have proposed a basic idea of this scheme where nodes charge for providing services and atone for receiving a service. In their protocol, for each node, there is a counter, called a nuglet counter, in a tamper-resistant hardware module. When the node sends its packets the counter is decreased, and when the node forwards packets sent by other nodes it is increased. The counter must remain positive or else the node will not be allowed to send its packets. Therefore, each node is patronized to provide forwarding services.

2.2.2. *The Packet Purse Model and the Packet Trade Model.* Buttyin and Hubaux [14] have introduced the packet purse model (PPM) and the packet trade model (PTM). In the PPM model, the originator of the packet pays for the packet forwarding service. The service charge is distributed among the forwarding nodes. The originator loads it with the number of beans sufficient to reach the destination. Each forwarding node obtains one or several beans from the packet and thus, increases the supply of its beans. The packet is discarded when the packet does not have enough beans to be forwarded. The disadvantage of this approach is that it is difficult to estimate the number of beans that are needed to reach a given destination. In the PTM model, the packet does not carry beans but the packet is traded for beans by intermediate nodes. Each intermediary buys it from the previous one for some beans and sells it to the next one for more beans. Destination of the packet covers the total cost of forwarding the packet. An advantage of this approach is that the originator doesn't need to know in advance the number of beans required to deliver a packet. The main disadvantages of the PPM model are as follows. If the packet does not have sufficient beans, then the intermediate node will drop that packet. To forward the packet source node must have the appropriate amount of beans. PTM requires tamper-proof hardware so that no node in the network can increase its beans un-authentically. This is the disadvantage of this method as it increases the cost of the network.

2.2.3. *Energy-Based Credit System (EBCS).* Mubeen and Johar [15] have proposed the Energy Based Credit System (EBCS) for selfish node detection. In this system, the threshold values of energy in the whole the nodes that are suspicious of selfishness. If a regular node sends the packets towards the neighboring nodes, the regular nodes energy will be engaged as reinforcement for sending the packet ECBS increases. In EBCS, if the energy of the node is less than the energy of the threshold, it is recognized as a selfish node. The NS-2 simulator is utilized to appraise the performance of EBCS. The results of the simulation show that EBCS can be improved the packet delivery ratio, throughput, and delay.

2.2.4. *Neighbor Credit Value-based AODV (NCV- AODV).* Abirami and Sumithra [16] have presented the Neighbor Credit Value-based AODV (NCV- AODV), which extends from the AODV protocol. This type is applied in securing networks against selfish nodes. This system detects the node by relying on the observation of the packets that have been redirected from the neighboring node, but this strategy fails as soon as the neighboring node tends to drop the data packet for a real reason. When the node is identified as selfish, a credit value-based (NCV- AODV) running the agent will send a fake packet to the suspect node for making sure whether or not it is indeed selfish. A major benefit of applying such a method is that the detection load is not increased. The NCV-AODV successfully detects the selfish nodes and therefore tends to avoid the forwarding of packets to them. This method increased the overall performance significantly.

2.2.5. *New Adaptive Credit-Based Stimulation Scheme (NADS).* Bounouni and Medjkoune [17] have presented the New Adaptive Credit-Based Stimulation Scheme (NADS) for the detection of selfish nodes in MANET. In this scheme, the cooperation between the nodes is simplified and justice between them is guaranteed. In the NADS scheme, nodes include three discrete ranks that are based on their credit values. Prices and gratuities are described according to the node credit rating. The NS-2.34 simulator is used to test the efficiency of performance. 40 nodes were used for the simulation. The results of the simulation display that the NADS scheme reduces the delivery ratio of selfish and monopolized times of selfish nodes.

2.3. **The Acknowledgement-Based Scheme.** This scheme uses an acknowledgment technique to detect misbehaving nodes.

2.3.1. *Two-Acknowledgment (TWOACK).* Balakrishnan et al. [18] have proposed a network-layer acknowledgment-based scheme, called TWOACK, to detect misbehaving nodes. In the TWOACK scheme, each node observes the behavior of its next-hop using acknowledgments instead of the overhearing technique. Ambiguous collisions, receiver collisions, and limited transmission power are some problems of the overhearing technique that the TWOACK scheme can resolve. TWOACK is an early version of the 2ACK scheme.

2.3.2. *2ACK Scheme over DSR.* Liu et al. [19] have considered only packet forwarding misbehavior. When a node forwards a data packet successfully over the next hop, the destination node of the next hop will send back a special two-hop acknowledgment called 2ACK. This method works along with the DSR protocol.

2.3.3. *The NACK scheme.* The 2ACK scheme can only prevent routing misbehaviors but NACK can also detect collusions attacks. Sun et al. [20] are proposed the NACK scheme. It is a novel acknowledgment-based approach and can be implemented in DSR. Figure 2 shows the configuration of the NACK scheme. In figure 2, N1, N2, ..., Nn are intermediate nodes. NACK scheme uses a special packet format that is just like a receipt. After a data packet is sent, each node Ni monitors the next-hop to check whether or not the next-hop, Ni+1, forwards the data packet. If Ni+2 receives the data packet correctly, it must send an acknowledgment called NACK packet as a receipt for Ni. If Ni does not receive the NACK packet from Ni+2, Ni will consider Ni+1 a misbehavior node, otherwise, it will consider Ni+1 a normal node.

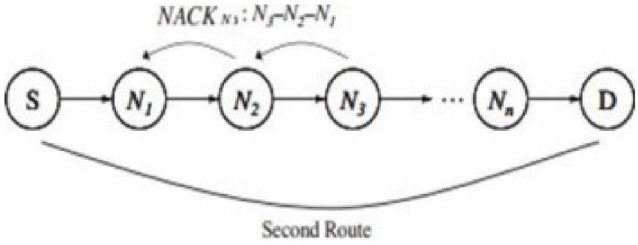

FIGURE 2. The NACK scheme [20].

2.3.4. *Enhanced TWOACK (E-TWOACK).* Sayyar et al. [21] have proposed the Enhanced TWOACK protocol that they built over AODV. Compared with the DSR+TWOACK scheme, the proposed AODV+E-TWOACK scheme can enhance the performance of the network. In the proposed E-TwoAck scheme, the sender node detects a selfish node attack by resending the data packet twice again and waits for an acknowledgment before discarding the existing route. Additionally, the proposed protocol detects selective forwarding attacks by calculating the discard ratio of the existing route. The simulation results show that this scheme performs more efficiently than DSR+TWOACK in terms of packet delivery ratio, routing overhead, and end-to-end delay.

2.3.5. *Digitally Signed Secure Acknowledgement Method (DSSAM).* Srivastava et al. [22] have proposed the Digitally Signed Secure Acknowledgement Method (DSSAM) using the RSA digital signature. In this method, secure acknowledgment, packet authentication, and node authentication, which are three significant security factors in MANET, are considered. The DSSAM applies the mechanism of cryptography to secure the network. This scheme prevails the weakness of available techniques of intrusion detection such as the problem of false identity and receiver collision. The QualNet Simulator-7.0 is used to evaluate the performance of DSSAM. The results of the simulation show that the DSSAM compared to Watchdog and 2-ACK under DSR routing protocol is improved the detection rate. However, this method begets more overhead of routing.

2.4. **The Game-Theoretic Scheme.** In a game-theoretic scheme, the Intrusion Detection System (IDS) compares the node's performance against other nodes based on a repeated game. Implementation of this scheme is easy but it needs fair comparison among nodes otherwise it may falsely identify a node as an adversary node [23]. In-game theory, there is an assumption that an entity wants to maximize its payoff, which is usually regarded as selfish. For tempting cooperativeness and discouraging selfishness most existing work used rewards or incentives so that each entity tries to obtain the best individual payoff [24]. Generally, games can be categorized as non-cooperative and cooperative games. Non-cooperative game theory is concerned with the analysis of strategic choices and explicitly models the decision-making process of a player out of his/her interests. Unlike in non-cooperative games, in cooperative games, the players can make binding commitments [25].

2.4.1. *Selfish Dynamic Punishment Scheme (SDPS).* Sharah et al. [26] have proposed a mechanism that concerns rehabilitation rather than excluding the selfish node by tracking them in the network. The proposed mechanism is based on the game theory where node coalition is used to monitor the selfish behavior and motivate selfish nodes to cooperate. The main goal of the punishment strategy is to ensure that the nodes will start cooperating again and not cause any further problem for the coalition, also focus on promoting and motivating nodes rather than just excluding them.

2.4.2. *Selfish Link and behavior Adaptation to produce Cooperation (SLAC) algorithm.* Hales [27] has introduced the Selfish Link and behavior Adaptation to produce Cooperation (SLAC) algorithm. It assumes that nodes want to use their abilities selfishly to increase their utility greedily. The algorithm depends on Selfish Link and behavior Adaptation to produce Cooperation (SLAC). SLAC generates some measure of utility U (The number of files downloaded or jobs processed) according to the activities of each node. Periodically each node (i) compares its performance against another node (j), randomly selected from the network. If the utility Ui¡Uj node then node I drop all current links to j.

2.4.3. *Generous TIT-FOR-TAT (GTFT) algorithm.* Srinivasan et al. [28] have proposed the Generous TIT-FOR-TAT (GTFT) algorithm. Nodes use the GTFT algorithm to consider relay requests made by the neighbor nodes and decide to accept or reject a relay request. It shows that the GTFT algorithm provides maintenance of Nash balance in the network and the system move to the rational and optimal operating point. For each node, the algorithm defines the Normalized Acceptance Rate (NAR). It is the ratio of the number of successful relay requests generated by the node, to the number of relay requests made by the node. According to the NAR selfishness can be decided.

3. The comparison of techniques

In Table 1, we express the advantages and disadvantages of different techniques for detecting selfish nodes [9, 25, 29-31]. Also, in Table 2 the comparison of mentioned routing protocols for detecting selfish nodes based on various parameters is summarized.

4. Conclusion

Ad hoc networks are a set of nodes that are connected via wireless links without using a fixed infrastructure or centralized administration. Due to this feature of ad hoc networks, the security of these networks is a significant topic. In Mobile Ad hoc Networks (MANETs) the selfish nodes do not participate in the routing process, which intentionally delays and drops the packet. These misbehaviors of the selfish nodes will impact efficiency, reliability, and fairness. The selfish node utilizes the resources for its purpose, and it neglects to share the resources with other nodes. So, it is important to detect the selfish nodes in MANET. In this paper, we explained some techniques that have been proposed to detect selfish nodes in MANETs. After that comparison of them showed in Tables 1 and 2.

References

[1] K. Susan, K. C., J.-O. A. M., and M. E. S., *An Improved Token-Based Umpiring Technique for Detecting and Eliminating Selfish Nodes in Mobile Ad-hoc Networks*, Egypt. Comput. Sci. J., vol. 44, no. 2 (2020) 74–85.

[2] J. S. Raja. and I. J. Raja, *Survey on Selfishness Handling In Mobile Ad Hoc Network*, A International Journal of Emerging Technology and Advanced Engineering vol. 2, no. 11 (2012) 688–692.

[3] H. Yadav and H. K. Pati, *A Survey on Selfish Node Detection in MANET*, Proceedings of International Conference on Advances in Computing, Communication Control and Networking, ICACCCN, (2018), 217—221.

[4] S. Aifa and T. Thomas, *Review on Different Techniques Used in Selfish Node Detection*, Proceedings of the IEEE International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), (Kottayam, India, 2018), 1—4.

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

[6] J. H. Choi, K. S. Shim, S. Lee, and K. L. Wu, *Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network*, IEEE Transactions on Mobile Computing vol. 11, no. 2 (2012) 278–291.

[7] N. K. Gupta, A. K. Sharma, and A. Gupta, *Selfish Behaviour Prevention and Detection in Mobile Ad-Hoc Network Using Intrusion Prevention System (IPS)*, International Journal of Research Review in Engineering Science and Technology (IJRREST) vol. 1, no. 2 (2012) 31–34.

Table 1. The comparison of techniques for detection of selfish nodes.

	The Reputation-based Scheme	The Credit-based scheme	The Acknowledgement-based Scheme	The Game-Theoretic scheme
Based on	Reputation metric for each node	Virtual Money Concept	Acknowledgment	credit, reputation, and Acknowledgement
Advantages	It relies on observations from multiple sources. Resistant to the diffusion of false information from a small group of lying nodes.	Successful in stimulating cooperation. Useful in multi-hop wireless networks, where the action and its reward are not simultaneous.	The TWOACK scheme can resolve the problems of the overhearing technique such as ambiguous collisions, receiver collisions, and limited transmission power.	It is a powerful tool to study situations of conflict and cooperation, which is concerned with finding the best actions for individual decision-makers (i.e., players).
Disadvantages	Resource consuming. Susceptible to the dissemination of false information from large groups of lying nodes. It needs for authentication techniques complex systems.	Failure to detect selfish/malicious nodes. The average credit level within the system needs to be kept at a reasonable level for incentives to work properly. In most cases complicated and difficult to implement. Resource consuming. Unfair distribution of credits, particularly for remote nodes. for remote nodes The monetary reward may cause as an incentive for cheating for a node	Compared to overhearing techniques, the 2ACK scheme has a higher routing overhead.	It is not practical to assume that players know their payoffs and the payoffs of others. The techniques of solving games involving mixed strategies, particularly in the case of a large pay-off matrix are very complicated. All the competitive problems cannot be analyzed with the help of game theory.

Table 2. The comparison of mentioned routing protocols for detecting selfish nodes.

Methods	Based on	Routing protocol	Software simulation	Strategy	Disadvantage
SNRRM (2021) [10]	Reputation	-	NS2.35	Detect selfish node and choose reliable rout	In the SNRRM scheme, the selfish nodes are not cooperative with each other, therefore the famous nodes are detected via the communication ratio analysis between the nodes
Watchdog & pathrate (2012) [11]	Reputation	DSR	OPNET	Detect and choose the optimal path	Watchdog may not detect a misbehaving node because of ambiguous collisions, receiver collisions, limited transmission power, false behavior, collusion, and partial dropping.
Chimp-CoCoWa-AODV (2021) [12]	Reputation	AODV	NS2.35	Detect and isolate selfish node	Chimp-CoCoWa-AODV does not use encryption to protect data or nodes. It uses behavior grading by monitoring downstream nodes but is vulnerable to numerous MANET behavior attacks.
SCSM (2003) [13]	Credit	GPFA	C++	Detect selfish node	SCSM is restricted to unicast traffic, and it seems to be difficult to extend it to multicast. Also, in this method is assumed that every packet has the same size.
PPM and PTM (2000) [14]	Credit	-	-	Detect and choose the optimal path	In PPM, if the packet does not have sufficient beans, then the intermediate node will drop that packet. To forward the packet, the source node must have the appropriate amount of beans. PTM requires tamper-proof hardware so that no node in the network can increase its beans un-authentically. This is the disadvantage of this method as it increases the cost of the network.

EBCS (2019) [15]	Credit	DSR	NS2	Detect and eliminate selfish node	This method eliminates the selfish node from packet transferring.
NCV-AODV (2018) [16]	Credit	AODV	NS2.35	Detect and prevent selfish node	This method fails as soon as the adjacent node tends to drop the packet of data for a real reason.
NADS (2018) [17]	Credit	DSR	NS2.34	Detect and motivate collaboration	Since NADS enable nodes to share their recommendations, selfish nodes may share fake recommendations to improve falsely the reputation value of selfish node or to deteriorate the reputation value of an honest node, known as a false dissemination attack.
TWOACK (2005) [18]	Acknowledge	DSR	NS2	Detect and avoid selfish node	This method improved the packet delivery ratio, with a reasonable additional routing overhead but with some expected increase of false alarms.
2ACK (2007) [19]	Acknowledge	DSR	NS2	Detect and mitigate the effect of selfish node	This method is focused only on link misbehavior. It is more difficult to decide the behavior of a single node.
NACK (2012) [20]	Acknowledge	DSR	NS2	Detection of routing misbehavior and collusion attack	Although NACK can resist a successful collusion attack, it only considers the case of two consecutive nodes.
E-TWOACK (2018) [21]	Acknowledge	AODV	NS2.35	Detect selfish node	In this method, the sender may not receive an acknowledgment.
DSSAM (2021) [22]	Acknowledge	DSR	QualNet Simulator-7.0	Detect selfish node	DSSAM creates more routing overhead.

SDPS (2020) [26]	Game theory	-	NS2	Detect and motivate collaboration	In SDPS, only neighbors who have a direct connection with a specific node can testify the degree of cooperation for that node and only these nodes can update their misbehaving table.
SLAC (2004) [27]	Game theory	-	Ada	Detect selfish node	Nodes that never change their behavior from selfish options could be the worst enemies of a SLAC approach.
GTFT (2003) [28]	Game theory	AODV	-	Detect and motivate collaboration	In GTFT is assumed that nodes are rational, therefore nodes will not always be willing to expand their energy resources to relay traffic generated by other users.

[8] S. Marti, T.J. Giuli, K. Lai, and M. Baker, *Mitigating routing misbehavior in mobile ad hoc networks*, Proceedings of the 6th annual international conference on Mobile computing and networking (New York, NY, United States, 2000), 255-–265.

[9] R. kaushikand J. Singhai, *Detection, and Isolation of Reluctant Nodes Using Reputation Based Scheme in an Ad-hoc Network*, International Journal of Computer Networks & Communications (IJCNC) vol. 3, no. 2 (2011) 95–105.

[10] M. Ponnusamy, Dr. A. Senthilkumar, Dr.R.Manikandan, *Detection of Selfish Nodes Through Reputation Model In Mobile Adhoc Network – MANET*, Turkish Journal of Computer and Mathematics Education vol. 12, no. 9 (2021) 2404–2410.

[11] T. H. Lacey, R.F. Mills, B.E. Mullins, R.A. Raines, M. E. Oxley, and S.K. Rogers, *RIPsece- Using Reputation-based Multilayer Security to Protect MANETs*, Computers and Security vol. 31 (2012) 122–136.

[12] B.V. Sherif and P. Salini, *Detection and Isolation of Selfish nodes in Manet using Collaborative Contact-Based Watchdog with Chimp-AODV*, Research Square, springer (2021) DOI: https://doi.org/10.21203/rs.3.rs-754829/v1.

[13] L. Buttyan, J.P. Hubaux, *Stimulating cooperation in self-organizing mobile ad hoc networks*, ACM/Kluwer Mobile Networks and Applications vol. 5, no. 8 (2003) 579—592.

[14] L. Buttyan and J.P. Hubaux, *Enforcing Service Availability in Mobile Ad-Hoc WANs*, Proceedings of 2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No.00EX444), (Boston, MA, USA, 2000), 87–96.

[15] S. Mubeen and S. Johar, *Detection and Elimination of the Selfish Node in Ad-Hoc Network Using Energy Credit Based System*, J. Netw. Inf. Secure. vol. 7, no. 2 (2019) 18–22.

[16] 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.

[17] M. Bounouni and L. Bouallouche-Medjkoune, *Adaptive Credit-Based Stimulation Scheme for Dealing with Smart Selfish Nodes in Mobile Ad Hoc Network*, Proceeding of the 2018 International Symposium on Programming and Systems (ISPS), (Algiers, Algeria, 2018), 1–5.

[18] K. Balakrishnan, J. Deng, and P. K. Varshney, *TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks*, Proceeding of the IEEE Wireless Communications and Networking Conference, WCNC, (New Orleans, LA, USA, 2005), 2137—2142.

[19] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, *An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs*, IEEE Transactions on Mobile Computing vol. 6, no. 5 (2007) 536–550.

[20] H. M. Sun, Ch. H. Chen and Y. F. Ku, *A Novel Acknowledgment-based Approach Against Collude Attacks in MANET*, Expert Systems with Applications vol. 39 (2012) 7968–7975.

[21] S. Sayyar, A. Khan, F. Ullah, H. Anwar, and Z. Kaleem, *Enhanced TWOACK Based AODV Protocol for Intrusion Detection System*, Proceeding of the 2018 International Conference on Computing, Mathematics and Engineering Technologies, (Sukkur, Pakistan, 2018), 1-–4.

[22] A. Srivastsva, S.K. Gupta, M. Najim, N. Sahu, G. Aggarwal, and B.D. Mazumdar, *DSSAM: digitally signed secure acknowledgment method for mobile ad hoc network*, EURASIP Journal on Wireless Communications and Networkingvol. 12 (2021) https://doi.org/10.1186/s13638-021-01894-7.

[23] D. B. Roy and R. Chaki, *MADSN: Mobile Agent-Based Detection of Selfish Node in MANET*, International Journal of Wireless & Mobile Networks(IJWMN) vol. 3, no. 4 (2011) 225-235.

[24] J. H. Cho and I. R. Chen, *On the Tradeoff Between Altruism and Selfishnessin MANET Trust Management*, Ad Hoc Networks vol. 11 (2013) 2217–2234.

[25] L. Zhao, J. Zhang, K. Yang, and H. Zhang, *Using Incompletely Cooperative Game Theory in Mobile Ad Hoc Networks*, Proceedings of the 2007 IEEE International Conference on Communications, (Glasgow, UK, 2007), 3401–3406.

[26] A.A. Sharah, M. Alhaj, and M. Hassan, *Selfish Dynamic Punishment Scheme: Misbehavior Detection in MANETs Using Cooperative Repeated Game*, International Journal of Computer Science and Network Security (IJCSNS) vol. 20, no. 3 (2020) 168–173.

[27] D. Hales, *From Selfish Nodes to Cooperative Networks – Emergent Link-based incentives in Peer-to-Peer Networks*, Proceedings of the Fourth International Conference on Peer-to-Peer Computing (P2P'04), (Zurich, Switzerland, 2004), 151–158.

[28] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao, *Cooperation in Wireless Ad Hoc Networks*, Proceedings of the IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), (San Francisco, CA, USA, 2003), 808–817.

[29] A. Gupta and A. Saxena, *Detection and Prevention of Selfish Node in MANET using Innovative Brain Mapping Function: Theoretical Model*, International Journal of Computer Applications vol. 57, no. 12 (2012) 17–20.

[30] D. E. Charles, K. D. Georgilakis and A. D. Panagopoulos, *ICARUS: Hybrid Incentive Mechanism for Cooperation Stimulation in Ad hoc Networks*, Ad Hoc Networks vol. 10 (2012) 976–989.

[31] http://www.universalteacherpublications.com/univ/ebooks/or/Ch9/limit.htm (Available at March 15, 2010).

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

Hamideh Fatemidokht
Orcid number: 0000-0002-6087-6499
Department of Computer Science
Faculty of Mathematics and Computer
Shahid Bahonar University of Kerman
Kerman, Iran
Email address: h.fatemidokht@math.uk.ac.ir