Hindawi
Security and Communication Networks
Volume 2022, Article ID 6486816, 20 pages
https://doi.org/10.1155/2022/6486816

Review Article

Detecting Noncooperation Nodes Mechanisms in Wireless Networks: A Survey

Solmaz Nobahary,[1] **Hossein Gharaee Garakani,**[2] **and Ahmad Khademzadeh**[2]

[1]*Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*
[2]*ICT Research Institute, ITRC, Tehran, Iran*

Correspondence should be addressed to Solmaz Nobahary; solmaz_nobahary@yahoo.com

Received 9 February 2022; Revised 30 May 2022; Accepted 26 June 2022; Published 20 July 2022

Academic Editor: Marimuthu Karuppiah

Wireless networks face security problems compared with traditional wired networks. In wireless networks such as wireless sensor networks (WSNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), and the internet of things (IoT), nodes have limited radio bandwidth and power supply then. They require cooperation in sending messages. It increases the motivation of nodes not to cooperate in such networks. This paper reviews different methods for identifying and stimulating nodes for focused cooperation. The performance of each method, its advantages, and its disadvantages have been reviewed and functionally categorized and compared with the metrics of false positive/negative rate and detection accuracy, throughput, and other metrics.

1. Introduction

Nowadays, data collection, sampling, and analysis are carried out to improve production efficiency and the optimal use of resources and save cost; wireless networks are a practical solution to this goal. Wireless networks are particular computer network that uses wireless data communications between nodes. With wireless networking, there is no longer an expensive cabling process in residential homes, companies, and so on [1–3].

Wireless networks enable the desired convenience and mobility for the user. Widespread different wireless technologies have their performance characteristics, each optimized for a specific task and context. The different wireless technologies led to various wireless networks such as MANET, VANET, WSN, and IoT [3–5].

Since all nodes are connected through wireless communication, the existence of nodes with a limited range of wireless connections necessitates the cooperation of these network nodes and the multihop communication between them. Due to the limited wireless communication range, routing is essential in such nodes. Providing security in such multihop communication environments is a critical issue [6–9] so that each node sends its neighbors' packets to the other nodes, providing the nodes to communicate between nodes that are not in the range of each other. However, the cooperation of the nodes puts these networks in serious trouble due to the limited range of signal transmission and open-transfer media, with the power and limited power of the nodes [10, 11].

Some nodes do not cooperate and provide services to other nodes, putting the network at serious risk. In general, such nodes are called selfish nodes that use the network facilities. The selfish nodes do not contribute to saving energy and establish and maintain the other nodes, a rout, by not participating in the routing and packet forwarding. As a result, network performance significantly decreases in the presence of selfish nodes. The discussion of the selfish nodes is not only crucial in the IoT but also ad hoc networks, vehicle ad hoc networks, and wireless sensor networks. Detection and management of selfish nodes are essential to overcome the noncooperation of nodes in the network [11, 12].

Several approaches have been proposed to detect noncooperation nodes and stimulate them to cooperate with other nodes. According to their nature, these approaches are divided into seven groups known as reputation-based approaches, credit-based approaches, punishment-based approaches, acknowledgment-based approaches, game theory approaches, fuzzy logic-based approaches, and nonformal approaches.

The article's main contribution is to introduce extensive research on detecting selfish and malicious nodes.

(i) The study summarized and categorized the different mechanisms in their structure and process

(ii) The different metrics are investigated to present the advantage and disadvantages of the mechanism

(iii) The metrics are investigated, such as end-to-end delay, percent of detection, false positive/negative rate, and packet delivery rate

(iv) The article used comparative analysis to recognize the crucial weaknesses and open issues to motivate new algorithms to detect noncooperation nodes in wireless networks

The remainder of this paper is organized as follows. Related work is explained in Section 2. Section 3 expresses the definition of selfishness and the features of the selfish node. All different methods of detecting noncooperation nodes that investigated the pros and cons of the techniques are categorized in Section 4. Section 5 analyzes and discusses the open issue of selfish and malicious node detection in wireless networks. Finally, in Section 6, the conclusion is presented.

2. Related Work

Some articles have discussed several approaches for dealing with selfish nodes in mobile ad hoc networks [13–18]. It categorized the methods as incentive protocols and identified and isolated selfish nodes protocols; then, it expressed the techniques' weaknesses and strengths in each group [19].

Padiya et al. designed the mechanism to detect misbehaving nodes in MANET. The article has classified the proposed methods into three categories: reputation-based techniques, credit-based techniques, and acknowledgment-based techniques. It surveyed the reputation-based technique relies on building a reputation table according to the nodes' behavioral patterns; the credit-based technique relies on providing incentives to all nodes in the network to perform networking functions faithfully. Furthermore, acknowledgment-based techniques rely on the reception of an acknowledgment message from destination nodes to verify that a packet has been forwarded. The research explained the structure of the protocols in each different classification and the advantages and disadvantages of methods [20].

Samian et al. summarized existing cooperation stimulation mechanisms to detect selfish nodes in wireless networks and discussed important metrics in different protocols such as false positive rate, detection accuracy, and network throughput. They discussed an open issue to improve the critical metrics in the network and divided the stimulated mechanism into the incentive- and the punishment-based mechanism. Also, the mechanisms are divided as follows: credit-based, reputation-based, game-theory-based, fuzzy-logic-based, and hybrid schemes. The different mechanisms' structure and their strength and weakness have been investigated to resolve the problem of selfish node detection in wireless networks [21].

Other articles have investigated selfish and malicious node detection in MANET [13, 22, 23]. The articles briefly summarized mobile ad hoc networks and its feature that lead to nodes behaving selfishly. Misbehave nodes are divided into selfish and malicious nodes and discussed their effect on the network. Different watchdog schemes and other methods are explained in the articles to detect misbehavior nodes.

As mentioned above, all the articles summarized the detection of the selfish node, but they did not compare the methods with essential metrics. This article investigated the different noncooperative nodes and then categorized the detection schemes into groups by their structure and compared them in each group. Comparison of schemes can help us motivate new mechanisms and design better protocols to overcome misbehavior nodes in network application. Important metrics are checked in different schemes to design better protocols.

3. Noncooperation and Selfish Nodes

Wireless networks have various networks, and it is inconceivable to use a definition of selfishness and malicious as noncooperation nodes. A threat to the wireless mesh network is very different from a threat to WSN or VANET. For this reason, we first discuss the general definition of selfishness and malicious [12, 24].

The fundamental differences are between malice and selfishness; the malicious nodes are in the first tendency to hurt the network, while selfishness tends to use network resources more and more. From the view of classical security, only malice has been investigated: for some reason, an attacker intends to attack at full, but it is not too late. Security applications are not confined to military cases, and they have a full-color role in commercial applications. In other business applications, the previous security mechanisms are not working because, first, it is challenging to identify the attackers; second, those who design the security mechanisms do not benefit the winners; and finally, it is not easy to prevent the use of the most network resources.

Definition 1. Misbehavior and malice behavior are personal or group behavior that has been isolated to prevent standard behavior or prescribed behavior from achieving a specific goal. It is assumed that standard and prescribed behavior is generally defined.

Definition 2. Misbehavior is selfishness if an attempt to take benefits can be expressed as a single number (bit rate, joule) in the network; any other behavior is considered malicious.

If the selfish node cooperates with other nodes, it can prolong the network lifetime, but it seeks to achieve the most preferences for its own. It will be checked in the forwarded data packet to clarify more. A node can send packets to the base station if it sends this packet to another node closer to the base station and consumes less energy. If the node sends the packet to the destination to help the other node, that node will consume more energy. The selfish node is only friendly to requesting help from the remaining nodes and not helping them. This definition does not exist in networks that are managed by a central system because all nodes have a common goal; it performs tasks in such a way to prolong the network lifetime. However, the definition makes sense when there are multiple scenarios, such as IoT networks so that several sensor networks or other wireless networks that are individually managed and implemented in a region. These networks, the fact that they play cooperation between them, lead to their lifetime, but because the game has endings, they lead them to misbehavior and selfishness. Initially, the selfish node is not inherent in the network. However, when a node is conquered by a hostile and has changed the nodes' hardware and software, selfish behavior is possible even on a wireless sensor network. Nevertheless, since the purpose of conquering nodes is damage to the network, these nodes are called malicious nodes.

We can define the types of nodes in the wireless network, consisting of three categories of regular, selfish, and malicious nodes.

> Normal node: the network nodes are the case that deal with their normal activities for sending and receiving packets and do nothing to cause a malfunction or misuse of the network.
>
> Selfish nodes: these nodes are divided into three categories derived from their behavior in routing algorithms such as dynamic source routing (DSR) [25]. These three categories are as follows:
>
> > Selfish nodes type 1: these nodes participate in the routing phase and maintain the best route between the source and destination but do not forward the next node packet during the transmission phase.
> >
> > Selfish nodes type 2: these groups of nodes do not participate in the routing phase to find the best route between the source and destination and do not forward the next node packet during the transmission phase. These nodes merely use their energy and resources to send and receive their packets.
> >
> > Selfish nodes type 3: behavior or misbehavior of these nodes changes with different environments. The behavior of these nodes depends on their energy level. When the energy levels of these nodes are between their maximum energy (E) and the first set threshold (T1), they behave like normal nodes. If their energy levels are between the first threshold (T1) and the second set threshold (T2), they will behave like the first type nodes. Furthermore, finally, if their energy levels are less than the second threshold (T2), they will behave like second-order nodes. The relationship between threshold values and maximum energy is $\mathrm{T2} < \mathrm{T1} < E$ [12, 26].
>
> Malicious node: a malicious node refers to a node that is a network member and is looking for malicious purposes in the network. The common goals among the malicious nodes are as follows:

(i) Try to maximize disruption to network operation and performance

(ii) Try to cheat the normal nodes

(iii) Try to ignore or drop the packets and not forward them

(iv) Try to direct packets into the wrong path

(v) Try to waste the energy of the normal nodes

(vi) Try to hide their malicious behavior from intrusion detection systems and other normal nodes

The strategy that adopts a malicious node is as follows:

1. First, it cooperates with normal nodes to get their trust.
2. It attempts to attack to eliminate network performance or achieve its malicious purpose. It will increase its usefulness.
3. It runs before the other nodes collect sufficient evidence against it.
4. Enter the network as a new node.

Several approaches have been developed to discover noncooperative nodes and stimulate them to cooperate with other nodes in the network. According to their nature, these approaches are divided into six groups known as reputation-based approaches, credit-based approaches, punishment-based approaches, acknowledgment-based approaches, game theory approaches, and hybrid and specified approaches. The main classification of noncooperation detection methods is shown in Figure 1.

4. Detection and Stimulation of Noncooperation Nodes Mechanisms in Wireless Networks

4.1. Reputation-Based Mechanism. In reputation-based methods, network nodes cooperate in providing feedback for a set of particular nodes. Each node is assigned a reputation value for its feedback. The nodes have more reputation value to recognize as trusted nodes in the network, and the nodes have less reputation as noncooperative nodes. These methods' advantages are applying low traffic on the network to discover noncooperative nodes and not sending data packets on paths with noncooperative nodes. However, the main disadvantages of these methods are low efficiency, low scalability, high overhead (regulation and information, hardware), nonvalidation, unreliable channel, and collusion of noncooperative nodes.

The most common approach is a watchdog method based on the reputation mechanism in which the watchdog is responsible for detecting misbehaving nodes [27]. In this approach, when the watchdog node receives a packet, it will compare it with the packets in its buffer, and if the watchdog matches the packet with one of the packets, it will remove the above packet from the buffer. If a node's packet is not deleted from the buffer after a certain period, the sender node is a misbehaving node. If the node misbehaving exceeds a predetermined threshold, the misbehaving of the node will prove, and the source node will communicate with the misbehaving

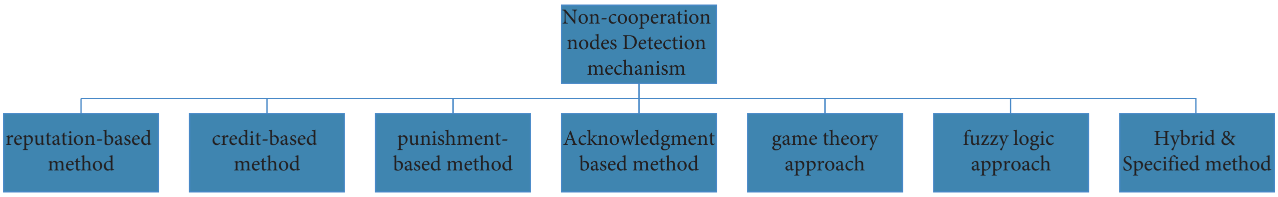

Figure 1: Classification of noncooperation nodes detection methods.

node by sending a message to the source node. When the nodes' mobility increases and nodes change their coordinate, the selfish nodes can detect by watchdogs, and the network throughput increases. This approach is the dynamic source routing (DSR) protocol implant to detect the network layer's misbehaving nodes responsible for sending packets. The disadvantage of the watchdog approach may not be able to detect selfish or malicious nodes in the event of an ambiguous collision, a collision in the receiver, a limited range transmission, collusion, detecting misbehavior by changing the range, dropping the packets, and not punishing the selfish nodes. Marti et al. proposed a path-rater approach based on the reputation approach to detect the misbehaving nodes by all network nodes. In this protocol, to select a high-reliability path, the knowledge associated with suspicious nodes to misbehavior with related data has been integrated with the reliance on linking capabilities. Each node assigns a value for all nodes within its range, which points to the reliability of that node. The advantages of the path-rater approach have high performance and throughput, but the disadvantage is that by increasing the node's mobility, transmission overhead also increases.

The OCEAN (observation-based cooperation enforcement in ad hoc networks) approach [28] is the DSR protocol developed and a reputation-based approach. This approach is similar to [16, 29], based on the monitoring method. It uses five packets called node monitoring, route control, radio-based routing, traffic injections to detect misbehaving nodes, and a recurrence mechanism. In this approach, network nodes rated other nodes at first and then updated the rates after monitoring a particular incident. This approach classifies these nodes as misbehaving and selfish nodes by observing misbehavior when applying traffic on the network. If a node cooperates by discovering a route but does not forward a packet, it is the misbehaving node because it misses the nodes to pass the packets.

Nevertheless, if a node does not cooperate in the route discovery process, it will be called the selfish node. The advantages of this approach are a method of self-assessment and reducing the false alarm rate in detecting selfish and malicious nodes. However, its disadvantages are high energy consumption, not being a privacy policy, and being an unreliable channel [30].

A reputation-based approach called HEAD (hybrid mechanism to enforce node cooperation) was presented to resolve the weaknesses of the OCEAN approach [31]. In the approach in the identification phase, the warning message is used instead of displaying the list of faults and selfish nodes. It also uses the DSR routing protocol, which, by interacting with the protocol, can detect the misbehavior of nodes in the production process of data packets and isolate them in the route discovery process. By discovering the misbehavior, these node types are classified into three categories: malicious, selfish, and conquered nodes. All these nodes are identified and isolated from the network. This defect approach has solved the OCEAN method failure problem. However, other advantages and disadvantages of the method remain.

An intelligent reputation-based approach called the separation of detection authority (SDA) is designed to detect selfish nodes in the network [32]. Unlike previous approaches in this approach, the network's reliability is also considered. This approach is based on a central organization to recognize the credit of the nodes, which consists of three sections: reporters, agents, and a central authority. In this approach, when a node observes suspicious behavior from its neighboring node(s), it introduces itself as a reporter to the central authority. Then the central authority assigns nodes to the neighboring suspect nodes as agents to determine the behavior of the suspect nodes and determine whether the node is suspicious forwards the data packets. After observing a period, each node sends the results of its observations to the central authority. The agents send the results of the observations, and the central organization will make final judgments by majority vote about the suspect nodes based on the results. This approach also suffers from the disadvantages of previous approaches.

A reputation-based method has been proposed based on the nodes' energy consumption and information distributed in the network to identify selfish nodes and implement cooperation between nodes [33]. The proposed method considers the resources used by the nodes as the consumption-to-cooperation ratio (C2C), which has presented the general behavioral history of the nodes. A node has exploited several resources for its benefit and how much it has helped the network. To calculate the reputation of the nodes, each node in the network maintains a C2C table to record the consumption and cooperation of other nodes. Under this mechanism, each node in an ad hoc network implements an independent reputation assessment scheme that aims to identify nodes that do not work together and are separated from the network to store the resources of other cooperative nodes. The proposed method has high detection accuracy and a higher data packet delivery rate. However, this method has communication and memory overhead.

4.2. *Punishment-Based Mechanism.*

In punishment-based methods, each node directly or indirectly monitors how other nodes cooperate and the results of observations and information used to punish or encourage other nodes. In these methods, the punishment of selfish or malicious nodes stimulates them to cooperate with other nodes and provide services in the network. These features of the methods have some benefits, such as resilience to collision attack, the collusion of the nodes and denial of service (DOS) attack, and high scalability. The major disadvantage of these methods is low efficiency, overhead, high energy consumption, and nonvalidated and unreliable channels—the articles are classified as a punishment- and reputation-based mechanisms in Table 1.

Michiardi and Molva have proposed a mechanism that encourages and punishes the nodes for finding selfish nodes in the network and called it CORE (collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks) [35]. This approach combines the watchdog mechanism and the reputation-based system, which sets reputation tables (RTs), and it can discover the routes, send the packets, network, and node management. The advantages of the method can be expressed to encourage the cooperation nodes and punish the misbehavior nodes, the network tolerability against misbehaving nodes such as ending battery life, disconnecting malicious nodes, not to reduce the reputation of a node by malicious nodes, and to resistant DOS attack. The disadvantages of the methods can be precised to be slow in detecting the selfish nodes, be incapable of spoofing attack, and avoid the distribution of the negative reputations against the nodes collision.

A punishment- and reputation-based approach called SORI (secure and objective reputation-based incentive scheme for ad hoc networks) detects selfish nodes in the network [36]. This approach stimulates the network nodes to forward the packets to the other nodes. This approach used three monitoring packets: the neighborhood, the release reputation, and the punishment packets. The approach involves the monitoring component, which acts as the watchdog node mechanism. Whenever a node wants to properly execute one of the network's tasks monitored by its neighboring nodes, it calls for this mechanism. The reputation component is another component that determines the reliability of each network node in terms of the information that it receives from the monitoring component. The advantages of this approach are practical calculations of this method compared to other methods and low communication overhead. The disadvantages of this approach are the lack of distinction between malicious and selfish nodes, lower efficiency, higher energy consumption, no privacy policy, and unreliable channel.

A punishment-based approach is proposed to detect selfish nodes and stimulate them to cooperate with the network [37]. The primary responsibility of the nodes in the approach is to send messages, monitor, and report. The encouragements and punishments considered in this approach for nodes make them cooperate. This approach involves three steps, collaborating on selecting, sending data, and monitoring the neighbor nodes. The method has clustered the nodes in VANET and used three watchdogs to monitor the nodes. The cluster head applies the modified extended Dempster–Shafer model to detect the selfish node using watchdogs. The advantages of this approach are increasing cooperation between nodes, increasing the percentage of selfish node detection, reducing the false alarm rate, and increasing the stability of the clusters. The disadvantages are reduced performance by increasing bandwidth, data packet overhead, and high power consumption.

Another punishment-based approach is proposed to detect selfish nodes and stimulate them to cooperate with the network [38]. The proposed method uses a control data packet to detect the selfish node. So that when the data packet is sent from the source node to the destination node when the data packet reaches the intermediate node as a selfish node, then the data packet will not be sent by this node. Due to not receiving the control packet from the destination node, the source node will retransmit the packet data, and the number of retransmissions will increase. If the number of retransmission packets exceeds the predetermined threshold, the network will have a selfish node. The self-node is detected by listening to the channel of other nodes.

4.3. Credit-Based Mechanism.

In credit- or virtual-based methods, the nodes that have a data packet to send are paying for their data packets, or the nodes trade them between themselves and sell them at a higher price after buying a packet. The advantages of the methods are included as reducing overhead (information and hardware), a high percentage of non-cooperative node detection, low traffic in the network to discover non-cooperative nodes, high scalability, high performance in most cases, credit-based methods, and lower energy consumption. The main disadvantages of these methods are the collision attack, nonvalidating, unreliable channels, and no punishment of the noncooperation nodes [39]. Table 2 shows more details of credit-based mechanisms.

The approach proposed to detect the selfish nodes in the network using Nuglets [40]. It is the combination of the packet purse model (PPM) and a packet trade model (PTM) by the credit-based approaches [36, 37]. It is assumed that an end-user independently controls each node. The PPM approach is based on payment for the sending packets by the source node and encourages the middle nodes to send the packets of other nodes. In the PTM approach, there is no need to pay for the cost of the packets, but each network node purchases the packet from the previous node and sells it to the next node at a higher cost. In this approach, the source node does not need to know the number of the middle nodes. A credit-based approach called SPRIT (simple, cheat-proof, credit-based system) is presented to detect selfish nodes in ad hoc networks [41]. In this approach, credits stimulate the nodes to cooperate with other nodes so that each node, when receiving a message, will store the message's receipt in the node's memory. There is a credit clearance service (CCS); the nodes report to the CCS by transferring receipts for each sent/received message. The advantages of this approach are no need for any tamper-proof hardware to detect fraud, the lower power consumption, and lack of overhead for monitoring the nodes, and the disadvantages of the approach are the existence of a collision attack, the overhead of the packets, and the complexity of calculating costs and payments.

Table 1: Comparison of the reputation- and punishment-based mechanism.

Features	Watchdog/path-rater [27]	OCEAN [28]	HEAD [31]	SDA [32]	Reputation-based method [34]	CORE [35]	SORI [36]	PPS [37]
Year	2000	2003	2007	2012	2022	2002	2004	2015
Type	Reputation-based					Punishment-based		
Layer	Data link/network	MAC/network	Network	Network	Network	Network	Network	Network
Observation	Local	Local	Local	Global	Global	Local	Global	Local
Detection	Selfish node/malicious	Selfish node	Selfish node/malicious	Selfish node/malicious	Selfish node	Selfish node	Selfish node	Selfish node
Second chance	Yes	No	Yes	No	No	No	No	No
Robustness against collusions	No	Yes	Yes	No	Yes	No	No	Yes
Overhead	$O(N^2)$	O(N)	O(N)	O(kN)	O(N)	O(N)	$O(N^2)$	O(N)
False positive rate	10%~40%	10%~60%	—	28%~37%	8%~12%	10%~30%	15%~65%	10%~40%
Reliable channel	No	No	No	Yes	No	No	No	No

Table 2: Comparison of the credit-based mechanisms.

Features	Nuglet	Sprit	MODSPRITE	Improved-Nuglet	Credit-based mod
Year	2001–2003	2003	2011	2015	2018
Design	Promiscuous/distributed	Promiscuous/distributed	Promiscuous/distributed	Promiscuous/standalone	Promiscuous/distributed
Layer	Data link/network	Network	Network	MAC/network	MAC/network
Observation	local	Global	Local	Local	Global/local
Detection	Selfish node/Malicious	Selfish node	Selfish node	Selfish node	Selfish node
Overhead	O(3N)≅O(N)	O(2N)≅O(N)	O(3N/2)≅O(N)	O(N/2)≅O(N)	O(N/m)≅O(N)
Second chance	Yes	No	No	No	Yes
Robustness against collusions	No	No	No	Yes	Yes
Routing overhead (bytes)	0.18–0.51	0.27~0.52	0.16~0.24	0.21~0.34	0.7~0.18
False positive rate	5%~25%	0%~40%	—	30%~45%	1%~5%
Reliable channel	No	No	No	No	No

The SPRITE approach has been improved, and a new credit-based approach, called MODSPRITE, cooperates with noncooperative nodes in the network [42]. In this approach, if a node receives a data packet, it will store its receipt and then communicate with the cluster head responsible for providing credit and charging it to the other cluster member nodes. The proposed approach reduces the breakpoint as if the credit service fails, the credit program will collapse completely, but the cluster heads have corrected this problem in the MODSPRITE approach. If the cluster head is in trouble, the problem will be solved by changing the cluster head from one node to another.

The new Nuglet approach combines PPM and PTM approaches to identifying selfish nodes in the network [43, 44]. In this approach, it is assumed that all network nodes have a steady amount of virtual currency. At first, the source node generates some virtual currency using the PPM approach in this approach. Then, the virtual currency generated in the form of a packet between nodes is traded with the help of the PTM approach until the content reaches zero. The advantage of this approach is detecting selfish nodes in the network and stimulating them to co-operate with other nodes by allocating virtual currency to them. The disadvantages of the method are high energy consumption, high overhead packets, and requiring more memory to store tables.

A credit-based method is proposed to detect selfish nodes in MANET [14]. The algorithm clustered the network nodes and selected the cluster head and watchdog nodes. The cluster head nodes control the network feature of cluster member nodes, such as traffic, delay, and throughput. However, the watchdog nodes monitor the nodes in the clusters and report the selfish nodes that are not forward the packets to the cluster head. When the cluster head finds abnormal behavior in the member nodes, it will call the watchdogs to monitor the nodes. The disadvantages of the method are high latency and communication overhead. However, the advantages of the credit-based strategy are high selfish node detection accuracy, false positive rate, and low average end-to-end delay.

4.4. Acknowledgment-Based Mechanism. The receiver node sends an acknowledgment message to ensure the sender node is in acknowledgment-based methods. In these methods, a node sends an acknowledgment message to the source node when it wants to forward the packet. If a source node does not receive an acknowledgment message, it is considered a misbehavior node.

Balakrishnan et al. have developed a TWOACK to detect selfish nodes in the network [26]. In this approach, send data first between the source and destination of the routing, and then a route between source and destination is created. Each intermediate node is sent a spatial message with a specific packet identifier to the previous node when they are on the route of the following two steps from the packet sender. This process continues until the destination node receives the packet. The S-TWOACK scheme is proposed to reduce the traffic congestion on the routing by sending an acknowledgment message to modify and improve the TWOACK method [45].

The S-TWOACK scheme waits until a certain number of the data packets after receiving the first packet. Then, it sends one TWOACK message, which contains the number of the received data packet.

In order to improve the TWOACK approach, Liu et al. presented a new acknowledgment-based approach called 2ACK for detecting selfish nodes in the network [46]. In this approach, to maintain the integrity of packets against fake attacks, the authentication of 2ACK packets is done by a one-way chain process. In this scheme, they use step-by-step or end-to-end acknowledgment; when the destination node does not generate the acknowledgment message to the source node or is discarded by one of the intermediate nodes, it can be interpreted as a selfish node. The routing overhead of the proposed approach is low. The advantage of the 2ACK method is detecting intrusive communication, and the disadvantage is traffic congestion and high communication overhead.

The AACK method is acknowledgment-based in the network layer that combines the TWOACK method and end-to-end acknowledgment method based on the DSR routing protocol [47]. The proposed method has two modes, AACK and TACK, that use a bit to determine it; in the TACK mode, the acknowledgment message is sent to the nodes in the two steps, but in AACK mode, only the end-to-end acknowledgment message is sent that the packet has dropped the packet. The proposed method reports misbehavior links more than a misbehavior node. If the misbehavior link exceeds the threshold, it will be reported as a misbehaving link. It should be noted that the threshold varies according to the amount of data; in this method, punishment and isolation of the offending nodes are not used, but the data packets are sent from other routes. That is the main reason for detecting malicious nodes, but selfish nodes that only send their data packets are not identified, which is one of the disadvantages of the proposed method. However, the main advantages of the AACK approach are to solve the problems of the watchdog and increase the network throughput of the TWOACK method by reducing the routing overhead and maintaining better performance.

The EAACK method consists of three primary partitions: ACK, S-ACK, and MRA malicious authentication [48]. It is an end-to-end acknowledgment model. It acts as part of a hybrid scheme at EAACK that aims to reduce network overhead where no misbehaving has been detected in the network. S-ACK is an improved version of the TWOACK scheme, with all three consecutive nodes in a group working to identify misbehaving nodes. The third node must send an acknowledgment S-ACK packet to the first node for all three consecutive nodes on the path. However, unlike the TWOACK model, the source node does not immediately rely on a misbehaving report and needs to change its MRA state and approve misbehavior reporting. It is a crucial step in identifying misbehaving reporting. The core of the MRA model is to confirm whether the destination node receives the lost packet's report through a different path. Each of the three EAACK sections uses a digitally signed digital signature and retrieves the message. The proposed method can detect a collision attack and has high performance. Moreover, the disadvantage of this method's overhead is the high percentage of misbehaving nodes.

In 2018, Bounouni proposed an acknowledgment-based method to discover malicious and selfish nodes [49]. The proposed approach consists of four models for punishing malicious nodes and stimulating selfish nodes to cooperate with other nodes. The monitoring model is responsible for controlling the sending of routing packets and data packets by the acknowledgment packet in the network. The reputation model evaluates each node's neighbors by sharing the nodes' reputation, and according to the rules of trust, for this purpose, three types of direct, indirect, and general reputation are defined and fulfilled. The stimulator model manages and updates nodes' credit accounts; this module is intended to stimulate nodes by cooperating to send routing and data packets. They can increase their credit account balance and improve their reputation among neighboring nodes. Finally, the isolator model punished malicious and selfish nodes whose reputation is lower than the threshold. The advantages of this method are the high efficiency of the method compared to existing methods and a high percentage of detection of selfish and malicious nodes. The proposed method has a high overhead and cannot detect collision attacks and selective forwarding misbehavior. In the following, Table 3 compares acknowledgment-based methods in different metrics.

4.5. Game-Theory-Based Mechanism. Game theory is an applied mathematical theory; it models and analyzes systems in which each person tries to find the best strategy that others have chosen to find success [50]. It is primarily used in economics to model competition between companies. In wireless networks, the game theory may be used as a tool for building a partnership between institutions such as nodes, terminals, or network providers. Over the past years, game theory has also been used in network applications. In most cases, to solve the routing and allocation of resources, problems were introduced in a competitive environment and recently applied in wireless communications: logical users or network operators are decision-makers in the game that control the communication devices themselves.

The game consists of a principle and a finite set of players $N = \{1, 2, \ldots, n\}$. Each of them chooses a si ∈ Si strategy to

Table 3: Comparison of the acknowledgment-based mechanisms.

Features	TWOACK	S-TWOACK	2ACK	AACK	EAACK	Acknowledgment-based method
Year	2005	2005	2007	2009	2013	2018
Design	Distributed	Distributed	Distributed	Distributed	Distributed	Distributed
Layer	Network	Network	Network	Network	Network	Network
Observation	Local/active	Local/active	Local/active	Local/active	Local/active	Local/active
Detection	Selfish node	Selfish node	Selfish node	Malicious node	Malicious and selfish node	Malicious and selfish node
Overhead	$O(n^n)$	$O(n^s)$	$O(n^2)$	$O(n^{n/2}) + O(m)$	$O(n^{n/s}) + O(n^s)$	$O(n)$
Second chance	No	No	No	No	No	Yes
Robustness against collusions	No	No	No	No	Yes	No
Routing overhead (bytes)	0.18–0.52	0.15–0.24	0.11–0.19	0.18–0.51	0.23–0.68	0.02–023
False positive rate	10%–18%	8%–15%	1%–20%	5%–15%	4%–8%	2%–5%
Reliable channel	Yes	Yes	No	No	Yes	No

improve the utility function Ui (s): $S \longrightarrow R$ that denotes the sensitivity of each player to everyone's actions.

Cooperation/noncooperation: noncooperative games compete between players of a complete type, and the participants are entirely confronted. However, the union games are games in which several contributors unite against each other; in such games, the set of strategies for each group of players have formed a coalition with each other in Cooperation/non-cooperation games. It comes from a set of strategies for players participating in that coalition.

Dynamic/static: if one of the players first performs their actions and then the other player chooses to act with the knowledge of the first player's action, the game is dynamic, but if both players decide on their move without knowing the competing opponent's action, the game is static.

Repeated/one interaction: in game theory, a repeated game is an extensive form game consisting of several repetitions of some base game (called a stage game).

Finite/infinite: review repeated games and investigate outcomes and behaviors that lead to a strategic interaction between the players' long-term interests. There are two essential points in these games: the finite or infinite number of repetitions of the game. The players are not aware about other players game in the previous stages. In other words, the previous record of players participating in the game is available to others. If the number of repeated games is predefined and finite, the repeated game will be finite. However, if the number of repetitions tends to be infinitely more or too large, a repeated game will be infinite.

N-person/two-person: two-person games are played between two players, each seeking to earn the most out of the game. However, in *N*-person games, there are more than two players in the game. The players make their decisions independently, and each one unilaterally leads to a minimum loss of profit; depending on the ratio options, other players will behave wisely and cleverly.

An approach based on a dynamic auction framework, noncooperative, and finite-repetition game theory is presented to detect selfish nodes and stimulate them to cooperate with other nodes in the network [51]. The pricing-based mechanism used in this approach is auctioning the second-lowest price in the network security framework. In the approach, the source node is trying to find a route with the lowest cost to send packets and, at auction, uses the second-lowest payment bid because if the first lowest bid is used, it may lead to the collusion of selfish nodes. The advantages of this approach are the high accuracy of selfish node detection and high performance. Its disadvantages are high routing overhead and, in parallel, low efficiency on a large scale.

Pandana et al. presented an approach based on game theory and an infinite repeated-game framework to detect selfish nodes in the network [52]. This approach consists of two steps called nodes to maintain the cooperation stage, which means that node operation is monitored, and if they do not cooperate, they will be punished. Moreover, the learning stage is formed by choosing the best node for the packet forwarding. By updating the probabilities of selecting the next node and assuming the total monitoring of nodes by all and local observations is assumed for each step of the two modes. In this approach, using an infinite repeated game has led to the high stimulation of selfish nodes for cooperation with other nodes. The proposed approach is also distributional, and all nodes are involved in decision-making. This approach is used in the DSR routing algorithm, which has a high data overhead in large-scale networks due to adding the route to the packets. In addition, this approach has a low scalability feature.

Zhang et al. proposed a game-based approach to detect selfish wireless stations in a wireless cooperative relaying network [53]. The game used in this approach for wireless stations and access points is bargaining between two persons. The proposed strategy uses a Nash bargaining solution to satisfy the four axioms of invariance, efficiency, independence of irrelevant alternatives, and symmetry. Also, in this game, the value of each player's utility function effect the other players' decision to act. In this approach, the stations closer to the access point have better bandwidth, and there is a provision for fairly distributed bandwidth between stations. Moreover, the selfish nodes cannot use network resources for their utility and fair sharing of resources between the stations. This approach is unsuitable for unstructured wireless networks (without an access point) and limited resources.

Niu et al. have developed a game-theory-based and infinite repeated game approach to detect selfish nodes and stimulate them to cooperate with other nodes in the network [54]. The game's purpose in this approach is to allocate the least payoffs to the offending players to absolute fairness. The punishment mechanism based on the worst behavior tit-for-tat incentive strategy has been used to stimulate selfish nodes to cooperate with other nodes. In this approach, the complex Gaussian distribution for the possibility of correctly receiving a packet from the base station (BS) to the nodes and modeled the game to compute the Nash equation. The algorithm is implemented with imperfect monitoring, in which each node is monitoring other neighbor nodes so that the algorithm is first divided into smaller intervals. Then the behavior of the nodes is analyzed in each interval. Network nodes select their power of data forwarding at the beginning of each step, and at the end of each step, they also exchange the level of their behavioral indicator. The disadvantages of the approach are the selfish nodes do not gain less payoff if they follow the deviation from the Nash equation and low performance in high confusion environments. The proposed method has a high percentage of selfish nodes detection and stimulates them to cooperate.

A game-theory-based approach is presented to detect and punish the selfish nodes in the network [55]. In the game used by this approach, which is a two-player game, it is assumed that each node can generate its public and private encryption key. It is also assumed that each cooperation node must send the acknowledgment packet to the sender of the data packet unless the node is not the cooperation node and is a selfish node. Each node also stores previous actions of its neighbors in its memory, which will prevent the punishment of the other nodes. In detecting selfish nodes, if the intermediate node does not receive the acknowledgment packet from the next node, it considers the next node as a selfish node. In this approach, the infinitely repeated prisoner's dilemma for modeling the packet between two nodes and the punishment mechanism based on the worst behavior tit-for-tat incentive strategy has been used to stimulate selfish nodes to cooperate with other nodes. When high energy nodes, this approach is an efficient method for detecting and punishing the selfish nodes. Also, the proposed approach is not appropriate for large-scale networks and more selfish nodes. High energy consumption, low scalability, and the need for more memory are the disadvantages of this approach.

The proposed game-theory-based method for optimizing network coverage in wireless sensor network that suffers from selfish nodes mainly tries to improve network coverage by identifying and solving selfish behavior [56]. The node acts randomly to network cover in the proposed method and identifies its neighboring nodes. In the following steps, the node determines the best mode for the duration of sleep, but selfish nodes tend to sleep for a long time. Hence, the proposed method, with the implementation of repeated games and increasing their payoffs, tends to stimulate these nodes to cooperate with other nodes. If the node is known as the selfish node and its reputation is less than the predefined threshold and the nodes send a message, it will be informed to the others to prevent cooperation with the node. The proposed method has high efficiency in coverage. The existence of the collusion attack and selective forwarding misbehavior are the disadvantages of the proposed method.

A dynamic and self-learning repeated game was proposed to improve transmission efficiency by considering the noncooperative network nodes [47]. In this approach, the entire ad hoc network is assumed to be a directed graph. Each node's goal is to maximize its transmission efficiency and minimize energy consumption. In this approach, each node has two decision-making stages: the first decision to send its packet, and the subsequent decision is to forward the packets to other nodes. Given the infinite repeated game theory, the precision of detection of noncooperative nodes in the proposed approach is very high. Also, the approach presented with noncooperative nodes in a network with an average number of nodes has high efficiency in packet transmissions. High latency and low performance in high confusion environments are considered the disadvantages of the approach [57].

An approach based on game theory, infinite repeated, and static game on how to identify noncooperative nodes was done [58]. In the two-player game used in this approach, in which two players are two neighboring nodes, it is assumed that both neighbors in the network can send data packets to each other, and on the other hand, the relationship between them is two-way. In addition to the individual players' payoffs, the game's payoff is expected. The proposed approach game is an infinitely repeated game, where nodes that do not advance the data packets for the other nodes are punished by them and isolated from the network. In this approach, network nodes first create a neighboring table for their neighboring nodes. Then, according to the neighborhood table, the possible routes are selected by the sender of the packet data to the destination node. Each route's cost will be declared after calculating to the source node. When the route is set, if the number of selfish behaviors of the node is more significant than a predetermined threshold, then that node is known as a selfish node and sent to all members of the network nodes with a broadcast message. Eventually, the route is selected with the lowest cost after routing, and the data packets are sent to the destination node through that route. The main goal of this approach is to detect the selfish nodes and send the packets through the least costly route to reduce the cost of sending the data packets in the network. Unable to detect the sending of the data packets from one node to another and send an acknowledgment packet from the destination are the disadvantages of this approach.

The proposed scheme is a selfish node detection and prevention method called SENDER [59]. The scheme consists of two steps: the detection and prevention phase. An adaptive threshold algorithm has been used to identify all nodes in the detection phase. Selfish behavior is avoided in the prevention phase based on a repeated game. The number of forwarded packets should be compared between current and expected behavior to identify selfish behavior, consisting of three steps. Initially, the threshold value is set to the previous values. Next, the packet forward ratio (PFR) is calculated. Finally, the comparative threshold algorithm is used to compare with a threshold value to determine whether the current node shows selfish behavior or not. If the PFR is lower than the threshold value, the node is selfish, raising the alarm. Otherwise, the threshold value will be updated following the current PFR and the new threshold value for the next interval. The proposed method uses repeated games to prevent selfish behavior in the prevention phase. The game with payments is designed so that nodes gain fewer payoffs if they choose the selfish strategy; hence, they are unwilling to choose it. If some nodes sometimes choose the selfish strategy, they will choose a regular strategy after a certain period due to reduced payoffs. Therefore, in the prevention phase, selfish behavior can be prevented by choosing a regular strategy.

The approach presented a game-theory-based approach, which uses a limited credit to detect malicious and selfish nodes in the network [60]. In this approach, when the credit of a node is less than a predetermined threshold, the node is known as a selfish node, and it is sent a broadcast message. When the node's credit is less than the predefined threshold in a selfish node, the node is known as a malicious node and is notified to all nodes in the network. The game theory is used to decide the behavior of selfish nodes and identify them in the network, and selfish nodes are discarded from the network. The advantages of this approach are low end-to-end delay, a low number of packets lost, and high detection accuracy of selfish nodes. However, due to the high number of messages sent to the network, this approach also increases energy consumption. As a result, noncooperative nodes are less punished. Less stringency has been done about this problem.

A game-theory-based approach has been developed to detect selfish wireless stations in multirate wireless networks [61]. The game used in this approach is to associate users of wireless stations to prevent heterogeneous and poor performance based on joint resource allocation and association of wireless stations. The payoff of wireless stations is based on the individual power of each station. The proposed method is extensive use of Nash bargaining, and some of the user-specific properties allow players to incentive their motivation. The method performs better than similar methods for heterogeneous wireless stations and reduces the adverse effects of media access control abnormalities. The proposed mechanism can add a virtual layer for better performance in controlling access to the user's media. Although the proposed method is proposed to control the association of users, it is also capable of controlling selfish stations and stimulating them to cooperate.

Vijayakumaran et al. proposed a novel detection of the selfish node, consisting of "generation phase" and "verification phase" [62]. The generation phase also includes the routing task confirmation step, routing-report generation step, and coordination-confirmation report generation step. The routing task confirmation step will run when the source node is routed to the destination node. The middle relay node assigns a new routing task to the new node. This assignment confirmation should be created for it, which is assumed by the hash function as a signature function by the supervisor in the verification phase. However, in the step of routing-report generation, in the process of sending packets, a relay node will generate a routing report to indicate that it successfully forwards the packet from the upstream nodes to the destination node. In the coordination-confirmation report generation step, a new synchronization confirmation report is generated whenever two nodes are in the transmission range of each other, and the synchronization confirms these nodes in a communication session. The session nodes must generate signatures using a hash function to authenticate each other. In the confirmation phase, the supervising agent will approve the request to the middle relay nodes, and all nodes in the cluster will send the report to the supervising agent. From the collected information, the supervising agent can detect the noncooperation nodes.

A mechanism is proposed by Nobahary to discover selfish nodes based on game theory. The proposed method has three phases: a clustered network, sending data and playing a multiperson game, and update and stimulating noncooperative nodes [63]. The first phase is performed to set up the IoT nodes with a clustered network. Moreover, the nodes work together in phase two to deliver the packets to the destination. For this purpose, the nodes play a hierarchical repeated game and infinite game in the second phase while moving and forwarding their data packets or neighboring nodes. In the third phase, the node monitors the performance of its neighbor nodes. The nodes determine noncooperation nodes that have sent the packets by delay or have not sent data packets. The cooperation process analysis identifies noncooperation nodes and updates the reputation table. Encourage these noncooperation nodes to cooperate by punishing and not cooperating with them and reducing their reputation among other nodes.

Table 4 shows the comparison of the different methods using game theory. The table compares noncooperation nodes detection method in (dynamic, static), (cooperation, noncooperation), (n-person, two-person), (infinite, finite), (pricing-based, reputation-based) games.

4.6. Fuzzy-Logic-Based Mechanism. Another mathematical model representing uncertainty problems in life is the fuzzy logic system. Zadeh proposes to model the problems [64]. The system has input and output and membership functions. The natural range of the input and output values is mapped in different domains using the member function. The level of mapped value is one of the "high," "medium," and "low." domain ranges. The roles have shown the relation between inputs and outputs in the mapped domain.

Table 4: Comparison of game-theory-based mechanisms.

Ref	Year	Cooperative	Noncooperative	Repeated	infinite	finite	Two-person	*N*-person	Static	Dynamic	Reputation-based	Pricing-based	Throughput	Scalability	traffic	overhead
[60]	2019	—	✓	✓	✓	—	—	✓	—	✓	✓	—	91%	1~10CBR	—	
[59]	2017	—	✓	✓	✓	—	✓	—	—	✓	✓	—	—	—	—	—
[58]	2017	✓	—	✓	—	✓	✓	—	—	✓	—	✓	91%	5	1/ 2CBR	O(2^w)
[57]	2016	—	✓	✓	✓	—	—	✓	✓	—	✓	—	95%	45	2CBR	✓
[56]	2015	✓	—	✓	✓	—	—	✓	—	—	✓	✓	—	80%	20	—
[55]	2015	—	✓	✓	✓	—	✓	—	✓	—	—	✓	—	—	—	✓
[54]	2014	—	✓	✓	✓	—	✓	—	✓	—	✓	—	—	—	—	—
[53]	2013	✓	—	✓	✓	—	—	✓	—	✓	✓	—	91%	81	2CBR	—
[52]	2013	—	✓	✓	—	✓	✓	—	—	✓	✓	—	—	—	—	—
[51]	2011	✓	—	✓	✓	—	✓	—	—	✓	✓	—	94%	100	1CBR	
[50]	2011	✓	—	✓	✓	—	✓	—	✓	—	✓	—	84%	100	2CBR	✓
[49]	2008	—	✓	✓	—	✓	✓	—	✓	—	—	✓	49%	600	1CBR	✓
[48]	2008	✓	—	✓	✓	—	—	✓	—	✓	✓	—	80%	9–81	1CBR	
[47]	2008	✓	—	✓	✓	—	—	✓	—	✓	—	✓	34%	10–30	8CBR	✓

A new selfish node detection of accurate energy consumption mechanism has been proposed using fuzzy logic in MANET [15]. In the scheme, the node's trust level is determined by the percentage of packets dropped, and it is treated as a fuzzy input variable. The method uses direct trust for each node, and this direct trust is calculated by monitoring nodes, and neighbor nodes calculate indirect trust. The direct and indirect trust are sent to fuzzy logic to decide the cooperation and selfish node. It means the fuzzy logic output is the trust level of a node. If its level is lower than a predefined threshold, it will be tagged as a selfish node. The mechanism has high detection accuracy but a low packet delivery rate and throughput in MANET.

The system has been proposed to distinguish noncooperative behavior by intrusion detection system with fuzzy logic in MANET [65]. The mechanism can detect attacks, such as black hole attacks and gray hole attacks. The mechanism can prevent attacks and isolate the noncooperation node. The fuzzy logic system in the proposed mechanism is based on the number of packets dropped, which is an indifferent range. The number of packets dropped has shown the type of attack in a particular node and defined different thresholds to identify the attacks. The value of threshold and number of packets dropped are set in a matrix as fuzzy system input and estimated and member function in the fuzzy system using trapezoidal membership method. The output of the fuzzy system is sent to the IPS mechanism. IPS mechanism determines the misbehavior node and changes the packet's route to provide a secure route. Its advantage is the higher packet delivery rate. However, it has lower throughput in some attacks.

In the proposed approach, considering the concept of fuzzy logic related to trust, the problem of noncooperative behavior is investigated between nodes in the network [66]. The fuzzy-based analysis identified and identified and isolated noncooperative behavior as selfish and trusted nodes to identify and isolate noncooperative nodes. Fuzzy logic is composed of if-then rules. Fuzzy-based logic is a multiple-valued logic, and the actual values range from false (0) to (1) true. When identifying a problematic element, whether it belongs to one set or another, fuzzy logic is the best option for decision-making. The system output in fuzzy logic depends on if-then rules. In the proposed method, each network node continuously monitors its neighbors for its actions. Each node calculates the trust of the neighbors observed. These trust values are passed to an undefined function mapped to different classes, and the result classes represent the trust level of the observed nodes. Based on calculating the trust value, the estimated trust value is compared with the defined threshold value. If the particular trust is less than the threshold, then that node must be selfish, and the noncooperative nodes identified will be set aside from the active path in the network. The fuzzy-based proposed method is strong enough to detect the release of packets in the network. The unique feature of the proposed method is only the first-hand information used to calculate the trust value, and seven floors are defined for maximum tolerance. The advantages of the fuzzy-based method are the high detection accuracy of the selfish nodes and high efficiency, and less delivery of the data packets.

A new fuzzy-based method is designed by Javidi and Baseri to provide secure routing and detect selfish nodes [67]. The selfish node detection ad hoc on-demand distance vector routing protocol is designed based on fuzzy logic and parameters of the number of the input control packet, number of the input data packet, number of the output control packet, and number of the output data packet as alpha and energy-level of nodes are inputs in the fuzzy system. The trust value of the nodes is the output of the fuzzy system. Energy-level has reverse relation with trust value, but alpha directly relates to it. FSDAODV protocol has a high packet delivery rate and performance by detecting selfish nodes, but it has high energy consumption.

A fuzzy-based method is proposed to detect the selfish node by Hasani and Babaie [68]. The technique used three metrics the node's energy, the count of hops to the destination, and the history of the node in cooperation or selfishness in the ad hoc network. The fuzzy logic system applied the metrics as input to calculate the degree of nodes' cooperation. The nodes cooperated in the past; then, it has more probability of cooperating in the next round of the network operation. The fuzzy logic system is applied to the MAX–MIN function to extract output rules. The novel method can calculate the hop count to the destination node, and also, other metrics are sent as input to a fuzzy system, and rules can evaluate the nodes' statuses. The method's advantages are the high detection accuracy, low latency, and delivery cost. But high computational overhead is the disadvantage of the technique.

The mechanism is proposed to secure routing and prevent selfish node damage in the network [69]. OLSR fuzzy cost (OLSR–FC) is designed based on a fuzzy system, and it is an extension of the OLSR protocol to provide security. The residual energy, connectivity, and IPP inputs for the fuzzy logic system. The cost function is the fuzzy system output to detect selfish nodes. The neighbor nodes are calculated the cost function about the particular node, and the average vote about it will be decided about the selfish and cooperation statues. The method has low jitter, but communication overhead is high.

The method has been proposed to detect selfish nodes in the IoT environment [70]. It consists of three phases: in the first phase, the nodes have clustered and the cluster heads were selected using the Harris hawk algorithm. In the second phase, the base station has considered the general network parameters such as dropped packets and residual energy of nodes. Moreover, it can detect the selfish nodes in the network; if the base station detected the selfish node, it would be informed the cluster heads to control the member nodes in each cluster. In the last phase, the fuzzy logic has calculated the reputation of nodes, and the cluster head in each cluster decides on the status of the member nodes as selfish or cooperation nodes. They have combined fuzzy logic idea and base station idea about the cooperation of the nodes. The method's advantages are the high detection accuracy and low false-negative rate. However, it has a high computational and communication overhead.

4.7. Hybrid and Specification Mechanism. In hybrid methods, the methods use credit-based or reputation-based, or other groups of methods to benefit the hybrid methods. Therefore, these methods have advantages such as high efficiency of the methods more than 85%, and the quick discovery of noncooperative nodes is a feature of these methods. Low traffic on the network to discover noncooperative nodes, low overhead (hardware, time, information) and resistance to the collision attack, and node collusion, but there are disadvantages such as low scalability, nonvalidation, unreliable channels, and high energy consumption. Table 5 shows the different metrics in hybrid mechanisms.

The approach proposed in [16] for fair cooperation of nodes is reputation-based in MANET. In this approach, a node is used as a credit manager called CONFIDANT, responsible for maintaining the credibility of watchdog nodes and path-rater. The protocol uses four packages: monitoring system, repeat system, trust management, and route manager. The advantages of this approach are direct and indirect monitoring of the neighboring node, the lack of predefined service packets (punishment of the nodes) for noncooperative and low-reputed nodes as selfish nodes, and reduced packet traffic in the network fails to send packets from incorrect paths. The disadvantages of this approach are unauthorized nodes, lack of eavesdropping, high energy consumption, and ignoring the nodes in the black-list that are considered selfish nodes, and there is also no central decision-maker for a node. There are conflicting evaluations of a node.

A hybrid approach called hybrId inCentive mechAnism for coopeRation stimUlationS (ICARUS) is proposed to improve the distribution of unfair credit between nodes far from the base station using a credit estimate to control the exchange of credit between nodes [72]. This proposed mechanism extends DARWIN based on the reputation-based method [71]. This credit-based method of punishing the noncooperation nodes after detecting the selfish nodes stimulates the nodes' motive to forward the packets to the other nodes. This method guarantees the fairness of credit for the nodes far from the base station and the other nodes and prevents false negative judgments of the selfish nodes against inaccurate and false data. This method detects the selfish nodes much faster and isolates them in the network. Considering that the node is far from the base station and is less likely to participate in forwarding the other node's packets, they will have less credit that will not be fair, but the proposed method focuses on this problem. The advantages of credit-based approaches are also used in the proposed approach, in addition to the advantages of the DARWIN approach.

The authors proposed an efficient replica allocation to detect partial selfishness in the network, and the novel can help the replica allocation technique deal with partial selfishness [17, 73–76]. The selfish node may not share its memory space and store the replica to benefit other nodes. The method develops the secure replica allocation by the hill cipher algorithm. Each node calculates a credit risk value for the neighbor and connected nodes in the algorithm, and each node will construct an SCF tree. When the nodes update the tree by asking the connected node replica allocation, if the selfish nodes refuse to cooperate, they will be eliminated in the SCF tree and smoothed out the tree based on graph theory. The method advantages significantly reduce the cost of communications, and the time of detecting and eliminating the selfish node is fast.

An incentive detection mechanism for cooperation and stimulation of the selfish is proposed [77]. This mechanism consists of two modules: the detection module is based on the retransmission numbers punishment module. During the detection module, a real-time statistic will be computed by each node for the number of retransmission and the renumbering records in a particular period. Finally, the nodes will compute the average retransmission packets for each node. If the condition is satisfactory, it will indicate that the node is selfish; otherwise, it is normal. In implementing the entire network, if the node is identified as a selfish node, the next time, using the punishment module gives incentives to work with neighboring nodes. The punishment module is that the contention window will increase the selfish node for giving incentives, in which case the neighboring nodes of the channel's resources compete.

The QoS-OLSR method was proposed by Sondi et al. to provide a quality of service routing protocol and counteract misbehaving nodes [78]. In this method, clustering is used for better monitoring and selecting watchdog nodes. A node with a higher reputation score is selected as a cluster head in a short period in the cluster to collect the data packets. The data packets sent by the source are stored in a table by the intermediate nodes. Each intermediate node sends the data and compares the watchdog node with the data in the table, and if it is not identical, it is known as a suspect node. By changing several watchdog nodes, data aggregation should be performed on the status of the suspicious nodes, which has done this with the Dempster–Shafer relationship to identify the selfishness or cooperation node and noticed by other cluster member nodes.

Chakrabarti and Roy presented an automated mechanism for detecting and avoiding malicious nodes during the data communication process [79]. The reputation of nodes is estimated based on cooperation with other nodes to identify malicious nodes in the network. In this mechanism, an observational dynamic estimation method is proposed for identifying selfish nodes in which a group of independent monitoring nodes is assigned to monitor the behavior of the nodes as transmitters and receivers. The scheme suggests that after a complete and successful exchange of data packets between nodes, the reputation among them is exchanged to confirm good cooperation between the nodes. A node holds two lists: forwarder trust token and receiver trust token. The node counts the number of these lists of forwarders collected and calculates its cooperation coefficient list. Each node periodically distributes its cooperation coefficient list to nearby nodes. During updating the matrices, nodes can modify behavior that observers apply based on the behavior of the nodes in the matrix of its overall reputation. The reputation matrix of the entire grid is then published by observers in the relevant monitoring area so that local nodes

Table 5: Comparison of hybrid and specification mechanisms.

Observation	Local	Local	Global	Local	Local	Local	Local	Global/ active	Local	Local/ active	Local/ active	Local	Local/ active	Global/active	Global/ active	Global/ active	Local/active
Detection	Selfish node	Selfish node/	Selfish node	Selfish node	Selfish node	Selfish node	Selfish/ malicious	Selfish node	Selfish node	Selfish node	Selfish/ malicious	Selfish/ malicious	Selfish/ malicious	Selfish/ malicious	Selfish node	Selfish node	Selfish node
Overhead	O(N)	O(N^2)	O(N)	O(log(n))	O(N)	O(N^2)	O(N)	O(N^2)	O(N)	O(N/m)	O(N)	O(N/m)	O(N)	O(N)	O(N)	O(N)	O(N)
Second chance	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No
Robustness Against collusions	No	No	Yes	No	Yes	No	No	No	No	Yes	No	Yes	No	Yes	No	Yes	Yes
Scalability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No	No	Yes
Packet delivery rate (PDR)	10%~91%	18%~97%	78%~98%	77%~97%	78%~83%	62%~81%	75%~98%	95%~99%	90%~92%	70%~98%	82%~96%	73%~91%	85%~92%	61%~91%	25%~45%	55%~75%	72%~100%
False positive rate	20%~60%	20%~40%	5%~20%	—	0%~4%	24%~ 47%	10%~17%	2%~21%	10%~25%	8%~15%	12%~23%	10%~ 24%	10%~30%	8%~11.2%	—	5%~12%	7%~23%
Design	Distributed	Distributed	Centralized	Distributed	Distributed	Clustered	Distributed	Distributed	Distributed	Centralized	Distributed	Clustered	Distributed	Distributed	Distributed	Distributed	Distributed
Year	2002	2007	2012	2012–2013	2013	2013	2014	2014	2015	2015	2016	2017	2017	2020	2020	2020	2021
Features	Confident [16]	DARWIN [71]	ICARUS [72]	Replica-methods [17, 73–76]	Two-phases methods [77]	QOS-OLSR [78]	Automated-methods [79]	RCM [80]	SDM [81]	Green-approach [82]	Smart-method [83]	CoCowa [84]	TEEM [18]	Conjectural based Framework [85]	reputation-based epidemic [86]	Token-Based [34]	RRR [87]

can use it for reliable selection. Suppose the node's reputation value is less than the threshold reputation. In that case, the node receives the alert message to improve its behavior by the observer nodes monitoring the misbehaving nodes.

A hybrid approach called reputation-based credit mechanism (RCM) is presented for detecting selfish nodes in the network [80]. This mechanism is based on reputation and credit approaches. In this approach, first, a game is arranged between neighboring nodes to forward the data packets. In the following, the Nash equation is calculated to give the optimal reward to the cooperation nodes and make a reasonable decision regarding noncooperative nodes. The middle nodes can maximize the gains of payoff. This mechanism comprises two models: payment model and cost model. This approach is a reputation-based credit approach. The balance is established between the efficiency of detecting selfish nodes and the efficiency of payment of credits and has been introduced as an indirect assessment method of local reputation. A noncooperative game mode is provided in the routing process to control the data packets' behavior in the source node and middle nodes. Also, the optimal reward allocation has been investigated from the source node and the fair burden-sharing on the network. Compared to popularity, reputation-based, and credit-based approaches, RCM has lower efficiency and lower payoff rate for the selfish nodes while a low percentage of selfish nodes in the network.

Selfish node detection and motivation (SDM) is a hybrid approach based on reputation, and acknowledgment-based methods have been proposed to detect selfish nodes and stimulate these nodes to forward the data packets' of the nodes in the network [81]. This approach consists of two phases: the detection phase and the motivation phase. In the first step, nodes have identified that they refuse to forward the data packets for various reasons, such as failure or the impact of external destructive factors, such as bad media connections. After detecting the selfish nodes, the selfish nodes are stimulated to cooperate with the other nodes to forward the data packets in the next step. Otherwise, they will not be served on the network. In this approach, the nodes involved in data packet transitions store their reputation with the *Ri* index for each node *i* in its memory in the detection phase. Suppose a node sends data packets. The destination node forwarded the acknowledgment packet before the timeout for each successful send. In that case, the reputation of that node's value increases by *a*, and for each failure in sending data packets, the node's reputation decreases by *b*. If the nodes' reputation is less than the predefined threshold, the node's packets will be dropped, and the node is known as the selfish node. The disadvantage of the method is traffic congestion and high communication overhead.

A hybrid approach has been developed in a green solution for selfish detection in wireless LAN [82]. This approach is based on overall network monitoring and consists of two phases: global and local. In the first phase, the network is considered for the existence or absence of selfish nodes, and in the next phase, selfish nodes in the network are identified if they exist. In this approach, the multiphase approach is also called. In the global phase, this approach collects global metrics of the network to detect selfish behavior and abnormalities behavior deviation from the normal state of the network.

The researchers proposed a novel solution for detecting smart misbehaviors based on threshold adaptive control in VANET [83]. In addition to identifying malicious nodes, the proposed method makes the attackers behave normally. The strategy uses direct and indirect trust to detect misbehavior nodes, while the nodes can define direct trust by interactions between neighbor nodes. The nodes define indirect trust by evaluating direct interactions between the two nodes and the other nodes' opinions about the cooperation of nodes. When the number of interactions increases, direct trust is more than indirect trust (based on recommendations) at acceptable levels of trust. The direct trust between the two nodes is calculated by the direct report generated by a node on another node. Indirect trust is calculated based on recommendations from neighbors of a node about other nodes. In order to avoid an impact on communication bandwidth, it is suggested that the message format is periodically changed by adding neighbor and sender identification. To overcome false judgment behavior, when a node detects that neighboring trust begins to decrease, it adjusts the detection threshold depending on this unwanted misbehavior. Hence, instead of using only one fixed threshold, the adaptive threshold is related to each neighbor depending on its behavior. The advantages of the proposed method are the high efficiency for both parameters of the detection accuracy and delivery of data packets. However, the false positive/negative rate of malicious nodes has increased.

The approach is based on a combination of trust deriving from the network, and the quality of service (QoS) is named as a collaborative contact-based watchdog (CoCoWa) for detecting selfish nodes [84]. In the proposed system, the network is distributed in clusters, and each cluster has a cluster head that monitors the nodes to forward and receive more data packets. The buffer level of all nodes is monitored to identify packet loss, and it is determined whether the node is malicious. This method combines the watchdog node with dissemination on the network. The primary goal of CoCoWa is to increase the detection accuracy and decrease the selfish node detection time in the network. The watchdog improvement protocol is proposed with some modifications to overcome the problem of the watchdog protocol. This improved watchdog protocol is beneficial for identifying the real reason for the loss of the packet. The security protocol does not identify the risks of network transmission. It only observes that whenever the packet sending time is greater than the closed time, it sends an alert in the system and displays the node as malicious. The advantages of this method are to increase network performance in the presence of selfish nodes, increase packet delivery rates, and reduce latency in the destination.

TEEM is a trust-based approach to detecting malicious and selfish nodes in mobile ad hoc and wireless sensor networks, which usually depends on the watchdog approach. However, such monitoring devices have more energy consumption [18]. TEEM is working by the time division of the monitoring strategy to achieve high-security levels. This method includes the trust and the link duration between the valid cooperation pairs relative to the diving period of the monitoring, which is entirely distributed by switching hello messages between the nodes. In TEEM, network nodes are commonly monitored from the beginning. Then, the trusted pairs distribute the network monitoring task and can save the energy supply of nodes.

This method proposes a reputation-based framework for the distributed system, which combines selfish and malicious node detection. The router vector is expanded on demand and uses an extensive deep packet scrutiny (EDPS) technique to detect suspicious activity from network nodes before packets are discarded. In order to classify selfish and malicious nodes, supervised learning methods are based on deep neural networks (DNN). The Vickrey, Clarke, and Groves (VCG) models are used to change the behavior of selfish nodes to cooperate and encrypt packets. The proposed method increases the advantages, such as the quality of service criteria. Network lifetime and network power are improved on average. Packet delay, packet delivery ratio, overhead, and reliability are also reduced with routing overhead and average end-to-end delay. Nodes that have acted as selfish nodes are given a second chance. The fundamental limitation of the proposed method is that no framework includes a direct or indirect reputation-based approach to identifying and defending malicious and selfish nodes [85].

A reputation-based epidemic algorithm has been proposed in this mechanism that combines selfish behavior and the inability to send a message. Conceptually, reputation should be considered to reflect the nodes' behavior and meet the parameter's performance requirements. However, many parameters are related to reputation calculation, such as data delivery rates, memory, delay, and bandwidth consumption, and they affect each other and require high computational capabilities. For the protocol, reputation is calculated using the successful message sent, representing all the factors indicating the message was sent successfully. The behavior of the candidate node is evaluated by monitoring the relay, and a reputation-based message mechanism is established for sending. When node *j* meets node *i* without a message, node *j* calculates the credit value of node *i*. A message is sent to node *i* for the relay if the threshold is exceeded. Nodes with a good reputation as candidate nodes for relay service are the priority of selection and service. In order to achieve routing service, selfish nodes must be honest and good at relaying messages to gain a good reputation. This mechanism stimulates everyone to cooperate in the relay message. In the beginning, since contact between nodes is not frequent, direct reputation may not be effective in showing overall reputation. When most nodes communicate with each other, the amount of reputation may reflect the truth to some extent. Finally, a selfish node is disconnected from the network when its reputation is below a predetermined threshold and stimulates all nodes to cooperate in posting to gain a higher reputation [86]. Susan et al. have introduced a method based on punishment and encouragement. A selfish node requires an incentive to send packets to other nodes because this is a required cost (energy and other resources). The encouragement mechanism ensures that node messages are not accepted by default, but the mechanism forces them to cooperate in sending their message. The system has applied signs in analysis to facilitate identifying and eliminating selfish nodes. Each node is created with a password that includes three fields: node ID, status, and reputation. Each node must declare its password status and reputation value to participate in any network activity. If the status and validity bits are "1" and "−1," the protocol does not allow any activity on the network. The isolated nodes' number has been reduced by introducing the sign field for tolerance, which is implemented because of the reduction of the isolation effect of the selfish node by placing the selfish node in the block list [34].

The credit-based reputation system, known as RRR, is an algorithm that combines reputation- and credit-based methods [87]. The proposed approach is presented to identify selfish and malicious nodes. The proposed system is a decentralized system that determines the reputation of each node and encourages cooperation. Routing in this method is reliable. The whole network is divided into regions based on their distance to the base station, where all nodes know their coordinates. The routing algorithm works with nodes with a higher reputation and credit and uses protection methods to limit membership in the routing and network.

This paper proposes to detect selfish nodes in IoT (DISOT) [88]. The method includes three phases: The setup and clustering phase identifies the neighbor nodes and then clusters all the nodes in the network. The global phase, which indicates whether a selfish node(s) exists in the clusters or not using the main cluster head and the cluster heads in each cluster, must identify the selfish node(s) within the local phase.

5. Open Issues

Today's world is using more and more networks such as IoT. They have high scalability; studying and providing methods to overcome scalability problems will be more beneficial. It is necessary to avoid methods dependent on the central system to have better scalability because the increase in traffic and high latency and communication overhead in the central system will ultimately reduce the efficiency of the network. Due to the high number of nodes in distributed systems, it is not easy to control these systems. However, taking advantage of the features of both distributed and centralized systems requires further research.

Comparisons of the various detection mechanisms are summarized in Tables 1–3. The results have also shown that various techniques are proposed to detect the noncooperation nodes, but some metrics still have an open issue. Detection rate is one of the metrics that should be worked on to improve it, and increasing the detection rate can increase throughput and packet delivery rate (PDR) and decrease end-to-end delay and latency. Other metrics are the false positive rate (FPR) and the false negative rate (FNR). The false positive rate indicates the ratio of the normal nodes number detected as a selfish node by error to the total number of normal nodes detected by mistake and the number of normally detected nodes in the network. FPR has the inverse relationship in the network, so its low level shows the accuracy of the approaches. The higher the number of cooperation nodes correctly detected, the higher the network performance; if the detection were mistaken, it would reduce the network efficiency and lower the data packets to the destination. FNR is also used to evaluate the efficiency of selfish node detection methods, which is the ratio of the number of the selfish nodes detected as the cooperation node by error to the total number of selfish nodes and normal nodes in the network. Both FNR and FPR are specific metrics to evaluate nodes' behavior, and they can influence network performance.

The concept of machine learning methods such as supervised methods or unsupervised methods can be expressed in network anomaly detection that a learner can classify events into natural events and anomalies. Theoretically, each machine learning method has its advantages and disadvantages that can be understood based on how these methods work. By overcoming the disadvantages of the methods, these tools can also be used to detect malicious and selfish nodes in the network. It can be said that the hybrid proposed methods used two or more methods as mentioned above. They have better network performance results, packet delivery rate, and other essential metrics. The reason is that hybrid methods profit several methods of advantages and have better results as evaluate other similar techniques. It can be used to provide hybrid methods for improving the standard parameters of the networks.

6. Conclusion

This paper presents a comprehensive review of cooperation in wireless networks consisting of WSN, MANET, VANET, and IoT, focusing on the mechanisms of detection and identification that have been proposed to address the issue of selfish/malicious nodes. Weaknesses and strengths of the selfish/malicious node detection approaches are discussed to adopt and motivate new strategies. Comparing different methods and strategies highlights the weaknesses of these methods and finding solutions to determine malicious or selfish nodes accurately. New approaches are expected to be considered more closely to measuring the false positive/negative rate, which is, in fact, unfair judgments about node behavior. This article evaluates some metrics that play an essential role in developing each mechanism for detection and stimulation. The proposed solutions still have a workplace for improvement and find ways to accurately explore the noncooperative nodes and stimulate these nodes to work with others. Given these challenges and the increasing use of wireless communication networks, the mechanisms for detecting malicious and selfish nodes in wireless communication networks still require extensive research and careful research studies that provide many opportunities for discoveries and innovations.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] L. Azari and A. Ghaffari, "Proposing a novel method based on network- coding for optimizing error recovery in wireless sensor networks," *Indian Journal of Science and Technology*, vol. 8, no. 9, pp. 859–867, 2015, þ.

[3] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *Proceedings of the 2013 International Conference on Machine Intelligence and Research Advancement*, IEEE, Katra, India, 21-23 December 2013.

[4] S. K. Mousavi and A. Ghaffari, S. Besharat and H. Afshari, Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 2033–2051, 2021, þ.

[5] G. Deverajan, "Public key encryption with equality test for Industrial Internet of Things system in cloud computing," *Transactions on Emerging Telecommunications Technologies*, Article ID e4202, 2021.

[6] A. J. Manuel, A. Deverajan, R. Patan, and A. H. Gandomi, "Optimization of routing-based clustering approaches in wireless sensor network: review and open research issues," *Electronics*, vol. 9, no. 10, p. 1630, 2020.

[7] S. Ghasemnezhad and A. Ghaffari, "Fuzzy logic based reliable and real-time routing protocol for mobile ad hoc networks," *Wireless Personal Communications*, vol. 98, no. 1, pp. 593–611, 2018, þ.

[8] L. Krishnasamy, R. Dhanaraj, D. Ganesh Gopal, T. Reddy Gadekallu, M. Aboudaif, and E. Abouel Nasr, "A heuristic angular clustering framework for secured statistical data aggregation in sensor networks," *Sensors*, vol. 20, no. 17, p. 4937, 2020.

[9] H. D. Nikokheslat and A. Ghaffari, "Protocol for controlling congestion in wireless sensor networks," *Wireless Personal Communications*, vol. 95, no. 3, pp. 3233–3251, 2017, þ.

[10] X. Jiang, "Challenges and opportunities of network virtualization over wireless mobile networks," *Mobile Information Systems*, vol. 2017, 2017.

[11] S. K. Mousavi and A. Ghaffari, S. Besharat and H. Afshari, Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515–1555, 2021, þ.

[12] A. Ghaffari and A. M. Rahmani, "Fault tolerant model for data dissemination in wireless sensor networks," in *Proceedings of the 2008 international symposium on information technology*, vol. 4, þ, Kuala Lumpur, Malaysia, 26-28 August 2008.

[13] J. Sengathir and R. Manoharan, "Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: a review," *Wireless Personal Communications*, vol. 97, no. 3, pp. 3427–3447, 2017.

[14] S. Nobahary and S. Babaie, "A credit-based method to selfish node detection in mobile ad-hoc network," *Applied Computer Systems*, vol. 23, no. 2, pp. 118–127, 2018.

[15] R. Vijayan, V. Mareeswari, and K. Ramakrishna, "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic," *International Journal of Research and Reviews in Computer Science*, vol. 2, no. 3, p. 647, 2011.

[16] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: fairness in

dynamic adhoc NeTworks)," *MobiHoc '02 Proc. 3rd ACM Int. Symp. Mob. ad hoc Netw. Comput.*, pp. 226–236, 2002.

[17] P. J. Kumar and P. Ilango, "An optimized replica allocation algorithm amidst of selfish nodes in MANET," *Wireless Personal Communications*, vol. 94, no. 4, pp. 2719–2738, 2017.

[18] A. Lupia, C. A. Kerrache, and F. De Rango, "Teem: trust-based energy-efficient distributed monitoring for mobile ad-hoc networks,"vol. 1, pp. 133–135, in *Proceedings of the 2017 Wireless Days*, vol. 1, pp. 133–135, IEEE, Porto, Portugal, 29-31 March 2017.

[19] J. Vijithanand and K. Sreerama Murthy, "A survey on finding selfish nodes in mobile ad hoc networks," *International Journal of Computer Science and Information Technologies*, vol. 36, pp. 5454–5461, 2012.

[20] S. A. G. A. R. Padiya, R. Pandit, and S. Patel, "Survey of innovated techniques to detect selfish nodes in MANET," *International Journal of Computer Networking, Wireless and Mobile Communications*, pp. 2250–1568, 2013, ISSN.

[21] N. Samian, Z. A. Zukarnain, W. K. G. Seah, A. Abdullah, and Z. M. Hanapi, "Cooperation stimulation mechanisms for wireless multihop networks: a survey," *Journal of Network and Computer Applications*, vol. 54, pp. 88–106, 2015.

[22] M. A. Al-Jaoufi, "Study on selfish node incentive mechanism with a forward game node in wireless sensor networks," *International Journal of Antennas and Propagation*, vol. 2017, 2017.

[23] S. Misra, "A survey on selfish node detection in mobile ad hoc network," *Gyancity Journal of Electronics and Computer Science*, vol. 3, no. No.2, pp. 28–31, 2018.

[24] Y. Zhang, "Detection and isolation of packet droppers in wireless ad-hoc networks," *Business*, 2011.

[25] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, pp. 153–181, 1986.

[26] K. Balakrishnan, J. D. J. Deng, and V. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," *IEEE Wirel. Commun. Netw. Conf.*vol. 4, no. C, pp. 0–5, 2005.

[27] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. 6th Annu. Int. Conf. Mob. Comput. Netw. MobiCom 00*, vol. 1, no. 18, pp. 255–265, 2000.

[28] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *Networking and Internet Architecture*, vol. 2003, p. 10, 2003.

[29] S. Senthilkumar and J. William, "A survey on reputation based selfish node detection techniques in mobile ad hoc network," *Journal of Theoretical and Applied Information Technology*, vol. 60, p. 2, 2014.

[30] I. Technology and I. Technology, "Survey of innovated techniques to detect selfish nodes in manet," *Quantitative Social Research*, vol. 3, no. 1, pp. 221–230, 2013.

[31] G. U. O. Guo, L. I. U. Liu, D. Dong, Y. Yang, and Head, "HEAD: a hybrid mechanism to enforce node cooperation in mobile ad hoc networks," *Tsinghua Science and Technology*, vol. 12, no. S1, pp. 202–207, 2007.

[32] O. León, J. Hernández-Serrano, and M. Soriano, "Outwitting smart selfish nodes in wireless mesh networks," *International Journal of Communication Systems*, vol. 23, no. 5, pp. 633–652, 2010.

[33] M. Fayaz, G. Mehmood, A. Khan, S. Abbas, M. Fayaz, and J. Gwak, "Counteracting selfish nodes using reputation based system in mobile ad hoc networks," *Electronics Journal*, pp. 1–22, 2022.

[34] K. Susan, C. Konyeha, A. M. John-Otumu, and E. S. Mughele, "An improved token-based umpiring technique for detecting and eliminating selfish nodes in mobile ad-hoc networks," *Egyptian Computer Science Journal*, pp. 1–12, 2020.

[35] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," *Advanced Communications and Multimedia Security*, vol. 100, 2002.

[36] He Qi, D. Wu, and P. Khosla, "SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks,"-vol. 2, pp. 825–830, in *Proceedings of the 2004 IEEE Wirel. Commun. Netw. Conf. (IEEE Cat. No.04TH8733)*, vol. 2, IEEE, Atlanta, GA, USA, 21-25 March 2004.

[37] A. Jesudoss, S. V. Kasmir Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme," *Ad Hoc Networks*, vol. 24, no. PA, pp. 250–263, 2015.

[38] S. K. Das, P. S. Chatterjee, and M. Roy, "Detecting and punishing the selfish node and its behavior in WSN," in *Proceedings of the IEEE 5th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, vol. 4, no. 2, pp. 11–15, Hefei, China, 2014.

[39] N. Samian, Z. A. Zukarnain, W. K. G. Seah, A. Abdullah, and Z. M. Hanapi, "Cooperation stimulation mechanisms for wireless multihop networks: a survey," *Journal of Network and Computer Applications*, vol. 54, pp. 88–106, 2015.

[40] L. Buttyan and J. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks 1 introduction," pp. 1–15, Technology, 2001.

[41] J. Chen and Y. R. Yang, "Sprite: a Simple, cheat-proof," *Credit-Based System for Mobile Ad-Hoc Networks*, vol. 00, no. C, pp. 1987–1997, 2003.

[42] R. Kaushik and J. Singhai, *MODSPIRITE: A Credit Based Solution to Enforce Node Cooperation in an Ad-hoc Network*, vol. 8, no. 3, pp. 295–302, 2011.

[43] G. Rizwana and G. Wasim, "Enhanced intrusion detection & prevention mechanism for selfishness in MANET," *Int. J. Innov. Res. Comput. Commun. Eng.*vol. 3, no. 10, pp. 10131–10138, 2015.

[44] C. Science and S. Engineering, "A comparative study of selfish node detection methods in manet," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 8, pp. 306–310, 2015.

[45] S. Senthilkumar and J. William, "A survey on reputation based selfish node detection techniques in mobile ad hoc network," in *Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, vol. 60, 2014.

[46] 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, pp. 536–550, 2007.

[47] T. S. A. Al-roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," *Regular Paper*, pp. 273–282, 2009.

[48] E. M. Shakshuki, S. Kang, N. Sheltami, and T. R. Sheltami, "EAACK-A secure intrusion-detection system for MANETs," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, 2013.

[49] M. Bounouni, "Acknowledgment-based punishment and stimulation scheme for mobile ad hoc network," *The Journal of Supercomputing*, 2018.

[50] T. Basar and G. Jan Olsder, *Dynamic Noncooperative Game Theory*, vol. 23, no. Siam, 1999.

[51] Z. Ji, W. Yu, and K. J. R. Liu, "A game theoretical framework for dynamic pricing-based routing in self-organized MANETs," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 7, pp. 1204–1217, 2008.

[52] C. Pandana, Z. Han, and K. J. R. Liu, "Cooperation enforcement and learning for optimizing packet forwarding in autonomous wireless networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 3150–3163, 2008.

[53] Z. Zhang, J. Shi, H. H. Chen, M. Guizani, and P. Qiu, "A cooperation strategy based on nash bargaining solution in cooperative relay networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2570–2577, 2008.

[54] B. Niu, H. V. Zhao, and H. Jiang, "A cooperation stimulation strategy in wireless multicast networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 5, pp. 2355–2369, 2011.

[55] D. Z. Tootaghaj, F. Farhat, M. R. Pakravan, and M. R. Aref, "Game-theoretic approach to mitigate packet dropping in wireless Ad-hoc networks," in *Proceedings of the 2011 IEEE Consum. Commun. Netw. Conf. CCNC'2011*, pp. 163–165, IEEE, 09-12 January 2011.

[56] I. Ben Abid and N. Boudriga, "Game theory for misbehaving detection in wireless sensor networks," in *Proceedings of the The International Conference on Information Networking 2013 (ICOIN)*, 28-30 January 2013.

[57] A. Velayudham, G. V. S. Gohila, R. Hariharan, and M. M. Ramya Selvi, "A novel coalition game theory based resource allocation and selfish attack avoidance in cognitive radio ad-hoc networks," *Journal of Theoretical and Applied Information Technology*, vol. 64, no. 1, pp. 180–189, 2014.

[58] D. Das, K. Majumder, and A. Dasgupta, "Selfish node detection and low cost data transmission in MANET using game theory," *Procedia Computer Science*, vol. 54, pp. 92–101, 2015.

[59] T. Lei, S. Wang, J. Li, I. You, and F. Yang, "Detecting and preventing selfish behaviour in mobile ad hoc network," *The Journal of Supercomputing*, vol. 2015, pp. 3156–3168, 2015.

[60] A. S. Sani and R. Syeda, "Defending selfish node in MANET using game theory approach," *Journal of Information Science and Engineering*, vol. 32, no. 3, pp. 559–573, 2016.

[61] M. Touati, R. El-Azouzi, M. Coupechoux, E. Altman, and J. M. Kelif, "A controlled matching game for WLANs," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 707–720, 2017.

[62] C. Vijayakumaran and T. A. Macriga, "An integrated game theoretical approach to detect misbehaving nodes in MANETs," in *Proceedings of the Proc. 2017 2nd Int. Conf. Comput. Commun. Technol. ICCCT 2017*, pp. 173–180, IEEE, Chennai, India, 23-24 February 2017.

[63] S. Nobahary, "Selfish node detection based on hierarchical game theory in IoT," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1–19, 2019.

[64] J. Bezdek, "Fuzzy models-What are they, and why? [Editorial]," *IEEE Transactions on Fuzzy Systems*, vol. 1, no. 1, pp. 1–6, 1993.

[65] E. V. Balan, M. K. Priyan, C. Gokulnath, and G. U. Devi, "Fuzzy based intrusion detection systems in MANET," *Procedia Computer Science*, vol. 50, pp. 109–114, 2015.

[66] Z. Ullah, M. S. Khan, I. Ahmed, N. Javaid, and M. I. Khan, "Fuzzy-based trust model for detection of selfish nodes in MANETs,"vol. 2016, pp. 965–972, in *Proceedings of the Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016, IEEE, Crans-Montana, Switzerland, 23-25 March 2016.

[67] M. M. Javidi and M. V. Baseri, "Fuzzy selfish detection ad hoc on-demand distance vector routing protocol (FSDAODV)," *Journal of Computer Science & Computational Mathematics*, vol. 71, pp. 7–12, 2017.

[68] H. Hasani and S. Babaie, "Selfish node detection in ad hoc networks based on fuzzy logic," *Neural Computing & Applications*, pp. 1–12, 2018.

[69] D. José and M. Antonio, "OLSR Fuzzy Cost (OLSR-FC): an extension to OLSR protocol based on fuzzy logic and applied to avoid selfish nodes," *Revista de Informática Teórica e Aplicada*, vol. 26, no. 1, pp. 60–77, 2019.

[70] A. Akhbari and A. Ghaffari, "Selfish node detection based on fuzzy logic and Harris hawks optimization algorithm in IoT networks," *Security and Communication Networks*, vol. 2021, 2021.

[71] J. J. Jaramillo and R. Srikant, "Darwin: distributed and adaptive reputation mechanism for wireless ad-hoc networks," in *Proceedings of the Proc. 13th Annu. ACM Int. Conf. Mob. Comput. Netw. - MobiCom*, vol. 07, p. 87p. 87, January 2007.

[72] D. E. Charilas, K. D. Georgilakis, and A. D. Panagopoulos, "ICARUS: HybrId inCentive mechAnism for coopeRation stimUlation in ad hoc networkS," *Ad Hoc Networks*, vol. 10, no. 6, pp. 976–989, 2012.

[73] N. Muthumalathi and M. Mohamed Raseen, "Fully selfish node detection, deletion and secure replica allocation over manet," in *Proceedings of the 2013 Int. Conf. Curr. Trends Eng. Technol. ICCTET*, pp. 413–415, IEEE, Coimbatore, India, 03-03 July 2013.

[74] M. I. Shanthi and D. S. Shanthi, "Detection of false alarm in handling of selfish nodes in MANET with congestion control," vol. 10, no. 1, pp. 449–457, 2013.

[75] S. Geethanjali and K. Nagendran, "Detection of selfish node in replica allocation for improving data accessibility in MANET selvam college of technology," *Namakkal , India*, vol. 1, no. 2, pp. 148–152, 2013.

[76] D. G. Gopal and R. Saravanan, "Selfish node detection based on evidence by trust authority and selfish replica allocation in DANET," *International Journal of Information and Communication Technology*, vol. 9, no. 4, pp. 473–491, 2016.

[77] B. Chen, J. L. Mao, N. Guo, G. H. Qiao, and N. Dai, "An incentive detection mechanism for cooperation of nodes selfish behavior in wireless sensor networks," in *Proceedings of the 2013 25th Chinese Control Decis. Conf. CCDC*, pp. 4021–4024, IEEE, Guiyang, China, 25-27 May 2013.

[78] P. Sondi, D. Gantsou, and S. Lecomte, "Design guidelines for quality of service support in Optimized Link State Routing-based mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, no. 1, pp. 298–323, 2013.

[79] C. Chakrabarti and S. Roy, "An observer-based distributed scheme for selfish- node detection in a post-disaster communication environment using delay tolerant network," in *Proceedings of the 2014 Applications and Innovations in Mobile Computing (AIMoC)*, 27 February 2014 - 01 March 2014.

[80] X. Wang, Y. Cai, and Z. Li, "A novel hybrid incentive mechanism for node cooperation in mobile cyber-physical systems," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 29, no. 3, pp. 316–336, 2014.

[81] D. Abdelmohsen and T. Abdelkader, "Detecting selfish nodes and motivating cooperation in Mobile Ad-hoc Networks," *Proc. - 2015 10th Int. Conf. Comput. Eng. Syst. ICCES*, pp. 301–306, 2015.

[82] T. Hayajneh, G. Almashaqbeh, and S. Ullah, "A green approach for selfish misbehavior detection in 802.11-based

wireless networks," *Mobile Networks and Applications*, vol. 20, no. 5, pp. 623–635, 2015.

[83] C. A. Kerrache, A. Lakas, and N. Lagraa, "Detection of intelligent malicious and selfish nodes in VANET using threshold adaptive control," in *Proceedings of the Int. Conf. Electron. Devices, Syst. Appl*, Ras Al Khaimah, United Arab Emirates, 19 January 2017.

[84] I. Introduction, "A review on node activity detection," *SELFISH & MALICIOUS BEHAVIORAL PATTERNS USING WATCHDOG*, pp. 1–5, 2017.

[85] V. Geetha and S. A. Hariprasad, "A conjectural based framework to detect & defend/classify selfish nodes and malicious nodes in manet using AODV," *International Journal of Innovations in Engineering and Technology (IJIET)*, pp. 8–14, 2020.

[86] H. Lin and F. Zhang, "A scheme for stimulating message relaying cooperation," *International Journal of Distributed Sensor Networks*, pp. 1–8, 2020.

[87] Y.-T. Chuang and T. Jia-Jun, "cRedit-based and reputation retrieval system," *The Journal of Supercomputing*, pp. 1–42, 2021.

[88] S. Nobahary, "ISOT: distributed selfish node detection in internet of things," *International Journal of Information & Communication Technology Research*, vol. 10, no. 3, pp. 19–30, 2018.

[89] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks 1 introduction," *Tech. Rep. DSC/2001/046*, pp. 1–23, EPFL-DI-ICA, 2001.

[90] B. Srikanth, "Detecting selfish nodes in MANETs," in *Proceedings of the 2010 6th International Conference on Wireless and Mobile Communications*, IEEE, Valencia, Spain, 20-25 September 2010.

[91] Y. Sun, Y. Guo, Y. Ge, S. Lu, J. Zhou, and E. Dutkiewicz, "Improving the transmission efficiency by considering non-cooperation in ad hoc networks," *The Computer Journal*, vol. 56, no. 8, pp. 1034–1042, 2013.