

Research Article

A Survey on the Noncooperative Environment in Smart Nodes-Based Ad Hoc Networks: Motivations and Solutions

Muhammad Altaf Khan ¹, **Moustafa M. Nasralla** ², **Muhammad Muneer Umar** ¹,
Zeeshan Iqbal ¹, **Ghani Ur Rehman** ³, **Muhammad Shahzad Sarfraz**,⁴
and Nikumani Choudhury ⁵

¹Institute of Computing, Kohat University of Science & Technology, Kohat 26000, Pakistan

²Department of Communications and Networks Engineering, Prince Sultan University, Riyadh, Saudi Arabia

³Department of Computer Science & Bioinformatics, Khushal Khan Khattak University, Karak, Pakistan

⁴Department of Computer Science, National University of Computer and Emerging Sciences, Chiniot Faisalabad Campus, Chiniot 35400, Islamabad, Pakistan

⁵Department of Computer Science & Information System, Birla Institute of Technology & Science, Hyderabad, India

Correspondence should be addressed to Moustafa M. Nasralla; mnasralla@psu.edu.sa

Received 17 March 2021; Accepted 22 May 2021; Published 30 May 2021

Academic Editor: Helena Rifà-Pous

Copyright © 2021 Muhammad Altaf Khan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In ad hoc networks, the communication is usually made through multiple hops by establishing an environment of cooperation and coordination among self-operated nodes. Such nodes typically operate with a set of finite and scarce energy, processing, bandwidth, and storage resources. Due to the cooperative environment in such networks, nodes may consume additional resources by giving relaying services to other nodes. This aspect in such networks coined the situation of noncooperative behavior by some or all the nodes. Moreover, nodes sometimes do not cooperate with others due to their social likeness or their mobility. Noncooperative or selfish nodes can last for a longer time by preserving their resources for their own operations. However, such nodes can degrade the network's overall performance in terms of lower data gathering and information exchange rates, unbalanced work distribution, and higher end-to-end delays. This work surveys the main roots for motivating nodes to adapt selfish behavior and the solutions for handling such nodes. Different schemes are introduced to handle selfish nodes in wireless ad hoc networks. Various types of routing techniques have been introduced to target different types of ad hoc networks having support for keeping misbehaving or selfish nodes. The major solutions for such scenarios can be trust-, punishment-, and stimulation-based mechanisms. Some key protocols are simulated and analyzed for getting their performance metrics to compare their effectiveness.

1. Introduction

Unlike other traditional data communication networks, ad hoc networks are considered very ideal in scenarios where rapid deployment of a network is preferred. The typical variants of ad hoc networks can be Wireless Sensor Networks (WSNs) [1], Mobile Ad hoc Networks (MANETs), Delay Tolerant Networks (DTNs), and Vehicular Ad hoc Networks (VANETs) [2]. Due to the exceptional features of wirelessly connected devices in ad hoc networks, these networks can be

used for a variety of drives like gathering environmental data [3] and controlling smart homes, cities, and industrial equipment [4]. Since the nodes in such networks are designed to be inexpensive and small in size, these nodes have to work with a limited set of resources like storage, battery, processing, and radio frequency power [5, 6].

Each node in ad hoc networks can operate without the existence of a central router and can be programmed to support multihop communication for inexpensive and speedy utilization. In multihop communication, a source node can

connect another target node through a chain of various intermediate nodes. Each node, besides its fundamental functionalities, also offers relaying services to other nodes to develop a collective, cooperative environment throughout the network. In some wireless ad hoc networks, nodes are deployed randomly and may move in undecided directions [7]. Moreover, such nodes form a dynamic topological structure that allows them to learn their degrees and route information by periodic exchange of information. Therefore, each node is desired to adequately coordinate with its neighborhood for keeping the route information updated.

The ad hoc networks are unorganized and infrastructureless networks. The nodes in such types of networks perform many operations along with the routing functionalities. The term smart node refers to the nodes which perform their operations autonomously without any input from others. These nodes intelligently adopt some strategies according to their own needs or preferences. In most of the game-theoretic approaches, the nodes are considered to be smart during the data routing in the network. These nodes are programmed in such a way that they learn from the environment and intelligently take decisions of their own interests.

The devices' scarcity of various resources in ad hoc networks can be associated with the nature of their exertion and physical structure. In WSNs, the nodes' processing power and energy are always assumed to be very limited. In almost all the routing protocols, the energy consumption rate is very deeply tested. Many research proposals are purely targeting the energy efficiency in WSNs [8–13] and fog networks [14], while in DTNs, the size of storage queues is assumed to have a vital role. The limited storage of devices highly degrades the opportunistic nature of data communication in DTNs. Moreover, the nonavailability of the relay or target node also reduces the network performance. In VANETs, various parameters are considered as important and limited. Primarily the bandwidth, storage buffers, and energy are considered as vital in such networks. Moreover, the high rate of mobility is also a challenge in VANETs [15]. In most ad hoc networks, the nodes operate on restricted batteries, which bounds the lifetime of the nodes and the entire network. In some cases, the social likeness or dislikeness of smart devices also affects data communication and network efficiency.

Each node consumes its resources on its own operations and the collective objective of the entire network. To accomplish the overall objectives, the nodes must cooperate with one another during the information exchange and data transmission from a source to a target node. While keeping the aggregate interest, each node consumes an additional amount of energy and storage queue for giving relaying services to other source nodes. This additional resource consumption can lead to shortening the nodes' life and can degrade its own data transfer. A node can eradicate these issues by simply not cooperating with other nodes. Nodes having a noncooperative behavior can be called selfish nodes. Selfish nodes prefer to be entertained by other nodes but in return do not like to consume their resource for others. The study in [16] defines two categories of selfish

nodes: The first class of nodes participates in the routing by receiving and acknowledging the reception of packets. However, these nodes drop the received packets and do not forward any data or control packets generated by a source node. The second class of nodes does not take part in the routing and never accepts any route request packets (RREQ). Some authors also refer to selfish nodes as malicious nodes in their work [17]. In many literatures, the selfish nodes are considered nondestructive or nonmalicious as they only try to preserve their own resources. However, such nodes can influence the performance of other nodes and degrade the overall functionality of the network.

A node can adopt selfish behavior for its own advantage due to various reasons. In return, a selfish node can highly degrade the network performance up to a very high peak. The main issues caused by the existence of selfish nodes can be higher packet drops, increased energy consumption, imbalanced load among nodes, and nonavailability of optimal paths for data transmission. Additionally, a selfish node can be used by some malicious nodes for black hole attacks. In a black hole attack, the packets are intentionally dropped by the attacker nodes for a malicious purpose [18].

Various techniques have been introduced to manage selfish nodes in ad hoc networks. Some authors suggest the act of selfishness as beneficial up to some extent [19]. However, there should be a proper mechanism to control or allow such behavioral aspects of network nodes. The most popular techniques for selfish node management are trust management, incentive-based, and evolutionary game-theoretic mechanisms. In some cases, Intrusion Detection Systems (IDSs) can also be utilized to block noncooperative nodes in a network. Usually, the researchers propose their mechanisms to target some particular types of ad hoc networks. These mechanisms can be interchangeably considered for other types of the network with some modifications and assumptions.

The main object of this work is to enlighten the noteworthy aspect of the noncooperative environment caused by intelligent nodes in ad hoc networks. The primary drives for pushing smart nodes to act selfishly in different flavors of ad hoc networks are discussed and classified. Different domains causing the noncooperative communication environment targeted by various articles are discussed in this work. Moreover, several types of protocols designed for ad hoc networks and having support for selfishness management are studied and categorized. At the end of this work, protocols of different categories are simulated and their performance metrics are calculated. The differences and similarities of experimented protocols are discussed in detail and some valuable conclusions are made.

The article is divided into six sections. In the next section, a detailed description of the noncooperative environment in ad hoc networks is given. In this section, the fundamentals about the selfishness of nodes are discussed. Nodes can adapt selfish behavior due to various motives based on their preferences and limitations. A detailed description of the motivations for the adaptation of selfishness is given in the third section of this article. The solutions for handling the selfish behavior of nodes are given in the fourth

section. A selfish node can be isolated or/and stimulated by adopting some state-of-the-art schemes. In the fifth section, an analytical study is performed to check the effectiveness of various proposed techniques. In the last section conclusion of our work is given.

2. Noncooperative Behavior in Ad Hoc Networks

The routing protocols used in ad hoc networks can be categorized as proactive and reactive. In the proactive routing protocols, the nodes learn about the topology of the network and the availability of routes by exchanging some periodic messages. These messages are referred to as topology control messages or HELLO messages. Each node generates such messages after a particular period of time. Upon reception of such messages, the node responds with its availability. The generator and the respondent nodes keep their routing tables updated with the help of topology control messages. Destination Sequence Distance Vector (DSDV) and Optimized Link State Routing (OLSR) are the examples of proactive routing protocols. In reactive routing protocols, the message initiating node broadcasts a route request to all the network nodes to discover the network topology. The route discovery is made up by flooding the route request message throughout the entire network. These protocols are known as on-demand routing protocols. The destination node upon receiving the route request responds to the source node and a path is established between the two nodes. Examples of reactive protocols are Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) [20]. In both types of routing protocols the coordination and cooperation of nodes are always required.

The cooperative operation of the network nodes is always desired in ad hoc networks. In ad hoc networks node can be assumed as members of a community in which each member inputs something for the fulfillment of the combined objectives of the community. The contribution to problem solution binds the individual resource consumption with the aggregate interests of community members. However, nodes controlled by humans or programmed with intelligence may lead to some undesired circumstances for having self-interests. The nodes sometimes cannot judge the importance of their existence in the community. This self-interest can lead to noncooperation among the nodes [21]. If the developed infrastructure does not log the nodes' data traffic in an appropriate manner and allows nodes to smartly adapt their strategies, this leads to nodes' independence. An independent node may think that its own resources being meant for its use may lead to selfish behavior.

The selfishness of a node is somehow similar to a black hole attack in such networks. In the black hole attacks, the attackers intend to drop the data packets whenever they are supposed to forward those packets. The main intention for pack dropping in black hole attack is to degrade the network performance or another malicious purpose [22]. However, in the case of selfishness, the nodes adopt a noncooperative behavior only for their own benefit rather than any malicious

objective. The existence of selfish nodes in such type of networks can lead to various unwanted outcomes. A selfish node can increase the number of overall packet drops but not giving a relay service to some or all source nodes. The selfish node can drop the received packets any time which are needed to be forwarded to the next hop in the network towards the destination. Due to this behavior, the load distribution is imbalanced among the network nodes. Consider a scenario shown in Figure 1; a single selfish node can involve other normal nodes to become intermediate hops in a data transmission channel, causing the involved nodes to take the load which is not supposed to be taken. Due to imbalanced load distribution, the energy consumption is also not uniform. Some nodes exhaust their energies earlier and die before a normal period. The selfish nodes can increase the end-to-end delays by not allowing a source node to get the shortest paths towards the destination.

The article in [23] takes Dynamic Source Routing (DSR) as a case study and determines that the selfishness associated with routing can be classified into three major categories:

- (a) *Type 1 Selfish Nodes.* The selfish nodes participate in the normal control data packets' transmission during the routing discovery and maintenance phases but do not become a relay for forwarding normal data packets. Such type of nodes is considered very dangerous for the overall operations in the data routing. These nodes initially participate in the route discovery to establish paths but later they start denying the relay service for others. In such cases, the packet drops and end-to-end delays are highly increased. It is also possible that the selfish nodes do not adopt noncooperative response for all the nodes but only selected nodes are targeted. The major reason can be social likeness or dislikeness.
- (b) *Type 2 Selfish Nodes.* The selfish nodes do not participate in anything associated with data transmission for other nodes either in the route discovery phase or in the route maintenance phase. Such nodes only use their energies to be consumed by their own data processing and transmission. The routing protocols usually do not consider such types of nodes. No route information is gathered from or transferred to this class of selfish nodes. These nodes can highly degrade the overall data communication traffic and network connectivity. However, the routing protocols do not consider these as a major threat to the discovery and maintenance of routes in an ad hoc network.
- (c) *Type 3 Selfish Nodes.* Such nodes adjust their cooperation level according to their resource levels. These nodes in the beginning act like normal nodes. With the passage of time, the nodes start decline in their cooperation with others due to a reduction in their resource levels. In a smart environment, it is possible that nodes interrelate their remaining energy levels with their selfishness levels. The multiple levels of selfishness, referred to as Multiple Threshold

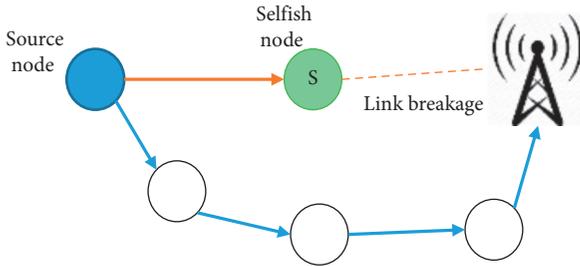


FIGURE 1: Effect of a selfish node in routing.

Selfishness (MTS), are well defined by [18, 24]. Such nodes are similarly dangerous as type 1 selfish nodes. The nodes support the route discovery flow for forming a topology but later interrupt the data flow by dropping data packets. Such type of nodes causes the routing protocol to reinitiate the route discovery process or adopt another alternate route for data transmission.

The selfish nodes usually adopt their distinct behavior for their own interest and do not develop an intention for the degradation of the network performance. However, it is understood that the selfish nodes bring unwanted and rapid topological changes in the network which put a very big impact on the overall performance of the network. Some authors, like Umar et al. [18], use the selfishness of nodes as a key for the establishment of paths and load balancing among the sensor nodes in a WSN. Some authors suggest that selfishness can be used in a positive sense and the network can benefit from such behavior of nodes up to some extent [19]. A mechanism allowing selfishness can permit some nodes to keep their resource preserved for some vital motives in the future. The nodes having some extra responsibilities can be permitted to not give any relay service to others in a selfish manner.

A node having persistent noncooperative behavior can raise the rate of packet loss in an ad hoc network up to 100%. However, the ratio of packet loss due to a selfish node diminishes with an evolution in the density of normal cooperative nodes in the ad hoc network [24]. Due to this assumption, we can say that the network having a large number of nodes will face comparatively less damage due to the presence of selfish nodes in it. More precisely, the number of selfish nodes can be directly associated with the network performance.

3. Motivations for Selfishness Adoption

A node in any variant of ad hoc networks can adopt selfishness whenever it is programmed with smartness or controlled by another intelligent entity. The intelligent entity can be another device, module, program, or human. Selfishness is very common in human-operated personal devices like smartphones and personal digital assistants [25]. A node can be adequately programmed so that it becomes independent of other nodes in the network and decides its own functionalities [26]. A smart node can adjust its behavior for several reasons. The foremost reason is the energy

preservation in all the ad hoc networks. In Table 1, some ad hoc networks are given along with the potential motivations for their nodes' being selfish. All the motivational factors for pushing smart nodes to change their cooperative behavior are as follows.

3.1. Energy. Almost in all types of wireless ad hoc networks, the nodes use batteries as the only power source. These batteries are usually disposable and non-rechargeable in most of the WSNs and similar networks. Nodes are randomly thrown into a field and then left unattended in such networks. Therefore, battery replacement or recharge cannot be made feasible, while in some cases these batteries can be recharged by the operators like in VANETs and MANETs. However, the energy source in ad hoc networks is always assumed as finite and scarce [11].

A node consumes its energy on various types of functionalities. The foremost are data processing, transmission, sensing, and reception. Energy consumption can be categorized as useful or wasteful. Energy consumed on data transmission and reception, data processing, and control messaging in the network can be considered as useful, while wasteful energy expenditure is carried by overhearing, generation, and processing of control packets, idle listening, and retransmission of lost packets [9]. If a node stops or reduces any of these functionalities it can be a detriment in various ways. To reduce the energy consumption on data transmission, it is possible for nodes to not forward others' data packets. The forwarding nodes usually consume additional energy on the reception of data and then retransmission. The selfish nodes reduce their energy consumption by never opting to give any relay service.

Suppose a node depletes ax amount of energy on transmitting a single bit and consumes bx amount of energy on the reception of a single bit. As per wireless communication fundamentals, the value of a must be greater than b , i.e., $a > b$ [10]. Ignoring all other parameters used in data communication, i.e., range, etc., a normal node will consume $ax + bx$ amount of energy for forwarding a single bit, while a selfish node can save this by only hearing the single bit with bx amount of energy and does not use amount on retransmitting the same bit.

The selfishness of nodes for the sake of energy preservation is very common in most of the ad hoc networks. Most of the researchers take sensor nodes with disposable batteries as their case studies [18, 27]. However, any type of ad hoc network where the nodes are operated by a finite power source can be assumed to have the possibility of a noncooperative environment among the nodes. Some authors marked the selfishness of nodes as the most effective tool for their energy-saving and life-lengthening [18].

3.2. Storage Buffer. The nodes in ad hoc networks operate on limited storage space. It is obvious that the nodes must store the received contents temporarily before their transmission to the next hops. Sometimes the nodes need to choose which data content is useful for them and should be stored in their storage buffers. Most of the nodes try to keep their storage

TABLE 1: Types of ad hoc networks and their motivations for the selfishness adoption.

Network type	Primary concerns	Secondary concerns	No concerns
WSN	The nodes operate on limited energy, storage, and bandwidth.	Social likeness can be considered secondarily. Some intelligent nodes may prefer some other selected nodes for cooperation.	In most of WSNs, the nodes do not move. The mobility does not affect the behavior of nodes in WSNs.
DTN	Social likeness associated with limited storage buffer can be considered. The nodes prefer to use their storage buffer for some known nodes.	Energy can also be considered for behavioral change. The nodes may operate on a limited set of energy.	Privacy and mobility are not considered in most of the DTNs.
VANET	In most of the VANETs, the data privacy, social likeness, and mobility of network nodes are considered.	Bandwidth in some cases may be considered due to the huge amount of traffic.	Usually, energy and storage are not focused in most of the VANETs.
Smart phones ad hoc network	The smart nodes use a limited set of batteries. The phone may carry some sensitive private data and the users may have some social affiliations	The phone set may have a limited amount of storage for keeping the data being forwarded to others.	Mobility and bandwidth are not considered in such networks.
Mobile sensor network	Limited energy, storage, and mobility of nodes may affect the routing behavior.	Bandwidth, secondarily, may lead to a selfish behavior.	Usually, such nodes do not consider the data privacy.

buffer for their own collected data, which in return does not allow another node to be entertained. All the nodes keep the received relayed data saved with them until they get the connectivity with their next hops. It is possible that the nodes delete the received data before it is transmitted to sparing their storage buffer for their own data [28]. The limited buffer size leads to defining appropriate buffer management schemes. In some ad hoc networks, like DTNs, the buffer management policy describes which message to keep and which to discard. This policy of prioritizing messages for data buffer is assumed to be very fruitful by [29]. In DTN, the nodes can adopt a selfish behavior due to their limited buffer storage which in turn can benefit them for their own data transmission. However, the source nodes needing multiple hops towards their destinations are highly affected. The selfish nodes in such case never bother to request others for relay service with buffer usage for their data transmission but in return regret for not giving any space in their buffer to keep the relay requesters data messages. Such act of selfish nodes is also referred to as routing misbehavior [28]. Figure 2 shows some nodes using their limited storage buffers during data communication.

3.3. Social Likeness. Internet-based social networks have made many interconnected relationships among the users. Such networks touch countless aspects of our daily lives and enable us to get people having similar mindsets. In social networks, the selfishness of the user cannot be overlooked in many terms. The far most reason for selfishness is the likeness and dislikeness [30]. Similarly, the smart or humanly controlled nodes in an ad hoc network can also consider the aspect of the social likeness during their communication. Practically, sometimes the intermediate nodes drop the packets due to not giving any attention to the sender node. Social selfishness is usually associated with the DTNs type of networks in which most of the nodes are either operated by humans or installed in vehicles [31]. The nodes having no social ties do not cooperate with one another with

a determination to save their resources. An example of the mobile social network can be considered for such a case. People like to share common interests which form a community via mobile phones. These communities can be considered as interest groups of mobile nodes where each member tends to assist its community members only and does not like to spare its resources on any stranger node. Moreover, previous connectivity and behavioral records can also influence a node to socially like or dislike others [32].

3.4. Bandwidth. In a network where nodes transmit bulky data their assigned bandwidth may need to be utilized. The size of bandwidth is always limited in nature. It is possible that the nodes adopt particular cooperation or noncooperative behavior according to the size of their assigned bandwidth. Sometimes, the nodes cannot entertain any other relay requester for data transmission due to the own bulky data [31]. Bandwidth limitation in most of the ad hoc networks is a considerable issue and addressed by many researches. In WSNs, the sensor nodes operate on a very limited bandwidth as they cannot manage a higher data spectrum with their lower energies and processing capabilities. Many authors proposed node-level processing to reduce the load on communication bandwidth [33]. Therefore, the nodes, if programmed with intelligence, prefer to use their communication channel for their own data.

3.5. Mobility Rate. In most of the MANETS, due to the mobility of nodes, the topological interconnections change with the passage of time. If a node moves from one place to another, it may break some connections and may establish some new connections. It is palpable that the higher rate of mobility nodes can exceedingly degrade the network performance. Sometimes, a relay node cannot change its location in the network to avoid any data loss of the source node. It is also possible that a source node requests the relay nodes to not move until the completion of the data

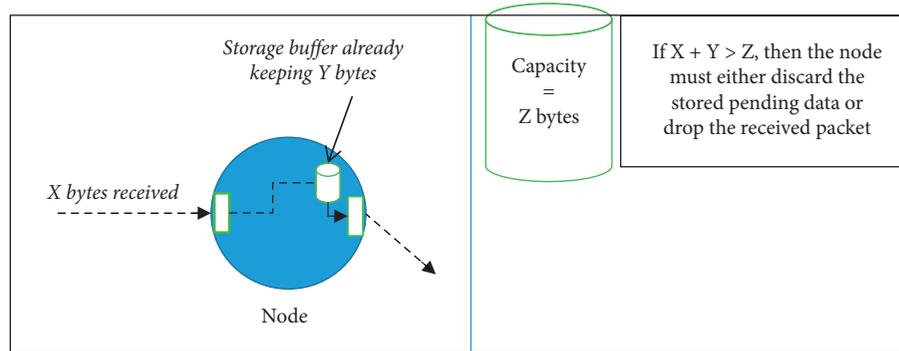


FIGURE 2: Use of storage buffer during data transmission.

transmission. Since each smart node considers its own benefits, they may act selfishly and change their location without favoring any source node. Moreover, mobility control can be incorporated into the mechanism for fault tolerance [34]. The concept of cooperative mobility and communication appeared in the related literature in the 1970s. This key meaning is that each node in the network has two possible modes, i.e., (a) selfish, which does not move for others but only prefers its own optimization, and (b) cooperative, which takes care of the entire network and tries to attain the aggregate goal [35].

3.6. Privacy Concern. During communicating with each other, some nodes may require others' private data. In a general context, we can say that a network of mobile phones exists and each phone shares its location with others through some applications. It is possible that a phone reads the locations of all the connected ones but never likes to share its own location. Such type of selfishness can be categorized into privacy or personal data sharing. According to a scheme proposed by HE et al. [36] for WSNs, clusters may share common data with each other while inside clusters some nodes may need to share their private data.

4. Solutions for Selfishness Management

Many researchers target a primary domain like energy efficiency, load balancing, reduced end-to-end delays, and efficient storage buffer management while designing a selfish node management protocol. Various classifications of selfish node management schemes have been proposed in the area of security and routing in ad hoc networks. The schemes can be classified in various ways. In this work, we divide the selfish node management schemes into four classes: (a) IDS; (b) trust-based mechanism; (c) incentive-based mechanism; (d) evolution games theoretic approaches. Each class target some particular types of ad hoc networks and have some pros and cons. For example, in WSNs, lightweight schemes which do not put extra load on radio transmission are preferred. Some articles like [18] suggest credit-incentives-based schemes as a more suitable solution handling non-cooperative environment in WSNs. The mentioned classes are explained in Table 2.

4.1. Intrusion Detection System. An IDS can be a device or an embedded program that monitors the data traffic in a network and detects any inappropriate behavior violating a predefined policy or pattern. A typical IDS provides information about the nodes' abnormal/malicious behavior in a network. However, the same can be utilized for the detection of selfish nodes in the network. The IDS can be used for detection purposes only and cannot be utilized for node stimulation towards cooperation [41]. There are three major classifications of IDSs: misuse-based detection, anomaly-based detection, and specification-based detection [22].

4.2. Trust Management Schemes. Some proposed systems use a trust development procedure among the nodes. The trust levels are defined based on the nodes' cooperation level in the network. The nodes share their experiences about one another which ultimately let all the nodes understand each other's behavior. The knowledge-sharing about the past experiences of nodes leads them to develop a trust level about each node in the network. The selection of relay relies on the trust level of the next nodes in the potential route [42]. Various typical and sophisticated schemes have been introduced in this domain. Most of the schemes are considered as the fundamental and classical schemes for addressing selfishness in ad hoc networks. The trust is usually associated with the nodes; however, the same can also be applied with the data. Data trust can be used to verify the authenticity of data in the various types of ad hoc networks. Some authors give a description of node trust and data trust in the VANETs [43].

An old but still the most effective approach, watchdog and pathrater [37], is a selfish node detection and punishment scheme. This approach is used to detect routing faults by monitoring the behavioral aspects of involved network nodes. This scheme targets selfish and malicious nodes. Watchdog is a detection module while pathrater is used to block the misbehaving or problematic nodes. Another similar approach, CONFIDENT [44], targets the malicious nodes in a network. Four major modules are designed for this approach. These modules are programmed in each network node to achieve the aggregate goal of the optimal performance of the network. Many articles are using these two techniques as baselines for their proposed mechanisms.

TABLE 2: Classes of schemes used for selfish node management.

Class type	Description	Example
Detection mechanisms	Detects and adaptively reports/blocks the noncooperative or misbehaving nodes in the network Simple and straightforward schemes for treating all the nodes	Marti et al. [37]
Trust-based mechanisms	Some trust levels are defined among the nodes Behavioral history of each node is logged and the nodes consider the trust levels among them	Shaikh et al. [38]
Reputation-based incentive mechanisms	A reputation level is made based on incentives granted Nodes try to get more incentive by offering frequent relaying services for their better reputation	He et al. [39]
Credit-based incentive mechanisms	A pricing model is made Nodes are given some values for their data exchange The relaying service is paid by the source nodes for forwarding their data	Umar et al. [18]
Evolutionary game-theoretic approaches	A repetitive type of procedure is adopted in such mechanisms Each node learns with the passage of time and adjusts its strategies to obtain an equilibrium point for the entire network Most of the evolutionary games are applied in cluster-based WSNs	Gameda et al. [40]

Some trust-based mechanisms like [38] are effective in group or cluster-based ad hoc networks. The profiles of all the nodes are kept and distributed among all the nodes through the group heads. The trust values are directly affected by the behavioral aspects of nodes during the communication and cooperation among the nodes. For effective and secure routing some trust-based schemes also incorporate public keys for trust maintenance.

The protocols laying in this class can also be referred to as node punishment-based mechanisms. The ultimate goal of carrying the detection and trust management in such schemes is to punish the noncooperative or misbehaving nodes by blocking them in the network. The blocked nodes are also called black-listed nodes. Such nodes are not entertained for their own relay request by other nodes. Moreover, these nodes are not requested for any cooperation during the data transfer by any source node.

The trust-based schemes are also introduced in the emerging M2M and IoT architecture. In such types of ad hoc networks, the heterogeneity of nodes is also considered at the base level [45].

4.3. Incentive-Based Mechanism. Many researchers assume the incentive-based mechanisms as the most effective techniques in the same domain. These approaches consider the network nodes as rational and autonomous of any restriction for cooperation with one another. The nodes are supposed to have their policy for adopting a work contribution strategy based on their individual interest. In such scenarios, the nodes are stimulated by using some incentives to let them cooperate with each other. The theme of these approaches can be simply called “give and take” or “tit-for-tat” procedures. The incentive-based mechanisms can be classified as reputation-based incentives and credit-based incentives. For designing such systems, many researches proposed the incorporation of game theory in their proposed mechanisms. The role of game theory and the two

classes of incentive-based mechanisms are explained in the following subsections.

4.3.1. Role of Game Theory. For the development of incentive-based mechanisms in ad hoc networks, game theory is given a vital role in the realization of the procedural analysis and quantization in the designing phase. Basically, the game theory is introduced in economics for the evaluation and processing of financial matters. This area is also used in social and biological sciences. However, this theory is recently adopted by many researchers for their proposals in wireless networks. A game can be considered as a set of players, strategies of each player, payoff functions, the output or gains, and the equilibrium function. A typical ad hoc wireless network can be aligned with the game theory by taking network nodes as players, strategies as features and actions of nodes, and the payoff functions as the point where a node can balance its work with its energy consumption efficiently. The output can be considered as the outcome in terms of various concerns in a network like energy efficiency, bandwidth usage, nodes’ storage usage, and overhead on each node. Finally, the equilibrium point in a wireless network can be considered as a situation in which each node gets its optimal position addressing the aggregate benefits of the entire network.

In most of the incentive-based selfish node management systems, game theory is used to intelligently handle the nodes’ behavior according to the needs of a network. Various game types can be incorporated into the incentives schemes. Examples of games are cooperative, noncooperative, repetitive, evolutionary, and bargaining games. The selection of a game type for a scheme is dependent on the nature of the network and the requirements. For example, repetitive games are suitable for such networks where nodes do not keep all the information in the beginning. Similarly, evolutionary games are considered more effective in cluster-based ad hoc networks.

4.3.2. Reputation-Based Mechanisms. The main theme of such techniques is inspired from the usage of reputation levels of users in web-based services like Amazon and eBay. The sellers and buyers are assigned some points according to their behavior. The nature of users in such web-based stores can be judged by looking into their earned points. A similar concept can be used to evaluate the nodes' participative behavior in ad hoc networks. In the reputation-based mechanisms, several reputation stages are made to classify the nodes according to their level of participation. Those nodes which do not cooperate or have less than a specified level of cooperation are punished by other nodes. Usually, such nodes are not offered any relay service by others. To obtain an acceptable state of behavior, each node tries to obtain adequate incentives by adaptively offering its services to other nodes. It is a kind of stimulation in which each node is pushed to cooperate for the sake of its better reputation in the network [39].

The trust and reputation of network nodes cannot be considered similar due to many reasons. The trust is an active entity while reputation can be considered passive. Trust is a kind of peer node's belief and so can be extended from a peer to its node, while reputation is the perception level of nodes about each other. In some articles the trust is also associated with risk factors and reputation is something based on the history of a node.

Paper [46] points out the major issues associated with the reputation-based incentives mechanisms. The foremost issue is that these approaches do not adequately handle the node assessment process. The second issue is that the structuring of groups of nodes cannot be designed efficiently in ad hoc networks. The third issue with reputation-based mechanisms is that the nodes used their radio transmission excessively for obtaining information about each other. Therefore, many authors suggest the usage of credit-incentive-based mechanisms for controlling the nodes' behavior in a network.

4.3.3. Credit-Based Mechanisms. These schemes are also called pricing-based schemes. Such schemes consider the data transmission and relaying support by network nodes as a service that must be paid. In credit-based incentive schemes, the worth for handling buy and sell or lease and rent mechanism is obtained by several forms of values. Some of these are referred to as virtual currency, scores, money, and points. The pricing schemes also need an additional log for keeping the record of exchanges of these values. Each node upon giving relaying service obtains an amount of virtual currency from the source nodes. Each relaying node earns this currency and uses it for its data transfer. Nodes having no or fewer values of currency cannot be able to pay the relaying service and so cannot transmit their data. In such a scenario, each node tries to maintain a trade-off between its resource consumption and virtual currency collections. Such techniques give nodes a degree of intelligence for optimization of their resources along with the network performance [46].

The credit-incentive schemes can be applied in many ways. Some articles introduced a bargaining environment between the relaying and the source nodes. The game theory

of a bargaining model is used in such schemes. The main purpose is to make a competitive environment among the network nodes. Moreover, the calculation of currency for buying and selling is also aligned with some procedures. For example, the key parameters of nodes, i.e., energy, storage, and network hierarchical level, etc., can be considered for fixing the amount of currency.

In some ad hoc networks, like WSNs, nodes are connected to a central control through some hop nodes. Some nodes are directly connected to the central station and do not need any relaying service. Therefore, such nodes do not need to cooperate in any way and do not care about any currency maintenance. To overcome such cases, the central control also takes some exceptional measures by applying a reputation or punishment-based mechanism [18]. Some authors also proposed a movement cost for letting the nodes move for the sake of an aggregate benefit [34]. The nodes are given some benefits for their sacrificial movement in the field in a cooperative manner. The main purpose of such incentives is to stimulate the network nodes for moving in the area for the sake of fault tolerance.

4.4. Evolutionary Games. In evolutionary games, the nodes primarily do not use their strategic reasoning in the initial stage. All the nodes in the network learn from their experiences and then develop a model to design their strategies. This game is also known as a repetitive model in which the network nodes learn with the passage of time [40]. In the same manner with the passage of time the nodes evolve their behavior and adjust the cooperation at an optimal level where both the individual node and the entire network are benefitted. The most stable situation in such type of mechanism is referred to as an evolutionary stable strategy or evolutionary equilibrium. Most of the evolutionary-based mechanisms are designed for cluster-based WSNs [8, 40]. The evolutionary games can also be incorporated into the trust-based and incentive-based mechanism. Table 3 shows some proposed schemes for handling selfish nodes in ad hoc networks.

Table 4 shows some classical mechanisms which are considered useful as guidelines and base techniques for developing new schemes. Most of these are taken as baselines for the development of advanced techniques for selfishness management in ad hoc networks.

5. Analysis of Proposed Schemes and Discussion

In this work, a comparative analysis of five different protocols is made by taking a WSN as a model network. These protocols are DSR[ref], DSR with selfish nodes [18], Reward-based Mechanism (RwBM) [18], GREET [40], and GTMS [38]. The results are made by varying three major parameters, i.e., the number of nodes, pause time, and the ratio of selfish nodes. The results are calculated for taking the five performance metrics in the network, i.e., energy consumption, end-to-end delays, throughput, packet delay ratio (PDR), and packet loss ratio. The work is simulated in NS2.35 under Ubuntu operating system. The key parameters for simulation are listed in Table 5.

TABLE 3: Proposed schemes for selfish node management in ad hoc networks.

Article	Mechanism	Description
Attiah et al. [8], 2018	Evolutionary game	(i) A route selection problem is modeled by using a game-theoretic approach. (ii) The replicator dynamics mechanism is used to indicate that the nodes can be trained from their strategies and hence modify their strategies sets with time.
Subba et al. [41], 2018	Detection	(i) The work combines a lightweight neural network with specification rules for anomaly detection to identify misbehaving nodes in the network. (ii) A Bayesian game is designed which takes the IDS and the sensor nodes as two noncooperative players.
Umar et al. [18], 2018	Incentive-based	(i) Virtual currency referred to as scores is used for selfish node stimulation. (ii) Scores are calculated by taking many nodes' and network's parameters.
Raja et al. [42], 2018	Trust management	(i) The selection of cluster heads is done by using the multiple constraint aware glow worm swarm optimization approach (MC-GSO). Every node is evaluated in the network according to this approach. (ii) Various objectives are achieved for the trust metrics during the cluster head selection.
Yang et al. [47], 2017	Incentive-based	(i) Particularly designed for clustered WSN with an aim to balance the consumption of energy among all the nodes. (ii) A convex payoff function is designed for the behavior of each node. The game is derived with the help of this convex optimization.
Gemeda et al. [40], 2017	Evolutionary game-based	(i) Targets cluster-based WSNs. (ii) Mainly focus on the cluster heads manipulation and selection process.
Yu [48], 2016	Incentive-based	(i) Nodes are pushed to cooperate in routing by using some incentives. (ii) Some values are exchanged for getting data communication and relay services.
Li et al. [43], 2015	Trust management	(i) The work is proposed for VANETs where the trustworthiness of both mobile sensor nodes and transmitted data is evaluated. (ii) The recommendation trust and functional trust are categorized to indicate nodes' performance.
Duan et al. [17], 2014	Trust management	(i) A trust-aware routing frame is designed by incorporating lightweight and proficient attacks resistant mechanism. (ii) The common features associated with attacks in terms of trust awareness are addressed. (iii) The trust derivation is based on the analysis of results.
Chen et al. [21], 2013	Detection	(i) The cooperation level of each node is calculated and the selfish nodes are punished by blocking them in the network.
Xu and Guo [49], 2012	Incentive-based	(i) Particularly target opportunistic networks. (ii) The incentive exchange is made through various rounds of a bargaining game.
Bao et al. [50], 2012	Detection	(i) Uses highly expandable cluster and hierarchical trust-based management protocol for efficiently detecting the malicious and the selfish.

TABLE 4: Fundamental/classical selfishness management schemes.

Article	Mechanism	Description
Marti et al. [37], 2000	Reputation and detection	(i) Well-known as watchdog and pathrater (ii) Watchdog detects misbehaving nodes and pathrater blocks targeted nodes
Boudec and le [44], 2002	Trust and detection	(i) CONFIDENT, a reactive routing protocol that uses four major modules for detection and blockage of selfish nodes
Buttayan and hubaux [51], 2003	Detection and incentive-based	(i) Only the cooperative nodes are allowed to transfer their data (ii) The concept of virtual currency is used by introducing packet trade and packet purs
Zhong et al. [52], 2003	Incentive-based	(i) A credit-based incentive exchange scheme is used (ii) The scheme particularly targets mobility in MANETs like networks
Chen et al. [26], 2011	Evolutionary game-based	(i) Nodes operate according to a predefined set of states (ii) The nodes adjust their selfishness level with time

5.1. Energy Consumption. Since energy consumption is always considered in ad hoc networks, almost all the protocols designed for such networks are evaluated in terms of the nodes' life. The energy consumption rate can be affected by the simulation parameters and the routing protocol design. A network energy consumption can be evaluated by

considering either the routing energy consumption or the average energy consumption. In routing energy consumption, the network layer of the protocol is checked only to determine the energies of nodes in a network, while the average energy consumption is the mean value of all nodes' consumed energies. Energy can be calculated by taking the

TABLE 5: Simulation parameters.

Parameter	Value
Area	500 × 500
Network type	WSN
Number of nodes	50–300
Ratio of selfish nodes	Up to 5%
Node distribution	Random
Comparisons	DSR, DSR with selfish nodes, GREET, GTMS, and RwBM
Initial energy	100
Rx power	0.3
Tx power	0.6
Size of the packet header	4 bytes
RSc header size (RwBM)	4 bytes
IBSc header size (RwBM)	4 bytes
Movement trace	Off
Cluster size (GREET)	Game-based (varying)
Cluster size (GTMS)	9 nodes
Traffic source	CBR
Packet protocol	TCP
Threshold distance for CNs (RwBM)	50
Threshold participation (RwBM)	0.4
Threshold lambda (RwBM)	0.5

sum of transmit, idle, receive, and sleep power in all layers in a simulation environment. The existence of selfish nodes in an ad hoc network can highly affect the rate of energy consumption in the overall network.

In Figure 3 the average energy consumed over 15 different time pauses of the experimented protocols is recorded. For this experiment, a set of 100 nodes with 5% selfish nodes are taken. The DSR protocol is mainly designed for ad hoc networks having mobile nodes. In WSN DSR does not utilize its features for handling the mobility of nodes. Therefore, its performance may be not optimal as compared to specialized protocols designed for WSNs having static nodes. The performance of SELFISH-DSR is the worst in the figure. It is because there is no such selfish node handling mechanism. GTMS is quite responsive by giving a moderate level of results for energy consumption. This mechanism mainly utilizes the trust reciprocity among the nodes. The technique is much better than DSR and SELFISH-DSR protocols. However, due to a simple mechanism for reputation and mutual trust mechanism, GTMS is giving comparatively lower results than GREET and RwBM protocols. GREET has the lowest level of energy consumption at most of the time. Since this protocol is cluster-based and mainly designed to evaluate all the previous strategies of nodes, it has put less communication overhead on nodes for passing control and information messages. RwBM initially loads the scoring mechanism which takes some time to give the accurate result values. In initial pause times, it is giving very low values which indicates that the communication is not started properly. GREET, compared with RwBM, gives comparatively the best results for many time pauses. However, due to its cluster-based type, after a longer period, the increase in energy consumption can be noted due to the rapid elimination of nodes from the network. In cluster-based networks, all the nodes may start dying rapidly one after another.

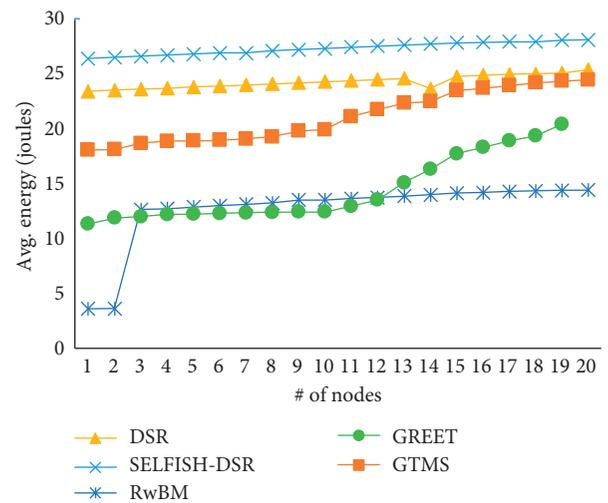


FIGURE 3: Average energy consumption at twenty time pauses.

In Figure 4, there are 5% selfish nodes and values are noted at time pause 10. All the mechanisms are giving consistent values except the SELFISH-DSR. Since there is no mechanism for the selfishness of nodes, energy consumption is increasing with the increased number of nodes. The number of selfish nodes is proportional to the number of nodes but the placement of selfish nodes over the same area greatly affects the performance of SELFISH-DSR. GTMS is giving similar results as in the previous experiment of pause times. However, its performance is declining with a number of nodes higher than 200. We can assume that the trust mechanism may start failing with a large number of nodes. It is also possible that the trust mechanism with densely deployed nodes may not be efficiently effective. The incentive-based mechanism, RwBM, is giving almost similar values for all the variations in the number of nodes. RwBM has a mechanism to deal with the nodes' individual

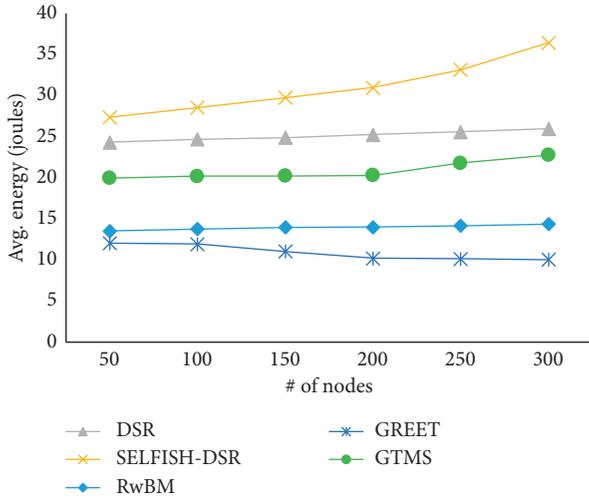


FIGURE 4: Average energy consumption with an increasing number of sensor nodes.

importance based on the nodes' density in the network. Therefore, the mechanism aligns the values of incentives according to the number of nodes and the average energy consumption is not affected by the increased number of nodes, while GREET has very impressive results by giving the least values in this experiment. The energy consumption by nodes is decreased with the increased number of nodes. It is because the mechanism is based on evolutions and the nodes learn from each other and the time period. As the number of nodes is increased, the optimal point or the nodes' maturity level is obtained earlier, and the optimal strategies are adopted by all the nodes well in time.

Figure 5 shows the third experiment relating the average energy consumption of the nodes in a WSN. There are 100 sensor nodes and the time pause used for recording values is 10. The response for an increased number of selfish nodes is notable in all the protocols. SELFISH-DSR is giving support for selfishness; therefore, the energy consumption is highly increased with each rise in the number of selfish nodes. The performance of GTMS is also not well with the higher number of selfish nodes. It is because of the mutual reputation and trust mechanism. Each node mutual with a selfish node also changes its behavior. GREET and RwBM are giving similar results. These protocols have incorporated appropriate mechanisms for handling selfish nodes in the network; therefore, both are giving very little hike in the energy consumption against the increased number of selfish nodes.

5.2. Throughput. Throughput is the total quantity of data that reaches a destination node from the source node at a particular time. It can be used to determine the effectiveness of a routing scheme.

In Figure 6, the average throughput of SELFISH-DSR is very low at 6 kbps for almost all the pause times. It is giving lower throughput than a normal DSR in a network without any selfish node. The throughput of GTMS is moderate and consistent due to its communication style. The nodes are

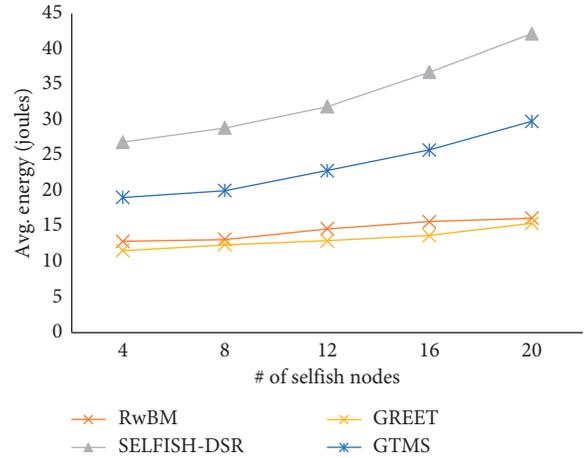


FIGURE 5: Average energy consumption with an increased number of selfish nodes.

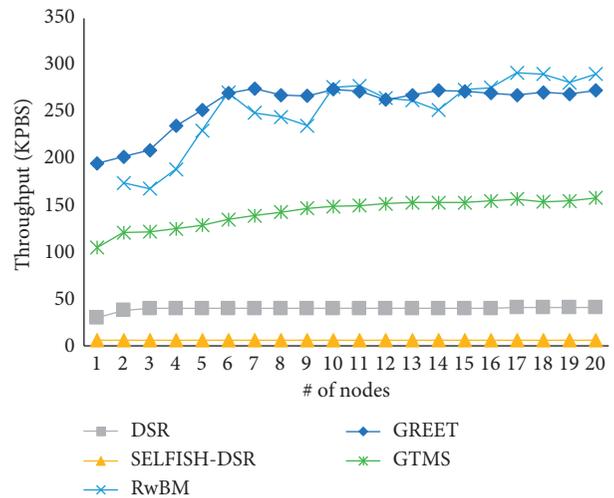


FIGURE 6: Average throughput at twenty time pauses.

taken in a smooth flow and equally treated in GTMS. Therefore, the throughput of this protocol is slightly increasing with time and becomes consistent after time pause 9. The throughputs of RwBM and GREET are very unpredictable but higher than GTMS and DSR protocols. RwBM does not give any value at time pause 1 in our simulation environment due to its score loading and configuration process. Later due to scores' exchange and periodic updating of each node the throughput highly fluctuates. GREET initially has similar throughput as in RwBM. In GREET, the nodes learn repetitively by using an evolutionary game. Therefore, the throughput is lower and cannot be predicted at initial pause times. Later once the nodes learn from the environment, after time pause 5, the nodes adjust their utility functions and deliver a better throughput.

The effect of a varying number of nodes on the experimented protocols is shown in Figure 7. The values are recorded at time pause 10 and the ratio of selfish nodes is 5%. The results are similar to the previous figure. The evolution game-based approach, GREET, is giving a very positive

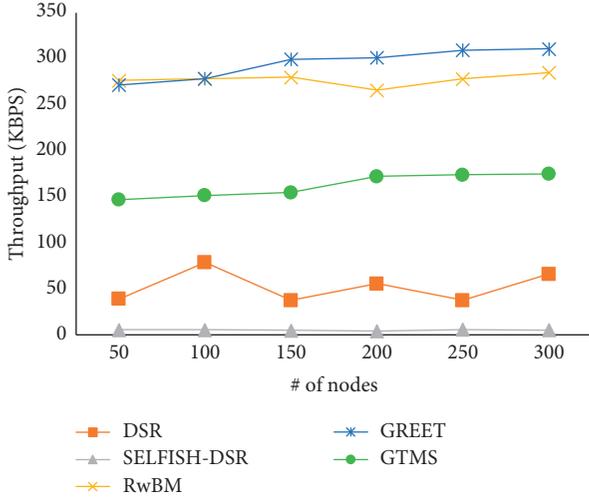


FIGURE 7: Average throughput with an increasing number of sensor nodes.

response to the increased number of nodes. RwBM is giving similar fluctuating results for each experiment. Here again, we can conclude that the RwBM, due to its scoring mechanism, gives slightly random results. However, RwBM is giving much better results than GTMS and DSR. The throughput of GTMS is also increased in this experiment.

In the last experiment for throughput, shown in Figure 8, 100 nodes are taken. The performance of GTMS is very low with an increased number of selfish nodes. It cannot manage the higher number of selfish nodes that leads to a lower value of the throughput. RwBM and GREET are also marginally affected. However, this decrease in the throughput can be considered as a very minor effect. In this experiment, the GREET outperforms due to its advanced mechanism.

5.3. End-to-End Delays. In ad hoc networks, the high data rates are not essentially required but delay constraint is greatly considered. If the required information is delayed, then it might be not useful in the network. Therefore, we calculate the average delay rate in each protocol to determine their performance. The packet end-to-end delay is the meantime that a packet consumes to reach the destination from a source node. In our scenario of WSN, we are taking the base station as the destination node. Delays in a network usually associate the speed of MAC control exchange, buffer queues, radio transmission, and routing mechanisms. In our assessment, we are comparing the routing mechanism and all other parameters are considered as similar.

In Figure 9, nodes are taken. The ratio of selfish nodes is 5%. The experiments indicate that the end-to-end delays for DSR are higher than other protocols. DSR can be more efficient if used in a mobile node environment. Moreover, reactive protocols are less efficient than proactive protocols in delays matrix. The reputation and trust levels in GTMS are developed over time. Each node considers the history of its connected hops; therefore, in the higher pause times, the delay is decreased. GREET initially produces higher delays due to its learning nature. The nodes cannot respond quickly

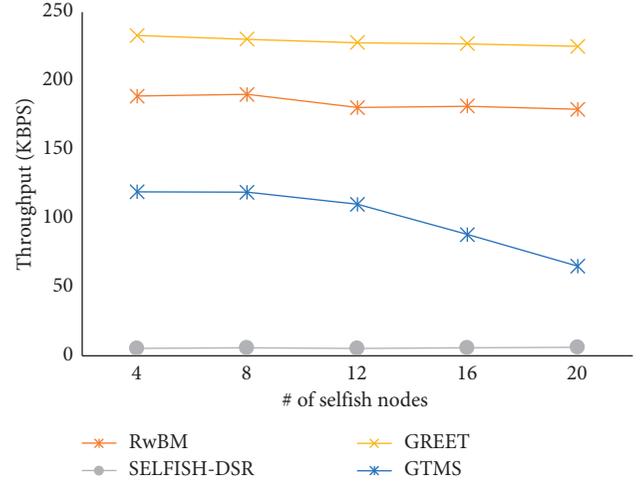


FIGURE 8: Average throughput with an increased number of selfish nodes.

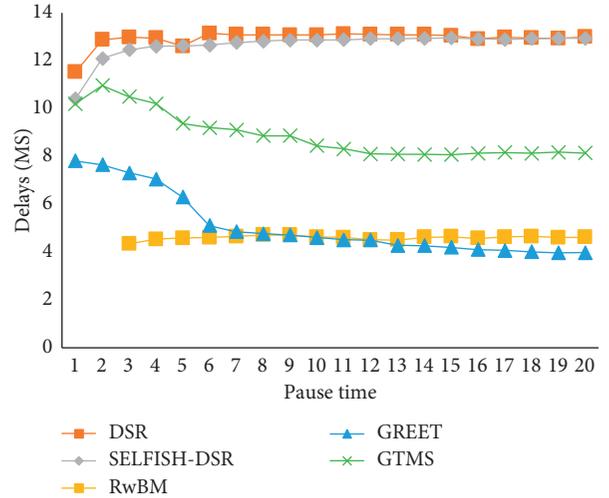


FIGURE 9: Average end-to-end delays at twenty time pauses.

and the act of selfishness is not handled properly. Moreover, in cluster scenarios it is common to have higher delays in the initial stages. RwBM and GREET are giving similar results after time pause 6. RwBM does not give the values in our simulation environment which is most likely due to the scoring mechanism and the adjustment of selfishness by each individual node. Moreover, the work is taking all the parameters of nodes which takes some time to be communicated and configured properly. One of the nodes is configured and the scoring mechanism is loaded; then the delays become similar at all the time intervals.

Figure 10 shows the end-to-end delays with respect to an increased number of nodes in a network. The results show that GREET is the only protocol that gives no effect to the delays with the changed number of nodes. RwBM is also giving somehow similar results. RwBM also uses a card system which may take some time to process. In the card system, some nodes are blocked. Node blockage can also increase the delays in a network by breaking some routes.

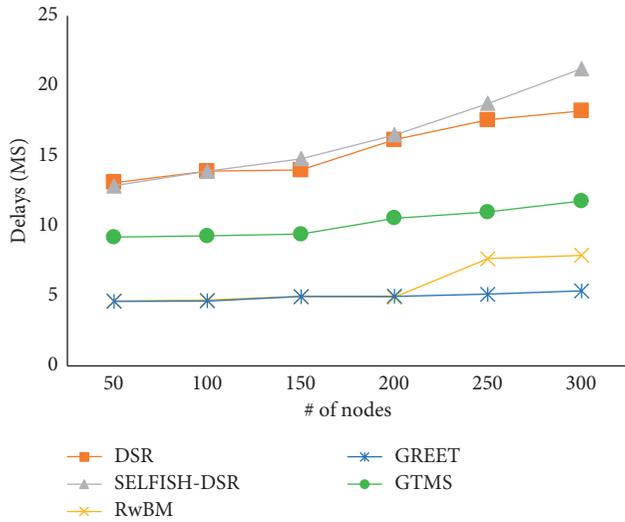


FIGURE 10: Average end-to-end delays with an increasing number of sensor nodes.

However, the change is noted at 200 and 300 nodes in the experiments. GTMS is giving similar results till 150 nodes. It is also affected by the higher number of nodes in many experiments.

Figure 11 shows the end-to-end delays with an increased number of selfish nodes in the network. A set of 100 nodes is taken for these experiments. The response ratio of delays in all the protocols is similar. Each protocol is giving a negative result due to the increased number of selfish nodes. In comparison, GREET and RwBM are giving the best results in these experiments.

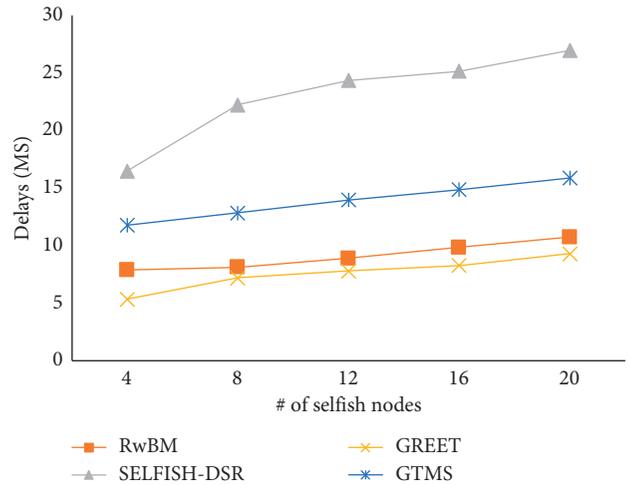


FIGURE 11: Average end-to-end delays with an increased number of selfish nodes.

5.4. Packet Delivery Ratio. PDR is the ratio of the number of data packets sent by a source node to the number of data packets received by the source node. This metric can be used to measure the success or loss rate and characterizes the efficiency and correctness of routing protocols in ad hoc networks. The higher PDR indicates the better performance of a protocol.

Figure 12 shows the PDR for each node at different time pauses. 100 nodes with 5% selfish nodes are taken. Almost all the protocols except SELFISH-DSR are giving similar PDR. Initially, GREET gives lower PDR due to its learning phase. RwBM is giving appropriate values for PDR after time pause 4. SELFISH-DSR does not keep any selfishness management; therefore, its performance in this experiment is the worst.

Figure 13 shows the PDR for each protocol with the increased number of nodes in the network. Here again, the results of all the protocols are similar except SELFISH-DSR which has lower but consistent PDR for all the sets of nodes. As the number of nodes is increased, the PDR value is also increased. It is due to the availability of multiple routes and the decreasing possibility of packet losses. All the results are taken at time pause 10 and the ratio of selfish nodes is set to 5%.

The number of selfish nodes, if increased, also does not affect the experimented protocols as shown in Figure 14. The

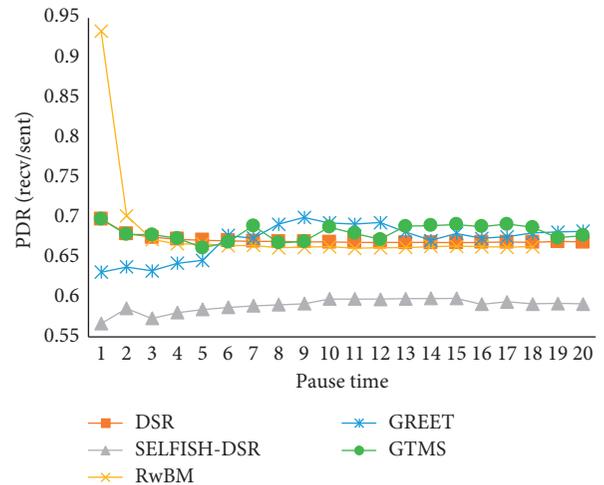


FIGURE 12: Packet delivery ratio at twenty time pauses.

PDR is decreasing in SELFISH-DSR only due to its incompleteness. In GREET, every node is a selfish node; therefore, the increased number of selfish nodes does not affect any change in its PDR value. RwBM, as usually, is giving uneven PDR for each number of selfish nodes. It is due to the provision for selfishness level adjustment and scoring and card system in the mechanism. GTMS is comparatively giving very interesting results by producing higher PDR values for the higher number of selfish nodes. Nodes operate on trust levels and selfishness is managed through reputations and trust reciprocation among the nodes.

5.5. Packet Loss Ratio. The packet loss ratio is used to get the failure rate of reception of transmitted packets. This value can be associated with signal degradation, the existence of misbehaving or selfish nodes, and routing mechanisms. In Figures 15, 16, and 17, the results are reflected by the results for PDR already discussed. Here in these experiments, the

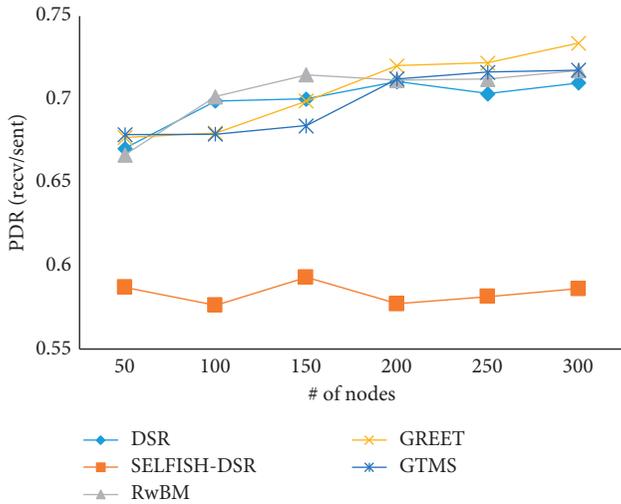


FIGURE 13: Packet delivery ratio with an increasing number of sensor nodes.

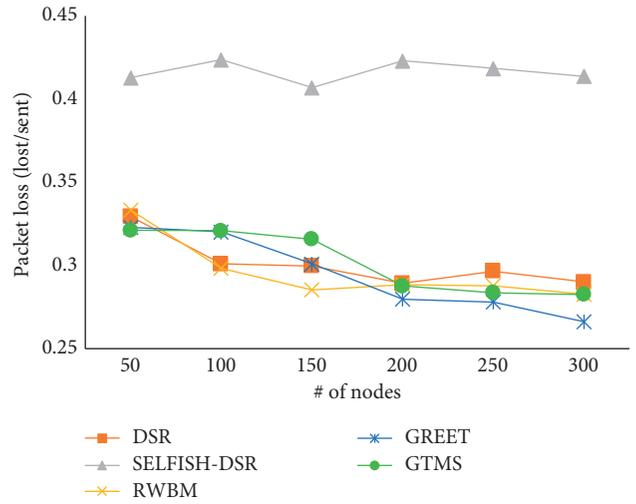


FIGURE 16: Packet loss ratio with an increasing number of sensor nodes.

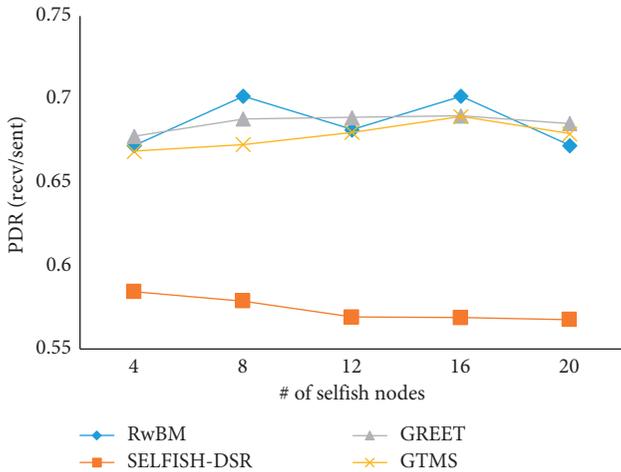


FIGURE 14: Packet delivery ratio with an increased number of selfish nodes.

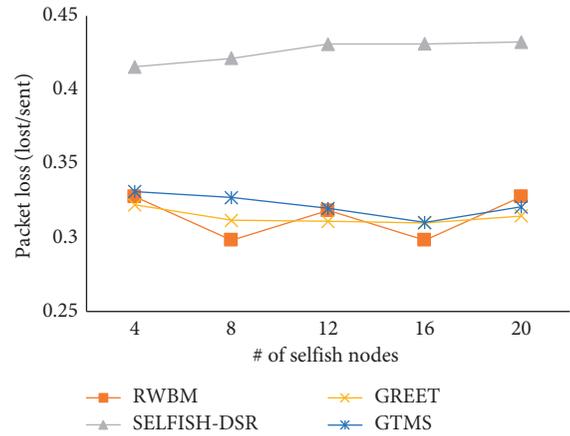


FIGURE 17: Packet loss ratio with an increased number of selfish nodes.

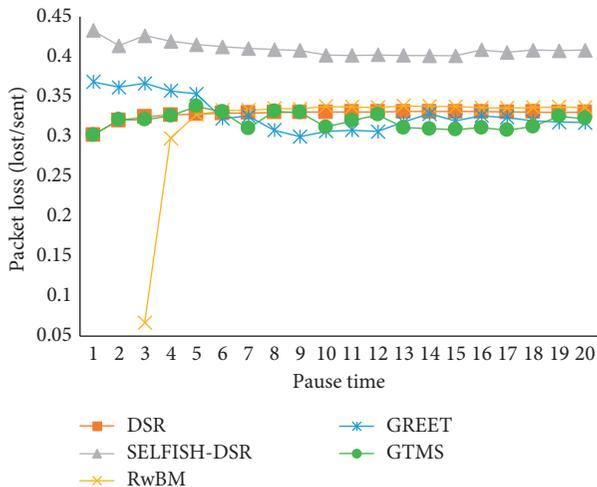


FIGURE 15: Packet loss ratio at twenty time pauses.

packet loss ratio for SELFISH-DSR is comparatively higher than other protocols. All other protocols are giving similar results in these experiments.

6. Conclusion

The existence of selfish nodes is widespread in wireless networks, particularly in ad hoc networks where an intelligent program or human controls the nodes. The nodes can be programmed to preserve their individual resources by not cooperating in the aggregate network goals. Several schemes have been introduced to overcome the issues of having such nodes in an ad hoc network. The selfish nodes can be managed either by blocking them or by stimulating them to participate in the network. In recent literature, credit-based incentive schemes are considered more effective and efficient for handling misbehaving or noncooperative nodes in ad hoc networks. Game theory is also used to realize the design and implementation of incentive-based schemes.

The incentive-based schemes can be used by opting for artificial neural networks (ANN) instead of the application of game theory. The repeated games can be replaced with an ANN module in which the neurons are trained with the passage of time. Moreover, the prevailing schemes can be interchangeably used in other forms of ad hoc networks. For example, a scheme designed for WSNs can be used in MANETs by handling the mobility or can be used in Internet of Things by considering various factors like heterogeneity and mobility. Moreover, the types of games can be changed in such schemes for better optimization of the network performance.

The simulation results show that the network performance is highly degraded without any mechanism for selfishness, as reflected by SELFISH-DSR protocol. The trust management scheme, GTMS, is giving acceptable results by addressing the target scenarios. However, it has relatively lower performance in almost all the experiments except the PDR and packet loss ratio experiments. GREET is outperforming in many experiments due to its advanced technique of letting the nodes understand the situation and adjust their cooperation level according to their benefits and the network needs. RwbM is also giving very good results due to its sophisticated technique by considering all the nodes' parameters and a state-of-the-art design of incentives for data communication. According to our experimental results, we can conclude that the selfishness of nodes can be managed by either the incentive-based or the evolutionary-based mechanisms. However, it must be noted that these experiments are made according to our understanding and cannot be considered as perfect. More work can be done in the analysis and comparisons of various protocols designed in the domain of selfish node management in ad hoc networks.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge Prince Sultan University and Smart Systems Engineering Lab for their valuable support and provision of research facilities that were essential for completing this work. Furthermore, the authors acknowledge the support of PSU for paying the Article Processing Charges (APC) of this publication.

References

- [1] N. Choudhury, R. Matam, M. Mukherjee, and L. Shu, "Beacon synchronization and duty-cycling in ieee 802.15.4 cluster-tree networks: a review," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1765–1788, 2018.
- [2] D. G. Reina, M. Askalani, S. L. Toral, F. Barrero, E. Asimakopoulou, and N. Bessis, "A survey on multihop ad hoc networks for disaster response scenarios," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, Article ID 647037, 2015.
- [3] M. M. Nasralla, N. Khan, and M. G. Martini, "Content-aware downlink scheduling for LTE wireless systems: a survey and performance comparison of key approaches," *Computer Communications*, vol. 130, pp. 78–100, 2018.
- [4] C. Zhang and J. Wang, "Energy-efficient resource allocation for energy harvesting-based cognitive machine-to-machine communications," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 3, pp. 595–607, 2019.
- [5] N. Choudhury, R. Matam, M. Mukherjee, and J. Lloret, "LBS: a beacon synchronization scheme with higher schedulability for ieee 802.15.4 cluster-tree-based IoT applications," *IEEE Internet of Things Journal*, vol. 6, no. 5, 2019.
- [6] N. Choudhury and R. Matam, "Distributed beacon scheduling for IEEE 802.15.4 cluster-tree topology," in *Proceedings of the 2016 IEEE Annual India Conference (INDICON)*, pp. 1–6, New York, NY, USA, December 2016.
- [7] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANS," in *Proceedings of the First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No.00EX444)*, Catania, Italy, July 2000.
- [8] A. Attiah, M. F. Amjad, M. Chatterjee, and C. Zou, "An evolutionary routing game for energy balance in Wireless Sensor Networks," *Computer Networks*, vol. 138, pp. 31–43, 2018.
- [9] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004.
- [10] X. Wu, G. Chen, and S. K. Das, "Avoiding energy holes in wireless sensor networks with nonuniform node distribution," *IEEE Transactions On Parallel And Distributed Systems*, vol. 19, no. 5, pp. 710–720, 2008.
- [11] G. S. Brar, S. Rani, V. Chopra, R. Malhotra, H. Song, and S. H. Ahmed, "Energy efficient direction-based PDORP routing protocol for WSN," *IEEE Access*, vol. 4, pp. 3182–3194, 2016.
- [12] M. M. Nasralla, I. García-Magariño, and J. Lloret, "MASE-MUL: a simulation tool for MovementAware manet scheduling strategies for multimedia communications," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6651402, 12 pages, 2021.
- [13] K. M. S. Huq, S. Mumtaz, J. Rodriguez et al., "Enhanced C-ran using D2D network," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 100–107, 2017.
- [14] M. Mukherjee, R. Matam, L. Shu et al., "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.
- [15] H. Gong, L. Yu, and X. Zhang, "Social contribution-based routing protocol for vehicular network with selfish nodes," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, Article ID 753024, 2014.
- [16] S. N. Shah and R. H. Jhaveri, "A survey of various approaches to detect selfishness in wireless adhoc networks," in *Proceedings of the Green Computing and Internet of Things (ICGCIoT)*, Greater Noida, India, January 2015.
- [17] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, Article ID 209436, 2014.
- [18] M. M. Umar, S. Khan, R. Ahmad, and D. Singh, "Game theoretic reward based adaptive data communication in

- wireless sensor networks,” *IEEE Access*, vol. 6, no. 1, pp. 28073–28084, 2018.
- [19] H.-Y. Shi, “Game theory for wireless sensor networks: a survey,” *Sensors*, vol. 12, no. 7, Article ID 90559097, 2012.
- [20] H. A. Muhammad, T. A. Yahiy, and N. Al-Salihi, “Comparative study between reactive and proactive protocols of (MANET) in terms of power consumption and quality of service,” in *Proceedings of the International Conference on Computer Networks*, Madurai, India, December 2019.
- [21] 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 and Decision Conference (CCDC)*, Guiyang, China, May 2013.
- [22] I. Butun, S. D. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.
- [23] K. Balakrishnan, J. Deng, and V. K. Varshney, “TWOACK: preventing selfishness in mobile ad hoc networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference*, New Orleans, LA, USA, May 2005.
- [24] J. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, “Evaluating selfishness impact on MANETs,” in *Proceedings of the International Conference on Telecommunications and Multimedia*, Xi’an, China, July 2014.
- [25] A. Mei and J. Stefa, “Give2Get: forwarding in social mobile wireless networks of selfish individuals,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 569–582, 2012.
- [26] Z. Chen, Y. Qiu, J. Liu, and L. Xu, “Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game,” *Computers & Mathematics with Applications*, vol. 62, no. 9, pp. 3378–3388, 2011.
- [27] M. Manjula and P. Elango, “A survey of selfish nodes behaviour in Mobile Adhoc network,” *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, no. 6, pp. 1848–1851, 2013.
- [28] S. J. Borah, S. K. Dhurandher, I. Woungang, and V. Kumar, “A game theoretic context-based routing protocol for opportunistic networks in an IoT scenario,” *Computer Networks*, vol. 129, pp. 572–584, 2017.
- [29] J. F. Naves, I. M. Moraes, C. V. Albuquerque, and L. e. Irf, “Políticas de gerenciamento de buffer eficientes para redes tolerantes a atrasos e desconexões,” *Simpósio Brasileiro de Redes de Computadores (SBRC 2012)*, vol. 15, pp. 293–305, 2012.
- [30] C. Sinha, “Providing social likeness within a messaging context”. U.S Patent 8600901, 3 December 2013..
- [31] Q. Li, W. Gao, S. Zhu, and G. Cao, “A routing protocol for socially selfish delay tolerant networks,” *Ad Hoc Networks*, vol. 10, no. 8, pp. 1619–1632, 2012.
- [32] Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, “The impact of node selfishness on multicasting in delay tolerant networks,” *IEEE Transactions on Vehicular Technology*, vol. 60, no. 5, Article ID 22242238, 2011.
- [33] J. M. Sánchez-Matamoros, J. M.-d. Dios, and A. Ollero, “Cooperative localization and tracking with a camerabased WSN,” in *Proceedings of the 2009 IEEE International Conference on Mechatronics*, Málaga, Spain, April 2009.
- [34] G. Brahim, A. Al-Fuqaha, M. Guizani, and B. Khan, “A model for cooperative mobility and budgeted QoS in MANETs with heterogenous autonomy requirements,” in *Proceedings of the IEEE Global Telecommunications Conference, 2008. IEEE GLOBECOM*, New Orleans, Louisiana, December 2008.
- [35] A. Al-Fuqaha, B. Khan, A. Rayes, M. Guizani, O. Awwad, and G. B. Brahim, “Opportunistic channel selection strategy for better QoS in cooperative networks with cognitive radio capabilities,” *IEEE Journal On Selected Areas In Communications*, vol. 26, no. 1, pp. 156–167, 2008.
- [36] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, “Pda: privacy-preserving data aggregation in wireless sensor networks,” in *Proceedings of the INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, Washington, DC, May 2007.
- [37] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of the MOBICOM*, Article ID 255265, New York, NY, USA, 2000.
- [38] R. A. Shaikh, H. Jameel, B. J. d’Auriol, H. Sungyoung Lee, and Y. J. Young-Jae Song, “Group-based trust management scheme for clustered wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.
- [39] Q. He, D. Wu, and P. Khosla, “SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks,” *IEEE Wireless Communications and Networking Conference*, vol. 2, 2004.
- [40] K. A. Gameda, G. Gianini, and M. Libsie, “An evolutionary cluster-game approach for wireless sensor networks in non-collaborative settings,” *Pervasive and Mobile Computing*, vol. 42, 2017.
- [41] B. Subba, S. Biswas, and S. Karmakar, “A game theory based multi layered intrusion detection framework for wireless sensor networks,” *International Journal of Wireless Information Networks*, vol. 25, 2018.
- [42] R. Raja and P. G. Kumar, “Designing a novel framework for evaluation of trust in mobile ad-hoc networks,” *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 1, pp. 338–344, 2018.
- [43] W. Li and H. Song, “ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2015.
- [44] S. B. Boudec and J.-Y. Le, “Performance analysis of the CONFIDANT protocol,” in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing - MobiHoc ’02*, New York; NY; USA, July 2002.
- [45] Y. B. Saied, A. Oliveureau, D. Zeghlache, and M. Laurent, “Trust management system design for the Internet of Things: a context-aware and multi-service approach,” *Computers & Security*, vol. 39, pp. 351–365, 2013.
- [46] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, “A secure credit-based cooperation stimulating mechanism for MANETs using hash chains,” *Future Generation Computer Systems*, vol. 25, no. 8, pp. 926–934, 2009.
- [47] L. Yang, Y. Lu, L. Xiong, Y. Tao, and Y. Zhong, “A game theoretic approach for balancing energy consumption in clustered wireless sensor networks,” *Sensors*, vol. 17, no. 11, p. 2654, 2017.
- [48] Q. L. X. Yu, “An incentive mechanism game theory based for cooperation in wireless ad hoc networks,” in *Proceedings of the 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Datong, China, October 2016.
- [49] Q. Xu, Z. Su, and S. Guo, “A game theoretical incentive scheme for relay selection services in mobile social networks,”

- IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6692–6702, 2016.
- [50] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection,” *IEEE Transactions On Network And Service Management*, vol. 9, no. 2, pp. 169–183, 2012.
- [51] L. Buttyán and J.-P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks,” *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.
- [52] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: a simple, cheat-proof, credit-based system for mobile adhoc networks,” in *Proceedings of the IEEE INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, San Francisco, CA, USA, March 2003.