Received March 24, 2018, accepted April 29, 2018, date of publication May 7, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2833468

Game Theoretic Reward Based Adaptive Data Communication in Wireless Sensor Networks

MUHAMMAD MUNEER UMAR[1], SHAFIULLAH KHAN[1], RASHID AHMAD[2], AND DHANANJAY SINGH[3], (Senior Member, IEEE)
[1]Institute of Information Technology, Kohat University of Science and Technology, Kohat 26000, Pakistan
[2]Department of Physics, Kohat University of Science and Technology, Kohat 26000, Pakistan
[3]Department of Electronics Engineering, Hankuk University of Foreign Studies, Yongin 449-791, South Korea

Corresponding author: Dhananjay Singh (dsingh@hufs.ac.kr)

This work was supported by the Hankuk University of Foreign Studies Research Fund 2018.

ABSTRACT Selfish or non-cooperative behavior of nodes can degrade the performance of a wireless sensor network in many ways. These nodes can cause increased end-to-end delays and unfair energy consumption among the nodes due to higher packet loss ratio and non-utilization of optimal routes. Various nodes' stimulation techniques have been proposed. Credit-based incentives with game theoretic approaches are said to be more effective in such experiments. This paper introduces a game theoretic reward-based mechanism to balance the work load among network nodes by stimulating them to equally cooperate in data forwarding toward the base station. Various possible parameters associated with a network and its nodes are considered. In addition, a card-based punishment system is introduced, which is rationally applied on the nodes according to their individual importance in the network. A new technique for finding nodes' individual importance in the network is designed for better manipulation of nodes.

INDEX TERMS Wireless sensor networks, routing, routing protocols, energy efficiency, selfish nodes, game theory, incentive-based routing.

I. INTRODUCTION

Wireless sensor networks (WSNs) are composed of small sensing devices installed for a variety of purposes. Mostly, such networks are deployed for sensing environmental changes in a periodic fashion. WSNs can be applied in military, industry, forestry and vehicle tracking etc. for various motives. A WSN may consist a very large number of self-organizing nodes and a central station known as base station (BS) [1]. Each node in such networks operates on a limited set of battery life, processing power, wireless transmission and data storage capacity [2]. These sensing nodes are usually disposable and kept dedicated for some ad hoc purposes. Therefore, the manufacturers try to put less costs on making such nodes [3].

In WSNs nodes generate, send, forward and receive data packets while coordinating and cooperating with each other. Since most of the nodes don't lay in the transmission range of the BS, therefore, they need others' cooperation to connect the BS. It is always assumed that the nodes in an ad hoc wireless network, like WSNs, must cooperate with one another for smooth operations of the network [4]. Such cooperation for data forwarding is known as multi-hop communication. The procedure for forwarding data packets in WSNs can be defined in different ways by various routing protocols. Beside this distinctive facility, nodes in such networks usually operate on very limited battery life. While performing in a network, some nodes do involve too much in the packets forwarding operation, which ultimately shorten their lives. On the other hand, some nodes are always kept idle due to their inappropriate locations in the network or their non-cooperative behavior. Idle nodes keep their energies at the higher peak but in return they don't contribute in the network operations [5].

The communication for battery operated nodes is usually very costly. To transmit a bit over a distance of 10 to 100 m, a node consumes more energy than performing millions of arithmetic operations [6]. A node can save its energy by reducing its operations, particularly by not cooperating in packet forwarding function. Such non-cooperative nodes are known as selfish nodes. Selfish nodes try to keep their energies for their own data transmission while not entertaining others' requests for packet forwarding. A selfish node would like to be benefitted by the network but would not input its role in the network. Such nodes may not have any intention for damaging the network but their continuous selfishness greatly affect the performance of other nodes. On the other side, the selfish behavior is very beneficial for some nodes. With this manner they extend energies for a period of time. Moreover, such behavior can be embedded in all the nodes up to some extent, if it does not lower the overall network performance [7].

A single node with constant selfish behavior can take the probability of packet dropping up to 100 %. While this probability ratio drops with a growth in the density of nodes in the network [8]. Moreover, if a node's selfishness is interrelated to its energy level then there will be notable reduction in the ratio of packet drops. Multiple Threshold Selfishness refers to the dynamic behavior of a node operating on multiple levels of selfishness [8]. Selfish nodes can degrade a network's performance by unbalancing the energy consumption and increasing the end-to-end delays and packet drops. Additionally, selfish nodes can increase the overhead on some nodes by pushing them to repeat the forward requests and route discovery operations.

For analysis of resource management in wireless networks, various approaches can be applied. Among these game theoretic approaches are being considered as popular for getting decent outcomes. Generally, game theory was used for financial matters directly connected with economic problems. In recent research, this theory is used for non-economic statistics associated with wireless networks [9]. The nodes are always desired to be energy efficient in the network while do contributing in well manners. Since energy is highly wasted due to cooperation for data forwarding. Therefore, in such conflict of interest invites the game theoretic mechanism to be implemented in the network [10]. Game theory can also be used to analyze the gains and losses among the nodes and can lead towards the achievement of equilibria for all the concerned nodes. For selfish nodes management, game theory has been used in various articles. Incentive based mechanism has been successfully applied in many approaches for load balancing, energy efficiency etc. in wireless networks. Such mechanisms are categorized into credit-based and reputation based [11].

The main objective of this work is to stimulate all the network nodes to cooperate in the network. This scheme can be used to balance the workload among all the nodes to enhance the energy consumption and prolong the networks' life. A game theoretic reward based mechanism, grounded on fundamental parameters of the involved nodes, has been introduced. In this scheme, each source node is given some scores by the BS on reception of the sensed data. Nodes collect and pay these scores in the forwarding service. The intermediate nodes after doing some bargaining on the volume of scores, forward data packets for the source nodes. Nodes having less scores may not be able to pay the intermediate nodes for forwarding their data packets. Therefore, each node considers its energy level and tries to increase its scores by involving itself in the forwarding operation, accordingly. The entire work of scoring mechanism focuses on an adaptive and rational data transmission. A game theoretic approach based on Rubinstein Sthal bargaining model is used to analyze the overall mechanism. Moreover, this work introduces a card system through which highly selfish nodes can be blocked by BS or black listed for other nodes. The decision for allotting cards is also highly influenced by the importance of the concerned nodes.

The remainder of this paper is organized as follows: related work is in section II. In section III the preliminaries are given. These are the building blocks for the proposed mechanism. Section IV describes the whole mechanism. While section V gives mathematical and procedural formation of the mechanism. In section VI simulation results are discussed. Lastly, section VII includes the conclusion and future work.

II. RELATED WORK

A remarkable work has been done in the area of selfish node management in wireless ad hoc networks and WSNs specifically. The incentive based techniques are usually used for stimulating nodes to cooperate in the network. These methods can be characterized into two techniques. The first one is based on the reputation mechanism and the second on is credit mechanism [12], [13]. The reputation-based mechanism relies on the evaluation of nodes' behavior. In these type of approaches, different reputation stages are made to determine the nodes' cooperation level. The forwarding services by intermediate nodes are made according to the reputation value of the source nodes [14], [15]. In the credit-based mechanism, the nodes gain credit scores by offering relaying services. Some researches like [16] refer these credits as virtual currency.

A reputation-based approach Watchdog and Pathrater [17] is proposed to lessen the problem of routing errors by detecting unwanted behavior of the nodes in ad hoc networks. Watchdog is used for the detection process while pathrater is used to block the malicious and selfish nodes from the routes. This work only blocks the non-cooperating node while does not contain any adaptive rational routing or stimulating mechanism for nodes. CONFIDANT [18] approach is an updated on-demand routing protocol. This technique purely quarantines selfish or non-participating nodes. Four main modules are used in each node to tackle the whole management. This technique also does not effectively stimulate nodes for cooperation in the network.

According to some authors like [19], reputation- based approaches have some major issues. The foremost issue is that these approaches do not complete evaluation mechanism in proper means. The second known defect is the structuring a group of nodes being involved in a scheme to maximize their helpfulness. The third flaw is that these schemes can consume more energy of nodes with the excessive use of antennas. While in credit-based approaches, the nodes can perform more rationally by exchanging some values with one another. The credit-based mechanism beats the reputation-based and many researchers have exposed particular interest in such techniques [19], [20].

In Nuglet technique [21], a node can only be allowed to initiate its own data when it forwards sufficient data packets for other nodes. The terms packet trade and packet purse are used in this work. In packet purse the initiating source nodes puts some credit. Each forwarding node grabs its share from the credit score available in the purse. In packet trade model, the forwarding nodes make a chain of buyers and sellers in a hierarchy. This scheme does not include any central observation from the BS. Therefore, a tamper proof hardware is required for each node to make sure that credits are not falsely added or subtracted.

The authors in [5] proposed an incentive based mechanism for detection and punishment of selfish nodes in WSNs. The detection module collects the maximum average value of retransmission number of nodes and do comparisons accordingly. The strategy of selfish nodes is changed by the punishment module so that they cooperate like normal nodes in the network. The work is purely focusing on these two modules while does not consider important parameters like energy, importance of nodes' location and routes for nodes in the network.

Lin *et al.* [22] in their work "a Game Theory-based Real-time & Fault-tolerant (GTRF)" focus on the real-time successful transmission in WSNs. The nodes' behavior is regulated by applying a game theory model in the first stage. While in the second stage real-time delivery of data packets is ensured by adopting a jumping transmission method. This work is purely implied in cluster based WSN.

In research article [23], the authors propose a mechanism based on evolutionary game. In this work each node has assigned three main strategies as a part of the game. The nodes learn and update themselves about a part of the game states. These states are further used to determine the fitness of strategies. The nodes can adjust their selfishness level by considering their energies and storages.

A trust-based routing protocol [24] proposes a game theoretic approach to detect the nodes having non-cooperating or abnormal behavior. This scheme applies the repeated games to separate malicious nodes through the analysis of their trust and cooperation level. The method is purely focusing the maliciousness of nodes and does not work on the stimulation of non-cooperating nodes in WSNs.

Various popular game theoretic proposed schemes are punishment-based. These use a strategy known as Tit-for-Tat (TFT) to punish non-cooperative node [25], [26]. In TFT strategy, a node takes similar action (cooperative or selfish) according to previous node. It is done in such a technique that a node cooperates in the first stage and the next action relies on the behavior of opponent in the following stage. The technique does not rely on incentive mechanism. The authors gave considerable results for their approaches. Since the main concern is achieving nodes rationality and selfishness management by using game theory. It is possible that such strategies may not stimulate rational nodes for cooperation more effectively.

Anderegg and Eidenbenz [27] propose Ad hoc-VCG protocol for stimulating nodes to cooperate in the data forwarding operation in an ad hoc wireless network. Ad hoc-VCG is a cost-efficient reactive routing protocol for achieving truthfulness and real cost for forwarding data in the network. The mechanism involves sealed price auction activities. Another nodes' stimulation technique is introduced by Buttyan and Hubaux [28]. In this technique a simple counter is used. The counter increases its value on each forward operation while on sending own data its value is decremented. This counter is an additional hardware module attached with each node. The nodes try to maintain their counters by forwarding others data frequently. Zhong *et al.* [29] introduce a new protocol known as Sprite to manage selfish mobile nodes by providing incentive to them. By using game theory, each node is encouraged to report its actions fairly. The work also introduces a centralized clearing center for credit and balance management.

III. PRELIMINARIES

This section gives the details of fundamentals relating to the main mechanism of our work. It is divided into two major segments as: assumptions and factors.

A. ASSUMPTIONS

In this work, a simple WSN having a finite number of $\boldsymbol{n}$ nodes is considered. Each node has a unique identification number $\boldsymbol{i}$ in the network N ($i \in N = \{1, 2, 3 \ldots, n\}$). The network may include fewer to thousand number of mobile nodes. All the nodes wirelessly communicate with each other. Each route R, from source to the BS, may consists some number of intermediate nodes.

The nodes' participation is evaluated by considering the sequence of all involved nodes in a data transfer transaction. Therefore, the basic principles of Dynamic Source Routing (DSR, RFC 4728) protocol are used for the fundamental routing functionalities in the network. Moreover, researches indicate that DSR protocol costs lesser than AODV protocol in WSNs [30]. For control message passing the Optimized Link State Routing Protocol (OLSR, RFC 3626), has been used. Scores among the participants in the network are distributed through control messages.

This is the foremost priority of each node to have transmitted its own sensed data to the BS in the possible shortest period of time. However, the nodes may be given an option to contribute in data forwarding process or behave selfishly. The value of selfishness of node $\boldsymbol{i}$ can be denoted as Sel_i.

It is assumed that nodes are not liars. Each node has to keep the value for its participation in the network. However, such values related to each individual node can also be calculated at BS at any time.

Different hardware provides different energy levels in mobile devices, but this cannot be said as the source of imbalanced consumption of power in the network. Imbalanced energy consumption is very common is such type of networks having multi-hop communication. In this work it is assumed that each node $\boldsymbol{i}$ is operating on limited battery power E_i. It stores the percentage values of the remaining energy of a node $\boldsymbol{i}$.

Nodes are divided into their hop-levels. A node having direct connection with the BS will have hope-level equal to 1. Nodes having one intermediate node towards BS will have hop-level equal to 2. At extreme level a node can have n hop-level in the network. Each sensor node keeps some storage space for routing and control purpose. Beside the fundamental routing information, the nodes must be able to store information about their neighbors' location, energy levels and demanding scores. Also, the nodes must be able to calculate their own scores in this approach.

B. FACTORS

For each node in the network, some values are calculated during their status change and activities. These values are formalized by considering seven major parameters associated to nodes. These parameters are referred as factors. The scores in the major mechanism depend on these calculated factor values. These factors are (a) energy of nodes, (b) the participation level of nodes (c) the significance of routes (d) density and importance of nodes (e) the number of transfer attempts (f) the hop-levels of nodes and (g) the selfishness level of each individual node. The nodes adjust their selfishness factor rationally. This factor does not need any formalization.

Other factors during calculation are further multiplied with a coefficient β. This multiplier is used to adjust the importance of these factors in overall mechanism. The value of β can affect a factor in various ways as stated in table I. The β multiplier can be adjusted according to the needs of a network. For example, if we want to put less importance to the energy of nodes in the system then it can be set to the smallest value. However, in most of the cases β is considered as equal to 1.

TABLE 1. Effects of beta on factors.

Value	Effects of a factor
$1 < \beta$	Importance Increased
$0 < \beta < 1$	Importance Decreased
$\beta = 0$	Factor is Eliminated
$\beta = 1$	No change in the importance

1) ENERGY FACTOR

Each node has a limited remaining level of energy. E_i denotes the remaining percentage energy of node i. The equation for energy factor of node i at time T can be as following:

$$FaE_i^T = \beta_E * E_i \tag{1}$$

2) ROUTE IMPORTANCE FACTOR

This factor is used to determine an optimal route for node i towards the BS with highest energy and least number of hops. It is not necessary that the node must use this route. The route selection depends upon the scoring mechanism discussed in next sections. For each route from node i towards BS, the sum of energies and hop-levels of involved nodes are considered. Value of optimal route OpR_i can be calculated by taking the highest value among all the calculated routes for node i. Equation (2) shows the optimal route as following:

$$OpR_i = max\left[\frac{\sum_{j=1}^{l} E_j}{\sum_{j=1}^{l} HopLevel_j}\right] \tag{2}$$

In this equation the energies of all nodes $j = \{1, 2, 3, \ldots l$ lying in a route are added and then divided by the sum of their hop-levels. The route importance factor for node i at time T can be calculated by multiplying the coefficient β_R with OpR_i as shown in (3).

$$FaR_i^T = \beta_R * OpR_i \tag{3}$$

3) NODES' DENSITY AND IMPORTANCE

If there are densely deployed nodes at certain positions in the network. It is sure that they will get relatively similar sensed data and same relaying requests by the source nodes. In such scenarios omission of one or few nodes does not affect the overall network performance. Therefore, we can say that some of such densely deployed nodes can be given less importance. Moreover, nodes having less energies or having closed neighbors(CNs) with higher energies will also have likely less contribution in the network. In this factor, for each node $\boldsymbol{i}$ a set of closely connect nodes i.e. CNs are calculated by using the simple distance formula as shown below:

$$D_{i,j} = \sqrt{(x_i - x_j)^2 - (y_i - y_j)^2} \tag{4}$$

$$CN_i = \{j : D_{i,j} \le DIST_{tr}\} \tag{5}$$

CN_i are all those nodes which lay in a specified threshold distance $DIST_{tr}$ with node $\boldsymbol{i}$. The value of $DIST_{tr}$ can be adjusted according to network size, nodes transmission range and their placement pattern. For example, $DIST_{tr}$ can be given a lower value in case of densely deployed nodes. In another case, if we give this value equal or higher to the transmission power of nodes then it will be useless and will not give any considerable results. The importance of a node is calculated by considering the energy of node $\boldsymbol{i}$ with the sum of energies of its CNs multiplied with their number cn at a specified time period t. The energy levels of CNs and their frequency can put direct impact on a node's individual importance. If a node has higher value of cn, means more CNs, then it will have less importance. The node importance λ_i^t for a time period t is show in (6).

$$\lambda_i^t = \frac{E_i^t}{cn \sum_{j=1}^{cn} E_{CNj}^t} \tag{6}$$

Higher value of λ_i^t indicates the likelihood of having low energy of node and/or low number of CNs. Moreover, higher energies of CNs also decreases the value of node importance. We can simply say that a node's individual importance has direct relation with its energy level, while inverse relation with the number of CNs and their energy levels. Hence, this factor needs to be incorporated as it is in the proposed scheme. Therefore, it is not multiplied with the coefficient.

4) PARTICIPATION FACTOR

Participation of node i can be calculated by considering the total number of forward transmissions and total requests to node $\boldsymbol{i}$ and its CNs. Below formula can be used to calculate the value of participation p_i.

$$p_i = \frac{TPF_i}{(TFR_i)^2}\left[\sum_{j=1}^{cn}[TFR_j] - \sum_{j=1}^{cn}[NMFR_j]\right] \quad (7)$$

In (7) TPF denotes the number of total packets forwarded, TFR stands for total forward requests. The technique also sums up the TFR of each CN. $j = \{1, 2, 3, \ldots cn$ is a set of all possible CNs of node i. Moreover, some CNs may get forward request non-mutual to node $\boldsymbol{i}$. NMFR are these non-mutual forward requests to CNs. Equation (8) shows the participation factor.

$$FaP_i^T = \beta_p * p_i \quad (8)$$

5) TRANSFER ATTEMPTS COUNTER

A simple counter is used for considering the repeated transfer attempts by a single node. The transfer attempt counter TCr_i starts from 1 on first transfer attempt and reaches to the last limit referred as counter limit CrL i.e. $1 \leq TCr_i < CrL$. The transfer attempts factor can be calculated by multiplying it with the coefficient β_{TCr} as shown in (9).

$$FaTCr_i^T = \beta_{TCr} * TCr_i \quad (9)$$

6) HOP-LEVEL FACTOR

The nodes are divided hierarchically in the network. As stated earlier each node has been given a hop-level. The value of hop level for each node is used in the main scheme for calculation of scores. The nearest nodes to the BS having direct connection are said to be having hop-level equal to 1. At maximum the value can be total number of nodes (n) in the network.

$$1 \leq HpL_i \leq HpL^{max} \quad (10)$$

A node having hop level HpL^{max} means that it is at the bottom most level. Such nodes usually don't connect any backward nodes so usually do not perform forwarding operation. However, in some cases these nodes may cooperate their sibling nodes of same hop. Equation (11) shows the hop-level factor for node i.

$$FaHpL_i^T = \beta_{HpL} * HpL_i \quad (11)$$

7) NODES' SELFISHNESS

The value of nodes' selfishness is adjusted by the nodes independently. It has no effect on the reward scores (RSc). However, higher value of node selfishness leads to higher demand of score for forwarding operation. Since it is entirely set by nodes rationally. Therefore, this parameter is not multiplied with any coefficient. Usually selfish nodes set this value at the peak so that they demand too much during bargaining for forwarding operation.

IV. PROPOSED MECHANISM

The major motivation of this work is to consider all the possible parameter as stated in the previous section and then design a bargaining and monitoring system to manage the selfish nodes in a network. The selfish nodes are stimulated by pushing them to cooperate by using a scoring system. Moreover, nodes are assigned cards based on their calculated participation factor.

Fig. 1 gives a general look of our model in which sensor nodes are connected with the BS directly or through other nodes. In this approach BS knows about all the parameters associated to each node and gives rewards to the source nodes accordingly. The BS may charge a score for accepting data from some nodes. This score charging is referred as *BASEPRICE* and explained later in the article. S1, S2 and S3 are selfish nodes. S3 is alone in the route and may have some considerable energy level therefore it has given more importance than the other two selfish nodes. BS assigns red cards to S1 and S2 for their selfishness. S3 has higher importance therefore it is given a yellow card. X, the source node, pays F1 after a bargaining session with F1 and F2 for forwarding its data. F1 further pays F12 for the same data packet forwarding.

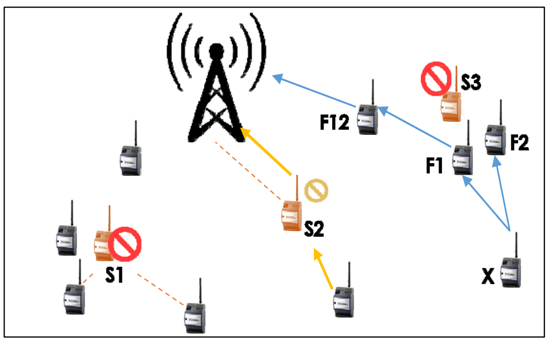

FIGURE 1. Overview of the proposed scheme.

This section is divided into card management, scoring mechanism, RSc, the game model and bargaining among the nodes.

A. CARD MANAGEMENT

Each node is assigned a card either green, yellow or red. Normal nodes in the network are considered to have green cards. While nodes not participating or returning a less amount of participation factor are assigned yellow or red cards. The card type is updated periodically after a time interval t. The importance of each non-cooperating node is calculated before changing their card status. Yellow cards are given to those nodes which do not cooperate but do keep the advantage of a higher level of importance λ. The network always keeps a hope from these nodes and consider that they may start contribution at some stage. The BS does not announce these nodes as blacklisted. Such nodes can be requested for data forwarding by their neighbors. However, the BS station does not accept their own initiated data. This act of BS can be said as punishment for such nodes. Red cards are given to those nodes which are non-cooperative and do not have enough level of importance factor. These nodes can be easily eliminated from the network. The BS blacklist such type of nodes for a period of time t. The BS broadcast the red card holding nodes among their neighbors. Such nodes don't get any message from their neighbors. Since the BS keeps track of all the transmission in the network. It can also allot a red card, if a node violates an already established session. Such type of violation can be detected by the BS in three ways: (a) by sending an enquiry control packet to the involved nodes through alternate routes (b) by receiving a report from the source node. The source nodes may connect the BS through alternate routes and (c) the intermediate forwarding nodes may report to the BS about the unfortunate breakage of the session.

B. SCORING MECHANISM

Each node keeps some virtual money referred as score. Scores are exchanged by the nodes while doing some cooperation for data transfer towards the BS. If a node wants to transmit its own data, it must give some score to all the involved intermediate nodes in the route. The involved nodes also keep a demanded limit for such cooperation. Each involved node gains some scores by giving the relying service to others. The demanding scores are replied to each route requesting node. The nodes consider their energies and set their selfishness values for calculating their demanding scores.

C. REWARD SCORES

An *RSc* is assigned to each source nodes by the BS station on reception of sensed data. Nodes pay some of their gained scores to the intermediate nodes for their forwarding service. The *RSc* is calculated by the BS based on the calculated parameters. The *RSc* assignment is made is such a way that all the nodes are treated according to their locations.

D. THE GAME MODEL

In the work, a game theoretic model for stimulating nodes to cooperate in the network has been used. A typical game consists of players, strategies and a payoff function. Since, it is assumed that all nodes are part of the network and input some performance, therefore the nodes can be considered as the players. The players can be divided into four possible sets i.e. (a) source to forwarders (b) forwarder to forwarders (c) forwarder to BS and (d) source to BS. In each case a single player makes direct interaction with one or a set of similar players. The set of players can be denoted as a set of positive integers where each node has an id i i.e. $N = \{i\}$ where $i = 1, 2, 3, \ldots n$. Each player operates on some strategies. These strategies are based on the parameters already formulized in earlier section. The variations in the factors for each node can be said as a set of strategies for it. For each node i a strategy set can be made as $S_i = \{S_i^j\}$ where j is a finite number of strategies associated with node i. The set of all possible strategies for all players can be said as $\gamma = \{S_i^*\}$. This work is using a Rubinstein-Stahl bargaining game for relaying function among the nodes towards the BS. At each stage bargaining on the scores is made between the sender and forwarders

E. BARGAINING AMONG NODES

The BS initially sets a reward score for each source node. The gained reward score is added up with the present score of the node. For data transfer, the source node broadcasts a forward request to all its one-hop up neighbors. Nodes upon receiving such requests, reply with their *IBSc* to the source node. The source node selects a forwarder having the least *IBSc*. It is possible that the node may not have enough score to pay any forwarder. In such case the node then tries its same-hop neighbors. Nodes with less amount of scores usually can't make a deal with any forwarder. To increase their scores, such nodes then start reduction in their selfishness level and try to give relying service to others. These nodes also do attempt again for the same request. As stated, the BS increases the value of reward score on each repeated attempt by considering their particular attempt factor. A *BASEPRICE* is also set by the BS for its direct score deduction from the source node. Since some nodes may not need any forwarders, therefore, this amount can be used to control their act in the network.

V. FORMALIZATION OF PROPOSED MECHANISM

This section includes the quantitative formulas and procedures used for the formalization of our proposed work. As reflected by the previous section, the section is similarly divided into card management, scoring mechanism, *RSc*, and game based bargaining among the nodes.

A. CARD MANAGEMENT

The BS periodically checks and updates the cards assigned to each node. The red cards are reverted to yellow cards after a specified period of time. This card reversion is done

Algorithm 1 Assignment of Cards

1. *If* $\mathrm{Card_i} = \mathrm{RED}$ *then*
2. SET $\mathrm{Card_i} = \mathrm{YELLOW}$
3. *Else If* $FaP_i^T \leq \mathrm{Part^{tres}}$ *then*
4. *If* $\lambda_i^t \leq \lambda^{tres}$ AND $\mathrm{Card_i} = \mathrm{YELLOW}$ *then*
5. SET $\mathrm{Card_i} = \mathrm{RED}$
6. *Else*
7. SET $\mathrm{Card_i} = \mathrm{YELLOW}$
8. *End If*
9. *Else*
10. SET $\mathrm{Card_i} = \mathrm{GREEN}$
11. *End If*

for seeking a hope from a selfish node and giving them an opportunity to become normal nodes again. Algorithm I is used for assignment of cards.

Yellow cards are given by checking their importance factor. For assigning a card the participation factor FaP_i^T is compared with a threshold participation ($Part^{tres}$) value. $Part^{tres}$ can be adjusted according to the network features. Densely deployed networks may not need too much cooperation of nodes, therefore this value can be kept at lower level. Table II shows the impact of factors on the cards management mechanism.

TABLE 2. Impact of factors on the cards assignment.

Factor	Impact
Energy	No Consideration
Route Importance	No Consideration
Participation	Higher level of participation factor leads to a little chance of having a yellow or red card
Nodes' Density	Higher λ leads to lower chances of red card. However, the nodes can get a yellow card with higher λ
Transfer Attempts	No Connection
Hop Level	Not Calculated
Selfishness Value	Not Calculated

B. SCORING MECHANISM

Equation (12) describes the demand score referred as Individual Bargaining Score (*IBSc*) of node ***i*** at time ***T***. This value is calculated by considering the parameters: hop-level, selfishness level and remaining energy of node ***i***. The energy is also multiplied with the number of CNs (***cn***) for putting the impact of nodes' density in the equation.

$$IBSc_i^T = \frac{FaHpL_i^T \times Sel_i}{cn \times FaE_i^T} \tag{12}$$

Table III shows the impact of factors on the scoring for an individual node.

TABLE 3. Impact of factors on IBSc.

Factor	Impact
Energy	Lower energy leads to higher value of IBSc
Route Importance	No direct impact
Participation	No impact
Nodes' Density	Higher λ means the source has more options from forwarders. The forwarder nodes give likely lower scores
Transfer Attempts	No impact
Hop Level	Higher hop-level will give higher demand for scores
Selfishness Value	Direct impact on the IBSc of a node. Higher selfishness values give higher scores

C. REWARD SCORES

At a specific time T the *RSc* for node ***i*** can be calculated as shown in (13).

$$RSc_i^T = \frac{FaTCr_i^T \times FaHpL_i^T \times FaR_i^T}{FaE_i^T} \times fb_i \tag{13}$$

The *RSc* for a node can be obtained by considering the factors: transfer attempts (FaR_i^T), hop-level (FaR_i^T), route importance (FaR_i^T) and energy factor (FaR_i^T) of the node. Additionally, a term *fb* is multiplied which is the ratio of connected forward neighbors to the backward neighbors of certain node. The ratio gives the weightage of forwarding options for a source node and can be calculated as:

$$fb = \frac{number\ of\ forward\ Nodes + 1}{number\ of\ backward\ Nodes + 1}.$$

The neighbors directly connected with node i laying in upper and lower hops are considered in this ratio. The nodes' energy level has inverse relation with their rewards. It is because node having higher energies will be given less rewards so the BS pushes them to gather scores by offering relaying services. Table IV shows the influence of factors on the values of reward score for a node.

TABLE 4. Impact of factors on RSc.

Factor	Impact
Energy	Higher energy means that the node can live longer so the BS gives lesser RSc.
Route Importance	BS tries to utilize the optimal routes on priority basis. For higher values of this factor, the nodes are given higher RSc.
Participation	No impact on the *RSc*
Nodes' Density	The ratio of forward neighbors to the backward neighbors is considered, instead.
Transfer Attempts	For each new repeated transfer attempt, the value of *RSc* is increased.
Hop Level	Higher hop-level means that the node needs more intermediate forwarders. A higher *RSc* is given for higher hop-level.
Selfishness Value	Not Calculated for Reward Score

D. GAME BASED BARGAINING

Equation (14) shows the *BSc* for node i at time T.

$$BSc_i^T = BASEPRICE + IBSc_j^T + \omega_j \tag{14}$$

BASEPRICE is rationally set for immediate nodes with the BS. For the rest of the game formation this value is kept as equal to zero. Since it is sure that each forwarding node may depend on some other forwarding nodes towards the BS. ω_j denotes the sum of minimum possible bargaining scores in each consecutive upper hop level from node j. ω is repeated for each upper level as shown in (15).

$$\omega_j = MIN\left[IBSc_{j-1}^T + \omega_{j-1}\right] \tag{15}$$

The hop-level one nodes pay a *BASEPRICE* only and this value can be considered as an *IBSc* of upper node for them.

In a single session of data transfer the involved nodes i.e. the source and the forwarders gather some scores. These scores can be considered as benefits. The benefits for both parties can be said as two parts of the RSc. In (16), b_i is the benefit value for node i, while b_{Fi} is the share of benefit for the forwarder nodes.

$$RSc_i^T = b_i + b_{Fi} \tag{16}$$

The source node may get an *RSc* that does not fulfill the demand i.e. *BSc*. In such case the node must use its own earned score for forwarding purpose. So, the value of b_i can be negative in such case. The value of b_{Fi} is directly connected with *IBSC*, therefore, it cannot be negative. Equation (17) shows the possible set of possible benefits for source and forwarders in the first round upon finalized deal.

$$\mathrm{X} = \{(\mathrm{x}_S, \mathrm{x}_{Fi}) \in \mathrm{R} : \mathrm{x}_{Fi} > 0, \mathrm{x}_S \in \mathrm{R}\} \tag{17}$$

The bargaining may run several times. Each time the node may get increased reward, if the transfer attempt factor is considered. This repetition is a major aspect in Rubinstein Stahl model. Since each repetition consumes some amount of energy, therefore the amount of benefit for both parties decreases.

After a failure at time period t, the benefits for both players shrink from X_t to $\mathrm{X}_{t+\delta}$ as stated in the equation below:

$$\mathrm{X} = \{(\delta \mathrm{x}_S, \delta \mathrm{x}_{Fi}) \in \mathbb{R} : \mathrm{x}_{Fi} > 0, \mathrm{x}_S \in \mathbb{R}\} \tag{18}$$

δ can be said as the margin of loss due to each increase in the round for the source and the forwarders. It can be assumed $0 < \delta < 1$ as stated by [31]. The ultimate value of δ can become equal to zero, if the deal has not been made. The utility function for source node in our work can be made as in (19).

$$\mathrm{u}_S = \left[RSc_S^T - MIN(BSc_s^T)\right] \times \delta_S^{FaTCr-1} \tag{19}$$

Similarly, the utility function for each forwarding node can be defined by (20).

$$\mathrm{u}_{Fi} = \left[IBSc_{Fi}^T\right] \times \delta_{Fi}^{FaTCr-1} \tag{20}$$

The value of δ is dependent on the number of rounds i.e. the transfer attempts factor.

The possible number of rounds can be dependent on the link availability. We can say that for each round in the bargaining involved players consume t_R amount of time. By considering the method from [32] we can calculate the maximum possible rounds for a deal between the source and the forwarder.

$$R = Int\left(\frac{TL_{S,Fi} - Lm/B}{\mathrm{t}_R}\right) \tag{21}$$

Equation (21) gives us the integer value for maximum number of rounds. $TL_{S,Fi}$ is the link duration between the source and each forwarder. *Lm* is the length of message m, while B denotes the bandwidth of the link.

In Rubinstein-Stahl bargaining game, cost and profit margins affects the number of rounds between the source and each forwarder. We can refer the repetitive attempts of the source as a value of patience. This patience is a non-negative value less than or equal to 1. The patience of source can be defined by following:

$$\frac{d\delta_s(SC_s^t \times R_s^t \times TTL_m)}{d\delta_s(SC_s^t \times R_s^t \times TTL_m)} > 0 \tag{22}$$

Where $\delta_s(0) = 0$ and $\delta_s(\infty) = 1$, SC_s^t is the current score of source for a time period t, TTL_m is the possible life of message m. The term patience is referred from [33] as show below in the equation:

$$\delta_s(x) = \frac{e^{\gamma x} - e^{-\gamma x}}{e^{\gamma x} + e^{-\gamma x}} \tag{23}$$

Where γ is the coefficient of patience for the source node.

Since each forwarding node tries to get its score at the peak by offering a bargaining score. The forwarder nodes consume energy in each round of bargaining. This is referred as the patience of forwarder nodes. Considering the same procedure of source node, we can conclude (24) and (25).

$$\frac{d\delta_{Fi}(SC_{Fi}^t \times R_{Fi}^t \times TTL_m)}{d\delta_{Fi}(SC_{Fi}^t \times R_{Fi}^t \times TTL_m)} > 0 \tag{24}$$

$$\delta_{Fi}(x) = \frac{e^{\rho x} - e^{-\rho x}}{e^{\rho x} - e^{-\rho x}} \tag{25}$$

$\boldsymbol{\rho}$ is the coefficient of patience for each forwarding node.

We can obtain a perfect unique subgame Nash Equilibrium based on Rubinstein-Stahl model as show in (26). This equilibrium function is based on previous equations according to the principles of [33].

$$(x_S^*, x_{Fi}^*) = \left[\frac{1-\delta_{Fi}}{1-\delta_S\delta_{Fi}}, \frac{\delta_S(1-\delta_{Fi})}{1-\delta_S\delta_{Fi}}\right] \tag{26}$$

The involved nodes in a single set of time finally reach into an amount of score which can be optimal for both.

VI. SIMULATION RESULTS

The initial calculations for all the values have been analyzed by using MATABL 11 under windows. The impact of variations in the values of factors on the *RSc* and the *IBSC* for each node is examined. Table V shows the factors values along with their computed *RSc* and *IBSC* for a sample of 6 nodes.

TABLE 5. Sample of computed values.

ID	*FaP*	*FaE*	*cn*	*Sel*	*fb*	*FaHpl*	*FaR*	*RSc*	*IBSc*
1	0.639	39.08	1	66.238	2/3	4	35.397	2.415	3.397
2	3.698	87.19	7	53.566	2/9	3	58.836	0.449	0.230
3	0.413	61.60	0	69.474	4/1	9	13.131	3.837	5.075
4	2.425	0	5	28.579	2/2	3	14.292	0	0
5	2.415	8.75	4	10.592	6/4	2	90.273	30.924	0.483
6	0.363	70.03	2	76.389	2/3	4	27.348	1.041	1.454

The work is then simulated by using NS2.34 under Red Hat 9. The simulation is performed in five modules. In first module we obtained results for DSR protocol based on our setup. In second module we examined the same DSR protocol by injecting 4% selfish nodes in it. Third module contains our own work. Fourth module contains the comparison among all the attained results. The last module is not directly connected with the first four modules. In this module we tested the robustness of our work by varying the number of selfish nodes. The principal parameters used for the simulation are as following:

TABLE 6. Parameter values for simulation.

Parameter	Value
Area	500 x 500
Base Protocols	DSR, OLSR
Number of Nodes	50,100
Node Distribution	Uniform
Initial Energy	100
Rx Power	0.3
Tx Power	0.6
Movement Trace	Off
Comparisons	DSR, DSR with Selfish nodes, Proposed Work
Size of packet header	4 bytes
RSc header size	4 bytes
IBSc header size	4 bytes
Maximum number of messages per packet	4
Address size	4 bytes
Traffic Source	CBR
Packet Protocol	TCP
Threshold Distance (*DISTtr*)	50

The performance metrics considered are packet delivery ratio (PDR), end-to-end delays, Average energy consumption and throughput. Fig. 2 shows the comparison of average end-to-end delays among the three protocols. DSR protocol having selfish nodes (SELFISH-DSR) and a plain DSR protocol entirely work in reactive manners. Therefore, the delays are caused due to route discovery and frequent packet folding mechanism. In SELFISH-DSR some packets are dropped which are not considered in calculation of end-to-end delays but effect other performance metrics. These packets drop slightly decreases the value of average delays than a normal situation. Our mechanism, referred as reward based mechanism (RwBM) in this section, is giving very good results for delays. The results for RwBM, in this case, are even better than a simple DSR protocol. It is because RwBM does not use many mobility and route discovery related procedures as followed by DSR. Moreover, for better results we have used OLSR for messaging and control packets transfers. OLSR gives comparatively lower end-to-end delays, if compared with DSR [30].

The results for average energy consumption can be seen in Fig. 3. The work reduces the number of unattended requests and sometimes applies the node black-listing mechanism.

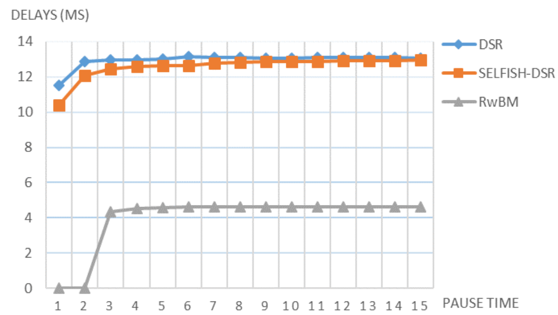

FIGURE 2. Comparison on average delays.

Therefore, RwBM gives comparatively better results for average energy consumption. In SELFISH-DSR the nodes consume more energies due to the non-cooperative behavior of selfish nodes. Some nodes need to repeat their transmission in SELFISH-DSR.

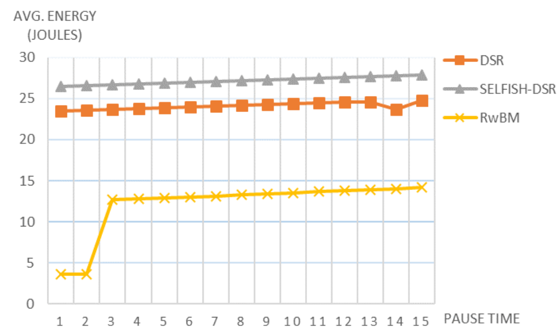

FIGURE 3. Average energy consumption.

Fig. 4 shows the average packet delivery ratio (PDR) for each protocol. PDR is the portion of sent packets which are received at the BS. In the simulation environment, RwBM takes some time for configuration and loading all the factors. Therefore, in most of the simulation results we can't get the accurate values for first two seconds. After pause time 4 the value of PDR becomes consistent for RwBM. It is because the system initially loads and molds all the nodes by reward based mechanism. Here in this case, RwBM gives results similar to simple DSR protocol having no selfish nodes.

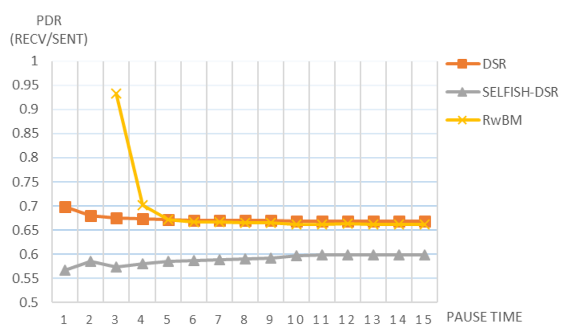

FIGURE 4. Comparison of PDR.

The average throughputs for three protocols are shown in Fig. 5. The performance matric throughput indicates the average rate of successful packet delivery in a specified period of time. Our protocol gives relatively better results than both DSR and DSR-SELFISH. The higher throughput is due to increased use of control messaging as compared to a normal DSR protocol. The curve in the throughput graph does not change smoothly. It is because some traffic is affected by the generated scores for nodes and then bargaining among nodes.

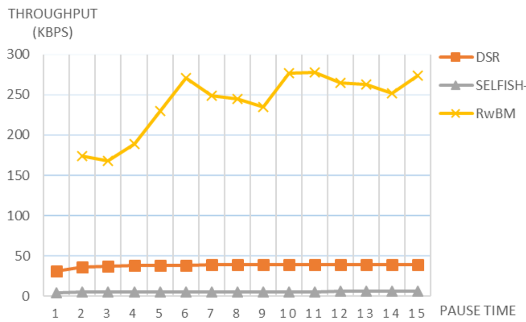

FIGURE 5. Average throughput.

Fig. 6 gives the packet loss ratio results. The values indicate that our work is giving a performance similar to the plain DSR protocol in this experiment too.

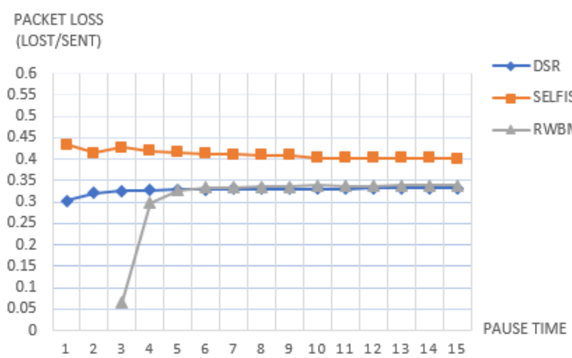

FIGURE 6. Packet loss ratio.

The network's life is presented by the ratio of dead nodes with time intervals as shown in Fig 7. In experiments, the nodes having energy less than 0.5 were considered as dead nodes. The results show that in RwBM protocol, the dead node ratio is uniform and due to less energy consumption the ratio is lower than other two protocols. SELFISH-DSR has non-uniform pattern of dead nodes as the mechanism does not handle any selfish activity in the network. DSR also gives even ratio of dead nodes as it does not keep any selfish node in it.

Fig. 8 shows the impact of number of selfish nodes on the network performance. For this unit, an experiment of 100 nodes is taken. In each set of experiment, the number of selfish nodes is increased and results are recorded at time pause 5. The results show that there is no considerable impact of the increased number of selfish nodes in the network.

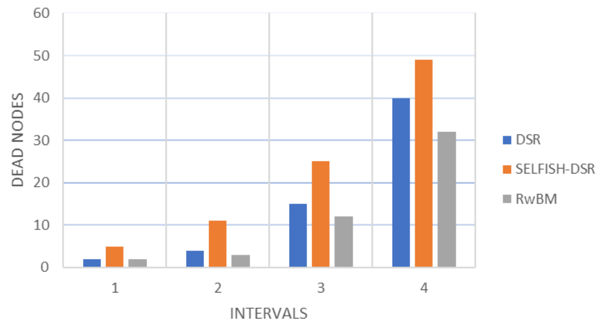

FIGURE 7. Ratio of dead nodes.

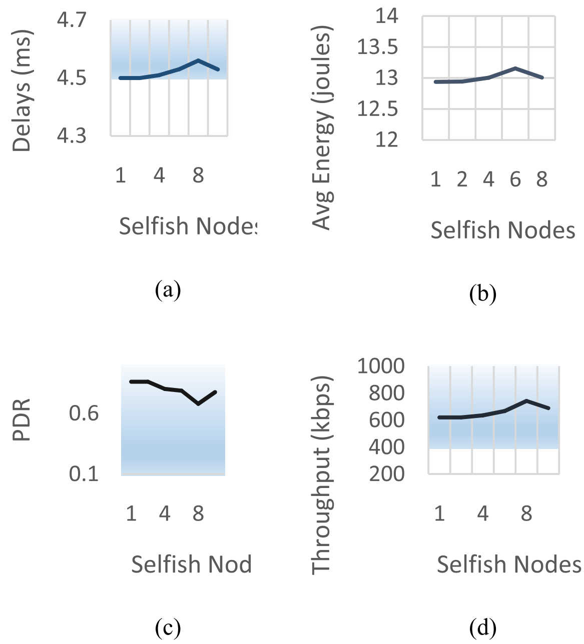

FIGURE 8. Performance verses number of selfish nodes. (a) End-to-end Delays. (b) Avg. Energy Consumed. (c) Packet Delivery Ratio. (d) Throughput.

VII. CONCLUSION AND FUTURE WORK

Various incentive based mechanisms have been introduced to control the non-cooperative environment in wireless network. The main motive of these approaches is to stimulate or/and punish the selfish nodes. Our work is purely applied to WSNs and consider all the passible parameters associated with the nodes and their operations in the network. Additionally, we incorporated few novel features in this work, like the card system and the calculation of nodes individual importance in the entire network. An adaptive strategy is developed to handle the selfish nodes. Initially the nodes are stimulated by using the scoring mechanism. Later, if a node does not change its behavior then the cards are applied to it based on its importance in the network. A bargaining game theoretic approach is used to analyze the optimal benefits for all the nodes. The simulation results prove the effectiveness of our work. This work gives outperforming results as compared to standard DSR protocol having selfish nodes. This work can be further expanded by using it in a cluster based WSNs, where we can assign some special monitoring functions to the cluster heads. Moreover, evolutionary game theory can be incorporated in this mechanism.

REFERENCES

[1] L. Parra, E. Karampelas, S. Sendra, J. Lloret, and J. J. P. C. Rodrigues, ''Design and deployment of a smart system for data gathering in estuaries using wireless sensor networks,'' in *Proc. Int. Conf. Comput. Inf., Telecommun. Syst. (CITS)*, Gijon, Spain, Jul. 2015, pp. 1–5.

[2] S. Sendra, J. Lloret, M. García, and J. F. Toledo, ''Power saving and energy optimization techniques for wireless sensor networks,'' *J. Commun.*, vol. 6, no. 6, pp. 439–459, 2011.

[3] S. R. Takhur and P. H. Zope, ''Study of wireless sensor network for IoT application,'' *Int. J. Adv. Electron. Commun. Syst.*, vol. 6, no. 2, pp. 6–12, 2017.

[4] L. Parra, S. Sendra, J. Lloret, and J. J. P. C. Rodrigues, ''Design and deployment of a smart system for data gathering in aquaculture tanks using wireless sensor networks,'' *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3335, 2017.

[5] 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 *Proc. 25th Chin. Control Decision Conf. (CCDC)*, May 2013, pp. 4021–4024.

[6] Y. Yoo and D. Agrawal, ''Why does it pay to be selfish in a MANET?'' *IEEE Wireless Commun.*, vol. 13, no. 6, pp. 87–97, Dec. 2006.

[7] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, ''Game theory for wireless sensor networks: A survey,'' *Sensors*, vol. 12, no. 7, pp. 9055–9097, 2012.

[8] D. G. Kampitaki, E. D. Karapistoli, and A. A. Economides, ''Evaluating selfishness impact on MANETs,'' in *Proc. Int. Conf. Telecommun. Multimedia (TEMU)*, Jul. 2014, pp. 64–68.

[9] L. Dasilva, H. Bogucka, and A. Mackenzie, ''Game theory in wireless networks,'' *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 110–111, Aug. 2011.

[10] T. AlSkaif, M. G. Zapata, and B. Bellalta, ''Game theory for energy efficiency in wireless sensor networks: Latest trends,'' *J. Netw. Comput. Appl.*, vol. 54, pp. 33–61, Aug. 2015.

[11] B. Arisian and K. Eshghi, ''A game theory approach for optimal routing: In wireless sensor networks,'' in *Proc. Int. Conf. Comput. Intell. Softw. Eng.*, Sep. 2010, pp. 1–7.

[12] X. Yu and Q. Liu, ''An incentive mechanism game theory based for cooperation in wireless ad hoc networks,'' in *Proc. 9th Int. Congr. Image Signal Process., BioMed. Eng. Informat. (CISP-BMEI)*, Oct. 2016, pp. 1085–1090.

[13] O. Diallo, J. J. P. C. Rodrigues, M. Sene, and J. Lloret, ''Distributed database management techniques for wireless sensor networks,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 604–620, Feb. 2015.

[14] D. Yang, X. Fang, and G. Xue, ''Game theory in cooperative communications,'' *IEEE Wireless Commun.*, vol. 19, no. 2, pp. 44–49, Apr. 2012.

[15] C. Zhu, Y. Wang, G. Han, J. J. P. C. Rodrigues, and J. Lloret, ''LPTA: Location predictive and time adaptive data gathering scheme with mobile sink for wireless sensor networks,'' *Sci. World J.*, vol. 2014, Sep. 2014, Art. no. 476253.

[16] Q. Xu, Z. Su, and S. Guov, ''A game theoretical incentive scheme for relay selection services in mobile social networks,'' *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6692–6702, Aug. 2016.

[17] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ''Mitigating routing misbehavior in mobile ad hoc networks,'' in *Proc. MOBICOM*, New York, NY, USA, 2000, pp. 255–265.

[18] S. Buchegger and J.-Y. Le Boudec, ''Performance analysis of the CONFIDANT protocol,'' in *Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, 2002, pp. 226–236.

[19] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M. S. Fallah, ''A secure credit-based cooperation stimulating mechanism for MANETs using hash chains,'' *Future Generat. Comput. Syst.*, vol. 25, no. 8, pp. 926–934, Sep. 2009.

[20] P. Marbach and Y. Qiu, ''Cooperation in wireless ad hoc networks: A market-based approach,'' *IEEE/ACM Trans. Netw.*, vol. 13, no. 6, pp. 1325–1338, Dec. 2005.

[21] L. Buttyán and J.-P. Hubaux, ''Stimulating cooperation in self-organizing mobile ad hoc networks,'' *Mobile Netw. Appl.*, vol. 8, no. 5, pp. 579–592, 2003.

[22] C. Lin, G. Wu, and P. Pirozmand, ''GTRF: A game theory approach for regulating node behavior in real-time wireless sensor networks,'' *Sensors*, vol. 15, no. 6, pp. 12932–12958, Jun. 2015.

[23] Z. Chen, Y. Qiu, J. Liu, and L. Xu, ''Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game,'' *Comput. Math. Appl.*, vol. 62, no. 9, pp. 3378–3388, Nov. 2011.

[24] Y. B. Reddy and S. Srivathsan, ''Game theory model for selective forward attacks in wireless sensor networks,'' in *Proc. 17th Mediterranean Conf. Control Autom.*, Jun. 2009, pp. 458–463.

[25] S.-K. Ng and W. K. G. Seah, ''Game-theoretic approach for improving cooperation in wireless multihop networks,'' *IEEE Trans. Syst., Man, Cybern. B. Cybern.*, vol. 40, no. 3, pp. 559–574, Jun. 2010.

[26] F. Milan, J. J. Jaramillo, and R. Srikant, ''Achieving cooperation in multihop wireless networks of selfish nodes,'' in *Proc. Workshop Game Theory Commun. Netw. (GameNets)*, 2006, pp. 1–10.

[27] L. Anderegg and S. Eidenbenz, ''Ad hoc-VCG: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents,'' in *Proc. 9th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2003, pp. 245–259.

[28] L. Buttyan and J.-P. Hubaux, ''Enforcing service availability in mobile ad-hoc WANs,'' in *Proc. 1st Annu. Workshop Mobile Ad Hoc Netw. Comput. (MobiHOC)*, Aug. 2000, pp. 87–96.

[29] S. Zhong, J. Chen, and Y. R. Yang, ''Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,'' in *Proc. IEEE 22nd Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, Mar./Apr. 2003, pp. 1987–1997.

[30] M. M. Umar, N. Alrajeh, and A. Mehmood, ''SALMA: An efficient state-based hybrid routing protocol for mobile nodes in wireless sensor networks,'' *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 2, p. 2909618, Jan. 2016.

[31] K. Binmore, J. Swierzbinski, and C. Tomlinson, ''An experimental test of Rubinstein's bargaining model,'' ESRC Center Econ. Learn. Social Evol., London, U.K., ELSE Working Paper #260, 2007.

[32] Y. T. Wu, W. Liao, C. L. Tsao, and T. N. Lin, ''Impact of node mobility on link duration in multihop mobile networks,'' *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2435–2442, Jun. 2009.

[33] V. Le, Y. Lin, X. Wang, Z. Feng, and P. Zhang, ''A cell based dynamic spectrum management scheme with interference mitigation for cognitive networks,'' in *Proc. IEEE VTC*, May 2008, pp. 1594–1598.

MUHAMMAD MUNEER UMAR received the B.S. and M.S. degrees from the Kohat University of Science and Technology in 2006 and 2009, respectively, where he is currently pursuing the Ph.D. degree in computer science. His research main areas are routing and security in wireless networks. He has also authored some articles in the same areas during his Ph.D. research work.

SHAFIULLAH KHAN received the Ph.D. degree in wireless networks security from Middlesex University, U.K. He is currently with the Institute of Information Technology, Kohat University of Science and Technology, Pakistan, as an Associate Professor. His research mainly focuses on wireless broadband network architecture, security and privacy, security threats, and mitigating techniques. He is serving as an editor in many international well-reputed journals.

RASHID AHMAD received the Ph.D. degree in physics from the Technische Universität Wien in 2010. He is currently an Associate Professor with the Department of Physics, Kohat University of Science and Technology, Kohat, Pakistan. His areas of interests are theoretical plasma physics and high-energy physics. His research in computer science mainly focuses game theoretic approaches and artificial neural networks. He is an Associate Editor of the *International Journal of Communication Networks and Information Security*.

DHANANJAY SINGH (SM'14) received the B.Tech. degree in computer science and engineering from UCER, Allahabad, India, in 2003, the M.Tech. degree in wireless communication and computing from IIT Allahabad, Allahabad, India, in 2006, and the Ph.D. degree in ubiquitous IT from Dongseo University, Busan, South Korea, in 2010. He was working as a Post-Doctor Researcher with the National Institute of Mathematical Sciences and a Senior Member of Engineering Staff of future Internet architecture with the Electronics and Telecommunication Research Institute, Daejeon, South Korea, from 2010 to 2012. He is currently the Director of the ReSENSE Laboratory, Hankuk University of Foreign Studies, Global Campus, Yongin, South Korea, where he has been an Assistant Professor with the Department of Electronics Engineering, since 2012. He has received the best paper award from IEEE conferences three times and fellowship award two times from APAN meeting for Singapore and Manila. He has authored over 100 refereed scientific papers, served over 100 TPC memberships, and delivered over 50 invited talks into the major IEEE conferences/workshop. He is a Senior Member of the ACM Society. He is also an ACM Distinguished Speaker.