applied sciences

MDPI

Review

# Game theory-based Routing for Wireless Sensor Networks: A Comparative Survey

**Md Arafat Habib and Sangman Moh ***

Department of Computer Engineering, Chosun University, Gwangju 61452, Korea
* Correspondence: smmoh@chosun.ac.kr; Tel.: +82-62-230-6032

Received: 4 June 2019; Accepted: 15 July 2019; Published: 19 July 2019

check for updates

**Abstract:** Wireless sensor networks (WSNs) have become an important and promising technology owing to their wide range of applications in disaster response, battle field surveillance, wildfire monitoring, radioactivity monitoring, etc. In WSNs, routing plays a significant role in delivery latency, energy consumption, and packet delivery ratio. Furthermore, as these applications are used in critical operations with limited irreplaceable batteries, routing protocols are required to be flawless as well as energy efficient. The dynamic environment also requires intelligent and adaptive routing. Game theory is widely used for designing routing protocols in WSNs to achieve not only reduced energy consumption but also increased packet delivery ratio. The core features of efficiently designed game theory-based routing protocols include optimal cluster head selection in hierarchical routing, energy-efficient and delay-aware route discovery, fault-tolerant data delivery, and coalition forming and grouping among nodes for stringent data transfer. In this paper, different routing protocols based on various types of games are extensively reviewed, which have been reported so far for improving energy consumption, delay, route establishment time, packet delivery ratio, and network lifetime. The different game theory-based routing protocols are qualitatively compared with each other in terms of major features, advantages, limitations, and key characteristics. For each protocol, possible applications and future improvements are summarized. Certain important open concerns and challenges are also discussed, along with future research directions.

**Keywords:** energy consumption; game theory; network lifetime; packet delivery ratio; routing protocol; wireless sensor networks

## 1. Introduction

A wireless sensor network (WSN) consists of sensor nodes with the ability to sense, process, and communicate. The nodes are fixed in most cases and are subject to limited human intervention. It is a special kind of ad hoc network with minimal or no mobility [1]. It helps us monitor and analyze any unknown environment. Typically, WSNs are data centric. Despite requesting data specific to a node, data are collected based on certain attributes, like temperature and humidity. Therefore, many sensors must be deployed to accurately reflect the physical attributes in a given area [1]. The progress in recent technology has made it possible to deploy thousands of sensor nodes within a network, which are programmable and can sense multiple parameters. Wireless sensors can be deployed at the site of interest without any prior organization. This is a great advantage because it decreases the installation cost and saves time. Moreover, replacing a wired macrosensor with smaller wireless sensors for the same cost can provide us with a wider range of benefits. Another advantage of WSNs is that the failure of one sensor node does not affect the whole network, because there are adjacent nodes collecting a similar kind of data in the target region [1].

There are certain additional features that ideal sensor networks should possess, including attribute-based addressing. Addresses may consist of a group of attribute value pairs.

For example, an attribute address may be (temperature > 45 °C, location = "Gwangju") [1]. Therefore, the responding sensor nodes will be a node in "Gwangju", sensing a temperature greater than 45 °C. Sensor nodes should also provide an accurate and precise response if there are any sudden changes in the environment. Location awareness is another required feature for WSNs. Data collection is mostly based on location, and nodes are expected to know their positions if required. Thus, basically, a WSN consists of sensor nodes, a user, and an interconnected backbone [2].

Currently, WSNs are widely used in significantly crucial applications [3]. In the case of military assignments, the application of WSNs can be identified in information collection, enemy tracking, battlefield surveillance, or target classification [4,5]. One real time example is the intrusion detection system implemented by the University of Virginia, presented in [6]. Moreover, there is wide-scale usage of WSNs in environmental monitoring. A tracking system for the recognition and improvisation of the waste management system in Seattle is presented in [7]. There are innumerous examples of WSN applications. Readers can refer to [2,8,9] if they are interested in more information. Therefore, WSNs are required to confront various challenges, like detection, filtering, and estimation, through different applications, which were studied in [10–16].

Routing in WSNs is challenging and certain important aspects should be carefully considered. First, because a WSN consists of numerous nodes, it is impracticable to create and incorporate a global addressing scheme for the deployment of sensor nodes. This is owing to the overhead of the identity management system. Moreover, sensor nodes should be self-organizing because they are deployed in a random and ad hoc manner. Next, the sensed data in WSNs should be transmitted back towards the base stations. Thus, we can compare its dimensions to the rational thinking of players and strategic games. Furthermore, prompt and reliable communication is necessary because WSNs are often deployed in critical mission scenarios that also require the careful consideration of resources such as energy and storage capacities. Finally, the nodes in traditional WSNs are stationary. A minimal number of mobile nodes can be present, but the mobility is low. Therefore, WSNs are not exposed to unpredictable and frequent topology changes [17].

As mentioned earlier, one of the distinctive properties of WSNs is random deployment without access to external resources [18]. Resources such as energy, battery power, bandwidth, and communication speed are considered vital in WSNs. Among all these resources, the most vital resource is energy, because it is directly related to network lifetime and performance. Hence, routing metrics like end-to-end delay, packet delivery ratio, network lifetime, and routing establishment time should also be considered while designing routing protocols for WSNs.

Using game theory to design the routing protocol for WSNs is a superior method. Owing to the unique nature of WSNs, game theory can be considered an attractive and robust solution for designing a routing protocol that can eventually lead to a pragmatic and agile network. The rational behavior of players makes game theory applicable in system operations analysis in self-organizing and decentralized networks. Several existing works that used game theory to design routing protocols for WSNs promise better performances than other existing protocols in terms of end-to-end delay, network lifetime, packet delivery ratio, energy efficiency, and route establishment time. To the best of our knowledge, three prior survey papers [19–21] have covered game theory-based routing protocols in WSNs. In [19], four protocols were reviewed: competitive routing with polynomial cost [22], flow and routing control policy with multiple competitive users [23], analysis of a multi-stream game for multipath routing [24], and the Nash equilibrium for combined flow control and routing [25]. In [20], a collaborative, energy, and information aware routing algorithm using game theory [26] was reviewed. In [21], four protocols were reviewed: prolonging the network lifetime via nodal energy balancing in heterogeneous WSNs [27], game theory-based energy-balanced routing protocol for WSNs [28], game theory used for reliable routing modeling in WSNs [29], and predictable energy-aware routing based on dynamic game theory in WSNs [30]. The latest routing protocols [31–45] published after 2012 will be surveyed and discussed in more detail in this survey. Apart from [19], [20], and [21], two other survey papers have briefly discussed game theory-based routing protocols, even though their focus was not on game theory. In [46], three routing protocols based on game theory were critically analyzed, but they were published before 2009. Because our target is to review the latest protocols, we do not review these. Even though [41] and [42] are reviewed in [47], we have included them in our survey because they are two of the major papers published in recent years that cover the implementation of the cluster-based WSNs using evolutionary game theory (EGT).

We have considered three criteria for choosing the papers that have been incorporated in this survey. They are the publication year, journals/conferences where the papers have been published, and the implications of the three different types of game theories. This paper aims at presenting a thorough study of the most recent works, therefore, only the routing protocols published after 2012 were considered. We considered papers from reputable journals and conferences, which were collected from famous scientific databases. Game theory can be classified into three types: cooperative, noncooperative, and evolutionary game theory. A more detailed explanation will be described in the following section. A routing protocol may become considerably conducive for a specific application just because it has a different game approach. For example, EGT is sufficiently suitable for clustering-based routing protocols. Table 1 lists the limitations of the existing surveys of [19–21,46,47].

**Table 1.** Limitations of existing surveys.

| Survey Article | Limitations |
|---|---|
| Reference [19] | • No practical example for readers on how to imply game theory for routing;<br>• No classification of the protocols based on game theory;<br>• No qualitative comparison based on the advantages, disadvantages, and main features is shown;<br>• Possible applications of the designed protocols are not presented;<br>• Possible future improvements of the protocols are not discussed;<br>• Challenging and open research issues are not addressed. |
| Reference [20] | • No practical example of how game theory can optimize a wireless sensor network (WSN) is presented;<br>• It discusses different roles of game theory in WSNs for target tracking, power control, topology control, routing protocol design, etc. The focus of the survey is not in routing protocols, and thus the survey ends up discussing only one routing protocol [26]. |
| Reference [21] | • No practical example for readers on how to imply game theory for routing;<br>• No qualitative comparison based on the advantages, disadvantages, and main features is shown;<br>• Possible applications and future improvements of the designed protocols are not presented. |
| Reference [46] | • No practical example for readers on how to apply game theory for routing;<br>• Qualitative comparison among the protocols is not given;<br>• Future improvements of the designed protocols are not explicitly presented. |
| Reference [47] | • No practical example for readers on how to apply game theory for routing;<br>• Qualitative comparison among the protocols is not given;<br>• Future improvements of the designed protocols are not explicitly presented. |

As WSNs are application specific, it is critical to choose a particular routing protocol based on the target application. Certain applications may require data reliability more than any other metrics. Conversely, for other applications, latency may not be considered a concern, however, prolonging the network lifetime can be very important. This depends on the purpose for which the WSN is deployed. Because game theory can introduce rationality among sensor nodes, it is moderately easy to design a routing protocol demanding certain special requirements for any type of application. Therefore, a qualitative comparison demonstrating the major features, pros, and cons of the routing protocols can be helpful for researchers and engineers to decide the type of routing protocol that can fit their application demand. Furthermore, we present a network architecture-based comparison of the protocols in this paper, based on parameters like topology, data transmission, and location awareness, which can be helpful in choosing a routing protocol with the desired properties for a particular application. We also present possible applications and future improvements for the discussed protocols. This can aid readers to sort out the protocols in an application specific way and can help researchers to consider possible improvements for the future designs of game theory-based routing protocols. This paper also discusses the open concerns and challenges in implementing game theory for routing in WSNs, along with future research directions. Table 2 presents a comparative view of this survey with the existing surveys. The main contributions of the paper are as follows:

- Theoretical key concepts required to understand the use of game theory in WSN routing are briefly discussed;
- Routing protocols are examined in relation to their operational principles and key features;
- Routing protocols are classified based on the game applied;
- Routing protocols are compared with each other in terms of major characteristics, pros, and cons;
- Certain challenging problems in the design and implementation of a routing protocol are discussed, in addition to future research directions;
- Possible applications and future improvements of the protocols are discussed.

The rest of this paper is organized as follows: in the following section, game theory for wireless sensor networks, along with the most commonly used metrics for game theory-based routing protocols is introduced; in Section 3, the latest routing protocols based on game theory are presented, along with their technical strengths, weaknesses, possible improvements, and applications; in Section 4, game theory-based routing protocols are compared with each other in terms of major features, advantages, limitations, and network architecture; in Section 5, certain future research directions and challenging research concerns are discussed; finally, the paper is concluded in Section 6.

**Table 2.** Comparison of our survey with existing surveys.

| Survey Article | Practical Examples of Implementation | Classification of the Protocols Based on Game Theory | Qualitative Comparison of the Protocols | Possible Applications of the Protocols | Possible Future Improvements of the Protocols | Challenging and Open Research Issues |
|---|---|---|---|---|---|---|
| Reference [19] | No | No | No | No | No | No |
| Reference [20] | No | Yes | No | No | No | No |
| Reference [21] | No | Yes | No | No | No | Yes |
| Reference [46] | No | No | No | No | Yes | Yes |
| Reference [47] | No | No | No | No | No | Yes |
| Our Survey | Yes | Yes | Yes | Yes | Yes | Yes |

## 2. Preliminaries

This section is divided in two parts. The first part will describe the basics of game theory. For further information, the readers can refer to [48] and [49]. In the second part, the different types of games that have been used until now in designing routing protocols for WSNs will be elaborated.

### 2.1. Basics of Game Theory

In game theory, a game consists of $n$ players, each player selects a strategy $s_i$ from a set $S$. The objective is in maximizing the utility. A game in game theory can be modeled as:

1. $P = \{p_1, p_2, p_3, \ldots, p_n\}$, which is a set of $n$ players;
2. $A = \{a_1, a_2, a_3, \ldots, a_m\}$, which is a set of $m$ actions;
3. $S = \{s_1, s_2, s_3, \ldots, s_k\}$, which is a set of $k$ strategies;
4. $U$ = pay-off function to calculate the pay-off.

*Player*: A player is an agent who makes rational decisions in a game.

*Game*: A game is a formal description of a strategic situation.

*Rationality*: We call a player rational if they play such that their own pay-off is maximized. It is often assumed that the rationality of all the players is common knowledge.

*Strategy*: A strategy is one of the possible actions among the given actions.

*Pay-off*: A pay-off is a number that is also called the utility. It presents the desirability of an outcome for a player. Given that the outcome is random, pay-offs are weighted with probabilities. The expected pay-off is highly related to the player's intention of taking risks.

*Action profile*: An action profile is a list of actions, one for each player in the game.

*Nash equilibrium*: A Nash equilibrium is an action profile $a^* = \{a_1{}^*, a_2{}^*, a_3{}^*, \ldots, a_\mathrm{n}{}^*\}$, where any player $p_i$ cannot perform better by choosing an action different from $a^*$ [48]. It is to be noted that $a_i{}^*$ is the set of possible actions that player $p_i$ can choose to lead the Nash equilibrium.

A game-theoretic modeling of a routing algorithm for a WSN [42] will be briefly discussed here. A cluster-based routing protocol is assumed, where sensor nodes decide whether to be the cluster head (CH) or not on the basis of their residual energy. As discussed above, a game in game theory can be represented as $G = (P, A, S, u_i)$, where $P = \{NH, NL\}$ is a set of players, where $NH$ represents nodes with high energy, $NL$ represents nodes with low energy; $S$ = {*Decision of being a cluster head, Remaining as a normal cluster member*}, is a set of strategies;, $A$ = {*To be a cluster head, Not to be a cluster head,*} is a set of actions; and $i = 0, 1, 2, \ldots, n$.

If the residual energy (i.e., amount of energy left in the node) of a node is higher, it is logical to assume that it will become a CH. Players in this game should have this rationality. In set $A$, two actions have been listed. This list is called the action profile for a game. The pay-off function $u_i$ for node $i$ with higher energy is given by,

$$u_i = r_i - c_i, \tag{1}$$

where $r_i$ and $c_i$ are the reward and penalty for the action that node $i$ chooses, respectively. If node $i$ chooses to be a CH despite having low residual energy, it will get a higher penalty than reward. Conversely, if it chooses to be a CH when it has more residual energy than the surrounding nodes, it will receive a higher reward than penalty. For example, if node $i$ receives a reward of 20 and a penalty of 10 for being a CH, the pay-off is 10. In this example, nodes must compare with each other in terms of residual energy and decide collectively who must be the CH. They use two actions together in the action set, which we can call joint actions, and the pay-offs they generate are collective pay-offs as they are achieved through cooperative coalition. If two players choose two different strategies and there is no other strategy that can maximize the pay-off if one chooses another given that the other player retains the strategy chosen before, a Nash equilibrium is achieved.

### 2.2. Games in Routing for WMSNs

This survey discusses the routing protocols that were published over five years, since 2012. After a comprehensive study of all the protocols published so far, we found three types of games that were used in WSNs for the routing protocol development: cooperative games, noncooperative games, and evolutionary games. A reputation-based game was also used in one of the routing protocols. This falls into the category of cooperative games, however, owing to its distinct features, we discuss it separately. After discussing each type of game in detail, we discuss the implication of each through an example. The aim is to facilitate readers to comprehend each type of game and the methods used to implement them.

Certain useful roles of game theory in WSNs are summarized below.

*(i) CH selection:* Cluster-based routing protocols are widely applicable in WSNs. One crucial challenge for this kind of routing is selecting the optimal CH in the setup phase. Introducing a rational decision-making process among the nodes competing to be the CH based on the pay-off function, which considers residual energy level, link quality, etc., can ease the process of CH selection.

*(ii) Route discovery excluding the malicious nodes:* Typically, sensor nodes are required to collaborate with each other for data transmission and each node can be considered a potential routing node. It is possible for malicious nodes to drop packets deliberately in a WSN. Therefore, finding a secure and energy-efficient routing path is a great challenge in WSNs. This kind of problem can be easily countered with reputation-based games. Any kind of deliberate dropping of the data packets will lead to the punishment of the node and its reputation will be decreased in an exponential manner. Nodes with high reputation, energy, and positions closer to the destination will be selected as one-hop routing paths, excluding the malicious nodes.

*(iii) Facilitating grouping:* In many WSNs, grouping is used to facilitate the organization of the node cooperation. Each group contains a leader that is responsible for communicating outside of the group. Let us assume a self-organizing WSN, where a group leader forms and manages the group. The management is performed such that it is beneficial for the other group members; moreover, group members must have the ability to transfer data to the group leader through direct data transmission. In this kind of network, a new node may want to join a group and the group needs to decide whether to accept the node. This kind of group extension scenario may require a complex decision-making process that can be achieved by cooperative game theory.

*(iv) Finding an energy and delay-aware route:* Nodes can decide to play noncooperative games and try to increase their own benefits by choosing the transmission path to the sink node that requires the least energy and delay.

*(v) Supporting energy imbalance in WSNs:* Game theory is especially suitable for supporting energy imbalance among nodes in WSNs. For example, if there are nodes with variant energy levels, it can optimize this energy imbalance with intelligent decision-making processes.

Cooperative game theory is a process used to make decisions in strategic settings, where it is necessary to factor the preferences and rational choices of other players into the decision-making process [50]. If there is an added benefit through cooperation, it is favorable to form coalitions for mutual advantage. In cooperative games, we focus on the coalitions that will form the joint actions that groups take and the resulting collective pay-off. When coalitions are formed with more than one action from the action set, we call it a joint action. As coalitions involve more than one player, their pay-offs are considered collective. An advantage of cooperative game theory is that it does not require a precisely defined structure for the actual game. For example, each coalition of nodes in a WSN may exchange information to become CHs consecutively in a clustering routing protocol. It is not necessary to know what offers and counter offers they present. A coalition is a subset of the set of players. Coalitions are formed such that the players can coordinate strategies and agree on how the total pay-off will be divided among the members. This type of game consists primarily of two elements. One is the set of players and the other is the characteristic function specifying the value created by the different subsets of the players in the game. Let us consider $P$ to be the set of players and the number of players is $N$. In fact, a cooperative game is a pair $\{N, v\}$, where $N$ is a finite set and $v$ is a function that maps subsets of $N$ to numbers.

If no cooperation is allowed among the players, we consider the paradigm of noncooperative games. When a solution point exists where none of the players can improve their pay-off by a unilateral move, it is known as a noncooperative equilibrium or the Nash equilibrium. According to [51], for the precise formulation of a noncooperative game, we have to specify: (i) the number of players, (ii) the possible actions available to each player and any constraints that may be imposed on them, (iii) the objective function of each player that he attempts to optimize (minimize or maximize, as the case may be), (iv) any imposed time requirements for the execution of the actions if the players are allowed to act more than once, (v) any information acquisition that occurs and how the information available to a player at each point in time depends on the past actions of other players, and (vi) whether the action of a player (nature) is the outcome of a probabilistic event with a fixed (known) distribution.

Let us assume a WSN where a flat routing protocol is implied, which uses relay nodes to send the data packet from the source to the destination. The source sends the data to four of the relay nodes that are within its range. The relay nodes will have to decide among themselves whether to transmit the data and choose a node among themselves to do it. This will require a complex decision-making process to find an optimal relay node. In noncooperative games, the players (nodes in the WSN) attempt to maximize their own benefit by increasing their pay-off through optimal strategy adaptation. The goal is to reach an equilibrium point where nodes will behave selfishly to obtain a strategy to overwhelm the benefit, which would result in a decrease in the pay-off of other nodes. If the four relay nodes have different energy levels, it is not advisable for the low energy node to forward the data packet. Conversely, even nodes with high energy will be reluctant to aggregate the data packet to save their energy for a longer survival time in the network. In that case, not sending the data will result in a decrease in pay-off of the other nodes and eventually reduced functionalities of the network. Alternatively, other scenarios are possible, such as if a node has a low energy or if it is very near to the destination node, it may decide to send the data packet for reduced delay and overall network lifetime increase. There are many strategies that can be specified. The target is to find strategies that will uniformly distribute the benefit of the entire performance by finding out the Nash equilibrium and using carefully designed pay-off functions.

In evolutionary game theory, the behavior of large populations of agents who repeatedly engage in strategic interactions is studied. The key concepts of evolutionary games are the numerous behaviors involving the interaction of multiple organisms in a population. The success of any of these organisms is highly dependent on how it interacts with others. Therefore, the fitness of an organism should not be measured individually, instead, it must be measured considering the full population where it resides.

To elaborate evolutionary game theory with an example related to WSNs, let us assume a cluster where there are nodes that have different energy levels. The goal is to use evolutionary game theory to increase the network lifetime through the interaction of the sensor nodes. A node which is CH will have to send data to the sink node, which is a costly operation in terms of energy expenditure. Conversely, nodes in the cluster which will not become CH will have to send data to the CH. This is an operation with a low cost in terms of energy. We assume that it is an inherent nature of the nodes to remain selfish and avoid becoming the CH, to save their energy for surviving in the network. If none of the nodes becomes the CH, the cluster will fall, and every single node will have to send data to the sink node in a single hop manner, which will deplete energy very fast. Under these circumstances, to survive in the network, all the nodes will have to choose their strategies to play their role as a CH or as a cluster member (CM) in such a way that both kinds can survive in the network longer, while interacting in the cluster. If the game is designed well, it will eventually lead to an evolutionarily stable strategy and the network lifetime will increase. Routing protocols based on the evolutionary game theory are elaborately discussed in Section 3. Further mathematical formulations can be observed in that section regarding evolutionary game theory.

Reputation is one of the most practical tools for measuring the partners' quality and incentivizing the partners' behaviors [52]. To the best of our knowledge, only one routing protocol so far has used reputation-based games. In fact, the approach is cooperative but depends highly on the reputations of the nodes. This leads us to classify it as a separate type of game, applied for the design of routing protocols for WSNs.

The above-mentioned four kinds of games used in various routing protocols for WSNs are comparatively summarized in Table 3.

**Table 3.** Comparison of four kinds of games used in routing for wireless sensor networks (WSNs).

| Game | Key Features | Comparative Characteristics | Routing Metrics |
|---|---|---|---|
| Cooperative game theory | Considers preferences and rational choices of other nodes in the routing game of a WSN. | Binding agreements needed for mutual benefit in games designed for routing. | Considers energy and packet delivery ratio as routing metrics. |
| Noncooperative game theory | Considers situation when no two sensor nodes can benefit more by any move after a certain point given that a player sticks to some strategies. | Reaching Nash equilibrium is needed for successful implication. | Considers energy as the main routing metric in most of the protocols. |
| Evolutionary game theory | Does not need to consider the preferences of other routing nodes. | Evolutionarily stable strategy is needed for the implication of this type of games in routing. | Considers network lifetime as primary routing metric. |
| Reputation-based games | The nodes are cooperative in this type of game. | Measures the partners' quality and incentivizes the partners' behaviors. | Considers average throughput and network life time in the routing protocol. |

## 2.3. Routing Metrics

In the literature, various routing protocols consider different routing metrics to compare their performance with the already established routing protocols. This subsection discusses the different routing metrics adopted by the game theory-based routing protocols.

Routing metrics are defined as measures used by routing protocols to make routing decisions [53]. Routing protocols use different routing metrics to choose the best routing path, starting from the source to the destination. The quality of a routing path is indicated by the routing metrics [54]. The routing metrics given below are the ones incorporated by the recent approaches that have used game theory to design routing protocols for WSNs.

Sensor nodes are powered using batteries with a small capacity [55]. The deployment of the sensor nodes takes place in a predominantly unattended environment. Hence, energy scavenging is not an option for the sensor nodes in WSNs. Energy consumption is directly related to network lifetime. Therefore, energy consumption is the most important routing metric. To denote energy as a routing metric, two measures are to be considered. One is the path energy and the other is the residual energy of the intermediate nodes. Path energy includes the amount of energy spent for data transmission, starting from the source to the destination. A path cannot be considered efficient if it merely displays the minimal path energy. The residual energy of the intermediate nodes should also be considered. The energy required for data transmission and data reception are also considered. If a protocol is a clustering-based protocol, energy consumption can occur in three cases. They are the transmission and reception of data among the cluster members, cluster heads, and sink node.

The packet delivery ratio is the ratio of the number of packets successfully received to the number of total packets sent. Because certain packets may get lost during transmissions, the packet delivery ratio is meaningful with respect to network performance as well as communication reliability. We consider the total number of transmitted data packets and the total number of successfully received data packets in a WSN be $N_s$ and $N_r$, respectively. Then, the packet delivery ratio $R$ can be represented as $R = N_r/N_s$. Note that $(1 - R)$ is the packet loss ratio.

Network lifetime is defined as the period when a WSN remains fully functional and operative. We can also consider network lifetime as the time up to when the first node is alive, because the death of a node can reduce certain functionalities. According to [55], this is defined as the maximum time duration that the deployed sensor nodes can monitor the phenomena of interest. The routing protocol for WSNs should be designed such that the network lifetime is prolonged.

After the deployment of sensor nodes, a considerable amount of time is required to set up the network and for it to subsequently attain a steady state. A certain reliable route must be established from the source to the destination. Different approaches have been used in various routing protocols for route discovery and establishment. Latency in first-time route establishment is not acceptable, as WSNs are deployed in mission critical cases. Therefore, it is also a considerable routing metric for WSNs to design a routing protocol. Throughput can be considered the amount of data transferred per unit of time. It is the rate of successful message delivery over a communication channel.

The routing approaches in WSNs that are based on game theory consider two or more routing metrics simultaneously. We can denote this as a cumulative metric. For example, energy consumption and packet delivery ratio can be considered together as a routing metric to design a routing protocol. Simultaneous considerations of these metrics can ensure a robust path selection in a complex routing scenario.

## 3. Game Theory-Based Routing Protocols in WSNs

Routing approaches based on game theory vary depending on the types of game used. In this section, the existing game theory-based routing protocols for WSNs are reviewed and discussed in detail. Possible future improvements along with their applications are discussed too. They can be categorized as in Figure 1, according to the taxonomy discussed earlier. All the routing protocols that will be discussed in this section are listed in this figure.

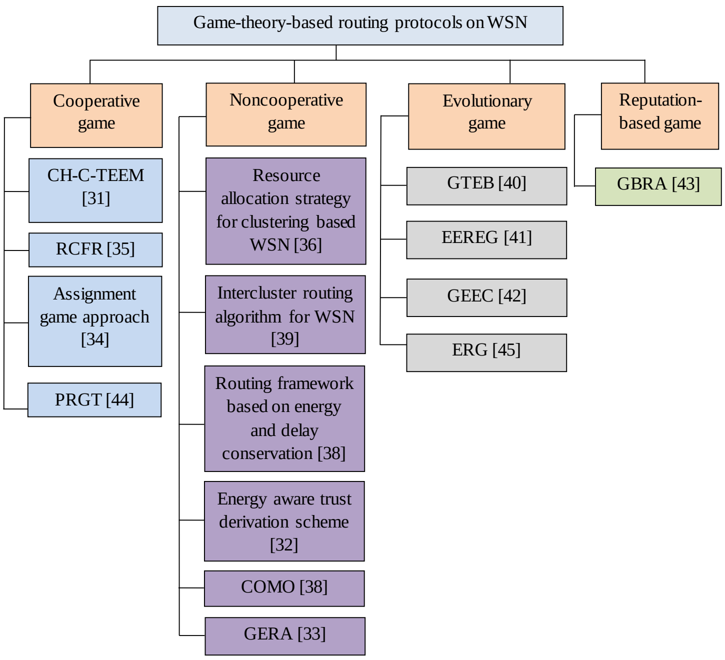


**Figure 1.** Categories of game theory-based routing protocols for wireless WMSNs: CH-C-TEEM: Cluster Head Cooperative Trustworthy Energy-Efficient multiinput multioutput; RCFR: Reliable Coalition Formation Routing; PRGT: Probabilistic Routing Based on Game Theory; COMO: Cooperation Optimal Protocol for Multirate Opportunistic Routing; GERA: Game-Theory-Based Energy-Efficient Routing Algorithm; GTEB: Game Theoretic Energy Balanced Routing; EEREG: Energy-Efficient Routing Protocol based on Evolutionary Game; GEEC: Game-Theory-Based Energy-Efficient Clustering; ERG: Evolutionary Routing Game; GBRA: Game-Theory-Based Routing Algorithm.

## 3.1. Routing Protocols Based on Cooperative Games

### 3.1.1. Cluster Head Cooperative Trustworthy Energy-efficient Multi-input Multi-output (CH-C-TEEM) Routing Protocol

WSNs are energy constrained and they require energy-efficient routing protocols for a fading environment. Many of the state-of-the-art works utilized a multi-input multi-output (MIMO) scheme to increase energy efficiency in a fading environment. Sathian et al. designed the cluster head cooperative trustworthy energy-efficient MIMO (CH-C-TEEM) routing algorithm to manage the fading environment in a WSN [31]. This protocol was based on game theory and its performance was analyzed based on energy consumption. Channel fading and interference may cause a reduced network lifetime of the sensor nodes. To increase the lifetime, a CH-based cooperative MIMO scheme was designed. In the MIMO scheme, it was possible to create small groups among the sensor nodes participating in routing. The cooperative game theory was used to form such small groups for cooperative data transmission, as discussed in [31].

The CHs cooperate among themselves for data transmission and each node becomes a CH consecutively. The CH-C-TEEM also incorporates a trust-based framework through a game-theoretic model to reduce packet loss and routing overhead by eliminating malicious nodes, which tend to drop useful data packets. Sensors in the game-theoretic model are intelligent routing agents. A CH election game is designed in the following way:

$N$ = A set of players (sensor nodes in this case);

$A$ = A set of available actions for a sensor node to finalize a decision;

$L = \{l_1, l_2, l_3, \ldots, l_n\}$, where $L$ is a set of strategies. If any node $n_1$ chooses a strategy $l_1$, the value of $l_1$ is "1" if the node chooses to be a CH and "0" otherwise;

The pay-off set is $\{u_1, u_2, u_3, \ldots, u_n\}$, a set containing numerical values generated from the strategy profile. The pay-off function for the CH election game is:

$$U = \alpha \frac{E_i}{E_{init}} + \beta R_i - \gamma n, \tag{2}$$

where $\alpha$ is the weight parameter of the node's residual energy level, $\beta$ is the weight parameter of the node's trust level, $\gamma$ is the weight parameter corresponding to average path loss, $E_{init}$ is the node's initial energy level, $E_i$ is the node's current residual energy level, and $R_i$ is node's trust level.

The cooperative nodes that participate in the MIMO communication are chosen based on a coalitional game designed using the residual energy level of the sensor nodes that act as players, and the game is played to sort out a particular set of nodes for cooperative data transmission and reception. The aim of this kind of grouping is to decrease the total power consumption. The game is modeled as $(N, v, S)$, where $N$ = a set of CH nodes, $v$ = characteristic function, and $S$ is the partition of $N$ $(S \subseteq N)$. The characteristic function of the system was based on network lifetime and it is presented by,

$$vS_j = x^{S_j} \in R^{|S_j|} | x_i^{S_j} = T_{net}, \ \forall i \in S, \tag{3}$$

where $x_i^{S_j}$ is the utility of the node within the coalition $S_j$, $|S_j|$ is the number of sensor nodes in $S_j$, $T_{net}$ is the network lifetime.

The network lifetime in this protocol is defined as the time taken for the first sensor node to run out of energy. We assume $T_{co1}$ and $T_{co2}$ to be the lifetime of the first two nodes that are in coalition and are cooperatively participating in data communication. Then, $T_{non-co1}$ and $T_{non-co2}$ are the lifetimes of the other two nodes that are not in coalition and are not participating in data communication. It is presented by the following equation:

$$T_{net} = min(T_{co1}, T_{co2}, T_{non-co1}, T_{non-co2}). \tag{4}$$

The residual energy $E_o$ from [31] is defined as:

$$E_o = E_{init} - E_t, \tag{5}$$

where $E_{init}$ is the initial energy of the sensor node and $E_t$ is the energy of the sensor node after a specific round. The CH-C-TEEM was compared with the trustworthy energy-efficient MIMO (TEEM) that uses the same pay-off function and game formulation to select the CH [56], and we identified that the CH-C-TEEM performed better in terms of network lifetime and residual energy. According to the simulation results, the residual energy using CH-CH-TEEM was 98% higher than TEEM and the nodes in TEEM were alive for 5000 rounds, whereas the CH-C-TEEM could successfully run 11,750 times in the same simulation environment. This drastic rise in output is achieved merely by introducing merging and splitting coalitions during the coalition formation among cluster members. In Figure 2, the CHs in clusters 1 and 2 send data to the sink node cooperatively by making a pair. Furthermore, the CHs in clusters 5 and 3 act as a pair and send their data cooperatively.

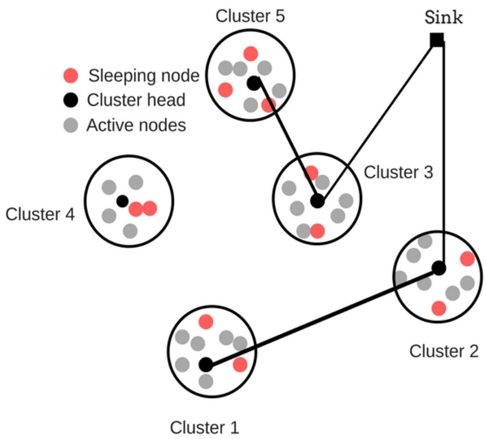


**Figure 2.** Cooperative transmission of data by cluster heads (CHs) in pairs.

Technical strengths:

- Cooperation among CHs leads to energy efficiency;
- Consideration of network security via elimination of the malicious nodes.

Technical weaknesses:

- Routing metrics like packet delivery ratio and end-to-end delay are also important and should have been considered while designing the protocol;
- In [31], it was mentioned that the coalition formation of the sensor nodes was performed using a merge and split algorithm. However, nowhere in the paper [31] was this algorithm elaborated. This led to ambiguity in terms of understanding the functionality of the protocol;
- CH-C-TEEM was compared with TEEM [56], a protocol developed by the same authors of [31]. To prove the superiority of CH-C-TEEM, it is necessary that the protocol is compared with more of the existing state-of-the-art routing techniques in terms of important routing metrics.

Applications:

- Highly applicable for a channel fading environment where network security is a priority with lesser packet loss ratio.

Possible future improvements:

- Coalition formation algorithm can be elaborated;

- More comparative analysis with the existing protocols;
- Performance analysis with important routing metrics like packet-delivery-ratio, end-to-end delay can be considered.

#### 3.1.2. Assignment Game Approach

Future generation wireless networking is expected to be quite challenging as the number of devices will drastically increase, making the WSN paradigm more energy constrained. To deal with this problem, the authors in [34] addressed the reduction of energy consumption of the energy-constrained wireless devices through the cooperative relaying of nodes in heterogeneous networks using game theory.

In [34], mobile users were considered coalition forming agents and encompassed multiple relays and sources. Devices pooled their resources like battery and antenna and relayed to each other for minimizing energy expenditure collectively. The problem was designed as an assignment game and it addressed the optimal method of identifying relays. They derived the core solution of the game. Furthermore, the process of conflict avoidance through this solution was elaborated. Subsequently, the authors of [34] defined a characteristic function along with the utility function to evaluate the amount of energy saving of the relaying nodes. The scheme focused on a two-hop relaying system.

Figure 3 presents a radio access network (RAN) that denotes a long-term evolution or WiFi network. The RAN considered in this scheme served multiple-user equipment (UE) that included mobile phones, sensors, and machines. The UE employed technologies for both short and long ranges of communication. The devices were assumed to be within the coverage of RAN, with different channel qualities. There are three ways that UEs can send their traffic to the RAN. They can send it through direct communication over a conventional cellular link or through short-range relaying link. Alternatively, communication can take place in two hops. The first hop is short-ranged and takes place between the source and relay. The second hop is long-ranged and takes place mainly between the relay and the RAN. The bounded ellipsoidal area in Figure 3 is the RAN's coverage area subjected to path loss and shadowing. In the mentioned ellipsoidal area, $S_1$ remains in the deep shadowing area and $S_2$, despite having good channel quality, suffers from low battery level. Both $S_1$ and $S_2$ can commence scanning their neighborhood using their short-range interface. For the mentioned scenario in Figure 3, $S_1$ will be able to identify $R_1$ and $S_2$ will be able to identify $R_2$ within their short-range coverage. Subsequently, $S_1$ and $S_2$ could start sending their traffic via relay nodes to the RAN. $S_3$ was assumed to have both good battery level and channel quality. Consequently, it could send directly to the RAN.

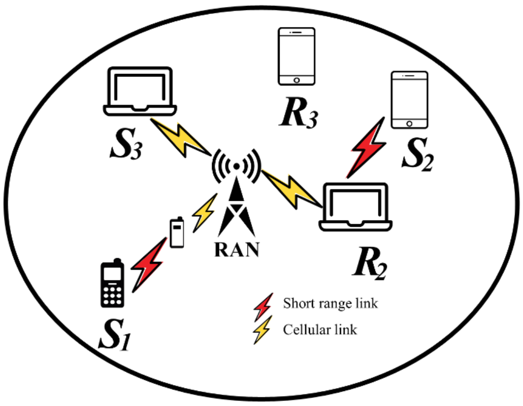


**Figure 3.** Coalitional short-range relaying.

Authors of [34] also assumed that the information gathered by the UEs could be shared with each other and they could periodically sense and communicate. There were two scenarios where coalitions could be formed among the nodes. A UE could join a nearby coalition after discovering it or certain UEs close to each other could create a new coalition by clinging to a certain profitable group strategy. The UEs were also responsible for acquiring information about the data rate and transmission power of the short-range and long-range links. This information could later be transferred to the RAN by the UEs. After receiving this necessary information from all the UEs, the RAN solved the problem of relay selection. Nodes were then informed by the RAN about their cooperative patterns.

The main concept of this routing scheme was in designing a coalitional relay selection game, in which the UEs built coalitions to pool their resources and relay packets for each other to decrease the overall energy consumption. A simple example of coalition formation consisted of two players. To design a characteristic function for this, the utility function was formulated as a weighted function of the energy saving process and battery life extension of UEs. The energy saving process was defined as the amount of energy saved through cooperation and battery life extension referred to the highest battery level of the UEs in a coalition. The utility was non-negative always, because nodes were supposed to act individually if there was no profit to be gained by forming or joining a coalition.

Technical strengths:

- The protocol is extremely energy-efficient and can perform well when several devices are involved.

Technical weaknesses:

- The main weakness of the protocol is not considering the downstream links (RAN to UEs)

Applications:

- The scheme is especially suitable for internet of things (IoT) devices deployed using WSN paradigm;
- The protocol can be applicable for a scenario where several devices are involved.

Possible future improvements:

- Consideration of downstream links;
- More routing metrics can be introduced in the performance analysis.

### 3.1.3. Reliable Coalition Formation Routing (RCFR) for WSNs

Reliable data delivery is challenging in WSNs. The routing protocol designed in [35] focused on this problem and ensured cooperation among nodes for reliable data delivery at a minimum routing cost. First, a coalitional game model was designed with a characteristic function based on performance metrics like packet forwarding rate and remaining energy. Subsequently, an algorithm with good convergence speed was designed to form coalition partitions in the game. Based on the coalitional game model, the authors finally designed a reliable coalition formation routing (RCFR) protocol that determines an appropriate route in the network on the basis of the lowest cost principle.

The authors in [35] considered the sensor nodes in WSNs as playing a coalitional game. A characteristic function was defined, along with the establishment of the pay-off allocation method among the coalition members. The coalitional game model was formulated as $\Gamma = <A, U>$, where $A = \{a_1, a_2, \ldots, a_n\}$ is a set of players that interact with each other and form groups that cooperate in routing. $U$ is the characteristic function. The strategy set consisted of two strategies. Assuming that the strategy set is $\Gamma_{a_i} = \{join, not\ join\}$, it referred to the strategies that a node may or may not join a certain coalition. A coalition set in [35] was denoted by $S$, where $S \subseteq A$.

The designed game had a frame work where it was assumed that time was divided into several slots. It was denoted by $t_K$ (K = 0, 1, 2, 3 . . . ..). The characteristic function of coalition $S$ at a time slot $t_K$ was presented as:

$$U\left(S^{t_K}\right) = \lambda|S| - f_S(PFR_i, RCR_i, RER_i), \quad (6)$$

where $\lambda \in (0, 1]$ was used for adjustment, $|S|$ represented the number of members in the coalition $S$, and $f_S$ was the function for calculating the cost. Then, $PFR_i$, $RCR_i$, and $RER_i$ presented the rate of packet forwarding, the rate of correctly reporting an event, and the rate of remaining energy for any node $i$, respectively. The pay-off function for any coalition member $a_i \in S$ at a time slot $t_K$ was calculated as:

$$\phi_{a_i}\left(S^{t_K}\right) = \frac{U\left(S^{t_K}\right)}{|S^{t_K}|}. \quad (7)$$

In coalitional game theory, forming appropriate coalitions is crucial. Nodes with common interest form coalitions and perform reliable data delivery as groups. Starting from a certain time slot, the nodes conduct a normal routing and forwarding process. They also collect historical records of the performance of the nodes. At the end of certain time slots, the performance metrics are updated, and the characteristic function computed. For all the coalitions S (S ⊂ A), with a source and destination node, the coalition formation is performed. The following parameters are assumed in RCFR: the players (sensor nodes), $A = \{a_1, a_2, \ldots, a_n\}$; computed characteristic function = $U\left(S^{t_K}\right)$; coalition partition, $\theta^* = S_1^{t^*}, S_2^{t^*}, \ldots, S_k^{t^*}$; strategy space, $\Gamma = \Gamma_1 \times \ldots \times \Gamma_n$; and routes from source to destination, $R = \{r_1, r_2, \ldots, r_k\}$. For each node $a_i$ from set $A$ and each route $r_i$ from set $R$, the pay-off could be calculated using (6). The node $a_i$ joins a coalition that has a maximum pay-off using the *join* strategy.

The designed coalitional game model was merged with the ad hoc on-demand distance vector (AODV) routing protocol [55] to integrate a fully functional routing protocol. The main differences between RCFR and AODV are:

- Information ($PFR_i, RCR_i, RER_i$) regarding the created coalitions is put into the table entry that is maintained by each node;
- In the route reply message of AODV, the route residual energy ratio and route cost fields are appended;
- Routes with the lowest costs are selected to find an optimal pathway using coalitional game theory;
- Rate of route residual energy parameter is presented for the optimization of the route maintenance mechanism.

In the simulation scenario in [35], 100 packets were sent to the destination. These packets were sent taking into consideration that a certain percentage of nodes were selfish. According to the simulation results in [35], as the number of selfish nodes increased, the packet delivery ratio decreased. RCFR was compared with the AODV protocol [55] and the method designed by Kazemeyni [57]. It performed better than the methods discussed in [55] and [57] in terms of packet delivery ratio. Furthermore, the simulation experiments were undertaken on route establishment time to evaluate the convergence time of RCFR. One hundred rounds of simulation were conducted and, in each round, the time for establishing a successful route between a source node and the destination node was recorded. After calculating the average route establishment time for the three protocols, it was concluded that the performance of RCFR was superior. The amount of consumed energy increased as the number of selfish nodes increased. The simulation results in [35] also demonstrated that RCFR outperformed all the compared protocols, even in terms of energy consumption.

Technical strengths:

- Reliable data delivery and route maintenance;
- The coalition formation game model can be integrated with the traditional protocols like AODV and dynamic source routing (DSR) [1] for better performance.

Technical weaknesses:

- RCFR did not consider the scenario where joining a coalition would yield a negative pay-off:
- No consideration for node failure scenario.

Applications:

- Applicable for a scenario where reliable data delivery is needed.

Probable future improvements:

- More routing metrics can be introduced for performance analysis;
- Implementation with DSR can be presented.

#### 3.1.4. Probabilistic Routing Scheme Based on Game Theory (PRGT)

Opportunistic networks (OppNets) do not always guarantee an end-to-end path from source to destination. In OppNets, routing is quite challenging because of the intermittent network connection. Nodes may act selfishly and show an unwillingness to participate in message forwarding. To address this issue, Qin et al. proposed a probabilistic routing scheme based on game theory (PRGT) to simulate cooperation among the selfish nodes [44].

In PRGT, an incentive probabilistic routing scheme for message transmission in OppNets was proposed. Based on the previous history of the nodes meeting each other, the authors of [44] established a first-order Markov process. Then, a game-theoretic approach was proposed to reduce the selfishness of the relay nodes and increase cooperation among them. All the messages to be transmitted and received were sole identities that were addressed as commodities. Nodes in the network were assumed to have virtual money that could be used to buy and sell the commodities. When nodes did not participate in message forwarding, they would lack enough money to have more profits. To precipitate cooperation among nodes, if a destination node received a message, all the other nodes involved in the transmission process got rewarded.

PRGT considers a general opportunistic model, where there is no assurance that an end-to-end path would exist. Nodes in the network communicate with each other via a store-carry-forward mechanism. Initial node energy is represented as $E_s$ and the buffer size as $B_s$. The authors introduced a credit clearance center (CCC) and each node had an account in it. CCC is basically a server connected to the Internet. When a message is forwarded by a node, it is supposed to produce a receipt of a digital signature. After that, the receipt is submitted by both the message carrier and the relay node. When the destined node finally received the message, it would inform the CCC about the reception and the CCC awards all the relay nodes. This phenomenon indicates that the relay node would have enough virtual money to forward more messages so that they could gain more profits.

To maximize cooperation among the nodes, the message forwarding process was modeled as a bargaining game. The game consisted of two players: buyer and seller. The message-carrying node was assumed as a seller ($S$) and the relay as a buyer ($B$). It was necessary that both players reach a transaction price for every message in a round. A deal was put forward by seller $S$ first at the beginning of the bargaining game. Buyer $B$ must decide if the deal would be accepted. If the deal was accepted, the game ended. Otherwise, it would go to the next round. This process was repeated unless the transaction was done completely.

In PRGT, every node is considered as a message storage entity. Therefore, the forwarding process of the message ($m$) is regarded as a binary set having a series of discrete positions ($P_i^m$), and time elements ($T_i^m$). The transfer process of the messages is described as:

$$PT = \left\{(P_1^m, T_1^m),\ \ldots,\ \left(P_i^m,\ T_i^m\right),\ \ldots, (P_n^m, P_n^m)\right\}, \tag{8}$$

where $(P_i^m, T_i^m)$ indicates that at the $T_i^m$ moment, the message $m$ is in the position $P_i^m$. The process was also described as a Markov chain [44]. Nodes in the network represent the set of states ($S$): $S = \{1, 2, 3, \ldots, i, \ldots, n\}$. Here, $i$ denotes a message in a certain node $N_i$. The transfer probability matrix is denoted as $P$. $Pi, j \in P$ denotes the transition probability between states $i$ and $j$. In other words, it is the probability of the message $m$ to be forwarded from $N_i$ to $N_j$.

The selfishness of the nodes participating in the routing process is divided into two types. One is self-centered selfishness (SCS), which is related to residual energy and buffer the nodes. The other is social selfishness (SS), which denotes the unwillingness of the nodes to forward messages to the nodes that are not friendly. In OppNets, the energy and buffer of the nodes are pretty much limited because of the overhearing issues. Therefore, SCS is prominent in OppNets because the limited energy and buffer size of the nodes compel them to deal with their own messages only. SCS is mathematically defined using the following equation:

$$SCS = (\alpha . \frac{E_r(t)}{E_s} + \beta . \frac{B_r(t)}{B_s} + 1)^{-1}, \quad (9)$$

where $E_r(t)$ is the remaining energy if node $r$ at time $t$. Similarly, $B_r$(t) is the remaining buffer of node $r$ at time $t$. $\alpha$ and $\beta$ are the influence weights of energy and buffer on the node's SCS, respectively. SS is a common feature among the nodes in OppNets.

In [44], the proposed PRGT protocol was compared with some classical routing algorithms (epidemic routing, SprayAndWait) in terms of message delivery ratio, latency, and overhead ratio. PRGT showed a better performance in terms of all the metrics.

Technical strengths:

- It could successfully deal with the selfishness of the nodes and build cooperation for better routing to save energy;
- The mathematical formulation for the bargaining game is sound and in detail. It will be convenient for real life implementation with the sensor networks.

Technical weaknesses:

- Proposed protocol requires a centralized scheme. Not suitable for distributed architecture.

Applications:

- Applicable for a scenario where there is a reliable backbone for the Internet. Not suitable for deployment during natural disasters.

Probable future improvements:

- More routing metrics can be introduced for performance analysis.

#### 3.1.5. Comparison of the Protocols Based on the Technical Strengths and Weaknesses

The technical strengths and weaknesses of the protocols discussed in Section 3.1 are comparatively summarized in Table 4 for readers.

**Table 4.** Comparison of routing protocols based on cooperative games in terms of technical strengths and weaknesses.

| Protocol | Technical Strengths | Technical Weaknesses |
|---|---|---|
| CH-C-TEEM [1] [31] | • Cooperation among CHs leads to energy efficiency.<br>• Consideration of network security via elimination of the malicious nodes. | • Routing metrics like packet delivery ratio, end-to-end delay are not considered.<br>• Comparison with more of the existing state-of-the-art routing techniques in terms of important routing metrics. |
| RCFR [2] [35] | • Reliable data delivery and route maintenance.<br>• Integration with other protocols for better performance is possible. | • No consideration for node failure scenario. |
| Assignment game approach [34] | • Extremely energy-efficient and can perform well when a lot of devices are involved. | • No consideration for the downstream links |
| PRGT [3] [44] | • Avoidance of selfishness among the nodes and building cooperation for better routing to save energy. | • Not suitable for distributed architecture. |

[1] Cluster Head Cooperative Trustworthy Energy-Efficient multiinput multioutput; [2] Reliable Coalition Formation Routing; [3] Probabilistic Routing Based on Game Theory.

### 3.2. Routing Protocols Based on Noncooperative Games

#### 3.2.1. Resource Allocation Strategy for Cluster-based WSNs

Lee et al. designed a fair resource management scheme for WSNs based on the Nash bargaining solution (NBS) [36]. NBS is a game theoretic concept that provides a solution to game theory by maximizing the product of utilities that a user can obtain through cooperation compared to that achieved through noncooperation. The authors of [36] also modeled the energy consumption for the cluster members and data transmission.

In this routing scheme, the focus was on the resource allocation for frequency interference between clusters. A static cluster based WSN was assumed. Each cluster had the same number of members and they used identical frequency and bandwidth. CMs were assumed to communicate with the CH in a time division multiple access (TDMA) fashion. The sensor nodes with omni-directional antennas were used. The number of members in a certain cluster was equal to the time slot length ($N$) of a frame. The scheduling order was pre-assumed for the designed routing scheme. In [36], an additive white Gaussian noise channel was used for each link. An energy consumption model was presented that only considered the energy consumption of the CMs. The energy consumption of the CHs and sink node were ignored. The minimum transmission power required to transmit data packets can be given by:

$$p_i(n) = I_i(n)\left(2^{\frac{r_i(n)}{W_i(n)}} - 1\right)/|h_{ii}(n)|^2, \tag{10}$$

where $n$ is a particular time slot, $i$ is any node in a certain cluster, $r_i(n)$ is the rate of node $i$ in time slot $n$, $h_{ii}(n)$ denotes the channel gain of a link from a cluster member to its CH, $W_i(n)$ is the bandwidth of operation, and $I_i(n)$ is the total amount of interference and noise power. The lifetime of a cluster member $i$ was formulated as,

$$\tau_i(n) = \frac{E_i}{P_i(n)}, \tag{11}$$

where $\tau_i(n)$ is the network lifetime, $P_i(n)$ is the minimum transmission power needed at a certain data rate, and $E_i$ is the energy of the cluster member $i$. A set of achievable utility $U$, and a disagreement vector $u^c = [u_i^c, \ldots, u_L^c]^T$ were used to present NBS. The disagreement vector was designed using a noncooperative game. The NBS was applied for resource allocation between clusters through the utility of the CMs. The utility was modeled based on the lifetime of the CMs. The utility function was designed as,

$$U = \left\{u_i(W_i(n)) | W_i(n) \in W_n, u_i(W_i(n)) \geq u_i^c\right\}, \tag{12}$$

where $W_n$ is the frequency vector, $W_i(n)$ is the bandwidth of operation, and $u_i^c$ is the disagreement vector for node $i$. When there was a failure between the clusters while bargaining, the disagreement vector of the introduced model was obtained. The model assumed that the disagreement vector consisted of constants to put an emphasis on resource allocation for successful bargaining. The utility function ($U$) was determined to be convex and NBS was unique. It was obtained through the following equation:

$$\rho = arg\ max_{u_{i \in \mathrm{U}}} \prod_{i=1}^{L}\left(u_i - u_i^c\right), \tag{13}$$

where $u_i$ is the utility of node $i$, $U$ is the overall utility, $L$ is the number of nodes in a certain cluster, and $u_i^c$ is the disagreement vector for node $i$. Finally, for a certain slot $n$, the optimal power control and resource allocation problem was solved in a joint manner using the following formulation:

$$max_{u_{i \in \mathrm{U}}} \sum_{i=1}^{L} \log\left(u_i(W_i(n), p_i(n)) - u_i^c(n)\right), \tag{14}$$

where $W_i(n)$ is the fraction of bandwidth in slot $n$, $W$ is the total bandwidth of operation, and $u_i^c$ is the disagreement vector for node $i$.

Technical strengths:

- Development of an energy consumption model with resource allocation scheme;
- The coalition formation game model can be integrated with the traditional protocols like AODV and DSR for a better performance.

Technical weaknesses:

- The energy consumption model is incomplete. It was based on the data transmission of the CMs. The energy consumed by the sink node and CHs were ignored.

Applications:

- Application cannot be specified owing to the incomplete protocol.

Probable future improvements:

- The data transmission phase between the CHs and sink node should be included;
- The energy consumption for data reception can be included in the energy consumption model;
- A performance comparison with the existing state-of-art protocols can be added.

#### 3.2.2. Inter Cluster Routing Algorithm for a WSN

Link quality and node residual energy are two key factors to be considered in routing. Xin et al. designed a routing protocol based on game theory taking into consideration these two key factors [39]. They developed a game model based on the quality of service (QoS) and node residual energy. They claimed that the designed game theoretic model had a unique Nash equilibrium solution.

The assumed network in the protocol [39] had sensor nodes with limited energy. A hexagonal cluster topology identical to a cellular network was deployed. The CH was placed at the center and had a fixed position. The ordinary sensor nodes gathered data required by the system in a periodic manner. They sent the data to their own subnet CH. The CH processed this data to further transmit it to the sink node through multiple hops. The CHs had limited range and were bound to collaborate with each other for data forwarding.

The clustering algorithm designed in [39] can be regarded as a compromise between the network QoS and energy consumption. From the perspective of game theory, it was a game between the QoS and energy consumption of the nodes. The Nash equilibrium of the game was determined through the game solving process that extended the survival time of the network. The CH nodes that forwarded the data to the sink nodes were the players of the game. The CHs had to collaborate with each other for an extended range. There were two strategies, from which one could be chosen: (i) being a relay CH to help in the data forwarding process to the sink node, and (ii) not being a relay. The utility function was defined with the QoS demand ($M_i$) and the residual energy of the nodes,

$$U(M) = \sum_{i=1}^{k} M_i e_i - \frac{1}{2\left(\sum_{i=1}^{k} M_i^2 + 2\rho \sum_{i\neq j} M_i M_j\right)} - \sum_{i=1}^{k} E_i M_i, \tag{15}$$

where $M = \{M_1, M_2, \ldots, M_K\}$ is the QoS of $k$ different nodes, $i$ and $j$ are CH nodes where one node wants to transfer data to the sink node and another has to relay it, $\rho$ is the competitive factor between different values of QoS, and $e_i$ is the efficiency factor of $M_i$. Normally, the CH node would select a route with good QoS for packet forwarding. If the QoS requirements were higher, the energy consumption of the node would also be higher. Assuming that a node $i$ decided to use node $j$ as the next hop node and both $i$ and $j$ had the same amount of maximum energy, the decision function to select $j$ as a next hop node was expressed as,

$$u_j = \frac{\pi_j}{C_j}, \tag{16}$$

where $\pi_j$ is the revenue function for node $j$ and $C_j$ is the cost function for node $j$, if it is selected as a relay node. $\pi_j$ and $C_j$ were expressed by the following two equations:

$$\pi_j = M_{ji}\rho + \frac{E_j}{E}(1-\rho), \tag{17}$$

$$C_j = (E_j^r + E_j^t).n/\left(E_i + E_j\right), \tag{18}$$

where $M_{ji}$ is the QoS between node $j$ and $i$, $E_j$ and $E_i$ are the current surplus energy of nodes $j$ and $i$, respectively, E is the initial energy of the node, $\rho$ is an adjustable parameter, $E_j^r$ is the energy consumed by node $j$ while receiving data, $E_j^t$ is the energy consumed by node j while transmitting data, $n$ is the forwarding data volume to node. The best strategy function in the designed game of this protocol was $BRF(E_{-i}) = argmax\ (E_{-i} \cup \{E_i\})$. Here, $E_{-i}$ is the residual energy of the nodes except for node $i$. The vector, $E^* = \left(E_1^*, E_2^*, \ldots, E_{i-1}^*, E_i^*, E_{i+1}^*, E_k^*\right)$ was regarded as the Nash equilibrium as it was true for all the nodes.

Figure 4 illustrates a network scenario presenting the discussed protocol. Node $A$ does not have a range to transmit data directly to the sink node. It must collaborate with another CH node, node $B$ to transfer data. The designed game model in the protocol was used to decide if node B will act as the relay node for A.

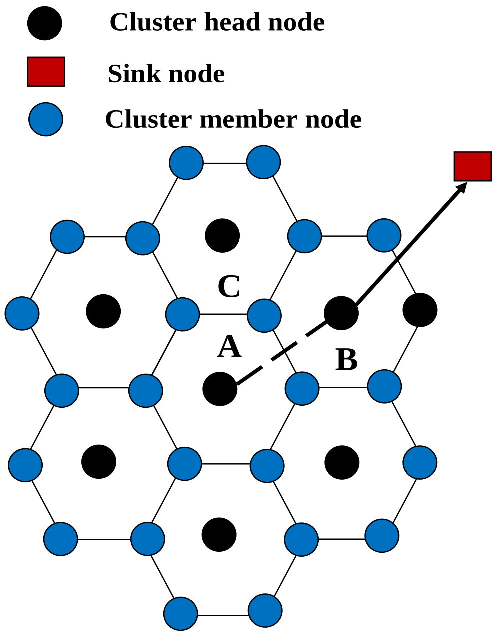


**Figure 4.** Cooperative data transmission between two CHs in the protocol.

Technical strengths:

- Leads to higher residual energy of the nodes.

Technical weaknesses:

- The protocol is supposed to suffer from an energy hole problem. As CHs aggregate data to the sink node through cooperation, the CHs that are lying in the vicinity of the sink node will deplete energy faster;
- The authors of [39] claimed to reach Nash equilibrium point using certain conditions. Their calculations were not sufficient to prove their claim on finding the equilibrium point;
- The protocol only defines communication among the CHs. Communication between CHs and CMs should have been defined or assumed.

Applications:

- It is challenging to specify any application for this protocol because it does not elaborate intra-cluster communication. Furthermore, knowing that the protocol may suffer from an energy hole problem, the network failure owing to nodes near the sink node dying early is inevitable. Improvement of this protocol before real time deployment is necessary.

Probable future improvements:

- This kind of protocol, where data is aggregated by the CHs to the sink node in a cooperative manner, requires multiple sink nodes. The protocol can be redesigned by putting in effort to deploy multiple sink nodes to avoid energy hole problem and to support numerous sensor nodes participating in routing.

### 3.2.3. Routing Framework based in the Energy and Delay Conservation

To determine optimal routing paths using signal-to-interference and noise ratio (SINR), Jamin et al. designed a game theory-based routing protocol in [37] for WSNs. The game was modeled to be a noncooperative, dynamic, and incomplete information game. The sensor nodes were assumed to be static and they acted as players in the designed game. The utility function was formulated to facilitate a balance between delay and energy consumption. The authors of [37] demonstrated that the Nash equilibrium was self-imposed if the players played their best response strategy.

The designed routing game in [37] considered the SINR and channel capacity between two communicating nodes. The objective of this routing scheme was to find out a route that could jointly decrease the energy consumption and delay. The formulated game precipitated the system to achieve Nash equilibrium. Owing to this, all the nodes in the network could optimally utilize its energy and increase its lifetime. The network considered consisted of randomly deployed nodes. The nodes were homogeneous in nature. The maximum amount of interference was infinite in amount. The nodes in the network acted as players in the game, as mentioned earlier, and could choose a strategy depending on the utility function. The selection of a node as a next hop depended on the congestion at that node.

The designed game in [37] consisted of $N$ players (sensor nodes), where $N = \{i_1, i_2, i_3, \ldots, i_n\}$. Each player $i$ had its own finite set of possible strategies. The strategies declared were the combination of the next forwarding node and transmission power level. A pay-off function to map the strategies was also designed. All the players in the game were bound to choose a strategy that would reduce the long-term cost and increase longevity. Even though the nodes were assumed to be homogeneous, the information regarding the quality of data transmission and chosen optimal path were not shared among the players. Consequently, the game was mentioned as an incomplete information game. The nodes could maximize their benefit by choosing the transmission energy level and optimal path towards the sink node. In every iteration of the game, pay-offs were generated based on the mentioned parameters. The utility of a chosen strategy for the $i$th node was addressed as $S_i$. All the other players had a strategy $S_{-i}$. The designed utility function of the game model in this routing scheme was:

$$U_i(S_i, S_{-i}) = \frac{LR}{Mp_i} + f(\gamma_i), \tag{19}$$

where $L$ is the information bits at a rate $R$, $p_i$ is the power level of node $i$, and $f(\gamma_i)$ is the efficiency function. This function was defined as $f(\gamma_i) = (1 - 2P_e)^M$. Here, $P_e$ is the bit error rate, $\gamma_i$ is the SINR of node $i$. The cost function of the game for the $i$th node was designed using the energy consumption of the node and delay incurred in routing. It was expressed as:

$$C_i = \left(\frac{E}{E_{ref}}\right) + \left(\frac{D}{D_{ref}}\right), \tag{20}$$

where $E$ is the initial energy of the nodes, $D_{ref}$ is the reference delay in the network, $Delay$ is the routing path delay, $E_{ref}$ is the reference energy in the network. The net utility of the game was given by:

$$U_{net}(S_i, S_{-i}) = \frac{LR}{Mp_i} + f(\gamma_i) - \frac{E}{E_{ref}} + \frac{Delay}{D_{ref}}. \tag{21}$$

For each stage of the game, the net utility was calculated for all neighboring nodes and the node that maximized the net utility.

According to the performance study in [37], the delivery latency was improved in the designed protocol, and its energy consumption was considerably less than that of the destination-sequenced distance vector routing [1], AODV [55], and DSR [1]. This protocol claimed to outperform the two very popular routing protocols of AODV and DSR in terms of energy efficiency only. The simultaneous transmission of all the nodes can easily lead to network congestion in this protocol.

Technical strengths:

- The protocol can successfully decrease network delay to a significant amount;
- Energy consumption was successfully decreased to a fair amount.

Technical weaknesses:

- The authors did not consider sufficient routing metrics in the performance comparison. A performance comparison graph on network lifetime was necessary to prove the robustness of the protocol with the compared ones.

Applications:

- Applicable where an application requires continuous data delivery without any delay.

Probable future improvement:

- The authors claimed that the Nash equilibrium was self-imposed. They did not provide sufficient proof to support their claim.

#### 3.2.4. Cooperation Optimal Protocol for Multi-rate Opportunistic (COMO) Routing and Forwarding

Multi-rate opportunistic routing can achieve high throughput in WSNs. However, the performance of a multi-rate opportunistic routing cannot be ensured when the nodes participating in routing have selfish behaviors. In [38], Wu et al. designed a cooperative-optimal protocol for multi-rate opportunistic routing (COMO) that can guarantee the faithfulness of each player.

The presented routing protocol achieved social efficiency and Pareto-efficient Nash equilibrium with faithfulness as a given property. The term social efficiency implied the maximum end-to-end throughput in the COMO. In the Pareto-efficient Nash equilibrium, no node can improve its utility without reducing the utility of at least one player. This routing scheme was the first scheme to integrate game theory with opportunistic routing. The authors of [38] modeled the problem of multi-rate opportunistic routing as a strategic game. Each player (node) in the routing game belonged to a set $N$. S was the set of strategies in the COMO where $S = \{S_1, S_2, S_3, \ldots, S_n\}$. The utility function ($u_i$) was expressed as the difference between payment $p_i$ and cost $c_i$ for forwarding data packets:

$$u_i = p_i - c_i. \tag{22}$$

It was assumed that the players (nodes) were rational and they aimed to increase their net utilities.

Technical strengths:

- Considerable amount of throughput is gained in presence of the selfish nodes.

Technical weaknesses:

- No comparison with the existing state-of-art protocols was demonstrated.

Applications:

- Applicable for high throughput multimedia data transmission.

Probable future improvements:

- The only routing metric that COMO [38] covers is the end-to-end throughput. This metric is defined as the number of packets transmitted per second. Certain other important routing metrics for the performance comparison could have been considered to prove the robustness of the designed protocol.

3.2.5. Energy-Aware Trust Derivation Scheme

Security is a prime concern for a WSN-based IoT. The traditional routing protocols in most cases assume that the network environment is trustworthy, which is not pragmatic. The WSNs are deployed in remote places and are vulnerable to security attacks that are almost impossible to manage physically and may result in performance degradation, accompanied by a malfunction of the WSN. Cryptographic schemes can be a solution to deal with the security concerns, however, they are not feasible for memory-limited tiny sensor nodes with limited processing power. Because of the lesser complexity in computation and higher resistance in the internal attacks, trust evaluation [58,59] is an effective solution for WSNs, contrary to cryptographic measures. Duan et al. in their paper [32] designed an energy-aware trust derivation scheme for WSNs. The aim of this scheme was to decrease the energy consumption and latency of the network. The trust derivation process refers to the method of calculating the synthesis trust value. The synthesis trust value is based on the combination of the direct trust and collected indirect trust. The direct trust is computed when the nodes participating in data communication are directly observed for trustworthiness. Conversely, indirect trust is obtained based on the recommendation of the other nodes. Readers can refer to [60–63] for further information about the trust derivation process.

Initially, the authors of [32] provided a method to analyze the risk-strategy to simulate cooperation among the nodes. Subsequently, a trust derivation dilemma game (TDDG) was designed to decrease the overhead of the network. Finally, through simulations, it was demonstrated that the designed routing scheme could simultaneously ensure energy consumption and latency. In the designed routing protocol, a few sink nodes and several sensor nodes were distributed in the network area. A node in the network area could detect an event and transmit the data packet. End-to-end communication was achieved in a multi-hop way. Compared to normal sensor nodes, the sink nodes were assumed to be more trustworthy. Two types of attacks, active and passive, were tackled by the designed routing scheme. In passive attacks, the sensor nodes involved in routing passively gather sensitive information or behave in a selfish manner by not collaborating with other sensor nodes in the routing process. In the case of active attacks, the sensitive information is requested directly by the malicious nodes. This kind of attack directly harms the normal operation of the WSNs.

Each sensor node in the network was responsible for observing the behavior of the nodes within its vicinity falling under the radio range. The observation results were used for the calculation of trust. A random node in the network had trust level $T$ that was formed with direct trust $T_D$ and indirect trust $T_I$. The final trust computation results were used for secure routing and access control. The trust computation model that was used in the paper [32] was adopted from [64]. Figure 5 illustrates the trust deviation for an arbitrary node. In Figure 5, $j$ represents the node being evaluated and $i$ is the node that is conducting the evaluation.

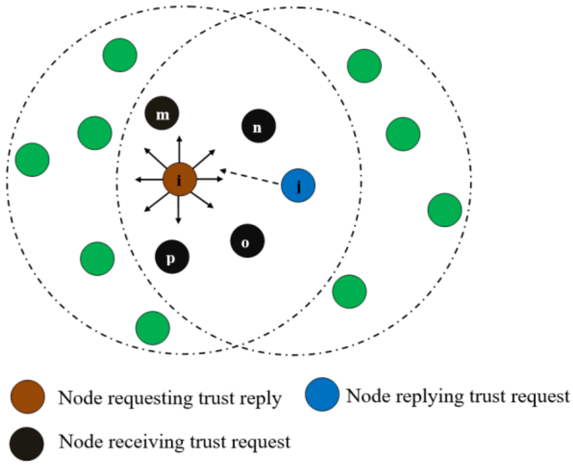


**Figure 5.** Process of trust derivation.

The hop-limited trust derivation procedure of the routing was as follows. The trust deviation process was initialized by a source node *i*. The target was node *j*. The node *i* broadcast a trust request packet towards node j. A hop-limit value was introduced to handle the overhead of the flooding mechanism. When a node received a trust request packet, it checked whether it had received an identical request. If it had, the packet was discarded within the shortest possible time. However, if the hop limit was greater than zero, the packet was rebroadcast. The node that obtained the trust request packet transmitted towards it should subsequently check if node *j* was its neighbor. If node *j* was a neighbor, it might unicast a trust reply to source node *i* using a reverse route. The decision of node *j* to reply or not depended on a dilemma game, which is explained later in this section. After getting the recommendation, the source node *i* computed the trust value by joining the direct trust with the indirect trust. At this stage, node *i* decided if node *j* could be trusted based on the obtained computed result.

This routing scheme considered recommendations from the neighbors of the evaluated node. This is mainly because the malicious behaviors of a node can be best observed by its neighbors and this mechanism can reduce network overhead. The algorithm applied for trust computation was beyond the scope of this routing scheme [32]. The authors of [32] assumed that a robust trust evaluation algorithm was implemented for trust computation. However, an efficient design was required to ensure that the trust information obtained from a certain set of selected neighbors fulfilled the desired security requirements. A game-theoretic approach was considered to deal with this problem.

The TDDG was designed with $N$ nodes, where $N$ presents the number of specified evaluated nodes' neighbors, excluding the evaluating node. There were two strategies for the participating nodes: "reply" and "not reply". "Reply" refers to the event that nodes replied to the evaluating node during the trust request reception. "Not reply" refers to the strategy where the nodes would ignore the trust request after receiving it. Assuming that $k$ is the minimum number of recommendations needed to fulfill the security requirements, the network was regarded as secured if the number of recommendations was greater than $k$. The nodes participating in the TDDG did not include themselves in the game if they had low energy. There could be two cases in the TDDG. Considering a case where $k = 1$, the security requirement could be met if any node sent a trust reply. The pay-off matrix, probability of sending trust reply, strategic form, and Nash equilibrium were derived for this case. There could also be a case where $k > 1$. The strategic form and Nash equilibrium for TDDG in this case were derived too.

Two important parameters for this scheme were the utility and cost for an arbitrary node for trust reply. From the simulation results in [32], it was concluded that the energy consumption increased as the ratio of the above mentioned two parameters increased. The reason for this is that the high ratio of utility and cost encourages nodes to reply to a trust request packet, which increases network overhead and congestion resulting in long network latency.

Technical strengths:

- Security of a WSN is considered with highest priority;
- Performance analysis with security attacks like bad mouthing [65] and distributed denial of service (DDoS) [66].

Technical weaknesses:

- No performance comparison with the existing state-of-the-art algorithms;
- The trust derivation problem is hop-limited. This can lead to a contradiction. Flooding in an uncontrolled and random manner may lead to energy wastage and latency. For this, hop-limited flooding is useful, but it may lead to reduced trust information collection. The authors of [32] did not mention any solution for this contradictory situation.

Applications:

- Highly suitable and applicable for military applications.

Possible future improvements:

- Introducing more routing metrics for performance evaluation;
- Comparison of the performance analysis with any existing state-of-art routing protocol;
- Introducing a new intelligent method of broadcasting other than hop-limited flooding to avoid energy wastage and facilitate efficient trust information gathering simultaneously.

#### 3.2.6. Game Theory-based Energy-efficient Routing Algorithm (GERA)

Energy consumption is a critical concern for WSNs and clustering techniques are popular for reducing energy consumption via lessening the number of transmissions to the sink node. Usually, routing protocols based on clusters have a CH in each cluster. Selecting a CH in a cluster is a difficult task and should be handled carefully, as selecting a node with a lower energy level as the CH may result in network malfunction. In their paper, Pitchai et al. [33] designed a game theory-based energy-efficient routing algorithm (GERA). It is a clustering algorithm that adopts game theory, in which CHs are optimally selected based on a utility function of the node. The cluster formation process relies on a cost function.

The designed routing scheme consists of three phases: CH selection, cluster formation, and data transmission. CHs are optimally selected using game theory. Before this process, all the nodes in the network gather local information of their neighboring nodes and broadcast a “hello” message. The nodes in the network are aware of the number of neighbors who had received the “hello” packets. The “hello” message consists of information like the location of the node, node energy level, and node’s existence. The CH election game is defined as:

$$CG = \langle N,\ S,\ U\rangle, \tag{23}$$

where $N$ is a set of players (sensor nodes in this case), $S$ is a set of available strategies, and $U$ is the utility function. The strategy set consists of two elements. Thus, the strategy set, $S = \{AVOW, DISAVOW\} = \{A, DA\}$. *DISAVOW* refers to the strategy of not declaring a node as a CH and *AVOW* presents the strategy of a node being declared as a CH. As mentioned earlier, assuming $N$ players are taking part in a clustering game, the utility function of any player $i$ could be defined as:

$$U(S_i) = \begin{cases} G - E_A\ if\ S_i = A, \\ G - E_{DA}\ if\ S_j = A\ where\ i \neq j, \\ 0\ if\ S_j = 0\ for\ all\ j \in N, \end{cases} \tag{24}$$

where $U(S_i)$ is the utility function of the node $i$, $G$ is the gain obtained by each node during packet forwarding to the sink node, $E_A$ is the energy consumed by the CH in forwarding the aggregated data to the sink node, and $E_{DA}$ is the amount of energy consumed by the CM to transmit the data to the CH.

After certain nodes have declared themselves as CHs, they do not participate in the CH election process and the probability of these nodes being CH in the upcoming round is set to zero. The nodes that do not become CHs send a request message to the nearby identified CH. Based on the already enrolled cluster members, the CH could either send a *JOIN_ACC* message that allows a requesting node to be a cluster member or it could send a *REQ-REJ* message to reject a requesting node from being a cluster member. The CHs directly transmit the data packets to the sink nodes in the data transmission phase of the routing protocol.

The routing metrics considered in this protocol are energy consumption and packet delivery ratio. In this protocol, the total energy consumption of a node is defined as the amount of energy consumed by a node while performing its role in routing. It is the summation of the energy required for sensing the data, aggregating the data, and transmitting the data in [33]. In this protocol, the packet delivery ratio is considered as packets delivered by the node in the network for a certain number of rounds. The GERA claims superiority over the density-based energy-efficient game-theoretic routing algorithm [67] and low-energy adaptive clustering hierarchy (LEACH) [68] routing protocols based on these parameters.

Technical strengths:

- Energy is well conserved by preventing the nodes that were CHs in the previous round from being CHs in the ongoing round;
- Energy consumption was considered for both data transmission and reception.

Technical weaknesses:

- It is basically an extension of the LEACH protocol [68], with an improvised method of CH selection using game theory. The authors did not elaborate on the intra-cluster communication between the CMs and CH. Further, an effort should have been made to explain the LEACH protocol for a better understanding of GERA;
- The protocol cannot adapt to any kind of topology change and node failure.

Applications:

- GERA can be applied to typical static WSNs that are not subjected to any kind of topology change.

Possible future improvements:

- Explanation of intra-cluster time slotting can be added;
- Routing metrics like end-to-end delay and latency can be introduced for performance comparison.

#### 3.2.7. Comparison of the Protocols Based on the Technical Strengths and Weaknesses

The technical strengths and weaknesses of the protocols discussed in Section 3.2 are comparatively summarized in Table 5 for readers.

**Table 5.** Comparison of routing protocols based on noncooperative games in terms of technical strengths and weaknesses.

| Protocol | Technical Strengths | Technical Weaknesses |
| --- | --- | --- |
| Resource allocation strategy for clustering-based WSNs [36] | • Energy consumption model with resource allocation scheme.<br>• Can be integrated with the traditional protocols like adhoc on-demand distance vector routing and dynamic source routing for better performance. | • Incomplete energy consumption model |
| Intercluster routing algorithm for WSNs [39] | • Leads to higher residual energy of the nodes. | • Suffers from an energy hole problem.<br>• Communication between CHs and CMs should have been defined or assumed. |
| Routing framework based on energy and delay conservation [37] | • The protocol can successfully decrease network delay to a significant amount.<br>• Energy consumption was successfully decreased to a fair amount. | • Do not consider sufficient routing metrics in the performance comparison. |
| COMO [1] [38] | • Considerable amount of throughput is gained in presence of the selfish nodes. | • No comparison with the existing state-of-art protocols was demonstrated. |
| Energy-aware trust deviation scheme [32] | • Security of a WSN is considered with highest priority. | • No performance comparison with the existing state-of-the-art algorithms. |
| GERA [2] [33] | • Energy is well conserved by preventing the nodes that were CHs in the previous round from being CHs in the ongoing round. | • The protocol cannot adapt to any kind of topology change and node failure |

[1] Cooperation Optimal Protocol for Multirate Opportunistic Routing; [2] Game-Theory-Based Energy-Efficient Routing Algorithm.

## *3.3. Routing Protocols Based on Evolutionary Games*

### 3.3.1. Game Theoretic Energy Balanced (GTEB) Routing Protocol

Sensor nodes in the network are energy constrained and the lifetime of the network is always limited in a WSN. It is better for the network if the nodes die at the same time, as the network functionality is ensured if all the nodes are alive at the same time. Addressing this problem, Mehmood et al. presented a novel game theoretic energy balanced (GTEB) geographical routing protocol that could successfully increase network lifetime, ensuring the fact that the forwarding nodes will die at approximately the same time [40]. Based on the network density, the forwarding regions of a sender node were divided into a set. To deduce the amount of forwarding traffic to be sent to those regions, the EGT was used. This operation also depended on the available energy in a region. The classical game theory (CGT) was used to select one forwarding node within the forwarding region to forward a data packet.

The main design concern of GTEB is to ensure energy balance to the randomly deployed homogeneous sensor nodes, that are assumed to have a transmission range of $r$ and an initial energy of $E$. The nodes are assumed to have location awareness, with each possessing the knowledge of their destination node. Every single node could report any nearby event periodically to the destination node. The transmission range in GTEB is divided into $K$ subregions, depending on the network density

$\rho$. A sending node forwards a data packet to a certain subregion based on EGT. The neighboring nodes of the sender in the subregions must decide for which region the data packet has been sent. To make this process easy, the sending node incorporates the angle that encompasses the desired subregion, location, and the number of sensor nodes in that region. Subsequently, one of the nodes in the selected subregion is selected, using CGT as a forwarding node. The selected node again deduces a forwarding zone using EGT and a forwarding node is chosen from the newly selected forwarding zone. This process continues until the destination node is determined.

In this section of the protocol description, the formulation of EGT in GTEB will be briefly discussed. In the case of EGT, a sender node is supposed to distribute $\boldsymbol{\lambda}$ packets over $K$ forwarding subregions. This $\boldsymbol{\lambda}$ parameter can be represented as:

$$\lambda = \sum_{k=1}^{k} \lambda_k, \tag{25}$$

where $\lambda_k$ is the number of packets to be transmitted to the subregion $k$. The selection of a subregion by the sender node depends on the adoption of a particular strategy from the strategy set. The sender node plays the evolutionary game for the packets. The proportion of the packets to be forwarded through a certain region can be formulated as:

$$X_k = \frac{\lambda_k}{\lambda}. \tag{26}$$

The vector $X$ presents the population state over all the subregions. It is presented as:

$$X = X_1,\ X_2,\ \ldots, X_k. \tag{27}$$

This vector can be calculated using the replicator dynamics discussed later in this section of the paper. Before digging deep into the replicator dynamics, the fitness function and switching probability must be designed for EGT. The fitness function $F_k(X)$ can be presented as:

$$F_k(X) = E_k - \lambda X_k(2N_k E_{TR} + E_{TX}), \tag{28}$$

where $E_{TR}$ is the energy consumed by a node while receiving a packet, $E_{TX}$ is the energy consumed while transmitting the same packet, $N_K$ is the number of nodes in the $k^{th}$ subregion, and $E_K$ is the remaining energy in subregion $k$ for a packet. The fitness-function expresses that if the remaining energy per packet in a subregion is greater than the energy needed for data reception and forwarding, the data packet will be forwarded. The replicator dynamics in EGT are used to capture the variation in the proportions of the population. Here, the population refers to the data packets. This packet population opts for different region forwarding strategies. It is the decision of the sending node that up to which proportion the data packets will be transmitted to different subregions. At every single game-interval, the sender attempts to evolve new proportions of packets by switching them to variant subregions. The switching probability $P_{kl}(X)$ from any subregion $l$ with fitness $F_l(X)$ to the selected subregion $k$ with fitness $F_k(X)$ is calculated in GTEB [40]. A converse option (from subregion $k$ to subregion $l$) is calculated too. The replicator dynamics that capture the net change in the number of packets for region $k$ can be given as:

$$X_k = \sum_{l \neq k} X_l p_{kl}(X) - \sum_{l \neq k} X_k p_{lk}(X), \tag{29}$$

where $X_l$ is the vector presenting the population state over the subregion $l$, $X_k$ is the vector presenting the population state over the subregion $k$, $P_{kl}(X)$ is the switching probability from any subregion $l$ with fitness $F_l(X)$ to the selected subregion $k$ with fitness $F_k(X)$, $P_{lk}(X)$ is the switching probability from any subregion $k$ to subregion $l$.

To determine the forwarding node within the selected forwarding region (selected using EGT), a noncooperative game is formulated. The main goal is to establish the energy balance in the region. In this energy balanced noncooperative game, $N$ is a set of nodes (players) in the selected subregion and it is mandatory that $N$ at least had two elements for playing the game. If there is one element, it would transfer the data packet directly to the destination. The strategy set $S$ contains two elements, $S = \{T, \overline{T}\}$, where T presents the data transmission of a node and $\overline{T}$ presents no data transmission of a node. We do not further elaborate the methods to determine the pay-off calculation and Nash equilibrium that were obtained by the authors of [40], as our focus in this section of the paper is EGT. In Figure 6, a sender ($S$) forwards a packet to one of the subregions based on the EGT. $R_1$, $R_2$, . . . ., $R_K$ are subregions in the figure and $R_2$ is the subregion selected using EGT. Within that region, a forwarding node is selected using CGT.

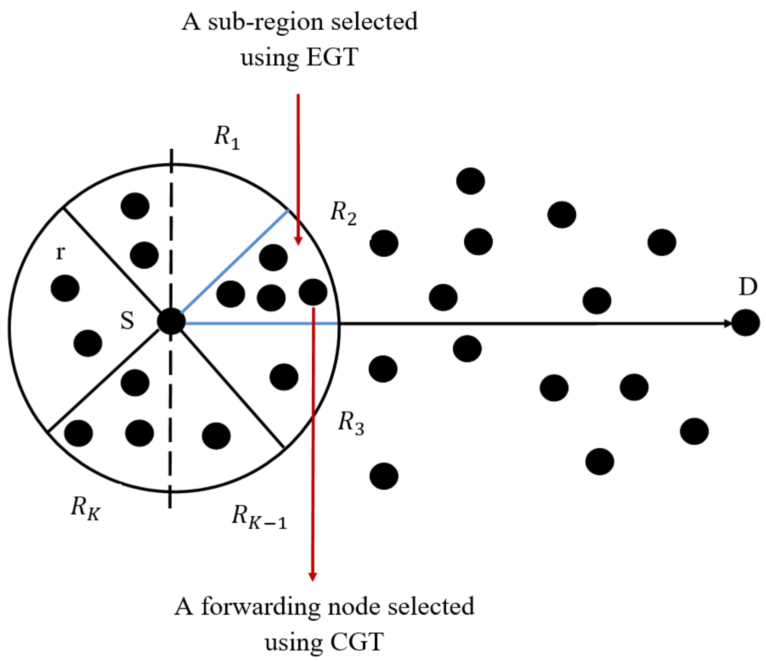


**Figure 6.** Subregion and node selection.

The ratio of the number of delivered packets and the total number of generated packets is defined as packet delivery ratio in GTEB. If any sensor node fails to function properly, owing to energy depletion, the time taken until that event occurs is considered to be the network lifetime. The energy consumption per packet is defined as the average energy required for a packet to be successfully transmitted. GTEB was compared with real-time load distribution [69] and reserve path adaptive routing [70]. Compared to these protocols, the GTEB increased the network lifetime by approximately 33–129%. The rate of packet arrival was 1–14 packets per second in the simulation scenario in [40]. The intelligent spreading of traffic over wide regions through energy balanced forwarding process helped to increase the network lifetime in this protocol. The GTEB also reduced redundant transmission of the data packet through the game-theoretic approach, which eventually led to the reduction of energy consumption by up to 40 percent when compared to the other examined protocols. The packet delivery ratio was also higher in GTEB than the state-of-the-art protocols.

Technical strengths:

- Creates an energy balance and increases network lifetime significantly;
- Intelligent method to evenly distribute network traffic in a WSN.

Technical weaknesses:

- Sensor nodes are capable of reporting a nearby event to the destination on a periodic manner. If the destination is far away, this may lead to energy wastage;
- The protocol is more energy efficient when there are more nodes in a subregion. If there is only one node in a subregion, the data packet is to be transmitted directly to the destination. This is a serious flaw in the protocol, as this may lead to energy wastage;
- The network lifetime was the most prioritized routing metric for GTEB. Unfortunately, the authors did not compare GTEB with a sufficient number of protocols for this metric. It was compared only to the probabilistic forwarding method and that does not prove the superiority of GTEB over the state-of-the-art protocols.

Applications:

- Applicable for energy-efficient geographical routing.

Possible future improvement:

- Mathematical ambiguity can be removed from the protocol. In one case, K was denoted as a set of subregions in the network, but later K was introduced as a set of strategies, which was ambiguous.

#### 3.3.2. Energy-Efficient Routing Protocol Based on Evolutionary Game (EEREG)

A WSN consists of more than hundreds, or sometimes even more than thousands, of battery-powered nodes. Increasing the network lifetime of a WSN is of utmost priority and careful attention should be paid to the energy efficiency of the network. It is inevitable in a typical WSN that certain nodes will run out of their energy earlier than the other nodes. In particular, nodes close to the sink nodes die earlier. This problem is known as the hotspot problem. It considerably affects the performance of the network. The performance deteriorates when nodes with low energy tend to become CHs in a clustering-based network. To deal with these problems, Lin et al. designed a mathematical model, aiming to counter the hotspot problem by optimizing the cluster size, using an optimal cluster size (OCS) algorithm. Subsequently, an energy-efficient routing protocol based on evolutionary game (EEREG) theory was presented for terminating anarchism during CH selection [41].

In this routing protocol, a network sector is assumed to be divided into $k$ annular sections. The sector encompasses an angle $\theta$ at the center. The sink node is assumed to be at the center of the sector. Each ring has a width of $d$ and the area of the sector is $A$. Every node in the network is deployed randomly. The OCS algorithm presented in [41] was quite simple. The sensor nodes in the network periodically send "hello" packets to the sink nodes to inform them of their location and energy level. After receiving the "hello" packet, the sink node divides the area into $k$ parts. Next, it calculates the cluster size. Finally, it broadcasts messages to all the sensor nodes to let them know the optimal cluster size. Furthermore, the number of clusters, along with the percentage of the CHs, could be obtained. The sensor nodes in a WSN expend energy while sensing, receiving, and transmitting data. The scheme designed in [41] considered energy expenditure for data transmission only. The energy required to transmit one bit of data from one node to another with a distance $d$ is $e_{tx}$, which is represented as:

$$e_{tx} = E_{elec} + \varepsilon_{amp}.d^{\alpha}, \tag{30}$$

where $E_{elec}$ and $\varepsilon_{amp}$ represent the energy consumption of the transmitter circuit and the transmitter amplifier, respectively, and $\alpha$ is the propagation loss exponent value, which lies between 2 to 4.

In a network area with $N$ nodes, the CH election game based on evolutionary game theory is formulated as $G$ $(P, S, U)$. Here, $P$ is the set of nodes, $S$ is the strategy set, and $U$ is the utility. $P$ has two subsets: $H$ and $L$. $H$ denotes a set with higher energy level and $L$ denotes a set with a lower energy level. Usually, the nodes in set $H$ are supposed to be CHs and broadcast an advertisement packet ($ADV$) to other CMs within the transmission range. Typically, the nodes with low energy would also try to send $ADV$ messages. This is where EGT played an important role in [41], where evolutionary stable strategies hindered such a phenomenon by not allowing nodes with lower energy level to become CHs. To encourage nodes in set $H$ to become CHs and discourage nodes in set $L$ from being CHs, a utility function for any node $i$ was formed as:

$$u_i = r_i - p_i, \tag{31}$$

where $r_i$ and $p_i$ denote the profit and penalty of node $i$, respectively.

The routing protocol mainly consists of three components: the optimal cluster size finding, cluster formation, and transmission of data. The first component (optimal cluster size determination) is achieved via the previously explained OCS algorithm. The last component (transmission of data) is the same as the existing clustering algorithms. The main contribution of the paper was in the energy-efficient and controlled cluster selection using game theory. When the energy level is congruent for all the nodes in the cluster, any node could be the CH. When there is an energy imbalance among the nodes, only the nodes in set $H$ tend to become CHs. Furthermore, the higher the range of energy for the nodes, the higher the probability of them becoming CHs. When the sensor nodes send "hello" messages to the sink node, they generate certain parameters: $P_H$ = the proportion of the nodes in set $H$, $P_L$ = the proportion of the nodes in set $L$, $e$ = the energy consumed when acting as CH, $\Delta$ = the energy difference between the nodes in sets $H$ and $L$, and $\overline{E_{re}}$ = the average residual energy of the nodes. These parameters are adjusted, taking into consideration the changes in WSNs after a certain cycle $T$. The sink node broadcasts the value of $\overline{E_{re}}$ to the sensor nodes. After receiving the broadcast message, a random number is generated by a sensor node that has a range between *0* to *1*. The residual energy is compared with the $\overline{E_{re}}$ parameter and the class to which a node belongs to (either $H$ set or $L$ set) is decided based on this comparison. The nodes falling in set $H$, which is the set of nodes with higher energy level, are compared with another threshold value, that eventually decides which node would be the CH.

EEREG was compared with low energy adaptive clustering hierarchy (LEACH), distributed hierarchical agglomerative clustering [71,72], threshold-sensitive energy-efficient routing in sensor networks [73], and power-efficient gathering in sensor information systems [73] in terms of the different network lifetime metrics, which were the time until the first node dies, time until half of the nodes die, and time until the last node dies.

Technical strengths:

- Cluster size is maintained optimally;
- Avoidance of the low energy nodes becoming a CH;
- Introducing rationality among the nodes so that the nodes with high energy level are encouraged to become CHs.

Technical weaknesses:

- Network lifetime is considered as the time taken for the first node to dies in the network. This is impractical because WSNs may still remain fully functional even after the death of the first node.

Applications:

- Animal and plant habitat monitoring.

Probable future improvements:

- The complexity of the protocol is high. In particular, complex computation involving optimal cluster size determination could have been simplified.

#### 3.3.3. Game Theory-Based Energy-Efficient Clustering (GEEC)

WSNs are energy limited networks and significant attention has been focused on increasing the life span of WSNs. Increasing the network lifetime of a WSN can be achieved by designing efficient routing protocols. Lin et al. designed a game theory-based energy efficient clustering routing protocol

(GEEC) that used an EGT mechanism to achieve simultaneous energy exhaust equilibrium and lifetime expansion [42].

Sensor nodes deplete their energy through operations like sensing, receiving, and transmitting. Only the energy consumption for data transmission was considered in this protocol [42]. It can be formulated using (28), similar to the previous EGT-based routing protocol. All the nodes in the network are capable of varying their transmission power for different communication ranges using a power control mechanism. The sensor nodes are location aware and have fixed positions. The authors of [42] also assumed that the sink node had an infinite amount of processing power and energy. They were randomly deployed in the network area.

Based on the basic principles of EGT, the CH selection game in [42] had three components. The structure of the game model could be presented as *G (P, S, U)*. Here, P was the set of players (nodes), *S* was the set of strategies, and *U* was the utility function. The players were divided into two classes. Class *M* contained the players with more energy than the others and class *L* had the nodes with lesser amount of energy. The players in set *P* could opt for two strategies: to either become a CH or to remain in the cluster as a CM. Therefore, it can be said that *P = (M, L)* and *S = (being CH, being CM).* The utility function consisted of a reward and penalty. It was formulated as:

$$u = r - p, \tag{32}$$

where $r$ is the reward and $p$ is the penalty.

Usually, the nodes with higher energy level send out the information of CH status to other nodes within the transmission range. After receiving the CH announcement, other nodes decide if they will join the cluster or not. It is possible for the nodes with low energy to send CH advertisements repeatedly to other nodes in the transmission range, owing to their limited rationality. Owing to this phenomenon, several control messages are sent, causing energy wastage. The novelty of GEEC lies in the avoidance of this energy wastage by introducing rationality to the nodes through EGT. The utility function is designed in a way that it encourages the nodes in class *M* to become CHs.

We discussed replicator dynamics (change rate of the players' action) in previously discussed protocols. The authors of [42] formulated equations for replicator dynamics. It was assumed that the rate of class *M* nodes in selecting the strategy of becoming CH was $x$ and *M* nodes opting for the strategy of remaining as CMs was *(1-x)*. Similarly, the rate of class *L* nodes selecting the strategy of becoming CH was assumed to be $y$ and *L* nodes opting for strategy to remain as CMs was *(1-y)*. The utility functions of the nodes in class *M* choosing the strategy of becoming CHs ($U_{M-CH}$) and choosing the strategy of remaining as CMs ($U_{M-CM}$) were formulated subsequently by the following two expressions:

$$U_{M-CH} = ya + (1-y)(a + 2\Delta), \tag{33}$$

$$U_{M-CM} = y(a - \Delta) + (1-y)(-\Delta), \tag{34}$$

where $a$ is the reward for the *M* nodes in becoming a CH, $\Delta$ is the step to punish or encourage. The average revenue of nodes in class *M* thus was formulated as:

$$\overline{U_M} = x(a + 2\Delta - 2y\Delta) + (1-x)(ya - \Delta). \tag{35}$$

After stringent mathematical analysis, the replicator dynamic equation of class *M* nodes was formulated as:

$$\frac{dx}{dt} = F(x) = x\left(U_{M-CH} - \overline{U_M}\right). \tag{36}$$

Like the nodes in class *M*, the expected utility functions of class *L* nodes for two different strategies were determined by the following two expressions:

$$U_{L-CH} = xb + (1-x)(b + \Delta), \tag{37}$$

$$U_{L-CM} = x(b + 2\Delta) + (1 - x)(-\Delta), \quad (38)$$

where $b$ is the cost for $L$ nodes becoming the CH. The average revenue for nodes falling under class $L$ was:

$$\overline{U_L} = y(b + \Delta - x\Delta) + (1 - y)(bx + 3x\Delta - \Delta). \quad (39)$$

The replicator dynamic equation for nodes in class $L$ was formulated as:

$$\frac{dy}{dt} = G(y) = y\left(U_{L-CH} - \overline{U_L}\right). \quad (40)$$

The routing protocol was designed to have three phases: the initial, cluster formation, and data transmission phases. In the initial phase, all the nodes in a WSN transmit an initial message to the sink node, containing the information of node identity (ID) and residual energy $E_{res}$. After this initial transmission of messages by the sensor nodes, the sink node sorts them based on the $E_{res}$ value. It also generates an energy threshold value, $E_{th}$. The sensor nodes, after determining the $E_{th}$ value, classify themselves as either class $M$ (class of nodes with more energy than the threshold) or class $L$ nodes (class of nodes with less energy than the threshold). In the cluster formation phase, the nodes decide to become either the CH or the CM, based on the pay-off functions. When a node decides to become the CH, it sends out *ADV* messages that contain its ID and $E_{res}$. The nodes that do not become CHs reply to the CHs by transmitting a join request. There can be a rare case when a node may not receive an *ADV* message. In that case, it would directly transmit data to the sink node. In the data transmission phase, all the CHs divide the time slots and announce them to the CMs. The CMs send the data to the CHs using TDMA and the cluster structure is maintained for a certain time. The CHs finally transmit the data to the sink.

GEEC outsmarts LEACH and LEACH-Centralized (LEACH-C) in terms of network lifetime. Four parameters were introduced to compare the network lifetime with the LEACH protocol. They were: (1) the time taken for the first node to exhaust its energy, (2) the time taken for the first node to die, (3) the time taken for all the nodes to run out of energy, and (4) the number of nodes alive during simulation. These parameters were considered in the simulation study in [42]. In all cases, GEEC was identified to perform better.

Technical strengths:

- Introduces rationality to the low energy nodes;
- Pay-offs were considered differently for nodes with higher and lower energy levels.

Technical weaknesses:

- Some nodes may not receive advertisement from the CHs resulting in clusters with one node that directly transmits to the sink node.

Applications:

- Any kind of energy-efficient target tracking and environment monitoring.

Possible future improvements:

- Energy threshold determination procedure can be elaborated for the betterment of the protocol.

#### 3.3.4. Evolutionary Routing Game for Energy Balance in WSN (ERG)

Finding out a desirable route in a WSN is always challenging. Some disparate routes may frequently suffer from congestion and exhaust fast. Since all the nodes in the network will act upon saving energy, choosing one good route suddenly by many nodes may result in faster energy depletion in such routes. As a result, network lifetime may be shortened. Attiah et al. analyzed this issue in [45] and proposed an evolutionary routing game (ERG) for balancing energy in WSNs. They modeled the routing problem as an evolutionary anti-coordination routing game.

The authors of [45] derived an evolutionary stable strategy for the proposed ERG. Also, the replicator dynamics of the formulated evolutionary game were derived. The proposed anti-coordination routing game had a set of $N$ homogeneous sensors (players). They were randomly distributed in a certain area. Each player must choose a path for data packets. The set of next hops were presented as $R$. The path of each packet was controlled independently by rational players so that the cost of transmission and latency was minimized. Each hop in the route had a specific cost $C_r$, that was related to the distance between transmitter and receiver. Sensor nodes in the network were rational and non-cooperative. In the proposed model [45], the cost (C) of forwarding a packet consisted of two parts: the energy needed to transmit a data packet and the other is the energy required for receiving the packet. Therefore, the total cost is calculated as:

$$C = C_{tx}(d) + C_{rx}, \tag{41}$$

where $C_{tx}(d)$ is the cost of transmitting the packet over a distance $d$, and $C_{rx}$ is the cost of receiving the packet. The evolutionary routing game in [45] is presented as:

$$G = \langle R, S, U \rangle, \tag{42}$$

where $R$ is the set of next available hops, $S = \{S_r | r \in R\}$ is the strategy space denoting the set of actions that the players can alternatively choose. $U$ is the pay-off function. The pay-off function is defined as follows:

$$U(s_r, s_t) = \begin{cases} \left(\frac{1}{C_{vr}}, \frac{1}{C_{vt}}\right) when\ r \neq t,\ v \in \{A, B\} \\ (0, 0)\ when\ r = t \end{cases} \quad G = \langle R, S, U \rangle, \tag{43}$$

where $C_{vr}$ is the transmission cost of the packet through hop $r$, that belongs to population either $A$ or $B$. $t$ is another alternative hop other than $r$. Therefore, $C_{vt}$ is the transmission cost of the packet through hop $t$. The authors provided a reasonable amount of simulation results that proved the feasibility of implying evolutionary game theory [45]. Unfortunately, the proposed scheme was not compared with any other state-of-the-art protocols.

Technical strengths:

- Pure strategy Nash equilibrium and replicator dynamics of the evolutionary game were explained and formulated comprehensively. Players can not only learn strategies but also can modify it.

Technical weaknesses:

- One-hop transmission among nodes are discouraged by imposing lower pay-off. Multi-hop transmissions can be energy consuming.

Applications:

- Any kind of energy–efficient multi-hop data transmission for WSNs.

Possible future improvements:

- Some experimental results involving network lifetime could be added.

### *3.4. Routing Protocol Based on Reputation-Based Game*

#### 3.4.1. Game Theory-Based Routing Algorithm (GBRA) Based on Reputation

Typical WSNs consist of resource-limited (processing power, energy, memory, bandwidth, etc.) sensor nodes. Energy is wasted more when the malicious nodes deliberately drop the data packets forwarded to them. This kind of phenomenon is known as selective forwarding attack. This type of security problem results in more challenges while designing an energy-efficient routing protocol for WSNs. Keeping this in mind, Li et al. designed a game theory-based routing approach (GBRA) [43] using a reputation-based game in which sensor nodes were modeled as rational and intelligent agents that could cooperate with each other for increasing their pay-offs in a sensor game.

In this routing protocol, each hop is a game between a sender and the next hop relay node. Both nodes would attempt to increase their own pay-offs owing to the selfish nature of the designed game. The pay-off function of the sensor node was designed on the basis of the competing node's reputation, remaining energy, and distance between the competing node and the destination. The pay-off function of the relay node was designed based on the proportion of the sender's reputation. The sender selects the relay nodes that could maximize its pay-off. Conversely, relay nodes are supposed to help only those sensor nodes that have a higher reputation. Using a watchdog mechanism, every single node monitors the behavior of the neighbors and evaluates their reputation.

The detailed steps of the designed routing protocol are given below:

1. When there is a packet to send and the destination was within the communication range, the sender sends a *ROUTE REQUEST* message to its neighbors;
2. After certain nodes have received the *ROUTE REQUEST* message, there could be two scenarios. In the first scenario, a node receiving the *ROUTE REQUEST* message is itself the destination or knows the destination. In this case, step 5 is followed. In the second scenario, each node getting the *ROUTE REQUEST* message checks its remaining energy $E_{rem}$. If $E_{rem}$ was less than $E_c$, the energy cost of the data transmission, the node would not transmit the data packet to save its energy. The node calculates its pay-off only when $E_{rem} \geq E_c$. If the value obtained through this calculation is greater than zero, the node sends an acknowledgement (ACK) to the sending node and acts as a relay node.
3. After receiving back the ACKs from the receiving nodes, the sender node selects one among them (receiving nodes) that could maximize the sender's pay-off to the greatest extent. Next, the sender sends a *REPLY* message to the chosen relay node.
4. When the *REPLY* messages reach the relay node, a new game starts between the relay node and its next hop. The new sender attaches its ID in the source route and again forwards the *ROUTE REQUEST* message to its neighbors. Step 2 is repeated until a route is found.
5. If the receiving node is the destination node or at least has a route to the destination, the node does not forward the packet. Rather, it replies to the sending node with the full route in a reverse order.
6. Finally, when the message reaches the destination, the deduced routing path is selected.

In GBRA, the reputation of a node is determined based on the cooperativeness of a node. The value of reputation ($R_{ij}$) is fixed between 0 and 1. If node $i$ is observing node $j$, the decrease of node $j$'s reputation if it deliberately drops data packets is formulated as:

$$R_{ij} = \frac{R_{ij}}{2}. \quad (44)$$

If node $j$ participates in packet forwarding actively rather than dropping packet deliberately, its reputation would increase using the following equation:

$$R_{ij} = R_{ij} + 0.1. \quad (45)$$

Because node $i$ is the receiver node and node $j$ is the sender node, the pay-off function for node $i$ is expressed as:

$$U_i = \xi R_{ij} - \eta E_c \ (\xi,\ \eta \in [0,\ 1],\ \xi + \eta = 1). \quad (46)$$

The pay-off function for node $j$ was expressed as:

$$U_i = \xi R_{ij} - \eta E_{dest} * E_{tot} / E_{rem}. \ (\xi,\ \eta \in [0,\ 1],\ \xi + \eta = 1). \quad (47)$$

As mentioned earlier, there can be a scenario where the neighboring nodes know the route to the destination, or one among them is itself the destination. Figure 7 presents such a scenario in the network. In Figure 7, node *E* and *F* are the neighboring nodes of the source node *C*. *I* is the destination node. *C*, after sending a route request (RREQ) message to *E* and *F*, receives back a reply about the optimal route from node *F*, as it already knows the route.

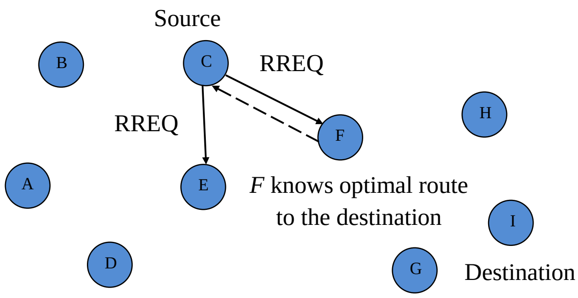


**Figure 7.** Network scenario where the neighboring node knows the optimal route to the destination.

There can also be a scenario where the neighboring node does not know the optimal route to the destination. Figure 8 illustrates this scenario. After receiving RREQ from the source node *A*, node *B* and node *C* calculate if $E_{rem}$ is greater than $E_c$. Furthermore, they compare if the pay-off (calculated using (41)) is greater than zero. If both conditions are satisfied, the neighboring nodes will send ACK messages to the source node. Node *A* (source node) calculates its own pay-off using (42) to find out the optimal relay node, as illustrated in Figure 8b. If source node *A* determines that node *B* is an optimal relay node after pay-off calculation, a new game will start between nodes *B* and *C*. This process continues till it reaches destination node *I*. Once the destination is reached, the destination node sends back the route to the source for data transmission. Nodes append their IDs when they switch one node for another for a new game.

The simulation results demonstrate that the designed protocol performed better than LEACH in terms of prolonging network life time. The reason for this is that the LEACH protocol selects a CH among all the nodes with equal probability and the residual energy of the nodes is not considered during this selection. Furthermore, the distance to the destination during this selection is not considered. This causes early deaths of some nodes, owing to energy wastage for distant transmissions. In the second scenario of the simulation, 20% of malicious nodes were kept in the network. The scheme designed in [43] demonstrated a higher throughput than LEACH. The reason for this is that the malicious nodes were kept aloof from other nodes in the network by reputation mechanism.

Technical strengths:

- Good mechanism to stop packet drops;
- Mechanism to avoid malicious nodes from routing path.

Technical weaknesses:

- No technical integration process was mentioned for the watchdog mechanism that was used to monitor the neighboring nodes;
- No mathematical formulation or definition regarding who can be the neighbors of a sending node was presented.

Applications:

- Applicable for any data sensitive application that requires continuous information sending.

Possible future improvements:

- Network architecture is not well defined. To make the protocol GBRA deployable, it is necessary that the authors clarify the network architecture.

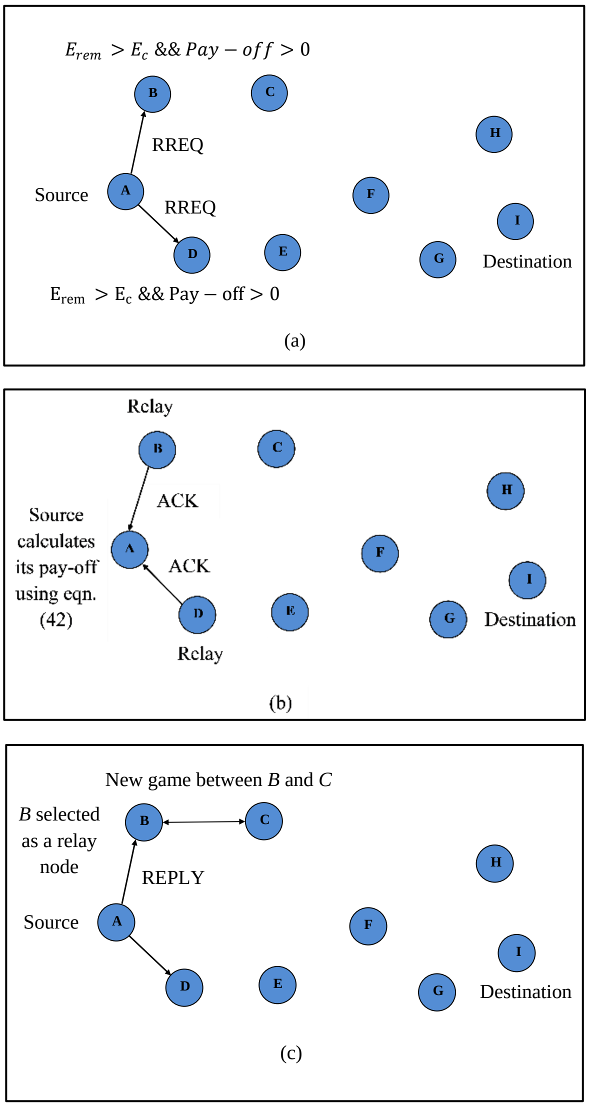


**Figure 8.** Network scenarios where the neighboring node does not know the optimal route to the destination: (**a**) the source nodes send route request message to neighbor nodes and the neighboring nodes decide if they can be a relay, (**b**) the source node receives acknowledgements (ACKs) from the relays and calculates its own pay-off, and (**c**) the source node chooses its new relay game between *B* and *C*.

### 3.4.2. Comparison of the Protocols Based on the Technical Strengths and Weaknesses

The technical strengths and weaknesses of the protocols discussed in Sections 3.2 and 3.4 are comparatively summarized in Table 6 for readers.

**Table 6.** Comparison of routing protocols based on evolutionary and reputation-based games in terms of technical strengths and weaknesses.

| Protocol | Technical strength | Technical weakness |
|---|---|---|
| GTEB [1] [40] | • Creates an energy balance and increases network lifetime significantly;<br>• Intelligent method to evenly distribute network traffic in a WSN. | • If the destination node is far away, this may lead to energy wastage;<br>• The protocol is more energy efficient when there are more nodes in a subregion. If there is only one node in a subregion, the data packet is to be transmitted directly to the destination. This is a serious flaw in the protocol, as this may lead to energy wastage. |
| EEREG [2] [41] | • Cluster size is maintained optimally;<br>• Avoidance of the low energy nodes becoming a CH. | • Network lifetime is considered as the time taken for the first node to dies in the network. This is impractical because WSNs may still remain fully functional even after the death of the first node. |
| GEEC [3] [42] | • Introduces rationality to the low energy nodes;<br>• Pay-offs were considered differently for nodes with higher and lower energy levels. | • Energy threshold determination procedure can be elaborated for the betterment of the protocol. |
| ERG [4] [45] | • Players can not only learn strategies, but can also modify them. | • One hop transmissions among the nodes are discouraged by imposing lower pay-off. Multi-hop transmissions can be energy consuming. |
| GBRA [5] [43] | • Good mechanism to stop packet drops;<br>• Mechanism to avoid malicious nodes from routing path. | • No mathematical formulation or definition regarding who can be the neighbors of a sending node was presented. |

[1] Game Theoretic Energy Balanced Routing; [2] Energy-Efficient Routing Protocol based on Evolutionary Game; [3] Game-Theory-Based Energy-Efficient Clustering; [4] Evolutionary Routing Game; [5] Game-Theory-Based Routing Algorithm.

## 4. Comparison of the Routing Protocols

In this section, we qualitatively compare the routing protocols of the WSNs that were discussed earlier, in Section 3. The prime target for most of the protocols is to provide an energy-efficient routing path, because energy is the most important resource in WSNs. The major features, advantages, and limitations of different game theory-based routing protocols were compared. We also extensively compared the protocols based on their different properties and characteristics (topology, data transmission type, scalability, fault tolerance, etc.).

Table 7 summarizes the qualitative comparison of the routing protocols based on a cooperative game. Routing protocols developed using a cooperative game theory can balance energy usage and have a higher packet delivery ratio. These types of protocols can be chosen for overall energy efficiency in WSN applications. CH-C-TEEM [31] is suitable for a WSN that is operating in a fading channel and it supports MIMO communication. It is highly energy efficient too. The RCFR [35] mechanism can co-exist with AODV [55], which is a standard protocol. RCFR can also be integrated with other existing standard protocols for better energy efficiency. Network engineers can choose RCFR if they intend to make WSN applications deployed with the standard protocol with energy efficiency. The assignment game approach presented in [34] can provide energy efficient routing with numerous devices being involved. It can also support heterogeneous network architecture. PRGT [44] has been developed to support opportunistic networks, and ensures cooperation among nodes for improving routing efficiency in terms of packet delivery ratio and latency, but the protocol requires a centralized scheme which makes it not deployable for emergency situations like post disaster services.

**Table 7.** Comparison of routing protocols based on cooperative games.

| Protocol | Routing Metric | Major Features | Advantages | Limitations |
|---|---|---|---|---|
| CH-C-TEEM [1] [31] | Energy, network lifetime | • Mitigation of fading effects through energy efficient multi-input, multi-output communication;<br>• Cooperative CHs;<br>• Selection of CHs and cooperative nodes using game theory. | • Highly energy-efficient;<br>• Performs better than TEEM and saves 50% of the residual energy. | • No other routing metrics considered other than energy;<br>• Considers cooperative transmission only. This protocol does not consider cooperative sending and receiving groups in cluster. |
| RCFR [2] [35] | Energy, packet delivery ratio | • Characteristic function to be shared among coalitional members;<br>• Stable cooperation among nodes for simultaneous packet delivery and minimum route cost. | • Coalition formation algorithm can be integrated with other routing protocols. Example: AODV. | • Excludes selfish nodes from routing paths that do not form a coalition. |
| Assignment game approach [34] | Energy | • Heterogeneous network architecture;<br>• Credit-based system to reward cooperative players;<br>• Exclusion of selfish nodes from cooperative coalitions. | • Introduces energy reduction mechanism in heterogeneous WSNs through cooperative relaying;<br>• Increases network lifetime up to 22% with extensive increase in battery life. | • Excessive coalition formation creates data sharing overhead among nodes. |
| PRGT [3] [44] | Packet delivery ratio, average latency, overhead ratio | • Implementation of the first-order Markov process based on the meeting history of nodes;<br>• Participation of relay nodes is ensured to introduce cooperation in the network;<br>• Reward-based system to reward cooperative players. | • Performance comparison with the state-of-the-art protocols;<br>• Significant improvement in packet delivery ratio and latency for opportunistic networks. | • Not enough mathematical formulation for game theory is presented. To implement the protocol in real life, more precise description is necessary. |

[1] Cluster Head Cooperative Trustworthy Energy-Efficient multiinput multioutput; [2] Reliable Coalition Formation Routing; [3] Probabilistic Routing Based on Game Theory.

Table 8 lists the qualitative comparison of the routing protocols based on a noncooperative game. Except for COMO [38], noncooperative games have been applied extensively to design routing protocols that are highly energy efficient. The resource allocation strategy for clustering-based WSNs [36] is extremely robust to node failures. Failure of a portion of nodes in a cluster does not affect the routing process. The inter-cluster routing algorithm for WSNs [39] is really a crucial protocol because it is interoperable between WSNs and mobile networks. A routing framework based on energy and delay conservation in [37] was designed and implemented in a scenario where all the nodes were static. COMO [38] is the only routing protocol that has considered end-to-end throughput instead of energy as a routing metric among the routing protocols that exploit noncooperative games. Conversely, GERA [33] was designed to enhance the LEACH protocol by limiting the cluster size.

Table 9 summarizes the qualitative comparison of the routing protocols based on the evolutionary and reputation-based games. The focus of the routing protocols designed using evolutionary games was to increase network lifetime. GTEB [40] was designed to outsmart the existing protocols by increasing the average packet delivery ratio. It can robustly avoid redundant transmissions. The routing process in [40] was complex because it used both CGT and EGT. The EEREG's advantage lies in handling hotspot problem in WSNs, and it can support both centralized and distributed deployments of WSNs [41]. The GEEC [42] can be applied only if the nodes are location-aware in the network. The ERG [45] can be applied in a distributed manner that ensures evolutionary stable strategy through pure strategy Nash equilibrium. According to the best of our knowledge, GBRA [43] is the only one protocol in this type of game. It considers network lifetime and average throughput as routing metrics and supports only one hop routing path way.

Table 10 lists the comparisons of the game theory-based routing protocols based on their important characters and properties. We compared the protocols in terms of topology, type of data transmission, scalability, fault tolerance, communication reliability, protocol complexity, and location awareness.

**Table 8.** Comparison of routing protocols based on noncooperative games.

| Protocol | Routing Metric | Major Features | Advantages | Limitations |
|---|---|---|---|---|
| Resource allocation strategy for clustering-based WSNs [36] | No routing metric | • Use of Nash bargaining solution to analyze clustering;<br>• Uniform routing scheme for energy consumption on CHs, cluster members, and sink node. | • Failure of the first node does not affect other cluster members. | • Not feasible for multihop WSNs;<br>• Cannot function as a distributed scheme;<br>• No comparative study shown with other existing protocols. |
| Intercluster routing algorithm for WSNs [39] | Energy | • Hexagonal cluster topology like cellular network.<br>• Multihop routing.<br>• Interoperability between WSNs and mobile networks. | • The game model shows a unique Nash equilibrium solution and reduces energy as well as prolongs lifetime. | • Only one routing metric considered.<br>• No comparative study shown with other existing protocols. |
| Routing framework based on energy and delay conservation [37] | Energy | • Sensor nodes are fully static;<br>• Game modeled as dynamic, noncooperative, and incomplete information;<br>• Cost function comprises of SINR. | • Considers SINR to determine most optimal paths;<br>• Nash equilibrium is self-imposed when the nodes use their best response strategy. | • Infinite amount of interference;<br>• Congestion highly affects the choice to select a mode as the next hop. |
| COMO [1] [38] | End-to-end throughput | • Guarantee of achieving strong Pareto-efficient Nash equilibrium with faithfulness as a given property;<br>• Takes link loss probability as input and outputs the number of times of forwarding and dissemination bit rate;<br>• Random selection of source-destination pairs. | • When all the nodes follow the routing and incentive protocol, system optimization occurs. | • Congestion among multiple nodes not addressed. |
| Energy-aware trust deviation scheme [32] | Energy, average packet delivery ratio, packet loss ratio | • Proposal of a risk strategy model to simulate cooperation among nodes;<br>• Use of mixed strategy Nash equilibrium to obtain the optimal ratio of gain to cost and the probability of selected strategy.<br>• Multi-sink and multihop network. | • Handles bad mouthing and distributed denial of service (DDoS) attacks very well;<br>• Manages routing overhead while maintaining adequate security of WSNs. | • Overhead of the trust requests not considered;<br>• No comparative study shown with other protocols. |
| GERA [2] [33] | Energy, packet delivery ratio | • Setting of the utility function based on the benefit and energy consumption;<br>• Iterative selection of CHs;<br>• Coverage of both intercluster and intracluster routing. | • The protocol is compared with an already established protocol, LEACH;<br>• Introduces a balancing factor to limit the cluster size. | • Node mobility not considered;<br>• Uniform transmission radius for all nodes. |

[1] Cooperation Optimal Protocol for Multirate Opportunistic Routing; [2] Game-Theory-Based Energy-Efficient Routing Algorithm.

**Table 9.** Comparison of routing protocols based on evolutionary and reputation-based games.

| Protocol | Routing Metric | Major Features | Advantages | Limitations |
|---|---|---|---|---|
| GTEB [1] [40] | Average packet delivery ratio, network lifetime | • Forwarding nodes run out of energy exactly simultaneously;<br>• Forwarding regions are set based on the network density;<br>• Combination of classical game theory and evolutionary game theory for routing protocol design. | • Combination of two types of games leads to achieving network-wide balance;<br>• Avoidance of redundant transmissions among a finite number of nodes within a contention domain. | • Increased complexity of routing method as two types of games are implied. |
| EEREG [2] [41] | Energy, network lifetime | • Optimizes cluster size using optimal cluster size algorithm;<br>• Terminates anarchism during the process of CH selection;<br>• Proposes mathematical model to ease the energy burden of the nodes near the sink node. | • Handles hotspot problem in WSNs;<br>• Routing scheme is both centralized and distributed. | • Complex routing process owing to the combination of OCS algorithm and evolutionary game model. |
| GEEC [3] [42] | Energy, network lifetime | • Adoption of evolutionary game theory to achieve exhausted equilibrium;<br>• Stationary deployment of location aware nodes;<br>• Random and distributed deployment of nodes. | • Reduced energy dissipation;<br>• Location awareness. | • The sink node has an unlimited source of energy and processing power that are not realistic in design. |
| ERG [4] [45] | No routing metric | • Evolutionary game-based routing ensuring evolutionary stable strategy that cannot be invaded by any other greedy strategy;<br>• The fairness of the proposed equilibrium solution under selfish node behavior is analyzed. | • Can be deployed in a distributed manner;<br>• Successful in covering the strategy choices to evolutionary stable strategy under dynamic conditions. | • No comparative analysis with the other protocols in terms of the crucial performance metrics. |
| GBRA [5] [43] | Average throughput, network lifetime | • Node's reputation depends on its behavior;<br>• Routing path from sender to destination is designed as a hop-by-hop game;<br>• The pay-off function of a sender node is related to its opponent's reputation, remaining energy, and the distance between its opponent and the destination. | • Malicious nodes are punished and isolated. | • Supports one hop-routing path only. |

[1] Game Theoretic Energy Balanced Routing; [2] Energy-Efficient Routing Protocol based on Evolutionary Game; [3] Game-Theory-Based Energy-Efficient Clustering; [4] Evolutionary Routing Game; [5] Game-Theory-Based Routing Algorithm.

**Table 10.** Comparison of routing protocols with regard to network architecture.

| Protocol | Type of Game | Topology | Data Transmission | Scalability | Fault Tolerance | Communication Reliability | Protocol Complexity | Location Awareness |
|---|---|---|---|---|---|---|---|---|
| CH-C-TEEM [1] [31] | Cooperative | Hierarchical | Multihop | No | No | No | Low | No |
| RCFR [2] [35] | Cooperative | Flat | Multihop | No | Yes | Yes | Moderate | No |
| Assignment game approach [34] | Cooperative | Flat | | Yes | No | Yes | High | Yes |
| PRGT [3] [44] | Cooperative | Flat | Multihop | No | Yes | Yes | High | No |
| Resource allocation strategy for clustering-based WSNs [36] | Noncooperative | Hierarchical | Multihop | No | Yes | Yes | Moderate | No |
| Intercluster routing algorithm for WSNs [39] | Noncooperative | Hierarchical | Single hop | No | No | No | Low | No |
| Routing framework based on energy and delay conservation [37] | Noncooperative | Flat | Multihop | No | No | No | Moderate | Yes |
| COMO [4] [38] | Noncooperative | Grid | Multihop | No | No | Yes | High | Yes |
| Energy-aware trust deviation scheme [32] | Noncooperative | Flat | Multihop | Yes | Yes | Yes | High | No |
| GERA [5] [33] | Noncooperative | Hierarchical | Multihop | No | No | No | Moderate | Yes |
| GTEB [6] [40] | Evolutionary | Hierarchical | Multihop | No | No | No | High | Yes |
| EEREG [7] [41] | Evolutionary | Hierarchical | Multihop | Yes | Yes | Yes | High | Yes |
| GEEC [8] [42] | Evolutionary | Hierarchical | Multihop | Yes | Yes | Yes | High | Yes |
| ERG [9] [45] | Evolutionary | Flat | Multihop | No | No | Yes | High | Yes |
| GBRA [10] [43] | Reputation | Flat | Multihop | No | Yes | Yes | Moderate | No |

[1] Cluster Head Cooperative Trustworthy Energy-Efficient multiinput multioutput; [2] Reliable Coalition Formation Routing; [3] Probabilistic Routing Based on Game Theory; [4] Cooperation Optimal Protocol for Multirate Opportunistic Routing; [5] Game-Theory-Based Energy-Efficient Routing Algorithm; [6] Game Theoretic Energy Balanced Routing; [7] Energy-Efficient Routing Protocol based on Evolutionary Game; [8] Game-Theory-Based Energy-Efficient Clustering; [9] Evolutionary Routing Game; [10] Game-Theory-Based Routing Algorithm.

## 5. Future Directions and Challenges

In this section, we discuss future research directions for using game theory to design routing protocols for WSNs. Then, certain challenges while using game theory to develop such routing protocols are briefly discussed.

### *5.1. Future Research Directions*

Although a decade of research has passed in the field of WSNs, there are concerns still to be addressed for future research. The following research directions can be followed to design new routing protocols based on game theory.

For a robust and efficient routing, multiple routing metrics should be considered. For example, a routing protocol can be energy efficient but may lead to a lower packet delivery ratio, or a protocol can increase network lifetime but may result in greater end-to-end delay. Therefore, cumulative routing metrics should be considered. Furthermore, some QoS metrics can be combined with these routing metrics, namely link quality, path reliability, and packet loss. The protocols discussed herein hardly include the problem of combining routing metrics along with QoS metrics. Certain protocols consider only one routing metric. Existing protocols can be improved by proving their robustness through a performance comparison with hybrid and cumulative routing metrics.

WSNs are prone to many security concerns that have not been dealt with in many of the designed routing protocols. The vulnerability of the network to eavesdropping, unauthorized access, spoofing, and DDoS attacks has increased owing to the wireless communication between sensor nodes [74]. Moreover, resource limitation in WSNs resulted in us considering the effectiveness of the traditional security mechanisms. It is quite easy to make a WSN secure through the implication of game theory-based routing protocols. As these protocols can make sensor nodes in a WSN rational, it is possible to exclude malicious nodes from the routing path. The protocol presented in [43] is an example of this. Few protocols have used game theory to ensure secure routing. This can be a future research subject.

As we have already discussed that WSNs are resource-constrained networks, data redundancy can lead to more resource limitations. To prevent this, we must ensure the freshness of data. This implies that the data are recent and ensures that no adversary can replay old messages. Existing works that use game theory-based algorithms to design routing protocols do not cover the problem of data redundancy. If the game is designed in such a way that the pay-off of a sensor node decreases when it causes unnecessary redundant transmissions, the data redundancy concern can be avoided.

The energy hole problem is another crucial concern, and it is very important to solve this problem through routing techniques to keep a WSN fully functional. The nodes near the sink region will die sooner because the nodes send their own data as well as forward data from outer subregions to the sink [75]. Only GTEB [40], among the routing protocols discussed here, considers this problem. Certain protocols in the literature have used the cooperative game theory to ensure cooperative routing for the sake of reducing energy consumption. There is a high risk that these protocols would result in an energy hole problem causing harm to the network's functionality. This problem should be carefully handled in the future design of a routing protocol.

Game theory is important for WSN routing because the game theory makes the nodes rational. For example, certain protocols involve rational decision making, which incorporates a node's decision on whether to be a CH or not on the basis of residual energy [41,42]. Furthermore, a protocol may involve the rational decision of the nodes when they transmit the data packet selfishly or cooperatively [43]. Designing these types of strategies to make the nodes rational is a great challenge. Although it varies based on the design and implementation of routing protocols, the main objective is to increase energy efficiency by decreasing delay through the introduction of rationality among nodes. Therefore, game theory-based routing protocols are suitable for applications where energy is a critical resource. In wireless multimedia sensor networks (WMSNs) for environment monitoring, for example, wirelessly interconnected sensor nodes are equipped with multimedia devices, such as cameras and microphones, and are capable of retrieving video and audio streams as well as scalar sensor data [75].

Energy is more crucial here because dealing with multimedia contents requires a higher bandwidth and improved data rate. A game theory-based routing protocol may suit the subtle energy-saving requirement of WMSNs.

### 5.2. Challenging Problems

Certain existing works related to game theory-based protocols even apply two types of games to design the routing protocol. Furthermore, some protocols incorporate a secondary algorithm along with game theory-based models. It is obvious that sensor nodes have limited processing power and memory capacity. Too much complexity in a routing protocol design is not feasible with the core design of sensor nodes. For cooperative games, cooperation overhead always exists. Too many coalition formations may reduce the network lifetime, as the nodes have to exchange the data frequently. For noncooperative games, it is difficult to attain the Nash equilibrium and obtain the optimal strategies. Selfish nodes are often excluded from the routes in other types of games. This may also lead to network isolation. It is a significant challenge to design a routing protocol using game theory that is also simple and can be implemented in energy critical sensors.

The main hypothesis of game theory is the assumption of the nodes being rational in a WSN, where they also seek for their best interest. This behavior of the nodes is hard to guarantee because a WSN is subjected to numerous changes (change of energy level, topology, network structure).

In cooperative games, players cooperate with each other to increase an overall benefit. The players (nodes) in a game sometimes tend to be selfish and have a tendency to display selfish behavior. Incentive mechanisms are necessary to ensure cooperation, which is a tough task.

Designing and formulating pay-off functions for a game is crucial and challenging. A bad design may not satisfy the needs and introducing rationality among the players (nodes) can fail drastically.

The formulation of noncooperative game theory requires the attainment of Nash equilibrium, where no player can benefit without decaying another's pay-off through a unilateral move. This equilibrium point is not always guaranteed to be attained by the players. Attaining this point is one of the biggest challenges in formulating noncooperative game theory in a WSN paradigm.

## 6. Conclusions

In this paper, the various game theory-based routing protocols for WSNs were reviewed and discussed extensively. The routing protocols were classified into the four different types of games, and their key characteristics and operations were reviewed protocol by protocol. Subsequently, they were qualitatively compared with each other in terms of major features, advantages, and limitations. The results of our comparison can make it easy to choose a particular protocol based on the application requirement. Existing unresolved concerns and possible challenges, along with future research directions, were discussed too. They will be analyzed in the future design of game theory-based routing protocols for WSNs such that the routing becomes more efficient and robust.

**Author Contributions:** The individual contributions of the authors are as follows. M.A.H. categorized, analyzed, and summarized game theory-based routing protocols for WSNs. S.M. directed research and contributed to the review and analysis of routing protocols. The paper was drafted by M.A.H. and subsequently revised and approved by S.M.

**Funding:** This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MIST) (No. 2019R1F1A1060501). Correspondence should be addressed to Sangman Moh (smmoh@chosun.ac.kr).

**Acknowledgments:** The authors would like to thank the editor and anonymous referees for their upcoming helpful comments in improving the quality of this paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References


1. Agrawal, D.; De Morais Cordeiro, C. *Ad Hoc And Sensor Networks*, 3rd ed.; World Scientific Publishing Company: Singapore, 2006.
2. Ali, A.; Ming, Y.; Chakraborty, S.; Iram, S. A Comprehensive Survey on Real-Time Applications of WSN. *Future Internet* **2017**, *9*, 77. [CrossRef]
3. Khan, M.; Rinner, B. Energy-aware task scheduling in wireless sensor networks based on cooperative reinforcement learning. In Proceedings of the 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, Australia, 10–14 June 2014.
4. Li, D.; Wong, K.D.; Hu, Y.H.; Sayeed, A.M. Detection, classification, and tracking of targets. *IEEE Signal Process. Mag.* **2002**, *19*, 17–29.
5. Zhu, R.; Ma, M.; Zhang, Y.; Hu, J. Collaborative Wireless Sensor Networks and Applications. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 352761. [CrossRef]
6. He, T.; Krogh, B.; Krishnamurthy, S.; Stankovic, J.; Abdelzaher, T.; Luo, L.; Stoleru, R.; Yan, T.; Gu, L.; Hui, J. Energy-efficient surveillance system using wireless sensor networks. In Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services—MobiSYS, New York, NY, USA, 6–9 June 2004.
7. Boustani, A.; Girod, L.; Offenhuber, D.; Britter, R.; Wolf, M.; Lee, D.; Miles, S.; Biderman, A.; Ratti, C. Investigation of the waste-removal chain through pervasive computing. *IBM J. Res. Dev.* **2011**, *55*, 11:1–11:11. [CrossRef]
8. Aldeer, M. A summary survey on recent applications of wireless sensor networks. In Proceedings of the 2013 IEEE Student Conference on Research and Development, Putrajaya, Malaysia, 16–17 December 2013.
9. Arampatzis, T.; Lygeros, J.; Manesis, S. A Survey of Applications of Wireless Sensors and Wireless Sensor Networks. In Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, Limassol, Cyprus, 27–29 June 2005.
10. Ciuonzo, D.; Salvo Rossi, P. Distributed detection of a non-cooperative target via generalized locally-optimum approaches. *Inf. Fusion* **2017**, *36*, 261–274. [CrossRef]
11. Ciuonzo, D.; Salvo Rossi, P. Decision Fusion with Unknown Sensor Detection Probability. *IEEE Signal Process. Lett.* **2014**, *21*, 208–212. [CrossRef]
12. Ribeiro, A.; Giannakis, G. Bandwidth-constrained distributed estimation for wireless sensor Networks-part I: Gaussian case. *IEEE Trans. Signal Process.* **2006**, *54*, 1131–1143. [CrossRef]
13. Shirazinia, A.; Dey, S.; Ciuonzo, D.; Salvo Rossi, P. Massive MIMO for Decentralized Estimation of a Correlated Source. *IEEE Trans. Signal Process.* **2016**, *64*, 2499–2512. [CrossRef]
14. Ribeiro, A.; Giannakis, G. Bandwidth-constrained distributed estimation for wireless sensor networks-part II: Unknown probability density function. *IEEE Trans. Signal Process.* **2006**, *54*, 2784–2796. [CrossRef]
15. Chong, C.Y.; Kumar, S. Sensor networks: Evolution, opportunities, and challenges. *Proc. IEEE* **2003**, *91*, 1247–1256. [CrossRef]
16. Pattem, S.; Poduri, S.; Krishnamachari, B. Energy-Quality Tradeoffs for Target Tracking in Wireless Sensor Networks. In *Information Processing in Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2003.
17. Al-Karaki, J.; Kamal, A. Routing techniques in wireless sensor networks: A survey. *IEEE Wirel. Commun.* **2004**, *11*, 6–28. [CrossRef]
18. Kosunalp, S. A New Energy Prediction Algorithm for Energy-Harvesting Wireless Sensor Networks with Q-Learning. *IEEE Access* **2016**, *4*, 5755–5763. [CrossRef]
19. Pavlidou, F.; Koltsidas, G. Game theory for routing modeling in communication networks—A survey. *J. Commun. Netw.* **2008**, *10*, 268–286. [CrossRef]
20. Shi, H.; Wang, W.; Kwok, N.; Chen, S. Game Theory for Wireless Sensor Networks: A Survey. *Sensors* **2012**, *12*, 9055–9097. [CrossRef] [PubMed]
21. AlSkaif, T.; Guerrero Zapata, M.; Bellalta, B. Game theory for energy efficiency in Wireless Sensor Networks: Latest trends. *J. Netw. Comput. Appl.* **2015**, *54*, 33–61. [CrossRef]
22. Crosby, G.; Pissinou, N. Evolution of Cooperation in Multi-Class Wireless Sensor Networks. In Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN 2007), Dublin, Ireland, 15–18 October 2007.
23. Felegyhazi, M.; Hubaux, J.; Buttyan, L. Cooperative Packet Forwarding in Multi-Domain Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops, Kauai Island, HI, USA, 8–12 March 2005.

24. Kannan, R.; Iyengar, S. Game-Theoretic Models for Reliable Path-Length and Energy-Constrained Routing with Data Aggregation in Wireless Sensor Networks. *IEEE J. Sel. Areas Commun.* **2004**, *22*, 1141–1150. [CrossRef]
25. Zakiuddin, I.; Hawkins, T.; Moffat, N. Towards A Game Theoretic Understanding of Ad-Hoc Routing. *Electron. Notes Theor. Comput. Sci.* **2005**, *119*, 67–92. [CrossRef]
26. Schillings, A.; Yang, K. VGTR: A Collaborative, Energy and Information Aware Routing Algorithm for Wireless Sensor Networks through the Use of Game Theory. In *GeoSensor Networks*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 51–62.
27. Behzadan, A.; Anpalagan, A.; Ma, B. Prolonging Network Lifetime via Nodal Energy Balancing in Heterogeneous Wireless Sensor Networks. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011.
28. Jia, Z.; Mu, C.D.; Hu, J.B. Game Theoretic Energy Balance Routing in Wireless Sensor Networks. In Proceedings of the 2007 Chinese Control Conference, Hunan, China, 26-31 July 2007.
29. Zheng, M. Game Theory Used for Reliable Routing Modeling in Wireless Sensor Networks. In Proceedings of the 2010 International Conference on Parallel and Distributed Computing, Applications and Technologies, Wuhan, China, 8–11 December 2010.
30. Sun, D.; Huang, X.; Liu, Y.; Zhong, H. Predictable Energy Aware Routing based on Dynamic Game Theory in Wireless Sensor Networks. *Comput. Electr. Eng.* **2013**, *39*, 1601–1608. [CrossRef]
31. Sathian, D.; Baskaran, R.; Dhavachelvan, P. Lifetime enhancement by Cluster Head Cooperative Trustworthy Energy Efficient MIMO routing algorithm based on game theory for WSN. In Proceedings of the 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12), Coimbatore, India, 26–28 July 2012.
32. Duan, J.; Gao, D.; Yang, D.; Foh, C.; Chen, H. An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. *IEEE Internet Things J.* **2014**, *1*, 58–69. [CrossRef]
33. Pitchai, K.; Paramasivan, B.; Bhuvaneswari, M. Game Theoretical Computation Based Energy Efficient Routing for Wireless Sensor Networks. In Proceedings of the 2014 3rd International Conference on Eco-Friendly Computing and Communication Systems, Mangalore, India, 18–21 December 2014.
34. Saghezchi, F.; Radwan, A.; Rodriguez, J. Energy-aware relay selection in cooperative wireless networks: An assignment game approach. *Ad Hoc Netw.* **2017**, *56*, 96–108. [CrossRef]
35. Feng, R.; Yu, N.; Wu, Y.; Li, T. Reliable routing in wireless sensor networks based on coalitional game theory. *IET Commun.* **2016**, *10*, 1027–1034. [CrossRef]
36. Lee, D.; Shin, H.; Lee, C. Game theory-based resource allocation strategy for clustering based wireless sensor network. In Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication—ICUIMC'12, Kuala Lumpur, Malaysia, 20–22 February 2012.
37. Jamin, B.; Chatterjee, M.; Samanta, T. A game theoretic routing framework based on energy-delay conservation in WSNs. In Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 7–9 April 2015.
38. Wu, F.; Gong, K.; Zhang, T.; Chen, G.; Qiao, C. COMO: A Game-Theoretic Approach for Joint Multirate Opportunistic Routing and Forwarding in Non-Cooperative Wireless Networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 948–959. [CrossRef]
39. Xin, Z.; Xin, Z.; Guo, H.Y.; Qian, L. The Inter-Cluster Routing Algorithm in Wireless Sensor Network Based on the Game Theory. In Proceedings of the 2013 Fourth International Conference on Digital Manufacturing & Automation, Qingdao, China, 29–30 June 2013.
40. Abd, M.; Singh, B.; Rubeaai, S.; Tepe, K.; Benlamri, R. Game theoretic energy balanced (GTEB) routing protocol for wireless sensor networks. In Proceedings of the 2014 IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 6–9 April 2014.
41. Lin, D.; Wang, Q.; Lin, D.; Deng, Y. An Energy-Efficient Clustering Routing Protocol Based on Evolutionary Game Theory in Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 409503. [CrossRef]
42. Lin, D.; Wang, Q. A game theory-based energy efficient clustering routing protocol for WSNs. *Wirel. Netw.* **2016**, *23*, 1101–1111. [CrossRef]
43. Li, F.; Gao, F.; Yao, L.; Chang, G. A Game Theory Based Approach for Routing in Wireless Sensor Networks. *Adv. Eng. Forum* **2011**, *2–3*, 599–603. [CrossRef]

44. Qin, X.; Wang, X.; Wang, L.; Lin, Y.; Wang, X. An efficient probabilistic routing scheme based on game theory in opportunistic networks. *Comput. Netw.* **2019**, *149*, 144–153. [CrossRef]
45. Attiah, A.; Amjad, M.; Chatterjee, M.; Zou, C. An evolutionary routing game for energy balance in Wireless Sensor Networks. *Comput. Netw.* **2018**, *138*, 31–43. [CrossRef]
46. Yetgin, H.; Cheung, K.; El-Hajjar, M.; Hanzo, L. A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 828–854. [CrossRef]
47. Ogundile, O.; Alfa, A. A Survey on an Energy-Efficient and Energy-Balanced Routing Protocol for Wireless Sensor Networks. *Sensors* **2017**, *17*, 1084. [CrossRef]
48. Osborne, M. *An Introduction to Game Theory*; Shanghai University of Finance & Economics Press: Shanghai, China, 2005.
49. Turocy, T.; Stengel, B. Game Theory. Available online: http://www.cdam.lse.ac.uk/Reports/Files/cdam-2001-09.pdf (accessed on 17 May 2019).
50. Chalkiadakis, G.; Elkind, E.; Wooldridge, M. Cooperative Game Theory: Basic Concepts and Computational Challenges. *IEEE Intell. Syst.* **2012**, *27*, 86–90. [CrossRef]
51. Jin, H.; Jiang, W. *Handbook of Research on Developments and Trends in Wireless Sensor Networks*; Information Science Reference: Hershey, PA, USA, 2010.
52. Sasaki, T.; Yamamoto, H.; Okada, I.; Uchida, S. The Evolution of Reputation-Based Cooperation in Regular Networks. *Games* **2017**, *8*, 8. [CrossRef]
53. Singh, K.; Moh, S. Routing protocols in cognitive radio ad hoc networks: A comprehensive review. *J. Netw. Comput. Appl.* **2016**, *72*, 28–37. [CrossRef]
54. Youssef, M.; Ibrahim, M.; Abdelatif, M.; Chen, L.; Vasilakos, A. Routing Metrics of Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 92–109. [CrossRef]
55. Sohraby, K.; Minoli, D.; Znati, T. *Wireless Sensor Networks: Technology, Protocols, and Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
56. Sathian, D.; Baskaran, R.; Dhavashelvan, P. A trustworthy energy efficient MIMO routing algorithm based on game theory for WSN. In Proceedings of the IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM-2012), Tamil Nadu, India, 30–31 March 2012.
57. Kazemeyni, F.; Johnsen, E.; Owe, O.; Balasingham, I. Grouping Nodes in Wireless Sensor Networks Using Coalitional Game Theory. In *Formal Techniques for Distributed Systems*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 95–109.
58. Theodorakopoulos, G.; Baras, J. On trust models and trust evaluation metrics for ad hoc networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 318–328. [CrossRef]
59. Zhang, C.; Zhu, X.; Song, Y.; Fang, Y. A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks. In Proceedings of the 2010 Proceedings IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010.
60. Xia, H.; Jia, Z.; Li, X.; Ju, L.; Sha, E. Trust prediction and trust-based source routing in mobile ad hoc networks. *Ad Hoc Netw.* **2013**, *11*, 2096–2114. [CrossRef]
61. Ren, Y.; Boukerche, A. Performance Analysis of Trust-Based Node Evaluation Schemes in Wireless and Mobile Ad Hoc Networks. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009.
62. Mahmoud, M.; Shen, X. Trust-Based and Energy-Aware Incentive Routing Protocol for Multi-Hop Wireless Networks. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011.
63. Ren, Y.; Boukerche, A. Modeling and Managing the Trust for Wireless and Mobile Ad Hoc Networks. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008.
64. Duan, J.; Gao, D.; Foh, C.; Zhang, H. TC-BAC: A trust and centrality degree based access control model in wireless sensor networks. *Ad Hoc Netw.* **2013**, *11*, 2675–2692. [CrossRef]
65. Deng, H.; Jin, G.; Sun, K.; Xu, R.; Lyell, M.; Luke, J. Trust-Aware In-Network Aggregation for Wireless Sensor Networks. In Proceedings of the GLOBECOM 2009—2009 IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009.
66. Liu, X.; Yang, X.; Xia, Y. NetFence. *ACM SIGCOMM Comput. Commun. Rev.* **2010**, *40*, 255. [CrossRef]
67. Xu, Z.Y.; Yin, Y.; Wang, J. A Density-based Energy-efficient Routing Algorithm in Wireless Sensor Networks Using Game Theory. *Int. J. Future Gener. Commun. Netw.* **2002**, *5*, 62–70.

68. Heinzelman, W.; Chandrakasan, A.; Balakrishnan, H. An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **2002**, *1*, 660–670. [CrossRef]
69. Chipara, O.; He, Z.; Xing, G.; Chen, Q.; Wang, X.; Lu, C.; Stankovic, J.; Abdelzaher, T. Real-time Power-Aware Routing in Sensor Networks. In Proceedings of the 14th IEEE International Workshop on Quality of Service, New Haven, CT, USA, 19–21 June 2006.
70. Pantazis, N.; Nikolidakis, S.; Vergados, D. Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 551–591. [CrossRef]
71. Lung, C.; Zhou, C. Using hierarchical agglomerative clustering in wireless sensor networks: An energy-efficient and flexible approach. *Ad Hoc Netw.* **2010**, *8*, 328–344. [CrossRef]
72. Manjeshwar, A.; Agrawal, D. TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. In Proceedings of the 15th International Parallel and Distributed Processing Symposium, San Francisco, CA, USA, 23–27 April 2001.
73. Seah, W.; Tan, Y. *Sustainable Wireless Sensor Networks*; Tech: Rijeka, Croatia, 2010.
74. Pathak, A.; Tiwari, M.K. Minimizing the Energy Hole Problem in Wireless Sensor Networks by Normal Distribution of Nodes and Relaying Range Regulation. In Proceedings of the Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, India, 3–5 November 2012.
75. Akyildiz, I.; Melodia, T.; Chowdhury, K. A survey on wireless multimedia sensor networks. *Comput. Netw.* **2007**, *51*, 921–960. [CrossRef]

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).