Wireless Engineering and Technology, 2014, 5, 62-73
Published Online July 2014 in SciRes. http://www.scirp.org/journal/wet
http://dx.doi.org/10.4236/wet.2014.53008

Scientific Research

An Efficient Billing Scheme for Trusted Nodes Using Fuzzy Logic in Wireless Sensor Networks

Mohammad M. Shurman[1], Zaid A. Alomari[2], Khaldoon M. Mhaidat[2]

[1]Network Engineering and Security Department, Jordan University of Science and Technology, Irbid, Jordan
[2]Computer Engineering Department, Jordan University of Science and Technology, Irbid, Jordan
Email: alshurman@just.edu.jo, zaid.alomari@gmail.com, mhaidat@just.edu.jo

Received 25 January 2014; revised 26 March 2014; accepted 27 April 2014

Abstract

Extending the lifetime of the wireless sensor networks (WSNs), where recharging sensors is not always possible, has been a major concern for researchers for the past decade. In this paper, we study the cooperation between nodes in wireless sensor networks in forwarding packets to others, and we propose a new collaboration technique which stimulates intermediate nodes to forward packets toward their destination. Some nodes show selfish behavior by denying the forwarding packets to other nodes in commercial networks in an effort to preserve their own energy. This paper applies a technique which is used to prolong the network lifetime, based on a node's energy and trust value, and additionally incorporates fuzzy logic, which stimulates nodes to forward packets by rewarding cooperation. According to simulation results, the proposed approach surpasses the *Nuglets* (virtual currency) approach and the *Reputation* approach in network energy and thus prolongs the network lifetime. Additionally, our proposed approach demonstrates better results in the number of dropped packets, PDR and forwarded packets to neighboring nodes.

Keywords

Wireless Sensor Network (WSN), Charging, Trusted Node, Rewarding, Billing, Cluster Area, Packet Forwarding

1. Introduction

Wireless Sensor Networks (WSNs) have spread rapidly these days for many real-life applications and have become a hot topic for researchers. WSNs handle two types of networks for node communication, depending on

How to cite this paper: Shurman, M.M., Alomari, Z.A. and Mhaidat, K.M. (2014) An Efficient Billing Scheme for Trusted Nodes Using Fuzzy Logic in Wireless Sensor Networks. *Wireless Engineering and Technology*, **5**, 62-73.
http://dx.doi.org/10.4236/wet.2014.53008

the availability of their infrastructure: infrastructure and infrastructure-less networks [1]. In infrastructured networks, nodes communicate with a BS (base station) to send and receive packets. Infrastructure-less networks consist of wireless mobile nodes that move dramatically and communicate with each other without any central controller. The main difference between infrastructure and infrastructure-less networks is that the communication between nodes in the former is managed by an access point that may be connected to the Internet or intranet.

Wireless sensor networks consist of wireless nodes that are communicating in a wireless environment. Communication between these nodes is accomplished through the use of routing protocols, by which wireless sensor nodes act as senders, receivers and routers. As nodes are deployed freely into the network, the network topology allows the nodes to collaborate with each other to send and receive packets from source nodes to destination nodes. The communication distance from the source to the destination may be small or large, with the larger distance consuming the higher power for packet delivery. Additionally, the nodes between the source and destination may be untrusted and may drop packets in transit to other nodes. This behavior negatively affects the network functionality [2] [3].

Furthermore, some nodes between the source and destination drain their energy in forwarding packets to their neighbors without benefit, which affects the network functionality and lifetime [4]. To prolong the network lifetime and maintain network functionality, we employed a billing technique to encourage packet forwarding by nodes to other nodes.

Studying the trusted node or trusted path model [5] differs from studying the security models in WSNs [6]. Security models address the preservation of a network from malicious nodes that may attack the network and strain their resources. Trust models are used to evaluate the trustworthiness of other nodes, since the network lifetime is dependent on the trusted nodes and their cooperation between each other. Authors of [7] studied the concept of "trust" and its meaning in varying fields. The trust concept exists in social science research, human communication, psychological aspects, etc. Trust is an indication about reliability. Hence, trusted nodes in WSNs will be able to provide safe passage for communication between nodes, allowing them to convey information among each other reliably.

Once trusted nodes cooperation is established, some nodes may demonstrate an unwillingness to communicate with other nodes [8]. This behavior negatively affects network efficiency. However, by obligating these selfish nodes into cooperation with other nodes, the network lifetime is ameliorated.

Going to fuzzy logic technique, we are talking about range of possible values (degree of truth) like temperature, height, speed, etc. Fuzzy is not a logic technique having two values, true or false, but fuzzy uses the logic in describing the fuzziness. In other side, binary logic is talking about sharp values true or false [9]. For example, if a person's height is greater than 170 cm, we said "the person is tall else if his height is less than 170 cm" then we said "he is short". In fuzzy logic, there is no distinct edge for the object property value, if the height of 170 cm is tall then how a height of 169 cm is considered short. Thus, fuzzy logic uses possibility theory to assign values for the property based on the human sense (*i.e.*, 169 cm can be considered not tall or little short). Degree of the membership identifies the fuzzy value for the variable that the fuzzy system needs to measure like the height in our previous example. If the person is very tall we give it fuzzy values between 0.8 and 1, but if the person is too short we give it fuzzy values between 0 and 0.2 and so on for different values of height. In the changeable environment's parameters values, we can see fuzzy logic clear since we cannot have exact value for each variable parameter. For example if the temperature is 30˚C, the weather is hot, but if the temperature is not 30˚C, we cannot say the weather is not hot. Linguistic variables like (small, tall, medium, hot, cold, etc.) are used in fuzzy rules to generate the desired system results. The rules are written in IF-THEN format. Mamdani fuzzy logic is the famous fuzzy system uses four steps, fuzzification of input variables, rule evaluation, aggregation of the rule outputs, and finally defuzzification.

The remaining of our paper is organized as follows: Section 2 describes relevant related work. The methodology and detailed approach are explained in Section 3. Experimentation and simulation results are presented in Section 4. And finally, Section 5 presents our conclusion and the future work.

2. Related Work

In this section, an overview of related work that focuses on forcing nodes into collaboration to forward packets from source to destination is part of our discourse. Nuglet mechanism, virtual currency is used to pay for nodes

involved in forwarding the packets. Billing accounts for rewarding and charging the nodes are created. Rewarding means that the intermediate nodes which are involved in communication will be rewarded for the forwarding service they provide for the neighbors [10]. Charging means that the node which tries to send its packets will be charged, and its billing account will be decreased. Nuglet counter at each node is used to calculate the nuglet value when the node forwards or generates packets. The approach provides a nuglets amount for each node. Once the node wants to send its own packets, its nuglets value will be decreased. At the same time, if the node wants to forward packets for neighbors, its nuglets counter will increase.

Reputation mechanism uses a reputation value for each node in the network. The reputation value reflects how much the node is collaborating in the network and how much this node misbehaves [11]. Using this mechanism in WSNs, allows identifying the misbehavior nodes like selfish node or any malicious node in security fields. High reputation value means high rank of collaboration for that node. Reputation value for each node is calculated depends on the observation of the nodes that reflects how much the node is collaborative in the network. If the value of the reputation is less than threshold, then the node will be considered as a selfish or misbehavior node.

In [12], rational collaboration for the selfish node scheme is proposed. In this scheme, researchers studied the rewarding and charging of network nodes. The Base station is used for communication with mobile nodes in order to send and receive packets. All nodes and base station sutilize the same level of energy to communicate with each other. Communication is accomplished by sending packets from a source node to a source base station and finally to a base station at the destination. Ultimately, the packets are sent from the destination base station to destination node. This approach charges and rewards nodes that collaborate in forwarding packets by means of a specific credit amount. Rewarding is also used when the destination node sends an acknowledgment to the destination base station. This scheme uses an external operator which has an account for each node to charge and reward the nodes with credit.

Nodes in commercial networks are not always willing to cooperate in the forwarding of packets to other nodes since this lessens their energy resources. A load-based approach is proposed in [13]. This approach considers the number of packets generated by the node and packets forwarded to neighbor nodes as the main metrics to build the load based scheme. Virtual currency, ornuglets, is used to pay nodes for involvement in forwarding packets. A nuglet counteris used for each node to calculate the total nuglet value for each time the node forwards or generates packets. The nuglet scheme does not take into account the nodes' existing energy or the energy required to send and receive data packets for different node locations.

In [14], a novel approach conceives the use of a receipt message when the node sends packets to other nodes. This receipt message remains with the node until the *Credit Clearance Services* (*CCS*) becomes active. The CCS collects this receipt from the node and then credits all nodes that participated in the packet transmission. The node can collect credits by forwarding packets to neighbor nodes. In this scheme, the CCS system employs a reduced receipt message size, economizing bandwidth and storage. A hardware module was used in [15], this module contains a nuglet counter which engages to reward and charge nodes. The nuglet counter's tabulation increases when a node forward spackets to other nodes, and conversely, decreases when this node generates its own packets. In this mechanism, the node forwards packets to other nodes but is not allowed to disseminate large quantities of packets to destination nodes, since the available bandwidth for each node decreases when the number of nodes increases in the network. This scheme uses prescripts to decide whether the packets will be dropped or forwarded, which serve to secure communication.

Authors of [16] demonstrate how cooperation increases the network lifetime. Communication in a small area radius can be accomplished without cooperation, but for large transmission distances, cooperation between nodes is needed to minimize power consumption. The relationship between communication distance and number of reachable nodes within that distance was studied with the aim to discover the optimal power consumption. The packet generated by the source node in this approach was divided into small packets and sent over multiple paths. Nodes in these paths cooperate to send these small packets to the destination node. This approach accomplished better results when compared to non-cooperative approaches.

Researchers in [17] studied the selection of trusted nodes in packet forwarding. Their trust approach was built based on the past and current history of nodes using neighboring observations or direct observations from the node itself. Trust initialization, evidence gathering, trust calculation/decision making, and trust update are the principle observations used to determine if nodes are trusted to forward packets. In this approach, the untrusted nodes are isolated, since they were uncooperative in forwarding packets to other nodes, and only generated their

own packets.

In [18], another type of cooperation between intermediate nodes was studied to consummate efficient localization. A new localization algorithm for mobile nodes was established, which uses two techniques to construct localization based on node cooperation. The first technique exploits the localized nodes to locate unknown nodes. Nodes in the second technique overhear information from the neighbors' localization messages exchange. This algorithm works on demand; once the node moves and reaches a location with incident, such as an invalid location, the algorithm tries to identify the location of that node.

Greedy nodes are identified and isolated in [19]. A *Self-Centered Friendship* algorithm was built which isolates uncooperative nodes. The isolation of non-cooperative nodes prevents them from utilizing network resources to send their own packets. Credit risk is also given to each node to specifically identify which node is greedy and which node is not. Once the credit risk of the node between the source and destination is less than the threshold value, the node is identified as greedy and consequently isolated.

Caching data for fast response in wireless sensor networks and the cooperation between nodes in selecting the important node to cache data was studied in [20]. Nodes with enough energy and that are located on the shortest paths are considered important nodes and are selected based on the node's centrality to its neighboring nodes and on the node's remaining energy. Thus, nodes residing on the shortest path are taken into account as being important nodes.

Cooperation over MAC protocol was proposed in [21]. A group ID is embedded within sensor nodes, as well as with nodes that can broadcast messages to its neighbors with a specific group ID. If this group ID in the message header matches the group ID of the sensor node, this sensor is considered as a relay for that node, which forward spackets to other nodes.

In [22], virtual currency was proposed to observe how cooperation can be accomplished with the exchanging of virtual currency between nodes. This method resolves the selfishness of nodes by crediting cooperative nodes that allow communication through them. A charging model was used to simulate the virtual currency, and a protection model was implemented to guard the communication during the currency exchange.

Cooperative communication groups and an algorithm were built to grow these groups in the network was proposed in [23]. Nodes in these groups can cooperate to transmit data from a group to another group within the network. The cooperative group has a cooperative-group-head responsible for communication with the base station and with other groups. The cooperative-group-head is selected based on its energy; therefore, the node with the highest energy within the group is selected as the head of that group during communication.

In [24], researchers studied the implementation of self-learning networks that were used to uncover the most cooperative nodes. Additionally, researchers studied the enforcement of node cooperation and the assurance of this cooperation. They proposed a search algorithm for nodes with the best cooperation features. Flooding and prediction were used to identify these nodes, which in turn forced greedy/selfish nodes into cooperative ones.

3. Proposed Approach

In this section, we present our proposed approach which forces nodes into cooperation of forward packets to neighboring nodes in WSN. The main three proposed mechanisms are:

- Charging the source node that generates packets.
- Selecting nodes with a high level of trust to act as intermediate nodes to forward packets.
- Rewarding the intermediate nodes that cooperate in forwarding packets.

In **Figure 1**, we can see that our main algorithm divides the network topology into a specific number of clustered areas which allows for full control over the network. Once the network is divided, deployment of nodes in the network is done arbitrarily. Nodes have an initial energy for transmission of packets, and an initial nuglets value assigned for the forwarding of packets to their neighbors.

A billing account is created directly for each node once the network life has begun. The account contains the initial nuglet values used in charging the node once any packet for transmission is generated, and thus reward the intermediate nodes after forwarding packets to its neighbors. Once a billing account is established for each node, we then calculate the trust level for each node using fuzzy logic, based on four input parameters. The trust value for each node is calculated using if-then rules in the fuzzy system we built. The inputs for this fuzzy system are: node energy, distance between nodes, number of packets dropped (by the node we wish to entrust), and accrued nuglet value of the node. The node's trust value is then generated by our fuzzy logic system.

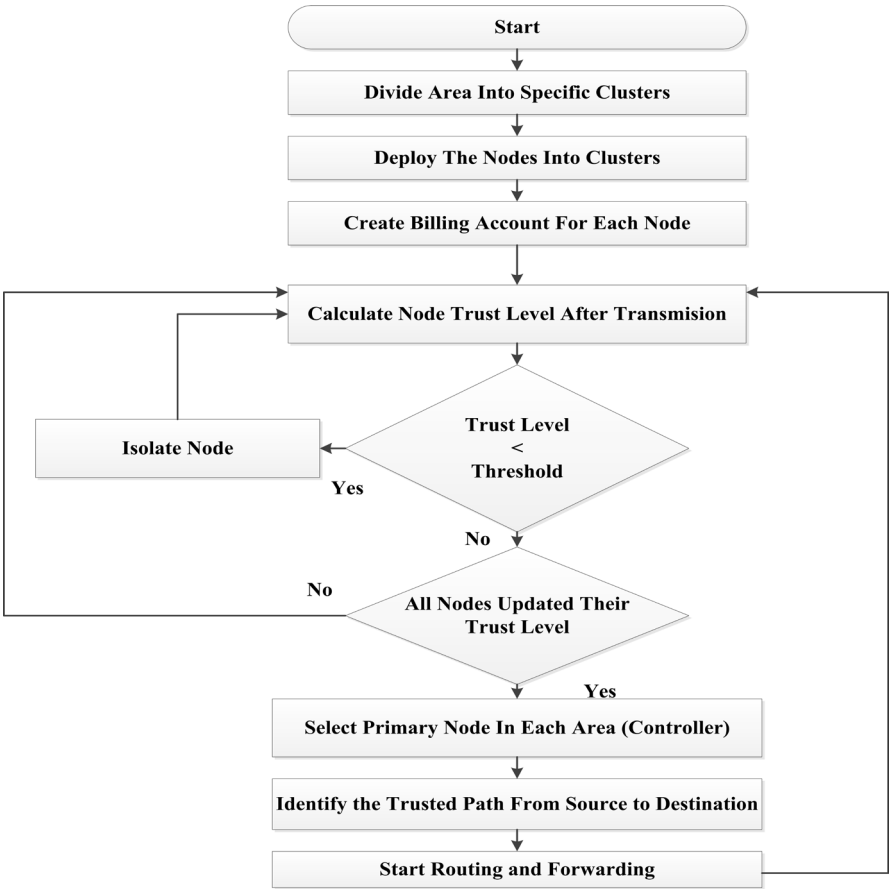

Figure 1. Main algorithm.

A primary node was selected in each cluster area to be responsible for that area. The primary node works as a comptroller for that area to charge and reward nodes. We select the comptroller node based on the updated trust value that is calculated every time the transmission process completed. This comptroller (gateway) node changes periodically to distribute comptroller role power consumption among all nodes in the cluster, and it represents the point of contact between the cluster and nodes in other clusters.

Trust value for each node is calculated, so that if an untrusted node is encountered, it is isolated from forwarding packets to neighbor nodes, which mitigates the dropped packets value. This isolated node canregenerate its own packets once its trust level is increased with the forwarding of packets to neighboring nodes; otherwise, it cannot generate any packet and remains in waiting until its trust value increases. Comptroller nodes recognize trusted nodes and then select the nodes with the highest trust values to carry on transmission of packets from the source to the comptroller. At this point, packets routing and forwarding is initiated.

The process for routing and forwarding packets is summarized in **Figure 2**. The figure shows the main sub processes for packet forwarding. The initial step sends the packets from the source node to the comptroller node in the vicinity of the source node over a trusted path. The second step forwards the packets from the comptroller node located in the source area vicinity to the comptroller node located in the destination vicinity (gateway communication). At this time, the comptroller node at the source area updates the billing accounts for the nodes that are involved in the transmission of packets in its area The third step is to forward the packets from comptroller node located in destination vicinity to the final destination, or target node, over a trusted path. The comptroller node at the destination area then updates the billing accounts for each node involved in the forwarding process in its area. It is noteworthy to mention that the comptrollers are not charged or credited, since the role of comptroller node lasts for only a short period and rotates among all nodes in the cluster. Thus, the node acts as a comptroller momentarily will change to a regular node later, which is charged or credited for cooperation.

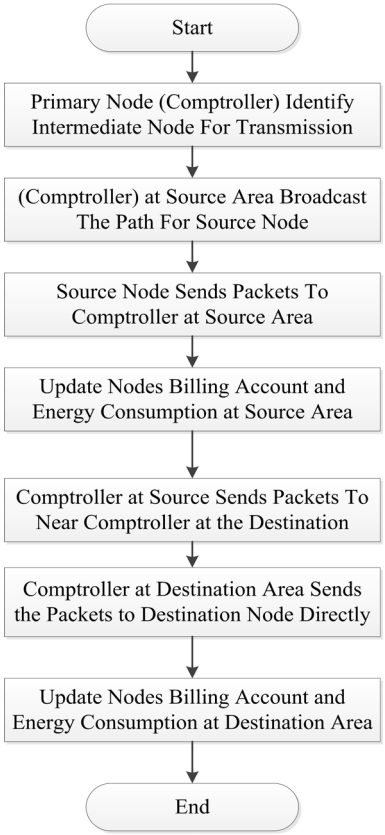

Figure 2. Routing and forward packets algorithm.

Fuzzy logic system is used to build our approach using four input parameters with three fuzzy representations for each input parameter as shown in **Table 1**. The system has 81 rules to construct the trust value (our model calculates and chooses one value out of six possible trust values) for each node. These 81 rules originate from the four input parameters (node's energy, nuglet value, distance and dropped packet rate) with three sets of values for each parameter, which outputs 81 combinations:

$$81 \text{ rules} = (3 \text{ term set values for energy}) * (3 \text{ term set values for nuglet}) * (3 \text{ term set values for distance}) * (3 \text{ term set values for dropped packet})$$

In **Figure 3**, the proposed system utilizes *Mamdani* [25] fuzzy logic system to calculate the trust value for each node. The implementation of fuzzy logic is a key concept as there are several parameters used to sort the information and identify a node's trust value. For example, if the normalized distance value is 0.5 (medium), dropped packet is 0.5 (medium), energy is 0.826 (high) and nuglet value is 0.519 (high) for a node then the fuzzy system will generate trust value for that node equals to 0.45 (UnD is trust) based on our81 fuzzy rules.

4. Simulation Results and Discussion

MATLAB was used to simulate and analyze the proposed approach. We divided the network into clustering areas, deployed the nodes in the network, and then we calculated the distance, energy and other metrics for the nodes. Identifying trusted nodes is done using fuzzy logic, which is a form of artificial intelligence (AI) techniques. The fuzzy logic toolbox in MATLAB allowed a means to provide a modeling approach for analyzing, designing, and simulating the system. The fuzzy logic toolbox permitted us to convert this complex system into a simple one by utilizing fuzzy logic rules. Reputation approach and nuglet approach, which both use virtual currency, were compared against our approach. Our proposal uses the novel approach of 81 rules to simulate the network by implementing the fuzzy logic system. Based on our knowledge and the available wireless sensor

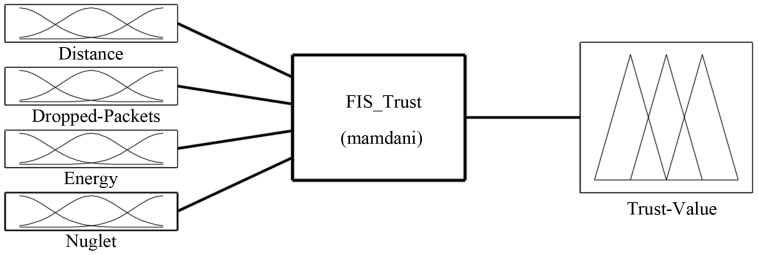

Figure 3. Fuzzy system to specify trust value.

Table 1. Trusted nodeselection parameters and their term sets*.

Parameter	Set values
Energy	Low, medium, high
Nuglet	Low, medium, high
Distance	Close, medium, far
Dropped packet	Few, medium, large
Trust value	High distrust, distrust, undistrust, untrust, trust, high trust

*Term sets: the values used by parameters as a representation of the parameters' values in our fuzzy logic system.

nodes collaboration's research, this is the first proposed approach which uses fuzzy logic to force the nodes into the collaboration of forwarding packets over trusted paths. These trusted paths ensure that the packets are delivered to their destination without being dropped.

4.1. System Assumption

Different assumptions are presumed in our system, they are as follows:

- A homogenous environment to implement our approach is assumed.
- Base station (sink) is fixed within the network.
- Wireless sensor nodes are stationary.
- The area is classified into three clusters.
- LEACH routing protocol is used in the network.

Various experimental scenarios were built using parameters mentioned in **Table 2**. Simulations were run for a number of different rounds to analyze how our approach behaves within the network. We compared our approach with the nuglets and reputation approaches. Different metrics were used in our comparison; the following are the important metrics we used to analyze our approach:

1) Packet delivery ratio: ratio number of packets that are correctly received to the number of packets are sent, which is defined as:

$$\text{PDR} = \text{Packets Received} / \text{Packets Sent}$$

2) Number of dropped packets during network lifetime: the total number of the packets that were dropped by all nodes in the network during network lifetime.

3) Number of forwarded packets from own and neighbor nodes.

a) Forwarded packets from own is the total number of packets that generated by the nodes themselves.

b) Forwarded packets from neighbors are the total number of packets that were forwarded by the nodes for neighboring nodes.

4) Network residual energy: the average remaining energy for all nodes in the network at a specific time during network lifetime.

4.2. Simulation Results

4.2.1. Remaining Energy Parameter

Figure 4 represents the residual energy in the network for different simulation rounds. The figure depicts the

Table 2. Parameters of our experiments.

Parameter	Value
Area	(100×100) m^2
Node numbers	25, 50, 75, 100
Simulation rounds (thousands)	10, 20, 30, 40, 50
Node initial energy	1 J
Transceiver energy	50 nJ/bit
Free space loss (E_{fs})	10 pJ/bit/m^2
Multi path loss (E_{mp})	1.3×10^{-3} pJ/bit/m^2
Initial nuglets	100 nuglets
Initial trust value	1

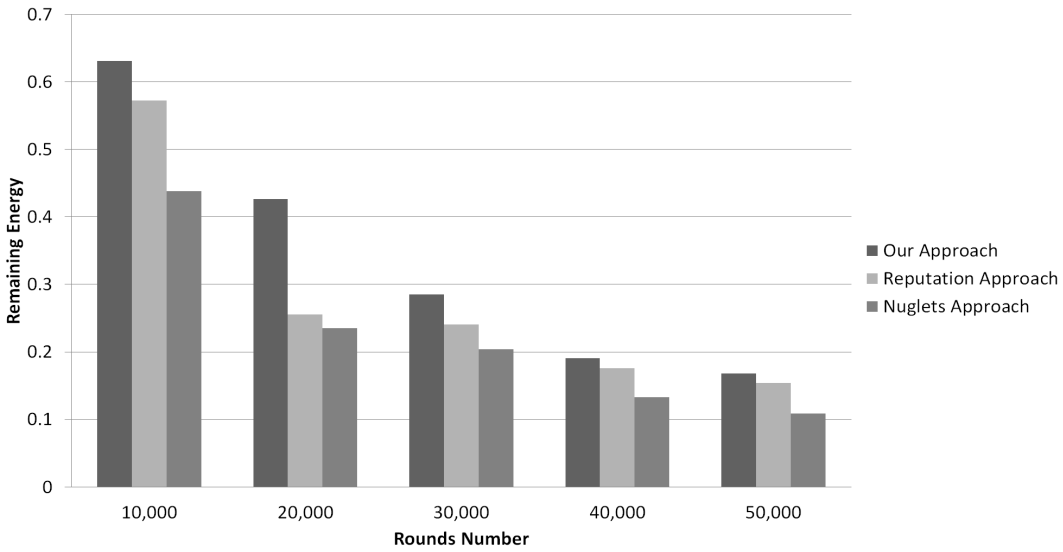

Figure 4. Remaining energy for small network.

behavior of our approach and that of other approaches when the network area size is small. Our proposed approach conserves the total network energy by distributing transmitted packets to all nodes in the network based on the trust value approach constructed. Our approach selects trusted routes with minimal energy consumption required to send packets. Reputation approach behaves better than the nuglets approach because the prior focuses on the reputation value for each node. The reputation value depends on the number of packets a node forwarded for itself and for its neighbors.

Figure 5 shows the remaining energy when deploying nodes in large network. Our approach still conserves significant energy, which means the network lifetime is prolonged in comparison to the nuglets approach and reputation approach. The nuglets approach is concerned only with node nuglet value without considering other parameters that may affect the network lifetime. The remaining energy for each node is one of these parameters that nuglets approach does not consider which affects the total residual energy in the network. The reputation approach shows better results than the nuglet approach since the reputation approach focus on the reputation value, which is calculated based on the number of transmitted packets through the nodes. Increasing the number of rounds shows a clear difference in the remaining energy between all approaches. This variance occurs as the total number dead nodes increases dramatically for nuglets and reputation approaches; whereas, nodes in our proposed approach remain active longer. **Figure 5** confirms that our approach conserves more energy during the lifetime of the network with differing time rounds.

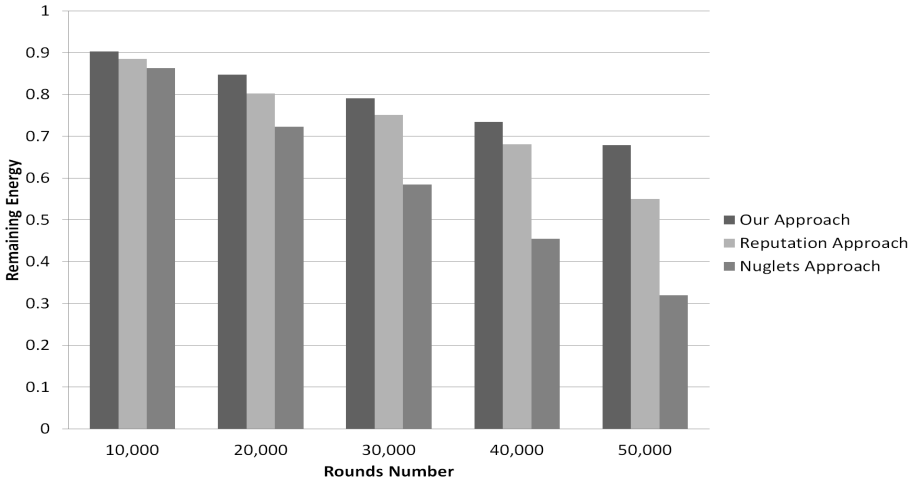

Figure 5. Remaining energy for large network.

4.2.2. Dropped Packets Parameter

Another factor in which our approach surpasses the nuglets approach and reputation approach is in the total number of dropped packets. In **Figure 6**, we can see that the nuglets approach has a large number of dropped packets. The justification for this increase is the high number of dead nodes in the network. Packets travel over nodes with a large number of nuglets, thus the paths are used many times which my provoke nodes to prematurely expire. Conversely, in the reputation approach, the number of dropped packets is decreased when compared to the nuglets approach, since only few nodes die early. Our approach uses distinct parameters with different paths to identify trusted nodes for transmission of packets to their destination with minimum energy consumption. Using trusted paths decreases the fortuity for packets being dropped; therefore, our approach meliorates packet dropping. Another interesting observation about dropped packets is that the dropped packet rate in small network is higher in the nuglets approach versus that of the reputation approach and our own approach. Our approach accomplishes better results in network with large number of nodes in the same fixed area space.

4.2.3. Packet Delivery Ratio Parameter

Figure 7 depicts the Packet Delivery Ratio (PDR) for all approaches, and it is noticeable that our approach has better PDR when compared against the two aforementioned approaches in small network size. The figure demonstrates the PDR value in different network sizes with different number of rounds. We used different number of rounds (from 10,000 to 50,000 rounds) to observe the PDR in our approach and the other approaches. In a large network size, we observed that the PDR for all approaches are close to each other, but our approach accomplished the best values for all network sizes, as shown in the less number of dropped packets, which directly improves the PDR value in our approach compared to the other approaches.

4.2.4. Forwarded Packets to Neighbors

To see how our approach forces the nodes to forward the packets to other nodes, **Figure 8** demonstrates how many packets are sent by nodes to neighboring nodes. Our approach has the largest number of forwarded packets to neighbor nodes for all network area sizes. Alternatively, the nodes in our approach forward the packets to neighbor nodes, which allow them to collect nuglets, and in turn permit them to generate their own packets in the future to prevent them from being isolated in the network. This high number of forwarding to neighbor's nodes decreases the number of dropped packets in the network as more trusted paths are established to send packets through. In this regard, our approach provides the best results compared to nuglets and reputation approach.

4.2.5. Forwarding Own Packets

Figure 9 shows the number of packets generated by the nodes themselves. Observing the nuglets approach, we observe that this approach focuses on forwarding nodes generated by the nodes themselves. The reputation approach shows a lower number of forwarding of nodes own packets than the nuglets approach, which demon-

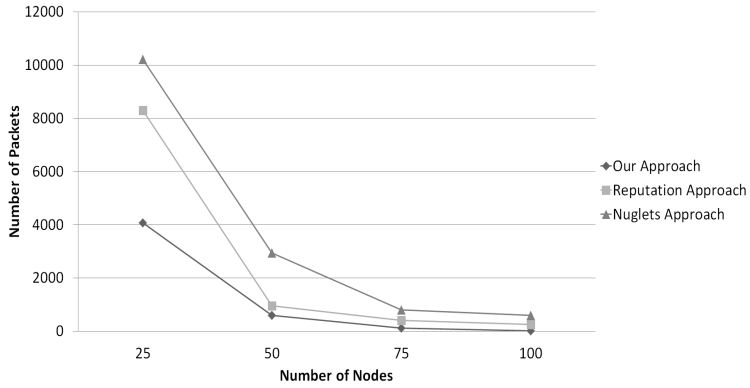

Figure 6. Dropped packets in different network sizes.

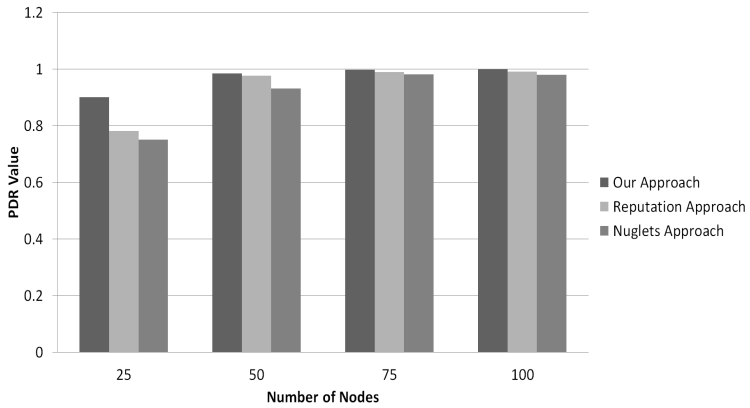

Figure 7. PDR values for different network sizes.

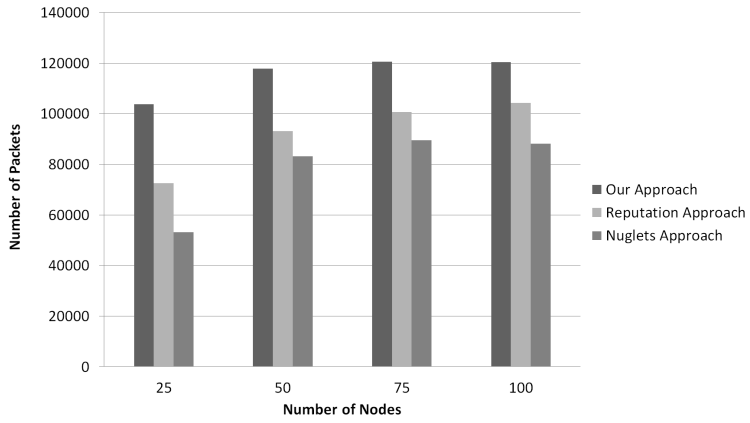

Figure 8. Packets forwarded toneighbors results.

strates a higher level of cooperation in the network with the reputation approach than with the nuglets approach. Our approach coerces the nodes to forward packets to neighbor nodes as a way to balance the energy in network's entirety, and also increases the number of nuglets in node's account. In our approach, the number of a node's own packet forwarding is the smallest. The forwarding of a node's own packets factor counteracts the previous factor (forwarding for neighbors packets). Once we have less number of a node's own packets generated, we achieve a higher collaboration in the network of the forwarding of packets to other nodes. The network lifetime is prolonged with the increase of the available trusted paths for communication, which are established through the focus on increasing the value of packet forwarding to neighbor nodes, rather than the forwarding a node's own packets, mitigating the "selfish" behavior in the network.

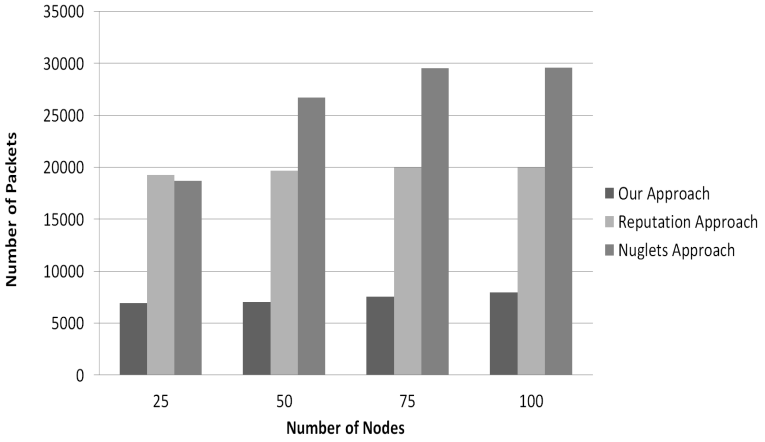

Figure 9. Node's own packet forwarding results.

5. Conclusions and Future Work

Wireless sensor network represents an important and raging topic in the field of research as a number of applications use sensors to collect and forward data from a source point to destination point (base stations) for data processing and decision making. In this paper, we proposed a new approach that is different from other approaches by using fuzzy logic to construct cooperation between nodes and prolong the network lifetime.

Simulation results based on different metrics show that our approach provides the best results over two well-known approaches, the nuglets approach and the reputation approach. Simulation results confirmed that we conserved the network energy, forced nodes into collaboration, and delivered the highest number of packets to their destinations.

It would be of a great addition to this paper to study the operation of the proposed approach on different routing protocols rather than LEACH, and to apply the proposed approach on ad hoc network nodes, which will be addressed in our next research.

References

[1] ANSI/IEEE Standard 802.11 (1999) Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Publication, Part 11.

[2] Sun, J.-Z. (2001) Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing. Info-Tech and Info-Net, China.

[3] Corson, S., Freebersyser, J. and Sastry, A. (1999) Mobile Networks and Applications (MONET). Special Issue on Mobile Ad Hoc Networking.

[4] Ito, Y., Mineno, H. and Ishihara, S. (2005) A Scheme Encouraging Mobile Nodes to Forward Packets via Multiple Wireless Links Aggregating System between the Internet and Mobile Ad Hoc Networks. Springer-Verlag, Berlin Heidelberg.

[5] Momani, M. and Challa, S. (2010) Survey of Trust Models in Different Network Domains. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **1**.

[6] Walter, J.P., Liang, Z., Shi, W. and Chaudhary, V. (2006) Wireless Sensor Network Security: A Survey. *Proceedings of Distributed, Grid, and Pervasive Computing*, CRC Press.

[7] McKnight, D.H. and Chervany, N.L. (1996) The Meanings of Trust. MIS Research Center, Carlson School of Management, University of Minnesota.

[8] Christh, R., Edwin, G. and Kusampudi, K. (2013) A Survey on Detecting Selfish Nodes in Wireless Sensor Networks Using Different Trust Methodologies. *IJEAT*, **2**.

[9] http://en.wikipedia.org/wiki/Fuzzy_logic

[10] Hu, J. (2005) Cooperation in Mobile Ad Hoc Networks. Technical Report, Computer Science Department, Florida State University.

[11] Jaydip, S. (2014) A Survey on Reputation and Trust-Based Systems for Wireless Communication Networks. Embedded Systems Research Group, Tata Consultancy Services, EPIP Industrial Estate, Bangalore, INDI.

[12] Ben Salem, N., Buttyán, L., Hubaux, J.P. and Jakobsson, M. (2003) A Charging and Rewarding Scheme for Packet Forwarding in Multi-Hop Cellular Networks. MobiHoc, USA.

[13] Mohan, M. and Joiner, L. (2004) Solving Billing Issues in Ad Hoc Networks. *Proceedings of the* 42*nd Annual South-east Regional Conference*, USA.

[14] Zhong, S., Chen, J. and Yang, Y.R. (2003) Sprite: A Simple, Cheatproof, Credit-Based System for Mobile Ad Hoc Networks. *IEEE Infocom* 03, USA.

[15] Buttyan, L. and Hubaux, J.P. (2003) Stimulating Cooperation in Self Organizing Mobile Ad Hoc Networks. *Journal of Mobile Networks and Applications*, **8**, 579-592. http://dx.doi.org/10.1023/A:1025146013151

[16] Zhang, J., Ci, S., Sharif, H. and Alahmad, M. (2009) A Battery-Aware Deployment Scheme for Cooperative Wireless Sensor Networks. GLOBECOM, USA.

[17] Gonzalez, J.M., Anwar, M. and Joshi, J.B.D. (2011) Trust-Based Approaches to Solve Routing Issues in Ad-Hoc Wireless Networks: A Survey. *IEEE* 10*th International Conference on Security and Privacy in Computing and Communications*, Changsha, 16-18 November 2011, 556-563.

[18] Rezazadeh, J., Moradi, M. and Ismail, A.S. (2011) Efficient Localization via Middle-Node Cooperation in Wireless Sensor Networks. *Proceedings of International Conference on Electrical, Control, and Computer Engineering*, Malaysia.

[19] Chhillar, P. and Smita, Ms. (2013) Implementation of SCFT Algorithm to Detect and Solve Greedy Nodes in Wireless Sensor Networks. *International Journal of Engineering and Computer Science*, **2**.

[20] Dimokas, N. and Katsaros, D. (2013) Detecting Energy-Efficient Central Nodes for Cooperative Caching in Wireless Sensor Networks. 27*th IEEE International Conference on* (*AINA*), USA.

[21] Mainaud, B., Gauthier, V. and Afifi, H. (2008) Cooperative Communication for Wireless Sensors Network: A Mac Protocol Solution. WD 08 1st IFIP, UAE.

[22] Buttyan, L. and Hubaux, J.-P. (2001) Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Ad Hoc Networks. Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne.

[23] Irfan, A., Peng, M. and Wang, W. (2007) Energy Efficient Cooperative Nodes Selection in Wireless Sensor Networks. *International Conference on Parallel Processing Workshops* (*ICPPW*), China.

[24] Pandana, C., Han, Z. and Liu, K.J.R. (2008) Cooperation Enforcement and Learning for Optimizing Packet Forwarding Probability in Autonomous Wireless Networks. *IEEE Transactions on Wireless Communications*, **7**, 3150-3163. http://dx.doi.org/10.1109/TWC.2008.070213

[25] Anderson, D.H. and Hall, L.O. (1999) MR. FIS: Mamdani Rule Style Fuzzy Inference System. *IEEE International Conference on Systems, Man, and Cybernetics*, Tokyo, 12-15 October 1999, 238-243.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.