# An Improved Trust Based Energy Efficient Routing Protocol for Wireless Sensor Networks

J. B. Shajilin Loret[1], T. Ganesh Kumar[2]

[1] Department of Information Technology, Francis Xavier Engineering College, India
[2] School of Computing Science and Engineering, Galgotias University, India
shajilinphd@gmail.com, tganeshphd@yahoo.com

## Abstract

Wireless Sensor Networks (WSNs) is emerged as a promising technology in wireless networks and is considered as an effective research area because of its wide scope of applications in networking. Wireless Sensor Networks are a form of self-organizing networks with limited energy and communication ability. The limited power batteries in sensor nodes, it is very difficult and expensive to extend network lifetime for wireless sensor networks. It is one of the main essential issues in WSNs is to use an energy efficient routing protocol to extend the network lifetime. In this paper, we propose an Improved Trust based Energy Efficient Routing Protocol (ITEERP) which includes energy efficiency in the network and trust is ensured in routing with minimal delay. The ITEERP is used for finding the optimal trusted path between the source and destination by using the weighted trust value of individual sensor node and cluster head. The periodic end-to-end trust evaluation is done between two SNs and between two CHs. Each SN is responsible to report its trust evaluation to other neighbor SNs, in the same cluster to its CH. An achieves a reliable secured data transmission in WSNs and also extends the network lifetime of a network.

**Keywords:** Wireless sensor networks, Routing algorithm, Energy efficient network

## 1 Introduction

Wireless Sensor Network (WSN) is an enormous collection of intelligent, low-power, and multifunctional sensor nodes which are connected to the base stations (BS) [1-2]. The huge number of nodes, less available data rates, and the resource constraints have restricted the usability of generic ad-hoc routing protocols in WSN. In order to increase the network lifespan and to overcome limited battery capacity, capacity, the routing protocols in WSN support the resource-awareness and adaptivity [3-5]. Now-a-days modern technological advances in Wireless Sensor Networks (WSN) have led to the emergence of tiny battery-powered sensors.

Hence, designing energy efficient routing protocols in WSN, which utilize the limited network resources is a key challenge to maximize the network lifetime. In wireless sensor networks, routing protocols can be categorized into three main types which include Flat-based routing protocols, Location-based routing protocols and Hierarchical-based routing protocols.

A flat routing architecture permits the sensor nodes to carry out identical roles in the routing process. Generally, the network is considered as homogeneous, in Flat-based routing i.e., the same random access wireless channel is shared by all the nodes in the network, therefore the status and ability of each node are identical. For this reason, all sensor nodes are set to forward the sensed packets directly to base stations. Some examples for Flat-based routing protocols include SPIN [6], DD [7], Rumor [8] etc.

In order to provide better network scalability and to reduce the overhead of flat sensor network architecture another one hierarchical architecture was proposed. This architecture segments the sensor nodes into clusters and the nodes are differentiated based on the tasks performed within each cluster. The size of the network, is a design paradigm to reduce the energy consumption because, with the help of hierarchy of network, it eliminates network-wide flooding for control information delivery and decreases the number of data transmissions [9]. In a two-layer hierarchy structure, low-level nodes also called as cluster members (CM) are liable for sensing data from the environment and also to forward the data to their respective cluster head (CH). Whereas the high-level nodes also called cluster heads are responsible for compressing and sending the collected data to the Base Stations (BS) [13]. Some example Hierarchical-based protocols include LEACH [10], TEEN [11], TTDD [12] and so on.

We propose a secured, low energy and clustering hierarchical routing algorithm named Improved Trust based Energy Efficient Routing Protocol (ITEERP) which includes energy efficiency in the network and

*Corresponding Author: J. B. Shajilin Loret; E-mail: shajilinphd@gmail.com
DOI: 10.53106/160792642021122207005

trust is ensured in routing with minimal delay. This achieves a reliable data transmission in WSNs and also extends the network lifetime of a network. ITEERP adopts a three-layer hierarchy structure to reduce the load on cluster heads and uses multi-hop transmission for intra-cluster communication. This paper evaluates ITEERP against other WSN routing protocols in terms of network performance with respect to changes in the network size. Simulation results show that ITEERP outperforms better in term of Trust computation, Throughput and Energy efficiency for large scale WSNs. Environment-fusion multipath routing protocol (EFMRP) to provide sustainable message forwarding service under harsh environments [22]. QoS-aware trust-based node-disjoint multipath routing mechanism between source node and destination node in two-layer clustered multimedia sensor networks [23]. K-Means clustering where the Frequent Pattern-growth (FP-growth) algorithm applied to each cluster [24].

## 2 Security Issues in WSNs

A wide variety of applications are used by the WSN and also to deploy them in real world environments, there is a need of efficient protocols and algorithms. In WSN, security is one of the significant factors. Generally, in the sensor networks, network layer attacks falls into one of the below mentioned categories [20].

(a) *Selective Forwarding attack :* In a selective forwarding attack, malicious nodes may attack WSN by simply dropping packages received or by refusing to forward messages.

(b) *Sinkhole Attacks:* In this, with respect to the routing algorithm, a malicious node attracts all the traffic from a particular area.

(c) *Wormholes:* In this attack, a malicious node to be found near the base station can tunnel messages over a low latency link and the traffic is completely interrupted.

(e) *HELLP Flood Attack*: In HELLP flood attacks, the attacker broadcast routing or other information with greater transmission power could convince every node in the network that the opponent is its neighbor. To provide security solutions to WSNs, Numerous techniques have been developed such as Intrusion Detection Systems (IDS), and secure routing protocols. Our work focuses on Trust based Energy Efficient Routing Protocol for WSNs.

## 3 Trust and Reputation Systems

Trust is a particular level of the subjective probability with which an agent will perform a particular action; the classification of Node trust models can be falls under two categories: Centralized and Distributed models. In Centralized trust models, to calculate trust values of sensor nodes, base station or a trusted intermediate node is used (indirect trust). But in distributed trust models, sensor nodes calculate trust values by themselves (Direct trust).

Usually, a trust and reputation model is composed of various components [14-15]: The primary component of a trust and reputation system called Gathering information which is liable for collecting behavioral information about other entities, for example peers, agents, or paths. The collected information might come from different sources [18]. It could be direct observation (direct trust) or information provided by peers (indirect trust). Once information about an entity has been properly combined and weighed, a reputation score is then computed. The primary objective is to provide the clients a quantifiable approach in order to decide which server node is most trustworthy. The second step is that a client selects the most trustworthy or reputable server entity, providing certain service and then effectively has an interaction with it. Once it receives the service provided, the client will access the result and give a score of satisfaction. With respect to the satisfaction obtained, the final step accepting and rejecting, is carried out. Two innovative trust and reputation models, namely BTRM-WSN [16], and Peer Trust [17] are discussed.

## 4 Proposed Method

The proposed Improved Trust based Energy Efficient Routing Protocol (ITEERP) is used for finding the optimal trusted path between the source and destination. These trusted paths were identified using the weighted trust value of individual sensor node and cluster head. The frequent peer-to-peer trust evaluation is done between two SNs and between two CHs. In the SN level, each SN is responsible to report its trust evaluation to other neighbor SNs in the same cluster to its CH which performs CH-to-SN trust evaluation towards all SNs in its cluster. Similarly a CH is responsible to report its trust evaluation towards other CHs in the network to the base station which performs station-to-CH trust evaluation towards all CHs in the system. This ITEERP is used to calculate the trust weighted value between the nodes and also the overall trust metric is generated by combining both direct and indirect method and can prevent security breaches more efficiently.

### 4.1 Network Modelling

In this paper, it is assumed that in network model all the sensor nodes are homogeneous and deployed randomly. Also the sensor nodes are categorized into clusters and the inter-cluster communications is managed by a Cluster-Head (CH). On the other hand the Cluster Members (CM) are responsible for sensing and collecting the data about a particular phenomenon.

Thus, a cluster-based WSN is used which consists of multiple clusters, and for each cluster, a cluster head (CH) and a number of Sensor Nodes (SN). The Figure 1 shows the network architecture.

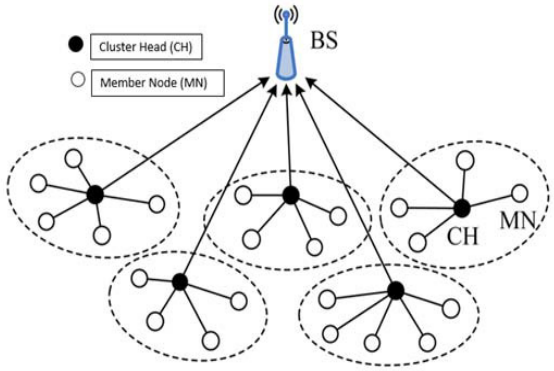


**Figure 1.** Network architecture

The network setting used is based on the assumptions which include

- Every base station and sensor nodes are stationary nodes.
- Each sensor nodes have the same resources and has a unique identifier.
- The communication link among any two nodes is identical.

These assumptions ensure an application-oriented reliability and set the scope of the network model in terms of node distribution, initial battery store, and mobility status.

The CH nodes in each cluster have more energy and resources than SN nodes. The CH in each cluster may be selected based on the balance energy consumption and its functionality. A SN in a cluster forwards its sensor reading to its CH through its neighbor nodes in the same cluster and thus the CH forwards the data to the base station or the destination node (or sink node) through other CHs.

## 4.2 ITEERP

The overall architecture of ITEERP is described in this section. When a source node wants to obtain the trust value of a destination node, both one hop trust model and multihop trust model is used. If the destination ID is within the cluster, direct trust model is used or else the indirect trust model is used. Trust can be defined as a confidence level that if a node can trust another node. Here the trust value is used to find whether a node is able to perform normally in WSNs. In this paper, the trust value is assumed to be in the range from 0 to 1 as in [19]. The node is completely trustworthy and considered if the trust value is between 0.6- 0.9 or 1, and the node can be avoided if it is between 0.1- 0.5 or 0. Direct trust can be calculated if a source node can communicate or transmit the data directly or without any intermediate nodes. Based on the recommendations from other neighboring nodes the indirect trust value is evaluated. The main properties of trust include residual energy, communication and data content as on [16] and [17]. Based on the above properties the probability of the trust value is calculated to find the path trust value.

In this paper **ITEERP** technique is used to find the available trusted paths between the source and the destination node. To calculate the trustworthiness of the nodes, in this paper the combination of both direct trust and indirect trust are used as in [18].

## 4.3 Methodology

### 4.3.1 Computation of Trust Value by Direct Trust

In Sensor Network, the nodes usually collaborate and communicate with sensor nodes and also with the cluster head to perform their tasks. Usually, all communications in the network will consume a certain amount of energy to transmit the information or the data packets. Hence, the trust value for data content, residual energy and communication are defined in ITEERP. In order to find whether the data transmitted have reached the destination without any alteration the data content is used. To measure if the node is proficient in performing its intended functions or not the residual energy is used and the communication is used to find whether the packets transmitted by a node have reached the destination correctly or the node is a selfish node, or replica node or malicious node. The trust values for the above properties using direct trust are computed as follows.

**A. Data Content**

The data content is evaluated based on the packet drop ratio [16]. Packet dropping is defined as the ratio between total numbers of packet lost to the total number of packets send. This can be derived using the Gaussian probability as follows

$$P_{dc} = \frac{1}{\sqrt{2\sigma^2\pi}} e^{-\frac{(d_i-\mu)^2}{2\sigma^2}} \quad \textbf{(1)}$$

Where $P_{dc}$ denotes the data content probability, $d_i$ indicates the packet delivery ratio of $i^{th}$ time and i varies between 1, 2, …, n. $\mu$ is mean (and also its median and mode). $\sigma$ is standard deviation and $\sigma^2$ is variance.

For each node the probability value is calculated and if the probability value is high that particular node is chosen and used for the path selection to transmit the data. Packet dropping ratio is low if the packet send by the source node is received correctly by the destination without any loss and has the high Packet dropping rate if the packet received by the destination is less.

Trust value for data content $\tau$ is computed as the probability of the difference in number of probability of packets dropped not occurring at time *t*. Thus the data trust is calculated by

$$\tau_{dc} = (1 - P_{dc}(t)) \quad \textbf{(2)}$$

**B. Residual Energy**

Every time when there is a data transmission takes place the residual energy of that particular node will be consumed. Then the probability value of remaining energy is calculated and from that the trust value is found which ranges between 0-1.

In general, an energy threshold $T_e$ is predefined for a sensor node as in [19] and it is compared with the probability of residual energy $p_r$. If the $p_r < T_e$, then due to insufficient energy the particular node is not considered for the path selection. The residual energy $p_r$ of a sensor node is considered to be in the range of 0-1. The residual energy $p_r$ is calculated based on the consumption energy rate $E_c$ of a sensor node, where $E_c \in [0, 1]$. It is defined as the difference between total energy of the node to the energy used by the node. The probability of residual energy is calculated by:

$$p_r = \frac{1}{\sqrt{2\sigma^2\pi}} e^{-\frac{(e_i-\mu)^2}{2\sigma^2}} \quad \textbf{(3)}$$

Where $e_i$ denotes the energy consumed of $i^{th}$ time and i varies between 1, 2, … n.

The trust value $\tau_{re}$ for residual energy can be computed as the probability of the difference in the probability of energy consumed not occurring at time *t*. It is calculated by

$$\tau_{re} = (1 - p_r(t)) \quad \textbf{(4)}$$

**C. Communication Trust**

Communication trust $C_t$ is a significant parameter to calculate the trust value of a sensor node. Communication $C_t$ is defined in a way such that if the numbers of packets send by a source node has reached the destination correctly without any packet loss. Packet Delivery Ratio (PDR) is defined as the ratio between total numbers of packet received to the total number of packet send.

Thus PDR is evaluated as

$$C_t = \frac{1}{\sqrt{2\sigma^2\pi}} e^{-\frac{(d_{r_i}-\mu)^2}{2\sigma^2}} \quad \textbf{(5)}$$

Where $C_t$ denotes the communication trust based on the packet delivery ratio, $d_{r_i}$ is the number of packet received in $i^{th}$ period and i ranges between 1,2,…n. Therefore the trust value for the communication is considered as probability of the difference in the probability of packet received not occurring at time *t*. It is calculated by

$$\tau_{ct} = (1 - C_t(t)) \quad \textbf{(6)}$$

**Algorithm 1.** Trust Calculation Algorithm

Input : Source node A, Dest Node B
Output: Trust Value T

**Step 1:** Source node A Find the List of Neighbours $N_i$ . in the cluster

**Step 2**: the Id of dest node B is checked in List of Neighbours $N_i$ in the cluster by A,

**Step 3:** if the dest node B is in the list $N_i$, Source node A and dest B have direct communication.

**Step4:** (a) Calculate Data trust by means of Packet Dropping Ratio by Gaussian probability as eqn (1) and the trust value is evaluated as $\tau_{dc} = (1 - P_{dc}(t))$

(b) Probability of Residual Energy is evaluated by eqn (3) and the trust value is evaluated as $\tau_{re} = (1 - p_r(t))$

(c) Communication trust probability is calculated using Packet Delivery Ratio as in eqn 5 and the trust value is computed as $\tau_{ct} = (1 - C_t(t))$

**Step 5:** If the dest node B is not in the list $N_i$, it will check for the other clusters and the Source node A and dest B have indirect communication. ie. A should get the information from other cluster heads.

**Step 6:** tore the Trust Value T

#### 4.3.2 Weighted Trust Value Calculation by Direct Trust

To find the trust value for every path, the weighted trust value for the individual sensor node is identified. The weighted value for each individual node using direct trust $T_{wd}$ is calculated by the summation of all the parameters such as data content, residual energy and communication trust. The weighted trust value for direct trust $T_{wd}$ of a single node is derived as follows

$$T_{wd} = \Sigma P_{dc} + P_r + C_t \quad \textbf{(7)}$$

Where $T_{wd}$ is the weighted trust value for direct trust, $P_{dc}$ denotes the probability of data content, $p_r$ indicates the probability of residual energy, $C_t$ denotes the communication trust based on the packet delivery ratio.

#### 4.3.3 Weighted Trust Value Calculation by Indirect Trust

In this paper, to calculate the probability trust value using indirect trust, Dempster-Shafer theory is used for each individual node as the concept in [19]. The belief function is the main part and is based on two fundamental ideas which include degrees of belief about a proposition. This can be obtained from subjective probabilities, and these degrees of belief can

be combined together on condition that they are from independence evidence [20-21].

The probability trust value for indirect trust is evaluated by means of this belief function and by combining the rule of belief; we can combine more results from neighbor nodes. Based on the Dempster-Shafer theory $K_{DS}$ is defined as:

$$KD_s = x_{n1}(T) + x_{n2}(T) + x_{n3}(T) + \cdots\cdots\cdots\cdots + x_{ni}(T) \quad \textbf{(8)}$$

Where node $n1 \leq x \leq n$, is an one-hop neighbor of node *S* and node *D*.

The same process is used for indirect trust $I_t$ to find the weighted trust value. It can be derived as follows

$$ID_t = KD_s \quad \textbf{(9)}$$

Where $ID_t$ is the weighted trust value for is indirect trust, and $K_{DS}$ is the probability of summation of all the one hop neighbor nodes. This process can be repeated for all the available sensor nodes in each cluster in the network. After the calculation of weighted trust value of individual nodes by both direct and indirect trust the average weighted trust value can be calculated.

**Average Weighted value**

Based on the node weighted trust value, the average weighted trust value for a single path for both direct and indirect trust can be computed as follows

$$A_{wt} = \frac{1}{N}\sum_{i=1}^{N} T_{wd} + ID_t \quad \textbf{(10)}$$

Where $A_{wt}$ is the average weighted trust value for a single path, $T_{wd}$ is the weighted trust value of direct trust for a single node, $ID_t$ is the weighted trust value of indirect trust for a single node and N is the number of available paths,. Thus the average path trust value is identified by means of this equation and this technique is used to decide whether the particular path can be selected for data transmission or not.

## 5 Performance Analysis

In order to examine the performance of the proposed **ITEERP,** we implemented our proposed system in Network Simulator (NS2). The proposed IEESRP system is compared with PEGASIS, ECRA, LEACH, EBTRM. The parameters used in the simulation experiments are listed in the below Table 1.

Several performance metrics are considered for analyzing the performance the proposed method such as Energy Consumption, Packet Delivery Ratio, Trust Value Computation and Average Throughput.

**Table 1.** Simulation parameters

| Parameters | Value |
|---|---|
| No of Nodes | 100-300 |
| Topology size | 400 x 400 |
| Simulation Duration | 500 sec |
| Packet Size | 400 bytes |
| Initial energy | 1 joules |
| Packet Interval | 2 |
| Communication Range | 30 m |

### 5.1 Energy Consumption

Energy consumption is defined as the consumption of power or energy. Normally while increasing the number of nodes the utilization of energy is also high. Thus our proposed system consumes less energy when compared with the existing protocols. The energy consumption graph is shown below in Figure 2.

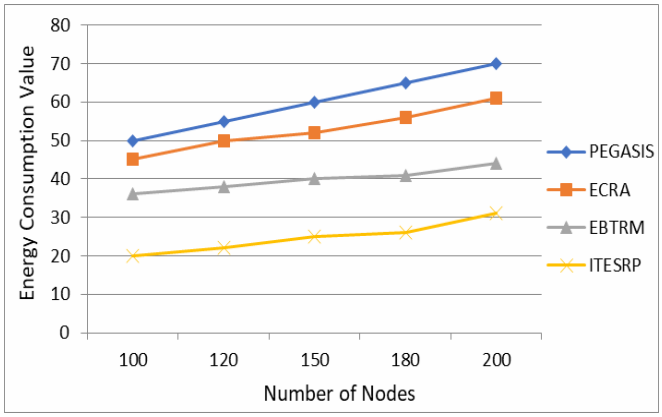


**Figure 2.** Performance analysis of energy consumption

From the Figure 2, it is analyzed that, there is a gradual increase in the energy consumption when the number of nodes in the network increases. However, when it is compared with the existing protocol the energy consumption is less and it gives better result.

### 5.2 Packet Delivery Ratio (PDR)

In order to analyze the performance of the network based on delivered packets Packet Delivery Ratio is an important metric. PDR is defined as the relation between the numbers of correctly delivered packets from the total numbers of packets available.

Packet Delivery Ratio,

$$PDR = \frac{N_{dp}}{N_{ap}} \quad \textbf{(11)}$$

Where $N_{dp}$ the total numbers of delivered packets is, $N_{ap}$ is the total numbers of packets available. The comparison analysis graph of existing methodologies based on the network size is shown in the Figure 3.

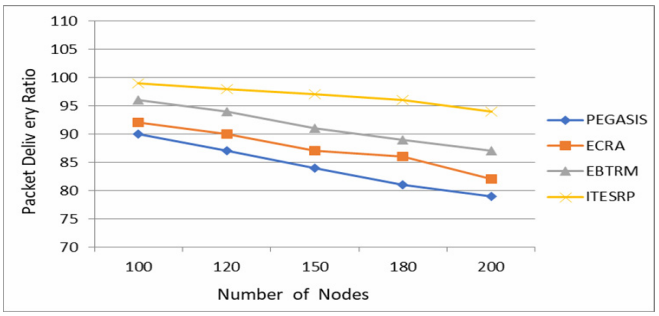


**Figure 3.** Performance analysis of packet delivery ratio

From the Figure 3, it is analyzed that, **ITEERP** has the better packet delivery ratio when compared with other protocols. But it has the finer result with minimum number of nodes.

## 5.3 Computation of Trust Value

Computation of Trust value can be done based on the number of received packets. The variation among the number of packets sent to number of received packets can be observed easily. These variations may be cause by alteration of packets, addition of packets, and packet loss. The probability value of packets that has been altered, added and missed can be derived as

$$T_r = \frac{p_{rp}}{P_{tp}} \tag{12}$$

Where $P_{rp}$ is the remaining packets and is defined as $P_r = P_s - P_r$, $P_s$ is the number of packets send, $P_r$ is the number of received packets and $P_{tp}$ is the total packets. The performance analysis graph for the computation of trust value shown in the Figure 4.

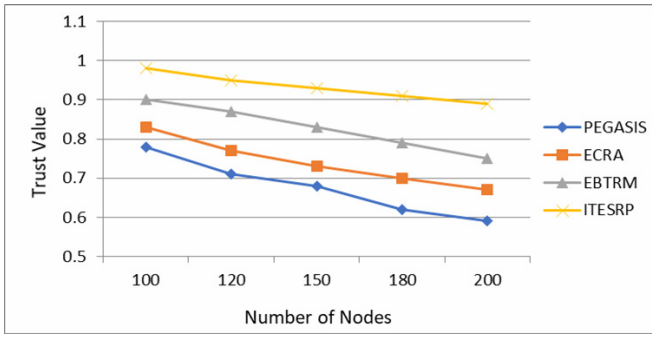


**Figure 4.** Performance analysis of trust value computation

It is observed from the Figure 4 that, there is a progressive decrease in the trust value of the node when there is an increase in number of nodes. Thus our proposed system gives better results with high trust value when it is compared with the other existing protocols.

## 5.4 Average Throughput (AT)

One of the main important performance metrics is Average throughput. AT is the average successful message delivery rate over a communication channel. Generally, the average throughput will be high for the best system when the number of nodes increases. This metric is considered to analyze the performance of our proposed system by increasing the number of nodes. Here the throughput is calculated by using the below formula

$$T_{avg} = \frac{s_p}{T_p} \tag{13}$$

Where $S_p$ denotes the total number of packets successfully transmitted and $T_p$ is the total number of packets. The comparison analysis graph of the existing protocols with the proposed is shown in Figure 5.

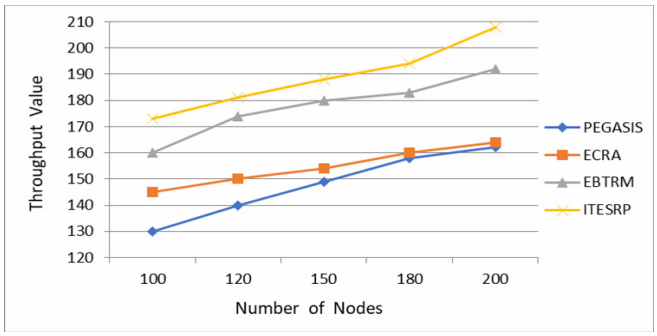


Figure 5. Performance analysis of energy consumption

From the Figure 5, it is examined that the throughput value of the proposed method is increased while there is an increase in number of nodes when compared with other methods. Also the proposed scheme gives better results when the number of nodes in the network increases.

# 6 Conclusions

In WSN, an efficient trust model is essential for handling the trust related information in a secure and reliable way. In this paper, we proposed an Improved Trust based Energy Efficient Routing Protocol (ITEERP) which improves the security in path selection by integrating both direct as well as indirect trust. The trust weighted value between the nodes and also the overall trust metric is calculated. The Simulation results show that ITEERP outperform well by achieving a reliable secured data transmission in WSNs and also the network lifetime of a network is extended. Our proposed protocol is compared with other similar trust models such as PEGASIS, ECRA, LEACH, EBTRM and gives better results by considering the parameters such as Energy consumption, PDR, Trust value computation and Average throughput.

## References


[1] X. Liu, Atypical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review, *IEEE Sensors Journal*, Vol. 15, No. 10, pp. 5372-5383, October, 2015.

[2] C. Gherbi, Z. Aliouat, M. Benmohammed, A Survey on Clustering Routing Protocols In Wireless Sensor Networks, *Sensor Review*, Vol. 37, No. 1, pp. 12-25, January, 2017.

[3] M. R. Mundada, S. Kiran, S. Khobanna, R. N. Varsha, S. A. George, A Study on Energy Efficient Routing Protocols in Wireless Sensor Networks, *International Journal of Distributed Parallel System*, Vol. 3, No. 3, pp. 311-330, May, 2012.

[4] Y. Sun, W. Dong, Y. Chen, An Improved Routing Algorithm Based on Ant Colony Optimization in Wireless Sensor Networks, *IEEE Communications Letters*, Vol. 21, No. 6, pp. 1317-1320, June, 2017.

[5] A. Al-Baz, A. El-Sayed, A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks, *International Journal of Communication System*, Vol. 31, No. 1, Article No. e3407, January, 2018.

[6] J. Kulik, W. Heinzelman, H. Balakrishnan, Negotiation-based protocols for disseminating information in wireless sensor networks, *Wireless Networks*, Vol. 8, No. 2-3, pp. 169-185, March, 2002.

[7] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, Directed diffusion for wireless sensor networking, *IEEE/ACM Transactions on Networking*, Vol. 11, No. 1, pp. 2-16, February, 2003.

[8] D. Braginsky, D. Estrin, Rumor routing algorithm for sensor networks, *Proceeding of the 1st ACM International workshop on wireless sensor networks and applications*, Atlanta, Georgia, USA, 2002, pp. 22-31.

[9] W. Choi, P. Shah, S. K. Das, A Framework for Energy-Saving Data Gathering Using Two-Phase Clustering in Wireless Sensor Networks, *Proceeding of the International Conference on Mobile and Ubiquitous Systems: Networking and Service (MOBIQUITOUS)*, Boston, MA, USA, 2004, pp. 203- 212.

[10] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, *Proceeding of the 33rd Annual Hawaii International Conference on System Sciences*, Maui, HI, USA, 2000, pp. 1-10.

[11] A. Manjeshwar, D. P. Agrawal, TEEN: A routing protocol for enhanced efficiency in wireless sensor networks, *Proceeding of the 15th International Parallel and Distributed Processing Symposium*, San Francisco, CA, USA, 2001, pp. 2009-2015.

[12] F. Ye, H. Luo, J. Cheng, S. Lu, L. Zhang, A two-tier data dissemination model for large-scale wireless sensor networks, *Proceeding of the 8th Annual International Conference on Mobile Computing and Networking*, Atlanta, Georgia, USA, 2002, pp. 148-159.

[13] S. K. Singh, P. Kumar, J. P. Singh, A Survey on Successors of LEACH Protocol, *IEEE Access*, Vol. 5, pp. 4298-4328, February, 2017.

[14] S. Marti, H. Garcia-Molina, Taxonomy of Trust: Categorizing P2P Reputation Systems, *Computer Networks*, Vol. 50, No. 4, pp. 472-484, March, 2006.

[15] F. G. Mármol, G. M. Pérez, Towards Pre-Standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems, *Computer Standards and Interfaces*, Vol. 32, No. 4, pp. 185-196, June, 2010.

[16] F. G. Mármol, G. M. Pérez, Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique, *Telecommunication Systems*, Vol. 46, No. 2 pp. 163-180, February, 2011.

[17] L. Xiong, L. Liu, PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16, No. 7, pp. 843-857, July, 2004.

[18] M. Dorigo, M. Birattari, T. Stutzle, Ant Colony Optimization, *IEEE Computational Intelligence Magazine*, Vol. 1, No. 4, pp. 28-39, November, 2006.

[19] Z. Wei, H. Tang, F. R. Yu, M. Wang, P. Mason, Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning, in *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 9, pp. 4647-4658, November, 2014.

[20] G. Shafer, J. Pearl, *Readings in Uncertain Reasoning*, Morgan Kaufmann, 1990.

[21] T. M. Chenand, V. Venkataramanan, Dempster-Shafer theory for intrusion detection in ad hoc networks, *IEEE Internet Computing*, Vol. 9, No. 6, pp. 35-41, November-December, 2005.

[22] X. Fu, G. Fortino, P. Pace, G. Aloi, W. Li, Environment-fusion multipath routing protocol for wireless sensor networks, *Information Fusion*, Vol. 53, pp. 4-19, January, 2020.

[23] Q. Ye, Y. Wang, Y. Tang, J. Lv, Y. Zhang, A Node-disjoint Trust-based Multipath Routing Mechanism for Multimedia Sensor Networks, *Journal of Internet Technology*, Vol. 22, No. 1, pp. 219-228, January, 2021.

[24] M. Zhu, X. Xia, J. Zhang, D. Zhang, A Clustering Approach Using Enhanced K-Means in 5G Networks, *Journal of Internet Technology*, Vol. 21, No. 7, pp. 1885-1892, December, 2020.


## Biographies

**J. B. Shajilin Loret** works as Associate Professor at the Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, India. She received her BTech degree in Information Technology from Anna University Chennai and MTech degree under Manonmaniam Sundaranar University. She has completed her research in Wireless Mesh Network at Anna University Chennai. She has published many Indian Patents. She has published many SCI and Scopus Indexed Journals. Her

area of interest includes Network Security, Medical Imaging and Wireless Networks.

**T. Ganesh Kumar** received his Master of Engineering in Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, India. He has completed Fulltime PhD in Computer Science and Engineering in Department of Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli in the year of 2016. Currently He is working as an Associate Professor in School of Computing Science & Engineering, Galgotias University, Greater Noida, Delhi NCR, India. He has published many SCI and Scopus Indexed Journals. He has published many Indian patents and international patents. His area of interest includes Computer Networks, Remote Sensing and Medical Imaging.