FEBSRA: Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm for Secured Communications in WSNs

Anitha R
S A Engineering College
Tapas Bapu B R (tapasbabu1885@gmail.com)
S A Engineering College
Kuppusamy P G
Siddharth Institute of Engineering and Technology
Partheeban N
Galgotias University
Sasikumar A N
Panimalar Engineering College

Research Article

Keywords: Energy Efficiency, Delay, Wireless Sensor Networks, Security, Trust, Fuzzy Logic and Routing

Posted Date: April 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-347272/v1

FEBSRA: Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm for Secured Communications in WSNs

R. Anitha[1], Dr. B. R. Tapas Bapu[2,*], P. G. Kuppusamy[3], N. Partheeban[4], A. N. Sasikumar[5]

Abstract – Energy efficiency is playing major role in the design of a sensor network for improving the network lifetime and the trust is also important for providing the security to the data communication process. Delay is also major challenge today due to the enormous volume of network users. For overcoming all these issues, many researchers have been developed energy efficient security mechanisms for fulfilling the requirements. Even though, they are not able to satisfy the current requirements and users in terms of energy consumption, delay and security. For this purpose, this paper propose a new algorithm called Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) which is able to provide the effective delay constrained secured routing algorithm which uses the fuzzy logic is a form of many-valued logic in which the truth values of variables may be any real number between 0 and 1 both inclusive for making final decision over sensor nodes with the consideration of number of hops between the source and destination nodes, energy level of the nodes and the trust scores. Moreover, a new trust model is also introduced new formulae for calculating the trust scores with the consideration of energy level of the communication delay which is calculated by using number of hops used for the specific communication. The experimental results of the proposed secured routing algorithm demonstrated that the performance in terms of energy consumption, less delay and high throughput with security is better when compared to the existing systems.

Keywords: Energy Efficiency, Delay, Wireless Sensor Networks, Security, Trust, Fuzzy Logic and Routing.

1. Introduction

In the recent years, the Wireless Sensor Networks (WSNs) have achieved reasonable appreciation in our life. The majority of applications use different sensors to provide society with sophisticated facilities. In this scenario, the secure routing algorithms used to ensure the secure data communication and safeguard the WSN and also that maintained the performance in terms of network life time (Younis et al 2004). Moreover, the majority of secure routing algorithms use the cryptography algorithms for exchanging the data between the nodes and authentication schemes that are not suitable for WSN. Here, the misbehaviour of each sensor nodes is assumed that the participating sensor nodes are cooperative and also trustworthiness. Therefore, this assumption are not reliable for the inner attacks or the node misbehaviour attacks (Danyang et al 2017). Usually, all these traditional security mechanisms required a single administration for managing the security that is not available for ad-hoc networks.

Mrs. R. Anitha

Assistant Professor Department of Computer Applications
S. A. Engineering College,
annithar1985@gmail.com
Corresponding Author: Dr. B. R. Tapas Bapu
Professor, Department of Electronics & Communication Engineering,
S. A. Engineering College,
Correspondence email: tapasbabu1987@gmail.com
P. G. Kuppusamy
Professor Department of Electronics & Communication Engineering, S A Engineering College,
nagarajuvr1987@gmail.com
N. Partheeban
Computer Science and Engineering , Galgotias university , India.
pradeepsp1970@gmail.com
A. N. Sasikumar
Computer Science and Engineering, Panimalar Engineering College, Chennai.
Saankumar34@gmail.com

Moreover, the available network security mechanisms are not able to satisfy the user's requirements in terms of high computation, memory occupation and the energy consumption that limit the system implementation in resource limited sensor nodes (Trong-Thua et al 2016).
Energy is an important resource for the sensor oriented networks in a effective communications with delay. For this purpose, many energy aware routing algorithms have been developed by many researchers for the effective data communications in WSN (Logambigai et al 2018). However, many sensors based applications in the position to transmit the data with very less time from the source node to destination node. So, the main objective to provide better service in wireless sensor networks is to minimize the energy consumption and the communication delay between the nodes. Clustering process is a method which is used effectively for achieving the energy efficiency over the sensor networks. In clustering process, the sensor nodes select themselves as cluster head that is according to the probability values. The optimized cluster-head values are known as probability value. In WSNs, a sensor only able to contact with other sensors that are presence in the network topology within the limited frequency range. Here, the sensor must form a multi-hop network for communicating between two sensors of the network. When the WSN uses a clustering algorithm, every cluster must have Cluster Head (CH) individually and it used to collect all of the sensing data from CHs and it also used to transfer the data to the specific destination. Moreover, the communication between the CH and destination consumes more energy than usual when their distance is far. Here, the energy consumption is exponential to the distance (Heinzelman et al 2002) so that it minimizes the delay. Generally, the multi-hop communication is energy efficient but it increases the communication delay (Ahmed et al 2016).
Generally, the trust is a belief of the sincerity on each other Rathore et al (2016). The trust score of the particular node is used to identify the right node for transferring the data between the nodes in a network environment. Trust management technique is a right and easy way to solve the security issues that are available in the networks. Recently, trust based routing mechanism is widely used for secured communications in wireless networks by various researchers for monitoring the nodes behaviours in the network scenario in different time and situation. According to the changes of nodes behaviours the genuineness of the nodes are to be finalized and also finalized the data security without applying any cryptographic algorithms. Trust score is considered as a reliability level of the node in wireless network communications. The trust based mechanisms provides the facility to predict the future movement of the participating nodes in the network according to their earlier activities that are observed by the admin and it also used for making effective decisions for identifying the malicious nodes among the participating nodes in the network topology. Moreover, the trust based routing algorithms are achieving better performance in terms of energy consumption, delay and security than other techniques (Trong-Thua et al 2016). Even though, the presence of layers in the sensor node not able to supply a holistic security algorithm for detecting all types of attacks in a network.

However, the trust based routing algorithms are not able to ensure the security of multi-hop communications fully due to the trust can handle inherent attacks and they are failed to predict new attacks, trust score only considered for the data transmission and failed to care the standard quality of service metrics such as energy, distance and number of hops. Finally, most of the trust based routing algorithm uses existing routing algorithms only. All these reasons, the existing trust based routing algorithms are not able to achieve better performance. This paper introduces a new Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) that is able to resolve the communication overhead and multi-hop communication issues. The proposed FEBSRA is able to improve the security level of the network and ensure the data security over the multi-hop communication based network. Moreover, it reduces the communication delay and communication overhead. In addition, it considered the traditional QoS metrics and also take care of new attacks that are to be occurred in future with the help of the dynamic trust scores and also generating the new types of fuzzy rules that are able to check the nodes genuineness in terms of all the properties.

Rest of this paper is organized as follows: Section 2 discusses in detail about the related works of the proposed model such as wireless sensor networks, multi-hop communication, trust based routing, energy efficiency and delay. Section 3 provides the overall architecture of the proposed system. Section 4 shows the better explanation of proposed FEBSRA and provides the sufficient explanation too. Section 5 demonstrated that the efficiency of the proposed FEBSRA through the various experiments that are focused in the metrics such as energy efficiency, communication delay, communication overhead and the security. The paper presented the conclusion of the FEBSRA with highlighting the achievement and the future directions in Section 6.

2. Literature Survey

There are many works have been done in this direction of Wireless Sensor Networks, Secure Routing, Energy Efficient Routing, Clustering, Multi-hop routing and Trust by the various researchers in the past. Among them, Liangy in et al (2014) demonstrated that the $(n + 1)^{th}$ hop anchor neighbours that are more useful when it is compared with the n^{th}-hop anchor neighbours for performing localisation which is range-free in WSNs. Moreover, their model mentioned that the localisation accuracy which is not able to be unlimitedly enhanced with increasing of hop counts. In practically, the hop count 'n' is a set between 2 and 4 based on the real scenarios to the desired accuracy of localisation. Adnan et al (2015) propose a new trust and energy-conscious routing protocol (TERP) to boost protection for WSN in the presence of several malicious and unreliable nodes. TERP focuses on two crucial trustworthiness and energy efficiency considerations that are most important to WSN 's survival in hostile environments and intense attacks. TERP guides the sensor nodes through the shortest paths to forward packets consisting of trusted and energy-efficient nodes that result in balancing energy consumption between trusted nodes. The weights implemented in trust estimation and in composite routing metric allow for versatile adjustment and configuration, fine algorithm tuning and trade off between different parameters. The combined trust and energy management principle allows TERP to keep records of participating nodes' trustworthiness and energy levels. This multifaceted strategy helps pick a safe and energy-efficient route that is essential to WSN's lifetime network. The results of the simulation show better TERP efficiency as opposed to current schemes.

Trong et al (2015) presented a model called a wake-up variation reduction PM for resolving the wireless networks issues. Their model applied for the wireless sensor nodes that are powered by a sequence and the periodic energy source over a constant cycle of whole day. Their model is not only follows ENO condition and it is also reducing the wake-up interval variations of the wireless sensor nodes. Ahmed et al (2016) presented a new low-cost localization algorithm that accounts for the heterogeneous nature of the wireless sensor networks. Moreover, their algorithm is able to locate the wireless sensor nodes which owning accurately for a new low-cost implementation which avoids any other additional energy consumption. Moreover, a correction method that complies with the heterogeneous nature of wireless sensor nodes that has been developed for improving localization further accurately without incurring any other additional costs. Their model performed well than other models in the direction of energy efficient communications.

Slim et al (2016) developed a new localization algorithm that exploits that in addition to that the hop-based information. Moreover, the average location estimation between the two different anchor nodes of the network topology that has been derived in the closed form and it also compared. They have shown the performance of the proposed model by conducting the experiments in terms of accuracy. Moreover, they have proved that confirms the unambiguousness with higher accuracy. Ganapathy et al (2012) presented a new classifier which uses the clustering algorithm that perform clustering process by using K-Means clustering along with Minkowski distance measurement formula and achieved better performance. Trong et al (2016) developed a new clustering technique which is working distributed in nature for determining the best cluster-head for all clusters in wireless sensor networks for reducing the energy consumption level and the communication delay between the nodes. In their technique, they have introduced a new cost effective function which is used to perform inter-cluster multi-hop routing process according to the new clustering technique. Since, they have proposed a multi-hop routing process between any two CHs to the base station with less energy conservation which is based on the communication delay. Moreover, they have conducted various experiments for the comparative analysis and also identified the optimal parameter values to the trade-off from power consumption and the communication delay between the nodes in the particular size of network topology.

Danyang et al (2017) presented a new trust sensing based secure routing mechanism with the lightweight of features and the capability of resisting many general types of intrusions simultaneously. In addition, they optimized the route selection process by considering the trust level and the quality of service metrics into account. They have improved the security level and the overall efficiency of the WSN. Muthu rajkumar et al (2017) presented an intelligent secured and energy efficient routing algorithm for mobile ad-hoc networks. They have applied intelligence for making decision over the routing process. Selvi et al (2017) developed a rule based energy efficient method which is delay constrained for effective routing and data communication in WSN. They have applied effective rules that are developed based on the delay and energy level of the sensor nodes. Their experimental results proved that their effectiveness of WSN in terms of less delay.

Xiaofeng et al (2017) presented a multi-hop connected clustering problem for the particular wireless network which is a homogenous network that is formed as finding a minimum d-hop connected dominating set problem for a given graph. Moreover, they have proposed a

distributed approximation algorithm named Connected Sparse Clustering Scheme for resolving the issue. Moreover, their system consists of three stages such as dominator selection stage, connector insertion stage and the redundancy elimination stage. Their experimental results achieved that the better performance than the existing works that are available in this direction. Thangaramya et al (2017) presented a new and energy efficient clustering approach using spectral graph theory in WSNs. They have used a spectral graph theory for making decision over the clustering process in the proposed model.

Boyun and Donghui (2018) categorized the wireless sensor network threats into two types and also analysed that the defensive capacity of trust aware secure routing models that are introduced by various researchers in the past for identifying and detecting the various types of malicious attacks. Moreover, they have proposed a new trust based routing algorithm which is robust with the consideration of multi valued attributes according to the communication overhead, the data overhead, energy level, and the recommendation for assisting the wireless sensor nodes in the process of establishing the reliable routes while designing the sliding window time method which combines with attack frequency detection and it also have applied for identifying the attackers with the adjustable attack frequency. Their experimental results show the wireless network which deployed the proposed model that achieved better performance over the different routing paths or for aiming to detect various attacks. Logambigai et al (2018) presented a new routing algorithm called Energy Efficient Grid based routing algorithm that uses intelligent fuzzy rules. They have achieved better performance in terms of energy efficiency.

Xiao et al (2018) presented a new trust based scheme for improving the data packet arrival ratio. In their method, abstract information of the data packet which is transmitted to the sink node when the source nodes transfer a data packet into the sink node. In this model, the malicious nodes are dropping the data packets but the abstract of the data packet is received from the source node and it received by the sink nodes. In this scenario, the sink node knows the route and the malicious node location and the sink node reduces its evaluation trust score of the node in the specific route. End of many data packets transmission, the participating nodes of the networks will contact each other. Now, the malicious nodes have been identified according to the nodes trust values and declared as malicious nodes. This method has been achieved better performance in terms of security. Philip et al (2018) presented and explained that a newly developed decentralized trust management scheme for filtering out the malicious nodes over the delay tolerant networks. In their method, the acknowledgement for the successful transformation is merged that the energy level of the nodes that are used to formulate the direct trust. Then, the recommendation score is calculated from the indirect trust score, the recommendation credentials and the recommendation familiarity. The recommendation credentials increase the overall trust score by filtering out the dishonest recommendations. They have compared their new model with the cooperative watchdog method which is a recommendation score based model. The experimental results of their model handling the malicious behaviour nodes effectively in delay tolerant networks including all the trust based attacks.

Yaw-Wen et al (2018) designed a new IoT based system which is useful for the wide area and the various heterogeneous applications. Their system is capable of controlling the timing errors and it permit us for relaxing the synchronize time period that is used to reduce the wasted energy in WSNs. Their system is able to increase the efficiency of the protocol. Moreover, it is able to accommodate the sensor nodes which have high throughput and rate. The experimental results of their system that have been implemented and evaluated their system special characteristics and it also creates a secured connection with the database over the Internet. Yimei and Yao (2018) designed a new compressed sensing method that is able to recover the sensing data at the destination node with the high delight when the situation arises to collect very less number of data packets that leads to reduce the network transmission time and enhance the network lifetime. Moreover, their method is efficient and easy to implement over the resource limited motes that are used to store any part of the random projection matrix. In addition, a new systematic approach by applying machine learning algorithms for finding a suitable representation in WSNs. Finally, they have validated their approach and also evaluated the performance by applying real time and outdoor multi-hop sensor networks. They have achieved the better performance than other existing systems in terms of reducing the data recovery errors and wireless communication costs.

Farhad et al (2018) introduced two new network methods that are used to manage the trust in static and distributed environment of WSNs. Their methods are capable of adopting the logic for generating and adjusting the trust scores for each node in WSN based on node observations. Moreover, it exploits the spatio-temporal related information that exists in the sensed data in wireless sensor networks by deploying a sliding window concept. Moreover, their method uses the location and data of each node that is used to find the trust score for

each node in the network. Their experiments show the efficiency of their system in terms of detection rate with high reliability and energy conservation. Shilpa and Sangeeta (2018) proposed a new hybrid data aggregation model which deploys the optimal number of hops. Moreover, their system improved the effectiveness of finding the routes with optimal number of hops for the possible routes from the source node to the destination node. Their system performance is proved that in terms of energy consumption and also compared with the individual other data aggregation schemes that are available in the literature by conducting the experiments. Zengwei et al (2019) proposed a new Hybrid Particle Swarm Optimization with Genetic Algorithm (HPSOGA) for resolving the NP-Hard problem. They have conducted many experiments which proved that the periodic charging planning is able to avoid the node deaths and also keeps the energy level of the wireless sensor nodes that are varying periodically. Their hybrid approach performed well than the Genetic Algorithm (GA) and Particle Swarm Optimization (PSO).

3. System Architecture

The overall architecture of the proposed Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) is given in figure 1. The proposed FEBSRA structure consists of ten important components such as sensor nodes, data collection module, energy efficient model, energy manager, trust model, routing model, clustering model, decision manager, rule manager, and knowledge base.

Sensor Nodes: The collections of nodes are to be considered for collecting the necessary details such as nodes energy level and the trust score.

Data collection Module: The data collection module is used to collect the necessary information that is available in the sensor nodes. The collected information is forwarded into the decision manager.

Energy Model: The energy model is responsible for managing the energy according to the requirement that uses standard energy formulae to compute the energy efficiency over the WSNs.

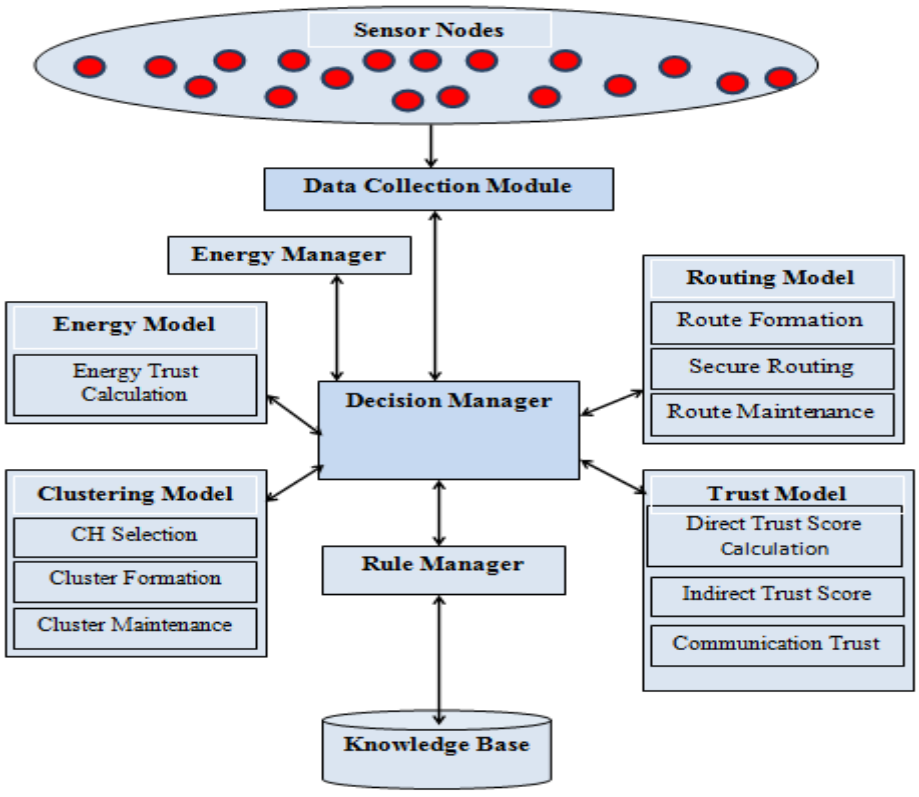

Fig.1. Overall System Architecture

Energy Manager: It is responsible for managing the energy level. The necessary information is forwarded into the energy model through the decision manager and it use for making effective decision over the energy balancing process.

Trust Model: This model consists of three sub components such as trust score calculation, communication cost and dynamic trust score. In trust score calculation, the suitable formulae are used for calculating the trust score which calculation is based on the direct trust, indirect trust and the reputation score. In communication cost, the communication cost is calculated according to the time taken for communicating a message between the nodes. In dynamic trust score calculation, dynamically trust scores are to be calculated for all the participated sensor nodes. For these purpose, three different formulae are introduced in this paper.

Routing Model: This routing model consists of three sub components such as route formation, secure routing process and the route maintenance. Here, a newly proposed FEBSRA is deployed for performing routing process with the help of energy model, energy manager and the decision manager. The potential routes must be efficiently maintained earlier in the routing process.

Clustering Model: The clustering model is responsible for grouping the nodes according to the distance similarity between the sensor nodes in this work. It consists of three sub components such as Cluster head selection, cluster formation and the cluster maintenance. Here, the cluster heads (CHs) are selected according to the distance, energy level and the individual nodes trust. Group the relevant nodes according to the energy level, trust score and the distance between the nodes. Finally, it maintains the route which we have been grouped as a cluster.

Decision Manager: It is an overall responsible and more important model also for completing the tasks that are able to supply the necessary information to the energy model from this manager. It received the necessary information from the data collection module and it forwarded to the trust model for trust score calculation, transfer to the energy model for balancing the energy level, and transfer these all received nodes information for grouping the nodes and it able to route the data packets based on the routing model suggestion.

Rule Manager: This rule manager is used to manage the rules that has to be finalized by the decision manager and also to store the necessary rules in the knowledge base.

Knowledge Base: The knowledge base contains the rules and facts that are useful for making decision over the processes of energy efficiency, clustering process, routing process and the trust score calculation process in the network.

4. Proposed Work

This section discusses about the proposed Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) which is used for effective data communications in WSNs. The FEBSRA considered the energy level, delay, and trust scores, number of hops between the source and destination and with the nodes. Moreover, a new introduction of new formulae for calculating the various trust distance between the source and sink, and fuzzy rules for making final decision over sensor trust model is also introduced scores such as direct trust, indirect trust, reputation score and data communication cost as communication score. Moreover, an efficient energy model is used in this work. In addition to this, an existing clustering approach called K-Means clustering algorithm is also used for grouping the nodes that are useful for performing routing process. Finally, it generates the necessary fuzzy rules according to the trapezoidal fuzzy membership function for making final decision over the sensor nodes. The fuzzy rules are framed with the consideration of energy, delay, number of hops and trust scores that are to be used for making final decision accurately.

The proposed FEBSRA is designed according to the trust scores and the sensor network design, fuzzy inference model and the cluster and trust based routing algorithm. For trust and network designing, the dynamic trust scores are calculated by using the dynamic rules over the sensor nodes and the links between the source and destination. For the effective network design, the rules over the positioning the wireless sensor nodes and the destination nodes are finalized by using the fuzzy rules. The newly generated fuzzy rules have been applied in this

work for designing an inference model, cluster based routing, applying the rules over the trust score calculation, cluster formation, identifying the malicious nodes and unknown attacks, cluster head selection process and also performed the routing process.

4.1 Sensor Network Design

In this sensor network design process, the sensor node positioning and identifying the destination nodes are considered severely. The proposed model considers a sensor networking model that contains 'n' number of wireless sensor nodes which are deployed uniformly and randomly in a circular fashion with the radius value 'r' that must be less than 100 meters distance and a destination node is initially positioned at the centre of the circular area. Initially, in this framed circular contains around 50 wireless sensor nodes as participating nodes that must be positioned randomly. This process is to be repeated for covering the specific area like (100 X100) m where the m indicates the meters. The participating nodes of this wireless sensor nodes have been connected using connectionless link in wireless environment. These wireless sensor nodes are able to move forward from one position to another one position and also associated with the various destination nodes. Here, the possible destination nodes are able to communicate with each other nodes and also to do the data sharing also takes optimal and right decisions collaboratively.

4.2 Attack Design

In this work, old and new types of attacks are considered for detection and prevention. The dynamic trust scores are calculated for all the participated nodes in the uniform time interval according to the fuzzy rules. The nodes behaviour, traffic density level, nodes movement and the available neighbour nodes are considered while calculating the trust score and making decision over the sensor nodes. Here, the Denial of Service (DoS) based attacks that are belongs to flooding attacks and black hole attacks according to the nodes comparisons that are identified based on their trust scores. Dynamic trust scores have been calculated in this work according to the response time, energy consumption, number of packets dropped during the particular time period and reputation score of the nodes that is given by the neighbour nodes. The proposed trust model supplies the dynamic trust scores for all the participating nodes that are available in cluster links and entire networks that all will come under the base station and it also can be extended. This attack model considered the black hole attacks that are to be formulated by the compromising sensor nodes in WSNs. Moreover, these are eliminated with their data packets and also to minimize the capability of neighbour sensor nodes of the entire sensor network and especially the current nodes. These kinds of sensor nodes are identified and removed from all the activities of the sensor networks by using the dynamic trust score.

4.3 Energy Model

The proposed FEBSRA used in the existing energy model (Logambigai et al 2018). It is used in equation 1 for calculating the energy level for transmitting the data from source node to destination node in the network. In addition, the equation 2 is helpful for calculating the required energy to receive the data packets. The standard symbols D1, D2 and E_{el} are to be used for representing the transmission circuit loss, automatic energy reduction and the energy reduction due to the multipath fading process in WSN. In addition, the standard symbols ε_{fs} and ε_{amp} are also to be used for representing the respective energy level that are required for energy strengthening in the two different energy models that are available already. Finally, the energy consumption is required to receive an *l*-bit data packet that is shown in the equation 2. In addition, the standard symbols such as'd' and 'd_0' are indicating the real distance and the threshold distance values for the nodes from the base station.

$$\begin{cases} E_{member} = l\,E_{el} + l\,\varepsilon_{fs} d^2 & if\ d \le d_0 \\ E_{member} = l\,E_{el} + l\,\varepsilon_{amp} d^4 & if\ d > d_0 \\ E_R(l) = l\,E_{el} \end{cases} \quad (1)$$

$$\{E_R(l) = l\,E_{el} \quad (2)$$

4.4 Dynamic Trust Model

This sub section explains in detail about the dynamic trust score calculation process for each node which is presence in the WSNs. Here, we have calculated the direct trust, indirect trust, reputation score and the communication trust score are to be considered as dynamic trust score that has been calculated during the particular period of time. This section is summarized one by one in detail.

4.4.1 Direct Trust

Generally, the sensor nodes behaviour is monitoring by the neighbour nodes in the wireless sensor networks. Hence, the wireless sensor nodes are considered more in the process of calculating the energy level of the node, current energy level of the node, available memory space and the network bandwidth and it is not sufficient for judging the trust scores of the participated sensor nodes only through monitoring the sensor nodes behaviour (Xu et al 2014). Therefore, this work is combined the behaviour of the node with energy level for evaluating the degree of nodes trust worthiness. First, it calculates the direct behaviour trust of each participated nodes that are involved in the process of communication. This work is calculated the direct behaviour trust scores (DBTS) of all participated nodes by using the equation (1).

$$DBTS(a,b)^{m} = \gamma_1 \times DBTS_{P(b)}(a,b)^{m-1} + \gamma_2 \times DBTS_{N(b)}(a,b)^{m-1} + CBN(a,b)^{l} \quad (1)$$

where $DBTS_{P(b)}(a,b)^{m-1}$ indicates that the direct behaviour trust score of the node a and the node b in the past, $DBTS_{N(b)}(a,b)^{m-1}$ represents that the direct behaviour trust score of b for a based on the worst attitude of the node b in earlier days. Here, n indicates the total number of available neighbour nodes and 1 denotes that the sequence number of the available records. Moreover, γ_1 and γ_2 represents that the self- adaptive exponential decay time factor of the positive evaluation and the negative evaluation respectively.$CBN(a,b)^{l}$indicates that the evaluation for the nodes current behaviour trust of node b by applying instruction detection system [35]. In addition, $CBN(a,b)$is defined as per the given equation (2).

$$CBN(a,b) = \begin{cases} P(b), & 0 < P(b) < 1 \\ 0, & uncertain \\ N(b), & -1 < N(b) < 0 \end{cases} \quad (2)$$

where P(b) and N(b) indicate that the positive evaluation and the negative evaluation for the sensor nodes behaviour respectively. Here, the sensor nodes behaviour is not to be accurate when the predicted score is in fuzzy state. So, the $CBN(a,b)$ value is 0. In this situation, the value of γ_1 is reduced for normal character and the $\gamma_2$value is increased the malicious behaviour that can be adjusted for ensuring the bad attitude is memorized from a long time than the good attitude.

Next, the sensor nodes energy trust score is calculated in this work. Normally, the sensor node which has highest trust score is to be selected for transferring the data in the secure routing algorithm. Here, it consumed more energy of the sensor nodes with high trust score with uneven network load and the even network segmentation. The energy trust score is calculated by using the formula which is given in equation (3) and the equation (4) according to [36].

$$RecC(l,e) = E_{el} \times l \quad (3)$$

$$\text{SenC (l,e)} = E_{el} \times l + E_{amp} \times l + E_{amp} \times l \times e^{2} \quad (4)$$

Where L indicates the number of bits for a message, e represents the distance between the nodes a and b, E_{elec} indicates that the volume of total consumed energy for forwarding the messages through node b and E_{amp} indicates that the consumed energy for achieving better performance during data forwarding process. So that the total consumed energy of the node b is for transferring the data is:

$$EnCst = E_{el} \times l \times 2 + l \times e^2 \quad (5)$$

Moreover, the network initial energy level is EnInit and the energy EnS of the node b is:

$$EnSt = EnInit - EnCst \quad (6)$$

Here, the sensor node surplus energy is greater than the threshold value of the energy Th_{En}.
Otherwise, no matter how high the node's degree of behavioural trust, it cannot participate in the transmission of information. Node b Degree of Energy Trust EnTDb is classified as:

$$EnTD_b = \begin{cases} 1, & EnSt > Th_{En} \\ 0, & EnSt < Th_{En} \end{cases} \quad (7)$$

The degree of direct behaviour trust score calculation of $D\_DBTS(a,b)^m$ is considered the sensor nodes behaviour and the energy trust score of the sensor nodes in the WSN as given in equation (8).

$$D_{DBTS(a,b)^m} = \frac{1}{2}\gamma_1 \times DBTS_{P(b)}(a,b)^{m-1} + \frac{1}{2}\gamma_2 \times DBTS_{N(b)}(a,b)^{m-1} + \frac{1}{2}CBN(a,b)^l + \frac{1}{2}EnTD_b \quad (8)$$

Where the sensor nodes behaviour and the energy level of the sensor nodes that are equally important for computing the degree of nodes trust behaviour the value of $D_{DBTS(a,b)^m}$ and the $EnTD_b$ that are assigned equally.

4.4.2 Indirect Trust

The indirect trust score is the trustworthiness level between the nodes that are able to provide by the neighbour nodes of the source nodes that are connected in the network. Similar to the direct trust model, the indirect trust level which is compose of the sensor nodes indirect behaviour trust degree and the indirect energy trust degree. Here, the energy consumption is serious consideration along with the trust score degree of the same node similar to the direct behaviour trust score calculation. Here, the indirect nodes behaviour trust degree is also considered. If the node b which is directly connected in the wireless sensor network that is C_b, $INBTD(a,b)^m$ indicates the indirect nodes behaviour trust degree which is computed by using the nodes based on the recommendations that are provided by all other neighbour nodes in C_b by using the equation (9).

$$INBTD(a,b)^m = \sum_{\vartheta \in C_b, \vartheta \neq x} (DBTS(a,\vartheta)^m \times DBTS(\vartheta,b)^m) \quad (9)$$

This $INBTD$ is used to identify and prevent the bad mouthing and collusion attacks by using the direct behaviour node trust score. By defult, this score of all the nodes must be verified by available and participating nodes in C_b. The dissimilarity nodes trust degree of the target node 'b' for node 'a' by using the equation (10).

$$CS(a,b)^m = \frac{INBTD(a,b)^m + DBTS(a,b)^m}{\sum_{\vartheta \in C_b, \vartheta \neq x}(DBTS(a,\vartheta)^m + 1)} \quad (10)$$

For any other neighbour node ϑ in the direct connected domain of target node b, $INBTD_k(\vartheta,b)^m + CS_k(a,\vartheta)^m$ k> m, the recommended node ϑ is not to be adopted. Here, dissimilarity threshold checking process is fixed value that is related to the specific network topology and the relevant data. Finally, the malicious nodes in the set of credible nodes are identified and detected in this work and also considered the false positive rate of them and also to be excluded from the concern wireless sensor network environment. Similar to the procedure of calculating the direct nodes behaviour trust degree, the node 'a' is obtained the indirect nodes behaviour trust degree value of the specific node b:

$$INBTD(a,b)^m = \frac{1}{2}\gamma_1 \times INBTD_{P(b)}(a,b)^{m-1} + \frac{1}{2}EnTD_b$$
$$= \frac{1}{2}\sum_{\vartheta \in C_b, \vartheta \neq x}(DBTS(a,\vartheta)^m \times DBTS(\vartheta,b)^m) + \frac{1}{2}EnTD_b \quad (11)$$

where the weightage of the $INBTD(a,b)^m$ and the $EnTD_b$ are also to be equal that areassigned like the equation (8).

4.4.3 Energy Trust

Energy is an important feature in sensor networks and it is determined the network life time. In addition, the energy consumption is used to find whether a misbehave node that launched the malicious attack which is able to arise the security problems or not. Therefore, this work uses two energy trust metrics such as residual energy ratio and the energy consumption rate ratio. In the residual energy ratio, the residual energy ratio of the object node which is added to the data packet information when the object node sends the data to the subject node. Suppose, the subject node finds the residual energy of the object sensor node and that value is minimum of finalized threshold. Moreover, the object sensor node is considered as an ineligible sensor node that is not to appear in the process of normal data packet transmission anymore and also set this energy is to 0. On the other hand, in the energy consumption rate differentiation transmits the current energy consumption with residual energy sequentially by the object node. Here, energy rate is different from node to node and also not exactly the same value due to the presence of the sensor nodes and the availability of the neighbour nodes. Here, the number of hops also considered for finalizing the energy trust score. Some researchers introduced few techniques to measure the trustworthiness of the energy (Chen et al 2015) and it utilizes the energy consumption rate differentiation using the equation (1) for detecting the anomalous. The energy trustworthiness score of the object node is calculated by using the equation (12).

$$EnTr^{i,j} = \begin{cases} ResEn^s\ (1 - \Delta p) & ResEn^s \geq \mu \text{ and } \Delta q \leq \gamma \\ 0 & ResEn^s < \mu \text{ or } \Delta q > \gamma \end{cases} \quad (12)$$

Where $EnTr^{i,j}$ indicates that the energy trust score of the nodes i to j. Even though, no effective inspection technique is used for judging the accuracy of the energy related data that is supplied by the object node in the current network topology.

In case, if the node provides wrong report about the energy consumption and the residual energy then the sensor node selected by the neighbour nodes that are available as trustworthy next hop nodes. This wrong report affects the attack detection. So, the malicious node must provide right data truthfully and it can be verified through experiments.

4.4.4 Data Communication Trust Score

The data communication trust score is a very basic data which is used for examining the credibility of the object node in the process of trust score evaluation. For detecting the black hole attacks and the grey whole attacks by using the data communication trust and also adopts two data communication trust metrics such as packet received feedback and the packet forwarding. Here, the feedback is received from the object node within the limited time duration then it is considered and also encountered the particular communication process is done successfully otherwise the particular communication process is considered as failed. In the packet forwarding metric, the particular node received the feedback from object node by the watchdog mechanism within the time duration then it is considered as a successfully to forwarded into the destination node otherwise the data communication process is encountered as failure. Moreover, the data communication trust is able to predict whether the object node is behaved normally or not in the future and also perform the trust calculation simply enough for safeguarding the sensor node energy. The data communication trust is calculated by using the equation (13).

$$DCTS^{i,j} = \frac{SDC^{i,j}+1}{(SDC^{i,j}+1)+(UDC^{i,j}+1)} \quad (13)$$

Where $DCTS^{i,j}$ indicates the data communication trust of the subject node i into the object node j while $SDC^{i,j}$ and $UDC^{i,j}$ indicate that the total numbers of successful data communication and the unsuccessful data communication process between the nodes i and j through the direct data communication trust metrics respectively.

4.4.5 Overall Trust Score

The overall trust score (OTS) is calculated by using the direct node behaviour trust score (DDBTS), indirect nodes behaviour trust score (INBTD), energy trust score (EnTr) and the data communication trust score (DCTS) by applying the equation (14).

$$OTS < t1, t2 >= DDBTS < t1, t2 > + INBTD < t1, t2 > + EnTr < t1, t2 > + DCTS < t1, t2 > \quad (14)$$

Where, t1 and t2 are indicating the starting time and the ending time. Here, the overall trust score is finalized for the particular time duration only by the results of the direct, indirect, energy and data communication trust scores at the same time interval. The overall trust score is considered for finalizing whether the node is normal or malicious.

4.5 Clustering Model

This section explains in detail about the clustering model which uses in the proposed model for grouping the nodes that are available in WSNs. Here, the cluster is formed according to the distance between the nodes and the residual energy level of the node. Moreover, the distance between the nodes is calculated by using the Minkowski distance measurement formula (Ganapathy et al 2012). In addition, this model uses the fuzzy rules that are generated newly in this work according to the values of energy level of the node and the distance between the node and the neighbours. After that, a cluster head (CH) is selected according to the nodes energy level and the position of the node in the sensor nodes of the sensor network. Here, the fuzzy logic has been used with fuzzy rules that have been generated according to the overall trust score, energy level and the distance. New fuzzy inference model is also introduced in this paper that contains the process of fuzzification, fuzzy inference engine, fuzzy rule firing and the defuzzification. In this fuzzification process, five fuzzy variables such as low, medium, high medium and high are applied over the trapezoidal fuzzy membership function to perform the decision making process. In addition, it avoids the malicious nodes during the routing process.

4.6 Routing Model

This section explains the proposed routing algorithm called Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) for secured data communication in WSNs. The proposed FEBSRA used in the energy model, trust model, clustering model and the routing model. All these models are containing various newly proposed techniques that are useful for making effective decision over the sensor nodes in the routing process. The proposed FEBSRA consists of five phases such as clustering model, trust model, energy model, security model and the routing model. In this five phases, the necessary steps are available for performing the clustering process, calculates the trust scores such as direct trust score, indirect trust score and the data communication trust score. In third phase, energy trust is calculated for each node and checks whether the specific node is normal or attack by applying fuzzy rules that are generated by using the overall trust score and the energy level of the node and the number of hops in fourth phase of FEBSRA. Finally, the routing process is performed by using the eligible nodes. The various steps of the proposed secure routing algorithm are given below and also explained in detailed about the working process of the algorithm in this section.

Trust and Energy aware Secure Routing Algorithm

Input : Wireless Sensor Nodes, Destination Node

Output: Clusters and the Secured Routes

Phase 1: Clustering Model

Step 1: Locate the wireless sensor nodes within the area of circle randomly.

Step 2: Positioned the destination node at the centre of the circle which is fixed early.

Step 3: Create a new cluster by applying the standard clustering algorithm called K-Means clustering and mention the current density of the node.

Step 4: Assign the initial trust score for all the sensor nodes and the destination node to 0.6 each.

Step 5: Generate fuzzy rules that are based on the energy level, mobility and the trust score.

Step 6: Select the cluster head according to the particular node with better trust score, less movement and minimum distance to the neighbour nodes in the group.

Step 7: Select the possible routes to reach the destination from the cluster heads.

Step 8: Initially, transmit a set of data packets from the specific sensor nodes to the destination node and also the base station of the network.

Step 9: Repeat the steps 10 to 17 until the sensor network has 'NO POSSIBLE TRUSTED ROUTE'

Phase 2: Trust Model

Step 10: Call the trust model ( ) for calculating the trust scores.

10a. Calculate the direct trust score by using the formula

$$DBTS(a,b)^m = \gamma_1 \times DBTS_{P(b)}(a,b)^{m-1} + \gamma_2 \times DBTS_{N(b)}(a,b)^{m-1} + CBN(a,b)^l$$

10b. Calculate the indirect trust score by applying the formula

$$INBTD(a,b)^m = \frac{1}{2}\gamma_1 \times INBTD_{P(b)}(a,b)^{m-1} + \frac{1}{2}EnTD_b$$

$$= \frac{1}{2}\sum_{\vartheta \in C_b, \vartheta \neq x} (DBTS(a,\vartheta)^m \times DBTS(\vartheta,b)^m) + \frac{1}{2}EnTD_b$$

10c. Calculate the data communication trust by using the formula

$$DCTS^{i,j} = \frac{SDC^{i,j} + 1}{(SDC^{i,j} + 1) + (UDC^{i,j} + 1)}$$

10d. Find the overall trust score by using the direct, indirect and data communication trust by applying the formula $OTS = DDBTS + INBTD + EnTr + DCTS$.

Phase 3: Energy Model

Step 11: Calculate the energy cost of the participating nodes in the sensor network by using the formulae

$$EnTr^{i,j} = \begin{cases} ResEn^{s}\ (1 - \Delta p) & ResEn^{s} \geq \mu \text{ and } \Delta q \leq \gamma \\ 0 & ResEn^{s} < \mu \text{ or } \Delta q > \gamma \end{cases}$$

Phase 4: Security Model

Step 12: Compare the trust scores of the cluster heads and the member nodes that are available in the sensor network.

Step 13: Apply fuzzy rules for identifying the DoS attacks and maintains the total number of attacks available in the sensor network.

Step 14: Apply fuzzy rules for finding the black hole attacks and also keep the numbers.

Step 15: Perform the re-clustering process by using the fuzzy rules and also to select the cluster heads if new clusters are formed during the re-clustering process.

Step 16: If the attacker is identified from DoS or Black hole attacks then those nodes must be de-activated and also change the network topology if necessary.

Step 17: Transmit a new set of data packets and calculate the new trust scores for the nodes once again by calling the trust model.

Step 18: List the nodes that are identified as unbelievable or not useful for the routing process.

Phase 5: Routing Model

Step 19: Route formation by using the eligible sensor nodes for reaching the destination node.

Step 20: Perform route maintenance.

Step 21: Send the data packets through the finalized secure route.

The proposed FEBSRA uses the existing clustering algorithm called K-means clustering algorithm for grouping the nodes according to the distance that is calculated by using the distance measurement formula called Minkowski distance. Moreover, the existing energy model is used for measuring the energy level of the nodes. Here, the energy trust value is also calculated newly in this work. In addition, new trust model has been proposed in this work for calculating the direct trust, indirect trust, data communication trust and the overall trust score for all the nodes that are useful for classifying the nodes as normal or attack. In this FEBSRA, a new security model is also proposed by applying newly generated fuzzy rules by using the overall trust score and the energy trust score. Finally, send the data packets through the finalized routes and also produce a list which contains the nodes are not eligible for participating in the routing process.

5 Results And Discussion

This work has been implemented by using the network simulation tool called Network Simulator version 2 (NS-2). The simulation parameters which are used to carry out this work are shown in Table 1. The performance of our proposed method is compared LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017), TRPM (Boyuan and Donghui 2018)

Table 1 Network Simulation Parameters

Parameters	Value
Network Area	1000x1000 m^2
No. of Sensor Nodes	500
Initial Node Energy	2J
E_{elec}	100 nJ/bit
ε_{fs}	20 pJ/bit/m^2
ε_{mp}	0.0026pJ/bit/m^4
Size of each Packet	4096 bits
Routing Protocol	DSR
Simulation time	500 s

The packet delivery ratio analysis is shown in figure 2 which considered the proposed algorithm and also the existing routing protocols for the analysis. There are five different experiments have been conducted for this packet delivery ratio.

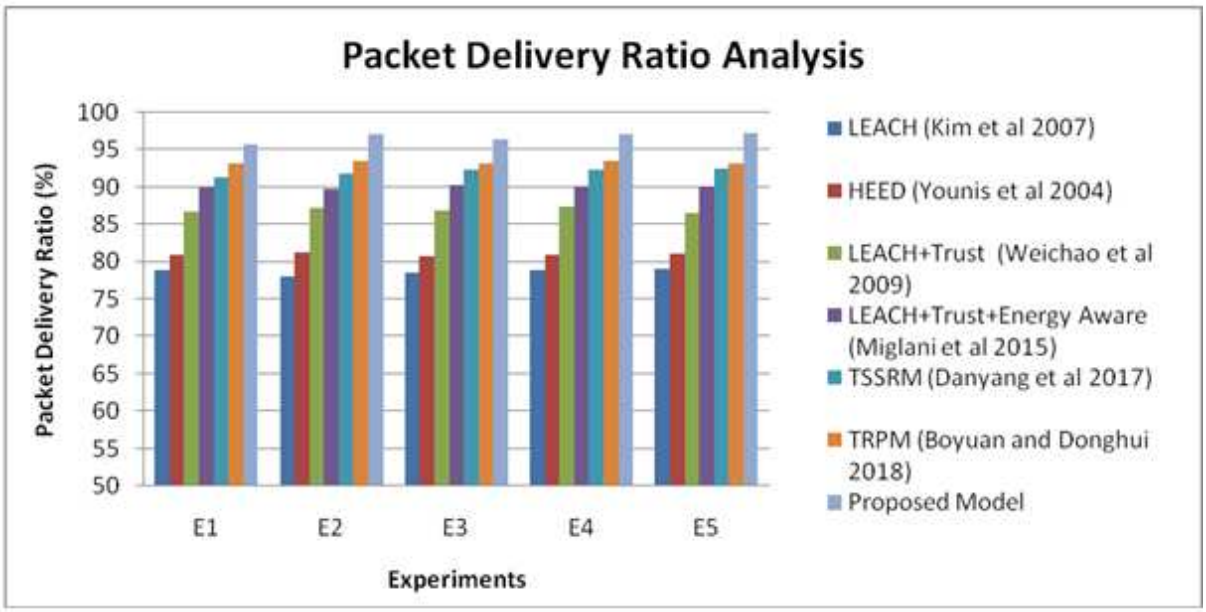

Fig 2. Packet Delivery Ratio Analysis

From figure 2, it can be noted that the use of the direct and indirect trust score which are improved the packet delivery ratio in the proposed model when it is compared to the other existing secured routing algorithms such as LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017) and TRPM (Boyuan and Donghui 2018)which are used trust mechanism and clustering technique for making clusters in the network. The reason for the better packet delivery ratio achieved in the proposed model is the use of trust score calculation, energy level consideration and the incorporation of new outlier detection algorithm.

Figure 3 depicts the communication delay comparison between the routing algorithms namely LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017), TRPM (Boyuan and Donghui 2018) and the proposed TESRA.

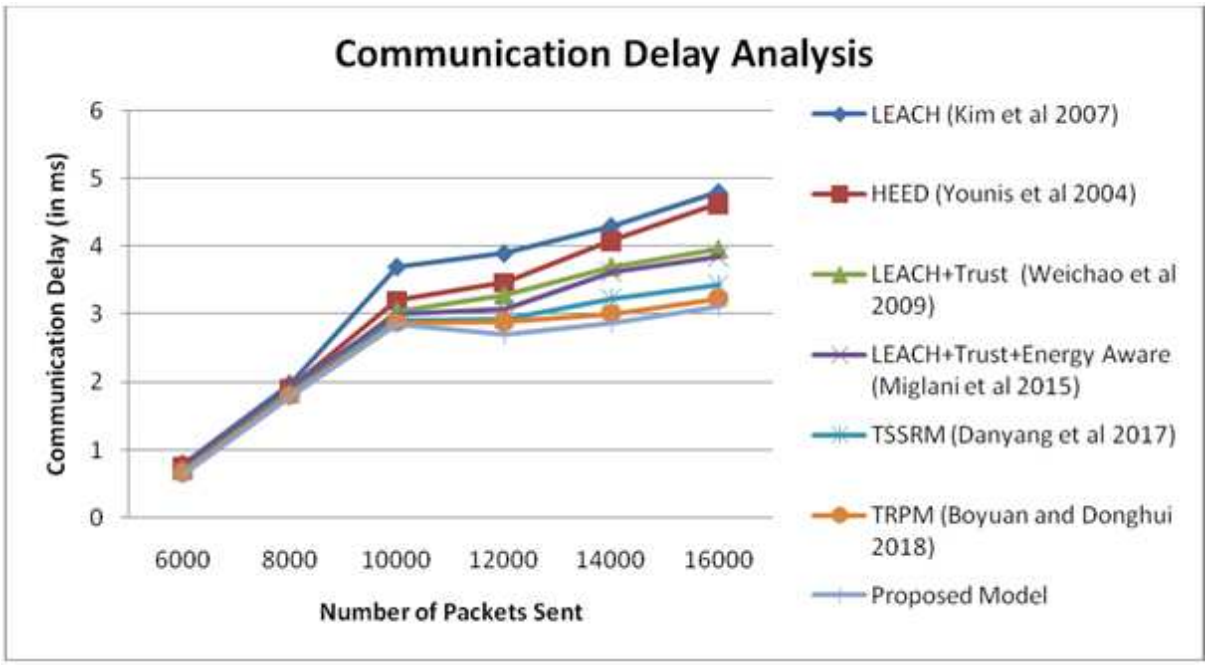

Fig 3. Communication Delay Analysis

From the experimental results shown in figure 3, many observations can be made. First, the clustering process reduces the delay by grouping the sensor nodes. Second, the use of trust values reduces the communication delay by preventing the malicious nodes from introducing intended delay. Finally, the use of clustering, fuzzy rules, energy trust along with trust modeling enhances the security by the application of fuzzy rules more efficiently leading to reduction in overall delay.

Figure 4 is used to show the comparison of the number of packets delivered when the packets are routed using the exiting algorithms such as LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017), TRPM (Boyuan and Donghui 2018) and also the proposed secured routing model that uses fuzzy rules and trust modeling along with energy trust. In this process, five different experiments have been conducted by varying the mobility speeds of sensor nodes from 10 m/s to 50 m/s.

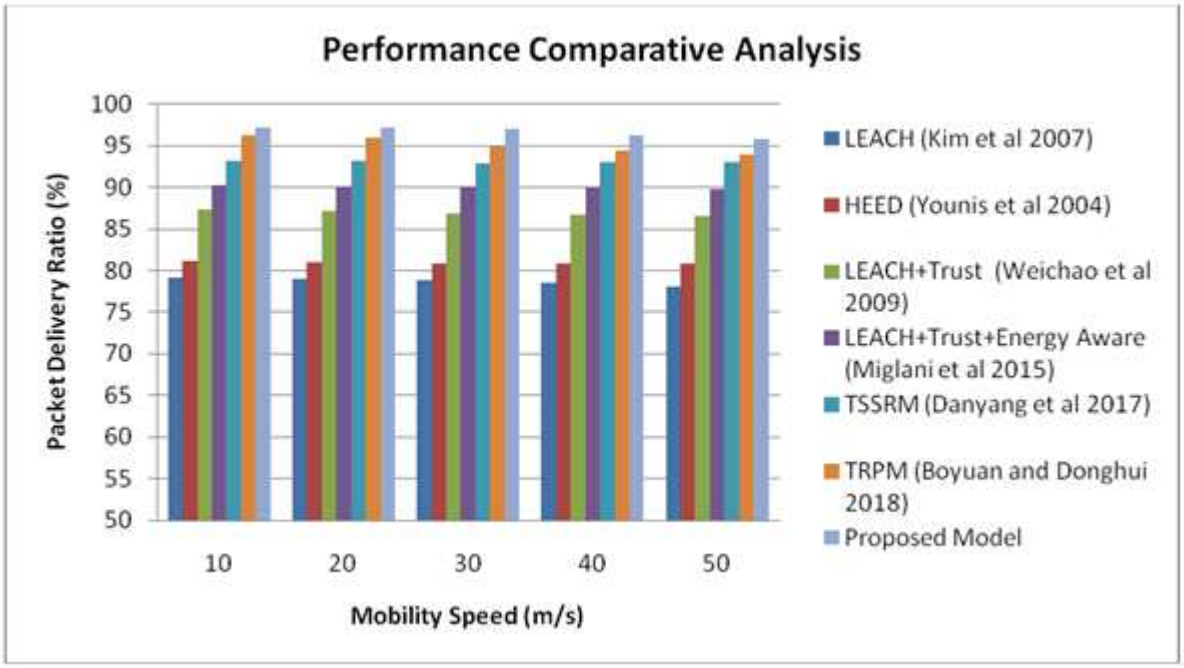

Fig 4. Performance Comparative Analysis

From the results shown in Figure 4, it should be noted that in terms of the number of packets delivered with different mobility speeds, the performance of the routing algorithm with confidence modeling is better than the algorithms that do not consider trust modeling. The routing algorithm proposed also outperforms all other current routing algorithms considered in this work due to the use of fuzzy rules, clustering, trust management and energy trust.

Figure 5 shows the comparative analysis between different existing routing algorithms namely LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017), TRPM (Boyuan and Donghui 2018) and the proposed secured routing algorithm that are tested by applying varying mobility speeds in each rounds.

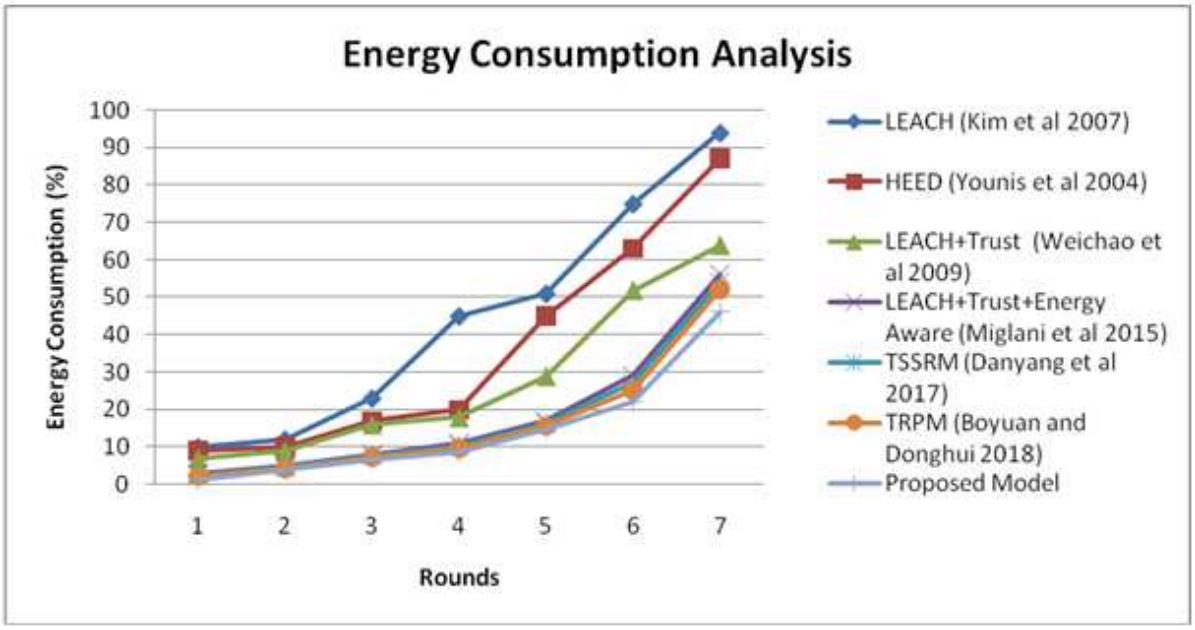

Fig 5. Comparative Analysis based on Energy Consumption

From figure 5, it can be noted that the energy consumption is minimum when the packets are routed through the proposed FEBSRA than the other routing algorithms namely LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009), LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017) and TRPM (Boyuan and Donghui 2018). Here, the performance improvement has been achieved not only through the application of fuzzy rules, trust mechanism, clustering and energy trust.

Figure 6 shows the security level analysis for the newly proposed secured routing algorithm and the other routing algorithms namely LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009) and LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017) and TRPM (Boyuan and Donghui 2018). Moreover, five different experiments have been carried out with various set of nodes in the sensor network scenario like 100, 200, 300, 400 and 500 for analyzing the security level of the proposed work.

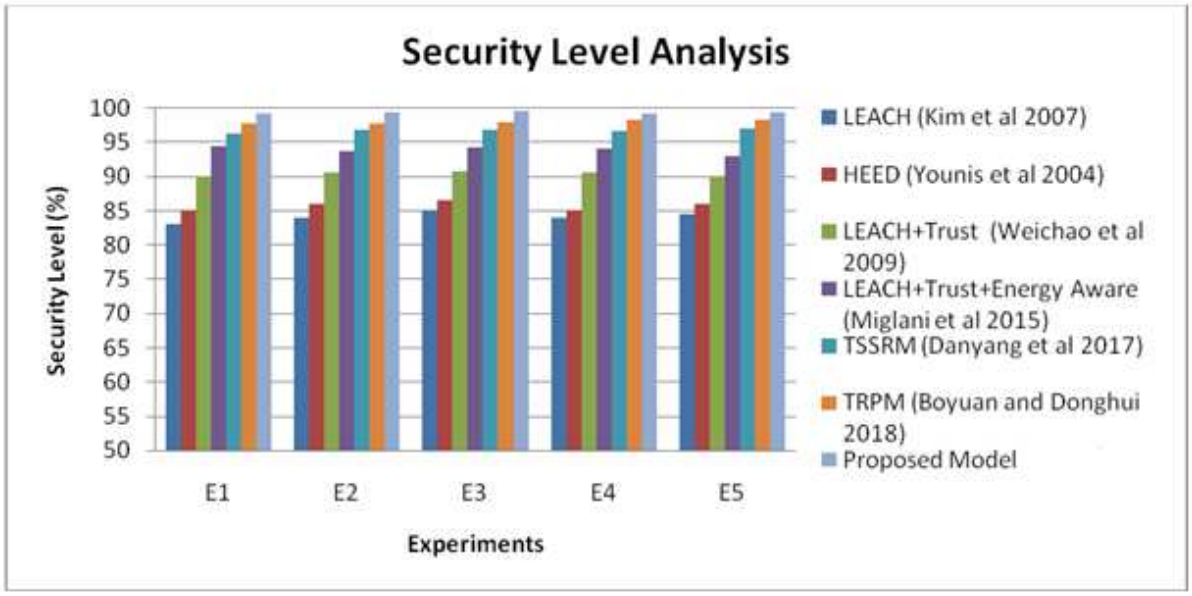

Fig 6. Security Level Analysis

From figure 6, it can be observed that the performance of the newly proposed secured routing algorithm is better when it is compared with the other routing protocols namely LEACH routing algorithm (Kim et al 2007), HEED (Younis et al 2004), LEACH with trust mechanism (Weichao et al 2009) and LEACH with trust and energy consideration (Miglani et al 2015), TSSRM (Danyang et al 2017) and TRPM (Boyuan and Donghui 2018). The reason for this improvement is to be the use of energy trust, intelligent fuzzy rules, effective direct, indirect, and communication trust and the consideration of energy while making the effective decision over the routing process. The newly proposed intelligent weighted fuzzy cluster based secured routing algorithm that is used to evaluate the different performance metrics like energy consumption, end-to-end delay, security and the packet delivery ratio. The overall performance of this proposed work is significantly improved when it is compared with other routing algorithms.

6 Conclusion and Future Work

Fuzzy Trust Based Energy Aware Balanced Secure Routing Algorithm (FEBSRA) has been proposed and implemented for providing the effective secured data communications in WSNs. The proposed FEBSRA considered the delay constrains, fuzzy logic and fuzzy rules for making final decision over sensor nodes with the consideration of number of hops between the source and destination nodes, energy level of the nodes and the trust scores. Moreover, a new dynamic trust model also has been proposed and implemented with the use of newly introduced formulae for calculating the trust scores dynamically with the consideration of energy level of the communication delay which is calculated by using number of hops used for the specific communication. The proposed FEBSRA achieved better performance in terms of energy consumption, delay, throughput, overhead and security is better when compared to the existing systems. Future works will be focus on introducing an intelligent agent for enhancing the decision making and communication processes.

References

1. Danyang Qin, Songxiang Yang, ShuangJia, Yan Zhang, Jingya Ma, And Qun Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network", IEEE Access, Vol.5, pp. 9599-9609, 2017.
2. ZengweiLyu, Zhenchun Wei, Jie Pan, Hua Chen, Chengkai Xia, Jianghong Han, Lei Shi, "Periodic charging planning for a mobile WCE in wireless rechargeable sensor networks based on hybrid PSO and GA algorithm", Applied Soft Computing Journal, Vol. 75, pp. 388–403, 2019.
3. Liangyin Chen, XundeXiong, Yanru Chen, Kai Liu, Jingyu Zhang, Yushi Jiang, Feng Yin and QianLuo, "Why (n + 1)th-hop neighbours are more important than nth-hop ones for localisation in multi-hop WSNs", Electronics Letters, Vol. 50, No. 22, pp. 1646–1648, 2014.

4. Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network", IEEE Sensors Journal, Vol. 15, No. 12, pp. 6962-6972, 2015.
5. TrongNhan Le, Alain Pegatoquet, Olivier Berder, and Olivier Sentieys, "Energy-Efficient Power Manager and MAC Protocol for Multi-Hop Wireless Sensor Networks Powered by Periodic Energy Harvesting Sources", IEEE Sensors Journal, Vol. 15, No. 12, pp. 7208-7220, 2015.
6. Ahmad El Assaf, Slim Zaidi, SofièneAffes, NahiKandil, "Low-Cost Localization for Multihop Heterogeneous Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 15, No. 1, pp. 472-484, 2016.
7. Slim Zaidi, Ahmad El Assaf, SofièneAffes, NahiKandil, "Accurate Range-Free Localization in Multi-Hop Wireless Sensor Networks", IEEE Transactions on Communications, Vol. 64, No. 9, pp. 3886- 3900, 2016.
8. Trong-Thua Huynh, Anh-Vu Dinh-Duc, and Cong-Hung Tran, "Delay-Constrained Energy-Efficient Cluster-based Multi-Hop Routing in Wireless Sensor Networks", Journal of Communications and Networks, Vol. 18, No. 4, pp. 580-588, 2016.
9. XiaofengGao, Xudong Zhu, Jun Li, Fan Wu, Guihai Chen, Ding-Zhu Du, Shaojie Tang, "A Novel Approximation for Multi-Hop Connected Clustering Problem in Wireless Networks", IEEE/ACM Transactions on Networking, Vol. 25, No. 4, pp. 2223-2234, 2017.
10. Boyun Sun and Donghui Li, "A Comprehensive Trust-Aware Routing Protocol with Multi-Attributes for WSNs", IEEE Access, Vol. 6, pp. 4725-4741, 2018.
11. Xiao Liu, NaixueXiong, Ning Zhang, Anfeng Liu, HailanShen, Changqin Huang, "A Trust With Abstract Information Verified Routing Scheme for Cyber-Physical Network", Vol. 6, pp. 3882- 3898, 2018.
12. Philip Asuquo, Haitham Cruickshank, Chibueze P. AnyigorOgah, Ao Lei, Zhili Sun, "A Distributed Trust Management Scheme for Data Forwarding in Satellite DTN Emergency Communications", IEEE Journal on Selected Areas in Communications, Vol. 36, No. 2, pp. 246 -256, 2018.
13. Yaw-Wen Kuo, Cho-Long Li, Jheng-Han Jhang, and Sam Lin, "Design of a Wireless Sensor Network-Based IoT Platform for Wide Area and Heterogeneous Applications", IEEE Sensors Journal, Vol. 18, No. 12, pp. 5187-5197, 2018.
14. YimeiLi,Yao Liang, "Compressed Sensing in Multi-Hop Large-Scale Wireless Sensor Networks Based on Routing Topology Tomography", IEEE Access, Vol.6 , pp.27637-27650, 2018.
15. FarhadFiroozi, Vladimir I. Zadorozhny, Frank Y. Li, "Subjective Logic-Based In-Network Data Processing for Trust Management in Collocated and Distributed Wireless Sensor Networks", IEEE Sensors Journal, Vol. 18, No. 15, pp. 6446-6460, 2018.
16. Shilpa M. Lambor, Sangeeta M. Joshi, "Optimal Hops for Minimal Route Power under SINR Constraints in Wireless Sensor Networks", IET Wireless Sensor Systems, Vol. 8, No. 4, pp. 176-182, 2018.
17. S Muthurajkumar, S Ganapathy, M Vijayalakshmi, A Kannan, "An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs",Wireless Personal Communications, Vol. 96, No. 2, pp. 1753-1769, 2017.
18. M Selvi, P Velvizhy, S Ganapathy, HK Nehemiah, A Kannan, "A Rule Based Delay Constrained Energy Efficient Routing Technique for Wireless Sensor Networks",Cluster Computing, pp. 1-10, 2017.
19. R Logambigai, S Ganapathy, A Kannan, "Energy–Efficient Grid–Based Routing Algorithm using Intelligent Fuzzy Rules for Wireless Sensor Networks",Computers & Electrical Engineering, Vol. 68, pp. 62-75, 2018.
20. K Thangaramya, R Logambigai, L SaiRamesh, K Kulothungan, A Kannan S Ganapathy, "An Energy Efficient Clustering Approach Using Spectral Graph Theory in Wireless Sensor Networks",2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pp.126-129, 2017.
21. Younis O, Fahmy S, “HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks”, IEEE Transactions on Mobile Computing, Vol. 3, No.4, pp.366-379, 2004.
22. Kim, J, Jang, KY, Choo, H & Kim W, “Energy efficient LEACH with TCP for wireless sensor networks”, Computational Science and its Applications–ICCSA 2007, pp. 275-285, 2007.
23. W.Weichao, D.Fei, X.Qijian, an Improvement of LEACH Routing Protocol Based on Trust for Wireless Sensor Networks, 2009, 5th Conference on Wireless Communications and Mobile Computing, pp.1-4, 2009.

24. S Ganapathy, P Yogesh, A Kannan, "Intelligent Agent-Based Intrusion Detection System using EnhancedMulticlass SVM", Computational intelligence and neuroscience, Art. No.: 2012, pp. 1-9, 2012.
25. A.Miglani, T.Bhatia, S.Goel, "Trust based Energy Efficient Routing in LEACH for Wireless Sensor Networks", Proceedings of 201 Global Conference on Communication Technologies, pp. 361-365, 2015.
26. H. Rathore, V. Badarla, and S. Shit, ``Consensus-Aware Socio-Psychological Trust Model for Wireless Sensor Networks," ACM Transactions on Sensor Networks, Vol. 12, No. 3, Art. No. 21, 2016.
27. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, “An Application Specific Protocol Architecture for Wireless Sensor Network,” IEEE Transactions on Wireless Communications, Vol. 1, No. 4, pp. 660–670, 2002.
28. Z. Chen, M. He, W. Liang, and K. Chen, ``Trust-aware and lowenergy consumption security topology protocol of wireless sensor network," Journal ofSensors, Vol. 2015, 2015, Art. No. 716468, doi: 10.1155/2015/716468.2015.

Figures

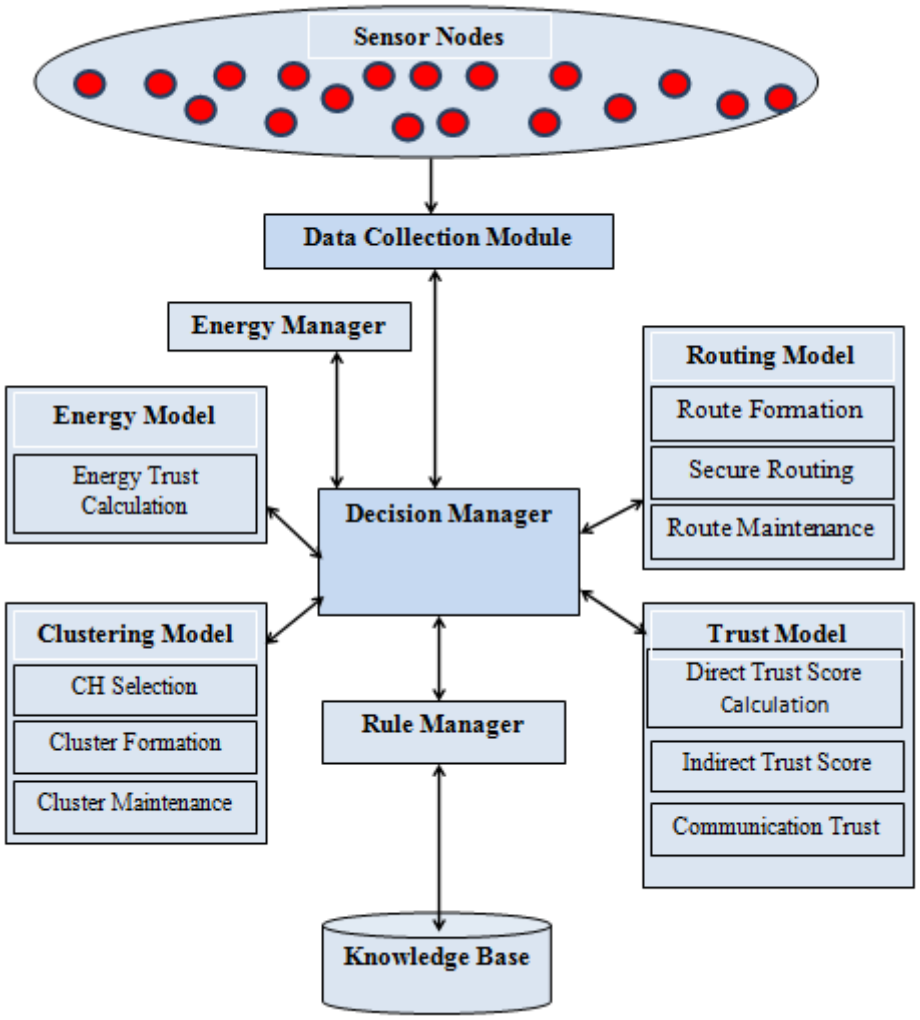

Figure 1

Overall System Architecture

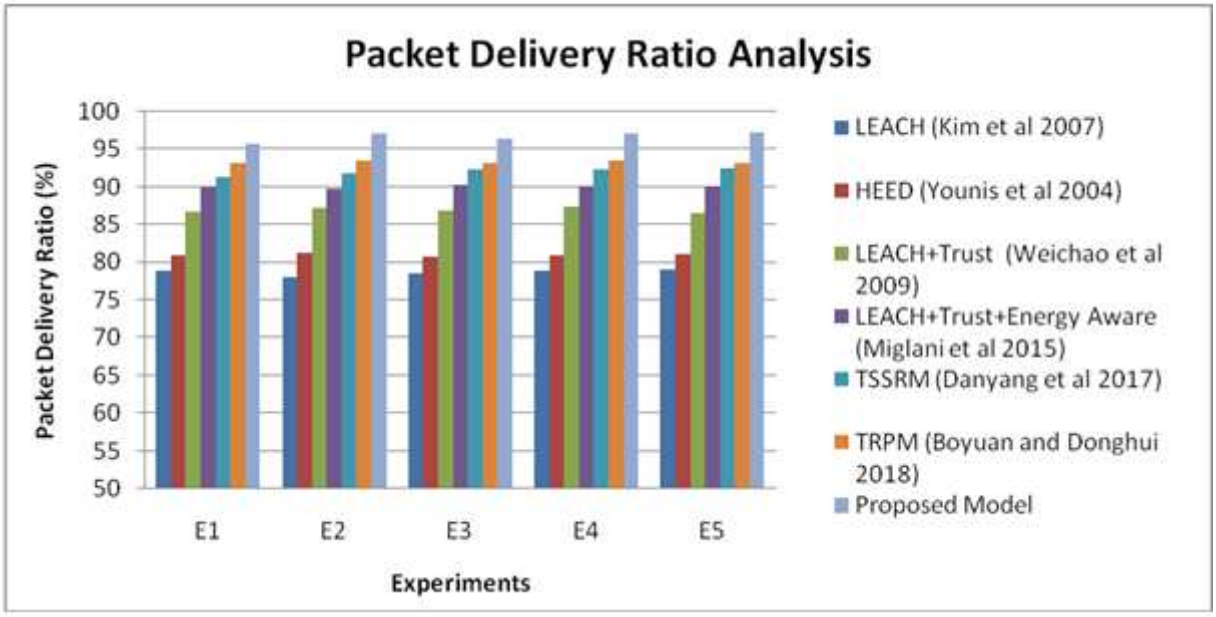

Figure 2

Packet Delivery Ratio Analysis

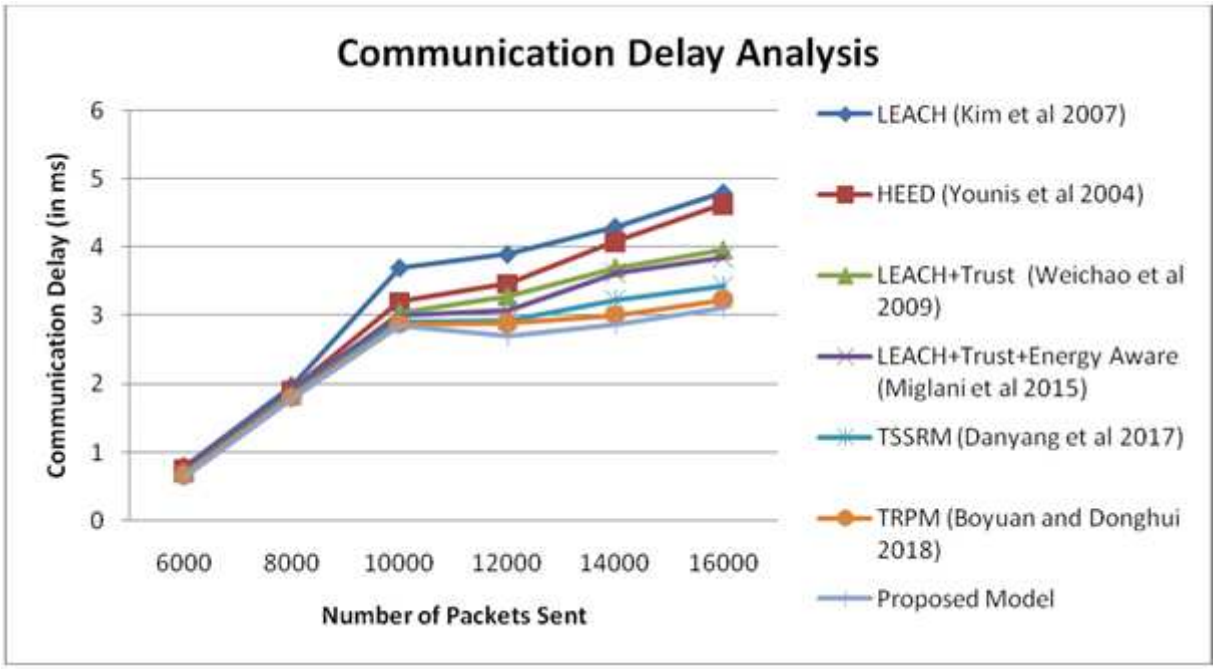

Figure 3

Communication Delay Analysis

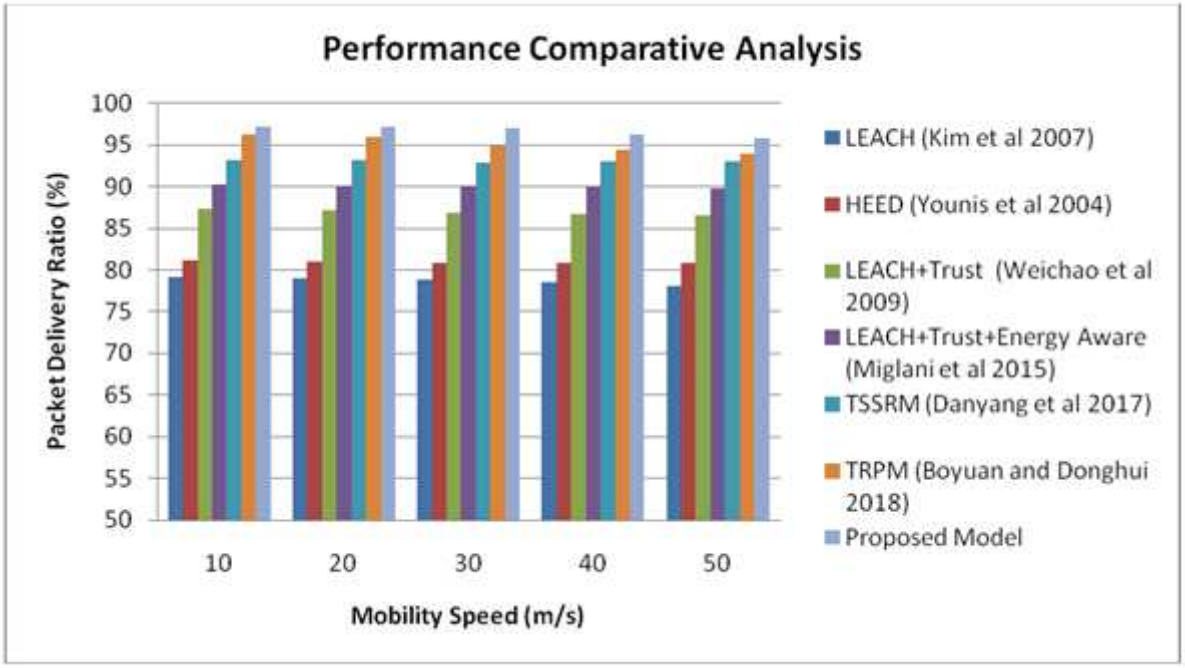

Figure 4

Performance Comparative Analysis

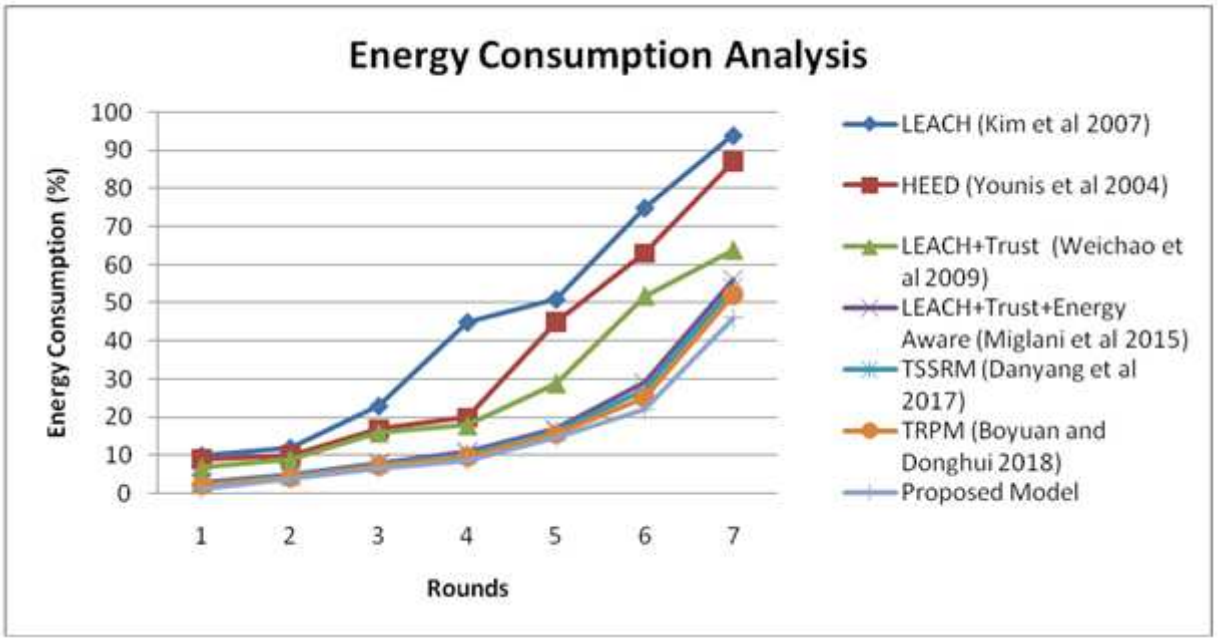

Figure 5

Comparative Analysis based on Energy Consumption

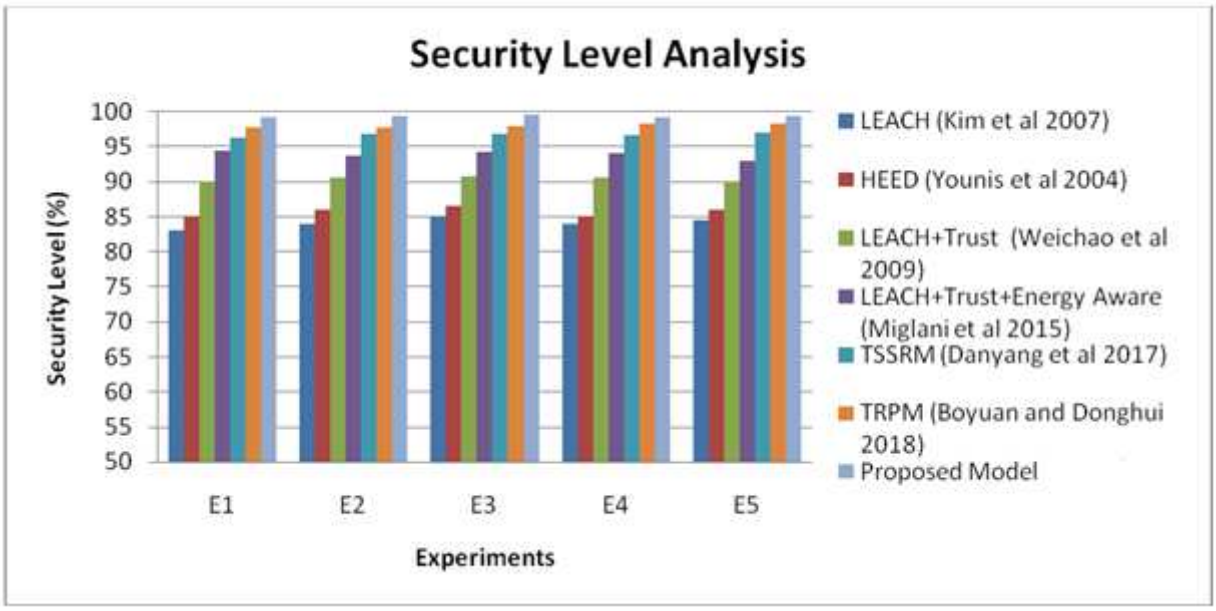

Figure 6

Security Level Analysis