Wireless Personal Communications (2020) 110:1637–1658
https://doi.org/10.1007/s11277-019-06788-y

# QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks

**Thangaramya Kalidoss[1] · Logambigai Rajasekaran[1] · Kulothungan Kanagasabai[1] · Ganapathy Sannasi[2] · Arputharaj Kannan[3]**

Published online: 1 October 2019


**Abstract**
In Wireless Sensor Network (WSN), the lifetime optimization based on minimal energy consumption and security are the crucial issues for the effective design of protocols to perform multi-hop secure routing. In order to address these issues, we propose a new routing protocol called Secured Quality of Service (QoS) aware Energy Efficient Routing Protocol in this paper which is designed based on trust and energy modelling for enhancing the security of WSN and also to optimize the energy utilization. In this proposed work, the trust modelling uses an authentication technique with a key based security mechanism for providing trust scores. Moreover, three types of trust scores namely direct, indirect and overall trust scores are calculated in this work for enhancing the security of communication. In addition, a cluster based secure routing algorithm is proposed in this work in which the cluster head has been selected based on QoS metrics and trust scores to perform cluster based secure routing. Finally, the final path has been selected based on path-trust, energy and hop count to efficiently carry out the secure routing process. The proposed work has been assessed by simulations carried out using NS2 simulator. The simulation results demonstrate that the proposed algorithm provides better performance in terms of increase in packet delivery ratio, network life time and security. Moreover, it provides reduction in delay and energy consumption when the proposed secure routing algorithm is compared to the other related secure routing algorithms.

**Keywords** Trust score · Wireless sensor networks · Quality of Service · Security · Trust based routing · Energy efficiency

## 1 Introduction

Wireless Sensor Networks (WSNs) comprise of tiny devices called sensor nodes having low battery power, minimum computational capacity and limited storage capacity which are deployed in a geographical area for sensing the environment for data collection and

✉ Thangaramya Kalidoss
thangaramya112@gmail.com

✉ Arputharaj Kannan
kannan.a@vit.ac.in

Extended author information available on the last page of the article

communicating the data. In this scenario, the sensor nodes route the gathered information through intermediate nodes connected through wireless links to send the data to the sink node. Therefore, a suitable routing protocol is necessary for transmitting the information gathered by different nodes present in the network through a multi-hop routing path within its range to the sink node. In multi-hop routing path, each of the sensor nodes has to transmit its data as well as other nodes data. The optimization of the power in WSNs is an important performance metric because of the availability of minimum battery power present in the sensor nodes based on the design. The usage of energy must be reduced by applying intelligent decision making techniques based on rules and also clustering [1] of nodes for performing optimal routing. However forming clusters of nodes, selecting a cluster head for each cluster and routing through the cluster heads reduces the number of participating nodes and hence it leads to reduction in energy consumption.

In cluster based routing, the cluster head collects the data from its member nodes, aggregates it and transmits the aggregated data to the sink through a single-hop or multi-hop routing. The multi-hop routing provides an opportunity for the nodes to monitor the malicious activities present in the nodes of the WSNs. Due to the presence of malicious nodes, design of secure routing protocols is the most important issue in WSNs. These malicious nodes may drop the packets purposefully or misdirect the messages in routes or repeats the routing of active packets from reputed sensor nodes to the trustful neighbour nodes followed by cluster heads having high trust for effective secured routing in WSN. In such a scenario, the cluster heads must be selected based on high trust values for preventing the attacking nodes from becoming the cluster head. Moreover, malicious nodes must be isolated from other cluster members as well for reducing the illegal activities for avoiding the tampering activities in the network leading to reduction in accuracy of trust values.

As mentioned already, secure routing algorithm design is an important and challenging issue in WSN due to the presence of attackers. Therefore, it is necessary to develop a security mechanism and safeguard the communication in the network. There are two important methods with which a secure routing algorithm can be developed. In the first method, the attackers can be identified by placing firewalls and intrusion detection systems at the nodes of the network. However, the attackers try to overcome these security mechanisms by developing efficient techniques to break the security methods provided in firewalls and intrusion detection systems. In the second method, a trust based secure routing protocol can be developed by performing user authentication using keys, encryption and decryption mechanisms. This method needs the support of effective key generation, key distribution, verification and rekeying algorithms in order to provide enhanced security.

Authentication protocols have been proposed in the past to perform better user authentication. Many methods have been proposed by researchers for centralized key management and distributed key management techniques. Both these techniques are useful to perform user authentication more effectively. Most of the authentication mechanisms use the user credentials such as the user name, password, Internet Protocol (IP) address and a Captcha to perform the first step in authentication. It can be further verified using better key management techniques with encryption and decryption methods, use of nonce for enhancing the security and also by generating and sending One Time Passwords (OTPs). In spite of the availability of all these methods, the hackers try to break the security system by communicating with the users for getting their credentials in order to perform eavesdropping attacks and also by hacking the mobile phone numbers in order to know the security credentials including OTP. Therefore, it is necessary to perform multilevel mutual

authentication by generating keys, communicating with encrypted messages and also by exchanging acknowledgements through e-mail, alternate phone numbers and some shared secret information by maintaining anonymity using privacy preservation techniques.

The trust evaluation process is an important task in multi-hop secure routing in WSNs. The trust scores are dynamically changing due to the occurrences of various types of attacks at different times in many paths. Moreover, trust score is a mathematical representation of attitude of nodes and also the computation of the attitude of another node in the network. Trust can be computed either at one time or it can be evolved over a period of time. If the trust is computed once and it is used for decision making, such a model is called as static trust model. On the other hand, if the trust values are updated periodically by observing the node behaviour continuously, such a trust model is called as a dynamic trust model. In the network environment, dynamic trust model is able to monitor the user activities and finds the malicious users more effectively when it is compared with the static trust computation model. Most of the trust computation models simply use the past and current behaviour of the nodes and assign a trust value. In another method, these assigned trust values are further improved by considering the trust values evaluated and provided by the neighbour nodes. However, a centralized trust controller or a coordinator for the communication can make the participating nodes to perform mutual authentication through the generation of keys, encrypting the identities and by validating the identities using decryption methods by applying the keys. This type of authentication based dynamic trust modelling includes analysis of past data and present data to perform the prediction of future behaviour, consideration of neighbour opinions and enhanced security using key sharing and verification. Hence, a new trust model which performs key based authentication and considers neighbour information for computing the node trust, path trust and network trust has been proposed in this work in order to enhance the security of the communication in the network. Moreover, the proposed secured routing algorithm has been designed in such way that it performs authentication based trust modelling is proposed to perform cluster based routing where the cluster head nodes are constrained with high level security.

In the past, many QoS [2] routing protocols have been proposed in the literature with the aim of increasing the QoS with high packet delivery ratio, low delay and minimum energy consumption. Among them, the QoS aware Energy Efficient Routing (QEER) algorithm [3] is an important work in the provision of QoS in the routing process. The QEER model considered two important QoS metrics namely the hop count and energy preservation for finding the most suitable and optimal route for routing the packets. In this model, the QoS metrics are focused more but not the reliability with respect to delay and security [4]. Therefore, it is required to develop a secure routing algorithm that takes care of optimal energy consumption and increased security. Therefore, an efficient QoS based routing algorithm with an authentication and key based trust modelling has been proposed in this paper in order to enhance the reliability of communication. The proposed protocol called Secured QoS aware Energy Efficient Routing (SQEER) has been developed by enhancing the QEER protocol to work with clustering based effective routing where the cluster head nodes have been selected with high security constraints for providing an effective secured routing protocol. The proposed model focuses more on energy optimization in the network nodes and in finding the secured route for successful transmission of the collected data packets with security based trust values. Moreover, this proposed SQEER works in three phases namely hop tree and cluster formation phase, authentication based trust modelling

phase for security and the cluster head election cum routing phase. The hop tree has been formed by modifying the algorithm proposed by Logambigai and Kannan [3] with temporal constraints. In the security phase, trust computation through user authentication, past and current behaviour analysis using temporal rules for performing prediction based temporal reasoning and the collection of neighbour information to compute the initial trust. This process is repeated with rekeying and authentication with new keys, cluster head rotation using new trust values and energy levels in subsequent communications. In the cluster selection phase, the trust values are used along with residual energy and mobility parameters for dynamically selecting the cluster heads by applying probabilistic modelling. Moreover, route establishment is performed by identifying the nodes with minimum distance, high trust values, minimum mobility and high energy. Finally, routing is performed through the current cluster heads to send the data to the sink node. The major contributions of the work proposed in this paper are as follows:

- Proposal of an energy optimized secure routing algorithm for enhancing the QoS metrics in WSNs.
- An authentication based method for evaluating the genuineness of nodes.
- Use of spatial and temporal constraints in the proposed trust modelling along with the consideration of direct trust, indirect trust and recommendation trust.
- Proposal of a non-monotonic reasoning approach in coordination with spatial and temporal reasoning in the trust modelling for evaluating the medium level nodes.
- Energy modelling to provide energy efficient routing.

The reminder of this paper has been developed in the following sequence. Section 2 provides the literature survey in the related areas. Section 3 explains the architecture of the proposed system. Section 4 details the methods used in the proposed system. Section 5 depicts the results derived in this work. Section 6 provides suitable conclusions for this work and some future enhancements.

## 2 Related Works

In WSNs, secured and energy efficient transmissions are needed to prolong the network lifetime. In this direction, many researchers proposed energy efficient protocols using various models including cluster based routing techniques. Moreover, there are many articles that are discussing about cluster based secured routing [5–13]. Routing protocols must be provided with security since the data travel through multiple nodes in the network. Therefore in multi-hop routing, secured transmission is very important because the malicious nodes which are present in the route may attack the packets transmitted through them. So, many researchers worked on the development of secured routing protocols and many such protocols are available in the literature [14–17]. In the past, Zhan et al. [18] proposed a Trust-Aware Routing Framework (TARF) for securing the data communicated in WSN. They used trust [19] and energy modelling techniques for achieving this goal. Thippeswamy et al. [20] proposed another Secured routing [21] based on energy and trust modelling for WSN. However, they considered dynamic flow of data for identifying the attackers. Therefore, the deduction accuracy decreases for new types of attacks.

Duan et al. [22] proposed a Trust-aware Secured Routing model to resist various attacks. In their model, the authors proposed specific methods for trust computation and trust derivation schemes to deal with the attacks. Their protocol considers the trust metric as well as QoS requirements in the path selection and hence provides additional security mechanisms. Gu et al. [23] designed a secure communication protocol for providing reliable and secured end to end communication in WSN. In spite of the presence of all these algorithms, a unique routing algorithm which considers energy and security based on trust modelling is necessary to enhance the routing performance for providing reliable communication.

Murthy et al. [24] proposed a multipath routing protocol for WSN using digital signature crypto system for transmitting the data packets in a secure manner. Ganesh and Amutha [25] proposed an efficient and secure routing protocol through SNR-based dynamic clustering mechanisms. In their work, error recovery process was considered in inter-cluster routing. Mahmoud et al. [26] proposed a new secure routing protocol that combines the energy with trust values. Their algorithm stimulates the nodes for relaying the data and for routing strength for providing a secured route report with sufficient battery power.

Li et al. [27] designed a new routing scheme which provides the efficient and fault-tolerant routing. In their work, QoS metrics and path vacant ratio are used to assess and locate an arrangement of connection disjoint paths from all accessible paths. Moreover, they proposed two more algorithms namely a congestion control algorithm and a load-balancing algorithm for multi-hop routing. Their congestion control algorithm adjusts the load on multi-paths and their threshold sharing algorithm splits the packets into multiple segments which are delivered via multipath to the destination using the path vacant ratio in the network. Lee et al. [28] proposed a secured alternate path based routing algorithm for WSN that identifies and separates the malicious nodes which attempt to infuse conflicting routing details from the system by introducing a neighbour report framework.

Liu et al. [29] developed an attack detection model using trust values for effective detection of active attacks. The authors considered the parameters such as node trust and route trust based on the packet drop probability, drop and successful routing probabilities, security score and scalability. Their model is able to detect not only the node trust values but also it avoids the malicious nodes which are present in the routing path for enhancing the network performance. Xiong and Qin [30] developed a new authentication technique which considers non-repudiation as well as client anonymity based on keys for enhancing the security. Moreover, the authors used a digital certificate-less encryption scheme in their model along with a revocation scheme that provides facilities such as remote authentication and scalability. Kerrache et al. [31] explained that the main threats and also the adversary models are handled by the existing trust based security models. In their survey paper, the authors highlighted the challenges and concluded that trust modelling and cryptographic techniques are able to enhance the security of communication effectively.

Hamdane et al. [32] explained about the security methods based on trust modelling for securing the Named Date Networks. The authors proposed a hierarchical identity based cryptography for performing signature verification. Their model is providing better performance in terms of key management based security. Selvi et al. [33] proposed a new Fuzzy Temporal Algorithm for performing Energy Efficient Routing in WSN. Moreover in another work by Selvi et al. [34], the authors proposed a rule based and delay constrained algorithm with energy efficiency in WSN. However, such approaches must be enhanced with security constraints to enhance the security of the routing process. Muthurajkumar

**Table 1** Comparative analysis

| S. No. | Protocols | QoS parameters (PDR and delay) | Security parameters | Energy efficiency |
|---|---|---|---|---|
| 1 | LEACH | High | Not considered | Yes |
| 2 | QEER | High | Not considered | Yes |
| 3 | TARF | Average | Yes | Average |
| 4 | STEAR | Average | Yes | Yes |
| 5 | Trust-aware secure routing framework | Yes | Yes | Not considered |
| 6 | CASER | Average | Yes | Yes |
| 7 | Active trust based secured routing | Yes | Yes | Not considered |
| 8 | Remoting authentication scheme | Average | Yes | Not considered |
| 9 | Fuzzy temporal model | Yes | Not considered | Yes |
| 10 | Rule based delay aware model | Yes | Not considered | Yes |
| 11 | Intelligent secured routing | Average | Yes | Yes |

et al. [35] proposed another routing protocol with security and rules for efficiency in the communication process for MANETs. This work can be extended to work with both static and mobile sensor networks for providing secured and reliable routing process for WSNs. Umar et al. [36] proposed a security architecture for performing intelligent and secure communication in networks. Moreover, the authors applied a fuzzy logic based trust model for handling uncertainty in the trust estimation process and also to perform secure routing.

In spite of the presence of all these algorithms, the routing performance is affected due to the attackers [37]. Hence, a new trust and energy aware secure routing protocol is proposed in this paper. Comparing with the existing works available in literature, the secure routing protocol proposed in this work is novel in three ways. First, it uses a key based authentication scheme in which encryption is performed in the authentication process for enhancing the security. Second, a trust model has been proposed based on the authentication scheme, history of nodes and links and current trust values. Finally, an intelligent temporal reasoning approach has been used to predict the future behaviour of nodes and links based on past data, current data, the rules governing change and the temporal constraints. Therefore, the proposed model provides a secured and reliable routing technique which is more secured and reliable than the existing secure routing protocols.

Table 1 shows the comparative analysis of the existing QoS routing protocols stating their strengths and limitations.

From Table 1, it is observed that most of the QoS routing protocols did not focus on the security issues. Few works on secure routing did not consider the energy efficiency as the major focus. Therefore, a new energy efficient and secure routing protocol is proposed in this paper for enhancing the QoS, security and energy efficiency more effectively.

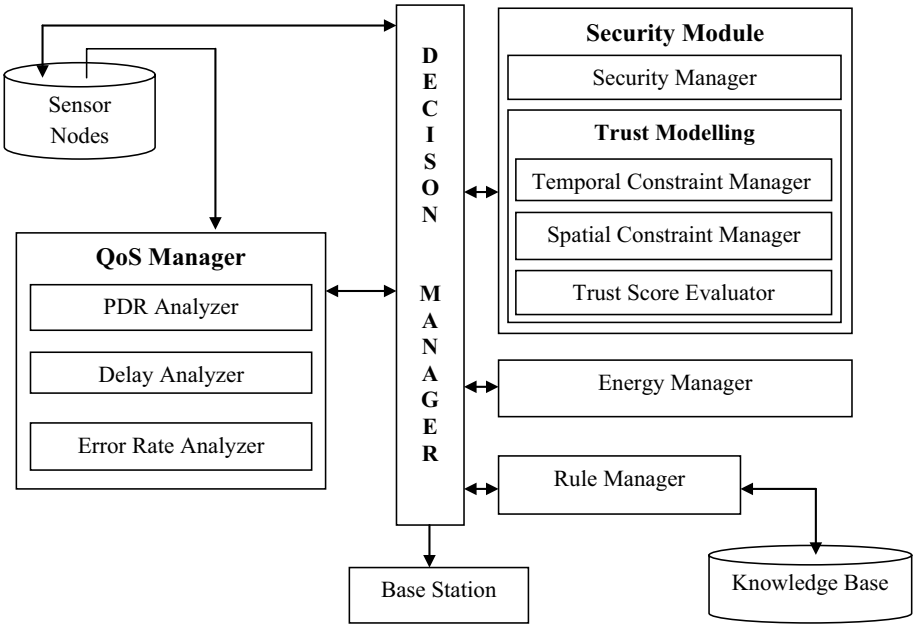



**Fig. 1** System architecture

## 3 Sytem Architecture

The architecture of the QoS routing system proposed in this research work is shown in Fig. 1. It has seven major components including Trace Data, Decision Manager, Security Module, QoS Manager, Energy manager, Rule Manager and Knowledge base.

The decision manager controls the overall activities of the secured routing system. For this purpose, it uses the services of QoS manager, Security Manager and Energy Manager. The QoS manager performs analysis by calling PDR analyser, Delay Analyser and Error Rate Analyser for checking the QoS. The security module is responsible for maintaining trust using spatial and temporal constraint manager and also by interacting with the security manager for performing authentication. The energy manager computes the energy levels and sends them to the decision manager for making energy efficient decision. The rule manager fires the rules present in the knowledge base for making efficient inferences which are used by the decision manager for making secure routing decisions.

## 4 Proposed System

The basic system model of the proposed work includes the components namely sensor nodes which are deployed randomly to monitor an environment. Moreover, the sensor nodes are homogeneous and have the same initial energy. Sensor nodes and the base station are static. The nodes in the sensor network are energy limited and are left unattended after arrangement and the sink is equipped with unlimited energy resource. The base station also called as sink is collecting the routed data from the nodes.

The sensor nodes form a cluster [38] of different sizes. A node with high energy and trust is chosen as the cluster head for each cluster. The data sensed by the sensor nodes is sent to the cluster head and it is transmitted to the sink. The QoS manager performs the quality analysis. The security manager and the energy manger are responsible for improving the security and energy efficiency.

### 4.1 Energy Model

In this work, the energy model used is similar to the works presented in [39, 40]. The transmission energy is required for sending l-bit message to a distance d is computed as per the following Eq. (1)

$$E_T(l,d) = \begin{cases} l\,E_{elec} + l\varepsilon_{fs}d^2 & \text{for} \quad d < d_0 \\ l\,E_{elec} + l\varepsilon_{mp}d^4 & \text{for} \quad d \geq d_0 \end{cases} \tag{1}$$

where $d_0 = \sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$.

The receiving energy needed for an l-bit message is given in Eq. (2).

$$E_R(l) = l\,E_{elec} \tag{2}$$

where $E_{elec}$, electronic energy; $\varepsilon_{fs}$, amplifier energy in free space and $\varepsilon_{mp}$, amplifier energy in multipath.

### 4.2 Trust Score Evaluation

Trust is a level of subjective likelihood hold by a trust or believing a trustee [41] and it is a relationship between two neighbour nodes. It is evaluated by a trust degree that one node gets from another sensor node in order to provide some services. In the literature [42], two types of trust evaluations techniques namely direct and recommendation based trust are available. In this work, both direct as well as recommendation trust evaluation have been used for trust modelling. In addition, the spatial and temporal constraints are also used to compute the final trust score. The direct trust is the direct observation of nodes which is obtained by the behaviour of the node by the trust management system. The recommendation trust is the indirect observation or recommendations or opinions obtained from other nodes or trustworthy third-party about their neighbours. Between the two nodes i and j, the direct trust is denoted as $DTS_{ij}$ and recommendation trust is denoted as $RTS_{ij}$ and the spatio temporal constraints are denoted by f(t1,t2,s) where, t1 and t2 indicate the start time and end time of observation, s is the situation at which the trust value is computed for a node. It uses the situation logic to perform reasoning on situations. Moreover, it uses temporal logic in combination with the non-monotonic logic to perform reasoning under time intervals with uncertainty.

### 4.3 Direct Trust Score Calculation

The Direct Trust Score (DTS) is calculated for each node in the network based on the following two groups. When a node sends their acknowledgement to the neighbour nodes, after receiving the message packets it is considered as Group-1 node which is a genuine node. When a node drops one or few packets, it is considered as Group-2 node and will be subject to analysis further based on the network congestion level, type of application and spatio-temporal

constraints. If a node drops packets very frequently even in scenarios where there is no congestion, such nodes can be black listed those put in Group-3. The trusted routing technique will choose only Group-1 nodes for important applications and both Group-1 as well as Group-2 nodes for normal applications.

The trust score (TS) for Group-1 is calculated using Eq. (3)

$$TS_{G1j} = \left[(ACKP/RP) * 100\right] + f(t1, t2, s) \tag{3}$$

where $TS_{G1j}$ is the Trust score of node $j$ when it is group-1, $ACKP$ is the number of acknowledgement packets sent and $RP$ is the count (number) of packets received from the neighbours.

Moreover,

$$\begin{aligned} &TS = 1; \quad \text{if} \quad TS_{G1j} \geq 1, \\ &\qquad \text{else TS} = TS_{G1j} \\ &\text{f(t1,t2,s)} = \text{s; if} \quad \text{t1} = \text{t2} \\ &\text{else} \quad \text{f(t1,t2,s)} = \text{t1} - \text{t2}; \quad \text{if} \quad \text{t1} \geq \text{t2} \\ &\text{else} \quad \text{f(t1,t2,s)} = \text{t2} - \text{t1}; \quad \text{if} \quad \text{t1} < \text{t2} \end{aligned}$$

The trust score for Group-2 is calculated using Eq. (4).

$$TS_{G2j} = \left[100 - ((NDP/TDP) * 100\right] + f(t1, t2, s) \tag{4}$$

where $TS_{G2j}$ is the Trust score of node $j$ when it is group-2, $NDP$ is the count of packets dropped, $TDP$ is the overall sum (total) of packets dropped in the network. For every t1, t2∈TC, where TC is the set of time points satisfying the interval comparison operators defined by Allen [43] for before (t1,t2), after (t1,t2), overlaps (t1,t2), meets (t1,t2) and their inverse operations. This computation provides an initial value of $TS_{G2j}$. Now, TS = $TS_{G2j}$ if this value ≥ 1 and the Group-2 node is allowed to take part in the current communication. Otherwise, add constraints c1, c2, …, cn to the temporal constraints and re-compute the value of $TS_{G2j}$ and find the TS value. If the new value of TS is greater than the old value of $TS_{G2j}$ then the node is allowed to take part in the communication. This process is repeated till all the possible constraints are applied and checked. If the TS value does not improve under non-monotonic reasoning process used above, the node is isolated and transferred to Group-3.

If a node has a trust score < threshold, then the node is found to drop greater than 50% of packets. Hence, the node is put into Group-3 and is not allowed to take part in the communication at all situations.

The Final Trust Score of node j is calculated using Eq. (5).

$$\begin{aligned} &FTS_j = \frac{\left(TS_{G1j} + TS_{G2j} + TS_{G3j}\right)}{3}, \quad \text{if} \quad t1 < t \leq t2,\ s1 < s \leq s2, \\ &\text{else} \quad FTS_j = \frac{\left(TS_{G1j} + TS_{G2j} + TS_{G3j}\right)}{6} \end{aligned} \tag{5}$$

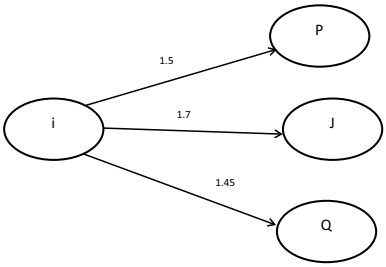



**Fig. 2** Sample network to compute RTS

**Table 2** Recommendation trust score computation

| From node i | RTS from its neighbours | RTS |
|---|---|---|
| P | jp – 0.7 | 0.8 |
| | qp – 0.8 | |
| J | pj – 0.9 | 0.9 |
| | qj – 0.75 | |
| Q | pq – 0.8 | 0.8 |
| | jq – 0.77 | |

The Direct trust score of a node *j* in node *i* is denoted as

$$DTS_{ij} = FTS_j \tag{6}$$

where $DTS_{ij}$ is the direct trust score of node *j* in node *i*.

### 4.4 Recommendation Trust Score Calculation

Recommendation Trust Score (RTS) is used in this work for computing the trust of nodes based on the neighbour information. Therefore, a node gets the recommendation trust value about a node from different neighbours. A node assigns trust values based on their own experience with their neighbour nodes. The trusted node gets the recommendation trust value from its neighbours. The threshold value *Th* is set by trust or using Eq. (7) which is the average value of the all the trust score received from the nodes. The trusted node considers the recommendation trust values of a node from their neighbour nodes which are above the threshold value.

$$Th = \sum_{i=1}^{n} TS_i/n \tag{7}$$

where *Th* is the threshold value used in this model and n is the number of nodes present in the network.

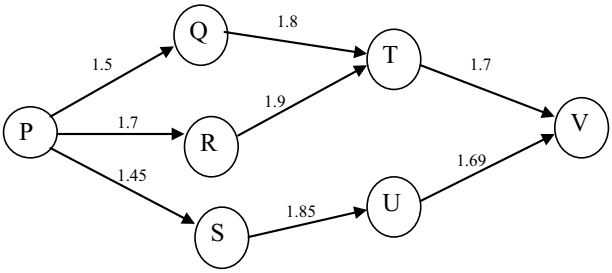



**Fig. 3** Path trust score evaluation

After eliminating the recommendation values, if more than one recommendation values are selected then the trusted node takes the maximum recommendation trust value using Eq. (8)

$$RTS_{ij} = \max\left\{RTS_{wj}\right\} \tag{8}$$

where w is the neighbours of j.

Figure 2 shows the part of the network to calculate the recommendation trust score.

Here, we assign the direct trust score for the nodes p, j and q near the node i as 0.7, 0.8 and 0.65 respectively. We also assume the threshold value as 0.6 and the recommendation trust scores are shown in Table 2.

### 4.5 Node Authentication

Let G be a cyclic group with generator g and is formed with n members who are given an identification number using the following formula:

$$\text{ID(i)} = \text{user ID(i)}||\text{IP address(i)}||\text{group member ID(i)}$$

where, group member ID (i) = user ID (i) mod p, p is a prime number which takes the values of the members of the cyclic group G.

AU_ID(i) = E(ID(i), k(i)), where k is a key generated by the group coordinator. The group key K = (k1 × k2 × ⋯ × kn) in which the product of kj where i ≠ j is provided by the group coordinator. The group member must find the value of K using his k(i) value and it is verified by the co-ordinator before allowing the encryption. The encrypted AU_ID(i) value must be used in all the communications by every node in order to show that the particular node is a genuine node.

### 4.6 Overall Trust Score

In this section, the Overall Trust Value (OTV) of a node is calculated using Eq. (9) after receiving the direct trust score and the recommendation trust score. If node is authenticated then

$$OTV_{ij} = DTS_{ij} + RTS_{ij} \tag{9}$$

else, the Overall Trust value is assigned the value of 0.

Then the Overall Trust value from node i to p, j and q are obtained as 1.5, 1.7 and 1.45 respectively and it is shown in Fig. 3.

### 4.7 Path Trust Score Evaluation

The route has been selected based on the overall trust values of the nodes present in the network including the start node, sink node and the intermediate nodes. The sum of the overall trust values (OTV) of the route is the path trust score ($PTS_{sd}$)as given in Eq. (10).

$$PTS_{sd} = \sum_{\substack{s \le i \le d-1 \\ j=i+1}} OTV_{ij} \tag{10}$$

If multiple paths are available between the source and the destination, then those routes path trust score are greater than the threshold value (*Thres*) will be selected. The *Thres* is the average value of the total trust score of all the nodes in the network.

$$Thres = \sum_{\substack{i=1 \\ j=i+1}}^{n} OTV_{ij}/n \tag{11}$$

In Fig. 3, the $OTV_{PQ}$ is 1.5 and the trust score of the path P(PQTV) is 5.0 (i.e. $PTS_{PV} = OTV_{PQ} + OTV_{QT} + OTV_{TV} = 1.5 + 1.8 + 1.7 = 5.0$). From Fig. 3, it can be seen that there are three different routing paths from P to V are available. Assume the *Thres* value as 5.1 and among these routes, the route P(P,R,T,V) is the most trustworthy route since its path trust score is greater than the *Thres* value.

### 4.8 Secured Qos Aware Energy Efficient Routing Algorithm

The main objective of developing this SQEER algorithm is the construction of the energy efficient tree with trusted path for transmitting the packets from source to sink. The proposed SQEER algorithm is an enhancement of the existing QEER [3] algorithm. In addition to the QEER algorithm, SQEER algorithm provides the secured path for the effective transmission. The proposed SQEER algorithm works in 3 phases. In the first phase, the tree is constructed from the source to sink. The sink node initiates the tree construction according to [3]. In the second stage, the cluster head selection is made using the proposed algorithm and the steps are given in Algorithm 1.

**Algorithm 1: Trust based Energy Efficient Cluster Head selection**

***Input*** *: S - set of nodes in a cluster*

***Output*** *: Elected cluster head (u)*

***Step 0:*** *Assign the trust score to 0 for all the nodes.*

***Step 1:for each*** *node in S calculate the Overall Trust value (OTV) using equation (6), (8) and (9).*

***Step 2: for*** *i := 1 to S*

***Step 3:*** ***if*** *OTV(i) < Th* ***then*** *remove it from the cluster // malicious node*

***Else***

***Step 4:*** *Assign_ role ( i , CH)*

***Step 5:*** *Announcement(Event_ detection)*

***Step 6: for*** *j : = 1 to* $N_i$ *//Ni – The Neighbors of node i*

***Step 7:*** ***if*** *OTV(j) < Th* ***then*** *remove it from the cluster // malicious node*

***else***

***Step 8: if*** *i <> j*

***Step 9.1****: if (Hop_Count(i) > Hop_Count(j)) and (*$Coord_{prob}$*(i) <= *$Coord_{prob}$* (j)) and (OTV(i) <OTV(j))****then***

***Step 9.1.1****: Assign (Role( i ), Member)*

***End if***

***Step 10:endfor***

***Step 11:if*** $role_i$ *= CH* ***then***

***Step 12:*** *Add(NID(i), Cluster_Head set( C))*

***End if***

***Step 13: endfor***

***Step 14:*** *Node u with maximum* $Coord_{prob}$ *and maximum trust score in the set C will form the Cluster Head.*

***Step 15:*** *Announce Cluster_Head_condition*

***Step 16:*** *Other_nodes( C –Members_ of_ the_ cluster)*

The algorithm works as follows. Once the cluster is formed, the overall trust score for each node is calculated and the malicious nodes are removed from the cluster. Then the node with minimum hop count, maximum $Coord_{prob}$ [3] and maximum trust score is selected as a cluster head. In the case of tie break, the node with maximum $Coord_{prob}$ and maximum trust score is selected as a cluster head.

### 4.9 Trust Based Secure Routing Algorithm

The final stage of the proposed work is the route establishment. The cluster members in a cluster transmit the collected information to the cluster head. Moreover, the cluster head node gathers the information from participant nodes and transmits to the sink. If the sink is within the transmission range of the cluster head then it transmits the collected information directly to the sink. Otherwise, it sends through the relay nodes. Here, the selection of the relay nodes is very important. The wrong selection of relay nodes may leads to minimum network lifetime. The steps of the proposed algorithm are shown in Algorithm 2.

**Algorithm 2: Trust based Secure Routing Algorithm**

***Step 1:****Source node s discovers the path to the destination d.*

***Step 2****: For each path calculate the PTS (Path Trust Score) from source to destination using equation (10)*

***Step 3:*** ***If*** $PTS_{sd} > Thres$ ***Then***

***Step 4:*** *Add this route to the qualified route set Q*

***Step 5: Endif***

***Step 6: End for***

***Step 7: If*** *more than one route in Q,* ***then***

***Step 8:*** *Select the route with maximum energy and minimum hop count as a final route from source s to destination d*

In this protocol, a source node (i.e. cluster head) selects the trusted path based on the path trust value. If more than one path has the path trust value greater than *Thres* value, then the path with maximum energy and minimum hop count to the base station will be selected as a final route.

## 5 Results and Discussions

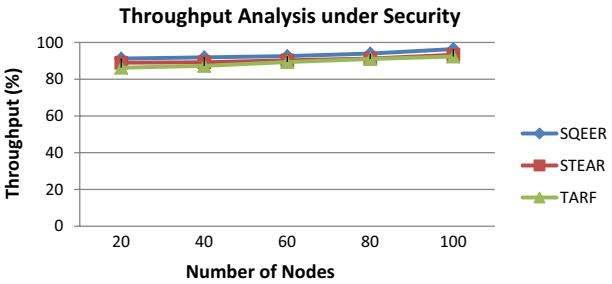
The proposed algorithm SQEER had been simulated by using the NS2 simulator. The parameters used for simulation are shown in Table 3. The sensor nodes have been deployed randomly over a region of $200 \times 200$ $m^2$. The sensors nodes are varying from 20 to 100 are deployed with the initial energy of 0.5 J. The proposed algorithm is evaluated and its performance is compared with QEER, STEAR and TARF algorithms. Comparison is also made with the trust based secured routing algorithm SQEER and without trust based secured routing QEER.

The throughput of the system is evaluated with different algorithms. Figure 3a, b show the throughput of the network. The throughput of the system increases as the number of nodes increases. It is clear from both the figures that the throughput of the proposed model is higher than the other algorithms.

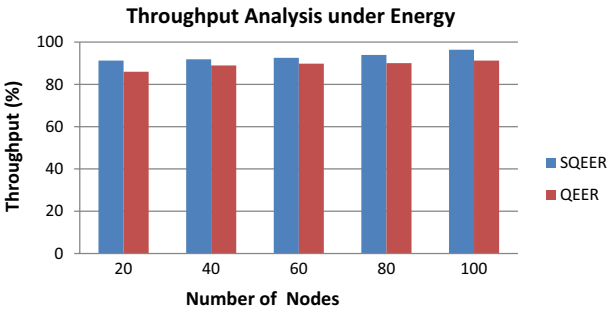
**Table 3** Simulation parameters

| Parameter_ name | *Parameter_Value* |
|---|---|
| Network_Area | 200 m × 200 m |
| Nodes Deployed | 100 nodes |
| Initial_energy | 0.5 J |
| $E_{elec\_value}$ | 50 nJ per bit |
| $\varepsilon_{fs\_value}$ | 10 pJ per bit per $m^2$ |
| $\varepsilon_{mp\_value}$ | 0.0013 pJ per bit per $m^4$ |
| Packet_size | 4000 (bits) |

**Fig. 4** Throughput



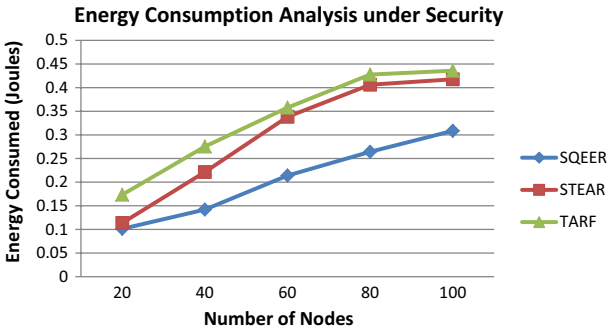

**(a)** Throughput comparison with secured routing algorithms



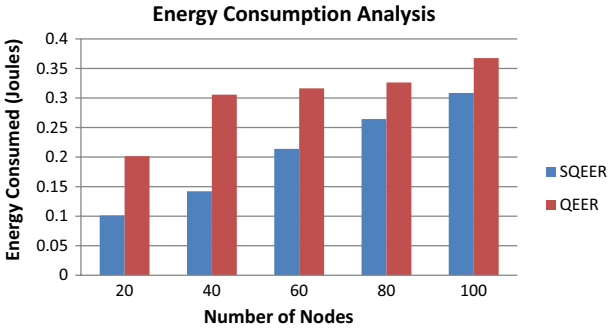

**(b)** Throughput analysis for cluster based routing

In Fig. 4a, the throughput of the STEAR algorithm is better than the TARF algorithm. But the throughput of this proposed algorithm has been proved to be better when compared to the other existing algorithms. The justification behind is in the proposed work the cluster head chooses the relay node based on the hop_count, residual_energy and the trust score. The malicious nodes are identified with the threshold value and only the normal nodes participate in the cluster formation and routing. In Fig. 4b, the throughput of the proposed work is higher than the other. The reason is in the QEER algorithm the relay nodes are selected based on the residual energy and hop count. Here the malicious nodes are not identified. This cause is loss of more packets. But in the SQEER algorithm, malicious nodes are identified thus reduce the loss of packets.

Figure 4a, b show the energy consumption of the sensor nodes in the network. It is observed from the figures that the energy consumption of the system is increasing when the number of nodes is increasing. In these figures, it is shown that the energy consumption




**(a)** Energy Comparison with secured routing algorithms




**(b)** Cluster Based Energy Efficient Routing Algorithms

**Fig. 5** Energy consumption analysis

of the proposed work is less than the energy consumption of other algorithms. The reason is more energy is optimized in the proposed model by using the cluster technique and rules (Fig. 5).

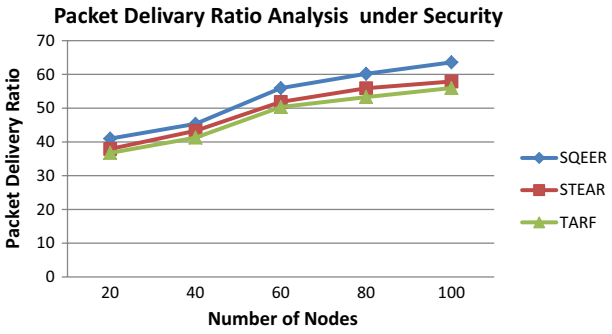
Figure 6a, b show the packet delivery analysis of the proposed system. In both the diagrams the SQEER gives better performance than the existing algorithms. The reason is in the SQEER, cluster formation and trust based secure routing are performed. This proposed work identifies the malicious nodes very effectively and it results in transmission of more number of packets.

Figure 6 shows the number of malicious packets captured in SQEER algorithm. The five experiments are conducted by increasing the number of nodes from 20 to 100. In all the experiments, the proposed algorithm effectively identifies the malicious packets when this model is compared with the other existing security models namely STEAR [20], TARF [18] and Active Trust Model [29].

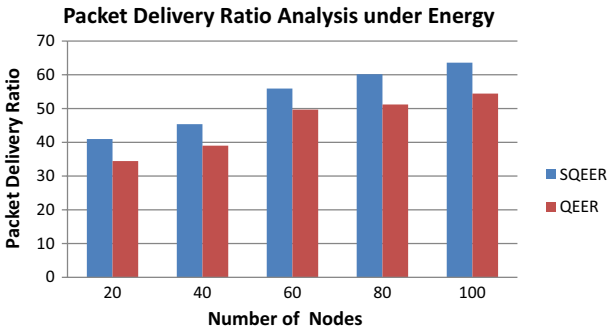
Figure 7 shows the comparison of number of malicious packets detected by various algorithms. From this figure, it is noticed that this proposed algorithm identifies the malicious nodes very effectively than the other algorithms. The reason behind this is that in the proposed work, the malicious nodes have been identified in the cluster formation as well as during routing.

Figure 8 shows the malicious nodes detection ratio. From this figure, we can see that the accuracy of detecting the intruding nodes in the proposed work is higher than the other algorithms. The reason is that evaluation of the trust score is based on group-1, group-2 types of nodes, individual trust value as well as the path trust value.

**Fig. 6** Packet delivery ratio

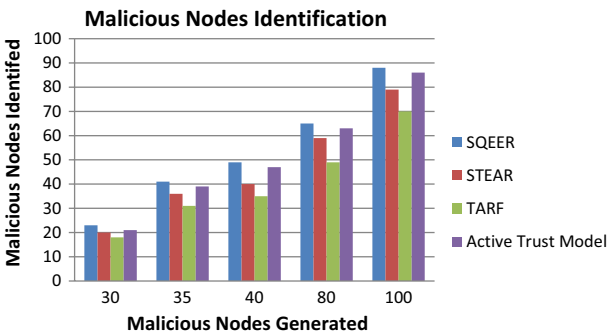



**(a)** Packet Delivery Ratio Analysis under Security




**(b)** Packet Delivery Ratio Analysis under Energy

**Fig. 7** Comparison of malicious nodes detection of various algorithms




## 6 Conclusion

In this paper, a novel secured and energy efficient routing technique named Secure and QoS aware Energy Efficient Routing (SQEER) has been proposed for effective routing in WSNs. In this model, the trust scores are used for selecting the genuine node which acts as a cluster head in a cluster and is used to identify the malicious nodes. All routing tasks are carried out only through the genuine nodes which are energy efficient and close to the sink. Moreover, special trust score evaluation techniques have been proposed for enhancing the

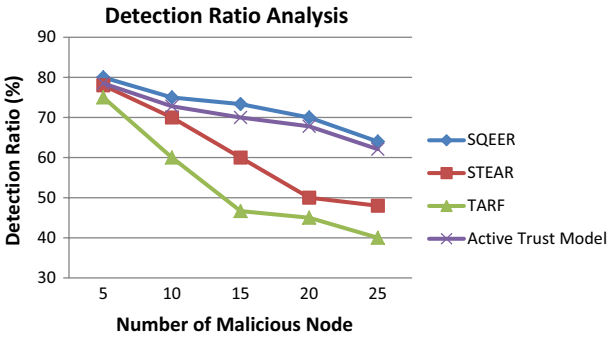



**Fig. 8** Detection accuracy analysis of various algorithms

security. The proposed algorithm has been assessed using simulations. From the experiments conducted, it has been noted that our proposed algorithm has shown better performance in terms of throughput, delay and packet transmission when compared to related algorithms. The main advantages of this proposed secured routing algorithm includes the change in the cluster formation with the genuine nodes, increase in malicious node detection accuracy, removal of malicious nodes and improvement in the routing performance. Future works on this model is the application of fuzzy rules for handling uncertainty.

## References

1. Munuswamy, S., Saravanakumar, J. M., Sannasi, G., Harichandran, K. N., & Arputharaj, K. (2018). Virtual force-based intelligent clustering for energy-efficient routing in mobile wireless sensor networks. *Turkish Journal of Electrical Engineering & Computer Sciences, 26*(3), 1444–1452.
2. Ayyasamy, A., & Venkatachalapathy, K. (2015). Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. *Wireless Networks, 21*(2), 421–430.
3. Logambigai, R., & Kannan, A. (2014). QEER: QoS aware energy efficient routing protocol for wireless sensor networks. In *IEEE 6th international conference on advanced computing (ICoAC)* (pp. 57–60).
4. Viswanathan, S., & Kannan, A. (2019). Elliptic key cryptography with Beta Gamma functions for secure routing in wireless sensor networks. *Wireless Networks*. https://doi.org/10.1007/s11276-019-02073-9.
5. Baraa, A. A. (2011). Energy-aware evolutionary routing protocol for dynamic clustering of wireless sensor networks. *Swarm and Evolutionary Computation, 1*(4), 195–203.
6. Villas, L. A., Boukerche, A., Ramos, H. S., de Oliveira, H. A. B. F., de Araujo, R. B., & Loureiro, A. A. F. (2013). DRINA: A lightweight and reliable routing approach for in-network aggregation in wireless sensor networks. *IEEE Transactions on Computers, 62*(4), 676–689.
7. Nakamura, E. F., de Oliveira, H. A., Pontello, L. F., & Loureiro, A. A. F. (2006). On demand role assignment for event detection in sensor networks. In *11th IEEE symposium on computers and communications (ISCC'06), Sardinia, Italy* (pp. 941–947).
8. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2010). Energy-efficient communication protocol for wireless microsensor networks. In *Annual Hawaii international conference, system sciences* (p. 10).
9. Younis, O., & Fahmy, S. (2004). HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 3*(4), 366–379.
10. Rahman, M. N., & Matin, M. A. (2011). Efficient algorithm for prolonging network lifetime of wireless sensor network. *Tsinghua Science and Technology, 16*(6), 561–568.
11. Mathapati, B. S., Patil, S. R., & Mytri, V. D. (2012). A cluster based energy efficient reliable routing protocol for wireless sensor networks. In *Proceedings on 1st international conference, ET2ECN* (pp. 1–6).

12. Kuila, P., & Jana, P. K. (2014). Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. *Engineering Applications of Artificial Intelligence, 33,* 127–140.
13. Logambigai, R., & Kannan, A. (2015). Fuzzy logic based unequal clustering for wireless sensor networks. *Wireless Networks, 22,* 1–13.
14. Wood, A., & Stankovic, J. (2002). Denial of service in sensor networks. *Computer, 35*(10), 54–62.
15. Kulothungan, K., Ganapathy, S., Indra Gandhi, P., & Yogesh, P. (2011). Intelligent secured fault tolerant routing in wireless sensor networks using clustering approach. *International Journal of Soft Computing, 6*(5), 210–215.
16. Ganapathy, S., Kulothungan, K., Muthuraj Kumar, S., & Vijayalakshmi, M. (2013). Intelligent feature selection and classification techniques for intrusion detection in networks: A survey. *EURASIP Journal on Wireless Communication and Networking, 271*(1), 1–16.
17. Kumar, S. V. N. S., & Palanichamy, Y. (2018). Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. *Wireless Networks, 24*(4), 1343–1360.
18. Zhan, G., Shi, W., & Deng, J. (2012). Design and implementation of TARF: A trust-aware routing framework for WSNs. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 184–197.
19. Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications, 105*(4), 1475–1490.
20. Thippeswamy, B. M., Reshma, S., Tejaswi, V., Shaila, K., Venugopal, K. R., & Patnaik, L. M. (2015). STEAR: Secure trust-aware energy-efficient adaptive routing in wireless sensor networks. *Journal of Advances in Computer Networks, 3*(2), 146–149.
21. Sethuraman, P., Tamizharasan, P. S., & Arputharaj, K. (2019). Fuzzy genetic elliptic curve Diffie Hellman algorithm for secured communication in networks. *Wireless Personal Communications, 105*(3), 993–1007.
22. Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. *International Journal of Distributed Sensor Networks, 10,* 1–14.
23. Gu, W., Dutta, N., Chellappan, S., & Bai, X. (2011). Providing end-to-end secure communications in wireless sensor networks. *IEEE Transactions on Network and Service Management, 8*(3), 205–218.
24. Murthy, S., D'Souza, R. J., & Varaprasad, G. (2012). Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks. *IEEE Transactions on Sensors Journal, 12*(10), 2941–2949.
25. Ganesh, S., & Amutha, R. (2013). Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. *Journal of Communications and Networks, 15*(4), 422–429.
26. Mahmoud, M. M., Lin, X., & Shen, X. S. (2015). Secure and reliable routing protocols for heterogeneous multihop wireless networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(4), 1140–1153.
27. Li, S., Zhao, S., Wang, X., Zhang, K., & Li, L. (2014). Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks. *IEEE Systems Journal, 8*(3), 858–867.
28. Lee, S.-B., & Choi, Y.-H. (2006). A secure alternate path routing in sensor networks. *Computer Communications, 30*(1), 153–165.
29. Liu, Y., Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
30. Xiong, H., & Qin, Z. (2015). Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Transactions on Information Forensics and Security, 10*(7), 1442–1455.
31. Kerrache, C. A., Calafate, C. T., Cano, J. C., Lagraa, N., & Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access, 4,* 9293–9307.
32. Hamdane, B., Boussada, R., Elhdhili, M. E., & El Fatmi, S. G. (2017). Hierarchical identity based cryptography for security and trust in named data networking. In *2017 IEEE 26th international conference on enabling technologies: Infrastructure for collaborative enterprises* (pp. 226–231).
33. Selvi, M., Logambigai, R., Ganapathy, S., Ramesh, L. S., Nehemiah, H. K., Arputharaj, K. (2016). Fuzzy temporal approach for energy efficient routing in WSN. In *Proceedings of the international conference on informatics and analytics* (pp. 117–122).
34. Selvi, M., Velvizhy, M., Ganapathy, S., Nehemiah, H. K., & Kannan, A. (2017). A rule based delay constrained energy efficient routing technique for wireless sensor networks. *Cluster Computing*. https://doi.org/10.1007/s10586-017-1191-y.

35. Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., & Kannan, A. (2017). An intelligent secured and energy efficient routing algorithm for MANETs. *Wireless Personal Communications, 96*(2), 1753–1769.
36. Umar, I. A., Hanapi, Z. M., Sali, A., & Zulkarnain, Z. A. (2017). TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks. *IEEE Access, 5,* 2550–2562.
37. Tang, D., Li, T., Ren, J., & Jie, W. (2015). Cost-aware secure routing (CASER) protocol design for wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(4), 960–973.
38. Thangaramya, K., Kulothungan, K., Logambigai, R., Selvi, M., Ganapathy, S., & Kannan, A. (2019). Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Computer Networks, 151,* 211–223.
39. Mhemed, R., Aslam, N., Phillips, W., & Comeau, F. (2012). An energy efficient fuzzy logic cluster formation protocol in wireless sensor networks. *Procedia Computer Science, 10,* 255–262.
40. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications, 1*(4), 660–670.
41. Guo, Q., Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Modeling and evaluation of trust in cloud computing environments. In *IEEE 3rd international conference on advanced computer control (ICACC 2011)* (pp. 112–116).
42. Xia, H., Jia, Z., Ju, L., Li, X., & Sha, E. H. (2013). Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. *Computer Communications, 36,* 1078–1093.
43. Allen, J. F. (1983). Maintaining knowledge about temporal intervals. *Communications of the ACM, 26*(11), 832–843.



**Thangaramya Kalidoss** completed her B.E. and M.E. degrees in Computer Science and Engineering from Anna University, Chennai. Currently, she is working as a Faculty in the Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai. Now, she is pursuing her Ph.D. research work in the area of Network Security. Her areas of interest include Computer Networks, Cryptography and Security, Database Management Systems and Programming languages.

**Logambigai Rajasekar** completed her M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai. Currently, she is working as a Faculty in the Department of Mathematics, College of Engineering Guindy, Anna University, Chennai. Her areas of interest include Computer Networks, Network Security and Cloud Computing. She has published more than 10 papers in reputed conferences and journals.

**Kulothungan Kanagasabai** completed his M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai. Currently, he is working as an Assistant Professor (SG) in the Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai. Now, he is guiding research scholars in the areas of Wireless Sensor Networks and Network Security. His areas of interest include Computer Networks, Information Security and Database Management Systems. He has published more than 50 papers in reputed conferences and journals.

**Ganapathy Sannasi** completed his M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai. Currently, he is working as an Assistant Professor (Sr) in the School of Computing Science and Engineering, VIT Chennai Campus, Chennai. Now, he is guiding research scholars in the areas of Cloud Computing and Network Security. His areas of interest include Computer Networks, Network Security, Data Mining and Programming languages. He has published more than 50 papers in reputed conferences and journals.

**Arputharaj Kannan** completed his M.E. and Ph.D. degrees in Computer Science and Engineering from Anna University, Chennai. Currently, he is working as a Senior Professor in the School of Computer Science and Engineering, VIT Vellore Campus. Now, he is guiding research scholars in the areas of Data Mining, Cloud Computing, Network Security and Artificial Intelligence. His areas of interest include Database Management Systems, Artificial Intelligence, Computer Networks, Network Security, Data Mining and Programming languages. He has published more than 300 papers in reputed conferences and journals. He has guided and completed 41 Ph.D. research scholars.

## Affiliations

**Thangaramya Kalidoss[1] · Logambigai Rajasekaran[1] · Kulothungan Kanagasabai[1] · Ganapathy Sannasi[2] · Arputharaj Kannan[3]**

Logambigai Rajasekaran
rlogambigai_14@yahoo.com

Kulothungan Kanagasabai
kulo.tn@gmail.com

Ganapathy Sannasi
sganapathy@vit.ac.in

[1] Department of Information Science and Technology, CEG Campus, Anna University, Chennai 600 025, India

[2] School of Computing Science and Engineering, Vellore Institute of Technology, Chennai 600 127, India

[3] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 600 127, India