Soft Computing (2020) 24:16483–16497
https://doi.org/10.1007/s00500-020-04955-z

METHODOLOGIES AND APPLICATION

Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN

K. Thangaramya[1] · K. Kulothungan[1] · S. Indira Gandhi[2] · M. Selvi[3] · S. V. N. Santhosh Kumar[4] · Kannan Arputharaj[3]

Published online: 23 April 2020

Abstract
In wireless sensor networks (WSNs), energy optimization and the provision of security are the major design challenges. Since the wireless sensor devices are energy constrained, the issue of high energy consumption by the malicious nodes must be addressed well in order to enhance the network performance by making increased network lifetime, reduced energy consumption and delay. In the past, many researchers worked in the provision of new techniques for providing improved security to WSN in order to enhance the reliability in the routing process. However, most of the existing routing techniques are not able to achieve the required security through the use of intelligent techniques for safeguarding the sensor nodes from malicious attacks. In order to address these problems, a new fuzzy temporal clustering-based secured communication model with trust analysis and outlier detection has been developed in this research work. For this purpose, a new fuzzy temporal rule-based cluster-based routing algorithm with trust modelling and outlier detection for monitoring the nodes participating in the communication has been proposed. In addition, a fuzzy temporal rule- and distance-based outlier detection algorithm is also proposed in this paper for distinguishing the malicious nodes from other nodes within each cluster of the network and has been used in the secured routing algorithm. The proposed secure routing algorithm uses the temporal reasoning tasks of explanation-based learning and prediction as well as spatial constraints for making efficient routing decisions through the application of trust and key management techniques for performing effective authentication of nodes and thereby isolating the malicious nodes from communication through outlier detection. By applying these two proposed algorithms for communication in the proposed work, it is proved through experiments that the proposed secure routing algorithm and the outlier detection algorithm are able to perform secured and reliable routing through genuine cluster head nodes more effectively. Moreover, these two algorithms provide improved quality of service with respect to the reliability of communication, packet delivery ratio, reduction in end-to-end delay and reduced energy consumption.

Keywords Fuzzy rules · Trust score · Energy efficiency · Secure routing and cluster-based routing · Temporal reasoning · Wireless sensor networks

Communicated by V. Loia.

✉ S. V. N. Santhosh Kumar
santhoshkumar.svn@vit.ac.in

K. Thangaramya
thangaramyaramya112@gmail.com

K. Kulothungan
kulo@auist.net

S. Indira Gandhi
indira@mitindia.edu

M. Selvi
selvi.m@vit.ac.in

Kannan Arputharaj
Kannan.a@vit.ac.in

[1] Department of Information Science and Technology, CEG Campus, Anna University, Chennai 600025, India

[2] Department of Electronics Engineering, MIT Campus, Anna University, Chennai 600044, India

[3] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

[4] School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India

1 Introduction

In the recent years, sensor networks are used in many day-to-day applications. Moreover, these wireless sensor networks (WSNs) are made of tiny devices called sensor nodes which have low battery power, minimum computing capacity and limited memory for data storage. Such sensor nodes are deployed in a systematic way or randomly in a geographical terrain for effective sensing of the environment to perform data collection and also to communicate the collected data to the sink node (base station) through the application of effective routing algorithms. In such a scenario, the sensor nodes must route the gathered data through other sensor nodes which are connected through wireless links to the base station. Moreover, many routing protocols are present in the literature on WSN for performing the routing process. Among them, intelligent cluster-based routing protocols are able to route the packets with minimum number of network hops. However, the decisions that are made in the routing process require complete information about the network topology. This is possible only in the scenario where the nodes are static. On the other hand in a mobile sensor network, the sensor nodes move from one place to another in order to provide extended coverage area and fast data collection. Therefore, a new routing protocol which can take efficient decisions even under mobility and uncertainty with respect to security, data collection and communication is necessary to enhance the network performance. This can be achieved by proposing an intelligent cluster-based secure routing algorithm which can make more efficient decisions on routing and security with respect to data collection, routing, trust analysis and outlier analysis under uncertainty.

Fuzzy logic provides facilities for handling uncertainty occurring in communication through the effective gradation of truth values using rules and by converting the quantitative information into qualitative information (Zadeh 1965). A system performs deductive inference more effectively by the application of fuzzy rules. In this scenario, the combination of fuzzy logic with other higher order logics such as temporal logic, non-monotonic logic and modal logic helps to infer new knowledge from the facts and rules available in the knowledge base through rule firing. In network security, trust is an important security parameter which analyses the traffic and node behaviour and assesses the risk involved in the communication of data through untrusted nodes (Bao et al. 2012; Das and Islam 2012; Shaikh et al. 2009). Moreover, the combination of trust modelling and fuzzy inference is useful to make more accurate security decisions through authentication, key management and isolation of malicious node from the communication. In the past, many researchers have discussed about the application of trust management systems and reputation-based systems in order to maintain the integrity and also to detect the attacks carried out by both inside attackers and outside attackers (Ganeriwal et al. 2008). Such systems when integrated with fuzzy rules, temporal constraints and outlier detection using classification algorithms will enhance the security of data communication in WSNs (Logambigai and Kannan 2016).

Temporal mining consists of important tasks namely searching for temporal patterns from datasets, classification and clustering of temporal data in order to analyse the past data and prediction of the future behaviour for making more effective decisions. In the past, many researchers worked in the areas of temporal reasoning for efficient decision making through data analysis in many applications including medical diagnosis systems, intrusion detection systems, market trend analysis and fraud analysis in financial applications (Dean and McDermott 1987). For this purpose, Allen (1983) proposed an interval algebra that analyses the dependencies between time intervals and provides operators for performing temporal reasoning through explanation-based learning and predictive analysis (Russell and Norvig 1994). Later, many researchers applied Allen's interval algebra and also proposed new temporal reasoning techniques through the development of temporal constraint networks, discriminant networks and fuzzy temporal cognitive maps (Sethukkarasi et al. 2014; Kosko 1986).

In a cluster-based routing protocol, the data are sent through a shortest and multi-hop optimal routing path. In multi-hop routing, all nodes tend to loose their energy if each of the sensor nodes has to transmit their data to the base station and take part in the routing process by sending their data to the base station through other intermediate nodes. These nodes consume energy for data collection, forwarding of data and analysis of data packets. Therefore, the optimization of power is an important performance metric to be considered in the design of WSN. Since the sensor nodes are operating using limited battery power, it is necessary to optimize the energy consumption by these nodes for routing the data packets.

The use of energy by sensor nodes can be minimized by using clustering and performing cluster-based routing. In this method, the cluster head (CH) selection process is carried out and then task of routing through CHs is performed where uncertainty is handled using rules. In such a scenario, the cluster heads must be with higher energy, lower mobility and highly trusted nodes. In order to select cluster heads and to perform routing through cluster heads, many different algorithms are available in the literature (Izadi et al. 2015; Lin et al. 2015). However, most of the cluster-based routing algorithms consider the formation of

equal size clusters and do not detect the outliers which are not performing the routing operations like other normal nodes. Such nodes may be attackers or the nodes may perform malicious activities (Donald et al. 2015). However, a good secure routing algorithm must perform outlier detection, and then, it must isolate the outlier nodes even in intra-cluster routing. In this way, it is possible to increase the security of communication leading to increase in the reliability of communication.

A clustering algorithm groups the related data items into a single cluster and forms a set of clusters by forming individual clusters (Han et al. 2011). In such a scenario, the data item which cannot be included in any of the clusters is called as outlier (Hodge and Austin 2003). In network communication, outliers are the nodes with anomalous behaviour whose properties with respect to packet forwarding, energy consumption and cooperation in communication will be different from the rest of the nodes that are members of some clusters. In cluster-based secure routing algorithms, outlier detection is one of the most important and fundamental tasks that are implemented through cluster analysis, classification, temporal analysis and association rule mining (Moonesignhe and Tan 2006). In this work, a new distance- and behaviour-based outlier detection algorithm is proposed to identify the outliers based on distance, trust scores and behaviour analysis and the malicious nodes are identified by the proposed outlier detection algorithm more effectively using fuzzy rules and temporal constraints in the clustering and cluster-based routing process. The major contributions of this paper are as follows:

1. First, a new security model has been developed in this work for providing secured communication based on fuzzy temporal rules, clustering, trust management and outlier detection.
2. Second, a new fuzzy temporal rule-based cluster-based routing algorithm with trust modelling and outlier detection (FTRCRA-TO) has been proposed in this paper for effective monitoring of the behaviour of the sensor nodes that are participating in the data collection and routing process.
3. Third, a fuzzy temporal rule- and distance-based outlier detection algorithm (FTRDODA) has been proposed in this work which is capable of detecting the malicious nodes by outlier detection anomalous behaviour analysis.
4. Fourth, temporal rules have been used to check the dynamic behaviour of nodes due to mobility and communication with other nodes. This helps to identify the malicious patterns and enables the system to predict the future behaviour of nodes.
5. A new trust model and security analysis techniques have been proposed in the design of the secure routing algorithm that performs the temporal reasoning tasks of explanation of the past, learning new rules and forecasting the future behaviour of nodes and to isolate them through outlier detection and trust analysis.
6. Finally, new authentication techniques are proposed to enhance the security of communication by incorporating key management, encryption and decryption techniques.

The major advantages of the proposed model include the increase in packet delivery ratio, network throughput, reduction in delay and reduced energy consumption. This model has been tested through simulations using NS-3 simulator and also using real network scenario in the network test bed, and the verification of the algorithms proposed in this research work is explained in this paper.

The rest of this paper is formulated as shown below: Sect. 2 presents the related works in the area of cluster-based secured routing protocols in WSNs. Section 3 portrays the architecture of the secured routing system discussed in this paper. Section 4 describes the novelties of the proposed secured routing model and explains the outlier detection algorithm and secure routing algorithms for enhancing the communication security. Section 5 provides the results obtained from this work and also provides suitable discussions. Section 6 gives relevant conclusions to this research work and highlights some possible future enhancements.

2 Related works

Many works have been carried out in the past by different researchers who worked in the areas of cluster-based routing, fuzzy rule-based clustering, temporal mining and secure routing algorithms for WSNs (Shiva Murthy et al. 2012; Dang and Wu 2010; Mahmoud et al. 2015). Among them, Shiva Murthy et al. (2012) proposed a new multipath secure routing algorithm for WSN using the digital signature algorithm for authenticating the nodes before they are allowed to take part in the routing process. This model increases the security in the routing process leading to an increase in reliability of data delivery. Mahmoud et al. (2015) developed a novel secure routing protocol where the authors used the signal-to-noise ratio as the metric for forming and measuring clusters. In their work, the authors introduced a new error recovery process for enhancing the reliability of communication. One important contribution of these authors is the proposal of a security model which is used to isolate the malicious nodes by using a new technique called signal-to-noise ratio based dynamic clustering.

Lee and Choi (2006) introduced a new secured routing algorithm by combining two prominent security models namely, the payment model and the trust model for providing energy-aware routing. Moreover, the trust values of nodes in their models are evaluated by the payment system and it rewards the nodes which relay the packets of other nodes based on their trust values. This model is useful to enhance the overall network security through the application of optimal cost modelling.

Li et al. (2014) developed a novel fault-tolerant routing protocol that provides energy efficiency and satisfies the quality of service (QoS) requirements and the authors used a path vacant ratio which is used to assess and locate an alternate arrangement for the connection disjoint paths from all the access paths. Moreover, the authors proposed new algorithms for efficient congestion control and load balancing. Liu et al. (2016) proposed a secured alternate path-based routing algorithm for WSNs. Their model is capable of detecting and isolating the malicious nodes by applying the security information received from the neighbour nodes. Liu et al. (2016) designed a trust model which consists of two components namely active trust modelling and secure routing model for improving the efficiency of communication through the trusted nodes in the network. Kerrache et al. (2016) proposed a remote authentication-based security modelling approach for enhancing security using digital certificate-less encryption scheme. In their model, a certificate revocation scheme is also proposed for enhancing the security features through the remote authentication. Kerrache et al. (2016) explained about the main threats in trust models by introducing an adversary model and by comparing the features of various trust models for enhancing the network security. In their survey, the authors explained the uses of trust modelling and cryptographic techniques with respect to the enhancement of security in communication more effectively. Hamdane et al. (2017) detailed the security models based on trust computations which are used for securing the networks. Moreover, the authors also proposed a new hierarchical identity-based cryptographic technique for performing effective signature verification. Their model is useful for enhancing security through the proposal of effective techniques for key generation, signature formation and signature verification. Thangaramya et al. (2019) suggested the use of neuro-fuzzy rules for carrying out the routing process in WSNs. The main advantage of their algorithm is the reduction in energy consumption during the routing process. Moreover, Mazinani et al. (2019) proposed an intelligent fuzzy multi-cluster-based routing protocol which performs effective and energy-efficient routing in WSNs (Santhosh Kumar and Palanichamy 2018). Sethukkarasi et al. (2014) proposed a new knowledge representation technique based on neuro-fuzzy modelling with temporal constraints by extending the fuzzy cognitive maps for mining temporal patterns. This model is able to predict the diabetics level more effectively by the application of fuzzy temporal rules. Jaisankar et al. (2012) proposed an intelligent intrusion detection system using the fuzzy rough sets for identifying the malicious nodes through the detection of outliers more effectively in the networks. Logambigai et al. (2018) proposed an energy-efficient and cluster-based clustering approach which is working in a hybrid manner for transmitting the data between the source and destination. Kim et al. (2007) introduced an energy-efficient routing protocol by extending the low-energy adaptive clustering hierarchy (LEACH) protocol for performing effective data communication between the nodes in WSNs (Sun et al. 2019). Muthurajkumar et al. (2017) proposed a new secured and energy-efficient routing protocol which uses intelligent agents for enhancing the data communications in mobile ad hoc networks. Their secure routing protocol achieved better performance in terms of attack detection accuracy and network lifetime with less energy consumption. Logambigai et al. (2018) introduced a grid-based energy-efficient routing algorithm for providing effective data communications between the nodes in WSNs. Here, the authors have used fuzzy rules for making an effective decision on the node communication process. They have achieved better performance in terms of network lifetime and packet delivery ratio with reduced energy consumption.

Weichao et al. (2009) improved the standard cluster-based routing protocol called LEACH with the incorporation of the trust scores for the various nodes in WSN. They have achieved better performance in terms of network lifetime and security. Duan et al. (2011) discussed the issues of trust management for nodes in mobile wireless sensor networks that improved the security of the networking system. Miglani et al. (2015) enhanced the existing LEACH protocol with the introduction of trust management and energy optimization techniques. Their model achieved better performance in terms of less energy consumption, reduced delay, and improved packet delivery ratio and network lifetime. Deng et al. (2010) proposed a new trust-aware routing algorithm for WSN. Their algorithm is able to route the data packets dynamically according to the current trust scores of the participating nodes in WSNs. They have achieved better security when compared with other existing routing algorithms. Ayadi et al. (2017) provided a survey of works on outlier detection and provision of security in wireless sensor networks. Moreover, the authors presented a comparative analysis and suggested methodologies for node selection in WSN during cluster formation and routing. Shamim Hossain et al. (2019) developed a new multimedia sensor network application in order to reduce the delay in communication.

Moreover, they focussed on the optimization of energy consumption and improvement in network performance. They developed techniques for multipath routing in order enhance the quality of service (QoS) in WSN by applying effective planning methods has very high requirements for the end-to-end transmission delay. Mazinani et al. (2019) proposed a fuzzy multi-cluster-based routing algorithm with a constant threshold for energy optimized routing in WSN. Their model used clustering and performed cluster-based multi-hop routing for sending the data collected by the nodes to the base station. They focused on increasing the network lifetime by reducing the number of transmissions by selecting suitable nodes as cluster heads. They compared their results with other related algorithms, and they established that they have improved the network performance through their model by the application of fuzzy rules. Anwar et al. (2019) proposed a security model through trust computation and established that the use of trust scores for making decisions has improved the reliability of communication. They explained that the detection of malicious nodes using trust values enables the routing algorithm to isolate the malicious nodes from communication with other genuine nodes, and hence, the attackers are prevented from carrying out malicious activities in the network leading to increase in energy consumption. Gilbert et al. (2018) proposed new techniques for prediction of attacks using time series model based on autoregression and trust analysis. Their model is able to predict the attackers in advance, and hence, it is able to secure the communication more efficiently. However, they focused on energy efficiency by considering compressed sensing and relay selection instead of focussing more on the routing process. Sree Rathna Lakshmi et al. (2017) proposed a new architecture for wireless sensor networks and explained about the QoS-based routing algorithm developed by them. They considered the issues namely mobility, link failure, routing overhead and packet delivery ratio in order to improve the network performance. Fawzy et al. (2013) proposed a new model for secure routing through outlier detection, and they prevented the communication of noisy data in order to increase the security of communication. Moreover, they performed knowledge extraction for identifying the malicious users and measured the amount of data collected and sent by nodes in order to measure the packet drop rate at nodes that are present in the WSN. Their model is useful to enhance the security and to improve the data collection and delivery process. Thangaramya et al. (2019) proposed a new routing algorithm for the WSNs that are used in the effective design of Internet of Things (IoT). In their model, they focussed on fairness, data collection and energy optimization in order to perform effective QoS-based routing. Through the experiments carried out in their work, the authors have proved that their model optimizes the energy consumption, reduces the delay and increases the network performance. Jabeen and Fernandes (2012) explained the design of intelligent WSN by considering spatial constraint, network topologies and the geometries involved in the network area. Their model is useful for node deployment and to observe the behaviour of the network based on temporal and spatial constraints.

Alshammari et al. (2018) developed an outlier detection method for solving security problems in wireless sensor networks. In their model, they proposed a new technique called nonnegative matrix factorization method to solve the security problems through outlier detection and statistical methods in various domains like agriculture monitoring, health care and security of data communication for providing reliable communication. Saeed et al. (2019) explained about the model developed by them for underwater communication by the use of sensors in optical wireless sensor networks. They also proposed a geographical routing algorithm along with a method for outlier detection for optimizing the placement of anchors in order to enhance the network performance and security. Shahid et al. (2012) used support-vector machines (SVM)-based classification algorithm for performing outlier detection in WSN. Their model is useful to detect the malicious nodes and to isolate them for performing secure routing.

Though many algorithms are available in this area, the routing performance in WSN has been affected continuously due to the presence of malicious nodes. Therefore, a new fuzzy rule-based approach for developing trust and energy-aware secure routing protocol is used in this research work. This protocol is performing better with respect to security and reliable routing in WSN. This is possible because of the introduction of a key based authentication scheme in which encryption using a newly proposed authentication process in order to enhance the security in WSN. Moreover, a new trust model is proposed in this work which uses a new encryption and decryption-based security model with an authentication scheme that uses temporal constraints for performing effective trust analysis. Finally, intelligent temporal analysis and reasoning techniques using fuzzy temporal rules are carried out in this work for making effective decisions on trust-based secure routing leading to increasing in reliability in the packet delivery by applying fuzzy temporal rules.

3 Proposed system framework

Figure 1 depicts the architecture of the proposed system for providing data collection and energy-efficient secured routing. The major components of the proposed system are sensor nodes, clustering module, decision manager, outlier detection module, security module, routing manager, knowledge base and base station.

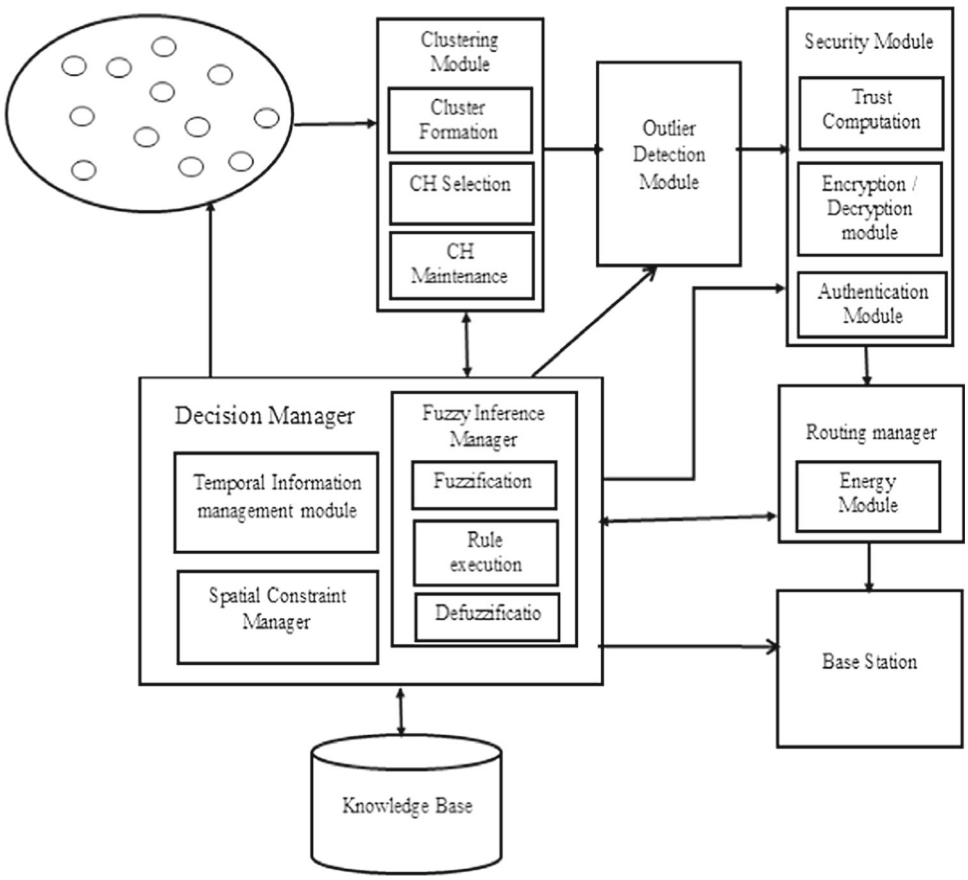

Fig. 1 Proposed system architecture

The sensor nodes are the tiny autonomous devices which are deployed in the sensing area, and they are used to sense the natural phenomenon from the sensing domain and to transmit the sensed data to the base station through multi-hop communication. The clustering modules collect the sensed data from the deployed sensor nodes and form temporal reasoning-based clustering of sensor nodes for performing routing of sensed data to the base station. The clustering module consists of three subcomponents for cluster formation, cluster head selection and cluster maintenance. In cluster formation phase, the temporal rules are used to form dynamic clusters based on distance and by using k-means clustering algorithm. In cluster head selection phase, for each corresponding cluster members are analysed for distance, mobility speed, energy availability and security parameters to select a suitable cluster head with high energy, low mobility and minimum distance with high trust. After selecting the cluster heads for all the clusters, the data collected by the sensor nodes are routed to the base station though the cluster head nodes. Whenever, there is a necessity to carry out re-clustering, the cluster manger forms new clusters and performs cluster head election. In this way, clusters are created and maintained by the clustering module. The outlier detection module finds the nodes that are not a member of any of the clusters. Such nodes will be isolated from data collection and routing activities since these nodes are with less energy, low trust and malicious nodes. In this way, the nodes with low distance and minimum mobility are considered as the eligible members to become cluster heads and to perform clustering-based routing. The security module consists of three subcomponents namely trust computation component, encryption and decryption component and the authentication component. The trust computation component is responsible for computing the nodes own trust and the trust values of all the other members nodes present in the same cluster. The encryption and decryption component is responsible for computing the key and to carry out encryption and decryption of data. The authentication component checks the identity of the nodes which are communicating with a particular node. Moreover, all nodes are made to authenticate themselves by communicating with the base station and the decision manager present in the base station for performing effective authentication of nodes. The routing module is performing the route discovery, route maintenance and routing processes more effectively with energy efficiency. For maintaining minimum energy by the nodes and also to

performing routing through nodes with high energy and energy manager component is present in the routing module. The decision manager is the most important subsystem of the proposed system. The decision manager interacts with all the modules of the system, controls them and communicates with all the modules in the system for making coordination in the entire process of data collection and routing the data to the base station. The decision manager has three sub-modules namely fuzzy inference system, temporal information management module and the special constraint manager. The fuzzy inference system forms inference rules through the fuzzification process and executes them using forward chaining rules that are executed by the inference system. Defuzzification module is used to convert the fuzzy decisions into real world decisions that are used for making efficient routing decisions and followed by the routing module. The temporal and spatial constraint modules that are checked for making routing decisions are maintained by the temporal information management module. The knowledge base consists of domain rules and general rules for making effective inference on routing the collected data into the network. The base station collects all the data provided by the routing module after performing an authentication process.

4 Proposed work

The proposed system consists of a set sensor nodes which has been deployed randomly in the sensing domain to sense the natural phenomenon. The sensed events are transmitted to the base station via multi-hop communication. The set of sensor nodes is used for the data collection to monitor the given environment. The proposed system works in four phases namely clustering phase, outlier detection phase, security maintenance phase and the secured routing phase. Finally, the secured routing phase consists of three sub-phases namely trust computation process, encryption and decryption process and authentication process.

4.1 Clustering phase

This section explains the tasks carried out in the clustering phase namely cluster formation, cluster head selection, cluster maintenance due to mobility and re-clustering processes. The procedure used in the clustering phase is explained in Algorithm 1.

Algorithm 1 Clustering of sensor nodes

Input: Set of deployed sensor nodes
Output: Clustering of sensor nodes.
// cluster formation phase
Begin
1. For all the nodes (N1, N2…Nn)
Do
2. Transmit bacon signal (BS, Nodes) // BS transmits the Bacon signal to set of deployed nodes
3. Compute dist (BS, nodes) // compute the distance between BS and sensor nodes using Received Signal Strength Indicator (RSSI) of the bacon signal and it also computes the distances between nodes and base station using Euclidean distance.
4. Compute residual energy = (node total energy – consumed energy)
5. End For
6. If dist (BS, Nodes) = = less && RE (nodes)= = high then " Layer 1 cluster is formed"
7. If dist (BS, Nodes) = = medium && RE (nodes)= = high then " Layer 2 cluster is formed"
8. If dist (BS, Nodes) = = high && RE (nodes)= = high then " Layer 3 cluster is formed"
9. If dist (BS, Nodes) = = high && RE (nodes)= = medium then " Layer 4 cluster is formed"
10. If dist (BS, Nodes) = = high && RE (nodes)= = low then " Layer 4 cluster is formed"
11. Repeat process until N layers are formed.
End IF
// Cluster head selection process.
12. For all the cluster nodes (CH1, CH2…CHn)
13. Compute nodes (residual energy, trust score , mobility)
14. If (residual energy = = high && trust score = = high, && mobility = = low) then "Select the corresponding node as CH"
// cluster maintenance phase
15. For all the cluster nodes (CH1, CH2…CHn) after time T
Do
16. Set nodes threshold (Residual energy, trust score, mobility)
17. If nodes (residual energy > threshold) && nodes (trust score > threshold) && nodes (mobility > threshold) Then repeat steps 12-14.
End IF
END

Initially, each node is assigned a node number for identifying the node in the subsequent communications. The cluster formation process divides the region into

k geographical areas in such a way that the nodes near the base station will have an area of a Xa square metre which is decided by both Euclidean distance and RSSI values. These areas are used for the initial deployment of nodes, and hence, the nodes are not clustered initially. The next layer will have geographical areas with **2**a X **2**a square metres. This method is repeated to form the last areas with **n**a X **n**a square metres, where n is the value to be decided by the decision manager based on the count of nodes present in the WSN. In addition, the nodes are allowed to perform mobility to another sensing area after obtaining permission from the decision manager which will be intimated to the base station by the decision manager immediately. Re-clustering is also performed by the clustering module due to the movement of nodes. The nodes with higher energy level, lower mobility speed, higher trust score and authenticated perfectly are chosen as the CH. In addition, the distance of all the nodes from the cluster head node must be minimal and the distance between the CH and the sink node must also be optimal. In the cluster formation, The fuzzy temporal rules are used to make efficient decisions by including spatial constraints based on distance in the fuzzy rules. The fuzzy rules are fired using forward chaining inference mechanism to perform deductive inference on the type of nodes to be included in the clusters.

4.2 Outlier detection phase

In this work, outlier detection and prevention of outliers are considered as the attacker model since the outlier nodes are considered to be the malicious nodes. Such nodes are identified by their activities based on the packet drops, energy consumed and delay created by such nodes with the intention of performing passive attacks. In addition, the nodes may perform active attacks through flooding of data during routing.

In this section, a fuzzy rule and distance-based outlier detection algorithm (FRDOA) is proposed for distinguishing the outlier nodes within the network. It uses the relative location initially, and weights are assigned based on two parameters namely distance and the security level. Here, we used the Euclidean distance between points ($x1$, $y1$), ($x2$, $y2$), …(xn, yn). After initial clustering based on the mobility, the next level adjustment is carried out. All the nodes which are not trusted and are not authenticated properly are included in the list of outlier nodes during the re-clustering process. The proposed fuzzy rule and distance-based outlier detection algorithm has been explained in this section.

Algorithm 2 : Fuzzy Rule and Distance-Based Outlier Detection Algorithm (FRDOA)

Input: Set of sensor nodes
Output: Set of outlier nodes
Begin
1. For all clusters (C1, C2,… Cn) Do Begin
2. Compute Node_weightage factor = 0.4 x Initial _distance + 0.3 x Energy _level + 0.3 x mobility-speed
3. Call trust _score (Nodes) // compute the trust score of each node present in the cluster by calling trust score computation algorithm
4. Call Authentication _Score (Nodes) // compute the authentication score of the nodes
5. for i= 1 to m do // m is the number of nodes
Compute Security _level(i) = (trust_score(i)+ authentication_ score(i))/2
End For
End For
6. Initialize outlier _node_set = { };
// outlier detection for cluster nodes.
7. If (Trust_ score(node) = = high && security _level(Node) = = high) then "node is allowed in cluster"
Else
Outlier_node_set = Outlier_node_set U node //Add the node in Outlier _detection list

// Outlier detection for newly joined nodes
8. for newly_ Joined nodes i = 1 to m do begin

9. Call trust _score (Node(i));
10. Call Autentication_score(Node(i));)
11. Compute Security _level(i) = (trust_score(i)+ authentication_ score(i))/2
End For
11. Call Fuzzy _ inference (Rules, Temporal_Constraints);
12. If range (Newly_Arrived_Node) = = HIGH && Security level = = HIGH then add the new node to a suitable cluster".
End If
Else
Add the new nodes to the Outlier_Node_Set
End IF
End for
13. Return (outlier _Node_list);
End

Table 1 Fuzzy rules for outlier detection

S. no.	Fuzzy rules
1	IF (Distance is Nearer) and (Energy Consumption is Minimum) and (Mobility is Least Frequent) THEN (Chance of outlier is Least Possible)
2	IF (Distance is Nearer) and (Energy Consumption is Minimum) and (Mobility is Frequent) THEN (Chance of outlier is Minimum Possible)
3	IF (Distance is Nearer) and (Energy Consumption is Minimum) and (Mobility is Most Frequent) THEN (Chance of outlier is Min-Medium Possible)
4	IF (Distance is Nearer) and (Energy Consumption is Medium) and (Mobility is Least Frequent) THEN (Chance of outlier is Minimum Possible)
5	IF (Distance is Nearer) and (Energy Consumption is Medium) and (Mobility is Frequent) THEN (Chance of outlier is Min-Medium Possible)
6	IF (Distance is Near) and (Energy Consumption is Minimum) and (Mobility is Least Frequent) THEN (Chance of outlier is Minimum Possible
7	IF (Distance is Near) and (Energy Consumption is Minimum) and (Mobility is Frequent) THEN (Chance of outlier is Min-Medium Possible)
8	IF (Distance is Near) and (Energy Consumption is Minimum) and (Mobility is Most Frequent) THEN (Chance of outlier is Medium Possible)
9	IF (Distance is Far) and (Energy Consumption is Higher) and (Mobility is Least Frequent) THEN (Chance of outlier is Max-Medium Possible)
10	IF (Distance is Far) and (Energy Consumption is Higher) and (Mobility is Frequent) THEN (Chance of outlier is More Possible)
11	IF (Distance is Near) and (Energy Consumption is Minimum) and (Mobility is Most Frequent) THEN (Chance of outlier is Medium Possible)
12	IF (Distance is Far) and (Energy Consumption is Higher) and (Mobility is Least Frequent) THEN (Chance of outlier is Max-Medium Possible)
13	IF (Distance is Far) and (Energy Consumption is Higher) and (Mobility is Frequent) THEN (Chance of outlier is More Possible)
14	IF (Distance is Far) and (Energy Consumption is Higher) and (Mobility is Most Frequent) THEN (Chance of outlier is Most Possible)

The fuzzy rules applied by the fuzzy inference system are shown in Table 1. This outlier detection algorithm assigns weights to the nodes using the initial distance, energy level, and mobility; then, it calculates the number of clusters based on the number of nodes and checks the trust values of nodes. After that, it computes the security level of nodes based on their authentication score and trust values for each node.

Now, the algorithm includes all the nodes with less security level than the threshold value to become a member of the set of outliers. Moreover, it calculates weights and distances of all the newly arriving nodes. If the range of newly arrived nodes is high and security level is also high, then it adds the new node to a suitable cluster. Otherwise, the new nodes are added to the outlier node set and then it returns the list of outlier nodes. In this process, the set of outlier nodes is initially set to empty set. Now, the boundary nodes which are equidistance from two cluster head nodes and are very near to other nodes with higher energy will be transferred to the outlier set. Later on, all the nodes which are not secured are also added to the outlier set by applying the proposed outlier detection algorithm.

4.3 Security analysis phase

The security analysis phase consists of two sub-processes namely trust score calculation phase and the authentication process.

4.3.1 Trust score calculation

In this phase, the trust scores are calculated for all the nodes present in the network. Here, initially two types of security trusts are used namely the direct and the indirect trusts. Later, a new type of trust namely the reputation score is considered for different time intervals and this is

Algorithm: 2
Trust calculation algorithm
Begin
Step 1. For all nodes i = 1 to k belonging to different clusters C1,C2, …Cn do begin
Step 2. Initialize FTS(i) = 0 // FTS is Final Trust Score of node i.
Step 3. Compute DTS (i) = packets_sent(i) / packets-received(i) // where DTS is the Direct Trust Score.
Step 4 Compute PTS (i, BS) = $Sum\,(DTS)/n$ // where the Path Trust Score (PTS) is calculated by finding the average trust scores of the participating nodes connecting the path. Where, 'n' denotes the number of nodes that are to be connected in the current path.
Step 5 Compute IDST (i) = $IDTS = (RS(1) + RS(2) + \cdots + RS(i-1) + RS(i+1))/n$ // Indirect trust score is computed based using the recommendation scores received from the neighbor nodes for the given node.
Step 6: Compute AS(i) = Call Authentication_Score(i);
Step 6 Compute FRS(i) = $(W1 * IDTS(i) + W2 * AS(i) + W3 * DTS(i))/(W1 + W2 + W3)$ // where, the FRS values indicates the recommendation scores provided by the neighbors and n represents the number of neighbor nodes. AS indicate authentication score.
Step 7 Compute FTS (i) = $Sqrt(FRS(i) + IDTS(i) + DTS(i))$
Step 8 : Return FTS(i)
End
FTS(i) gives the final trust score for the node i. If the value of FTS becomes less than 0.5 for any node, such node will be tagged as a malicious node and is included in the outlier list and hence it will not be allowed to take part in the communication.

also included in the computation of the final trust score for each node present in the network.

FTS(i) gives the final trust score for the node i. If the value of FTS becomes less than 0.5 for any node, such node will be tagged as a malicious node and is included in the outlier list, and hence, it will not be allowed to take part in the communication.

4.3.2 Authentication process

Each node must authenticate them before communicating with the base station which performs decision making using the decision manager based on the authentication score with values from 0 to 1. The value 0 indicates that the node is not authentically fully, 1 indicates that the node is fully authenticated, and the intermediate values indicate that the node is partially authenticated. Here, the encryption and decryption are carried out using Advanced Encryption Standard (AES) (Stallings 2005).

After performing authentication, the data are allowed for sending to the base station.

4.4 Routing phase

In the routing phase, the trust scores and authentication score are used to find the secured an optimal route for routing in the first process. The fuzzy rules used for finding the malicious users are shown in Table 2.

Using these rules, the proposed routing algorithm routes the data packets through the best path selected by the route discovery process. Therefore, the new fuzzy temporal rule- and cluster-based secured routing with Outlier Detection (FRCSROD) algorithm that has been proposed in this work for performing effective and secure routing is employed here to perform the secured transmission of the data collected by the sensor nodes. Moreover, in the routing process, all the data collected by the sensor nodes are sent to their respective cluster head nodes for routing further. The route discovery process discovers the optimal route from

Algorithm 3 : Authentication of nodes
Begin // Computes the Authentication Score
Step 1. Node to Base station: send (IP address, Node ID) to the Base station // Each node sends its IP address and its node ID to the base station to start the authentication process.
Step 2. BS replies (KP, Sum of nodes ID, Nonce) to the nodes// Where KP is the prime number which is used for key for communication.
Step 3. For nodes i = 1 to n do begin
Step 4 Compute P(node) = KP(i) Modulo (Sum of node IDs)// The current node finds the modulo 'p' value for the sum of node IDs and uses them for encryption using Diffie Hellman algorithm.
End For
Step 5 Node replies $TAS(i) = [IP(i)||ID(i) + Sum(IDs) - ID(i)] mod\ p$ to the base station.
6. IF (TAS > 0) Then
Return AS(i) = Enc (TAS, KP(i), Nonce) // where AS is the Authentication Score issued by the Base Station and KP is the key which is used for encryption and decryption process.// Encryption is performed using AES.
Else
Step 7 Prevent node i from communication.
End For
End

Table 2 Fuzzy rules for malicious node detection

Distance	Energy consumption	Mobility	Chance of malicious node
Nearer (0)	Minimum (0)	Least frequent (0)	Least possible (0)
Nearer (0)	Minimum (0)	Frequent (1)	Minimum possible (1)
Nearer (0)	Minimum (0)	Most frequent (2)	Min-medium possible (2)
Nearer (0)	Medium (1)	Least frequent (0)	Minimum possible (1)
Nearer (0)	Medium (1)	Frequent (1)	Min-medium possible (2)
Nearer (0)	Medium (1)	Most frequent (2)	Medium possible (3)
Nearer (0)	Higher (2)	Least frequent (0)	Min-medium possible (2)
Nearer (0)	Higher (2)	Frequent (1)	Medium possible (3)
Nearer (0)	Higher (2)	Most frequent (2)	Max-medium possible (4)
Near (1)	Minimum (0)	Least frequent (0)	Minimum possible (1)
Near (1)	Minimum (0)	Frequent (1)	Min-medium possible (2)
Near (1)	Minimum (0)	Most frequent (2)	Medium possible (3)
Near (1)	Medium (1)	Least frequent (0)	Min-medium possible (2)
Near (1)	Medium (1)	Frequent (1)	Medium possible (3)
Near (1)	Medium (1)	Most frequent (2)	Max-medium possible (4)
Near (1)	Higher (2)	Least frequent (0)	Medium possible (3)
Near (1)	Higher (2)	Frequent (1)	Max-medium possible (4)
Near (1)	Higher (2)	Most frequent (2)	More possible (5)
Far (2)	Minimum (0)	Least frequent (0)	Min-medium possible (2)
Far (2)	Minimum (0)	Frequent (1)	Medium possible (3)
Far (2)	Minimum (0)	Most frequent (2)	Max-medium possible (4)
Far (2)	Medium (1)	Least frequent (0)	Medium possible (3)
Far (2)	Medium (1)	Frequent (1)	Max-medium possible (4)
Far (2)	Medium (1)	Most frequent (2)	More possible (5)
Far (2)	Higher (2)	Least frequent (0)	Max-medium possible (4)
Far (2)	Higher (2)	Frequent (1)	More possible (5)
Far (2)	Higher (2)	Most frequent (2)	Most possible (6)

the source to the destination only through the cluster head nodes present in various clusters. The routing of data packets are performed after checking the node credentials by applying fuzzy temporal rules which are working with an authentication process and a trust modelling approach that have been discussed already in this paper.

The steps of the proposed secured routing algorithm are as below:

Input: Clusters, nodes, cluster heads and security scores
Output: Optimal path for routing.

Step 1: Let DTS = 0.01, IDTS = 0.01, FTS = 0.01, AS = 0.01;
Step 2: Each node is triggered to communicate with the sink node using rules for getting their trust score and authentication score
Step 3: The sink node sends the route request packets to all the member nodes to form a route using the destination-sequenced routing (DSR) algorithm
Step 4: All nodes are allowed to receive the route request packets from their neighbours through flooding and broadcast them again to the neighbours until the packets reach the destination node
Step 5: Compute the trust scores for paths based on node trust using PTS = Sum (DTS)/n
Step 6: Compute the authentication score for each node using the formula AS = Enc(TAS, k, Nonce)
Step 7: Find the path with minimum distance and PTS > Thresh1 AND AS > Thresh2
Step 8: Perform route reply by the destination node
Step 9: Apply fuzzy rules for finding malicious nodes and to isolate them from routing
Step 10: Perform k-means clustering again using genuine nodes
Step 11: Repeat the route discovery process again
Step 12: Send packets through the shortest path consisting of cluster heads
Step 13: Perform security checking periodically and perform re-clustering

Step 14: Store the data at the base station and output the best path used

In this way, the proposed algorithm performs clustering for each group of data collected by the sensor nodes and helps in the secure routing of the collected data.

5 Experimental results and discussion

This proposed model has been implemented through network simulations by using the network simulation (NS2) tool. The simulation parameters which are used to carry out this work are shown in Table 3.

The performance of the proposed routing algorithm named fuzzy rule and cluster-based secured routing without the introduction of the outlier detection process based on packet delivery ratio is depicted in Fig. 2. Here, the standard LEACH routing algorithm (Younis and Fahmy 2004), HEED (Kim et al. 2007), LEACH with trust mechanism (Weichao et al. 2009), have been considered for packet delivery ratio analysis along with the proposed model. Therefore, five experiments such as $E1$, $E2$, $E3$, $E4$ and $E5$ were conducted in order to evaluate the overall routing performance of this proposed secured routing system in a particular time period. These experiments indicate the varying number of packets sent in the experiments conducted for a period of 10 s.

Table 3 Network simulation parameters

Parameters	Values
Network area	1000×1000 m^2
Maximum no. of sensor nodes	500
Initial node energy	2 J
E_{elec}	100 nJ/bit
ε_{fs}	20 pJ/bit/m^2
ε_{mp}	0.0026 pJ/bit/m^4
Size of each packet	4096 bits
Routing protocol	DSR
Mobility speed	10 m/s to 50 M/s
Mobility model	Random waypoint

From Fig. 2, it can be observed that the performance of the secured routing algorithm without outlier detection provides better performance than the related routing algorithms such as LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009) and the proposed model. This performance improvement is achieved by the application of trust scores in order to identify the trusted nodes and isolating them using the proposed trust modelling technique for effective communication in the network for the particular time period. In addition, fuzzy temporal rules have been used for formation of clusters, and hence, the clustering accuracy has improved in the process of routing more effectively to achieve the increase in packet delivery ratio.

The end-to-end communication delay analysis between the existing routing algorithms namely LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009), and the proposed secured routing algorithm before the introduction of outlier detection is shown in Fig. 3. Different experiments were carried out for measuring the overall quality of the network using the delay metric using the existing models and proposed model.

From the results shown in Fig. 3, it is concluded that the application of trust scores is able to identify the malicious nodes and helps to isolate them from the routing process leading to a reduction in delay. Here, the malicious nodes were flooding the packets with the intent of making congestion in the network so that the delay will be introduced artificially which will increase the overall communication delay. However, the proposed algorithm isolated all the malicious nodes and routed the packets only through the genuine nodes. Therefore, the delay is reduced while applying the proposed algorithm when it is compared with the existing routing algorithms.

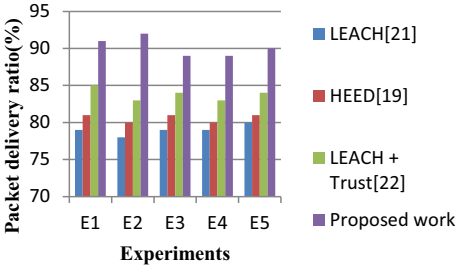

Fig. 2 Packet delivery RATE WITHOUT outlier detection

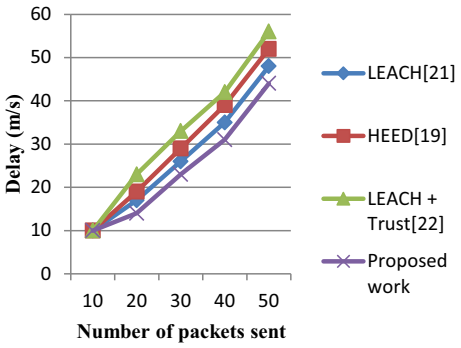

Fig. 3 End-to-end delay analysis

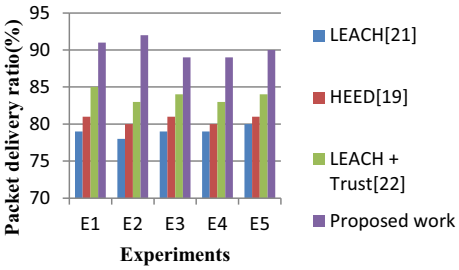

Fig. 4 Packet delivery ratio analysis with outlier detection

The packet delivery ratio analysis is shown in Fig. 4 which considered the proposed algorithm and also the existing routing protocols namely LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009) and the proposed IFCSRA without outlier detection for the analysis. There are five different experiments have been conducted for this packet delivery ratio. These experiments indicate the variation in the number of packets sent.

From Fig. 4, it can be noted that the use of the DTS and IDTS which have 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 and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009), which are using clustering technique for making cluster-based routing in the network. The reason for achieving better packet delivery ratio in the proposed model is due to the use of trust score calculation, energy-level consideration and the incorporation of a new outlier detection algorithm that uses fuzzy temporal rules for inference and decision making.

Figure 5 is used to show the comparison of network throughput through the application of the existing algorithms such as LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009) and also the proposed secured routing model that uses fuzzy rules and trust modelling along with outlier detection. In this process, five different experiments have been conducted by varying the mobility speeds of sensor nodes from 10 to 50 m/s.

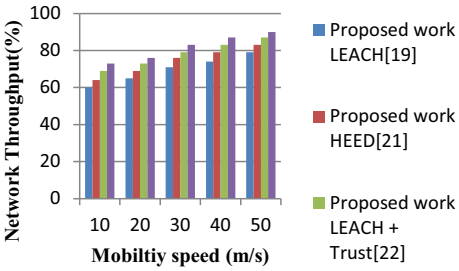

Fig. 5 Through put analysis

From the results shown in Fig. 5, it is to be noted that the performance of the proposed routing algorithm with trust modelling is better in terms of network throughput measured under different speeds of mobility than the algorithms that do not consider the trust modelling. Moreover, the proposed routing algorithm outperforms all the other existing routing algorithms considered in this work due to the use of fuzzy rules, temporal constraints, clustering, trust management and outlier detection.

Figure 6 shows the energy comparison analysis between different existing routing algorithms namely LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009) and the proposed secured routing algorithm that are tested for varying number of rounds

From Fig. 6, it can be noted that the energy consumption is minimum when the packets are routed through the proposed FCSROD than the other routing algorithms namely LEACH routing algorithm (Kim et al. 2007), HEED (Younis and Fahmy 2004), LEACH with trust mechanism (Weichao et al. 2009). Here, the performance improvement has been achieved not only through the application of fuzzy rules, trust mechanism and clustering. Moreover, the attackers were not allowed to dry the energy in the proposed work by isolating them from the routing process.

Figure 7 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 and Fahmy 2004) and LEACH with trust mechanism (Weichao et al. 2009). Moreover, five different experiments have been carried out with various set of nodes in the sensor network scenario by varying the number of malicious users in the range of 5–10.

From Fig. 7, it can be observed that the performance of the newly proposed secured routing algorithm is better with respect to security when it is compared with the other routing protocols. The reason for this security improvement is because of the use of outlier detection, application of intelligent fuzzy rules, constraint satisfaction using temporal and spatial constraints.

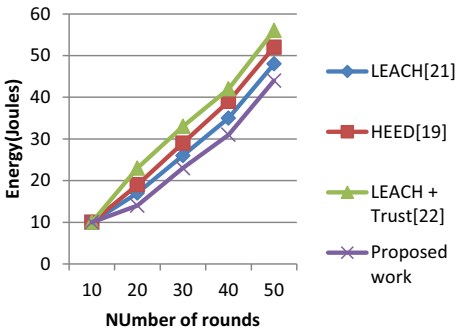

Fig. 6 Comparative analysis based on energy consumption

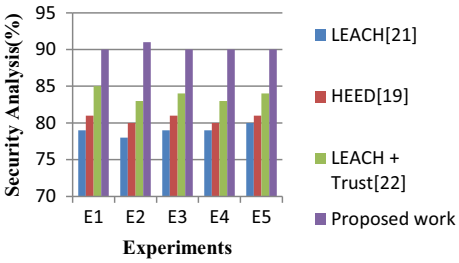

Fig. 7 Security level analysis

6 Conclusion and future works

In this paper, a new secured routing algorithm called fuzzy rule and cluster-based secured routing with outlier detection (FRCSROD) algorithm has been proposed and implemented for performing secured communication in WSNs. Moreover, a new outlier detection algorithm called fuzzy rule and distance-based outlier detection algorithm (FRDOA) is also proposed and incorporated with the proposed model which is used for distinguishing the normal nodes from malicious nodes which are available in the WSNs. In this proposed work, fuzzy temporal rules have been generated and used to make effective decisions over the process of cluster formation, security analysis and the routing process. Security modelling has been carried out by developing a trust model and an authentication process. The experimental results of this work have proved that the newly proposed secured routing algorithm improves the security, reliability and packet delivery rate and also reduces the communication delay in the network. Therefore, the proposed algorithm enhances the lifetime of the network by reducing unusual energy consumption by malicious nodes. For enhancing the performance of this model in future, new intelligent agents-based approach can be used for the effective data communication and coordination between the sensor nodes that are identified as source and a sink node for the particular communication process.

Acknowledgements We wish to thank Dr.S.V.N. Santhosh kumar and Dr.M.Selvi Assistant Professors from VIT, Vellore, Tamil Nadu, India, who has supported us along the way. We are grateful to our family members and friends who have provided us through moral and emotional support in our life.

Funding Not applicable.

Compliance with ethical standards

Conflict of interest All authors state that there is no conflict of interest.

Human and animal rights Humans/Animals are not involved in this work. We used our own data.

References

Allen JF (1983) Maintaining knowledge about temporal intervals. Commun ACM 26(11):832–843

Alshammari H, Ghorbel O, Aseeri M, Abid M (2018) Non-negative matrix factorization (NMF) for outlier detection in wireless sensor networks, pp 506–511

Anwar RW, Zainal A, Outay F, Yasar A, Iqbal S (2019) BTEM: belief based trust evaluation mechanism for wireless sensor networks. Future Gener Comput Syst 96:605–616

Ayadi A, Ghorbel O, Obeidad AFM, Abid M (2017) Outlier detection approaches for wireless sensor networks: a survey. Comput Netw 129(1):319–333

Bao F, Chen IR, Chang M, Cho JH (2012) Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manag 9(2):169–183

Dang H, Wu H (2010) Clustering and cluster-based routing protocol for delay-tolerant mobile networks. IEEE Trans Wirel Commun 9(6):1874–1881

Das A, Islam MM (2012) Secured trust: a dynamic trust computation model for secured communication in multiagent systems. IEEE Trans Dependable Secure Comput 9(2):261–274

Dean TL, McDermott DV (1987) Temporal database management. Artif Intell 32(1):1–55

Deng H, Yang Y, Jin G, Xu R, Shi W (2010) Building a trust-aware dynamic routing solution for wireless sensor networks. In: Proceedings of the IEEE GLOBECOM workshop, pp 153–157

Donald DM, Sanchez S, Madria S, Ercal F (2015) A survey of methods for finding outliers in wireless sensor networks. J Netw Syst Manag 23(1):163–182

Duan J, Qin Y, Zhang S, Zheng T, Zhang H (2011) Issues of trust management for mobile wireless sensor networks. In: 7th international conference on wireless communications, networking and mobile computing, pp 1–4

Fawzy A, Mokhtar HMO, Hegazy O (2013) Outliers detection and classification in wireless sensor networks. Egypt Inform J 14:157–164

Ganeriwal S, Balzano LK, Srivastava MB (2008) Reputation based framework for high integrity sensor networks. ACM Trans Sens Netw 4(3):66–77

Gilbert EPK, Kaliaperumal B, Rajsingh EB, Lydia M (2018) Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks. Comput Electr Eng 72:894–909

Hamdane B, Boussada R, Elhdhili ME, El Fatmi SG (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

Han J, Kamber M, Pei J (2011) Data mining: concepts and techniques. The Morgan Kaufmann series in data management systems, 3rd edn. Morgan Kaufmann Publishers, Burlington

Hodge V, Austin J (2003) A survey of outlier detection methodologies. Artif Intell Rev 22:85–126

Izadi D, Abawajy J, Ghanavati S (2015) An alternative clustering scheme in WSN. IEEE Sens J 15(7):4148–4155

Jabeen F, Fernandes AAA (2012) An algorithmic strategy for in network distributed spatial analysis in wireless sensor networks. J Parallel Distrib Comput 72:1628–1653

Jaisankar N, Ganapathy S, Yogesh P, Kannan A, Anand K (2012) An intelligent agent-based intrusion detection system using fuzzy rough set based outlier detection. Soft Comput Tech Vis Sci 395:147–153

Kerrache CA, Calafate CT, Cano J-C, Lagraa N, Manzoni P (2016) Trust management for vehicular networks: an adversary-oriented overview. IEEE Access 4:9293–9307

Kim J, Jang KY, Choo H, Kim W (2007) Energy efficient LEACH with TCP for wireless sensor networks. In: Computational science and its applications–ICCSA 2007, pp 275–285

Kosko B (1986) Fuzzy cognitive maps. Int J Man Mach Stud 24(1):65–75

Lee S-B, Choi Y-H (2006) A secure alternate path routing in sensor networks. Comput Commun 30(1):153–165

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 Syst J 8(3):858–867

Lin H, Wang L, Kong R (2015) Energy efficient clustering protocol for large-scale sensor networks. IEEE Sens J 15(12):7150–7160

Liu Y, Liu Y, Dong M, Ota K, Liu A (2016) ActiveTrust: secure and trustable routing in wireless sensor networks. IEEE Trans Inf Forensics Secur 11(9):2013–2027

Logambigai R, Kannan A (2016) Fuzzy logic based unequal clustering for wireless sensor networks. Wirel Netw 22:945–957

Logambigai R, Ganapathy S, Kannan A (2018) Energy–efficient grid-based routing algorithm using intelligent fuzzy rules for wireless sensor networks. Comput Electr Eng 68:62–75

Mahmoud MEM, Lin X, Shen X (2015) Secure and reliable routing protocols for heterogeneous multihop wireless networks. IEEE Trans Parallel Distrib Syst 26(4):1140–1153

Mazinani A, Mazinani SM, Mirzaie M (2019) FMCR-CT: an energy-efficient fuzzy multi cluster based routing with a constant threshold in wireless sensor network. Alex Eng J 58:127–141

Miglani A, Bhatia T, Goel S (2015) Trust-based energy efficient routing in LEACH for wireless sensor networks. In: Proceedings of 2015 global conference on communication technologies, pp 361–365

Moonesignhe HDK, Tan P-N (2006) Outlier detection using random walks. In: IEEE international conference on tools with artificial intelligence (ICTAI'06), pp 532–539

Muthurajkumar S, Ganapathy S, Vijayalakshmi M, Kannan A (2017) An intelligent secured and energy efficient routing algorithm for MANETs. Wirel Pers Commun 96(2):1753–1769

Russell S, Norvig P (1994) Artificial intelligence: a modern approach. Prentice Hall, Englewood

Saeed N, Al-Naffouri TY, Alouini M-S (2019) Outlier detection and optimal anchor placement for 3-D underwater optical wireless sensor network localization. IEEE Trans Commun 67(1):611–622

Santhosh Kumar SVN, Palanichamy Y (2018) Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. Wirel Netw 24(4):1343–1360

Sethukkarasi R, Ganapathy S, Yogesh P, Kannan A (2014) An intelligent neuro fuzzy temporal knowledge representation model for mining temporal patterns. Int J Fuzzy Syst 26(3):1167–1178

Shahid N, Naqvi IH, Qaisar SB (2012) Quarter-sphere SVM: attribute and spatio-temporal correlations based outlier & event detection in wireless sensor networks. In: 2012 IEEE wireless communications and networking conference: mobile and wireless networks, pp 2048–2053

Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712

Shamim Hossain M, You X, Xiao W, Song JLE (2019) QoS-oriented multimedia transmission using multipath routing. Future Gener Comput Syst 99:226–234

Shiva Murthy G, D'Souza RJ, Varaprasad G (2012) Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks. IEEE Trans Sens J 12(10):2941–2949

Sree Rathna Lakshmi NVS, Babu S, Bhalaji N (2017) Analysis of clustered QoS routing protocol for distributed wireless sensor network. Comput Electr Eng 64:173–181

Stallings W (2005) Cryptography and network security principles and practices, 4th edn. Prentice Hall, Englewood

Sun G, Li Y, Hongfang Yu, Vasilakos AV, Xiaojiang D, Guizani M (2019) Energy-efficient and traffic-aware service function chaining orchestration in multi-domain networks. Future Gener Comput Syst 91:347–360

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. Comput Netw 151:211–223

Weichao W, Fei D, Qijian X (2009) An improvement of LEACH routing protocol based on trust for wireless sensor networks, 2009. In: 5th conference on wireless communications and mobile computing, pp 1–4

Younis O, Fahmy S (2004) HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans Mob Comput 3(4):366–379

Zadeh LA (1965) Fuzzy sets. Inf Control 8(3):338–353