Improving Data Accuracy Using Proactive Correlated Fuzzy System in Wireless Sensor Networks

Barakkath Nisha U[1], Uma Maheswari N[2], Venkatesh R[3] and Yasir Abdullah R[4]

[1,2] Department of Computer Science& Engg, PSNA College of Engg & Technology
Dindigul, Tamilnadu - India
[e-mail: ubnisha@gmail.com, numamahi@gmail.com]

[2] Department of Information Technology, PSNA College of Engg & Technology
Dindigul, Tamilnadu - India
[e-mail:rlvenkatesh@gmail.com]

[4] Department of Computer Science& Engg, Sri Subramanya College of Engg & Technology
Palani, Tamilnadu - India
[e-mail: yasirsince1984@gmail.com]

*Corresponding author: Barakkath Nisha U

Received April 20, 2015; revised June 23, 2015; accepted July 15, 2015;
published September 30, 2015

Abstract

Data accuracy can be increased by detecting and removing the incorrect data generated in wireless sensor networks. By increasing the data accuracy, network lifetime can be increased parallel. Network lifetime or operational time is the time during which WSN is able to fulfill its tasks by using microcontroller with on-chip memory radio transceivers, albeit distributed sensor nodes send summary of their data to their cluster heads, which reduce energy consumption gradually. In this paper a powerful algorithm using proactive fuzzy system is proposed and it is a mixture of fuzzy logic with comparative correlation techniques that ensure high data accuracy by detecting incorrect data in distributed wireless sensor networks. This proposed system is implemented in two phases there, the first phase creates input space partitioning by using robust fuzzy c means clustering and the second phase detects incorrect data and removes it completely. Experimental result makes transparent of combined correlated fuzzy system (CCFS) which detects faulty readings with greater accuracy (99.21%) than the existing one (98.33%) along with low false alarm rate.

Keywords: Wireless sensor networks, robust fuzzy c- means clustering, proactive fuzzy system, data accuracy, correlation, combined correlated fuzzy system.

http://dx.doi.org/10.3837/tiis.2015.09.013 **ISSN : 1976-7277**

1. Introduction

Wireless sensor networks face challenges in providing accurate data in base station. Anomalies are refined by increasing data accuracy in WSNs. In a group of data, some data may follow a deviated pattern from the other data and are termed as "Anomalies". Dynamic environments are usually monitored by sensors over a period of time where the logs are created for future use. Self directed, minuscule and low power sensor nodes are presented in all WSNs. Sensing, Storing, Computing and Communication are the individual threads of sensor nodes [1]. All sensor nodes sense the available environment, save data in the main memory, interact the data between neighbor nodes and evaluate the computation process. They require energy for performing the above mentioned operations. Since the sensor node's battery capacity is very small, these energies should be utilized only for important processes. According to G.J Pottie, the energy needed for communication is more than the energy needed for computation [2]. Transceivers send and receive packets by consuming smaller energy. All researches focus only on reduction in communication overhead while transmitting the packets but unwanted data transmissions reduce the energy used in WSNs [3]. In this context, data aggregation avoids incorrect data in which sensors are designed to do so. It also tries to eliminate redundant data transmission by reducing the energy consumption of nodes. An important function of any WSNs is in analyzing the data which is saved as log in the form of readings by sensor nodes.

Large numbers of highly correlated data are entailed by redundant data and energy is exhausted in larger amount which again will be processed and received by the base station. Network lifetime is increased by providing fused information and eliminating redundant transmission through data aggregation [4]. When anomalies are not detected during the data aggregation process, the data inaccuracy occurs [5]. Data aggregation uses cluster structure, where data travels from source to sink in a hierarchical way. The data collected by clusters from one or more cluster members is applied to aggregation functions. Sink often receives the aggregated value then and there. In this context, some faulty nodes may be present, which can produce incorrect readings and deviate the exact output.

In general, anomaly detection can be classified into prior knowledge based like statistical, rule-based etc., and prior knowledge free namely data mining, computational intelligence etc., An ideal anomaly detection system should increase the level of data accuracy in base station and cluster head. Prior knowledge free technique lacks in giving accurate anomaly detection due to missing quick updating of normal profile, high computational complexity by introducing complex machine learning algorithms and slow detection by developing training model with agents. Prior knowledge based approach like statistical based techniques provide good detection rate with less false alarm rate and it requires a mathematical model, which takes more computational time [6] [7]. To overcome these problems, a proactive fuzzy system is implemented by using rule based anomaly detection scheme which is developed based on mathematical assumptions and information predicted by experts. Fuzzy rule based anomaly detection system provides high anomaly detection accuracy by generating confidence decision making rules and less computational complexity with fewer number of rules [10].

In the proposed system, the term "proactive" refers to a fuzzy system which is executed in each cluster head for avoiding duplicate and abnormal data before the data is being sent to base station. After removing the bad data, base station receives accurate information by employing proactive system which is implemented in distributed fashion. Two levels of anomaly elimination process are dealt in this paper. The first level concentrates on finding faulty nodes in individual sensor nodes. The second level expresses mediator node's logs and based on those logs it finds the faulty mediator nodes and discard those nodes over the distributed networks. Fuzzy c-means clustering focus on creating input space for the fuzzy system. Input space partitioning acts as an input for the proposed proactive fuzzy system. Anomaly will be discovered by applying fuzzy logic with all qualified correlation techniques like spatial, temporal and attribute correlation. The leftovers of the paper are organized as follows: Section 2 is endowed with some important connected concepts needed for our proposed algorithm. Section 3 explains the network model and problem statement. Section 4 presents the proposed approach and methodology. Section 5 infers the experimental evaluation based on both synthetic and real data sets. Finally section 6 elucidates the future work by concluding the paper.

2. Related Work

Anomaly detection and removing noisy data in wireless sensor networks have been examined in varieties of research works [6]. Existing anomaly detection techniques can be categorized into two stream classes. The first stream uses supervised learning that formulates prior knowledge in developing a customary profile. The second stream is placed on an unsupervised learning to develop a customary profile that is generated based on prior knowledge of sensed data. In clustered sensor architecture, nodes perform different roles like sensing and leading node. The leading node or cluster head performs aggregation and sensing nodes sense the reading at different time slots. Cluster generation can be performed by various conventional clustering protocols like LEACH, HEED [8] [9] etc., The existing clustering protocols separate the nodes based on Euclidean distance metrics without considering the correlation distance among the sensor nodes which lead to informal cluster formation where clusters will not guarantee in providing reliable and accurate data to base station. To overcome this issue, a robust fuzzy c-means clustering is proposed for effective cluster formation with less computational complexity.

Previous works attempt in anomaly detection by aiming specifically in classifying the data as correct or incorrect without analyzing logic and originally happened event status in the environment. Daniel et al.[11] have proposed classification based voting method for anomaly detection. They have proposed five different classifiers that are used to detect anomaly with reliable estimations to replace the measurement affected by anomalies. This method fails in cases where large dataset are considered. Suat et al [12] have focussed data aggregation and authentication protocol for security, confidentiality and false data detection. It also reduces communication complexity upto 60% and computational complexity is increased. The author in [13] proposed a statistical data analysis for outlier detection on high dimensionality data with high false negative which fails to focus neither on spatial correlation nor spatio-temporal correlation. Janakiram et. al [14] presents a technique based on bayesian belief network to identify local anomalies by focusing on spatial and temporal with attribute correlation based on conditional probability for detecting anomaly effectively. This method is not suitable for dynamic network topology. Fuzzy system concludes its results based on decisions made by fuzzy inference system.

Chitradevi et.al [15] proposed anomaly detection based on distributed agglomerative clustering approach where anomaly is removed both at local and global level. Cluster distance and density measures are used to form optimal cluster thereby removing anomalies with affordable computational and communication complexity. Yanz zhang et al. [16] have proposed an ellipsoidal based support vector machine, which classifies sensor node data as anomaly by using ellipsoidal SVM based online anomaly detection and adaptive anomaly detection for multivariate data. They used the time window concept for identifying changes in normal behavior of the system. This technique suffers from some computational complexity due to updating a normal profile periodically. Y.Zhang et.al [17] proposed a statistical based outlier detection which is based on time series and geostatistics analysis with spatial and temporal correlation concepts. Their way of modeling temporal correlation by fitting auto regressive moving average (ARMA) model and spatial correlation model is developed by using variogram model. Krasimira kapitanova's et al. [18] proposed general fuzzy logic system for event detection by using spatial and temporal semantics. They decrease the number of rules by combining simple rules and trimming unwanted rules in rule base system. They used fuzzy logic instead of taking fixed thresholds and crisp values, which improve the accuracy of fire event detection. Liang et. al [19] proposed a double sliding window detection to increase the detection rate of event detection. However, they elaborate the effect of fuzzy logic and the power of spatial and temporal possessions of the data in classifying of detection rate. The authors Heshan Kumaragea et al. [20] proposed a fuzzy data modeling for distributed anomaly detection in different real data sets. Scalability and sensitivity of this approach are low while considering a large number of nodes.

From the literature survey, It is evident that an ideal anomaly detection system should produce high accuracy with minimal energy consumption. The proposed method has three main contributions. First, an input space partitioning is created by using robust fuzzy c-means clustering that results in forming more accurate clusters. Second, sensor's space, time and attribute correlation acts are incorporated into the fuzzy logic rule-base to further improve the accuracy of anomaly detection. Third, rules generated by rule based system are reduced by applying rule trimming function without affecting the detection rate of the system.

3. Network Model and Problem Statement

A distributed heterogeneous WSN is considered where enormous number of sensor nodes with limited power resource senses the physical phenomena and the little number of aggregator nodes perform anomaly detection with data aggregation. The network topology which uses undirected graph is considered G(S,E) where S represents sensor nodes and E as edges that connects two nodes within a cluster. It is assumed that sensor nodes and base station are fixed after deployment and each sensor has a separate identifier. **Fig. 1** presents the sensor network's topology. Initially, all nodes perform the clustering operation on their own local data. An appropriate clustering protocol for implementing distributed clustered wireless sensor network is proposed, where the deployment area is grouped into several clusters. Each cluster head performs distributed data aggregation from the cluster members, where data aggregation reduces unwanted data transmission and increases the level of data accuracy by eliminating duplicate and unwanted data.

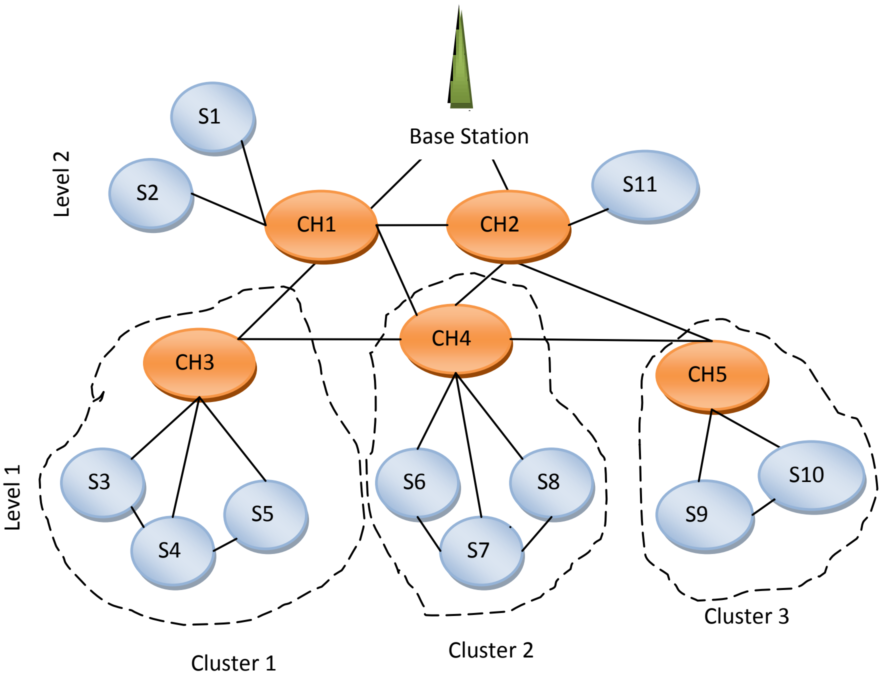


Fig. 1. Distributed clustered network representation

The aim is to perform anomaly detection and separate anomalous data in each cluster of the network. Let C_k denote numbers of clusters where each cluster is having n numbers of sensor nodes i.e $\{ S_1, S_2, S_3 \ldots\ldots\ldots S_n \in C_k\}$ and each cluster head is interconnected with all other cluster heads in the network. A_n denote number of attributes involved in multi sensor nodes i.e $\{ A_1\ A_2, A_3 \ldots\ldots\ldots A_n$ € $S_n \}$ where, each attribute has partial or full dependency with other attributes. In the first phase of the proposed system, energy consumption is reduced with single-hop distance between the node and cluster head by applying the robust fuzzy c-means clustering. In the second phase, a fuzzy based comparative correlation technique is implemented and it removes unwanted data transmission by eliminating the anomalous data that are characterized as observations from a given sensor that are corrupted due to sensor malfunction.

4. Proposed Methodology

The proactive anomaly detection system starts by input space partitioning, where robust fuzzy c-means clustering is employed and it ends by detecting incorrect data accurately and removing it entirely by employing correlative fuzzy logic algorithm. By testing the conventional techniques, it is inferred that it ensures whether the data is incorrect or not and does not concentrate on analyzing the event based approach. To solve this issue, a fuzzy logic is put into practice with correlation technique for extracting the different regions for analyzing erroneous, suspicious and acceptable sample data generated by sensor nodes at different point of time.

4.1 Fuzzy Logic System

The proposed fuzzy classification system includes two basic steps. First step explains structure confirmation process which contains robust fuzzy c-means algorithm based on robust mahalanobis distance and new dissimilarity function. In second step, fuzzy inference engine classifies the input sample according to fuzzy rule set and reasoning method generated by fuzzy-spatial, fuzzy-temporal and fuzzy-attribute correlation acts. The proposed method is summarized in **Fig. 2**. Fuzzy system is characterized by a set of linguistic statements based on experts knowledge. The experts knowledge are usually in the form of "*if-then*" rules [21][22]. Fuzzification process converts the crisp input into fuzzy membership function and fuzzy inference system performs rule decision making and de-fuzzification converts fuzzy output into crisp output.

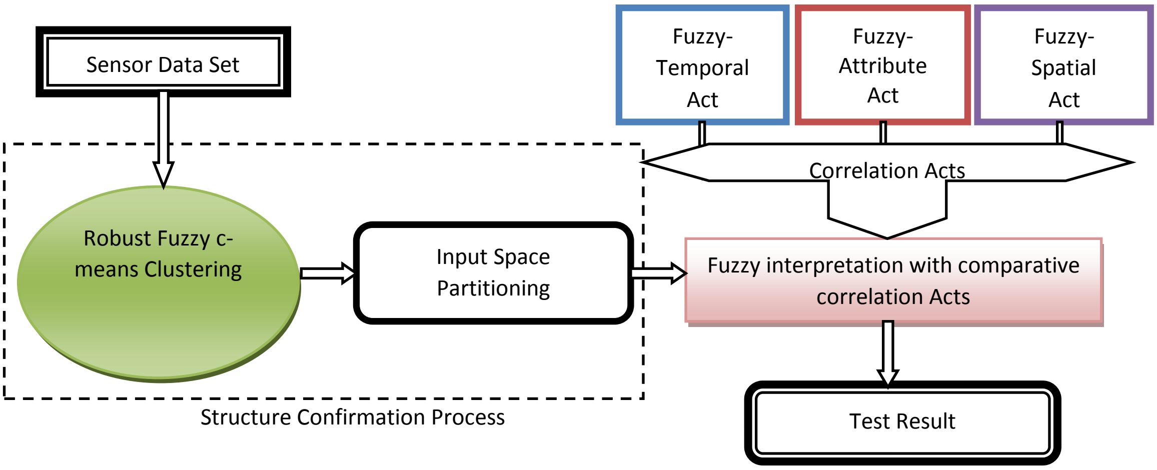


Fig. 2. Framework model of Proactive Fuzzy system with anomaly detection

4.2 Robust Fuzzy C-means Clustering

The conventional Fuzzy c-means (FCM) clustering analysis is applied to assemble same type of data in one cluster where the similar form of data should be near, and the dissimilar form of data should be farer. It can hold lot of information about the data than hard k- means clustering algorithm [23] [24]. FCM uses the Euclidean distance concept and simple cost function for cluster formation. The cluster heads are responsible for collecting data from the group and conveying to the next level cluster head or base station finally for detection. A variety of fuzzy clustering methods have been proposed and most of them are based on distance criteria [25] [26].

Clustering partitions a dataset into several groups in such a manner that the similarity within a group is larger than that among its peers**.** In the proposed robust fuzzy c-means clustering (RFCM), the concept of robust mahalanobis distance and new cost function based on typicality measure and density measure are used. The distance of the vector from the centroid in a multidimensional space is defined by the term "Robust Mahalanobis Distance (RMD)" represented by a correlated independent variable [27]. Cost function is calculated by using distance and density measures. RFCM partitions the number of sensor nodes into different fuzzy groups. Let $\{S_i : i=1,2\ldots n\}$ be a set of sensor nodes. Each node S_i senses m number of physical phenomena like light, voltage and humidity, such that $S_i\{x_1, x_2 \ldots\ldots\ldots x_m\}$. The process of clustering is to assign the sensor nodes into number of clusters (C_k) where $\{C_k: k=1,2\ldots n\}$ by using distance metrics and dissimilarity function [28].

Step 1: Initialize the membership matrix G which is allowed to have elements with values between 0 and 1.

$$\sum_{i=1}^{CC_i} G_{ij}=1 , \qquad \forall_j=1,2,\ldots n \tag{1}$$

RFCM allows each feature vector belonging to every cluster with a fuzzy truth value ranging between low (0) and high (1) and CC_i denoting cluster center.

Step 2: Calculate centroids of fuzzy cluster centers CC_i where, i=1, 2... n

$$CC_i = \frac{\sum_{i=1}^{n} [G_i(S_i)]^p S_i}{\sum_{i=1}^{n}[G_i(S_i)]^p} \quad \forall_i \in C_k \tag{2}$$

where p is the degree of fuzzification.

Step 3: Compute dissimilarity function for RFCM based on density and typicality measures. It replaces conventional fuzzy c-means clustering distance (Euclidean distance) with RMD.

Step 3.1: Compute typicality measure $\mathcal{F}_{\urcorner}$.

$$\mathcal{F}_{\urcorner} = \sum_{i=1}^{n} \sum_{k=1}^{C_k} [G_k(S_i)]^2 \, {RMD_{ki}}^2 \tag{3}$$

where, n is the number of training data, C_k is the number of clusters, $G_k(S_i)$ membership of sensor node i in cluster k and ${RMD_{ki}}^2$ is expressed as follows:

$${RMD_{ki}}^2 = (D(X_i) - CC_k)' \, \delta_m \, (D(X_i) - CC_k) \tag{4}$$

$$\delta_m = \sqrt{\frac{1}{n-1} \sum_{i,k=1}^{n} (D(X_i) - CC_k)^2} \tag{5}$$

where δ_m is the sample standard deviation of $D(X_i)$.

Step 3.2: Compute density measure $\mathcal{F}_{\mathcal{D}}$.

$$\mathcal{F}_{\mathcal{D}} = \sum_{i=1}^{n} \sum_{j=1}^{n} \left\{ \left[\sum_{k=1}^{C_k} \left(G_k(S_i) - G_k(S_j) \right)^2 \right] - {d_{ij}}^2 \right\}^2 \tag{6}$$

Where, d_{ij} is the distance between i and j which indicates position of sensor nodes.

Final dissimilarity function is optimized by iterating $\mathcal{F} = \mathcal{F}_{\urcorner} + \mathcal{F}_{\mathcal{D}}$ using equation 3 and 4.

$$\sum_{i=1}^{n} G_i(S_i) = 1 \qquad \forall_i \in C_k \tag{7}$$

and

$$0 < \sum_{i=1}^{n} G_i(S_i) < n \qquad \forall_i \in C_k \tag{8}$$

Step 4: Compute new membership function $G_{i,j(new)}$

$$G_{i,j(new)} = \frac{1}{\sum_{k=1}^{C_k}\left(\frac{d_{ij}}{d_{kj}}\right)^{\frac{2}{(p-1)}}} \tag{9}$$

where p is the degree of fuzzification, d_{ij}, d_{kj} are calculated by using equation 4. The cluster centers $\mathrm{CC_n}$ and the membership $\mathrm{G_i(S_i)}$ are optimized by using RFCM.

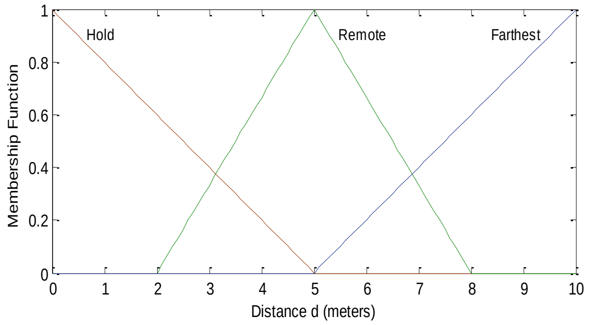
4.3 Anomaly Detection using Fuzzy Reasoning based on Correlation Acts

Sensors should be continuously monitored where anomaly is available and the readings are taken from multiple sensors over a period of time since they are considered to be highly dependable and volatile. While analyzing the existing methods it is understood that no methodology is implemented by applying fuzzy logic with attribute, spatial and temporal correlation to anomaly detection. Hence fuzzy logic is applied with comparative correlation techniques for classifying of error and originally happened events. Anomaly detection is the combined output of all physical phenomena's readings in time and spatial location and is the rate of change of all attributes used in the sensor deployment area. Fuzzy reasoning for anomaly detection uses various linguistic variables for spatial, temporal and attribute acts. The outputs of the three separate techniques are given as input to the proactive anomaly detection system which will classify the percentage level of anomalies present in the environment and named them as superior, doubtful and inferior respectively.

4.3.1 Spatial Act

Spatial act is commonly known as the relationship among the nearest neighbor node readings. To make the system accurate and reduce the false alarm, an anomaly detection system needs to be designed with care [29]. For this, various readings from multiple sensors are included at various time intervals. There lies a negative correlation between the true probability report and the distance among the reported sensors. Hence while dealing with anomaly detection logic, spatial location concepts are added [30]. The spatial protector or linguistic variable is augmented with the rules in the rule-base. This spatial act rule is applied at each cluster generated by robust fuzzy C-means algorithm. **Fig. 3** shows the confidence decision making of spatial act. In **Table 1** three linguistic variables are declared as Hold (H), Remote (R), and Farthest (F). These are used to analyze the sensor's farthest distance. The format of the rules and membership function $\mu_{SA}(d)$ described in spatial act are as follows:

IF S_1 is H and S_2 is H and S_3 is H ...... and S_n is H;
THEN Correlation assurance level is HSA



The assurance levels of spatial act are classified as Low Spatial Act (LSA), Medium Spatial Act (MSA) and High Spatial Act (HSA) where, LSA denotes too farthest nodes, MSA comprises of nodes which fall between nearer and farthest nodes and HSA comprises of nodes which are too nearer.

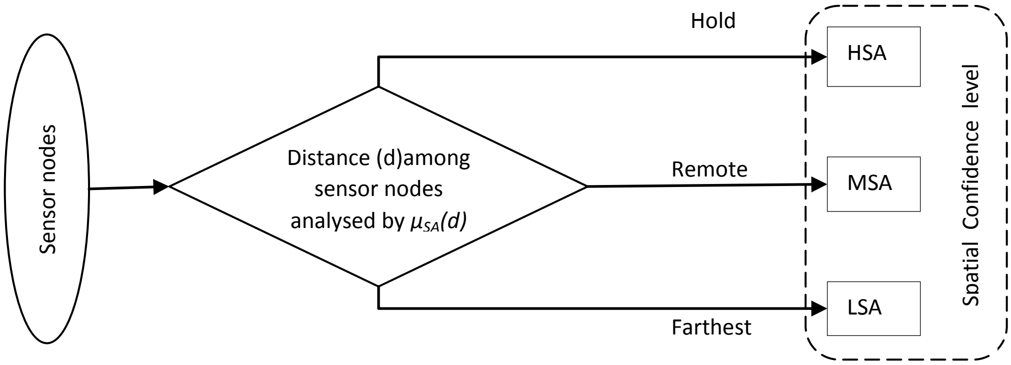


Fig. 3. Decision making of spatial act

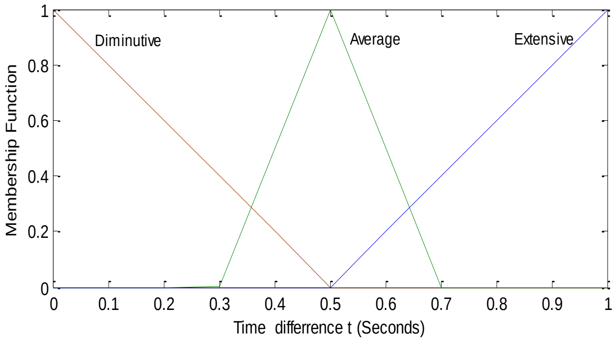
Table 1. Spatial Act Rule Structure

Rule®	S_1	S_2	S_3	S_4	S_5	…….	S_{n-1}	S_n	Assurance Level
1	F	F	F	F	F	…….	F	F	LSA
2	F	F	F	F	F	…….	F	R	LSA
3	F	F	F	F	F	…….	F	H	LSA
4	F	F	F	F	F	…….	R	F	LSA
α	⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
						…….			
α+1	R	R	R	R	R	…….	R	R	MSA
α+2	R	R	R	R	R	…….	R	F	MSA
α+3	R	R	R	R	R	…….	R	H	MSA
α+4	R	R	R	R	R	…….	F	R	MSA
β	⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
β +1	H	H	H	H	H	…….	R	H	HSA
β +2	H	H	H	H	H	…….	H	F	HSA
β +3	H	H	H	H	H	…….	H	R	HSA
β +n	H	H	H	H	H	…….	H	H	HSA

4.3.2 Temporal Act

Temporal act is the relationship between the data in the current moment at time t and the data in the previous moment at time t-1. The sensor readings of the temporal properties are considered in order to decrease the false alarms. The sensor readings indicate a particular data generated at short interval of time to achieve high anomaly detection confidence. Anomaly detection confidence is increased whenever the temporal distance between the sensor readings decrease and vice versa. The inherent nature of sensor communication makes the temporal work specifically important [29]. The temporal defender is applied at each cluster generated by robust fuzzy c-means algorithm. **Fig. 4** shows the confidence decision making of temporal act. In **Table 2** three variables are declared as Diminutive (D), Average (A), and Extensive (E).These are used to analyze the sensor's readings time difference. The assurance levels of temporal act are classified as Low Temporal Act (LTA), Medium Temporal Act (MTA), and High Temporal Act (HTA) where, LTA denotes too longer time duration of readings, MTA covers the node's reading which falls between short and wide time difference and HTA consists of sensor nodes readings generated with shorter duration. The format of the rules and membership function $\mu_{TA}(t)$ described in temporal act are as follows:

IF S_1 is D and S_2 is D and S_3 is D ...... and S_n is D;
THEN Correlation assurance level is HTA



Temporal act can be processed on same sensor readings at different time interval or a node's reading is analyzed with its neighbor node's readings with same time duration.

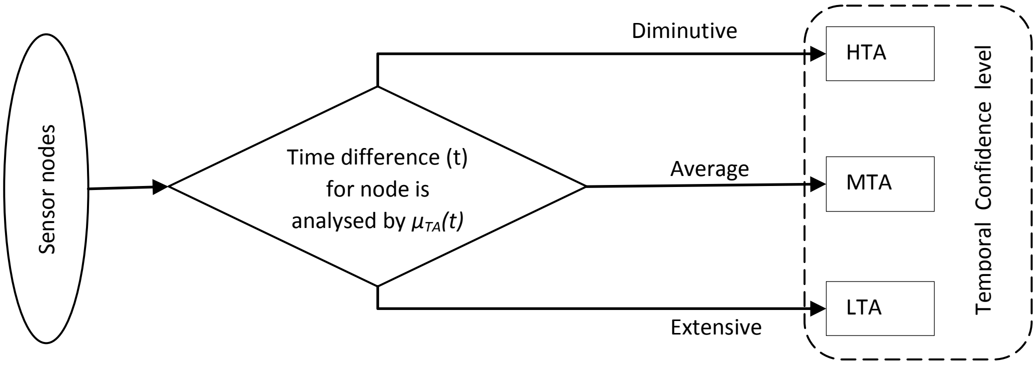


Fig. 4. Decision making of temporal act

Table 2. Temporal Act Rule Structure

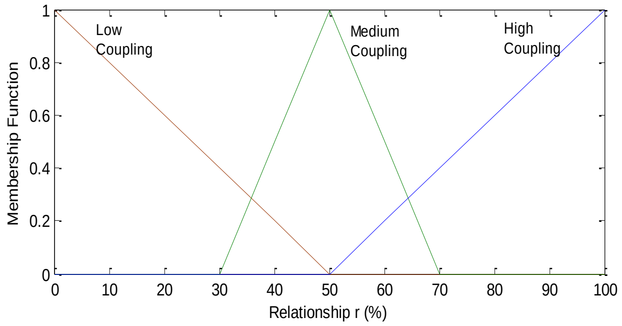
Rule ®	S_1	S_2	S_3	S_4	S_5	…….	S_{n-1}	S_n	Assurance Level
1	E	E	E	E	E	…….	E	E	LTA
2	E	E	E	E	E	…….	E	A	LTA
3	E	E	E	E	E	…….	E	D	LTA
4	E	E	E	E	E	…….	A	E	LTA
α	⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
α+1	A	A	A	A	A	…….	A	A	MTA
α+2	A	A	A	A	A	…….	A	E	MTA
α+3	A	A	A	A	A	…….	A	D	MTA

α+4	A	A	A	A	A	…….	E	A	MTA
β	⋮	⋮	⋮	⋮	⋮		⋮	⋮	⋮
β +1	D	D	D	D	D	…….	A	D	HTA
β +2	D	D	D	D	D	…….	D	E	HTA
β +3	D	D	D	D	D	…….	D	A	HTA
β +n	D	D	D	D	D	…….	D	D	HTA

4.3.3 Attribute Act

Attribute act can be expressed as the relationship among the sensed physical phenomena of sensor nodes. Basically, common relationship should exist among the physical phenomena like temperature and pressure in multi sensor node [14]. The proposed anomaly detection system's accuracy is increased by incorporating attribute act with spatial and temporal correlation acts. Multi-sensor senses the number of readings with respect to number of attributes (A_n) sensed by the node. Fully dependent attribute values should be coherent with each other. For this reason, when dealing with anomaly detection logic, attribute cohesive concepts are added. The attribute shield is augmented with the rules in fuzzy reasoning. This attribute act rule is applied at each node in the cluster generated by RFCM algorithm. **Fig.5** shows the confidence decision making of attribute act. In **Table 3** three variables are declared as Low Coupling (LC), Medium Coupling (MC), and High Coupling (HC). These are used to analyze the dependency of attributes readings. The format of the rules and membership function $\mu_{AA}(c)$ described in attribute act is as follows:

IF A_1 is HC and A_2 is HC and A_3 is HC ...... and
A_n is HC;
THEN Correlation assurance level is HAA



The assurance levels of attribute act are classified as Low Attribute Act (LAA), Medium Attribute Act (MAA) and High Attribute Act (HAA) where, LAA denotes less dependency, MAA comprises of semi-dependency among the attributes and HAA expresses the full dependency relationship among the attribute values of sensor node.

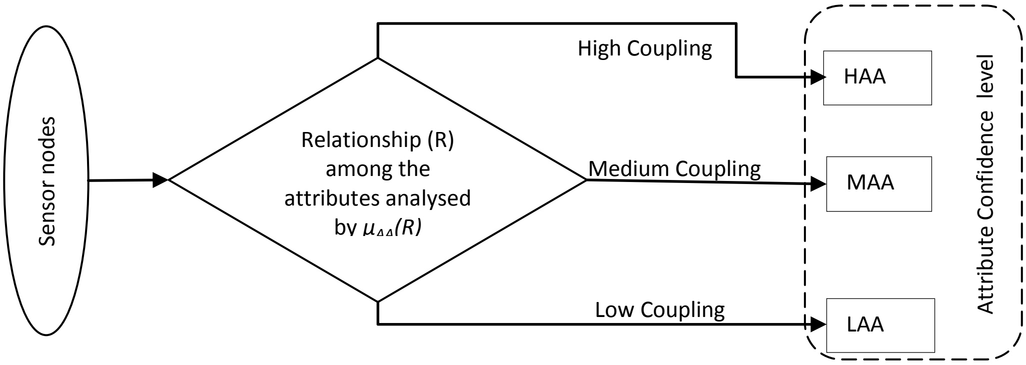


Fig. 5. Decision making of attribute act

Table 3. Attribute Act Rule Structure

Rule®	A_1	A_2	A_3	…….	A_{n-1}	A_n	Assurance Level
1	LC	LC	LC	…….	LC	LC	LAA
2	LC	LC	LC	…….	LC	MC	LAA
3	LC	LC	LC	…….	LC	HC	LAA
4	LC	LC	LC	…….	MC	LC	LAA
α	⋮	⋮	⋮		⋮	⋮	⋮
α+1	MC	MC	MC	…….	MC	MC	MAA
α+2	MC	MC	MC	…….	MC	HC	MAA
α+3	MC	MC	MC	…….	MC	LC	MAA
α+4	MC	MC	MC	…….	HC	MC	MAA
β	⋮	⋮	⋮		⋮	⋮	⋮
β +1	HC	HC	HC	…….	MC	HC	HAA
β +2	HC	HC	HC	…….	HC	LC	HAA
β +3	HC	HC	HC	…….	HC	MC	HAA
β +n	HC	HC	HC	…….	HC	HC	HAA

4.3.4 Anomaly Detection with Comparative Correlation Act

Anomaly detection with comparative correlation system comprises spatial, temporal and attribute acts. Test data is evaluated by using proactive fuzzy system. In **Table 4** three correlation act's assurance level are declared as linguistic variables for final proactive anomaly detection system. **Fig. 6** shows the final decision making process with combined correlation acts. The anomaly assurance levels of the proposed system are classified as Inferior Nodes (IN), Doubtful Nodes (DN) and Superior Nodes (SN). Anomaly detection assurance level is judged by self-assurance of Spatial Act (SA), Temporal Act (TA) and Attribute Act (AA). The format of the rules described in anomaly detection engine is as follows:

IF SA is LSA and TA is LTA and AA is LAA;
THEN Anomaly classification is IN

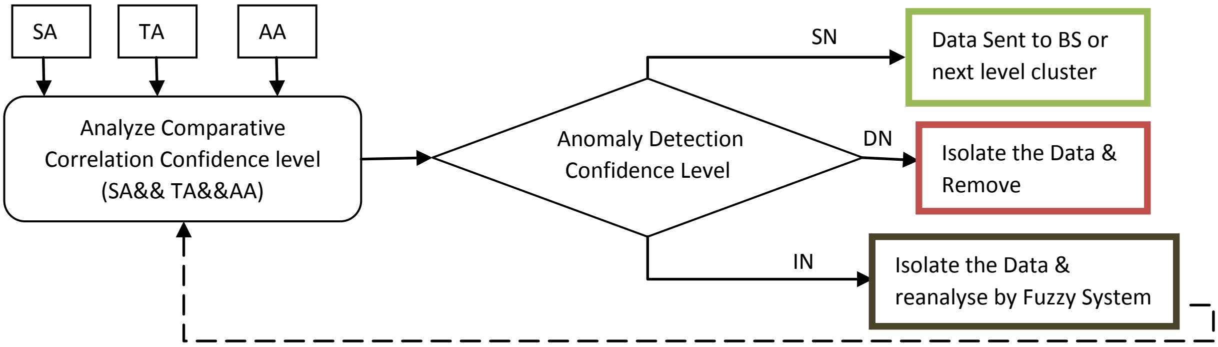

SA
TA
AA
Analyze Comparative Correlation Confidence level (SA&& TA&&AA)
Anomaly Detection Confidence Level
SN
DN
IN
Data Sent to BS or next level cluster
Isolate the Data & Remove
Isolate the Data & reanalyse by Fuzzy System

Fig. 6. Framework model of Anomaly with correlation acts

Table 4. Anomaly detection rule structure

Rule®	SA	TA	AA	Anomaly Assurance Level
1	LSA	LTA	LAA	IN
2	LSA	LTA	MAA	IN
3	LSA	LTA	HAA	IN
4	LSA	MTA	LAA	IN
5	LSA	HTA	LAA	IN
6	LSA	MTA	MAA	SN
7	LSA	MTA	HAA	DN
8	LSA	HTA	MAA	SN
9	LSA	HTA	HAA	DN
10	MSA	LTA	LAA	IN
11	MSA	LTA	MAA	SN
12	MSA	LTA	HAA	DN
13	MSA	MTA	LAA	SN
14	MSA	HTA	LAA	DN
15	MSA	MTA	MAA	SN
16	MSA	MTA	HAA	SN
17	MSA	HTA	MAA	DN
18	MSA	HTA	HAA	SN
19	HSA	LTA	LAA	IN
20	HSA	LTA	MAA	DN
21	HSA	LTA	HAA	SN
22	HSA	MTA	LAA	DN
23	HSA	HTA	LAA	DN
24	HSA	MTA	MAA	SN
25	HSA	MTA	HAA	SN
26	HSA	HTA	MAA	SN
27	HSA	HTA	HAA	SN

4.3.5 Mitigating Correlation Rules

The number of correlation rules generated by fuzzy rule mining technique can be large. Large number of rules may contain tedious rules that may mislead the classification process and they may increase the computation time to classify the anomaly [31] [32]. Trimming repetitive and unsuitable rules will increase the accuracy of the performance of the proposed system. The following three rule mining conditions are examined in removing unimpressive rules .

1. First, eliminate specific rules and retain only the general rules with high confidence. i.e Joining rules with akin conclusion.

   It is assumed that there are two rules only

   ®$_1$: X ⇒ Z and ®$_2$: Y ⇒ Z and X⊆Y, first rule ®$_1$ is the general rule and accepted if

   a. the confidence of ®$_1$ is greater than the confidence of ®$_2$ or
   b. the confidence of ®$_1$ is equal to the confidence of ®$_2$ but support of ®$_1$ is greater than support of ®$_2$ or
   c. both the confidence and support of ®$_1$ is equal to the confidence and support of ®$_1$ and ®$_1$ ⊂ ®$_2$ then ®$_2$ is eliminated.
2. Second, the controversy rules like ®$_1$: X ⇒ Y and ®$_2$: X ⇒ Z are also be eliminated.
3. Third, remove imperfect rules which do not satisfy the spatial,temporal and attribute restrictions. i.e every possible combination of input variables should be analyzed by each rule in fuzzy inference system.

In this work, these three rule mining conditions are considered to eliminate duplicate, uninteresting and controversial rules and produce a trimmed set of rules. Final Rules are stored in the transactional database which has been used for building a new proposed anomaly detection. If none of the rules in the rule-base is persuaded, we pioneer a default rule is pioneered.

5. Experimental Classification Results and Analysis

The proposed proactive anomaly detection system is tested using both synthetic and real data sets. In this section, these experiments and the results are described. This is performed in terms of anomaly detection rate or sensitivity, specificity and false alarm rate for both clean and unclean data sets. The algorithm on two real-life data sets is evaluated. The first dataset is obtained from Intel Berkeley Research Lab (IBRL) [33] and the second dataset is obtained from SensorScope project, which was located at the Grand-St-Bernard (GSB) pass at 2400 m between Switzerland and Italy [34]. **Fig. 7** shows the deployment location of sensor nodes in the IBRL. **Fig. 8** shows the deployment location of sensor nodes in the Grand St. Bernard deployment. In addition, comparative analysis is also performed between the proposed system and the work in [20] to check the rare effectuation of the proposed anomaly system.

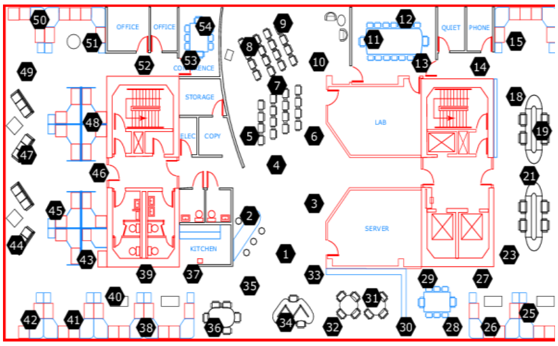


Fig. 7. Sensor nodes in IBRL deployment

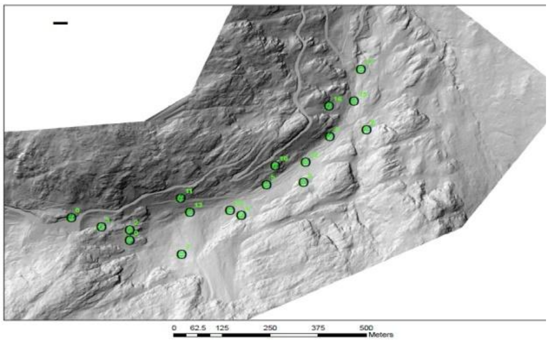


Fig. 8. Sensor nodes in GSB

5.1. Performance Evaluation

The performance of the proposed anomaly system is evaluated in terms of overall accuracy, sensitivity, specificity, positive predictive value and negative predictive value. Overall accuracy is the ability of the proposed system to detect the anomaly correctly. Sensitivity or Detection rate is the ability of the system to detect positive (abnormal) cases. Specificity is the ability of the system to detect negative (normal) cases. False Alarm Rate (FAR) is the ability of the system to detect positive (normal) cases. Positive Projection Rate (PPR) is defined as the proportion of positive test results that are true positives and Negative Projection Rate (NPR) is the proportion of those with a negative test result. The measures are described below:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \qquad \text{Sensitivity} = \frac{TP}{TP + FN}$$

$$\text{Specificity} = \frac{TN}{TN + FP} \qquad \text{False Alarm Rate} = \frac{FP}{FP + TN}$$

$$\text{Positive Projection Rate} = \frac{TP}{TP + FP} \qquad \text{Negative Projection Rate} = \frac{TN}{TN + FN}$$

where TP, TN , FP and FN are referred to True Positive rate (abnormal data correctly classified) ,True Negative rate (normal data correctly classified), False Positive rate (normal data classified as abnormal) and False Negative rate (abnormal data classified as normal one) respectively.

5.2. IBRL Dataset

IBRL data set is analysed, which has 54Mica2Dot sensors with 4 attributes, during the 720 hours period between 28th February 2004 and 5th April 2004. During the 30 day period, the 54 sensors collected about 2.3 million readings [33]. The data in the data set is sticked at the time of exportation, namely March 2004 during the time interval 00:00 am to 03:59 am. The skeleton structure of the data set is illustrated in **Table 5**. Only three features are considered namely temperature, humidity and voltage. Particularly variations in voltage are highly correlated with temperature.

Table 5. Skeleton Structure of Intel Lab Data Set

date: yyyy-mm-dd	time: hh:mm:ss.xxx	epoch:int	moteid:int	temperature: real	humidity: real	light: real	voltage :real

The synthetic data is also generated for the above said features by using the multivariate random generation function with different corruption level for checking scalability of the proposed anomaly detection system.

5.3. SensorScope Dataset

The SensorScope project of GSB data set is analysed, which has 23 sensors with several meteorological attributes such as temperature, humidity, solar radiation, soil moisture, and so on [34]. During the period of 2 months between September 2007 and October 2007, the 23 sensor nodes sense the readings with a sampling frequency of 2 minutes and are grouped in two clusters. Five numbers of nodes are enclosed in one cluster and remaining eighteen numbers of nodes are enclosed in another cluster.

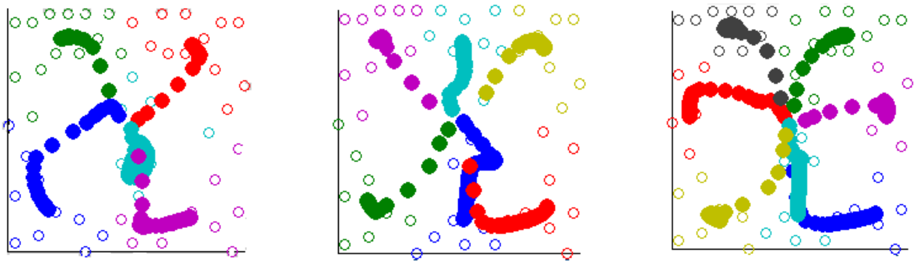
Table 6. Skeleton Structure of GSB Data Set

Station ID	Year	Month	Hour	Minute	Second	Time	Ambient Temperature [°C]	Surface Temperature[° C]	Solar Radiation [W/m^2]	Relative Humidity [%]	Soil Moisture [%]	Watermark [kPa]	Rain Meter [mm]	Wind Speed [m/s]	Wind Direction [°]

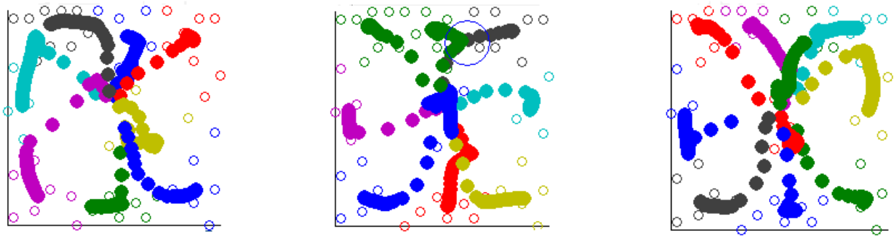
The data in the data set is kept intact at the time of exportation, namely 29-30 September 2007 during the time interval 06:00 am to 14:00 am. The skeleton structure of the data set is illustrated in **Table 6**. Only three features namely ambient temperature, surface temperature and relative humidity are considered.

5.4. Evaluation on Datasets

To assess the proposed method, first the data sets are normalized by identifying extreme values or specious effects and removing them. Cleaned data were regarded as customary data with the use of scatter plot and chi-square test. Anomalies were randomly inserted in one or more nodes in each cluster, varying the range of data corruption level from 10% to 70%. Proposed system is implemented in the MATLAB version 2013 environment. The accuracy of data classification is investigated with respect to identifying anomalous and normal data points by calculating the values for sensitivity, specificity and positive projection rate. Considering the IBRL dataset, the proposed System is applied to several numbers of clusters ranging from 5 to 10. Robust fuzzy c- means algorithm is applied for finding optimal number of clusters in the data set. **Fig. 9** shows the number of optimal clusters used for evaluating anomaly detection technique by using IBRL. Six cases were selected with respect to the number of clusters from 5 to 10. By considering the GSB dataset, three cases were selected with respect to the number of clusters from 3 to 5. **Fig. 10** shows the optimal clusters used for evaluating anomaly detection technique in GSB.

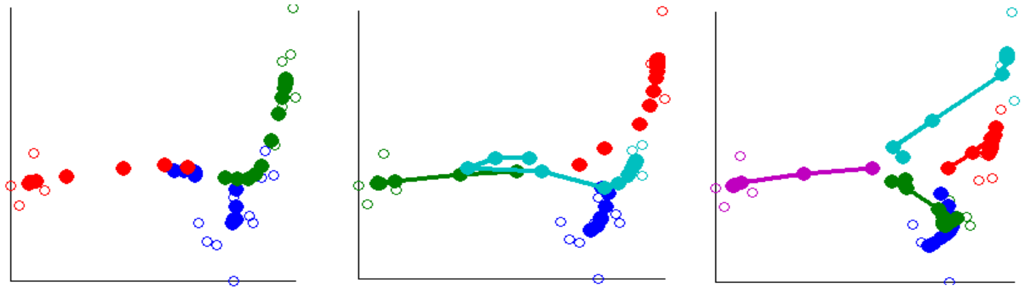


a) 5 clusters b) 6 clusters c) 7 clusters



d) 8 clusters e) 9 clusters f) 10 clusters

Fig. 9. Robust Fuzzy C-means Clusters in IBRL



a) 3 clusters b) 4 clusters c) 5 clusters

Fig.10. Robust Fuzzy C-means Clusters in GSB

Each cluster readings were experimented by applying spatial, temporal and attribute acts. Assurance level of each act can be evaluated for separating inferior, superior and doubtful nodes. **Fig. 11** depicts the relationship among the attributes involved in the evaluation by using IBRL and GSB data sets. **Fig. 12.1** and **Fig. 12.2** show the membership functions of sensor readings in cluster 5 and report low, medium and high assurance level based on the correlation act.

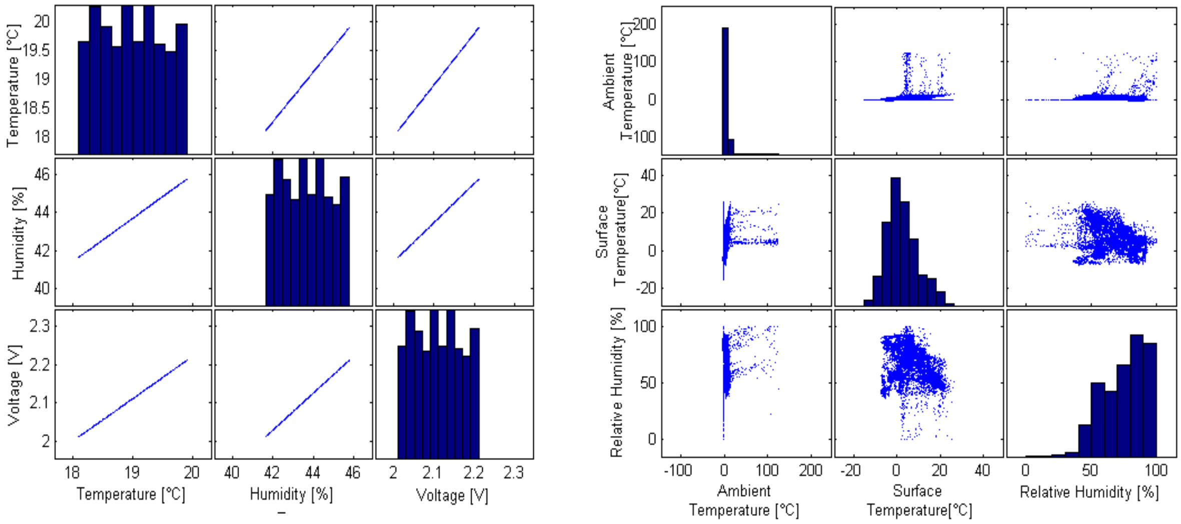


Fig. 11. Data Distribution with attribute correlation in IBRL (left), Data Distribution with attribute correlation in GSB (right)

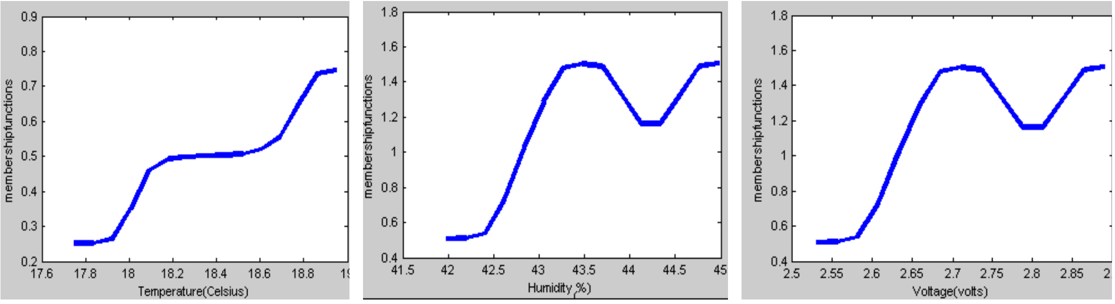


Fig. 12.1 Fuzzy Membership function with attributes in IBRL

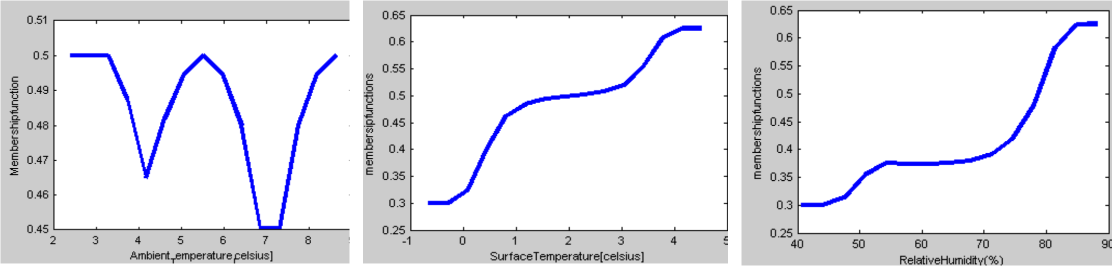


Fig. 12.2 Fuzzy Membership function with attributes in GSB

In general, detection accuracy of the proposed system is the ability to diagnose the anomalous data correctly. Sensitivity measures the proportion of actual positive cases (Anomaly) which are correctly identified as the percentage of incorrect data is correctly identified. Specificity measures the proportion of negative cases (Conformity) which are correctly identified as the percentage of correct data are correctly identified. FAR measures the proportion of positive cases (Anomaly) which are incorrectly identified as the percentage of correct data are incorrectly identified. PPR implies probable presence of anomaly in a given positive test result. NPR implies the probable absence of anomaly in a given negative test result. **Table 7** shows the overall performances of proposed anomaly detection system. Here the performance of the proposed system is compared with that of approach in [20]. Therefore, it is clear that the proposed system achieves significant gain in detecting accuracy compared to the existing work [20].

Table 7. Performances of Fuzzy-spatial, Fuzzy-Temporal, Fuzzy-Attribute and existing work compared with proposed correlated fuzzy system

Data Set	Techniques	Accuracy	Sensitivity	Specificity	FAR	PPR	NPR
IBRL DATA SET	**CCFS**	99.87	99.74	98.85	2.57	95.87	96.64
	Existing work in [20]	98.33	95.00	99.00	13.57	96.52	92.45
	Fuzzy Temporal	83.40	82.50	87.30	8.52	88.70	79.24
	Fuzzy Attribute	88.11	85.37	89.54	6.54	86.67	77.55
	Fuzzy Spatial	80.30	83.00	81.70	10.95	84.59	82.31
GSB DATA SET	**CCFS**	99.31	98.31	97.83	4.28	96.53	95.61
	Existing work in [20]	97.52	96.45	95.62	7.64	97.49	90.58
	Fuzzy Temporal	87.87	88.50	77.44	10.58	89.11	84.20
	Fuzzy Attribute	91.40	93.90	81.82	7.25	88.51	78.69
	Fuzzy Spatial	86.51	87.09	76.53	8.94	84.28	85.33

Fig. 13 and **Fig. 14** illustrate the performance of the proposed system for evaluating IBRL and GSB dataset. It is observed that the approach in [20] has less sensitivity and high false alarm rate compared to CCFS. Specifically, the proposed method considers fuzzy based correlation of data, offers 0% false alarm and 100% detection rate till 40% of the nodes in the network are found to be anomalous. Even for corruption level above 40% to 70% the average false alarm created is simply 2.57% in IBRL and 4.28% in GSB data set respectively.

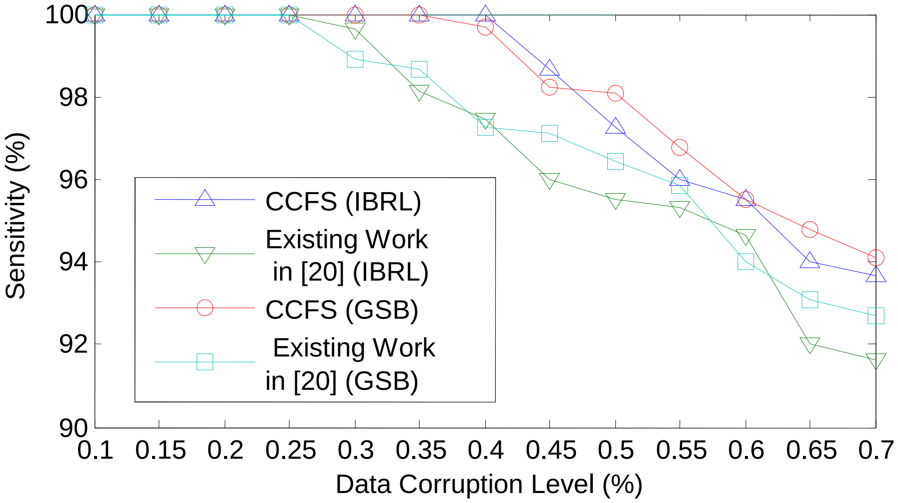


Fig. 13. Sensitivity for altering corruption level

Fig. 15 shows the performance of proposed system with varying cluster sizes. For this evaluation, different set of test data are randomly generated. The detection rate and false alarm rate are evaluated both for IBRL and GSB dataset. In each case, five clusters in IBRL and 3 clusters in GSB are considered and the anomaly is randomly inserted in the clusters. As observed from this figure, the proposed system improves the detection rate by taking into reflection and combining efficiently several correlation acts with respect to the optimal clusters through the use of RFCM. As observed in **Fig. 16**, anomaly detection and misdetection fractions are attractively stable while the numbers of nodes from 50 to 500 are increased. This result implies that our fuzzy based anomaly detection has very fastidious scalability as it works well under different network sizes without losing its performance.

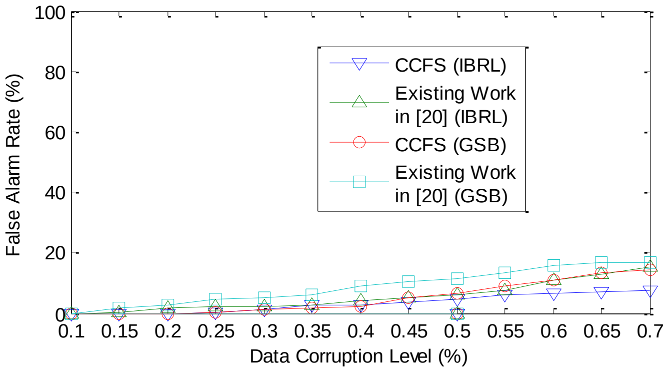
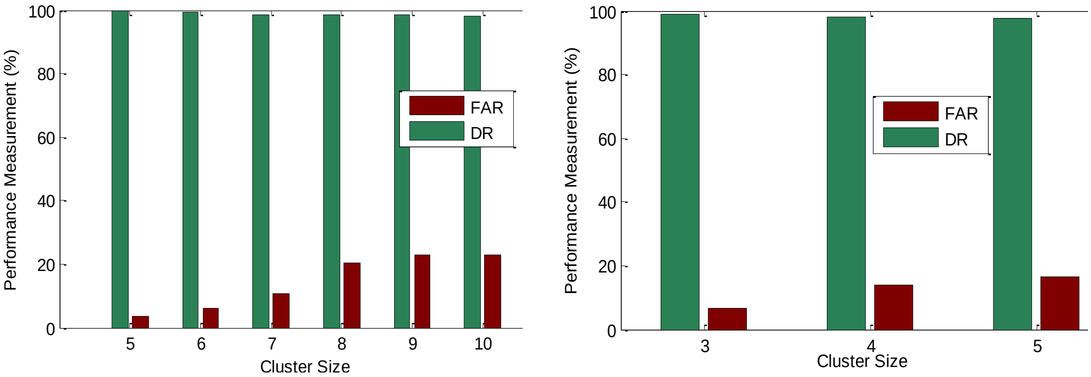


Fig. 14. Sensitivity for altering corruption level



a) IBRL Data set b) GSB Data set

Fig. 15. Performance assessment for shifting cluster size

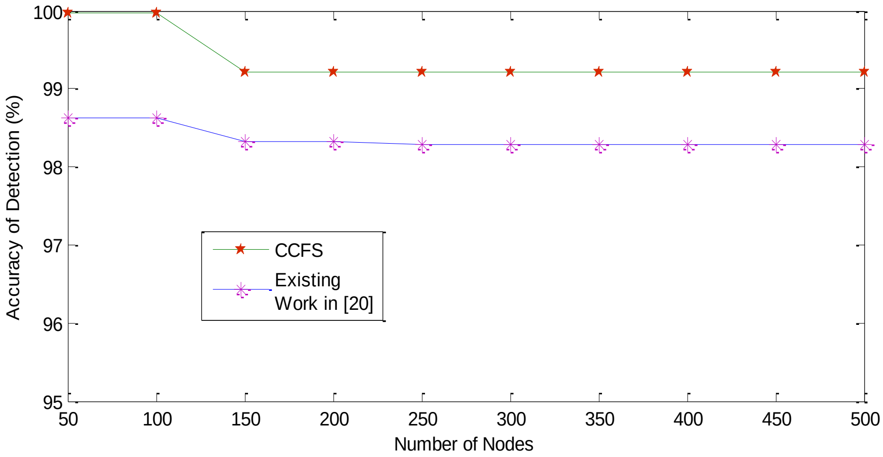


Fig. 16. Scalability Comparison

Finally, these performances at various anomalous percentages ranging from 10% to 70% are evaluated for 500 nodes. Anomalous percentage is defined as the ratio between total numbers of malicious nodes in network to total number of nodes present in the current network.

Table 8. Complexity Analysis of Anomaly Detection

Techniques	Computational Complexity	Communication Complexity	Memory Complexity
CCFS	$O(ndc+ \alpha+p+q)$	$O(nd)$	$O(ndr)$
Ellipsoidal SVM based	$O(nd^2)$	$O(nvd)$	$O(nvd^2)$
Approach in [20]	$O(nd^2)$	$O(nvd^2)$	$O(nvd^4)$
Statistical based	$O(n(n-1)d+pq)$	$O(nd^2)$	$O(nd^2+(n-1)d^2)$
Agglomerative clustering based	$O(nd^6c)$	$O(nd^3)$	$O(nd^4)$

Legends: n - Number new of records at time, d-dimension of the observations, α- Attribute correlation, p-spatial correlation, q- temporal correlation, c - Number of clusters, v-intermediate values, r-number of rules

To further understand the behaviour of the proposed CCFS approach, it is necessary to compare it with well established state of the art anomaly detection algorithm. To evaluate the efficiency of the CCFS model, the computational complexity, communication overhead and memory complexity are considered. The computational complexity incurred by our model is O(nd+α+p+q) related to the calculation of spatial, temporal and attribute correlation. The communication overhead is O(nd). Correlation act has no communication overhead because the analysis was performed locally at each node. The memory complexity is represented as O(ndr), where r represents number of rules. Less number of rules saves more memory space. **Table 8** explains the complexity of different state of the art anomaly detection approaches. Albeit our method infers this method proves that the detection rate is high compared to other methods. Computational complexity, communicational complexity and memory complexity are slightly reduced when compared to other techniques.

6. Conclusion

In this paper, a system which employs fuzzy based anomaly detection is developed and it uses fuzzy logic to classify anomaly and conformity based on the spatial, temporal and attribute correlation acts. Each act is evaluated for various numbers of clusters generated by robust fuzzy c-means clustering. After cataloguing of data, superior nodes are labelled as customary, inferior nodes as anomaly and doubtful nodes are retested until fixing the final decision. The experimental result proves that the proposed CCFS outperforms existing work in various aspects like anomaly detection accuracy, false alarm, sensitivity and specificity in decision making support.

References

[1] P. Rawat, K.D.Singh, H.Chaouchi and J.M.Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies," *Journal of super computing,* vol. 68, pp. 1-48, April 2014. Article (CrossRef Link)

[2] G.J. Pottie and W.J. Kaiser, "Wireless Integrated network sensors," *ACM Communications*, Vol. 43, no.5, pp. 51-58 May 2000. Article (CrossRef Link)

[3] H.Xu, L. Huang, Y. Zhang, H. Huang, S. Jiang, G.Liu, "Energy Efficient cooperative data aggregation for wireless sensor networks," *Journal of parallel and distributed computing ,* vol. 70, no. 9, pp. 953-961 ,September 2010. Article (CrossRef Link)

[4] Bo Sun, Xuemei Shan, Kui Wu, Yang Xiao, "Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks," *IEEE Systems Journal,* vol. 7, no.1, pp.13 - 25, March 2013. Article (CrossRef Link)

[5] S Roy, M Conti, S Setia, S Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Information Forensics and Security, vol.*7, no. 3, pp.1040–1052, June 2012. Article (CrossRef Link)

[6] Miao Xie, Song Han, Biming Tian, Sazia Parvin, "Anomaly Detection in Wireless Sensor Networks: A survey," *Journal of Network and computer Applications*, vol.34, pp.1302-1325, March 2011. Article (CrossRef Link)

[7] O'Reilly C, Gluhak A, Imran M.A, Rajasegarar S, "Anomaly Detection in Wireless Sensor

Networks in a Non-Stationary Environment," *IEEE Communications Surveys & Tutorials,* vol. 16. no.3, pp.1-20, September 2013. Article (CrossRef Link)

[8] P.Forero, A. Cano, G.Giannakis, "Distributed clustering using wireless sensor networks," *IEEE Journal of Selected Topics in Signal processing,* vol.5, no.4,pp 702-724, August 2011. Article (CrossRef Link)

[9] Neamatollahi, P, Mashhad Iran, Taheri H, Naghibzadeh M,Yaghmaee M, "A hybrid clustering approach for prolonging lifetime in wireless sensor networks," *IEEE International Symposium on Computer Networks and Distributed Systems*, pp. 170-174, February 2011. Article (CrossRef Link)

[10] Baig, Z.A. Khan, S.A., "Fuzzy Logic-Based Decision Making for Detecting Distributed Node Exhaustion Attacks in Wireless Sensor Networks," in *Proc. of Second International Conference on Future Networks, IEEE,* pp.185-189, January 2010. Article (CrossRef Link)

[11] Daniel-Ioan Curiac , Constantin Volosencu, "Ensemble based sensing anomaly detection in wireless sensor networks," *Journal of Expert Systems with Applications,* vol. 39, pp. 9087–9096, March 2012. Article (CrossRef Link)

[12] Suat Ozdemir, Hasan Çam , "Integration of False Data Detection With Data Aggregation and Confidential Transmission in Wireless Sensor Networks," *ACM Transaction on Networking*, vol. 18, no. 3, pp.736-749, June 2010. Article (CrossRef Link)

[13] Chitra Devi.N, Palanisamy .V, Baskaran.K and Barakkath Nisha.U, "Outlier aware Data Aggregation in Distributed Wireless Sensor Network using Robust Principal Component Analysis," in *Proc. of Second International Conference on Computing, Communication and Networking Technologies, IEEE,* pp. 1-9, July 2010. Article (CrossRef Link)

[14] Janakiram .D Mallikarjuna.A, Reddy.V, Kumar.P, "Outlier Detection in wireless sensor networks using Bayesian belief Networks," in *Proc. of International IEEE Workshop on Software for Sensor Networks*, pp. 1-6, August 2006. Article (CrossRef Link)

[15] Chitra Devi.N, Palanisamy .V, Baskaran.K and Prabeela S "Efficient distributed clustering based anomaly detection algorithm for sensor stream in clustered Wireless Sensor Network," *European Journal of Scientific Research,* vol. 54, no.4, pp.484-498, June 2011. Article (CrossRef Link)

[16] Yang Zhang, Nirvana Meratnia, Paul J.M Havinga, "Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine," *Journal of Ad Hoc Networks,* vol. 11, pp. 1062-1074, November 2012. Article (CrossRef Link)

[17] Y. Zhang, N.A.S. Hamm, N. Meratina, A.Stein, M. Van de Voort and P.J.M. Havinga, "Statistics based outlier detection for wireless sensor networks," *International Journal of Geographical Information Science,* pp. 1-20, December 2011. Article (CrossRef Link)

[18] K. Kapitanova, S. H. Son and K.-D. Kang, "Using fuzzy logic for robust event detection in wireless sensor networks," *Journal of Ad Hoc Networks*, vol.10, pp. 709-722, June 2011. Article (CrossRef Link)

[19] Q. Liang, L. Wang, "Event detection in wireless sensor networks using fuzzy logic system," in *Proc. of International Conference on Computational Intelligence for Homeland Security and Personal Safety, IEEE*, pp. 52–55, April 2005. Article (CrossRef Link)

[20] Heshan Kumaragea, Ibrahim Khalil , Zahir Tari , Albert Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modeling," *Journal of Parallel and Distributed Computing*, vol. 73.pp.790–806., March 2013. Article (CrossRef Link)

[21] L.A. Zadeh, "Soft Computing and Fuzzy Logic," *ACM Journal of Software*, vol. 11, no. 6, pp.48-56, November 1994. Article (CrossRef Link)

[22] H.J.Zimmermann, "Fuzzy Set Theory and Its Applications," *Publisher kluwer Academic Publishers Norwell*, 3rd edition, pages 435, 1996 Article (CrossRef Link)

[23] J.C. Bezdek, R. Ehrlich, W. Full, "FCM: the fuzzy c-means clustering algorithm," *Journal of Computers & Geosciences*, vol.10, no.3, pp.191–203 March 1984. Article (CrossRef Link)

[24] H.Izakian, W.Pedrycz, "Anomaly detection in time series data using a fuzzy c means clustering," *IFSA World Congress and NAFIPS Annual Meeting, IEEE*, pp.1513-1518, June

2013. Article (CrossRef Link)

[25] S.Shamshirband, A.Amini, N.Anur ,M.Kiah, Y.Teh and S.Furnell, "D-FICCA: A density based fuzzy imperialist competitive clustering algorithm for intrusion detection in wireless sensor networks," *Journal of Measurement, Elsevier*, vol. 55,pp. 212-226, May 2014. Article (CrossRef Link)

[26] C. Tang, S.G. Wang, "Adaptive fuzzy clustering model based on internal connectivity of all data points," *Acta Automatica Sinica,* Issue no.11, pp.1544-1556, 2010. Article (CrossRef Link)

[27] Barnett, V. & Lewis, T, "Outliers in Statistical Data," *3rd edition. John Wiley & Sons,* 1994. Article (CrossRef Link)

[28] Weiling Cai, Song chen, Daoqiang Zhang, "Fast and robust fuzzy c-means clustering algorithms incorporating local information for image segmentation," *Journal of Pattern Recognition*, vol. 40, no.3, pp 825-838, March 2007. Article (CrossRef Link)

[29] M. C. Vuran, B. Akan, and I.F. Akyildiz, "Spatio-temporal correlation: Theory and applications for wireless sensor networks," *Computer Networks: International Journal of Computer and Telecommunication Networking,* vol.45, no.3, pp. 245-259, June 2004. Article (CrossRef Link)

[30] Zhidan Liu ,Wei Xing ,Bo Zeng, Yongchao Wang ,Dongming Lu, "Distributed Spatial Correlation-based Clustering for Approximate Data Collection in WSNs," in *Proc. of IEEE International Conference on Advanced Information Networking and Applications,* pp.56-63, March 2013. Article (CrossRef Link)

[31] H. Ishibuchi, T. Nakashima, T. Kuroda, "A hybrid fuzzy GBML algorithm for designing compact fuzzy rule-based classification systems," in *Proc. of IEEE International Conference on Fuzzy Systems*, pp. 706–711. May 2000. Article (CrossRef Link)

[32] Sushmita Mitra, and Yoichi Hayashi, "Neuro–Fuzzy Rule Generation: Survey in Soft Computing Framework," *IEEE Transactions on Neural Networks*, vol.11, no.3, pp 1-20, May 2000. Article (CrossRef Link)

[33] IBRL Dataset: http://db.csail.mit.edu/labdata/labdata.html

[34] SensorScope Dataset: http://lcav.epfl.ch/page-86035-en.html

U. Barakkath Nisha had received her Bachelor of Engineering in Computer Science & Engineering in 2008 with distinction from Anna University, Chennai. She got her Master of Engineering in Computer Science & Engineering from Anna University, Coimbatore in 2010 as full time student with distinction. Currently she is working as assistant professor in Department of Computer Science & Engineering in PSNA College of Engineering of Technology, Dindigul. Her research interests are Ad hoc Networks, Wireless Networks, Information Security, Computer Networks, and Sensor Networks etc. She had published various national, international conferences related to Wireless Sensor Networks for the past 2 years.

N. Uma Maheswari received her M.E in Computer Science and Engineering from the Madras University, Chennai, India in 2002 and Ph.D. in Information and Communication Engineering in 2011 from Anna University, Chennai. Currently, she is working as a Professor in the Department of Computer Science and Engineering at the P.S.N.A. College of Engineering and Technology, Dindigul, India. She has totally 15 years of teaching experience which includes 11 years of research experience. Her research interests include Biometrics, Image processing, Compiler design, Artificial Intelligence, Speech Processing, and Wireless Sensor Networks. She has published 20 papers in International journals, 2 papers in National journals, and presented 22 papers at International conferences, and 10 papers at National conferences. She has co-authored a book entitled ‘‘Compiler Design’’ published by Yes Dee Publishing. She is a recognized Ph.D. supervisor in Anna University of Technology in the area of Image processing; Cloud computing, Network security and Networks.

R. Venkatesh received his M.E in Computer Science and Engineering from Anna University Chennai in India, in 2007 and Ph.D. Computer Science and Engineering in 2010 at Alagappa University, Karaikudi. Currently, he is working as a Professor in the Department of Information Technology in PSNA College of Engineering and Technology, Dindigul, India. He has totally twenty years of teaching experience which includes 11 years of research experience. He has published 20 papers in International journals, 2 papers in National journals, and presented 22 papers at International conferences and 10 papers at National conferences. His research interests include Biometrics, Artificial intelligence, Compiler design, Neural Networks, Soft computing, Network security and Networks. He has co-authored a book entitled ‘‘Compiler Design’’ published by Yes Dee Publishing.

R.Yasir Abdullah received his Bachelor of Engineering in Electronics & Communication Engineering in 2005 from Anna University , Chennai. He got his Masters in Computer Science & Engineering as full time student with distinction by Anna University - Coimbatore, Tamilnadu, India in 2009. Currently he is working as assistant professor in Computer science Department for SSCET, Palani, India. His research interests’ lie in Wireless Networks, Information Security, Computer Networks, Sensor Networks etc. He is been publishing various national conferences related to Wireless Networking for the past 3 years.