ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20211109073558
Original scientific paper

A Novel Biometric Key Security System with Clustering and Convolutional Neural Network for WSN

Nivedetha BALAN*, Vennila ILA

Abstract: Development in Wireless Communication technologies paves a way for the expansion of application and enhancement of security in Wireless Sensor Network using sensor nodes for communicating within the same or different clusters. In this work, a novel biometric key based security system is proposed with Optimized Convolutional Neural Network to differentiate authorized users from intruders to access network data and resources. Texture features are extracted from biometrics like Fingerprint, Retina and Facial expression to produce a biometric key, which is combined with pseudo random function for producing the secured private key for each user. Individually Adaptive Possibilistic C-Means Clustering and Kernel based Fuzzy C-Means Clustering are applied to the sensor nodes for grouping them into clusters based on the distance between the Cluster head and Cluster members. Group key obtained from fuzzy membership function of prime numbers is employed for packet transfer among groups. The three key security schemes proposed are Fingerprint Key based Security System, Retina Key based Security System, and Multibiometric Key based Security System with neural network for Wireless Sensor Networks. The results obtained from MATLAB Simulator indicates that the Multibiometric system with kernel clustering is highly secured and achieves simulation time less by 9%, energy consumption diminished by 20%, delay is reduced by 2%, Attack Detection Rate is improved by 5%, Packet Delivery Ratio increases by 6%, Packet Loss Ratio is decreased by 27%, Accuracy enhanced by 2%, and achieves 1% better precision compared to other methods.

Keywords: biometric key; clustering; convolutional neural network: facial expression; fingerprint; WSN

1 INTRODUCTION

Wireless Sensor Networks are deployed with large amount of tiny and economical sensor nodes for exchanging the data with any sensor nodes [1]. They communicate within the same or different clusters and face a lot of security threats during their transmission. By using the various clustering approaches, the grouping of nodes will be modified each time a network is formed. Inside a cluster, the members can be similar or of different characteristics [2]. When the entire network is subdivided into number of clusters, a cluster head is assigned to take care of all the transactions [3]. Clustering increases the inter and intra group packet transfer with less time and more security [4-6]. In order to provide a secure and safe communication biometric based authentication is one of the suitable approaches, as it identifies each individual with their physical and behavioural features [7]. Physical biometric indicates the physiological features on human beings like Finger-vein, Palm-print, Retina, and Face. Behavioural biometric considers the users cognitive behaviour like voice interaction with device, keystroke speed, handwriting, and many more. Each biometric feature is unique and used to differentiate the authorized user from a fake person. The usage of biometric methods is increasing day by day to protect the highly confidential information from unauthorized persons. Biometric key and fuzzy key [8] can be obtained from biometric texture and fuzzy membership functions [9].

The biometric features can be captured without impinging or interacting with the individual. Fingerprint detection is most commonly used Security enforcement method, as it is easy to capture and use. The images acquired will contain some unwanted noise and distortions, so they have to be filtered using filters [10]. Bilateral filter, fuzzy filter and adaptive median filter are the filters suitable to remove salt and pepper noises [11-14]. The texture properties of fingerprint are extracted using Haar Wavelet Transform [15]. Retina based identification is a biometric technology which makes use of unique blood vessel pattern of a user for recognition. This technique acquires and examines the structure of blood vessels on the thin nerve behind the eyeball that permits light to enter into the pupil. Facial recognition is the fastest and most excellent biometric identification of an individual using face images [16] that can be used in unsupervised areas with variation in obstacles, climatic changes, and interference. Using Facial expression, humans can be identified based on any of their facial emotions like angry, hatred, panic, glad, sorrow, and shock [17]. The existing systems utilize cryptographic methods, unimodal biometrics and small network size. Optimized Convolutional Neural Network (OCNN) model [18] is used in the proposed system to train people's biometric features like fingerprint, retina and facial expressions. An improved segmentation method and better Support Vector Machine (SVM) classifier based on fingerprint, retina and facial image identification using neural network gives better authentication for dynamic WSN.

2 PROPOSED METHODOLOGY

In this work, Multibiometric authentication key is generated for the clustered network to perform authorized packet transfer in WSN model. The three key schemes are Fingerprint Key based Security System (FKSS), Retina Key based Security System (RKSS), and Multibiometric Key based Security System (MKSS) for Wireless Sensor Networks, shown in Fig. 1. Multibiometric key based Security scheme uses three different biometric features like fingerprint, retina, and facial expression. This method is implemented in three stages: In stage 1, clustering is done separately by APCMC and KFCMC. In stage 2, Multibiometric key is generated from the texture features of fingerprint, retina and Facial expression images. In stage 3, key is verified using Optimized Convolutional Neural Network (OCNN) and packets are exchanged successfully.

2.1 Fingerprint Key Based Security System (FKSS)

FKSS methodology uses fingerprint biometric for creating user key. The fingerprint features are attained using Haar Wavelet Transform (HWT). Two stages of feature extraction are 2D wavelet decomposition for high pass filtering to measure rotation region and 1D wavelet decomposition for low pass filtering to get features of fingerprint.

Adaptive Possibilistic C-Means Clustering (APCMC) and Kernel based Fuzzy C-Means Clustering **(**KFCMC) clustering methods are utilized for grouping the nodes into clusters.

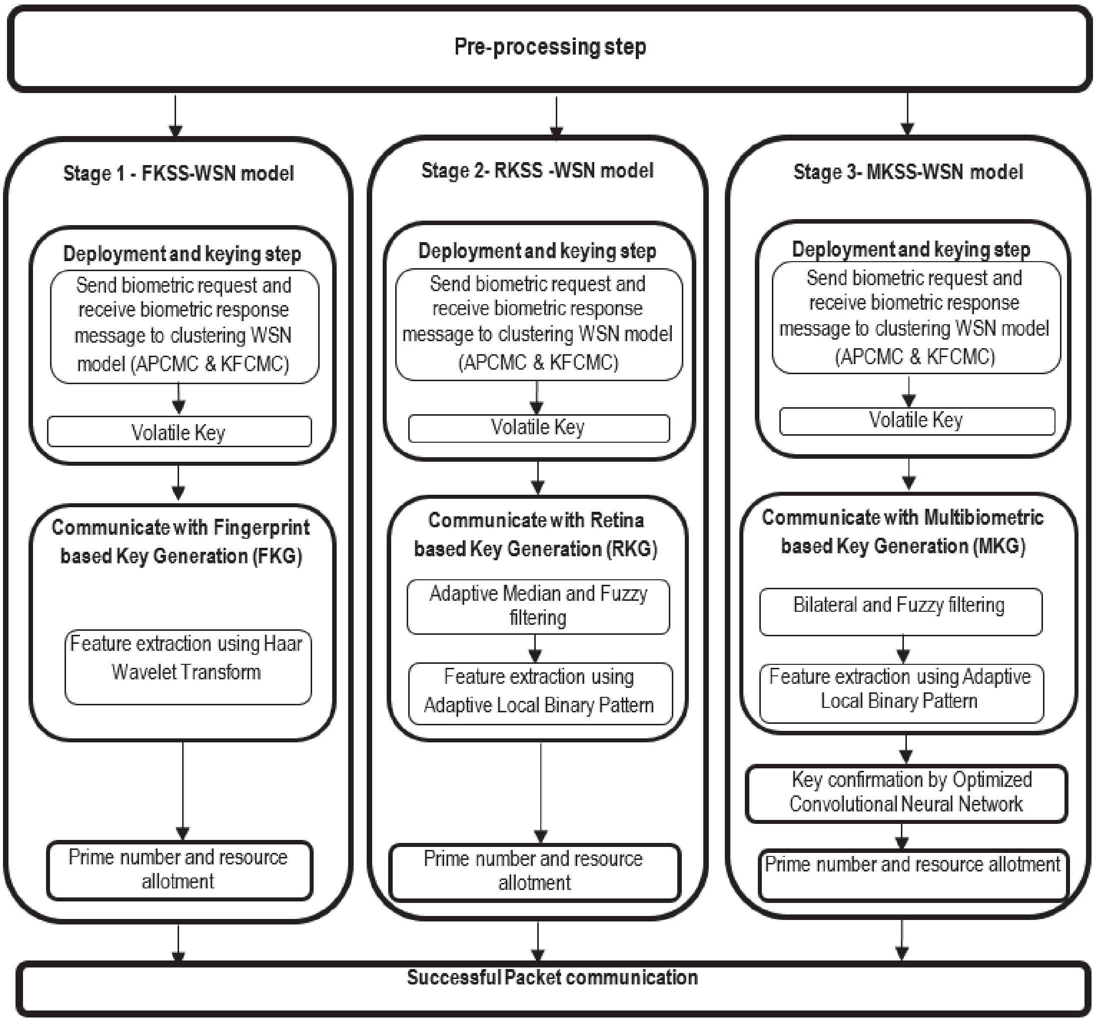
Pre-processing step
Stage 1 - FKSS-WSN model
Deployment and keying step
Send biometric request and receive biometric response message to clustering WSN model (APCMC & KFCMC)
Volatile Key
Communicate with Fingerprint based Key Generation (FKG)
Feature extraction using Haar Wavelet Transform
Prime number and resource allotment
Stage 2- RKSS -WSN model
Deployment and keying step
Send biometric request and receive biometric response message to clustering WSN model (APCMC & KFCMC)
Volatile Key
Communicate with Retina based Key Generation (RKG)
Adaptive Median and Fuzzy filtering
Feature extraction using Adaptive Local Binary Pattern
Prime number and resource allotment
Stage 3- MKSS-WSN model
Deployment and keying step
Send biometric request and receive biometric response message to clustering WSN model (APCMC & KFCMC)
Volatile Key
Communicate with Multibiometric based Key Generation (MKG)
Bilateral and Fuzzy filtering
Feature extraction using Adaptive Local Binary Pattern
Key confirmation by Optimized Convolutional Neural Network
Prime number and resource allotment
Successful Packet communication

Figure 1 Block diagram of proposed multibiometric security system

2.2 Retina Key Based Security System (RKSS)

RKSS scheme use Retina image for generating user private key. The image is filtered to remove noise using Adaptive Median filtering (AMF) and Fuzzy filtering. Adaptive Local Binary Pattern (ALBP) performs the feature extraction of retina. APCMC and KFCMC clustering methods are utilized for grouping the nodes into clusters.

2.3 Multibiometric Key Based Security System (MKSS)

MKSS method utilizes fingerprint, retina and facial expression as biometrics for the generation of biometric based user key. Then noises are filtered with bilateral filtering and Fuzzy filtering from all biometric traits. Adaptive Local Binary Pattern (ALBP) performs the feature extraction of both biometrics. APCMC and KFCMC clustering methods are utilized for grouping the nodes into clusters. Optimized Convolutional Neural Network (OCNN) is the key authentication method that is used for the verification during message transmission.

3 CLUSTERING BASED WSN MODEL

In this work, two types of clustering methodologies are used namely Adaptive Possibilistic C-Means Clustering (APCMC) and Kernel Based Fuzzy C-Means Clustering (KFCMC).

3.1 APCMC Clustering

Adaptive Possibilistic C-Means Clustering (APCMC) is obtained using Eq. (1)

$$\gamma_j = \frac{\hat{\eta}}{\alpha}\eta_j \tag{1}$$

where $\hat{\eta}$ means a user-distinct between every η_j's to manage nearly positioned clusters, $\hat{\eta} = \min_j \eta_j$. α is a parameter indicating the closer located nodes and approximate to value 1. η_j indicates mean absolute divergence of cluster Cl_j given by Eq. (2)

$$\eta_j = \frac{\sum_{i=1}^{n} u_{ij}^{\text{FCM}} \left\| n_i - \theta_j \right\|}{\sum_{i=1}^{n} u_{ij}^{\text{FCM}}} \tag{2}$$

where n_i represents the i-th node in the network, assigning value to θ_j's is done by using final cluster values captured from FCMC and u_{ij} must meet the condition given in Eq. (3)

$$0 < \sum_{i=1}^{N} u_{ij} \le N, j = 1, \ldots m \tag{3}$$

3.2 KFCMC Clustering

In cluster formation, the total number of sensor nodes is separated into small groups. From the cluster members, one of the suitable members is selected to be clusterhead using random selection method. Clusterhead is initialized by sending a cluster member request message enclosing message type, sender ID, biometric attribute vector validated with sender's private key to overcome spoofing attack. The response will have message type, cluster member node ID, and private key from cluster member nodule. The request and response message will finalize the key of a cluster. KFCMC steps are given below.

1) Select cluster number *Cl* and termination parameter $\varepsilon_1 > 0$.

2) Select Polynomial kernel function *K*, $K\left(x_i, x_j\right) = \left(1 + x_i x_j\right)^p$, degree of polynomial $p = 2$.

3) Choose cluster centroids v_j, for $j = 1, 2, ..., Cl$.

4) Calculate membership degrees u_{ij} in Eq. (4) for nodules x_i in j-th cluster for $i = 1, 2, ..., l$

$$u_{ij} = \frac{\left(\dfrac{1}{d^2\left(x_i, v_j\right)}\right)^{\frac{1}{m-1}}}{\sum_{p=1}^{Cl} \left(\dfrac{1}{d^2\left(x_i, v_p\right)}\right)^{\frac{1}{m-1}}} \tag{4}$$

where $d^2\left(x_i, v_j\right) = K\left(x_i, x_i\right) - 2K\left(x_i, v_p\right) + K\left(v_p, v_p\right)$

5) Compute the new kernel matrices $K\left(x_i, v_p^{\text{New}}\right)$ and $K\left(v_p^{\text{New}}, v_p^{\text{New}}\right)$ as in Eq. (5) and Eq. (6)

$$K\left(x_i, v_p^{\text{New}}\right) = \frac{\sum_{k=1}^{l} \left(\mu_{kp}\right)^m K\left(x_k, x_i\right)}{\sum_{k=1}^{l} \left(\mu_{kp}\right)^m} \tag{5}$$

$$K\left(v_p^{\text{New}}, v_p^{\text{New}}\right) = \frac{\sum_{k=1}^{l} \left(\mu_{kp}\right)^m \left(\mu_{np}\right)^m K\left(x_k, x_n\right)}{\left(\sum_{k=1}^{l} \left(\mu_{kp}\right)^m\right)^2} \tag{6}$$

6) Revise membership degrees μ_{ij} to μ_{ij}^{new}, as in Eq. (4).

7) When $\max\limits_{i,j} \left| u_{ij} - u_{ij}^{\text{new}} \right| < \varepsilon_1$ stop, else go to step 5.

4 KEY GENERATION

If a new user enters into the system, then an encryption key is created randomly for every user and it is stored in the gateway node. Multibiometric key is generated using the fused features of fingerprint, retina and facial expression. The various steps involved in this process are filtering, texture extraction and fusion.

4.1 Filtering

In-order to remove the noises present in the images and to increase the quality of the image filters like bilateral and fuzzy are used in this work. Adaptive Median Filtering (AMF) uses two filters, AMF for calculation of local noise density along with switching median filter to protect local details in image. The two stages involved in noise removal are noise detection and noise reduction as given in Eq. (7). η means impulse noise level ranges from 0 to 1, *K* indicates noise pixels and $M \times N$ refers to total amount of pixels in image.

$$\eta = K / \left(MN\right) \tag{7}$$

Bilateral filter is a non-linear filter used for smoothing the images by protecting the edges. In this method, strength of every pixel is replaced by the weight average of nearby pixels based on Gaussian distribution. The weight is based on Euclidean distance among pixels and colour intensity.

$$I^{\text{filtered}}\left(y\right) = \frac{1}{W_p} \sum_{y_i \in \Omega} I\left(y_i\right) k_r \left(\left\| I\left(y_i\right) - I\left(y\right) \right\|\right) g_s \left(y_i - y\right) \tag{8}$$

In Eq. (8), $I^{\text{filtered}}\left(y\right)$ represents noise removed image, *I* denotes the given image, *y* indicates order of actual pixel for filtering, Ω symbolizes window centre in *y*, $y_i \in \Omega$ means other pixel. By Gaussian function, k_r denotes kernel for removing deviation in intensities and g_s indicates spatial (or domain) kernel for removing deviation in coordinates. Weight W_p is obtained by spatial closeness between g_s and k_r. Assume pixel is situated at (i, j) which has to be treated for noise removal using the nearby pixel at (k, l) which is given by Eq. (9).

$$w\left(i, j, k, l\right) = \exp\left(-\frac{\left(i-k\right)^2 + \left(j-l\right)^2}{2\sigma_d^2} - \frac{\left\| I\left(i, j\right) - I\left(k, l\right) \right\|^2}{2\sigma_r^2} \right) \tag{9}$$

where σ_d and σ_r indicate the smoothing variables, $I(i, j)$ and $I(k, l)$ denote the strength of pixel (i, j) and (k, l) respectively. Compute the weights and normalize them as in Eq. (10) and I_D represents noise removal strength of pixel (I, j)

$$I_\mathrm{D}\left(i,j\right)=\frac{\sum_{k,l}I\left(k,l\right)w\left(i,j,k,l\right)}{\sum_{k,l}w\left(i,j,k,l\right)} \tag{10}$$

Fuzzy filter is used for removing impulse and additive noise. Calculate the α-trimmed mean for group of elements in $A = \{a_1, a_2 ,..., a_n\}$ using Eq. (11)

$$\mu_\alpha=\frac{1}{n-\alpha}\sum_{i=\left(\frac{\alpha}{2}\right)+1}^{n-\left(\frac{\alpha}{2}\right)-1}a_i \tag{11}$$

where α is obtained from group of elements after trimming $\alpha/2$ at top and bottom. Mean of k-middle is obtained from the fuzzy membership Eq. (12)

$$M_k\left(A\right)=\begin{cases}\dfrac{1}{2k-1}\displaystyle\sum_{i=h-k+1}^{h+k-1}a_i,\text{if } n=\left(2h-1\right)\\ \dfrac{1}{2k}\displaystyle\sum_{i=h-k+1}^{h+k}a_i,\text{if } n=2h\end{cases} \tag{12}$$

where a_i indicates i-th order in set of A. When $k = 1$, measure is equal to median and for $k = h$, measure is equal to mean. For each pixel p_{ij} in location (i, j) from the image, consider $(2M + 1) \times (2M + 1)$ nearby area with p_{ij} as centre. Group of pixel strength in region R_{ij}^M is obtained from Eq. (13).

$$R_{ij}^M=\left\{p_{i+k,j+l}\mid -M\le k,l\le M\right\} \tag{13}$$

Fuzzy set $\mathcal{U}_{ij}^M$ is defined in Eq. (14) for each element p_k in the group R_{ij}^M, which is related to the Gaussian membership function. μ_{ij}^M, σ_{ij}^M and M_k is the mean for k-middle measure and group Λ_{ij}^M is obtained by Eq. (15), Eq. (16), and Eq. (17).

$$m_{\mathcal{U}_{ij}^M}\left(p_k\right)=\mathrm{e}^{-\frac{\left(p_k-\mu_{ij}^M\right)}{2\left(\sigma_{ij}^M\right)^2}} \tag{14}$$

$$\mu_{ij}^M=M_{K_1}\left(R_{ij}^M\right) \tag{15}$$

$$\sigma_{ij}^M=M_{K_2}\left(\Lambda_{ij}^M\right) \tag{16}$$

$$\Lambda_{ij}^M=\left\{\left(p_k-\mu_{ij}^M\right)^2,\forall p_k\in R_{ij}^M\right\} \tag{17}$$

By using the bilateral and Fuzzy filter the noises are removed from the biometric images and feature extraction is carried out.

4.2 Feature Extraction

Local Binary Pattern (LBP) technique discovers the texture features of biometrics by averaging the nearby pixels and obtains result in binary number. The standard deviation data related to the nearby pixels is utilized to get rotation in-variance in Adaptive LBP (ALBP) method. The variation in mean and standard deviation is reduced using the directional difference equation $\left|g_c-w_p\cdot g_p\right|$. The weight element w_p which is used to reduce directional difference is given by Eq. (18).

$$w_p=\arg\min_{w}\left\{\sum_{i=1}^{N}\sum_{j=1}^{M}\left|g_c\left(i,j\right)-w_p\cdot g_p\left(i,j\right)\right|^2\right\} \tag{18}$$

where N and M indicates total amount of rows and columns within the image. ALBP is specified in Eq. (19) and Eq. (20). By applying ALBP, texture of the biometrics images is extracted and fused to get user key.

$$\mathrm{ALBP}_{P,R}=\sum_{p=0}^{P-1}s\left(g_c-w_p\cdot g_p\right)2^p, \tag{19}$$

$$s\left(x\right)=\begin{cases}1 \text{ if } x\ge 0\\ 0 \text{ if } x<0\end{cases} \tag{20}$$

4.3 Feature Fusion

Feature level fusion is obtained by concatenating the three features vectors $U'=\left\{u_1',\ldots,u_m'\right\}$, $V'=\left\{v_1',\ldots,v_n'\right\}$ and $X'=\left\{x_1',\ldots,x_o'\right\}$. The novel biometric feature vector is found by $U'V'X'=\left\{u_1',..,u_m',v_1',..,v_n',x_1',..,x_o'\right\}$, $UVX\in R^{m+n+o}$.

4.4 Multibiometric Key Security System

In MOSS-GROWN framework, pre-configuration is the first phase where volatile master key $\mathrm{Ke_v}$ is inserted into few nodes for sharing of information secretly. Next in deployment and keying phase, the neighbouring nodes are identified with a biometric request and response. During MKG step, confidential key between sensor nodes is formed with pseudo random number and conveyed to all sensor nodes. Group key is obtained by using fuzzy membership on prime numbers, which is utilized for security during cluster to cluster transmission. Biometric based key authentication is done with Optimized Convolutional Neural Network (OCNN). At last, packets are transmitted between two nodes successfully.

5 OPTIMIZED CONVOLUTIONAL NEURAL NETWORK (OCNN)

In this work, authentication is achieved by training the OCNN with fingerprint, retina and facial expression images.

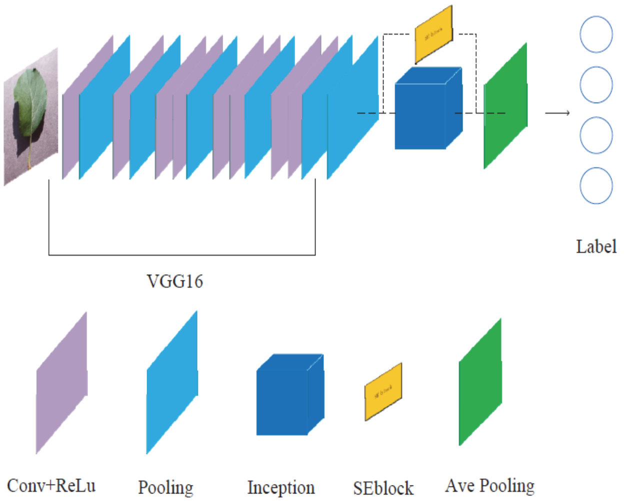

Figure 2 OCNN structure

OCNN used in this work includes five types of convolutional layers as in VGG16 model, collection of squeeze and excitation section and then Inception structure for good self-learning rate of low-to-high biometric features. Deep convolutional levels decrease the pixel of feature sets along with extraction of higher intensity features. Noise is removed from the extracted features using max pooling layer. In Inception structure, features are fused and embedded SE module helps to re-calibrate exact features in required dimension. Fig. 2 represents the OCNN structure used for key authentication.

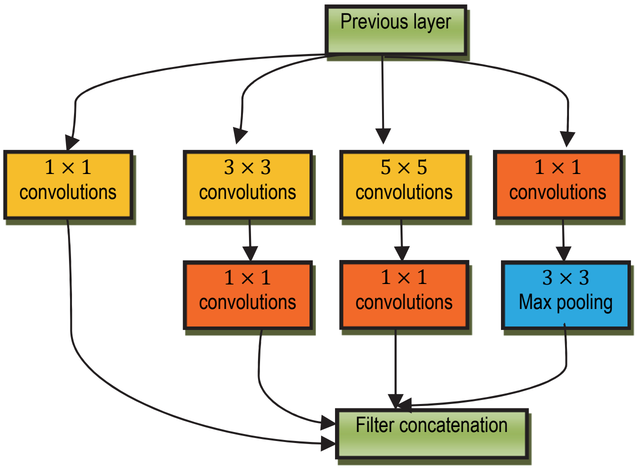

Figure 3 Inception structure model

In this work, stochastic gradient descent optimization method is employed for training the model with biometric features. The initial learning rate is kept as 0.001, momentum as 0.0005 and weight attenuation to be 0.9. Dropout layer is used to avoid over-fitting of images during training phase and to elevate their efficiency. Inception structure as shown in Fig. 3 is implemented with enlarged depth and width of network. This model uses three various Convolutional kernels 1 × 1, 3 × 3, and 5 × 5 convolutions along with 3 × 3 max pooling level. This method chooses the three unique scale characteristics and creates a multi-scale feature map to increase the authentication level.

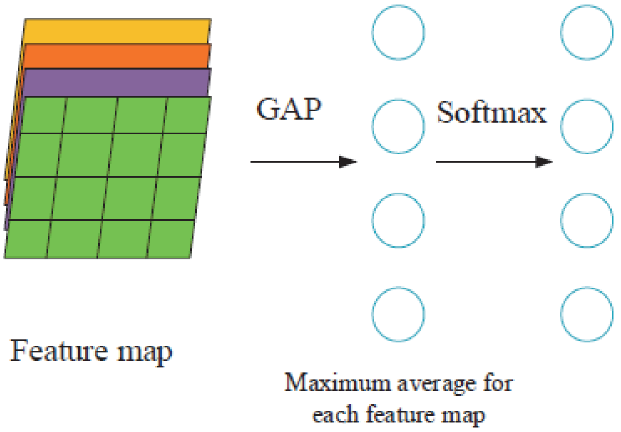

Figure 4 GAP layer

Fully connected level is altered with Global Average Pooling (GAP), which averages every pixel of feature map and sends to softmax for verification. Fig. 4 depicts the difference between fully connected and GAP model. Squeeze and Excitation (SE) module takes the input X from biometric images and N_{FC} indicates the Number of Feature Channels. In this method, selection, crossover and mutation operation are considered to re-calibrate weight value. Genetic algorithm chooses the weight to be $WE = \left(we_1, \dots we_n\right)$. At the beginning, a random weight is taken and later using selection process like Roulette Wheel Selection the parents are selected based on fitness and chromosomes. In crossover operation, two new off-springs are produced from two parents utilizing the weight values of classifier. Similarly in mutation operation, off-springs are produced by either combining the equal proposition of two parents or from single parent using random selection operator.

6 EXPERIMENTAL SETUP

The proposed methods are experimented in MATLAB 2017 simulator tool with Intel(R) Core(TM) i5-2450M CPU @ 2.50 GHz processor, 4 GB RAM, 64 bit OS, Windows 10. The biometric verification is carried out using three datasets namely Fingerprint Verification Competition 2004 (FVC2004), Digital Retinal Images for Vessel Extraction (DRIVE) and Extended Cohn-Kanade (CK+) are employed for simulation. The network used is homogeneous WSN with Static sensor nodes that are evenly disseminated in a 2D fashion.

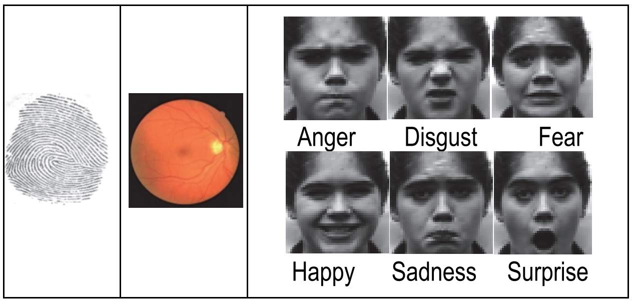

Figure 5 Sample fingerprint, retina and facial expressions

Fig. 5 represents the sample input image of fingerprint, retina, facial expression. The experimental properties are in Tab. 1.

Table 1 Experimental set-up

Parameter	Value
Amount of Sensor nodes	$n = 500$
Message size	$k = 4000$ bits
Area	150 × 150 m
Node location	(50, 50)
Amount of trials	10
MAC protocol	TDMA
Connection model	Bidirectional
Initial energy of normal node	0.5 J
Data sharing strength	5 nJ/bit/message

7 RESULTS AND DISCUSSION

The performance of the three security methods FKSS, RKSS and MKSS is compared in terms of six metrics namely Simulation time, Energy consumption, Delay, Attack Detection Rate (ADR), Packet Delivery Ratio (PDR), and Packet Loss Ratio (PLR).

7.1 Simulation Time and Energy Consumption

Simulation time indicates the total time for executing the entire operation. Energy Consumption is the total quantity of energy consumed for entire transmission and reception of all packets.

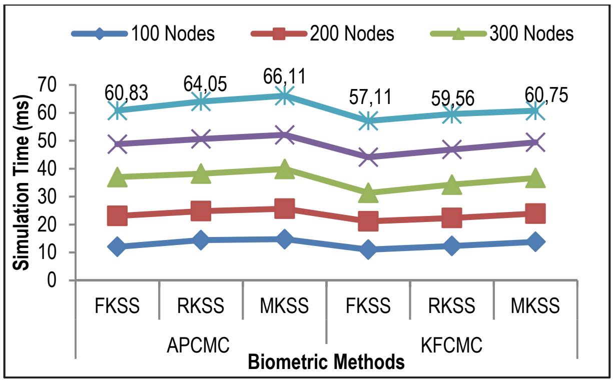

Figure 6 Simulation time of biometric methods

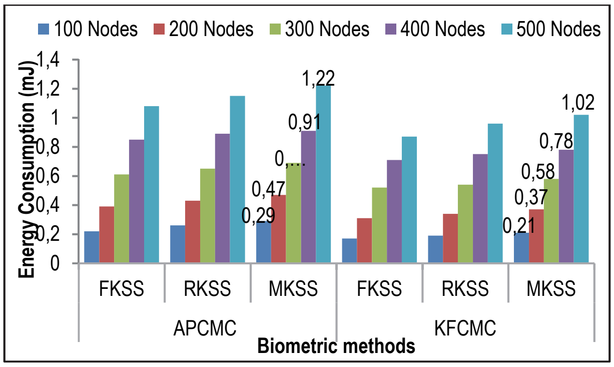

Figure 7 Energy consumption of biometric methods

Fig. 6 and Fig. 7 show the simulation time and energy consumed of three proposed methods in two different clustering approaches for 500 quantity of nodes. The result shows that MKSS using KFCMC clustering needs 60.75 ms for execution which is 9% less simulation time and low energy consumption of 1.02 mJ which is 20% less when compared to APCMC clustering MKSS method.

7.2 Delay and Attack Detection Rate (ADR)

Delay indicates the time taken for successful packet transmission from source to destination node. ADR indicates the quantity of attacks like physical, replay, selective forwarding and Hello flood attack in the transmission of packets. Delay is (87.19 ms) 2% more in APCMC clustering approaches compared to KFCMC and highest ADR of around (97.28 %) which is 5% more in MKSS method using KFCMC clustering for 500 amount of nodes as shown in Fig. 8 and Fig. 9.

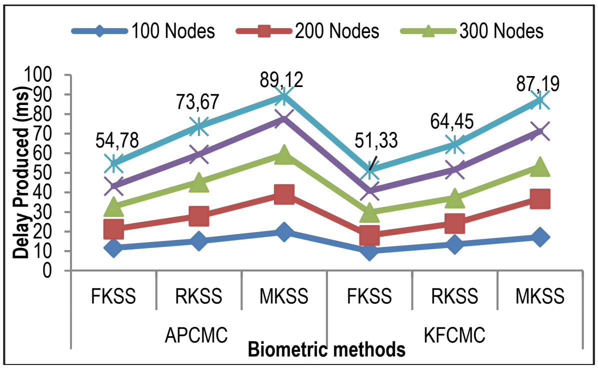

Figure 8 Delay Produced by biometric methods

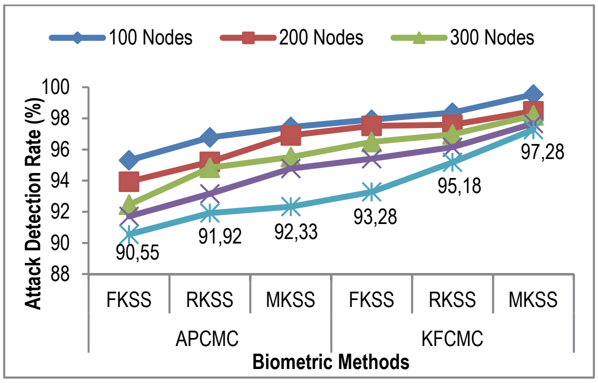

Figure 9 ADR of proposed methods

7.3 Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR)

PDR means total packets received by receiver to total packets transmitted by sender. PLR is the ratio of total messages not delivered at receiver to total messages transmitted by sender.

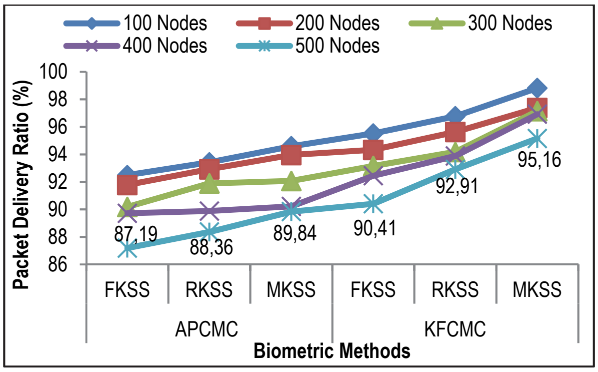

Figure 10 Packet Delivery Ratio

As shown in Fig. 10 and Fig. 11, PDR of KFCMC based MKSS is high compared to other methods and low PLR for MKSS in KFCMC clustering for 500 amount of nodes.

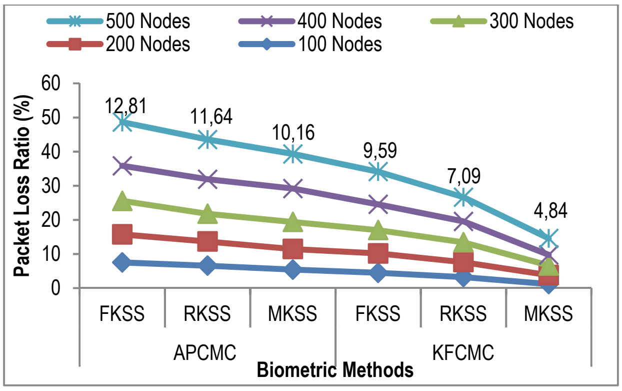

Figure 11 Packet Loss Ratio

7.4 Biometric Authentication Metrics

The performance of the proposed methods FKSS, RKSS, and MKSS is compared based on metrics like precision, recall, F-measure and accuracy. Precision is the identification of exactly real positive in total amount of positive class. Recall is the amount of real positive to collection of real positive and incorrect negative. F-measure indicates the weighted harmonic mean of the precision and recall. Accuracy defines the total of real positive and negative to all positive and negative variables.

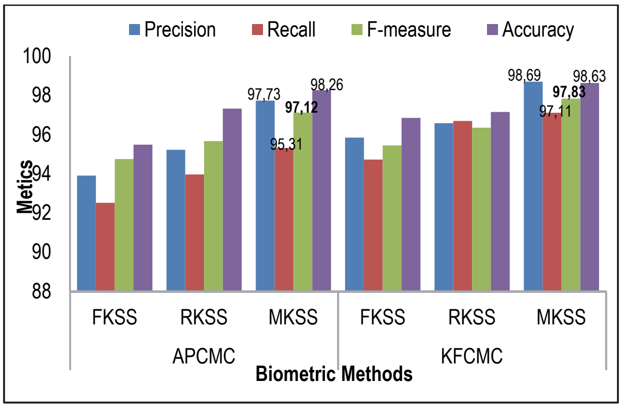

Figure 12 Biometric authentication metrics

Fig. 12 indicates the performance relation between the three biometric authentication methods in APCMC and KFCMC Clustering. Precision, Recall, F-measure and Accuracy are better in KFCMC clustering based MKSS method compared to other FKSS and RKSS methods.

8 CONCLUSION

In this work, Multibiometric Key based Security Scheme with OCNN Recognition for Wireless Sensor Network is proposed using fingerprint, retina and facial expression images. The three methodologies projected are Fingerprint Key based Security System (FKSS), Retina Key based Security System (RKSS) and Multibiometric Key based Security System (MKSS) with Adaptive Possibilistic C-Means Clustering (APCMC) and Kernel based Fuzzy C means Clustering (KFCMC). This scheme has three steps namely clustering based WSN model, Multibiometric based Key Generation using biometrics, and key verification using Optimized Convolutional Neural Network (OCNN) for packet transmission. The results obtained from MATLAB Simulator indicate that the new MKSS system with KFCMC clustering is highly secured and achieves 9% less simulation time, 20% of low energy consumption, delay is reduced by 2%, Attack Detection Rate is improved by 5%, Packet Delivery Ratio reaches 6% more compared to other methods, Packet Loss Ratio is decreased by 27%, Accuracy enhanced by 2%, and achieves 1% better precision.

9 REFERENCES

[1] Lim, S.-L. (2021). A Chain-Based Wireless Sensor Network Model Using the Douglas-Peucker Algorithm in the IoT Environment. *Tehnički vjesnik*, *28*(6), 1825-1832. https://doi.org/10.17559/TV-20200916075229

[2] Azad, P. & Sharma, V. (2015). Pareto-optimal clustering scheme using data aggregation for wireless sensor networks. *International Journal of Electronics*, *102*(7), 1165-1176. https://doi.org/10.1080/00207217.2014.966775

[3] Salar, A. (2021). Fuzzy C-Means clustering algorithm for data with unequal cluster sizes and contaminated with noise and outliers: Review and development. *Expert Systems with Applications*, 165. https://doi.org/10.1016/j.eswa.2020.113856

[4] Srijayanthi, S. & Sethukarasi, T. (2021). A Real-Time Data Clustering Scheme Using K-Medoids Based Optimal Neural Network Approach for Integrating Demographics and Diagnosis Codes. *IETE Journal of Research*, *1*(12). https://doi.org/10.1080/03772063.2021.1977192

[5] Sumathi, R. & Mandadi, V. (2021). Towards Better Segmentation of Abnormal Part in Multimodal Images Using Kernel Possibilistic C Means Particle Swarm Optimization With Morphological Reconstruction Filters: Combination of KFCM and PSO With Morphological Filters. *International Journal of E-Health and Medical Communications (IJEHMC)*, *12*(3), 55-73. https://doi.org/10.4018/IJEHMC.20210501.oa4

[6] Xenaki, S. D., Koutroumbas, K. D., & Rontogiannis, A. A. (2016). A Novel Adaptive Possibilistic Clustering Algorithm. *IEEE Transactions on Fuzzy Systems*, *24*(4), 791-810. https://doi.org/10.1109/TFUZZ.2015.2486806

[7] Nivedetha, B. & Vennila, I. (2020). FFBKS: Fuzzy Fingerprint Biometric Key Based security schema for Wireless Sensor Networks. *Computer Communications*, *150*, 94-102. https://doi.org/10.1016/j.comcom.2019.11.007

[8] Chang, T. Y. & Yuan Ku, C. C. (2021). Fuzzy filtering ranking method for multi-criteria decision making. *Computers and Industrial Engineering*, *156*, 1-9. https://doi.org/10.1016/j.cie.2021.107217

[9] Deng, J. X. & Deng, Y. (2021). Information Volume of Fuzzy Membership Function. *International Journal of Computers, Communications and Control*, *16*(1), 1-14. https://doi.org/10.15837/ijccc.2021.1.4106

[10] Fu, B., Zhao, X., Li, Y., Wang, X., & Ren, Y. (2019). A convolutional neural networks denoising approach for salt and pepper noise. *Multimedia Tools and Applications*, *78*(21), 30707-30721. https://doi.org/10.1007/s11042-018-6521-4

[11] Luo, P., Zhang, X., Chang, Z., & Liu, W. (2021). Research on Salt and Pepper Noise Removal Method Based on Adaptive Fuzzy Median Filter. *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 387-392. https://doi.org/10.1109/IAEAC50856.2021.9390923

[12] Sotoodeh, M., Moosavi, M. R., & Boostani, R. (2019). A novel adaptive LBP-based descriptor for colour image retrieval. *Expert Systems with Applications*, *127*, 342-352. https://doi.org/10.1016/j.eswa.2019.03.020

[13] Thanh, D. N. H. & Engínoğlu, S. (2019). An iterative mean filter for image denoising. *IEEE Access*, *7*, 167847-167859. https://doi.org/10.1109/ACCESS.2019.2953924

[14] Li, X., Zhou, F., Tan, H., Zhang, W., & Zhao, C. (2021). Multimodal medical image fusion based on joint bilateral filter and local gradient energy. *Information Sciences*, *569*, 302-325. https://doi.org/10.1016/j.ins.2021.04.052

[15] Rojas, A. & Dolecek, G. J. (2021). Fingerprint Recognition Based on Wavelet Transform and Ensemble Subspace Classifier. *2021 IEEE URUCON*, 508-511. https://doi.org/10.1109/URUCON53396.2021.9647176

[16] Rangayya, R., Virupakshappa, V., & Patil, N. (2021). An enhanced segmentation technique and improved support vector machine classifier for facial image recognition. *International Journal of Intelligent Computing and Cybernetics*. https://doi.org/10.1108/IJICC-08-2021-0172.

[17] Connie, T., Al-Shabi, M., Cheah, W. P., & Goh, M. (2017). Facial Expression Recognition Using a Hybrid CNN-SIFT Aggregator. *International Workshop on Multi-disciplinary Trends in Artificial Intelligence, MIWAI 2017*, *10607*, 1-11. https://doi.org/10.1007/978-3-319-69456-6_12

[18] Lin, M., Chen, Q., & Yan, S. (2013). Network in network. *Neural and Evolutionary Computing*, 1-10.

Contact information:

Nivedetha BALAN, Assistant Professor
(Corresponding author)
Department of Electrical and Electronics Engineering,
PSG College of Technology, Peelamedu,
Coimbatore-641 004, Tamilnadu, India
E-mail: bna.eee@psgtech.ac.in

Vennila ILA, Professor
Department of Electrical and Electronics Engineering,
PSG College of Technology, Peelamedu,
Coimbatore-641 004, Tamilnadu, India
E-mail: iven.eee@psgtech.ac.in