Resbee Publishers

Multimedia Research (MR)

Received 9 June, Revised 25 August, Accepted 22 September

Intrusion Detection Based on Piecewise Fuzzy C-Means Clustering and Fuzzy Naïve Bayes Rule

Neenavath Veeraiah
Department of ECE
DVR & DHS MIC College of Technology
Kanchikacherla, Andhra Pradesh, India
neenavathveeraiah@gmail.com

Dr.B.T.Krishna
Department of ECE
JNTUK University
Kakinada, Andhra Pradesh, India

Abstract: Intrusion detection has paramount importance in network security. Intrusion detection depends on energy dissipation, whereas trust remains a hectic factor. In this paper, a trust-aware scheme is proposed to detect intrusion in Mobile Ad Hoc Networking (MANET). The proposed method uses Piecewise Fuzzy C-Means Clustering (pifCM) and fuzzy Naive Bayes (fuzzy NB) for the intrusion detection in the network. The pifCM helps to determine the cluster heads from the clusters. After the selection of cluster heads, the intrusion in the network is determined using fuzzy Naive Bayes with the help of node trust table. The node trust table contains the updated trust factors of all the nodes and the presence of intruded nodes are found with the help of the trust table. After the intrusion is detected, they are eliminated and this reduces the delay in transmission. The effectiveness of the proposed method is analyzed based on the metrics, such as throughput, detection rate, delay, and energy. The proposed method has the delay at the rate of 0.003, energy dissipation of 0.657, the detection rate of 9.85, and throughput of 0.659.

Keywords: trust factors, MANET, pifCM, intrusion detection, fuzzy Naïve Bayes.

1 Introduction

MANETs are a group of mobile wireless nodes without a fixed network infrastructure. The nodes communicate beyond the radio ranges by forwarding packets. The characteristics of the MANET are dynamic topology, multi-hop routing, and high user density. The MANET also has the ability to communicate and to operate independently with a fixed network using an interface or gateway. A node contains the operating modes, such as sensing, computing, and communicating nodes. The sensing node uses battery energy and the amount consumed depends on the transmission range, which varies exponentially with the energy and the signal propagation is consumed for the transmission between the nodes. MANET is also vulnerable to attacks as they have cooperative algorithms, requires a clear line of defense, lack of centralized monitoring and open medium [7]. The attacks in MANET are detected using Intrusion Detection (ID) techniques [12] [13] [14]. The intrusion detection system is motivated by factors, such as the security flaws in the existing systems that lead to intrusion, penetrations and other form of abuse; developing secure systems; replacing the existing systems with more attractive features; misusing the privileges of the system by insiders [8].

The goal of ID is to identify the attacks and secure the network. Network-based IDS are used in preventing the attacks in computer networks. The Network-based ID alarms during a possible potential malicious activity. Generally, the IDS are categorized into two methods: anomaly detection [10] and misuse detection [11]. The misuse detection uses the malicious activity that has well-defined patterns to detect the intrusion and they doesn't alert during new attacks. Anomaly detection recognizes the malicious traffic when there are deviations in the normal pattern and the system features, such as statistical measures helps in detecting malicious traffic. The anomaly detection techniques detect unknown attacks more than the misuse detection technique [9]. The proposed method uses intrusion detection based on pifCM and Fuzzy NB method. Initially, the optimal cluster heads are selected using pifCM based clustering. The cluster head is the node with maximum trust value. The routing occurs after the selection of cluster heads. The trust factors are determined for all the nodes as the intrusion

detection depends on the trust factor. The nodes that are intruded are detected and eliminated using Fuzzy Naive Bayes. The intruded nodes are removed to reduce the delay in the transmission.

The organization of the paper is: Section 1 introduces the paper, section 2 elaborates the literature review of the intrusion detection methods. The proposed method of intrusion detection is discussed in section 3, section 4 details the results and discussion of the proposed method. Finally, section 5 concludes the paper.

2 Literature Survey

Singh et al.[1] developed an Elliptic Curve Cryptography (ECC) algorithm with trust management for the identification of intruders. ECC was the solution for public key cryptography. To maintain high security in MANET, the malicious node was eliminated from the network. This method provided high throughput, minimized the packet loss, provided efficient end to end delivery and minimized the delay. However, this method detected some selective attack only. Subba et al.[2] developed a MANET IDS with Bayesian game theory. This method provided a high detection rate and a high false alarm rate. However, the MANET IDS did not consider the false positive rate and the detection rate in their modules. Neenavath Veeraiah et al.[3] designed a trust-aware system to detect the intrusion in the MANET. This method uses fuzzy Naive Bayes and Trust-aware fuzzy clustering method. Based on optimal centroid, the nodes were clustered and it evaluated the trustworthiness of the nodes effectively. Sumaiya Thaseen Ikram et al.[4] developed an intrusion detection model with a multi-class Support Vector Machine (SVM) and chi-square feature selection method. In this method, a multi-class SVM model is constructed, which increases the accuracy of individual classification of network attacks. In this method, the patterns are not analyzed and better optimization techniques should be used for optimization.

2.1 Challenges

The challenges for intrusion detection systems are as follows,

- To prevent attacks in the intrusion detection system, advanced architecture should be used.
- Intrusion detection systems suffer from false alarm issue. During the intrusion, the wireless IDS denies the service as the data packets are abandoned, which in turn leads to improper reaction while facing attack.
- The intrusion detection system requires adequate intelligence to identify database application attacks [3].
- The prevention of passive sniffing is an important challenge. The passive sniffing is prevented using proper protection through encryption [2].

3 PifCM- Fuzzy NB Method for Intrusion Detection in Nodes

In MANET environment, each cluster head is assigned with mobile nodes and they act as a controller. The MANET nodes are given as,

$$m = \{m_1, m_2, ..., m_r, ..., m_p\} \quad (1)$$

where, p is the number of nodes in MANET and m_r is the r^{th} node in MANET. The cluster heads are denoted as,

$$L = \{L_1, L_2, ..., L_k, ...L_n\} \quad (2)$$

where, L_k is the k^{th} cluster head in MANET and n denotes the cluster heads in MANET. Let F be the trust factor, which is denoted as,

$$F = \{F_1, F_2, ..., F_h, ..., F_x\} \quad (3)$$

where, x indicates the total trust factor which is equal to 6.

MANET contains six trust models, such as direct trust, recent trust, indirect trust, trust based on data bytes, trust depending on data delivery, and trust based on error. Initially, the total trust nodes are assumed as one and they are considered for transmitting the data. Additionally, the delay in the transmission and the trustworthiness of the nodes is improved by BDE-based factors, such as Trust based on Data Packet delivery, Trust based on error and Trust based on data bytes

3.1 Block Diagram of Proposed IDS Method Based on PifCM and Fuzzy NB Rule

Fig. 1 shows the block diagram of the proposed IDS method based on pifCM and Fuzzy NB rule. In the proposed method, the trustworthiness of the nodes is defined by the trust factor. Initially, the optimal cluster heads are selected using pifCM based clustering. The cluster head is the node with maximum trust and they have the complete information of the nodes. The routing occurs between the sink node and cluster heads subsequent to the selection of cluster heads. Intrusion detection is done by evaluating the trust factors in nodes. After the intrusion detection, the intruded nodes are eliminated to reduce the delay in transmission using Fuzzy NB rule. Once the intrusions are eliminated the trust of the nodes are updated.

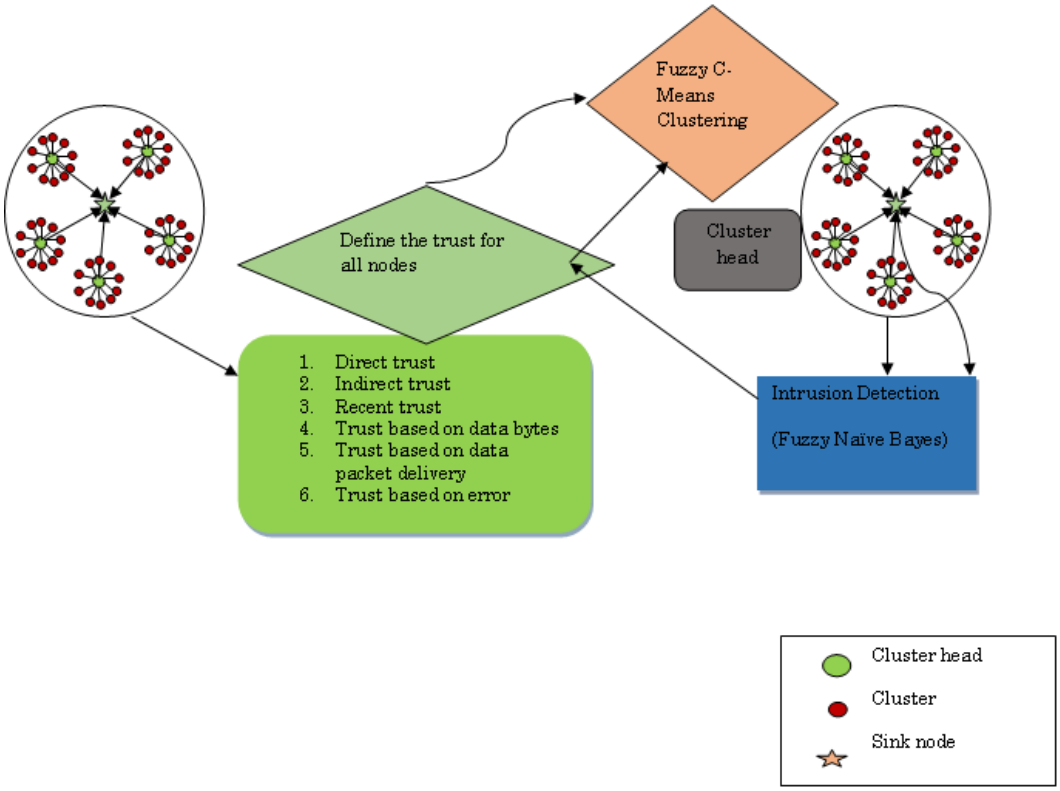

Fig. 1.*Block diagram of the proposed IDS method based on pifCM and Fuzzy NB rule.*

3.2 PifCM for Cluster Head Selection

To better understand the data objects and the centroids, multi-membership data is formulated in pifCM. Let $M=\{m_1,...,m_n\}$ be the membership dataset derived from the set of BPs with,

$$m_1=(\beta_o^{(1)},...,\beta_o^{(j)},...,\beta_o^{s}) \tag{4}$$

The piecewise clustering for the fuzzy clustering is given as,

$$u_b=\{u_b^{(1)},...,u_b^{j},...,u_b^{s}\} \tag{5}$$

Where, $u=\{u_1,...,u_b\}$, u_b is the dimensional vector with s pieces, u_b^{j} is the b^{th} centroid of M in the j^{th} piece, whereas u_b is the piecewise centroid for M. To minimize J_{mf}, we are taking the fuzzy c-means clustering on the multi membership data and the piecewise centroid and the distance from m_o to v_k is given as,

$$a(m_o,u_b)=\sum_{j=1}^{s} z_j(\beta_o^{(j)},u_b^{(j)})\ \forall o,b \tag{6}$$

From the above equation, an algorithm is formulated for minimizing J_{mf}. Thus the optimal cluster heads, which has maximum trust values are selected from the clusters.

3.3 Fuzzy NB for Intrusion Detection in MANET Nodes

After clustering, Fuzzy NB is used for detecting the intruded nodes [5]. The sink node helps in detecting the intrusion depending on the information sent by cluster heads. The information regarding the six

trust factors is obtained from the node trust table. The sink node with the help of Fuzzy NB method analyzes the trust table of the nodes and determines whether the node is intruded or normal. The probable class is obtained by classifying the nodes using Fuzzy NB. The membership values are the output from Fuzzy NB, which is based on class and trust factor. The output of the Fuzzy NB rule is given as,

$$V^{test} = \arg_{l=1,2,} \max \gamma(D_l / X) \tag{7}$$

where, X is the trust factor of the node to be tested.

$$X = \{X_1 . X_2, ..., X_h, ..., X_x\};\ X \in F_h \tag{8}$$

where, X_1, X_2 are the direct and indirect trust of the node. X_3, X_4, X_5, X_6 are the test data of the recent trust, objective trust, static trust, and dynamic trust respectively. The conditional probability of the class is considered as, $D_l \in dom(d)$, which is evaluated based on the trust factor. The maximum trust factor is determined by,

$$\gamma(D_l \mid X) = \gamma(D_l) \prod_{h=1}^{x} \frac{\gamma(X_h \mid D_l)}{\gamma(D_l)} \times w_h^x \tag{9}$$

where, $dom(d)$ is the total class $\gamma(D_l \mid X) = \gamma(D_l) \prod_{h=1}^{x} \frac{\gamma(X_h \mid D_l)}{\gamma(D_l)} \times w_h^x$ (9)

where, $dom(d)$ is the total class and the smoothening of measured probabilities are done using Laplacian-corrections and they don't deal with zero probabilities.

4 Results and Discussion

This section discussed the results of the proposed pifCM- Fuzzy NB method. The comparative analysis is done by comparing the proposed method with the existing methods like K-means NB, NBTrust, Fuzzy NB and Naive BAYES.

4.1 Experimental Setup

The proposed technique operates in windows 8 operating system, 4 GB RAM and Intel i4 is implemented in NS2 simulator.

4.2 Performance Metrics

The performance metrics such as throughput, energy, detection rate, and delay are the metrics employed for the analysis of the proposed method. For the effective method, throughput and detection rate should be maximum, whereas delay and energy dissipation should be minimum.

4.3 Comparative Methods

The proposed pifCM-Fuzzy NB method is compared with existing methods like K-means NB [6], NBTrust [2], Fuzzy NB[3] and Naive BAYES [2] for evaluating the performance of the proposed method.

4.4 Comparative Analysis

The comparative analysis is carried out without network node attacks and black hole attacks and the performance metrics are calculated for both attacks.

4.4.1 Black Hole attack

Fig. 2 shows the analysis of the network during the black hole attack. Fig. 2 a) shows the delay of the methods during the black hole attack. When the time is 30 s, the delay of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB is 0.00507, 0.00434, 0.00603, 0.00596 and 0.003 respectively. Fig. 2 b) depicts the detection rate of the methods during the black hole attack. The detection rate of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB at 30 s, is 0.584, 0.637, 0.566, 0.556 and 0.657 respectively. Fig. 2 c) shows the energy dissipation of the methods during the black hole attack. The energy dissipation of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB at 30 s, is 10.138, 9.98, 10.456, 10.487 and 9.85 respectively. Fig. 2 d) shows the throughput of the methods during the black hole attack. The throughput of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB at 30 s, is 0.607, 0.642, 0.546, 0.537 and 0.659 respectively.

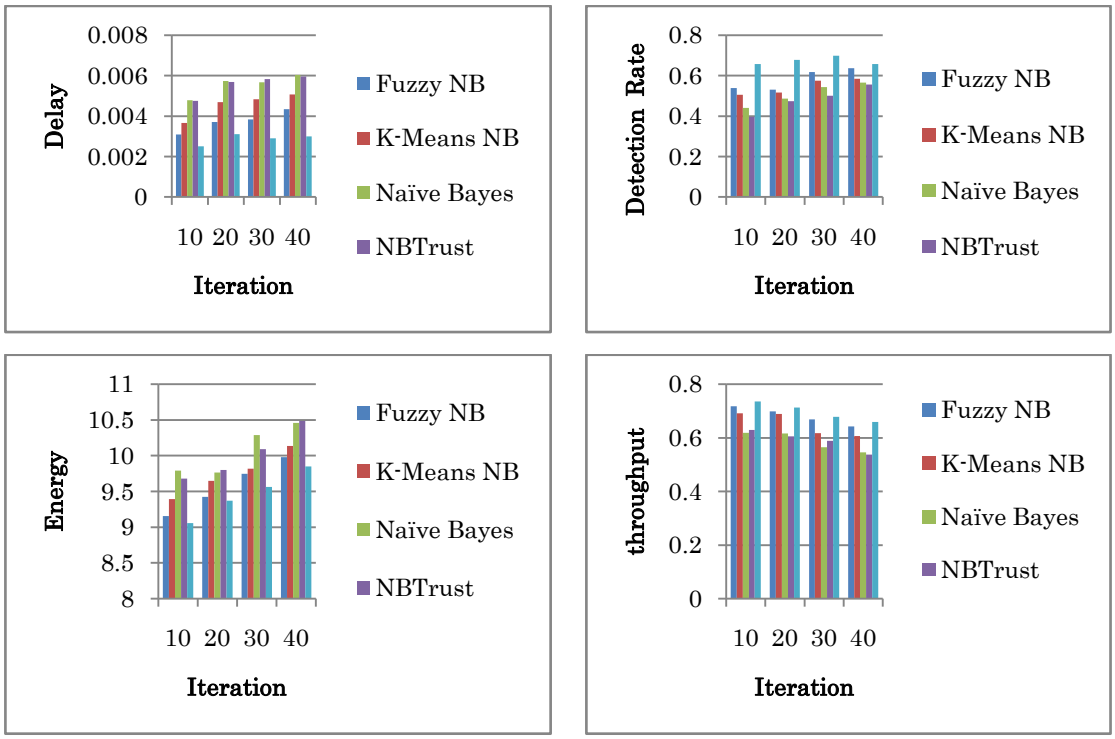

Fig. 2. *Analysis using black hole attack a) delay, b) detection rate, c) energy, d) throughput*

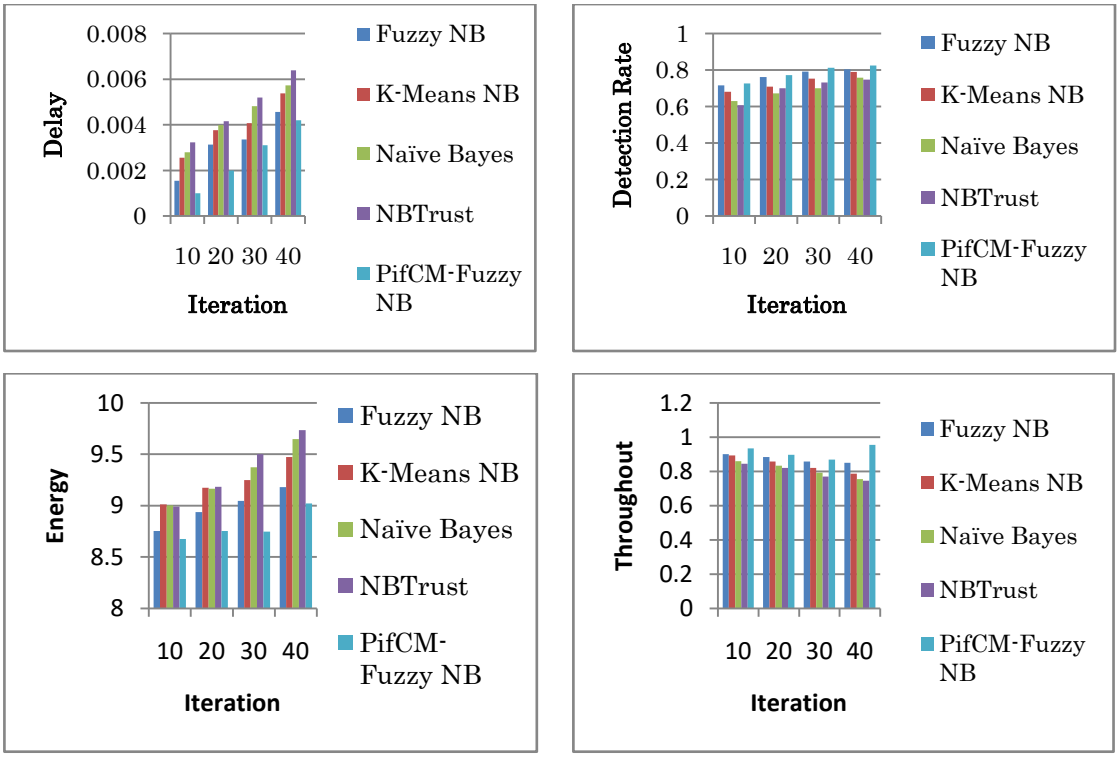

Fig. 3.*Analysis without attack a) delay, b) detection rate, c) energy, d) throughput*

4.4.2 Without attack

Fig. 3 shows the analysis of the network without node attack. Fig. 3 a) shows the delay of various methods without node attack. The delay of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB at 30 s is 0.00407, 0.00336, 0.00482, 0.0052 and 0.0031 respectively. Fig. 3 b) shows the detection rate without node attack. The detection rate of K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB at 30 s is 0.752, 0.791, 0.7, 0.732 and 0.812 respectively. Fig. 3 c) shows the energy dissipation of various methods without node attack. When the time is 30 s, the energy dissipation of the K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB is 9.248, 9.048, 9.375, 9.5 and 8.748 respectively. Fig. 3 d) shows the throughput of various methods

without node attack. At 30 s, the throughput of K-Means NB, Fuzzy NB, Naïve Bayes, NBTrust and proposed pifCM-Fuzzy NB method is 0.821, 0.858, 0.792, 0.77 and 0.869 respectively.

5 Conclusion

In this paper, we have proposed an intrusion detection method based on piecewise fuzzy c-means clustering and Fuzzy Naïve Bayes rule. The pifCM helps to determine the cluster heads from the clusters. The fuzzy NB uses Laplacian smoothening theory smoothens the probability values. The intrusion in the network is determined using fuzzy Naive Bayes with the help of node trust table. The node trust table is updated based on the trust factors of all the nodes, to find the intruded node. The simulation results ensured the efficiency of the proposed intrusion detection method and the network is analyzed for intrusion with black hole attacks and without attacks. The proposed method has the delay at the rate of 0.003, energy dissipation of 0.657, the detection rate of 9.85, and throughput of 0.659. The further extension of this research will be based on hybrid clustering and intrusion detection techniques.

References

[1] Singh O, Singh J, and Singh R, " Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET,"Cluster Computing, 21(1), 51–63, 2018.

[2] Subba B, Biswas S, and Karmakar S," Intrusion detection in Mobile Ad hoc Networks: Bayesian game formulation,"Engineering Science and Technology, an International Journal, 19(2), 782–799, 2016.

[3] Neenavath Veeraiah, B. Tirumala Krishna, "Trust-aware Fuzzy Clus-Fuzzy NB: intrusion detection scheme based on fuzzy clustering and Bayesian rule," Wireless Networks, pp 1–15, 2019.

[4] Sumaiya Thaseen Ikram, Aswani Kumar Cherukuri,"Intrusion detection model using fusion of chi-square feature selection and multi class SVM," Journal of King Saud University - Computer and Information Sciences, 29, 462–472, 2017.

[5] Storr H. H. P, Xu Y, and Choi J, " A compact fuzzy extension of the Naive Bayesian classification algorithm," In Proceedings of InTech/VJFuzzy, 2002.

[6] Marchang N, Datta R, and Das S. K," A novel approach for efficient usage of intrusion detection system in mobile ad hocnetworks,"IEEE Transactions on Vehicular Technology, 66(2), 1684–1695, 2017.

[7] Yian Huang and Wenke Lee ,"A Cooperative Intrusion Detection System for Ad Hoc Networks," Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Pages 135-147, 2003.

[8] Dorothy E. Denning ,"An Intrusion-Detection Model," IEEE transactions on software engineering, vol. se-13, no. 2, february 1987.

[9] Mostafa A. Salama, Heba F. Eid, Rabie A. Ramadan, Ashraf Darwish, and Aboul Ella Hassanien,"Hybrid Intelligent Intrusion Detection Scheme,"Soft Computing in Industrial Applications, pp 293-303, 2011.

[10] E. Biermann, E. Cloete and L.M. Venter, "A comparison of intrusion detection Systems", Computer and Security, vol. 20, pp. 676-683, 2001.

[11] T. Verwoerd and R. Hunt, "Intrusion detection techniques and approaches", Computer Communications, vol. 25, pp.1356-1365, 2002.

[12] S. D. Thepade and P. Bidwai, "Iris recognition using fractional coefficients of transforms, Wavelet Transforms and Hybrid Wavelet Transforms," 2013 International Conference on Control, Computing, Communication and Materials (ICCCCM), Allahabad, 2013, pp. 1-5.

[13] S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019.

[14] J. Zuniga-Mejia, R. Villalpando-Hernandez, C. Vargas-Rosales and A. Spanias, "A Linear Systems Perspective on Intrusion Detection for Routing in Reconfigurable Wireless Networks," in IEEE Access, vol. 7, pp. 60486-60500, 2019.