

Dingo algorithm-based forwarder selection and huffman coding to improve authentication

Nageswaran Usha Bhanu¹, Prathaban Banu Priya², Tiruveedhula Sajana³,
Shanmugasundaram Shanthi⁴, Murugan Mageshbabu⁵, Erram Swarnalatha⁶,
Kuntiyellannagari Bhagya Laxmi⁷, Kannabiran Saravanan⁸

¹Department of Electronics and Communication Engineering, SRM Valliammai Engineering College, Chennai, India

²Department of Networking and Communications, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Chennai, India

³Department of Artificial Intelligence and Data Science, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India

⁴Department of Electronics and Communication Engineering, CARE College of Engineering, Tiruchirapalli, India

⁵Department of Electronics and Communication Engineering, Saveetha School of Engineering

Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, India

⁶Department of Electronics and Communication Engineering, Guru Nanak Institute of Technology, Hyderabad, India

⁷Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

⁸Department of Information Technology, R.M.D Engineering College, Chennai, India

Article Info

Article history:

Received Feb 23, 2023

Revised May 30, 2023

Accepted Jul 2, 2023

Keywords:

Anomalous node detection

Dingo algorithm

End to end authentication

Huffman coding

Support vector machine

Wireless sensor networks

ABSTRACT

In wireless sensor network (WSN), the high volume of observe and transmitted data among sensor nodes make it requires to maintain the security. Even though numerous secure data transmission approaches designed over a network, an inadequate resource and the complex environment cause not able to used in WSNs. Moreover, secure data communication is a big challenging problem in WSNs especially for the military application. This paper proposes a dingo algorithm-based forwarder selection and huffman coding (DAHC) to improve authentication in internet of things (IoT) WSN. Initially, it detects the anomalous nodes by applying support vector machine (SVM) algorithm based on sensor node energy, node selfishness, and signal to noise ratio (SNR). Next, we using the dingo algorithm to select the forwarder node. This dingo algorithm computes the fitness function based on node degree, node distance and node energy. Finally, the huffman coding to provide end to end authentication established on node energy from sender to receiver. During data transmission, the huffman coding to build the binary hop count value, it improves the authentication in the WSN. Performance results specify that this approach enhances the detection ratio and throughput.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Nageswaran Usha Bhanu

Department of Electronics and Communication Engineering, SRM Valliammai Engineering College

Chennai, Tamil Nadu, India

Email: ushabhanu123@gmail.com

1. INTRODUCTION

A wireless sensor network (WSN) is a multi-hop self-organizing network that contains several tiny sensor nodes distributed in the forest area [1]. Several security demands should be addressed in WSN to enable the broad agreement of the internet of things (IoT) [2]. Authentication is an important security provision that needs broad attention from IoT security [3]. The latest advancements in IoT, cloud computing, and artificial intelligence algorithm improve the network application [4]. Authentication and authorization are two key elements to defend network services [5]. Authentication is the sensor identification procedure that verifies the

validity of the sensor nodes [6]. Secure lightweight authentication approach is applying automatic security verification algorithm like ProVerif to confirm the security [7]. Machine learning (ML)-based algorithms introduced a light security authentication to satisfy high precision and low delay [8]. Among these methods, artificial intelligence leads to authentication improvement by adaptive retraining for the recognition model [9]. An optimization-based artificial bee colony algorithm (OABC) enhances the data collection, reduces total energy utilization, and increases reliability. However, this system can't provide network security. It increases the energy hole and the maintenance cost [10]. To solve these issues, dingo algorithm-based forwarder selection and Huffman coding (DAHC) mechanism is proposed. The contribution of this paper is; i) initially, it detects the anomalous nodes by applying support vector machine (SVM) algorithm based on sensor node energy, node selfishness, and signal to noise ratio (SNR); ii) next, we using the dingo algorithm to select the forwarder node. This dingo algorithm computes the fitness function based on node degree, node distance and node energy; and iii) lastly, the Huffman coding to provide end to end authentication established on node energy from sender to receiver. During data transmission, the Huffman coding to build the binary hop count value, it improves the authentication in the WSN.

SVM is the popular ML algorithm utilized for malicious detection because it can defeat the curse of dimensionality. This approach uses information gain ratio and K-mean algorithm to SVM for detecting malicious nodes [11]. The SVM is utilized to identify the nodes [12]. Multi SVM classifier with mutual information-based feature selection technique to detect attacks. The multiple SVM classifiers in which every classifier to identifies a specific attack [13]. Anomaly detection is a key dispute in assuring security and avoiding malicious attacks in WSNs [14]. Elliptic curve digital signature (ECDSA) algorithm to evaluate the HELLO message count, key generation time, and packet size [15]. Elliptical curve cryptography and ECDSA algorithm have computationally efficient and offer more security [16]. The elliptic curve diffie-hellman (ECDH) algorithm is an asymmetric key cryptosystem to improve authentication [17].

Trust aware SVM based intrusion detection system (IDS) approach purpose to discover and separate the abnormal nodes. The linear correlation coefficient based feature extraction (LCCBFE) algorithm is used to reduce the training time as well as improve the lifespan. The trust level node is measured by applying the behavior and remaining energy level. Behavior analysis based trust algorithm to calculate the trust level of nodes [18]. IDS is designed to identify malicious by applying cuckoo search (CS) with artificial intelligence. CS is utilized to feature optimization with the assist of the fitness function and is classified by normal and attackers. This approach is used to improve the QoS [19]. The IDS can notice the attacks with the minimum computing time. Furthermore, it enhanced the reliability and discarded the malicious nodes [20]. Deep learning (DL)-enabled security authentication approach using blind feature learning and neural networks introduced physical layer authentication to recognize malicious nodes [21]. An artificial neural network algorithm raises the network's lifetime [22]. Decryption and encryption methods to solve the security issues. Several encryption approaches to protect data protection, chaotic encryption systems widely applying a chaotic map for encrypting the data [23]. Fusion of CS and hill climbing techniques (CSHC) based select the best forwarder selection and notice the abnormal nodes. A Bayesian thresholding method is used to compute the received signal strength as well as the link reliability parameter for distinguishing abnormal nodes. However, it increases the routing overhead [24]. Secure and efficient signature approach that provide a security during data transmission [25].

2. PROPOSED METHOD

This approach is a lightweight intelligent authentication and meets great accuracy and lesser latency. Figure 1 demonstrates the architecture of the DAHC scheme. This approach objective is to detect the anomalous nodes by SVM algorithm. Then we use the dingo algorithm to choose the forwarder nodes. Finally, the Huffman coding technique to improve the authentication in the network.

2.1. SVM based anomalous node detection

During route finding, the sender initiates the route request (RREQ) request message to the receiver. This message comprises node ID, position, energy level, SNR, and selfishness degree. The receiver node receives the RREQ message then the SVM algorithm decides whether that node is a normal or anomalous node in the route. Figure 2 illustrates the SVM based anomalous nodes classification in the WSN.

Node energy: during route discovery, the sender node checks the routing nodes energy level based on the RREQ packet. The energy represents the amount of energy remaining. The node energy (E) calculation is specified in:

$$E = \exp\left(\frac{1}{1 + \frac{(IE - (RE - TE))}{IE}}\right) \quad (1)$$

here, IE indicates initial energy, RE represents the residual energy, and TE denotes the transmission energy. This computation makes sure that selecting the relay node has a lesser energy utilization rate. The node balance energy is greater than the average energy among neighbour nodes, that node encounters an anomalous node.

Node selfishness: the first category nodes represent the non-selfishness. These nodes hold by other nodes in the limits of their memory space. The second category nodes denote the fully selfish node. These nodes do not hold other nodes but distribute replicas to other nodes for their accessibility. The third category nodes indicate the partially selfish node. These nodes utilize their memory space partly for other nodes. But, we calculate the received packet value to detect the selfish nodes efficiently. Received packet (RP) indicates the ratio of packets received from the sender and the forward packet count. This received packet is lesser than an average value, that node encounters anomalous nodes. This received packet calculation is specified in (2).

$$RP = 1 - \left(\frac{\text{Count of Received Packet}}{\text{Count of Forward Packet}} \right) \tag{2}$$

Signal-to-noise ratio: The SNR value decides the link throughput to discover the most excellent route selection. This SNR parameter to measures the link quality node. The lowest SNR value decides that node chances the anomalous node in the WSN.

$$SNR = \gamma \times SNR + (1 - \gamma) \times SNR_{new} \tag{3}$$

Here, γ represents the threshold and SNR_{new} indicates the current SNR value. The SVM algorithm detect and isolates an anomalous node by SNR, energy, and selfishness features. Initially, the sender gathers node features from the node RREP message; then, the sender decides on a normal or anomalous node by applying the SVM algorithm.

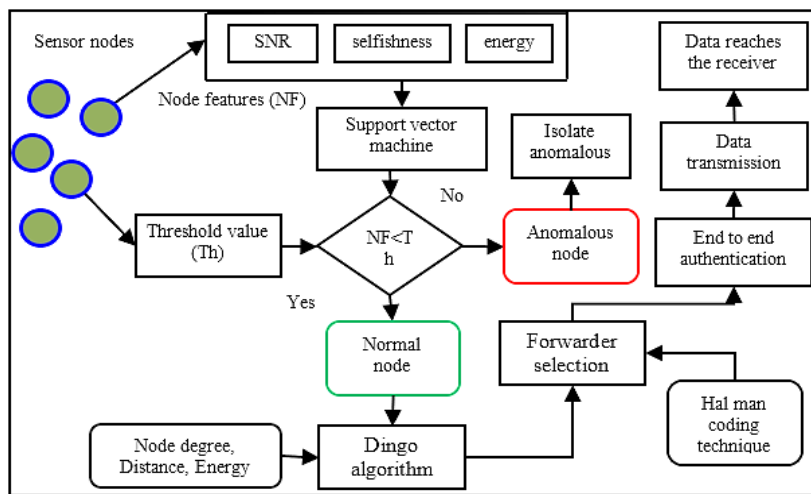


Figure 1. Architecture of the DAHC scheme

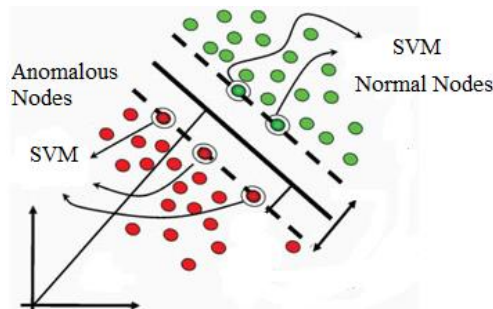


Figure 2. SVM based anomalous nodes classification

2.2. Dingo algorithm-based forwarder selection

Dingoes have an accurate sense of communication and it intercommunicate with each other by sensing several sound intensities [26]. In this method, dingo makes sound feedback, the dingoes replace their information with others. The amplitude of the shaking is updated by the strength of the person as the dingo moves into a new position from the earlier one. Group search is a concerning behavior of dingoes that builds its more extension to the behavior of dingoes. Figure 3 illustrates the dingo algorithm-based forwarder selection. The dingos algorithm procedure is classified such as: surrounding, tracking and attacking target. Dingoes are able to discover the position of the target. After tracing the position, the pack adopted by alpha circles the target. It is accepted that the accessible best agent is the target that is similar to the optimal because the chase region is not identified a priori.

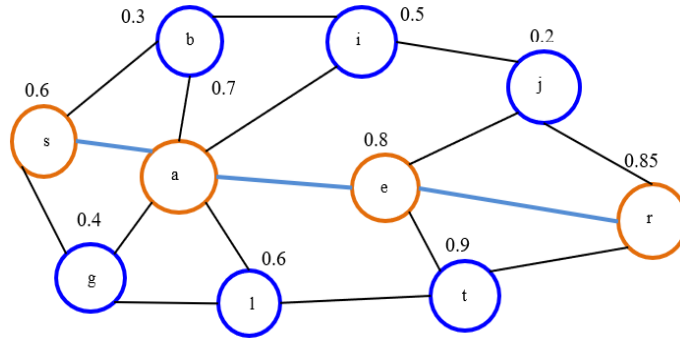


Figure 3. Example diagram of DAHC mechanism

Surrounding: along with the situation of the target (P^*, Q^*), a dingo can renew its position at the position of (P, Q). The feasible positions are marked approximately the best agent, regarding the present position by altering the vectors value. It is obviously shown how arbitrary vectors a_1 and a_2 allow dingoes to enter any position between the points. The dingoes to modify their positions inside the search region about the target in any arbitrary position is shown in (4) and (5).

$$\vec{D}_m = \left| \vec{U} \cdot \vec{P}_p(x) - \vec{P}(i) \right| \tag{4}$$

$$\vec{P}(i + 1) = \vec{P}_p(i) - \vec{V} \cdot \vec{D}(m) \tag{5}$$

Where, $\vec{U} = 2 \cdot \vec{u}_1, \vec{V} = 2 \cdot \vec{v} \cdot \vec{u}_2 - \vec{v}$ and $\vec{b} = 3 - \left(I * \left(\frac{3}{I_{max}} \right) \right)$

Tracking: in this section, all pack members like alpha and beta have a better awareness about the position of target. The alpha dingo forever controls the searching. Conversely, sometimes beta dingoes also contribute in searching. As per the position of a better search agent, other dingoes necessitate to inform their position. It can be denoting that alpha; beta dingoes modify their positions arbitrarily and compute the position of the target in the search space. Then we compute each dingo intensity (I) is given (6), (7), (8), and (9).

$$\vec{D}_\alpha = \left| \vec{U}_1 \cdot \vec{P}_\alpha - \vec{P} \right| \tag{6}$$

$$\vec{D}_\beta = \left| \vec{V}_1 \cdot \vec{P}_\beta - \vec{P} \right| \tag{7}$$

$$\vec{I}_\alpha = \log \left(\frac{1}{F_\alpha - (1E-100)} + 1 \right) \tag{8}$$

$$\vec{I}_\beta = \log \left(\frac{1}{F_\beta - (1E-100)} + 1 \right) \tag{9}$$

Attacking target: if there is no situation revise, it represents dingo ceased the hunt by attacking the target. Dingoes hunt for the target typically along with the pack's position. They always move advance to track for and hit predators. For that reason, it is utilized for arbitrary values, if the value is less than -1, it denotes target is traveling gone from the search agent, however if the value is better than 1, it represents pack approaches the prey. This interference assists the dingos to examine the targets globally.

2.3. Huffman coding based end to end authentication

To build the data transmission among the in-between nodes huffman coding is applied. After estimation of the energy and communication range, the node is assured for huffman security; if it matches huffman code next that specific node can access the data from the prior hop node. Figure 3 explains an example diagram of DAHC approach. The hop p security code is corresponding to binary value of 'k' acted as HC_k , here, $k=1,2,\dots$ Table 1 illustrates a hop count generation. At hop 1, the code of security is 01, and the continuous node security code is 10. The procedure of huffman coding is given below.

Table 1. Hop count generation

Route	Energy	HC security
s-a	0.7	01
s-g	0.4	01
s-b	0.3	01
a-i	0.5	10
a-e	0.8	10
a-l	0.6	10
e-j	0.2	11
e-r	0.85	11
e-t	0.9	11

Compute the node energy of neighboring nodes correspondingly. Choose the node with the highest energy. For security function, binary value for every hop is premised. If it equals accepted else attacker node. Then applying an authentication process by using an energy values huffman code in the routing nodes. The huffman code (HMC) computation equation is given;

$$HMC = C_m C_{m-1} \dots C_2 \quad (10)$$

here, m denotes the energy value length and C_m indicates the huffman code.

In this approach, the highest energy route nodes are s-a-e-r and routing nodes energy values are 0.7, 0.8, and 0.85. These nodes makes the huffman code is 111001. This procedure is repeated till the receiver received the data. Thus, an eavesdropper can't access the data and huffman code provide th authentication from sender to receiver in the network.

3. SIMULATION ANALYSIS

In this section, we examine the security of the DAHC and equate its execution with the OABC, CSHC and LCCBFE approaches are implemented by applying NS-2.35 [27]. The network topology is $550 \times 750 \text{ m}^2$. Here, we build the WSN with 100 sensor nodes and 10 anomolous nodes. This approach uses the traffic model like the constant bit rate traffic model and the priority queue to release the data from buffer [28]. The packet size is 512 bytes. The throughput, packet loss, residual energy, average, and delay factors are measures of the efficiency of the above-mentioned approaches.

Figure 4 illustrates the throughput of DAHC and OABC approaches with sensor nodes. From this figure, when increases the sensor node count, the DAHC and OABC approach throughput is minimized. Here, the OABC approach builds the route through an artificial bee colony algorithm, and this algorithm improves only routing efficiency. But, the DAHC approach has the highest throughput than the OABC approach, because the DAHC approach detects anomolous nodes by applying the SVM algorithm and the dingo algorithm selects the forwarder node efficiently. As a result, the DAHC approach increases the throughput. Figure 5 denotes the average delay of DAHC, and OABC approaches with sensor nodes. The average delay of the OABC approach is very high when increases the sensor node count. However, the DAHC mechanism is small increases the average delay since it selects the forwarder by the dingo algorithm. In addition, the huffman coding to improve the authentication in the network.

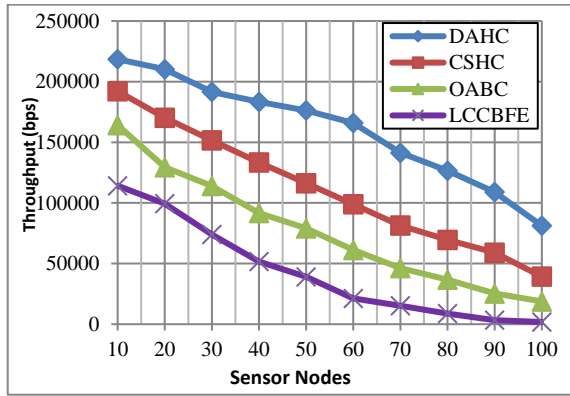


Figure 4. Throughput of DAHC, CSHC, LCCBFE, and OABC approaches with sensor nodes

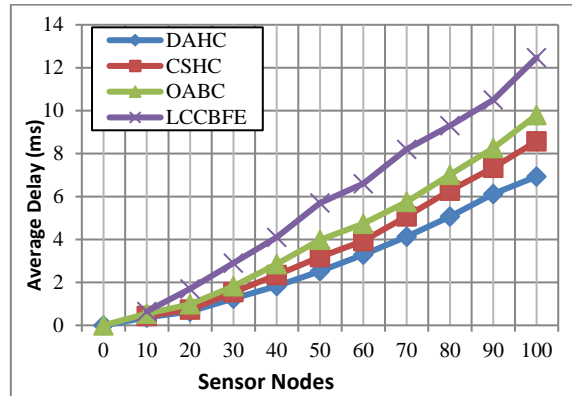


Figure 5. Average delay of DAHC, CSHC, LCCBFE, and OABC approaches with sensor nodes

Figure 6 illustrates the packet loss of DAHC and OABC approaches with sensor nodes. This figure clearly says that the DAHC approach minimizes packet losses since it detects the anomalous node efficiently. Furthermore, the Huffman coding to improve end-to-end authentication in the WSN. But, the OABC approach can't detect the anomalous node accurately; hence, it raises the packet loss rate. Residual energy is a significant factor for measuring network performance. Figure 7 demonstrates the residual energy of OABC and DAHC approaches based on sensor nodes.

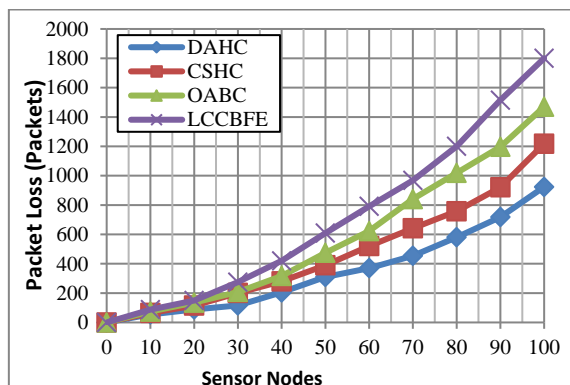


Figure 6. Packet loss of DAHC, CSHC, LCCBFE, and OABC approaches with sensor nodes

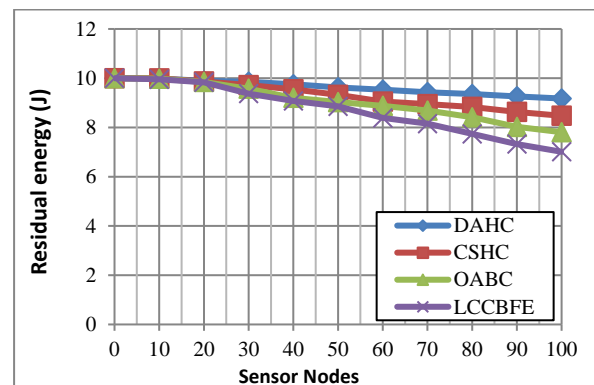


Figure 7. Residual energy of DAHC, CSHC, LCCBFE, and OABC approaches with sensor nodes

From this figure, the sensor node increases the sensor node residual energy also minimized due to sensor nodes consuming the energy during data transmission. The OABC approach consumed the highest amount of energy. Still, the DAHC approach consumes less energy since it detects the anomalous node efficiently by applying SVM with the dingo algorithm selects the forwarder efficiently. Therefore, the DAHC mechanism reduces the energy consumption.

4. CONCLUSION

The WSN fundamental challenges is offering an adequate security level to communicate the data safely. This article presents dingo algorithm-based forwarder selection and Huffman coding to improve authentication. This approach is a lightweight algorithm and the computational cost is very low. This approach aims to detect an anomalous node and improve the sensor node authentication. The sender node measures the node energy, node selfishness and SNR parameters to detect an anomalous node by employing SVM algorithm. The dingo algorithm fitness function selects the forwarder from sender to receiver efficiently based on node degree, node distance and node energy. During data transmission, the Huffman coding to build the binary hop count value, it improves the authentication in the WSN. Furthermore, the Huffman coding algorithm

is used to verify node authentication. Simulation analysis illustrates that the DAHC approach enhanced the anomalous nodes detection ratio and the throughput. Furthermore, the DAHC mechanism reduced the delay and increases the throughput. In future, we predict the forest fire by applying machine learning algorithm in WSN.




REFERENCES

- [1] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Networks*, vol. 24, no. 5, pp. 1821–1829, Jul. 2018, doi: 10.1007/s11276-016-1439-0.
- [2] S. Sharma, D. Sethi, and P. Bhattacharya, "Artificial neural network based cluster head selection in wireless sensor network," *International Journal of Computer Applications*, vol. 119, no. 4, pp. 34–41, Jun. 2015, doi: 10.5120/21058-3710.
- [3] C. Haixia, D. Ronghua, L. Ping, and L. Xiaying, "Clustering application of SVM in mobile ad-hoc network," in *Proceedings - International Conference on Intelligent Computation Technology and Automation, ICICTA 2008*, Oct. 2008, vol. 2, pp. 924–926, doi: 10.1109/ICICTA.2008.247.
- [4] A. R. Rajeswari, K. Kulothungan, S. Ganapathy, and A. Kannan, "Trust aware svm based ids for mitigating the malicious nodes in manet," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 8, pp. 185–197, 2019.
- [5] X. Qiu, Z. Du, and X. Sun, "Artificial intelligence-based security authentication: applications in wireless multimedia networks," *IEEE Access*, vol. 7, pp. 172004–172011, 2019, doi: 10.1109/ACCESS.2019.2956480.
- [6] S.-I. Chu, Y.-J. Huang, and W.-C. Lin, "Authentication protocol design and low-cost key encryption function implementation for wireless sensor networks," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2718–2725, Dec. 2015, doi: 10.1109/jsyst.2015.2487508.
- [7] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*, Jan. 2017, pp. 1–7, doi: 10.1109/ICACCS.2017.8014590.
- [8] C. Lai, H. Li, R. Lu, and X. Shen, "SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, no. 17, pp. 3492–3510, Dec. 2013, doi: 10.1016/j.comnet.2013.08.003.
- [9] A. Gupta and M. Kalra, "Intrusion detection and prevention system using cuckoo search algorithm with ANN in cloud computing," in *PDGC 2020 - 2020 6th International Conference on Parallel, Distributed and Grid Computing*, Nov. 2020, pp. 66–72, doi: 10.1109/PDGC50313.2020.9315771.
- [10] A. Kumar and B. Kaur, "Improved elliptic curve digital signature algorithm in wireless sensor networks," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2021*, Sep. 2021, pp. 1–5, doi: 10.1109/ICRITO51393.2021.9596478.
- [11] K. I. Ahmed, M. Tahir, M. H. Habaebi, S. L. Lau, and A. Ahad, "Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction," *Sensors*, vol. 21, no. 15, p. 5122, Jul. 2021, doi: 10.3390/s21155122.
- [12] E. Eziam, K. Tepe, A. Balador, K. S. Nwizege, and L. M. S. Jaimes, "Malicious node detection in vehicular ad-hoc network using machine learning and deep learning," in *2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOCOMW.2018.8644127.
- [13] R. F. Mansour, A. E. Amraoui, I. Nouaouri, V. G. Diaz, D. Gupta, and S. Kumar, "Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems," *IEEE Access*, vol. 9, pp. 45137–45146, 2021, doi: 10.1109/ACCESS.2021.3066365.
- [14] H. Yang, X. Zhang, and F. Cheng, "A novel algorithm for improving malicious node detection effect in wireless sensor networks," *Mobile Networks and Applications*, vol. 26, no. 4, pp. 1564–1573, Aug. 2021, doi: 10.1007/s11036-019-01492-4.
- [15] S. M. Shareef, Z. A. Abbas, and Z. M. Hilal, "A survey of security and smart home automation based on internet of things technology," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 3, pp. 1581–1588, Jun. 2022, doi: 10.11591/ijeecs.v26.i3.pp1581-1588.
- [16] B. H. Hameed, A. Y. Taher, R. K. Ibrahim, A. H. Ali, and Y. A. Hussein, "Based on mesh sensor network: design and implementation of security monitoring system with Bluetooth technology," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 1781–1790, Jun. 2022, doi: 10.11591/ijeecs.v26.i3.pp1781-1790.
- [17] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Anomaly detection in medical wireless sensor networks using SVM and linear regression models," *International Journal of E-Health and Medical Communications*, vol. 5, no. 1, pp. 20–45, Jan. 2014, doi: 10.4018/ijehmc.2014010102.
- [18] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical internet of things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019, doi: 10.1109/ACCESS.2019.2912870.
- [19] Y. K. Hatada and T. Fujii, "Receiver beacon transmission interval design using q-learning focused on packet delivery rate for multi-stage wireless sensor networks," in *2020 International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2020*, 2020, pp. 212–217, doi: 10.1109/ICAIIIC48513.2020.9065265.
- [20] Y. Yue, J. Li, H. Fan, and Q. Qin, "Optimization-based artificial bee colony algorithm for data collection in large-scale mobile wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 1–12, 2016, doi: 10.1155/2016/7057490.
- [21] S. A. Mulay, P. R. Devale, and G. V. Garje, "Intrusion detection system using support vector machine and decision tree," *International Journal of Computer Applications*, vol. 3, no. 3, pp. 40–43, 2010, doi: 10.5120/758-993.
- [22] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, Jan. 2021, doi: 10.1007/s12652-020-02020-z.
- [23] K. T. Saleh, N. A. A. Jabr, and I. H. Al-Qinani, "Chaotic map technique for enhancement security for android mobile system based on image encryption," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 3, pp. 1698–1703, Sep. 2022, doi: 10.11591/ijeecs.v27.i3.pp1698-1703.
- [24] S. Madhuri and J. Mungara, "Fusion of cuckoo search and hill climbing techniques based optimal forwarder selection and detect the intrusion," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 27, no. 1, pp. 328–335, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp328-335.
- [25] L. Kakkar *et al.*, "A secure and efficient signature scheme for IoT in healthcare," *Computers, Materials and Continua*, vol. 73, no. 3, pp. 6151–6168, 2022, doi: 10.32604/cmc.2022.023769.
- [26] K. Aravind and P. K. R. Maddikunta, "Dingo optimization based cluster based routing in internet of things," *Sensors*, vol. 22, no. 20, p. 8064, Oct. 2022, doi: 10.3390/s22208064.




- [27] H. Azath, A. K. Velmurugan, K. Padmanaban, A. M. S. Kumar, and M. Subbiah, "Ant based routing algorithm for balanced the load and optimized the AMNET lifetime," in *AIP Conference Proceedings*, 2023, vol. 2523, p. 020073, doi: 10.1063/5.0110676.
- [28] S.G. Rameshkumar, "Improving Quality of Service through enhanced node selection technique in Wireless Sensor Networks," *International Journal of MC Square Scientific Research*, vol. 8, no. 1, pp. 141-150, 2016.

BIOGRAPHIES OF AUTHORS






Dr. Nageswaran Usha Bhanu    received her Ph.D. in 2014, from the College of Engineering, Anna University, Chennai, India. She had completed her B.E. in Electronics and Communication Engineering in 1996 from Bharathiar University and M.E. in VLSI Design 2006 from Anna University. She is currently working as Professor in the Department of ECE in SRM Valliammai Engineering College, Tamil Nadu, India. Her areas of research interest include VLSI design, signal and image processing, and internet of things. She can be contacted at email: ushabhanu123@gmail.com.






Dr. Prathaban Banu Priya    was born on 3rd February 1991 in Tamil Nadu, India. She received her Ph.D. in Electronics and Communication Engineering from SRM Institute of Science and Technology, Chennai, India. She is graduated from Anna University, Chennai in 2012 with the bachelor of technology degree in electronics and communication engineering. She received the Master of Technology degree in Embedded Systems Technologies from Anna University, Chennai in 2014 with gold medal. She is currently working as an assistant professor in the department of Networking And Communications, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Kancheepuram, Chennai, India. She has published more than 20 research papers in national, international conferences, journals including 6 in science citation indexed journals with 45 citations. She has published 5 patents and received a grant-in-aid from institutions of engineers (India) (R.6/2/DR/2019- 20/DR2020005) for her doctorate degree research in 2018. Her research interests include embedded systems, IoT, artificial intelligence, deep learning, data science, signal processing and image processing. She is a life member of Institutions of Engineers India (IEI) and Institution of Electronics and Telecommunication Engineers (IETE) and Associate Member of Institute of Electrical and Electronics Engineers (IEEE). She can be contacted at email: banupriyaprathaban@gmail.com.






Dr. Tiruveedhula Sajana    is currently working as Associate Professor in Department of AI and DS, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Received Ph.D. from Koneru Lakshmaiah Education Foundation, Vaddeswaram in 2019. M.Tech. in CSE in 2011. B.Tech. in CSE from K.L.C.E, Acharya Nagarjuna University in 2007. Research interests are machine learning, big data analytics, deep learning. published 12 papers in international journals, presented 9 papers national and international conferences. Obtained 2 Indian Patent and applied 1 Indian patent. Reviewer for the peer-reviewed journal advances in science, technology and engineering systems journal. Resource person for various technical talks. Organized several workshops, technical talks, guest lectures, workshops. She can be contacted at email: sajana.cse@kluniversity.in.






Dr. Shanmugasundaram Shanthi, M.E., Ph.D.,    is Passionate in Teaching and Administrative Works. She has Completed Doctorate in Information and Communication Engineering from Anna University Chennai. She has done Research in Biomedical Engineering and Artificial Intelligence. She brings with her an Industry Experience of 6 Years and Teaching Experience of 21 Years in Engineering Colleges. Presented research papers in National and International conferences. Published 28 research papers in International Journals. Published 2 patents. She is a recognized Supervisor in Anna University Chennai. Highly motivated Professor, inspiring students to pursue academic and personal excellence. Positive approach, consistently strive to create a challenging and engaging learning environment in which the students become lifelong scholars and learners. She can be contacted at email: sshanthijj@gmail.com.






Murugan Mageshbabu    is Research Associate of Saveetha School of Engineering, Chennai. He studied B.Tech.-Electronics and Communication Engineering at Vellore Institute of Technology, Vellore in the year 2005 and M.E.-Electronics and Control Engineering at Sathyabama University, Chennai in 2012. He worked as a lecturer at Thiruvalluvar College of Engineering from 2005 to 2007 and also as lecturer and assistant professor from 2007 to 2018. He attended many faculty developments programs and national and international conferences. He has more knowledge and interest about this electronics field. He can be contacted at email: mageshbabum2002.sse@saveetha.com.



Erram Swarnalatha    is currently working as Assistant Professor in Department of ECE, Embedded Systems, Guru Nanak Institute of Technology, Hyderabad, India. Research interests are machine learning, big data analytics, deep learning. published 12 papers in international journals, presented 9 papers national and international conferences. obtained 2 Indian patent and applied 1 Indian patent. Reviewer for the peer-reviewed journal advances in science, technology and engineering systems journal. She can be contacted at email: swarnalatha.ecegnit@gniindia.org.



Mrs. Kuntiyellannagari Bhagya Laxmi    is currently Perusing Ph.D. at SRM Institute of Science and Technology Kattankulathur Tamil Nadu and working as Assistant Professor in Department of CSE, Matrusri Engineering College Hyderabad India. M.Tech. in CSE in 2010 from JNTUH. Research interests are machine learning, big data analytics, deep learning. Published 11 papers in international journals, presented 3 papers national and international conferences. She can be contacted at email: bhagyalaxmi@matrusri.edu.in.



Dr. Kannabiran Saravanan B.E., M.E., Ph.D.,    is an Associate Professor in the Department of Information Technology since 2010. He completed his B.E. degree in Computer Science and Engineering in the year 2003 from G.K.M. College of Engineering and Technology (Madras University), Chennai and M.E. degree in Embedded System Technologies in the year 2007 from Veltech Engineering College (Anna University), Chennai. He has obtained his Ph.D. in Information and Communication Engineering from Anna University, Chennai, in 2020. His research interests include wireless networks. He has 17 years of teaching experience and he has presented and published many articles. He can be contacted at email: saravanan.it@rmd.ac.