Bayesian decision model based reliable route formation in internet of things

Mohanavel Jothish Kumar[1], Suman Mishra[2], Elangovan Guruva Reddy[3], Madasamy Rajmohan[4], Subbiah Murugan[5], Narayanasamy Aswin Vignesh[6]
[1]School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, India
[2]Department of Electronics and Communication Engineering, CMR Engineering College, Hyderabad, India
[3]Department of Artificial Intelligence and Data Science, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[4]Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Chennai, India
[5]Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India
[6]Department of Computer Science, Annai Vailankanni Arts and Science College, Affiliated to Bharathidasan University, Thanjavur, India

Article Info

Article history:

Received Jan 22, 2024
Revised Feb 25, 2024
Accepted Mar 16, 2024

Keywords:

Active unreliable recognition
Bayesian decision model
reliable routing
Internet of things
Passive unreliable recognition
Quality of service

ABSTRACT

Security provisioning has become an important issue in wireless multimedia networks because of their crucial task of supporting several services. This paper presents Bayesian decision model based reliable route formation in internet of things (BDMI). The main objective of the BDMI approach is to distinguish unreliable sensor nodes and transmit the data efficiently. Active and passive attack recognition methods identify unreliable node sensor nodes. Remaining energy, node degree, and packet transmission rate parameters to observe their node possibilities for recognizing the passive unreliable nodes. In active recognition, the base station (BS) confirms every sensor node identity, remaining energy, supportive node rate, node location, and link efficiency parameters to detect active unreliable sensor nodes. The Bayesian decision model (BDM) efficiently isolates an unreliable sensor node in the multimedia network. Simulation outcomes illustrate that the BDMI approach can efficiently enhance unreliable node detection and minimize the packet loss ratio in the network.

Corresponding Author:

Mohanavel Jothish Kumar
School of Computer Science Engineering and Information Systems, Vellore Institute of Technology
Chennai, India
Email: jothishkumar.m@vit.ac.in

1. INTRODUCTION

The initiation of technologies in 5G and the internet of things (IoT) indicates the next signal of ubiquitous linked society [1]. In exacting, multimedia networks [2] and their continuing union with machine learning technologies are broadly predictable to get exciting services and applications for observing, pleasurable, training, and functioning in smart homes, smart cities, hills areas [3], healthcare and transportation [4]. Conventional security solutions may suffer from opponent attacks in composite multimedia transmission scenarios because of the rising count of multimedia sensors and the broad range of applications [5]. Security approaches are executed to conquer the conflict between costs and security [6]; as a result, failure to defend legitimate transmissions [7], [8]. Hence, this paper concentrates on unreliable node detection and improves IoT network security. The Bayesian decision model (BDM) algorithm uses probabilistic models and statistical decision-making methods to decide on routing depending on the network's state and the data transmission reliability needs [9]. The steps involved are as follows [10]: The program continually scans the network to acquire data on connection quality, congestion levels, and other pertinent characteristics.

Problem formulation: trust aggregation authentication protocol founded on the machine learning technique (TAML) approach is derived from the trust value based on node behavior [11]. In this approach, the sensor node trust value is lesser than a threshold that the node authentication token is unacceptable; next, neglect that node. The support vector machine (SVM) algorithm calculates an adaptive trust threshold value. However, this approach needs to improve the routing efficiency. BDM-based reliable roting in multimedia networks is introduced to solve such issues. It uses a BDM to detect unreliable nodes efficiently.

Work contribution: the proposed mechanism uses active and passive attack recognition methods to identify unreliable node sensor nodes. Remaining energy, node degree, and packet transmission rate parameters to observe their node possibilities for recognizing the passive unreliable nodes. In active recognition, the base station (BS) confirms every sensor node identity, remaining energy, supportive node rate, node location, and link efficiency parameters to detect active unreliable sensor nodes. The BDM efficiently isolates an unreliable sensor node in the multimedia network. Simulation outcomes illustrate that the Bayesian decision model based reliable route formation in internet of things (BDMI) approach can efficiently enhance unreliable node detection and minimize the packet loss ratio in the network. The BDMI approach isolated many attacks, for example, clone attacks, blackhole attacks, routing attacks, and malicious attacks.

Reliable data transmission with a high-security approach using particle swarm optimization for selecting an optimal relay node [12]. Encryption encrypts the digital signature, enhancing transmission security and confidentiality. However, the cryptography algorithm increases complexity and routing overhead. Neural network and SVM algorithms detect the attacker [13]. But, it needs routing efficiency for better data transmission. A Bayesian network origin encoding technique is established on dynamic and overlapped arithmetic coding that solves the network issues [14]. The Bayesian mechanism contains pricing and auctions and receives the Nash Equilibrium points of the fundamental Bayesian games [15]. The prices and allocations are adapted by applying the Bayesian information. Bayesian pricing approach that the prices are tailored using the Bayesian information to ensure the quality of service (QoS) necessities [16]. The regression learning algorithm is utilized to make the condition possible to detect malicious nodes. The Bayesian Nash Equilibrium method estimates the effect of imperfect information on fulfilling the QoS necessities. However, the Bayesian learning algorithm can’t be able to differentiate active and passive attackers.

Deep learning algorithm enabled sensor node authentication to enhance network security [17]. This approach uses blind feature learning and lightweight authentication methods to detect malicious nodes. But, it needs to improve the routing efficiency. A secure and efficient privacy-preserving unspecified authentication approach offers data security and privacy [18]. A trust-based formal model depicts the fault identification procedure and confirms faults [19]. However, this approach not satisfied QoS requirements. The Bayesian filter model computes the trust factor by the node behavior to detect the misbehaving nodes [20]. A Bayesian trust method that precisely integrates abnormal behavior and observing uncertainty [21]. This method to learn the thresholds for categorizing nodes as reliable or unreliable is established on their trust values. Trust evaluation and update mechanisms are significant in defending network security [22]. Here, the trust is computed by the data, link, and node evidence. The penalty and reward components update the trust established on the sliding time window [23]. Machine and deep learning introduced the trust model for detecting unreliable nodes [24]. This approach applies a Bayesian neural network that joins deep learning with possibility modeling for intelligent results in the trust calculation of reliable and unreliable nodes. However, these approaches need to improve the routing efficiency in the network. The cooperative routing objective is to enhance the lifetime and minimize the route detection cost [25]. This approach uses the fresher encounter algorithm to improve energy efficiency and solve dead node issues. But it does not concentrate detects unreliable nodes.

The structure of the remaining parts of the article is as follows: section 2 describes Bayesian decision model based reliable route formation in IoT. Passive unreliable node recognition and active unreliable node recognition parts are described this section. Next, we evaluate the network performance based on simulation results are specified in section 3, and the article’s conclusion in section 4.

2. PROPOSED METHOD

The transmission efficiency minimizes because of channel interference, bandwidth, and packet drop. In a wireless multimedia network, every sensor node updates information like node degree, remaining energy, faulty status, and node-link status. A sensor node decides the node’s reliability by the BDM. The BDM computes the condition possibility using the parameters like node remaining energy, link efficiency, and node bandwidth to verify the node reliability. Figure 1 explains the block diagram of the BDMI approach.

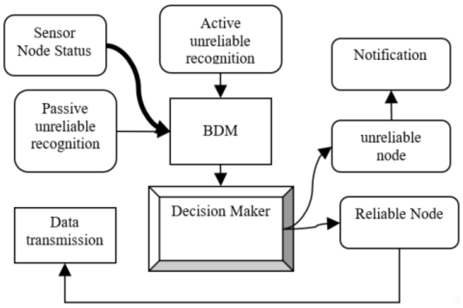

Figure 1. Architecture of the BDMI scheme

Here, the possibility is greater than the threshold that the node is reliable. The unreliable detection model is done at two levels using BDM algorithm. This approach may be communicated by creating the prior possibilities of all sender nodes. The BDM is used to simplify the computation of conditional possibility for detecting unreliable nodes. The sender node with the receiver in a BDM has an involved conditional probability.

2.1. Passive unreliable node recognition

This approach identifies an unreliable node sensor through passive and active attack recognition. Managing the execution in dynamic link failures remains a complex role. Wireless link quality degrades because node energy is drained, time to live expires, obstacles, or other interference. When the sensor node is identified in passive recognition, i.e., link failure occurs at a time; the nodes go to an inactive state in the network. In passive attack recognition, sensor nodes are essential to sporadically the node's remaining energy, node degree, and packet transmission ratio parameters to observe their node possibilities for recognizing the passive attack. Energy weakening is the foremost cause of the node's rapid expiry. The node's remaining energy indicates an amount of energy remaining at a particular time. The node remaining energy (RE) calculation is specified in (1).

$$RE = Initial\ Energy - Utilized\ Energy \quad (1)$$

Each sensor node observes the link quality by the node route request (R_{REQ}) and route reply (R_{REP}) messages to ensure connectivity among all sensor nodes called node degree (ND). The failed links are recognized utilizing information about the inactivity of wireless connections among nodes. The packet transmission ratio (PTR) measures the node-link quality; as a result, the packet can forward to the receiver successfully at a lesser cost. The PTR computation is shown in (2), and node passive attack reorganization is given in (3).

$$PTR = \frac{Received\ Packet}{Transmitted\ Packet} \quad (2)$$

$$Node\ Efficiency = \frac{ND * RE * PTR}{3} \quad (3)$$

Where ND indicates the node degree, RE represents the residual energy, and PTR denotes the packet transmission ratio. Every sensor node updates its RE, PTR, and ND; then the BS computes the node efficiency. Next, the BDM decides whether the node is reliable or unreliable. Finally, isolates passive unreliable nodes from the network.

2.2. Active unreliable node recognition

The BS continually confirms every sensor node status in active unreliable node recognition. The BS preserves the updated details like sensor node identity, remaining energy, node supportive rate, node location, and link efficiency. Depending on the updated information, the BS computes the truthful value of every sensor node. In this method, each node handles the truthful value table. This table value contains node identity (ID), supportive rate, link efficiency, node location, and remaining energy. Sometimes unreliable nodes show the wrong ID and wrong position. The node RE indicates the amount of energy remaining at a particular time. The unreliable node has the highest RE compared to the other nodes. Thus, these reasons are chances that the node is unreliable. The node supportive rate (NSR) indicates the rate of supportive (Supp) and unsupportive (UnSupp) rates between two nodes. That recognizes node behaviors, and this calculation is specified in (4).

$$NSR = \begin{cases} PS_{i,j} = \frac{Supp_{i,j}}{Supp_{i,j}+UnSupp_{i,j}+2} \\ PUS_{i,j} = \frac{UnSupp_{i,j}}{Supp_{i,j}+UnSupp_{i,j}+2} \end{cases} \tag{4}$$

Where $PS_{i,j}$ indicates the probability that node i trust node j will execute supportively during R_{REQ} packet distribution action and probability unsupportive ($PUS_{i,j}$) represents the probability that node i trust node j will perform not supportively during R_{REP} packet distribution action. $Supp_{i,j}$ and $UnSupp_{i,j}$ are the supportive and unsupportive rates that node i control for node j. If probability supportive ($PS_{i,j}$) is larger than the threshold, that node chances the reliable and/or $PUS_{i,j}$ is larger than the threshold, and that node chances an active unreliable node in the network. The link efficiency represents the link strength between two nodes. Link efficiency can be measured by applying parameters, for example, received signal strength indication (RSSI) [26], distance and node degree. the link efficiency computation is specified in the (5).

$$Link\ Efficiency = \frac{RSSI-ND}{\text{Dist}} \tag{5}$$

Where RSSI represents the received signal strength indication, dist represents the distance, and ND indicates the node degree. The BS checks the sensor node ID, location, link efficiency and NSR values. Then, decides whether the node is reliable or actively unreliable by applying the BDM. Finally, separates an active unreliable node from the network.

2.3. BDM

The specified suggestions are utilized in originating a rational decision from true evidence. In this approach, the BDM is used to decide the possibilities of specific event types. The suggestion is applied to calculate the conditional probability for variables with specified information regarding other sensor nodes. BDM is a technique of inference in that Bayes' rule is utilized to inform the possibility evaluate for a suggestion as an extra confirmation. The BDM purpose is to compute the node trust values in a network. Assume that the entire node forwards data from a node to a receiver self-governing from each other. That is, if one node is established as unreliable, the possibility of the following packet is unreliable. This possibility assumption represents that the attacks can emerge in several forms in one or many nodes. Figure 2 explains the flowchart of the BDMI approach.

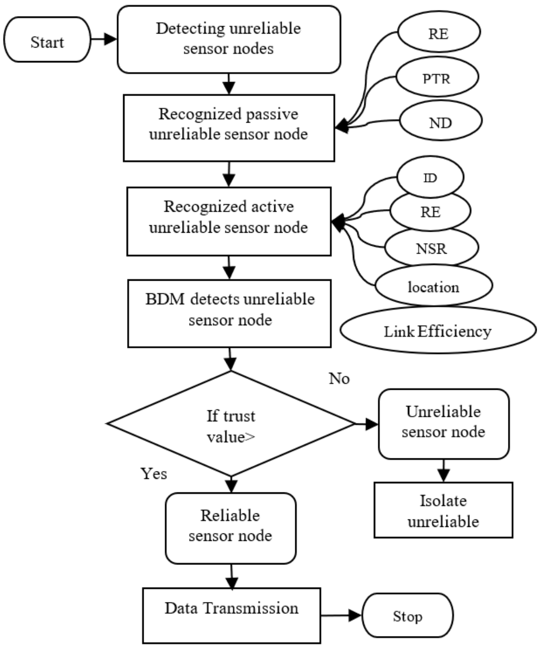
Start
Detecting unreliable sensor nodes
RE
PTR
ND
Recognized passive unreliable sensor node
ID
RE
NSR
location
Recognized active unreliable sensor node
BDM detects unreliable sensor node
Link Efficiency
No
If trust value>
Unreliable sensor node
Yes
Isolate unreliable
Reliable sensor node
Data Transmission
Stop

Figure 2. Flowchart of BDMI approach

From Figure 2, RE, PTR, and ND factors are used to recognize the passive unreliable sensor nodes, and node ID, RE, NSR, location, and link efficiency factors are used to recognize the active unreliable sensor node. Then, the BDM algorithm concludes an unreliable sensor node based on sensor node possibility. If the sensor node possibility is higher than a threshold, that node decides it is unreliable or else unreliable. The threshold value is present between 0 and 1. The threshold value is set to 0.5 value. The BDM assumption applies to passive unreliable, active unreliable, and reliable sensor nodes specified in (6)-(8). Here, n_i indicates a sensor node, UN represents the total unreliable sensor node, P indicates the possibility of reliable and unreliable sensor nodes, and RN indicates the reliable sensor node.

$$P(UN|Passive\ Unreliable) = \frac{\mathrm{P}\left(n_{i\ is\ passive\ unreliable}|UN\right)*P(UN)}{\mathrm{P}\left(n_{i\ is\ passive\ unreliable}\right)} \quad (6)$$

$$P(UN|Active\ Unreliable) = \frac{\mathrm{P}\left(n_{i\ is\ active\ unreliable}|UN\right)*P(UN)}{\mathrm{P}\left(n_{i\ is\ active\ unreliable}\right)} \quad (7)$$

$$P(RN|\ Reliable) = \frac{\mathrm{P}\left(n_{i\ is\ reliable}|RN\right)*P(RN)}{\mathrm{P}\left(n_{i\ is\ reliable}\right)} \quad (8)$$

3. SIMULATION ANALYSIS

In this work, the network simulator -2.35 tool measures the network function of TAML and BDMI approaches. The simulation environment utilizes 100 sensor nodes, and these nodes' transmission range is set to 250 meters [27]. BDMI and TAML approach simulation time is 200 seconds, using 30 unreliable sensor nodes. Every node communicates data packets at a pre-set rate is 2 Mega bits per seconds, and it applies to the 802.11 system. The computational complexity of the BDMI approach is O(n^3). It detects the performance of TAML and BDMI approaches in terms of the packet transmission ratio, average delay, throughput ratio, packet loss ratio, normalized routing load and unreliable node detection ratio based on several unreliable nodes. Figure 3 explains the packet transmission ratio and Figure 4 explains an average delay based on the number of unreliable nodes.

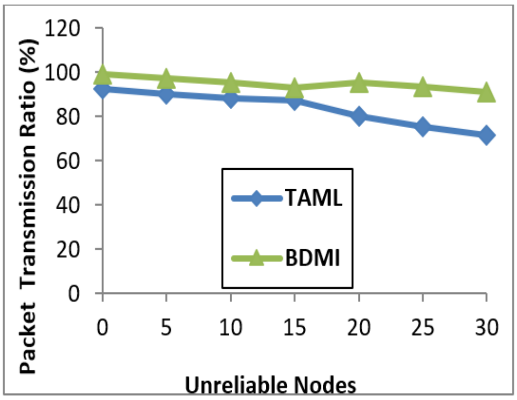

Figure 3. Packet transmission ratio of TAML and BDMI based on the number of unreliable nodes

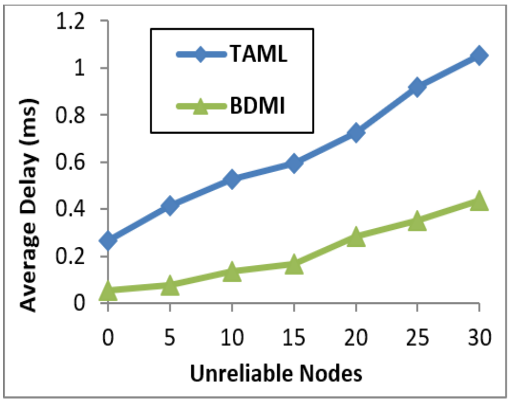

Figure 4. Average delay of TAML and BDMI based on the number of unreliable nodes

Figure 3 minimizes the packet transmission ratio with the number of unreliable nodes increasing. In the TAML approach, the packet transmission ratio is meager when the number of unreliable nodes is high. The following hop selection for forwarding a node-link quality is terrible. But, the BDMI approach selects the forwarder node by opportunistic routing; as a result, it raises the packet transmission ratio. From Figure 4, the unreliable node rises, and the average delay value increases since an unreliable node makes an additional delay. However, the BDMI approach has a lesser average delay since it detects unreliable nodes efficiently by the Bayesian decision model. Figure 5 displays the throughput ratio and Figure 6 demonstrates a detection ratio based on the number of unreliable nodes.

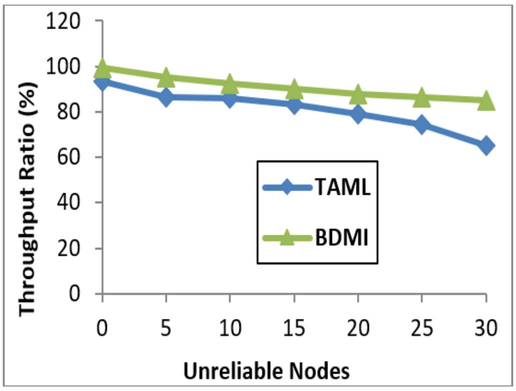

Figure 5. Throughput ratio of TAML and BDMI based on the number of unreliable nodes

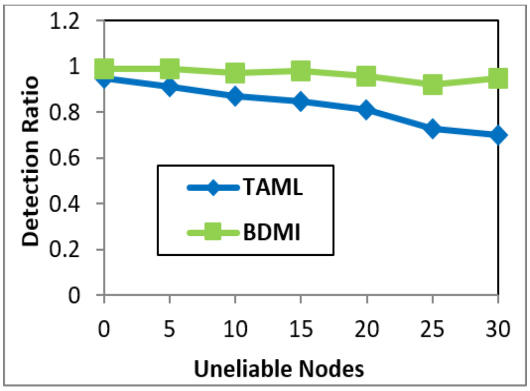

Figure 6. Detection ratio of TAML and BDMI based on the number of unreliable nodes

According to Figure 5, the BDMI approach uses a BDM for isolating unreliable nodes and forwarder node selection based on node energy, node RSSI, node packet transmission ratio, and node available bandwidth to improve the routing efficiency. Thus, the BDMI approach increases the network throughput in the network. From Figure 6, the BDMI approach has the highest detection ratio compared to the TAML approach since the BDMI approach uses a BDM to separate an active by applying ND, RE, and PTR parameters. In addition, the BDM isolates passive unreliable sensor nodes based on sensor node ID, RE, location, link efficiency, and NSR values. Though, the TAML approach using the trust method can't detect unreliable nodes efficiently. Figure 7 explains packet loss ratio and Figure 8 displays the normalized routing load based on the number of unreliable nodes.

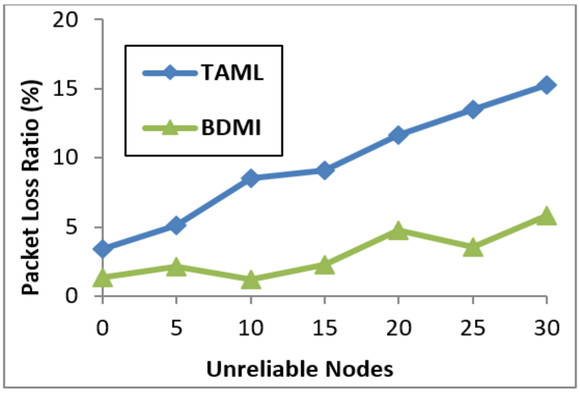

Figure 7. Packet loss ratio of TAML and BDMI based on the number of unreliable nodes

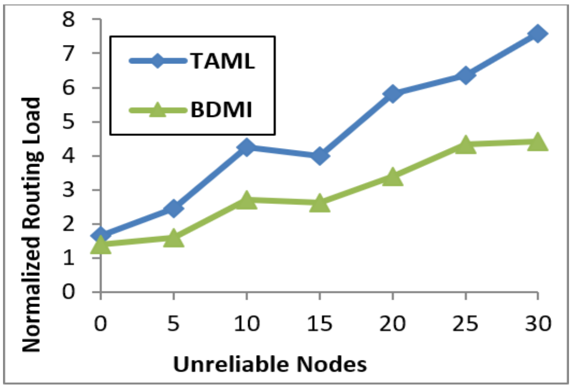

Figure 8. Normalized routing load of TAML and BDMI based on the number of unreliable nodes

Figure 7 raises the packet loss ratio with the number of unreliable nodes increasing. In the TAML approach, the packet loss ratio is high when the number of unreliable nodes is high. The following hop selection for forwarding a node-link quality is terrible. But, the BDMI approach detects the active and passive unreliable node efficiently; as a result, it minimizes the packet loss ratio. From Figure 8, the unreliable node rises, and the normalized routing load value increases since an unreliable node makes an additional routing load. However, the BDMI approach has a lesser routing load since it detects unreliable nodes efficiently by the Bayesian decision model. The existing TAML mechanism has the highest routing load compare to the BDMI mechanism since it can't detect an unreliable node efficiently.

4. CONCLUSION

Traditional security solutions lack computing effectiveness and deal with promising security challenges. Generally, in a wireless network, passive unreliable nodes affect the network simply, and active unreliable nodes affect the network efficiently. Thus, active and passive attack recognition is vital for detecting unreliable node sensor nodes. Remaining energy, node degree, and packet transmission ratio parameters observed their node possibilities for recognizing the passive unreliable sensor nodes. In active unreliable node recognition, the BS confirmed every sensor node identity, remaining energy, node supportive rate, node location, and link efficiency parameters detected active attacks. Next, the BDM confirmed active and passive unreliable sensor nodes efficiently. Simulation results demonstrated that the BDMI approach reduced packet losses and network delay. Furthermore, the BDMI approach raised the packet transmission ratio and increased unreliable sensor nodes detection efficiently. The BDMI approach isolated many attacks, for example, clone attacks, blackhole attacks, routing attacks, and malicious attacks. However, the BDMI approach can't be able to detect a gray hole attack. The data integrity algorithm may be used to detect the gray hole attack in the future.

REFERENCES

[1] V. G. Sivakumar, V. V. Baskar, M. Vadivel, S. P. Vimal, and S. Murugan, "IoT and GIS integration for real-time monitoring of soil health and nutrient status," in *International Conference on Self Sustainable Artificial Intelligence Systems, ICSSAS 2023 - Proceedings*, Oct. 2023, pp. 1265–1270, doi: 10.1109/ICSSAS57918.2023.10331694.

[2] 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.

[3] H. R. Singh, "Wireless sensor network for environmental monitoring in hill areas as a preventive measure of global warming," *International Journal of Advances in Signal and Image Sciences*, vol. 5, no. 2, p. 1, Dec. 2019, doi: 10.29284/ijasis.5.2.2019.1-6.

[4] N. R. Patel and S. Kumar, "Wireless sensor networks' challenges and future prospects," in *Proceedings of the 2018 International Conference on System Modeling and Advancement in Research Trends, SMART 2018*, Nov. 2018, pp. 60–65, doi: 10.1109/SYSMART.2018.8746937.

[5] W. Chen and F. Wang, "Retraction note: practical application of wireless communication network multimedia courseware in college basketball teaching(EURASIP Journal on Wireless Communications and Networking, (2021), 2021, 1, (73), 10.1186/s13638-021-01943-1)," *Eurasip Journal on Wireless Communications and Networking*, vol. 2023, no. 1, p. 3, Jan. 2023, doi: 10.1186/s13638-023-02215-w.

[6] M. Ghadi, L. Laouamer, and T. Moulahi, "Securing data exchange in wireless multimedia sensor networks: perspectives and challenges," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3425–3451, Mar. 2016, doi: 10.1007/s11042-014-2443-y.

[7] Y. Liu, L. Zhu, and F. Liu, "Design of multimedia education network security and intrusion detection system," *Multimedia Tools and Applications*, vol. 79, no. 25–26, pp. 18801–18814, Jul. 2020, doi: 10.1007/s11042-020-08724-w.

[8] S. Harikishore and V. Sumalatha, "Retraction note to: a reliable multi-hop opportunistic routing scheme with bandwidth guarantee for multimedia wireless mesh networks (Journal of Ambient Intelligence and Humanized Computing, (2021), 12, 5, (4583-4592), 10.1007/s12652-020-01838-x)," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. S1, p. 63, Apr. 2023, doi: 10.1007/s12652-022-03944-4.

[9] R. K. Vanakamamidi, N. Abirami, C. S. Kumar, L. Ramalingam, S. Priyanka, and S. Murugan, "IoT security based on machine learning," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 683–687, doi: 10.1109/SmartTechCon57526.2023.10391727.

[10] M. Liang *et al.*, "Evaluating the comprehensive performance of 5G base station: a hybrid MCDM model based on bayesian best-worst method and DQ-GRA technique," *Mathematical Problems in Engineering*, vol. 2022, 2022, doi: 10.1155/2022/4038369.

[11] S. A. Soleymani *et al.*, "A trust model using edge nodes and a cuckoo filter for securing VANET under the NLoS condition," *Symmetry*, vol. 12, no. 4, p. 609, Apr. 2020, doi: 10.3390/SYM12040609.

[12] Y. Gao and W. Liu, "BeTrust: A dynamic trust model based on Bayesian inference and Tsallis entropy for medical sensor networks," *Journal of Sensors*, vol. 2014, pp. 1–10, 2014, doi: 10.1155/2014/649392.

[13] S. Chinnaswamy and A. K, "Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks," *Computers and Electrical Engineering*, vol. 91, p. 107130, May 2021, doi: 10.1016/j.compeleceng.2021.107130.

[14] C. Wang and E. Bertino, "Sensor network provenance compression using dynamic Bayesian networks," *ACM Transactions on Sensor Networks*, vol. 13, no. 1, pp. 1–32, Feb. 2017, doi: 10.1145/2997653.

[15] A. K. Chorppath, T. Alpcan, and H. Boche, "Bayesian mechanisms for wireless network security," in *2014 IEEE International Conference on Communications, ICC 2014*, Jun. 2014, pp. 865–870, doi: 10.1109/ICC.2014.6883428.

[16] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2024, pp. 1755–1759, doi: 10.1109/iceca58529.2023.10394962.

[17] A. K. Chorppath, F. Shen, T. Alpcan, E. Jorswieck, and H. Boche, "Bayesian mechanisms and learning for wireless networks security with QoS requirements," in *IEEE International Conference on Communications*, Jun. 2015, vol. 2015-September, pp. 7180–7185, doi: 10.1109/ICC.2015.7249472.

[18] S. Calisir and M. K. Pehlivanoglu, "Model-free reinforcement learning algorithms: a survey," in *27th Signal Processing and Communications Applications Conference, SIU 2019*, Apr. 2019, pp. 1–4, doi: 10.1109/SIU.2019.8806389.

[19] 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.

[20] S. Jegadeesan, M. Azees, N. R. Babu, U. Subramaniam, and J. D. Almakhles, "EPAW: efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020, doi: 10.1109/ACCESS.2020.2977968.

[21] R. Raman, S. Muthumarilakshmi, G. Jethava, R. Jagtap, M. Lalitha, and S. Murugan, "Energy monitoring in solar-powered buildings using internet of things," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 318–322, doi: 10.1109/SmartTechCon57526.2023.10391826.

[22] S. Bhattacharjee, M. Chatterjee, K. Kwiat, and C. Kamhoua, "Multinomial trust in presence of uncertainty and adversaries in DSA networks," in *Proceedings - IEEE Military Communications Conference MILCOM*, Oct. 2015, vol. 2015-December, pp. 611–616, doi: 10.1109/MILCOM.2015.7357511.

[23] J. Jiang, X. Zhu, G. Han, M. Guizani, and L. Shu, "A dynamic trust evaluation and update mechanism based on C4.5 decision tree in underwater wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9031–9040, Aug. 2020, doi: 10.1109/TVT.2020.2999566.

[24] E. Eziama, 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. 2018, pp. 1–6, doi: 10.1109/GLOCOMW.2018.8644127.

[25] A. Unnikrishnan and V. Das, “Cooperative routing for improving the lifetime of wireless ad-hoc networks,” *International Journal of Advances in Signal and Image Sciences*, vol. 8, no. 1, pp. 17–24, Jan. 2022, doi: 10.29284/ijasis.8.1.2022.17-24.

[26] S. N. Reddy and J. Mungara, “Received signal strength indication based clustering and aggregating data using Q-learning in mobile Ad Hoc network,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 27, no. 2, pp. 867–875, Aug. 2022, doi: 10.11591/ijeecs.v27.i2.pp867-875.

[27] B. Meenakshi, B. Gopi, L. Ramalingam, A. Vanathi, S. Sangeetha, and S. Murugan, “Wireless sensor networks for disaster management and emergency response using SVM classifier,” in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 647–651, doi: 10.1109/SmartTechCon57526.2023.10391435.

BIOGRAPHIES OF AUTHORS

Mohanavel Jothish Kumar received his Ph.D., in Computer Science and Engineering from College of Engineering, Guindy Campus, Anna University (2019) and master’s degree in information technology from Sathyabama University (2007). Currently he is working as Assistant Professor- Senior, Department of Smart Computing, School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore. He has been in professional field for more than 15 years and has served in various capacities. His research interest includes congestion control, IoT, and unmanned aerial system. He can be contacted at email: jothishkumar.m@vit.ac.in.

Suman Mishra is working as Professor and Head of the Department of Electronics and Communication Engineering in CMR Engineering College, Hyderabad. He has over 21years of teaching and research experience coupled with4 years of industrial experience. He is guiding a fulltime research scholar for Ph.D. degree. His research areas include digital image processing, embedded systems, and wireless sensor networks. He has guided 18M.Tech dissertations and 45B.Tech projects. He has published his research findings in 32 journals and conferences both in national and international level. He is lifetime member of AMIE, ISTE and IAENG. He is the reviewer for two International Journals and has been a member of technical committees fortwo International Conferences. He has acted as examiner for Ph.D. theses. He has been guiding student community to develop excellent path breaking projects that are useful to mankind. He can be contacted at email: emailssuman@gmail.com.

Elangovan Guruva Reddy received his B.E. degree from University of Madras in 1995, his M.E. degree from CEG, Anna University in 2005, and completed his Ph.D., in “Wireless Networks” at MAHER, Chennai in 2022. He has more than twenty years of teaching experience in various Institutions and teaches postgraduate and undergraduate courses in wireless sensor networks, ad-hoc networks, digital system design, microprocessor, transmission lines and wave guides, computer architecture, operating systems and object-oriented programming. He is currently working as Associate Professor in the Department Artificial Intelligence and Data Science, at Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. He as presented many papers in National and International Conferences. Also, he has published books “Transmission Lines and Networks”, Umayal Publishers. 2006, and “Advanced Computer Architecture”, Umayal Publishers, Umayal Publisher, 2011. He is a member in IEEE, CSI, and life member is ISTE. He can be contacted at email: gurugovan@gmail.com.

Madasamy Rajmohan is working as an Assocaite Professor in Department of Electronics and Communication Engineering at Hindustan Institute of Technology Science, Chennai, Tamilnadu, India. He completed his Ph.D. degree from Hindustan Institute of Technology Science, Chennai. He received his Master degree in VLSI Design from Dr.M.G.R. Educational and Research Institute, Chennai and Bachelor degree under Manonmanium Sundranar University, Tirunelveli. He is having more than 15 years of teaching experience and has published 31 articles in various indexed journals and conferences. His current research interests are software defined radio, cognitive radio, FIR filter design, and 5G communication. He can be contacted at email: rajmohan.madasamy@gmail.com.

Subbiah Murugan is an Adjunct Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, TamilNadu, India. He published his research articles in many international and national conferences and journals. His research areas include network security and machine learning. He can be contacted at smuresjur@gmail.com.

Narayanasamy Aswin Vignesh received UG Degree in A.V.V.M Sri Pushpam College (Autonomous), PG Degree in A.V.V.M Sri Pushpam College (Autonomous), Ph.D. in Jamal Mohamed College (Autonomous), Tiruchirappalli. Under Bhrathidasan University. Now, his working as a Guest Lecturer in Department of Computer Science in Government Arts and Science College, Thirukkattupalli. He has fourteen years of experience as an Assistant Professor. My specialization is data mining and big data in computer science. He can be contacted at email: aswin.pn@gmail.com.