International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission

T. Shanthi[1], M. Sahaya Sheela[2], J. J. Jayakanth[3], M. Karpagam[4],G. Srividhya[5], T. V. S. Gowtham Prasad[6]

Submitted:26/04/2023 **Revised:**27/06/2023 **Accepted:**07/07/2023

Abstract: The Internet of Things relies on wireless sensor networks (WSNs) to gather data and transmit it to centralized databases. Most of the power used by these sensors goes toward detecting or collecting and delivering the data because they run on batteries and have limited resources. Wormhole attacks are the most devastating threat that may befall these networks, making data security a top priority throughout data exchange. The communication, security, and performance of the network are severely compromised by these assaults since they are launched without first gathering essential information. Due to limited resources in sensors, it is more difficult to prevent in an IoT-based network environment. If an unwanted node is present in the system, it will slow everything down. In order to keep malicious software and hacking attempts out of WSNs, secure routing protocols must be implemented. Since security is paramount in WSN, several different safe routing protocols have been created to enhance the efficiency with which packets may be sent. Using the multipath link routing protocol along with improved blow fish model (MLRP-IBFM), our proposed strategy creates a safe path for private IoT data to travel between sensor nodes with varying levels of available power. Data transfer rates, power consumption, latency from beginning to finish, system lifespan, and information storage space are only few of the performance metrics where this routing protocol excels when compared to two other current routing protocols.

Keywords: *Internet of Things, Security, Wireless Sensor Networks, Routing Protocols, Safe Path.*

1.Introduction

Years ago, the term "internet of things" (IoT) was used [1] to describe a network of intelligent, networked gadgets. IoT devices have sensors, a processor, memory, and wifi connections that facilitate conversation with one another due to the rising need for data transfer and computing [2]. The Internet of Things (IoT) is a sophisticated network comprised of disparate sensors, endpoint devices, and control infrastructures [3]. Using the capabilities of wireless networks, IoT's primary goal is to collect data from authorized users. Management and the improvement of conventional public services like transportation and parking, lighting, public space surveillance and maintenance, historical and cultural artifact conservation, trash collection, public health care, and educational institutions could all be aided by an urban IoT. As a result, the public can gain an improved awareness of the state of their town and their standard of life thanks to the urban IoT's greater exposure to all kinds of data that will be saved to the cloud or assembled by a center for data. Local governments and administrations find the IoT paradigm's potential application to the smart city appealing and expanding; nonetheless, widespread adoption of IoT technology will take some time.

To filter out lighting, WSN [4] offers essential connectivity in the battle regions or defense-oriented programs, whether the enemy is sending electromagnetic signals, toxic or biological vapors, or if they are breaching a border. When nodes are in motion, it becomes difficult to provide security in WSNs while also optimizing energy consumption. Due to the fact that the most important component in security is controlling the localization of sensor nodes and mobile enemies. The goals and motivations of those who launch assaults can vary widely, leading to a wide range of possible outcomes [5]. Any wireless sensor node can function as an adversary if it has the necessary hardware and software to sense the wireless channel and steal the sent data. As a result, the functionality, efficiency, and service of the sensor nodes might suffer if an attacker is able to successfully modify what they normally do through hacking in order to disrupt the wireless sensor network's operations [6]. Due to the transparency of IoT, the information gathered by sensor nodes may be at risk. To ensure its legitimacy and use it for future decision making, it is necessary to perform a security check on the data acquired from the sensor nodes in WSN. Denial of service (DoS) prevents authorized users from accessing the system as a result of unauthorized requests for association with the system. The conversation between the sender and the receiver is vulnerable to eavesdropping. This is, thus, an assault on privacy;

Department of Electronics and Communication Engineering, Madanapalle Institute of Technology and Science, Angallu Madanapalle-517325 Andhra Pradesh, Email: vaishu.shan@gmail.com
[2]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology Chennai-600062, Tamil Nadu. Email: hisheelu@gmail.com
[3]Department of Computational Intelligence, SRM Institute of Science & Technology, Kattankulathur, Chennai, India-603 203 ,
Email: jj.jayakanth @gmail.com
[4]Assistant Professor, Department of Computational Intelligence, Faculty of Engineering and Technology, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, 603203, Chennai, Tamil Nadu, India.
Email: karpsit@gmail.com
[5]Department of Electronics and Communication Engineering, Panimalar engineering college, Poonamallee, Chennai - 600 123.
Email: srividhyakrishiv@gmail.com
[6]Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College (Autonomous), Tirupati, Chittoor (District), Andhra Pradesh-517102, Email: tvsgowtham@gmail.com
*Corresponding Author: M. Sahaya Sheela**

In Man in the middle a client acting as a delegate can gain access to one side's key and carry on conversations as if they were the authorized party. The Saturation is an invader makes extensive use of the authorized party's resources in an effort to exploit its physical and mental strengths. An intruder disguises themselves as a legitimate customer by adopting a false identity. This means it can dismantle IoT's infrastructure, and

If you alter the input, the result will be different. This approach is able to detect the key by monitoring for software updates.

Thangaramya et al. [7] have dedicated their efforts to improving the network conceptual designs, which led to effective routing decisions in 2019. Analysis was eventually performed, and the results established the success of the suggested method with regard to delay, longevity, and PDR. Deebak and Fadi [8] developed a new safe routing protocol in 2020 using the TF symmetric key architecture to identify and sidestep problems plaguing the wider WSN. The multipath delivery was finally guaranteed when the results achieved with the accepted model showed its advantage over alternative models. Effective routing in IoT networks was achieved in 2020 thanks to a novel technique dubbed SARP created by Mauro et al. [9]. The implemented strategy also reduced the delay ratio, overhead, and energy consumption, which contributed to the system's improved efficiency. To protect the Internet of Things (IoT) from cyberattacks, David et al. [10] presented the SecTrust-RPL routing architecture in 2019. The implemented scheme's improvement in terms of robustness and efficiency was also calculated and confirmed.

Waqas et al. [11] introduced an innovative QCM2R method for WSNs in 2020. Thus, implementations were done to test the improvement of the "QCM2R protocol," showing that the accepted model is preferable in terms of reliability, throughput, latency, and lifespan. To accommodate a wide range of use cases in IoT networks, Badis et al. [12] established a "protected trust management and multipath routing architecture" in the year 2020. Last but not least, the simulated results established the superiority of the provided strategy in terms of scalability, effectiveness, and safety. Using the Crow Whale-ETR and an objective function designed to take into account the nodes' energy and trustworthiness, Shende, D.K., and Sonavane [39] developed an efficient multicast routing system in 2020.

To solve the WSN energy problem, Rahim [13] proposed in 2020 using a Taylor-based Grey Wolf Optimization algorithm (TGWOA). In order to achieve multi-hop routing, the introduced approach combines the Taylor series with Grey Wolf Optimization.

For congestion detection in networks, Yu et al. [14] combined DSR routing with ant-colony optimization to steady the signaling power. The original concept for blocking the high-mobility node to find other paths was projected by Swidana et al. [15]. For better ad hoc on-demand routing [17], Khalaf et al. [16] presented a two-probability model to increase the speed of perception. To address the routing issue inherent in multipath routing networks, Brahmbhatt et al. [1]8 introduced a trustworthy routing that choose a strong node to maintain constant signal strength. Physical layer real-time packet categorization has been the focus of research by Alejandro Proano and LoukasLazos [19].

Although Gope et al. [20] presented a lightweight two-factor protocol for WSN, Luo et al. [21] identified various flaws in this approach and offered an alternative technique. The enhanced system is still not secure, though. After finding that the authentication and key agreement scheme proposed by Turkanovi et al. [22] for wireless sensor networks is vulnerable to identity theft and eavesdropping attacks, Banerjee et al. [23] developed a new plan that incorporates biometrics and smart cards.

In [23], Banerjee et al. claimed their approach is secure against a wide range of adversarial techniques. In this work, we show that their system has some flaws, namely that it is vulnerable to offline password guessing attacks and impersonation attacks and that it does not succeed in protecting users' privacy by maintaining their session keys' secret, separating their identities from each other, and ensuring complete forward secrecy. P. Satyanarayana et al. [24] carried out privacy preservation in MANET for IoT applications. Therefore suggested MU-HHO and MS-ASFO methods for secure communication. P. Satyanarayana et al. [25] focused on enhancing the network lifetime based on the EEACBR algorithm in WSN. However, the offered method has a challenging process for prolonging the network lifetime and energy efficiency. D. Hemanand et al. [26] concentrated on intrusion detection based on CSGO and LSVM techniques using NSL-KDD and UNSW-NB15 datasets. Nevertheless, the main problems are extended latency, decreased performance, ineffective processing of large dimensional datasets and high false classification results to predict IDS in WSN.

2.Materials and method

Problem formulation

The problem of secure routing in WSNs aims to establish a safe path for private IoT data transmission between sensor nodes while mitigating the risks associated with wormhole attacks and ensuring data security. The objective is to design a routing protocol that exploits the efficiency of data exchange while considering the limited resources, such as power and computational competences, of the sensor nodes.

Let $G = (V, E)$ represent the wireless sensor network, where V is the set of sensor nodes and E is the set of communication links among nodes. The goal is to find a secure routing protocol R that minimizes the impact of malicious nodes and optimizes performance metrics while ensuring the safe transmission of private IoT data.

$$R: G \rightarrow P \quad (1)$$

where P represents the set of all possible secure routing protocols. The objective function is formulated as follows:

$$\text{minimize } \Phi(R) \quad (2)$$

subject to the Security Constraints, such as Minimization of wormhole attacks

$$\Psi(R) \leq \Psi_{max} \quad (3)$$

Prevention of malicious software and hacking attempts:

$$\Omega(R) \leq \Omega_{max} \quad (4)$$

Performance Metrics, throughput refers to the rate at which data is successfully communicated from source to terminus in the network. Maximizing throughput aims to achieve high data transmission rates, ensuring efficient utilization of the available bandwidth. The performance metric Θ_{min} represents the minimum acceptable throughput threshold that needs to be met by the routing protocol R.

$$\Theta(R) \geq \Theta_{min} \quad (5)$$

Energy efficiency focuses on minimizing the power consumption of sensor nodes during data transmission. Optimizing energy efficiency ensures that the routing protocol minimizes energy expenditure, allowing the sensor nodes to operate for extended

periods without requiring frequent battery replacements or recharging. Λ_{min} represents the minimum acceptable energy efficiency level that the routing protocol R should achieve.

$$\Lambda(R) \geq \Lambda_{min} \quad (6)$$

Latency refers to the time delay experienced in transmitting data. Minimizing end-to-end latency aims to reduce the overall delay, allowing real-time or near real-time data transmission. Σ_{max} represents the maximum acceptable latency threshold that needs to be maintained by the routing protocol R. End-to-end latency minimization:

$$\Sigma(R) \leq \Sigma_{max} \quad (7)$$

Network longevity refers to the capability of the system to sustain its operations over an extended period without significant disruptions or failures. Enhancing network longevity involves minimizing the depletion of network resources, such as power and memory, and ensuring the network's stability and resilience. Δ_{min} represents the minimum required network longevity level that the routing protocol R should achieve.

$$\Delta(R) \geq \Delta_{min} \quad (8)$$

Data storage capacity utilization focuses on efficiently utilizing the available storage resources in the system. It objects to maximize the usage of storage capacity for storing IoT data while minimizing wastage or congestion. Φ_{min} represents the minimum acceptable level of data storage capacity utilization that should be achieved by the routing protocol R.

$$\Phi(R) \geq \Phi_{min} \quad (9)$$

By considering these performance metrics, the routing protocol can be evaluated and compared based on its ability to deliver high throughput, optimize energy consumption, minimize latency, enhance network longevity, and effectively utilize data storage capacity. The problem is to find the routing protocol R^* that optimizes the objective function while satisfying the security constraints and performance metrics:

$$R^* = \arg\min \Phi(R) \quad (10)$$

Multipath Link Routing Protocol (MLRP)

The Multipath Link Routing Protocol (MLRP) is a routing protocol intended for wireless sensor networks (WSNs) to establish multiple paths between sensor nodes for efficient and reliable data transmission. MLRP aims to progress system performance, resilience, and energy productivity by utilizing multiple paths simultaneously. The Fig.1. Overall structure of Secure Routing in WSN represents the visual depiction of the architecture or conceptual framework of the secure routing solution designed for WSNs.

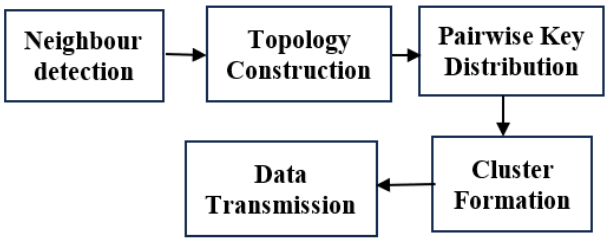

Fig.1. Overall structure of Secure Routing in Wireless Sensor Networks

In neighbor detection stage, sensor nodes detect and identify their neighboring nodes within their communication range. The nodes exchange control packets to establish neighbor relationships, enabling them to communicate and form a network topology. After neighbor detection, the sensor nodes construct the network topology. The topology represents the structure of the network, including the relationships and connectivity between sensor nodes. MLRP constructs multiple paths between sensor nodes to provide redundancy and fault tolerance. To ensure secure communication, MLRP distributes pairwise keys between neighboring nodes. Pairwise keys are shared only between the nodes that require direct communication. This step enables encryption and decryption of data transmitted between the nodes, ensuring confidentiality and data integrity.

MLRP forms clusters within the network to organize and manage the communication between sensor nodes effectively. Cluster heads are elected based on predefined criteria such as node capabilities or energy levels. The cluster heads coordinate data transmission within their respective clusters, optimizing the use of available paths. Once the network is established and clusters are formed, MLRP facilitates data transmission between sensor nodes. The protocol leverages multiple paths available within the network, enabling parallel data transmission along different routes. This multipath approach enhances throughput, reduces congestion, and improves overall network performance.

The recital of the MLRP routing protocol can be assessed using various metrics. One such metric is the end-to-end delay (D), which represents the time engaged for data to be communicated from the source node to the destination node. The end-to-end delay can be calculated using the following equation:

$$D = \Sigma (D_i) \quad (11)$$

where D_i represents the delay experienced along each path among the foundation and destination nodes. MLRP aims to minimize the end-to-end delay by utilizing multiple paths and distributing data traffic effectively. Additionally, MLRP can optimize other efficiency indicators including battery life, uptime, and packet delivery rate. The specific equations for these metrics may vary depending on the evaluation criteria and objectives set for the WSN deployment.

Improved Blow Fish Model (IBFM)

Blowfish is a symmetric key block cipher known for its security and efficiency in cryptographic operations. While the Blowfish algorithm itself is considered secure, there are several enhancements and improvements that can be made to enhance its secure transmission capabilities. Here is an algorithm of an improved Blowfish model for secure transmission

Algorithm 1. ImprovedBlowfish Algorithm

```
Function ImprovedBlowfishEncrypt(plaintext, key):
    Initialize the Blowfish cipher with the given key
    Split the plaintext into blocks of fixed size (e.g., 64 bits)
    for each block in plaintext:
        Apply a padding scheme if necessary
        Initialize the left and right halves of the block
        Apply a number of encryption rounds
        while keeping track of the round keys:
            Perform a Feistel round using the Blowfish F-function
            Update the left and right halves based
        Swap the left and right halves
        Apply a final Feistel round without XORing
        Combine the left and right halves
    Return the encrypted ciphertext
Function ImprovedBlowfishDecrypt(ciphertext, key):
    Initialize the Blowfish cipher with the given key
    Split the ciphertext into blocks of fixed size (e.g., 64 bits)
    for each block in ciphertext:
        Initialize the left and right halves of the block
        Apply a number of decryption rounds (e.g., 16 rounds)
        while keeping track of the round keys:
            Perform a Feistel round using the Blowfish F-function
            Update the left and right halves based on round key
```

```
        Swap the left and right halves
        Apply a final Feistel round without XORing
        Combine the left and right halves
        Remove any padding from the decrypted block
    Return the decrypted plaintext
Function Main ():
        ImprovedBlowfishEncrypt(plaintext, key)
       ImprovedBlowfishDecrypt(encryptedText, key)
```

3. Performance Evaluation

Network Size column indicates the number of sensor nodes present in the system. In the given example, the network sizes range from 10 to 50 nodes. The throughput column represents the rate of data transmission in the network, restrained in megabits per second (Mbps). Higher throughput values indicate a higher amount of data being successfully transmitted within a given time frame.

The amount of time, in milliseconds (ms), that it takes for data to travel from its origination point to its final location is displayed in the End-to-End Delay (ms) field. Lower values indicate reduced latency and faster data delivery. The energy efficiency column measures the amount of energy consumed per bit of data transmitted in the network, represented in joules per bit (J/bit). Lower values indicate more energy-efficient data transmission, resulting in longer battery life for the sensor nodes.

The table 1 represents different performance metrics for a wireless sensor network (WSN) at various network sizes. Each row in the table corresponds to a specific network size, and the columns represent different performance metrics measured in the network.

Table 1 Network size and throughput comparison

Network Size	Throughput (Mbps)	End-to-End Delay (ms)	Energy Efficiency (J/bit)	Network Lifetime (hours)	Data Storage Capacity (GB)
10	50	5	0.2	100	10
20	75	8	0.18	150	15
30	90	10	0.15	200	20
40	100	12	0.14	250	25
50	110	15	0.12	300	30

Network Lifetime (hours) indicates the estimated duration for which the network can operate without requiring battery replacements or recharging. It represents the total time in hours that the network can remain functional before the sensor nodes' energy resources are depleted. The data storage capacity column represents the amount of storage available in the network for storing collected data, measured in gigabytes (GB). It indicates the maximum capacity for data storage within the network.

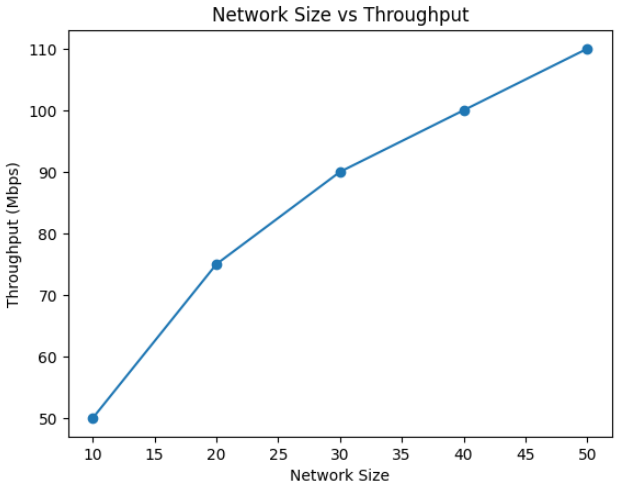

Fig.2. Network Size vs Throughput

The "Network Size" column in the fig.2 represents the number of sensor nodes present in the wireless sensor network (WSN), ranging from 10 to 50 nodes. The "Throughput" column corresponds to the throughput values measured in megabits per second (Mbps) for each network size. The specific throughput values provided in the table are 50, 75, 90, 100, and 110 Mbps. As the network size increases from 10 to 50 nodes, the throughput values also increase incrementally from 50 Mbps to 110 Mbps. This trend suggests that larger network sizes tend to have higher throughput capacities, enabling the transmission of more data within a given time period

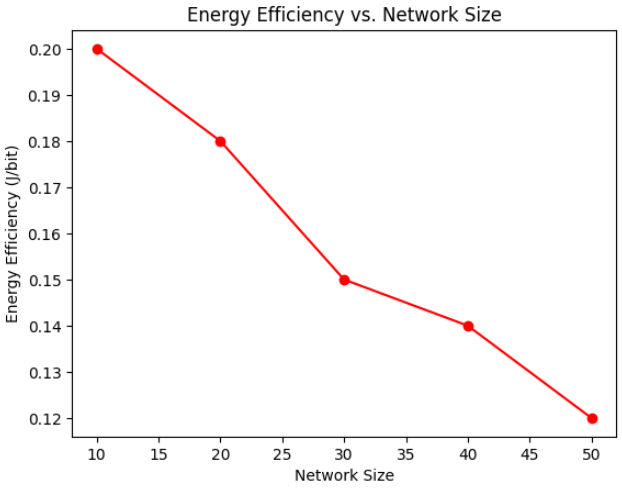

Fig.3. Network size vs Energy efficiency

The network size from fig.3 in the given range of 10 to 50 nodes is being compared against different energy efficiency values of 0.2, 0.18, 0.15, 0.14, and 0.12. Energy efficiency represents the amount of energy consumed per bit of data transmitted in the network, measured in joules per bit (J/bit).

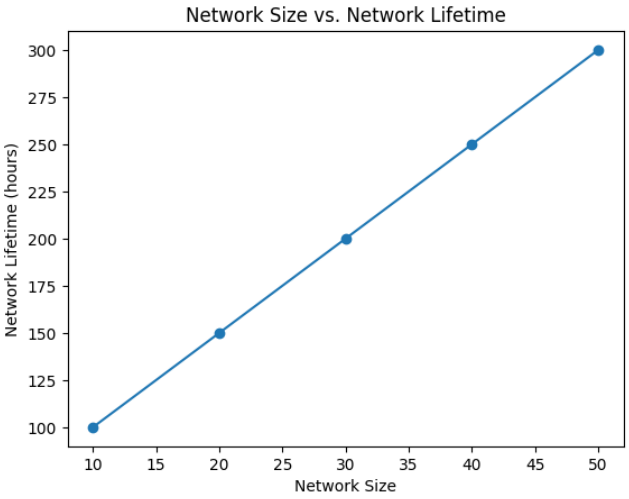

Fig.4. Network Size vs Network Lifetime

The "Network Size" column in the fig.4 represents the number of sensor nodes present in the wireless sensor network (WSN), ranging from 10 to 50 nodes. The corresponding values in the "Network Lifetime" column represent the estimated duration for which the network can operate before the sensor nodes' energy resources are depleted.

4. Conclusion

In conclusion, WSNs play a crucial role in enabling the IoT by collecting and transmitting data to centralized databases. However, the limited resources and battery-powered nature of these sensors pose challenges in terms of power consumption and data security. Among the various threats that WSNs face, wormhole attacks are particularly devastating as they compromise communication, security, and overall network performance. To address these challenges and ensure secure data exchange, it is essential to prioritize data security in WSNs. Secure routing protocols are crucial in preventing malicious software and hacking attempts from compromising the network. Several safe routing protocols have been developed to enhance the efficiency of data transmission in WSNs. In this context, our proposed strategy combines the multipath link routing protocol (MLRP) with an improved Blowfish model (IBFM) to create a secure path for private IoT data transmission between sensor nodes. The MLRP-IBFM strategy considers varying levels of available power and excels in various performance metrics. By leveraging the strengths of MLRP-IBFM, WSNs can mitigate the impact of wormhole attacks, enhance data security, and optimize network performance. This integrated approach addresses the challenges posed by limited sensor resources and provides a robust solution for protected data transmission in IoT-based network environments. However, it is important to acknowledge that the ever-evolving landscape of IoT security demands continuous research and advancements in secure routing protocols. Ongoing efforts to develop and improve upon existing protocols will be crucial to staying ahead of emerging threats and ensuring the long-term security and efficiency of WSNs in the IoT ecosystem.

References

[1] Silva JS, Zhang P, Pering T, Boavida F, Hara T, Liebau NC. People-centric internet of things. IEEE Commun Mag. 2017;55(2):18-19.

[2] Verikoukis C, Minerva R, Guizani M, Datta SK, Chen Y, Muller HA. Internet of things: part 2. IEEE Commun Mag. 2017;55(2):114-115.

[3] Garcia-de-Prado A, Ortiz G, Boubeta-Puig J. COLLECT: COLLaborativE ConText-aware service oriented architecture for intelligent decision-making in the internet of things. Expert Syst Appli. 2017;85:231-248.

[4] I.F. Akyildiz et al., "Wireless sensor networks: A survey", Computer Networks 38 (4) (2002) 393–422.

[5] Yun Zhou et al., "Securing Wireless Sensor Networks: A survey", IEEE Communication Surveys, Volume 10, No.3, 2008.

[6] S.H. Jokhio et al., "Node capture attack detection and defence in wireless sensor networks, Published in IET Wireless Sensor Systems", 8 August 2011.

[7] K. Thangaramya, K. Kulothungan, R. Logambigai, M. Selvi, S. Ganapathy, and A. Kannan, ''Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT,'' Comput. Netw., vol. 151, pp. 211–223, Mar. 2019

[8] F. Al-Turjman, ''A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks,'' Ad Hoc Netw., vol. 97, Feb. 2020, Art. no. 102022.

[9] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, ''Attestation-enabled secure and scalable routing protocol for IoT networks,'' Ad Hoc Netw., vol. 98, Mar. 2020, Art. no. 102054.

[10] D. Airehrour, J. A. Gutierrez, and S. K. Ray, ''Sectrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,'' Future Gener. Comput. Syst., vol. 93, pp. 860–876, Apr. 2019.

[11] W. Rehan, S. Fischer, M. Rehan, Y. Mawad, and S. Saleem, ''QCM2R: A QoS-aware cross-layered multichannel multisink routing protocol for stream based wireless sensor networks,'' J. Netw. Comput. Appl., vol. 156, Apr. 2020, Art. no. 102552.

[12] B. Hammi, S. Zeadally, H. Labiod, R. Khatoun, Y. Begriche, and L. Khoukhi, ''A secure multipath reactive protocol for routing in IoT and HANETs,'' Ad Hoc Netw., vol. 103, Jun. 2020, Art. no. 102118

[13] R. Rahim, S. Murugan, S. Priya, S. Magesh, and R. Manikandan, ''Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol,'' Int. J. Comput. Netw. Appl., vol. 7, no. 4, p. 93, Aug. 2020.

[14] Yu, Y.; Ru, L.; Chi, W.; Liu, Y.; Yu, Q.; Fang, K. Ant colony optimization-based polymorphism aware routing algorithm for ad hoc UAV network. Multimed. Tools Appl. 2016, 75, 14451– 14476.

[15] Swidana, A.; Abdelghanya, H.; Saifana, R.; Zilic, Z. Mobility and Direction Aware Ad-hoc on Demand Distance Vector Routing Protocol. Procedia Comput. Sci. 2016, 94, 49–56.

[16] Khalaf, M.; Al-Dubai, Y.; Min, G. New efficient velocity-aware probabilistic route discovery schemes for high mobility Ad hoc networks. J. Comput. Syst. Sci. 2015, 81, 97–109.

[17] Perkins, C.E.; Royer, E.M. Ad-hoc on-demand distance vector routing. In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, 25–26 February 1999.

[18] Brahmbhatt, S.; Kulshrestha, A.; Singal, G. SSLSM: Signal Strength Based Link Stability Estimation in MANETs. In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks, Jabalpur, India, 12–14 December 2015.

[19] Alejandro Proano and LoukasLazos, "Packet Hiding method for Selective Jamming Attacks", IEEE Transactions on Dependable and Secure Computing", Volume 1, January/February 2012.

[20] P. Gope, T. Hwang, A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans. Industr. Electron. 63(11), 7124–7132 (2016)

[21] H. Luo, G. Wen, J. Su, Lightweight three factor scheme for real-time data access in wireless sensor networks. Wirel. Netw. 26(2), 955–970 (2020)

[22] M. Turkanović, B. Brumen, M. Hölbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Netw. 20, 96–112 (2014)

[23] S. Banerjee, C. Chunka, S. Sen, R.S. Goswami, An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wirel. Pers. Commun. 107, 1–28 (2019)

[24] Satyanarayana, P., Diwakar, G., Subbayamma, B. V., Phani, N. V., Kumar, S., Arun, M., & Gopalakrishnan, S. Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications, Computer Communications Volume 198,Issue, C15(January) 2023pp, 262–281.

[25] P. Satyanarayana, U. D. Yalavarthi, Y. S. S. Sriramam, M. Arun, V. G. Krishnan and S. Gopalakrishnan, "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR)Algorithm to Improve Network Lifetime in WSN's," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6.

[26] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293.

[27] Taylor, D., Roberts, R., Rodriguez, A., González, M., & Pérez, L. Efficient Course Scheduling in Engineering Education using Machine Learning. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/121

[28] Anand, R., Khan, B., Nassa, V. K., Pandey, D., Dhabliya, D., Pandey, B. K., & Dadheech, P. (2023). Hybrid convolutional neural network (CNN) for kennedy space center hyperspectral image. Aerospace Systems, 6(1), 71-78. doi:10.1007/s42401-022-00168-4