A Secure Framework based on Hybrid Cryptographic Scheme and Trusted Routing to Enhance the QoS of a WSN

Mohammad Sirajuddin
Department of I.T, Kallam Haranadhareddy Institute of Technology, Guntur, Andhra Pradesh, India
siraj538@gmail.com (corresponding author)

Chittibabu Ravela
Department of C.S.E, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
ravelalikes@kluniversity.in

S. Rama Krishna
Department of C.S.E, GITAM (Deemed to be University), Hyderabad, Telangana, India
rsankara@gitam.edu

Shaik Khaleel Ahamed
Department of C.S.E, Methodist College of Engineering and Technolgoy, Hyderabad, Telangana, India
khaleelska@gmail.com

S. Karimulla Basha
Department of C.S.E, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, Andhra Pradesh, India
kareeem768@gmail.com

N. Md. Jubair Basha
Department of I.T, Kallam Haranadhareddy Institute of Technology, Andhra Pradesh, India
jubairbasha@gmail.com

Received: 24 April 2024 | Revised: 21 May 2024 and 22 May2024 | Accepted: 25 May 2024

ABSTRACT

Achieving Quality of Service (QoS) in Wireless Sensor Networks (WSNs) is challenging, due to their dynamic nature, and many parameters must be taken into account. The main objective of this work is to propose a hybrid cryptographic system with trust-based routing to improve the QoS. This study considers ways to improve QoS while maintaining security. To enhance the performance of the WSN, a framework that uses a hybrid cryptographic system based on a logistic map and the trust-based routing protocol CTBSR that can recognize and counteract a variety of security threats is presented. The findings of this study support the claim that the proposed framework ensures better security than the existing approaches in terms of confidentiality, integrity, and authentication. The performance of the framework introduced is evaluated by employing the NS2 simulator.

Keywords-cryptographic scheme; trusted routing; energy consumption reduction; QoS; WSN

I. INTRODUCTION

A Wireless Sensor Network (WSN) is an infrastructure-less consortium of interconnected sensor nodes. WSNs are dynamic in nature and due to this feature they can be deployed in a diverse range of applications. WSNs are employed to collect, disseminate, and analyze data. They have certain characteristics like versatile topology, self-organization, and multihop communication that make them vulnerable to various security threats. The presence of security attacks degrades the performance of the WSNs. Due to the open communication medium of WSNs, any node can join the network and get involved in data transmission. This feature attracts attackers to launch their attacks through malicious nodes. Such a behavior is not acceptable for applications where sensitive data are captured and transmitted. The presence of malicious nodes degrades the performance of the network because sometimes they may discard the data transmitted by legitimate nodes. So it becomes a prominent task to identify malicious nodes and mitigate them from WSN.

In this research, a hybrid cryptographic method is proposed that consumes less power and ensures secure data transmission. Optimizing the power of sensor nodes is essential in enhancing the lifetime of the network. A master node-based trusted routing protocol is also introduced to ensure secure routing and enhance the QoS of the WSN. Both approaches collectively improve performance by reducing the power consumption of sensor nodes. The main contributions of the current paper are:

- Analyzing existing cryptographic schemes and trust-based routing protocols to determine their limitations.
- Designing a lightweight cryptographic scheme using the logistic map approach.
- Enhancing a trust-based routing protocol that incorporates a lightweight cryptographic scheme to ensure secure communication in WSNs.
- Evaluating the performance of the proposed framework and conducting a comparative study of the existing techniques alongside the proposed framework by considering various performance metrics.

Every sensor node should capture and transmit the sensed data to the sink node by applying any routing algorithm recommended for WSNs [1]. To ensure secure data exchange, the routing algorithm shall be incorporated with security schemes. This inclusion of a security scheme in routing will increase the battery power consummation of the node. To optimize the battery consumption, it is necessary to implement routing algorithms and security schemes that use light weight computation. Hence, it is crucial for the energy-intensive tasks to be performed with considerable caution. One of the main goals of a routing algorithm in WSNs is to reduce latency while increasing energy efficiency and network longevity. When combined these components increase the routing mechanism's effectiveness and functionality [2]. WSNs are susceptible to various security threats and demand powerful security measures. Authors in [3] recommended the use of ECC to secure WSN from security threats. Authors in [4] utilized TinyMD5 algorithm to convert sense data into one-way hash value. Authors in [5] deployed TASRP multifactor routing protocol to improve the performance of the WSN. This protocol uses trust scores, residual energy, and path length to generate reliable routing paths between trusted sensor nodes. Authors in [6] designed the DTC-BR routing protocol to improve the performance of MWSN. DTC-BR is a cluster-based routing protocol that uses virtual MCZ.

Public Key Infrastructure (PKI) is a popular identity authentication technique propounded for WSN-based applications. This strategy, however, has some flaws, such as a single point of failure and difficult key management. In order to make message signing and signature verification in wireless networks simpler, some studies concentrated on identity-based batch verification algorithms. Several researchers focused on boosting the effectiveness of batch verification approaches rather than enhancing the capacity to recognize fraudulent signatures [7-11]. Such batch verification techniques affect performance. Many researchers have proposed numerous cryptographic techniques to ensure secure communication in WSNs. However, there has not been much progress made in developing cryptographic algorithms that are more energy-efficient and prolong network lifetime. Several researchers are expanding WSNs to support scattered healthcare applications by integrating cutting-edge technologies including cloud computing, fog computing, and big data analytics [11, 12]. It is critical to lower the energy consumption of wireless nodes or sensors in order to increase the lifespan of the network. Energy-efficient techniques must be utilized to manage network life. Authors in [13] proposed the WOA-SA technique to cut down the wireless sensor's energy usage. The new Trust-Based Secure Intelligent Opportunistic Routing Protocol (TBSIOP) was proposed in [14], without emphasizing other QoS metrics as CIA characteristics. It solely takes secure routing and energy consumption into account and operates in multiple phases, which demand high computational complexity. Authors in [15] presented three main aspects that are clustering, duty cycling, and routing. Still, this approach leads to computation overhead, while the CIA triad is not justified in this method. Authors in [16] introduced a model that describes the behavior of sensor nodes and uses secure routing based on node information, leading, too, to memory overhead. Authors in [17] proposed NDSC-based PSO to maximize the lifespan of the WSNs. Authors in [18] presented CR-WSN clustering approach to enhance the performance of the WSN. Authors in [19] proposed the CSCO algorithm for optimal CH selection to improve the communication in WSNs.

It is difficult to achieve QoS in WSNs. Multiple factors must be taken into account in order to attain QoS. This study's major goal is to provide a hybrid cryptographic system with trust-based routing to improve the WSN's QoS.

II. THE PROPOSED METHOD

This section enlightens the functionality of the proposed system. To improve the QoS of the WSN, the following factors were considered:

- Lightweight cryptographic approach for secure data transmission to minimize power consumption: It is necessary to employ a strong cryptographic approach to ascertain secure data transmission. The cryptographic scheme will operate by consuming less battery power from a node. So, lightweight computations must be included in the cryptographic scheme.
- Detection of malicious nodes: The presence of malicious nodes may degrade the throughput of the network, because malicious nodes may drop the packets intentionally without forwarding them to the sink node.

- Trust-based routing to reduce packet dropping: Trust-based routing was considered. The trust value of every node is assed and monitored.

A. Network Model

In the proposed network model, one node is designated as the Master Node (MN). This node is included in the network to provide secure communication in the latter. The MN is responsible for generating keys for every sensor node and monitors the behavior of nodes to detect malicious activity. All sensor nodes must be registered with the MN to be involved in the communication. After successful registration with the MN, every sensor node is assigned with a unique id and a shared Session Key (SK). The shared session key is generated by the MN for every sensor node using logistic map based cryptographic approach and it is encrypted by deploying the public key of the sensor node. Every sensor node makes a public and private key pair by applying the RSA algorithm. The following steps are performed.

B. Logistic Map based Hybrid Cryptographic Algorithm

1. Every sensor node makes a pair of public and private keys (PU_n , PR_n) by using the RSA algorithm, where PU_n = public key of a node, PR_n = private key of a node.
2. Each sensor node registers with the MN. After registration, the MN generates a unique ID and assigns it to the sensor node. This unique ID appended with the hash of the ID is sent to the sensor node. SHA algorithm is utilized as the hashing function.
3. Prior to sending data to the MN, the sensor node requests a session key by sending its ID along with its hash to the MN.
4. The MN verifies the identity of the sensor node and follows a logistic map-based approach to generate a session key. The process is illustrated as:

   a. The MN uses:

$$Z_{n+1} = rZ_n (1 - Z_n) \quad (1)$$

where r is a control parameter whose value ranges from 3.83 to 4.0 and $Z \in [0.0, 1.0]$.

   b. Create a series with the chosen *r* value, which is 3.99, and put the values in the array KS[].

   c. Pick one value at random from KS[] and enter it in the K1 variable.

   d. K2 = round(K1 ∗ α), where α is a constant positive integer which is generated randomly by the MN node deploying a random number generation function.

   e. Take into account a seed value for the linear feedback left shift operation. Transform the seed value into a binary sequence, and then conduct an XOR operation between the values of b_0, b_4, b_5, b_7, b_{10}, b_{12}, b_{14}, and b_{15} bits.

   f. The output of XOR is provided as a feedback. The final binary sequence is transformed into decimal value and saved in K3.

   g. Step f is again repeated by considering the binary value of K3 as the seed value to create a new sequence and store it in K4.

   h. Then, the values of K2, K3, and K4 are XORed to produce the SK.

$$SK = K2\ (XOR)\ K3\ (XOR)\ K4 \quad (2)$$

   i. The MN node encrypts a key SK before sending it to the sensor node using the sensor node's public key. The hash of SK and encrypted SK are sent to the requestor which is represented mathematically as:

$$Y = E(SK, R_{PU}) \quad (3)$$

where Y represents the encrypted session key (SK), E is defined as the encryption function with SK and the public key of the requestor (R_{PU}).

$$H(SK)\|Y \quad (4)$$

where H(SK) is the hash value of the session key generated by the MN.

   j. The sensor node utilizes its private key to perform decryption after receiving the encrypted SK. The hash value of the decrypted session key is computed and compared with the hash value received from the MN.

$$X = D(SK,RPR) \quad (5)$$

where X is the decrypted session key, D is the decryption function with SK and the private key of the requestor (R_{PR}).

5. After acquiring the SK, the sensor node may send its sensitive data by encrypting it by using SK. The following equation represents the encryption process:

$$C = E(P,SK) \quad (6)$$

where C = cipher text, E= encryption function, and P= plain text.

6. When MN receives encrypted data from a sensor node, it decrypts it by utilizing the same session key:

$$P = D(C,SK) \quad (7)$$

where P = plain text, D = decryption function, and C = cipher text.

7. The set of SKs generated by an MN is stored as a dictionary. This is mathematically expressed as:

$$D_N= \{\ H_{IDN} : SK_N) \quad (8)$$

where D_N = dictionary containing the SK of the N node and H_{IDN} = Hash(ID of sensor node), SK_N = SK of the N node.

8. The same process of key generation, encryption and decryption is performed between MN and the base station.

This algorithm employs both symmetric and asymmetric approaches for certifying secure data transmission. Furthermore, this proposed hybrid cryptographic approach consists of lightweight computations that consume less battery power. The proposed cryptographic algorithm supports the following properties

- Avalanche effect.
- Low computation time.
- Low key generation time O(n).
- Consumes less battery power.

C. *Cryptographic and Trust-Based Secure Routing (CTBSR) Algorithm*

The other part of the proposed methodology is trust-based routing. Trust-based routing allows only trusted sensor nodes to communicate. Many trust-based routing protocols have been proposed, but they have not considered cryptographic schemes for data transmission. In the introduced routing scheme, once a network is formed with the trusted nodes, data transmission between nodes is done by applying the cryptographic algorithm. It is an additional benefit, which provides confidentiality in the network. CTBR is a behavioral model for trust computation and routing in WSNs. In this algorithm, the trust value of every node is computed and propagated in the network to handle security attacks. The following parameters are used to measure the trust value of a node:

- Loyalty in forwarding the packets.
- Available battery power or energy level.
- Continuance of nodes in the network

The trust value ranges between 0.0 and 1.0. Threshold trust value is 0.7 and maximum trust value is 1.0. To measure the loyalty of node, let packet transmissions from node A to node B be considered. The loyalty can be measured as:

$$L(A, B) = \frac{\text{No.of packets forwarded sucessfully}}{\text{No.of packets received} + \text{No.of packets discarded}}$$

The energy level of a node is measured by:

$$EL = \frac{Ef(N) + Er(N) + Ec(N)}{T.E}$$

where EL is the energy level of a node, Ef(N) is the energy consumed by a node in forwarding the packets, Er(N) is the energy consumed by a node to receive the packets, and Ec(N) is the energy consumed by a node to send control packets.

Node continuance in the network is measured based on recorded timestamps. Trust value is defined as:

$$T = (L, EL, C)$$

where T is the trust value of a node, L is the loyalty, and C is the node continuance.

The trust values of the nodes are estimated and monitored to detect malicious nodes. A node that exhibits lowest trust value will be detached from the network by considering it malicious node. This information is propagated in the network so that the trusted nodes update their routing information to bypass the malicious node. One of the nodes in a network is designated as MN to monitor the entire communication in the network. A MN must have the following properties.

- High node degree: MN has the highest degree among the nodes in the network.
- Must exhibit high battery power or energy level.
- Must have higher memory than the other sensor nodes.
- Must have high trust value.
- Must be available in the network for longer duration.

An MN manages the network based on the trust value of nodes. It uses rule based inference to designate a node as legitimate or malicious. Once an MN detects a malicious behavior, that information is propagated to all the nodes in the network. This propagated information is utilized by the trusted nodes to detach the malicious node.

III. PERFORMANCE ANALYSIS

The proposed network model was simulated in NS-2. The following metrics were taken into account while assessing the performance of the proposed technique.

- Packet delivery ratio: This metric represents the proportion of successfully delivered packets to all packets received.
- Energy consumption: Is the amount of energy that a network uses to run its operations.
- Throughput: This parameter represents the rate at which data packets are sent successfully.

The simulation parameters depicted in Table I were explored in order to assess the performance of the suggested method.

TABLE I. SIMULATION PARAMETERS

Simulation Parameters(QoS)	Values
Area of deployment	500 × 500
Total number of nodes	100 (maximum)
Total number of malicious nodes	5, 10, 15, 20, 25, 30
Energy of a node	100 J
Energy threshold	70 J
Trust value	0.0 to 1.0

Table II illustrates the services provided by the proposed CTBSR algorithm. The proposed algorithm supports CIA triad. Also, the CTBSR increases the life span of the network because it uses lightweight computations that consume less battery power. Table II justifies that the proposed algorithm exhibits better security than the existing approaches to ensure QoS in a WSN.

Packet delivery ratio, energy consumption, and throughput of the proposed CTBSR along with the comparison with the existing known algorithms can be evidenced in Figures 1-3.

TABLE II. COMPARISON WITH EXISTING TECHNIQUES WITH RESPECT TO QoS

Algorithm	Confidentiality	Integrity	Authentication	Secure routing	Energy aware
TBSIOP [15]	No	No	No	Yes	Yes
E2SDRL [16]	No	No	No	Yes	Yes
IASR [17]	No	No	No	Yes	Yes
CTBSR (Proposed)	Yes	Yes	Yes	Yes	Yes

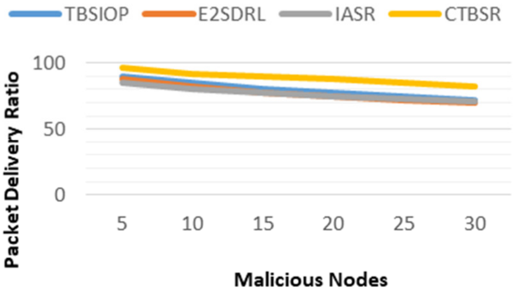

Fig. 1. Comparison of the proposed and existing aproaches regarding packet delivery ratio.

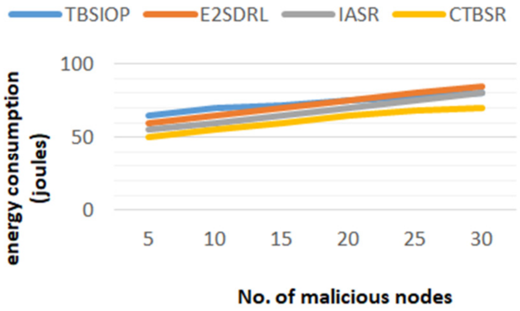

Fig. 2. Comparison of the proposed and existing aproaches regarding energy consumption.

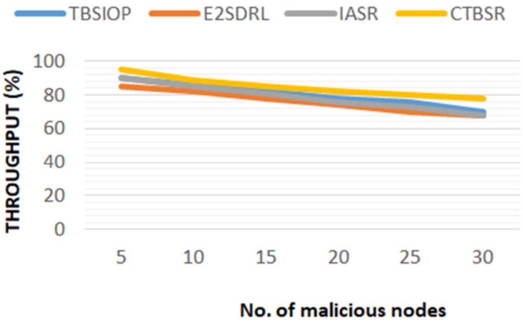

Fig. 3. Comparison of the proposed and existing aproaches regarding throughput.

The simulation results prove that the proposed CTBSR algorithm exhibits better performance in the presence of malicious nodes while consuming less battery power. This algorithm detects and mitigates various attacks like black hole attacks, wormhole attacks, and DoS attacks. Hence, the QoS of the network is increased. The proposed algorithm considers multiple factors to improve the QoS effectively.

IV. CONCLUSION

In this work, a secure framework to enhance the QoS of WSN is proposed. The proposed framework uses a logistic map-based hybrid cryptographic scheme along with the secure CTBSR algorithm to improve the performance of the WSN. The novelty of the proposed framework is that it applies a hybrid cryptographic algorithm based on logistic map function to generate session keys and pairs of public and private keys for secure information exchange. Furthermore, this hybrid cryptographic scheme is integrated with the trust-based routing protocol CTBS, which provides secure communication between trusted sensor nodes only under the supervision of the master node. Furthermore, CTBSR provides confidentiality, authentication and integrity of computed trust values. The proposed framework enhances QoS by overcoming security attacks that are launched by the malicious nodes. In the present study it was found that many existing algorithms emphasized on improving the security of WSN by either utilizing cryptographic schemes or implementing secure routing algorithms. The proposed framework deploys both a light weight cryptographic algorithm and a trust-based secure routing algorithm to ensure enhanced security in WSNs. The simulation results justify that the proposed framework certifies QoS parameters, like the packet delivery ratio, throughput, and life span of the network by consuming less battery power. In the future, more security attacks will be explored and a robust protocol to overcome these attacks by incorporating cryptographic signatures and smart intrusion detection mechanisms will be proposed.

REFERENCES

[1] K. Akkaya and M. Younis, "Energy-aware routing to a mobile gateway in wireless sensor networks," in *IEEE Global Telecommunications Conference Workshops*, Dallas, TX, USA, Dec. 2004, pp. 16–21, https://doi.org/10.1109/GLOCOMW.2004.1417542.

[2] C.-H. Cheng, H. Liang, Y.-F. Huang, and T.-Y. Wu, "Energy Efficient Block Division Methods for Data Aggregation in Wireless Sensor Networks," in *Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, Italy, Jul. 2012, pp. 454–458, https://doi.org/10.1109/IMIS.2012.22.

[3] S. Sinha and S. Aggarwal, "Cryptographic Algorithms for Security in Wireless Sensor Networks," in *3rd International Conference on Intelligent Engineering and Management*, London, United Kingdom, Apr. 2022, pp. 111–117, https://doi.org/10.1109/ICIEM54221.2022.9853139.

[4] K. Bok, Y. Lee, J. Park, and J. Yoo, "An Energy-Efficient Secure Scheme in Wireless Sensor Networks," *Journal of Sensors*, vol. 2016, no. 1, 2016, Art. no. 1321079, https://doi.org/10.1155/2016/1321079.

[5] T. Khan and K. Singh, "TASRP: a trust aware secure routing protocol for wireless sensor networks," *International Journal of Innovative Computing and Applications*, vol. 12, no. 2–3, pp. 108–122, Jan. 2021, https://doi.org/10.1504/IJICA.2021.113750.

[6] M. E. Al-Sadoon, A. Jedidi, and H. Al-Raweshidy, "Dual-Tier Cluster-Based Routing in Mobile Wireless Sensor Network for IoT Application,"

IEEE Access, vol. 11, pp. 4079–4094, 2023, https://doi.org/10.1109/ACCESS.2023.3235200.

[7] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 10, pp. 7059–7067, Oct. 2022, https://doi.org/10.1109/TII.2021.3084753.

[8] H. Xiong *et al.*, "On the Design of Blockchain-Based ECDSA With Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977–1986, May 2022, https://doi.org/10.1109/JBHI.2021.3112693.

[9] Ch. Rupa and D. J. Kumari, "Network Based Adaptation of Block Chain Technology," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9, pp. 1588–1591, Jul. 2019, https://doi.org/10.35940/ijitee.G6317.078919.

[10] V. Nikhila and Ch. Rupa, "Intensifying Multimedia Information Security Using Comprehensive Cipher," in *Innovations in Power and Advanced Computing Technologies (i-PACT)*, Vellore, India, Mar. 2019, vol. 1, pp. 1–4, https://doi.org/10.1109/i-PACT44901.2019.8960002.

[11] S. Gadamsetty, R. Ch, A. Ch, C. Iwendi, and T. R. Gadekallu, "Hash-Based Deep Learning Approach for Remote Sensing Satellite Imagery Detection," *Water*, vol. 14, no. 5, Jan. 2022, Art. no. 707, https://doi.org/10.3390/w14050707.

[12] S. Juneja, G. Dhiman, S. Kautish, W. Viriyasitavat, and K. Yadav, "A Perspective Roadmap for IoMT-Based Early Detection and Care of the Neural Disorder, Dementia," *Journal of Healthcare Engineering*, vol. 2021, no. 1, 2021, Art. no. 6712424, https://doi.org/10.1155/2021/6712424.

[13] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and Md. J. Piran, "A metaheuristic optimization approach for energy efficiency in the IoT networks," *Software: Practice and Experience*, vol. 51, no. 12, pp. 2558–2571, 2021, https://doi.org/10.1002/spe.2797.

[14] D. K. Bangotra, Y. Singh, A. Selwal, N. Kumar, and P. K. Singh, "A Trust Based Secure Intelligent Opportunistic Routing Protocol for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 127, no. 2, pp. 1045–1066, Nov. 2022, https://doi.org/10.1007/s11277-021-08564-3.

[15] R. Sinde, F. Begum, K. Njau, and S. Kaijage, "Refining Network Lifetime of Wireless Sensor Network Using Energy-Efficient Clustering and DRL-Based Sleep Scheduling," *Sensors*, vol. 20, no. 5, Jan. 2020, Art. no. 1540, https://doi.org/10.3390/s20051540.

[16] Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, "Information-Aware Secure Routing in Wireless Sensor Networks," *Sensors*, vol. 20, no. 1, Jan. 2020, Art. no. 165, https://doi.org/10.3390/s20010165.

[17] S. Kamel, A. A. Qahtani, and A. S. M. Al-Shahrani, "Particle Swarm Optimization for Wireless Sensor Network Lifespan Maximization," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13665–13670, Apr. 2024, https://doi.org/10.48084/etasr.6752.

[18] S. Panbude, B. Iyer, A. B. Nandgaonkar, and P. S. Deshpande, "DFPC: Dynamic Fuzzy-based Primary User Aware clustering for Cognitive Radio Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12058–12067, Dec. 2023, https://doi.org/10.48084/etasr.6279.

[19] S. Panbude, P. Deshpande, B. Iyer, and A. B. Nandgaonkar, "Enhancing Cognitive Radio WSN Communication through Cluster Head Selection Technique," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13347–13351, Apr. 2024, https://doi.org/10.48084/etasr.6803.