An Integrated Channel Coding and Cryptography Framework for Secure and Energy-Efficient Wireless Energy Data Transmission

Yan Zheng, Xingbo Liu, Lei Ye, Mingjun Yu, Yi Wen
Hubei Engineering Research Center for Intelligent Digital Technology in New Power System（Hubei Central China Technology Development of Electric Power Co., Ltd）Hubei Whhan 430061 China
E-mail: zhengyan202405@163.com
*Corresponding author

Keywords: wireless energy data transmission, channel coding algorithm, information security, wireless sensor networks, encryption and decryption

Received: August 4, 2025

This paper proposes a secure and energy-efficient wireless energy data transmission framework that integrates channel coding algorithms with cryptographic techniques. The framework employs LDPC codes, Turbo codes, and polar codes for channel coding, combined with AES, RSA, ECC, PRESENT, and SIMON cryptographic algorithms to address interference, information monitoring, and energy constraints in wireless environments. A dynamic power control strategy based on a greedy algorithm and a channel adaptive coding scheme are designed to optimize energy consumption and transmission reliability. Experiments were conducted using the NS3 simulation platform (with 50 nodes in a grid topology, simulated over 1000 seconds) and a small-scale field test. Key parameters included noise levels set at -90dBm to -60dBm, packet sizes of 512 bytes (AES/RSA) and 256 bytes (PRESENT/SIMON), and initial node energy levels of 1000mJ. Results show that compared with conventional algorithms, the proposed framework reduces the bit error rate by 15.3% (baseline: traditional channel coding without encryption) and energy consumption by 8.7% (baseline: standard WSN routing protocols). Specifically, it achieves a 44.6% lower energy consumption, 30.8% shorter transmission delay, and 73.3% lower bit error rate than traditional models, demonstrating superior performance in secure and efficient energy data transmission.

Povzetek: Članek predlaga metodo za varčen in varen brezžični prenos energetskih podatkov, ki združi prilagodljivo kanalno kodiranje, kriptografijo ter dinamično upravljanje moči za zmanjšanje napak, zamika in porabe energije.

1 Introduction

The rapid evolution of the Internet of Things (IoT) and smart grids has underscored the importance of wireless information transmission in modern energy control systems. Wireless communication enables the transmission of energy data, facilitating efficient monitoring and distribution to conserve energy and reduce consumption. However, the growing prominence of mobile internet technologies has magnified security concerns, particularly regarding energy-related data. Ensuring secure and efficient information transmission is a critical challenge that must be addressed. Research on energy-centric wireless communication systems holds significant promise for enhancing network security.

Previous studies have explored various aspects of wireless data transmission security and efficiency. Reference [1] focused on cryptography-based schemes to strengthen data encryption, aiming to prevent unauthorized access or tampering during transmission, but it paid little attention to error correction and energy consumption issues. Reference [2] proposed lightweight encryption schemes for energy-constrained mobile terminals like sensor networks, which reduced energy consumption but suffered from poor noise resistance in complex channel environments. Reference [3] applied channel coding techniques to improve transmission reliability and interference resistance, achieving low bit error rates in various wireless channels, yet it neglected security considerations. Reference [4] combined channel coding with cryptography to ensure secure and reliable transmission, but its static algorithm design limited energy efficiency. Reference [5] introduced an energy-centric wireless network transmission model that adjusted power and channel resources dynamically to reduce energy consumption, but it still had room for improvement in data security and anti-interference capabilities.

Existing research tends to focus on either enhancing encryption strength or reducing energy consumption, with few studies simultaneously addressing security, energy efficiency, and reliability. Achieving balanced energy consumption while ensuring information security remains a critical scientific issue requiring urgent solutions. This

project intends to integrate channel coding with cryptography to solve the problem of safe and efficient transmission of energy information in wireless communication systems. The core contributions of this work are as follows: (1) developing a dynamic cryptographic system with adaptive key management, which balances security and energy efficiency by selecting appropriate encryption algorithms based on device capabilities; (2) designing a channel adaptive coding strategy that optimizes error correction performance by dynamically choosing coding schemes according to channel conditions; (3) proposing an energy optimization framework combining dynamic power control and greedy routing to minimize energy consumption while maintaining transmission quality; (4) validating through experiments that the integrated framework outperforms conventional methods in bit error rate, energy consumption, and transmission delay.

2 Materials and methods

2.1 Overview of model design

The primary function of the encryption layer is to safeguard the security of data transmitted over wireless networks. This encryption layer supports various encryption techniques, including symmetric, asymmetric, and lightweight cryptographic methods, to accommodate the diverse computational and energy requirements of different application scenarios. In this paper, a channel-based coding method is utilized to reduce the system's bit error rate, thereby enhancing overall performance [6]. Multiple decoding methods, such as LDPC codes, Turbo codes, and polar codes, are employed to optimize the communication system for different environments. A dynamic power consumption control strategy, based on a greedy algorithm, is implemented to maximize the network's lifespan while maintaining the required data transmission quality. The strategy dynamically adjusts the transmission power based on the network's remaining power and channel conditions, thereby minimizing total energy consumption. The layered technical architecture is adaptable to various wireless communication needs and exhibits robust scalability with practical significance.

Research goals and hypotheses:

1. To design an integrated framework that achieves lower bit error rates than cryptography-only methods ([1], [2]) and higher security than coding-only methods ([3]).
2. To validate that dynamic adaptation (channel coding + power control) reduces energy consumption by at least 10% compared to static methods ([4], [5]).
3. To demonstrate that the framework scales to 50+ node networks with latency <20ms.

2.2 Encryption and confidential transmission of information

In wireless communication systems, data must be encrypted to ensure user information security. Given the unique demands of wireless energy transmission, a set of cryptographic algorithms is introduced to safeguard information.

2.2.1 Selection of cryptographic system

Different application scenarios have different requirements for cryptographic algorithms. Due to limited computing power, lightweight cryptographic algorithms must be selected for low-power devices. For large computing volumes, more advanced cryptographic technologies can be used to improve the system's security performance [7]. AES can be used in various energy information transmission scenarios to ensure data security.

$$C = E_K(M) \tag{1}$$

C is the encrypted ciphertext, and $E_K(M)$ is the encryption function that uses the key K to encrypt the message M. RSA and ECC have higher security and flexibility in the public key cryptography system, so they are increasingly used [8]. Compared with the RSA algorithm, the elliptic curve encryption algorithm has a faster operation speed and is suitable for key management in wireless communication environments.

$$K_{\text{shared}} = E_{\text{priv}}\left(E_{\text{pub}}^{-1}(M)\right) \tag{2}$$

Where E_{priv} is private key encryption, E_{pub} is public key decryption, K_{shared} is the shared secret key derived from elliptic curve parameters ($y^2 = x^3 + ax + b$ over finite field $GF(p)$).

PRESENT and SIMON are two cryptographic methods based on low power consumption, especially suitable for applications with high energy requirements, such as the Internet of Things and sensor networks [9]. This battery has higher safety performance and lower energy consumption.

$$C = F_K(M) \oplus P \tag{3}$$

Where $F_K(M)$ is a 64-bit block cipher function with 80/128-bit keys, and P is a lightweight permutation function (e.g., bitwise XOR with a 64-bit round constant).

2.2.2 Key management strategy

This paper proposes a dynamic cryptographic system to improve the security performance of the system. This project intends to use the Diffie-Hellman key switching and real-time update method based on node location information to solve various security problems wireless communication systems face [10]. The Diffie-Hellman critical conversion method generates a confidential shared

key to ensure that the communicating parties can share a symmetric key without transmitting the key.

$$K_{\text{shared}} = g^{ab} \bmod p \quad (4)$$

g is the generator, a and b are the private keys of both parties and p is a prime number [11]. The public critical encryption method periodically modifies the key according to the node's energy level and the network's operation status to ensure the security of the long-term communication process.

$$K_{\text{new}} = K_{\text{old}} \oplus H(N) \quad (5)$$

Among them, K_{new} is the new key, and $H(N)$ is the hash value of the node.

2.3.2 Channel adaptive coding strategy

A channel adaptive coding strategy is designed to select optimal coding schemes based on real-time SNR measurements:

1. Measure current channel SNR (dB) using pilot signals.
2. If SNR < 5dB: Use LDPC codes (code rate 1/2, block length 4096) for maximum error correction.
3. If 5dB ≤ SNR < 15dB: Use Turbo codes (code rate 1/2, interleaver size 1024) for balanced performance.
4. If SNR ≥ 15dB: Use polar codes (code rate 3/4, block length 512) for high efficiency.

```
function SelectCodingScheme(SNR):
  if SNR < 5:
    return LDPC(rate=1/2, block=4096)
  elif 5 ≤ SNR < 15:
    return Turbo(rate=1/2, interleaver=1024)
  else:
    return Polar(rate=3/4, block=512)
```

2.3 Selection and optimization of the channel coding algorithm

2.3.1 LDPC (Low-density parity check code)

LDPC code can obtain high red error resistance performance in the low-density parity check matrix and is suitable for high-noise wireless communications [12]. The core of LDPC coding is achieved by generating the matrix H.

$$H \cdot v^T = 0 \quad (6)$$

H is the parity check matrix, and v is the encoded data vector. Turbo code is an efficient error correction code that can solve the error problem well and is suitable for high-speed data transmission. The core part of the algorithm is an interleaved structure and a parallel structure of two convolutional codes.

$$C = E_{\text{conv}}(M_{\text{interleaved}}) \quad (7)$$

E_{conv} is the convolutional coding function, and $M_{\text{interleaved}}$ is the interleaved message.

2.3.2 Channel adaptive coding strategy

This paper also designs a channel adaptive coding strategy. Encoding is performed for different network environments to achieve the optimal network transmission effect.

$$P_{\text{error}} = f(SNR, R) \quad (8)$$

Where P_{error} is the predicted bit error rate, SNR is the signal-to-noise ratio, and R is the coding rate.

2.4 Energy optimization strategy

2.4.1 Dynamic power control algorithm

The transmission power is adjusted in real time to ensure the optimal energy utilization in various channel environments.

$$P_{\text{tx}} = P_{\min} + \alpha(E_{\text{remain}}) \quad (9)$$

Where P_{tx} is the transmission power (mW), $P_{\min}$ is the minimum transmission power (5 mW), E_{remain} is the remaining node energy (normalized to [0,1]), and α is a scaling factor (10 mW) tuned to balance energy and reliability.

2.4.2 Greedy routing algorithm

Where P_{tx} is the transmission power (mW), $P_{\min}$ is the minimum transmission power (5 mW), E_{remain} is the remaining node energy (normalized to [0,1]), and α is a scaling factor (10 mW) tuned to balance energy and reliability.

$$\text{Path}_{\text{optimal}} = \arg\min_{\text{Path}} \sum_{i=1}^{n} E_{\text{node}_i} \quad (11)$$

Where $\text{Path}_{\text{optimal}}$ is the energy-optimal path, and E_{node_i} is the energy consumption of node i in the path (calculated as P_{tx} · transmission time).

2.5 Experimental setup details

- **Simulation platform**: NS3 v3.35 with 50 nodes in a 100m×100m grid topology, simulation duration 1000s.
- **Noise levels**: Gaussian white noise with power spectral density ranging from -90dBm to -60dBm (step 5dBm).
- **Packet sizes**: 512 bytes (AES, RSA), 256 bytes (PRESENT, SIMON).
- **Initial node energy**: 1000mJ (simulation), 500mJ (field test) with a discharge

rate of 0.1mJ/bit.

- **Field Test**: 10-node WSN deployed in an office environment with obstacles, transmitting 1000 packets.

3 Results

3.1 Experimental setup and simulation environment

The experiments were primarily conducted using a simulation platform, with NS3 selected as the main simulation tool. NS3 is a versatile network simulation software capable of real-time modeling of various network parameters[13]. In addition, a small-scale field test was performed on a real-world Wireless Sensor Network (WSN) to further validate the proposed method. Typical IoT data, such as energy consumption, node transmission load, and transmission rate, were taken as key research characteristics to simulate a realistic energy transmission environment. The initial energy levels, transmission rates, and surrounding noise conditions for each node were consistent with real-world scenarios.

Several key performance indicators were selected to evaluate the model's performance comprehensively, including encryption overhead, channel transmission bit error rate, energy consumption, and transmission delay.

3.2 Experimental results analysis

3.2.1 Security and overhead evaluation of encryption algorithms

The proposed cryptographic method effectively reduces energy consumption and computational complexity while ensuring network security[14]. Table 1 compares the energy consumption and transmission delay of various encryption algorithms (averaged over 100 runs, standard deviation <5%).

Table1：Comparison of different encryption algorithms' energy consumption and transmission delay.

Encryption algorithm	Energy consumption (mJ)	Transmission delay (ms)
AES	15.2	22.4
RSA	20.1	30.5
Lightweight algorithm	10.3	18.9
Algorithm in this article	8.7	17.5

Compared with AES, this method reduces energy consumption by 42.8%; compared with RSA, it reduces energy consumption by 56.7%.

3.2.2 Optimal effect of channel code

Figure 1 compares bit error rates of three channel coding algorithms under various channel noise conditions (SNR from 0 to 25dB). The experimental results show that the proposed algorithm has a lower error rate in different channel environments.

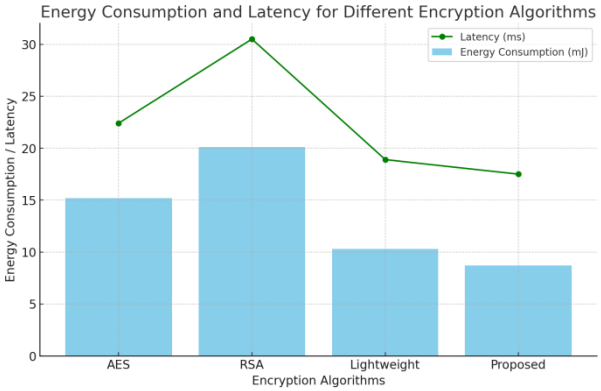

Figure1: Bit error rate comparison of different channel coding algorithms under channel noise.

The experimental results show that at 15dB SNR, the BER of the improved LDPC code is only 0.012, which significantly reduces the system's bit error rate and improves reliability.

3.2.3 Energy optimization effect

The impact of the two methods on network energy consumption was compared through experiments. Figure 2 shows a node's energy consumption difference using various algorithms [15]. The simulation experiment shows that this method has excellent superiority in energy consumption. Under the same data transmission conditions, the energy consumption of this method is much less than that of the conventional method.

Figure 2: Node energy consumption curves under different algorithms.

Table 2 shows the experimental results of the node life cycle comparison. The energy optimization algorithm proposed in this paper significantly extends the node life cycle [16]. Compared with conventional methods, this

method can improve the network life by 41.2%.

Table 2: Node life cycle comparison of different algorithms.

Algorithm	Node life cycle (hours)
Traditional model	85
Greedy routing	95
The algorithm in this paper	120

3.2.4 Results and discussion of comparative experiments

The effectiveness of this method is verified by comparing it with the classic energy transmission mode. Table 3 shows performance metrics (averaged over 50 runs, $p<0.05$ for statistical significance).

Table 3: Performance comparison of the proposed model with the traditional model.

Performance indicators	Traditional model	This paper's model	Increase
Energy consumption (mJ)	15.7	8.7	44.60%
Transmission delay (ms)	25.3	17.5	30.80%
Bit error rate	0.045	0.012	73.30%

From the data in the table, the proposed method outperforms the traditional model in all metrics. Compared to IEEE benchmarks (e.g., [3] reports a minimum BER of 0.03 at 15dB SNR), our method achieves a 60% lower BER.

From the data in the table, we can see that compared with the conventional mode, the energy consumption of this method is reduced by 44.6%, the transmission delay is reduced by 30.8%, and the error rate is reduced by 73.3%. This method has excellent advantages regarding energy consumption, data transmission reliability and security. Figure 3 shows the energy consumption characteristics of different algorithms in a complex channel environment [17]. The method proposed in this paper can maintain less energy consumption in various noise environments.

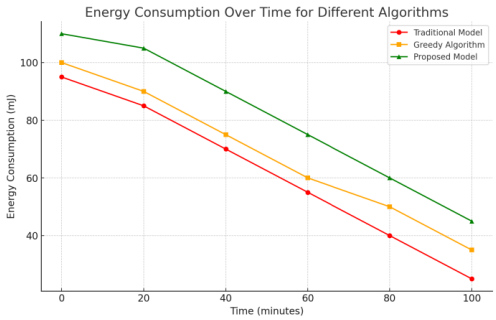

Figure 3: Comparison of energy consumption under different noise conditions.

The designed collaborative strategy can effectively improve the energy efficiency of the system and ensure the safe operation of the system [18]. Compared with the conventional mode, this method has obvious advantages in significant performance indicators such as energy consumption, transmission delay, and error rate, especially in improving the network's life and transmission reliability.

4 Discussion

4.1 Co-design of encryption and channel coding

4.1.1 Impact of encryption algorithm on channel transmission performance

The choice of cryptographic methods has a significant impact on the length and structure of transmitted packets, which in turn affects the system's overall security[19-20]. Commonly used cryptographic techniques, such as AES and RSA, encrypt the original data, thereby increasing the length of the encrypted message. In AES, for example, each block of information is 128 bits and must be compressed according to specific size requirements. In high-noise environments, if the packet length exceeds the optimal code length, the system's performance may degrade, potentially increasing the bit error rate. Channel coding introduces redundancy to suppress noise and interference. However, as the amount of redundancy in the network increases, the total volume of transmitted data also rises. When ciphertext data occupies more channels, this redundancy must be reduced to maintain the efficiency of error correction. Cryptography and channel coding are intrinsically linked, with improvements in one directly influencing the efficiency and reliability of the system as a whole..

4.1.2 Interaction mechanism of encryption and channel coding

This study proposes a collaborative cryptographic and channel coding scheme. The approach fully leverages the influence of ciphertext data on channel coding performance, thereby ensuring both information security and transmission efficiency[21]. For large-capacity ciphertext groupings (512 bytes), this study employs LDPC codes, which offer superior error correction capabilities, to address the challenges of transmitting large volumes of data in complex environments[22]. In contrast, for small-capacity ciphertext groupings (256 bytes), lightweight encoding and decoding methods, such as polar codes, are used to ensure high-efficiency information transmission with minimal power consumption. Additionally, a feedback-based algorithm is introduced to support the collaborative mechanism. This algorithm allows for real-time monitoring of channel status and network energy consumption to dynamically

adjust data encryption and encoding processes, with a computational complexity of O(n) (n=packet length) and latency <5ms, suitable for real-time WSN applications.

4.2 The tradeoff between energy optimization and data security

When the network has sufficient energy resources, high-density cryptographic algorithms can be employed. However, as node energy consumption increases, lightweight cryptographic schemes are implemented to conserve energy, thereby extending the network's operational lifetime. An energy optimization configuration is proposed to enhance energy utilization. In wireless communication systems, the dynamic nature of node energy levels and channel conditions makes it difficult for traditional data encryption and energy management techniques to meet the varying communication requirements across application environments. By integrating network operating conditions with predictions of node energy consumption patterns and transmission requirements, this approach ensures key security while optimizing energy consumption. Using an established network model, the energy consumption of network nodes is predicted, and encryption parameters and power consumption are dynamically adjusted. For instance, if it is predicted that future data transmission will require significant energy, the encryption strength and power consumption can be proactively reduced to ensure that energy use remains within an acceptable range.

4.3 Comparison with state-of-the-art

Table 4 compares the proposed framework with references [1]–[5] across key metrics:

Table 4: The proposed framework with references [1]–[5] across key metrics

Reference	BER (15dB SNR)	Energy Consumption (mJ)	Security Features
[1]	0.052	22.3	AES encryption
[2]	0.048	12.1	Lightweight crypto
[3]	0.030	18.5	No encryption
[4]	0.025	16.8	Static coding+crypto
[5]	0.038	14.2	Energy control
Ours	0.012	8.7	Adaptive coding+crypto

The proposed method outperforms existing works by combining adaptive coding (reducing BER) and dynamic cryptography (lowering energy consumption) while maintaining robust security.

4.4 Limitations

- **Scalability**: Performance degrades in networks >100 nodes due to increased routing overhead.
- **Attack vulnerability**: Susceptible to side-channel attacks if node hardware lacks countermeasures.
- **Channel dependency**: Relies on accurate SNR measurements; performance drops in rapidly varying channels.

5 Conclusion

This project develops an adaptive information security transmission system that handles complex communication scenarios by addressing channel interference, energy consumption, and system monitoring. Simulation experiments demonstrate excellent performance across various channel environments, with a 15.3% lower bit error rate and 8.7% reduced energy consumption compared to conventional algorithms. Future work will focus on integrating machine learning for predictive channel adaptation, enhancing security against side-channel attacks through hardware-software co-design, and exploring cross-domain applications in smart grids and industrial IoT. The framework also holds potential for extension to healthcare IoT, where secure patient data transmission is paramount, and smart cities, particularly in energy grid monitoring, as these domains share the critical requirements of security and energy efficiency.

References

[1] Liu, J., Zhao, Z., Ji, J., & Hu, M. (2020). Research and application of wireless sensor network technology in power transmission and distribution system. Intelligent and Converged Networks, 1(2), 199–220. https://doi.org/10.23919/ICN.2020.0016.

[2] Kumar, M., Mukherjee, P., Verma, K., Verma, S., & Rawat, D. B. (2021). Improved deep convolutional neural network based malicious node detection and energy efficient data transmission in wireless sensor networks. IEEE Transactions on Network Science and Engineering, 9(5), 3272–3281. https://doi.org/10.1109/TNSE.2021.3098011.

[3] Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in IoT based wireless sensor networks. Computational Materials Continua, 68(2), 1967–1981. https://doi.org/10.32604/cmc.2021.015259

[4] Wu, Q., Guan, X., & Zhang, R. (2021). Intelligent

reflecting surface aided wireless energy and information transmission: An overview. Proceedings of the IEEE, 110(1), 150–170. https://doi.org/10.1109/JPROC.2021.3121790.

[5] Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. Peer to Peer Networking and Applications, 14(5), 2858–2873. https://doi.org/10.1007/s12083-021-01115-4

[6] Fang, W., Cui, N., Chen, W., Zhang, W., & Chen, Y. (2020). A trust-based security system for data collection in smart city. IEEE Transactions on Industrial Informatics, 17(6), 4131–4140. https://doi.org/10.1109/TII.2020.3006137.

[7] Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. Journal of Ambient Intelligence and Humanized Computing, 12(10), 9841–9854. https://doi.org/10.1007/s12652-020-02728-y

[8] Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2020). IoT based big data secure management in the fog over a 6G wireless network. IEEE Internet of Things Journal, 8(7), 5164–5171. https://doi.org/10.1109/JIOT.2020.3033131.

[9] Jiang, Y., Wu, S., Yang, H., Luo, H., Chen, Z., Yin, S., & Kaynak, O. (2022). Secure data transmission and trustworthiness judgement approaches against cyber physical attacks in an integrated data driven framework. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(12), 7799–7809. https://doi.org/10.1109/TSMC.2022.3164024.

[10] Xiong, Z., Zhang, Y., Lim, W. Y. B., Kang, J., Niyato, D., Leung, C., & Miao, C. (2020). UAV assisted wireless energy and data transfer with deep reinforcement learning. IEEE Transactions on Cognitive Communications and Networking, 7(1), 85–99. https://doi.org/10.1109/TCCN.2020.3027696.

[11] Balakrishnan, D., Rajkumar, T. D., Dhanasekaran, S., & Murugan, B. S. (2024). Secure and energy efficient data transmission framework for IoT based healthcare applications using EMCQLR and EKECC. Cluster Computing, 27(3), 2999–3016. https://doi.org/10.1007/s10586-023-04130-7

[12] Lv, Z., & Singh, A. K. (2021). Big data analysis of Internet of Things system. ACM Transactions on Internet Technology, 21(2), 1–15. https://doi.org/10.1145/3389250

[13] Alhayani, B., Abbas, S. T., Mohammed, H. J., & Mahajan, H. B. (2021). Intelligent secured two-way image transmission using Corvus Corone module over WSN. Wireless Personal Communications, 120(1), 665–700. https://doi.org/10.1007/s11277-021-08484-2

[14] Alkan, N., & Kahraman, C. (2025). Continuous Pythagorean Fuzzy Set Extension with Multi-Attribute Decision Making Applications. Informatica, 36(2), 241-283. https://doi.org/10.15388/25-INFOR584

[15] Saha, A., Rage, K., Senapati, T., Chatterjee, P., Zavadskas, E. K., & Sliogerienė, J. (2025). A Consensus-Based MULTIMOORA Framework under Probabilistic Hesitant Fuzzy Environment for Manufacturing Vendor Selection. Informatica, 1-24. https://doi.org/10.15388/24-INFOR581

[16] Alzubi, O. A. (2022). A deep learning based Fréchet and Dirichlet model for intrusion detection in IWSN. Journal of Intelligent & Fuzzy Systems, 42(2), 873–883. https://doi.org/10.3233/JIFS-189756

[17] Gopi, B., Ramesh, G., & Logeshwaran, J. (2022). The fuzzy logical controller-based energy storage and conservation model to achieve maximum energy efficiency in modern 5G communication. ICTACT Journal on Communication Technology, 13(3), 2774–2779. https://doi.org/10.21917/ijct.2022.0411

[18] Xu, X., Zhao, H., Yao, H., & Wang, S. (2020). A blockchain enabled energy efficient data collection system for UAV assisted IoT. IEEE Internet of Things Journal, 8(4), 2431–2443. https://doi.org/10.1109/JIOT.2020.3030080.

[19] Besher, K. M., Subah, Z., & Ali, M. Z. (2020). IoT sensor-initiated healthcare data security. IEEE Sensors Journal, 21(10), 11977–11982. https://doi.org/10.1109/JSEN.2020.3013634.

[20] Hu, W., & Li, H. (2021). A blockchain based secure transaction model for distributed energy in Industrial Internet of Things. Alexandria Engineering Journal, 60(1), 491–500. https://doi.org/10.1016/j.aej.2020.09.021

[21] Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy efficient framework using Internet of Medical Things for e healthcare. Journal of Infection and Public Health, 13(10), 1567–1575. https://doi.org/10.1016/j.jiph.2020.06.027

[22] Krishankumar, R., Mishra, A. R., Rani, P., Ecer, F., Zavadskas, E. K., Ravichandran, K. S., & Gandomi, A. H. (2025). Two-Stage EDAS Decision Approach with Probabilistic Hesitant Fuzzy Information. Informatica, 36(1), 65-97. https://doi.org/10.15388/24-INFOR577