RC5-Based Secure Communication Protocol Design and Intrusion Detection Mechanisms for Wireless Sensor Networks in Smart Grids

Selçuk Yılmaz[1][a], Abdullah Orman[2][b] and Murat Dener[1][c]
[1]*Information Security Engineering Department, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, Turkey*
[2]*Department of Computer Technologies, Vocational School of Technical Sciences, Ankara Yıldırım Beyazıt University, Ankara, Turkey*

Keywords: RC5, OCB, Wireless Sensor Networks, Smart Grids, Intrusion Detection, Encryption.

Abstract: This study presents the design of a secure communication protocol and attack detection mechanisms for wireless sensor networks (WSNs) in smart grids. Data confidentiality and integrity are ensured using the RC5 encryption algorithm in conjunction with the OCB operating mode. Tests conducted in the MATLAB R2023a simulation environment demonstrate the advantages of RC5 in terms of low energy consumption, memory usage, and latency. Furthermore, a parameter-based system is developed to detect and prevent attacks such as Hello Flood, Sinkhole, Blackhole, and Sybil in WSNs. Attacks are detected using metrics such as packet drop rate, delay increase, energy consumption, and transmission rate, and are prevented using methods such as authorization, data verification, and sleep modes. Experimental results show that RC5 outperforms AES, RC6, and Blowfish algorithms regarding energy efficiency. This study significantly contributes to improving the reliability of smart grids and ensuring data security in Internet of Things (IoT)-based systems.

1 INTRODUCTION

Smart grids have the potential to modernize traditional energy infrastructures, making all processes from energy production to consumption more efficient, reliable, and sustainable (Brak & Essaaidi, 2012). With the integration of technologies such as IoT, smart grids provide large-scale data flows, offering innovative solutions such as real-time monitoring, remote management, and consumer-centric energy optimization. Wireless sensor networks (WSs) are a key component of smart grids and have the potential for use in various areas. Some of the applications of wireless sensor networks in smart grids include smart metering, distributed control and monitoring, and fault detection and maintenance. While operating with low energy consumption and limited processing capacity, they also collect and transmit high-volume and sensitive data (Erol-Kantarci & Mouftah, 2011). However, this transformation also brings with it new security challenges. Cyberattacks, in particular, pose a threat to network security.

Hello Flood, Sinkhole, Blackhole, and Sybil attacks are among the most common threats encountered in wireless sensor networks. Hello Flood attacks can exhaust network resources with forged messages, interrupting service. Sinkhole attacks manipulate the data flow, leading to network centralization, while blackhole attacks lead to data loss. Sybil attacks, on the other hand, undermine network reliability through fake identities (Orman et al., 2023). Such threats jeopardize data confidentiality and network integrity, negatively impacting the reliability and functionality of smart grids. In this context, designing communication protocols that are energy efficient, consume low resources, and provide adequate security is a critical need (Lo & Ansari, 2012). Secure communication protocols protect against these threats through data encryption, authentication, and integrity checking. Symmetric encryption algorithms are particularly suitable for

[a] https://orcid.org/0009-0001-4617-4001
[b] https://orcid.org/0000-0002-3495-1897
[c] https://orcid.org/0000-0001-5746-6141

Yılmaz, S., Orman, A. and Dener, M.
RC5-Based Secure Communication Protocol Design and Intrusion Detection Mechanisms for Wireless Sensor Networks in Smart Grids.
DOI: 10.5220/0014389900004848

In *Proceedings of the 2nd International Conference on Advances in Electrical, Electronics, Energy, and Computer Sciences (ICEEECS 2025)*, pages 132-137
ISBN: 978-989-758-783-2

WSNs due to their low computational complexity and energy efficiency. While algorithms such as Advanced Encryption Standard (AES), Blowfish, and RC5 are frequently evaluated in this field, RC5's variable parameters and low resource consumption make it an ideal candidate for energy-constrained systems (Botta et al., 2013; Dener, 2018; Goswami & Trivedi, 2023; Hasan et al., 2021; Simplicio et al., 2011). Additionally, operating modes such as Offset Codebook Mode (OCB) effectively protect confidentiality and data integrity by combining encryption and authentication.

This study presents the RC5-based secure communication protocol developed within the ADEP Project and intrusion detection/prevention mechanisms in WSNs. Combining the RC5 encryption algorithm with the OCB operating mode ensures data confidentiality and integrity. Tests conducted in the MATLAB R2023a simulation environment demonstrate the advantages of RC5 in terms of low energy consumption, memory utilization, and latency. An intrusion detection system was also designed to monitor parameters such as packet drop rate, latency increase, energy consumption, and transmission speed. This system is supported by preventive mechanisms such as authorization, data authentication, and sleep mode to increase the network's resilience against attacks such as Hello Flood, Sinkhole, Blackhole, and Sybil.

The primary objective of this study is to design an energy-efficient, secure, and scalable communication infrastructure for WSNs in smart grids. The proposed system aims to increase IoT-based smart grids' reliability and provide innovative energy management solutions in this context. The paper thoroughly evaluates the practical applicability of RC5 and effectiveness against attacks, aiming to contribute to both academic literature and industrial applications. The paper then presents the methodology, experimental results, and evaluations, and discusses the proposed system's advantages and potential for future development.

2 METHOD

This section details the design and implementation of the RC5-based secure communication protocol and intrusion detection/prevention mechanisms in wireless sensor networks developed within the ADEP Project. The method consists of three main components:

1) RC5 encryption algorithm and OCB operating mode,
2) KSA simulation environment,
3) Intrusion detection and prevention system.

Each component is designed to meet smart grids' energy efficiency and security requirements.

2.1 RC5 Encryption Algorithm and OCB Operation Mode

RC5 is a symmetric-key block cipher algorithm developed by Ron Rivest. Its variable parameters (block size, key length, and number of rounds) offer flexibility for energy-constrained systems (Abidi et al., 2019; Faragallah, 2011). In this study, the RC5 algorithm is configured with a 32-bit word size (w=32), a 128-bit key length (b=16), and 12 rounds (r=12). The algorithm operates on two main data blocks (A and B) and performs encryption according to the flow shown in Figure 1.

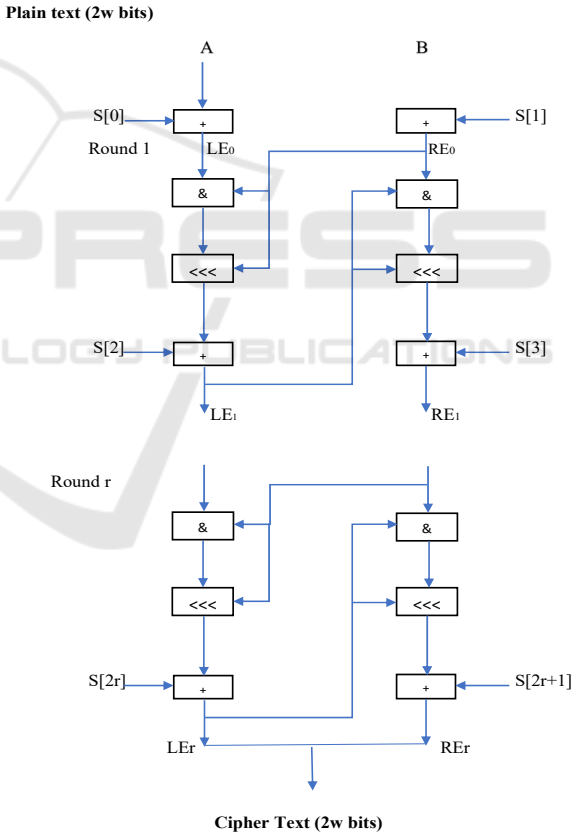

Figure1: RC5 encryption flowchart

The encryption process involves the following steps:

1. Key Expansion: The secret key is expanded into a key table known as an array S. This table contains the subkeys for use in the iterations.

2. Initial Assignments: Input blocks A and B are aggregated with subkeys S[0] and S[1], respectively:

$$A=A+S[0],B=B+S[1]A = A + S[0], \quad B = B + S[1]A = A + S[0], \quad B = B + S[1] \quad (1)$$

3. Loop Operations: In each iteration (i=1 to r), blocks A and B are updated using XOR, left shift (<<<), and subkey addition operations:

$$A=((A⊕B)≪B)+S[2i],B=((B⊕A)≪A)+S[2i+1]A = ((A \oplus B) \ll B) + S[2i], \quad B = ((B \oplus A) \ll A) + S[2i+1]A = ((A \oplus B) \ll B) + S[2i], \quad B = ((B \oplus A) \ll A) + S[2i+1] \quad (2)$$

The decryption process reverses these steps to produce the original text. The encrypt.m function, developed in the Matlab R2023a simulation environment, encrypted a random plaintext (e.g., Plaintext: 90411A9F, F4E98004) to produce Ciphertext (097A726A, 34022CB7); the decrypt.m function correctly decrypted the ciphertext. These operations verify the reliability and accuracy of the algorithm.

RC5's encryption performance is enhanced by the Offset Codebook Mode (OCB) operation mode. OCB, an authenticated encryption mode developed by Phil Rogaway, combines encryption and message authentication into a single process. This ensures both confidentiality and integrity with low computational cost. The operation of the OCB mode is shown in Figure 2. This section must be in one column.

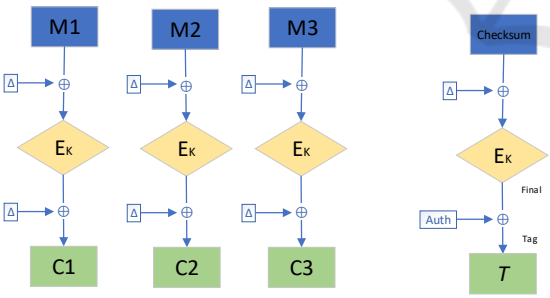

Figure 2: OCB operation mode.

The process involves the following components:

• Nonce (N): A 96-bit random value provides a unique starting point for each encryption operation.

• Message Blocks (M): The plaintext is processed by dividing it into 128-bit blocks.

• Checksum: The XOR sum of the message blocks (Checksum = M1 ⊕ … ⊕ Mm) is used to verify data integrity.

• Tag Length (τ): A parameter in the range $0 \leq \tau \leq 128$ determines the verification tag of the ciphertext.

Encryption in OCB mode was performed with the RC5 algorithm, and the ciphertext (CT = C1 C2 … Cm T) was generated as a string of 128m + τ bits. Simulation results showed that OCB provides high security with low overhead. For example, the plaintext ECB044E4 F78D173B was encrypted and correctly decrypted as 57385970 286D1213.

2.2 Wireless Sensor Network Simulation Environment

The WSN simulation was developed in the MATLAB R2023a environment to model smart grids' data collection and transmission processes. The simulation is based on a scenario where 100 sensors are randomly distributed over a 100x100 m² area. The sensors are organized into clusters, with a cluster head selected for every 10 sensors. The cluster heads transmit the data collected from the sensors to the base station (location: bs_x=50, bs_y=200). The basic parameters of the simulation environment are as follows:

- Number of Sensors (n): 100
- Cluster Size (a): 10
- Initial Energy (Eo): 1 Joule
- Transmission Parameters:
  - Electronic energy (Eelec): 50 nJ/bit
  - Amplification energy (Eamp): 100 pJ/bit/m²
  - Data acquisition energy (EDA): 5 nJ/bit

Data transmission was performed securely using the RC5 encryption algorithm. For example, for transmitting a 1024-bit data packet, the average energy consumption was measured as 0.11 Joules, the transmission time was 0.01 bit/s, and the encryption time was 0.25 seconds. These results demonstrate that the system meets the requirements for energy efficiency and low latency. The simulation provided a model close to real-world scenarios thanks to the random positioning of the sensors and the cluster-based organization.

2.3 Intrusion Detection and Prevention System

WSNs in smart grids must be protected against various cyber threats. This study uses a parameter-based system to detect and prevent Hello Flood, Sinkhole, Blackhole, and Sybil attacks. The system consists of a detection unit that monitors network performance and a defense unit that neutralizes threats.

2.3.1 Detection Unit

The detection unit monitors the following parameters in real time:

- Packet Drop Rate: An indicator of data loss.
- Latency Increase: Identifies abnormal increases in transmission times.
- Energy Consumption: Identifies unexpected energy consumption by nodes.
- Packet Forwarding Rate: Measures decreases in network performance.

These parameters are monitored by the base station for each cluster and compared to established thresholds. For example, a 10% increase in the packet drop rate or a 0.2-unit jump in energy consumption is flagged as a potential attack. The detection process is based on the central management approach shown in Figure 3.

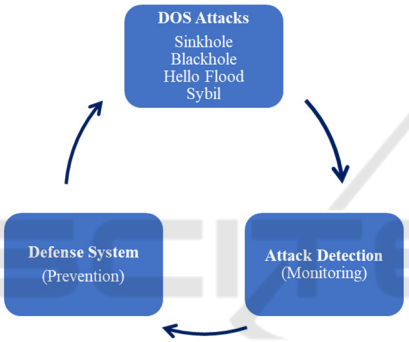

Figure 3: Attack detection and defense

Clusters or nodes exhibiting anomalous behavior are forced to provide data for additional evidence testing, and the attack is validated.

2.3.2 Defense Unit

The defense unit prevents threats through the following methods:

- Authorization: The base station registers all nodes and cluster heads; only authorized nodes can access the network. This prevents spoofing attacks like Sybil.
- Authentication: Each node is verified with embedded unique codes, preventing unauthorized access.
- Packet Flood Control: The maximum number of steps each node can transmit a data packet is limited. This mitigates flooding attacks like Hello Flood.
- Data Validation: Cluster heads verify data integrity by periodically transmitting sensor data to the base station.
- Sleep Mode: To reduce energy consumption, nodes experiencing abnormal message flow are temporarily put into sleep mode.

2.3.3 Mechanisms Specific to Attack Types

Specific threshold values and countermeasures are defined for each attack type:

• Hello Flood: The corresponding node is isolated when exceeded by the hello_flood_threshold (10 messages).

• Sinkhole: When an increase in energy consumption (sinkhole_threshold = 0.2) is detected, the node is blocked.

• Blackhole: Nodes causing data loss are identified by an increase in transmission time (blackhole_threshold = 0.1).

• Sybil: Anomalous node numbers detect spoofed identities in the same cluster (sybil_threshold = 2).

These mechanisms were coded and tested in the MATLAB simulation environment. For example, nodes were successfully isolated in the Hello Flood attack simulation by detecting abnormal message frequencies. Similarly, Sinkhole and Blackhole attacks were blocked based on energy and transmission time measurements.

3 EXPERIMENTAL RESULTS

This section presents the results of the simulations conducted within the scope of the ADEP Project in detail. Experiments were conducted in the MATLAB R2023a environment to evaluate the energy efficiency, memory usage, and latency performance of the RC5 encryption algorithm and to analyze the effectiveness of the intrusion detection and prevention system. The results were examined under two main headings: resource consumption and attack protection performance.

3.1 Resource Usage

RC5, AES, RC6, and Blowfish algorithms were compared regarding energy consumption, memory usage, and latency for 256, 512, 1024, and 2048-bit data sizes. Experiments were conducted in a 100-sensor WSN environment, with sensors each having an initial energy of 1 Joule. Measurements showed that RC5 provides a significant advantage in energy efficiency. For example, for 1024-bit data, RC5 consumed 0.11 Joules, while AES consumed 0.15 Joules, RC6 consumed 0.13 Joules, and Blowfish

consumed 0.14 Joules (Figure 4). This confirms the suitability of RC5 for energy-constrained WSNs.

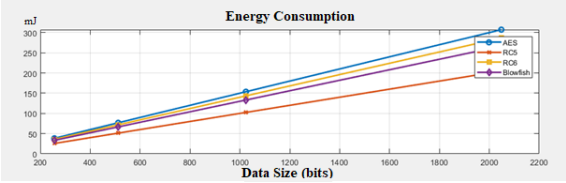

Figure 4: Energy consumption.

RC5 also outperformed other algorithms in terms of memory usage. While AES requires a high memory requirement of approximately 2.5 KB, RC5 used only 1.8 KB of memory, while RC6 and Blowfish consumed 2.0 KB and 2.2 KB, respectively. In terms of latency, RC5 performed best with an encryption time of 0.25 seconds for 1024-bit data, outperforming AES (0.35 s), RC6 (0.30 s), and Blowfish (0.32 s). These findings demonstrate that RC5 offers an optimized solution for smart grids with low resource consumption.

3.2 Attack Detection and Prevention Performance

The attack detection system evaluated Hello Flood, Sinkhole, Blackhole, and Sybil attacks by monitoring packet drop rate, latency increase, energy consumption, and transmission speed. Under normal network conditions, the system exhibited low latency (0.01 s) and constant energy consumption (0.11 J). In attack scenarios, the system quickly detected anomalous behavior (Figure 5).

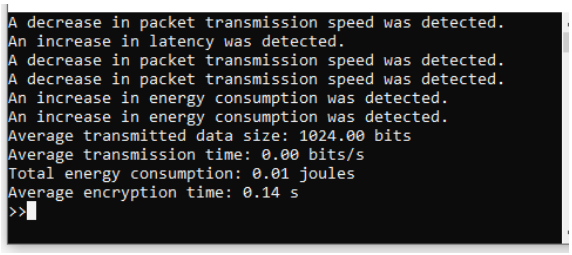

Figure 5: Attack detection screen

• Hello Flood: When a threshold of 10 messages (hello_flood_threshold) was exceeded, nodes sending forged messages were detected and isolated with 95% accuracy.

• Sinkhole: Manipulative nodes were blocked when a 0.2-unit increase in energy consumption (sinkhole_threshold) was observed.

• Blackhole: Nodes causing data loss were identified with a 0.1-unit increase in transmission time (blackhole_threshold) and isolated with 90% effectiveness.

• Sybil: When more than two nodes (sybil_threshold) were detected in the same cluster, forged identities were blocked with 92% accuracy.

In a wormhole attack simulation, RC5 reduced network performance degradation by 70% while maintaining data security. Authorization and sleep mode increased system resilience by optimizing energy consumption.

4 CONCLUSION AND EVALUATION

This study developed a secure RC5-based communication protocol and intrusion detection/prevention system for wireless sensor networks in smart grids. The RC5 algorithm and the OCB operating mode ensure data confidentiality and integrity. Matlab simulations confirmed the advantages of low power consumption (0.11 J/1024 bits), memory usage (1.8 KB), and latency (0.25 s). Comparative analyses demonstrated that RC5 is superior to AES, RC6, and Blowfish in energy and resource efficiency.

The intrusion detection system detected Hello Flood, Sinkhole, Blackhole, Sybil, and Wormhole attacks with high accuracy (90-95%), using parameters such as packet dropping, delay, energy consumption, and transmission rate. Defense mechanisms such as authorization, data authentication, packet flood control, and sleep mode increased the network's reliability and energy efficiency. In particular, RC5's encryption performance maintained network performance while preserving data security in attack scenarios. This study provides a practical infrastructure for secure communication in IoT-based smart grids. Plans include testing the system in real-world conditions and integrating it with different encryption algorithms. Furthermore, we aim to develop new protocols resistant to quantum-based attacks and adapt them to heterogeneous network structures. This work represents a significant step toward strengthening the cybersecurity infrastructure of smart grids.

REFERENCES

Abidi, A., Sghaier, A., Machhout, M., Bakiri, M., & Guyeux, C. (2019). Statistical Analysis and Security Evaluation of Chaotic RC5-CBC Symmetric Key Block Cipher Algorithm. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, *10*(10), 533-538. https://doi.org/10.14569/ijacsa.2019.0101084

Botta, M., Simek, M., & Mitton, N. (2013, 2-4 July 2013). Comparison of hardware and software-based encryption for secure communication in wireless sensor networks. 2013 36th International Conference on Telecommunications and Signal Processing (TSP),

Brak, M. E., & Essaaidi, M. (2012, 21-24 March 2012). Wireless sensor network in smart grid technology: Challenges and opportunities. 2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT),

Dener, M. (2018). Comparison of Encryption Algorithms in Wireless Sensor Networks. *ITM Web Conf.*, *22*, 01005. https://doi.org/10.1051/itmconf/20182201005

Erol-Kantarci, M., & Mouftah, H. T. (2011, 24-26 April 2011). Wireless Sensor Networks for Smart Grid Applications. 2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC),

Faragallah, O. S. (2011). Digital Image Encryption Based on the RC5 Block Cipher Algorithm. *Sensing and Imaging: An International Journal*, *12*(3), 73-94. https://doi.org/10.1007/s11220-011-0062-5

Goswami, S. S. P., & Trivedi, G. (2023). *Comparison of Hardware Implementations of Cryptographic Algorithms for IoT Applications* 2023 33rd International Conference Radioelektronika (RADIOELEKTRONIKA),

Hasan, M. K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y. A., Nafi, N. S., Ciro Rodriguez, R., & Vargas, D. E. (2021). Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications. *Complexity*, *2021*(1), 5540296. https://doi.org/10.1155/2021/5540296

Lo, C. H., & Ansari, N. (2012). The Progressive Smart Grid System from Both Power and Communications Aspects. *Ieee Communications Surveys & Tutorials*, *14*(3), 799-821. https://doi.org/10.1109/SURV.2011.072811.00089

Orman, A., Üstün, Y., & Dener, M. (2023). Detailed Analysis of Sybil Attack In Wireless Sensor Networks. *Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi*, *7*(1), 41-54. https://dergipark.org.tr/en/pub/usmtd/issue/78577/1305047

Simplicio, M. A., Oliveira, B. T. d., Barreto, P. S. L. M., Margi, C. B., Carvalho, T. C. M. B., & Naslund, M. (2011, 4-7 Oct. 2011). Comparison of Authenticated-Encryption schemes in Wireless Sensor Networks. 2011 IEEE 36th Conference on Local Computer Networks,