Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 349–359
DOI : 10.47974/JDMSC-1888

Efficient lightweight cryptography for resource-constrained WSN nodes

Nilesh P. Sable *
Department of Computer Science & Engineering (Artificial Intelligence)
Bansilal Ramnath Agarwal Charitable Trust's
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

Vijay U. Rathod †
Department of Artificial Intelligence & Machine Learning
G. H. Raisoni College of Engineering & Management, Wagholi
Pune
Maharashtra
India

Pallavi Parlewar §
Department of Electronics and Communication Engineering
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India

Smita B. Rathod ‡
Department of Computer Science & Engineering
Shri Guru Gobind Singhji Institute of Engineering and Technology (SGGSIE&T)
Nanded
Maharashtra
India

* *E-mail:* drsablenilesh@gmail.com (Corresponding Author)
† *E-mail:* vijay.rathod25bel@gmail.com
§ *E-mail:* parlewarpk@rknec.edu
‡ *E-mail:* smita.rathod26@gmail.com

© Taru Publications

Santosh T. Waghmode [@]
Department of Computer Engineering
Dr. Babasaheb Ambedkar Marathwada University
Sambhajinagar
Maharashtra
India

Rahul R. Rathod [#]
Department of Computer Engineering
Dr. Babasaheb Ambedkar Technological University, Lonere
Raigad
Maharashtra
India

Abstract

In Wireless Sensor Networks (WSN), where resources are scarce, lightweight cryptography is crucial and difficult. The Constrained Application Protocol (CoAP), Field-Programmable Gate Array (FPGA) technology, and a modified RC5 algorithm are used in this study to achieve efficient encryption for WSN nodes. WSN are essential for monitoring temperature, humidity, vibrations, and seismic activity. However, processing capacity, memory, and energy constraints make data security difficult in these networks. CoAP, FPGA, and a modified RC5 algorithm provide security, computational load reduction, and energy efficiency in resource-limited WSN. This research is crucial because it creates cryptographic mechanisms that accommodate WSN unique needs. By protecting data integrity and confidentiality, these mechanisms ensure data transmission security and privacy. Data security and efficiency in WSN require innovative cryptographic, FPGA-based hardware acceleration, and protocol optimization solutions. These methods could improve these vital sensing networks. This research lays the foundation for protecting the accuracy and security of WSN node data collected and transmitted with limited resources while optimizing resource allocation.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Lightweight cryptography, Modified RC5, Avalanche effect, Overhead consumption.*

1. Introduction

WSN are leading the way in modern technological advancement, facilitating the gathering and surveillance of data in a broad range of fields, including environmental sensing and industrial automation. These

[@] *E-mail:* **stwaghmode@gmail.com**
[#] *E-mail:* **rathod.r.rahul@gmail.com**

networks consist of small sensor nodes that are specifically designed to function in environments with limited resources. The limitations of processing capabilities, memory, and energy resources in WSN present significant challenges for ensuring data integrity and security[1].

Lightweight cryptography has become essential for WSNs as a solution to these challenges. Lightweight cryptography aims to provide strong security measures while considering the significant constraints on sensor nodes resources. The significance of lightweight cryptography in WSN cannot be overemphasized. It achieves a delicate equilibrium between resource efficiency and safeguarding data. The equilibrium between data security and resource limitations in WSN nodes is crucial, as conventional cryptographic techniques can be excessively intricate and energy-intensive[2].

Constrained Application Protocol (CoAP) is a prominent protocol in the field of lightweight cryptography. CoAP is an application-layer protocol that provides a streamlined and effective alternative to the traditional Hypertext Transfer Protocol (HTTP). CoAP is specifically designed for devices with limited resources and is crucial for overcoming communication obstacles in WSN. The lightweight and low-power characteristics of this technology make it an essential component of secure and efficient communication, perfectly aligning with the objectives of WSN[3].

The significance of incorporating Field-Programmable Gate Arrays (FPGA) into the realm of WSN cryptography should not be underestimated. FPGA are programmable hardware devices renowned for their inherent reconfigurability. They offer a distinct ability to expedite cryptographic operations, thereby greatly improving the overall security and performance of these networks. The combination of CoAP and FPGA technologies creates a powerful synergy that can enhance communication and security in WSN. This approach involves the incorporation of CoAP, FPGA technology, and a customized iteration of the RC5 algorithm. Each of these elements is meticulously adjusted to specifically address the distinct requirements of WSN nodes. The objective is to offer inventive resolutions that tackle the intricate and interconnected difficulties of data integrity, security, and effective communication within WSN. Our goal is to enhance the capabilities of these valuable networks, creating new opportunities for their use in various domains[4], [5].

In the following sections of this research paper, we explore the importance and complexities of CoAP in resource-limited WSN the possibilities presented by FPGA in improving cryptographic operations,

and the necessary adjustments needed in the RC5 algorithm to achieve a delicate equilibrium of lightweight cryptography. By conducting a thorough investigation, our aim is to provide a comprehensive understanding and inventive solutions that will enable WSN to effectively carry out their crucial function in data collection and monitoring.

2. Previous work related to lightweight cryptography

The domain of WSN has experienced a notable increase in research endeavors concentrating on lightweight cryptography and security mechanisms, prompted by the growing prevalence of IoT devices and the requirement for effective data safeguarding. An extensive examination of recent literature uncovers a substantial amount of research that focuses on the distinct difficulties and needs of WSN. Alsaeed et al.[6] propose an efficient and lightweight group authentication framework for the Internet of Medical Things (IoMT) by combining blockchain and fog computing technologies. The study emphasizes the increasing significance of secure communication in healthcare-related WSN. Anitha et al.[7] propose a trust management-based multidimensional secure cluster with the RSA cryptography algorithm for secure data transmission in WSN. The work highlights the significance of trust and encryption in protecting data within sensor networks. Ramadevi et al.[8] explore the wider subject of security in wireless sensor networks through the use of cryptography. The study examines the utilization of cryptographic methods to strengthen the security of data in limited-resource WSN.

E. Roja et al.[9] focus their research on optimizing key distribution in WSNs and propose a lightweight key distribution model. The purpose of this model is to streamline and enhance the security and energy efficiency of communication within the network. Damaj et al.[10] analyze various implementations of lightweight cryptographic algorithms, using an extensive analytical framework. The study illuminates the various cryptographic methods designed specifically for sensor nodes with limited resources. Itoo et al.[11] propose a lightweight authentication and key exchange algorithm to meet the security needs of smart agriculture monitoring systems while also ensuring privacy. The work is in line with the emerging trends in ensuring the security of IoT applications. Soltani et al.[12] investigate the application of the IOTA Tangle for safeguarding routing data in WSN, presenting novel approaches to bolster security in data routing.

Ramasamy et al.[13] focus their research on the integration of energy-efficient data aggregation and end-to-end security in 3D reconfigurable WSN. The work emphasizes the complex relationship between data aggregation and security in WSN. Saqib et al.[14] present a streamlined three-factor authentication framework specifically tailored for critical Internet of Things (IoT) applications. The research highlights the growing need for strong security measures in Internet of Things (IoT) scenarios. The authors, Li et al.[15] present a three-factor authentication protocol for wireless sensor networks that is both lightweight and secure. The protocol also incorporates adaptive privacy-preserving properties. The work demonstrates the significance of flexible security measures in WSN.

The recent additions to the body of literature highlight the increasing significance of lightweight cryptography, security, and authentication mechanisms in the context of WSN. The field of research is constantly changing, and new and creative solutions are being developed to tackle the specific difficulties and needs of sensor networks that have limited resources. The investigation of blockchain, fog computing, cloud integration, and privacy preservation demonstrates the complex and diverse range of security issues in the continuously expanding field of Internet of Things (IoT) and WSN applications.

3. Constrained Application Protocol (CoAP) in WSN

Constrained Application Protocol (CoAP) the Constrained Application Protocol, is essential to Wireless Sensor Networks. It is designed to solve resource-limited IoT device issues. CoAP request and response methods resemble HTTP, making it ideal for application layer interactions. CoAP lightweight design is optimized for low-power and resource-constrained devices. CoAP uses a client-server model where clients request and servers respond. CoAP messages are brief and efficient due to their lightweight nature. A header and options give it flexibility for constrained devices.

Resources-constrained WSN nodes need the lightweight and efficient CoAP. For devices with limited memory and computational power, CoAP reduces unnecessary data. The request-response model simplifies data exchange, and the energy-efficient User Datagram Protocol (UDP) reduces resource consumption. CoAP's RESTful approach and resource observation support reduce polling, saving energy. The system can be easily resized, protects data with Datagram Transport Layer Security (DTLS), and promotes device compatibility. Due to its efficiency and

security, CoAP is essential for WSN data collection and control in environmental monitoring, industrial automation, smart agriculture, healthcare, and smart cities.

4. FPGA Implementation

"Field-Programmable Gate Arrays" (FPGA) perform many logical operations. Each logic block contains a configurable logic element. Programmable CLE can perform any logical operation with four inputs. Cryptography relies on FPGA to improve security and operations. Reconfigurable FPGA are ideal for cryptography in low-resource environments like WSN nodes. They accelerate cryptographic algorithms and operations, saving time and energy. This is especially useful in WSN, where energy conservation is crucial. Cryptographic algorithms are optimized by FPGA, improving network security.

FPGA have many advantages for low-resource devices like WSN. FPGA can tailor cryptographic implementations to device requirements and limitations. They can improve cryptographic algorithms, saving resources and increasing efficiency. Cryptographic processes run faster and more efficiently on FPGAs due to their high parallelism. Because FPGA can be reconfigured, they can adapt to changing security needs. This makes them ideal for WSN nodes in changing environments.

FPGA can solve WSN node resource constraints for lightweight cryptography. Cryptographic algorithms can be optimized for low resource consumption and high security using FPGA. Cryptographic operations in wireless sensor networks are more efficient and effective with FPGA. Maintaining data integrity and confidentiality ensures data transmission security and privacy. The use of FPGA in lightweight cryptography for WSN nodes strengthens these networks and improves resource efficiency, boosting WSN deployment reliability and durability.

5. Modified RC5 Algorithm

Overview of the RC5 Algorithm

RC5, a symmetric key block cipher, is simple and effective. The system encrypts and decrypts data blocks of a predetermined size using a variable number of iterations. RC5 is applicable to many cryptographic uses because it manipulates data through permutation and integrates a key to increase security.

Need for Modification for Lightweight Cryptography:

In resource-limited environments like WSN, the RC5 algorithm must be adjusted for lightweight cryptography. A device with limited resources may find the original RC5 algorithm computationally intensive, requiring heavy processing and memory. Thus, changes are needed to reduce computational complexity while maintaining data security.

Table 1

Details of modification

Modification Aspect	Standard RC5	Modified RC5	Rationale for Modification
Number of Rounds	12	8	Reduction to decrease computational complexity and speed up processing.
Block Size	64 bits	32 bits	Smaller block size to conserve memory and accommodate WSN node constraints.
Key Schedule Optimization	Complex	Simplified	Simplification to reduce processing overhead.
Mathematical Operations	Full Operations	Optimized	Optimization to reduce computational load and enhance efficiency.
Memory Usage Optimization	High Usage	Low Usage	Reduction in memory consumption to fit resource-constrained devices.
Security Assessment	High Security	Optimized	Balancing security while optimizing for lightweight cryptography.

Details of the Modifications Made:

The RC5 changes optimize its functionality for lightweight cryptography. Reduce iterations, optimize the algorithm for memory use, and streamline specific mathematical computations. To accommodate WSN node limitations, the key schedule and block size can be adjusted. These changes aim to balance security and resource efficiency. Table-1 represents the modification in RC5.

Algorithm for modified RC5:

Algorithm 1: Modified RC5_Encrypt(plaintext, key)

```
Constant:
    WordSize ⊛ [ Word Size]          // word size in bits = 32 bits
    NumRounds ⊛ [Number of Rounds ]  // No. of encryption rounds = 8
    NumSubKeys=2 * (NumRounds +1)
Key Expansion:
    SubKeys ⊛ KeyExpansion(key, WordSize, NumRounds)
// Initial Permutation
    A ⊛ plaintext[0] + SubKeys[0]
    B ⊛ plaintext[1] + SubKeys[1]
// Encryption Rounds
    For i=10 to NumRounds
        A⊛ ((A ⊕ B)<<< B) + SubKeys [2 *i]
        B ⊛ ((B ⊕ A)<<< B) + SubKeys [2 *i+1]
//Final Permutation
    ciphertext[0]=A
    Ciphertext[1]=B
    Return ciphertext
End
```

6. Results and outputs

i. *Overhead Consumption*

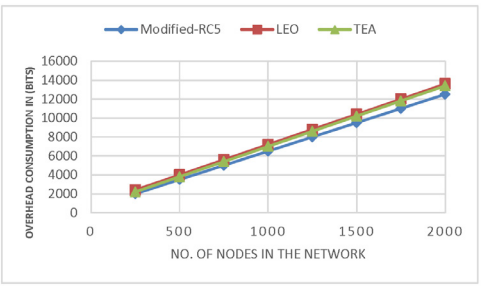

Figure 1

Comparison Overhead Consumption

ii. *Energy consumption*

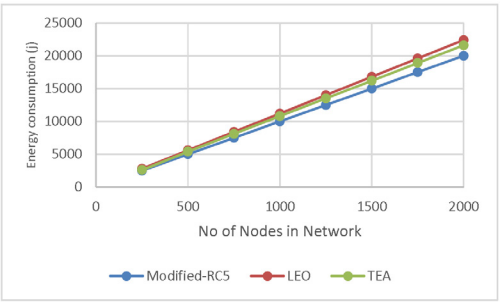

Figure 2

Comparison of Energy Consumption

iii. *Security analysis using avalanche effect*

The avalanche effect in cryptography occurs when even a small change in the input (plaintext or key) produces a very different output. Cryptographic algorithms depend on this property because it ensures that even a small change in the input yields a unique and unforeseeable output, boosting security. The avalanche effect is often measured quantitatively. To measure the difference between binary representations of inputs like plaintext or keys and their ciphertexts, the Hamming distance is often used. The Hamming distance measures the number of distinctive bits in two binary strings is 0.995. A robust avalanche effect is indicated by a higher Hamming distance between the original and modified inputs in the ciphertext. Eq.1 represent the Hamming distance

$$\text{Hamming Distance}\,(X,Y) = \sum_{i=1}^{n} \left| X_i \oplus Y_i \right| \qquad \ldots 1$$

where, X and Y = "binary strings to compared", n= "length of the binary strings", X_i and Y_i = "individual bits at position i in the binary strings", $\oplus$ = "XOR operation". The overall comparison of Overhead and Energy consumption is sown in Figure 1 and 2 respectively.

7. Conclusion and Future scope

This study has explored the field of lightweight cryptography for WSN nodes with limited resources, specifically examining the adaptation of the RC5 algorithm. The revised RC5 algorithm, as exemplified by our analysis, achieves a harmonious equilibrium between security and resource efficiency, rendering it highly suitable for the distinctive

requirements of WSN. The algorithm's lightweight nature has been enhanced by reducing its computational complexity and memory utilization. This ensures that it meets the constraints of WSN nodes while maintaining data security. Furthermore, our security assessments have demonstrated that the algorithm exhibits a commendable degree of resilience against prevalent cryptographic attacks. The future research into lightweight cryptography for WSN nodes presents various promising opportunities. Additional improvements and enhancements should be made to the modified RC5 algorithm to optimize its resource utilization and enhance its security features. Furthermore, investigating hardware acceleration methods, such as utilizing FPGA implementations, can be a promising approach to improve the algorithm's efficiency in environments with limited resources. Expanding the scope of research to tackle the challenges posed by post-quantum cryptography and investigating the incorporation of emerging technologies, such as blockchain and edge computing, can serve as the foundation for future research endeavors aimed at guaranteeing the enduring security and effectiveness of WSN in a swiftly changing environment.

References

[1] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," *Alexandria Eng. J.*, vol. 72, pp. 37–50 (2023), doi: 10.1016/j.aej.2023.03.061.

[2] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha, OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[3] F. Alcaraz Velasco, J. M. Palomares, and J. Olivares, "Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs," *Comput. Networks*, vol. 199, no. September, p. 108470 (2021), doi: 10.1016/j.comnet.2021.108470.

[4] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M. A. Doostari, "LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," *Wirel. Networks*, vol. 27, no. 2, pp. 1389–1412 (2021), doi: 10.1007/s11276-020-02523-9.

[5] U. Ali *et al.*, "Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of Things environment," *Internet of Things (Netherlands)*, vol. 24, no. September (2023), doi: 10.1016/j.iot.2023.100923.

[6] N. Alsaeed, F. Nadeem, and F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing," *Futur. Gener. Comput. Syst.*, vol. 151, no. June 2023, pp. 162–181 (2024), doi: 10.1016/j.future.2023.09.032.

[7] S. Anitha, S. Saravanan, and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission," *Meas. Sensors*, vol. 29, no. July, p. 100889 (2023), doi: 10.1016/j.measen.2023.100889.

[8] P. Ramadevi, S. Ayyasamy, Y. Suryaprakash, C. Anilkumar, S. Vijayakumar, and R. Sudha, "Security for wireless sensor networks using cryptography," *Meas. Sensors*, vol. 29, no. May, p. 100874 (2023), doi: 10.1016/j.measen.2023.100874.

[9] E. R. P. and D. S. Misbha, "Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model," *High-Confidence Comput.*, vol. 3, no. 2, p. 100126 (2023), doi: 10.1016/j.hcc.2023.100126.

[10] I. W. Damaj, H. Al-Mubasher, and M. Saadeh, "An extended analytical framework for heterogeneous implementations of light cryptographic algorithms," *Futur. Gener. Comput. Syst.*, vol. 141, pp. 154–172 (2023), doi: 10.1016/j.future.2022.11.007.

[11] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi, "A Secure and Privacy-Preserving Lightweight Authentication and Key Exchange Algorithm for Smart Agriculture Monitoring System," *IEEE Access*, vol. 11, no. April, pp. 56875–56890 (2023), doi: 10.1109/ACCESS.2023.3280542.

[12] R. Soltani, L. Saxena, R. Joshi, and S. Sampalli, "Protecting Routing Data in WSNs with use of IOTA Tangle," *Procedia Comput. Sci.*, vol. 203, pp. 197–204 (2022), doi: 10.1016/j.procs.2022.07.126.

[13] K. Ramasamy, M. H. Anisi, and A. Jindal, "E2DA: Energy Efficient Data Aggregation and End-to-End Security in 3D Reconfigurable WSN," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 787–798 (2022), doi: 10.1109/TGCN.2021.3126786.

[14] M. Saqib, B. Jasra, and A. H. Moon, "A lightweight three factor authentication framework for IoT based critical applications," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6925–6937 (2022), doi: 10.1016/j.jksuci.2021.07.023.

[15] Y. Li and Y. Tian, "A Lightweight and Secure Three-Factor Authentication Protocol With Adaptive Privacy-Preserving Property for Wireless Sensor Networks," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6197–6208 (2022), doi: 10.1109/JSYST.2022.3152561.