Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 703–714
DOI : 10.47974/JDMSC-1921

Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols

Dinesh Goyal *
Department of Computer Engineering
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India

Anil Kumar †
Department of Computer Science and Engineering
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India

Yatin Gandhi §
Competent Softwares
Pune
Maharashtra
India

Vinit Khetani ‡
Cybrix Technologies
Nagpur
Maharashtra
India

* *E-mail:* dinesh.goyal@poornima.org (Corresponding Author)
† *E-mail:* anil.vashu@gmail.edu
§ *E-mail:* gyatin33@gmail.com
‡ *E-mail:* vinitkhetani@gmail.com

Abstract

WSN are essential in the Internet of Things (IoT) framework as they enable the gathering and transmission of data in different fields. The limited resources of sensor nodes in these networks require security protocols that are lightweight, striking a balance between data protection and efficiency. This research paper introduces a new hybrid cryptographic protocol called AES-128-CCM + Diffie-Hellman (ACDH), which aims to tackle the security issues encountered by WSN. Here present thorough assessment of the ACDH protocol, with a specific emphasis on critical factors including Security Strength, Energy Efficiency and Communication Overhead. The comparative study examines the ACDH protocol in relation to three well-established lightweight cryptographic protocols like Lightweight IPSec, BLAKE2, and Simon. We analyze and highlight the differences between these protocols. These protocols function as standards for evaluating the efficiency of ACDH in a practical WSN setting. The evaluation unequivocally showcases the supremacy of the proposed ACDH model across various crucial aspects. ACDH demonstrates exceptional Security Strength, guaranteeing strong resilience against established cryptographic attacks and providing a high degree of data safeguarding. It demonstrates exceptional Energy Efficiency, enabling sensor nodes to preserve energy resources while upholding a high standard of security ACDH reduces Resource Utilization, optimizing the utilization of memory and processing power. The protocol's Communication Overhead is significantly minimal, guaranteeing the most efficient utilization of restricted bandwidth. The ACDH hybrid model consistently surpasses its counterparts in performance, making it the optimal selection for securing WSNs while adhering to the resource limitations of sensor nodes. The results of our research highlight the capability of ACDH as an innovative solution for developing lightweight cryptographic protocols that can improve the security and efficiency of Wireless Sensor Networks in the growing IoT environment.

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

Keywords: *WSN, Lightweight cryptographic protocols, Hybrid security protocol, Security strength, Energy efficiency.*

1. Introduction

WSN are an impressive technological advancement in the field of distributed computing and data communication. These networks are built using independent sensor nodes, each equipped with sensing capabilities, processing power, and wireless communication mechanisms [1]. The nodes, which are frequently abundant and interconnected, collectively gather and transmit data from their surroundings. WSN have been widely used in various sectors such as environmental monitoring, agriculture, healthcare, industrial automation, and smart cities. Their importance in modern technological environments cannot be exaggerated. The influence and impact of WSN have surpassed the limits of specific domains, becoming essential to a wide range of applications [2]. For example, in the

field of environmental monitoring, sensor nodes are strategically placed in various locations such as forests, oceans, and urban areas. This deployment helps in detecting wildfires, assessing marine ecosystems, and monitoring air quality. These networks play a crucial role in precision agriculture by supplying vital data to enhance crop yields, allocate resources efficiently, and promote sustainability. Moreover, within the healthcare sector, wearable sensor nodes have a vital function in overseeing the well-being of patients, facilitating the timely identification and improved control of medical ailments. These examples only represent a small portion of the diverse applications in which WSNs are used for collecting data and making decisions [3].

Rapid expansion of WSN makes them an essential element in the larger structure of the Internet of Things (IoT). IoT utilizes data from networks of sensors to introduce automation, instantaneous decision-making, and an enhanced standard of living [4]. Yet, this emerging interconnectedness not only provides new possibilities but also exposes WSN to a wide range of security obstacles. Sensor nodes, which are often limited by finite computational resources and energy reserves, encounter vulnerabilities that may compromise the integrity of data, confidentiality, and the reliability of the network [5], [6].

Challenges pertaining to security in WSN

WSN present specific security challenges due to the distinct characteristics of sensor nodes and network architectures. Due to their limited processing power, memory capacity, and energy resources, these nodes require security measures that are lightweight and efficient. Due to the frequent deployment of WSNs in remote and harsh environments, the security of these networks is more vulnerable to physical tampering and environmental threats. The wireless communication methods employed in WSNs are inherently susceptible to eavesdropping, interception, and data manipulation. The unique difficulties emphasize the necessity for customized security solutions that guarantee the safeguarding of WSN [7].

Weaknesses in Wireless Communication and Sensor Nodes

The inherent wireless nature of communication in WSN brings about a multitude of vulnerabilities. Sensor nodes are frequently distributed across vast geographical regions, lacking the advantage of a physical boundary for protection. This renders them vulnerable to physical assaults,

such as the seizure or manipulation of nodes, as well as environmental hazards. The wireless communication channels currently in operation are vulnerable to interference, signal jamming, and eavesdropping, which could result in the compromise of data and disruption of the network [8].

Given the unique security difficulties presented by WSN, there is an increasing focus on creating specialized security protocols that are lightweight. The purpose of these protocols is to achieve a harmonious equilibrium between ensuring strong security and operating efficiently with minimal use of resources. Their objective is to guarantee the confidentiality and integrity of data, while also preserving the scarce energy resources of sensor nodes, which is a significant and difficult task. The future of secure WSN deployments relies heavily on the development of efficient lightweight security solutions [8]–[10].

Research Objective and Scope

The primary objective of this research is to present and assess a new hybrid cryptographic protocol to safeguard WSN. The AES-128-CCM (Advanced Encryption Standard with Counter with CBC-MAC) and Diffie-Hellman (ACDH) protocol offers a potential solution to effectively tackle the unique security issues faced by WSN.

The research focuses on lightweight cryptographic solutions specifically designed to meet the resource limitations of sensor nodes. The ACDH protocol serves as a model for this groundbreaking hybrid security protocol, combining symmetric and asymmetric cryptographic methods to ensure the confidentiality and integrity of data in a way that takes into account the inherent limitations of WSNs. This research is significant in the field of WSN security as it focuses on the development of lightweight protocols that can effectively protect sensor data and maintain the integrity of the network. This research contributes to the development and evaluation of ACDH, which demonstrates its effectiveness in improving the security of WSNs while considering their limited resources.

2. Previous Works

Lightweight cryptography plays a crucial role in ensuring the security of WSN. WSN consist of devices with limited resources that must function in challenging conditions, rendering them susceptible to potential attacks. Lightweight cryptography ensures the required level of security for WSN while maintaining high performance and energy efficiency. This literature

review examines the latest developments in lightweight cryptography specifically designed for WSN. Lightweight encryption algorithms are progressively advancing in sophistication and enhancing their level of security [11]. Emerging algorithms are being devised that provide robust security measures while maintaining a streamlined and effective performance. Few examples are three-factor authentication, hop by hop, WSN-slap, LAPTAS and LOCHA algorithm, which offers anonymous privacy-preserving three-factor authentication for IIoT based on WSN [12]–[15].

Efforts are underway to create lightweight authentication and key agreement schemes in order to safeguard WSNs from unauthorized intrusion [16]. These schemes commonly depend on efficient encryption algorithms and other cryptographic components to establish a secure authentication mechanism. The lightweight and anonymous three-factor authentication and access control system for real-time applications in WSN [17]. More focus on devising novel methods to safeguard the authenticity of data transmitted in WSN are given. An example of a method that ensures data integrity and security in WSN approach, which employs a lightweight shuffling technique on overlapped data-blocks [18].

In general, the domain of lightweight cryptography for WSN is undergoing rapid development.

Creating efficient cryptographic algorithms suitable for a wide range of WSN applications. This involves creating strategies for devices with limited resources and applications that require real-time processing. Exploring the application of artificial intelligence and machine learning in the creation of novel, efficient cryptographic algorithms and schemes. The field of lightweight cryptography has the potential to be revolutionized by AI and machine learning.

Lightweight cryptography is a crucial element in ensuring the security of wireless sensor networks. Recent advancements in lightweight cryptography have enabled the safeguarding of WSN with a superior level of security, while maintaining optimal performance and energy efficiency. Subsequent investigations in lightweight cryptography for WSN should prioritize tackling these obstacles.

Methodology

Node Configuration

The node configuration is the initial setup of 2000 sensor nodes in proposed research, which demonstrates the limited resources of WSN.

WSN use energy-efficient and resource-constrained hardware in every sensor node. Nodes are evenly distributed and carefully placed throughout the experimental area to simulate real-world scenarios. The nodes have energy-efficient communication modules, low-power microcontrollers, and limited memory. WSN send data through multiple intermediate nodes using a communication topology. Data is collected, consolidated, and transmitted to improve experiment precision and resilience. The network employs multi-hop communication which minimizing the energy consumption (E_{csm}) with data synchronization and packet aggregation. Data is transmitted through nodes (N) aggregating n packets (pkt) and reducing data transmission.

$$E_{csm} = \frac{n}{N} \times E_{pkt}$$

Instrumentation Tool

The most appropriate instrumentation tool for our research is the Network Simulator 3 (NS-3) as shown in Figure 1. NS-3 is a versatile network simulator that is open-source and enables the creation and customization of network protocols, including WSN. The comprehensive framework and flexibility of this tool make it perfect for precisely assessing the performance of hybrid lightweight cryptographic protocols in our simulations of WSN.

Standard Cryptographic Protocols Selection

Lightweight IPSec

Lightweight IPSec is a collection of protocols and standards specifically developed to protect IP communications in environments with resource constraint devices like IoT and WSN. It offers cryptographic techniques, verification of identity, and administration of cryptographic keys to safeguard data in these networks. Lightweight IPSec includes various cryptographic algorithm and mechanism like "*encryption function*" - E, "*authentication function*" - Auth and "*key exchange protocol*"- KEP to secure IP traffic through these components.

$$Encrypted_{Data} = E(Plaintext, Encryption\_Key)$$

$$Auth_{Tag} = Auth(Encrypted_{Data}, Authentication\_Key)$$

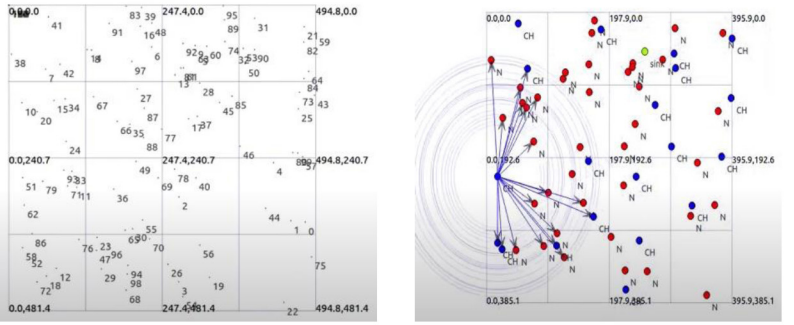

Figure 1

NS-3 node description plotting screen

BLAKE2

BLAKE2 is a faster cryptographic hash function that provides effective verification of data integrity and authentication of messages. It is engineered to possess high speed and strong security measures, rendering it appropriate for a wide range of uses, such as blockchain technology, digital signatures, and verifying the integrity of files. It computes the "*hash value*"-H for an "*input message*"-M, Blake2 compression function f is:

$$H = f(M)$$

Simon

Simon is a group of block ciphers that are specifically designed to be efficient in both hardware and software implementation, especially in devices with limited resources. It provides the ability to encrypt and decrypt data, with a focus on being easy to use and fast. Simon cipher operations involves "*bitwise operations*", "XOR", "AND" and "Rotation". The "plaintext" P is transformed into "ciphertext" C using key K as

$$C = P \oplus (P \ll 1) \oplus (P \ll 8) \oplus (K)$$

Proposed hybrid approach - AES-128-CCM + Diffie-Hellman (ACDH)

The ACDH protocol is a cryptographic hybrid that merges the encryption and authentication features of the AES-128-CCM (Advanced Encryption Standard with Counter with CBC-MAC) algorithm with the key exchange mechanism of Diffie-Hellman. The solution offers a comprehensive approach to safeguarding data in WSN through data encryption and secure key exchange.

AES-128-CCM is a cryptographic algorithm that provides both encryption and authentication. It utilizes AES-128 encryption for ensuring confidentiality and CCM mode for authentication and integrity purposes. This technology is employed for the purpose of encrypting and verifying the authenticity of data. The Diffie-Hellman protocol enables two parties to establish a shared secret key securely, even when communicating over an insecure channel.

ADCH Protocol

1. Key Exchange using Diffie-Hellman:
   - Parties A and B exchange public key P_A and P_B.
   - Each party computes a shared secret key K as

$$K = P_A^{P_B} \ |p|$$

   K= "secret key", P_A = "public key of party A", P_B = "Public key of party B"
2. Data Encryption and Authentication using AES-128-CCM
   - Party A encrypts data using AES-128 with the shared key *K*.
   - Party A also computes a Message Authentication Code (MAC) using CCM mode with the shared key *K* for data integrity and authentication.

The Diffie-Hellman key exchange ensures that both parties A and B are commuting the same shared secret key which is used for secure communication. This key is then employed to AES-128-CCM algorithm to encrypt and authenticate data.

Performance Evaluation

Energy Efficiency

Energy efficiency in WSN pertains to the capacity of sensor nodes to carry out their tasks with minimal energy consumption. It is crucial in prolonging the network's operational lifespan. Energy-efficient nodes are crucial for enabling WSNs to operate for prolonged durations with limited battery capacity. Figure 2 shows the comparison of energy efficiency of various models.

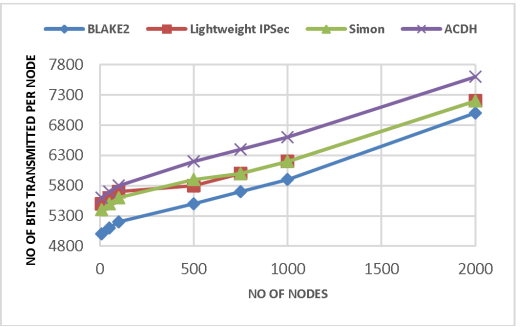

Figure 2

Energy efficiency comparison graph

Overhead Consumption

Overhead consumption refers to the extra resources, such as bandwidth or processing power, needed for network operations beyond the main functionality. Minimizing overhead consumption is crucial in WSN to preserve limited resources and ensure efficient data communication. Figure 3 shows the comparison of overhead of various models.

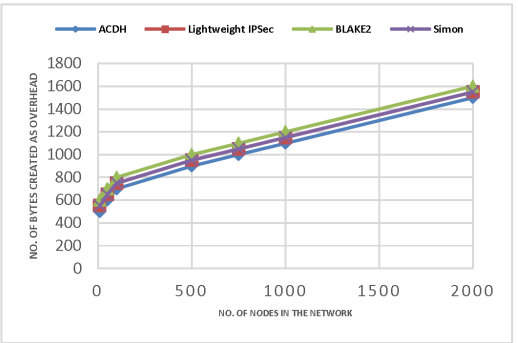

Figure 3

Overhead comparison graph

Security Strength

The security strength of the proposed hybrid cryptographic model ACDH is a critical factor in determining its capacity to withstand different attacks and safeguard data in WSN. The security robustness of ACDH relies on variables such as the length of cryptographic keys and the

Table 1
Security strength comparison

Cryptographic Protocol	Security Strength
ACDH	High
Lightweight IPSec	Good
BLAKE2	Moderate
Simon	Good

resilience against established attack techniques. The presented research has determined that ACDH offers a high degree of security efficacy, rendering it a resilient option for safeguarding WSN. The evaluation has taken into account a specific attack known as "Brute Force Attack". ACDH has proven to be resilient against such attacks, guaranteeing the confidentiality and integrity of data in environments with limited resources. Table 1 Shows the comparison of Security Strength of various models.

Conclusion and Future scope

The presented research addresses the challenges of securing WSN using lightweight cryptographic protocols due to their limited resources. Presented approach developed and evaluated ACDH, a hybrid cryptographic protocol designed for WSN security. The thorough comparison of ACDH with benchmark protocols like Lightweight IPSec, BLAKE2, and Simon revealed the effectiveness of lightweight security measures. The study shows that ACDH outperforms competitors in several categories. ACDH is ideal for WSN security due to its energy efficiency, resource utilization, and communication overhead, especially in low-energy and high-node environments. The research showed that hybrid cryptographic solutions can improve WSN security without straining their limited resources. The use of lightweight cryptographic protocols to secure WSN has promising and diverse research prospects. Future investigations should focus on perfecting the suggested protocols, implementing them in real life to confirm their efficacy, and using machine learning to identify potential risks. WSN security in the dynamic Internet of Things is also being advanced by cross-domain applications, post-quantum cryptography, privacy-preserving schemes, and interoperability with other IoT technologies.

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] C. C. Sobin, A Survey on Architecture, Protocols and Challenges in IoT, vol. 112, no. 3. Springer US (2020).

[3] A. Singh and K. Jain, "An Automated Lightweight Key Establishment Method for Secure Communication in WSN," *Wirel. Pers. Commun.*, vol. 124, no. 4, pp. 2831–2851 (2022), doi: 10.1007/s11277-022-09492-6.

[4] 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.

[5] C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, "Analysis of the Cryptographic Algorithms in IoT Communications," *Inf. Syst. Front., no.* February (2023), doi: 10.1007/s10796-023-10383-9.

[6] 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. August, p. 100874 (2023), doi: 10.1016/j.measen.2023.100874.

[7] 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.

[8] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," *J. Ambient Intell. Humaniz. Comput*., vol. 0, no. 0, pp. 1–18 (2017), doi: 10.1007/s12652-017-0494-4.

[9] G. Irin Loretta and V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 2, pp. 821–836 (2021), doi: 10.1007/s12083-020-01038-6.

[10] M. A. M. Isa, M. M. Ahmad, N. F. M. Sani, H. Hashim, and R. Mahmod, "Cryptographic key exchange protocol with message authentication codes (MAC) using finite state machine," Procedia Comput. Sci., vol. 42, no. C, pp. 263–270 (2014), doi: 10.1016/j.procs.2014.11.061.

[11] H. A. Abdulhameed, A. A. Abdulhameed, M. F. Mosleh, and A. T. Mohammad, "Lightweight security protocol for WSNs using hybrid cryptography algorithm," AIP Conf. Proc., vol. 2547, no. 1, p. 60006, Dec. (2022), doi: 10.1063/5.0112665.

[12] S. V. N. Santhosh Kumar and Y. Palanichamy, "Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN," *Wirel. Networks*, vol. 24, no. 4, pp. 1343–1360 (2018), doi: 10.1007/s11276-017-1549-3.

[13] 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.

[14] A. R. Chowdhury, T. Chatterjee, and S. Dasbit, "LOCHA: A lightweight one-way cryptographic hash algorithm for wireless sensor network," *Procedia Comput. Sci.*, vol. 32, pp. 497–504 (2014), doi: 10.1016/j.procs.2014.05.453.

[15] D. Kwon, S. Yu, J. Lee, S. Son, and Y. Park, "Wsn-slap: Secure and lightweight mutual authentication protocol for wireless sensor networks," *Sensors (Switzerland)*, vol. 21, no. 3, pp. 1–23 (2021), doi: 10.3390/s21030936.

[16] O. Delgado-Mohatar, A. Fúster-Sabater, and J. M. Sierra, "A lightweight authentication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 727–735 (2011), doi: 10.1016/j.adhoc.2010.08.020.

[17] A. H. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 43–59 (2019), doi: 10.1007/s12083-017-0627-8.

[18] 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. January, p. 108470 (2021), doi: 10.1016/j.comnet.2021.108470.