A Lightweight Layered Security Scheme for Secure RSSI-Based Indoor Localization

Rafina Destiarti Ainul* and Djuwari
Electrical Engineering Department, Universitas Surabaya (UBAYA), Indonesia
Email: rafina@staff.ubaya.ac.id (R.D.A.); djuwari@staff.ubaya.ac.id (D.J.)

Manuscript received November 17, 2025; revised January 21, 2026; accepted February 5, 2026
*Corresponding author

***Abstract*—Indoor localization is a key application of Wireless Sensor Networks (WSNs) for tracking objects, where secure communication is essential to protect sensitive location data. This paper proposes a lightweight, layered security scheme for indoor localization systems deployed on resource constrained WSN devices. The scheme integrates multiple cryptographic algorithms: Ascon-Authenticated Encryption with Associated Data (AEAD) for authenticated encryption, X25519 for key exchange, ED25519 digital signatures over a SHA-256 hash of the encrypted payload to ensure strong source authentication, data provenance, and non-repudiation of localization data and timestamp-based replay protection. Raspberry Pi devices serve as Anchor (AN) and Unknown Nodes (UN), where AN transmits encrypted data containing estimated position parameters, including Received Signal Strength Indicator (RSSI) and Pathloss Exponent (PLE) values. UN then decrypt data from the three nearest AN. Experimental results show the system requires only 17.82 ms processing time at AN and 6.48 ms at UN using Raspberry Pi 3B devices and using Wi-Fi File Transmission Protocol (FTP) transmission averaging 3.12 ms per packet. This approach provides enhanced security assurance for indoor localization data, outperforming traditional cryptographic combinations methods such as Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES), and Message Digest 5 (MD5) in terms of efficiency and suitability for WSN environments.**

***Index Terms*—Ascon-Authenticated Encryption with Associated Data (AEAD), lightweight layered security, Received Signal Strength Indicator (RSSI)-based indoor localization, raspberry Pi, Wi-Fi**

I. Introduction

Wireless Sensor Networks (WSNs) have been widely deployed in various applications such as environmental monitoring, logistics, healthcare and military, by enabling wireless data exchange and communication through its distributed sensor nodes [1, 2]. These systems are usually applied for dynamic or constrained environments which is required real-time monitoring capabilities. Indoor localization as one of WSN application is determining the position of the object within indoor location area. Received Signal Strength Indicator (RSSI)-based localization remains popular due to its simplicity and cost-efficiency at hardware implementation. However, RSSI data measurement have high fluctuated distribution especially when implemented in indoor areas, which is directly affected to the estimated position accuracy result. Therefore, improving the accuracy of RSSI-based localization has been a major focus in recent research.

Unlike the accuracy data from RSSI-based localization, applying privacy data protection in localization is still considered a challenging issue and less explored area. Besides positioning accuracy, data security, especially in wireless transmission, is also a critical aspect in secure localization systems. This is because sensitive location data transmitted over wireless channels is vulnerable to various attacks, including replay attacks, Sybil attacks, man-in-the-middle attacks and data tampering [3, 4]. Hence, securing data transmission in RSSI-based localization system is become essential to preserve privacy and maintain a trustworthy system.

In our previous work [1], we proposed a secure data transmission scheme for indoor mobile cooperative localization using Rivest–Shamir–Adleman (RSA) for key exchange, Advanced Encryption Standard (AES) for symmetric encryption, and Message Digest 5 (MD5) for data integrity. While this approach addressed relative high processing time, which is not appropriate for lightweight and low power WSNs device deployment. To address these limitations, many researches have investigated lightweight cryptographic approach. Design of lightweight authenticated key agreement protocol for Intra- and Inter-IoT (internet of thing) device communication using Elliptic Curve Cryptography (ECC) with FPGA implementation (DEAC-IoT) [4] introduced a lightweight authenticated key agreement protocol based on ECC and implemented on FPGA, which is enabling secure communication for IoT devices communication. KeyEncoder [5] proposed discrete wavelet transform and autoencoders to extract the biometric features from the Electroencephalogram (EEG) signals that used to generate cryptographic keys. While Scalable Authentication and Key Agreement (SAKA) [6] offered scheme suited for edge–fog–multicloud systems. SAKA scheme is also integrated a configurable key evolution mechanism with a sound synchronization and elliptic curve Diffie–Hellman key exchange method. Other lightweight authentication protocols have been also proposed, such as in [7] for digital forensics in industrial Internet of Things (IoT), and [8], which supports scalable batch authentication for IIoT gateways with minimal overhead.

Further studies include ECC-based schemes for vehicular-to-grid systems [9], secure elements integration in a novel ECC-based authenticated key Exchange

Between Industrial IoT Devices Using Secure Element (EBAKE-SE) [10], and certificateless lightweight approaches such as Enhanced Lightweight and Secure Certificateless Authentication Scheme (ELWSCAS) [11]. Ephemeral Diffie–Hellman Over Cose (EDHOC) [12] provides a compact key exchange protocol tailored for constrained IoT devices. Ascon as the cryptography algorithm has also been a focus, with comprehensive surveys [13], its performance evaluations on Arduino implementation [14], and its technical documentation of Ascon v1.2 [15]. Then, the authors in [16] review several approaches of authenticated encryption schemes which is adjusted to the cryptographic trend and nowadays technology requirement. Hybrid algorithm which is combined from AES, Data Encryption Standard (DES) and Rivest Chipper 6 (RC6) approach involves for cloud and data integrity have been proposed in [15, 17]. Hardware and software implementation feasibility have been proposed using FPGA in [18], defence applications [19], and IoT platforms [20]. Focus on application contexts such as healthcare [21], general IoT implementation [22], and large-scale constrained devices [23] are also validate that Ascon is applicable in wide range of areas. An additional proof is confirm that Ascon has strength level of security and efficient are in implementation of reliable lightweight encryption for network communication from [24], Application Specific Integrated Circuit (ASIC)-based hardware realization for securing IoT ecosystem [25], and the comparative evaluations with the other cryptography at [26, 27].

National Institute of Standards and Technology (NIST) as a U.S. agency responsible for standardizing cryptographic algorithms decided that Ascon as the lightweight encryption standard due to its low latency, low memory footprint and still maintains strong security guarantees [13, 15, 27–29]. According to several previous research from [24–27, 29] consistently identify that Ascon still as one of the most effective lightweight encryption schemes for secure data communication under various environmental conditions. Based on these findings, this paper adopts the Ascon scheme as the authenticated encryption algorithm to replace the RSA–AES–MD5 combination used in our previous work. The integration of Ascon into the proposed system provides a more efficient, lightweight, and secure solution for privacy-sensitive data transmission in RSSI-based indoor localization systems. In accordance with NIST security service classifications, authenticated encryption schemes such as Ascon-AEAD are designed to provide confidentiality and integrity, while key establishment mechanisms such as X25519 [30, 31] enable secure session key agreement. However, these mechanisms alone do not inherently provide non-repudiation or long-term data origin accountability, as AEAD authentication tags are valid only within the scope of a shared symmetric session key and do not cryptographically bind messages to a verifiable sender identity once the session context is no longer available.

To address this limitation, an ED25519 digital signature is applied to a SHA-256 hash of the localization data, enabling verifiable source authentication, data provenance, and non-repudiation in accordance with NIST security service definitions. This approach allows independent verification of the integrity and origin of RSSI measurements during data aggregation, storage, and offline analysis, without requiring access to symmetric session keys. Such security properties are not achievable through authenticated encryption alone and are particularly relevant for maintaining trust in indoor localization systems. Although digital signatures introduce additional computational overhead, their inclusion represents a deliberate design choice aimed at strengthening the overall security assurance of localization data rather than introducing redundant cryptographic operations. Moreover, ED25519 is also recommended in NIST [32] for digital signature applications due to its compact signature size and efficient verification performance, making it suitable for deployment in resource constrained wireless sensor network environments.

Therefore, according to the confidentiality, integrity and availability requirement standard for security level, in this paper we are also combined Ascon-AEAD which is used for authenticated encryption with X25519 for its key exchange, Edwards-Curve Digital Signature Algorithm (EdDSA) over curve25519 (ED25519) for digital signature, Secure Hash Algorithm (SHA)-256 bit for integrity verification and timestamp-based replay protection. This layered security scheme aims to enhances our previous work [1], in which a conventional hybrid cryptographic stack was employed, consisting of RSA for asymmetric key distribution, AES for symmetric data encryption, and MD5 for message authentication and integrity checking. In that previous architecture, RSA was not used for bulk data encryption but solely for securely sharing the symmetric AES key, reflecting a typical hybrid security model rather than a standalone cryptographic primitive.

In contrast, our proposed scheme is using modern lightweight cryptographic specifically designed for constrained environments. X25519 enables efficient and secure key agreement without the high computational overhead associated with RSA, while Ascon-AEAD inherently integrates encryption and authentication within a single primitive. To further strengthen security guarantees, ED25519 based digital signatures and SHA-256 hashing are incorporated to support authenticity, integrity, and non-repudiation. This layered yet lightweight approach significantly reduces processing overhead while enhancing security robustness, making it more suitable for real-time WSN based indoor localization systems.

This proposed security scheme is also implemented together with localization scenario at Raspberry Pi 3B devices. Unknown node is continuously move to the specified position and received RSSI and several data of estimated position parameters in the form of secured frame data from the three nearest anchor nodes. Each anchor node constructs encrypted frame data that includes its coordinates, RSSI value, and PLE parameter. This encrypted data is transmitted to the unknown node via Wi-

Fi. Upon receiving data from the three nearest anchor nodes, the unknown node decrypts the information and uses trilateration to estimate its position. All processes are executed on Raspberry Pi devices, leveraging their flexibility and support for advanced cryptographic operations. By replacing RSA, AES, and MD5 with ASCON, X25519, and ED25519, the new scheme addresses the resource inefficiency of previous implementations and offers a secure, lightweight alternative tailored to constrained environments. Therefore, the main contributions of this work are summarized as follows: 1) A lightweight and secure cryptographic architecture is introduced, utilizing NIST-standardized primitives Ascon-AEAD, X25519, ED25519, SHA-256, and timestamp-based replay protection to replace the previous RSA, AES, and MD5 design, resulting in stronger security with significantly lower computational overhead; 2) A secure RSSI-based indoor localization framework is developed on Raspberry Pi 3B devices, in which encrypted anchor information (coordinates, RSSI values, and PLE parameters) is exchanged and processed by the unknown node to perform trilateration algorithm scheme; 3) An improvement in efficiency and robustness over previous work is showing that the proposed lightweight cryptographic scheme supports reliable real-time operation and is well-suited for resource-constrained WSN and IoT environments.

The remainder of this paper is organized as follows: Section II describes the adopted cryptography algorithms and their relevance to lightweight scheme. Section III presents the construction of the proposed system, including the network model and localization scenario. Section IV detail the implementation setup and experimental measurements conducted to evaluate system performance. Section V discuss the performance result analysis, and Section VI conclude the paper by summarizing key findings and outlining potential directions for future research.

II. Adopted Cryptographic Algorithm

In this section is described the several adopted cryptographic algorithms in the form of lightweight schemes, including Ascon-AEAD, X25519, ED25519, SHA and timestamp-based replay protection. These algorithms are selected to form a complete lightweight security architecture that provides secure key establishment, data confidentiality, integrity, and authentication. This design enhances our previous implementation, which employed a conventional hybrid cryptographic stack consisting of RSA for symmetric key distribution, AES for data encryption, and MD5 for integrity verification. By replacing the combination of RSA, AES, and MD5 architecture with modern lightweight cryptography algorithm, it can reduce computational overhead and improved data security level requirement especially for indoor localization system.

A. Ascon-AEAD

Ascon-AEAD stands for Ascon–Authenticated Encryption with Associated Data. Ascon-AEAD as the one of lightweight symmetric cryptographic algorithm is primary recommended by NIST. Ascon provide both confidentiality and message integrity through its AEAD structure and efficient lightweight encryption. Ascon operates using 128-bit secret key S_k and 128-bit nonce, which have the ciphertext C output with 128-bit authentication tag. The main process of Ascon is using permutation-based sponge over 320-bit internal state, then divided into five 64-bit words, and it will be updated iteratively through nonlinear substitution and linear diffusion layers. The encryption process can be expressed as [13–15]:

$$C, T \equiv \text{Encrypt}_{S_k}(N, A, P) \tag{1}$$

$\text{Encrypt}_{S_k}(\cdot)$ denotes as the Ascon-AEAD encryption function with secret key S_k, where T is the authentication tag, N is the public nonce which is initialized before by internal state. Associated data A is absorbed into the state without producing output, for ensuring the authenticity. Plaintext blocks P are XOR into the state to produce ciphertext C. Then, the decryption process function with S_k $\text{Decrypt}_{S_k}(\cdot)$, is defined as:

$$P \equiv \text{Decrypt}_{S_k}(N, A, C, T) \tag{2}$$

The correctness of the output depends on successful tag verification. In the finalization phase, the key is reintroduced, and the authentication tag T is generated. During decryption, the process is executed in reverse, and the plaintext is released when the tag verification is succeeds. As a symmetric cipher, Ascon-AEAD requires that both the sender and receiver share the same secret key. However, it does not specify how this key is to be established. To enable secure key agreement in environments where pre-shared keys are not feasible, an asymmetric key exchange mechanism such as X25519 can be adopted. X25519, based on elliptic-curve Diffie–Hellman over Curve25519, allows two parties to derive a shared secret over an insecure channel. This shared secret can then be processed through a key derivation function (e.g., HKDF) to produce a suitable 128-bit key for use with ASCON. Thus, the integration of X25519 and Ascon-AEAD enables a hybrid cryptographic scheme that combines secure key agreement with efficient lightweight encryption, making it particularly suitable this low power indoor localization application.

B. X25519 (Elliptic Curve Diffie-Helman Key Exchange)

X25519 is an optimized scheme which is developed from Diffie-Helman key exchange and improved using Montgomery curve Curve25519, defined as follow [9, 10, 12, 33]:

$$E : y^2 = x^3 + 486662x^2 + x (\text{mod } p) \tag{3}$$

where $p = 2^{255} - 19$. According to the equation (3), it is produced base point or generator point as (x,y) point at the curve. This base point which called as G is the main value for determining key process of X25519 scheme. This scheme begins by generating a private scalar k at each sender. Then each private scalar k is multiplied by the base point G to obtain the corresponding public key $Q = k\ G$.

After exchanging public keys, both senders independently determined the shared secret key by multiplying their private key and the public key, can be defined as following equation:

$$S_{k_A} = k_A Q_B \rightarrow \text{user A} \quad (4)$$

$$S_{k_B} = k_B Q_A \rightarrow \text{user B} \quad (5)$$

According to the mathematical properties of elliptic curves, both shared secret key results are identical. It means that have same secret point on the curve. In this context k_A and k_B as private scalar from each user A and user B generate the shared secret (S_{kA}, S_{kB}), which is mathematically equivalent in the resulting point. Therefore, the shared secret S_k can be formally expressed as:

$$S_{k_A} = S_{k_B} = S_k \quad (6)$$

This mechanism ensures that the derived key remains confidential even when the communication is intercepted, as the private scalars k_A and k_B are never disclosed. This shared secret key S_k is processed by a Key Derivation Function (KDF) to produce symmetric key which is suitable for encryption and authentication processes especially at Ascon-AEAD.

C. ED25519 (EDSA over Curve25519)

ED25519 as the part of secure digital signature scheme is developed over the twisted Edwards form of Curve25519, which is defined as follows:

$$E : -x^2 + y^2 = 1 + dx^2y^2;\ d = -\frac{121665}{121666} (\text{mod } p) \quad (7)$$

$$p = 2^{255} - 19 \quad (8)$$

In Eq. (7), x and y denote the coordinates of a point on the elliptic curve, d is a constant defining the curve, and p is the prime modulus used for all arithmetic operations on the curve. A base point $G = (x_G, y_G)$ is selected on this curve and serves as the generator for subsequent key computations.

This scheme begins with key generation, where private key a is chosen randomly from the interval $[0, L-1]$, where L is the order of the subgroup generated by G base point. Then, the corresponding public key A is calculated based on G the base point on the elliptic curve at (6), as follow:

$$A = aG \quad (9)$$

During the signing phase, the signer creates a temporary random value r, which is called as nonce by hashing part of the private key h_b together with the message M, as follow:

$$r = \big(H(h_b, M)\big) \text{mod } L \quad (10)$$

Here, h_b is derived from private key and L is the group order. Then, this nonce is used to calculate auxiliary public value R, as follow:

$$R = rG \quad (11)$$

The next step is generated hashing value k using the combination from R, the public key A, and the message M:

$$k = \big(H(R, A, M)\big) \text{mod } L \quad (12)$$

So, the signature scalar is calculated as:

$$S = (r + ka) \text{ mod } L \quad (13)$$

Therefore, the complete signature can be expressed as the pair:

$$\sigma = (R, S) \quad (14)$$

For verification phase, the validator recalculates k values and check this following condition holds:

$$\text{Validation (SG)} = \begin{cases} \text{True, if SG} = R + kA \\ \text{False, if SG} \neq R + kA \end{cases} \quad (15)$$

If this equation is valid, the signature, SG, is confirmed to be authentic and it prove that only the holder of the private key could have generated it. While, the signature will be rejected when the result is different. According to the ED25519 process from the key generation, signing and verification, ensures that have three main process at security level in the form of unforgeability, authenticity and non-repudiation, especially when it also combined by other cryptography scheme.

III. Construction of Proposed System

In this section, we describe our proposed system of secure RSSI-based indoor localization using lightweight authenticated encryption scheme which consist of network topology model and proposed secured data transmission scheme.

A. Network Model Topology

RSSI-based indoor localization as the part of WSN system which have several usage nodes. Those are Anchor Nodes (ANs) as the RSSI data sender or transmitter, Unknown Node (UN) as the target which receiving data continuously from AN, gateway node will be forwarded data from UN to the PC server and PC server will be visualized the result of UN position. The placement ANs are on 0.6 meters height of the wall, while UN, GN and PC server are on 0.3 meters height from the floor. All communication inter-node of this system is using File Transfer Protocol (FTP) via Wi-Fi from Raspberry pi device at ad-hoc network. The realistic scenario system had been placed at indoor environment of electrical engineering department UBAYA lecturer room.

According to Fig. 1, ANs are transmitted to the secured message to the UN every 10 seconds, then UN should wait for the secure message up to 5 seconds. This system is using distributed calculation for estimating the UN position. It means that the estimated position process, including decrypting and authenticating secure messages from ANs, as well as calculating distance and estimated coordinates from RSSI-based values using a trilateration algorithm, occurs at the UN side. By performing these computations locally, the UN reduces communication overhead and enhances data privacy, since sensitive positioning data are not transmitted back to the central server. This distributed approach also minimizes latency and improves the scalability of the indoor positioning system. The UN continuously receives three secured messages from the three nearest ANs for every 2-meter movement.

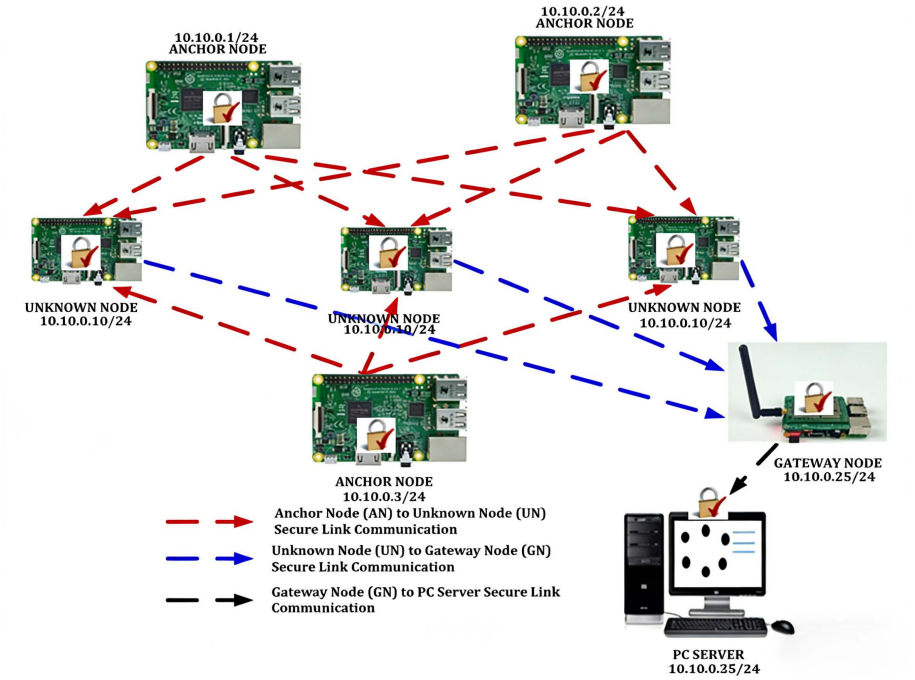

Fig. 1. Network model topology of secure RSSI-based indoor localization.

B. Proposed Lightweight Authenticated Encryption Scheme

In this system, we propose a secure data exchange mechanism for an RSSI-based indoor localization system by integrating multiple modern lightweight cryptographic primitives into a layered security architecture. The proposed scheme employs X25519-based asymmetric cryptography to establish a secure shared secret, which is subsequently used by Ascon-AEAD to provide authenticated encryption ensuring confidentiality and integrity of RSSI data during transmission. Furthermore, SHA-256 is applied to generate a cryptographic hash of the decrypted Ascon-AEAD output, which is then signed using ED25519 digital signatures. This design guarantees strong data origin authentication, message integrity, and non-repudiation of RSSI measurements, which are essential for preventing spoofing and manipulation in indoor localization systems. This system is also equipped timestamp for checking that the message is new and hasn't been replayed. As shown in Fig. 2, the proposed secure lightweight communication scenario is divided into two main processes: the transmitter (Tx) part which is carried out by AN performs timestamp initialization, encryption, message authentication, hashing and signing, while the receiver (Rx) part by UN which performs signature verification, authentication, decryption and also checking the timestamp result.

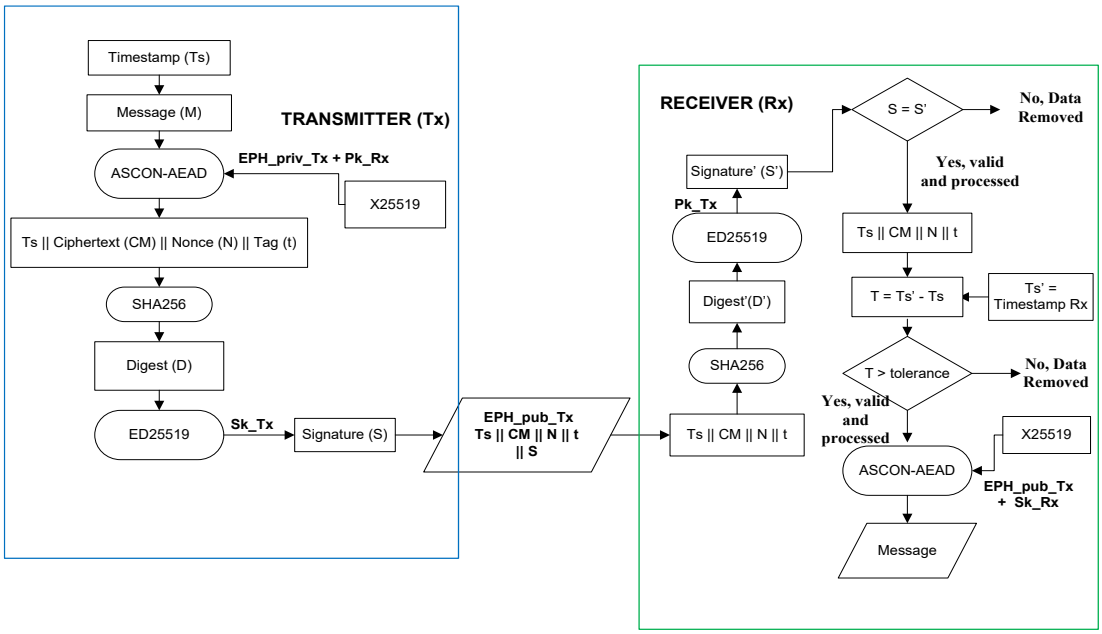

Fig. 2. Proposed lightweight authenticated encryption scheme.

Initially, the transmitter generates a timestamp (TS, 8 bytes) to ensure message freshness and prepares the original message (M, 37 bytes). Both transmitter and receiver generate their own X25519 key pairs. Using an Elliptic Curve Diffie–Hellman (ECDH) process, the transmitter derives a shared session key from its ephemeral private key (EPH_priv_Tx) and the receiver's public key (Pk_Rx). The original message (M) is encrypted using Ascon-AEAD, while the Timestamp (TS) is included as Associated Data (AD). By placing the timestamp in AD, its integrity and authenticity are protected by the AEAD authentication tag without increasing ciphertext size. The encryption process outputs a Ciphertext Message (CM), a nonce (Nonce), and an Authentication Tag (TAG). To provide sender authentication and protect the transmitted data against forgery, the transmitter computes a SHA-256 hash over the authenticated components, including TS||CM||Nonce||TAG, and signs this hash using ED25519 with its private key (Sk_Tx), producing a digital signature (*S*). The final transmitted packet consists of EPH_pub_Tx||TS||CM||Nonce||TAG||S.

Upon reception, the receiver first verifies the digital signature (S) using the sender's ED25519 public key (Pk_Tx) over the hash of TS||CM||Nonce||TAG. If the signature verification fails, the message is immediately discarded without further processing. If the signature is valid, the receiver checks the timestamp (TS) to ensure the message is fresh and within the allowed time window, effectively preventing replay attacks before decryption. Only after both signature and timestamp verification succeed does the receiver reconstruct the shared session key using its X25519 private key (Sk_Rx) and the sender's ephemeral public key (EPH_pub_Tx), and then decrypts the ciphertext (CM) using Ascon-AEAD. A valid authentication tag confirms message integrity and authenticity, and the decrypted message (M) is accepted for further processing.

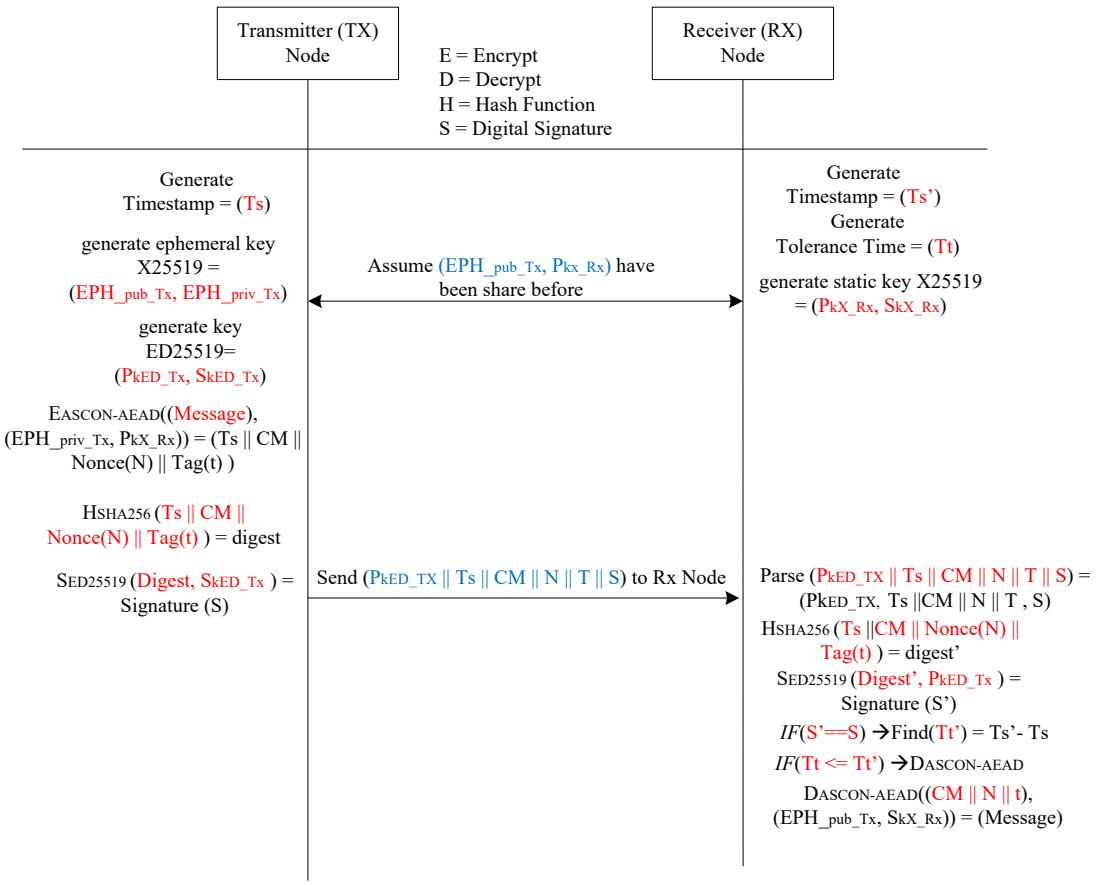

Fig. 3. Proposed secure message transmission scheme.

The overall secure transmission scenario between transmitter and the receiver is illustrated in Fig. 3. The transmitter transmits the complete set of parameters, including EPH_pub_Tx (32 bytes), Ts (8 bytes), CM (37 bytes), Nonce (16 bytes), TAG (16 bytes), and S (64 bytes), obtained from the Ascon-AEAD encryption, SHA-256, ED25519 digital signature operations, to the receiver (totalling approximately 173 bytes for each secure message) for localization computation. This approach ensures end-to-end confidentiality, integrity, authenticity, and message freshness, while maintaining lightweight performance suitable for resource-constrained devices in RSSI-based indoor localization systems.

C. Secure RSSI-Based Indoor Localization

In the proposed secure data transmission scheme, the AN act as the transmitter, sending all necessary parameters required for localization (as illustrated in Fig. 4). The UN receives data from the three nearest ANs and performs computations to estimate its position. Meanwhile, the GN

is responsible for collecting data from the UN and forwarding it to the central server. All information exchanged among AN, UN, GN, and the server is transmitted as secure messages, ensuring confidentiality, integrity, authenticity, and freshness.

There are two types of data frames in this system: (1) data frames from AN to UN, and (2) data frames from UN to GN or from GN to the PC server.

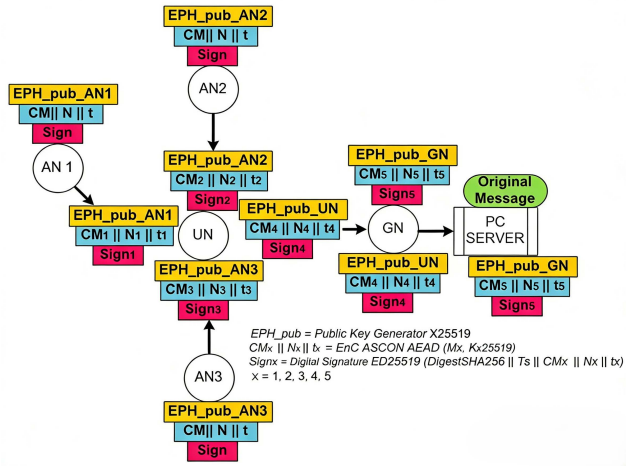

Fig. 4. Secure RSSI-based indoor localization.

ID AN	S	X AN Coordinate	S	Y AN Coordinate	S	PLE	S	RSSI	S	$RSSI_0$	S	Std	S	Route Number
A1	@	5	@	108	@	1.43	@	-48.2	@	-42.6	@	0.04	@	01

Fig. 5. Data frame structure AN to UN communication.

1) Data frame structure AN to UN

The AN sends messages to the UN containing the node ID and parameters required for position estimation. As illustrated in Fig. 5, each data frame includes several pre-determined parameters, such as ID number and the AN coordinates (X, Y), the Path Loss Exponent (PLE) based on the propagation environment, the received signal strength indicator (RSSI) as the main distance estimation parameter, the reference RSSI at 1 meter ($RSSI_0$), the standard deviation of the measurements, and the route number position of UN. These parameters are combined into a single string using a separator character (e.g., "@") before encryption, as the original message.

The combined message (indoor localization parameters, ~37 bytes) is encrypted and authenticated using ASCON-AEAD, producing a ciphertext (CM, 37 bytes), a Nonce (16 bytes), and an authentication tag (TAG, 16 bytes). To ensure authenticity, integrity, and non-repudiation, the SHA-256 digest of Ts||CM||Nonce||TAG is signed using ED25519, resulting in a digital signature (Sign, 64 bytes). The ephemeral X25519 public key of the sender (EPH_pub_Tx, 32 bytes) is also included in the transmitted frame for key agreement. Thus, the total size of the secure data frame sent from AN to MN is approximately 173 bytes, consisting of EPH_pub_Tx||CM||Nonce||TAG||Sign. The proposed scheme provides a lightweight and fixed-length secure structure that achieves higher efficiency compared to other modern cryptographic combinations, while ensuring end-to-end confidentiality, integrity, authenticity, and message freshness for RSSI-based indoor localization systems.

2) Data frame structure UN to GN or GN to server

After receiving the secure message from the ANs, the UN decrypts and authenticates it using the Ascon-AEAD algorithm and the session key derived through X25519 key exchange. Once the message authenticity and freshness are verified, the UN separates the decrypted data according to the parameters required for distance and position estimation. Using the obtained RSSI, path loss exponent (PLE), and standard deviation X_σ values, the UN calculates the estimated distance for each anchor ($d_{i(1,2,3)}$) according to the propagation model, as shown in this following equation [1, 34]:

$$d_{i(1,2,3)} = 10^{\frac{\mathrm{RSSI}_0 - \mathrm{RSSI} + X_\sigma}{10\ \mathrm{PLE}}} \quad (16)$$

Each estimated distance ($d_{i(1,2,3)}$) from AN1, AN2, and AN3 is then used to compute the position estimation using the trilateration algorithm, which also requires the anchor coordinates $\left(X_{\mathrm{AN}i\,(1,2,3\to n=3)}, Y_{\mathrm{AN}i(1,2,3\to n=3)}\right)$. The estimated position (X_{tri}, Y_{tri}) which is derived based on trilateration algorithm, as expressed in this following equation:

$$X_{\mathrm{tri}} = \frac{(D_1(Y_{\mathrm{AN3}} - Y_{\mathrm{AN1}})) - (D_2(Y_{\mathrm{AN2}} - Y_{\mathrm{AN1}}))}{2[(X_{\mathrm{AN2}} - X_{\mathrm{AN1}})(Y_{\mathrm{AN3}} - Y_{\mathrm{AN1}}) - (X_{\mathrm{AN3}} - X_{\mathrm{AN1}})(Y_{\mathrm{AN2}} - Y_{\mathrm{AN1}})]} \quad (17)$$

$$Y_{\mathrm{tri}} = \frac{(D_2(X_{\mathrm{AN2}} - X_{\mathrm{AN1}})) - (D_1(X_{\mathrm{AN3}} - X_{\mathrm{AN1}}))}{2[(X_{\mathrm{AN2}} - X_{\mathrm{AN1}})(Y_{\mathrm{AN3}} - Y_{\mathrm{AN1}}) - (X_{\mathrm{AN3}} - X_{\mathrm{AN1}})(Y_{\mathrm{AN2}} - Y_{\mathrm{AN1}})]} \quad (18)$$

where:

$$D_1 = {d_1}^2 - {d_2}^2 + {X_{\mathrm{AN2}}}^2 - {X_{\mathrm{AN1}}}^2 + {Y_{\mathrm{AN2}}}^2 - {Y_{\mathrm{AN1}}}^2 \quad (19)$$

$$D_2 = {d_1}^2 - {d_3}^2 + {X_{\mathrm{AN3}}}^2 - {X_{\mathrm{AN1}}}^2 + {Y_{\mathrm{AN3}}}^2 - {Y_{\mathrm{AN1}}}^2 \quad (20)$$

The estimated position result is concatenated with the route number and a separator character, as illustrated in Fig. 6, forming a 15-bytes message. A timestamp is then added to ensure message freshness, resulting in a 24-bytes data frame.

Route Number	S	X estimated position Coordinate	S	Y estimated position Coordinate
01	@		@	128.03

Fig. 6. Data frame structure UN to GN or GN to server communication.

This message is then encrypted and authenticated using the Ascon-AEAD algorithm, producing a ciphertext (CM, 16 bytes), a Nonce (16 bytes), and an authentication tag (TAG, 16 bytes). The hash of Ts||CM||Nonce||TAG is generated using SHA-256, and the resulting digest is digitally signed with ED25519, yielding a 64-bytes signature (S). The UN ephemeral X25519 public key (EPH_pub_Tx, 32 bytes) is also included in the transmitted frame. Hence, the total size of the secure data frame sent from the UN to the GN is approximately 152 bytes, consisting of EPH_pub_Tx||Ts||CM||Nonce||TAG||S.

After that, the GN verifies both the ED25519 digital signature and the ASCON-AEAD authentication tag to ensure message integrity and authenticity. Once validated, the GN generates a new timestamp to preserve message freshness, appends it to the verified message, and re-encrypts the complete data using the same ASCON-AEAD procedure before forwarding it to the central server. This process guarantees an end-to-end secure, authenticated,

and freshness-preserved communication flow, while maintaining lightweight performance suitable for real-time RSSI-based indoor localization in resource-constrained systems.

TABLE I: NODE DEVICES SPECIFICATIONS

Nodes	Devices	Specifications
AN1, AN2, AN3, UN, GN	Raspberry Pi 3B	Networking 2.4 GHz 802.11n Wireless CPU 4x ARM Cortex-A53, 1.2 GHz
Server	Laptop Asus ZenBook 14	Networking Wi-Fi 2.4 GHz 802.11 b/g/n, Intel® Core™ i5-8265U (8th Generation, 1.6 GHz base, up to 3.9 GHz Turbo Boost, 4 cores, 8 threads)
Software and OS Addition		
Raspberry Pi OS (64-bit), GCC 11.3.0, C Language, Libsodium (X25519, Ed25519, SHA-256), Ascon-AEAD (Ascon-128), POSIX Socket API		

IV. IMPLEMENTATION AND EXPERIMENTAL MEASUREMENT

In this section, we describe the realistic implementation of secure data transmission using RSSI-based indoor localization scenario. The data length, memory and processor specification will be affected by the effectiveness of this proposed security scheme implementation. The system effectiveness is validated using the performance result from these several data analysis which include data security implementation, measurement of data transmission and evaluation from this proposed security scheme. Several node specifications are also directly influenced to the performance results, which show both software configurations and hardware specification in Table I.

A. Evaluation of Data Security Implementation

The processing time performance of all nodes, including three AN1–AN3, the UN, and the GN, was evaluated under uniform hardware conditions using Raspberry Pi 3 devices. Each node executed a series of lightweight cryptographic operations, including key generation (X25519), authenticated encryption and decryption (Ascon-AEAD), hashing (SHA-256), and digital signature processing (ED25519). The measured parameters also included preparation, synchronization, and timestamping times. As presented in Table II, the synchronization process consistently required the longest non-cryptographic duration, ranging from 2.55 ms to 2.75 ms, reflecting the communication setup time between transmitter and receiver nodes.

The cryptographic computation shows that the Ascon-AEAD algorithm dominates the total processing overhead, with average encryption and decryption times of approximately 11.46 ms and 12.53 ms, respectively. The decryption stage required slightly longer time due to the additional authentication tag verification process inherent to Ascon-AEAD schemes. Key generation using X25519 was relatively stable at around 0.9 ms to 1.0 ms, indicating efficient elliptic-curve scalar multiplication on the Raspberry Pi 3B platform. Meanwhile, the ED25519 signature and verification operations took 1.9 ms to 2.6 ms, with verification consistently longer than signing. The hashing process using SHA-256 contributed minimal delay (below 0.11 ms), showing that its computational footprint is negligible in comparison with AEAD and signature operations.

TABLE II: PROCESSING TIME PERFORMANCE OF EACH NODE

Processing time performance of Transmitter Node							
Transmitter Node	Prepare Time (ms)	Sync. Time (ms)	Timestamp (ms)	Key generation X25519 time (ms)	ASCON-AEAD encrypt (ms)	Hash SHA-256 (ms)	Sign ED25519 (ms)
AN 1 (Pi 3)	0.291	2.568	0.054	0.908	11.527	0.044	1.916
AN 2 (Pi 3)	0.31	2.752	0.05	0.911	11.462	0.043	1.934
AN 3 (Pi 3)	0.318	2.723	0.048	0.911	11.409	0.046	1.914
UN (Pi 3)	0.431	2.557	0.048	1.095	11.485	0.033	2.003
GN (Pi 3)	0.308	2.644	0.047	0.907	11.353	0.038	1.897
Processing time performance of Receiver Node							
Receiver Node	Prepare Time (ms)	Sync. Time (ms)	Timestamp (ms)	Key generation X25519 time (ms)	ASCON-AEAD decrypt (ms)	Hash SHA-256 (ms)	Verify Sign ED25519 (ms)
AN 1 (Pi 3)	0.192	2.576	0.043	0.912	12.53	0.108	2.479
AN 2 (Pi 3)	0.193	2.568	0.055	0.91	12.641	0.112	2.53
AN 3 (Pi 3)	0.194	2.752	0.044	0.914	12.448	0.118	2.632
UN (Pi 3)	0.193	2.723	0.047	0.973	12.42	0.115	2.484
GN (Pi 3)	0.194	2.557	0.0483	1.068	12.638	0.108	2.442

For clarity, the performance evaluation in this section is conducted by comparing the proposed lightweight cryptographic scheme with our previous work, which employed conventional hybrid security architecture based on AES, RSA, and MD5. The comparison focuses specifically on processing time, as this metric is critical for real-time RSSI-based indoor localization systems.

In the previous implementation [1], AES was used as the symmetric encryption algorithm to protect localization data, while RSA was applied to securely distribute the AES session key due to the symmetric nature of AES. In addition, MD5 was employed as a lightweight message digest function to support basic message authentication and integrity verification. Although this hybrid construction fulfilled confidentiality and integrity requirements, it introduced notable computational overhead, particularly due to RSA operations. Experimental results obtained on the same Raspberry Pi 3B platform show that AES and MD5 operations incur minimal processing cost. AES encryption and decryption

require 0.064 ms and 0.105 ms, respectively, while MD5 authentication and verification require only 0.032 ms and 0.112 ms. However, the dominant source of delay in the legacy system arises from RSA processing. While RSA encryption requires 2.164 ms, RSA decryption is significantly more expensive, reaching 60.26 ms, resulting in high processing latency at the receiving node, as shown at Table III.

TABLE III: PROCESSING TIME AVERAGE COMPARISON ON RASPBERRY PI 3B

Cryptographic Scheme	Transmitter Node (ms)	Receiver Node (ms)
RSA-AES-MD5 at Previous work [1]	3.93	69.96
Ascon-AEAD + X25519, SHA-256 + ED25519 at proposed system	17.46	19.01

In the proposed scheme, RSA based key distribution is replaced by X25519, which provides efficient elliptic-curve-based key agreement with substantially lower computational cost. Data confidentiality and integrity are jointly provided using Ascon-AEAD, removing the need for separate encryption and authentication steps. Furthermore, ED25519 digital signatures and SHA-256 hashing are incorporated to provide data origin authentication and non-repudiation, which were not supported in the previous design.

Despite offering enhanced security services, the proposed lightweight scheme achieves a total processing time ranging from 18 ms to 22 ms across all nodes. This indicates a more balanced computational load between transmitting and receiving devices when compared to the previous AES, RSA, and MD5 combination architecture. The delay achieved is acceptable for real-time applications such as secure indoor localization and monitoring, where both confidentiality and low latency are essential.

Then, to achieve secure and efficient indoor localization in resource constrained IoT and wireless sensor network environments, this paper also evaluates the proposed scheme on two different platforms with different purposes. The Raspberry Pi 3B is used to validate the complete end-to-end system, including timestamp verification, key exchange, authenticated encryption, and digital signature verification, under a realistic deployment scenario. In addition, processing time benchmarks are conducted on an ESP32 microcontroller to evaluate the lightweight properties of the cryptographic components. These benchmarks focus on algorithm level performance using the same data frame format, rather than implementing the full indoor localization workflow. The corresponding processing-time results are summarized in Table IV.

TABLE IV: CRYPTOGRAPHIC PROCESSING TIME ON ESP32 MICROCONTROLLER

Cryptographic algorithm	Transmitter node (ms)	Receiver node (ms)
Ascon-AEAD	0.0578	0.0754
SHA-256	0.0816	0.0912
ECDSA	436.28	446.87

In the ESP32 experiments, ECDSA is used instead of ED25519 due to platform limitations, which directly affects the processing time of digital signature operations. The ESP32 evaluation is limited to transmission and reception processing and measures the execution time of individual cryptographic algorithm. The results show that Ascon-AEAD executes in approximately 0.058–0.075 ms, while SHA-256 consistently requires less than 0.1 ms. These results indicate that the symmetric cryptographic operations introduce very low overhead and are suitable for resource-constrained devices. In contrast, ECDSA requires up to 446.87 ms on the ESP32, showing that public key signature operations dominate the computational cost on microcontroller platforms.

On the Raspberry Pi 3B, the processing time of Ascon-AEAD approximately 11–12 ms operation integrated with the X25519 key exchange, while ED25519 signature operations require approximately 2 ms. Thus, the measured latency reflects the cumulative overhead of the complete security process rather than the cost of the Ascon-AEAD primitive alone. In contrast, the significantly higher signature processing time observed on the ESP32 originates from the use of ECDSA instead of ED25519. ECDSA relies on generic elliptic curve arithmetic over prime fields and involves computationally intensive modular operations, which are costly on microcontrollers without dedicated cryptographic hardware acceleration. ED25519, on the other hand, is designed for efficiency and employs optimized curve arithmetic with fixed parameters, resulting in substantially lower computational overhead even on resource limited platforms.

According to the evaluation setups and cryptographic configurations on the Raspberry Pi and ESP32 differ, these results are not intended for direct numerical comparison. Therefore, our future work will focus on implementing the completely proposed system on constrained platforms such as ESP32 or Arduino-class devices, including secure key exchange mechanisms and full indoor localization functionality.

B. Evaluation of Content Data Transmission Phase

In this phase, the transmission performance is evaluated based on message size and communication distance across different node links. The communication between the AN and UN transmits a secure message of 173 bytes, while the communication between the UN and GN, as well as between the GN and the Server, transmits 152 bytes of data. All transmissions are carried out using the File Transfer Protocol (FTP) over Wi-Fi which is embedded on Raspberry Pi 3B hardware. To ensure accurate timing and prevent clock deviation, all nodes are synchronized using the Network Time Protocol (NTP) before the measurements are performed.

The experimental results plotted in Fig. 7 show that transmission time increases progressively with distance from 1 meter to 30 meters. For the 173 bytes message, the transmission time grows from 18.62 ms to 41.00 ms, while for the 152 bytes message, it increases from 18.20 ms to 40.64 ms. This pattern indicates that propagation delay and signal attenuation are the main factors affecting the communication delay as distance increases. Despite the

different message sizes, the resulting transmission times are closely aligned, with deviations of less than 1%, implying that under short-range indoor Wi-Fi conditions, distance has a stronger effect on latency than message size.

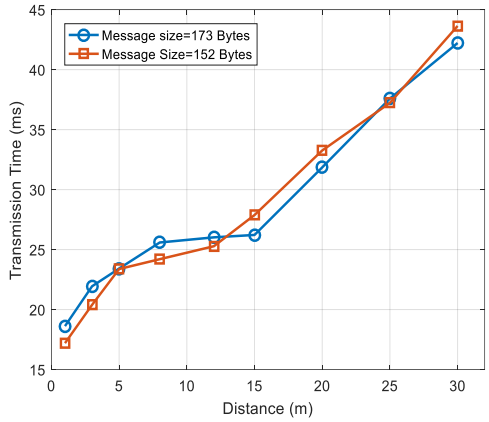

Fig. 7. The influence of time transmission performance to the message size and distance.

Overall, the results confirm that the proposed lightweight security schemes maintain consistent performance across varying message sizes and distances. The minimal impact of payload size on delay shows the efficiency of the implemented lightweight encryption and authentication scheme, which adds negligible overhead to the communication process. Consequently, the system can maintain low latency and stable throughput, meeting the requirements of real-time and secure indoor localization.

C. Evaluation of Proposed Lightweight Security Scheme

This section presents the evaluation of the proposed system security strength by introducing an attacker node that acts as a fake node within the network. The attacker can impersonate any legitimate node, including AN, UN, GN, or Server. The fake node behaves as a transmitter attempting to inject a malicious secure message to disrupt the communication process or to gain access to confidential data. When a fake message is received by a valid node, the verification process using the SHA-256 digest and ED25519 signature is immediately executed. If the verification fails, the message is rejected, and the process is terminated automatically.

The evaluation results show that the layered cryptographic design provides security properties beyond those achievable using authenticated encryption alone. To clarify the necessity of the proposed layered security design, the system behaviour is further analysed under partial compromise scenarios. Although Ascon-AEAD ensures confidentiality and integrity within an established secure communication channel, it does not inherently provide cryptographic proof of data origin once the ciphertext has been successfully decrypted. In contrast, the integration of SHA-256 hashing and ED25519 digital signatures enables independent verification of RSSI data authenticity and origin, even in situations where encrypted packets are logged, forwarded, or analysed outside the original communication session. This additional verification layer effectively prevents forged localization data from being accepted as legitimate, thereby significantly strengthening trust and accountability in indoor localization systems.

Even if the attacker successfully passes the signature phase, decryption using Ascon-AEAD will still fail because the shared session key, derived from the X25519 key exchange, is unique to each session and cannot be reproduced without the legitimate private key. Invalid data from the fake node results in an incorrect authentication tag (TAG) during Ascon verification, thus preventing unauthorized access.

Furthermore, message freshness is ensured through hop-by-hop timestamping across all communication links. A timestamp is appended to each data packet by transmitting node at the AN before sending to the UN, at the UN before forwarding to the GN, and at the GN before transmitting it to the server. Each receiving node verifies the timestamp to ensure temporal validity and to detect replayed or delayed messages. This timestamp is included in the Authenticated Data (AD) during Ascon encryption, allowing the receiver to detect replayed or delayed messages. Upon decryption, the receiver compares the timestamp T_{msg} with its local reception time T_{rcv}. If the absolute time difference ΔT exceeds a predefined threshold of 3 seconds, the message is considered invalid and automatically discarded, as shown to this following equation:

$$\Delta T = \left| T_{\text{rcv}} - T_{\text{msg}} \right| \tag{21}$$

The selected threshold follows the implementation-dependent design principle recommended in NIST [35, 36], where timestamp tolerance is determined by system latency characteristics rather than fixed standard values. In this work, the 3-seconds window is chosen based on empirical observations under indoor Wi-Fi conditions, accounting for clock drift, transmission latency, and processing delays on Raspberry Pi 3B devices, while remaining sufficiently strict to prevent replay attacks. This mechanism balances network delay tolerance with strong replay attack resistance. The verification process incurs negligible computational overhead since the timestamp comparison and threshold evaluation are performed locally at the GN without additional cryptographic operations. Consequently, any retransmission of previously valid data or artificially delayed messages is effectively detected and dropped, ensuring both temporal validity and integrity of the system's communication.

The implementation of the proposed secure transmission framework for indoor localization fulfils the essential security properties of confidentiality, integrity, authenticity, and freshness using lightweight cryptographic primitives optimized for Raspberry Pi hardware. Unlike conventional AEAD based secure channels, the proposed scheme supports non-repudiation by associating RSSI measurements with the originating AN through ED25519 digital signatures over SHA256. After successful verification, the transmitted RSSI or path loss exponent (PLE) values can be attributed to their UNs, which is relevant for forensic analysis, fault diagnosis, and trust evaluation in indoor localization systems. This aspect

is particularly relevant when localization results are employed for access control, asset tracking, or monitoring applications.

Although digital signatures are commonly regarded as more computationally demanding than symmetric cryptographic primitives, experimental results obtained on Raspberry Pi devices indicate that the additional processing overhead introduced by the combined use of SHA-256 hashing and ED25519 signature verification remains below 2 ms per packet. This processing latency remains within acceptable bounds for real-time RSSI-based indoor localization, suggesting that the proposed layered security design maintains a lightweight implementation while providing enhanced security properties.

Data Confidentiality: The location and parameter data are protected using Ascon-AEAD, ensuring both encryption and authentication in a single operation. Since Ascon uses a 128-bit key derived from X25519 key exchange, only the legitimate receiver possessing the corresponding private key can decrypt the ciphertext. The ephemeral key exchange mechanism guarantees that the session key differs for every communication instance, thereby preventing key reuse and data exposure.

Data Integrity and Authenticity: Message integrity and authenticity are verified using the SHA-256 digest and ED25519 digital signature. Any modification of ciphertext or authentication tag during transmission causes immediate verification failure, effectively preventing data tampering and message forgery.

Freshness and Replay Protection: Timestamp verification at the GN ensures the temporal validity of each message. When a delayed or duplicated packet is detected, the receiver rejects the message based on timestamp mismatch. The adopted threshold of 3 seconds provides adequate tolerance for network delay while maintaining robust protection against replay attacks.

Collusion Resistance: In cases where multiple ANs simultaneously transmit data to an unknown node, the inclusion of timestamp and node identity (ID) in the encryption phase prevents collusion and message reuse. Each encrypted packet is uniquely bound to its sender through key agreement and timestamp association, ensuring that trilateration-based localization operates solely with valid, authenticated, and fresh data.

Therefore, the proposed lightweight cryptographic framework not only ensures confidentiality, integrity, authenticity, and freshness, but also provides strong non-repudiation and data provenance guarantees for RSSI-based indoor localization. This layered security approach effectively mitigates impersonation, forgery, replay, and data manipulation attacks while maintaining low computational overhead, making it suitable for real-time deployment in resource constrained WSN and IoT environments.

V. Conclusion

In this paper, we proposed a lightweight secure data transmission scheme for RSSI-based Indoor localization. The proposed cryptographic scheme combines timestamp, X25519 key exchange, Ascon-AEAD encryption, SHA-256 hashing, and ED25519 digital signatures to ensure confidentiality, integrity, authenticity, and data freshness. All nodes, including the Anchor Node (AN), Unknown Node (UN), and Gateway Node (GN), were implemented on Raspberry Pi 3 devices communicating via Wi-Fi using the FTP protocol. Experimental results show that the proposed cryptographic scheme achieves efficient performance, with an average encryption time of 11.4 ms and decryption time of 12.5 ms, while maintaining total node processing time below 20 ms. The transmission test results with 173-bytes, and 152-bytes data sizes indicate stable performance, with transmission delays ranging from 18.2 ms to 41.0 ms over distances up to 30 meters.

These results confirm that the proposed lightweight cryptographic schemes provide strong security with minimal computational overhead, making it suitable for real-time and secure indoor localization applications. In future work, this scheme will be further developed and implemented on low-power devices such as ESP32 and integrated with LoRa-based communication to enable wider coverage and energy-efficient secure transmission across heterogeneous IoT networks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Rafina Destiarti Ainul had programmed the system, data collection, data validation; modeling the system, analyzed the data, wrote the paper, PIC research grant; Djuwari had conceptualization, hardware selection, proofread and error correction; All authors had approved the final version.

Acknowledgment

This research was fully supported by research grant of LPPM Universitas Surabaya.

References

[1] A. R. Destiarti, P. Kristalina and A. Sudarsono, "Secure data transmission scheme for indoor mobile cooperative localization system," in *Proc. 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA),* Surabaya, Indonesia, 2017. doi: 10.1109/ELECSYM.2017.8240378

[2] Y. Cui, J. Li, C. Wang, C. Gu, and W. Liu, "A lightweight key renewal scheme based authentication protocol with configurable RO PUF for clustered sensor networks," *Microelectronics J.*, vol. 117, 105265, July 2021. doi: 10.1016/j.mejo.2021.105265

[3] P. Joshi and B. Mazumdar, "Microelectronics reliability SSFA: Subset fault analysis of ASCON-128 authenticated cipher," *Microelectron. Reliab.*, vol. 123, 114155, Mar. 2021. doi: 10.1016/j.microrel.2021.114155

[4] M. Abdussami, S. Kumar, and T. Al-shehari, "DEAC-IoT: Design of lightweight authenticated key agreement protocol for intra and inter-IoT device communication using ECC with FPGA implementation," *Comput. Electr. Eng.*, vol. 120, 109696, 2024. doi: 10.1016/j.compeleceng.2024.109696

[5] E. Barbierato, S. Caputo, L. Hern, L. Gonz, and L. Mucchi, "KeyEncoder: A secure and usable EEG-based cryptographic key generation mechanism," *Pattern Recognition Letters*, vol. 173, pp. 1–9, Jun. 2023. doi: 10.1016/j.patrec.2023.07.008

[6] G. Chen, J. Huang, J. Zeng, and Y. Zhou, "Journal of network and computer applications SAKA: Scalable authentication and key

agreement scheme with configurable key evolution in edge-fog-multicloud computing environments," *J. Netw. Comput. Appl.*, vol. 242, 104220, Apr. 2025. doi: 10.1016/j.jnca.2025.104220
[7] N. Xiao, Z. Wang, and X. Sun, "A secure and lightweight authentication scheme for digital forensics in industrial internet of things," *Alexandria Eng. J.*, vol. 121, pp. 117–127, Feb. 2025. doi: 10.1016/j.aej.2025.02.059
[8] X. Ding, "Lightweight batch authentication and key agreement scheme for IIoT gateways," *J. Syst. Archit.*, vol. 160, 103368, Feb. 2025. doi: 10.1016/j.sysarc.2025.103368
[9] S. Itoo, F. Syeed, and M. Ahmad, "Sustainable energy, grids and networks ensuring secure connectivity in smart vehicular to grid technology: An elliptic curve-based authentication key agreement framework," *Sustain. Energy, Grids Networks*, vol. 42, 101696, Apr. 2025. doi: 10.1016/j.segan.2025.101696
[10] C. Patel, A. Kashif, A. Ali, and R. Jhaveri, "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element," *Digit. Commun. Networks*, vol. 9, no. 2, pp. 358–366, 2023. doi: 10.1016/j.dcan.2022.11.001
[11] U. Ali, Y. I. B. Idris, J. Frnda *et al.*, "Enhanced Lightweight and Secure Certificateless Authentication Scheme (ELWSCAS) for internet of things environment", *Internet of Things*, vol. 24, 100923, Sep. 2023. doi: 10.1016/j.iot.2023.100923
[12] A. Arias-jimenez and J. Gallego-madrid, "Internet of things lightweight authenticated key exchange for low-power IoT networks using EDHOC," *Internet of Things*, vol. 31, 101539, Jan .2025. doi: 10.1016/j.iot.2025.101539
[13] J. Kaur, S. Florida, and U. States, "A survey on the implementations, atacks, and countermeasures of the NIST lightweight cryptography standard: ASCON", *ACM Comput. Surv.* vol. 58, no. 1, 6, January 2026. doi: 10.1145/3744640
[14] V. S. Laborda, L. Hernández-Alvarez, L. H. Encinas, J. I. S. García, and A. Queiruga-Dios, "Study about the performance of ascon in arduino devices," *Applied Sciences*, vol. 15, no. 7, 4071 2025. doi: 10.3390/app15074071
[15] G. Nwatuzie, O. M. Ijiga, I. P. Idoko, L. A. Enyejo, and E. O. Ali, "Design and evaluation of a user-centric cryptographic model leveraging hybrid algorithms for secure cloud storage and data integrity," *American Journal of Innovation in Science and Engineering*, vol. 4, no. 2, pp. 49–65, 2025. doi: 10.54536/ajise.v4i2.4482
[16] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "A ASCON v1.2: Lightweight authenticated encryption and hashing," *Journal of Cryptology*, vol. 34, 33, 2021. doi: 10.1007/s00145-021-09398-9
[17] M. A. Jimale, M. R. Z'aba, M. L. M. Kiah *et al.*, "Authenticated encryption schemes: A systematic review," *IEEE Access*, vol. 10, pp. 14739–14766, 2022. doi: 10.1109/ACCESS.2022.3147201
[18] A. R. Alharbi, A. Aljaedi, A. Aljuhni, M. K. Alghuson, and S. S. Jamal, "Evaluating ascon hardware on 7-series FPGA devices," *IEEE Access*, vol. 12, pp. 149076–149089, 2024. doi: 10.1109/ACCESS.2024.3471694
[19] V. Bangera, Z. Amrin, and C. Engineering, "WSN in defence field: A security overview," in *Proc. Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2020, pp. 258–264. doi: 10.1109/I-SMAC49090.2020.9243406
[20] G. Cagua, V. Gauthier-Umaña and C. Lozano-Garzon, "Implementation and performance of lightweight authentication encryption ASCON on IoT devices," *IEEE Access*, vol. 13, pp. 16671–16682, 2025. doi: 10.1109/ACCESS.2025.3529757
[21] O. Sabri, B. Al-shargabi, A. Abuarqoub, and T. A. Hakami, "A lightweight encryption method for IoT-based healthcare applications: A review and future prospects," *IoT*, vol. 6, no. 3, 23, 2025. doi: 10.3390/iot6020023
[22] S. Koteshwara, A. Das, and I. Corporation, "Comparative study of authenticated encryption targeting lightweight IoT applications," *IEEE Design & Test*, vol. 34, no. 4, pp. 26–33, Aug. 2017. doi: 10.1109/MDAT.2017.2682234
[23] P. Rosa, "Light-SAE : A lightweight authentication protocol for large-scale iot environments made with constrained devices," *IEEE Trans. on Network and Service Management*, vol. 20, no. 3, pp. 2428–2441, 2023. doi: 10.1109/TNSM.2023.3275011
[24] Z. Lv, W. Zhang, N. Li, C. Chen and J. Cai, "A highly reliable lightweight distribution network communication encryption scheme," in *Proc. 2019 IEEE International Conference on Power Data Science (ICPDS)*, Taizhou, China, 2019, pp. 11–14. doi: 10.1109/ICPDS47662.2019.9017202
[25] S. Khan, K. Inayat, F. B. Muslim *et al.*, "Securing the IoT ecosystem: ASIC-based hardware realization of Ascon lightweight cipher," *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3653–3664, 2024. doi: 10.1007/s10207-024-00904-1
[26] R. I. Devices, I. Radhakrishnan, and S. Jadon, "Efficiency and security evaluation of lightweight cryptographic," *Sensors,* vol. 24, no. 12, 4008. doi: 10.3390/s24124008
[27] C. Lefevre and B. Mennink, "SoK: Security of the ascon modes," *IACR Trans. Symmetric Cryptol.*, vol. 2025, no. 1, pp. 138–210, 2025. doi: 10.46586/tosc.v2025.i1.138-210
[28] K. Nguyen, G. S. Member, T. Dang, and G. S. Member, "ASIC implementation of ASCON lightweight cryptography for IoT applications," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 72, no. 1, pp. 278–282, 2025. doi: 10.1109/TCSII.2024.3483214
[29] I. Elsadek E. Elgendy, S. Abouzeid *et al.*, "State-of-the-art ASCON ASIC achieving," *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 72, no. 8, pp. 4021–4030, 2025. doi: 10.1109/TCSI.2024.3522193
[30] Joint Task Force, "Security and privacy controls for information systems and organizations," *NIST Special Publication 800-53*, rev. 5, Gaithersburg, MD, USA, Sept. 2020. doi: 10.6028/NIST.SP.800-53r5
[31] E. Barker, L. Chen, A. Roginsky, and M. Smid, "Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography," *NIST Special Publication 800-56A*, rev. 2, Gaithersburg, MD, USA, May 2013. doi: 10.6028/NIST.SP.800-56Ar2
[32] L. Chen, D. Moody, A. Regenscheid, A. Robinson, and K. Randall, "Recommendations for discrete logarithm-based cryptography: elliptic curve domain parameters," *NIST Special Publication 800-186*, Gaithersburg, MD, USA, Feb. 2023. doi: 10.6028/NIST.SP.800-186
[33] A. Langley, M. Hamburg, and S. Turner, "Elliptic curves for security," *Informational, Internet Research Task Force (IRTF)*, RFC 7748, Jan. 2016. doi:10.17487/RFC7748
[34] R. Destiarti A, P. Kristalina, and A. Sudarsono, "SWOT: Secure wireless object tracking with key renewal mechanism for indoor wireless sensor network," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 2, pp. 520–531, Mar. 2018. doi: 10.18517/ijaseit.8.2.5268
[35] M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," *NIST Special Publication 800-38D*, Gaithersburg, MD, USA, Nov. 2007. doi: 10.6028/NIST.SP.800-38D
[36] A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines", *NIST Special Publication 800-63-3*, Gaithersburg, MD, USA, June 2017. doi: 10.6028/NIST.SP.800-63-3

Rafina Destiarti Ainul Rafina Destiarti Ainul earned her B.Eng. degree in telecommunication engineering from Politeknik Elektronika Negeri Surabaya (PENS), Indonesia, in 2015, and received her M.Eng. degree in electrical engineering from the same institution in 2017. She joined the University of Surabaya (UBAYA) as a full-time faculty member in 2018 and is currently serving as an assistant lecturer in the Department of Electrical Engineering. She is actively involved in the telecommunication engineering specialization, where she teaches courses and supervises student projects related to wireless communications and embedded systems. Her primary research interests lie in the development and optimization of Indoor Positioning Systems (IPS), with a particular emphasis on IoT integration, location-aware services, and lightweight network security mechanisms to support smart environments. In addition to her teaching and research, she has participated in various interdisciplinary projects involving real-time positioning, mobile applications, and geofencing technologies for smart campus and smart mobility solutions. She has authored more than 20 research papers in reputable national and international journals and conference proceedings.

Djuwari earned his B.Eng. degree in electrical engineering from Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia, in 1997, and completed his Ph.D. degree in telecommunications engineering at the Royal Melbourne Institute of Technology (RMIT), Australia, in 2006. He is currently a faculty member in the Department of Electrical Engineering at the University of Surabaya (UBAYA), where he teaches courses and supervises research in telecommunications and signal processing. His primary research interests include digital signal processing, wireless communication systems, and advanced telecommunication technologies for emerging network applications. In addition to his academic role, he has been involved in various interdisciplinary projects related to communication system design, signal analysis, and network performance optimization. He has authored 11 research papers published in national and international journals and conference proceedings.