Contents lists available at IdNNS
Indonesian Journal of Machine Learning and Intelligent Systems
Volume X ; Issue X
journal homepage: https://journal.idnns.org/index.php/ijmlis

Speck-64/128 Encrypted LoRa V2V Communication: Security-Performance Trade-off in Mining Environments

Desi Marlena[a,*], Hendra Fernanda[a], Dion Ogi[a] and Zaky Fahri Alfiansyah[a]

[a] *Cryptographic Hardware Engineering, Politeknik Siber dan Sandi Negara, Bogor, Indonesia*

ARTICLE INFO

Keywords:
Embedded Security
Lightweight Cryptography
LoRa V2V Communication
Mining Vehicle Safety
Security–Performance Trade-off

ABSTRACT

Mining operations require reliable and protected Vehicle-to-Vehicle (V2V) communication in infrastructure-constrained environments. This study presents the design, implementation, and evaluation of a LoRa-based V2V communication system integrated with Speck-64/128 lightweight encryption on ESP32 nodes using LoRa SX1278 modules at 433 MHz. Unlike previous studies that separately evaluate LoRa communication and lightweight cryptography, this work provides an integrated system-level evaluation across communication delay, calculated Time on Air (ToA), power consumption, RSSI, and payload confidentiality under evaluated sniffing and spoofing scenarios. Controlled experiments ($n = 20$) compared unencrypted and encrypted configurations. Results show that encryption increased mean communication delay from 27.5 ms to 116.35 ms, while mean power consumption increased slightly from 0.571 W to 0.599 W. Payload interpretation success during the evaluated attack scenarios decreased from 100% to 0% in the encrypted configuration. ToA analysis across SF7–SF12 further indicates that LoRa physical-layer parameters contribute more significantly to overall transmission delay than cryptographic computation. These findings demonstrate that lightweight encryption can improve payload confidentiality with acceptable communication and energy overhead for low-rate V2V warning systems in mining environments.

1. Introduction

Vehicle collision remains one of the dominant safety hazards in mining operations, frequently caused by excessive speed, delayed braking, and limited situational awareness among heavy-duty vehicle operators in dynamic, low-visibility environments (Sanmiquel et al., 2024; Kecojevic et al., 2007). Accident analyses consistently indicate that failures in inter-vehicle coordination and communication significantly contribute to collision incidents, highlighting the critical need for reliable vehicle communication mechanisms (Qian et al., 2022).

Vehicle-to-Vehicle (V2V) communication has been widely proposed as a solution to improve operational safety by enabling direct exchange of critical data such as speed, position, and warning signals (Abboud et al., 2016; Soto et al., 2022; Abdul Razak et al., 2023). Conventional V2V technologies, including Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X), offer low communication delays and high reliability for vehicular communication (Abboud et al., 2016; Storck and Duarte-Figueiredo, 2020). Several studies have demonstrated the effectiveness of DSRC-based communication for cooperative collision warning systems (Chehri et al., 2020; Xiang et al., 2014). However, these technologies rely heavily on fixed communication infrastructure. Their deployment complexity further limits applicability in remote and infrastructure-constrained environments such as mining sites (Abdelkader et al., 2021; Beaulieu et al., 2015).

In contrast, Low Power Wide Area Network (LPWAN) technologies, particularly LoRa (Long Range), have emerged as a promising alternative for vehicular communication due to their long-range capability, low power consumption, and flexible deployment characteristics (Augustin et al., 2016). Unlike conventional V2V technologies, LoRa communication can operate with minimal infrastructure requirements, making it

*Corresponding author
desi.marlena@poltekssn.ac.id (D. Marlena);
hendra.fernanda@bssn.go.id (H. Fernanda);
dion.ogi@poltekssn.ac.id (D. Ogi);
zaky.fahri@student.poltekssn.ac.id (Z.F. Alfiansyah)
ORCID(s):

suitable for mining environments where network availability is limited (Torres et al., 2021; Vinodhini and Rajkumar, 2023). Prior studies have demonstrated the feasibility of LoRa-based V2V communication in terms of communication coverage, energy efficiency, and mobility support (Sanmiquel et al., 2024; Kecojevic et al., 2007; Qian et al., 2022; Abboud et al., 2016; Abdul Razak et al., 2023; Torres et al., 2021; Haque et al., 2020b,a). Nevertheless, LoRa communication is inherently constrained by lower data rates and higher communication delay compared to DSRC or C-V2X systems (Zadobrischi and Havriliuc, 2024).

Despite these advantages, the integration of encrypted communication mechanisms in LoRa-based V2V systems remains insufficiently explored, particularly in safety-critical environments. Due to the broadcast nature of wireless communication, LoRa systems are vulnerable to various attacks, including eavesdropping, spoofing, and man-in-the-middle attacks (Conti et al., 2016; Tzoannos et al., 2024). Recent studies have also investigated physical-layer security and encrypted communication mechanisms for IoT- and V2V-based systems (Farraj and Hammad, 2024; Gupta et al., 2021; Aliev et al., 2020). In mining operations, such vulnerabilities may lead to incorrect warnings or manipulated vehicle information, potentially resulting in severe operational accidents.

To address these challenges, lightweight cryptographic algorithms have been proposed for resource-constrained embedded and IoT systems (Thakor et al., 2021; El-hajj et al., 2023). Among these, the Speck family of lightweight block ciphers has gained attention due to its simple ARX (Add-Rotate-XOR) structure and efficient implementation on embedded devices (Beaulieu et al., 2015; Usman et al., 2017). Compared to conventional cryptographic algorithms, lightweight ciphers provide lower computational overhead while maintaining adequate security levels for constrained systems (Thakor et al., 2021).

However, integrating encryption into real-time communication systems inevitably introduces additional communication delay and energy consumption, potentially affecting system responsiveness. In V2V communication, where timely data exchange is critical, this creates an important trade-off between security and performance. Existing studies generally evaluate LoRa-based communication or lightweight cryptography independently, without analyzing their combined interaction at the system level.

To address this gap, this study integrates Speck-64/128 encryption into a LoRa SX1278-based V2V prototype implemented on ESP32 nodes and provides a comprehensive system-level evaluation of the resulting security–performance trade-off. The proposed system is evaluated using five metrics, namely communication delay, calculated Time-on-Air (ToA), power consumption, RSSI, and payload interpretation outcomes under simulated attack scenarios. The study contributes to the development of an encrypted LoRa-based V2V communication system designed for infrastructure-constrained mining environments. In addition, Speck-64/128 lightweight encryption is integrated and implemented on an ESP32 embedded platform to enhance communication security while maintaining low computational overhead. Furthermore, a comparative experimental evaluation between encrypted and unencrypted communication scenarios is conducted to analyze the impact of lightweight encryption on communication performance and security characteristics across multiple operational metrics.

Vehicle safety in mining environments has received significant research attention, particularly regarding collision avoidance and risk mitigation. Vehicle-related accidents remain a dominant safety hazard, frequently caused by limited visibility, reduced operator awareness, and insufficient inter-vehicle coordination (Sanmiquel et al., 2024; Qian et al., 2022; Kim and Choi, 2022). Proposed solutions include computer vision-based detection and proximity warning systems (Kim and Choi, 2022; Imam et al., 2023). However, these approaches are highly sensitive to environmental conditions such as dust, poor lighting, and occlusion, reducing reliability in harsh mining environments.

To overcome these limitations, communication-based V2V systems have been widely explored. Conventional V2V technologies, including Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X), have demonstrated low communication delay and high reliability in vehicular communication (Abboud et al., 2016; Soto et al., 2022; Storck and Duarte-Figueiredo, 2020). Several studies have implemented DSRC-based collision warning systems and cooperative communication protocols to improve traffic safety (Chehri et al., 2020; Xiang et al., 2014). Nevertheless, their reliance on fixed infrastructure and deployment complexity limits their applicability in remote or infrastructure-constrained environments such as mining sites (Abdelkader et al., 2021; Lu et al., 2014; Jadaan et al., 2017).

In this context, Low Power Wide Area Network (LPWAN) technologies, particularly LoRa, have emerged as a viable alternative for vehicular communication. LoRa provides long communication range, low power consumption, and flexible deployment without requiring extensive infrastructure (Augustin et al., 2016). Prior studies have demonstrated the feasibility of LoRa-based V2V communication in terms of coverage, reliability, and energy efficiency (Torres et al., 2021; Vinodhini and Rajkumar, 2023; Haque et al., 2020b,a). Experimental evaluations confirm that LoRa maintains stable performance under vehicle mobility scenarios (Haque et al., 2020a). Other works extend its application to intelligent transportation systems and lane-change warning systems (Abdul Razak et al.,

2023; Vinodhini and Rajkumar, 2023; Soy et al., 2025). However, most existing studies focus primarily on communication performance, with limited attention to integrated security mechanisms in real-time vehicular systems.

Security remains a critical concern in wireless V2V communication. Due to the broadcast nature of wireless channels, such systems are inherently vulnerable to various attacks, including eavesdropping, spoofing, and man-in-the-middle attacks (Conti et al., 2016; Tzoannos et al., 2024). Recent studies have also investigated physical-layer security approaches and encrypted communication mechanisms for IoT- and V2V-based systems (Abdul Razak et al., 2023; Farraj and Hammad, 2024; Aliev et al., 2020). Although these approaches improve security, they often introduce significant computational overhead, limiting suitability for resource-constrained embedded systems in real-time environments.

Lightweight cryptographic algorithms have been proposed to address security in resource-constrained systems. Thakor et al. (2021) provide a comparative evaluation of lightweight ciphers for IoT devices, while El-hajj et al. (2023) benchmark these algorithms on embedded hardware platforms. The Speck and Simon cipher families, proposed by Beaulieu et al. (2015), offer efficient ARX-based implementations particularly suited to 32-bit microcontrollers. Additional studies have explored lightweight encryption schemes for embedded IoT systems (Usman et al., 2017). However, these works focus primarily on computational efficiency and cryptographic strength, without evaluating the combined impact of encryption on real-time LoRa-based vehicular communication. Despite these advancements, existing research treats LoRa-based V2V communication and lightweight cryptography as separate domains, with no comprehensive system-level study jointly evaluating both within a safety-critical embedded platform.

As shown in Table 1, existing studies primarily focus on individual aspects such as communication performance, security mechanisms, or lightweight cryptographic efficiency. Vision-based approaches are limited by environmental conditions, while conventional V2V technologies rely heavily on infrastructure support. While LoRa-based systems offer deployment flexibility, they largely lack integrated security mechanisms. Lightweight cryptography studies similarly focus on computational efficiency without evaluating real-time communication impact. This underscores the need for the integrated approach proposed in this study.

2. Method

This study adopts a quantitative experimental approach to evaluate the security–performance trade-off

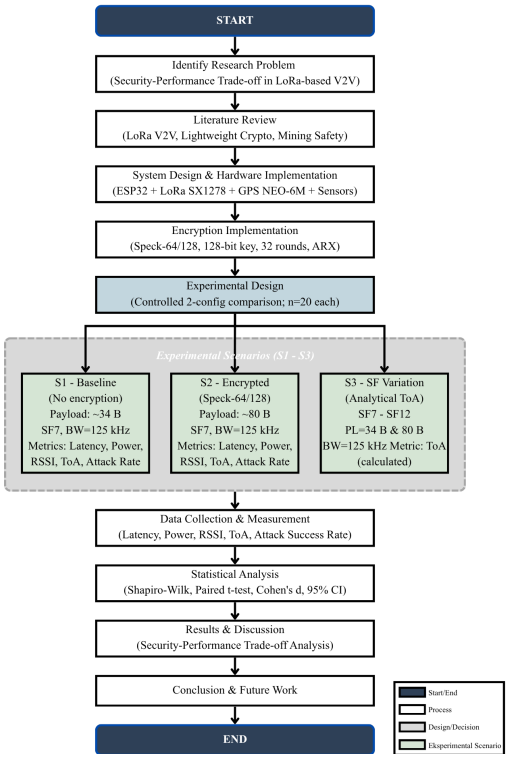


Figure 1: Research methodology flowchart: from problem identification to conclusion, including experimental scenarios S1 (Baseline), S2 (Encrypted), and S3 (SF Variation).

of integrating Speck-64/128 encryption into a LoRa-based Vehicle-to-Vehicle (V2V) communication system. The methodology is designed to enable controlled comparison between encrypted and unencrypted configurations under identical conditions, ensuring objective measurement of system performance and security. The overall research methodology workflow is illustrated in Fig. 1.

The research methodology proceeds sequentially through five preparatory stages before branching into three parallel experimental scenarios. The process begins with the identification of the research problem, followed by a structured literature review covering LoRa-based V2V communication, lightweight cryptography, and mining vehicle safety.

Based on the literature, the system is designed and physically implemented using an ESP32 microcontroller, LoRa SX1278 transceiver, GPS module, and supporting sensors, after which the Speck-64/128 encryption algorithm is integrated into the firmware. The experimental design stage defines the controlled two-configuration comparison framework with $n = 20$ measurements per scenario. The methodology then branches into three parallel experimental scenarios. S1 (Baseline) evaluates system performance without encryption using a 34-byte plaintext payload at SF7. S2 (Encrypted) applies the same radio configuration with Speck-64/128 encryption active, expanding the payload

Table 1
Comparison of related works and research gap.

Reference	Research focus	Technology	Security aspect	Main contribution	Limitation
Sanmiquel et al., 2024; Kecojevic et al., 2007; Jadaan et al., 2017	Mining vehicle safety and accident analysis	Mining monitoring	None	Collision risk identification	No real-time communication framework
Kim and Choi, 2022; Imam et al., 2023	Collision avoidance and warning systems	CV / AI	None	CV-based collision detection	Sensitive to dust, lighting, and occlusion
Abboud et al., 2016; Soto et al., 2022; Storck and Duarte-Figueiredo, 2020; Chehri et al., 2020; Xiang et al., 2014	Conventional V2V communication	DSRC / C-V2X	Basic	Low-latency vehicular communication	Infrastructure dependency
Abdul Razak et al., 2023; Torres et al., 2021; Haque et al., 2020b,a	LoRa-based vehicular communication	LoRa / LPWAN	Limited	Long-range LPWAN feasibility	Limited integrated security evaluation
Chehri et al., 2020; Conti et al., 2016; Tzoannos et al., 2024; Farraj and Hammad, 2024; Aliev et al., 2020	Wireless communication security	IoT security	Authentication and mitigation	Secure V2V communication mechanisms	Additional computational overhead
Beaulieu et al., 2015; Thakor et al., 2021; Elhajj et al., 2023; Usman et al., 2017	Lightweight cryptography for embedded systems	Lightweight ciphers	Lightweight encryption	Efficient cryptography for constrained devices	Limited real-time V2V analysis
This work	Encrypted LoRa-based V2V communication for mining	LoRa SX1278 + ESP32	Speck-64/128	Integrated evaluation of delay, ToA, RSSI, power, and payload confidentiality	Prototype-scale evaluation

Source: Compiled by authors based on related literature review.

to 80 bytes. S3 (SF Variation) analytically characterizes Time on Air (ToA) across SF7 to SF12 for both payload sizes, isolating the contribution of LoRa physical-layer parameters to overall communication delay.

The results are then synthesized into a security–performance trade-off analysis, leading to conclusions and recommendations for future work.

2.1. System Overview

Fig. 2 illustrates the overall system architecture, including sensing, processing, encryption, and wireless communication components. Each vehicle node consists of a GPS module, a speed sensor, an ESP32 microcontroller, and a LoRa transceiver (SX1278). The GPS module provides real-time geographic coordinates, while the speed sensor measures vehicle velocity.

These data are processed by the ESP32 and formatted into a data packet containing vehicle ID, speed, latitude, and longitude. In the encrypted configuration, the data packet is segmented into fixed-size blocks and encrypted using the Speck-64/128 algorithm before transmission. In the baseline configuration, the data are transmitted in plaintext. The packet is then transmitted via LoRa to the receiving node.

Upon reception, the receiving node processes the packet by performing decryption (if enabled) and parsing the data. The decoded information is displayed on an OLED screen, and an alert is triggered if predefined conditions are met, such as excessive speed (> 48 km/h) or sudden deceleration (< -0.45 g). Both nodes operate as transceivers, enabling bidirectional real-time communication.

2.2. Experimental Design

This study employs a controlled two-configuration experimental design. Configuration 1 (C1) uses LoRa-based V2V communication without encryption, while Configuration 2 (C2) applies Speck-64/128 lightweight encryption to the same system.

The independent variable in this study is the encryption configuration (C1 vs. C2). The evaluated metrics include communication delay, calculated Time on Air (ToA), power consumption, RSSI, and success rate under the evaluated sniffing and spoofing scenarios. Several variables were held constant across all experiments to ensure comparability: the hardware platform, LoRa radio parameters, packet transmission interval (1 second), packet structure, communication distance, and testing environment conditions.

Each configuration was measured $n = 20$ times under identical conditions. The repeated-measurement approach reduces random variation and improves result reliability. Each encrypted measurement was paired with the corresponding unencrypted measurement collected under identical transmission direction, radio configuration, and experimental conditions.

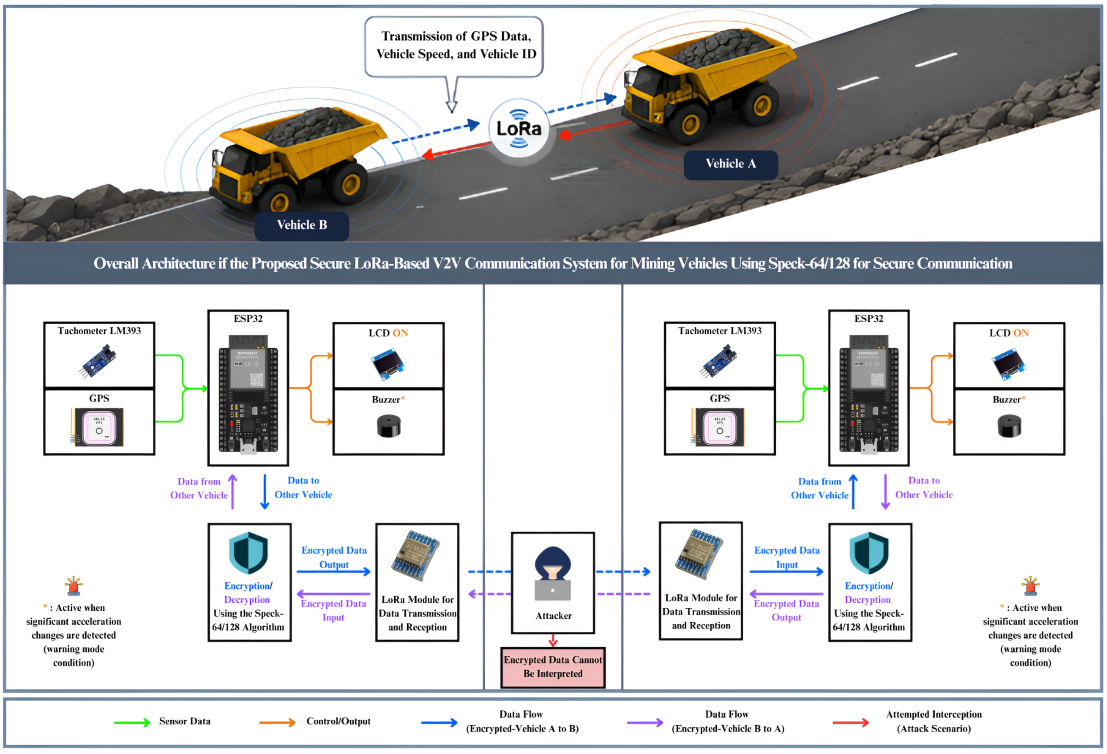


Figure 2: Overall system architecture of the proposed LoRa-based V2V communication node.

2.3. Hardware Implementation

Each vehicle communication node is implemented on an ESP32 microcontroller responsible for sensor data acquisition, Speck-64/128 encryption and decryption, LoRa communication management, warning logic execution, and real-time data display. The wireless subsystem uses a LoRa SX1278 transceiver at 433 MHz for long-range V2V communication, while a GPS NEO-6M module provides vehicle positioning. An LM393 speed sensor monitors wheel rotation to estimate vehicle speed. A 3.7 V 1500 mAh Li-Po battery powers the entire node, enabling fully decentralized operation without relying on external communication infrastructure. The complete hardware specification is summarized in Table 2. Fig. 3 shows the hardware implementation results of the proposed LoRa-based V2V.

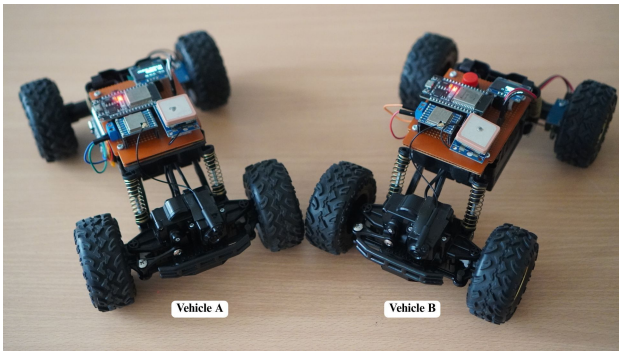


Figure 3: Implementation results of the proposed LoRa-based V2V hardware.

2.4. LoRa Communication Configuration

The proposed V2V communication system uses LoRa SX1278 modules at 433 MHz (ISM band). The radio parameters were selected to balance communication range, communication delay, and reliability under mining operational conditions: bandwidth of 125 kHz, coding rate 4/5, preamble length of 8 symbols, CRC enabled, and explicit header mode. For the communication delay and power measurements (Scenarios S1 and S2), the Spreading Factor was fixed at SF7 to minimize Time on Air. SF7 through SF12 were evaluated analytically in Scenario S3 to characterize their impact on calculated ToA. The complete parameter configuration is listed in Table 3.

The increase in payload size is primarily caused by the block-based encryption process and hexadecimal encoding representation of encrypted data. This payload expansion directly affects the LoRa calculated Time on Air (ToA), resulting in longer transmission duration for encrypted communication. The ToA is expressed as:

$$T_{packet} = T_{preamble} + T_{payload} \tag{1}$$

$$T_{preamble} = (n_{preamble} + 4.25) \times T_{sym} \tag{2}$$

$$T_{payload} = \Big(8 + \max\Big(\Big\lceil \frac{8PL - 4SF + 28 + 16CRC - 20IH}{4\,(SF - 2DE)} \Big\rceil$$

Table 2
Hardware specification of vehicle communication node.

Component	Model / Type	Key specifications	Quantity	Role in system
Microcontroller	ESP32 (WROOM32)	Dual-core Xtensa LX6, 240 MHz; 520 KB SRAM; 4 MB Flash; 3.3 V	1 per node	Central processing, encryption, communication control
LoRa Transceiver	SX1278 (Ra-02)	433 MHz; TX power up to 17 dBm; RX sensitivity -148 dBm; SPI interface	1 per node	Long-range wireless V2V communication
GPS Module	NEO6M	UART interface; position accuracy $<$ 2.5 m CEP; update rate 1–5 Hz	1 per node	Vehicle position acquisition
Speed Sensor	LM393 (IR encoder)	Digital pulse output; comparator-based; 3.3–5 V supply	1 per node	Wheel rotation/vehicle speed estimation
OLED Display	SSD1306 (0.96")	128×64 pixels; I2C interface; 3.3–5 V supply	1 per node	Real-time data display and warning notification
Buzzer	Active buzzer (5 V)	Digital trigger via GPIO; audible alert on warning condition	1 per node	Audible collision/overspeed warning
Push Button	Tactile switch	GPIO digital input with pull-up resistor	1 per node	Manual emergency alert trigger
Power Supply	Li-Po battery	3.7 V, 1500 mAh; supplies ∼0.572–0.599 W during operation	1 per node	Portable battery-powered embedded operation

Source: Authors' hardware implementation; component datasheets (Espressif ESP32, Semtech SX1278, u-blox NEO-6M, Solomon Systech SSD1306).

$$\times (CR+4), 0)\Big) \times T_{sym} \tag{3}$$

$$T_{sym} = \frac{2^{SF}}{BW} \tag{4}$$

in which PL is the payload length (bytes), SF the Spreading Factor, CR the Coding Rate, and T_{sym} the symbol duration (Semtech Corporation, nd). Consequently, the communication delay is influenced not only by cryptographic overhead but also by increased physical-layer transmission time. Expanding from 34 bytes to 80 bytes directly increases ToA and therefore observed communication delay.

2.5. Encryption Implementation

The Speck-64/128 lightweight block cipher was implemented on the ESP32 platform using a custom software-based cryptographic library. The algorithm operates on 64-bit data blocks with a 128-bit symmetric key over 32 encryption rounds.

In the encrypted communication configuration, the plaintext payload was segmented into 8-byte blocks and encrypted sequentially prior to LoRa transmission. At the receiver node, the received ciphertext was decrypted and reconstructed into its original data format before subsequent processing and display. A pre-shared 128-bit symmetric key is initialized at system startup and shared between both nodes prior to deployment. No dynamic key exchange mechanism was implemented, as this study focuses specifically on evaluating the performance impact of static-key lightweight encryption in a LoRa-based V2V context.

The encryption was implemented using Electronic Codebook (ECB) mode. The use of ECB mode may introduce potential pattern leakage because identical plaintext blocks produce identical ciphertext blocks. Although this limitation is well known in cryptographic literature (Beaulieu et al., 2015; Thakor et al., 2021), its practical impact in this study is reduced by the short and dynamic nature of the transmitted V2V payloads, which rarely contain repeated block patterns. ECB was selected primarily due to its implementation simplicity and minimal computational overhead on the resource-constrained ESP32 platform. Nevertheless, authenticated encryption modes such as CCM and GCM are recommended for production-scale deployment to provide both confidentiality and message integrity.

Table 3
LoRa SX1278 communication parameter configuration.

Parameter	Value	Remarks
Carrier Frequency	433 MHz	ISM band
Bandwidth (BW)	125 kHz	Fixed throughout experiments
Spreading Factor (SF)	SF7 (fixed); SF7–SF12 (ToA analysis)	Higher SF = longer range, higher ToA
Coding Rate (CR)	4/5	Minimum overhead
Preamble Length	8 symbols	LoRa default
CRC	Enabled	Error detection active
Implicit Header (IH)	Disabled (Explicit Header)	IH = 0
Low Data Rate Optimize (DE)	Disabled (SF $\leq$ 10)	DE = 0
Sync Word	0x12 (Private network)	Dedicated V2V network
TX Output Power	17 dBm	Max. SX1278 output
Receiver Sensitivity	-148 dBm (SF12)	Semtech SX1278 datasheet
Packet Transmission Interval	1 second	Fixed throughout experiment
Payload Size (Without Encryption)	∼34 bytes	Speed, GPS, warning status
Payload Size (With Encryption)	∼80 bytes	After Speck-64/128 + hex encoding

Source: Authors' system configuration; Semtech SX1278 datasheet.

Table 4
Summary of experimental scenarios.

Scenario	Description	Encryption	Payload (B)	SF	BW / CR	Metrics evaluated	n (repetitions)	Objective
S1 – Baseline	Unencrypted LoRa V2V communication	None (Plaintext)	∼34	SF7	125 kHz / 4/5	Communication delay, Power, RSSI, calculated ToA, Payload Interpretation Success Rate	20	Establish performance reference; confirm security vulnerability
S2 – Encrypted	Speck-64/128 encrypted LoRa V2V communication	Speck-64/128 (128-bit key)	∼80	SF7	125 kHz / 4/5	Communication delay, Power, RSSI, calculated ToA, Payload Interpretation Success Rate	20	Quantify encryption overhead; verify evaluated payload confidentiality
S3 – SF Variation	ToA analysis across SF7–SF12 for both payload sizes	Both (S1 and S2)	34 & 80	SF7–SF12	125 kHz / 4/5	Calculated ToA	6 SF values (analytical)	Show SF dominance over cryptographic overhead in application-level processing delay

2.6. Experimental Setup

Experiments were conducted under Line-of-Sight (LoS) conditions in an open outdoor environment using two identical vehicle communication nodes at a fixed inter-node distance of 50 meters. Tests were performed across multiple sessions (morning, afternoon, and evening) to improve measurement consistency and reduce temporal bias. All measurements were recorded via onboard system logging and serial monitoring tools.

To minimize external variability, the experiments were conducted under relatively stable environmental conditions with minimal external wireless interference. Nevertheless, minor variations may still occur due to wireless channel fluctuations, signal propagation effects, timing resolution limitations, and environmental noise during LoRa communication.

Scenario S1 in Table 4 uses the same hardware and radio parameters as S2 but without encryption. Vehicle data (∼34 bytes plaintext) are transmitted at SF7, BW = 125 kHz, CR = 4/5. It establishes baseline values for all metrics and confirms system vulnerability to sniffing and spoofing in the absence of encryption.

Scenario S2 uses identical radio parameters to S1 (SF7, BW = 125 kHz, CR = 4/5) with Speck-64/128 encryption active, as described in Section 2.5. Hex encoding of the ciphertext expands the payload from ∼34 bytes to ∼80 bytes. This enables direct comparison of all performance metrics against S1, isolating the overhead from cryptographic processing and payload expansion. Evaluated payload confidentiality is also verified in this scenario.

The SF variation scenario investigates how LoRa physical-layer parameters — specifically the Spreading Factor — influence Time on Air (ToA) for both the plaintext (PL = 34 B) and encrypted (PL = 80 B) packet configurations. The SF varies across six values: SF7, SF8, SF9, SF10, SF11, and SF12. All other radio parameters are held constant: BW = 125 kHz, CR = 4/5, preamble = 8 symbols, and CRC enabled. ToA values are analytically calculated using the Semtech LoRa ToA formula as specified in the SX1276/77/78/79 datasheet (Semtech Corporation, nd) rather than measured experimentally, providing a theoretical characterization of how Spreading Factor selection affects transmission duration. This scenario demonstrates that LoRa physical-layer parameters dominate overall communication delay, and that SF selection is a more effective optimization lever than reducing cryptographic overhead.

2.7. Measurement and Evaluation Metrics

Five metrics were evaluated across both system configurations. The first metric was communication delay (ΔT), which refers to the application-level processing delay measured from packet preparation at the transmitter until successful payload parsing at the receiver. The second metric was the calculated Time on Air (ToA), which was determined based on LoRa transmission parameters and payload size. The third metric was power consumption, measured using a digital multimeter and calculated using

$$P = V \times I. \tag{5}$$

The fourth metric was the Received Signal Strength Indicator (RSSI), obtained directly from the LoRa module during packet reception. The fifth metric was the payload interpretation outcome during sniffing and spoofing scenarios, evaluated based on successful packet interception and forged packet acceptance under simulated attack conditions.

Two wireless attack models were used for security evaluation: (1) sniffing, passive interception of transmitted packets; and (2) spoofing, injection of forged packets imitating legitimate nodes.

An additional LoRa node configured with identical communication parameters (433 MHz, BW = 125 kHz,

CR = 4/5, and matching SF) was deployed as the attacker device during the security evaluation. This node operated independently of the two legitimate vehicle communication nodes and was positioned within communication range of both nodes throughout the experiments.

In the sniffing scenario, the attacker node passively intercepted packets transmitted between the legitimate vehicle nodes without transmitting any signal of its own. A sniffing attempt was considered successful when the intercepted payload could be captured and meaningfully interpreted by the attacker. Under C1 (unencrypted), transmitted plaintext packets could be directly read and analyzed. Under C2 (encrypted), intercepted ciphertext could not be interpreted without the pre-shared symmetric key, rendering the captured payload unintelligible.

In the spoofing scenario, the attacker node generated forged packets by replicating the packet structure and radio transmission parameters of a legitimate vehicle node. A spoofing attempt was considered successful when the receiving node accepted and processed the forged packet as a valid message. Under C1, forged packets were successfully interpreted as legitimate vehicle data. Under C2, forged packets failed to produce valid payload interpretation due to encryption mismatch and invalid ciphertext decoding at the receiving node.

Each attack type was evaluated across 20 repeated trials under identical communication conditions. Payload interpretation success rate was calculated as the percentage of successful attacks relative to the total number of attempts, and results are reported in Table 10 and Fig. 7.

2.8. Data Analysis

The data collected were analyzed using descriptive analytical methods, including mean, standard deviation, percentage difference, and graphical comparison between encrypted and unencrypted configurations. The analysis focuses on evaluating the security–performance trade-off of the proposed system across communication delay, calculated Time on Air (ToA), power consumption, RSSI, and payload interpretation resistance under sniffing and spoofing attack scenarios.

3. Results and Discussion

3.1. Communication Delay Analysis

This section evaluates the effect of Speck-64/128 encryption on communication delay under configurations C1 (without encryption) and C2 (with Speck-64/128). Communication delay was measured at the application layer, from packet preparation at the transmitter until successful payload parsing at the receiver. Measurements were conducted separately for both transmission directions, Vehicle A to B (ΔT_1) and Vehicle B to A (ΔT_2), across 10 trials each, yielding $n = 20$ per configuration when combined. Mean communication delay increased from 27.50 ± 12.04 ms in the unencrypted configuration to 116.35 ± 25.31 ms in the encrypted configuration, representing an increase of approximately 4.23 times. The additional delay is primarily caused by payload expansion and increased LoRa calculated Time on Air (ToA) due to encryption. Despite the increase in communication delay, communication performance remained acceptable for low-rate V2V warning communication in mining environments. The experimental results are summarized in Table 5.

Table 5
Communication delay comparison between encrypted and unencrypted configurations ($n = 20$ per configuration).

Configuration	Mean (ms)	Std. Dev (ms)	Min (ms)	Max (ms)
Without Encryption	27.5	12.0	< 1	48
With Speck-64/128	116.35	25.31	92	182

Source: Authors' experimental measurements ($n = 20$ per configuration: 10 measurements per transmission direction).

The communication delay increase is attributable to encryption overhead, not random variation, and remained within acceptable bounds for low-rate V2V warning communication. The minimum observed communication delay in the unencrypted configuration was below the measurable timing resolution of the implemented ESP32-based application-level measurement framework and is therefore reported as < 1 ms. Because the measurement was performed at the application layer rather than as physical-layer end-to-end latency, very short processing intervals may appear below the effective timer granularity.

As shown in Fig. 4, the encrypted configuration also exhibits greater variability (SD = 25.31 ms vs. 12.0 ms). This behavior is primarily driven by payload expansion from 34 to 80 bytes, which increases LoRa ToA and therefore overall communication delay. This pattern is consistent with prior LoRa studies showing that communication delay scales with packet length rather than application-layer processing (Augustin et al., 2016; Vinodhini and Rajkumar, 2023).

As shown in Table 6, calculated Time on Air (ToA) increases considerably with higher Spreading Factor values for both plaintext and encrypted payload configurations. At SF7, the calculated ToA is 112.90 ms for the plaintext payload and 232.70 ms for the encrypted payload. At SF12, the values increased to 2433.02 ms and 4497.41 ms, respectively. The increased calculated ToA in the encrypted configuration is primarily caused by payload expansion from 34 bytes to 80 bytes after encryption and hexadecimal encoding.

These results indicate that LoRa physical-layer parameters, particularly the Spreading Factor, contribute more substantially to overall communication delay than the cryptographic computation itself. Therefore,

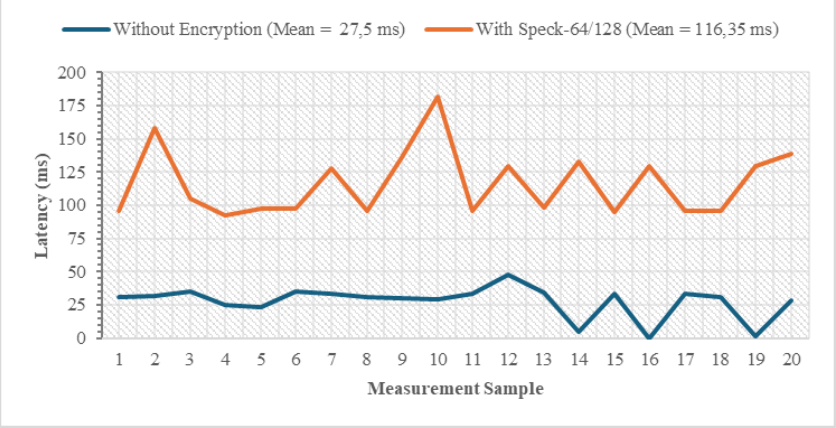


Figure 4: Comparison between encrypted and unencrypted configurations (samples 1–10: A→B; samples 11–20: B→A).

Table 6
Calculated Time on Air (ToA) for SF7–SF12 (BW = 125 kHz, preamble = 8 symbols, CRC enabled).

SF	ToA Plain (ms) PL = 34 B	ToA Encrypted (ms) PL = 80 B	ΔToA (ms)	Ratio (Enc./Plain)
SF7	112.90	232.70	119.80	2.06
SF8	207.36	410.11	202.75	1.98
SF9	377.86	746.50	368.64	1.98
SF10	681.98	1345.54	663.56	1.97
SF11	1216.51	2543.62	1327.11	2.09
SF12	2433.02	4497.41	2064.39	1.85

Source: Calculated by authors using Semtech LoRa ToA formula (AN1200.13); BW = 125 kHz, CR = 4/5, preamble = 8, CRC enabled, IH = 0, DE = 0.

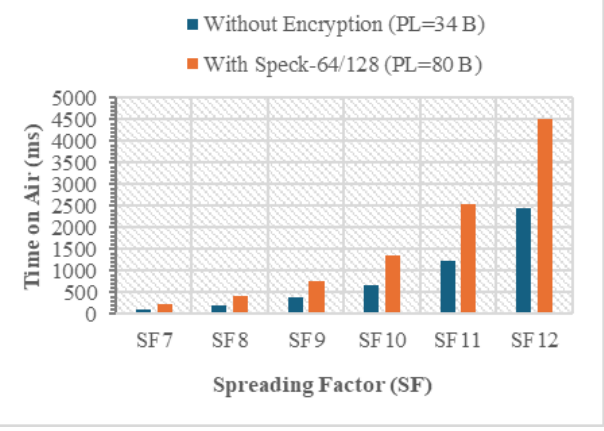


Figure 5: Calculated Time on Air (ToA) comparison for SF7–SF12.

reducing the Spreading Factor represents a more effective optimization strategy for delay reduction than removing encryption mechanisms. As shown in Fig. 5 and Table 6, calculated ToA increases exponentially with SF for both configurations.

At SF7 (the lowest SF tested), calculated ToA is 112.90 ms for the unencrypted packet and 232.70 ms for the encrypted packet, with a ratio of 2.06×. At SF12, the values rise to 2433.02 ms and 4497.41 ms respectively, confirming that LoRa physical-layer characteristics dominate overall communication delay performance.

The absolute overhead introduced by payload expansion (34 B to 80 B) grows from 119.80 ms at SF7 to 2064.39 ms at SF12, demonstrating that reducing the Spreading Factor is a more effective communication delay optimization strategy than removing encryption. The ratio of encrypted to plain calculated ToA ranges from 1.85× to 2.09× across all tested SF values, consistently approaching 2× due to the near-doubling of payload size (34 B to 80 B) introduced by the Speck-64/128 cipher output.

Table 7
Power consumption comparison between encrypted and unencrypted configurations.

Configuration	Mean (W)	Std. Dev (W)
Without Encryption (C1)	0.571	0.055
With Speck-64/128 (C2)	0.599	0.052

Source: Authors' experimental measurements ($n = 40$ per configuration: 10 measurements × 4 scenarios).

3.2. Power Consumption Analysis

This section evaluates the impact of Speck-64/128 encryption on node power consumption. Power was calculated from voltage and current measurements across four transmission and reception scenarios per configuration (Vehicle A→B send, Vehicle B receive; Vehicle B→A send, Vehicle A receive), yielding $n = 40$ per configuration (10 measurements × 4 scenarios). Results are summarized in Table 7.

The per-scenario breakdown is provided in Table 8 for transparency. Although AES-128 benefits

Table 8
Per-scenario mean power consumption.

Scenario	Mean Current (mA)	Mean Power (W)
Transmit A→B, No Encryption	177.2	0.655
Receive B from A, No Encryption	137.2	0.508
Transmit B→A, No Encryption	150.4	0.556
Receive A from B, No Encryption	153.8	0.569
Transmit A→B, Encrypted	184.1	0.681
Receive B from A, Encrypted	148.6	0.550
Transmit B→A, Encrypted	157.7	0.583
Receive A from B, Encrypted	158.0	0.585

Source: Derived from experimental measurements using $P = V \times I$, with $V = 3.7$ V.

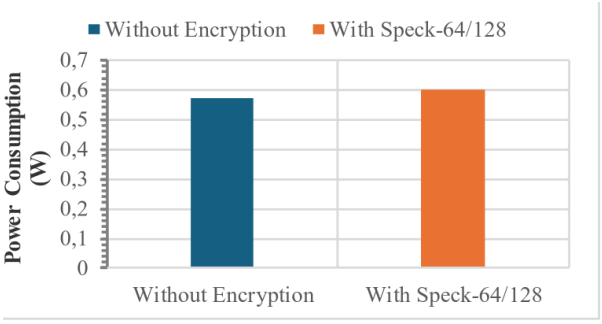


Figure 6: Power consumption comparison between encrypted and unencrypted configurations.

from broader standardization and hardware acceleration support on ESP32 platforms, Speck-64/128 remains attractive for lightweight embedded implementations due to its simple design and low computational overhead.

Fig. 6 presents a comparison of mean power consumption between the encrypted and unencrypted configurations. The encrypted configuration exhibits a slightly higher average power consumption, although the overall increase remains relatively small. This behavior indicates that the additional energy overhead introduced by Speck-64/128 encryption is minimal compared to the overall power consumption dominated by LoRa radio transmission activity.

Given the lightweight design objectives and resource constraints of the proposed LoRa-based V2V communication system, Speck-64/128 was selected as the encryption algorithm for this implementation.

3.3. Security Evaluation

The rationale for selecting Speck-64/128 over AES-128 is summarized in Table 9. Key advantages include its ARX structure (no S-Box required), low RAM usage, and higher software throughput on 32-bit MCUs without hardware acceleration (Beaulieu et al., 2015; Thakor et al., 2021; El-hajj et al., 2023).

Table 9
Specification comparison: Speck-64/128 vs. AES-128.

Parameter	Speck-64/128	AES-128
Block Size	64 bits	128 bits
Key Size	128 bits	128/192/256 bits
Number of Rounds	32	10/12/14
Algorithm Structure	ARX (Add-Rotate-XOR)	SPN (Sub Bytes, Shift Rows, Mix Columns)
S-Box / Lookup Table	None required	Required (256-byte S-Box)
Hardware Acceleration	Not required	Recommended for efficient SW implementation.
RAM Usage	Very low (~few bytes)	Higher (>256 bytes for S-Box)
Throughput on MCU (32-bit)	Higher (optimized for SW)	Lower without HW acceleration
Standardization	NSA proposal; not NIST-standardized	NIST FIPS 197 standard
Suitability for ESP32 (no HW AES)	High	Moderate (HW acceleration available on ESP32)

Source: Adapted from Beaulieu et al. (2015), Thakor et al. (2021), and El-hajj et al. (2023).

Table 10
Security evaluation results: payload interpretation success rate comparison.

Configuration	Sniffing payload interpretation success rate	Spoofing payload interpretation success rate
Without Encryption (C1)	100%	100%
With Speck-64/128 (C2)	0%	0%

Source: Authors' experimental security evaluation results.

As shown in Table 9, Speck-64/128 offers several advantages for resource-constrained embedded systems, including low memory usage, simple ARX-based operations, and efficient software-oriented implementation without requiring S-Box lookup tables.

The security performance of both configurations was evaluated by measuring the successful payload interpretation rate against sniffing and spoofing scenarios attacks. Table 10 presents the results, and Fig. 7 illustrates the successful payload interpretation rate for each configuration and attack type.

The security evaluation demonstrates that the implementation of Speck-64/128 encryption enhances payload confidentiality by reducing successful payload interpretation under the evaluated sniffing and spoofing attack scenarios.

However, this study evaluates basic attack models (sniffing and spoofing) only. Advanced vectors such as replay attacks, side-channel attacks, and key extraction remain open for future work. The use of ECB mode may introduce pattern leakage for identical plaintext blocks, though the practical risk is limited given the dynamic, short-length nature of the transmitted payload.

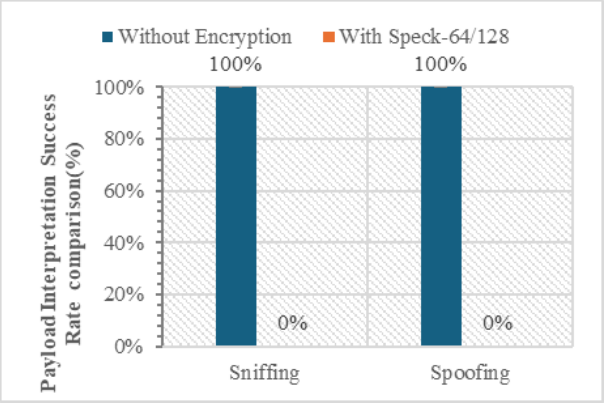


Figure 7: Security evaluation: successful payload interpretation rate for sniffing and spoofing scenarios under encrypted and unencrypted configurations.

Table 11
RSSI per distance summary.

Distance (m)	Module 1 Mean (dBm)	Module 1 Std. Dev (dBm)	Module 2 Mean (dBm)	Module 2 Std. Dev (dBm)
10	−88.00	5.60	−84.40	3.53
20	−92.60	1.35	−90.50	1.58
30	−95.90	1.29	−90.60	0.52
40	−94.40	1.35	−92.20	0.42

Source: Authors' experimental measurements ($n = 10$ per distance per module, encrypted configuration).

Authenticated encryption (e.g., CCM or GCM-adapted modes) and dynamic key exchange are recommended for production deployments.

3.4. RSSI Analysis

RSSI measurements were obtained from both LoRa modules across distances of 10 to 40 meters under LoS conditions during moving vehicle tests. For each distance, 10 measurements were recorded per direction (LoRa Module 1: A→B; LoRa Module 2: B→A), yielding $n = 40$ per module across the four valid distances (10, 20, 30, 40 m). The 50-meter distance was excluded from the aggregate statistics due to substantial packet loss. The per-distance summary is presented in Table 11, and overall statistics are summarized in Table 12.

At a distance of 50 meters, severe packet loss was observed: LoRa Module 1 successfully received only 3 out of 10 packets (70% loss), while LoRa Module 2 received only 2 out of 10 packets (80% loss), indicating the practical communication range limit of the system under moving conditions. Importantly, despite the integration of Speck-64/128 encryption, no substantial degradation in RSSI performance was observed between communication nodes.

This confirms that the lightweight cryptographic mechanism does not directly affect radio signal propagation or reception quality, consistent with prior

Table 12
RSSI summary statistics: LoRa Module 1 vs. Module 2.

Parameter	Mean (dBm)	Std. Dev (dBm)	Min (dBm)	Max (dBm)
LoRa Module 1	−92.72	4.18	−97	−80
LoRa Module 2	−89.42	3.56	−93	−79

Source: Authors' experimental measurements ($n = 40$ per module: 10 measurements × 4 distances, encrypted configuration).

LoRa studies reporting that signal strength is governed by physical-layer channel conditions rather than application-layer processing (Gupta et al., 2021; El-hajj et al., 2023).

As illustrated in Fig. 8 and summarized in Table 12, LoRa Module 1 exhibited higher signal variability (std. dev = 4.18 dBm), largely driven by the 10-meter measurement where greater fluctuation was observed (std. dev = 5.60 dBm), potentially due to near-field antenna effects and multipath propagation at short range.

LoRa Module 2 demonstrated comparatively more stable signal quality (std. dev = 3.56 dBm), with notably consistent readings at 30 and 40 meters (std. dev = 0.52 and 0.42 dBm, respectively). RSSI values also show a general trend of decreasing signal strength with increasing distance, as expected from free-space path loss. Both modules remained well above the LoRa SX1278 receiver sensitivity threshold (approximately −148 dBm at SF12), confirming reliable link quality throughout the valid measurement range.

3.5. Design Implications

These findings suggest that system optimization should focus primarily on communication parameters, such as the LoRa Spreading Factor, rather than sacrificing security mechanisms. Communication delay reduction can be achieved through physical-layer communication tuning without compromising system security.

In safety-critical mining environments, encryption should be treated as a fundamental system requirement rather than an optional feature, given the minimal performance cost demonstrated in this study.

3.6. Trade-off Analysis

The results reveal a clear trade-off between security and performance. While Speck-64/128 encryption increases mean communication delay by approximately 4.23× (from 27.50 ms to 116.35 ms), the dominant contributor is the LoRa physical layer, specifically, payload expansion affecting Time on Air, rather than cryptographic computation. The observed overhead is primarily influenced by payload expansion and calculated Time on Air (ToA), including the effect of hexadecimal ciphertext encoding, rather than cryptographic computation alone.

From an energy perspective, the impact is negligible (∼1.05× increase, 0.028 W absolute), confirming that

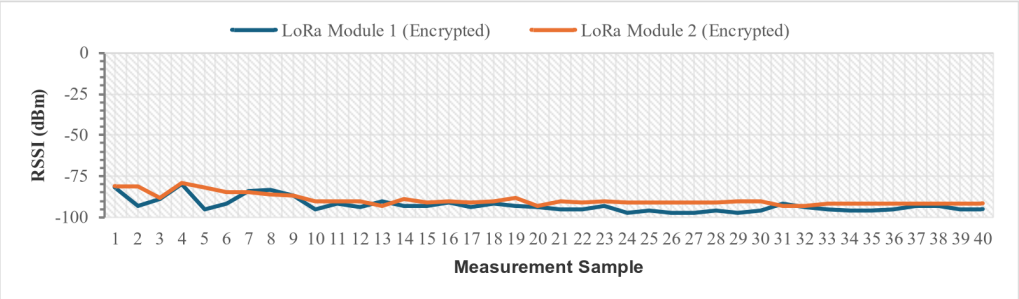


Figure 8: RSSI measurement: LoRa Module 1 vs. Module 2 (samples 1–10: 10 m; samples 11–20: 20 m; samples 21–30: 30 m; samples 31–40: 40 m).

lightweight cryptography does not impose a meaningful burden on battery-powered nodes. In contrast, both sniffing and spoofing successful payload interpretation during evaluated attack scenarios decreased from 100% to 0%.

Collectively, these findings indicate a favorable trade-off: substantial improvement in payload confidentiality with acceptable performance cost. Communication delay can be effectively reduced by tuning the Spreading Factor without sacrificing security, reinforcing encryption as a fundamental requirement rather than an optional feature.

3.7. Limitations

This study has several limitations. First, the experiments were conducted on a scaled prototype platform using RC vehicles under LoS conditions, which may not fully represent the complexity of real mining environments, including non-LoS propagation, multipath effects, wireless interference, and longer communication distances. The effective communication range observed in this study was limited to 40 meters, with substantial packet loss occurring at 50 meters, further constraining the generalizability of results to larger-scale deployments.

Second, the proposed system employs a pre-shared symmetric key without a dynamic key management mechanism, which may limit scalability and long-term security in large-scale vehicular communication deployments.

Third, the use of ECB mode in the encryption process may introduce potential data pattern leakage under certain conditions. However, the practical impact is limited in this study due to the short and dynamic payload characteristics transmitted within the V2V communication system.

Fourth, communication delay and RSSI measurements for each configuration combine data from both transmission directions (A→B and B→A). Although preliminary observations showed relatively similar behavior between both directions, this assumption was not verified under all environmental conditions and should be treated with appropriate caution when generalizing results.

Fifth, this study is limited to prototype-scale evaluation under controlled Line-of-Sight conditions. Replay attacks, physical key extraction, side-channel attacks, and jamming attacks remain outside the scope of the current evaluation and are proposed as future work directions.

In addition, this study does not experimentally benchmark AES-128 using ESP32 hardware acceleration, which may provide different performance characteristics compared to the software-oriented Speck-64/128 implementation.

4. Conclusion

This study demonstrates that integrating Speck-64/128 encryption into a LoRa-based V2V communication system is both feasible and effective for mining environments. Although encryption increases communication delay, the additional overhead is relatively small compared to the inherent LoRa transmission constraints and can be reduced through communication parameter optimization. Power consumption exhibits only marginal variation, while the implementation enhances payload confidentiality and reduces successful payload interpretation under the evaluated sniffing and spoofing attack scenarios.

The key finding is that communication delay is governed primarily by LoRa physical-layer parameters—specifically the Spreading Factor—rather than cryptographic overhead. Performance optimization should therefore focus on communication parameter tuning rather than removing encryption mechanisms.

Future work should extend evaluation to full-scale mining vehicles under non-LoS and multipath conditions and explore multi-node V2V topologies and real-world deployment in operational mining sites. On the security side, authenticated encryption modes (e.g., CCM or GCM-adapted), dynamic key management, and benchmarking of alternative ciphers (Simon, PRESENT) against Speck-64/128—including

AES-128 with hardware acceleration on the ESP32—are recommended to provide a more comprehensive security–performance analysis.

Acknowledgements

The authors would like to thank National Cyber and Crypto Polytechnic (Politeknik Siber dan Sandi Negara) for providing support and facilities for this research. This research received no external funding.

References

Abboud, K., Omar, H. A., and Zhuang, W. (2016). Interworking of DSRC and cellular network technologies for V2X communications: A survey. *IEEE Transactions on Vehicular Technology*, 65(12):9457–9470.

Abdelkader, G., Elgazzar, K., and Khamis, A. (2021). Connected vehicles: Technology review, state of the art, challenges and opportunities. *Sensors*, 21(22):7712.

Abdul Razak, S. F., Ren, T. Y., Yogarayan, S., Kamis, N. H., and Yusof, I. (2023). Lane change decision aid and warning system using LoRa-based vehicle-to-vehicle communication technology. *Bulletin of Electrical Engineering and Informatics*, 12(4):2428–2437.

Aliev, H., Kim, H., and Choi, S. (2020). A scalable and secure group key management method for secure V2V communication. *Sensors*, 20(21):6137.

Augustin, A., Yi, J., Clausen, T., and Townsley, W. (2016). A study of LoRa: Long range & low power networks for the internet of things. *Sensors*, 16(9):1466.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference*, pages 1–6, New York, NY, USA. ACM.

Chehri, A., Chehri, H., Hakim, N., and Saadane, R. (2020). Realistic 5.9 GHz DSRC vehicle-to-vehicle wireless communication protocols for cooperative collision warning in underground mining. In *Smart Innovation, Systems and Technologies*, pages 133–141. Springer.

Conti, M., Dragoni, N., and Lesyk, V. (2016). A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3):2027–2051.

El-hajj, M., Mousawi, H., and Fadlallah, A. (2023). Analysis of lightweight cryptographic algorithms on IoT hardware platform. *Future Internet*, 15(2):54.

Farraj, A. and Hammad, E. (2024). A physical-layer security cooperative framework for mitigating interference and eavesdropping attacks in internet of things environments. *Sensors*, 24(16):5171.

Gupta, M., Awaysheh, F. M., Benson, J., Alazab, M., Patwa, F., and Sandhu, R. (2021). An attribute-based access control for cloud enabled industrial smart vehicles. *IEEE Transactions on Industrial Informatics*, 17(6):4288–4297.

Haque, K. Z., Abdelgawad, A., Yanambaka, V. P., and Yelamarthi, K. (2020a). LoRa architecture for V2X communication: An experimental evaluation with vehicles on the move. *Sensors*, 20(23):6876.

Haque, K. Z., Abdelgawad, A., Yanambaka, V. P., and Yelamarthi, K. (2020b). A LoRa based reliable and low power vehicle to everything (V2X) communication architecture. In *2020 IEEE International Symposium on Smart Electronic Systems (iSES)*, pages 177–182. IEEE.

Imam, M. et al. (2023). The future of mine safety: A comprehensive review of anti-collision systems based on computer vision in underground mines. *Sensors*, 23(9):4294.

Jadaan, K., Zeater, S., and Abukhalil, Y. (2017). Connected vehicles: An innovative transport technology. *Procedia Engineering*, 187:641–648.

Kecojevic, V., Komljenovic, D., Groves, W., and Radomsky, M. (2007). An analysis of equipment-related fatal accidents in U.S. mining operations: 1995–2005. *Safety Science*, 45(8):864–874.

Kim, Y. and Choi, Y. (2022). Smart helmet-based proximity warning system to improve occupational safety on the road using image sensor and artificial intelligence. *International Journal of Environmental Research and Public Health*, 19(23):16312.

Lu, N., Cheng, N., Zhang, N., Shen, X., and Mark, J. W. (2014). Connected vehicles: Solutions and challenges. *IEEE Internet of Things Journal*, 1(4):289–299.

Qian, M., Zhao, K., Li, B., Gong, H., and Seneviratne, A. (2022). Survey of collision avoidance systems for underground mines: Sensing protocols. *Sensors*, 22(19):7400.

Sanmiquel, L., Rossell, J. M., Bascompta, M., Vintró, C., and Yousefian, M. (2024). Data mining of accidents in Spanish underground mines in the period 2003–2021 caused by a collision with a moving object. *Heliyon*, 10(2):e24716.

Semtech Corporation (n.d.). SX1276/77/78/79: 137 MHz to 1020 MHz low power long range transceiver, datasheet, rev. 7. https://www.semtech.com/products/wireless-rf/lora-connect/sx1276.

Soto, I., Calderon, M., Amador, O., and Urueña, M. (2022). A survey on road safety and traffic efficiency vehicular applications based on C-V2X technologies. *Vehicular Communications*, 33:100428.

Soy, H., Ateş, T. F., and Özkan, A. O. (2025). Feasibility of LoRa-based infrastructure-to-vehicle (I2V) communication for road weather information systems. *International Journal of Communication Systems*, 38(4).

Storck, C. R. and Duarte-Figueiredo, F. (2020). A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE Access*, 8:117593–117614.

Thakor, V. A., Razzaque, M. A., and Khandaker, M. R. A. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*, 9:28177–28193.

Torres, A. P. A., Da Silva, C. B., and Filho, H. T. (2021). An experimental study on the use of LoRa technology in vehicle communication. *IEEE Access*, 9:26633–26640.

Tzoannos, Z.-R., Kosmanos, D., Xenakis, A., and Chaikalis, C. (2024). The impact of spoofing attacks in connected autonomous vehicles under traffic congestion conditions. *Telecom*, 5(3):747–759.

Usman, M., Ahmed, I., Imran, M., Khan, S., and Ali, U. (2017). SIT: A lightweight encryption algorithm for secure internet of things. *International Journal of Advanced Computer Science and Applications*, 8(1):1–10.

Vinodhini, M. and Rajkumar, S. (2023). Performance analysis of vehicle-to-everything communication using internet of LoRa computing for intelligent transportation system. *Intelligent Decision Technologies*, 17(2):577–594.

Xiang, X., Qin, W., and Xiang, B. (2014). Research on a DSRC-based rear-end collision warning model. *IEEE Transactions on Intelligent Transportation Systems*, 15(3):1054–1065.

Zadobrischi, E. and Havriliuc, Ş. (2024). Enhancing scalability of C-V2X and DSRC vehicular communication protocols with LoRa 2.4 GHz in the scenario of urban traffic systems. *Electronics*, 13(14):2845.