Secure Satellite Communication Using Shamir's Secret Sharing-Based Frequency Hopping Technique*

Su-Kyoung Kim, So-Yeon Kim and Il-Gu Lee*
Sungshin Women's University, Seongbuk, Seoul, Korea
{220254012, 220237014, iglee}@sungshin.ac.kr

Abstract

Satellite communication systems provide continuous connectivity over a wide area. However, they are vulnerable to jamming and eavesdropping attacks, and achieving security and efficiency with limited power resources is challenging. Conventional approaches either require high computational complexity or rely on channel-state information (CSI), limiting their practicality in satellite communication environments. To address these limitations, this study proposes a Shamir secret sharing-based frequency-hopping (SSS-FH) technique that shares messages into multiple shares and transmits them through FH. The proposed technique achieved a message recovery rate (MRR) that was 77.9%p higher than that of friendly jamming (FJ) and frequency hopping spread spectrum (FHSS) at a signal-to-interference-plus-noise ratio (SINR) of 0 dB, and it maintained a superior performance as the jamming intensity increased. Furthermore, when evaluating the MRR of the eavesdropper (Eve) under varying information leakage rate (ILR) conditions, the proposed technique reduced Eve's MRR by 42.1%p compared with FJ and by approximately 43.2%p compared with FHSS. In terms of transmission efficiency, the proposed technique maintained stable efficiency across all SINR ranges and recorded approximately 0.3%p higher efficiency than FJ and FHSS, even under SINR values below 0 dB.

Keywords. Network, Satellite Communication, Shamir's Secret Sharing, Frequency Hopping

1 Introduction

Recently, the demand for global network services has increased, and satellite communication technology has emerged as a core technology for next-generation communication infrastructures (Luo et al., 2024; Xiao et al., 2024). The growing importance of satellite communications in various fields, including the Internet of Things (IoT), disaster response, and maritime and aviation communications, has been extensively documented (Centenaro et al., 2021; Wang et al., 2023; Li et al., 2020; Wang et al., 2024). According to Global Market Insights, the global satellite communications market reached $2.31 billion in 2024 and is projected to grow at a compound annual rate of 12.3% through 2034 (Gujar, 2024). However, satellite communications propagating over vast areas enable malicious actors to

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 62, December 16-18, 2025, Sapporo , Japan.
† Corresponding author

receive signals and execute high-power jamming attacks to disrupt communication (Kang et al., 2024). Furthermore, satellites operate in power-constrained environments, restricting the deployment of complex security techniques. These vulnerabilities necessitate research to enhance the reliability and security of satellite communication.

Conventional studies are generally categorized into cryptographic- and physical-layer security techniques based on their approaches (Zhang et al., 2023). Cryptographic security techniques are higher-layer security methods that protect data. This method enhances the confidentiality and integrity of the data transmitted over satellite links through encryption, authentication, and key management (Tedeschi et al., 2021). Physical-layer security techniques leverage the inherent characteristics of transmission signals and wireless channel properties to improve communication security in lower protocol layers. Representative approaches include beamforming and friendly jamming (FJ); the former concentrates the signal energy in the desired directions, whereas the latter introduces artificial noise to degrade the performance of an eavesdropper (Eve) (Li et al., 2020). However, these approaches have limitations when the characteristics of satellite communication environments are considered. Cryptographic security techniques incur high computational complexity and power consumption. Contrarily, physical-layer security techniques typically rely on channel state information (CSI), which is difficult to accurately estimate and requires additional antenna deployment and computational resources. The frequency-hopping spread spectrum (FHSS) is gaining attention (Duan et al., 2024). This technique reduces the effectiveness of jamming signals with low power consumption, as the transmitter and receiver switch frequencies according to a predefined pattern without channel estimation. However, an inherent limitation is that the entire communication system becomes vulnerable when a hopping pattern is exposed.

Consequently, this study proposes a Shamir secret sharing-based frequency-hopping (SSS-FH) technique that ensures jamming resistance and confidentiality while featuring low computational complexity and eliminating the need for channel estimation. The proposed technique ensures the confidentiality of the hopping pattern by implementing a secret distribution, rendering it suitable for satellite communication environments characterized by limited power resources.

The main contributions of this paper are as follows:

- It proposes an SSS-FH technique, which divides messages into shares and transmits them using FH to counter jamming and eavesdropping in satellite communication environments.
- In the jamming resilience evaluation, the proposed technique achieved a message recovery rate (MRR) of 77.9%p higher than FJ and FHSS under signal-to-interference-plus-noise ratio (SINR) conditions at or below 0 dB. In the data confidentiality evaluation, Eve's MRR was reduced by 42.1%p compared with FJ and by 43.2%p compared with FHSS. In terms of transmission efficiency, the proposed technique maintained an approximately 0.3%p higher efficiency than both FJ and FHSS under SINR conditions below 0 dB.

The remainder of this paper is organized as follows. Section 2 provides an examination of related research on satellite communication security. Section 3 proposes an FH technique based on the SSS methodology. Section 4 analyzes the performance evaluation results of the proposed and conventional techniques. Finally, section 5 concludes the paper.

2 Related work

Table 1 compares the proposed technique with the existing satellite communication security research. These techniques can be categorized into cryptographic and physical-layer security approaches. Four key requirements were defined: Jamming Resilience (JR), Data Confidentiality (DC), Low Complexity (LC), and CSI Independence (CSII), with each technique's compliance analyzed.

Features	Ref.	Contribution & Limitation	Requirements			
			JR	DC	LC	CSII
Crypto-graphic Security	Bentoutou et al. (2020)	- Improved security and speed of satellite images - High complexity arises from memory overhead during key stream storage and the need to manage both Advanced Encryption Standard (AES) and Chaos keys simultaneously	X	O	△	O
	Pirzada et al. (2020)	- Enhanced resistance to side-channel attacks and improved transmission speed - Reducing the number of rounds in the encryption process lowers security	X	O	△	O
	Jeon et al. (2022)	- Mitigates the Avalanche Effect in AES and enhances error correction performance with Turbo codes - Computational overhead occurs during the adjustment of Turbo decryption iterations - Increased key management burden due to the need to manage different key pairs for each block	X	O	△	O
Physical Layer Security	Liu et al. (2023)	- Increases the secret capacity of legitimate links over Eve - Performance degradation due to CSI errors and self-interference	△	O	X	X
	Nguyen et al. (2023)	- Enhances security by inserting artificial noise into Eve channels to improve legitimate channel gain - Incomplete CSI and multipath/fading environments cause artificial noise to interfere with legitimate channels, resulting in performance degradation	△	O	X	X
	Dua et al. (2024)	- Reduces Bit Error Rate (BER) and packet loss rate while improving throughput and FH success rate - Requires high-complexity computations during LSTM network training and inference -Strongly dependent on predicting CSI	O	X	X	X
	Kim et al. (2025)	- Enhances spectrum efficiency and continuity - FH signals interfere with navigation signals, increasing decoding error probability - Risk of eavesdropping if hopping patterns are exposed	△	X	O	O
	Our Work	- Enhance security by dividing messages into shares using SSS and transmitting them via FH - Trade-off includes increased transmission latency owing to the share generation and reconstruction processes	O	O	O	O

Table 1: Comparison of existing methods and our method of addressing the issues associated with Satellite Communication Security

In the domain of cryptographic security techniques, Bentoutou et al. (2020) proposed an encryption method that integrates an advanced encryption standard counter mode (AES-CTR) with a 2D logistic-adjusted-sine chaos map. This approach enhanced the security and speed of satellite image encryption. However, it introduces memory overhead because a pre-generated key stream should be stored during encryption, and it also requires the management of multiple keys (AES key, chaos key, and Initialization

Vector (IV)), which complicates key management. Pirzada et al. (2020) proposed a parallel-structure-based authenticated encryption technique for secure and fast data transmission. By combining IV randomization with periodic rekeying in AES-CTR, this method prevents IV misuse, provides resistance against side-channel attacks, and improves transmission speed. However, its security decreases if the number of encryption rounds is reduced, and key management remains complex. Jeon et al. (2022) proposed the CFB-AES-TURBO technique to strengthen secure satellite communication. This mitigates the Avalanche Effect of AES and improves error correction using turbo codes. However, encrypting all messages significantly increases the power consumption, and additional computational costs arise from optimizing the EBS and adjusting the turbo decryption iterations. Furthermore, the use of different key pairs for each block imposes a heavy burden on key management.

In the domain of physical layer security techniques, Liu et al. (2023) proposed a method to enhance integrated satellite-terrestrial uplink security. In this method, the base station transmits artificial noise along with legitimate signals to degrade Eve's performance, thereby increasing the secrecy capacity of the legitimate links. However, in actual satellite environments, channel distortion and synchronization errors prevent artificial noise from being completely removed, leaving residual interference that affects legitimate signals. The performance is further degraded by CSI estimation errors and base-station self-interference. Subsequently, Nguyen et al. (2023) proposed amplify-and-forward and decode-and-forward relay techniques under FJ and imperfect CSI environments to balance security and reliability in satellite-ground relay networks. This method improves the legitimate channel gain by inserting artificial noise to the target Eve, thereby enhancing both security and jamming resilience. However, incomplete CSI and multipath/fading environments cause artificial noise that interferes with legitimate channels, resulting in performance degradation.

In the field of physical layer security techniques, Duan et al. (2024) proposed an adaptive FH technique based on long short-term memory (LSTM) networks to address frequency resource contention in satellite communications. This method reduces the bit error rate (BER) and packet loss while improving throughput and FH success rates. However, it requires high computational complexity during the LSTM training and inference, and its performance strongly depends on accurate CSI predictions. Additionally, Kim et al. (2025) proposed a technique that embeds navigation signals into FH communication waveforms to enhance the spectral efficiency and continuity. However, FH signals interfere with navigation signals, thereby increasing the probability of decoding errors, and the system remains vulnerable to eavesdropping if the hopping patterns are exposed.

As indicated in previous studies, satellite communication security research has primarily focused on achieving data confidentiality and transmission reliability. However, cryptographic security techniques encounter significant challenges in bandwidth-constrained environments, such as high computational overhead, complex key management, and limited resistance to jamming. Physical-layer security techniques rely on channel characteristics, and they suffer from the inherent drawback that artificial noise degrades Eve's performance and interferes with legitimate channels. In particular, FH approaches remain vulnerable to confidentiality breaches once hopping patterns are exposed, enabling Eve to trace the transmission sequences. To address these limitations, this study proposes the SSS-FH technique, which ensures both jamming resilience and data confidentiality while accounting for resource constraints and eliminating reliance on CSI.

3 Shamir's Secret Sharing-Based Frequency Hopping

This section presents the proposed SSS-FH technique and describes its operational methodology. SSS is a secret sharing technique proposed in 1979 that divides an original secret into n shares, where the original secret can be reconstructed only when k or more shares are available (Adi Shamir, 1979). This approach utilizes polynomial operations based on Lagrange interpolation, ensuring information-

theoretic security, while maintaining low computational complexity. The proposed technique divides messages into a predetermined number of shares through SSS for each frame, and then transmits the shares distributed across a time-frequency grid through FH. When a sufficient number is obtained, the receiver can reconstruct the original message by collecting shares. Figure 1 illustrates a flowchart of the proposed technique.

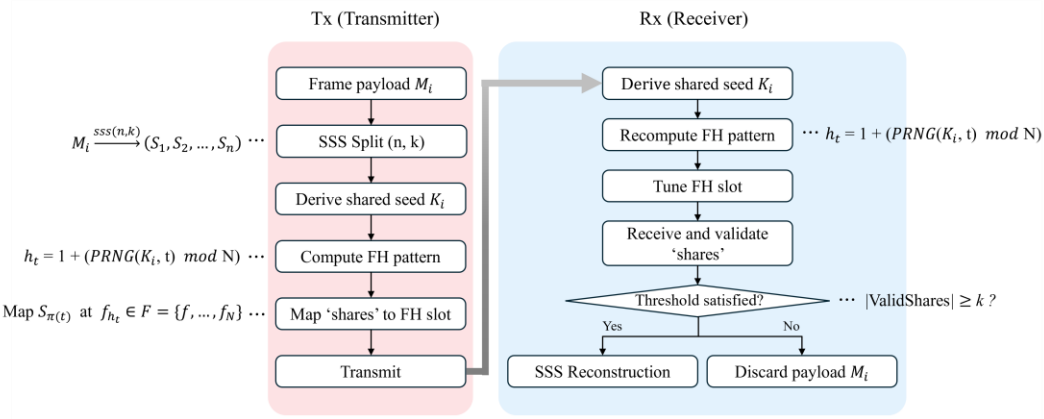


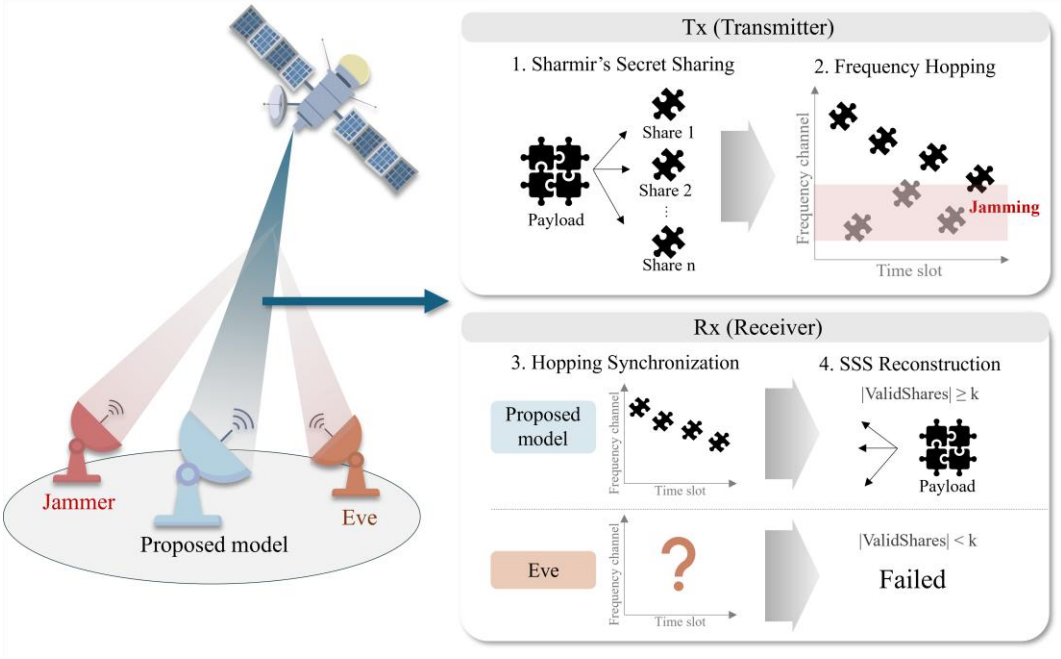
Figure 1: Flowchart of the SSS-FH technique

The transmitter divides each frame message M_i into n shares $(S_1, S_2, \dots, S_n)$ using the SSS technique with the required minimum threshold of k shares for reconstruction. Subsequently, the transmitter derives the shared secret K_i for frame scheduling and calculates the frequency index h_t corresponding to timeslot t using a pseudo-random number generator (PRNG), as expressed in Equation (1).

$$h_t = 1 + (\mathrm{PRNG}(\mathrm{K_i}, \mathrm{t}) \ \mathrm{mod\ N}) \tag{1}$$

where N represents the number of available frequencies. The transmitter selects share $S_{\pi(t)}$ according to the share index $\pi(t)$ and transmits it through the designated frequency f_{h_t} from the frequency set $F = \{f, \dots, f_N\}$. Each share is distributed across specific slots in the time-frequency grid for transmission. The receiver regenerates the shared secret K_i using the same method and calculates the frequency index for each time slot using Equation (1). Subsequently, the receiver synchronizes to frequency f_{h_t} at time slot t to receive share $S_{\pi(t)}$ and performs validity verification. When the number of successfully collected shares exceeds threshold k, the SSS reconstruction algorithm is applied to recover the original message, and the corresponding payload is discarded upon reconstruction failure.

Figure 2 illustrates the operational process of the proposed technique in satellite communication environments where jamming and eavesdropping threats are present.



(a) and (b).

Figure 2: Proposed technique under jamming and eavesdropping threats: (a) satellite communication scenario with a jammer and Eve, (b) transmission and reception process of the proposed technique.

Figure 2(a) illustrates a threatening environment in which jamming interference and eavesdropping by Eve can occur during message transmission from satellites to terrestrial users. Figure 2(b) demonstrates how the reception outcomes may vary under jamming and eavesdropping attacks when message shares are transmitted through the FH. The upper section depicts the transmission process of the transmitter, and the lower section shows the status of the reconstruction of the legitimate receiver and Eve. This architecture exhibits the following characteristics: First, even when a jammer transmits interference signals that target specific frequency resources, the receiver can reconstruct the message if it receives k or more valid shares. Second, the receiver reconstructs the same FH pattern as the transmitter to receive only the valid shares for restoration purposes. Conversely, Eve, lacking knowledge of the FH pattern, cannot determine the precise locations of shares, potentially resulting in message reconstruction failure. Third, because the FH pattern is determined through the PRNG, the CSI calculation becomes unnecessary. Therefore, this architecture can be effectively utilized in satellite communication environments where jamming and eavesdropping threats exist and computational resources are constrained.

4 Evaluation Results and Analysis

4.1 Evaluation Environment

This section evaluates the performance of the proposed technique in terms of Jamming Resilience, Data Confidentiality, and Communication Efficiency. Conventional physical layer security techniques,

namely, FJ and FHSS, were selected as comparative benchmarks, and simulations were conducted in a MATLAB environment. The key parameters used in the experiments are listed in Table 1.

Parameter	Meaning	Value
L_m	Message length (bits)	16,000 bits
L_{frame}	Frame length (bits)	2,048 bits
L_{slot}	Slot length (bits)	100 bits
L_{share}	Share length (bits)	512 bits
SNR_{legit}	SNR (Signal-to-Noise Ratio) of legitimate receiver (dB)	8 dB
SNR_{eve}	SNR of Eve (dB)	6 dB
$SINR$	SINR (Signal-to-Interference-plus-Noise Ratio) (dB)	-
f	Jammed channel ratio (%)	0.3
T_{slot}	Slot duration (ms)	0.5 ms
T_{guard}	Guard interval (ms)	0.05 ms
T_{tune}	Frequency switching time (ms)	0.05 ms
T_{switch}	Slot switching time (ms)	0.05 ms
T_{coord}	Coordination overhead (ms)	5.0 ms
n	Number of shares	9
k	Reconstruction threshold	4
N	Number of frequency channels	10
G	Beamforming gain (dB)	3 dB
J_{legit}	Jammer attenuation factor (%)	50 (%)
J_{eve}	Eve's SNR penalty (dB)	-3 dB

Table 1: Definitions of notations

The total message length was L_m = 16,000 bits with a frame length L_{frame} = 2,048 bits distributed across time slots of L_{slot} = 100 bits each. For the parameters of the proposed technique, the original message was divided into nine shares, requiring four shares for successful reconstruction. The share length was set to L_{share} = 512 bits. The communication channel assumed an additive white Gaussian noise (AWGN) environment. The legitimate receiver's signal-to-noise ratio (SNR) was SNR_{legit} = 8 dB, whereas Eve's SNR was SNR_{eve} = 6 dB. Under these conditions, the performance was evaluated by examining two critical threats that can occur independently: jamming and eavesdropping.

4.2 Jamming Resilience

This experiment evaluated the MRR in environments where portions of the frequency band were subjected to jamming. Jamming was considered in the form of interference, and the performance was evaluated based on the SINR. The SINR was calculated using Equation (2).

$$SINR = \frac{Signal\ Power}{Interference\ +Noise\ Power} \tag{2}$$

As the jamming intensity increased, the interference escalated and the SINR decreased, leading to performance degradation. In this experiment, the MRR was measured for each technique while the SINR levels were varied. Jamming was randomly applied to 30% ($f = 0.3$) of the total number of N = 10 frequency channels, where the MRR represents the ratio of successfully reconstructed messages to the total messages. However, as each technique defines different reconstruction conditions, the definition also varies accordingly. The MRR for the conventional techniques, FJ and FHSS, is expressed in Equation (3).

$$MRR_{conventional} = (SRR^{[L_{frame}/L_{slot}]})^{[L_m/L_{frame}]} \quad (3)$$

- $[L_m/L_{frame}]$ denotes the ratio of the message length L_m to the frame length L_{frame}
- $L_{frame}/L_{slot}]$ denotes the ratio of frame length L_{frame} to slot the length L_{slot}

The MRR for the proposed technique is defined by Equation (4).

$$MRR_{proposed} = \sum_{i=k}^{n} \binom{n}{i} S^i (1-S)^{n-i} \quad (4)$$

- S denotes the probability that a single share is successfully recovered.

Conventional techniques require all the slots constituting each frame to be successfully transmitted; therefore, the overall MRR was calculated as the product of the individual slot success probabilities. Conversely, the proposed technique divides the original message into *n* shares, enabling complete message reconstruction when *k* or more shares are successfully transmitted, resulting in an MRR that follows a binomial distribution. Consequently, although conventional techniques fail to complete message reconstruction even if a single slot fails, the proposed technique can reconstruct the entire message despite partial share losses.

In conventional techniques, the MRR is calculated as the probability that all bits in each slot are correctly received, that is, the slot recovery rate (SRR). When the probability of selecting a jammed channel for each slot is f and the probability of selecting other channels is (1 - f), the SRR is expressed as shown in Equation (5)

$$SRR = f \times (1 - BER)^{L_{slot}} + (1-f) \times (1 - BER_{clean})^{L_{slot}} \quad (5)$$

- BER depends on the SINR and is calculated in the form of $Q(\sqrt{2 \cdot \mathrm{SINR}})$
- *Q-function* denotes the upper tail cumulative distribution function of a standard Gaussian distribution.

Here, $(1 - BER_{jammed})^{L_{slot}}$ represents the SRR for jammed channels and $(1 - BER_{clean})^{L_{slot}}$ represents the SRR for the other channels. The MRR for the FHSS techniques followed a similar approach. However, FJ techniques utilize beamforming to focus signals in the desired direction and employ cooperative jamming to achieve indirect interference mitigation. This study assumed that legitimate receivers obtain approximately G = 3 dB of the received gain through beamforming. This represents an ideal combination of gains achieved using two transmitting antennas in beamforming (Nguyen et al., 2022). Moreover, cooperative jamming signals were assumed to be generated at partial power, considering that the original jamming signal strength was reduced by approximately 50% (J_{legit} = 0.5) for legitimate receivers. The receivers were then configured accordingly. Based on these assumptions, the BER for the FJ techniques was calculated using Equation (6).

$$BER_{FJ} = Q\left(\sqrt{\frac{SNR_{legit}+G}{1+J_{legit}\cdot\left(\frac{Interference}{Noise}\right)}}\right) \quad (6)$$

The SRR for the FJ techniques was calculated as $\left(1 - BER_{FJ}\right)^{L_{slot}}$, and the MRR was derived by weighting according to f.

In the proposed technique, when the number of successfully received shares is denoted as S, the MRR becomes $\sum_{i=k}^{n}\binom{n}{i}S^i(1-S)^{n-i}$. Here, S is calculated as $(1-BER)^{L_{share}}$, where L_{share} represents the length of each share. The proposed technique has the advantage of enabling complete message reconstruction even when some shares are lost. Based on these principles, the simulation results for evaluating the MRR of each technique according to the SINR are presented in Figure 3.

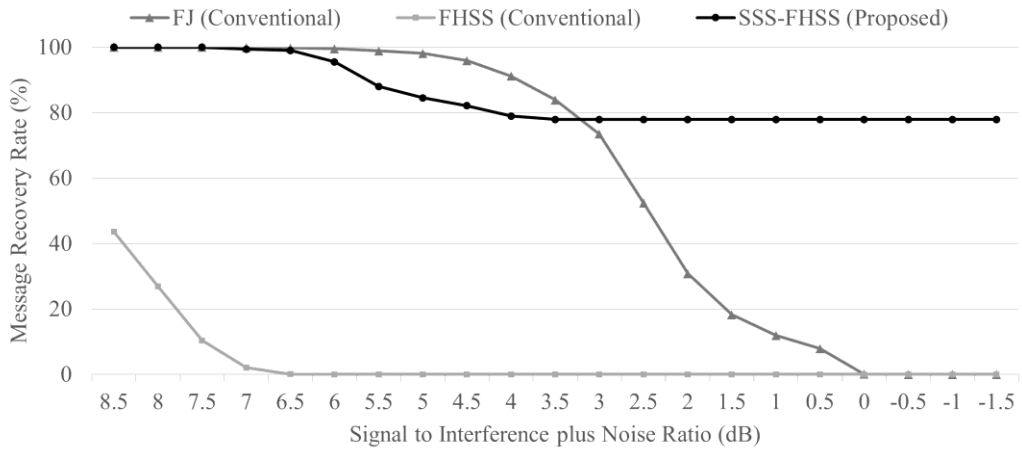


Figure 3: MRR (%) of FJ, FHSS, and the proposed SSS-FH technique as a function of SINR (dB).

According to the experimental results, the FHSS techniques exhibited the most vulnerable performance to jamming attacks, with the SINR decreasing to below 6.5 dB. The FJ techniques maintained an MRR above 99% until approximately 7.0 dB, demonstrating their ability to recognize beamforming gains and cooperative jamming effects. However, the performance significantly degraded thereafter, converging to 0% below 0 dB. Conversely, the proposed technique achieved a 100% MRR above 8.0 dB, showing optimal performance, and maintained a high MRR above 95% even in the 7.0-6.0 dB range. Furthermore, even under severe jamming conditions with an SINR below 5.0 dB, the technique maintained approximately 77% stable performance, demonstrating superior results compared to FJ and FHSS. These results indicate that, while the proposed technique maintains stable communication even under partial losses in strong jamming environments, conventional techniques face stringent conditions requiring complete message reconstruction.

4.3 Data Confidentiality

This experiment evaluated Eve's MRR based on the information leakage rate (ILR). The ILR is defined as the probability that Eve can identify and synchronize with the transmission slot structure. Higher values indicate that Eve has acquired more temporal structural information. This study evaluated this parameter across a range of 0% to 100%. Eve's MRR is defined by the ILR and the probability that synchronized slots are correctly reconstructed from the leaked information, calculated using Equation (7).

$$MRR_{conventional}^{Eve} = ((ILR \times SRR)^{[L_{frame}/L_{slot}]})^{[L_m/L_{frame}]} \quad (7)$$

The confidentiality of FHSS techniques depends on the unpredictability of the FH patterns. Here, ILR is defined as the probability that Eve correctly identifies the frequencies in each slot when the hopping pattern is not perfectly known, thereby calculating Eve's MRR. Conversely, FJ techniques assume that Eve can intercept jamming signals in the present environment, reducing Eve's SNR to -3

dB ($J_{eve} = -3\ dB$). This reflects an environment in which Eve faces interference when attempting to intercept, which causes the effective received SNR_{eve} to decrease substantially. Consequently, Eve's BER increased, and the SRR decreased. In the proposed technique, if Eve obtains fewer than k shares, message reconstruction becomes impossible, which results in an MRR of 0%. Here, the probability that Eve successfully obtains individual shares is defined as $ILR \times S$, and message reconstruction follows Equation (8).

$$MRR_{Proposed}^{Eve} = \sum_{i=k}^{n} \binom{n}{i} (ILR \times S^i)(1 - ILR \times (1 - S))^{n-i} \quad (8)$$

Figure 4 presents the comparative evaluation results of each model under these conditions.

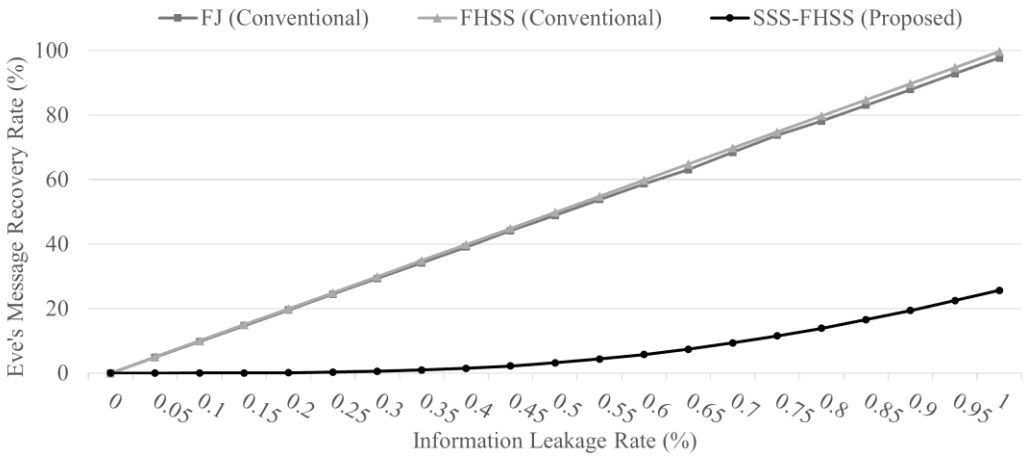


Figure 4: Eve's MRR (%) for FJ, FHSS, and the proposed SSS-FH technique as a function of ILR (%).

Experimental results demonstrated that at 20% ILR, FHSS Eve achieved 19.9% MRR, whereas FJ Eve recorded 19.5% MRR, indicating similar eavesdropping vulnerabilities of 59.9% and 58.6%, respectively, at 60% ILR. Under severe eavesdropping conditions at 80% ILR, FHSS Eve achieved 79.8% MRR, and FJ Eve recorded 78.2% MRR, revealing high eavesdropping vulnerability in both techniques. Conversely, with the proposed technique, Eve maintained a 0.01% MRR at 20% ILR and a 5.8% low MRR at 60% ILR. Even under 80% ILR conditions, Eve's MRR remained limited to 13.9%, demonstrating a confidentiality performance more than 65%p higher than that of conventional techniques.

4.4 Communication Efficiency

In this section, we analyzed the transmission delay times of each technique to measure the comprehensive communication efficiency. The total transmission time for FHSS and the proposed technique was calculated by summing the slot-based transmission losses, as expressed in Equation (9).

$$T_{FHSS} = [L_m / L_{slot}] \times (T_{slot} + T_{guard} + T_{tune}) \quad (9)$$

where T_{slot} represents the message transmission time, T_{guard} denotes the guard time, and T_{tune} indicates the time required for frequency synchronization. In the proposed technique, all the shares should be transmitted, resulting in a total slot count of n$\times$ $[L_{share}/L_{slot}] \times [L_m/L_{frame}]$. FJ techniques

transmit across 10 channels in parallel, reducing the delay time transmission, but incurring beam switching and cooperative jamming overhead, as calculated by Equation (10).

$$T_{FJ} = \{\frac{L_m/L_{slot}}{N}] \times (T_{slot} + T_{guard} + T_{switch}) + T_{coord} \quad (10)$$

Here, N represents the number of available channels, T_{switch} denotes the time required for beam-direction switching, and T_{coord} represents the overhead for cooperative node coordination. To evaluate the overall performance comprehensively, a communication efficiency metric incorporating jamming resilience, data confidentiality, and latency is defined in Equation (11).

$$\text{Communication Efficiency} = \frac{Message\ Recovery\ Rate_{legit} \times (1 - Message\ Recovery\ Rate_{EVE})}{Latency} \quad (11)$$

This metric enabled a comparative assessment of the effectiveness of each technique. The numerator represents the product of the legitimate receiver's MRR and Eve's message recovery failure rate, and indicates the degree to which jamming resilience and confidentiality are secured during communication. The denominator represents the latency by calculating the transmission time per unit time. Figure 5 shows the comprehensive effectiveness variations of each technique by varying the SINR under ILR conditions of 30%, 60%, and 90%, thereby evaluating the relative performance priorities at different threat levels.

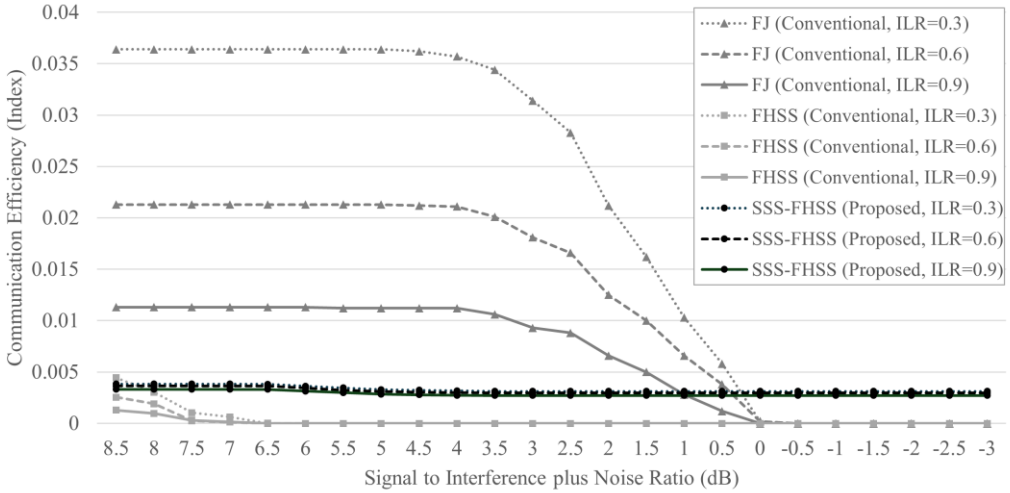


Figure 5: Communication efficiency (Index) for FJ, FHSS, and the proposed SSS-FH technique as a function of SINR (dB) under different ILR (30%, 60%, and 90%).

The experimental results demonstrate that FHSS techniques exhibit efficiencies approaching zero when the SINR decreases below 6.5 dB. FJ techniques maintained relatively high efficiency in the 1.0-7.5 dB SINR range but gradually decreased with lower SINR values, converging to zero below 0 dB. Conversely, the proposed technique maintained a consistent efficiency across all experimental conditions, demonstrating stable performance even when the SINR decreased below 0 dB. While conventional techniques experience performance degradation in jamming environments above certain levels, the proposed technique operates stably across the entire SINR range, with the relative advantages becoming more pronounced under stronger jamming conditions. Although FJ techniques exhibit a relatively high efficiency above 0 dB SINR, they require multi-antenna beamforming and CSI

estimation to control the legitimate receiver and Eve directions, incurring additional resources and computational costs. Considering these limitations, the proposed technique, which maintains stable efficiency without additional resources, is a more practical alternative for real-world applications.

5 Conclusion

Satellite communications offer the advantage of continuous communication over wide areas, but are vulnerable to jamming and eavesdropping while being constrained by limited computational resources, making it challenging to achieve both security and efficiency simultaneously. Furthermore, conventional research approaches exhibit limitations as they require high computational complexity or depend on CSI. To address these issues, this study proposes an SSS-FH technique, which divides messages into shares and transmits them across frequency-time slots. The proposed technique achieved a 77.9%p higher MRR than FJ and FHSS in 0 dB SINR environments and maintained the highest performance as the jamming intensity increased. Moreover, in environments with increasing ILR, the proposed technique demonstrated a 42.1%p lower Eve's MRR than FJ and approximately 43.2%p lower than that of FHSS. The communication efficiency evaluation results showed that the proposed technique maintained consistent efficiency levels across all SINR ranges, recording approximately 0.3%p higher efficiency than FJ and FHSS, even under extreme jamming conditions below 0 dB SINR, thereby demonstrating superior performance. Future research is planned to propose techniques for reducing latency and validate these approaches in actual satellite communication testbeds.

Acknowledgements. This work was supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry [grant number RS-2024-00415520] supervised by the Korea Institute for Advancement of Technology (KIAT), the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program [grant number IITP-2022-RS-2022-00156310] and National Research Foundation of Korea (NRF) grant [RS-2025-00518150], and the Information Security Core Technology Development program [grant number RS-2024-00437252] supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP).

References

Luo, X., Chen, H., & Guo, Q. (2024). LEO/VLEO Satellite Communications in 6G and Beyond Networks–Technologies, Applications, and Challenges. *IEEE Network*, 38, 273-285. Retrieved from https://doi.org/10.1109/mnet.2024.3353806.

Xiao, Y., Ye, Z., Wu, M., Li, H., Xiao, M., Alouini, M., Al-Hourani, A., & Cioni, S. (2024). Space-Air-Ground Integrated Wireless Networks for 6G: Basics, Key Technologies, and Future Trends. *IEEE Journal on Selected Areas in Communications*, 42, 3327-3354. Retrieved from https://doi.org/10.1109/jsac.2024.3492720.

Centenaro, M., Costa, C., Granelli, F., Sacchi, C., & Vangelista, L. (2021). A Survey on Technologies, Standards, and Open Challenges in Satellite IoT. *IEEE Communications Surveys & Tutorials*, 23, 1693-1720. Retrieved from https://doi.org/10.1109/COMST.2021.3078433.

Wang, Q., Li, W., Yu, Z., Abbasi, Q., Ansari, S., Sambo, Y., Wu, L., Li, Q., & Zhu, T. (2023). An Overview of Emergency Communication Networks. *Remote. Sens.*, 15, 1595. Retrieved from https://doi.org/10.3390/rs15061595.

Li, X., Feng, W., Wang, J., Chen, Y., Ge, N., & Wang, C. (2020). Enabling 5G on the Ocean: A Hybrid Satellite-UAV-Terrestrial Network Solution. *IEEE Wireless Communications*, 27, 116-121. Retrieved from https://doi.org/10.1109/MWC.001.2000076.

Wang, J., Jiang, C., Kuang, L., & Han, R. (2024). Satellite Multi-Beam Collaborative Scheduling in Satellite Aviation Communications. *IEEE Transactions on Wireless Communications*, 23, 2097-2111. Retrieved from https://doi.org/10.1109/TWC.2023.3295382.

Gujar, S. (2024). Satellite Communication (SATCOM) Market Size – Solution, Platform, Frequency, Industry Vertical Analysis, Share, Growth Forecast, 2025–2034. *Global Market Insights Inc*. Retrieved from https://www.gminsights.com/industry-analysis/satellite-communication-market

Kang, M., Park, S., & Lee, Y. (2024). A Survey on Satellite Communication System Security. *Sensors (Basel, Switzerland),* 24. Retrieved from https://doi.org/10.3390/s24092897.

Zhang, Y., Zhao, S., He, J., Zhang, Y., Shen, Y., & Jiang, X. (2023). A Survey of Secure Communications for Satellite Internet based on Cryptography and Physical Layer Security. *IET Inf. Secur.*, 2023, 1-15. Retrieved from https://doi.org/10.1049/2023/5604802.

Tedeschi, P., Sciancalepore, S., & Pietro, R. (2021). Satellite-Based Communications Security: A Survey of Threats, Solutions, and Research Challenges. *Comput. Networks,* 216, 109246. Retrieved from https://doi.org/10.1016/j.comnet.2022.109246.

Li, B., Fei, Z., Zhou, C., & Zhang, Y. (2020). Physical-Layer Security in Space Information Networks: A Survey. *IEEE Internet of Things Journal,* 7, 33-52. Retrieved from https://doi.org/10.1109/JIOT.2019.2943900.

Duan, P., Zou, B., Hu, Y., Liu, G., Zhang, X., & He, Y. (2024). Optimization of Adaptive Frequency Hopping Strategies for Satellite Communications Applying LSTM Neural Networks. *2024 IEEE 2nd International Conference on Electrical, Automation and Computer Engineering (ICEACE),* 42-47. Retrieved from https://doi.org/10.1109/ICEACE63551.2024.10898856.

Bentoutou, Y., Bensikaddour, E., Taleb, N., & Bounoua, N. (2020). An improved image encryption algorithm for satellite applications. *Advances in Space Research, 66,* 176-192. Retrieved from https://doi.org/10.1016/j.asr.2019.09.027.

Pirzada, S., Murtaza, A., Xu, T., & Liu, J. (2020). Architectural Optimization of Parallel Authenticated Encryption Algorithm for Satellite Application. *IEEE Access*, 8, 48543-48556. Retrieved from https://doi.org/10.1109/ACCESS.2020.2978665.

Jeon, S., Kwak, J., & Choi, J. (2022). Cross-Layer Encryption of CFB-AES-TURBO for Advanced Satellite Data Transmission Security. *IEEE Transactions on Aerospace and Electronic Systems*, 58, 2192-2205. Retrieved from https://doi.org/10.1109/taes.2021.3134988.

Liu, S., Zhu, X., Chen, H., & Han, Z. (2023). Secure Communication for Integrated Satellite–Terrestrial Backhaul Networks: Focus on Up-Link Secrecy Capacity Based on Artificial Noise. *IEEE Wireless Communications Letters*, 12, 1369-1373. Retrieved from https://doi.org/10.1109/lwc.2023.3274761.

Nguyen, T., Van Chien, T., Tran, D., Phan, V., Voznák, M., Chatzinotas, S., Ding, Z., & Poor, H. (2023). Security-reliability tradeoffs for satellite–terrestrial relay networks with a friendly jammer and imperfect CSI. *IEEE Transactions on Aerospace and Electronic Systems, 59,* 7004-7019. Retrieved from https://doi.org/10.1109/TAES.2023.3282934.

Kim, S., & Pham, K. (2025). Integrated navigation and frequency-hopping communication. *Proceedings of the 2025 International Conference on Computing, Networking and Communications (ICNC)* (pp. 813-817). IEEE. Retrieved from https://doi.org/10.1109/ICNC64010.2025.10993775.

Adi Shamir. (1979). How to share a secret. *Commun. ACM 22*, 11 (Nov. 1979), 612–613. Retrieved from https://doi.org/10.1145/359168.359176

Nguyen, H., & Noubir, G. (2022). Universal Beamforming: A Deep RFML Approach. *Proceedings of the 25th International ACM Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*. Retrieved from https://doi.org/10.1145/3551659.3559041.