Enhancing NextG Wireless Security: A Lightweight Secret Sharing Scheme with Robust Integrity Check for Military Communications

Abhisek Jha[1], SeyedMohammad Kashani[2], Mohammadi Hossein[3], Andre Kirchner[3], Minglong Zhang[3],
Rémi A. Chou[1], Sang Wu Kim[2], Hyuck M. Kwon[4],Vuk Marojevic[3], Taejoon Kim[5]
[1]Dept. of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX, USA
[2]Dept. of Electrical and Computer Engineering, Iowa State University, Ames, IA, USA
[3]Dept. of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS, USA
[4]Dept. of Electrical and Computer Engineering, Wichita State University, Wichita, KS, USA
[5]School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ, USA
Email: akj9565@mavs.uta.edu, kashani@iastate.edu, hm1125@msstate.edu, amk694@msstate.edu,
mz354@msstate.edu, hyuck.kwon@wichita.edu,
vuk.marojevic@ece.msstate.edu, swkim@iastate.edu, remi.chou@uta.edu, taejoonkim@asu.edu

Multipath communication is a promising approach to enhance confidentiality and resilience in NextG wireless communications, particularly in critical military applications. By integrating threshold secret sharing with multipath communication, we can further protect against attacks that target a single path. However, most existing schemes rely on computationally demanding polynomial interpolation, which limits their practicality in real-world scenarios. This paper introduces a lightweight XOR-based secret sharing scheme, coupled with an efficient two-dimensional (2D) integrity check mechanism, specifically designed for multipath communication scenarios. The proposed scheme significantly reduces computational overhead, achieving a 13.42x faster encoding time and a 360x faster decoding speed compared to Shamir's Secret Sharing, using an input size of 8.2 KB. Our method ensures the secure and resilient transmission of data, even in adversarial environments, by effectively detecting and pinpointing tampered shares.

***Index Terms*—Multipath, Perfect Security, DoS, Resilient Communication**

I. Introduction

The rapid advancement of wireless communication has revolutionized communication systems, offering unprecedented opportunities for military applications [1], [2]. Military reliance on NextG communication is expected to increase significantly, particularly in foreign territories where secure and resilient communication is essential [3], [4]. However, this dependence introduces new challenges, as these networks must operate on hostile and unpredictable conditions.

Ensuring the confidentiality, integrity, and availability of communications in such environments is one of the most pressing challenges [2]. Approaches such as encryption and redundancy, while effective, may not be sufficient to meet the demands of future-sensitive military applications, as adversaries equipped with sophisticated jamming capabilities can disrupt communications [5].

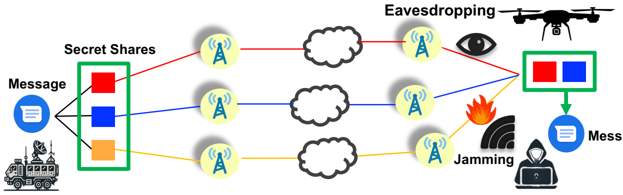

Fig. 1: Conceptual illustration of the proposed secret sharing multipath scheme for NextG networks.

Multipath communication has emerged as a promising solution to enhance the resilience and security of networks, particularly in critical military applications [6]–[8]. Transmitting data over multiple paths significantly increase the difficulty for adversaries to intercept and reconstruct the entire message. Figure 1 illustrates the conceptual framework of this multipath communication scheme, demonstrating how secret sharing can be integrated to secure transmissions across various paths in wireless networks.

In this context, related work has leveraged secret sharing in a multipath scenario to further enhance communication security and resilience [8]–[10]. Distributing communication across multiple paths and applying secret sharing techniques ensures that eavesdropping on any single path will not reveal any information about the message. Moreover, the message can still be recovered even if some packets are modified or lost on a single path, providing defense against jamming and other disruptive attacks.

Research Significance

Most related works utilize polynomial interpolation-based secret sharing approaches, which are computationally intensive and may face challenges in detecting erroneous and tampered shares, especially in wireless network environments.

This paper introduces a lightweight secret sharing scheme that integrates a 2D integrity check mechanism, specifically optimized for multipath scenarios. Our simulation results demonstrate a 360x improvement in decoding speed and a 13.42x faster encoding time compared to traditional polynomial interpolation as in Shamir's secret sharing.

The performance gains of our proposed scheme stem from the use of simple bitwise XOR operations for both encoding and decoding processes. Unlike Shamir's Secret Sharing, which relies on polynomial arithmetic over finite fields, our method reduces computational complexity, leading to faster processing times and lower energy consumption. This efficiency is particularly beneficial for resource-constrained devices such as military drones and IoT sensors, where computational resources and energy availability are limited.

The remainder of this paper is organized as follows: Section II provides an analysis of existing secret sharing and integrity check mechanisms within the context of multipath applications. Section III presents the methodology of our proposed schemes. Section V compares and highlights the advantages of the encoding and decoding runtime of our scheme with state-of-the-art approaches. Section IV presents the security analysis of the proposed XOR-based multipath communication scheme. Finally, Section VI discusses further directions for enhancing security and efficiency.

II. Literature Review

Wireless Communication has brought transformative potential to military operations. Unlike previous generations, 5G is designed to connect a vast array of devices, which could support smart military bases and autonomous operations. Additionally, key technologies such as millimeter-wave communication, massive MIMO, and device-to-device (D2D) communication enable ultra-reliable and low-latency communications (URLLC), which are crucial for mission-critical operations [1].

Despite its numerous advantages, the 5G standard introduces a range of security challenges critical for military applications. One primary concern is the increased attack surface resulting from the vast number of connected devices in 5G networks [2], [3]. Integrating IoT devices, sensors, and autonomous systems in military operations means that each connected device could potentially serve as an entry point for cyber threats. Additionally, higher frequency bands, such as millimeter waves, pose new physical security and interference challenges. Although these bands offer higher data rates and reduced latency, they are also more susceptible to physical obstacles and interference, which adversaries could exploit to disrupt communications [5].

Emerging threats such as Distributed Denial of Service (DDoS) attacks and signaling storms are particularly concerning in 5G and next generation networks due to the increased interconnectivity of devices [5]. In military applications, these threats can disrupt critical communications and operations. Countermeasures like network slicing and anomaly detection systems are under development to address these issues, though their effectiveness in highly dynamic and adversarial environments is still under evaluation [1], [2].

Addressing these challenges in the future generation networks is essential. This effort requires the development of advanced encryption methods, jamming resistance techniques, and robust integrity check schemes to protect critical military communications in the NextG era.

A. Multipath Secret Sharing

Multipath communication emerges as a promising solution to enhance the resilience and security of future communication infrastructure. By spreading data across multiple channels, this approach significantly reduces the likelihood that an adversary can intercept and reconstruct the message [6], [7]. Additionally, multipath communication provides redundancy, ensuring that communication remains robust even if some paths fail due to network disruptions or attacks [6], [7].

Existing solutions often combine multipath communication with secret sharing to enhance the overall network security [8]–[11]. Distributing shares across multiple paths, provides both security and fault tolerance against eavesdropping or Denial of Service (DoS) attacks. However, secret sharing often involves significant computational and communication overhead, which may limit their applicability in resource-constrained environments like drones and IoT devices [12].

For instance, in SPREAD [8], Shamir's Secret Sharing is employed to divide a secret message into multiple shares using a threshold scheme, where any T shares are sufficient to reconstruct the message. However fewer than T shares provide no information about the secret [13]. These shares are transmitted across multiple paths in the network using a multipath routing algorithm. This approach ensures that even if some paths are compromised, an adversary must intercept shares from at least T different paths to reconstruct the message. Multipath routing enhances security by selecting paths with minimal overlap and making it significantly harder for an attacker to capture enough shares to decrypt the message successfully.

Despite high-security guarantees, scalability remains a significant concern, as increasing the number of shares adds complexity to the encoding and decoding process, which requires polynomial interpolation [7], [9], [13]. Additionally, Shamir's secret sharing does not detect tampered shares.

B. Integrity Check

Message Authentication Code (MAC) mechanisms are essential for detecting and preventing the use of modified shares, thereby ensuring the integrity of the secret. However, attaching individual tags to every share significantly increases bandwidth utilization and imposes substantial computational overhead.

To mitigate this issue, [14] proposed an approach that aggregates the tags of multiple messages before transmission, effectively reducing the required bandwidth. Similarly, other works have attempted to minimize the overhead associated with MAC calculation and transmission by concatenating messages and generating a single tag for the combined data [15].

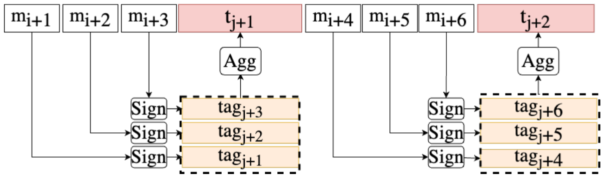

Fig. 2: The Aggregate MAC scheme reduces the number of transmitted tags, with t_j representing the combined tag for multiple messages m_i.

Figure 2 illustrates the concept of the Aggregate MAC scheme, where multiple message tags are combined into a single tag, reducing the total number of tags transmitted, as proposed in [14].

While the aggregation schemes proposed in [14], [15] are effective in maintaining the integrity of a group of shares, they fall short in identifying which specific share within the group has been tampered with if the combined tag is invalid. Some approaches, such as those presented in [16], [17], offer solutions to detect the altered share within the group, but this comes at the cost of increased overhead and complexity.

The need for an integrity check mechanism that can efficiently pinpoint modified shares without introducing significant overhead remains largely unaddressed in the literature.

In this paper, we address the challenges of integrating secret sharing algorithms in multipath scenarios by proposing a lightweight XOR-based secret sharing scheme. This scheme is combined with an integrity check mechanism that can precisely pinpoint tampered shares, thereby ensuring the integrity of the secret.

III. Methodology

This section presents a XOR-based secret sharing scheme optimized for multipath communication suitable for NextG networks, focusing on minimal computational overhead and efficient integrity checks. We begin by formulating the threat model, followed by a detailed description of the proposed secret-sharing algorithm. Finally, we introduce the 2D integrity check mechanism that is optimized for multipath scenarios, allowing for the detection of tampered shares.

A. Threat Model

We assume the adversary operates within a wireless communication environment, possessing the capability to eavesdrop on communication paths and jam wireless signals, leading to potential denial of service (DoS) by preventing legitimate messages from being transmitted or received. The adversary is also capable of injecting fraudulent messages into the network, modifying intercepted messages, replaying previously captured transmissions, and deleting messages to disrupt the communication flow. These capabilities pose significant risks to the integrity, confidentiality, and availability of the communication system.

B. XOR-based Secret Sharing

The original message is split, encoded, and transmitted across diverse paths.

1) Message Encoding

The message M is a binary sequence split into two parts, M_1 and M_2, of same size (zero-padding is used if the length of M is odd). R_1 and R_2 are random binary sequences with the same size as M_1. The message is encoded in three parts as

$$E_1 = \begin{pmatrix} R_1 \\ M_2 \oplus R_2 \end{pmatrix},\ E_2 = \begin{pmatrix} M_1 \oplus R_1 \\ R_2 \end{pmatrix},\ E_3 = \begin{pmatrix} M_1 \oplus R_2 \\ M_2 \oplus R_1 \end{pmatrix}$$

where $\oplus$ denotes the bit-wise XOR operation.

2) Transmission

The three parts E_1, E_2, E_3 are transmitted via different communication paths. The number of paths L is selected to be greater than the number of paths z that could be affected by DoS attacks. However, in this paper, we focus on $L = 3$ and $z = 1$ for simplicity.

3) Message Decoding

The receiver must observe at least two of the three paths, to reconstruct the message M. Specifically, the message can be recovered using the combination of any two of the three shares (E_1, E_2, E_3) as follows:

- **Using** E_1, E_2: Recover R_1 from $E_1[1]$, R_2 from $E_2[2]$. Derive $M_1 = E_2[1] \oplus R_1$ and $M_2 = E_1[2] \oplus R_2$.
- **Using** E_2, E_3: Recover R_2 from $E_2[2]$, then $M_1 = E_3[1] \oplus R_2$, $R_1 = E_2[1] \oplus M_1$, and $M_2 = E_3[2] \oplus R_1$.
- **Using** E_1, E_3: Recover R_1 from $E_1[1]$, then $M_2 = E_3[2] \oplus R_1$, $R_2 = E_1[2] \oplus M_2$, and $M_1 = E_3[1] \oplus R_2$.

C. Integrity Check Mechanism

To address the challenge of tampered shares in wireless environments, one practical solution is to generate and transmit Hash-based Message Authentication Codes (HMAC) for each share, ensuring both the integrity and authenticity of the message. Upon receiving a share, the HMAC tag is validated, and the share is either retained or discarded based on the validation result. To further enhance efficiency beyond appending a single tag per share, we extend the approach proposed in [14], [15], [17] by transitioning from a one-dimensional to a two-dimensional scheme. In this extended method, shares from multiple secrets are organized into a 2D matrix arrangement, where tags are calculated for both rows and columns.

For instance, Figure 3 illustrates a system's 2D integrity check mechanism utilizing three distinct paths, where three sets of shares are generated for three messages. These shares are arranged in a two-dimensional matrix. This approach allows for efficient integrity verification by leveraging the combined row and column tags.

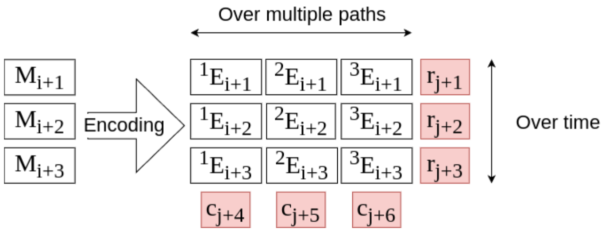

Fig. 3: 2D integrity for 3x3 arrangement.

To further discuss the benefits of this approach, let us consider the following example, where if share ${}^{2}E_{i+2}$ is altered, the corresponding tags c_{j+5} and r_{j+2} will detect and precisely pinpoint the modification. This method utilizes the time domain to calculate column tags c_j and takes advantage of different paths in a multipath setup to calculate row tags r_j.

While this scheme effectively pinpoints a single modified packet, it guarantees the detection of two or more modifications.

IV. Security Analysis

In this section, we analyze the security features of the proposed XOR-based multipath communication scheme, particularly focusing on its resilience against various attacks, including Denial-of-Service (DoS) attacks, and its robustness in the presence of noise and interference, and security against data manipulation.

A. Resilience Against DoS Attacks

Unlike traditional methods that rely on the security measures provided by the base station, our approach is independent of such constraints, making it suitable for deployment in adversarial environments.

a) Attack-Agnostic Design: The system is built to withstand any DoS attack on a single communication path.

b) Multipath Strategy: By splitting the original message into multiple encoded portions and transmitting them over diverse communication paths, the method ensures that if at most one path becomes unavailable, then the message can still be reconstructed from the remaining paths.

c) Proactive Approach: The method ensures message delivery by proactively leveraging multiple paths, without the need to first detect an attack.

B. Security Against Eavesdropping

The XOR-based scheme ensures that no single share reveals information about the original message. Specifically, the encoded shares are independent of the original message M:

$$I(E_j; M) = 0, \quad \forall j \in \{1, 2, 3\},$$

where I denotes mutual information.

C. Error Analysis in the Presence of Noise

The reliability and integrity of the system are critical for secure communications, especially in adversarial environments where noise and interference are prevalent. We analyze the probability of error during decoding when the communication paths are subject to jamming and noise, modeling each path as a Binary Symmetric Channel (BSC).

In scenarios involving Additive White Gaussian Noise (AWGN) and Gaussian noise jamming, the received symbol y_0 is represented as:

$$y_0 = x_0 + j_0 + n_0$$

where x_0 is the BPSK transmitted symbol, j_0 is the Gaussian noise jamming signal with power $J = \sigma_j^2$, and n_0 is the AWGN with power $N = \sigma_n^2$. The Signal-to-Interference-plus-Noise Ratio (SINR) is then calculated as:

$$\text{SINR} = \frac{S}{\sigma_j^2 + \sigma_n^2} = \frac{S}{J + N} = \frac{S}{N\left(\frac{J}{N} + 1\right)} = \frac{\text{SNR}}{1 + \text{JNR}}.$$

where SNR is the signal-to-noise ratio and JNR is the jamming-to-noise ratio.

The crossover probability ϵ, which measures the likelihood of a bit being flipped due to noise and interference in the BSC, is given by:

$$\epsilon = Q\left(\sqrt{2\text{SINR}}\right)$$

where Q is the tail probability of the normal density function.

By calculating the crossover probability ϵ, we can optimize the system parameters to enhance the reliability under adverse conditions.

a) Decoding Error Probability: We assess the error probability when decoding the original message M fron pairs of shares, assuming independent bit flips with probability ϵ.

- **Recovering M from (E_1, E_2):**
$$P(M \neq \hat{M}) = 4\epsilon(1 - \epsilon). \tag{1}$$
- **Recovering M from (E_1, E_3):**
$$P(M \neq \hat{M}) = 2\epsilon(1 - \epsilon)\left[2(1 - \epsilon)^2 + 2\epsilon^2 + 1\right]. \tag{2}$$
- **Recovering M from (E_2, E_3):**
$$P(M \neq \hat{M}) = 2\epsilon(1 - \epsilon)\left[1 + 2(1 - \epsilon)^2 + 2\epsilon^2\right]. \tag{3}$$

b) Maximum Bit Error Rate (BER): The maximum Bit Error Rate (BER) is given by

$$\text{BER} \leq 3\epsilon + 2\epsilon^3 \approx 3\epsilon. \tag{4}$$

D. Security Against Data Manipulation

The 2D integrity check mechanism embedded within the scheme efficiently detects and precisely pinpoints any manipulated shares. This feature is vital for maintaining the integrity of the communication.

V. Simulation Result

To evaluate the performance of our proposed XOR-based secret sharing scheme compared to the traditional implementation of Shamir's Secret Sharing scheme [13], we conducted a series of simulations focusing on encoding and decoding runtime with a fixed input size of 8.2 KB.

In our experiments, we compare the coding scheme of Section III-B to a traditional implementation of Shamir's scheme that incloves polynomial interpolation over a finite field. We tested the decoding process for all combinations of the shares to verify the system's efficiency.

The full implementation of the simulation, along with the source code, is available in the GitHub repository.[1]

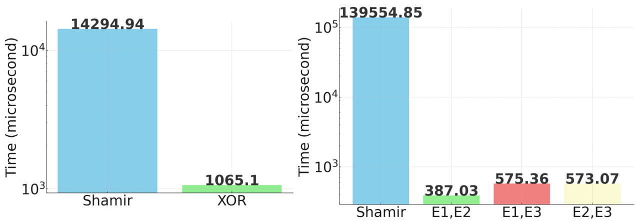

Fig. 4: Average Runtime for Encoding and Decoding.

Figure 4 compares the performance of XOR-based encoding and decoding against Shamir's Secret Sharing scheme for a fixed input size of 8.2 KB. The XOR-based encoder is approximately 13.42 times faster than the Shamir-based encoder. The XOR-based decoder is significantly faster, achieving speedups ranging from approximately 243x to 360x compared to the Shamir-based decoder. This substantial improvement in both encoding and decoding times highlights the efficiency of the XOR-based approach, making it more suitable for applications requiring high-speed processing.

Figure 5, and 6 illustrate the average encoding and decoding runtimes for both Shamir's and XOR-based secret sharing schemes across different input sizes, respectively. The results show that the XOR-based scheme consistently outperforms Shamir's scheme in terms of speed, with the most significant improvements observed as input sizes increase. This demonstrates the scalability and efficiency of the XOR-based approach.

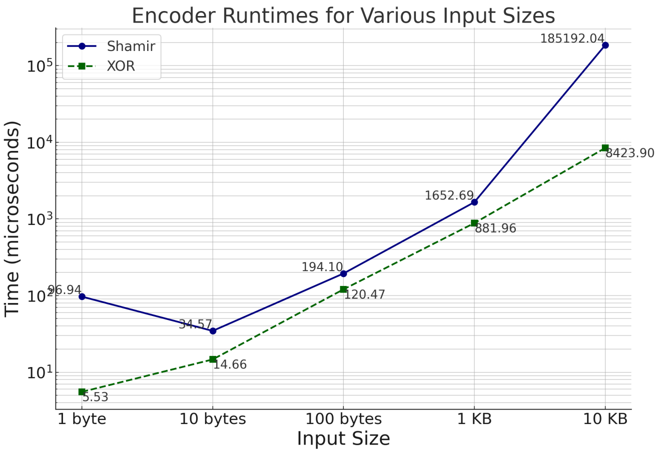

Fig. 5: Average Encoding Runtimes for Various Input Sizes.

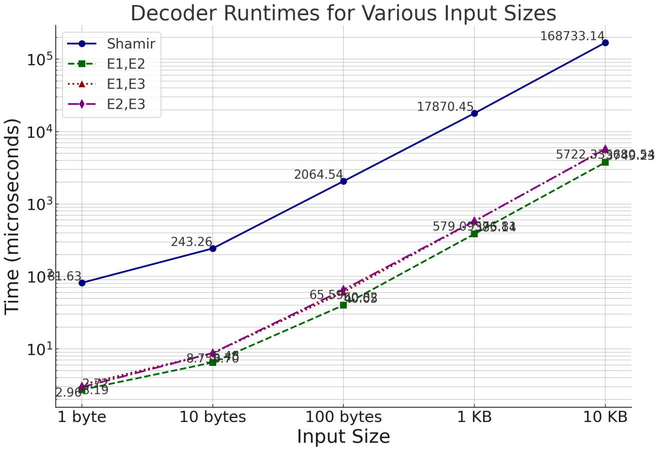

Fig. 6: Average Decoding Runtimes for Various Input Sizes.

A. Communication Cost Analysis

While our scheme reduces computational overhead, transmitting multiple shares increases the total data sent over the network, which impacts both bandwidth and energy consumption, particularly in IoT environments. However, we note that the size of our share is optimal, and thus cannot be improved, given the requirement that no individual share reveals any information about the message, while allowing the message to be reconstructed from any two shares [18].

B. Evaluation of 2D Integrity Check Mechanism

Furthermore, to evaluate the efficiency of the 2D MAC schemes, we have simulated an insider attacker modifying packets with different probabilities. We measured the performance in terms of goodput, which is calculated as the total number of authenticity-verified bits of messages over the total number of bits transmitted.

Fig. 7 demonstrates up to 13% improvements in goodput compared to the traditional scheme where every share has

[1] GitHub repository: https://github.com/abhisekjha/ShamirSSvXORSS

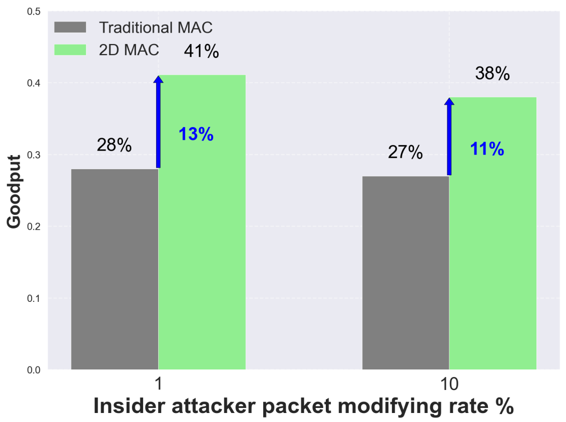

Fig. 7: 2D MAC goodput vs. the Traditional MAC by different packet modifying rate

a tag. On the other hand, 2D MAC might increase the implementation complexity compared to the traditional MAC; however, in applications where goodput is a critical metric, 2D MAC delivers a significant improvement.

VI. Conclusion and Future Work

In this paper, we have introduced an approach to enhance the resilience and security of NextG communication systems, by integrating lightweight XOR-based secret sharing with multipath communication. Our approach efficiently divides messages into multiple shares using XOR operations and transmits them across multiple paths, ensuring that no single compromised relay can jeopardize the overall communication. This strategy provides robust protection against various threats, including eavesdropping and denial-of-service (DoS) attacks on any single path, while maintaining data integrity and minimizing computational overhead.

The performance evaluations demonstrate a 13.42x faster encoding time and a 360x faster decoding speed, highlighting the efficiency of our proposed scheme.

Future research could refine the 2D integrity check to further reduce overhead. Additionally, implementing our approach and exploring its integration with adaptive routing protocols to enhance performance in dynamic network environments could further strengthen its applicability in securing critical applications.

References

[1] L. Bastos, G. Capela, A. Koprulu, and G. Elzinga, “Potential of 5G technologies for military application,” in *International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1–8.

[2] A. Bhardwaj, “5G for military communications,” *Procedia Computer Science*, vol. 171, pp. 2665–2674, 2020.

[3] I. Almaameri and L. Blázovics, “An overview of drones communication, application and challenge in 5G network,” in *6th International Conference on Engineering Technology and its Applications (IICETA)*, 2023, pp. 67–73.

[4] N. Hosseini, H. Jamal, J. Haque, T. Magesacher, and D. W. Matolak, “UAV command and control, navigation and surveillance: A review of potential 5G and satellite systems,” in *IEEE Aerospace Conference*, 2019, pp. 1–10.

[5] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” *IEEE Communications Surveys Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[6] P. M. Mohan, T. J. Lim, and M. Gurusamy, “Fragmentation-based multipath routing for attack resilience in software defined networks,” in *IEEE 41st Conference on Local Computer Networks (LCN)*, 2016, pp. 583–586.

[7] M. Li, A. Lukyanenko, Z. Ou, A. Ylä-Jääski, S. Tarkoma, M. Coudron, and S. Secci, “Multipath transmission for the Internet: A survey,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2887–2925, 2016.

[8] W. Lou, W. Liu, and Y. Fang, “SPREAD: Improving network security by multipath routing,” in *IEEE Military Communications Conference*, vol. 2, 2003, pp. 808–813 Vol.2.

[9] Y. Liu, K. Liu, and M. Li, “A secret sharing scheme based on multipath routing in wireless sensor networks,” *Journal of Sensors*, 2015.

[10] Y. Li, Y. Guo, and G. Xu, “Dynamic security parameters for multichannel secret sharing protocols,” *IEEE Access*, vol. 9, pp. 39 614–39 625, 2021.

[11] D. Wu, J. Liu, and X. Sun, “Secure data transmission in wireless sensor networks using multipath routing and secret sharing,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 3312–3324, 2018.

[12] P. Miao, A. Srinivasan, and P. N. Vasudevan, “Efficient leakage resilient secret sharing,” 2019.

[13] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, p. 612–613, nov 1979.

[14] J. Katz and A. Y. Lindell, “Aggregate message authentication codes,” in *Cryptographers’ Track at the RSA Conference*. Springer, 2008, pp. 155–169.

[15] D. K. Nilsson, U. E. Larson, and E. Jonsson, “Efficient in-vehicle delayed data authentication based on compound message authentication codes,” in *IEEE 68th Vehicular Technology Conference*, 2008, pp. 1–5.

[16] V. Kolesnikov, W. Lee, and J. Hong, “MAC aggregation resilient to DoS attacks,” in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2011, pp. 226–231.

[17] F. Armknecht, P. Walther, G. Tsudik, M. Beck, and T. Strufe, “ProMACs: Progressive and resynchronizing MACs for continuous efficient authentication of message streams,” in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, 2020, p. 211–223.

[18] E. Karnin, J. Greene, and M. Hellman, “On secret sharing systems,” *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 35–41, 1983.