Fortifying 5G Networks: Defending Against Jamming Attacks with Multipath Communications

Hossein Mohammadi, Minglong Zhang, Abhisek Jha*, Vuk Marojevic, Rémi Chou*, Taejoon Kim+

Department of Electrical and Computer Engineering, Mississippi State University, MS, USA
*Department of Computer Science and Engineering, University of Texas at Arlington, TX, USA
+Department of Electrical Engineering and Computer Science, University of Kansas, KS, USA
Email: {hm1125, mz354, vm602}@msstate.edu
*akj9565@mavs.uta.edu, *remi.chou@uta.edu, +taejoonkim@ku.edu

***Abstract*—The advent of 5G technology introduces significant advancements in speed, latency, and device connectivity, but also poses complex security challenges. Among typical denial-of-service (DoS) attacks, jamming attack can severely degrade network performance by interfering critical communication channels. To address this issue, we propose a novel security solution utilizing multipath communication, which distributes message segments across multiple paths to ensure message recovery even when some paths are compromised. This strategy enhances network resilience and aligns with zero-trust architecture principles. Moreover, the proposed scheme has been implemented in our testbed to validate the concept and assess the network performance under jamming attacks. Our findings demonstrate that this method eliminates the negative impacts caused by DoS attacks, maintaining the integrity and availability of critical network services. The results highlight the robustness of multipath communication in securing 5G networks against sophisticated attacks, thereby safeguarding essential communications in dynamic and potentially hostile environments.**

I. Introduction

The advancement of 5G technology offers remarkable speed, lower latency, and the capability to connect many devices simultaneously. However, 5G networks still face significant security challenges, particularly jamming attacks, which can severely impact network performance. To address this, we introduce a multipath strategy for 5G networks that enhances security by distributing message segments over multiple paths, ensuring message recovery even when some paths are compromised, in alignment with zero-trust architecture principles [1].

Our research implements this multipath strategy on a 5G testbed using open-source software srsRAN and software-defined radio (SDR) devices. We detail how this strategy secures communications under jamming attacks and describe the 5G testbed setup and multipath implementation. Extensive experiments involving unexpected jamming attacks demonstrate that our approach maintains reliable communications and preserves critical network service integrity.

II. Principles of the Multipath Technique

The main idea of the coding scheme in the multipath method is inspired by [2] and depicted in Fig. 1 for a three-path case ($L = 3$) and a denial of service attack on any one of the paths ($z = 1$). The ad-hoc codes in the coding scheme adopt exclusive-or (XOR) operations, avoiding computationally demanding finite field operations. The core of our solution is a network coding approach that leverages the existing infrastructure of multiple network providers.

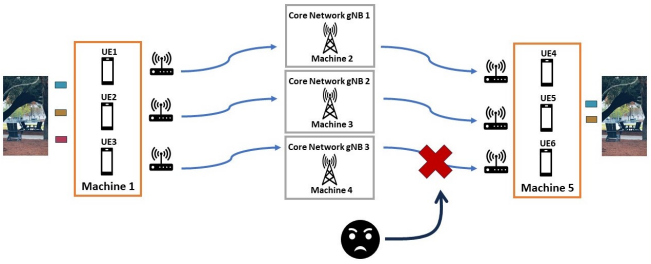

Fig. 1. Conceptual illustration of the proposed multipath communications.

In Fig. 1, assume that the message to be transmitted M is a sequence of bits that are split into 2 sub-sequences of same length, i.e., $M = M_1 \| M_2$, where $\|$ denote concatenation. Then, M is encoded into three shares E_1, E_2, E_3 that are sent over three different communication paths as

$$E_1 = M_1, E_2 = M_2, E_3 = M_1 \oplus M_2,$$

where the notation $\oplus$ denotes the bit-wise XOR operation. Apparently, the original message M can be reconstructed by any two shares, which defends against jamming attacks occurring in any one path.

The coding scheme can be extended for more complex scenarios. As a case in point, considering a case with $L = 4$ and $z = 2$, M is split into 8 sub-sequences of same length, i.e., $M = M_1 \| M_2 \| M_3 \| M_4 \| M_5 \| M_6 \| M_7 \| M_8$. Then, M is encoded into four parts E_1, E_2, E_3, E_4 (each part is sent over a different communication path) as

$$E_1 = \begin{pmatrix} M_1 \\ M_2 \oplus M_8 \\ M_3 \oplus M_7 \\ M_4 \oplus M_6 \end{pmatrix}, E_2 = \begin{pmatrix} M_1 \oplus M_5 \\ M_2 \\ M_3 \oplus M_8 \\ M_4 \oplus M_7 \end{pmatrix},$$

$$E_3 = \begin{pmatrix} M_1 \oplus M_6 \\ M_2 \oplus M_5 \\ M_3 \\ M_4 \oplus M_8 \end{pmatrix}, E_4 = \begin{pmatrix} M_1 \oplus M_7 \\ M_2 \oplus M_6 \\ M_3 \oplus M_5 \\ M_4 \end{pmatrix}.$$

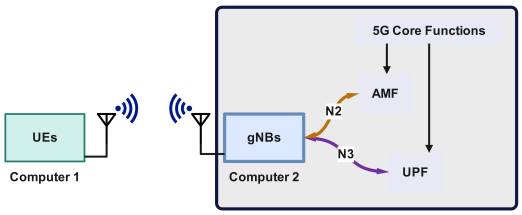

Fig. 2. srsRAN 5G over the air testbed architecture

Obviously, M can be recovered from any two parts above, meaning that our coding strategy is resilient to attacks on two communication paths. Moreover, our coding strategy is lightweight. Specifically, for the case with 4 paths, the encoding and decoding only needs $\frac{3}{2}|M|$ and $\frac{3}{4}|M|$ bit-wise XOR operations, respectively.

III. Implementation on 5G Testbed

A. Testbed Setup

As depicted in Fig. 2, the 5G over-the-air testbed consists of the following components. **User Equipment (UEs):** Multiple UEs (3 UEs as the source for uplink and 3 UEs in the downlink as the destination) emulated by adopting srsRAN to represent end-user devices, capable of connecting to multiple gNBs for multipath communication. **gNodeBs (gNBs):** Three gNBs deployed on separate machines to provide connectivity to UEs, supporting simultaneous connections and facilitating multipath routing. **5G Core Functions:** The 5G core network includes essential components such as the Access and Mobility Management Function (AMF) and User Plane Function (UPF), responsible for managing session states, mobility, and routing data packets. **Network Interfaces:** Interfaces between UEs, gNBs, and the 5G core are established over standardized protocols (N2 and N3 interfaces). The N2 interface handles control plane signaling, while the N3 interface manages user plane data.

In Fig. 1, the testbed setup slightly differs with the conceptual gragh as shown in Fig. 1. In this configuration, Machines 1 and 5 are connected to six USRP B210 devices acting as UEs, with three serving as sources and three as destinations to enable end-to-end communication. Machines 2, 3, and 4 in Fig. 1 function as the gNBs and the 5G core. The computers used for UEs and gNBs are equipped with 11th Gen Intel Core i9 processors featuring 16 cores running at 3.5 GHz and 64 GB of memory.

B. Implementation of Multipath Based on the Testbed

Our multipath communication strategy leverages the distributed nature of the testbed to enhance network resilience. The implementation involves the following steps: **1) Message segmentation:** messages are divided into smaller segments before transmission. Each segment is independently encoded and prepared for transmission over different paths. **2)Path selection:** multiple paths are dynamically selected based on network conditions and availability through the transmitter side. The paths traverse different gNBs to ensure redundancy. **3) Transmission and monitoring:** segments

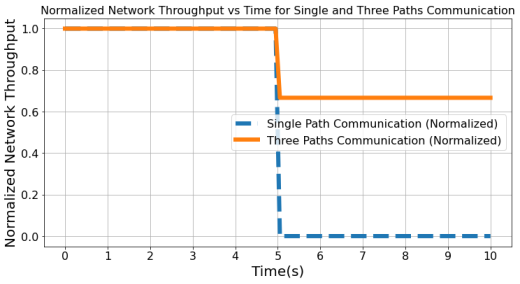

Fig. 3. Normalized Network throughput comparison between single and multipath communication strategy.

are transmitted simultaneously across multiple paths. Continuous monitoring of path performance and availability is conducted to detect any anomalies or attacks. **4) Reassembly and recovery:** at the receiver end, the segments are reassembled to reconstruct the original message. If some paths are compromised, the redundant segments from other paths ensure message recovery.

IV. Demonstration

In our demonstration of multipath communications, we implemented three end-to-end communications via three distinct paths. Each path was subject to potential jamming attacks. During the experiments, we intentionally interrupted the communication links intermittently to observe the system's behavior under compromised conditions. As shown in Fig. 3, when a link is interrupted, the network throughput drops to 66.6% of the original throughput by our proposed strategy, in contrast to zero throughput in the single path case. Our observations revealed that the multipath strategy effectively maintained communication integrity and minimized data loss, thus providing a reliable communication framework even in hostile environments.

V. Conclusion

Our multipath strategy aims to secure 5G networks against jamming attacks by distributing message segments across independent paths. Through tests in the 5G testbed, this method maintains communication integrity and availability, enhancing network resilience. We will optimize the path selection and consider combining other techniques to further enhance the system robustness in future.

Acknowledgment

This work is supported by NSF and Office of the Under Secretary of Defense (OUSD) – Research and Engineering, under Grant ITE2326898, as part of the NSF Convergence Accelerator Track G: Securely Operating Through 5G Infrastructure Program.

References

[1] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE access*, vol. 10, pp. 57143–57179, 2022.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.