Poster: Securing Relay Satellite System: Direct MAC Transmission by Superposition Coding

***Abstract*—Relay-assisted satellite networks rely on multi-hop architectures that expose data integrity to malicious or compromised relays. End-to-end Message Authentication Codes (MACs) avoid trusting relays but delay error detection until the destination, incurring costly retransmissions over long-delay space links, while hop-by-hop integrity requires trusting intermediate nodes.**

We propose a superposition-coded integrity scheme in which the source embeds the end-to-end MAC tag directly into the physical-layer waveform, allowing the destination to recover the tag independently of relay behavior. This prevents tag forgery even when a relay possesses the end-to-end key and eliminates the need to forward authentication data through relays. We validate the approach using a three-node software-defined radio testbed and show improved authentication reliability under malicious relay scenarios.

I. Introduction

Relay-assisted communication is a cornerstone of modern space and non-terrestrial networks, particularly for long-distance links such as Earth–Moon and Earth–Mars communication. Direct transmission over these distances suffers from severe path loss, long propagation delays, and intermittent connectivity. Architectures based on LEO/GEO relays, including NASA's LunaNet, address these challenges by forwarding data through intermediate satellites to extend coverage and improve link reliability. As such systems increasingly rely on multi-hop relaying, ensuring end-to-end data integrity in the presence of untrusted intermediate nodes becomes a critical concern.

Conventional integrity protection relies on Message Authentication Codes (MACs). End-to-end MAC verification avoids trusting relays but defers detection of message corruption until the destination, triggering costly retransmissions over long-delay links. Hop-by-hop integrity verification enables early error detection, but expands the trust boundary by requiring each relay to hold and process integrity keys. Existing hybrid approaches combine both mechanisms at the cost of additional overhead and remain vulnerable when the end-to-end key is exposed, allowing a compromised relay to forge valid tags.

In this paper, we propose a relay-resilient integrity scheme that avoids these trade-offs by embedding the end-to-end MAC tag directly into the physical-layer waveform using superposition coding. The tag is delivered to the destination over a weak auxiliary link that is independent of relay behavior, preventing forgery even when a relay possesses the MAC key. Using a three-node software-defined radio testbed and LDPC-based simulations, we demonstrate that the proposed approach improves authentication reliability without increasing transmission overhead or requiring trusted relays.

II. Related Work

Integrity protection in space and delay-tolerant networks is typically provided using either end-to-end or hop-by-hop mechanisms. Classical end-to-end arguments advocate pushing integrity verification to the endpoints to simplify intermediate nodes and avoid redundant functionality [1]. In Delay-Tolerant Networking, Bundle Protocol Security (BPSec) follows this model by allowing integrity to be applied between designated security endpoints, avoiding reliance on trusted relays but deferring error detection to the destination [2], [3].

At the space link layer, the Space Data Link Security (SDLS) protocol provides hop-by-hop authentication and integrity for telemetry and telecommand frames [4]. While this enables early error detection, it requires relays to be trusted and to manage per-link security associations, increasing the impact of relay compromise [5]. Combining end-to-end and hop-by-hop protection is possible but incurs additional overhead due to repeated transmission of authentication tags at each hop [3].

Complementary physical-layer approaches embed auxiliary authentication information directly into the waveform. Recent superposition-based schemes demonstrate that a low-rate authentication tag can be reliably overlaid on a primary signal using power-domain multiplexing [6]. Unlike prior work, which focuses on throughput or device identification, our approach uses superposition coding to deliver an end-to-end MAC tag directly to the destination, preventing forgery by compromised relays while remaining compatible with existing security frameworks.

III. Proposed Scheme

We consider a relay-assisted communication setting in which a source transmits data to a destination through one or more intermediate relays that are not assumed to be trustworthy. A relay may arbitrarily modify forwarded messages and may possess the end-to-end MAC key shared between the source and destination, but it cannot block a weak direct physical-layer transmission from the source to the destination. Under this model, conventional end-to-end MAC-based integrity verification fails, as a compromised relay can forge valid tags for modified messages.

Workshop on Security of Space and Satellite Systems (SpaceSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-02-2
https://dx.doi.org/10.14722/spacesec.2026.23087
www.ndss-symposium.org

To address this, we employ a superposition-based transmission strategy in which the end-to-end MAC tag is embedded directly into the physical-layer waveform alongside the message. Rather than forwarding the authentication tag through relays, the source independently encodes the message and the tag and superimposes the two coded streams prior to transmission. The relay decodes and forwards only the high-power message layer, while the destination recovers the MAC tag from its direct reception of the superposition-coded signal.

In conventional systems, the message and its MAC tag are channel-coded and transmitted sequentially. In contrast, the proposed scheme transmits the message and tag simultaneously using superposition coding, without increasing transmission duration or total transmit power.

Let m and t denote the message and tag lengths, respectively, and let R be the channel code rate. Under sequential transmission, the total number of transmitted coded bits is $\frac{m}{R} + \frac{t}{R}$. The superposition-based scheme transmits the same total number of symbols, $\frac{m+t}{R}$, but effectively allocates redundancy unevenly between the two components. The resulting effective code rates are

$$R_m = \frac{Rm}{m+t}, \qquad R_t = \frac{Rt}{m+t}.$$

When $m \gg t$, the message experiences essentially the same effective code rate as the conventional scheme, while the tag rate approaches zero. As a result, the tag is protected by very strong redundancy, enabling reliable recovery at the destination even over a weak direct link.

Power allocation between the message and tag layers is controlled by a parameter α, which determines the fraction of total transmit power assigned to the tag. Increasing α improves tag recoverability at the destination but reduces the power available to the message layer. This trade-off is evaluated experimentally. Importantly, the relay does not observe a usable version of the end-to-end tag and does not participate in its generation or verification, preventing forgery even when the relay holds the MAC key.

IV. Evaluation and Results

Setup. We evaluate our integrity scheme on a three-node SDR testbed (Source–Relay–Destination) with approximately 36 cm spacing between adjacent nodes. The relay path (Source→Relay and Relay→Destination) is intentionally strong, while the direct Source→Destination path is weak, matching the intended operating regime of our design. Each trial runs in two phases: (i) the Source transmits one frame containing a superposition-coded message and end-to-end MAC tag, received by both Relay and Destination; (ii) the Relay forwards only the decoded message to the Destination, which then extracts the tag from its phase-(i) recording and verifies integrity of the forwarded message.

Methodology. Across SNR points (swept via transmit gain), we measure the uncoded bit error rate (BER) of the message and the recovered tag at the Destination. We then translate the measured tag BER into an authentication reliability estimate by simulating LDPC decoding over a binary symmetric channel parameterized by the measured BER, and reporting the resulting tag block error rate (BLER). Since the relay links were error-free in our runs, end-to-end authentication success is governed by tag recovery on the weak direct link.

BER trade-off. Figure 6a and 6b, reports Destination BER for both layers under different power-splitting factors α. As expected, increasing α allocates more power to the tag layer and improves tag BER, but it also degrades the message BER due to the reduced power available to the message layer. In the moderate regime ($0.2 \leq \alpha \leq 0.3$), message BER remains close to the baseline while tag BER improves substantially, yielding a practical operating point.

Authentication reliability. The LDPC block error rate (BLER) results are summarized in Figure 7 of the poster, which reports decoding performance based on the experimentally measured tag BER. The baseline sequential-tag approach benefits from full transmit power but repeatedly carries tag overhead along the relay path. In contrast, our scheme exploits the long message payload to provide a very low effective tag rate (high redundancy) without additional airtime. As a result, for $\alpha 0.3$ the proposed method achieves lower tag BLER (higher authentication success), while keeping the relay oblivious to the end-to-end tag.

Takeaway. Overall, the results confirm the core design goal: the destination can authenticate using a tag it receives directly (not via the relay), while α provides an explicit knob to balance message robustness and tag recoverability.

V. Conclusion

We introduced a superposition-coded integrity scheme that enables end-to-end authentication in relay-assisted networks without trusting intermediate nodes. By delivering the MAC tag directly to the destination over a weak auxiliary link, the scheme prevents forgery even under relay compromise. Experimental results demonstrate reliable tag recovery and improved authentication performance without additional transmission overhead.

References

[1] J. H. Saltzer, D. P. Reed, and D. D. Clark, “End-to-end arguments in system design,” *ACM Transactions on Computer Systems (TOCS)*, vol. 2, no. 4, pp. 277–288, 1984.

[2] E. J. Birrane and K. McKeever, “Bundle Protocol Security (BPSec),” RFC 9172, Jan. 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9172

[3] Consultative Committee for Space Data Systems, “CCSDS Bundle Protocol Security Specification,” CCSDS, Draft Recommended Standard (Red Book) 734.5-R-2, 2023. [Online]. Available: https://public.ccsds.org/Pubs/734x5r2.pdf

[4] ——, “Space Data Link Security Protocol,” CCSDS, Recommended Standard (Blue Book) 355.0-B-2, 2022. [Online]. Available: https://public.ccsds.org/Pubs/355x0b2.pdf

[5] D. Fischer, I. Aguilar Sanchez, B. Saba, G. Moury, B. Bailey, C. Biggerstaff, H. Weiss, M. Pilgram, and D. Richter, “Finalizing the ccsds space-data link layer security protocol: Setup and execution of the interoperability testing,” in *AIAA SPACE 2015 Conference and Exposition*, 2015, p. 4577.

[6] S. W. Kim and K. D. Pham, “Low-latency authentication of navigation message,” in *Proceedings of the ION 2024*, 2024.

IOWA STATE UNIVERSITY

Department of Electrical and Computer Engineering

Securing Relay Satellite Systems

SeyedMohammad Kashani [1] Branden Buhler [2] Sang Wu Kim [2] Ashfaq Khokhar [2]

[1]University of Wisconsin-Madison [2]Iowa State University

Motivation: Integrity in Multi-hop Space Relays

Relay-assisted architectures (e.g., LEO/GEO relays for Earth–Moon links) improve availability and link quality, but introduce a critical integrity challenge: **untrusted relays can tamper with traffic**. End-to-end MACs avoid trusting relays, but detect corruption only at the destination, causing costly end-to-end retransmissions under large propagation delays. Hop-by-hop checks detect errors early but **require trusting each relay**.

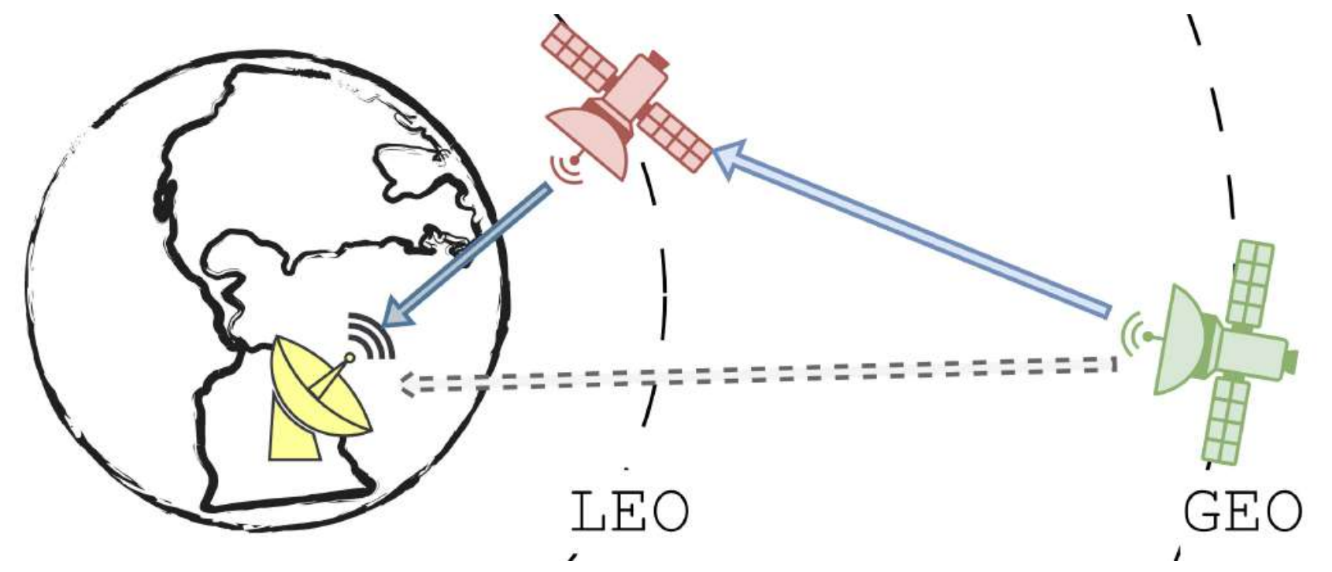
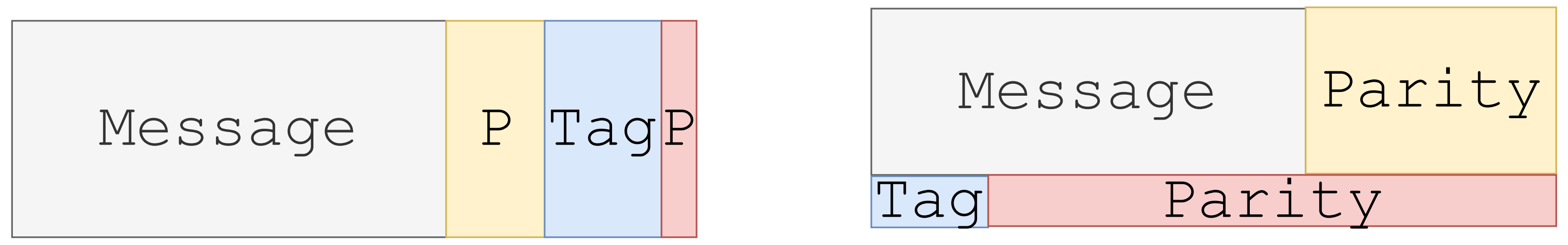


Figure 1. A LEO satellite relaying the message from a GEO satellite to a ground station.

Goal: Detect relay tampering *without trusting relays*, while preserving the latency benefits of local/hop-by-hop recovery.

Key Idea: Direct Tag Delivery via Superposition Coding

Instead of forwarding the end-to-end MAC tag through relays (where a compromised relay can rewrite both message and tag), the source **superimposes** the MAC tag on the PHY waveform so that the destination can recover the tag **independently of the relay**.



(a) Current practice (b) Proposed scheme

Proposed Scheme: Superposition-coded Integrity

We transmit a message layer and a MAC-tag layer simultaneously:

$$x = \sqrt{\alpha P}\, x_{\text{tag}} + \sqrt{(1-\alpha)P}\, x_{\text{msg}}, \quad 0 < \alpha < 0.5.$$

Why it helps:

- Destination receives the tag through a weak direct link, **not via the relay**.
- Even if the relay has the end-to-end key, it **cannot alter the destination's received tag layer**.
- Tag can be given **very strong redundancy** (extremely low effective code rate) when message length is large.

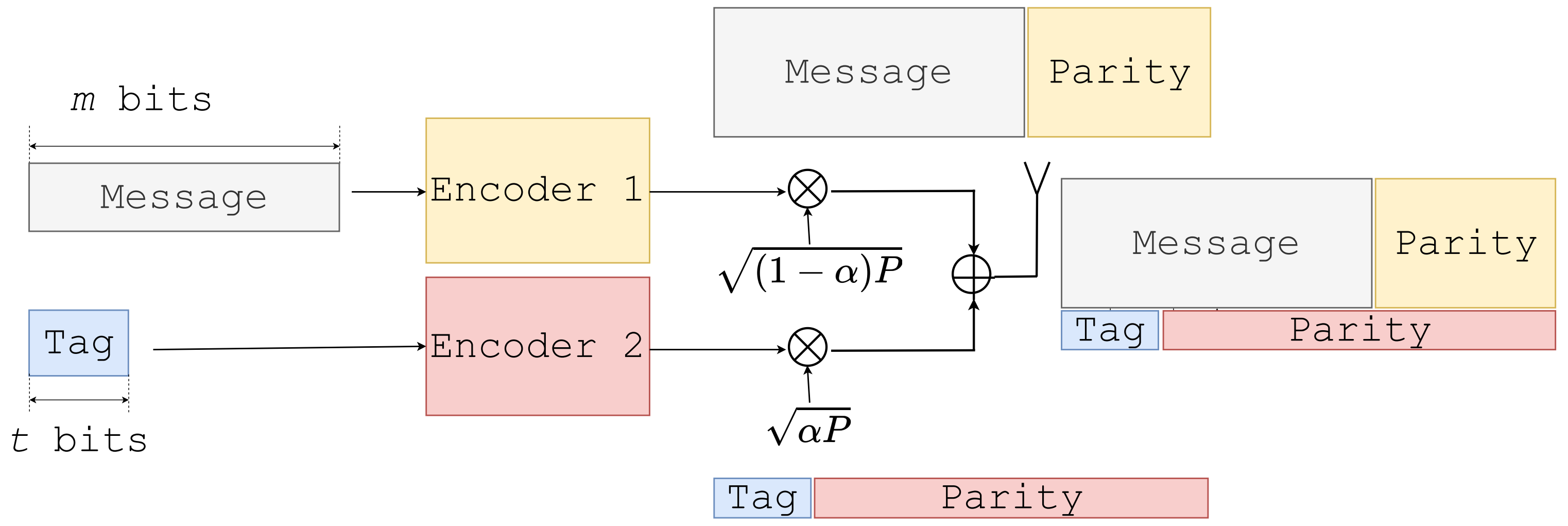


Figure 3. Encoding/superposition: message and tag streams combined with power split α.

Joint AM/FM Demodulation for Superposition-coded FSK

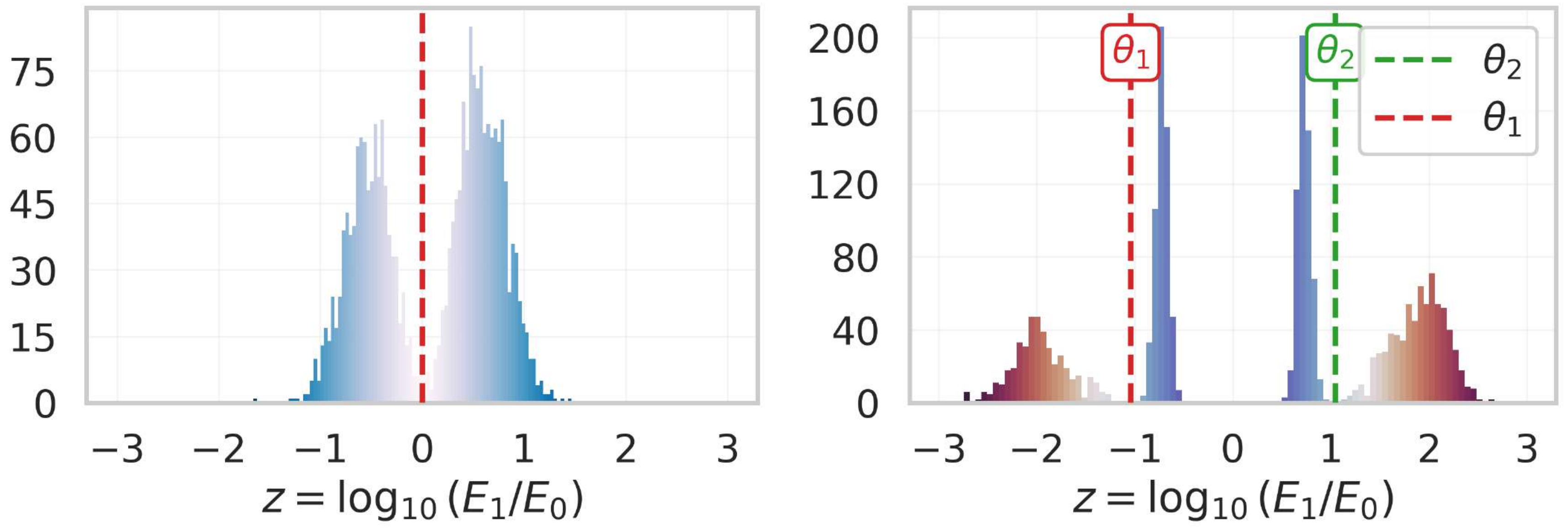
With superposition-coded FSK, we compute tone energies:

$$E_0 = \int_0^T |r(t)\cos(2\pi f_0 t)|^2 dt, \quad E_1 = \int_0^T |r(t)\cos(2\pi f_1 t)|^2 dt,$$

and form the statistic:

$$z = \log\left(\frac{E_1}{E_0}\right).$$

Using thresholds (θ_1, θ_2), we map z into decision regions for the joint (message, tag) bits. Histograms of z show separability improving with SNR and appropriate α.



(a) $\alpha = 0$ (no SC), $SNR = 3.6$ dB (b) $\alpha = 0.1$, $SNR = 13.9$ dB

Figure 4. Histograms of $z = \log(E_1/E_0)$ for thousands of samples.

Experimental Testbed (3 SDR Nodes)

We validate feasibility using a 3-node SDR setup (Source–Relay–Destination) with a strong relay path and a weak direct path to the destination.

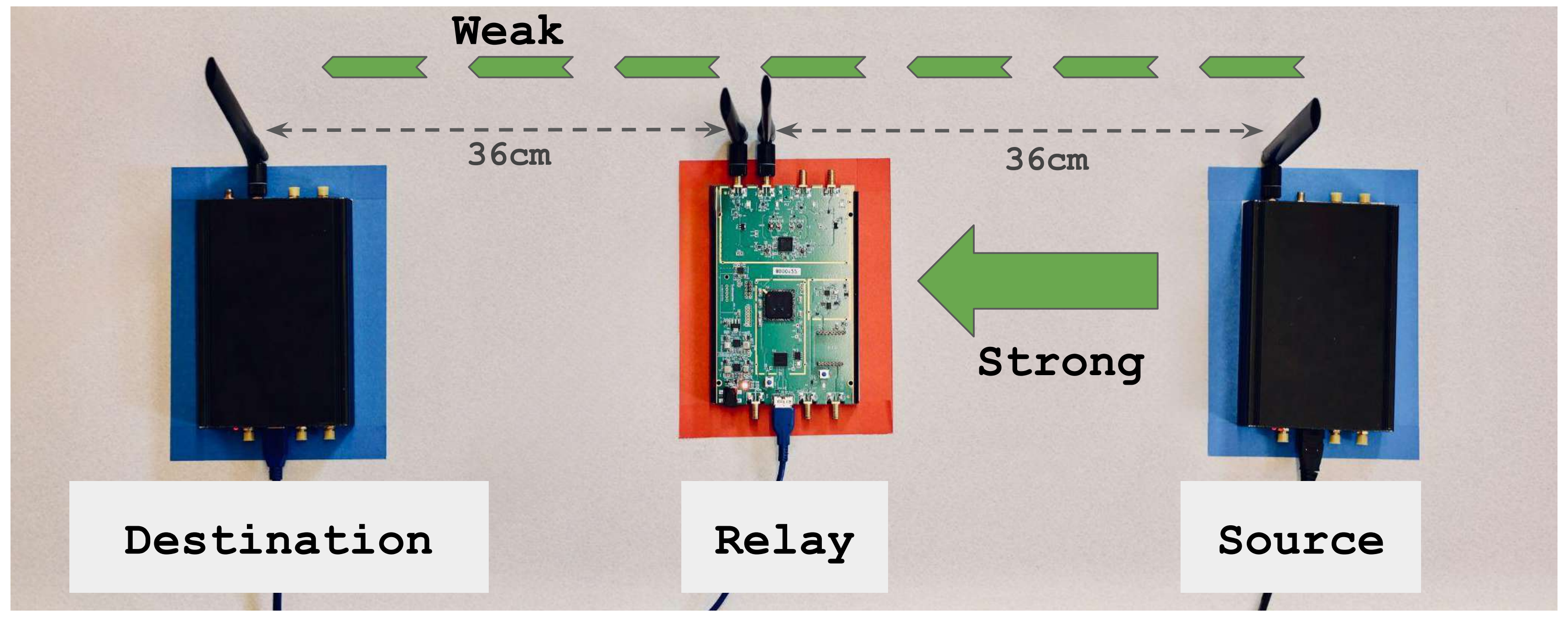


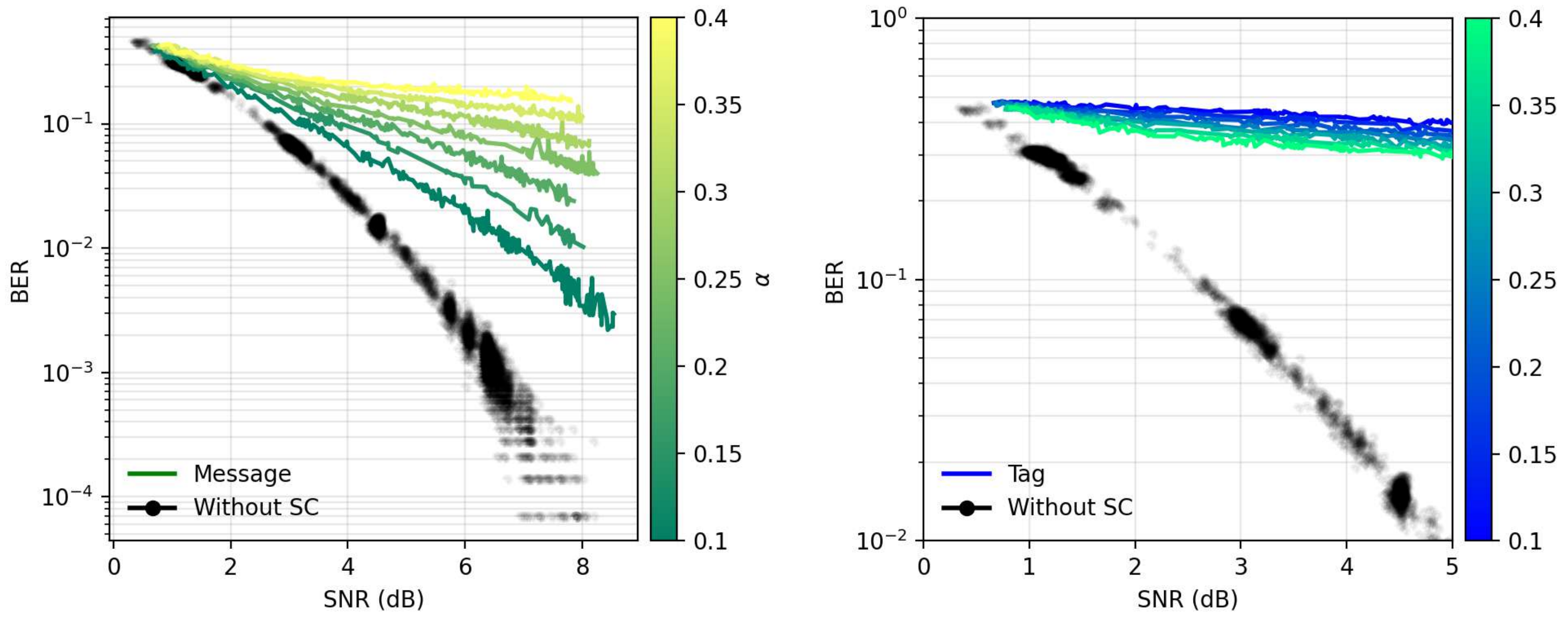
Figure 5. Two-phase operation: (i) Source transmits; (ii) Relay forwards decoded message.

Key parameters (paper setup):

- USRP B210 SDRs; carrier 1.9 GHz; FSK modulation
- TX 1 MSPS, RX 5 MSPS; LPF 300 kHz; 40 samples/symbol
- Message length 8000 bits; MAC tag length 256 bits

Results: BER Trade-off and Authentication Success

Because Source→Relay and Relay→Destination links were effectively error-free in the reported runs, authentication depends on **tag recovery over the weak direct link**. Larger α improves tag BER but degrades message BER (power-splitting trade-off).



(a) Message BER vs SNR (b) Tag BER vs SNR

Using measured BER values, LDPC simulations estimate tag BLER and authentication success. With long messages enabling very low effective tag code rate, the proposed method improves authentication success (reported improvement: **at least ∼20% higher** under evaluated conditions).

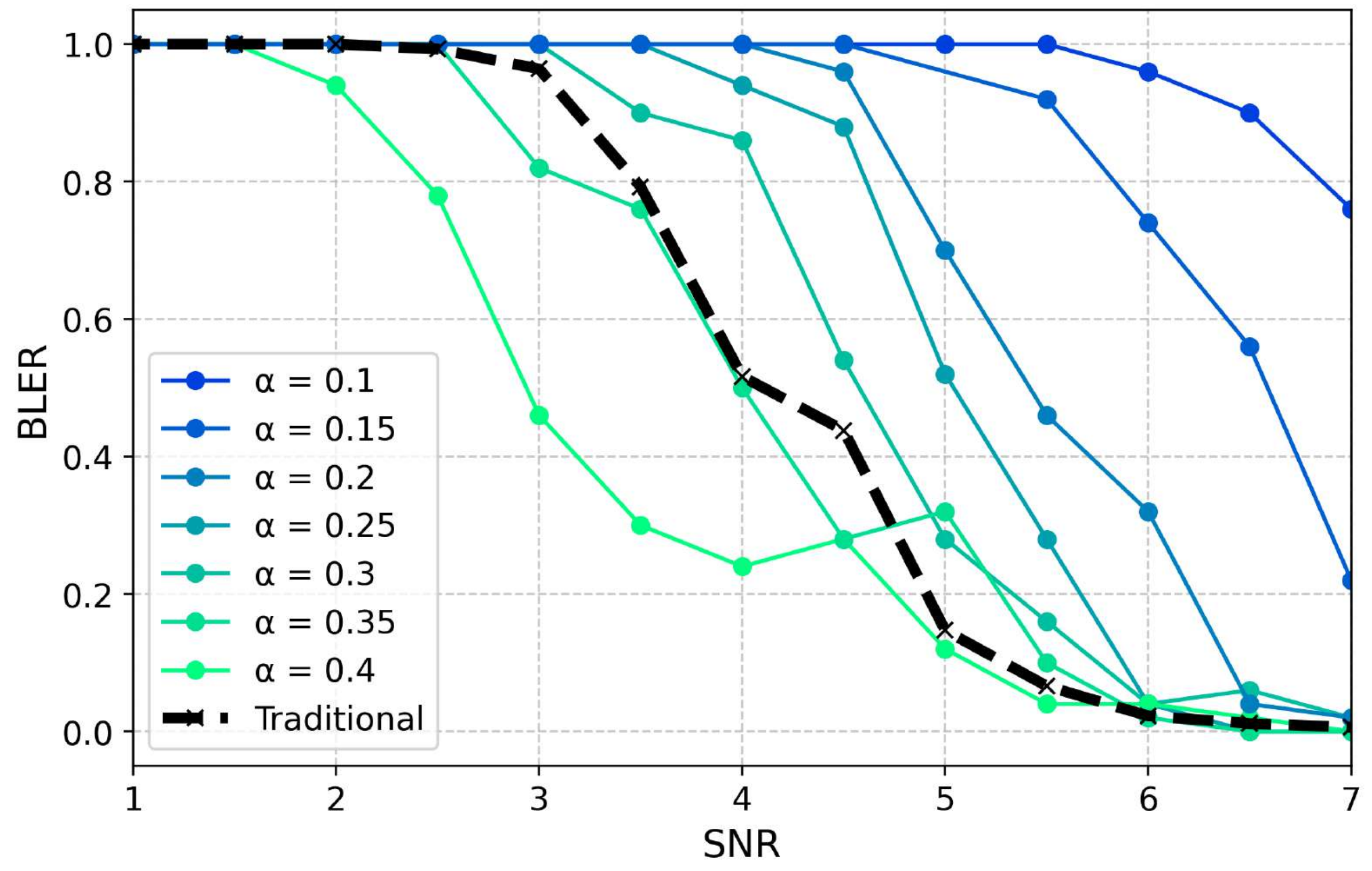


Figure 7. The dashed black curve corresponds to the traditional scheme using a $(512, 256)$ LDPC code. And the proposed scheme with $(16512, 256)$ LDPC code.

References

[1] X. Lin, H. Zhang, G. Pan, S. Wang, and J. An, "Leo relay-aided geo satellite-terrestrial transmissions," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 16899–16904, 2023.

[2] S. W. Kim and K. D. Pham, "Low-latency authentication of navigation message," in *Proceedings of the ION 2024*, 2024.

[3] R. K. Ganti, Z. Gong, M. Haenggi, C. Lee, S. Srinivasa, D. Tisza, S. Vanka, and P. Vizi, "Implementation and experimental results of superposition coding on software radio," in *2010 IEEE International Conference on Communications*, pp. 1–5, 2010.

Github: https://github.com/mkashani-phd/Secure_Wireless_Relay.git

skashani@wisc.edu