AFRL-RV-PS-
TR-2023-0106

AFRL-RV-PS-
TR-2023-0106

LOW LATENCY AUTHENTICATION OF NAVIGATION MESSAGE

Sang Wu Kim

Department of Electrical and Computer Engineering Iowa State University
2215 Coover Hall
Ames, IA 50011

31 July 2023

Final Report

AIR FORCE RESEARCH LABORATORY
Space Vehicles Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776

DTIC COPY

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research which is exempt from public affairs security and policy review in accordance with AFI 61-201, paragraph 2.3.5.1. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RV-PS-TR-2023-0106 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//SIGNED//	//SIGNED//
Dr. Khanh D. Pham Program Manager, AFRL/RVB	Mark E. Roverse, Chief AFRL Geospace Technologies Division

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
31-07-2023	Final Report	13 Apr 2021 – 07 Jun 2023

4. TITLE AND SUBTITLE
Low Latency Authentication of Navigation Message

5a. CONTRACT NUMBER
FA9453-21-1-0021

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
C6601S

6. AUTHOR(S)
Sang Wu Kim

5d. PROJECT NUMBER
4846

5e. TASK NUMBER
EF133864

5f. WORK UNIT NUMBER
V1NT

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Department of Electrical and Computer Engineering
Iowa State University
2215 Coover Hall
Ames, IA 50011

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Avenue SE
Kirtland AFB, NM 87117-5776

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RVBYC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RV-PS-TR-2023-0106

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited (AFRL-2023-486 dtd 02 Oct 2023).

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The primary objective of this research is to develop low-latency authentication methods in the Global Navigation Satellite System (GNSS). The proposed approach is to superimpose the authentication tag onto the navigation message and transmit them simultaneously within the same frequency band. This innovative approach enables instantaneous authentication, as both the navigation message and the authentication tag are received simultaneously. A comprehensive evaluation was conducted, focusing on key performance metrics such as the Authentication Error Rate (AER), Time Between Authentications (TBA), and Authenticated Throughput. To further reduce authentication latency, we investigated the option of segmenting the navigation message into multiple segments, enabling simultaneous transmission alongside the authentication tag. This segmentation approach showcased notable gains in authentication latency, leading to faster and more efficient verification processes. Moreover, our proposed method exhibited a substantial improvement in authenticated throughput compared to existing techniques.

15. SUBJECT TERMS
global navigation satellite systems, low latency authentication, time between authentication, authentication error rate, power allocation factor, decoding error probability

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Khanh D. Pham
Unclassified	Unclassified	Unclassified	Unlimited	42	**19b. TELEPHONE NUMBER** *(include area code),*

This page is intentionally left blank.

TABLE OF CONTENTS

Section **Page**

LIST OF FIGURES

Figure **Page**

1 SUMMARY

The primary objective of this research is to develop low-latency authentication methods in the Global Navigation Satellite System (GNSS). The proposed approach is to superimpos the authentication tag onto the navigation message and transmit them simultaneously within the same frequency band. This innovative approach enables instantaneous authentication, as both the navigation message and the authentication tag are received simultaneously. A comprehensive evaluation was conducted, focusing on key performance metrics such as the Authentication Error Rate (AER), Time Between Authentications (TBA), and Authenticated Throughput.

To further reduce authentication latency, we investigated the option of segmenting the navigation message into multiple segments, enabling simultaneous transmission alongside the authentication tag. This segmentation approach showcased notable gains in authentication latency, leading to faster and more efficient verification processes. Moreover, our proposed method exhibited a substantial improvement in authenticated throughput compared to existing techniques.

As a result, the developed approach holds immense value in the GNSS domain, where timely verification of the authenticity of received navigation messages is of utmost importance. These innovative methods pave the way for enhanced security and more reliable navigation systems, benefiting a wide range of applications and users.

2 INTRODUCTION

With the continuous advancements in radio frequency microelectronics, generating Global Navigation Satellite System (GNSS) signals has become more accessible and cost-effective. However, this accessibility has also led to a growing concern about spoofing attacks, where counterfeit GNSS signals are broadcasted to provide false information to victim receivers.

In response to this emerging hazard, Navigation Message Authentication (NMA) techniques have been developed [1–6]. The core idea behind NMA is to send the navigation message along with authentication tags, allowing verification of its correctness and making it difficult for attackers to alter them through cryptography. Unfortunately, current NMA techniques suffer from latency issues due to the need for long authentication tags, which are appended to the navigation message. Consequently, the time between authentications (TBA) is negatively affected, leading to poor performance.

This proposed research aims to address this challenge by developing a low-latency authentication methods that involve superimposing the authentication tag onto the navigation message and sending them simultaneously within the same frequency band. This approach enables instantaneous authentication since both the navigation message and the authentication tag are received simultaneously. In contrast, existing systems require additional time to receive and verify the navigation message after receiving the authentication tag. By reducing authentication latency, the proposed method allows the receiver to promptly verify the authenticity of the received navigation message.

We present three innovative methods for superimposing the authentication tag onto the navigation message in GNSS. In scenarios where the message length exceeds the tag length,

which is common in GNSS applications, we can augment the authentication tag with additional parity bits. This enhancement significantly bolsters the forward error correction capability of the tag. Another technique involves stretching out the tag symbol durations, resulting in increased processing gain and coherent integration time. By doing so, we can substantially improve the anti-jamming and tracking capabilities of a GNSS receiver. Additionally, we explore a novel approach of splitting the navigation message into multiple segments, allowing for simultaneous transmission alongside the authentication tag. This approach effectively reduces the authentication latency, promoting faster and more efficient verification.

We assess the effectiveness of the proposed methods through a comprehensive evaluation, focusing on key performance metrics, including the Authentication Error Rate (AER), Time Between Authentications (TBA), and Authenticated Throughput. These metrics allow us to gauge the reliability, frequency, and efficiency of the authentication process, providing valuable insights into the overall system's performance and security capabilities.

The implications of this proposed methods are significant for latency-critical applications, such as autonomous space vehicles, where immediate verification and actions are crucial upon receiving a navigation/sensor message. Additionally, the shorter TBA provided by this method creates smaller windows for potential adversaries to inject false data, making spoofing attacks less successful. As a result, this approach will be highly valuable in the GNSS, where timely verification of the authenticity of received navigation messages is of utmost importance.

Prior Works:

The idea of superimposing one message onto another message and communicating them simultaneously, known as superposition coding, has been first introduced by Cover in 1970 in a talk titled "Simultaneous Communication," and appeared in his 1972 paper [7]. The benefit of superposition coding is the increased capacity (data rate) over orthogonal transmissions, such as time-division multiplexing or frequency-division multiplexing. Since then, superposition coding has been applied in numerous problems, including multiple access communications [8], interference channels [9–11], relay communications [12], and confidential communications [13, 14]. In this project, we apply the superposition coding to send the navigation message and authentication tag simultaneously, thereby reducing the authentication latency. It can also make the authentication tag undetectable (invisible), thereby *proactively* protect against spoofing attacks by avoiding the radar of spoofers in the first place. The scope of this project is focused on low-latency authentication offered by the superposition of navigation message and authentication tag.

Mitigation against spoofing attacks in GNSS has been a major research focus for the past several years [1, 15, 16]. Anti-spoofing techniques can be categorized as either message- or signal-based. The message-based schemes, known as Navigation Message Authentication (NMA), typically involve cryptographic operations to the navigation message [2,3,5,6,17,18]. The core idea is to add signal features useful to verify the correctness of the received signals and to make it difficult for an attacker to alter them. Authentication and integrity of the transmitted message can be provided through asymmetric or symmetric cryptographic means, as a digital signature or a message authentication code (hereafter referred to as au-

thentication tag), respectively [19,20]. The energy and computational cost of GNSS message authentication have been examined in [21].

A signal-level spoofing attack is to send a set of false signals that are similar to the true signals but have different spreading code phases and carrier phases such that a false position/timing fix is induced at the victim receiver [1]. The presence or absence of such signal-level spoofing attack can be detected by taking a cross-correlation between the signal received at one location with a nearly synchronous signal received at a remote (preferably trusted) station [22–25]. Other work has demonstrated an increased probability of detection by utilizing distributed, low-cost receivers as opposed to one reference station [26]. These works require the signal samples are transmitted from one receiver to the other receiver in a secure manner.

3 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Methods

We consider a GNSS in which a transmitter (satellite) broadcasts a navigation message $\mathbf{v} = (v_1, \cdots, v_n)$ of length n bits, each of duration T_s, and its authentication tag $\mathbf{u} = (u_1, \cdots, u_m)$ of length m bits, each of duration T_s, to receivers. We assume $\mathbf{u}$ and $\mathbf{v}$ are codewords of length m and n bits, respectively. If the information bit rate is R_b (bits per second) and the code rate is r, then $T_s = r/R_b$. We assume that $E[u_j] = E[v_i] = 0$ and $E[u_j v_i] = E[u_j]E[v_i]$ for all i, j. Further, we assume $E[|u_j|^2] = E[|v_i|]^2 = C$. We assume that the channel gain is 1. Hence, C represents the received signal power. Each navigation message bit and each

auther

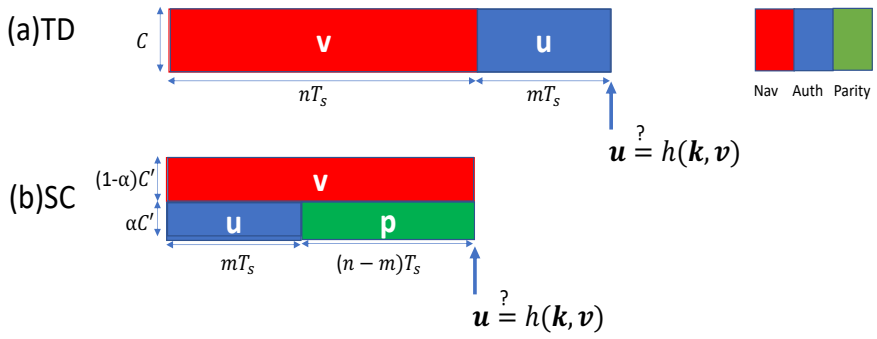

Figure 1: (a)TD: conventional frame structure and (b) SC: proposed frame structure

In the current state-of-the-art, **u** and **v** are sent in time division (TD) multiplexing mode as illustrated in Figure 1(a). As a result, the ground receivers may verify the authenticity of the received navigation message **v** at time $(n+m)T_s$. To reduce the authentication latency, we propose superimposing **v** and **u** and sending them at the same time over the same frequency. For $n > m$, one may add $n-m$ parity symbols to the authentication message **u**, as illustrated in Fig. 1(b). The addition of $n-m$ parity bits to the authentication message results in a code rate of rm/n, thereby enhancing the FEC capability for the tag. In addition, the superposition coding (SC) of **v** and **u** enables the receivers to verify the received navigation message at time nT_s, reducing the authentication latency by a factor of $n/(n+m)$ over the current state-of-the-art. The transmitter architecture of the proposed scheme is depicted in Figure 2.

The transmitted signal in the proposed scheme can be expressed by

$$\mathbf{x} = \sqrt{1-\alpha} v_i \mathbf{p}_v + \sqrt{\alpha} u_i \mathbf{p}_u \tag{1}$$

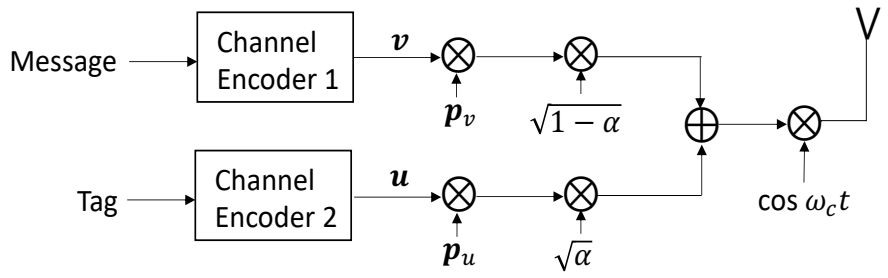

Figure 2: Transmitter architecture of superposition coding scheme

for $i \in \{1, \cdots, n\}$, where $\alpha \in (0, 1)$ is the fraction of power allocated to the authentication bits. After applying $\mathbf{x}$ to the pulse shaping filter, one obtains the baseband signal

$$x(t) = \sum_{v=1}^{N} \sqrt{1-\alpha} v_i p_v g(t - vT_c) + \sum_{u=1}^{N} \sqrt{\alpha} u_i p_u g(t - uT_c), \tag{2}$$

where $g(t)$, $t \in [0, T_c]$, is the impulse response of the pulse shaping filter, T_c is the chip duration, and $N = T_s/T_c$ is the spreading gain (number of chips per code symbol) of the message and tag. Without loss of generality, we assume $\int_0^{T_c} g^2(t)dt = T_c$. For the same total transmission energy as in the TD scheme, the transmission power for $x(t)$ can be increased to

$$C' = (1 + m/n)C. \tag{3}$$

The received signal is given by

$$y(t) = \sum_{k=1}^{K} x_k(t) + j(t) + n(t), \tag{4}$$

where K is the number of visible satellites, $x_k(t)$ is the baseband signal from the kth satellite, $j(t)$ is the jammer's signal which is a Gaussian random process with $E[j(t)] = 0$ and

$E[|j(t)|^2] = J$, and $n(t)$ is zero-mean white Gaussian noise with one-sided power spectral density N_0, namely $E[n(t)n(s)] = N_0\delta(t-s)$. The signal-to-interference-plus-noise power ratio (SINR) of the navigation message and the tag are given by

$$\gamma_v = \frac{(1-\alpha)C'}{(K-1+\alpha)C'/N + J/N + N_0/T_s} \tag{5}$$

$$\gamma_u = \frac{\alpha C'}{((K-1)+(1-\alpha))C'/N + J/N + N_0/T_s}, \tag{6}$$

respectively, where $(K-1)C'$ is the interference power from $K-1$ other satellites before despreading and $N = T_s/T_c$ is the processing gain.

For the TD approach (conventional scheme), the SINR of $\mathbf{v}$ and $\mathbf{u}$ is given by

$$\gamma = \frac{C}{(K-1)C/N + J/N + N_0/T_s}. \tag{7}$$

Remark 1: In GNSS, the interference power $(K-1)C/N$ in (7) is much smaller than the noise power N_0/T_s. This is due to the weak signal power (small C) and large processing gain (large N). In such a *noise-limited* system, transmitting additional messages along with the existing navigation message would not significantly affect the SINR of the navigation message. That is, there is room for sending additional messages without affecting the SINR of the navigation message. This is unlike the terrestrial cellular systems where interference is much stronger than the background noise (*interference-limited*) so that the transmission of additional messages degrades the SINR of other messages.

Remark 2: Since the multipath/delay spread on the spreading codes $\mathbf{p}_v$ and $\mathbf{p}_u$ are exactly the same, one searcher circuit for acquisition will suffice. When a marker is embedded

into the spreading code for the spreading code authentication, the marker can be embedded onto $\mathbf{p}_v$ only. Hence, the code tracking based on $\mathbf{p}_u$ is not affected by the marker insertion on $\mathbf{p}_v$.

3.2 Decoding Error Probability

In this section, we derive the decoding error probability for the navigation message $\mathbf{v}$ and the tag $\mathbf{u}$.

Lemma 1: For a given transmission rate R, received SINR Γ, and block length N, the decoding error probability is approximated by [27]

$$P_e \simeq Q\left(\sqrt{\frac{N}{p(1-p)}}\frac{\mathcal{C}-R}{\log_2((1-p)/p)}\right), \tag{8}$$

where p is the bit error rate (BER) before channel decoding and

$$\mathcal{C} = 1 + p\log_2(p) + (1-p)\log_2(1-p) \tag{9}$$

is the capacity of binary symmetric channel with crossover probability p. The decoding error probability in (8) is tight even for relatively small N, e.g., $N = 200$ [27].

Lemma 2: For the BPSK signal, the BER is given by

$$p = Q(\sqrt{2\Gamma}) \tag{10}$$

in AWGN channel without jamming. With pulsed jamming, the jammer is either on with probability ρ and off with probability $1-\rho$, i.e., ρ is the duty cycle of the jammer transmission. The resulting maximum average BER with the optimum duty cycle is given by [28]

$$p = \begin{cases} \frac{0.0803}{\Gamma}, & \Gamma > 0.709 \\ Q(\sqrt{2\Gamma}), & \Gamma \leq 0.709. \end{cases} \tag{11}$$

3.2.1 Time Division

For the TD scheme, the decoding error probability of the navigation message of length n and the tag of length m are given by

$$P_{e,v} \simeq Q\left(\sqrt{\frac{n}{p(1-p)}}\frac{\mathcal{C}-r}{\log_2((1-p)/p)}\right) \tag{12}$$

$$P_{e,u} \simeq Q\left(\sqrt{\frac{m}{p(1-p)}}\frac{\mathcal{C}-r}{\log_2((1-p)/p)}\right) \tag{13}$$

with Γ in (10) and (11) replaced by γ.

3.2.2 Superposition Coding

For the SC scheme, the decoding error probability of the navigation message and the tag are given by

$$P_{e,v} \simeq Q\left(\sqrt{\frac{n}{p_v(1-p_v)}}\frac{\mathcal{C}_v-r}{\log_2((1-p_v)/p_v)}\right) \tag{14}$$

$$P_{e,u} \simeq Q\left(\sqrt{\frac{n}{p_u(1-p_u)}}\frac{\mathcal{C}_u-rm/n}{\log_2((1-p_u)/p_u)}\right) \tag{15}$$

where p_v and p_u are given by (10) and (11) with Γ replaced by γ_v and γ_u, respectively, and

$$\mathcal{C}_v = 1 + p_v \log_2(p_v) + (1 - p_v) \log_2(1 - p_v), \tag{16}$$

$$\mathcal{C}_u = 1 + p_u \log_2(p_u) + (1 - p_u) \log_2(1 - p_u). \tag{17}$$

3.3 Stretching Tag Symbols

For $n > m$, one may stretch out the tag symbol durations such that the tag and the message are of the same length, as illustrated in Fig. 3(b). It offers the tag symbol duration to be

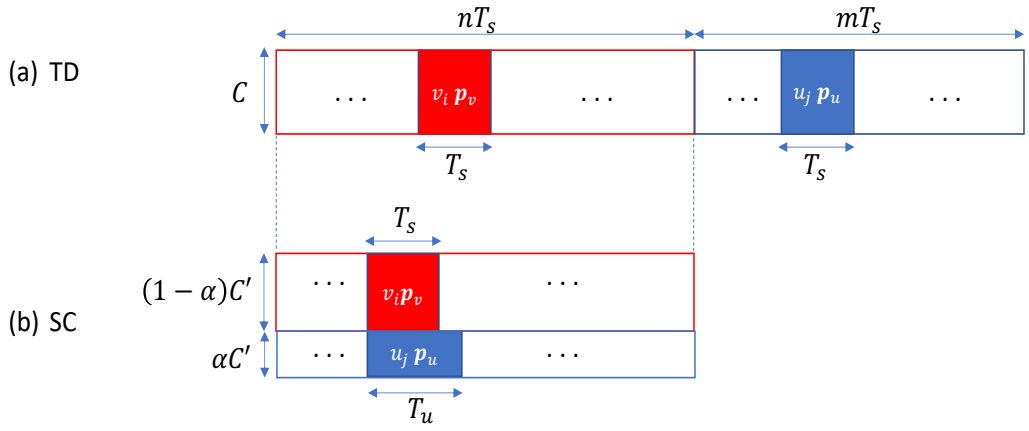

Figure 3: (a) Time-division (TD) multiplexing, (b) superposition coding (SC) of navigation message and authentication tag

3.3.1 Code Loop Tracking Threshold

Stretching the tag length provides additional benefit of increasing the coherent integration time by a factor of n/m compared to TD without affecting the effective data rate (bits per

second). The GNSS signals are very weak, hence are vulnerable to jamming attack. The key to jamming suppression in the code tracking stage is to integrate longer and longer to average out the effects of the jammer noise. The required carrier-to-noise density (C/N_0) for the code tracking, called the code loop tracking threshold, decreases as the coherent integration time increases. This threshold determines whether a GNSS receiver can lock on to the GNSS signal. Therefore, the code tracking can be accomplished at a lower carrier-to-noise-density by stretching the tag length, improving the tracking capability of a GNSS receiver. By Remark 2, it helps improve the tracking of the navigation message.

3.3.2 SINR

The signal-to-interference-plus-noise power ratio (SINR) of the navigation message, $\mathbf{v}$, and the tag, $\mathbf{u}$, are given by

$$\gamma_v = \frac{(1-\alpha)C'}{((K-1)+\alpha)C'/N + J/N + N_0/T_s} \tag{18}$$

$$\gamma_u = \frac{\alpha C'}{((K-1)+(1-\alpha))C'/N_u + J/N_u + N_0/T_u}, \tag{19}$$

respectively.

3.3.3 Decoding Error Probability

The BER, p_v and p_u, of the message and the tag can be computed using Lemma 2 with Γ replaced by γ_v and γ_u, respectively. The decoding error probability of the message and the

tag are given by

$$P_{e,v} \simeq Q\left(\sqrt{\frac{n}{p_v(1-p_v)}}\frac{\mathcal{C}_v - r}{\log_2((1-p_v)/p_v)}\right) \quad (20)$$

$$P_{e,u} \simeq Q\left(\sqrt{\frac{n}{p_u(1-p_u)}}\frac{\mathcal{C}_u - r}{\log_2((1-p_u)/p_u)}\right) \quad (21)$$

where $\mathcal{C}_v$ and $\mathcal{C}_u$ are given by (16) and (17), respectively.

3.4 Rate Splitting

The time to send the navigation message and the tag, termed authentication latency, can be further reduced by splitting the navigation message $\mathbf{v}$ into L segments $\mathbf{v}_1, \cdots, \mathbf{v}_L$[1], and spreading each segment using different spreading code as illustrated Fig. 4. This approach, hereafter referred to as rate splitting (RS), reduces the time to send the message and tag (authentication latency) to

$$T = \lceil nT_s/L \rceil, \quad (22)$$

where $\lceil x \rceil$ is the ceiling of x. Therefore, the SC/RS scheme can reduce the authentication latency by a factor of $1/(L(1+m/n))$ compared to the conventional TD scheme. Fig. 5(c) illustrates the frame structure of the SC/RS scheme for the case of $L = 2$.

[1]For example, if $\mathbf{v} = (x_1, x_2, x_3, x_4, x_5, x_6)$ and $L = 3$, then $\mathbf{v}_1 = (x_1, x_2)$, $\mathbf{v}_2 = (x_3, x_4)$, $\mathbf{v}_3 = (x_5, x_6)$.

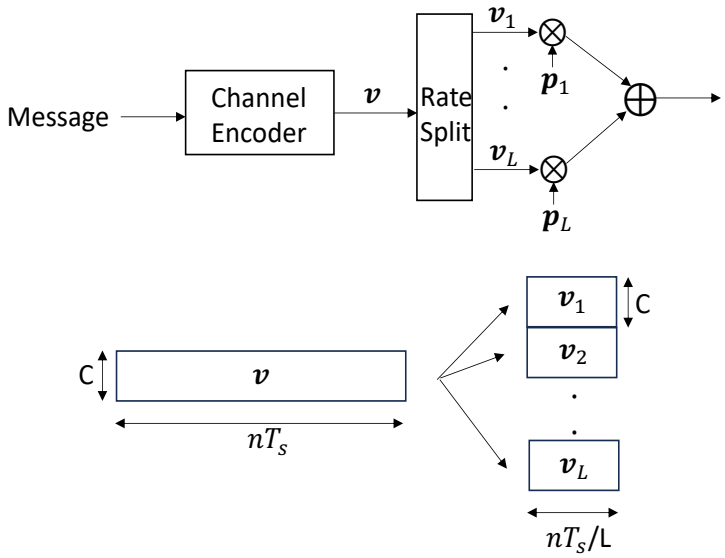

Figure 4: Rate splitting architecture

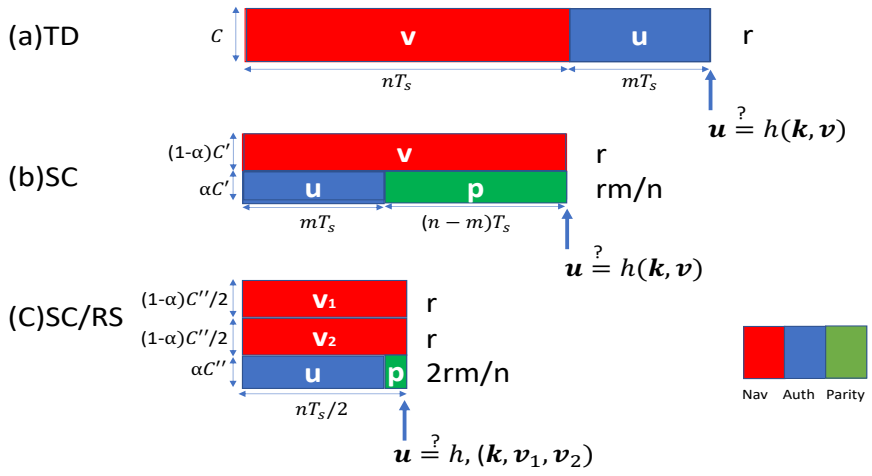

Figure 5: Transmission schemes: (a)TD, (b) SC, (c) SC/RS for $L = 2$

The spreading codes, $\mathbf{p}_{v,1}, \cdots, \mathbf{p}_{v,L}$ and $\mathbf{p}_{u,1}, \cdots, \mathbf{p}_{u,L}$, can be made orthogonal by multiplying the Walsh-Hadamard codes to the spreading code assigned to each satellite, such as the C/A code and P code. In this case, there will be no intra-interference, namely no interference between $2L$ segments within a satellite. However, the spreading codes across

different satellites are not orthogonal.

On the receiver side, the synchronization/acquisition subsystem can be demanding, especially when the carrier-to-noise density is low. However, the receiver does not require an L-fold complexity increase in synchronization/acquisition. Since the multipath/delay spread on the parallel spreading codes are exactly the same, one searcher circuit for acquisition will suffice for all the parallel codes.

For the case of $n/L > m$, one may add $n/L - m$ parity symbols to the authentication message $\mathbf{u}$, resulting in a code rate of Lrm/n for the tag. The code rate for $\mathbf{v}_l$, $l = 1, \cdots, L$ remains r because $(\mathbf{v}_1, \cdots, \mathbf{v}_L) = \mathbf{v}$. To maintain the same total transmission energy as in the TD scheme, the transmission power for SC/RS can be increased to

$$C'' = L(1 + m/n)C. \tag{23}$$

This yields the SINR of $\mathbf{v}$ and $\mathbf{u}$ as

$$\gamma_v = \frac{(1-\alpha)C''/L}{((K-1) + (L-1)(1-\alpha)/L + \alpha)C''/N + J/N + N_0/T_s} \tag{24}$$

$$\gamma_u = \frac{\alpha C''}{((K-1) + (1-\alpha))C''/N + J/N + N_0/T_s}, \tag{25}$$

respectively, where $(K-1)C''$ is the interference from other satellites and $(L-1)(1-\alpha)C''/L$ in (24) is the interference caused by other sub-codewords of the navigation message from the same satellite. Then, the decoding error probability of the navigation message of length n

bits and the authentication tag of length n/L bits are given by:

$$P_{e,v} \simeq Q\left(\sqrt{\frac{n}{p_v(1-p_v)}}\frac{\mathcal{C}_v - r}{\log_2((1-p_v)/p_v)}\right) \tag{26}$$

$$P_{e,u} \simeq Q\left(\sqrt{\frac{n/L}{p_u(1-p_u)}}\frac{\mathcal{C}_u - Lrm/n}{\log_2((1-p_u)/p_u)}\right), \tag{27}$$

respectively, where

$$p_v = Q(\sqrt{2\gamma_v}) \tag{28}$$

$$p_u = Q(\sqrt{2\gamma_u}) \tag{29}$$

are the bit error rate (BER) of the navigation message bits and the authentication tag bits, respectively.

3.5 Authentication Error Rate

The authentication error rate (AER) determines the expected rate at which the receiver cannot verify the authenticity of the navigation message. An authentication error occurs if the navigation message and/or the authentication tag are received in error. Hence, the AER is given by

$$AER = 1 - (1 - P_{e,v})(1 - P_{e,u}) = P_{e,v} + P_{e,u} - P_{e,v}P_{e,u}. \tag{30}$$

It depends on the number of navigation message bits, n, the number of authentication tag bits, m, and the power allocation α between them. In the presence of jamming, the processing gain plays a major role in suppressing the jamming power and reducing the AER.

3.6 Time Between Authentications

If the time to send the navigation message and the authentication tag is T and the AER is P_a, then the average time between authentications (TBA) is given by

$$\begin{aligned} TBA &= T(1-P_a) + 2TP_a(1-P_a) + 3TP_a^2(1-P_a) + \cdots && (31) \\ &= \frac{T}{1-P_a} && (32) \\ &\simeq T(1+P_a) && (33) \end{aligned}$$

where (32) follows from $\sum_{n=1}^{\infty} nP_a^{n-1} = 1/(1-P_a)^2$ and (33) holds true for $P_a \ll 1$.

For the TD scheme in Fig. 1(a) where the authentication tag bits are appended to the navigation message bits, T is given by

$$T = (n+m)T_s, \tag{34}$$

where T_s is the bit duration of the navigation message and the authentication tag. For the SC scheme in Fig. 1(b) where the authentication tag is superimposed onto the navigation message, T is given by

$$T = nT_s, \tag{35}$$

assuming $n \geq m$. Therefore, the proposed scheme (SC) reduces T by a factor of $n/(n+m)$ over the conventional scheme (TD). For the SC/RS scheme in Fig. 1(c) where the authentication tag is superimposed onto the segments of the navigation message, T is given

by

$$T = nT_s/2, \tag{36}$$

3.7 Authenticated Throughput

The authenticated throughput represents the amount of information that can be reliably delivered and verified by a receiver per channel use. In order for a message to be successfully delivered and verified, both the message and the tag need to be successfult decoded. Therefore, the authenticated throughput (bits per second) for SC is given by:

$$\begin{aligned} W &= R_b(1 - P_{o,u})(1 - P_{o,v}) && (37) \\ &\simeq R_b(1 - P_{o,u} - P_{o,v}), && (38) \end{aligned}$$

where the approximate authenticated throughput is maximized when $P_{o,u} = P_{o,v}$. It follows from the inequlity $X + Y \geq 2\sqrt{XY}$ for any $X, Y \geq 0$ and the minimum is achieved when $X = Y$. The authenticated throughput (bits per second) for TD is given by:

$$W = R_b(1 - P_{o,u})(1 - P_{o,v})/(1 + m/n) \tag{39}$$

where the factor $1 + m/n$ account for the addtional transmission time for TD compared to SC.

4 RESULTS and DISCUSSION

4.1 Authentication Error Rate

Figure 6 showcases the AER versus carrier-to-noise power spectral density ratio, C/N_0. The parameter α is chosen to minimize the AER. It can be observed that the proposed SC reduces the required C/N_0 by approximately 1.5 to 2 dB over TD for AER ranging from 10^{-2} to 10^{-10}.

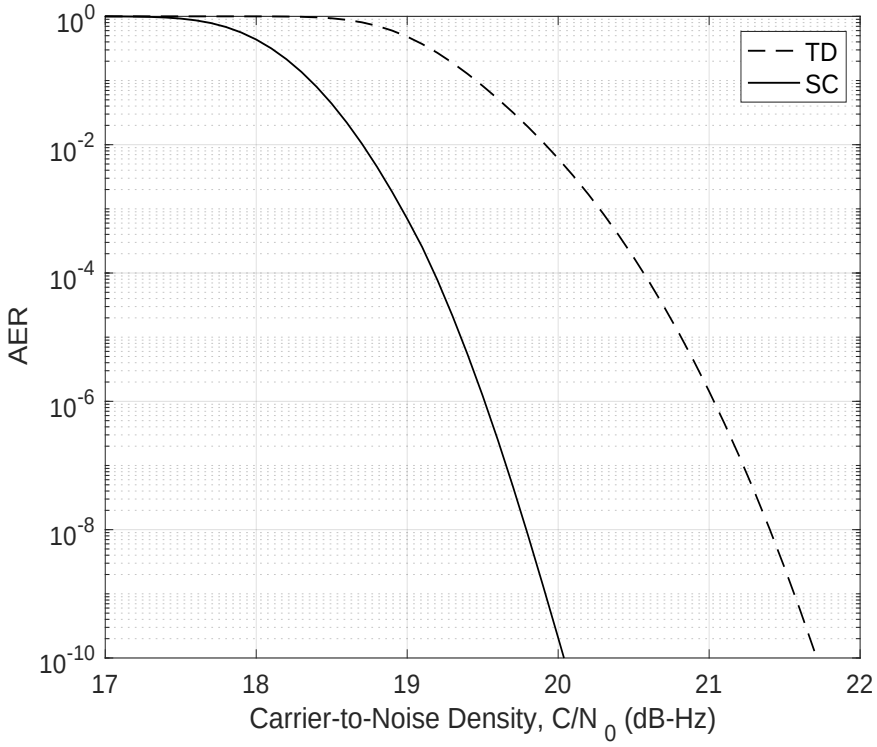

Figure 6: Authentication error rate of TD and SC versus carrier-to-noise power spectral density ratio, C/N_0 (dB-Hz); $K = 11$, $J = 0$, $R = 1/2$, R_b=50 bps, $R_c = 10$ Mcps, $n = 1200$, $m = 548$

Figure 7 illustrates the relationship between the required C/N_0 and the code rate, r, for achieving an AER smaller than 10^{-5}. In this scenario, $n-m$ parity symbols are added to the

tag to improve its forward error correction (FEC) capability while keeping T_u equal to T_s. It can be observed that both TD (Time Division) and SC (Superposition Coding) exhibit an optimal code rate around 1/3, which minimizes the required C/N_0 for achieving the desired AER.

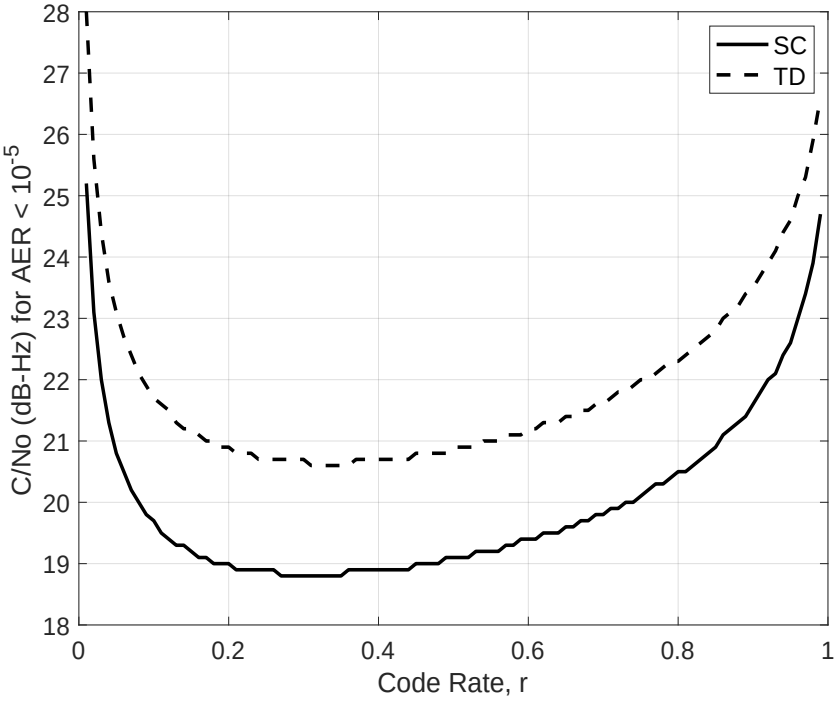

Figure 7: Required C/N_0 (dB-Hz) for the AER to be smaller than 10^{-5} versus the code rate r; $K = 11$, $J = 0$, R_b=50 bps, R_c = 10 Mcps, $n = 1200$, $m = 548$

Fig. 8 illustrates the AER of the conventional scheme (TD) and the proposed scheme (SC) in the presence of jamming. It can be seen that pulsed jamming has a more detrimental effect on SC than TD, particularly at a low jamming-to-signal power ratio (JSR). The latter indicates that the pulsed jamming is more effective when the jamming power is limited.

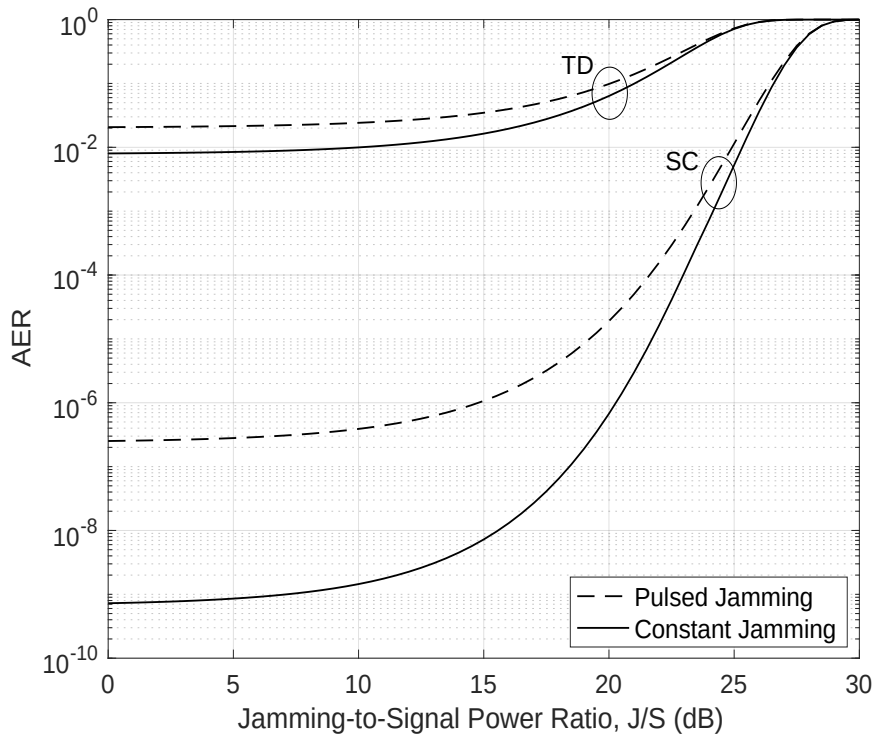

Figure 8: Authentication error rate of TD and SC versus the jamming-to-signal power ratio, J/S; $C/N_0 = 20$ dB-Hz, $r = 1/2$, R_b=50 bps, $n = 1200$, $m = 548$, $N = 1023$

4.2 Stretching Tag Symbols

Fig. 9 illustrates the AER for SC with stretching tag symbol and adding tag parity versus jamming-to-signal power ratio, J/C. The power allocation factor α is chosen to minimize the AER in both schemes. It can be seen that by adding tag parity a lower AER can be provided than stretching tag symbols. However, the improvement diminishes as the jamming power increases.

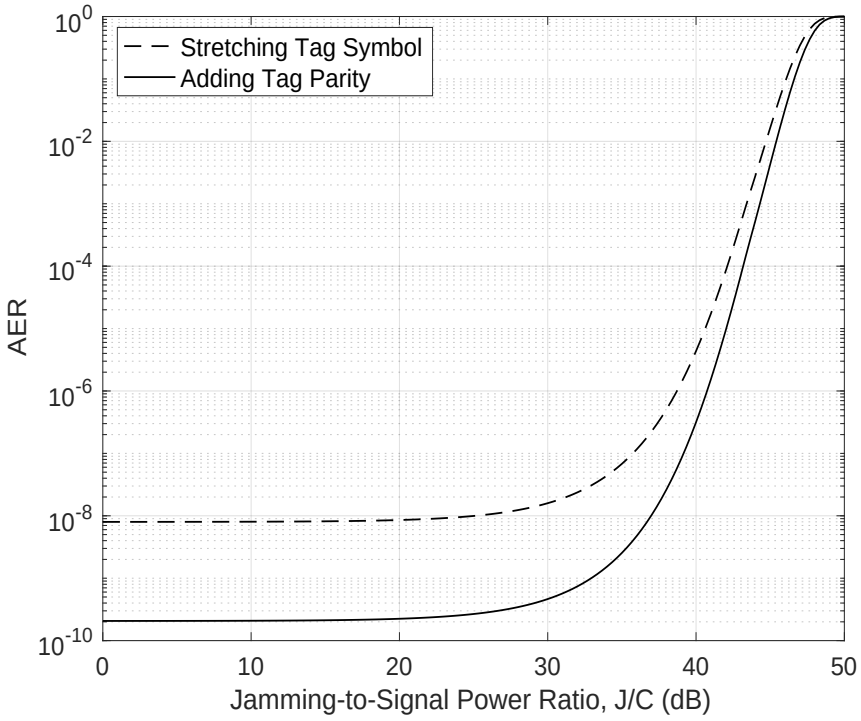

Figure 9: Authentication error rate versus jamming-to-signal power ratio, J/C (dB); $C/N_0 =$ 20 dB-Hz, $K = 11$, $r = 1/2$, $n = 1200$, $m = 548$, R_b=50 bps, $R_c = 10$ Mcps

4.3 Rate Splitting

Figure 10 illustrates the relationship between the Authentication Error Rate (AER) and the carrier-to-noise power spectral density ratio, C/N_0, for different t ransmission s c hemes. The parameter α is chosen to minimize the AER. It can be seen that SC/RS provides a higher AER than SC due to the increase of the code rate for the tag by a factor of 2 compared to SC. However, SC/RS still provides a lower AER than TD over the entire range of C/N_0.

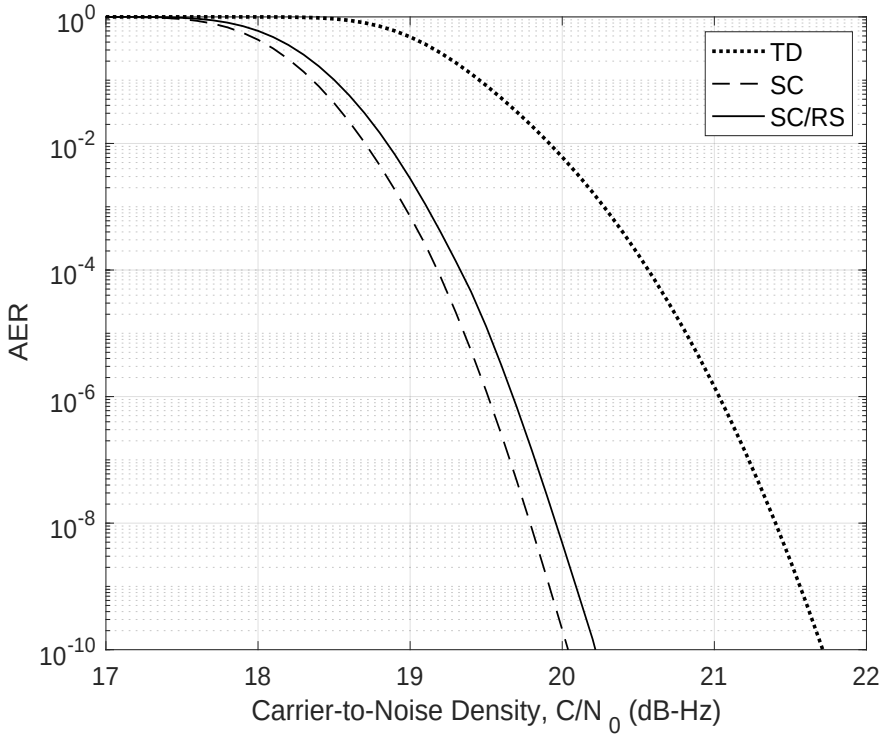

Figure 10: Authentication error rate of TD, SC, and SC/RS for $L = 2$ versus carrier-to-noise ratio C/N_0 (dB-Hz); $K = 11$, $J = 0$, R_b=50 bps, $R_c = 10$ Mcps, $n = 1200$, $m = 548$, $r = 1/2$

Figure 11 illustrates the relationship between the Authentication Error Rate (AER) and the authentication latency for different transmission schemes. The authentication latency values for TD, SC, and SC/RS schemes are $(n+m)T_s$, nT_s, $3nT_s/4$, and $nT_s/2$, respectively. For the case of $L = 4/3$, where the authentication latency is $3nT_s/4$, the block length of the message and the tag are $3n/2$ and $3n/4$, respectively, and their code rates are $2r/3$ and $4rm/(3n)$, respectively. It is evident that there is an optimal authentication latency that minimizes the AER for the SC/RS scheme. By selecting the appropriate code length for the tag, the SC/RS scheme can achieve a significantly lower AER compared to TD, while still

maintaining a low authentication latency.

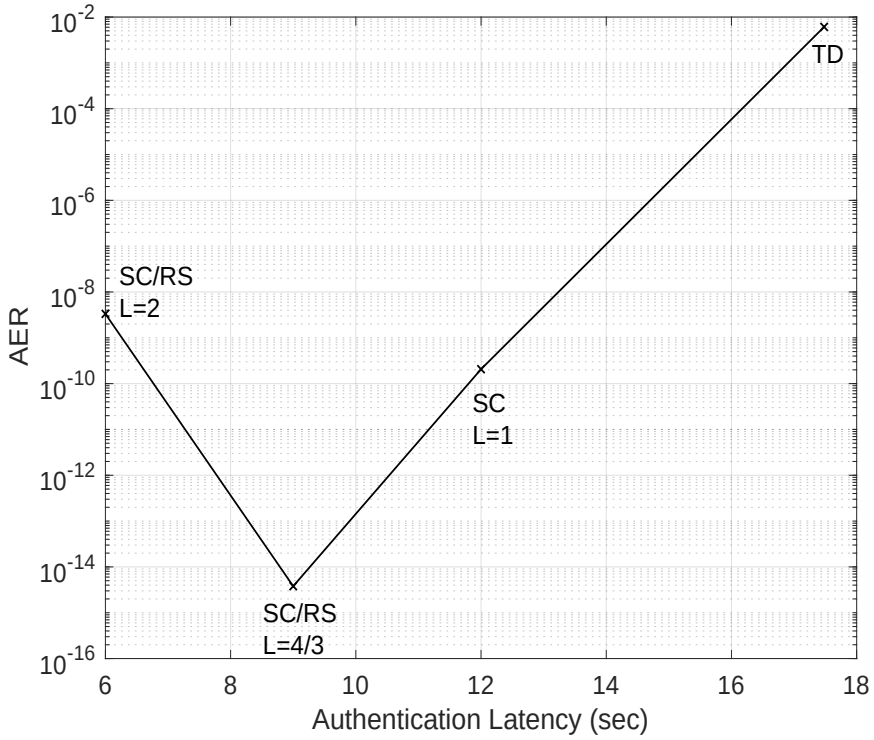

Figure 11: Authentication error rate versus authentication latency; $C/N_0 = 20$ dB-Hz, $K = 11$, $J = 0$, R_b=50 bps, $R_c = 10$ Mcps, $n = 1200$, $m = 548$, $r = 1/2$.

4.4 Time Between Authentications

Figure 12 illustrates the average Time Between Authentications (TBA) of three techniques, TD, SC, and SC/RS with $L = 2$ as a function of the carrier-to-noise density, C/N_0, in an Additive White Gaussian Noise (AWGN) channel without jamming. At high C/N_0, it can be observed that the average TBA of TD and SC/RS converge to the limits of $(n + m)T_s$ and $nT_s/2$, respectively. Similarly, the average TBA of SC converges to the limit of nT_s. As a result, SC can achieve a reduction in the average TBA by a factor of $n/(n + m)$ compared to TD. However, when C/N_0 falls below certain thresholds, the average TBA increases

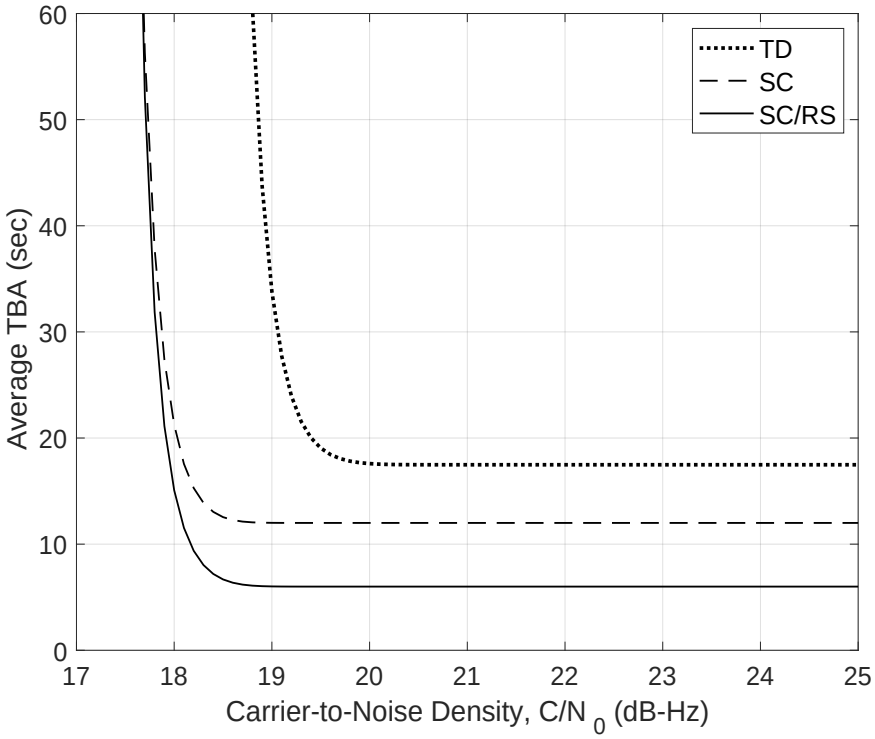

Figure 12: Average time between authentication of TD, SC, and SC/RS for $L = 2$ versus carrier-to-noise density, C/N_0 (dB-Hz); $K = 11$, $J = 0$, $r = 1/2$, R_b=50 bps, $n = 1200$, $m = 548$, $N = 1023$

rapidly due to the AER (Authentication Error Rate) being close to 1. Additionally, it can be observed that SC/RS provides a lower TBA than SC and TD over the entire ranges of C/N_0.

4.5 Authenticated Throughput

Figure 13 illustrates the relationship between the authenticated throughput and the code rate under various signal-to-noise ratios (SNRs). It is evident that SC (Superposition Coding) offers a substantial improvement compared to TD (Time Division). Additionally, it can be observed that the optimal code rate, which maximizes the authenticated throughput, increases as the C/N_0 (channel-to-noise power spectral density ratio) rises. This observation

stems from the fact that a better channel condition (higher SNR) necessitates less redundancy, leading to an increase in the optimal code rate.

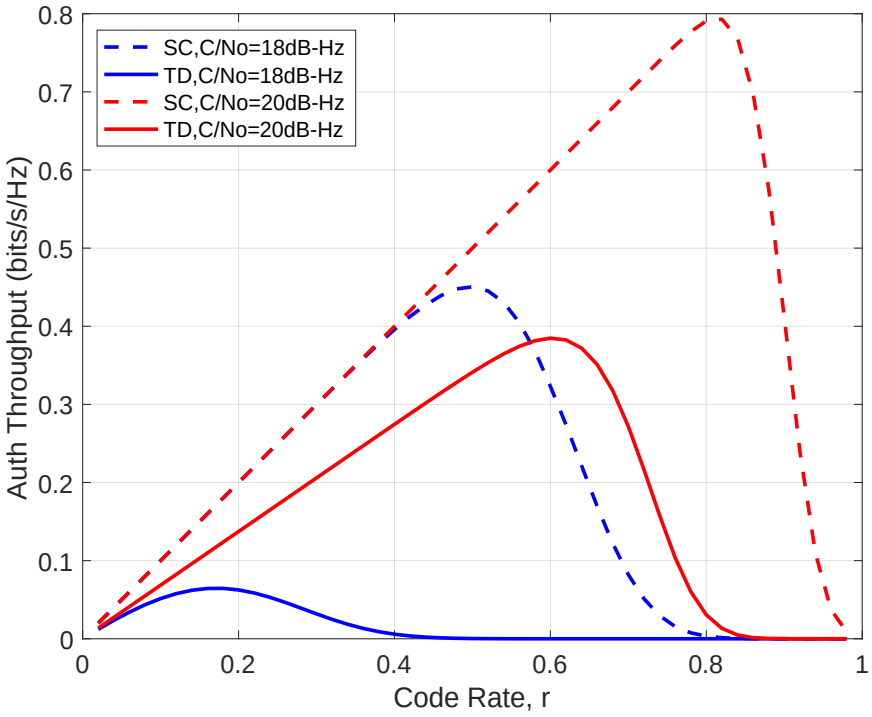

Figure 13: Authenticated throughput versus the code rate r; $K = 11$, $J = 0$, R_b=50 bps, $R_c = 10$ Mcps, $n = 1200$, $m = 548$

Figure 14 illustrates the relationship between the optimal power allocation for the tag to maximize the authenticated throughput in the proposed SC scheme and the code rate under various signal-to-noise ratios (SNRs). It can be seen that the power allocation for the tag needs to be reduced as the code rate increases.

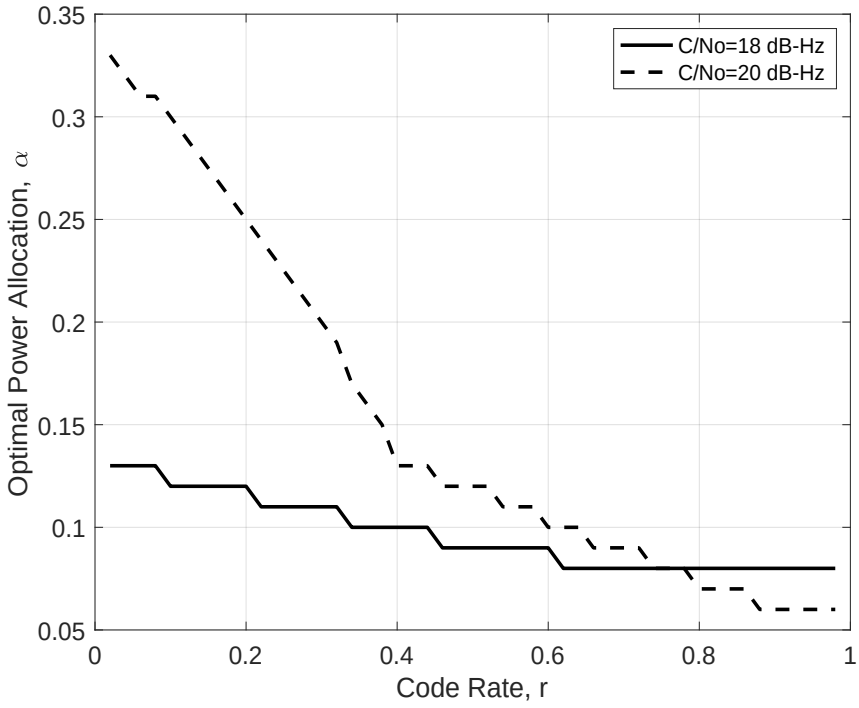

Figure 14: Optimum power allocation factor α that maximixzes authenticated throughput versus the code rate r; $K = 11$, $J = 0$, R_b=50 bps, R_c= 10 Mcps, $n = 1200$, $m = 548$

Figure 15 illustrates the relationship between authenticated throughput and C/N_0 for different code rates. An interesting observation is that the optimal code rate, which maximizes authentication throughput, rises as C/N_0 increases. As C/N_0 reaches high levels, enabling successful decoding of both the message and the tag, the authentication throughput converges to r and $nr/(n+m)$ for SC and TD, respectively. It is worth noting that SC offers a gain of $1 + m/n$ over TD.

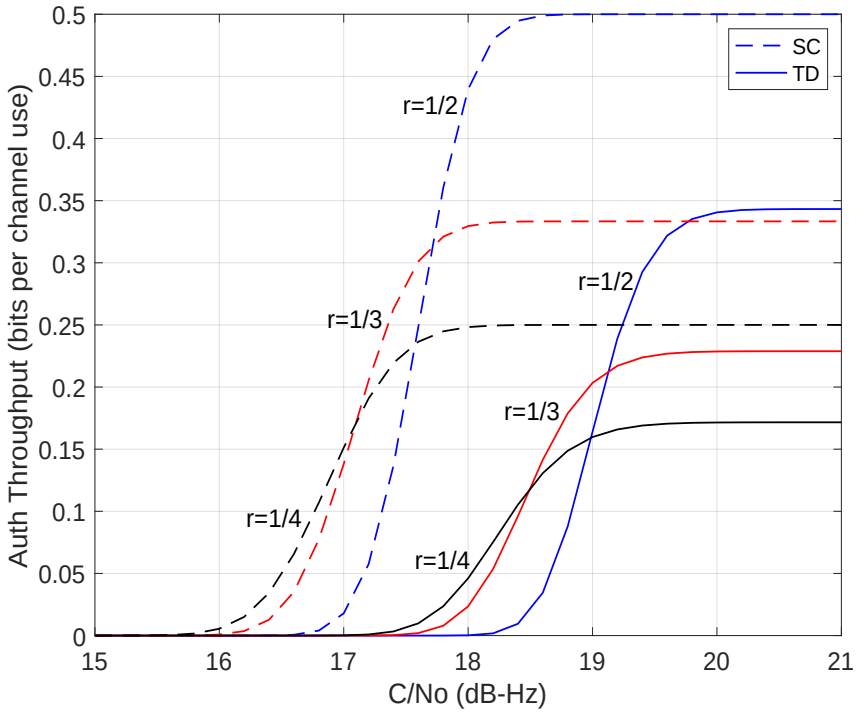

Figure 15: Authenticated throughput versus C/N_o (dB-Hz) for different code rates; $K = 11$, $J = 0$, R_b=50 bps, $R_c = 10$ Mcps, $n = 1200$, $m = 548$

Figure 16 illustrates the relationship between authenticated throughput (bits/s) and information transmission rate (bits/s), R_b, for different values of code rate, r, when the length of the message bits and tag bits, k_m and k_a, are fixed. For a given k_m, k_a, and R_b, the codelength for the message and the tag are $n = k_m/r$ and $m = k_a/r$, respectively, and the code symbol rate R_s is R_b/r. An interesting observation is that there is an optimal R_b, which maximizes authentication throughput, and that the optimal R_b rises as r decreases. Additionally, it can be observed that SC provides a significant gain over TD.

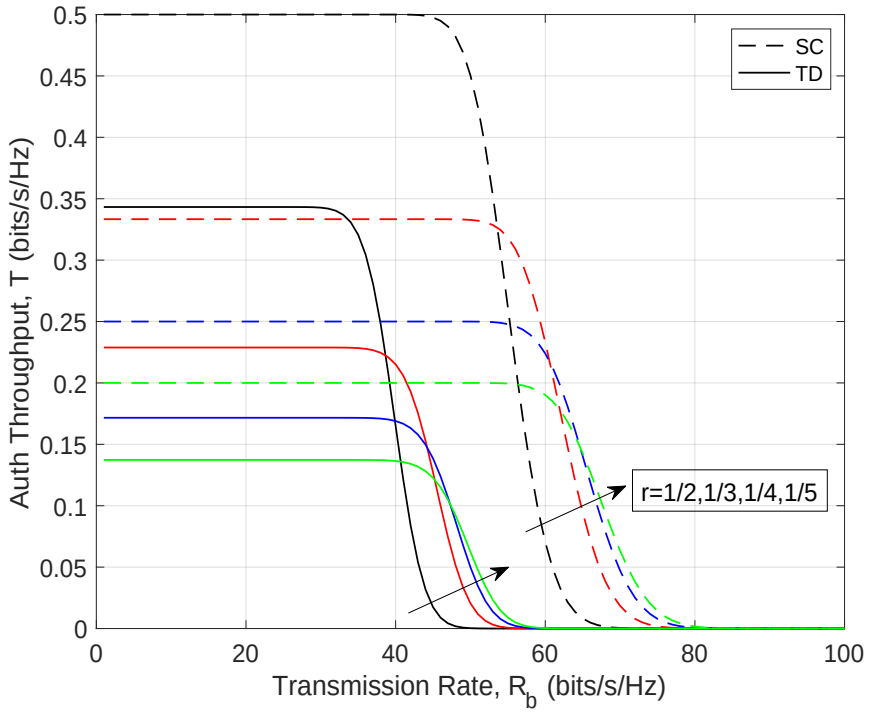

Figure 16: Authenticated throughput versus information transmission rate, R_b, (bits/s) for different code rates ; $K = 11$, $J = 0$, $R_c = 10$ Mcps, $k_m = 600$, $k_a = 274$

Figure 17 illustrates the relationship between the optimal power allocation for the tag to maximize the authenticated throughput in the proposed SC scheme and the information transmission rate, R_b under various code rates. It can be seen that the power allocation for the tag decreases as R_b increases and it increases as r decreases.

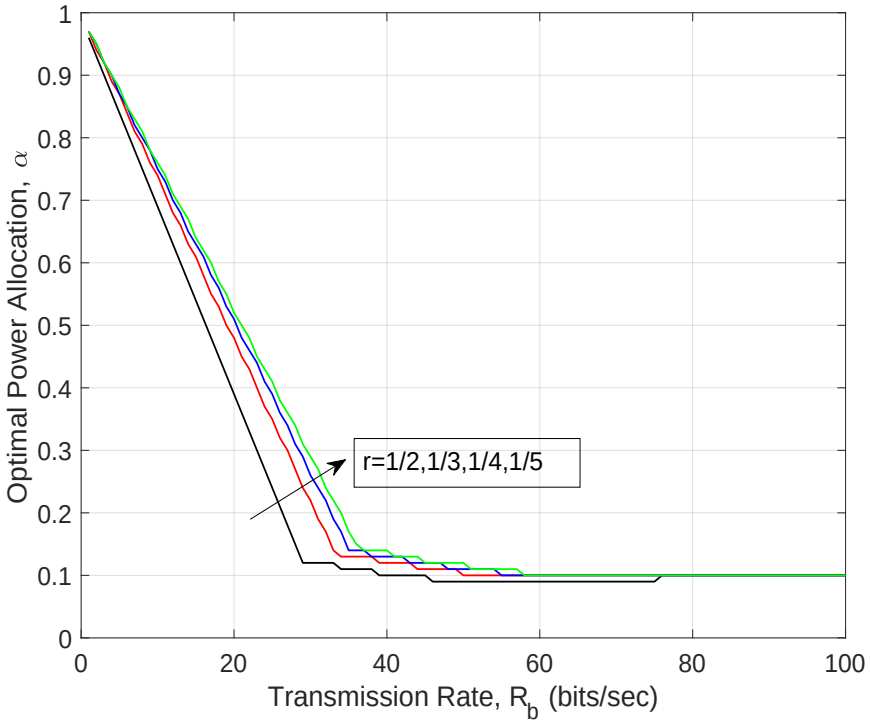

Figure 17: Optimum power allocation factor α that maximixzes authenticated throughput versus information transmission rate, R_b, (bits/s) for different code rates; $K = 11$, $J = 0$, R_b=50 bps, $R_c = 10$ Mcps, $k_m = 600$, $k_a = 274$

5 CONCLUSIONS

In this study, we have introduced three innovative methods for reducing authentication latency in GNSS by superimposing the authentication tag onto the navigation message. A comprehensive evaluation was conducted, focusing on key performance metrics such as the Authentication Error Rate (AER), Time Between Authentications (TBA), and Authenticated Throughput.

Our findings reveal that by superimposing the authentication tag (of length m bits) onto

the navigation message (of length n bits), we achieved a remarkable reduction in authentication latency by a factor of $n/(n+m)$ compared to the current state-of-the-art. Additionally, this approach provides a SNR gain of 1.5 ~ 2 dB over the current state-of-the-art for AER ranging from 10^{-2} to 10^{-10}.

To further reduce authentication latency, we explored the option of segmenting the navigation message into multiple segments, allowing for simultaneous transmission alongside the authentication tag. This approach demonstrated significant gains in authentication latency, promoting faster and more efficient verification processes.

Furthermore, the proposed method exhibited a substantial improvement in authenticated throughput compared to existing techniques. As a result, our approach holds immense value in GNSS, where timely verification of the authenticity of received navigation messages remains crucial. These innovative methods pave the way for enhanced security and more reliable navigation systems.

References

[1] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[2] C. O'Driscoll, "What is navigation message authentication?," *InsideGNSS*, 2018.

[3] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/ GNSS 2003)*, pp. 1543–1552, 2003.

[4] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 27–37, 2017.

[5] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing," *IEEE Internet of Things*, vol. 7, no. 4, pp. 2840–2854, 2019.

[6] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *Proceedings of the 30th International Technical Meeting of the Satellite Division*, pp. 2388–2416, The Institute of Navigation, 2017.

[7] T. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 2–14, 1972.

[8] A. J. Grant, B. Rimoldi, R. L. Urbanke, and P. A. Whiting, "Rate-splitting multiple access for discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 873–890, 2001.

[9] A. Carleial, "Interference channels," *IEEE Transactions on Information Theory*, vol. 24, no. 1, pp. 60–70, 1978.

[10] H.-F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On the Han–Kobayashi region for the interference channel," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3188–3195, 2008.

[11] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE transactions on Information Theory*, vol. 27, no. 1, pp. 49–60, 1981.

[12] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572–584, 1979.

[13] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2748–2765, 2012.

[14] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[15] M. Psiaki and T. Humphreys, "Civilian GNSS spoofing, detection, and recovery," *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, vol. 1, pp. 655–680, 2020.

[16] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020.

[17] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 48, no. 4, pp. 1–31, 2016.

[18] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pp. 262–269, IEEE, 2014.

[19] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174–1194, 2016.

[20] C. Caparra, Gianlucaand Wullems, S. Ceccato, S. Sturaro, N. Laurenti, O. Pozzobon, R. T. Ioannides, and M. Crisci, "Navigation message authentication schemes," *InsideGNSS*, 2016.

[21] J. Curran and N. Hanley, "On the energy and computational cost of message authentication schemes for GNSS," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 1, pp. 40–53, 2019.

[22] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, vol. 4, no. 5, pp. 30–39, 2009.

[23] P. Levin, D. S. De Lorenzo, P. K. Enge, and S. C. Lo, "Authenticating a signal based on an unknown component thereof," June 28 2011. US Patent 7,969,354.

[24] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[25] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pp. 1485–1491, IEEE, 2018.

[26] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 4, pp. 1794–1805, 2014.

[27] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2307–2359, 2010.

[28] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill Education, 2002.

DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218 1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776 1 cy

Official Record Copy
AFRL/RVB/Dr. Khanh D. Pham 1 cy