5G-and-Beyond Positioning against Amplify-and-Forward Relay Jamming

Hyuck M. Kwon, Jyothi Sri Sai Manne, and Khanh Pham

***Abstract*—An amplify-and-forward (AF) relay jamming signal can pass through any civil and military wireless communication system. Hence, AF relay jamming is dangerous and should be detected and suppressed before demodulation/decoding/decryption in wireless communication systems. The 5G positioning reference signal (PRS) and 5G synchronization reference signal (SRS) play critical roles especially for autonomous driving and link establishment between a user equipment (UE) and a near gNodeB. Both the PRS and SRS are publicly known and vulnerable to AF relay jamming. The goal of this paper is to present an effective and low-complexity 5G-and-beyond UE positioning algorithm against an AF 2-dimensional time delay (TD) and frequency shift (FS) relay jamming. Preliminary results for the proposed algorithm using a Global Positioning System (GPS) receiver scenario are presented under a 1D AF TD relay jamming environment to validate the effectiveness of the proposed algorithm.**

I. Introduction

Direct-sequence spread-spectrum (DSSS) and frequency-hopping (FH) have been popular for protecting civil and military communication systems from intentional interference/jamming. However, an amplify-and-forward (AF) relay jamming signal can pass through any civil and military wireless communication system, for example, encrypted/non-encrypted, DSSS/no-spread, and FH/non-FH systems. Hence, AF relay jamming is dangerous and should be detected and suppressed before the demodulation/decoding/decryption in wireless communication systems. Please refer to Fig. 1.

Recently, 5G wireless communication systems have been launched, and 5G-and-beyond systems, e.g., 6G, have been under discussion for next-generation systems. The 5G positioning reference signal (PRS) and 5G synchronization reference signal (SRS) play critical roles, especially for autonomous driving and link establishment between user equipment (UE) and a near gNodeB (gNB) node. The 2D time delay (TD) and frequency shift (FS) structure of PRS and SRS are similar to each other, and publicly known. Hence, both are vulnerable to AF relay jamming.

This work was supported in part by 2023 Air Force Summer Faculty Fellowship Program, and National Science Foundation awards 2326898 and 2226447.

Hyuck M. Kwon and Jyothi Sri Sai Manne are with the Department of Electrical and Computer Engineering, Wichita State University, Wichita, KS 67260 USA (e-mail: hyuck.kwon@wichita.edu; jxmanne@shockers.wichita.edu).

Khanh Pham is with AFRL, Kirtland AF Base, 3550 Aberdeen Avenue, SE Kirtland AFB, NM 87117-5776 (email: khanh.pham.1@spaceforce.mil).

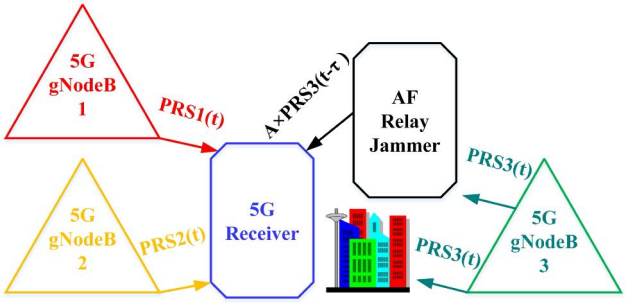

Fig. 1: 5G UE positioning scenario using three PRSs against AF relay jamming under NLOS frequency selective Doppler frequency shift mobile fading environment.

The goal of this paper is to present an effective and low-complexity 5G-and-beyond UE positioning algorithm against a 2D AF TD and FS relay jamming. Some preliminary results using a Global Positioning System (GPS) scenario under an AF 1D TD relay jamming are only presented. This is to demonstrate the proposed algorithm usefulness. In future a more comprehensive assessment of the proposed positioning algorithm against the 2D AF TD FS relay jamming will be presented including various practical channel environments.

II. TECHNICAL APPROACH

In this paper the coherent system is assumed for a worst-case analysis under jamming where the phase and time of the receiver are synchronized to those of the AF relay jamming signal. Described below is the proposed algorithm that can detect and eliminate an amplify-and-forward time delay and frequency shift relay jamming signal $x_{AF}(t) = A_{AF}y_{AF}(t-\tau_{AF})$ in the received signal $r(t)$ for UE positioning, where $y_{AF}(t)$, A_{AF} , and τ_{AF} are, respectively, the received signal, amplifying gain, and time delay at the AF relay jammer:

Step 1. Take a 2D cyclic-cross correlation between the discrete-time received signal vector $\mathbf{r} = (r[0], ..., r[N-1])^T$ (which is taken at the UE receiver after discrete-time Fourier transform (DFT) or fast Fourier transform (FFT)) and the known 5G PRS vector $\mathbf{b} = (b[0], ..., b[N-1])^T$, which is assigned in both the orthogonal frequency division multiplexing (OFDM) subcarrier frequency and the OFDM symbol time domain. Here, N can represent the number of subcarriers per

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

OFDM symbol (or can be extended to the total number of subcarriers in the assigned 2D resource blocks [RBs] for a PRS).

Step 2. Detect the presence of an AF TD and FS relay jamming signal by observing whether or not the 2D cyclic-cross correlation peak value is larger than a normal operation threshold which should be designed in prior.

Step 3. Estimate the AF TD and FS relay jamming signal using the peak value and the peak position lag, and filter out any AF relay jamming signal that is detected.

Step 4. Retake the 2D cyclic-cross correlation between the known PRS vector $\mathbf{b}$ and the received signal vector $\hat{\mathbf{r}} = (\hat{r}[0], ..., \hat{r}[N-1])^T$ after the AF relay jamming signal is eliminated.

Step 5. Repeat Steps 1 to 4 for the other two gNB PRSs (or three more when the UE clock offset is unknown).

Step 6. Apply a trilateral algorithm, and estimate the UE position using all three estimated waveform propagation time delays between the UE and the three (or four) gNBs.

A. Anticipated Results and Application

- The proposed algorithm was tested under an AWGN channel and found to be effective for the existing Global Positioning System (GPS) positioning, which is a 1D propagation time delay τ search against AF relay jamming.
- The 5G PRS is publicly known and vulnerable to AF relay jamming. Better PRS performance results are anticipated with the proposed 2D algorithm for 5G-and-beyond positioning than the 1D GPS because the positioning resolution accuracy can be enhanced by 16 and 1,000 times due to the variable PRS bandwidth (BW) than 4G and L1 C/A GPS positioning, respectively.
- The 5G SRS is also allocated in 2D RBs, publicly known and vulnerable to AF relay jamming. Better SRS performance is also anticipated with the proposed 2D search algorithm against AF relay jamming by replacing the PRS with the SRS pattern.
- Figure 2 shows an example of the 5G PRS and SRS allocated in RBs [1]. Here, BS stands for a base station, which is a 5G gNB.
- The proposed algorithm can be applicable for various systems, for examples, 5G-and-beyond positioning, 5G-and-beyond synchronization, 5G-and-beyond autonomous driving vehicles, autonomous guided vehicles in factory, drones, automatic positioning, navigation, and timing (PNT) services, emergency services, etc.

B. Existing 5G-and-beyond Positioning against AF Relay Jamming

Existing 5G positioning methods, in general, are derived from timing, angular, power-based techniques and their combination. Release 17 (Rel-17) in [2] proposes improved signaling and procedures over Release 16 (Rel-16), considering the following: (a) wider bandwidth that increases timing measurements resolution, and (b) larger antenna array apertures in massive multiple input multiple output (MIMO) technology. To the limited knowledge of the authors, there has been no investigation yet about 5G-and-beyond positioning or synchronization against AF relay jamming, although there is multiple literature on global navigation satellite system (GNSS) spoofing. And the AF relay jamming signal is similar to but different from a GNSS spoofing signal. The AF relay jamming can be more involved in a game theory than a spoofing signal.

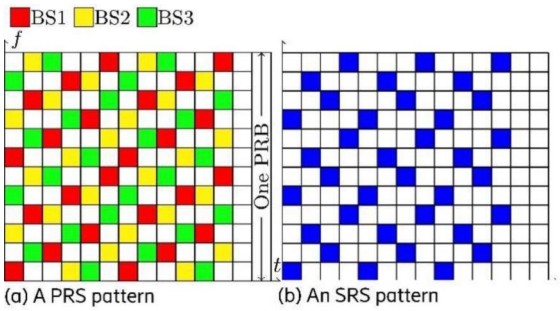

Fig. 2: (a) 5G PRS pattern for three base stations (BSs) allocated in one physical resource block (PRB) and (b) 5G SRS pattern [1].

C. Current 5G PRS Resource Block and Resolution

Figure 3 shows an example for 5G PRS OFDM symbol allocation [3]. There are 14 OFDM symbols per subframe and ten subframes per frame. Therefore, the subframe interval is 933.38 $\mu s \approx 1$ ms, and the 5G frame interval is 9.3338 ms $\approx$ 10 ms. This implies that there are seven OFDM symbols per slot and two slots per frame in 5G. The 5G PRS subcarrier size F_{sc} varies from 15 kHz to 30 kHz to 60 kHz to 120 kHz to 240 kHz. This implies that the 5G PRS bandwidth is flexible, and that the 5G PRS positioning resolution can be 16 times better than the 4G positioning resolution and 1,000 times better than the GPS L1 coarse acquisition (C/A) resolution. This is because the 5G subcarrier size can be 240 kHz while the 4G subcarrier size is fixed at 15 kHz, which is 16 times smaller, and the GPS chip time interval T_c is 1/chip rate, where the GPS L1 C/A chip rate $R_c = 1.023$ Mcps. For example, the 5G positioning resolution can be 20 to 30 cm, the 4G resolution 3.2 to 4.8 m, and the GPS L1 C/A resolution $cT_c = 293.1m$, where c is the speed of light. For a general 5G PRS design guideline, the 5G OFDM sampling interval T_s is inversely proportional to the variable PRS BW, which is the number of resource blocks (NRB) times 12 subcarriers, i.e., $BW_{PRS} = 12N_{RB}F_{sc}$ because each RB consists of 12 subcarriers. If the subcarrier size is $F_{sc} = 240kHz$ and the number of RBs is 347, then

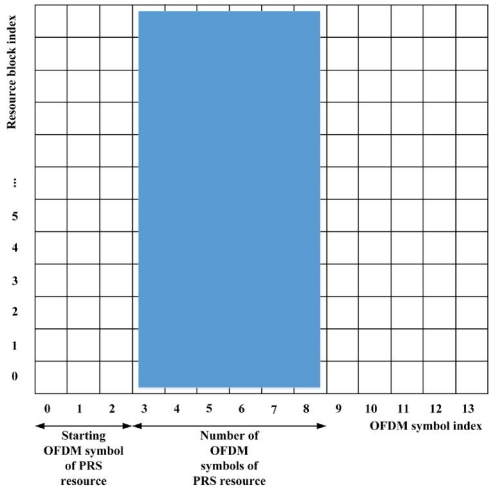

Fig. 3: 5G PRS OFDM symbols allocation [3].

the 5G BW_{PRS} becomes 1 GHz. In this case, the 5G OFDM sampling interval T_s will be $1ns$, and the positioning resolution will be $cT_s = 0.3m$.

III. PROPOSED 5G – AND - BEYOND POSITIONING SOLUTION AGAINST AF RELAY JAMMING

Figure 4 shows the proposed 5G-and-beyond positioning method against AF relay jamming. The existing 5G PRS OFDM signal processing blocks under a no-jamming environment are shown in black. The proposed additional blocks that can eliminate an AF relay jamming signal are highlighted in red. Software for the proposed 2D-correlator in red can be implemented with low complexity because it handles the signal with fast Fourier transform linear processing.

In [4] and previous works, an AF relay jamming signal has not been investigated.

A. Presence of both AF Relay Jamming and gNB PRS Signals

The necessary notations are introduced as follows: $\tau_{gNB,AF}$ is the waveform propagation time delay from the gNB to the AF TD FS jammer, $\tau_{AF,RX}$ is the waveform propagation time delay from the AF TD FS jammer to the 5G receiver, τ_{AF} is the intentional time delay introduced by the AF TD FS jammer, n_{AF} is the intentional subcarrier shift introduced by the AF TD FS jammer, $w_{AF}[n]$ is the AWGN frequency noise at the AF TD FS relay jamming, and $w_{RX}[n]$ is the additive white Gaussian noise (AWGN) frequency noise at the 5G receiver.

The stacked received vector contributed by the AF TD FS relay jamming signal after the DFT in Fig. 4 can be written as

$$\mathbf{r}_{gNB,AF,RX} = \mathbf{A}_{gNB,AF,RX}\mathbf{h}_{AF,RX}[n_{AF}] + \sqrt{2P_{AF}}\tilde{\mathbf{w}}_{AF} + \mathbf{w} \quad (1)$$

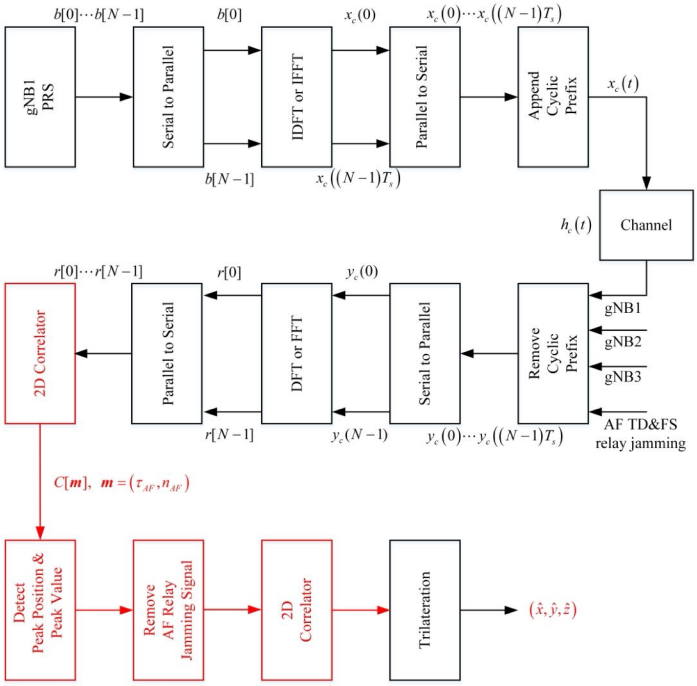

Fig. 4: Proposed 5G-and-beyond positioning solution against an AF TD and FS relay jamming.

Therefore, the overall $(N \times 1)$ received vector at the 5G PRS receiver contributed by both the gNB and the AF TD FS relay jamming signal after the DFT in Fig. 4 can be written as

$$\mathbf{r} = \mathbf{r}_{gNB} + \mathbf{r}_{gNB,AF,RX} \quad (2)$$

and if three gNBi, i = 1,2,3, are present under the AF TD FS relay jamming as shown in Figure 1, then the received vector can be written as

$$\mathbf{r} = \sum_{i=1}^{3} \mathbf{r}_{gNBi} + \mathbf{r}_{gNB3,AF,RX}. \quad (3)$$

Received vector $\mathbf{r}$ in (3) can be fed into the proposed algorithm in Step 1 for cyclic cross-correlation, and the power P_{AF}, time delay τ_{AF}, and subcarrier frequency shift n_{AF} of the AF TD FS relay jamming can be estimated.

IV. PRELIMINARY RESULTS

Preliminary results of the proposed positioning algorithm are presented, considering one-dimensional search (i.e., only time delay) for L1 coarse acquisition (C/A) GPS signal under an AF TD relay jamming.

The period of the pseudo noise (PN) sequence is $N = 1,023$ chips, as in the L1 C/A GPS signal. In the GPS, there are 20 PN sequence periods per bit, which means that $20N$ chips per bit = 20,460 chips/bit. In this paper, only one PN sequence period per bit is assumed to demonstrate the proposed algorithm. The signal-to-noise is the bit energy-to-noise power spectral density

ratio, i.e., E_b/N_0. The received signal at a GPS receiver was modeled as

$$r(t) = p(t-10) + p(t-40) + p(t-30) + A_{AF}p(t-\tau_{AF}) + n(t) \quad (4)$$

where $p(t-10)$, $p(t-40)$, and $p(t-30)$ are assumed from the three legitimate GPSs with waveform propagation time delays of $10T_c$, $40T_c$, and $30T_c$, respectively; the chip time interval T_c is normalized to 1 second for simulation; the AF relay jamming signal is an amplified and time-shifted version of the same m-sequence $p(t)$ with amplifier gain $A_{AF} = 10$ and time-shift $\tau_{AF} = 50$; and $n(t)$ is the AWGN at the GPS receiver with mean zero and power equal to the inverse of SNR. Figure 5 shows an example of the discrete time received signal $r[n]$.

The cyclic cross-correlation $R[m]$ between the GPS receiver signal $r[n] = r(t = nT_c)$ in (4) and the PN sequence $p[n] = p(t = nT_c)$ versus the lag m is taken under the AF TD relay jamming signal of $A_{AF} = 10$ and $\tau_{AF} = 50$, and $SNR = 10dB$. The $R[m]$ can be written as

$$R[m] =< r[n], p[n] > (m) = \sum_{n=0}^{N-1} r[n]p[n+m]. \quad (5)$$

Three peaks around value 1,023 and a large peak around value 10,230 in the cross-correlation can be observed in Fig. 6, as expected. The largest peak is due to the AF TD relay jamming, and its peak position is at 50, which is the TD introduced by the jammer.

The TD can be estimated as the cross-correlation peak position m_{peak}. Hence, the AF TD relay jamming signal can be estimated as

$$\hat{A}_{AF}p(t-\hat{\tau}_D) = \sqrt{\frac{R[m_{peak}]}{N}}p(t-m_{peak}T_c) \quad (6)$$

and subtracted from the received signal as

$$\hat{r}(t) = r(t) - \hat{A}_{AF}p(t-m_{peak}T_c). \quad (7)$$

Then, the discrete-time signal $\hat{r}[n]$ is fed to Step 4 of the proposed algorithm, Section II. Figures 7 and 8 show examples for the received signal after elimination of AF TD jamming signal in (7) and the cyclic cross-correlation between the reference PN signal $p[n]$ and filtered signal $\hat{r}[n]$, respectively. All these operations in Steps 1 through 4, i.e., (5) through (7), can be performed with FFT.

Figure 9 shows the probability of success versus $A_{AF} = A$ for $SNR = -10dB$. For each jamming signal amplitude A_{AF}, 500 trials were made. Here, the probability of success means that the GPS receiver successfully detects the presence of the AF TD relay jamming signal, removes it from the received signal, and correctly finds the propagation time delays of the three legitimate GPS signals. The following observations can be made:

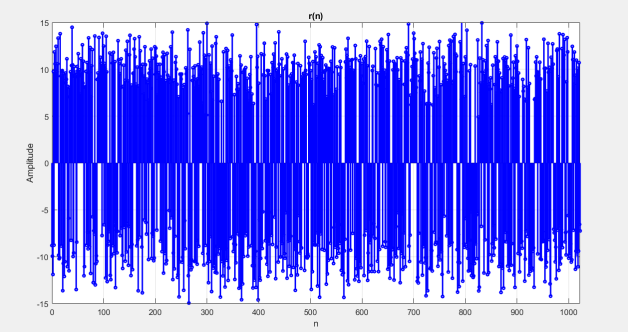

Fig. 5: Received signal $r[n] = r(t = nT_c)]$ in (4) under AF relay jamming signal.

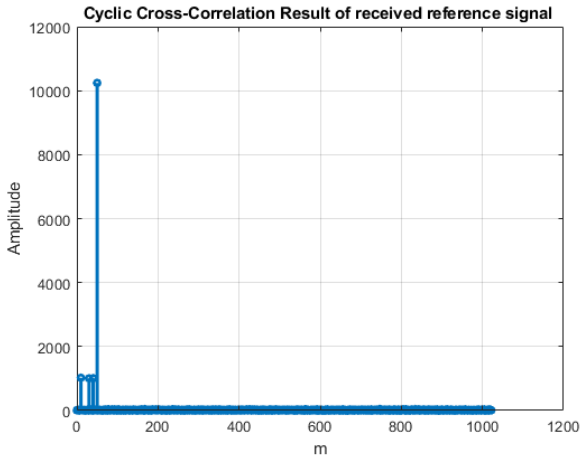

Fig. 6: Cyclic cross-correlation between the GPS receiver signal $r[n]$ in (4) and the PN sequence $p[n]$ versus the lag m.

- The probability of successfully detecting the AF TD relay jamming signal becomes 1 when the jamming amplitude $A_{AF} \geq 2.3$, ≥ 1.5, ≥ 1.2, and ≥ 1.1, and the E_b/N_0= –20 dB, –10 dB, 0 dB, and 10 dB, respectively.
- In other words, the critical AF TD relay jamming amplitude, beyond which the probability of successfully detecting becomes 1, decreases as the SNR increases. The jammer should decrease its amplitude to be effective

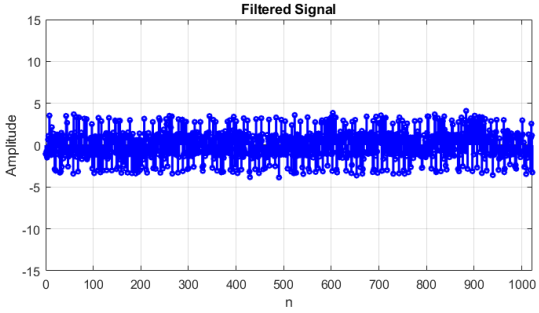

Fig. 7: Received signal after elimination of AF TD jamming signal.

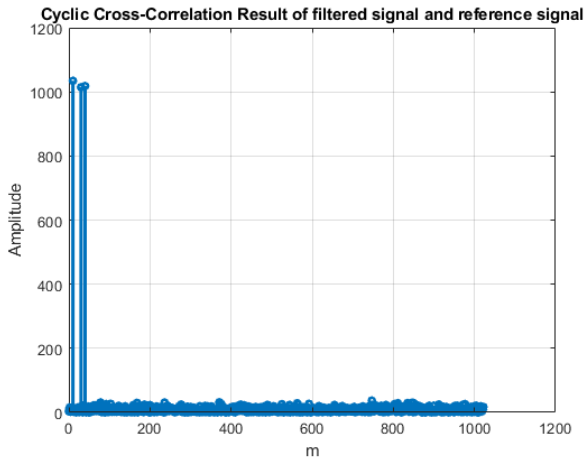

Fig. 8: Cyclic cross-correlation between reference PN signal $p[n]$ and filtered signal $\hat{r}[n]$ in (7).

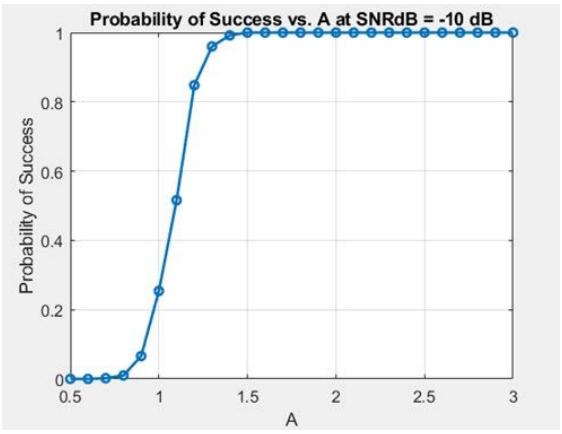

Fig. 9: Probability of success versus amplitude A, SNR = –10 dB.

against the proposed algorithm.

- However, when the jamming signal amplitude $A_{AF} < 1$, the probability of successfully finding the GPS receiver position increases. A game theoretical analysis can be involved in finding the equilibrium of the AF relay jamming amplitude.

The probability of successfully detecting the AF TD relay jamming signal presence is analytically derived under an AWGN channel and an AF TD relay jamming signal when three legitimate GPS received signals have equal power. The probability of success can be written for an AF relay jamming signal amplitude as

$$Pr[Success|A_{AF} = A] = [\int_{-\infty}^{\infty} Q((x - NA)/\sigma) \cdot 1/\sqrt{2\pi\sigma^2} \cdot exp(-(x - N)^2/(2\sigma^2))dx]^3 \quad (8)$$

where $Q(\alpha) = \int_{\alpha}^{\infty} e^{-t^2/2}/\sqrt{2\pi}dt$.

The analysis in (8) can be extended for the case when three legitimate GPS received signals have different power levels. It was observed that the estimated positioning outputs were close to those of the ideal case, i.e., no jamming and no thermal noise when the estimated AF TD jamming signal was removed, whereas the estimated positioning outputs when AF TD relay jamming was present were much different from the true ones.

V. Conclusion

AF TD FS relay jamming is most dangerous because it can pass through and damage any wireless communication system. In this paper, a low-complexity 2D 5G-and-beyond positioning algorithm was analytically derived for use against this serious AF TD FS relay jamming and expressed in 2D DFT or FFT. It is capable of accessing the proposed analytical 2D 5G-and-beyond positioning algorithm against AF TD FS relay jamming under practical channel environments in the future. Results of the 1D GPS positioning simulation confirmed the success of this proposed algorithm. For example, the probability of successfully detecting and removing an AF TD relay jamming signal becomes 1 when the AF TD relay jamming amplitude is higher than 1.1 under LOS AWGN and $E_b/N_0 = 10dB$. The critical AF TD relay jamming amplitude decreases when E_b/N_0 increases from –20 dB to 10 dB. The proposed algorithm can be applicable for synchronization also because the synchronization reference signal uses similar 2D OFDM resource blocks. The proposed algorithm can be useful for various civil and military positioning and synchronization devices against AF TD FS relay jamming.

VI. Acknowledgments

This work was supported in part under the 2023 Air Force Summer Faculty Fellowship Program, and National Science Foundation awards 2326898 and 2226447. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force and NSF.

References

[1] S. Dwivedi and et. al, "5G positioning: What you need to know," in *Ericsson*, 2020.

[2] 3GPP, "5G; NR; Physical layer procedures for control (3GPP TS 38.213 version 17.4.0 Release 17)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.213, 01 2023, version 17.4.0.

[3] 5G Mathworks, 2022. [Online]. Available: https://www.mathworks.com/help/5g/ug/5g-new-radio-prs.html

[4] J. Q. Alejandro Gonzalez-Garrido and S. Chatzinotas, "5g positioning reference signal configuration for integrated terrestrial/non-terrestrial network scenario," in *IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA*. IEEE, April 24-27, 2023, pp. 1–6.