Research Article

A Spectrum-Efficient Cross-Layer RF Distance Bounding Scheme

Yihang Song , Songfan Li , Chong Zhang , and Li Lu

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China

Correspondence should be addressed to Li Lu; luli2009@uestc.edu.cn

Received 26 November 2020; Revised 10 February 2021; Accepted 22 February 2021; Published 8 March 2021

Academic Editor: Kuo-Hui Yeh

Copyright © 2021 Yihang Song et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Distance bounding protocols guarantee a credible distance upper bound between the devices which require the spatial distance as a security parameter to defend Mafia Fraud attacks. However, in RF systems, the realization of distance bounding protocol faces obstacles due to low spectrum efficiency, since the distance bound estimation consumes a significant amount of frequency band in existing schemes. This hinders RF distance bounding from being practically deployed, especially in commonly used ISM bands. In this work, we propose an alternative, spectrum-efficient scheme for RF distance bounding. We build the physical layer as well as a protocol design based on SFCW signal and SFCW ranging. Thus, comparing existing schemes that consume many frequency bands, our scheme frees many spectrum resources. We propose solutions to the unique challenges facing such an SFCW-based scheme design, namely, data communication over unintelligent SFCW signals, and secure synchronization in the SFCW-based challenge-response exchange. We evaluate our scheme via the security analysis and physical layer simulations. The results show (i) its resistance to attacks commonly concerned in distance bounding, (ii) the feasibility of the physical layer design such as accurate ranging and data communication function, and (iii) the communication noise tolerance and the ability of multipath signal discrimination.

1. Introduction

In wireless applications that contain authentication protocols, sometimes one device would like to determine its spatial distance to another device as a security parameter. For instance, when a PKES (passive keyless entry and start) car is validating the identity of a key fob, it is better to confirm that the key fob is in close proximity at the same time. Otherwise, thieves can relay signals from a remote key fob to start the car and steal it [1, 2], as shown in Figure 1. These Mafia Fraud attacks (relay attacks) also appear in other RF systems such as proximity-based access control systems [3, 4], contactless payment [5], and secure location verification [6, 7].

As an appealing countermeasure, distance bounding protocol [8] denotes a class of authentication protocols that can measure the credible distance upper bound between a verifier (e.g., a PKES car) and a legitimate prover (e.g., a car key fob or a wireless token). The distance bound measurement relies on measuring the round trip time (RTT) of the challenge bits transmitted by the verifier and corresponding response bits replied by the prover.

To effectively realize distance-bounding protocol in RF systems, existing solutions have made much progress in solving two key issues [9]: (i) *Lowering the Prover Processing Time*. The prover needs to spend some time (i.e., the processing time) on generating response bits after receiving the challenge bits. If the processing time is nonnegligible, it will lengthen the RTT and cause inaccurate distance measurement results (e.g., a processing time of 50ns causes a ranging error of 7.5 m). That makes the protocol vulnerable to distance modification attacks, such as overclocking attacks on prover and Distance Fraud [10]. The solution to this issue is employing analog concatenation operations at the prover, which can reduce the processing time to nanoseconds [11, 12]. (ii) *Precise Distance Estimate*. After solving the first issue above, the next step is to equip the verifier with precise distance estimate functions; i.e., the verifier should accurately time the RTT. To address this, wideband signals such as FMCW (frequency modulated continuous wave) and UWB (ultra-wideband) signals are introduced into distance bounding schemes to measure the RTT [13–15] and offer cm-scale ranging resolutions.

FIGURE 1: An example of Mafia Fraud. An authentication is successfully executed when the prover (i.e., PKES key fob) is legitimate and close to the verifier (i.e., PKES car), as shown in Figure 1(a). Mafia Fraud attackers can amplify and relay the challenge-response signal at the physical layer to masquerade as a legitimate prover, as shown in Figure 1(b). (a) A normal authentication. (b) Mafia Fraud attack on PKES cars.

While these solutions and schemes are promising for enabling distance bounding in RF systems, they suffer from a constraint—their low spectrum efficiency. Existing schemes must use wideband signals, i.e., FMCW and UWB signals, to estimate the distance bound. These signals cause huge RF spectrum consumption and preclude these solutions from practical deployment. For example, to offer a ranging resolution of 1.5 m, FMCW and UWB signals entirely consume an RF band of 100 MHz [14, 15], which is as wide as the 2.4 – 2.5 GHz ISM band [16]. The wideband signals will interfere with other wireless communications within its frequency band. This fact hinders RF distance bounding from being deployed in the ISM band or coexisting with other wireless communications (e.g., 2.4 GHz Wi-Fi and Bluetooth).

To increase the spectrum efficiency in RF distance bounding realization, we explore a new realization scheme that utilizes stepped frequency modulated continuous wave (SFCW) as a basic physical layer to precisely estimate the distance bound. At a high level, SFCW utilizes the signals at discrete frequency points to build a “virtual” wideband signal (Figure 2) and thereby frees the spectrum resource which lies between the frequency points. Then, the freed spectrum resource could be utilized by other wireless communications or communication channels. Consequently, our design features higher spectrum efficiency and better compatibility with ISM radio regulations in practical deployments.

To minimize the prover processing time, we design a physical concatenation process that is compatible with the SFCW-based physical layer. On the protocol side, our design primarily follows the classical precommitment strategy [8, 11]. However, designing such a realization scheme based on the SFCW signal still faces unique challenges:

Challenge-Response Communication over Unintelligent SFCW Signals. SFCW signal is an unintelligent radar signal [17] that has no ability of data communication. However, in distance bounding protocols, distance measurement must be integrated with challenge-response communication so as to confirm that the prover is cryptographically legitimate, and it stays within legitimate distance. Thus, the legacy SFCW signal is required to be modified in our scheme and equipped with data communication functions. We tackle this challenge by encoding and modulating the challenge

and response bits on legacy SFCW signals. We encode challenge bits by switching the varying directions of SFCW signals’ frequencies (see 4.2). At the prover, by evolving backscatter communication as the concatenation process, the incoming challenge signals are reflected upon its arrival, and meanwhile, the pre-commitment response bits are encoded on the reflected signals in ASK modulation.

Synchronization in the Challenge-Response Exchange. In the challenge-response exchange phase, the synchronization mechanism prevents the prover from mistakenly sending response bits out too early or too late. That is, the operations performed by the prover, such as concatenating and transmitting the response bits, must be synchronized with the arriving pace of the challenge bits. However, in our case, extracting the synchronization information from the challenge bits which are encoded in SFCW signals is infeasible—demodulating SFCW signals requires complex processing (e.g., down-conversion and FFT computing) which inevitably increases the prover’s computing and energy overhead, thereby resulting in reduced battery life and high fabricating cost. To address this, we modify the classical protocol and add a secure synchronization round. In the round, transmitting the synchronization information is isolated from SFCW signals. The information can be transmitted in normal ways, such as using ASK modulation and PIE encoding, and easily extracted by passive RF front ends, which are similar to RFID tags [18].

To show the security of the proposed scheme, we analyze the resistance of our scheme to various attacks, including guessing attack, Distance Fraud, Mafia Fraud, overclocking attack, Terrorist Fraud, early bit detection (Early Detect), and deferred bit signaling attacks (Late Commit). To demonstrate the feasibility of our physical layer, we conduct a simulation model to validate the scheme function and investigate the performance of ranging accuracy, noise resistance, and multipath signal discrimination of our scheme.

The major contributions in this work are presented as follows. First, we address the low spectrum efficiency problem in RF distance bounding schemes by leveraging the SFCW signal as a basic physical layer. Second, we propose a scheme including both physical layer and protocol design to address the challenges of data communication and secure

FIGURE 2: The illustration of the SFCW signal and its spectrum consumption. (a) The SFCW signal shown in the time domain. It utilizes signals at discrete frequency points to compose a wideband signal. (b) The SFCW signal shown in the frequency domain. SFCW signal only occupies discrete frequency points, thereby freeing the spacings between the frequency points.

synchronization in our SFCW-based scheme. Finally, we present both the security analysis and the physical layer simulation to demonstrate the security and feasibility of our scheme.

The rest of the paper is organized as follows. Section 2 presents the background of distance bounding protocol and the related works. In Section 3, we introduce the SFCW signal and SFCW ranging principle. The proposed scheme, as well as the solutions to the challenges, is discussed in Section 4. Some issues that we encountered in designing the scheme are discussed in Section 5. We analyze the security and simulate the physical layer in Sections 6 and 7, respectively. Finally, we conclude the paper in Section 8.

2. Background and Related Works

2.1. Distance Bounding Protocol. The distance bounding protocol was firstly proposed [8] to prevent the Mafia Fraud attack on access control systems. For instance, Figure 1 illustrates the scenario of Mafia Fraud on PKES cars. Distance bounding protocol solves this problem by allowing a verifier (e.g., PKES car) to check its proximity to a legitimate prover (e.g., a legitimate key fob).

As shown in Figure 3, a typical distance bounding protocol consists of setup, exchange, and verification phases [11]. In the most critical exchange phase, the following rapid bit exchange is repeated for n rounds: in each round, the verifier challenges the prover with a freshly generated bit $C[i]$ ($i = 1, 2, 3, \dots, n$); upon receiving the $C[i]$ ($i = 1, 2, 3, \dots, n$), the prover calculates a response bit $R[i]$ and sends it back to the verifier immediately. When exchange rounds are finished, the verifier measures the average round trip time of the challenge-response exchange and computes the upper bound on distance as

$$\text{distance} = \frac{T_{\text{RTT}} - T_{\text{process}}}{2} \cdot c, \quad (1)$$

where T_{RTT} is the measured round trip time, c is the propagation speed of radio signal (i.e., the speed of light), and T_{process} is the processing time taken by the prover to generate the response (i.e., to demodulate the challenge and compute and modulate the response).

However, due to the processing time at the prover, this draft RTT-based distance bounding scheme suffers from a series of physic layer attacks. By speeding up the prover's

clock (i.e., reducing the processing time), an overclocking attacker [10] can convince the verifier that the prover is closer than it really is. Similarly, in the Distance Fraud attack [11], a malicious prover can pretend to be closer to the verifier by reducing its processing time or replying sooner than it does in normal times. A more "powerful" attacker which has a higher signal processing speed can exploit the verifier's large-signal receiving duration to launch the sophisticated physical layer attacks like Early Bit Detect [10] and Late Commit [19] (more details are discussed in Section 6) and thereby fabricates fake proximity between the verifier and prover.

2.2. Existing RF Distance Bounding Schemes

2.2.1. Round Trip Time (RTT) Based Schemes. To eliminate the vulnerability caused by the prover's processing time, the CRCS [11] scheme implements a time-saving concatenation operation at the physical layer to reply with the response and reduces the prover's processing time to 1ns. In the scheme, each of the response bits is prepared in advance, and its binary value determines which communication channel will be used in uplink communication. Thus, the verifier can listen to all of the two uplink channels to understand the response bit. The same concept with a low-power design is proposed in TIGHT [12] to enable low-power distance bounding in passive wireless tokens like RFID tags.

Although these works dramatically lower processing time to ns-level at the prover side, they can not be considered as complete distance bounding solutions since the verifier is still incapable to measure the round trip time. In detail, all the above works primarily focus on the prover design; however, they have little consideration of the verifier design and commonly use costly laboratory instruments to act as verifiers, which are unsuitable for practical applications. Thus, the cost and efficiency of round-trip-time measurement are increasingly becoming a bottleneck of distance bounding schemes.

2.2.2. Wideband Signal Based Schemes. To achieve precise and efficient round-trip-time measurement and thereby increase the accuracy in distance bound estimation, wideband signals are employed in distance bounding schemes, such as FMCW and UWB signals. (a) *FMCW-Based Schemes.* By introducing the FMCW signal into distance

FIGURE 3: A typical distance bounding protocol consists of a setup phase, an exchange phase, and a verification phase. In the most critical exchange phase, the verifier estimates the distance bound by timing the round trip time of cryptographic challenge and response bits. To enhance the protocol security against physical layer attacks, most cross-layer distance bounding schemes focus on effectively minimizing $T_{process}$ and measuring the RTT.

measurement, the scheme [13] enables a verifier to compute (but not to directly measure) the RTT in ns-level accuracy. To be specific, the FMCW-based verifier measures the frequency difference between its transmitting signal and the echo signal reflected by the prover to compute the signal round trip time and then computes the distance. As for challenge-response communication, in this scheme, the challenge bits are phase modulated while the prover adjusts the gain of its amplifier to modulate the response bits in the form of on-off keying (OOK). The low-power version is further proposed in [9], which offers a processing time of less than 20 ns. By introducing backscatter communication and ASK modulation similar to RFID tags [18, 20], the prover design proposed in [14] reduces its processing time virtually to zero. (b) *UWB-Based Schemes*. UWB signal is an effective choice to increase the ranging accuracy in RTT-based schemes because of its low signal period. The use of UWB signals is analyzed in [21] for accurate ranging in distance bounding. Then, Hancke and Kuhn present a scheme [22] that offers a processing time of 2.5 ns through the use of logic gates. UWB distance bounding system is further demonstrated through a high-speed FPGA prototype [15], which offers a processing time of 100 ns and a ranging resolution of 7.5 cm.

Although the FMCW-based schemes have realized accurate RTT measurement at the verifier side, these schemes face significant limitations due to their low spectrum efficiency. The reason stems from the fact that the accuracy of FMCW ranging depends on its signal bandwidth (e.g., 100 MHz bandwidth offers a theoretical ranging resolution of 37.5 cm). To satisfy the accuracy requirement of distance bounding (i.e., ns-level time measurement and cm-scale ranging), the scheme consumes a continuous frequency band that extends to tens of megahertz (MHz) to hundreds of megahertz. The huge bandwidth consumption is

unaffordable to current wireless spectrum space. If such a scheme, which entirely consumes a continuous 100 MHz band to achieve distance measurement, is deployed in the frequently used 2.4 – 2.5 GHz ISM band, it will cause interference to (or be easily interfered with by) other wireless communications. For example, if FMCW and UWB signals are employed in the n round exchange phase, all the Wi-Fi and Bluetooth channels will be interfered with. This fact limits the future development of FMCW-based distance bounding schemes in both commercial and industrial scenarios.

Similar to FMCW-based schemes, UWB-based schemes utilize signals which have large bandwidth (> 500 MHz) and short pulses to improve the ranging accuracy. Thus, they are also limited by low spectrum efficiency. Besides, to receive and transmit the short pulses, both the prover and the verifier require high sampling rate ADCs and DACs, which consume significant power (typically around 1–4W) [9].

3. Primer for SFCW Ranging

According to the above analysis, although the wideband signal-based schemes are efficient in hardware overhead and energy cost and achieve high ranging resolution, they consume significant spectrum resources. Thus, within such a wide frequency band, other wireless communications will interfere if the distance bounding protocol is running. Facing the situation, we believe that the spectrum efficiency has now become the major bottleneck restricting the widespread application of distance bounding. We observe that differing from FMCW or UWB signals which occupy a wide and continuous frequency band during their ranging, SFCW ranging can offer the same ranging accuracy with a high spectrum efficiency. To minimize the spectrum

consumption, SFCW ranging uses signal segments at discrete frequencies to replace the wideband signal which occupies a continuous frequency band. This makes SFCW ranging a compelling choice for distance bounding schemes.

The theory, implementation, and performance of SFCW ranging and SFCW-based radar are well documented and widely investigated in papers such as [17, 23, 24]. Instead of investigating SFCW ranging itself, we plan to introduce it into the distance bounding scheme and thereby obtain high spectrum efficiency. Hence, we just make a brief introduction to SFCW ranging in this section.

SFCW signal is the continuous wave signal whose frequency increases by Δf at regular intervals (which are denoted by T_s), as shown in Figure 2(a). In other words, the SFCW signal is a “virtual” wideband signal which consists of signals at discrete frequencies. Thus, the spacings between the discrete frequencies are freed and could be used by other RF radios, as shown in Figure 2(b).

The basic principle of SFCW ranging is described as follows. *Firstly*, the transceiver transmits an SFCW signal to the ranging target, and then the signal is reflected back and received by the transceiver. Thus, in the transceiver’s view, the reflected signal has a signal propagation delay τ when compared with the transmitting signal. *Secondly*, the verifier generates the beat signal by quadrature demodulating the receiving signal. The sample of the beat signal is a periodic function whose frequency depends on the signal propagation delay. The measured propagation delay and the distance between the transceiver and the target are given by

$$\tau = \frac{f_s \cdot T_s}{\Delta f}, \quad (2)$$

$$d = \frac{c f_s \cdot T_s}{2 \Delta f}, \quad (3)$$

where f_s is the frequency of the sampled beat signal.

Besides, according to [24], the ranging resolution is given by

$$\delta d = \frac{c}{2B}. \quad (4)$$

In this equation, the letter “ B ” denotes the total signal bandwidth, as shown in Figure 2(a). c represents the speed of light.

We give an overall proof that describes the combination of SFCW ranging and our communication scheme over SFCW signals in 4.2.

4. SFCW-Based Distance Bounding Scheme

4.1. Protocol Description. Our scheme mainly follows pre-commitment distance bounding protocol [8,11]. We first introduce our basic protocol design which consists of three phases in Section 4.1. The communication scheme during the exchange phase is discussed in Section 4.2. Besides, we should point out that the prover can not decode the incoming challenges and sign them in the verification phase,

since it has the limited computing performance to demodulate and decode chirp signals. As a remedy, in Section 4.3, we further add a secure synchronization round to this protocol, which can prevent the attacker from preasking the prover for its responses.

The basic protocol design is illustrated in Figure 4. In the setup phase, the prover picks an n -bit nonce R and sends a signed commitment to R (e.g., a signed hash of the string) to the verifier. Then, the verifier generates an n -bit nonce C and starts the exchange phase. During the critical exchange phase, each single challenge bit $C[i]$ is encoded on SFCW carriers and sent to the prover. Upon receiving $C[i]$, the prover concatenates a single bit $R[i]$ on $C[i]$ via backscatter communication and meanwhile reflects both the $C[i]$ and $R[i]$ to the verifier immediately. The exchange phase is discussed in detail in Section 4.2. When the exchange phase is finished, the prover signs the response R and the identity of the verifier V and communicates to the verifier. The verifier will check the following things: the C and R recovered in exchange phase must match the transmitted C and the commitment sent in the setup phase, respectively; the final signature must be valid and correspond to the identity of the prover which sends the signed commitment in the setup phase.

4.2. Data Communication over SFCW Signals

4.2.1. Communication Scenario in Exchange Phase. In the challenge-response exchange phase, the communication of challenge and response bits must be performed on SFCW signals. There are two reasons: (1) the round trip time of SFCW signals is used to estimate the distance bound between the verifier and prover; (2) in the meantime, the SFCW signals must carry challenge and response bits to insure the cryptographic legitimacy of the prover (i.e., to confirm the prover is not a forgery). Hence, we need to achieve data communication function on SFCW signals, which originally have no ability to carry any binary bits.

The communication scenario is shown in Figure 5. The SFCW signals are transmitted for n times in the exchange phase. Thereby, the verifier measures the RTT for n times, and the challenge-response exchange executes for n rounds (the figure only shows four rounds). Each exchange round contains downlink and uplink parts. (1) On the downlink, the verifier needs to transmit a single challenge bit $C[i]$ to the prover. To encode $C[i]$, the verifier switches the varying directions of the SFCW signals’ frequencies to represent 0/1 binary values. For example, the SFCW signal with descending frequency represents that the value of $C[i]$ is “0” and the signal with ascending frequency represents that the value of $C[i]$ is “1”. (2) On the uplink, the prover encodes $R[i]$ in amplitude modulation using backscatter communication. The prover achieves backscatter communication by switching the impedance among Z_0 and Z_1 and thereby changing the amplitude of the reflected signals. Then, the $C[i]$ and $R[i]$ are received and recovered by the verifier.

FIGURE 4: Similar to typical distance bounding protocols, our basic protocol design follows precommitment scheme and includes three phases. Differing from typical protocols, our exchange phase design is based on the SFCW physical layer, and the protocol that is shown here still needs further modifications to achieve secure synchronization.

FIGURE 5: The scenario of data communication on SFCW signals. On the downlink, the varying directions of the signal frequency (i.e., the signal varies from high frequency to low frequency or in reverse) represent 0/1 challenge bits; on the uplink, the SFCW signals which have been encoded with challenge bits are further encoded with response bits in ASK modulation by employing backscatter communication.

4.2.2. Mathematical Description and Proof. To carry the challenge and response bits in the exchange phase, SFCW signals are modified in our scheme and become different from typical SFCW signals: typically, the frequency of SFCW signals only increases during the ranging (as shown in Figure 5), but the frequency of modified SFCW signals can be either increasing or decreasing so as to achieve challenge bits encoding (as shown in Figure 5). The fact incurs a question: can such a scheme perform SFCW ranging as normal when the SFCW signals are modified and encoded with challenge bits? We give the mathematical description and proof of the exchange phase (including encoding challenge bits on SFCW signals as well as the ranging process based on the modified SFCW signals) as below.

Figure 6 shows SFCW signal transmitting and processing procedures.

In each of n exchange rounds, if the challenge bit which is about to be transmitted is “1”, the verifier will transmit an SFCW signal which is denoted by $\text{TX}_1(t)$ and expressed as

$$\text{TX}_1(t) = \sum_{n=0}^{N-1} \left\{ \text{rect}\left(\frac{t - nT_s - T_s/2}{T_s}\right) \cdot \cos[2\pi(f_0 + n\Delta f)t] \right\}, \quad (5)$$

where

$$\text{rect}\left(\frac{t - nT_s - T_s/2}{T_s}\right) = \begin{cases} 1, & \text{if } \left| \frac{t - nT_s - T_s/2}{T_s} \right| < \frac{1}{2}, \\ 0, & \text{other,} \end{cases} \quad (6)$$

FIGURE 6: The illustration of signal processing procedures which are mentioned in our mathematical proof given in 4.2.

and N , T_s , f_0 , and Δf are defined in Figure 2. As described by this equation, the signal frequency increases by Δf once after a time interval T_s .

Similarly, if the challenge bit that is about to be transmitted is 0, the verifier will transmit an SFCW signal which is denoted by $TX_0(t)$ and expressed as

$$TX_0(t) = \sum_{n=0}^{N-1} \left\{ \text{rect}\left(\frac{t - nT_s - T_s/2}{T_s}\right) \cdot \cos[2\pi(f_0 - n\Delta f)t] \right\}. \quad (7)$$

This indicates that the signal frequency increases by Δf once after a time interval T_s .

The transmitted signal is reflected back by the prover and then received by the verifier. The receiving signal $R_X(t)$ has a propagation delay (i.e., the RTT) of τ . For the sake of simplicity, we use one equation to describe the receiving signal in which “ $\pm$ ” is used to describe both the frequency increases and the frequency decreases. The equation is given as

$$RX(t) = \sum_{n=0}^{N-1} \text{rect}\left(\frac{t - nT_s - T_s/2}{T_s}\right) \cos[2\pi(f_0 \pm n\Delta f)(t - \tau)]. \quad (8)$$

The received signal processed using quadrature demodulating and the output IF signal (intermediate frequency signal) which contains in-phase (I) and quadrature (Q) components is represented as

$$S_{IF}(t) = \sum_{n=0}^{N-1} \text{rect}\left(\frac{t - nT_s - T_s/2}{T_s}\right) \exp[-j2\pi(f_0 \pm n\Delta f)\tau]. \quad (9)$$

The graph of the intermediate frequency signal consists of N segments corresponding to N time interval T_s . In each segment, the value of $S_{IF}(t)$ is constant and depends on τ . Then, this IF signal is sampled at each of the segments. The sampled signal is expressed as

$$S_{IF}(n) = \exp[-j2\pi(f_0 \tau \pm n\Delta f \tau)] \quad (n = 0, 1, \dots, N-1). \quad (10)$$

This can be regarded as the sample of a sinusoidal signal whose frequency cannot be affected by the symbol “ $\pm$ ”.

After putting the time variable $t = nT_s$ into (10), the frequency of $S_{IF}(n)$ is expressed as

$$f_s = \frac{\tau \Delta f}{T_s}. \quad (11)$$

Since f_s can be measured from the sampled signal, the propagation delay τ between the verifier and the prover is expressed as

$$\tau = \frac{f_s \cdot T_s}{\Delta f}. \quad (12)$$

This is the same as (2). Thus, according to our proof, the data communication scheme based on SFCW signals is feasible, and it will not affect the normal ranging function.

4.3. Synchronizing the Prover and Verifier. In the challenge-exchange phase, it is necessary to keep the prover synchronized with the verifier. Otherwise, the response bits could be transmitted too early or too late and can not be concatenated to the corresponding challenge bits. To synchronize, classic schemes, such as [9, 11], usually rely on extracting the synchronization information from received challenge bits or downlink signals. However, in our case, extracting the synchronization information from the downlink SFCW signals seems to be infeasible because demodulating the SFCW signals requires complex signal processing such as downconversion and FFT computing. This signal processing will increase the energy and computing overhead and thereby is not affordable to energy or performance-constrained provers.

To address this, we modify the classical protocol and add a secure synchronization round before the exchange phase. The communication in this round is isolated from SFCW signals—it uses pulse-interval encoding (PIE) and the prover can demodulate the PIE signals using a passive demodulator similar to RFID tags [18].

The modified protocol with a synchronization round is shown in Figure 7. The synchronization round is executed as follows. Firstly, the verifier picks and passes m -bit random data D to the prover using PIE. Secondly, the verifier extracts the data D from the received PIE signals using passive demodulators. Besides, it can also obtain synchronization clocks from the extracted PIE signals. Thirdly, the prover

FIGURE 7: Proposed protocol design with a secure synchronization round. In the synchronization round, the verifier selects a nonce string D and sends D to the prover in a bit-by-bit fashion using PIE (pulse-interval encoding). The prover extracts the synchronization clock and string D from the PIE data. The signed D is sent to the verifier in the verification phase. Then, the verifier will check the signed D to prevent that the attacker may use fake D to cheat the prover before the synchronization round, thereby getting the prover's response bits preemptively.

gets synchronized, and then both parties start the exchange phase. Finally, in the verification phase, the extracted data D should be signed and sent to the verifier. The verifier will check whether the D extracted by the prover matches with the D transmitted in the synchronization round. The check is necessary; otherwise, attackers can leverage fake data D to cheat the prover and thereby preask the prover for its responses.

5. Discussion

5.1. Processing Time. To minimize the prover processing time, our protocol follows precommitment distance bounding scheme and requires the prover to be equipped with backscatter communication. By employing the precommitment scheme, the prover is able to prepare response bits before the exchange phase and does not need to take time to compute response bits during the exchange. In addition, the backscatter communication modulates response bits on incident SFCW signal and meanwhile reflects the combined signal without any delay, similar to reflecting radar signals from an object such as airplanes [18]. Hence, the prover processing time spent on response generating, signal demodulating (as is discussed in 4.3), and modulating is reduced virtually to zero.

5.2. SFCW Maximum Unambiguous Range. SFCW ranging method has a limitation called maximum unambiguous range [24]. The maximum unambiguous range depends on the frequency step (Δf) of SFCW signals and is given by

$$D_{\max} = \frac{c}{2\Delta f}. \quad (13)$$

If the prover stays out of $D_{\max}$, SFCW ranging will be unreliable, and the ranging result will unexpectedly show that the prover is still within $D_{\max}$. The relationship of measured distance and actual distance is given by

$$D_{\text{measured}} = D_{\text{actual}} \bmod D_{\max}, \quad (14)$$

where D_{measured} is the measured distance and D_{actual} is the actual distance between the verifier and the prover. So, it seems that our scheme can only work within $D_{\max}$.

We tackle this problem by employing cross-correlation [25], a common algorithm which is used to estimate the similarity of two signal sequence in modern communication systems [26]. At a high level, cross-correlation is used to confirm that the prover is within $D_{\max}$. For example, if we set Δf to 100 kHz, $D_{\max}$ will be 1500 m ($5\mu\text{s}$ round trip time). Within the first $5\mu\text{s}$ after sending its challenge, the verifier keeps receiving and starts cross-correlation to detect whether the desired response exists in the received signal.

Thus, the verifier knows that the prover is within D_{MAX} if the desired response is contained in the received signal, and it is able to further use SFCW-based ranging to achieve fine-grained distance estimation.

5.3. Multipath Signal Discrimination. The scheme proposed in 4.2 is prone to be affected by the multipath effect. The multipath effect brings diverse signal components to the IF signal (9) and disturbs the distance measurement. The problem could be solved by performing inverse fast Fourier transform (IFFT), which is widely used in SFCW-based ground penetrating radar (GPR) to detect and discriminate multiple buried targets [27].

At a high level, IFFT is performed to the sample of IF signal (e.g., equation (10)), and all the echoes, including the LOS echo and NLOS echoes, can be distinguished on the output graph, as shown in Figure 8. In traditional SFCW-based GPR radar, the multiple echoes are caused by multiple buried targets since they have diverse propagation paths. This is similar to our scenario in which the signals travel between the verifier and prover and have both LOS (line-of-sight) and NLOS (non-Line-of-Sight) propagation paths.

In Figure 8, the pulses indicate different signal propagation paths. The propagation delay τ and the distance are given by

$$\tau = \frac{i}{N\Delta f} \quad (i = 0, 1, \dots, N-1), \quad (15)$$

$$d = \frac{ci}{2N\Delta f} \quad (i = 0, 1, \dots, N-1), \quad (16)$$

where i is the abscissa value where the curve reaches the first peak in Figure 8 since the LOS propagation path has minimum RTT. N is the number of frequency steps shown in Figure 2(a).

The multipath signal discrimination is simulated in 7, and the mathematical proof is given in the appendix.

6. Security Analysis

In this section, we analyze the resistance of the proposed scheme to various attacks on distance bounding protocols.

6.1. Distance Fraud. Distance Fraud, which is also called Lone Distance Fraud in [28], is launched by a remote dishonest prover. The dishonest prover may deviate from the protocol and mislead the verifier into believing that it is local [29]. Distance Fraud occurs if the protocol allows the prover to send its reply before receiving the challenge [28], or the prover reduces its processing time secretly [9]. In our design, the prover must concatenate each of the response bits on the corresponding challenge bit, and then both the challenge and response bit are reflected back for further check. That is, our protocol prohibits the situation in which the prover can send its reply before receiving the challenge. Besides, since the prover processing delay has been reduced to virtually zero, the dishonest prover cannot launch Distance Fraud by further reducing its processing time.

FIGURE 8: By employing IFFT, the signals that propagate along the LOS path or the NLOS path are transformed into pulses in the time domain. The first pulse represents the signal which propagates along the LOS path.

6.2. Guessing Attack. Guessing attack could be classified into Distance Fraud [11] in which a dishonest prover guesses the challenge in advance to deceive distance measurement. With the guessed challenge, the prover is able to reply to the verifier with response bits sooner than he normally does. This attack will be effective when it is launched in single-exchange challenge-response protocols with a multibit packet. In such a protocol, the attacker can guess the value for the last bit transmitted by the verifier and preemptively transmit a response [10]. In our protocol, the dishonest prover must guess all the challenge bits transmitted in the n round challenge-response exchange phase since each of the challenge bits must be reflected back and then checked by the verifier separately. We believe that the probability of launching a successful guessing attack is $(1/2)^n$. To verify, we simulate the guessing attack with the simulation configurations used in Section 7. During the simulation, an attacker knows the whole process of the protocol except the four-bit response which is held by the legitimate prover. To deceive the verifier, the attacker guesses four bits as a response and transmits them to the verifier in advance. We simulate this attack scenario 1000 times, and the success rate of attack is 15.7%, which is approximately 16%.

6.3. Overclocking Attack. Overclocking attack involves one remote honest prover and an attacker which tries to trick the verifier into believing the prover is within the distance bound [10]. To reduce the distance measured by the verifier, the attacker increases the clock speed of the prover processor, thereby reducing its processing time. Increasing the clock speed is feasible by leveraging physical means such as interfering with the processor's crystal oscillator. Similar to the case of Distance Fraud, our scheme is resistant to overclocking attacks due to the processing time which is close to zero.

6.4. Mafia Fraud. The Mafia Fraud (which is also called relay attack or man-in-the-middle attack) [8] is performed by external attackers which stay in the middle of the prover and the verifier. The attackers can relay the challenge and response signals at the physical layer to convince the verifier that the prover is close to the verifier. Distance bounding

protocol natively prevents Mafia Fraud unless the protocol is based on slow medium (e.g., using ultrasonic as the medium), so attackers are able to relay the challenge and response signals using the medium with fast signal propagation speed, such as radio signal, to gain advantages [10, 30]. In our design, the SFCW signals propagate at the speed of light, so the attackers cannot launch Mafia Fraud.

6.5. Early Bit Detection and Deferred Bit Signaling. The attack leveraging early bit detection and deferred bit signaling [10] could be considered as a variation of Mafia Fraud [19]. In early bit detection, the attacker uses a receiver that has m -times better signal-to-noise ratio than a regular receiver to preemptively detect the symbol using about $1/m$ of the symbol's regular receiving time. In deferred bit signaling, an attacker transmits m times the symbol amplitude to the verifier or the prover in the final $1/m$ -th of the symbol period. To sum up, early bit detection and deferred bit signaling gain time in symbol receiving and committing, so the time saved could be used in relaying signals between a verifier and a remote honest prover. The attack which combines early bit detection and deferred bit signaling includes the following steps: (i) a proxy prover (actually it is an attacker) gains time by early detecting a challenge symbol transmitted by the honest verifier and then relays the symbol to a remote proxy verifier (which is actually another attacker); (ii) the proxy verifier late commits the challenge symbol to an honest, remote prover using $1/m$ -th of the regular symbol period; (iii) the proxy verifier early detects the response symbol and relays it to the proxy prover; (iv) the proxy prover late commits the response symbol to the honest verifier.

In our scheme, indeed, the attackers can early detect the challenge bits encoded on the SFCW signal and fabricate a fake echo signal to manipulate the measured distance. However, the attackers cannot cheat an honest prover out of correct response bits and thereby cannot concatenate the response bits to the fake echo signal since prover replying to the response bits is based on synchronization information communicated in the secure synchronization round. Besides, the secure synchronization round is resistant to early bit detection and deferred bit signaling since we employ PIE in the round and the binary value of a PIE symbol depends on the pulse duration time but not on the symbol amplitude or energy, as shown in classical PIE demodulation circuits [18].

6.6. Terrorist Fraud. Terrorist Fraud involves an attacker located close to the verifier and a remote dishonest prover. The dishonest prover colludes with the attacker by sharing its short-term secrets (e.g., the nonce challenge and response bits) to cheat the verifier [31, 32]. Terrorist fraud resilient protocols [31, 33] bind the prover's long-term secret to the nonce challenge and the response bits picked in the setup phase. Thus, the prover cannot reveal its short-term secrets unless it discloses its valuable long-term secret [9]. If needed, our scheme is capable of employing those Terrorist Fraud

resilient protocol designs since our scheme design is independent of and capable of these high-level protocol designs.

6.7. Distance Hijacking Attack. In Distance Hijacking Attack [28], a remote dishonest prover exploits one or more honest provers, which are close to the verifier, to deceive the verifier with the fake verification information. In the attack, a dishonest prover jams the signature sent by an honest prover in the verification phase and replaces it with the signature of itself. Thus, the dishonest prover misleads the verifier into believing that the dishonest prover is close to the verifier. In our verification phase, the verifier checks if the signature corresponds to the identity of the prover which sends the signed commitment in the setup phase. Thus, the dishonest prover cannot launch the Distance Hijacking Attack by replacing the signature in the verification phase.

7. Physical Layer Simulation

We build a model in Matlab Simulink to simulate our physical layer design and demonstrate its function, ranging accuracy and noise resistance of data communication.

7.1. Basic Function Simulation. The simulation model consists of a prover, a verifier, and the propagation channel. The verifier transmits SFCW signals which carry challenge bits to the prover. The signals will be delayed and get disturbed by noise in the propagation channel. When the prover receives the signals, it will encode response bits to the incoming signals and reflect the signals back to the verifier. Finally, if the received signals are demodulated and decoded successfully, the verifier can recover the challenge and response bits from the signals and meanwhile obtain the distance bound.

The parameters in the simulation are presented as follows. The total bandwidth of the SFCW signal B is equal to 500MHz; the frequency increment Δf is 1MHz; the number of frequencies used in SFCW signals N is 500. The simulation results of SFCW ranging and challenge-response communication are shown in Figure 9.

The challenge bits and corresponding frequency varying directions are shown in Figure 9(a) for $C = 1$ and Figure 9(b) for $C = 0$. Figures 9(c) and 9(d) show SFCW signal segments at different frequencies. The ASK modulation performed by the prover is shown in Figures 9(e) and 9(f). The demodulated ASK bits and the beat signal are shown in Figures 9(g) and 9(h). Then, the sampled beat signal is processed in Matlab using 500-point IFFT, and the result is shown in Figure 9(i). In our 50 simulations, all the n values that we get are within the range of 25 ± 0.1 and are corrected to 25 because the n value should be an integer. According to (16), we get the $\tau = 50$ ns. Thus, the function of the physical layer scheme runs as desired.

7.2. Ranging Accuracy and Bit Error Rate under Noise Environment. The setup for ranging accuracy and data communication simulations is given as follows. We add

FIGURE 9: The simulation results of SFCW ranging and challenge-response communication. (a) The SFCW frequency in the time domain ($C=1$). (b) The SFCW frequency in the time domain ($C=0$). (c) The SFCW waveform segments @ 620 MHz, 820 MHz, 1020 MHz. (d) The SFCW waveform segments @ 1120 MHz, 920 MHz, 720 MHz. (e) The 100 kHz ASK baseband signal. (f) The ASK modulation on the SFCW signal. (g) The ASK bits demodulated by the envelope detector. (h) The IF signal (about 50 kHz) after the down-conversion. According to (2), the τ is about 50 ns. (i) The Curve of IFFT result. The LOS pulse arrives when n equals 25. According to (15), we get the $\tau = 50$ ns.

FIGURE 10: The simulation results of the multipath signal identification. (a) The peaks that we obtained in multipath signal identification simulation. The three peaks in this graph correspond to one LOS signal and other two multipath signals, respectively. (b) The results of 50 simulations ($E_b/N_0 = 7$ dB). The average propagation delays correspond to the LOS signal and the multipath signals can be obtained by leveraging equation (15), where i is the average of abscissa values that correspond to the LOS peaks or the multipath peaks shown in this graph. In the simulations, the estimated average propagation delays of these three signals are 50 ns, 56 ns, and 70 ns.

FIGURE 11: Continued.

FIGURE 11: Signal with AWGN noise and Uplink BER rate. (a) ASK modulation on the SFCW signal. (b) Uplink signal with AWGN noise ($E_b/N_0 = 7$ dB). (c) Measured uplink BER rate.

TABLE 1: Benchmark with existing schemes.

Scheme	Parameters						
	Processing Delay	Precise Distance Measurement	Spectrum Consumption	Clocking	EP/LC	Terrorist	Hijacking
Brands & Chaum [8]	>50 ns	No	—	No	No	Yes	Yes
CRCS [11]	1ns	No	—	Yes	Yes	Yes	Yes
UWB-based [15, 22]	2.5 ns	Yes (cm-level)	High (100 s of MHz)	Yes	No	Yes	Yes
FMCW-based [14]	≈ 0	Yes (cm-level)	High (100 s of MHz)	Yes	Yes	Yes	Yes
SFCW-based (this scheme)	≈ 0	Yes (cm -level)	Low (discrete frequencies)	Yes	Yes	Yes	Yes

The authors discuss the protocol security against various attacks in Section 6 but only list four types of attacks (Clocking, Early Detect, Late Commit, and Distance Hijacking attacks) due to space limitations of the page. Actually, all the five types of schemes listed in Table 1 can resist the attacks not listed in the table.

extra propagation paths (which have propagation delays of 56.6 ns and 70 ns, respectively) in the simulation model to simulate the multipath effect. Besides, we add an AWGN (Additive White Gaussian Noise) channel model to each of the propagation paths to simulate the noisy environment. The AWGN channels have E_b/N_0 values that vary from 0 to 15 dB. For each E_b/N_0 value, we conduct 50 simulations using different challenge and response bits to estimate the propagation delay and the communication BER.

The results of propagation delay estimation are shown in Figure 10. An example of the simulation result is shown in Figure 10(a). In this figure, the LOS signal and two multipath signals are identified. For each E_b/N_0 value, we repeat the simulation 50 times. An example of simulation results which has the E_b/N_0 value of 7 dB is illustrated in Figure 10. According to the simulation results, the average propagation delays of these three signals are 50 ns, 56 ns, and 70 ns. *The Results of IFFT*. That means the range resolution of our simulation achieves the theoretical *cm*-scale resolution.

In the simulation for uplink BER analysis, we choose four bit rates: 50 kbps, 100 kbps, 200 kbps, and 400 kbps.

Figures 11(a) and 11(b) show the SFCW signals with ASK modulation and AWGN. The communication BERs under different AWGN are shown in Figure 11(c). Since we employ backscatter in uplink communication, the uplink communication is not as reliable as downlink communication and performs better when the E_b/N_0 is above 12 dB.

8. Conclusion and Future Works

In this paper, we propose an RF distance bounding scheme to address the low spectrum efficiency problem in RF distance bounding realization. Our scheme exploits the SFCW signal as a basic physical layer to gain high spectrum efficiency. We propose solutions to the challenges which appear when we try to merge the SFCW signal with distance bounding protocol, namely, achieving data communication over the unintelligent SFCW signals, and a secure synchronization scheme for the SFCW-based challenge-response exchange. We analyze the protocol security against attacks on distance bounding and then validate the performance of the physical layer by conducting simulations. As illustrated in Table 1, comparing with existing cross-layer RF

distance bounding schemes, our scheme maintains the features of low processing time and accurate ranging and meanwhile achieves higher spectrum efficiency. This helps RF distance-bounding systems to coexist well with other wireless communications, especially when deployed in ISM bands.

Future improvements could focus on promoting practice deployment of the scheme. For deployment on vehicles, it is compelling to integrate our scheme with existing SFCW-based vehicle radars [34–36] to save the fabricating cost. For deployment on battery-powered verifiers, such as handheld RFID readers, future work could focus on improving the

power efficiency of signal processing such as SFCW signal quadrature demodulation and IFFT operation to improve the device battery life.

Appendix

Proof of Multipath Signal Discrimination

For the sake of simplicity, the authors firstly perform IFFT to the sample of IF signal (10) which is corresponding to the LOS propagation path. This is illustrated as

$$\begin{aligned}
 S(i) &= \frac{1}{N} \sum_{n=0}^{N-1} S_{\text{IF}}(n) \exp\left(jn \frac{2\pi i}{N}\right) \\
 &= \frac{1}{N} \sum_{n=0}^{N-1} \exp(-j2\pi f_0 \tau) \exp(-j2\pi n \Delta f \tau) \cdot \exp\left(jn \frac{2\pi i}{N}\right) \\
 &= \frac{1}{N} \exp(-j2\pi f_0 \tau) \cdot \exp\left[j \frac{N-1}{N} \pi (i - N \Delta f \tau)\right] \cdot \frac{\sin[\pi (i - N \Delta f \tau)]}{\sin[\pi/N (i - N \Delta f \tau)]}, \quad (i = 0, 1, \dots, N-1).
 \end{aligned} \tag{A.1}$$

The value of $S(i)$ will be maximum when

$$i = \tau N \Delta f. \tag{A.2}$$

Thus, by leveraging i which is the abscissa value when the value of $S(i)$ is maximum, the propagation time of the LOS signal is given by

$$\tau = \frac{i}{N \Delta f}. \tag{A.3}$$

In practice, considering NLOS signals, after quadrature demodulation, the IF signal (9) consists of multiple signals caused by both LOS and NLOS echoes. IFFT will transform all the signals to peaks, which is similar to the transformation shown in (A.1). The peak, which represents the LOS propagation path, is the first one in the graph since the LOS signal has a minimum propagation time. Thus, the LOS and NLOS signals can be discriminated.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61872061.

References

- [1] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, Zürich, Switzerland, February 2011.
- [2] M. Humphries, "Tesla model s stolen in 30 seconds using keyless hack," 2019, <https://www.pcmag.com/news/tesla-model-s-stolen-in-30-seconds-using-keyless-hack>.
- [3] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 410–419, Chicago IL, USA, November 2009.
- [4] S. K. Gupta, T. Mukherjee, K. Venkatasubramanian, and T. Taylor, "Proximity based access control in smart-emergency departments," in *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, Pisa, Italy, March 2006.
- [5] S. Drimer and S. J. Murdoch, "Keep your enemies close: distance bounding against smartcard relay attacks," in *USENIX Security Symposium*, vol. 312, 2007.
- [6] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM Workshop on Wireless Security*, pp. 1–10, New York; NY, USA, September 2003.
- [7] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, p. 7, Chengdu, China, October 2005.
- [8] S. Brands and D. Chaum, "Distance-bounding protocols," in *Advances in Cryptology — EUROCRYPT '93*, pp. 344–359, Springer, Berlin, Germany, 1994.
- [9] A. Ranganathan, B. Danev, and S. Capkun, "Low-power distance bounding," 2014.

- [10] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: distance-bounding attacks in wireless networks," in *Proceedings of the European Workshop On Security in Ad-Hoc and Sensor Networks*, pp. 83–97, Hamburg, Germany, September 2006.
- [11] K. B. Rasmussen and S. Capkun, "Realization of rf distance bounding," in *Proceedings of the USENIX Security Symposium*, pp. 389–402, Baltimore, MD, USA, August 2010.
- [12] M. J. Hussain, L. Lu, and H. Zhu, "Tight: a cross-layer rf distance bounding realization for passive wireless devices," *IEEE Transactions on Wireless Communications*, vol. 14, no. 6, pp. 3076–3085, 2015.
- [13] A. Ranganathan, B. Danev, and C. Srdjan, "Fmcw-based realization of distance bounding protocols," *Technical Report*, vol. 753, 2012.
- [14] L. Lu, M. J. Hussain, and Z. Han, "A fmcw-based cross layer rf distance bounding scheme," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4009–4016, 2016.
- [15] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "Uwb rapid-bit-exchange system for distance bounding," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless And Mobile Networks*, pp. 1–12, New York, NY, USA, June 2015.
- [16] ITU, "Radio regulations Edition of 2016," <http://handle.itu.int/11.1002/pub/80da2b36-en>.
- [17] K. Iizuka and A. P. Freundorfer, "Detection of nonmetallic buried objects by a step frequency radar," *Proceedings of the IEEE*, vol. 71, no. 2, pp. 276–279, 1983.
- [18] D. M. Dobkin, "The Rf in RFID: Uhf RFID in practice," in *NewnesElsevier*, Boston, MA, USA, 2012.
- [19] G. P. Hancke and M. G. Kuhn, "Attacks on time-of-flight distance bounding channels," in *Proceedings of the First ACM Conference on Wireless Network Security*, pp. 194–202, Alexandria, VA, USA, March 2008.
- [20] U. Karthaus and M. Fischer, "Fully integrated passive uhf rf id transponder ic with 16.7- μ minimum rf input power," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 10, pp. 1602–1608, 2003.
- [21] M. Kuhn, H. Luecken, and N. O. Tippenhauer, "Uwb impulse radio based distance bounding," in *Proceedings of the Positioning Navigation and Communication (WPNC) 2010 7th Workshop on*, pp. 28–37, Bertinoro, Italy, September 2010.
- [22] G. P. Hancke, "Design of a secure distance-bounding channel for rf id," *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 877–887, 2011.
- [23] L. A. Robinson, W. B. Weir, and L. Young, "Location and recognition of discontinuities in dielectric media using synthetic rf pulses," *Proceedings of the IEEE*, vol. 62, no. 1, pp. 36–44, 1974.
- [24] P. Van Genderen and I. Nicolaescu, "System description of a stepped frequency cw radar for humanitarian demining," in *Proceedings Of the 2nd International Workshop On Advanced Ground Penetrating Radar*, pp. 9–15, Delft, The Netherlands, May 2003.
- [25] 2020 Wikipedia, "Cross Correlation," <https://en.wikipedia.org/wiki/Cross-correlation>.
- [26] A. Fort, J.-W. Weijers, V. Derudder, W. Eberle, and A. Bourdoux, "A performance and complexity comparison of auto-correlation and cross-correlation for ofdm burst synchronization," in *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. II–341, Hong Kong, October 2003.
- [27] V. Mikhnev and P. Vainikainen, "Discrimination of near-surface targets in step-frequency radar," in *Proceedings of the 2001 31st European Microwave Conference*, pp. 1–4, London, England, October 2001.
- [28] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance Hijacking Attacks on Distance Bounding Protocols," in *Proceedings of the 2012 IEEE Symposium On Security And Privacy*, pp. 113–127, Oakland, CA, USA, May 2012.
- [29] T. Chothia, J. De Ruiter, and B. Smyth, "Modelling and analysis of a hierarchy of distance bounding attacks," in *Proceedings of the 27th USENIX Security Symposium USENIX Security 18*, pp. 1563–1580, Baltimore, MD, USA, July 2018.
- [30] S. Sedihpour, S. Capkun, S. Ganerwal, and M. Srivastava, "Implementation of attacks on ultrasonic ranging systems," in *Proceedings of the Demo at the ACM Conference On Networked Sensor Systems (SenSys)*, San Diego, CA, USA, March 2005.
- [31] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Proceedings of the IFIP International Information Security Conference*, pp. 223–238, Auckland, New Zealand, July 2005.
- [32] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the fiat-shamir passport protocol," in *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques*, pp. 21–39, Amsterdam, The Netherlands, October 1987.
- [33] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, pp. 204–213, Singapore, March 2007.
- [34] Z. Liu and F. Bien, "A new multi-target detection for vehicle radar," in *Proceedings of the 2014 International SoC Design Conference (ISOCC)*, pp. 28–29, Jeju, South Korea, April 2014.
- [35] Z. Liu and F. Bien, "An improved model of vehicle radar for multi-target based on stepped frequency pulse radar," in *Proceedings of the 2014 IEEE International Wireless Symposium (IWS 2014)*, pp. 1–3, Xi'an, China, March 2014.
- [36] B. Lu, X. Zhang, Q. Song, Z. Zhou, and J. Wang, "A vehicle based sfcw sar for differential interferometry," in *Proceedings of the 2011 3rd International Asia-Pacific Conference on Synthetic Aperture Radar (APSAR)*, pp. 1–4, Seoul, South Korea, January 2011.