Physical Layer Secret Key Generation Using Joint Interference and Phase Shift Keying Modulation

Najme Ebrahimi, *Member, IEEE*, Hun-Seok Kim, *Member, IEEE*, and David Blaauw, *Fellow, IEEE*

***Abstract*— In existing physical layer security (PLS) and key generation protocols, major assumptions, including channel reciprocity, localization, and synchronization between the legitimate parties, are often considered. However, these assumptions are arguable in practice leading to major barriers in building systems based on PLS protocols. To overcome these barriers, we proposed, designed, and implemented a novel embedded architecture for distributed Internet-of-Things (IoT) networks that utilize a master–slave full-duplex communication to exchange a random secret key. In the proposed architecture, an IoT node generates a phase-modulated random key/data and transmits it to a master node in the presence of an eavesdropper, referred to as Eve. The master node, simultaneously, broadcasts a high-power signal using an omnidirectional antenna, which is received as a jammer signal or interference by Eve. This results in a high bit error rate (BER) making the data undetectable by Eve. The two legitimate nodes communicate in a full-duplex fashion and, consequently, subtract their transmitted signals from the received signal (self-interference cancellation). Our proposed protocol does not require any knowledge of the node locations. In particular, we show, using theoretical and measurement results, that our proposed approach provides significantly better security measures, in terms of the BER at Eve's location, compared to a conventional method based on directional beamforming antennas. Also, it is proved that in our novel system, the possible eavesdropping region, BER $< 10^{-1}$, is always smaller than the reliable communication region, BER $< 10^{-3}$.**

***Index Terms*— Full-duplex technology, interference, Internet of Things (IoT), physical layer, secret key, security.**

I. Introduction

THE anticipated growth of the Internet-of-Things (IoT) sensor networks and cellular networks in future systems, 5G and beyond, poses a higher risk of malicious attacks against message confidentiality in communication systems. In the next generation of distributed wireless world, we need security at all layers from the application layer and network layer [1] to the MAC layer [2] and to the physical layer [3]–[9].

Security is often guaranteed in the higher layers of the network architecture using cryptographic protocols [10]–[14]. Such protocols require a secure and random key sequence shared between the authenticated nodes *a priori* [10]–[14]. This makes centralized cryptographic-based techniques not scalable as the future networks will be massively distributed. In addition, by advancing quantum computers/supercomputers, the encryption algorithms with fixed secret keys can be broken in a fraction of a second. Hence, it is highly desirable to regularly and securely update the shared key between the wireless nodes in order to minimize the chances of successful attacks. To this end, secure communication and random key generation in physical layer, i.e., referred to as physical layer security (PLS), using characteristics of the channel is of utmost interest [3]–[9].

Due to the broadcasting nature of the wireless channel in physical layer, there will be adversarial attacks, including eavesdropping and jamming. An eavesdropper tries to passively extract the data from the channel without interfering with the communication, while a jammer intends to interrupt the intended receivers. The implementation of a PLS system has several aspects, including theoretical guarantees of security as well as properly employing hardware and antenna techniques. On the theoretical side, the channel phase and fading information can be employed to generate the secret key with information-theoretic guarantees of security [15]–[24]. However, due to the inherent channel randomness, the implementation based on such an information-theoretic approach requires fast channel estimation necessitating high power consumption that is not feasible in IoT networks.

In the main prior line of work focusing on hardware implementation of PLS protocols, employing directional antennas and beamforming methods is considered in order to transmit signal/key securely using a narrow beam [25]–[27], as shown in Fig. 1(a). Besides common issues with PLS including arguable assumptions of channel reciprocity and synchronization, another major problem with this approach is the information leakage in sidelobes [26]–[37]. Also, there has been an ongoing effort on the feasibility of eavesdropping using a small antenna or reflector in the main lobe of the directional antenna without deteriorating the main radiation pattern making the attack undetectable [38]. Directional modulation with array synthesizing using switching antennas [26]–[37] and employing artificial noise [39], [40] is other proposed solutions to use an array of antennas to destructively distort the signal at Eve's location while being added constructively at the intended receiver to securely transmit the signal, as shown in Fig. 1(b). This technique requires localization of the intended receiver as well as the knowledge of the location of Eve and, hence, requires power-hungry

Manuscript received September 18, 2020; revised January 5, 2021; accepted January 15, 2021. Date of publication February 24, 2021; date of current version May 5, 2021. *(Corresponding author: Najme Ebrahimi.)*

The authors are with the Electrical Engineering and Computer Science (EECS) Department, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: najme@umich.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TMTT.2021.3058183.

Digital Object Identifier 10.1109/TMTT.2021.3058183

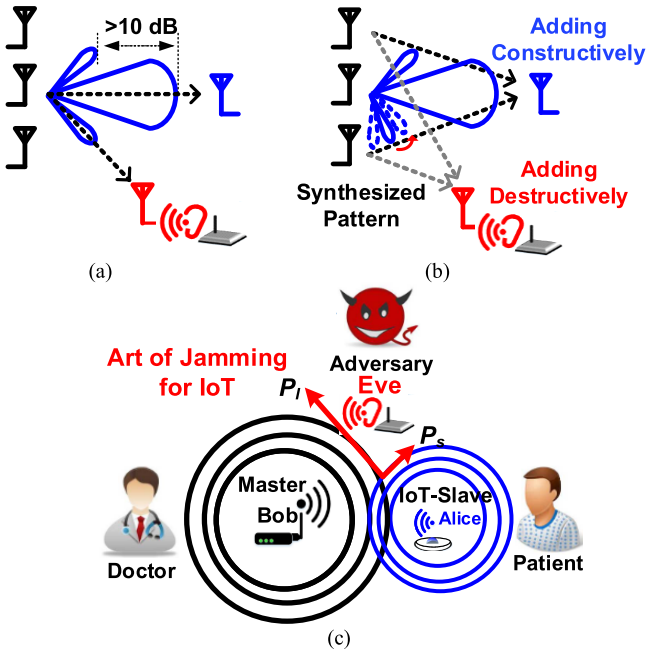


Fig. 1. Physical layer communication with different antenna architectures. (a) Directive communication introducing larger than 10-dB sidelobes. (b) Directional modulation to cancel the sidelobe leakage at a particular location. (c) Proposed joint interference-data transmission using all omnidirectional antennas and full-duplex technology.

techniques while having the problem of information leakage at the main lobe.

In this work, we propose a novel technique employing an omnidirectional antenna that does not require any location awareness. In our proposed protocol, secret keys transmitted by the IoT node to the intended master node will be masked at Eve's receiver using an intentional jammer or interference signal transmitted by the master node at the same time and frequency [see Fig. 1(c)]. The master node can decode the received data using the full-duplex technology and by canceling out the self-interference leakage. This concept is also referred to as an "art of jamming" or electronic countermeasure that has been widely used in military radar equipment, where by transmitting additional radio signal toward adversarial users, their communication will be interrupted and jammed. However, reliable communications between the intended users and the jammer radar will be interrupted, too, requiring additional security techniques such as frequency hopping or spread spectrum. These are, however, key-based enciphering (cryptographic) techniques and are vulnerable to be broken. In this work, we employ the jamming technique to provide PLS, for the first time, for low-power IoT networks. The IoT node shares the secret key in a phase shift keying (PSK) modulation format that will be masked by the master's jammer's power at Eve's receiver. The security is characterized in terms of the effective bit-error rate (BER) at Eve. Also, reliability, in terms of the BER between the master node and the IoT node, is characterized. It is then proved that in our novel system, the possible eavesdropping region is always smaller than the reliable communication region.

This article expands on earlier work from IMS 2019 [41] that proposed full-duplex communication to enhance the security compared to directional techniques. The expansion includes a more thorough analytical expression of security guarantees as well as protocol explanations. Section II describes our proposed protocol to securely exchange the secret key between distributed IoT nodes together with theoretical and analytical comparisons with the directional beamforming technique. Section III presents the embedded system implementation, and the measurement results will be expressed in Section IV. Section V concludes this article.

II. Principle of the Proposed Security Protocol

A. Full-Duplex Simultaneous Interference-Key Transmission

The proposed protocol to update the shared secret key in the physical layer is based on the full-duplex technology [42]–[48]. In this setup, each node, which can be an IoT node, e.g., patient's vital IoT sensors, updates its key by transmitting a random sequence to the master node in the IoT network, e.g., a doctor's controlling unit, using a PSK modulation format, as shown in Fig. 1(c). The goal is to keep the transmitted random sequence, which is used to generate the secret key, secure from a passive eavesdropper, referred to as Eve. To this end, the master node simultaneously transmits a constant sinusoidal signal at the same time and the same frequency in order to jam Eve' receiver and to provide the desired security in the physical layer. At the same time, the intended master node extracts the secret key from the signal transmitted by the IoT node by incorporating principles of full-duplex technology, in particular, self-interference cancellation. The security of the proposed technique is described and measured based on the BER of the received PSK modulation signal at Eve expressed in [41], as shown in the following equation:

$$\text{BER} = p_e = \frac{1}{k}\text{erfc}\left(\sqrt{k \times (\text{SINR})}\sin\left(\frac{\Delta\theta}{2}\right)\right) \tag{1}$$

where erfc is the Gaussian error function, $k = \log_2^M$ is the number of bits associated with each modulation symbol, and M is the total number of symbols in the modulation. Also, SINR is the signal-to-interference and noise ratio, and $\Delta\theta$ is the phase shift that depends on the maximum phase shift bound, denoted by θ_b, as follows:

$$\Delta\theta = \frac{2 \times \theta_b}{M}. \tag{2}$$

The maximum phase bound, θ_b, in a conventional setting without interference is equal to $\pm\pi$ for M-PSK modulation. For instance, for 8-PSK modulation, shown in Fig. 2(a), the phase shift, $\Delta\theta$, is 45°. However, in the presence of interference, both SINR and the phase shift, $\Delta\theta$, highly depend on the interference level measured in terms of the interference-to-signal power (P_I/P_S) at the receiver. Let the parameter ρ denote the ratio (P_I/P_S). Then, we can find the SINR and $\Delta\theta$ in different regimes as follows.

1) Interference Power Is Much Smaller Than the Signal Power: $P_I/P_S \ll 1$ ($\rho \ll 1$): When the interference power is relatively small, the error can be modeled the same as the phase noise effect. This is shown in Fig. 2(b). However, the exact effect of phase variation can be calculated by adding the variation as $\theta_n = \arcsin(P_I/P_S)$ to the phase shift

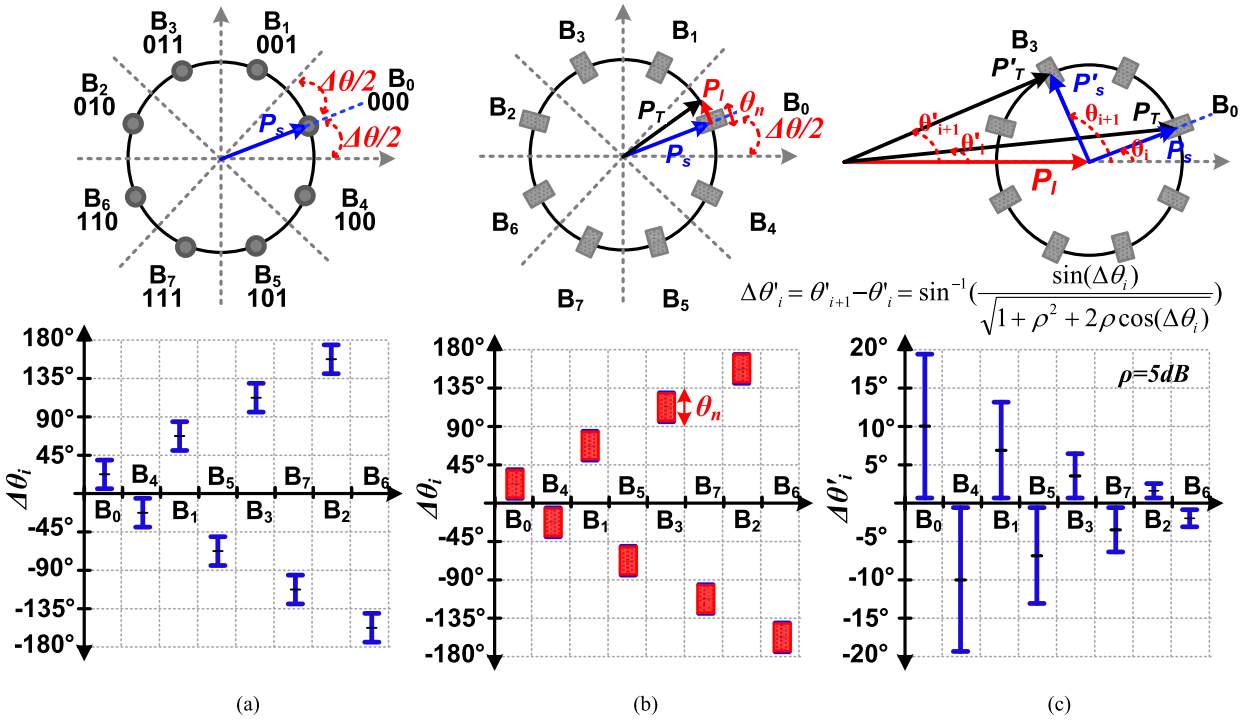


Fig. 2. Proposed joint interference-phase shift key modulation protocol for distributed secret key generation using physical wireless link. (a) No interference. (b) Interference power is small. (c) Interference power is comparable or larger with intended signal power.

term, $\Delta\theta$, in (1). For example, when the interference power is ten times smaller the signal power, i.e., $\rho = 0.1$, the phase noise variation is near 5°, which is negligible compared to the 45° phase shift for the conventional 8-PSK modulation.

2) Interference Power Is Comparable or Is Much Larger Than the Signal Power: $0.1 < P_I/P_S < 10$ ($0.1 < \rho < 10$) or $P_I/P_S > 10$ ($\rho > 10$): At the presence of a comparable interference power, for each pair of modulation symbols, e.g., θ_i and θ_{i+1}, with a phase shift of $\Delta\theta_i$, the resulting phase shift at Eve's, $\Delta\theta'_i$, will be always smaller than the 45° phase shift in a conventional setting [see Fig. 1(c)]. The new phase shift, $\Delta\theta'_i$, can be found using geometric computations. This is illustrated for the three vectors involved in the computation in Fig. 2(c). In particular, the power received at Eve's is denoted by P'_T and the interference power is P_I. Then, we have

$$\Delta\theta'_i = \theta'_{i+1} - \theta'_i = \sin^{-1}\left(\frac{\sin(\Delta\theta_i)}{\sqrt{1+\rho^2+2\rho\cos(\Delta\theta_i)}}\right). \quad (3)$$

The new phase shifts at the presence of interference for two consecutively indexed symbols from $i = 0$ to $i = M-1$, where $M = 8$ in 8-PSK, are shown for different values of the interference-to-power ratio ρ in Fig. 3. This demonstrates that for one change in the key bits, which changes one symbol to a neighboring symbol, e.g., B_i to B_{i+1}, the 45° phase shift, desired for 8-PSK, is reduced significantly when the interference power is increased. For example, the maximum worst case phase shift is near 5° for $\rho = 10$, which is equivalent to the approximated value derived from $\arcsin(P_I/P_s)$ as proposed in IMS2019 by Ebrahimi *et al.* [41]. However, here, we consider the exact values for the phase shift for different pairs of neighboring symbols, as shown in Fig. 2,

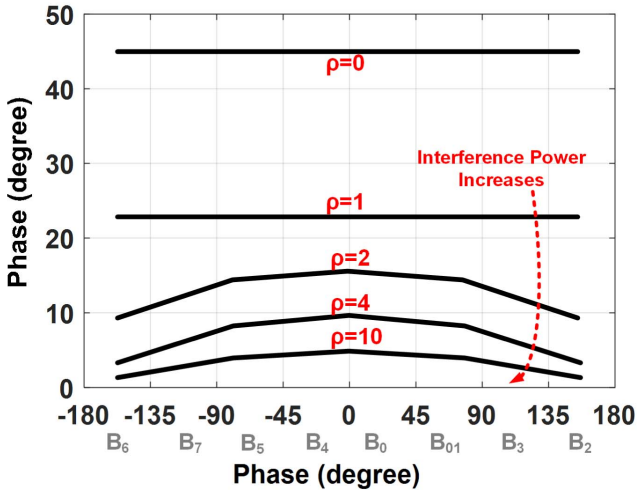


Fig. 3. Received phase shift at Eve's versus transmitted phase shift as secret key, B_0–B_7, from IoT under different interference-to-power ratio, ρ.

resulting in tight exact expressions for the security level of the key. Note also that with the new analysis presented in (3), the phase shift corresponding to each bit variation depends on the relative location and angles. For instance, when the interference and the signal symbol have the same phase, then the 180° phase shift with the next symbol results in the smallest phase shift variation to detect, which is actually 0. However, the SNR would be different, which is discussed later. In order to consider all the cases of phase variation in an average sense, the characterization of the resulting BER at Eve's receiver should take an average over the error rate of

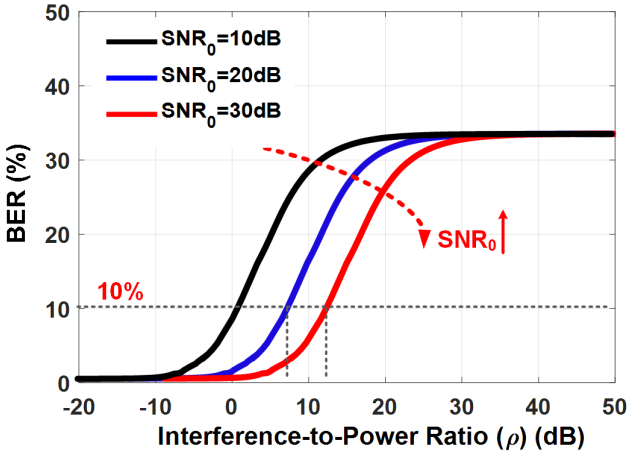


Fig. 4. Received BER at Eve's versus interference-to-power ratio, ρ, shown in (3), (4), and (5) for different reference signal-to-noise power ratio, and SNR_0, received at Eve (SNR_0 is pure IoT transmitted power received at Eve's with no interference power included).

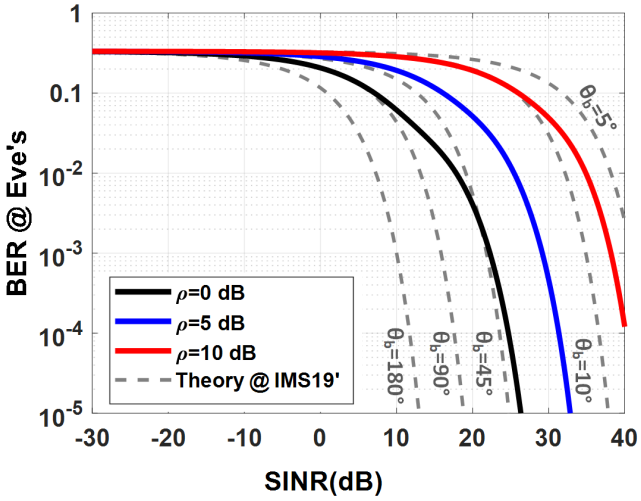


Fig. 5. Received BER at Eve's versus total signal to interference and noise power, SINR, under different interference-to-power ratio, ρ, and comparison with the simplified theory presented at IMS2019 [41] by authors (gray dotted plots).

every bit from B_0 to B_7, i.e., BER_i, for $i = 0$ to $i = M-1$ as

$$\text{BER} = \frac{1}{M}\sum_{i=0}^{M-1}\text{BER}_i = \frac{1}{M}\sum_{i=0}^{M-1}\frac{1}{k}\text{erfc}\left(\sqrt{k\times(\text{SNR}_i)}\sin\left(\frac{\Delta\theta_i'}{2}\right)\right) \quad (4)$$

where $\Delta\theta_i'$ is expressed in (3) and plotted in Fig. 3. Also, SNR_i in (4) is the signal-to-noise ratio associated with B_i that can be found through a geometric computation, as shown in Fig. 2(c). More specifically, it depends on the interference-to-power ratio, ρ, the initial phase shift of the symbol transmitted by the IoT node, $\Delta\theta_i$, that can be derived as

$$\text{SNR}_i = \frac{P_{s(i)}}{P_n} = \text{SNR}_0\sqrt{1+\rho^2+2\rho\cos(\Delta\theta_i)} \quad (5)$$

where SNR_0 is the pure P_s/P_n received at Eve from the IoT node when there is no interference. By plugging (5) and (3) into (4), one can plot the total BER variation versus interference-to-power ratio, ρ, for different values of SNR_0, as shown in Fig 4, and the BER versus SNR for different values of ρ, as shown in Fig. 5.

Based on observations in Fig. 4, for an interference-to-power ratio larger than 5 dB and a typical SNR_0 of 10 dB, the BER is larger than 10%, which is assumed to be the threshold for a detectable value. If the received SNR at Eve is increased, e.g., Eve uses larger antenna gains, and an optimistic value of 30-dB SNR is obtained by Eve, then the interference-to-power ratio of 10 dB is required to jam Eve's receiver. Note that, this is a very optimistic SNR, from Eve's perspective, that she could hope for with the currently available technology.

The total average BER versus the received SNR at Eve's, shown in Fig. 5 for different values of the interference-to-power ratio ρ, leads to a similar conclusion. The results shown for three different values for ρ, namely, 1, 5, and 10 dB, can be used to estimate the minimum required SNR and the interference-to-power ratio in order to jam Eve. Generally, as the interference-to-power ratio increases to 10 dB, an SNR larger than 30 dB is required to reach the 10% threshold for key detection. Also, this is increased proportionally as the interference power is increased. The theoretical bounds for the BER using the maximum phase bound presented in IMS2019 by Ebrahimi *et al.* [41] are also plotted in Fig. 5, by plugging (2) into (1), assuming different values of the interference-to-power ratio that determines the θ_b values. It is evident that the novel theoretical analysis provides a better bound, from the security perspective, for predicting BER at Eve compared to the simplified analytical expressions in IMS2019. For example, for $\rho = 1$ (0 dB), the new analytical result has an average value between the two extreme values for θ_b, which are 45° (equivalent to maximum phase bound value of $\rho = 1$) and 90°, showing that the BER has deteriorated more for smaller SNR values, which was not captured in the simplified equations. The main reason is that in the conventional PSK modulation in [41], described by (1) and (2), only the maximum phase variation is considered, i.e., $\arcsin(P_I/P_s)$. Note that the peak value shown in Fig. 3 is for the reference B_0. The new analytical result considers all the phase shift bound variations corresponding to all bit variations and the associated SNR, resulting in a more accurate bound.

Therefore, by using the proposed protocol, which utilizes simultaneous phase shift-keying modulation and sufficient interference power generated by the master, the secret keys are jammed at eavesdroppers, while they can be reliably demodulated at the master node using full-duplex communication techniques as will be described in Section II-B1.

B. Proposed Omnidirectional Full-Duplex Communications Versus Directional Communications

In a PLS setting, it is natural to assume that all the nodes in the network, both legitimate and adversary nodes, have access to the same radio with similar antenna architectures,

e.g., directional or omnidirectional antennas. In general, a directional antenna creates a narrow beam in a certain direction and nulls out the interference at sidelobes. This technology is often considered as a natural solution to provide PLS within a narrow beamwidth. However, directional communication suffers from a sidelobe leakage often larger than 10 dB.

In general, one can consider two scenarios in which directive antennas can be used in the PLS setting. The first one is that the IoT node uses directive antennas to transmit the secret key to the master node while canceling out the signal received by Eve. The second one is that Eve's receiver uses a narrow-beam directional array to cancel out the interference transmitted from the master node in our proposed setup. However, both of these scenarios will be suffered from the aforementioned sidelobe leakage issue. More specifically, in the second scenario, Eve's antenna still receives part of the interference in its sidelobe even though a directive antenna technology is employed. If the technology is significantly enhanced to resolve the sidelobe issue, then the IoT node can use it as well, as suggested in the first scenario. In general, regardless of which scenario is considered, significantly narrower beams and almost optimal sidelobe cancellation are required to provide the desired security to the directive communication.

Directional modulation, shown in Fig. 1(b), is a common technique to distort the signal at sidelobes; however, it requires an accurate knowledge of the adversary node's location, which is not feasible for distributed networks. In our protocol shown in Fig. 1(c), it is proposed to simultaneously transmit data and interference in order to jam Eve's receiver using omnidirectional antennas. Hence, this method is effective regardless of Eve's location. Even if Eve uses directive antennas to cancel out the interference transmitted from the master node while pointing out the antenna to the IoT node, it will still receive part of the interference through its sidelobes. Furthermore, accurate localizations and beam alignments to every IoT node in the network is required. Therefore, our proposed protocol provides a solution to overcome the conventional challenges of directive communications, including sidelobe leakage, accurate localization, and beam-alignment while also providing larger security regions (see Section IV).

In general, in a PLS setting, two major criteria of reliability and security need to be satisfied. In particular, in our proposed protocol, we aim at attaining the following goals.

1) *Reliability:* Master node extracts the secret key from the signal transmitted by the IoT node.
2) *Security Enhancement:* Jamming Eve's receiver.

1) Reliable Communication for Master Node Using Full-Duplex Communications: In this setup, the master node is the only intended node to reliably extract the secret key that the IoT node transmits. The reliability condition here is defined as having the condition BER $< 10^{-3}$ being satisfied as in a typical digital communication system. In order to have a reliable transmission of the secret key from the IoT node to the master node, the master node should cancel out the self-interference leakage, shown as β in Fig. 6, which is the dominating factor in characterizing the reliability of secret key.

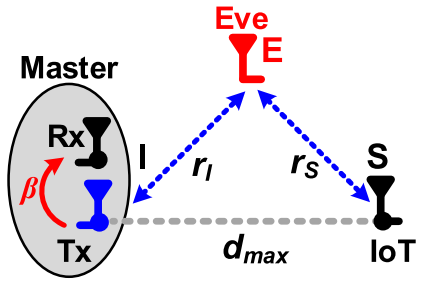


Fig. 6. Reliable communication links between IoT and master using full-duplex communications with self-interference cancellation of β.

To this end, the master node will use technologies developed for full-duplex communication protocols.

It can be observed in Fig. 5 that in order to have reliability, i.e., BER $< 10^{-3}$, in the PSK modulation with maximum phase bound of 90° or 180° for modulation symbols, an average 15-dB SINR is required. Since the self-interference power is typically much larger than the noise power, the SINR can be simplified as signal-to-interference power ratio, SIR, as follows:

$$\mathrm{SIR}_{\mathrm{master}} = \frac{\gamma_{\mathrm{IS}} P_S}{\beta\, P_I} \tag{6}$$

where P_S is the transmitted power by the IoT node, denoted by **S** in Fig. 6, P_I is the transmitted interference power from the master node denoted by I in Fig. 6, an undesired self-interference leaked back to the master's receiver is denoted by a ratio β, and γ_{IS} is the channel gain between the master node and the IoT node as follows:

$$\gamma_{\mathrm{IS}} = \left(\frac{\lambda}{4\pi\, d_{\max}}\right)^2 G_s G_I \tag{7}$$

where λ is the wavelength and G_s and G_I are the IoT and the master antenna gains, respectively. Also, $d_{\max}$ is the maximum reliable communication link, which can be calculated as being near two meters for an SIR of 15 dB, P_I/P_S of 10 dB, and the self-interference cancellation being between 50 and 60 dB. By advancing the full-duplex communication and enhancing self-interference cancellation up to 100 dB, [42]–[47], the communication range can be increased. However, the short range of a few meters is sufficient for indoor IoT sensor networks, such as patients' sensors at hospitals or RFID tags in stores.

The modulation bandwidth of the proposed protocol is limited by the integrated noise power over the BW, the interference power, and other source of errors that can be modeled as amplitude and phase errors or noise. This includes LO phase noise, mismatch between paths, and phase and group delay. The proposed protocol is implemented using discrete components, which introduces larger group delay between the components, resulting in data rate of tens of b/s. However, it should be highlighted that the security of the shared key, to be used for encryption and decryption, for the main intended high-speed communications between sensor nodes in the network is the most important factor of the protocol and is also the focus of our work. The achieved speed of tens of b/s for the key/data rate means that the key can be

updated every few seconds, depending on the length of the key which is in the order of few tens. This is sufficient for current applications. Note that a higher speed of secret key generation can also be achieved by using integrated circuits with high-speed calibration circuitry.

2) Security Enhancement: Jamming Eve's Receiver: In order to find the security region, where Eve's signal is considered to be jammed, we characterize the SINR region where it is larger than a certain threshold $\text{SINR}_{\min}$

$$\text{SINR}_{\text{Eve}} = \frac{P_S\,\gamma_{\text{SE}}}{P_I\,\gamma_{\text{IE}}} = \frac{P_S\,G_S}{P_I\,G_I}\frac{r_I^2}{r_S^2} \tag{8}$$

where γ_{SE} and γ_{IE} are the channel gains between Eve and the IoT and the master nodes, respectively. Also, r_I/r_S is the ratio of Eve's distance to the master node (interference source) and the IoT node (desired data source), as shown in Fig. 6. The eavesdropping region, defined as Eve having BER $< 10^{-1}$, is approximated when SINR_{Eve} from (8) is larger than the minimum required $\text{SINR}_{\min}$ expressed in Fig. 5 and analyzed in (4) and (5)

$$\text{SINR}_{\text{Eve}} \geq \text{SIR}_{\min} \overset{(8)}{\longleftrightarrow} \frac{r_I}{r_S} \geq \sqrt{\frac{P_S\,G_S}{P_I\,G_I}\text{SIR}_{\min}}. \tag{9}$$

The geometrical representation of (9) is a circle centered at C_E and with radius R_E while considering the IoT data source node as the reference of the coordinate system, as shown in Fig. 7(a)

$$R_E = \left|\frac{\alpha_r}{\alpha_r^2 - 1}\right| d, \quad C_E = \left|\frac{1}{\alpha_r^2 - 1}\right| d \tag{10.a}$$

$$\alpha_r = \sqrt{(P_I G_I / P_S G_S)\text{SIR}_{\min}} \tag{10.b}$$

where d can reach up to the maximum communication distance, $d_{\max}$, as expressed in (7). The key is not secure to the nodes inside this circle, called the eavesdropping region, with SIR larger than $\text{SIR}_{\min}$ corresponding to the BER of 10^{-1}, while the protocol provides sufficient security outside of this region, called the security region. Note that a larger ratio of P_I/P_S will reduce the circle radius and, consequently, will enhance the security region.

In order to consider both the conditions for reliability and security in our comparison, we compute the integrated area for both the reliability and the security regions. Let S_{Eve} denote the eavesdropping region, where we have BER $< 10^{-1}$ for Eve node in this region. Similarly, the reliable communication region S_{Comm} is the region of all locations for the intended receiver with BER $< 10^{-3}$. Then, the security factor SF is defined as the ratio of areas of these two regions as follows:

$$\text{SF} = \frac{S_{\text{Eve}}\left(\text{BER} < 10^{-1}\right)}{S_{\text{Comm}}\left(\text{BER} < 10^{-3}\right)}. \tag{11}$$

The security factor SF can be used for a fair comparison between different PLS techniques. More specifically, given a protocol, a smaller value of SF indicates a higher level of security, in terms of the covered area. Note that the security factor for our proposed technique can be found by using (6), (7), and (9) as follows:

$$\text{SF}_{\text{prop}} = \left|\frac{\alpha_r}{1-\alpha_r^2}\right|^2 \approx \frac{1}{\alpha_r^2} = \frac{1}{\text{SIR}_{\min}}\frac{P_S G_S}{P_I G_I}. \tag{12}$$

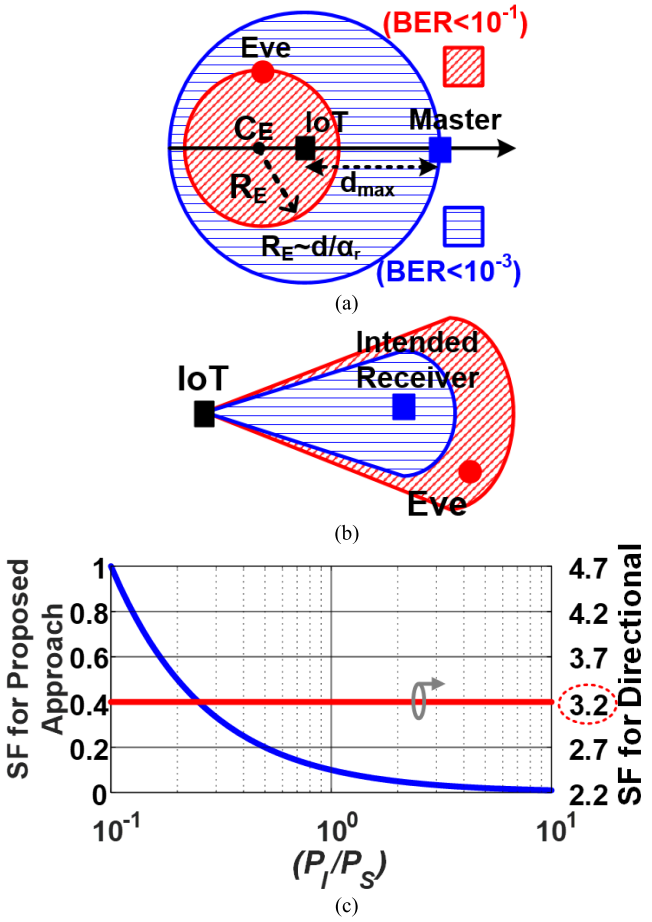


Fig. 7. Reliability and security comparison. (a) Proposed approach. (b) Directional antenna. (c) Security enhancement factor, SF, and comparison.

The proposed SF metric is plotted in Fig. 7(c) versus P_I/P_S. As it is illustrated, the security factor of our proposed approach is smaller than 1 under the simultaneous interference-data transmission condition where $(P_I/P_S \gg 1)$. As the interference power is increased, then the SF is enhanced, which means that the security is enhanced.

Next, we compute the areas of eavesdropping region for directional communication. In the directional antenna approach, the area of region can be expressed as $(\theta_d/2)r^2$, where r is the maximum distance of Eve from the IoT node given a specific probability of error and θ_d is the directivity angle of the IoT antenna node, as shown in Fig. 7(b). As shown in Fig. 5, the typical constraints (BER $< 10^{-1}$) and (BER $< 10^{-3}$) correspond to $\text{SNR}_{\min}$ of 10 and 15 dB, respectively. Therefore, the maximum distance for the directive communication is shown in the following equation:

$$r_{\max} = \sqrt{\left(\frac{\lambda}{4\pi}\right)^2 \frac{G_S(\theta)\,G_r}{\text{SNR}_{\min}}\frac{P_S}{P_N}} \tag{13}$$

where λ is the wavelength, P_n is the integrated noise power at the receiver, G_r is the receiver's antenna gain, assuming an omniantenna for Eve, and $G_s(\theta)$ is the antenna directive gain.

Assuming that both intended receiver and Eve have the same G_r and P_n, for communication and the eavesdropping area, the SF ratio of the directional antenna technique can be

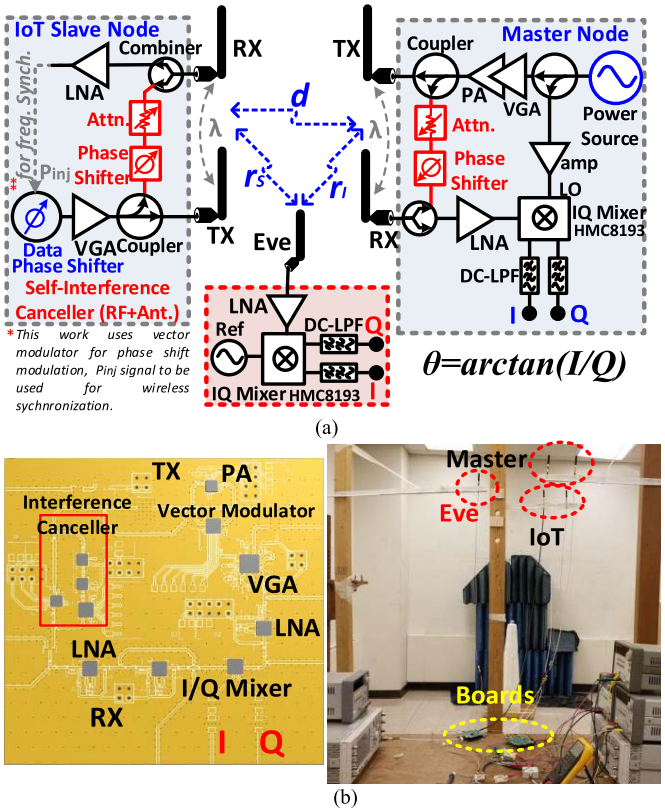


Fig. 8. System implementation for the proposed protocol. (a) Proposed block diagram for master, IoT, and Eve. (b) Implemented layout of the block that can be shared and used by IoT, Eve, and master with the measurement setup.

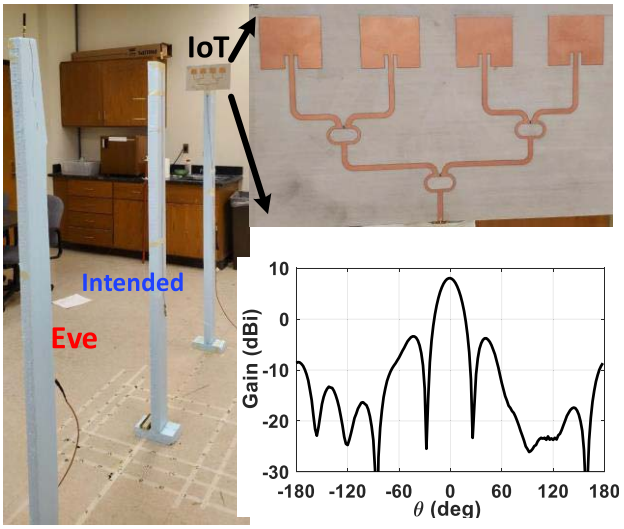


Fig. 9. Directional antenna array measurement setup with four-element patch antenna array with 8-dB gain at the main lobe and −3-dB gain at sidelobe.

formulated in terms of the SNR as follows:

$$\mathrm{SF}_{\mathrm{direc}} = \frac{\mathrm{SNR}_{\min}\left(\mathrm{BER} = 10^{-3}\right)}{\mathrm{SNR}_{\min}\left(\mathrm{BER} = 10^{-1}\right)} > 1. \tag{14}$$

Therefore, for the directional antenna scheme, the eavesdropping region is always larger than the reliable communication region, which is shown in Fig. 7(c) for both directional array and our proposed protocol. It can be observed that our proposed approach is significantly more secure comparing to the directional approach as the eavesdropping region is always smaller than the reliable communication region.

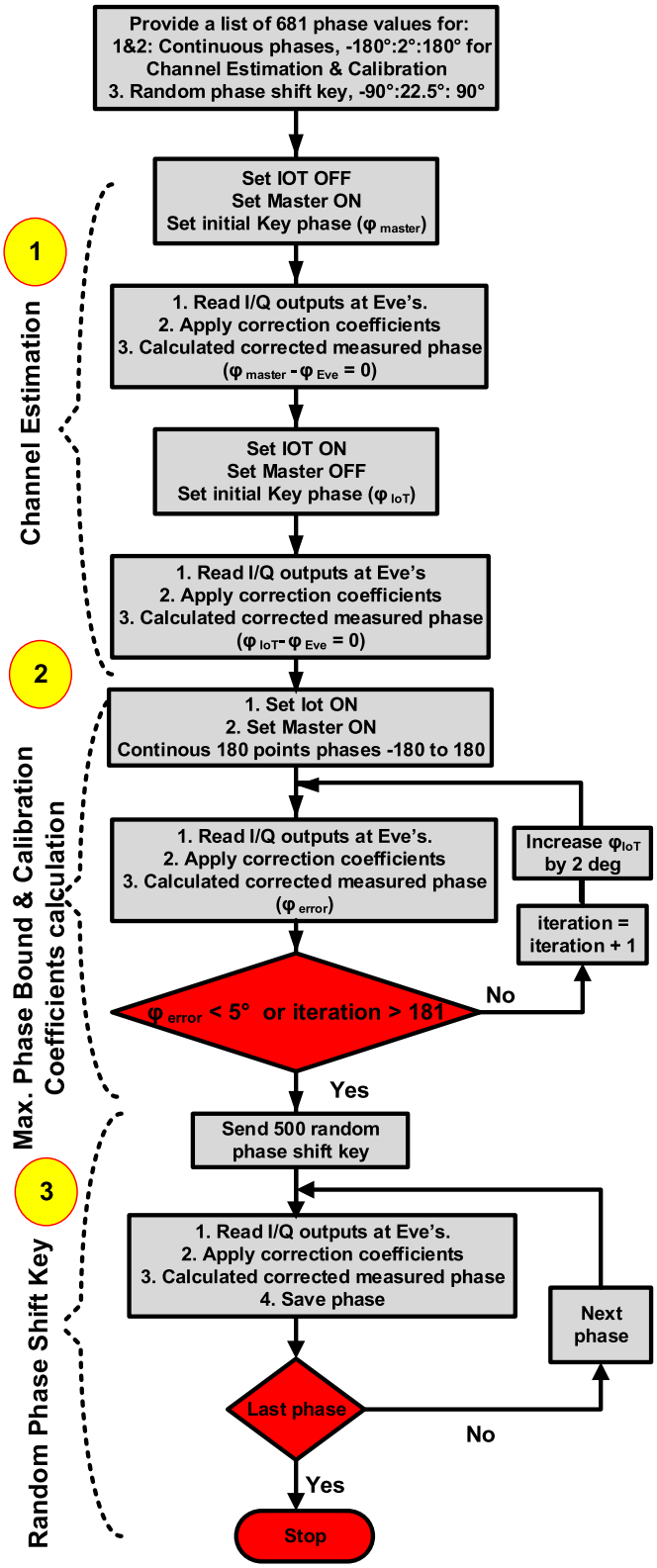


Fig. 10. Embedded algorithms flowchart for the system with initial channel estimation, calibration, and bit-error-rate measurement.

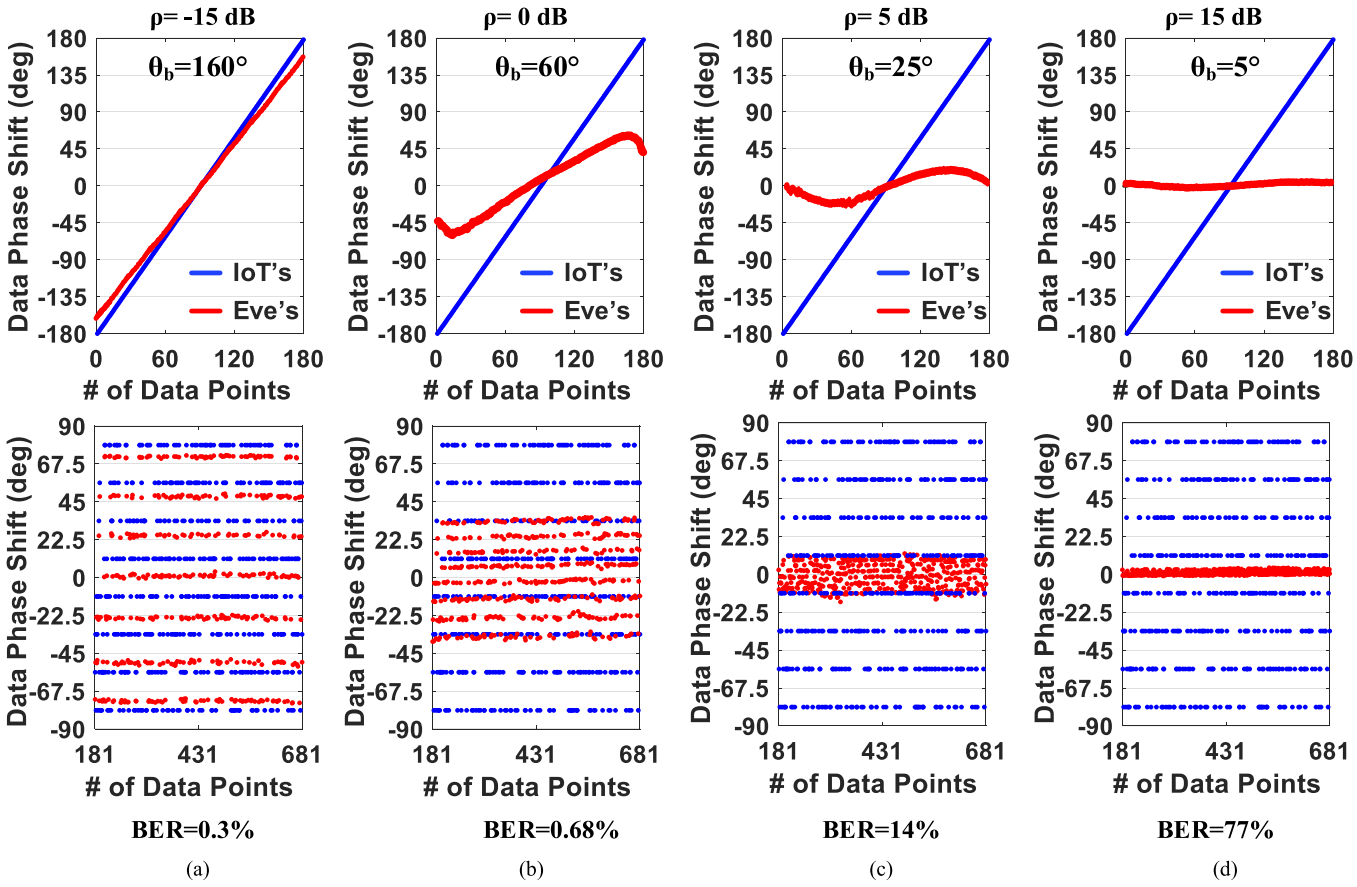


Fig. 11. Measured received results at Eve's for different interference-to-power (ρ) ratio of (a) $\rho = -15$, (b) 0, (c) 5, and (d) 15 dB. Top figures: for 180 continuous phase shift states from $-180°$ to 180° for maximum phase shift measurement. Bottom figures: for BER measurements with 500 random phase shifts between-90° to 90° [−78.75, −56.25, −37.75, −11.25, 11.25, 33.75, 56.25, 78.75].

III. Embedded System Implementation

The block diagram of the proposed system operating at 2.4 GHz is shown in Fig. 8(a). For the full-duplex implementation, two identical omnidirectional antennas, with distance λ apart, are deployed for both Tx and Rx. A vector modulator (HMC631) is used as phase shifter and attenuator for RF self-interference cancellation on both ends, providing more than 50-dB rejection.

In order to have a variable interference-to-power ratio (ρ) between the master and the slave, a variable gain amplifier (VGA: ADL5246) is deployed. The maximum output power by the transmitter at the master node varies between −10 and 10 dBm, while it varies at a lower level, between −10 and 0 dBm, at the slave/IoT side. For the Rx path, the master node uses an LNA (PMA-33GLN+) to further amplify the received data and to drive the IQ mixer (HMC8193). The reference LO port of the IQ mixer is also driven by a coupled power of master source. Using a dc low-pass filter (LPF) (LFCN-160+), the modulated code phase shift can be extracted as $\arctan(I/Q)$. The passive eavesdropper also employs the same IQ mixer with a separate LO reference to extract the phase-modulated key.

In order to randomly generate the key, a continuous and random phase shift is generated at the IoT node. A vector modulator (HMC631) is used to generate a continuous 360° phase shift with the variable insertion loss (−51∼−11 dB). An injection-locked oscillator is an alternative candidate for the proposed system to generate the continuous phase shift, which also enables locking and synchronizing the frequency to the master source. In that case, an LNA can be inserted at the IoT node to amplify the received power from the master source by the injection-locked oscillator for frequency synchronization [49]–[52]. This would also serve as the random phase modulator. This could be an interesting future direction for this work, which relates to the wireless coupled oscillator techniques that have been previously proposed to use for wireless synchronization [49]–[52].

The board is fabricated on FR4 and its layout is shown in Fig. 8(b), which has 8 × 8 cm size. The measurement setup is also shown in Fig. 8(b), with IoT, master, and Eve's antenna placement being a few meters above the ground to minimize the interference in the channel reflected from surfaces. The measurement setup for the directional antenna approach is also shown in Fig. 9 with the four-element patch antenna array used for IoT nodes. The directional antenna has 8-dB gain at the main lobe and −3-dB gain at the sidelobe, as shown in Fig. 9. The system is fully embedded and controlled with algorithms shown in Fig. 10 using the Labview platform. The vector modulator generates 680 phase states, with the first 180 phases being from-180° to 180° with 2° phase step in

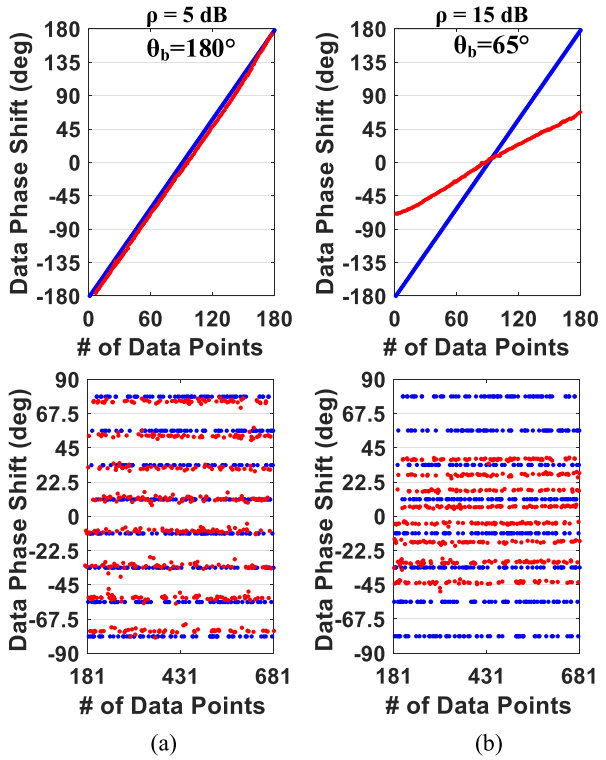


Fig. 12. Measured received results at intended master's receiver for different interference-to-power (ρ) ratio of a) $\rho = 5$ dB and b) 15 dB. Top figures: for 180 continuous phase shift states from $-180°$ to $180°$. Bottom figures: for BER measurements with 500 random phase shifts between $-90°$ to $90°$.

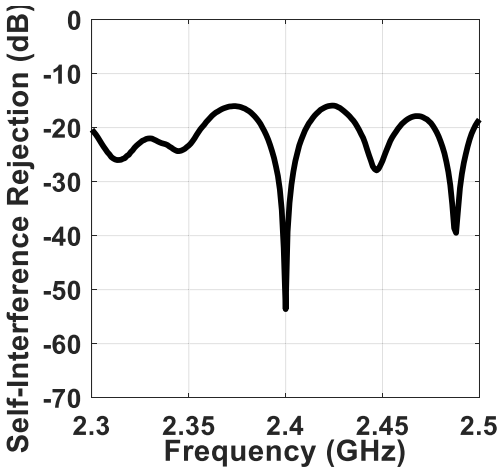


Fig. 13. Measured self-interference rejection at master node.

the continuous format to first measure the maximum phase shift bound, θ_b, and then to calibrate the channel nonidealities between Eve's and the IoT as well as between Eve's and the master. The calibration is done to eliminate the other interference and multipath effect and to only consider the intentional interference effect transmitted by the master in our proposed protocol. The next 500 phase states are transmitted randomly to measure the BER of the system.

At the first calibration state, the IoT is OFF, while the master is ON and sending the phase data to Eve that can be used to calibrate the channel's nonidealities. Then, the

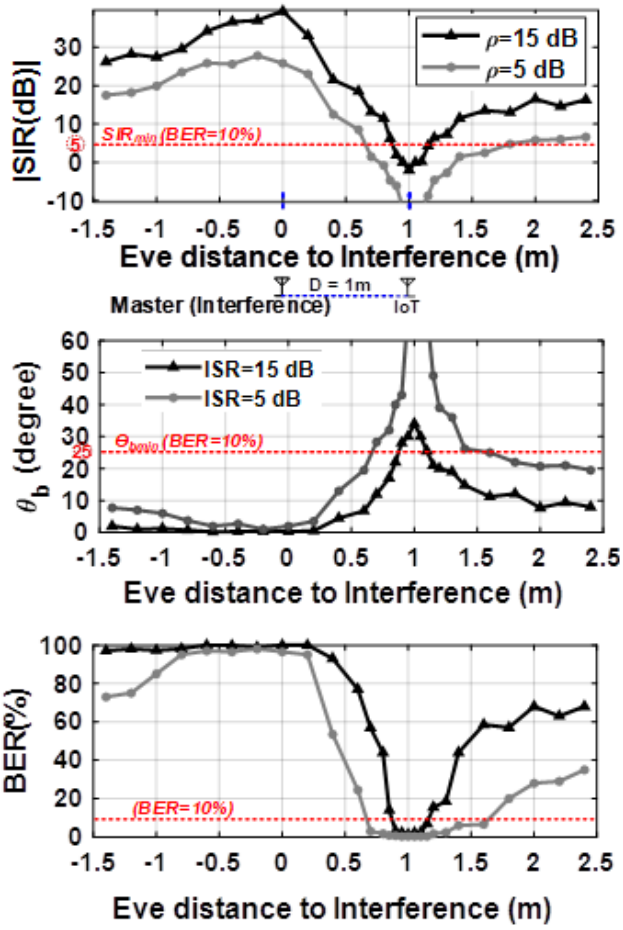


Fig. 14. Measurement results at Eve's at different distances to interference power (master) which is located at 0-point with IoT at distance of 1 m under two interference-to-power (ρ) ratio and 15 dB. (a) signal-to-interference ratio (SIR). (b) Maximum phase shift, θ_b. c) bit-error rate (BER) (%).

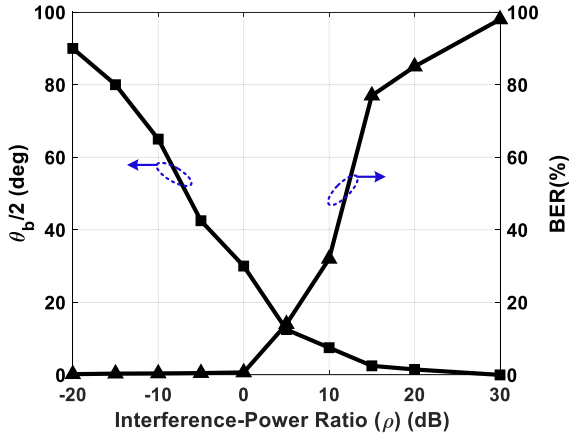


Fig. 15. Measured maximum phase shift, θ_b, and BER measurement versus interference-to-power (ρ) ratio.

IoT turns ON, while the master is OFF to compensate and calibrate the channel between the IoT and Eve's. After that, the first continuous 180 round of phase shift from $-180°$ to $180°$ is transmitted, while both the IoT and the master are ON. The received data by both Eve and the master are plotted in the top figures of Figs. 11 and 12, respectively. The continuous

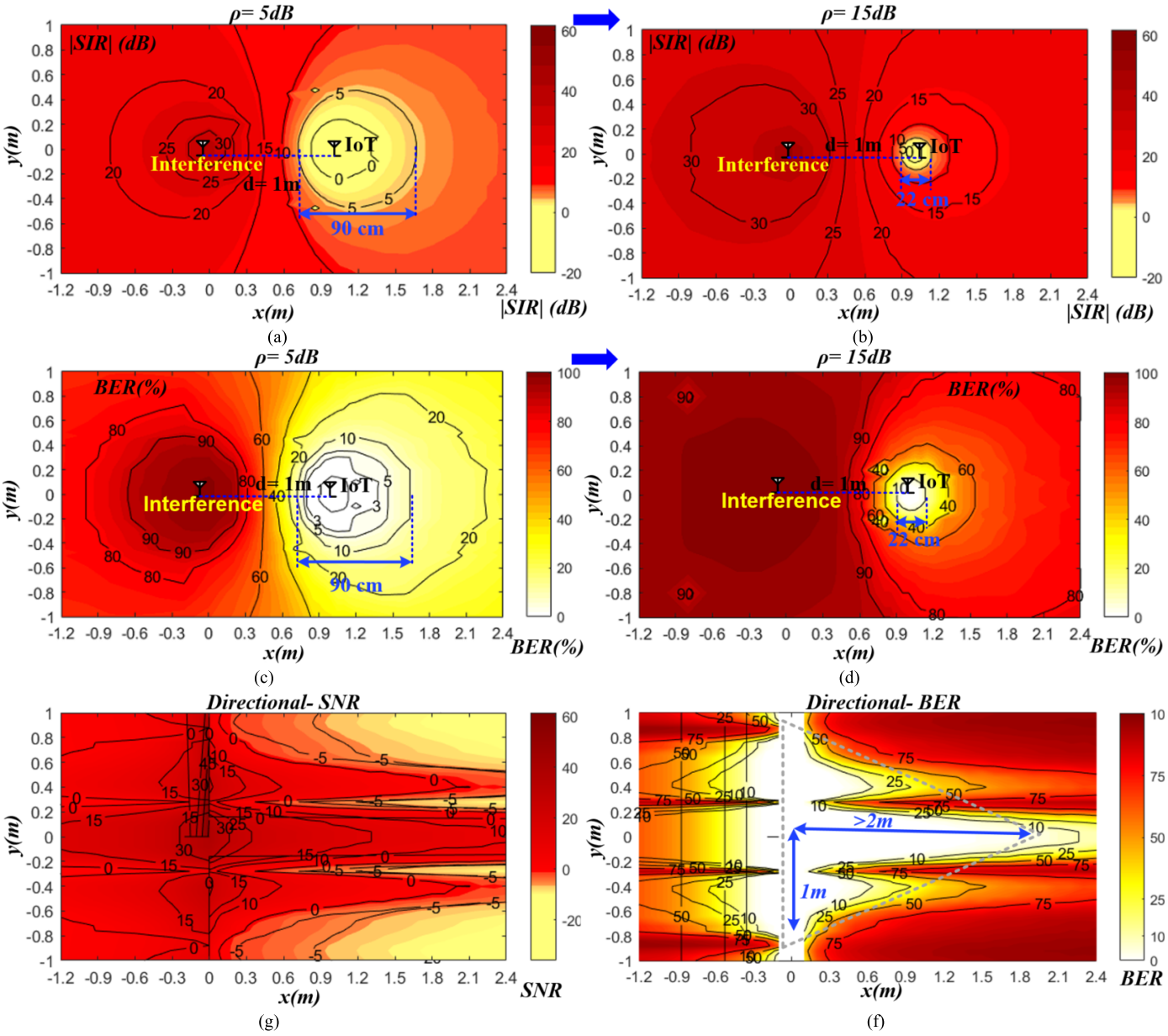


Fig. 16. Measured results and comparison between proposed protocol and directional antenna technique with Eve's at different location at *xy*-axis, x (-1.2 to 2.4 m) and y (-1 to 1 m) with master at 0 point and IoT at (1.0) point ($d = 1$ m). (a) Signal-to-interference ratio (SIR) at Eve's for interference-to-power ratio (ρ) of 5 dB. (b) SIR for ρ of 15 dB. (c) BER at Eve's for ρ of 5 dB. (d) BER at Eve's for ρ of 15 dB for the proposed protocol. (g) Received SNR at Eve's for IoT using directional antenna communication. (h) Received BER at Eve's for IoT using a directional antenna.

phase shift measurement indicates the maximum phase shift, θ_b, with a phase wrapping error that occurred around 90°. This phase wrapping is generated from our circuit as it calculates the phase shift from $\arctan(I/Q)$ equation. Therefore, to send a random phase key, the 500 random phases are randomly selected between $-90°$ and 90°.

IV. Measurement Results

The measurement results for Eve's receiver in our proposed protocol with four different values for the master power to IoT power ratio (ρ) of -15, 0, 5, and 15 dB are plotted in Fig. 11. In this scenario, Eve's receiver is placed exactly in the middle between the IoT and the master nodes ($d/2$). The top figure shows the results for the 180 continuous phase shifts, which shows that for the interference-to-power ratio larger than 5 dB, the maximum phase shift is reduced to 25°. This phase shift is approximately close to the predicted $\arctan(P_I/P_S)$ in Section II and [41]. The BER obtained from transmitting the 500 random phases are also measured under these conditions, showing that the BER is larger than 10% for the interference-to-power larger than 5 dB.

The received data at the master node are also measured with the self-interference rejection around 40– 60 dB, shown in Fig. 13, and, consequently, with the maximum communication link around 1–2 m. The utilized canceller is a vector modulator (HM631) acting as VGA and phase shifter, shown in Fig. 8,

to cancel the self-interference leakage. The vector modulator provides continuous 360° phase shift and continuous 40-dB gain control, which were measured separately via network analyzer. Each gain and phase shift state is calculated separately and then applied to the canceller path in order to achieve the 50-dB interference cancellation at the targeted frequency. The received maximum phase shift and BER at the master's under the interference-to-power ratio of 5 and 15 dB are shown in Fig. 12. Under larger interference power of 15 dB, the phase shift is reduced to 65° corresponding to BER of 0.3%. As it is predicted, a larger ratio of ρ will cause self-jamming at the master's receiver and avoiding the reliable detection of the key. Therefore, within the 1–2 m of communication distance, the maximum master to IoT power ratio, ρ, should be between 10 and 20 dB (around 15 dB).

Furthermore, in order to measure the security and the eavesdropping regions and to evaluate the derived eavesdropping radius calculated in Section II-B, we measured Eve's performance at different relative distances toward the IoT and the master node at X-axis with the IoT and the master separated by a distance, $d = 1$ m. The measured received signal-to-interference power ratio (SIR) at Eve's at different distances under two different values for master to IoT power ratio (ρ) of 5 and 15 dB is plotted in Fig. 14(a). As it is illustrated, at far-field distance ($r > d$) the SIR at Eve's merges to the master to IoT power ratio, (ρ), e.g., 5 or 15 dB. The measured maximum phase shift, θ_b, is also shown in Fig. 14. (b), being reduced as ρ and relative SIR are increased. The BER is also shown in Fig. 14(c), indicating that for $\theta_{b-\min}$ smaller than 25°, the BER is larger than 10%. The eavesdropping radius can be calculated from these measurements shown in Fig 14. The eavesdropping radius, R_E, is reduced from R_E of 11 cm for $\rho = 15$ dB to R_E of near 50 cm for $\rho = 5$ dB. These calculated values match perfectly with the derived equation in 10 (a). The BER and θ_b for different interference-to-power ratios, ρ, from-20 to 30 dB, are also measured and shown in Fig. 15. It confirms the other test set-up that for ρ larger than 5 dB, θ_b and BER fall in the undetected region.

In order to compare the security enhancement factor with directional antenna array communication, the measurement is performed at different X and Y locations for Eve's relative distance to the IoT and the master separated by 1 m. The relative signal-to-interference ratio SIR and BER for two different values of master to IoT power, ρ, of 5 and 15 dB are plotted in Fig. 16 (a)–(d). The measurement results confirm the analyzed eavesdropping region derived in Section II-B, 10(a) and (b), for the proposed protocol, which is a circle around IoT with the radius R_E depending on the square root of master to IoT power, $(P_I/P_S)^{1/2}$. Increasing the interference-to-power ratio by l0 dB reduces the eavesdropping region radius by approximately three times, from 45 to 11 cm.

The measurement results for the directional antenna scenario, with setup shown in Fig. 9, are also shown in Fig. 16(g) and (f). With antenna gain around 8 dB and the minimum sensitivity of −60 dBm for Eve's receiver, the measured reliable link is 2.5 m. The minimum detectable SNR and BER are shown in Fig. 16. The minimum detectable SNR for the eavesdropping region, BER $< 10\%$, and the communication region, BER $< 0.1\%$, differs by 3 dB and the area of eavesdropping region is always larger than that of the communication region. In other words, there is always an information leakage at any angle and distance for directive communication. However, in our proposed protocol, the security enhancement factor improves significantly by making the eavesdropping region always smaller than the communication region, SF < 1.

V. Conclusion

This work presents a novel technique for PLS in the IoT distributed networks using joint interference and phase shift key modulation. Each IoT node generates a phase shift key modulated data as a secret key and transmits it to a master node as an intended node in the presence of an eavesdropper Eve. The master node, simultaneously, broadcasts a high-power signal using the omnidirectional antenna, which is received as interference by Eve and results in a higher BER at its receiver. In particular, we show, using theoretical and measurement results, that our proposed approach provides significantly better security measures, in terms of the BER at Eve's location compared to a conventional directive communication protocol without requiring localization or accurate beam alignment. It is shown that in our novel system, the possible eavesdropping region, BER $< 10^{-1}$, is always smaller than the reliable communication region, BER $< 10^{-3}$. Furthermore, for intended reliable communication between the two legitimate intended nodes, the master, and the IoTs, a full-duplex technology is employed to subtract the transmitted signals at each node, as a known reference, from the received signal (self-interference cancellation) and to extract the data, i.e., secret key for master.

References

[1] F. Foukalas, V. Gazis, and N. Alonistioti, "Cross-layer design proposals for wireless mobile networks: A survey and taxonomy," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 1, pp. 70–85, 1st Quart., 2008, doi: 10.1109/COMST.2008.4483671.

[2] R. Jurdak, C. V. Lopes, and P. Baldi, "A survey, classification and comparative analysis of medium access control protocols for ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 6, no. 1, pp. 2–16, 1st Quart., 2004.

[3] M. Takai, J. Martin, and R. Bagrodia, "Effects of wireless physical layer modeling in mobile ad hoc networks," in *Proc. 2nd ACM Int. Symp. Mobile Netw. Comput.*, New York, NY, USA, 2001, pp. 87–94.

[4] C. Saradhi and S. Subramaniam, "Physical layer impairment aware routing (PLIAR) in WDM optical networks: Issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 109–130, 4th Quart., 2009.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014, doi: 10.1109/SURV.2014.012314.00178.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016, doi: 10.1109/JPROC.2016.2558521.

[7] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, Jan. 2020, doi: 10.1109/TIFS.2020.2974621.

[8] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011, doi: 10.1109/MWC.2011.5751298.

[9] N. Aldaghri and H. Mahdavifar, "Fast secret key generation in static environments using induced randomness," in *Proc. IEEE Global Commun. Conf.*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–6, doi: 10.1109/GLOCOM.2018.8647945.

[10] K. Yang, D. Blaauw, and D. Sylvester, "Hardware designs for security in Ultra-Low-Power IoT systems: An overview and survey," *IEEE Micro*, vol. 37, no. 6, pp. 72–89, Nov. 2017, doi: 10.1109/MM.2017.4241357.

[11] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988, doi: 10.1109/5.4440.

[12] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, 1998, doi: 10.1109/2.708447.

[13] G. Kapoor and S. Piramuthu, "Vulnerabilities in some recently proposed RFID ownership transfer protocols," in *Proc. 1st Int. Conf. Netw. Commun.*, Chennai, India, 2009, pp. 354–357, doi: 10.1109/NetCoM.2009.90.

[14] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proc. IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012, doi: 10.1109/JPROC.2012.2188769.

[15] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2008.

[16] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Norwell, MA, USA: Springer, 2009.

[17] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st. ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[18] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

[19] E. A. Jorswieck, A. Wolf, and S. Gerbracht, *Secrecy on the Physical Layer in Wireless Networks, Trends in Telecommunications Technologies*. 2010, pp. 413–435. [Online]. Available: http://www.intechopen.com/books/trends-in-telecommunications-technologies/secrecy-on-thephysical-layer-in-wireless-networks

[20] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Trans. Amer. Inst. Electr. Eng.*, vol. 14, pp. 295–301, Jan. 1926, doi: 10.1109/T-AIEE.1926.5061224.

[21] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[22] P. R. Geffe, "Secrecy systems approximating perfect and ideal secrecy," *Proc. IEEE*, vol. 53, no. 9, pp. 1229–1230, Sep. 1965, doi: 10.1109/PROC.1965.4175.

[23] M. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 3, pp. 289–294, May 1977, doi: 10.1109/TIT.1977.1055709.

[24] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[25] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Aug. 2013, Art. no. 760834.

[26] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417–1420, 2011, doi: 10.1109/LAWP.2011.2178384.

[27] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009, doi: 10.1109/TAP.2009.2027047.

[28] W. Kummer, A. Villeneuve, T. Fong, and F. Terrio, "Ultra-low sidelobes from time-modulated arrays," *IEEE Trans. Antennas Propag.*, vol. AP-11, no. 6, pp. 633–639, Nov. 1963, doi: 10.1109/TAP.1963.1138102.

[29] B. Lewis and J. Evins, "A new technique for reducing radar response to signals entering antenna sidelobes," *IEEE Trans. Antennas Propag.*, vol. AP-31, no. 6, pp. 993–996, Nov. 1983.

[30] S. Yang, Y.-B. Gan, and P. Khiang Tan, "Linear antenna arrays with bidirectional phase center motion," *IEEE Trans. Antennas Propag.*, vol. 53, no. 5, pp. 1829–1835, May 2005.

[31] S. Yang, Y. B. Gan, and T. P. Khiang, "A new technique for power-pattern synthesis in time-modulated linear arrays," *IEEE Antennas Wireless Propag. Lett.*, vol. 2, pp. 285–287, Sep. 2003, doi: 10.1109/LAWP.2003.821556.

[32] S. Yang, Ye, A. Qing, and P. Khiang Tan, "Design of a uniform amplitude time modulated linear array with optimized time sequences," *IEEE Trans. Antennas Propag.*, vol. 53, no. 7, pp. 2337–2339, Jul. 2005.

[33] S. D. Keller, W. D. Palmer, and W. T. Joines, "Electromagnetic modeling and simulation of a directly-modulated L-band microstrip patch antenna," in *Proc. IEEE Antennas Propag. Soc. Int. Symp.*, Honolulu, HI, USA, Jun. 2007, pp. 4489–4492, doi: 10.1109/APS.2007.4396540.

[34] E. J. Baghdady, "Directional signal modulation by means of switched spaced antennas," in *IEEE Trans. Commun.*, vol. 38, no. 4, pp. 399–403, Apr. 1990, doi: 10.1109/26.52647.

[35] C. M. Elam and D. A. Leavy, "Secure communication using array transmitter," U.S. Patent 6275679, Aug. 14, 2001.

[36] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2008, pp. 188–605, doi: 10.1109/ISSCC.2008.4523120.

[37] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008, doi: 10.1109/JSSC.2008.2004864.

[38] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018, doi: 10.1038/s41586-018-0609-x.

[39] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[40] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[41] N. Ebrahimi, B. Yektakhah, K. Sarabandi, H. S. Kim, D. Wentzloff, and D. Blaauw, "A novel physical layer security technique using master-slave full duplex communication," *IEEE MTT-S Int. Microw. Symp. Dig.*, Boston, MA, USA, Jun. 2019, pp. 1096–1099, doi: 10.1109/MWSYM.2019.8700776.

[42] A. Hamza, C. Hill, H. AlShammary, and J. Buckwalter, "High-rejection RF code domain receivers for simultaneous transmit and receive applications," *IEEE J. Solid-State Circuits*, vol. 55, no. 7, pp. 1909–1921, Jul. 2020, doi: 10.1109/JSSC.2020.2970718.

[43] N. Reiskarimian *et al.*, "One-way ramp to a two-way highway: Integrated magnetic-free nonreciprocal antenna interfaces for full-duplex wireless," *IEEE Microw. Mag.*, vol. 20, no. 2, pp. 56–75, Feb. 2019, doi: 10.1109/MMM.2018.2880497.

[44] S. Jain, A. Agrawal, M. Johnson, and A. Natarajan, "A 0.55-to-0.9 GHz 2.7 dB NF full-duplex hybrid-coupler circulator with 56 MHz 40 dB TX SI suppression," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2018, pp. 400–401.

[45] T. Chen, J. Diakonikolas, J. Ghaderi, and G. Zussman, "Hybrid scheduling in heterogeneous Half-and full-duplex wireless networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 764–777, Apr. 2020, doi: 10.1109/TNET.2020.2973371.

[46] J. Zhou, T.-H. Chuang, T. Dinc, and H. Krishnaswamy, "Integrated wideband RF self-interference cancellation for FDD and full-duplex wireless," *IEEE J. Solid-State Circuits*, vol. 50, no. 12, pp. 3015–3031, Dec. 2015.

[47] K. E. Kolodziej, B. T. Perry, and J. S. Herd, "In-band full-duplex technology: Techniques and systems survey," *IEEE Trans. Microw. Theory Techn.*, vol. 67, no. 7, pp. 3025–3041, Jul. 2019.

[48] J. Tamminen *et al.*, "Digitally-controlled RF self-interference canceller for full-duplex radios," in *Proc. 24th Eur. Signal Process. Conf. (EUSIPCO)*, Budapest, Hungary, Aug. 2016, pp. 783–787.

[49] X. Y. Wang, R. K. Dokania, and A. Apsel, "PCO-based synchronization for cognitive duty-cycled impulse radio sensor networks," *IEEE Sensors J.*, vol. 11, no. 3, pp. 555–564, Mar. 2011, doi: 10.1109/JSEN.2010.2051326.

[50] N. Ebrahimi and J. F. Buckwalter, "A high-fractional-bandwidth, millimeter-wave bidirectional image-selection architecture with narrowband LO tuning requirements," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2164–2176, Aug. 2018, doi: 10.1109/JSSC.2018.2828855.

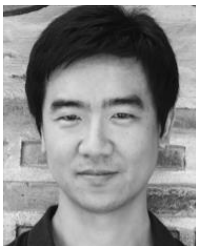
[51] N. Ebrahimi, H. Mahdavifar, and E. Afshari, "A novel approach to secure communication in physical layer via coupled dynamical systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–7.

[52] N. Ebrahimi, M. Bagheri, P.-Y. Wu, and J. F. Buckwalter, "An E-band, scalable 2×2 phased-array transceiver using high isolation injection locked oscillators in 90nm SiGe BiCMOS," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, San Francisco, CA, USA, May 2016, pp. 178–189.

Najme Ebrahimi (Member, IEEE) received the B.S. degree (Hons.) in electrical engineering from Shahid Beheshti University, Tehran, Iran, in 2009, the M.S. degree (Hons.) in electrical engineering from the Amirkabir University of Technology, Tehran, in 2011, and the Ph.D. degree in electrical and computer engineering from the University of California at San Diego, La Jolla, CA, USA, in 2017.

She was a Post-Doctoral Research Fellow with the University of Michigan from 2017 to 2020. Her research interests include RF, millimeter-wave, and THz integrated circuits and systems, communication electronics, wireless communications and sensing, Internet of Things (IoT) connectivity and communications, physical layer security, and sensing.

Dr. Ebrahimi was a recipient of the Jacobs School of Engineering Fellowship at the University of California at San Diego, the 2019 and 2020 EECS Rising Star, and the 2018–2020 IEEE Microwave Society Chapter Chair for Southeastern Michigan.



Hun-Seok Kim (Member, IEEE) received the B.S. degree in electrical engineering from Seoul National University, Seoul, South Korea, in 2001, and the Ph.D. degree in electrical engineering from the University of California at Los Angeles (UCLA), Los Angeles, CA, USA, in 2010.

He is currently an Assistant Professor with the University of Michigan, Ann Arbor, MI, USA. His research focuses on system analysis, novel algorithms, and very-large-scale integration (VLSI) architectures for low-power/high-performance wireless communications, signal processing, computer vision, and machine learning systems.

Dr. Kim was a recipient of the 2018 Defense Advanced Research Projects Agency (DARPA) Young Faculty Award (YFA) and the National Science Foundation (NSF) Faculty Early Career Development (CAREER) Award 2019. He is an Associate Editor of IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and IEEE SOLID-STATE CIRCUITS LETTERS.

David Blaauw (Fellow, IEEE) received the B.S. degree in physics and computer science from Duke University, Durham, NC, USA, in 1986, and the Ph.D. degree in computer science from the University of Illinois at Urbana–Champaign, Champaign, IL, USA, in 1991.

Until August 2001, he worked at Motorola, Inc., Austin, TX, where he was the Manager of the High Performance Design Technology Group and won the Motorola Innovation Award. Since August 2001, he has been on the faculty of the University of Michigan, where he is the Kensall D. Wise Collegiate Professor of EECS. He is also the Director of the Michigan Integrated Circuits Lab. He has published over 600 articles, has received numerous best paper awards, and holds 65 patents. He has researched ultralow-power wireless sensors using subthreshold operation and low-power analog circuit techniques for millimeter systems. This research was awarded the MIT Technology Review's, "one of the year's most significant innovations." His research group introduced so-called near-threshold computing, which has become a common concept in semiconductor design. Most recently, he has pursued research in cognitive computing using analog, in-memory neural-networks for edge devices and genomics for precision health.

Dr. Blaauw was a member of the IEEE International Solid-State Circuits Conference (ISSCC) analog program subcommittee and the General Chair of the IEEE International Symposium on Low Power. He received the 2016 SIA-SRC Faculty Award for lifetime research contributions to the U.S. semiconductor industry.