Protego: Securing Wireless Communication via Programmable Metasurface

Xinyi Li*†, Chao Feng*†‡, Fengyi Song†, Chenghan Jiang†, Yangfan Zhang†
Ke Li†, Xinyu Zhang♯, Xiaojiang Chen†§⋄
†Northwest University, China, ♯University of California San Diego, USA
§Internet of Things Research Center, Northwest University, China
‡Shaanxi International Joint Research Centre for the Battery-Free Internet of Things, China
†{xinyili,songfengyi,jiangchenghan,zhangyangfan1}@stumail.nwu.edu.cn,
†{chaofeng,like,xjchen}@nwu.edu.cn, ♯xyzhang@ucsd.edu

ABSTRACT

Phased array beamforming has been extensively explored as a physical layer primitive to improve the secrecy capacity of wireless communication links. However, existing solutions are incompatible with low-profile IoT devices due to cost, power and form factor constraints. More importantly, they are vulnerable to eavesdroppers with a high-sensitivity receiver. This paper presents Protego, which offloads the security protection to a metasurface comprised of a large number of 1-bit programmable unit-cells (i.e., phase shifters). Protego builds on a novel observation that, due to phase quantization effect, not all the unit-cells contribute equally to beamforming. By judiciously flipping the phase shift of certain unit-cells, Protego can generate artificial phase noise to obfuscate the signals towards potential eavesdroppers, while preserving the signal integrity and beamforming gain towards the legitimate receiver. A hardware prototype along with extensive experiments has validated the feasibility and effectiveness of Protego.

CCS CONCEPTS

• **Hardware → Wireless devices**; • **Security and privacy → Mobile and wireless security**.

KEYWORDS

Metasurface, Smart Surface, IoT Security, Securing Wireless Communication, Security, Eavesdropping, Physical Layer Security

ACM Reference Format:
Xinyi Li*†, Chao Feng*†‡, Fengyi Song†, Chenghan Jiang†, Yangfan Zhang†, Ke Li†, Xinyu Zhang♯, Xiaojiang Chen†§⋄. 2022. Protego: Securing Wireless Communication via Programmable Metasurface. In *The 28th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '22), October 17–21, 2022, Sydney, NSW, Australia.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3495243.3560547

*Co-primary authors, both authors contributed equally to this research.
⋄ Corresponding author.

ACM MobiCom '22, October 17–21, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9181-8/22/10…$15.00
https://doi.org/10.1145/3495243.3560547

1 INTRODUCTION

The Internet of Things (IoT), as a new wave of revolution in the digital world, is transforming every aspect of human life, through smart home [51], intelligent transportation [33, 40], precision healthcare [9, 20], smart agriculture [44], etc. Wireless communication technology has been acting as a cornerstone in IoT, enabling the connection between human and things and melding between the virtual and physical world. The deep penetration of wireless technology into daily lives, however, is raising an outcry of privacy concerns. Due to the broadcast nature of the wireless medium, an adversary can eavesdrop on a legitimate link to steal personal information [19, 48], and even take control over personal IoT devices such as voice assistants and autonomous vehicles [38]. To mitigate such risks, a straightforward solution is to employ sophisticated encryption protocols. Current IoT devices, however, generally adopt weak encryption algorithms due to their low cost and low energy budget, leaving them vulnerable to security attacks [24, 27].

Beamforming represents a fundamental primitive that can enhance the quality and security of a wireless link at the physical layer. With a large array of antennas, a beamforming transmitter can focus the signal power towards the intended receiver, effectively suppressing signal leakage towards undesired angles, thereby improving the secrecy capacity [31]. However, high directionality beamforming entails a massive number of antenna elements, which is infeasible for commodity wireless IoT devices due to cost and form factor constraints.

Recent research has attempted to enhance the capacity and security of low-profile devices by using metasurfaces as a beamforming proxy. For instance, RFcous [5] achieves beamforming by configuring the signal to pass through or reflect from a metasurface which consists of a large number of unit-cell elements. RFLens [14] realizes an area-efficient metasurface by simultaneously employing all unit-cells as 1-bit phase shifters, and aligning their phases to achieve beamforming. These state-of-art systems can use directional beams to improve the throughput of RF links and reduce the risk of passive eavesdropping (i.e., improving the secrecy capacity). However, they can only weaken the eavesdropped signals, and are defenseless against adversaries with a highly sensitive receiver.

In this paper, we ask the following question: Can we create a smarter radio environment that can electronically reconfigure itself to enhance the legitimate wireless link while obfuscating undesired communication with malicious users? We propose *Protego* [1],

[1]"Protego" is derived from the incantation "protego totalum" in Harry Potter.

which realizes the vision by deploying a smart metasurface near the wireless transmitter to serve as a security "shield". The Protego metasurface essentially moves the beamforming and security protection functions from the radio transmitter to the environment. The metasurface dynamically "reshapes" the RF signals passing through it, by reconfiguring the hundreds of binary phase shifters (i.e., unit-cells) and forming a highly directional mainlobe towards the legitimate receiver, while decreasing the signal leakage towards sidelobe directions. By doing so, it reduces the eavesdropping risk and improves the secrecy capacity [14]. Unfortunately, even with unprecedented directionality, it still bears the aforementioned vulnerability against a highly sensitive eavesdropper.

To address this challenge, we introduce a novel solution, namely random chaotic constellation scheme (*RCCS*), to ensure adversaries cannot decode the information even if they can overhear the transmitter. With RCCS, the Protego metasurface randomizes the wireless channel by generating artificial phase noise towards the eavesdropper. The design of RCCS stems from a novel insight: due to the 1-bit quantization, the phase compensation generated by different unit-cells exhibits an unbalanced contribution to beamforming. The unit-cells whose phase compensation values are close to the upper quantization boundary only make negligible contributions in forming the mainlobe, but can significantly impact the signals along sidelobe directions. We refer to such unit-cells as "*weak unit-cells*". By dynamically flipping the quantized phase compensation (i.e., 0 or π) of each weak unit-cell, we can intentionally introduce different phase noise values, and obfuscate the modulated signals' phases along the undesired sidelobe directions, without any noticeable impact on the mainlobe.

So, how to evaluate if a unit-cell is weak? The more weak unit-cells there are, the more obfuscation along the sidelobes, but meanwhile, the constructive combination of phase vectors along the mainlobe will inevitably be weakened, thus lowering the beamforming gain towards the legitimate receiver. On the other hand, if we only assign a small number of weak unit-cells, the diversity of phase noise for the sidelobes will be undermined, thus weakening the protection. To strike a balance, we introduce a *maximum quantization boundary optimization algorithm*, which maximizes the number of variable unit-cells while preserving the mainlobe.

In addition, we observe that a fully random flip of the quantized phase compensation values across weak unit-cells is not necessarily optimal–Instead, it sometimes only results in intra-quadrant rotation of the transmitted symbol in the constellation, leaving the eavesdropper a chance to decode. To overcome this loophole, we judiciously select the quantized phase compensation values, so that the resulting phase noise value approaches one of three "useful" values $\pi/2$, $-\pi/2$, and π, which randomizes the transmitted symbol across quadrants. Notably, merely using a single "useful" phase noise only induces a constant rotation of the received symbols in the In-phase and Quadrature (I/Q) domain, which risks being brute-forced. We thus employ three "useful" phase noise values simultaneously to obfuscate the data.

The above protection measures assume a single eavesdropper whose direction relative to the transmitter is known to the Protego metasurface. To maintain Protego's protection against multiple randomly located eavesdroppers, our basic insight is to randomize the wireless channels in all directions except that of the legitimate receiver. To this end, we first quantize the potential eavesdropper's locations into a discrete number of fan zones, each represented using a single angle/direction. We then extend the above RCCS, so that the set of phase compensation values across unit-cells can simultaneously generate useful phase noise along all the discretized directions. A brute-force search for such a configuration entails exponential complexity. We thus make a compromise by creating a chaotic coding pattern set which includes multiple phase compensation configurations, each protecting a subset of directions. We then switch across these configurations at random over time. We propose an obfuscation entropy metric that measures effectiveness of channel protection in all directions across a time slice. If the metric falls below a threshold along a specific direction, we update the chaotic coding pattern set until the metric is large than the threshold in all directions.

We implement Protego on a metasurface consisting of 16×16 unit-cells and spanning an area of $0.484 \times 0.484\ m^2$. Our experiments show that Protego can obfuscate undesired communication while enhancing the legitimate wireless link. Protego enables a symbol error rate (SER) higher than 0.6 in the eavesdropping directions while keeping it lower than 10^{-4} in the legitimate direction. In addition, Protego can achieve up to 19.7 dB signal strength improvement through mainlobe beamforming. Our field tests also demonstrate that Protego works well across different modulation schemes (e.g., QPSK, 16QAM, and OFDM), and different radio environments (multipath-rich and even NLoS).

The main contributions of Protego can be summarized as follows. To our knowledge, Protego represents the first programmable metasurface-assisted security protection scheme that leverages phase quantization errors to thwart wireless eavesdropping attacks. Protego combines space domain (i.e., directional beamforming) and I/Q domain (i.e., obfuscated constellation) protection. We propose a novel RCCS method which can effectively obfuscate constellation on the sidelobes (i.e., the potential directions of adversaries), while preserving the signal power and integrity along the mainlobe (i.e., the legitimate receiver). Our method can effectively protect against multiple adversaries with unknown locations. Finally, we implement the Protego hardware and validate its effectiveness in a wide range of practical scenarios.

2 RELATED WORK

Prior work on defending wireless communication against passive eavesdropping attacks has mainly focused on improving the cryptographic protocols [7, 8]. Crypto schemes, however, are often too demanding for low-cost, low-energy, and lightweight IoT devices that cannot afford the computation load [43]. Thus, IoT devices use weak encryption schemes that often suffer from certain vulnerabilities [3, 4]. Meanwhile, physical layer security has emerged as a new means of enhancing the security of wireless communications and is generally considered as a lightweight complement to the existing encryption mechanisms, rather than a replacement of them [53]. Examples include injecting artificial noise [18, 32], directional beamforming [23, 31, 45, 50], etc. Artificial noise based solutions rely on MIMO radios or cooperative relays [17, 35]. They often escalate the energy expenditure and require a large number of antennas, which are impractical for IoT devices [52]. Protego's design principle marks a clear contrast to existing solutions. It

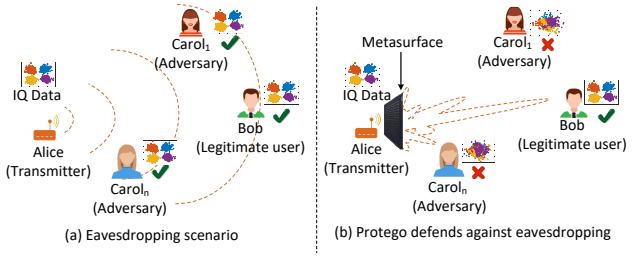


Figure 1: Illustration of Protego use cases. (a) Malicious users and the legitimate user can correctly decode the transmitted data. (b) Protego can utilize beamforming to reduce the SNR at the malicious users' direction, and obfuscate the transmitted data to prevent malicious users from correctly decoding.

introduces companion programmable metasurfaces to create a security environment around the wireless transmitter, thus shielding low-profile IoT transmitters against eavesdroppers.

Besides beamforming towards the legitimate receiver, a transmitter can also proactively protect its signals by forming nulls towards eavesdroppers or interferers [6, 16, 22, 28, 29]. However, it needs to know the locations of attackers in advance. In contrast, Protego evades such assumptions. One major reason is that its metasurface acts as a scalable beamforming array–Owing to the massive number of unit-cell elements, it can sacrifice certain weak unit-cells for RCCS obfuscation, without noticeably impacting the mainlobe signals towards the legitimate receiver.

Recently, smart surfaces are gaining traction as a way to "smarten" the radio environment. They can dynamically control the electromagnetic wave propagation to enhance the wireless link quantity and improve the secrecy capacity [11, 15, 26, 42, 46, 47, 49]. For example, RFcous [5] achieves beamforming by allowing the signal to either pass through or reflect from the surface elements. ScatterMIMO [12] uses a reflecting surface to induce multipath, thereby improving the channel conditions and capacity of a MIMO link. RFLens [14] uses 1-bit phase shifters on all unit-cells simultaneously, and aligns the phase of each unit-cell to achieve pass-through beamforming. Li et al. [25] utilize an 81-element single-layer reflectarray to perform reflective beamforming. These state-of-art systems mainly focus on improving the directionality, i.e., beamforming gain. Although directional beams can reduce the risk of passive eavesdropping and thus improve the secrecy capacity, they are defenseless against a highly sensitive eavesdropper.

Therefore, it is crucial to disturb the eavesdropping channel between the transmitter and adversaries, and corrupt the eavesdropped signal regardless of its strength. Many techniques have been developed and demonstrated to attain this goal [34, 37]. For example, RF-Cloak [21] introduces signal randomization to protest RFID tags from multi-antenna eavesdropping. It mechanically rotates eight directional antennas using a fan motor, and randomly selects the antennas for transmission. PhyCloak [36] deploys a full-duplex helper radio, which can obfuscate the wireless channel amplitudes, delays, and Doppler shifts between the transmitter and a receiver. By disturbing the Wi-Fi CSI, it can prevent adversaries from sensing the users' private activities. Eltayeb et al. [13] propose a physical layer security technique for vehicular communications based on a large mmWave antenna array. They employ a random subset of antennas to perform coherent beamforming to the receiver, while using the remaining antennas to randomize the far field radiation pattern at non-receiver directions. In contrast, Protego uses a lightweight programmable metasurface to build an intelligent environment to improve the secrecy capacity of IoT devices. Unlike the antenna array in [13], the Protego metasurface achieves beamforming through 1-bit phase shifters. It leverages the quantization errors on judiciously selected weak unit-cells to thwart potential eavesdroppers.

3 OVERVIEW

3.1 Threat Model

We consider a generic wireless link between Alice and Bob. By default, we focus on the forward link, i.e., Alice is the default transmitter. A Protego metasurface (MTS) is placed close to Alice, and there are n adversaries (i.e., Carol_1, ... , Carol_n) who are interested in eavesdropping on Alice's transmission, as shown in Figure 1. Neither the number n nor the locations of the adversaries are known to Protego. We assume Bob is static or at least quasi-stationary relative to Alice (potential extension to mobile cases is discussed in Sec. 9). The Protego MTS knows Bob's relative direction. There is no synchronization or other run-time coordination between the Protego MTS and Alice. In other words, the MTS configures its beamforming unit-cells independent of the packet/symbol timing of the transmitter.

We assume the transmitter Alice's antenna has a certain degree of directionality, so that its outgoing signals can all go through the MTS, hence under its protection. In practice, when the MTS is located in close proximity to Alice, the directionality requirement can be relaxed substantially. For example, a 50 cm×50 cm MTS located 15 cm away can easily cover a transmitter with up to 120 degrees of directionality. This is typically the intrinsic directionality for commodity patch-antenna transmitters [1]. In case when a wider field-of-view is needed, Alice can be equipped with multiple such patch antennas, each shielded by a Protego MTS. On the other hand, Bob and Carol can use arbitrary types of antennas.

Protego is designed to protect privacy-sensitive IoT devices in smart home or smart enterprise environment. For example, Alice can be a surveillance camera, a smart doorlock, an energy meter, etc.; whereas Bob is the smart hub that receives information from such sensors. The eavesdropping equipment could be camouflaged as a mobile power supply or WiFi-connected smart LED [39]. A maintenance personnel could have used the door-to-door service opportunity to install such eavesdroppers.

3.2 System Goals

By adding the MTS in front of Alice without explicit cooperation from any other nodes, Protego targets the following 3 objectives: (1) Obfuscate the wireless communication between Alice and Carol in order to prevent Alice from eavesdropping attacks. A side benefit is that Protego can protect replay or other active signal injection attacks from Carol, because Alice can only decode signals from Bob. (2) Preserve the signal integrity between Alice and Bob, so that they can communicate using the normal wireless physical layer. (3) Enhance the link capacity between Alice and Bob through highly directional MTS beamforming. By default, Protego protects the forward link (Alice→Bob) against eavesdropping. To enforce the

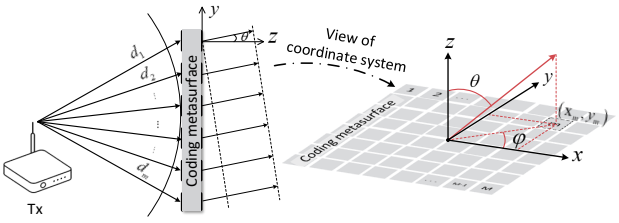


Figure 2: The geometry of the coding MTS.

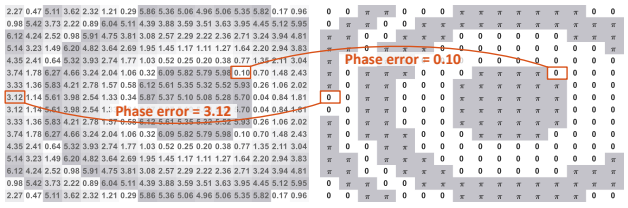


Figure 3: The phase error between ideal and quantization phase. The phase value is in radians.

same protection on the reverse link, Bob also needs a Protego MTS which covers its antenna's field of view.

4 A PRIMER ON PROTEGO METASURFACE BEAMFORMING

Similar to state-of-the-art smart beamforming metasurfaces [14], Protego comprises a large number of binary phase shifters to realize highly directional phased array beamforming. In this section, we describe the theoretical underpinning and working principles of Protego's beamforming scheme.

As shown in Figure 2, the MTS has $M \times N$ unit-cells ($M = N = 16$ in our prototype). The propagation distance experienced by the incident electromagnetic wave before impinging on the $(m,n)^{th}$ unit-cell is $d_{(m,n)}$, which leads to an initial phase shift of $\phi^I_{(m,n)} = -kd_{(m,n)}$, where $k = 2\pi/\lambda$; λ is the wavelength of signal; $m \in [1, M]$ and $n \in [1, N]$. Suppose the direction of the legitimate receiver is (θ_l, φ_l), where θ_l and φ_l are the elevation and azimuth angles, respectively. Therefore, to beamform the signal towards the direction (θ_l, φ_l), the theoretical phase distribution is:

$$\phi^T_{(m,n)} = -k\left(x_m \sin\theta_l \cos\varphi_l + y_n \sin\theta_l \sin\varphi_l\right), \tag{1}$$

where x_m and y_n are the X-axis and Y-axis distances of the $(m,n)^{th}$ unit-cell relative to the origin of coordinate. Thus, the *ideal phase compensation* generated from each unit-cell should be the difference of $\phi^I_{(m,n)}$ and $\phi^T_{(m,n)}$:

$$\phi^C_{(m,n)} = \phi^T_{(m,n)} - \phi^I_{(m,n)}. \tag{2}$$

Protego is a 1-bit programmable MTS, which means each unit-cell only provides two phase states: 0 or π. So in its most basic form, Protego uses a *quantized phase compensation* $\mathrm{Q}\left(\phi^C_{m,n}|_{1-bit}\right)$ to approach the ideal as follows:

$$\mathrm{Q}\left(\phi^C_{(m,n)}|_{1-bit}\right) = \begin{cases} 0, & if\ 0 \le \phi^C_{(m,n)} < \pi \\ \pi, & otherwise \end{cases}. \tag{3}$$

A quantized phase compensation value (i.e. 0 or π) is also referred to as a *coding parameter*, and the set of coding parameters

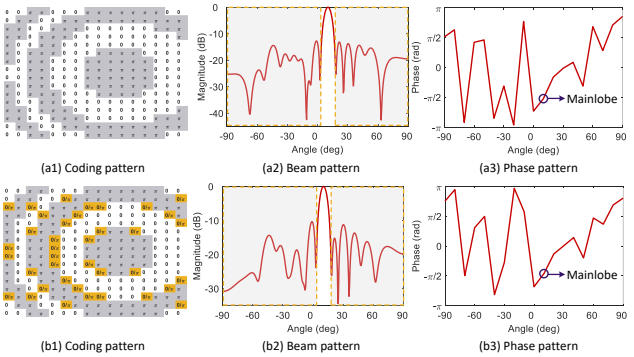


Figure 4: (a1)~(a3) are the coding/beam/phase pattern corresponding to the 1-bit quantization rule, respectively. (b1)~(b3) are the coding/beam/phase pattern after randomly changing the coding parameters of weak unit-cells, respectively.

for all the unit-cells is also called a *coding pattern*. By encoding the phase compensation, Protego can dynamically manipulate electromagnetic waves to focus the signal power towards the legitimate receiver. In this way, Protego can reduce the risk of eavesdropping and improve the secrecy capacity.

Note that the quantization boundary of Eq. (3) can be configured in different ways, such as mapping $[0, \pi)$ to 0 or $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ to 0. But different quantization boundaries have different applications. For instance, mapping $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ to 0 and 1 otherwise is the optimum selection for achieving beamforming because the phase compensation is completely symmetrical. However, this quantization rule loses weak unit-cells since the phase error of each unit-cell is the minimum. In other words, all unit-cells can produce the largest contribution to the mainlobe under this quantization rule. However, if we can map $[0, \pi)$ to 0 and 1 otherwise, the different unit-cells will have different contributions to the mainlobe. This observation can help Protego forms a highly directional mainlobe, while decreasing the signal leakage towards sidelobe directions.

5 PROTEGO: THE KEY INSIGHT

Beamforming alone weakens, but does not obfuscate the wireless channels between the transmitter and the eavesdroppers. Observing the distribution of phase compensation values across different unit-cells provides a new angle to tackle this limitation.

The Protego MTS with $M \times N$ layout can be regarded as an antenna array, the array factor [11] of which can be expressed by:

$$AF = \sum_{m=1}^{M}\sum_{n=1}^{N} a_{(m,n)} e^{jk(x_m u + y_n v)}, \tag{4}$$

where $u = \sin\theta\cos\varphi$ and $v = \sin\theta\sin\varphi$, θ and φ vary from $-\pi$ to π, $a_{(m,n)}$ is the amplitude. *The MTS needs to generate a compensated phase $\phi^C_{(m,n)}$ for the $(m,n)^{th}$ unit-cell when the desired beamforming direction is (θ_l, φ_l).* Therefore, Eq. 4 can be written as:

$$AF^{ideal} = \sum_{m=1}^{M}\sum_{n=1}^{N} a_{(m,n)} e^{j\left(k(x_m u + y_n v) - \phi^C_{(m,n)} - \phi^I_{(m,n)}\right)}. \tag{5}$$

If the MTS can realize the ideal phase compensation , then each unit-cell would contribute equally to beamforming. In practice, however, the 1-bit phase quantization of Protego would inevitably introduce

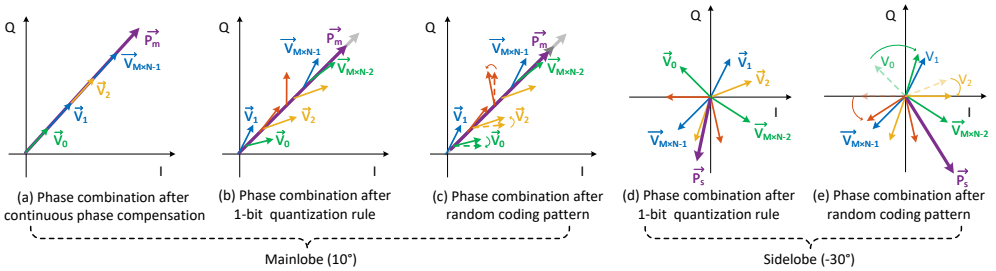


Figure 5: The essential reason for the mainlobe sightly changed while the sidelobe drastically changed when the coding pattern changed.

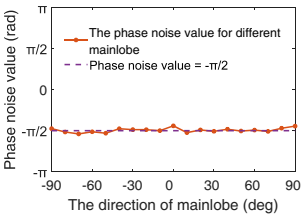


Figure 6: Phase noise value of different mainlobes.

phase error, which is denoted as $\phi^{err}_{(m,n)}$ for each unit-cell (m, n):

$$\phi^{err}_{(m,n)} = \phi^{C}_{(m,n)} - \phi^{Q}_{(m,n)}, \tag{6}$$

where $\phi^{Q}_{(m,n)} = \phi^{C}_{(m,n)}\,|_{1-bit}$ is the quantized phase. Hence, the actual array factor becomes:

$$AF^{actual} = \sum_{m=1}^{M}\sum_{n=1}^{N} a_{(m,n)} e^{j\left(k(x_m u + y_n v) - \phi^{C}_{(m,n)} + \phi^{err}_{(m,n)} - \phi^{I}_{(m,n)}\right)}. \tag{7}$$

Figure 3(a) and Figure 3(b) plot the ideal/quantized phase compensation of different unit-cells, for an example scenario where the beamforming mainlobe points towards 10°. We can observe that the phase compensation values of some unit-cells are closer to the quantization boundary (i.e., 0 or π), while some are not. For example, the ideal phase compensation of the $(8,1)^{th}$ and the $(6,13)^{th}$ unit-cell are disparate (3.12 and 0.10, respectively); whereas they both become 0 after quantization. Among different unit-cells, some exhibit phase errors close to π, and some close to 0. This phenomenon results in an *unbalanced contribution of different unit-cells to the desired beamforming mainlobe*. Based on the array factor in Eq. 7, we can also infer that the contribution of the $(6,13)^{th}$ unit-cell is greater than the $(8,1)^{th}$ unit-cell since the former's phase error is closer to 0.

The foregoing analysis leads to two important findings:

(i) If a unit-cell's ideal phase compensation is closer to the upper quantization boundary, the unit-cell contributes less to the mainlobe. We refer to such unit-cells as "*weak unit-cells*". Figure 4(a2) shows an example beam pattern where the Protego MTS beamforms towards 10° azimuth angle using the quantized phase compensation. Then, we randomly flip the coding parameters (i.e., 0 or π) of some weak unit-cells. Note that the threshold for defining weak unit-cells here is that the ideal phase compensation of the unit-cell belongs to $[7\pi/9, \pi)$ or $[17\pi/9, 2\pi)$. From Figure 4(a1) and (a2), we can see that although the coding pattern of MTS is different, the mainlobe's beamforming gain is preserved (Figure 4(b2)).

(ii) The smaller the contribution to the mainlobe, the greater the impact on the sidelobes. To understand the essential reason, consider the example shown in Figure 5, where the beamforming generates a mainlobe at 10° and a sidelobe at -30°. Each vector $\overrightarrow{V}_*$ represents the signal emitted from a given unit-cell. $\overrightarrow{P_m}$ and $\overrightarrow{P_s}$ are the signal along the mainlobe and sidelobe direction, respectively. Figure 5(a) shows the constructive combination of different unit-cells' signals under the ideal continuously compensated phase. Figure 5(b) shows that, with the 1-bit quantization, the $\overrightarrow{V}_*$ vectors have different phase errors, so the mainlobe is slightly weakened (by around 3.8 dB in this example). On the other hand, along the sidelobe direction of -30°, the signal vectors sum up to $\overrightarrow{P_s}$ as shown in Figure 5(d). The essential goal of Protego is to intentionally change these vectors by changing the coding parameters of the weak unit-cells, so as to disturb the sidelobe signal $\overrightarrow{P_s}$ (e.g., shifting it to a different constellation quadrant as shown in Figure 5(e)), while preserving the mainlobe signal $\overrightarrow{P_m}$ (Figure 5(c)).

6 PROTEGO: RANDOM CHAOTIC CONSTELLATION SCHEME

Based on the above insights, we propose a novel random chaotic constellation scheme (RCCS), which leverages the Protego MTS to randomize the wireless channels from the transmitter to eavesdroppers, thus overcoming the vulnerability of the beamforming-only solution (Section 4).

6.1 How Does the Legitimate User Decode?

The goal of the legitimate user is to demodulate the received signal and retrieve the transmitted data. For brevity, we denote each symbol on the constellation by:

$$S_r = \sqrt{E_0} e^{j\phi(r)}, \tag{8}$$

where E_0 represents the average energy per symbol and r is the index of the transmitted symbol in a signal frame. Protego can reconfigure coding patterns of the MTS, equivalently imposing different phase compensation values for signals going through different unit-cells. The received symbol can thus be expressed as:

$$S'_r = S_r e^{j\phi^{noise}_r} e^{j\phi^{path}_r}, \tag{9}$$

where $e^{j\phi^{noise}_r} = \sum_{m=1}^{M}\sum_{n=1}^{N} e^{j(\phi^{T}_{(m,n)} - \phi^{err}_{(m,n)})}$, ϕ^{noise}_r is the phase noise value induced by the MTS for the r^{th} symbol, and ϕ^{path}_r is the path phase induced by the transmission between the MTS and receiver.

To accurately decode the received symbols, the legitimate user needs to eliminate the terms ϕ^{noise}_r and ϕ^{path}_r in Eq. (9). Standard wireless PHY layer protocols usually embed a known preamble on the transmitted signals, enabling the receiver to perform channel estimation and obtain the calibration phase ϕ^{cali}_r. The receiver can subsequently equalize the received symbols as:

$$S_r = \frac{S'_r}{e^{j\phi^{cali}_r}}. \tag{10}$$

By doing so, the legitimate user can easily eliminate the phase noise value from the received symbols. The same equalization can

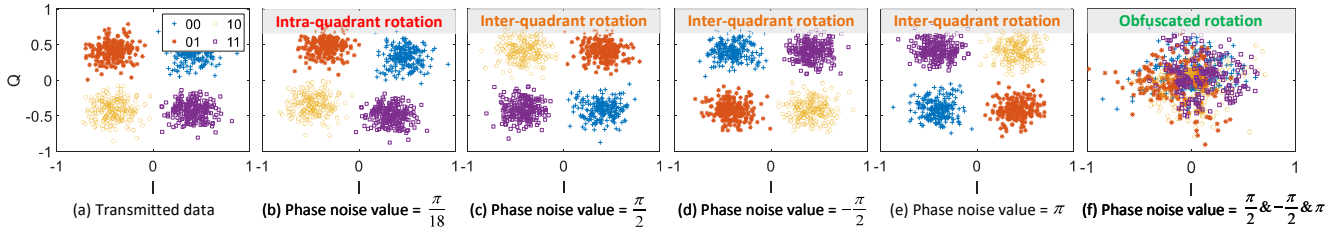


Figure 7: Different phase noise values result in different rotations of the I/Q data in the quadrants.

be reused within the channel coherence time. Note that to ensure the same equalization can be reused, ϕ_r^{noise} should be a stable value within the channel coherence time.

6.2 Defending Against Eavesdroppers

To simplify the exposition, we describe RCCS first assuming a single eavesdropper whose relative direction is known to Protego. Then we introduce a chaotic coding pattern set to simultaneously protect against multiple unknown eavesdroppers.

6.2.1 How to evaluate if a unit-cell is weak? Recall that we can flip the coding parameters of some weak unit-cells to vary the constructive combination of the phase vector for different sidelobes (Section 5). The caveat is that, with too many weak unit-cells, the beamforming gain of the mainlobe will inevitably suffer a significant drop. Conversely, too few weak unit-cells may not effectively distort and obfuscate signals along the sidelobes.

To strike a balance, we design a *maximum quantization boundary optimization algorithm* to assign the weak unit-cells. Specifically, rather than using 0 and π as the lower/upper boundaries of phase quantization, we aim to optimize the beam pattern by reconfiguring the boundaries. The optimization problem can be formulated as:

$$\min_{LB}\min_{UB} Q^*\left(\phi^C_{(m,n)}\Big|_{LB}^{UB}\right) = \begin{cases} 0, if\ 0 \le \phi^C_{(m,n)} < LB \\ \pi, if\ \pi < \phi^C_{(m,n)} \le UB \\ 0/\pi, otherwise \end{cases} \tag{11}$$

$s.t.$

$$AF^{Q^*}_{main} - \max\left(AF^{Q^*}_{side}\right) \ge \xi \tag{12}$$

$$[\angle \sum_{m=1}^{M}\sum_{n=1}^{N} e^{j(\phi^T_{(m,n)} - \phi^{err}_{(m,n)})} - \angle \sum_{m=1}^{M}\sum_{n=1}^{N} e^{j(\phi^T_{(m,n)} - \phi^{err^*}_{(m,n)})}]_{(\theta_l,\varphi_l)} \le -\frac{\pi}{2} \pm \gamma \tag{13}$$

$$LB \in [0, \pi] \tag{14}$$

$$UB \in (\pi, 2\pi], \tag{15}$$

where $\phi^{err^*}_{(m,n)} = \phi^C_{(m,n)} - \phi^{Q^*}_{(m,n)}\Big|_{LB}^{UB}$. LB and UB are the lower and upper boundary of the new quantization rule Q^*, respectively. $AF^{Q^*}_{main}$ and $AF^{Q^*}_{side}$ are the gain of mainlobe and sidelobes under the new quantization rule Q^*, respectively. ξ is the difference gain between the mainlobe and sidelobe under the new quantization rule. γ is the difference of phase noise values of mainlobe between the original 1-bit and the new quantization rule. The constraint (12) represents the fact that we trade the gain of beamforming for more weak unit-cells. Note that the phase noise value of mainlobe is induced by the 1-bit quantization rule of the MTS, which is approximated to $-\frac{\pi}{2}$ in all potential directions (Figure 6), so the constraint (13) represents the offset range of the phase noise value of the mainlobe, which ensures the legitimate user can perform normal channel estimation to obtain the calibration phase for equalization. In our implementation, we set $\xi = 10$ and $\gamma = \frac{\pi}{36}$, respectively. Eq. (14) and Eq. (15) are the range of boundary constraints, respectively. We employ a particle swarm optimization (PSO) algorithm [30] to solve the above formulation.

6.2.2 Against One Known Eavesdropper. Based on the analysis in Section 5, we can simply generate different artificial phase noise values by configuring the weak unit-cells' coding parameters, so as to disturb signals along a sidelobe (pointing towards the eavesdropper). Although the phase noise value can vary from $-\pi$ to π, not all values are "useful" for disturbing the signals. To further understand the effectiveness of a phase noise value, consider the QPSK modulation as an example in Figure 7. The bits 00, 01, 10, 11 are mapped to symbols of equal magnitude $\sqrt{E_0}$ but different phases ($\frac{\pi}{4}$ to $\frac{7\pi}{4}$) in the constellation, as shown in Figure 7(a). Following Eq. (9), we can introduce a phase noise value ϕ_r^{noise} when the incident wave goes through the MTS. Note that ϕ_r^{path} is stable within the channel coherence time, thereby we only discuss the impact of ϕ_r^{noise}. When ϕ_r^{noise} is not properly set (e.g., to $\frac{\pi}{18}$ as in Figure 7(b)), the transmitted data rotates only within the same quadrant. Hence, the eavesdropper can still demap the constellation and recover the transmitted symbols. Therefore, to ensure Protego can effectively obfuscate signals along the sidelobe direction, it is crucial to identify the "useful" phase noise values.

But how to define whether a phase noise value is "useful" or not? Our solution RCCS builds on the following key knowledge: The eavesdropper's decoding will fail, as long as we can skew its signals randomly across different quadrants–and of course, without disturbing the legitimate receiver. RCCS thus uses a set of three values, $\frac{\pi}{2}$, $-\frac{\pi}{2}$ or π, as the "useful" phase noise values. Any one of these 3 phase noise values will ensure the transmitted symbol is skewed to a different quadrant in the I/Q constellation, regardless of whether the symbol is modulated by QPSK, QAM, etc. It can also be extended straightforwardly to OFDM modulation, which is widely used in modern wireless standards. Specifically, we simply apply RCCS on a per-subcarrier basis, wherein each subcarrier is modulated in QPSK, QAM, etc.

Once the "useful" phase noise values are determined, we need to search for three corresponding coding patterns based on the maximum number of weak unit-cells. The three coding patterns need to satisfy the following constraint:

$$\sum_{m=1}^{M}\sum_{n=1}^{N}\left|k(x_m u_{eve} + y_n v_{eve}) - \phi^C_{(m,n)} + Q^*_\alpha(\phi^C_{(m,n)}\Big|_{LB}^{UB})\right| \le \alpha \pm \rho, \tag{16}$$

where $u_{eve} = \sin\theta_{eve}\cos\varphi_{eve}$ and $v_{eve} = \sin\theta_{eve}\sin\varphi_{eve}$, θ_{eve} and φ_{eve} is the azimuth/elevation direction of the known eavesdropper. $\alpha \in \{\frac{\pi}{2}, -\frac{\pi}{2}, \pi\}$ is the target "useful" phase noise value. ρ is the

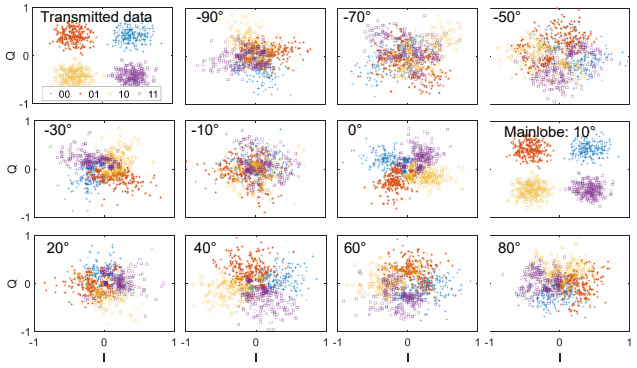


Figure 8: Simulation results from several angles after using a chaotic coding pattern set.

tolerance range of "useful" phase noise values and set to $\frac{\pi}{18}$ by default.

As shown in Figure 7(c-e), with phase noise value $\alpha \in \{\frac{\pi}{2}, -\frac{\pi}{2}, \pi\}$, the transmitted symbols undergo significant inter-quadrant rotation. Notably, simply using a uniform "useful" phase noise value will result in all symbols rotated by a fixed angle in the I/Q domain. Hence, it is still vulnerable to a brute-force decoder which performs a linear search across different phase noise.

Therefore, an effective protection scheme needs to introduce different "useful" phase noise values on different symbols. In our system, we obfuscate the constellation by switching α across the three "useful" phase noise values over time. With this measure, those symbols originally in the same quadrant are scattered in different quadrants, as illustrated in the example in Figure 7(f).

6.2.3 Against Unknown Eavesdroppers. To extend the protection mechanism to multiple eavesdroppers with unknown locations, our basic insight is to randomize the wireless channels in all directions except that of the legitimate receiver. We first quantize the potential eavesdropper's locations into a discrete number of fan zones (i.e., 18 subareas, from -90° to 90° by the step of 10°). Here, we represent each subarea using a single angle (i.e., potential eavesdropping direction). We then extend the above RCCS, so that the set of phase compensation values across unit-cells can simultaneously generate "useful" phase noise along all the discretized directions. However, searching for such configuration is infeasible due to the exponential computational complexity.

Therefore, we make a compromise by creating a *chaotic coding pattern set* which includes multiple phase compensation configurations to reduce the computational complexity. Specifically, each phase compensation configuration protects a subset of directions (i.e., 3 directions) instead of all possible eavesdropping directions. Then, we alternately use different phase compensation configurations to protect all directions. However, how to judge whether the configurations included in the current chaotic coding pattern set can together achieve security protection in all directions?

We propose an *obfuscation entropy metric* that estimates the effectiveness of channel protection in all directions across a time slice. Using this metric, we run an iterative search algorithm offline to construct the chaotic coding pattern set. Specifically, we perform an offline simulation of the phase noise effects imposed by the MTS over a generic link under Rayleigh fading. We cluster the received data into four categories corresponding to four quadrants, calculate the centroid for each cluster and use them to re-plan the coordinate axes. Finally, we calculate the obfuscation entropy e of each new quadrant as follows:

$$e = \sum_{i=1}^{L_{cluster}} \frac{R_c^i}{R_c} e_i, \qquad e_i = -\sum_{j=1}^{L_{class}} P_{ij} \log_2 P_{ij}, \tag{17}$$

where $P_{ij} = R_c^{ij} \Big/ R_c^i$. $L_{cluster}$ is the number of clusters, L_{class} is the number of classes, P_{ij} is the probability of belonging to class j in the data of cluster i, R_c is the total number of transmitted symbols, R_c^i is the number of transmitted symbols in cluster i, and R_c^{ij} is the number of symbols belonging to j-th class in i-th cluster.

Intuitively, if the e falls below a threshold (i.e., 0.5), the obfuscation along the corresponding sidelobe direction becomes too weak, so we update the chaotic coding pattern set by adding more phase compensation configurations that can especially protect that direction. This search process iterates until the e metric of all directions exceeds the threshold. We then directly use the resulting chaotic coding pattern set to defend against potential eavesdropping directions. Although this may slightly decrease the obfuscation entropy of well protected directions, it eliminates the protection bottleneck and approaches global optimality.

To demonstrate the effectiveness of the proposed chaotic coding pattern set, we simulate the constellation of transmitted data by using QPSK modulation and the results after using a chaotic coding pattern set. The mainlobe points towards 10°. From the result in Figure 8, we can observe that: 1) the legitimate user at the mainlobe can correctly decode the transmitted information with near zero error. 2) Protego can effectively thwart adversaries to decoding in directions (i.e., form -90° to 90° by the step of 20°) except that of the legitimate user.

7 IMPLEMENTATION

Metasurface Prototype. Our current Protego is implemented on a MTS operating at 5 GHz Wi-Fi band. The MTS consists of 256 functional unit-cells with a total surface area of 48.4 × 48.4 cm^2 and a thickness of 6.2 mm. Each unit-cell has two PIN diodes (SMP1340-040LF [2]) placed in the same orientation. When a bias voltage (0 V/5 V) is applied to the PIN diodes, the unit-cell acts as a 1-bit phase shifter (e.g., 0 and π). We carefully optimize the material and geometric parameters of the unit-cell, so that Protego MTS can work well in all 5 GHz ISM frequency bands. As shown in Figure 9 and Figure 10, the phase difference between ON/OFF states is stable at 180° and the transmission loss is larger than -3 dB across the entire 5 GHz frequency band. We note that the same design can be easily transferable to other frequency bands, such as 2.4 GHz and 900 MHz, commonly used by IoT devices.

Metasurface Control. To independently control each unit-cell, we employ one Kintex-7 FPGA and 32 SN74HC595 shift registers to provide the bias voltages to the PIN diodes. More specifically, we divide the 256 unit-cells into 8 groups in parallel, and each group consists of 4 shift registers, which serially control 32 unit-cells. The chaotic coding pattern set for each legitimate direction is stored in the FPGA in advance. When the legitimate direction is determined,

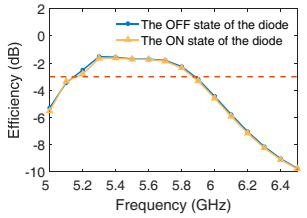


Figure 9: Simulated efficiency of metasurface.

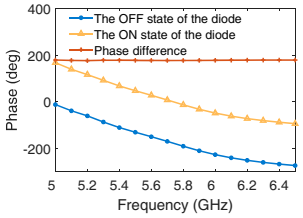


Figure 10: Simulated phase of metasurface.

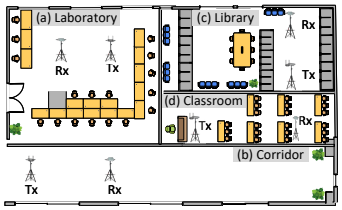


Figure 11: Deployment layout.

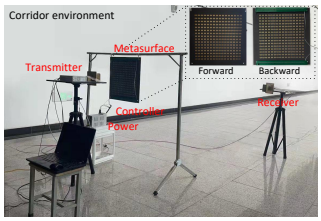


Figure 12: Evaluation setup.

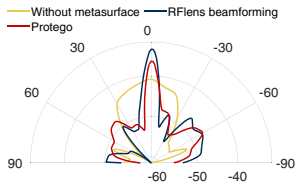


Figure 13: The performance of beamforming.

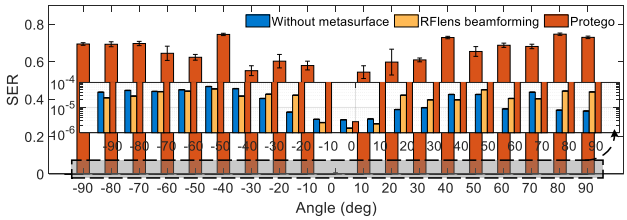


Figure 14: The performance of symbol error rate.

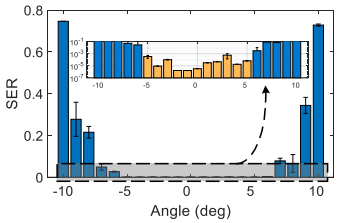


Figure 15: The SER performance in a subarea.

we randomly select a coding pattern from the corresponding chaotic coding pattern set to reconfigure the MTS. To parallelly control, we also divide the coding pattern into 8 groups, which are then input into 8 data storages. Then, we use 8 data GPIO pins to output the data from data storages to registers and 8 Enable GPIO pins to make registers output the coding pattern to the MTS. To ensure 32 shift registers to output the coding pattern at the same time, we employ 8 Clock GPIO pins to make the output of registers under the same clock. After that, by iteratively calling the coding patterns file under the corresponding address of the storage, the MTS can quickly output the whole chaotic coding pattern set.

Experimental setup. For controlled experiments, we use one USRP N210 software-defined radio with a UBX-40 daughterboard as the radio transceiver. The transmitter uses a directional antenna and the receiver uses both directional and omni-directional antennas. We conduct extensive experiments in four indoor environments to evaluate the performance of Protego: three multipath-rich environments (classroom, library, and laboratory) and a relatively open corridor environment. Figure 11 illustrates the layout of the 2 scenarios and Figure 12 shows a typical experimental scenario in the corridor environment. In the default setup, we transmit signals in QPSK modulation mode and add a fixed PAM signal as a preamble for channel estimation. The carrier frequency is set to 5.8 GHz and the transmission symbol rate is 125K symbols/sec. The switching rate of the MTS is 160K coding patterns/sec.

Security Metric. In our paper, we use the symbol error rate (SER) experienced by the adversary as a metric to evaluate the system's security against eavesdroppers. The reasons for selecting the SER metric instead of bit error rate (BER) are as follows: 1) Protego performs security protection by adding phase noises to make the transmitted *symbol* skew to a different quadrant in the I/Q constellation, thus corrupting the eavesdropper's decoding; 2) The SER metric can be invariant to the symbol modulation scheme, e.g., QPSK vs. BPSK, where each symbol contains different number of bits. Ideally, a fully secure system should have a SER of at least 25% at the adversary for QPSK, which is equivalent to the result of a random guess between four quadrants in the I/Q domain.

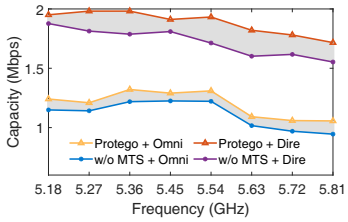
8 EVALUATION

8.1 Micro-benchmark

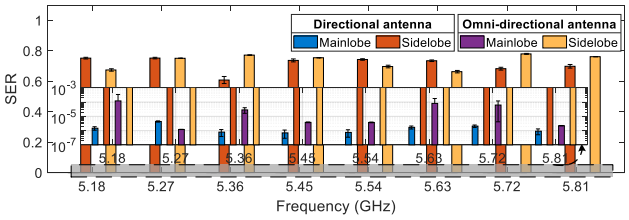
Beamforming verification. Our first experiment compares Protego against state-of-the-art RFLens MTS with 1-bit phase shifters [14], and the case without MTS. We move the receiver (Rx) along a semicircle (3 m radius) from -90° to 90° with a step of 10°, while the transmitter (Tx) stays in the center with the MTS 0.3 m away from it. Figure 13 shows Protego's security power comes at the cost of slight decreases of signal strength on the mainlobe–less than 3 dB relative to RFLens. The gap depends on the number of weak unit-cells. On the other hand, Protego adds a 4.28 dB gain compared with the case without the MTS, and the gain easily scales as the number of unit-cells increases [14]. In addition, its mainlobe is 11.2 dB higher than the sidelobe on average. Overall, with beamforming alone, Protego can already provide a reasonable level of isolation against eavesdroppers while improving the link quality towards the legitimate Rx.

Symbol error rate (SER). We use the eavesdropper's SER as a metric for end-to-end security protection, under the same setup as above. We move the Rx along a semicircle (3 m radius) from -90° to 90° with a step of 10°. For each location of Rx, we collect 10 measurements and plot the results in Figure 14. We observe that, with the RFLens beamforming, the eavesdropper's average SER is higher than the case without the MTS, but remains around 10^{-5} to 10^{-4}. So the eavesdropper is very likely to decode majority of the information. In contrast, with Protego, the minimum, median, and maximum SER of potential eavesdropping directions (i.e., sidelobes) are 0.55, 0.70, and 0.75, respectively. So the information is fully obfuscated from the eavesdropper, while the legitimate user (i.e., mainlobe at 0°) always maintains a low SER.

Verification of using a single angle covers a subarea. Recall that Protego employs a single angle's chaotic coding pattern set to represent one subarea (Section 6.2.3), we now examine how it impacts SER performance. Specifically, we repeat the same setup as above, except that the Rx now moves along the semicircle from $-10°$ to $10°$ with a step of $1°$. We use the chaotic coding pattern set



(a) Channel capacity.



(b) Symbol error rate.

Figure 16: Experimental results of power improvement and SER at different operating frequencies.

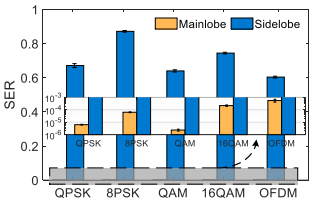


Figure 17: Results of different modulation schemes.

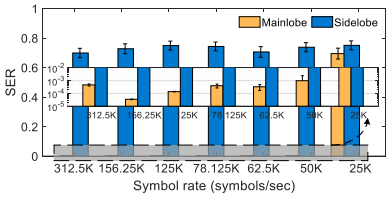
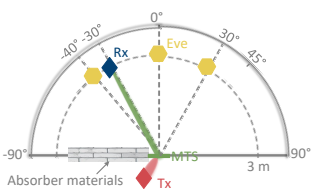
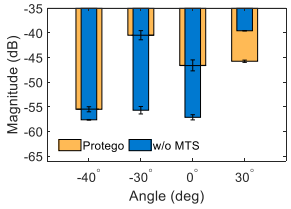


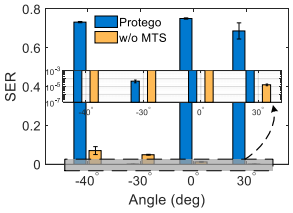
Figure 18: Results under different transmission symbol rates.



(a) Setup.



(b) Beamforming.



(c) Symbol error rate.

Figure 19: Experimental setup and evaluation results of power improvement and SER under NLoS scenarios.

of the mainlobe at 0° to randomly reconfigure the MTS. Figure 15 shows the SER is always less than 3.26×10^{-4} when the Rx is within ±5°, which implies we can use a single angle to represent one subarea about 10° without affecting the SER performance.

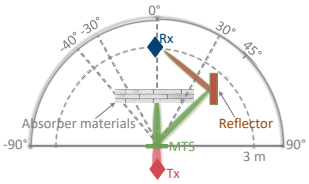
8.2 Performance Evaluation

Performance across a wide spectrum and with different antenna patterns. To verify the effectiveness of Protego across the entire 5 GHz ISM frequency band, we measure the channel capacity and SER by varying the operating frequency from 5.18 GHz to 5.81 GHz. Meanwhile, we evaluate both directional and omni-directional antennas (referred to as Dire and Omni) on the Rx. Figure 16(a) demonstrates that Protego is capable of boosting channel capacity efficiently for both the Dire and Omni under different frequencies. However, since the Omni antenna is more susceptible to multipath, the improvement for Omni antenna is smaller than Dire antenna. Figure 16(b) further shows that, regardless of the frequency and Rx antenna pattern, Protego can effectively defy the eavesdroppers and ensure the legitimate user maintains a low SER.

Impact of different modulation schemes. In this experiment, we keep the legitimate user and eavesdropper at 0° (i.e., mainlobe) and 30° (i.e., sidelobe) respectively without loss of generality, while varying the modulation scheme across QPSK, 8PSK, QAM, and 16QAM. Figure 17 shows that, the SER is always near 0 along the mainlobe, and above 0.64 (up to 0.87) along the sidelobe. *The SERs of higher-order modulations (e.g., 8PSK and 16QAM) are significantly higher*, because they require finer-grained constellation, making the transmitted data more easily obfuscated. We further study the performance of Protego when operating with WiFi OFDM modulation. The OFDM signal includes 56 subcarriers and the center frequency is 5.18 GHz with over 20 MHz bandwidth. We can see that the SER is slightly lower than that of other modulation schemes, but still reaches 0.60. The reason is that the transmission efficiency of the MTS always exceeds -3 dB across the entire 5.15~5.89 GHz band (Figure 9), so Protego can work well under a wider bandwidth. Overall, Protego performs consistently well on different modulation schemes.

Impact of different transmission symbol rates. We now vary the Tx's symbol rate from 312.5 KHz to 25 KHz, while keeping the switching rate of MTS at 160K codes/sec, to verify the impact of asynchronization between them. The legitimate Rx and eavesdropper are located at 0° and 20°, respectively. Figure 18 shows that, as the symbol rate decreases, the SER is always larger than 0.7 and less than 9×10^{-4} for the eavesdropper and legitimate user, respectively. An exception occurs at 25 KHz, when the legitimate user's SER becomes 0.69. This is expected because when the MTS switches too frequently, one data symbol may span multiple RCCS phase noise values. Therefore, the Protego switching rate should be kept at a reasonably low level.

Performance under NLoS scenario between Rx and Tx. The foregoing experiments always place the Rx within the LoS of the Tx. Now we create a NLoS scenario, as shown in Figure 19(a), by placing a barrier wall of absorber material at the LoS link with 30 cm away from the Tx, and the MTS is placed aside along the barrier wall. The angle between Tx and the MTS is 30°. The legitimate Rx is located at −30° with a radius of 3 m compared to the center of the MTS, and the eavesdropper Rx is located at −40°, 0° and 30°, respectively. We reconfigure MTS by using the chaotic phase coding pattern set of −30° in order to resteer the beam towards the direction of legitimate Rx while obfuscating the transmission of eavesdroppers. We then run 20 measurements in each location. Next, we remove the MTS and repeat the measurements. As shown in Figure 19, we can see that with the help of MTS, Protego can improve 15.2 dB signal strength to the legitimate Rx. Besides, Protego can successfully protect the NLoS link from eavesdropping. For example, when a MTS is deployed, the SER of the eavesdropper located at the direction of 30° increases from 1.65×10^{-5} to 0.687, implying that Protego works well in the NLoS scenario between Rx and Tx.

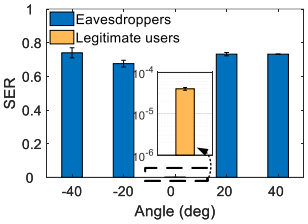


(a) Setup

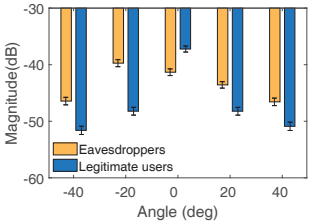
Distance	Without Reflector		With Reflector$_{Tin}$		With Reflector$_{Cardboard}$	
	RSS (dB)	SER	RSS (dB)	SER	RSS (dB)	SER
1 m	-67.87	N/A	-58.53 +(9.34)	0.65	-62.22 +(5.65)	N/A
1.5 m	-67.88	N/A	-61.11 +(6.75)	N/A	-64.11 +(3.77)	N/A
2 m	-67.63	N/A	-67.24 +(0.41)	N/A	-67.24 +(0.39)	N/A

(b) RSS and SER.

Figure 20: Experimental setup and evaluation results for the NLoS scenario.

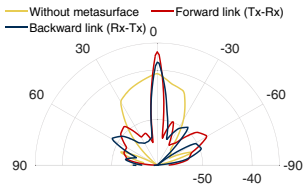


(a) Symbol error rate.

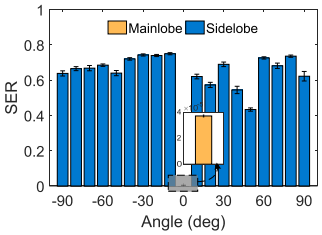


(b) Beamforming.

Figure 21: Experiment results with multiple eavesdroppers located in different directions.

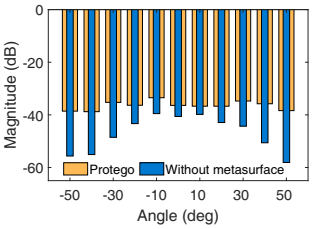


(a) Beamforming.

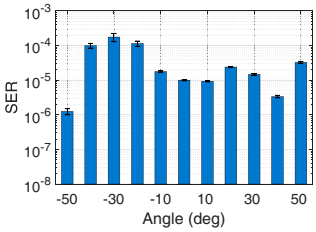


(b) Symbol error rate.

Figure 22: The beamforming and symbol error rate of backward link (i.e., receiver to transmitter).



(a) Beamforming.



(b) Symbol error rate.

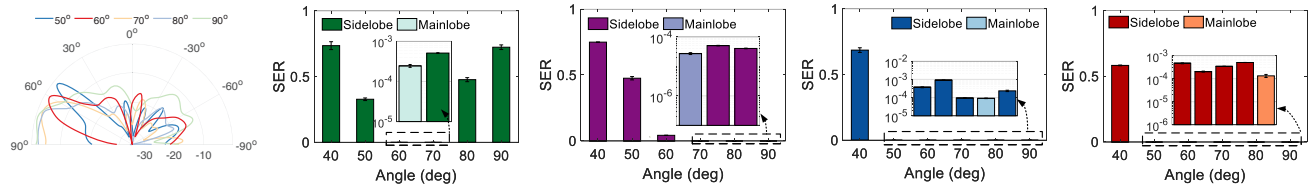
Figure 23: Impact of the legitimate user at different directions (i.e., $[-50°, 50°]$).

Performance under NLoS between MTS and Rx. In this experiment, we evaluate whether the sidelobe interferes with the mainlobe. The deployment scenario is shown in Figure 20(a). We use absorber materials to block the line-of-sight between the MTS and Rx. The absorbing material absorbs a large amount of signal energy and dramatically reduces the SNR, making the legitimate receiver barely able to decode the transmitted information. To emulate the effect of nearby reflecting objects, a reflector is placed at 1 m, 1.5 m, and 2 m from the mid-perpendicular of the Rx and MTS. We experiment with two types of reflector materials: tin foil and cardboard. Figure 20(b) illustrates the received signal strength and SER. In cases when the SNR is so low that the packet preamble cannot be decoded, the corresponding SER is marked as N/A. We observe that when the tin foil reflector is 1 m away from the mid-perpendicular, the signal strength of the mainlobe increases by 9 dB. However, the SER of the mainlobe also rises up to 0.65. The reason is that, the signals of the sidelobes, originally directed towards potential eavesdroppers, is now leaked to the desired receiver due to multipath reflections. Fortunately, when the distance of the reflector exceeds 1.5 m, the interference from the sidelobe is almost negligible. We emphasize that the LoS absorber plus strong tinfoil reflector is an extreme scenario. In practice, as long as the LoS dominates and the reflectors are not too close, the desired receiver is unlikely to be affected.

Performance under multiple eavesdroppers. In this experiment, we evaluate the Protego performance when multiple eavesdroppers coexist. The legitimate user stays at the default 0° position, and the four eavesdroppers are at $-40°$, $-20°$, 20°, and 40°, respectively. The results are shown in Figure 21(a). Except for the mainlobe, the SER all exceeds 0.7. In addition, Protego can effectively reduce the eavesdroppers' received signal strength. These results indicate that Protego can work effectively against multiple eavesdroppers.

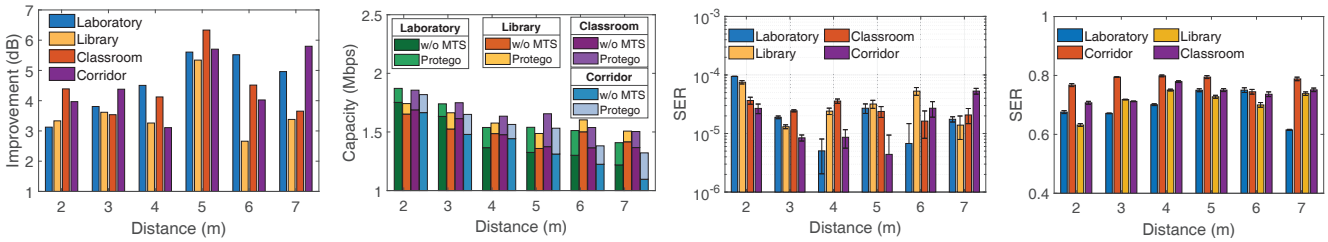
Performance of the backward link. By default, Protego protects the forward link (i.e., Tx to Rx), but it also brings side benefits to the backward link (Section 3). To verify this feature, we repeat the microbenchmark measurement but focus on the backward link (i.e., Rx to Tx). We separate the Tx and Rx by 3 m and the MTS is located at 30 cm in front of the Tx. Figure 22(a) shows that, the signal strength suppression is less than that of the forward link due to the location of the MTS remaining unchanged during forward link and backward link communication (i.e., Rx-MTS distance is 2.7 m). Figure 22(b) further shows that, the SER is large (0.4 to 0.63) except along the mainlobe direction, implying that an active attacker's command is unlikely to be decoded by the legitimate Tx.

Beamforming towards different mainlobe directions. In this experiment, we evaluate Protego when placing the legitimate Rx at different mainlobe directions. We deploy the Tx at the center of a semicircle (3 m radius) while the Rx moves along the semicircle from $-90°$ to 90° with a step of 10°. For different mainlobe directions, we use the relevant chaotic coding pattern set to evaluate whether the legitimate Rx can decode correctly. The results are shown in Figure 23 and Figure 24. From Figure 23(a), we can see that the Rx experiences the same signal strength from 50° to $-50°$ with a step of 10° after beamforming of Protego. The minimum, median, and maximum signal strength improvement are 3.1 dB, 9.6 dB, and 19.7 dB, respectively, relative to the case without the MTS. The improvements vary drastically because Protego is particularly effective for locations with lower signal strengths. Furthermore, Figure 23(b) illustrates the SER remains less than 1.7×10^{-4} almost in all mainlobes. These results verify that, Protego's beamforming and RCCS function work well as long as the Rx falls in the MTS's field of view. Figure 24 illustrates that if the mainlobe is directed towards 90°, Protego's performance is significantly dropped. According to Figure 24(a), the MTS is like a patch antenna array with a limited field of view of $[-60°, 60°]$. Meanwhile, from Figure 24(b)



(a) Beamforming (b) SER with mainlobe at 60°. (c) SER with mainlobe at 70°. (d) SER with mainlobe at 80°. (e) SER with mainlobe at 90°.

Figure 24: Impact of the legitimate user at ultra metasurface's field of view.



(a) Improvement. (b) Channel capacity. (c) SER of mainlobe. (d) SER of sidelobe.

Figure 25: Experimental results in different multipath environments.

to Figure 24(e), we can observe that the correct decoding range becomes significantly larger when the mainlobe moves towards 90°. For example, the correct decoding range is about [60°, 70°], [70°, 90°], [50°, 90°], and [50°, 90°] when the mainlobe is at 60°, 70°, 80°, and 90°, respectively. This issue can be solved by deploying multiple metasurfaces whose joint field-of-view can cover the entire 360°.

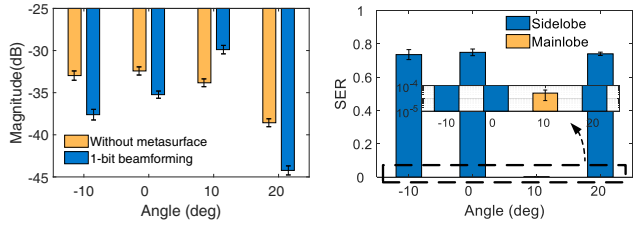
Impact of different environments. To evaluate the performance of Protego in different scenarios, we conduct extensive experiments in four indoor environments: a laboratory, a library, a classroom, and a spacious corridor. For each, we vary the Tx-Rx distance from 2 m to 7 m by the step of 1 m, while keeping the MTS 30 cm from the Tx. When the distance changes, the multipath effects cause variations in received signal strengths, but Protego achieves at least 2.6 dB (up to 6 dB) gain in both environments (Figure 25(a)). Compared with the best beamforming gain of the RFLens MTS under different environments (i.e., about 9 dB) [14], we lose around 3 dB in balancing the beamforming gain and security protection capability. Figure 25(b) further illustrates that Protego can consistently increase the link capacities (assuming 500 KHz bandwidth) as the distance increases, although the gain differs across environments. In addition, Figure 25(c) and Figure 25(d) illustrates the SER performance of the legitimate user (located at 0°) and the eavesdropper (located at 30°), we can see that the SER of the undesired sidelobes remains high in different environments while that of the mainlobe is extremely low, implying that the security protection of Protego is insensitive to multipath.

Performance in 3D space. In this experiment, we verify the performance of Protego in practical 3D scenarios, by varying φ_l instead of θ_l. We set the mainlobe towards (θ_l=10°,φ_l=10°). The eavesdropper is located at the direction from $\varphi_l = -10°$ to $\varphi_l = 20°$. Figure 26(a) reports that Protego can successfully achieve beamforming to the legitimate user. Figure 26(b) shows that the SER is below 3×10^{-4} along the mainlobe direction and above 0.7 otherwise, implying that Protego can work effectively in the 3D space.

Impact of different number of weak unit-cells on beamforming gain. We now explore how different number of "weak unit-cells" impacts the beamforming and SER performance, under the same setup as the previous experiment. We first obtain different number of "weak unit-cells" by changing ξ in Eq. (13), and generate a corresponding chaotic coding pattern set. Then, we measure the beamforming gain and SER in each case. Figure 27 shows that *as the number of weak unit-cells increases from 0 to 132, the beamforming improvement degrades from 8.52 dB to 3.62 dB, and the sidelobe SER performance increases from 0.038 to 0.748*, whereas the mainlobe SER is always lower than 2.9×10^{-5}. The results reveal an interesting *tradeoff between beamforming gain and obfuscation power against the eavesdropper*. To balance this tradeoff, we use 108 weak unit-cells by default in Protego. Note that the number of weak unit-cells utili zed for security protection is only related to the potential direction of eavesdroppers, rather than distance, relative to the Rx.

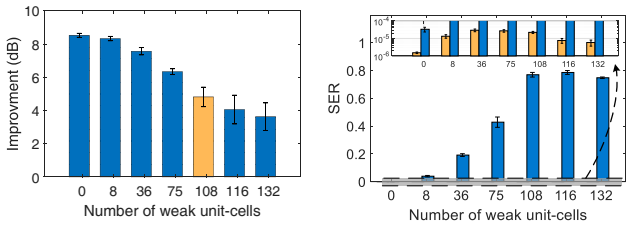
Impact of different number of weak unit-cells on beamwidth. To evaluate the tradeoff between the number of weak unit-cells and the mainlobe beamwidth, we conduct a simulation experiment. As shown in Figure 28, the beamwidth increases with the number of weak unit-cells, due to the smaller number of unit-cells used to shape a "pencil beam". Hence, to ensure Protego can achieve a good beamforming gain towards the mainlobe while obfuscating the information leaked to the sidelobes, we employ a moderate number of 108 weak unit-cells by default.

Impact of different entropy value and time consumption. We now evaluate how different entropy values impact the Protego performance. Recall the entropy indicates the obfuscation degree of constellation. The higher the entropy value, the more confusing the constellation will be for eavesdroppers. Figure 29 confirms this intuition. However, higher entropy values correspond to longer computational search time. When the entropy value is 0.5 and 0.6, the time cost is 25 and 135 minutes, respectively. To strike a balance between the time cost and the obfuscation degree, we choose the entropy value is 0.5 as the experimental setup.



(a) Beamforming. (b) Symbol error rate.

Figure 26: Beamforming and symbol error rate under 3D scenario.



(a) Beamforming. (b) Symbol error rate.

Figure 27: Beamforming VS. SER under different number of weak unit-cells.

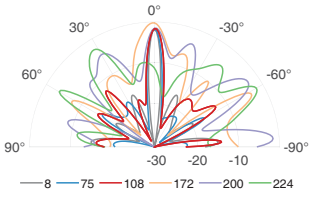


Figure 28: Beamwidth with different number of weak unit-cells.

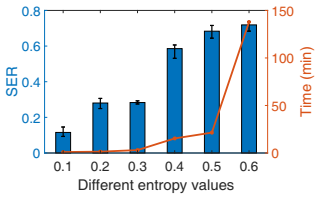


Figure 29: SER VS. time cost under different entropy values.

9 DISCUSSION AND FUTURE WORK

Eavesdropping attack on the mainlobe. Protego can defend against adversaries within the MTS's field of view. However, when an adversary is located along same direction as the legitimate Rx, it can still eavesdrop on the transmitted information. This is a common caveat of beamforming based physical layer security mechanisms [41]. Nevertheless, due to the RCCS obfuscation mechanism, Protego can already significantly improve the secrecy capacity compared with conventional beamforming solutions. Moreover, owing to the high-directionality created by the massive number of unit-cells, Protego can potentially squeeze the attacking zone to a "pencil beam" region, making it easier to expose the eavesdroppers. We note that this equivalently achieves a secrecy capacity gain of 180/10 = 18× compared with state-of-the-art beamforming methods such as RFLens [14]. By narrowing the attacking region, it becomes much easier to spot the eavesdroppers, if any. In addition, Protego can complement encryption-based methods to further improve the communication security when the adversary is located along the same direction as the legitimate Rx.

Multiple legitimate users. Our current Protego design focuses on a single legitimate Rx. Simultaneously achieving spatial domain and I/Q domain protection for multiple legitimate users is beyond our scope. One potential solution is to create multi-armed beams towards multiple receivers [14]. This will be the future exploration.

Mobile receivers. The current Protego design assumes the legitimate Rx stays at a known direction relative to the Tx. Protego can work for quasi-stationary scenarios in general, where the Rx occasionally moves. In such cases, Protego does need to perform beam steering to search for the mainlobe direction that maximizes the received signal strength, similar to RFLens [14]. This would induce certain communication and control overhead between the Tx and the MTS. Specifically, the Tx needs to tell the MTS the beam pattern index to be scanned. But such control-channel overhead is very small [14], so that a very simple communication link suffices. For example, we may use a simple digital control line or low-rate wireless link to connect the Tx and MTS. The actual implementation has been explored in recent works [10, 12, 14] and is beyond the scope of this paper.

Practicality and scalability of Protego. The current version of Protego needs to assume the Tx Alice's antenna has a certain degree of directionality, so that its outgoing signals can all go through the MTS, hence under its protection. Commodity patch antennas have intrinsic directionality that can satisfy this requirement [1]. On the other hand, Bob and Carol can use arbitrary types of antennas. As for deployment cost, the current prototype of Protego still occupies a large space relative to many tiny IoT devices, the advantage of the MTS is that it is a thin surface. So it can potentially be embedded into the facades of environment (e.g., furniture and walls) to reduce the footprint.

Modulation scheme. Current Protego only focuses on phase-based modulation schemes (i.e., n-PSK and n-QAM). For ASK-based modulation, Protego is feasible because different coding patterns correspond to the different radiation patterns. The actual implementation is left as our future work. Protego is not suitable for FSK since Protego MTS does not provide any frequency-shift functions.

10 CONCLUSION

This paper introduces Protego, a metasurface-aided system to protect the security of wireless links. By electronically reconfiguring a metasurface near the wireless transmitter, Protego can enhance the legitimate wireless link while obfuscating undesired communication with malicious users. Our prototype implementation demonstrates that Protego can enable up to 0.75 SER along potential eavesdropping directions, while keeping high beamforming gain (up to 19.7 dB) and extremely low SER (below 10^{-4}) in the legitimate receiver's direction. Protego also can protect against passive eavesdropping and enhance the legitimate wireless link in NLoS scenarios.

ACKNOWLEDGMENT

This work is supported by the NSFC A3 Foresight Program Grant 62061146001, and the National Natural Science Foundation of China 61972316. This work is also supported by the Shaanxi International Science and Technology Cooperation Program (2020KWZ-013). We thank our reviewers and shepherd for their insightful feedback which helped improve this paper.

REFERENCES

[1] [n.d.]. patch antenna. https://www.amazon.cn/s?k=patch+antennas.

[2] [n.d.]. SMP1340-040LF. https://www.skyworksinc.com/Products/Diodes/SMP1340-Series.
[3] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. 2020. BIAS: bluetooth impersonation attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 549–562.
[4] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. 2020. Key negotiation downgrade attacks on bluetooth and bluetooth low energy. *ACM Transactions on Privacy and Security (TOPS)* 23, 3 (2020), 1–28.
[5] Venkat Arun and Hari Balakrishnan. 2020. RFocus: Beamforming using thousands of passive antennas. In *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*. 1047–1061.
[6] C Baird and G Rassweiler. 1976. Adaptive sidelobe nulling using digitally controlled phase-shifters. *IEEE Transactions on Antennas and Propagation* 24, 5 (1976), 638–649.
[7] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. 2007. Public-key cryptography for RFID-tags. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. IEEE, 217–222.
[8] George Robert Blakley. 1979. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*. IEEE Computer Society, 313–313.
[9] Justin Chan, Kelly Michaelsen, Joanne K Estergreen, Daniel E Sabath, and Shyamnath Gollakota. 2022. Micro-mechanical blood clot testing using smartphones. *Nature communications* 13, 1 (2022), 1–12.
[10] Lili Chen, Wenjun Hu, Kyle Jamieson, Xiaojiang Chen, Dingyi Fang, and Jeremy Gummeson. 2020. Pushing the Physical Limits of IoT Devices with Programmable Metasurfaces. *arXiv preprint arXiv:2007.11503* (2020).
[11] Kun Woo Cho, Mohammad H Mazaheri, Jeremy Gummeson, Omid Abari, and Kyle Jamieson. 2021. mmWall: A Reconfigurable Metamaterial Surface for mmWave Networks. In *Proceedings of the 22nd International Workshop on Mobile Computing Systems and Applications*. 119–125.
[12] Manideep Dunna, Chi Zhang, Daniel Sievenpiper, and Dinesh Bharadia. 2020. ScatterMIMO: Enabling virtual MIMO with smart surfaces. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom)*. 1–14.
[13] Mohammed E Eltayeb, Junil Choi, Tareq Y Al-Naffouri, and Robert W Heath. 2016. On the security of millimeter wave vehicular communication systems using random antenna subsets. In *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE, 1–5.
[14] Chao Feng, Xinyi Li, Yangfan Zhang, Xiaojing Wang, Liqiong Chang, Fuwei Wang, Xinyu Zhang, and Xiaojiang Chen. 2021. RFlens: metasurface-enabled beamforming for IoT communication and sensing. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 587–600.
[15] Keming Feng, Xiao Li, Yu Han, Shi Jin, and Yijian Chen. 2020. Physical layer security enhancement exploiting intelligent reflecting surface. *IEEE Communications Letters* 25, 3 (2020), 734–738.
[16] R Ghayoula, N Fadlallah, A Gharsallah, and M Rammal. 2009. Phase-only adaptive nulling with neural networks for antenna array synthesis. *IET microwaves, antennas & propagation* 3, 1 (2009), 154–163.
[17] Dennis Goeckel, Sudarshan Vasudevan, Don Towsley, Stephan Adams, Zhiguo Ding, and Kin Leung. 2011. Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. *IEEE Journal on Selected Areas in Communications* 29, 10 (2011), 2067–2076.
[18] Satashu Goel and Rohit Negi. 2008. Guaranteeing secrecy using artificial noise. *IEEE transactions on wireless communications* 7, 6 (2008), 2180–2189.
[19] Jeremy J Gummeson, Bodhi Priyantha, Deepak Ganesan, Derek Thrasher, and Pengyu Zhang. 2013. EnGarde: Protecting the mobile phone from malicious NFC interactions. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*. 445–458.
[20] Unsoo Ha, Salah Assana, and Fadel Adib. 2020. Contactless seismocardiography via deep learning radars. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*. 1–14.
[21] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. 2015. Securing RFIDs by Randomizing the Modulation and Channel. In *12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15)*. 235–249.
[22] Randy L Haupt. 1997. Phase-only adaptive nulling with a genetic algorithm. *IEEE Transactions on Antennas and Propagation* 45, 6 (1997), 1009–1015.
[23] Suraj Jog, Jiaming Wang, Junfeng Guan, Thomas Moon, Haitham Hassanieh, and Romit Roy Choudhury. 2019. Many-to-many beam alignment in millimeter wave networks. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 783–800.
[24] Karl Koscher, Ari Juels, Vjekoslav Brajkovic, and Tadayoshi Kohno. 2009. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. In *Proceedings of the 16th ACM conference on Computer and communications security*. 33–42.
[25] Yuezhou Li, ME Bialkowski, KH Sayidmarie, and NV Shuley. 2010. 81-element single-layer reflectarray with double-ring phasing elements for wideband applications. In *2010 IEEE Antennas and Propagation Society International Symposium*. IEEE, 1–4.
[26] Zhuqi Li, Yaxiong Xie, Longfei Shangguan, Rotman Ivan Zelaya, Jeremy Gummeson, Wenjun Hu, and Kyle Jamieson. 2019. Towards programming the radio environment with large arrays of inexpensive antennas. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*. 285–300.
[27] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. 2017. Systematically evaluating security and privacy for consumer IoT devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. 1–6.
[28] Chuang Lu, Yan Wu, Reza Mahmoudi, Marion K Matters-Kammerer, and Peter GM Baltus. 2012. A mm-wave analog adaptive array with genetic algorithm for interference mitigation. In *2012 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2373–2376.
[29] Sohrab Madani, Suraj Jog, Jesus O Lacruz, Joerg Widmer, and Haitham Hassanieh. 2021. Practical null steering in millimeter wave networks. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*. 903–921.
[30] Federico Marini and Beata Walczak. 2015. Particle swarm optimization (PSO). A tutorial. *Chemometrics and Intelligent Laboratory Systems* 149 (2015), 153–165.
[31] Amitav Mukherjee and A Lee Swindlehurst. 2010. Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Transactions on Signal Processing* 59, 1 (2010), 351–361.
[32] Rohit Negi and Satashu Goel. 2005. Secret communication using artificial noise. In *IEEE vehicular technology conference*, Vol. 62. Citeseer, 1906.
[33] John Nolan, Kun Qian, and Xinyu Zhang. 2021. RoS: passive smart surface for roadside-to-vehicle communication. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*. 165–178.
[34] Yanjun Pan, Ziqi Xu, Ming Li, and Loukas Lazos. 2021. Man-in-the-middle attack resistant secret key generation via channel randomization. In *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*. 231–240.
[35] Jake Bailey Perazzone, L Yu Paul, Brian M Sadler, and Rick S Blum. 2021. Artificial noise-aided MIMO physical layer authentication with imperfect CSI. *IEEE Transactions on Information Forensics and Security* 16 (2021), 2173–2185.
[36] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. 2016. PhyCloak: Obfuscating Sensing from Communication Signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. 685–699.
[37] Sekhar Rajendran, Zhi Sun, Feng Lin, and Kui Ren. 2020. Injecting reliable radio frequency fingerprints using metasurface for the Internet of Things. *IEEE Transactions on Information Forensics and Security* 16 (2020), 1896–1911.
[38] Madhusudan Singh and Shiho Kim. 2018. Branch based blockchain technology in intelligent vehicle. *Computer Networks* 145 (2018), 219–231.
[39] Nicolas Sklavos and I. D. Zaharakis. 2016. Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. 1–2.
[40] Elahe Soltanaghaei, Akarsh Prabhakara, Artur Balanuta, Matthew Anderson, Jan M Rabaey, Swarun Kumar, and Anthony Rowe. 2021. Millimetro: mmWave retro-reflective tags for accurate, long range localization. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. 69–82.
[41] Daniel Steinmetzer, Joe Chen, Jiska Classen, Edward Knightly, and Matthias Hollick. 2015. Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves. In *2015 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 335–343.
[42] Xin Tan, Zhi Sun, Dimitrios Koutsonikolas, and Josep M. Jornet. 2018. Enabling Indoor Mobile Millimeter-wave Networks Based on Smart Reflect-arrays. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 270–278. https://doi.org/10.1109/INFOCOM.2018.8485924
[43] Wade Trappe, Richard Howard, and Robert S Moore. 2015. Low-energy security: Limits and opportunities in the internet of things. *IEEE Security & Privacy* 13, 1 (2015), 14–21.
[44] Ju Wang, Liqiong Chang, Shourya Aggarwal, Omid Abari, and Srinivasan Keshav. 2020. Soil moisture sensing with commodity RFID systems. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. 273–285.
[45] Song Wang, Jingqi Huang, Xinyu Zhang, Hyoil Kim, and Sujit Dey. 2020. X-array: Approximating omnidirectional millimeter-wave coverage using an array of phased arrays. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom)*. 1–14.
[46] Allen Welkie, Longfei Shangguan, Jeremy Gummeson, Wenjun Hu, and Kyle Jamieson. 2017. Programmable radio environments for smart spaces. In *Proceedings of the 16th ACM Workshop on Hot Topics in Networks*. 36–42.
[47] Qingqing Wu and Rui Zhang. 2019. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. *IEEE Communications Magazine* 58, 1 (2019), 106–112.
[48] Meng Zhang, Anand Raghunathan, and Niraj K Jha. 2013. MedMon: Securing medical devices through wireless monitoring and anomaly detection. *IEEE Transactions on Biomedical circuits and Systems* 7, 6 (2013), 871–881.

[49] Qianqian Zhang, Ying-Chang Liang, and H Vincent Poor. 2020. Large intelligent surface/antennas (LISA) assisted symbiotic radio for IoT communications. *arXiv preprint arXiv:2002.00340* (2020).

[50] Renjie Zhao, Timothy Woodford, Teng Wei, Kun Qian, and Xinyu Zhang. 2020. M-cube: A millimeter-wave massive MIMO software radio. In *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (MobiCom)*. 1–14.

[51] Yue Zheng, Yi Zhang, Kun Qian, Guidong Zhang, Yunhao Liu, Chenshu Wu, and Zheng Yang. 2019. Zero-effort cross-domain gesture recognition with Wi-Fi. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services*. 313–325.

[52] X. Zhou and M. R. Mckay. 2010. Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation. 59, 8 (2010), 3831–3842.

[53] Yulong Zou, Jia Zhu, Xianbin Wang, and Lajos Hanzo. 2016. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* 104, 9 (2016), 1727–1765.