Metasurface-enabled smart wireless attacks at the physical layer

Menglin Wei
peking university

Hanting Zhao
peking university

Vincenzo Galdi
University of Sannio https://orcid.org/0000-0002-4796-3600

Lianlin Li
peking university https://orcid.org/0000-0001-9394-3638

Tie Jun Cui (✉ tjcui@seu.edu.cn)
State Key Laboratory of Millimeter Waves https://orcid.org/0000-0002-5862-1497

Article

Keywords:

Posted Date: August 5th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1857836/v1

Metasurface-enabled smart wireless attacks at the physical layer

Menglin Wei[1,+], Hanting Zhao[1,+], Vincenzo Galdi[2], Lianlin Li[1], Tie Jun Cui[3]

[1] State Key Laboratory of Advanced Optical Communication Systems and Networks,
School of Electronics, Peking University, Beijing 100871, China

[2] Department of Engineering, University of Sannio, Corso Garibaldi 107, I-82100 Benevento, Italy

[3] State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, China

[+] These authors contributed equally to this work.

Abstract

Information security is of paramount importance in the modern society, and it is crucial that communication systems are conceived and implemented in order to be inherently resilient in this respect. In current wireless communication systems, some of the most sophisticated attack strategies aim at the physical layer, i.e., at the electromagnetic wave signal carrying the information, but the implied physical interaction with the target inherently leaves traces in the physical environment, which render these attacks typically detectable. However, this may not be the case for future (the 6th generation and beyond) wireless networks, whose current vision relies on the concept of "smart radio environment", empowered by suitably engineering reflecting devices (also called as metasurfaces) that can manipulate the wave signals in unconventional fashions (e.g., non-specular reflections) and that can be reconfigured at will. These metasurface elements, which should be pervasively deployed and suitably disguised in the indoor and outdoor environment, potentially introduce new vulnerabilities to the physical-layer attacks that should be fully understood and addressed. To this aim, here, we put forward the concept of smart wireless attacks at the physical layer by exploiting the unique capabilities of programmable metasurfaces in the joint manipulations of radio waves and digital information in a wireless scenario. Specifically, we illustrate both passive and active operational modes. In the passive mode, an attacker is capable of eavesdropping and breaking the target wireless information transfer by controlling the programmable metasurface, without radiating any signal actively. In the active mode, an attacker can not only eavesdrop but also furtively falsify the target wireless communications by sending some deceptive information to the target. In both operational modes, the detectability of the attacker can be minimized. As a proof of concept, we design and realize an attacker prototype working in the Wi-Fi band around 2.4GHz, and demonstrate experimentally its ability to hack wireless data streams. Our results raise awareness on the new types of security threats and challenges that the next-generation wireless networks will likely have to face, and indicate that suitable mitigation strategies and specific security protocols need to be conceived and developed at the present stage, while the smart-radio-environment concept is still in its infancy.

Introduction

In recent years, physical-layer security (PLS) has been widely concerned, and several techniques, such as noise, interference and diversity, have been proposed to improve the secrecy performance of wireless systems.[1–3] As the information security is becoming of paramount importance in modern society, cryptographic encryption methods are designed to be increasingly more complex and reliable. Therefore, direct attacks at the physical layer are becoming a more viable alternative, especially in the wireless communications, with the signals propagating in an unbound physical space and the consequent risk of information leakage. Conventional physical-layer attackers utilize diverse penetration methods such as vulnerability analysis, information gathering, traffic analysis, replay attack, forensic sniffing and spoofing tools, maintaining access, reverse engineering, hardware hacking, etc. Nevertheless, almost all these types of attackers inevitably leave traces in the physical space, which makes them vulnerable and traceable. However, the current trends in wireless communications, with increasing reliance on advanced control and manipulation of electromagnetic (EM) waves at the physical layer, may inspire novel types of attacks that are much more sophisticated and harder to detect.

Modern information systems typically rely on massive antenna arrays in combination with the beamforming techniques to simultaneously improve the range of wireless links and to reduce unwanted interferences.[1] However, this bulky, costly and power-hungry hardware increasingly struggles to meet the requirements of ever-growing amounts of connection nodes, especially with the advent of the "green" internet of things.[2] Within this framework, programmable coding metasurfaces are emerging as an attractive alternative paradigm for advanced EM wave manipulation.[3–5] These ultrathin and inexpensive arrays of *in-situ* programmable meta-atoms hold great technological promises thanks to their ability to control EM waves in flexible and powerful fashions. Initially, these platforms were designed to serve on the transmitter side in combination with a carefully deployed antenna source, as an attractive alternative to phased-array antennas for beamforming in (quasi) free space.[3,6,7] More generally, they can be viewed as a multi-port device linking in an adaptive manner multiple input channels (sources) to multiple output channels (receivers), in terms of geometrical (number and location) and physical (signal response) port properties.[8] These platforms, under the broad umbrella of "reconfigurable intelligent surfaces,"[9,10] can be actively integrated within the propagation environment, endowing it with programmability that can be used as an alternative relaying mechanism in (quasi) free space, to optimize the available channels in scattering-rich environments.[11] The concept of "smart radio environment"[12,13] is at the core of the grand vision for future (the 6th-generation and beyond) wireless communication systems,[14] and relies on metasurfaces as a key enabling technology.[15] Moreover, different metasurface-enabled encryption schemes have been recently proposed in optics.[16,17]

Besides the aforementioned advantages, the envisioned pervasive deployment of (passive and active) metasurface elements disguised in the propagation environment (e.g., in the form of wallpapers, window glasses, building facades, roadside billboards) also introduces new types of vulnerabilities to physical-layer attacks, since they could also be exploited maliciously to hack the system. These potential vulnerabilities and threats need to be carefully explored and understood upfront in order to conceive future network architectures that are inherently resilient. A basic principle of physical-layer security is to increase the performance difference between a legitimate receiver and an eavesdropper link by means of suitable beamforming for transmitting antennas and/or sending noise or interference signals to eavesdroppers. For attackers, this security measure can be overcome by deploying a large reflective antenna array in the channel to manipulate the wireless links. However, such bulky and power-hungry equipment is clearly not suitable for low-detectability attacks. Conversely, metasurfaces can be easily hidden in the environment, and still provide powerful beam and signal manipulation capabilities for physical-layer wireless attackers. For instance, it was recently demonstrated that a quickly and inexpensively fabricated (passive) metasurface could be effectively used to eavesdrop a millimeter-wave communication channel in an essentially undetectable fashion.[18]

Here, we put forward and demonstrate a new scheme of smart wireless attacks at the physical layer based on programmable metasurfaces, which can operate on Wi-Fi signals, and may be rendered essentially undetectable. Unlike conventional (passive) metasurfaces, which enable eavesdropping by redirecting part of the signal toward an unintended user,[18] programmable metasurfaces can actively transmit information via backscattering wireless communication schemes that leverage commodity Wi-Fi signals,[19,20] which considerably expands the range of potential wireless attacks. As conceptually illustrated in Fig. 1, besides conventional eavesdropping, our proposed scheme enables smarter types of attacks that can alter the information exchanged with multiple users at will and in real-time. Our results, which can be readily extended to other wireless communications scenarios, raise awareness of inherent vulnerabilities that could become very critical in smart radio environments of interest for future wireless networks.

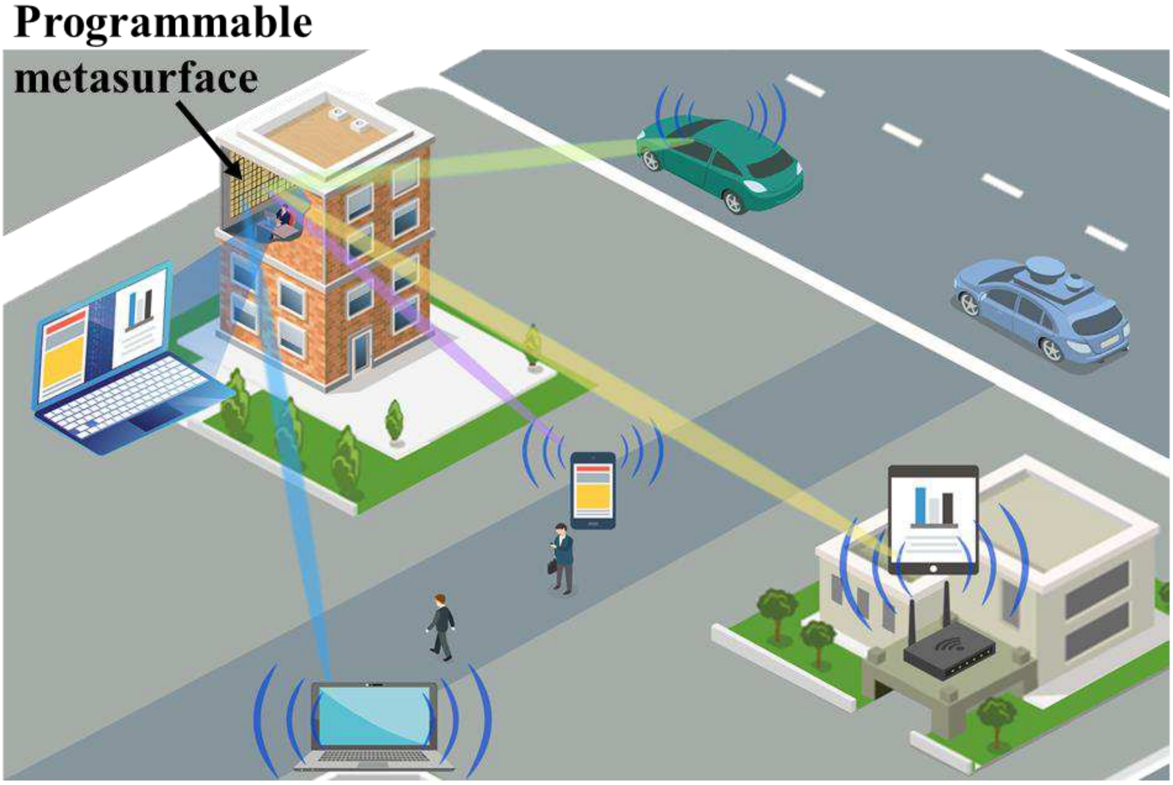

Figure 1. Conceptual illustration of a metasurface-enabled smart wireless attack. A scenario for hacking a wireless local-area network (WLAN) in a typical indoor environment, where a wireless attacker eavesdrops and falsifies the clients' information via metasurface-enabled directional wireless communication links. Here, four clients (laptop, mobile phone, router and car) are considered.

Results

System configuration. The schematics of our proposed wireless attackers (passive and active) are illustrated in Fig. 2. For illustration purposes, the system is designed to operate at a frequency of 2.4GHz, and, to facilitate our implementation, a universal software radio peripheral (Ettus USRP X310) is utilized to generate or/and acquire the radio signals. In the passive mode (Fig. 2a), a legitimate transmitter (Alice) intends to transfer the information to a legitimate receiver (Bob) via wireless communication, while an attacker (Eve) attempts to eavesdrop the communication channel at the physical layer without actively radiating any radio signals, by deploying and controlling a programmable metasurface in the surrounding physical environment. In particular, the attacker snoops around the channel and captures Alice's data packets, by relying on the metasurface, which serves as a controllable relay by establishing an eavesdropping link with high capacity and suitably re-directing the wireless signals. Alternatively, the attacker may aim at disrupting the communication between Alice and Bob. All these types of attacks can be implemented via suitable control of the EM response of each tunable meta-atom composing the metasurface (see Materials and Methods for more details).

In the active mode (Fig. 2b), besides eavesdropping the information, Eve also intends to furtively falsify the information directed to Bob by transmitting deceptive data. In this scenario, the programmable metasurface plays an additional pivotal role, by serving as a backscattering wireless communication system,[19,20] under illumination by a single-tone carrier radio signal generated by the USRP. More specifically, as for the passive mode, Eve controls the metasurface to establish a directional wireless link with Alice (eavesdropping link), and then utilizes the USRP to collect the signal intended to Bob. Furthermore, Eve controls the same metasurface also to establish a directional wireless link with Bob (falsifying link) to transmit the deceptive information (see Materials and Methods for more details).

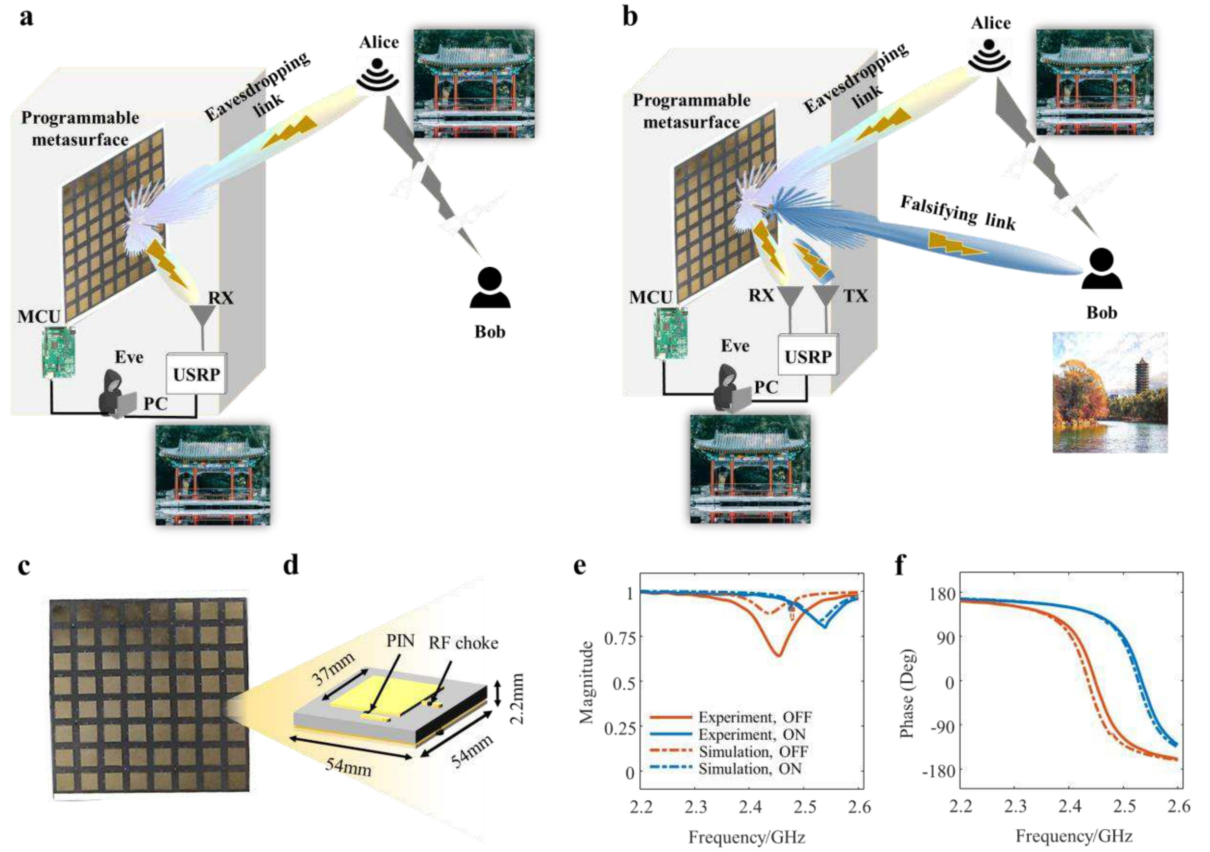

Figure 2. System configuration of a metasurface-enabled smart wireless attack. a Passive mode: Alice intends to transfer the information to Bob (legitimate user), via wireless communication, and Eve is an eavesdropper that attempts to capture (or disrupt) the information directed to Bob by exploiting a programmable metasurface deployed in the surrounding environment. **b** Active mode: Besides eavesdropping, Eve also intends to falsify Bob's information by transmitting the deceptive data via a metasurface-modulated backscattering wireless communication scheme. Rx: receiver; Tx: transmitter; PC: personal computer; URSP: universal software radio

peripheral, MCU: micro control-unit. **c** Front-view photo of a programmable metasurface panel comprising 8×8 meta-atoms; the entire metasurface consists of 3×4 identical panels. **d** Schematic of the designed meta-atom controlled by a PIN diode. **e,f** Comparison between amplitude and phase responses, respectively, of the simulated and experimental reflection coefficient of a meta-atom, as a function of frequency, for the two possible states (ON/OFF) of the PIN diode.

Programmable metasurface. Our proposed attacker relies on a one-bit coding programmable metasurface, designed to work at around 2.4 GHz, corresponding to the frequency range of commodity 2.4GHz Wi-Fi signals. The whole metasurface has a size of 1.7×1.3m^2, and comprises 32×24 independently controllable meta-atoms (each of size 54×54mm^2), arranged in 3×4 identical panels (each comprising 8×8 meta-atoms, see Fig. 2c) due to fabrication-related size restrictions. As shown in Fig. 2d, each meta-atom is integrated with a positive-intrinsic-negative (PIN) diode, and can exhibit two possible physical states (labelled with the bits "0" and "1") corresponding to two opposite reflection phases (i.e., 0 and 180°, respectively) under plane-wave illumination, when the PIN diode is switched from ON to OFF (and vice versa) within the frequency range 2.41-2.48 GHz. Such phase change can be attained by switching the bias direct-current (DC) voltage applied to the PIN diode from 3.3V to 0V. As shown in Figs. 2e and 2f, this condition can be attained at the desired operation frequency, with good agreement between numerical simulations and measurements. To enable real-time and flexible control of all 768 PIN diodes, a micro control-unit (MCU) of size of 95×145mm^2 is designed and assembled on the upper rear of the metasurface. The MCU relies on a field-programmable gate array (FPGA) circuit, and is responsible for dispatching all commands sent from a master computer subject to one common clock signal; in our work, the adopted clock is 100MHz, and the switching time of the PIN diode is about 2μs each cycle (see Materials and Methods and Supplementary Note 1 for more details). In this way, the EM response of the metasurface can be dynamically and flexibly manipulated by suitably controlling its binary coding pattern.

As previously mentioned, the programmable metasurface is designed at Eve's side to play two critical roles: i) eavesdropping the legitimate information directed from Alice to Bob, by altering the signal propagation path, and ii) falsifying the information received at Bob's side by sending deceptive data via a point-to-point backscattering wireless communication link.[19,20] For this twofold aim, the design of the binary-coding control sequence of the programmable metasurface can be addressed by maximizing the following objective function:

$$J = \underbrace{\left(\log_2\left(\frac{P_{\mathrm{EA}}}{\sigma_{\mathrm{EA}}^2}\right) - \alpha\log_2\left(\frac{P_{\mathrm{BA}}}{\sigma_{\mathrm{BA}}^2}\right)\right)}_{\mathrm{R_e}} + \beta\underbrace{\log_2\left(\frac{P_{\mathrm{BE}}}{\sigma_{\mathrm{BE}}^2}\right)}_{\mathrm{R_f}} \qquad (1)$$

which follows from Ref. 21 with some important modifications, as detailed below. Here, the subscripts A, B, and E indicate Alice, Bob, and Eve, respectively. For instance, we denote by P_{BA} and σ_{BA}^2 the received signal and noise powers, respectively, at Bob's side when an information-encoded signal is transmitted from Alice's side; the meaning of the other symbols can be inferred readily (see also Materials and Methods for more details). The term $\mathrm{R_e}$ quantifies the eavesdropping communication rate, reflecting the relative eavesdropping performance of Eve with respect to Bob in terms of the communication capacity. Since our scope here is different from that in Ref. 21, we introduce a positive coefficient α to balance the potential constraint imposed on the legitimate communication link. In particular, setting $\alpha = 0$ implies that the legitimate link is largely unaffected, and thus the eavesdropping link is essentially undetectable at Bob's side. On the other hand, the term $\mathrm{R_f}$ characterizes the falsifying performance of Eve. Considering that the wireless communication channels are usually reciprocal, it turns out that the optimal solutions for both $\mathrm{R_e}$ and $\mathrm{R_f}$ cannot be simultaneously achieved, and therefore a positive trade-off factor β is introduced in Eq. (1). We highlight that the optimization in Eq. (1) is very challenging from the computational viewpoint, since it entails an NP-hard combinational problem, and the Green's function of the underlying physical environment is not known analytically. In our approach, as detailed in Supplementary Note 2, we employ a line-search algorithm initialized with the modified Gerchberg-Saxton (G-S) method.

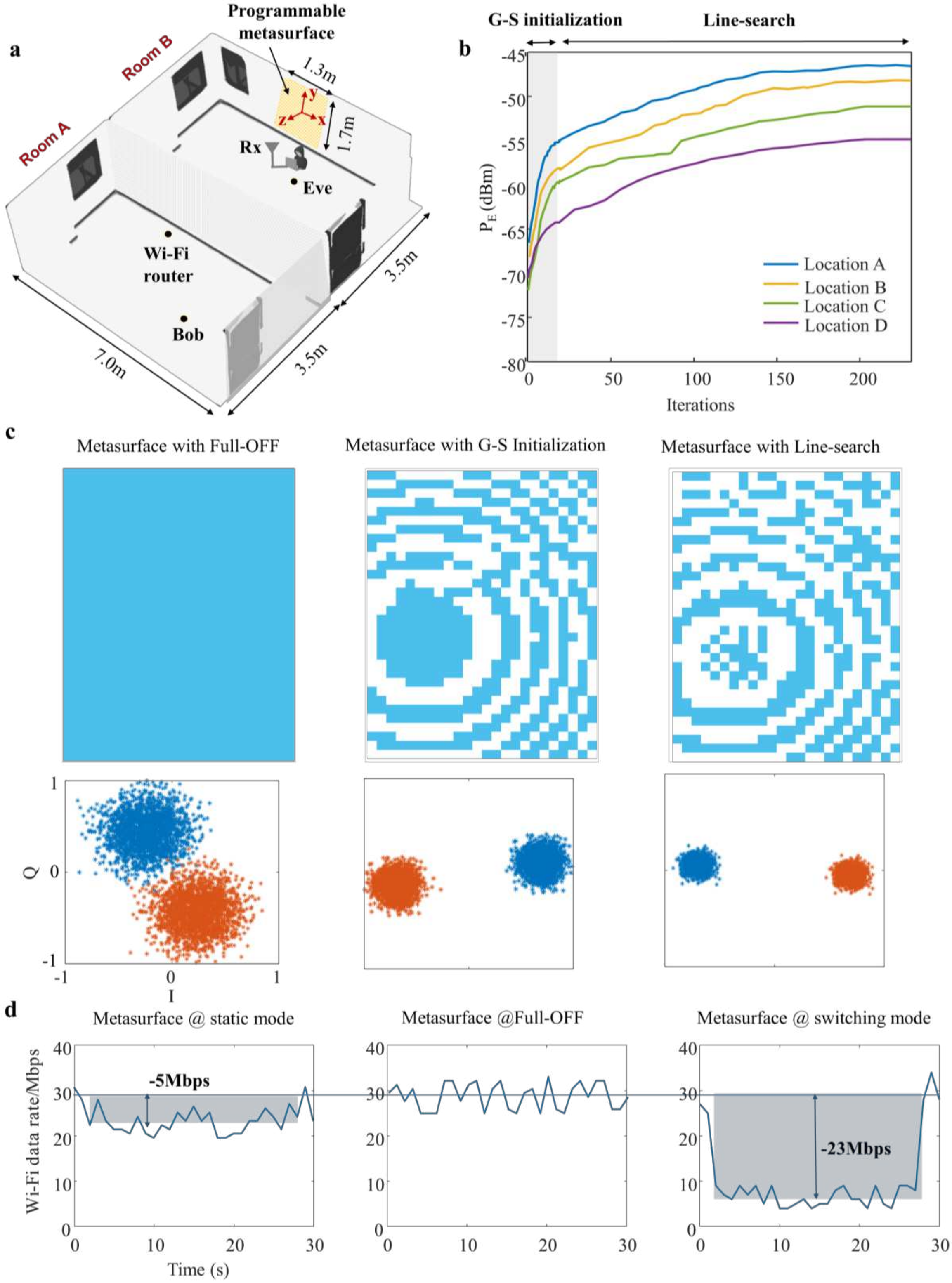

Figure 3. Selected experimental results on passive attacks. a Experimental setup: Eve (in room B) attempts to eavesdrop the information intended to Bob from Alice (in room A) by controlling the metasurface; Rx denotes the

receiver at Eve's side. **b** Eavesdropping power at Eve (P_E) as a function of the iteration order in the metasurface coding-pattern optimization, for four different Rx locations. **c** Top row: Metasurface coding patterns in the full-OFF state (left), G-S initialization (center), and line-search optimization result (right); the blue and white squares correspond to the OFF and ON states, respectively, for the meta-atoms. Bottom row: Corresponding constellation diagrams of the Wi-Fi signals decoded at Eve's side. **d** Wireless communication rates detected at Bob's side for the metasurface configured with the optimized coding pattern (left), full-OFF state (center), dynamically switching patterns (right).

Experimental results on passive attacks. We first assess the performance of the developed wireless metasurface attacker in the passive mode. As schematized in Fig. 3a for our experimental setting, Eve (in room B) attempts to eavesdrop the information intended to Bob from Alice (in room A) by controlling the programmable metasurface. In our implementation, Alice is a commodity Wi-Fi router (Mercury MW150R) working with a binary phase-shift keying (BPSK) modulation and the 802.11b protocol at the 7th subchannel of 2.442GHz. When Eve tries to snoop the Wi-Fi information intended to Bob from Alice, the programmable metasurface acts as a controllable passive relay that suitably redirects the Wi-Fi signal over the established eavesdropping link. To this end, the control coding pattern of the programmable metasurface needs to be determined, which can be achieved by maximizing $\mathrm{R_e}$ in Eq. (1), along with $\beta = 0$ and $\alpha = 1$. The procedure is initialized by exploiting the modified G-S algorithm, and then a line-search is implemented. Figure 3b shows the power levels P_E received at Eve's side as a function of the iteration order in the optimization process, for different Bob's locations: Location A (0.2m, 1m, 4.0m), Location B (0.5m, 2m, 4m), Location C (0.2m, 1m, 4m) and Location D (0.2m, 0.2m, 4.5m), with Eve and Alice located at (-0.1m, 0.1m, 1.2m) and (0.1m, 1m, 4m), respectively. Figure 3c shows some representative coding patterns of the metasurface for the full-OFF state (i.e., all meta-atoms in the OFF state, equivalent to a conventional metallic reflector), the G-S initialization, and the result of the line-search optimization, together with the corresponding BPSK constellation diagrams of the decoded wireless signals eavesdropped at Eve's side, from which we can visually estimate the quality of the transmission. In particular, we observe a progressive improvement (in terms of reduced spread in the constellation points) going from the full-OFF state to the optimized one, which can be quantified in a about 16 dB power enhancement of information eavesdrop on average (see Fig. 3b), without extra energy consumption. Moreover, Fig. 3d (left and center panels) show the communication data rates detected at Bob's side pertaining to the optimized and full-OFF coding patterns, respectively. We observe that, as a consequence of the eavesdropping link, the target communication link between Alice and Bob is moderately deteriorated with a loss of 5Mbps on average, as highlighted by the blue shaded area. This can be expected since part of Alice's signal energy has been redirected toward Eve by the programmable metasurface. As previously mentioned, the effect on Bob's communication rate from the eavesdropping link can be minimized by solving the optimization problem in Eq. (1) with $\alpha = 0$ (see Supplementary Note 3).

In addition, our proposed wireless attacker is capable of breaking down the communication between Alice and Bob by switching rapidly the coding patterns of the metasurface, with an extra energy consumption of a few watt. To demonstrate this possibility, Fig. 3d illustrates the results (in terms of data rate) of a set of experiments where the control coding pattern of the metasurface is switched between the full-OFF and the optimized result with a switching period of 2μs. It can be observed that the communication rate from Alice to Bob can be remarkably decreased by ~23Mbps when the eavesdropping link is dynamic. This can be expected since the dynamic eavesdropping link can not only decrease remarkably Bob's received power (and hence the signal-to-noise ratio), but it also breaks the stationary property of the wireless channel.

Experimental results on active attacks. We now move on to assessing the performance of the proposed wireless attacker in the active mode. For illustration purposes, and to avoid the complicated key decryption at the digital level, the Wi-Fi signal at Alice's side is generated by means of the USRP. With reference to the experimental setting schematized in Fig. 4a (with parameters in Table 1), Eve (in room B) tries to eavesdrop and falsify the information intended to Bob and Carol from Alice (in room A), while remaining essentially untraceable for a possible detector (Dave). To this aim, by controlling the metasurface, Eve establishes two independent falsifying links with Bob and Carol, and actively transmits two independent deceptive data streams to them. Thus, there are now two kinds of wireless links: the eavesdropping one and the falsifying ones. To render Eve's communications with Bob and Carol furtive, we optimize the control binary coding pattern of the metasurface with the two-fold objective of: i) maximizing the falsifying communication rate (R_f), and ii) transferring the counterfeit data to Bob and Carol by exploiting a modulated-metasurface backscattering wireless communication scheme.[19,20] Basically, the deceptive data is directly encoded into the programmable metasurface, which is illuminated by a 2.442GHz single-tone carrier, and radiates directive beams so as to minimize Eve's detectability. Accordingly, the metasurface is controlled in such a way such that the three information-carrying radiation beams pointing towards Bob, Carol and Eve can be generated and manipulated independently. Here, for illustration purposes, we consider a *physical* BPSK modulation for the falsifying wireless links (from Eve to Bob and Carol). On the other hand, the eavesdropping link (from Alice to Eve) works in a different fashion, since it is utilized for energy manipulation and does not rely on the metasurface modulation[7] (see Materials and Methods for more details on both schemes). As a consequence, we need to design four control patterns of the metasurface for the resulting three-channel backscattering wireless communication, where the channels 1, 2 and 3 correspond to Eve, Bob and Carol, respectively.

Figure 4b shows the eavesdropping and falsifying power levels at Eve, Bob, and Carol (P_E, P_B, and P_C, respectively) as a function of the iteration order of the optimization process, whereas Fig. 4c shows the four optimized binary coding patterns. Assuming that a red-green-blue (RGB) image is transferred from Alice to Bob, Eve can not only eavesdrop this image by manipulating the programmable metasurface (leftmost panel in Fig. 4d**)**, but can also arbitrarily falsify the images at Bob's and Carol's sides, as shown, for instance, in the second and rightmost panels of Fig. 4d, respectively. In addition, to highlight the metasurface-enabled capability of energy refocusing within an intended local spot, we also monitor the performance of a detector (Dave) placed in the vicinity of Bob (see Fig. 4b). The third panel of Fig. 4d shows the image received at Dave's side, whose significantly poorer quality demonstrates the low visibility of the attack, in spite of some leaking information around Bob. Additional results are also available in Supplementary Video 1. In addition, the top row of Fig. 4e shows typical (17ms-long) Wi-Fi signals received at Bob's, Eve's, Dave's and Carol's sides, with some magnified details shown in the bottom row, and the corresponding decoded constellation diagrams shown in Fig. 4f, from which the significantly poorer quality of the signal at Dave's side is also apparent. On the basis of these results, we can conclude that the proposed metasurface-based wireless attacker is capable of eavesdropping, disrupting and/or falsifying simultaneously the data streams in complicated indoor environments, while maintaining a low detectability.

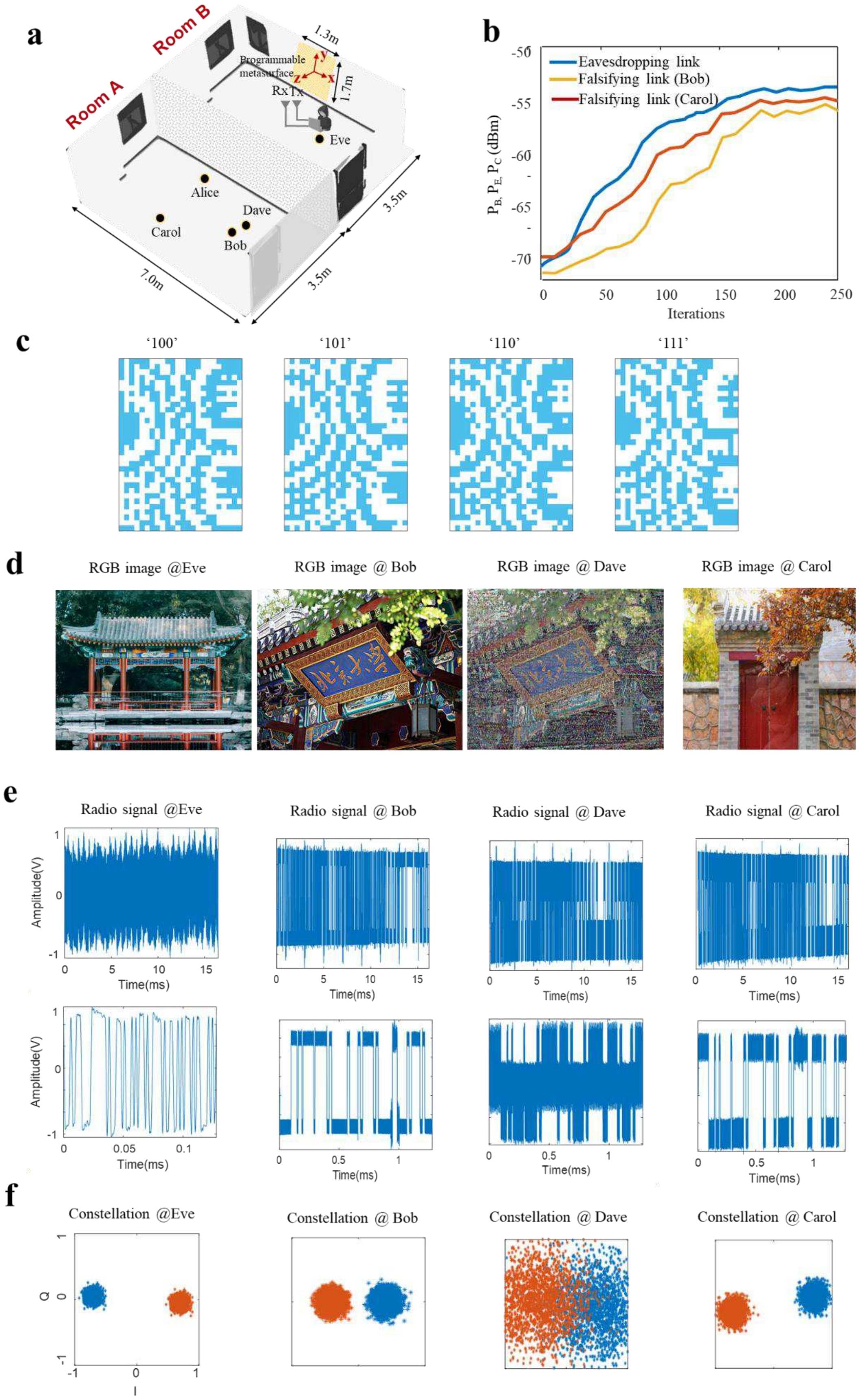

Figure 4. Selected experimental results on active attacks. a Experimental setup: Eve (in room B) tries to eavesdrop and falsify the information intended to Bob and Carol from Alice (in room A), in the presence of a nearby detector (Dave); Rx and Tx denotes the receiver and single-tone transmitter, respectively, at Eve's side.

The locations are: Alice (0.1m, 1m, 5m), Bob (0.1, -0.6m, 5.5m), Carol (0.3m, 0.6m, 4m), Dave (0.1m, -1.3m, 5.5m), Eve_Tx (-0.1m, 0.1m, 1.2m), and Eve_Rx (0.1m, -0.6m, 1.2m). **b** Eavesdropping (P_E) and falsifying (P_B, P_C) powers as a function of the iteration order in the metasurface coding-pattern optimization. **c** Optimized binary coding patterns for three-channel (Eve, Bob and Carol) modulated-metasurface backscattering wireless communication. For instance, '110' denotes the binary phases of 180°, 180 ° and 0 ° at Eve, Bob and Carol, respectively. **d** From left to right: RGB images acquired at Eve, Bob, Dave and Carol. **e** Top row (from left to right): 17ms-length time-domain Wi-Fi signals received at Eve, Bob, Dave and Carol. Bottom row: Corresponding magnified details. **f** Corresponding decoded constellation diagrams.

Table 1. Main parameters of the prototype. MIMO: multiple-input multiple-output.

Parameter	Value
Carrier wave frequency	2.442GHz
Transmission scheme	2×3 MIMO
Modulation scheme	BPSK
Symbol rate	0.5Mbps
Sample rate	8Mbps
Samples per packets/Frame	1638400
Transmit power	-10dBm
Receiver gain	15dB

Materials and Methods

Design of the programmable coding metasurface. The designed programmable metasurface consists of 32×24 meta-atoms operating at ~2.4GHz, as shown in Supplementary Figures 1c and 1d, with the schematic and details of the electronically controllable meta-atoms (of size $54\times54\text{mm}^2$) illustrated in Supplementary Figures 1a and 1b, respectively. In each meta-atom, a PIN diode (SMP1345-079LF) is integrated to control the EM reflection phase, and the corresponding frequency responses are shown in Figs. 2e and 2f (magnitude and phase, respectively). The meta-atom is composed of two substrate layers: the top layer is made of F4B (with relative permittivity of 2.55 and loss tangent of 0.0019), while the bottom layer is made of FR4 (with relative permittivity of 4.4 and loss tangent of 0.03). The top square patch, integrated with the PIN diode, has a size of $0.37\times 0.37\text{mm}^2$. In addition, a 33 nH inductor (Murata LQW04AN10NH00) is used to achieve good separation between the radio-frequency (RF) and DC signals. For the design and simulation of the meta-atom, the commercial software package CST Microwave Studio[22] is used. Specifically: (1) the reflection response of the meta-atom is investigated under different operation states (ON/OFF) of the PIN diode; (2) a Floquet port is use d to simulate an *x*-polarized wave incidence on the metasurface and to monitor the reflected wave; and (3) periodic boundary conditions are set on the four sides to mimic an infinite array.

Information theoretical concepts. A typical wiretap channel model used to analyze the secrecy of a wireless communication system features a legitimate transmitter (Alice) and a receiver (Bob) communicating in the presence of an eavesdropper (Eve). Here, we assume that the communication is mediated by a metasurface, and accordingly refer to h_{AB} and h_{AE} as the channel coefficients modeling the direct paths (with the subscripts *A*, *B*, and *E*, pertaining to Alice, Bob, and Eve, respectively), and to $\mathbf{h}_{\text{AM}}$, $\mathbf{h}_{\text{ME}}$, $\mathbf{h}_{\text{MB}}$ as the *N*-length column vectors representing the channel response mediated by the metasurface (indicated with the subscript *M*) to Alice, Bob and Eve, respectively.

For a unit-power transmitting signal from Alice side, the system responses at Bob and Eve sides can be formally expressed as[23]

$$y_{\mathrm{BA}} = h_{\mathrm{AB}} \;\; + \;\; \mathbf{h}_{\mathrm{MB}}^{T} \cdot \mathbf{\Phi} \cdot \mathbf{h}_{\mathrm{AM}} + n_{\mathrm{BA}},$$

and

$$y_{\mathrm{EA}} = h_{\mathrm{AE}} \;\; + \;\; \mathbf{h}_{\mathrm{ME}}^{T} \cdot \mathbf{\Phi} \cdot \boldsymbol{h}_{\mathrm{AM}} + n_{\mathrm{EA}},$$

respectively, where the superscript T indicates the vector transpose operation, n_{BA} and n_{EA} are additive zero-mean Gaussian white noise (with power σ_{BA}^{2} and σ_{EA}^{2}, respectively) at Bob's and Eve's sides, respectively, and a time-harmonic dependence $\exp(j\omega t)$ has been assumed and dropped. In addition, $\mathbf{\Phi} = \mathrm{diag}(a_1 \mathrm{e}^{\mathrm{j}\theta_1}, a_2 \mathrm{e}^{\mathrm{j}\theta_2}, \dots \dots, a_N \mathrm{e}^{\mathrm{j}\theta_N})$ is the response matrix of the metasurface (composed of N meta-atoms). For the programmable one-bit coding metasurface in our study, we ideally assume unit amplitude ($a_n = 1$) and binary phases $\theta_n \in \{0, \pi\}, n \in \{1,2, \dots, \mathrm{N}\}$. Then, the safe communication rate of the wireless communication system can be expressed as[24]

$$\mathrm{R_e} = \left(\log_2\left(\frac{P_{\mathrm{EA}}}{\sigma_{\mathrm{EA}}^{2}}\right) - \log_2\left(\frac{P_{\mathrm{BA}}}{\sigma_{\mathrm{BA}}^{2}}\right)\right)$$

where $P_{\mathrm{BA}} = |h_{\mathrm{AB}} + \; \mathbf{h}_{\mathrm{MB}}^{T} \cdot \mathbf{\Phi} \cdot \mathbf{h}_{\mathrm{AM}}|^2 + \sigma_{\mathrm{BA}}^{2}$ and $P_{\mathrm{EA}} = |h_{\mathrm{AE}} + \mathbf{h}_{\mathrm{ME}}^{T} \cdot \mathbf{\Phi} \cdot \boldsymbol{h}_{\mathrm{AM}}|^2 + \sigma_{\mathrm{EA}}^{2}$ denote the received powers at Bob's and Eve's sides, respectively. Assuming that the noise power is the same at both sides (i.e., $\sigma_{\mathrm{BA}}^{2} = \sigma_{\mathrm{EA}}^{2}$), it follows that $\mathrm{R_e} > 0$ if $P_{\mathrm{EA}} > P_{\mathrm{BA}}$. Such condition can be in principle attained by suitably optimizing the metasurface coding, resulting in the capture of the wireless signal or the disruption of the original secure communication. By increasing the power P_{EA} received at Eve's side, it is possible to improve the quality of the eavesdropped signal and/or to increase the monitoring range.

Metasurface-enabled backscattering wireless communications. In the active mode (see Fig. 4), our proposed wireless attacker relies on two different types of metasurface-enabled backscattering wireless communication strategies,[19,20] namely, a modulated-metasurface scheme for the information falsification, and a non-modulated-metasurface scheme for the information eavesdropping. In the former case, the binary digital sequence to be transferred is directly encoded in the metasurface, and the signal modulation is attained under illumination by a single-tone carrier signal. In the latter case, the programmable metasurface simply acts a passive reflector, redirecting the incoming beam towards the intended direction. Referring to Fig. 4, there are two independent falsifying links (i.e., Eve_Tx-Metasurface-Bob, Eve_Tx-Metasurface-Carol), for which we utilize a BPSK modulation scheme on the physical layer; to avoid confusion with conventional BPSK modulation at the digital level, we use the term "*physical* BPSK modulation" referring to the (modulated-metasurface) falsifying links. More specifically, the signal demodulated at Bob's (or Carol's) side has binary phase states: 0° and 180 °, which we associate to the digits '0' and '1', respectively. Thus, for the two falsifying wireless links, we have four different combinations of demodulated information bits in total, i.e., '00', '01', '10', and '11'. On the other hand, since no direct modulation at the metasurface level is involved for the eavesdropping link (i.e., Alice-Metasurface-Eve_Rx), only one state of the radiation beam is required. For illustration, we have chosen the phase of the radiation beam at Eve's side as 180 °. As a consequence, we need to design four different coding patterns, each corresponding to one possible combination of phases at Eve's, Bob's and Carol's sides, i.e., '100', '101', '110', '111'. Note that, consistently with our choice on the eavesdropping link (180°), the first bit in the sequence is always '1'. The arising optimization problem can be addressed by means of the line-search algorithm detailed in Supplementary Note 2.

Conclusion

To sum up, we have put forward and demonstrated the concept of metasurface-enabled smart wireless attack at the physical layer. By comparison with recent studies relying on passive metasurfaces,[18] our results indicate that the use of programmable metasurfaces enables more sophisticated and smarter types of attacks, either in passive or active modes, ranging from the conventional eavesdropping to disruption of communication, and even information falsification. In both passive and active modes, the footprints of the attack in the physical space, and hence its detectability, can be minimized. Although our results are exemplified for 2.4GHz Wi-Fi signals, their implications are much broader, and apply to generic wireless communication systems. Considering the crucial role and pervasiveness of metasurfaces in the envisioned future (6th-generation and beyond) wireless networks, it is of paramount importance that the potential vulnerabilities arising from their malicious hacking are fully understood, and that suitable countermeasures are developed at the early stage of the underlying smart-radio-environment technology. Accordingly, current and future studies are aimed at exploring new types of vulnerabilities and at developing new systems and protocols that are inherently resilient to physical-layer attacks.

Author contribution: L. L., T. J. C. and V. G. conceived the idea, and wrote the manuscript. M.W. and H. Z. designed and developed the system, and conducted the experiments. All authors participated in the data analysis and interpretation, and read the manuscript.

Data availability: The data that support the findings of this study are available from the last author upon request.

Code availability: Code that supports the findings of this study is available upon reasonable request from L. L.

Acknowledgements: This work was supported by the National Key Research and Development Program of China under Grant Nos. 2021YFA1401002, 2017YFA0700201, 2017YFA0700202, and 2017YFA0700203, and the 111 Project under Grant No. 111-2-05.

Conflict of interest statement: The authors declare no conflicts of interests.

References

1. Larsson, E. G., Edfors, O., Tufvesson, F. & Marzetta, T. L. Massive MIMO for next generation wireless systems. *IEEE Commun. Mag.* **52**, 186–195 (2014).
2. Albreem, M. A., Sheikh, A. M., Alsharif, M. H., Jusoh, M. & Mohd Yasin, M. N. Green internet of things (GIoT): Applications, practices, awareness, and challenges. *IEEE Access* **9**, 38833–38858 (2021).
3. Cui, T. J., Qi, M. Q., Wan, X., Zhao, J. & Cheng, Q. Coding metamaterials, digital metamaterials and programmable metamaterials. *Light Sci. Appl.* **3**, e218 (2014).
4. Li, L. & Cui, T. J. Information metamaterials – from effective media to real-time information processing systems. *Nanophotonics* **8**, 703–724 (2019).
5. Li, L. *et al.* Intelligent metasurface imager and recognizer. *Light Sci. Appl.* **8**, 97 (2019).
6. Liu, S. & Cui, T. J. Concepts, working principles, and applications of coding and programmable metamaterials. *Advanced Opt. Mater.* **5**, 1700624 (2017).
7. Cui, T. J., Liu, S., Bai, G. D. & Ma, Q. Direct transmission of digital message via programmable

coding metasurface. *Research* **2019**, 2584509 (2019).

8. Shuang, Y. *et al.* One-bit quantization is good for programmable coding metasurfaces. *Sci. China Inf. Sci.* **65**, 172301 (2022).
9. Basar, E. *et al.* Wireless communications through reconfigurable intelligent surfaces. *IEEE Access* **7**, 116753–116773 (2019).
10. Pan, C. *et al.* Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions. *IEEE Commun. Mag.* **59**, 14–20 (2021).
11. Cheng, Q. *et al.* Reconfigurable intelligent surfaces: Simplified-architecture transmitters–from theory to implementations. *Proc. IEEE*, early access (2022), doi:10.1109/JPROC.2022.3170498.
12. Di Renzo, M. *et al.* Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and road ahead. *IEEE J. Sel. Areas Commun.* **38**, 2450-2525 (2020).
13. Flamini, R. *et al.* Towards a heterogeneous smart electromagnetic environment for millimeter-wave communications: An industrial viewpoint. *IEEE Trans. Antennas Propag.*, early access (2022) doi:10.1109/TAP.2022.3151978.
14. Akyildiz, I. F., Kak, A. & Nie, S. 6G and beyond: The future of wireless communications systems. *IEEE Access* **8**, 133995–134030 (2020).
15. Martini, E. & Maci, S. Theory, analysis, and design of metasurfaces for smart radio environments. *Proc. IEEE*, early access (2022) doi:10.1109/JPROC.2022.3171921.
16. Zheng, P. *et al.* Metasurface-based key for computational imaging encryption. *Sci. Adv.* **7**, eabg0363 (2021).
17. Georgi, P. *et al.* Optical secret sharing with cascaded metasurface holography. *Sci. Adv.* **7**, eabf9718 (2021).
18. Shaikhanov, Z., Hassan, F., Guerboukha, H., Mittleman, D. & Knightly, E. Metasurface-in-the-middle attack: From theory to experiment. in *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks* 257–267 (ACM, 2022). doi:10.1145/3507657.3528549.
19. Zhao, H. *et al.* Metasurface-assisted massive backscatter wireless communication with commodity Wi-Fi signals. *Nat Commun* **11**, 3926 (2020).
20. Li, L., Zhao, H., Liu, C., Li, L. & Cui, T. J. Intelligent metasurfaces: control, communication and computing. *eLight* **2**, 7 (2022).
21. Yener, A. & Ulukus, S. Wireless Physical-layer security: Lessons learned from information theory. *Proc. IEEE* **103**, 1814–1825 (2015).
22. CST Studio Suite 3D EM simulation and analysis software. https://www.3ds.com/products-services/simulia/products/cst-studio-suite/.
23. Lu, X., Lei, J., Shi, Y. & Li, W. Intelligent reflecting surface assisted secret key generation. *IEEE Signal Process. Lett.* **28**, 1036–1040 (2021).
24. Leung-Yan-Cheong, S. & Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **24**, 451–456 (1978).

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SM0714VGLLVGTJ.pdf
- SupplVideo.mp4