Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges

Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro
Division of Information and Computing Technology (ICT)
College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU)
Doha, Qatar
e-mail: {ptedeschi, ssciancalepore, rdipietro}@hbku.edu.qa

***Abstract*— The recent advancements in hardware miniaturization capabilities have boosted the diffusion of systems based on Energy Harvesting (EH) technologies, as a means to power embedded wireless devices in a sustainable and low-cost fashion. Despite the undeniable management advantages, the intermittent availability of the energy source and the limited power supply has led to challenging system trade-offs, resulting in an increased attack surface and a general relaxation of the available security services.**

In this paper, we survey the security issues, applications, techniques, and challenges arising in wireless networks powered via EH technologies. We explore the vulnerabilities of EH networks, and we provide a comprehensive overview of the scientific literature, including attack vectors, cryptography techniques, physical-layer security schemes for data secrecy, and additional physical-layer countermeasures. For each of the identified macro-areas, we compare the scientific contributions across a range of shared features, indicating the pros and cons of the described techniques, the research challenges, and a few future directions. Finally, we also provide an overview of the emerging topics in the area, such as Non-Orthogonal Multiple Access (NOMA) and Rate-Splitting Multiple Access (RSMA) schemes, and Intelligent Reconfigurable Surfaces, that could trigger the interest of industry and academia and unleash the full potential of pervasive EH wireless networks.

***Index Terms*—Energy Harvesting Security; Green Communications Security; IoT Security; Physical-Layer Security; Lightweight Cryptography.**

I. Introduction

Next-generation wireless networks are increasingly evolving toward pervasive and ubiquitous systems, able to bring new capabilities in a variety of environments and application scenarios [1]. This paradigm evolution has been enabled in the late 1990s thanks to the rise of Wireless Sensor Networks (WSNs), and it has progressed to a large scale thanks to the evolution of Internet of Things (IoT), Cyber-Physical Systems (CPS), and, more recently, 5G networks [2].

Despite the massive growth and the increasing computational capabilities of tiny wireless devices, energy availability and consumption still remain critical issues [3]. Indeed, while improvements in hardware embedding capabilities widened the computing efficiency and potential applications of wireless devices, the energy budget required to power the devices increases accordingly, severely affecting the lifetime and availability of the associated wireless networks. At the same time, increasing the capacity of batteries on-board of these devices is only a time-limited solution, further postponing the issue and impacting on the form-factor and ubiquity of the devices [4].

These issues motivated the recent exponential growth of the *Energy Harvesting (EH)* research area. Several solutions, such as solar, thermoelectric, and mechanical harvesting techniques, have been re-introduced and improved in their size and features to be suitable to power embedded devices, in a tentative to move toward perpetual battery-free pervasive communications [5]. At the same time, the theoretical studies describing the usage of existing or dedicated Radio Frequency (RF) transmissions to power embedded devices have finally translated into real devices and hit the market, thanks to dedicated prototypes and commercial products building on RF power harvesting to provide energy to embedded devices [6]. The potentials of EH for the next-generation low-power wireless networks are confirmed by several projects, funded by the most important funding agencies throughout the world. For instance, the EU funded several projects related to EH under the Horizon 2020 (H2020) research and innovation program, including Tryst Energy [7], DuraCap [8], EnABLES [9], Plug-N-Harvest [10], and Re-Vibe [11], to name a few. The US National Science Foundation also funded several pilot studies, such as CORE [12], SMALL [13], and CAREER [14]. In addition, the National Science Foundation of China is also supporting several scientific contributions focusing on the development of EH technologies, such as [15], [16], and [17].

This is finally confirmed also by recent pilot studies, indicating EH techniques such as ambient backscatter and RF energy harvesting as crucial enabling technologies for *sixth generation* (6G) wireless networks [18], [19], [20].

Despite their appealing features and significant advantages, the switch to EH sources generally widens the attack surface of wireless networks and cyber-physical systems. On the one hand, powering embedded devices via intermittent energy sources and, in the case of wireless powering, removing wired power connections, expose the devices to inexpensive and easy eavesdropping attacks [21], [22], [23]. On the other hand, the

This is a personal copy of the authors. Not for redistribution. The final version of the paper is available through the IEEExplore Digital Library, at the link: https://ieeexplore.ieee.org/document/9170604, with the DOI: 10.1109/COMST.2020.3017665.

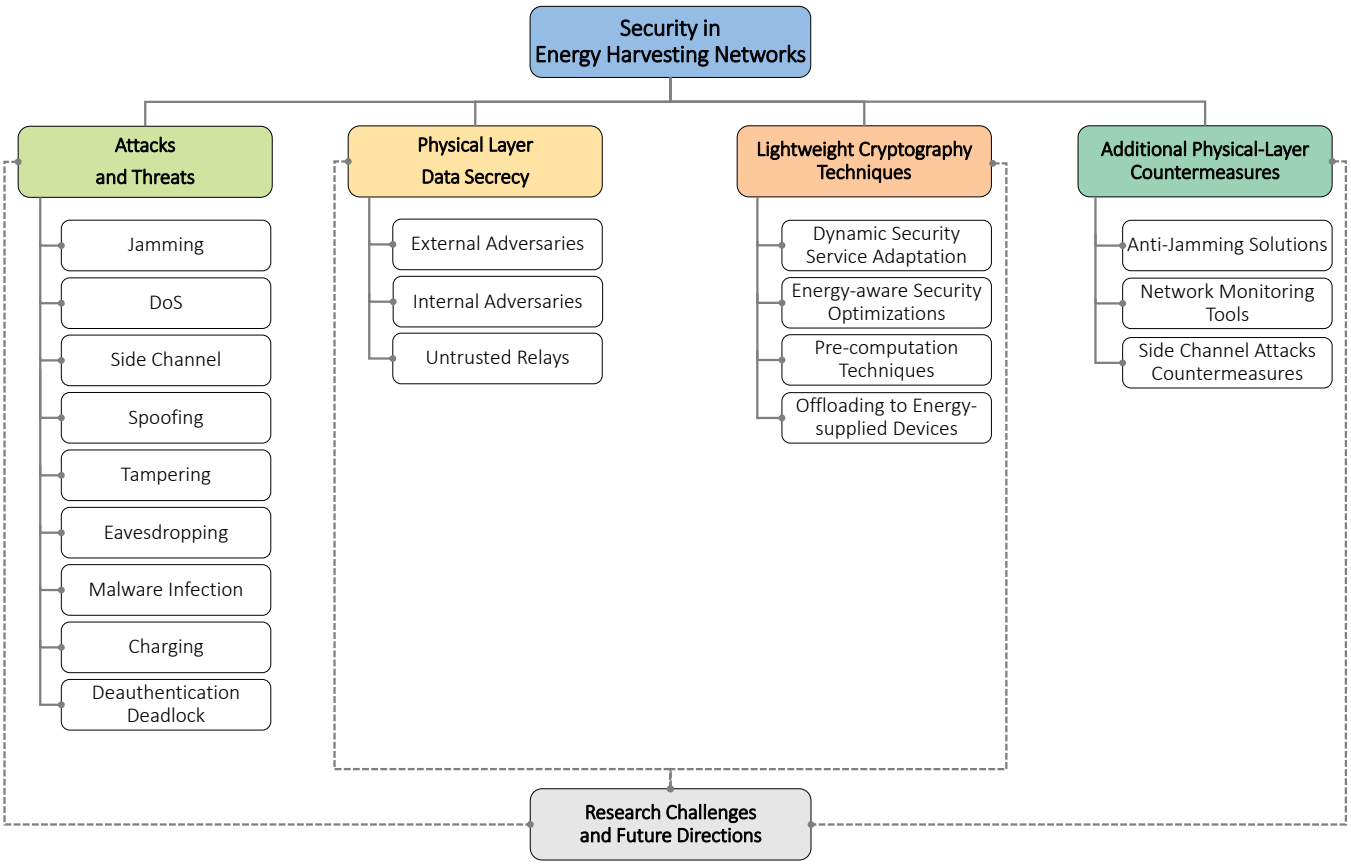

Fig. 1. Taxonomy and classification of the scientific contributions in this survey. We identified four macro-areas related to security issues in EH networks, being them dedicated to the investigation of attacks, physical-layer data secrecy issues, lightweight cryptography approaches, and additional physical-layer countermeasures. Within each area, we further identify distinguishing adversarial models and specific design trends. Finally, for each of the investigated topics, we identify crucial research challenges and future directions .

shift to EH power sources exacerbates the well-known trade-off between energy and security, further decreasing the energy budget available for security operations [24]. Considering the traditional low awareness of security vulnerabilities by wireless network administrators (for the sake of immediate services availability), the reduction of the energy budget often brings to the reduction of security barriers [25].

Security issues in EH networks have been quickly touched by few position papers and surveys available in the literature. An overview of their main features and differences with this contribution is provided in Tab. I.

Several pioneering contributions, such as [26], [27], [22], and [28], preliminarily identified the main attacks and security issues affecting RF EH networks, inspiring a relevant literature production over the last years. However, besides considering only a limited set of weaknesses in wireless-powered EH networks, the cited contributions did not provide any overview of possible defense schemes and countermeasures. Similarly, the position paper by the authors in [30] described the usage of cooperative strategies in wireless-powered EH networks, highlighting their benefits also from the security perspective. However, the cited paper did not consider the literature in the security domain, and security issues were not addressed, too. Looking at the main surveys available in the literature, valuable contributions are provided by the authors in [21], [29], [32], and [34]. However, they focused either on the description of the main aspects and challenges of RF EH technologies (such as [21]), or on specific techniques and phenomena, such as interference [29], beamforming [32], and Simultaneous Wireless Information and Power Transfer (SWIPT) technologies [34]. We also report the recent survey by the authors in [36] on physical-layer security, where a few physical-layer security approaches based on EH concepts are mentioned, without any further detail. Finally, the recent study by the authors in [33] only provides an overview of the techniques used to improve physical layer security in SWIPT networks. However, the main attacks, defensive technologies, network availability considerations, countermeasures, and research challenges related to the security domain are not discussed. In addition, we notice that none of the surveys and position papers currently available in the literature widens the analysis, practically excluding other EH sources, such as solar, wind, mechanical, and thermoelectric sources that, instead, we take into full consideration in this survey. Further, the cited contributions also did not consider all the works that adapted cryptography approaches to work efficiently on EH nodes.
Therefore, we remark that the literature is actually missing a comprehensive survey specifically conceived to tackle all the security aspects connected to the operation of EH networks, including information secrecy at the physical layer, cryptog-

TABLE I
COMPARISON BETWEEN THE TOPICS TACKLED IN THIS PAPER AND THE RELATED SURVEYS TOUCHING NETWORK SECURITY ISSUES IN EH NETWORKS.

Ref.	RF Sources	Solar Sources	Mechanical Sources	Wind Sources	Thermoelectric Sources	Cryptography Approaches	Additional PHY-layer counter-measures	Research Challenges
[26]	✓	×	×	×	×	×	×	×
[27]	✓	×	×	×	×	×	×	×
[22]	✓	×	×	×	×	×	×	×
[28]	✓	×	×	×	×	×	×	×
[29]	✓	×	×	×	×	×	×	×
[30]	✓	×	×	×	×	×	×	✓
[31]	✓	×	×	×	×	×	×	×
[21]	✓	×	×	×	×	×	×	×
[32]	✓	×	×	×	×	×	×	×
[33]	✓	×	×	×	×	×	×	×
[34]	✓	×	×	×	×	×	×	✓
[35]	✓	×	×	×	×	×	✓	✓
[36]	✓	×	×	×	×	×	×	×
This survey	✓	✓	✓	✓	✓	✓	✓	✓

raphy techniques, attacks, additional physical-layer defensive technologies, and, finally, network availability considerations.

Contribution. In this paper, we close the above-introduced gap by providing a comprehensive survey on security issues, applications, approaches, and research challenges characterizing wireless networks and embedded systems powered via Energy Harvesting sources. Building on the existing literature, we first describe the threats and vulnerabilities affecting wireless networks operating thanks to EH sources. Next, we survey the security schemes related to EH networks available in the literature, classifying them across reference macro-areas, such as physical-layer approaches for data secrecy, lightweight cryptography techniques, and additional physical-layer countermeasures. For each of these macro-categories, as a novel contribution, we describe the adversarial models, the assumptions, the solutions, and we cross-compare the scientific works available in the literature via their distinctive features (see Figure 1 for a high-level overview).

Finally, we provide future research directions along the above-described macro-areas, as well as, some additional crucial research challenges, whose further investigation could unleash the full potential of EH technologies, toward the large-scale adoption of EH sources in wireless networks.

We remark that this paper is not yet another survey on physical-layer security. Indeed, in this paper we survey security issues, approaches, and applications strictly connected to all EH networks (not only RF), where dedicated RF and natural energy sources are used to enable Device-to-Device Communications (D2D) communications in IoT and generic wireless networks. These networks include embedded systems powered via solar, mechanical, wind, and electromagnetic sources, such as ambient backscatter, Wireless Powered Communication Network, SWIPT networks, to name a few. Therefore, technologies such as Radio Frequency IDentification (RFID), Near Field Communication (NFC), and traditional tag-to-reader backscatter networks are not within the scope of this survey, as these communication schemes can neither power embedded systems, nor detect transmissions of other nearby devices, nor power D2D networks, but they can communicate exclusively to compatible devices (e.g. RFID and NFC readers) [37] —the interested readers can refer to [38] and [39] for a comprehensive survey on the security issues related to the cited technologies.

Roadmap. The rest of this paper is organized as follows. Section II provides an overview of the technologies enabling energy harvested embedded systems; then, Section III describes the threats and vulnerabilities intrinsic to the operation of EH networks, motivating the study of several security schemes in the areas. The application and customization of cryptography schemes in EH networks is discussed in Section IV. Then, the mechanisms and strategies deployed to enhance physical-layer data secrecy are described in Section V. Additional physical-layer countermeasures deployed to face the afore-mentioned attacks are described in Section VI. Emerging research areas and future research directions are described in Section VII and, finally, Section VIII tightens conclusions.

II. OVERVIEW OF ENABLING TECHNOLOGIES

In this section, we introduce the enabling technologies considered in this work, as well as some important background concepts that have been introduced in the literature when dealing with security in EH networks. Specifically, Section II-A reports some basic notions on energy harvesting technologies using non-RF sources, such as solar-based sources, mechanical sources, and thermoelectric generators, while RF harvesting methods are introduced in Section II-B. Preliminary details regarding Ambient Backscatter Communication Network (ABCN) are introduced in Section II-C, while Section II-D focuses on the principles enabling Wireless Powered Communication Networks. Section II-E provides an overview of the logic and hardware architectures adopted in SWIPT networks. Finally, few distinctive features of EH networks crucial for the design of security solutions are discussed in Section II-F. We highlight that the aim of this section is to

let the reader familiarize with harvesting technologies and their main features, with reference to security issues. For exhaustive discussion on the main hardware considerations behind EH technologies, we refer the reader to dedicated books, such as [40].

A. Energy Harvesting via non-RF Sources

Energy Harvesting (EH) processes refer to the set of techniques used to capture electrical energy from ambient sources, thanks to dedicated conversion circuits, to be used to extend the lifetime of battery-powered wireless devices [40], [41].

EH capabilities are appealing for a variety of applications, especially the ones involving pervasive devices, such as Wireless Body Area Networks (WBANs), WSNs, and IoT. Indeed, from the networking perspective, one of the main challenges of these applications domains has been always the limited energy availability provided by on-board batteries, as well as the high maintenance costs deriving by batteries replacement operations. On the one hand, EH capabilities can provide additional energy availability for battery-powered devices, enabling enhanced services (e.g., higher throughput, increased devices availability). On the other hand, EH circuits could replace batteries, possibly reducing operational costs, the form factor of the devices, and their impact on the surrounding context.

Several environmental or non-dedicated sources can be used to scavenge energy and to power embedded circuits, enabling wireless networks [42], [43]. An overview of the main features of these sources is provided below, while a summary of the harvesting capabilities of the several sources is provided in Table II.

TABLE II
OVERVIEW OF ENERGY HARVESTING SOURCES AND RELATED POWER DENSITIES.

EH Source Type	Power Density	Ref.
Solar	$[0.006 - 15]\ mW/cm^2$	[44]
Wind	$[0.065 - 28.5]\ mW/cm^2$	[45], [46]
Mechanical - Piezoelectric	$[0.11 - 7.31]\ mW \cdot g^2/cm^3$	[40]
Thermoelectric	$[15 - 60]\ \mu W/cm^3$	[44]
RF	$[1.2 \cdot 10^{-5} - 15]\ mW/cm^2$	[44], [47]

Solar Sources. Historically, solar-to-DC conversion techniques have been the most investigated ones in the research community. The devices powered through solar energy use solar panels to convert light into energy. Due to the intermittent presence of the solar source (e.g., due to the adverse weather conditions or during darkness periods), rechargeable batteries and capacitors are used to store the excess energy and to guarantee continuous energy availability. We refer the interested readers to the valuable contribution in [48] for an overview of the most important challenges and hardware design considerations about solar-powered embedded systems. Generally speaking, the latest scientific sources available in the literature show that solar cells for embedded systems can achieve a power density in the range $[0.006 - 15]\ mW/cm^2$ per time unit, depending on the luminosity level [44].

Mechanical Sources. Natural mechanical vibrations are among the most popular and attractive sources for energy harvesting. Indeed, mechanical vibrations generated from natural events (such as seismic motion and water tides) produce kinetic energy, characterized by a power density that is significant enough to power embedded devices [40]. The systems leveraging mechanical sources for energy harvesting are usually classified based on the physical principle used to transduce from kinetic to electrical energy, and they can be partitioned into piezoelectric, electromagnetic, and electrostatic systems. Piezoelectric systems work according to the *piezoelectric effect* first described by Marie Curie in 1880, by using the electric charge produced within a material as a consequence of a mechanical stress [49]. These systems often use dedicated materials, such as the zinc oxide and polymer-based materials, that are well-known to be characterized by relevant electromagnetic coupling. Electromagnetic harvesters leverage the *electromagnetic induction* principle, by generating voltage as a result of the variation of the magnetic field. Compared to piezoelectric-based systems, they are more difficult to integrate with modern Micro-Electrical Mechanical Systems (MEMS), but in medium-size products, they exhibit a suitable behavior, especially for low-frequency applications. Conversely, electrostatic harvesters are particularly suitable for IoT sensors. This latter class of harvesters leverages the *variable capacitance* principle, generating different voltages by changing the capacitance of the system. This is usually achieved by oscillating a mass attached to a plate, thus varying the distance of this element from another plate. This class of harvesters is particularly suitable for embedded integration. However, these systems usually require an external voltage source, necessary to charge the plates, and they generate a limited amount of power.

Without loss of generality, mechanical EH systems generate power proportionally to the weight of the harvester (e.g., the mass in electrostatic harvesters) [50]. Therefore, when integrated with wireless devices, on the one hand the mass of the harvester should be maximized while, on the other hand, satisfying the specific constraints on the size of the system. Given that the production of the energy can be disjoint from its usage, the energy scavenged from mechanical sources is typically stored in rechargeable batteries, exhibiting slower discharge processes than capacitors. Several applications and even commercial products using a mechanical source for EH are available on the market [51]. The hardware details regarding mechanical energy harvesting can be found in [40]. The same source indicates that piezoelectric EH systems generate a normalized power density in the range $[0.117.31]\ mW \cdot g^2/cm^3$, while recent works such as [43] report values of $184\ \mu W/cm^3$ at 10 Hz for electrostatic harvesters and $0.21\ \mu W/cm^3$ at 12 Hz for electrostatic harvesters. These values have been also reported in the updated Table II.

Wind Sources. Similarly to the renewable energy sources previously discussed, wind sources for EH have been widely investigated in the literature. These systems use wind micro-turbines as the mechanical source enabling movement and, thus, AC generation. More in detail, the movement of the magnets on the stator of the micro-turbine generate AC elec-

tricity, that is then converted into DC using a bridge rectifier. However, compared to solar and additional mechanical EH sources, wind EH systems often require bulky equipment, very hard to be integrated with embedded devices. In addition, the wind power source is generally more unreliable than the other ones, as wind phenomena are more intermittent and time-varying. More details on hardware-related trade-offs and integration can be found in [46]. The same source indicates that wind micro-turbines suitable for embedded systems can achieve a power density in the range $[0.065 - 28.5]\, mW/cm^2$ per time unit, assuming a wind speed of $6.3m/s$ and a turbine with a length of $30cm$. Overall, we notice that the power density of wind EH sources depends strictly on (i) the wind intensity, (ii) the air density, (iii) the wind speed, and (iv) the length of the turbine rotor blade [46].

Thermoelectric Sources. These sources have been historically used mainly in the first space and terrestrial applications of EH, and they are recently expanding also in other contexts, such as underwater [52]. Overall, systems using EH via thermo-electric sources leverage the temperature difference between two poles to generate energy. Recently, their usage has been proposed also for embedded devices, especially for WBANs and micro-structured devices, thanks to the frequent temperature difference involved in such scenarios. Overall, thermoelectric power harvesters are considered more reliable and long-lasting than other EH sources, especially the mechanical ones, because of the relatively reduced exposition to movements and mechanical shocks. The hardware considerations regarding thermoelectric generators can be found in the contributions by the authors in [53]. The latest scientific sources available in the literature indicate that thermoelectric harvesters used with embedded systems can reach a power density level in the range $[15 - 60]\ \mu W/cm^3$ per time unit, depending on the specific thermoelectric source [46].

We highlight that all the above-described sources leverage *green* sources, i.e., natural phenomena not requiring any pre-existing system deployment. This is different from RF harvesting, where existing network infrastructure is adopted. Wireless charging methods are described in the following section.

B. Energy Harvesting via RF Sources

The energy to power an embedded system can be obtained also via electromagnetic power transfer. This is the most promising and attractive technology for embedded devices, as the power generation process takes place via wireless links, without any physical connection between the energy source and the powered device. More in detail, embedded devices powered via electro-magnetic sources use dedicated circuits, able to extract power from the surrounding electromagnetic field, thanks to inductive, capacitive, and magneto-dynamic coupling principles. We refer the interested readers to the contributions by the authors in [54] for an overview of the hardware principles driving electromagnetic energy harvesting. The latest scientific sources available in the literature indicate that RF signals used to power embedded devices can achieve a power density in the range $\left[1.2 \cdot 10^{-5} - 15\right]\ mW/cm^2$ per time unit, depending on factors such as the distance from the RF source and the peak power of the signal [44], [47].

Overall, three main electromagnetic wireless powered network architectures can be identified: (i) Ambient Backscatter Communication Networks (ABCN); (ii) Wireless Powered Communication Networks (WPCN); and, (iii) Simultaneous Wireless Information and Power Transfers (SWIPT). The architectures and networking considerations crucial for the description of security issues and services connected to these technologies are described in sections II-C, II-D, and II-E, respectively.

C. Ambient Backscatter Communication Networks (ABCN)

The devices resorting to ambient backscatter for power supply rely on RF signals already available in the environment to gain energy. These RF sources include WiFi, Cellular, Radio, and TV Broadcast, i.e., signals that are used for tasks other than the specific power supply of the device. From the hardware perspective, dedicated antennas are used to convert such signals in a small portion of power (typically in the order of μWatts), used to reflect the signal with encoded data. In turn, other ABCN devices in the network use the same principle to reply and enable D2D communications [55].

Let us assume a generic ABCN network, as the one represented in Figure 2, where a generic RF source is used as the ambient RF signal powering K ABCN Transmitters to deliver information to a single ABCN Receiver.

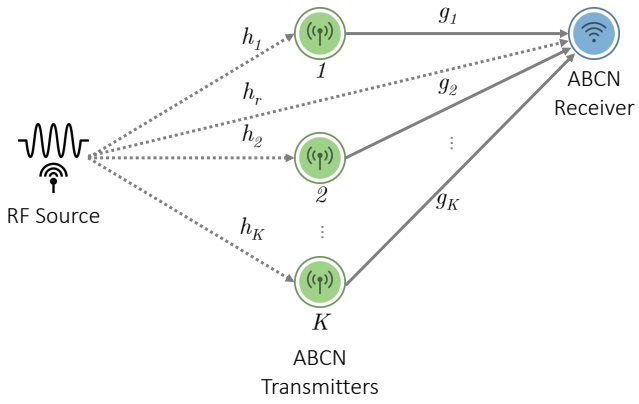

Fig. 2. System Model of a generic Ambient Backscatter Communication Network.

Denoting with h_k the channel between the RF source and the $k-th$ ABCN transmitter, and with g_k the channel between the $k-th$ ABCN transmitter and the ABCN receiver, the signal $y(n)$ related to the n^{th} bit of the message received by the ABCN receiver can be modeled as in the following Eq. 1, as the sum of the direct component from the RF source and the reflections from the K ABCN transmitters.

$$y(n) = h_r \cdot s(n) + \sum_{k=1}^{K} h_k \cdot g_k \cdot \eta_k \cdot s_k(n) + e(n), \qquad (1)$$

where $s_k(n)$ denotes the complex baseband signal originated by the $k-th$ ABCN transmitter, $e(n)$ is channel noise, modeled as Additive White Gaussian Noise (AWGN), and, finally, η_k is the *backscatter efficiency factor*, being $\eta \in [0, 1]$, indicating the backscatter efficiency of the $k-th$ transmitter.

D. Wireless Powered Communication Networks

Wireless Powered Communication Networks (WPCN), often referred to as *Far-Field Wireless Power Transfer (WPT) networks*, are communication networks enabled through the presence of dedicated power sources, providing the necessary energy to power the devices via the WPT technology. An exemplary system model is depicted in Figure 3, where a power beacon transmits a dedicated RF signal that is used by the source to accumulate the necessary energy to communicate with multiple destination devices.

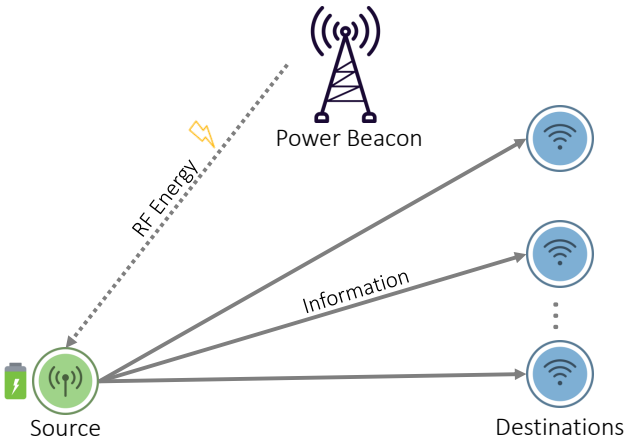

Fig. 3. System Model of a generic Wireless Powered Communication Network. The power beacon emits RF source that powers the transmitter and enable it to communicate with a receiver.

Compared to backscatter communication networks, WPCNs use dedicated signals (not used for other communication tasks), characterized by larger communication ranges, thanks to larger transmitting antennas compared to the radiation wavelength [21].

Compared to SWIPT working according to the Time Splitting (TS) architecture (see Section II-E), instead, the main difference lies in the fact that the harvested energy is used to enable the transmission of information rather than the recharge of the devices, thus anticipating the communication phase (this communication paradigm is often referred as *harvest-then-transmit*). Moreover, the signal that powers the devices is decoupled from the information signal, as it is not specifically meant to transfer information.

Assuming that τ_0 is the amount of time dedicated to energy harvesting in a block duration of time T, such energy harvesting time should be optimized to trade-off between the power available at the device and the data rate, being these metrics directly related to the Signal to Noise plus Interference Ratio (SINR) at the destination and thus to the secrecy capacity of the communication link (see Sec. II-E). Moreover, severe security issues at the physical layer arise especially for devices located far from the power source, that can harvest less energy than the others but require more power to push the transmission farther.

We refer the interested readers to the valuable contribution by the authors in [56] for more details about the networking issues characterizing WPCNs, while security-related scientific contributions will be investigated in Sec. V.

E. SWIPT

As shown in Figure 4, Simultaneous Wireless Information and Power Transfer (SWIPT) networks are characterized by contextual EH and information transfer processes, via dedicated hardware architectures.

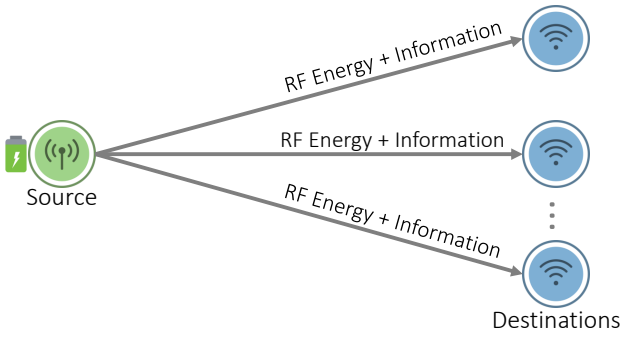

Fig. 4. System Model of a generic Single-Input Multiple-Output Simultaneous Wireless Information and Power Transfer network. A battery-powered source emits a signal transferring information and RF energy, at the same time.

Generally speaking, SWIPT systems are characterized by an emitting power station and several N ($N > 1$) of destination nodes. For the sake of simplicity, in the following, we introduce the notation for the case of a Single-Input Multiple-Output (SIMO) system, where the multiple receiving entities are equipped each with a single antenna, while the extension for multiple-antenna systems is straightforward.

The complex baseband signal transmitted by the source, namely $\mathbf{x}$, is given by the linear combination of the symbols emitted by the transmitting antennas to the receivers, as in the following Eq. 2.

$$\mathbf{x} = \sum_{n=1}^{N} \mathbf{w_n} \cdot s_n, \tag{2}$$

where $\mathbf{w_n}$ are the weights that are modulated by the transmitting antenna to the signal s_n for the n^{th} receiver, generally referred to as a *beamforming vector*.

The complex signal available at the generic n^{th} receiving antenna, denoted as y_n, depends on both the transmitted signal $\mathbf{x}$ and the distortion introduced by the wireless channel, modeled by the matrix $\mathbf{h_n}$. Without loss of generality, the following Eq. 3 holds:

$$y_n = \mathbf{h_n}^H \cdot \mathbf{x} + e_n, \tag{3}$$

where the H exponent denotes the Hermitian transformation of the matrix $\mathbf{h_n}$ (i.e., the transpose and conjugate of the matrix), while e_n is a noise component at the n^{th} receiving antenna, modeling undesired channel effects as AWGN with variance σ_n^2. In addition, $\mathbf{h_n}$ is the distortion caused by the wireless channel, and it is frequently modeled according to a circularly symmetric complex normal distribution, having zero mean and noise covariance matrix, i.e., $\mathcal{S}$, namely $e \sim \mathcal{CN}(0, \mathcal{S})$. In most of the works analyzed in this paper, the covariance matrix is statistically modeled according to the flat-fading Rayleigh model, while the Nakagami-m model is used when aerial links are involved [57].

The following manipulation of the signal at the receiver depends on the hardware architecture assumed for the receiving device. The literature mainly considers four hardware architectures: Time Switching (TS), Power Switching (PS), Separate Receivers (SR), and Antenna Switching (AS). The first three architectures are discussed in the following subsections, while we neglect the logic of the AS architecture given that none of the scientific contributions studied in this paper investigated this configuration (the interested readers can refer to the description in [58] for more details).

1) Time Switching (TS) Receiver Architecture: Time-Switching (TS) EH receivers split the time duration of a time block T in two distinct non-overlapping phases, lasting $\alpha_n T$ and $(1-\alpha_n)T$, where α_n is referred as the *time-switching parameter*. In the first period, namely *Information Decoding (ID) Phase*, lasting αT, the receiver decodes information; then, in the remaining part of the time block, namely the *Energy Harvesting Phase*, it uses the signal to harvest energy and charge the device. It is worth noting that, differently from the logic of a Wireless Powered Communication Network (WPCN), the energy harvesting phase follows the information decoding phase.

The signal available for ID at the receiver, namely y^I, can be expressed as in the following Eq. 4, where the signals emitted by the source toward other users are considered as interfering transmissions.

$$\begin{aligned} y^I &= \sum_{n=1}^{N} \mathbf{h_n}^H \cdot \mathbf{x} = \\ &= \mathbf{h_n}^H \cdot \mathbf{w_n} \cdot s_n + \mathbf{h_n}^H \cdot \sum_{j \neq n} \mathbf{w_j} \cdot s_j + e_n. \end{aligned} \tag{4}$$

Thus, the SINR for the n^{th} user can be expressed as in the following Eq. 5.

$$SINR_n = \frac{|\mathbf{h_n}^H \cdot \mathbf{w_n}|^2}{\sum_{j \neq n} |\mathbf{h_n}^H \cdot \mathbf{w_j}|^2 + \sigma_n^2}. \tag{5}$$

The SINR can be used to obtain the capacity of the channel for each user, i.e., the maximum rate of information available at the user. According to the Shannon Theorem on channel capacity, it is defined as in the following Eq. 6.

$$C_n = \alpha_n \log_2(1 + SINR_n), n \in N. \tag{6}$$

2) Power Switching (PS) Receiver Architecture: When the receiver works according to the Power Switching (PS) hardware architecture, the information decoding phase and the energy harvesting phase take place at the same time. This is achieved thanks to dedicated circuit design, splitting the received power signal in a part used for information decoding and another part used for EH, according to a *power splitting factor*, namely ρ_n. As for the TS architecture, the information signal available at the receiver can be modeled as depicted in Eq. 7.

$$\begin{aligned} y^I &= \sqrt{\rho_n} \left(\sum_{n=1}^{N} \mathbf{h_n}^H \cdot \mathbf{x} \right) + q_n = \\ &= \sqrt{\rho_n} \left(\mathbf{h_n}^H \cdot \mathbf{w_n} \cdot s_n + \mathbf{h_n}^H \cdot \sum_{j \neq n} \mathbf{w_j} \cdot s_j + e_n \right) + q_n, \end{aligned} \tag{7}$$

where q_n models an additional AWGN due to the non-idealities introduced by RF-to-DC conversion circuits, having variance δ_n^2. From the above expression, it is possible to obtain the SINR and the channel capacity for the generic user n, as in the following Eq. 8 and Eq. 9, respectively.

$$SINR_n = \frac{\rho_n |\mathbf{h_n}^H \cdot \mathbf{w_n}|^2}{\rho_n \sum_{j \neq n} |\mathbf{h_j}^H \cdot \mathbf{w_j}|^2 + \rho_n \delta_n^2 + \sigma_n^2}. \tag{8}$$

$$C_n = \log_2(1 + SINR_n), n \in N. \tag{9}$$

3) Separated Receiver (SR) Architecture: While TS and PS are different hardware architectures, the Separated Receivers (RC) is a scenario where some receivers are specifically dedicated to EH activities, while others are specifically dedicated to communication tasks. Defining A the set of users dedicated to communication tasks and B the ones dedicated to EH (with $|A|$ + $|B|$ = N), the signal transmitted by the source can be modeled as in the following Eq. 10:

$$x = \sum_{n \in A} \mathbf{w_n} \cdot s_n + \sum_{m \in B} \mathbf{w_m} \cdot s_m, \tag{10}$$

where s_n and s_m are the information signal and the energy signal, respectively. Considering the generic n^{th} user selected for information decoding, the signal received at this user is expressed by the following Eq. 11.

$$\begin{aligned} y_n^I &= \sum_{n=1}^{N} \mathbf{h_n}^H \cdot \mathbf{x} = \\ &= \sum_{n \in A} \mathbf{h_n}^H \mathbf{w_n} s_n + \sum_{m \in B} \mathbf{h_m}^H \mathbf{w_m} s_m + e_n = \\ &= \mathbf{h_n}^H \mathbf{w_n} s_n + \sum_{j \in A, j \neq n} \mathbf{h_j}^H \mathbf{w_j} s_j + \sum_{m \in B} \mathbf{h_m}^H \mathbf{w_m} s_m + e_n. \end{aligned} \tag{11}$$

As in the previous hardware designs, the information signal can be used to derive the SINR and the channel capacity for the scenario, as in the following Eq. 12 and Eq. 13, respectively.

$$SINR_n = \frac{|\mathbf{h_n}^H \cdot \mathbf{w_n}|^2}{\sum_{j \in A, j \neq n} |\mathbf{h_j}^H \cdot \mathbf{w_j}|^2 + \sum_{m \in B} |\mathbf{h_m}^H \cdot \mathbf{w_m}|^2 + \sigma_n^2}, \tag{12}$$

$$C_n = \log_2(1 + SINR_n), n \in A. \tag{13}$$

F. Unique Features in EH Networks

Without loss of generality, we can notice that embedded devices powered via EH technologies exhibit unique energy availability features, severely influencing, in turn, the design of security solutions.

Overall, two main features can be highlighted. First, the availability of the specific source used to generate power supply is both intermittent and out-of-scale for embedded devices, as qualitatively shown in the following Figure 5.

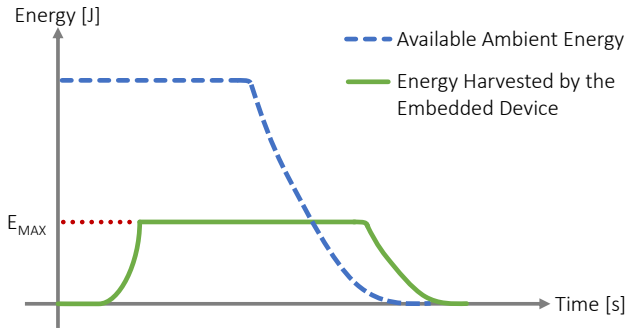

Fig. 5. Qualitative description of the EH process. When high energy is available, the EH circuits power the capacitors on embedded devices, up to a maximum level of E_{MAX}. When the energy source is not available, the energy is quickly drained.

The overall energy available for the re-charging is generally characterized by periods of high availability, alternated with periods of low/no availability. During the full availability periods, the EH circuits can harvest energy up to a maximum level, (indicated as E_{MAX} in the Figure 5), while the remaining energy cannot be harvested. When the availability of the external source decreases, the capacitors or batteries on-board of the embedded system usually start losing energy after a little time, quickly exhausting the energy resource based on the current drain of the load system.

In addition, the level of the energy harvested by the embedded system is usually strictly connected with the received level on the re-charging equipment. The higher the impact of the energy source on the EH circuit, the higher the energy recycled, and the higher the energy available for the system. Especially when considering electromagnetic EH, the received energy source level could have a severe impact on the overall harvested energy per time unit, and thus on its availability for the embedded device. These considerations have motivated several scientific contributions, such as [59] and [60], that provided energy consumption models suitable for specific application scenarios involving EH, such as aircraft and WSN applications, respectively.

We want to remark that all these unique features are all taken into consideration when designing security solutions for EH networks.

III. Attacks and Threats in Energy Harvesting Networks

The underlying mechanisms and strategies enabling EH principles expose wireless devices and networks to several attacks at different layers of the protocol stack. These threats extend beyond trivial eavesdropping attacks, and target the overall availability of the network, its reliability, and its dependability.

Different attacks have been identified and discussed in the literature, each requiring specific tools and features by the adversary and targeting specific enabling technologies. A summary of these attacks is provided in Table III, concerning the techniques and capabilities employed by the adversary.

Eavesdropping. First, as highlighted by several contributions such as [21], [22], and [23], RF EH networks are usually deployed without any built-in encryption mechanism, exposing the delivered energy and information to eavesdropping attacks. Indeed, given that RF EH networks are usually characterized by reduced energy availability compared to other EH sources, integrating off-the-shelf encryption techniques is often not suitable. These considerations have motivated a significant literature production, both considering physical-layer security schemes to improve data secrecy and suitable cryptography techniques, tailored to devices with reduced energy availability. These research areas are discussed in details in the following sections V and IV of this paper.

DoS. Moreover, the literature provides several descriptions and practical examples of Denial of Service (DoS) attacks, aimed at disrupting the availability of EH networks. In this context, networks powered via RF signals are particularly exposed. In this context, one of the simplest strategies to quickly exhaust the energy provision of EH devices is to realize *energy-depletion attacks*. As highlighted by the authors in [26], an *energy depletion* attack is a form of DoS attack, where the adversary sends bogus packets to a wireless-powered node. The radio and processing operations required to analyze and reject these bogus packets lead to a quick drain of the device's battery, preventing any further operation of the node in the network. An example of energy depletion is the flooding attack discussed by the authors in [61]. They considered several attack scenarios where, for instance, the adversary could: (i) introduce a malware in a WSN to increase the transmission power (and thus, the energy consumption) of legitimate devices; (ii) adopt *jamming* techniques to introduce noise on the communication channel, to require the nodes to increase the power transmission and increase the energy consumption; and (iii) exploit the weakness of some traffic aggregation scheme, to increase the size of the re-transmitted packet.

When the transmitting devices use beamforming techniques to increase physical-layer security, an attacker can launch *Beamforming Vector Poisoning* attacks, injecting a malicious signal on the same frequency used for legitimate communications [22]. This translates into a jamming attack and produces destructive interference with the main communication link, reducing the amount of energy that the node can use either for energy charge or information decoding.

While being valid in the context of WSNs, the above considerations apply also to the IoT, as discussed by the authors in [68]. In this reference contribution, the authors highlighted the feasibility of most common attack techniques, such as jamming, replay, and spoofing towards the IoT constrained devices. Moreover, they introduced the *de-authentication dead-*

TABLE III
OVERVIEW OF ATTACKS AFFECTING ENERGY HARVESTING NETWORKS

Ref.	Attack Name	Target Enabling Technologies	Attack Class	Vulnerability	Threat
[21], [22], [23]	Unauthorized Information Sniffing	WPCN, SWIPT	Eavesdropping	No encryption	Data leakage, passive information acquisition
[61]	Flooding	WPCN	DoS	No native anti-malware and intrusion detection systems	Quick battery exhaustion
[62], [63], [64], [65], [66], [67], [68], [69]	Jamming	Generic EH network	DoS	No anti-jamming solutions	Throughput degradation, service interruption
[22]	Beamforming Vector Poisoning	WPCN, SWIPT	DoS	No interference detection and anti-jamming solutions	Resources exhaustion
[70], [71], [72]	Stealthy Collision	WPCN	DoS	No centralized coordination entities	Energy depletion and devices batteries exhaustion
[68]	Deauthentication Deadlock	WPCN	DoS	No authentication and encryption	Connection interruption
[73], [74]	Electromagnetic leaks, Power Consumption, Timing, Powering Leakages	SWIPT, WPCN	Side Channel	No tamper-resistant solutions	Sensitive data leakage
[75]	Back-scattered RF Reflection	ABCN	Side Channel	No physical shielding mechanisms	Sensitive data leakage
[76]	Checkpoint Tampering, Power Interruption	Generic EH network	Device Tampering	No integrity, confidentiality, authenticity	Full control of power supply, infinite loops
[68]	Playback	WPCN	Replay	No freshness of cryptography materials	Malicious (re)transmissions of valid data
[77]	Pilot Signal Spoofing	ABCN	Spoofing	No messages authentication	Unauthorized delivering of messages and energy
[22]	Charging (Cheating, Leeching, Flooding)	WPCN	Spoofing	No authentication and throughput balance solutions	Energy depletion and battery exhaustion; malicious nodes collude to create packet collisions against legitimate nodes
[68], [22]	Impersonation	ABCN, WPCN, SWIPT	Man In The Middle	No authentication	Unrecognizable fake nodes
[22]	Malware	WPCN	Malware infection	No suitable anti-malware solutions	Energy depletion, interruption of charging operation

lock attack. It is a type of DoS attack, affecting wireless nodes authenticated to an access point. In this scenario, a malicious user could spoof the victim device and inject unauthorized de-authentication frames directed to the access point, forcing the disconnection of the victim. Specific protection technologies to defeat de-authentication deadlock attacks are discussed in Section VI.

Other attacks at the physical layer of a WPCN are discussed by the authors in [22]. Specifically, despite jamming can be used also for dedicated network protection purposes (see Section V-C), malicious adversaries can use this attack vector to poison the communication channel used for the re-charging of the devices, leading to a DoS. Several contributions in the literature highlighted the issues related to the jamming attacks against a system with energy harvesting. With specific reference to the control theory, the authors in [66] analyzed the effects of the remote state estimation in a closed-loop system under the jamming attacks, taking into account the communication channel properties. Further, they study how jamming affects the performance in a scenario where energy harvesting is employed for battery-powered sensors (transmitter-side), by deriving a policy for the optimal energy allocation. Similarly, the authors in [69] considered a WPCN where an attacker intercepts the energy transmitted to a legitimate user. They provided a theoretical model integrating game theory concepts, and they leveraged this model to optimize the energy required for the data transmission, and the attack policy to achieve effective jamming attacks.

Side-channel. Side-channel attacks allow an adversary to gain relevant information from the device, including secrets keys or private data, by leveraging physical-layer features such as electromagnetic and magnetic leaks, timing information, and energy consumption. As discussed by the authors in [73] and [74], side-channel attacks are a threat also for EH

networks. For instance, correlating the instantaneous energy consumption and the electromagnetic leaks generated during cryptography operations can reveal the secret key computed by the node.

Replay & Spoofing. As highlighted by some contributions such as [75] and [77], signals enabling ABCNs are not authenticated, and thus they can be easily replayed and spoofed by an attacker. While the authors in [77] contextualized this attack in a WBAN, a specific type of side-channel attack technique has been described also by the authors in [75], where a powerful software malware is deployed in the network. This malware extracts sensitive information from the victim, and it leverages a WiFi Network Interface Card (NIC) to force wireless devices to backscatter surrounding RF signals, thus enabling a side-channel used to stealthily transmit the information.

Device Tampering. Recently, the authors in [76] introduced a side-channel attack specific to intermittent computing systems, such as EH devices. During a power loss period, these systems use to save the state of the program as checkpoint(s) into non-volatile memory. At the restoration time of the power supply, the checkpoints are used to recover the state of the system, to further proceed with the computations. Malicious adversaries can exploit the *power interruption* as an attack vector, to: (i) read the checkpoint data; (ii) tamper the checkpoint after the system restore; and (iii) finally, execute a checkpoint replay attack, where the same checkpoint is restored infinitely by executing the same section of code.

Malware Infection. We recall that another way for the attacker to quickly drain devices' battery include typical malicious applications, deployed on purpose on the target device to send multiple energy requests, degrading the system throughput. An example has been provided by the authors in [75] (previously described), where malware is used to force a specific behavior on the target victim.

Other attacks specific to RF EH networks are the ones targeting the trust of the messages used to provide the RF energy to charge the devices. As discussed in Section II, WPCNs require specific *pilot* signals emitted by dedicated power beacons, that physically enable the harvested device. However, these signals usually do not integrate any security service, such as authentication, integrity, and confidentiality. Thus, as summarized by the authors in [27], several attacks can be launched.

Looking at the transmission side, the pilot signal used for energy charging can be spoofed, leading to a *Pilot Signal Spoofing* attack. This could happen also when the EH device specifically requests power, sending a beacon request packet. In such a scenario, the adversary can intercept this message and impersonate the power beacon, reducing the throughput and the lifetime of the EH device [77].

WPCNs are also vulnerable to *charging attacks*, that can be categorized in *leeching*, (ii) *greedy*, and (iii) *cheating* charging attacks. Leeching attacks are physical-layer attacks where devices keep re-charging without sending explicit requests, i.e., by taking advantage of energy leakages when powering neighboring devices. This can affect the awareness of a power beacon, especially if this is interested in maintaining an accurate map of the energy availability of the EH nodes [22].

Greedy charging attacks involve *greedy devices*, continuously requesting energy from the source, and thus preventing other devices to request energy.

Cheating charging attacks, instead, involve a compromised EH node, reporting inaccurate energy measurements to the power source, forcing it to adjust (increasing or decreasing) the reference power level. This can translate either in a DoS or in an *unauthorized energy charging* attack. In the former, the reduction of the power level of the RF source decreases the size of the area where the signal is received, possibly excluding some devices from receiving enough energy. In the latter, increasing the power level of the pilot signal increases the area where such signal is received, possibly enabling malicious EH devices, controlled by the adversary.

We also highlight that, as discussed by the authors in [22], the harvested energy is subject to sensitive changes due to the presence of people in the deployment area. This property could enable the attacker to infer sensitive information about the status of the area surrounding the physical environment where the EH network is deployed, such as the number of people in the area, their movement, and distribution over time, to cite a few, leading to severe privacy attacks.

Cooperative EH Networks. Finally, besides the above-described attacks, it is worth mentioning some specific attacks targeting the novel concept of *Cooperative Energy Harvesting Networks*, highlighted by the authors in [27].

In cooperative EH networks, a generic source node S transfers energy towards a destination node D, by leveraging one or more relay nodes R. These networks do not support any inherent security property hence, besides sharing the same vulnerabilities of traditional WPCNs, these networks are exposed to further threats. In particular, since energy messages do not satisfy implicitly the integrity property, these networks are exposed to *energy state forgery* attacks, where an adversary can tamper the information about its energy state, and send the tampered information towards a cooperator for illicit goals. For instance, when a legitimate node requests energy to the attacker, this latter one can refuse to provide it, claiming an insufficient energy level. Moreover, a compromised node can trigger *repudiation of energy* attacks, denying to own a given amount of energy after the transfer process initiated by a cooperator. In this case, the compromised node acts as a *black hole*, accumulating energy locally and reducing the energy availability on other cooperating devices. These attacks can be anticipated by *energy cheating* attacks, where the compromised node obtains sufficient trust from the victim. First, the compromised node sends messages and operates in the network as a legitimate device, gaining the necessary trust from the network. Then, when the trust is established, it requests energy from other devices and exhausts their energy availability. Finally, cooperative EH networks could be also exposed to *collusion attacks*, where multiple devices collude to deny the reception of energy from a target cooperator device, forcing it to repeat the energy delivering operations, quickly exhausting the available energy.

The techniques to mitigate the above attacks leverage either lightweight tailored cryptography solutions or physical-layer features. The details are provided in sections IV and VI,

respectively.

IV. Cryptography Techniques for EH Devices and Networks

A significant branch of the works on security issues for EH networks focus on the application of cryptography techniques to EH devices, adapting the operations and the implementation of the security operations to the new wave of systems. Specifically, the scientific contributions in this area strive to optimize the implementation and the software/hardware architecture of well-known cryptography approaches, based on the features and requirements typical of energy-harvesting networks. The final aim is to come up with customized versions of cryptography techniques, characterized by either intermittent or less-demanding energy consumption, thus being suitable for integration in devices powered via harvested sources.

Compared to the large amount of scientific contributions investigating data secrecy issues at the physical-layer (see Section V, cryptography approaches can guarantee the specific security service in a deterministic fashion, while physical-layer data approaches are characterized by a probabilistic security protection. At the same time, these approaches usually involve higher demand on the system, thus requiring the implementation of dedicated optimization mechanisms.

An overview of the most important systemic features of these proposals is provided in Table IV. Indeed, despite each of these proposals is specifically meant for a particular EH technique, we argue that the logic and strategies of these proposals can be fully re-used even for additional EH sources and networks, being a valuable alternative to physical-layer security schemes and leading to feasible cryptography algorithms for generic EH networks.

Adapting dynamically the provied security service is one of the earliest strategies realized to cope with the limited energy availability of EH devices, and it has been conceived by the authors in [78], in the context of IEEE 802.15.4 networks. They provided a software solution enabling a constrained WSN device to change at run-time its communication security settings, adapting dynamically to the charge level and increasing the lifetime. Besides, they designed their system to reduce the number of delivered packets (and thus, the energy consumption) when scarce energy is available. They contextualized their proposal and evaluated the energy and lifetime gain via simulations. Recently, the authors in [79] tackled a similar scenario, contextualizing the problem in the novel Software Defined Networking (SDN) computing paradigm.

The authors in [80] proposed a lightweight data scheduling strategy, trading off between data security and energy efficiency. Specifically, the proposed scheduling algorithm includes two security primitives, i.e., a stronger but energy-hungry one and a weaker but energy-efficient one. Depending on the available energy on the wireless platform, for each batch of data, the scheduler selects the most suitable, minimizing the impact of secure data transmission on the lifetime of the EH platform.

The authors in [81] studied energy consumption optimization strategies to balance between security processing and energy harvesting. Considering that during RF harvesting periods the EH device cannot transmit or receive, and that the availability of the RF source is intermittent, the authors compared the effectiveness of either transmitting more small packets or less long packets, as well as running security algorithms, considering the harvesting availability of the devices.

A valuable contribution towards the identification and definition of the energy requirements for the authentication protocols in EH devices has been provided by the authors in [82]. The authors evaluated the energy consumption of 18 different authentication algorithms, measuring the energy expenditure with different software configuration and hardware optimizations. Using a solar-powered MSP430 hardware platform, they confirmed via experimental tests that energy efficiency can be improved by including software optimizations, as well as by a dynamic adaptation of the security level. A similar study has been also provided recently by the authors in [96] on a PIC micro-controller.

Many contributions, such as [83] – [87] exploited pre-computation techniques. Indeed, as discussed in [97], EH networks are characterized by intermittent connectivity and charging periods, where time frames characterized by high energy availability are alternated with periods of scarce charging. In addition, EH circuits in WPCN devices always lose energy after reaching a given re-charge threshold, not fully exploring the advantages of EH capabilities. Thus, pre-computation techniques can be triggered during periods with high energy availability, to both use all the available energy and anticipate energy-demanding tasks, whose execution and energy cost could be too demanding in other time frames. The authors in [83] investigated the adaptability of well-known cryptography algorithms to EH networks. Specifically, they worked on the algorithm part, and they found that pre-computing and storing a few key streams or parts of them can be useful when the system experiences a low charging level. Thanks to hybrid HW/SW optimizations, they optimized the CPU cycles to reduce the time and the energy required by cryptography operations, and they tested their methodology on real devices, such as the MSP430 and the ATMega128L micro-controllers. Pre-computation techniques were also exploited by the authors in [84], to allow devices equipped with both IEEE 802.15.4 communication capabilities and EH principles to integrate dedicated cryptography techniques, such as the Ciphertext Policy - Attribute Based Encryption (CP-ABE) technique. In the proposed framework, namely AGREE, they provided specific optimizations to the CP-ABE cryptography algorithm, they pre-compute scalar multiplications during high-charge periods, and they use the CP-ABE technique to encode a session key instead of the data itself, translating an access control problem into an encryption one. They implemented their strategy in real constrained devices (the TelosB and MicaZ devices charged by photo-voltaic cells), showing the effectiveness and the reduced energy consumption of their methodology for EH networks. Similarly, pre-computation techniques have been used by the authors in [86] to reduce the energy cost of digital signature algorithms by 44%, making them feasible for execution on a solar-cell powered micro-controller.

Considering the heterogeneity in the harvesting capabilities of

TABLE IV
COMPARISON BETWEEN APPROACHES CONTEXTUALIZING CRYPTOGRAPHY SOLUTIONS IN EH NETWORKS.
THE SYMBOL *N/A* INDICATES THAT THE SPECIFIC FEATURE IS NOT APPLICABLE.

Scheme	Scenario	Target Security Service	Solution Type	Assessment Methodology	Hardware Board	EH Source	Proposed Technique
[78], [79]	IEEE 802.15.4	Authentication, Confidentiality, Integrity	Software	Simulations	N/A	Generic	Security service dynamic adaptation
[80]	IMD - WSN	Confidentiality	Software	Real-Devices Experiments	WISP	RF Signal	Security service dynamic adaptation
[81]	IoT	Confidentiality	Software	Simulations	N/A	RF signals	Security service dynamic adaptation
[82]	WSN	Authentication	Mixed Hardware - Software	Real-Devices Experiments	MSP430	Solar cells	Security service dynamic adaptation
[83]	WSN	Confidentiality	Mixed Hardware - Software	Emulation	MSP430 and the AVR ATmega128l	Generic	Pre-computation techniques
[84]	IEEE 802.15.4	Confidentiality, Access Control	Software	Real-Devices Experiments	TelosB	Photovoltaic Cells	Pre-computation techniques
[85]	IEEE 802.15.4	AES	Mixed Hardware - Software	Emulation	MSP430, ARM-Cortex M4	Generic	Pre-computation techniques
[86]	WSN	Digital Signature	Software	Real-Devices Experiments	MSP430	Solar cells	Pre-computation techniques
[87]	IEEE 802.15.4	Generic Exponentiation Operations	Software	Real-Devices Experiments	MagoNode++, TelosB, and MICA2 motes	Photovoltaic cells and micro wind turbines	Pre-computation techniques
[88]	IEEE 802.15.4	Generic Exponentiation Operations	Software	Emulation	TelosB	Generic	Offloading to energy-supplied devices
[89]	WSN	Mutual Authentication	Software	Simulations	N/A	Generic	Implementation optimizations for reduced energy consumption
[90]	WBAN	Mutual Authentication	Software	Simulations	N/A	Electro-cardiac signals	Implementation optimizations for reduced energy consumption
[73]	WSN	Encryption	Mixed Hardware - Software	Real-Devices Experiments	MonoStick	Solar Cells	Implementation optimizations for reduced energy consumption
[91]	IEEE 802.15.4	Authentication and Encryption	Software	Real-Devices Experiments	GreenNET	Photovoltaic cells	RF Operations Optimization
[92]	WSN	Key Agreement	Software	Simulations	N/A	Generic	Optimization based on the energy available on neighboring devices
[93]	IoT	Secure Context Saving	Hardware	Emulation	Not Available	Generic	Dedicated cryptography techniques for context saving
[94]	WSN	Hashing, Encryption	Hardware	Real-Devices Experiments	EHS Platform	Solar Panel	Implementation optimizations for reduced energy consumption
[95]	IoT	Block Ciphers	Software	Simulations	N/A	Generic	Implementation optimizations for reduced energy consumption

an RF EH network, the authors in [88] designed HELIOS, a distributed protocol that allows network elements experiencing low energy availability to outsource the most energy-demanding operations to other nodes in the networks, being them power-supplied or with excess energy available. Considering also the presence of untrusted devices in the network, the authors discussed also specific strategies to reduce the impact of untrusted network elements, thanks to batch verification schemes. The authors extended their study in [87], where they focused on the well-known Elliptic Curve Digital Signature Algorithm (ECDSA) protocol, used for authentication and integrity verification. Specifically, they coupled well-known ECC pre-computation techniques with the energy harvesting concepts previously introduced, optimizing the usage of excess energy and reducing energy waste due to the limited harvesting capabilities of embedded devices. Similar pre-computation optimizations were also provided by the authors in [85], where the authors referred to the excess amount of data generated during excess energy peaks as *coupons*. Such coupons have been demonstrated to be a useful tool to speed up the execution of the Advanced Encryption Standard (AES) algorithm in CTR mode, as well as to speed-up hardware-based random numbers generation.

Other contributions, instead, addressed the energy shortage of EH networks by reducing the overall energy consumption of the security protocol. For instance, the authors in [89] de-

signed a mutual authentication protocol for EH WSN that can split computationally-demanding operations among multiple periods, leveraging energy-aware checkpoints where the state of the system is saved and restored. Similarly, a protocol using electro-cardiac signals for harvesting and key generation has been proposed by the same authors in [90].

In [91], the authors address security issues as well. In particular, the authors introduced and described the novel GREEN-net harvested hardware platform. This platform integrates application-layer security with the OSCAR architecture, which enjoys reduced energy consumption by decreasing the unnecessary handshake operations required by the standardized DTLS protocol.

The authors in [92] focused on the key agreement security problem, and provided a strategy that allows optimizing the pairwise keys selection and distribution in an EH WSN. The optimization consists of balancing the number of reinforcement links and the availability of reinforcement neighbors based on the harvested energy available on the devices willing to share a key. Moreover, it is worth highlighting the recent disclosure of a hardware platform specifically dedicated to the testing of cryptography algorithms in EH-powered devices, recently presented by the authors in [94]. In their demonstration, they showed that a maximum charging time of 60 s is necessary to execute the most energy-demanding cryptography scheme, i.e., HMAC-SHA. While this latter work provides action on the hardware perspective, the authors in [95] focused on the software part, optimizing the size and the operations required by a block cipher to reduce its energy consumption, making it feasible for EH devices.

Finally, in the context of cooperative EH networks, the authors in [27] discussed some countermeasures against the attacks described in Section III. They evaluated the inclusion of a registration authority and a trusted module in each device, to include additional security features in EH Cooperative Networks. High-level countermeasures such as the inclusion of period energy state reports via trusted modules, energy dual signatures via PKI-based methods, and the integration of symmetric and asymmetric encryption techniques are discussed. However, there is no evaluation of their impact on networks with a very limited budget, neither proposals to make their integration energy-friendly.

A. Lessons Learned

From the literature review summarized in the previous subsection, we notice that devices powered via non-RF sources (solar, wind, mechanical, thermoelectric) are usually characterized by higher energy availability per unit of time, if compared to systems powered via RF sources. Therefore, they can likely afford the execution of a limited set of cryptography primitives, optimized in such a way to meet the constraints of these devices.

Without loss of generality, as the most important lesson learned from our study, three main research methodologies have been identified by the literature overview provided in the previous section.

Dynamic Security Service Adaptation. Given that energy availability in EH devices is intermittent, one of the strategies highlighted in the literature is to provide a framework that acts in strict combination with an energy indicator. As soon as more energy becomes available, authentication and confidentiality are strengthened, while they are relaxed when the available energy reduces. Despite such schemes are valuable in balancing energy and security, they are particularly subject to jamming attacks. Indeed, it is enough for the adversary to reduce the charging profile of the device to lower the corresponding security level.

Security Operations Optimization. Following a similar logic to the one already used in constrained environments such as WSNs, other contributions cope with the energy limitation in EH networks by reducing the overall energy consumption of the cryptography protocols. This is achieved both by outsourcing the most demanding security operations and by optimizing the energy cost of some operations within block ciphers, often at the cost of a reduced security level. Despite being less vulnerable to jamming attacks, these strategies are often characterized by a reduced security level, not being suitable for deployment scenarios where adversaries can enjoy unlimited capabilities.

Pre-Computation to Optimize Energy Usage in EH Networks. One of the most effective strategies to provide security in EH networks is pre-computation. Indeed, pre-computation techniques take advantage of the periods when the device is fully powered, and anticipate the execution of the most energy-demanding tasks in these periods. Despite requiring significant engineering efforts on the cryptography protocols logic, pre-computation techniques allow maintaining the same security level of well-known solutions, successfully defeating both temporary jamming attacks and powerful adversaries. However, there are two main drawbacks. First, when the device experiences a prolonged period of reduced energy availability, the pre-computed values could be exhausted, leaving the device with no more energy to execute security tasks. Second, the design of pre-computation strategies should be validated by the scientific community, avoiding the creation of vulnerabilities in widely-accepted cryptography techniques.

B. Future Directions

A few appealing research directions for cryptography solutions in the context of EH networks are provided below.

Optimization Strategies Integration. Despite the three strategies discussed in the previous subsections have received significant attention from the latest literature, still the integration between such strategies has not been explored. For instance, coupling the optimization of encryption operations with the dynamic adaptation of the security service could increase the minimum security level of the device. In this context, efficient frameworks are required to synchronize energy availability, expenditure, and security level tuning operations.

EH Platforms Security Evaluations. At the time of this writing, there is no scientific contribution experimentally validating the security of cryptography solutions on EH devices. Indeed, benchmarking the security of solutions tailored for EH devices, such as pre-computation techniques, is crucial to validate their strength and refine their security against evolving

adversaries. In parallel, automatic security validation tools could help in establishing the security of either code optimization techniques and pre-computation strategies, avoiding the deployment of possibly weak security techniques.

V. Data Secrecy Issues in Energy Harvesting Networks

Building on the very limited energy availability of EH networks and the general unsuitability of traditional cryptography techniques, several scientific contributions provided strategies to enforce physical-layer data secrecy in EH networks. More in detail, the schemes discussed and cross-compared in Section V implicitly assume that EH-powered devices are not able to run cryptography primitives, and thus they can neither encrypt data nor manage energy-consuming TCP-s connections. Thus, without any further protection, the related RF communications would be easily eavesdropped by a passive adversary. This is the reason motivating the intensive literature production intended to achieve security via non-cryptography schemes.

These contributions largely focused on RF EH, for two main reasons. First, as highlighted by the comparison in Table II, RF EH harvesting techniques usually provide the least amount of power per time unit, justifying the assumption about the impracticality of cryptography techniques [98]. Second, the research community has been attracted by the challenging trade-offs between energy, security, throughput, and reliability, typical of wireless-powered networks.

In this section, we first introduce the security objectives most used when investigating data secrecy at the physical-layer (see Section V-A). Then, we describe the logic driving the introduction of relaying and friendly jamming strategies in RF EH networks (see Section V-B and Section V-C). Without loss of generality, we notice that, despite investigating all the same security metrics discussed in Section V-A, the contributions available in the literature are characterized by many differences, related to the assumed scenario, the adversarial model, and the specific objective.

To provide a meaningful and insightful overview of these works, we split the overall literature into three main categories, according to the specific adversarial model. Three adversarial models are mainly assumed: (i) external (Section V-D); (ii) internal (Section V-E); and, (iii) untrusted relays (Section V-F). The most important take-home messages arising from our discussion are summarized in Section V-G, while Section V-H highlights appealing future research directions in the area.

We remark that this section investigates and classifies only scientific contributions specifically tackling data secrecy security issues in EH networks. Thus, schemes focusing on EH network performance, not considering security issues, are out of scope for our work (indeed, exhaustive description and classification of these approaches can be found in dedicated surveys, such as [35] and [34]).

A. Security Objectives

The operations of ABCN, WPCN, and SWIPT networks can be optimized based on several design objectives, by selecting suitable beamforming vectors, or optimizing the transmission strategies and the deployment of the entities in the system.

Several features are optimized in the literature, including the total transmission power at the transmitter, the energy expenditure at the receivers, the harvested power, and the throughput of the communication link.

In this manuscript, being focused on security issues, we are particularly interested in two security-related metrics, which are the *secrecy rate* and the *secrecy outage probability*.

Considering an eavesdropper E is deployed in the scenario and it is interested in the correct decoding of information directed toward one of the legitimate devices, the *secrecy rate* of the legitimate source-to-destination communication link at the physical layer is defined as in the following Eq. 14:

$$S_n = C_n - C_e, \tag{14}$$

where C_n is the capacity of the legitimate channel and C_e is the capacity of the channel source-eavesdropper [99]. A large part of contributions in the literature formulate proposals to maximize the secrecy rate (Secrecy Rate Maximization (SRM) problem), by suitably selecting the power splitting ratio, the time splitting factor, and the weights in the beamforming vector. At the same time, other contributions investigated the performance bounds of the secrecy capacity, such as the strictly positive secrecy capacity (SPSC) problem, defined as the probability that the secrecy capacity remains strictly positive.

Another important security metric evaluating the physical layer data secrecy of a transmission scheme is the *Secrecy Outage Probability (SOP)*, defined as the probability that the instantaneous secrecy capacity drops below a specific threshold value S, as defined in the following Eq. 15

$$SOP_n = Pr\left(S_n < S\right) = Pr\left[\log_2\left(\frac{1+SINR_n}{1+SINR_e}\right) < S\right]. \tag{15}$$

Few papers in the literature focused on an additional security-related metric, which is the *Ergodic Secrecy Rate (ESR)*. It is defined as the maximum achievable transmission rate of the legitimate link, not enabling correct decoding of the information on the eavesdropper. As in the following Eq. 16, it can be modeled as the average of the instantaneous secrecy rate jointly considering all the possible channel realizations:

$$\begin{aligned} E_n &= E\left[C_n - C_e\right] = \\ &= E\left\{\frac{1}{2}\left[\log_2\left(1+SINR_n\right) - \log_2\left(1+SINR_e\right)\right]^+\right\}, \end{aligned} \tag{16}$$

where the operator $(\cdot)^+$ refers to the maximum positive value.

Other scientific contributions such as [100], [101], and [102], focused on the optimization of the *Secrecy Energy Efficiency (SEE)* metric, that is a trade-off between the secrecy rate of the communication link and the energy consumption on the EH devices. In practice, energy metrics (such as the power consumption on the transmitter and the consumed energy at the receiver) are coupled with the above security metrics, not to decrease below a given threshold.

Finally, it is worth noting that the above-introduced metrics could also be treated as constraints of an optimization problem. Thus, many contributions in the literature focus on the optimization of a non-security-related metric, while minimum constraints on the secrecy rate or maximum constraint on the secrecy outage probability are included in the optimization problem to still guarantee data secrecy at the physical layer.

B. Relaying Models and Strategies

While the above considerations are valid for single-hop EH networks, many contributions in the literature also investigated multi-hop scenarios, where either the receivers forward the information to intermediate nodes in the network or there is not a direct link between the source and the intended destination. In these cases, dedicated relaying nodes are introduced to accomplish communication tasks.

To enable energy harvesting and information forwarding at the same time, two relaying strategies are mainly discussed in the literature, namely *Decode and Forward (DF)* and *Amplify and Forward (AF)*.

In the DF mode, after the reception of the signal, the relay decodes and re-transmits it as a new signal. In the AF mode, instead, without decoding the signal, the relay amplifies it using a power factor depending on the amount of harvested energy. It is worth noting that, as discussed by the authors in [103], either the TS or the PS hardware architectures can be adopted on the relay for EH and information processing, leading to different SNR, throughput, and security considerations.

While most of the scientific contributions assumed trusted relays, few of them introduced untrusted relays and provide strategies to protect the information from *honest-but-curious* relays, achieving their forwarding tasks but also interested in stealing the information. More details on this adversary model are provided in Section V-F.

C. Artificial Noise

As discussed in the previous sections, the security of the legitimate source-destination communication link, evaluated through metrics such as the secrecy rate and the secrecy capacity (see Sec. V-A), is strictly dependent on the difference between the SINR at the legitimate destination and the SINR experienced by the eavesdropper. Thus, an effective strategy to further reduce the SINR at the eavesdroppers is to deploy a *friendly jammer*. A friendly jammer emits artificial noise on the communication channel in a way that its effect is almost nullified at the legitimate receiver, while it is amplified on any other device in the network, leading to an overall decrease of the SINR.

Artificial noise can be introduced in the network by different entities, i.e., a helper node and the destination. When artificial noise is introduced by the helper, the scenario typically involves a dedicated jammer device, continuously emitting noise on the channel. Other contributions couple the roles of the relay and the jammer, selecting helper devices in the set of relays that are not used for signal relaying at a particular time.

At the same time, artificial noise can be also introduced by the legitimate destination when the receiving device is equipped with multiple antennas. In this case, while one or more of the antennas are receiving the signal, the remaining ones emit artificial noise, summing up (in voltage) to one of the legitimate signals. On the one hand, the signal available at the receiver results corrupted by the noise. On the other hand, given that the receiving node is aware of the samples of the noise, it can cancel out (by subtraction) the intentional interference and confidentially recover the original signal. Several schemes employing friendly jamming are discussed in the sections below.

D. External Adversaries

We define an *external* adversary as a device that does not take part in the regular communication patterns in the network, thus remaining *anonymous* to the network devices. This scenario is typical of any wireless network scenario, including WSN and IoT networks, where an external eavesdropper simply needs a receiving antenna tuned on the same frequency of the legitimate communication channel to successfully decode the information — assuming no cryptography techniques are deployed.

The distinguishing feature of these works is the unavailability of any information about the adversary. From the model perspective, this assumption translates in the general unavailability of the Channel State Information (CSI) experienced by the eavesdropper communication links, further complicating the design of an optimally-secure solution. Indeed, with no information about the adversary and the quality of the channel it experiences, it is possible to work only on the main communication links, either minimizing the probability that the information is correctly decoded by other devices in the network or maximizing the secrecy rate of the main communication links.

A classification of the scientific contributions assuming external adversaries is provided in Table V, considering the features and capabilities of the adversaries. It is worth noting that all the scientific contributions discussed hereby assumed completely-passive eavesdroppers, that do not transmit anything on the RF spectrum.

We notice that, overall, very different adversarial models are considered in the literature.

Single Single-Antenna External Eavesdropper. The simplest adversary model is a single external eavesdropper, equipped with a single omnidirectional antenna, such as the one assumed in [104]— [117].

To provide a few examples, the authors in [104] contextualized the concepts of RF-SWIPT in Visible Light Communications (VLC) systems, studying the energy harvesting performance when visible-light signals are used as a source. Assuming a single-antenna eavesdropper and a random location of the eavesdropper to the receiver, they derived the exact analytical expressions of the asymptotic SOP, by using the stochastic geometry method, and they evaluated the overall secrecy rate via simulations. Assuming the same adversarial model, the authors in [106] provided a significant contribution to the definition of the secrecy rate that can be achieved via cooperative

TABLE V
QUALITATIVE COMPARISON AMONG APPROACHES INVESTIGATING PHY-LAYER DATA SECRECY IN EH NETWORKS CONFRONTING EXTERNAL EAVESDROPPERS.

Adversary	CSI Availability	Adversarial Distribution	Collusion	Adversarial Receiving Antennas	Adversarial Antenna Type	Adversary Mobility	Distance Considera-tions	Scheme	Security Treatment
External	✗	Single	✗	Single	Omni-directional	✗	✗	[104], [105], [106]	Minimum SOP
								[107]	Constraint, Minimum SOP
								[108], [109], [110]	Average Secrecy Rate
								[111]	SOP, ESR
								[112]	SOP, SRM
								[113], [114]	Secrecy Capacity Maximization
								[115]	SPSC Bounds
								[116]	Secrecy Outage Capacity
								[117]	SOP, Secrecy Rate
								[118]	Multiple Users Secrecy Rate
								[119]	Secrecy Rate
External	Imperfect	Single	✗	Single	Omni-Directional	✗	✗	[120], [121]	SRM
								[122]	SOP and SPSC probability
								[123]	SOP
External	✗	Single	✗	Multiple	Omni-Directional	✗	✗	[124]	SRM
								[125]	Constraint, Minimum Secrecy Rate
								[126]	SOP Minimization
External	✗	Multiple	✗	Single	Omni-Directional	✗	✗	[127], [128], [129]	Secrecy Capacity Definition and Maximization
								[130]	SOP
								[131], [132]	SRM, SOP Minimization
								[133]	Constraint, Minimum SOP
								[134]	Secrecy Capacity
External	✗	Multiple	✗	Single	Directional	✗	✗	[135]	SRM, Ergodic Secrecy Capacity
External	Imperfect	Multiple	✓	Single	Omni-Directional	✗	✗	[136]	SOP
External	Imperfect	Multiple	✗	Multiple	Omni-Directional	✗	✗	[137], [138]	Constraint, Minimum Secrecy Rate
								[139]	SOP
								[140]	Secrecy Rate
External	Imperfect	Multiple	✗	Single	Omni-Directional	✗	Imperfect Locations	[15]	Secrecy Rate
External	✗	Multiple	✗	Single	Directional	✗	HPPP	[141]	Secrecy Rate
								[142]	Lower-bound SRM

jamming strategies. They showed that the deployment of a full-duplex jammer node can improve significantly the secrecy rate, and such improvement is highly dependent on the time split ratio for EH activities, the features of the channel, and the topology of the scenario. The authors in [109] focused on buffer-aided networks, where the messages can be temporarily stored on the relays for several slots, waiting to select the transmission link that maximizes the communication secrecy. Assuming either an offline or an online knowledge of the main communication channels, the authors developed a protocol that can jointly optimize the power allocation at the transmitter and the secrecy rate at the receiver, considering the relay transmit power optimization and link selection strategies. We also highlight the work by the authors in [116], wherein a constrained relay is considered. This relay is equipped with a large number of input and output antennas, according to the Massive-Multiple-Input Multiple-Output (MIMO) technology. The authors unveiled explicit closed-form expressions for the secrecy outage capacity of a link where the above-described relay is deployed, both assuming the Amplify and Forward and the Decode and Forward relaying mode.

While the previous contributions assumed no knowledge and previous information about the adversarial channel, the authors in [120]— [123] worked with the *Imperfect CSI* assumption, still considering a single adversary with a single antenna. In these settings, they evaluated the impact of such an assumption on the achievable security metrics.

For instance, the authors in [120] considered a generic Multiple-Input Single-Output (MISO) scenario. However, differently from previous works, they maximize the worst-case secrecy rate of the communication link by decoupling the optimization problem into three unique optimization problems. Using such a strategy, they found a locally-optimum solution utilizing the alternating optimization algorithm. In the context of a multi-relay network, the authors in [121] introduced a relay selection scheme where the relays that can not decode the signal assume the role of friendly jammers, further improving the physical layer security of the scheme compared to regular beamforming schemes. Differently, the authors in [122] focused on the design of a novel jammer, working accordingly to the *Accumulate-and-Jam* logic. This jammer, being energy-constrained, stores energy locally and then uses such energy to perform cooperative jamming. It is worth noting that, differently from other approaches, here the focus is mainly on the communication link between the source of a message and the jammer, where the jammer is intended as a destination. The authors investigated both the design logic of the jammer and its performance in a wiretap channel, considering a single-antenna eavesdropper. Finally, they show the benefits of such design compared to a regular Half-Duplex approach.

Single Multi-Antenna External Eavesdropper. While the above contributions assumed a single adversarial device equipped with a single antenna, other works, such as [124]— [126] provided similar studies assuming a more powerful external adversary, characterized by multiple receiving antennas. For instance, the authors in [125] analyzed the effect of non-idealities such as residual hardware impairments in EH devices, CSI imperfections, and non-linearity of EH circuits on the security and energy performance of a SWIPT EH network. In this challenging system model, they considered the secrecy rate of the system toward a multiple-antenna eavesdropper, and they minimized the total power consumption while, at the same time, guaranteeing the minimum required secrecy rate of the main communication links.

Multiple Non-Colluding Single-Antenna External Eavesdroppers. A slightly different adversarial model is the one where there are multiple adversaries, each equipped with a single omnidirectional receiving antenna. It is worth noting that this adversarial model could be either more powerful or similar to the one where there is a single adversary equipped with multiple antennas, based on the possibility that the adversaries collude. Indeed, if the adversaries do not collude, i.e., do not share information, this model has the same strength and modeling than the single adversary - single antenna attacker model. Instead, when the adversaries can share information, additional statistic analysis and processing tools can be used, based on the difference in the location where the raw signals are acquired.

The contributions in [127]— [133] assumed non-colluding adversaries, and investigated the secrecy and energy performance of RF EH networks in this adversarial models. For instance, the authors in [127] considered a MISO system, where a single source node, equipped with multiple antennas, would like to transmit a signal to a specific destination node. The authors formulated an optimization problem by defining the channel secrecy capacity as the system performance metric to be optimized, and they used the semi-definite relaxation mathematical tool to solve the optimization problem. Their general finding is that increased values of the SINR lead to increased secrecy capacity, while the proposed resolution strategy helps to reduce the overall transmit power to achieve a given level of secrecy capacity, compared to traditional approaches. Assuming the same adversarial model, the authors in [128] considered the effect on the secrecy rate of destination-assisted jamming, as discussed in Section V-C. Assuming a relay-based network working in the AF mode, they organized the transmission of the secret signal in two stages. In the first one, when the source node transmits the signal to the relay, the destination emits artificial noise to both protect the secrecy of the signal and power the relay node. Then, in the second phase, the destination receives the message from the relay and cancels out its own signal, recovering the intended message from the source node. The authors provided a thorough investigation of the secrecy capacity in this scenario, assuming either TS-based or PS-based hardware architecture, and considering the impact of several system parameters, including the time dedicated to EH, the power splitting ratio, the noise, and the location of the participating entities. Their study revealed that PS generally outperforms TS when all the other parameters do not change. Besides, they analytically proved that the secrecy capacity of the system can be maximized in several different ways, including the increase of the number of relays, the noise power, and the distance of the eavesdropper to the main communication links.

The performance in the presence of a dedicated friendly

jammer device are investigated by the authors in [131], assuming both the knowledge and the absence of the CSI of the eavesdroppers. Assuming a MISO scenario, the authors investigated the SRM and the SOP minimization in a WPCN, where the jammer is powered via EH and follows a TS logic. They also extend the results to a MIMO scenario, demonstrating that their solutions are even more successful in protecting data at the physical layer when more users and more eavesdroppers are considered.
A novel two-way relaying WPCN scenario has been considered by the authors in [129], where a source node eliminates its own component from the signal received by the relay, through self-cancellation techniques. In this novel setting, the authors derived optimally secure protocols based on power-splitting and time-splitting, able to maximize the secrecy capacity of the link assuming multiple non-colluding eavesdroppers.

Multiple Non-Colluding Multi-Antenna External Eavesdroppers. Multiple non-colluding eavesdroppers equipped with multiple antennas are considered by the contributions in [137]— [140]. For instance, the authors in [138] jointly used constructive interference and artificial noise to achieve secure communications in SWIPT systems. Assuming the sample case of an 8-PSK modulation, they showed that constructive interference pre-coding schemes can achieve significant power savings compared to interference management approaches, while also getting rid of EH outages that characterize legacy approaches. While the main focus on this contribution is on the power management part, the secrecy rate of the link is considered as a constraint of the problem, in a way to decade below a given acceptable threshold.

Multiple Colluding External Eavesdroppers. Multiple colluding external adversaries have been considered recently, only by the authors in [136]. In this context, the authors first verified that colluding capabilities improve the performance of the adversary, thanks to the sharing of information. In addition, they demonstrate that a trade-off between security and reliability exists. Indeed, when more relaxed constraints on the secrecy outage probability are imposed, higher SINR values can be achieved, improving the reliability of the communication link.

Directional Antennas. Other significant contributions are the works in [135]— [142], where multiple non-colluding adversaries are equipped with directional antennas. In particular, while omnidirectional antennas are characterized by almost an equal receiving range in all directions, directional antennas can boost the receiving range along a particular direction. From the security perspective, this is an additional powerful feature, as it can help to eliminate interferences caused by other RF activities, while focusing on a given target device or communication link.
Specifically, the authors in [142] focused on a mmWave IoT relay network, where the relays are mobile Unmanned Aerial Vehicless (UAVs). A unique assumption of this work is the inclusion of a statistical distribution of the distance of the eavesdroppers from the main communication link, following an independent Homogeneous Poisson Point Process (HPPP) distribution with density λ on the ground. The inclusion of directional antennas is modeled via the usage of a 3D antenna gain model, to approximate the antenna gain pattern of all nodes, as described in [143]. The authors analyzed the impact of the density and the distribution of the adversaries around the target device, deriving lower bounds on the average secrecy rate relatively to the transmit power, the power splitting ratio and the deployment of the UAVs. In [141], the same authors of the above cited paper, were among the first ones to investigate the secrecy performance of mmWave SWIPT UAV-based relay systems. An important difference characterizing this work is in the model of the air-to-ground channels, that are considered as Nakagami-m small-scale fading. Under these new assumptions, the authors computed the expressions of the achievable secrecy rate, assuming both Detect-and-Forward (DF) and Amplify-and-Forward (AF) schemes at the relay, and they investigated the relationship between all the metrics of the system.

The usage of UAVs as elements of the network infrastructure can be found also in the contribution by the authors in [15]. A distinctive feature of this work is in the application of EH capabilities on the UAVs, essentially for information decoding and relay, while an onboard battery supplies energy for the flight control of the UAVs. The authors assume multiple non-colluding terrestrial eavesdroppers, trying to infer on the data transmitted by a source, and relayed by the UAVs to the intended destination. In this scenario, they derived the secrecy rate of the communication link, considering as a new factor of the optimization problem the relative position of the UAV toward the source and the destination. UAVs are also used as transmitters in the contribution by the authors in [119], in combination with the Non-Orthogonal Multiple Access (NOMA) technique to achieve secure transmissions against a single single-antenna eavesdropper. To further improve the secrecy of the communication, the authors use artificial friendly jamming, to further decrease the chances for the eavesdropper to fully decode the data delivered by the UAV. Considering a non-linear EH model, the authors derived the secrecy rate of the communication link and maximize jointly the throughput of the communication link, the TS ratio, and the PS ratio.
Finally, we highlight that while these valuable contributions brought the novelty of directional antennas in the RF EH physical-layer security area, they did not explore collusion capabilities, still posing severe constraints on the capabilities of the adversary.

E. Internal Adversaries

We define an *internal* adversary as a device that is a legitimate member of the network, actively taking part in the network activities by transmitting and receiving information. In the physical-layer security literature for RF EH networks, such an adversarial model is often referred to as an *active eavesdropper*, being it characterized both by active legitimate features (authorized transmissions/reception operations) and by unauthorized passive features (i.e., unauthorized passive eavesdropping of the communications) [144].

While this scenario could be typical of any wireless network, it is particularly adopted in the context of Cognitive Radio Networks. Specifically, Cognitive Radio Networks (CRNs)

involve both primary users and secondary users. Primary users are express-class licensed devices that pay a fee to experience a minimum guaranteed level of Quality of Service (QoS) for their traffic. Secondary users, often referred to as *cognitive users*, are non-licensed users that are allowed to use the same spectrum of primary users provided that their RF operations do not interfere with them or do not cause excessive degradation of the service offered to primary users. Overall, a CRN is classified based on the paradigm used by secondary users to access the spectrum, and it can be either interweave, underlay, or overlay. While the underlying logic and techniques used by CRNs are out of the scope of this contribution, the most interesting feature of CRNs within the scope of this survey is the assumed knowledge of the presence of eavesdropping adversaries, often identified in the secondary users, interested in decoding RF activities of the primary users.

Given that these devices are part of the network and actively participate in the communications, the CSI experienced by these devices can be assumed as well-known or, at least, statistically available on the source of the confidential communication. Thus, the transmission and the security of the communication link can be optimized by degrading its perceived quality on the eavesdroppers, boosting its secrecy rate.

A comprehensive classification of the scientific contributions assuming internal adversaries is provided in Table VI, with reference to the features and capabilities of the adversaries.

Single Single-Antenna Internal Eavesdropper. The most common scenario investigated in the literature assumes a single internal adversary, whose CSI is well-known, equipped with a single omni-directional antenna, as in the contributions by the authors in [145]— [168].

To provide a few examples, the authors in [150] were the first to consider a system with a single source node and one destination node, where the information transfer is aided by a network of cooperative relays. In this scenario, all the relays work according to the EH-TS logic, and they are partitioned in two subsets. Some of them only forward packets to the destination, while the remaining ones, also referred to as *helpers*, act as friendly jammers, injecting random noise. This *jamming* operation is performed smartly, to minimally affect the SINR of the signal on the intended destination, while degrading the most the SINR at any other location. At the same time, the scenario includes a single-antenna eavesdropper, located far from the main communication links. In the paper, the authors obtained via the semi-definite relaxation mathematical tool the configuration of the beamforming matrix that can achieve the maximization of the secrecy rate of the main communication link, by also controlling the power consumption on the relays. Considering the same system scenario and adversary model, the authors in [159] extended the analysis, and they found that the secrecy of the data can be enhanced either by increasing the number of relays, or by increasing the SINR at the destination, or by balancing the TS ratio between energy harvesting and information decoding.

In the same network model assumed by the authors in [159], the authors in [149] modeled the batteries of the destination node as a queuing system, and they proposed a scheme to maximize the secrecy rate optimizing the transmission time of the source node. At the same time, the artificial noise emission by the jammer is optimized to cancel at the destination's location, while being effective at other locations. Assuming a similar scenario than [159] and [150], the authors in [145] considered an SR hardware design, and a single relay, only working according to the TS-AF scheme. The authors assumed that the CSI of the whole network is known and, under this assumption, they proposed an iterative algorithm rooted in the Constrained Concave Convex Procedure (CCCP) mathematical tool. Their proposed algorithm provides a locally-optimum solution, maximizing the secrecy rate of the link, simultaneously fulfilling the constraints on the overall transmission power and harvested energy on the receiver. Still assuming a SISO system but with a Power Splitting (PS) hardware architecture, the authors in [146] first introduced the concept of the active eavesdropper. They focused on the relaying logic, evaluating the secrecy capacity of the communication link when either the DF or the AF strategy is used by the EH relays. Via Monte-Carlo simulations, they demonstrated the DF strategy to be more *confidential* than the AF strategy, and that both the strategies have the potential to improve the secrecy rate when an increased number of relays are deployed, and when the relays are closer to the destination than the eavesdropper. A MIMO system has been considered by the authors in [147], where the receivers are based on the Separate Receiver (SR) hardware architecture. Initially, without including any relay nor jamming activity in the system model, they considered two specific scenarios (single-stream and full-stream), and for each of them they point out globally optimum solutions based on the semi-definite relaxation mathematical tool. Then, for an expanded scenario including relays producing artificial noise via jamming, they discuss the solution of an equivalent problem based on the Inexact Block Coordinate Descent (IBCD) algorithm, and they evaluate its performance in maximizing the secrecy rate of the communication link. In the same scenario, the authors in [148] considered a receiver equipped with only a single antenna, and modeled the channel as slow-fading. They formulated the optimization problem to maximize the worst-case secrecy, assuming the overall transmission power and the amount of harvested energy as the constraints of the optimization problem.

Despite many contributions considered the involvement of relays in the system, the reason motivating network devices to behave as nodes has received only minimal attention by the community. In this context, a pioneering contribution has been provided by the authors in [153], where the relays are selected by the transmitter from a set of devices, and they are following remunerated in the form of minimum provided energy, that can be harvested and used by the relay to fulfill their own tasks in the network. To ensure fair participation of the relays, and to motivate them to reveal trustful information, the authors developed a relay selection strategy enforcing their honest behavior, while dishonest ones are penalized by decreasing their trust degree.

The secrecy rate at the physical layer has been investigated also by the authors in [154], considering a network using the Orthogonal Frequency Division Multiplexing (OFDM)

TABLE VI
QUALITATIVE COMPARISON AMONG APPROACHES INVESTIGATING PHY-LAYER DATA SECRECY IN EH NETWORKS CONFRONTING INTERNAL ADVERSARIES.

Adversary	CSI Availability	Adversarial Distribution	Collusion	Adversarial Receiving Antennas	Adversarial Antenna Type	Adversary Mobility	Distance Considera-tions	Scheme	Security Treatment
Internal	✓	Single	✗	Single	Omni-Directional	✗	✗	[145], [146], [147], [148], [149], [150], [151], [152], [153], [154], [155], [144]	SRM
								[156]	SRM, Constraint SOP
								[157]	Constraint, Minimum Secrecy Rate
								[158], [159], [160], [161], [162], [163], [164]	SOP Minimization
								[165], [166]	Secrecy Capacity Definition and Maximization
								[167]	Eavesdropping Probability
								[168], [169]	Secrecy Rate - Harvesting Ratio Trade-Off
								[170]	Secrecy Throughput
Internal	Imperfect	Single	✗	Single	Omni-Directional	✗	✗	[171]	Constraint, Minimum SOP
Internal	✓	Single	✗	Multiple	Omni-Directional	✗	✗	[172], [173]	Minimum SRM
								[173]	ESR
								[174]	Constraint, Minimum Secrecy Rate
Internal	✗	Single	✗	Single	Omni-Directional	✗	✗	[175]	SOP, SRM
Internal	N/A	Single	✗	Multiple	Omni-Directional	✗	✗	[176]	Avg. Secrecy Capacity, Lower Bound SOP
Internal	✓	Multiple	✗	Single	Omni-Directional	✗	✗	[177], [178]	Constraint, Minimum Eavesdropper SINR
								[179], [180]	Constraint, Maximum SOP
								[181], [182]	Constraint, Minimum Eavesdropper Secrecy Rate
								[23], [183], [184], [185], [186]	SOP
								[187], [188]	SRM
Internal	Imperfect	Multiple	✗	Single	Omni-Directional	✗	✗	[189]	SOP
								[190]	Constraint, SOP
Internal	✗	Multiple	✗	Multiple	Omni-Directional	✗	✗	[102], [100], [101]	Constraint, Minimum Secrecy Rate
								[139]	SOP
Internal	✓	Multiple	✓	Single	Omni-Directional	✗	✗	[191]	SOP
Internal	Imperfect	Multiple	✓	Single	Omni-Directional	✗	✗	[192]	SRM
Internal	✓	Multiple	✓	Multiple	Omni-Directional	✗	✗	[193], [194], [195]	Constraint, Maximum Outage Secrecy Rate

scheme. To improve the achievable secrecy rate, the authors deployed a jammer that is cooperative with the legitimate devices. The jammer works accordingly to the harvest-and-jam logic, gaining energy from the information message in the first phase of the information transmission, and jamming the message at the eavesdropper in the second phase. Differently from previous contributions assuming this scenario, following a logic similar to the previous contribution in [196]. the authors considered two different kinds of receivers, namely Type I and Type II, equipped or not with the capabilities of removing the noise on the reception side, respectively. Thus, they derive SRM definition in this scenario with the above constraints, optimizing simultaneously the source transmit power and the jammer signal over the OFDM sub-carriers.

The authors in [158] used artificial noise at the transmitter, by splitting the transmission power into two parts: one for information transmission and one for noise emission. A key pre-distribution scheme is assumed between the transmitter and the receiver, in a way that the noise could be canceled out at the receiver but not at the transmitter.

The authors in [157] integrated SWIPT concepts within cellular networks based on the Orthogonal Frequency Division Multiplexing Access (OFDMA) modulation scheme. Specifically, assuming the secrecy rate as a constraint of the problem, they provide two sub-optimal solutions for the maximization of the harvested power, by efficiently allocating the power on different sub-carriers. The authors in [160] derived the SOP of two competing antenna-selection schemes, namely the optimal antenna selection (OAS) scheme and suboptimal antenna selection (SAS). They compared the performance of these schemes against traditional transmission schemes via simulations, verifying that OAS outperforms SAS when RF constraints are considered. Differently from other contributions, the authors in [156] investigated also power optimization problems on the transmission side. Specifically, they evaluated the best power control policy on the transmitter, achieving the secrecy rate maximization on the receiver. To this aim, they derive a relationship between the secrecy rate and the SNR at the receiver, developing an algorithm that reduces at minimum the complexity and the computational burden on the transmitting device. Moreover, their evaluation shows that a high transmission power does not guarantee, at the same time, minimum secrecy rate and energy harvesting requirements. An interesting contribution is provided also by the authors in [166]. In this contribution, the authors proposed two relaying schemes based on power splitting and time-splitting (namely, PSR and TSR), where the relays can tune the ratios in a way to trade-off computational and harvesting processes. Interestingly, they provide results showing that the channel information at the eavesdroppers does not affect these metrics (note that the usefulness of the CSI is not discussed in the derivation of the maximum secrecy rate of the system). Finally, they show that the PSR scheme outperforms the TSR when secrecy capacity is considered.

It is worth also mentioning the work by the authors in [144], where the adversary is a jammer, besides being characterized by the standard eavesdropping capabilities.

The *Imperfect CSI* assumption is used in [171], still considering a single single-antenna eavesdropper scenario. The authors assumed the secondary users to be energy-constrained devices, requiring power from the primary users to operate in the network. Given that these devices are constrained, the authors assume that they do not have enough capabilities to perform energy harvesting and data decoding at the same time; thus, a TS architecture is assumed. In this context, the authors designed a multi-objective optimization framework based on a Pareto-optimal resource allocation algorithm, leveraging the weighted Tchebycheff approach, where the maximization of the secrecy rate is one of the objectives of the optimization.

Single Multi-Antenna Internal Eavesdropper. A single internal eavesdropper equipped with multiple antennas is considered by the authors in [172]— [174].

The contribution by the authors in [173] is particularly interesting from the security perspective, given that they considered not only information eavesdropping but also unauthorized EH activities. This work considered the adversary as a two-antenna active energy harvester, working according to the SR logic, able to legitimately harvest energy via one antenna, and illegitimately and actively eavesdropping the signal using the second antenna. Therefore, during information transmission activities, this node is a regular eavesdropper. At the same time, during EH activities, it is interested in acquiring much energy and recharging its battery more than expected, using hardware circuitry that is more performant than the legitimate devices. The authors formulated asymptotic expressions of the lower bound on the ESR and the average harvested energy, and they used these results to optimize the system design, reducing the power and information leakage based on several system parameters. They also demonstrated the existence of a trade-off between the worst-case ESR and the worst-case average for the harvested energy. It is worth also mentioning the recent work in [174], where the authors experimentally verified their findings through a real proof-of-concept, using off-the-shelf Software Defined Radios and backscatter systems. Note that this is the only work on physical-layer data secrecy that provides experimental tests and verification of the theoretical findings. No knowledge about the eavesdropper's channel conditions is also assumed in the work by the authors in [176], where a Nakagami-m channel model is assumed. The context assumed by this work is very specific, as it considers a SIMO RF network integrating SWIPT concepts mixed with a free-space optical communication link. The authors considered a single energy harvesting receiver, potentially behaving as an eavesdropper, and they investigated the average secrecy capacity and the lower bound of the SOP taking into account different physical-layer parameters, such as the architecture of the receiver and the deployment of multiple antennas.

Multiple Single-Antenna Internal Eavesdroppers. Multiple non-colluding eavesdroppers equipped with single omni-directional antennas are considered as adversaries in [177]— [188]. Specifically, the authors in [177] have been the first to integrate EH concepts in the context of cellular networks. Here, the Cellular Network Base Stations are assumed as the transmitters, and the authors investigated the secrecy capacity of the link assuming the receivers are equipped with EH modules (considering an SR hardware architecture). The

authors formulated the optimization problem to minimize the overall transmit power of the system, while taking the link secrecy rate as a constraint of the optimization problem, and they used the Semi-Definite Relaxation tool to find a convex form of the problem.

The authors in [184] proposed a protocol to enhance the secrecy rate of a WPCN, thanks to the deployment of a power beacon. First, the power beacon transmits RF energy to charge a node. Then, it protects the transmission of this device by emitting friendly jamming, thus degrading the SNR at the eavesdroppers. They studied the problem using finite-state Markov Chains, deriving the expressions of the SOP and secrecy rate in this scenario, evaluating also the reliability and security of the communication link.

In the context of overlay CRNs, the authors in [185] proposed and evaluated a dedicated scheme, namely EARTH, where the residual harvested energy is assumed as a constraint of an optimization problem. Assuming as a metric the trade-off between secrecy rate and outage probability, they derived the SOP of the system and compared its performance against standard scheduling methods, such as round-robin, showing superior performance. Assuming a MISO scenario, the authors in [188] considered the maximization of the sum logarithmic secrecy rates, by considering energy harvesting constraints. To achieve the objective, they use specific optimization tools, such as the Software Defined Radio (SDR) and the successive convex centralized beamforming design. They demonstrated that the transmission of single streams does not affect the secrecy rate.

Imperfect knowledge of the adversarial CSI is assumed in the works by the authors in [189] and [190]. In particular, the authors in [189] provided a complete study on the performance of EH-NOMA schemes in CRNs, by assuming a realistic non-linear EH model. Also in this case, the physical-layer data secrecy is enhanced thanks to the deployment of cooperative jamming techniques. The authors used the SDR method to derive closed-form expressions for the problem, and showed that their proposed solution achieves better secrecy rate than the conventional OFDM schemes.

Multiple Non-Colluding Multi-Antenna Internal Eavesdroppers. Multiple non-colluding multi-antenna eavesdroppers are considered in [100]— [102], and [139], all investigating the SEE problem. Besides introducing and formalizing the SEE problem, the authors in [100] investigated a weighted-sum secrecy rate maximization problem, considering at the same time the secrecy rate of the communication link and the total power consumption on the transmitter. They solved the problem using an iterative algorithm based on the Dinkelbach method [197], and they validated the effectiveness of such a method via numerical analysis. In the context of overlay CRNs, the authors in [139] proposed optimal relay selection (ORS) strategies assuming both the time switching relay (TSR) protocol and power splitting relay (PSR) protocol. They derived exact closed-form expressions related to the SOP of primary users and the ergodic rate of secondary users. An important contribution by the authors is the derivation of the SOP of the primary users assuming an infinite number of eavesdroppers and high SNR on the adversarial side.

The authors in [192] considered multiple colluding single-antenna eavesdroppers, where the *maximum SINR receive beamforming* technique is used by the eavesdroppers to aggregate information. The authors formulated the optimization problem to maximize the secrecy rate of the main communication link, considering the total harvested power and the power consumption as constraints of the optimization problem. They found that despite the maximum secrecy rate is constrained by the total harvested power constraint, only a little reduction in the secrecy rate is achieved, especially when the information about the CSI of the eavesdroppers is available.

Multiple Colluding Multi-Antenna Internal Eavesdroppers. Multiple colluding multi-antenna eavesdroppers are considered in [193]— [195], with either imperfect or full CSI knowledge. In this context, while most of the schemes considered a perfect or imperfect knowledge of the CSI at the eavesdroppers, the authors in [194] considered a realistic scenario, where the CSI of the eavesdroppers is not known by the legitimate entities. Assuming multiple, multi-antenna, possibly-colluding eavesdroppers, the authors formulated a power minimization problem, assuming the maximum achievable secrecy rate as a constraint of the problem. They also found the maximum secrecy rate of the system, assuming as constraints of the problem a maximum transmission power and a minimum outage probability.

The authors in [191] investigated the multi-hop multipath wireless network scenario, where all the nodes in the path are energy-harvested devices. They proposed three different protocols for the path selection from a source node to a destination node, to minimize the SOP and maximize the harvested energy, at the same time. Besides considering multiple non-cooperative eavesdroppers, they also include hardware impairments in the model, deriving expressions that closely match real deployments.

Finally, we highlight that all of the above approaches considered neither directional antennas nor included considerations regarding the physical distribution of the eavesdroppers in the scenario. At the same time, in line with the results of our analysis regarding external adversaries, mobile adversaries are not considered.

F. Untrusted Relays

We already introduced in Section V-B and discussed in the two previous subsections the deployment motivations and main working strategies of *trusted* relay nodes. Especially in deep-fading and highly distributed scenarios, dedicated relay nodes provide a crucial service, by forwarding a (possibly amplified) version of the signal from the source toward the destination.

However, relays can be characterized by malicious behaviors. Indeed, they could be either untrusted devices, deployed by network operators other than the ones operating the EH network, or they can be attacked by malicious adversaries. In both scenarios, an attacker controlling the relay owns a crucial network element, potentially disclosing a significant part of the information. Especially when working with physical-layer security measures only (as in the contributions discussed hereby), no further protection measures can ensure

the confidentiality of the information. These are the main reasons motivating many studies in RF EH networks, where untrusted relays are considered. The most common model is a *honest-but-curious* relay, still achieving its relaying tasks in the networks, but trying also to stealthily access the information exchanged between the source and the destination.

A classification of the scientific contributions assuming untrusted relays in RF EH networks is provided in Table VII, considering the features and capabilities of the untrusted relay(s).

Single Untrusted Relays. A single untrusted relay equipped with a single omni-directional antenna is assumed as the adversarial model by the authors in [198]— [203].

To protect the information from eavesdropping on the relay, the authors in [198] described a destination-assisted jamming strategy, where the destination coordinates with the source to transmit a jamming signal in parallel with the reception of the information signal transmitted by the source to the relay. Besides providing benefits in terms of EH (the relay is powered by the jamming signal), the destination-assisted jamming also enhances the security of the information at the relay. Indeed, the signal received at the relay is the combination of the jamming and the information, not revealing the main message to the relay. When the relay forwards the original message to the destination, the final receiving node can subtract the noise and recover the original information. The authors evaluated the SOP and the ESR assuming the usage of both the TS and the PS strategy at the relay, and they concluded that extended benefits in terms of physical-layer data secrecy are provided via the use of the PS strategy. Similar advantages in terms of data secrecy can be provided when the relay is closer to the destination than to the source.

Still assuming a single untrusted relay, the authors in [205] recently studied the effect of an outdated CSI estimation on the achievable outage performance and secrecy rate of a communication link leveraging an untrusted relay. Similarly to previous work, this contribution involves the use of friendly jamming strategies to hide the message from the relay. However, due to the imperfection of the CSI estimate, this contribution also studied the impact of an imperfect jamming cancellation on the secrecy performance of the communication link. Specifically, this work finds the expression and configuration of several parameters, such as the jamming power ratio, power splitting factor and time-splitting ratio that can optimize the secrecy performance metrics, finding sub-optimal but realistic solutions.

Despite the authors in [198] assumed the use of the DF strategy on the relay, all the other works listed in Tab. VII assumed a relay working according to the AF strategy. In general, this latter technique is preferable from the security perspective, as it does not allow the relay to decode the information while in transit toward the destination.

Assuming destination-assisted jamming, the authors in [202] derived the closed-form expression of the secrecy rate and the SOP for a MIMO network, where a base station equipped with multiple antennas transmits confidential information toward multi-antenna receivers. They also showed that increasing the SINR on the destination provides enhancement on the secrecy rate, even if the secrecy rate approaches a constant value by increasing the SINR.

Multiple Non-Colluding Untrusted Relays. Multiple non-colluding untrusted relays equipped with a single receiving antenna are considered only in the work by the authors in [206] and [207]. For instance, the authors in [207] delegated the jamming activities to a dedicated friendly jamming device, emitting noise according to a time profile that is known (and thus, cancellable) at the receiver.

G. Lessons Learned

The discussion and classification reported in the previous subsections highlighted several take-away messages, summarized in the following.

Security and Energy Trade-off. Security and energy are often contrasting objectives. Indeed, when the maximum secrecy rate is required, more energy than the optimal is required from the source, leading to a non-optimal energy efficient configuration. At the same time, minimizing the power consumption on the source or maximizing the harvesting ratio on the receiver always leads to sub-optimal secrecy rate, as well as secrecy outage effects. In this context, several approaches, such as [100], [101], and [102], introduced hybrid security-energy metrics, trading off between security and energy availability. Considering the overall scarce energy availability of RF EH scenarios, configuring the network in a way to achieve such a trade-off is crucial to guarantee, at the same time, network lifetime, usability, and reliability constraints.

Channel State Information (CSI) Awareness. The availability of the CSI on the eavesdropper(s) side is crucial in calibrating the optimality of the solution from the security perspective. When the CSI of the eavesdropper-source link is known, it is possible to maximize the secrecy capacity and to select the beamforming vector and the jamming to minimize the SNR on the adversary. Another common approach is to consider data secrecy or secrecy capacity as a constraint of the optimization problem, assuring that the secrecy rate does not degrade over a minimum threshold or, equivalently, the secrecy outage probability does not exceed a specified upper bound.

Physical-Layer Security and Data Secrecy issues in Non-Orthogonal Multiple Access (NOMA) networks. During the last few years, a significant amount of scientific contributions have focused on physical-layer and data secrecy security issues in EH networks working according to the Non-Orthogonal Multiple Access (NOMA) paradigm. Compared to previous technologies based on orthogonal multiple access, such as OFDMA, NOMA schemes allow overcoming issues related to the limited number of orthogonal resources available in the spectrum and the limited number of users that can be served, tolerating interferences and removing them on the user's side thanks to Successive Interference Cancellation (SIC) techniques [208]. However, the application of such advanced techniques generally introduce an increase in the cost and complexity of the receivers, drastically impacting the energy budget of such devices. Therefore, one of the key challenges that have attracted the interest of Academia is the

TABLE VII
QUALITATIVE COMPARISON AMONG APPROACHES INVESTIGATING PHY-LAYER DATA SECRECY IN EH NETWORKS ASSUMING UNTRUSTED RELAYS.

Adversary	CSI Availability	Adversarial Distribution	Collusion	Adversarial Receiving Antennas	Adversarial Antenna Type	Adversary Mobility	Distance Considera-tions	Scheme	Security Treatment
Untrusted Relay	✓	Single	✗	Single	Omni-Directional	✗	✗	[198], [199], [200]	ESR and SOP Definition
								[201], [202], [203]	SOP and Secrecy Rate
								[204]	SRM
Untrusted Relay	Imperfect	Single	✗	Single	Omni-Directional	✗	✗	[205]	Average Secrecy Rate
Untrusted Relay	✓	Multiple	✗	Single	Omni-Directional	✗	✗	[206]	SOP and Secrecy Rate
								[207]	ESR

trade-off between energy and security, guaranteeing that users can harvest sufficient energy from the received signals, while also guaranteeing minimum thresholds on the security-related metrics, such as the secrecy rate. Other recent works such as [118] have also brought UAVs into the play, improving the SINR on the receivers and managing energy-security trade-offs on the UAVs.

Relationship between SINR and location. The largest part of the papers discussed in the previous subsections did not specifically consider the physical deployment of the adversary, i.e., its position to the main communication link. This is because the distance eavesdropper-target is mimicked by the SINR experienced at the eavesdropper. Without loss of generality, the above contributions assumed a homogeneous scenario, where high values of eavesdropping SINR correspond to locations of the eavesdropper close to the target communication link, while low values of SINR experienced by the eavesdropper are consistent with a positioning far from the main communication link. However, translating SINR values to a real distance from the target has been not investigated in the literature.

H. Future Directions

Despite the large body of scientific contributions available in the literature, EH security issues still include some unexplored research directions, listed below.

Multiple Colluding Directional Antennas. Few recent works investigated the secrecy rate that can be achieved via physical-layer security schemes when the adversaries use a directional antenna (see [141] and [142]). However, to the best of the authors' knowledge, none of these contributions considered the use of multiple directional antennas. Such a scenario could be particularly interesting from the security perspective, especially when the adversary could take advantage of different eavesdropping locations, such as when collusion is considered. In this scenario, the adversary could effectively reject or minimize the impact of the intentional interference caused by other network elements, thus experiencing an SINR very close to the one in the target destination location.

Antenna Identification Mechanisms. All the approaches discussed in this section investigated physical-layer security from the information-theoretic perspective, looking at the security metrics discussed in Section V-A. However, given that these strategies deal with RF signals, further security aspects should be analyzed, such as the possibility to identify single-antenna contributions to the final signal. For instance, in the context of audio signals, the Independent Component Analysis (ICA) method has been already demonstrated to be a successful tool to identify and reconstruct the waveform emitted by a single antenna [209], thanks to the deployment of a network of colluding eavesdropping antennas. To the best of the authors' knowledge, these physical-layer security analyses have not been provided in the literature.

UAVs and Mobile Adversary. Despite some recent work assuming RF EH devices included mobile devices, such as UAVs, the adversary (either single or multiple) is always considered as a static network element, and only a single work (e.g., [146]) assumed location diversity. We notice that a mobile adversary could explore location diversity techniques to boost its SINR, as well as it could get closer to the target (mobile) adversary to improve its data decoding chances. In addition, multiple adversarial UAVs can be even more capable of decoding correctly the information delivered by the source, as they could explore location diversity and correlate different measurements. Without any doubt, further investigations are needed to establish the robustness of current schemes against mobile UAV-equipped adversaries.

Untrusted UAVs Relays. When UAVs are included in the scenario, all the works surveyed in this contribution considered trusted UAV relays, always cooperating with the intended source and destination. However, UAVs can be also hijacked by the adversary. Moreover, they could behave according to the *honest-but-curious* paradigm, i.e., behaving as intended, but trying to access the information delivered from the source. While these scenarios could appear similar to the ones discussed in Section V-F, the inherent mobility features of the UAVs can provide additional advantages to the adversary, as highlighted in the previous point. Hence, there is a need for further research in this challenging scenario, calling for solutions able to mitigate the presence of single/multiple untrusted UAVs relays.

Active Adversaries. The recent contribution by the authors in [144] has been the first to consider an active adversary,

not only interesting in decoding the confidential information but also in the disruption of the main communication link. Indeed, a powerful adversary able to inject noise on the communication channel, eventually using a directional antenna pointed toward the target communication link, could decrease the SINR experienced by the legitimate destination, leading to an increased number of errors and increased guessing chances by the adversary itself.

Determination of Relay Trust. The discussion in Section V-F highlighted some directions to keep the information confidential from untrusted relays, at the cost of a destination-assisted or device-assisted jamming. However, the level of trust of the relays in the network should be established at the deployment or at the boot time, and not at run-time. This is crucial to avoid the unnecessary cost of friendly jamming in terms of network and interference management or to reduce network information exposure to a relay. Thus, dedicated mechanisms and strategies to determine the level of trust of a relay should be implemented. To the best of the authors' knowledge, these considerations have not been addressed in the contributions available in the literature.

Clustering and Energy Availability Issues in EH-NOMA networks. One of the key challenges when designing secure NOMA networks is the clustering logic. In this specific context, *clusters* refer to groups of devices sharing the same frequency-time resource, while the clustering refers to the process of assigning resources to the clusters. We notice that optimizing the clustering of the users might involve undesired effects, such as the unwanted delivery of sufficient energy to eavesdroppers, enabling them to decode information and let the secrecy rate of the main communication links to fall below the desired threshold. Based on the above considerations, this is one of the key challenges to address when designing *optimized* NOMA networks, especially for locations with medium-to-low SNR. The solutions could leverage mobile devices, such as UAVs, equipped with directional antennas, in a way to minimize the leakage of the signal to undesired/insecure locations.

Energy Harvesting - Rate-Splitting Multiple Access (RSMA) schemes. While NOMA schemes rely on the full decoding of the interference, Rate-Splitting Multiple Access (RSMA) schemes take into account the potentially destructive nature of the interference, and therefore, they treat the received signal partially as noise and partially as *intended* constructive interference, decoding it [210]. The usage of RSMA schemes has been recently studied mainly in the context of cellular networks, in broadcast-channel single-cell scenarios [211], [212], and interference-channel multi-cell setup [213].

Similar to the case of NOMA schemes, it is straightforward to apply RF EH principles with networks operating according to RSMA techniques. Indeed, hybrid access points could broadcast dedicated energy signals in the downlink to cellular and D2D users working according to the RF EH principles discussed in Sections II-D and II-E. Hybrid access points can further gather the information transmitted by the users in the uplink, relaying them to the base station. In this context, several optimization problems can be formulated, in a way to reduce the energy consumption, minimize the delay in information reporting, or maximizing the throughput, eventually considering friendly jamming techniques and the imperfections/non-idealities of real EH circuits [214], [215], [216].

RSMA schemes have a high potential to be used for security applications. Indeed, RSMA schemes can split the user's message into a private part, decodable by only a specific user, using a fraction of the overall available power, and a common part, decodable by a given group of users, using the remaining part of the available power [213]. However, at the time of this writing, the literature does not provide any specific study investigating classical security-related metrics in the context of energy harvesting RSMA schemes, such as the secrecy rate, the secrecy outage probability, and the secrecy capacity. Note that this is a particularly challenging area, as the energy consumption of EH users should not exceed the related EH capabilities of the users. We expect this area to be particularly promising in terms of research contributions, in the months to come.

Performance in Real Deployment Scenarios. The recent work by the authors in [174] has been the first to provide an experimental evaluation of the analytical and simulation findings in the RF EH physical-layer security area. Indeed, providing experimental testbeds and open-source code could help the research community to either validate and verify the findings of a specific work, as well as to easily extend that results in different scenarios. Moreover, the translation from the simulation to the experimental validation could help to refine the theoretical models and highlighting technical issues, such as network synchronization and interference cancellation. Furthermore, real experimental evaluations could help to translate from security evaluations based on SINR at the eavesdropper to the definition of *secure deployment areas*, where the minimum required secrecy rate is achieved. At this time, despite the presence of a large number of theoretical results validated by simulations, almost no experimental results or real testbeds (excluding the one mentioned before) are available in the literature.

VI. Additional Physical-Layer Countermeasures

Techniques focusing on physical-layer data secrecy and lightweight cryptography schemes addressed only a limited part of the attacks and threats described in Section III. The current literature includes also additional countermeasures, deployed on purpose to protect EH networks against specific threats. These approaches, falling neither in techniques aimed at protection data secrecy, nor in lightweight cryptography schemes, have been discussed in this section, and cross-compared along different common features.

A security-oriented overview of such scientific contributions is provided in Table VIII.

The following discussion provides more details about the schemes listed in Table VIII, introducing them based on the target security service.

Many scientific contributions in the last years, such as [62]— [67], provided physical-layer solutions to guarantee the availability of an EH network. More in detail, to face malicious jamming sources, the contributions in [62], [63], [64], [67]

TABLE VIII
OVERVIEW OF PHYSICAL-LAYER PROTECTION TECHNIQUES ADOPTED IN EH NETWORKS

Scheme	Enabling Technologies	Scenario	Considered Threat	Defense Tools	Target Security Service	Analysis Tool
[61]	Generic	WSN	Flooding Attacks	Throughput degradation estimation, Intrusion Detection Based, Path Reassignment, Traffic aggregation	Availability	Markov Process
[62], [63]	Generic	Generic EH Wireless Network	Jamming	Channel Hopping (OFDM), Power Spreading	Availability	Game Theory
[64]	Generic	Generic EH Wireless Network	Jamming	Time Splitting EH	Availability	Game Theory
[65]	Cognitive Radio Networks	Generic EH Wireless Network	Jamming	Deception Tactic (fake transmissions)	Availability	Markov Process
[66]	Generic	Wireless Communication Control Systems	Jamming	Optimal non-causal Energy Allocation Policy	Availability	Markov Process
[67]	Interference Alignment Wireless Network	Generic EH Wireless Network	Jamming	Opportunistic Interference Alignment	Availability	MinIL Algorithm
[72]	Generic	IoT, WSN	DoS (network level), Stealthy Collision Attacks	Adaptative Acknowledgement Approach (AAA)	Availability	Markov Process
[70], [71]	Generic	Generic EH Wireless Network	Energy DoS	Power Positive Networking (PPN)	Availability	Resurrection Duckling Based
[22]	WPCN	Generic EH Wireless Network	Jamming, Spoofing, Monitoring, Charging Attacks, Malicious Applications	FDMA, TDMA, frequency hopping, Interference Alignment; Digital Signatures; Data and Energy exchanging estimation	Availability, Confidentiality	Experimental
[68]	ABCN	IoT	Jamming, Deauthentication, Replay, Channel Spoofing	Ambient Backscattering, Multi-path Propagation Signatures	Availability, Authenticity	One-Class SVM
[74]	Generic	Generic EH Wireless Network	Power and Timing Side Channels	Quantization Controllers	Confidentiality	Implementation Optimization
[75], [77]	ABCN	Mobile Devices, WBAN	Side Channels, Authenticity	Shielding, Software Layer Solutions, Backscatter Signal Authentication with Propagation Signatures	Confidentiality, Authenticity	Physical-Layer Analysis
[76]	Generic	Intermittent Computing Systems	Power Interruption Attacks	Secure Checkpoints	Confidentiality, Integrity, Authenticity, Availability	Input/Output

recommended the use of well-known frequency hopping and spreading spectrum techniques. Other contributions, such as [62], [63], [64] convert the jamming signal power into useful transmission power, used to charge the legitimate devices. Following game theory concepts, they modeled the interaction between a pair of legitimate nodes and a jammer as zero-sum-game, and they found optimal solutions (i.e., equilibrium conditions) that minimize the impact of the jammer and maximize the harvesting energy on the legitimate devices.

In the context of Energy Harvested Cognitive Radio Network, the authors in [65] considered the use of a deception tactic to exhaust energy resources of the attackers, i.e., to send fake transmission data to compromise the attackers' capabilities, to deplete their energy. This countermeasure allows the secondary users in a cognitive radio network to deal with jamming attacks, reducing the impact of the attack. The authors in [66] proposed a solution against jamming attacks in closed-loop systems, by working on the solution of the optimization energy allocation problem. An optimal non-causal energy allocation policy allows the system to estimate the state of the control process (leveraging a Kalman Filter) while ensuring availability and stability. Similarly, the authors in [67] considered interference alignment methods (i.e., beamforming strategies) to mitigate adversarial jammers. The anti-jamming solution has the main goal of creating an Interference Alignment network comprising some of the legitimate devices (e.g., the transmitter and the EH nodes), while the remaining nodes are dedicated to EH tasks. Both the interference signal and the

jamming signal are considered as the sources of RF EH on the compatible devices.

A protection scheme to guarantee network availability under flooding attacks in the WSN scenario has been proposed by the authors in [61]. Specifically, they used EH concepts and Markov Process theory to identify ongoing flooding attacks. They modeled the traffic state of the network via a Markov process, and they provide an estimation of the sensor node throughput degradation under flooding attacks, comparing it to a threshold. The higher the degradation, the higher the probability of ongoing flooding attacks.

To face DoS attacks, the authors in [72] conceived a framework to identify stealthy and malicious nodes that transmit packets for intentional packet drop in a EH network. They exploited the Packet Delivery Ratio (PDR) feature and an Adaptive Acknowledgment Approach (AAA) to identify these stealthy collision attacks. In the AAA strategy, each node sends a data packet, monitors the next transmission of its first hop downstream node and waits for the acknowledgment from the second hop downstream node. If the acknowledgment is not received in the timing window, there is a high probability of an attack.

The authors in [70] and [71] provided methods to mitigate DoS attacks, by offloading the power requirements of the EH node to the device that is sending networking requests. Specifically, they designed an alternative channel, namely Power-Positive-Networking (PPN), where each received signal allows to recharge the battery of the device. Being very similar to the underlying concept of SWIPT networks (see Section II-E), these alternative channels stop energy DoS attacks, given that any jamming signal aimed at interrupting wireless charging results in a re-charge of the EH device.

The authors in [22] highlighted qualitatively some possible countermeasures that could be used in WPCN against various types of attacks. To face jamming attacks, the authors proposed to leverage traditional modulation schemes, such as Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), and frequency hopping, or to use interference alignment principles (beamforming). To thwart spoofing attacks, they indicated the possible use of digital signatures, to provide authenticity and integrity of the messages. To detect monitoring attacks, they proposed to listen to the communication channel and discover the presence of data exchanged between the energy harvester nodes and possible malicious nodes. Concerning charging attacks, the authors proposed to perform frequent estimations of the energy that nodes are harvesting in the network, and to detect anomalies in the charging profile. Finally, to defeat malicious applications, the authors proposed to verify the application signatures and to check if they are trusted/valid. Alternatively, they indicated the possibility to design energy-aware mechanisms, such that every application could leverage an energy budget to be used for computations and transmissions. Finally, to address the privacy issues discussed in Section III, they proposed to collect the RF fingerprints from the environment, and to compare them with the ones acquired at run-time.

In the context of the IoT networks powered via ambient backscatter, the authors in [68] identified the possibility to enforce the authenticity of the communication via multi-path propagation signatures, thus securing pairing and data communication processes. They found that the interaction of the RF source with the environment and the location of the specific device is unique. Thus, it can be used to provide a probabilistic and ambient-dependent authentication, as well as a tool to identify replay and de-authentication deadlock attacks.

Other approaches investigated solutions to avoid side-channel attacks. For instance, the authors in [74] investigated the hardware design of a system adopting quantization controllers, using the harvested energy to carry out a secure computation in an isolated environment.

In the ABCN scenario, the authors in [75] proposed two strategies, i.e.: (i) to block the incident/reflected signal; and (ii) to adopt software solutions (e.g. set permissions on a device file, stop the network manager, hiding the WiFi interface). The usage of propagation signatures to identify the attacker has been also proposed and discussed by the authors in [77]. Finally, to face *power interruption attacks* at the physical layer, the authors in [76] proposed a secure protocol for devices with intermittent connectivity, characterized by several security features. The protocol uses random nonces to protect against checkpoint replays attacks, leverages a pre-shared key to avoid sensitive data leakage, exploits hash chains to ensure data integrity, preserves the correct order of the operations by ensuring the consecution between the checkpoints, and, finally, improves the resilience of the device towards power loss issues by storing redundant copies of the system state.

A. Lessons Learned

The non-cryptographic protection strategies and tools discussed in the previous section highlighted several take-home messages and guidelines to be considered when deploying EH technologies. The key considerations are summarized below.

Protecting the Availability of EH Networks. Most of the solutions previously discussed focused on improving the resilience of the network against attacks targeting its availability. Indeed, differently from traditional IoT networks, energy provisioning in EH networks is often intermittent, and thus denying its availability could be the easiest way to disrupt network operation. While traditional means such as solar, wind, and mechanical sources are easiest to be disrupted, stopping RF harvesting is not easy. Hence, jamming the source only increases the amount of RF energy available, resulting in an increased amount of power available at the devices. This is the reason motivating the even more diffused consideration of the RF source as a secure harvesting method.

Side-Channel Attacks in EH Networks. Traditional EH sources, as well as RF harvesting solutions, have not been designed with physical security in mind. Therefore, well-known side-channel attacks are even more powerful and easy-to-perform than in traditional wireless networks. Due to the hard integration of classical hardware approaches, countermeasures available in the literature use physical-layer techniques (such as the identification of propagation signatures), whose security is probabilistic and not fully tested.

B. Future Directions

Few future research directions concerning lightweight non-cryptographic countermeasures for EH networks can be identified.

Experimental energy expenditure evaluations. Despite being effective, none of the above-described protection technologies provided an evaluation of the related energy consumption. This is a crucial aspect, because of the energy-security trade-off vastly described in this paper. Currently, it is still not clear if traffic analysis and physical-layer security techniques are effectively less energy-consuming than traditional cryptography approaches, especially considering the optimizations of cryptography techniques described in Section IV.

Detecting Physical Presence in EH Networks. As described in the previous subsection, a side-channel attack is still one of the most challenging threats in EH networks. It is worth noticing that side-channel attacks require physical adversaries, able to approach the target devices and deploy dedicated tools. Hence, to prevent such an attack, a solution to detect the presence of a physical intruder could be coupled with the deployment of EH networks, providing viable protection schemes. For instance, considering the sensitivity of RF EH technologies to modifications of the surrounding environment, physical adversaries can be identified, triggering appropriate response strategies. At the same time, further research directions could evaluate the feasibility of running such systems on the EH device or dedicated battery-supplied nodes.

VII. Emerging Research Challenges

The previous sections highlighted the most prominent research areas involving EH devices and networks, as well as some future directions that can be pursued in the related macro-areas. Besides these promising study areas, there are a few other security application domains involving EH principles and devices that, over the last years, have received little (if any) attention from the scientific community. Some of them are described below, along with key challenges to be solved to finally unlock their potentials.

Intelligent Surfaces. Intelligent surfaces have recently gained momentum, as one of the most appealing new attractive technologies in the wireless communications research domain [217]. In the literature we often found an interchangeable use of the terms Large Intelligent Surfaces (LIS) and Intelligent Reconfigurable Surfaces (IRS). Overall, LIS mainly refer to Active LIS-based Massive MIMO, as discussed in [218]. They are used for data transmission (while IRS are used for reflection), and they consist of massive antenna arrays, organized on surfaces, and characterized by a fixed transmit power per volume-unit constraint. At this time, they are mainly considered for indoor applications, where they are shown to be particularly successful for interference cancellation [219].
Without loss of generality, an IRS can be defined as a bidimensional planar surface, consisting of a large number of cheap and passive electromagnetic elements, structured in arrays. The phase shift of the reflecting elements in the array can be controlled independently via software, without requiring a dedicated energy source, in a way to reflect the incident signal with specific desired properties, such as attenuation and scattering [220]. Therefore, any software-controlled change in the coefficients of the IRS contributes to shape the incident signal with specific amplitude and phase, modifying the wireless propagation environment and boosting the reception of the signal towards specific locations [221]. Compared to existing solutions, such as ABCNs, Amplify-and-Forward schemes, and LISs, IRSs offer real-time flexibility and tuning of the coefficients, without requiring any additional energy budget or additional information to be delivered on the wireless channel [222].
From the security perspective, intelligent surfaces have already started to attract the interest of many researchers, especially the ones working on physical-layer security and data secrecy schemes, as thoroughly discussed in Section V. While LIS have been mainly investigated from the performance perspective, many very recent contributions have focused on the security properties offered by IRS. Indeed, using IRSs it is possible to precisely control the phase, the amplitude, the frequency, and the polarization of the signals, including neither complex encoding/decoding schemes, nor energy-consuming processing operations. The usage of IRSs is particularly appealing when the potential eavesdroppers are closer to the source than the destination, or when the adversaries lie in the same direction of the intended destination of the message [220]. In addition, the number of reflecting elements, as well as the specific phase shift adopted by the reflecting elements, and the IRS's reflect beamforming, can be all combined and optimized to restrict the received beams to specific locations, to cancel beams at the location of the eavesdroppers, to reduce the energy consumption on the transmitter, or to maximize the SINR at the intended receivers [223].
Therefore, research groups working on physical-layer security have already started to consider schemes that can optimize one or more metric, by taking into account the remaining system or security-related metrics as constraints of the optimization problems. In this direction, we can notice that the literature already includes some works that apply the findings and results discussed in Section V to the new scenario, considering the configuration of the coefficient of the IRS as new parameters of the optimization problems.
For instance, the authors in [224], [225], [226], [227] have already provided preliminary studies considering single external eavesdroppers, equipped with single receiving antennas. Internal adversaries, in the context of Cognitive Radio Networks (CRN), have been already considered by the authors in [222]. Single eavesdroppers equipped with multiple antennas have been considered in [228], while other very recent contributions considered non-colluding multiple eavesdroppers, equipped with either single [229] or multiple antennas [230], [231]. Other recent works, such as [232] are also evaluating the benefits of Artificial Intelligence (AI) techniques to boost the secrecy rate towards multiple eavesdroppers. Similarly to the studies discussed in Section V, we also notice different formulations of the problem, based on the availability (or not) of the CSI [233]. In line with the previous discussion,

the objectives pursued by the proposed optimization problems are very similar to the ones discussed in Section V, such as the Secrecy Rate Maximization [234] and the definition of the secrecy capacity and outage probability [224], while other works consider the secrecy rate as a constraint of the optimization problem [235]. Recent works are also considering the joint effect of friendly jamming, as a way to further improve the secrecy of the main communication links against external adversaries [236], [237].

Overall, following the current trend, we expect that a significant number of scientific contributions will appear in the upcoming months in the IRS area. Indeed, all the studies and findings consolidated in the last years in the context of data secrecy in EH networks can be revisited in the emerging IRS context, taking into account also the new degree of freedom offered by the coefficients of the IRS and their energy efficiency, paving the way for new appealing research challenges. For instance, to the best of our knowledge, none of the contributions in the current literature considered the chances of multiple colluding eavesdroppers to reduce the secrecy rate of networks using IRS, as well as none of them included considerations on the particular directivity of the antennas used by the legitimate devices and the eavesdroppers. In addition, new security challenges emerge: an attacker can take the control of the IRS, and modify at will the pattern of the incident signals (e.g., directing the beam towards unintended locations, at the advantage of the attacker); moreover, an attacker can also locate the IRS and get physically closer, improving its SINR. We expect also that the introduction of IRS will move data secrecy and physical-layer security issues to new application domains, such as vehicular networks, Flying-Ad-hoc Networks (FANET), and Ultra-Dense Networks (UDN).

Physical-Layer Authentication using EH Signals. Some recent contributions, such as [238], [77], and [239], investigated physical-layer authentication schemes leveraging EH properties and devices. However, the authors in [238] and [77] used physical-layer features, i.e., the frequency offset and the on-body backscattering reflections related to wave propagations, respectively, and contextualized their usage when EH devices are involved, thus not fully exploring EH features. Instead, the authors in [239] were the first and only to use properties specific to EH phenomena, i.e., the profile of the energy harvested by a human during his regular gait. Using the EH profile over time derived by EH processes, they created a gait-based authentication protocol that does not require the continuous sample of the accelerometer, drastically reducing the overall energy consumption (up to 84%). In this context, the authors reported slightly lower performance than typical gait-based authentication schemes (89% in harsh conditions) and significant success performance in spoofing attacks (up to 14.1 $\%$). Thus, further enhancements are possible, e.g., by coupling the gait with the movements of other parts of the human body (e.g., hands and wrists). Besides, the methodology could be even re-used in other contexts, such as the authentication of embedded devices in industrial plants, that can be characterized by distinctive features.

Overall, we can notice that despite physical-layer authentication schemes have been investigated in the context of RFID (see, for instance, [240]) and traditional backscattering systems (e.g., the works in [241] and [242]), the usage of EH properties for devices' authentication still lacks complete studies. For instance, studies about the unique charging profile of EH devices or the presence of any imperfection in the EH transfer are still not available in the literature, and can pave the way to a completely new wave of physical-layer authentication protocols, possibly overcoming the limitations of current schemes.

Integrated Space and Terrestrial Networks (ISTN). In their intended design, 5G wireless systems are mainly terrestrial networks, and therefore their coverage area is limited. 6G systems are expected to bring Low-Earth-Orbit (LEO) satellites into the system architecture, to provide worldwide broadband connectivity, including users in open sea and remote areas [243], [244]. Despite LEO satellites are the most feasible to accomplish this task, due to the reduced distance from the Earth and the consequently reduced latency, the prevalence of the Line of Sight (LOS) component creates co-channel interference effects, and in turn, signal degradation effects. From the security perspective, LEO satellites are far from the ground, and very difficult to be hijacked physically. However, due to their distance, they can hardly be modified ex-post in their hardware features, or augmented with new enabling technologies. Therefore, their security properties should be carefully verified and tested before deployment. In this context, harvesting technologies can play a dual role. On the one hand, solar cells integrated into satellites can boost the energy available on the satellites, and increase the power available for transmission and relay operations. On the other hand, physical-layer information-theoretic security techniques can be combined with dedicated harvesting technologies leveraging Free Space Optical (FSO) communication links to further enhance the security of the communication links and, at the same time, increase the energy available at the receivers [245].

Physical Unclonable Functions using EH Principles. In line with previous considerations on authentication using EH principles, recently the authors in [246] described how to use the dispersion of the power generation time of the solar cells to identify the specific semiconductor, and thus the device using the generated power. The usage of similar principles in other harvesting technologies, such as RF, still has not been investigated in the literature, and can provide anti-counterfeiting strategies, hardware random number generation tools, and auxiliary authentication solutions for EH devices.

Key Agreement Schemes using EH Properties. Despite a large number of scientific contributions investigated innovative and lightweight key agreement schemes using physical-layer security mechanisms (see [247] for an overview), key establishment mechanisms in EH networks have received only minimal attention. A pioneering contribution in the context of ABCN is the one described in [248], where the authors got rid of the secret reconciliation procedure typical of physical-layer key agreement schemes, improving the efficiency of such schemes. However, the usage of physical-layer features specific to energy harvesting, such as the ratio of harvested energy over time and its relationship with unique devices'

features for key agreement, still has not received enough attention by the scientific community.

Privacy Considerations. EH devices, especially IoT devices using EH capabilities, could be subject to potential privacy breaches, derived by the analysis of the energy consumption and re-charging patterns, as well as their positioning toward the source. Few recent scientific contributions, such as the ones by the authors in [249] and [250], highlighted these privacy issues in electricity and healthcare scenarios, respectively. At the same time, the authors in [251] identified the potential of RF harvesting properties for enhancing the privacy level of smart meters, as they can differentiate energy sources and decorrelate the final consumed energy from the profile of the energy expected from the legitimate source, thus defending against side-channel attacks. The challenge here is to come up with privacy-preserving frameworks, that can mask the re-charging profiles and the energy expenditure behavior, while minimally affecting the system availability (i.e., being characterized by reduced energy consumption).

Secure Protocol Stack for EH Devices. The unique systemic features of EH devices and networks, highlighted in the previous sections, require the design of dedicated solutions at all the layers of the protocol stack. Besides the significant work on physical layer security described in previous sections, several contributions investigating MAC protocols tailored for EH devices have been classified and described by the authors in [43]. At the same time, few contributions such as [252] and [253] investigated secure routing protocols for EH networks, mainly concentrating on reducing the energy footprint of such schemes. Especially when the EH network is targeted by attacks disrupting its availability, dedicated routing protocols are required, that can rebalance the network traffic towards nodes with high energy-budget, thus improving its overall throughput.

Using Energy Harvesting for Security-Related Applications. Finally, only a few contributions are describing commercial products using EH principles to enhance the physical security of devices and people. For instance, the authors in [254] recently presented the implementation of a physical access control system based on energy harvesting, regulating the access of people to rooms in a building. However, several additional applications are possible, not only limited to the smart home application scenario, but also extending to industrial control systems, entertainment, and intelligent transportation (e.g. autonomous vehicles, UAVs), to name a few.

VIII. Conclusion

In this paper, we survey the prominent security issues, mechanisms, techniques, and applications related to Energy Harvesting for wireless networks. In particular, we first provide background information on models and technologies necessary to delve into the EH field. Later, we address the security domain. In detail, after a discussion of the possible attacks, we have partaken the security domain for EH wireless networks into three main macro-areas, i.e.: data secrecy at the physical layer; lightweight cryptography techniques; and, additional physical-layer countermeasures. Within these areas, we classified the available scientific contributions along some common features, such as the assumed adversarial model and the target security service, we discussed common approaches and distinguishing strategies, and we identified future promising research directions. Furthermore, we have highlighted appealing research problems related to EH networks, such as Intelligent Reconfigurable Surfaces (IRS) and physical-layer security issues in Rate-Splitting Multiple Access schemes. We believe that the exposed challenges show that the development of security techniques for EH networks is still an exciting research area, and that it can be inspiring for researchers, industry, and start-ups, striving for innovative, non-invasive, and computationally lightweight means to enforce systems security in constrained energy-limited environments.

Acknowledgements

The authors would like to thank the anonymous reviewers for their comments and suggestions, that helped improving the quality of the manuscript.
This publication was partially supported by awards NPRP11S-0109-180242 and NPRP X-063-1- 014 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF.

References

[1] M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.
[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
[3] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in Wireless Energy Harvesting Communications Systems: A Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1329–1360, Secondquarter 2018.
[4] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, "Energy Harvesting Wireless Communications: A Review of Recent Advances," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 3, pp. 360–381, March 2015.
[5] Y. He, X. Cheng, W. Peng, and G. L. Stuber, "A survey of energy harvesting communications: models and offline optimal policies," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 79–85, June 2015.
[6] W. Guo, S. Zhou, Y. Chen, S. Wang, X. Chu, and Z. Niu, "Simultaneous Information and Energy Flow for IoT Relay Systems with Crowd Harvesting," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 143–149, November 2016.
[7] Cordis Europa, https://cordis.europa.eu/project/rcn/218156/factsheet/it, 2019, accessed: 2020-08-14.
[8] Cordis Europa, https://cordis.europa.eu/project/rcn/221100/factsheet/en, 2019, accessed: 2020-08-14.
[9] Fraunhofer Institute, https://www.iis.fraunhofer.de/en/ff/lv/iot-system/anwproj/enables.html, 2019, accessed: 2020-08-14.
[10] Plug-N-Harvest Project Official Website, https://www.plug-n-harvest.eu/, 2019, accessed: 2020-08-14.
[11] Cordis Europa, https://trimis.ec.europa.eu/project/vibration-energy-harvesters-power-iot-revolution, 2019, accessed: 2020-08-14.
[12] US National Science Foundation, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1704176&HistoricalAwards=false, 2020, accessed: 2020-08-14.
[13] US National Science Foundation, https://www.nsf.gov/awardsearch/showAward?AWD_ID=1320543&HistoricalAwards=false, 2020, accessed: 2020-08-14.

[14] US National Science Foundation, https://www.nsf.gov/awardsearch/showAward?AWD_ID=0845874&HistoricalAwards=false, 2020, accessed: 2020-08-14.

[15] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dobre, "Energy-Constrained UAV-Assisted Secure Communications with Position Optimization and Cooperative Jamming," *IEEE Transactions on Communications*, pp. 1–1, 2020.

[16] H. Yang, Y. Ye, X. Chu, and M. Dong, "Resource and Power Allocation in SWIPT Enabled Device-to-Device Communications Based on a Non-Linear Energy Harvesting Model," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[17] Y. Ye, L. Shi, X. Chu, and G. Lu, "On the Outage Performance of Ambient Backscatter Communications," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[18] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Towards 6G Networks: Use Cases and Technologies," *CoRR*, vol. abs/1903.12216, 2019.

[19] W. Saad, M. Bennis, and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *CoRR*, vol. abs/1902.10265, 2019.

[20] T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," *IEEE Access*, vol. 7, pp. 78 729–78 757, 2019.

[21] T. D. Ponnimbaduge Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 264–302, Firstquarter 2018.

[22] Q. Liu, K. S. Yildirim, P. Pawełczak, and M. Warnier, "Safe and secure wireless power transfer networks: challenges and opportunities in RF-based systems," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 74–79, Sep. 2016.

[23] V. N. Vo, T. G. Nguyen, C. So-In, and D. Ha, "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer," *IEEE Access*, vol. 5, pp. 25 196–25 206, 2017.

[24] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2019.

[25] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2019.

[26] A. Di Mauro, D. Papini, and N. Dragoni, "Security Challenges for Energy-harvesting Wireless Sensor Networks," in *PECCS*, 2012, pp. 422–425.

[27] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, H. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 114–121, Aug. 2015.

[28] X. Chen, D. W. K. Ng, and H. Chen, "Secrecy wireless information and power transfer: challenges and opportunities," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 54–61, Apr. 2016.

[29] N. Zhao, S. Zhang, F. R. Yu, Y. Chen, A. Nallanathan, and V. C. M. Leung, "Exploiting Interference for Energy Harvesting: A Survey, Research Issues, and Challenges," *IEEE Access*, vol. 5, pp. 10 403–10 421, 2017.

[30] H. Chen, C. Zhai, Y. Li, and B. Vucetic, "Cooperative Strategies for Wireless-Powered Communications: An Overview," *IEEE Wireless Communications*, vol. 25, no. 4, pp. 112–119, Aug. 2018.

[31] L. Wang, K. Wong, S. Jin, G. Zheng, and R. W. Heath, "A New Look at Physical Layer Security, Caching, and Wireless Energy Harvesting for Heterogeneous Ultra-Dense Networks," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 49–55, Jun. 2018.

[32] Y. Alsaba, S. K. A. Rahim, and C. Y. Leow, "Beamforming in Wireless Energy Harvesting Communications Systems: A Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1329–1360, Secondquarter 2018.

[33] P. Jindal and R. Kumar, "Physical Layer Security with Energy Harvesting Techniques: A Study," in *Information and Communication Technology for Competitive Strategies*. Springer, 2019, pp. 223–233.

[34] M. A. Hossain, R. Md Noor, K. A. Yau, I. Ahmedy, and S. S. Anjum, "A survey on simultaneous wireless information and power transfer with cooperative relay and future challenges," *IEEE Access*, vol. 7, pp. 19 166–19 198, 2019.

[35] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2734–2771, Thirdquarter 2019.

[36] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[37] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient Backscatter: Wireless Communication out of Thin Air," *SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 39–50, Aug. 2013.

[38] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, Feb 2006.

[39] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," *Wireless personal communications*, vol. 71, no. 3, pp. 2259–2294, 2013.

[40] O. Brand, G. K. Fedder, C. Hierold, J. G. Korvink, and O. Tabata, *Micro Energy Harvesting*. John Wiley & Sons, 2015.

[41] C. Moser, J.-J. Chen, and L. Thiele, "An Energy Management Framework for Energy Harvesting Embedded Systems," *J. Emerg. Technol. Comput. Syst.*, vol. 6, no. 2, pp. 7:1–7:21, Jun. 2008.

[42] S.Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *IEEE SoutheastCon 2008*, Apr. 2008, pp. 442–447.

[43] H. H. R. Sherazi, L. A. Grieco, and G. Boggia, "A comprehensive review on energy harvesting MAC protocols in WSNs: Challenges and tradeoffs," *Ad Hoc Networks*, vol. 71, pp. 117 – 134, 2018.

[44] M. Prauzek, J. Konecny, M. Borova, K. Janosova, J. Hlavica, and P. Musilek, "Energy Harvesting Sources, Storage Devices and System Topologies for Environmental Wireless Sensor Networks: A Review," *Sensors*, vol. 18, no. 8, p. 2446, 2018.

[45] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," *IEEE Communications Surveys Tutorials*, vol. 13, no. 3, pp. 443–461, Third 2011.

[46] M. Habibzadeh, M. Hassanalieragh, A. Ishikawa, T. Soyata, and G. Sharma, "Hybrid Solar-Wind Energy Harvesting for Embedded Applications: Supercapacitor-Based System Architectures and Design Tradeoffs," *IEEE Circuits and Systems Magazine*, vol. 17, no. 4, pp. 29–63, Fourthquarter 2017.

[47] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient RF Energy-Harvesting Technologies for Self-Sustainable Standalone Wireless Sensor Platforms," *Proceedings of the IEEE*, vol. 102, no. 11, pp. 1649–1666, Nov 2014.

[48] V. Raghunathan, A. Kansal, J. Hsu, J. Friedman, and M. Srivastava, "Design Considerations for Solar Energy Harvesting Wireless Embedded Systems," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, ser. IPSN '05. Piscataway, NJ, USA: IEEE Press, 2005. [Online]. Available: http://dl.acm.org/citation.cfm?id=1147685.1147764

[49] U. Alvarado, A. Juanicorena, I. Adin, B. Sedano, I. Gutiérrez, and J. de No, "Energy harvesting technologies for low-power electronics," *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 8, pp. 728–741, 2012.

[50] Pozo, Garate, Araujo, and Ferreiro, "Energy Harvesting Technologies and Equivalent Electronic Structural Models - Review," *Electronics*, vol. 8, no. 5, p. 486, Apr. 2019.

[51] N. G. Elvin and A. A. Elvin, "Vibrational Energy Harvesting From Human Gait," *IEEE/ASME Transactions on Mechatronics*, vol. 18, no. 2, pp. 637–644, Apr. 2013.

[52] J. Buckle, A. Knox, J. Siviter, and A. Montecucco, "Autonomous Underwater Vehicle Thermoelectric Power Generation," *Journal of electronic materials*, vol. 42, no. 7, pp. 2214–2220, 2013.

[53] M. Alhawari, B. Mohammad, H. Saleh, and M. Ismail, "A survey of thermal energy harvesting techniques and interface circuitry," in *2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS)*, Dec 2013, pp. 381–384.

[54] S. Bi, Y. Zeng, and R. Zhang, "Wireless Powered Communication Networks: An Overview," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 10–18, 2016.

[55] N. Van Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient Backscatter Communications: A Contemporary Survey," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2889–2922, Fourthquarter 2018.

[56] S. Bi, C. K. Ho, and R. Zhang, "Wireless powered communication: opportunities and challenges," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 117–125, April 2015.

[57] J. P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 6, pp. 1211–1226, Aug 2002.

[58] L.-G. Tran, H.-K. Cha, and W.-T. Park, "RF power harvesting: a review on designing methodologies and applications," *Micro and Nano Systems Letters*, vol. 5, no. 1, p. 14, Feb 2017.

[59] A. Corona, S. Zoppi, W. Kellerer, J. Klaue, T. Becker, and D. Schupke, "A TDMA Energy Consumption Model for WSN Radio Selection in On-Board Aerospace Systems," in *IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, 2018, pp. 71–76.

[60] J. M. Jornet, "A joint energy harvesting and consumption model for self-powered nano-devices in nanonetworks," in *IEEE International Conference on Communications (ICC)*, 2012, pp. 6151–6156.

[61] V. Shakhov, S. Nam, and H. Choo, "Flooding Attack in Energy Harvesting Wireless Sensor Networks," in *Proc. of Int. Conf. on Ubiquitous Information Management and Communication*. New York, NY, USA: ACM, 2013, pp. 49:1–49:5.

[62] E. V. Belmega and A. Chorti, "Protecting Secret Key Generation Systems Against Jamming: Energy Harvesting and Channel Hopping Approaches," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2611–2626, Nov 2017.

[63] E. V. Belmega and A. Chorti, "Energy harvesting in secret key generation systems under jamming attacks," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[64] G. Rezgui, E. V. Belmega, and A. Chorti, "Mitigating Jamming Attacks Using Energy Harvesting," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 297–300, Feb 2019.

[65] D. T. Hoang, D. Niyato, P. Wang, and D. I. Kim, "Performance Analysis of Wireless Energy Harvesting Cognitive Radio Networks Under Smart Jamming Attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 1, no. 2, pp. 200–216, 2015.

[66] S. Knorn and A. Teixeira, "Effects of Jamming Attacks on a Control System With Energy Harvesting," *IEEE Control Systems Letters*, vol. 3, no. 4, pp. 829–834, Oct 2019.

[67] J. Guo, N. Zhao, F. R. Yu, X. Liu, and V. C. M. Leung, "Exploiting Adversarial Jamming Signals for Energy Harvesting in Interference Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1267–1280, Feb 2017.

[68] Z. Luo, W. Wang, J. Qu, T. Jiang, and Q. Zhang, "ShieldScatter: Improving IoT Security with Backscatter Assistance," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '18, 2018, pp. 185–198.

[69] D. Niyato, P. Wang, D. I. Kim, Z. Han, and L. Xiao, "Game Theoretic Modeling of Jamming Attack in Wireless Powered Communication Networks," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 6018–6023.

[70] S.-Y. Chang, S. L. S. Kumar, B. A. N. Tran, S. Viswanathan, Y. Park, and Y.-C. Hu, "Power-positive Networking Using Wireless Charging: Protecting Energy Against Battery Exhaustion Attacks," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '17, 2017, pp. 52–57.

[71] S.-Y. Chang, S. L. S. Kumar, Y.-C. Hu, and Y. Park, "Power-Positive Networking: Wireless-Charging-Based Networking to Protect Energy Against Battery DoS Attacks," *ACM Transactions on Sensor Networks*, vol. 15, no. 3, May 2019.

[72] C. Pu, S. Lim, B. Jung, and M. Min, "Mitigating stealthy collision attack in energy harvesting motivated networks," in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, Oct 2017, pp. 539–544.

[73] Y. Nozaki and M. Yoshikawa, "Tamper Resistance Evaluation Method for Energy Harvester," in *3rd International Conference on Computational Intelligence and Applications (ICCIA)*, July 2018, pp. 200–204.

[74] M. Moukarzel and M. Hicks, "Reap What You Store: Side-channel Resilient Computing Through Energy Harvesting," in *Proceedings of the Fifth ACM International Workshop on Energy Harvesting and Energy-Neutral Sensing Systems*, ser. ENSsys'17, 2017, pp. 21–26.

[75] Z. Yang, Q. Huang, and Q. Zhang, "NICScatter: Backscatter As a Covert Channel in Mobile Devices," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '17, 2017, pp. 356–367.

[76] A. S. Krishnan, C. Suslowicz, D. Dinu, and P. Schaumont, "Secure Intermittent Computing Protocol: Protecting State Across Power Loss," in *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2019, pp. 734–739.

[77] Z. Luo, W. Wang, J. Xiao, Q. Huang, T. jiang, and Q. Zhang, "Authenticating On-Body Backscatter by Exploiting Propagation Signatures," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 123:1–123:22, Sep. 2018.

[78] A. V. Taddeo, M. Mura, and A. Ferrante, "QoS and security in energy-harvesting wireless sensor networks," in *International Conference on Security and Cryptography (SECRYPT)*, Jul. 2010, pp. 1–10.

[79] B. Mao, Y. Kawamoto, J. Liu, and N. Kato, "Harvesting and threat aware security configuration strategy for ieee 802.15.4 based iot networks," *IEEE Communications Letters*, vol. 23, no. 11, pp. 2130–2134, Nov 2019.

[80] C. Copello and N. Weng, "Adaptive scheduling to enhance data security and energy efficiency on energy harvesting platform," *Microprocessors and Microsystems*, vol. 60, pp. 24 – 37, 2018.

[81] X. Fang, M. Yang, and W. Wu, "Security Cost Aware Data Communication in Low-Power IoT Sensors with Energy Harvesting," *Sensors*, vol. 18, no. 12, p. 4400, Dec 2018.

[82] P. Schaumont, B. Yuce, K. Pabbuleti, and D. Mane, "Secure authentication with energy-harvesting: A multi-dimensional balancing act," *Sustainable Computing: Informatics and Systems*, vol. 12, pp. 83 – 95, 2016.

[83] S. Pelissier, T. V. Prabhakar, H. S. Jamadagni, R. VenkateshaPrasad, and I. Niemegeers, "Providing security in energy harvesting sensor networks," in *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, Jan 2011, pp. 452–456.

[84] G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, "AGREE: exploiting energy harvesting to support data-centric access control in WSNs," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2625 – 2636, 2013.

[85] C. Suslowicz, A. S. Krishnan, and P. Schaumont, "Optimizing Cryptography in Energy Harvesting Applications," in *Proceedings of the 2017 Workshop on Attacks and Solutions in Hardware Security*, ser. ASHES '17, 2017, pp. 17–26.

[86] B. Lv, Z. Peng, and S. Tang, "Precomputation Methods for UOV Signature on Energy-Harvesting Sensors," *IEEE Access*, vol. 6, pp. 56 924–56 933, 2018.

[87] G. Ateniese, G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, "Low-Cost Standard Signatures for Energy-Harvesting Wireless Sensor Networks," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 3, pp. 64:1–64:23, Apr. 2017.

[88] G. Ateniese, G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, "HELIOS: Outsourcing of Security Operations in Green Wireless Sensor Networks," in *IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017, pp. 1–7.

[89] N. Ellouze, S. Rekhis, and N. Boudriga, "Energy Harvesting Based Protection of Border Surveillance Systems," in *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, ser. SAC '15, 2015, pp. 621–626.

[90] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga, "Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting," in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, ser. TrustED '13, 2013, pp. 35–42.

[91] L. Varga, G. Romaniello, M. Vucinic, M. Favre, A. Banciu, R. Guizzetti, C. Planat, P. Urard, M. Heusse, F. Rousseau, O. Alphand, E. Duble, and A. Duda, "GreenNet: An Energy-Harvesting IP-Enabled Wireless Sensor Network," *IEEE Internet of Things Journal*, vol. 2, no. 5, pp. 412–426, Oct 2015.

[92] A. D. Mauro and N. Dragoni, "Adaptive Multipath Key Reinforcement for Energy Harvesting Wireless Sensor Networks," *Procedia Computer Science*, vol. 63, pp. 48 – 55, 2015.

[93] E. Valea, M. Da Silva, M. Flottes, G. Di Natale, S. Dupuis, and B. Rouzeyre, "Providing Confidentiality and Integrity in Ultra Low Power IoT Devices," in *International Conference on Design Technology of Integrated Systems In Nanoscale Era (DTIS)*, Apr. 2019, pp. 1–6.

[94] A. Hylamia, M. Spanghero, A. Varshney, T. Voigt, and P. Papadimitratos, "Security on Harvested Power," in *Proc. of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '18, 2018, pp. 296–298.

[95] B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," *IEEE Access*, vol. 6, pp. 35 966–35 978, 2018.

[96] L. Vracar, M. D. Stojanovic, A. S. Stanimirovic, and Z. D. Prijic, "Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems," *Journal of Sensors*, Apr. 2019.

[97] A. Cammarano, C. Petrioli, and D. Spenza, "Pro-Energy: A novel energy prediction model for solar and wind energy-harvesting wireless

sensor networks," in *IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012)*, Oct 2012, pp. 75–83.

[98] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1878–1911, Secondquarter 2019.

[99] G. Aliberti, R. D. Pietro, and S. Guarino, "Reliable and perfectly secret communication over the generalized Ozarow-Wyner's wire-tap channel," *Computer Networks*, vol. 109, pp. 21 – 30, 2016, special issue on Recent Advances in Physical-Layer Security.

[100] H. Yu, S. Guo, Y. Yang, L. Ji, and Y. Yang, "Secrecy Energy Efficiency Optimization for Downlink Two-User OFDMA Networks With SWIPT," *IEEE Systems Journal*, vol. 13, no. 1, pp. 324–335, March 2019.

[101] D. Zhao, H. Tian, and P. Zhang, "A Secure Wireless Information and Energy Cooperation Transmission Strategy in Spectrum Sharing Networks With Untrusted Dual-Relay," *IEEE Access*, vol. 7, pp. 115 487–115 504, 2019.

[102] G. Wang, C. Meng, W. Heng, and X. Chen, "Secrecy Energy Efficiency Optimization in AN-Aided Distributed Antenna Systems With Energy Harvesting," *IEEE Access*, vol. 6, pp. 32 830–32 838, 2018.

[103] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[104] G. Pan, J. Ye, and Z. Ding, "Secure Hybrid VLC-RF Systems With Light Energy Harvesting," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4348–4359, Oct 2017.

[105] D. Wang and S. Men, "Secure Energy Efficiency for NOMA Based Cognitive Radio Networks With Nonlinear Energy Harvesting," *IEEE Access*, vol. 6, pp. 62 707–62 716, 2018.

[106] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-Powered Full-Duplex Relay and Friendly Jamming for Secure Cooperative Communications," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

[107] A. El Shafie, "Comparison Between TDMA and Random Multiple-Access Energy-Harvesting Networks Under Security Constraints," *IEEE Communications Letters*, vol. 23, no. 2, pp. 334–337, Feb 2019.

[108] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Security of an Ordered-Based Distributive Jamming Scheme," *IEEE Communications Letters*, vol. 21, no. 1, pp. 72–75, Jan 2017.

[109] D. Wang, P. Ren, and J. Cheng, "Cooperative Secure Communication in Two-Hop Buffer-Aided Networks," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 972–985, Mar. 2018.

[110] X. Hong, P. Liu, F. Zhou, S. Guo, and Z. Chu, "Resource Allocation for Secure UAV-Assisted SWIPT Systems," *IEEE Access*, vol. 7, pp. 24 248–24 257, 2019.

[111] C. Yin, H. T. Nguyen, C. Kundu, Z. Kaleem, E. Garcia-Palacios, and T. Q. Duong, "Secure Energy Harvesting Relay Networks With Unreliable Backhaul Connections," *IEEE Access*, vol. 6, pp. 12 074–12 084, 2018.

[112] G. Hu and Y. Cai, "Analysis and Optimization of Wireless-Powered Cooperative Jamming for Sensor Network Over Nakagami- m Fading Channels," *IEEE Communications Letters*, vol. 23, no. 5, pp. 926–929, May 2019.

[113] S. Sharma, S. D. Roy, and S. Kundu, "Secrecy outage in a two-hop decode and forward relay network with accumulated harvested energy," *Physical Communication*, vol. 36, p. 100792, 2019.

[114] J. Wang, S. Lin, Y. Qiu, N. Huang, and J. Wang, "Tradeoff Between Secrecy Capacity and Harvested Energy for Secure Visible Light Communications With SWIPT," *IEEE Access*, vol. 7, pp. 29 543–29 552, 2019.

[115] J. Zhang, G. Pan, and H. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887–3893, 2016.

[116] X. Chen, J. Chen, and T. Liu, "Secure Transmission in Wireless Powered Massive MIMO Relaying Systems: Performance Analysis and Optimization," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8025–8035, Oct 2016.

[117] X. Tang, Y. Cai, Y. Deng, Y. Huang, W. Yang, and W. Yang, "Energy-Constrained SWIPT Networks: Enhancing Physical Layer Security With FD Self-Jamming," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 212–222, 2019.

[118] N. Zhao, Y. Li, S. Zhang, Y. Chen, W. Lu, J. Wang, and X. Wang, "Security Enhancement for NOMA-UAV Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 3994–4005, 2020.

[119] W. Wang, J. Tang, N. Zhao, X. Liu, X. Y. Zhang, Y. Chen, and Y. Qian, "Joint Precoding Optimization for Secure SWIPT in UAV-Aided NOMA Networks," *IEEE Transactions on Communications*, pp. 1–1, 2020.

[120] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative Jamming Aided Robust Secure Transmission for Wireless Information and Power Transfer in MISO Channels," *IEEE Transactions on Communications*, vol. 63, no. 3, pp. 906–915, Mar. 2015.

[121] H. Guo, Z. Yang, Y. Zou, T. Tsiftsis, M. R. Bhatangar, and R. C. D. Lamare, "Secure beamforming for cooperative wireless-powered networks with partial csi," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6760–6773, Aug 2019.

[122] Y. Bi and H. Chen, "Accumulate and Jam: Towards Secure Communication via A Wireless-Powered Full-Duplex Jammer," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1538–1550, Dec 2016.

[123] J. Zhang, G. Pan, and Y. Xie, "Secrecy Analysis of Wireless-Powered Multi-Antenna Relaying System With Nonlinear Energy Harvesters and Imperfect CSI," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 460–470, Jun. 2018.

[124] A. Biason, N. Laurenti, and M. Zorzi, "Achievable Secrecy Rates of an Energy Harvesting Device," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1502–1517, May 2016.

[125] E. Boshkovska, D. W. K. Ng, L. Dai, and R. Schober, "Power-Efficient and Secure WPCNs With Hardware Impairments and Non-Linear EH Circuit," *IEEE Transactions on Communications*, vol. 66, no. 6, pp. 2642–2657, Jun. 2018.

[126] X. Liu, Z. Li, and C. Wang, "Secure Decode-and-Forward Relay SWIPT Systems With Power Splitting Schemes," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7341–7354, Aug 2018.

[127] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, Aug 2014.

[128] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical Layer Security With RF Energy Harvesting in AF Multi-Antenna Relaying Networks," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3025–3038, July 2016.

[129] K. Lee, J. Hong, H. Choi, and T. Q. S. Quek, "Wireless-Powered Two-Way Relaying Protocols for Optimizing Physical Layer Security," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 162–174, Jan 2019.

[130] N. Nguyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, and L. Shu, "Secure 5G Wireless Communications: A Joint Relay Selection and Wireless Power Transfer Approach," *IEEE Access*, vol. 4, pp. 3349–3359, 2016.

[131] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy Performance Optimization for Wireless Powered Communication Networks With an Energy Harvesting Jammer," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 764–774, Feb. 2017.

[132] H. Niu, B. Zhang, Y. Huang, D. Guo, Z. Chu, and Z. Zhu, "Robust Secrecy Beamforming and Power-Splitting Design for Multiuser MISO Downlink With SWIPT," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1367–1375, 2019.

[133] Y. Lu, K. Xiong, P. Fan, Z. Ding, Z. Zhong, and K. B. Letaief, "Global Energy Efficiency in Secure MISO SWIPT Systems With Non-Linear Power-Splitting EH Model," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 216–232, Jan. 2019.

[134] Y. Hu, L. Li, H. Zhang, W. Liang, and A. Gao, "Wireless Powered D2D Communication Security Using LSTM in Emergency Communication System," in *Wireless and Optical Communications Conference (WOCC)*, May 2019, pp. 1–5.

[135] K. Cao, B. Wang, H. Ding, and J. Tian, "Adaptive Cooperative Jamming for Secure Communication in Energy Harvesting Relay Networks," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1316–1319, Oct 2019.

[136] X. Li, M. Huang, C. Zhang, D. Deng, K. M. Rabie, Y. Ding, and J. Du, "Security and Reliability Performance Analysis of Cooperative Multi-Relay Systems With Nonlinear Energy Harvesters and Hardware Impairments," *IEEE Access*, vol. 7, pp. 102 644–102 661, 2019.

[137] H. Niu, D. Guo, Y. Huang, and B. Zhang, "Robust Energy Efficiency Optimization for Secure MIMO SWIPT Systems With Non-Linear EH Model," *IEEE Communications Letters*, vol. 21, no. 12, pp. 2610–2613, Dec 2017.

[138] M. R. A. Khandaker, C. Masouros, K. Wong, and S. Timotheou, "Secure SWIPT by Exploiting Constructive Interference and Artificial

Noise," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1326–1340, Feb 2019.

[139] M. Li, H. Yin, Y. Huang, Y. Wang, and R. Yu, "Physical Layer Security in Overlay Cognitive Radio Networks With Energy Harvesting," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 274–11 279, Nov 2018.

[140] W. Zhao, R. She, and H. Bao, "Security Energy Efficiency Maximization for Two-Way Relay Assisted Cognitive Radio NOMA Network With Self-Interference Harvesting," *IEEE Access*, vol. 7, pp. 74 401–74 411, 2019.

[141] X. Sun, W. Yang, Y. Cai, R. Ma, and L. Tao, "Physical Layer Security in Millimeter Wave SWIPT UAV-Based Relay Networks," *IEEE Access*, vol. 7, pp. 35 851–35 862, 2019.

[142] X. Sun, W. Yang, Y. Cai, Z. Xiang, and X. Tang, "Secure Transmissions in Millimeter Wave SWIPT UAV-Based Relay Networks," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 785–788, Jun. 2019.

[143] Y. Zhu, G. Zheng, and M. Fitch, "Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Matérn Hardcore Point Processes," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1397–1409, Jul. 2018.

[144] Q. V. Do, T. Hoan, and I. Koo, "Optimal Power Allocation for Energy-Efficient Data Transmission Against Full-Duplex Active Eavesdroppers in Wireless Sensor Networks," *IEEE Sensors Journal*, vol. 19, no. 13, pp. 5333–5346, Jul. 2019.

[145] Q. Li, Q. Zhang, and J. Qin, "Secure Relay Beamforming for Simultaneous Wireless Information and Power Transfer in Nonregenerative Relay Networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2462–2467, Jun 2014.

[146] P. N. Son and H. Y. Kong, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Communications*, vol. 9, no. 17, pp. 2131–2139, 2015.

[147] Q. Shi, W. Xu, J. Wu, E. Song, and Y. Wang, "Secure Beamforming for MIMO Broadcasting With Wireless Information and Power Transfer," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2841–2853, May 2015.

[148] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust Secure Transmission in MISO Simultaneous Wireless Information and Power Transfer System," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 400–405, Jan 2015.

[149] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Security of Rechargeable Energy-Harvesting Transmitters in Wireless Networks," *IEEE Wireless Communications Letters*, vol. 5, no. 4, pp. 384–387, Aug 2016.

[150] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *IEEE Global Communications Conference*, Dec 2014, pp. 3145–3150.

[151] A. El Shafie and N. Al-Dhahir, "Secure Communications in the Presence of a Buffer-Aided Wireless-Powered Relay With Self-Energy Recycling," *IEEE Wireless Communications Letters*, vol. 5, no. 1, pp. 32–35, Feb. 2016.

[152] Z. Mobini, M. Mohammadi, and C. Tellambura, "Security enhancement of wireless networks with wireless-powered full-duplex relay and friendly jammer nodes," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2017, pp. 1329–1334.

[153] M. R. A. Khandaker, K. Wong, and G. Zheng, "Truth-Telling Mechanism for Two-Way Relay Selection for Secrecy Communications With Energy-Harvesting Revenue," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3111–3123, May 2017.

[154] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless Powered Cooperative Jamming for Secure OFDM System," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[155] Z. Deng, Q. Li, Q. Zhang, L. Yang, and J. Qin, "Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network with SWIPT," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[156] W. Xiang, M. Johnston, and S. Le Goff, "Low-Complexity Power Control and Energy Harvesting Algorithms for Wiretap Channels Employing Finite-Alphabet Input Schemes," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 318–326, Feb 2018.

[157] M. Zhang and Y. Liu, "Energy Harvesting for Physical-Layer Security in OFDMA Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 154–162, Jan 2016.

[158] H. Xing, L. Liu, and R. Zhang, "Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, Jan 2016.

[159] T. M. Hoang, T. Q. Duong, N. Vo, and C. Kundu, "Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[160] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M. Alouini, "On Secure Underlay MIMO Cognitive Radio Networks With Energy Harvesting and Transmit Antenna Selection," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 192–203, June 2017.

[161] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang, and Y. Cai, "Energy-Efficient Secure Transmission for Wireless Powered Internet of Things With Multiple Power Beacons," *IEEE Access*, vol. 6, pp. 75 086–75 098, 2018.

[162] P. Maji, S. Dhar Roy, and S. Kundu, "Physical layer security in cognitive radio network with energy harvesting relay and jamming in the presence of direct link," *IET Communications*, vol. 12, no. 11, pp. 1389–1395, 2018.

[163] Y. Zhang, F. Gao, L. Fan, X. Lei, and G. K. Karagiannidis, "Secure Communications for Multi-Tag Backscatter Systems," *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1146–1149, Aug 2019.

[164] P. Nguyen-Huu, K. Ho-Van, and V. N. Q. Bao, "Secrecy outage analysis of energy harvesting two-way relaying networks with friendly jammer," *IET Communications*, vol. 13, no. 13, pp. 1877–1885, 2019.

[165] S. Ghosh, M. R. Bhatnagar, A. Singh, and B. K. Panigrahi, "Secrecy Capacity in CRN With Malicious Energy Harvester Using Game Theoretic Techniques," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 3, pp. 343–360, Sep. 2017.

[166] K. Lee, J. Hong, H. Choi, and M. Levorato, "Adaptive Wireless-Powered Relaying Schemes With Cooperative Jamming for Two-Hop Secure Communication," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2793–2803, Aug. 2018.

[167] F. Jameel, S. Wyne, and Z. Ding, "Secure Communications in Three-Step Two-Way Energy Harvesting DF Relaying," *IEEE Communications Letters*, vol. 22, no. 2, pp. 308–311, Feb 2018.

[168] J. Wu, J. Wu, L. Chen, and Y. Wu, "Secrecy rate and residual energy trade-off in energy harvesting cognitive radio networks," *Physical Communication*, vol. 37, p. 100857, 2019.

[169] F. Zhao, W. Hao, L. Shen, G. Sun, Y. Zhou, and Y. Wang, "Secure Energy Efficiency Transmission for mmWave-NOMA System," *IEEE Systems Journal*, pp. 1–4, 2020.

[170] J. Ren, X. Lei, P. D. Diamantoulakis, Q. Chen, and G. K. Karagiannidis, "Buffer-aided Secure Relay Networks with SWIPT," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2020.

[171] D. W. K. Ng, E. S. Lo, and R. Schober, "Multiobjective Resource Allocation for Secure Communication in Cognitive Radio Networks With Wireless Information and Power Transfer," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3166–3184, May 2016.

[172] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy Rate Beamforming for Multicell Networks With Information and Energy Harvesting," *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677–689, Feb 2017.

[173] M. Alageli, A. Ikhlef, and J. Chambers, "SWIPT Massive MIMO Systems With Active Eavesdropping," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 233–247, Jan 2019.

[174] P. Wang, N. Wang, M. Dabaghchian, K. Zeng, and Z. Yan, "Optimal Resource Allocation for Secure Multi-User Wireless Powered Backscatter Communication with Artificial Noise," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, April 2019, pp. 460–468.

[175] B. Ji, Y. Li, S. Chen, C. Han, C. Li, and H. Wen, "Secrecy Outage Analysis of UAV Assisted Relay and Antenna Selection for Cognitive Network under Nakagami-m Channel," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2020.

[176] M. J. Saber, A. Keshavarz, J. Mazloum, A. M. Sazdar, and M. J. Piran, "Physical-Layer Security Analysis of Mixed SIMO SWIPT RF and FSO Fixed-Gain Relaying Systems," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2851–2858, Sep. 2019.

[177] T. A. Le, H. X. Nguyen, Q. Vien, and M. Karamanoglu, "Secure Information Transmission and Power Transfer in Cellular Networks," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1532–1535, Sep. 2015.

[178] Y. Huang, Z. Li, F. Zhou, and R. Zhu, "Robust AN-Aided Beamforming Design for Secure MISO Cognitive Radio Based on a Practical Nonlinear EH Model," *IEEE Access*, vol. 5, pp. 14 011–14 019, 2017.

[179] H. Gao, T. Lv, W. Wang, and N. C. Beaulieu, "Energy-Efficient and Secure Beamforming for Self-Sustainable Relay-Aided Multicast

Networks," *IEEE Signal Processing Letters*, vol. 23, no. 11, pp. 1509–1513, Nov 2016.

[180] K. Tang, R. Shi, H. Shi, M. Z. A. Bhuiyan, and E. Luo, "Secure beamforming for cognitive cyber-physical systems based on cognitive radio with wireless energy harvesting," *Ad Hoc Networks*, vol. 81, pp. 174 – 182, 2018.

[181] L. Jiang, H. Tian, C. Qin, S. Gjessing, and Y. Zhang, "Secure Beamforming in Wireless-Powered Cooperative Cognitive Radio Networks," *IEEE Communications Letters*, vol. 20, no. 3, pp. 522–525, Mar. 2016.

[182] E. Boshkovska, N. Zlatanov, L. Dai, D. W. K. Ng, and R. Schober, "Secure SWIPT Networks Based on a Non-Linear Energy Harvesting Model," in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Mar. 2017, pp. 1–6.

[183] V. Nhan Vo, T. G. Nguyen, C. So-In, Z. A. Baig, and S. Sanguanpong, "Secrecy Outage Performance Analysis for Energy Harvesting Sensor Networks With a Jammer Using Relay Selection Strategy," *IEEE Access*, vol. 6, pp. 23 406–23 419, 2018.

[184] Y. Bi and A. Jamalipour, "Accumulate Then Transmit: Toward Secure Wireless Powered Communication Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 7, pp. 6301–6310, Jul. 2018.

[185] P. Yan, Y. Zou, and J. Zhu, "Energy-Aware Multiuser Scheduling for Physical-Layer Security in Energy-Harvesting Underlay Cognitive Radio Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2084–2096, March 2018.

[186] T. G. Nguyen, C. So-In, H. Tran, S. Sanguanpong *et al.*, "Secrecy Performance in the Internet of Things: Optimal Energy Harvesting Time Under Constraints of Sensors and Eavesdroppers," *Mobile Networks and Applications*, pp. 1–18, 2019.

[187] M. Alageli, A. Ikhlef, and J. Chambers, "Optimization for Maximizing Sum Secrecy Rate in MU-MISO SWIPT Systems," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 537–553, Jan 2018.

[188] H. Ma, J. Cheng, and X. Wang, "Proportional Fair Secrecy Beamforming for MISO Heterogeneous Cellular Networks With Wireless Information and Power Transfer," *IEEE Transactions on Communications*, vol. 67, no. 8, pp. 5659–5673, Aug 2019.

[189] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial Noise Aided Secure Cognitive Beamforming for Cooperative MISO-NOMA Using SWIPT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, Apr. 2018.

[190] L. Ni, X. Da, H. Hu, Y. Huang, R. Xu, and M. Zhang, "Outage Constrained Robust Transmit Design for Secure Cognitive Radio With Practical Energy Harvesting," *IEEE Access*, vol. 6, pp. 71 444–71 454, 2018.

[191] T. D. Hieu, T. T. Duy, and B. Kim, "Performance Enhancement for Multihop Harvest-to-Transmit WSNs With Path-Selection Methods in Presence of Eavesdroppers and Hardware Noises," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 5173–5186, June 2018.

[192] M. R. A. Khandaker and K. Wong, "Masked Beamforming in the Presence of Energy-Harvesting Eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 40–54, Jan 2015.

[193] H. Niu, D. Guo, Y. Huang et al., "Outage Constrained Robust Energy Harvesting Maximization for Secure MIMO SWIPT Systems," *IEEE Wireless Communications Letters*, vol. 6, no. 5, pp. 614–617, Oct 2017.

[194] M. Khandaker, K. Wong, Y. Zhang et al., "Probabilistically Robust SWIPT for Secrecy MISOME Systems," *IEEE Trans. on Information Forensics and Security*, vol. 12, no. 1, pp. 211–226, Jan 2017.

[195] X. Chen, L. Guo, X. Li, C. Dong, J. Lin, and P. T. Mathiopoulos, "Secrecy Rate Optimization for Cooperative Cognitive Radio Networks Aided by a Wireless Energy Harvesting Jammer," *IEEE Access*, vol. 6, pp. 34 127–34 134, 2018.

[196] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO Beamforming for Simultaneous Wireless Information and Power Transfer," *IEEE Transactions on Signal Processing*, vol. 62, no. 18, pp. 4798–4810, Sep. 2014.

[197] A. Zappone and E. Jorswieck, *Energy Efficiency in Wireless Networks via Fractional Programming Theory*. Now Foundations and Trends, 2015.

[198] S. S. Kalamkar and A. Banerjee, "Secure Communication via a Wireless Energy Harvesting Untrusted Relay," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2199–2213, Mar. 2017.

[199] B. He, J. Chen, Y. Kuo, and L. Yang, "Cooperative Jamming for Energy Harvesting Multicast Networks with an Untrusted Relay," *IET Communications*, vol. 11, no. 13, pp. 2058–2065, 2017.

[200] M. T. Mamaghani and R. Abbas, "Security and reliability performance analysis for two-way wireless energy harvesting based untrusted relaying with cooperative jamming," *IET Communications*, vol. 13, no. 4, pp. 449–459, 2019.

[201] H. Shi, W. Yang, D. Chen, Y. Luo, and Y. Cai, "Secure Transmission for Simultaneous Wireless Information and Power Transfer in AF Untrusted Relay Networks," *Sensors*, vol. 19, no. 1, p. 76, 2019.

[202] H. Shi, Y. Cai, D. Chen, J. Hu, W. Yang, and W. Yang, "Physical Layer Security in an Untrusted Energy Harvesting Relay Network," *IEEE Access*, vol. 7, pp. 24 819–24 828, 2019.

[203] D. Chen, Y. Cheng, X. Wang, W. Yang, J. Hu, and Y. Cai, "Energy-efficient secure multiuser scheduling in energy harvesting untrusted relay networks," *Journal of Communications and Networks*, vol. 21, no. 4, pp. 365–375, Aug 2019.

[204] R. Yao, Y. Lu, T. A. Tsiftsis, N. Qi, T. Mekkawy, and F. Xu, "Secrecy Rate-Optimum Energy Splitting for an Untrusted and Energy Harvesting Relay Network," *IEEE Access*, vol. 6, pp. 19 238–19 246, 2018.

[205] K. Lee, J. Lim, and H. Choi, "Impact of Outdated CSI on the Secrecy Performance of Wireless-Powered Untrusted Relay Networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1423–1433, 2020.

[206] V. Nhan Vo, D. Tran, C. So-In, and H. Tran, "Secrecy Performance Analysis for Fixed-Gain Energy Harvesting in an Internet of Things With Untrusted Relays," *IEEE Access*, vol. 6, pp. 48 247–48 258, 2018.

[207] A. El Shafie, A. Mabrouk, K. Tourki, N. Al-Dhahir, and R. Hamila, "Securing Untrusted RF-EH Relay Networks Using Cooperative Jamming Signals," *IEEE Access*, vol. 5, pp. 24 353–24 367, 2017.

[208] M. Elbayoumi, M. Kamel, W. Hamouda, and A. Youssef, "NOMA-Assisted Machine-Type Communications in UDN: State-of-the-Art and Challenges," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[209] M. Caprolu, S. Sciancalepore, and R. Di Pietro, "Short-Range Audio Channels Security: Survey of Mechanisms, Applications, and Research Challenges," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[210] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-Splitting Multiple Access for Coordinated Multi-Point Joint Transmission," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019, pp. 1–6.

[211] B. Clerckx, Y. Mao, R. Schober, and H. V. Poor, "Rate-Splitting Unifying SDMA, OMA, NOMA, and Multicasting in MISO Broadcast Channel: A Simple Two-User Rate Analysis," *IEEE Wireless Communications Letters*, vol. 9, no. 3, pp. 349–353, 2020.

[212] C. K. Thomas, B. Clerckx, L. Sanguinetti, and D. Slock, "A Rate Splitting Strategy for Mitigating Intra-Cell Pilot Contamination in Massive MIMO," 2020.

[213] C. Hao, B. Rassouli, and B. Clerckx, "Achievable DoF Regions of MIMO Networks With Imperfect CSIT," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6587–6606, 2017.

[214] Y. Mao, B. Clerckx, and V. O. K. Li, "Rate-Splitting for Multi-Antenna Non-Orthogonal Unicast and Multicast Transmission: Spectral and Energy Efficiency Analysis," *IEEE Transactions on Communications*, vol. 67, no. 12, pp. 8754–8770, 2019.

[215] A. Flores, R. C. de Lamare, and B. Clerckx, "Study of Linear Precoding and Stream Combining for Rate Splitting in MU-MIMO Systems," 2020.

[216] Z. Li, C. Ye, Y. Cui et al., "Rate Splitting for Multi-Antenna Downlink: Precoder Design and Practical Implementation," 2020.

[217] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Towards Smart Radio Environment for Wireless Communications via Intelligent Reflecting Surfaces: A Comprehensive Survey," 2019.

[218] S. Hu, F. Rusek, and O. Edfors, "Beyond Massive MIMO: The Potential of Data Transmission With Large Intelligent Surfaces," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2746–2758, 2018.

[219] Q. Nadeem, A. Kammoun, A. Chaaban et al., "Asymptotic Max-Min SINR Analysis of Reconfigurable Intelligent Surface Assisted MISO Systems," 2019.

[220] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[221] S. Li, B. Duo, X. Yuan et al., "Reconfigurable Intelligent Surface Assisted UAV Communication: Joint Trajectory Design and Passive Beamforming," *IEEE Wireless Communications Letters*, pp. 1–1, 2020.

[222] J. Chen, Y. Liang, Y. Pei, and H. Guo, "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[223] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. Alouini, and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[224] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces," 2019.

[225] K. Feng and X. Li, "Physical layer security enhancement exploiting intelligent reflecting surface," 2019.

[226] B. Feng, Y. Wu, and M. Zheng, "Secure Transmission Strategy for Intelligent Reflecting Surface Enhanced Wireless System," in *Int. Conf. on Wireless Communications and Signal Processing*, 2019, pp. 1–6.

[227] M. Cui, G. Zhang, and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[228] W. Jiang, Y. Zhang, J. Wu, W. Feng, and Y. Jin, "Intelligent Reflecting Surface Assisted Secure Wireless Communications with Multiple-Transmit and Multiple-Receive Antennas," 2020.

[229] X. Lu, W. Yang, X. Guan, Q. Wu, and Y. Cai, "Robust and Secure Beamforming for Intelligent Reflecting Surface Aided mmWave MISO Systems," 2020.

[230] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-Noise-Aided Secure MIMO Wireless Communications via Intelligent Reflecting Surface," 2020.

[231] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and Secure Wireless Communications via Intelligent Reflecting Surfaces," 2019.

[232] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Deep Reinforcement Learning Based Intelligent Reflecting Surface for Secure Wireless Communications," 2020.

[233] X. Yu, D. Xu, and R. Schober, "Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces," 2019.

[234] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy Rate Maximization for Intelligent Reflecting Surface Assisted Multi-Antenna Communications," *IEEE Communications Letters*, vol. 23, no. 9, pp. 1488–1492, 2019.

[235] Z. Chu, W. Hao, P. Xiao, and J. Shi, "Intelligent Reflecting Surface Aided Multi-Antenna Secure Transmission," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 108–112, 2020.

[236] X. Guan, Q. Wu, and R. Zhang, "Intelligent Reflecting Surface Assisted Secrecy Communication: Is Artificial Noise Helpful or Not?" *IEEE Wireless Communications Letters*, pp. 1–1, 2020.

[237] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource Allocation for Secure IRS-assisted Multiuser MISO Systems," 2019.

[238] M. M. U. Rahman, S. Kanwal, and J. Gross, "Simultaneous Energy Harvesting and Sender-Node Authentication at a Receiver Node," in *IEEE Int. Conf. on Ubiquitous Wireless Broadband*, Oct 2015, pp. 1–5.

[239] W. Xu, G. Lan, Q. Lin, S. Khalifa, M. Hassan, N. Bergmann, and W. Hu, "KEH-Gait: Using Kinetic Energy Harvesting for Gait-based User Authentication Systems," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 139–152, Jan 2019.

[240] Q. Yao, J. Ma, R. Li, X. Li, J. Li, and J. Liu, "Energy-Aware RFID Authentication in Edge Computing," *IEEE Access*, vol. 7, pp. 77 964–77 980, 2019.

[241] A. Ranganathan, B. Danev, and S. Capkun, "Proximity Verification for Contactless Access Control and Authentication Systems," in *Proceedings of the 31st Annual Computer Security Applications Conference*, ser. ACSAC 2015, 2015, pp. 271–280.

[242] Q. Yao, J. Ma, S. Cong, X. Li, and J. Li, "Attack Gives Me Power: DoS-defending Constant-time Privacy-preserving Authentication of Low-cost Devices Such As Backscattering RFID Tags," in *Proc. of ACM Workshop on Mobile Sensing, Computing and Communication*, 2016, pp. 23–28.

[243] N. Rajatheva, I. Atzeni, E. Bjornson, et al., "White Paper on Broadband Connectivity in 6G," 2020.

[244] G. Oligeri, S. Sciancalepore, and R. Di Pietro, "GNSS Spoofing Detection via Opportunistic IRIDUM Signals," in *Proceedings of the 13th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '20, 2020.

[245] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.

[246] Y. Nozaki and M. Yoshikawa, "Physical Unclonable Function Using Energy Harvesting," in *IEEE International Meeting for Future of Electron Devices, Kansai (IMFEDK)*, June 2018, pp. 1–2.

[247] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[248] S. Lv, X. Lu, Z. Lu, et al., "Zero reconciliation secret key extraction in MIMO backscatter wireless systems," in *IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[249] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart Meter Privacy With Renewable Energy and an Energy Storage Device," *IEEE Trans. on Information Forensics and Security*, vol. 13, no. 1, pp. 129–142, Jan 2018.

[250] M. Min, X. Wan, L. Xiao, et al., "Learning-Based Privacy-Aware Offloading for Healthcare IoT With Energy Harvesting," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4307–4316, Jun. 2019.

[251] O. Tan, D. Gunduz, and H. V. Poor, "Increasing Smart Meter Privacy Through Energy Harvesting and Storage Devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, Jul. 2013.

[252] N. A. Alrajeh, S. Khan, J. Lloret, and J. Loo, "Secure routing protocol using cross-layer design and energy harvesting in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 1, p. 374796, 2013.

[253] J. Tang, A. Liu, J. Zhang, et al., "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks," *Sensors*, vol. 18, no. 3, p. 751, 2018.

[254] A. M. Zungeru, J. Gaboitaolelwe, B. Diarra et al., "A Secured Smart Home Switching System based on Wireless Communications and Self-Energy Harvesting," *IEEE Access*, vol. 7, pp. 25 063–25 085, 2019.

Pietro Tedeschi is a PhD Student in Computer Science and Engineering at HBKU-CSE, Doha, Qatar. He is an active member of the Cyber-Security Research Innovation Lab. He received his Bachelor's degree in Computer and Automation Engineering in 2014 with a thesis on the Analysis of Security Protocols for the Internet of Things, in IEEE 802.15.4e Networks, and his Master's degree (with honors) in Computer Engineering in 2017 with a thesis on the Development of Security Architectures in Intelligent Transport Systems for EU Horizon 2020 BONVOYAGE project, both from the "Politecnico di Bari". From 2017 to 2018, he worked as Security Researcher at CNIT (Consorzio Nazionale Interuniversitario per le Telecomunicazioni), Italy, for the EU H2020 SymbIoTe project. His research interests span over UAV/Drone Security, Wireless Security, Internet of Things (IoT), Applied Cryptography, and Cyber-Physical Systems.

Savio Sciancalepore Savio Sciancalepore is currently Post Doc at HBKU-CSE-ICT, Doha, Qatar. He obtained his Master's degree in Telecommunications Engineering in 2013 and the PhD in Electric and Information Engineering in 2017, both from the Politecnico di Bari, Italy. He received the prestigious award from the ERCIM Security, Trust, and Management (STM) Working Group for the best Ph.D. Thesis in Information and Network Security in 2018. He is also serving as an Academic Editor for the journal Security and Communication Networks (Hindawi). His major research interests include network security issues in Internet of Things (IoT) and Cyber-Physical Systems.

Roberto Di Pietro, ACM Distinguished Scientist, is Full Professor in Cybersecurity at HBKU-CSE. Previously, he was in the capacity of Global Head Security Research at Nokia Bell Labs, and Associate Professor (with tenure) of Computer Science at University of Padova, Italy. He also served 10+ years as senior military technical officer. Overall, he has been working in the cybersecurity field for 23+ years, leading both technology-oriented and research-focused teams in the private sector, government, and academia (MoD, United Nations HQ, EUROJUST, IAEA, WIPO). His main research interests include security and privacy for wired and wireless distributed systems (e.g. Blockchain technology, Cloud, IoT, On-line Social Networks), virtualization security, applied cryptography, computer forensics, and data science. Other than being involved in M&A of start-up—and having founded one (exited)—, he has been producing 230+ scientific papers and patents over the cited topics, has co-authored two books, edited one, and contributed to a few others. He is serving as an AE for ComCom, ComNet, PerCom, Journal of Computer Security, and other Intl. journals. In 2011-2012 he was awarded a Chair of Excellence from University Carlos III, Madrid. In 2020 he received the Jean-Claude Laprie Award for having significantly influenced the theory and practice of Dependable Computing.