sensors

MDPI

Article

A Physical-Layer Security Cooperative Framework for Mitigating Interference and Eavesdropping Attacks in Internet of Things Environments

Abdallah Farraj [1,*] and Eman Hammad [2]

[1] Department of Electrical Engineering, Texas A&M University-Texarkana/RELLIS Campus, Bryan, TX 77807, USA
[2] Engineering Technology and Industrial Distribution Department, Texas A&M University, College Station, TX 77843, USA; eman.hammad@tamu.edu
* Correspondence: afarraj@tamut.edu

Abstract: Intentional electromagnetic interference attacks (e.g., jamming) against wireless connected devices such as the Internet of Things (IoT) remain a serious challenge, especially as such attacks evolve in complexity. Similarly, eavesdropping on wireless communication channels persists as an inherent vulnerability that is often exploited by adversaries. This article investigates a novel approach to enhancing information security for IoT systems via collaborative strategies that can effectively mitigate attacks targeting availability via interference and confidentiality via eavesdropping. We examine the proposed approach for two use cases. First, we consider an IoT device that experiences an interference attack, causing wireless channel outages and hindering access to transmitted IoT data. A physical-layer-based security (PLS) transmission strategy is proposed in this article to maintain target levels of information availability for devices targeted by adversarial interference. In the proposed strategy, select IoT devices leverage a cooperative transmission approach to mitigate the IoT signal outages under active interference attacks. Second, we consider the case of information confidentiality for IoT devices as they communicate over wireless channels with possible eavesdroppers. In this case, we propose a collaborative transmission strategy where IoT devices create a signal outage for the eavesdropper, preventing it from decoding the signal of the targeted devices. The analytical and numerical results of this article illustrate the effectiveness of the proposed transmission strategy in achieving desired IoT security levels with respect to availability and confidentiality for both use cases.

Keywords: Internet of Things (IoT); physical-layer security (PLS); wireless communication; information availability; information confidentiality; interference attacks; eavesdropping; cooperative transmission strategy

Citation: Farraj, A.; Hammad, E. A Physical-Layer Security Cooperative Framework for Mitigating Interference and Eavesdropping Attacks in Internet of Things Environments. *Sensors* **2024**, *24*, 5171. https://doi.org/10.3390/s24165171

Academic Editor: Naveen Chilamkurti

Received: 29 June 2024
Revised: 6 August 2024
Accepted: 9 August 2024
Published: 10 August 2024

1. Introduction

The daily activities of modern living have become more integrated and, in many cases, reliant on technology. This holds true on the consumer level, as well as industrial and enterprise levels. Technologies that provide versatility and connectivity and enable efficient operations with simpler user experience have become prevalent. One of the most dominant technologies in this context are devices that can sense and/or actuate and control some physical quantity, are connected to the Internet, and can communicate with users or other devices. Such devices have become known as Internet of Things (IoT) devices. IoT devices can be loosely categorized into consumer and industrial general types, with predictions expecting the number of connected IoT devices globally to exceed 32 billion by 2030 [1]. IoT expands a large spectrum of technologies from drones, robots, connected vehicles, health devices, controllers, grid electric transformers, and many other industries. IoT devices have existed since the early days of the Internet and have since become an increasingly fascinating manifestation of technological development.

Industrial use cases across many domains extensively utilize IoT to perform sensing and actuation tasks with minimal human intervention [2], thus supporting higher levels of automation and autonomy. Hence, cybersecurity and resilience become critical, specifically in ensuring the integrity, confidentiality, and availability of the IoT devices and communication connectivity to the devices. While IoT devices vary largely in capabilities and the nature of available computational resources, the general trend in the industry optimizes on-device resources such as processing, memory, storage, energy usage, and cost based on functionality and purpose. This often has resulted in IoT technologies suffering from serious security flaws and gaps. In fact, several major cybersecurity attacks during the past few years have leveraged IoT devices as part of the attack kill chain [3,4]. Most recently, many efforts have focused on improving IoT built-in security.

Cybersecurity encompasses technologies and practices to safeguard information's availability, integrity, and confidentiality. Traditional cybersecurity measures primarily focus on preventing the unauthorized access, disruption, and modification of information. The evolution of such controls was historically based on a special class of technologies (Information Technologies or IT) used in information systems within typical computer networks. Traditional cybersecurity defenses and controls, such as access control, key management, and encryption schemes, often prove impractical for ecosystems with limited storage, processing, and transmission capabilities [5–7]. Security priorities in an IoT system rely heavily on the nature of the system, whereas, in delay-sensitive critical infrastructures, availability and integrity are of the highest priority. In other IoT environments, such as health monitoring, confidentiality may be of higher priority. In critical control operations and industrial processes, measures for the confidentiality of information prevent unauthorized access to sensor measurements by an illegitimate eavesdropper, thus avoiding the disclosure of the industrial process's critical information. Data theft in wireless IoT networks raises concerns related to violations of privacy, infringements of intellectual property, and reverse engineering of system settings.

To fully capitalize on the benefits of IoT ecosystems, it is crucial to apply robust security controls [8–12]. Inadequate security and negligence of proper risk understanding and management may cause significant damage from adversaries, particularly when IoT is part of critical industrial control systems [7,13]. Ensuring information integrity and availability becomes paramount in such environments. Information availability guarantees that controllers receive timely access to IoT-transmitted data as needed. Similarly, information confidentiality measures ensure that only devices allowed to read the information are able to do so.

IoT systems are widely employed in various industries and mostly utilize a form of wireless communication for connectivity. Using wireless communication technologies can support scalability in large-scale IoT systems' deployments and operations. Machine-to-machine communication links (e.g., Zigbee, LoRa, Bluetooth) often prove to be useful for large-scale deployments [1,14–16]. Modern wireless technologies, such as spectrum-sharing communication systems, present new opportunities to enable IoT connectivity [17]. This is particularly interesting in newer generations of cellular communication, such as 6G, where massive machine-type communication continues to be a key driver. Due to the shared nature of the communication channel, wireless IoT networks face critical challenges in ensuring information security [18]. The complexity of emerging security threats targeting IoT devices further exacerbates the issue, especially in resource-constrained IoT systems. Incidents like the Mirai attack have highlighted the vulnerability of IoT systems to cyber attacks [7,18,19].

The dominant use of wireless communication channels in IoT environments cast them as attractive targets for threat vectors that exploit the inherent vulnerabilities in such channels' physical and data layers. For example, in attacks that target availability, an adversary may intentionally interfere with and degrade wireless communication channels. Such attacks may disrupt industrial control system operations, raising concerns related to health,

safety, and quality. Similarly, an adversary who has access to the wireless communication medium may sniff the spectrum to reverse engineer transmitted information.

This work acknowledges current IoT security challenges, particularly in resource-constrained devices, to address IoT interference and eavesdropping attacks. In this article, we present an alternative approach to security at the physical layer, focusing on two use cases with different security objectives. We motivate the physical-layer security (PLS) approach as a complementary approach to other network and application layer mechanisms. Due to the challenges in securing IoT systems and the inherent computational limitations of the devices, PLS methods are becoming more popular [5,6,20,21]. A major benefit of PLS approaches for IoT environments lies in their ability to provide enhanced security within the constrained resources of the IoT devices as we illustrate in this article with the proposed strategies. Other security controls on the network and application layers are often limited due to restricted device resources.

First, we consider the challenge of interference attacks, where we investigate a scenario where an IoT device transmits its sensor data to a receiver unit through a wireless channel that is subjected to an intentional interference attack by an *adversary*. The malicious interference negatively affects the legitimate IoT's received signal, which results in channel outages that impede timely access to IoT data at the receiver unit, thereby disrupting the availability of IoT data. In the IoT system under investigation, the legitimate device can coordinate its transmission with other IoT devices in the ecosystem to mitigate the negative impacts of the interference attack conducted by the adversary. One objective of the proposed security approach is to limit the average outage probability of the legitimate device's signal to an acceptable threshold during the interference attack. The approach employed in this work focuses on employing a spectrum-sharing cognitive communication framework [22] to address information availability at the physical layer. Cooperative communications between devices in the IoT ecosystem are employed to enhance the quality of service (QoS) of the received signal during the interference attack.

Second, we consider a setup with several IoT devices utilizing a wireless channel to communicate their sensor measurements. A set of the IoT devices, called primary devices, require higher signal quality guarantees at the receiver compared with the the rest of the devices (called secondary devices), which have lower transmission priority. The primary and secondary IoT devices may use different receiving units. Additionally, there is an illegitimate device, referred to as the eavesdropper, attempting to decode the primary device's transmission. A coordinated transmission strategy by secondary IoT devices is developed in this article to ensure the information confidentiality of the primary device's signal in the presence of the eavesdropper.

In the remaining parts of the articles, we discuss security for IoT systems in Section 2, and we discuss the proposed solutions for interference attacks in Section 3 and for eavesdropping in Section 4. Simulation results illustrating the performance of the proposed solutions are shown and discussed in Section 5. Conclusions and future work are presented in Section 6.

2. Background and Motivation

Recently, security strategies originally developed for sensor networks have been extended to IoT environments due to their similarities [5,16,23–29]. However, the widespread deployment of IoT devices, coupled with their unique computational capabilities and energy efficiency, presents challenges for existing security approaches. For instance, security schemes relying on compressive sensing, probabilistic ciphering, and channel state information scalability suffer as the number of devices increases. Additionally, computationally complex schemes like compressive sensing are impractical for resource-limited IoT devices [2,5]. Moreover, the sheer number of IoT devices and the complexity of interconnected systems make it more challenging to identify and address security vulnerabilities.

Physical-layer security leverages wave propagation and transmitter/receiver designs and offers an approach to information security by enabling secure communication over

wireless channels [2,5,26,30,31]. In the context of IoT systems, PLS approaches have the capability to overcome some of the constraints of conventional cybersecurity solutions and offer extra layers of protection against cyber attacks [20,21]. It can make eavesdropping and disrupting IoT communications more difficult for attackers without transmitting additional information.

A review of physical-layer security approaches for achieving information security in wireless channels is provided in [5,32]. The challenges and opportunities of using PLS in IoT systems are discussed in surveys such as [31,33–35]. Several PLS techniques can be employed in IoT systems, including beamforming to direct signals toward intended receivers and away from eavesdroppers as well as the use of artificial noise to hinder eavesdroppers in decoding transmitted signals. Other existing PLS methods include operating within the secrecy capacity, exploiting channel signatures, using spectrum spreading techniques, and node cooperation to degrade the eavesdropper's communication channel [36]. Additional results on PLS security are summarized in [6].

The work in [37] investigated security solutions for heterogeneous IoT and multi-access mobile edge computing (MA-MEC) in smart cities, focusing on physical-layer security technologies like secure wiretap coding, resource allocation, signal processing, and multi-node cooperation to address emerging security threats. The researchers in [38] proposed a Gaussian-tag-embedded physical-layer authentication scheme for IoT security, using a weighted fractional Fourier transform to verify signal authenticity, and they conducted security analysis and experiments to demonstrate the scheme's robustness against spoofing and replay attacks. The study in [39] explored a secure wireless communication scenario in IoT for protecting data collection from detection and eavesdropping attacks. The work in [40] studied secure beamforming design in a two-way cognitive radio IoT network with simultaneous wireless information and power transfer with the aim to maximize the secrecy sum rate for primary users by designing beamforming solutions and optimization algorithms to balance complexity and performance.

Studies have examined the average secrecy capacities of wireless multi-user networks against passive or active eavesdroppers [41]. Physical-layer security approaches for wireless sensor networks include distributed co-phasing-based transmissions [26] and energy-efficient solutions for securing downlink IoT connections through interference exploitation [6]. A unified framework for various physical-layer security systems has been proposed [42]. In [20], physical-layer security measures for an IoT environment under jamming signals are discussed, utilizing a game-theoretic formulation for distributed IoT channel access. However, scaling this game-theoretic approach becomes challenging as the number of IoT devices increases due to transmission collisions and retransmissions.

The proposed solutions for interference and eavesdropping attacks in this article are innovative as they do not waste resources, provide opportunities for IoT cooperation, complement other security measures that are in place, strengthen defense-in-depth strategy, and quantify a measure of information availability and confidentiality using outage probability. The proposed algorithms use a round-robin approach to include secondary IoT devices, providing a chance to communicate over the channel for all devices and leading to more fairness in the IoT network. The algorithms also include a degree of flexibility through setting the value of a cooperation factor. It is important to note here that the proposed cooperative transmission strategy for interference attacks requires accurate estimates of the adversary channel gains, which is feasible using channel estimation techniques for active interfering agents.

In the following, we discuss the proposed PLS solutions for IoTs under interference attack in Section 3 and for eavesdropping attacks in Section 4. The theoretical framework and the cooperative transmission strategies that enable the IoTs to respond to the cyber attacks will be developed for both use cases.

3. PLS for Interference Attacks Defense

Consider a communication system consisting of multiple IoT devices that need to transmit data using a wireless channel. Within this ecosystem, certain devices, referred to as primary IoT devices, require higher information availability guarantees at their respective receivers compared to others, known as secondary IoT devices. It should be noted that primary and secondary IoT devices may have different receiver units. In this scenario, an adversary specifically targets the data transmission of a primary IoT device by conducting interference attacks that jam its receiver unit. To address this challenge, a spectrum-sharing cognitive communication paradigm is utilized [43]. Secondary IoT devices can concurrently transmit over the shared channel along with the primary IoT device to ensure a target level of signal quality for the primary device. The primary outage probability is considered as the QoS metric in this setup.

To utilize the channel, the secondary IoT device cooperates with the primary device by allocating a portion of its power to relay the primary device's signal and using the remaining power to transmit its own data. Consequently, the simultaneous transmission of signals introduces additional interference at the intended receiver. However, the QoS of the received signal can be improved through cooperative communication from the secondary IoT devices in the system. This cooperative communication approach allows the primary IoT device to achieve a certain measure of information availability while under interference attacks by the adversary.

3.1. System Model

Consider the spectrum-sharing uplink communication environment depicted in Figure 1. This setup includes a legitimate primary IoT device that intends to transmit its data (for example, sensor readings) to a primary receiver unit (PR). Also, the wireless communication environment includes other secondary devices (collectively referred to as ST) that aim to transmit their information to a secondary receiver unit (SR). In this communication system, the PR and SR can simultaneously transmit over the shared wireless channel. Additionally, the communication system includes an adversary device (referred to as AT) that attacks the data transmission of the PT by causing an interference at the PR. In a similar way, the adversary's transmission introduces additional interference at the SR as well. In addition, the secondary transmission by the ST causes interference at the PR. In a similar fashion, the primary transmission by the PT leads to additional interference at the secondary receiver SR.

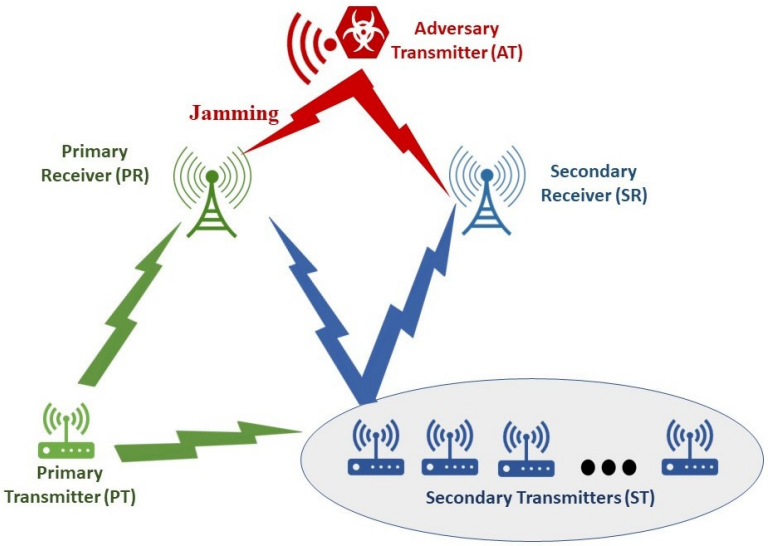

Figure 1. Interference attacks problem setup.

Furthermore, the PT utilizes the secondary transmission by the cooperative ST to alter the composition and characteristics of its received signals at the PR, with the goal of limiting the average value of the outage probability of the primary signal at the PR in order to achieve certain degree of information availability during the AT's interference attack. Throughout the time duration of interest, the PR transmits its data at a rate of R_p with a power of P_p. Each transmission interval involves the selection of a secondary device to communicate over the shared channel with a power of P_s and a rate of R_s. In addition, the adversary user causes interference utilizing a transmission power of P_a. Finally, the PR and SR experience additive white Gaussian noise (AWGN) signals with zero mean and a variance of σ_p^2 and σ_s^2, respectively.

The wireless channels between the different IoT devices and receiver units in this environment undergo independent and identically distributed (i.i.d.) Rayleigh block fading. Figure 2 illustrates the power gains of the channels between the PT and PR and the PT and SR as g_{pp} and g_{ps}, respectively, with average values of λ_{pp} and λ_{ps}. Likewise, the power gains of the channels between the AT and PR and the AT and SR are termed as g_{ap} and g_{as}, respectively, with average values of λ_{ap} and λ_{as}. Finally, the power gains of the channels between the ST and PR and the ST and SR are represented by g_{sp} and g_{ss}, respectively, with average values of λ_{sp} and λ_{ss}. These different λ values capture pertinent characteristics of the communication environment, such as propagation distance between the transmitter and receiver units, path loss, shadowing, and the general fading state of the channel.

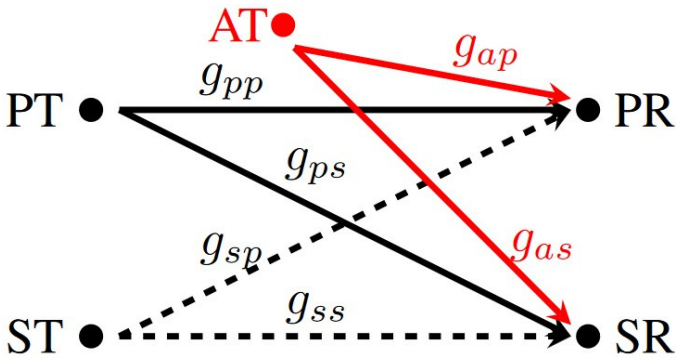

Figure 2. Interference attacks problem model.

3.2. Cooperation Model

To mitigate the impact of the interference signal injected by the adversary unit and facilitate cooperation with the primary IoT device, the secondary device allocates a portion of its transmission power (P_s) for relaying the PT's data. In this communication environment, the following assumptions are made:

1. The PT and ST are relatively close to each other so that the propagation time between the PT and ST is insignificant compared to that between the PT and PR.
2. The ST possesses accurate retransmission capability for PT's data.
3. The ST dedicates a fraction αP_s of its transmission power to cooperate with the PT, and the remaining fraction $(1-\alpha)P_s$ is used for transmitting ST's own coded signal.

Here, α represents the cooperation factor, satisfying the condition $0 \leq \alpha < 1$. Although we realize that the first two assumptions might not be very practical at all times, nevertheless, they provide us with a direct way to derive the following mathematical terms and keep the developed expressions traceable.

Let γ_p represent the signal-to-interference plus noise ratio (SINR) of the PT's signal that is received at the PR, and let γ_s denote the ST's signal SINR that is received at the SR.

Given the concurrent transmissions between the different IoT devices, γ_p and γ_s can be expressed as

$$\begin{aligned} \gamma_p &= \frac{P_p g_{pp} + \alpha P_s g_{sp}}{(1-\alpha) P_s g_{sp} + P_a g_{ap} + \sigma_p^2}. \\ \gamma_s &= \frac{(1-\alpha) P_s g_{ss}}{P_p g_{ps} + P_a g_{as} + \sigma_s^2}. \end{aligned} \tag{1}$$

For the case of Rayleigh fading in the channel, the cumulative distribution function (CDF) of g_{pp} can be written as

$$F_{g_{pp}}(x) = \left(1 - \exp\left(-\frac{x}{\lambda_{pp}}\right)\right) u(x) \tag{2}$$

where $u(\cdot)$ denotes the unit step function. Similar formulas can be found for the other channel gains in this environment.

The expression for γ_p can be expanded into $\gamma_p = \gamma_{p_1} + \gamma_{p_2}$, where

$$\begin{aligned} \gamma_{p_1} &= \frac{P_p g_{pp}}{(1-\alpha) P_s g_{sp} + P_a g_{ap} + \sigma_p^2} \\ \gamma_{p_2} &= \frac{\alpha P_s g_{sp}}{(1-\alpha) P_s g_{sp} + P_a g_{ap} + \sigma_p^2}. \end{aligned} \tag{3}$$

Further, to ensure tractability in deriving the CDF expression for γ_p, consider the scenario in γ_{p_2} where $P_a g_{ap} + \sigma_p^2 \ll P_s g_{sp}$ (i.e., the secondary power received at the PR is considerably stronger compared to that of the adversary and noise powers). In this case, the expression for γ_{p_2} can be further simplified to

$$\begin{aligned} \gamma_{p_2} &= \frac{\alpha}{1-\alpha + \frac{P_a g_{ap} + \sigma_p^2}{P_s g_{sp}}} \\ &\approx \frac{\alpha}{1-\alpha}. \end{aligned} \tag{4}$$

For this case, we can approximate γ_p as

$$\gamma_p \approx \gamma_{p_1} + \frac{\alpha}{1-\alpha}. \tag{5}$$

The distribution function of γ_{p_1} can be written as

$$F_{p_1}(x) = 1 - \exp\left(-\frac{\sigma_p^2}{\lambda_{pp} P_p} x\right) \frac{1}{1 + (1-\alpha)\frac{\lambda_{sp} P_s}{\lambda_{pp} P_p} x} \frac{1}{1 + \frac{\lambda_{ap} P_a}{\lambda_{pp} P_p} x}. \tag{6}$$

Following the results of (5) and (6), the CDF of γ_p is calculated using

$$F_p(x) = 1 - \frac{\exp\left(-\gamma_{np}\left(x - \frac{\alpha}{1-\alpha}\right)\right)}{\left(1 + (1-\alpha)\gamma_{sp}\left(x - \frac{\alpha}{1-\alpha}\right)\right)\left(1 + \gamma_{ap}\left(x - \frac{\alpha}{1-\alpha}\right)\right)} \tag{7}$$

where $\gamma_{np} = \frac{\sigma_p^2}{\lambda_{pp} P_p}$, $\gamma_{sp} = \frac{\lambda_{sp} P_s}{\lambda_{pp} P_p}$, and $\gamma_{ap} = \frac{\lambda_{ap} P_a}{\lambda_{pp} P_p}$. Let ρ_p denote the average outage probability of the received primary IoT signal at the PR; thus, ρ_p can be expressed as

$$\begin{aligned} \rho_p &= \mathbb{P}\{\log_2(1+\gamma_p) \leq R_p\} \\ &= \mathbb{P}\{\gamma_p \leq \theta_p\} \\ &= F_p(\theta_p) \\ &= 1 - \frac{\exp\left(-(\theta_p - \frac{\alpha}{1-\alpha})\gamma_{np}\right)}{\left(1 + (1-\alpha)(\theta_p - \frac{\alpha}{1-\alpha})\gamma_{sp}\right)\left(1 + (\theta_p - \frac{\alpha}{1-\alpha})\gamma_{ap}\right)} \end{aligned} \tag{8}$$

where $\mathbb{P}\{\cdot\}$ is the probability operator and $\theta_p = 2^{R_p} - 1$.

Similarly, the CDF of the SINR of ST's signal at its intended receiver SR (i.e., γ_s) can be expressed as

$$F_s(x) = 1 - \frac{\exp\left(-\gamma_{ns}\frac{x}{1-\alpha}\right)}{(1+\gamma_{ps}\frac{x}{1-\alpha})(1+\gamma_{as}\frac{x}{1-\alpha})} \tag{9}$$

where $\gamma_{ns} = \frac{\sigma_s^2}{\lambda_{ss}P_s}$, $\gamma_{ps} = \frac{\lambda_{ps}P_p}{\lambda_{ss}P_s}$, and $\gamma_{as} = \frac{\lambda_{as}P_a}{\lambda_{ss}P_s}$. Then, the average outage probability of ST's signal received at its intended receiver unit is found from

$$\rho_s \quad = 1 - \frac{\exp\left(-\frac{\theta_s}{1-\alpha}\gamma_{ns}\right)}{(1+\frac{\theta_s}{1-\alpha}\gamma_{ps})(1+\frac{\theta_s}{1-\alpha}\gamma_{as})} \tag{10}$$

where $\theta_s = 2^{R_s} - 1$.

The development above shows that the F_p moves to the right as α increases, as increasing the value of α leads to increasing the $\frac{\alpha}{1-\alpha}$ term in the CDF formula in Equation (7), leading to a shift to the right. Furthermore, the secondary CDF formula in (9) explains the impact of varying the cooperation factor on the F_s. In addition, when α increases, the primary outage probability decreases while the secondary IoT device's outage probability increases as indicated in Equations (8) and (10).

3.3. Transmission Strategy

Let N_s represent the number of secondary devices in the IoT environment. Suppose that ζ_p and ζ_s are the outage levels that the primary IoT device (i.e., PT) and the secondary IoT devices (i.e., ST) can tolerate, respectively. In practice, we have $0 < \zeta_p \ll \zeta_s < 1$. To mitigate the negative results of the interference attack on the PR, one secondary device is chosen from the pool of N_s IoT devices to cooperate with the PT. To enable cooperation with the PT and to simultaneously transmit its own data, the selected secondary IoT device needs to utilize a cooperation factor $\alpha \leq \alpha_{\max}$ that ensures that the following constraints are satisfied:

$$\begin{aligned} \rho_p &\leq \zeta_p \\ \rho_s &\leq \zeta_s. \end{aligned} \tag{11}$$

This formula allows the PT and ST to cooperate to mitigate the impact of the interference attack caused by the AT by limiting the PT's signal average outage probability to a level of ζ_p. This ensures that the PT maintains a certain level of information availability. Simultaneously, the formulation also provides the ST with an opportunity to communicate over the wireless channel while guaranteeing a limited outage probability ζ_s for the ST. This approach offers a balance between ensuring information availability for the PT and enabling limited communication for the ST in the presence of interference.

Consider the case of fixed P_s and α values. Let $A_1 = \frac{\exp\left(-(\theta_p - \frac{\alpha}{1-\alpha})\gamma_{np}\right)}{1+(\theta_p - \frac{\alpha}{1-\alpha})\gamma_{ap}}$ and $B_1 = (1-\alpha)(\theta_p - \frac{\alpha}{1-\alpha})$ in (8); then, the value of ρ_p can be expressed as

$$\rho_p = 1 - \frac{A_1}{1 + B_1\gamma_{sp}}. \tag{12}$$

Following the transmission constrains in (11), the limit on γ_{sp} is rephrased as

$$\gamma_{sp} \leq \frac{A_1 - 1 + \zeta_p}{(1-\zeta_p)B_1}. \tag{13}$$

Similarly, let $A_2 = \frac{\exp\left(-\frac{\theta_s}{1-\alpha}\gamma_{ns}\right)}{1+\frac{\theta_s}{1-\alpha}\gamma_{as}}$ and $B_2 = \frac{\theta_s}{1-\alpha}$ in (10); the value of ρ_s becomes

$$\rho_s = 1 - \frac{A_2}{1 + B_2\gamma_{ps}}. \tag{14}$$

Using the constraint on ρ_s in (11) and the development in (14), γ_{ps} is limited as

$$\gamma_{ps} \leq \frac{A_2 - 1 + \zeta_s}{(1 - \zeta_s)B_2}. \tag{15}$$

Recall that $\gamma_{sp} = \frac{\lambda_{sp}P_s}{\lambda_{pp}P_p}$ and $\gamma_{ps} = \frac{\lambda_{ps}P_p}{\lambda_{ss}P_s}$; then, the secondary IoT device has to satisfy the following constraints on the transmission power:

$$\begin{aligned} P_s &\leq \frac{A_1 - 1 + \zeta_p}{1 - \zeta_p} \frac{\lambda_{pp}}{\lambda_{sp}} \frac{P_p}{B_1} \\ P_s &\geq \frac{1 - \zeta_s}{A_2 - 1 + \zeta_s} \frac{\lambda_{ps}}{\lambda_{ss}} B_2 P_p. \end{aligned} \tag{16}$$

The cooperative transmission strategy proposed in this work to satisfy the PT's information availability requirements is illustrated in Algorithm 1. In the proposed transmission strategy, each secondary IoT device has its own constraints and environment settings, including parameters such as ζ_s, $\alpha_{\max}$, λ_{ss}, λ_{sp}, R_s, P_s, and others. The proposed algorithm verifies each candidate ST in a round-robin fashion to determine if it satisfies the transmission criteria outlined in (11). The algorithm begins by collecting and estimating the communication environment setting parameters, including the number of secondary IoT devices, channel strengths between the devices, noise levels, transmission rates and powers, and outage probability requirements. Each secondary IoT device is then verified to determine if it satisfies the proposed transmission criteria in (11).

Algorithm 1: Transmission Strategy for Interference Attacks Defense

```
Determine: ζ_p.
Collect: P_p, P_a, R_p, σ_p^2, σ_s^2.
Estimate: λ_pp, λ_ps, λ_ap, λ_as.
Determine: N_s.
while TRUE do
    if PT has no more data to transmit then
        Break.
    end if
    Initialize: n ← 1.
    while n ≤ N_s do
        Determine: ST_n.
        Determine: P_s, R_s, λ_ss, λ_sp of ST_n.
        Determine: ζ_s, α_max.
        Calculate: S_α ← {0 < α ≤ α_max} that satisfies outage requirements.
        if S_α ≠ [] then
            Assign: ST ← ST_n.
            Assign: α ← max(S_α).
            while TRUE do
                Access: ST uses αP_s for PT's signal and (1 − α)P_s for its signal.
                if ST has no more data to transmit then
                    Break.
                end if
            end while
        end if
        n ← n + 1.
    end while
end while
```

During each transmission interval, the scheduled secondary IoT device retransmits the primary signal with a transmission power of αP_s while also communicating its own signal with a transmission power of $(1 - \alpha)P_s$ using the shared channel. Then, data transmission by the ST alters the SINR value of the PT's signal that is received at the PR. However, by ensuring that the ST's transmission satisfies the constraints in (11), the average outage probability of the PT remains below the maximum threshold of ζ_p, and the ST experiences an average outage probability less than its limit of ζ_s. Even though there is an interference attack by the AT, the information availability constraint is fulfilled for

the primary device due to the cooperative secondary communication. Simultaneously, the cooperating secondary device is granted an opportunity to communicate over the shared wireless channel, achieving a less stringent outage probability constraint.

4. PLS for Eavesdropping Attacks Defense

The same principles can be employed to devise a PLS collaborative approach to enhance confidentiality against eavesdropping. In this case, we consider a setup with several IoT devices communicating their sensor measurements using a wireless communication channel. A set of the IoT devices, termed as primary devices, require higher signal quality guarantees at the receiver compared with other secondary IoT devices, which have lower transmission priority. Again, the primary and secondary devices may use different receiving units. Additionally, there is an illegitimate device, referred to as the eavesdropper, attempting to decode the primary device's transmission. We develop a coordinated transmission strategy by secondary IoT devices to ensure the information confidentiality of the primary device's signal in the presence of the eavesdropper.

When secondary transmissions occur, they introduce interference to the communication system, which can be detected by both the PR and the eavesdropper EVE. Also, primary transmissions will cause interference at the SR. Using a spectrum-sharing communication paradigm, secondary devices transmit with the primary device simultaneously. The simultaneous transmission occurs while ensuring a minimum quality level of the received primary signal, measured by satisfying an average primary outage probability constraint. Further, the simultaneous transmission of the signals adds extra interference to the received signal at the EVE, thus making it more challenging for the EVE to decode the primary signal. This approach helps the primary IoT device achieve a confidentiality level. The PT utilizes the ST secondary transmission to inflict a signal outage at the EVE, again preventing the EVE from decoding the PT's signal and thus ensuring confidentiality in its transmission.

This innovative transmission scheme enables IoT devices to communicate wirelessly while strategically inducing channel outages to prevent eavesdroppers from decoding the transmitted signals. An algorithmic transmission strategy that enables IoT devices, threatened by an eavesdropper, is developed to collaborate and cause signal outages, thus reducing the eavesdropper's ability to decode the signal of interest. This strategy leverages a spectrum-sharing communication model to enhance information confidentiality for IoT devices. By strategically inducing signal outages on the eavesdropper, the IoT devices ensure that sensitive information remains protected during wireless communication.

4.1. System Model

The wireless communication setup consists of a spectrum-sharing system as shown in Figure 3. This system depicts a primary transmitter communicating with a primary receiver unit using a wireless channel. There also exist multiple secondary transmitters aiming to communicate with another secondary receiver unit. The PR and SR IoT devices can simultaneously transmit their data wirelessly. The threat model considers an adversary, referred to as an EVE, attempting to eavesdrop on data transmitted by the PT. Let the PR transmit at a rate of R_p with a power of P_p; both are assumed to remain constant during the communication period. During every transmission round, a secondary IoT transmitter is chosen to start transmitting with a power of P_s over the wireless channel. At the primary receiver, the noise is assumed to be AWGN with a mean of zero and σ_p^2 variance. Also, we assume that the eavesdropper EVE and SR have AWGN with respective variances of σ_e^2 and σ_s^2.

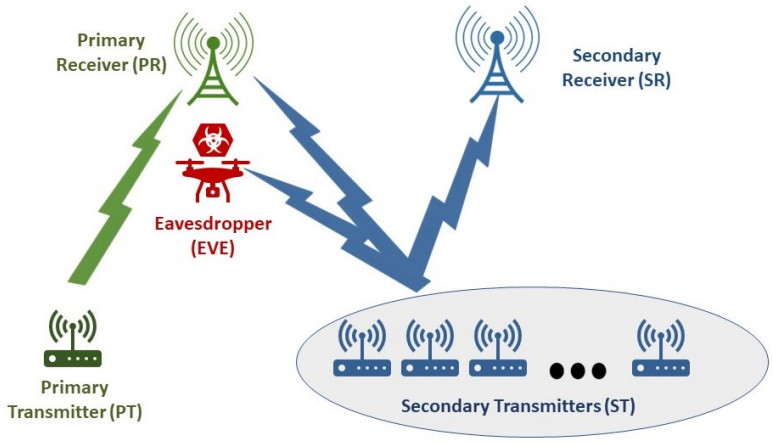

Figure 3. Eavesdropping attacks problem setup.

Between the two IoT devices and the receiver units, the wireless channels are modeled as i.i.d. block-fading channels with Rayleigh distribution. Figure 4 illustrates this setup, where the channel power gains between the PT and PR, SR, and EVE are defined as g_{pp}, g_{ps}, and g_{pe}, with corresponding respective averages of λ_{pp}, λ_{ps}, and λ_{pe}. Moreover, channel power gains between the ST and PR, SR, and EVE are defined as g_{sp}, g_{ss}, and g_{se}, with respective averages of λ_{sp}, λ_{ss}, and λ_{se}. Here, the λ's are different real and positive values that reflect relevant communication environment characteristics.

The cumulative distribution function (CDF) of g_{pp} can be mathematically described as

$$F_{g_{pp}}(x) = \left(1 - \exp\left(-\frac{x}{\lambda_{pp}}\right)\right) u(x). \tag{17}$$

The CDF mathematical model for other channel power gains such as g_{ps} and g_{pe} will be similar:

$$\begin{aligned} F_{g_{ps}}(x) &= \left(1 - \exp\left(-\tfrac{x}{\lambda_{ps}}\right)\right) u(x) \\ F_{g_{pe}}(x) &= \left(1 - \exp\left(-\tfrac{x}{\lambda_{pe}}\right)\right) u(x). \end{aligned} \tag{18}$$

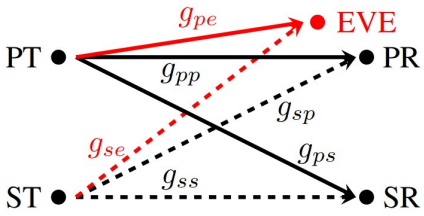

Figure 4. Eavesdropping attacks problem model.

4.2. Cooperation Model

Let γ_e and γ_p denote the SINR of the PT's signal at the EVE and at the PR, respectively, and let the SINR of the ST's signal at its own receiver unit (i.e., SR) be termed as γ_s. Then, with concurrent transmissions from the primary and secondary, the previous SINR values can be expressed as

$$\begin{aligned} \gamma_p &= \frac{g_{pp}P_p}{g_{sp}P_s + \sigma_p^2}. \\ \gamma_e &= \frac{g_{pe}P_p}{g_{se}P_s + \sigma_e^2}. \\ \gamma_s &= \frac{g_{ss}P_s}{g_{ps}P_p + \sigma_s^2}. \end{aligned} \tag{19}$$

Further, the CDF cof γ_p an be calculated using

$$\begin{aligned} F_p(x) &= \mathbb{P}\{\gamma_p \leq x\} \\ &= \mathbb{P}\{\tfrac{g_{pp}\ P_p/\sigma_p^2}{g_{sp}\ P_s/\sigma_p^2+1} \leq x\} \\ &= \mathbb{P}\{g_{pp} \leq \tfrac{x}{P_p/\sigma_p^2}(g_{sp}\ P_s/\sigma_p^2+1)\} \\ &= \int_0^\infty \left(1-\exp\left(-\tfrac{x(yP_s/\sigma_p^2+1)}{\lambda_{pp}P_p/\sigma_p^2}\right)\right)\tfrac{\exp\left(-\frac{y}{\lambda_{sp}}\right)}{\lambda_{sp}}\mathrm{d}y. \end{aligned} \tag{20}$$

This integration is simplified as

$$F_p(x) = \left(1-\frac{\exp\left(-\frac{x}{\lambda_{pp}P_p/\sigma_p^2}\right)}{1+\frac{\lambda_{sp}}{\lambda_{pp}}\frac{P_s}{P_p}x}\right)u(x). \tag{21}$$

Following a similar derivation process for γ_e CDF results in

$$F_e(x) = \left(1-\frac{\exp\left(-\frac{x}{\lambda_{pe}P_p/\sigma_e^2}\right)}{1+\frac{\lambda_{se}}{\lambda_{pe}}\frac{P_s}{P_p}x}\right)u(x). \tag{22}$$

An outage in the wireless communication channel happens when the transmitted data rate exceeds the capacity of the channel. Hence, the outage probability of the PT's transmission when measured at the PR can be expressed using $\rho_p = \mathbb{P}\{\log_2(1+\gamma_p) \leq R_p\} = \mathbb{P}\{\gamma_p \leq 2^{R_p}-1\}$. With (21), this leads to an outage probability of the PT as

$$\rho_p = 1-\frac{\exp\left(-\frac{2^{R_p}-1}{\lambda_{pp}P_p/\sigma_p^2}\right)}{1+\frac{\lambda_{sp}}{\lambda_{pp}}\frac{P_s}{P_p}(2^{R_p}-1)}. \tag{23}$$

Following a similar derivation, the average channel outage probability of the EVE is expressed as $\rho_e = \mathbb{P}\{\log_2(1+\gamma_e) \leq R_p\}$. With the results in (22), the outage probability is found to be

$$\rho_e = 1-\frac{\exp\left(-\frac{2^{R_p}-1}{\lambda_{pe}P_p/\sigma_e^2}\right)}{1+\frac{\lambda_{se}}{\lambda_{pe}}\frac{P_s}{P_p}(2^{R_p}-1)}. \tag{24}$$

In a spectrum-sharing communication system, a secondary transmission could be controlled by limiting the additional interference that is received at the primary receiver unit. In the described setup, the outage probability of the primary signal at the PR is limited with a maximum value of ζ_p. This limiting helps to account for the secondary interference such that $\rho_p \leq \zeta_p$. Hence, the transmission power of the ST is limited to

$$P_s \leq \frac{\exp\left(-\frac{2^{R_p}-1}{\lambda_{pp}P_p/\sigma_p^2}\right)+\zeta_p-1}{\frac{\lambda_{sp}}{\lambda_{pp}}\frac{2^{R_p}-1}{P_p}(1-\zeta_p)}. \tag{25}$$

Further, the secondary transmission is employed to control the lower limit of the average outage probability of the EVE as $\rho_e \geq \zeta_e$. Here, $\zeta_e \gg \zeta_p$, which consequently limits the transmission power of the secondary as

$$P_s \geq \frac{\exp\left(-\frac{2^{R_p}-1}{\lambda_{pe}P_p/\sigma_e^2}\right)+\zeta_e-1}{\frac{\lambda_{se}}{\lambda_{pe}}\frac{2^{R_p}-1}{P_p}(1-\zeta_e)}. \tag{26}$$

Thus, a level of confidentiality of the PT's signal at the EVE can be achieved by requiring the transmission power of the secondary to satisfy (25) and (26). By satisfying (25), the ST avoids causing excessive channel outage at the primary receiver, and by satisfying (26), the ST causes more outages at the EVE. The PT's objective is to transmit its data to the PR while hindering the EVE's ability to decode the transmitted information. Using the proposed strategy, the PT allows the ST to transmit data over the wireless channel, causing a secondary interference that will results in an additional outage at the PR and EVE. The secondary transmission is controlled such that it causes a lower-limit outage of ζ_e at the EVE and an upper-limit outage of ζ_p at the PR.

4.3. Transmission Strategy

To establish the base case before developing the cooperative transmission strategy, consider the case with no secondary transmission (i.e., $P_s = 0$). Hence,

$$\begin{aligned} \gamma_{p_0} &= \tfrac{g_{pp}P_p}{\sigma_p^2} \\ \gamma_{e_0} &= \tfrac{g_{pe}P_p}{\sigma_e^2}. \end{aligned} \tag{27}$$

The CDF expressions of γ_{p_0} and γ_{e_0} will then simplify to

$$\begin{aligned} F_{p_0}(x) &= \left(1-\exp\left(-\tfrac{x}{\lambda_{pp}P_p/\sigma_p^2}\right)\right)u(x). \\ F_{e_0}(x) &= \left(1-\exp\left(-\tfrac{x}{\lambda_{pe}P_p/\sigma_e^2}\right)\right)u(x). \end{aligned} \tag{28}$$

Then, the outage probability can be evaluated as

$$\begin{aligned} \rho_{p_0} &= 1-\exp\left(-\tfrac{2^{R_p}-1}{\lambda_{pp}P_p/\sigma_p^2}\right). \\ \rho_{e_0} &= 1-\exp\left(-\tfrac{2^{R_p}-1}{\lambda_{pe}P_p/\sigma_e^2}\right). \end{aligned} \tag{29}$$

Note here that the symbol subscript of zero in (27)–(29) signifies that $P_s = 0$ and results in base case values.

Let P_{s_L} and P_{s_U} designate the lower and upper limits on the secondary transmission power. Then, combining (25), (26), and (29) will result in a set of requirements for transmission power expressed as

$$\begin{aligned} P_s &\leq P_{s_U} = \tfrac{\zeta_p-\rho_{p_0}}{1-\zeta_p}\tfrac{\lambda_{pp}}{\lambda_{sp}}\tfrac{P_p}{2^{R_p}-1}. \\ P_s &\geq P_{s_L} = \tfrac{\zeta_e-\rho_{e_0}}{1-\zeta_e}\tfrac{\lambda_{pe}}{\lambda_{se}}\tfrac{P_p}{2^{R_p}-1}. \end{aligned} \tag{30}$$

To ensure concurrent transmission over the wireless channel, any secondary transmitter must operate within a specific power range, defined as $P_{s_L} \leq P_s \leq P_{s_U}$. This constraint guarantees that the EVE experiences an outage probability exceeding the minimum requirement (ζ_e) while simultaneously ensuring that the primary receiver's outage probability remains below the maximum threshold (ζ_p), where $\zeta_p \ll \zeta_e$.

The communication system is assumed to be composed of N_s available secondary transmitters, each characterized by its unique maximum transmit power ($P_{s_{\max}}$) and channel strength. A round-robin approach is employed to verify if each secondary transmitter can meet the condition in (30). Upon satisfying this criterion, a secondary transmitter is permitted to transmit using a power level of $P_s = \min(P_{s_U}, P_{s_{\max}})$. This carefully selected transmission power ensures that the ST adheres to the outage probability requirements for both the EVE and PR.

The transmission strategy depicted in Algorithm 2 outlines the transmission strategy designed to meet the confidentiality constraint. It begins by gathering system parameters, including outage requirements, data rates, noise powers, channel strengths, and the number of potential secondary transmitters. Using a round-robin approach, each secondary transmitter is evaluated to determine if it meets the proposed transmission criteria. If a secondary transmitter satisfies these criteria, it is selected to transmit its data over the shared channel, thereby introducing interference and additional outage to both the EVE and PT. Given that (30) is satisfied for the selected secondary transmitter, the outage probability for the PT will remain within the acceptable limit (ζ_p), while the EVE will experience an outage probability of no less than ζ_e. As a result, the confidentiality metric is upheld.

Algorithm 2: Transmission Strategy for Eavesdropping Attacks Defense

```
Determine: ζ_p, ζ_e.
Collect: P_p, R_p, σ_p^2, σ_e^2, λ_pp, λ_pe.
Calculate: ρ_{p_0}, ρ_{e_0}.
Determine: N_s.
while TRUE do
    if PT has no more data to transmit then
        Break Loop.
    end if
    Initialize: n ← 1.
    while n ≤ N_s do
        Determine: ST_n.
        Determine: λ_sp, λ_se of ST_n.
        Find: P_{s_max}.
        Calculate: P_{s_L}, P_{s_U}.
        if P_{s_L} ≤ P_{s_U} AND P_{s_L} ≤ P_{s_max} then
            Assign: ST ← ST_n.
            Assign: P_s ← min(P_{s_U}, P_{s_max}).
            while TRUE do
                Access: ST transmits data with P_s.
                if ST has no more data to transmit then
                    Break.
                end if
            end while
        end if
        n ← n + 1
    end while
end while
```

Consider the case where the ST communicates over the channel with a rate of R_s. Given the value of γ_s in (19), and following a similar development to that of the PT, the CDF of γ_s, termed as F_s, is calculated using

$$\begin{aligned} F_s(x) &= \mathbb{P}\{\gamma_s \leq x\} \\ &= \mathbb{P}\{\tfrac{g_{ss}P_s}{g_{ps}P_p+\sigma_s^2} \leq x\} \\ &= \mathbb{P}\{g_{ss} \leq \tfrac{x}{P_s/\sigma_s^2}(g_{ps}\, P_p/\sigma_s^2 + 1)\} \\ &= \int_0^\infty \left(1 - \exp\left(-\tfrac{x(yP_p/\sigma_s^2+1)}{\lambda_{ss}P_s/\sigma_s^2}\right)\right) \tfrac{\exp\left(-\frac{y}{\lambda_{ps}}\right)}{\lambda_{ps}} \mathrm{d}y. \end{aligned} \tag{31}$$

This leads to F_s being expressed as

$$F_s(x) = \left(1 - \frac{\exp\left(-\frac{x}{\lambda_{ss} P_s/\sigma_s^2}\right)}{1 + \frac{\lambda_{ps}}{\lambda_{ss}} \frac{P_p}{P_s} x}\right) u(x). \tag{32}$$

Next, for a transmission rate of R_s, the outage probability of the ST's transmission at the SR is calculated using $\rho_s = \mathbb{P}\{\gamma_s \leq 2^{R_s} - 1\}$; then, using F_s from (32), the outage probability of the ST becomes

$$\rho_s = 1 - \frac{\exp\left(-\frac{2^{R_s}-1}{\lambda_{ss} P_s/\sigma_s^2}\right)}{1 + \frac{\lambda_{ps}}{\lambda_{ss}} \frac{P_p}{P_s} (2^{R_s} - 1)}. \tag{33}$$

Recall that the ST has to satisfy the outage probability constraints on the PR and EVE; this means that the ST has upper and lower transmission power limits of P_{s_U} and P_{s_L}, respectively, as indicated in (30). As the ST will try to maximize its received signal level at the SR, $P_s = \min(P_{s_U}, P_{s_{\max}})$ as mentioned previously. Given these transmission limits on P_s, the outage probability of the ST will be bounded as $\rho_{s_L} \leq \rho_s \leq \rho_{s_U}$, where

$$\begin{aligned} \rho_{s_L} &= 1 - \frac{\exp\left(-\frac{2^{R_s}-1}{\lambda_{ss} P_{s_U}/\sigma_s^2}\right)}{1 + \frac{\lambda_{ps}}{\lambda_{ss}} \frac{P_p}{P_{s_U}} (2^{R_s} - 1)}. \\ \rho_{s_U} &= 1 - \frac{\exp\left(-\frac{2^{R_s}-1}{\lambda_{ss} P_{s_L}/\sigma_s^2}\right)}{1 + \frac{\lambda_{ps}}{\lambda_{ss}} \frac{P_p}{P_{s_L}} (2^{R_s} - 1)}. \end{aligned} \tag{34}$$

5. Results and Discussion

5.1. PLS for Interference Attacks Defense

This section assesses the effectiveness of the proposed PLS cooperative transmission scheme outlined in Algorithm 1 for interference attacks defense by demonstrating the rate of finding appropriate secondary devices that satisfy the constraints specified in (11) under different system settings. The following numerical values are used in this section: $\alpha_{\max} = 0.49$, $\lambda_{as} = 0.75$, $\lambda_{ap} = 0.75$, $\lambda_{ss} = 1$, $\lambda_{sp} = 0.75$, $\lambda_{ps} = 0.75$, $\lambda_{pp} = 1$, $\sigma_s^2 = 0.1$, $\sigma_p^2 = 0.1$, $R_s = 0.5$, $R_p = 1$, $P_a = 5$, $P_s = 7.5$, and $P_p = 10$. Further, $\zeta_p = 0.05$ and $\zeta_s = 0.2$ are also used in Figures 5–8.

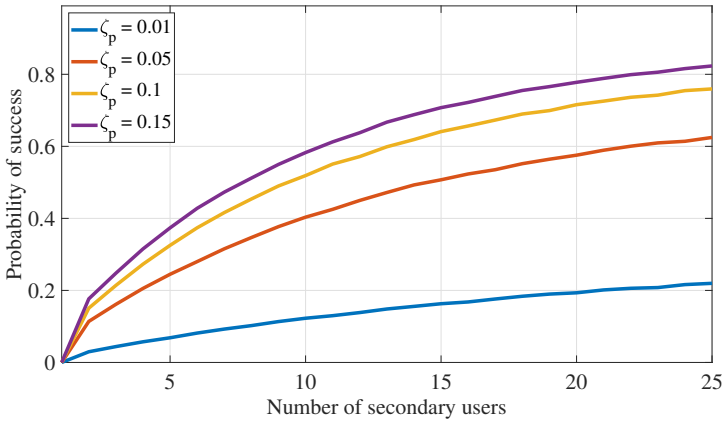

Figure 5. PLS for interference attack defense: impact of the outage constraints on the algorithm success probability (ζ_p).

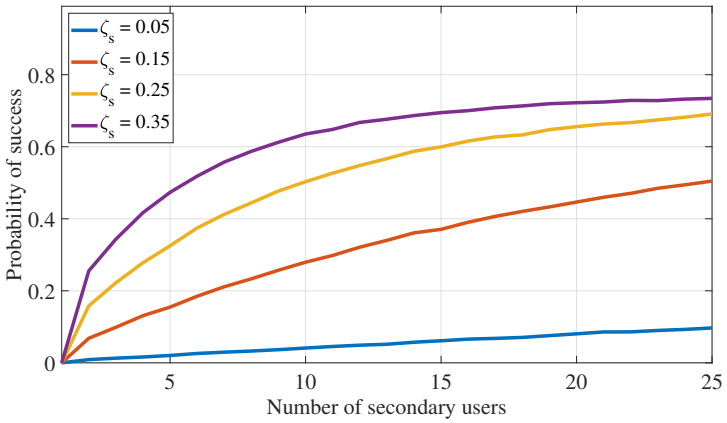

Figure 6. PLS for interference attack defense: impact of the outage constraints on the algorithm success probability (ζ_s).

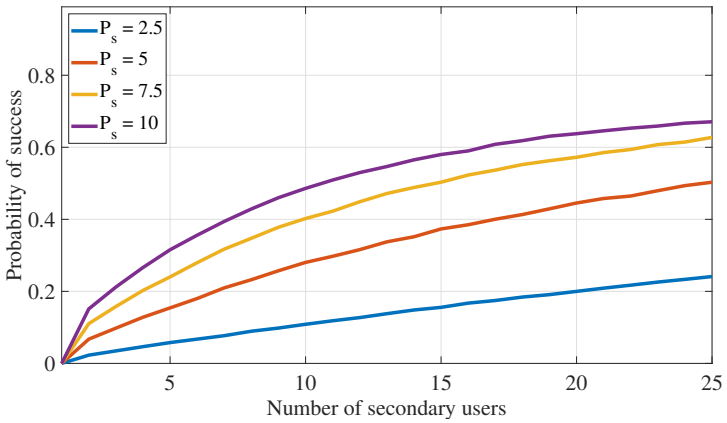

Figure 7. PLS for interference attack defense: impact of the secondary transmission power on the algorithm success probability.

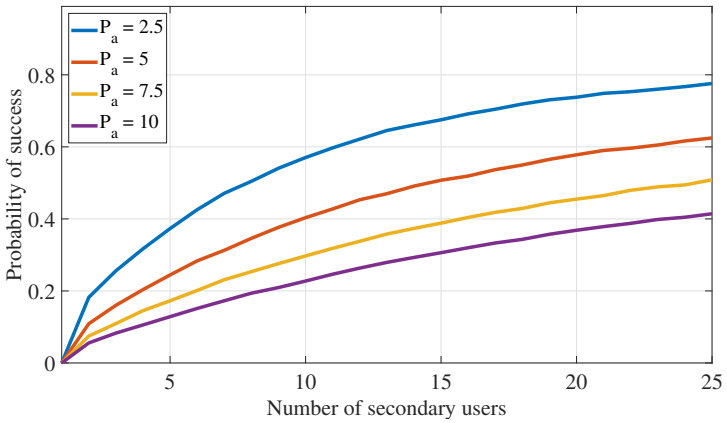

Figure 8. PLS for interference attack defense: impact of P_a on the algorithm success probability.

Recall that the success rate of the proposed transmission strategy can be measured using the probability of selecting appropriate secondary devices that satisfy the transmission constraints outlined in (11). Figures 5 and 6 investigate how the number of available secondary devices (N_s) impacts the success rate of the communication strategy in Algorithm 1. Here, Figure 5 shows that, with increasing the number of available secondary IoT devices (N_s), the proposed transmission algorithm has better chances of identifying a secondary device that satisfies the primary and secondary outage probability constraints of (11). Also, this figure confirms that as outage probability constraints (ζ_p or ζ_s) become more relaxed (i.e., increase), the proposed transmission algorithm has more chances of

identifying secondary IoT devices that satisfy the outage probability constraints of (11), leading the algorithm to achieve higher rates of success.

Finally, Figures 7 and 8 illustrate the impact of varying the amount of transmission power for the secondary user and the adversary, respectively, on the probability of finding a suitable ST that meets the transmission and interference constraints in (11). As expected, increasing available P_s enhances the algorithm's ability to find STs that satisfy the outage probability requirements. On the other hand, higher transmission power for the adversary reduces the algorithm's success rate.

5.2. PLS for Eavesdropping Attack Defense

This section evaluates the efficacy of the proposed PLS cooperative transmission algorithm, as illustrated in Figure 3, in defending against eavesdropping attacks. Through simulation results, we demonstrate that the transmission strategy presented in Algorithm 2 successfully achieves the target outage probability requirements for both the EVE and the primary receiver. The numerical analysis in this section focuses on the probability of identifying suitable secondary transmitters that satisfy the conditions specified in (30) under various system configurations. For the subsequent numerical results, we assume the following parameters: primary transmitter power $P_p = 1$, primary transmission rate $R_p = 1$, and noise power $\sigma^2 = 0.1$ at the PR, EVE, and SR. Also, let $\lambda_{sp} = 0.75$, $\lambda_{se} = 0.5$, $\lambda_{ss} = 1$, $\lambda_{pp} = 1$, $\lambda_{pe} = 0.5$, and $\lambda_{ps} = 0.75$.

Figure 9 examines how the number of available secondary transmitters affects the algorithm's success rate. In this analysis, the secondary transmission power is constrained between $P_{s_{\min}} = 0.75 \times P_p$ and $P_{s_{\max}} = 1.25 \times P_p$. The target outage probabilities are set at $\zeta_e = 0.8$ for the EVE and $\zeta_p = 0.2$ for the PR. As N_s increases, the likelihood of identifying a secondary transmitter that satisfies the conditions in (30) also rises. Additionally, higher primary transmission rates, combined with secondary interference, make it more challenging for the EVE to successfully decode the primary signal. This results in increased outages at the EVE and, consequently, a higher probability of finding suitable secondary transmitters.

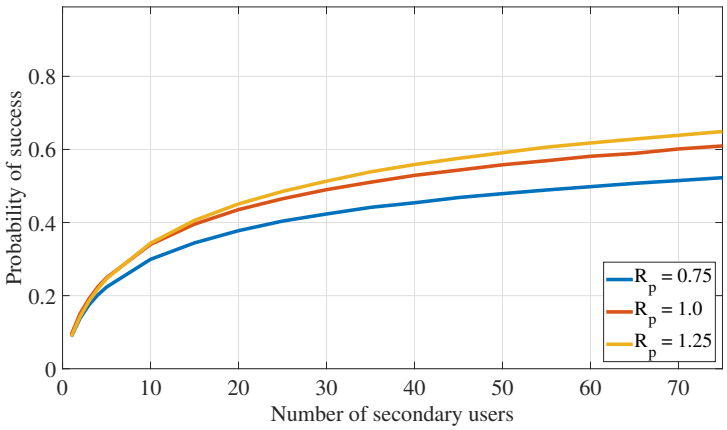

Figure 9. PLS for eavesdropping attack defense: impact of number of transmitters.

The impact of varying outage probability requirements at the EVE and the primary receiver is examined, with the number of secondary transmitters set to $N_s = 25$ and power limits of $P_{s_{\max}} = 1.25 \times P_p$ and $P_{s_{\min}} = 0.75 \times P_p$. The results show that relaxing the outage requirements, either by increasing the acceptable primary outage or reducing the EVE's outage probability, leads to higher success rates, as illustrated in Figure 10.

The impact of channel strength is investigated, revealing that an increase in λ_{sp} results in lower success rates due to more stringent transmission limits for the ST. Conversely, higher values of λ_{pp} improve success probability by allowing the ST to transmit at lower power levels. Similar trends are observed for the effects of increasing λ_{se} and λ_{pe} on the algorithm's success rate. These observations are illustrated in Figures 11 and 12.

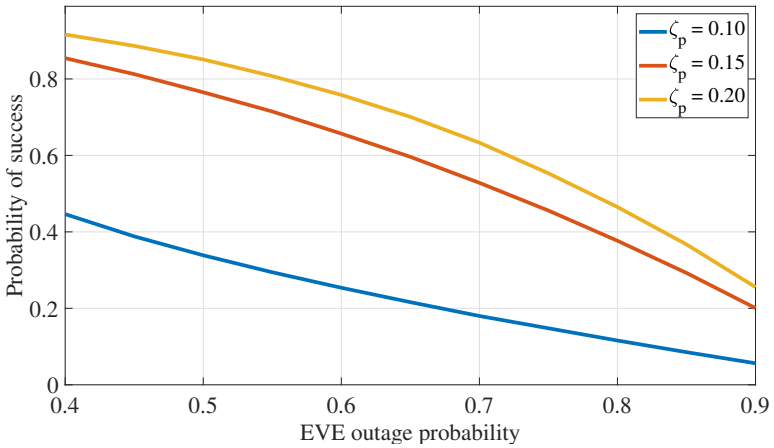

Figure 10. PLS for eavesdropping attack defense: impact of outage requirement.

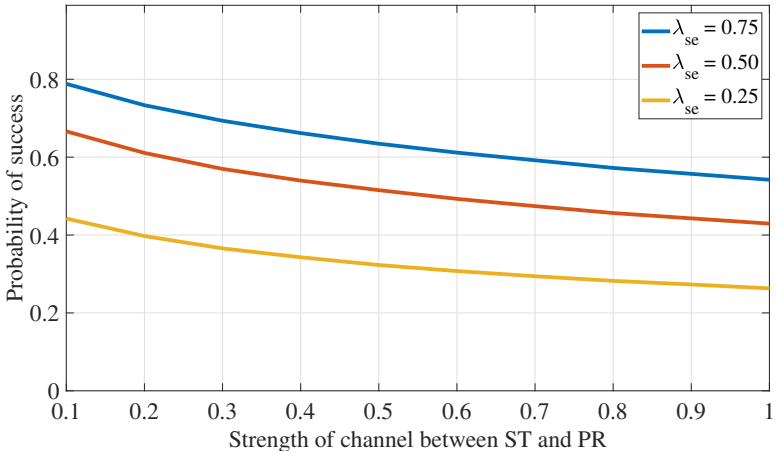

Figure 11. PLS for eavesdropping attack defense: impact of secondary channel strength.

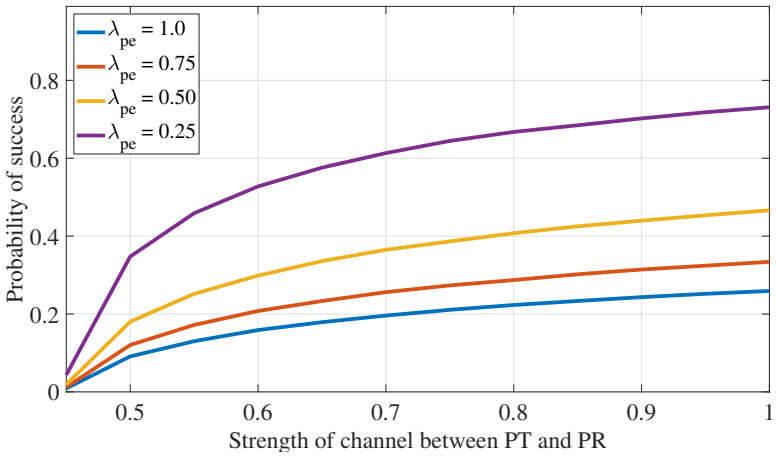

Figure 12. PLS for eavesdropping attack defense: impact of primary channel strength.

Figure 13 compares the simulated and theoretical values of the CDF of γ_p, where the values of $P_p = P_s = \lambda_{pp} = \lambda_{sp} = 1$ and $\sigma_p^2 = 0.1$ are used in calculating the theoretical value in (21) and simulating the environment. The figure confirms that the simulated CDF is very close to the theoretical one, with a very small gap for very low SINR values.

For the next three figures, consider a simulated communication environment similar to the one shown in Figure 4. Let $N_s = 100$ with a transmission rate of $R_s = 0.5$ bit/sec/Hz. The PT transmits at a rate of $R_p = 1$ bit/sec/Hz with $P_p = 1$ power unit. Similarly, $\sigma^2 = 0.01$ power unit at the PR, SR, and EVE. Let also $\lambda_{sp} = 0.5$, $\lambda_{se} = 0.75$, $\lambda_{ss} = 1$, $\lambda_{pp} = 1$, $\lambda_{pe} = 0.75$, and $\lambda_{ps} = 0.5$. Further, assume that $\zeta_p = 0.05$ as the maximum primary outage

requirement and $\zeta_e = 0.85$ as the minimum eavesdropper outage probability requirement. Let $P_{s_{\max}} = 10P_p$ and $P_{s_{\min}} = 0.95P_p$. For a representative simulated communication environment with 1000 trials, each has 100 block-fading periods.

Figure 14 illustrates the outage probabilities experienced at the PR, EVE, and SR (i.e., ρ_p, ρ_e, and ρ_s) following the implementation of the proposed coordinated transmission strategy in Algorithm 2, and Figure 15 displays the channel capacity of users in the IoT environment. As shown in Figure 14, the achieved outage probability at the PR and EVE are about 5% and 85%, respectively, as predicted by (30) and in Algorithm 2. In addition, the results of Figure 15 emphasize the diminished channel conditions that the eavesdropper experiences compared to the primary and secondary IoT devices.

In addition, the results of Figure 16 show the probability that the cooperative transmission strategy of Algorithm 2 is successful in finding users that help to mitigate the eavesdropping attack on the PT. The figure confirms our intuition that the transmission strategy is more likely to find suitable users that achieve the target outage probability requirements for both the EVE and PR while increasing the pool of available users to choose from.

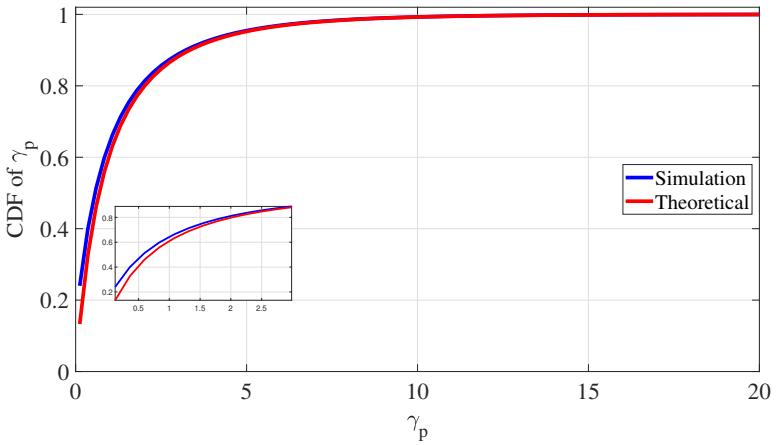

Figure 13. PLS for eavesdropping attack defense: simulated and theoretical CDF of γ_p.

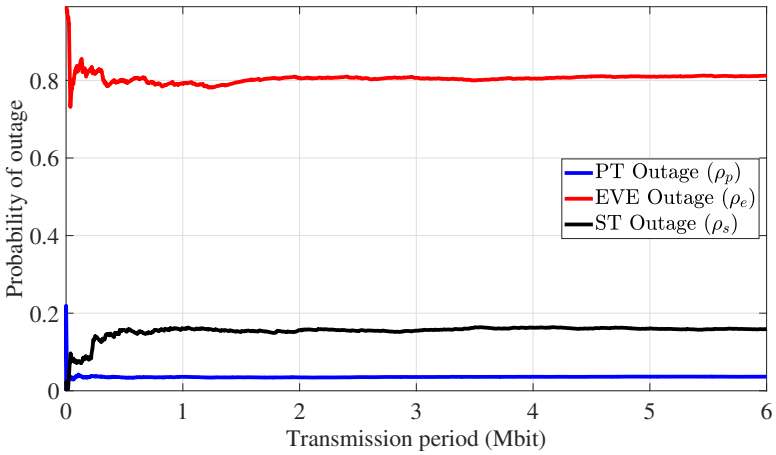

Figure 14. PLS for eavesdropping attack defense: moving average of outage probability over time.

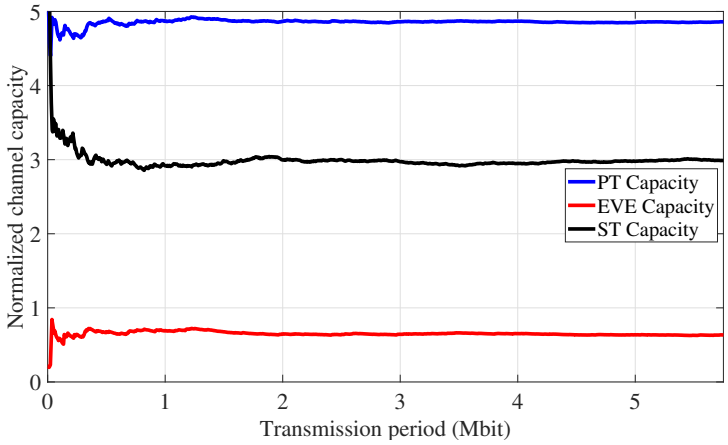

Figure 15. PLS for eavesdropping attack defense: moving average of channel capacity over time.

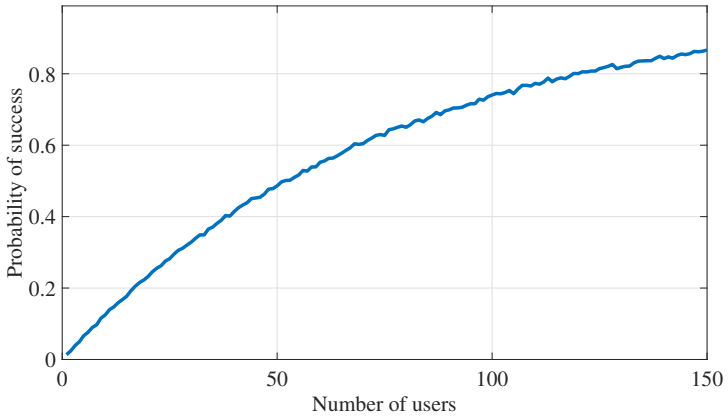

Figure 16. PLS for eavesdropping attack defense: algorithm's success rate versus number of users.

5.3. Discussions

General observations from the above numerical results include that there is a better chance of mitigating interference attacks with an increasing number of IoT devices; this result favors large-scale IoT environments. Further, relaxing the information availability constraints for the primary and/or secondary IoT devices (through having higher outage probability constraints) leads to better success rates in finding suitable STs that could counter the interference attack. Additionally, the algorithm has a better success rate with higher secondary transmission power and/or lower adversary interference power. The numerical results demonstrate the feasibility in using the proposed cooperative IoT transmission strategy in Algorithm 1 to combat interference attacks and maintain information availability. Also, the performance metrics and the practical advantages of using this strategy are supported by the analytical discussions in Section 4.3.

The proposed transmission strategy only relies on the knowledge of the channel gains between the IoT devices, receiver units, and the eavesdropper. Presented numerical results illustrate the proposed algorithm practicality and the capability of IoT devices to concurrently meet the desired signal quality and availability and confidentiality objectives. This approach demonstrates that, by leveraging spectrum-sharing and collaborative transmission strategies, IoT devices can effectively protect sensitive information while maintaining efficient communication performance in wireless environments.

While recent research on physical-layer security is advancing, the focus has primarily been on information-theoretic solutions, with practical implementations being less common. This work proposes algorithmic transmission strategies to achieve uplink IoT information integrity and confidentiality in the presence of adversaries. The proposed solution is tailored to IoT systems, considering the computational and energy limitations of IoT devices by restricting the number of retransmissions and necessary information for the

algorithmic transmission strategy. Moreover, the solution accommodates IoT environments by allocating transmission opportunities to available IoT devices based on their channel strengths. The approach also incorporates elements from spectrum-sharing systems to facilitate device cooperation and concurrent transmissions.

6. Conclusions

A cooperative IoT transmission strategy is presented in this article to enhance information security in IoT environments; specifically, this work focuses on ensuring IoT information availability during jamming interference attacks and ensuring IoT information confidentiality during eavesdropping attacks. This research contributes to tackling security challenges inherent in wirelessly connected IoT devices and emphasizes the importance of safeguarding information availability and confidentiality across diverse IoT applications and critical industrial processes.

The proposed PLS algorithm for interference attack defense facilitates cooperative communication among IoT devices by involving secondary devices, aiming to maintain the desired outage probability for the primary device and achieve a certain level of information availability. Through relaying the primary device's data, secondary devices actively contribute and help to meet the primary device's outage probability requirements. The numerical results presented in this article demonstrate the effectiveness of the proposed transmission strategy, particularly in large-scale IoT environments. The findings emphasize that, by applying the proposed solution, the IoT devices have the capability to attain specific levels of information security even when facing interference attacks. The proposed PLS algorithmic transmission strategy for eavesdropping attack defense employs secondary IoT devices to ensure the quality of IoT signals while deliberately causing channel outages that hinder eavesdroppers from decoding the IoT transmission effectively. Through this collaborative transmission strategy, eavesdroppers' capability to intercept and decipher sensitive IoT signals is significantly restricted.

Author Contributions: A.F. and E.H. contributed to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Statista Research Department. Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023, with Forecasts from 2024 to 2033. 2024. Available online: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 29 June 2024).
2. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
3. Gelgi, M.; Guan, Y.; Arunachala, S.; Samba Siva Rao, M.; Dragoni, N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors* **2024**, *24*, 3571. [CrossRef] [PubMed]
4. Husar, A. IoT Security: 5 Cyber-Attacks Caused by IoT Security Vulnerabilities. 2022. Available online: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities (accessed on 29 June 2024).
5. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 19–26. [CrossRef] [PubMed]
6. Wei, Z.; Masouros, C.; Liu, F.; Chatzinotas, S.; Ottersten, B. Energy-and cost-efficient physical layer security in the era of IoT: The role of interference. *IEEE Commun. Mag.* **2020**, *58*, 81–87. [CrossRef]
7. Line Larrivaud. State of Enterprise IoT Security in North America: Unmanaged and Unsecured; A Forrester Consulting Thought Leadership Paper Commissioned By Armis Inc. 2019. Available online: https://info.armis.com/rs/645-PDC-047/images/State-Of-Enterprise-IoT-Security-Unmanaged-And-Unsecured.pdf (accessed on 29 June 2024).
8. Alvi, A.N.; Ali, B.; Saleh, M.S.; Alkhathami, M.; Alsadie, D.; Alghamdi, B. Secure Computing for Fog-Enabled Industrial IoT. *Sensors* **2024**, *24*, 2098. [CrossRef] [PubMed]

9. Ahakonye, L.A.C.; Nwakanma, C.I.; Kim, D.S. Tides of Blockchain in IoT Cybersecurity. *Sensors* **2024**, *24*, 3111. [CrossRef] [PubMed]
10. Ullah, F.; Turab, A.; Ullah, S.; Cacciagrano, D.; Zhao, Y. Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory. *Sensors* **2024**, *24*, 4152. [CrossRef] [PubMed]
11. Rahaman, M.; Lin, C.Y.; Pappachan, P.; Gupta, B.B.; Hsu, C.H. Privacy-Centric AI and IoT Solutions for Smart Rural Farm Monitoring and Control. *Sensors* **2024**, *24*, 4157. [CrossRef] [PubMed]
12. Zhang, Y.; Tang, Y.; Li, C.; Zhang, H.; Ahmad, H. Post-Quantum Secure Identity-Based Signature Scheme with Lattice Assumption for Internet of Things Networks. *Sensors* **2024**, *24*, 4188. [CrossRef] [PubMed]
13. Hammad, E.; McLaren, C.; Leiden, J. Demystifying Cybersecurity Experiential Learning for Operational Technologies (OT) and Industrial Control Systems (ICS). In Proceedings of the 2024 ASEE-GSW, Canyon, TX, USA, 10–12 March 2024.
14. Al-Obaidi, K.M.; Hossain, M.; Alduais, N.A.; Al-Duais, H.S.; Omrany, H.; Ghaffarianhoseini, A. A review of using IoT for energy efficient buildings and cities: A built environment perspective. *Energies* **2022**, *15*, 5991. [CrossRef]
15. Oyewobi, S.S.; Djouani, K.; Kurien, A.M. A review of industrial wireless communications, challenges, and solutions: A cognitive radio approach. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e4055. [CrossRef]
16. Gulati, K.; Boddu, R.S.K.; Kapila, D.; Bangare, S.L.; Chandnani, N.; Saravanan, G. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today Proc.* **2022**, *51*, 161–165. [CrossRef]
17. Farraj, A. Switched-Diversity Approach for Cognitive Scheduling. *Wirel. Pers. Commun.* **2014**, *74*, 933–952. [CrossRef]
18. Dutta, A.; Hammad, E. 5G Security Challenges and Opportunities: A System Approach. In Proceedings of the IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 10–12 September 2020; pp. 109–114.
19. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the Mirai Botnet. In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August 2017; pp. 1093–1110.
20. Hammad, E.; Farraj, A. A Physical-Layer Security Approach for IoT Against Jamming Interference Attacks. In Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Virtual Event, 12–17 September 2021; pp. 1–6.
21. Farraj, A.; Hammad, E. A Game-Theoretic Approach for Uncoordinated Access to Cognitive Resources. In Proceedings of the IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Virtual Event, 12–17 September 2021; pp. 1–6.
22. Farraj, A.; Hammad, E. Impact of Quality of Service Constraints on the Performance of Spectrum Sharing Cognitive Users. *Wirel. Pers. Commun.* **2013**, *69*, 673–688. [CrossRef]
23. Ma, C.Y.; Rao, N.S.; Yau, D.K. A Game Theoretic Study of Attack and Defense in Cyber-Physical Systems. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, China, 10–15 April 2011; pp. 708–713.
24. Luo, Y.; Szidarovszky, F.; Al-Nashif, Y.; Hariri, S. Game Theory Based Network Security. *J. Inf. Secur.* **2010**, *1*, 41. [CrossRef]
25. Zhu, Q.; Başar, T. A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures. In Proceedings of the International conference on High Confidence Networked Systems, Beijing, China, 17–18 April 2012; pp. 41–46.
26. Chopra, R.; Murthy, C.R.; Annavajjala, R. Physical layer security in wireless sensor networks using distributed co-phasing. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2662–2675. [CrossRef]
27. Farris, I.; Taleb, T.; Khettab, Y.; Song, J. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 812–837. [CrossRef]
28. Varga, P.; Peto, J.; Franko, A.; Balla, D.; Haja, D.; Janky, F.; Soos, G.; Ficzere, D.; Maliosz, M.; Toka, L. 5G support for Industrial IoT Applications—Challenges, Solutions, and Research gaps. *Sensors* **2020**, *20*, 828. [CrossRef] [PubMed]
29. Sun, L.; Wan, L.; Liu, K.; Wang, X. Cooperative-evolution-based WPT resource allocation for large-scale cognitive industrial IoT. *IEEE Trans. Ind. Inf.* **2019**, *16*, 5401–5411. [CrossRef]
30. Li, B.; Fei, Z.; Zhou, C.; Zhang, Y. Physical-layer security in space information networks: A survey. *IEEE Internet Things J.* **2019**, *7*, 33–52. [CrossRef]
31. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
32. Zhou, X.; Song, L.; Zhang, Y. *Physical Layer Security in Wireless Communications*; CRC Press: Boca Raton, FL, USA, 2013.
33. Liu, Y.; Chen, H.H.; Wang, L. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Commun. Surv. Tutorials* **2016**, *19*, 347–376. [CrossRef]
34. Soni, A.; Upadhyay, R.; Jain, A. Internet of Things and wireless physical layer security: A survey. In *Computer Communication, Networking and Internet Security*; Springer: Singapore, 2017; pp. 115–123.
35. Rojas, P.; Alahmadi, S.; Bayoumi, M. Physical layer security for IoT communications—A survey. In Proceedings of the 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14 June–31 July 2021; pp. 95–100.
36. Pecorella, T.; Brilli, L.; Mucchi, L. The role of physical layer security in IoT: A novel perspective. *Information* **2016**, *7*, 49. [CrossRef]
37. Wang, D.; Bai, B.; Lei, K.; Zhao, W.; Yang, Y.; Han, Z. Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City. *IEEE Access* **2019**, *7*, 54508–54521. [CrossRef]
38. Zhang, N.; Fang, X.; Wang, Y.; Wu, S.; Wu, H.; Kar, D.; Zhang, H. Physical-Layer Authentication for Internet of Things via WFRFT-Based Gaussian Tag Embedding. *IEEE Internet Things J.* **2020**, *7*, 9001–9010. [CrossRef]

39. Wu, H.; Zhang, Y.; Shen, Y.; Jiang, X.; Taleb, T. Achieving Covertness and Secrecy: The Interplay between Detection and Eavesdropping Attacks. *IEEE Internet Things J.* **2024**, *11*, 3233–3249. [CrossRef]
40. Deng, Z.; Li, Q.; Zhang, Q.; Yang, L.; Qin, J. Beamforming Design for Physical Layer Security in a Two-Way Cognitive Radio IoT Network With SWIPT. *IEEE Internet Things J.* **2019**, *6*, 10786–10798. [CrossRef]
41. Chorti, A.; Perlaza, S.M.; Han, Z.; Poor, H.V. Physical Layer Security in Wireless Networks with Passive and Active Eavesdroppers. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 4868–4873.
42. Solaija, M.; Salman, H.; Arslan, H. Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks. *IEEE Open J. Veh. Technol.* **2022**, *3*, 321–343. [CrossRef]
43. Farraj, A.; Hammad, E. Performance of Primary Users in Spectrum Sharing Cognitive Radio Environment. *Wirel. Pers. Commun.* **2013**, *68*, 575–585. [CrossRef]