Secretory Performance Analysis of Wireless Powered Sensor Networks Under Saturation Nonlinear Energy Harvesting and Activation Threshold

Xiaohui Shang 1,2,*, Hao Yin 2, Yida Wang 1, Mu Li 3 and Yong Wang 1

1 College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China; dadawang333@sina.com (Y.W.); wangyong_85@126.com (Y.W.)
2 Institute of Systems Engineering, AMS, Beijing 100039, China; yinhao10201214@163.com
3 61618 Troops of PLA, Beijing 100094, China; lmson3690@sina.com
* Correspondence: shangxiaohui1214@126.com; Tel.: +86-1861-2309-006

Received: 7 February 2020; Accepted: 11 March 2020; Published: 14 March 2020

Abstract: In this paper, we investigate the impact of saturation nonlinear energy harvesting (EH) and activation threshold on the multiuser wireless powered sensor networks (WPSNs) from the physical layer security (PLS) perspective. In particular, for improving the secrecy performance, the generalized multiuser scheduling (GMS) scheme is exploited, in which the Kth strongest sensor is chosen based on the legitimate link. For evaluating the impact of various key parameters on the security of system, we obtain the exact closed-form expressions for secrecy outage probability (SOP) under linear EH (LEH), saturation nonlinear EH (SNEH) and saturation nonlinear EH with activation threshold (SNAT), respectively, and solve the maximization problem of secure energy efficiency (SEE). Simulation results demonstrate that: (1) the number of source sensors, the EH efficiency and the transmit power of power beacon (PB) all have positive impact on SOP, and the smaller generalized selection coefficient is advantageous for secrecy performance; (2) LEH is an ideal situation for SNEH when the saturation threshold is large enough and SNEH is a special situation for SNAT when the activation threshold is low enough; (3) the time-switching factor and the activation threshold both have an important impact on the secrecy performance, which are worth considering carefully.

Keywords: wireless powered sensor networks; nonlinear energy harvesting; activation threshold; generalized multiuser scheduling; secrecy outage probability; physical layer security

1. Introduction

The Internet of Things (IoT), as the intelligent infrastructure in the fifth-generation (5G) mobile communication networks, has been popularized and applied all over the world in recent years [1–3]. It plays a remarkable role in all aspects of our daily lives and can be deployed in many fields, including healthcare, automobile, industrial appliances, sports, homes, and so on. Billions of small “things” talk to each other and cooperate to fulfill some sophisticated tasks, which not only arouse exciting opportunities for economic growth, but also opens the door to a variety of new security threats. However, restricted by the objective demand of low cost and lightweight, the devices in IoT, especially in wireless sensor networks (WSNs) [4,5], which are considered to be the main application scenario of the future IoT, are generally characterized by limited resources, battery power supply, low energy consumption and poor computing capacity. The rapid development of wireless communication will give rise to the massive deployment of sensors nodes and a vast amount of information exchange, making it unfeasible to flexibly recharge and control the power-constricted devices. Therefore, energy shortage is one of the biggest challenges restricting the effective and
widespread application of WSNs and IoT [6]. Due to the rising power costs, green-oriented methods have inevitably become the dominating design consideration in the WSNs system. Fortunately, wireless powered communication (WPC) technology based on the far field radio frequency (RF) energy harvesting (EH), as a promising paradigm to tackle the energy barrier suffered by traditional wireless communication networks as well as emerging WSNs, has been attracting worldwide attention by the researchers in recent years [7–12]. In contrast to traditional wireless sensors, which rely on batteries or are powered by wired charging for their energy need, the devices in wireless powered sensor networks (WPSNs) can be able to harvest energy from RF signals wirelessly. Consequently, it can fundamentally release the heavy burden caused by frequent battery replacement and/or recharging, avoid the communication interruption caused by energy loss, and ensure theoretical permanent life for communication systems [13]. A basic hurdle of WPSNs rest with the fast attenuation of radio frequency (RF) signals with distance changing. Moreover, energy amount harvested at wireless powered devices is fairly restricted, which limits the coverage severely and has become a bottleneck for the widespread application of WPSNs. Consequently, the design of an energy-efficient transmission is of great significance to introduce the green concept into future WPSNs.

Meanwhile, compared with the traditional WSNs, both the topological structure and the radio environment of WPSNs are more complex and the nodes are more diverse, which makes information interaction face more severe security threats [12,13]. Typically, the algorithms based on the upper layer encryption mechanism are explored to ensure information security in wireless communication. Unfortunately, with the continuous development of computer technologies and the emergence of quantum computers, the conventional cryptographic techniques can no longer satisfy the requirements for confidentiality of wireless transmissions. In addition, the tedious algorithms are restricted for many lightweight sensors owing to requirements of high hardware complexity and more energy. Therefore, for the further enhancement of information security, physical layer security (PLS), which is a promising way to ensure the security of wireless networks, has been considered an effective supplement for the existing solutions [14–16]. With regard to the wireless PLS, its basic idea is to make use of the characteristics of randomness and openness of wireless channels to reliably transmit information from legitimate transmitters to expected receivers, and to ensure that confidential information is not intercepted or eavesdropped [15]. To improve the secrecy performance of wireless communication network effectively, the researchers have carried out a lot of approaches to expand the difference between the legitimate channel and the eavesdropping channel. At present, the widely used enhancement technologies of PLS can be divided into several categories [17]: physical layer secret key generation, coding-based secure transmission, security-oriented beamforming; artificial noise (AN) assisted technology and security diversity technology, etc.

Recently, many works have investigated the PLS in cognitive radio networks (CRNs) [18,19] and in WPSNs [20–33]. Specifically, the authors in [18] analyze a secure dual-hop mixed radio frequency-free space optical (RF-FSO) downlink simultaneous wireless information and power transfer system. The authors in [19] consider an underlay multiple-input-multiple-output (MIMO) CRN. On the other hand, aimed at direct communication scenarios, the authors in [22] investigated the secure beamforming schemes in a multi-input single-output (MISO) downlink system with a multi-antenna transmitter and multiple energy receivers (ERs). Secrecy performance for a single-input multi-output (SIMO) wireless powered network is presented in [23]. Later, in [24], the system model in [23] was extended to a wireless powered MIMO network. For further improving the security of WPSNs, Refs. [25–27] explored the rational use of wireless powered friendly jammer, where the jammer harvests wireless energy from external RF signal before sending the artificial noise (AN) to confuse eavesdroppers. On the other hand, for the dual-hop cooperative communication scenarios, the cooperative jamming (CJ) scheme and the zero-forcing beamforming was designed to enhance the security of WPSNs in [28–30]. With the help of relay-selection strategy, [31–33] investigated secure communication in multiple relays aided WPSNs. In particular, ref. [33] designed a secure energy-efficient (SEE) transmission strategy for wireless powered IoT with multiple power beacons.
PBs), which can provide a stable energy supply for the WPSNs flexibly. It is worth remarking that most of works pay much more attention to the improvement of secrecy performance contributed by multi-antenna diversity, cooperation diversity and AN-aided method, but a few pay attention to the practical scenario with multiuser scheduling [34,35], which can be seen as the typical application of future WSNs.

On the other hand, a major limitation of aforementioned works is that they all considered the linear mode for energy harvester, which has the advantage of easy analysis and processing. However, as a matter of fact, the practical EH circuits usually show a nonlinear feature rather than a linear one. Compared to the nonlinear EH model, the linear one may lead to the significant performance degradation in practical WPSNs. In particular, the recent advanced works in [36–38] pointed out that the nonlinear EH mode is more reasonable due to the power conversion circuits, capacitors, inductors, and diodes used in the electronic devices are nonlinear commonly. The over-simplified linear EH modes do not capture the nonlinear characteristics of the rectenna accurately enough and may lead to severe resource allocation mismatches, resulting in the performance to drop significantly in practical applications [11,39]. Furthermore, the authors in [40] introduced that the saturation nonlinear mode is closer to the experimental results derived from the actual RF-based EH devices. Recently, although several works have investigated the impacts of the saturation nonlinear EH mode on the secrecy performance of WPSNs [36,39,41], the considered models are too complex and the computational complexity of the proposed schemes is too high, which is unhelpful to extract deep insights of the practical saturation nonlinearity. Moreover, the exact closed-form expression of secrecy outage probability (SOP), which is regarded as an important indicator of secrecy performance, has been not given in [36]. Additionally, it is necessary to explore the effect of activation threshold of the power conversion circuits on the security of WPSNs. The so-called activation threshold means that when the input power of the EH circuit is lower than the threshold value, it will always be inactive, resulting in the device unable to transmit information. On the contrary, it can turn on the energy harvester and provide continuous power for the normal transmission of information [33,38]. Specifically, for the considered WPSNs, the nonlinearity of EH has an important impact on the secrecy performance of the system. Therefore, to expose the trade-off between the energy consumption and the security, SEE is a proper metric to indicate this relationship. Although there are lots of papers about the secure transmission or energy-saving in WPSNs, they always ignore this trade-off.

Enlightened by previous observations, this paper investigates the impact of nonlinear EH and activation threshold on the multiuser WPSNs with generalized multiuser scheduling (GMS) from the PLS perspective, where multiple source sensors that perform monitoring or operating tasks in the local group harvest energy from the dedicated PB in the presence of an external eavesdropper. In particular, the GMS scheme is used at the source sensors based on the legitimate link to improve the secrecy performance. Moreover, by comparing with general linear EH mode, we deeply analyze the influence of nonlinear EH circuit and energy activation threshold on the secrecy performance of WPSNs. The main contributions of this paper are as below:

- We explore the PLS in the multiuser WPSNs with GMS scheme, where the Kth-best source sensor is chosen by the main channel for improving the security. Furthermore, we obtain the exact closed expressions for SOP of the system under linear energy harvesting (LEH), saturation nonlinear energy harvesting (SNEH) and saturation nonlinear energy harvesting with activation threshold (SNAT), respectively.
- With the help of the SOP expressions, we further discuss the impact of various key parameters on secrecy performance of the multiuser WPSNs, including the number of source sensor, the EH efficiency factor, the generalized selection coefficient, the saturation threshold, the activation threshold, the transmit power of PB and the time-switching coefficient. To get a deeper insight, we further investigate the maximization problem of SEE and compare the SEE under three different EH modes.
• Simulation results demonstrate that increasing the number of source sensors, enhancing the EH efficiency and strengthening the transmit power of PB all favorable to improve secrecy performance of the multiuser WPSNs. Meanwhile, the smaller generalized selection coefficient is beneficial for SOP in three EH modes. Furthermore, the SOP of SNEH is better when the saturation threshold is higher and LEH is an ideal situation for SNEH when the saturation threshold is large enough. The SOP of SNAT is better when the activation threshold is lower and SNEH is a special situation for SNAT when the activation threshold is low enough. In addition, for providing secure and efficient communication, the time-switching factor should be optimized seriously. Finally, the activation threshold has an important impact on the SEE of the considered system, which is worth considering carefully.

The remainder of this paper is arranged as follows. We provide details including the system model, the process of wireless power transfer (WPT) and signal analysis, the GMS scheme and three EH modes in Section 2. Section 3 analyzes the secrecy performance of the considered model, derives the exact SOP under three different EH modes and solves the optimization problem of SEE. In Section 4, numerical results and the corresponding discussions are presented. Finally, Section 5 presents the conclusion of this paper.

2. System Model and Signal Analysis

2.1. System Model

An uplink transmission in the multiuser WPSNs is considered to be illustrated in Figure 1, which consists of a dedicated power beacon (PB), multiple source sensors $S_n, n \in \mathcal{N} = \{1, \cdots, N\}$, an intended destination $D$, and an eavesdropper (Eve) $E$. Due to the limitation of terminal devices, $S_n$ ought to acquire energy by WPT from the dedicated PB to support information transmission. In contrast, the destination $D$ is powered by on-grid power. Additionally, we assume that each sensor $S_n$, the destination $D$ and the Eve $E$ are single-antenna and half-duplex devices [42]. It is worth noting that the model has numerous practical applications, such as in IoT and in low power wide area network (WAN), where the multiple sensors that restricted to a single antenna owing to cost and size limitations upload information to the access point (AP) or the base station (BS) directly.

![Figure 1. System model.](image)

Furthermore, in this paper, all the channels experience Rayleigh fading, which has been commonly considered to be the special case of Rician fading under the situation that the line-of-sight component is assumed to be zero. Meanwhile, it is usually adopted in works that investigating the secrecy performance of WPSNs [31–33,43], because it can be seen as the foundation for exploring the more practical Rician fading circumstance. It is considered that the additive white Gaussian noise (AWGN) at destination has zero mean and variance $N_0$. In addition, compared with the full channel situation information (CSI) assumption in [32,34], we assume only the statistic CSI is available in the
passive wiretap scenario, which is more reasonable because the weak computation ability and small memory of the lightweight devices in the future wireless communication network [33]. In practice, wireless communication environments are very complex and changeable, resulting in the full CSI is hard to acquire.

For the convenience of mathematical modeling, the channel coefficients of the $P \rightarrow S_n$, $S_n \rightarrow D$ and $S_n \rightarrow E$ links are denoted by $h_{PS_n}$, $h_{S_nD}$, $h_{S_nE}$, respectively, which are considered to be subject to independent quasi-static Rayleigh fading. Furthermore, we consider that multiple source users are close in proximity, i.e., they are assumed to form a cluster. This consideration is often exploited in the investigation on WPSNs [32], which brings about the equivalent average link power gains of the channel $P \rightarrow S_n$, $S_n \rightarrow D$ and $S_n \rightarrow E$, respectively. For convenience, we define $\lambda_{PS_n} = \lambda_{PS}$, $\lambda_{S_nD} = \lambda_{SD}$ and $\lambda_{S_nE} = \lambda_{SE}$ for any $n \in \mathcal{N}$.

2.2. Wireless Power Transfer and Signal Analysis

For WPT, the receiver in the terminal adopts EH mode based on rectangular antenna structure [44]. Specifically, the authors in [44] explore the rectenna nonlinearity from a stochastic geometry point of view. Furthermore, with regard to the rectangular rectenna, the RF signal will convert into the direct current (DC) signal through a rectifier that was composed of the passive low-pass filter (LPF) and the Schottky diode [45]. Then, it is considered that for all users, the harvested energy at the stage of WPT is entirely used for data transmission in wireless information transmission (WIT), i.e., the so-called harvest-use (HU) mode introduced as in [43] is adopted.

If the link fading factors keep unchanged within a transmission time slot $T$, one HU period including two time windows can be shown as in Figure 2. In the first phase that is denoted by $\alpha T$, where $\alpha \in (0, 1)$ is the time-switching factor, the multiple sources harvest energy from broadcast RF signal transmitted by the PB. In addition, another time window $(1 - \alpha)T$ represents the second phase, in which a $K$th-best sensor is scheduled from multiple source sensors based on the channel quality of legitimate link (i.e., the link $S_n \rightarrow D$) to upload data for improving the secrecy performance, and the $E$ also interpret the message transmitted from the selected sensor. Then, the harvested energy at $S_n$ can be shown as below [33,46]:

$$E_{S_n} = \eta P_B \alpha T |h_{PS_n}|^2,$$

where $10\% < \eta < 80\%$ denotes the EH efficiency factor, which mainly determined by the EH circuitry and frequencies [47]. Specifically, the relationship between the rectenna’s RF-to-DC conversion efficiency and the frequency is discussed in detail in [48]; $P_B$ denotes the transmit power of PB; $|h_{PS_n}|^2$ is power gains of the channels from the PB to $S_n$. It should be emphasized that the sources in WPSNs are passive sensors whose received noise power is far less than the received power contributed by PB [49]. Therefore, the harvested energy from noise is negligible.

![Figure 2. Time-switching scheme.](image-url)
To be specific, assume that the $n^*$-th sensor, which is denoted by $S_{n^*}$, is selected based on the GMS scheme as the information transmitting node during the latter phase. Then, the received signals at destination $D$ and eavesdropper $E$ are respectively expressed as

$$y_D = \sqrt{P_{S_n^*}} h_{S_{n^*},D} x + n_D,$$

$$y_E = \sqrt{P_{S_n^*}} h_{S_{n^*},E} x + n_E,$$

where $x$ denotes the confidential data transmitted by the selected sensor user, $P_{S_n^*}$ represents the transmit power of $S_{n^*}$, $h_{S_{n^*},D} \sim \text{CN}(0, \lambda_{SD})$ is the channel fading coefficients between $S_{n^*}$ and $D$, and $h_{S_{n^*},E} \sim \text{CN}(0, \lambda_{SE})$ is the channel fading coefficient between $S_{n^*}$ and $E$. $n_D \sim \text{CN}(0, N_0)$ and $n_E \sim \text{CN}(0, N_0)$ are AWGN at $D$ and $E$, respectively.

Furthermore, the SNRs at $D$ and $E$ are represented as $\gamma_{S_{n^*},D}$ and $\gamma_{S_{n^*},E}$, respectively, which can be expressed as

$$\gamma_{S_{n^*},D} = \frac{P_{S_n^*} |h_{S_{n^*},D}|^2}{N_0},$$

$$\gamma_{S_{n^*},E} = \frac{P_{S_n^*} |h_{S_{n^*},E}|^2}{N_0},$$

where $|h_{S_{n^*},D}|^2$ and $|h_{S_{n^*},E}|^2$ are power gains of the channels from the $S_{n^*}$ to $D$ and $S_{n^*}$ to $E$.

### 2.3. Generalized Multiuser Scheduling

As described above, the Eve is a passive wiretapping node, i.e., the full CSI of Eve is unavailable. Hence, with the help of the GMS scheme, we select the sensor $S_{n^*}$ based on the legitimate channel only, the index of certain sensor is given as

$$n^* = K^{th} \max_{n \in \{1, \cdots, N\}} \left(|h_{S_{n^*},D}|^2\right), 1 \leq K \leq N,$$

where $K^{th} \max (\cdot)$ denotes the function used to decide the $K$th strongest sensor, $K$ is the generalized selection coefficient and $N$ is the number of source sensor.

**Lemma 1.** If $X_n, n \in \mathcal{N} = \{1 \cdots N\}$, is the random variable with the independent and identical exponential distribution (i.i.d.), the probability density function (PDF) of $X = K^{th} \max (X_n)$ can be given by [50,51]:

$$f_X (x) = \sum_{n=1}^{N-K} (-1)^n \binom{N-K}{n} \binom{N}{K} K^{\lambda_X} \exp \{- (n + K) \lambda_X x\},$$

where $x$ denotes the random variable of PDF, $K$ is the generalized selection coefficient.

In line with the Lemma 1, the PDF of $|h_{S_{n^*},D}|^2$ can be given as:

$$f_{|h_{S_{n^*},D}|^2} (x) = \sum_{n=1}^{N-K} (-1)^n \binom{N-K}{n} \binom{N}{K} K^{\lambda_{SD}} \exp \{- (n + K) \lambda_{SD} x\},$$

where $\frac{1}{\lambda_{SD}} = E \left[|h_{S_{n^*},D}|^2\right]$, and $E [\cdot]$ is an expectation operator.
On the other hand, the Kth-best sensor is scheduled based on the main channel, which is independent of the wiretapping channel and corresponds to a random sensor for Eve. Consequently, the PDF of $|h_{S_n,E}|^2$ is exponentially distributed with parameters $\frac{1}{\lambda_{SE}}$, which is shown as:

$$ f_{|h_{S_n,E}|^2}(x) = \lambda_{SE} e^{-\lambda_{SE}x}, \quad (9) $$

where $\frac{1}{\lambda_{SE}} = E[|h_{S_n,E}|^2]$.

2.4. Energy Harvesting Mode

In this part, we introduce three different EH modes, i.e., linear EH (LEH), saturation nonlinear EH (SNEH) and saturation nonlinear EH with activation threshold (SNAT), respectively. In the LEH mode, the output power of the source sensor is proportional to the harvested energy, which means that the relationship between the transmit power of the sensor and the harvested energy is linear. In comparison, the transmit power of the sensor is limited by the saturation threshold in the SNEH mode. On the other hand, when considering the SNAT mode, the transmit power of the sensor is affected by both the saturation threshold and the activation threshold.

2.4.1. Linear Energy Harvesting Mode

LEH mode has been widely used in a large number of previous works contributed by the intuitive and concise expression. According to the [31–33] and with the help of (1), under the LEH mode the output power of certain $S_n$, i.e., $P_{S_n}$, can be expressed as:

$$ P_{S_n} = \frac{E_{S_n}}{(1-\alpha)^2} = \eta \alpha \frac{P_B |h_{PS_n}|^2}{1-\alpha}, \quad (10) $$

It needs to be highlighted that (10) gives a general linear power conversion mode on the premise that the wireless device has infinite battery capacity [40].

2.4.2. Saturation Nonlinear Energy Harvesting Mode

In practice, the wireless sensors have limited battery capacity commonly. When the harvested energy exceeds a certain threshold, the output power will reach saturation state [38]. Moreover, the LEH mode is really too simplified, which is not demonstrated by circuit simulations and measurements [11,40]. However, it is quite complicated to deal with the accurate nonlinear mode. Consequently, we hereby adopt a simplified SNEH model, which captures the real characteristics of practical EH circuit closely. It was shown that the SNEH mode is a tractable parameter model [52]. It is worth noting that for ease of analysis, it is assumed that all sensors have the same saturation threshold.

In line with [36,53], for SNEH mode, the output power $P_{S_n}$ can be given as:

$$ P_{S_n} = \begin{cases} \frac{\eta s}{1-\alpha} P_B |h_{PS_n}|^2 & \text{if } |h_{PS_n}|^2 < \frac{\Gamma_{th,S}^B}{\Gamma_{th,S}^a} \\ \frac{\eta s}{1-\alpha} \Gamma_{th,S} & \text{if } |h_{PS_n}|^2 > \frac{\Gamma_{th,S}^B}{\Gamma_{th,S}^a} \end{cases}, \quad (11) $$

where $\Gamma_{th,S}^B$ denotes the saturation threshold of the receiver at $S_n$.

2.4.3. Saturation Nonlinear Energy Harvesting with Activation Threshold

On the other hand, in order to provide continuous power for information transmission, the harvested energy at receiver must be larger than the minimum threshold, which is used to activate the EH circuitry and to sustain the power conversion. Conversely, when the harvested energy is less than the activation threshold, EH circuit keeps inactive resulting in the sensor has not enough power to transmit information. Similarly, it is assumed that all harvesters have the same EH circuit,
which means that all sensors have the same saturation threshold and activation threshold. For SNAT mode, the output power $P_{Sn}$ can be shown as:

$$
P_{Sn} = \begin{cases} 
0 & \text{if } |h_{PSn}|^2 < \frac{\Gamma_{th-A}}{P_B} \\
\frac{n_a}{1-a} p_{\bar{B}} |h_{PSn}|^2 & \text{if } \frac{\Gamma_{th-A}}{P_B} < |h_{PSn}|^2 < \frac{\Gamma_{th-S}}{P_B} \\
\frac{n_a}{1-a} \Gamma_{th-S} & \text{if } |h_{PSn}|^2 > \frac{\Gamma_{th-S}}{P_B} 
\end{cases}, \quad (12)$$

where $\Gamma_{th-A}$ denotes the activation threshold of the receiver at $S_n$.

### 3. Secrecy Performance Analysis

The comprehensive secrecy performance analysis for the multiuser WPSNs with GMS scheme under abovementioned three different EH modes is presented in this section.

#### 3.1. Preliminaries

According to [31], the achievable secrecy capacity of the scenario can be given as:

$$
C_s = (1 - \alpha) \left[ \log_2 (1 + \gamma_{S_n,D}) - \log_2 (1 + \gamma_{S_n,E}) \right]^+, \quad (13)
$$

where $C_s$ is the achievable secrecy capacity of the considered multiuser WPSNs, which mainly refers to the difference of the channel capacity between the main channel and the wiretap channel; $\gamma_{S_n,D}$ and $\gamma_{S_n,E}$ are the instantaneous SNRs at $D$ and $E$, respectively, which has been given in Equations (4) and (5); $[x]^+ = \max(x, 0)$.

It should be noted that for evaluating the secrecy performance, we resort to the SOP as the figure of merit, which is regarded as an important indicator of PLS generally and is mainly used to investigate the secrecy performance of the system when the specific CSI of the wiretap channel cannot be obtained. From information-theoretic sense, when the secrecy capacity $C_s$ of the system is lower than a predetermined secrecy rate threshold $R_{th}$, the transmission incurs secrecy outage.

#### 3.2. Secrecy Outage Probability Analysis

Specifically, the SOP of each EH mode $P_{sop}^{(mod)}$ can be shown as

$$
P_{sop}^{(mod)} = \Pr \left\{ C_{s}^{(mod)} < R_{th} \right\} = 1 - \Pr \left\{ C_{s}^{(mod)} > R_{th} \right\}, \quad (14)
$$

where $mod \in \{LEH, SNEH, SNAT\}$ and $\Pr \{ \cdot \}$ is the probability.

#### 3.2.1. Derivation for LEH Mode

According to Equation (14), the exact SOP of considered multiuser WPSNs with GMS scheme under LEH mode can be formulated as:

$$
P_{sop}^{(LEH)} = 1 - \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K_{SD} \lambda_{SE}}{\lambda_{SD} + \lambda_{SE}} \\
\times 2 \sqrt{\frac{\xi \lambda_{PS}}{\gamma_P \lambda_{SD}(n+K)}} K_1 \left( 2 \sqrt{\frac{\xi \lambda_{PS} \lambda_{SD}}{\gamma_P} (n+K)} \right), \quad (15)
$$

where $P_{sop}^{(LEH)}$ is the SOP when the wireless powered sensors operate in the LEH mode, $\gamma_P = \frac{P_B}{N_0}$, $\xi = \frac{(1-\alpha)(\beta-1)}{\eta_a}$ and $\beta = 2 \gamma_{th} \lambda_{SE} = \frac{\lambda_{SE}}{\beta}$, $K_1 (\cdot)$ described in [54] is the modified Bessel function of the second kind.

**Proof.** Appendix A provides the proof. $\square$
3.2.2. Derivation for SNEH Mode

Similarly, according to (14), the SOP for SNEH is calculated as:

$$p_{sop}^{(\text{SNEH})} = 1 - \sum_{n=1}^{N-K+\infty} \left( \begin{array}{c} N \cr K \end{array} \right) \left( \begin{array}{c} N-K \cr n \end{array} \right) (-1)^{n+k}$$

$$\times \frac{K\lambda_{SD}\lambda_{SE}}{\lambda_{SD} + \lambda_{SE}} \frac{\left( \frac{\lambda_{PS}x^k}{\lambda_{PS}} \right)}{k!} \left( \frac{\xi}{\theta} \right)^{-\frac{\xi}{2}} \left[ \lambda_{SD} (n + K) \right]^{\frac{k}{2}-1}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

where $p_{sop}^{(\text{SNAT})}$ is the SOP when the wireless powered sensors operate in the SNAT mode, $\Gamma_{S} = \frac{\Gamma_{th,S}}{N_0}$, $W_{A,\mu}(\cdot)$ is Whittaker function as defined in [44], Equation (3.381.6).

**Proof.** Appendix B shows the proof.

3.2.3. Derivation for SNAT Mode

Furthermore, according to Equation (14), the exact SOP for SNAT is given as:

$$p_{sop}^{(\text{SNAT})} = 1 - \sum_{n=1}^{N-K+\infty} \left( \begin{array}{c} N \cr K \end{array} \right) \left( \begin{array}{c} N-K \cr n \end{array} \right) (-1)^{n+k}$$

$$\times \frac{K\lambda_{SD}\lambda_{SE}}{\lambda_{SD} + \lambda_{SE}} \frac{\left( \frac{\lambda_{PS}x^k}{\lambda_{PS}} \right)}{k!} \left( \frac{\xi}{\theta} \right)^{-\frac{\xi}{2}} \left[ \lambda_{SD} (n + K) \right]^{\frac{k}{2}-1}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\Gamma_{SD}(n+K)} W_{-\frac{1}{2}, \frac{1}{2} - \frac{k}{2} \Gamma_{SD}(n+K)}}$$

where $p_{sop}^{(\text{SNAT})}$ is the SOP when the wireless powered sensors operate in the SNAT mode, $\Gamma_{A} = \frac{\Gamma_{th,A}}{N_0}$.

**Proof.** Appendix C presents the proof.

**Remark 1.** According to Equations (15)–(17), we find that for the all three EH modes, the number of the source sensors and the EH efficiency factor play a positive role on the SOP of the multiuser WPSNs. On the other hand, the smaller value of the generalized selection coefficient is beneficial for the SOP in three EH modes. Meanwhile, we observe that the secrecy performance of SNEH is better in the case of higher saturation threshold, and the secrecy performance of SNAT is better when the activation threshold is lower. The above discussions will be analyzed and proved specifically in Section 4.
3.3. Secure Energy Efficiency Maximization

In general, the improvement of security often comes at the expense of more energy. In terms of energy-limited WSNs, the excessive pursuit of secrecy improvement has negative impact on the network performance. Therefore, it is valuable to make sure the secure communication with low energy consumption. According to the above analysis, the SEE is used as the proper metric for evaluating the secrecy performance of the multiuser WPSNs, which is commonly adopted to measure the trade-off between the secrecy performance and energy consumption [33]. Generally, the SEE is defined as the ratio between the secure throughput and the total energy consumption. Mathematically, the SEE of above discussed EH modes can be shown as

$$
\eta^{(\text{mod})}_s = \frac{R_{\text{th}}(1 - P_{\text{coop}}^{(\text{mod})})}{P_t},
$$

where $\eta^{(\text{mod})}_s$ denotes the SEE of each EH mode, $P_t = \kappa P_B + P_c$ represents the total power cost at PB, $\kappa$ denotes the power factor, $P_c$ and $P_B$ stand for the fixed power and transmit power at PB. It is considered that the harvested energy by the source sensors is fully depleted for information transmission while the power cost of the circuitry is neglected.

To find the best transmit power of PB, the SEE maximization problem can be given as

$$
\max_{P_B} \eta^{(\text{mod})}_s = \frac{R_{\text{th}}(1 - P_{\text{coop}}^{(\text{mod})})}{P_t} \quad \text{s.t.} \quad 0 < P_B \leq P_{\text{max}},
$$

where $P_{\text{max}}$ denotes the maximum transmit power of PB. It is obviously that the solving process of the exact expressions for $P_B$ is quite complex. Fortunately, with the help of the searching method, we can get the optimal $P_B$ based on the simulation and numerical analysis. It is worth noting that the hereinabove SEE optimization problem can be considered to be the guide to the practical implementation, which can be applied to engineering decision-making. Meanwhile, the expression in (19) is more practical for the future communication.

Remark 2. With the help of Equations (15)–(17), we find that the security performance can be improved by increasing the transmit power in PB. However, the denominator of SEE in (18) is an increasing function of the transmit power. Therefore, overload transmit power has a negative effect on the SEE. On the other hand, increasing time-switching factor can effectively increase the transmit power of the sensors, but also decrease the communication performance of the system due to the reduction of information transmission time. Thus, how to maximize the SEE by optimizing the transmit power in PB and the time-switching factor is of more practical operational significance for the considered multiuser WPSNs.

4. Numerical Results and Discussion

The analytical and simulation results are provided in this section for evaluating the impact of key parameters on the security of the multiuser WPSNs, including the number of source sensors, the EH efficiency factor, the generalized selection coefficient, the saturation threshold, the activation threshold, the transmit power of PB and the time-switching factor. It is worth noting that all the numerical results in this section come from the simulation environment of MATLAB, which all are true experimental results. Combining the parameter setting in the article with the program code, all the results can be reproduced. Unless otherwise stated, the system parameters and the initial conditions are set as below: $N = 3$, $K = 2$, $\eta = 0.6$, $(R_{\text{th}} = 0.1 \text{ bits/s/Hz})$, $\gamma_P = 30 \text{ dB}$, $\alpha = 0.5$, $\Gamma_{\text{th},S} = 10 \text{ dB}$, $\Gamma_{\text{th},A} = 0 \text{ dB}$, $k = 0.01$, $P_t = 100 \text{ mW}$ and $\lambda_{\text{PS}} = \lambda_{\text{SD}} = 1$. Specifically, the times of the simulation set to 100000. It should be emphasized that the ratio of the main channel to the eavesdropping channel can be expressed as $\tau = \frac{\lambda_{\text{PS}}}{\lambda_{\text{SD}}} [36]$, whose value is considered between $-10 \text{ dB}$ and $50 \text{ dB}$ in this section.
From the figures, it is obvious that the simulation results are in accurate agreement with the theoretical calculation results, which verifies the correctness of our derivations.

As shown in Figures 3–5, we provide the SOP of the considered multiuser WPSNs with GMS versus $\tau$ for three different EH modes under various $N$, $\eta$, and $K$. From Figure 3, we can observe that for the all three EH modes, the number of the source sensors has a positive impact on the SOP, i.e., a larger value of $N$ brings about better SOP performance. The reason is that the better sensor scheduling advantage can be acquired when more alternative sensors are available, which can provide better multiuser diversity gain. Figure 4 illustrates that the EH efficiency factor plays a positive role on the SOP. This is due to the fact that a higher energy conversion efficiency contributes to harvest more energy and power for secure communication. On the other hand, Figure 5 shows that the smaller value of $K$ is beneficial for the SOP in three EH modes. It can be explained that a better sensor in terms of secrecy capacity is chosen, which is helpful to enhance the security of the system.

Figure 3. Secrecy outage probability versus $\tau$ for three EH modes under various $N$, where $N = \{3, 5\}$.

Figure 4. Secrecy outage probability versus $\tau$ for three EH modes under various $\eta$, where $\eta = \{0.6, 0.8\}$. 
Figure 5. Secrecy outage probability versus $\tau$ for three EH modes under various $K$, where $K = \{1, 2\}$.

Figure 6 depicts the SOP versus $\tau$ for LEH and SNEH under different saturation thresholds. It is shown that the secrecy performance of SNEH is better in the case of the saturation threshold $\Gamma_{th,S}$ is higher on account of that batteries with large capability can provide more stored energy for secure communication. However, it exists a floor, in which the SOP keeps unchanged as $\Gamma_{th,S}$ increases. This is because increasing $\Gamma_{th,S}$ can only enhance the battery capability rather than the EH capacity. In addition, it is noted that LEH is an ideal situation for SNEH when the saturation threshold is large enough.

Figure 7 presents the SOP versus $\tau$ in three different EH modes under different activation threshold. As can be easily observed that the secrecy performance of SNAT is better when the activation threshold is lower. This can be explained by the fact that the lower activation threshold is beneficial for more source users to participate in the information transmission, which makes the WPSNs to get better multiuser diversity gain. On the other hand, as shown in the figure, it can be inferred that SNEH is a special situation for SNAT when the activation threshold is lower enough.
Figure 7. Secrecy outage probability versus $\tau$ for three EH modes under various $\Gamma_{th_A}$, where $\Gamma_{th_S} = 10$ dB and $\Gamma_{th_A} = \{-\infty, 0, 5, 8\}$.

Figure 8 plots the impact of the transmit power of PB on SOP for three different EH modes. As shown clearly in the figure that the SOP of LEH and SNEH is almost identical when the transmit power of PB is lower. The reason is that the lower transmit power of PB makes the energy acquired in all sensors difficult to achieve the saturation threshold, leading to the multiuser WPSN operates in the LEH mode. In contrast, the SOP of SNAT and SNEH is almost consistent when the transmit power of PB is higher. It is because the large transmit power of PB contributes to activate all the source sensors to harvest energy for information transmission, which is leading to all the sensors of SNAT work in the SNEH mode.

Figure 9 shows the SOP performance under various $\alpha$ in three different EH modes. It can be observed that the function of SOP and $\alpha$ are both unimodal function. The reason is that for the smaller value of $\alpha$, which means that the time for EH is less, the harvested energy is usually insufficient for the operation of multiple source sensors. On the contrary, when $\alpha$ is large enough, the time for information
transmission will be limited seriously, which in turn leads to high communication interruption probability. Consequently, $\alpha$ should be considered carefully to provide efficient communication.

![Figure 9](image)

**Figure 9.** Secrecy outage probability versus $\alpha$ in three EH modes, where $\tau = 20$ dB.

Figure 10 describes the SEE of the considered WPSN versus $\tau$ in different EH modes. From the figure, we can find that the activation threshold limits the secrecy performance of the system in SNAT mode. By comparison, the impact of the saturation threshold on the security in SNEH mode is relatively small. Therefore, it is very valuable to investigate the influence of activation threshold on secrecy performance for WPSNs.

![Figure 10](image)

**Figure 10.** Secure energy efficiency versus $\tau$ in three EH modes, where $\Gamma_{th,S} = 3$ dB.

5. Conclusions

In this paper, we explored the PLS in the multiuser WPSNs with GMS scheme. First, we analyzed the impact of various key parameters on the secrecy performance of the system, including the number of source sensor, the EH efficiency factor, the generalized selection coefficient, the saturation threshold, the activation threshold, the transmit power of PB and the time-switching coefficient. Furthermore,
to get a deeper insight, we discussed the maximization problem of SEE and compared the SEE under three different EH modes. Simulation results demonstrated that: (1) the number of source sensors, the EH efficiency and the transmit power of PB all have positive impact on SOP, the smaller generalized selection coefficient is advantageous for secrecy performance; (2) LEH is an ideal situation for SNEH when the saturation threshold is large enough and SNEH is a special situation for SNAT when the activation threshold is lower enough; (3) the time-switching factor and the activation threshold have an important effect on the secrecy performance, which should be considered carefully. It is worth noting that the more complex topology, such as the network following the random geometric distribution, is not considered in this paper, which can be explored in our future works. In addition, the model of the EH nonlinearity in this paper is relatively simple and basic, only the characteristics of the rectifier are preliminarily described, and the next step is to consider a more practical rectifier model.

Author Contributions: X.S. searched literature, conducted the simulation and wrote the paper; H.Y. conducted the experiments, analyzed the data and revised the paper; Y.W. (Yida Wang) designed the algorithm; M.L. proposed the idea and revised the paper; Y.W. (Yong Wang) proposed the idea, designed the algorithm, analyzed the data and revised the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

Appendix A

First, from Equation (14), $P_s^{(LEH)}$ can be given as
\[
P_s^{(LEH)} = 1 - \Pr \left\{ C_s^{(LEH)} > R_{th} \right\}
\] (A1)

Furthermore, with the help of (4), (5), (10) and (13), $\Pr \left\{ C_s^{(LEH)} > R_{th} \right\}$ can be derived and the expansion is listed below:
\[
\Pr \left\{ C_s^{(LEH)} > R_{th} \right\} = \Pr \left\{ \frac{1 + \gamma S_n D}{1 + \gamma S_n E} > 2^{\frac{R_{th}}{\eta}} \right\}
\] (A2)

where $Z = |h_{S_n D}|^2 - \beta |h_{S_n E}|^2$.

By introducing the result in [28], Equation (39) and aided by Equations (8) and (9), the PDF of $Z$ can be further expressed as
\[
f_Z(z) = \int_0^{+\infty} f_{|h_{S_n D}|^2} (z+y) \left( \frac{y}{\beta} \right)^{\frac{N-K}{2}} (\frac{y}{\beta}) dy
\]
\[= \frac{N-K}{N} \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K\lambda_{SD}\lambda_{SE}}{\lambda_{SD} + \lambda_{SE}} \times \exp \left[ -\lambda_{SD} (n + K) z \right]
\] (A3)

Then, by substituting Equation (A3) into Equation (A2) and with the help of [44], Equation (3.324.1), we have
Pr \left\{ C_s^{(LEH)} > R_{th} \right\} = \int_{0}^{+\infty} \int_{0}^{+\infty} f_{P_{SN}}(x) f_{Z}(z) \, dx \, dz

= \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K\lambda_{SD}\lambda_{SE}}{\lambda_{SD} + \lambda_{SE}}

\times \int_{0}^{+\infty} \exp \left[ -\frac{4\lambda_{PS}}{4z} - \lambda_{SD} (n+K) z \right] \, dz

= \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K\lambda_{SD}\lambda_{SE}}{\lambda_{SD} + \lambda_{SE}}

\times 2 \sqrt{\frac{\xi\lambda_{PS}}{\gamma_{P}\lambda_{SD}(n+K)}} K_1 \left( 2 \sqrt{\frac{\xi\lambda_{PS}\lambda_{SD}(n+K)}{\gamma_{P}}} \right)

(A4)

Finally, by substituting Equation (A4) into Equation (A1), \( P_{sop}^{(LEH)} \) in Equation (15) can be derived.

**Appendix B**

Following the same line of derivation used for obtaining \( P_{sop}^{(LEH)} \), from Equation (14), \( P_{sop}^{(SNEH)} \) can be shown as

\[
P_{sop}^{(SNEH)} = 1 - Pr \left\{ C_s^{(SNEH)} > R_{th} \right\}
\]  

(A5)

With the help of Equations (4), (5), (11) and (13), \( Pr \left\{ C_s^{(SNEH)} > R_{th} \right\} \) can be obtained and the expansion is listed below:

\[
Pr \left\{ C_s^{(SNEH)} > R_{th} \right\} = \frac{\eta}{1-\alpha} \left| h_{PS_{s+}} \right|^2 \gamma_B \left( \left| h_{S_{s+}} \right|^2 - \beta \left| h_{S_s} \right|^2 \right) > \beta - 1
\]  

(A6)
Then, by substituting Equation (A3) into Equation (A6) and using the Maclaurin series of the term $e^{-\frac{z}{\gamma_p}} = \sum_{k=0}^{\infty} (-1)^k \frac{\lambda_p}{k!} z^k$ [55], aided by the [44], Equation (3.381.6), i.e., Whittaker function, we have

$$
\Pr \left\{ C_s^{(\text{SNAT})} > R_{th} \right\} = \int_{\frac{R_{th}}{\gamma_p}}^{\infty} \exp \left\{ -\frac{\xi}{\gamma_p} \lambda_p S \right\} f_z(z) \, dz
$$

$$
= \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K \lambdaSD \lambdaSE}{\lambdaSD + \lambdaSE} \sum_{k=0}^{+\infty} \frac{\lambda_p S}{\gamma_p} \frac{1}{n!} \left( -\lambdaSD (n+K) z \right) \, dz
$$

$$
= \sum_{n=1}^{N-K} \sum_{k=0}^{+\infty} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K \lambdaSD \lambdaSE}{\lambdaSD + \lambdaSE} \frac{\lambda_p S}{\gamma_p} \frac{1}{n!} \left( -\lambdaSD (n+K) z \right) \, dz
$$

Finally, by substituting Equation (A7) into Equation (A5), $p_{(\text{SNAT})}$ in Equation (16) can be obtained.

Appendix C

Similarly, from Equation (14), we can derive $p_{(\text{SNAT})}$ as

$$
p_{(\text{SNAT}} = 1 - \Pr \left\{ C_s^{(\text{SNAT})} > R_{th} \right\}
$$

With the help of Equations (4), (5), (12) and (13), $\Pr \left\{ C_s^{(\text{SNAT})} > R_{th} \right\}$ can be obtained and the expansion is listed below as Equation (A9):

$$
\Pr \left\{ C_s^{(\text{SNAT})} > R_{th} \right\} = \Pr \left\{ \frac{\eta}{1-\alpha} |h_p| S > \frac{\gamma_p}{\gamma} \left( |h_p| S - \beta |h_p| E \right) \right\}
$$

$$
= \Pr \left\{ \frac{\Gamma_{h,A}}{P_B} < |h_p| S < \frac{\Gamma_{h,S}}{P_B} \right\}
$$

$$
+ \Pr \left\{ \frac{\eta}{1-\alpha} \frac{\Gamma_{h,S}}{N_0} \left( |h_p| S - \beta |h_p| E \right) > \beta - 1 \right\}
$$

$$
= \Pr \left\{ |h_p| S > \frac{\xi}{\gamma_p} \frac{\gamma_A}{\gamma_p} \left( \frac{\Gamma_{h,A}}{\gamma_p} < |h_p| S < \frac{\Gamma_S}{\gamma_p} \right) \right\}
$$

$$
+ \Pr \left\{ Z > \frac{\xi}{\Gamma_S} \right\}
$$

$$
= \Pr \left\{ |h_p| S > \frac{\xi}{\gamma_p} \frac{\gamma_A}{\gamma_p} \left( \frac{\Gamma_{h,S}}{\gamma_p} < |h_p| S < \frac{\Gamma_S}{\gamma_p} \right) \right\}
$$

$$
+ \Pr \left\{ Z > \frac{\xi}{\Gamma_S} \right\}
$$
Then, by substituting Equation (A3) into Equation (A9) and using the Maclaurin series of the term $e^{-\frac{\xi}{\gamma^{p^2}}} = \sum_{k=0}^{\infty} (-1)^k \frac{\mu^k}{k! \gamma^{p^2}}$ [55], with the help of [44], Equation (3.381.6), we have

$$\Pr \left\{ c^{(SNAT)} > R_{th} \right\} = \int_{\frac{\xi}{\gamma_T}}^{+\infty} \Pr \left\{ \frac{\xi}{\gamma_T} < \left| h_{PS_{n}} \right|^2 < \frac{\xi}{\gamma_T} \right\} f_{Z}(z) \, dz$$

$$+ \int_{\frac{\xi}{\gamma_T}}^{+\infty} \Pr \left\{ \left| h_{PS_{n}} \right|^2 > \frac{\xi}{\gamma_T} \right\} f_{Z}(z) \, dz$$

$$- \int_{\frac{\xi}{\gamma_T}}^{+\infty} \Pr \left\{ \left| h_{PS_{n}} \right|^2 > \frac{\xi}{\gamma_T} \right\} f_{Z}(z) \, dz$$

$$+ \int_{\frac{\xi}{\gamma_T}}^{+\infty} \Pr \left\{ \left| h_{PS_{n}} \right|^2 > \frac{\xi}{\gamma_T} \right\} f_{Z}(z) \, dz$$

(A10)

$$= \sum_{n=1}^{N-K} \sum_{k=0}^{+\infty} \binom{N}{K} \binom{N-K}{n} (-1)^n k! \lambda_{SD} \lambda_{SE} \left( \frac{\Delta_{PS}}{\gamma_T^2} \right)^k \left( \frac{\xi}{\gamma_T} \right)^{-\frac{k}{2}} \left[ \lambda_{SD} (n + K) \right]^{\frac{k}{2} - 1}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\gamma_T} \lambda_{SD}(n+K) W_{-\frac{1}{2} \frac{1}{\gamma_T}} \left[ \frac{\xi}{\gamma_T} \lambda_{SD} (n + K) \right]}$$

$$- \sum_{n=1}^{N-K} \sum_{k=0}^{+\infty} \binom{N}{K} \binom{N-K}{n} (-1)^n k! \lambda_{SD} \lambda_{SE} \left( \frac{\Delta_{PS}}{\gamma_T^2} \right)^k \left( \frac{\xi}{\gamma_T} \right)^{-\frac{k}{2}} \left[ \lambda_{SD} (n + K) \right]^{\frac{k}{2} - 1}$$

$$\times e^{-\frac{1}{2} \frac{\xi}{\gamma_T} \lambda_{SD}(n+K) W_{-\frac{1}{2} \frac{1}{\gamma_T}} \left[ \frac{\xi}{\gamma_T} \lambda_{SD} (n + K) \right]}$$

$$+ \sum_{n=1}^{N-K} \binom{N}{K} \binom{N-K}{n} (-1)^n \frac{K \lambda_{SD} \lambda_{SE}}{\lambda_{SD} + \lambda_{SE}} e^{-\left[ \frac{\Delta_{PS}}{\gamma_T^2} \right] + \frac{\xi}{\gamma_T} \lambda_{SD}(n+K)}$$

Finally, by substituting Equation (A10) into Equation (A8), we have $P_{sop}^{(SNEH)}$ in Equation (17).
References

1. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE Access 2018, 6, 3619–3647. [CrossRef]

2. Agiwal, M.; Roy, A.; Saxena, N. Next generation 5G wireless networks: A comprehensive survey. IEEE Commun. Surv. Tutor. 2016, 18, 1617–1655. [CrossRef]

3. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805. [CrossRef]

4. Li, Q.; Feng, G.; Leung, V. Optimal Transmission Policies for Relay Communication Networks with Ambient Energy Harvesting Relays. IEEE J. Sel. Areas Commun. 2016, 34, 3754–3768.

5. Sudevalayam, S.; Kulkarni, P. Energy Harvesting Sensor Nodes: Survey and Implications. IEEE Commun. Surv. Tutor. 2011, 13, 443–461. [CrossRef]

6. Rajesh, R.; Sharma, V.; Viswanath, P. Capacity of gaussian channels with energy harvesting and processing cost. IEEE Trans. Inf. Theory 2014, 60, 2563–2575. [CrossRef]

7. Alevizos, P.N.; Bletsas, A. Sensitive and nonlinear far-field RF energy harvesting in wireless communications. IEEE Trans. Wirel. Commun. 2018, 17, 3670–3685. [CrossRef]

8. Bi, S.; Ho, C.K.; Zhang, R. Wireless powered communication: Opportunities and challenges. IEEE Commun. Mag. 2015, 53, 117–125. [CrossRef]

9. Bi, S.; Zeng, Y.G.; Zhang, R. Wireless powered communication networks: An overview. IEEE Trans. Wirel. Commun. 2016, 23, 10–18. [CrossRef]

10. Tabassum, H.; Hossain, E.; Ogundipe, A.; Kim, D.I. Wireless powered cellular networks: Key challenges and solution techniques. IEEE Commun. Mag. 2015, 53, 63–71. [CrossRef]

11. Niyato, D.; Kim, D.I.; Miso, M.; Han, Z. Wireless powered communication networks: Research direction and technological approaches. IEEE Wireless Commun. 2017, 24, 88–97. [CrossRef]

12. Ramezani, P.; Jamalipour, A. Toward the evolution of wireless powered communication networks for the future internet of things. IEEE Netw. 2017, 31, 62–69. [CrossRef]

13. Chen, H.; Zhai, C.; Li, Y.; Vucetic, B. Cooperative strategies for wireless-powered communications: An comprehensive survey. IEEE Wirel. Commun. 2018, 25, 1–8. [CrossRef]

14. Ortega, Y.R.; Upadhyay, P.K.; da Costa, D.B.; Bithas, P.S.; Kanatas, A.G.; Dias, U.S.; de Sousa Junior, R.T. Joint effect of jamming and noise on the secrecy outage performance of wiretap channels with feedback delay and multiple antennas. IEEE Trans. Emerg. Telecommun. Technol. 2017. [CrossRef]

15. Bloch, M.; Barros, J. Physical-Layer Security: From Information Theory to Security Engineering; Cambridge University Press: Cambridge, UK, 2011.

16. Rodriguez, L.J.; Tran, N.H.; Duong, T.Q.; Le-Ngoc, T.; Elkashlan, M.; Shetty, S. Physical layer security in wireless cooperative relay networks: State of the art and beyond. IEEE Commun. Mag. 2015, 53, 32–39. [CrossRef]

17. Hamamreh, J.M.; Furqan, H.M.; Arslan, H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Commun. Surv. Tutor. 2019, 21, 1773–1828. [CrossRef]

18. Lei, H.; Dai, Z.; Park, K.; Lei, W.; Pan, G.; Alouini, M. Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems. IEEE Trans. Commun. 2018, 66, 6384–6395. [CrossRef]

19. Lei, H.; Xu, M.; Ansari, I.S.; Pan, G.; Qaraqe, K.A.; Alouini, M. On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection. IEEE Trans. Green Commun. Netw. 2017, 1, 192–203. [CrossRef]

20. Lee, K.; Lim, J.-T.; Choi, H.-H. Impact of Outdated CSI on the Secrecy Performance of Wireless-Powered Untrusted Relay Networks. IEEE Trans. Inf. Forensics Secur. 2019, 15, 1423–1433. [CrossRef]

21. Sun, X.; Yang, W.; Cai, Y.; Xiang, Z.; Tang, X. Secure transmissions in millimeter wave SWIPT UAV-based relay networks. IEEE Wirel. Commun. Lett. 2019, 8, 785–788. [CrossRef]

22. Ng, D.; Lo, E.; Schober, R. Robust beamforming for secure communication in systems with wireless information and power transfer. IEEE Trans. Wirel. Commun. 2014, 13, 4599–4615. [CrossRef]

23. Pan, G.; Tang, C.; Li, T.; Chen, Y. Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems. IEEE Trans. Commun. 2015, 63, 3423–3433. [CrossRef]
24. Shi, Q.; Xu, W.; Wu, J.; Song, E.; Wang, Y. Secure beamforming for MIMO broadcast with wireless information and power transfer. *IEEE Trans. Wirel. Commun.* 2015, 14, 2841–2853. [CrossRef]
25. Liu, W.; Zhou, X.; Durrani, S.; Popovski, P. Secure communication with a wireless powered friendly jammer. *IEEE Trans. Wirel. Commun.* 2016, 15, 401–415. [CrossRef]
26. Moon, J.; Lee, H.; Song, C.; Lee, I. Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer. *IEEE Trans. Commun.* 2017, 65, 764–774. [CrossRef]
27. Shafie, A.E.; Niyato, D.; Al-Dhahir, N. Security of an ordered-based distributive jamming scheme. *IEEE Wirel. Commun. Lett.* 2017, 21, 72–75. [CrossRef]
28. Li, B.; Fei, Z.; Chen, H. Robust artificial noise-aided secure beamforming in wireless powered non-regenerative relay networks. *IEEE Access* 2016, 4, 7921–7929. [CrossRef]
29. Zhao, M.; Wang, X.; Feng, S. Joint power splitting and secure beamforming design in the multiple non-regenerative wireless-powered relay networks. *IEEE Commun. Lett.* 2015, 19, 1540–1543. [CrossRef]
30. Xing, H.; Wong, K.K.; Nallanathan, A.; Zhang, R. Wireless powered cooperative jamming for secrecy multi-AF relaying networks. *IEEE Trans. Wirel. Commun.* 2016, 15, 7971–7984. [CrossRef]
31. Nguyen, N.P.; Duong, T.Q.; Ngo, H.Q.; Hadzi-Velkov, Z.; Shu, L. Secure 5G wireless communications: A joint relay selection and wireless power transfer approach. *IEEE Access* 2016, 4, 3349–3359. [CrossRef]
32. Vo, V.N.; Nguyen, T.G.; So-In, C.; Baig, Z.A.; Sanguanpong, S. Secrecy outage performance analysis for energy harvesting sensor networks with a jammer using relay selection strategy. *IEEE Access* 2018, 6, 23406–23419.
33. Wang, Y.; Yang, W.; Shang, X.; Hu, J.; Huang, Y.; Cai, Y. Energy-efficient secure transmission for wireless powered internet of things with multiple power beacons. *IEEE Access* 2018, 6, 75086–75098. [CrossRef]
34. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Secure multiuser scheduling in downlink dual-hop regenerative relay networks over Nakagami-m fading channels. *IEEE Trans. Wirel. Commun.* 2016, 15, 8009–8024. [CrossRef]
35. Yang, M.; Guo, D.; Huang, Y.; Duong, T.Q.; Zhang, B. Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks. *IEEE Trans. Commun.* 2016, 64, 5189–5202. [CrossRef]
36. Zhang, J.; Pan, G.; Xie, Y. Secrecy analysis of wireless-powered multi-antenna relaying system with nonlinear energy harvests and imperfect CSI. *IEEE Trans. Green Commun. Netw.* 2018, 2, 460–470. [CrossRef]
37. Wang, D.; Negra, R. Design of a dual-band rectifier for wireless power transmission. In Proceedings of the 2013 IEEE Wireless Power Transfer (WPT), Perugia, Italy, 15–16 May 2013.
38. Le, T.; Mayaram, K.; Fiez, T. Efficient far-field radio frequency energy harvesting for passively powered sensor networks. *IEEE J. Solid-State Circuits* 2008, 43, 1287–1302. [CrossRef]
39. Boshkovska, E.; Ng, D.W.K.; Dai, L.; Schober, R. Power-efficient and secure WPCNs with hardware impairments and non-linear EH circuit. *IEEE Trans. Commun.* 2018, 66, 2642–2657. [CrossRef]
40. Clerckx, B.; Zhang, R.; Schober, R.; Ng, D.W.K.; Kim, D.I.; Poor, H.V. Fundamentals of wireless information and power transfer: From RF energy harvester models to signal and system designs. *IEEE J. Sel. Areas Commun.* 2019, 37, 4–33. [CrossRef]
41. Niu, H.; Guo, D.; Huang, Y.; Zhang, B. Robust energy efficiency optimization for secure MIMO SWIPT systems with non-linear EH models. *IEEE Commun. Lett.* 2017, 21, 2610–2613. [CrossRef]
42. Fan, L.; Lei, X.; Yang, N.; Duong, T.Q.; Karagiannidis, G.K. Secrecy cooperative networks with outdated relay selection over correlated fading channels. *IEEE Trans. Veh. Technol.* 2017, 68, 7599–7603. [CrossRef]
43. Chen, Z.; Hadley, L.; Ding, Z.; Dai, X. Improving secrecy performance of a wirelessly powered network. *IEEE Trans. Commun.* 2017, 65, 4996–5008. [CrossRef]
44. Mekikis, P.-V.; Antonopoulos, A.; Kartsakli, E.; Lalos, A.S.; Alonso, L.; Verikoukis, C. Information Exchange in Randomly Deployed Dense WSNs with Wireless Energy Harvesting Capabilities. *IEEE Trans. Wirel. Commun.* 2016, 15, 3008–3018. [CrossRef]
45. Paing, T.; Shin, J.; Zane, R.; Popovic, Z. Resistor emulation approach to low-power RF energy harvesting. *IEEE Trans. Power Electron.* 2008, 23, 1494–1501. [CrossRef]
46. Zhou, X.; Zhang, R.; Ho, C.K. Wireless information and power transfer: Architecture design and rate-energy tradeoff. *IEEE Trans. Commun.* 2013, 63, 4754–4767. [CrossRef]
47. Shinohara, N. *Wireless Power Transfer via Radiowaves*; Wiley: Hoboken, NJ, USA, 2014.
49. Kang, X.; Liang, Y.; Yang, J. A new spectrum sharing paradigm for wireless-powered IoT devices. *IEEE Trans. Wirel. Commun.* 2018, 17, 6335–6347. [CrossRef]

50. Huang, Y.; Al-Qahtani, F.S.; Duong, T.Q.; Wang, J. Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. *IEEE Trans. Commun.* 2015, 63, 2959–2971. [CrossRef]

51. Li, M.; Yin, H.; Huang, Y.; Wang, Y. Impact of correlated fading channels on cognitive relay networks with generalized relay selection. *IEEE Access* 2017, 6, 6040–6047. [CrossRef]

52. Dong, Y.; Hossain, M.J.; Cheng, J. Performance of wireless powered amplify and forward relaying over Nakagami fading channels with nonlinear energy harvester. *IEEE Wirel. Commun. Lett.* 2016, 20, 672–675. [CrossRef]

53. Boshkovska, E.; Ng, D.W.K.; Zlatanov, N.; Schober, R. Practical non-linear energy harvesting model and resource allocation for SWIPT systems. *IEEE Wirel. Commun. Lett.* 2015, 19, 20822–22085. [CrossRef]

54. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 7th ed.; Academic: New York, NY, USA, 2007.

55. Do, N.T.; Costa, D.B.D.; Duong, T.Q.; Ng, V.; Bao, Q.; An, B. Exploiting direct links in multiuser multirelay SWIPT cooperative networks with opportunistic scheduling. *IEEE Trans. Wirel. Commun.* 2017, 16, 5410–5427. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).