Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 02, June 2025.

SECURING WIRELESS COMMUNICATIONS WITH ENERGY HARVESTING AND MULTI-ANTENNA DIVERSITY

Nguyen Quang Sang[1], Tran Cong Hung[2], Tran Trung Duy[1], Minh Tran[3] and Byung Seo Kim[4]

(Received: 29-Nov.-2024, Revised: 19-Jan.-2025, Accepted: 10-Feb.-2025)

ABSTRACT

This paper presents a secure wireless communication system that integrates Physical Layer Security (PLS) with Energy Harvesting (EH) to enhance both data confidentiality and network sustainability. The proposed system uniquely employs Maximal Ratio Combining (MRC) and Selection Combining (SC) techniques at the multi-antenna destination node D, which is a novel approach in EH-driven PLS systems. The system model features a source node S, powered by energy harvested from spatially distributed power stations, a multi-antenna destination node D and an eavesdropper node E within the communication range. A time-switching protocol allows the source node S to alternate between energy harvesting and secure data transmission. To improve signal quality and security, the destination node D employs Maximal Ratio Combining (MRC) and Selection Combining (SC) techniques to mitigate fading and eavesdropping risks. Analytical expressions for the Signal-to-Noise Ratios (SNRs) at the destination and eavesdropper are derived, along with the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) of these SNRs under block Rayleigh fading. We also provide an exact formulation for Secrecy Outage Probability (SOP), quantifying the likelihood of information leakage under different system configurations. The model is validated through Monte Carlo simulations, confirming the accuracy of the theoretical analysis. Simulation results highlight the impact of key parameters—energy harvesting efficiency η, time- switching parameter α, number of antennas M , number of beacon nodes N and the power of beacon nodes—on Secrecy Outage Probability (SOP), offering valuable insights for optimizing secure and energy- efficient communication in wireless networks. An asymptotic analysis is also provided to characterize system performance at high SNR.

KEYWORDS

Physical layer security, Energy harvesting, Selection combining, Maximal ratio combining.

1. INTRODUCTION

In wireless communications, ensuring data security is a critical concern due to the inherent vulnerability of wireless channels to eavesdropping and interference [1]. Traditional security measures often rely on cryptographic techniques at higher layers; however, these can be resource-intensive and may not be fully effective in dynamic or low-power environments. Physical Layer Security (PLS), first conceptualized in the mid-20th century and developed further in the 2000s, leverages the physical properties of the wireless channel to protect data from interception. PLS focuses on optimizing the signal-to-noise ratio and channel conditions in favor of legitimate users while limiting the information available to potential eavesdroppers. Presently, research in PLS involves integrating advanced techniques, such as beamforming, artificial noise generation and cooperative relay strategies, to enhance security while minimizing energy costs [2].

In cooperative communication systems, Decode-and-Forward (DF) and Amplify-and-Forward (AF) are two widely adopted relaying protocols that enhance the robustness and coverage of wireless networks. Studies have shown that improving the capacity in various relay models, such as the half-duplex relay channel, can further optimize these protocols by addressing specific phase-transmission

1. N. Q. Sang and T. T. Duy are with Posts and Telecommunications Institute of Technology, Ho Chi Minh City, Vietnam. Emails: sangnq@ptit.edu.vn and duytt@ptit.edu.vn
2. T. C. Hung is with the School of Computer Science & Engineering, The SaiGon International University, Ho Chi Minh City, Vietnam. Email: tranconghung@siu.edu.vn
3. M. Tran (Corresponding Author) is with the Advanced Intelligent Technology Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam. Email: tranhoangquangminh@tdtu.edu.vn
4. B.-S. Kim is with the Department of Software and Communications Engineering, Hongik University, Sejong, South Korea. Email: jsnbs@hongik.ac.kr

challenges [3]. In DF, the relay node decodes the received signal, processes it and then retransmits it, effectively mitigating noise but adding processing delay. This approach is particularly advantageous in scenarios where data integrity is critical [4]-[7]. On the other hand, AF relays amplify the received signal, including any noise, before forwarding it, resulting in a simpler implementation, but potentially amplifying noise as well [8]-[9]. The choice between DF and AF often depends on specific network requirements, such as the desired balance between complexity, latency and reliability [10]. Recent studies in secure cooperative communications have demonstrated the impact of DF and AF on system security and efficiency, especially in energy-constrained and eavesdropping-prone environments [11]-[15]. For example, various secure cooperative transmission protocols have been developed for two-way energy-constrained relaying networks, which improve secrecy outage and throughput performance even in the presence of multiple eavesdroppers through strategic relay and jammer selection. Notably, protocols for secure two- way communication in energy-constrained relaying networks demonstrate improved secrecy outage and throughput performance by implementing cooperative relay strategies, including relay and jammer selection to mitigate eavesdropping [16]. Combining binary jamming at relay nodes with network coding at source nodes has demonstrated improvements in outage performance by limiting eavesdroppers' ability to decode the transmitted messages in two-way relaying networks [17]. The work in [18] introduces a relay-assisted model combined with friendly interference collaboration, achieving improved secrecy performance in multi-destination transmissions.

Energy harvesting (EH) is a transformative approach to prolonging the lifespan of wireless devices by collecting energy from the environment, including sources like solar, wind and even radio-frequency (RF) signals from nearby devices or dedicated beacon nodes. In wireless systems, EH allows nodes to operate autonomously, reducing the dependency on traditional power sources. Two prevalent EH techniques are Time Switching (TS) and Power Splitting (PS) [19]-[23]. Time switching separates data and energy reception into distinct time slots, allowing devices to focus on either energy harvesting or data transmission at any moment. Power splitting, on the other hand, enables simultaneous data and energy reception by dividing the incoming signal into two paths; one for energy harvesting and the other for information processing. Hybrid protocols, such as the Hybrid Time Switching and Power Splitting-based Relaying (HTPR) protocol, have been shown to further optimize the throughput in cooperative SWIPT networks by leveraging the benefits of both approaches and using techniques like Maximum Ratio Combining (MRC) at the destination [24]. Both methods are widely researched and continue to be optimized for maximum efficiency and practical deployment in real-world wireless systems. The research demonstrates that energy harvesting with power splitting in cooperative networks can significantly enhance performance, even under complex channel conditions like Nakagamim/Rayleigh fading [25]. Recent research highlights that optimizing for user performance and handling hardware impairments in ambient backscatter systems can significantly improve system reliability and efficiency [26].

Integrating PLS and EH is highly significant in wireless communications, as it addresses both security and energy sustainability [27]-[28]. Studies on decode-and-forward full-duplex networks using power-splitting and self-energy recycling techniques underscore the balance between system security and reliability, even with eavesdroppers present [29]. By incorporating EH, nodes can continually replenish their energy, supporting the implementation of PLS without straining power resources. The integration of simultaneous wireless information and power transfer (SWIPT) in amplify-and-forward (AF) IoT networks provides a significant trade-off between security and reliability, highlighting the advantages of employing friendly jammers alongside power-splitting relaying strategies to mitigate eavesdropping risks [30]. A study on the physical layer security in SWIPT-based decode-and-forward relay networks shows that employing dynamic power splitting significantly enhances outage and secrecy performance in the presence of eavesdroppers [31]. Additionally, PLS with RF energy harvesting in SWIPT cooperative networks enhances information-transmission security and prolongs network lifetime, as discussed in recent studies [32]. The interplay between EH and friendly jammers has been shown to substantially improve both reliability and security in wireless-powered networks, especially in hostile eavesdropping environments, as demonstrated by research on cooperative jamming techniques [33]. Moreover, recent studies also highlight security and reliability enhancements in satellite-terrestrial networks, where a satellite transmits confidential information *via* multiple relay nodes, incorporating friendly jammers to improve secure transmission amidst imperfect

channel conditions [34]. To enhance system outage performance in energy harvesting-based two-way relaying protocols, relay-selection methods were proposed, demonstrating significant reliability improvements in data transmission over fading channels [35]. This combination is especially beneficial in systems where nodes operate remotely or autonomously, such as in sensor networks or IoT applications [36]. The performance analysis of time-switching energy harvesting in half-duplex sensor networks under hardware impairments reveals critical insights into outage probability and throughput, emphasizing the viability of energy-harvesting strategies in Rician fading environments [37]. The authors in [38] evaluate the secure performance of multi-hop relay networks by employing joint relay and jammer-selection strategies under imperfect channel conditions, enhancing the system's resistance to multiple eavesdroppers. In the context of cognitive radio networks, cooperative multi-hop transmission protocols can enhance secrecy performance, especially in the presence of hardware impairments, as demonstrated by analyzing the effective signal-to-interference-plus-noise ratio and deriving expressions for end-to-end secrecy outage probability [39]. Utilizing EH alongside PLS allows for sustainable, secure communication channels capable of resisting eavesdropping attempts while ensuring long-term operational viability, even in energy-limited settings. The authors in [40] highlight the impact of power beacon-assisted energy harvesting on device-to-device communication networks, particularly under the influence of co-channel interference and eavesdropping threats, offering closed-form expressions for outage and secrecy outage probabilities. The authors in [41] analyze the security and reliability of power splitting-based relaying schemes in IoT networks, revealing the advantages of dynamically adjusting power-splitting ratios to enhance system performance.

For further enhancing system performance, especially in secure and energy-harvesting-based wireless systems, the use of multiple antennas at the receiving node provides substantial advantages. Multiple antennas increase spatial diversity, which improves both reliability and security in data transmission. Techniques like Selection Combining (SC) and Maximal Ratio Combining (MRC) are commonly employed [42]-[43]. SC chooses the antenna with the highest received signal-to-noise ratio (SNR), simplifying the hardware requirements while maintaining reasonable performance gains. MRC, meanwhile, combines signals from all antennas in proportion to their SNR, resulting in maximal signal enhancement. Both techniques enhance the robustness of the communication link, with MRC often offering superior performance in environments with high interference or noise.

In this paper, we develop and analyze a wireless communication model where a source node, powered by energy harvested from nearby beacon nodes, transmits data securely to a destination node with multiple antennas. An eavesdropper node attempts to intercept the transmission, but the system's security is ensured through PLS techniques. The destination node employs SC and MRC to maximize the signal quality. We derive the security outage probability to assess the system's performance and validate our analytical results through Monte Carlo simulations in Matlab, highlighting the model's effectiveness in secure, sustainable wireless communications.

The list of important contributions of this paper is shown as follows:

1) We develop a secure wireless communication model, integrating PLS and EH, where the destination node uses multiple antennas and selection combining (SC) or maximal ratio combining (MRC) techniques to enhance signal quality.
2) We derive SOP for the system and provide detailed mathematical formulations, which are validated through Monte Carlo simulations.
3) To validate the analytical results, we conduct extensive numerical simulations, evaluating the system's performance under the effects of various parameters, including the power and number of beacon nodes, the number of antennas at the destination and the time-switching factor. Additionally, we investigate the asymptotic behavior to analyze the system's performance under high SNR conditions.

To better highlight the novelty of our work and how it differs from existing studies, we present a comparison with relevant papers in Table 1. This comparison emphasizes the unique aspects of our proposed approach, particularly in the integration of PLS with EH and the use of advanced combining techniques, like SC and MRC.

"Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity", N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and S.-W. Kim.

Table 1. Comparison between our work and previous papers in terms of novelty.

Ref. / Prop.	PLS	EH	SC and MRC
[2]	✓	X	X
[24]	X	✓	X
[25]	X	✓	X
[29]	✓	✓	X
[30]	✓	✓	X
[33]	✓	✓	X
[41]	✓	✓	X
[42]	X	✓	✓
[43]	✓	X	✓
Our study	✓	✓	✓

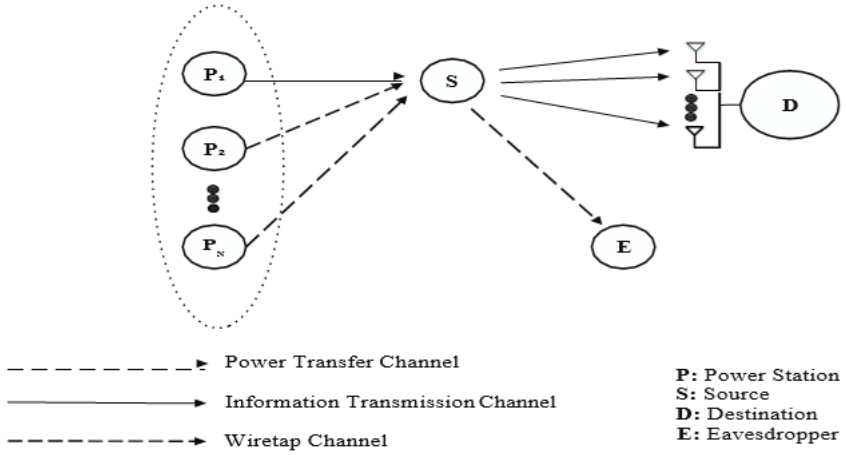

Figure 1. System model of secure wireless communication with PLS and EH, including power stations $\{P_n\}$, source S, destination D and eavesdropper E.

Organization: The remainder of this paper is organized as follows. Section 2 details the system model. In Section 3, we present the performance analysis and Section 4 follows with simulation results to evaluate system performance. Finally, Section 5 concludes the paper, summarizing key insights and potential avenues for future research.

2. SYSTEM MODEL

In this study, we consider a secure wireless communication model that integrates both PLS and EH to enhance data confidentiality and system sustainability. The system comprises four primary components: a set of power stations, denoted as $\{P_n|n = 1, \dots, N\}$, a source node S, a destination node D and an eavesdropper node E. The nodes P_n, S and E are each equipped with a single antenna, while the destination node D is equipped with M antennas.

Table 2. Time allocation for the proposed secure communication scheme.

Phase	Duration	Description
Energy Harvesting	αT	S harvests energy from N beacon nodes P_n for $n = 1,\dots,N$.
Information Transmission	$(1-\alpha)T$	S transmits data to D using SC or MRC, while E attempts to intercept the data during the same time.

2.1 Energy Harvesting from Power Stations

The source node S is powered by energy harvested from multiple power stations P_n, $n = 1, \dots, N$, spatially distributed around S. Each power station transmits energy over a dedicated Power Transfer Channel, modeled as a block Rayleigh fading channel. The harvested power at S, denoted by P_S, is given by:

Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 02, June 2025.

$$P_S = \frac{E_h}{(1-\alpha)T} = \frac{\eta\alpha T P_{\mathrm{P}} \sum_{n=1}^{N} |hP_nS|^2}{(1-\alpha)T} = \varkappa P_{\mathrm{P}} \sum_{n=1}^{N} |hP_nS|^2 \quad (1)$$

where:

- $\gamma_{P_n}S = |h_{P_n}S|^2$ is the *channel gain* between the power station P_n and the source node *S*,
- E_h represents the total energy harvested at the source node *S*,
- α is the fraction of time dedicated to energy harvesting,
- T is the total time duration of one transmission block,
- η *is the energy-conversion efficiency of the harvesting process,*
- P_{P} *is the transmit power of each power station,*
- $\kappa = \frac{\eta\alpha}{(1-\alpha)}$ *is a constant that consolidates several parameters for simplicity.*

This harvested power enables *S* to operate autonomously, sustaining secure communication without reliance on conventional power sources. A time-switching (TS) strategy is employed at *S*, alternating between energy harvesting and information processing.

2.2 Secure Information Transmission to the Destination Node and Eavesdropping Threat from a Wiretap Channel

The source node *S* transmits confidential information to the destination node *D* over the primary *Information Transmission Channel*, modeled as a block Rayleigh fading channel. This channel is subject to fading and potential eavesdropping, with an eavesdropper node *E* positioned within the vicinity of *S*, posing a significant security threat by intercepting the transmitted signal over a *Wiretap Channel*, also modeled as a block Rayleigh fading channel.

To counteract these vulnerabilities, the destination *D* is equipped with M antennas, denoted as D_m for $m = 1, \ldots, M$ and employs two diversity-combining techniques: Selection Combining (SC) and Maximal Ratio Combining (MRC). SC enhances energy efficiency by selecting the antenna with the highest signal- to-noise ratio (SNR), while MRC linearly combines signals from all antennas in proportion to their SNRs, maximizing the received signal strength. This multi-antenna setup at *D* significantly improves the system's security and resilience against fading, interference and eavesdropping.

In this phase, the received signals at the destination *D* and at the eavesdropper *E* are expressed as follows:

$$y_D^{\zeta} = \sqrt{P_S} h_{SD}^{\xi} x_S + n_D^{\zeta}$$
$$y_E = \sqrt{P_S} h_{SE} x_S + n_E \quad (2)$$

where n_D^{ζ} and n_E are zero-mean Additive White Gaussian Noise (AWGN) terms with variance N_0, $\zeta \in \{\mathrm{SC}, \mathrm{MRC}\}$ indicates the diversity-combining technique employed at *D* and *E* $\{\bullet\}$ denotes the expectation operator.

In this phase, the received signals at the destination *D* and at the eavesdropper *E* are expressed as follows:

$$y_D^{\zeta} = \sqrt{P_S} h_{SD}^{\zeta} x_S + n_D^{\zeta}$$
$$y_E = \sqrt{P_S} h_{SE} x_S + n_E \quad (3)$$

where:

- $\zeta \in \{\mathrm{SC}, \mathrm{MRC}\}$ represents the diversity-combining technique employed at the destination node *D*. Specifically, ζ can take the value "SC" for Selection Combining (SC) or "MRC" for Maximal Ratio Combining (MRC).
- x_S represents the transmitted signal from the source node *S*. Specifically, it is the data signal that is transmitted to both the destination node *D* and the eavesdropper node *E*. The signal x_S is assumed to have a unit power, i.e., $\mathbb{E}\{x_S^2\} = 1$, where $\mathbb{E}\{\cdot\}$ denotes the expectation operator.
- n_D^{ζ} *and* n_E are zero-mean Additive White Gaussian Noise (AWGN) terms with variance N_0, present at the destination node *D* and the eavesdropper node *E*, respectively.

"Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity", N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and S.-W. Kim.

The SNRs at the destination *D* and the eavesdropper *E*, which determine the ability to successfully decode the transmitted signal x_S, are given by:

$$\gamma_D^{\zeta} = \frac{P_S \gamma_{SD}^{\zeta}}{N_0}, \quad \gamma_E = \frac{P_S \gamma_{SE}}{N_0} \tag{4}$$

where γ_{SD}^{ζ} and γ_{SE} represent the effective channel gains from *S* to *D* and from *S* to *E*, respectively. This configuration allows the system to dynamically optimize its security by leveraging the SC or MRC technique at *D* to either maximize energy efficiency or signal strength, effectively countering the interception attempts by *E* and ensuring robust, secure communication.

By substituting (1) into (3), we have:

$$\gamma_D^{\zeta} = \varkappa \Psi \gamma_{SD}^{\zeta} \gamma P_N S \quad \gamma_E = \varkappa \Psi \gamma_{SE} \gamma P_N S \tag{5}$$

where $\Psi = \frac{P_p}{N_o}$ represents the ratio of transmit power from the power station to the noise power at the receiver, indicating the effectiveness of energy harvesting. The term $\gamma P_N S = \sum_{n=1}^{N} |h P_n S|^2$ signifies the cumulative channel gain from all power stations to the source node S, reflecting the overall channel quality experienced by *S*.

Considering all channels characterized by block Rayleigh fading, we can express the cumulative distribution function (CDF) and probability density function (PDF) for the squared amplitudes of the channel gains as follows:

$$F_{\gamma_{SE}}(x) = 1 - \exp(-\lambda_{SE} x) \tag{6}$$

$$f_{\gamma_{SE}}(x) = \frac{\partial F_{\gamma_{SE}}(x)}{\partial x} = \lambda_{SE} \exp(-\lambda_{SE} x) \tag{7}$$

Here, λ_{SE} represents the mean of the exponential random variable γSE. In this context, it is important to note that similar definitions apply to other channel gains, including γ_{SD} and $\gamma P_n S$, reflecting the overall channel conditions across the network.

To incorporate path loss into our model, we define the parameters as:

$$\lambda_{SE} = (d_{SE})^{\beta} \tag{8}$$

where d_{SE} denotes the link distance between nodes *S* and *E* and β is the path loss exponent.

3. PERFORMANCE ANALYSIS

3.1 Derivation of CDF for γ_{SD}^{ζ} and $\gamma P_N S$

In this sub-section, we undertake the derivation of the Cumulative Distribution Functions (CDFs) for the random variables γ_{SD}^{ζ} and $\gamma P_N S$, as delineated in Equation (4). The determination of these CDFs is critical for evaluating the performance of the system, particularly in terms of reliability and security. We will provide a comprehensive mathematical derivation of these CDFs to facilitate a deeper analysis of system performance.

3.1.1 MRC Case

In the MRC scenario, we calculate the PDF and CDF of $\gamma_{\mathrm{SD}}^{\mathrm{MRC}}$ as well as the PDF for $\gamma P_N S$. The PDF of $\gamma_{\mathrm{SD}}^{\mathrm{MRC}} = \sum_{m=1}^{M} |h_{SD_m}|^2$ can be expressed as follows [44]:

$$f_{\gamma_{\mathrm{SD}}^{\mathrm{MRC}}} = \frac{(\lambda_{SD})^M}{(M-1)!} x^{M-1} \exp(-\lambda_{SD} x) \tag{9}$$

where $\lambda_{SD} = \lambda_{SDm}$, $\forall m \in (1, 2, ..., M)$ represents the mean of the random variable (RV) $\gamma_{\mathrm{SD}}^{\mathrm{MRC}}$.

Next, based on this PDF, the CDF of $\gamma_{\mathrm{SD}}^{\mathrm{MRC}}$ can be derived as:

$$F_{\gamma_{\mathrm{SD}}^{\mathrm{MRC}}}(x) = \int_0^x f_{\gamma_{\mathrm{SD}}^{\mathrm{MRC}}}(t) dt = \frac{1}{\Gamma(M)} \times \gamma(M, \lambda_{SD} x) \tag{10}$$

where Γ(●) and γ (*a*, *b*) denote the Gamma function and the lower incomplete Gamma function, respectively.

For the PDF of $\gamma P_N S = \sum_{n=1}^{N} |hP_n S|^2$, we can express it as:

$$f_{\gamma P_N S}(x) = \frac{(\lambda_{PS})^N}{(N-1)!} x^{N-1} \exp(-\lambda_{PS} x) \tag{11}$$

where $\lambda_{PS} = \lambda_{PnS}$, $\forall n \in (1, 2, ..., N)$ is the mean of the RV $\gamma P_N S$.

3.1.2 SC Case

In this sub-section, we focus on deriving the PDF and CDF of $\gamma_{SD}^{SC} = \max\left(|h_{SD_1}|^2, |h_{SD_2}|^2, \ldots, |h_{SD_M}|^2\right)$, which can be derived as follows [8]:

$$F_{\gamma_{SD}^{SC}}(x) = (1 - \exp(-\lambda_{SD} x))^M = 1 + \sum_{m=1}^{M} (-1)^m \binom{M}{m} \exp(-m\lambda_{SD} x) \tag{12}$$

where $\lambda_{SD} = \lambda_{SDm}$, $\forall m \in (1, 2, ..., M)$ denotes the mean of the RV γ_{SD}^{SC}.

3.2 Secrecy Outage Probability (SOP) Analysis

In the domain of physical layer security, considerable attention has been devoted to the capacity to transmit confidential messages at a positive rate—termed the secrecy rate—between a source and a legitimate destination, while ensuring that an eavesdropper remains uninformed. The successful transmission hinges on the condition that the source-destination channel exhibits superior performance compared to the source-eavesdropper channel. Notably, the secrecy rate improves as the disparity in channel strengths increases, allowing for more secure communications.

The secrecy rate is mathematically expressed as [44]:

$$C_{sec} = \max(C_D - C_E, 0), \tag{13}$$

where CD = (1 − α) log2 (1 + γ_D^{ζ}) is the achievable rate at the destination and CE = (1 − α) log2 (1+ γ_E) is the rate at the eavesdropper. Here, α represents the fraction of time allocated for secure transmission, while γ_D^{ζ} and γ_E denote the signal-to-noise ratios (SNRs) at the destination and eavesdropper, respectively.

Secrecy outage occurs when the secrecy capacity drops below a specified target secrecy rate, an event that poses significant challenges for secure communication. The Secrecy Outage Probability (SOP) is defined as:

$$SOP = \Pr(C_{sec} < C_{th}) = \Pr\left(\frac{1+\gamma_D^{\zeta}}{1+\gamma_E} < \gamma_{th}\right) \tag{14}$$

where C_{th} is the threshold secrecy rate and $\gamma_{th} = 2^{\frac{C_{th}}{1-\alpha}}$ defines the critical boundary for secure transmission. This formulation underscores the relationship between channel conditions and the achievable secrecy rate, thus informing strategies for optimizing secure communication performance under varying operational scenarios.

3.3 Exact Analytical Expression for Secrecy Outage Probability (SOP)

3.3.1 SOP for MRC Case

Substituting (4) into (13), we can assert:

$$\begin{aligned} \text{SOP}^{\text{MRC}} &= \Pr\left(\frac{1 + \kappa\Psi\gamma_{SD}^{MRC}\gamma P_N S}{1 + \kappa\Psi\gamma_{SE}\gamma P_N S} < \gamma_{th}\right) = \Pr\left(\kappa\Psi\gamma_{SD}^{MRC}\gamma P_N S < \gamma_{th}\kappa\Psi\gamma_{SE}\gamma P_N S + \tilde{\gamma}_{th}\right) \\ &= \int_0^{+\infty} \underbrace{\Pr\left(\kappa\Psi\gamma_{SD}^{MRC} x < \gamma_{th}\kappa\Psi\gamma_{SE} x + \tilde{\gamma}_{th}\right)}_{\Upsilon} . f_{\gamma P_N S}(x) dx \end{aligned} \tag{15}$$

where $\tilde{\gamma}_{th} = \gamma_{th} - 1$.

From (14), Υ can be computed as follows:

$$\Upsilon = \Pr\left(\kappa\Psi\gamma_{SD}^{MRC}\gamma P_N S < \gamma_{th}\kappa\Psi\gamma_{SE}\gamma P_N S + \tilde{\gamma}_{th}\right) = 1 - \Pr\left(\gamma_{th}\kappa\Psi\gamma_{SE} x \le \kappa\Psi\gamma_{SD}^{MRC} x - \tilde{\gamma}_{th}\right)$$

"Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity", N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and S.-W. Kim.

$$= 1 - \int_0^{\frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}} F_{\gamma_{SE}}\left(\frac{y}{\gamma_{th}} - \frac{\widetilde{\gamma}_{th}}{\gamma_{th}\kappa\Psi x}\right) f_{\gamma_{SD}^{MRC}}(y)dy$$

$$= 1 - \int_0^{\frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}} \left\{1 - \exp\left(-\lambda_{SE}\left[\frac{y}{\gamma_{th}} - \frac{\widetilde{\gamma}_{th}}{\gamma_{th}\kappa\Psi x}\right]\right)\right\} \frac{\lambda_{SD}^M}{(M-1)!} y^{M-1}\exp(-\lambda_{SD}y)dy$$

$$= 1 - \frac{\lambda_{SD}^M}{(M-1)!}\int_0^{\frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}} y^{M-1} exp\,(-\lambda_{SD}y)dy + \frac{\lambda_{SD}^M}{(M-1)!}\exp\left(\frac{\lambda_{SE}\widetilde{\gamma}_{th}}{\gamma_{th}\kappa\Psi x}\right)\int_0^{\frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}} y^{M-1}\exp(-y[\frac{\lambda_{SE}}{\gamma_{th}} + \lambda_{SD}])dy \quad (16)$$

Using Equation (3.381.1) from [45], we derive:

$$\Upsilon = 1 - \frac{\gamma\left(M, \frac{\lambda_{SD}\widetilde{\gamma}_{th}}{\kappa\Psi x}\right)}{\Gamma(M)} + \left(\frac{\lambda_{SE}}{\gamma_{th}\lambda_{SD}} + 1\right)^{-M} \times \frac{\exp\left(\frac{\lambda_{SE}\widetilde{\gamma}_{th}}{\gamma_{th}\kappa\Psi x}\right)}{\Gamma(M)} \times \gamma(M, \frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}\left[\frac{\lambda_{SE}}{\gamma_{th}} + \lambda_{SD}\right]) \quad (17)$$

Finally, substituting (10) and (16) into (14) allows us to express:

$$\mathrm{SOP}^{\mathrm{MRC}} = \frac{\lambda_{PS}^N}{(N-1)!}\int_0^{+\infty} \Upsilon.\, x^{N-1}\exp(-\lambda_{PS}x)\, dx. \quad (18)$$

3.3.2 SOP for SC Case

Following a similar approach as in Equation (14), we derive SOP for the SC scenario, denoted as $\mathrm{SOP}^{\mathrm{SC}}$:

$$\mathrm{SOP}^{\mathrm{SC}} = \int_0^{+\infty} \underbrace{\Pr\left(\kappa\Psi\gamma_{SD}^{SC}x < \gamma_{th}\kappa\Psi\gamma_{SE}x + \widetilde{\gamma}_{th}\right)}_{\Xi} . f_{\gamma P_N S}(x)dx \quad (19)$$

In this formulation, Ξ is expressed in Equation (18) as:

$$\Xi = \int_0^{+\infty} F_{\gamma_{SD}^{SC}}(\gamma_{th}y + \frac{\widetilde{\gamma}_{th}}{\kappa\Psi x}) \times f_{\gamma_{SE}}(y)dy \quad (20)$$

By combining Equations (6) and (11), we can further expand Equation (19) as:

$$\Xi = 1 + \sum_{m=1}^{M}(-1)^m\lambda_{SE}\binom{M}{m}\exp(-\frac{m\lambda_{SD}\widetilde{\gamma}_{th}}{\kappa\Psi x})\int_0^{+\infty}\exp(-y[m\lambda_{SD}\gamma_{th} + \lambda_{SE}])\, dy =$$

$$1 + \sum_{m=1}^{M}(\frac{(-1)^m\lambda_{SE}}{m\lambda_{SD}\gamma_{th}+\lambda_{SE}})\binom{M}{m}\exp(-\frac{m\lambda_{SD}\widetilde{\gamma}_{th}}{\kappa\Psi x}) \quad (21)$$

where $\binom{M}{m} = \frac{M!}{m!(M-m)!}$ as the combination of *M* items taken m at a time, *M*! is the factorial of *M* and *m*! is the factorial of *m*.

Inserting Equation (20) into (18), the SOP for SC, $\mathrm{SOP}^{\mathrm{SC}}$, can be computed as:

$$\mathrm{SOP}^{\mathrm{SC}} = 1 + \sum_{m=1}^{M}(\frac{(-1)^m\lambda_{SE}}{m\lambda_{SD}\gamma_{th}+\lambda_{SE}})\frac{(\lambda_{PS})^N}{(N-1)!}\binom{M}{m} \times \int_0^{+\infty} x^{N-1}\exp(-\frac{m\lambda_{SD}\widetilde{\gamma}_{th}}{\kappa\Psi x} - \lambda_{PS}x)dx \quad (22)$$

Utilizing the integral identity (3.471.9) in [45], we obtain the final expression:

$$\mathrm{SOP}^{\mathrm{SC}} = 1 + 2\sum_{m=1}^{M}\left(\frac{(-1)^m\lambda_{SE}}{m\lambda_{SD}\gamma_{th}+\lambda_{SE}}\right)\frac{1}{(N-1)!}\binom{M}{m} \times \left(-\frac{m\lambda_{SD}\lambda_{PS}\widetilde{\gamma}_{th}}{\kappa\Psi}\right)^{\frac{N}{2}} K_N(2\sqrt{\frac{m\lambda_{SD}\widetilde{\gamma}_{th}}{\kappa\Psi\lambda_{PS}}}) \quad (23)$$

where $K_v(\cdot)$ represents the modified Bessel function of the second kind and *v* order.

4. PERFORMANCE EVALUATION THROUGH SIMULATION

In the context of modern wireless communication systems, performance evaluation through simulations is essential for validating theoretical models and ensuring practical applicability. This section presents a comprehensive analysis of the performance of the proposed system through simulations, focusing on various parameters, including Signal-to-Noise Ratio (SNR), energy-harvesting efficiency and the impact of different combining techniques, such as MRC and SC. Monte Carlo simulations, implemented using MATLAB, were employed to generate the results, providing an accurate representation of the system's behavior under various scenarios. The simulation parameters used for generating Figures 2 to 5 are detailed in Table 3, ensuring reproducibility and transparency of the presented results. By varying these parameters, we gain valuable insights into the Secrecy Outage Probability (SOP) and how it is influenced by the interplay of these factors. The results obtained from

the simulations provide a deeper understanding of the trade-offs involved in enhancing security and reliability in wireless communication systems. Following the simulations, we discuss the implications of the observed results, as illustrated in the figures, to highlight the effectiveness of our approach in mitigating eavesdropping risks.

Figure 2 presents SOP as a function of the Signal-to-Noise Ratio denoted by Ψ across different combining techniques: MRC and SC. The results indicate that MRC consistently outperforms SC, achieving lower SOP values across the entire range of Ψ. Notably, as Ψ increases, SOP decreases for both techniques, with MRC demonstrating a more significant reduction. For instance, at Ψ = 5 dB, MRC yields an SOP of approximately 0.0884, compared to SC's 0.2512. Additionally, the asymptotic behavior of the SOP reveals that MRC stabilizes at 0.0871, while SC converges to 0.2468 as SNR approaches infinity. The close alignment between simulation and analytical results underscores the reliability of the mathematical analysis. These findings highlight the enhanced security and reliability of MRC in mitigating eavesdropping risks in secure wireless communication systems.

Table 3. Simulation parameter settings for performance analysis in Figures 2–5.

Para.	**Description**	**Figure 2**	**Figure 3**	**Figure 4**	**Figure 5**
λ_{SD}	Average channel gain for Source-Destination	1	1	1	1
λ_{PS}	Average channel gain for Power Station	1	1	1	1
λ_{SE}	Average channel gain for Source-Eavesdropper	1	1	1	1
C_{th}	Secrecy capacity threshold	0.1	0.1	[0.1,0.2]	0.1
Ψ (dB)	Signal-to-Noise Ratio in dB	[−20 : 30]	5	5	5
M	Number of diversity branches in MRC/SC	4	[1 : 7]	4	4
N	Number of relay nodes	4	[2, 4]	2	2
η	Energy-harvesting efficiency	0.6	0.6	[0 : 1]	0.6
α	Power-splitting ratio	0.6	0.6	0.6	[0.1 : 0.9]
loop	Number of Monte Carlo simulation iterations	10^5	10^5	10^5	10^5

Figure 3 illustrates SOP for MRC and SC techniques, considering two distinct scenarios: $N = 2$ and $N = 4$ power beacons. The results highlight the significant impact of the number of antennas at the destination (M) on SOP performance, with higher values of M leading to improved secrecy performance across both combining techniques. The simulation results (denoted by markers) are in close agreement with the analytical models (solid lines), validating the accuracy of the derived expressions. Notably, the SOP decreases as the number of antennas increases, demonstrating the effectiveness of antenna diversity in enhancing security. Additionally, the comparison between MRC and SC shows that MRC consistently outperforms SC in terms of secrecy outage, especially when the number of antennas is large. These findings underscore the importance of antenna selection in optimizing secure communication performance in practical wireless networks, particularly in energy-constrained environments.

Figure 4 illustrates SOP as a function of the energy-harvesting factor η for both MRC and SC schemes, considering two different threshold capacities $C_{th} = 0.1$ and $C_{th} = 0.2$. As η increases, a significant reduction in SOP is observed, which indicates an improvement in the system's security performance due to more efficient energy harvesting. This behavior is attributed to the fact that higher η values provide more available energy for secure communication, thereby lowering the probability of secrecy outage. However, after reaching a certain threshold of η, the SOP curve begins to level off, signifying that further increases in energy harvesting yield marginal benefits. This phenomenon can be explained by the fact that once the energy harvested exceeds the minimal requirement for reliable transmission, additional energy does not substantially affect the SOP, leading to a saturation effect.

In terms of combining techniques, the MRC approach consistently outperforms SC, as shown by its

lower SOP values across all scenarios. This is expected, given that MRC utilizes all available signal paths to maximize the received signal strength, leading to a more reliable secure transmission compared to SC, which only selects the best available path. Furthermore, the results demonstrate that a higher threshold capacity C_{th} results in an increased SOP, implying that as the required transmission rate (or secrecy rate) becomes more stringent, the system becomes more vulnerable to secrecy outages. This trade-off underscores the importance of balancing the energy-harvesting capabilities with the required secrecy performance in practical wireless communication systems. These findings provide valuable insights into optimizing energy-harvesting techniques and combining strategies for secure and efficient communication.

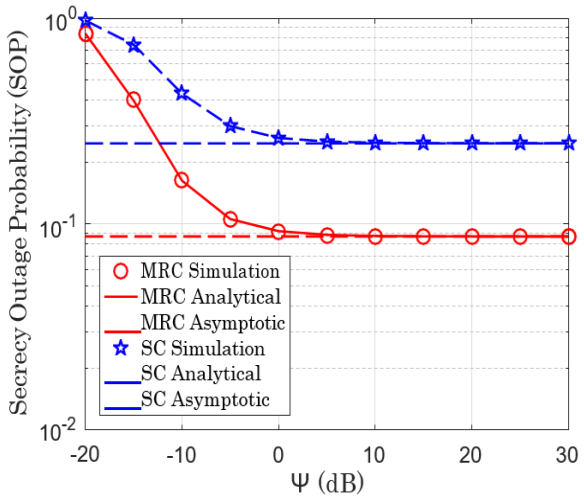

Figure 2. Secrecy outage probability as a function of the signal-to-noise ratio denoted by Ψ for MRC and SC.

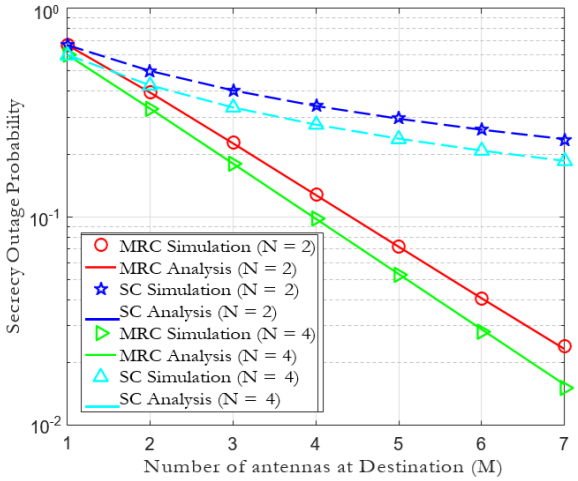

Figure 3. Secrecy outage probability (SOP) *vs.* number of antennas at the destination (*M*) for different scenarios of MRC and SC.

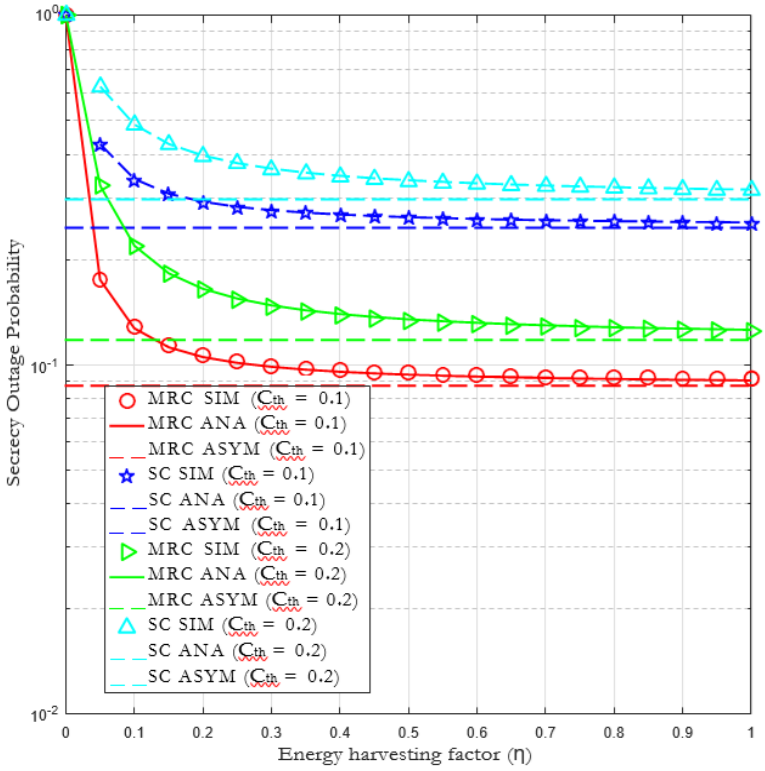

Figure 4. Impact of η and C_{th} on secrecy outage probability (SOP) for various MRC and SC configurations.

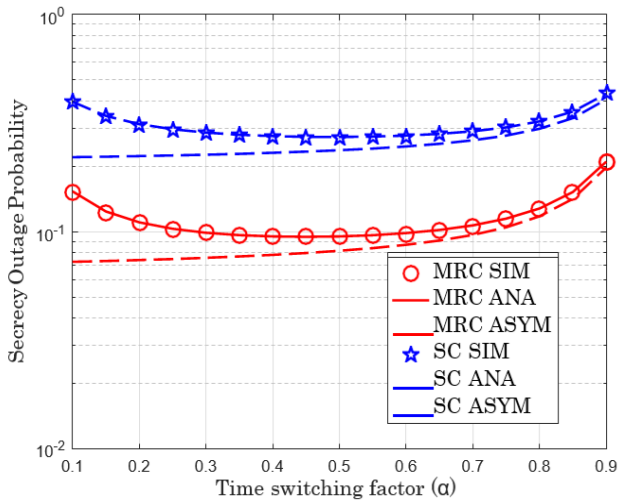

Figure 5. Effect of time switching factor (α) on secrecy outage probability for MRC and SC.

Figure 5 illustrates the impact of the time switching factor (α) on secrecy outage probability (SOP) for both MRC and SC schemes. As observed, increasing α from 0.1 results in a decrease in SOP, indicating improved system performance. This is due to the increased time available for energy harvesting at the source node (S), allowing more energy to be used for transmitting information to the destination node (D). However, when α exceeds a threshold of approximately 0.7, SOP begins to rise. This can be attributed to the fact that as α increases, more time is devoted to energy harvesting, leaving less time for signal transmission, which reduces the achievable rate at the destination node (D) and thus increases the probability of secrecy outage. This demonstrates the trade-off between energy harvesting and communication efficiency in energy-constrained systems.

5. CONCLUSION

In this paper, we analyzed the performance of a secure wireless communication system that integrates Physical Layer Security (PLS) and Energy Harvesting (EH) under various system configurations. We considered a cooperative communication model where a source node transmits data to a destination node, equipped with multiple antennas, while harvesting energy from beacon nodes in the presence of an eavesdropper. The analytical expressions for the Secrecy Outage Probability (SOP) were derived, incorporating key parameters such as the Signal-to-Noise Ratio (SNR), energy-harvesting efficiency (η), the number of interference nodes (M), the number of beacon nodes (N) and the time-switching factor (α).

Monte Carlo simulations were employed to assess the impact of these parameters on SOP. The results indicate that increasing η and Ψ enhances SOP performance by improving both the system's energy-harvesting efficiency and the quality of the received signals. The time-switching factor α plays a crucial role in balancing energy harvesting and data transmission: higher values of α prioritize energy harvesting, which may reduce the time available for data transmission, leading to increased SOP when α exceeds a certain threshold. Furthermore, an increase in the number of antennas at the destination node and the number of beacon nodes N contributes to a reduction in SOP, thereby improving both signal diversity and energy availability. In contrast, a higher number of interference nodes M tends to increase SOP, emphasizing the trade-offs in secure communication system design.

The theoretical results derived in this work were validated through simulations, demonstrating the accuracy and robustness of the proposed analytical models. These findings underscore the potential of combining EH and PLS to enhance both security and efficiency in wireless communication networks. Future work could explore adaptive time-switching strategies, multi-relay configurations and alternative energy-allocation methods to optimize system performance and security in dynamic environments. Adaptive time-switching techniques could be implemented to dynamically adjust the time allocation between energy harvesting and transmission, based on real-time environmental conditions, improving energy efficiency and communication reliability. Multi-relay configurations, leveraging energy-harvesting relays, could increase system reliability and coverage, especially in challenging environments with limited direct links. Additionally, the techniques presented in [46] and

[47], which apply convolutional neural networks (CNNs) for surface-defect detection, could potentially enhance the current system by introducing advanced machine-learning models to improve decision-making processes and system efficiency in wireless communication security. Emerging technologies, like 6G networks and machine learning offer significant potential to complement and further enhance the proposed system, especially in complex, real-world scenarios with unpredictable conditions.

REFERENCES

[1] D. Grenar, J. Frolka, K. Slavicek, O. Dostal and M. Kyselak, "Network Physical Layer Attack in the Very High Capacity Networks," Advances in Electrical and Electronic Eng., vol. 21, no. 1, pp. 37-47, Mar. 2023.

[2] W. Guo, C. Song, X. Xia, F. Hu, H. Zhao, S. Shao and Y. Tang, "Analysis of Cooperative Jamming Cancellation with Imperfect Time Synchronization in Physical Layer Security," IEEE Wireless Communications Letters, vol. 10, no. 2, pp. 335-338, Feb. 2021.

[3] Z. Al-qudah and K. A. Darabkh, "A Simple Encoding Scheme to Achieve the Capacity of Half-duplex Relay Channel," Advances in Electrical and Electronic Eng., vol. 20, no. 1, pp. 33-42, Mar. 2022.

[4] T. N. Nguyen, P. T. Tran, T. H. Q. Minh, M. Voznak and L. Sevcik, "Two-way Half Duplex Decode and Forward Relaying Network with Hardware Impairment over Rician Fading Channel: System Performance Analysis," ELEKTRONIKA IR ELEKTROTECHNIKA, vol. 24, no. 2, pp. 74-78, 2018.

[5] T. N. Nguyen, M. Tran, T.-L. Nguyen and M. Voznak, "Adaptive Relaying Protocol for Decode and Forward Full-duplex System over Rician Fading Channel: System Performance Analysis," China Communications, vol. 16, no. 3, pp. 92-102, Mar. 2019.

[6] P. T. Tin, N. T. Luan, T. N. Nguyen, M. Tran and T. T. Duy, "Throughput Enhancement for Multi-hop Decode-and-Forward Protocol Using Interference Cancellation with Hardware Imperfection," Alexandria Engineering Journal, vol. 61, no. 8, pp. 5837-5849, Aug. 2022.

[7] T. N. Nguyen, L.-T. Tu, D.-H. Tran, V.-D. Phan, M. Voznak and S. Chatzinotas, "Outage Performance of Satellite Terrestrial Full-duplex Relaying Networks with Co-channel Interference," IEEE Wireless Communications Letters, vol. 11, no. 7, pp. 1478-1482, Jul. 2022.

[8] T. N. Nguyen, T. T. Duy, P. T. Tran, M. Voznak, X. Li and H. V. Poor, "Partial and Full Relay Selection Algorithms for AF Multi-relay Full-duplex Networks With Self-energy Recycling in Non-identically Distributed Fading Channels," IEEE Transactions on Vehicular Technology, vol. 71, no. 6, pp. 6173-6188, Mar. 2022.

[9] Y. Lee, "End-to-end Error-rate Based Incremental Relaying for AF Cooperative Communications," IEEE Communications Letters, vol. 17, no. 9, pp. 1806-1809, Sep. 2013.

[10] W. Su and X. Liu, "On Optimum Selection Relaying Protocols in Cooperative Wireless Networks," IEEE Transactions on Communications, vol. 58, no. 1, pp. 52-57, Jan. 2010.

[11] R. Saini, D. Mishra and S. De, "OFDMA-based DF Secure Cooperative Communication with Untrusted Users," IEEE Communications Letters, vol. 20, no. 4, pp. 716-719, Apr. 2016.

[12] J. Mo, M. Tao and Y. Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective," IEEE Communications Letters, vol. 16, no. 6, pp. 878-881, Jun. 2012.

[13] R. Bassily and S. Ulukus, "Secure Communication in Multiple Relay Networks through Decode-and-Forward Strategies," Journal of Communications and Network, vol. 14, no. 4, pp. 352-363, Aug. 2012.

[14] H.-M.Wang, M. Luo, X.-G. Xia and Q. Yin, "Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems with Individual Power Constraint and No Eavesdropper's CSI," IEEE Signal Processing Letters, vol. 20, no. 1, pp. 39-42, Jan. 2013.

[15] C. Jeong, I.-M. Kim and D. I. Kim, "Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System," IEEE Transactions on Signal Processing, vol. 60, no. 1, pp. 310-325, Jan. 2012.

[16] S. Q. Nguyen and H. Y. Kong, "Improving Secrecy Outage and Throughput Performance in Two-way Energy-Constrained Relaying Networks under Physical Layer Security," Wireless Personal Communications, vol. 96, pp. 6425-6457, May 2017.

[17] S. Q. Nguyen and H. Y. Kong, "Combining Binary Jamming and Network Coding to Improve Outage Performance in Two-way Relaying Networks under Physical Layer Security," Wireless Personal Communications, vol. 85, pp. 2431-2446, July 2015.

[18] L. Liang, X. Li, H. Huang, Z. Yin, N. Zhang and D. Zhang, "Securing Multi-destination Transmissions with Relay and Friendly Interference Collaboration," IEEE Internet of Things Journal, vol. 11, no. 10, pp. 18782-18795, May 2024.

[19] X. Zhou, R. Zhang and C. K. Ho, "Wireless Information and Power Transfer: A Dynamic Power Splitting Approach," IEEE Transactions on Communications, vol. 61, no. 9, pp. 3991-4003, Sep. 2013.

[20] R. Jiang, K. Xiong, P. Fan, Y. Zhang and Z. Zhong, "Power Minimization in SWIPT Networks with

Coexisting Power-Splitting and Time-switching Users under Non-linear EH Model," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8853-8869, DOI: 10.1109/JIOT.2019.2923977, Oct. 2019.

[21] X. Zhou, R. Zhang and C. K. Ho, "Wireless Information and Power Transfer in Multi-user OFDM Systems," IEEE Transactions on Wireless Communications, vol. 13, no. 4, pp. 2282-2294, Apr. 2014.

[22] F. K. Ojo and M. F. M. Salleh, "Throughput Analysis of a Hybridized Power-Time Splitting Based Relaying Protocol for Wireless Information and Power Transfer in Cooperative Networks," IEEE Access, vol. 6, pp. 24137-24147, DOI: 10.1109/ACCESS.2018.2828121, Apr. 2018.

[23] R. Tao, A. Salem and K. A. Hamdi, "Adaptive Relaying Protocol for Wireless Power Transfer and Information Processing," IEEE Communications Letters, vol. 20, no. 10, pp. 2027-2030, Oct. 2016.

[24] P. S. Lakshmi and M. G. Jibukumar, "A Hybrid Protocol for SWIPT in Cooperative Networks," Advances in Electrical and Electronic Eng., vol. 19, No. 1, pp. 28-41, Mar. 2021.

[25] T. N. Nguyen, M. Tran, T.-L. Nguyen, D.-H. Ha and M. Voznak, "Performance Analysis of a User Selection Protocol in Cooperative Networks with Power Splitting Protocol-based Energy Harvesting over Nakagami-m/Rayleigh Channels," Electronics, vol. 8, no. 4, 2019.

[26] M.-S. V. Nguyen and H.-P. Dang, "Exploiting Performance of Ambient Backscatter Systems in Presence of Hardware Impairment," Advances in Electrical and Electronic Eng., vol. 19, no. 4, pp. 314-321, 2021.

[27] B. C. Nguyen et al., "Cooperative Communications for Improving the Performance of Bidirectional Full-duplex System with Multiple Reconfigurable Intelligent Surfaces", IEEE Access, vol. 9, pp. 134733 - 134742, Nov. 2021.

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

[29] B. V. Minh et al., "Self-energy Recycling in DF Full-duplex Relay Network: Security-Reliability Analysis," Advances in Electrical and Electronic Eng., vol. 22, no. 2, pp. 85-95, 2024.

[30] T. N. Nguyen, D.-H. Tran, T. V. Chien, V.-D. Phan, M. Voznak, adn P. T. Tin, "Security–Reliability Trade-off Analysis for SWIPT- and AF-based IoT Networks with Friendly Jammers," IEEE Internet of Things Journal, vol. 9, no. 21, pp. 21662-21675, June 2022.

[31] V-. D. Pham et al., "A Study of Physical Layer Security in SWIPT-based Decode-and-Forward Relay Networks with Dynamic Power Splitting," Sensors, vol. 21, no. 7, Aug. 2021.

[32] T. N. Nguyen et al., "Physical Layer Security in AF-based Cooperative SWIPT Sensor Networks," IEEE Sensors Journal, vol. 23, no. 1, pp. 689-705, Jan. 2023.

[33] V. D. Phan, T. L. Nguyen, T. T. Phu and V. V. Nguyen, "Reliability-Security in Wireless-powered Cooperative Network with Friendly Jammer," Advances in Electrical and Electronic Engineering Journal, vol. 20, no. 4, pp. 584-591, Jan. 2022.

[34] W. Zeng, J. Zhang, D. W. K. Ng, B. Ai and Z. Zhong, "Two-way Hybrid Terrestrial-satellite Relaying Systems: Performance Analysis and Relay Selection," IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 7011-7023, Jul. 2019.

[35] T. N. Nguyen et al., "Performance Enhancement for Energy Harvesting Based Two-way Relay Protocols in Wireless *Ad-Hoc* Networks with Partial and Full Relay Selection Methods," *Ad Hoc* Networks, vol. 81, pp. 178-187, Mar. 2019.

[36] P. T. Tin, T. N. Nguyen, M. Tran, T. T. Trang and L. Sevcik, "Exploiting Direct Link in Two-way Half-duplex Sensor Network over Block Rayleigh Fading Channel: Upper Bound Ergodic Capacity and Exact SER Analysis," Sensors, vol. 20, no. 4, Feb. 2019.

[37] T. N. Nguyen, T. H. Q. Minh, P. T. Tran and M. Voznak, "Energy Harvesting over Rician Fading Channel: A Performance Analysis for Half-duplex Bidirectional Sensor Networks under Hardware Impairments," Sensors, vol. 81, no. 6, 2018.

[38] C. T. Dung, T. M. Hoang, N. N. Thang, M. Tran and T. T. Phuong, "Secrecy Performance of Multi-user Multi-hop Cluster-based Network with Joint Relay and Jammer Selection under Imperfect Channel State Information," Performance Evaluation, vol. 147, p. 102193, 2021.

[39] P. T. Tin, D. T. Hung, T. N. Nguyen, T. T. Duy and M. Voznak, "Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission with and without Presence of Hardware Impairments," Entropy, vol. 21, no. 2, 2019.

[40] B. V. Minh, T. H. Q. Minh, V. D. Phan and H. T. Nguyen, "D2D Communication Network with the Assistance of Power Beacon under the Impact of Co-channel Interferences and Eavesdropper: Performance Analysis," Advances in Electrical and Electronic Eng., vol. 21, no. 4, pp. 351-359, 2023.

[41] M. Tran et al., "Security and Reliability Analysis of the Power Splitting-based Relaying in Wireless Sensors Network," Sensors, vol. 24, no. 4, Feb. 2024.

[42] T. M. Hoang, X. N. Tran, B. C. Nguyen and L. T. Dung, "On the Performance of MIMO Full-Duplex Relaying System with SWIPT under Outdated CSI," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15580-15593, Dec. 2020.

[43] L. Liang, X. Li, H. Huang, Z. Yin, N. Zhang and D. Zhang, "Securing Multi-destination Transmissions

"Securing Wireless Communications with Energy Harvesting and Multi-antenna Diversity", N. Q. Sang, T. C. Hung, T. T. Duy, M. Tran and S.-W. Kim.

with Relay and Friendly Interference Collaboration," IEEE Internet of Things Journal, vol. 11, no. 10, pp. 18782-18795, Mar. 2024.

[44] H. D.-Hung, T. N. Nguyen, M. Tran, X. Li, P. T. Tran and M. Voznak, "Security Analysis of a Two-way Half-duplex Wireless Relaying Network Using Partial Relay Selection and Hybrid TPSR Energy Harvesting at Relay Nodes," IEEE Access, vol. 8, pp. 187165-187181, Oct. 2020.

[45] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series and Products, 7th Edn, ISBN: 978-0-12-373637-6, Editor: A. Jeffrey, Burlington, MA: Academic Press, 2007.

[46] D. Zhang, X. Hao, D. Wang, C. Qin, B. Zhao, L. Liang and W. Liu, "An Efficient Lightweight Convolutional Neural Network for Industrial Surface Defect Detection," Artificial Intelligence Review, vol. 56, pp. 10651-10677, March 2023.

[47] Z. Dehua, H. Xinyuan, L. Linlin, L. Wei and Q. Chunbin, "A Novel Deep Convolutional Neural Network Algorithm for Surface Defect Detection," Journal of Computational Design and Engineering, vol. 9, no. 5, pp. 1616-1632, 2022.

ملخص البحث:

تقدِّم هذه الورقة نظام اتّصالاتٍ لاسلكيةٍ آمناً يجمع بين أمان الطبقّات الفيزيائية (PLS) وحَصَاد الطّاقة (EH) لتحسين كلٍّ من سِرّية البيانات واستدامة الشّبكة. ويوظّف النّظام المقترح تجميع النّسب القصوى (MRC) وتجميع الانتقاء (SC) لعُقدة الهدف (D) متعدّدة الهوائيات، باعتبارها طريقة مبتكرة لأنظمة أمانِ الطّبقات الفيزيائية المشغَّلة بحصاد الطّاقة.

ويرتكز النّظام في نموذجهِ على عُقدة مَصْدَرٍ يتمّ تشغيلها بطاقةٍ يجري حصادُها من محطّاتِ قُدْرَةٍ موزَّعة توزيعاً حَيّزيّاً، وعُقدة هدفٍ متعدَّدة الهوائيات، وعُقدة اختراقٍ، ضمن مدى الاتّصال. ويعمل بروتوكول تبديل زمني على جعل عُقدة المصدر تتناوب بين حصاد الطّاقة والنّقل الآمن للبيانات. ولتحسين جودة الإشارة وأمانها، توظِّف عقدة الهدف تقنيات تجميع النّسب القصوى وتجميع الانتقاء للتّخفيف من مخاطر الاضمحلال والاختراق.

من ناحيةٍ أخرى، نقدّم تشكيلاً دقيقاً لاحتمالية خروج السّرّية للوصْف الكمّيّ لاحتمالية تسرُّب المعلومات تحت تشكيلاتٍ مختلفة للنّظام. وقد جرى التّحقُّق من النّموذج من خلال محاكاة مونتي كارلو، لإثبات دقّة التّحليلات النّظرية. وتُلقي نتائج المحاكاةِ الضّوءَ على المتغيّرات الأساسية (فعالية حَصاد الطّاقة، و التّبديل الزّمني، و عدد الهوائيات، و عدد العُقد العاملة كمناراتٍ وقُدْرتها) على احتمالية خروج السّرّية (SOP)، مقدِّمين بذلك تحليلاً عميقاً لأجْل تحسين أداء أنظمة اتّصالٍ لاسلكية آمنة وذات فعالية من حيث الطّاقة. كذلك قدّمْنا تحليلاً لوصفِ أداء النّظام عند نسب إشارةٍ إلى ضجيج عالية.