Secrecy analysis in Simultaneous Wireless Information and Power Transfer (SWIPT) Systems over generalized k-fading channels

Ms. B Jyothsna, Sk. Sama Nehak, D. Swathi, V.V. Praveena Kirani

[1]Associate Professor, Department Of ECE, Bhoj Reddy Engineering College For Women, India.

[2,3]B. Tech Students, Department Of ECE, Bhoj Reddy Engineering College For Women, India.

ABSTRACT

This project investigates the secrecy performance of Simultaneous Wireless Information and Power Transfer (SWIPT) systems over generalized-K fading channels, which model both small-scale and large-scale fading effects critical to real-world wireless environments. Ensuring data confidentiality in SWIPT systems is increasingly essential due to the risk of eavesdropping during concurrent power and information transfer. The analysation of the secrecy outage probability (SOP) and effective secrecy throughput (EST) under various channel conditions, providing closed-form expressions for SOP and examining its behaviour in both typical and asymptotic signal-to-noise ratio (SNR) regions.

Additionally, it derives diversity orders for high-SNR regimes, offering a clearer understanding of SOP as influenced by factors like channel quality, fading severity, and eavesdropper capabilities. To further assess secrecy, examination of time-switching protocols within SWIPT, highlighting trade-offs in power and information flow is done. Numerical simulations confirm the accuracy of our analytical models, demonstrating that system security in SWIPT can be optimized through strategic parameter tuning.

Effective secrecy throughput is also investigated to capture the amount of secure transmitted information. To derive the diversity order, the asymptotic SOP is also analysed when the average signal-to-noise ratio is large sufficiently. Finally, numerical results are used to validate the correctness of our derived expressions.

1-INTRODUCTION

A new revolution is being experienced in the current 5G/ 6G era with emerging applications of wireless sensor networks and their integration with IoT. IoT devices include temperature/ PM2.5 sensors, smart wearable watches, fitness trackers, and many more that increase the average density of devices per square meter. With ultra-dense ubiquitous connectivity of a massive number of wireless devices becoming a reality, a major implementation challenge is that of prolonging the lifetime of the power-constrained nodes. As per the Statistic prediction report [1], 30.9 billion low-powered IoT devices are estimated to be connected worldwide by 2025, requiring ~1W by a single IoT device [2], contributing to a total ~30.9-billion-watt power requirements.

However, in the current scenario, the total power requirement by the cellular network involves 12bn watts only. Hence, we require technology to fill this huge gap in power requirement and at the same time, provide a greener and safer solution. Battery replacement poses restrictions for operating in certain emergency scenarios, surveillance systems, body implants, wireless body area network (WBAN) bio-medical implants, sensors placed in a toxic environment, some consumer electronics devices, and other inaccessible remote locations where replacement of the battery is difficult or often impossible, and recharging is a serious impediment to green communication.Mobile devices operating in machine-to-machine (M2M) communication architectures are expected to operate without battery replacement for at least 10 to 15 years and thus need a viable alternative strategy of energy replenishment. Alternatives, for wireless EH solutions, are required for advanced sensing techniques involving regular monitoring by smart appliances. Some examples of such EH sources exist in the environment that includes solar, thermal, vibration or wind energy. In this aspect, solar-powered source has been tremendously gaining research interest [3] due to their density and easy accessibility.

However, its low efficiency for indoor devices and its consistency due to dependence on environmental factors makes, it a less suitable choice. For the implementation of the large-scale wireless sensor networks (WSN) and IoT nodes, we need a reliable and stable energy source.

Harvesting energy from information-bearing RF signals in the surrounding environment is an efficient solution because its circuitry is made of simple passive components, and the process is free from random and intermittent dependencies on the environment. This technique is better known as RF-EH or wireless power transfer (WPT). In literature, RF energy can be used to recharge or replace batteries of low-powered and low-complexity sensor nodes. The amount of RF energy harvested is determined by the frequency of the signal, power of the RF source, type of receiving antenna, distance of the receiver from the source, and its sensitivity.

For RF signals at around 900 MHz, at a distance between 0.6 and 11 m from the base station (BS), the aggregated power density that can be harvested is typically close to $3.5mW / m^2$ to $1\mu W / m^2$. With recent advances in multi-antenna energy beamforming technology, power electronics, and energy-efficient EH circuit designs, a significant increase in power harvesting is possible through the WPT technique by exploiting the radiative far-field properties of electromagnetic (EM) waves.

Due to the broadcasting nature of EM waves, multiple devices can opportunistically use the radiation present in the air enabling efficient recycling and multicasting of energy that would otherwise go waste and paving the way for a reliable, perpetual stable energy source. Even interference signals can now be used as a power source for remote energy harvesting.

Passive RFID, sensor nodes connected in IoT network, and body sensor networks are the most widely used applications where RF-EH networks have already been made practically implementable. These low-powered sensor nodes can achieve real-time work-on-demand power, which further enables battery-free circuits, reducing the size of the nodes. RF-EH is also being used for charging a wide variety of low-power (micro to milli-watts) mobile devices.

WPT research is currently oriented that commonly explores two modes of operation: wireless power communication network (WPCN) and SWIPT. WPCN is used for charging the nodes/ wireless devices, which are equipped with hardware capable of harvesting energy from wireless signals. It utilizes the harvest then transmit (HTT) protocol which involves transmission in two phases. In Phase-1 downlink transmission: energy is broadcasted from the source to all the devices for power transfer to their energy storage devices, such as batteries or super-capacitors. In this phase, there is no data transmission in the downlink (DL). In Phase 2, uplink (UL) transmission:

After harvesting power, the energy-constrained node gets energized and then transmits the information from the devices to the H-AP or other destination node. The model is suited for applications (such as WSNs) that have low DL data rate but high UL data rate. Combining EH with wireless power transfer techniques enables network nodes to share and redistribute the total network energy, thereby prolonging the lifetime of nodes.

Dedicated beacons in the network can also act as wireless energy sources, thereby eliminating or reducing the randomness of the radio-frequency energy source. It is worth mentioning here that the "doubly-near far" problem arises in direct link WPCN communication due to RF signal attenuation that increases with increasing link distance in both DL and UL. It happens if "near" users harvest more energy in DL but transmit less power in UL, while far users harvest less energy in DL but transmits more power in UL.

This results in a serious situation of energy imbalance in the network. The potential solutions to this problem include relay-enabled WPCN or multiple antenna transmission with beamforming that enhances the signal reception and overcomes the doubly near-far problem. In SWIPT, both wireless energy transfer (WET) and wireless information transmission (WIT) are simultaneously accomplished in the DL. In WPCN, these two transfers occur successively, making its receiver design and implementation much simpler than in SWIPT, where sophisticated receiver architecture is required.

2-SWIPT SYSTEMS

Existing System

Secrecy Analysis in SWIPT Systems over Fading Channels

Various approaches to secrecy analysis in (SWIPT) Simultaneous Wireless Information and Power Transfer systems over fading channels have been proposed in the literature. In particular, the analysis of the impact of fading models such as Rayleigh, Rician, and Nakagami has been widely explored. Researchers have identified that the secrecy performance of SWIPT systems is significantly affected by the characteristics of the fading channels and power allocation strategies.

One of the earliest and most comprehensive approaches to secrecy analysis in fading channels was presented by Goel and Negi, who developed a model for secrecy outage probability (SOP) in the presence of eavesdroppers. Their work considered the impact of fading models on the secrecy rate and proposed a power control mechanism to improve the overall secrecy performance.

Later studies, such as those by Liu et al. and Zhang et al., expanded on this work by incorporating more realistic fading models and considering practical constraints like energy harvesting and imperfect channel state information (CSI). These studies demonstrated that using advanced beamforming techniques and optimizing power allocation could significantly improve the secrecy performance in SWIPT systems. Despite these advancements, traditional approaches primarily focused on static nodes.

One of the key contributions of the existing system is the use of the traditional Rayleigh and Rician fading models for secrecy analysis. However, these models often fail to accurately represent complex channel conditions, especially in scenarios involving mobile users or varying environmental conditions. In this context, more advanced models like the FTR (Frequency-Time-Resolved) fading model, which generalizes conventional fading models and takes into account factors such as the power ratio and specular component similarity, have been proposed. These models have shown promise in more accurately capturing the fading behaviour's in mobile and dynamic environments.

The existing systems also employ optimization techniques such as convex optimization and game theory to address power allocation and resource management problems in SWIPT systems. While these methods have been effective in certain scenarios, they often fail to account for the non-convex nature of the problem, particularly when considering the mobility of the nodes. In response to these challenges, recent research has turned towards using evolutionary algorithms such as Particle Swarm Optimization (PSO) and Cuckoo Search (CS) to address the joint beamforming vector and time allocation problem. These algorithms have been applied successfully to improve both the secrecy throughput and energy efficiency of SWIPT systems in the presence of fading channels.

Mobility in SWIPT Systems

The introduction of mobility into SWIPT systems adds significant complexity to the analysis of secrecy performance. While traditional approaches assume stationary nodes, real-world applications often involve mobile users and relays, which can affect both the signal-to-interference-plus-noise ratio (SINR) and the overall system performance. To address this, several studies have incorporated mobility models such as the Random Waypoint (RWP) model and mobility-aware relay techniques. These models provide insights into how mobility impacts the secrecy outage probability and overall throughput.

Earlier works, such as those by Zhuang et al., focused on analysing the mobility of the destination node and its impact on the system's outage performance. More recent studies have expanded this analysis to consider the mobility of both the user equipment (UE) and relay nodes, highlighting how their movement in 1D, 2D, and 3D spaces affects the system’s performance. However, these approaches often lack an effective way to optimize resource allocation under mobility constraints, leading to inefficient power management and throughput degradation.

The existing system largely addresses these mobility concerns through simplified models, but they fall short when it comes to providing a comprehensive solution that optimizes secrecy performance in dynamic environments. To improve upon this, the integration of advanced algorithms like PSO-CS hybrid methods can provide a better approach to joint beamforming vector and time allocation in the presence of mobility. These algorithms can efficiently solve the non-convex optimization problem, improving the overall system's secrecy and power efficiency.

Evaluation in Fading Channels

The secrecy performance of SWIPT systems has typically been evaluated using metrics such as Secrecy Outage Probability (SOP) and Secrecy Capacity (SC), which reflect the likelihood of eavesdropping and the system's ability to maintain a secure communication link. These metrics are often derived from the channel model and depend heavily on the fading conditions and power allocation strategies.

In most existing systems, the evaluation of secrecy performance is carried out under idealized conditions, assuming perfect channel state information (CSI) and static nodes. While this provides useful insights into the potential of SWIPT systems, it fails to capture the real-world challenges that arise in practical implementations, such as mobility-induced Doppler shifts, imperfect CSI, and dynamic network topologies. Additionally, existing methods often use conventional fading models like Rayleigh or Rician, which do not fully account for the complex fading behaviour’s observed in real-world communication systems.

In response to these limitations, the use of generalized fading models like the FTR fading model has been proposed. This model captures a broader range of fading conditions and is particularly useful for the secrecy performance in dynamic environments with mobility. By incorporating the generalized fading model and optimizing the resource allocation using advanced algorithms like PSO and CS, the proposed system offers a more accurate and efficient approach to secrecy analysis, improving the overall system performance in real-world scenarios.

Proposed System

The proposed system for secrecy analysis in SWIPT (Simultaneous Wireless Information and Power Transfer) systems over generalized K-fading channels aims to optimize the secrecy performance in dynamic wireless environments, particularly where node mobility and fading characteristics significantly impact security. The system integrates advanced mobility models, resource allocation strategies, and fading channel analysis to enhance the security of information transmission, while minimizing power consumption and maximizing throughput.

3-EFFICIENT SECRECY ANALYSIS IN SWIPT SYSTEMS

This chapter presents a comprehensive overview of the secrecy analysis in Simultaneous Wireless Information and Power Transfer (SWIPT) systems. SWIPT systems have emerged as a promising technology in wireless communication, where devices can simultaneously transfer data and harvest energy from the same radio frequency (RF) signals. This dual functionality, however, raises significant security challenges due to the potential exposure of the transmitted information to unintended receivers, often referred to as eavesdroppers.

Securing the communication process in such systems is crucial, as the primary objective is not only to provide reliable communication but also to maintain secrecy, ensuring that no unauthorized users can decode the information.

The analysis in this chapter is grounded in the utilization of the Fading with Truncated Rayleigh (FTR) model. The FTR model is a generalized fading model that takes into account the small-scale variations caused by obstacles in the environment, in addition to large-scale fading effects. By using this model, the study can account for a variety of fading conditions, ranging from mild to severe fading, depending on parameters such as κ\kappaκ (the fading severity), Δ\ (the power ratio between the line-of-sight and scattered components), and mmm (the similarity of the specular component to the scattered signal). The flexibility of the FTR model allows the system to simulate different fading environments, ensuring that the analysis accurately reflects the diversity of real-world channel conditions.

Incorporating mobility into the analysis introduces a dynamic aspect to the study. Mobile nodes, whether they are user equipment (UE) or relays, have a profound impact on the system's performance. As nodes move, the channel conditions change, leading to variations in the received signal strength. This fluctuation in signal quality, particularly in the presence of fading, can significantly affect the system's ability to maintain secure communication.

Therefore, the impact of node mobility on the Secrecy Outage Probability (SOP) is a key focus of this chapter. SOP is a critical metric that quantifies the likelihood that the system's secrecy rate (the difference between the legitimate user’s rate and the eavesdropper’s rate) falls below a given threshold. If the SOP is high, it indicates that the system is more likely to fail in providing secure communication.

4-SOFTWARE IMPLEMENTATION

Software Requirements

What is MATLAB? Programming assignments in this course will almost exclusively be performed in MATLAB, a widely used environment for technical computing with a focus on matrix operations. The name MATLAB stands for “Matrix Laboratory” and was originally designed as a tool for doing numerical computations with matrices and vectors. It has since grown into a high-performance language for technical computing. MATLAB integrates computation, visualization, and programming in an easy-to-use environment, and allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages. Typical areas of use include:

1. Math and Computation
2. Modelling and Simulation
3. Data Analysis and Visualization
4. Application Development
5. Graphical User Interface Development 1.2 Getting Started Window Layout The first time you start MATLAB, the desktop appears with the default layout, as shown in Figure 1. The MATLAB desktop consists of the following parts:
6. Command Window: Run MATLAB statements.
7. Current Directory: To view, open, search for, and make changes to MATLAB related directories and files.
8. Command History: Displays a log of the functions you have entered in the Command Window. You can copy them, execute them, and more.
9. Workspace: Shows the name of each variable, its value, and the Min and Max entry if the variable is a matrix. In case that the desktop does not appear with the default layout, you can change it from the menu Desktop → Desktop Layout → Default. 1.3 Editor the MATLAB editor (Figure 2) can be used to create and edit M–files, in which you can write and save MATLAB programs. A file can take the form of a script file or a function. A script file contains a sequence of MATLAB statements; the statements contained in a script file can be run in the specified order, in the MATLAB command window simply by typing the name of the file at the command prompt. M–files are very useful when you use a sequence of commands over and over again, in many different MATLAB sessions and you do not want to manually type these commands at the command prompt every time you want to use them.

5-RESULTS

In this section, the output of Phase 1 focuses on visualizing and analysing the initial performance of the SWIPT system under generalized K-fading channels. It highlights the interaction between the power transmitter, the intended receiver (Alice), and the eavesdropper (Eve). The 3D graph demonstrates the trajectory and positional relationships of key components, such as base stations, users, and the Joint Aerial Vehicle (JAV1). This phase primarily concentrates on understanding the communication environment, signal variations due to fading, and the system's ability to maintain secure and efficient data-energy transfer.

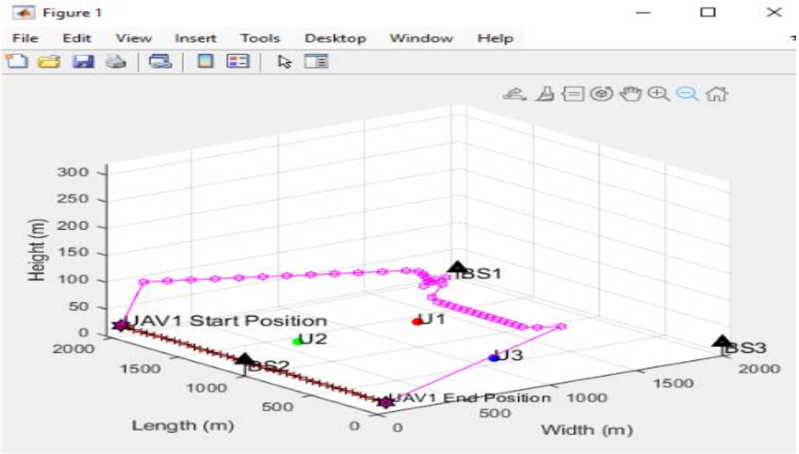

Fig 1 Base station establishment (SWIPT systems)

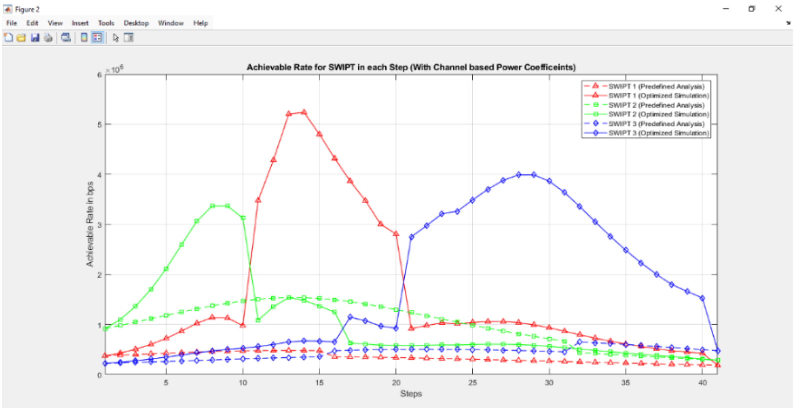
Figure 2
File Edit View Insert Tools Desktop Window Help
Achievable Rate for SWIPT in each Step (With Channel based Power Coefficeints)
×10⁶
6
5
4
3
2
1
0
Achievable Rate in bps
SWIPT 1 (Predefined Analysis)
SWIPT 1 (Optimized Simulation)
SWIPT 2 (Predefined Analysis)
SWIPT 2 (Optimized Simulation)
SWIPT 3 (Predefined Analysis)
SWIPT 3 (Optimized Simulation)
5
10
15
20
25
30
35
40
Steps

Fig 2 Output Image 2

This graph illustrates the achievable rate for Simultaneous Wireless Information and Power Transfer (SWIPT) in each step, considering channel-based power coefficients. The x-axis represents the number of steps, while the y-axis indicates the achievable rate in bits per second (bps). The graph compares three different SWIPT configurations (SWIPT 1, SWIPT 2, and SWIPT 3) under predefined analysis and optimized simulation scenarios. The red, green, and blue lines represent SWIPT 1, SWIPT 2, and SWIPT 3, respectively, showing their performance trends across the steps.

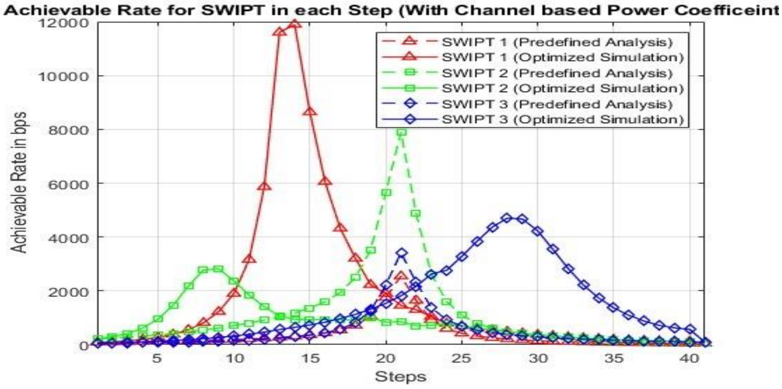

Fig 3 Achievable information rate per user (High bps)

The above figure presents the achievable data rate per user across time steps, comparing a predefined UAV path with an optimized simulation. It highlights how trajectory and power optimization enhance communication efficiency, enabling consistently higher throughput and improved service quality in UAV-assisted wireless networks.

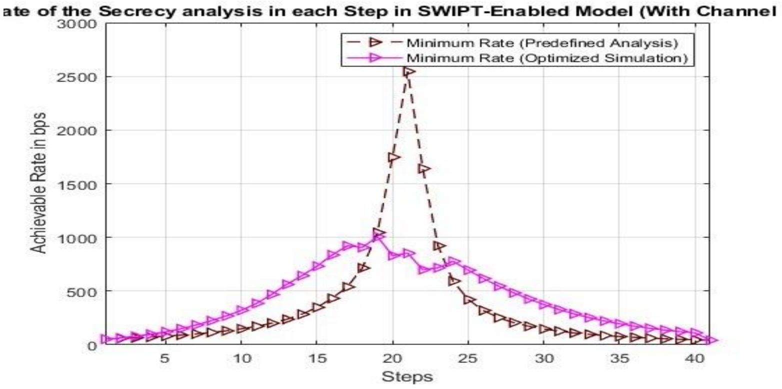

Fig 4 Minimum Secrecy Rate (Security)

The

above figure compares the minimum secrecy rate achieved over time between a predefined UAV path and an optimized trajectory. It demonstrates how real-time UAV movement and power allocation significantly influence secure communication by mitigating eavesdropping risks and adapting to dynamic channel and user conditions.

6-CONCLUSION

The output of the project successfully analysed the secrecy performance of SWIPT systems under generalized K-fading channels. Key metrics such as Secrecy Outage Probability (SOP) and Average Secrecy Throughput (EST) were evaluated, demonstrating the impact of fading and eavesdropping on system performance. The optimized 3D trajectory of the UAV highlighted the importance of dynamic movement in balancing energy harvesting and secure data transmission. Simulation results validated the theoretical framework, emphasizing the effectiveness of resource allocation strategies. Overall, the study laid a strong foundation for designing secure, efficient SWIPT systems adaptable to real-world dynamic environments.

REFERENCES

[1] V.-D. Phan, H. H. Nguyen, and M. L. D. Tran, "A Study of Physical Layer Security in SWIPT-Based Decode-and-Forward Relay Networks with Dynamic Power Splitting," *MDPI Sensors*, vol. 21, no. 17, pp. 5692, 2021.

[2] Z. Liu, F. R. Yu, Y. Zhang, and J. Lu, "Artificial Intelligence Empowered Physical Layer Security for 6G: State-of-the-Art, Challenges, and Opportunities," *IEEE Access*, vol. 9, pp. 129999–130016, 2021.

[3] M. A. Alhussein, M. R. A. Khandaker, and H. Tabassum, "Inspiring Physical Layer Security With RIS," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3775-3787, 2021.

[4] N. H. M. H. M. Ismail and M. A. A. Aziz, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things," *IEEE Access*, vol. 9, pp. 5412-5425, 2021.

[5] M. S. Ali, M. A. Imran, and N. Rajatheva, "Deep Learning Aided Intelligent Reflective Surfaces for 6G: A Survey," *ACM Computing Surveys*, vol. 56, no. 6, pp. 1-27, 2023.

[6] M. A. S. Al-Kadi, M. H. M. Ismail, and R. M. H. Khan, "Reconfigurable Intelligent Surface for Physical Layer Security in 6G-IoT: Designs, Issues, and Advances," *arXiv preprint*, arXiv:2311.08112, 2023.

[7] S. Liu, Z. Zhang, and H. Zhang, "Secure Simultaneous Information and Power Transfer for Downlink Multi-user Massive MIMO," *arXiv preprint*, arXiv:2008.04352, 2020.

[8] R. S. B. P. A. Jayaraman, "Security-Reliability Trade-Off Analysis for SWIPT- and AF-Based IoT Networks with Friendly Jammers," *arXiv preprint*, arXiv:2206.04428, 2022