TẠP CHÍ KHOA HỌC VÀ CÔNG NGHỆ ĐẠI HỌC DUY TÂN
DTU Journal of Science and Technology 5(72) (2025) 4-13
ĐẠI HỌC DUY TÂN
DUYTAN UNIVERSITY

Securing wireless networks with proactive UAV jamming

Bảo mật mạng không dây bằng UAV gây nhiễu chủ động

Tran Van Trinh[a,b], Bui Tien Lap[c], Vo Nhan Van[a,b], Nguyen Quoc Long[a,b*]
Trần Văn Trình[a,b], Bùi Tiến Lập[c], Võ Nhân Văn[a,b], Nguyễn Quốc Long[a,b*]

[a]*Faculty of Information Technology, School of Computer Science, Duy Tan University, Da Nang, 550000, Viet Nam*
[a]*Khoa Công nghệ Thông tin, Trường Khoa học Máy tính, Đại học Duy Tân, Đà Nẵng, Việt Nam*
[b]*Institute of Research and Development, Duy Tan University, Da Nang, 550000, Viet Nam*
[b]*Viện Nghiên cứu và Phát triển Công nghệ cao, Đại học Duy Tân, Đà Nẵng, Việt Nam*
[c]*DATCOM Lab, College of Technology, National Economics University, Ha Noi, Viet Nam*
[c]*DATCOM Lab, Trường Công nghệ, Đại học Kinh tế Quốc dân, Hà Nội, Việt Nam*

(Date of receiving article: 14/08/2025, date of completion of review: 20/08/2025, date of acceptance for posting: 29/08/2025)

Abstract

This research proposes and analyzes an effective anti-eavesdropping technique for relay wireless networks where direct transmission is hindered by long distances and complex terrain. To simultaneously address connectivity and security challenges, a proposed system utilizes a half-duplex decode-and-forward (HD-DF) relay and a proactive jamming unmanned aerial vehicle (UAV). The research has developed a mathematical model and derived closed-form analytical expressions for two key performance metrics: outage probability (OP) and information leakage probability (ILP). The analysis results confirm the effectiveness of the jamming UAV in improving security. Furthermore, the research also analyzes the critical trade-off between system performance and security.

Keywords: wireless communication security; half-duplex decode-and-forward relay; proactive UAV jamming; outage probability; information leakage probability.

Tóm tắt

Nghiên cứu này đề xuất và phân tích một kỹ thuật chống nghe lén hiệu quả cho mạng không dây chuyển trong điều kiện truyền tin trực tiếp bị cản trở bởi khoảng cách xa và địa hình phức tạp. Để giải quyết đồng thời vấn đề kết nối và bảo mật, một hệ thống sử dụng thiết bị chuyển tiếp hoạt động ở chế độ bán song công kết hợp phương thức giải mã và chuyển tiếp (half-duplex decode-and-forward (HD-DF)) và một máy bay không người lái (unmanned aerial vehicle (UAV)) gây nhiễu chủ động được đề xuất. Nghiên cứu đã xây dựng mô hình toán học và chứng minh các biểu thức giải tích dạng tường minh cho hai chỉ số hiệu năng chính: xác suất dừng (outage probability (OP)) và xác suất rò rỉ thông tin (information leakage probability (ILP)). Các kết quả phân tích đã khẳng định hiệu quả của UAV gây nhiễu chủ động trong việc cải thiện bảo mật. Đồng thời, nghiên cứu cũng phân tích sự đánh đổi quan trọng giữa hiệu năng hệ thống và bảo mật.

Từ khóa: bảo mật truyền thông không dây; thiết bị giải mã và chuyển tiếp bán song công; gây nhiễu chủ động bằng UAV; xác suất dừng; xác suất rò rỉ thông tin.

[*]*Corresponding author:* Nguyen Quoc Long
Email: quoclongdng@gmail.com

1. Introduction

Nowadays, the Internet of Things (IoT) has emerged as a foundational platform that drives the Fourth Industrial Revolution [1], [2]. IoT refers to a network that connects mechanical, digital, and computing devices, allowing them to automatically exchange data over wireless communication channels without the need for direct human interaction. However, due to the broadcast nature of wireless communication and the unpredictable locations of eavesdroppers (EAVs), IoT networks are highly vulnerable to information leakage and malicious attacks [3].

Although traditional upper-layer security techniques, such as encryption and user authentication, remain essential, they can be compromised when attackers possess strong computational capabilities. More importantly, these methods fail to provide protection in the physical layer, which is often the most vulnerable point in the transmission process. As a result, physical layer security (PLS) has been extensively studied as an effective approach to safeguard confidential data at its core.

One widely adopted PLS technique is proactive jamming, where dedicated jamming devices actively emit interference signals to degrade the quality of the eavesdropping channel, thus enhancing the secrecy of the legitimate link [4]. Static ground-based jammers have demonstrated certain levels of effectiveness in protecting data [5]. However, these devices suffer from limited coverage and lack mobility, making them less effective when the EAV is located far from the jamming source.

To address these limitations, unmanned aerial vehicles (UAVs) have been considered a promising solution due to their high mobility, low deployment cost, and ability to establish line-of-sight (LoS) links. UAVs are particularly suitable for complex terrains such as dense forests, mountainous areas, or remote regions [6]. When deployed as mobile proactive jammers, UAVs can actively transmit jamming signals to degrade the EAV channel and disrupt data interception attempts [7]. In practice, the location of the EAV can be detected using UAV mounted equipment such as cameras or radars, which allows precise and efficient jamming [8].

In [4], the authors investigated the effectiveness of using UAVs as friendly jamming devices to protect IoT systems from cooperative attacks between malicious jammers (MJ) and EAVs. The system was modeled with the energy harvesting and information transmission phases, utilizing NOMA technology to increase the bandwidth for legitimate IoT destinations (LID). The research findings showed that the friendly UAV helped reduce the likelihood of information leakage from EAVs and improved the system's security performance.

Motivated by these advantages, this study proposes a proactive UAV jamming technique to secure wireless links against eavesdropping in relay wireless communication networks. The proposed model is presented in detail in the system model section. In this system, the UAV transmits jamming signals to weaken the eavesdropping channel, thereby improving the secrecy performance of the data transmission, especially in scenarios involving challenging terrain or battlefield environments. Note that the secret UAV communication system has recently been studied in [4], while the key difference from this letter is that the relay devices continuously harvest power instead of receiving power from a power beacon, and there is no presence of malicious jammers. The EAV only receives the leaked information from the relay. In this article, we focus on this scenario to evaluate the system performance of a secure IoT system. The primary contributions of this article are summarized as follows:

• We propose a communication protocol for an IoT system using the half-duplex decode-and-forward (HD-DF) protocol to improve latency and enhance the signal quality of legitimate IoT destinations. Furthermore, a UAV is employed as a proactive jammer to defend against eavesdropping by the EAV.

• We derive a closed-form expression of the OP for the signals received by the legitimate IoT destination. Assessment of how external interference affects the system's performance.

• We derive a closed-form expression of the information leakage probability (ILP) for the signals received by the EAV. The impact of UAV altitude, power, and external interference on secrecy performance is also evaluated.

2. System model and communication protocol

2.1. System model

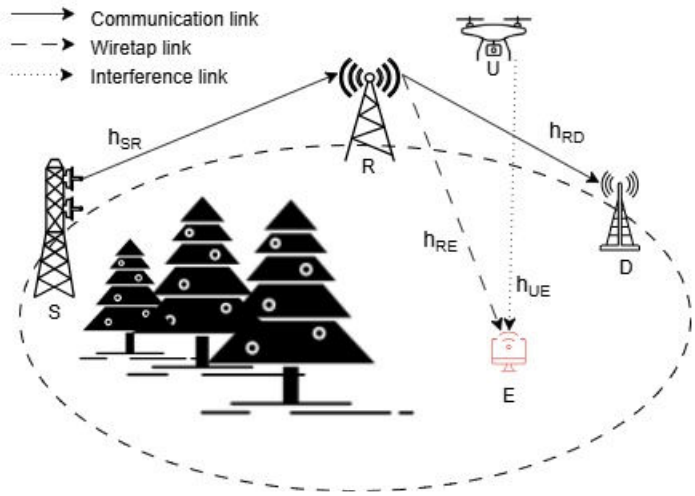

Figure 1. An illustration of an IoT system architecture with a ground base station S, a relay R, an LID D, an EAV E, and a proactive UAV jammer U against E's eavesdropping.

We consider a system model as illustrated in Figure 1, where a single ground base station (*S*) sends tactical data packets to a single legitimate IoT destination (*D*) through a half-duplex relay (*R*) strategically placed on the battlefield to extend coverage. A proactive UAV jammer (*U*) hovers at an altitude h and transmits jamming signals to the EAV (*E*) of the enemy, who is attempting to intercept the signal transmitted from R. It is assumed that the position of *E* on the ground is fixed, has been detected by *U*, and the jamming signal from *U* only affects *E* without impacting either *S*, *R*, or *D*.

In this system model, all devices, including *R*, *U*, and *D* are powered by external sources (e.g., integrated batteries, solar energy, or residential power grid) to maintain operation throughout the signal transmission and jamming process.

• Ground base station - *S*: responsible for transmitting secure signals to the relay *R*.

• Legitimate IoT destination - *D*: receives data from *S* via an *R*.

• Relay - *R*: acts as an IoT relay using HD-DF protocol. The relay improves connectivity and coverage, particularly in areas with terrain obstacles such as forests or mountains.

• Proactive UAV jammer - *U*: deployed as a mobile UAV with the capability of active jamming to counteract eavesdropping by the EAV. The use of the UAV as a proactive jammer is advantageous due to its mobility, ability to

access various areas, and capability to establish line-of-sight (LoS) links with ground devices, providing more effective jamming compared to ground-based jammers. We assume that the UAV can detect EAV's position using cameras or radar.

• EAV - *E*: a malicious agent on the ground attempting to access and steal sensitive information from the legitimate communication link between *R* and *D*.

The distance between two ground nodes *X* and *Y* and the distance from a ground node *X* to the UAV are represented, respectively, as follows:

$$d_{XY} = \sqrt{\left(x_X - x_Y\right)^2 + \left(y_X - y_Y\right)^2}\ , \qquad (1)$$

$$d_{XU} = \sqrt{\left(x_X - x_U\right)^2 + \left(y_X - y_U\right)^2 + h^2}\ , \quad (2)$$

where $\left(x_X, y_X\right), \left(x_Y, y_Y\right)$, and $\left(x_U, y_U\right)$ are the coordinates of the ground node *X*, *Y*, and *U*, respectively; and *h* is the altitude of the UAV and this altitude is assumed to be fixed or changes slowly over a given period. It is assumed that all transmission channels in the system are independent. Each channel is modeled using the Nakagami-*m* fading model with a severity parameter m_{XY} [9]. In this model, the channel power gain, $|h_{XY}|^2$, follows a Gamma distribution. Therefore, its probability density function (PDF) and cumulative distribution function (CDF) are given by [10]:

$$f_{|h_{XY}|^2}(x) = \left(\frac{m_{XY}}{\Omega_{XY}}\right)^{m_{XY}} \frac{x^{m_{XY}-1}}{\Gamma\left(m_{XY}\right)} \exp\left(-\frac{m_{XY}x}{\Omega_{XY}}\right), (3)$$

$$F_{|h_{XY}|^2}(x) = 1 - \sum_{j=0}^{m_{XY}-1} \left(\frac{m_{XY}x}{\Omega_{XY}}\right)^j \frac{1}{j!} \exp\left(-\frac{m_{XY}x}{\Omega_{XY}}\right), \quad (4)$$

where x represents an instance of the channel power gain, $\Omega_{XY} = \mathbb{E}[|h_{XY}|^2]$ is the average channel power gain for the *X*-*Y* link, m_{XY} is the Nakagami-m fading severity parameter, and $\Gamma(\cdot)$ is the Gamma function.

The general path loss between two nodes *X* and *Y* is expressed as

$$PL_{XY}\left(d_{XY}\right) = \kappa_0 \left(\frac{d_{XY}}{d_0}\right)^{\alpha_p}, \qquad (5)$$

where α_p is the path-loss exponent and κ_0 is a reference gain at distance d_0, d_{XY} is the distance between two nodes *X* and *Y*. The average path loss for all links in the system, including both ground-to-ground and air-to-ground, is described by the general model in (5). While it is acknowledged that air-to-ground channels can involve more complex models that depend on line-of-sight (LoS) or non-line-of-sight (NLoS) conditions, this paper adopts a unified model for analytical tractability. Furthermore, the small-scale fading characteristics for all channels are modeled using the Nakagami-m distribution.

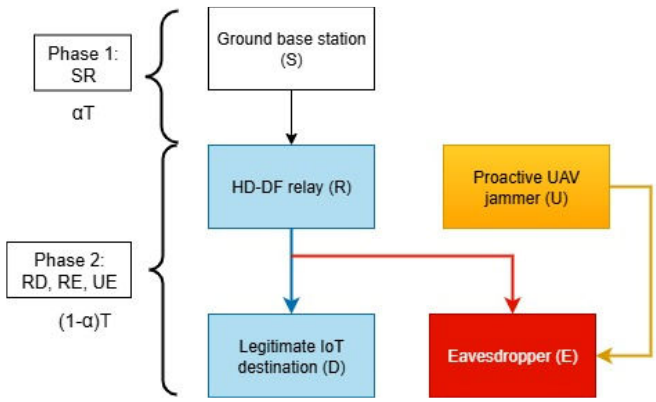

Figure 2. Proposed communication protocol with time division for information transmission, eavesdropping, and proactive jamming.

2.2. Communication protocol

We adopt a HD-DF protocol with two main phases during the total transmission time T as

• Phase 1 αT : Transmission of signals from S to R. The source node *S* transmits signals to the relay node *R*. Thus, the signal-to-interference-plus-noise ratio (SINR) at the relay is given by:

$$\gamma_{SR} = \frac{\frac{P_S |h_{SR}|^2}{PL_{SR}}}{N_0 + I_{ext}}, \quad (6)$$

where N_0 and I_{ext} represent the noise power and interference from other sources, respectively.

• Phase 2 $(1-\alpha)T$: Transmission of signals from *R* to *D* and jamming of *E* from *U*. The relay *R* uses DF techniques to forward the received signal to *D*. Therefore, the SINR at destination *D* is

$$\gamma_{RD} = \frac{\frac{P_R |h_{RD}|^2}{PL_{RD}}}{N_0 + I_{ext}}. \quad (7)$$

At the same time, *U* transmits jamming signals to counteract the EAV. It is assumed that legal devices (such as *S*, *R*, and *D*) can ignore the jamming signals of *U* due to prior synchronization information, while *E* receives both the legitimate signal from *R* and the jamming signal from *U*. When information is forwarded from *R* to *D*, it can also be overheard by *E*. Then, the instantaneous SINR at *E* is given by

$$\gamma_{RE} = \frac{\frac{P_R |h_{RE}|^2}{PL_{RE}}}{N_0 + I_{ext} + \frac{P_U |h_{UE}|^2}{PL_{UE}}}. \quad (8)$$

Therefore, the end-to-end SINRs at the destination and EAV are as follows:

$$\gamma_{E2E}^{(D)} = \min\{\gamma_{SR}, \gamma_{RD}\}, \quad (9)$$

$$\gamma_{E2E}^{(E)} = \min\{\gamma_{SR}, \gamma_{RE}\}. \quad (10)$$

2.3. Performance analysis

2.3.1. Successful transmission condition

To analyze the system performance, we consider a communication link from a transmitting node *X* to a receiving node *Y*. It is assumed that a packet of size L (bits) must be transmitted within an allocated time interval of αT . Based on the Shannon-Hartley theorem, the maximum instantaneous data rate, also known as the channel capacity, of the link from *X* to *Y* (denoted as R_{XY}) is determined by

$$R_{XY} = B \log_2(1 + \gamma_{XY}), \quad (11)$$

where *B* is the channel bandwidth, γ_{XY} is the SINR at the receiving node *Y*. To successfully transmit all *L* bits within the time interval αT, the total amount of data that the channel can carry must be greater than or equal to L. This leads to the following constraint:

$$\alpha T \cdot B \log_2(1 + \gamma_{XY}) \geq L. \quad (12)$$

From condition (12), we can derive the minimum SINR threshold required for the receiving node to successfully decode the packet

$$\gamma_{XY} \geq 2^{\frac{L}{\alpha TB}} - 1. \quad (13)$$

In this system model, *T* is the total duration of a complete transmission slot that consists of two phases. We assume that time is equally allocated to both phases; therefore, the time allocation factor $\alpha = 1/2$. In this case, the required SINR threshold $\gamma_{\text{threshold}}$ is the same for each phase and is calculated as follows:

$$\gamma_{\text{threshold}} = 2^{\frac{L}{(T/2)B}} - 1. \quad (14)$$

2.3.2. Outage probability of the legitimate link

The outage probability of the *S-D* transmission link is defined as the probability that the instantaneous SINR falls below the threshold required for successful decoding. The outage probability of the legitimate link is defined by:

$$O_{SD} = Pr\left\{\gamma_{E2E}^{(D)} < \gamma_{threshold}\right\}. \tag{15}$$

By substituting (9) into (15) and using the properties of probability, we have the following:

$$O_{SD} = Pr\left\{\min\left\{\gamma_{SR}, \gamma_{RD}\right\} < \gamma_{\text{threshold}}\right\} = 1 - \underbrace{\Pr\left\{\gamma_{SR} \geq \gamma_{\text{threshold}}\right\}}_{O_{SR}}.\underbrace{\Pr\left\{\gamma_{RD} \geq \gamma_{\text{threshold}}\right\}}_{O_{RD}}. \tag{16}$$

In particular, the probability O_{SR} is calculated as

$$O_{SR} = 1 - \Pr\left\{\gamma_{SR} < \gamma_{\text{threshold}}\right\} \tag{17}$$

By substituting (6) into (17) and applying the CDF (4) for the random variable $|h_{SR}|^2$ yields the following:

$$O_{SR} = 1 - \sum_{j=0}^{m_{SR}-1}\left(\frac{m_{SR}\sigma\gamma_{\text{threshold}}PL_{SR}}{\Omega_{SR}P_S}\right)^j \frac{1}{j!}\exp\left(-\frac{m_{SR}\gamma_{\text{threshold}}\sigma PL_{SR}}{\Omega_{SR}P_S}\right), \tag{18}$$

where $\sigma = N_0 + I_{\text{ext}}$ denotes the total noise and interference power. Similarly, the probability O_{RD} is rewritten as

$$O_{RD} = 1 - \Pr\left\{\gamma_{RD} < \gamma_{\text{threshold}}\right\}. \tag{19}$$

After the mathematical manipulations, the probability O_{RD} is obtained by

$$O_{RD} = 1 - \sum_{j=0}^{m_{RD}-1}\left(\frac{m_{RD}\sigma\gamma_{\text{threshold}}PL_{RD}}{\Omega_{RD}P_R}\right)^j \frac{1}{j!}\exp\left(-\frac{m_{RD}\gamma_{\text{threshold}}\sigma PL_{RD}}{\Omega_{RD}P_R}\right). \tag{20}$$

2.3.3. Information leakage probability of the eavesdropping link

We define the information leakage event as the probability that EAV can successfully decode the information from *R*, specifically when the SINR of the EAV is greater than or equal to the decoding threshold, i.e.,

$$I_{SE} = \Pr\left\{\gamma_{E2E}^{(E)} \geq \gamma_{\text{threshold}}\right\}. \tag{21}$$

In which, substituting (10) into (21), the probability of I_{SE} is rewritten as:

$$I_{SE} = \underbrace{\Pr\left\{\gamma_{SR} \geq \gamma_{\text{threshold}}\right\}}_{O_{SR}}.\underbrace{\Pr\left\{\gamma_{RE} \geq \gamma_{\text{threshold}}\right\}}_{I_{RE}}. \tag{22}$$

By substituting (8) into (22) and applying mathematical manipulations with the integral identities of [11], the probability of I_{RE} is derived as follows:

$$\begin{aligned} I_{RE} = {} & \sum\nolimits_{j=0}^{m_{RE}-1}\left(\frac{m_{RE}}{\Omega_{RE}}\right)^j \frac{1}{j!}\left(\frac{m_{UE}}{\Omega_{UE}}\right)^{m_{UE}} \frac{1}{\Gamma\left(m_{UE}\right)}\exp\left(-\frac{m_{RE}\gamma_{\text{threshold}}\sigma PL_{RE}}{P_R\Omega_{RE}}\right) \\ & \times\left(\frac{\gamma_{\text{threshold}}\sigma PL_{RE}}{P_R}\right)^{j-k} \sum\nolimits_{k=0}^{j}\binom{j}{k}\left(\frac{P_U\gamma_{\text{threshold}}\sigma PL_{RE}}{P_R PL_{UE}}\right)^k \frac{\Gamma\left(m_{UE}+k\right)}{\left(\frac{m_{RE}P_U\gamma_{\text{threshold}}PL_{RE}}{\Omega_{RE}P_S PL_{UE}} + \frac{m_{UE}}{\Omega_{UE}}\right)^{m_{UE}+k}}. \end{aligned} \tag{23}$$

3. Numerical results

In this section, we present numerical results to evaluate the security and reliability performance of the considered system. Specifically, we investigate the impact of external interference I_{ext}, transmit power on

both the OP and the ILP, as well as the effects of source transmit power and UAV altitude *h* on the ILP. The theoretical results are validated through Monte Carlo simulations to ensure their accuracy. Unless otherwise stated, the following system parameters are used for both analysis and simulation: a path loss exponent of α_p=2 [12]. The coordinates of the ground nodes are *S*(0,0), *R*(3,3), *D*(5,10), *E*(6,9), and the proactive UAV jammer U is located at *U*(4,4). All ground-to-ground and air-to-ground channels are modeled using Nakagami-m fading with a severity parameter $m_{SR} = m_{RD} = m_{RE} = m_{UE} = m_{fading} = 2$ and an average channel power gain $\Omega_{SR} = \Omega_{RD} = \Omega_{UE} = \Omega_{RE} = 1$. The path loss exponent is set to $\alpha_p = 2$. The bandwidth of $B = 100$ MHz, the packet of size $L = 819200$ bits and the total transmission time of $T = 1$ s, with a transmission time fraction for each phase $\alpha = 1/2$. The noise power is set to $N_0 = 1$ dB.

Figures 3 and 4 illustrate the impact of external interference I_{ext} and transmit power at S and R on the system and security performances.

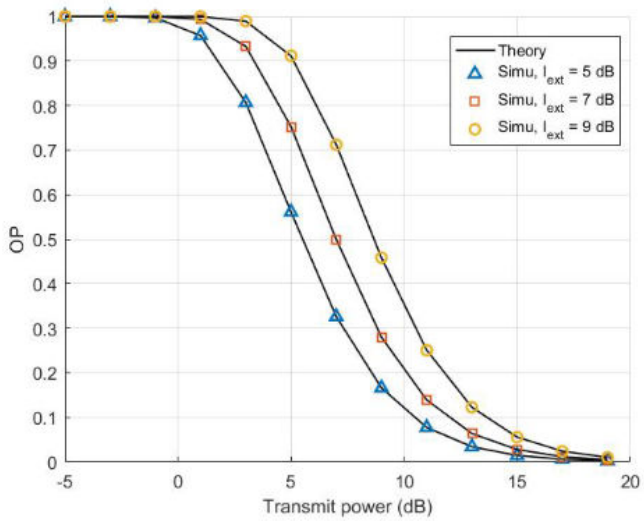

Figure 3. Impact of I_{ext} and transmit power at S and R on OP of S-D link.

Specifically, Figure 3 demonstrates that a higher level of external interference degrades system performance by increasing OP. This occurs because interference reduces the SINR at the legitimate receiver and the SINR at the relay. For instance, at a ground base station and relay's transmit power of 5 dB, increasing I_{ext} from 5 dB to 9 dB causes the OP to grow from approximately 0.57 to 0.92. In contrast, Figure 4 shows a security benefit, as the same interference significantly reduces the ILP by acting as a natural jammer against the EAV. At the same 5 dB transmit power, the ILP drops from 0.49 to 0.12 as I_{ext} increases in the same range. These results highlight a clear trade-off: a noisier communication environment diminishes system reliability while passively enhancing its security.

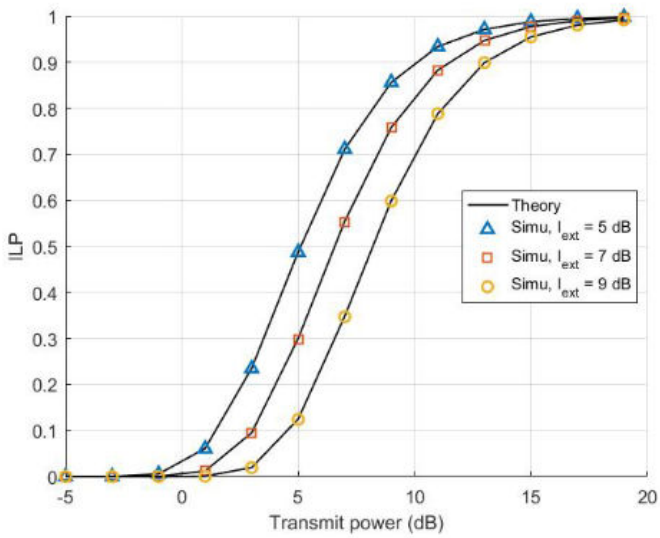

Figure 4. Impact of I_{ext} and transmit power at S and R on ILP of the S-E link with $P_u = 10$ dB, and $h = 3$ m.

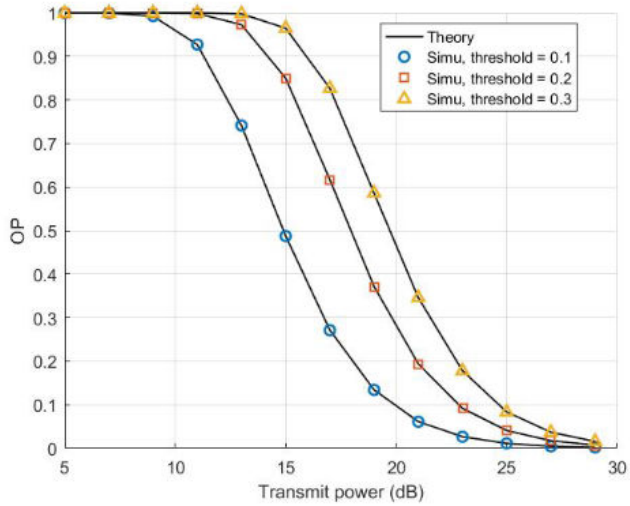

Figure 5. Impact of the threshold and transmit power at S and R on OP of the S-D link with $I_{\text{ext}} = 5$ dB, and $h = 3$ m.

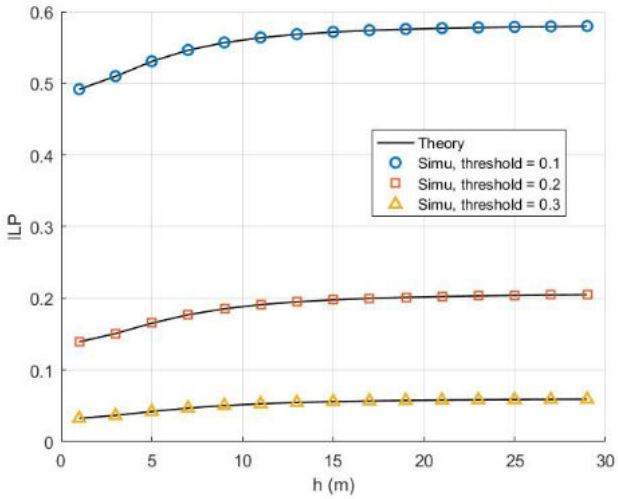

Figure 6. Impact of the threshold and UAV height on ILP of S - E link with $I_{\text{ext}} = 5$ dB, $P_u = 15$ dB, $h = 3$ m, and transmit power at S and R = 15 dB.

Figures 5 and 6 analyze the impact of the SINR decoding threshold $\gamma_{\text{threshold}}$ on system performance, revealing a fundamental trade-off between reliability and security. Figure 5 shows that for a given threshold, the OP decreases dramatically as the transmit power increases because the signal at the receiver becomes stronger. At the same time, for a fixed transmit power, the OP increases significantly as the threshold $\gamma_{\text{threshold}}$ becomes stricter (increasing from 0.1 to 0.3). This is because a higher signal quality requirement makes it more difficult for the legitimate link to meet, reducing reliability. Figure 6 analyzes the ILP as a function of the UAV's altitude. The graph shows that the ILP increases slightly as the UAV flies higher, which is due to the increased path loss of the jamming signal, reducing its protective effect. More importantly, at any given altitude, the ILP decreases dramatically as the threshold $\gamma_{\text{threshold}}$ increases. This stricter decoding requirement also poses a greater challenge for the EAV, significantly reducing the likelihood of a successful interception and thereby enhancing security. These results once again confirm a critical design trade-off: selecting a higher $\gamma_{\text{threshold}}$ enhances security (lower ILP) at the cost of reduced reliability (higher OP).

4. Conclusion

In this paper, we have successfully developed a mathematical model and derived closed-form expressions for key performance metrics, including the OP of the legitimate link and the ILP at the EAV. The accuracy of the theoretical model was validated through a close agreement between analytical and Monte Carlo simulation results. An important finding is that the numerical results indicate that changing UAV parameters, such as power and altitude, has a direct impact on improving system security. The analysis also highlights the crucial trade-off between reliability and security when changing system parameters such as the SINR threshold and the source transmit power at the ground base station and the relay.

References

[1] Yalli, S. J., Hasan, M. H. and Badawi, A. A. (2024). "Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade". *IEEE Access*, 12, 91357-91382.

[2] Villegas-Ch, W., Govea, J., Buenaño-Fernandez, D., and Mera-Navarrete, A. (2025). "Automating the Design of Scalable and Efficient IoT Architectures Using Generative Adversarial Networks and Model-Based Engineering for Industry 4.0". *IEEE Access*, 13, 112271-112291.

[3] Nguyen, A.-N., Ha, D.-B., Trương, T. V., Vo, V. N., Sanguanpong S. and So-In, C. (2023). "Secrecy Performance Analysis and Optimization for UAV-Relay-Enabled WPT and Cooperative NOMA MEC in IoT Networks". *IEEE Access*, 11, 127800-127816.

[4] Vo, V. N., So-In, C., Tran, H., and Tran, D.-D. and Pham, H. T. (2020). "Performance Analysis of an Energy-Harvesting IoT System Using a UAV Friendly Jammer and NOMA Under Cooperative Attack". *IEEE Access*, 8, 221986-222000.

[5] Ceviz, O., Sen, S. and Sadioglu, P. (2024). "A survey of security in UAVs and FANETs: Issues, threats, analysis of attacks, and solutions". *IEEE Communications Surveys & Tutorials*. 1-40. DOI: 10.1109/COMST.2024.3515051.

[6] Hussain, Y., Schlögel, R., Innocenti, A., Hamza, O., Iannucci, R., Martino S. and Havenith, H.-B. (2022). "Review on the geophysical and UAV-based methods applied to landslides". *Remote Sensing*, 14(18), 45-64.

[7] Hu, G., Si, J., Cai, Y. and Zhu, F. (2021) "Proactive eavesdropping via jamming in UAV-enabled suspicious multiuser communications". *IEEE Wireless Communications Letters*, 11(1), 3-7.

[8] Sun, G., Zheng, X., Sun, Z., Wu, Q., Li, J., Liu, Y. and Leung, V. C. (2023). "UAV-enabled secure communications via collaborative beamforming with imperfect eavesdropper information". *IEEE Transactions on Mobile Computing*, 23(4), 3291-3308.

[9] Ji, B., Li, Y., Zhou, B., Li, C., Song, K., and Wen, H. (2019). "Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting". *IEEE Access*, 7, 38738-38747.

[10] Ji, B., Li, Y., Chen, S., Han, C., Li, C., and Wen, H. (2020). "Secrecy Outage Analysis of UAV Assisted Relay and Antenna Selection for Cognitive Network Under Nakagami-m Channel". *IEEE Transactions on Cognitive Communications and Networking*, 6(3), 904-914.

[11] Gradshteyn, I. S. and Ryzhik, I. M. (2014). *Table of integrals, series, and products, Academic press*. Elsevier.

[12] Miranda, J., Abrishambaf, R., Gomes, T., Gonçalves, P., Cabral, J., Tavares, A., and Monteiro, J. (2013). "Path loss exponent analysis in wireless sensor networks: Experimental evaluation," *11th IEEE international conference on industrial informatics (INDIN), Bochum, Germany, 29-31 July 2013*. IEEE.