entropy

MDPI

Article

Security- and Reliability-Guaranteed Transmission Control of Time-Sensitive Physical Layer Security Systems

Jianye Li [1], Yunquan Dong [1,2,*] and Chengsheng Pan [1]

[1] School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China; 20211249233@nuist.edu.cn (J.L.); 003150@nuist.edu.cn (C.P.)
[2] School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei 230009, China
* Correspondence: yunquandong@nuist.edu.cn

Abstract: In this paper, we consider information transmission over a three-node physical layer security system. Based on the imperfect estimations of the main channel and the eavesdropping channel, we propose reducing the outage probability and interception probability by hindering transmissions in cases where the main channel is too strong or too weak, which is referred to as an *SNR-gated transmission control scheme*. Specifically, Alice gives up its chance to transmit a packet if the estimated power gain of the main channel is smaller than a certain threshold so that possible outages can be avoided; Alice also becomes silent if the estimated power gain is larger than another threshold so that possible interceptions at Eve can be avoided. We also consider the timeliness of the network in terms of the violation probability of the peak age of information (PAoI). We present the outage probability, interception probability, and PAoI violation probability explicitly; we also investigate the trade-off among these probabilities, considering their weight sum. Our numerical and Monte Carlo results show that by using the SNR-gated transmission control, both the outage probability and the interception probability are reduced.

Keywords: age of information; physical layer security; transmission control; outage probability; interception probability

Citation: Li, J.; Dong, Y.; Pan, C. Security- and Reliability-Guaranteed Transmission Control of Time-Sensitive Physical Layer Security Systems. *Entropy* **2023**, *25*, 1040. https://doi.org/10.3390/e25071040

Academic Editor: Shu-Chuan Chu

Received: 29 May 2023
Revised: 29 June 2023
Accepted: 6 July 2023
Published: 11 July 2023

1. Introduction

In recent years, with the wide development of wireless communications, privacy and security in wireless communication networks are receiving increased attention. The main reason is that, due to the broadcasting nature of wireless transmissions, the communication between legitimate users is vulnerable to eavesdropping by malicious third parties. To enhance security, many encryption schemes have been proposed to improve the security of wireless communications. However, these encryption schemes inevitably increase the overhead of communications [1,2]. The encryption and decryption processes also require more processing resources, which impair the timeliness of the information deliveries.

In order to address security concerns, physical layer security has been proposed as a promising technology for ensuring secure wireless communications. Note that wireless channels suffer from random fading and noises. These physical characteristics can be used to encrypt the information under transmission by reducing the amount of data that can be accessed by potential eavesdropping nodes. In [3], Wyner extended Shannon's cryptosystem in the framework of information theory in 1975. Wyner proposed the security capacity concept to evaluate the information rate that could be reliably and securely transmitted over a wireless channel. He concluded that when the eavesdropping channel quality is poorer than that of the primary channel, there exists a coding method that can provide reliable communication for the legitimate user while making it impossible for a malicious eavesdropper to decode any useful information from the captured signal. Specifically, when the instantaneous capacity of the eavesdropping channel from the source

node to the eavesdropping node is smaller than the rate of the transmitted codeword, the eavesdropping node is unable to decode the source node information; thus, the legitimate transmission remains secure. However, if the instantaneous capacity of the eavesdropping channel is higher than the rate of the source codewords, the eavesdropping node would be able to successfully decode the source node's codewords. In this case, an interception event occurs. Thus, we can reduce the *interception probability* and improve the security level by increasing the coding rate of the source. Nevertheless, *the probability of outages* (i.e., when the instantaneous capacity of the main channel is smaller than the coding rate of the source) decreases with the coding rate. In light of this contradiction, the optimal trade-off between the security and the reliability of physical layer communication has been widely investigated in [4]. Previous works, e.g., [5,6], also presented many meaningful results in the field of physical layer security. However, few works have demonstrated the ability to reduce these issues at the same time.

For communication systems, we need to consider the reliability and security of the system as well as the timeliness of communications. In previous works, the delay was widely used to measure the timeliness of communications. Recently, the emergence of AoI [7] has become a better option for precisely measuring timeliness. Specifically, the average AoI and peak AoI of systems are often used to describe the performances of real-time systems. For systems gathering information and providing status updates, however, more stringent timeliness is required. Thus, more researchers are measuring timeliness with the AoI violation probability instead of the mean AoI and peak AoI. The AoI violation probability was defined in [8] to highlight the potential damage caused by very large ages. For a single source single destination system with an FCFS serving policy, the explicit AoI violation probability has been studied in [9]. The violation probability of the peak AoI in wireless communication systems, considering practical physical layer constraints, was investigated in [10]. An approximate closed expression of the outage probability of the peak AoI exceeding a certain threshold was presented in [11]. In this paper, we investigate the timeliness of the system in terms of the violation probability of peak AoI as a measure of communication timeliness.

1.1. Motivations

Due to the contradiction between the outage probability and the interception probability, we are motivated to consider the following problem.

Can we design a transmission mechanism that simultaneously reduces the outage probability and the interception probability to some extent?

In this paper, we propose an *SNR-gated transmission control* for the source node. Specifically, the proposed method improves performance by hindering packet transmissions in slots when an outage or an interception is expected to occur. Specifically, Alice gives up its chance to transmit a packet if the estimated power gain of the main channel is smaller than a certain threshold so that possible outages can be avoided. We also consider the timeliness of transmissions in terms of the probability of peak AoI. By using a weighted sum function of the outage probability, the interception probability, and the violation probability of the peak AoI, we are able to know how these metrics vary with the transmitting power and arrival rate of the source node.

1.2. Related Works

Most of the existing studies on physical layer security assume that the legitimate receivers have perfect estimations of channel conditions. Since the channel estimations are often not error-free, this assumption is not very practical. In fact, channel estimation errors exist in both legitimate receivers and eavesdroppers [12–14]. In most channel estimation techniques, the channel state information (CSI) is obtained through a transmitted signal in the guided frequency band. However, it is usually difficult or impossible for the transmitter to know the state of the channel to the eavesdropper through estimations. In [12], it was shown that the errors in the channel estimation decrease the traversal secrecy rate. In [14],

the authors investigated the optimal power allocation for artificial noise in the secure transmission, which considers the effect of the imperfect CSI on legitimate receivers.

In physical layer security-related research, errors in channel estimation reduce both the reliability and security of the system. Moreover, the correlation between the main and eavesdropping channels can also have a significant impact on system reliability and security. Most researchers assumed independent premises for the main and eavesdropping channels [15]. In actual radio environments, the proximity between the legitimate receiver and eavesdropper, along with similar surrounding scatterers, can cause a high correlation between the received signals of the two receivers. Some research has shown that this correlation can improve performance under certain conditions [16–18]. However, the results in [16] indicate that this correlation causes a loss in traversal secrecy capacity. Nonetheless, a strong channel correlation does not necessarily indicate a high probability of communication disruption. Reference [17] proposed that the correlation impact on the system security performance is not singular but is related to various factors, such as the average signal-to-noise ratio at the receiver, the channel gain ratio, and the set target rate.

In this paper, we propose an SNR-gated transmission control scheme for a three-node system accounting for channel estimation error and correlation between the main and eavesdropping channels. We use the outage probability as a measure of system reliability, and the interception probability as a measure of system security. With these metrics, we investigate the performances of systems with and without the SNR-gated transmission control, and with saturated or unsaturated traffic input, respectively. We also investigate the trade-off among these metrics through a weighted-sum function. By using some mathematical tools, the minimum weighted sum can be found efficiently.

1.3. Main Contributions

The contributions of this paper are summarized as follows.

(1) We propose a novel SNR-gated transmission control scheme to reduce the outage probability and the interception probability at the same time. By hindering transmissions with possible outages and interceptions, the power consumption of the system is also reduced, which further enhances the timeliness of the system.
(2) We consider the performances of systems with unsaturated traffic input, which is more realistic in practical engineering.
(3) We present the outage probability, the interception probability, and peak AoI violation probability explicitly, which are essential for improving and optimizing the reliability, safety, and timeliness of the system.

1.4. Organization

The rest of the paper is organized as follows. We present the transmission model for wireless networks in Section 2. In Section 3, we present the proposed SNR-gated transmission control scheme and derive the outage probability, the interception probability, and the violation probability of peak AoI in closed form. The Monte Carlo simulation and numerical results are presented in Section 4. Finally, we present our conclusions in Section 5.

2. System Model

We consider a wireless network wherein Alice transmits confidential information to Bob, while a third party (Eve) attempts to eavesdrop on this confidential information, as shown in Figure 1. We denote the received signals at Bob and Eve, respectively, as $y_i = \sqrt{P}h_{\mathrm{b},i}x_i + n_{\mathrm{b},i}$, $z_i = \sqrt{P}h_{\mathrm{e},i}x_i + n_{\mathrm{e},i}$. We denote the average transmit power of Alice as P. We assume that the channels suffer from block Rayleigh fading and additional white Gaussian noise. Thus, the channel gain coefficients (h_{b} and h_{e}) are zero-mean Gaussian random variables, while the noises (n_{b} and n_{e}) are independent complex Gaussian random variables with zero mean and variances (N_{b}^2 and N_{e}^2). We denote the distance between Alice and Bob as d_{b}, the distance between Alice and Eve as d_{e}, and the path loss factor as α. The

instantaneous received signal-to-noise ratio at Bob and Eve can be expressed as $\gamma_b = \frac{|h_\mathrm{b}|^2 P_\mathrm{t}}{d_\mathrm{b}^\alpha N_\mathrm{b}^2}$, $\gamma_\mathrm{e} = \frac{|h_\mathrm{e}|^2 P_\mathrm{t}}{d_\mathrm{e}^\alpha N_\mathrm{e}^2}$.

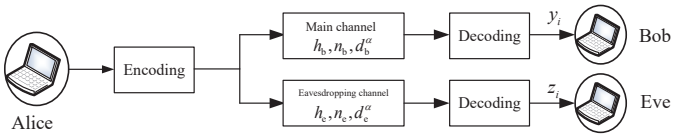

Figure 1. System model.

We denote the signal bandwidth as W. Thus, the instantaneous capacities of the main channel and eavesdropping channel are given, respectively by:

$$\begin{cases} C_\mathrm{b} = W_\mathrm{b} \log_2(1+\gamma_\mathrm{b}) \\ C_\mathrm{e} = W_\mathrm{e} \log_2(1+\gamma_\mathrm{e}). \end{cases} \tag{1}$$

2.1. Channel Estimation

We estimate the fading gain of the channel by using an MMSE estimator during the guided frequency transmission period [19]. The estimation of Bob's channel gain and the estimation error are denoted by $\hat{h}_\mathrm{b}$ and $\tilde{h}_\mathrm{b}$, respectively. Thus, we have,

$$h_\mathrm{b} = \hat{h}_\mathrm{b} + \tilde{h}_\mathrm{b}. \tag{2}$$

We assume that $\hat{h}_\mathrm{b}$ and $\tilde{h}_\mathrm{b}$ are independent zero-mean complex Gaussian random variables, and have [20]

$$E\left\{|h_\mathrm{b}|^2\right\} = E\left\{\left|\tilde{h}_\mathrm{b}\right|^2\right\} + E\left\{\left|\hat{h}_\mathrm{b}\right|^2\right\}. \tag{3}$$

As we know in [21], the estimation error of the channel coefficient error variance is $\beta_b = \sigma_{\tilde{h}_b}^2 = \frac{1}{1+P_\mathrm{p}}$, where P_p is the pilot power. We denote the estimated SNR at Bob as $\hat{\gamma}_\mathrm{b} = \frac{P_t|\hat{h}_\mathrm{b}|^2}{d_\mathrm{b}^\alpha N_\mathrm{b}^2}$ and $\tilde{\gamma}_\mathrm{b} = \frac{P_\mathrm{t}|\tilde{h}_\mathrm{b}|^2}{d_\mathrm{b}^\alpha N_\mathrm{b}^2}$, both of which are exponentially distributed given by random variables with the pdf:

$$\begin{cases} f_{\hat{\gamma}_\mathrm{b}}(\hat{\gamma}_\mathrm{b}) = \dfrac{d_\mathrm{b}^\alpha N_\mathrm{b}^2}{P_\mathrm{t}(1-\beta)} e^{-\frac{\hat{\gamma}_\mathrm{b} d_\mathrm{b}^\alpha N_\mathrm{b}^2}{P_\mathrm{t}(1-\beta)}}, \ \hat{\gamma}_\mathrm{b} > 0 \\ f_{\tilde{\gamma}_\mathrm{b}}(\tilde{\gamma}_\mathrm{b}) = \dfrac{d_\mathrm{b}^\alpha N_\mathrm{b}^2}{P_\mathrm{t}\beta} e^{-\frac{\tilde{\gamma}_\mathrm{b} d_\mathrm{b}^\alpha N_\mathrm{b}^2}{P_\mathrm{t}\beta}}, \ \tilde{\gamma}_\mathrm{b} > 0. \end{cases} \tag{4}$$

Due to the estimation errors, the actual instantaneous SNR at Bob can be expressed as a function of the estimated SNR and the SNR error [22]:

$$\gamma_\mathrm{b} = \frac{P_\mathrm{t}\left|\hat{h}_\mathrm{b}\right|^2}{P_\mathrm{t}\left|\tilde{h}_\mathrm{b}\right|^2 + 1} = \frac{\hat{\gamma}_\mathrm{b}}{\tilde{\gamma}_\mathrm{b} + 1}. \tag{5}$$

2.2. Channel Correlation Coefficient

Since Bob and Alice are closely located, the main channel and the eavesdropping channel would be correlated. Thus, the channel gain coefficient between Alice and Eve can be expressed as in [23]:

$$h_{AE} = \xi_{AE} h_\mathrm{b} + \sqrt{1-\xi_{AE}^2}\, h_\mathrm{e}. \tag{6}$$

In Equation (6), h_{AE} is the channel gain coefficient of the main channel. h_b and h_e are zero-mean Gaussian random variables that are independently and identically distributed. Parameter ξ_{AE} represents the correlation coefficient between the gain of the main channel

and the eavesdropping channel. Moreover, the signal received by Eve can be expressed as $y_i = \sqrt{P}h_{AE}x_i + n_{E,i}$, where $n_{E,i}$ represents the additive white Gaussian noise at the eavesdropper's receiver. Thus, the SNR at Eve can also be expressed as follows:

$$\gamma_{\mathrm{e}} = \frac{P_{\mathrm{t}}}{d_{\mathrm{e}}^2 N_e^2}\left[\xi_{AE}^2|h_{\mathrm{b}}|^2 + (1-\xi_{AE}^2)|h_{\mathrm{e}}|^2\right]. \tag{7}$$

2.3. Traffic Model

In most previous studies, it was assumed that Alice always had packets to transmit (i.e., the saturated traffic model), so that the probability of the unsuccessful packet reception equals the probability that the channel gain is smaller than a certain threshold. In practical implementations, we need to consider the unsaturated traffic model instead. Specifically, the unsaturated model and the saturated model are explained as follows.

- Saturated traffic model: The next packet arrives immediately when the transmission of the previous packet is complete so that Alice always has packets to transmit.
- Unsaturated traffic model: The packets are generated according to a certain random process. Thus, there are slots where Alice does not have a packet to transmit. In this paper, we assume that the packets arrive with a geometric process with parameter λ. That is, Alice has a new packet with a probability λ in each slot. Thus, the average inter-arrival time would be $E[X_k] = \frac{1}{\lambda}$.

2.4. Reliability and Safety Metrics

We denote the code word transmission rate as R_{b} and the confidential message rate as R_{s}. If the main channel capacity is less than the data rate R_{b}, an outage event occurs. That is, the outage probability is given by:

$$P_{\mathrm{out}} = \Pr(C_{\mathrm{b}} < R_{\mathrm{b}}). \tag{8}$$

Since the transmission of a packet is successful with probability $\mu = 1 - P_{\mathrm{out}}$ (no outage occurs), the service time of a packet (i.e., the number of slots to transmit a packet to Bob successfully) follows a geometric distribution with parameter μ. That is,

$$\Pr\{S = j\} = (1-\mu)^{j-1}\mu. \tag{9}$$

Thus, we have $E[S] = \frac{1}{\mu}$.

We denote the cost of protecting message transmissions from eavesdropping as $R_{\mathrm{e}} = R_{\mathrm{b}} - R_{\mathrm{s}}$. If the capacity of the eavesdropping channel satisfies $C_{\mathrm{e}} > R_{\mathrm{e}}$, Eve will be able to decode the message and an interception event occurs. Thus, the interception probability of the eavesdropping channel is given by:

$$P_{\mathrm{int}} = \Pr(C_{\mathrm{e}} > R_{\mathrm{e}}). \tag{10}$$

Note that both the above-mentioned outage probability and interception probability are probabilities conditioned on the fact that there are always enough messages for transmission. That is:

$$\begin{cases} P_{\mathrm{out}} = \Pr(C_{\mathrm{b}} < R_{\mathrm{b}}|\mathrm{Saturation}) \\ P_{\mathrm{int}} = \Pr(C_{\mathrm{e}} > R_{\mathrm{e}}|\mathrm{Saturation}). \end{cases} \tag{11}$$

2.5. Violation Probability of Peak AoI

The AoI of the system is defined as the length of the period between the current time and the time at which the latest received update is generated. Thus, a smaller AoI indicates fresher information. At the moment t, AoI is expressed as [7]:

$$\Delta(t) = t - r(t), \tag{12}$$

wherein $r(t)$ is the timestamp of the latest update received at the receiver at time t. The peak AoI is defined as the age of a packet at the time it is received [24], i.e.,

$$\Delta_p(t) = Y_k + T_{k-1}, \tag{13}$$

wherein Y_k is the inter-departure time and T_{k-1} is the system time of the packet.

3. SNR-Gated Transmission

In order to reduce the outage probability and the interception probability simultaneously, we propose an SNR-gated transmission control scheme in this section. Note that an outage might occur when the main channel is poor while an interception may occur if the main channel is relatively strong. Therefore, it is reasonable to control the transmission of Alice, and only perform transmission in slots where the estimated SNR of the main channel is neither too small nor too large. Figure 2 shows the transmission process of data packets under the SNR-gated transmission control.

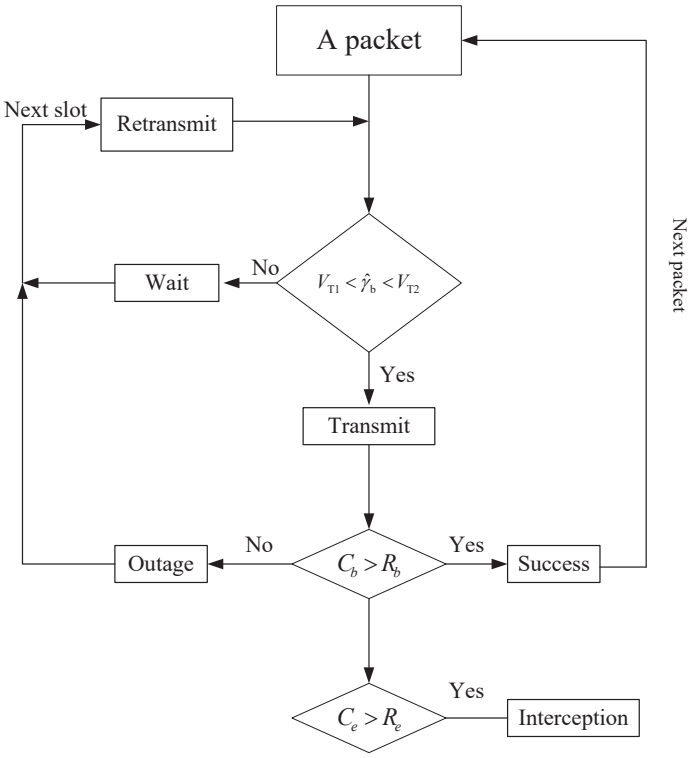

Figure 2. Packet transmission under SNR-based control.

Specifically, when the packet obtains its chance to be transmitted, we shall check if the estimated SNR of the main channel falls into the desired range (V_{T1}, V_{T2}). If yes, the packet will be transmitted. If not, the packet needs to wait and will be retransmitted in the next time slot. When the packet is transmitted in the current slot, an outage can still possibly occur, in which case, the packet will be retransmitted in the next time slot. A packet is considered as successfully transmitted only if no outage occurs.

3.1. Outage Probability

3.1.1. Outage Probability under Saturated Model

We denote the lower and upper SNR thresholds of the control scheme as V_{T1} and V_{T2}. That is, Alice performs a transmission if and only if the estimated SNR satisfies $V_{T1} < \hat{\gamma}_b < V_{T2}$. In other cases, the packet will not be transmitted; thus the probability of outage and interception is reduced. First, the outage probability of the saturated model is given by the following proposition.

Proposition 1. *Regarding saturated transmission, the outage probability is expressed as follows:*

$$\begin{aligned}\hat{P}_{\text{out.s}} &= \Pr\{C_{\text{b}} < R_{\text{b}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \Pr\{V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \\ &= \left(e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{\text{T2}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)} \\ &+ \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T1}}}{k}-1)}{P_t \beta}\right)} - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)}\right) \cdot e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \\ &- \frac{1-\beta}{k\beta+1-\beta} e^{-\left(\frac{k W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \cdot \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T1}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right. \\ &\left. - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right). \end{aligned} \tag{14}$$

Proof. See Appendix A.1. □

3.1.2. Outage Probability under the Unsaturated Model

Second, in the unsaturated model, Alice does not have any transmission slot with probability $\frac{\lambda}{\mu}$. The corresponding actual outage probability is given by the following proposition.

Proposition 2. *Regarding unsaturated transmissions, the outage probability is expressed as follows:*

$$\begin{aligned}\hat{P}_{\text{out.us}} &= \Pr\{C_{\text{b}} < R_{\text{b}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \Pr\{V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \frac{\mu}{\lambda} \\ &= \left(e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{\text{T2}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)} \\ &+ \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T1}}}{k}-1)}{P_t \beta}\right)} - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)}\right) \cdot e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \\ &- \frac{1-\beta}{k\beta+1-\beta} e^{-\left(\frac{k W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \cdot \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T1}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right. \\ &\left. - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right) \frac{\mu}{\lambda}. \end{aligned} \tag{15}$$

Proof. See Appendix A.2. □

From Appendix A.2, the load factor plays a crucial role in the unsaturated transmission scenario.

3.2. Interception Probability

3.2.1. Interception Probability under Saturated Model

Since we determine whether to transmit a packet based on the estimated SNR of the main channel, we will define and derive the interception probability of the system as follows.

Proposition 3. *In saturated transmissions, the interception probability can be expressed as follows:*

$$\begin{aligned}\hat{P}_{\text{int.s}} &= \Pr\{C_{\text{e}} > R_{\text{e}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \Pr\{V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \\ &= \left(e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{\text{T2}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_2 N_2 d_2^{\alpha}(\frac{V_{\text{T2}}}{k_2})}{P_t \sigma_{\text{e}}}\right)} \\ &+ \left(e^{-\left(\frac{W_2 N_2 d_2^{\alpha} V_{\text{T1}}}{P_t \beta k_2}\right)} - e^{-\left(\frac{W_2 N_2 d_2^{\alpha} V_{\text{T2}}}{P_t \beta k_2}\right)}\right) \cdot e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \\ &- \frac{1-\beta}{k\sigma_{\text{e}} + 1 - \beta} \cdot \left(e^{-\left(\frac{W_2 N_2 d_2^{\alpha}(\frac{V_{\text{T1}}}{k})(k\sigma_{\text{e}}+1-\beta)}{P_t \sigma_{\text{e}}(1-\beta)}\right)}\right. \\ &\left. - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k})(k\sigma_{\text{e}}+1-\beta)}{P_t \sigma_{\text{e}}(1-\beta)}\right)}\right). \end{aligned} \tag{16}$$

Proof. See Appendix A.3. □

Equation (16) indicates that the transmission of data through the channel is determined by the channel quality of the main channel. As the system is fully saturated in terms of transmission, the probability of the packet being intercepted in the channel is the probability that the capacity of the eavesdropping channel is greater than the secrecy overhead.

3.2.2. Interception Probability under Unsaturated Model

Proposition 4. *Regarding unsaturated transmissions, the interception probability is expressed as follows:*

$$\begin{aligned}\hat{P}_{\text{int.us}} &= \Pr\{C_{\text{e}} > R_{\text{e}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \Pr\{V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} \frac{\mu}{\lambda} \\ &= \left(e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{\text{T2}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_2 N_2 d_2^{\alpha}(\frac{V_{\text{T2}}}{k_2})}{P_t \sigma_{\text{e}}}\right)} \\ &+ \left(e^{-\left(\frac{W_2 N_2 d_2^{\alpha} V_{\text{T1}}}{P_t \beta k_2}\right)} - e^{-\left(\frac{W_2 N_2 d_2^{\alpha} V_{\text{T2}}}{P_t \beta k_2}\right)}\right) \cdot e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \\ &- \frac{1-\beta}{k\sigma_{\text{e}} + 1 - \beta} \cdot \left(e^{-\left(\frac{W_2 N_2 d_2^{\alpha}(\frac{V_{\text{T1}}}{k})(k\sigma_{\text{e}}+1-\beta)}{P_t \sigma_{\text{e}}(1-\beta)}\right)}\right. \\ &\left. - e^{-\left(\frac{W_1 N_1 d_1^{\alpha}(\frac{V_{\text{T2}}}{k})(k\sigma_{\text{e}}+1-\beta)}{P_t \sigma_{\text{e}}(1-\beta)}\right)}\right) \frac{\mu}{\lambda}. \end{aligned} \tag{17}$$

Proof. See Appendix A.4. □

Therefore, after our comparative analysis and calculation, we see that, by using the SNR-gated transmission control, the reduction of the possibility of sending packets on the sender side does reduce the outage probability and interception probability. Thus, it satisfies our expectation to improve transmission reliability and security simultaneously.

3.3. Timeliness Analysis

We formulate the transmission over the main channel as a Geom/Geom/1 queuing policy [25] and measure the timeliness of the received packet by Bob by the violation probability of the peak AoI.

Since the traffic models of packets in the channel are different, we will analyze the timeliness in two parts. There are two commonly used packet service policies: the first-come, first-served policy (FCFS) and the last-come, first-served policy (LCFS) [24]. In this paper, we assume that the packets are served according to the FCFS rule. In the unsaturation traffic model, we assume that the state updates are generated according to a geometric process. Thus, both the inter-arrival time X_k and service time S_k are independent and geometrically distributed random variables, with mean $E[X_k] = \frac{1}{\lambda}$ and $E[S_k] = \frac{1}{\mu}$, respectively.

First, if the service of a packet is completed before the arrival of the next packet, the service of the next packet begins immediately upon its arrival. Second, if the service of the current packet is not completed before the next arrives, the arriving packet needs to wait before starting its service. Thus, interval Y_k between the departures can be expressed as follows:

$$Y_k = \begin{cases} S_k, \mathrm{X}_k \leq T_{k-1} \\ X_k - T_{k-1} + S_k, \mathrm{X}_k \geq T_{k-1}. \end{cases} \tag{18}$$

The distribution of the inter-arrival time, the service time, and the system time can be expressed as follows:

$$\begin{cases} \Pr(X_\mathrm{k} = i) = \lambda(1-\lambda)^{i-1}, i \geq 1 \\ \Pr(S_\mathrm{k} = i) = \mu(1-\mu)^{i-1}, i \geq 1 \\ \Pr(T_{\mathrm{k}-1} = i) = p_0(1-p_0)^{i-1}, i \geq 1, \end{cases} \tag{19}$$

wherein $p_0 = \frac{1-\mu}{1-\lambda}$.

We use the violation probability of the peak AoI as the measure of data freshness, which is expressed as follows:

$$P_{\Delta_\mathrm{p}}(A_\mathrm{T}) = \Pr(\Delta_\mathrm{p} > A_\mathrm{T}), \tag{20}$$

where A_T is the threshold value of the peak AoI [26].

We compare the service rate before and after using the SNR-gated transmission control. For the transmission without SNR-gated transmission control, since there is no transmission constraints, packets can be sent in each slot, with a successful probability:

$$\mu = 1 - P_\mathrm{out}. \tag{21}$$

By using our SNR-gated transmission control, we only attempt to transmit a packet when the estimated SNR $\hat{\gamma}_b$ of the main channel is greater than A_{T_1} and less than A_{T_2}. Thus, the service rate of the main channel is:

$$\hat{\mu} = \Pr\{\text{send packets}\} - \hat{P}_\mathrm{out.us}. \tag{22}$$

Since SNR-gated transmission control reduces the possibility of transmission, the probability of a successful packet delivery would also be reduced.

3.3.1. Saturation Transmission Model

In this case, the server is loaded at full capacity. Specifically, a new state update arrives precisely when the last update packet leaves the queue. At this point, the inter-departure time Y_k is equal to the service time S_k. Therefore, we have $E[Y_k T_k] = E[S_k^2]$ and $E[X_k] = \frac{1}{\lambda}$. Thus, we have:

$$\Delta_\mathrm{p} = Y_k + T_{k-1} = 2S_k. \tag{23}$$

For the saturated transmission model, the service rate is mainly affected by the SNR-gated transmission control. Since the saturation transmission model generates a new packet immediately when a packet is delivered, the packet arrival rate can be considered as $\lambda = 1$. Thus, we have:

$$P_{\Delta_\mathrm{p}} = \Pr(\Delta_\mathrm{p} > A_{\mathrm{T}_1}) = \hat{\mu}^{A_{\mathrm{T}_1}}. \tag{24}$$

3.3.2. Unsaturated Transmission Model

In the unsaturated transmission model, the server is not fully loaded, so the load factor is not equal to one. In this case, Y_k is not equal to S_k due to the additional waiting time.

We know that our SNR-gated transmission control mainly changes the service rate to $\hat{\mu}$. By replacing μ with $\hat{\mu}$, we have

Proposition 5. *The violation probability of peak AoI can be expressed explicitly as follows:*

$$P_{\Delta p}(A_T) = \frac{\hat{\mu}^2}{\lambda^2}\left(\frac{1-\hat{\mu}}{1-\lambda}\right)^{A_T-2} + \frac{(1-\lambda)^{A_T-2}\hat{\mu}^2}{(\hat{\mu}-\lambda)^2}. \tag{25}$$

Proof. See Appendix A.5. □

3.4. Joint Optimization of Safety, Reliability, and Timeliness

In this section, we jointly optimize the safety, reliability, and timeliness of the system through a weighted sum function $J = \eta_1 P_{\text{out}} + \eta_2 P_{\text{int}} + \eta_3 P_{\Delta_{\text{p}}}$, wherein $\eta_1, \eta_2, \eta_3 \in [0,1]$ are weighing coefficients and $\eta_1 + \eta_2 + \eta_3 = 1$. By using different weights, the performance-oriented aspects of the transmission system are different. For example, when we set η_1 close to unity, the reliability of the system plays the most significant role among the three dimensions. When we require a better timeliness performance, we could set η_3 as close to unity. We can find the optimal solution more intuitively by using the MATLAB construction function. Specifically, the optimization problem of the integrated performance can be expressed as follows:

$$\begin{aligned} &\min_{P_{\text{t}},\lambda} \; J = \eta_1 \hat{P}_{\text{out.s}} + \eta_2 \hat{P}_{\text{int.s}} + \eta_3 \hat{P}_{\Delta_{\text{p.s}}} \\ &\text{s.t.} \;\; \varepsilon_1 \le P_{\text{t}} \le \varepsilon_2 \\ &\quad\; 0 \le \lambda \le 1, \end{aligned} \tag{26}$$

wherein λ is the updating rate of Alice, $[\varepsilon_1, \varepsilon_2]$ is the range of power. In the saturated transmission model, we do not need to consider the optimization over λ since we have $\lambda = 1$. In this case, J can be rewritten as follows:

$$\begin{aligned} &\min_{P_{\text{t}}} \; J = \eta_1 \hat{P}_{\text{out.s}} + \eta_2 \hat{P}_{\text{int.s}} + \eta_3 \hat{P}_{\Delta_{\text{p.s}}} \\ &\text{s.t.} \;\; \varepsilon_1 \le P_{\text{t}} \le \varepsilon_2. \end{aligned} \tag{27}$$

Since the above equation is an inequality-constrained optimization problem that satisfies the Karush–Kuhn–Tucker (KKT) condition [27], we will discuss it in the following cases. By setting $\frac{\partial J}{\partial P_t} = 0$, the optimized transmit power P_t can be obtained. We simplify $\hat{P}_{\text{out}.s}$, $\hat{P}_{\text{int}.s}$, and $\hat{P}_{\Delta_{p.s}}$, and have the following proposition:

Proposition 6. *In the saturated transmission model, the optimal transmit power is given by:*

(1) When $\varepsilon_1 > \frac{\ln\left(\frac{(\eta_1-\eta_3)+1}{1-(\eta_1-\eta_3)\eta_2}\right)}{\omega_2-\omega_1}$, *the optimal solution is* $P_t = \varepsilon_1$;

(2) When $\varepsilon_2 > \frac{\ln\left(\frac{(\eta_1-\eta_3)+1}{1-(\eta_1-\eta_3)\eta_2}\right)}{\omega_2-\omega_1}$, *the optimal solution is* $P_t = \varepsilon_2$;

(3) When $\varepsilon_1 < \frac{\ln\left(\frac{(\eta_1-\eta_3)+1}{1-(\eta_1-\eta_3)\eta_2}\right)}{\omega_2-\omega_1} < \varepsilon_2$, *the optimal solution is* $P_t = \frac{\ln\left(\frac{(\eta_1-\eta_3)+1}{1-(\eta_1-\eta_3)\eta_2}\right)}{\omega_2-\omega_1}$,

wherein ω_1 *is* $\frac{V_{T1}W_1N_1d_1^{\alpha}}{1-\beta}$ *and* ω_2 *is* $\frac{V_{T2}W_1N_1d_1^{\alpha}}{1-\beta}$.

Proof. See Appendix A.6. □

4. Simulation Results

In this section, we evaluate the safety, reliability, and timeliness of the system through the simulation results. We set the main channel bandwidth as $W_1 = 10^7$ Hz, the eavesdropping channel bandwidth as $W_2 = 10^7$ Hz, the distance between Alice and Bob as $d_1 = 200$ m, and the distance between Alice and Eve as $d_2 = 150$ m. We set the main channel noise power spectral density as $N_1 = 4 \times 10^{-12}$ W and the eavesdropping channel noise power spectral density as $N_2 = 4 \times 10^{-12}$ W. The main channel Rayleigh channel parameter λ_1 is set to 4 and the path loss factor α is set to 2 [28]. To verify the obtained theoretical (TH) results, we also performed corresponding Monte Carlo (MC) simulations. Specifically, we

set the simulation time to 10,000 s and block spacing to 10^{-3}. We assume that the main channel and the eavesdropping channel are correlated.

In Figure 3, we compare the interception probabilities and outage probabilities with and without using the SNR-gated transmission control scheme. From the figure, we can see that the outage probability decreases with the increase in transmit power P_t. More importantly, both the outage probability and interception probability are significantly decreased when the SNR-gated transmission control scheme is used. Therefore, we can conclude that the SNR-gated transmission control scheme can effectively improve reliability and safety simultaneously.

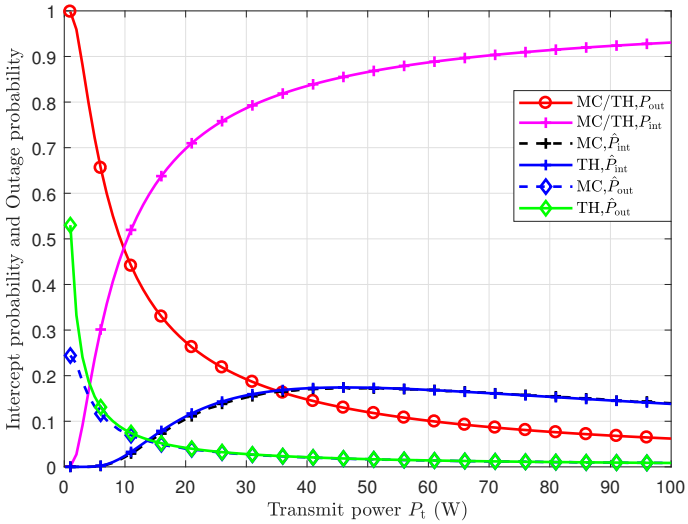

Figure 3. The outage probability and interception probability vary with different transmitting powers.

In Figure 4, we investigate the correlation between the transmitted power and the probability of peak AoI violation in the saturated model with SNR-gated transmission control. It is seen that as the transmission power increases, the probability of peak AoI violation decreases. By reducing the threshold of violation, the probability of peak AoI violation also decreases. This is due to the fact that increasing the threshold results in a smaller probability for the peak AoI exceeding the threshold.

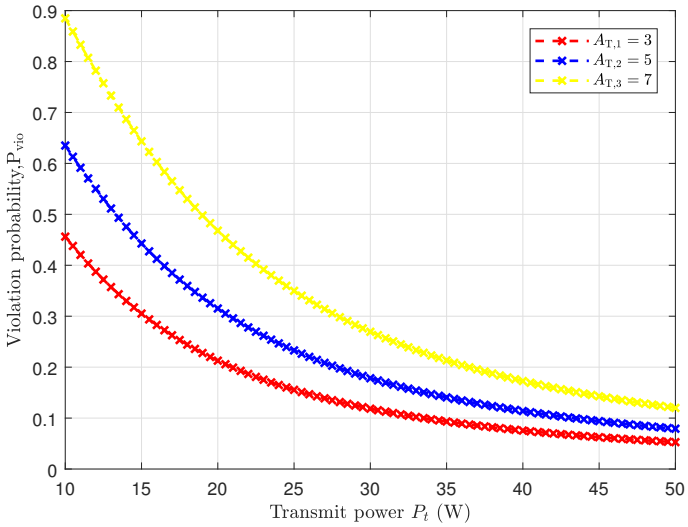

Figure 4. The variation of the probability of peak AoI violation with transmission power under SNR-gated transmission control. P_t is set to 5 W. The left threshold is set to 4, the right threshold is set to 15, the pilot power is 0.7 W, and R_b = 2.4 bps.

Figure 5 shows how the violation probability of peak AoI varies with the packet arrival rate λ under the unsaturated traffic model. We observe that the violation probability decreases first and then increases. However, the peak AoI violation probability is larger than when the SNR-gated transmission control scheme is not used. This is because many transmissions are stopped, which leads to a lower service rate and, thus, degrades the timeliness.

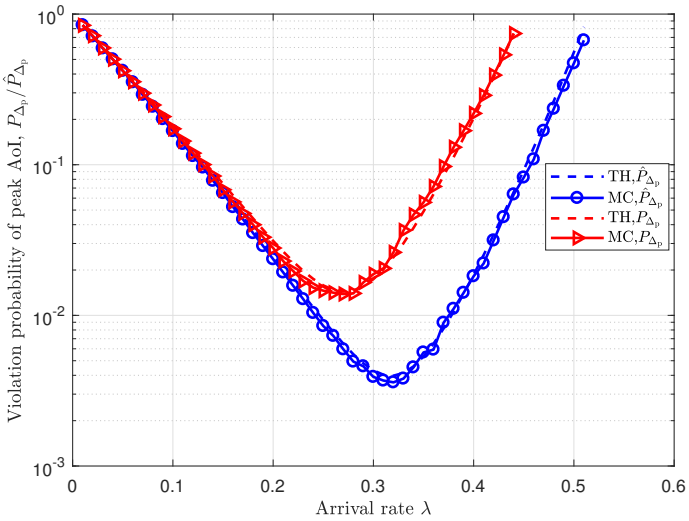

Figure 5. The variation in the probability of peak AoI violation with the arrival rate λ under SNR-gated transmission control and without SNR-gated transmission control.

In Figure 6, we present a three-dimensional graph of the weighted sum of the outage probability, interception probability, and PAoI violation probability. The x-axis represents the transmit power, the y-axis represents the arrival rate λ, and the z-axis represents the weighted sum of the three probabilities J. It is observed that the weighted sum has a bowl-shaped structure with a minimum point when the transmit power and the arrival rate are neither too small nor too large. This optimal point can be calculated through numerical computation.

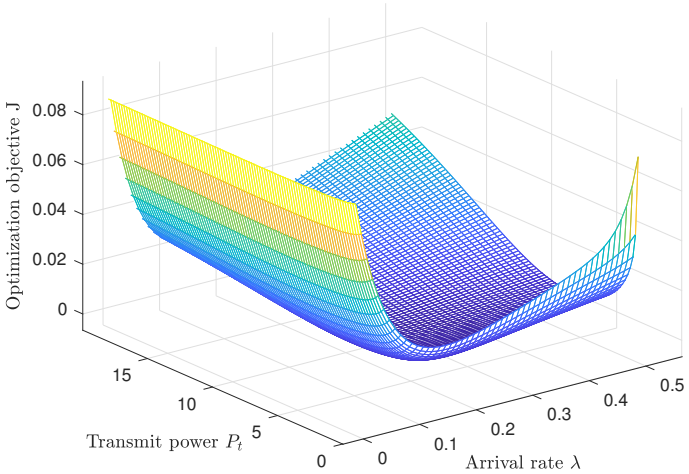

Figure 6. The three-dimensional graph for the weighted sum of the outage probability, interception probability, and PAoI violation probability.

5. Conclusions

In this paper, we investigate the security, reliability, and timeliness of a three-node physical layer security system, where the main channel and the eavesdropping channel are correlated. We propose an SNR-gated transmission control scheme and derive closed-form

expressions for the outage probability, interception probability, and peak AoI violation probability. Our analysis and numerical results demonstrate the effectiveness of the proposed SNR-gated transmission control scheme; we explicitly derive the probabilities of data outage and interception while enhancing timeliness through the control of the data arrival rate. Moreover, we optimize the transmit power of the source node to minimize the weighted sum probability of outages, interceptions, and peak AoI violations. In the future, we plan to study the system with the adaptive rate, which is an interesting direction, as well as explore the eavesdropping channel model with relay nodes, which is another interesting research direction.

Author Contributions: Conceptualization, Y.D.; methodology, J.L. and Y.D.; writing—original draft preparation, J.L.; writing—review and editing, Y.D and C.P. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Y. Dong was supported by the National Natural Science Foundation of China (NSFC) under grant 62071237. The work of C. Pan was supported by the National Natural Science Foundation of China (NSFC) under grant 61931004.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the editors and the reviewers for their insightful comments and suggestions, which resulted in substantial improvements to this work.

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

Appendix A

Appendix A.1. Proof of Proposition 1

For the actual outage probability of packets in the channel under saturated transmission, we provide the following proof:

The actual outage probability event is the product of events, where the main channel capacity is less than the encoding rate and events where data can be transmitted.

$$\begin{aligned}
\hat{P}_{\text{out.s}} &= \Pr\{C_{\text{b}} < R_{\text{b}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} P_{suc} \\
&= \Pr\{W_1 \log 2(1+\gamma_{\text{b}}) < R_{\text{b}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} P_{suc} \\
&= \Pr\{W_1 \log 2(1+\frac{\hat{\gamma}_{\text{b}}}{\tilde{\gamma}_{\text{b}}+1}) < R_{\text{b}} | V_{\text{T1}} < \hat{\gamma}_{\text{b}} < V_{\text{T2}}\} P_{suc} \\
&= \Pr\{V_{\text{T1}} < \hat{\gamma}_{\text{b}} < \min(k(\tilde{\gamma}_{\text{b}}+1), V_{\text{T2}})\}
\end{aligned} \tag{A1}$$

Since $\hat{\gamma}_{\text{b}}$ follows an exponential distribution, we can perform the following integration operations:

$$\begin{aligned}
&= \int_{\frac{V_{\text{T1}}}{k}-1}^{\frac{V_{\text{T2}}}{k}-1} f(\tilde{\gamma}_{\text{b}}) \mathrm{d}(\tilde{\gamma}_{\text{b}}) \int_{V_{\text{T1}}}^{k(\tilde{\gamma}_{\text{b}}+1)} f(\hat{\gamma}_{\text{b}}) \mathrm{d}(\hat{\gamma}_{\text{b}}) \\
&+ \int_{\frac{V_{\text{T2}}}{k}-1}^{+\infty} f(\tilde{\gamma}_{\text{b}}) \mathrm{d}(\tilde{\gamma}_{\text{b}}) \int_{V_{\text{T1}}}^{V_{\text{T2}}} f(\hat{\gamma}_{\text{b}}) \mathrm{d}(\hat{\gamma}_{\text{b}}) \\
&= \left(e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{\text{T2}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \right) \cdot e^{-\left(\frac{W_1 N_1 d_1^{\alpha} (\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)} \\
&+ \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha} (\frac{V_{\text{T1}}}{k}-1)}{P_t \beta}\right)} - e^{-\left(\frac{W_1 N_1 d_1^{\alpha} (\frac{V_{\text{T2}}}{k}-1)}{P_t \beta}\right)} \right) \cdot e^{-\left(\frac{V_{\text{T1}} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \\
&- \frac{1-\beta}{k\beta+1-\beta} e^{-\left(\frac{k W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} \cdot \left(e^{-\left(\frac{W_1 N_1 d_1^{\alpha} (\frac{V_{\text{T1}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)} \right. \\
&\left. - e^{-\left(\frac{W_1 N_1 d_1^{\alpha} (\frac{V_{\text{T2}}}{k}-1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)} \right),
\end{aligned} \tag{A2}$$

wherein $k = 2^{\frac{R_b}{W_1}} - 1$ and $\Pr\{V_{T1} < \hat{\gamma}_b < V_{T2}\} \triangleq P_{suc}$.

Appendix A.2. Proof of Proposition 2

For the actual outage probability of packets in the channel under unsaturated transmission, we provide the following proof:

$$\begin{aligned}
\hat{P}_{\text{out.us}} &= \Pr\{C_b < R_b | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \Pr\{W_1 \log 2(1+\gamma_b) < R_b | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \Pr\{W_1 \log 2(1+\frac{\hat{\gamma}_b}{\tilde{\gamma}_b+1}) < R_b | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \left(e^{-\left(\frac{V_{T1} W_1 N_1 d_1^\alpha}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{T2} W_1 N_1 d_1^\alpha}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_1 N_1 d_1^\alpha (\frac{V_{T2}}{k} - 1)}{P_t \beta}\right)} \\
&+ \left(e^{-\left(\frac{W_1 N_1 d_1^\alpha (\frac{V_{T1}}{k} - 1)}{P_t \beta}\right)} - e^{-\left(\frac{W_1 N_1 d_1^\alpha (\frac{V_{T2}}{k} - 1)}{P_t \beta}\right)}\right) \cdot e^{-\left(\frac{V_{T1} W_1 N_1 d_1^\alpha}{P_t(1-\beta)}\right)} \\
&- \frac{1-\beta}{k\beta+1-\beta} e^{-\left(\frac{k W_1 N_1 d_1^\alpha}{P_t(1-\beta)}\right)} \cdot \left(e^{-\left(\frac{W_1 N_1 d_1^\alpha (\frac{V_{T1}}{k} - 1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right. \\
&\left. - e^{-\left(\frac{W_1 N_1 d_1^\alpha (\frac{V_{T2}}{k} - 1)(k\beta+1-\beta)}{P_t \beta(1-\beta)}\right)}\right) \frac{\mu}{\lambda},
\end{aligned} \tag{A3}$$

where $k = 2^{\frac{R_b}{W_1}} - 1$.

Appendix A.3. Proof of Proposition 3

For the actual interception probability of packets in the channel under saturated transmission, we provide the following proof:

The actual interception probability event is a product of the events where the eavesdropping channel capacity is greater than the encoding rate (which aims to prevent eavesdropping) and the events where data can be transmitted.

$$\begin{aligned}
\hat{P}_{\text{int.s}} &= \Pr\{C_e > R_e | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{W_2 \log 2(1+\gamma_e) > R_e | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{\gamma_e > 2^{\frac{R_e}{W_2}} - 1 | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{\xi^2 \hat{\gamma}_b + (1-\xi^2)\gamma_A > k_1 | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{\hat{\gamma}_b > \frac{k_1 - (1-\xi^2)\gamma_A}{\xi^2} | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{\max(V_{T1}, \frac{k_1 - (1-\xi^2)\gamma_A}{\xi^2}) < \hat{\gamma}_b < V_{T2}\}
\end{aligned} \tag{A4}$$

Since $\hat{\gamma}_b$ follows an exponential distribution, we can perform the following integration operations:

$$
\begin{aligned}
&= \int_{\frac{V_{T1}}{k_2}}^{\frac{V_{T2}}{k_2}} f(\tilde{\gamma}_b)\mathrm{d}(\tilde{\gamma}_b) \int_{V_{T1}}^{k(\tilde{\gamma}_b+1)} f(\gamma_A)\mathrm{d}(\gamma_A) \\
&+ \int_{\frac{V_{T2}}{k_2}}^{+\infty} f(\tilde{\gamma}_b)\mathrm{d}(\tilde{\gamma}_b) \int_{V_{T1}}^{V_{T2}} f(\gamma_A)\mathrm{d}(\gamma_A) \\
&= \left(e^{-\left(\frac{V_{T1}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{T2}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_2N_2d_2^{\alpha}(\frac{V_{T2}}{k_2})}{P_t\sigma_e}\right)} \\
&+ \left(e^{-\left(\frac{W_2N_2d_2^{\alpha}V_{T1}}{P_t\beta k_2}\right)} - e^{-\left(\frac{W_2N_2d_2^{\alpha}V_{T2}}{P_t\beta k_2}\right)}\right) \cdot e^{-\left(\frac{V_{T1}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)} \\
&- \frac{1-\beta}{k\sigma_e+1-\beta} \cdot \left(e^{-\left(\frac{W_2N_2d_2^{\alpha}(\frac{V_{T1}}{k})(k\sigma_e+1-\beta)}{P_t\sigma_e(1-\beta)}\right)}\right. \\
&\left. - e^{-\left(\frac{W_1N_1d_1^{\alpha}(\frac{V_{T2}}{k})(k\sigma_e+1-\beta)}{P_t\sigma_e(1-\beta)}\right)}\right),
\end{aligned} \tag{A5}
$$

where $k_2 = 2^{\frac{R_e}{W_2}} - 1$.

Appendix A.4. Proof of Proposition 4

For the actual interception probability of packets in the channel under unsaturated transmission, we provide the following proof:

$$
\hat{P}_{\text{int.us}} = \Pr\{C_e > R_e | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc}, \tag{A6}
$$

owing to the fact that in an unsaturated transmission state, we need to consider the load rate of the server, so we need to multiply the load rate.

$$
\begin{aligned}
&= \Pr\{W_2 \log 2(1+\gamma_e) > R_e | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \Pr\{\gamma_e > 2^{\frac{R_e}{W_2}} - 1 | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \\
&= \Pr\{\xi^2\hat{\gamma}_b + (1-\xi^2)\gamma_A > k_1 | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \Pr\{\hat{\gamma}_b > \frac{k_1 - (1-\xi^2)\gamma_A}{\xi^2} | V_{T1} < \hat{\gamma}_b < V_{T2}\} P_{suc} \frac{\mu}{\lambda} \\
&= \Pr\{\max(V_{T1}, \frac{k_1 - (1-\xi^2)\gamma_A}{\xi^2}) < \hat{\gamma}_b < V_{T2}\} \frac{\mu}{\lambda} \\
&= \left(e^{-\left(\frac{V_{T1}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{T2}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_2N_2d_2^{\alpha}(\frac{V_{T2}}{k_2})}{P_t\sigma_e}\right)} \\
&+ \left(e^{-\left(\frac{W_2N_2d_2^{\alpha}V_{T1}}{P_t\beta k_2}\right)} - e^{-\left(\frac{W_2N_2d_2^{\alpha}V_{T2}}{P_t\beta k_2}\right)}\right) \cdot e^{-\left(\frac{V_{T1}W_1N_1d_1^{\alpha}}{P_t(1-\beta)}\right)} \\
&- \frac{1-\beta}{k\sigma_e+1-\beta} \cdot \left(e^{-\left(\frac{W_2N_2d_2^{\alpha}(\frac{V_{T1}}{k})(k\sigma_e+1-\beta)}{P_t\sigma_e(1-\beta)}\right)}\right. \\
&\left. - e^{-\left(\frac{W_1N_1d_1^{\alpha}(\frac{V_{T2}}{k})(k\sigma_e+1-\beta)}{P_t\sigma_e(1-\beta)}\right)}\right) \frac{\mu}{\lambda},
\end{aligned} \tag{A7}
$$

where $k_2 = 2^{\frac{R_e}{W_2}} - 1$.

Appendix A.5. Proof of Proposition 5

For $X_k \leq T_{k-1}$, we have $Y_k = S_k$. Thus, we can obtain the following:

$$\begin{aligned} P_{\Delta_p}(A_T) &= \Pr(\Delta_{peak} A_T) \\ &= \Pr\{T_{k-1} + S_k > A_T | X_k \le T_{k-1}\} \\ &= \frac{\Pr\{T_{k-1} > \{X_k, A_T - S_k\}_{\max}\}}{\Pr\{X_k \le T_{k-1}\}}, \end{aligned} \tag{A8}$$

When $X_k > A_T - S_k$, the above equation is meaningless; thus, we can obtain the following:

$$\begin{aligned} &\frac{\Pr\{T_{k-1} > \{X_k, A_T - S_k\}_{\max}\}}{\Pr\{X_k \le T_{k-1}\}} \\ &= \frac{\Pr\{T_{k-1} > A_T - S_k\}}{\Pr\{X_k \le T_{k-1}\}} \\ &= \frac{\sum_{i=1}^{\infty} \Pr\{S_k = i\} \Pr\{T_{k-1} + i > A_T\}}{\Pr\{X_k \le T_{k-1}\}} \\ &= \frac{\sum_{i=1}^{\infty} \Pr\{S_k = i\}(1 - \Pr\{T_{k-1} + i \le A_T\})}{\Pr\{X_k \le T_{k-1}\}} \\ &= \sum_{i=1}^{\infty} \Pr\{S_k = i\} \left(\frac{1-\mu}{1-\lambda}\right)^{A_T - i - 1} = \left(\frac{\mu}{\lambda}\right)^2 \left(\frac{1-\mu}{1-\lambda}\right)^{A_T - 2}. \end{aligned} \tag{A9}$$

For $X_k \ge T_{k-1}$, we have $Y_k = S_k + X_k - T_{k-1}$. Thus, can obtain the following:

$$\begin{aligned} &\frac{\Pr\{T_{k-1} + Y_k > A_T\}}{\Pr\{X_k > T_{k-1}\}} \\ &= \frac{\Pr\{X_k > A_T - S_k\}}{\Pr\{X_k > T_{k-1}\}} \\ &= \frac{\sum_{i=1}^{\infty} \Pr\{S_k = i\} \Pr\{X_k + i > A_T\}}{\Pr\{X_k > T_{k-1}\}} \\ &= \sum_{i=1}^{\infty} \mu(1-\mu)^{i-1}(1-\lambda)^{A_T - i - 1} = \frac{(1-\lambda)^{A_T - 2}\mu^2}{(\mu - p)^2}. \end{aligned} \tag{A10}$$

Appendix A.6. Proof of Proposition 6

For the optimization issues, we provide the following proofs:

$$\begin{aligned} &\min_{P_t} \; J = \eta_1 \hat{P}_{\text{out.s}} + \eta_2 \hat{P}_{\text{int.s}} + \eta_3 \hat{P}_{\Delta_{\text{p.s}}} \\ &\text{s.t, } \varepsilon_1 \le P_t \le \varepsilon_2. \end{aligned} \tag{A11}$$

In order to simplify the calculation, we can simplify:

$$\begin{aligned} \hat{P}_{\text{out.s}} &\approx \left(e^{-\left(\frac{V_{T1} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{T2} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_1 N_1 d_1^{\alpha} \left(\frac{V_{T2}}{k} - 1\right)}{P_t \beta}\right)}, \\ \hat{P}_{\text{int.s}} &\approx \left(e^{-\left(\frac{V_{T1} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)} - e^{-\left(\frac{V_{T2} W_1 N_1 d_1^{\alpha}}{P_t(1-\beta)}\right)}\right) \cdot e^{-\left(\frac{W_2 N_2 d_2^{\alpha} \left(\frac{V_{T2}}{k_2}\right)}{P_t \sigma_e}\right)}, \\ \hat{P}_{\Delta_{\text{P}}} &\approx (1 - \hat{P}_{\text{out.s}}). \end{aligned} \tag{A12}$$

We denote $\omega_1 = \frac{V_{T1} W_1 N_1 d_1^{\alpha}}{(1-\beta)}$, $\omega_2 = \frac{V_{T2} W_2 N_2 d_2^{\alpha}}{(1-\beta)}$ and $\omega_3 = \frac{V_{T2} W_2 N_2 d_2^{\alpha}}{\sigma_e}$. From $\frac{\partial J}{\partial P_t} = 0$, we know that:

$$(e^{-\frac{\omega_1}{P_t}}\frac{\omega_1}{{P_t}^2}-e^{-\frac{\omega_2}{P_t}}\frac{\omega_2}{{P_t}^2})((\eta_1-\eta_3)e^{-\frac{\omega_2}{P_t}}+\eta_2 e^{-\frac{\omega_3}{P_t}})$$
$$+(e^{-\frac{\omega_1}{P_t}}-e^{-\frac{\omega_2}{P_t}})(e^{-\frac{\omega_2}{P_t}}\frac{\omega_2}{{P_t}^2}-e^{-\frac{\omega_3}{P_t}}\frac{\omega_3}{{P_t}^2}))=0, \quad \text{(A13)}$$

where $\omega_2 \approx \omega_3$; thus, we can conclude the following:

$$P_t=\frac{\ln(\frac{(\eta_1-\eta_3)+1}{1-(\eta_1-\eta_3)\eta_2})}{\omega_2-\omega_1}. \quad \text{(A14)}$$

References

1. Hellman, M.E. An overview of public key cryptography. *IEEE Commun. Mag.* **2002**, *40*, 42–49. [CrossRef]
2. Kartalopoulos, S.V. A primer on cryptography in communications. *IEEE Commun. Mag.* **2006**, *44*, 146–151. [CrossRef]
3. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
4. Leung-Yan-Cheong, S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
5. Tashman, D.; Hamouda, W. Cascaded κ-μ fading channels with colluding and non-colluding eavesdroppers: Physical-layer security analysis. *Future Internet* **2021**, *13*, 205. [CrossRef]
6. Phan, V.D.; Nguyen, T.N.; Le, A.V.; Voznak, M. A study of physical layer security in SWIPT-based decode-and-forward relay networks with dynamic power splitting. *Sensors* **2021**, *21*, 5692. [CrossRef] [PubMed]
7. Kaul, S.; Yates, R.; Gruteser, M. Real-time status: How often should one update? In Proceedings of the 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012 ; IEEE: Piscataway, NJ, USA , 2012; pp. 2731–2735.
8. Devassy, R.; Durisi, G.; Ferrante, G.C.; Simeone, O.; Uysal-Biyikoglu, E. Delay and peak-age violation probability in short-packet transmissions. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 2471–2475.
9. Hu, L.; Chen, Z.; Dong, Y.; Jia, Y.; Wang, M.; Liang, L.; Chen, C. Optimal status update in IoT systems: An age of information violation probability perspective. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 18 November–16 December 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–5.
10. Champati, J.P.; Al-Zubaidy, H.; Gross, J. Statistical guarantee optimization for AoI in single-hop and two-hop FCFS systems with periodic arrivals. *IEEE Trans. Commun.* **2020**, *69*, 365–381. [CrossRef]
11. Seo, J.B.; Choi, J. On the outage probability of peak age-of-information for D/G/1 queuing systems. *IEEE Commun. Lett.* **2019**, *23*, 1021–1024. [CrossRef]
12. Taylor, J.M.; Hempel, M.; Sharif, H.; Ma, S.; Yang, Y. Impact of channel estimation errors on effectiveness of eigenvector-based jamming for physical layer security in wireless networks. In Proceedings of the 2011 IEEE 16th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Kyoto, Japan, 10–11 June 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 122–126.
13. Zhou, X.; McKay, M.R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
14. Liu, T.Y.; Lin, S.C.; Chang, T.H.; Hong, Y.W.P. How much training is enough for secrecy beamforming with artificial noise. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 4782–4787.
15. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
16. Zhu, J.; Takahashi, O.; Jiang, X.; Nakamura, Y.; Shiraishi, Y. Outage secrecy capacity over correlated fading channels at high SNR. In Proceedings of the 2012 International Conference on Mobile Computing and Ubiquitous Networking, Barcelona, Spain, 23–28 September 2012; pp. 92–97.
17. Sun, X.; Wang, J.; Xu, W.; Zhao, C. Performance of secure communications over correlated fading channels. *IEEE Signal Process. Lett.* **2012**, *19*, 479–482. [CrossRef]
18. Liu, X. Outage probability of secrecy capacity over correlated log-normal fading channels. *IEEE Commun. Lett.* **2012**, *17*, 289–292. [CrossRef]
19. He, B.; Zhou, X. Secure on-off transmission design with channel estimation errors. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1923–1936. [CrossRef]
20. Kay, S.M. *Fundamentals of Statistical Signal Processing: Estimation Theory*; Prentice-Hall, Inc.: Upper Saddle River, NJ, USA, 1993.
21. Hassibi, B.; Hochwald, B.M. How much training is needed in multiple-antenna wireless links? *IEEE Trans. Inf. Theory* **2003**, *49*, 951–963. [CrossRef]
22. Vakili, A.; Sharif, M.; Hassibi, B. The effect of channel estimation error on the throughput of broadcast channels. In Proceedings of the 2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, Toulouse, France, 14–19 May 2006; IEEE: Piscataway, NJ, USA, 2006; Volume 4, p. IV.

23. Lokur, A. Effects of Correlation of Channel Gains on the Secrecy Capacity in the Gaussian Wiretap Channel. Master's Thesis, University of Nebraska, Lincoln, NE, USA, 2019.
24. Yates, R.D.; Sun, Y.; Brown, D.R.; Kaul, S.K.; Modiano, E.; Ulukus, S. Age of information: An introduction and survey. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 1183–1210. [CrossRef]
25. Akar, N.; Dogan, O. Discrete-time queueing model of age of information with multiple information sources. *IEEE Internet Things J.* **2021**, *8*, 14531–14542. [CrossRef]
26. Emara, M.; ElSawy, H.; Bauch, G. A spatiotemporal model for peak AoI in uplink IoT networks: Time versus event-triggered traffic. *IEEE Internet Things J.* **2020**, *7*, 6762–6777. [CrossRef]
27. Gong, S.; Xing, C.; Jing, Y.; Wang, S.; Wang, J.; Chen, S.; Hanzo, L. A unified MIMO optimization framework relying on the KKT conditions. *IEEE Trans. Commun.* **2021**, *69*, 7251–7268. [CrossRef]
28. Peng, D.; Hu, C.; Pan, C.; Dong, Y.; Fan, P.; Letaief, K.B. Timely Communications With and Without Relaying and Buffering. *IEEE Internet Things J.* **2022**, *9*, 24903–24918. [CrossRef]