

## Article

# Optimal Power Allocation for Channel-Based Physical Layer Authentication in Dual-Hop Wireless Networks

Ningbo Fan <sup>1</sup>, Jiahui Sang <sup>2</sup>, Yulin Heng <sup>2</sup>, Xia Lei <sup>2,\*</sup> and Tao Tao <sup>2</sup><sup>1</sup> China Academy of Space Technology (Xi'an), Xi'an 710000, China; fnb504@163.com<sup>2</sup> National Key Laboratory of Science and Technology on Communication of UESTC, Chengdu 611731, China; 202121220118@std.uestc.edu.cn (J.S.); 17378700918@163.com (Y.H.); 18208107300@163.com (T.T.)

\* Correspondence: leixia@uestc.edu.cn

**Abstract:** Channel-based physical-layer authentication, which is capable of detecting spoofing attacks in dual-hop wireless networks with low cost and low complexity, attracted a great deal of attention from researchers. In this paper, we explore the likelihood ratio test (LRT) with cascade channel frequency response, which is optimal according to the Neyman–Pearson theorem. Since it is difficult to derive the theoretical threshold and the probability of detection for LRT, majority voting (MV) algorithm is employed as a trade-off between performance and practicality. We make decisions according to the temporal variations of channel frequency response in independent subcarriers separately, the results of which are used to achieve a hypothesis testing. Then, we analyze the theoretical false alarm rate (FAR) and miss detection rate (MDR) by quantifying the upper bound of their sum. Moreover, we develop the optimal power allocation strategy between the transmitter and the relay by minimizing the derived upper bound with the optimal decision threshold according to the relay-to-receiver channel gain. The proposed power allocation strategy takes advantage of the difference of noise power between the relay and the receiver to jointly adjust the transmit power, so as to improve the authentication performance on condition of fixed total power. Simulation results demonstrate that the proposed power allocation strategy outperforms the equal power allocation in terms of FAR and MDR.

**Keywords:** physical-layer authentication; dual-hop wireless networks; optimal power allocation; false alarm rate; miss detection rate



**Citation:** Fan, N.; Sang, J.; Heng, Y.; Lei, X.; Tao, T. Optimal Power Allocation for Channel-Based Physical Layer Authentication in Dual-Hop Wireless Networks. *Sensors* **2022**, *22*, 1759. <https://doi.org/10.3390/s22051759>

Academic Editor: Zahir M. Hussain

Received: 15 January 2022

Accepted: 20 February 2022

Published: 24 February 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Wireless communication is more vulnerable to eavesdropping and spoofing attacks due to its broadcast nature. Conventionally, the security of wireless networks is addressed by cryptographic protocols above the physical layer that primarily depend on the computation complexity [1]. With the rapid development of advanced computers, wireless networks urgently demand more comprehensive protections that need to be lightweight, flexible, and compatible besides maintaining security [2], especially in the upcoming 6G. Ref. [3] mentioned the trend of using UAV to build cellular networks, and the security of physical layer must be considered.

At present, physical-layer authentication can be divided into three types according to the unique characteristics of extracted signals as follows: (1) authentication based on channel characteristics [4]; (2) authentication based on signal watermarking [5]; (3) authentication based on radio frequency fingerprint [6]. Among them, physical-layer authentication based on channel characteristics is widely studied because of its low computational complexity and broad signal format requirements.

Physical-layer authentication exploits the physical characteristics of channels, devices, and signals to meet the requirements of flexibility and compatibility [4]. The principle of channel-based physical-layer authentication is that the channel response decorrelates

rapidly from one transmit–receive path to another if the paths are separated by the order of a wavelength [7]. Specifically, Xiao et al. [8,9] proposed authentication schemes and practical test statistics by analyzing the time and frequency domain of channels. Liu and Wang in [10] proposed an enhanced scheme that integrates multipath delay characteristics into the channel impulse response (CIR)-based physical-layer authentication. With the development of artificial intelligence technology, it was also applied in various fields of communication, including physical-layer authentication. In [11], machine learning was used for physical-layer authentication, and in [12], deep learning was used to optimize UAV trajectory.

In large-scale wireless communication scenarios represented by the Internet of Things and 6G mobile communication network, terminal devices are widely distributed and resource allocation is limited. Power distribution is becoming an issue to be considered. The D2D communication proposed in [13] requires optimal power distribution. End-to-end communication usually requires relays for assistance, and there are only a few research works at present. Zhang et al. in [14] jointly utilized the location-specific features of both amplitude and delay interval of cascaded channels in authentication, while the multipath was assumed to be identical regarding variation in simplifying the consideration; the effects of noise at the relay were not analyzed. We explore the authentication scheme with cascaded channel frequency response based on research on independent subcarriers in the frequency domain, and then we derive theoretical expression of false alarm rate (FAR) and miss detection rate (MDR). Based on the above, we further derive and analyze the way of optimal power distribution.

The remainder of this paper is organized as follows. Section 2 describes the system model. Section 3 describes an authentication scheme with cascaded channel frequency response and a simplified scheme based on majority voting. Section 4 derives the theoretical expressions of FAR and MDR and provides decision threshold under different criteria. Section 5 explores the optimal power allocation by deriving the upper bound for the sum of FAR and MDR. Simulation results and analysis are shown in Section 6. Section 7 concludes the paper.

For the sake of comparison, above schemes are shown in Table 1.

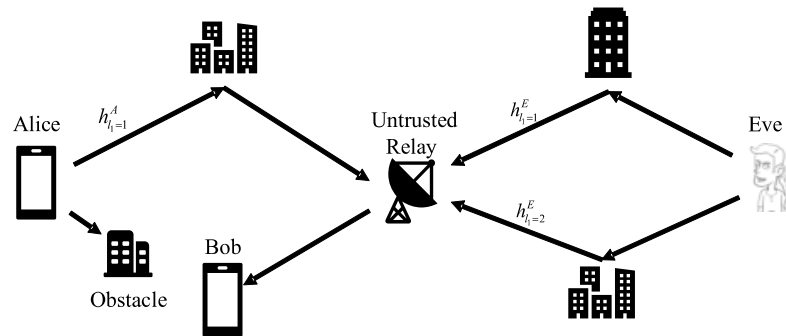
**Table 1.** Comparison of several authentication schemes.

	Authentication based on time domain multipath channel characteristics	Authentication based on frequency domain multipath channel characteristics	Authentication based on signal watermarking	Authentication based on fingerprint identification
Principle	Based on time domain impulse response	Based on frequency domain impulse response	Transmit secret security authentication code or label with message	Based on physical differences of analog equipment
Main defects	Limited by the number of multipaths and the ability to distinguish	Limited by Doppler changes	Low power efficiency; watermark has an impact on the main signal	Characteristics are random and weak; poor stability

## 2. System Model

As shown in Figure 1, we consider a ubiquitous dual-hop wireless network model with four entities that are represented by Alice (A), Eve (E), Relay (R), and Bob (B). Due to long distance, Alice and Bob can not communicate directly, and node R is required to relay signals. Alice and Eve are in different places, so their signals reach the relay through

different buildings, indicating that the two sides pass through different multipath channels in the first hop. Whether the signal is sent by Alice or Eve, Relay amplifies and forwards signals to Bob. Supposing that the last frame Bob received is from Alice, if the new frame Bob receives is from Alice, its channel characteristics will have a strong correlation with the previous frame. Otherwise, if it is from Eve, the channel from Eve to the Relay and the channel from Alice to the Relay are independent, and the channel characteristics will be different from the previous frame so that Bob can use this feature to identify the sender.



**Figure 1.** System model: Alice communicates with Bob with aid of amplify and forward (AF) relay; Eve is a would-be intruder impersonating Alice.

Assuming that there are abundant reflectors in the propagation environment, each segment of the cascade channel can be considered as a time-varying multipath channel. Alice sends signal  $s(t)$  with Power  $P_1$ , and Relay receives and forwards it to Bob with amplification factor  $\kappa$ . Transmission power of Eve is  $P_1$ , which is supposed to imitate Alice. Thus, the signal Bob receives can be presented as:

$$y(t) = \kappa \sqrt{P_1} \sum_{l_1=1}^{L_1} \sum_{l_2=1}^{L_2} h_{l_1}^X(t) * h_{l_2}(t) * s(t) + \kappa \sum_{l_2=1}^{L_2} h_{l_2}(t) * n_1(t) + n_2(t) \quad (1)$$

where  $*$  is signal convolution, and  $h_{l_1}^X(t)$  is the channel impulse response of  $l_1$  multipath of the first hop.  $n_1$  and  $n_2$  are additive white Gaussian noises (AWGN) at R and B, the powers of which are denoted by  $N_1$  and  $N_2$ , respectively. Relay retransmits the received signal to Bob at power  $P_2$ , and the multiplied amplification factor is:

$$\kappa = \sqrt{\frac{P_2}{P_1 + N_1}}. \quad (2)$$

The work in [14] obtains multiple independent detection statistics by assuming multipath channels have the same average gain and different delay to improve detection probability. Considering the actual situation, multipath channels usually have different gain levels, and this paper uses the broadband multicarrier transmission mode to obtain multiple channel fading coefficients in the frequency domain to expand the application scenarios. The signal Bob receives in frequency domain can be presented as:

$$Y(k, t) = \kappa H_{RB}(k, t) \times \left( \sqrt{P_1} H_{XR}(k, t) \times S(k, t) + N_R(k, t) \right) + N_B(k, t) \quad (3)$$

where  $H_{XR}(k, t)$  and  $H_{RB}(k, t)$  are the channel frequency responses of X-R and R-B on the  $k$ th subcarrier at time  $t$ .

To describe the temporal variation of channel frequency response in each hop between two adjacent time instants, we employ the auto-regressive model of order 1 in [10], which can be expressed as:

$$\begin{cases} H_{XR}(k, t) = \rho_1 H_{XR}(k, t-1) + \sqrt{1 - \rho_1^2} u_1 \\ H_{RB}(k, t) = \rho_2 H_{RB}(k, t-1) + \sqrt{1 - \rho_2^2} u_2 \end{cases} \quad (4)$$

where  $u_1$  and  $u_2$  are complex Gaussian variables that are independent of  $H_{XR}(k, t-1)$  and  $H_{RB}(k, t-1)$  respectively, as denoted by  $u_1 \sim CN(0, 1)$  and  $u_2 \sim CN(0, 1)$ .  $\rho_1$  and  $\rho_2$  are correlation coefficients between samples spaced by  $T$  in the first and second hop, given by:

$$\begin{cases} \rho_1 = J_0(2\pi T f_{d1}) \\ \rho_2 = J_0(2\pi T f_{d2}) \end{cases} \quad (5)$$

where  $J_0(\cdot)$  is the zero order Bessel function of the first kind,  $f_{d1}$  and  $f_{d2}$  are the maximum Doppler frequency of two channels, respectively, and  $T$  is the time duration of an orthogonal frequency division multiplexing (OFDM) symbol.

Bob receives signal and uses pilot information to estimate frequency response of cascade channel. Without loss of generality, with the least square method, results can be expressed as:

$$\hat{H}_{XB}(k, t) = \kappa \sqrt{P_1} H_{XR}(k, t) \times H_{RB}(k, t) + \underbrace{\kappa \hat{N}_R(k, t) \times H_{RB}(k, t) + \hat{N}_B(k, t)}_W \quad (6)$$

where  $\hat{N}_R(k, t)$  and  $\hat{N}_B(k, t)$  are the estimation error caused by AWGN and can be modeled as complex Gaussian variables with zero mean, and the variance is denoted by  $N_1$  and  $N_2$  [9]. In Formula (6), the first term is the effective term, and the last two terms are equivalent noise terms.  $\hat{H}_{XB}(k, t)$  follows complex Gaussian distribution. No matter whether the current message is from  $A$  or  $E$ , the second hop it passes through is  $R$ - $B$ , and  $B$  can extract the channel frequency response of  $R$ - $B$  by exploiting channel estimation technique in [14,15].

### 3. Authentication Scheme Based on Channel Characteristics

#### 3.1. Scheme Based on Likelihood Ratio

Supposing that the actual sender of the current signal is  $X$ , channel frequency response changes  $\Delta \hat{H}_{XB}(k)$  such that what Bob obtains from the  $k$ th carrier can be expressed as:

$$\begin{aligned} \Delta \hat{H}_{XB}(k) &= \hat{H}_{XB}(k, t) - \hat{H}_{AB}(k, t-1) \\ &= \underbrace{\kappa \sqrt{P_1} [H_{RB}(k, t) H_{XR}(k, t) - H_{RB}(k, t-1) H_{AR}(k, t-1)]}_{X_1} + \\ &\quad \underbrace{\kappa H_{RB}(k, t) \hat{N}_R(k, t) - \kappa H_{RB}(k, t-1) \hat{N}_R(k, t-1) + \hat{N}_B(k, t) - \hat{N}_B(k, t-1)}_{X_2}. \end{aligned} \quad (7)$$

If the signal is from Alice,  $H_{AR}(k, t)$  and  $H_{AR}(k, t-1)$  are correlated. According to Formulas (4) and (7), in case  $H_{RB}(k, t)$  and  $H_{RB}(k, t-1)$  are provided,  $\Delta \hat{H}_{AB}(k)$  can be presented as the sum of independent Gaussian variables, which follow complex Gaussian with zero mean, and variance can be presented as:

$$\begin{aligned} \sigma_{Ak}^2 &= \frac{P_1 P_2}{P_1 + N_1} (\rho_1 H_{RB}(k, t) - H_{RB}(k, t-1))^2 + \frac{P_1 P_2}{P_1 + N_1} (1 - \rho_1^2) H_{RB}(k, t)^2 \\ &\quad + \frac{P_2 N_1}{P_1 + N_1} (H_{RB}(k, t)^2 + H_{RB}(k, t-1)^2) + 2N_2. \end{aligned} \quad (8)$$

If the signal is from Eve, similarly, the variance of  $\Delta\hat{H}_{EB}(k)$  can be presented as:

$$\sigma_{E,k}^2 = P_2 \left( H_{RB}(k,t)^2 + H_{RB}(k,t-1)^2 \right) + 2N_2. \quad (9)$$

Alice has a correlation at the adjacent time, so  $\sigma_{Ak}^2$  is smaller than  $\sigma_{E,k}^2$ .

We define  $\Delta\hat{H}_{XB}(k)$  as a vector consisting of temporal channel variation from  $N$  independent subcarriers, which is denoted by:

$$\Delta\hat{H}_{XB} \triangleq \left[ \hat{\Delta}_{XB}(1), \Delta\hat{H}_{XB}(2), \dots, \Delta\hat{H}_{XB}(N) \right] \quad (10)$$

Each element of  $\Delta\hat{H}_{XB}(k)$  follows Gaussian with zero mean, and its variance is shown in Formulas (8) and (9). Each element is statistically independent, so joint probability density function of  $\Delta\hat{H}_{XB}$  can be presented as:

$$f(\Delta\hat{H}_{XB}; H_n) = \frac{1}{(2\pi)^{N/2} \prod_{k=1}^N \sigma_{X,k}} \exp \left\{ - \sum_{k=1}^N \frac{1}{2\sigma_{X,k}^2} \left( \hat{H}_{XB}(k,t) - \hat{H}_{AB}(k,t-1) \right)^2 \right\} \quad (11)$$

where  $n = 0, 1$  are null hypothesis and alternative hypothesis respectively. Then, likelihood ratio functions can be expressed as:

$$L(\Delta\hat{H}_{XB}) = \frac{f(\Delta\hat{H}_{XB}; H_1)}{f(\Delta\hat{H}_{XB}; H_0)} = \sum_{k=1}^N \left( \frac{\sigma_{E,k}^2 - \sigma_{A,k}^2}{\sigma_{A,k}^2 \sigma_{E,k}^2} \right) \left( \hat{H}_{XB}(k,t) - \hat{H}_{AB}(k,t-1) \right)^2 \frac{H_1}{H_0} l_0 \quad (12)$$

Each summation item in Formula (12) represents change in different subcarriers. Likelihood ratio function in each carrier can be presented as:

$$L(\Delta\hat{H}_{XB}(k)) = \underbrace{\left( \frac{\sigma_{E,k}^2 - \sigma_{A,k}^2}{\sigma_{A,k}^2 \sigma_{E,k}^2} \right)}_{\varphi_k} \left( \hat{H}_{XB}(k,t) - \hat{H}_{AB}(k,t-1) \right)^2 \quad (13)$$

where  $\varphi_k$  is different from each subcarrier, which is related to fading and subcarrier number of two hops. In conclusion, Formula (13) is sum of squares of independent Gaussian variables that have different variance. It is hard to obtain optimal detection threshold  $l_0$ .

### 3.2. Scheme Based on Majority Voting

To simplify analysis, we make decisions on  $N$  independent subcarriers respectively. The temporal variation of channel frequency response on the same subcarrier between two adjacent time instants is compared with that of a threshold  $Th_k$ . If it is larger than the threshold, the voting result is recorded as one, which suggests that the current message is more likely from the illegitimate transmitter  $E$ . On the contrary, if the temporal variation is smaller than the threshold, the result outputs zero. This process can be mathematically expressed as:

$$Q_k = \begin{cases} 1, & \left( \frac{\sigma_{E,k}^2 - \sigma_{A,k}^2}{\sigma_{A,k}^2 \sigma_{E,k}^2} \right) \left( \hat{H}_{XB}(k,t) - \hat{H}_{AB}(k,t-1) \right)^2 > Th_k \\ 0, & \text{otherwise} \end{cases} \quad (14)$$

where  $Th_k$  is the decision threshold. We perform the same operation shown in expression Formula (14) over  $N$  independent subcarriers, and then sum up  $N$  results with equal gain, which are denoted by

$$\Omega = \sum_{k=1}^N Q_k. \quad (15)$$

Based on the above voting results in Formula (15), we establish a binary hypothesis testing to differentiate the illegal transmitter  $E$  from  $A$ . More specifically, we make the

authentication decision by comparing the sum Formula (15) with a non-negative integer, which can be formulated as:

$$\begin{aligned} H_0 : \Omega &\leq Z \\ H_1 : \Omega &> Z \end{aligned} \quad (16)$$

where  $Z$  is the overall decision threshold.

#### 4. Performance Analysis Based on False Alarm Rate and Miss Detection Rate

Considering that FAR and MDR are two fundamental metrics of authentication performance, in this section we analyze FAR and MDR based on [14], and then derive the theoretic decision threshold.

##### 4.1. False Alarm Rate

Supposing that the signal is from Alice, Formulas (7) and (8) entail that frequency response change  $\Delta\hat{H}_{AB}(k)$  follows complex Gaussian with zero mean and variance  $\sigma_{A,k}^2$ . Based on probability statistics,  $|\Delta\hat{H}_{AB}(k)|^2$  follows exponential distribution with parameter  $\sigma_{A,k}^2$ , and its probability density function can be expressed as:

$$f_{|\Delta\hat{H}_{AB}(k)|^2}(x) = \frac{1}{\sigma_{A,k}^2} e^{-\frac{x}{\sigma_{A,k}^2}} \quad (17)$$

where  $\sigma_{A,k}^2$ , shown in Formula (8), is a time-variance function. Based on majority voting, each independent  $|\Delta\hat{H}_{XB}(k)|^2$  is multiplied by  $\varphi_k$ , and then compared with threshold  $Th_k$ . So at time  $t$ , the probability that decision in the  $k$ th subcarrier outputs one is:

$$\begin{aligned} P_{H_0}(Q_k = 1 | H_{RB}(k, t), H_{RB}(k, t - 1)) &= \int_{Th_k/\varphi_k}^{\infty} \frac{1}{\sigma_{A,k}^2} e^{-\frac{x}{\sigma_{A,k}^2}} dx \\ &= \exp\left\{-\frac{\sigma_{E,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\} \end{aligned} \quad (18)$$

Then, the probability that the voting outputs one under null hypothesis is the expectation of Formula (18) about  $H_{RB}(k, t)$  and  $H_{RB}(k, t - 1)$ , which is given by:

$$P_{H_0}(Q_k = 1) = E\left\{\exp\left\{-\frac{\sigma_{E,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\}\right\} \quad (19)$$

where  $E$  is expectation of  $H_{RB}(k, t)$  and  $H_{RB}(k, t - 1)$ . We use  $P_{H_0}(Q_k = 0)$ , denoting the probability that the voting outputs zero under null hypothesis, which is the complement of  $P_{H_0}(Q_k = 1)$ . Moreover, since noises are white and the transmit power is equally allocated on each subcarrier, the probability  $P_{H_0}(Q_k = 1)$  is identical for all independent subcarriers, and so is  $P_{H_0}(Q_k = 0)$ . The probability of  $Z$  out of  $N$  outputting one is:

$$P_{H_0}(\Omega = z) = \binom{N}{z} P_{H_0}(Q = 1)^z P_{H_0}(Q = 0)^{N-z}. \quad (20)$$

So, the theoretical expression of FAR can be expressed as [14]:

$$P_{fa} = \sum_{z=Z+1}^N \binom{N}{z} P_{H_0}(Q = 1)^z P_{H_0}(Q = 0)^{N-z}. \quad (21)$$

##### 4.2. Miss Detection Rate

Derivation of the MDR is similar with FAR. We derive probability of each subcarrier and obtain theoretical expression of MDR after majority voting.

Similar with  $|\Delta\hat{H}_{AB}(k)|^2$ ,  $|\Delta\hat{H}_{EB}(k)|^2$  follows exponential distribution with parameter  $\sigma_{E,k}^2$ , and its probability density function can be expressed as:

$$f_{|\Delta\hat{H}_{EB}(k)|^2}(x) = \frac{1}{\sigma_{E,k}^2} e^{-\frac{x}{\sigma_{E,k}^2}}. \quad (22)$$

We can obtain the probability that the  $k$ th voting outputs one (Eve) at time  $t$  by integrating the probability density function, which is shown as:

$$\begin{aligned} P_{H_1}(Q_k = 1 | H_{RB}(k, t), H_{RB}(k, t - 1)) &= \int_{Th_k}^{\infty} \frac{1}{\sigma_{E,k}^2} e^{-\frac{x}{\sigma_{E,k}^2}} dx \\ &= \exp\left\{-\frac{\sigma_{A,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\}. \end{aligned} \quad (23)$$

Similarly, we can obtain the probability that the voting outputs one under alternative hypothesis, which is given by:

$$P_{H_1}(Q = 1) = E\left\{\exp\left\{-\frac{\sigma_{A,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\}\right\}. \quad (24)$$

Then, we can derive the theoretical expression based on majority voting [14], which is expressed as:

$$P_{md} = \sum_{z=0}^Z \binom{N}{z} P_{H_1}(Q = 1)^z P_{H_1}(Q = 0)^{N-z}. \quad (25)$$

#### 4.3. Decision Threshold

In this section, we analyze two threshold criteria. One is constant FAR threshold based on Neyman-Perarson criterion, whose FAR is obtained by Formula (21), which can be applied to scenarios with strict requirement on FAR. The other one is a threshold based on minimum error probability criterion. We define  $V$  as the sum of FAR and MDR:

$$V \triangleq P_{fa} + P_{md}. \quad (26)$$

Based on Formulas (21) and (25),  $P_{fa}$  and  $P_{md}$  are the sum of two binomial distributions with different probabilities, so the Formula (26) is hard to analyze directly. To simplify analysis, we approximate the minimum sum of error rate after majority voting as minimum sum of error rate on single subcarrier. The function can be rewritten as:

$$\bar{V} \triangleq P_{H_0}(Q = 1) + P_{H_1}(Q = 0). \quad (27)$$

Formula (27) can be regarded as a special case when  $N = 1$  and  $Z = 0$  in Formula (26). The channel characteristics of each subcarrier are independent and the distribution characteristics are consistent; thus, changing threshold  $Th_k$  to let Formula (27) be the smallest can also make Formula (26) smallest. Based on Formula (21) and Formula (24), the derivative of Formula (27) with respect to  $Th_k$  can be rewritten as:

$$\frac{\partial \bar{V}}{\partial Th_k} = E\left\{-\frac{\sigma_{E,k}^2}{\sigma_{E,k}^2 - \sigma_{A,k}^2} \exp\left\{-\frac{\sigma_{E,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\} + \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2 - \sigma_{A,k}^2} \exp\left\{-\frac{\sigma_{A,k}^2 Th_k}{\sigma_{E,k}^2 - \sigma_{A,k}^2}\right\}\right\}. \quad (28)$$

Then, we can obtain poles of the Formula (28):

$$Th_k = \ln(\sigma_{E,k}^2) - \ln(\sigma_{A,k}^2). \quad (29)$$

The pole in Formula (28) is clearly an extremely small point.



## 5. Optimal Power Distribution Scheme Based on Authentication Performance

In dual-hop networks, relay nodes and receivers are often different in both equipment performance and surrounding environment. This section describes how to adjust the power ratio between the sender and trunk nodes to optimize the authentication performance of the system.

### 5.1. Optimized Module

In this section, we can optimize the transmit power allocation between  $P_1$  and  $P_2$ , improving the authentication performance. More specifically, the optimization problem is to minimize the sum of FAR and MDR on condition of fixed total transmit power, which can be mathematically expressed as:

$$\begin{aligned} \min_{P_1, P_2} \quad & V \triangleq P_{fa} + P_{md} \\ \text{s.t.} \quad & P_1 + P_2 = P \end{aligned} \quad (30)$$

To simplify the analysis, the objective function is replaced by  $P_{H_0}(Q_k = 1) + P_{H_1}(Q_k = 0)$ , which represents the sum of FAR and MDR when making a decision on a single carrier. The more correct the decision on each subcarrier is, the less that errors will occur in the final combined decision; therefore, the optimization problem is updated to:

$$\begin{aligned} \min_{P_1, P_2} \quad & V \triangleq P_{H_0}(Q_k = 1) + P_{H_1}(Q_k = 0) \\ \text{s.t.} \quad & P_1 + P_2 = P \end{aligned} \quad (31)$$

The optimal threshold provided in Formula (29) is a time-varying value, and the value for each subcarrier is different, which makes use of the last and present channel estimation of the second hop  $R$ - $B$ . Substituting Formula (29) into Formula (31), the objective function can be rewritten as:

$$V = E \left\{ \left( \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} \right)^{\frac{\sigma_{A,k}^2}{\sigma_{E,k}^2 - \sigma_{A,k}^2}} \left( \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} - 1 \right) \right\} + 1. \quad (32)$$

Ignoring the constant term at the end of Formula (32), the expectation in Formula (32) is a double integration of Gaussian variables  $H_{RB}(k, t)$  and  $H_{RB}(k, t - 1)$ , and the item to be integrated is also complicated. We denote the item in the expectation operator as:

$$\psi \triangleq \left( \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} \right)^{\frac{\sigma_{A,k}^2}{\sigma_{E,k}^2 - \sigma_{A,k}^2}} \sigma_{A,k}^2 \left( \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} - 1 \right). \quad (33)$$

The expression in Formula (33) can be simplified by taking the logarithm, and a minus sign is added since  $\sigma_{A,k}^2 < \sigma_{E,k}^2$ , which yields:

$$\ln(-\psi) = \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2 - \sigma_{A,k}^2} \ln \left( \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} \right) + \ln \left( 1 - \frac{\sigma_{A,k}^2}{\sigma_{E,k}^2} \right). \quad (34)$$

After above simplification, the concerned optimization problem can be rewritten as:

$$\begin{aligned} \min_{P_1, P_2} \quad & \frac{N_1}{P_1} + \frac{N_2}{P_2} + \frac{N_1 N_2}{P_1 P_2} \\ \text{s.t.} \quad & P_1 + P_2 = P \end{aligned} \quad (35)$$



### 5.2. Upper Bound of the Objective Function

In Formula (35), the double integral of Gaussian variables still exists, which prevents us from finally solving the problem. When solving optimization problems, we usually use the upper bound to replace the objective function that needs to be minimized if the original one is difficult to solve. Here, we provide the proposition  $E\{\sigma_{A,k}^2\}/E\{\sigma_{E,k}^2\}$  is the upper bound of the objective function.

**Proof.** We define  $\Delta$  as the difference between  $\sigma_{A,k}^2$  and  $\sigma_{E,k}^2$  to simplify the function, which can be rewritten as:

$$\Delta \triangleq \sigma_{E,k}^2 - \sigma_{A,k}^2 = \frac{2\rho_1 P_1 P_2}{P_1 + N_1} H_{RB}(k, t) \cdot H_{RB}^*(k, t - 1) \quad (36)$$

$H_{RB}(k, t - 1) \approx H_{RB}(k, t - 1)$ ,  $H_{RB}(k, t - 1)$  and  $H_{RB}(k, t)$  are in coherent time. Thus, the first derivative of  $\Delta$  with respect to  $H_{RB}(k, t)$  can be represented as:

$$\frac{\partial \Delta}{\partial H_{RB}(k, t)} = \frac{4\rho_1 P_1 P_2}{P_1 + N_1} H_{RB}(k, t) \quad (37)$$

Based on Formula (9), the first derivative of  $\sigma_{E,k}^2$  with respect to  $H_{RB}(k, t)$  can be expressed as:

$$\frac{\partial \sigma_{E,k}^2}{\partial H_{RB}(k, t)} = 4P_2 H_{RB}(k, t) \quad (38)$$

Comparing Formulas (37) and (38), we can derive that:

$$0 < \frac{\partial \Delta}{\partial H_{RB}(k, t)} < \frac{\partial \sigma_{E,k}^2}{\partial H_{RB}(k, t)}. \quad (39)$$

As  $H_{RB}(k, t)$  goes up,  $\sigma_{E,k}^2$  goes up, while  $\Delta/\sigma_{E,k}^2$  goes down. Thus, the correlation between the two is less than zero, which can be rewritten as:

$$\begin{aligned} \text{cov}\left(\sigma_{E,k}^2, \frac{\Delta}{\sigma_{E,k}^2}\right) &= E\left\{\sigma_{E,k}^2 \times \frac{\Delta}{\sigma_{E,k}^2}\right\} - E\{\sigma_{E,k}^2\}E\left\{\frac{\Delta}{\sigma_{E,k}^2}\right\} \leq 0 \\ &\Leftrightarrow E\{\sigma_{E,k}^2\}E\left\{\frac{\Delta}{\sigma_{E,k}^2}\right\} \geq E\{\Delta\} \end{aligned} \quad (40)$$

Substituting (36) into (40), we can obtain the following inequation:

$$E\left\{\frac{\sigma_{A,k}^2}{\sigma_{E,k}^2}\right\} \leq \frac{E\{\sigma_{A,k}^2\}}{E\{\sigma_{E,k}^2\}} \quad (41)$$

□

In Rayleigh channel, correlation coefficient of  $H_{RB}(k, t)$  and  $H_{RB}(k, t - 1)$  with zero mean and one variance is  $\rho_2$  in Formula (5). Thus,  $E\{\sigma_{A,k}^2\}$  can be written as:

$$\begin{aligned} E\{\sigma_{A,k}^2\} &= \frac{P_1 P_2}{P_1 + N_1} \left[ \rho_1^2 E\{H_{RB}(k, t)^2\} - 2\rho_1 E\{H_{RB}(k, t)H_{RB}^*(k, t - 1)\} + E\{H_{RB}(k, t - 1)^2\} \right] \\ &+ \frac{P_1 P_2}{P_1 + N_1} (1 - \rho_1^2) E\{H_{RB}(k, t)^2\} + \frac{P_2 N_1}{P_1 + N_1} \left[ E\{H_{RB}(k, t)^2\} + E\{H_{RB}(k, t - 1)^2\} \right] + 2N_2 \quad (42) \\ &= 2P_2 + 2N_2 - \frac{2P_1 P_2 \rho_1 \rho_2}{P_1 + N_1} \end{aligned}$$

Similarly,  $E\{\sigma_{E,k}^2\}$  can be written as:

$$E\{\sigma_{E,k}^2\} = P_2 \times \left( E\{H_{RB}(k, t)^2\} + E\{H_{RB}(k, t - 1)^2\} \right) + 2N_2 = 2P_2 + 2N_2. \quad (43)$$

Thus, the upper bound of objective function can be represented as:

$$\frac{E\{\sigma_{A,k}^2\}}{E\{\sigma_{E,k}^2\}} = \frac{2P_2 + 2N_2 - \frac{2P_1P_2\rho_1\rho_2}{P_1+N_1}}{2P_2 + 2N_2} = 1 - \frac{\rho_1\rho_2}{1 + \frac{N_1}{P_1} + \frac{N_2}{P_2} + \frac{N_1N_2}{P_1P_2}}. \quad (44)$$

### 5.3. Approximate Optimal Solution

In (44), parameters of upper bound  $E\{\sigma_{A,k}^2\}/E\{\sigma_{E,k}^2\}$  contain power of the sender  $P_1$ , power of the relay  $P_2$ , noise power of the relay  $N_1$ , noise power of the receiver  $N_2$ , correlation coefficient in first hop  $\rho_1$ , and correlation coefficient in second hop  $\rho_2$ , where  $P_1$  and  $P_2$  are adjustable variables. Usually,  $\rho_1$  and  $\rho_2$  remain unchanged for a period of time; thus,  $\rho_1$  and  $\rho_2$  in Formula (44) have little influence on power distribution. As a result, we ignore  $\rho_1, \rho_2$  and constant item in (44), so the optimization problem can be written as:

$$\begin{aligned} \min_{P_1, P_2} \quad & \frac{N_1}{P_1} + \frac{N_2}{P_2} + \frac{N_1N_2}{P_1P_2} \\ \text{s.t.} \quad & P_1 + P_2 = P \end{aligned} \quad (45)$$

We define  $\mu$  as the ratio of transmission power and total power, and  $T$  as objective function in (45). Thus,  $T$  can be written as:

$$T = \frac{(N_2P - N_1P)\mu + N_1P + N_1N_2}{(\mu - \mu^2)P^2}. \quad (46)$$

We take the derivative of  $T$  with respect to  $\mu$  and let it equal to 0:

$$\frac{P^2[(N_2P - N_1P)\mu^2 + (2N_1P + 2N_1N_2)\mu - N_1P - N_1N_2]}{[(\mu - \mu^2)P^2]^2} = 0. \quad (47)$$

Combining three cases of  $N_1$  and  $N_2$ , we can write the power allocation  $\mu$  as:

$$\mu_0 = \frac{P_1}{P} = \frac{\sqrt{N_1P + N_1N_2}}{\sqrt{N_1P + N_1N_2} + \sqrt{N_2P + N_1N_2}}. \quad (48)$$

## 6. Simulation Results

In this section, for the purpose of validating the theoretical results of Sections 4 and 5, we use MATLAB to simulate the theoretical results.

We define the signal-noise ratio (SNR) of the dual-hop wireless networks in the concerned scenario as the total power transmitted to the noise power, given by:

$$\text{SNR} = \frac{P_1 + P_2}{N_1 + N_2}. \quad (49)$$

The key simulation parameter settings are illustrated in Tables 2 and 3.

As shown in Table 2, carrier frequency, subcarrier interval and channel parameters used in the table are typical LTE system parameters [16]. In addition, the number of subcarriers corresponds to the minimum bandwidth of 1.25 MHz in LTE. In fact, with the increase in bandwidth, the number of independent subcarriers that can be obtained in the frequency domain increases, which will be more favorable to the algorithm in this paper. The false alarm probability of identity authentication is selected as a typical value of 5%.

Without loss of generality, the coherent bandwidth can be calculated by the parameters in the Table 2. Moreover, independent subcarriers can be selected, and the total transmit power is assumed to be 1.

**Table 2.** System parameters.

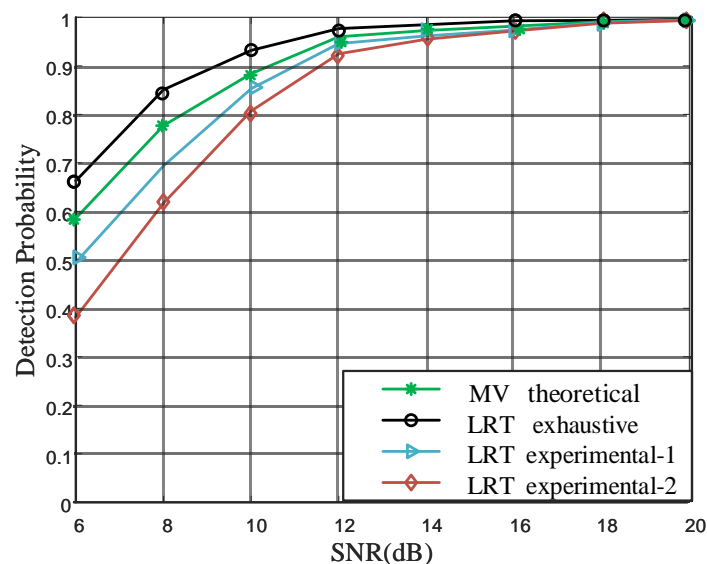
Carrier frequency	2.4 GHz
Subcarrier interval	15 kHz
Number of subcarriers	128
Relative speed	200 km/h

**Table 3.** Channel parameters of extended vehicular A (EVA) model.

Number of multipaths	9
Multipath time delay (ns)	(0 30 150 310 370 710 1090 1730 2510)
Multipath relative power (dB)	(0 −1.5 −1.4 −3.6 −0.6 −9.1 −7.0 −12.0 −16.9)

To explore the difference in authentication performance between likelihood ratio test (LRT) and majority voting algorithm (MV), we compare them in terms of the probability of detection while keeping FAR constant as 0.05. The threshold involved in MV is theoretically derived, while the decision threshold in LRT is found by exhaustive method to keep FAR constant. We also attempt to find the threshold while ignoring the influence of cascade channel, as well as the threshold based on single-carrier threshold multiplied by the number of independent subcarriers. The simulation results are shown in Figure 2 (the vertical axis represents the detection probability, and the horizontal axis the signal-to-noise ratio).

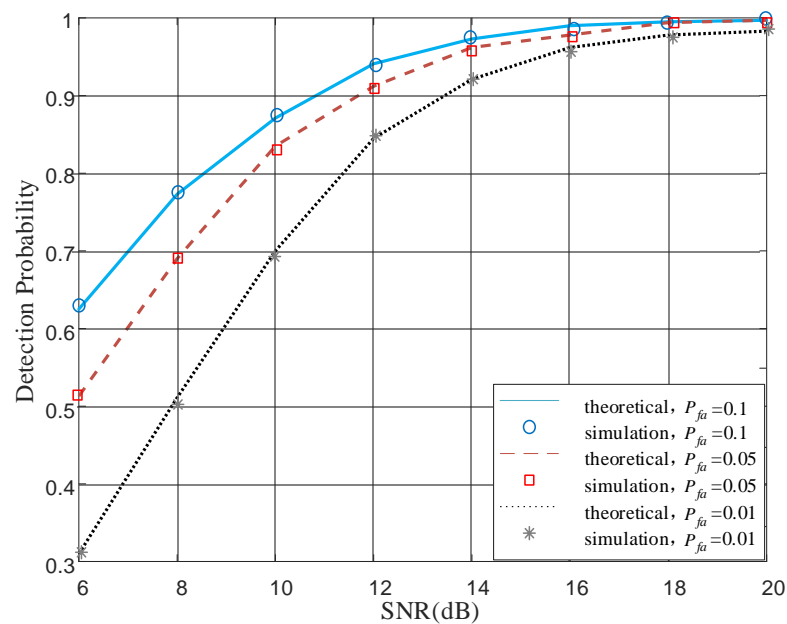
As shown in Figure 2, MV is better than two experimental LRTs, while exhaustive is better than MV. Because the temporal channel variation on different subcarriers can be summed up in LRT, which has a smooth effect. While the decision on each subcarrier can be regard as one-bit quantization, and some precision is lost. The gap between exhaustive LRT, experimental-1 LRT, experimental-2 LRT, and MV reduces in the high SNR region, where the detection probability is more than 95%, meeting the requirements of general systems.

**Figure 2.** Likelihood ratio test (LRT) and majority voting algorithm comparison.

To validate the theoretical expression for FAR and MDR, derived in Formulas (21) and (25), we compare them with simulation results. In MV algorithm, we can adjust the decision threshold to realize constant FAR as needed, and the probability of detection with different FAR is shown in Figure 3 (the vertical axis represents the detection probability and the horizontal axis the signal-to-noise ratio).

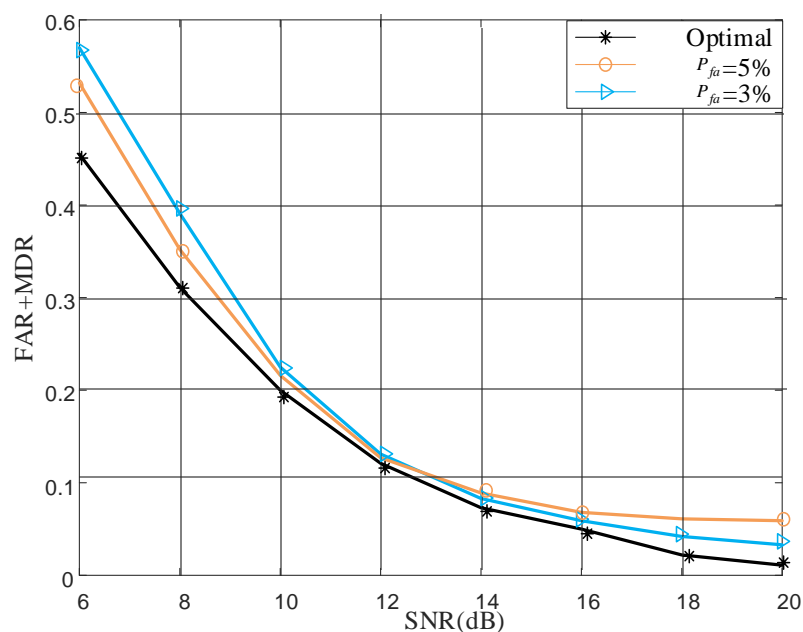
In Figure 3, the theoretical results are consistent with simulation results under different parameters, which prove the correctness of the formulas Formulas (21) and (25). The authentication based on majority voting algorithm can be a theoretically analyzed

performance, which is a major advantage over LRT and also makes it more practical. Under constant false alarm condition, the missed detection probability tends to a minimum value with the increase in SNR by optimizing the threshold.



**Figure 3.** Theoretical expression for false alarm rate (FAR) and miss detection rate (MDR) validation.

To validate minimum error probability threshold proposed in Formula (29), we compare sum of FAR and MDR in three simulation scenarios that are optimal: 5% FAR and 3% FAR. As shown in Figure 4, optimal threshold is below the other two curves, which meets its physical meaning. In addition, two curves with different FARs intersect, since at low SNR, the difference between legal and illegal transmitter is small, causing MDR to go down as FAR goes up, and this is the opposite case when SNR is high.



**Figure 4.** Authentication performance at different thresholds.

To prove the universality of the threshold Formula (29), comparative analysis was conducted in several different scenarios, which are characterized by the noise power at relay

since the total noise power was controlled as one. In Figure 5, authentication performance of theory and exhaustion fits perfectly in three scenarios.

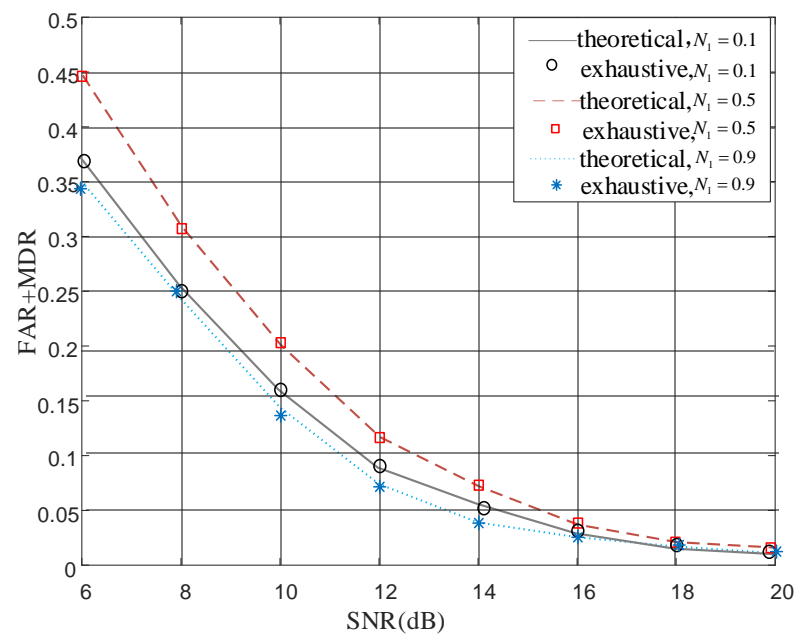


Figure 5. Authentication performance in different relay noise power.

To compare authentication under two power allocation schemes, we perform simulation at different SNRs, and results are shown in Figure 6. As shown in Figure 6, optimal scheme is better than equal allocation, especially at low SNR, since difference between legal and illegal transmitter has more influence than noise at high SNR.

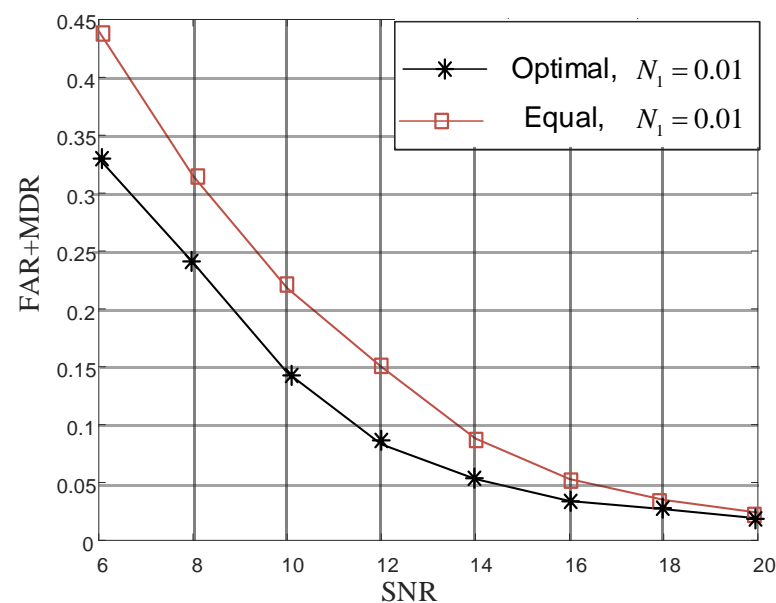


Figure 6. Performance comparison of two allocation schemes.

To validate the performance of the theoretically approximate optimal scheme, we compare it with exhaustive optimal scheme in Figure 7, where theoretical approximate optimal scheme is derived in Formula (48) and exhaustive optimal scheme is designed to exhaust power allocation with small granularity. As shown in Figure 7, the gap between the practical minimum sum of FAR and MDR and the sum caused by the proposed power

allocation is about 0.002. The small gap implies that Formula (48) is approximately optimal and effective in practice.

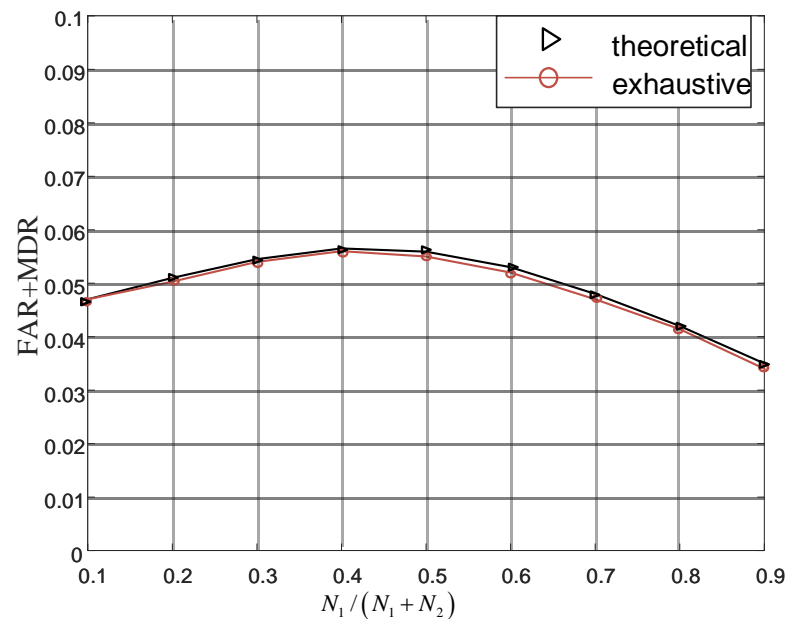


Figure 7. Optimal threshold validation.

## 7. Conclusions

This paper explored channel-based physical-layer authentication in dual-hop wireless networks. By analyzing the characteristics of cascaded channel, we established the likelihood ratio test (LRT) at first. To simplify, the majority voting algorithm was employed. Based on this simplification, we derived the theoretical expressions for false alarm rate (FAR) and miss detection rate (MDR), and we analyzed the upper bound for their sum. Moreover, we proposed an optimal decision threshold that utilized the channel estimation of the second hop to provide a more accurate decision. With this threshold, the optimal power allocation minimizing the sum of FAR and MDR was derived. In addition, it is expected that the proposed power allocation is useful and provides a novel mode of thought in optimizing dual-hop physical-layer authentication. When in a mobile state, the authentication performance based on channel characteristics declines. Adjusting the number and position of pilots used for authentication can optimize the performance. In addition, the algorithm can be further optimized by channel state prediction and other technologies.

To sum up, in 6G large-scale heterogeneous network, there are a large number of devices with different upper-layer access protocols. The physical-layer authentication technology is transparent to the upper-layer protocols, and thus it has good compatibility and can complement the existing upper-layer traditional security schemes to jointly build a more comprehensive security system.

**Author Contributions:** All the authors have contributed in various degrees to ensuring the quality of this work: conceptualization, N.F. and J.S.; methodology, X.L. and Y.H.; validation, T.T., N.F. and J.S.; formal analysis, X.L.; writing—original draft preparation, Y.H.; writing—review and editing, Y.H. and T.T.; funding acquisition, X.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by the National Preresearch Project (Y18-TJZY-11) and the Foundation of Stability Support Plan for National Key Lab (IFN2020104).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

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

## Abbreviations

The following abbreviations are used in this manuscript:

LRT	Likelihood ratio test
MV	Majority voting
FAR	False alarm rate
MDR	Miss detection rate
GLRT	Generalized likelihood ratio test
CIR	Channel impulse response
AWGN	Additive white Gaussian noises
OFDM	Orthogonal frequency division multiplexing
SNR	Signal Noise Ratio
AF	Amplify and Forward
UAV	Unmanned Aerial Vehicle
$E\{\}/\exp\{\}$	expectation
*	convolution
$\Sigma$	sum
$J_0(\cdot)$	zero order Bessel fun
$\binom{N}{z}$	permutation and combination

## References

1. Kartalopoulos, S.V. A primer on cryptography in communications. *IEEE Commun. Mag.* **2006**, *44*, 146–151. [\[CrossRef\]](#)
2. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What will 5G be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [\[CrossRef\]](#)
3. Li, B.; Fei, Z.; Zhang, Y.; Guizani, M. Secure UAV communication networks over 5G. *IEEE Wirel. Commun.* **2019**, *26*, 114–120.
4. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [\[CrossRef\]](#)
5. Xu, Z.; Yuan, W. Watermark BER and Channel Capacity Analysis for QPSK-Based RF Watermarking by Constellation Dithering in AWGN Channel. *IEEE Signal Process. Lett.* **2017**, *24*, 1068–1072. [\[CrossRef\]](#)
6. Lin, Y.; Tu, Y.; Dou, Z. An Improved Neural Network Pruning Technology for Automatic Modulation Classification in Edge Devices. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5703–5706. [\[CrossRef\]](#)
7. Hou, W.; Wang, X.; Chouinard, J.-Y.; Refaey, A. Physical-layer authentication for mobile systems with time-varying carrier frequency offsets. *IEEE Trans. Commun.* **2014**, *62*, 1658–1667. [\[CrossRef\]](#)
8. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2571–2579. [\[CrossRef\]](#)
9. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Channel based spoofing detection in frequency-selective Rayleigh channels. *IEEE Trans. Wirel. Commun.* **2009**, *8*, C5948–C5956. [\[CrossRef\]](#)
10. Liu, J.; Wang, X. Physical-layer authentication enhancement using two-dimensional channel quantization. *IEEE Trans. Wirel. Commun.* **2016**, *15*, C4171–C4182. [\[CrossRef\]](#)
11. Fang, H.; Wang, X.; Hanzo, L. Learning-Aided Physical Layer Authentication as an Intelligent Process. *IEEE Trans. Commun.* **2019**, *67*, 2260–2273. [\[CrossRef\]](#)
12. Fotouhi, A.; Ding, M.; Hassan, M. Deep Q-Learning for Two-Hop Communications of Drone Base Stations. *Sensors* **2021**, *21*, 1960. [\[CrossRef\]](#)
13. Rahman, M.A.; Lee, Y.; Koo, I. Energy-efficient power allocation and relay selection schemes for relay-assisted d2d communications in 5 g wireless networks. *Sensors* **2018**, *18*, 2865. [\[CrossRef\]](#)
14. Zhang, P.; Zhu, J.; Chen, Y.; Jiang, X. End-to-End Physical Layer Authentication for Dual-Hop Wireless Networks. *IEEE Trans. Access* **2019**, *7*, 38322–38336. [\[CrossRef\]](#)
15. Liu, F.J.; Tang, H. Robust physical-layer authentication using inherent properties of channel impulse response. In Proceedings of the 2011 MILCOM 2011 Military Communications Conference, Baltimore, MD, USA, 12 January 2011.
16. 3GPP (3rd Generation Partnership Project). *User Equipment Conformance Specification; Radio Transmission and Reception; Part1 Conformance Testing*, 3GPP TS 36.521-1; 3GPP: Sophia Antipolis, France, 2009.