Entropy **2015**, *17*, 368-383; doi:10.3390/e17010368

OPEN ACCESS
entropy
ISSN 1099-4300
www.mdpi.com/journal/entropy

Article

Message Authentication over Noisy Channels

Fanfan Zheng [1], Zhiqing Xiao [2], Shidong Zhou [2,3,4], Jing Wang [2,3,4] and Lianfen Huang [1,*]

[1] Department of Communication Engineering, Xiamen University, Xiamen 361005, China; E-Mail: zhengfanf@foxmail.com

[2] Department of Electronic Engineering, Tsinghua University, Beijing 100084, China; E-Mails: xzq.xiaozhiqing@gmail.com (Z.X.); zhousd@tsinghua.edu.cn (S.Z.); wangj@tsinghua.edu.cn (J.W.)

[3] State Key Laboratory on Microwave and Digital Communications, Tsinghua University, Beijing 100084, China

[4] Tsinghua National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China

* Author to whom correspondence should be addressed; E-Mail: lfhuang@xmu.edu.cn; Tel.: +86-0592-2580142.

Academic Editors: James Park and Wanlei Zhou

Received: 15 October 2014 / Accepted: 12 January 2015 / Published: 14 January 2015

Abstract: The essence of authentication is the transmission of unique and irreproducible information. In this paper, the authentication becomes a problem of the secure transmission of the secret key over noisy channels. A general analysis and design framework for message authentication is presented based on the results of Wyner's wiretap channel. Impersonation and substitution attacks are primarily investigated. Information-theoretic lower and upper bounds on the opponent's success probability are derived, and the lower bound and the upper bound are shown to match. In general, the fundamental limits on message authentication over noisy channels are fully characterized. Analysis results demonstrate that introducing noisy channels is a reliable way to enhance the security of authentication.

Keywords: authentication; information-theoretic security; wireless communication; physical layer; wiretap channel

---

1. Introduction

One of the prominent problems in communication is security, and authentication is the first step to ensure a secure communication. The failure to properly authenticate users will result in serious damage since the opponent can do whatever any valid user can do [1]. Usually, authentication is more important than confidentiality [2], because the threats of active attacks are always more serious than those of the passive ones.

In the studies of conventional authentication, most of the mechanisms [3–5] are based on encryption. The transmitter and the receiver communicate according to a previously coordinated encryption agreement with a secret key, where messages are authentic if the receiver can successfully decrypt the transmission. However, these cryptographic security mechanisms need key management to distribute, refresh, and revoke the secret keys. Due to the open air nature of wireless networks, the key management can be difficult, especially in ad hoc networks [6]. Therefore, this paper considers utilizing the noisy nature of wireless channels to extend the service life of the secret keys.

The authentication model over noiseless channels was developed by Simmons [7]. In the model, the transmitter and the receiver share a secret key K, and both of them are assumed to be honest to each other. Meanwhile, an opponent wants to trick the receiver. When the transmitter intends to send a source message M over a public channel, it transmits an encoded message $W = f(K, M)$, where $f(\cdot)$ is an authentication coding function. Upon receiving a message $\hat{W}$, the receiver should determine whether it comes from the legitimate transmitter or the opponent. The receiver uses a decoding function $d(\cdot)$ to obtain an estimate of the source message and the secret key, *i.e.*, $(\hat{M}, \hat{K}) = d(\hat{W})$. If $\hat{K} = K$, the receiver accepts $\hat{M}$; otherwise, the receiver rejects it.

There are two types of attacks considered in [7]. The first one is called an *impersonation attack*, in which the opponent sends a malicious message W' to the receiver before the legitimate transmitter sends anything. The second one is called a *substitution attack*, in which after intercepting a message W, the opponent modifies it into an erroneous message W' and sends it to the receiver. (Actually, there are two aspects of the substitution attack. Another kind of substitution attack, which is called power-substitution attack, occurs in the transmission from the transmitter to the legitimate receiver. The opponent modifies messages by overpowering the transmitter's signal with its malicious signal [3]. In the following, it will be distinguished in particular when to employ the power-substitution attack.) If the false message W' of the impersonation attack or the substitution attack is deemed as authentic and accepted by the receiver, it is called a successful attack. The success probability of the impersonation attack and the substitution attack are denoted by P_I and P_S, respectively. The lower bounds on P_I and P_S have been derived in [7], which are respectively shown as $P_I \geq 2^{-I(K;W)}$ and $P_S \geq 2^{-H(K|W)}$, where $I(K;W)$ denotes the mutual information between K and W, and $H(K|W)$ denotes the conditional entropy of K given W. One can easily figure out a tradeoff between P_I and P_S, since $H(K|W) = H(K) - I(K;W)$. Because the attack with higher success probability will be preferentially chosen, the success probability P_D of the opponent is $P_D = \max(P_I, P_S)$. Obviously, the lower bound on P_D is $P_D \geq 2^{-H(K)/2}$. It means that the best defensive strategy is to use half of the key information to protect against the impersonation attack and the other half to protect against the substitution attack.

Similar to Simmons' work, current practices firstly convert a noisy channel into a noiseless one, and then design an authentication code over the noiseless channel. However, according to the results of Wyner's wiretap channel [8], the work in [9] jointly designed the channel coding and the authentication code over noisy channels. In this way, as long as the wiretap channel's perfect secrecy capacity C_s is nonzero, the secret key can be kept hidden from the opponent by using a codebook whose codeword rate is higher than the channel capacity between the source and the opponent. Thus, the substitution attack is prevented due to the fact that the opponent cannot obtain any information about the secret key from its observed messages. Then, all the information of the secret key can be used to protect against the impersonation attack. Regarding the bounds on P_D, it has been shown that $2^{-H(K)} \leq P_D \leq 2^{-H(K)} + \alpha e^{-n\beta}$, where α and β are positive constants, and n is the codeword length. The upper bound is shown to match the lower bound as n goes to infinity. Compared with the performance of the Simmons' model, [9] brings additional security gain.

However, the work in [9] has several flaws. Firstly, it may incur the power-substitution attack. When the function $f(\cdot)$ is linear, during the transmission, an agent (e.g., Eve) could tamper with the legitimate message by a synchronously transmitted and well-designed malicious signal. Secondly, its lower bound on P_S is given by simply ignoring the intercepted information Z^n. Unfortunately, evident security flaws will happen if the coding scheme is not well-designed [10–13], then the intercepted information Z^n may provide much information about the secret key. Though it can be proved that there exists a code scheme to attain this lower bound when the codeword length n goes to infinity, it is impracticable because the codeword length is indeed limited. Thirdly, it exposes the secret key because the wiretap channel's secrecy capacity cannot be guaranteed to stay nonzero, e.g., the channels are time-varying or Eve's channel is not easy to obtain. (The works in [14–16] provide the calculation and measurement of the probability of a nonzero secrecy capacity $P(C_s > 0)$ for Rayleigh fading channels, *etc.*)

This paper makes the following contributions. Firstly, we propose an enhanced message authentication scheme. Specifically, we securely transmit an authentication tag T instead of the secret key K in [9]. This authentication tag T encapsulates the information of the secret key K and the source message M. Secondly, this scheme can protect against the power-substitution attack. Thirdly, we derive our scheme's information-theoretic lower bounds on P_I, P_S and P_D, and give the sufficient and necessary conditions for tightness. In addition, we also derive our scheme's information-theoretic upper bound on P_D.

The rest of this paper is organized as follows. Section 2 provides various aspects of our authentication scheme in the designated scenario. Section 3 introduces the security analysis of our scheme and the performance comparison with the previous works in detail. Section 4 concludes the paper.

Notation: Throughout this paper, random variables are denoted by upper case letters (e.g., X), the realizations of the corresponding random variables are denoted by lower case letters (e.g., x), and the corresponding finite alphabets are denoted by calligraphic letters (e.g., $\mathcal{X}$). The n-length sequences of the elements X and x are denoted by X^n and x^n, respectively.

2. System Overview

2.1. Scenario

This paper considers the scenario depicted in Figure 1, where three nodes share a wireless medium. Bob is a critical node that has sensitive information, and only Alice has access rights to him. Eve is a potentially malicious attacker who wishes to disrupt the authentication process by causing Bob to accept inauthentic messages. In this context, Bob and Alice agree on a keyed authentication scheme that allows Bob to verify that the messages he receives are intact from Alice.

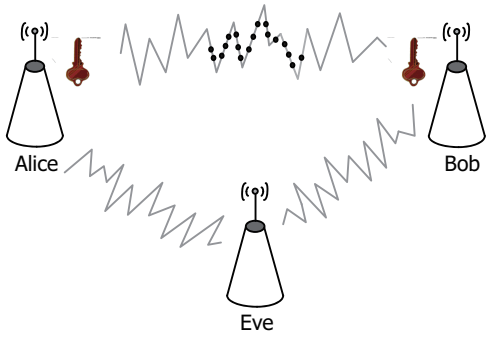

Figure 1. The scenario of authentication.

As is shown in Figure 2, Alice and Bob share a secret key K. The secret key is assumed only known to both Alice and Bob, and it has been allocated before the communication. In order to authenticate, Alice sends an additional proof, which is called an authentication tag T, together with the source message M for Bob's verification. Generally, the tag T is a function of the source message M and the secret key K. When a signal Y^n is received, Bob decodes it and determines whether the message is authentic or not.

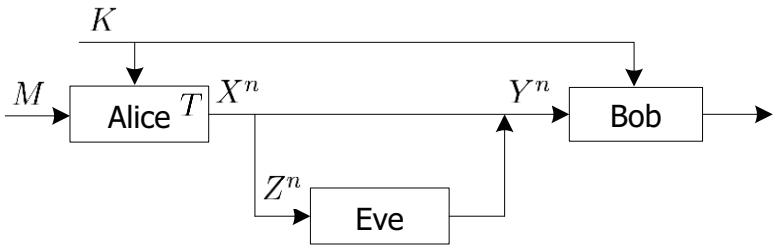

Figure 2. The authentication channel.

Meanwhile, when Alice sends X^n to Bob, Eve can eavesdrop or intercept an observation Z^n. Eve's primary purpose is to have her messages accepted by Bob, so she will try her best to impersonate or substitute Alice's messages. Without loss of generality, we assume that Eve is aware of all details except the secret key of the authentication scheme between Alice and Bob.

2.2. Proposed Authentication Scheme

Let $\mathcal{M}$, $\mathcal{K}$ and $\mathcal{T}$ denote the finite alphabet of the source message, the secret key and the authentication tag, respectively. The random variables of the source message M and the secret key K are assumed

statistically independent. Alice and Bob share a common secret key K uniformly chosen from $\mathcal{K}$. When Alice intends to send a message M from $\mathcal{M}$ to Bob, she transmits the authentication tag T together with it. The transmitted signal of Alice is denoted by

$$X^n = f(M, T) \tag{1}$$

where the function $f(\cdot)$ encapsulates any prospective coding or modulation. For the purpose of covering the secret key, the authentication tag T is a function of the source message M and the secret key K, *i.e.*,

$$T = g(M, K) \tag{2}$$

where a source message M and a secret key K uniquely determine an authentication tag T by the authentication coding function $g(\cdot)$. (Generally, $|\mathcal{M}| \geq |\mathcal{T}| \geq |\mathcal{K}|$ in practice.)

The authentication relies on the destination terminal. Upon receiving a signal Y^n, which may come from either Alice or Eve, Bob uses a decoding function $d(\cdot)$ to obtain an estimate of the source message and the authentication tag, *i.e.*, $(\hat{M}, \hat{T}) = d(Y^n)$. If it is determined that the observation Y^n demonstrates knowledge of the secret key, *i.e.*, $\hat{T} = g(\hat{M}, K)$, the message $\hat{M}$ is considered authentic and Bob will accept it; otherwise, the message $\hat{M}$ will be rejected.

2.3. Channel Model

Firstly, a less noisy wiretap channel [17,18] is introduced to ensure that the wiretap channel's perfect secrecy capacity is positive. A wiretap channel $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$ is less noisy if the main channel is less noisy than the source–wiretapper channel. If a wiretap channel is less noisy, the perfect secrecy capacity is given [17,18] by

$$C_s = \max[I(X;Y) - I(X;Z)]. \tag{3}$$

In this paper, the channels between every two nodes among Alice, Bob and Eve are considered to be noisy, except that the channel between Eve and Bob is noiseless (this assumption of giving Eve an advantage does not incur any loss of generality). In addition, we consider that the Alice–Bob channel $P_{Y|X}$ is less noisy than the Alice–Eve channel $P_{Z|X}$.

As is depicted in Figure 3, a codebook $\mathcal{C}$ is designed to transmit the secret key in a perfectly secure way. In the transmission, if Alice intends to transmit source message m using secret key k, she randomly chooses a codeword $x^n(m,t)$ from the mth bin of the tth subset using a uniform distribution, where $t = g(m,k)$. According to Lemma 1 in the following, the authentication tag can be kept hidden from Eve by channel noise.

Lemma 1. *[13,19] Consider a less noisy wiretap channel $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$. For a distribution $p(x)$, generate $2^{n(R_m+R_t+\delta)}$ x^n sequences through $p(x^n) = \prod_{i=1}^{n} p(x_i)$ where $\delta > 0$, and index these sequences as $x^n(m,t)$ according to the codebook $\mathcal{C}$ shown in Figure 3 where $m \in \{1, ..., 2^{nR_m}\}$ and $t \in \{1, ..., 2^{nR_t}\}$. The codeword $x^n(m,t)$ is picked from the mth bin of the tth subset using a uniform distribution. Then, rate $R = R_m + R_t$ can be delivered to the legitimate receiver as long as $R \leq I(X;Y)$, and by setting $R_m = I(X;Z)$, $R_t = I(X;Y) - I(X;Z)$ is an achievable equivocation rate.*

Proof. Please refer to [19] for technical details. □

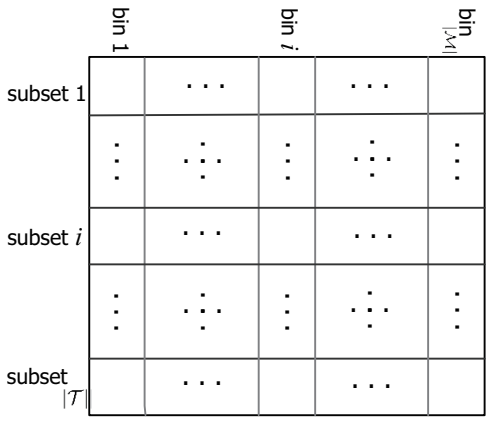

Figure 3. The codebook used in our authentication scheme. The codebook is divided into $|\mathcal{T}|$ subsets, each of which further partitioned into $|\mathcal{M}|$ bins. Each subset corresponds to an authentication tag t, and each bin in each subset corresponds to a source message m.

3. Security Performance Analysis

In this section, the impersonation attack and the substitution attack are primarily considered. The performances of protecting against the impersonation attack and the substitution attack are respectively analyzed.

Firstly, for an impersonation attack, the optimal strategy for Eve is to transmit a codeword $x^n(m,t)$ corresponding to the secret key k that has the largest probability of being accepted by Bob. Hence, Eve's success probability of an impersonation attack P_I is

$$P_I = \max_{m\in\mathcal{M}} \max_{t\in\mathcal{T}} \sum_{k\in\mathcal{K}} \Pr[t = g(m,k)]. \tag{4}$$

From (4), it can be seen that the success probability of the impersonation attack does not relate to the channels $P_{Y|X}$ or $P_{Z|X}$. Therefore, to simplify the analysis, we finish the derivation by recalling the following lower bound on P_I in [7], and we have the following lemma.

Lemma 2. *The opponent's success probability of the impersonation attack is lower bounded by*

$$P_I \geq 2^{-I(K;X^n)}. \tag{5}$$

Proof. Please refer to [7] for technical details. □

Remark 1. *The lower bound $P_I \geq 2^{-I(K;X^n)}$ is the infimum on P_I. Due to the fact that $I(K;X^n) = H(K) - H(K|X^n)$, the lower bound $P_I \geq 2^{-H(K)}$ is achievable when $H(K|X^n) = 0$. That is, the performance of protecting against the impersonation attack relates to the design of the authentication code (*i.e.*, the design of the generation function $g(\cdot)$).*

Secondly, for a substitution attack, Eve intercepts an additional observation $z^n = h(x^n)$, where $h(\cdot)$ represents the channel between Alice and Eve. Eve has to replace the intercepted source message m^* with another message m ($m \neq m^*$); otherwise, Eve becomes a relay node. Note that m^* denotes the estimated source message according to the observation $z^n = h(f(m^*, g(m^*,k)))$, and according to

Lemma 1 Eve can estimate the source message correctly by setting $R_m = I(X;Z)$, *i.e.*, $p(m^*|z^n) = 1$. The optimal strategy for Eve is to transmit a codeword $x^n(m,t)$ $(m \neq m^*)$ corresponding to the secret key k that has the largest probability of being accepted by Bob to replace the intercepted one. Hence, based on the information z^n, the success probability of a substitution attack P_S is

$$P_S = \sum_{z^n} p(z^n) \max_{\substack{m \in \mathcal{M} \\ m \neq m^*}} \max_{t \in \mathcal{T}} \sum_{k \in \mathcal{K}} \Pr[t = g(m,k)|z^n]. \tag{6}$$

To simplify the analysis, we have the following theorems.

Theorem 1. *The opponent's success probability of the substitution attack is lower bounded by*

$$P_S \geq 2^{-I(K;X^n|Z^n)} \tag{7}$$

where X^n and Z^n come from two distinct source messages with the same secret key.

Proof. Please refer to Appendix A for technical details. □

Theorem 2. *The lower bound*

$$P_S \geq 2^{-I(K;X^n)} \tag{8}$$

is achievable iff $H(K|Z^n) = H(K)$.

Proof. Please refer to Appendix B for technical details. □

Remark 2. *The lower bound $P_S \geq 2^{-I(K;X^n|Z^n)}$ in Theorem 1 is the infimum on P_S. The condition $H(K|Z^n) = H(K)$ means that Eve cannot acquire any knowledge about the secret key from her observations. According to Lemma 1, Theorems 1 and 2 show that the performance of protecting against the substitution attack relates to the codebook $\mathcal{C}$ and the function $f(\cdot)$. Furthermore, the lower bound $P_S \geq 2^{-H(K)}$ is achievable due to the same reason in Remark 1.*

According to the theorems and lemmas above and [9], we draw the following theorem.

Theorem 3. *If K satisfies the uniform distribution, $H(K|X^n) = 0$ and the perfect secrecy capacity C_s of the wiretap channel $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$ is nonzero, then there exist constants $\alpha > 0$ and $\beta > 0$ so that*

$$2^{-H(K|Z^n)} \leq P_D \leq 2^{-H(K)} + \alpha e^{-n\beta} \tag{9}$$

where n is the codeword length that satisfies $n > \max\{\frac{\log_2|\mathcal{T}|}{I(X;Y)-I(X;Z)-2\delta}, \frac{\log_2|\mathcal{T}||\mathcal{M}|}{I(X;Y)-\delta}\}$ $(\delta > 0)$. The sufficient and necessary conditions for $P_D = 2^{-H(K)}$ are that K satisfies the uniform distribution, $H(K|X^n) = 0$ and $H(K|Z^n) = H(K)$.

Proof. Please refer to Appendix C for technical details. □

Remark 3. *The condition that $H(K|X^n) = 0$ reveals the optimal design of the authentication coding function $g(\cdot)$ (e.g., $g(m,k) = hash(m) \oplus k$). The condition $H(K|Z^n) = H(K)$ reveals that it should choose an appropriate codebook $\mathcal{C}$ and the function $f(\cdot)$ (e.g., [20–24]) to prevent the information leakage of the secret key.*

Remark 4. *$P_D \geq 2^{-H(K|Z^n)}$ is the infimum on P_D, and $P_D \leq 2^{-H(K)} + \alpha e^{-n\beta}$ is the supremum on P_D. When the perfect secrecy capacity C_s of the wiretap channel $\mathcal{X} \to (\mathcal{Y}, \mathcal{Z})$ is nonzero, there exist a codebook $\mathcal{C}$ and a function $f(\cdot)$ such that $I(K; Z^n) \to 0$ when $n \to \infty$ [12,23–25]. At this time, it becomes secrecy from channel resolvability [26], that is, Eve cannot distinguish between the uniform input distribution on sub-$\mathcal{C}$ (*i.e.*, *a subset of $\mathcal{C}$) and $\mathcal{C}$ by observing only Z^n. Then, the upper bound can be derived. Thus, as n goes to infinity, the upper bound of P_D matches its lower bound,* i.e., *$P_D = 2^{-H(K)}$.*

Remark 5. *Theorem 3 shows that the substitution attack can be prevented due to the fact that the secret key is completely hidden from Eve, then all the information about the secret key can be used to protect against the impersonation attack.*

4. Comparisons With Previous Works

Compared with conventional authentication modes over noiseless channels, introducing channel noise to protect the transmission of the secret key brings additional security gain, which has been discussed in [9]. Another merit is that the service life of the secret key can be efficiently extended. In classical authentication schemes, after eavesdropping several transmissions between Alice and Bob, the knowledge of encoded messages enables the information of the secret key to be determined [27]. However, if the information of the secret key is primarily protected by channel noise, its security will not rely on any assumption on the computational power of attackers. Thus, it can efficiently extend the service life of the secret key. Moreover, compared with the work in [9], ours has the following advantages.

(1) Our work can scale the optimal security performance exactly even if the codeword length n is limited. Specifically, this paper considers the intercepted observation Z^n, directly derives the infimums on P_S and P_D and gives the sufficient and necessary conditions for tightness. Moreover, these results reveal the optimal design of the authentication scheme (*i.e.*, Remark 3). However, the work in [9] only proves the reachability of the optimal security performance when the codeword length n goes to infinity. Thus, our work is more significant and practicable.

(2) The authentication model in [9] may incur the power-substitution attack, especially in linear code schemes (e.g., superposition coding is encapsulated in $f(\cdot)$ [10]). For example, as is depicted in Figure 3, a codeword could be modified into another one by a synchronously transmitted and well-designed malicious signal. However, in our scheme, since the authentication tag encapsulates the source message and the secret key (*i.e.*, Equation (2)), the power-substitution attack can be effectively limited in the subsets of the source message, and with an additional trick it can be prevented. (Please refer to Appendix D for more technical details.) Instead of designing specific code schemes in $f(\cdot)$, our scheme introduced $g(\cdot)$ (*i.e.*, Equation (2)) to defend against the power-substitution attack. Thus, our scheme can be applied in the existing wireless communication systems with minimal modifications.

(3) Our authentication model degrades to the one in [9] when $T = g(M, K) = K$. Thus, the authentication model in [9] can be seen as a special case of ours. This special case is not the optimal one and is not permitted in our scheme due to the reasons above. In addition, it is obvious that the scheme in [9] exposes the secret key when the wiretap channel's secrecy capacity cannot be guaranteed to be nonzero according to its codebook. However, when the authentication tag leaks to Eve, our

scheme degrades to the Simmons' model [27]. Thus, we can adjust the construction of $g(\cdot)$ to adapt the time-varying channels.

5. Conclusions

In this paper, we have reformulated the authentication problem in [9] and proposed an enhanced authentication scheme. We primarily analyzed the eavesdropping agent's success probability of impersonation and substitution attacks, derived the necessary and sufficient conditions for secure authentication codes, and offered the optimal constructions of the authentication scheme. Consequently, we provided general perspectives to show that it is a reliable way to utilize channel noise in message authentication applications.

Acknowledgments

The authors would like to thank Xianglin Yan for her language revision on this paper.

This work was supported in part by the National High Technology Research and Development Program (ss2015AA011306), National Basic Research Program of China (2013CB329002), National Natural Science Foundation of China (61172097), National S&T Major Project (2013ZX03001024-004), Keygrant Project of Chinese Ministry of Education (313005), International Science and Technology Cooperation Program (2012DFG12010), The Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2012D02), Natural Science Technology of Fujian (2013H0048) , and Tsinghua-Qualcomm Joint Research Program.

Author Contributions

Fanfan Zheng conceived of this work and contributed the derivation of all conclusions and the composition of this paper. Zhiqing Xiao participated in the derivation of the conclusions and contributed valuable suggestions to develop the composition. Shidong Zhou, Jing Wang and Lianfen Huang conducted the theoretical analyses of this work and contributed valuable suggestions to consummate this paper. All authors have read and approved the final manuscript.

Appendix

A. Proof of Theorem 1

By recalling (6), it can be seen that $\sum_{k\in\mathcal{K}} \Pr[t = g(m,k)|z^n] = p(t|m,z^n)$ [7,28], thus P_S is updated to $P_S = \sum_{z^n\in\mathcal{Z}} p(z^n) \max_{m\in\mathcal{M}\setminus\{m^*\}} \max_{t\in\mathcal{T}} p(t|m,z^n)$. Hence, we have

$$
\begin{aligned}
& -\log P_S \\
=& -\log \sum_{z^n} p(z^n) \max_{m\in\mathcal{M}\setminus\{m^*\}} \max_{t\in\mathcal{T}} p(t|m,z^n) \\
\overset{(a)}{\leq}& -\log \sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) \max_{t\in\mathcal{T}} p(t|m,z^n) \\
\overset{(b)}{\leq}& -\sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) \log \max_{t\in\mathcal{T}} p(t|m,z^n) \\
\overset{(c)}{=}& -\sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) \sum_{t\in\mathcal{T}} p(t|m,z^n) \log \max_{t'\in\mathcal{T}} p(t'|m,z^n) \\
\overset{(d)}{\leq}& -\sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) \sum_{t\in\mathcal{T}} p(t|m,z^n) \log p(t|m,z^n) \\
=& \sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) H(T|m,z^n) \\
\overset{(e)}{=}& \sum_{z^n} p(z^n) \sum_{m\in\mathcal{M}} q(m|z^n) [H(K|z^n,m) - H(K|z^n,m,T)] \\
=& \sum_{z^n} p(z^n) [H(K|z^n,M) - H(K|z^n,M,T)] \\
=& H(K|Z^n,M) - H(K|Z^n,M,T) \\
\overset{(f)}{=}& H(K|Z^n) - H(K|Z^n,X^n) \\
=& I(K;X^n|Z^n).
\end{aligned}
\tag{10}
$$

In this expression, the inequality (a) follows from the fact that the maximum must be greater than or equal to the weighted average of a distribution, and $q(m|z^n)$ is the probability of substituting the original source message with m when given the observation z^n, especially $q(m|z^n) = 0$ if $m = m^*$; (a) with equality iff $\max_{t\in\mathcal{T}} p(t|m,z^n)$ is constant for all $m \in \mathcal{M}\setminus\{m^*\}$; the inequality (b) comes from Jensen's inequality, and (b) with equality iff $\max_{t\in\mathcal{T}} p(t|m,z^n)$ is constant for all $z^n \in \mathcal{Z}^n\setminus\{z^n : p(z^n) = 0\}$ and $m \in \mathcal{M}\setminus\{m^*\}$; the equality (c) holds due to the fact that $\max_{t\in\mathcal{T}} p(t|m,z^n)$ is constant when m and z^n are given; the inequality (d) follows from the fact that the maximum must be greater than all other individuals of a distribution, and (d) with equality iff $p(t|m,z^n)$ is constant for all $t \in \mathcal{T}$; the equality (e) comes from the fact that

$$
\begin{aligned}
H(K,T|z^n,m) &= H(K|z^n,m) + H(T|z^n,m,K) \\
&= H(T|z^n,m) + H(K|z^n,m,T)
\end{aligned}
$$

where $H(T|z^n,m,K) = 0$, since the source message and the secret key uniquely determine the authentication tag; the equality (f) holds due to the fact that $K \to Z^n \to M$ forms a Markov chain.

In addition, notice that X^n and Z^n come from two distinct source messages with the same secret key K. In this way, it is necessary to define a probability distribution on $\mathcal{X}^n \times \mathcal{Z}^n$, with the stipulation that $p_{\mathcal{X}^n\times\mathcal{Z}^n}(m_1,m_2) = 0$ when $m_1 = m_2$.

Hence, we have

$$
P_S \geq 2^{-I(K;X^n|Z^n)},
$$

with equality iff $p(t|m,z^n)$ is constant for all $t \in \mathcal{T}$, $z^n \in \mathcal{Z}^n \backslash \{z^n : p(z^n) = 0\}$, and $m \in \mathcal{M} \backslash \{m^*\}$ due to the concentration of the conditions for the equality of (a), (b) and (d) in (10).

B. Proof of Theorem 2

We prove sufficiency followed by necessity.

Sufficiency: According to (7), when $H(K|Z^n) = H(K)$, we have

$$\begin{aligned} P_S &\geq 2^{-I(K;X^n|Z^n)} \\ &= 2^{-H(K|Z^n)+H(K|Z^n,X^n)} \\ &= 2^{-H(K)+H(K|X^n)} \\ &= 2^{-I(K;X^n)}. \end{aligned} \tag{11}$$

Then, the sufficiency is proved.

Necessity: By recalling Lemma 1, from the intercepted observation z^n, the eavesdropping agent Eve can obtain a correct source message estimate m but with a fuzzy authentication tag estimate $\tilde{t}$, *i.e.*, $d(z^n) = (m, \tilde{t})$. Thus, the equivocation about the authentication tag is $H(T|Z^n) = H(T|Z^n, M) \in [0, H(K)]$ due to the fact that $t = g(m,k)$. When $H(T|Z^n) = H(K)$, it means that Eve cannot acquire any information about the secret key, that is, it is equivalent to $H(K|Z^n) = H(K)$.

On the other hand, we draw that $I(K; X^n|Z^n)$ is an increasing function as the equivocation of Z^n grows, since

$$I(K; X^n|Z^n) = H(X^n|Z^n) - H(X^n|K, Z^n)$$

where $H(X^n|Z^n)$ increases as $H(T|Z^n)$ grows, and $H(X^n|K, Z^n)$ is constant.

Thus, $I(K; X^n|Z^n) = I(K; X^n)$ only if $H(K|Z^n) = H(K)$. Then, the necessity is proved.

C. Proof of Theorem 3

C.1. Proof of $P_D \geq 2^{-H(K)}$

By recalling the lower bound on P_I in (5),

$$\begin{aligned} P_I &\overset{(g)}{\geq} 2^{-I(K;X^n)} \\ &= 2^{-H(K)+H(K|X^n)} \\ &\overset{(h)}{\geq} 2^{-H(K)} \end{aligned} \tag{12}$$

where (g) with equality iff $p(t|m)$ is constant for all $m \in \mathcal{M}$ and $t \in \mathcal{T}$ [7]; the inequality (h) follows from the fact that $H(K|X^n) \geq 0$, and (h) with equality iff $H(K|X^n) = 0$. $H(K|X^n) = 0$ holds iff $p(k) = p(t|m)$, which means $\forall m \in \mathcal{M}, k_1, k_2 \in \mathcal{K}$ such that $k_1 \neq k_2$ satisfies $f(m,k_1) \neq f(m,k_2)$. Thus, the lower bound $P_I \geq 2^{-H(K)}$ is achievable iff $H(K|X^n) = 0$ and K is uniformly distributed.

Next, according to (7), we have

$$\begin{aligned} P_S &\geq 2^{-I(K;X^n|Z^n)} \\ &= 2^{-H(K|Z^n)+H(K|Z^n,X^n)} \\ &\overset{(i)}{\geq} 2^{-H(K|Z^n)} \end{aligned} \tag{13}$$

where (i) with equality iff $H(K|X^n) = 0$.

Hence, we have the infimum

$$\begin{aligned} P_D &= \max\{P_I, P_S\} \\ &\geq 2^{-H(K|Z^n)}, \end{aligned} \tag{14}$$

with equality iff K is uniformly distributed and $H(K|X^n) = 0$.

According to Theorem 2, we have that the lower bound $P_D \geq 2^{-H(K)}$ is achievable iff K is uniformly distributed, $H(K|X^n) = 0$ and $H(K|Z^n) = H(K)$.

C.2. Proof of $P_D \leq 2^{-H(K)} + \alpha e^{-n\beta}$

We reprise the derivation of the upper bound of P_S from the channel resolvability. Let

$$d_{av}(f) = \sum_{z^n \in \mathcal{Z}^n} p(z^n) \sum_{k \in \mathcal{K}} |p(k|z^n) - q(k)| \tag{15}$$

be the average $\mathcal{L}_1$ (*i.e.*, variational) distance between the conditional distribution $p(k|z^n)$ and the prior distribution $q(k)$, where $q(k)$ represents the probability of guessing the secret key

$$q(k) = \sum_{m \in \mathcal{M}} p(m)\mathrm{Pr}[t = g(m,k)|m]. \tag{16}$$

Notice that in our work, k is uniformly distributed. Thus, $q(k)$ satisfies the uniform distribution. When $H(K|X^n) = 0$, we have

$$\min q(k) = 2^{-H(K)}. \tag{17}$$

If $d_{av}(f)$ can be arbitrarily small by appropriately choosing a codebook $\mathcal{C}$ and function $f(\cdot)$, Eve cannot distinguish the distributions between $p(k|z^n)$ and $q(k)$. That is, Eve cannot acquire any information about k by only observing z^n.

Following from the same proof steps as those used in [9], we can get an upper bound

$$P_S \leq q(k) + \alpha e^{-n\beta} \tag{18}$$

where the constants $\alpha > 0$, $\beta > 0$ and the codeword length n satisfies

$$n > \max\left\{ \frac{\log_2 |\mathcal{T}|}{I(X;Y) - I(X;Z) - 2\delta}, \frac{\log_2 |\mathcal{T}||\mathcal{M}|}{I(X;Y) - \delta} \right\} (\delta > 0). \tag{19}$$

According to (17), we draw that $P_S \leq 2^{-H(K)} + \alpha e^{-n\beta}$ is the supremum on P_S.

This completes our proof.

D. The Power-substitution Attack

We assume that Alice's messages can be predicted, since authentication does not provide privacy and Eve can intercept Alice's messages to cause message retransmission. Moreover, the linear code scheme (e.g., superposition coding) is an easy and common implementation in practice [10]. Thus, the power-substitution attack is potentially dangerous.

When the code scheme in $f(\cdot)$ is linear, Eve can successfully modify Alice's message m into m' (which also can be authenticated by Bob) with malicious message ε by the power-substitution attack in [9]'s model. That is,

$$\begin{aligned} f(m,k)+\varepsilon &= f_1(m)+f_2(k)+\varepsilon \\ &= f_1(m)+f_2(k)+[f_1(m')-f_1(m)] \\ &= f(m',k) \end{aligned} \tag{20}$$

where $\varepsilon = f_1(m') - f_1(m)$. Therefore, to prevent the power-substitution attack, the model in [9] has to construct specific nonlinear code schemes and may need lots of modifications on the existing communication system.

However, in our model the authentication code function $g(\cdot)$ is introduced, and if Eve wants to successfully modify Alice's message m into m' with a malicious message ε, we have

$$\begin{aligned} f(m,t)+\varepsilon &= f_1(m)+f_2(t)+\varepsilon \\ &= f_1(m)+f_2(g(m,k))+[f_1(m')-f_1(m)+f_2(g(m',k))-f_2(g(m,k))] \\ &= f(m',g(m',k)) \\ &= f(m',t') \end{aligned} \tag{21}$$

where $\varepsilon = f_1(m') - f_1(m) + f_2(g(m',k)) - f_2(g(m,k))$. Obviously, if ε is varying with k, then the power-substitution attack is prevented.

Since $f_2(\cdot)$ is unknown, it is hard to construct explicit $g(\cdot)$ to prevent the power-substitution attack. Furthermore, whether there exist constructions of $g(\cdot)$ to prevent the power-substitution attack relates to the size of the alphabets $\mathcal{M}, \mathcal{T}$, and $\mathcal{K}$.

Take $t = g(m,k) = hash(m) \oplus k$ (one of the construction of $g(\cdot)$ according to the conclusion in Remark 3) for example, and assume that $f_2(\cdot)$ represents BPSK modulation (define that BSPK respectively modulates "0" to the symbol "+1" and "1" to the symbol "−1"). We have

$$\begin{aligned} f_2(t')-f_2(t) &= f_2(g(m',k))-f_2(g(m,k)) \\ &= f_2(hash(m')\oplus k)-f_2(hash(m)\oplus k) \\ &= f_2(hash(m')).*f_2(k)-f_2(hash(m)).*f_2(k) \\ &= [f_2(hash(m'))-f_2(hash(m))].*f_2(k). \end{aligned} \tag{22}$$

When $|\mathcal{M}| > |\mathcal{T}|$, there must exist a subset of $\mathcal{M}$ that has the same hash value. Thus, if Alice transmits a message from this subset, Eve can successfully modify it into any other messages in the same subset without any knowledge of the secret key.

However, if $N = \lceil |\mathcal{M}|/|\mathcal{T}| \rceil$ is large, we can prevent the power-substitution attack by other techniques. For example, divide $\mathcal{M}$ into N subsets (*i.e.*, $\mathcal{M} = \mathcal{M}_{s1} \cup \cdots \cup \mathcal{M}_{sN}$), and each subset

satisfies that $\forall m' \neq m \in \mathcal{M}_{si}$ $(1 \leq i \leq N)$, $hash(m') \neq hash(m)$. Then, it can design a protocol that only one subset is valid in each transmission.

Furthermore, the example above contributes to the analysis of the relationship between Eve's success probability of the power-substitution attack and the size of the alphabets $\mathcal{M}, \mathcal{T}$, and $\mathcal{K}$. We have the following theorem.

Theorem 4. *When $|\mathcal{M}| > |\mathcal{T}|$, there exist $m' \neq m \in \mathcal{M}$ and $k \in \mathcal{K}$ satisfying $g(m', k) = g(m, k)$, that is, Eve has nonzero success probability of the power-substitution attack.*

Proof. Assume that $|\mathcal{M}| = |\mathcal{T}| + 1$, and $\mathcal{M} = \mathcal{M}_s \cup \{m'\}$. Then, there must exist a $k \in \mathcal{K}$ and a $t \in \mathcal{T}$ satisfying $t = g(m', k)$.

According to (22), we can draw that when $|\mathcal{M}| = |\mathcal{T}|$ there exists a $g(\cdot)$ (*i.e.*, $t = m \oplus k$, padding zeros on the high-order bits of k when $|\mathcal{K}| < |\mathcal{M}|$) satisfying that $\forall \underline{m} \neq \bar{m} \in \mathcal{M}, k \in \mathcal{K}$, it has $g(\underline{m}, k) \neq g(\bar{m}, k)$. Therefore, with the same k and t, there must exists a $m \in \mathcal{M}_s$ that satisfies $t = g(m, k)$. □

In conclusion, though the power-substitution attack is inevitable when $|\mathcal{M}| > |\mathcal{T}|$, it is still feasible to introduce $g(\cdot)$ into the existing linear code schemes (e.g., superposition coding) to defend against the power-substitution attack. Together with other techniques, it is an efficient solution.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Yu, P.; Baras, J.; Sadler, B. *An Implementation of Physical Layer Authentication Using Software Radio*; Technical report, DTIC Document, ARL-TR-4888; U.S. Army Research Laboratory: Adelphi, MD, USA, July 2009.
2. Yu, T.; Hartman, S.; Raeburn, K. The perils of unauthenticated encryption: Kerberos version 4. In Proceedings of the 11th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 4–6 February 2004, Available online: http://www.internetsociety.org/doc/perils-unauthenticated-encryption-kerberos-version-4 (accessed on 12 January 2015).
3. Yu, P.L.; Baras, J.S.; Sadler, B.M. Physical-layer authentication. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 38–51.
4. Wang, X.; Wu, Y.; Caron, B. Transmitter identification using embedded pseudo random sequences. *IEEE Trans. Broadcast.* **2004**, *50*, 244–252.
5. Fei, C.; Kundur, D.; Kwong, R.H. Analysis and design of secure watermark-based authentication systems. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 43–55.
6. Zeng, K.; Govindan, K.; Mohapatra, P. Non-cryptographic authentication and identification in wireless networks. *IEEE Trans. Wirel. Commun.* **2010**, *17*, 56–62.
7. Simmons, G. Authentication theory/coding theory. In *Advances in Cryptology*; Springer: Berlin, Germany, 1985; Volume 196, pp. 411–431.
8. Wyner, A.D. The Wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.

9. Lai, L.; El Gamal, H.; Poor, H.V. Authentication over noisy channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 906–916.
10. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011.
11. Bennett, C.H.; Brassard, G.; Crépeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923.
12. Maurer, U.; Wolf, S. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology—EUROCRYPT 2000*; Preneel, B., Ed.; Springer: Berlin, Germany, 2000; pp. 351–368.
13. Csiszár, I. Almost independence and secrecy capacity. *Probl. Peredachi Inf.* **1996**, *32*, 48–57.
14. Barros, J.; Rodrigues, M.R.D. Secrecy capacity of wireless channels. In Proceedings of 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006; Volume 1, pp. 356–360.
15. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534.
16. Chrysikos, T.; Dagiuklas, T.; Kotsopoulos, S. Wireless information-theoretic security in an outdoor topology with obstacles: Theoretical analysis and experimental measurements. *EURASIP J. Wirel. Commun. Netw.* **2011**, *2011*, 628–747.
17. Csiszár, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348.
18. Ozel, O.; Ulukus, S. Wiretap channels: Roles of rate splitting and channel prefixing. In Proceedings of 2011 IEEE International Symposium on Information Theory Proceedings, St. Petersburg, FL, USA, 31 July–5 August 2011; pp. 628–632.
19. Ulukus, S. Information theoretic security. Presented at 2012 European School of Information Theory, Antalya, Turkey, April 2012.
20. Thangaraj, A.; Dihidar, S.; Calderbank, A.R.; McLaughlin, S.W.; Merolla, J.M. Applications of LDPC codes to the wiretap channel. *IEEE Trans. Inf. Theory* **2007**, *53*, 2933–2945.
21. Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.; Kwak, B.J. LDPC codes for the Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540.
22. Richardson, T.J.; Shokrollahi, M.A.; Urbanke, R.L. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans. Inf. Theory* **2001**, *47*, 619–637.
23. Mahdavifar, H.; Vardy, A. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Trans. Inf. Theory* **2011**, *57*, 6428–6443.
24. Subramanian, A.; Thangaraj, A.; Bloch, M.; McLaughlin, S.W. Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 585–594.
25. Subramanian, A.; Suresh, A.T.; Raj, S.; Thangaraj, A.; Bloch, M.; McLaughlin, S. Strong and weak secrecy in wiretap channels. In Proceedings of the 6th International Symposium on Turbo Codes and Iterative Information Processing, Brest, France, 6–10 September 2010; pp. 30–34.
26. Zhou, X.Y.; Song, L.Y.; Zhang, Y. *Physical Layer Security in wireless Communications*; CRC Press: Boca Raton, FL, USA, 2013.
27. Walker, M. Information-theoretic bounds for authentication schemes. *J. Cryptol.* **1990**, *2*, 131–143.

28. Stinson, D.R. *Cryptography: Theory and Practice*, 3rd ed.; CRC Press: Boca Raton, FL, USA, 2005.