Authentication Using Modulation Domain Watermarking

Fanfan Zheng[1], Lianfen Huang[1], and Jing Wang[2]
[1] Department of Communication Engineering, Xiamen University, Xiamen, 361005, China
[2] Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
Email: zhengfanf@foxmail.com; lfhuang@xmu.edu.cn; wangj@tsinghua.edu.cn

Abstract —Digital watermarking is typically applied to identify audio or image data copyright ownership. This paper propose a flexible and low complexity framework for authentication at the physical layer where the authentication information is embedded as watermarking into the baseband modulated waveforms of main messages. This authentication scheme is stealthy to uninformed users, robust to channel interference and secure for the verification of identity and information integrity. Performance analyses are presented that demonstrate the potential application to strengthen wireless communication systems security.

Index Terms—Authentication, modulation, watermarking, physical layer.

I. INTRODUCTION

One of the prominent problems in communication is security. Compared with cable transmission systems, wireless communication faces more challenges due to its channel's open air nature. Authentication is the first step to ensure secure communication. Without properly authenticate users will result in serious damage because adversaries can do what any valid users can do. In some cases, authentication is more important than encryption because the threat of active attacks are always more serious than passive attacks.

Most authentication mechanisms (e.g., certificates) are dependent on the upper layer (MAC layer and above) to realize secure communication. A more reliable way is to exploit the physical layer authentication to enhance communication security [1]. In physical layer authentication studies, authentication based on encryption is mature. The transmitter and receiver communicate according to a prior coordinated agreement using a secret key, where the identity of the transmitter is authentic if the receiver can successfully decode the transmission. Supangkat *et al*. [2] proposed one such authentication for telephony, where the authentication is realized by embedding an encrypted watermarking into the conversation speech signal. Similarly, Wang *et al*. [3] proposed an authentication scheme for broadcast television where each transmitter embeds a unique low-power watermarking signal into its transmissions to prove its identity to the receivers. Yu *et al*. [4] put forward an authentication scheme which synchronously transmits main messages and authentication messages using signal superposition. Relative to the upper layer's authentication scheme, these authentication schemes transmit authentication information without occupying additional bandwidth and compatible with the receivers which lack a peer to peer authentication mechanism.

Another kind of physical layer authentication is based on fingerprinting [5]-[7], such as Channel-based Fingerprinting and Hardware-based Fingerprinting [8], [9]. Xiao *et al*. [5], proposed one such authentication scheme utilizing CSI (Channel State Information) as channel fingerprinting to verify if the current transmitter is the same one that communicated the previous attempt. However, the major disadvantage of this approach is that wireless devices are immobile. If a device moves, its observed CSI fingerprinting changes as well. It is also unable to perform well when the channel is fast time-varying [10]. Brik *et al*. [8] proposed an authentication scheme named PARADIS which extracts the modulator imperfections (e.g., frame frequency error, frame SYNC correlation, and frame I/Q origin offset) as radiometric fingerprinting. The fingerprinting is unique and covert, but the fatal weakness is that once these features are sniffed by a powerful attacker, such as a SDR user or high-end signal transmitter, the features can be easily impersonated [10], [11]. Though the schemes proposed above utilized the inherent channel characteristics or the hardware for authentication instead of the conventional secret key, the disadvantages is obvious that they are too limited for practical applications.

We have two main goals when constructing our authentication scheme. First, we want it to be applied in a potential physical environment. That is, our scheme must be robust to the effects of the wireless channel, and suitable for most scenarios (e.g., mobile environments). Second, we want our authentication to be easily added to existing systems, and our scheme should only improve the physical layer behavior without any modification of upper layer's protocol. Thus, we propose an authentication scheme using modulation domain watermarking, due to the fact that small deviations of the constellation points are not able to disturb the demodulator's output [12], [13]. The watermarking is an embedded signature that claims the unique identity of the transmitter and the validity of its messages. (In this paper,

Manuscript received October 17, 2014; revised March 26, 2015.
The work presented in this paper was partially supported by National High Technology Research and Development Program (2015AA01A707), National Natural Science Foundation of China (61172097), and Natural Science Technology of Fujian (2013H0048).
Corresponding email: lfhuang@xmu.edu.cn.
doi:10.12720/jcm.10.3.154-160

©2015 Journal of Communications

the "watermarking" is the embedded "signature" in the modulation domain.) This paper inherits the advantage of Yu *et al*. [4] etc. which without occupying additional bandwidth and the advantage of Brik *et al*. [8] etc. which with the covert property of fingerprinting.

The robustness, stealth and security of our scheme are analyzed. The robustness describes the authentication resistance to interference. Without loss of generality, we use time diversity to protect the signature transmission on the wireless fading block channels. The stealth describes how covert the watermarking is to bystanders. The presence of the watermarking cannot be easily detectable if we carefully limit the watermarking power. The security describes the inability of adversaries to mount successful attacks. Several kinds of attacks are considered in this paper. Furthermore, the tradeoffs between these properties are given.

This paper is organized as follows. Section Ⅱ provides various aspects of our approach in the giving scenario. Section Ⅲ introduces the properties analysis of the scheme. Finally, Section Ⅳ concludes the paper.

II. System Overview

A. *Scenario and the Proposed Scheme*

This paper considers the scenario depicted in Fig. 1 where three nodes share a wireless medium. Suppose that Bob is a critical node with sensitive information and only Alice has access rights to him. Eve is a potential malicious attacker. In this context, Bob and Alice agree on a keyed authentication scheme that allows Bob to verify the messages that he receives are intact from Alice.

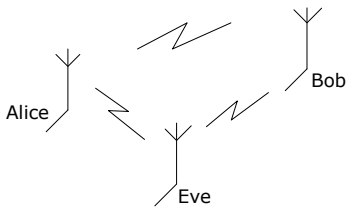

Fig. 1. Scenario with Alice, Bob, and Eve

The block diagram of our authentication system is illustrated in Fig. 2. Alice sends an additional signature together with the main message for Bob's verification. The signature is a function (e.g., hash) of the main message and a secret key negotiated between Alice and Bob before. This key is used to claim the unique identity of Bob and the validity of the message. Alice embeds the signature into the baseband modulated message signal as a watermarking and transmits them to Bob. The secret key is assumed uniquely known to both Alice and Bob and it has been allocated well before the communication starts. At the receiver, Bob decodes the main message while treating the embedded signature as noise and re-generates the signature using the secret key. Meanwhile, Bob extracts the signature from the received signal and then makes a judgment whether the message is authentic or not.

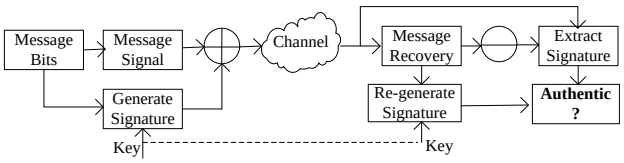

Fig. 2. Block diagrams of our approach

When Alice sends messages to Bob, Eve eavesdrops and tries to disturb the authentication as much as possible. Eve's primary purpose is to get the access rights to Bob, that is, Eve wants her messages can be accepted by Bob. Without loss of generality, assume that Eve is powerful; she knows the details of the authentication scheme only without the secret key. Thus, she can decode Alice's messages. However, she cannot authenticate them because of lacking the secret key.

The way to embed the signature into the modulated message signal is additional modulation. That is to modulate the baseband modulation signal again using the signature. The additional modulation parameters can be frequency, magnitude and phase. For example, additional magnitude modulation is intuitively shown as regular dithering of constellation points along the polar axis. It is implemented by superimposing the modulated signature signal onto the original message waveform at an imperceptible level. Considering the dynamic constraint on power amplifier and channel interference, the watermarking should be unobtrusive. Constellation dithering should be small enough to meet the modulation system requirements [12], [13].

B. *The Transmitter*

Assume the main message $\mathbf{b}$ that Alice sends to Bob is a binary sequence. The main message signal is denoted by $\mathbf{s} = f_s(\mathbf{b})$, where $f_s(\cdot)$ is an encoding function includes any prospective coding or modulation. The signature bits $\mathbf{d}$ is a function of the main message $\mathbf{b}$ and the secret key $\mathbf{k}$, which is denoted by

$$\mathbf{d} = g(\mathbf{b}, \mathbf{k}) \tag{1}$$

where the secret key $\mathbf{k}$ is used for the unique identity of the transmitter. Function $g(\cdot)$ is required to be collision resistant enough so that when $\mathbf{b}' \neq \mathbf{b}$ and $\mathbf{k}' \neq \mathbf{k}$, $g(\mathbf{b}', \mathbf{k}') = g(\mathbf{b}, \mathbf{k})$ with negligible probability. The signature signal (i.e., watermarking) is denoted by $\mathbf{w} = f_w(\mathbf{d})$, where function $f_w(\cdot)$ means the prospective coding and additional modulation, etc. $\mathbf{s}$ and $\mathbf{w}$ are assumed to be normalized signals, which meet $E[\mathbf{s}] = 0$, $E|\mathbf{s}|^2 = 1$ and $E[\mathbf{w}] = 0$, $E|\mathbf{w}|^2 = 1$, respectively.

The transmit signal $\mathbf{x}$ from Alice encapsulates signal $\mathbf{s}$ and $\mathbf{w}$, which is formulated by

$$\mathbf{x} = \rho_s \mathbf{s} + \rho_w \mathbf{w} \tag{2}$$

where $0 < \rho_s, \rho_w < 1$, and $\rho_s^2 + \rho_w^2 = 1$. Assume that $E[\mathbf{s}^H \mathbf{w}] = 0$, so ρ_s^2 and ρ_w^2 can represent the power

allocation ratios of the message and signature respectively. Obviously, when $\rho_w = 0$ the transmit signal $\mathbf{x} = \mathbf{s}$. So that signal $\mathbf{x}$ also meets $E[\mathbf{x}] = 0$, $E|\mathbf{x}|^2 = 1$.

C. The Channel Model

We take Rayleigh block fading channel for example. The channel of the symbols in the same block is highly correlated, but independent in different blocks. Set the channel of the i th block is h_i and $h_i \sim CN(0, \sigma_h^2)$. Each block of the transmitted signal observed at Bob is

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{n}_i \tag{3}$$

where $n_i \sim CN(0, \sigma_n^2)$ is complex white Gaussian noise.

To facilitate future discussion, three SNR terminologies are introduced here. The reference signal-to-noise ratio $\gamma = 1/\sigma_n^2$ represents the power ratio of the normalized transmitting signal to the noise. The message signal-to-noise ratio γ_s represents the SNR of the main message at the receiver. The signature signal-to-noise ratio γ_w represents the SNR of the extracted signature after the main message is decoded. Then, we have

$$\gamma_{s,i} = \frac{\rho_s^2 |h_i|^2}{\rho_w^2 |h_i|^2 + \sigma_\omega^2} = \frac{\rho_s^2 |h_i|^2 \gamma}{\rho_w^2 |h_i|^2 \gamma + 1}, \tag{4}$$

$$\gamma_{w,i} = \rho_w^2 |h_i|^2 / \sigma_\omega^2 = \rho_w^2 |h_i|^2 \gamma. \tag{5}$$

D. The Receiver

Upon receiving a message, Bob needs to verify it whether comes from Alice or not. Bob extracts the signature for authentication once he receives all blocks of a message frame. Assume Bob's channel estimate is $\hat{h}_i = h_i + v_i$, where v_i represents the estimated error of the equalizer. Function $f_s^{-1}(\cdot)$ is used to recover the message bits $\hat{\mathbf{b}}$, which satisfies $z = f_s^{-1}[f_s(z)]$ for all z. Bob recovers the message bits

$$\hat{\mathbf{b}}_i = f_s^{-1}(\mathbf{y}_i / \rho_s \hat{h}_i) \tag{6}$$

and extracts the watermarking

$$\hat{\mathbf{w}}_i = [\mathbf{y}_i - \hat{h}_i \rho_s f_s(\hat{\mathbf{b}}_i)] / \rho_w \hat{h}_i \tag{7}$$

Bob uses function $f_w^{-1}(\cdot)$ to recover the signature bits from the extracted watermarking

$$\hat{\mathbf{d}} = f_w^{-1}(\hat{\mathbf{w}}) \tag{8}$$

where $f_w^{-1}(\cdot)$ satisfies $z = f_w^{-1}[f_w(z)]$ for all z. On the other hand, the signature can be re-generated from the secret key

$$\tilde{\mathbf{d}} = g(\hat{\mathbf{b}}, \mathbf{k}). \tag{9}$$

E. Authentication

According to the analysis above, the authentication problem is equivalent to the transmission of weak signals in a fading wireless channel in which the gain is $h_i \sim CN(0, \sigma_h^2)$ and noise is $n_i \sim CN(0, \sigma_n^2)$. In this paper, time diversity is used to achieve this goal. It is not losing generality because a complex plan (e.g. error correction codes) can easily obtain better performance.

Function $f_w(\cdot)$ implements the time diversity. The time diversity is used to scatter the signature coding elements across different message blocks to ensure each of them experience approximate independent decline. Assume the signal length of $\mathbf{s}$ and $\mathbf{w}$ is L, the signature length of $\mathbf{d}$ and single message block length is M, then the diversity gain is $G_d = \lfloor L/M \rfloor$, and each message block contains a complete signature. Thus, the watermarking carried by the i th message block can be denoted by $\mathbf{w}_i = [d_{i,1}, d_{i,2}, ..., d_{i,L}]$, where $d_{i,j}$ indicates the i th repeat of the signature bit d_j. Bob estimates the signature by

$$\hat{\mathbf{d}} = f_w^{-1}(\mathbf{w}) = \sum_{i=1}^{R} \hat{\mathbf{w}}_i. \tag{10}$$

Bob believes the message is authentic if $\hat{\mathbf{d}} = \tilde{\mathbf{d}}$. So the probability of authentication for the message is

$$P = p(\hat{\mathbf{d}} = \tilde{\mathbf{d}}) = (1 - p_d)^M \tag{11}$$

where p_d is the bit error rate between $\hat{\mathbf{d}}$ and $\tilde{\mathbf{d}}$.

III. Properties

A. Robustness

A scheme is robust if it can continue the authentication process through inevitable channel interference and noise. Improving the robustness maintains high authentication probability. From (11) the authentication probability is directly related to the signature bit BER. Assume that Bob can get perfect channel estimation ($\hat{\mathbf{h}} = \mathbf{h}$), and decode the main message correctly ($\hat{\mathbf{b}} = \mathbf{b}$). Then, the average BER of the signature $\mathbf{d}$ can be formulated according to (5) and (10)

$$\begin{aligned} p_e &= Q\left(\sqrt{2\textstyle\sum_{i=1}^{G_d} \gamma_{w,i}}\right) \\ &= Q\left(\sqrt{2\rho_w^2 \|\boldsymbol{h}\|^2 \gamma}\right) \end{aligned} \tag{12}$$

where $\|\mathbf{h}\|^2 = \sum_{i=1}^{G_d} |h_i|^2$. $\|\mathbf{h}\|^2$ follows the distribution of $\|\mathbf{h}\|^2 \sim \chi^2(2G_d)$ when $\sigma_h^2 = 1$, and its probability density function is

$$f(x) = \frac{1}{(G_d - 1)!} x^{G_d - 1} e^{-x}, \quad x \geq 0 \tag{13}$$

and the average BER of the signature is

$$p_e = \int_0^\infty Q\left(\sqrt{2\rho_w^2 x \gamma}\right) f(x) dx. \tag{14}$$

From Fig. 3, the average BER of the signature p_e

markedly declines along with the increasing diversity gain G_d or its power allocation ρ_w^2. However, the signature's power allocation is not the more the better (see the analysis in the next sub-section), and the time diversity method is not always effective. When the length L is not large enough, e.g., Alice sends a short message to Bob. It cannot support a large diversity gain and then causes a high p_e. Aiming at this case, error correction codes (e.g., BCH, LDPC) can be cascaded before time diversity to decrease the signature error bits.

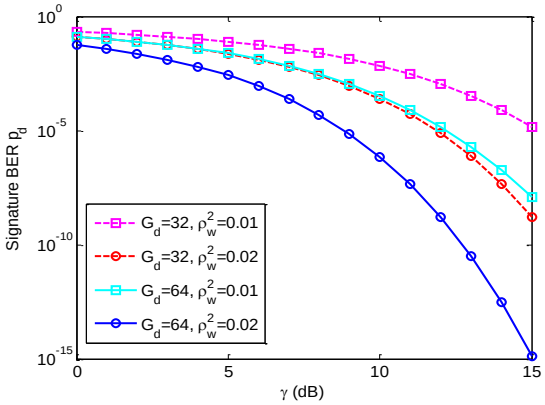

Fig. 3. The signature BER at different diversity gain and power allocation versus reference SNR

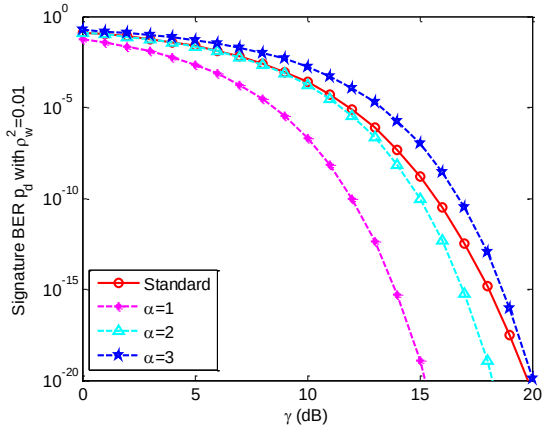

Fig. 4. The signature's power allocation versus reference SNR for different diversity gain

To ensure the scheme is robust enough, assume that the probability for authentication P should reach a threshold P^{th} at least. Since the signature is generated from (1), then the diversity gain G_d is fixed, there should have a lower bound of ρ_w^2. However, it's hard to figure out the necessary power allocation for the signature according to (14) at a given threshold P^{th} versus varying reference SNR, because the power allocation ρ_w^2 is always small and (14) cannot be simplified. Therefore a "relaxation-and-contraction" method is used to get an approximate lower bound for ρ_w^2.

The "relaxation" is to calculate the BER of the signature **d** by using the average SNR, then (12) is update to the following formulation when $\alpha = 1$.

$$p_e' = Q(\sqrt{2\rho_w^2 \gamma G_d / \alpha}) \tag{15}$$

where α is a control variable for the relaxation and contraction. As is depicted in Fig. 4, when $\alpha = 1$, the relaxed BER is much less than the standard BER from (12). The "contraction" increases α to meet the inequality $p_e' \geq p_e$ versus low reference SNR γ. For example, when $\rho_w^2 = 1$, $\alpha = 2$ is a proper contraction for $\gamma < 10$ dB according to Fig. 4. When given a threshold P^{th}, the BER threshold P_e^{th} of the signature meets the equation (11); for that Q function is a monotony decrease function, the approximate lower bound of ρ_w^2 is obtained from the inverse function of (15) at a proper α

$$\rho_w^2 \geq \frac{InvQ(p_e')\alpha}{2\gamma G_d} \tag{16}$$

where $InvQ(\cdot)$ is the inverse of Q function, p_e' is a contracted BER meets $p_e' > p_e^{th}$.

In order to satisfy the authentication threshold, when the diversity gain is low, it should increase the signature's power allocation correspondingly. However, with the power allocation constraint, it can be seen that using time diversity singly is not effective to achieve a high authentication probability especially at low reference SNR from Fig. 3. In this case, error correction codes are necessary.

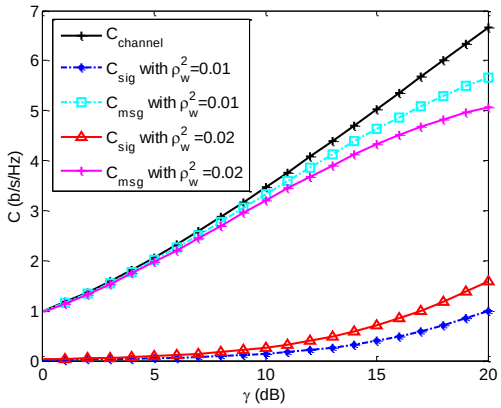

Fig. 5. The Shannon capacities versus reference SNR for different power allocation of the signature

B. Stealth

There are two aspects of a stealthy scheme. First, it should be covert. If it is obvious to adversaries that there has a stealthy transmission of authentication information, they may attempt to do damage. Second, it should be unobtrusive and not have a noticeable effect on the receivers' ability to recover the main messages. In this way, the scheme can be compatible with the common nodes which lack of peer to peer authentication mechanism.

The watermarking is covert against detection by

adversaries at any power when it is distributed as noise [4]. However, it should be at low power to achieve very slight data degradation, because the signature is equivalent to noise in the main message signal. As is depicted in Fig. 5, the channel capacity $C_{channel}$ is divided into two parts: the main message channel capacity C_{msg} and signature channel capacity C_{sig}. Though the capacity of signature channel is grown when the signature's power allocation increases, the capacity of main message channel is declined, and the decline is serious especially at high reference SNR.

From (4), the main message degradation can be denoted by

$$\lambda = E[\frac{\gamma_i}{\gamma_{s,i}}] = E[\frac{\rho_w^2 \mid h_i \mid^2 \gamma + 1}{\rho_s^2}] \tag{17}$$

where $E[\cdot]$ is the expectation. λ represents the degradation which caused by the watermarking. When give a threshold λ^{th}, the limit of the power allocated to the signature should meet

$$\rho_w^2 \le \frac{\lambda^{th} - 1}{\gamma + \lambda^{th}}. \tag{18}$$

Actually, low-power signature will reduce the robustness of the authentication. In this case, to continue the authentication, the gain of time diversity should large enough or the error correction codes are necessary, which had been discussed in the previous sub-section.

C. Security

A secure scheme should be resistant to adversarial attacks. In this sub-section we will examine the security of our scheme in several kinds of adversary models.

Without loss of generality, we assume that Eve is a powerful adversary. She knows the authentication scheme only without the secret key. Her main purpose is to make her messages be received by Bob. The following three attack models may be used by Eve.

1): Replay attacks: Eve can simply resend a message that Alice transmitted in the past. She wants Bob to receive the replayed message. This kind of attack is called the replay attack. If the replayed message is authenticated, Bob will be blocked by a lot of these useless messages.

Once Eve has captured a message that Alice transmitted to Bob, she could recover the main message and extract an estimated signature. Assume that Eve is powerful and her estimated signature is correct. Eve can then transmit the signature and main message together to Bob like Alice. However, Bob will not accept it if the secret key is time varying, that is, the signature is valid only on the first transmission by Alice to Bob.

It is difficult to distribute, refresh and revoke the secret key, especially in ad hoc networks. However, the CSI is suitable for secret key update because of its time varying attribute [1]. Assume in the Time Division Duplex wireless communication system, Bob replies with a confirm message when he receives a message. The message reply is short enough, which maybe only contain the pilot and the confirmed frame number, so that it can be transmitted within one block. Suppose that the channel Alice estimated according to the reply message is $\hat{\mathbf{h}}_N^{BA}$, and it is same of $\hat{\mathbf{h}}_N^{AB}$,where N represents the frame number and $\hat{\mathbf{h}}_N^{AB}$ is Bob's estimated channel for the last block of the received authentic message. Through proper quantitative method [14], [15], [16], the secret key $\mathbf{k}_{N+1}$ of Alice and Bob is generated by $\hat{\mathbf{h}}_N^{BA}$ and $\hat{\mathbf{h}}_N^{AB}$ respectively. So the secret key for the next transmission has updated.

2) Impersonation attacks: Eve may try to create her own messages like Alice, and hope they could be accepted by Bob. Unfortunately, she lacks the secret key, so she must generate valid signatures based on her observations. According to (1), each message is required to have a valid signature. Eve may decrypt the secret key from the main message and the signature she recovered from Alice. Without loss of generality, if the Alice-Eve channel is noiseless, Eve can estimate the main messages and signatures accurately. Then, Eve may make more attempts to gain information about the secret key.

Thus, a powerful signature creation function $g(\cdot)$ is needed to increase the difficulty for Eve's attack, or using a time-varying secret key with CSI.

3) Substitution attacks: There are two aspects to the substitution attack. The first possible case happens after Eve has acquired a message $\mathbf{b}$ from Alice to Bob. Eve modifies it to $\mathbf{b}'$ which is a malicious message and transmits it to Bob. The attack is successful if the receiver accepts $\mathbf{b}'$. However, along with $\mathbf{b}$, Alice will transmit a signature $\mathbf{d}$ to verify the completeness of $\mathbf{b}$. According to (1), if Eve modifies $\mathbf{b}$ to $\mathbf{b}'$, she should construct a new matching $\mathbf{d}' = g(\mathbf{b}', k)$. Since the secret key $\mathbf{k}$ is unknown to Eve, this kind of substitution attack is prevented.

Another kind of substitution attack occurs on the transmission of Alice to Bob. When Alice transmits messages to Bob, Eve may try to modify some symbols by overpowering Alice's signal with her malicious signal. In this case, Eve only corrupts the original signal incoherently. The distorted messages will be discarded by Bob because they are not authentic. Eve will have great difficulty succeeding with this attack. However, if Eve only wants to disturb the authentication, the optimal way is to jam the signature signal by concentrating her energy. If the jamming signal pollutes several blocks it could not create a fatal disaster because of the time diversity. If most blocks of the frame suffer from pollution, the result depends on the robustness of the authentication. We will give tradeoffs among the robustness, stealth and security

in the next sub-section.

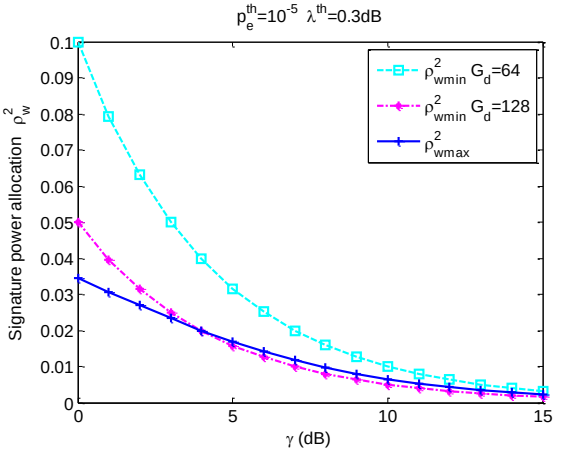

Fig. 6. The signature's power allocation versus reference SNR at giving thresholds.

D. Tradeoffs

The tradeoffs primarily aim to guide the signature's power allocation ρ_w^2 versus different reference SNR.

According to the analysis of sub-sections A and B, that the scope of the signature's power allocation ρ_w^2 versus reference SNR at giving thresholds p^{th} and λ^{th} is depicted in Fig. 6. When the threshold λ^{th} is given, the upper bound of signature's power allocation $\rho_{w\max}^2$ is decided. The threshold p^{th} guides an approximate lower bound of signature's power allocation $\rho_{w\min}^2$ together with diversity gain G_d. If G_d is not large enough, then error correction codes are necessary. For example, this case happens if $\gamma < 4$ dB when the thresholds $p^{th} = 10^{-5}$, $\lambda^{th} = 0.3$ dB and diversity gain $G_d = 128$ according to Fig. 6.

For the robustness, $\rho_{w\max}^2$ is optimal, but for stealth, $\rho_{w\min}^2$ is optimal. For the security, $\rho_{w\max}^2$ is resistant to the jamming attack but helpful for Eve's brute-force attacks if the secret key is stable. A time-varying secret key is more effective to enhance the scheme security. Thus, we would like to set $\rho_w^2 = \rho_{w\max}^2$.

Furthermore, due to the dynamic constraint on the power amplifier, embedding watermarking should meet the requirements of the modulation system [8], where the error tolerances of modulator for the metrics with respect to the ideal signal are presented in the physical layer protocol specification of IEEE 802.11 [12], [13].

IV. Comparisons with Previous Works

The works in [2] and [3] show the typical applications of digital watermarking to identify the multimedia copyright ownership. Similarly, by utilizing an inherent characteristic of the modulator, we introduce the digital watermarking into the message authentication. Because of imperfect product technologies of the hardware, it allows minor errors existing in its modulated signals [12], [13]. Thus, the low-power watermarking can be embedded into the baseband modulated signal. Moreover, the advanced watermarking technologies in [2], [3] *et al.* are suitable to be applied in our work.

Compared with the work in [4], the first improvement is that we embed the authentication information at modulation domain. Our work imitates the imperfection of the modulator by the Software Defined Radio (SDR), then for the opponent, it is hard to distinguish the watermarking and the inherent errors of the modulated signal. The second improvement is that we authenticate the entire message instead of each message block. When a block suffers deep fading, it is difficult to decode the embedded authentication message, and it will cause a high misdiagnosis rate. However, in our work, the time diversity scatters the deep decline of some blocks into other blocks, then, each block can experience approximate the same decline. Moreover, authentication messages are not independently embedded in each block in case of the impersonation attack of single message block.

Furthermore, compared with the work in [8], we introduce watermarking to improve its disadvantages. Though the hardware-based fingerprinting of the work in [8] is transmitted in a covert way, it still can be easily sniffed and impersonated by powerful attackers [10], [11]. Because the hardware-based fingerprinting cannot be refreshed and revoked. However, the watermarking in our work can be seen as a mask of the real features (i.e., the hardware-based fingerprinting) of the legal transmitter. Thus, by renewing the secret key (i.e., equation (1)), we can easily protect against opponents' impersonation attack.

In general, based on the previous works above, we introduced watermarking, which is traditionally applied to identify multimedia copyright ownership, into the area of message authentication in wireless communications.

V. Conclusion

The essence of authentication is the transmission of unique and non-reproduced identification information, which is used to verify whether the transmitter is legitimate and the message is valid. In this paper, the authentication becomes the transmission of weak signals in wireless channels. This transmission is implemented by modulation domain watermarking. Guidelines of the signature's power allocation are given according to the threshold of the robustness and stealth. Meanwhile, the scheme security is ensured by a powerful signature creation function. In general, a flexible and low complexity framework for physical layer authentication schemes is presented, and can be used together with upper layer security schemes to provide a more secure system.

References

[1] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security," *IEEE Wireless Communications*, vol. 17, pp. 63-70, 2010.
[2] S. H. Supangkat, T. Eric, and A. S. Pamuji, "A public key signature for authentication in telephone," *Circuits and Systems*, vol. 2, pp. 495-498, 2002.
[3] X. Wang, Y. Wu, and B. Caron, "Transmitter identification using embedded pseudo random sequences," *IEEE Trans. on Broadcasting*, vol. 50, pp. 244-252, 2004.
[4] P. L. Yu, J. S. Baras, and B. M. Sadler, "MIMO authentication via deliberate fingerprinting at the physical layer," *IEEE Trans. on Information Forensics and Security*, vol. 6, pp. 606-615, 2011.
[5] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. on Wireless Communications*, vol. 7, pp. 2571-2579, 2008.
[6] X. Wang, F. J. Liu, D. Fan, H. Tang and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. ICC'11 Conf*., 2011, pp. 1-5.
[7] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "BANA: Body area network authentication exploiting channel characteristics," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1803-1816, 2013.
[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM International Conference on Mobile Computing and Networking*, 2008, pp. 116-127.
[9] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. on Information Forensics and Security*, vol. 6, pp. 1346-1354, 2011.
[10] M. Edman and B. Yener, "Active attacks against modulation-based radiometric identification," *Rensselaer Institute of Technology, Technical report*, pp. 09-02, 2009.
[11] B. Danev and L. Heinrich, "Physical-layer Identification: Secure or not?" *ETH*, vol. 8, pp. 10, 2009.
[12] IEEE Standards Association. IEEE Std 802.11a. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11a-1999.pdf
[13] IEEE Standards Association. IEEE Std 802.11b. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11b-1999.pdf
[14] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communication," *IEEE Wireless Communications*, vol. 18, no.4, pp. 6-12, August 2011.
[15] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. on Vehicular Technology*, vol. PP, no. 99, pp. 1-1, 2014.
[16] O. Gungor, F. Chen, and C. E. Koksal, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. on Mobile Computing*, vol. 12, pp. 917-930, 2013.

Fanfan Zheng received the B.S. degree from the Department of Electronic Engineering, Anhui Jianzhu University, Hefei, China, in 2009, and is currently pursuing the Ph.D. degree in the Department of Communication Engineering, Xiamen University. His research interests mainly focus on wireless communication security and optimization theory.

Lianfen Huang received her B.S. degree in Radio Physics in 1984 and Ph.D. in Communication Engineering in 2008 from Xiamen University. She was a visiting scholar in Tsinghua University in 1997 and visiting scholar in the Chinese University of Hong Kong in 2012. She is a professor of Communication Engineering, Xiamen University, Xiamen, China. Her current research interests include wireless communication, wireless network and signal processing.

Jing Wang received the B.S. and M.S. degree in electronic engineering from Tsinghua University, Beijing, China in 1983 and 1986 respectively. He has been on the Faculty at the Tsinghua University since 1986. He currently is a professor of the School of Information Science and Technology. He serves as the deputy director of Tsinghua National Lab for Information Science and Technology. His research interests are in the area of wireless communications, including transmission and networking technologies of 4G/B4G.