# Security Analysis of Authentication Overlaying Tag Signal

Song Huawei(✉), Liang Jin, and Shengjun Zhang

National Digital Switching System Engineering and Technological R&D Center,
Zhengzhou, China
greatboy_song@sina.com

**Abstract.** This paper presents a new method for authentication based on overlaying tag signal. The tag signal and communication signal are superimposed to form the signal "watermark". From the point of view of signal transmission, the tag signal can achieve the dual "binding" of shared key and channel. Security analysis and simulation results indicate that it can achieve high authentication success rate and low failure rate. This method does not require complex cryptographic algorithms. So it can achieve security under the premise of reduce the computational amount in the communication process.

**Keywords:** Tag signal · Authentication · Physical layer security

## 1 Introduction

Authentication technology is an important part of information security [1]. Generally, authentication includes both identification authentication and message authentication. The former is used to authenticate the user identity; the latter is used to ensure the non-repudiation of communication and the integrity of the transmission of information. In the existing mobile communication system, the identity authentication and message authentication are based on cryptographic algorithm. That is to say, the authentication implementation is carried out at the high level, using the cryptographic algorithm to calculate numerical results which are difficult to be counterfeited. The eavesdropper can get the message content of the transmission, and the security is completely dependent on the difficulty of deciphering the cryptographic algorithm. Simmens summarizes this authentication security model [2], and points out that success rate of attack are related to the size of the key space |K|. It is depressing that the lower bound of the attack success rate is, which is much higher than guessing the key. Maurer further proves that the success rate of attack is also related to the times of authentication, and it may increase with the growth of times [3].

In traditional communication system, a cryptographic algorithm is used to compute MAC (Message Authentication Code). Due to both of legal sides sharing private key, the generated MAC will be the same. The receiver can determine whether the message is from legitimate senders by comparing MAC. This method is equivalent to make tag at the message level for authentication. In this paper, a new method using tag signal

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 173–180, 2018.
https://doi.org/10.1007/978-3-319-90802-1_15

realizes the physical layer authentication. Taking the advantage of legality sides sharing a private key and having coherent channel state information in short time, the sender produce tag signal from spread frequency code and measured channel state information, then overlap the tag signal on the communicational signal. The receiver can detect the correct tag signal and demodulate the communicational signal. This method can avoid using complex cryptographic algorithm, reduce the amount of calculation, and prevent passive eavesdropping and active attack effectively.

## 2 Related Works

In recent years, the physical layer security technology has attracted more and more attention of researchers. Wireless channel has characteristics of uniqueness, diversity and reciprocity. It provides a new direction for information security [4, 5]. Authentication in physical layer has already become a new hot spot in the authentication technology. Xiao et al. proposed the method of authentication using "channel fingerprint". Hypothesis test can check channel characteristic similarity [6]. But this kind of methods need cipher algorithm to complete authentication for the first time [7, 8]. The physical layer "challenge-response" method hidden key and authentication information in the wireless channel amplitude and phase information [9, 10]. It can be used to enhance authentication security when user access networks for the first time, but this method does not apply to the message authentication. Adding tag information on the frequency spectrum of the signal is also a good method. It has been used in the key generation [11], wireless spectrum identification and determining the interference [12, 13]. But these methods are not very applicable to wireless authentication.

## 3 System Model

Alice and Bob are legitimate sender and receiver and they pre-allocated the private key K. Eve is a malicious third party, who knows time slot, frequency band, and modulation mode, etc. The channel between Alice and Bob is $\mathrm{h_{AB}}$, the channel between Alice and Eve is $\mathrm{h_{AE}}$, and the channel between Eve and Bob is $\mathrm{h_{EB}}$. Suppose that Alice sends signal x, and Bob receives signal y and Eve receives signal z, then:

$$\mathrm{y = x * h_{AB} + n_{AB}} \tag{1}$$

$$\mathrm{z = x * h_{AE} + n_{AE}} \tag{2}$$

In (1) and (2), $\mathrm{n_{AB}}$ and $\mathrm{n_{AE}}$ are the noise between Alice and Bob, Alice and Eve. And they are independent of each other. The asterisk represents convolution operation. In TDD (time division duplex) system, the channel parameters of the two parties are basically unchanged in a short period of time, which can be considered as short-term reciprocity. It means that $\mathrm{h_{AB} \approx h_{BA}}$. Eve might receive a signal from Alice, or send a signal to Bob and try to make Bob accept it (Fig. 1).

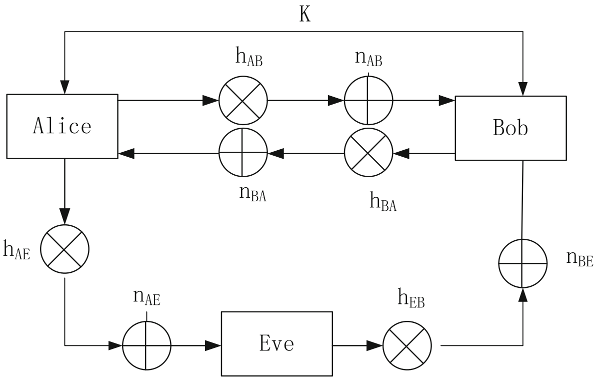

**Fig. 1.** System model

## 4 Process of Overlaying Tag Signal Authentication

Alice produces tag signal, and overlay with communication signals. Bob can normally demodulate signal, and check the correction of tag signal at the same time. Because the tag signal is generated by the shared key and reciprocity channel quantitative values through common produce m-sequence spread spectrum, Alice and Bob can generate the same tag signal. The tag signal and communication signal realize reuse in the wireless

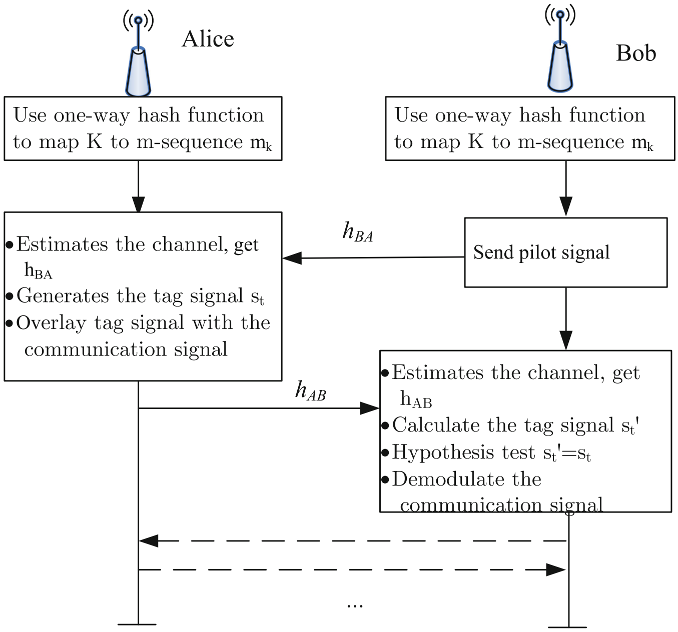
Alice
Bob
Use one-way hash function to map K to m-sequence $m_k$
Use one-way hash function to map K to m-sequence $m_k$
$h_{BA}$
Send pilot signal
• Estimates the channel, get $h_{BA}$
• Generates the tag signal $s_t$
• Overlay tag signal with the communication signal
$h_{AB}$
• Estimates the channel, get $h_{AB}$
• Calculate the tag signal $s_t$'
• Hypothesis test $s_t'=s_t$
• Demodulate the communication signal
...

**Fig. 2.** Process of overlaying tag signal authentication

channel. Eve don't know the spread spectrum code, so he can only rely on guessing to fake Alice. Within limited times of attacks, it is difficult to succeed for Eve.

As shown in Fig. 2, the process of overlaying tag signal authentication has five steps.

**Step 1:** The preparation stage

Prior to the start of the communication, Alice and Bob pre-assigned private key K and public spread sequences {$m_i$}, i = 0, 1,..., N. Let's set the set space of key K is |K|. And it is satisfied that N > |K|. Alice and Bob use the same one-way hash function to map K to the same spread-spectrum m-sequence $m_k$. The one-way hash function should have the following properties:

(1) The randomness of hash value has no obvious statistical characteristics;
(2) Small amount of computation can be realized quickly;
(3) Unidirectional. It is difficult to obtain input in reverse according to the result of hashing, preventing secret information from being leaked;
(4) Anti-collision. It is very difficult to ensure that another input with the same hash value is found, which is to prevent Eve's dictionary attack.

**Step 2:** Bob sends the pilot, and Alice estimates the channel $h_{BA}$

Bob send pilot signal to Alice. Alice estimate $h_{BA}$ and get approximate value $\hat{h}_{BA}$. In this course, equal probability of quantitative measurement is used. Because of the influence of the noise, $\hat{h}_{BA}$ is the noisy version of the real channel. That is: $\hat{h}_{BA} = h_{BA} + n_{BA}$, $\hat{h}_{BA} \sim CN(0, \sigma_h^2)$, $n_{BA}$ is random variable which obey the complex Gaussian distribution. $n_{BA} \sim CN(0, \sigma_n^2)$. And the signal-to-noise ratio can be written as $SNR = \sigma_h^2/\sigma_n^2$.

**Step 3:** Alice generates the tag signal and sends it overlaying with the communication signal.

Alice spread spectrum for $\hat{h}_{BA}$ with m-sequence $m_k$, then gets tag signal $s_t$. The tag signal and communication signal are overlaid to send to Bob, that is:

$$s_t = m_k \hat{h}_{BA} \tag{3}$$

$$x = s_s + s_t \tag{4}$$

The signal Bob received is:

$$y = \left(s_s + s_t\right) * h_{AB} + n_{AB} \tag{5}$$

**Step 4:** Bob receives the signal and checks the tag

Bob estimates the channel $h_{AB}$, then get the approximate value $\hat{h}_{AB}$ through the same method as Alice. Bob may calculate the tag signal $s_t' = m_k \hat{h}_{BA}$. According to the principle of spread spectrum communication, communication signal can still normally despread under higher spread spectrum gain. After eliminating the tag signal $s_t'$, the received signal can continue to demodulate. There are two alternative assumptions:

$H_0$: The tag signal $s_t$ is sent by Alice;
$H_1$: The tag signal $s_t$ is not sent by Alice.

Accordingly, due to the influence of channel noise, the channel characteristics of Alice and Bob may not be completely consistent. The bit strings resulting from $\hat{h}_{AB}$ and $\hat{h}_{BA}$ may be written as str($\hat{h}_{AB}$) and str($\hat{h}_{BA}$). Here quantitative difference rate is defined as $\rho$, which means a percentage through comparing each bit of two series of string. We set hypothesis threshold as $\Gamma$, which usually can be chosen as constant, such as $\Gamma = 99\%$. Then the hypothesis criteria may be: $H_0$ is accepted when $\rho \geq \Gamma$, alternatively $H_1$ is accepted when $\rho < \Gamma$.

**Step 5:** Alice and Bob correspond continuously

After the success of the authentication, Alice and Bob can continuously communicate, maintaining normal pilot signal and channel estimation. If the conditions that channel are not satisfied for the reciprocity after a long interval, we may return to step 2 for a new round of authentication.

## 5 Safety Analysis

For the security of the authentication, there are two type indicators of success rate and failure rate. And there are two major errors in the hypothesis test. One is that Alice superimposes the tag signal without being tested, and Bob rejected the signal that Alice sent. It is called the false alarm rate. The second is that Eve was accepted by Bob as Alice, which is called the missing alarm rate. The reason for the first type of error is similar to the successful rate, and the second error will be analyzed below.

As mentioned above, the success rate of the attacker is higher than $1/\sqrt{|K|}$ in the traditional authentication model [2]. Under the authentication method of this paper, if Eve wants to fake the tag signal, he needs to fake a spread signal that can pass the hypothesis test. According to the above assumptions, the space of m-sequence is $|m|$, and the space is big enough: $|m| > |K|$. Because of the one-way hash function, the lower bounds of attack success rate is $1/|K|$. That is to say that it is worst for Eve to guess the key. Due to the mutual correlation characteristics of m-sequence, different m-sequences are unrelated. In the process of authentication, Eve even may get some sample tag signal. But Eve cannot get useful related peak. So the success rate of Eve is still limited to $1/|K|$. That is the same as guessing the key. Specific analysis is made on different attacks against Eve.

### 5.1 Passive Eavesdropping

In some cases, it is the Contact Volume Editor that checks all the pdfs. In such cases, the authors are not involved in the checking phase.

This method realizes the hidden transmission of the tag signal. In general, due to the location of Bob and Eve won't be exactly the same, the legal channel hAB is not related to hacking channel hAE. So Eve cannot obtain legal channel information. The assumption on position of Eve is very reasonable in actual communication system, and it is also very easy to satisfy [14]. On the other hand, Alice and Bob's key are pre-allocated safely, and Eve is not available. Since the tag signal is generated by the channel information and the key, this is equivalent to "double locks" for the tag signal. Eve cannot obtain any information about the tag signal.

In the process of signal transmission, the design of matched filter needs to know the frequency response of the signal. It is difficult for Eve to receive and detect the tag signal. Even if Eve get part information of the tag signal by using the method of statistical signal processing, it is still difficult to pose a security threat. Because the channel is time-varying, the tag signal has a natural of timeliness and it made useless for Eve's passive eavesdropping.

## 5.2 Substitution Attack

Eve can attack by eavesdropping and modifying the signal that Alice sends. Eve will firstly remove the legal tag signal and then attach a forged tag signal. If the signal is received and passed through authentication successfully by Bob, Eve's attack is considered successful. The probability of successful attack is represented by $\beta$, which indicates the probability that Bob will receive the signal sent by Eve.

Because the tag signal is generated by a one-way hash function based on the channel and key, Eve can generate the tag signal by guessing the channel and key, or simply forging the tag signal. For a particular key K, if the inconsistency probability of the fake tag with the legal tag is less than Γ, the attack is successful. Therefore, the attack rate can be expressed as:

$$\beta = P(\rho < \Gamma) = \sum_{i=1}^{\Gamma M} C_M^i (\frac{1}{2})^i (\frac{1}{2})^{M-i} = \sum_{i=1}^{\Gamma M} C_M^i (\frac{1}{2})^M \tag{6}$$

It is analyzed that Eve was less likely to acquire a tag signal through passive eavesdropping. So it is difficult to make a successful attack, even in a passive and alternative way.

## 5.3 The Attack of Man-in-the-Middle

Assuming that Eve adopts an aggressive way of amplifying and forwarding, this type of attack is also known as transparent forwarding. Eve doesn't change the signal. According to the system model, the signal Bob received is changed to:

$$y = (x * h_{AE} + n_{AE}) * h_{EB} + n_{EB} \tag{7}$$

After finishing, it becomes:

$$y = x * (h_{AE} * h_{EB}) + (n_{AE} * h_{EB} + n_{EB}) \tag{8}$$

It can be seen that both the channel and the noise of Bob have changed. In (8), $n_{AE} * h_{EB} + n_{EB}$ is considered to be new noise. The channel between Alice and Bob $h_{AB}$ becomes the cascade of the channel $h_{AE}$ and $h_{EB}$. The conditions for the reciprocity of Alice and Bob are still satisfied. At the same time, because of Eve's involvement, Bob received a signal that was mixed with Eve's noise. The increase of noise may worsen the signal-to-noise ratio, which has an impact on the performance of the authentication. But Eve is unable to implement the replacement of Alice, and there is no difference in tag signal acquisition with passive eavesdropping.

## 6 Simulation Analysis

BPSK is exampled as the communication signal. The m-sequence with a length of 100 bits is used as the spread spectrum sequence. The channel parameters obey 3GPP standard Urban channel model, and 10,000 times of monte-carlo simulation is adopted.

Firstly, the influence of power distribution of the tag signal and communication signal is shown in Fig. 3. Because they are superimposed in the time domain, an important measurement is the proportion of power distribution. Making SNR = 10 dB as a typical value, the simulation is carried out when spread spectrum code length is 100 bits. It can be seen from Fig. 3(a), when tag power accounted for more than 1%, false alarm rate and missing alarm rate achieve a lower level. Because the amplification gain can resist the equivalent interference, the normal demodulation of the communication signal is not affected when the label power ratio is less than 50%. And the bit error rate is stable. Keeping 10% of the tag signal power ratio, simulation is carried out under different signal-to-noise ratio in Fig. 3(b). It can be found that in low SNR, false alarm rate and the bit error rate are both high, and it can achieve good indicators when SNR is higher than 10 dB.

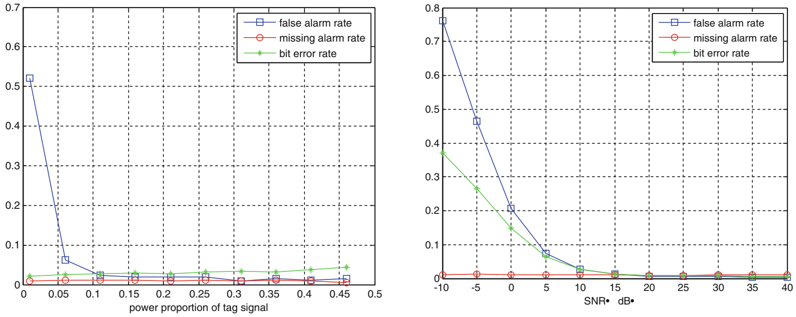

**Fig. 3.** Simulation diagram of performance, (a) power proportion, (b) SNR

## 7 Conclusion

The method of overlaying tag signal authentication in physical layer can get rid of the cipher algorithm. The dual authentication of channel and identity is realized at the signal level. It can reduce the computational complexity in the process of communication, and achieve security enhancement to the existing authentication process. It also can be used to make up for the defect of business data authentication, and can be applied to "light-weight" authentication of the future mobile communication in low delay, high reliable scenarios.

## References

1. Li, Z., Zhan, B., Yang, Y.: A survey of identification and authentication. Acta Electron. Sin. **27**(1), 98–102 (1999)
2. Maurer, U.M.: Authentication theory and hypothesis testing. IEEE Trans. Inf. Theory **46**(4), 1350–1356 (2000)
3. Yuan, H.: Research on key technologies of wireless network physical layer authentication based on radio frequency fingerprinting, Ph.D. dissertation. Southeast University (2011)
4. Paul, L.Y., Baras, J.S., Sadler, B.M.: Physical-layer authentication. IEEE Trans. Inf. Forensics Secur. **3**(1), 38–51 (2008)
5. Zeng, K., Govindan, K., Mohapatra, P.: Non-cryptographic authentication and identification in wireless networks. IEEE Wireless Commun. **17**(5), 56–62 (2010)
6. Xiao, L., Greenstein, L.J., Mandayam, N.B., et al.: A physical-layer technique to enhance authentication for mobile terminals. In: Proceedings of IEEE International Conference on Communications, Beijing (2008)
7. Tugnait, J.K., Kim, H.: A channel-based hypothesis testing approach to enhance user authentication in wireless networks. In: Proceedings of Second International Conference on Communication Systems and Networks, Bangalore (2010)
8. Shukla, M.K., Trivedi, A., Pandey, O.J.: Physical layer authentication for mobile terminals over MIMO fading wiretap channels. In: Proceedings of International Conference on Advances in Computing, Communications and Informatics, Mysore (2013)
9. Shan, D., Zeng, K., Xiang, W., et al.: PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. IEEE J. Sel. Areas Commun. **31**(9), 1817–1827 (2013)
10. Du, X., Shan, D., Zeng, K., et al.: Physical layer challenge-response authentication in wireless networks with relay. In: Proceedings of IEEE International Conference on Computer Communications (2014)
11. Molière, R., Delaveau, F., Ngassa, C.L.K., et al.: Tag signals for early authentication and secret key generation in wireless public networks. In: Proceedings of European Conference on Networks and Communications, Paris (2015)
12. Liu, Z., Xu, J., Zhao, K.: Spectrum water printing technology based on spectrum signal. J. Hebei Univ. Sci. Technol. **S1**, 116–118 (2011)
13. Zhang, Y., Xu, J., Liu, Y., et al.: Spectrum tag embedding and extracting method based on correlation identifier. Chin. J. Radio Sci. **31**(1), 185–192 (2016)
14. Jakes, W.C., Cox, D.C.: Microwave Mobile Communications. Wiley, Hoboken (1994)