Review of Physical Layer Security Technology in Battlefield Network

Jialong Wu*, Qinghua Ren, Ming Li, Zhikai Fan, Guangda Zhang

College of Information and Navigation, Air Force Engineering University, Xi’an, Shannxi, 710000, China

*Corresponding author’s e-mail: 813544351@qq.com

Abstract. Global openness of battlefield network makes it face many security threats, the physical security technology can provide an important support to traditional security system and strong protection to messages transmission, studying its application in battlefield network is of great significance. In view of the current and future network development trend, this paper studies the physical layer security problem from the perspective of battlefield network under modern warfare conditions, summarizes and analyzes the basic model of physical layer security, sorts out and introduces the physical layer security technology of wireless communication, and finally summarizes the risks and challenges still faced by the physical layer of the current battlefield network.

1. Introduction

Currently, faced with the information environment of great development of 5G technology and the significant improvement of communication Key Performance Indicator (KPI), the vision of interconnection of everything and integration of heaven and earth has gradually become possible. However, with the rapid development of information technology, the increasing dependence on technology also highlights the absolute importance of information security.

Different from the computer network, the wireless network is characterized by its broadcast characteristics of information transmission. The medium of wireless communication is open, and the signal is transmitted in the air by the base station as a transit. Theoretically, as long as there are devices similar to the base station, the signal can be received. Therefore, information security has a typical "bucket effect". Wireless communication becomes the "shortest board" of information security just because of its open nature.

As the battlefield network is restricted by the confident information, and the resource space on the upper layer of the network is greatly limited, which means that in the whole network architecture, most of the current research schemes are no longer applicable to the battlefield network environment, and the demand of battlefield network security is bound to call for the emergence of new technologies. As the bottom layer of the protocol stack, the physical layer provides the possibility to solve the security problem of wireless battlefield communication network from the source. At present, the transformation of network structure from Internet to Cyberspace also promotes the gradual development of network security from outside to inside. The uniqueness of wireless channel reflects the endogenous security attribute of wireless channel, which undoubtedly points out a new direction for the development of battlefield network security situation.

The application of hollow technologies greatly increases the channel transmission of information, which makes the endogenous security elements of wireless network also get abundance. At the same
time, the abundance of endogenous security element also brought the ascension and progress of physical security. Physical layer security technology, which does not depend on high computational complexity, undoubtedly provides a new security system with high applicability for the significant improvement of KPI of battlefield network.

2. Review of physical layer security model

For complex and changeable security problems, the physical layer security based on information theory security mainly develops into two main lines: wireless key security mechanism led by Shannon and non-key security mechanism led by Wyner.

2.1. Shannon model of information theory

In 1949, Shannon put forward the basic principle of Communication Secrecy in his article "Communication Theory of Secrecy Systems" [1]. The fundamental principle of confidentiality is to ensure that the receiving party can receive the message from the sender without any error, and that the transmission process of the message cannot be eavesdropped by other users.

In the perfect confidentiality model proposed by Shannon, the message sender tries to send the message to the receiver through encoding, but the codeword can be obtained unconditionally and completely by the eavesdropping party in the eavesdropping channel without any confidentiality measures. In the actual information transmission environment, there are always different forms of noise interference, so in order to ensure the security of communication in such a complex communication environment, compared with the eavesdropping party, the legitimate receiver must have a certain degree of advantage. It proposes a "one time one secret" encryption scheme based on random key, which decrypts the code word by the key known to only the legal parties, obtains the code word before sending and then obtains the message $M$ by decoding.

By quantifying the average uncertainty of eavesdropping users, the mathematical representation of secure communication is obtained: the information entropy $H(M|X)$ of the message under the given code word can be used to calculate the information security. $H(M|X)$ represents the uncertainty of the message after the eavesdropping party receives the code word, and can be expressed as the loss entropy of the eavesdropping party. Assume that hacking the damage equals the uncertainty of information entropy, namely

$$H(M|X) = H(M)$$  \hspace{1cm} (1)

If the above formula is true, the system has perfect confidentiality. It also indicates that the code word and the message are independent of each other, and there is no correlation between them, so it can ensure that the eavesdropper cannot obtain any information through the code word no matter what means it takes. In addition, from the perspective of encryption, when the system has perfect confidentiality, the uncertainty of the selected key will not be less than the uncertainty of the message, namely

$$H(K) \geq H(M)$$  \hspace{1cm} (2)

![Figure 1. Physical layer security authentication model](image-url)
2.2. Wyner hacking model

In 1975, Wyner proposed an eavesdropping channel model in order to further understand the secure communication in the case of noise due to the existence of random noise and non-erasable interference in the actual physical channel [2]. Unlike the Shannon model, which requires the legitimate receiver to have an advantage in a certain aspect that the eavesdropper does not have, the confidentiality condition defined by the Wyner model stipulates that if the code word length $n$ is large enough, the suspicion rate is required to be infinitely close to the entropy rate of the information, which relaxes the condition for achieving perfect confidentiality, namely

$$\frac{1}{n} H(M|Z) = H(M)$$

The information theory security standard proposed by Wyner can be expressed as follows:

$$I(Z;M) = 0$$

That is, the average amount of information transmitted in a perturbed discrete channel is 0.

In general, the security of legitimate users under the Wyner model can be measured by the security capacity, that is, the error probability of the legitimate recipient can reach the maximum transmission rate of any hour under the appropriate coding method:

$$C_i = \max [I(X;Y) - I(X;Z)]$$

Through the current research and analysis, the security of users can also be measured by other indicators like bit error rate, signal-to-noise ratio, traversal security rate, security terminal probability and so on.

![Physical layer security authentication model](image)

2.3. Maurer scheme

In 1993, based on the two models of Wyner and Shannon, the reciprocity of wireless Channel makes Channel State Information (CSI) detected by both parties have strong correlation, which enables both parties to generate a set of symmetric keys without error on the basis of public Channel discussion [3]. Meanwhile, the fast time-variability of wireless Channel also ensures the dynamic change of key, so as to prevent illegal users from eavesdropping.

According to the characteristics of this principle, Maurer proposed a new scheme based on security keys in his article "Secret Key Agreement by Public Discussion From Common information", aiming at making the communication security of eavesdropping channel better than that of legal channel possible.

3. Review of physical security method

The physical security method is based on information theory and aims at achieving unconditional security. In the process of information instruction transmission, in order to ensure the security of tactical wireless network, the physical layer security problems can be divided into three parts: authentication, encryption processing and secure transmission. The authentication mechanism is used to verify the identity of users and restrict certain users (authorized users) to use network resources. The encryption mechanism is used to encrypt the data of the wireless link to ensure that the data of the
wireless network can only be accepted and understood by the expected users. The scheme of secure transmission ensures that the message cannot be obtained by the illegal eavesdropper due to the influence of network environment and means.

3.1. The physical layer security authentication

Different from the authentication scheme on the upper layer of the network, the physical layer authentication is to verify and analyze the channel characteristics of both ends by combining the spatial and temporal characteristics of the transmission message and the transceiver channel, so as to realize the authentication of both sides of the communication in the physical layer. The identity authentication of physical layer can effectively guarantee the high reliability in the process of sending and receiving messages. In this way, the amount of information obtained by the hacking party will be got down to almost zero. The advantages of low complexity and fast authentication speed correspond to the high dynamic demand of tactical network, which can provide an effective scheme for the security of tactical network without considering the implementation of the upper layer protocol.

The traditional authentication scheme is based on the Shared secret key of both legal parties. The security of authentication and even the security of the whole network message transmission will depend on it. Meanwhile, the Shared secret key cannot adapt to the whole communication network and has limitations in application. The new authentication scheme is mainly based on Wyner eavesdropping model, which can provide a strong guarantee for the security authentication of network high level. In the physical layer authentication model shown in figure 3, Alice sends messages to Bob via wireless network. In order to verify its security and reliability, Bob needs to conduct identity authentication when receiving the messages, so as to confirm that the messages come from Alice rather than other malicious illegal users. Eve can eavesdrop on the message transmission between Alice and Bob in both active and passive ways in the eavesdropping channel.

![Figure 3. Physical layer security authentication model](image)

At present, the physical layer certification can be divided into four categories:

1. Authentication mechanism based on hardware radio frequency (RF) fingerprint

Kohno's team at Tohoku university in Japan and Capkun's team at the Swiss federal institute of technology in Zurich used the imperfections of the hardware to extract unique features of the device to come up with a certification scheme based on "RF fingerprints" [13,14,15]. Hardware RF fingerprint is also known as the fault of the transceiver device. The impossibility of cloning these defects makes the only interaction between the transceiver and the transceiver be confirmed. The mechanism can be divided into two categories: The first is based on the matching and interaction of radio signal transient characteristics when hardware switch on/off. The performance of authentication depends not only on the interference of noise in the channel, but also on the accuracy of feature separation and extraction. The other is based on the characteristics of the modulated signal.

Hardware RF fingerprint feature makes it face huge risk in imitate attack, due to the availability of RF fingerprint scheme, illegal wiretapping attack just repetition signal recognition, the low accuracy
and high cost of signal analysis in complex channel environment inevitably lead to the decrease of authentication performance, and the authentication scheme of hardware RF fingerprint is also limited by the application scenarios.

(2) wireless channel-based authentication mechanism
A team led by professor Trappe of the state university of New Jersey proposed a channel fingerprint-based authentication scheme based on the short-term invariance of channel characteristics and location. The spatio-temporal uniqueness of wireless channels which means that the corresponding CSI under different spatio-temporal conditions is generally different, which provides a new scheme for identity identification, which enables the physical layer authentication under stable conditions to make better use of this feature. However, due to the spatio-temporal correlation of CSI, channel fading, noise interference and propagation loss, CSI transformation in dynamic environment is relatively frequent, and the physical layer authentication relying only on CSI identification is no longer applicable. At the same time, some studies show that under the imitation attack model, when the distance between the eavesdropper and the legitimate sender is close, the CSI of the legitimate channel can be obtained, which increases the security risk of the authentication process.

(3) authentication mechanism based on signal watermarking
In order to save band resources and improve resource utilization, the Baras team of the university of Maryland proposed a digital watermarking technology based on physical layer. It is a digital watermarking technology that hides the authentication information of the application layer in the amplitude or phase information of the signal and transmits it together with the signal to the identity identification scheme of the receiver [16]. This scheme can improve the security of encrypted messages by controlling the density of watermark bits and disturbing the illegal eavesdroppers. However, the communication environment cannot be kept absolutely safe, so the watermark embedding process of signals is also risky, and the transmission may cause the waste of resources in high-risk communications environments such as battlefield networks.

(4) PHY-CRAM mechanism based on physical layer
Due to the limitations of previous physical layer authentication schemes, Shan et al., university of Michigan, took advantage of the characteristics of wireless channel to realize the security enhancement of identity authentication [23]. They used OFDM technology to set the shared key onto the subcarrier amplitude and proposed the authentication mechanism named "PHY-CRAM". In addition, "PHY-PCRAS", "PHY-CRAMR", "PHY-AUR" and other algorithms are all schemes for identity recognition by sending excitation response signals to each other according to communication models under different conditions. Since they can be used in dynamic channel environment without high cost consumption, they provide a new idea for physical layer security authentication at the present stage.

3.2. The physical layer encryption algorithm
The physical layer encryption algorithm is based on the physical security requirements, the network upper cryptography encryption method is applied to the physical layer. According to the information transmission mode of the physical layer, the encryption processing of the physical layer can be divided into three categories: channel coding/decoding encryption, signal modulation/demodulation encryption, and signal spread spectrum/demodulation encryption.

Encoding/decoding encryption refers to the encryption method applied after the message is encoded in the channel. It mainly depends on channel error code and key deviation to affect the attack implementation of non-cooperative parties. However, it can only be well applied in the coding scheme of block codes, while there are application restrictions in the coding scheme of soft decision such as Turbo code and convolutional code.
The modulation/demodulation encryption scheme mainly encrypts the signal constellation and the mapping process, controls the phase and amplitude of the signal through the encryption algorithm, improves the confusion degree of the signal constellation diagram, and interferes the demodulation recognition of the non-cooperative party. The unitary matrix protection algorithm can also be used to protect the encrypted signal from eavesdroppers.

Spread spectrum/de-amplification encryption scheme makes use of the characteristics of low detection and low interception of spread spectrum signals to combine spread spectrum and encryption at the information sending end, and the receiver uses the encryption sequence generated by the known key to complete the de-amplification and decryption operation of the signal, which can realize the synchronization of encryption and decryption and signal processing.
3.3. Physical layer security transmission

In the keyless security scheme based on the Wyner model, the redundancy of the system airspace is utilized to design the system security capacity optimization scheme based on Artificial noise (AN), relay node collaboration, beamforming, large-scale MIMO and other technologies.

(1) AN

The main idea of AN assistive technology is to improve the safe transmission capacity by adding appropriate noise to the message to reduce the quality of eavesdropping channel.

Because the eavesdropping channel and the legal channel are generally different, there exists certain differences in the value of the space. In order to make the noise only to the eavesdropping channel interference will not affect the normal transmission of the legal channel, Goel.S and Negi. R proposed adding artificial noise to the null space of the legitimate channel, and the noise distributed in the "value space" of the eavesdropping channel would interfere with the eavesdropping process [7]. At the same time, the added noise would also avoid interfering with the normal message transmission, so as to achieve the purpose of worsening the eavesdropping. However, CSI needs to be accurately understood through channel interference selection, which highlights the limitation of this scheme in practical application.

In a communications system, set the main channel coefficient $h^H \in C^{b \times N}$, eavesdropping channel coefficient $g^H \in C^{c \times N}$, AN $z \in C^{b \times N}$ meet the following requirements:

$$h^H z = 0$$

The sending signal at the source is expressed as:

$$s = x + z$$

$$z = Wn$$

In the formula, $x$ is the signal bearing the secret message, which meets the power limit $E|x|^2 \leq P$, $W$ is the beamforming matrix, $n$ is the noise vector of the complex gaussian distribution generated randomly.

Then the signals of both sides can be expressed as:

$$y_b = h^H s + n_b$$
$$= h^H x + h^H z + n_b$$
$$= h^H x + n_b$$

$$y_c = g^H s + n_c$$
$$= g^H x + g^H z + n_c$$
$$= g^H x + g^H Wn + n_c$$

In the formula, $n_b, n_c \sim CN(0, \sigma^2)$ is the random noise of the channel.

The signal-to-noise ratio of both sides can be expressed as:

$$\gamma_b = \frac{\|h^H\|_{\infty}^2 P}{\sigma^2}$$

$$\gamma_c = \frac{\|g^H\|_{\infty}^2 P}{\sigma^2 g^H W^H g + \sigma^2}$$

The accessible security rate of the communication system can be expressed as:

$$R_s = \left[ \log \left( 1 + \frac{\|h^H\|_{\infty}^2 P}{\sigma^2} \right) - \log \left( \frac{\|g^H\|_{\infty}^2 P}{\sigma^2 g^H W^H g + \sigma^2} \right) \right]$$

Thus, with the support of AN assistive technology, the secret transmission rate can still be greater than zero, and the secure transmission can be realized under the condition that channel quality is not dominant.
(2) Beam Forming

Different from AN assistant technology, the core of beamforming technology is to make the signal sent in the null space of the eavesdropping channel, so as to realize the zero reception of the eavesdropping party to the secret message, namely:

$$g^H w = 0$$ (14)

In the formula, $w$ is the beamforming vector.

Beamforming, as one of the precoding technologies, has been widely used in MIMO communication systems and collaborative networks. Meanwhile, due to the difficulty in acquiring the eavesdropping channel CSI and the high sensitivity between CSI and $w$, most of them have certain limitations in practical application. Based on this situation, Pei Y et al. analyzed and designed some known systems of CSI in 2011. In 2012, Lu M proposed a joint scheme to reduce CSI sensitivity and system complexity combined with multi-user MIMO system.

(3) Relay coordination

The scenarios of B5G and 6G application in the future have gradually made the integration of heaven and earth become a reality. The communication distance of wireless network has been significantly improved, and the limitation of transmitting power has made people seek for new long-distance transmission methods. Therefore, cooperative relay communication emerges as The Times require. The relay nodes' processing methods for signals can be divided into three categories: forwarding, interference and cooperation. Forwards are divided into two ways: one is the relay node will forward the received signal after demand amplification appropriate to the target node; the other is that relay node decode the received signal, then forward the target node after coding modulation based on the requirements, namely amplification forward (AF) and decode forward (DF). Different forwarding methods affect the security capacity of the system. AF reduces the probability of eavesdropping without decoding, so it can more effectively improve the security rate of the system compared with DF. In 2007, Oohama Y made the first research and analysis on the forward and relay eavesdropping channel model. In 2010, He X pointed out that the rate of system security still can be improved even if the relay node is not credible, and designed the $w$ of hacking user communication system for 3 relay schemes of AF, DF and Cooperative Jamming (CJ).

4. The challenges that physical layer of battlefield networks still faces

At present, the research on the battlefield network security problem has made some achievements, but the network edge security issues are still needed to consider, namely, the distance between both sides in the battlefield environment is relatively close, making the network signal reconnaissance intercepted easier. At the same time, there are many types of devices in the network, and all kinds of terminals have security vulnerabilities. Even intelligent terminals have hard-to-find vulnerabilities, which may provide the enemy with the opportunity to invade the network.

Although existing technologies can be used to improve network bandwidth, with limited channel resources, the move of sensing the use of wireless channels and dynamically allocating idle resources to online users can improve network bandwidth, but frequent channel switching also brings security problems in authentication, tactical networks may face replay attacks from the enemy, and the vulnerability of battlefield network physical layer is the focus that needs to be solved urgently.

The physical security technology application in the actual battlefield network still faces many challenges, the current study is under the background of passive eavesdropping. However, the attacks in the battlefield network are persistent and varied, and the vulnerability of physical layer security scheme is obvious when facing the attack of active eavesdropping party. Therefore, it is urgent to study the physical layer security scheme to deal with active attackers.

Physical layer security has not been well solved in the initial authentication problem, which still needs the assistance of traditional cryptography algorithms. How to use the characteristics of the physical layer to achieve real keyless authentication security still remains to be explored.

For now, physical security system has not yet reached the height of replacing the existing security system, and can only be used as a supplementary means to effectively ensure network security.
Acknowledgments
This work was financially supported by cooperative fund for state key laboratories (KX162600022).

References
[1] Shannon C E. Communication Theory of Secrecy Systems[J]. The Bell System technical journal, 1948, 28(4):656–715.
[2] Wyner, A. D. The Wire-Tap Channel[J]. Bell System Technical Journal, 1975, 54(8):1355-1387.
[3] Maurer, U. M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3):733-742.
[4] He X, Yener A. Cooperation With an Untrusted Relay: A Secrecy Perspective[J]. IEEE Transactions on Information Theory, 2010, 56(8):3807-3827.
[5] Dong L, Han Z, Petropulu A P, et al. Improving Wireless Physical Layer Security via Cooperating Relays[J]. IEEE Transactions on Signal Processing, 2010, 58(3):1875-1888.
[6] Pei Y, Liang Y C, Teh K C, et al. Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information[J]. IEEE Transactions on Signal Processing, 2011, 59(4):1683-1693.
[7] Goel S, Negi R. Guaranteeing Secrecy using Artificial Noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6):2180-2189.
[8] Xiao L, Greenstein L, Narayan M. Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication[J]. Computer Science, 2007:4646-4651.
[9] Hao, Peng, Wang, et al. Physical-Layer Authentication for Wireless Security Enhancement: Current Challenges and Future Developments[J]. IEEE Communications Magazine: Articles, News, and Events of Interest to Communications Engineers, 2016.
[10] Liu J, Wang X. Physical Layer Authentication Enhancement Using Two-Dimensional Channel Quantization[J]. IEEE Transactions on Wireless Communications, 2016, 15(6):1-1.
[11] Rahman M M U, Abbasi Q, Chopra N, et al. Physical Layer Authentication in Nano Networks at Terahertz Frequencies for Biomedical Applications[J]. IEEE Access, 2017:1-1.
[12] Bernard S, Clément Chatelain, Sébastien Adam, et al. The Multiclass ROC Front method for cost-sensitive classification[J]. Pattern Recognition, 2016, 52(C):46-60.
[13] Kohno T, Brodico A, Claffy K C. Remote Physical Device Fingerprinting[J]. IEEE Transactions on Dependable & Secure Computing, 2005, 2(2):93-108.
[14] Danev B, Capkun S. Transient-based Identification of Wireless Sensor Nodes[C]. International Conference on Information Processing in Sensor Networks, San Francisco, 2009: 25-36.
[15] Danev B, Zanetti D, Capkun S. On Physical-layer Identification of Wireless Devices[J]. ACM Computing Survey, 2012, 45(1): 1-29
[16] Yu P L, Baras J S, Sadler B M. Physical Layer Authentication [J]. IEEE Transactions on Information Forensics & Security, 2008, 3(1):38-51.
[17] Wen H, Ho P H, Gong G. A Novel Framework for Message Authentication in Vehicular Communication Networks[C]. in Proceedings of Global Telecommunications Conference, Honolulu, 2009: 1-6.
[18] Wen H, Wang Y, Zhu X, et al. Physical Layer Assist Authentication Technique for Smart Meter System[J]. Iet Communications, 2013, 7(7): 189-197.
[19] Wen H. Physical Layer Assisted Authentication for Wireless Sensor Networks[J]. IET Information Security, 2011, 4(4): 390-396.
[20] Wen H, Ho P H. Physical Layer Technique to Assist Authentication based on PKI for Vehicular Communication Networks. [J]. Kiex Transactions on Internet & Information Systems, 2011, 5(2):440-456.
[21] Zhang J, Wen H, Song H, et al. Using Basis Expansion Model for Physical Layer Authentication in Time-Variant System[C]. IEEE Communications and Network Security(CNS). Philadelphia, 2016:348-349.
[22] Xiao L, Greenstein I J, Mandayam N B, et al. Fingerprints in the Ether: Using the Physical Layer
for Wireless Authentication[C]. IEEE International Conference on Communications. Glasgow UK, 2007:4646-4651.

[23] Shan D, Zeng K, Xiang W, et al. PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9):1817-1827.