Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 1230387, 10 pages
http://dx.doi.org/10.1155/2016/1230387

Review Article

Information Security of PHY Layer in Wireless Networks

Weidong Fang,[1,2] Fengrong Li,[2] Yanzan Sun,[1] Lianhai Shan,[3,4] Shanji Chen,[5] Chao Chen,[5] and Meiju Li[5]

[1]*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444, China*
[2]*Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 201899, China*
[3]*Shanghai Internet of Things Co., Ltd., Shanghai 201899, China*
[4]*Shanghai Research Center for Wireless Communications, Shanghai 200335, China*
[5]*College of Physics and Electronic Information Engineering, Qinghai University for Nationalities, Xining, Qinghai 810000, China*

Correspondence should be addressed to Fengrong Li; lifengrongsim@mail.sim.ac.cn

Received 2 December 2015; Accepted 16 February 2016

Academic Editor: Fei Yu

Since the characteristics of wireless channel are open and broadcasting, wireless networks are very vulnerable to be attacked via eavesdropping, jamming, and interference. As traditional secure technologies are not suitable for PHY layer of wireless networks, physical-layer security issues become a focus of attention. In this paper, we firstly identify and summarize the threats and vulnerabilities in PHY layer of wireless networks. Then, we give a holistic overview of PHY layer secure schemes, which are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based. Along the way, we analyze the pros and cons of current secure technologies in each category. In addition, we also conclude the techniques and methods used in these categories and point out the open research issues and directions in this area.

1. Introduction

With the development of information technology, wireless networks have evolved from initial single networks into multimode, multistandard networks (3G, 4G, wireless sensor networks, ad hoc networks, etc.), which made mobile users convenient to access. However, because of broadcast nature of wireless communication, dynamic topology, mobility, signal channel instability, and so forth [1], they are also vulnerable to various security threats and attacks such as DoS (Denial of Service), counterfeiting, tampering, leakage, interference, network flooding, eavesdropping, and traffic analysis [2]. Particularly, with the popularity of intelligent terminals, some bad information, such as obscenity information, viruses, and Trojans, becomes more and more widespread [3]. This bad information not only occupies lots of user's traffic, but also endangers the privacy of users. Therefore, the issue of information security has become a key challenge to the development of wireless networks.

To solve the issues of information security threats and attacks in wireless networks, the traditional technologies mainly focus on encryption/decryption [4], trust management [5, 6], authentication [7], and so forth. However, for complex structure of wireless networks, only depending on encryption/decryption method is not enough to ensure the information security of wireless networks. For example, it cannot eliminate the issues of eavesdropping and interference in PHY layer. Fortunately, with the emergence of new technologies, some novel security technologies can overcome the above drawbacks in PHY layer, such as cooperative techniques [8, 9] and structured signaling schemes [10]. For one thing, these technologies can make full use of the characteristics of the wireless channel for information transmission without high computational complexity. For another thing, they can also eliminate or mitigate the risks of intentional or unintentional security attacks and interferences by means of spread spectrum, random parameter, and so on.

Although Shannon had put forward the Communication Theory of Secrecy Systems in 1948, security technologies of PHY layer were seldom paid attention to by researchers in recent years. In this paper, the threats and vulnerabilities in PHY layer of wireless networks are identified first. The rest of this paper is organized as follows: attack technologies in PHY layer are described and summarized in Section 2. Section 3 illustrates classification of the existing secure schemes. Various secure schemes are analyzed in Section 4. Finally, conclusions are made in Section 5.

2. Attacks to PHY Layer

PHY layer of wireless networks is at the bottom of the network, which is mainly responsible for frequency selection, carrier frequency generation, and signal detection and modulation. Meanwhile, it receives wireless signals from the air interface and transmits the demodulated data stream to the upper layer. Because of PHY layer transmission characteristics, major types of physical attacks include interference, jamming, eavesdropping, and traffic analysis. In general, these attacks fall into two categories: active attacks and passive attacks.

2.1. Active Attacks. Active attacks mainly include interference and jamming. These two kinds of active attacks are implemented similarly in principle by broadcasting interference signals on some specific frequency bands. The differences between them are the different objectives they attack. Jamming attacks by means of continuing occupying the channel cause the transmitter failure. Interference attacks by deteriorating the legal signal result in the receiver failure. Most of the jamming attacks are malicious attacks, and interference suffers not only from hostile attackers, but also from other users around the signal over the same channel or environmental effects. For example, a large number of sensor nodes are randomly distributed in wireless sensor networks (WSNs), and through multihop transmission for communication, signal interferences of transmission to other nodes are very easy.

According to the difference of jamming attack technologies, the common jamming can be divided into spot jamming, sweep jamming, barrage jamming, and deceptive jamming [11]:

(1) *Spot Jamming.* It mainly focuses on single frequency jamming, by transmitting high enough power to cover the original signal. It is simple and widely applied.

(2) *Sweep Jamming.* The attacker frequently hops from one frequency to another. The advantage is that it can cover a wide range of frequencies and be an effective attack to frequency hopping technology. However, it cannot cover multiple frequencies at the same time.

(3) *Barrage Jamming.* It can attack a large range of frequencies at the same time and cause great impact on the user communication under its coverage. Due to limitations of transmission power, the wider the frequency it attacks, the weaker its jamming ability is.

(4) *Deceptive Jamming.* The attackers transmit forged data packets in the network and make the user receive them as normal data packets. This kind of jamming is not easy to be detected and is very destructive.

The attacker also has two types of interference methods: active interference and passive interference [12]. Active jamming can be further divided into sustained interference, random interference, and on-demand interference [13]:

(1) *Sustained Interference.* It refers to the attacker continuously sending interference signal, thus affecting user normal communication. Its purpose is long-term occupation of the user channel so that the channel could keep busy. Meanwhile, it interferes with the ongoing data transmission and also destroys the transmitting message.

(2) *Random Interference.* It refers to the attacker randomly interfering with the user. The interference time and cycle are uncertain. Compared with the sustained interference, it can effectively save the attacker's energy consumption and lead to a great impact on the multihop WSNs.

(3) *On-Demand Interference.* It is to maintain idle state if the channel is idle. Otherwise, the signal interfered with will be transmitted to interrupt ongoing transmission and information hiding technique is implemented. Direct Sequence Spread Spectrum (DSSS) has low power spectrum density of transmitted signal. Its signal spectrum is similar to noise signal so that it could effectively enhance the information hiding.

The signal bandwidth of interference attacks and jamming attacks can also be classified as narrowband and wideband. The frequency range interfered with is usually narrow in narrowband attack. However, with the development of 3G and 4G technology, the bandwidth of interference and jamming could be up to several megahertz.

2.2. Passive Attacks. Passive attacks are mainly divided into two categories: eavesdropping and traffic analysis. The two attacks are caused by the fundamental characteristic of wireless medium, namely, broadcast. The broadcast nature of wireless communication makes it difficult to shield transmitted signals from unintended recipients, while these legal or illegal users within the transmission range analyze and utilize wireless broadcast signals.

Eavesdropping on the communication information of other users leads to information disclosure problems and can be easily achieved due to open access of wireless channels. Traffic analysis refers to an attacker according to changes in the flow of information in the network, some attacks prompted through extracting information from ongoing transmission. For example, an attacker can judge the base station position according to the changes of network traffic in wireless sensor networks. In a word, the attacker interferes with or captures the base station, which leads to paralysis of the entire wireless sensor networks.

3. Results and Discussion

The theoretical basis behind the concept of information security in PHY layer security transmission, which builds on Shannon's notion of perfect secrecy in 1949 [13], was laid by Wyner [14] and then expanded by Csiszár and Korner [15]. In [16], Shannon proved that there exist channel codes guaranteeing the security of the information if secret key length is longer than or equal to the transmission of information. Wyner proved that source and destination can securely transmit information when the legitimate user's channel condition is superior to the eavesdropper.

Nowadays, with emergence of a variety of novel technologies, many security technology methods in PHY layer are put forward for SIMO (single-input multiple-output), MIMO (multiple-input multiple-output), and relay channel. These schemes have possibly increased the potential secrecy capacity and enhanced PHY layer security using these technologies, which to a certain extent can increase the channel capacity of the networks [17]. Subsequently, the system can enhance the PHY layer security by combining with some other PHY layer security technologies. In [18], Barcelo-Llado et al. proposed the amplify-and-forward compressed sensing (AF-CS) framework to assess the physical-layer secrecy performance when malicious eavesdropping nodes are listening. According to the different types of technology, this section will introduce some common and novel PHY layer security methods from the view of the spatial domain, frequency domain, and time domain [19] and finally conclude security technologies from the point of PHY layer attacks.

3.1. Spatial Domain Technologies. Spatial domain technologies consist of directional antenna, beamforming, and some improved technologies based on beamforming. Through suitable antenna technology of avoiding signal interference or realization of the randomization of the channel parameters, the system can achieve anti-interference and antijamming and resist wiretap.

3.1.1. Directional Antenna and Beamforming Technology. Directional antenna has high transmission power in one or more specific directions with the characteristics of long transmission distance and wide geographical coverage. When the signals were received, the directional antenna made the main beam align with the direction of useful information and the nulling align with the interfering signals. Thereby, the directional antenna could reduce or eliminate the interference signal and achieve the purpose of interference and jamming. At the same time, it avoids or degrades the interference and achieves anti-interference and antijamming goal [19]. Compared to unidirectional antenna, directional antenna can significantly enhance the antijamming performance [20]. It has smaller energy consumption than unidirectional antenna. Meanwhile, in the case of lower transmit power and equal equivalent isotropically radiated power in receiver, the directional antenna can effectively reduce the probability of being detected. Hence, the directional antenna has more invisibility in an adverse environment [21]. With directional antenna miniaturization and gain performance improvement, it has also been widely used in various wireless mesh networks, ad hoc networks to enhance its performance [22]. The directional antennas can be a good solution to network interference and connectivity issues; it has higher spatial multiplexing and farther transmission distance. However, the cost of directional antenna is relatively higher. Furthermore, the breakthrough of antenna polarization and gain are to exploit the characteristic of complex wireless channel, such as fading or noise.

Beamforming also is a specific alterable directional antenna, named smart antenna, which is composed of a multiantenna array. It can realize the transformation of the antenna beam direction through configuration of number of the antennas, element spacing, and geometry. The antenna radiation direction towards the legitimate receiver could avoid interference [23]. Moreover, because transmitting signal is intense and concentrated, it enhances the ability to resist the eavesdropping [24], jamming, and cross talk among multiple users. However, it cannot apply to some energy limited networks because its power consumption is far higher than the directional antenna using multiantennas. Reference [25] designs joint information beamforming and jamming beamforming to protect both transmit security and receive security for a full-duplex base station. Chen et al. proposed multiantenna secure relaying technologies to aid wireless physical-layer security [26]. The proposed large-scale multiple-input multiple-output (LS-MIMO) relaying technology can solve the problem with short-distance interception under adverse conditions.

At present, smart antenna has been widely applied in 3G and 4G. It also makes the communication rate improve while effectively solving multiuser communication interference issue. Besides, beamforming not only uses multiple antenna arrays, but also uses the cooperative relay for some multinode cooperative relay networks [27].

3.1.2. Random Parameters and Random Antenna Technology. Random parameter is developed based on the beamforming. Random transmission antenna weight causes randomization of received eavesdropper's signals and the trained legitimate users are not affected through channel preestimation. It exploits the redundancy of transmit antenna arrays for deliberate signal randomization. The multiplication of channel parameters and default random coefficient is fixed value, and demodulation is not affected [28]. This randomized array transmission scheme guarantees wireless transmissions with inherent low probability of interception (LPI) via proving the indeterminacy of the eavesdropper's blind deconvolution.

The random antenna is similar to the random parameter. The difference between random antenna and random parameter is that the random antenna can achieve the randomness of the receiver signal, while the random parameter is realized by the random weighting coefficient. The random antenna method is most used in multiple-input and multiple-output systems. In the process of signal transmission, the transmitter transforms the transmitting antenna continuously and randomly, so as to realize the channel randomization between the transmitter and the legal or illegal users [29]. Hong et al. presented a secure multiple-input single-output (MISO)

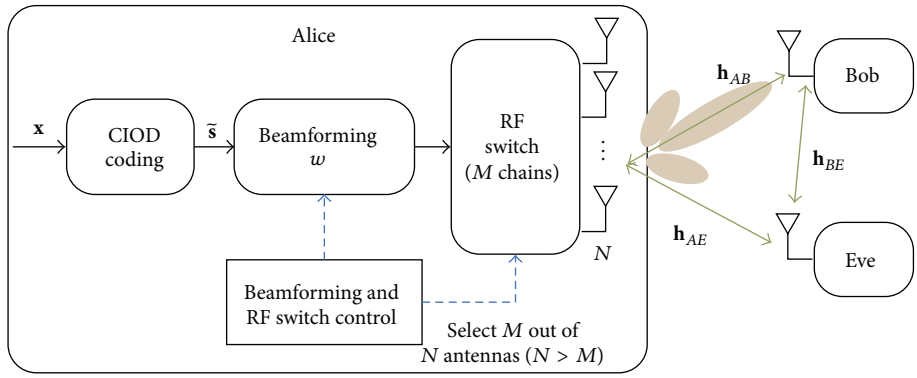

Figure 1: System model of ASM with CIOD.

wireless transmission scheme based on a combination of the random Antenna Subset Modulation (ASM) scheme and Coordinate Interleaved Orthogonal Designs (CIOD) [30]. The proposed scheme enjoyed both diversity and array gains to guarantee against potential eavesdropping. The system model was shown in Figure 1. Valliappan et al. proposed ASM scheme to take advantage of massive antenna arrays at mm-wave frequencies [31]. In ASM, the radiation pattern of the array was modulated at the symbol rate to achieve direction dependent data transmission. ASM provided security by introducing additional points in the constellation that appear to be effectively random to an undesired receiver. Similar to the random parameters, the legitimate user after training channel can smoothly demodulate the signal, but the received signal of eavesdropper has confusing superposition. In addition, the allocation of the antennas number can also enhance performance [17]. However, low signal utilization is the inherent weakness of this technology due to its use of multiple transmit antennas.

3.1.3. Artificial Noise Technology. Artificial noise acquires higher secrecy capacity of legitimate channel than that of the eavesdropping channel when the Channel State Information (CSI) of the legitimate channel is better than the eavesdropping channel [14] or deteriorates the eavesdropping channel or optimizes the legitimate channel. The transmitter utilizes some of the available power to produce artificial noise, such that only the eavesdropper's channel is degraded. At present, the common method used is artificial noise aided beamforming.

The initial research of artificial noise assisted beamforming method was proposed by Goel and Negi [32], which used multiantenna array to develop a "zero space." Then, it introduced noise signal into zero space of the legitimate channel, which made the legitimate receiver extract the information via noise filtering, but the illegal users are impacted by these introduced noise signals. In recent years, the researchers have carried out many subsequent studies and optimization based on this method [33, 34]. For example, ensuring the quality of service, [35] used the limited indicator signal to interference plus noise ratio (SINR) to assist artificial noise, and to achieve energy saving and secrecy capacity improvement, [36] extended the artificial noise from the null space to signal space and achieved better performance. Deng et al. presented analog network coding systems based on artificial noise to enhance physical-layer security [37]. In this scheme, the relay node selected part of antennas from its total antennas as the received reference signal in broadcast phase and then derived the beamforming matrix and artificial noise vector from the equivalent channel fading matrix. The simulated results showed that the proposed scheme outperforms classical beamforming scheme. Cepheli and Kurt extended the existing artificial noise techniques to MIMO-OFDM (Orthogonal Frequency Division Multiplexing) and proposed a spatiotemporal selective artificial noise approach to cause extensive channel estimation error for eavesdroppers [38]. However, comprehensive technology is still high in practical applications, and there are still many issues to be solved.

3.2. Frequency Domain Technologies. Frequency domain technology especially spread spectrum is the most applied PHY defense technology. It usually reduces or avoids the interference of the carrier frequency band by using the wide range and variability of carrier frequency. The concept of spread spectrum was first introduced by Nicola Tesla, and then spread spectrum was real studied in the U.S. Military. Because of its good antijamming property, it has been applied in the military field and gradually applied to civil area until the beginning of the last century in the 1980s [39].

The principle of spread spectrum is to modulate the transmitted signal with a pseudorandom sequence, while the receiver then demodulates the signal using the same sequence to get the original signal. In this process, the signal noise ratio (SNR) is increased, and the influence of the interference is also reduced.

According to the method of extending narrowband signal, spread spectrum can be divided into the following categories: FHSS (Frequency Hopping Spread Spectrum), DSSS, THSS (Time Hopping Spread Spectrum), CSS (Chirp Spread Spectrum), and the combination of these techniques. We majorly study FHSS and DSSS, which have better anti-jamming performance than others.

The principle of DSSS modulation is that the sender modulates signal with a pseudo noise sequence on a broad band. The modulated signal spectrum is similar to the noise sequence, which decreases the interference effects

and enhances the concealment of the signal. The receiver demodulates the spread signal by the same sequence. Then, the spectrum density of the useful signal is increased and the spectrum density of the interference noise is very small. It finally gets the original signal by filtering most of the noise. In this process, the impact of narrowband interference will be very limited because of its wide bandwidth. There also are many hybrid DS/FH DSSS technologies, which can get better performance in the face of jamming, multiuser interference, and channel fading [40, 41].

The FHSS mentions that the sender uses a set of pseudorandom code sequences to realize the carrier frequency hopping fast in different frequency and the sequence of hopping frequency (i.e., code sequence) only known between the sender and receiver. The recipients can use the sequence to despread the received signal [42]. On the one hand, the security of FHSS depends on the complexity of frequency hop pattern. Leukhin et al. presented a new method for constructing CDMA sequence sets with the linear complexity of the Legendre sequences and formed new frequency hop patterns [43]. However, the freshness of the hopping sequences and terminals synchronization were difficult to obtain [44]. On the other hand, the FHSS can hop in a wide range so that it has stronger ability to resist interference of the narrowband signal. Otherwise, it increases the hop rate for the more intelligent tracking jamming to improve the anti-interference ability [45]. The higher the frequency jumps, the stronger the antijamming performance of tracking. The jump of the carrier frequency can affect the attacker's monitoring of the signal flow and can better resist the traffic analysis attack. However, with FHSS of different frequency fast hopping, the sender and receiver strictly need synchronization requirements. Based on the OFDM framework and the secure subcarrier assignment algorithm, Hao et al. introduced collision-free frequency hopping (CFFH) to achieve high information capacity through collision-free multiple access [46]. The proposed CFFH could resolve the strict synchronization limitation and ensure that each user still transmitted through a pseudorandom frequency hopping scheme. CFFH could maintain the inherent antijamming and anti-interception security features of the conventional FH system.

In addition, except for the good performance of the fast frequency hopping (FFH), adaptive frequency hopping technology can effectively resist the intelligence and sweep frequency jamming via adaptive carrier frequency, power [47, 48]. In [49], the authors put forward a new algorithm with blacklisting which can generate frequency hopping sequences (FHSs) in the presence of interference without regeneration overhead and maintains optimal/near-optimal properties with different channel number from one original sequence. A random spread spectrum based wireless communication called Frequency Quorum Rendezvous (FQR) is described in [50]. FQR coordinates two random hopping sequences to prevent eavesdropping and active attacks and exploits a quorum system that is a tool for increasing the availability and efficiency of replicated services in distributed computing. Chen et al. introduced a differential jamming rejection (DJR) receiver in FFH M-ary Frequency Shift Keying (MFSK) systems with worst-case band multitone jamming (MTJ) [51]. Based on detecting frequency spectrum difference in forward-backward time slot while the FFH/MFSK signal arrives at receiver, the proposed receiver implemented differential suppression of worst-case band multitone jamming without any side information. The FHSS has better antijamming performance and lower bit error rate (BER). Because hardware requirements of FHSS are lower than DSSS, FHSS can be applied to many low hardware networks, and the data transmission rate is as high as DSSS.

3.3. Time Domain Technologies. Time domain is the main technique of channel coding, which was firstly studied by Shannon [16]. Shannon in his channel model proved that encoded information can be in the presence of noise which can realize the secure transmission by the channel capacity of arbitrary rate below. In addition, channel coding can play an essential role in correcting the transmission of information using addition of some check code. The receiver can utilize these symbols to check whether transmission information has error or not and correct error timely to reduce the influence of jamming attacks. Nowadays, there are many channels coding schemes such as convolution codes [52], BCH (Bose, Ray-Chaudhuri) [53], Turbo [54], LDPC (Low-Density Parity Check) code [55, 56], and soft decode-compress-forward scheme [57].

In addition, Kwak et al. introduced a binary numeral system called Yarg code [58], which can be used as a QAM (Quadrature Amplitude Modulation) symbol mapping scheme to map a sequence of multiple binary bits to the symbols of QAM constellation. The characteristic of this Yarg code was different from the QAM symbol mapping scheme Gray code. That was due to the fact that the objective of Gray code [59] was to minimize the required SNR that achieves the target BER, but the objective of Yarg code was to minimize the security gap. Through researching the usage of nonsystematic codes based on scrambling matrices, Baldi et al. estimated the security gap over the AWGN (Additive White Gaussian Noise) wiretap channel as a measure of the effectiveness of several transmission schemes [60]. This scheme used puncturing techniques to reduce the security gap between the authorized and unauthorized channels. Hence, the proposed security gap could be further reduced by using nonsystematic codes and scramble information bits within the transmitted codeword.

Among them, LDPC is a hot research channel code after Turbo and has been widely used in military, civil, commercial, and other fields due to its good error correction. Besides single encoding, the joint coding is also used. For example, the downlink and uplink of the communication use different coding or joint source channel coding. The video transmission and some high-speed network have achieved good results. Taieb and Chouinard proposed a physical-layer coding scheme based on nonsystematic Rate Compatible Low-Density Parity Check (RC-LDPC) codes to secure communications over the Gaussian wiretap channel [61]. In the coding scheme, a finer granularity rate compatible code was used to increase the eavesdropper decoding failure rate; meanwhile, a rate estimator based on the wiretap channel capacity was used to reduce decoding delays. The proposed

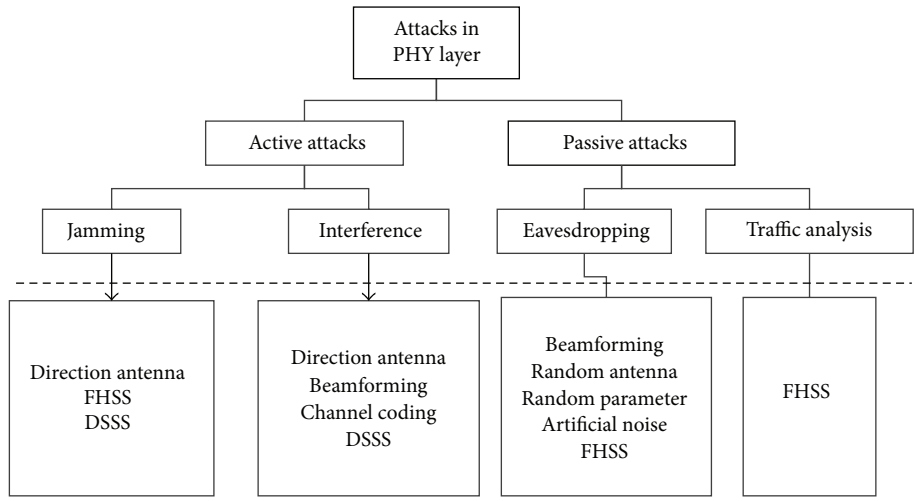

Figure 2: Attacks and defense in PHY layer.

coding scheme could improve security of PHY layer in terms of error amplification, and negative security gaps could also be achieved at the PHY layer. Yang et al. proposed a scheme where LDPC code and artificial noise were combined in wiretap channel to enhance the security in physical layer [62]. In the scheme, artificial noise was designed such that it spans a null space at the legitimate receiver but acts as random interference at the eavesdropper receiver and is added at the transmitter using precoding. A scrambling matrix was designed and used in LDPC code to reduce the outage probability of the wiretap channel deduced. Baldi et al. researched the reliability and secrecy performance achievable by practical LDPC codes and proposed a code optimization algorithm to design irregular LDPC codes, which was able to approach the ultimate performance limits [63]. Zhang et al. proposed a concatenated coding scheme based on polar codes and LDPC codes for the AWGN wiretap channel. They analyzed the BER performance of the proposed coding scheme through the density evolution (DE) and then investigated the security gap that the proposed coding scheme could achieve. Finally, a transmission scheme using rate compatible Polar-LDPC codes was presented to adapt to the dynamic environments [64]. However, the computational complexity of the channel code is a critical problem. In the practical application, the channel coding can also be considered as the flexible optimized coding rate and algorithm, which makes the channel coding powerful.

This section mainly concludes a number of common PHY security technology and development applications in the perspective of the security defense. The category of PHY attack is listed in Figure 2.

4. Analysis of Security Technology and Future Issues in PHY Layer

In this section, the security technology in PHY layer is analyzed and compared, and then some very innovative trends for future research are identified.

As mentioned above, the secure techniques of PHY layer could effectively defend against the interference, jamming, and eavesdropping attack. In this section, we analyze, compare, and summarize the previous secure techniques of PHY layer in wireless networks, through the research of the factors affecting the technical characteristics, ability to defend against attacks, and complexity which is illustrated in Table 1, with (—) signifying no consideration or weakness.

From Table 1 secure techniques are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based. Strictly speaking, random parametric technique does not act as defense against eavesdropping attacks from space but relies on randomization of weighting coefficients to achieve the eavesdropper's received signal randomization. However, because there are the same beamforming technology-based and many similarities of representation formula, we compare the random parameter with random antenna in Section 3.

Research field of physical security, especially in mobile devices, becomes increasingly widespread in recent years. Much effort has been (and is being) made worldwide for providing secrecy in the absence of complete or perfect channel knowledge of the parties. As shown in Table 1, we could claim that secure techniques defending against eavesdropping attacks have mainly three types:

(i) *Directional Transmission Technology (Beamforming and Directional Antenna).* It can only enhance the resilience of the eavesdropping attack to some extent but is not able to effectively eliminate the threat from eavesdropping attacks. However, with the development of antenna technology, defensive performance could gradually be improved.

(ii) *Random Parameters, Random Antennas, and FHSS.* Through randomization of weighting coefficients, channel parameters, and carrier frequency, an eavesdropper cannot effectively demodulate the correct information. These secure techniques have a high ability to resist eavesdropping.

Table 1: Comparison of PHY layer's security technique in wireless networks.

Secure technique	Type	Technical characteristics	Ability to defend against eavesdropping attacks	Ability to defend against jamming attacks	Ability to defend against interference attacks	Complexity
Directional antenna	Spatial domain	Increased receive gain in particular direction of space	Low	Medium	Low	Low
Beamforming		Superimposed multiantenna signal	Medium	—	Low	High
Random antennas		Increased channel randomness	Higher	—	—	High
Artificial noise		Increased channel diversity	High	—	—	High
Random parameters	—	Increased signal randomness	Higher	—	—	High
FHSS	Frequency domain	Fast hopping of carrier frequency	Higher	High	—	Medium
DSSS		Increased bandwidth	—	Higher	Medium	Medium
Channel coding	Time domain	Powerful error correction capability	—	—	High	Low

(iii) *Artificial Noise*. It relies on adding artificial noise to increase channel diversity in the channel, make eavesdropping channel quality far worse than legitimate channel quality, impact eavesdropper's information demodulation.

In general, the latter two technologies rely on the unknown of legitimate channel's CSI information for eavesdroppers. Thereby, the eavesdroppers could not correctly demodulate the signal information. Artificial noise and random parameters are developed based on the beamforming, which enables users to track multiple directions. Therefore, accurately tracking user location and selecting the best transmission channel are an important research direction of the beamforming technology. At the same time, large-scale application of smart antenna technology is required to have low cost and complexity and new development of beamforming technology is another research direction. The application implementation of random parameters and artificial noise is a difficult issue in the research. Random antenna technology achieves data confidentiality of the eavesdropper by array antenna redundancy. However, this technology caused low signal utilization and it cannot guarantee the security of the information if the number of antennas of the eavesdropper is larger than those of itself. How to improve the signal utilization and enhance the signal confidentiality is the promising issue, which can make it have a wide range of applications. Spread frequency and directional antenna are mainly technologies that defend against jamming attack. DSSS and FHSS have similar characteristics. Their frequency ranges are wide. To defend against jamming attack, the former depends on the extension of spectrum, while the latter relies on the carrier frequency hopping. The former has a higher transmission rate, and complexity of its hardware implementation is also higher. The directional antenna with high antenna gain is suitable for long distance signal transmission, and it is the jamming avoidance in space. Therefore, Therefore, the high-gain directional antenna is one of the important research directions for defending against jamming attack.

For jamming attack, directional antenna and beamforming mainly depend on the orientation of their transmission signals to reduce interference. Then, the DSSS signal is dispread by the spread signal to achieve the low noise density spectrum, so that it has a strong attack on the interference resilience. Nevertheless, the channel coding and the former are not the same type of technology. It corrects the interference receiving code word based on powerful error correction capability. In a communications system, there are a wide variety of conflicting design tradeoffs. If channel coding technology is used to enhance the physical-layer security in the WSN and ad hoc networks, it will provide guidelines for engineers to balance between complexity and security. Nowadays, the research demonstrates that optimization of H matrix in LDPC can effectively reduce the computational complexity, which seems to be the relevant tradeoff. In general, the directional antenna and the beamforming strongly depend on the hardware; moreover, the channel coding relies on complex calculations to achieve the error correction. Since the channel coding's ability is better than the directional antenna and the beamforming ability in defending against the interference attack, it is widely used in a variety of information transmissions.

5. Conclusions

We notice that a few researchers focus on the information security of PHY layer in wireless networks. In this paper, we firstly research the attacks of PHY layer in wireless networks.

From three aspects of the spatial domain, frequency domain, and time domain, previous secure techniques are described. However, the secure techniques of spatial domain have to face the implementation complexity and energy consumption. Otherwise, the implementation of PHY layer's information security requires larger storage spaces and more powerful computing capabilities and even requires additional hardware units.

In the current field of wireless communication, major secure techniques could be applied to defend against interference and jamming attacks. Defense against eavesdropping attack mainly depends on data encryption technology of upper level. Mostly novel security techniques of PHY layer are still in theoretical research stage; how theoretical research results in practical applications is one of the hotspots for future research.

Competing Interests

The authors declare no conflict of interests.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (61302113, 61501289), the Shanghai Natural Science Foundation (13ZR1440800), the Shanghai Rising-Star Program (14QB1404400), Shanghai Key Laboratory of Specialty Fiber Optics and Optical Access Networks (SKLSFO 2014-03), the Science and Technology Innovation Program of Shanghai (14511101303), Shanghai Sailing Program (15YF1414500, 14YF1408900), the International Science & Technology Cooperation Project of Qinghai (2014-HZ-821), and the Application Foundation Research Project of Qinghai (2015-ZJ-721).

References

[1] T. Jiang, T. Li, and J. Ren, "Toward secure cognitive communications in wireless networks," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 82–88, 2012.

[2] F. Yu, C.-C. Chang, J. Shu, I. Ahmad, J. Zhang, and J. M. de Fuentes, "Recent advances in security and privacy for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 169305, 2 pages, 2015.

[3] W. Zhang, Y. Zhang, and T.-H. Kim, "Detecting bad information in mobile wireless networks based on the wireless application protocol," *Computing*, vol. 96, no. 9, pp. 855–874, 2014.

[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[5] Z. Chen, M. He, W. Liang, and K. Chen, "Trust-aware and low energy consumption security topology protocol of wireless sensor network," *Journal of Sensors*, vol. 2015, Article ID 716468, 10 pages, 2015.

[6] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2015.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[8] R. Bassily, E. Ekrem, X. He et al., "Cooperative security at the physical layer: a summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.

[9] H. M. Wang and X. G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 47–53, 2015.

[10] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[11] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[12] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[13] W. Xu, W. Trapper, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '05)*, pp. 46–57, Chicago, Ill, USA, May 2005.

[14] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[15] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[16] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[17] Y. Zou, J. Zhu, and B. Zheng, "Defending against eavesdropping attack leveraging multiple antennas in wireless networks," in *Proceedings of the 8th International ICST Conference on Communications and Networking in China (CHINACOM '13)*, pp. 699–703, Guilin, China, August 2013.

[18] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 839–850, 2014.

[19] P. H. Yang, *Tactical communication network node immunity of the antenna based on OPNET [M.S. thesis]*, Xidian University, Xi'an, China, 2011.

[20] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *Wired/Wireless Internet Communications*, pp. 186–200, Springer, Berlin, Germany, 2014.

[21] X. Lu, F. D. Wicker, D. Towsley, Z. Xiong, and P. Lio, "Detection probability estimation of directional antennas and omnidirectional antennas," *Wireless Personal Communications*, vol. 55, no. 1, pp. 51–63, 2010.

[22] Y. Li, P. Michal, and L. Björn, "Fair flow rate optimization by effective placement of directional antennas in wireless mesh networks," *Performance Evaluation*, vol. 87, pp. 92–106, 2015.

[23] O. Bazan and M. Jaseemuddin, "A survey on MAC protocols for wireless adhoc networks with beamforming antennas," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 216–239, 2012.

[24] C. Walsh, D. Hakkarinen, and T. Camp, "Distributed decode and forward beamforming," in *Proceedings of the 37th Annual IEEE Conference on Local Computer Networks (LCN '12)*, pp. 436–444, IEEE, Clearwater, Fla, USA, October 2012.

[25] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, 2014.

[26] X. Chen, C. Zhong, C. Yuen, and H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 40–46, 2015.

[27] Z. Liu, C. Chen, L. Bai, H. Xiang, and J. Choi, "Transmit power minimization beamforming via amplify-and-forward relays in wireless networks with multiple eavesdroppers," in *Proceedings of the IEEE International Conference on Communications (ICC '14)*, pp. 4698–4703, Sydney, Australia, June 2014.

[28] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Communications*, vol. 2, no. 3, pp. 24–32, 2007.

[29] G. Y. Zhao, "Secure transmission in PHY layer of wireless communications based on random antenna array," *China CIO News*, vol. 5, p. 96, 2013.

[30] Y. Hong, S. Im, and J. Ha, "Secure antenna subset modulation with coordinate interleaved orthogonal designs," in *Proceedings of the 5th International Conference on Information and Communication Technology Convergence (ICTC '14)*, pp. 97–98, Busan, South Korea, October 2014.

[31] N. Valliappan, A. Lozano, and R. W. Heath Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.

[32] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[33] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Processing Letters*, vol. 20, no. 5, pp. 487–490, 2013.

[34] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.

[35] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.

[36] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.

[37] D. Deng, Z.-L. Yang, and M. Zhao, "PHY security enhancement in analog network coding based on artificial noise," in *Proceedings of the 6th International Conference on Wireless Communications and Signal Processing (WCSP '14)*, pp. 1–6, Hefei, China, October 2014.

[38] O. Cepheli and G. K. Kurt, "Efficient PHY layer security in MIMO-OFDM: spatiotemporal selective artificial noise," in *Proceedings of the IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, pp. 1–6, Madrid, Spain, June 2013.

[39] W. Xu, "Jamming attack defense," in *Encyclopedia of Cryptography and Security*, pp. 655–661, Springer, New York, NY, USA, 2011.

[40] M. Olama, S. Smith, T. Kuruganti, and X. Ma, "Performance study of hybrid DS/FFH spread-spectrum systems in the presence of frequency-selective fading and multiple-access interference," in *Proceedings of the IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR '12)*, pp. 1–5, San Diego, Calif, USA, May 2012.

[41] M. M. Olama, X. Ma, T. P. Kuruganti, S. F. Smith, and S. M. Djouadi, "Hybrid DS/FFH spread-spectrum: a robust, secure transmission technique for communication in harsh environments," in *Proceedings of the IEEE Military Communications Conference (MILCOM '11)*, pp. 2136–2141, IEEE, Baltimore, Md, USA, November 2011.

[42] M. Darnell and H. M. Yung, "Security considerations in frequency hopping radio systems," in *Proceedings of the IEE Colloquium on Security and Cryptography Applications to Radio Systems*, pp. 11/1–11/3, London, UK, 1994.

[43] A. Leukhin, O. Moreno, and A. Tirkel, "Secure CDMA and frequency hop sequences," in *Proceedings of the 10th International Symposium on Wireless Communication Systems (ISWCS '13)*, pp. 1–5, VDE, Ilmenau, Germany, August 2013.

[44] F. Meucci, S. A. Wardana, and N. R. Prasad, "Secure physical layer using dynamic permutations in cognitive OFDMA systems," in *Proceedings of the IEEE 69th Vehicular Technology Conference (VTC '09)*, pp. 1–5, Barcelona, Spain, April 2009.

[45] P. P. Pan and D. M. Zhang, "Research on anti-hopping communication system," *Neijiang Technology*, vol. 6, pp. 103–115, 2014.

[46] L. Hao, T. Li, and Q. Ling, "A highly efficient secure communication interface: collision-free frequency hopping (CFFH)," in *Proceedings of the IEEE Workshop on Signal Processing Applications for Public Security and Forensics (SAFE '07)*, vol. 4, pp. 1–4, Washington, DC, USA, April 2007.

[47] M. Putzke and C. Wietfeld, "Self-organizing fractional frequency reuse for femtocells using adaptive frequency hopping," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 434–439, IEEE, Shanghai, China, April 2013.

[48] M. K. Hanawal, M. J. Abdel-Rahman, and M. Krunz, "Game theoretic anti-jamming dynamic frequency hopping and rate adaptation in wireless systems," in *Proceedings of the 12th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '14)*, pp. 247–254, Hammamet, Tunisia, May 2014.

[49] C.-F. Shih, A. E. Xhafa, and J. Zhou, "Practical frequency hopping sequence design for interference avoidance in 802.15.4e TSCH networks," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 6494–6499, IEEE, London, UK, June 2015.

[50] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 46–52, 2012.

[51] Y. Chen, G. Li, S. Li, and Y. Cheng, "A new anti-jam receiver for MFSK/FFH system with multitone jamming," in *Proceedings of the 11th IEEE Singapore International Conference on Communication Systems (ICCS '08)*, pp. 451–455, Guangzhou, China, November 2008.

[52] Q. Yang and S. C. Liew, "Asynchronous convolutional-coded physical-layer network coding," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1380–1395, 2015.

[53] F. Rosas, G. Brante, R. D. Souza, and C. Oberli, "Optimizing the code rate for achieving energy-efficient wireless communications," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '14)*, pp. 775–780, Istanbul, Turkey, April 2014.

[54] M. F. Brejza, L. Li, R. G. Maunder, B. M. Al-Hashimi, C. Berrou, and L. Hanzo, "20 years of turbo coding and energy-aware design guidelines for energy-constrained wireless applications," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 8–28, 2016.

[55] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[56] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for physical layer security," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '09)*, pp. 1–6, IEEE, Honolulu, Hawaii, USA, December 2009.

[57] D. N. K. Jayakody and M. Flanagan, "A soft decode-compress-forward relaying scheme for cooperative wireless networks," *IEEE Transactions on Vehicular Technology*, 2015.

[58] B.-J. Kwak, N.-O. Song, B. Park, D. Klinc, and S. W. McLaughlin, "Physical layer security with yarg code," in *Proceedings of the 1st International Conference on Emerging Network Intelligence*, pp. 43–48, Sliema, Malta, October 2009.

[59] F. Gray, "Pulse code communication," U. S. Patent, 2,632,058, 1953.

[60] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Proceedings of the IEEE Information Theory Workshop (ITW '10)*, pp. 1–5, Dublin, Ireland, August-September 2010.

[61] M. H. Taieb and J.-Y. Chouinard, "Enhancing secrecy of the Gaussian wiretap channel using rate compatible LDPC codes with error amplification," in *Proceedings of the14th Canadian Workshop on Information Theory (CWIT '15)*, pp. 41–45, St. John's, Canada, July 2015.

[62] Z. Yang, Y. Fan, and A. Wang, "Artificial noise and LDPC code aided physical layer security enhancement," in *Proceedings of the International Conference on Information and Communications Technologies (ICT '14)*, pp. 1–6, Nanjing, China, May 2014.

[63] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC '15)*, pp. 435–440, IEEE, London, UK, June 2015.

[64] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Communications Letters*, vol. 18, no. 10, pp. 1683–1686, 2014.