Analysis of Physical Layer Security Communication in Smart Grid

Aidong Xu1*, Tengyue Zhang2, Liang Chen3, Jie Tang2, Yixin Jiang1, Juan Guo2, Lingzhi Fei2, Peng Zhang2 and Yunan Zhang1

1Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
2School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
3Science & Technology Department of Sichuan Province, Chengdu, China
Email: xuad@csg.cn; uestcztty@163.com; rsyzch@163.com; jiangyx@csg.cn; zhangyn@csg.cn; Corresponding Author Email: xuad@csg.cn

Abstract. In the smart grid environment, the secure transmission of power data is a major challenge for smart devices. Due to the broadcasting characteristics of wireless media, wireless communications in the power grid are vulnerable to eavesdropping attacks. Traditional encryption implementation requires high costs in wireless environments. In order to improve the security of data transmission in the power grid, physical layer security (PLS) has attracted widespread attention. However, there are too many idealized and unrealistic assumptions about the security research results in this field. This paper analyzes a physical layer security communication scheme considering the actual erection distance. When up-layer system breaks by opponent, the natural randomness of the physical channel will play a role in ensuring system security. We conducted simulations and analyzed the impact of the legal user's erection distance on the physical layer security performance of data transmission in the power grid, and adopted a targeted secure transmission scheme.

1. Introduction

In smart grid, large-scale smart devices are deployed in different geographical areas to collect various types of data in real time[1]. For example, smart meters and sensors can be deployed in different areas to collect electricity data from different households and monitor household activities. Wireless data transmission in smart grid has become more and more common and necessary [2-4]. Due to the broadcast nature of wireless network, wireless network lacks physical wireless boundary of wireless transmission, which is easy to be eavesdropped by passive eavesdroppers. Therefore, the security of wireless data transmission in smart grid has become a very important issue for large-scale network services in the future. Encryption technology is used in wireless network [5]. However, encryption technology does not consider using unique attributes of wireless domain to solve security threats.

In the physical layer security (PLS) communication, the system uses the physical characteristics of wireless channel, combined with signal processing methods, to achieve unconditional safe and reliable communication [3]. Work [4] proposed the so-called eavesdropping channel. Eavesdropping channel is a security model of physical layer security. In the degraded channel, the existence of secure coding is proved and unconditional secrecy is realized. A large number of studies have discussed the upper and lower bounds of achievable secrecy rate and secrecy capacity in various communication scenarios [6,7]. Goel [6] uses artificial noise to reduce the eavesdropper's channel without interfering with...
legitimate users. In order to reduce the data leakage from the data rate to the target user, various techniques such as artificial noise addition, beamforming, power control and cooperative jamming [8] are studied. However, if the path loss of the legitimate link is more serious than that of the unauthorized link, even if the above-mentioned traditional technology is adopted, the secrecy rate will degenerate to zero. Therefore, the deployment of communication providers is very important for PLS[9].

In this letter, we study the security of wireless channel data transmission in smart grid. Different from the research in [10-17], we consider the impact of legal users’ deployment on security performance, and simulate the positive security capacity probability (PSCP) and ergodic security capacity of any legal node with distance $d$ from the center. According to the distance and security performance of the randomly erected nodes, it is suggested to adopt a more appropriate security transmission scheme.

2. System Model
The physical layer security model of smart grid system is shown in Figure 1. Consider three single antenna users in a circular area with radius of $R=2000 m$. The sending node Alice is located in the center of the circular area and sends broadcast information set up to $N=5$ fixed legitimate user nodes Bob1, Bob2, …, BobN. There is an unknown eavesdropping user Eve in an unknown location outside the circular area, and neither Alice nor Bob knows the specific location of Eve. Considering the worst security performance, Eve can always eavesdrop on the boundary of a circular area as the lower bound value of security analysis. (If Eve adopts this scheme, Eve can be excluded by patrol inspection in practice). It is expected that $N=5$ legal nodes can be set up at any position in the circular area, so that all $N$ nodes can achieve secure communication (that is, the legal node with the worst security performance can achieve secure communication).

Figure 1. Physical layer security transmission model of smart grid system.

3. The Theoretical Analysis
In the fading channel, the channel changes rapidly, and legitimate nodes obtain secure communication with probability. The probability of secure interruption needs to be low enough to ensure the smooth progress of secure coding and decoding. Among them, the probability that the security capacity is greater than zero is also the probability of realizing secure communication, which is generally regarded as the worst performance bound estimation of the probability of realizing secure communication.

3.1. The Theoretical Basis
The positive security capacity probability (PSCP) represents the probability that the system security capacity is positive
where $h_{AB}$ and $h_{AE}$ denote the fading coefficients of the main channel and the eavesdropping channel respectively. For simplicity, let $r$ and $w$ denote the instantaneous received signal to noise ratio (SNR) of Bob and Eve respectively.

$$
 r = \frac{P |h_{AB}|^2}{\sigma_B^2}, \quad w = \frac{P |h_{AE}|^2}{\sigma_E^2}
$$

Then the ergodic security capacity (ESC) can be expressed as

$$
 C_S = \int_0^\infty \int_0^\infty \left[ \log(1 + r) - \log(1 + w) \right] + f(r)f(w)drdw
$$

where $f(r)$ and $f(w)$ are probability density functions (PDF) of $r$ and $w$ respectively.

3.2. The PSCP by Erecting Legal Nodes at Any Distance

Suppose the distance between Eve and Alice is $r_E$. At a certain time, the distance between Bob and Alice is $d_{AB}$, then the received signals of Bob and Eve can be expressed as follows

$$
 y_{Bob} = \frac{\sqrt{P_T}}{d_{AB}^{a/2}} h_{AB} s + n_B, \quad y_{Eve} = \frac{\sqrt{P_T}}{r_E^{a/2}} h_{AE} s + n_E
$$

where $a$ is the path loss coefficient [18], usually $2 \leq a \leq 10$ depending on the specific channel propagation environment. $P_T$ is the transmission signal power of Alice, $s$ is the transmitted unit power symbol, we set $|s|^2 = 1$, $0 < r_E, d_{AB} \leq R$. $n_B, n_E$ are the Gaussian white noise of Bob and Eve, which are independent zero mean unit variance Gaussian variables. $h_{AB}$ and $h_{AE}$ are the time-varying complex channel fading coefficients of Bob and Eve, respectively. If the scattering environment is sufficient, $h_{AB}$ and $h_{AE}$ follow the Rayleigh fading distribution. Considering that there may be strong direct path in the actual propagation environment, users may suffer from Rice-K channel factor fading. Any more complex fading, such as Rayleigh shadow complex fading, can be deduced by the similar method. The instantaneous received SNR of Bob and Eve can be expressed as

$$
 r = \frac{P_T |h_{AB}|^2}{d_{AB}^a}, \quad w = \frac{P_T |h_{AE}|^2}{r_E^a}
$$

The average SNR of Bob and Eve can be expressed as follows

$$
 \bar{r} = \frac{P_T}{d_{AB}^a}, \quad \bar{w} = \frac{P_T}{r_E^a}
$$

Then the instantaneous secrecy capacity can be expressed as

$$
 P(C_s > 0) = P\left( r(d_{AB}) > w(r_E) \right)
$$

Then the ergodic security capacity (ESC) can be expressed as

$$
 C_S^E = E_{r,w,d_{AB}} \left\{ C_s \left[ r(d_{AB}), w(r_E) \right] \right\}
$$
where $E_{x_1, x_2, ..., x_n}$ represents the expectation of expressions containing random variables $x_1, x_2, ..., x_n$.

4. Simulation Results

In this section, we simulate the physical layer security performance of wireless channel transmission with the change of legal user's erection distance. Due to Bob's random setup, it leads to a transient unknown variable $d_{AB}$, so the security performance will also change randomly. In the application, given $d_{AB}$, we can analyze the security performance indicators of the node. In practical application, for any legal node ($0 < d < 2000m$) erected at the distance of $d$ from the center during each communication, we analyze the security indicators of this node, which are respectively: a. Probability of achieving secure communication; b. Average secrecy capacity. When $N=5$ nodes are randomly set up (D1, D2, D3, D4, D5), the above two security performance indexes of the five nodes can be evaluated respectively, and appropriate security transmission strategy can be adopted.

Figure 2. PSCP of any legal node with a distance $d$ from the center.

Figure 3. PSCP of any legal node with a distance $d$ from the center under different Rice-K factors.

Figure 2 shows the probability that the security capacity of any legal node whose distance center is $d$ is greater than zero. The value range of distance is $0 < d < 2000m$. Figure 2 compares the probability of full capacity greater than zero under Rayleigh channel and Rice channel with K factor of 0 dB, 10 dB and 20 dB, respectively. Figure 2 shows that with the increase of erection distance, the probability of secrecy capacity greater than 0 is decreasing, and finally tends to 0.5. At the same time, the channel with stronger direct path has better performance. To maintain a 90% probability, for Rayleigh channels, the erection distance should not exceed the center distance of about 1200 meters. For the Rice-K = 20dB channel, the erection distance can be more than 1900 meters with the same probability.

Figure 3 compares the probability that the security capacity is greater than zero when the path loss is 2, 3, 4 in Rice channel. It is found that the higher the path loss, the higher the probability of security capacity greater than zero.
5. Conclusion
This paper studies the security of wireless transmission in power grid system. Through the analysis of the probability of establishing a legal node at any distance from the center of the circle in the region \(0 < d < 2000m\), the probability of realizing secure communication is analyzed. Two important conclusions are drawn, the probability of secure communication decreases with the increase of erection distance, the probability of secure communication increases with the increase of direct beam power. Therefore, if any random node is close to the center, the probability of secure communication is high and the security rate is high. On the other hand, if any random node is far away from the center or close to the boundary of the region, the probability that the node can achieve security is low. Therefore, it is suggested that a more appropriate security transmission scheme should be adopted according to the distance and security performance of each randomly erected node.

6. Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

7. References
[1] Chen S, Wen H, Wu J, Lei W, Hou W, Liu W and Jiang Y 2019 Internet of things based smart grids supported by intelligent edge computing IEEE Access vol 7 p 74089-74102
[2] Wen H, Wang Y, Zhu X, Li J and Zhou L 2013 Physical layer assist authentication technique for smart meter system IET Communications vol 7 pp 189-197
[3] Shannon C E 1949 Communication theory of secrecy systems Bell System Technical Journal vol 28 pp 656-715.
[4] Wyner A D 1975 The wire-tap channel Bell System Technical Journal vol 54 pp 1355-1387
[5] Ding L, Jin C, Guan J, Wang Q 2014 Cryptanalysis of Lightweight WG-8 Stream Cipher IEEE Transactions on Information Forensics and Security vol 9 pp 645-652
[6] Goel S, Negi R 2008 Guaranteeing Secrecy using Artificial Noise IEEE Transactions on Wireless Communications vol 7 pp 2180-2189.
[7] Hu L, Wen H, Wu B, Tang J, Pan F, Liao R F 2017 Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers IEEE Transactions on Vehicular Technology vol 67 pp 2108-2117.
[8] Hu L, Wen H, Wu B, Pan F, Liao R F, Song H, Tang J, Wang X 2018 Cooperative jamming for physical layer security enhancement in Internet of Things IEEE Internet of Things Journal vol 5 pp 219-228.

[9] Al-Hourani A, Kandeepan S, Lardner S 2014 Optimal LAP altitude for maximum coverage IEEE Wireless Communications Letters vol 3 pp 569-572.

[10] Liao R F, Wen H, Wu J, Song H, Pan F and Dong L 2018 The rayleigh fading channel prediction via deep learning Wireless Communications and Mobile Computing 2018

[11] Wen H, Ho P H, Qi C and Gong G 2010 Physical layer assisted authentication for distributed ad hoc wireless sensor networks IET information security vol 4 p 390-396

[12] Wen H, Ho P H and Wu B 2014 Achieving secure communications over wiretap channels via security codes from resilient functions IEEE Wireless Communications Letters vol 3 p 273-276

[13] Ji B, Li Y, Zhou B, Li C, Song K and Wen H 2019 Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting IEEE Access vol 7 p 38738-38747

[14] Wen H, Tang J, Wu J, Song H, Wu T, Wu B and Sun L M 2014 A cross-layer secure communication model based on Discrete Fractional Fourier Transform (DFRFT) IEEE Transactions on emerging topics in computing vol 3 pp 119-126

[15] Xie F, Wen H, Li Y, Chen S, Hu L, Chen Y, Song H 2018 Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things IEEE Internet of Things Journal vol 5 pp 3967-3977.

[16] Wen H, Ho P, Gong G 2009 A Novel Framework for Message Authentication in Vehicular Communication Networks Global communications conference pp 3067-3072.

[17] Wen H, Li S, Zhu X, Zhou L 2013 A framework of the PHY-layer approach to defense against security threats in cognitive radio networks IEEE Network vol 27 pp 34-39.

[18] Goldsmith A 2005 Wireless communications Cambridge university press