J Inf Process Syst, Vol.16, No.6, pp.1261~1270, December 2020
https://doi.org/10.3745/JIPS.03.0151

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

# Secure Performance Analysis Based on Maximum Capacity

Xiuping Zheng*, Meiling Li*, and Xiaoxia Yang*

**Abstract**

The physical security layer of industrial wireless sensor networks in the event of an eavesdropping attack has been investigated in this paper. An optimal sensor selection scheme based on the maximum channel capacity is proposed for transmission environments that experience Nakagami fading. Comparing the intercept probabilities of the traditional round robin (TRR) and optimal sensor selection schemes, the system secure performance is analyzed. Simulation results show that the change in the number of sensors and the eavesdropping ratio affect the convergence rate of the intercept probability. Additionally, the proposed optimal selection scheme has a faster convergence rate compared to the TRR scheduling scheme for the same eavesdropping ratio and number of sensors. This observation is also valid when the Nakagami channel is simplified to a Rayleigh channel.

**Keywords**

Intercept Probability, Maximum Capacity, Nakagami Channel, Physical Layer, Safety Performance

## 1. Introduction

Industrial wireless communication is the core of development of the Internet of Things (IoT) technology [1-3]. The reliability and security of transmission are influenced by factors such as the characteristics of wireless communication, various types of noise, and the interaction between machines [4,5]. It is essential to study the security and reliability of information transmission, and the failure to do so can lead to significant losses, such as abnormal production, damaged machines, and even threats to the lives of people. The security of wireless communication networks must be highlighted because these networks transmit signals that are generally personal and may be confidential [6]. In fact, both authorized and the unauthorized users can access wireless media freely, as the wireless transmission environment is always open due to its broadcast nature. As a result, wireless sensor networks (WSNs) are more vulnerable to eavesdropping attacks compared to wired sensor networks. Especially in industrial WSNs, many wireless access equipment exists, and the untrustworthy nodes can easily intercept the data of the devices, which can have adverse consequences. Thus, it is important to investigate the protective measures in industrial WSNs to provide safety from such eavesdropping attacks.

Conventionally, cryptographic techniques have been utilized to protect wireless communication from



Manuscript received June 26, 2020; first revision September 4, 2020; accepted September 20, 2020.

**Corresponding Author:** Meiling Li (meilingli@tyust.edu.cn)

* School of Electronic Information and Engineering, Taiyuan University of Science and Technology, Taiyuan, China (zhengxiuping9898@163.com, meilingli@tyust.edu.cn, S20180393@stu.tyust.edu.cn)

eavesdroppers. These techniques normally require high computational capability from the equipment. However, wireless sensors often have limited computational capability, which makes it difficult to utilize cryptographic techniques to assure secure communications. In information theory, when the capacity of an eavesdropping channel is lower than the data rate, the eavesdropper cannot decode a source signal. Therefore, in industrial WSNs, the security performance of a physical layer can be improved using the information-theoretic security principle [7].

In recent years, physical layer security is garnering more attention, which can be used to evaluate the secure transmission for wireless communication systems. Even if the eavesdroppers have unlimited computational power, physical layer security can protect the confidentiality of communication against eavesdropping attacks [8]. In [9], the authors considered a multi-hop relay system with secure communications, and the secure rate was analyzed. In [10], the authors considered a heterogeneous network, and investigated the security performance of the physical layer by using the average secrecy rate and secrecy coverage probability. In [11,12], the authors investigated the tradeoff among security, reliability, throughput and other security issues by considering the single-relay-single-eavesdropping and multiple-relay-single-eavesdropping scenarios. In [13], the improvement of secrecy capacity is reflected by the difference of channel capacity in the main link and the eavesdropping link. In [14], it is shown that an eavesdropping event will occur if the channel capacity of the main link is less than the channel capacity of an eavesdropping link. Hence, increasing secrecy capacity can effectively reduce the possibility of intercepting messages. Zou and Wang [15] put forward a scheduling scheme about optimal sensor. Secrecy capacity is defined as the difference between main channel capacity and eavesdropping channel capacity. Compared with the conventional scheduling scheme, this scheme shows lower intercept probability, which can enhance the physical layer security and provide protection for industrial WSNs from eavesdropping attacks.

Most of the literature focuses on the physical layer security performance in traditional wireless network. Intercept probability is one of the most effective methods [16]. Our study is intended to secure the physical layer transmission in industrial WSNs, which have more complex channels. The considered model is composed of multiple sensors and sink nodes. We assume that the main link channel and the eavesdropping link channel satisfy the Nakagami fading channel. The relationship between channel capacity and maximum transmission rate is used to derive the secure capacity. Based on the maximum channel capacity, the intercept probabilities of the diversity gain algorithms in the traditional round robin (TRR) are studied and compared with the intercept probabilities of the diversity gain algorithms optimal sensor scheduling schemes. Experimental results show that our proposed scheme is superior to the traditional scheme.

# 2. Model Description

## 2.1 System Model

The considered industrial WSN environment model is shown as Fig. 1. The WSN includes $N$ sensors nodes, an eavesdropper and a sink node which collects the data from each sensor and makes the final decision. In this paper, we assume that all of the nodes in the system are equipped with a single antenna. As shown in Fig. 1, the main links are represented by solid lines and the eavesdropping links are

represented by dashed lines. When a sensor transmits information to the node, a user receives a signal through the main link. An eavesdropper illegally receives the signal by using a sensor. It is worth noting that eavesdroppers can be both illegal and legal users that intercept other users' data. The $N$ sensors are denoted by $S = \{s_i | i = 1,2,\cdots,N\}$. In [17] and [18], the Nakagami model is close to the actual application environment and more complex than Rayleigh fading models. Both the main channel and the eavesdropping channel are assumed as Nakagami fading channels. In this paper, we also consider that the channel characteristics are known.

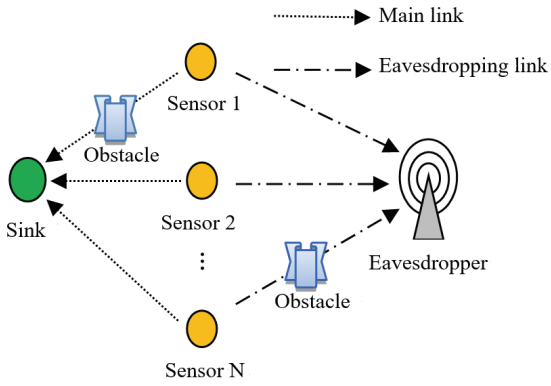


**Fig. 1.** Industrial WSN with one sink, N sensors, and an eavesdropper.

The received signal at the sink is denoted as $y_s$.

$$y_s = \sqrt{P_i} h_{is} x_i + n_s \tag{1}$$

In Eq. (1), $h_{is}$ is the channel coefficient of the $s_i$-to-sink link, $n_s$ is the complex AWGN which has zero-mean and variance $N_0$.

According to the Shannon channel capacity and Eq. (1), the achieved main channel capacity of the sensor $s_i$ to the sink link can be expressed as follows:

$$C_s(i) = log_2\left(1 + \frac{|h_{is}|^2 P_i}{N_0}\right) \tag{2}$$

where $i \in S$. We assume that the characteristic of the channel is known by the eavesdropper. However, the source signal $x_i$ is unknown. The signal received by the eavesdropper is denoted as $y_e$.

$$y_e = \sqrt{P_i} h_{ie} x_i + n_e \tag{3}$$

In Eq. (3), $h_{ie}$ is the channel coefficient of the eavesdropping link from $s_i$ to the eavesdropper, the $n_e$ is the complex AWGN, which also has zero-mean and variance $N_o$. It is to be noted that here we have assumed the eavesdropper to have the same noise channel as the legitimate users.

The channel of the eavesdropping link is indicated by $C_e(i)$.

$$C_e(i) = log_2\left(1 + \frac{|h_{ie}|^2 P_i}{N_0}\right) \tag{4}$$

With Eqs. (2) and (4), the secrecy capacity of the channel is considered as

$$C_{secrecy}(i) = max\{C_s(i) - C_e(i)\} \tag{5}$$

## 2.2 Channel Statistics

The Nakagami fading channel provides a good fit for measured data in industrial WSNs. That $|h_{is}|^2$ and $|h_{ie}|^2$ follow gamma distributions, which have the following expressions for the probability density function (PDF):

$$|h_{is}|^2 \sim \Gamma\left(m_i, \frac{{\delta_{is}}^2}{m_i}\right) \tag{6}$$

$$|h_{ie}|^2 \sim \Gamma\left(k_i, \frac{{\delta_{ie}}^2}{k_i}\right) \tag{7}$$

We define that $X_{is} = |h_{is}|^2$ and $X_{ie} = |h_{ie}|^2$. Since $|h_{is}|^2$ and $|h_{ie}|^2$ follow gamma distributions from Eqs. (6) and (7), the PDFs of $X_{is}$ and $X_{ie}$ are respectively given by

$$f_{X_{is}}(x_{is}) = \frac{1}{\Gamma(m_i)}\left(\frac{m_i}{{\delta_{is}}^2}\right)^{m_i} {x_{is}}^{m_i-1} exp\left(-\frac{m_i x_{is}}{{\delta_{is}}^2}\right) \tag{8}$$

$$f_{X_{ie}}(x_{ie}) = \frac{1}{\Gamma(k_i)}\left(\frac{k_i}{{\delta_{ie}}^2}\right)^{k_i} {x_{ie}}^{k_i-1} exp\left(-\frac{k_i x_{ie}}{{\delta_{ie}}^2}\right) \tag{9}$$

where $\Gamma(\cdot)$ denotes the gamma function.

# 3. Intercept Probability Analysis Based on Maximum Channel Capacity

Wyner [19] proposed to evaluate the secure transmission by Shannon theorem firstly. He assumed that when the Shannon capacity of C is larger than the target information rate of R in the system, the users can achieve successful transmission and the original information bits can be transferred to the destination in an arbitrarily small error probability. On the other hand, considering the eavesdropper, when the Shannon capacity of the intercepting link is higher than the target information rate of the users, the users' signals are intercepted successfully, and the intercept behavior happens. The intercept events at $s_i$-to-sink link can be defined as follows. In the process of information transmission, if the information rate of the wiretap link is not less than that of the main link, it means that the secrecy capacity is non-positive, and an intercept event is possible. Therefore, the intercept probability from $s_i$-to-sink is given by

$$\begin{aligned} P_{int} &= P_r(C_e(i) > R_d) \\ &= P_r\left(log_2\left(1 + \frac{|h_{ie}|^2 P_i}{N_0}\right) > R_d\right) \\ &= P_i(|h_{ie}|^2 > \partial) \end{aligned} \tag{10}$$

We define $\partial = \frac{(2^{R_d}-1)N_0}{P_i}$. Thus, we obtain

$$\begin{aligned} {P_{int}}^i &= Pr(|h_{ie}|^2 > \partial) \\ &= 1 - \int_0^{\partial} \frac{1}{\Gamma(k_i)}\left(\frac{k_i}{{\delta_{ie}}^2}\right)^{k_i} {x_{ie}}^{k_i-1} exp\left(-\frac{k_i x_{ie}}{{\delta_{ie}}^2}\right) dx_{ie} \\ &= exp\left(-\frac{k_i}{{\delta_{ie}}^2}\partial\right) \sum_{i=0}^{k_i-1} \frac{\left(\frac{k_i}{{\delta_{ie}}^2}\partial\right)^i}{i!} \end{aligned} \tag{11}$$

Assuming that the main and eavesdropping links have the same parameters, $m_i = k_i$ is obtained. For notational convenience, we utilize ${\delta_{is}}^2$ and ${\delta_{ie}}^2$ to represent the average channel gains of the main links and wiretap links respectively. Besides, letting $\lambda_{me}$ denote the main-to-eavesdropper ratio (MER) to represent the ratio of ${\delta_{is}}^2$ to ${\delta_{ie}}^2$, i.e., $\lambda_{me} = {\delta_{is}}^2/{\delta_{ie}}^2$. Therefore, according to Eq. (11), the following equation can be obtained:

$$\begin{aligned} {P_{int}}^i &= exp\left(-\frac{k_i}{{\delta_{ie}}^2}\partial\right)\sum_{i=0}^{k_i-1}\frac{\left(\frac{k_i}{{\delta_{ie}}^2}\partial\right)^i}{i!} \\ &= exp\left(-\frac{m_i}{{\delta_{is}}^2}\lambda_{me}\partial\right)\sum_{i=0}^{m_i-1}\frac{\left(\frac{m_i}{{\delta_{ie}}^2}\lambda_{me}\partial\right)^i}{i!} \\ &= Pr(|h_{is}| > \lambda_{me}\partial) \end{aligned} \tag{12}$$

where $\lambda_{me} \to \infty$ and ${P_{int}}^i \to \infty$.

# 4. Intercept Probability Analysis of Nakagami Fading Channel

We assume that there are N sensors in the system. The intercept probability at i-th channel sensor is defined as ${P_{int}}^i$. We analyze the intercept probabilities of the diversity gain algorithms of the traditional RR and optimal sensor selection algorithms in this section.

## 4.1 Intercept Probability of the Diversity Gain Algorithm of TRR Scheme

The achievable diversity gain obtained by the TRR scheme [20] is $d_{round} = \min_{i \in S} m_i$. According to the definition of the round robin scheme, in which, the eavesdropper will intercept the signal by each sensor, then average intercept results will be implemented by the round robin scheme. Therefore, the intercept probability of the TRR scheme is represented as ${P_{int}}^{round}$.

$${P_{int}}^{round} = \frac{1}{N}\sum_{i=1}^{N}{P_{int}}^i = \frac{1}{N}\sum_{i=1}^{N}\left[exp\left(-\frac{m_i}{{\delta_{is}}^2}\lambda_{me}\partial\right)\sum_{l=0}^{m_i-1}\frac{\left(\frac{m_i}{{\delta_{is}}^2}\lambda_{me}\partial\right)^l}{l!}\right] \tag{13}$$

## 4.2 Intercept Probability of the Diversity Gain Algorithm of Optimal Sensor Scheduling Scheme

The achievable diversity gain obtained by the optimal sensor selection scheme is $d_{proposed} = \sum_{i=1}^{N} m_i$. In this paper, we select the optimal sensor by the maximum channel capacity. Then, the intercept probability of the optimal sensor selection scheme can be calculated by ${P_{int}}^{Proposed}$.

$${P_{int}}^{proposed} = \prod_{i=1}^{N}{P_{int}}^i = \prod_{i=1}^{N} exp\left(-\frac{m_i}{{\delta_{is}}^2}\lambda_{me}\partial\right)\sum_{l=0}^{m_i-1}\frac{\left(\frac{m_i}{{\delta_{is}}^2}\lambda_{me}\partial\right)^l}{l!} \tag{14}$$

## 5. Analysis of Numerical Results

We analyze the industrial WSN model containing an eavesdropper using Eqs. (13) and (14). For the sake of convenience, we assume $\partial = 0.5$. The complex AWGN has zero-mean and variance $N_0 = 0.2$. We use the Nakagami fading channel to describe complex industrial environments. We evaluate the secure performance by comparing the intercept probabilities of the TRR scheme with the optimal sensor selection scheme. The intercept probabilities of the two schemes are simulated and analyzed based on the maximum channel capacity. The Nakagami fading channel degenerates into the Rayleigh fading channel when the shape factor satisfies the relation $m_i = k_i = 1$.

Fig. 2 shows that the probabilities of intercept varies with the MER when $m_i = k_i = 1$, according to Eqs. (13) and (14), under different sensor numbers. In Fig. 2, we can see that the traditional scheduling scheme of round robin shows a less obvious reduction in terms of intercept probabilities than the proposed optimal selection scheme, when the sensor numbers changes from $N = 2$ to $N = 4$. It shows that as the sensor numbers increases, the TRR scheduling scheme cannot significantly improve the secure performance. Besides, we can draw certain conclusions from Fig. 2; in the case of the same number of sensors, the optimal sensor scheduling scheme has better security performance by comparing the intercept probability.

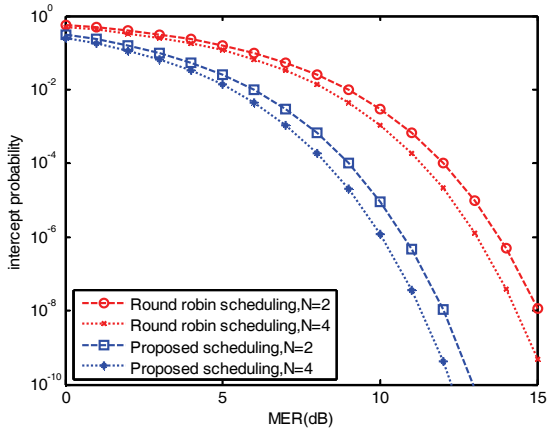


**Fig. 2.** Intercept probabilities versus MER when $m_i = k_i = 1$.

Fig. 3 demonstrates the intercept probability versus the sensor numbers when $m_i = k_i = 1$ for different MERs. As the MER increases from $\lambda_{me} = 3$ dB to $\lambda_{me} = 5$ dB, the intercept probability of the traditional scheduling scheme is almost constant. This shows that *N* has little impact on security benefit of round robin scheduling scheme. However, under the same conditions, the intercept probability can significantly decrease as N increases in the proposed optimal scheme. And the intercept probability also decreases when MER changes from $\lambda_{me} = 3$ dB to $\lambda_{me} = 5$ dB in the proposed optimal scheme. This indicates that, relative to the TRR scheduling scheme, the security benefit of the optimal scheduling scheme is better.

Fig. 4 shows the variations of the intercept probability with the MER. In the simulation, the parameters are set as: the Nakagami fading factor is defined as $m_i = k_i = 2$. When the number of sensors is changed, the probabilities of intercept under the TRR and optimal schemes both decrease significantly.

Furthermore, the convergence of the latter is more evident. When the number of sensors is the same, the rate of the optimal scheme is clearly superior to that of the traditional scheme.

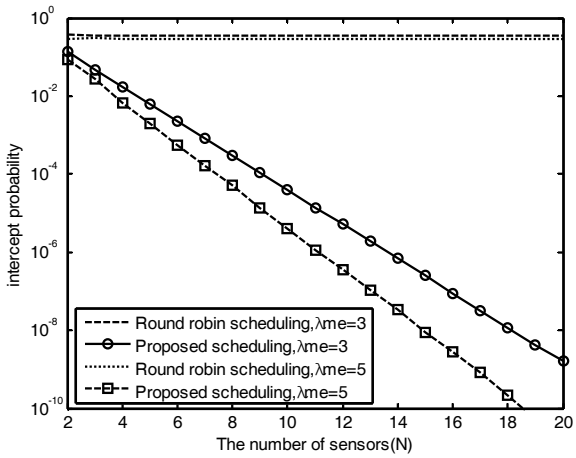


**Fig. 3.** Intercept probabilities versus the number of sensors when $m_i = k_i = 1$, $\lambda_{me} = 3$ dB to $\lambda_{me} = 5$ dB.

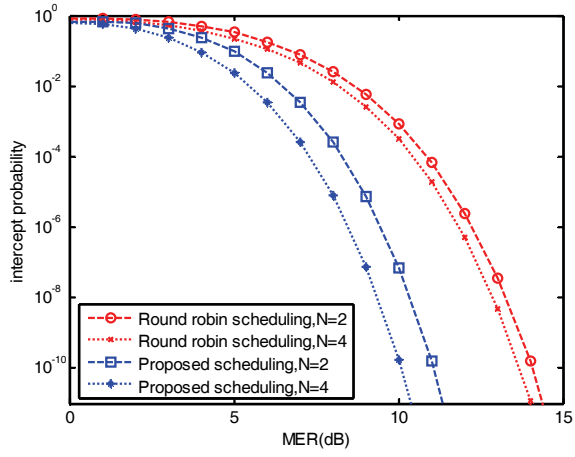


**Fig. 4.** Intercept probabilities versus MER when $m_i = k_i = 2$.

Fig. 5 illustrates intercept probabilities versus the number of sensors when $m_i = k_i = 2$, $\lambda_{me} = 3$ dB and $\lambda_{me} = 5$ dB. Fig. 5 also demonstrates that the intercept probabilities of the TRR scheme are constant. The change of the intercept probabilities of optimal scheduling schemes is also shown in Fig. 5. When $m_i = k_i = 2$, we simulated the cases for $\lambda_{me} = 3$ dB to $\lambda_{me} = 5$ dB. For the case of same MER, it can be seen that the lower probability of intercept can always be achieved by the optimal scheduling scheme than that of the TRR scheme, and the intercept probability of the TRR scheduling scheme is a straight line as *N* increases. The intercept probability of the proposed scheme decreases significantly when the MER is changed from 3 dB to 5 dB. Compared with the TRR scheduling scheme, the optimal scheduling scheme has better security benefits. In addition, for both of the scheduling schemes, the convergence rates of the intercept probabilities increase with increase in MER.

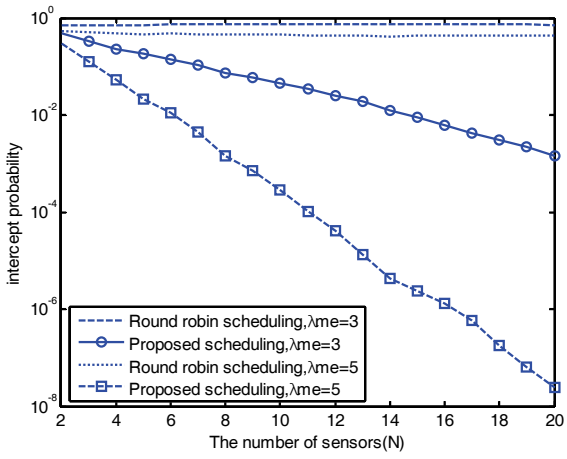


**Fig. 5.** Intercept probabilities versus the number of sensors when $m_i = k_i = 2$, $\lambda_{me} = 3$ dB to $\lambda_{me} = 5$ dB.

## 6. Conclusion

The physical layer transmission of industrial WSNs is affected by numerous factors such as the estimation error in a channel, change in the transmission environment of a sensor, real-time requirement of data, and priority level settings. We researched the physical layer security of the WSNs in the presence of an eavesdropper. We proposed a sensor selection scheme based on the maximum channel capacity considering Nakagami channel and compared it with the TRR scheduling scheme. The intercept probabilities of the optimal scheme and the traditional scheme were derived. When the number of sensors is invariant, we analyze the effect of different eavesdropping ratios on the intercept probability. Additionally, when the eavesdropping ratio is invariant, the trend of variation in the interception probability with the number of sensors is analyzed. The results show that the intercept probability of the optimal sensor scheduling scheme is superior in terms of convergence for both cases.

## Acknowledgement

This work was supported in part by the National Natural Science Foundation of China (No. 62001320), the Key Research and Development Program of Shanxi (No. 201903D121117), the Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (No. 201802090), Research Project Supported by Shanxi Scholarship Council of China (No. 2020-126), Graduate Education Innovation Project of Shanxi (No. 2020SY419).

## References

[1] G. B. Satrya and S. Y. Shin, "Evolutionary computing approach to optimize superframe scheduling on industrial wireless sensor networks," *Journal of King Saud University - Computer and Information Sciences*, 2020. https://doi.org/10.1016/j.jksuci.2020.01.014

[2] A. Bagdadee, M. Hoque, and L. Zhang, "IoT based wireless sensor network for power quality control in smart grid," *Procedia Computer Science*, vol. 167, pp. 1148-1160, 2020.

[3] D. Sun and S. Willmann, "Deep Learning-based dependability assessment method for industrial wireless network," *IFAC-PapersOnLine*, vol. 52, no. 24, pp. 219-224, 2019.

[4] X. Li, D. Li, J. Wan, A. V. Vasilakos, C. F. Lai, and S. Wang, "A review of industrial wireless networks in the context of Industry 4.0," *Wireless Networks*, vol. 23, no. 1, pp. 23-41, 2017.

[5] M. Kumar, R. Tripathi, and S. Tiwari, "QoS guarantee towards reliability and timeliness in industrial wireless sensor networks," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4491-4508, 2018.

[6] A. Khalil, A. Saadoui, M. Tabaa, M. Chehaitly, F. Moteiro, A. Oukaira, and A. Dandache, "Combined Reed-Solomon and convolutional codes for IWSN based on IDWPT/DWPT architecture," *Procedia Computer Science*, vol. 155, pp. 666-671, 2019.

[7] Z. Liu, J. Wang, R. Sun, and Z. Wang, "Review on physical-layer security techniques of wireless communications," *Communications Technology*, vol. 47, no. 2, pp. 128-135, 2014.

[8] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, 2015.

[9] Q. Lv, G. Han, and X. Fu, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Communications Letters*, vol. 22, no. 9, pp. 1882-1885, 2018.

[10] W. Zhao, Z. Chen, K. Li, B. Xia, and P. Chen, "Artificial interference aided physical layer security in cache-enabled heterogeneous networks," in *Proceedings of 2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Kalamata, Greece, 2018, pp. 1-5.

[11] G. Cherukuri, S. Sharma, S. D. Roy, and S. Kundu, "Secrecy outage probability of dual hop amplify and forward relay in presence of an eavesdropper," in *Proceedings of 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 694-698.

[12] H. Lei, Z. Yang, K. Park, I. S. Ansari, Y. Cao, G. Pan, and M. S. Alouini, "Secrecy outage analysis for cooperative NOMA systems with relay selection scheme," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6282-6298, 2019.

[13] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451-456, 1978.

[14] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653-2661, 2014.

[15] Y. Zou and G. Wang, "Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 780-787, 2016.

[16] J. M. Moualeu, W. Hamouda, and F. Takawira, "Intercept probability analysis of wireless networks in the presence of eavesdropping attack with co-channel interference," *IEEE Access*, vol. 6, pp. 41490-41503, 2018.

[17] D. Lee and B. J. Jeong, "Performance analysis of combining space-time block coding and scheduling over arbitrary Nakagami fading channels" *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2540-2551, 2014.

[18] S. Hussain and X. N. Fernando, "Closed-form analysis of relay-based cognitive radio networks over Nakagami-m fading channels," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 3, pp. 1193-1203, 2014.

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

[20] Y. Wang, T. Liao, and C. Wang, "An anti-eavesdrop transmission scheduling scheme based on maximizing secrecy outage probability in ad hoc networks," *China Communications*, vol. 13, no. 1, pp. 176-184, 2016.

**Xiuping Zheng** **https://orcid.org/0000-0002-5369-9885**

She received her master's degree in signal and information processing from Taiyuan University of Technology, Taiyuan, China, in July 2005. Currently, she is a teacher at Taiyuan University of Science and Technology. Her research interests span a wide range of topics in wireless communications and signal processing as well as their industrial applications, including wireless security and industrial wireless sensor networks.

**Meiling Li** **https://orcid.org/0000-0002-4596-4271**

She received her M.S. and Ph.D. degrees in Signal and Information Processing from Beijing University of Posts and Telecommunications (BUPT) in 2007 and 2012, respectively. She is now an associate professor in the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. She has been a visiting research scholar at the University of Warwick, UK. Her research interests include cognitive radio, cooperative communications, non-orthogonal multiple access and physical layer security technology.

**Xiaoxia Yang** **https://orcid.org/0000-0002-3805-4149**

She is now a graduate in Taiyuan University of Science and Technology. Her research interests include physical layer security and ambient backscatter technology.