Security Outage Probability Analysis of Cognitive Networks with Multiple Eavesdroppers for Industrial Internet of Things

Meiling Li[1], Hu Yuan[2], Carsten Maple[2], Ying Li[1], and Osama Alluhaibi[3]

***Abstract*—The Industrial Internet of Things (IIoT) has been recognised as having the potential to benefit a range of industrial sectors substantially. However, widespread development and deployment of IIoT systems are limited for some reasons, the most significant of which are a shortage of spectrum resources and network security issues. Given the heterogeneity of IIoT devices, typical cryptographic security techniques are insufficient since they can suffer from challenges including computation, storage, latency, and interoperability. This paper presents a physical layer security analysis of the underlying cognitive radio networks for IIoT. Through consideration of the spectrum, IIoT devices can opportunistically utilise the primary spectrum, thereby improving spectrum efficiency and allowing access by an increased number of devices. Specifically, we propose two cognitive relay transmission (CRT) schemes, optimal single CRT (O-SCRT) and multiple CRT (MCRT), to improve transmission reliability further. Since it is challenging to obtain channel state information in the wiretap link, we provide a sub-optimal single CRT scheme and derive closed-form expressions of security outage probability by invoking both selection combination and maximal ratio combination techniques at the eavesdropper. To provide a benchmark, the round-robin single CRT scheme is also analysed. Simulation results are provided to verify our analysis and show that O-SCRT provides the best system security outage performance.**

***Index Terms*—Multi-eavesdropping, single cognitive relay transmission, multi-cognitive relay transmission, security outage performance, selective combination, maximal ratio combination.**

I. INTRODUCTION

THEindustrial IoT (IIoT) is a subset of the IoT, which implements the IoT paradigm in industrial fields such as energy, manufacturing, transportation and logistics [1]. The IIoT provides a better understanding of the manufacturing process. Therefore, the IIoT can efficiently allocate manufacturing resources, customer demanding production, optimised manufacturing process, and fast environment adaptation [2].

Flexibility and scalability are the two characters of IIoT communications [3]. Thus wireless communication is the typical solution for IIoT connection. However, the massive "things" connecting to the internet wirelessly create much data to be transferred in IIoT communications, which challenges the spectrum resources. Therefore, cognitive radio (CR) technology has been deemed efficient in dynamic spectrum sharing to improve spectrum efficiency in limited spectrum scenarios [4].

Recently, researchers addressed the CR for IIoT in various domains. First, the authors highlight potential applications of CR-based IoT systems in [5]. Then, in [6], the authors investigated how to combine CR technology and IoT to reduce the blocking probability of higher-priority CU calls while maintaining a sufficient channel utilisation level. In [7], the authors discussed the applications, security-oriented issues and spectrum-related functions of cognitive IIoT. The spectrum resources allocation for cognitive IIoT was studied in [8]. The authors optimised the resources for spectrum sensing time, node transmission power, and the number of users in one cluster for maximising the average network throughput. It can be concluded that available spectrum resources can be expanded by combining the IIoT with CR, by which a massive amount of industrial data can be well transmitted. However, there are very few studies on combining IIoT with CR.

On the other hand, communication security is exceptionally significant for IIoT networks. The broadcast nature of the wireless medium makes IIoT communications susceptible to potential security threats such as eavesdropping and impersonation. Furthermore, the IIoT devices or sensors usually lack the computing power to apply complex key management, especially for massive heterogeneous networks. Consequently, traditional cryptographic techniques may result in high latency, which cannot satisfy the stringent latency requirement in IIoT communications. As a result, it is a great challenge to realise the security by the traditional signalling process in IIoT.

Physical layer security (PLS) is a low complexity approach to provide security to the users by utilising the dynamic properties of wireless communication [9, 10], which is more suitable to solve the secure transmission for a heterogeneous network like IIoT.

To the best of the authors' knowledge, there is little research on secure cognitive IIoT communications. Therefore,

Manuscript received 19 May, 2021; revised 28 Mar, 2022 and accepted 15 May 2022. This work was partly supported by the National Natural Science Foundation of China under Grant 62001320, Central government funds for guiding local scientific and technological development of Shanxi under Grant YDZJSX2021A037, Research Project Supported by Shanxi Scholarship Council of China under Grant 2021-133 and 2020-126. Professor Maple would like to acknowledge the support of UKRI through the grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research - University of Warwick), EP/N510129/1 (The Alan Turing Institute) and EP/S035362/1 (PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity). (Corresponding author: Meiling Li.)

[1]M. Li, and Y. Li are with School of Electronics Information Engineering, Taiyuan University of Science and Technology, 030024 Taiyuan, China (e-mail: meilingli@tyust.edu.cn, 564932926@qq.com).

[2]H. Yuan and C. Maple are with the WMG, University of Warwick, Coventry, CV4 7AL, UK (e-mail: H.Yuan.4@warwick.ac.uk, CM@warwick.ac.uk).

[3]Osama Alluhaibi is with the Department of Electrical, University of Kirkuk, Iraq (e-mail:osake@uokirkuk.edu.iq).

investigating how to combine CR and IIoT is critically essential. Based on this, a secure performance evaluation can be implemented, and the corresponding performance optimisation may be investigated further to improve IIoT communication security.

A. Related Works

Different sharing spectrum schemes with primary users have been presented in [11], including overlay, underlay and hybrid schemes. The critical idea of underlay CR networks is that cognitive user (CU) can share the spectrum of the primary users (PUs).

Security capacity in wireless networks such as wireless sensor networks, the cooperative relay network and CR networks attracts much attention. The authors in [12], analysed the security capacity performance of wireless sensor networks by evaluating the intercept probability of round-robin scheduling and optimal sensor scheduling under Nakagami channel fading.

The cooperative relay has been used to improve the transmission reliability with users cooperation, and in the meantime, it also enhanced the secure reliability of transmission by correctly relay selection schemes [13-16]. The authors studied the PLS performance of both amplify and forward (AF), and decode and forward (DF) relay scheme in [13, 14]. They analysed the information intercept probability and communication outage probability of different relay selection schemes with a multi-relay single-eavesdropping scenario. In [15], the authors proposed a two-way optimal DF relay selection scheme aided by artificial noise to reduce the received SNR of the eavesdropper. The PLS for multiuser relay networks is studied in [16]. The authors presented three relay selections criteria to improve the security performance by selecting the best relay user pair, the maximum SNR ratio of users to the eavesdroppers. Besides, in the presence of multiple passive eavesdroppers, the security performance of multi-hop DF relay was investigated over Nakagami-m fading channels in [17], showing the advantaged multi-hop DF relaying systems against eavesdropping attacks.

In CR networks, different sharing spectrum schemes with primary users have been presented in [11] , including overlay, underlay and hybrid schemes. The critical idea of underlay CR networks is that CU can opportunistically share the spectrum of the PUs when no PU occupies the licensed spectrum. In IIoT communications, heterogeneous devices can be CUs, which can realise their transmission by accessing the primary spectrum opportunistically.

In contrast with the conventional non-cognitive wireless networks, the physical-layer security in CR networks has to consider diverse additional challenges, including protecting the primary users' quality of service (QoS) and mitigating the mutual interference between the primary and secondary transmissions. The authors investigated the PLS for CR networks over Nakagami-m fading channels subject to the interference power constraint in [18]. In [19], the outage probability and intercept probability was derived for an energy-harvesting underlay CR system adopting the energy-aware multiuser scheduling scheme. In [20], the authors investigated the PLS for CR networks under imperfect channel state information (CSI).

In [21], the PLS of cognitive decode and forward (DF) relay networks over Nakagami-m fading channels was studied with outdated CSI. In [22], the PLS of underlay cognitive DF relay networks is investigated. Through multiple cognitive DF relays, a cognitive transmitter exchanged confidential information with a secondary destination. In [23], the security and reliability was studied in underlay cognitive with two-way relay network. In order to provide secure communication for secondary transmission, artificial noise was introduced to the cooperative scheme. In [24], the authors analysed how the signal transmission of the secondary users would affect the PUs in a single eavesdropper CR network. They derived the intercept probability of PUs and symbol error probability of secondary users. The results show that network security mainly depends on the two factors: channel condition between the CR node and the eavesdropper (E); and the transmission power of CR users. While in [25], the authors investigated the secure transmission scheme for the cognitive multi-relay networks based on energy harvesting utilising jamming signals. The secure cognitive transmission by artificial noise scheme has also been discussed in [26-28].

As mentioned above, the literature has played a vital role and laid a solid foundation for fostering PLS in CRs. However, there is still a lacks research on the security performance analysis in CR based IIoT networks.

B. Contributions and Paper Structure

In this article, we look into the secure transmission in IIoT communication networks with underlay CR, where a multi cognitive relay transmission system with multi-eavesdropping is considered. Furthermore, the secondary network is used for data transmission between IIOT devices by opportunistically utilizing the primary spectrum under certain interference constraints to improve the spectrum efficiency. The whole system model is presented first, followed by an analysis of the relevant performance. Precisely, the main contributions of this paper can be summarised as follows:

- For an IIoT network, a novel multiple cognitive relay strategy is developed. The security performance of single-cognitive relay (SCRT) and multi-cognitive relay (MCRT) in the presence of multiple cooperative eavesdroppers are investigated in Nakagami-m fading channel.
- The optimal single cognitive relay transmission (O-SCRT) and multi cognitive relay transmission (MCRT) schemes were proposed in cognitive DF relay networks. In addition, a sub-optimal cognitive relay transmission (SO-SCRT) scheme is introduced to select the cognitive relay with the best communication security performance.
- The security outage probabilities of transmission schemes were reduced by proposed relay schemes: selective combining (SC) and maximal ratio combining.
- As a benchmark, the security outage performance of the round-robin scheduling based SCRT scheme was also analysed when SC and MRC technologies were utilised at the eavesdropping system (RR-SCRT).

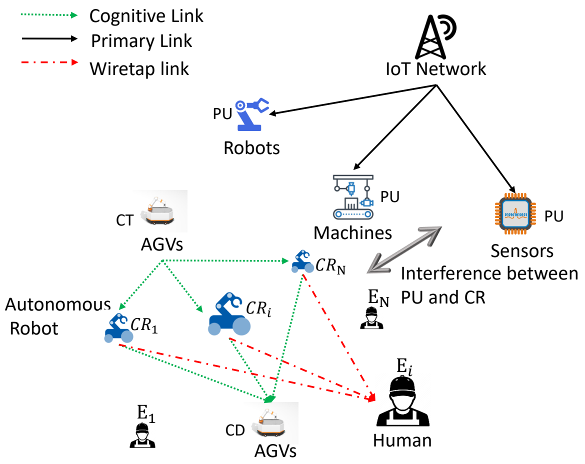


Fig. 1: Coexistence of a primary network and a cognitive multiply relay network for IIOT communications. One cognitive transmitter (CT) and one cognitive destination (CD) with N cognitive relays (CR) and M eavesdroppers.

The rest of this article is organised as follows. First, section II defines the system mode, and the relay selection with multi-eavesdropping is presented in Section III. Then, the security outage of the different relay selection models is presented in Section IV, and the numerical results are displayed in Section V. At last, the conclusions are discussed in Section VI.

II. System Model

This paper considered an underlay CR multi-relay wireless network for the IIoT system. The system is illustrated in Fig.1. Generally, the primary users are defined as the properties located in a fixed place for dedicated tasks. Meanwhile, the Cognitive users (CU) are set as the properties with multiple tasks and autonomous available. The cognitive transmitter (CT) sends a message to the cognitive destination (CD) via multiple cognitive relays CR_i $(CR_i, i = 1, 2 \cdots N)$, where N is the number of CTs. The eavesdroppers E_j $(E_j, j = 1, 2 \cdots M)$ are surrounding to wiretap the message sending by CT. To be specific, the CT should first detect whether the licensed spectrum is occupied by the primary user (PU) with spectrum sensing. To avoid interfering with the PUs, only if the CT has detected the idle spectrum can then start transmission to the CD via CRs on the unoccupied spectrum. The assumptions are made as (1) no direct link between the CT and the CD because of the deep channel fading; (2) the CRs cannot communicate with each other; (3) eavesdroppers can only attempt to intercept the secondary transmission from the CRs to the CD. It is noted that this assumption can be used for the scenario that both CD and E are assumed to be beyond the coverage area of the CT as considered in [29]. However, there is further case in which CD and the eavesdropper are within the coverage of the same source node. In such a case, both CD and the eavesdropper will receive two signals from CT and CR and can then combine them using diversity combining technologies. Thus, the enhanced SINR for CD and eavesdropper will be used for evaluating the SOP.

The cognitive transmission process is realised in two time slots: 1) CT transmits a signal x_T at power P_T on the detected a idle spectrum; 2) CRs receive the signal from the CT and uses the half-duplex DF method to decode the received signal and forward the decoded estimated signal to the CD. Let $\mathbf{D}$ denotes successful decoding set of CRs, then the sample space of $\mathbf{D}$ is denoted as $\Omega = \{\varnothing, D_1, D_2, \cdots D_n \cdots D_{2^N-1}\}$. $\varnothing$ indicates that no cognitive relay can successfully decode the source signal, D_n indicates that $|D_n|$ relay can successfully decode the source signal. $\Omega \neq \varnothing$ means at least one CR can decode the received signal. Two relay selection algorithms are: i) MCR scheme (all of the CRs that decoded the source signal successfully are used to forward the estimated signal to the CD); ii) SCR scheme (only one of the CR is selected to forward the estimated signal). In the MCR selection scheme, the CD and each eavesdropper will receive multiple signals from multiple CRs, which will be combined by MRC techniques at the CD and each eavesdropper. Finally, the eavesdropper system will utilise the SC technique and MRC technique to tackle the intercepted signals by each eavesdropper. In this paper, the Nakagami fading model is used for characterising all of the channels. As specific channel estimation is not the main objective of this paper, we consider the perfect CSI, which can be regarded as a bound to provide meaningful insights into the design of cognitive transmission in IIoT networks, although imperfect CSI should be more practical [26, 30].

As shown in [31], let H_0 represents the event that the licensed spectrum is unoccupied and H_1 means spectrum occupied by the PU during a particular time slot, respectively. Moreover, let $\hat{\mathrm{H}} = \mathrm{H}_0$ denotes the case that the licensed spectrum is unoccupied, while $\hat{\mathrm{H}} = \mathrm{H}_1$ indicates that the licensed spectrum is occupied by the CT. Moreover, let $P_d = \Pr(\hat{\mathrm{H}} = \mathrm{H}_1|\mathrm{H}_1)$ and $P_f = \Pr(\hat{\mathrm{H}} = \mathrm{H}_1|\mathrm{H}_0)$ denote the probability of correct detection and false alarm of the presence of primary user, respectively. Let $P_0 = \Pr(\mathrm{H}_0)$ represents the probability that the licensed spectrum is unoccupied by any nodes.

III. Cognitive Relay Transmission Scheme

A. Single cognitive relay transmission scheme

As shown in Fig.1, a total of N cognitive relays (CRs) are employed to assist the cognitive CT-CD transmission. The common control channel (CCC) [11] is available for coordinating the actions of the different network nodes. The half-duplex DF relay is utilised to realize the transmission. The half-duplex DF relay is utilised to realise the transmission. More specifically, once the licensed spectrum is deemed to be unoccupied, the CT first broadcasts its signal x_T at power P_T to the N CRs, which attempt to decode x_T from their received signals. The signal received by each $CR_i (i = 1, 2 \cdots N)$ can be expressed as:

$$y_{R_i} = \sqrt{P_T} h_T^{R_i} x_T + \sqrt{\alpha P_P} h_P^{R_i} x_P + n_{R_i}, \tag{1}$$

where h_a^b represents the channel fading coefficient from node a to node b, which subject to Nakagami fading. For notation conveniently, we denote CT as T, CR as R, CD as D and PU as P in the following equations respectively. $\alpha = \{0|\mathrm{H}_0 \text{ or } 1|\mathrm{H}_1\}$, where H_0 represents the licensed spectrum is unoccupied by PU and no primary signal is transmitted, leading to $\alpha = 0$. By contrast, H_1 represents PU is transmitting its signal x_P over the licensed spectrum, thus $\alpha = 1$. P_p is the transmit power of the PU, x_P is the signal transmitted by the PU, n_{R_i} is the additive white Gaussian noise, $n_{R_i} \sim \mathcal{CN}(0, \sigma^2_{R_i})$.

In the SCRT scheme, one of the cognitive relay CR$_i$ is selected in D_n to transmit its decoded estimated signal $\hat{x}_{R_i}$ to the destination CD. The signal received by the CD is

$$y^{\text{SCRT}}_{R_i \to D} = \sqrt{P_T} h^D_{R_i} \hat{x}_{R_i} + \sqrt{\alpha P_p} h^D_P x_P + n_D, \tag{2}$$

where $n_D \sim \mathcal{CN}\left(0, \sigma^2_D\right)$ is the additive white Gaussian noise.

The channel capacity in the main link from CR$_i$ to CD of SCRT scheme can be expressed as

$$C^{\text{SCRT}}_{M,R_i} = \frac{1}{2} log_2 \left(1 + \frac{\gamma_s \left|h^D_{R_i}\right|^2}{\left|h^D_P\right|^2 \alpha\gamma_p + 1}\right). \tag{3}$$

where $\gamma_s = P_T/\sigma^2_D$ and $\gamma_p = P_P/\sigma^2_D$.

At the same time, the eavesdropper E_j, where $j = 1, 2 \cdots M$, would also receive the signal from cognitive relay CR_i. The signal received by E_j is

$$y^{\text{SCRT}}_{E_j} = \sqrt{P_T} h^{E_j}_{R_i} \hat{x}^H_R + \sqrt{\alpha P_P} h^{E_j}_P x_P + n_{E_j}, \tag{4}$$

where $n_{E_j} \sim \mathcal{CN}(0, \sigma^2_{E_j})$ is the additive white Gaussian noise. In the following section, we consider that the additional noise in the main link and the eavesdropping link are the same, which is $\sigma^2_{R_i} = \sigma^2_D = \sigma^2_{E_j} = \sigma^2$, which assumption that can be regarded as the worst scenario so that the diversity order is 0.

From (3), the selected cognitive relay CR_i directly affect the channel link capacity. Three cognitive relay selection schemes are chosen in this paper, (1) Round-robin single cognitive relay transmission (RR-SCR) scheme, (2) optimal single cognitive relay transmission (Opt-SCR) scheme and (3) sub-optimal single cognitive relay transmission (Sub-SCR) scheme. On the other hand, at the eavesdropper, SC and MRC techniques will be utilised to combine each signal of E_j. The corresponding achievable capacities are different under each cognitive relay transmission schemes. The details are fully explained next.

1) Round Robin single cognitive relay transmission scheme (RR-SCRT):

In this paper, the SC and MRC techniques are employed at the eavesdropper, which results in different achievable channel capacity in the wiretap link. To be specific, in the RR SCRT scheme, we name them as RR-SC SCRT scheme and the RR-MRC SCRT scheme, respectively.

a) RR-SC SCRT scheme: From (4), when CR_i is selected to transmit the source signal to the CD, the achievable channel capacity at the eavesdropper can be expressed as follows

$$C^{\text{RR-SC}}_{E,R_i} = \max_j \left[\frac{1}{2} log_2 \left(1 + \frac{\gamma_s \left|h^{E_j}_{R_i}\right|^2}{\left|h^{E_j}_P\right|^2 \alpha\gamma_p + 1}\right)\right]. \tag{5}$$

b) RR-MRC-SCRT scheme: In the RR-MRC-SCRT scheme, the eavesdropper can adopt the maximal ratio combine method to wiretap the information. Note that the eavesdroppers are assumed far from the PU, so fading from PU to each eavesdropper can be deemed the same. Consequently, when CR_i is selected to transmit the source signal to the CD, the channel capacity at the eavesdroppers is

$$C^{\text{RR-MRC}}_{E,R_i} = \frac{1}{2} log_2 \left(1 + \frac{\sum^M_{j=1} \left|h^{E_j}_{R_i}\right|^2 \gamma_s}{\left|h^E_P\right|^2 \alpha\gamma_p + 1}\right). \tag{6}$$

2) Optimal single cognitive relay transmission scheme (O-SCRT):

In the optimal single cognitive relay transmission scheme (O-SCRT), we select the optimal relay with the maximum security capacity for assisted transmission in D_n which is

$$CR = \arg\max_{R_i} \left(C^{\text{SCRT}}_{M,R_i} - C^{\text{SCRT}}_{E,R_i}\right). \tag{7}$$

When the best cognitive relay CR_b is selected, SC is utilised to combine the intercepted signal. Thus the achievable channel capacity at the eavesdropper can be easily obtained via formula (5) by replacing R_i to R_b, which we denote as C^{O-SC}_E. In the same theory, when the MRC method is utilised to wiretap the information, the achievable channel capacity at the eavesdropper can also be easily obtained via formula (6) by replacing R_i to R_b, which we denote as $C^{\text{O-MRC}}_E$.

3) Sub-optimal single cognitive relay transmission scheme (SO-SCRT):

Because the O-SCRT scheme needs to know the wiretap CSI, which is difficult to obtain the information in practice. The cognitive relay with the largest channel capacity in the main channel is selected to forward the source signal in the SO-SCRT scheme,

$$CR_{\text{Sub}} = \arg\max_{R_i} C^{\text{SCRT}}_{M,R_i}. \tag{8}$$

Similarly, when the cognitive relay CR_d is selected to forward the source signal with SC technique is utilised to combine the intercepted signal at the eavesdropper, the achievable channel capacity at the eavesdropper can be obtained via (4) by replace R_i to R_d, which we denote as $C^{\text{SO-SC}}_E$. The achievable channel capacity at the eavesdropper with MRC method is utilised can also be easily obtained via formula (5) by replace R_i to R_d, which we denote as $C^{\text{SO-MRC}}_E$.

B. Multiple cognitive relay transmission scheme (MCRT)

In the MCRT scheme, all cognitive relays in D_n will transmit their decoded estimated signals to the destination, We consider that CD uses MRC technology to combine the received signals. The signals received by CD can be expressed as

$$\begin{aligned} y^{\text{MCRT}}_D = & \sum^{|D_n|}_{i=1} \sqrt{\frac{P_T}{|D_n|}} \left|h^D_{R_i}\right|^2 \hat{x}_{R_i} \\ & + \sum^{|D_n|}_{i=1} h^{D^*}_{R_i} n_D + \sum^{|D_n|}_{i=1} \sqrt{\alpha P_P} h^D_P h^{D^*}_{R_i} x_P \end{aligned}. \tag{9}$$

The achievable capacity at the CD can be expressed as

$$C_M^{\text{MCRT}} = \frac{1}{2}log_2\left(1+\sum_{i=1}^{|D_n|}\frac{\gamma_s\left|h_{R_i}^D\right|^2}{|D_n|\left|h_P^D\right|^2\alpha\gamma_p+|D_n|}\right). \quad (10)$$

Meanwhile, the eavesdropper E_j would also receive the signal $\hat{x}_{R_i}$ forwarded by CR_i. In this section, we consider that E_j utilises MRC technology to combine the received cognitive signal from multi cognitive relays. The combined signal at E_j is

$$\begin{aligned} y_{E_j}^{\text{MCRT}} = &\sum_{i=1}^{|D_n|}\sqrt{\frac{P_T}{|D_n|}}\left|h_{R_i}^{E_j}\right|^2\hat{x}_{R_i}+\sum_{i=1}^{|D_n|}h_{R_i}^{E_j^*}n_D \\ &+\sum_{i=1}^{|D_n|}\sqrt{\alpha P_P}h_P^{E_j}h_{R_i}^{E_j^*}x_P \end{aligned}. \quad (11)$$

When the SC technique is utilised to combine the signal from each eavesdropper, which also named as SC-MCRT scheme. We can get the wiretap channel capacity expression as formula (12).

$$C_E^{\text{SC-MCRT}} = \max_j\left[\frac{1}{2}\log_2\left(1+\frac{\gamma_s\sum_{i=1}^N\left|h_{R_i}^{E_j}\right|^2}{|D_n|\left|h_P^E\right|^2\alpha\gamma_p+|D_n|}\right)\right]. \quad (12)$$

Similarly, when the MRC technique is utilized to combine the signal from each eavesdropper, which also named as MRC-MCRT scheme. We can get the wiretap channel capacity expression as formula (13).

$$C_E^{\text{MRC-MCRT}} = \frac{1}{2}\log_2\left(1+\frac{\gamma_s\sum_{j=1}^M\sum_{i=1}^N\left|h_{R_i}^{E_j}\right|^2}{|D_n|\left(\left|h_P^E\right|^2\alpha\gamma_p+1\right)}\right). \quad (13)$$

To unify the notations, let C_M^A and C_E^A denote the achievable channel capacity at the CD and the eavesdropper under cognitive relay transmission scheme A, respectively. Then, the secure achievable capacity under scheme A can be expressed as $C_s^A = C_M^A - C_E^A$.

IV. Communication Security Outage

In the ME-CRT system, the CT-CD link outage occurs under two cases. (1) The cognitive relay decode set empty, i.e., $D = \varnothing$; (2) The cognitive relay decoding set is not empty, while the secure channel capacity $C_s^A < 0$, which means that the achievable channel capacity of C_M^A in the main link is less than the channel capacity of C_E^A in the eavesdropping link. The achievable security rate in the main link varies under different cognitive relay cooperation schemes.In this section, the secure outage performance in the SCR scheme and MCR scheme is analysed, respectively.

The SOP is studied under the condition that the licensed spectrum is detected to be unoccupied by the PU. In the case of $D = \varnothing$, no CR is chosen to forward the source signal and the outage happens. Therefore, the secure outage probability under the scheme can be expressed as

$$\begin{aligned} SOP^A = &\Pr(D=\varnothing|\hat{\mathrm{H}}=\mathrm{H}_0) \\ &+\sum_{n=1}^{2^N-1}\Pr(C_S^A<0, D=D_n|\hat{\mathrm{H}}=\mathrm{H}_0), \end{aligned} \quad (15)$$

By using the law of total probability rewrite (15) as

$$SOP^A = \underbrace{\sum_k\delta_k\prod_{i=1}^N P_{TR_i}^{\mathrm{H}_k}}_{SOP_{TR}}+\sum_k\delta_k\sum_{n=1}^{2^N-1}P_{R_i}^{A,\mathrm{H}_k}, \quad (16)$$

where, $k=\{0,1\}$, $P_{TR_i}^{\mathrm{H}_k} = \Pr(C_{T,R_i}<R|\mathrm{H}_k,\hat{\mathrm{H}}=\mathrm{H}_0)$ and $P_{R_i}^{A,\mathrm{H}_k} = \Pr(C_S^A<0, D=D_n|\mathrm{H}_k,\hat{\mathrm{H}}=\mathrm{H}_0)$.

The δ_k is given by [15]

$$\delta_k = \begin{cases}\dfrac{P_0\left(1-P_f\right)}{P_0\left(1-P_f\right)+\left(1-P_0\right)\left(1-P_d\right)}, k=0 \\ \dfrac{\left(1-P_0\right)\left(1-P_d\right)}{P_0\left(1-P_f\right)+\left(1-P_0\right)\left(1-P_d\right)}, k=1\end{cases}, \quad (17)$$

where, P_d and P_f are the successful detection probability and false alarm probability respectively. $P_0 = Pr\left(\mathrm{H}_0\right)$ is the probability that the authorised spectrum is not occupied.

By using (1), we can get the expression of the first item in (16) as

$$\mathrm{P}_{TR_i}^{H_k} = \Pr\left[\left|h_T^{R_i}\right|^2<\theta_s\left(\alpha\gamma_p\left|h_P^{R_i}\right|^2+1\right)\right], \quad (18)$$

with $\alpha=0$ when $k=0$, and $\alpha=1$ when $k=1$, $\theta_s = 2\left(2^{2R}-1\right)/\gamma_s$.

The Nakagami channel fading coefficient between the node a and the node b link is $h_{a\to b}$. The channels are i.d.d, let m_P, m_{PE}, m_M, m_E and σ_P^2, σ_{PE}^2, $\sigma_i^2(\sigma_D^2)$, σ_E^2 denote the Nakagami parameters in the link between PU and cognitive user, PU and eavesdropper, CT and CR$_i$ (CD), CT and eavesdropper, respectively. Then, we can arrive at

$$\mathrm{P}_{TR_i}^{H_0} = 1-E_i^{\theta_s}\sum_{k=0}^{m_M-1}C_{i,k}\theta_s^k, \quad (19)$$

$$\mathrm{P}_{TR_i}^{H_1} = 1-\Gamma_{Pi}E_i^{\theta_s}\sum_{k=0}^{m_M-1}\sum_{l=0}^{k}\binom{k}{l}\frac{C_{i,k}(\alpha\gamma_p\theta_s)^k\mu_P!}{\tau_i^{\mu_P+1}}. \quad (20)$$

where, $\Gamma_x = \frac{1}{\Gamma(m_x)}\left(m_x/\sigma_x^2\right)^{m_x}$, $\Gamma\left(\cdot\right)$ is the gamma function, $E_x = \exp\left(-\eta_x\right)$, $\eta_x = m_x/\sigma_x^2$, $C_{x,k} = \eta_x^k/k!$, $\mu_x = m_x + l - 1$, and $\tau_i = \eta_P + a\eta_i$. Fully details are in Appendix A.

By substituting (19) and (20) into (16), the unsuccessful decoded probability by CRs is SOP_{TR}. Since the secure capacities of $P_{R_i}^{A,\mathrm{H}_k}$ in (16) are different in each scheme, we will discuss them separately in the following.

$$P_{R_i}^{\text{RR-SC,H}_k} = \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\text{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\text{H}_k} \underbrace{\Pr\left[\frac{\left|h_{R_i}^{D}\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \max_j \left(\frac{\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2 \alpha\gamma_p + 1} \right) \right]}_{Q_1^{H_k}}, \tag{23}$$

$$\text{P}_{R_i}^{\text{RR-MRC,H}_k} = \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\text{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\text{H}_k} \underbrace{\Pr(\frac{\left|h_{R_i}^{D}\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \frac{\sum\limits_{j=1}^{M} \left|h_{R_i}^{E}\right|^2}{\left|h_P^{E_j}\right|^2 \alpha\gamma_p + 1})}_{Q_2^{\text{H}_k}}, \tag{27}$$

A. Single cognitive relay transmission scheme

1) RR-SCRT: In the RR-SCRT scheme, all cognitive relays in D_n transmit their decoded signals to the CD in turn. When CR_i transmits the signal to D, the total security outage probability $SOP_{R_i}^{\text{RR}}$ in the RR-SCR scheme is

$$SOP^{\text{RR}} = \frac{1}{|D_n|} \sum_{i=1}^{|D_n|} SOP_{R_i}^{\text{RR}}. \tag{21}$$

Each eavesdropper will first wiretap the signal forwarded by the CRs and then combine them to achieve the ultimate intercepting. The achievable capacities in the wiretap channels under the two combining techniques are different, which can be seen from (5) and (6), and result in the different security outage probabilities.

a) RR-SC-SCRT: In the RR-SC-SCRT scheme, when CR_i is selected to transmit the source signal to the CD, the security outage probability can be expressed as follows

$$SOP_{R_i}^{\text{RR-SC}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N - 1} P_{R_i}^{\text{RR-SC,H}_k}, \tag{22}$$

Under each condition of the status of PU, we can get the following results in (22) as shown in (23), where $\overline{P}_{TR_i}^{\text{H}_k} = 1 - P_{TR_i}^{\text{H}_k}$. It is recalling that $\alpha = 0$ when $k = 0$, $\alpha = 1$ when $k = 1$.

By using the results of Appendix B, we can obtain:

$$Q_1^{\text{H}_0} = 1 - \prod_{j=1}^{M} (1 - \sum_{k=0}^{m_E - 1} C_{E,k} \Gamma_D \mu_M! \tau_{B,0}^{-\mu_M - 1}), \tag{24}$$

$$Q_1^{\text{H}_1} = 1 - \prod_{j=1}^{M} [1 + \Gamma_{PE} \Gamma_P \mathfrak{E}_{\text{m}_E, \text{m}_M} \left(\Omega_{D,E} \right)], \tag{25}$$

where,

$$\Omega_{D,E} = \underset{q,r}{\Xi} \frac{(q+r)! \left[k_2 \text{-} \eta_D \text{-} \alpha\gamma_p \left(\mu_P + 1 \right) \left(q+r+1 \right) \left(\eta_E + \eta_D \right) \eta_D \right]}{\left(\eta_E + \eta_D \right)^{q+r+1}},$$

$$\underset{q,r}{\Xi} \left(\cdot \right) = \sum_q \binom{-\mu_{PE} - 1}{q} \sum_r \binom{-\mu_p - 1}{r} \frac{\eta_y^q \eta_x^r (\alpha\gamma_p)^{q+r}}{\eta_{PE}^{\mu_{PE}+q+1} \eta_P^{\mu_P + r + 1}} \left(\cdot \right)$$

and

$$\mathfrak{E}_{\varphi,\varsigma} \left(\cdot \right) = \sum_{k_1=0}^{\varphi - 1} \sum_{l_1=0}^{k_1} \binom{k_1}{l_1} \sum_{k_2=0}^{\varsigma - 1} \sum_{l_2=0}^{k_2} \binom{k_2}{l_2} \mu_{PE}! \mu_P! C_{E,k_1} C_{M,k_2} (\alpha\gamma_P)^{l_1 + l_2} \left(\cdot \right)$$

By substituting (22)−(25) into (21), we can get the SOP of the RR-SC SCRT scheme and rewrite as (26)

$$SOP^{\text{RR-SC}} = \frac{1}{|D_n|} \sum_{i=1}^{|D_n|} SOP_{R_i}^{\text{RR-SC}}. \tag{26}$$

b) RR-MRC-SCRT: In the RR-MRC-SCRT scheme, the eavesdropping system adopts the maximal ratio combine method to wiretap the information. When CR$_i$ is selected to transmit the source signal to the CD, we can get a similar expression as shown in (27). According to Appendix C, we can obtain:

$$Q_2^{\text{H}_0} = 1 - \frac{\eta_E^{Mm_E}}{\Gamma \left(Mm_E \right)} \sum_{k=0}^{m_M - 1} \frac{\mu_{M,E}! C_{D,k}}{\tau_{B,0}^{Mm_E + k}}, \tag{28}$$

where $\mu_{M,E} = Mm_E + k - 1$, and then

$$Q_2^{\text{H}_1} = 1 + \Gamma_P \Gamma_{PE} \mathfrak{E}_{Mm_E, m_M} \left(\Omega_{E,D} \right), \tag{29}$$

By substituting (19), (20), and (27) into (21), we can get the SOP of RR-MRC-SCRT scheme by rewriting (30)

$$SOP^{\text{RR-MRC}} = \frac{\sum\limits_{q=1}^{|D_n|} (SOP_{TR} + \sum\limits_k \delta_k \sum\limits_{n=1}^{2^N - 1} P_{R_i}^{\text{RR-MRC},H_k})}{|D_n|}. \tag{30}$$

2) O-SCRT: In the optimal single cognitive relay transmission scheme (O-SCRT), the optimal relay with the maximum security capacity in the successful decoding set of D_n is selected to forward the source signal to the CD, $C_S^{\text{O-SCRT}} = \max\limits_{R_i} \left(C_{S,R_i}^{\text{SCRT}} \right)$, with $C_{S,R_i}^{\text{SCRT}} = C_{M,R_i}^{\text{SCRT}} - C_{E,R_i}^{\text{SCRT}}$. According to (15), we can write the SOP in the O-SCRT scheme as follows

$$SOP^{\text{O-SCRT}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N - 1} P_{R_i}^{\text{O-SCRT,H}_k}. \tag{31}$$

$$P_{R_i}^{\text{O-SC},\mathrm{H}_k} = \prod_{R_i \in D_n} \overline{P}_{R_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{R_i}^{\mathrm{H}_k} \prod_{i=1}^{|D_n|} \underbrace{\Pr\left[\frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \max_j \left(\frac{\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2 \alpha\gamma_p + 1}\right)\right]}_{Q_3^{H_k}}. \tag{32}$$

$$P_{R_i}^{\text{O-MRC},\mathrm{H}_k} = \prod_{R_i \in D_n} \overline{P}_{R_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{R_i}^{\mathrm{H}_k} \prod_{i=1}^{|D_n|} \underbrace{\Pr\left(\frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \frac{\sum_{j=1}^{M}\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2 \alpha\gamma_p + 1}\right)}_{Q_4^{\mathrm{H}_k}}. \tag{34}$$

Similarly, each eavesdropper first wiretap the signal forwarded by the CR_s and then combine them to achieve the ultimate intercepting. We are assuming that the eavesdropper utilises SC and MRC techniques to combine the signals from each eavesdropper. The achievable capacities in the wiretap channels of C_{E,R_i}^{SCRT} under the two combining techniques are also different and result with the different SOP. Two schemes when the Optimal cognitive relay selection scheme is used, i.e., O-SC-SCRT and O-MRC-SCRT.

a) O-SC-SCRT: In the O-SC-SCRT scheme, the eavesdropping system uses SC to handle eavesdropping signals as in the RR-SC SCRT scheme. Therefore, we can get the following expressions as (32), where $Q_3^{\mathrm{H}_k} = Q_1^{\mathrm{H}_k}$. By substituting the results shown in (19), (20), (24) and (25), $P_{R_i}^{\text{O-SC},\mathrm{H}_k} = \Pr(\max_{R_i}(C_{S,R_i}^{\text{O-SC}}) < 0, D = D_n|\mathrm{H}_k, \hat{\mathrm{H}} = \mathrm{H}_0)$ and he closed form is in (32). Therefore, the secure outage probability of O-SC-SCRT scheme can be expressed as (33)

$$SOP^{\text{O-SC}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N-1} P_{R_i}^{\text{O-SC},\mathrm{H}_k}. \tag{33}$$

b) O-MRC-SCRT: In the O-MRC-SCRT scheme, the criteria for selecting an optimized relay are the same as for the O-SC-SCRT scheme. The difference is that the eavesdropping system uses the MRC method to process the eavesdropping signal. Then, With $Q_4^{H_k} = Q_2^{H_k}$, the results shown in (19)−(20) can easily obtain the closed form $P_{R_i}^{\text{O-MRC},\mathrm{H}_k} = \Pr(\max_{R_i}(C_{S,R_i}^{\text{O-MRC}}) < 0, D = D_n|\mathrm{H}_k, \hat{\mathrm{H}} = \mathrm{H}_0)$, which is in (34). Therefore, the secure outage probability of O-MRC-SCRT scheme as (35).

$$SOP^{\text{O-MRC}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N-1} P_{R_i}^{\text{O-MRC},\mathrm{H}_k}. \tag{35}$$

3) SO-SCRT: In the sub-optimal SCRT scheme, does not need to know the knowledge of the eavesdropping channels and select the optimal cognitive relay by maximising the channel capacity of main link as shown in (8). According to (15), The secure outage probability in the SO-SCRT scheme can be written as follows

$$SOP^{\text{SO-SCRT}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N-1} P_{R_i}^{\text{SO-SCRT},\mathrm{H}_k}. \tag{36}$$

Each eavesdropper first wiretap the signal forwarded by the CR$_s$ and then combine them to achieve the ultimate intercepting. The eavesdropper utilises SC and MRC techniques to combine the signals from each eavesdropper. The achievable capacities in the wiretap channels under the two combining techniques are also different and result in different security outage probabilities. Similar to the above analysis, it can get specific outage probabilities in the SO-SC and SO-MRC scheme as shown in (37) and (38) respectively.

$$\begin{aligned} P_{R_i}^{\text{SO-SC},\mathrm{H}_k} &= \Pr(C_S^{\text{SO-SC}} < 0, D{=}D_n|\mathrm{H}_k, \hat{\mathrm{H}}{=}\mathrm{H}_0) \\ &= \Pr(\max_{R_i} C_{M,R_i}^{\text{SO-SC}} < C_{E,R_{sub}}^{\text{SO-SC}}, D = D_n|\mathrm{H}_k, \hat{\mathrm{H}} = \mathrm{H}_0) \\ &= \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\mathrm{H}_k} Q_5^{H_k}, \end{aligned} \tag{37}$$

$$\begin{aligned} P_{R_i}^{\text{SO-MRC},\mathrm{H}_k} &= \Pr(C_S^{\text{SO-MRC}} < 0, D{=}D_n|\mathrm{H}_k, \hat{\mathrm{H}} = \mathrm{H}_0) \\ &= \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\mathrm{H}_k} Q_6^{\mathrm{H}_k}. \end{aligned} \tag{38}$$

where $Q_5^{\mathrm{H}_k}{=}\Pr[\max_{R_i}(\frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2\alpha\gamma_p+1}) < \max_j(\frac{\left|h_{R_{sub}}^{E_j}\right|^2}{\left|h_P^E\right|^2\alpha\gamma_p+1})]$ and $Q_6^{\mathrm{H}_k}{=}\Pr[\max_{R_i}(\frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2\alpha\gamma_p+1}) < \frac{\sum_{j=1}^{M}\left|h_{R_{sub}}^{E_j}\right|^2}{\left|h_P^E\right|^2\alpha\gamma_p+1}]$.

It is noted that it is challenging to obtain the closed-form of (37) and (38). However, we can obtain the numerical secure outage probability results with the aid of computer simulations.

B. Multiple cognitive relay transmission scheme

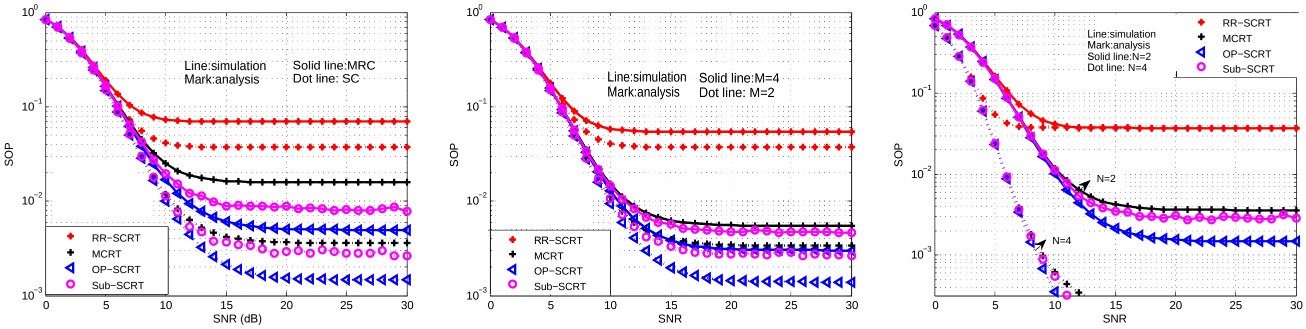
In the MCRT scheme, all of the cognitive relays that can correctly decode the source signals transmit their decoded estimated signals to the destination. The security outage probability of the MCR scheme can be expressed as

$$SOP^{\text{MCRT}} = SOP_{TR} + \sum_k \delta_k \sum_{n=1}^{2^N-1} P_S^{\text{MCRT},H_k}. \tag{39}$$

Further, the expressions for (39) in the MCRT-SC (the eavesdropper uses the SC technique to combine the intercepted signals) and MCRT-MRC (the eavesdropper uses the MRC

$$Q_7^{\mathrm{H}_0} = 1 - \prod_{j=1}^{M}\left[1 - \frac{1}{\Gamma\left(|D_n| m_M\right)}\eta_D^{|D_n| m_M} \sum_{k=0}^{|D_n| m_E - 1} C_{E,k}\left(k + |D_n| m_M - 1\right)!(\eta_D + \eta_E)^{-k - |D_n| m_M}\right], \tag{44}$$

$$Q_8^{\mathrm{H}_0} = 1 - \left[\frac{1}{\Gamma\left(|D_n| M m_E\right)}\eta_E^{|D_n| M m_E} \sum_{k=0}^{M m_M - 1} C_{D,k}\left(|D_n| M m_E - 1 + k\right)!(\eta_D + \eta_E)^{-|D_n| M m_E - k}\right]. \tag{45}$$



(a) SC and MRC scheme at eavesdropper.

(b) SC at eavesdropper with different M.

(c) SC at eavesdropper with different N.

Fig. 2: SOP vs. SNR under different relay schemes.

technique to combine the intercepted signals) schemes are shown in (40) and (41) respectively.

$$\begin{aligned} P_S^{\text{MCRT-SC}}, H_k &= \Pr\left(C_S^{\text{MCRT-SC}} < 0, D = D_n | \mathrm{H_k}, \hat{\mathrm{H}} = \mathrm{H}_0\right) \\ &= \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\mathrm{H}_k} Q_7^{H_k} \qquad , \end{aligned} \tag{40}$$

$$\begin{aligned} P_S^{\text{MCRT-MRC}, H_k} &= \Pr\left(C_S^{\text{MCRT-MRC}} < 0, D = D_n | \mathrm{H_k}, \hat{\mathrm{H}} = \mathrm{H}_0\right) \\ &= \prod_{R_i \in D_n} \overline{P}_{TR_i}^{\mathrm{H}_k} \prod_{R_i \in \bar{D}_n} P_{TR_i}^{\mathrm{H}_k} Q_8^{H_k} \qquad , \end{aligned} \tag{41}$$

where $Q_7^{H_k} = \Pr(\sum_{i=1}^{|D_n|} \frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \max_j \frac{\sum_{i=1}^{|D_n|}\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2 \alpha\gamma_p + 1})$ and $Q_8^{H_k} = \Pr(\frac{\sum_{i=1}^{|D_n|}\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2 \alpha\gamma_p + 1} < \frac{\sum_{j=1}^{M}\sum_{i=1}^{|D_n|}\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2 \alpha\gamma_p + 1})$.

Where, by using the results of Appendix D, we can get $Q_7^{H_k}$ and $Q_8^{H_k}$ in (40) and (41) at the bottom of this page.

$$Q_7^{\mathrm{H}_1} = 1 - \prod_{j=1}^{M}\left(1 + \Gamma_P \Gamma_{PE} \mathfrak{E}_{M m_E, M m_M}\left(\Omega_{D,E}\right)\right), \tag{42}$$

$$Q_8^{\mathrm{H}_1} = 1 + \Gamma_P \Gamma_{PE} \mathfrak{E}_{|D_n| m_M, |D_n| M m_E - 1}\left(\Omega_{D,E}\right), \tag{43}$$

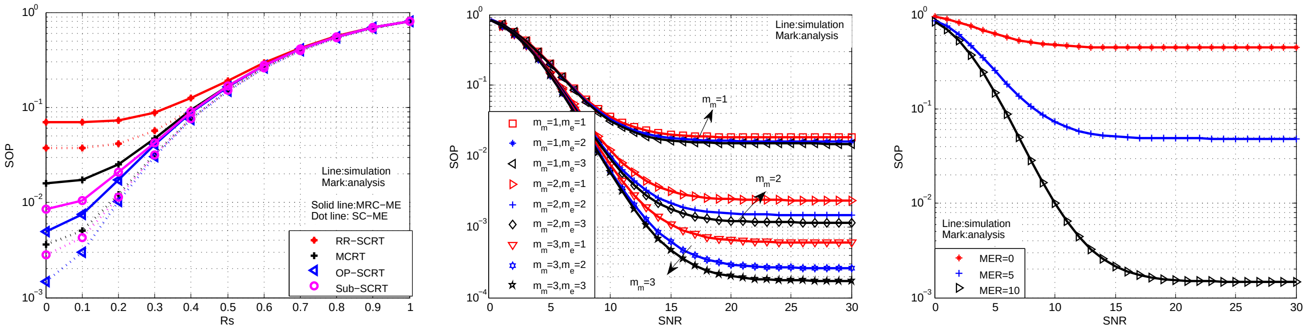
V. Simulation Results

In the simulation, the parameters are set as: $\sigma_{R_i}^2 = \sigma_D^2 = \sigma_{PD}^2 = \sigma_m^2$, $\sigma_{E_j}^2 = \sigma_{PE_j}^2 = \sigma_e^2$, where σ_m^2 and σ_e^2 are the average channel gains of the main link and the eavesdropping link, respectively. In addition, we define $\lambda_{me} = \frac{\sigma_m^2}{\sigma_e^2}$ as the main-to-eavesdropper ratio (MER). Unless otherwise stated, the other parameters are set as $P_f = 0.01$, $P_d = 0.99$, $\gamma_p = 5$, $P_0 = 0.8$, $\sigma_m^2 = 0$, $\sigma_e^2 = -10$, and codeword rate $R = 0.5$.

In Fig. 2(a), the SOP vs transmit signal to noise ratio (SNR) of the considered schemes are shown. $N = 2$, $M = 2$. It can be seen that with the increase of SNRs, the SOP of all schemes decreases. The proposed O-SC scheme can achieve the best SOP. It also can be seen that when the SOP is 10^{-2}, the difference between the Opt-MRC scheme and Sub-MRC schemes is about 3 dB, while the difference between Opt-SC and Sub-SC schemes is about 0.5 dB. In the Opt-SCR scheme, when the SOP is 10^{-2}, the SNRs difference is 2dB when SC and MRC were used respectively to wiretap the signals. In other words, when considering the worst case that the eavesdropper utilises MRC to wiretap the signals, it needs a 2dB channel gain than that by SC scheme to achieve the SOP of 10^{-2}. However, in the Sub-SCR scheme, the same difference is about 4dB, which means that the eavesdropper utilises MRC to wiretap the signals. It needs a 4dB channel gain than that by SC scheme to achieve the SOP of 10^{-2}.

In Fig. 2(b), the SOP vs SNRs with a different number of eavesdroppers under the RR-SC scheme, Opt-SC, Sub-SC, and SC-MCR, are shown in Figure 3. It can be seen that when the SOP is $10^{-2.5}$, there is a 1dB difference between the SNR when M increases from 2 to 4 in the Opt-SC scheme, and 5dB in the Sub-SC scheme.

In Fig. 2(c), the SOP vs SNRs with a different number of cognitive relays under the RR-SC scheme, Opt-SC, Sub-SC, and SC-MCR are shown. It can be seen that the number of cognitive relays does not affect the SOP in the RR-SC scheme. It also can be seen that when the SOP is 10^{-2}, there is a 4dB SNRs difference if N increases from 2 to 4 in the Sub-SC scheme or SC-SCR. The SOP decreases fastest when the



(a) SOP vs. R_s.

(b) SOP vs. SNR with different fading conditions.

(c) SOP vs. SNR with different MER.

Fig. 3: SOP performance with rate, fading and MER.

number of relay increases in the Opt-SC scheme. When the SOP is $10^{-2.5}$, there is a 6dB SNRs difference if N increases from 2 to 4 in the Opt-SC scheme. When N=4, the lowest SOP can be obtained by the Opt-SC scheme.

The SOP vs target data rate (R_s) under considered schemes are shown in Fig 3(a). It can be seen that with the increase of R_s, SOP of all schemes increases. When the R_s tends to one, SOP of all schemes tends to a constant value. Because when R_s approaches 1, it is challenging for cognitive relays to decode the source signal correctly. i.e. $\Pr\left(D=\varnothing\right)$. The transmission of the second slot does not continue. However, the criteria for choosing transmission relay in different relay selection schemes are based on the second time slot. Therefore, four relay selection methods tend to the same value when the R_s is too large.

In Fig. 3(b), we studied the influence of different m values in Nakagami-m fading vs the secure performance in the Opt-SC scheme. It can be seen from the figure that the improvement of the system performance is proportional to the parameter m. That is, increasing the value m can greatly reduce the outage probability of the system. When the SOP is $10^{-1.7}$, there is a 6 dB SNRs difference if m_m increases from 1 to 2 when the $m_e=1$. When the SOP is 10^{-3} , there is a 3 dB difference if m_m increases from 1 to 2 when the $m_e=3$. There is about 4 dB difference if m_e increases from 1 to 3 when the $m_m=3$. It can be concluded from the figure that the larger m_m is, the larger m_e can reduce the security performance of the system to a greater extent.

In Fig. 3(c), the SOP vs SNRs with different MER under Opt-SC scheme. As can be seen from the figure, the outage probability decreases with the MER increasing. Because the increase of MER represents the increase of the ratio of the main channel to the eavesdropping channel, the increase of the main channel or the decrease of the eavesdropping channel leads to increased security capacity. Therefore, the outage probability decreases and the outage probability decreases faster when MER equal 10 dB than when MER equal 5 dB. The SNR is equal to 10 dB, the outage probability of OP-SC-ME-SCR scheme when the MER equivalent 0dB is $10^{-0.5}$. The outage probability of the OP-SC-ME-SCR scheme when the MER equal 5 dB is $10^{-1.2}$. The outage probability of OP-SC-ME-SCR scheme when the MER equivalent 10 dB is 10^{-2}. Therefore, adding MER can improve physical layer security.

VI. Conclusion and Further Research

In this paper, the PLS performance with multi-eavesdropper of a cooperative cognitive relay network for the IIoT is studied. In the eavesdropping cognitive IIoT communication scenario, the communication security defined as SOP is analysed for both relay schemes, i.e. SCRT and MCRT. The eavesdropper system utilises the two combining technologies, i.e. SC and MRC, to get the final intercept signals. The results show that the security outage performance of Opt-SC is optimal compared with the rest, no matter whatever the combining technologies are used on the eavesdropper side. Also, the SOP can be greatly reduced by utilising SC than by MRC in a high SNR regime. However, the eavesdropper system should try its best to intercept the legitimate transmission to use MRC in the actual scenario. Consequently, combating eavesdropping effectively and improving the secure transmission performance when considering the worst scenario needs further investigation. Our further research will explore how the mobility of IoT devices affects the PLS [32] and the balance between network reliability and throughput [33].

Appendix A

We define the random variable of X_i as independent identical Nakagami distribution, and the corresponding PDF and CDF can be expressed as

$$f_{X_i}\left(x\right)=\frac{1}{\Gamma\left(m\right)}\left(\frac{m}{\sigma^2}\right)^m x^{m-1}\exp\left(-\frac{mx}{\sigma^2}\right), \tag{A.1}$$

$$F_{X_i}\left(x\right)=1-\exp\left(-\frac{mx}{\sigma^2}\right)\sum_{k=0}^{m-1}\frac{x^k}{k!}\left(\frac{m}{\sigma^2}\right)^k. \tag{A.2}$$

To obtain the results of (18), we first need to calculate the following probability. By using (A.1) and (A.2), we arrive at

$$\begin{aligned}&\Pr\left(X_1\le aX_2+b\right)\\&=\int_0^\infty F_{X_1}\left(ax+b\right)f_{X_2}\left(x\right)dx=1-\Gamma_2E_1^b\sum_{k=0}^{m_1-1}\eta_1^kI_A,\end{aligned} \tag{A.3}$$

where, $I_A = \int_0^\infty \frac{(ax+b)^k}{k!} x^{m_2-1} \exp(-\tau_0 x)\, dx$, $\tau_0 = \eta_2 + a\eta_1$.

By using binomial expansion, and $\int_0^\infty x^n \exp(-\mu x) dx = n!\mu^{-n-1}$, after some manipulations, we can rewrite I_A in (A.3) as

$$I_A = \frac{1}{k!} \sum_{l=0}^{k} \binom{k}{l} a^l b^{k-l} \mu_x! \tau_0^{-\mu_x - 1}. \tag{A.4}$$

By substituting corresponding parameters for m_1, m_2, σ_1^2 and σ_2^2, i.e. if the channel is from CBS to CR_i and CD, the corresponding parameters are m_M and $\sigma_i^2\left(\sigma_D^2\right)$, m_E and σ_{E}^2 for the channel between CBS and Eve, $m_{Pi}\left(m_P\right)$ and σ_{P}^2 for the channel between PU and CR_i and CD, and m_{PE} and σ_{PE}^2 for the channel between PU and Eve; (19) and (20) can be easily obtained.

Appendix B

Let $V_j = \left|h_{R_i}^{E_j}\right|^2$ with Nakagami parameters m_E and σ_E^2, $X = \left|h_{R_i}^{D}\right|^2$ with Nakagami parameters m_M and σ_D^2. To obtain (24),

$$\begin{aligned} &\Pr\left\{X < \max_j (V_j)\right\} = 1 - \Pr\left\{\max_j (V_j) < X\right\} \\ &= 1 - \prod_{j=1}^{M} \underbrace{\int_0^\infty F_{V_j}(x)\, f_X(x)\, dx}_{I_{B_1}}. \end{aligned} \tag{B.1}$$

Then, using (A.1) and (A.2), after some manipulations, we can get the expression of

$$I_{B_1} = 1 - \sum_{k=0}^{m_E - 1} C_{E,k} \Gamma_D \mu_M! \tau_{B,0}^{-\mu_M - 1}, \tag{B.2}$$

where $\mu_M = m_M + k - 1$, $\tau_{B,0} = \eta_D + \eta_E$, $C_{E,k} = \frac{\eta_E^k}{k!}$.

By substituting (B.2) into (B.1), we can get the expression of (24).

To obtain (25), we define $Y = X_1 / (aX_2 + 1)$, the random variables X_1 and X_2 obey Nakagami distribution, and their probability density function (PDF) is formula (1). The CDF of Y can be expressed as

$$F_Y(y) = \Pr\left(X_1 \le y\left(aX_2 + 1\right)\right) \tag{1}$$

$$= 1 - \Gamma_2 \sum_{k=0}^{m_1 - 1} \sum_{l=0}^{k} \binom{k}{l} \mu_2! a^l C_{1,k} \Psi_{k,l}^{B,1}(y), \tag{B.3}$$

where, $\tau_{B1} = \eta_2 + \eta_1 a y$, $\Psi_{k,l}^{B,1}(y) = y^k E_1^y \tau_{B1}^{-\mu_2 - 1}$.

By implementing differentiation to (1), we can obtain the PDF expression of Y as follows

$$f_Y(y) = -\Gamma_2 \sum_{k=0}^{m_1 - 1} \sum_{l=0}^{k} \binom{k}{l} \mu_2! a^l C_{1,k} \Psi_{k,l}^{B,2}(y). \tag{B.4}$$

where, $\Psi_{k,l}^{B,2}(y) = y^{k\text{-}1} E_1^y \tau_{B,1}^{-\mu_2}\left(k - \eta_1 a y\left(\mu_2 + 1\right) - \eta_1\right)$.

Let $Y_{1\mathrm{j}} = \left|h_{R_q}^{E_j}\right|^2 / (\alpha\gamma_p \left|h_P^E\right|^2 + 1)$, and $Y_2 = \left|h_{R_q}^{D}\right|^2 / (\alpha\gamma_p \left|h_P^D\right|^2 + 1)$, we denote the corresponding parameters in (B.4) as: m_E, m_{PE} and σ_E^2, σ_{PE}^2 from the CS and PU to the eavesdropper, m_M, m_P and $\sigma_R^2\left(\sigma_D^2\right)$, σ_P^2 from the CS and PU to the CR(CD). Using (1) and (B.4), we can get the CDF and PDF as

$$F_{Y_{1j}}(y) = 1 - \Gamma_{PE} \sum_{k_1=0}^{m_E - 1} \sum_{l_1=0}^{k_1} \binom{k_1}{l_1} \mu_{PE}! (\alpha\gamma_p)^{l_1} C_{E,k_1} \Psi_{k_1,l_1}^{B,E}(y), \tag{B.5}$$

$$f_{Y_2}(y) = -\Gamma_P \sum_{k_2=0}^{m_M - 1} \sum_{l_2=0}^{k_2} \binom{k_2}{l_2} \mu_P! (\alpha\gamma_P)^{l_2} C_{M,k_2} \Psi_{k_2,l_2}^{B,M}(y), \tag{B.6}$$

where, $\Psi_{k_1,l_1}^{B,E}(y) = y^{k_1} E_E^y \tau_{B,E}^{-\mu_{PE} - 1}$, $\Psi_{k_2,l_2}^{B,M}(y) = \frac{\left(k_2 - \eta_D y - \alpha\gamma_p y \eta_D (\mu_P + 1)\tau_{B,M}^{-1}\right)}{y^{1-k_2} E_D^{-y} \tau_{B,M}^{\mu_P + 1}}$, $\mu_{PE} = m_{PE} + l_1 - 1$, $\mu_P = m_P + l_2 - 1$, $\tau_{B,M} = \eta_P + \alpha\gamma_p \eta_D y$, and $\tau_{B,E} = \eta_{PE} + \alpha\gamma_p \eta_E y$.

By the following derivation, we can obtain the results of formula (25).

$$\begin{aligned} Q_1^{\mathrm{H}_1} &= 1 - \Pr\left(\max_j (Y_{1j} < Y_2)\right) \\ &= 1 - \prod_{j=1}^{M} \underbrace{\int_0^\infty F_{Y_{1j}}(y)\, f_{Y_2}(y) dy.}_{I_{B_2}} \end{aligned} \tag{B.7}$$

By substituting (B.5) and (B.6) into (B.7), we can get

$$I_{B_2} = 1 + \Gamma_{PE} \Gamma_P \mathfrak{C}_{\mathrm{m}_E, \mathrm{m}_M} \left(\underbrace{\int_0^\infty \Psi_{k_1,l_1}^{B,E}(y)\, \Psi_{k_2,l_2}^{B,M}(y)\, dy}_{\Omega_{D,E}} \right). \tag{B.8}$$

By substituting (B.6) and (B.7) into (B.5), using the expression of $(a + bx)^{-n} = \sum_{v=0}^{\infty} \binom{-n}{v} a^v (bx)^{-n-v}$, we can get the results of $\Omega_{D,E}$ and finally obtain the expression of (25).

Appendix C

Random variables $V_{i,1}, V_{i,2} \ldots V_{i,M}$ is independent and identically distributed and obeys Nakagami-m fading. $V_{i,j} \sim \Gamma\left(m_{v_{i,j}}, m_{v_{i,j}} / \sigma_{v_{i,j}}^2\right)$, then, the sum of them $\sum_{j=1}^{M} V_{i,j} = V_{i,1} + V_{i,2} + \cdots + V_{i,M} \sim \Gamma\left(M m_{v_i}, m_{v_i} / \sigma_{v_i}^2\right)$, the PDF and CDF of $V_i = \sum_{j=1}^{M} \left|h_{a_i}^{b_j}\right|^2$ is

$$f_{V_i}(v_i) = \frac{\exp\left(-\frac{m_{a_i}^b v_i}{\sigma_{a_i b}^2}\right)}{\Gamma\left(M m_{a_i}^b\right)} \left(\frac{m_{a_i}^b}{\sigma_{a_i b}^2}\right)^{M m_{a_i}^b} {v_i}^{M m_{a_i}^b - 1}, \tag{C.1}$$

$$F_{V_i}(v_i) = 1 - \exp\left(-\frac{m_{a_i}^b v_i}{\sigma_{a_i b}^2}\right) \sum_{k=0}^{M m_{a_i}^b - 1} \frac{{v_i}^k}{k!} \left(\frac{m_{a_i}^b}{\sigma_{a_i b}^2}\right)^k. \tag{C.2}$$

By using (A.2), (C.1), and assuming i.d.d., we can easily get $Q_2^{\mathrm{H}_0}$.

We define $W = \sum_{j=1}^{M} X_{1j} / (aX_2 + 1)$, the random variables X_{1j} and X_2 obey Nakagami distribution, and their probability density function (PDF) is formula (A.1), (C.1). The PDF and CDF of W can be expressed as

$$F_W\left(w\right)=\Pr\left(\sum_{j=1}^{M}X_{1j}<w\left(aX_2+1\right)\right)$$
$$=1-\Gamma_2\sum_{k=0}^{Mm_1-1}C_{1,k}\mu_2!\sum_{l=0}^{k}\binom{k}{l}\frac{a^k w^{k+l}E_1^w}{\tau_{C,1}^{\mu_2+1}}. \tag{C.3}$$

By implementing differentiation to (C.3), we can obtain the PDF expression of W as follows

$$f_W\left(w\right)=-\Gamma_2\sum_{k=0}^{Mm_1-1}C_{1,k}\mu_2!\sum_{l=0}^{k}\binom{k}{l}a^k\Psi_{k,l}^{C,0}\left(w\right). \tag{C.4}$$

where, $\Psi_{k,l}^{C,0}\left(w\right)$=$w^{k+l-1}E_1^w\tau_{C,1}^{-\mu_2-1}\left[k-\eta_1 w\text{+}\eta_1 aw(-\mu_2-1)\tau_{C,1}^{-1}\right]$, $\tau_{C,1}=\eta_2+\eta_1 aw$. By using (C.4), the expression of $Q_2^{\mathrm{H}_1}$ can be easily obtained.

Appendix D

Let $X=\sum\limits_{q=1}^{|D_n|}\left|h_{R_q}^D\right|^2$, $V_j=\sum\limits_{q=1}^{|D_n|}\left|h_{R_q}^{E_j}\right|^2$, according to the method of Appendix C, we arrive at

$$Q_7^{\mathrm{H}_0}\text{=}1-\Pr\left(\max_j\sum_{q=1}^{|D_n|}\left|h_{R_q}^{E_j}\right|^2<\sum_{q=1}^{|D_n|}\left|h_{R_q}^{D}\right|^2\right)$$
$$\text{=}1-\prod_{j=1}^{M}\left(1-\frac{\eta_D^{(|D_n|)m_M}}{\Gamma\left(|D_n|\right)m_M}\sum_{k=0}^{|D_n|m_E-1}\frac{C_{E,k}(\mathscr{K}-1)!}{\left(\eta_D+\eta_E\right)^{\mathscr{K}}}\right). \tag{D.1}$$

where $\mathscr{K}=k+\left(|D_n|\right)m_M$.

Let $W=\sum\limits_{i=1}^{|D_n|}\frac{\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2\gamma_p+1}$ and $W_E=\max\limits_j\frac{\sum_{i=1}^{|D_n|}\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2\gamma_p+1}$, we arrive at

$$Q_7^{\mathrm{H}_1}=1-\Pr\left(\max_j W_E<W\right)$$
$$=1-\prod_{j=1}^{M}\underbrace{\int_0^\infty f_{W_E}\left(w\right)F_W\left(w\right)dw.}_{I_D} \tag{D.2}$$

According to Appendix B, we can get I_D=1+$\Gamma_P\Gamma_{PE}\mathfrak{E}_{Mm_E,Mm_M}\left(\Omega_{D,E}\right)$. Then, $Q_7^{H_1}$ can be easily obtained.

Appendix E

Random variables $V_{1,1},V_{1,2}\ldots V_{i,j},\ldots V_{V,M}$ is independent and identically distributed and obeys Nakagami-m fading. $V_{i,j}\sim\Gamma\left(m_{v_{i,j}},m_{v_{i,j}}/\sigma_{v_{i,j}}^2\right)$, then, $\sum_{i=1}^{|D_n|}\sum_{j=1}^{M}V_{i,j}\sim\Gamma\left(|D_n|Mm_v,m_v/\sigma_v^2\right)$, the PDF and CDF of $V=\sum_{i=1}^{|D_n|}\sum_{j=1}^{M}V_{i,j}$ can be obtained similar to (C.1) and (C.2). Then, the expression of (45) can be easily obtained.

We define $R=\left(aX+1\right)^{-1}\sum_{j=1}^{M}\sum_{i=1}^{|D_n|}X_{i,j}$, the random variables $X_{i,j}$ and X_2 obey Nakagami distribution, and their probability density function (PDF) is formula (A.1). The PDF and CDF of R can be expressed as

$$F_R\left(\kappa\right)=\Pr\left(\sum_{j=1}^{M}\sum_{i=1}^{|D_n|}X_{ij}<\kappa\left(aX+1\right)\right)$$
$$=1\text{-}\Gamma_2E_1^\kappa\sum_{k=0}^{|D_n|Mm_1-1}\sum_{l=0}^{k}\binom{k}{l}\frac{C_{1,k}\mu_2!a^l\kappa^k}{\left(\eta_2+\eta_1 a\kappa\right)^{\mu_2+1}}. \tag{E.3}$$

By implementing differentiation to (E.3), we can obtain the PDF expression of R as follows

$$f_R\left(\kappa\right)=-\Gamma_2E_1^k\sum_{k=0}^{(|D_n|)Mm_1-1}\sum_{l=0}^{k}\binom{k}{l}C_{1,k}\mu_2!a^l\kappa^{k^{k-1}}\tau_E^{-\mu_2-1}$$
$$\times\left(\kappa^k-\eta_1\kappa^k+\eta_1 a\kappa^k\left(-\mu_2-1\right)\tau_E^{-1}\right). \tag{E.4}$$

where τ_E=$\eta_2+\eta_1 a\kappa$.

Let $W=\frac{\sum_{i=1}^{|D_n|}\left|h_{R_i}^D\right|^2}{\left|h_P^D\right|^2\gamma_p+1}$, $R_E=\frac{\sum_{j=1}^{M}\sum_{i=1}^{|D_n|}\left|h_{R_i}^{E_j}\right|^2}{\left|h_P^E\right|^2\gamma_p+1}$. $Q_8^{\mathrm{H}_1}$ can be easily obtained by using the same method to get I_{B_2} in (B.7).

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[2] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78 238–78 259, 2018.

[3] C. Zhu, J. J. Rodrigues, V. C. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 16–22, 2018.

[4] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE personal communications*, vol. 6, no. 4, pp. 13–18, 1999.

[5] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 17–25, 2017.

[6] A. Ali, L. Feng, A. K. Bashir, S. El-Sappagh, S. H. Ahmed, M. Iqbal, and G. Raja, "Quality of service provisioning for heterogeneous services in cognitive radio-enabled internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 328–342, 2020.

[7] F. Li, K.-Y. Lam, X. Li, Z. Sheng, J. Hua, and L. Wang, "Advances and emerging challenges in cognitive internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5489–5496, 2020.

[8] X. Liu and X. Zhang, "Noma-based resource allocation for cluster-based cognitive industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 8, pp. 5379–5388, 2020.

[9] M. Li, H. Yuan, X. Yue, S. Muhaidat, C. Maple, and M. Dianati, "Secrecy outage analysis for alamouti space-time block coded non-orthogonal multiple access," *IEEE Communications Letters*, vol. 24, no. 7, pp. 1405–1409, 2020.

[10] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[11] J. Zou, H. Xiong, D. Wang, and C. W. Chen, "Optimal power allocation for hybrid overlay/underlay spectrum sharing in multiband cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1827–1837, 2012.

[12] 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.

[13] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE journal on selected areas in communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[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, 2013.

[15] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, “Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 3930–3941, 2016.

[16] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, “Secure multiuser communications in multiple amplify-and-forward relay networks,” *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3299–3310, 2014.

[17] D.-D. Tran, N.-S. Vo, T.-L. Vo, and D.-B. Ha, “Physical layer secrecy performance of multi-hop decode-and-forward relay networks with multiple eavesdroppers,” in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2015, pp. 430–435.

[18] C. Tang, G. Pan, and T. Li, “Secrecy outage analysis of underlay cognitive radio unit over nakagami-m fading channels,” *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[19] P. Yan, Y. Zou, and J. Zhu, “Energy-aware multiuser scheduling for physical-layer security in energy-harvesting underlay cognitive radio systems,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 3, pp. 2084–2096, 2017.

[20] Z. Shang, T. Zhang, G. Hu, Y. Cai, and W. Yang, “Secure transmission for noma-based cognitive radio networks with imperfect csi,” *IEEE Communications Letters*, vol. 25, no. 8, pp. 2517–2521, 2021.

[21] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, “Secrecy performance analysis of cognitive decode-and-forward relay networks in nakagami-m fading channels,” *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2016.

[22] S. Jia, J. Zhang, H. Zhao, Y. Lou, and Y. Xu, “Relay selection for improved physical layer security in cognitive relay networks using artificial noise,” *IEEE Access*, vol. 6, pp. 64 836–64 846, 2018.

[23] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, and J. Wang, “Security-reliability tradeoff analysis for underlay cognitive two-way relay networks,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 6030–6042, 2019.

[24] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, “Securing physical-layer communications for cognitive radio networks,” *IEEE Communications Magazine*, vol. 53, no. 9, pp. 48–54, 2015.

[25] D. Wang, W. Liang, X. Hu, D. Zhai, and D. Zhang, “Cooperative privacy provisioning for energy harvesting based cognitive multi-relay networks,” *China Communications*, vol. 17, no. 2, pp. 125–137, 2020.

[26] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, “Artificial noise aided secure cognitive beamforming for cooperative miso-noma using swipt,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 918–931, 2018.

[27] Y. Jiang, Y. Zou, J. Ouyang, and J. Zhu, “Secrecy energy efficiency optimization for artificial noise aided physical-layer security in ofdm-based cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 11 858–11 872, 2018.

[28] P. Chen, J. Ouyang, W.-P. Zhu, M. Lin, A. E. Shafie, and N. Al-Dhahir, “Artificial-noise-aided energy-efficient secure beamforming for multi-eavesdroppers in cognitive radio networks,” *IEEE Systems Journal*, vol. 14, no. 3, pp. 3801–3812, 2020.

[29] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2014.

[30] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, “Relay selection for security enhancement in cognitive relay networks,” *IEEE wireless communications letters*, vol. 4, no. 1, pp. 46–49, 2014.

[31] X. Ding, T. Song, Y. Zou, and X. Chen, “Improving secrecy for multi-relay multi-eavesdropper wireless systems through relay selection,” *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 7, pp. 982–991, 2016.

[32] M. Li, X. Yang, F. Khan, M. A. Jan, W. Chen, and Z. Han, “Improving physical layer security in vehicles and pedestrians networks with ambient backscatter communication,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2022.

[33] J. Tang, H. Wen, H. Song, T. Zhang, and K. Qin, “On the security–reliability and secrecy throughput of random mobile user in internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 635–10 649, 2020.

Meiling Li is a Professor with the School of Electronics Information Engineering, Taiyuan University of Science and Technology (TYUST), China. She was also a Visiting Scholar at the University of Warwick, U.K and Tsinghua University. Her research interests include cognitive radio, V2X, cooperative communications, non-orthogonal multiple access, and physical layer security technology. She received M. S. and Ph.D degrees in signal and information processing from the Beijing University of Posts and Telecommunications, Beijing, in 2007 and 2012, respectively.

Hu Yuan is a research fellow in the University of Warwick, where his research focus on the security and privacy aspects of IoT, including internet of bio-nano things, vehicular communication networks, user behaviours identification and further space system. Hu involves several national research Hubs such as the PETRAS Cybersecurity of the Internet of Things Research Hub and Future AI and Robotics for Space (FAIRSPACE) Hub. He was invited to the House of Lord to present the IoT’s cyber security research findings. He was the leading researcher for the project IoT-Tram (IoT Transport and Mobility Demonstrator) the first real word cyber security test in the UK.

Carsten Maple is the Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research at the University and Professor of Cyber Systems Engineering in WMG. He is also a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. He is a Fellow of the Alan Turing Institute, the National Institute for Data Science and AI in the UK, where he is a principal investigator on a $ 5 million project developing trustworthy national identity to enable financial inclusion.

Ying Li received her M.Sc degree in electronic communication engineering from Taiyuan University of Science and Technology.

Osama Alluhaibi joined university of Kirkuk as a head of Electrical engineering department in Sep. 2019. His research interests include hybrid beamforming, performance analysis of 5G millimeter-wave wireless communications systems, and 5 G millimeter-wave communication for Industrial Internet of Things applications. From 2007 to 2010, he was associated with ABB Group, and Kalimat Telecom. In July 2018, he joined the Connectivity Group, WMG’s Intelligent Vehicles Research Team, University of Warwick, U.K., as a Research Fellow.