SCIENCE CHINA
Information Sciences

• REVIEW •

February 2020, Vol. 63 121301:1–121301:12
https://doi.org/10.1007/s11432-019-2650-4

Physical layer security for massive access in cellular Internet of Things

Qiao QI, Xiaoming CHEN*, Caijun ZHONG & Zhaoyang ZHANG

College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027*, China*

Received 19 June 2019/Revised 6 August 2019/Accepted 18 September 2019/Published online 15 January 2020

Abstract The upcoming fifth generation (5G) cellular network is required to provide seamless access for a massive number of Internet of Things (IoT) devices over the limited radio spectrum. In the context of massive spectrum sharing among heterogeneous IoT devices, wireless security becomes a critical issue owing to the broadcast nature of wireless channels. According to the characteristics of the cellular IoT network, physical layer security (PHY-security) is a feasible and effective way of realizing secure massive access. This article reviews the security issues in the cellular IoT network with an emphasis on revealing the corresponding challenges and opportunities for the design of secure massive access. Furthermore, we provide a survey on PHY-security techniques to improve the secrecy performance. Especially, we propose a secure massive access framework for the cellular IoT network by exploiting the inherent co-channel interferences. Finally, we discuss several potential research directions to further enhance the security of massive IoT.

Keywords 5G and beyond, PHY-security, massive access, cellular IoT

Citation Qi Q, Chen X M, Zhong C J, et al. Physical layer security for massive access in cellular Internet of Things. Sci China Inf Sci, 2020, 63(2): 121301, https://doi.org/10.1007/s11432-019-2650-4

1 Introduction

With the explosive growth of Internet of Things (IoT), a massive number of IoT devices desire to access wireless networks for realizing various advanced applications, e.g., smart city, industry automation, and remote medicine [1–3]. It is predicted that over 75.4 billion devices will be linked to the Internet all over the world by 2025, which means a nearly 500% growth for the ten years compared to 15.4 billion in 2015 [4, 5]. As shown in Table 1, among commonly used wireless access techniques, i.e., Bluetooth, Zigbee, WiFi, LoRa, and cellular, cellular is the best choice to provide wireless access with quality of service (QoS) guarantees for a massive number of IoT devices over a wide range [6]. Hence, the third generation partnership project (3GPP) has already identified the cellular IoT as one of the main application cases of 5G, and issued a specification for cellular IoT in Release 13 in 2015 [7]. In that specification, cellular IoT is categorized as the narrowband IoT (NB-IoT) for fixed and low-rate scenarios and LTE-machine (LTE-M) or enhanced MTC (eMTC) for mobile and high-rate scenarios.

In general, the cellular IoT has the characteristics of massive connectivity, low power, and wide coverage. To support massive connectivity over limited radio spectrum, IoT devices should share the same spectrum. As a result, massive access is susceptible to eavesdropping owing to the broadcast nature of wireless channels [8,9]. Traditionally, upper layer cryptography techniques are adopted to guarantee wireless security [10, 11]. With the fast development of information techniques, the eavesdropping capability of malicious nodes is increasingly strong, resulting in much more complicated cryptography techniques.

* Corresponding author (email: chen_xiaoming@zju.edu.cn)

Table 1 Comparison of wireless access techniques for IoT networks

	Bluetooth	Zigbee	WiFi	LoRa	Cellular
Spectrum	Unlicensed	Unlicensed	Unlicensed	Unlicensed	Licensed
Connectivity	Small	Medium	Large	Massive	Massive
Range	Short	Short	Medium	Long	Long
Power	Low	Low	High	Low	Low
Delay	Short	Short	Short	Short	Short
Security	Low	Medium	Medium	Medium	High
Mobility	Not	Not	Not	Yes	Yes
Cost	Low	Low	Low	High	Low

Table 2 Comparison of cryptography and PHY-security techniques

	Advantages	Shortcomings
Cryptography	(1) Low overhead (2) Independent of channel conditions	(1) Need extra secure channel for key exchange (2) High complexity for encryption
PHY-security	(1) Absolute security (2) Independent of eavesdropping capability	(1) High overhead for channel information acquisition (2) Extra resource consumption for security enhancement

Because most of IoT devices are simple nodes with limited computational capability, the complexity of cryptography techniques might be unaffordable. In this context, as a compliment of cryptography techniques, physical layer security (PHY-security) techniques are applied to the 5G cellular IoT network [12,13]. Generally speaking, PHY-security explores the random characteristics of wireless channels, e.g., fading, noise and interference, to make the information transmission rate greater than the capacity of the eavesdropping channel, and hence the eavesdropper cannot decode the interception signal [14–16]. Even with limited computational capability, PHY-security is able to provide secure communications for a massive number of IoT devices. Thus, PHY-security is particularly appealing to the 5G cellular IoT network [17–19]. The comparison of cryptography and PHY-security techniques is given in Table 2.

From an information-theoretical viewpoint, the essence of PHY-security is to increase the capacity of the legitimate channel and to decrease the capacity of the eavesdropping channel simultaneously, and hence maximizes the secrecy rate [20–22]. Inspired by that, many effective physical layer security techniques have been proposed [23–25]. In [26], a survey of PHY-security techniques for multiuser wireless networks was given. Multiple-antenna PHY-security techniques over multiple access channels were discussed in [27]. Moreover, a variety of relay-based PHY-security techniques were investigated in [28]. Compared to general wireless networks, the cellular IoT faces severe and complicated co-channel interference owing to massive connectivity over limited radio spectrum. Hence, it makes sense to exploit the originally harmful co-channel interference to enhance the secrecy performance according to the characteristics of massive access in the cellular IoT network. Commonly, B5G cellular IoT network is suggested to adopt the grant-free random access scheme for avoiding high overhead [29–31]. To be specific, the IoT devices can access B5G cellular network without a grant to transmit or a prior scheduling assignment. Owing to grant-free random access, an operation for user detection and channel estimation should be performed at the base station (BS) before data transmission [32–34]. Therefore, the co-channel interference would affect the schemes for user detection, channel estimation and data transmission, and then determines the secrecy performance. Because the co-channel interference would interfere with both the legitimate and eavesdropper nodes, it is possible to coordinate the co-channel interference from the perspective of improving the overall performance of the cellular IoT through spatial beamforming [26,27]. However, it is not a trivial task to coordinate the co-channel interference in the scenario of massive access. This is because the BS should have enough degrees of freedom and accurate channel state information (CSI). Yet, in the scenario of massive IoT, it is difficult to obtain accurate CSI about a massive number of legitimate IoT devices [35]. Especially, the eavesdroppers may attack the channel estimation by sending the same pilot sequence, which significantly decreases the accuracy of channel estimation [36]. On the other hand, the CSI about the eavesdropper is hard to be acquired in practical systems [37]. Thereby, it is desired to

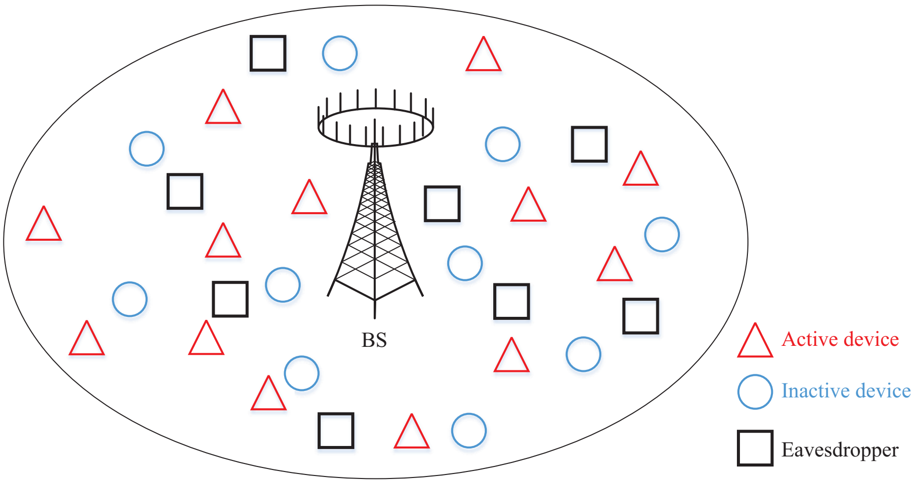

Figure 1 (Color online) A typical massive access scenario in the cellular IoT network.

coordinate the co-channel interference based on partial CSI, namely robust beamforming [38–40].

In general, one can hardly guarantee secure communications of a massive number of IoT devices with limited wireless resources, incurring a great deal of challenging issues in the design of PHY-security schemes for the cellular IoT network. Obviously, the traditional secure schemes cannot be applied to the cellular IoT network directly owing to the constraint on the computational capability at the IoT devices. Thus, it is desired to design the PHY-security schemes according to the characteristics and requirements of the cellular IoT network. In this article, we first investigate the security issues in the cellular IoT network with massive access, and point out the fundamental challenges for guaranteeing communication security. Then, we provide a survey of several effective physical-layer techniques to realize secure massive access, with an emphasis on revealing their performance advantages and limitations. Furthermore, we propose a secure massive access framework for the cellular IoT network by exploiting the inherent co-channel interference. Finally, we discuss several potential research directions to further enhance the security of massive IoT.

2 Challenging issues in secure massive access

The broadcast nature of wireless channels enables massive access over limited radio spectrum, but also incurs information leakage. As a result, there exist many challenging issues for realizing secure massive access, especially in the cellular IoT network with simple nodes. On the one hand, it is not a trivial task to support massive access owing to limited wireless resources [41]. On the other hand, massive access leads to a high interception probability owing to severe co-channel interference [42]. In what follows, we first give a brief introduction of massive access in the 5G cellular IoT network, and then analyze the potential security issues in massive access.

2.1 Massive access in cellular IoT

In the cellular IoT network, there usually exist a massive number of heterogeneous IoT devices distributed over the whole cell, as shown in Figure 1. Owing to the sporadic characteristics of IoT applications, only a part of IoT devices are active during a certain data frame [43]. Thus, the BS should first detect which devices are active, and then performs data transmission. However, the conventional multiple access protocols, e.g., ALOHA, which limit the number of access devices and require a high signalling overhead, are no longer really fit for the massive access systems [44, 45]. To solve this problem, the grant-free random access protocol is widely applied in the massive access systems [46, 47]. Specifically, each device is assigned with a unique pilot sequence for activity detection and channel estimation. At the beginning of each data frame, the active devices send their pilot sequences to the BS over the uplink

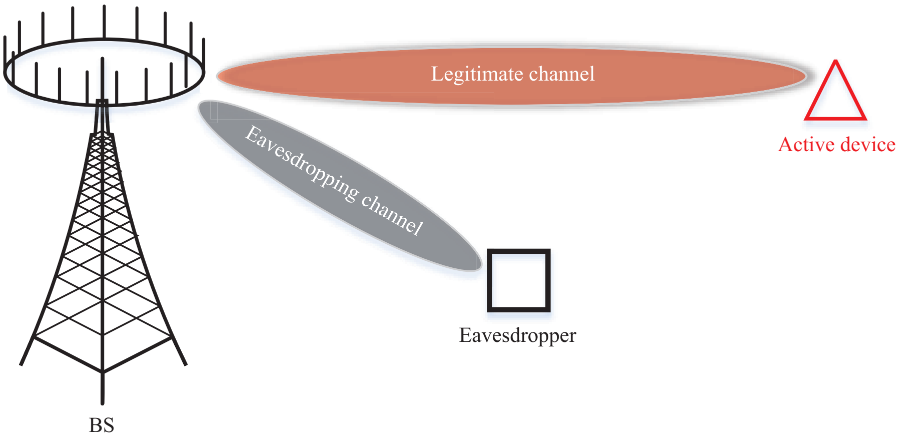

Figure 2 (Color online) A three-node PHY-security model.

channels simultaneously. Because only a part of devices are active, the received signal at the BS is sparse. Therefore, some effective sparse signal processing methods, e.g., compressive sensing (CS), can be utilized to detect the active devices and estimate the corresponding channels [48, 49]. Especially, if the number of BS antennas is large enough, the detection probability asymptotically approaches 1. Thereby, the active devices can be detected perfectly in B5G cellular IoT network, as the BS deploys a large-scale antenna array. However, for the channel estimation, even with a large-scale antenna array, the BS has difficulty in obtaining accurate CSI. This is because the CSI accuracy is mainly dependent of the quality of the received signal [50]. In the context of massive access, it is impossible to assign orthogonal pilot sequences to the devices, resulting in a high co-channel interference and a low signal-to-interference-plus-noise ratio (SINR) [51]. Consequently, the BS obtains a low-precision CSI, which seriously affects the performance of data transmission in sequence.

Once the active devices and the corresponding CSI are determined, the BS starts to exchange the data with the devices in the rest of a data frame. Because the 5G cellular network is suggested to work in a time division duplex (TDD) mode, a data frame consists of both uplink and downlink transmissions. To support efficient massive access over limited radio spectrum, the data transmission usually employs non-orthogonal communication schemes, e.g., non-orthogonal multiple access (NOMA) [52–54] and sparse code multiple access (SCMA) [55–57]. Generally speaking, in the uplink stage, the active devices transmit the signals concurrently, and the BS performs successive interference cancellation (SIC) for mitigating the co-channel interference. In the downlink stage, the BS broadcasts the superposition coded signal, and the devices may carry out SIC on the received signal independently.

2.2 Security issues in massive access

As shown in Figure 2, if the eavesdropper is or pretends to be a node, it is also able to receive the interested signal. Thus, the information might be eavesdropped by the malicious nodes. Especially in the cellular IoT network, the transmission rate is usually very low, leading to a high risk of information leakage. In the following, we analyze potential security issues in three stages of massive access, including activity detection and channel estimation, uplink data transmission, and downlink data transmission.

2.2.1 *Activity detection and channel estimation*

As mentioned above, at the beginning of a data frame, the active devices send pilot sequences over the uplink channels for activity detection and channel estimation. The estimated CSI is used for signal decoding in the uplink and signal precoding in the downlink. Thus, the CSI accuracy has a great impact on the secrecy performance of PHY-security techniques [58]. In order to increase the interception probability, the eavesdropper may send the jamming signal or even the pilot sequence to decrease the CSI accuracy [59]. The influences of the two active attacking ways are as follows.

• Jamming signal [60]: The eavesdropper sends a random jamming signal during the stage of activity detection and channel estimation. The jamming signal would interfere with all active devices' pilot sequences. As a result, the CSI accuracy about all devices is reduced, and the secrecy performance of the cellular IoT network is degraded accordingly.

• Pilot sequence [61]: The eavesdropper sends the same pilot sequence as that of the targeted device. This way may degrade the secrecy performance more severely. On the one hand, it decreases the CSI accuracy owing to co-channel interference. On the other hand, it leads to a high information leakage because there is a composition of the eavesdropping channel in the estimated CSI.

As a result of active attacking from the eavesdropper, the BS has low-precision CSI about the IoT devices. In a worse case, the BS may obtain false CSI. This is because if the eavesdropper sends the pilot sequence with a high power, the estimated CSI is dominated by the eavesdropping CSI. In this case, the quality of the received signal at the eavesdropper is higher than that at the legitimate device, which causes a high interception probability. Moreover, the accuracy of eavesdropping CSI plays a great role in the secrecy performance of PHY-security techniques. However, the acquisition of eavesdropping CSI has the following challenging issues.

• Internal node [62]: If the eavesdropper is an IoT node, the BS may obtain partial eavesdropping CSI at the stage of activity detection and channel estimation. However, the accuracy of eavesdropping CSI is still low owing to severe co-channel interference.

• External node [63]: If the eavesdropper is an external node, the BS cannot obtain eavesdropping CSI directly. Especially, if the eavesdropper hides itself, the BS may not have any eavesdropping CSI.

The design of PHY-security schemes requires both legitimate and eavesdropping CSI. However, the BS only has partial CSI or even no CSI in practical systems. Thus, it is a challenging issue to design effective secure schemes.

2.2.2 *Uplink data transmission*

In the stage of uplink data transmission, the IoT devices simultaneously send the data signals to the BS over the uplink channels. Meanwhile, the eavesdropper also receives the signal, and tries to decode it. In the scenario of massive access, there exists severe co-channel interference, resulting in a low information transmission rate. If the information transmission rate is less than the capacity of the eavesdropping channel, the eavesdropper can decode the signal correctly. In order to guarantee information security, it is necessary to decrease the quality of the received signal at the eavesdropper and to increase the quality of the received signal at the BS. However, because the IoT devices are usually simple nodes with limited computational capacity, it seems overburdened to conduct complicated signal precoding at the IoT devices for improving the secrecy performance. Therefore, the secure schemes are usually performed at the BS. For uplink data transmission, because the BS is at the receiving side, there exist the following security issues.

• Short-distance interception [64]: The BS is normally deployed at the center of the cell, and thus the edge-device has a long access distance. However, the eavesdropper might be close to the targeted device, namely short-distance interception. Thus, the received signal at the eavesdropper is stronger than that at the BS, giving rise to information leakage. Especially for the edge-device, there is a high eavesdropping probability.

• Short-packet transmission [65]: Because the IoT applications are in general sporadic with a low data amount, it is common to utilize the short-packet transmission technique. As is well known that short-packet transmission leads to a high decoding error probability. Especially in the uplink stage, the signal decoding would suffer severe co-channel interference from all the other active devices' signals, which further decreases the transmission reliability. In order to satisfy the requirements on the transmission reliability, it is desired to decrease the transmission rate. However, a low transmission rate may result in a high interception probability.

• Limited interference mitigation capability [66]: With the goal of enhancing the secrecy performance, the BS should resort to some interference mitigation schemes, e.g., zero-forcing (ZF) and successive interference cancellation (SIC). These interference mitigation schemes all require accurate CSI. However, because the BS only has partial CSI, the performance of interference cancellation at the BS is limited.

In the cellular IoT network, the IoT applications may have various quality of service (QoS) requirements, which substantially increases the processing complexity at the BS. Especially when the BS only has low-precision CSI, there is a high interception risk for the IoT applications.

2.2.3 *Downlink data transmission*

In the stage of downlink data transmission, the BS broadcasts messages over the downlink channels. Owing to massive access over limited radio spectrum, non-orthogonal multiple access schemes are usually adopted, resulting in severe co-channel interference and thus a high interception risk. In general, in order to enhance wireless security, the BS carries out precoding on the signals to be transmitted [67]. For instance, the BS can perform spatial beamforming to decrease or even avoid information leakage. However, owing to the characteristics of massive IoT, there are still numerous critical issues as follows.

- Capability-constrained IoT device [68]: In the cellular IoT network, most of IoT devices are simple nodes with limited power supply and computational capability. Thus, it is tough for the IoT devices to conduct complicated signal processing, e.g., SIC. In this context, there exists high residual interference at the IoT devices even with spatial interference cancellation at the BS.
- Unavailable artificial noise [69]: Artificial noise (AN) is a commonly used method to confuse the eavesdropper, and thus improves the secrecy performance. The AN signal is usually transmitted in the null space of the legitimate channel, so as to avoid the interference to the IoT device. However, because the BS only has partial CSI about the legitimate channels, the use of AN would interfere with the IoT devices inevitably. Moreover, there are no enough spatial degrees of freedom at the BS to transmit the AN signals for supporting massive access.
- Cooperative eavesdropping [70]: Multiple malicious nodes may cooperatively eavesdrop to enhance the interception capability. For example, they can combine the received signals to improve the quality of the eavesdropping signal. Thus, for simple IoT devices, there is a high interception risk.

For downlink data transmission, it is usual to exploit the powerful capability of the BS to assure secure communications. However, in the cellular IoT network with massive access, the BS may not have enough spatial degrees of freedom to combat the eavesdropping.

3 PHY-security techniques for massive access

As mentioned above, massive access in the cellular IoT network faces a variety of challenging issues. Thus, it is desired to adopt effective PHY-security techniques to realize secure massive access. Although there already have been a variety of PHY-security techniques, they might be not applicable in the cellular IoT network directly. In the sequel, according to the characteristics of the cellular IoT network, we introduce several feasible and powerful PHY-security techniques.

3.1 Pilot design

In the 5G cellular IoT network, pilot sequences are sent from the IoT devices to the BS for activity detection and channel estimation at the beginning of a data frame [71]. For ease of design, Gaussian distributed pilot sequences are widely applied in the most of previous relevant studies [72], yet they have a weak capability of anti-interference and anti-jamming. In the cellular IoT network, on the one hand, channel estimation suffers severe co-channel interference from the other IoT devices. On the other hand, the eavesdropper may transmit the jamming signal to further decrease the accuracy of channel estimation. Thus, the traditional Gaussian distributed pilot sequence might be not suitable for the secure cellular IoT networks. In order to obtain accurate CSI, it is imperative to design new pilot sequence.

Intuitively, to improve the accuracy of channel estimation under strong interference condition, it is likely to utilize coded sequences. Especially, if the coded sequence is randomly generated at the BS and IoT device based on the same seed, it is expected to solve the problem that the eavesdropper obtains the targeted device's pilot sequence. Note that the use of coded sequence requires to design the corresponding detection and estimation methods. As a first attempt, the Reed-Muller (RM) sequence is applied to construct deterministic measurement matrices and extract attributes of sparse signals in [73]. Because active detection and channel estimation in massive access is a sparse signal processing problem, the RM sequences can be used as the pilot sequences.

3.2 Massive MIMO

From an information-theoretic viewpoint, the essence of PHY-security is to increase the quality of the legitimate signal and decrease the quality of the eavesdropping signal. Intuitively, multiple-antenna techniques can achieve the both goals simultaneously by making use of the spatial degrees of freedom. For example, if the legitimate signal is transmitted in the null space of the eavesdropping channel, the eavesdropper cannot receive any signal. However, because the BS may not have eavesdropping CSI, there always exists information leakage to the eavesdropper. In such an adverse but practical scenario, it makes sense to adopt the massive MIMO techniques [74].

In fact, massive MIMO is a candidate technique of 5G wireless network. Thus, it is natural to use the massive MIMO techniques to enhance the security of the cellular IoT network. Specifically, in the massive MIMO systems, because the large-scale antenna array at the BS has a high spatial resolution, the information leakage can be reduced remarkably. Especially, if the number of BS antennas is large enough, the information leakage asymptotically approaches zero [75]. Thus, even without eavesdropping CSI, it is possible to realize secure communications. Meanwhile, the large-scale antenna array can provide a high array gain for improving the quality of the legitimate signals [76]. Moreover, owing to a large spatial degrees of freedom, the massive MIMO systems can admit great quantities of IoT devices. Hence, massive MIMO has a great potential of guaranteeing secure massive access.

3.3 Resource allocation

There are multiple kinds of available resources in the cellular IoT network, e.g., time, frequency, space and power. It is clear that the resource utilization plays an important role in massive access. On one hand, a massive number of IoT devices compete the limited wireless resource for efficient access. On the other, these resources have different effects on the quality of the received signals at the IoT devices and the eavesdroppers. Thus, it is imperative to allocate these wireless resource from the perspective of optimizing the secrecy performance of massive access [77, 78]. For instance, power allocation is a commonly used PHY-security technique in secure communications [79]. However, it is not a trivial task to allocate the wireless resource in the cellular IoT network with massive access, because the secrecy performance, e.g., secrecy rate, is in general a sophisticated function of wireless resources. To solve this problem, it is likely to choose some indirect performance metrics. As mentioned above, a key problem of secure massive access is to transform the originally harmful co-channel interference as an effective security enhancement tool. Thus, under a constraint of the maximum interference to the IoT devices, one can allocate the wireless resources by maximizing the interference to the eavesdroppers. Hence, it is possible to derive feasible resource allocation strategies for secure massive access in the cellular IoT networks.

3.4 User clustering

Because most of IoT devices are simple nodes with limited computational capability, the use of complicated PHY-security techniques at the IoT devices seems out of the question. However, as analyzed earlier, the IoT devices face a series of security issues in all stages of massive access. In this context, it is likely to improve the secrecy performance through multiple-device cooperation [80]. Specifically, multiple IoT devices form a cluster, and an IoT device with a high computational capability is selected as the head. The communication between the BS and the IoT devices is forwards by the head. The benefits of user clustering lie in two-fold. First, user clustering can effectively reduce the overhead for activity detection and channel estimation. Second, user clustering can effectively enhance wireless security by

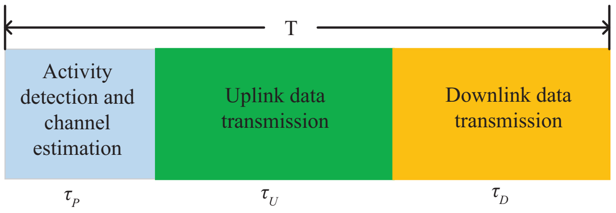
T
Activity detection and channel estimation
Uplink data transmission
Downlink data transmission
τ_P
τ_U
τ_D

Figure 3 (Color online) A secure massive access protocol in the cellular IoT network.

using advanced PHY-security techniques at the head. Moreover, even if there is not a strong IoT device in a cluster, it is also likely to decrease the interception probability by performing cooperative beamforming within multiple simple IoT devices.

4 Design of secure massive access

In above, we introduce the security challenges in massive access of cellular IoT and provide several feasible and effective secure schemes. In this section, we give a simple example for the design of secure massive access for cellular IoT from a comprehensive viewpoint. A typical massive access scenario as shown in Figure 1 is considered, where a large number of IoT devices with sporadic traffic access the cellular IoT network through a BS equipped with a large-scale antenna array in the presence of multiple eavesdroppers. Thus, during a transmission interval, only a part of IoT devices have data to transmit. According to the characteristics of IoT applications, a short data frame of duration T is utilized in the cellular IoT network, as shown in Figure 3. At the beginning of a framework, the active IoT devices send RM sequences of τ_P symbols over the uplink channels suffering jamming from the eavesdroppers. A reconstruction algorithm based on compressive sensing is run at the BS for activity detection and channel estimation. If the number of BS antennas is sufficiently large, e.g., 256, the BS can detect the active devices correctly, but only partial CSI. Then, the active devices transmit short packets of τ_U symbols over the uplink channels, and the BS recovers the transmitted packets from the received signal. Finally, the BS broadcasts the signal over the downlink channels, and the IoT devices decode the desired signal based on the received signal. For enhancing the security of massive access in the cellular IoT network, the following PHY-security techniques are adopted.

(1) Frame structure optimization: Because a short data frame is often employed in the cellular IoT network, it is necessary to distribute the limited duration to the three stages. In fact, the durations of the three stages carry weight to the secrecy performance. For example, a longer duration for channel estimation may obtain accurate CSI, but reduces the duration for information transmission. Thus, the frame structure optimization can effectively improve the secrecy performance.

(2) Co-channel interference exploration: Because the BS only has partial legitimate CSI and no eavesdropping CSI, it is impossible to confuse the eavesdroppers by sending the AN signals. Fortunately, the severe co-channel interference caused by massive access can be explored to confuse the eavesdroppers. Besides, the use of co-channel interference does not consume extra transmit power and spatial degrees of freedom. Thus, it is appealing in the cellular IoT network.

(3) Robust beamforming: In the presence of partial legitimate CSI, robust beamforming can be conducted at the BS to guarantee the secrecy performance in the worst case. Especially when there exists a high decoding error caused by short packets, robust beamforming can effectively enhance the transmission reliability over the legitimate channels, and thus improves the secrecy performance.

In Figure 4, we show the performance gain of the proposed secure massive access scheme over a fixed one from the perspective of maximizing the sum secrecy rate. Note that the proposed scheme obtains legitimate CSI based on an optimized frame structure, and then explores co-channel interference for security enhancement by using robust beamforming. The fixed scheme divides the frame length for three stages equally, and then adopts match filtering (MF) beamforming designed based on estimated CSI. It is seen that the proposed scheme performs better in the whole SNR region. Moreover, the performance

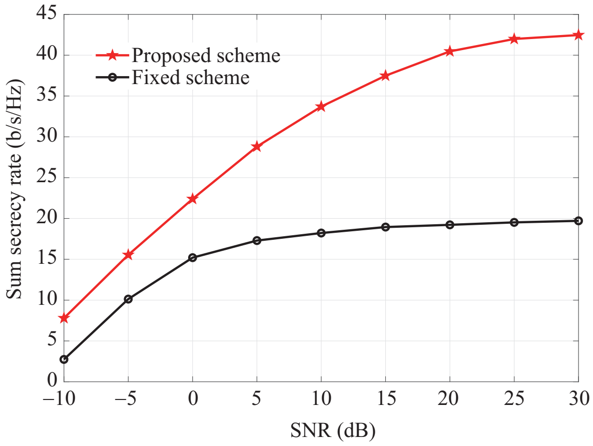

Figure 4 (Color online) Performance comparison of the proposed scheme and a fixed scheme.

gain increases as the SNR increases. Thus, the proposed scheme looks really promising for supporting secure massive access in the cellular IoT network.

5 Future research directions

Secure massive access in the 5G cellular IoT network has not been well addressed, and it will continue to be a critical issue in the B5G wireless networks. There are all sorts of challenging problems that needs to be addressed cover a wide range of disciplines including communication theory, information theory, and signal processing. In the following, we list some initial ideas to solve the remaining problems.

5.1 Adaptive anti-eavesdropping

As discussed above, eavesdropper CSI is critically important for the design of PHY-security techniques. However, because the eavesdropper hides itself well, it is not easy to obtain eavesdropping CSI. If there is no eavesdropping CSI, it is impossible to adopt adaptive anti-eavesdropping schemes, resulting in a poor secrecy performance. In order to further improve the secrecy performance, it is required to acquire eavesdropping CSI by some means. For instance, the eavesdropping may send the jamming signal to confuse channel estimation. In this case, the BS can obtain partial eavesdropping CSI through channel estimation. Moreover, it is possible to estimate eavesdropper CSI when the eavesdropper sends out the intercepted information.

5.2 Asymmetric secure schemes

In the cellular IoT network, there are plenty of IoT applications with different security requirements. For example, the BS may broadcast some common signal, which has a low security level. But when the BS sends the confidential signal, it is necessary to provide high security guarantee. Intuitively, if the cellular IoT network adopts the secure scheme regardless of security requirements, there would be a high waste of limited wireless resources. Thus, it makes sense to utilize asymmetric secure schemes according to the security requirements of IoT applications for realizing secure massive access with limited wireless resource.

5.3 Distributed secure access

In current wireless networks, the BS is equipped with a co-located antenna array. However, because the IoT devices usually distribute over the whole cell, the co-located antenna array easily causes the problem of short-distance interception. Moreover, there exists a severe near-far effect in the scenario of the co-located antenna array. Owing to these problems, the B5G wireless networks are suggested to adopt a distributed multiple-antenna architecture or even a cell-free architecture. By distributing the antenna units over the cell, it is likely to shorten the access distance, and thus solve the problem of short-distance interception.

5.4 Convergence of PHY-security and upper-bound cryptography techniques

Owing to complex propagation environments and heterogeneous performance requirements, it is difficult to provide security guarantee only by PHY-security techniques or upper-bound cryptography techniques. In future wireless networks, it is indispensable to design a hybrid secure scheme by combing PHY-security and upper-bound cryptography techniques. Thus, the cellular IoT network can achieve the benefits of the both secure techniques, so as to realize secure massive access in various scenarios.

6 Conclusion

This article gave a review of secure massive access from both theoretical and technical perspectives. First, we provided an introduction of massive access in the 5G cellular IoT network, with an emphasis on revealing the challenging issues. Then, we revealed a variety of effective PHY-security techniques, which may significantly improve the secrecy performance of massive access. Afterwards, we proposed a feasible and effective design method for secure massive access and showed the performance gain through numerical simulation. Finally, some potential research directions were discussed.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61871344, 61922071, U1709219, 61725104), National Science and Technology Major Project of China (Grant No. 2018ZX03001017-002), and National Key R&D Program of China (Grant No. 2018YFB1801104).

References

1 Zanella A, Bui N, Castellani A, et al. Internet of Things for smart cities. IEEE Internet Things J, 2014, 1: 22–32

2 Xu L D, He W, Li S. Internet of Things in industries: a survey. IEEE Trans Ind Inf, 2014, 10: 2233–2243

3 Zhang H B, Li J P, Wen B, et al. Connecting intelligent things in smart hospitals using NB-IoT. IEEE Internet Things J, 2018, 5: 1550–1560

4 Palattella M R, Dohler M, Grieco A, et al. Internet of Things in the 5G era: enablers, architecture, and business models. IEEE J Sel Areas Commun, 2016, 34: 510–527

5 Statista Research Department. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). 2016. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

6 Chen X M. Massive Access for Cellular Internet of Things: Theory and Technique. Singapore: Springer, 2019

7 3GPP. Cellular System Support for Ultra-Low Complexity and Low Throughput Internet of Things (CIoT) (Release 13). Technical Report, TR 45.820 V13.1.0. Technical Specification Group GSM/EDGE Radio Access Network, 2015. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719

8 Han S J, Xu X D, Fang S S, et al. Energy efficient secure computation offloading in NOMA-based mMTC networks for IoT. IEEE Internet Things J, 2019, 6: 5674–5690

9 Zi R, Liu J, Gu L, et al. Enabling security and high energy efficiency in the Internet of Things with massive MIMO hybrid precoding. IEEE Internet of Things J, 2019, 6: 8615–8625

10 Khari M, Garg A K, Gandomi A H, et al. Securing data in Internet of Things (IoT) using cryptography and steganography techniques. IEEE Trans Syst Man Cybernetics: Syst, 2019. doi: 10.1109/TSMC.2019.2903785

11 Liu Z, Seo H. IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms. IEEE Trans Inform Forensic Secur, 2019, 14: 720–729

12 Yang N, Wang L F, Geraci G, et al. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun Mag, 2015, 53: 20–27

13 Mukherjee A. Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. Proc IEEE, 2015, 103: 1747–1761

14 Gopala P K, Lai L, El Gamal H. On the secrecy capacity of fading channels. IEEE Trans Inform Theor, 2008, 54: 4687–4698

15 Chen X, Chen H H. Physical layer security in multi-cell MISO downlinks with incomplete CSI-A unified secrecy performance analysis. IEEE Trans Signal Process, 2014, 62: 6286–6297

16 Khisti A, Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel. IEEE Trans Inform Theor, 2010, 56: 3088–3104

17 Ji X S, Huang K Z, Jin L, et al. Overview of 5G security technology. Sci China Inf Sci, 2018, 61: 081301

18 Zhang J Q, Duong T Q, Woods R, et al. Securing wireless communications of the Internet of Things from the physical layer, an overview. Entropy, 2017, 19: 420
19 Shiu Y S, Chang S Y, Wu H C, et al. Physical layer security in wireless networks: a tutorial. IEEE Wirel Commun, 2011, 18: 66–74
20 Qi X H, Huang K Z, Li B, et al. Physical layer security in multi-antenna cognitive heterogeneous cellular networks: a unified secrecy performance analysis. Sci China Inf Sci, 2018, 61: 022310
21 Chen X M, Yin R. Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback. IEEE Wirel Commun Lett, 2013, 2: 503–506
22 Wang G, Lin Y, Meng C, et al. Secrecy energy efficiency optimization for AN-aided SWIPT system with power splitting receiver. Sci China Inf Sci, 2019, 62: 029301
23 Zou Y L, Zhu J, Wang X B, et al. A survey on wireless security: technical challenges, recent advances, and future trends. Proc IEEE, 2016, 104: 1727–1765
24 Chen X M, Lei L, Zhang H Z, et al. Large-scale MIMO relaying techniques for physical layer security: AF or DF? IEEE Trans Wirel Commun, 2015, 14: 5135–5146
25 Zhu J, Schober R, Bhargava V K. Secure transmission in multicell massive MIMO systems. IEEE Trans Wirel Commun, 2014, 13: 4766–4781
26 Mukherjee A, Fakoorian S A A, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun Surv Tutorials, 2014, 16: 1550–1573
27 Chen X M, Ng D W K, Gerstacker W H, et al. A survey on multiple-antenna techniques for physical layer security. IEEE Commun Surv Tutorials, 2017, 19: 1027–1053
28 Chen X M, Zhong C J, Yuen C, et al. Multi-antenna relay aided wireless physical layer security. IEEE Commun Mag, 2015, 53: 40–46
29 Zhang Z Y, Wang X B, Zhang Y, et al. Grant-free rateless multiple access: a novel massive access scheme for Internet of Things. IEEE Commun Lett, 2016, 20: 2019–2022
30 Ding J, Qu D M, Jiang H, et al. Success probability of grant-free random access with massive MIMO. IEEE Internet Things J, 2019, 6: 506–516
31 Jeong B K, Shim B, Lee K B. MAP-based active user and data detection for massive machine-type communications. IEEE Trans Veh Technol, 2018, 67: 8481–8494
32 Shao X, Chen X, Jia R. Low-complexity design of massive device detection via Riemannian pursuit. In: Proceeding of IEEE Global Communications Conference (GLOBECOM), 2019. 1–6
33 Ahn J, Shim B, Lee K B. EP-based joint active user detection and channel estimation for massive machine-type communications. IEEE Trans Commun, 2019, 67: 5178–5189
34 Liu L, Yu W. Massive connectivity with massive MIMO-Part I: device activity detection and channel estimation. IEEE Trans Signal Process, 2018, 66: 2933–2946
35 Chen X M, Zhang Z Y, Zhong C J, et al. Fully non-orthogonal communication for massive access. IEEE Trans Commun, 2018, 66: 1717–1731
36 Wu Y P, Schober R, Ng D W K, et al. Secure massive MIMO transmission with an active eavesdropper. IEEE Trans Inform Theor, 2016, 62: 3880–3900
37 Chen J, Chen X M, Gerstacker W H, et al. Resource allocation for a massive MIMO relay aided secure communication. IEEE Trans Inform Forensic Secur, 2016, 11: 1700–1711
38 Li S, Li Q, Shao S H. Robust secrecy beamforming for full-duplex two-way relay networks under imperfect channel state information. Sci China Inf Sci, 2018, 61: 022307
39 Zhu F C, Gao F F, Lin H, et al. Robust beamforming for physical layer security in BDMA massive MIMO. IEEE J Sel Areas Commun, 2018, 36: 775–787
40 Li B, Fei Z S. Probabilistic-constrained robust secure transmission for energy harvesting over MISO channels. Sci China Inf Sci, 2018, 61: 022303
41 Qi Q, Chen X M. Wireless powered massive access for cellular Internet of Things with imperfect SIC and nonlinear EH. IEEE Internet Things J, 2019, 6: 3110–3120
42 Zhang S, Xu X M, Peng J H, et al. Physical layer security in massive internet of things: delay and security analysis. IET Commun, 2019, 34: 93–98
43 Seo H, Hong J P, Choi W. Low latency random access for sporadic MTC devices in Internet of Things. IEEE Internet Things J, 2019, 6: 5108–5118
44 Jiang N, Deng Y S, Nallanathan A, et al. Analyzing random access collisions in massive IoT networks. IEEE Trans Wirel Commun, 2018, 17: 6853–6870
45 Jia D, Fei Z S, Xiao M, et al. Enhanced frameless slotted ALOHA protocol with Markov chains analysis. Sci China Inf Sci, 2018, 61: 102304
46 Shao X D, Chen X M, Zhong C J, et al. A unified design of massive access for cellular Internet of Things. IEEE Internet Things J, 2019, 6: 3934–3947
47 Jiang T, Shi Y M, Zhang J, et al. Joint activity detection and channel estimation for IoT networks: phase transition and computation-estimation tradeoff. IEEE Internet Things J, 2019, 6: 6212–6225
48 Chen Z L, Sohrabi F, Yu W. Sparse activity detection for massive connectivity. IEEE Trans Signal Process, 2018, 66: 1890–1904
49 Li Y, Xia M H, Wu Y C. Activity detection for massive connectivity under frequency offsets via first-order algorithms. IEEE Trans Wirel Commun, 2019, 18: 1988–2002

50 Yu G, Chen X, Ng D W K. Low-cost design of massive access for cellular internet of things. IEEE Trans Commun, 2019, 67: 8008–8020

51 Chen X M, Jia R D. Exploiting rateless coding for massive access. IEEE Trans Veh Technol, 2018, 67: 11253–11257

52 Chen X M, Zhang Z Y, Zhong C J, et al. Exploiting multiple-antenna techniques for non-orthogonal multiple access. IEEE J Sel Areas Commun, 2017, 35: 2207–2220

53 Ding Z G, Lei X F, Karagiannidis G K, et al. A survey on non-orthogonal multiple access for 5G networks: research challenges and future trends. IEEE J Sel Areas Commun, 2017, 35: 2181–2195

54 Jia R D, Chen X M, Zhong C J, et al. Design of non-orthogonal beamspace multiple access for cellular Internet-of-Things. IEEE J Sel Top Signal Process, 2019, 13: 538–552

55 Moon S, Lee H S, Lee J W. SARA: sparse code multiple access-applied random access for IoT devices. IEEE Internet Things J, 2018, 5: 3160–3174

56 Jia M, Wang L F, Guo Q, et al. A low complexity detection algorithm for fixed up-link SCMA system in mission critical scenario. IEEE Internet Things J, 2018, 5: 3289–3297

57 Alnoman A, Erkucuk S, Anpalagan A. Sparse code multiple access-based edge computing for IoT systems. IEEE Internet of Things J, 2019, in press

58 Yang T H, Zhang R Q, Cheng X, et al. Secure massive MIMO under imperfect CSI: performance analysis and channel prediction. IEEE Trans Inform Forensic Secur, 2019, 14: 1610–1623

59 Chen X M, Ng D W K, Chen H H. Secrecy wireless information and power transfer: challenges and opportunities. IEEE Wirel Commun, 2016, 23: 54–61

60 Wang H M, Huang K W, Tsiftsis T A. Multiple antennas secure transmission under pilot spoofing and Jamming attack. IEEE J Sel Areas Commun, 2018, 36: 860–876

61 Wu Y, Wen C K, Chen W, et al. Data-aided secure massive MIMO transmission under th pilot contamination attack. IEEE Trans Commun, 2019, 67: 4765–4781

62 Jeong S, Lee K, Kang J. Cooperative jammer design in cellular network with internal eavesdroppers. In: Proceedings of IEEE Military Commun Conf (MILCOM), 2012. 1–5

63 Deng Z, Sang Q, Gao Y, et al. Optimal relay selection for wireless relay channel with external eavesdropper: a NN-based approach. In: Proceedings of IEEE/CIC intern Conf Commun (ICCC), 2018. 515–519

64 Deng H, Wang H M, Yuan J H, et al. Secure communication in uplink transmissions: user selection and multiuser secrecy gain. IEEE Trans Commun, 2016, 64: 3492–3506

65 Wang H M, Yang Q, Ding Z G, et al. Secure short-packet communications for mission-critical IoT applications. IEEE Trans Wirel Commun, 2019, 18: 2565–2578

66 Mokari N, Parsaeefard S, Saeedi H, et al. Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks. IEEE Trans Signal Process, 2015, 63: 291–304

67 Chen X M, Zhang Y. Mode selection in MU-MIMO downlink networks: a physical-layer security perspective. IEEE Syst J, 2017, 11: 1128–1136

68 Chen X M, Jia R D, Ng D W K. On the design of massive non-orthogonal multiple access with imperfect successive interference cancellation. IEEE Trans Commun, 2019, 67: 2539–2551

69 Chen X M, Zhang Z Y, Zhong C J, et al. Exploiting inter-user interference for secure massive non-orthogonal multiple access. IEEE J Sel Areas Commun, 2018, 36: 788–801

70 Zhang Y Y, Shen Y L, Wang H, et al. On secure wireless communications for IoT under eavesdropper collusion. IEEE Trans Automat Sci Eng, 2016, 13: 1281–1293

71 Liu L, Larsson E G, Yu W, et al. Sparse signal processing for grant-free massive connectivity: a future paradigm for random access protocols in the Internet of Things. IEEE Signal Process Mag, 2018, 35: 88–99

72 Shao X D, Chen X M, Zhong C J, et al. Protocol design and analysis for cellular internet of things with massive access. In: Proceedings of IEEE International Conference on Communications (ICC), 2019. 1–6

73 Wang J, Zhang Z Y, Hanzo L. Joint active user detection and channel estimation in massive access systems exploiting reed-muller sequences. IEEE J Sel Top Signal Process, 2019, 13: 739–752

74 Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. IEEE Commun Mag, 2015, 53: 21–27

75 Lu L, Li G Y, Swindlehurst A L, et al. An overview of massive MIMO: benefits and challenges. IEEE J Sel Top Signal Process, 2014, 8: 742–758

76 Chen X M, Yuen C, Zhang Z Y. Exploiting large-scale MIMO techniques for physical layer security with imperfect channel state information. In: Proceedings of IEEE Global Communication Conference (GLOBECOM), 2014. 1–6

77 Xu C, Zeng P, Liang W, et al. Secure resource allocation for green and cognitive device-to-device communication. Sci China Inf Sci, 2018, 61: 029305

78 Hu J W, Yang N, Cai Y M. Secure downlink transmission in the Internet of Things: how many antennas are needed? IEEE J Sel Areas Commun, 2018, 36: 1622–1634

79 Li T Q, Ai Z Y, Ji W Z. Primate stem cells: bridge the translation from basic research to clinic application. Sci China Life Sci, 2019, 62: 12–21

80 Liu T Q, Han S, Meng W X, et al. Dynamic power allocation scheme with clustering based on physical layer security. IET Commun, 2018, 6: 2546–2551