A Physical Layer Approach for Securing Large-Scale Data Transmissions in Heterogeneous Wireless Networks

Yan Huo
School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China

***Abstract*—In this article, we outline a multi-tired heterogeneous networking architecture that is aimed for wirelessly transporting a large amount of data. This multi-tired architecture makes use of a few emerging technologies such as non-orthogonal multiple access and massive MIMO to help realize big data transmissions. These technologies can not only bring advances such as high-speed data transmissions and efficient spectrum utilization, but also give rise to new security challenges (e.g., eavesdropping). Hence, we introduce a number of physical layer countermeasures that can be employed by each of these technologies to address the corresponding security challenges. Particularly, the proposed countermeasures can secure wireless data via adjusting the achievable secrecy capacity. For each of these countermeasures we present details regarding how to achieve the desired secrecy capacity by controlling the received signal quality at the legitimate receiver and the eavesdropper. We also discuss the open research issues and the possible research focuses for future mobile big data related applications.**

***Index Terms*—Wireless big data, physical layer security; heterogeneous networks; secrecy capacity.**

I. Introduction

Data-intensive applications such as video streaming are experiencing an unprecedented surge as a digital savvy generation is on the rise. On the other hand, with the rapid development of mobile computing, cloud computing, and Internet of Things (IoT), a large volume of data has been moving within heterogeneous wireless networks on a daily basis [1]. These data contains sensitive and private information such as social relationships and financial transactions. As a result, the security of wireless networks is of critical importance for the wide deployment and acceptance of big data services in the future.

However, grand challenges exist to secure big data in wireless transmission systems due to the broadcast nature of the underlying communication channel. A malicious user can monitor the network activities and intercept the transmitted signals, causing user privacy violations. Traditionally, securing wireless data can be realized by cryptographic measures such as data encryption to protect against the disclosure of sensitive information [2]. With the emergence of new networking architectures such as sensor networks and IoT, cryptographic measures become unsuitable due to various constraints such as computational power. Hence, there is an increasing interest in exploiting the physical properties of the wireless channel to enable security services because information theory provides a natural platform for the study of this issue. One major benefit of the physical layer-based approach is that it requires low computational power, which is suitable for low-profile devices.

Recently, a considerable amount of studies has been made to develop a better understanding of the fundamental ability of the so-called physical layer to provide security in wireless networks. A number of physical layer-based security measures have been proposed for protecting the data exchanges among low-profile wireless devices. These measures typically exploit the characteristics of wireless medium to ensure that eavesdroppers cannot successfully decode the transmitted signals (i.e., information). Specifically, legitimate signals are transmitted with artificial noise or in a null space to achieve data security and privacy preservation. This can be regarded as setting up an umbrella to cover the legitimate information.

To meet the demands of the big data era, new wireless technologies have been developed and implemented to move more data at faster speeds for cellular subscribers, home network users, and smart edge terminals. Yet, there still lack studies on physical layer-based security measures for these new technologies under scenarios with massive distributed data sharing among a variety of devices (e.g., low-profile sensors or battery-powered smart terminals) in heterogeneous networks. For example, 5G-based multi-tiered heterogeneous networks may serve up to billions of devices from different locations with continuous data services in the near future.

To address this problem, we discuss a few issues of physical layer security measures for various novel wireless technologies under a 5G-based multi-tiered structure. In particular, inter-user interference and friendly jamming under various new access modes are investigated for covert communications, and anti-pilot contamination for massive MIMO is investigated for assisting legitimate user detection and restraining malicious node access. We also provide key issues and corresponding physical layer solutions for secure transmissions based on cognitive radio and co-frequency co-time full duplex mode. Furthermore, we enumerate the security solutions for three typical networks, i.e., cellular-based communications, device-to-device data sharing, and wireless big data in IoT.

The rest of the article is organized as follows. We provide a general wireless transmission model for big data in Section II, followed by a discussion on physical layer security for novel wireless technologies in Section III. Next, we elaborate on

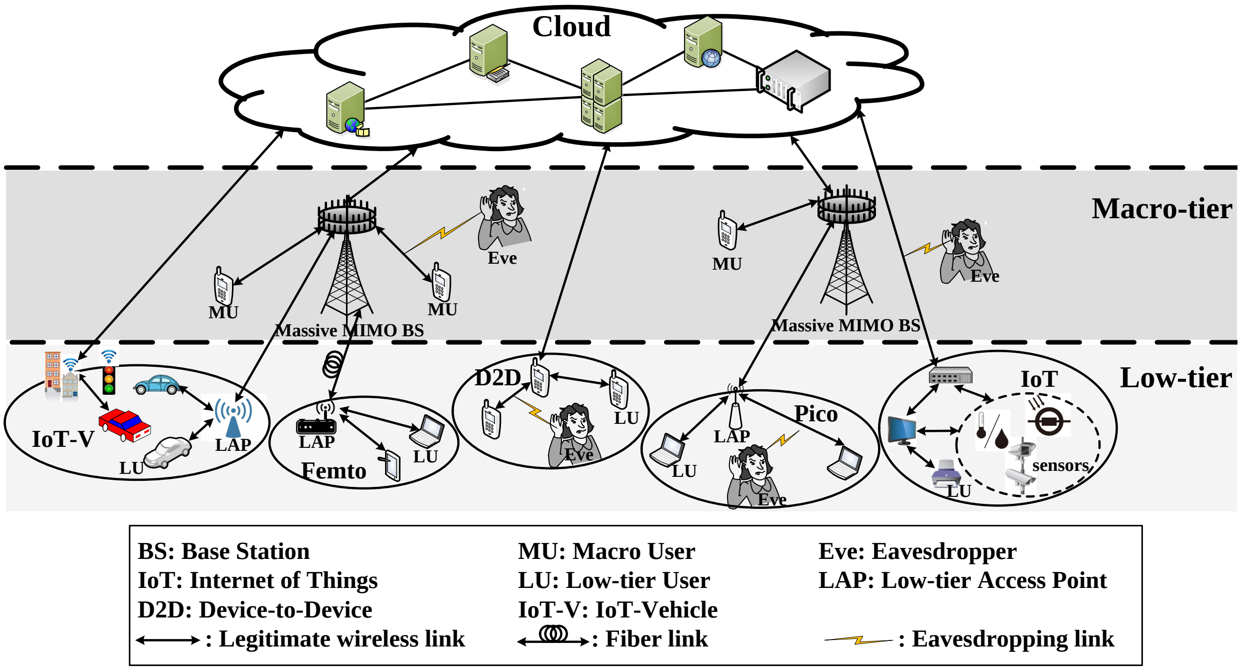


Fig. 1. The system model.

the physical layer security strategies under various network architectures for wireless big data services in Section IV. Finally, we conclude this article in Section V.

II. System Model and Preliminaries

A. Heterogeneous Network Model

The emergence of mobile big data puts forward higher requirements on wireless networks, including greater load capacity, more intelligent resource management strategies, better network deployment, and smarter nodes with integrated capabilities of computation, storage, analysis, and decision. As a result, novel wireless techniques and infrastructures are needed to support the upcoming mobile big data era. In this section, we present a basic model of heterogeneous networks, which can serve as a foundation for future ubiquitous wireless big data services.

The system model, shown in Fig. 1, is a multi-tiered structure that includes a macro-tier and a low-tier. The macro-tier is composed of base stations (BSs) with large-scale antenna arrays. Each BS provides access services for its associated macro users (MUs) to connect to cloud servers for data exchanges. Each MU may be allocated with licensed spectra. When MUs are densely deployed, the scarcity of spectrum resources occurs, causing poor performance of the overall system. For this reason, BSs need to adopt novel technologies such as the non-orthogonal multiple access and massive MIMO, to satisfy the demands of the MUs.

The low-tier is consisted of distributed micro-cell, pico-cell, femto-cell, ad hoc, IoT-vehicle (IoT-V), and device-to-device (D2D) networks. Each of these networks can provide access services to low-tier users (LUs), and connect to a BS or a cloud server through a low-tier access point (LAP). The connections between a LAP and a network in the low-tier can be serviced by wireless links or fiber channels. The low-tier can be ultra-dense when there are needs of high capacity and ubiquitous coverage. As a result, the spectrum resources become insufficient for LUs. In this case, LUs need to exploit technologies such as millimeter waves and spectrum reuse to obtain thousands-fold level capacity increase. Furthermore, the low-tier may need to have the cognitive capability to utilize idle spectra (also known as spectrum holes), so as to improve the spectrum utilization. With these designs and capabilities, the multi-tiered heterogeneous structure can address the access issues of diversified devices and provide ubiquitous services for the upcoming wireless big data services.

B. Security Challenges

The aforementioned network model places a great challenge to secure data transmissions because of the open wireless environments and the rich dynamics of the users. More specifically, eavesdroppers (abbreviated as Eve in Fig. 1) may be scattered in both macro- and low-tier networks. They can be active or passive, and malicious or benign. They can wiretap, intercept, and interfere with the legitimate signals, or steal private information for illegal profits. In addition, they can pretend to be a legitimate user to gain the trust of BSs or other users so as to launch advanced persistent attacks.

An even worse scenario occurs when there exist multiple collusive Eves, in which the Eves exchange the illegally acquired data with each other and then correlate the data to infer in-depth private information (e.g., social relationships and finical statues) based on powerful analytical tools (e.g., machine learning and artificial intelligence). Accordingly, one of the important design goals of the future security measures is to prevent collusive eavesdropping.

Note that cryptography based higher-layer security measures such as encryption have been proven to be insufficient or unsuitable when faced with large data correlations and analysis capabilities [3]. For this reason, we introduce physical layer security into the emerging wireless transmission technologies in heterogeneous networks complementing the cryptographic approaches.

C. Physical Layer Security Basics

In this section, we explain the basic concepts and definitions of physical layer security, which are applied in the subsequent security analyses. Secrecy capacity, denoted as C_s, is a key parameter that describes secure transmission performance in a wireless network from an information-theoretic perspective. It is defined as the maximal achievable rate difference between a legitimate channel and a wiretapped channel. Assume that there are M MUs, N LAPs, and L LUs, the perfect C_s of the uth user (either the uth macro-tier user or the uth low-tier user) can be formulated as follows,

$$C_s^{u,k} = \left[\log_2\left(1+\gamma_u\right) - \log_2\left(1+\gamma_{u,k}\right)\right]^+ , \tag{1}$$

where $[x]^+ = \max\{0, x\}$, γ_u and $\gamma_{u,k}$ represent the signal-to-interference-plus-noise-ratio (SINR) of the legitimate channel at the uth user and that of the wiretapped channel at the kth Eve, respectively. Considering the multi-tiered structure, γ_u is defined as

$$\gamma_u = \frac{P_u|\mathbf{H}_u|^2}{\sum\limits_{i\in\{\mathcal{M}\cup\mathcal{N}\cup\mathcal{L}\}, i\neq u} P_i|\mathbf{H}_{iu}|^2 + |\mathbf{n}_0|^2}, \tag{2}$$

and $\gamma_{u,k}$ is defined as

$$\gamma_{u,k} = \frac{P_u|\mathbf{H}_k|^2}{\sum\limits_{i\in\{\mathcal{M}\cup\mathcal{N}\cup\mathcal{L}\}, i\neq u} P_i|\mathbf{H}_{ik}|^2 + |\mathbf{n}_0|^2}, \tag{3}$$

where P_u is the signal power at the uth user; $\mathcal{M}$, $\mathcal{N}$, and $\mathcal{L}$ are respectively the sets of MUs, LAPs, and LUs; $\mathbf{H}_u$ and $\mathbf{H}_k$ respectively denote the channel state matrices for the uth legitimate channel and the kth wiretapped channel; $\mathbf{H}_{iu}$ and $\mathbf{H}_{ik}$ respectively refer to the channel state matrices of the interference signals (including the intra-tier and the inter-tier interference) for the uth legitimate channel and the kth wiretapped channel; and $|\mathbf{n}_0|^2$ represents the power of the Gaussian noise.

According to the aforementioned secrecy capacity definition, we next provide an analysis on the secure transmissions of heterogeneous networks based on a variety of novel communication technologies.

III. Physical Layer Security Solutions for Wireless Big Data

In this section, we introduce the key ideas of various novel technologies for securing transmission in wireless heterogeneous networks. Furthermore, we investigate the major threats and the corresponding physical layer countermeasures based on the definition listed in subsection II-C.

A. Non-Orthogonal Multiple Access

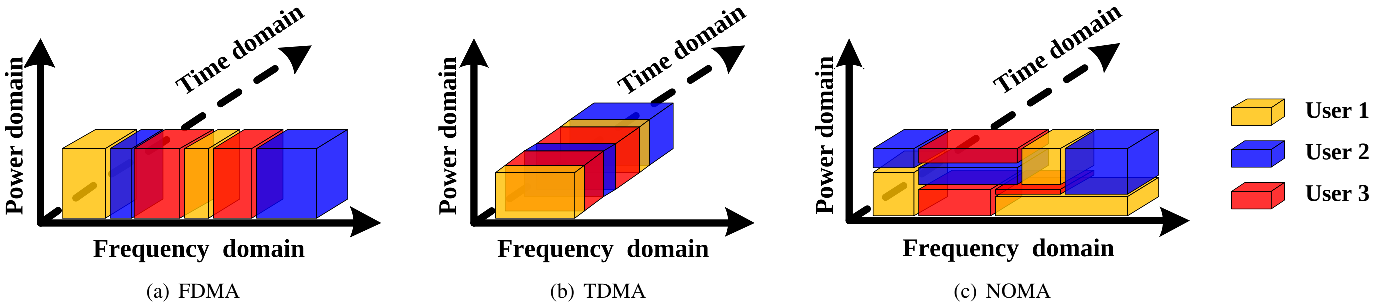
Traditional radio access schemes such as frequency division multiple access (FDMA) (shown in Fig. 2(a)) and time division multiple access (TDMA) (shown in Fig. 2(b)) exploit the orthogonality between signal streams to correctly differentiate and decode them in a cellular communication system. Faced with the problem of scarce spectrum, a promising multiple access scheme, called non-orthogonal multiple access (NOMA), as demonstrated in Fig. 2(c), emerges as an attractive solution to improve spectral efficiency and user experience. NOMA allows multiple users to transmit signals using the same time slot and the same carrier. Obviously, this can proactively introduce inter-user interference. To combat with such inter-user interference, receivers need to utilize successive interference cancellation (SIC) to achieve error-free demodulation.

More specifically, in a NOMA-based network, a legitimate user (assuming the uth user, $u \in \{\mathcal{M} \cup \mathcal{L}\}$) may receive data from cloud servers, BSs, or other users. Because of SIC, the received SINR of the user is just the signal-to-noise-ratio (SNR) of the output with maximal ratio combining, i.e., $\gamma_u = \frac{P_u|\mathbf{H}_u|^2}{|\mathbf{n}_0|^2}$. For an Eve without the SIC capability, signals from other sources are interference. Accordingly, the SINR of the received signal at the kth Eve is the same as (3). Hence, the received SINR of Eve can be severely degraded. The security performance of a single transmitter with the SIC capability was studied in terms of positive secrecy capacity probability, secrecy outage probability, and effective secrecy throughput in [4]. It was proved that the secrecy performance is only location-dependent in high SNR environments.

If Eve has the ability to perform SIC and diversity combining, signals from intra- and inter-tier stations cannot degrade her channel qualities. To address this issue, two possible measures have been proposed: i) the introduction of artificial noise (AN) and ii) the enhancement of signal directionality. In the following, we discuss the use of AN to improve the secrecy capacity of legitimate users because it can be easily integrated with NOMA.

The generation of AN needs to meet two requirements. First, AN needs to be able to effectively degrade Eve's SINR. The additional interference power introduced by AN, written as $\sum_{j\in\mathcal{J}} P_j|\mathbf{H}_{jk}|^2$, where $\mathcal{J}$ is the jammer set, is added to the denominator of (3). Clearly, the higher the $\sum_{j\in\mathcal{J}} P_j|\mathbf{H}_{jk}|^2$, the greater it can reduce the SINR of Eve. Second, AN should not have a negative impact on an intended receiver. Accordingly, the power allocation for each station needs to be carefully designed in a manner to null the jamming signals at the legitimate receivers (i.e., avoid unintended interference). Note that it is important to consider the total sum of the secrecy capacity of the network to optimize the overall security performance. In other words, the problem becomes the optimization of $\max\sum_{u,k} C_s^{u,k}$ under the condition of power-constrained wireless systems.

In the next subsection, we elaborate on beamforming based signal concentration techniques for massive MIMO because of their natural connections.



(a) FDMA

(b) TDMA

(c) NOMA

Fig. 2. Typical multiple access schemes.

B. Massive MIMO

Massive MIMO (MaMIMO) was proposed to improve the spectral efficiency by exploiting space diversity through a dense array of antennas on BSs in [5]. This advanced technique can focus the transmitted energy toward the intended receivers while reducing the inter-cell interference and noise when there are sufficient number of antennas. Naturally, this technique can be adopted in the aforementioned heterogeneous networks to support wireless big data transmissions. More specifically, a BS can send downlink signals to each legitimate user without inter-user interference after conducting the estimation of channel state information (CSI) [6]. The estimated downlink state of the mth legitimate macro-user, $\hat{\mathbf{H}}_m$, can be obtained based on the uplink estimation $\mathbf{H}_m$ and the channel reciprocity. Example estimation techniques include minimum mean square error (MMSE) estimation [7] and semi-blind estimation [8]. Intuitively, one can beamform legitimate signals in a targeted fashion using the estimated downlink state to decrease leakage in non-transmitting directions. Hence, we are able to reduce the risk of being wiretapped. It is worth noting that an inaccurately estimated CSI can hurt the performance of MaMIMO.

The existence of passive Eves, whose CSI information is not available, presents a challenge for a MaMIMO system. A preliminary study appeared in [9], where the secrecy outage capacities for amplify-and-forward and decode-and-forward were investigated under the situation when Eves' CSI was not available. Furthermore, a bound of the secrecy outage capacity was derived for the case when the number of antennas approaches infinity.

Another factor that can impact the secrecy performance for a MaMIMO system is pilot contamination, which is caused by reusing pilot signals between different cells (also known as inter-cell pilot multiplexing). A number of schemes have been proposed to mitigate pilot contamination during the phase of channel estimation [10]. Yet, a smart Eve with an active attack capability may send the same pilot sequences to interfere with the legitimate ones. So far, limited work exists in literature to address this issue. A preliminary study was presented in [11], where a unified design was proposed to deal with various scenarios of pilot contamination. Particularly, the combination of matched filter precoding and AN can be adopted for weak contamination attacks with low SNR; while the method of nulling space can be applied for the strong contamination attacks with high SNR.

Lastly, similar to the case of NOMA, the sum of secrecy capacities needs to be optimized when employing MaMIMO and its associated technologies (e.g., AN and precoding). This optimization problem can be formulated as $\max \sum_{u,k} C_s^{u,k}$. Note that the SINRs for the uth user and the kth Eve are different from those of NOMA. For example, the effect of precoding vectors should be taken into account when calculating SINR for a MaMIMO system.

C. Cognitive Radio

In the era of mobile big data, a large number of end-users are expected to concentrate on an access network, which can lead to serious conflicts in the shared spectra (e.g., inter-user interference). Cognitive radio (CR) technology has been proposed to improve the spectrum utilization by dynamically selecting channels without inter-user interference [12]. We assume that macro-tier users, also known as primary users (PUs), shown in Fig. 1, are assigned with licensed spectra. Low-tier users, also called the secondary users (SUs), sense and search for available spectra (i.e., spectrum holes illustrated in Fig. 3). SUs can use the discovered spectrum holes to send data.

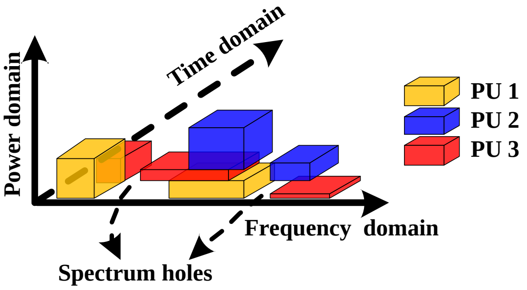


Fig. 3. The spectrum holes in wireless networks.

There are a number of security issues in CR. On one hand, active Eves may seize the licensed spectra, and thus, interfere with PUs' transmissions and reduce the spectrum sharing rate for the SUs. To make matters worse, active Eves can even block the spectrum access opportunities of legitimate SUs through malicious jamming. A number of techniques have been proposed to combat malicious jamming. Examples inlcude spread spectrum and interference alignment [13]. On the other hand, passive Eves may intend to wiretap the private communications of the PUs and SUs. For PUs, MaMIMO can be employed to thwart passive Eves. For SUs, the security challenge is greater because their communications are in the unlicensed spectra. In this case, the problem of security provisioning for SUs is similar to the MaMIMO optimization problem when $u \in \mathcal{L}$.

D. Co-Frequency Co-Time Full Duplex

Another technology that can help alleviate spectrum scarcity is co-frequency co-time full duplex (CCFD), which was proposed in [14]. Different from frequency division duplex (FDD) and time division duplex (TDD), CCFD employs the same frequency and the same time slot to exchange data simultaneously in both uplink and downlink. Typically, CCFD is used in a point-to-point (P2P) communication system for data exchange. Obviously, a CCFD system can introduce self-interference (SI) that results from the usage of the same carrier frequency for signal transmission and reception, which is shown in Fig. 4. As a result, SI can severely damage the received signal and lead to decoding errors.

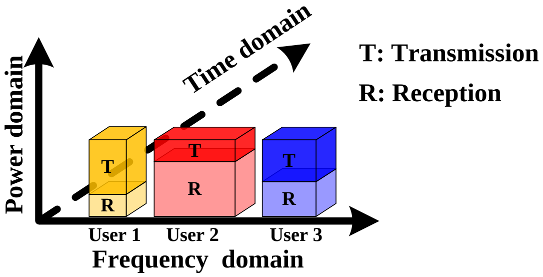


Fig. 4. The CCFD technology in P2P communication.

Nevertheless, SI can be exploited to function as beneficial jamming because it can degrade the received signal quality of an Eve. The key issue is how to cancel the SI for a legitimate user. Currently, the characteristics of various SI have been studied in terms of antenna, analog, and digital. A series of corresponding SI cancellation schemes were proposed in [15]. Specifically, there exist two types of SI cancellation schemes: i) passive suppression and ii) active cancellation, with the former suppressing the SI signal before processing at the receiver, and the latter subtracting a processed copy of the transmitted signal from the received signal.

For a legitimate user, it is relatively easier to utilize active cancellation because the user has the copy of the transmitted signal. The received SINR of the uth user with perfect SI cancellation can be described as γ_u, which can be defined similarly as the one for inter-user interference. The kth Eve without such a receiving capability is subject to the degraded version of the legitimate signals due to the sum of the SI power $\sum_{i \neq u} P_i |\mathbf{H}_{ik}|^2$, $i \in \{\mathcal{M} \cup \mathcal{L}\}$, where P_i is the transmitted power of the ith user with the same carrier frequency as the uth user. It is clear that the received CCFD signal at the Eve's side contains serious contamination. Thus, a CCFD system can improve the security of a communication link when a legitimate user can achieve interference-free receptions.

IV. Open Issues for Typical Applications

In this section, we explain how to apply the aforementioned security solutions in various real networks and applications, and list a few related open research issues.

A. Cellular-based Communications

As we are moving towards 5G cellular networks, advanced technologies such as NOMA and MaMIMO will be adopted to help move a large amount of data at high rates. Under these transmission technologies, suitable schemes such as inter-user interference, AN, and/or precoding may be needed to achieve security enhancement. Particularly, NOMA can help degrade the wiretapping ability of an Eve without affecting the quality of service (QoS) of the legitimate receivers. To further enhance the security performance of NOMA, AN (e.g., friendly jamming) can be applied. For MaMIMO, precoding (e.g., beamforming) can be utilized to improve security performance. Therefore, future research can focus on how to increase the secrecy capacity of the networks and the users by considering various aspects such as inter-user interference utilization, jammer selection, and precoding vector (or matrix) design.

B. Device-to-Device Communications

D2D communications is an emerging technology to improve spectrum utilization and energy efficiency by enabling short-range direct data transmissions between devices rather than through a BS. It can be used to exchange data between cloud servers and distributed sensors without the support from a pre-established infrastructure. In the mobile big data era, D2D communications needs to adopt novel technologies such as CR and CCFD. In general, stations in a typical CR and/or CCFD system usually communicate with each other under the interference of cellular networks. This is also called the underlay transmission mode. Thus, various types of interference and corresponding cancellation schemes need to be investigated in order to satisfy the security requirements of D2D systems.

C. IoT Applications

An IoT network can be composed of devices with integrated functions such as sensing, processing, and communications. Typical IoT applications include machine-to-machine (M2M) networks, vehicular networks, and even smart cities. Previous work in IoT has mainly explored the issues of networking, resource allocation, and scheduling. Recently, privacy and security issues have attracted much attention. More specifically, current studies on IoT focus on data encryption and authentication based on cryptographic tools. Yet, it is very challenging to achieve secure transmissions because of the rich dynamics (e.g., complicated interference and limited computing capabilities) of IoT devices. Subsequently, future research may focus on how to adapt the aforementioned technologies in Section III for IoT devices so as to realize correct signal decoding and degrade the received SINR of Eves under various interference constraints and security requirements.

V. Conclusion

In this article, we first outlined a multi-tired heterogeneous network architecture to support future mobile big data applications. Then, we explained a number of emerging wireless technologies that can be adopted in a multi-tired network architecture. Next we introduced a number of physical layer countermeasures corresponding to each of the emerging wireless technologies that can be employed for secure data transmissions. These countermeasures secured wireless data via adjusting the achievable secrecy capacity. We gave detailed explanations for each countermeasure on how to achieve the desired secrecy capacity by controlling the SINR at eavesdroppers and legitimate receivers. Lastly, we discussed a few open issues and possible research focuses for mobile big data related applications.

Acknowledgement

We are very grateful to all reviewers who have helped improve the quality of this article. This work was supported by the National Natural Science Foundation of China (61471028 and 61572070), the Fundamental Research Funds for the Central Universities (2017JBM004), and the National Science Foundation of the US (AST-1443858, CCF-1442642, and ECCS-1407986).

References

[1] A. Burg, A. Chattopadhyay, and K. Y. Lam, “Wireless communication and security issues for cyber-physical systems and the Internet-of-Things,” *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38–60, Jan 2018.

[2] Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-sanitization for preventing sensitive information inference attacks in social networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[3] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, “Jamming strategies for physical layer security,” *IEEE Wireless Communications*, vol. PP, no. 99, pp. 1–6, 2017.

[4] K. Jiang, T. Jing, Z. Li, Y. Huo, and F. Zhang, “Analysis of secrecy performance in fading multiple access wiretap channel with SIC receiver,” in *2017 Proceedings IEEE INFOCOM*, May 2017, pp. 1–9.

[5] S. Akbar, Y. Deng, A. Nallanathan, M. Elkashlan, and G. K. Karagiannidis, “Massive multiuser mimo in heterogeneous cellular networks with full duplex small cells,” *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4704–4719, Nov 2017.

[6] D. Mi, M. Dianati, L. Zhang, S. Muhaidat, and R. Tafazolli, “Massive MIMO performance with imperfect channel reciprocity and channel estimation error,” *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3734–3749, Sept 2017.

[7] S. Haghighatshoar and G. Caire, “Massive mimo pilot decontamination and channel interpolation via wideband sparse channel estimation,” *IEEE Transactions on Wireless Communications*, vol. 16, no. 12, pp. 8316–8332, Dec 2017.

[8] M. L. Wang, C. P. Li, and W. J. Huang, “Semiblind channel estimation and precoding scheme in two-way multirelay networks,” *IEEE Transactions on Signal Processing*, vol. 65, no. 10, pp. 2576–2587, May 2017.

[9] X. Chen, L. Lei, H. Zhang, and C. Yuen, “Large-scale MIMO relaying techniques for physical layer security: AF or DF ?” *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5135–5146, Sept 2015.

[10] O. Elijah, C. Y. Leow, T. A. Rahman, S. Nunoo, and S. Z. Iliya, “A comprehensive survey of pilot contamination in massive MIMO — 5G system,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 905–923, Secondquarter 2016.

[11] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, “Secure massive MIMO transmission with an active eavesdropper,” *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, July 2016.

[12] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, “Spectrum prediction in cognitive radio networks,” *IEEE Wireless Communications*, vol. 20, no. 2, pp. 90–96, April 2013.

[13] N. Zhao, J. Guo, F. R. Yu, M. Li, and V. C. M. Leung, “Antijamming schemes for interference-alignment-based wireless networks,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1271–1283, Feb 2017.

[14] J. Li, H. Zhang, and M. Fan, “Digital self-interference cancellation based on independent component analysis for co-time co-frequency full-duplex communication systems,” *IEEE Access*, vol. 5, pp. 10 222–10 231, 2017.

[15] D. Kim, H. Lee, and D. Hong, “A survey of in-band full-duplex transmission: From the perspective of PHY and MAC layers,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2017–2046, Fourthquarter 2015.