Received March 23, 2019, accepted April 17, 2019, date of publication May 1, 2019, date of current version May 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2913438

Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City

DONG WANG[1], BO BAI[2], (Senior Member, IEEE), KAI LEI[3,4], (Member, IEEE), WENBO ZHAO[1], YANPING YANG[5], AND ZHU HAN[6,7], (Fellow, IEEE)

[1]New Star Research Institute of Applied Technology, Hefei 230031, China
[2]Future Network Theory Laboratory, Huawei Technologies Co., Ltd., Hong Kong
[3]School of Electronic and Computer Engineering, Peking University, Shenzhen 518055, China
[4]Peng Cheng Laboratory PCL Research, Center of Networks and Communications, Shenzhen 518055, China
[5]Institute of Engineering Thermophysics, Chinese Academy of Sciences, Beijing 100190, China
[6]Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004, USA
[7]Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea

Corresponding author: Bo Bai (ee.bobbai@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61871401, in part by the Anhui Provincial Natural Science Foundation under Grant 1708085MF139 and Grant 1708085QF158, in part by PCL Future Regional Network Facilities for Large-scale Experiments and Applications under Grant PCL2018KP001, in part by the U.S. AFOSR MURI under Grant 18RT0073, and in part by the NSF under Grant CNS-1717454, Grant CNS-1731424, Grant CNS-1702850, and Grant CNS-1646607.

ABSTRACT Heterogeneous Internet of Things (IoT) and multi-access mobile edge computing (MA-MEC) are believed as supporting technologies for building a smart city. The advancement and flourish of IoT are facilitating the entry of human society into the Internet of Everything era, which lay the foundation of the smart city. To address the conflict between computation capability and low-cost mobile devices in IoT, the MA-MEC is available for supporting the resource-limited and computation-sensitive services and applications by computation offloading and distributed content delivery/caching. However, deploying cloud computing capability within the radio access network may face serious security threats, which stem from not only the existing technologies and networks but also the MA-MEC-based IoT itself. Therefore, in this paper, the solutions to address the security threats are investigated from physical layer perspectives, since physical layer security technologies have the advantages of achieving perfect secrecy, low-computational complexity, and resource consumption, and good adaptation for channel changes. Specifically, we investigate the secure wiretap coding, resource allocation, signal processing, and multi-node cooperation, along with physical layer key generation and authentication, to cope with the emerging security challenges. Finally, the paper is concluded with some possible future research directions.

INDEX TERMS Physical layer security, encryption-based security, multi-access mobile edge computing (MA-MEC), heterogeneous Internet of Things (IoT), smart city.

I. INTRODUCTION

Following the rapid development of information and communication technologies, along with the computer science, the vision of building a smart city is close to a reality than ever before [1]. The evolution of Internet of Things (IoT) [2], cloud computing, social networking, and others is pushing technology into the structure of smart city. In this process, the convergence of diversified wireless technologies is indispensable to support smooth technical transition and provide various personalized services. As shown in Fig. 1, multitudinous wireless networks with different infrastructures and technologies, as well as diverse intelligent terminals, often referred to as heterogeneous IoT [3], have been widely applied into smart city for supporting real-time surveillance, remote medical, and intelligent transportation [4], etc. To deploy heterogeneous IoT in practice, multi-access mobile edge computing (MA-MEC) utilizing various radio access technologies adaptively, has attracted increasing concerns, in particular in resource-limited and computation-sensitive scenarios [5]–[8]. MA-MEC, which deploys cloud computing capability within radio access network, provides a

The associate editor coordinating the review of this manuscript and approving it for publication was Jorge Parra.

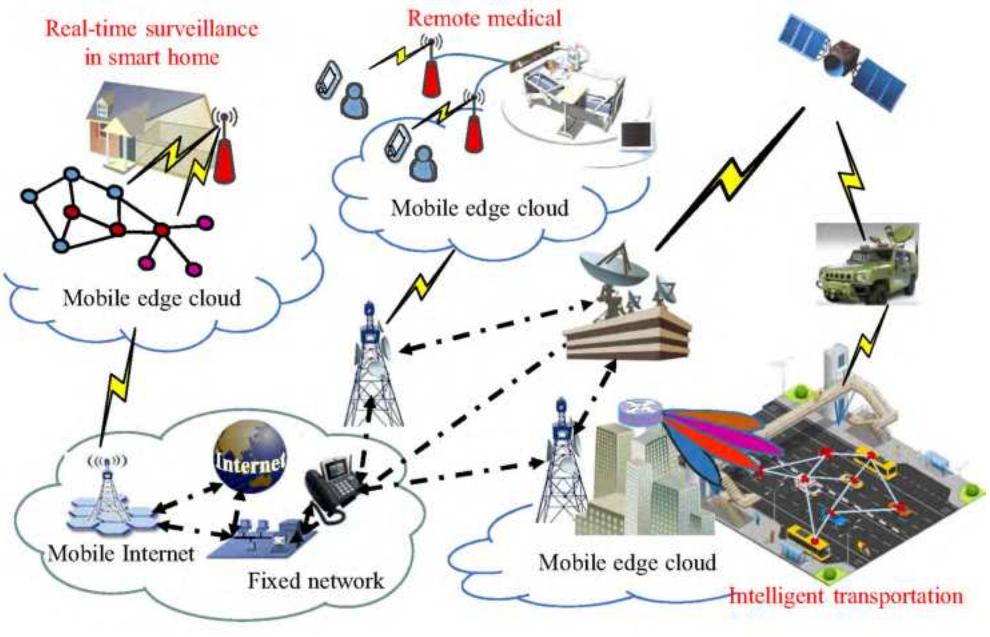


FIGURE 1. Multiple scenarios of MA-MEC based heterogeneous IoT in smart city.

novel perspective to mitigate the heavy computing tasks of mobile terminals by computation offloading [9]–[11]. Applying MA-MEC into smart city can significantly reduce the processing latency of the tasks, avoid the congestion of the central cloud computing, prolong the battery lifetime of mobile devices, and thus improve the quality of service and user experience [5]–[11].

However, some critical issues in building smart city which have been deeply concerned are whether the offered services are secure and trustworthy, and whether the people's data is securely transmitted and stored [12]. Specifically, while enjoying the benefits of MA-MEC based IoT in smart city, some inherent drawbacks are also introduced for accessing mobile edge cloud, which bring potential security risks for confidential data exchanges. For instance, the implementation of MA-MEC in heterogeneous IoT may expand the scope of malicious attack compared with the conventional local data exchanges, since MA-MEC needs to exchange data between smart devices and mobile edge cloud. Furthermore, the distributed and heterogeneous deployments of IoT are beneficial to adversaries to well disguise themselves, so that it is much more difficult to recognize the attacks. Although the densely deployed small cells will benefit the realization of MA-MEC, the evolution towards the architecture of high-density small cells in future heterogeneous access networks also bring critical issues on security, privacy, and reliability of IoT.

For providing security and privacy to smart city data, services, and applications, we need to cope with not only the intrinsic security threats of existing technologies and networks, but also the emerging security threats stemmed from the deployments heterogeneous IoT and MA-MEC. Currently, the developments of communication technologies have also enriched the methods of attacks. All the procedures of information transmission can be attacked by diversified means, such as eavesdropping, traffic analysis, resource consumption, message modification, masquerade attack, denial of service [13]. The real-time connectivity between mobile edge cloud and smart devices, as well as the confidentiality, integrity, correctness, and availability of confidential data can be destroyed. It has been reported in the survey produced by a strategy consulting group, Altman Vilandrie & Company in April 2017, that as many as 48 percent of companies in the US using an IoT network have been the victims of recent security breaches. Therefore, it is of great urgency to develop novel security technologies for building smart city. Consequently, the theories and technologies on information security to support the MA-MEC based IoT have become hot research topics in both academia and industry.

The solutions of information security can be roughly classified into two categories. The first one is the conventional encryption-based security technologies, which is dominant in information security and has been to demonstrate the significant effectiveness in many secure applications [14]. This kind of security technologies, based on the theory of cryptography, is generally adopted at the upper protocol layers above the physical layer [15]. The inherent disadvantages of such security technologies are high algorithm complexity and resource consumption which result from the complicated key generation and management. As discussed in [16] and [17], the traditional encryption-based algorithms and standards are not perfectly appropriate for resource-limited scenarios because of the computational cost and energy consumption. As an option, the other one is the physical layer security technologies, that are believed to be the effective supplementaries of the encryption-based security technologies to further enhance wireless network security from the physical layer. Compared with the encryption-based security technologies, the physical layer security technologies have the following distinctive advantages.

- Achieving perfect secrecy [18], [19]. It has been proved from the perspective of information theory that the physical layer security has the potential to achieve perfect secrecy even though the eavesdropper is computationally powerful. This fact is different from the encryption-based methods which can be decrypted by eavesdroppers via brute-force calculation.
- Low computational complexity and resource consumption [18]. Due to without needing to compute and manage key, physical layer security does not rely on the computing capability of hardware equipments, and is therefore lightweight in terms of computational complexity and resource requirements.
- Good adaptability to accommodate the changes of physical layer. By making full use of physical layer properties, such security technologies can accommodate the changes of wireless channel by optimizing the system parameters and transmission schemes.

Based on the abovementioned observations, this paper mainly focuses on enhancing information security in MA-MEC based IoT via physical layer approaches.

The rest of this paper is outlined as follows. First, wireless information security solutions are briefly reviewed in Section II. Next, in Section III, we focus on the physical layer approaches for enhancing information security in MA-MEC based IoT. Then, a few possible future directions are discussed in Section IV. Finally, we conclude the survey in Section V.

II. WIRELESS INFORMATION SECURITY SOLUTIONS

The conventional solutions to ensure wireless information security are the encryption-based security technologies, which occupy a pivotal position. In order to simplify network designs and facilitate engineering implementation, wireless networks generally adopt the classical open system interconnection protocol architecture, as shown in Fig. 2. By adopting the hierarchical structure of protocol stack, different security mechanisms can be deployed at each layer to achieve the comprehensive security requirements of authenticity, confidentiality, integrity, and availability [20]. For instance, at the link layer, secure medium access control (MAC) can be used for preventing unauthorized access of illegitimate users. At the network layer, the frameworks and secure strategies of virtual private networks (VPN) can be employed to provide the encrypted security services. The secure socket is suitable for deploying at the transport layer to authenticate the legitimacy of a user. The end-to-end encryption methods, such as secure hypertext transfer protocols, can be applied at the application layer to encrypt users' confidential information. These security technologies are deployed at the upper layers of protocol stack, which are based on the cryptography theories. All of them use encryption algorithms or secure logical protocol to implement identity authentication, key distribution, and secure information transfer. Because of the heavy computation workloads and high resource cost, it is limited for applying the encryption-based security technologies into some specific scenarios, such as in infrastructureless networks and low-end network in which the communication equipments may be low-cost with small battery capacity, and their computation capability may therefore be weak. A typical example of aforesaid networks is heterogeneous IoT.

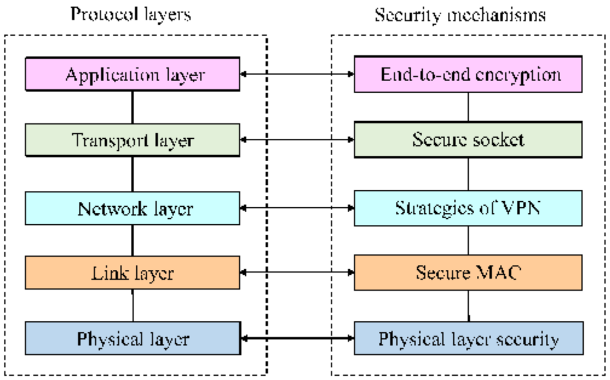


FIGURE 2. The classic hierarchical structure of communication protocol stack and the examples of security mechanisms deployed at each layer.

The pioneering works of information-theoretic secrecy communications and wiretap channel model proposed by Shannon and Wyner [21], [22], respectively, provide a new perspective to reconsider information security and open the door of the research field on physical layer security. Physical layer security based on information-theoretic framework, is considered as very promising security technologies, which focuses on the physical layer to cope with the challenges of wireless information security. The core idea of physical layer security is to implement data secrecy at the physical layer by utilizing the difference between the legitimate channels and wiretap channels which can be generated by the inherent randomness of wireless mediums (such as channel fading and noises) or artificial designs of transmission strategies. It is different from the encryption-based security technologies that physical layer security reduces computational complexity and resource consumption, since this technology does not heavily rely on the computation capability of mobile devices. These advantages make it possible to apply this technology into some resource-limited networks. Moreover, with the full utilization of wireless channel characteristics, physical layer security can flexibly adjust transmission schemes to match the channel changes by the instantaneous optimization and designs of secure transmission strategies.

In MA-MEC based IoT, many practical application scenarios have the following characteristics: no infrastructure, self-organized networking, weak computing capability, limited resources, and so on, which greatly restrict the deployments of the encryption-based security technologies. Physical layer security has the potential advantages of achieving perfect secrecy, low requirement for computing capa-

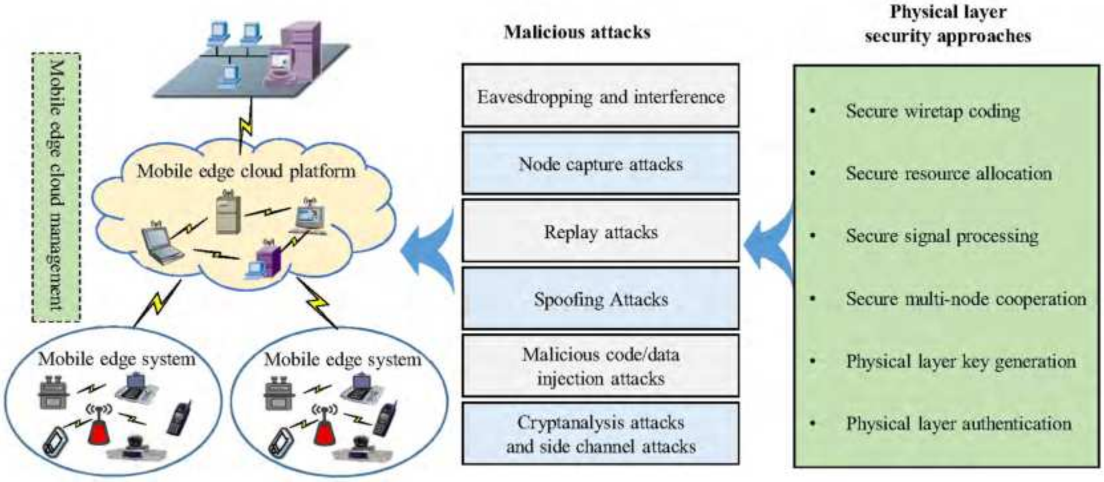

Mobile edge cloud management
Mobile edge cloud platform
Mobile edge system
Mobile edge system
Malicious attacks
Eavesdropping and interference
Node capture attacks
Replay attacks
Spoofing Attacks
Malicious code/data injection attacks
Cryptanalysis attacks and side channel attacks
Physical layer security approaches
Secure wiretap coding
Secure resource allocation
Secure signal processing
Secure multi-node cooperation
Physical layer key generation
Physical layer authentication

FIGURE 3. The malicious attacks to the physical layer of MA-MEC based IoT and the physical layer security approaches.

bility, good adaptation for channel changes, and accessible resource savings. Thus, it can be actively exploited to enhance the information security in the practical applications. Many instances can be observed as follows.

Firstly, for implementing secure information exchanges in computation offloading, secure wiretap coding can be performed to protect confidential information from eavesdropping and attacking. In this coding scheme, the conventional procedures of encryption and encoding are combined into a single design of secure wiretap encoding which ensures both reliability and security of information transmissions and eliminates the issues of key generation and management [18]. Additionally, the rapid increase of energy consumption in wireless networks raises the great demand for green computing [9]. The physical layer security technologies, e.g., secure resource allocation and beamforming/precoding, are beneficial to jointly design green and secure strategies to cope with the double challenges of energy consumption and security threats. It is worth noting that, some works have been shown the great potentials of these technologies for improving information security and energy efficiency simultaneously [23]–[27]. These potentials are very significant to the vulnerable and energy-limited applications in the MA-MEC based IoT. Furthermore, the use cases of MA-MEC in heterogeneous IoT, such as computation offloading and distributed content delivery/caching, may cause severe interference and security risk, especially in ultra dense networks [10], [28]. To address this issue, the secure signal processing technologies known as beamforming and precoding, can be exploited to strengthen or weaken signals in certain directions to achieve secrecy improvements and interference management. Moreover, to implement MA-MEC, we can utilize any network devices with the capabilities of computing, storage, and networking [29]. Thus, by using multiple mobile edge nodes, we can form a virtual multi-antenna system to perform distributed signal processing. Also, the mobile edge nodes can be utilized cooperatively not only for computing and storage [5], but also for forwarding confidential information to improve transmission quality [30], [31] and generating artificial interference to confuse attackers [32]–[34]. Besides, in the MA-MEC based IoT, the lightweight key generation approaches for hybrid security solutions are greatly required to lessen the computing burden of low-cost devices. The randomness and uniqueness of wireless channels can be explored for physical layer key generation which only requires non-complex operations and can be implemented using the off-the-shelf hardware with only a change to the drivers [35]. Finally, it is difficult for the attackers to impersonate the specific physical characteristics since that are closely related to the propagation environments and hardware imperfections of the transceivers. Accordingly, we can exploit the specific physical characteristics to perform physical layer authentication for securing MA-MEC based IoT.

Motivated by the aforementioned observations, in order to provide a comprehensive understanding for the advantages of physical layer security technologies, some security approaches based on physical layer viewpoints are discussed in the following section.

III. PHYSICAL LAYER SECURITY FOR SECURING MA-MEC BASED IOT

Due to the openness and sharing of the MA-MEC based IoT and the broadcast nature of wireless transmission, the information security is extremely vulnerable to malicious attacks, such as eavesdropping and interference, node capture attacks, replay attacks, spoofing attacks, malicious code/data injection attacks, cryptanalysis attacks and side channel attacks, etc. [29]. Therefore, the secure approaches focusing on the physical layer characteristics attract increasing concerns, which usually involve secure wiretap coding, resource allocation, signal processing, multi-node cooperation, physical layer key generation, and physical layer authentication, as illustrated in Fig. 3. In this section, we review these physical layer approaches to cope with the security challenges.

A. SECURE WIRETAP CODING

It has been demonstrated that the imperfections of wireless channels resulted from noise, fading, and interference are no longer the burdens for implementing secure communications at physical layer. Inversely, as discussed in [36]–[38], by suitable secure coding designs, the negative impacts of imperfect wireless channels can be harnessed to achieve not only error correction for legitimate users but also information-theoretic security against adversaries. To this end, the secure wiretap coding is the primary considered security strategy in MA-MEC based IoT, which usually involves stochastic coding, error-control coding, and network coding.

1) STOCHASTIC CODING

The classic secure wiretap coding is stochastic coding, in which a secrecy code must exhibit a nested code structure [18], [36], [39]. In this coding scheme, as illustrated in Fig. 4, a mother codebook with $2^{n(R_s+R_e)}$ codewords is generated through the distribution probability of inputs x_n, while the mother codebook is indexed by (w_s, w_e) with $w_s \in \left\{1, \cdots, 2^{nR_s}\right\}$ and $w_e \in \left\{1, \cdots, 2^{nR_e}\right\}$. Here, the code rate is split into the rate R_s of actual secret messages and the rate R_e of protection messages with no information content. For each of the messages $\boldsymbol{w}$ to be transmitted securely, a sub-codebook indexed by w_s of the mother codebook is associated with the given message, and the transmitted codeword is then randomly selected within the sub-codebook by selecting w_e randomly from $\left\{1, \cdots, 2^{nR_e}\right\}$. Accordingly, the codeword (w_s, w_e) will be sent. By such a stochastic encoding scheme, the reliability and security of confidential messages can be guaranteed simultaneously, since the enough redundancy of the mother codebook provides the safeguard for reliable decoding of legitimate receivers and the sufficient randomness of the sub-codebook increases the adversary's uncertainty about the transmitted message [39].

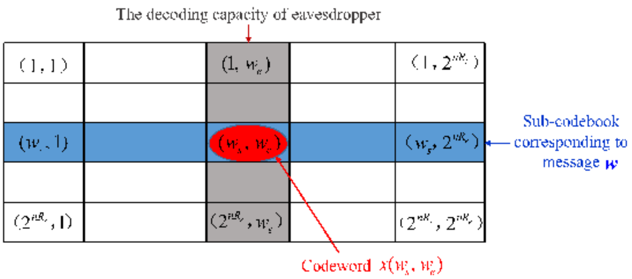


FIGURE 4. The nested structure of a secrecy code.

2) ERROR-CONTROL CODING

In addition to stochastic coding scheme, some popular channel coding schemes can be examined and exploited for the secrecy applications in MA-MEC based IoT. In the family of error-control coding, low-density parity-check (LDPC) codes and polar codes play very important roles in coding for secrecy. LDPC codes constitute a family of graph-based block codes, which can approach the fundamental limits of channel coding when the block length is large enough [19]. LDPC codes can be generated with a sparse parity-check matrix that is intuitively characterized by a bipartite graph known as a Tanner graph [36]. By constituting a Tanner Graph and its sparse parity-check matrix, we can easily define LDPC codes for secrecy. In practical applications, in order to construct a nested code structure for secrecy coding, some refined LDPC codes can be exploited, such as two-edge type LDPC codes, punctured LDPC codes, and coset coding with the dual of LDPC codes.

Polar codes [40]–[43], as a family of low-complexity linear block codes, are rooted in the channel polarization phenomenon [44]. Channel polarization, including channel combination and channel decomposition, can divide the channels into noiseless subchannels and pure-noise subchannels. By using the polarized channels, the information bits can be transmitted to the intended nodes and adversaries over the noiseless subchannels and pure-noise subchannels, respectively. Therefore, the intended nodes can decode the secret bits securely and reliably due to almost noiseless transmissions, whereas the adversaries cannot obtain any secret bit due to pure-noise transmissions [45]. Accordingly, the information security can be guaranteed by such a coding scheme. In addition, other coding schemes can also be adopted for secrecy improvements, such as turbo code based coding schemes and nested lattice coding schemes. In [46], a turbo code-based scheme for adaptive secure channel coding is proposed to enhance the security and reliability of information transmission. In [47], the nested lattice codes are exploited for cooperative jamming. The aforementioned coding schemes may be difficult in decoding, but they are typical and effective for secrecy at the access point side.

3) NETWORK CODING

Network coding which is extensively used in cooperative networks, can bring remarkable benefits in terms of throughput, reliability, and security [48], [49]. The core idea of network coding is that the coding strategy allows the intermediate nodes in a cooperative network to mix different data flows through algebraic combinations [19]. Considering a very common scenario of the MA-MEC based IoT, as illustrated in Fig. 5, where two nodes exchange data with an intermediate node, the network coding can then be performed at the intermediate node by simple exclusive-or operations with the two received messages, and a combined message is sent in a single broadcast transmission. Accordingly, the energy saving and delay reduction can be achieved due to the decrease of transmissions and timeslots, while the security

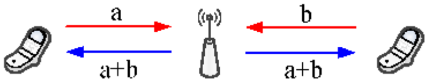


FIGURE 5. A typical example of wireless network coding.

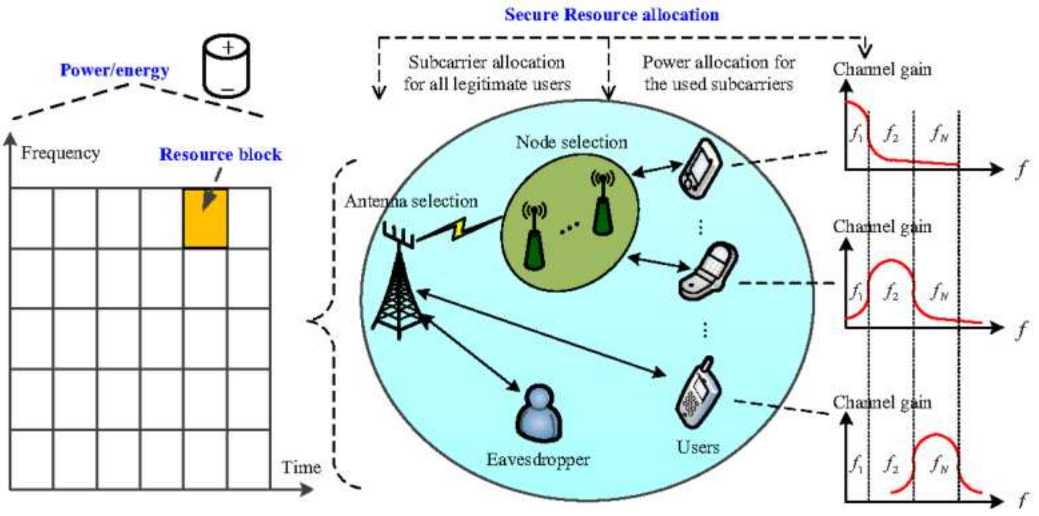


FIGURE 6. The multi-dimensional characteristics of wireless network resources.

can be guaranteed by the algebraic combinations of multiple datagrams that improve the ambiguity of the transmitted messages. To achieve high performance requirements, some complicated network coding schemes can be designed for transforming data packets into a collection of symbols from a specific finite set, and then a linear combination of these symbols is retransmitted over the network. According to [19], from the viewpoint of network security, the network coding protocols can be classified into two main categories including stateless and state-aware protocols, where the former without the need of any state information to compute a network code can be supported by random linear network coding and the latter relying on partial or full network state information to compute a network code can be carried out by optimizing coding operations.

B. SECURE RESOURCE ALLOCATION

It has been widely investigated that wireless network resources have great potentials for enhancing physical layer security. By exploiting the multi-dimensional resources of wireless networks, it is possible to intentionally extend the difference between legitimate channels and wiretap channels, so that a high rate for secrecy coding can be achieved to improve secrecy level. Therefore, secure resource allocation is an available countermeasure against security attacks in MA-MEC based IoT, which can be performed between end-devices and mobile edge cloud or implemented among cooperative edge nodes.

As shown in Fig. 6, the multi-dimensional wireless network resources typically include the frequency, timeslot, and power in orthogonal frequency division multiple access (OFDMA) networks. In multi-antenna and multi-node wireless networks, the resources generally refer to the spatial degrees of freedom provided by multiple antennas and nodes, which bring the opportunities for secure resource management in spatial dimension. In such multi-antenna and multi-node scenarios, secure resource management implies selecting appropriate antenna or node set for end-devices and mobile edge nodes with the multiple objectives of security, reliability, and power/energy savings.

When the MA-MEC is supported with OFDMA technology, some granular methods for secure resource allocation can be implemented to allocate the optimal time-frequency resource blocks and the power level for information transmission under the measurements of secure performance metrics. To be specific, secure resource allocation is to select the best time-frequency resource blocks (measured by secrecy rate or other secure performance metrics) for legitimate user pairs, and to allocate power adaptively over the selected resource blocks according to channel changes. For achieving these purpose, the global optimization of joint subcarrier and power allocation is performed over all resource blocks based on instantaneous channel state information (CSI) [50].

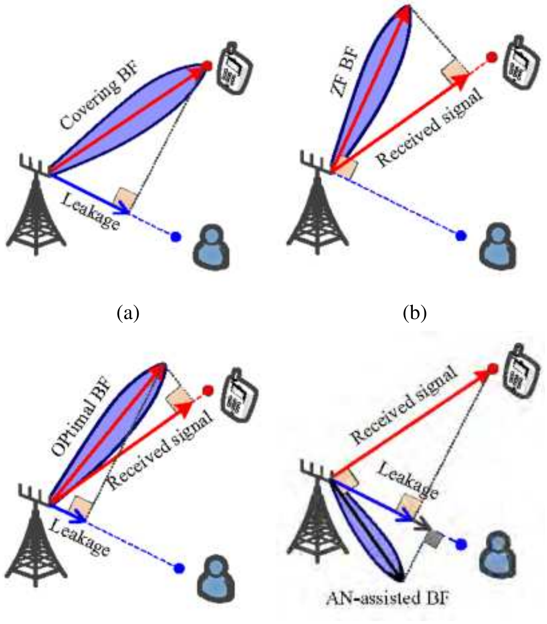
Following multi-antenna technologies applied into the heterogeneous IoT, the information secrecy can be improved from the spatial dimension by exploiting multiple antennas. In such scenarios, it may be harmful to directly use all antennas for transmission, since the received signals at legitimate user and eavesdropper can be enhanced simultaneously by multi-antenna diversity gains whereas the difference between them may be decreased. Therefore, in this case, secure resource management can be carried out to select appropriate antennas for legitimate user pairs to enlarge the difference between legitimate channels and wiretap channels and to save power/energy simultaneously [51], [52].

Furthermore, in cooperative networks, the relaying technologies can be introduced for establishing a network connection while protecting from eavesdropping. Then, the secure resource management will be further expanded to the cooperative edge nodes, which involves the optimal relay selection combined with subcarrier and power allocation. By designing the optimal security strategy of joint node management and resource allocation, the secrecy enhancements and power/energy savings can be achieved at the same time to support MA-MEC [23], [25], [27].

C. SECURE SIGNAL PROCESSING

The deployments of multiple antennas and nodes in the MA-MEC based IoT are beneficial to secure signal processing which usually refers to beamforming (BF) and precoding [53]. By secure beamforming, one-rank transmission is performed to transmit single secret data stream over multiple antennas or nodes, while by secure precoding, multi-rank transmission is carried out to transmit multiple data streams over multiple antennas or nodes. Generally speaking, the beamforming serves as a special case of the precoding [53]. Both of the two signal processing techniques are designed for taking advantage of spatial diversity or multiplexing gains, such that a high level of secrecy can be achieved, while achieving high transmission efficiency and reliability.

The secure beamforming/precoding can be roughly categorized into four classes, that are covering beamforming, zero-forcing (ZF) beamforming, optimal beamforming, and artificial noise (AN) assisted beamforming [45], as illustrated in Fig. 7. The covering beamforming, such as maximum ratio transmission beamforming, controls the beam towards the intended nodes for achieving precise coverage while strengthening the intended nodes' signals simultaneously. However, the covering beamforming may lead to information leakage on the direction to the adversary, as shown in Fig. 7(a). The ZF beamforming can overcome the faults of information leakage to the adversary by completely suppressing the beam towards the adversary, as depicted in Fig. 7(b). The ZF beamforming is of particular interest in practice because of its low-complexity implementation which can be easily carried out by finding the null space of the wiretap channels. As a result, the apparent feature of ZF beamforming is that the beam vector is orthogonal to the adversary's channel vector. However, the ZF beamforming is not optimal for precisely covering the intended node. In order to achieve the optimal performance requirements of physical layer security, the optimal beamforming is globally designed with the considered security objectives and resource constraints, as illustrated in Fig. 7(c). However, the resulting procedures and information leakages from such an optimal design may be inevitable. Therefore, some suboptimal beamforming schemes with low complexity may be more practical choices in MA-MEC based IoT.



(a) (b)

(c) (d)

FIGURE 7. An illustration of secure beamforming in multi-antenna systems. (a) Covering BF. (b) ZF BF. (c) Optimal BF. (d) AN-assisted BF.

In addition to the abovementioned beamforming techniques, the AN-assisted beamforming is also attractive in physical layer security [54], [55]. The key idea of the AN-assisted beamforming is that the transmitted signal is superimposed with AN by which we can disrupt the reception at the adversary. A simple but not optimal AN-assisted beamforming lets the AN lie in the null space of the legitimate channels, such that the intended node can completely avoid the unwanted influences generated by the AN, as shown in Fig. 7(d). To ensure the global optimal performance of secrecy, the AN-assisted beamforming is usually designed carefully, whereas the computational complexity and AN leakages to the intended node may be unavoidable. In addition, the use of AN may consume additional power, so that the power allocated for transmitting the secret messages is decreased consequentially. Therefore, the AN-assisted beamforming combined with power allocation between the AN and secret messages can be performed to achieve the global optimal performance of secrecy [55].

D. SECURE MULTI-NODE COOPERATION

Multi-node cooperation has been proved to have great potentials for securing wireless transmissions from the framework of information-theoretical security [56], which is also useful in MA-MEC based IoT. The distributed architecture in MA-MEC based IoT provides rich opportunities to carry out secure transmission by using cooperative diversity. Some well-developed cooperative relaying protocols are available, including decode-and-forward (DF), amplify-and-forward (AF), noise-forward (NF), and compress-and-forward (CF) protocols. The DF and AF protocols focus on strengthening the received signals of the intended nodes to improve the secrecy capacity. The NF protocol allows the relay nodes to forward information and emit AN simultaneously, such that the retransmitted signals are protected from eavesdropping. Specifically, the relays multiply its received signal by a weight, and then superimpose an AN onto the weighted signal, such that the legitimate channels between the relays and the destination are enhanced by the cooperative relaying while the wiretap channels between the relays and the adversaries are degraded by the AN [57]. The CF protocol can be viewed as a variation of the NF [56], in which the relay node retransmits a quantized version of its noisy observations to help the destination decode the source's message, and also transmits independent codewords of AN to confuse the adversaries. It is worth noting that, the cooperative relaying can also be implemented with untrusted nodes for achieving a higher secrecy rate while protecting the confidential data from them [58].

Another interesting strategy is cooperative jamming that allows the intermediate nodes emitting interference signals to degrade wiretap channels. In particular, in multi-hop or full-duplex transmission, not only the intermediate nodes but also the source node and the intended node can be employed for emitting interference signals. For example, in the multi-hop transmission, the destination node and the source node can be enabled to emit interference signals to jam the adversaries in the source broadcasting stage and the relaying stage, respectively [59]. Intuitively, the null-space cooperative jamming is a simple and effective way without any harm to legitimate nodes, since this strategy emits interference signals in the null space of the legitimate channels. It is onefold to perform pure relaying or jamming. The hybrid schemes, as illustrated in Fig. 8, can be developed to combine both advantages of the relaying and jamming strategies to improve secrecy further [60]. The key idea of the hybrid schemes can be summarized as that, by clustering the intermediate nodes, a part of intermediate nodes are used to retransmit the confidential massages while another part of intermediate nodes are used to confuse the potential adversaries. Then, the mode decisions for cooperation can be carefully designed in practice. Furthermore, the great gain of security performance can be obtained by combining the multi-node cooperation with the resource allocation and signal processing, such as multi-node cooperation with power allocation [61], beamforming [62], or AN precoding [57].

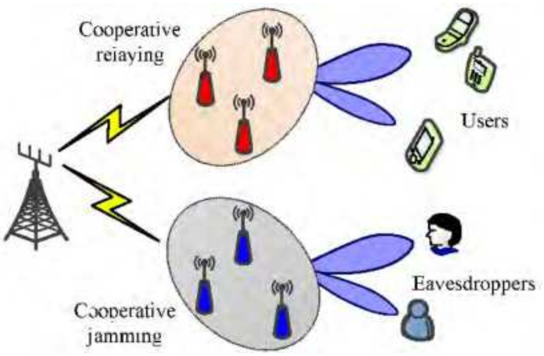


FIGURE 8. A hybrid scheme of cooperative relaying and jamming based on node selection.

E. PHYSICAL LAYER KEY GENERATION

The wireless information transmissions in MA-MEC based IoT provide sufficient randomness for implementing physical layer key generation. Such key generation mechanisms do not depend on computing capability and require any aid from other users. Unlike the traditional cryptographic security which relies on public key infrastructures and cryptographic algorithms to manage secret keys, physical layer key generation is an information-theoretical security technology, since it is based on the channel randomness involving CSI, received signal strength (RSS), and phase information (PI) [35]. In other words, the channel properties including temporal variation, spatial decorrelation, and channel reciprocity, serve as the basis for physical layer key generation [35], [63].

- Temporal variation is caused by the unpredictable movements of transceivers themselves or other objects in the propagation environment, which may make the received signal experience different fading along time. The randomness resulted from such unpredictable fading can be used for physical layer key generation.
- Spatial decorrelation indicates that channel variation is independent over space. To be specific, when an adversary locates more than one-half wavelength away from the legitimate transceivers, it will experience multipath fading that is uncorrelated with the fading between the legitimate user pairs. This property can be used as the random source for physical layer key generation.
- Channel reciprocity implies that the multipath and fading at both ends of the same wireless link (same carrier frequency) are theoretically identical. This property is essential for the physical layer key generation. By using the channel reciprocity, the legitimate users can convert their channel estimates into the same key bits.

A general process of physical layer key generation includes the following subprocesses: channel probing, randomness extraction, quantization, information reconciliation, and privacy amplification [35], as described in Fig. 9. Firstly, the channel probing is performed to collect channel

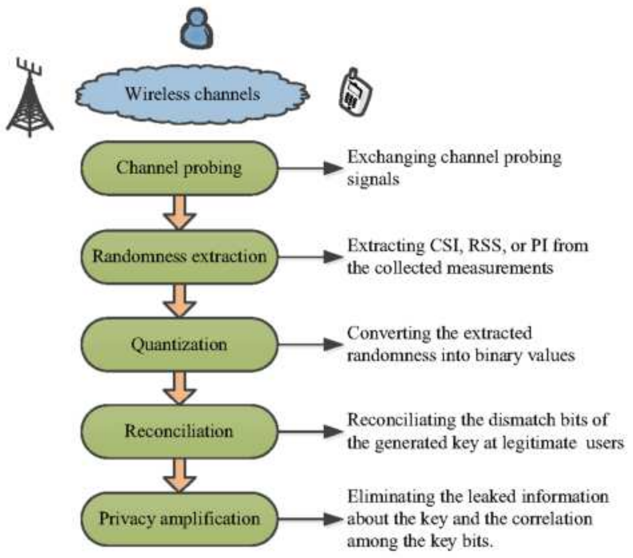

Wireless channels
Channel probing
Exchanging channel probing signals
Randomness extraction
Extracting CSI, RSS, or PI from the collected measurements
Quantization
Converting the extracted randomness into binary values
Reconciliation
Reconciliating the dismatch bits of the generated key at legitimate users
Privacy amplification
Eliminating the leaked information about the key and the correlation among the key bits.

FIGURE 9. The procedures of physical layer key generation.

measurements by exchanging channel probing signals between two legitimate nodes. The channel measurements can be CSI, RSS, or PI. And then the randomness used for key generation is extracted from the collected channel measurements. After that, the quantization is carried out to map the extracted randomness into binary values. When there are key disagreements between the two nodes after the quantization, the information reconciliation is implemented between them for guaranteeing that the keys generated separately at both nodes are identical. However, the information transmitted in the reconciliation stage may be eavesdropped by adversaries as well. This is harmful for the security of key generation. Thus, the privacy amplification is then performed for eliminating the adversaries' partial information about the key and the correlation among the key bits.

According to the choices of the channel parameters, there are four approaches for physical layer key generation, containing CSI-based, RSS-based, PI-based, and wiretap code based approaches, as discussed in [45]. i) The CSI-based approach uses pilot signals and channel estimations to obtain CSI and further to extract channel randomness for key generation, where the CSI mainly refers to the channel impulse response and channel frequency response. ii) The RSS-based approach is based on the measurements of the power carried by the received signals. The RSS is interesting for the key generation in practice, since it is convenient to get the RSS by pilot signals and channel estimations. To increase the key generation rate, the enhanced RSS-based approach can be developed by the deployments of multiple antennas and carriers. The intuitions behind those enhanced approaches are based on the fact that multiple antennas/carriers can provide more channel randomness than single antenna/carrier [63]. iii) The PI-based approach generates keys by using the randomness extracted from the PI of the received signals. This approach is popular, since such an approach can achieve a higher key generation rate and implement efficient group key generation [64]. iv) The wiretap code based approach actually uses the secure coding to transmit some confidential data over wireless channels for forming key bits, which is also available for the implementation of the joint reconciliation and privacy amplification.

F. PHYSICAL LAYER AUTHENTICATION

Generally speaking, authentication is in order to recognize the identity information of communication entities to determine whether the information transmission happens among authorized users and whether the received data has been altered. Traditionally, the secret key based authentication is usually deployed at the upper layers of protocol stack, which generally includes the authentication mechanisms of MAC layer, network layer, and transport layer [20], etc. In contrast, physical layer authentication is carried out at the physical layer by utilizing the physical properties of wireless channels and devices. This security technique may also be remarkably significant for the MA-MEC based IoT. In particular, this security technique may be more effective for resisting against impersonation attacks, since the specific physical characteristics are directly related to the propagation environments and the hardware devices which are rather difficult to impersonate [65].

A common approach towards physical layer authentication is the channel-based authentication which exploits the uniqueness of wireless channels between legitimate nodes to detect intruders. The basic procedures of the channel-based authentication are consisted of the channel probing to estimate CSI and the hypothesis test to determine the legitimation of nodes. Through channel probing and channel estimation, the intended node can measure and store the CSI between the source node and itself. In the initialization of communications, the intended node compares the current CSI with previous records to determine whether the current message comes form the same source node as the previous ones. If the two channel estimates are very close to each other, the intended node concludes that the current and previous messages are transmitted by the same source node, or the current message is transmitted by an intruder otherwise [45], [66], [67]. The mutual authentication of an user pair can be performed by using the similar procedures, as illustrated in Fig. 10.

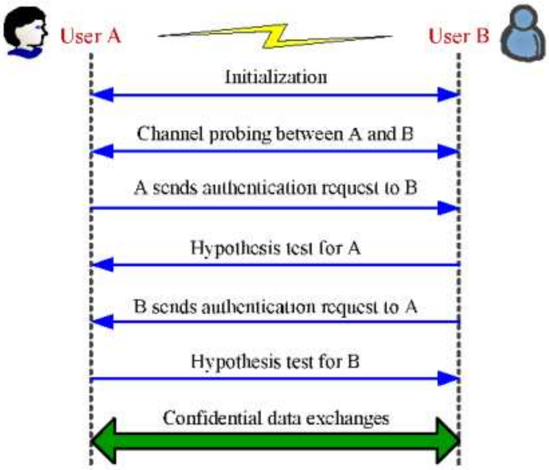

User A
User B
Initialization
Channel probing between A and B
A sends authentication request to B
Hypothesis test for A
B sends authentication request to A
Hypothesis test for B
Confidential data exchanges

FIGURE 10. The mutual channel-based authentication of an user pair.

In MA-MEC based IoT, the channel-based authentication can be implemented based on the fact that the CSI is location-specific, due to unique scattering, reflecting, spatial variability, and multipath delay which lay the foundations for the channel-based authentication. In addition, within the coherent time, the channel is substantially unchanged. This fact also provides the opportunity to employ the temporal correlation for message authentication [45], [68]. Furthermore, power spectral densities can also be used for authentication by comparing two random signal realizations to ascertain whether they have identical power spectral densities [69].

Besides the channel-based authentication, radio frequency fingerprinting is also useful for authentication. The core of this technique is based on the discriminating features extracted from the intrinsic physical properties of hardware

TABLE 1. The comparison of physical layer security approaches.

Approaches	Advantages	Disadvantages	Available countermeasures
Secure wiretap coding	• Increasing the adversary's uncertainty about the confidential data. • Resisting against eavesdropping and intercepting.	• Increasing information redundancy. • Sensitivity to channel fading and CSI.	• Improving secrecy rate by resource allocation, signal processing, multi-node cooperation, etc. • Robust designs for secrecy coding.
Secure resource allocation	• Being beneficial to improve resource efficiency. • Considering network performance and user experience jointly.	• Leading to multi-objective resource optimization with high complexity. • Sensitivity to channel fading and CSI.	• Designing suboptimal but well-performing algorithms with tradeoffs among the considered metrics. • Robust designs with security, effectiveness, reliability, and robustness.
Secure signal processing	• Enhancing transmission directions and/or eliminating interference. • Increasing secrecy rate/network throughput or saving resources.	• Bringing about high computational complexity. • Sensitivity to channel fading and CSI.	• Suboptimal designs to balance the performance requirements and computational complexity. • Robust beamforming/precoding.
Secure multi-node cooperation	• Strengthening the legitimate nodes' signals by cooperative relaying. • Emitting AN to confuse adversaries. • Being beneficial to implement cooperative beamforming/precoding.	• Expanding the scope of malicious attacks. • Generating additional power and energy consumption.	• Wiretap coding to resist against eavesdropping from untrusted nodes. • Designing hybrid cooperative strategies to operate in a confidential and green manner.
Physical layer key generation	• Not relying on computational capability. • Requiring no aid from other users.	• Key generation overhead due to reconciliation. • Low key generation rate in some scenarios.	• Accurate channel estimation to avoid key disagreements. • Enhanced approaches for key generation by using diversity technologies.
Physical layer authentication	• Being implemented without incurring additional security overhead. • Being deployed by using the off-the-shelf hardware. • Low cost due to less complicated operations.	• Sensitivity to the imperfection estimations of channels and devices. • Low reliability in dynamic and heterogeneous networks.	• Designing enhanced authentication mechanisms by using multiple attributes and observations. • Integrating the physical layer and the upper layer authentication.

devices and environmental conditions. In practice, the hardware components of wireless nodes usually show certain imperfections which may be caused by the environmental factors and the inherent defects of the hardware components themselves. These hardware specifications can be served as unique features for authentication. For example, spectral analysis can be used to discriminate among nodes with different wireless network interface cards [66], [70]. The carrier frequency offset is also an interesting metric with great flexibility for the device identification [71], [72]. Moreover, other device-specific characteristics including common phase error [72], inphase/quadrature imbalance [73], and the characteristics of digital-to-analog converter and the power amplifier [74], can also be exploited for device authentication.

Additionally, physical layer signal watermarking and wiretap code-based authentication are also within the category of physical layer authentication. The physical layer signal watermarking is an authentication mechanism which delivers the cryptographical credentials of a data source along with the transmitted messages. The scheme of wiretap code based authentication, as another applied approach, can be implemented by designing suitable wiretap codes which are used as authenticating codes. If a receiver can correctly decode the received signals which have been modulated by the authenticating codes, the corresponding transmitter is authenticated. As discussed in [13] and [45], such an authentication approach has been applied in practice, such as the spread spectrum coding which has the authentication function because of the fact that the intruder do not know the spreading codes and thus can not decode the intercepted signals.

In summary, we can briefly compare the abovementioned physical layer approaches in Table 1 for providing more comprehensive understanding. In MA-MEC based IoT, we should carefully design these approaches according to the practical applications to make best use of their advantages and bypass their disadvantages.

IV. FUTURE DIRECTIONS

Although the physical layer approaches for secrecy have been extensively investigated for general wireless networks, there may still be some challenges in applying these approaches into the practical systems of the MA-MEC based IoT in building smart city. Thus, great efforts are still required in this field.

First, the secrecy improvements supported by the physical layer approaches are sensitive to CSI which is essential for the optimal security designs. However, it is difficult to get the perfect CSI in many settings due to estimation error, feedback delay, channel mobility, or other reasons. Moreover, the noncooperation or passivity of the adversaries make it impossible to get any knowledge of the wiretap channels. Therefore, to apply the aforementioned approaches in practice should simultaneously consider the security, reliability, and robustness of confidential information transmission with the imperfect or unknown CSI.

Second, the security of MA-MEC based IoT should be supported by the physical layer approaches with high energy efficiency due to the requirements of green communication and computing, in particular in energy-limited settings. In physical layer security, some redundancy information is generated in wiretap coding and transmitted for protecting the confidential messages against eavesdropping, which however, brings extra energy/power consumption. In addition, at the same time that the information security is enhanced by the multi-antenna and multi-node diversity technologies, additional energy/power consumption is inevitable due to the deployments of multiple antennas and communication nodes. In this sense, the physical layer approaches for secrecy enhancements in the heterogeneous IoT should operate in a confidential and green manner to cope with both the security threats and energy limitation.

Furthermore, great efforts are required for the practical performance verifications and experimental applications of physical layer security approaches in MA-MEC based IoT. It is still theoretical to enhance security via physical layer approaches. The practical performances of the proposed approaches has not been fully verified in practice. The experimental applications of those proposed schemes has not yet been widely carried out. There may be many technical challenges needing to be solved when those approaches are applied into commercial MA-MEC and heterogeneous IoT, and especially when they encounter the novel physical layer technologies of next generation networks, such as massive antennas, millimeter wave communication, full duplex transmission, and dynamic heterogeneous networking.

Last, cross-layer security designs should be further explored by combining the physical layer approaches with the conventional upper layer approaches, so that a comprehensive solution can be designed to achieve high security level. The designs of hybrid security schemes based on the specific security technology at each protocol layer is therefore an interesting topic. However, such a security design is usually followed with extremely high complexity which may limit its practical application. Thus, it is of particular interest to design a low-complexity but well-performing hybrid security scheme according to practical scenarios in the MA-MEC based IoT.

V. CONCLUSIONS

Based on the radical evolution of IoT and cloud computing, as well as social networking and other technologies, smart city is being pushed into reality by many organizations, government agencies, and research institutes. To fulfill the interconnected, instrumented, and intelligent cities, diversified wireless technologies and networks are converged inevitably to support various personalized services with high reliability, security, and trustworthiness. The heterogeneous IoT and MA-MEC are believed as the supporting technologies for smart city, and therefore attract increasing concerns. However, pushing these technologies into the practical application in building smart city will bring potential vulnerabilities and security issues. Therefore, in this paper, we compare the encryption-based security with the physical layer security, and propose to cope with the security challenges in MA-MEC based IoT via physical layer approaches which involve the secure wiretap coding, resource allocation, signal processing, and multi-node cooperation, along with the physical layer key generation and authentication. These approaches are appropriate for the secure application scenarios with low-cost and energy-limited devices, thanks to their low computational complexity and resource consumption. By introducing physical layer security, combined with the upper layer security mechanisms, it can be expected that the information security in the MA-MEC based IoT will be guaranteed comprehensively.

REFERENCES

[1] K. M. Alam, M. Saini, and A. E. Saddik, “Toward social Internet of vehicles: Concept, architecture, and applications,” *IEEE Access*, vol. 3, pp. 343–357, Mar. 2015.

[2] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, “A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT),” in *Proc. IEEE Internet Technol. Appl. (ITA)*, Wrexham, U.K., Sep. 2015, pp. 219–224.

[3] K. Xu, Y. Qu, and K. Yang, “A tutorial on the Internet of Things: From a heterogeneous network integration perspective,” *IEEE Network*, vol. 30, no. 2, pp. 102–108, Mar. 2016.

[4] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, “Green Internet of Things for smart world,” *IEEE Access*, vol. 3, pp. 2151–2162, Nov. 2015.

[5] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, “On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[6] H. Guo, J. Liu, and J. Zhang, “Computation offloading for multi-access mobile edge computing in ultra-dense networks,” *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 14–19, Aug. 2018.

[7] H. Guo, J. Liu, and H. Qin, “Collaborative mobile edge computation offloading for IoT over fiber-wireless networks,” *IEEE Netw.*, vol. 32, no. 1, pp. 66–71, Jan. 2018.

[8] H. Guo, J. zhang, and J. liu, “FiWi-enhanced vehicular edge computing networks: Collaborative task offloading,” *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 45–53, Mar. 2019.

[9] Y. Mao, J. Zhang, Z. Chen, and K. B. Letaief, “Dynamic computation offloading for mobile-edge computing with energy harvesting devices,” *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3590–3605, Dec. 2016.

[10] J. Zhang *et al.*, “Energy-latency tradeoff for energy-aware offloading in mobile edge computing networks,” *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2633–2645, Aug. 2018.

[11] H. Guo, J. Liu, J. Zhang, W. Sun, and N. Kato, “Mobile-edge computation offloading for ultradense IoT networks,” *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4977–4988, Dec. 2018.

[12] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and privacy in smart city applications: Challenges and solutions,” *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[13] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, “Physical layer security in wireless networks: A tutorial,” *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY, USA: Pearson, 2011.

[15] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[16] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[17] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, Sep. 2018.

[18] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[19] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[20] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[21] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[22] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[23] D. Wang, B. Bai, W. Chen, and Z. Han, "Energy efficient secure communication over decode-and-forward relay channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 892–905, Mar. 2015.

[24] N. T. Nghia, H. D. Tuan, T. Q. Duong, and H. V. Poor, "MIMO beamforming for secure and energy-efficient wireless communication," *IEEE Signal Process. Lett.*, vol. 24, no. 2, pp. 236–239, Feb. 2017.

[25] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[26] Y. Wu, K. Guo, J. Huang, and X. S. Shen, "Secrecy-based energy-efficient data offloading via dual connectivity over unlicensed spectrums," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3252–3270, Dec. 2016.

[27] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: A physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861–1874, May 2016.

[28] M. Deng, H. Tian, and X. Lyu, "Adaptive sequential offloading game for multi-cell mobile edge computing," in *Proc. Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–5.

[29] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[30] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[31] Y. Zou and J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*. Cham, Switzerland: Springer, 2016.

[32] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[33] S. Zhang, X. Xu, H. Wang, J. Peng, D. Zhang, and K. Huang, "Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular Internet of Things," *IEEE Access*, vol. 6, pp. 58405–58417, Oct. 2018.

[34] J. Choi, "Physical layer security for channel-aware random access with opportunistic jamming," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2699–2711, Nov. 2017.

[35] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[36] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[37] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[38] R. A. Chou, B. N. Vellambi, M. R. Bloch, and J. Kliewer, "Coding schemes for achieving strong secrecy at negligible cost," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1858–1873, Mar. 2017.

[39] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[40] M. Andersson, R. F. Schaefer, T. J. Oechtering, and M. Skoglund, "Polar coding for bidirectional broadcast channels with common and confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1901–1908, Sep. 2013.

[41] R. A. Chou and M. R. Bloch, " Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[42] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7903–7921, Dec. 2018.

[43] M. Zheng, W. Chen, and C. Ling, "Polar coding for the cognitive interference channel with confidential messages," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 762–774, Apr. 2018.

[44] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[45] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[46] A. Payandeh, M. Ahmadian, and M. R. Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proc.-Commun.*, vol. 153, no. 2, pp. 313–316, 2006.

[47] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[48] A. Mukherjee and A. L. Swindlehurst, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in *Proc. IEEE 11th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Marrakech, Morocco, Jun. 2010, pp. 1–5.

[49] H.-M. Wang, Q. Yin, and X.-G. Xia, "Improving the physical-layer security of wireless two-way relaying via analog network coding," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Kathmandu, Nepal, Dec. 2011, pp. 1–6.

[50] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.

[51] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[52] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[53] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[54] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[55] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

[56] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[57] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[58] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[59] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[60] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.

[61] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[62] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[63] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[64] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1422–1430.

[65] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[66] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[67] S. Mathur *et al.*, "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.

[68] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[69] J. K. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

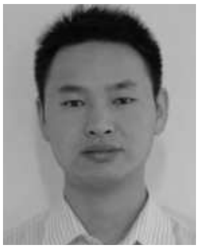
[70] C. Corbett, R. Beyah, and J. Ccpeland, "A passive approach to wireless NIC identification," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Istanbul, Turkey, Jun. 2006, pp. 2329–2334.

[71] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, May 2014.

[72] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346–1354, Dec. 2011.

[73] P. Hao, X. Wang, and A. Behand, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 613–618.

[74] A. C. Polak, C. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.



DONG WANG received the B.S. degree from Chongqing Communication College, Chongqing, China, in 2003, the M.S. degree from the New Star Research Institute of Applied Technology, Hefei, China, in 2010, and the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2016.

He is currently with the New Star Research Institute of Applied Technology, Hefei. His research interests include information security and cooperative communication. He has served as a Reviewer for the IEEE Transactions on Wireless Communications, the IEEE ICCS 2014, *China Communications*, the IEEE Access, and the IEEE Wireless Communications.

BO BAI (S'09–M'11–SM'17) received the B.S. degree (Hons.) from the School of Communication Engineering, Xidian University, Xi'an, China, in 2004, and the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2010.

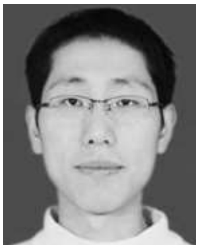
He has received the Honors of Outstanding Graduates of Shaanxi Province and the Honors of Young Academic Talent of Electronic Engineering from Tsinghua University. He was a Research Assistant and a Research Associate with the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, from 2009 to 2010, from 2010 to 2012, respectively. From 2012 to 2017, he was an Assistant Professor with the Department of Electronic Engineering, Tsinghua University. He has obtained the support from Backbone Talents Supporting Project of Tsinghua University. He is currently a Senior Researcher with the Future Network Theory Lab, 2012 Labs, and Huawei Technologies Co., Ltd., Hong Kong. He is leading a team to develop fundamental principles, algorithms, and systems for graph learning, cell-free mobile networking and edge computing, AI enabled networking, and quantum Internet. He is an USENIX Member. He has authored over 90 papers in major IEEE/ACM journals and conferences, 2 book chapters, and 1 textbook. He is one of the founded Vice Chairs of the IEEE TCCN SIG on social behavior driven cognitive radio networks. He has served as a Committee Member of IEEE ComSoc WTC and IEEE ComSoc SPCE. He has served as the TPC Co-Chair of the IEEE Infocom 2018-First AoI Workshop, and the IEEE Infocom 2019-Second AoI Workshop, the TPC Co-Chair of the IEEE ICCC 2018, and the Industrial Forum and Exhibition Co-Chair of the IEEE HotICN 2018. He also served as a TPC Member of several IEEE conferences such as ICC, Globecom, WCNC, VTC, and ICCC. He was a recipient of the Best Paper Award from the IEEE ICC 2016. He has served as a Reviewer of a number of major IEEE/ACM journals and conferences. He was a recipient of the Student Travel Grant from the IEEE Globecom 2009. He was invited as a Young Scientist Speaker at the IEEE TTM 2011.

KAI LEI received the B.S. degree from Peking University, China, in 1998, the M.S. degree from Columbia University in 1999, and the Ph.D. degree from Peking University, in 2015, all in computer science.

He was with companies, including the IBM Thomas J. Watson Research Center, Citigroup, Oracle, and Google, from 1999 to 2004. He is currently an Associate Professor with the School of Electronic and Computer Engineering, Peking University, Shenzhen, and the Director of Shenzhen Key Lab for Information Centric Networking and Blockchain Technologies (ICNLlab.cn). His research interests include data mining, networking, and blockchain.

WENBO ZHAO received the B.S. degree in electronic engineering and the M.S. degree in operations research from the New Star Research Institute of Applied Technology, Hefei, China, in 1994 and 1997, respectively, and the Ph.D. degree in pattern recognition and intelligent systems from the University of Science and Technology of China, Hefei, China, in 2003.

He is currently a Professor with New Star Research Institute of Applied Technology. His research interests include moving target tracking, radar data processing, and statistical signal processing.



YANPING YANG received the B.S. degree in automation and the M.S. degree in electronics engineering from Xidian University, Xi'an, China, in 2008 and 2013, respectively, and the Ph.D. degree from the National Digital Switching System Engineering and Technological Research and the Development Center, Zhengzhou, China.

Thereafter, he was with the Department of Electronic Engineering, Tsinghua University. He currently holds a postdoctoral position at the Institute of Engineering, Thermophysics, Chinese Academy of Sciences, Beijing, China. His research interests include UAV formation flight, wireless communications, cognitive radio networks, and network coding. He serves as a Reviewer for the IEEE JSAC, TCOM, TVT, ICC, and GlobeCom.

ZHU HAN (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, ID, USA. He is currently a John and Rebecca Moores Professor with the Electrical and Computer Engineering Department and the Computer Science Department, University of Houston, TX, USA. He is also a Chair Professor with the National Chiao Tung University, China. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grids. He has received the NSF Career Award, in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society, in 2011, the Best Paper Award for the *EURASIP Journal on Advances in Signal Processing*, in 2015, the IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award for the IEEE JSAC), in 2016, and several best paper awards in the IEEE conferences. He is an IEEE Communications Society Distinguished Lecturer, from 2015 to 2018. He has been a 1% highly cited researcher, since 2017 according to the Web of Science.