Tian, Feng Yu; Zhang, Peng; Yan, Zheng

A Survey on C-RAN Security

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2017.2717852

Published: 21/07/2017

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Tian, F. Y., Zhang, P., & Yan, Z. (2017). A Survey on C-RAN Security. *IEEE Access*, *5*, 13372-13386.
https://doi.org/10.1109/ACCESS.2017.2717852

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN COMPUTATIONAL INTELLIGENCE PARADIGMS FOR SECURITY AND PRIVACY FOR FOG AND MOBILE EDGE COMPUTING

Received May 24, 2017, accepted June 12, 2017, date of publication June 21, 2017, date of current version August 8, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2717852

A Survey on C-RAN Security

FENGYU TIAN[1], PENG ZHANG[1], AND ZHENG YAN[1,2], (Senior Member, IEEE)
[1]State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China
[2]Department of Communications and Networking, Aalto University, 02150 Espoo, Finland

Corresponding author: Zheng Yan (zhengyan.pz@gmail.com)

This work was supported in part by the National Key Research and Development Program of China under Grant 2016YFB0800700, in part by NSFC under Grant 61672410 and Grant U1536202, in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Program 2016ZDJC-06, in part by the 111 Project under Grant B08038 and Grant B16037, and in part by the Academy of Finland under Grant 308087.

ABSTRACT While 4G is speeding up its steps toward global markets, 5G has initiated its full development to satisfy an increasing demand on mobile data traffic and big data bandwidth. Centralized data processing, collaborative radio, real-time cloud infrastructure, and cloud radio access network (C-RAN), along with their excellent advantages are being sought by more and more operators to meet end-user requirements. As a promising mobile wireless network architecture, compared with traditional RAN, C-RAN has incomparable advantages in terms of low power consumption, reduced base station (BS) numbers, and economic capital and operating expenditure. It can also improve network capacity and BS utilization rate. Recently, C-RAN security has aroused special attention and concern. However, the literature still lacks an overall review on it in order to guide current and future research. In this paper, we first overview the architecture, deployment scenarios, and special characteristics of C-RAN. We then provide a thorough review on the existing security studies in the field of C-RAN based on its three logic layers and corresponding security threats and attacks. Particularly, we discuss whether the current literature can satisfy the expected security requirements in C-RAN. Based on this, we indicate open research issues and propose future research trends.

INDEX TERMS Cloud radio access network (C-RAN), security, security threats, 5G, trust.

I. INTRODUCTION

The consumption of wireless terminal data traffic has dramatically increased in recent years. According to a study conducted by Cisco, the global average mobile traffic consumption per user has jumped from 30 mega bytes per month in 2012 to 2000 mega bytes per month in 2017 [1]. The number of mobile devices has tremendously increased as well globally, with average yearly increase at 8.3% Compound Annual Growth Rate (CAGR) from 7 billions in 2012 to 10.3 billions in 2017. Due to the shortage of bandwidth and frequency spectrum, traditional Radio Access Networks (RAN) has such shortcomings as high capital expenditure (CAPEX)/operating expenditure (OPEX), poor user experience, and low spectral efficiency. Thus, it cannot meet increasing demands of both mobile users and mobile network operators. For example, the research in [2] and [3] indicated that a growing number of mobile network operators are becoming more and more cautious about Total Cost of Ownership (TCO) in order to keep their core network profitable and competitive despite the rate of Average Revenue Per User (ARPU) dropping every year.

For 2G, 3G or 4G, the Base Stations (BSs) in RANs are independent from each other. Each BS is located in a small area consisting of a set of sub-systems, e.g., cooling, stand-by power, backhaul network, monitoring system, etc. A RAN connects hundreds of mobile devices, receives and processes signals from an Optical Transmission Network (OTN). Despite its wide deployment, a traditional RAN implies serious waste of wireless spectrum resources [3]. Moreover, a mobile device is often inter-cell interfered by nearby BSs. To overcome the problems of the traditional RANs, IBM defined an initiative concept of Cloud Radio Access Network (C-RAN), which was called Wireless Network Cloud (WNC) at the beginning [4]. Since then C-RAN has drawn world-wide attention since it has potential to solve the shortcomings of the traditional RAN. The next generation mobile communication networks and wireless systems (5G) chose C-RAN as a typical RAN architecture for supporting new mobile communications and services in year 2020 horizon [5]. A C-RAN system consists of a virtualized BSs pool, Remote Radio Heads (RRHs), and a front-haul network connecting RRHs to the BSs pool. In C-RAN, all

BaseBand Units (BBUs) together form a virtualized BSs pool; RRHs collect the wireless signals of all wireless devices; the front-haul network achieves radio signal level cooperative transmission. Through a general processor and Digital Signal Processor (DSP) controller located in the BBUs pool, the C-RAN system can efficiently and dynamically reassign the front-haul network to address changing traffic needs of mobile devices [7]–[11]. Compared with the traditional RAN, C-RAN has the following advantages. First, based on the concept of centralization and virtualization of the BBUs pool, C-RAN manages multiple individual BS cells together as a whole in order to share their physical-layer resources (e.g., frequency spectrum, time and physical location). Second, through real-time cloud computing, C-RAN can effectively balance non-uniform traffic, implement load balancing, process aggregation and dynamic allocation during different timeframes, which solves the 'tidal effect' problem [6]. Third, C-RAN can greatly reduce inter-cell interference. The C-RAN architecture can support high scalability, which can easily add or subtract BBUs. It is a new architecture by applying various open network technologies (e.g., cognitive radio, wireless sensor and multiple input multiple output technology, etc.). By building BBUs in one pool, C-RAN can not only decrease site and bandwidth acquisition, but also make it possible to avoid inter-cell interference by applying joint transmission and reception or joint processing and coordinated beamforming technologies.

However, the security and trust problem of C-RAN is becoming more and more important and serious, which has aroused special concern. In a wireless network, due to its open broadcast nature, a user either authorized or illegitimate, can access it [13]. From the perspective of Open System Interconnection (OSI) network protocol architecture, malicious attacks can take place in different layers. For example, the two main primary attacks in physical layer (PHY) are eavesdropping and jamming attacks (a type of denial of service attacks); in Media Access Control (MAC) layer, the attackers' focus is more of using MAC spoofing, identity-theft attack, Man-in-the-Middle (MITM) attacks and network injection to impact Network Interface Controller (NIC) of multiple network nodes assigned MAC addresses; in network layer, attacks mainly include IP spoofing, IP hijacking and Smurf attack; transport-layer attacks mainly include TCP flooding attacks and sequence number prediction attacks, as well as UDP flooding; particularlly, application layer is the most vulnerable layer. Such attacks as malware attack, Structured Query Language (SQL) injection, cross-site scripting attack, File Transfer Protocol (FTP) bounce attack and Simple Message Transfer Protocol (SMTP) attack can easily happen. From the networking point of view, C-RAN could face various malicious attacks and security threats as described above.

Zuo *et al.* [13] defined a number of security requirements in wireless networks: (1) authenticity that allows the user or device only confirmed by a true network node can be authorized to access restricted network resources via a unique MAC address; (2) confidentiality that prevents unauthorized entities from accessing sensitive data and resources; (3) integrity that ensures the accuracy and reliability of the information transmitted over the wireless network throughout its lifecycle, which means the information cannot be falsified or modified by any malicious users; (4) availability that offers users the possibility to acquire their required network resources at anytime and anywhere, while the network should prevent the violation of availability, e.g., caused by Denial-of-Service (DOS) attacks.

Mitola creatively put forward the concept of Software Defined Radio (SDR) [14] and created such a new research direction of communication technology. Until it was completely defined by European Telecommunication Standards Institute (ETSI), it had attracted great attention. In 1999, Mitola first proposed the concept of Cognitive Radios (CRs) [15], CRs is a new type of radio, based on SDR, which can reliably sense a spectrum environment over a wide frequency band, detect the presence of a legitimate authorized user (primary user), adaptively use the under-utilized part of the spectrum at the same time without causing harmful interference to the primary user throughout its communication process. Cognitive Radio Networks (CRNs) consisting of CRs, as a new wireless network, inherite not only the threats of the aforementioned wireless networks (e.g., eavesdropping, MAC spoofing, identity-theft attack, etc.), but also faces new security threats and challenges. Due to its unique network characteristics, two basic CRNs research directions were proposed [16]: cognitive capability and reconfigurability. In both directions, CRNs face a number of new and specific security threats and attacks, such as Primary User Emulation Attack (PUEA), Spectrum Sensing Data Falsification (SSDF) attacks, Common Control Channel (CCC) attacks, Beacon Falsification (BF) attacks, Cross-layer attacks aimed at multiple layers and Software Defined Radio (SDR) attacks. Correspondingly, At the same time, the literature [17] defined the security requirements in SDR and CRNs as follows: (1) confidentiality that ensures controlled access to resources; (2) robustness that when the system is severely attacked, it cannot completely crash and can also provide basic communication services according to previous established communication protocol or strategy; (3) integrity that includes the protection of system integrity and data integrity; (4) compliance to regulatory frameworks that means a system should be designed by following local operator regulatory standards or frameworks; (5) non-repudiation that implies the system can investigate any users' actions, which cannot be denied, also called accountability; (6) verification of identities that means authenticity.

C-RAN is inherited from CRNs and is in essence a wireless network. Obviously, it also faces many common security threats, such as PUEA, SSDF attacks, etc. As a novel network architecture, due to its transmission and self-deploying nature, it is facing more serious security threats and trust problems than traditional wireless networks and CRNs, so security protection and trust management becomes very important in C-RAN applications. Besides those enumerated

above, there are also extra and new security threats and challenges that we need to explore and overcome when logging into such a new wireless network architecture environment. For example, security and trust should be considered with regard to the virtualized BBUs pool. C-RAN is a distributed network services architecture, its ultimate goal is to use joint processing and scheduling of radio resources to achieve high traffic capacity and to reduce interference of a cellular system. Most of existing literature mainly focused on the design of multi-point processing algorithms, which can take advantage of special channel information and cooperation among multiple antennas in different physical areas to achieve joint processing and scheduling. Nevertheless, the real-time multi-point processing, the transmission of the terminal device data and special channel information or dynamic traffic capacity allocation are done in the virtualized BSs pool. So, the security of the virtualized BSs pool and the trust of cooperation among resources located in different trusted domains are essentially crucial in the C-RAN. However, the existing research of C-RAN still lacks a comprehensive overview on C-RAN security and trust in order to guide current work and direct future research.

In this paper, we perform a thorough survey on C-RAN security by reviewing the existing security schemes of wireless networks, SDR networks and CRNs. We summarize potential security threats in C-RAN and propose security and trust requirements in order to put forward some future security research directions. In particular, the contributions of this paper are described below.

- We introduce the C-RAN architecture, discuss its main application scenarios and summarize its specific characteristics;
- We analyze the security threats and vulnerabilities of C-RAN. We then review the existing literature studies, introduce the solutions to security threats in different logic layers of C-RAN and discuss their pros and cons.
- We propose security and trust requirements in C-RAN and use them as a measure to figure out open problems and propose future research directions in order to motivate the research in C-RAN security and trust.

The rest of this survey is organized as follows. Section 2 introduces C-RAN architecture and main deployment scenarios. We compare C-RAN with the traditional RAN to highlight its specific characteristics. In Section 3, we review the existing solutions to overcome security attacks or threats in C-RAN based on a logical structure of C-RAN [18] that includes a physical plane, a control plane, and a service plane. Section 4 refines the security requirements of C-RAN by considering its specific characteristics. In Section 5, we use the refined security requirements as a measure to compare existing work for discussing open research problems and proposing future research trends in the field of C-RAN security and trust. Our conclusions are presented in the last section.

II. C-RAN ARCHITECTURE AND CHARACTERISTICS

A. C-RAN ARCHITECTURE

Based on the collaboration between the virtualized BBUs pool and RRHs, C-RAN has lower network delays compared to other cellular networks. According to a LTE protocol stack [3], there are L1, L2, and L3 layers in C-RAN. Among them, L1 is the physical layer (PHY), which mainly provides a data transmission service to the higher layers, channel coding, rate matching and Multiple Input Multiple Output (MIMO) technology, etc. L2 is the layer responsible for Media Access Control (MAC), Radio Link Control (RLC) and Packet Data Convergence Protocol (PDCR) that mainly provides data link control. L3 is the Radio Resource Control (RRC) layer that mainly provides signalling and radio resource control. In order to introduce the C-RAN into the traditional RANs and make them compatible with each other, China mobile research institute proposed two C-RAN system architectures [6]. The first is called ''full centralization'', and it integrates L1, L2, and L3 fully into a virtualized BBUs pool. The other is ''partial centralization'', which separates the L1 and integrates it into RRHs. Figure 1 shows the difference between these two solutions, and Figure 2 shows the two C-RAN architectures. The common ground between both is a front-haul link (e.g., digital radio over fiber, etc.), which provides an enormous transmission rate. In general, the virtualized BBUs pool and the BSs in the cloud are responsibility for limiting radio signal transmission and reception, then remote RRHs are used to collect and manage signals from end users based on a general processor and a Digital Signal Processor (DSP) controller.

The first architecture, shown in Figure 2a, integrates all layers (i.e., L1, L2 and L3) and baseband functions into the BBUs pool, benefitted from upgrading software and extending the existing network capacity. Moreover, due to all protocols are located in the virtualized BBUs pool, the operators can protect protocol layer against security threats (e.g., eavesdropping and jamming attacks, identity-theft attack, user access control, spectrum allocation, connection establishment, etc.). Besides, based on the virtualized BBUs pool, multi-standard digital signals can be flexibly and efficiently classified by a multi-cell collaborative signal processing technology. However, this goes along with that the OTN needs higher freeboard bandwidth to carry input/output (I/O) signals. Once the baseband suffers from Small-Backoff-Window (SBW) attack [16], a monopolize attack against baseband, the whole network will suffer from a huge loss.

The other architecture, shown in Fig 2b, integrates collaborative function, L2 and L3 scheduling, and wireless resource allocation into the BBUs pool, benefitted from scheduling the wireless resources and realizing the joint transmission or joint reception in the PHY layer to improve cell edge performance. Moreover, this architecture is similar to the present 4G network architecture, which minimizes the change on existing transport networks. However, due to the fact that RRH in C-RAN is deployed with limited functions (L1 only), the

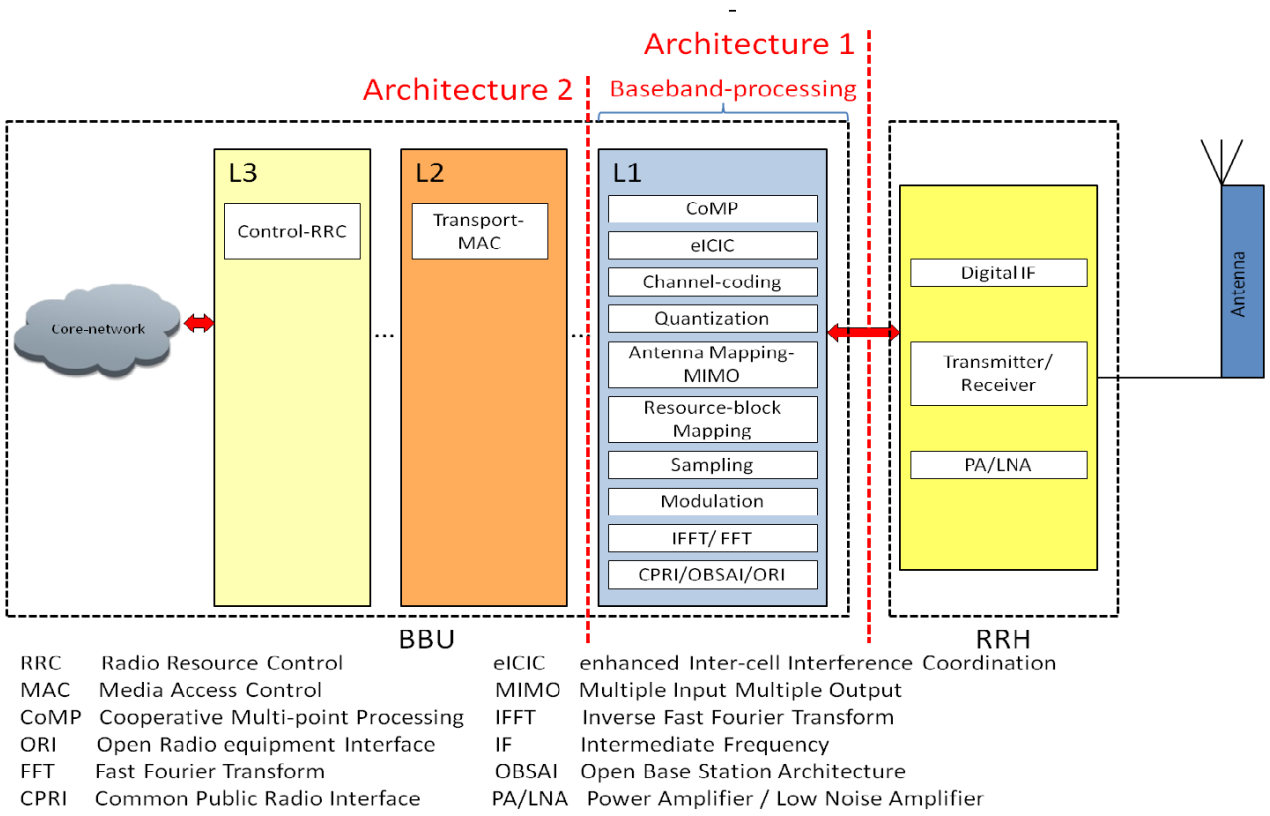

FIGURE 1. Two solutions of C-RAN achitecure design according to different separation of L1 function module.

C-RAN may be vulnerable to the attacks at RRH or fronthaul sides due to lack of authentication, access control, etc.

B. C-RAN DEPLOYMENT SCENARIOS

Current RAN technologies, e.g., Global System for Mobile Communication (GSM), Long Term Evolution (LTE), Long Term Evolution Advanced (LTE-A), etc., can hardly meet end users' traffic requirements. The C-RAN is expected to become a new technology to solve the aforementioned challenges. Different application scenarios (e.g., macro cell, micro cell, pico cell, indoor coverage system, etc) have been studied based on the C-RAN architecture [6]. They were discussed to play as a new alternative approach of current cellular network to improve network performance and deliver rich network services in a cost-effective manner. In this part, we do not discuss all deployment scenarios since they are not the emphasis of this article. We mainly overview some of the common scenarios that could be vulnerable to large-scale security threats.

1) SCENARIO 1

In this scenario, many people are assembled in highway, subway or railway, where they change their locations quickly [6]. In the traditional network architecture, when an end user's terminal device switches too fast from an original cell to a new one, drop call phenomena could often happen. In this scenario, the first architecture can solve the drop call problem better. First, it decreases the number of base stations by centralizing the deployment of the BBUs in outdoor machine rooms or a specialized management center. Second, small and flexible remote RRHs can be installed in lampposts, shelters or waiting halls, which is not only suitable for this scenario, but also avoids severe equipment damage and fast frequent handovers.

2) SCENARIO 2

In this scenario, we mainly discuss the places with the nature of a 'tidal effect' phenomenon, which is also called as Integrated Service Access Zone (e.g., high science and technology parks, residential neighborhoods, industrial parks or college campus, etc.). Moreover, in these places at a rush hour, BSs' spectrum efficiency is low, which cannot be solved by the traditional RAN well due to limited power, memory storage and computing capability [6]. In this scenario, the partial centralization architecture becomes a better choice. This architecture integrates the baseband processing into RRHs and deploys some BBUs in remote sites. The cooperation of both can quickly conduct joint transmission or joint reception in a cell interval based on the joint processing and coordinated beamforming technology. However, due to the L1 separates from the virtual BBUs pool, there are many security threats against the physical layer's functions.

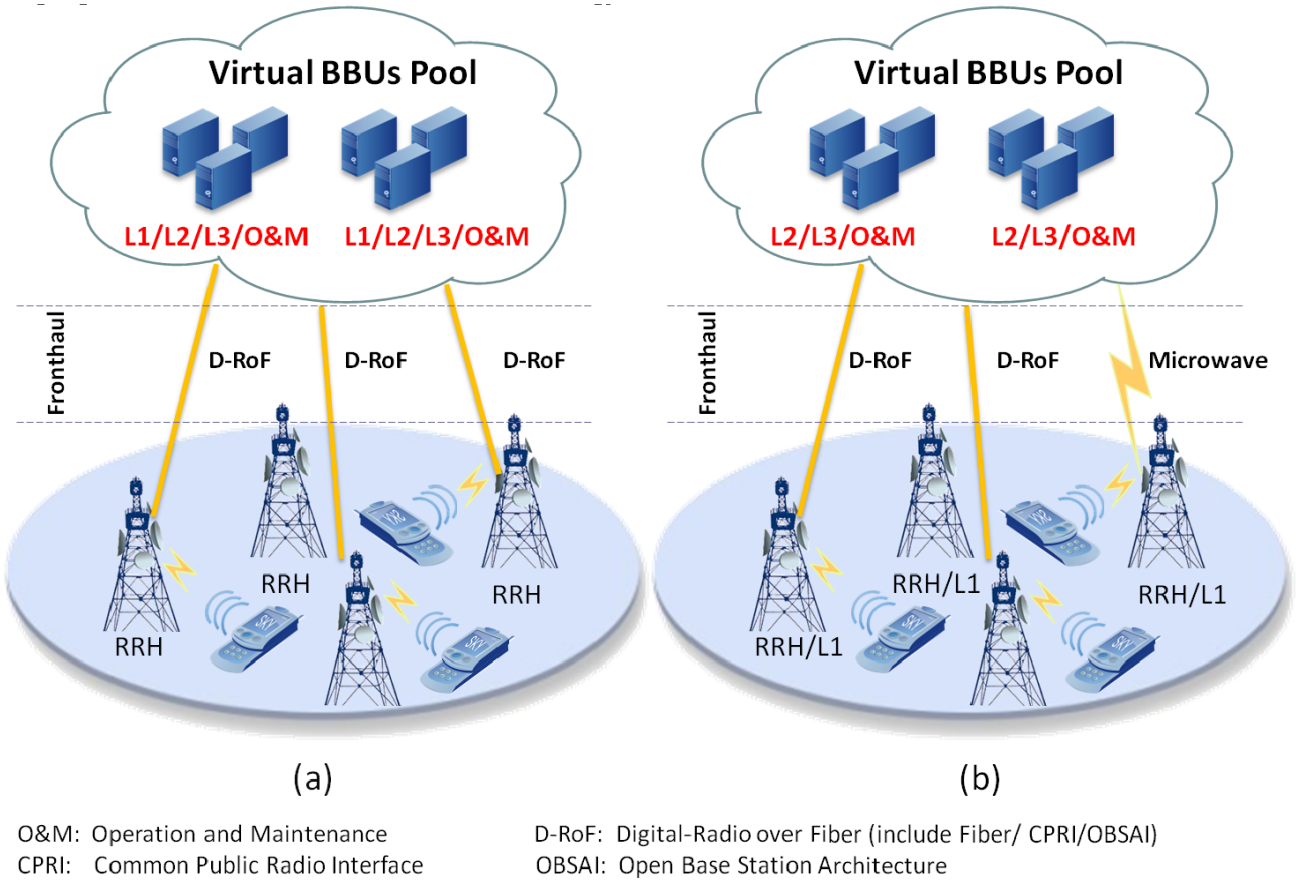

FIGURE 2. Two different C-RAN architectures based on different locations of L1 functions: (a) fully centralized architecture and (b) partially centralized architecture.

3) SCENARIO 3

Another representative application scenario occurs in the places where many different wireless access networks coexist, such as GSM, WLAN, Ad Hoc network, etc [6]. We call it a heterogeneous network environment. In this environment, different kinds of network connect to the core network, and integrate into a whole through a same gateway. A unified management platform manages all heterogeneous wireless network resources, which not only provides users with ubiquitous services and seamless handovers, but also improves the utilization of resources. Rawat *et al.* [10] discussed secondary users and primary users competitively shared one RAN system's idle spectrum resources. They proposed a secure spectrum resource sharing algorithm based on cloud computing. In this scheme, the spectrum occupancy information of heterogeneous cognitive radio networks is stored in a cloud computing unit. The cloud computing unit is in charge of secondary user identity authentication, the access of spectrum opportunities, and connection establishment. In this scenario, the remote cloud computing unit plays an important role in the whole RAN architecture. Once the cloud system is under wholesale attackes from the outside, the whole network service will be paralysed.

C. SPECIFIC C-RAN CHARACTERISTICS DISTINGUISHED FROM TRADITIONAL RAN

The C-RAN network architecture has some similarity to the traditional RAN, but it also has some distinct differences as described below [6].

First, BBUs are centralized. The traditional BSs' architecture is all-in-one, and each or some need a separate computer room. C-RAN applies a distributed architecture, and BBUs and RRHs together play the role of BSs. Hundreds and thousands of BBUs are placed centrally in a big computer room, and the RRHs are placed in the outdoor.

Second, different BBUs closely corporate with each other in the same virtualized BBUs pool. Different BBUs can quickly and efficiently exchange idle spectrum resources, channel information and user data by introducing a real-time and high-speed internal infrastructure, which reduces the inter-cell interference and improve the whole system's capacity.

Third, the relationship between BBUs and baseband computing resources is one-to-many. In the C-RAN architecture, baseband computing resources no longer belong to a BBU alone but belong to the virtualized BBUs pool. Moreover,

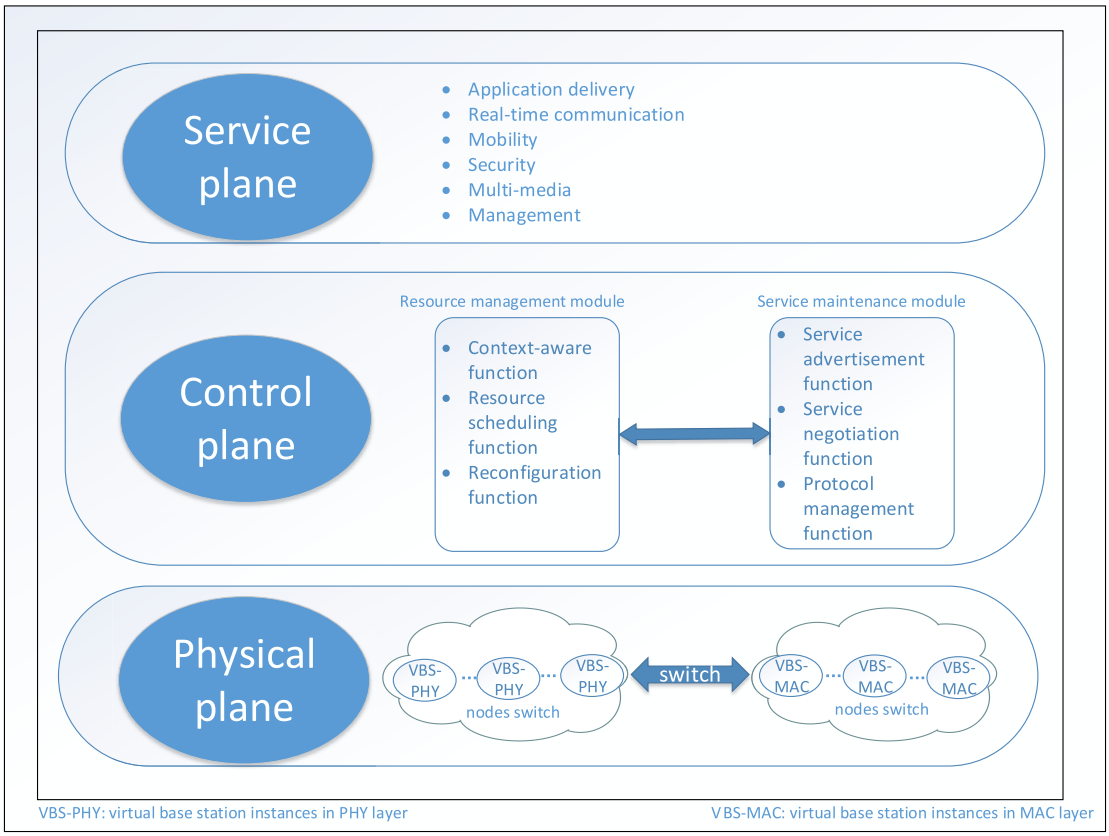

FIGURE 3. C-RAN logic architecture.

Resource allocation is shared in a common pool of virtualized resources.

Fourth, the base station is software defined. In the C-RAN architecture, the BBUs realize the function of baseband processing based on a uniform and open software radio platform. The BBUs can support multi-standard air interface protocols and easily upgrade wireless signal processing algorithms. In addition, virtualization technology makes BSs very flexible, and the BSs of different operators can establish collaboration and work together in an easy way, through sharing resources and processing power of the BSs. However, there still remains some unsolved security and trust problems in practice, such as identity authentication across operator domains, trusted collaboration establishment, trusted cooperation environment, etc.

III. SOLUTIONS OF SECURITY THREATS AND VULNERABILITIES IN C-RAN

In 2015, Wu *et al.* [18] proposed a novel logical structure of C-RAN, which includes physical plane, control plane, and service plane, as shown in Figure 3. It focuses on service-oriented cloud architecture, commerce and personal resource scheduling and management. In this section, we review and discuss existing solutions to resist the threats and attacks in the C-RAN communication system based on the C-RAN logical structure. We make a comprehensive investigation and summary on existing work about C-RAN security and point out their advantages and shortcomings.

A. SOLUTIONS TO OVERCOME THREATS RELATED TO PHYSICAL PLANE SECURITY

As we can see in Figure 3, the physical plane is mainly responsible for performing virtualized resource allocation, node switch (e.g., signal transmission and processing) and baseband pool interconnection based on the channel decoding technology, multi-point processing, Fast Fourier Transform (FFT), and so on. The safety of the physical plane is a foundation that guarantees a secure and reliable C-RAN system. This plane has been a focus of security concern. The existing work mainly focuses on overcoming the the following attacks and threats.

1) EAVESDROPPING ATTACK

Massive MIMO technology has drawn operators' attention and will be integrated in 5G network architecture. It is one of the key techniques of C-RAN physical layer. However, corresponding security problem occurs immediately. Eavesdropping attack is a common problem in all RANs. To prevent BS and channel estimation from passive eavesdropping and active attacks, Kapetanovic *et al.* [19] discussed the benefits of Massive Multiple-Input Multiple-Output systems to

physical security, and introduced two schemes for detecting the eavesdropping attack. In the first scheme, a legitimate user can generate an additional random phase-shift keying sequence, and the BS can effectively detect the eavesdropping attack through the received sequence. In the second scheme, there is no need to generate additional random sequences. The beamformer is adopted to detect the eavesdropping attack. Benefited from the same beamformer (between a BS and an initial user), the BS transmits a pilot to the initial user based on a received signal. The initial user can compare this pilot with a previously agreed value (between the BS and the initial user). When eavesdropper forges and modifies the original information to BS, this value will change. However, compared to a cooperative detection scheme, there is a shortcoming of these two schemes since they need more than two interactions (between the BS and the initial user) to detect the attack, which increases communication overhead.

2) JAMMING ATTACK

It is also called DoS attack, which means a malicious node interferes with other network nodes' radio frequencies by sending out white noise or other useless network traffic signals. Mpitziopoulos *et al.* [20] surveyed the most common jamming threats in wireless sensor networks, such as spot jamming, sweep jamming, barrage jamming, and deceptive jamming. The authors classified the jamming attacks and summarized four possible jamming goals: (1) through an immediate DoS attack to block user access to the radio network nodes; (2) occupying most of the spectrum and leaving a small portion of the spectrum to degrade core network functions; (3) learning the defense strategy of the core network in order to achieve the next attack; (4) herding of a jammer by attacking a radio network node concert with other malicious jammers.

3) IMPERSONATION ATTACK

Impersonation attack is often mentioned as a threat in the literature. In the traditional radio network architecture, there are two types of main impersonation attacks: Cognitive Radio (CR) node impersonation attack and primary user impersonation attack. In the first type, assuming that a CR node is attacked, it can cooperate with other attacked nodes, and provide false information (e.g., idle spectrum and user geographical location) to a normal node. More seriously, it may even refuse to provide services in order to achieve selfish aims or damage the core network. In the C-RAN architecture, due to its open nature, any CR nodes either illegitimate or not can access the core network functions. For example, in the scenario 3 as described above, the effects of different CR nodes are different in this heterogeneous network environment. It could be very common that when a user tries to access a malicious CR node, its spectrum sensing search cannot have any result.

Wang *et al.* [21] proposed a scheme to defend against CR node impersonation attack. They allocated a default threshold for each CR node and obtained the suspicious level of a node by analyzing node reports. When the suspicious level reaches the certain threshold, the node will be regarded as an impersonation malicious CR node and its report will be excluded. The scheme repeats this procedure for the remaining nodes until there are no malicious nodes detected. Experimental results showed that the scheme can improve the performance of collaborative processing of CR nodes, and efficiently detect malicious nodes. But this scheme has a shortcoming that it allows the suspicious level of a node change from high to normal. This means that malicious nodes may not be completely excluded.

4) PUEA (PRIMARY USER EMULATION ATTACKS)

In general, the traditional core network can authenticate a user's identity by Evolved Packet System (EPS) and Key Agreement Protocol. However, in C-RAN, there exist the primary users (PUs) and the secondary users (SUs). The network environment is more complex compared to the traditional core network. For example, malicious attackers can occupy a specific idle spectrum band by imitating the characteristics of the PUs, then interfere radio frequencies in the form of sending false signals or conducting a DoS attack. When the SUs want to achieve the spectrum resources, terminal nodes may refuse their demands by making an excuse that there are no idle resources.

Chen *et al.* [22] proposed a localization-based defense (LocDef) scheme to detect the signals that an adversary's CR emulated based on the PUs' signals. The proposed scheme can estimate a given signal's location and its signal characteristics to verify whether it is an incumbent signal. First, the LocDef scheme uses a spectrum sensor to generate snapshot of received signal strength measurements. Next, according to the peak of the snapshot, the scheme can estimate the identity and geographical location of a primary user. Simulation results showed that this scheme can effectively defeat PUEA and has strong expandability to meet the needs of various types of wireless network architecture. But this scheme has a shortcoming that it is easily to be disturbed by obstacles.

Yao *et al.* [23] proposed a physical layer authentication scheme and discussed the benefits of cryptographic signatures and wireless link signature technology to detect a primary user's signals and distinguish a legitimate user's signal from an attacker's signal. The scheme proposed that a helper node is placed physically around a primary user. The function of the helper node is to enable secondary users to verify cryptographic signature information sent by the helper node and obtain the helper node's authentic link signatures to verify whether the primary user's signal is true. In the whole process, the helper node plays as a role of a ''bridge''. The helper node can be applied to support the primary user's authentication and feedback. Besides, the authors also proposed a corresponding algorithm that can be used for authentication. Experimental results showed that this scheme is feasible, and greatly reduces the number of PUEAs. However, the weakness of this scheme is the security and trustworthiness of the

helper node are ignored. Once the helper node is attacked, the secondary users will not be able to judge the validity of the cryptographic signature information and the authentic link signatures.

Borle *et al.* [24] proposed a physical layer authentication scheme to defend PUEA. This scheme is divided into two steps: (1) when a primary user transmits a signal, it can use a one-way hash chain to generate an authentication tag. (2) the authentication tag is embedded into the signal by constellation shift. This is similar to the way of digital watermarking. Experimental results showed that this scheme is reliable and almost do not cause performance degradation. However, its shortcoming is this authentication tag is generated by a hash algorithm, which may result in a high tag bit error rate. The authors did not evaluate the computational overhead caused by the above operations.

Jin *et al.* [25] analyzed the advantages between Neyman-Pearson Composite Hypothesis Test (NPCHT) and Wald's Sequential Probability Ratio Test (WSPRT) in preventing from PUEAs. They discussed the feasibility of NPCHT and WSPRT to detect PUEAs in fading wireless channels in the presence of multiple malicious attackers. This study showed that when primary signal loss probability is above a critical threshold (e.g., 50%), NPCHT is more efficient against certain PUEAs than WSPRT, and vice versa. However, both NPCHT and WSPRT are used to detect PUEAs in a certain network radio frequency, they do not apply to all network types.

In current research, most of schemes defended PUEAs based on received signal power. Chen *et al.* [26] first designed a new PUEA, which actively obtains the key information of a primary user (e.g., the transmit power of the primary user, the channel parameter, etc.) by applying estimation techniques and learning methods. They then proposed a novel variance detection method to resist this attack. This detection method estimated the invariant of a communication channel, the variance of the received signal power of the primary user, then used this information to determine whether this signal is normal or from a malicious user. This work verified that the invariant of communication channel is important for preventing PUEAs. However, its drawback is when the variance of the signal power received by the primary user and the attacker are identical, this scheme will not work.

5) WIRELESS CHANNEL THREATS

According to whether channel state information is prefect, wireless channel security researches can be broadly divided into two categories. One is detecting security threats based on ideal channel state information (e.g., studying eavesdropping attack in no fading wireless environments, etc.) [27]–[32]. Safdar and Neill [30] described the advantages of common control channel for cognitive radio communication system security. Besides, a secure common control channel framework was proposed, which establishes a secure and effective communication session between two cognitive radio nodes after mutual authentication. Thus, nodes can reciprocally exchange encrypted information through certified cognitive radio nodes. In [31], the authors discussed multi-input multi-output wiretap channels and proposed a many-to-many transmitter and receiver pattern around the one to one transmitter and receiver pattern. For this multiple antenna channel, they drew a conclusion that this channel could load maximal security capacity. Dong *et al.* [32] used three cooperative relay protocols, that are decode-and-forward, amplify-and-forward and cooperative jamming, to improve the security of the physical wireless channels. However, there is a shortcoming that the above works are based on the ideal channel state information, which means the Channel Quality Indicator (CQI) is high, such as higher signal noise ratio and lower error code rate.

Other researchers studied wireless channel threats in the presence of Channel Estimation (CE) errors in fading wireless environments. Jia et al. [33] discussed the security and reliability of C-RAN wireless channel with CE errors. The authors analyzed the performance of C-RAN in the presence of CE errors in Rayleigh fading channels and proposed a three-phase (i.e., BBU, RRHs and users.) transmission scheme. This scheme first selects an optimal RRH in all RRHs, which is used as a bridge to exchange information between the BBU and users and prevent eavesdroppers from attacking the C-RAN channel. Simulation results showed that the more the number of RRHs is, the better the C-RAN security performance regarding CE error interference. However, a shortcoming of this scheme is that an eavesdropper can attempt to interfere the selection process or directly attack the optimal RRH.

B. SOLUTIONS TO OVERCOME THREATS RELATED RELATED TO CONTROL PLANE SECURITY

As shown in Figure 3, the control layer of C-RAN is divided into two modules: service maintenance module and resource management module. The resource management module is responsible for resource allocation and distribution with context-awareness. The service maintenance module contains the functions for service advertisement and negotiation, and protocol management (e.g., Quality-of-Service management, common control channel, spectrum resource allocation, MAC and network layer protocol management, etc.). The physical plane security is the precondition to guarantee a secure and reliable C-RAN system. However, control plane security is the core of C-RAN security. Current research in control plane security focuses on the following aspects.

1) NETWORK AND MAC LAYER PROTOCOL ATTACKS

As mentioned in Section 1, network layer protocol attacks mainly include IP spoofing, IP hijacking and Smurf attack [13]. We do not further discuss them herein. Targeting at the MAC layer attacks, previous literature often proposes novel cognitive radio MAC protocols to improve radio nodes' cognitive ability and security in a distributed cognitive radio architecture [34], [35]. In [34], Cormio and Chowdhury investigated the application scenarios, features, advantages

and disadvantages of the common cognitive radio MAC protocols, and divided them into three classes: random access protocols, time slotted protocols and hybrid ones. In [35], an opportunistic spectrum MAC protocol was proposed to protect MAC layer security. This protocol can be used for adaptively and dynamically seeking and utilizing available spectrum bands of licensing and unlicensed spectra. Different users can access and share these resources. Licensed and unlicensed users can mutually cooperate with each other. However, in order to ensure that different users can communicate with each other, this protocol depends on a trusted third authoritative party to divide available spectrum into a secure common control channel and multiple secure data channels.

2) COMMON CONTROL CHANNEL THREATS

A common control channel is different from a band channel in that the former uses a predefined frequency channel to send or receive information (e.g., collaborative processing requests, spectrum resource state and channel negotiation information, etc), which is very important for operators [16]. Fragkiadakis *et al.* [16] pointed out that a common control channel faces three threats: (1) MAC spoofing since most of current cognitive radio networks lack a model that can authenticate data integrity spread to every node; (2) extended DoS threats; (3) jamming attacks.

Bian and Park [36] analyzed two kinds of improper behaviors: DoS attacks and selfish misbehaviors. In the DoS attacks, attackers can exploit the control channel saturation problem to attack the common control channel and impair its functions (e.g., resource allocation function). Regarding the selfish misbehaviors, a selfish CR node impairs the common channel negotiation process by disrupting data packets forwarding, which causes false channel information (e.g., about channel availability). The authors also discussed an authenticating MAC layer control frames, which is similar to IEEE 802.22. However, it is infeasible for CRN, because it lacks a key management infrastructure.

3) IEEE 802.22 SPECIFIC THREATS

In 2006, IEEE 802.22 was designed as the first standard for providing confidentiality and authentication in the MAC layer. IEEE 802.22 adds some new air interfaces based on the Wireless Area Network (WAN). In [37], Bian and Park described the common threats that IEEE 802.22 faces, such as DoS attack, replay attack, special jamming attack, PUEAs, and wireless microphone beacon. Besides, they discussed a secure sub layer based on the IEEE 802.22 standard, which includes an encapsulation protocol and a privacy-preserving key management protocol. However, the secure sub layer lacks an effective solution to generate, manage and distribute related keys.

4) RADIO SPECTRUM RESOURCE THREATS

Niu *et al.* [38] first discussed the process of dynamic resource sharing in the C-RAN architecture, where end users subscribe to radio resources from their service providers. A network operator allocates radio resources to multiple service providers. They proposed a user-centric security resource allocation scheme and a corresponding algorithm based on user self-condition, such as user Quality-of-Service (QoS) requirements and data upload and download rates. However, the security problems of radio resource sharing were not discussed. C-RAN inherites RAN's advantages. It can widely sense spectrum band and modifies frequency parameters based on the change of radio frequency in real time. Rawat *et al.* [10] discussed spectrum resource threats in C-RAN. Compared to the traditional radio wireless network's one-to-one architecture, the C-RAN architecture uses distributed RRHs and centralized virtual BBUs pool management, which is more vulnerable in terms of spectrum security. For example, a malicious user or node selfishly uses unauthorized spectrum resources to induce a lot of traffic and occupy bandwidth, or it exploits this to generate a DoS attack to others.

Huang *et al.* [39] studied how to improve QoS required by users. Through maximizing the various modules of C-RAN (e.g., virtual BBUs pool, user groups, RRHs and transmit beamforming, etc.), they proposed two algorithms. One is dynamic user-centric scheduling algorithm for solving the imbalance between users' traffic and their non-uniform geographical locations. The other is transmit beamformer optimization algorithm to achieve an optimal allocation between each user's maximize QoS and each RRH's maximize capacity load. By applying both algorithms, the security performance and utility of the whole C-RAN system can be improved with sound QoS. However, this approach needs to collect user personal information, but does not consider user privacy.

5) SSDF ATTACK

Among radio spectrum resource threats, the most widely researched one is SSDF attack, in which malicious users disturb the accuracy of collaborative spectrum sensing and resource allocation by sending error observations in a CRN environment. Chen et al. [40] proposed a joint spectrum sensing and resource allocation scheme to resist the SSDF attack. In this scheme, they selected optimal users for cooperative spectrum sensing based on their trust degrees to avoid malicious attackers in resource allocation. The trust degree is evaluated based on the users' past behaviors. However, a drawback of this scheme is it has an error rate problem, which may mistakenly think a normal user as a malicious attacker. In the C-RAN architecture, to a certain extent, the centralized virtual BBUs pool defends against this attack by uniformly observing and processing the spectrum signals that remote RRHs sense. The SSDF attack seriously affects the balance of system spectrum resource allocation, especially for the virtual BBUs pool.

Cooperative spectrum sensing and resource allocation technique is a common method to prevent from attacks. There are lots of existing studies in this research direction [41]–[43]. Chen discussed several factors (e.g., signal-to-noise ratio,

signal-to-interference ratio, the number of secondary users, sample correlation, etc.) for reducing secondary user interferences in a collaborative spectrum sensing process [42]. The research results showed that the secondary user interferences are a controllable factor, which may cause varying damage on the collaborative spectrum system. However, this work cannot fundamentally defend against the SSDF attack. It only reduces the damage of collaborative spectrum as more as possible. Zheng et al. [43] discussed the effect of each cognitive node's signal-to-noise ratio on each node's sensing and reporting ability and proposed a collaborative spectrum algorithm based on the compasion of the signal-to-noise ratios of nodes. The research results showed that using the nodes with a sound signal-to-noise ratio can greatly improve the secrecy capacity of the collaborative spectrum sensing process. However, this algorithm estimates the quality of each node's signal-to-noise ratio by transmitting additional signal-to-noise ratio information to the core network. In this process, the confidentiality and integrity of the information cannot be guaranteed.

Weighted Sequential Probability Ratio Test (WSPRT) is a very effective way to prevent from the SSDF attack. Zhu and Seo discussed the shortcomings of this method. First, it needs high sampling numbers of nodes. Next, its robustness is low, and it easily deadlocks. Finally, it can only be applied into a simple and stable wireless environment. The authors proposed two solutions to overcome the above problems. One is Enhanced Weighted Sequential Probability Ratio Test (EWSPRT), which adds and updates five new functions: (1) weighting and allocating node's credit; (2) soft decision; (3) setting different nodes with different priorities; (4) periodically truncating terminals' signals, which is used for testing; (5) periodically measuring CRN's noise level. The other is Enhanced Weighted Sequential Zero/One Test (EWSZOT). Compared to EWSPRT, EWSZOT only lacks sequential test and soft decision function. This research showed that both EWSPRT and EWSZOT perform better for detecting the SSDF attack than WSPRT. However, the robustness of these two schemes cannot be ensured, which may cause additional instability and increase error rate.

Li *et al.* [45] proposed a new algorithm for detecting abnormal SSDF attacks. This algorithm estimates the abnormal realted to SSDF attacks based on a data mining technology by analyzing each user's historical informtation (e.g., user geographical locations). The advantage of this algorithm is that defenders do not need to know concrete attack types and various attacks can be flexibly detected. However, this algorithm needs to collect user personal information, which intrudes user privacy. But user privacy protection was not considered in this study.

C. SOLUTIONS TO OVERCOME THREATS RELATED TO SERVICE PLANE SECURITY

The service plane of the C-RAN architecture is a cloud platform, which directly interacts with the users or service providers. For example, with the service plane, end users only consider the QoS problem, but unaware of who is the service provider. The service provider only needs to meet users' requirements regardless of their identities. Recently, the service plane's safety has attracted increasing attention due to its importance. In C-RAN, the service layer should prevent the cloud infrastructure and the virtual BBUs pool from invasion and provide security functionalities such as identity authentication, access control, and so on. Current security research in the service layer focuses on overcoming the following attacks and threats.

1) TRANSPORT AND APPLICATION LAYER PROTOCOL ATTACKS

As discussed, the application delivery service mainly involves relevant protocols in the transport and application layers. The attacks in the transport layer or the application layer include TCP/UDP flooding attacks, sequence number prediction attacks, SQL injection, FTP bounce attacks and SMTP attacks, and so on [13]. This is similar to the traditional wireless network. Thus, we do not further discuss their detection solutions herein.

2) CLOUD COMPUTING SECURITY THREATS

One of the biggest difference between the traditional RAN and C-RAN is that cloud computing is applied in C-RAN. Thus, it is important to consider cloud computing security problems. At any time, when multiple base stations share a resource (e.g., service, hardware, data storage, etc.) over the cloud, a security risk could occur. The C-RAN architecture applies cloud computing related technology (e.g., virtualization technology, cloud storage, real-time data analysis and process, etc.), which brings new secure threats and challenges. In [46], the authors summarized the opportunities, solutions, and progress of cloud security and privacy research in recent years, such as data storage and management security, access control, trust management, and so on. They pointed out the shortcomings of the traditional cryptographic techniques and security policies, such as lengthy computations, the lack of reliable trusted third party and so on. In [47], the authors discussed the threats and security challenges of the cloud system, and defined the basic requirements for building a secure and trustworthy cloud system: (1) outsourcing security that the cloud provider shall be trustworthy by providing trust and privacy protection, and they should ensure the confidentiality and integrity of the outsourced data; (2) multi-tenancy security that the shared cloud platform should ensure the security of resource allocation in a a virtualized environment; (3) massive data and intense computation security that it is necessary to design new strategies and protocols to satify massive data and intense computation. But the authors did not discuss the trust attribute of the security cloud ecosystem.

Cloud Security Alliance (CSA) proposed nine security threats with regard to cloud computing in [48]. For C-RAN, the following security threats should be seriously considered: data loss and leakage, shared technology issues, abuse and nefarious use of cloud services, and Distributed Denial of

Service (DDoS) attacks. One example attack is a hacker can steal other virtualized machines' private key from one virtualized machine. Besides, virtualized BBUs are responsible for handling cloud services, user data, spectrum allocation and so on based on hardware resources. Once the virtualized BBUs pool is attacked, the core network performance will be greatly influeced, which may lead to serious damage and economic loss.

3) VIRTUALIZATION THREATS

One of main technology applied in cloud computing is virtualization. In the C-RAN architecture, virtualized BSs pool security is important for the overall network architecture. In [49], the authors discussed and summarized the current security solutions and challenges of virtualization technology. For current common virtualization attacks (e.g., tampering guest or host machine, virtual machine covert channel, virtual machine-based rootkits and Virtual Machine Manager (VMM) attacks), they summarized four defense methods: virtual machine-based intrusion detection, virtual machine-based kernel protection, virtual machine-based access control, and virtual machine-based trusted computing. But they did not carry out experiments to verify the validity of the defense methods.

4) PRIVACY THREATS

The privacy of users is easily attacked. In C-RAN application scenarios, it is common that idle spectrum resources are allocated to users based on the users' geographic locations. In this process, users' private information (e.g., personal affairs, personal information and personal domain, etc.) may be leaked to unauthorized parties. Thus, mobile user privacy should be considered, especially when a user is served by a cloud computing service that cannot be fully trusted. However, the literature still lacks study on this issue.

5) OTHER SECURITY THREATS

For C-RAN, some studies explored the cloud platform itself (e.g., openstack, cloudstack, etc.) to improve the security of the whole architecture. Sze *et al.* [50] aimed at the safety of the openstack cloud platform. They proposed an attack method. In this attack, the attackers hack into a computer node, get its administrator privileges of the virtual machine deployed on the node, then they can steal all tenant's token and the administrator rights of the whole platform. In order to resist this attack, they proposed a secure platform framework, which supports freely designing a security policy towards ensuring secure interaction between different components and nodes. But this framework has a limitation that it cannot prevent other types of attacks.

IV. SECURITY REQUIREMENTS OF C-RAN

In Section 1, we introduced the security requirements of the traditional wireless network, SDR network and CRNs. By discussing the C-RAN architecture and deployment scenarios in Section 2, we can see that C-RAN holds its own distinct characteristics, thus faces specific security challenges. Section 3 reviews security schemes related to C-RAN with regard to the threats and attacks in its three logic layers. In this section, we summarize the relevant security requirements that a C-RAN system should satisfy in order to resist various threats and attacks. We also use these requirements as a measure to compare existing security solutions (as shown in Table 1) and attempt to find open issues for directing future research trends. For some security requirements, we discuss them in terms of cloud computing services.

A. ACCESS CONTROL TO RESOURCES (AC)

This is the most basic security requirement that a C-RAN system should fulfill. The system should forbid unauthorized users to access resources or services anytime and anywhere. It is an effective solution to fight against PUEAs, privacy intrusions and cognitive radio node impersonation attacks.

B. ROBUSTNESS (Rb)

The C-RAN system should not only ensure the robustness of software or hardware resources, but also guarantee the robustness of the cognitive radio channel for meeting the QoS of communication services required by users. In some scenarios, the robustness of spectrum sensing should be enhanced when some sensing nodes are easily malfunctioned. Robustness is an essential requirement for overcoming the security threats caused by jamming, DoS or DDoS attacks.

C. CONFIDENTIALITY, INTEGRITY AND AVAILABILITY (C\I\A)

No matter which kind of framework, one-to-one architecture or novel C-RAN architecture, confidentiality, integrity and availability are commonly considered as three basic security properties. Integrity means that the system, the components of the system, and the data or information transmitted in the system are complete. Any data, such as user data and spectrum resources, should be confidential and available as a whole. In the C-RAN system, confidentiality requires data, no matter signal processing results, required cloud computing services, or user data, uploaded to the virtualized BBUs pool should have exclusiveness. Only authorized users can access or use these data. Integrity requires the data associated with cloud computing is complete, effective and real, which cannot be illegally manipulated, corrupted, tampered, and forged. Availability of the C-RAN requires any data or services is continuous and punctual, which is not interrupted or delayed.

D. AUTHENTICATION (Au)

Authentication is a very effective way to overcome CR node impersonation attacks and primary user impersonation attacks. By applying an authentication mechanism, the C-RAN system can verify who performs what, thus possible to detect fake CR nodes and malicious users. Moreover, it is essential to discuss a new authentication mechanism to support authentication across domains and collaboration among multiple mobile operators in order to resist potential security threats when switching or accessing CRN.

TABLE 1. Comparison of existing work based on C-RAN security requirements.

	Ref.	Attacks/Threats	C-RAN Security Requirements							
			AC	Rb	C\I\A	Au	Tr	CLRS	Pr	NR
Physical Plane	[19]	Eavesdropping attack	N	Y	Y	Y	N	Y	N	N
	[21]	CR node impersonation attack	Y	N	Y	Y	N	Y	N	Y
	[22]	Primary user emulation attack	Y	N	Y	Y	N	Y	Y	N
	[23]		Y	N	N	Y	N	Y	N	N
	[24]		Y	N	Y	Y	N	Y	N	N
	[25]		Y	N	Y	Y	N	Y	N	N
	[26]		Y	N	Y	Y	N	Y	N	N
	[30]	Wireless channels threats	N	N	Y	Y	N	Y	N	N
	[31]		N	N	Y	Y	N	Y	N	N
	[32]		N	Y	Y	Y	N	Y	N	N
	[33]		N	Y	Y	N	N	Y	N	N
Control Plane	[13]	Network layer protocols attacks	N	N	Y	Y	N	Y	N	N
	[34]	MAC layer attacks	N	Y	Y	Y	N	Y	N	N
	[35]		N	N	Y	Y	N	Y	N	N
	[36]	Common control channel threats	N	N	Y	Y	N	Y	N	N
	[37]	IEEE 802.22 threats	N	N	Y	Y	N	Y	N	N
	[38]	Radio spectrum resources threats	Y	N	Y	Y	N	Y	N	N
	[39]		Y	N	Y	Y	N	Y	Y	N
	[40]	SSDF attack	Y	N	Y	Y	N	N	Y	N
	[42]		N	N	Y	Y	Y	Y	N	N
	[43]		N	Y	N	N	N	Y	Y	N
	[44]		Y	N	Y	Y	N	Y	N	N
	[45]		N	Y	Y	N	N	Y	Y	N
Service Plane	[46] [47]	Cloud computing service threats	Y	Y	Y	Y	N	Y	Y	N
	[49]	Virtualization threats	Y	N	Y	Y	N	Y	N	N
	[50]	Other security threats	Y	N	Y	Y	N	Y	Y	N

Y: is validated; N: not considered

E. PRIVACY (Pr)

In C-RAN, the privacy of operators and end users should be considered. The privacy of end users can be divided into data privacy, identity privacy and personal information privacy. Most Communication services are to gather data and personal information around end users themselves, which may reveal information sensitive to their privacy. Adversaries would further extract more personal information about workers, such as location information, trajectory, and preference.

F. TRUSTWORTHINESS (Tr)

Compared to a traditional cellular network, the C-RAN communication environment has such characteristics as highly scalable, open and heterogeneous. Many C-RAN usage scenarios are accomplished effectively through the cooperation among mobile operators. Therefore, a trust management mechanism becomes crucially important to realize trustworthy collaboration among the operators. It may be an effective solution to overcome virtualization threats or MAC layer related threats.

G. COMPLIANCE TO LOCAL REGULATORY STANDARD (CLRS)

The C-RAN system should be designed to meet the regulatory standards of its local operator, which is a prerequisite for the establishment of a communication system. When the C-RAN architecture is deployed in a public place, it should meet all relevant security standards and requirements made by the Trans European Trunked Radio (TETRA) or the Association of Public-Safety Communications Officials (APCO).

H. NON-REPUDIATION (NR)

It is also called accountability. The C-RAN system can verify any users' actions, and this kind of action cannot be denied. It is an effective solution to overcome the threats caused by impersonation attacks and radio spectrum attacks.

V. OPEN RESEARCH ISSUES AND FURTURE RESEARCH TRENDS

A. OPEN RESEARCH ISSUES

We compare the existing work with regard to the above requirements. The result is shown in Table 1. The table is classified according to the C-RAN logic layers that face different security threats or attacks. We observe a number of open issues in the area of C-RAN security.

First, the literature lacks a comprehensive and universal C-RAN security framework that can fulfill all security requirements. Most existing work only concerned some specific security issues regarding different planes of the C-RAN logic architecture. As shown in Section 3, none of existing solutions can defend against all security threats and satisfy all security requirements.

Second, a more efficient radio resource allocation and management scheme should be studied to improve the security of the C-RAN system. Among the security requirements, secure spectrum resource management (e.g., spectrum sensing, spectrum sharing, and spectrum allocation, etc.) is considered to be the most important challenge. Original spectrum sensing techniques generally use energy detection methods, which do not resist all radio spectrum resource threats in the complex C-RAN communication environment. For example, the centralized and virtual BBUs pool can effectively resist the SSDF attack to some extent. But there exists security weakness that adversaries can attack the pool by massive attacks in a centralized way. The literature still lacks relevant researches to solve this problem.

Third, privacy preservation has been a hot topic discussed widely. But based on our survey, there is no much related work about privacy preservation in the field of C-RAN. In many C-RAN application scenarios, due to business requirements, the service providers need to obtain user personal information, such as user locations, personal identities and behaviors. So, it is necessary to propose a C-RAN privacy preservation method to avoid the leakage of user personal information. From a user point of view, he/she expects high QoS without worrying to sacrifice privacy. How to solve this problem is a still open research issue.

Forth, trust management in C-RAN is expected in practice, which, however, has not yet seriously explored. As discussed in Section 4, trust is important for virtualization security. In the current literature, there exist few schemes about trustworthy environment establishment in C-RAN. Most existing schemes requests further investigation in order to show their applicability. Niu *et al.* [38] described a trust scheme aimed at the MAC layer of C-RAN. This scheme builds a trust evaluation mechanism at each cognitive radio node, and the trust evaluation is based on node behaviors. When a node overly allocates shared spectrum resources or it hinders other nodes to communicate, its trust rating will be judged as worst. However, the availability of the model was not rigorously proven.

Fifth, achieving physical layer security is especially challenging due to the open nature of C-RAN. The phy

sical layer security has always been a hot spot of research. Although we can see all kinds of methods are used to prevent from physical layer attacks in the literature. Still, effective solutions for C-RAN physical layer security are missed.

Finally, there are other open issues which need us to discuss and research, such as, cloud computing security issues, virtualization security, and so on. Therefore, the open issues with regard to cloud computing security are well worth our research for achieving C-RAN security.

B. FURTURE RESEARCH TRENDS

Based on the open research problems discussed above, we further propose a number of promising research directions to motivate our future research.

1) INVESTIGATION OF A UNIVERSAL AND COMPREHENSIVE C-RAN SECURITY FRAMEWORK

This framework should integrate the current advance of C-RAN security technologies, which can resist various security threats and attacks in different logic layers. It should also take all security requirements into account for supporting different C-RAN deployment scenarios.

2) INVESTIGATION OF A UNIFORM, EFFICIENT AND SECURE AUTHENTICATION MECHANISM

When users access or switch a radio network node in C-RAN, this mechanism can uniformly authenticate a user and verify data security in all scenarios of C-RAN system. The traditional core network can authenticate user identities with Evolved Packet System (EPS) and Key Agreement Protocol. However, it cannot meet the practical security requirement of C-RAN, especially for roaming and inter-operator cases.

3) INVESTIGATION OF A SECURITY TECHNOLOGY THAT ALLOWS DIFFERENT OPERATORS TO SHARE THE MAXIMUM AMOUNT OF RESOURCES IN THE VIRTUALIZED BBUs POOL IN A TRUSTWORTHY WAY

Concretely, we need a trust mechanism to let an operator auditing and monitor how many resources have been consumed at another operator, especially for the ones borrowed from another operator.

4) INVESTIGATION OF NEW SECURITY SOLUTIONS THAT ENHANCE THE SECURITY OF C-RAN SYSTEM BASED ON TRUST RELATIONSHIPS AMONG USERS AND OPERATORS

For example, C-RAN system can inspect users' historical trust relationships to decide whether to issue access or provide services accordingly.

5) INVESTIGATION OF A PRIVACY PRESERVATION MECHANISM FOR C-RAN

When a service provider needs to obtain user personal information, this mechanism can prevent the leakage of user personal information.

6) INVESTIGATION OF SECURE VIRTUALIZATION MECHANISMS IN THE VIRTUALIZED BBUs POOL

How to ensure the security of the virtualized BBUs pool has not been explored seriously in the literature, which is a promising research topic.

VI. CONCLUSIONS

C-RAN has become an essential component of 5G infrastructure. In this paper, we introduced the C-RAN architecture and its deployment scenarios in order to illustrate its differences from the traditional RAN. By comparing the C-RAN with the traditional RAN, we highlighted its specific characteristics. Existing security solutions of C-RAN were reviewed based on its logic layers. By applying the security requirements of C-RAN as a measure, we compared the existing solutions in order to figure out open issues and direct future research. Through this survey, we found that C-RAN security is a new research area in its infancy. A comprehensive C-RAN security framework is still missing in the literature. Trust management and privacy preservation are highly requested in such a framework in order to support advanced networking services to gain user adoption.

REFERENCES

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2012–2017," Cisco, San Jose, CA, USA, Tech. Rep., Feb. 2013.

[2] Marketing Charts. (2015). *Mobile Network Operators Face Cost Crunch*. [Online]. Available: http://www.marketingcharts.com/wp/direct/mobile-networkoperators-face-cost-crunch-17700/

[3] Juniper Research. (2016). *Press Release: Mobile Network Operator Revenues*. [Online]. Available: http://juniperresearch.com/viewpressrelease.php?pr=245

[4] Y. Lin, L. Shao, Z. Zhu, Q. Wang, and R. K. Sabhikhi, "Wireless network cloud: Architecture and system requirements," *IBM J. Res. Develop.*, vol. 54, no. 1, pp. 4:1–4:12, Jan./Feb. 2010.

[5] I. Chih-Lin, C. Rowell, S. Han, Z. Xu, G. Li, and Z. Pan, "Toward green and soft: A 5G perspective," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 66–73, Feb. 2014.

[6] "C-RAN: The road towards green RAN, ver. 3.0," China Mobile, Hong Kong, White Paper, Dec. 2013.

[7] A. Checko *et al.*, "Cloud RAN for mobile networks—A technology overview," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 405–426, 1st Quart., 2015.

[8] P. Rost *et al.*, "Cloud technologies for flexible 5G radio access networks," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 68–76, May 2014.

[9] M. Peng, Y. Sun, X. Li, Z. Mao, and C. Wang, "Recent advances in cloud radio access networks: System architectures, key techniques, and open issues," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2282–2308, 3rd Quart., 2016.

[10] D. B. Rawat, S. Shetty, and K. Raza, "Secure radio resource management in cloud computing based cognitive radio networks," in *Proc. 41st Int. Conf. Parallel Process. Workshops (ICPPW)*, Sep. 2012. pp. 288–295.

[11] K. Guo, M. Sheng, J. Tang, T. Q. S. Quek, and Z. Qiu, "Exploiting hybrid clustering and computation provisioning for green C-RAN," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 4063–4076, Dec. 2016.

[12] D. Sabella *et al.*, "RAN as a service: Challenges of designing a flexible RAN architecture in a cloud-based heterogeneous mobile network," in *Proc. Future Netw. Mobile Summit*, Jul. 2013, pp. 1–8.

[13] 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.

[14] J. Mitola, III, "Software radios: Survey, critical evaluation and future directions," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 8, no. 4, pp. 25–36, Apr. 1993.

[15] J. Mitola, III, "Cognitive radio for flexible mobile multimedia communications," in *Proc. IEEE Int. Workshop Mobile Multimedia Conf. (MoMuC)*, Nov. 1999, pp. 3–10.

[16] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[17] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, 2nd Quart., 2012.

[18] J. Wu, Z. Zhang, Y. Hong, and Y. Wen, "Cloud radio access network (C-RAN): A primer," *IEEE Netw.*, vol. 29, no. 1, pp. 35–41, Jan. 2015.

[19] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[20] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[21] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov./Dec. 2009, pp. 1–6.

[22] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[23] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2010, pp. 286–301.

[24] K. M. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2013, pp. 2935–2939.

[25] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *ACM SIGMOBILE Comput. Commun. Rev.*, vol. 13, no. 2, pp. 74–85, Apr. 2009.

[26] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Ráez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proc. IEEE Int. Conf. Perform. Comput. Commun. (IPCCC)*, Dec. 2009, pp. 208–215.

[27] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2007, pp. 1296–1300.

[28] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[29] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[30] G. A. Safdar and M. O'Neill, "Common control channel security framework for cognitive radio networks," in *Proc. IEEE 69th Veh. Technol. Conf. (VTC Spring)*, Apr. 2009, pp. 1–5.

[31] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[32] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[33] J. You, Z. Zhong, G. Wang, and B. Ai, "Security and reliability performance analysis for cloud radio access networks with channel estimation errors," *IEEE Access*, vol. 2, pp. 1348–1358, 2014.

[34] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Netw.*, vol. 7, no. 7, pp. 1315–1329, Sep. 2009.

[35] B. Hamdaoui and K. G. Shin, "OS-MAC: An efficient MAC protocol for spectrum-agile wireless networks," *IEEE Trans. Mobile Comput.*, vol. 7, no. 8, pp. 915–930, Aug. 2008.

[36] K. Bian and J.-M. Park, "MAC-layer misbehaviors in multi-hop cognitive radio networks," in *Proc. US-Korea Conf. Sci., Technol., Entrepreneurship (UKC)*, Aug. 2006, pp. 1–8.

[37] K. Bian and J. M. J. Park, "Security vulnerabilities in IEEE 802.22," in *Proc. 4th Annu. Int. Conf. Wireless Internet*, Nov. 2008, p. 9.

[38] B. Niu, Y. Zhou, H. Shah-Mansouri, and V. W. S. Wong, "A dynamic resource sharing mechanism for cloud radio access networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8325–8338, Dec. 2016.
[39] X. Huang, G. Xue, R. Yu, and S. Leng, "Joint scheduling and beamforming coordination in cloud radio access networks with QoS guarantees," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5449–5460, Jul. 2016.
[40] H. Chen, M. Zhou, L. Xie, K. Wang, and J. Li, "Joint spectrum sensing and resource allocation scheme in cognitive radio networks with spectrum sensing data falsification attack," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9181–9191, Nov. 2016.
[41] T. C. Aysal, S. Kandeepan, and R. Piesiewicz, "Cooperative spectrum sensing with noisy hard decision transmissions," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.
[42] Y. Chen, "Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing," *Wireless Commun. Mobile Comput.*, vol. 12, no. 5, pp. 463–472, Apr. 2012.
[43] Y. Zheng, X. Xie, and L. Yang, "Cooperative spectrum sensing based on SNR comparison in fusion center for cognitive radio," in *Proc. Int. Conf. Adv. Comput. Control (ICACC)*, Jan. 2009, pp. 212–216.
[44] F. Zhu and S. W. Seo, "Enhanced robust cooperative spectrum sensing in cognitive radio," *J. Commun. Netw.*, vol. 11, no. 2, pp. 122–133, Apr. 2009.
[45] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *Proc. IEEE Symp. New Frontiers Dyn. Spectr.*, vols. 44–47. Apr. 2010, pp. 1–12.
[46] Z. Tari, "Security and privacy in cloud computing," *IEEE Cloud Comput.*, vol. 1, no. 1, pp. 54–57, May 2014.
[47] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843–859, 2nd Quart., 2012.
[48] *The Notorious Nine Cloud Computing Top Threats in 2013*, Cloud Secur. Alliance, Singapore, Jul. 2013, pp. 1–14.
[49] X. Wang, Q. Wang, X. Hu, and J. Lu, "Security technology in virtualization system: State of the art and future direction," in *Proc. IET Int. Conf. Inf. Sci. Control Eng. (ICISCE)*, Dec. 2012, pp. 1–7.
[50] W. K. Sze, A. Srivastava, and R. Sekar, "Hardening openstack cloud platforms against compute node compromises," in *Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, Jun. 2016, pp. 341–352.

FENGYU TIAN received the B.Sc. degree in telecommunications engineering from the Henan University of Science and Technology, Luo Yang, China, in 2015. He is currently pursuing the master's degree in electronics and communication engineering with Xidian University, Xi'an, China. His research interests are in security, privacy, and trust management in 5G network.

PENG ZHANG received the Ph.D. degree in computer and communication engineering from the Beijing University of Posts and Telecommunications, China. He conducted his post-doctoral research at the Helsinki University of Technology from 1999 to 2001. He is currently a Computer Scientist with an interest in trust and mobile services. He has published more than 60 papers and invented ten granted patents. He also served as an organization committee member for numerous international conferences and a reviewer for many prestigious journals.

ZHENG YAN (M'06–SM'14) received the B.Eng. degree in electrical engineering and the M.Eng. degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, and the M.Eng. degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science and the Doctor of Science in technology in electrical engineering from the Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007. She is currently a Professor with Xidian University, Xi'an, and a Visiting Professor with the Aalto University, Espoo, Finland. She authored over 160 peer-reviewed publications and solely authored two books. She is the inventor and co-inventor of over 60 patents and PCT patent applications. Her research interests are in trust, security and privacy, and data mining. She serves as an Associate Editor of *Information Sciences*, *Information Fusion*, the IEEE Internet of Things Journal, IEEE Access, *JNCA*, *Security and Communication Networks*, and *Soft Computing*. She is a leading Guest Editor of many reputable journals, including the ACM TOMM, the FGCS, the IEEE Systems Journal, and MONET. She served as a steering, organization, and program committee member for over 70 international conferences.