Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints

Danda B. Rawat and Amani Alshaikhi
Department of Electrical Engineering & Computer Science
Howard University, Washington, DC 20059, USA
E-mail: Danda.Rawat@howard.edu

***Abstract*—Wireless network virtualization is regarded as an emerging paradigm to enhance RF spectrum utilization to support exponentially increasing demand caused by emerging Internet-of-Things (IoT) applications. To create virtual wireless networks (VWNs), there are no automated secure approaches for allocating RF spectrum to meet the dynamically changing quality-of-service (QoS) requirements of the users. In wireless networks, RF spectrum is shared among many users and the given RF spectrum could be easily overcrowded because of the over commitment of limited resources by the service providers. There is a direct incentive in terms of revenue to service providers to have more number of users. In this paper, we propose to leverage a distributed Blockchain – also known as a public ledger – based scheme to create VWNs where primary wireless resource-owners (PWROs) sublease their wireless resources (e.g., slice of RF spectrum, infrastructure) to mobile virtual network operators (MVNOs) using machine-to-machine communication based on the service level agreements (SLAs) between PWROs and MVNOs. The proposed distributed Blockchain-based scheme provides security to participating PWROs and MVNOs as well as prevents PWROs from over committing their resources (that stops double spending) and helps MVNOs to meet the QoS requirements of their users. The US Federal Communications Commission (FCC) or similar regulatory bodies in other countries participate in this framework by providing the guidelines and regulations about maximum power levels, licensing and geographic coverages, etc. This essentially helps users to meet their desired QoS requirements while complying the government regulations. Performance is evaluated using numerical results.**

***Keywords*—** Blockchain for wireless virtualization, secure wireless virtualization, dynamic spectrum allocation.

I. Introduction

Over the last several decades, the world has adopted Information and Communication Technologies (ICT) at an unprecedented rate. Wireless networks have become ubiquitous and less expensive, leading to increased demand for new wireless services and applications. We have experienced tremendous growth in emerging wireless technologies geared toward different applications including Internet-of-Things (IoT) and cyber-physical systems (CPS) [1], [2]. These technological advancements promise to bring much more convenience to our daily life and tremendous economic as well as societal benefits. Recent studies have shown that the traditional way of assigning/licensing the RF spectrum to service providers for vast geographic area and long period of time is inefficient leading to most of the RF spectrum bands idle or underutilized most of the time even in big cities [3]. To enhance RF spectrum utilization, there are several approaches proposed based on spectrum sensing and opportunistic spectrum access [3]. However, there are several challenges in RF spectrum sensing and opportunistic spectrum access since licensed/primary users could use their licensed RF spectrum at any time and could be easily interfered by unlicensed opportunistic spectrum access.

In this paper, we leverage the distributed Blockchain based scheme that has been used in Bitcoin systems [4] to create Mobile Virtual Network Operators (MVNOs) using wireless network virtualization through dynamic configuration of RF spectrum based on the Service Level Agreements (SLAs) between PWROs and VNOs. Wireless network virtualization is regarded as an emerging technology to enhance RF spectrum utilization by subleasing the RF spectrum to create MVNOs to provide wireless services to end users using Radio-Resource-as-a-Service. MVNOs could easily meet QoS requirements of secondary users in a heterogeneous wireless environment. The proposed framework leverages the Blockchain based scheme for creating MVNOs securely without sharing their private information to anyone else to serve wireless users and enhance overall network capacity and coverage. Note that MVNOs will be working as an independent wireless service providers similar to T-Mobile, Verizon and AT&T without owning any network infrastructures. This concept is analogous to [5] "Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate." The underlying philosophy of this architecture is that the wireless access technology should be independent of services and frequencies and not the technology of each network, as is currently the case. In future wireless paradigm, end users may directly negotiate with MVNOs for resources needed to satisfy their security and Quality-of-Services (QoS) requirements instead of dealing with a traditional wireless service provider with statically allocated channels [3].

Main aim of the Blockchain based scheme in wireless virtualization is to sublease RF spectrum across heterogeneous wireless bands of which the organizations have no specific knowledge or control over any other service providers' data or provided services.

Note that the virtualization has been widely used in computer systems (e.g., virtual memory [6], virtual storage access network [7], wired networks [8]) and recently in cloud

978-15386-3652-7/18/$31.00 ©2018 IEEE

computing to enhance the network performance and resource utilization [9], [10]. Recently, wireless network virtualization has been proposed to enhance network coverage and capacity [11]–[14]. Other related works include wireless virtualization with cloud computing to enhance the overall performance of the wireless networks [13], [15]–[19]. A software defined centralized control plane for radio access networks (SoftRAN) [15] has been proposed as a radio access network where all base stations in a given local geographical area are combined into a virtual big-base station. For an LTE based system, a study through CloudIQ framework [16], which used cloud computing, has shown that it saved significant computing resources without degrading overall system performance. A network virtualization substrate for cellular networks has been proposed in [13] and a gateway level virtualization solution in [17] without changing MAC schedulers of base stations. Other related works include a software-defined cellular network architecture [18], Wi-Fi networks virtualization [20], wireless sensor network virtualization [21], WiMAX network virtualization [22], LTE network virtualization [19], wireless personal area network virtualization [23], cloud computing based cognitive radio networks [3], and wireless virtualization in HetNet [11]. None of these consider the wireless security while allocating frequency slices, however there are research works related to wireless communication security (e.g., [24]–[27]). All of these existing approaches consider wireless virtualization using a single base station, a single network or without considering double spending of wireless resources which is different from the proposed approach.

The overarching goal of this work is to create MVNOs on the fly without revealing private information to other competitors. The proposed approach uses the Blockchain based scheme with existing Internet for communications while creating MVNOs. Unlike the *centralized* cloud based radio access networks presented in the literature [13], [15], [16], [18], [20], the proposed approach employs Blockchain based *distributed* scheme to monitor overall status leaving user level signal processing to base stations to not require low latency back-haul links and to enhance overall network performance. Thus, the proposed approach is more than a spectrum sharing in cognitive radio networks [3] through a centralized radio access networking model.

The remainder of this paper is organized as follows. We present the brief overview of Bitcoin and Blockchain concept in Section II followed by the system model for privacy-aware information sharing in Section III. Section IV presents the Proof-of-Wireless-Resources and double spending problem and how we can avoid it in wireless virtualization for meeting QoS requirements of the MVNO users. Finally conclusions are presented in Section VI.

II. Brief Overview of Bitcoin and Blockchain

Bitcoin (developed by a programmer known as Satoshi Nakamoto – a name believed to be an alias) is based on cryptographic techniques that allows the recipient to receive money securely/genuinely without requiring a trusted third party, such as a bank or a company like PayPal [4], [28]. The Bitcoin network relies on a Blockchain – a distributed transaction public ledger – where a new block is generated by executing a consensus algorithm such as Proof-of-Work [4]. A Bitcoin client software helps users to connect to a decentralized network of other Bitcoin users through the Internet. Client software generates a pair of unique keys (private and public keys) which are used to exchange Bitcoins with other Bitcoin users. Private key is kept hidden on the computer and public key with a dubbed Bitcoin address is distributed to other Bitcoin users to exchange coins. It has been noted in [4], [28] that it is practically impossible to get the someone's private key from his/her public key which prevents users from impersonating attacks. To do a transaction, the Bitcoin client software performs a mathematical operation to combine the recipient's public key and sender's (i.e., your own) private key along with the amount of Bitcoins that you want to pay/send. Then the transaction is sent out to distributed Bitcoin network so as to verify by Bitcoin software clients/users other than the sender and recipient. All Bitcoin users that are on-line – other than sender and recipient – check 1) whether a true owner sent the money by exploiting mathematical relationship between its public and private keys; 2) the public transaction log stored on the computer of every Bitcoin user to make sure that sender has the Bitcoins to spend. Some of the clients – also known as 'miners' – also try to transfer their Bitcoins to their respective recipients through a public transaction log, by competing to solve a cryptographic puzzle [4]. It is reported in [4], [28] that the Bitcoin system is unbreakable since the mathematics involved in the Bitcoin ensures that the transactions can be easily verified but it is practically impossible to generate malicious transactions to spend somebody else's Bitcoins. Channels are treated as Bitcoins in the proposed framework to have verifiable, secure transactions.

III. System Model and Problem Statement

In Blockchain based wireless virtualization architecture, wireless resources such as RF channels are sliced into multiple (time/frequency) slices for MVNOs as shown in Fig. 1. Three entities in wireless virtualization architecture are: *wireless service providers* who participate in sharing or subleasing their wireless resources to MVNOs to create VWNs; *services*, that process data about sharing wireless resources; and *block managers, or BMs* that are trusted devices that maintain the Blockchain and distributed cryptographic keys and communicate with other BMs on behalf of the service providers as shown in Fig. 1. It is important to note that the PWROs participating in wireless virtualization use changeable public keys otherwise remain anonymous by hiding identity or private information of the participating PWROs. The Blockchain managers store service profiles on the Blockchain and verify PWROs' identities using public keys. Each transaction in Blockchain for wireless virtualization consists of bandwidth allocation information, maximum power allowed in the channel, data rate etc. which are used by the MVNOs while serving their users through VWNs. When spectrum is leased from a

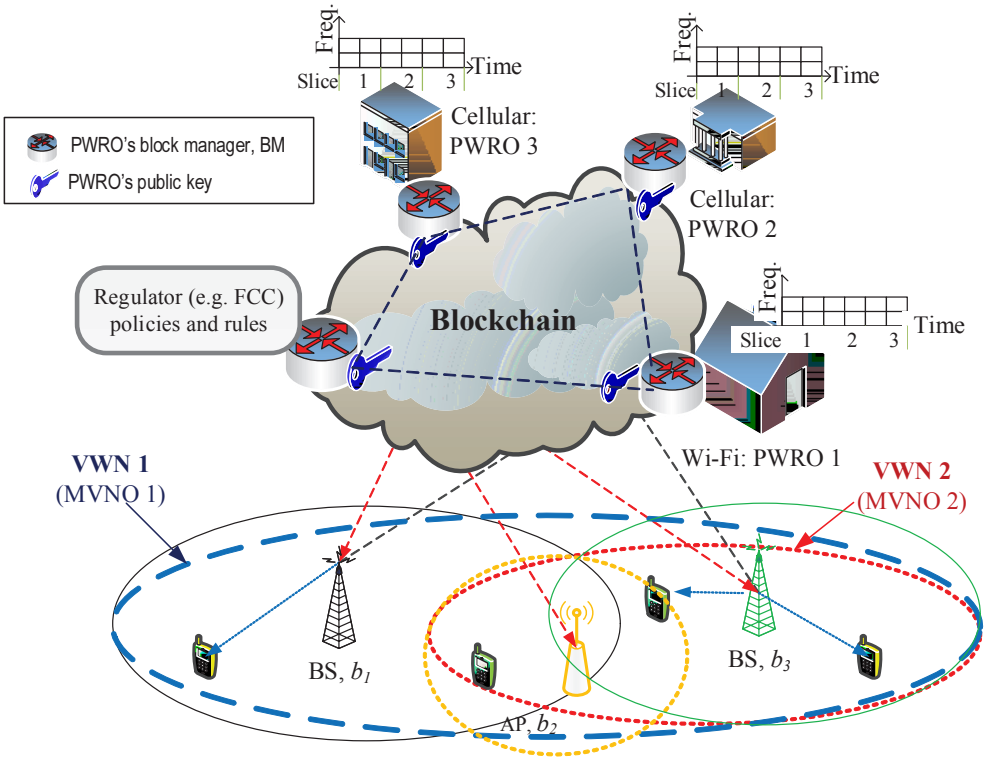

Fig. 1. A typical Blockchain based wireless virtualization framework to create virtual wireless networks for mobile virtual network operators, where Federal Communications Commission (FCC), wireless service providers such as T-Mobile, AT&T, Verizon, Sprint and Wi-Fi Hot-spots participate and communicate using the public Internet.

PWRO to a MVNO, the source is the PWRO whose resources are verified as in Blockchain in peer-to-peer communication as in Bitcoin systems [4] and the recipient is the MVNO who is tenant of the leased wireless resources. Similarly, when a given MVNO wants to release the leased wireless resources to its PWRO, source is the MVNO and the recipient is the PWRO where other participants sign digitally to prevent from double spending.[1] The demanded service area is covered by a set of wireless infrastructures or base-stations, i.e., $\mathcal{B} = 1, \ldots, M$ with aggregated bandwidth of W Hz which is sliced into a set of sub-carriers, $\mathcal{Q} = 1, \ldots, Q$ that are allocated to MVNOs. The bandwidth of each sub-carrier, i.e., $W_c = \frac{W}{Q}$. Note that the overall network monitoring is carried out by the Blockchain based scheme while leaving the signal processing at base stations of MVNOs. This architecture brings the wireless services closer to the end users using Radio-Resources-as-a-Service. In the proposed architecture, MVNOs are wireless service providers to their users without being an owner of any wireless infrastructures. In this case, MVNOs operate based on SLAs between MVNOs and the owners for the wireless infrastructures. The SLA helps both MVNOs and the owners for the wireless infrastructures to adjust their resources on the fly in Blockchain based wireless virtualization framework. The proposed approach combines the diverse set of wireless resources by exchanging their resources to make them available to MVNOs through VWNs. Note that, for a given location, there could be many base stations (e.g., T-Mobile, A&T, Verizon cell towers, or Wi-Fi access points) covering the same area. In this case, MVNOs and PWROs select the base station that meets demanded data rate requirements of the users and SLAs between MVNOs and PWROs. After creating MVNOs, end-users communicate through VWNs of MVNOs like in traditional wireless networks. The goal of each end-user is to communicate with its intended received with data rate greater than or equal to its required minimum data rate whereas the goal of the MVNOs is to maximize their revenues while providing competitive price and good coverage.

A. Blockchain Transaction Process in Wireless Virtualization

A typical Blockchain in wireless virtualization framework is shown in Fig. 2 which composed of blocks of a set of transactions. Each transaction in Blockchain for wireless virtualization consists of bandwidth allocation information, maximum power allowed in the channel, data rate etc. which are used by the MVNOs while serving their users through VWNs.

Blocks are practically impossible to manipulate without being caught since they are chained together using a hash, or a numeric digest of its content as shown in Fig. 2, that can be used to verify the integrity of the transactions. Furthermore,

[1]Double-spending is an error in a digital coin systems where a given digital coin is spent more than once as a digital coin can be falsified or duplicated [4], [29], [30]. In wireless virtualization process, double spending is the allocation of same wireless resources to multiple MVNOs with a hope of all MVNOs would not use their leased spectrum at the same time and with an aim of increasing PWROs' revenues. In case of double spending in wireless virtualization, end-users would not be able to meet their QoS requirements because of limited/same resources are used by more than a single MVNO.

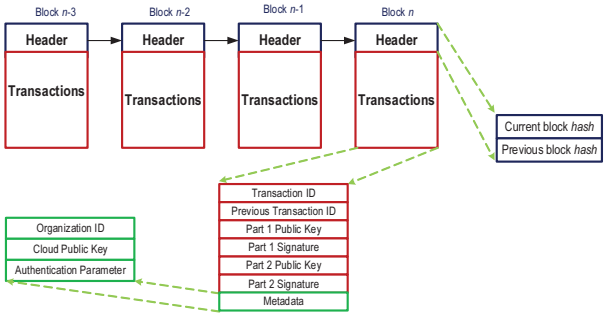

Fig. 2. A typical structure of the Blockchain in wireless virtualization framework where transactions in Blockchain reference actual resources via Uniform Resource Locators (URLs) to allow participating service providers to retain operational control of their private data and to support for provenance and audit trails for Blockchain ledger entries.

the hash of a block (say a block n) depends on its predecessor (say block $n-1$) as shown in Fig. 2 that makes the Blockchain immutable by malicious actions as a change in one block would require changes in the following blocks.

Organizations, in the wireless virtualization framework, participate collaboratively to create a Blockchain by verifying and storing new transactions into it. The digital signature and existence of the previous transactions in the same ledger are used to verify the legitimacy of the transactions in Blockchain. A new block is generated by executing a consensus algorithm such as Proof-of-Wireless-Resources (see Section IV-A) similar to the Proof-of-Work in [4]. The BM or GBM[2] then creates a new block and forwards it to other BMs for block verification which allows all BMs to contribute at least a transaction to digitally sign the block to endorse its correctness. Then, the block is returned to the original BM which then adds the block to its local Blockchain. Finally, a new Blockchain is distributed to all nodes in the system.

Organizations (with the help of BMs) are known by a changeable public keys in Blockchain which helps provide privacy. As mentioned earlier, the Blockchain does not rely on any centralized trusted authority but relies on distributed devices participating in the wireless virtualization. The proposed Blockchain network comprises different PWROs, FCC, cloud storage, devices such as laptops, cell phones, tablets, cyber-physical system devices and IoT devices.

IV. Proof-of-Wireless-Resources and Preventing Double Spending to Meet QoS Requirements

A. Proof-of-Wireless-Resources (PoWR)

In wireless virtualization, wireless resources such as idle channels that can be subleased to MVNOs should be checked whether they are literally available to MVNOs or not based on their SLAs. If a given PWRO says, there are channels that can be subleased to MVNOs but it does not provide those channels to MVNOs based on SLAs on the fly, then users of the given MVNOs would not be able to get desired services from MVNOs throug VWNs. Thus, the wireless virtualization process relies on the Proof-of-Wireless-Resources (PoWR) which is analogous to Proof-of-Works in Bitcoin systems [4]). For PoWR, FCC and all other participating PWROs sign each transaction by communicating it over the Internet. Note that the Blockchain based systems are unbreakable since each transactions can be easily verified with the help of digital signatures and it is practically impossible to generate malicious transactions to spend somebody else's resources such as Bitcoins in Bitcoin systems [4], [28]. The PoWR allows MVNOs to ensure that they have committed resources in their SLAs to sevre their users through VWNs. Next, PWROs could over commit their same resources more than once at the same time for a given location. This is also known as double spending attack which is discussed in the section IV-B.

[2]In case of partnering organizations, they can nominate a group leader (based on their business MoU) as a block manager and named as a group block manager (GBM). The gateway of each organization (e.g., org. 2 and org. 3) will be connected to a GBM and GBM maintains the public key for the group.

B. Prevent Double Spending Attack

Double-spending attack is the result of successful sharing of the same wireless resources by PWROs to more than one MVNOs. Proposed PoWR in Blockchain protects the system against double spending of same wireless recourses by verifying each transaction to ensure that the wireless resources planned to be shared with a given MVNO had not already been allocated to another MVNO at the same time and location. Double spending can be prevented by having a central authoritative entity such as a centralized cloud computing radio access network controller that follows sharing rules for authorizing each transaction. This centralized approach could easily suffer from a bottleneck problem when wide-band heterogeneous wireless network regime is considered. We leverage the Blockchain concept used in Bitcoin, which is a decentralized public ledger based system, for a consensus among participating BMs that replaces the central authority. To accomplish this without a trusted centralized party, transactions must be publicly announced as a public ledger without reveling their private information as in Bitcoin system in [4], and participants should agree on a single history transactions. When MVNOs do not need the wireless resources for their users and VWNs, they transfer the resources to their PWROs based up on their SLAs. This process is also verified by all other precipitants as shown in Fig. 1.

V. Performance Evaluation

To evaluate the performance of the MVNOs created by using wireless virtualization with and without the Blockchain based scheme, we consider three identical scenarios with two MVNOs in each scenario. Scenario 1 had both MVNOs with Blockchain where no double-spending was permitted. Scenario 2 had 2 MVNOs with Blockchain in one MVNO and no Blockchain approach in another MVNO (which had no checking mechanism for double spending). Scenario 3 had 2 MVNOs without Blockchain that had no checking of double spending of wireless resources. Fig. 3 shows that the normalized throughput of a MVNO is higher when there

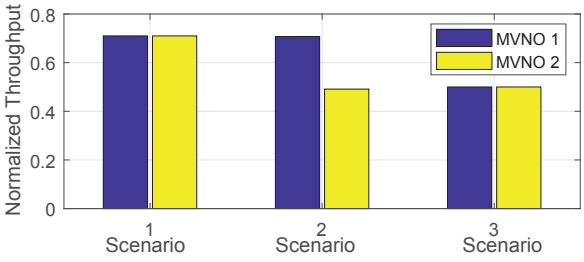

Fig. 3. Normalized throughput for 2 MVNOs with and without Blockchain implementation in 3 different scenarios.

was Blockchain scheme implemented (that checks the double-spending attack) than that of without Blockchain (that does not check the double-spending attack). For considered scenarios in Fig. 3, the users that have 0.50 or higher normalized-throughput/QoS requirements would not be able to meet their QoS requirements by MVNO 2 in scenarios 2 and 3 because of double spending (same wireless recourses shared twice to more than one MVNOs) by PWROs. Note that the security in the proposed system is achieved by using verifiable ledger to protect from malicious PWROs from double spending attacks.

VI. Conclusion

In this paper, we leveraged the distributed Blockchain based scheme to create VWNs where PWROs sublease their resources (e.g., slice of RF spectrum) to MVNOs using machine-to-machine communications based on their SLAs. The Blockchain-based scheme in wireless virtualization provides security to participating PWROs and MVNOs, and prevents PWROs from over committing their resources by stopping double spending attacks that eventually helps MVNOs to meet the QoS requirements of their users.

Out future work includes formal mathematical analysis and extensive evaluation of the framework.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation (NSF) under grants CNS-1658972 and CNS-1650831. However, any opinion, finding, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of NSF.

References

[1] S. Jeschke, C. Brecher, H. Song, and D. B. Rawat, *Industrial Internet of Things: Cybermanufacturing Systems*. Springer, USA, 2017.

[2] D. B. Rawat, *Cyber Physical Systems: From Theory to Practice*. CRC Press, 2015.

[3] D. B. Rawat, M. Song, and S. Shetty, *Dynamic Spectrum Access for Wireless Networks*. Springer Verlag, 2015.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, 2008," *URL (accessed on Aug. 2017): http://www.bitcoin.org/bitcoin.pdf*, 2008.

[5] https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface.

[6] C. Morin and I. Puaut, "A survey of recoverable distributed shared virtual memory systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 8, no. 9, pp. 959–969, 1997.

[7] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[8] N. M. K. Chowdhury and R. Boutaba, "A survey of network virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, 2010.

[9] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek, "The click modular router," *ACM Transactions on Computer Systems (TOCS)*, vol. 18, no. 3, pp. 263–297, 2000.

[10] Cisco Public Information, Cisco VN-Link: Virtualization-Aware Networking, A Technical Primer, White Paper 2015. http://www.cisco.com/c/en/us/solutions/collateral/switches/nexus-1000v-switch-vmware-vsphere/white_paper_c11-525307.html.

[11] D. B. Rawat, T. White, M. Song, and C. Zhang, "Leveraging Wireless Virtualization for Network Capacity Optimization in HetNets," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, 2017, pp. 1–6.

[12] Y. Zaki, L. Zhao, C. Goerg, and A. Timm-Giel, "Lte wireless virtualization and spectrum management," in *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, 2010, pp. 1–6.

[13] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "NVS: a substrate for virtualizing wireless resources in cellular networks," *Networking, IEEE/ACM Transactions on*, vol. 20, no. 5, pp. 1333–1346, 2012.

[14] L. DaSilva, J. Kibilda, P. DiFrancesco, T. K. Forde, L. E. Doyle *et al.*, "Customized services over virtual wireless networks: The path towards networks without borders," in *2013 Future Network and Mobile Summit (FutureNetworkSummit)*, Lisbon, Portugal, 3-5 July 2013, pp. 1–10.

[15] A. Gudipati, D. Perry, L. E. Li, and S. Katti, "SoftRAN: Software defined radio access network," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. ACM, 2013, pp. 25–30.

[16] S. Bhaumik, S. P. Chandrabose, M. K. Jataprolu, G. Kumar, A. Muralidhar, P. Polakos, V. Srinivasan, and T. Woo, "Cloudiq: a framework for processing base stations in a data center," in *Proceedings of the 18th annual international conference on Mobile computing and networking*, 2012, pp. 125–136.

[17] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "CellSlice: Cellular wireless resource slicing for active RAN sharing," in *Communication Systems and Networks (COMSNETS), 2013 Fifth International Conference on*, 2013, pp. 1–10.

[18] L. E. Li, Z. M. Mao, and J. Rexford, "CellSDN: Software-defined cellular networks," *Techinical Report, Princeton University*, 2012.

[19] Y. Zaki, L. Zhao, C. Goerg, and A. Timm-Giel, "LTE mobile network virtualization," *Mobile Networks and Applications*, vol. 16, no. 4, pp. 424–432, 2011.

[20] L. Xia, S. Kumar, X. Yang, P. Gopalakrishnan, Y. Liu, S. Schoenberg, and X. Guo, "Virtual WiFi: bring virtualization from wired to wireless," in *ACM SIGPLAN Notices*, vol. 46, no. 7, 2011, pp. 181–192.

[21] M. M. Islam, M. M. Hassan, G.-W. Lee, and E.-N. Huh, "A survey on virtualization of wireless sensor networks," *Sensors*, vol. 12, no. 2, pp. 2175–2207, 2012.

[22] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "NVS: a virtualization substrate for WiMAX networks," in *in the 16th Int'l Conf. on Mobile Computing & Networking*, 2010, pp. 233–244.

[23] H. Wen, P. Tiwary, and T. Le-Ngoc, *Wireless Virtualization*. Springer, 2013.

[24] Y. Xiao, H.-H. Chen, X. Du, and M. Guizani, "Stream-based cipher feedback mode in wireless error channel," *IEEE Tran. on Wireless Comm.*, vol. 8, no. 2, pp. 622–626, 2009.

[25] X. Yao, X. Han, X. Du, and X. Zhou, "A lightweight multicast authentication mechanism for small scale IoT applications," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693–3701, 2013.

[26] X. Du and H.-H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, 2008.

[27] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[28] Tom Simonite, "What Bitcoin Is, and Why It Matters," MIT Technology Review, May 25, 2011. URL (Accesed on June 1, 2017): https://goo.gl/Btqrfc.

[29] I. V. Krsul, J. C. Mudge, and A. J. Demers, "Method of electronic payments that prevents double-spending," Nov. 17 1998, uS Patent 5,839,119.

[30] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 906–917.