Multi-operator Network Sharing for Massive IoT

Yong Xiao, Marwan Krunz, and Tao Shu

Abstract

A recent study predicts that by 2020, up to 50 billion Internet-of-Things (IoT) devices will be connected to the Internet, straining the capacity of the wireless infrastructure, which has already been overloaded with data-hungry mobile applications. How to accommodate the demand for both massive-scale IoT devices and high-speed cellular services in the physically limited spectrum without significantly increasing the operational and infrastructure costs is one of the main challenges for operators. In this article, we introduce a new multi-operator network sharing framework that supports the coexistence of IoT and high-speed cellular services. Our framework is based on the radio access network (RAN) sharing architecture recently introduced by 3GPP as a promising solution for operators to improve their resource utilization and reduce system roll-out cost. We evaluate the performance of our proposed framework using real base station location data in the city of Dublin collected from two major operators in Ireland. Numerical results show that our proposed framework can almost double the total number of supported IoT devices and simultaneously coexist with other cellular services.

I. Introduction

The Internet-of-Things (IoT) is a holistic framework for supporting the communication of intelligent devices and services that are employed in diverse verticals, including e-health, environment control, smart city, and autonomous vehicles. It is considered as the key technology to fulfill 5G's vision of ubiquitous connectivity. The fast proliferation of IoT applications has

Y. Xiao is with the School of Electronic Information and Communications at the Huazhong University of Science and Technology, Wuhan, China 430074 (e-mail: yongxiao@hust.edu.cn).

M. Krunz is with the Department of Electrical and Computer Engineering, the University of Arizona, Tucson, AZ 85721 USA, and also with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: krunz@email.arizona.edu).

T. Shu is with the Department of Computer Science and Software Engineering at the Auburn University, Auburn, AL 36849 (e-mail: tshu@auburn.edu).

been driven by continuous decrease in cost, size, and power consumption of IoT devices and rapidly growing demand for intelligent services. According to Cisco, by 2020, up to 50 billion IoT devices will be connected to the Internet via cellular networks, generating over $1.9 trillion in revenue across a wide variety of industries [1].

Because no frequency bands are exclusively allocated to IoT services, IoT devices must share spectrum with other technologies. 3GPP recently introduces multiple solutions that enable the coexistence of IoT services and regular cellular services. The main challenge for operators is therefore to accommodate the traffic generated by both IoT and fast-growing high-speed cellular services (e.g., enhanced Mobile Broadband (eMBB)) without significantly increasing their operational and infrastructure costs. Recent 3GPP LTE standards promote the idea of *network sharing*, i.e., allowing operators to share radio access network (RAN) resources, including network infrastructure and spectrum, to improve the utilization of individual operator's resources and reduce the system roll-out cost/delay. Recent studies reported that network sharing has the potential to save more than 50% of the infrastructure cost in 5G deployment for a typical European cellular operator [2].

Despite its great potential, it is known that network sharing between multiple operators could significantly increase the implementation complexity of wireless systems. In addition, 3GPP's network sharing architecture is mainly introduced to support high-speed data service in which a single operator can temporally access a much wider frequency band to support the high-throughput service requested by a single user equipment (UE). However, IoT devices typically generate low-throughput traffic and their data transmission can be intermittent. How to quickly establish a large number of data connections and allocate the required frequency bands for a massive-scale IoT devices that can be associated with multiple operators is still an open problem.

In this article, we propose a novel network sharing framework that allows coexistence of IoT and high-speed data services across multiple operators. Our proposed framework is based on the active RAN sharing architecture recently introduced in 3GPP Releases 13-15. We present multiple new design solutions that aim at reducing the implementation complexity of network sharing for IoT applications. Furthermore, we simulate a multi-operator cellular system using actual BS location information obtained from two major telecommunication operators in Ireland. Such trace-driven simulations are used to evaluate the performance of our proposed framework under various practical scenarios. The rest of this article is organized as follows. We provide an overview of recent 3GPP solutions on IoT and discuss the challenges for a massive deployment

TABLE I

IoT SOLUTIONS IN 3GPP RELEASE 13 [3]

	EC-GSM-IoT	NB-IoT	eMTC
Frequency	850-900 MHz and 1800-1900 MHz GSM bands	2G/3G/4G spectrum between 450 MHz and 3.5 GHz; Sub-2 GHz bands are preferred for applications requiring good coverage	Legacy LTE between 450 MHz and 3.5 GHz
Bandwidth	200 kHz	180 kHz	1.08 MHz
Maximum Transmit Power	33 dBm, 23 dBm	23 dBm, 20 dBm	23 dBm, 20 dBm

of IoT services in cellular networks. We then introduce our proposed framework and discuss various design issues. Finally, we present numerical results to demonstrate the potential of our proposed framework.

II. Current Solutions and Challenges for IoT

A. IoT Solutions of 3GPP

Three solutions have been standardized by 3GPP for cellular IoT deployment: extended coverage GSM IoT (EC-GSM-IoT), narrowband IoT (NB-IoT), and enhanced machine-type communication (eMTC) [4], [5]. EC-GSM-IoT operates on legacy GSM bands and can support up to 240 kbps peak data rate over a 200 kHz channel. It applies advanced repetition and signal combining techniques to further extend the service coverage. NB-IoT is a new radio added to LTE. It focuses on low-end IoT applications. For example, T-mobile recently announced plans to provide NB-IoT service at a rate of $ 6 per year per device with up to 12 MB of data. This service can achieve up to 250 kbps peak data rate over 180 kHz bandwidth on a GSM or LTE band, or on an LTE guard-band. eMTC is derived from LTE but with new power saving functions that can support up to 10 years of operation with a 5 Watt-hour battery. Due to its low transmit power, eMTC can coexist with high-speed LTE services. eMTC devices can support up to 1 Mbps data rate in both uplink and downlink over 1.08 MHz bandwidth. We summarize the main specifications of 3GPP IoT solutions in Table I.

To further improve the battery life of IoT devices, all IoT solutions adopt discontinuous reception (DRX) cycle, similar to LTE. In this setting, each device will periodically check the system information broadcast on the control channel according to the DRX cycle and only request a channel connection if it identifies a service request (e.g., receiving calls, messages, and connection requests). A typical LTE device can have up to 2.56 seconds of DRX cycle. 3GPP further extended the concept of DRX by introducing new extended discontinuous reception (eDRX) power saving modes for all three IoT solutions. In particular, two modes have been introduced for NB-IoT and eMTC: connected mode (C-eDRX) and idle mode (I-eDRX). C-eDRX supports 5.12 seconds and 10.24 seconds of DRX cycles for eMTC and NB-IoT, respectively. In I-eDRX, the DRX cycle can be further extended to 44 minutes and 3 hours for eMTC and NB-IoT, respectively. EC-GSM-IoT supports up to 52 minutes of DRX cycles.

B. Challenges for Massive IoT Deployment

In spite of the strong push from industry and standardization organizations, many challenges remain to be addressed for massive deployment of IoT.

1) Coexistence of Massive IoT and High-speed Cellular Services: Motivated by the fact that IoT devices require low transmit powers and narrow bandwidth, most existing works focus on developing optimal power control, channel allocation, and scheduling algorithms for IoT services to adapt to the dynamics of the coexisting cellular traffic. However, IoT devices are usually low-cost with limited processing capacity to calculate and instantaneously adjust their transmit powers and channel usage. Some recent works suggest deploying edge/nano-computing servers at the edge of the network, e.g., BSs, to collect the necessary information and make decisions for near by IoT devices [6]. These solutions make optimal resource allocation and instantaneous interference control possible for IoT devices. However, deploying new infrastructure such as edge servers, enhanced/upgraded base stations, and new interfaces to support coordination and information exchange between BSs and edge servers requires extra investment from operators. For example, recent announcements from AT&T and Verizon revealed that billions of dollars are required to upgrade their infrastructure for supporting IoT-based 5G networks. Such investment will eventually be reflected in higher charges to end users.

2) Excessive Overhead and Inefficiency of Random Access Channel Procedure: Another issue is that the random access channel (RACH) procedure currently used in LTE and GSM incurs high energy consumption and a significant amount of signaling overhead to establish connections between devices and network infrastructure. Directly extending this procedure to IoT systems is uneconomic and unrealistic. In particular, it has been reported that in a typical cellular system, transmitting 100 bytes of payload from a mobile device requires up to 59 bytes and 136 bytes of overhead on the uplink and downlink, respectively [7]. In addition, the RACH procedure was originally designed to support only a limited number of mobile devices (around 100 mobile devices per cell). For example, if a device tries to establish a connection, it must randomly choose a preamble signal sent to the BS over the physical random access channel (PRACH). In existing LTE systems, each device can only choose one preamble from a set of 64 pre-defined preamble signals. If two or more devices choose the same preamble, a conflict will happen which will result in retransmission and further delay in resource allocation.

3) Diverse QoS Requirements: Another challenge related to the diverse requirements of IoT services is that existing IoT solutions treat data generated by different IoT services the same. In particular, for some massive-type IoT applications, such as long-term environmental monitoring and parcel tracking, a certain amount of data loss and data delivery latency can be tolerated. However, in mission-critical IoT applications, such as fire/gas alarm, health monitoring, and traffic safety, data delivery must be instant and highly reliable. How to differentiate the service requirements for different applications and distribute appropriate resources to meet the needs of various IoT services is still an open problem.

4) Mobility Management and Traffic Dynamic Control: Due to the mobility of UEs and IoT devices, as well as the time-varying traffic of different services, the resource demand and LTE/IoT coexisting topologies can be dynamic. Most existing solutions are focusing on optimizing the long-term performance based on a priori knowledge and/or prediction results. For example, an IoT device can predict the future change of its movement, change of data traffic as well as activities of other UEs in its proximity, so it can prepare for the future (e.g., scheduling/reserving a certain amount of bandwidth for future use if it predicts that these resources will soon be limited). However, always relying on each IoT device to predict its resource needs is impractical due to the limited processing capability. Currently, there is no simple and economic solution that allows each IoT device to instantaneously adapt to the environmental dynamics without sacrificing the device's cost and battery life.

III. Multi-operator Network Sharing for Massive IoT

A. Inter-operator Network Sharing Architecture

The concept of network sharing has been first introduced in 3GPP Release 10 to allow multiple operators to share their physical networks. Early development of network sharing mainly focused on infrastructure sharing, also referred to as *passive RAN sharing* [8], [9]. In this scenario, operators share site locations and supporting infrastructure such as power supply, shelters, and antenna masts. However, each operator still needs to install its own antennas and backhaul equipment for individual usage. 3GPP Release 14 introduces the *active RAN sharing* architecture. Operators can now share their spectrum resources as well as core network equipments (i.e., eNBs) based on a network sharing agreement, which can include mutual agreement on legal, finance, and joint operations. To ensure efficient and secure resource management, a master operator (MOP) is designated as the only entity that manages resource shared among the participating operators (POPs). The MOP can be a third-party manager designated by POPs. It can also be one of the POPs. In 3GPP's architecture, the MOP may charge POPs based on the requested data volume and the required QoS.

According to the entities shared by POPs, active RAN sharing architectures can be further divided into two categories:

- *RAN-only sharing*, also called multi-operator core network (MOCN). In here, a set of BSs sharing the same spectrum can be accessed by all POPs. Each POP, however, maintains its own core network elements, including the mobility management entity (MME) and serving and packet gateways (S/P-GW). Each POP can connect its core network elements to the shared RAN via the S1 interface.
- *Gateway core network* (GWCN). In addition to sharing the same set of BSs. In GWCN, POPs can also share a common MME to further reduce costs.

To simplify the exposition, in the rest of this section, we assume that each POP corresponds to a cellular operator that divides its network infrastructure and licensed spectrum into two parts: an *exclusive use* part that is reserved and exclusively used by itself, and a *shared* part that can be accessed by other operators. The shared parts of the infrastructure and spectrum of all the POPs are combined and managed by the MOP. Each IoT device or UE has already been assigned to a POP. The BSs of each POP need to calculate the channel reuse structure between the low-power NB-IoT devices and regular UEs so the cross-interference between both channel-sharing devices is below a tolerable threshold. In LTE, for example, the interference threshold for each UE is -72 dBm. If the exclusive use part of the spectrum is insufficient to support the traffic generated by the associated IoT and cellular services, the POP can temporally request a portion of shared spectrum from the MOP. If the spectrum requests of a POP are approved, the POP can assign any of its traffic (IoT or cellular) to the shared spectrum without consulting the MOP. If the spectrum requested by all POPs exceeds the total amount of shared spectrum, MOP will partition

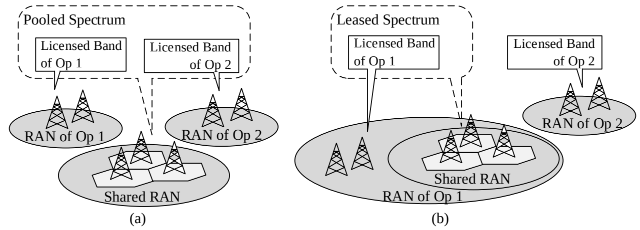

Fig. 1. Inter-operator network sharing: (a) spectrum pool, and (b) spectrum leasing.

the shared spectrum and assign the divided spectrum to each POP according to a predetermined mutual agreement. Both active RAN sharing architectures can be extended to our framework to support spectrum sharing between IoT and high-speed cellular services. In particular, RAN-only sharing allows each POP to adjust the traffic traversed through the shared network or its exclusive network resources according to the mobility of IoT devices (e.g., IoT services in wearable devices and vehicle networks). In this case, each POP needs to keep track of traffic dynamics and the required QoS requirements for both IoT services and its regular cellular services. The POP can then adjust the traffic sent through the shared infrastructure and its own exclusive infrastructure accordingly. GWCN further reduces the cost for each POP by sharing a common MME among all POPs. It, however, cannot provide the same flexibility as RAN-only sharing for each POP because in this case mobility of devices is restricted to inter-RAN scenarios. In other words, each POP cannot adjust the traffic sent through the shared infrastructure and its own exclusive infrastructure by itself. In this case, POPs will need to predict the traffic from IoT services and cellular services, and reserve resources for each service accordingly.

In active RAN sharing, different POPs can access/rent different part of the shared infrastructure (e.g., a set of BSs that can be accessed by all POPs). However, the BSs in the shared RAN must operate on the same spectrum. Based on the spectrum used by the shared RAN, the multi-operator network sharing architecture can be further divided into the following two sub-categories, as illustrated in Figure 1:

1) Spectrum Pooling: POPs can merge their licensed (GSM and/or LTE) bands to form a common pool to be used by the shared RAN as shown in Figure 1(a) [10]. Allowing the shared BSs to operate on the pooled spectrum can significantly reduce the complexity of spectrum management, i.e., it is uneconomic and too complex to allow each BS to switch its operational bands when it has been rented by different POPs. Spectrum pooling has been considered as one of the main use cases for the network sharing architecture in 3GPP's technical specification. In this architecture, each POP will need to coordinate with MOP's network management controller for channel assignment to avoid inter-cell interference between the BSs in the exclusive-use RAN and those in the shared RAN.

2) Spectrum Leasing: 3GPP's architecture allows one of the POPs to serve as the MOP to manage and control the resource allocation of the shared RAN as shown in Figure 1(b). In this case, it is possible for one POP to lease a part of its BSs and the licensed band to be shared with other POPs. In spectrum leasing, to maintain the required QoS for the MOP, IoT and UEs associated with MOP can have the priority to access the shared spectrum. The POPs can only offload a limited traffic to the shared RAN if the resulting impact (e.g., throughput degradation) to the existing traffic of the MOP is below a tolerable level. If two or more POPs can lease their network infrastructure and licensed bands to each other at different time periods according to their traffic demands and resource availabilities, the spectrum leasing becomes equivalent to the *mutual renting* introduced in METIS' future spectrum system concept [11]–[13]

B. Design Issues

There are several important issues when deploying IoT services using our proposed multi-operator network sharing framework:

1) Fair Revenue Division Among Operators for Spectrum Pooling: In 3GPP's network sharing architecture, MOP can charge services (e.g., IoT services) using the shared resource according to the data usage and required QoS profiles. One intrinsic problem is then how to divide the revenue obtained by MOP from serving IoT among all the resource-sharing POPs. This revenue division determines each POP's perception on the fairness of the sharing, and will in turn affect its willingness to share the licensed band with others. In other words, the revenue allocation must be fair in the sense that it needs to protect the interests of all the contributing operators and, more importantly, incentivize POPs to contribute their resources to the pool. In addition, to encourage operators with higher investment and more licensed spectrum resources to contribute, it must also take into consideration the contributions of different operators. In other words, operators that contribute more resources should have a larger share of the revenue from the pool. Various fairness criteria have been investigated for the spectrum pooling. In particular, in our previous work [10], we consider the scenarios that multiple operators form a spectrum pool and allow coexistence of their cellular service and other low-power services (e.g., IoT services) in the same band as long as the resulting interference is less than a tolerable threshold. We prove that operators can use the price charged to the spectrum access of low-power services to control the admission of devices. We also investigate the fair revenue division between resource sharing operators. This framework can be directly extended to analyze coexistence of IoT (e.g., eMTC) and cellular services. In this case, the IoT traffic admitted to the spectrum pool will be controlled by the price of the MOP.

2) NOMA for Coexistence between Cellular UEs and Massive IoT: As mentioned earlier, existing RA-based resource allocation approach cannot be applied to the IoT devices due to the physical limit of the licensed band and the inefficient design of the protocol. One possible solution is to apply non-orthogonal multiple access (NOMA). In particular, NOMA improves the utilization of cellular spectrum by exploiting power and code domain reuse. It provides the operators with more flexibility to increase the number of channel sharing devices, e.g., each BS can carefully choose different numbers of low-power IoT devices and high-power UEs at different locations to share the same channel. Furthermore, NOMA does not require IoT devices to perform RACH procedure for data transmission. In particular, in NOMA, the random access and data communication can be combined [14]. For example, each IoT device can randomly pick up a narrowband and start data transmission without waiting for the channel assignment from the BS. The BS can then perform successive interference cancellation to decode the message of each IoT device received in each frequency band. The authors in [3] suggested to apply rateless Raptor codes to generate as many coded symbols as required by each BS, so each BS can differentiate the message sent by different IoT devices. It has been observed that the more difference in channel gains between IoT/UE and the BS, the higher performance improvement can be achieved by the NOMA.

3) Network Slicing for Diverse IoT services: Network slicing is a concept recently introduced by 3GPP to further improve the flexibility and scalability of 5G. The main idea is to create logical partitions of a common resource (e.g., spectrum, antenna, and network infrastructure), known as the slices, to be orchestrated and customized according to different service requirements. Network slicing has the potential to significantly improve spectrum efficiency and enable more flexible and novel services that cannot otherwise be supported by the existing network architecture. In our previous work, we have proposed an inter-operator network slicing framework to support different services with different requirements on a commonly shared resource pool formed by

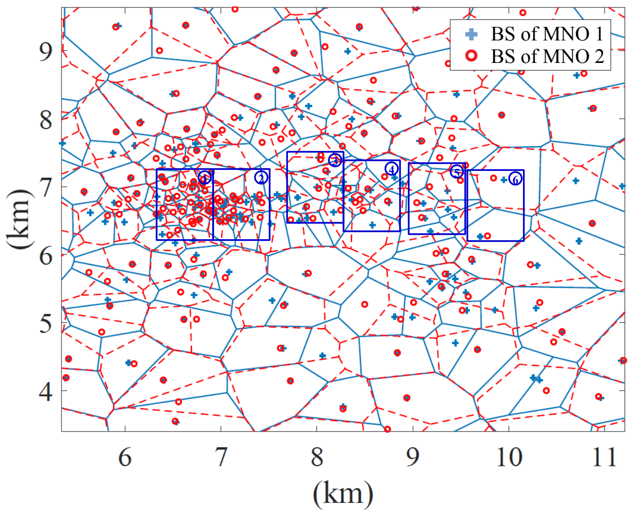

Fig. 2. Locations of BSs deployed by two major cellular operators in the city of Dublin.

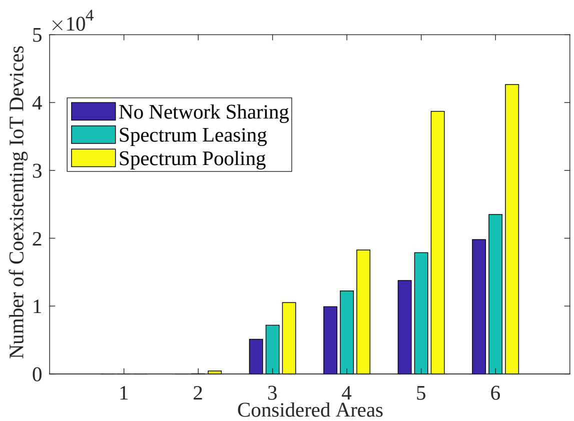

Fig. 3. Maximum number of IoT (eMTC) devices that can be coexisted with cellular UEs in different considered areas.

multiple operators [15]. In this framework, a software-defined mobile network controller will be deployed in the MOP's network infrastructure that can isolate and reserve a certain amount of resource for each type of IoT services (e.g., wearable IoT devices, machine-type IoT, and smart infrastructure). The controller will predict the possible future traffic of all the supported IoT services and can adjust the portion of the resource reserved for each service.

IV. Performance Evaluation

To evaluate the performance improvement that can be achieved by our framework, we simulate a multi-operator network sharing architecture using over 200 real BS locations in the city of

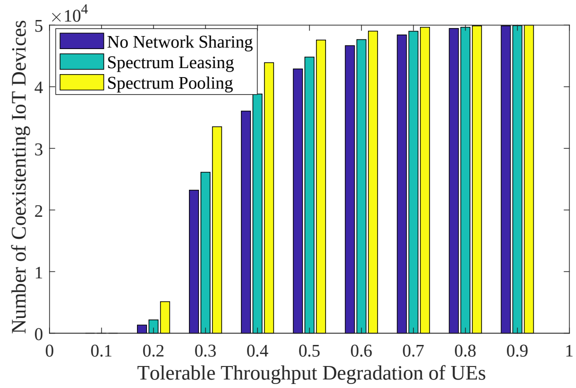

Fig. 4. Maximum number of IoT (eMTC) devices that can be coexisted with cellular UEs under various tolerable throughput degradation of UEs.

Dublin deployed by two major telecom operators in Ireland. The actual distribution and the deployment densities of BSs are shown in Figure 2. We consider saturated traffic for both UEs and IoT devices and evaluate the possible coexistence of IoT (e.g., eMTC) devices and cellular UEs for uplink data communication in the same LTE band. Our results can be regarded as the maximum performance improvement that can be achieved by multi-operator network sharing architecture. The transmit powers of each IoT device and cellular UE are set to 20dBm and 25dBm, respectively. We assume 20 UEs and 50,000 IoT devices are uniformly randomly located in each cell. Each UE occupies a 5 MHz bandwidth. Each IoT device is randomly allocated with a 1 MHz bandwidth channel and can only send data with 20 dBm of transmit power. IoT devices can only be supported when the interference to the UEs is lower than the LTE tolerable interference threshold (-62dBm).

In Figure 3, we carefully select 6 areas from the city center to suburban areas (representing different sizes and deployment density of cells) and compare the maximum number of IoT devices that can simultaneously transmit data with the UEs in the same LTE bands when each UE can tolerate 10% of throughput degradation. We observe that when the size of the cell is small, the number of IoT devices that can share the same spectrum as the UEs is limited due to the high cross-interference between IoT devices and cellular UEs. However, as the size of the cell increases, the total number of coexisting IoT devices can increase significantly. In addition, allowing both operators to share their spectrum via pooling can almost double the total number of IoT devices when the deployment density of BSs is low. This result complements the existing efforts of 3GPP on promoting the network sharing for 5G networks and could have the potential to influence the future practical implementation of the network sharing architecture between major operators.

In Figure 4, we compare the maximum number of IoT devices that can share the same channel with UEs when throughput degradations that can be tolerated by the each UE are different. We observe that the number of IoT devices increases when the UEs can tolerate a higher degradation for their throughput. In addition, network sharing provides more improvement in coexisting IoT traffic when the UEs can only tolerate a small throughput degradation, i.e., network sharing can almost double the maximum number of coexisting IoT devices when each UE can tolerate 20% throughput degradation. However, when the tolerable throughput degradation of UEs increases to 90%, the total number of coexisting IoT devices approaches the maximum values even without network sharing. In other words, network sharing can provide more performance improvement when the UEs require a stringent QoS guarantee with a limited interference tolerance.

V. Conclusion

In this article, we reviewed the current IoT solutions introduced by 3GPP. We then introduced a multi-operator network sharing framework based on 3GPP's network sharing architecture to support coexistence of massive IoT and regular cellular services offered by multiple operators. Various design issues were discussed. Finally, we simulated a multi-operator network sharing scenario using real BS location data provided by two major operators in the city of Dublin. Our numerical results show that our proposed framework can almost double the transport capacity of coexisting IoT traffic under certain scenarios.

Acknowledgment

The authors would like to thank Professor Luiz A. DaSilva and Dr. Jacek Kibilda at CONNECT, Trinity College Dublin for providing the BS location data in the city of Dublin. M. Krunz was supported in part by NSF (grants # IIP-1822071, CNS-1563655, CNS-1731164) and by the BWAC center. T. Shu is supported in part by NSF (grants # CNS-1837034, CNS-1745254, CNS-1659965, CNS-1659962, and CNS-1460897). Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

[1] Cisco, *Visual Networking Index: Forecast and Trends, 2017–2022*, Nov. 2018, white paper at www.cisco.com, Accessed: Jan 30, 2019. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html

[2] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, 2016.

[3] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular IoT: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, Sep. 2017.

[4] X. Lin, J. Bergman, F. Gunnarsson, O. Liberg, S. M. Razavi, H. S. Razaghi, H. Rydn, and Y. Sui, "Positioning for the internet of things: A 3gpp perspective," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 179–185, Dec. 2017.

[5] 3GPP, "Service requirements for next generation new services and markets," 3GPP TS 22.261, V1.0.0, Dec. 2016.

[6] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu, and Z. Han, "Computing resource allocation in three-tier iot fog networks: A joint optimization approach combining stackelberg game and matching," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1204–1215, Oct 2017.

[7] H. Shariatmadari, R. Ratasuk, S. Iraji, A. Laya, T. Taleb, R. Jantti, and A. Ghosh, "Machine-type communications: current status and future perspectives toward 5g systems," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 10–17, Sep. 2015.

[8] 3GPP, "Telecommunication management; network sharing; concepts and requirements," 3GPP TS 32.130, Jun. 2016.

[9] ——, "Network sharing; artechecture and functional description," 3GPP TR 23.251, Jun. 2016.

[10] Y. Xiao, D. Niyato, Z. Han, and K. Chen, "Secondary users entering the pool: A joint optimization framework for spectrum pooling," *IEEE J. Sel. Area Commun.*, vol. 32, no. 3, pp. 572–588, Mar. 2014.

[11] Y. Xiao, Z. Han, C. Yuen, and L. A. DaSilva, "Carrier aggregation between operators in next generation cellular networks: A stable roommate market," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 633–650, Jan 2016.

[12] B. Singh, S. Hailu, K. Koufos, A. Dowhuszko, O. Tirkkonen, R. Jantti, and R. Berry, "Coordination protocol for inter-operator spectrum sharing in co-primary 5g small cell networks," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 34–40, July 2015.

[13] Y. Xiao, K.-C. Chen, C. Yuen, Z. Han, and L. DaSilva, "A Bayesian overlapping coalition formation game for device-to-device spectrum sharing in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 4034–4051, July 2015.

[14] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE J. Sel. Area Commun.*, vol. 35, no. 10, pp. 2181–2195, Oct 2017.

[15] Y. Xiao, M. Hirzallah, and M. Krunz, "Distributed resource allocation for network slicing over licensed and unlicensed bands," *IEEE J Sel. Area. Commun.*, vol. 36, no. 10, pp. 2260–2274, Oct 2018.

Yong Xiao (S'09-M'13-SM'15) is a professor in the School of Electronic Information and Communications at the Huazhong University of Science and Technology (HUST), Wuhan, China. He received his B.S. degree in electrical engineering from China University of Geosciences, Wuhan, China in 2002, M.Sc. degree in telecommunication from Hong Kong University of Science and Technology in 2006, and his Ph. D degree in electrical and electronic engineering from Nanyang Technological University, Singapore in 2012. His research interests include machine learning, game theory, distributed optimization, and their applications in cloud/fog/mobile edge computing, green communication systems, wireless networks, and Internet-of-Things (IoT).

Marwan Krunz (S'93-M'95-SM'04-F'10) is the Kenneth VonBehren Endowed Professor in ECE at the University of Arizona. He is the center director for BWAC, a multi-university NSF/industry center that focuses on next-generation wireless technologies and applications. He previosuly served as the site director for the Connection One center. Dr. Krunz's research emphasis is on resource management, network protocols, and security for wireless systems. He has published more than 280 journal articles and peer-reviewed conference papers, and is a co-inventor on several patents. He is an IEEE Fellow, an Arizona Engineering Faculty Fellow, and an IEEE Communications Society Distinguished Lecturer (2013-2015). He received the NSF CAREER award. Currently, he serves as the Editor-in-Chief for the IEEE Transactions on Mobile Computing. He previously served as editor for numerous IEEE journals. He was TPC chair INFOCOM'04, SECON'05, WoWMoM'06, and Hot Interconnects 9. He was the general vice-chair for WiOpt 2016 and general co-chair for WiSec'12.

Tao Shu received the B.S. and M.S. degrees in electronic engineering from the South China University of Technology, Guangzhou, China, in 1996 and 1999, respectively, the Ph.D. degree in communication and information systems from Tsinghua University, Beijing, China, in 2003, and the Ph.D. degree in electrical and computer engineering from The University of Arizona, Tucson, AZ, USA, in 2010. He is currently an Assistant Professor in the Department of Computer Science and Software Engineering at Auburn University, Auburn, AL. His research aims at addressing the security, privacy, and performance issues in wireless networking systems, with strong emphasis on system architecture, protocol design, and performance modeling and optimization.