Dispersed Computer-Generated Resource Allocation In Small Cell Networks With Full Duplex Heterogeneous Wireless Sensor Network

P.MEENA[1], M.DEVADAS[2]

[1]Mtech in WMC, Dept of ECE, VCE, Warangal, Telangana,India

Email: meenapoola27@gmail.com

[2]Assoc.Prof,Dept of ECE ,VCE ,Warangal , Telangana, India

Email :das.deva@gmail.com

ABSTRACT:

Wireless network virtualization has attracted splendid attentions from every academia and employer. Another growing generation for next technology wireless networks is in-band complete duplex (FD) communications. Due to its promising fashionable primary universal overall performance, FD conversation has been considered as an powerful way to accumulate self-backhauls for small cells. In this paper, we introduce wi-fi virtualization into small cell networks, and recommend a virtualized small mobile network form with FD self-backhauls. We formulate the digital beneficial resource allocation hassle in virtualized small cell networks with FD self-backhauls as an optimization hassle. Since the formulated hassle is a mixed combinatorial and non-convex optimization trouble, its computational complexity is immoderate. Moreover, the centralized scheme may furthermore be stricken by signaling overhead, antique dynamics statistics, and scalability problems. To treatment it effectively, we divide the genuine trouble into sub problems. For the primary sub problem, we switch it to a convex optimization hassle, after which treatment it with the resource of an green alternating path technique of multipliers (ADMM)-based totally completely allotted set of hints. The 2ndsubproblem is a convex problem, which can be solved thru manner of every infrastructure business enterprise organization. Extensive simulations are finished with special tool configurations to expose the effectiveness of the proposed scheme Research problems are to decorate

an Intrusion Detection System (IDS) of a clustered HWSN to boom its lifetime operation and common overall performance of the tool within the presence of and malicious nodes. Also, to address the strength consumption, benefit in reliability, remove and safety with the reason to maximize the existence of a clustered HWSN at the same time as thrilling software QoS necessities. The proposed research is a quite scalable cluster-primarily based totally completely hierarchical keep in mind control protocol for wireless sensor networks (WSNs) to correctly cope with unreliable or malicious nodes. The proposed paintings considers take into account attributes derived from communication and social networks to evaluate the overall receive as actual with of a sensor node. System describes a heterogeneous WSN comprising a massive sort of sensor nodes with appreciably particular social and outstanding of provider (QoS) behaviors as a manner to yield "ground truth" node recognition through "weighted balloting" leveraging statistics of take delivery of as actual with/reputation of neighbor nodes. To show the software of the hierarchical bear in mind manipulate protocol, it can be exercise to really be given as real with-based definitely without a doubt sincerely truly intrusion detection gadget. For consider-primarily based totally really intrusion detection, there exists an crucial gain as real with threshold for minimizing fake positives and faux negatives hazard. Furthermore, remember-based intrusion detection outperforms conventional anomaly-based certainly intrusion detection techniques in each the detection possibility and the faux fantastic possibility. The proposed research furthermore makes use of AOMDV routing protocol which gives sturdy fault tolerance in WSNs. The protocol is based totally definitely totally on a state-of-the-art multipath structures paradigm this is described mainly for heterogeneous WSN. The method leverages an a good buy tons less steeply-priced growth within the community lifetime and a better resilience and fault tolerance.

INTRODCUTION:

Advances in wireless conversation and miniature electronics have enabled the development of small, low-rate, low-energy sensor nodes (SNs) with sensing and verbal exchange competencies. Thus, the issues of Wireless Sensor Networks (WSNs) have grown to be famous studies subjects. WSN is infrastructure based Network, the mass deployment of SNs is completed in WSN and network is usual. The primary function of WSN is to gather and monitor the associated data which about the unique surroundings. The SNs discover the encompassing surroundings or the given aim and deliver the facts to the sink the usage of wireless communiqué. The statistics is then analyzed to find out the dominion of the aim. However, due to the layout form of WSN and their hardware, WSNs be by means of many resource constraints, together with low computation functionality, confined reminiscence and restricted energy. Because WSNs are composed with the aid of numerous low-price and small devices that are generally deploy to an open, remote and unprotected place, they're liable to numerous types of assaults. A prevention mechanism is used to counteract well-known attacks. However, prevention mechanisms can't resist normal assaults. Therefore, the attacks are required to be detected. An Intrusion Detection System (IDS) is used frequently to stumble on the packets in a community, and decide whether they may be malicious packet or attackers. Additionally, IDS can help to increase the prevention device via received natures of attack. Many wireless sensor networks (WSNs) are deployed in an unattended environment wherein strength replenishment is hard. Due to restricted assets, a WSN is calls for to meet the software precise Qi's requirements together with reliability, minimum put off and security, and additionally reduce power consumption to lengthen the device beneficial lifetime. Recently, prior research efforts had been made to expand community architectures and sensor hardware on the way to successfully installation WSNs for a diffusion of applications. However, Due to a large type of WSN software necessities, a widespread-cause WSN design can't satisfy the goals of all packages. Network parameters which include sensing variety, node density and transmission variety should be carefully taken into consideration in step with specific programs, at the network format degree. In order to benefit this, it's miles very vital to seize the influences of various network parameters on community performance with recognize to utility specs. Intrusion detection (i.e., object monitoring) in a WSN may be seemed as a tracking gadget for detecting the intruder this is invading the community location. Thus, it's far critical to amplify the intrusion detection machine (IDS) that is able to dealing with more extensive malicious attacks with energy conservation mechanism to growth system lifetime. In a WSN, there are two ways for the detection of an interloper: unmarried-sensing detection and a couple of-sensing detection. The intruder may be efficaciously detected by most effective a single sensor, in the unmarried-sensing detection. On the opportunity hand, within the a couple of-sensing detection the intruder can best be detected with the resource of more than one sensor. In a few programs; the sensed records provided thru a single sensor might not be ok for spotting the intruder, due to the reality single sensors can most effective sense a portion of the intruder. The intrusion detection may be analyzed in step with the functionality of sensors in terms of the transmission range and sensing range. In a heterogeneous WSN a few sensors have a large electricity to gather an extended transmission variety and big sensing variety. Recent studies [2], [3] tested that using heterogeneous nodes can enhance performance and prolong the gadget lifetime. In the latter case, nodes with advanced sources function CHs appearing computationally in depth obligations at the same time as inexpensive less capable SNs are applied particularly for sensing the surroundings. Thus, the heterogeneous WSN will boom the detection opportunity for a given intrusion detection gadget. It is thought in the studies network that clustering [4], is a powerful answer for carrying out scalability, energy conservation, and reliability. Therefore the cluster based totally heterogeneous WSN can similarly improves the overall performance of the network. By abstracting and sharing resources among special parties, virtualization can extensively reduce the value of system and control in networks [1]. With the high-quality increase in Wi-Fi site visitors and issuer, it's far inevitable to make bigger virtualization to Wi-Fi networks [2], [3]. In wireless virtualization, bodily wireless community infrastructure and bodily radio assets are abstracted and sliced into digital wireless sources, which may be shared with the aid of multiple activities. After virtualization, the Wi-Fi community infrastructure owned.

LITERATURE REVIEW:

Over the past few years, many protocols exploring the energy consumption and QoS gain particularly in reliability in HWSNs have been proposed. In [8], the optimal communication range and communication mode were derived to maximize the HWSN lifetime. In, the authors devised intra-cluster scheduling and inter-cluster multi-hop routing schemes to maximize the network lifetime. They considered a HWSN with CH nodes having larger energy and processing capabilities than normal SNs in the network. The solution is drawn as an optimization problem to balance energy consumption across all nodes within the network along with their roles. In either work [8], [9], no consideration was taken in to the account about the existence of malicious nodes in the network. Relative to [9] the proposed work considers heterogeneous nodes with different densities and capabilities. However, the work also considers the presence of malicious nodes and explores the tradeoff in energy consumption and QoS gain in both security and reliability to maximize the system lifetime. In the context of secure multipath routing for intrusion tolerance, in [10] the authors considered a multipath routing protocol to tolerate black hole and selective forwarding attacks. The basic idea is to use overhearing to avoid sending packets to malicious nodes. In [11] the authors considered a disjoint multipath routing protocol to tolerate intrusion using multiple disjoint paths in WSNs. The research proposed work also uses multipath routing to tolerate intrusion. However, the work specifically focuses on the amount of energy being consumed for intrusion detection and also to reduced energy consumption in multipath routing to tolerate intrusion. Moreover, the work consider intrusion detection to detect and evict compromised nodes as well as the best rate to invoke intrusion detection so that the energy consumption is reduced considerably along with security and reliability gain to maximize the system lifetime. In, voting based IDS approach given the tradeoff between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime. In general there are two approaches by which energy efficient IDS can be implemented in WSNs. One approach is applicable to flat WSNs where an intermediate node provides a feedback about the maliciousness and energy status of its neighbor nodes to the sender node (e.g., the source or sink node) who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach the author adopt in [1] is to use local host-based IDS for energy conservation (with SNs monitoring neighbor SNs and CHs monitoring neighbor CHs only), coupled with voting to cope with node collusion for implementing IDS functions. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions. The solution author considers the optimal IDS detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime. Compared with existing works cited above, the proposed research work extends from [1] with considerations given to explore more extensive malicious attacks, security and reliability, and also investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. In addition to this, the proposed work also consider smart and insidious attackers which can perform more targeted attacks, capture certain nodes with high probability, alternate between benign and malicious behavior and concatenate with other attackers to avoid intrusion detection. Also to investigate the use of trust/reputation management [12], [13] to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbor nodes. Using weighted voting scheme in intrusion detection system (IDS) would considerably reduce the false positives (FPs) and false negatives (FNs) ratio. For effective fault tolerance ad hoc on-demand multipath distance vector (AOMDV) [14] is used to achieve reliability and QoS gain with minimum energy consumption.

LITERATURE REVIEW:

"Software-Defined and Virtualized Future Mobile and Wireless Networks: A Survey" With the proliferation of mobile demands and increasingly multifarious services and applications, mobile Internet has been an irreversible trend. Unfortunately, the current mobile and wireless network (MWN) faces a series of pressing challenges caused by the inherent design. In this paper, we extend two latest and promising innovations of Internet, software-defined networking and network virtualization, to mobile and wireless scenarios. We first describe the challenges and expectations of MWN, and analyze the opportunities provided by the software-defined wireless network (SDWN) and wireless network virtualization (WNV). Then, this paper focuses on SDWN and WNV by presenting the main ideas, advantages, ongoing researches and key technologies, and open issues respectively. Moreover, we interpret that these two technologies highly complement each other, and further investigate efficient joint design between them

"**Wireless world 2020: Radio interface challenges and technology enablers"**

Future pervasive communication system requirements for two to three orders of magnitude capacity improvement, flexible, fast deployment, and cost/energy efficiency are expected to revolutionize the way we design and use wireless networks. From a network infrastructure perspective, the emphasis is placed on achieving ubiquitous, real-time high data rate communications "anytime-anywhere," including at cell-edge, through Small Cell Network architectures and Heterogeneous Cellular Networks (HetNets). From a pervasive systems' perspective, the vision of the Internet of Things suggests the integration between ubiquitous computing and wireless communications targeting a reliable connectivity of things, i.e., computers, sensors, and everyday objects equipped with transceivers. From a backhaul bandwidth, network resource sharing, and optimization perspective, cloud-based processing and radio access network virtualization provide a revolutionary approach toward balancing the degree of centralization of physical and virtual resources management. In this article we analyze these three trends, present key technology enablers, and assess suitable performance merits in an effort to set the scene for the wireless evolution in the era beyond 2020. Over the last decade, cellular networks have evolved from providers of ubiquitous coverage for voice-communication services to access ports available "anytime-anywhere" for high data rate, Internet-based data services. A three-order of magnitude increase in the supported data rates has been achieved, from several kb/s in second generation, (2G) general packet radio service (GPRS) to tens of Mb/s in the latest long-term evolution (LTE) systems. Nevertheless, even these fourth-generation (4G) data rates may soon prove inadequate, since the need for mobile data capacity is growing at an unprecedented rate. Recent market studies conducted by global organizations [1], wireless forums [2], telecom companies [3], and operators [4], indicate that mobile data traffic has doubled every year. Projecting this demand a decade ahead, we are faced with the socalled 1000x data challenge or capacity crunch

"Network virtualization and resource description in software-defined wireless networks" Future networks will be defined by software. In contrast to a wired network, the software defined wireless network (SDWN) experiences more challenges due to the fast-changing wireless channel environment. This article focuses on the state-of-the-art of SDWN architecture, including control plane virtualization strategies and semantic ontology for network resource description. In addition, a novel SDWN architecture with resource description function is proposed, along with two ontologies for the resource description of the latest wireless network. Future research directions for SDWN, control strategy design, and resource description are also addressed. It is widely accepted that future networks will be defined by software. With an ever-increasing demand for broadband communications, new challenges for networks keep coming up, such as intelligent and ubiquitous connectivity, efficient and flexible allocation of resources, etc. To meet these challenges, future networks must support convergence over traditionally separated network domains and offer greater granularity and flexibility in control and in data throughput. With the core idea of separating the control and data planes, software defined networking (SDN) has been considered as one promising approach to meet those challenges in the future. SDN naturally virtualizes the network architecture and isolates the data/control traffic. The logically centralized control plane, with the global knowledge of the network state, is able to obtain, update, and even predict the global information. Thus, SDN can guide end users to select the best accessing network, or even provide them with services from multiple networks. SDN can be treated as one paradigm, rather than an ossified architecture, where one central software program, the controller, is employed to optimize and dictate the overall network behavior [1]. SDN can naturally be extended to versatile scenarios, such as optical networks, mobile wireless networks, data center networks, and cloud computing. The design of wireless network architecture is much more challenging as it must deal with various physical restrictions caused by the fast-changing nature of wireless channels [2, 3]. In the fifth generation (5G) wireless communications, by implementing SDN in eNodeB, distributing control is proven to have higher efficiency [3]. Server virtualization of wireless networks is also more challenging than that of wired networks, as the former has to satisfy the requirements of both coherency and hardware isolation [1]. Furthermore, to implement multiple control strategies at real networks, a universal agreed description of network resources is needed. However, to the best of the authors’ knowledge, no such effort has been reported for software defined wireless networking (SDWN),. One possible reason might be that the existing test-beds for SDWN are relatively small and simple, thus there is no need to develop specialized technologies for network resource description. Nevertheless, considering the heterogeneous networks that exist in the real world, it is important to reach an agreement on the format and schema to uniquely represent the network resources for all layers. Hence, the massive resources can be possibly manipulated simultaneously with high efficiency

SYSTEM MODEL:

In this section, we first describe the virtualized small cell network architecture. Then we present the FD self-backhauling mechanism where the SBSs can transmit and receive data on the same spectrum simultaneously.

A. Virtualized Small Cell Network Architecture

We present a virtualized small cell network architecture with multiple InPs and multiple MVNOs, as shown in Fig. 1. There are M InPs offering wireless access services in a certain geographical area. Each InP deploys and manages a cellular network with one MBS and several self-backhauled SBSs. There are N MVNOs, which provide various services to their subscribers through the same substrate networks. Following the general frameworks of wireless network virtualization [5], [26], the virtualized small cell network architecture consists of three layers: the physical resource layer (PRL), the control and management layer (CML), and the MVNO layer. The PRL, including base stations (BSs), spectrum, power and backhauls from different InPs, is responsible for providing available physical resources. Moreover, the PRL also provides CML with the interfaces needed to control resources. The CML virtualizes the physical resources from different InPs and enables the sharing for MVNOs. Then, the CML manages and allocates the virtual resources to different MVNO users. The resource management functions in CML are realized by a virtual network controller and a virtual resource manager (VRM). The virtual network controller of MVNOs is responsible to collect the resource consumption prices negotiated with InPs, and the users' information (e.g., payment information and QoS requirements) from MVNOs, then feedback the resource allocation results to MVNOs for the purpose of finishing the settlement between MVNOs and InPs. To maximize the total utility of all MVNOs, the VRM is responsible to dynamically allocate the virtual resources from multiple InPs to different MVNO users. Through the virtualization architecture above, each MVNO can have a virtual network composed of the substrate networks from multiple InPs. Hence each user can get services via different access points (either MBSs or SBSs) from different InPs.

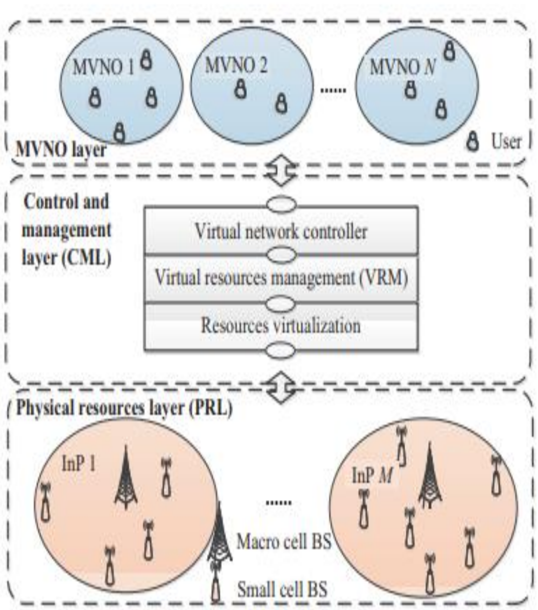

Fig: A virtualized small cell network architecture

B. Small Cell Self-backhauling Mechanism Based on Full Duplex Communications

As shown in Fig. 2(a), SBSs are equipped with FD hardware, which enables them to backhaul data for themselves. In the downlink (DL), a SBS can receive data from the MBS, while simultaneously transmitting to its users on the same frequency band. In the uplink (UL), a SBS can receive data from the users, , the SBS can effectively backhaul itself, eliminating the need for a separate backhaul solution and a separate frequency band. Therefore, self-backhauling can significantly reduce the cost and complexity of rolling out small cell networks. In order to distinguish DL from UL in access and backhaul transmissions, we call the relevant links as access UL, access DL, , the backhaul DL and access UL will suffer some self-interference from access DL and backhaul UL, respectively. Different from the FD relay mechanism in [20], the spectrum can be reused by different SBSs and the SBSs can allocate resource to their users flexibly in our self-backhaul scheme. Compared to DL, UL usually has less traffic. If the transmission of DL is satisfied, the transmission of UL will also be satisfied. As a result, we focus on the transmission of DL in this paper.

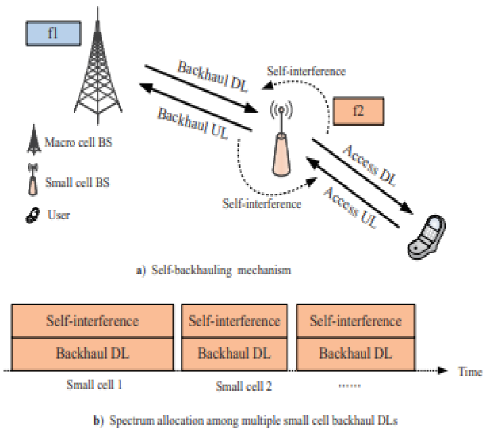

Fig:A small cell self-backhauling mechanism based on full duplex communications.

DISTRIBUTED VIRTUAL RESOURCE ALLOCATION ALGORITHMS

It can be observed that the considered problem is combinatorial and non-convexity. The combinatorial nature comes from the integer constraint C2. The non-convexity is caused by the objective function and constraint C1. As a result, a brute force approach can be used to obtain the optimal virtual resource allocation policy. However, such a method is computationally infeasible for a large system and does not provide useful system design insight. To reduce the computational complexity, firstly, we assume the spectrum allocation indicator vector α is fixed, and then we convert the original problem into a convex problem by variable transformation and perspective function theory to solve X, Y and Z. Secondly, based on the obtained results, we can prove that the problem is convex problem about α, then it's easy to get the optimized α by some convex optimization algorithms. Furthermore, we come back to first step with the result of α to get the new values of X, Y , and Z. By iterations like this for a number of times, the values of X, Y , Z and α will converge, Will introduce how to solve α when X, Y and Z are fixed. we describe the whole process of solution and the convergence of the proposed algorithms.

Algorithm 1 ADMM-based solution algorithm

1: Initialization
   a) At each InP m, collect channel state information of all users within its coverage;
   b) Initialize $X^0 \in \Phi$, $\lambda^0 > 0$ and a stop criterion threshold ξ_2 at the VRM
2: **while** $\|X^{t+1} - X^t\| > \xi_2$
   a) Broadcast X^t and λ^t to each InP;
   b) At each InP m, calculate $\mathcal{A}_m{}^{t+1}$;
   c) At the VRM, update X^{t+1} by combing the results of $X_m^{\ddagger\ t+1}$ from each InP;
   d) Update X^{t+1} via (33);
   e) Update λ^{t+1} via (30) at VRM;
   End
3: Recover Y and Z
4: Output the optimal resource allocation scheme X^*, Y^* and $Z*$

Algorithm 2 Distributed virtual resource allocation algorithm of small cell networks with FD self-backhauls and virtualization

---

1: Initialization
 a) At each InP m, collect channel state information of all users within its coverage;
 b) Initialize $\alpha^0 = 0.5$, $o = 0$ and a stop criterion threshold ξ_1 at the VRM;
2: **while** $\|{G'_{VRM}}^{o+1} - {G'_{VRM}}^{o}\|_2^2 > \xi_1$
 Push the value of α_m^o to the m-th InP
 Run **Algorithm 2**
 Update $\alpha^o \to \alpha^{o+1}$ based on the result of X^*, Y^*
 End
3: Output the optimal resource allocation scheme X^*, Y^*, Z^* and α^*

SIMULATION RESULTS:

In this section, the effectiveness of our proposed virtualized small cell networks with FD self-backhauls and distributed virtual resource allocation algorithm will be demonstrated by computer simulations. In the simulations, we consider a 1Km × 1Km square area covered by two InPs and two MVNOs. In each InPs, there are one macro BS and four SBSs. Each MVNO owns some subscribed users. The number of subscribed users in each MVNO will be varied in different simulation scenarios, and they are randomly located in the whole area. The available bandwidth of both of the two InPs are 10 MHZ. The transmit power of the macro BS and the transmit power of the SBS are 46dBm and 20dBm, respectively. The channel propagation model refers to [35]. The SBSs are randomly deployed in the area. This deployment of BSs is based on the consensus that the location of macro BS is usually calculated by network planning but the location of SBS (e.g., fem to cell) may depend on the users.

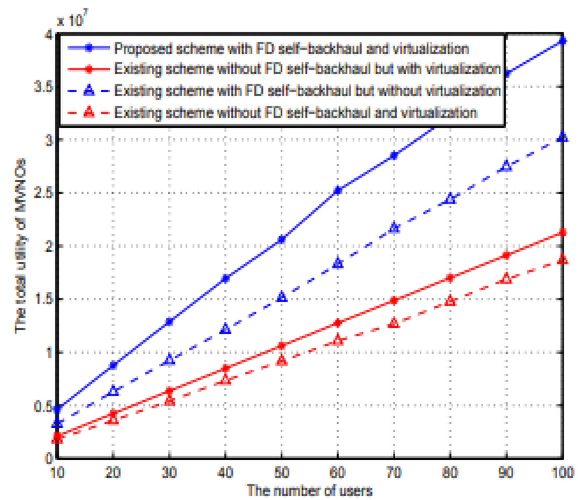

Fig :The total utility of MVNOs

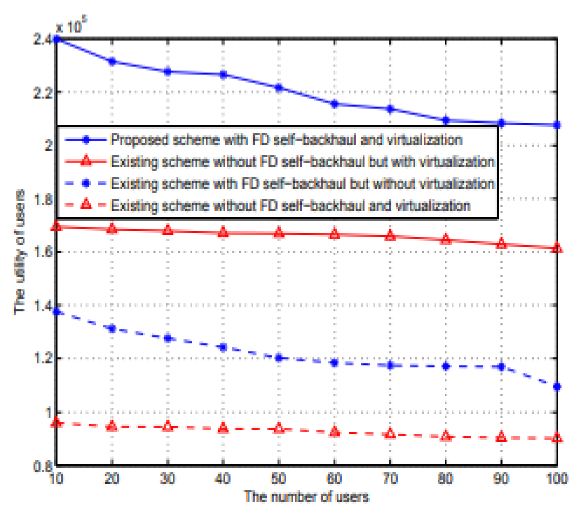

Fig: The average utility of users

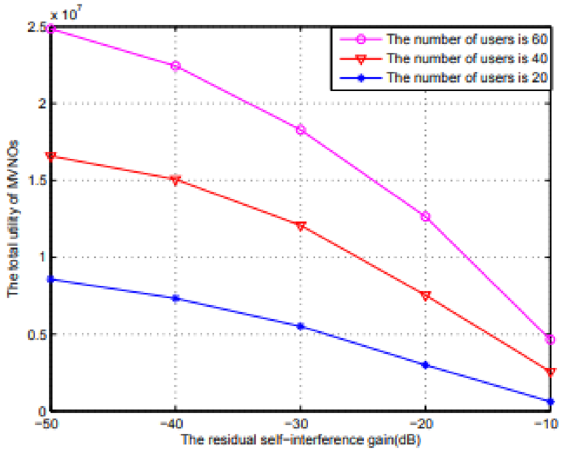

Fig: The total MVNO utility of different residual self interference gain

CONCLUSION:

we investigated the virtual resource allocation issues in small cell networks with FD self-backhauls and virtualization. We first introduced the idea of wireless network virtualization into small cell networks, and proposed a virtual resource management architecture, where radio spectrum, time slots, MBSs, and SBSs are virtualized as virtual resources. After virtualization, users can access to different InPs to get performance gain. In addition, we proposed to use FD communications for small cell backhauls. Furthermore, we formulated the virtual resource allocation problem as an optimization problem by maximizing the total utility of MVNOs. In order to solve it efficiently, the virtual resource allocation problem is decomposed into two sub problems. In this process, we transferred the first sub problem into a convex problem and solved it by our proposed ADMM-based distributed algorithm, which can reduce the computation complexity and overhead. The second sub problem can be solved by each InPs easily because of its convexity and incoherence among InPs. Simulation results showed that the proposed virtualized small cell networks with FD self-backhauls are able to take the advantages of both wireless network virtualization and FD self-backhauls. MVNOs, InPs, and users could benefit from it, and the average throughput of the small cell networks can be improved significantly. In addition, simulation results also demonstrated the effectiveness and good convergence performance of our proposed distributed virtual resource allocation

REFERENCES:

[1] N. M. K. Chowdhary and R. Boutaba, “A survey of network virtualization,” Computer Net., vol. 54, no. 5, pp. 862–876, Apr. 2010.

[2] C. Liang and F. R. Yu, “Wireless network virtualization: A survey, some research issues and challenges,” IEEE

Common. Surveys Tutorials, vol. 17, no. 1, pp. 358–380, First quarter 2015.

[3] C. Liang, F. R. Yu, and X. Zhang, "Information-centric network function virtualization over 5G mobile wireless networks," IEEE Network, vol. 29, no. 3, pp. 68–74, May 2015.

[4] M. Hoffmann and M. Staufer, "Network virtualization for future mobile networks: General architecture and applications," in Proc. IEEE ICC Workshops, 2011, pp. 1–5.

[5] F. Fu and U. C. Kozat, "Stochastic game for wireless network virtualization," IEEE/ACM Trans. Netw., vol. 21, no. 1, pp. 84–97, Feb. 2013.

[6] 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, Aug. 2011.

[7] G. Bhanage, D. Vete, I. Seskar, and D. Raychaudhuri, "SplitAP: Leveraging wireless network virtualization for flexible sharing of WLANs," in Proc. IEEE Globecom, Dec. 2010, pp. 1–6.

[8] A. Banchs, P. Serrano, P. Patras, and M. Natkaniec, "Providing throughput and fairness guarantees in virtualized WLANs through control theory," Mobile Networks and Applications, vol. 17, no. 4, pp. 435–446, Aug. 2012.

[9] R. Kokku, R. Mahindra, H. Zhang, and S. Rangarajan, "NVS: A substrate for virtualizing wireless resources in cellular networks," IEEE/ACM Trans. Netw., vol. 20, no. 5, pp. 1333–1346, Oct. 2012.

[10] A. Tzanakaki, M. P. Anastasopoulos, G. S. Zervas, and B. R. Rofoee, "Virtualization of heterogeneous wireless-optical network and IT infrastructures to support cloud and mobile cloud services," IEEE Comm. Mag., vol. 51, no. 8, pp. 155–161, Aug. 2013.

[11] H. Zhang, C. Jiang, N. Beaulieu, X. Chu, X. Wang, and T. Quek, "Resource allocation for cognitive small cell networks: A cooperative bargaining game theoretic approach," IEEE Trans. Wireless Common., vol. 14, no. 6, pp. 3481–3493, June 2015.

[12] S. Bu and F. R. Yu, "Green cognitive mobile networks with small cells for multimedia communications in the smart grid environment," IEEE Trans. Veh. Tech., vol. 63, no. 5, pp. 2115–2126, June 2014.

[13] C. Ranaveera, P. Iannone, K. Oikonomou, and K. Reichmann, "Design of cost-optimal passive optical networks for

small cell backhaul using installed fibers," IEEE/OSA J. Opt. Common. &Netw., vol. 5, no. 10, pp. A230–A239, Oct. 2013.

[14] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, "Femtocells: Past, present, and future," IEEE J. Sel. Areas Common., vol. 30, no. 3, pp. 497–508, Apr. 2012.

[15] W. Ni, I. Collings, X. Wang, and R. P. Liu, "Multi-hop point-to-point FDD wireless backhaul for mobile small cells," IEEE Wireless Comm., vol. 21, no. 4, pp. 88–96, Aug. 2014.

[16] S. Hur, T. Kim, D. J. Love, R. J. V. Krogmeier, T. A. Thomas, and A. Ghosh, "Millimeter wave beam forming for wireless backhaul and access in small cell networks," IEEE Trans. Common., vol. 61, no. 10, pp. 4391–4403, Oct. 2013.

.