Rochester Institute of Technology
RIT Digital Institutional Repository

Theses

6-1-2021

Exploring Wireless Data Center Networks: Can They Reduce Energy Consumption While Providing Secure Connections?

Sayed Ashraf Mamun
am7753@rit.edu

Follow this and additional works at: https://repository.rit.edu/theses

Recommended Citation
Mamun, Sayed Ashraf, "Exploring Wireless Data Center Networks: Can They Reduce Energy Consumption While Providing Secure Connections?" (2021). Thesis. Rochester Institute of Technology. Accessed from

This Dissertation is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.

Exploring Wireless Data Center Networks: Can They Reduce Energy Consumption While Providing Secure Connections?

by

Sayed Ashraf Mamun

A dissertation submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
in Computing and Information Sciences

B. Thomas Golisano College of Computing and
Information Sciences

Rochester Institute of Technology
Rochester, New York
1 June, 2021

Exploring Wireless Data Center Networks: Can They Reduce Energy Consumption While Providing Secure Connections?

by

Sayed Ashraf Mamun

Committee Approval:

We, the undersigned committee members, certify that we have advised and/or supervised the candidate on the work described in this dissertation. We further certify that we have reviewed the dissertation manuscript and approve it in partial fulfillment of the requirements of the degree of Doctor of Philosophy in Computing and Information Sciences.

Dr. Amlan Ganguly — Date
Dissertation Advisor

Dr. Andres Kwasinski — Date
Dissertation Committee Member

Dr. Minseok Kwon — Date
Dissertation Committee Member

Dr. Panos P. Markopoulos — Date
Dissertation Committee Member

Dr. Satish Kandlikar — Date
Dissertation Defense Chairperson

Certified by:

Dr. Pengcheng Shi — Date
Ph.D. Program Director, Computing and Information Sciences

©2021 Sayed Ashraf Mamun
All rights reserved.

Exploring Wireless Data Center Networks: Can They Reduce Energy Consumption While Providing Secure Connections?

by

Sayed Ashraf Mamun

Submitted to the
B. Thomas Golisano College of Computing and Information Sciences Ph.D. Program in Computing and Information Sciences
in partial fulfillment of the requirements for the
Doctor of Philosophy Degree
at the Rochester Institute of Technology

Abstract

Data centers have become the digital backbone of the modern world. To support the growing demands on bandwidth, Data Centers consume an increasing amount of power. A significant portion of that power is consumed by information technology (IT) equipment, including servers and networking components. Additionally, the complex cabling in traditional data centers poses design and maintenance challenges and increases the energy cost of the cooling infrastructure by obstructing the flow of chilled air. Hence, to reduce the power consumption of the data centers, we proposed a wireless server-to-server data center network architecture using millimeter-wave links to eliminate the need for power-hungry switching fabric of traditional fat-tree-based data center networks. The server-to-server wireless data center network (S2S-WiDCN) architecture requires Line-of-Sight (LoS) between servers to establish direct communication links. However, in the presence of interference from internal or external sources, or an obstruction, such as an IT technician, the LoS may be blocked. To address this issue, we also propose a novel obstruction-aware adaptive routing algorithm for S2S-WiDCN.

S2S-WiDCN can reduce the power consumption of the data center network portion while not affecting the power consumption of the servers in the data center, which contributes significantly towards the total power consumption of the data center. Moreover, servers in data centers are almost always underutilized due to over-provisioning, which contributes heavily toward the high-power consumption of the data centers. To address the high power consumption of the servers, we proposed a network-aware bandwidth-constrained server consolidation algorithm called Network-Aware Server Consolidation (*NASCon*) for wireless data centers that can reduce the power consumption up to 37% while improving the network performance. However, due to the arrival of new tasks and the

completion of existing tasks, the consolidated utilization profile of servers change, which may have an adverse effect on overall power consumption over time. To overcome this, *NASCon* algorithm needs to be executed periodically. We have proposed a mathematical model to estimate the optimal inter-consolidation time, which can be used by the data center resource management unit for scheduling *NASCon* consolidation operation in real-time and leverage the benefits of server consolidation.

However, in any data center environment ensuring security is one of the highest design priorities. Hence, for S2S-WiDCN to become a practical and viable solution for data center network design, the security of the network has to be ensured. S2S-WiDCN data center can be vulnerable to a variety of different attacks as it uses wireless links over an unguided channel for communication. As being a wireless system, the network has to be secured against common threats associated with any wireless networks such as eavesdropping attack, denial of services attack, and jamming attack. In parallel, other security threats such as the attack on the control plane, side-channel attack through traffic analysis are also possible. We have done an extensive study to elaborate the scope of these attacks as well as explore probable solutions against these issues. We also proposed viable solutions for the attack against eavesdropping, denial of services, jamming, and control-plane attack. To address the traffic analysis attack, we proposed a simulated annealing-based random routing mechanism which can be adopted instead of default routing in the wireless data center.

Acknowledgments

The completion of this dissertation and the research behind it would not be possible without the guidance, support, and encouragement from many individuals. I would like to take this opportunity to express my earnest and heartfelt gratitude towards them.

First and foremost, I would like to give special thanks to my advisor, Dr. Amlan Ganguly, for his constant support and mentorship throughout my Ph.D. tenure at Rochester Institute of Technology. He has taught me how to become a good and effective researcher. The meaningful discussions that we have shared during my research have been truly inspirational to me. He taught me how to apporach any reserach question in a thorough and focused way. I cannot thank him enough for his efforts on revising my manuscripts for journal and conference publications. His positive attitudes have influenced me deeply in both research and personal life, which I think will guide me for the rest of my professional and personal life.

I would also like to express my sincere appreciation to my Ph.D. dissertation committee members, Dr. Andres Kwasinski, Dr. Miseok Kwon and Dr. Panos Markopoulos. Without their critical observations, suggestions and thoughtful feedback it would not have been possible to come up with all the solutions to the research questions answered in this dissertation. I thank them from the bottom of my heart for managing time from their busy schedule for all of my research review meetings. I would also like to thank Dr. Satish G. Kandlikar for serving as my dissertation defense chair. I would also like to thank Dr. Pengcheng Shi for the support throughout my Ph.D. tenure. A very special thanks to Min-Hong Fu and Lorrie Jo Turner who helped me a lot by taking care of all the administrative task related to my Ph.D. life and let me focus more on my research work. I would like to thank my friends and lab mates M Meraj Ahmed, Abhishek Vashist, Md Shahriar Shamim, Naseef Mansoor, Sree Gowrishankar Umamaheswaran for their support and encouragement throughout this entire Ph.D. journey.

I would also like to express my gratitude towards my beloved wife Zinat Jahan Faruqui with whom I have passed all the ups and downs during my Ph.D. life. I feel that I am really blessed to have her in my life. I am also thankful to my son Sayed Safir Ashraf who is all the source of my strength and inspiration. I also cannot express with words my thankfulness to my parents, Sayed Mamun Akhter and Afroza Khanom, and my younger brother Sayed Mashroor Mamun, for their unconditional love and support at every step in my life. Everything in my life is meaningless without my family members.

The text of Chapter 3, 4, and 5 are in part a reprint of the material from the papers S. A. Mamun, S. G. Umamaheswaran, A. Ganguly, M. Kwon and A. Kwasinski, "*Performance Evaluation of a Power-*

Efficient and Robust 60 GHz Wireless Server-to-Server Datacenter Network,"in IEEE Transactions on Green Communications and Networking, vol. 2, no. 4, pp. 1174-1185, Dec. 2018, S. A. Mamun, A. Ganguly, P. P. Markopoulos, M. Kwon, A. Kwasinski, "*NASCon: Network-Aware Server Consolidation for server-centric wireless datacenters*," Sustainable Computing: Informatics and Systems, v. 29, p. 100452, Elsevier, 2021, S. A. Mamun, A. Ganguly, P. P. Markopoulos, A. Kwasinski and M. Kwon, "*What Can Ail Thee: New and Old Security Vulnerabilities of Wireless Datacenters*," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-7, respectively. The dissertation author was the primary researcher and author, and the co-authors involved in the publication assisted the research which forms the foundation for that manuscript.

The research presented in this dissertation is supported in part by US National Science Foundation (NSF) CAREER grant CNS-1553264, and does not necessarily reflect the position or the policy of the Government.

This Dissertation is dedicated to my loving Wife, my Son, and my Parents for their unconditional love, support and sacrifices.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Data centers have become an essential part of computing resources as they provide large storage banks and processing power for cloud services. Around the world, data centers consume enormous amounts of energy and power, exceeding two hundred Terra Watt-hour in 2020 [1]. The power consumption of the Data Center Network (DCN) will continuously increase to support the increasing demand for bandwidth [2]. Keeping this high-fidelity network active, often constructed from legacy switching fabrics, consumes 10 to 50% of the total IT power depending on server utilization [3] as shown in Fig. 1.1. This high-power consumption warrants immediate attention to improve efficiency and power consumption of data centers in general and DCNs in particular.

Traditionally, DCNs are interconnected with fat-tree topology using wired links over multiple hierarchical levels of aggregation. These tree-based networks exhibit inherent limitations in scalability and oversubscription as they rely on copper and optical cable-based links and a hierarchical topology [4]. Moreover, wired network technologies require power-hungry switches and create large bundles of cables, causing design overheads and maintenance challenges and obstructions to the flow of chilled air for cooling [5]. Inefficient cooling only exacerbates the energy efficiency problem, especially for small and mid-size data centers with hundred to a few thousands of individual servers in educational institutions and private enterprises because these are designed and deployed in an ad-hoc manner, often leading to structural and functional heterogeneity making regular systematic design impossible. To address these common design issues faced by wired data centers, wireless data center architectures are being investigated as a promising alternative. The capability of the unlicensed 60GHz wireless band to deliver very high communication rates has led to the development and approval of the `IEEE802.11ad` wireless local area network (WLAN) standard [6]. Therefore, recently

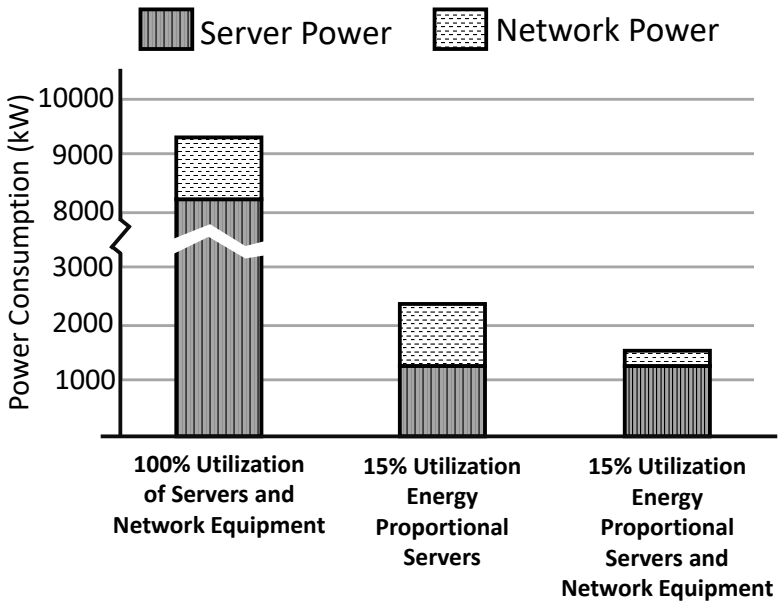


Figure 1.1: Comparison of server and network power at different utilization.

proposed designs leverage newly developed technologies in the unlicensed 60GHz wireless band for wireless DCNs [7, 8].

Recent developments in the millimeter-wave (mmWave), such as 60GHz technologies allow the transceivers to consume low power, in the range of a few Watts [9, 10] and establish multi-gigabit communication channels [11]. Directional horn antennas, which have been used in wireless DCNs [12] as well as more recently developed phased arrays of antennas in the 60GHz bands [13] are capable of providing high directional gains and beam steering capability between wireless transceivers. Using such antennas, the 60GHz channels can exhibit spatial reusability, allowing multiple concurrent links reusing frequency bands to be formed within the same data center. The low power consumption combined with the ability to form concurrent multi-gigabit channels makes these transceivers ideal for use in power-efficient wireless DCNs.

1.1 Data Centers

A data center is a centralized facility of an organization's IT operations and equipment, as well as where it stores, manages, and modifies its data. Data center houses a network's most critical systems and is vital to the continuity of daily operations [14]. The reliability and security of data is an essential requirement for any data center. Although every data center designs are unique and

depends on the purpose and location of the data center, they can generally be classified broadly into two classes- internet-facing and enterprise data centers. Internet-facing data centers usually support relatively few common applications, are typically browser-based, and have many users, typically unknown. On the other hand, enterprise data centers, which is also known as internal data centers, service fewer users but host more applications that vary from off-the-shelf to highly customized applications. Data center architectures and requirements can differ significantly. Data centers are consisted of different components. Although the components in the data center varies depending on the task done by the data center, generally the following equipment can be found in a general data center: IT equipment consisting of servers and network equipment, environment control system including computer room air conditioners (CRAC), heating, ventilation, and air conditioning (HVAC) systems, and exhaust systems, uninterruptible power source systems, cabling systems, power systems, racks, fire protection systems, physical security systems, electrical systems such as lighting.

Data centers have evolved significantly in recent years, adopting technologies such as virtualization to optimize resource utilization and increase IT flexibility. Different network architectures are being proposed and implemented in the data centers. The focus has been given to not only make the data center more powerful but also to make them more power efficient. Measures have been taken to reduce the enormous energy consumption of data centers by incorporating more efficient technologies and practices in data center management. Data centers constructed following these standards have been coined "green data centers." Data centers are being used in every aspect of life extending from "basic needs" of food, clothing, shelter, transportation, health care, to social activities that cover the relationships among individuals within a society. Most of the companies or entities providing these services such as Amazon, Facebook, Google, NASA, US government, FBI, IBM, Walmart, etc. have multiple numbers of data centers. Depending on the requirements, the size of the data center can vary significantly- ranging from a few servers to hundreds or thousands servers. Regardless of the size, all the data centers serve one major purpose, that is to process information. Servers in a data center most of the time requires to communicate internally between themselves to perform tasks. Hence, the servers in a data center are connected among themselves as well to the external world through a network called data center network. Different techniques and protocols exist to implement this network, each having its advantages and disadvantages. We have discussed about most relevant and common topologies currently found in actual data centers around the world in section 2.1

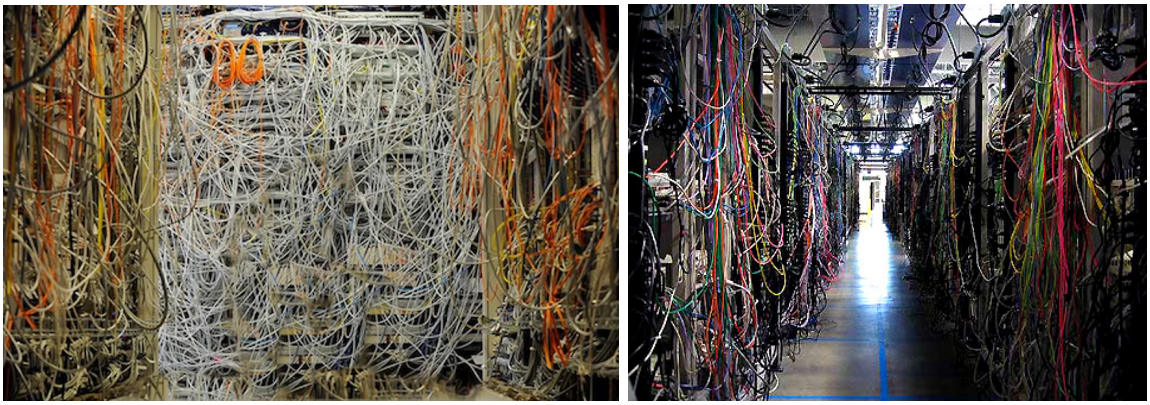


Figure 1.2: Examples of complex cabling in existing data centers.[1][2]

1.2 Existing Problems in Data Centers

The challenges in current DCN's are high design and maintenance cost, huge power consumption, high cabling complexity, hard to keep accurate per-cable information and inefficient cooling. Structured cabling bundle incur significant initial effort and cost to set up and still may cause airflow blockage.

Due to the use of diversity and complexity, it is difficult to generalize the energy consumption pattern in data centers. However, in general, there are five distinct sub-systems that constitute almost the entire power consumption of a data center. These are power conditioning equipment, server and storage systems, network equipment, cooling and weathering equipment, and finally lighting and physical security equipment.

A significant portion of the power consumption of a data center is due to the IT equipment consisting of servers and network devices which contributes more than 60% [15] towards the total power consumption of the data center. The next contributing factor in the power consumption in data center is the power consumption for the cooling and weathering control which is directly related to the power consumption of IT equipment as it is used to cool down the heat generated by the servers and switches. Therefore, the management of power consumption of the IT equipment is the most important significant factor for making the data center energy efficient. In most of the data centers active now around the worls, a large amount of the IT power is wasted due to the fact the systems that are idle or underutilized. In practice, most of the servers found in data centers have average utilization within the range of 20-30% [16]. This idle energy waste adversely affects the power consumption of the cooling infrastructure as the cooling system need to extract this additional heat

[1]Image sources: https://www.backupassist.com/blog/server-cable-disasters-that-look-like-famous-paintings
[2]Image sources: https://www.tempesttelecom.com/lepton-test-lab-automation/

generated from this idle activity of the servers and network devices, which ultimately leads to a 50-100% increase in power consumption in the entire data center [17]. Cabling complexity is another challenge in data center designing and maintenance. In practice, managing cables is an afterthought for most data centers. With time, as the number of servers in the data center increases, managing power and network cords becomes challenging. Two extreme cases of unmanaged cabling found in data centers are shown in Fig. 1.2. Moreover, improper and unstructured cabling causes overall airflow in data centers causing inefficient cooling.

1.3 Emerging Millimeter-Wave Wireless Communication

Advancements in the 60GHz technologies allow the transceivers to consume low power, in the range of a few watts [9, 10] and establish multi-gigabit communication channels. In some recent proposed works, it has been demonstrated that with advancement of the fabrication technology and adaptation of newer standards, power consumption of the transceivers can come down to as low as $0.309mW$ for 60GHz [18]. Directional horn antennas, which have been used in wireless DCNs [12] are capable of providing high directional gains and beam steering capability between wireless transceivers. However due to requirement of rotating the antennas when beam steering is necessary, usability of the horn antennas become very limited in the environment where high speed dynamic beam steering is necessary. More recently developed phased arrays of antennas in the 60GHz bands [13] can overcome the limitations of the horn antennas by electronically steering the beam within micro seconds. Using such antennas, the 60GHz channels can exhibit spatial reusability, allowing multiple concurrent links reusing frequency bands to be formed within the same data center. The capability of the unlicensed 60GHz wireless band to deliver very high communication rates has led to the development and approval of the `IEEE802.11ad` wireless local area network standard [6] which utilizes V-band of millimeter wave ranging from 57GHz to 64GHz, which can reach 6.7Gbps per channel. A very recent amendment of this standard enhances the frequency range from 57GHz to 71GHz. Therefore, recently proposed designs leverage newly developed technologies in the unlicensed 60GHz wireless band for wireless DCNs [7, 8]. Furthermore, another standard IEEE 802.11ay has been proposed recently which is expected to be finalized by the end of 2021 [19]. In this proposed standard, with a higher order of modulation, a single channel can support up to 176 Gbps data rate. Based on this standard, design of the transceivers are being proposed in recent years [18] However, in our work, we have adopted the `IEEE802.11ad` standard for communication protocol.

1.4 Research Objectives

1.4.1 Designing an Energy-Efficient Server-to-Server Wireless Data Center Network with an Obstruction-Avoidance Adaptive Routing with 60GHz wireless links to Reduce the Power Consumption of the Data Center Networks

The primary goal of this research is to overcome the problems of the data centers mentioned in section 1.2 by designing an energy-efficient server-to-server wireless architecture, which reduces the overall power consumption of the data center, while can sustain the network required load at the same time. The higher layer switching equipment of a data center consumes a large amount of power. To alleviate this issue, an alternate architecture is required to be developed where the number of the upper layer switches can be reduced without hampering the overall throughput while maintaining low latency.

Initially, we tried to reduce the power consumption of the DCN by eliminating the highest layer switches, particularly the core and aggregate layer switches. We designed a Top-of-Rack to Top-of-Rack (ToR-ToR) wireless data center network [20] which eliminates the core and aggregate layer switches. Instead, the access layer switches were equipped with a 60GHz transceiver to maintain the communication between the ToRs. Although a limited amount of improvement in energy efficiency was observed with the proposed ToR-ToR wireless architecture, it was not significant enough as access layer switches were still in the network. From this alternate architectures, we realized that to further improve the energy efficiency of a data center, all the physical layer switches, including the core, aggregate, and access layer switches, are required to be removed from the network altogether and develop a server-to-server wireless network architecture based on the 60GHz wireless technology. Through direct server-to-server wireless links using directional antenna arrays, the power-hungry switching fabric of traditional DCNs can be eliminated, which should result in significant power savings in the data center. However, to utilize 60GHz wireless links, Line-of-sight (LoS) between the communicating nodes is an essential requirement. A mechanism has to be developed to maintain LoS between the communicating servers inside the data center to sustain the communication links between the servers. Moreover, the presence of any obstruction in the data center aisles, such as an IT technician or any interference caused by an internal or external source, may result in blocking LoS or the links, causing a failure in data transmission. To overcome this situation, an obstruction avoidance routing algorithm needs to be developed also.

1.4.2 Design a Mechanism to Perform a Network-Aware Server Consolidation for Wireless Data Centers to Address the High Power Consumption of the Servers in the Data Center

Removing the different layer switches can reduce the power consumption of the network portion of the data center, whereas a significant amount of the power consumption comes from the servers in the data center. As most of the servers running in the data centers are underutilized, there is a provision of further improvement in the overall energy efficiency of the data center if the utilization of the servers can be improved and manage the load in the data center in a more efficient way. The servers in a data center can be utilized in a more efficient way by performing a server consolidation which has the potential of significantly reducing the total power consumption of the data center. On the contrary, server consolidation can adversely affect the network performance in case of aggressive consolidation done without considering the network requirements. To improve the energy efficiency of the data center while maintaining the required network performance, a new server consolidation technique is needed to be developed. Moreover, to maintain the energy efficiency of the data center, it is most likely that the consolidation operation needs to be repeated periodically. Hence a mechanism to identify the optimal time interval between two consecutive consolidation operations has to be developed alongside the consolidation algorithm.

1.4.3 Identify the Security Vulnerability of Proposed Server-to-Server Wireless Data Center Networks and Explore Solution Space for These Threats

Server-to-server wireless data center network architecture has the capability of reducing the power consumption of the data center by eliminating the different layers of power-hungry switches. Nevertheless, to become a practical and viable solution for data center network design in the real world, the security aspect of the DCN has to be ensured. The proposed server-to-server wireless data center can be vulnerable to a variety of different attacks as it utilizes wireless links over an unguided channel for communication. Wireless networks can be vulnerable to a variety of different attacks. As the wireless links are used to establish communication between pairs of servers, it inherits a few of this vulnerabilities of any traditional wireless network. A few of the possible attacks, including but not limited to, are eavesdropping, denial of services, network jamming, encryption tracking, authentication attack, MAC spoofing, node capture, mascaraed, rogue wireless device. Different solutions spaces for most of these attacks have already been proposed in the literature, but primarily for lower bandwidth sensor networks or traditional Wi-Fi networks. These solutions may or may not be applicable in the context of the proposed wireless data center. The primary reason for this

discrepancy is due to the usage of mmWave, such as 60GHz wireless links, whereas most of the solutions that exist in the literature are designed for 2.4/5 GHz wireless band or much lower frequency bands. For instances, for traditional Wi-Fi system, most of the communication happens with omnidirectional antennas where reflected wave bounced from different surface plays a significant role in the communication, whereas for the 60GHz mmWave, for reliable communication, a directional beam is essential. To ensure the data security of the data center, the possible threats are needed to be analyzed, and threat models are required to be developed. Possible defense mechanisms against these attacks are also required to be developed where existing security solutions can not be adopted directly.

1.5 Research Contributions

In this dissertation, we have designed and evaluated a novel Server-to-server wireless data center network architect, which reduces the power consumption of the data center network by almost an order of magnitude. Furthermore, to reduce the server power consummation, we have proposed a novel network-aware server consolidation technique for wireless data centers. Finally, we have identified the security vulnerability of the proposed wireless data center architecture and exploded possible solution space for these security threats. The principal contribution of this dissertation can be summarized as below:

1. **Design of a Server-to-Server Wireless Data Center Network (S2S-WiDCN) using 60GHz Wireless Links with an Obstruction-Avoidance Adaptive Routing**
    - Design a default *Horizontal-First* routing mechanism for S2S-WiDCN
    - Design a S2S-WiDCN architecture with an *obstruction-avoidance adaptive routing* for server-to-server communication using 60GHz wireless links
    - Evaluate the performance of S2S-WiDCN with different type of traffic patterns depending on different types of applications
    - Evaluate the performance of S2S-WiDCN in presence of obstructions to LoS paths
    - Model and estimate the power consumption of S2S-WiDCN and compare to traditional data center networks
2. **Design of a Network-Aware Server Consolidation Heuristic named Network-Aware Server Consolidation (*NASCon*) to Reduce the High Power Consumption of the Servers in Data Center**

- Design a Network-Aware Server Consolidation*NASCon* heuristic that takes advantage of the two distinctive features of the S2S-WiDCN, namely high link diversity for each server and the existence of a separate physical plane for achieving predictable latency in exchanging control information to reduce the computational complexity of the heuristics
- Compare the performance of the S2S-WiDCN with the *NASCon* algorithm with respect to a traditional fat-tree based wired network
- Derive a mathematical model to identify the optimal inter-consolidation time
- Validate the model through extensive simulations
- Evaluate the performance of the *NASCon* algorithm with high bandwidth future data center networks for both wired and wireless networks

3. **Identify the Potential Security Vulnerability of the S2S-WiDCN and Propose Viable Solutions Against These Threats**

- An in-depth analysis of the possible threats and attacks on the wireless data center network is done.
- Quantified the impact of such attacks on data security of the overall network's performance using a network-level simulator.
- Proposed a relatively light-weight security solution to tackle the eavesdropping attack in the S2S-WiDCN environment.
- Proposed a novel simulated annealing based routing mechanism to address the traffic analysis attack.
- Proposed a solution against the denial of services attack leveraging the unique control plane feature of the S2S-WiDCN.

1.6 Dissertation Organization

This dissertation is organized into six chapters. This chapter describes the existing problems of the traditional data centers and motivation for designing a server to server wireless data center (S2S-WiDCN) and Network-Aware Server Consolidation (*NASCon*) to address the high power consumption issue of the data centers. *Chapter 2* discusses the contemporary works on different data center network architectures including, wired and wireless interconnection, as well as recent works on different server consolidation techniques. This chapter also discusses the recent development of the low-power 60GHz wireless communication techniques, which ultimately motivates us to design

a complete server-to-server wireless data center to address the power consumption of the network portion of the data center, which is presented in *Chapter 3*. *Chapter 4* describes our proposed server consolidation technique *NASCon* which addresses the high power consumption of the servers in the data center due to over-provisioning. Nevertheless, to become a viable alternative to the existing data center architecture in the future, S22-WiDCN with *NASCon* has to meet the security requirement of the data centers. In *Chapter 5* we discuss the potential security vulnerabilities of the S2S-WiDCN and explore possible solutions to overcome these shortcomings. Finally, *Chapter 6*, summarizes the important lessons learned from all of these studies and possible research directions for the future.

Chapter 2

Related Work

With the aim to provide the necessary context to this dissertation, in this chapter, we briefly discuss the state-of-the-art research works in providing the solutions for the existing and anticipated network and power problems in the data centers. Several different approaches have been proposed to tackle the challenges in data center design, such as energy consumption, cabling complexity, scalability, and over-subscription. Designing some alternate topology for the DCN or consolidation of the servers has been widely explored. The most common DCN topology used today is a fat-tree topology [21], in which servers are connected through a hierarchy of access, aggregate, and core layer switches. The core switches also serve as gateways to the external Internet. The DCN with this topology suffers from congestion or over-subscription at the upper levels of the hierarchy, while the wired links cause design and maintenance challenges and obstruct the path of chilled air for cooling [5]. To address these issues, different data center architecture and topologies have been explored in the literature. Moreover, Servers in a data center are almost always underutilized due to over-provisioning, which contributes heavily toward the high-power consumption of the data centers. To overcome the under-utilization issue, different server consolidation techniques have been explored. These will be discussed in the following sub-sections.

2.1 Data Center Network Architectures

To address different data center issues, like high power consumption, scalability, design complexity different data center networks have been proposed in the literature. These can broadly be classified into two groups, i.e., wired DCNs and wireless DCNs. The most relevant works are discussed below.

2.1.1 Wired Data Center Network Architectures

Wired data center networks can be broadly classified into two groups – the first one is switch-centric design and the second one is server-centric design. Fat-tree is the most common form of switch-centric design. Some of the other switch-centric designs include VL2 [22], Jellyfish [23], etc. VL2 uses Valiant Load Balancing to spread traffic uniformly across network paths. Recently, server-centric DCN architectures have been proposed such as BCube [24], DCell [25] and FiConn [26]. BCube is a recursive topology specially designed for shipping container-based modular data centers. DCell is also a server-to-server network with a recursively defined structure. FiConn employs an interconnection structure utilizing two Ethernet ports on each server using commodity servers and switches to establish a scalable data center network. Being server-to-server wired DCNs, both these architectures have increased cabling complexity compared to a hierarchical fat-tree DCN. All these DCNs eliminate the need for the power-hungry hierarchical switching infrastructure of fat-tree DCNs with a cost of increasing cabling complexity. To improve the performance of DCNs, optical interconnects have been explored extensively [27]. DOS [28] is an optical DCN that exploits wavelength routing characteristics of a switching fabric based on an Arrayed Waveguide Grating Router that allows contention resolution in the wavelength domain. Helios [29] is a hybrid electrical and optical switch architecture that can deliver significant reductions in the number of switching elements. C-Through [30] is a hybrid packet, and circuit-switched data center network architecture having the aims of supplying high bandwidth to data intensive applications through high-speed optical circuit-switched network using the Top-of-Rack switches. All of these optical networks uses the hybrid network which still requires power hungry switching equipment as well as increases cabling complexities. While many such novel DCN architectures have been proposed, these innovations mainly rely on either copper or optical cables. They do not eliminate the challenges inherent to wired DCNs with physical links concerning cabling power consumption, complexity, implementation effort, and maintenance.

2.1.2 Wireless Data Center Networks

In [7, 12, 31, 32], it is proposed to use mmWave inter-rack links to alleviate high power consumption of DCNs. Also, recent work on wireless data centers proposes interconnecting entire racks of servers via 60GHz wireless links to utilize commodity Ethernet switching between servers inside individual racks [7]. Phased antenna arrays or directional horn antennas are used to establish wireless links between ToRs [32, 33]. In [34], a wireless DCN was proposed by bridging adjacent rows of racks by ToR wireless connections. Line-of-Sight (LoS) communication paths are necessary between the

antennas for reliable communication in a wireless data center [32] as paths through metal frames and racks increase losses due to obstructions. Hence, reflectors on ceilings and walls in the form of metallic mirrors or signal relays can be mounted to form paths where direct LoS does not exist [35]. All of these proposed work uses ToR switches, which contributes largely to the total power consumption of DCN. Moreover, these works establish the physical layer feasibility of the mmWave communication in a data center environment but do not evaluate the network-level characteristics such as data rates, flow completion durations and power consumption which is the focus of this paper. Cylindrical [36] or polygonal [37] arrangements of servers are proposed to create LoS wireless links between servers. This, however, requires non-traditional cylindrical or polygonal arrangement of servers having implications on cooling, server density, and scalability of the DCN that are not well-known at this point. In [38], an inter-rack wireless network solution named FireFly is proposed which uses free-space optics (FSO) to link the ToR of the data center. The inter-rack FSO based DCN will need ToR switches thereby not capable of removing the power-hungry switches in the architecture. Moreover, FSO links require precise alignments of lenses and mirrors. In [39], another FSO based data center architecture was proposed where ToRs can communicate directly with FSO with the help of disco ball shaped mirror assembly on the ceiling. However, in this thesis, we propose direct server-to-server wireless links in a DCN to eliminate the need for power-hungry switches at the Top of rack and higher hierarchical levels while maintaining the traditional rectangular arrangement of server racks. We evaluate the network-level performance characteristics such as data throughput, flow completion durations and network power consumption of 60GHz mmWave S2S-WiDCN with direct server-to-server links and compare it to several alternative DCNs.

2.1.3 Recent Developments in 60GHz Communication

Due to its high communication rates, the unlicensed 60GHz wireless band has attracted attention over the past several years [40, 41]. These efforts have led to the development and approval of the `IEEE802.11ad` wireless local area network standard [6]. This standard extends the `IEEE 802.11` family of WLAN standards to enable networking in the 60GHz unlicensed spectrum band within the V-Band frequencies in the United States and achieving data rates of up to $7Gbps$ [12]. More work has followed the approval of the standard with the design of the corresponding transceivers [40, 41]. Terahertz wireless links for data center are also being explored recently [42, 43]. We leverage the above-mentioned advances in 60GHz communication technologies to enable a wireless DCN while designing the S2S-WiDCN architecture.

2.2 Server Consolidation in Data Centers

To alleviate the power wastage due to underutilization of the servers, consolidation of the tasks virtual machines (VMs) running in different servers into fewer servers has become a major focus area in the research community [44,45,46,47,48,49,50,51]. Underutilization of the servers in a data center has always been observed mainly due to the overprovisioning for the peak demand hours [52]. Most of the prior works in this field focus on either reducing power consumption of the networking portion or the server portion of the data center without considering the impact of one on the other. In [44] various formulations of the cost-aware application placement problem for servers was first introduced. For each of the formulation, the model assumptions were described and the practicality of these assumptions to solve the corresponding problem was analyzed. It was proposed to use the ratio of migration cost and power cost during VM placement decision while the impact on network performance was not considered. Similarly, in [45], a system was proposed that optimizes power consumption, performance benefits, and transient costs incurred by server consolidation. In [46] an efficient power-aware resource scheduling strategy was proposed that reduces data center power consumption based on live VM migration. A framework for VM migration and placement was proposed in [47]. Both the network topology and network traffic demands were considered to minimize energy consumption while satisfying as many network-demands as possible. Similar work has been done in [53] where multiple VMs could be placed in a single server. In [48], energy-aware VM placement was proposed where, application dependencies were considered to reduce network energy consumption. In [49], a network-aware VM consolidation scheme was proposed for solving combined VM consolidation problem to conserve the energy of the data center. In [50], a heuristic to control VM migration based on prioritizing VMs with steady capacity was proposed. In addition to server consolidation, an opportunistic approach to reduce power consumption in DCNs is proposed in [54]. Due to rise of cloud computing, server consolidation in cloud environment has become a major research area in last few years [55, 56, 57]. However, server-consolidation with the sole objective of power reduction can impact the performance of the data center negatively if the network is incapable of supporting the resultant aggregated traffic patterns. However, the impact of server consolidation on such novel network architectures has not been investigated. Moreover, the impact of these novel networks on the consolidation algorithms is not studied either.

2.3 Security in Wireless Data Center Networks

Wireless communication in the data center environment is becoming a popular research area only for last few years. Although different communication architecture has been proposed and various techniques have been explored, the security of the wireless data center is still a vastly unexplored field. The primary goal for the security of any system is to ensure the following four things- Confidentiality, Integrity, Authentication, and Availability (CIAA) [58]. Confidentiality is the ability to shield the information or data from a passive attacker. Most of the time confidentiality is considered the most crucial goal for the security system. Data authentication is the ability to ensure that the information is sent by the original source and not from an intruder. The system should have the capability of identifying both the receiver and sender. The techniques commonly used for authentication can be roughly divided into two groups- symmetric and asymmetric mechanism. Although authentication is required for both wired and wireless networks, for wireless networks it is particularly much more challenging to ensure the authentication due to the wireless nature of the medium. Data integrity is the ability to make sure that the data has not been tampered with or changed in the medium by an attacker. The integrity of the data is compromised when an attacker or a malicious node sends some data to other node pretending to be some another node.

Many studies have been done on the security of wired data centers [59, 60, 61]. On the contrary, as wireless data centers are still being an emerging technology, not much study has been done on the security aspects of these types of data centers. It has also been widely considered that wireless systems are inherently more unsecured than their wired counterparts [62]. Moreover, being a wireless system, S2S-WiDCN also inherits most of the threats associated with any wireless network. Because of the direct wireless communication capability of every server, S2S-WiDCN can be compared with a traditional wireless sensor network (WSN). Many of the security threats associated with WSN [63] are also applicable for S2S-WiDCN. However, unlike WSNs, the nodes (servers) here are highly uniformly arranged, and the inter-server communication is done through highly-directional antennas having high-speed wireless links. Recent work has shown that, with the use of directional antennas, the security of the WSN can be enhanced to some extent [64]. Studies have been done on the security aspect of traditional wireless networks involving lower bandwidth and solutions have been proposed [65, 66, 67]. However, these solutions for traditional wireless systems are unlikely to be suitable for mmWave based wireless networks mainly because of a large number of antenna array involved and sensitivity of the frequency to physical blockage [68, 69]. On the contrary, some security related advantage exists because of the high directionality of the antenna arrays in mmWave bands. In [68], it was shown that with point-to-point mmWave wireless communication, significant

secrecy improvement compared to the conventional microwave systems can be achieved. On the contrary, in [70], it was shown that even with the highly directional transmission, eavesdropping is still possible by creating virtual periscope. However, the network-wide secrecy performance of the mmWave communication system is still unknown [71]. Denial-of-service (DoS) attack can be another attack which can severely hamper the performance of the entire data center. In [72], the authors showed that in any wireless controlled network system, DoS can have significantly adverse effect on the performance. In [73], a method was proposed to mitigate DDoS attack for 5G network involving network slicing. Another possible attack on a completely wireless system is the signal jamming attack. It can severely interfere with the normal operation of wireless networks [74]. In [75] the authors said that, due to the hardware constraints of mmWave transceivers, still it is not very feasible to do a jamming attack. But with emerging of newer higher frequency radios, jamming attack in mmWave is becoming imminent in the near future. To the best of our knowledge, no work exists on the security of an entirely wireless data center which is required to consider S2S-WiDCN as a viable alternative solution for wired networks. .

Chapter 3

Server-to-Server Wireless Data Center Network Architecture

In this chapter, a server-to-server wireless DCN architecture called S2S-WiDCN based on the 60GHz wireless technology for a small to medium-sized data center is proposed. Through direct server-to-server wireless links using directional antenna arrays, the power-hungry switching fabrics of traditional DCNs can be eliminated, resulting in a significant power savings in data transfer [76]. The communication between servers in the wireless DCN is achieved along horizontal lines and vertical planes as shown in Fig. 3.1, which shows only a few horizontal red lines and a single blue plane for clarity. The horizontal communication lines are used for data transfer between rows, whereas, the yellow planes are used for transmissions within the same row. However, the presence of any obstruction in the data center aisles such as an IT technician may result in blocking of the horizontal Line-of-Sights (LoS) or interference caused by other wireless signal may cause a failure in data transmission. Therefore, to recover from such obstructions a novel adaptive routing mechanism is proposed [77] in this work. The performance as well as power savings of the proposed server-to-server wireless DCN (S2S-WiDCN) is compared to that of a conventional hierarchical fat-tree-based DCN. Various kinds of data center traffic have been considered for these evaluations, which are typically encountered in index-search/query-response and multimedia/video applications. It is demonstrated later in this chapter that S2S-WiDCN is able to sustain and provide performance comparable to the conventional counterpart at five to seventeen times lower power consumption depending on the load on the data center network. The novel contributions of this chapter are:

- We propose a novel direct server-to-server wireless communication based fully wireless data

center architecture.

- We propose the S2S-WiDCN architecture with horizontal first routing.
- We design the S2S-WiDCN architecture with an obstruction-avoidance adaptive routing for server-to-server LoS communication using 60GHz wireless links.
- We evaluate the performance of S2S-WiDCN with different kinds of traffic patterns depending on different types of applications.
- We evaluate the performance of S2S-WiDCN in presence of obstructions to LoS paths.
- We modeled and estimate the power consumption of S2S-WiDCN and compare it to traditional tree-based DCNs.

3.1 Wireless Data Center Network Architecture

In this section, we discuss the architecture of S2S-WiDCN. We describe the design methodologies, the adopted antenna technology, and finally its communication protocols.

3.1.1 Wireless Data Center Network Topology

In S2S-WiDCN, the data center racks are laid out in the traditional rectangular pattern, adjacent to one another with aisles running between rows of racks. In order to avoid obstruction to the wireless communication links, wireless links are establish only along horizontal lines and vertical planes to communicate between any two servers in the three-dimensional space as shown in Fig. 3.1. To achieve this, each server will be equipped with two high gain 60 GHz antenna arrays. We propose attaching one of the antennas on the top of the server to enable the communication in the horizontal direction and other one on the back or front of the server projecting out from the rack as shown in Fig. 3.2 to enable communication in the vertical plane. To avoid interference and obstructions from the rack frames, communication in the horizontal planes are restricted only to a single line between horizontally aligned servers.

Data centers are typically arranged in hot aisle/cold aisle layout where servers in adjacent rows are either face-to-face or back-to-back [78]. To minimize the interference between two neighboring rows of racks, servers will have the provision to connect the antenna for vertical plane communication either on the back or on the front side. This will ensure that no two separate vertical planes will

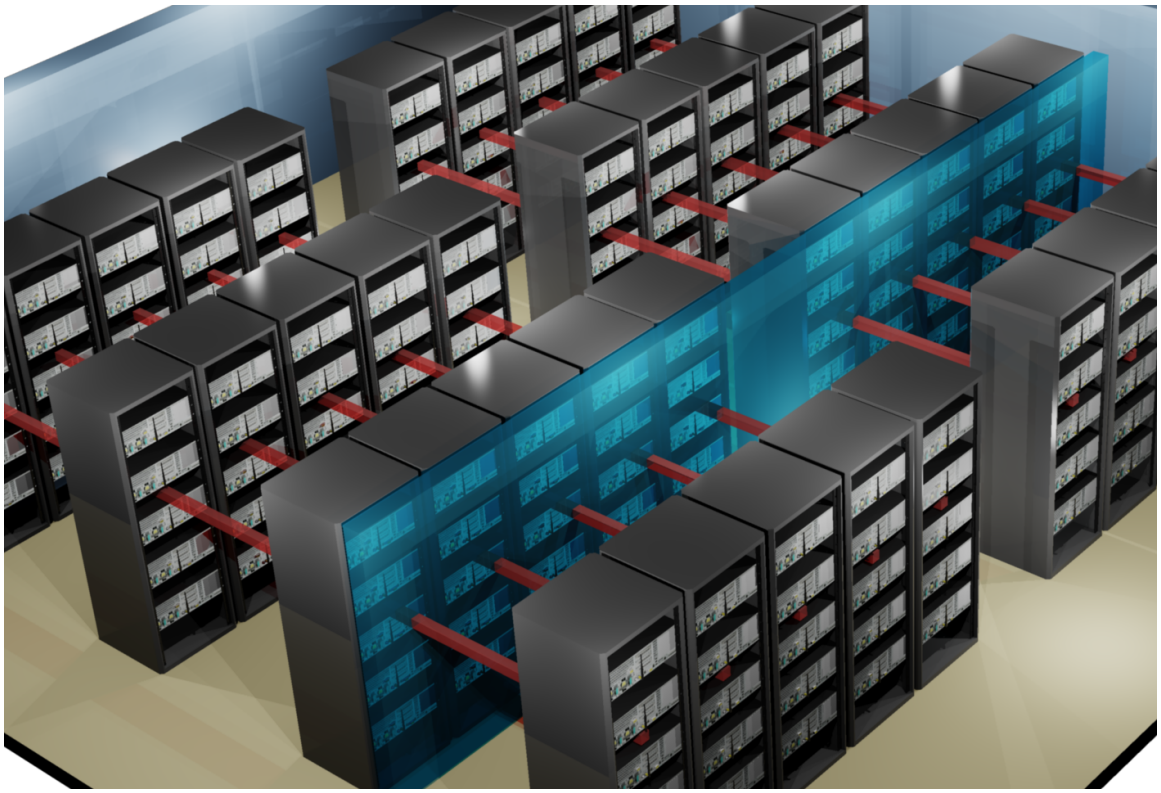


Figure 3.1: Server-to-server wireless data center network (S2S-WiDCN) showing some horizontal wireless paths (red) and one of the vertical wireless communication planes (blue).

exist in a single aisle and hence eliminate interference between vertical planes. Using the beam-steering capability of the antenna array, LoS links between communicating servers can be established with the help of a control interface discussed in Section 3.1.2. Each server is assigned a unique ID according to its geometric location in order to help determine the beam-steering angles. The angles are pre-computed depending on the location of the communicating servers. All the metallic surfaces and walls of the data center should be coated with anti-reflecting material cover [79] to eliminate the multi-path propagation of a signal. Such anti-reflection material with low reflection coefficients are relatively easily available and only add another additional layer to the building infrastructure without significant change in building design.

The proposed design can be adapted for racks having doors with few minor modifications. Traditional door for data center racks comes in two varieties- perforated metal sheet with breathable mesh design or acrylic glass with metal frame. For the perforated metal doors, we propose a series of rectangular opening areas as shown in Fig. 3.3(a), aligned with the top antenna in all the racks. This will ensure horizontal LoS between top antennas of the servers. The metal doors are perforated to aid in cooling air circulation, and the rectangular openings foster air conditioning fur-

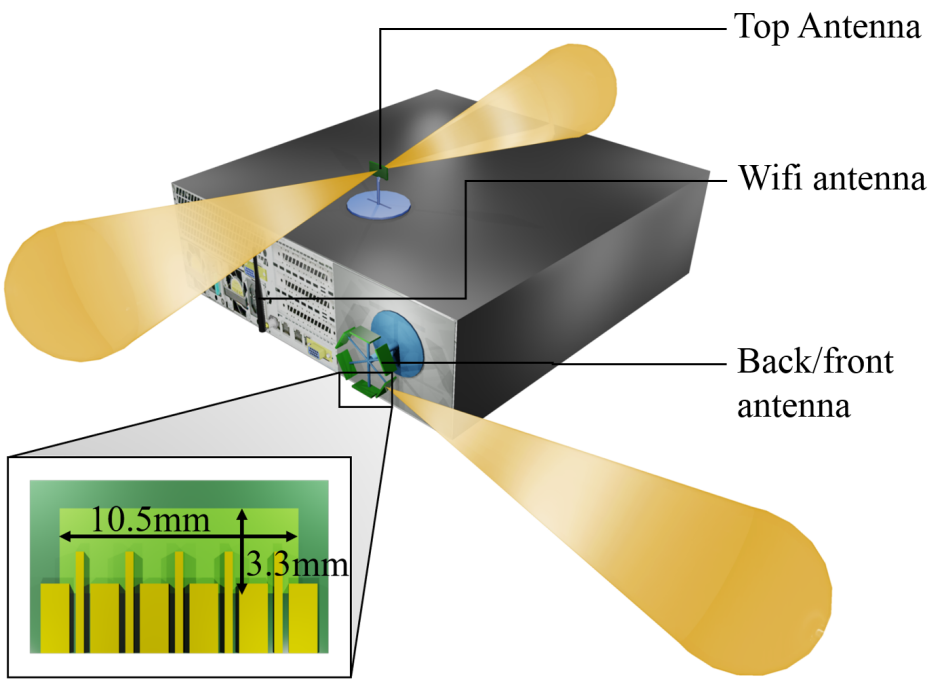


Figure 3.2: Single server showing two antenna arrays and the WiFi control module. Inset: each antenna array

ther. By contrast, for the doors with acrylic glass, the doors are designed to contain the chilled air implementing air conditioning which is different compared to data centers with metal doors. This material is relatively transparent to 60 GHz wireless band (compared to actual glass) with only 1.02 dB/cm of path loss through it [80]. While each door's glass is thinner than 1cm, in case of paths through many doors, the link-budget analysis should take into account this loss while designing the wireless data center with this type of door. Therefore, in case, the number of rows in the data center is high, this type of rack is not recommended for the S2S-WiDCN architecture. Furthermore, to use racks with glass door, the top antennas can be mounted on the side panel of the racks with a high quality, low loss 60GHz cable or wave guide rather than on top of the servers. To create LoS between the servers in different racks across multiple rows, a narrow open space is required between adjacent racks in the same row to accommodate the horizontal LoS lines through the sides of the racks. To prevent hot and cold air contamination, thermal ducts individually deployed in each rack as envisioned in [81], must be used in such racks to remove the hot air completely from the floor through the racks.

To create LoS in the vertical plane in presence of doors in the rack, we propose mounting the antenna arrays on an extended panel as shown in Fig. 3.3(a) and (b) for metal and acrylic door respectively. The antennas will be connected to the corresponding servers with high-quality, low-loss

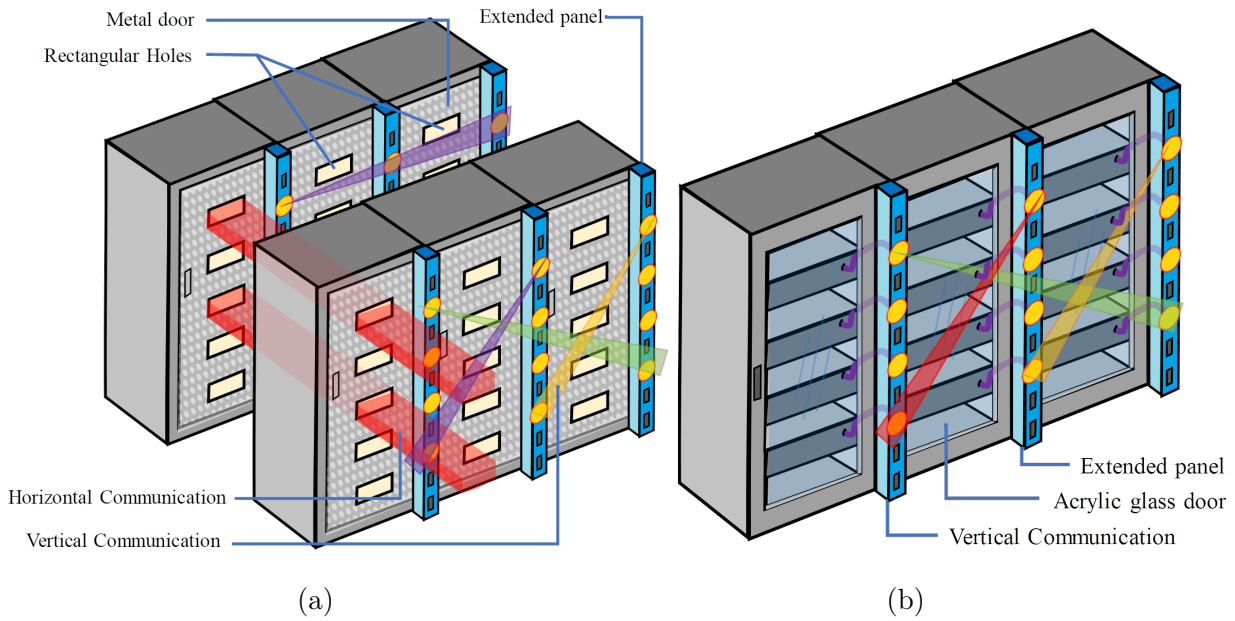


Figure 3.3: Creating LoS between servers in presence of (a) metal rack doors in horizontal and vertical planes and (b) acrylic glass door in vertical plane.

60GHz cable or wave-guide fitted to the frame which can be coupled to the servers. This will ensure that movements of the doors will not affect the antenna alignment.

3.1.2 Antenna Technology for the Wireless Data Center

Each server in S2S-WiDCN is equipped with a wireless module consisting of a transceiver and two accompanying antenna arrays [13]. This particular array is fabricated using semiconductor lithography techniques on a single wafer and hence, is extremely compact with a size of only $10.5mm \times 3.3mm$. As the radiation pattern suggests, the array provides high directional gain of $9dBi$ in the forward and backward directions. Moreover, by adjusting the relative phase of the antenna elements by activating various feed paths, beam-steering can be accomplished over an angle of 60°. As horizontal communication happens in a single straight line, no beam-steering is required in the antenna arrays on top of the servers. However, as the range of beam steering angle is 60° for this particular array, 6 antenna arrays are required to cover the entire 360° panorama in the vertical plane. Only one out of the 6 arrays will need to be signaled at any given point of time to establish a single link involving that server. Electronic beam-steering for the antenna array has negligible latency compared to mechanically steered horn antennas used in earlier wireless DCNs [20, 33]. Moreover, the antenna array being extremely compact requires very tiny space on top of each server to enable LoS communication in the horizontal direction. The effect of these spaces on the vertical server

density in the data center racks is discussed and quantified in the next section.

This beam-steering of the transmitting and receiving antennas is controlled by using a separate control interface using `IEEE 802.11` 2.4/5 GHz ISM bands. Although the data rates sustained by the IEEE 802.11 2.4/5 GHz bands are much lower than the 60GHz bands, it is sufficient for the short control packets. Moreover, the isotropic antennas in the `IEEE 802.11` 2.4/5 GHz modules do not require any antenna steering before the control messages can be transmitted. When a traffic flow between a pair of servers is created, a short control or header packet for the flow will be sent over the `IEEE 802.11` 2.4/5 GHz ISM band to enable communicating servers to steer their antenna beams towards each other when required. The details of the steering are discussed in 3.1.4.

3.1.3 Wireless Communication Protocols

Establishing connections between servers require reliable wireless 60GHz physical and Medium Access Control (MAC) layer protocols. The `IEEE802.11ad` standard [6] is designed for 60GHz wireless LANs. This standard defines a physical layer protocol that supports beam-forming, and also supports extremely high data rates in both a single carrier (SC) and Orthogonal Frequency Division Multiplexing (OFDM) mode of operation with maximum achievable data rates are 4.62Gbps and 6.76Gbps respectively. Motivated by these high data rates, `IEEE802.11ad` is adopted as the 60GHz physical layer protocol for wireless data centers. `IEEE802.11ad` MAC layer protocol incorporates a Carrier Sense Multiple Access (CSMA) mechanism for on-demand establishment of wireless links depending upon the traffic flow requirements. The MAC layer protocol establishes as many non-interfering links as possible, greedily on a first-come first-serve basis until all traffic flow demands are met or all the available OFDM channels are exhausted. The `IEEE802.11ad` standard only allows wireless links to be established where a bit error rate (BER) of 3×10^{-7} or lower can be achieved considering the signal to interference plus noise ratio (SINR) and the corresponding data rates to be sustained by the wireless link. Once a flow is found not to be feasible due to interference with already-existing flows in any of the OFDM channels, the flow is no longer considered serviced and that demand is left incomplete. The performance of the MAC layer protocol is evaluated through a comparison and analysis against similar-sized wired networks in our case studies in the next section. TCP/IP is used as the transport layer protocol for reliable packet delivery for its widespread use and well-known characteristics in data center networks as well as in the Internet.

The feasibility of 60GHz communication in data centers is established with physical channel measurements in [12, 32]. However, the effect of temperature on the 60GHz channel has not been considered. The 60GHz channel is known to be affected by molecular absorption, which in turn, is

affected by the temperature. Due to variation in temperature in a data center between hot and cold airflows, the wireless path loss may vary. However, the recommended range of temperature variation in a data center according to ASHRAE thermal guideline is between 18° to 27° Celsius [82]. The path loss varies by roughly $2dB/km$ for this range of temperature [83]. Therefore, for typical data center dimensions in the range of few meters, the variation is negligible.

3.1.4 Routing Protocol for S2S-WiDCN

In this section, the normal routing protocol, as well as an adaptive routing protocol for S2S-WiDCN, which is capable of routing traffic flows even in the presence of obstruction of the LoS between two servers due to reasons such as the presence of human beings along the data center aisles. First, we describe the default routing mechanism followed by our proposed method to make the default routing adaptive for robustness against obstruction of LoS.

Default Routing Mechanism

For the default routing mechanism, we develop a Horizontal-First routing described in this subsection. The server arrangement plays a vital role in the design of this routing protocol. For the purpose of the Horizontal-First routing algorithm, the servers are considered to be arranged in a 3D Cartesian coordinate system with each server having a unique 3D coordinate as shown in Fig. 3.4. In this coordinate system, X-axis runs along rows, Y-axis runs along columns and Z-axis runs along with racks as shown in Fig. 3.4 (a). Server-to-server communication in a data center can be broadly classified into two types, i.e., inter-rack and intra-rack communication based on the location of the source and destination servers. All the intra-rack communications are completed in one hop in the vertical plane as shown in Fig. 3.4(a) whereas inter-rack communication depends on the relative position of the source and destination servers. There are three possible scenarios for inter-rack communication:

- Both the source and destination servers are located in the same vertical plane (the same row or the same Y coordinate) as shown in Fig. 3.4(b). In this case, a direct single hop link will be established between the source and destination for data transfer.
- Both the source and destination servers are in the same column with same height above the ground (the same X and the same Z coordinates, but different Y coordinates). In this case,

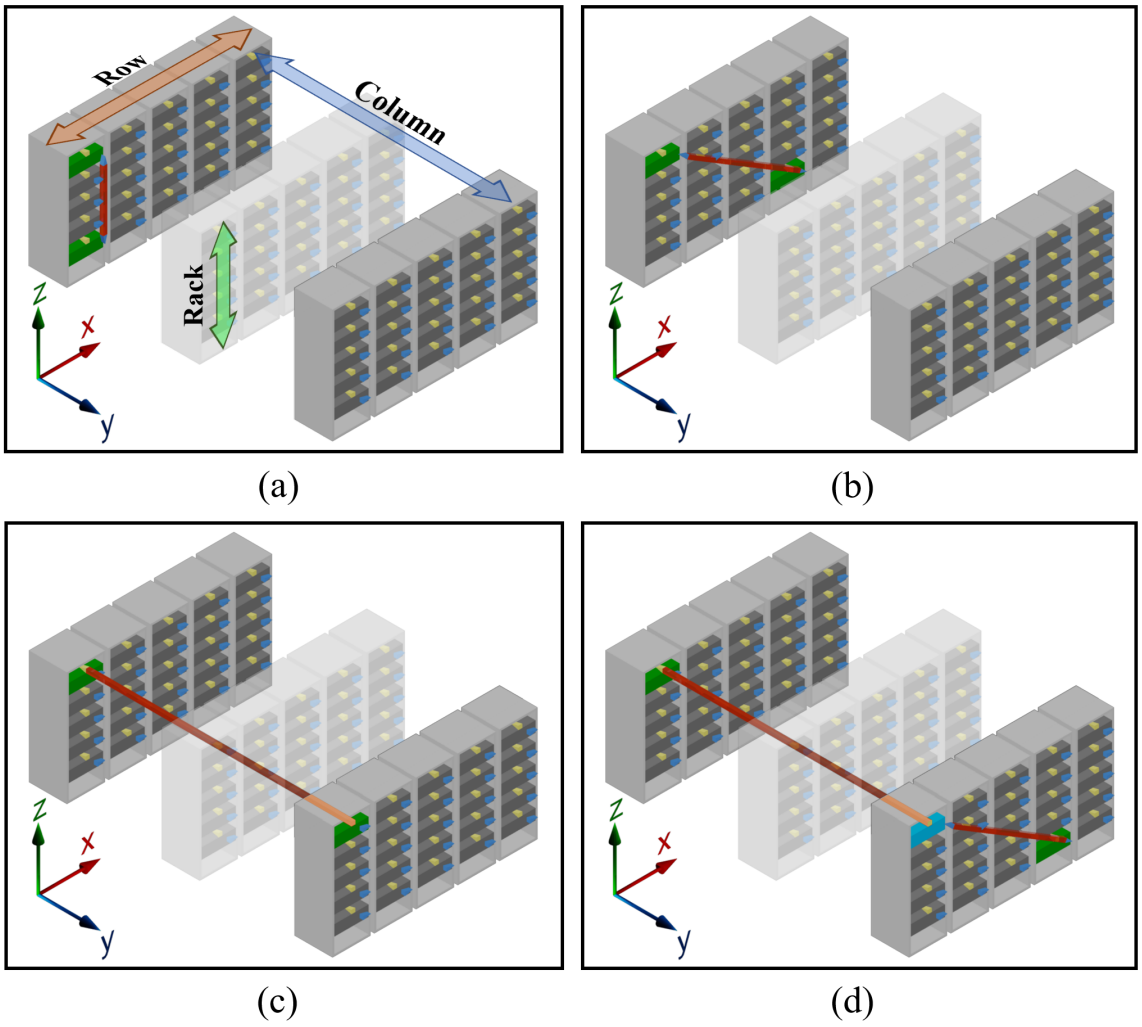


Figure 3.4: Possible communication paths between servers situated in (a) same rack, (b) same vertical plane, (c) same horizontal line, and (d) different horizontal lines and vertical planes.

a single hop direct link along a horizontal line will be established between the source and destination for communication as shown in Fig. 3.4(c).

- The source and destination servers are in different row and column (different X and Y co-ordinates, may or may not have the same Z coordinate). In this case a 2-hop link will be established for communication using an intermediate server as shown in Fig. 3.4(d). The intermediate server is the one that is in the same column and height from the source server, but in the row of the final destination (the same X and Z coordinates as that of the source and the same Y coordinate as the destination). As the data travels along the horizontal line first, the adopted routing protocol is referred to as Horizontal-First routing. In the proposed topology, every server is capable of working as a potential intermediate node.

Algorithm 3.1 Default Routing Mechanism: Horizontal-First Routing

```
1: if source and destination servers are in same rack then
2:     communication is done in 1 hop in vertical plane
3: else if source and destination servers are in same vertical plane and different rack then
4:     communication is done in 1 hop in vertical plane
5: else if servers are in different row but same column and same Height then
6:     communication is done in 1 hop in horizontal line
7: else
8:     select the server in destination row at same height and column as of source server as the intermediate node
9:     route the flow in 2 hop using Horizontal First routing
10: end if
```

The pseudocode of the Horizontal-First routing strategy for these various conditions is shown in Algorithm 3.1. Control information in the form of a control packet with instructions for intermediate and destination servers to steer their antennas in the correct directions is sent over a separate `IEEE 802.11` 2.4/5 GHz ISM band. Each server is equipped with an `IEEE 802.11` 2.4/5 GHz transceiver. As the radiation pattern has main lobes in both forward and backward directions, steering is not required for the horizontal linear communication a shown in Fig. 3.2. For communications in the vertical planes, the server, which is ready to send data, first sends a control packet to the receiving server while simultaneously steering its antenna array towards the receiver. Upon receipt of this control message, wireless module at the receiver chooses the antenna array in the correct sector out of the set of 6 and steers that array towards the sending server by activating the correct phase differences (paths connecting the elements). The `IEEE 802.11` 2.4/5 GHz ISM band is also used for sending the acknowledgments to enable the CSMA-based MAC for the 60GHz links using the `IEEE802.11ad` protocols. In order to provide access to the Internet with necessary bandwidth, we envision gateway functionalities to be hosted at multiple server locations within the rectangular arrangement in the wireless DCN. These gateways will, therefore, be connected directly or indirectly, to all the servers and will also need to run firewall and security functionalities as per the requirement of the data center.

Obstruction-Avoidance Routing Mechanism

In some scenarios, the LoS necessary for the Horizontal-First routing can be obstructed. For example, when a human technician or any other obstacle is in front of an aisle it can potentially obstruct the horizontal server-to-server LoS communication between all servers in the aligned racks as shown in Fig. 3.5. This will not only affect servers of the rows directly adjacent to the human obstruction but also servers in racks of all rows that use those horizontal paths for inter-row communication.

Algorithm 3.2 Adaptive Routing: Obstruction-Avoidance Routing

1: **if** *Obstruction detected* in the *Horizontal line* ← FALSE **then**
2: Default *Horizontal-First* Routing
3: **else**
4: **if** servers are in *different row* **and** *same column* **then**
5: **choose** a random server in source plane in a *different rack* as 1^{st} intermediate node
6: select the corresponding server in destination plane (*same height* **and** *same column* as of 1st intermediate node) as the 2^{nd} intermediate node
7: **if** *Obstruction detected* in the *Horizontal line* ← TRUE **then**
8: **go to:** 5
9: **else**
10: route the flow in **3 hop** using *Vertical-First* routing
11: **end if**
12: **end if**
13: **if** servers are in *different row* **and** *different column* **then**
14: **choose** the server in the source plane situated in the *same height* **and** *same column* of the destination server as intermediate node then
15: **if** *Obstruction detected* in the *Horizontal line* ← TRUE **then**
16: **go to:** 14
17: **else**
18: route the flow in **2 hop** using *Vertical-First* Routing
19: **end if**
20: **end if**
21: **end if**

We propose an Obstruction-Avoidance adaptive routing mechanism to address this failure model and to successfully route traffic flows in the presence of such obstructions between specific racks. In the adaptive routing, all servers start sending packets following the default Horizontal-First routing strategy outlined earlier. CSMA acknowledgment mechanism is utilized the to detect a failed transmission after several trials according to the `IEEE802.11ad` MAC. Then a re-transmission is attempted again using the adaptive routing algorithm as described in Algorithm 3.2.

In this adaptive routing strategy, after detecting a failed transmission, the sender determines the route of the next transmission attempt. If the destination server is in another rack in the same row, the sender retransmits the flow using the default Horizontal-First routing algorithm. This is because the failed transmission did not happen because of the horizontal LoS obstruction from the technician as that LoS link was not used in the first transmission attempt. The transmission happens over the back/front vertical plane, which is not obstructed by the failure model under consideration. However, if the destination is in another row, instead of adopting the Horizontal-First approach, a Vertical-First routing approach is adopted where, a server in the same row but a different rack

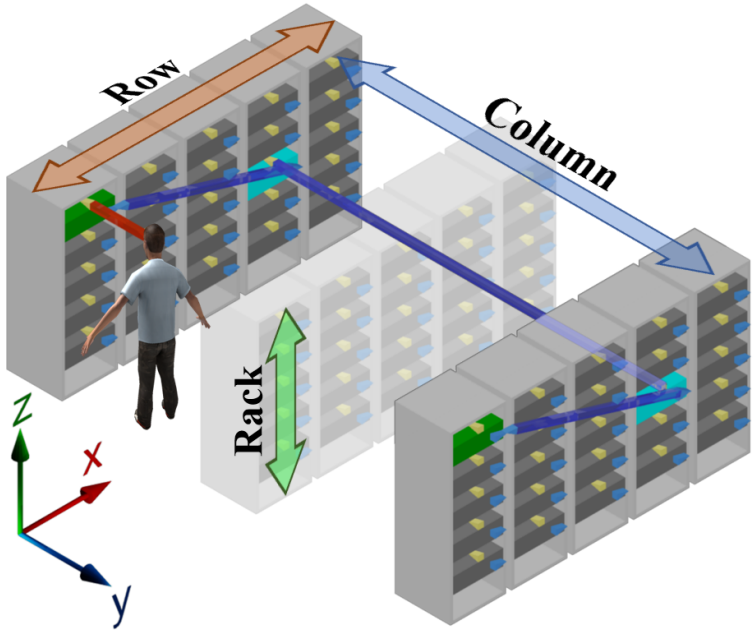


Figure 3.5: Possible communication paths between servers while obstruction is detected.

is chosen at random and the path is established to that server using the back/front vertical plane. Control packets are sent over the `IEEE 802.11` 2.4/5GHz ISM control plane to establish the links using beam-steering. From that other server, again the default Horizontal-First routing is adopted to reach the final destination. Such a path is shown in Fig. 3.5. If the randomly chosen intermediate server for Obstruction-Avoidance routing is also obstructed by another technician, the Obstruction-Avoidance routing approach can be repeated again till the Horizontal-First routing is successful to transfer packets to the destination row. In this way, this adaptive routing mechanism can be extended to an obstruction model with multiple technicians obstructing multiple racks in the data center. The performance of S2S-WiDCN in presence of such an obstruction will be degraded for the obstructed flows. In the next section, we describe the performance of S2S-WiDCN in presence of various flow traffic patterns and obstructions.

3.2 Modeling, Results, and Analysis

In this section, we present our modeling, results and the corresponding analysis of S2S-WiDCN. We first demonstrate that it can sustain comparable performance compared to that of conventional DCNs with network-level simulations in terms of communications between servers within a data center. Next, we present the estimates of power consumption to highlight the main benefit of S2S-WiDCN.

3.2.1 Simulation Platform

The Network Simulator-3 (NS-3) suite [84] was used to evaluate S2S-WiDCN. NS-3 supports the characteristics of wireless propagation as well as network-level communications. It is important to simulate both the propagation and network-level communication characteristics accurately in order to obtain credible performance results. A modified version of NS-3 extended with features of the wireless data center including the 60GHz band and the `IEEE802.11ad` standard as discussed in [12] was used. This extension incorporates interference modeling, bit error rates, and directional antenna modeling. The accuracy of these parameters is verified with physical layer measurements of prototype 60GHz hardware [12]. Additionally, we introduce criteria for wireless link selection to enable many concurrent links, and modify the `IEEE802.11ad` physical layer to allow multiple OFDM channels.

We have considered two data center sizes for this analysis to represent data centers belonging to two different classes. The first one, with a total of 800 servers, is a small-sized data center representing those in an educational institution. The second one is a mid-sized data center and has 1600 servers representing those in private enterprises [85, 86]. In both cases, the servers are arranged in a 20×8 array of racks as shown in Fig. 3.6. There are 10 racks arranged in a single row and two columns of 8 rows, totaling 160 racks. Each rack occupies an area of $0.6m \times 0.9m$ and is $2m$ high. Adjacent rows are separated by $1m$ and the width of the central aisle is $2m$. Each rack contains 5 and 10 servers for the 800 and 1600 server data centers respectively. In our simulations, the racks are assumed to be without any front or back side door.

To account for the latency required to set up the 60GHz communication links using the exchange of control information over the `IEEE 802.11` 2.4/5 GHz ISM band and beam-steering, we run a conservative simulation using NS-3 with the packet size of 200 bytes representing control packets of 60GHz S2S-WiDCN data center with beam-steering information. Each new flow according to the flow arrival process discussed in section 3.2.2 in the DCN is considered to generate a control packet. The flow arrival process is considered to be the same as described in Section 3.2.2. The simulation showed that a single wireless access-point can sustain the demand for the control packet traffic with an average latency of $266\mu s$ in a system with 240 servers. As the maximum number of servers in a single vertical plane is 200, a single access point per row should be enough to server the requirement. This latency overhead is considered in the evaluation of S2S-WiDCN next.

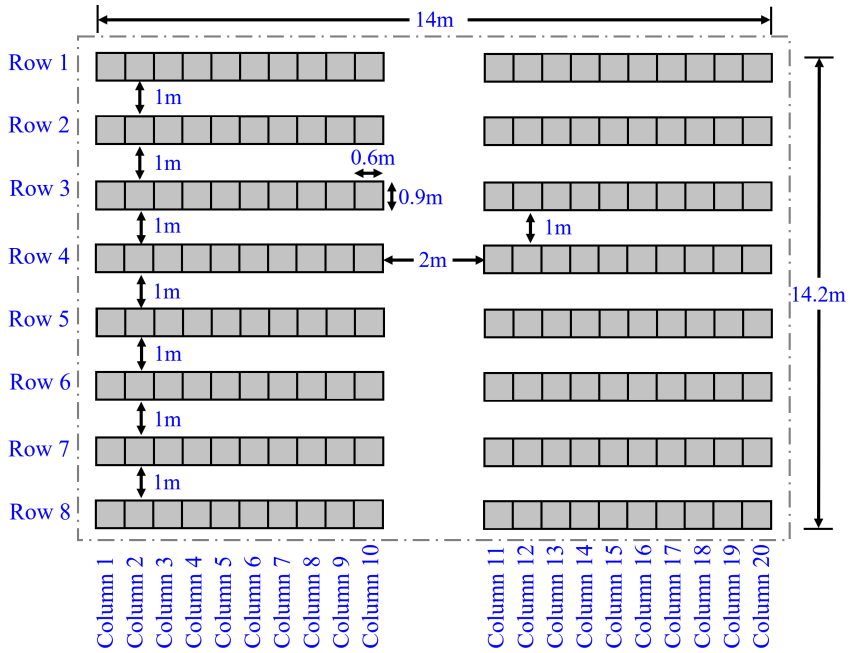


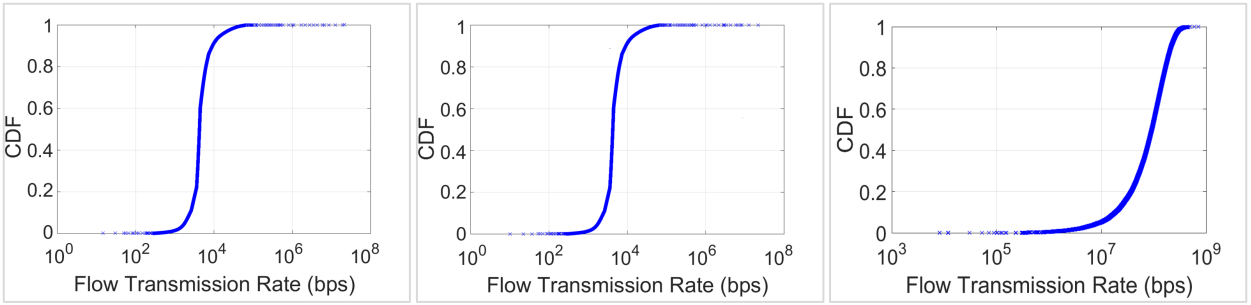
Figure 3.6: Data center layout floor plan.

3.2.2 Performance Evaluation and Analysis

Here we present the simulation results of S2S-WiDCN along with a comparative analysis with respect to existing DCNs in terms of flow completion duration and throughput. The throughput is defined as the average rate of bit transferred per second over the DCN. We compare S2S-WiDCN with a traditional wired fat-tree based DCN and a ToR-ToR wireless DCN. In the traditional wired fat-tree based DCN, we have considered 3 hierarchical layers consisting of 160 access, 2 aggregate and 2 core layer switches similar to the architecture evaluated in [31]. Each traditional DCN link between the access, aggregate and core level switches is considered to have a channel bandwidth of 10 Gbps. The intra-rack communication in the fat-tree based DCN occurs through the ToR switch, which has 1.0 Gbps direct links to each server in its rack. Although the proposed wireless DCN is a direct server-to-server network, we have not compared it with a wired server-to-server all-to-all DCN because such a network is not practical and will have extremely high degree of connectivity at each server. In the ToR-to-ToR wireless DCN (ToR-WiDCN) the intra-rack communication is managed in a traditional manner, same as in the conventional wired DCN. The inter-rack communication is done with ToR-to-ToR 60GHz wireless links using the same physical and MAC layers as in S2S-WiDCN. We use the simulation platform described in Section 3.2.1 and the data center traffic model discussed below to evaluate these DCNs.

Data Center Traffic Model

S2S-WiDCN is at first evaluated with a set of traffic flows based on application demands. These demands reflect real traffic within the network over a period of time. The application demands include information specifying the flow arrival time, identity of the source and destination, the flow size, and the data rate at which the traffic is generated. Real data center traffic for different classes of data centers such as educational (small), private (medium) and corporate (large) running typical query/response based applications like map-reduce and index-search are measured in [85]. Using these measured traffic flows, a Poisson shot-noise based model to synthesize data center traffic is proposed and verified in [86]. According to [86], the new flow arrival time, the flow duration and the injection rate for each application follow a Poisson, Pareto and, Gaussian distribution respectively. The new flow arrival time is generated using a Poisson distribution with an average flow arrival rate. The average flow arrival rate is considered to be 1000 flows/second for the small-sized and 3000 flows/second for the mid-sized data center [85]. The flow injection rate and the flow duration are independent parameters. The flow duration refers to the time required to inject the flow into the DCN and is different from the flow completion duration which is a performance metric. The flow size is a product of the injection rate and duration and therefore depends on both. In our evaluations, we have considered a skewed Gaussian distribution for the injection rate to have a mean of 1.0kBps such that 90% of the traffic rates are less than 10kBps and the remaining 10% can be as high as several MBps as per the traffic model from [86]. Application flow duration is generated following an independent Pareto distribution having a minimum duration of 10 microseconds [85]. The characteristic parameters for these distributions are summarized in Table 3.1. As customary for TCP traffic, we have considered the size of all packets in the generated flows equal to the maximum transmission unit (1500 bytes). The CDFs of the transmission rates of both of these two traffics are shown in Fig. 3.7 (a) and Fig. 3.7 (b).



(a) (b) (c)

Figure 3.7: CDF of flow transmission rates of the (a) index/query based traffic for small size (b) index/query based traffic for medium size (c) multimedia traffic for small size DCN.

Table 3.1: Parameters for index/query based traffic generation

Name	**Model**	**Parameters**
Flow arrival time, N	Poisson	$\lambda(t)$= 1000, for small DCN $\lambda(t)$= 3000, for medium DCN
Flow duration, D_n	Pareto	a_p= 1.504s M_p=1.0001s
Flow transmission rate, Y_n	Gaussian	E[Y_n] = 8.606 Kbps σ[Y_n] = 69.936 Kbps
Flow size, S_n	$Y_n.D_n$	E[S_n]= 1.0647KB

According to [85, 86], in a DCN, around 80% of the total traffic stays within the same rack. Only 20% communication takes place between the servers situated in different racks. For each new flow in our simulations, a random destination was chosen such that 80% of the destinations belonged to the same rack as the flow source. The simulations were conducted such that no new flows were allowed to be injected after 20 seconds but the simulations were run until the completion of all the established flows. Next, we analyze the performance of the DCNs in the presence of this traffic pattern.

Flow Completion Duration

Here, we estimate the flow completion duration of the applications in the different DCNs. The flow completion duration for both small and medium sizes of all 3 different DCNs are shown in Fig. 3.8. It can be seen that the average completion duration of S2S-WiDCN is lower than that of the wired network for both sizes because of the fewer number of hops involved, resulting in lower time of flight and switching overheads. For the wired network, two servers even in a single rack need to go through the access layer switch to communicate, requiring at least two hops. On the other hand, in the wireless architecture, those two servers can communicate directly using a single hop. As the major portion of communications in data centers is intra-rack [85], the reduction in delay of intra-rack flows in the wireless DCN is likely to reduce the overall average flow completion duration. The beam-steering latency is $266\mu s$ for exchange of control information over the control plane is considered while computing the flow completion duration of S2S-WiDCN as shown in Fig. 3.8.

Fig. 3.8. also captures the minimum and maximum flow completion durations for all the DCNs. The minimum flow completion duration in case of S2S-WiDCN is higher than that of the fat-tree based DCN due to the beam-steering latency. This effect is also seen in the ToR-WiDCN. However,

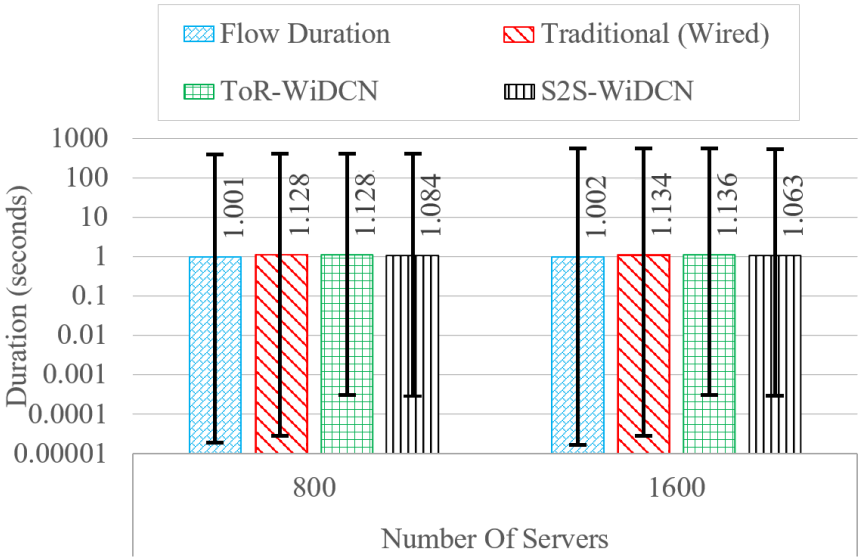


Figure 3.8: Average flow completion duration for index/query based traffic.

as seen in [85] only a very small fraction of the flows have such short flow duration.

Throughput

Fig. 3.9 shows the average throughput along with the minimum and maximum for all flows in each DCN. As we can see for both sizes S2S-WiDCN provides the same throughput as that of the wired traditional fat-tree based DCN. Even the ToR-WiDCN is capable of achieving a similar performance. All the DCNs achieve throughput which closely match the injection rate of the flows. This is because, in the traditional wired network, the available bandwidth per link is 1.0Gbps and that available for OFDM wireless channels is 0.563Gbps. We have considered 3 sub-carriers in the 60GHz band each with maximum OFDM rates of 6.76Gbps, which are in turn, split into 12 sub-channels each, to cater to all the application flows injected into the wireless DCNs. So, the physical bandwidths of both wired and wireless channels are much higher than the average injection rates encountered in these scenarios. Moreover, we find that in S2S-WiDCN the throughput is higher than that in both the traditional wired DCN and ToR-WiDCN. This is because the lower number of hops in S2S-WiDCN implies that the flow will encounter fewer intermediate nodes resulting in a reduced likelihood of being congested. Therefore, for the type of application considered here, S2S-WiDCN performs better than the fat-tree based DCN. Although the flow arrival rate increases with the number of servers, its impact on performance is marginal as the flow transmission rates of most of the flows are less than the 60GHz OFDM channel capacity.

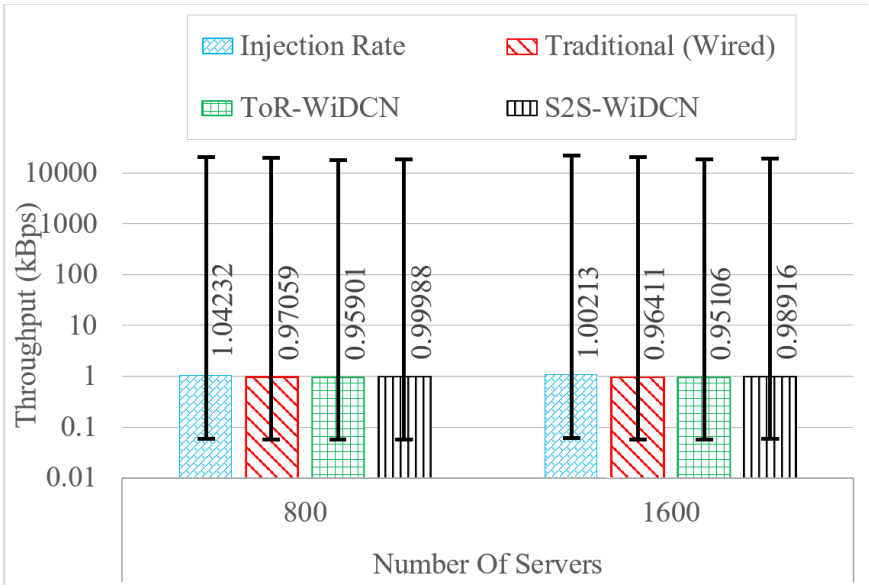


Figure 3.9: Average throughput of different data center networks for index/query based traffic.

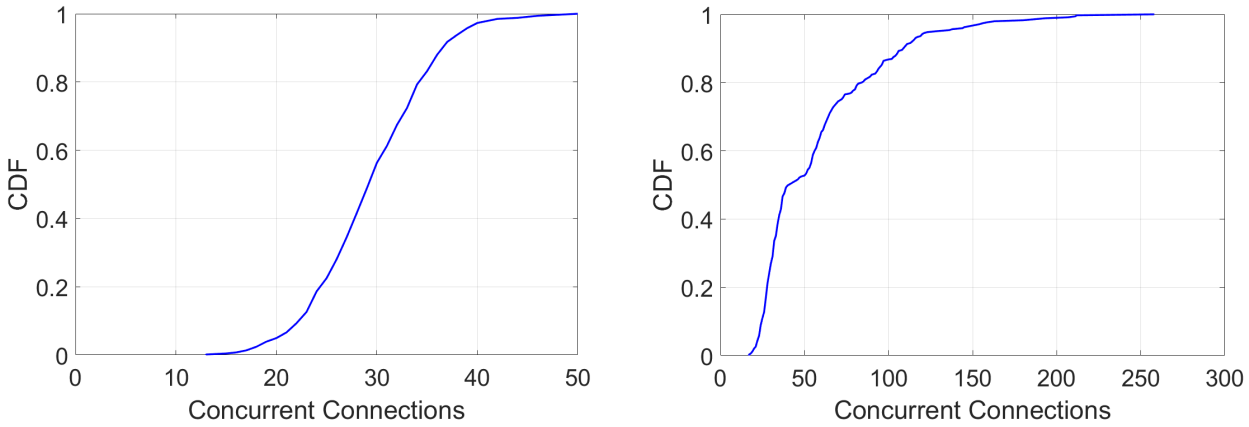
Evaluation with Different Traffic Patterns

In this subsection, we further evaluate S2S-WiDCN with a different traffic scenario that can be encountered in multimedia or video hosting/streaming servers. This kind of application is significantly different from query/index search applications primarily from two perspectives. First, this kind of traffic generally has a higher data rate requirement. Multimedia/video streaming servers hosting applications are seen to have average data rates of 100Mbps [87]. Second, these applications typically experience bursty flow arrivals [88]. In order to evaluate S2S-WiDCN with multimedia/video, traffic we adopt a bursty flow arrival rate with a high average data rate of 100Mbps based on [87]. Unlike the query-based traffic where the flow arrival process is assumed to be a Poisson process, the bursty flow arrival is modeled as a fractal process. The entire simulation duration is divided into windows of 30ms and each window is randomly chosen to be either in ON or OFF phase. New flow arrivals are allowed only in the ON phase. The new flows have an arrival rate such that the overall average flow arrival rate is the same as that of the query-based traffic for the simulation duration. The details of this traffic are listed in Table 3.2. The CDF of number of concurrent flow arrivals within a window size of 30ms for both the query-based traffic and the bursty multi-media traffic is shown in Fig. 3.10. It can be seen that in the Poisson arrival process typical in query/response applications, the number of concurrent flows is never higher than 50 whereas, it can be as high as 250 in the bursty flow arrival pattern. The bursty traffic pattern coupled with the high flow rate requirements of this traffic type is, therefore, expected to stress the DCN more compared to the query/response type traffic.

Table 3.2: Parameters for video/multimedia traffic generation

Name	**Model**	**Parameters**
Flow arrival time, N	Poisson	$\lambda(t)$= 1000
Flow duration, D_n	Pareto	a_p= 1.504s M_p=1.0001s
Flow transmission rate, Y_n	Gaussian	E[Y_n] = 100.0 Mbps σ[Y_n] = 114.153Mbps
Flow size, S_n	$Y_n.D_n$	E[S_n]= 101.025MB

Fig. 3.11 shows the average flow completion duration and average throughput of a small sized DCN with 800 servers for this multimedia/video traffic. We have compared the performance of S2S-WiDCN with a fat-tree based wired DCN with this traffic. Similar to query-based traffic, a few small flows with very low flow durations incur a higher flow completion duration in S2S-WiDCN as can be seen in the minimum of the flow duration range in Fig. 3.11 (a). This is because the beam-steering latency of S2S-WiDCN is higher than the flow duration of these very small flows. Moreover, we can see that some of the high data rate flows achieve lower throughputs in S2S-WiDCN compared to the fat-tree wired DCN as shown by the maximum value of the range of throughput of S2S-WiDCN in Fig. 3.11 (b). This is because the maximum data rate per OFDM channel that can be supported in S2S-WiDCN is 0.563Gbps. As the flow rates follow a Gaussian distribution with a mean of 100Mbps, a few flows require a data rate higher than 0.563Gbps. The effective throughputs of these flows are reduced in S2S-WiDCN. However, as can be seen from the CDF of flow rates in fig. 3.7 (c), these flows with data rates higher than 0.563Gbps are few in number and therefore do not affect the average throughput significantly.



(a) (b)

Figure 3.10: Distribution of number of concurrent connections for (a) query-based traffic (b) bursty multimedia traffic.

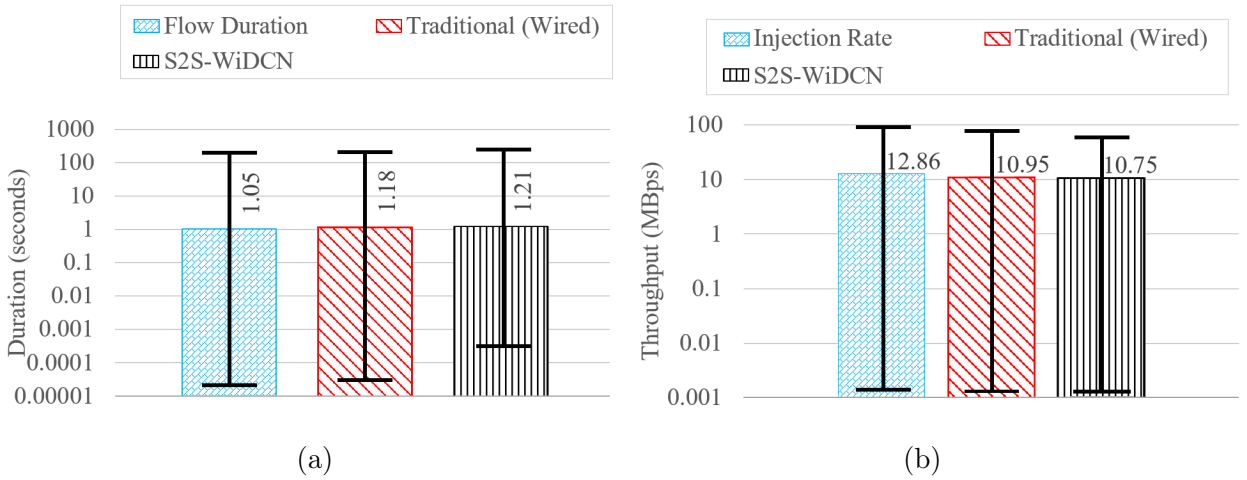


Figure 3.11: (a) Average flow completion duration and (b) average throughput of a small sized DCN with 800 servers for this multimedia/video traffic for different data center networks.

Evaluation in the Presence of LoS Obstruction

In this subsection, we evaluate the performance of S2S-WiDCN in the presence of a LoS obstruction. For this purpose, a scenario is assumed where an IT technician is present in front of the column 3 of row 2 in the floorplan shown in Fig. 3.6. We have assumed this obstruction to be stationary within the observed window of 20 seconds, which is reasonable as it is a human obstruction. Due to the presence of the obstruction, the traffic flows from all servers in all rows corresponding to the obstructed column, which were supposed to be routed through the horizontal lines in column 3 with the default Horizontal-First routing protocol, need to follow the alternate Obstruction-Avoidance routing mechanism. Fig. 3.12 shows the flow completion duration of the small-scale S2S-WiDCN with 800 servers with adaptive routing, in the presence of the obstruction. We have evaluated the impact of the obstruction on the overall flow completion duration as well as that of the affected traffic flows only. As 80% of the traffic generated from each server is intra-rack, they use the vertical plane for communication and are unaffected by the presence of a technician. Among the 20% inter-rack traffic, a smaller percentage requires inter-row paths going in the horizontal direction as inter-rack traffic in the same row also uses the vertical plane. The percentage of traffic flows from all rows, whose inter-row traffic is obstructed, is 1.87% of all the flows in S2S-WiDCN. Hence, the LoS obstruction has very little impact on the overall average flow completion duration due to the small percentage of traffic flows that are affected. We have further investigated the impact of the obstruction as a function of the number of re-transmission trials made before rerouting using the Vertical-First path of the adaptive routing method. As can be seen, in case of a higher number of allowed re-transmission attempts before rerouting the flow, the impact of the obstruction is higher. Hence, the number of re-transmission attempts can be customized based on the performance

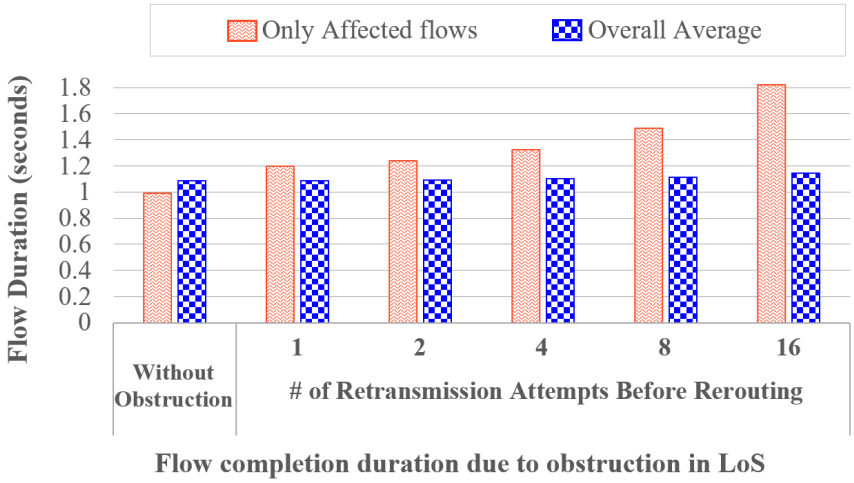


Figure 3.12: Comparison of average flow completion duration in presence of LoS obstruction.

demands of the applications.

3.2.3 Power Consumption Analysis

From the previous section it is seen that S2S-WiDCN can sustain comparable performance as that of a traditional fat-tree DCN. In this section we evaluate its most important benefit, which is the reduction in power consumption of S2S-WiDCN with respect to the traditional DCN. We discuss the model and parameters used in the power estimation followed by the results.

Power Model

It is a complex task to estimate the actual electrical power consumed by a data center. The power consumption depends on several internal factors such as utilization of computing power, the cooling mechanism, and data center networks. Data center power consumption is also affected by external parameters like geographical location, weather, temperature, and humidity. Our focus is solely on networking, and we only analyze the power consumption involved in networking. In this regard, we assume that the power consumption other than networking is identical in all the cases. We estimate power consumption for wired DCNs using commercially available data from Cisco network switches [89, 90, 91]. Specifically, we use Cisco 7702 for the core-level switches, Cisco 9508 at the aggregation level, and Cisco 9372 for access-level switches. We also use the data from Silicom PE2G2135 for the power consumption of the network interface cards (NIC) [92]. The power

Table 3.3: Power Consumption of Different Components

Device	**Model**	**Used in**	**Power(W)**
Access Layer Switch	Cisco 9372	Fat-Tree	210.0
Aggregate Layer Switch	Cisco 9508	Fat-Tree	2527.0
Core Layer Switch	Cisco 7702	Fat-Tree, S2S-WiDCN	837.0
Network Interface Card	Silicom PE2G2I35	Fat-Tree, S2S-WiDCN	2.64
60GHz Transceiver	Analog Device HMC 6300/6301	S2S-WiDCN	1.70
IEEE802.11 2.4/5 GHz ISM Adapter	D-link DWA-171	S2S-WiDCN	0.22

consumption of each core and aggregate switches are as follows:

$$P_{Core} = P_{I/OCards} + P_{FanTray} + P_{Sv}, \tag{3.1}$$

$$P_{Agg} = P_{I/OCards} + P_{FanTray} + P_{Sv} + P_{Fabric} + P_{SysCtrl}, \tag{3.2}$$

where, $P_{I/OCards}$, $P_{FanTray}$, P_{Sv}, P_{Fabric}, $P_{SysCtrl}$ represent the power consumption of the input/ output card, fanout ports, supervisor controller, cables and system controller respectively. Then the total network power is calculated as follows:

$$P_{Network} = N_{Core}P_{Core} + N_{Agg}P_{Agg} + N_{Acc}P_{Acc} + N_S P_{NIC}, \tag{3.3}$$

where, N_{Core}, N_{Agg}, N_{Acc}, N_S are the number of core, aggregation, access switches, and the total number of servers, respectively; P_{Core}, P_{Agg}, P_{Acc}, P_{NIC} are the power consumptions of an individual core, aggregation, access switches and network interface cards, respectively.

In S2S-WiDCN, however, no core, aggregate or access layer switches are needed, but only antennas, transceivers and NICs are required for wireless communication. The power consumption of the wireless 60GHz transceiver is modeled based upon the assessment of emerging 60GHz transceivers such as [9, 10]. The NICs of S2S-WiDCN are equipped with two transceivers for horizontal and vertical communication. In the traditional DCN, external connections are established via the two Cisco7702 switches. To provide equivalent connectivity in S2S-WiDCN, we employ two servers to work as gateways, and their power consumption is modeled as that of the Cisco 7702 switch. The power consumption of communication per server in S2S-WiDCN is calculated as:

$$P_{Wireless} = 7P_{60GHzTran} + P_{WifiControl} + P_{NIC}, \tag{3.4}$$

where, $P_{60GHzTran}$ is the power consumption of the 60GHz transceiver including the power transmitted through antenna, $P_{WifiControl}$ is the power consumption of the 802.11 2.4/5 GHz ISM adapter

Figure 3.13: Total power consumption of various DCN architectures.

for the control channel. We conservatively adopt $P_{60GHzTran}$ to be $1.7W$ [9, 10]. We consider $P_{WifiControl}$ to be $220mW$ from the datasheet of D-link DWA-171 2.4GHz ISM adapter. Finally, the total power consumption in S2S-WiDCN becomes:

$$P_{TotalWiDCN} = N_{Core}P_{Core} + N_S P_{Wireless} \tag{3.5}$$

The power consumption of all the off-the-shelf switching components used in our model is shown in Table 3.3.

Comparative Analysis of Power Consumption

We posit that the primary advantage of S2S-WiDCN is lower power consumption. To study this more deeply, the total power consumption estimated for the typical and maximum cases for all the DCNs is shown in Fig. 3.13. In the "typical" scenario, the average power consumption of every device is used, while their maximum power consumption is considered in the "maximum" scenario. For small-sized and mid-sized DCNs, the result shows eight-fold and five-fold reduction in power consumption of S2S-WiDCN compared to the traditional fat-tree based DCN topology in the "typical" case. The maximum improvement in power consumption is observed to be seventeen-fold for the small-sized DCN in the "maximum" utilization scenario. The complete elimination of power-hungry aggregate and access-layer switches contribute to this drastic reduction primarily. Since access-level switches are needed per rack in the ToR-WiDCN, its reduction in power consumption

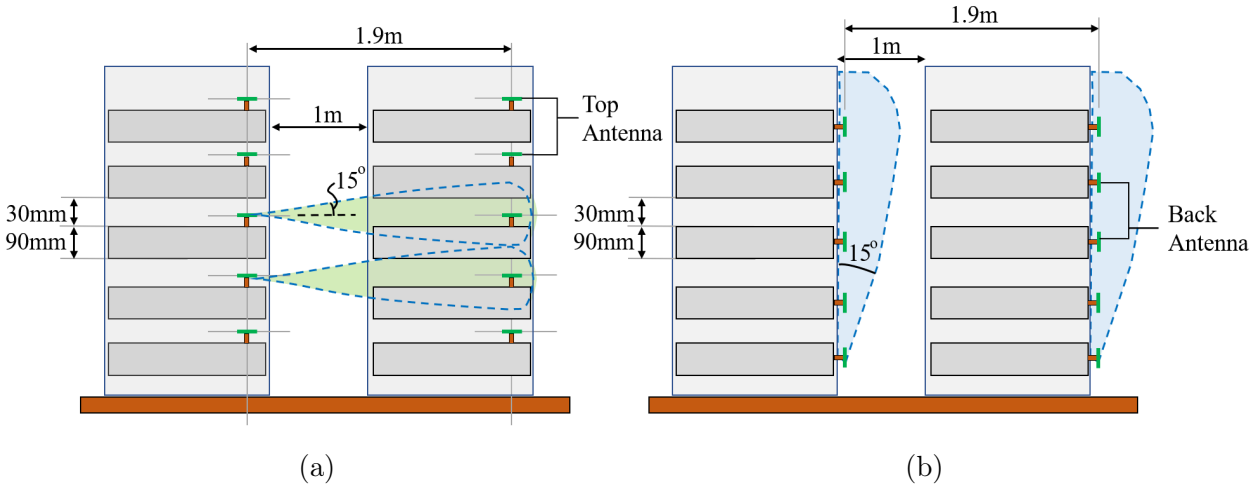


Figure 3.14: Separation between two adjacent transceivers (a) in horizontal lines (b) in vertical planes.

is not as significant as that of S2S-WiDCN. Therefore, by establishing direct links between servers S2S-WiDCN reduces the power consumption significantly compared to all the DCNs that require higher level switches.

3.2.4 Estimate of the Overheads

Vertically adjacent servers need to have space between them to accommodate the antenna arrays at the top of the servers. With the compact size of the antenna of only $10.5mm \times 3.3mm$, we envision a separation of $30mm$ between the servers should be enough. As the typical height of a server is $90mm$, we can reduce the vertical server density to be around 33%. In other words, this reduction in server density can increase in rack height by 33% to accommodate the same number of servers per rack. We anticipate that, this does not have a significant impact on infrastructure cost. In fact, this type of server arrangement will aid in cooling by enabling better chilled air circulation around each server.

As a narrow LoS exists between the servers communicating along the same horizontal line, the possibility of interference with adjacent receivers decreases as the top and bottom server structures do not allow the antenna radiation lobe to reach other vertically adjacent receivers as depicted in Fig. 3.14(a). While multi path transmission may still be caused by diffraction around rack structures even though non-reflective coating is used on all reflective surfaces, the narrow aperture to establish the LoS between the antennas makes it unlikely that the multipath non-LoS signals will have significant power. Similarly, the wireless communication in a vertical plane also does not interfere with the wireless communication with its adjacent vertical plane as row of racks will act

as a shield against the wireless signal of one plane interfering with a different plane as shown in Fig. 3.14(b). Moreover, the half-angle of the main radiation lobe is narrow enough to prevent the transmission from one vertical plane in reaching another. However, in both cases, receivers in the LoS of an active communication cannot use the same channel to receive data from another sender. A different OFDM channel is used in such a case to avoid interference.

3.3 Summary

The problems in current DCN's are high design and maintenance cost, huge power consumption, high cabling complexity, hard to keep accurate per-cable information and inefficient cooling. Power consumption of the network equipment in the data center including the different layer switches consumes considerable amount of power of the total power consumption of the data center. Structured cabling bundle incur significant initial effort and cost to set up and still may cause airflow blockage. All these challenges can be overcome by using the proposed completely wireless server-to-server DCN architecture. Adopting the S2S-WiDCN can eliminate the high power consuming switches altogether. We observe that S2S-WiDCN provides comparable flow completion duration and throughput to a conventional fat-tree based DCN for query/response and multimedia/video-based applications, while reducing the power consumption by five to seventeen times.

However, S2S-WiDCN minimizes the power consumption of the network portion of the data center but does not affect the power consumption of the servers. whereas servers consume the highest amount of IT power in the data center. In the next chapter, we are going to discuss a server consolidation method which can address the power consumption of the servers in a data center.

Chapter 4

Network-Aware Server Consolidation for Wireless Data Center

In this chapter we are going to discuss a network-aware server-consolidation technique called Network-Aware Server Consolidation (*NASCon*) for a S2S-WiDCN leveraging its high link diversity and separate control channel [93]. S2S-WiDCN can reduce the power consumption of the data center network portion, while does not affect the power consumption of the servers in the data center. On the contrary, with *NASCon*, the overall power consumption of the servers in a data center can drastically be reduced. We observed that up to 37% power reduction can be achieved if the *NASCon* algorithm is used with a S2S-WiDCN network. *NASCon* server consolidation consumes only 2.83% more power compared to optimal consolidation technique with exhaustive search but is far less computationally expensive. Moreover, being network bandwidth-aware, *NASCon* does not adversely affect the network performance of the data center whereas for higher bandwidth demanding network, the exhaustive search based consolidation results in degradation in the performance of the network. Because of multiple direction antenna arrays per server in S2S-WiDCN, multiple links per servers exists which can be leveraged by the *NASCon* consolidation to achieve higher performance after consolidation compared to conventional hierarchical architectures. On the other hand, in order to achieve scalability for the proposed server consolidation algorithm we adopt a divide and conquer mechanism involving clustering the data center into sub-networks of highly communicating servers. While network-aware server consolidation algorithms utilize this clustering as a first step [49] practical realization of data center-wide clustering requires maintenance of dynamically updated global communication and computation status of servers. This generally involves transfer of status updates across the DCN, potentially overloading the already oversubscribed network

and/or resulting in unpredictable latencies in the exchange of such status information, thereby limiting the efficiency and frequency of performing server consolidation [94, 95, 96]. In the proposed *NASCon* algorithm we leverage the separate control channel available in S2S-WiDCN for sharing the clustering related status updates across all the servers for dynamic clustering without the need of overloading the DCN links between servers.

While consolidating tasks can reduce the power consumption of data centers, due to the arrival of new tasks and completion of existing tasks, the consolidated utilization profile of the servers may change adversely affecting the power consumption over time. Hence, the *NASCon* consolidation algorithm should be repeated periodically. In this chapter, we have also proposed a method to find the optimal inter-consolidation time for a wireless data center and derive a mathematical formulation to estimate the optimal inter-consolidation time. This will enable optimally scheduling consolidation in a data center without the need for extensive simulations and measurements to achieve the optimality enabling real-time implementation of the consolidation after optimal intervals. The novel contributions of this chapter are:

- We designed a bandwidth constrained network aware server consolidation heuristic named Network-Aware Server Consolidation (*NASCon*). The proposed *NASCon* heuristics takes advantage of the two distinctive features of the S2S-WiDCN namely, high link diversity for each server and existence of a separate physical plane for achieving predictable latency in exchanging control information to reduce computational complexity of the heuristics.
- We compared the performance of the S2S-WiDCN with the *NASCon* algorithm with respect to a traditional fat-tree based wired network.
- Proposed *NASCon* can reduce the power consumption of S2S-WiDCN data center almost similar to consolidation based on exhaustive search while being much less computationally intensive. Moreover, *NASCon* does not adversely affect the network level performance of the DCN after the consolidation operation.
- We derived a mathematical model to identify the optimal inter-consolidation time. The model is validated through extensive simulations.
- We evaluate the performance of the *NASCon* algorithm with high bandwidth future data center networks for both wired and wireless networks.

4.1 Network Aware Server Consolidation

Server consolidation is a process where VMs running in one server are relocated to one or more different servers. However, as discussed earlier we propose a network-aware consolidation approach which takes into account the dense link diversity of the 60GHz S2S-WiDCN architecture along with the traffic interaction between the VMs running on the servers. In order for the VM migration approach to be network or traffic-aware, we first need to understand the nature of traffic interaction over the data center network.

4.1.1 Traffic Pattern Model

The traffic pattern in a data center network can be modeled in terms of multiple parameters such as flow arrival rates, flow injection rates, flow sizes, flow completion time and proportion of inter-rack and intra-rack flows [86]. In the S2S-WiDCN, there are six separate directional antenna arrays in the vertical plane of the server, and another one array on the top of the server. Therefore, seven simultaneous links from a server can co-exist at the same time.We represent the number of possible simultaneous links per server as θ. Let $\boldsymbol{F}$ be a vector whose elements are the number of existing flows along each sector determined from the number of flows existing in each server based on their destinations and the routing protocol. Let f denote the traffic flow rate. It is to be noted, that the flow rate f, has a Gaussian distribution [85, 86]. Therefore, to support 99.86% (one-sided z-distribution) of the flow rates, the required channel throughput should be

$$\boldsymbol{r} = f_{3\sigma}\boldsymbol{F}, \tag{4.1}$$

where elements of the vector $\boldsymbol{r}$, are the required channel throughput in each of the sectors and $f_{3\sigma}$ is the value of the flow rate which is three standard deviations higher than the mean. For the S2S-WiDCN, to accommodate multiple channel access, a single 60GHz `IEEE802.11ad` link is subdivided into n_{OFDM} separate OFDM channels. Therefore, the bandwidth of each OFDM channel is given by,

$$B_{\text{OFDM}} = B_{\text{60GHZ}}/n_{\text{OFDM}}, \tag{4.2}$$

where B_{60GHZ} is the bandwidth of the single physical channel. Therefore, to reduce the adverse effect of server consolidation on network performance, the following inequality must be satisfied for all wireless links or sectors from each server in the S2S-WiDCN,

$$r_x < B_{\text{OFDM}} \ \ \forall\, x, \tag{4.3}$$

where r_x is an element of $\boldsymbol{r}$. If the inequality in (4.3) cannot be satisfied due to high flow rates, consolidation will result in worsening of data center network performance as discussed in the results. Moreover, it has been observed from the measurement of a variety of data centers in [85], a large proportion of the server-to-server traffic flows, up to 80%, are intra-rack, meaning between servers in the same rack. Only a small remaining proportion of about 20% is inter-rack, or between servers in different racks. Therefore, to reduce the effective load on the network while consolidation, VMs that communicate more often should be migrated into the same physical server. Hence, in addition to reducing server underutilization, co-location of highly communicating VMs is also a desirable goal as it will reduce both power consumption and network traffic. This way, in our algorithm, we considered both the inequality of (4.3) and the proportion of inter and intra-rack traffic to make it network-aware.

4.1.2 The Network-Aware Consolidation Algorithm

The primary goal for consolidation is to reduce the total power consumption by reducing the number of active servers as well as network utilization. The underlying assumption is that the computational requirement for every VM running in the data center and the injection rates of every flow from each VM is known and readily available. In a single server, multiple VMs can run at a single instance. However, during the server consolidation, we considered all the VMs running as a single entity, meaning if migration is possible, all the VMs running on the server would be migrated to the new physical server for consolidation. The migrations happen in *online* mode following live migration [48]. While this will reduce the granularity of the consolidation, it is a more scalable approach suitable for large data centers with thousands of servers. Moreover, the task-level granularity for a network-aware consolidation requires the knowledge of traffic flow per task, which is difficult to model, predict or access in large data centers. Data center traffic rates are modeled usually among entire servers [86] limiting us to design consolidation algorithms at a server-level granularity.

We assume that every server has the same computational capacity and VMs running on a server utilizes a variable percent, collectively which can be represented by u. Let us assume that the maximum permissible utilization, without any significant degradation in performance or violation of legal contracts of any server, is D_u. D_u is a manufacturer specified parameter and can vary from model to model. The pseudo code for implementing the *NASCon* is shown in Algorithm 4.1. At first, all the servers running in the data center are divided into smaller clusters, such that servers within a cluster have a large number of flows exchanged among themselves, whereas servers in different clusters have a much smaller number of flows exchanged among them. Such a

Algorithm 4.1 Algorithm for *NASCon*

Input: Set of servers, $\boldsymbol{S} = \{s_1, s_2, ..., s_N\}$; Server utilizations, $\boldsymbol{u} = [\ u_1, u_2, ..., u_N]^T \in \mathbb{R}_+^n$; Flow injection rate $\boldsymbol{R} = [\boldsymbol{r_1}, \boldsymbol{r_2}, ..., \boldsymbol{r_N}] \in \mathbb{R}_+^{\theta \times N}$; Communication cost $\boldsymbol{\Psi} = \{\ \psi(i,j)\} \ \in \mathbb{R}_+^{N \times N}$

Output: Utilization profile $\boldsymbol{u}$ after *NASCon* Consolidation

1: **Clustering:**
2: $\{S_1, S_2, ..., S_k\} \in \boldsymbol{S} \leftarrow$ Graph-partition$(\boldsymbol{S}, \boldsymbol{\Psi})$ ▷ Kernighan-Lin
3: **for** $m = 1$ to k **do**
4: $S_m \leftarrow$ **sort** (S_m) ▷ ascending order of server utilization u
5: **for** $i = 1$ to size $(S_m) - 1$ **do** ▷ loop for migrating server
6: **for** $j =$ size (S_m) to $i + 1$ **do** ▷ loop for destination server
7: $\widetilde{u} = u_i + u_j$
8: $\widetilde{\boldsymbol{r}} = \boldsymbol{r_i} + \boldsymbol{r_j}$
9: **if** $(\widetilde{u} < D_u$ **and** $\forall\ x \in \{1, 2, ..., \theta\}\ \widetilde{r_x} < B_{\text{OFDM}})$ **then**
10: Migrate (s_i, s_j) ▷ s_i is the i-th entry of the sorted S_m
11: *break* ▷ Break from loop in line 6
12: **end if**
13: **end for**
14: **end for**
15: **end for**

clustering places highly communicating servers in the same cluster. This intra-cluster consolidation reduces the communication among these highly communicating servers. This clustering is a Graph Partitioning Problem, which is to partition graph vertices into disjoint groups with minimum edge cut cost. $Kernighan - Lin$ algorithm [97] is adopted for the graph-partitioning tasks in our work. Here we treat servers as vertices and the number of flows going outside of server as edge costs. After the partitioning, all the servers in each cluster are sorted according to their utilization u. The outer loop (`line 5` in Algorithm 4.1) in the proposed algorithm choose the candidate to migrate in the ascending order of utilization starting with the least utilized one. The inner loop (`line 6` in Algorithm 4.1) choose the destination to migrate in the descending order of utilization starting with the most utilized one. If the sum of utilization of the candidates to migrate and the potential destination is less than D_u and each element of the vector sum of their required injection rates is less than the channel throughput per OFDM channel, the candidate is migrated to the destination. Due to the link diversity and density of the wireless OFDM channels this constraint results in much higher consolidation than for a wired conventional DCN. Therefore, this step with the network-aware constraint results in higher consolidation in case of the S2S-WiDCN due to incorporating this

Algorithm 4.2 Migration Function

Input: Source and destination server for migration

Output: Updated utilization profile $\boldsymbol{u}$ after single migration

1: **function** MIGRATE(server a, server b)
2: $b \leftarrow$ VMs running on a
3: $u_b = u_a + u_b$
4: $\boldsymbol{r_b} = \boldsymbol{r_a} + \boldsymbol{r_b}$
5: $a \rightarrow$ *PowerNap* state
6: $u_a = 0$
7: $\boldsymbol{r_a} = \boldsymbol{0}$
8: **end function**

constraint in this manner in the NASCon algorithm. This flow rate related condition for migration is informed by our traffic model related constraint in (4.3). After a successful migration, the inner loop is broken out of, to choose the next server in the outer loop for potential migration. If either of the two conditions fails, the inner loop continues till the list of servers for the potential destination is exhausted. For each completion of the inner loop, the outer loop progresses to next candidate for migration.

The necessary steps of the migration function (*Migrate*) used in the pseudo code of *NASCon* Algorithm 4.1 are shown in Algorithm 4.2. The function migrates server a to server b. At first, all the VMs running in migrating server a is migrated in the destination server b. So the utilization of the destination server increases which is the summation of the utilization of both the servers. Vector $\boldsymbol{r_b}$ is updated based on all the flows running on server b post migration. After successful migration, server a is put into the PowerNap state [98] having zero utilization. In the PowerNap state, most of the components of the server are powered down except the network interface card (NIC), the wireless transceivers and a small portion of the CPU to get the signal for waking up when required.

The *NASCon* algorithm is illustrated with a few examples of migration attempts in Fig. 4.1. *State* 0 represents the state where the servers are already sorted according to their utilization prior to migration within a single cluster with the lowest utilization on the top. In *step* 1, the least utilized server s_1 tries to migrate to the most utilized server s_t in that cluster. If all the conditions of migration are satisfied and the migration is successful (represented with the top/green arrow), the algorithm tries to migrate the next least utilized server s_2 to the most utilized server in the next step, *step* 2. On the contrary, if the prior migration failed in *step* 1 (represented by bottom/red arrow), the algorithm tries to migrate s_1 into the next most utilized server s_{t-1} in *step* 2. This

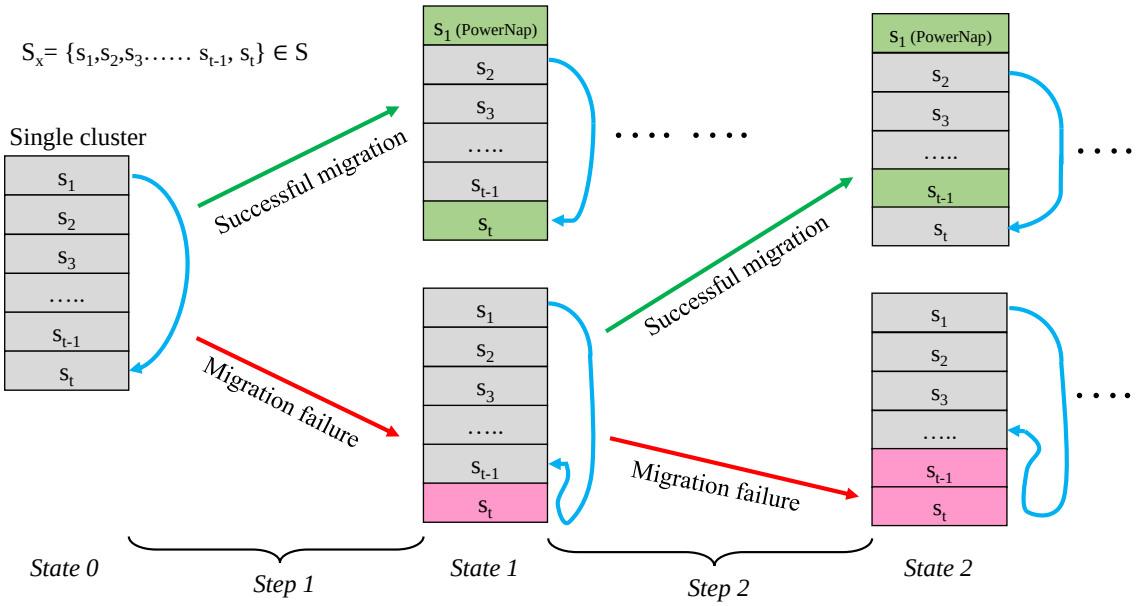


Figure 4.1: Bandwidth constrained consolidation in a single rack. The blue arrows show the next attempt of migration. Pink marks a failure while migration. Green denotes successful migration.

migration attempt can again be either successful (top in *state* 2) or failure (bottom in *state* 2). On a successful migration attempt in *state* 2, *step* 3 will attempt to migrate the next least utilized server s_2, to server st again. On the other hand, if the attempt fails, the same s_1 is attempted to migrate to the next server in the list, s_{t-2}. A similar process continues until the migration is attempted for all servers in the list. The same is done for all the clusters.

4.1.3 Complexity Analysis

The complexity of server consolidation over the entire data center to provide the optimal solution using exhaustive search method is $O(N^N)$ where N is the total number of servers in the entire data center. This is because N set of VMs can be potential candidates for migration to N servers in N ways. Therefore, each of N set of VMs has N options for potential migrations and for each of the N such scenarios the other sets of VMs also have all N options to create each possible migration scenario. However, this complexity is too high even for moderately large data centers. Therefore, we compare our proposed *NASCon* consolidation algorithm with the Clustered Exhaustive Search (CES) algorithm, which finds the optimal migration within each cluster using the exhaustive search.

We have adopted the $Kernighan - Lin$ algorithm to do the clustering in the beginning of the *NASCon* consolidation. If all the servers are equiprobable to have links between themselves, the computational complexity becomes $O(N^2 \log N)$ [97]. If the average number of servers in a cluster is

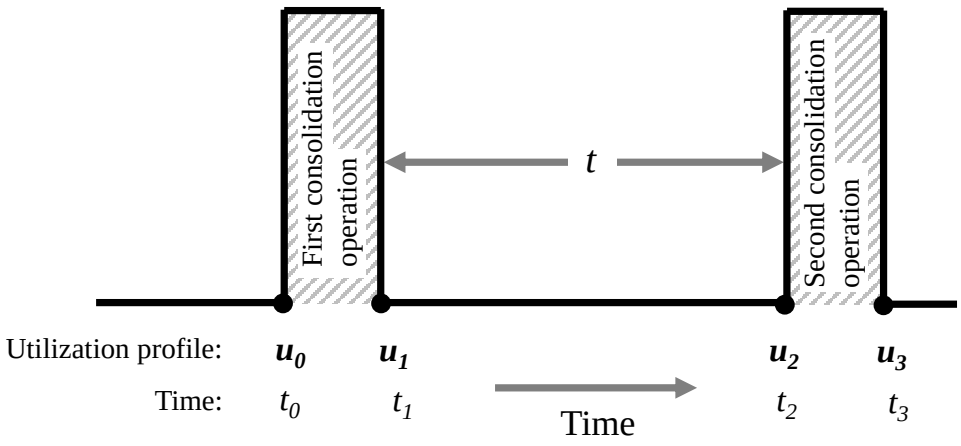


Figure 4.2: Timeline of consolidation operations.

n and if the number of the clusters formed is m, the computational complexity of the CES algorithm after clustering is $O(mn^n)$ and is an np-hard problem. With the clustering, the complexity of the CES algorithm is $O(N^2 \log N + mn^n)$. On the contrary, for the *NASCon* algorithm, inside each cluster, the servers are sorted according to their utilization having a complexity of $O(n \log n)$ using merge sort [99]. Next, the two loops for finding the source and destination of the migration has the complexity of $O(n^2)$ in the worst case. So the overall complexity of *NASCon* for all m clusters becomes $O(N^2 \log N + mn \log n + mn^2)$. Therefore, *NASCon* has a much lower complexity compared to the overall exhaustive search algorithm. As the clustering is similar in both CES and *NASCon*, the difference in their complexity comes from the mechanism of determining candidates for migration. The complexity of *NASCon* after clustering is $O(mn \log n + mn^2) \approx O(mn^2)$ which, is lower than that of the CES after clustering.

4.1.4 Optimizing the Inter-Consolidation Time

Due to the arrival of new tasks and completion of existing tasks, the consolidated utilization profile of the servers may change over time. Therefore, the power consumption of the data center may be adversely affected over time. Hence, the *NASCon* consolidation algorithm should be repeated periodically. Repeating the consolidation too often might not reduce the total power consumption enough to justify the additional network traffic introduced as a result of the consolidation. On the contrary, delaying the consolidation can adversely affect the potential opportunity to save power. Hence, to determine the optimal time interval between two consecutive consolidations, an appropriate cost function, to capture the trade-off between power savings and network traffic is required. We define the expected value of the time-dependant cost function $C(t)$ for inter consolidation time interval as

$$C(t) = \kappa E[A(t)] - E[B(t)], \tag{4.4}$$

where $A(t)$ is migration cost related to the network traffic which represents the total traffic movement for the consolidation operation, $B(t)$ is the total power saving due to the consolidation, t represents the time interval between two consecutive consolidation operation, and κ is a scaling constant which captures the relative significance of network traffic and power savings. $E[\cdot]$ represents the expected value and is necessary as random task arrivals and completion make $A(t)$ and $B(t)$ random processes. At the optimal inter- consolidation time interval t^*, the cost $C(t)$ should have the minimum value, that is,

$$t^* = \underset{t \in \mathbb{R}}{\operatorname{argmin}}\, C(t). \tag{4.5}$$

Fig. 4.2 represents the timeline for the consolidation operation which shows two consecutive consolidation operations. $\boldsymbol{u}$ denotes the utilization profile of all the servers in the data center, where $\boldsymbol{u} = [u_1, u_2, ...u_N]^T \in \mathbb{R}_+^{\mathrm{N}}$ if N is the total number of servers in the data center. At time t_0, when the utilization profile is $\boldsymbol{u}_0$, first consolidation operation takes place, and immediately after the consolidation, at time t_1, the utilization profile of the servers becomes $\boldsymbol{u}_1$. After t seconds at t_2 the utilization profile of the servers becomes $\boldsymbol{u}_2$ and a second consolidation is carried out which is completed at t_3 with a final utilization profile of $\boldsymbol{u}_3$. Hence, it can be written that, $\boldsymbol{u}_1 = \Gamma(\boldsymbol{u}_0)$ and $\boldsymbol{u}_3 = \Gamma(\boldsymbol{u}_2)$, where Γ represents the consolidation operation. Furthermore, it holds that,

$$\boldsymbol{u}_2 = \boldsymbol{u}_1 + \boldsymbol{\delta} t, \tag{4.6}$$

where $[\boldsymbol{\delta}]_i$ is the task increase rate. $A(t)$ is directly related to the amount of traffic transferred through the network for the migration. If the average size of traffic per migration is ν, then $A(t)$ can be represented by,

$$A(t) = \nu\Big(\|\boldsymbol{u}_1 + \boldsymbol{\delta} t\|_0 - \|\Gamma(\boldsymbol{u}_1 + \boldsymbol{\delta} t)\|_0\Big), \tag{4.7}$$

where $\|\cdot\|_0$ represents the ℓ_0-norm and returns the number of non-zero entries of its vector argument that is the total number of active servers. Therefore the difference between the ℓ_0-norms capture the total number of VMs migrating as a result of the consolidation.

Let, η_0, η_1, $\eta_2(t)$, and $\eta_3(t)$ represent the number of idle servers at time t_0, t_1, t_2, and t_3, respectively, where

$$\begin{aligned} \eta_0 &= N - \|\boldsymbol{u}_0\|_0, \\ \eta_1 &= N - \|\Gamma(\boldsymbol{u}_0)\|_0, \\ \eta_2(t) &= N - \|\boldsymbol{u}_1 + \boldsymbol{\delta} t\|_0, \\ \eta_3(t) &= N - \|\Gamma(\boldsymbol{u}_1 + \boldsymbol{\delta} t)\|_0, \end{aligned} \tag{4.8}$$

and N is the total number of servers in the data center. Hence, from (4.7) and (4.8), the expected value of $A(t)$ can be expressed as

$$E[A(t)] = \nu\big(\eta_3(t) - \eta_2(t)\big). \tag{4.9}$$

If the aggregate load running across the data center remains approximately constant between two consolidations, the expected number of idle servers after any consolidation operation will be similar, i.e. $\eta_1 \approx \eta_3(t)$ and does not depend on t. This assumption especially is valid when the granularity of the tasks are small compared to the capacity of an individual server. Hence, the expected value of $A(t)$ can be written as

$$E[A(t)] = \nu\big(\eta_1 - \eta_2(t)\big). \tag{4.10}$$

On the other hand, the expected value of $B(t)$ can be estimated as

$$E[B(t)] = P_{idle}\eta_2(t) + P.\|\boldsymbol{u}_1\|_1 + (N - \eta_2(t))P_0 - P_{idle}\eta_1 - P.\|\boldsymbol{u}_2\|_1 - (N - \eta_1)P_0. \tag{4.11}$$

Here, P_{idle} is the power consumption per server in the PowerNap mode and P_0 represents the power consumption per server just after waking up from the PowerNap mode. P is the slope of linear regime of the power profile of the server as shown in Fig. 4.3. $\|\cdot\|_1$ represents the ℓ_1-norm and returns the sum of the utilization of all the active servers.

As the aggregate load across the data center is approximately constant over time, the total utilization of all active servers is approximately constant. Moreover, as the power consumption of the *active* servers is almost a linear function, it can be estimated that, $\|\boldsymbol{u}_1\|_1 \approx \|\boldsymbol{u}_2\|_1$. Hence, equation (4.11) can be rewritten as

$$\begin{aligned} E[B(t)] &= P_{idle}\big(\eta_2(t) - \eta_1\big) - P_0\big(\eta_2(t) - \eta_1\big) \\ &= \big(\eta_2(t) - \eta_1\big)\big(P_{idle} - P_0\big) \\ &= \big(\eta_2(t) - \eta_1\big)K. \end{aligned} \tag{4.12}$$

Here $K = P_{idle} - P_0$ is a constant with respect to t. Combining equations (4.4), (4.10) and (4.12), the estimated cost of the consolidation after time interval t can be found to be

$$\begin{aligned} C(t) &= \kappa\nu\big(\eta_1 - \eta_2(t)\big) - K\big(\eta_2(t) - \eta_1\big) \\ &= \big(\eta_1 - \eta_2(t)\big)(\kappa\nu + K) \\ &= \big(\eta_1 - \eta_2(t)\big)K', \end{aligned} \tag{4.13}$$

where $K' = (\kappa\nu + K)$ is a constant with respect to t. Thus to estimate t that minimizes the cost, we have to find the t that minimizes $\eta_2(t)$, though $\eta_2(t)$ is not known. Below we present a model for approximate $\eta_2(t)$.

To approximate $\eta_2(t)$, we consider that the servers follow the model of $M/M/1$ queuing processes [100], where λ and μ represent the new task arrival rate and task finishing rate per server, respectively. Hence, if a server initially has a utilization i, then t seconds later it will have utilization k, with the probability,

$$p_k^{(i)}(t) = e^{-(\lambda+\mu)t}\left[\rho^{\frac{k-i}{2}} I_{k-i}(at) + \rho^{\frac{k-i-1}{2}} I_{k+i+1}(at) + (1-\rho)\rho^k \sum_{j=k+i+2}^{\infty} \rho^{-j/2} I_j(at)\right], \tag{4.14}$$

where $\rho = \frac{\lambda}{\mu}$, $a = 2\sqrt{\lambda\mu}$ and $I_k = \sum_{m=0}^{\infty} \frac{(-1)^m}{m!\Gamma(m+k+1)}\left(\frac{x}{2}\right)^{2m+k}$ represents the modified Bessel function of the first kind of k-th order [100]. This model is valid only for $\lambda < \mu$, which is essentially true for sustenance of data centers of interest. The probability that a node becomes idle at time t can be found from (4.14) by replacing k with zero. Hence the probability of a node becoming idle can be expressed as

$$p_0^{(i)}(t) = e^{-(\lambda+\mu)t}\left[\rho^{-\frac{i}{2}} I_{-i}(at) + \rho^{\frac{-i-1}{2}} I_{i+1}(at) + (1-\rho)\sum_{j=i+2}^{\infty} \rho^{-j/2} I_j(at)\right]. \tag{4.15}$$

Hence, the expected number of the idle nodes at $t_2 = t_1 + t$ can be expressed as,

$$\eta_2^{\text{model}}(t) = \sum_{l=0}^{N} \sum_{\mathcal{J}\subseteq[N]} \prod_{n\in\mathcal{J}} p_0^{i(n)}(t) \prod_{m\notin\mathcal{J}} \left(1 - p_0^{i(m)}(t)\right), \tag{4.16}$$

where $[N] = \{1, 2, 3, ..., N\}$ and $\mathcal{J}$ is all the possible realizations of l idle nodes. In view of (4.16) and (4.13), the inter consolidation cost can be approximated as

$$C^{\text{model}}(t) = \left(\eta_1 - \eta_2^{\text{model}}(t)\right)K' = \eta_1 K' - K' \sum_{l=0}^{N} \sum_{\mathcal{J}\subseteq[N]} \prod_{n\in\mathcal{J}} p_0^{i(n)}(t) \prod_{m\notin\mathcal{J}} (1 - p_0^{i(m)}(t)) \tag{4.17}$$

$C^{\text{model}}(t)$ in (4.17), can be calculated for any t, since $p_0^i(t)$ is known for any t. Thus optimal inter-consolidation time can be approximated by

$$t^*_{\text{model}} = \underset{t\in\mathcal{G}}{\operatorname{argmin}}\, C^{\text{model}}(t) = \underset{t\in\mathcal{G}}{\operatorname{argmax}}\, \eta_2^{\text{model}}(t), \tag{4.18}$$

where $\mathcal{G}$ is a finite-length fixed-step grid in $\mathbb{R}$. From this mathematical model, the optimal inter-consolidation time can be estimated without the need of thousands of simulations involving different random utilization profile of servers. The accuracy of the mathematical model is verified with a Monte-Carlo simulation in section 4.2.5. We have also compared the time required to compute the optimal consolidation time from both Monte-Carlo simulation and from (4.18) in Section 4.2.6.

4.2 Modeling, Results and Analysis

In this section, we discuss modeling, results and corresponding analysis of the proposed server consolidation method in a wireless data center. We first compare the performance of the proposed *NASCon* server consolidation algorithm with that of CES in terms of reduction of server power consumption in the data center. Next, we evaluate the network-level performance with the consolidation algorithm in a data center with both wired and wireless architecture with network-level simulations. Before presenting and analyzing the results we describe the data center traffic generation procedure and simulation platform in next subsections.

4.2.1 Data Center Traffic Generation

The *NASCon* algorithm is evaluated with a set of traffic flows based on application demands. Real data center traffic for different classes of data centers such as educational (small), private (medium) and corporate (large), running typical query/search type applications like map-reduce and index-search are measured in [85]. Using these measured traffic flows, a Poisson shot-noise based model to synthesize data center traffic is proposed and verified in [86]. According to [86], the new flow arrival time, the flow duration and the injection rate for each application follow a Poisson, Pareto and, Gaussian distribution respectively. The new flow arrival time is generated using a Poisson distribution with an average flow arrival rate. The average flow arrival rate is considered to be 1000 flows/second for the small-sized DCN [85]. In our evaluations, we have considered a Gaussian distribution for the injection rate to have a mean of 8.0kbps as the base case for the simulation. Application flow duration is generated following an independent Pareto distribution having a minimum duration of 10 microseconds [85] and a mean of 1 second. We then increased the average injection rates in an incremental basis to 8Mbps, 100Mbps, 400Mbps, and 650Mbps and regenerated new traffic which represents different types of multimedia traffic and repeat the simulations.

4.2.2 Simulation Platform

We use the Network Simulator-3 (NS-3) suite [84] to evaluate the performance of *NASCon* for both wired fat-tree and wireless S2S-WiDCN networks. NS-3 supports the characteristics of wireless propagation as well as network-level communications. It is important to simulate both the propagation and network-level communication characteristics accurately in order to obtain credible

performance results. A modified version of NS-3 extended with features of wireless data center including the 60GHz band and the `IEEE802.11ad` standard as discussed in [12] was used for this simulation. This extension incorporates interference modeling, bit error rates, and directional antenna modeling. The accuracy of these parameters is verified with physical layer measurements of prototype 60GHz hardware [12]. Additionally, we introduce criteria for wireless link selection to enable many concurrent links and modify the `IEEE802.11ad` physical layer to allow multiple OFDM channels. This simulation platform is used to evaluate the S2S-WiDCN with and without consolidation and compare it with the fat-tree wired DCN. For the fat-tree based wired data center architecture, we have considered 1.0Gbps links between servers to access switches and 40.0Gbps upper-layer links. We have compared the performance of the *NASCon* consolidation algorithm for S2S-WiDCN with traditional wired fat-tree based DCN. One of the limitation of the simulation platform is that, the migration cost for consolidation is not included in the performance analysis. Moreover, the computation power and time required to perform a full network level analysis of medium to large scale data center in NS-3 becomes impractically high. Hence we have considered a small data center consisting of 800 servers arranged in a 20×8 array of racks as [77].

Each of the rack houses 5 servers and occupies an area of $0.6m \times 0.9m$ and is $2m$ high. There are 10 racks arranged in a single row and two columns of 8 rows, totaling 160 racks. In our simulations, the racks are assumed to be without any front or back door. In the traditional wired fat-tree based DCN, we have considered the same number of servers arranged in same layout as S2S-WiDCN. We have considered 3 hierarchical network layers consisting of 160 access, 2 aggregate, and 2 core layer switches, where each rack having an access layer switch.

4.2.3 Power Consumption Analysis

In this section, we evaluate the power consumption and efficiency improvement by implementing *NASCon* for S2S-WiDCN, and wired data center. We also compare the results with the CES algorithm. We discuss the model and parameters used in power estimation followed by the results.

Power Model

It is not a straightforward task to estimate the actual electrical power consumed by a data center. The power consumption depends on several internal factors such as utilization of computing power, the cooling mechanism, and data center networks. Data center power consumption is also affected by external parameters like the geographical location, weather, temperature, and humidity. The

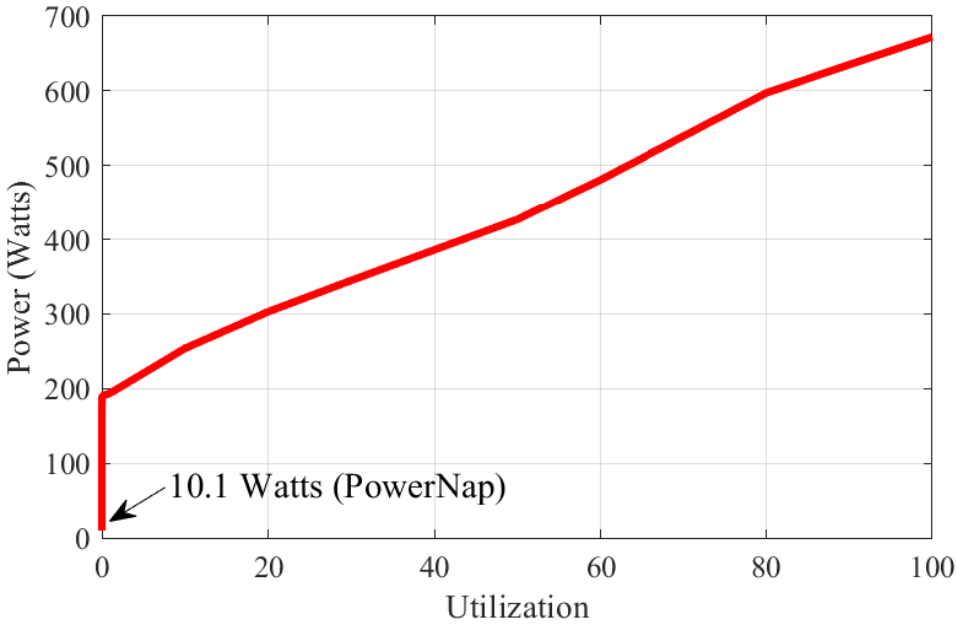


Figure 4.3: Power profile varying utilization of PowerEdge C5220 server.

total IT power consumption of a data center, P_{IT} consists of power consumption of the servers (P_{Server}) and network component ($P_{Network}$) of the data center. Hence,

$$P_{IT} = P_{Servers} + P_{Network}. \tag{4.19}$$

A major portion of P_{IT} comes from $P_{Servers}$ [2] [15]. However, the power consumption of servers varies significantly with the change in CPU utilization [98]. If the utilization of i-th server is denoted by u_i, the Power consumption of that server can be given by $P_{Server}(u_i)$, where the dependence of server power on utilization is adopted from [101]. Hence, equation (4.19) can be rewritten as

$$P_{IT} = \sum_{i=1}^{N} P_{server}(u_i) + P_{network}. \tag{4.20}$$

For the power analysis, we used the power profile of Dell Inc. $PowerEdgeC5220$ ($IntelXeonE3-1265LV2$) servers. Power consumption at different server utilization is modeled from the measurement done by the Standard Performance Evaluation Corporation's $SPECpower\_ssj2008$ database for the same server [101]. To keep the power model simple we did not consider any dynamic voltage-frequency adjustment for the servers during the operation. But in addition to the above power model for the server, we have considered an idle server to be placed in the PowerNap state [98] with minimal power consumption. The power profile of a server against different utilization is shown in Fig. 4.3. Although compared to the server power, the power consumption of the network of a data center is small, but it is not negligible [2]. One of the issue with the networking equipment is that they

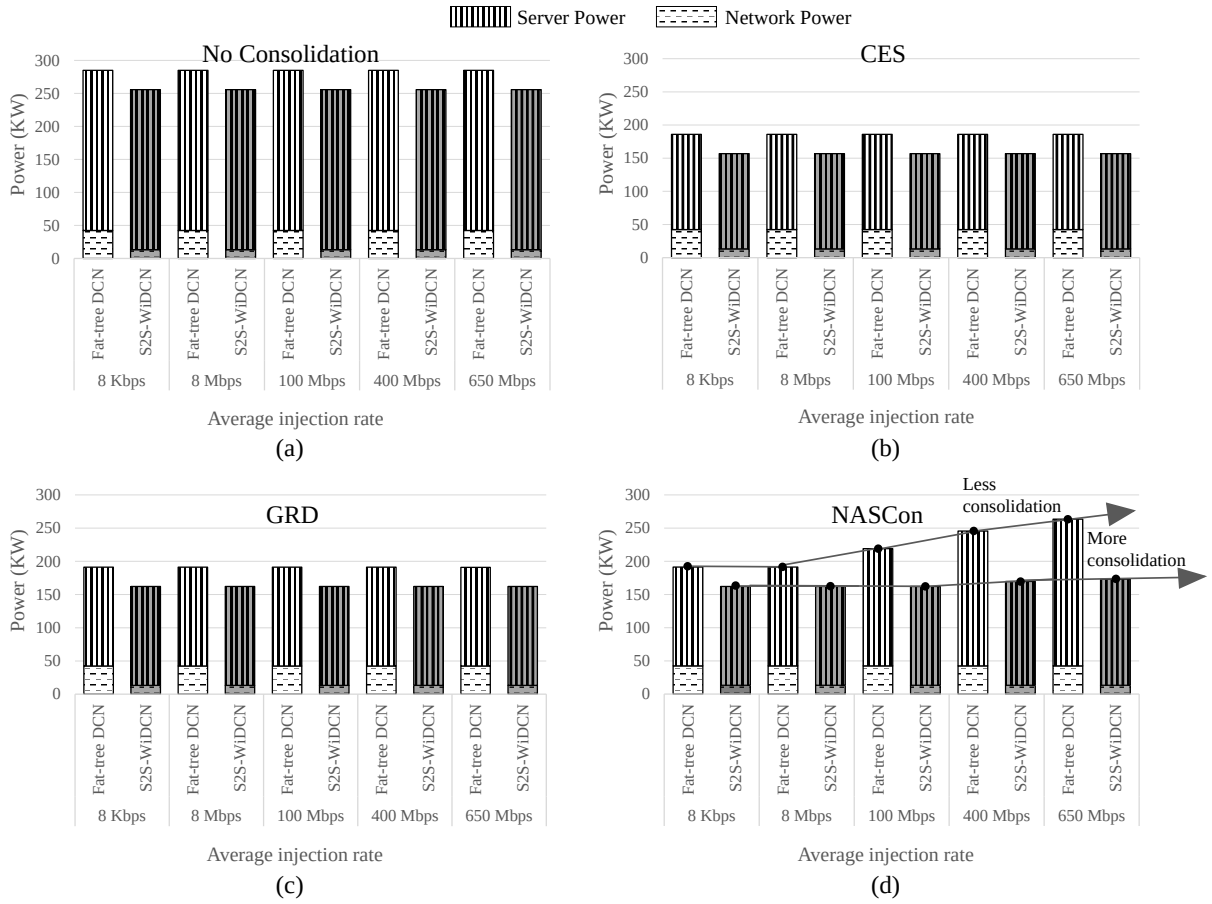


Figure 4.4: IT Power consumption comparison of different architecture for (a) no consolidation (NC) (b) clustered exhaustive search (CES) (c) Greedy approach base consolidation (GRD) and (d) Network-Aware Server Consolidation (*NASCon*). The arrows denote the power saving due to *NASCon*.

are needed to be turned on all the time. The static power portion of the networking equipment dominates the total power consumed by the network [102]. The main contributing factors for this dominance of the static power are the fixed overheads such as fans, switch chips, and transceivers which waste power at low loads. In [102], it has been shown that for a network switch, only eight percent power reduces during full load to no load transition. Moreover, for the wired network, upper-level switches experience a similar amount of traffic before and after the consolidation as majority of the flows remains inside of the rack. For this reason, we neglected the change in networking power equipment due to the variation in injection rate or throughput. We estimate power consumption for wired DCNs using commercially available data from Cisco network switches [103] and Silicom network interface cards (NIC) [92]. The power consumption of each device used in the network is shown in table. 3.3. The total network power is

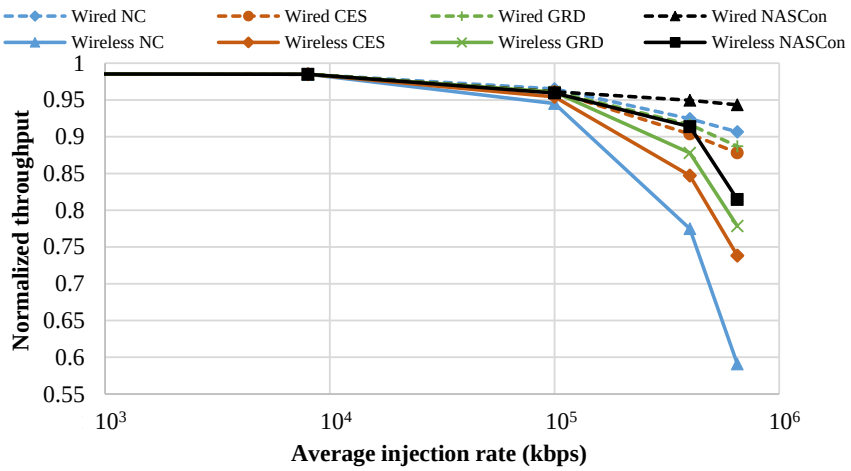


Figure 4.5: Average throughput for different data center architecture with NC, CES, GRD and *NASCon* consolidation normalized with flow injection rate.

$$P_{Network} = N_{Core}P_{Core} + N_{Agg}P_{Agg} + N_{Acc}P_{Acc} + NP_{NIC} \tag{4.21}$$

where N_{Core}, N_{Agg}, N_{Acc}, N are the number of core, aggregation, access switches, and the total number of servers, respectively; P_{Core}, P_{Agg}, P_{Acc}, P_{NIC} are the power consumption of an individual core, aggregation, access switches, and network interface cards, respectively. In S2S-WiDCN, however, no core, aggregate or access layer switches are needed, but only antennas, transceivers and NICs are required for wireless communication. The power consumption of the wireless 60GHz transceiver is modeled based upon the assessment of 60GHz transceivers [104]. The NICs of S2S-WiDCN are equipped with transceivers for horizontal and vertical communication. In the traditional DCN, external connections are established via the two Cisco 7702 switches. To provide equivalent connectivity in S2S-WiDCN, we employ two servers to work as gateways, and their power consumption is modeled as that of the Cisco 7702 switch. The power consumption for communication per server in S2S-WiDCN is calculated as:

$$P_{Wireless} = 7P_{60GHzTran} + P_{WifiCntrl} + P_{NIC}, \tag{4.22}$$

where $P_{60GHzTran}$ is the power consumption of a single 60GHz transceiver required for each of the 6 sectors and the horizontal link and $P_{WifiCntrl}$ is the power consumption of the `IEEE802.11` 2.4/5 GHz ISM adapter for the control channel. Finally, total power consumption in S2S-WiDCN is:

$$P_{Network(WiDCN)} = N_{Core}P_{Core} + N.P_{Wireless}. \tag{4.23}$$

Comparative Analysis of Power Consumption

The main advantage in power savings due to the server consolidation in the S2S-WiDCN is presented in this section. The IT power consumption of wired and S2S-WiDCN data centers with different consolidation methods including the *NASCon* algorithm with variation in the flow injection rate are shown in Fig. 4.4. Fig. 4.4(a) represents the power consumption of the data center with no consolidation (NC) while Fig. 4.4(d) represents *NASCon*. The figure also contains the power consumption pattern if CES algorithm is adopted instead of *NASCon* in Fig. 4.4(b). For the sake of comparison, we also simulate a network-unaware greedy approach based consolidation (GRD) similar to NICE [49] and the power consumption pattern is shown in Fig. 4.4(c). For both wired and wireless networks, at lower injection rates, all the consolidation techniques perform similarly and results in significant power reduction compared to NC. CES consumes the least power as it is an exhaustive search technique which is computationally impractical as discussed in Section 4.1.3. *NASCon* consumes only 2.83% more power than CES while being significantly computationally efficient and having better DCN performance which is discussed later in Section 4.2.4. From our analysis we observers that *NASCon* for S2S-WiDCN reduces about 37% of IT power consumption compared to NC case.

For higher injection rates, CES and GRD consumes significant less amount of server power compared to *NASCon* for wired networks. This is because the CES and GRD are not network bandwidth-aware, resulting in more aggressive consolidation compared to *NASCon*. Therefore, this difference becomes more apparent with increase in flow injection rates. However, this reduction of power comes at the cost of the lower throughput because the CES and GRD algorithms do not consider the network traffic characteristics. This impact on performance is discussed in details in Section 4.2.4.

For S2S-WiDCN network, the benefit of the *NASCon* consolidation becomes prominent compared to CES and GRD. As being unaware of the network characteristics, for CES and GRD power consumption remains same. Hence, at higher injection rate, CES and GRD consumes less power compared to *NASCon*. However, this reduction of power comes at the cost of lower throughput as CES and GRD algorithms do not consider the network traffic characteristics while consolidation. However, the increase in power consumption in *NASCon* for S2S-WiDCN is not as drastic as in the case of wired data center. This is demonstrated by the trend arrows in Fig. 4.4(d). At high injection rate of 650Mbps for S2S-WiDCN, *NASCon* consumes higher power compared to CES similar to low injections, while having significantly better network performance. This is because, in the S2S-WiDCN architecture, a server has the potential to sustain a maximum of seven simultaneous

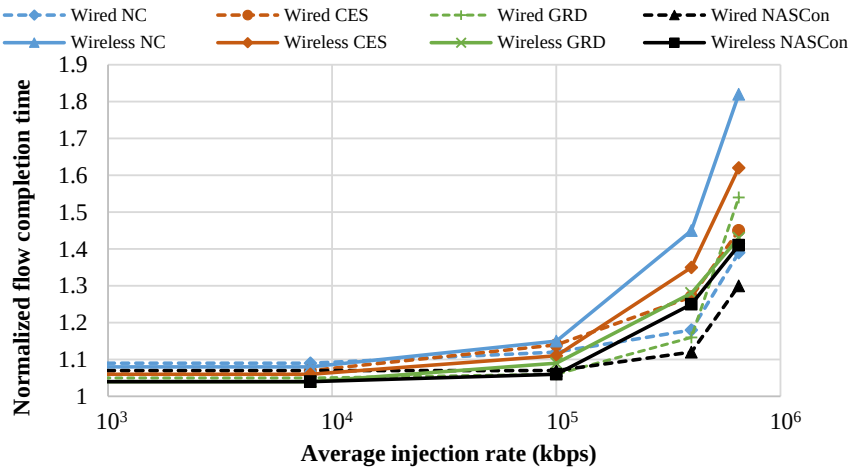


Figure 4.6: Average flow completion time for different data center architecture with NC, CES, GRD and *NASCon* consolidation normalized with flow injection duration.

links at a time with other servers in its vertical plane and horizontal line. On the contrary, in the wired architecture, there exists only one link per server albeit, of higher bandwidth. As a result, for the wired DCN with *NASCon*, many of the VM migration attempts fail due to the violation of the inequality of (4.3) compared to the S2S-WiDCN. This suggests that the network-aware server consolidation, *NASCon* is more effective on S2S-WiDCN.

4.2.4 Performance

Here we present the network-level performance of the S2S-WiDCN with *NASCon* along with a comparative analysis with respect to wired fat-tree DCNs in terms of throughput and flow completion duration.

Throughput

The throughput is defined as the average rate of bit transferred per second over the DCN. The normalized throughput of both S2S-WiDCN and fat-tree architecture for different injection rates at NC, CES, GRD and *NASCon* consolidation are shown in Fig. 4.5. Normalized throughput is defined as the ratio of the average throughput achieved and average injection rate. For NC, although it is seen that for lower injection rate both S2S-WiDCN and fat-tree network shows similar throughput, but for both the networks, the achieved throughput starts to decrease as the average injection rate goes beyond 100Mbps. However, degradation is different for wired and wireless DCNs. The

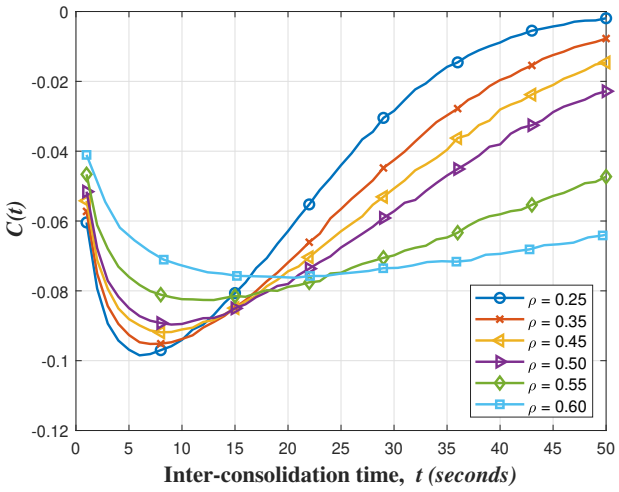


Figure 4.7: Consolidation cost measured from Monte Carlo simulation with respect to inter-consolidation time.

throughput reduces more for the wireless DCN than the wired counterpart for higher injection rates due to the lower physical bandwidth available per channel for the wireless links of 0.563Gbps compared to 1.0Gbps for the wires. Further, from Fig. 4.5, it can be seen that, for the lower injection rates, there is no significant difference in achieved throughput with *NASCon* consolidation for both wired and wireless data centers. These throughputs are also similar compared to that NC case. However, for higher injection rates beyond 100Mbps, for both S2S-WiDCN and fat-tree network, achieved throughput increases compared to the NC. The main contributing factor is that, due to the VM migrations, in many cases, both source and destination of flows end up in a same physical server. Therefore, these flows are effectively eliminated from the network, which ultimately increases the average throughput of the entire network compared to NC.

On the other hand, instead of *NASCon*, if CES or GRD consolidation is implemented, at lower injection rates, there is no significant difference in achieved throughput for both S2S-WiDCN and fat-tree networks compared to *NASCon*. For the higher injection rates beyond 100Mbps, the performance of the wireless networks improves compared to NC, but not as good as *NASCon*. However, the performance of the wired network degrades with the incorporation of CES or GRD consolidation algorithm. This contrasting behavior is mainly due to the number of channels available in different architectures. Due to all flows in the wired data center being channelized over the same link, the aggregate flow rate after CES or GED exceeds the physical link bandwidth violating (4.3). This causes degradation in throughput. On the contrary, in the S2S-WiDCN, due to the presence of multiple vertical sectors and the horizontal link a relatively larger number of flows will not violate (4.3) resulting in better performance compared to the wired data center.

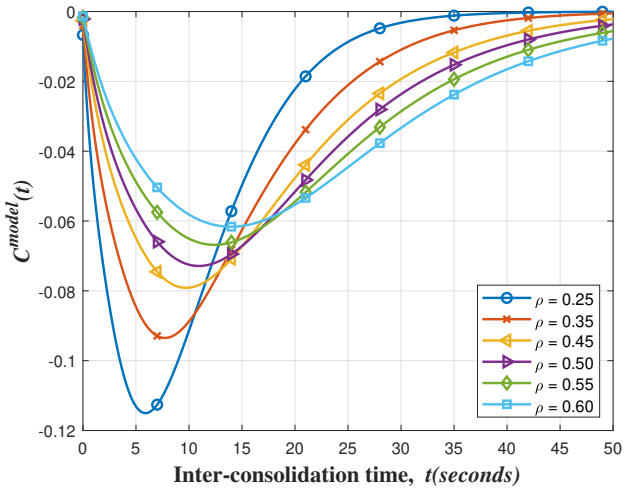


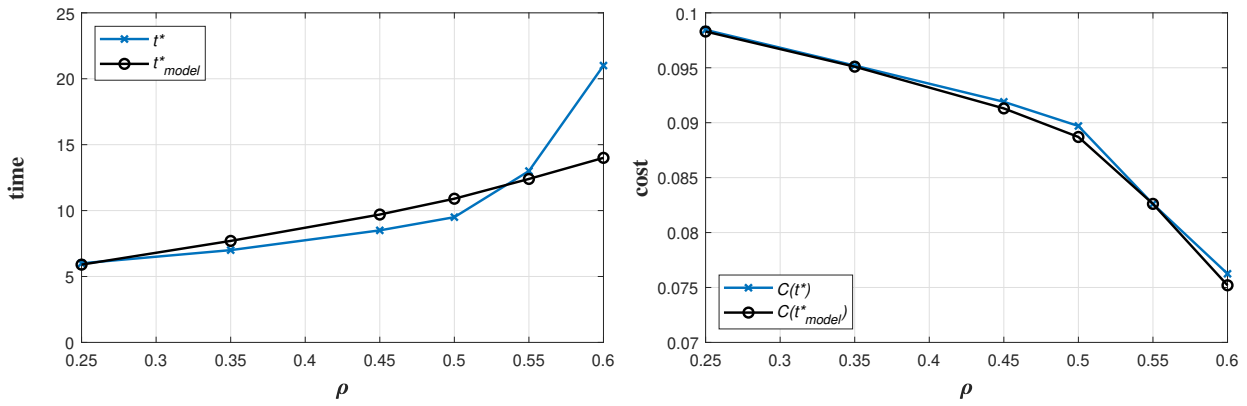
Figure 4.8: Consolidation cost estimated from mathematical model with respect to inter-consolidation time.

Flow Completion Duration

The normalized flow completion duration for both S2S-WiDCN and fat-tree DCNs for NC, CES, GRD and *NASCon* consolidation are shown in Fig. 4.6. We observe a similar trend like throughput for all the consolidations. For lower injection rate, the average flow completion time for the wired and wireless network are very similar. The average beam-steering latency is $266\mu s$ for exchange of control information over the control plane is considered while computing the flow completion duration of S2S-WiDCN. The difference in completion time is observed mainly when the average injection rate is higher than 100Mbps representing the multimedia type of traffic. *NASCon* algorithm outperforms all other techniques. With the *NASCon* algorithm, after consolidation, the normalized completion time for both S2S-WiDCN and wired network are improved compared to NC similar to throughput. From Fig. 4.5 and Fig. 4.6 it can be inferred that the impact of network-aware *NASCon* on network-level performance is positive for both wired and wireless DCNs. Therefore, the *NASCon* algorithm can improve both power consumption and network-level performance for both wired and wireless DCNs.

4.2.5 Accuracy of Inter-Consolidation Time Modeling

In this section, the inter-consolidation time for the *NASCon* algorithm is analyzed and the accuracy of the mathematical estimation of inter-consolidation time is evaluated. The expected inter consolidation cost estimated from (4.13) is shown in Fig. 4.8 for a small data center consisting of 800 servers as discussed in 4.2.2.



(a) (b)

Figure 4.9: Comparison of (a) optimal inter-consolidation time (b) actual cost at optimal point from model with actual measurement at different ρ.

To verify the mathematical model for cost of consolidation (4.13), we ran a Monte Carlo simulation for each ρ for three hundred times and calculated the value of the cost function. For these cases, the values for η_1, ν, κ considered here are, 200, 1000 and 1 respectively.

The average of the simulated values from different run for each ρ are shown in Fig. 4.7. The cost estimates in this method relies on many repetitive simulations and is highly computationally expensive as each of simulation at particular ρ and t was repeated at least thousand times to find the expected cost using Monte Carlo method. On the contrary, using (4.13) the cost and optimal inter-consolidation time can be approximated much faster. The optimal inter-consolidation time for different ρ identified from both methods are shown in Fig. 4.9(a). It is observed that for lower values of ρ, ($\rho \leq 0.55$) the optimal inter-consolidation time estimated from the mathematical equation closely approximates the measured value from the Monte Carlo simulation. On the contrary, for higher values of ρ, the optimal inter-consolidation time estimated from the mathematical analysis deviates from the value measured through simulations. However, at higher ρ, absolute value of the cost is less sensitive to the inter-consolidation time which can be observed from Fig 4.9(b) which shows the measured cost at the optimal inter consolidation time obtained from the mathematical model. This shows that although at higher ρ the inter-consolidation time suggested by the model may deviate from the actual optimal interval, the actual cost incurred at this non-optimal interval is not much different compared to that at the optimal interval. Hence the optimal inter-consolidation time can be estimated reasonably accurately from the mathematical form.

Table 4.1: Computational Time for Determining Optimal Inter-Consolidation Time

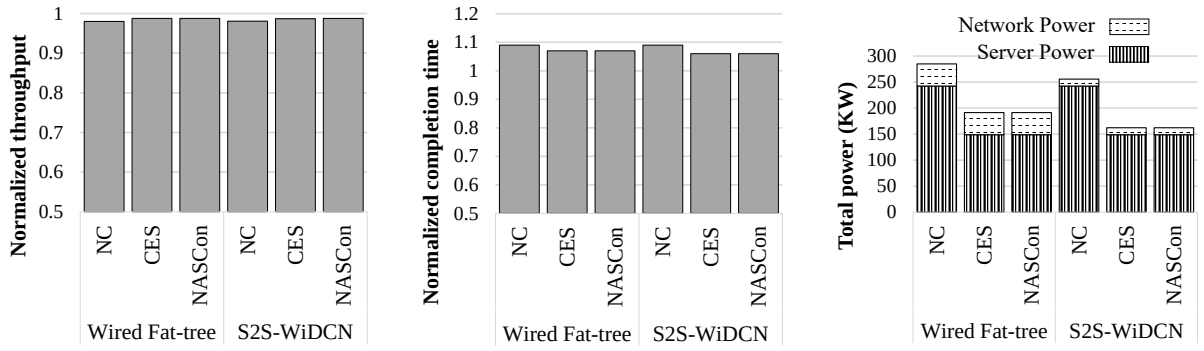
ρ value	Computational time required for Monte-Carlo simulation (seconds)	Computational time required for mathematical model (seconds)
0.25	1043.5	0.813
0.35	1032.4	0.797
0.45	1051.1	0.831
0.50	1029.8	0.772
0.55	1045.7	0.781
0.60	1037.1	0.791

4.2.6 Computation Time of Inter-Consolidation Time

In this section we compare the computation time required to determine the optimal inter-consolidation time from the proposed model with the inter-consolidation time determined from Monte-Carlo simulation. To obtain consistent values, Monte-Carlo simulation were run for one thousand cycles. We used MATLAB R2018b in a workstation having Intel Core i7-7800X with 3.50GHz with 16GB memory in Windows 10 OS to do both the calculations and the results are shown in Table. 4.1 From the table it is observed that identifying the inter-consolidation time from the model achieves a speedup of over 1000× compared to the Monte-Carlo simulations. Therefore, the model can be used in real-time in the data center in conjunction with the scalable *NASCon* heuristics to determine the inter-consolidation time and perform the consolidation periodically.

4.2.7 Consolidation for High-Bandwidth Networks

In recent wired data center architecture, 40Gbps links are becoming more common [105]. Use of optical fibers and advanced switching technologies are responsible for the design of such hi-fidelity data center networks. Although, originally the S2S-WiDCN [77] was proposed using the 60GHz mmWave channel, with 6.67Gbps bandwidth capacity per channel, it is to be noted that the channel capacity is likely to increase in the near future. In fact, in recent works [106], it is showed that by adapting `IEEE802.13.3d` standard for THz communications, 100Gbps wireless links are possible and can be used in data center communication. In this section, we analyze the performance of *NASCon* consolidation mechanism in these high capacity wired and wireless DCNs.



(a) (b) (c)

Figure 4.10: Comparison of *NASCon* and CES consolidation on both wires and wireless network for high bandwidth network data centers with average injection rate of 650Mbps (a) normalized throughput (b) normalized flow completion time (c) total power consumption.

For this comparison, the traffic used had an average injection rate following a Gaussian distribution having the mean of 650Mbps representing high-fidelity video/multimedia applications, which will be one of the dominant applications in the future. For the wireless channels, each 100Gbps channel is assumed to be subdivided into twelve OFDM channels each having 8.33Gbps capacity. For the wired data center, 10Gbps links are considered between servers and access layer switches and 40Gbps links between upper layer switches.

The comparative results for these simulations are shown in Fig. 4.10. It can be seen that with the use of emerging THz wireless communication, the networking bottleneck is not seen at higher injection rates, and wireless network performs equally well as wired network for NC, CES as well as the *NASCon* approach. This is because due to the much higher physical channel capacities (4.3) is not violated very often with consolidation. As seen in Fig. 4.10(c) Due to similar behavior in the wired and wireless networks for both consolidation methods, the reduction in power consumption achieved is also identical as the network-awareness does not alter the outcome of the consolidation unlike previously. However, this scenario may change and the trends observed in the previous experiments could repeat if applications have even higher flow rates than considered here.

4.3 Conclusions

The power consumption of the data center can be drastically reduced by adopting S2S-WiDCN network architecture with *NASCon* server consolidation algorithm. Although *NASCon* server consolidation consumes 2.83% more power compared to CES consolidation technique which involves exhaustive search, it is far less computationally intensive and suitable for real time operation. More-

over, being network bandwidth-aware, *NASCon* does not adversely affect the network performance of the data center whereas for higher bandwidth demanding network, CES can degrade the performance of the network. The network-aware constraint results in higher consolidation in case of the S2S-WiDCN due to the higher link density and diversity compared to conventional DCNs. Due to the arrival of new tasks and completion of existing tasks, the consolidated utilization profile of the servers have a potential to drift from the optimal profile, which ultimately can adversely affect the overall power consumption over time. To overcome this, *NASCon* algorithm needs to be executed periodically. We propose mathematical model to estimate the optimal inter-consolidation time. Using this mathematical model, data center resource management unit can schedule *NASCon* consolidation operation in real time and leverage the benefits of server consolidation.

Chapter 5

Security Vulnerabilities of Server-Centric Wireless Data Centers

Due to the adoption of the upcoming $5G$ technology and network densification, the number of small data centers will rise exponentially in the next few years [107] and S2S-WiDCN can be considered as a great candidate for this field. In addition to the small data centers, S2S-WiDCN can be adopted in large-scale cloud data centers as well due to the high data rates supported by the dense wireless links and highly directional antennas. However, ensuring the security of these data centers providing cloud services is the highest priority as tasks and applications from different organizations run concurrently in such multi-tenant data centers. However, being an emerging technology, no study has yet been done on the security aspect of the S2S-WiDCN whereas security is one of the highest design priorities in any data center.

There are a number of basic fundamentals threats associated with any conventional wireless network like wireless sensor networks or ad-hoc networks. These can be ranging from rogue node, eavesdropping, denial of services, passive capturing of a node, etc. [63,64]. Similar to wireless sensor or ad-hoc networks, having a wireless network architecture, S2S-WiDCN has the potential to inherit many or all of these threats. On the contrary, advantages exist in the security aspects for the wireless data centers because of using mmWave for communication, which is highly directional and has low penetration capability through metal or concrete structures. Therefore, the feasibility of various attack scenarios on an S2S-WiDCN needs to investigated thoroughly along with their potential impacts on data security, integrity, and performance. data center security refers to both the physical practices and virtual technologies used to protect a data center from external or internal threats and

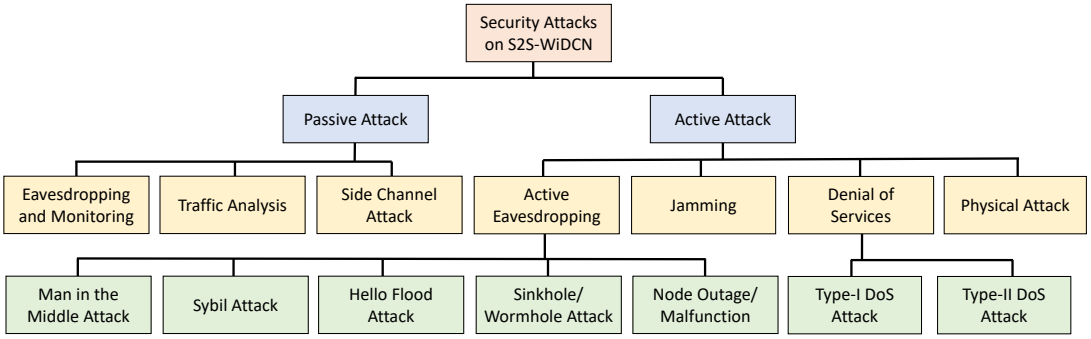


Figure 5.1: Possible attacks on S2S-WiDCN.

attacks. Security of a data center can be divided into two part, i.e. physical security and software security. *Physical Security* is mainly ensured by the robust building structure and layout of the data center and access control mechanism to the building. Most of the data centers do not have exterior windows and relatively few entry points. Access into a data center facility is fairly limited to the personnel directly working in that facility. On the contrary, *software security* is the mechanism to stop the attacker from accessing and altering the data contents of data centers digitally. In this chapter, we have done an in-depth analysis of the possible threats and attacks on the wireless data center network. In addition to analyzing the impact of such attacks on data security, we have measured their impact on the performance of the overall network using a network-level simulator.

5.1 Security Attacks on S2S-WiDCN DCN

As the S2S-WiDCN data center uses wireless links for communication, it may inherit most of the security vulnerabilities of any wireless system. The attacks possible on the DCN can broadly be classified in *active attack* and *passive attacks* [108]. In passive attacks, the attacker monitors and listens to the communication channel by unauthorized means. On the contrary, when the attacker not only listens and monitors, but also modifies the data is called an active attack. In Fig. 5.1 the probable attacks on S2S-WiDCN are classified into passive and active attacks. Passive attacks include eavesdropping and monitoring, traffic analysis, and side-channel attack. On the other hand, the active attack includes active eavesdropping, jamming, denial of services, as well as a physical attack. We argue that other attacks including the man in the middle attack, Sybil attack, hello flood attack, sinkhole/wormhole attack can be broadly classified as some extended version of active eavesdropping attack as all of these involve some sort of unauthorized listening as well as modification of data or data path. Depending on the information leaked to the intruder or severity of the performance compromised, the most significant attacks possible on S2S-WiDCN are eavesdropping, denial of services, and jamming attacks. In the next subsections, details about these attacks are discussed.

5.1.1 Eavesdropping Attack

Eavesdropping is widely considered as one of the most common security threats for any wireless system due to the broadcasting nature of the medium. S2S-WiDCN uses mmWave wireless links for communication which requires LoS between transmitter and the receiver. In, [70], the author showed that despite having highly directional transmission, an eavesdropper can successfully intercept a signal by creating virtual periscope. Nevertheless, as the data center is in a confined environment, we argue that the data security is relatively high as the 60GHz wireless link has an extremely low penetration capability through concrete or brick walls compared to traditional 2.4/5GHz wireless links. This reduces the possibility of an external eavesdropper, but still, there is a potential for an internal eavesdropper, who has access within the LoS of the wireless links. Depending on the involvement of the attacker, an eavesdropping attack possible for S2S-WiDCN can broadly be classified into two types - active eavesdropping and passive eavesdropping. Passive eavesdropping is where the attacker monitors the data and listens to the communication contents. This type of eavesdropping does not introduce any new adversarial effect on the network although privacy can be compromised. This type of attack is extremely hard to detect as it does not alter/modify any network parameters. On the contrary, active eavesdropping includes the attacks where the intruder or the compromised node simultaneously listens to the communication happening in the network as well as alters or obstruct the data. We argue that different types of attacks including- Sybil attack, hello flood attack, wormhole/sinkhole attack, node outage/malfunction can broadly be classified as a subset of active eavesdropping. S2S-WiDCN can be vulnerable to both active and passive eavesdropping.

The attacker can be located inside of the data center premises or outside of the data center premises. Based on the location of the eavesdropper, two types of attack models are possible.

External Eavesdropper

In this scenario, the attacker is located outside of the data center premises as shown as a blue circle in Fig. 5.2. In absence of any obstruction, the wireless power received by the external eavesdropper in free space can be calculated using Friis transmission formula,

$$P_R = \frac{P_T G_T G_R c^2}{(4\pi R f)^2}, \tag{5.1}$$

where P_R represents the power received by eavesdropper's antenna, P_T is the power transmitted by a legitimate server, G_R and G_T represents the respective gain of the receiving and transmitting

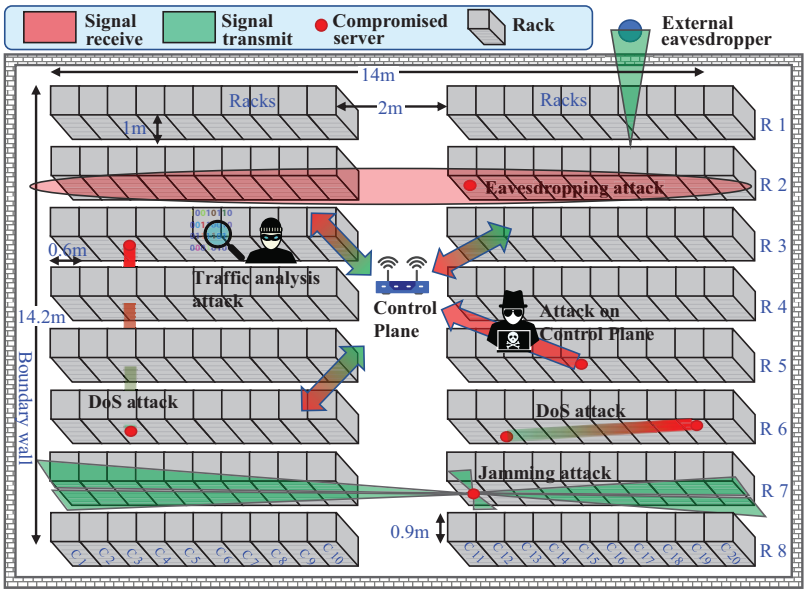


Figure 5.2: Layout of S2S-WiDCN showing different possible attacks

antennas, R represents the free-space distance between the server and the eavesdropper, c is the speed of light and f is the frequency. It is likely that R is significantly high compared to the distance between two servers in the data center. Moreover, the data center is surrounded by brick or metal walls. 60GHz mmWaves are used for communication which has an extremely low penetration capability through brick or metal structures. Both of these facts ensure that the signal power received by the eavesdropper antenna will be extremely low to decode any useful information out of it.

Internal Eavesdropper

Internal eavesdroppers are the eavesdroppers who are located inside of the data center premises. In this attack model, it is considered that servers in the data center can be compromised and can act as an internal eavesdropper. The number of eavesdropping nodes can either be single or multiple. The location of the compromised nodes also can either be random or can be strategically positioned by the attacker. If the attacker is not aware of the geographic layout of the data center while carrying the attack from a remote location, then it is likely that the servers are assumed to be compromised in a random manner. On the contrary, if the intruders are aware of the layout of the data center, they would try to strategically attack those servers which have the potential for highest eavesdropping. From the analysis and simulations done in Section 5.2.3, it was seen that based on the location of the server, eavesdropping capability varies from server to server. We conservatively assumed that whenever the attackers breach into a server, they have access to all traffic passing through it.

5.1.2 Denial-of-Services Attack

Denial-of-service (DoS) attack is a security attack where the attacker seeks to make the network resource unavailable to its intended users temporarily or indefinitely by flooding the target with malicious traffic. A single malicious VM running on a single server can use the network resources to launch a DoS attack which can significantly degrade the network performance while making it harder for the network administrator to identify the cause. The possibility of the DoS attack in the S2S-WiDCN is high if proper measures are not taken, as all the servers can communicate between themselves with one or two hop and multiple possible routes for communication exists between them. In this attack model, it is assumed that if a server is compromised by the attacker, it has a potential to launch a DoS attack by trying to flood the network with high volume malicious traffic with a target to exhaust all the available bandwidth, and make them unavailable for the legitimate traffics.

Sophisticated DoS Attack Model

In a DoS attack, the attacker tries to make the network resource inaccessible to the valid users. The simplest form of DoS attack would be the case where the attacker tries to occupy as many of the OFDM channels as possible to move illegitimate traffic. We define this type of DoS attack as a Type-I DoS attack. Although this type of DoS attack can cause maximum possible instantaneous disruption in the network, this type of DoS attack is relatively easier to detect as the traffic is much more resource demanding than the regular traffic. By observing the traffic profile of the data center, the network administrator or automated tools can identify the servers which are causing the DoS attack. Based on the identification, prompt measures can be taken to mitigate the effect of the DoS attack quickly by isolating the compromised servers. However, another sophisticated form of DoS attack can occur where the malicious flows injected by the DoS server resemble valid data center traffic having a higher flow injection rate, but within the normal distribution of the legitimate traffic of data center. We define this type of attack as Type-II DoS attack [109] as shown in Fig. 5.3. Although this type of DoS attack might not have the same instantaneous adverse effect as Type-I DoS attack, nevertheless it has the potential to reduce the overall performance significantly in the long run. Type-II DoS attacks would be harder to detect as they appear to behave like real traffic. Hence, we argue that, if the attackers have a goal to degrade the performance of the DCN for a long term basis, it is more likely that they would try to launch a Type-II DoS attack. For our analysis, we will observe the effect of Type-II DoS attack.

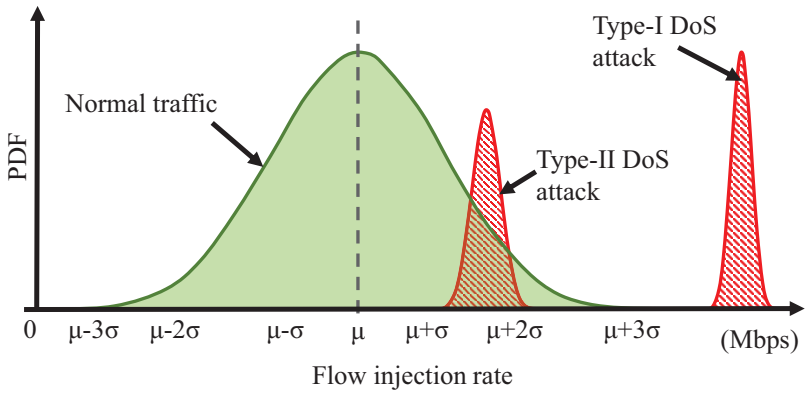


Figure 5.3: Different DoS attack traffic

5.1.3 Jamming Attack

In any wireless system, frequency jamming is always a possible attack against the system. As the communication in the S2S-WiDCN takes place in an open medium, frequency jamming can cause interference with legitimate OFDM channels and cause disruption in the network. Because of the jamming attack, authorized users are unable to access the legitimate traffic by the overwhelming frequencies of illegitimate traffic.

Attack Model

The jamming attack can initiate from an external source or any compromised server inside of the network. As the data center is in a confined environment, it is unlikely that any external jamming source will have any significant effect on the performance of the data center communication as the wireless channels used for the communication utilizes 60GHz which has extremely low penetration capability metal or brick wall. In [110] a brick wall of average thickness was found to have a loss of 28.3dB for 60GHz frequency. The most probable sources of jamming attacks are compromised servers inside of the data center. A single server can transmit in a particular OFDM channel using one of the antenna arrays. Although the antennas in the back-plane of the servers are directional, it can cover full 360^o area with the existence of 6 different arrays as discussed in Section 3.1.1. So it is possible for the compromised rogue server to cause interference for a particular channel and make that channel unusable to other servers in that particular vertical plane utilizing all of the 6 antenna arrays. In some instances, multiple servers can become rogue and jam several communication channels. However, in the extreme case, where the number of the compromised servers in a plane is equal or more than the number of OFDM channels available, there is a potential to jam the entire

communication of that vertical plane.

5.1.4 Attack on S2S-WiDCN Routing Table via Control Plane

S2S-WiDCN has a separate ISM band control plane to exchange the control packets between servers. The control channel utilizes symmetric key based encryption for the security [111]. However, an intruder can capture a server in the DCN, acquire the encryption key and access the control channel. Having access to the control network, then intruder has the capability to tamper the routing table for server-to-server communication, and create severe disruption in the network performance. This type of attack can exclusively occur in S2S-WiDNC architecture which utilizes a separate wireless control plane. Although by modifying the routing table, the attacker can cause full disruption in the data communication, this will raise an immediate red flag, and network administrators can quickly mitigate the problems by reloading a backup copy of the routing table in the system. A more effective attack would be, to modify the routing information of only a few of the nodes from the routing table and keeping the rest unchanged such that the attack stays “under-the-radar". With this approach, although the attacker can cause less disruption on performance, but has the potential to carry out the attack for a long period of time as it would be very hard for the network administrator to figure out the root cause of the degradation of the performance, i.e. whether the cause is an increase in server workload or a security breach. We evaluate the impact of this attack on the performance of S2S-WiDCN.

5.1.5 Side-Channel Attacks

A side-channel attack [112] is an attack based on information gained from the system, through a communication path that is not originally designed as a means of communication. In S2S-WiDCN, possible side-channel attacks include power consumption analysis, electromagnetic radiation detection, which can be exploited by the attacker. Although side-channel attack alone does not harm the system much, the information gained from a side-channel attack can be utilized to carry out other attacks. For instance, a power consumption analysis of the S2S-WiDCN provides the attacker the information about servers which are most active. This information can be utilized to carry out a more effective DoS or malware injection attack. An extension of the side-channel attack is a traffic analysis attack. Traffic analysis is the process of intercepting and examining messages to deduce information from patterns in communication, which can be performed even when the messages are encrypted [112]. In general, the greater the number of messages observed, or even intercepted and

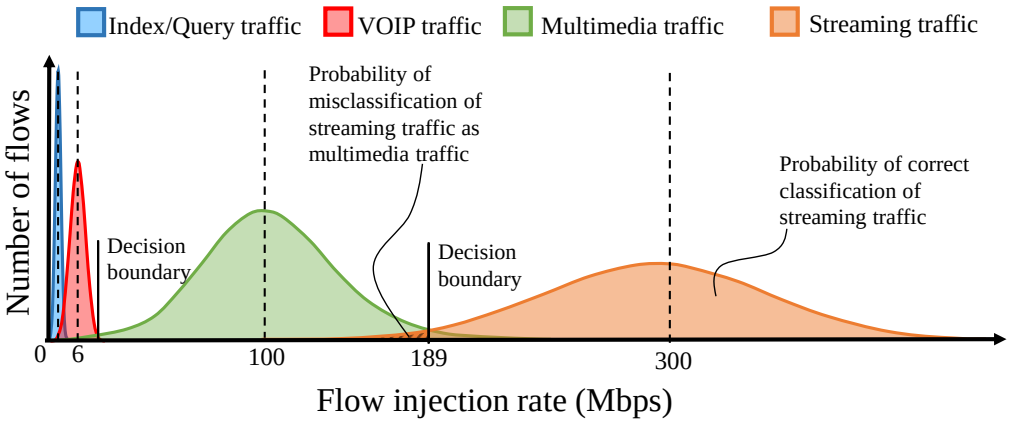


Figure 5.4: Traffic profiles for different type of applications.

stored, the more can be inferred from the traffic. An attacker can utilize an existing server in the data center to carry out a traffic analysis attack. With the rise of MTDC, the threat of a traffic analysis attack become more severe. Specifically, in the S2S-WiDCN each server works also as a relay for packet and data flow forwarding to other servers in addition to being a source and destination. Therefore, in an MTDC scenario, a server can be easily captured by a rogue application simply to perform this traffic analysis attack. If an attacker monitors the traffic activity of a single or few of the nodes in a data center, he/she can acquire significant information about the type of application running on the servers on the data center ultimately compromising the privacy of the user(s).

Effects of Side-Channel Attack through Traffic Analysis

In this attack model, we have assumed that the attacker can carry out a traffic analysis attack in a single node of the data center network. According to [85, 87] different types of applications running on the data center has distinctive traffic profile. In Fig. 5.4 traffic profiles of a S2S-WiDCN data center having 800 servers is shown for different types of traffic, ranging from index/query search [85], VOIP [113] and streaming [87] type of traffic. We assume that the attacker can monitor the flow rates of traffic through a single server an one instance. A single data flow monitored by the compromised server can be used by the attacker to classify the application among known types as shown in Figure 5.4. Many classification algorithms can be employed by the attacker such as simple fixed threshold based vs Machine Learning-based approaches. We demonstrate here, that even a simple threshold-based maximum likelihood classification can have very high classification accuracy in this scenario. For example, the mean flow rates of multimedia and streaming traffic are 100Mbps and 300Mbps respectively with a Gaussian distribution in both [87]. Assuming the

classification threshold to be at 189Mbps (the intersection of two distributions), the probability of misclassifying a single sample from streaming and multimedia traffic would be 3.22% and 2.41% respectively given by the integral of the Gaussian tail on the wrong side of the threshold. However, if the characteristics of the different traffics have similar traits, i.e. mean, standard deviation and shape, identifying accuracy by the attacker will drastically be reduced. The classification accuracy can be further improved by sampling the monitored data over a time window which is then used to compute a sample mean. This sample mean can then be used for classification instead of a single observed flow to increase the probability of correct classification.

If the actual distribution is not Gaussian but more "heavy-tail" skewed and the decision boundary point is inaccurate, the misclassification probability might be significant. That might be so, even if the means of neighboring distributions are far. To accurately estimate the decision boundary, attacker must have an accurate estimate of the low-probability parts of the distributions which may need extended period of time to record. The information obtained from this traffic analysis attack will compromise the user privacy and may help the attacker to carry out more directed attacks.

5.1.6 Man in the Middle Attack

A man-in-the-middle attack (MITM) [114] is an attack where the attacker relays and possibly alters the communications between two communicating nodes, which believe that they are directly communicating with each other. In S2S-WiDCN, the compromised server can carry out a MITM attack, if it falls in the LoS of two communicating servers. An external attacker, who has the physical access inside of the data center can come within the LoS of communication and run a MITM attack. As the S2S-WiDCN uses an ISM band control channel which utilizes 2.4/5GHz wireless frequency, an attacker can try to do a MITM attack in the control channel and provide the servers with false control packet, which ultimately can lead towards disruption in the overall performance of the DCN.

5.1.7 Sybil Attack

Sybil attack [115] is an attack where a single attacking node duplicates itself and presented in multiple locations. A compromised server in S2S-WiDCN can create an illusion by making multiple copies of it having different IDs. In [115], it is shown that with authentication and encryption techniques, the Sybil attack can be prevented in a WSN where the nodes of the network are geographically scattered placed. We argue that as the servers in the S2S-WiDCN are uniformly positioned, and

the angles for the beam-steering are recomputed, it will be unlikely that a Sybil attack can cause much disruption in the communication. Moreover, if the server cannot reach the destination server with a precomputed beam steering angle, the presence of a Sybil attack can be anticipated.

5.1.8 Hello Flood Attack

In the hello flood attack, an attacker sends or replays hello packets containing false routing and resource availability information, which can lead other servers trying to utilize that server for routing. In S2S-WiDCN, the control information for the communication between 2 servers is transmitted over a separate control channel. Hence the possibility of the hello attack is limited only to the control channel, not the mmWave wireless channel.

5.1.9 Sinkhole/Wormhole Attack

When the attacker tried to attract traffic to a specific node is called a sinkhole attack. In this attack, the attacker's goal is to attract as much traffic as possible from a particular area through a compromised server. Sinkhole attacks typically work by making a compromised server look especially attractive to surrounding nodes. In the wormhole attack, attacker attracts data traffic at one location in the network, tunnels them to another location, and re-transmits them into the network. In S2S-WiDCN, both sinkhole and wormhole attacks are possible. A single compromised server can act as the sinkhole which can drop all the traffic passing through it. Multiple compromised servers can carry out a wormhole attack by tunneling the traffic between themselves.

5.2 Modeling, Results, and Analysis

In this section, we discuss modeling, results, and the corresponding analysis of the security aspect of the S2S-WiDCN architecture. Before presenting and analyzing the results we describe the data center traffic model and simulation platform in next subsections.

5.2.1 Data Center Traffic Model and Generation

The performance of the DCN during different security threat is evaluated with a set of traffic flows based on application demands. Real data center traffic for different classes of data centers is

measured in [85]. Using these measured traffic flows, a Poisson shot-noise based model to synthesize data center traffic is proposed and verified in [86]. According to [86], the new flow arrival time, the flow duration, and the injection rate for each application follow a Poisson, Pareto and, Gaussian distribution respectively. The new flow arrival time is generated using a Poisson distribution with an average flow arrival rate. The average flow arrival rate is considered to be 1000 flows/second for the small-sized DCN [85]. Moreover, it has been observed from the measurement of a variety of data centers in [85], a large proportion of the server-to-server traffic flows, up to 80%, are intra-rack, meaning between servers in the same rack. Only a small remaining proportion of about 20% is inter-rack, or between servers in different racks. In our evaluations, we initially have considered a Gaussian distribution for the injection rate to have a mean of 1Mbps as the base case for the simulation. Application flow duration is generated following an independent Pareto distribution having a minimum duration of 10 microseconds [85] and a mean of 1 second. We then increased the average injection rates on an incremental basis to 10Mbps, 100Mbps, 400Mbps, and 650Mbps and regenerated new traffic which represents different types of multimedia traffic and repeat the simulations. In the S2S-WiDCN, there are six separate directional antenna arrays in the vertical plane of the server, and another one array on the top of the server. Therefore, seven simultaneous links from a server can co-exist at the same time.

5.2.2 Simulation Platform

We use the NS-3 suite [84] and MATLAB to evaluate the performance of the S2S-WiDCN networks in presence of eavesdropping, DoS, and jamming attack. NS-3 supports the characteristics of wireless propagation as well as network-level communications. It is important to simulate both the propagation and network-level communication characteristics accurately in order to obtain credible performance results. A modified version of NS-3 extended with features of wireless data center including the 60GHz band and the `IEEE802.11ad` standard as discussed in [12] was used for this simulation. This extension incorporates interference modeling, bit error rates, and directional antenna modeling. The accuracy of these parameters is verified with physical layer measurements of prototype 60GHz hardware [12]. Additionally, we introduce criteria for wireless link selection to enable many concurrent links and modify the `IEEE802.11ad` physical layer to allow multiple OFDM channels. This simulation platform is used to evaluate the S2S-WiDCN and compare it with the fat-tree wired DCN as well as ToR-ToR WiDCN architectures. For the fat-tree based wired data center architecture, we have considered 1.0Gbps links between servers to access switches and 40.0Gbps upper-layer links. We have considered a small data center consisting of 800 servers arranged in a 20×8 array of racks as [77]. Each of the rack houses 5 servers and occupies an area of $0.6m \times 0.9m$

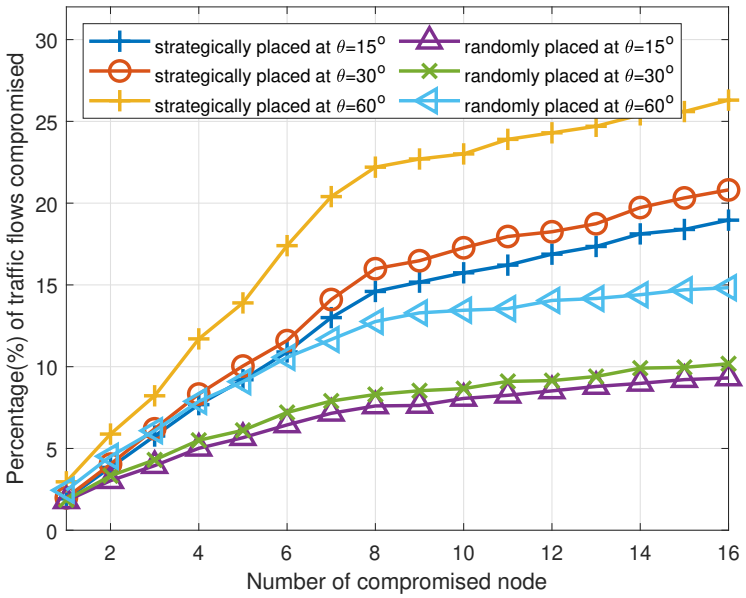


Figure 5.5: Percentage of communication compromised due to eavesdropping with the number of compromised node

and is $2m$ high. There are 10 racks arranged in a single row and two columns of 8 rows, totaling 160 racks. In our simulations, the racks are assumed to be without any front or back door. In the traditional wired fat-tree based DCN, we have considered the same number of servers arranged in the same layout as S2S-WiDCN. We have considered 3 hierarchical network layers consisting of 160 access, 2 aggregate, and 1 core layer switch, where each rack has an access layer switch.

5.2.3 Performance Evaluation and Analysis

In this subsection, we evaluate the performance of the wireless data center during eavesdropping attack, DoS attack, jamming attack, attack on control plane and traffic analysis attack.

Effect of Internal Eavesdropper

Security vulnerability due to randomly positioned compromised servers: In this attack model, the attacker captures the servers in the data center in random order and utilizes them as eavesdropping node. The assumption here is that the attacker is unaware of the geometric position of the servers, and hence unable to identify the servers which have the maximum potential for eavesdropping. Furthermore, the attacker can capture multiple servers at the same time, but in random order. To determine the severity of the eavesdropping, we use the percentage of the total

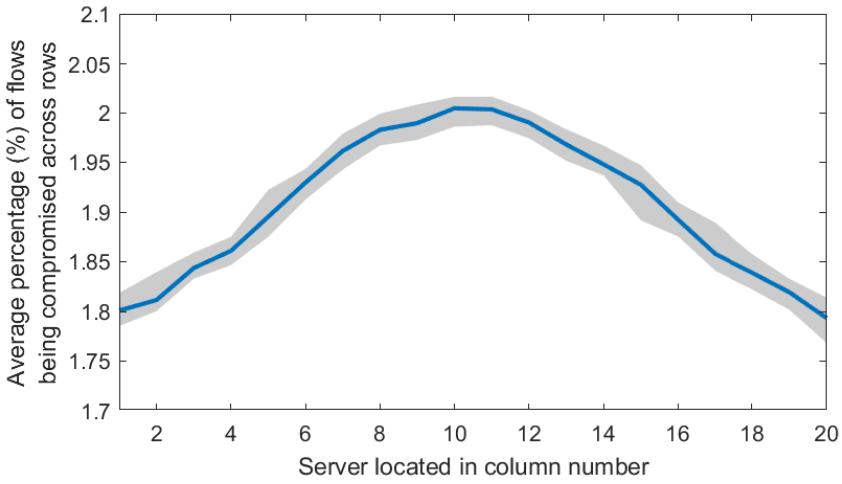


Figure 5.6: Average percentage (%) of flows being compromised by server located in column number with range.

flows that are exposed to the eavesdropping nodes as a metric for measurement with respect to the number of compromised servers. We generated the traffic for hundreds of times and run Monte-Carlo simulation to measure the effect of the eavesdropping due to the randomly positioned compromised nodes. We observed the effect of the eavesdropping for 3 different types of antenna arrays each one capable of achieving $\theta = 15°$, $\theta = 30°$, and $\theta = 60°$ beam-width used by the servers in the data center respectively. To determine whether a flow is compromised or not, we only use the primary lobe of the radiation pattern as it contains the maximum radiation energy. The results are shown in Fig. 5.5. From the results, it is observed that with the increase in the number of compromised nodes, the percentage of traffic flow being compromised increases for all beam-widths. However, the rate of increase in flows being compromised reduces as the number of compromised nodes increases. The main reason behind this phenomenon is, as the number of the compromised node increases, the probability of a few nodes ending up in a single rack increases resulting in marginal benefit to the eavesdropper. Furthermore, when the beam-width is narrow (15°), the total amount of traffic compromised is about 60% of the compromised traffic for wide beam-width (60°) antenna.

Security vulnerability due to strategically positioned compromised servers: In this model, the assumption is that the attacker is aware of the geometric position of the servers in the data center, and hence know the suitable spatial location of the server for maximizing eavesdropping capability. For a single vertical plane, we observed that servers in the central racks have the potential to intercept the highest amount of traffic flows compared to other servers in that plane as seen in Fig. 5.6. Hence, having this information, the attacker will try to position the eavesdropping node in this location. While capturing the next server, the attacker will try to capture a server in a different vertical plane. As there are 8 rows, and hence 8 vertical planes in the considered data

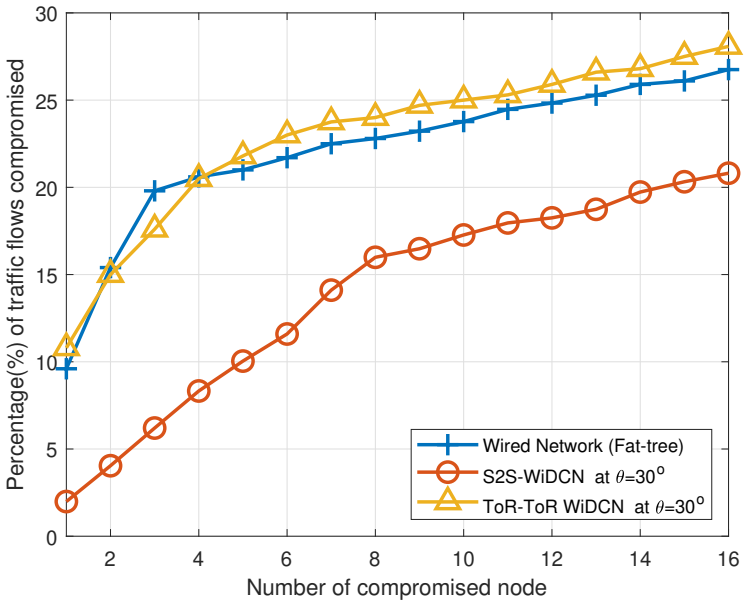


Figure 5.7: Effect of eavesdropping on different DCN architecture with the number of compromised node

center, the attacker will first strategically capture 8 servers in separate vertical planes. We use the same Monte-Carlo simulation used in the previous subsection to measure the effect of the eavesdropping for this type of attack model. Again, we observed the effect of the eavesdropping for 3 different types of antenna arrays each one capable of achieving 15°, 30°, and 60° beam-width respectively. The results are also shown in Fig. 5.5. It is observed that with the strategically positioned nodes the attacker can have access to up-to double amount of flows in the network compared to randomly captured nodes. The rate of flows being compromised per additional captured node decreases after the number of the compromised nodes goes beyond 8. This is due to the fact that after 8th node, the next captured nodes will be on a vertical plane already having a compromised node. Another observation is that, like randomly positioned nodes, if the antenna used has a beam-width of 60°, up to 33% more flows can be captured by the eavesdropper compared to the antennas having narrow beam-width of 15°.

Comparison of the effect of eavesdropping between wired-DCN, ToR-ToR WiDCN and S2S-WiDCN with the number of strategically positioned compromised nodes In this subsection, we compare the effect of eavesdropping in different data center network architectures for strategically positioned compromised node. In Fig. 5.7 the Comparison of the effect of eavesdropping between wired-DCN, ToR-ToR WiDCN, and S2S-WiDCN with the number of strategically positioned compromised nodes is shown. For the wired network, we considered the fat-tree archi-

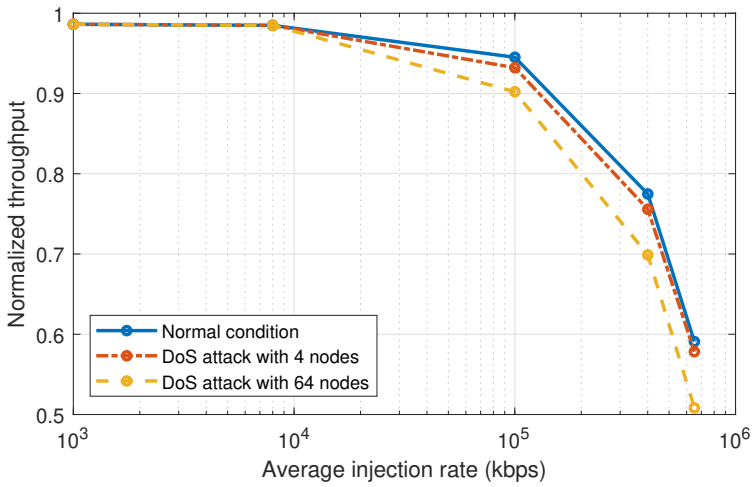


Figure 5.8: Effect of DoS attack on S2S-WiDCN

tecture as it is the most widely used DCN architecture in the industry. In the fat-tree network, the highest percentage of the traffic passes through the different higher layer switches. Hence, if the attackers can capture one or a few of the top-layer switches (i.e. core and aggregate layer), they have the potential to intercept the maximum amount of traffic.

Similarly, for the ToR-ToR WiDCN network, most of the traffic passes through the access layer switches. Hence, if the attacker can capture the access layer switches, there is a potential to intercept the highest amount of traffic. On the other hand, in S2S-WiDCN, most of the communications happen in a single hop, directly between two servers. As there are no switches in this architecture, to enable the communication which requires intermediate node, all the servers in the data center have the equal capability to become an intermediate node. The traffic through every server is approximately similar. Hence, even strategically positioned nodes can intercept only a fraction of traffic compared to the fat-tree or ToR-ToR WiDCN networks.

Security Vulnerability due to DoS Attack

With the DoS attack, the attacker tries to hamper the performance of the data center or disrupt the entire network. As discussed in Section 5.1.2, we have done this analysis for the Type-II DoS attack. We consider two different scenarios having 4 and 64 compromised servers carrying out DoS attack in the data center respectively. For each case considered, all the compromised servers are assumed to be in a single vertical plane. The compromised server transfers traffic with the injection rate equal to the 90th percentile injection value of the normal traffic. We measured the average throughput of the entire network, with and without the DoS attack. We then increased the average injection rates on an incremental basis from $1Mbps$ to $10Mbps$, $100Mbps$, $400Mbps$, and $650Mbps$

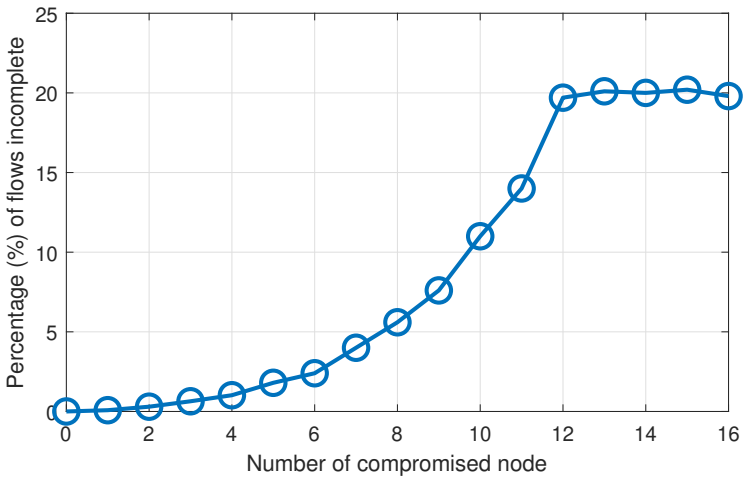


Figure 5.9: Effect of jamming attack with the number of compromised servers on a single vertical plane

and regenerated new traffic which represents different types of multimedia traffic and repeats the simulations. The results are shown in Fig. 5.8. At a lower average injection rate up to $10Mbps$, the Type-II DoS attack does not affect the throughput significantly. At a higher average injection rate beyond $100Mbps$, up-to 9% degradation in the overall throughput in DCN is observed for a 64 node DoS attack.

Security Vulnerability due to Jamming Attack

A single compromised server can cause jamming to a single OFDM channel for an entire vertical plane. However, due to the existence of multiple OFDM channels, the rest of the communication can take place with the remaining OFDM channels. However, the performance of the network will be adversely affected due to the jamming attack. Few of the communications will remain incomplete due to the unavailability of enough OFDM channels. As the number of compromised servers increases, more of the remaining OFDM channels become unusable due to the jamming at different frequencies. Fig. 5.9 shows the percentage of the incomplete flows of communication due to jamming caused by different numbers of compromised servers in a single vertical plane. It is observed that with the jamming of the first channel, only 0.08% flows are affected. Nevertheless, with the increase of the number of compromised servers per plane, the number of incomplete flows increases in incremental order. Whenever the number of compromised servers exceeds the number of available OFDM channels, twelve, in this case, the entire communication fails for that particular plane. It is also to be noted that, jamming caused by a rouge server in a particular vertical plane does not affect the communication in any other vertical place as the metal racks of the servers create a shield for the communications between any adjacent vertical planes as seen in Fig.3.1.

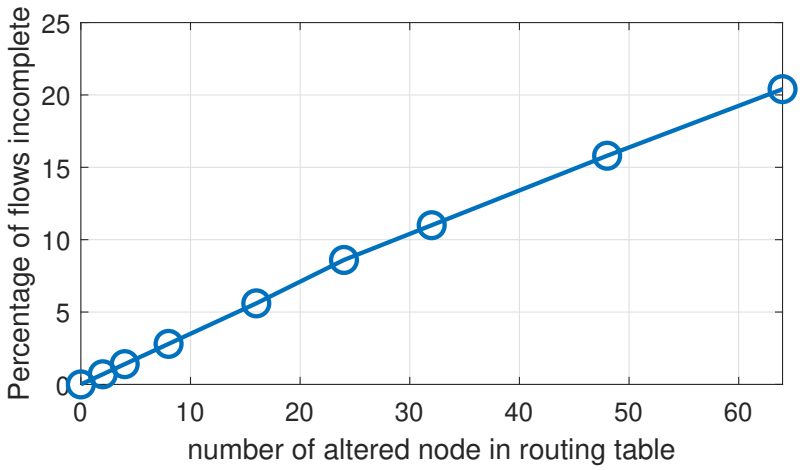


Figure 5.10: Effect of modifying the routing table by attacking the control plane.

Effect of Attack on the Control Plane

In Fig. 5.10 we present the effect of the attack on the control plane on the S2S-WiDCN. From the figure, it can be seen that as the number of nodes affected in the routing table increases, the percentage amount of the failed communication flow increases. When the attacker modifies the routing information of a server in the routing table, all the flows originated from and destined to that server are likely to fail as the route set-up by the control plane is different from the actual possible path. The flows which try to use that server as an intermediate node for communication will also have the potential to fail. As all the servers have similar traffic load, the percentage of incomplete flows increases almost linearly with the number of affected nodes in the tampered routing table. It is also to be noted that if the number of modified nodes becomes high, the percentage of flows that fail will increase significantly high, which will generate an obvious red flag to the network administrator, who can take immediate action to mitigate the attack. Hence if the attackers want to be undetected “under-the-radar", they can modify only a few nodes in the routing table.

5.3 Discussion on Probable Solutions

Defense against Eavesdropping Attack

In any wireless system, it is very hard, if not impossible to eliminate the possibility of a eavesdropping attack. Being in a confined environment having metal or concrete walls, the possibility of attack from an external eavesdropper reduced drastically compared to an internal eavesdropping attack. Due to the utilization of directional beam-forming, an internal eavesdropping node must be placed within

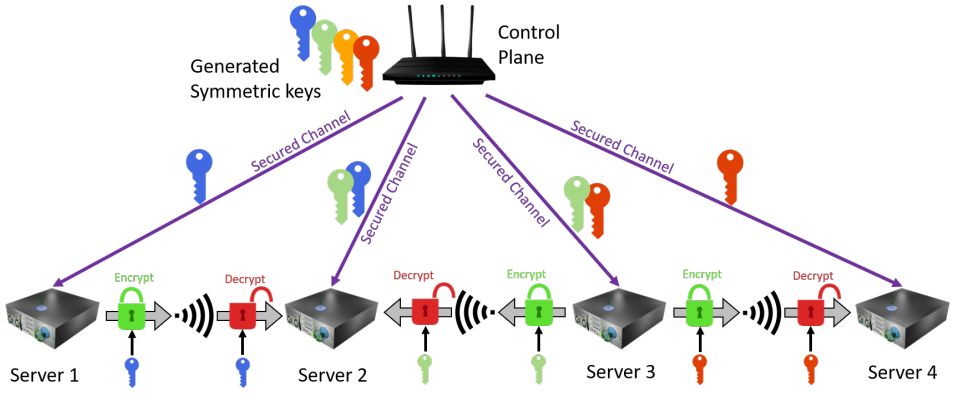


Figure 5.11: Symmetric key encryption and key exchange mechanism in S2S-WiDCN.

the LoS of a communication link to intercept any communication. Nevertheless, any rouge server can act as an eavesdropping node in the data center. This is more applicable in Multi-tenant data centers (MTDC) where a single physical data center is shared by multiple users from different organizations. Encryption is one of the most accepted and effective solutions against eavesdropping in the industry. We propose to utilize a strong symmetric key encryption i.e. $AES192$ or $AES256$ for the server to server direct communication. Different unique symmetric key will be used for the communication between any pair of servers. These keys are managed and generated by the control plane. The control plane utilizes a secured ISM band for communicating with the servers. The control plane shares the symmetric key for the encryption with the corresponding servers before communication and refreshes the keys after some predefined time intervals. Because of the existence of an already secured communication channel between the servers and the control plane, there is no need for a more complicated and computationally expensive key-exchange mechanism involving public-private key like Diffie-Hellman key exchange. The symmetrical key required for encryption/decryption can be shared with the corresponding servers during the control packet transferring for beam-steering as shown in Fig. 5.11. If the total number of servers in the DCN is n, then the control plane needs to generate a total $\binom{n}{2}$ of unique symmetric per time interval.

Defense against DoS Attack

It is well accepted that defense against a DoS attack involves three main steps - attack prevention, attack detection, and attack response [116]. For preventing the DoS attack, rigorous authentication mechanism can be adopted for the servers in the data center network. This limits any possibility of an external node to carryout a DoS attack on the S2S-WiDCN. However, a server inside the data center can become rouge and initiate a DoS attack. DoS attack detection process is differentiating between the legitimate traffic and the attack traffic. All the servers in the S2S-WiDCN need to

communicate with the control plane via control packets prior to any high-speed communications. By analyzing these control packets information, the control plane can maintain a traffic profile of the entire data center for a more extended period of time. If any of the rouge servers try to carry out a Type-I DoS attack, there will be a sudden spike in traffic requests, which can be cross-matched with the typical traffic profile. A short time burst in traffic might be cause by legitimate traffic, but if the spike persists for a long time, it would be a good indication of a potential DoS attack. Based on this, a flag may be raised, and the network administrator can take proper measures to mitigate the attack. As the control plane maintains the updated network parameters for every server in the data center, using this data, identifying the rouge node should not be difficult. The access to the high-speed network for the identified rouge server can be rescinded to isolate the DoS attack entirely.

Defense Against Jamming Attack

In S2S-WiDCN architecture, 60GHz wireless frequency is used with high directional antenna arrays, which are very sensitive to physical blockage. So any jamming attack carried out with any practical transmitter from a particular point inside of the data center is highly unlikely to cause disruption in all the communication happening at that frequency level in the data center, rather can cause failure in any particular plane or horizontal line. Moreover, S2S-WiDCN used multiple OFDM channels for communication and any jamming attack is unlikely to jam all the available OFDM channels. If any of the communication attempt fails due to jamming, the servers can try to utilize remaining OFDM channel until all of them are exhausted. In an unfortunate event where all of the OFDM channels are jammed or occupied due to a jamming attack in any particular plane or a horizontal line, the existence of high path diversity can be utilized to mitigate effect of jamming attack. Instead of the default *horizontal-first routing* algorithm, some other adaptive routing (i.e. *obstruction avoidance routing* [77]) can be adopted to reroute the communication avoiding the jammer.

Defense Against Attack on the Control Plane

With the attack on the control plane, the attacker can alter the routing table of the communication which can cause disruption in the communication in the data center. The attacker can try to stay “under-the-radar" by altering only a few nodes in the routing table and can cause long-term disruption. Hence, detecting whether an attack on the control plane already exists in the data center would be the utmost importance in the defense against this kind of attack. To identify whether this

attack exists or not, the control network can pair up all the servers in the network into groups of two. Each of the pair will exchange some test package between them. All the servers will report an acknowledgment of a successful receipt of the test package to the control plane. Receiving an acknowledgment about a servers test packet being received guarantees the information about that server in the routing table is correct. If the control plane fails to receive acknowledgment about any of the servers, a red flag may be raised, based on that, the network administrator can take action to mitigate the attack. Control plane will carry out this operation periodically. In each iteration, the pairing up of the nodes will be done randomly to ensure the integrity of the mechanism when multiple nodes are captured by the attacker.

Proposed Defense Mechanism for Traffic Analysis in S2S-WiDCN

In the traffic analysis, if an attacker can capture some data from the surrounding wireless communication going through the attacker node, even without having the proper decryption key for that particular communication, he/she can estimated the nature/type of the communication by comparing the traffic profile with some known type of traffic. The proposed defense mechanism against the traffic analysis attack, is based on obfuscating the traffic analysis mechanism by introducing controlled randomness in the routing of the communication between servers. The underlying principle is that with deterministic horizontal-first routing is S2S-WiDCN, the number of packets through a particular node/server is highly correlated to the application producing those packets. Alternatively, if the routing is made totally based on a random walk, the number of packets through any particular switch is essentially become random, losing predictable correlation with the underlying system parameters. However, completely random routing is shown to increase latency and potentially may never reach the destination, hence negatively impact the performance of the entire data center communication. Here we propose a distributed random routing for S2S-WiDCN based on Simulated Annealing (SA) heuristics [117].In this mechanism, SA is utilized not to identify the optimal path, rather to randomized the next hop during the path discovery for a flow. SA based random routing methodology enable a degree of control over the randomness of the routing decisions. In SA heuristic, at the beginning of the annealing schedule, the probability of taking random non-optimal decisions are higher. However, the probability of accepting random non-optimal solutions decreases as the temperature is reduced according to the annealing schedule. Similar to the SA, in the proposed routing algorithm, initially the probability of selecting a random intermediate node during communication is high and decreased over the lifetime of the communication. Hence, implementing the SA based routing will make the maximum number of hops during communication higher than 2-hop if default horizontal-first routing was used. The probability of taking a random

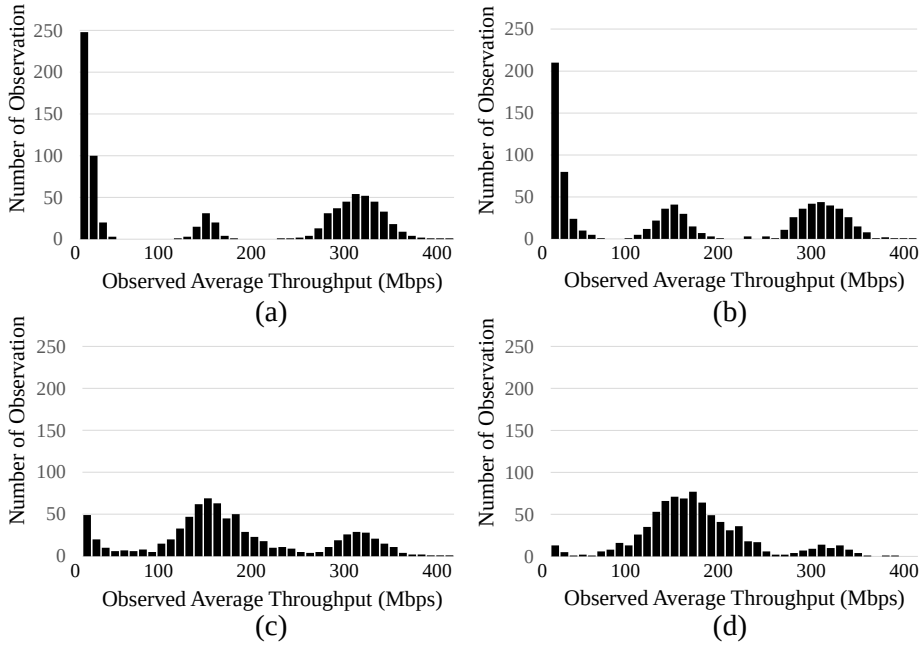


Figure 5.12: Traffic profile of the S2S-WiDCN running only VOIP and streaming type of traffic with (a) default Horizontal routing (b) SA based routing with $\alpha = 10$, (c) SA based routing with $\alpha = 0.1$, (d) SA based routing with $\alpha = 0.01$

node for the next hop is defined as,

$$cR_i = e^{\alpha(T_i - T)}, \tag{5.2}$$

where, T_i is the initial injection time and T is the current time. Here α is a design parameter that governs the degree of randomness. High value of α makes the routing more deterministic and make the traffic profile in the data center more like the default traffic profile with horizontal-first routing algorithm. On the other hand, a lower value of α makes the route selected for the communication more random and the traffic profile of the data center gets altered compared to the profile with the horizontal-first routing algorithm. The number of hops per application increases with decreasing the value of α.

To observe the effect of traffic analysis based side channel attack, we considered a S2S-WiDCN with 800 servers running only two different types of application, half running VOIP applications and other half running streaming applications having average injection rate of 10Mbps and 300Mbps respectively. We simulated the data center traffic for three different values of $\alpha = 10$, 0.1 and 0.01. In Fig. 5.12 the traffic profiles for the different scenarios mentioned above are shown with respect to the average injection rate observed per server. From the traffic profile of default horizontal-first routing shown in Fig. 5.12(a) two very distinctive peaks can be seen around 6Mbps and 300Mbps. Any attacker having prior knowledge about the traffic profile can predict the type of application

running with a high degree of accuracy. When SA based routing algorithm is adopted, in Fig. 5.12(a) $\alpha = 10$, the traffic profile is still very similar to the default traffic profile because of the low probability of randomness. However, as the α decreases and the degree of randomness in route selecting increase, the traffic profile becomes much different compared to the default traffic profile (Fig.5.12 (c) and (d)). In these cases, as the average number of hops involved for each flow increases, every server in the DCN has higher probability to pass both type of application through it during the time of communication. The average number of hops per flow is 1.174, 2.341, and 4.212 for the respective values of α of 10, 0.1, and 0.01. Any attacker having the access to the raw traffic passing through any server will observe a different traffic profile compared to original traffic profile with default routing mechanism hence, unlikely to predict the type of application running on the servers. For instances, for the default routing mechanism, if a simple threshold based maximum likelihood classification is adopted, the possibility of wrongly identifying a multimedia traffic as VOIP traffic is less than 9% whereas the probability of wrongly classify a VOIP traffic as multimedia is less than 2%. On the other hand with SA routing at $\alpha = 0.01$ the probability of wrongly identify multimedia traffic as VOIP is about 52% and VOIP traffic as multimedia traffic is 48%, which is almost equivalent to random guessing.

5.4 Summary

Due to the awareness of environmental sustainability, energy efficiency has become a major focus during design and construction of a modern data center. As S2S-WiDCN architecture has the capability of reducing the power consumption of the data center network significantly over its wired counterparts, it is considered as a definite option. Nevertheless, to become a practical and viable solution for data center network design, the security aspect of the DCN has to be ensured. S2S-WiDCN data center can be vulnerable to a variety of different attacks as it uses wireless links over an unguided channel for communication. In this chapter, we have shown that for S2S-WiDCN, eavesdropping, denial of services, jamming attacks, attack on the control plane and traffic analysis based side-channel attacks are the most critical security threats. We showed that eavesdropping attacks can be addressed by symmetric key-based encryption. Because of the existence of a secured control channel, symmetric key for the communication can be exchanged without the need for additional private-public key based key-exchange mechanism which ultimately does not effect adversely on the overall network performance of the data center. DoS attack is another possible attack on the S2S-WiDCN if any of the servers in the network become rogue. We showed that control packets sent by the servers on the control plane can be analyzed to detect whether any DoS attack exists and

based on that, attack initiating nodes can be isolated to mitigate the attack. The frequency jamming attack on the S2S-WiDCN network can be addressed with the existence of high path diversity in this architecture. An attack on the control plane to alter the routing table of the communication is possible in S2S-WiDCN. With periodical pinging between two random pairs of servers, this type of attack can be detected. To address the traffic analysis attack, a simulated annealing based random routing mechanism can be adopted instead of optimal *horizontal-first routing*.

Chapter 6

Conclusions and Future Works

This chapter concludes this dissertation by summarizing the significant contributions of this research. Furthermore, based on this dissertation, some possible future research directions have also been discussed later in this chapter.

6.1 Conclusions

The challenges in current DCN's are high design and maintenance cost, colossal power consumption, high cabling complexity, hard to keep accurate per-cable information and inefficient cooling. Structured cabling bundles incur significant initial effort and expense to set up and still may cause airflow blockage. Moreover, due to the awareness of environmental sustainability, energy efficiency has become a major focus during the design and construction of a modern data center. All these challenges can be overcome by adopting the proposed completely wireless server-to-server DCN architecture S2S-WiDCN. S2S-WiDCN provides comparable flow completion duration and throughput to a conventional fat-tree based DCN for query/response and multimedia/video based applications. S2S-WiDCN has the potential to reduce the power consumption of the data center network order of magnitude compared to a conventional fat-tree network. But S2S-WiDCN architecture, on its own, does not address the power consumption of the servers in a data center which contributed most towards the total power consumption of the data center.

To address the high power consumption of the servers of the data centers due to over-provisioning, we proposed a network-aware server consolidation technique, namely *NASCon*. The power consumption

of the data center can be drastically reduced by adopting S2S-WiDCN network architecture with *NASCon* server consolidation algorithm. Although *NASCon* server consolidation consumes 2.83% more power compared to exhaustive search based consolidation technique, but it is far less computationally expensive and suitable for real time operation. Moreover, being network bandwidth-aware, *NASCon* does not adversely affect the network performance of the data center, whereas for higher bandwidth demanding network, exhaustive search based consolidation can degrade the performance of the network. Due to the arrival of new tasks and completion of existing tasks, the consolidated utilization profile of the servers has the chance to drift from the optimal profile, which ultimately adversely affect the overall power consumption of the data center over time. To overcome this, *NASCon* algorithm needs to be executed periodically. We propose a mathematical model to estimate the optimal inter-consolidation time. Using this mathematical model, data center resource management unit can schedule *NASCon* consolidation operation in real time and leverage the benefits of server consolidation.

Nevertheless, to become a practical and viable solution for data center network design, the security aspect of the DCN has to be ensured. S2S-WiDCN data center can be vulnerable to a variety of different attacks as it uses wireless links over an unguided channel for communication. In this paper, we have shown that for S2S-WiDCN, eavesdropping, denial of services, jamming attacks, attack on the control plane and traffic analysis based side-channel attacks are the most critical security threats. We showed that eavesdropping attacks can be addressed by symmetric key-based encryption. Because of the existence of a secured control channel, symmetric key for the communication can be exchanged without the need for additional private-public key based key-exchange mechanism which ultimately does not effect adversely on the overall network performance of the data center. DoS attack is another possible attack on the S2S-WiDCN if any of the servers in the network become rogue. We argue that control packets sent by the servers on the control plane can be analyzed to detect whether any DoS attack exists and based on that, attack initiating nodes can be isolated to mitigate the attack. The frequency jamming attack on the S2S-WiDCN network can be addressed with the existence of high path diversity in this architecture. An attack on the control plane to alter the routing table of the communication is possible in S2S-WiDCN. With periodical pinging between two random pairs of servers, this type of attack can be detected. To address the traffic analysis attack, a simulated annealing based random routing mechanism can be adopted instead of optimal horizontal-first routing.

6.2 Future Directions

6.2.1 In the Realm of Tera-Hertz Communication

Tera-Hertz communication is emerging lately as an possible option for communication where high speed and low latency is required. In few of the recent works, the possibility of the 300 GHz is explored as an option for the rack-to rack communication in the data center [106] which showed promising results. In this paper the authors have characterized the tera-hertz channels for different conditions, including line-of-sight (LoS), obstructed-LoS (OLoS), reflected-non-LoS (RNLoS). These links can be extended for the communication inside of the racks for intra-rack communication between the servers in a single rack. 300 GHz channel has the potential to reduce the communication latency further into the sub micro seconds which is very lucrative for data centers which handles high volume data applications such as streaming or file hosting. In [118], the authors have envisioned that beyond the 5G, 6G will enable the terahertz communication which can sustain 400 Gbps datarate which seems very promising for a wireless data center in the future. S2S-WiDCN can leverage these communication technologies with or without some modification to serve the future demand of the data centers. Further extensive study is required to do the feasibility study of the terahertz links in the S2S-WiDCN environment.

6.2.2 High Density Data Center for Future Smart World

Due to the rise of internet of things (IoT) and related technologies, more and more devices are having the capability of connecting to the network and internet [119]. Traditional concept of having a single large data center to serve a mass population will not be able to sustain the requirement of future IoT devices ranging from smart home devices, personal fitness monitoring trackers, augmented reality (AR) and virtual reality (VR) capable devices and many more as shown in Fig. 6.1 Billions of devices will require high speed low latency connection links with the cloud simultaneously which is not sustainable for traditional tiered based network connections. A proper ecosystem will be required to enable scalable, agile infrastructures to serve these high number of connections. Such systems will have widely varying requirements on end-to-end latency, throughput, energy efficiency, security and privacy. Rather than having a large concentric data center, smaller distributed data center closer to the end users will become a norm. These smaller data centers are required to have strong backbone network connections between them. In densely populated cities, wireless will become most viable option for maintaining these back-end connections.

Figure 6.1: High density data center network for future smart city.

For the applications which require extremely low latency, edge computing is becoming a favorable solution for them [120]. As most of the data is being generated in the edge of the network, to transfer them to cloud for processing is very inefficient and slow with unpredictable latency. In these cases, if the data can be processed in the edge node directly connected to the device would be most efficient. As we are moving towards the future, the network distance between the user and end servers is becoming closer. This will accelerate the deployment and development of emerging 5G [121] and even 6G [122] communication technology. We envision a future world where every citizen will have digitally enhanced life with digital assistants, robotic assistants, AR/VR assistance, smart healthcare devices and connectivity. To enable this type of a world we envision pervasive existence of data centers in the sense that data centers will be found in every building or perhaps even in every room. This needs to come with scalable interconnection possibly using the 5G/6G infrastructure as a backbone, that requires little to no time in infrastructure set up. Moreover, the connectivity with mobile end users (MEUs) needs to be reconfigurable and programmable to achieve ad-hoc yet reliable connections on-demand. This leads us to envision a spectrum of computing infrastructure per user, spanning ultra-high capacity cloud with lightning throughput to ultra-low latency forward edge servers with multiple tiers in between, eventually blending into a continuum of nodes instead of a pre-defined or pre-determined number of tiers. Such infrastructure of the future should have the ability to provide compute and storage on-demand at demanded speed, privacy and security levels without the active involvement of the user relying on the infrastructure intelligence to provide this seamless support to the digital lifestyle of the user in a smart world.

The ideal scenario in the future would be the case where the user will be able to connect directly to the servers without any intermediate node for the best latency performance. This can be possible if

the servers in distributed data centers have high-speed wireless capability. Users can get connected to the intended servers directly without going through any intermediate switches. Future research will be required to develop such protocol which can handle this type of direct links between end user and servers. Furthermore, potential use of intelligent massive Multiple Input Multiple Output (MIMO) systems to establish ad-hoc on-demand inter-connectivity between MEUs and servers potentially bypassing a gateway-like architecture common in today's servers to eliminate bottlenecks. Finally, it will be required to create integrated computation and communication systems, architectures and devices to remove barriers between computer and communication devices, providing seamless support to users.

Bibliography

[1] E. Masanet, A. Shehabi, N. Lei, S. Smith, and J. Koomey, "Recalibrating global data center energy-use estimates," *Science*, vol. 367, no. 6481, pp. 984–986, 2020.

[2] A. Shehabi, S. J. Smith, D. A. Sartor, R. E. Brown, M. Herrlin, J. G. Koomey, E. R. Masanet, N. Horner, I. L. Azevedo, and W. Lintner, "United states data center energy usage report," Tech. Rep. LBNL-1005775, LBNL, 2016.

[3] D. Abts, M. R. Marty, P. M. Wells, P. Klausler, and H. Liu, "Energy proportional datacenter networks," *SIGARCH Comput. Archit. News*, vol. 38, p. 338–347, June 2010.

[4] M. Chen, H. Jin, Y. Wen, and V. C. M. Leung, "Enabling technologies for future data center networking: a primer," *IEEE Network*, vol. 27, no. 4, pp. 8–15, 2013.

[5] M. Pedram, "Energy-efficient datacenters," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 31, no. 10, pp. 1465–1484, 2012.

[6] J. Qin, L. Zhang, L. Zhang, and Y. Wang, "Analysis of factors in phase array antenna and rf units on system performance of the ofdm phy of IEEE 802.11ad standard," in *2016 IEEE Int. Conference on Electron Devices and Solid-State Circuits (EDSSC)*, pp. 322–325, Aug 2016.

[7] E. Baccour, S. Foufou, R. Hamila, and M. Hamdi, "A survey of wireless data center networks," in *2015 49th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, March 2015.

[8] K. Ramachandran, R. Kokku, R. Mahindra, and S. Rangarajan, "60ghz data-center networking: wireless=> worryless," tech. rep., NEC Technical Report, 2008.

[9] "Analog devices HMC6300 60 GHz millimeterwave transmitter datasheet." `http://www.analog.com/media/en/technical-documentation/data-sheets/HMC6300.pdf`. (Accessed on 04/04/2021), [Online].

[10] "Analog devices HMC6301 60 GHz millimeterwave receiver datasheet." `http://www.analog.com/media/en/technical-documentation/data-sheets/HMC6301.pdf`. (Accessed on 04/04/2021), [Online].

[11] S. K. Reynolds, B. A. Floyd, U. R. Pfeiffer, T. Beukema, J. Grzyb, C. Haymes, B. Gaucher, and M. Soyuer, "A silicon 60-ghz receiver and transmitter chipset for broadband communications," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 12, pp. 2820–2831, 2006.

[12] D. Halperin, S. Kandula, J. Padhye, P. Bahl, and D. Wetherall, "Augmenting data center networks with multi-gigabit wireless links," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 38–49, 2011.

[13] M. Kyrö, D. Titz, V. Kolmonen, S. Ranvier, P. Pons, C. Luxey, and P. Vainikainen, "5 × 1 linear antenna array for 60 ghz beam steering applications," in *Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP)*, pp. 1258–1262, 2011.

[14] H. Geng, *Data center handbook*. John Wiley & Sons, 2014.

[15] S. Pelley, D. Meisner, T. F. Wenisch, and J. W. VanGilder, "Understanding and abstracting total data center power," in *Workshop on Energy-Efficient Design*, vol. 11, 2009.

[16] L. A. Barroso and U. Hölzle, "The case for energy-proportional computing," *Computer*, vol. 40, pp. 33–37, Dec 2007.

[17] J. D. Moore, J. S. Chase, P. Ranganathan, and R. K. Sharma, "Making scheduling" cool": Temperature-aware workload placement in data centers.," in *USENIX annual technical conference, General Track*, pp. 61–75, 2005.

[18] J. Pang, S. Maki, S. Kawai, N. Nagashima, Y. Seo, M. Dome, H. Kato, M. Katsuragi, K. Kimura, S. Kondo, Y. Terashima, H. Liu, T. Siriburanon, A. Tharayil Narayanan, N. Fajri, T. Kaneko, T. Yoshioka, B. Liu, Y. Wang, R. Wu, N. Li, K. K. Tokgoz, M. Miyahara, A. Shirane, and K. Okada, "A 50.1-gb/s 60-ghz cmos transceiver for ieee 802.11ay with calibration of lo feedthrough and i/q imbalance," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 5, pp. 1375–1390, 2019.

[19] "Status of Project IEEE 802.11ay." `https://www.ieee802.org/11/Reports/tgay_update.htm` [Online]. Accessed: 2021-03-03.

[20] S. A. Mamun, S. G. Umamaheswaran, S. S. Chandrasekaran, M. S. Shamim, A. Ganguly, and M. Kwon, "An energy-efficient, wireless top-of-rack to top-of-rack data center network using

60ghz links," in *2017 IEEE International Conference on Green Computing*, pp. 458–465, June 2017.

[21] C. E. Leiserson, "Fat-trees: Universal networks for hardware-efficient supercomputing," *IEEE Transactions on Computers*, vol. C-34, no. 10, pp. 892–901, 1985.

[22] A. Greenberg, J. R. Hamilton, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. A. Maltz, P. Patel, and S. Sengupta, "Vl2: A scalable and flexible data center network," *SIGCOMM Comput. Commun. Rev.*, vol. 39, p. 51–62, Aug. 2009.

[23] A. Singla, C.-Y. Hong, L. Popa, and P. B. Godfrey, "Jellyfish: Networking data centers randomly," in *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 12)*, (San Jose, CA), pp. 225–238, USENIX Association, Apr. 2012.

[24] C. Guo, G. Lu, D. Li, H. Wu, X. Zhang, Y. Shi, C. Tian, Y. Zhang, and S. Lu, "Bcube: A high performance, server-centric network architecture for modular data centers," *SIGCOMM Comput. Commun. Rev.*, vol. 39, p. 63–74, Aug. 2009.

[25] C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, "Dcell: A scalable and fault-tolerant network structure for data centers," *SIGCOMM Comput. Commun. Rev.*, vol. 38, p. 75–86, Aug. 2008.

[26] D. Li, C. Guo, H. Wu, K. Tan, Y. Zhang, and S. Lu, "Ficonn: Using backup port for server interconnection in data centers," in *IEEE INFOCOM 2009*, pp. 2276–2285, 2009.

[27] C. Kachris and I. Tomkos, "A survey on optical interconnects for data centers," *IEEE Communications Surveys Tutorials*, vol. 14, no. 4, pp. 1021–1036, 2012.

[28] X. Ye, Y. Yin, S. J. B. Yoo, P. Mejia, R. Proietti, and V. Akella, "Dos: A scalable optical switch for datacenters," in *Proceedings of the 6th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ANCS '10, (New York, NY, USA), Association for Computing Machinery, 2010.

[29] N. Farrington, G. Porter, S. Radhakrishnan, H. H. Bazzaz, V. Subramanya, Y. Fainman, G. Papen, and A. Vahdat, "Helios: a hybrid electrical/optical switch architecture for modular data centers," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 339–350, 2011.

[30] G. Wang, D. G. Andersen, M. Kaminsky, K. Papagiannaki, T. E. Ng, M. Kozuch, and M. Ryan, "C-through: Part-time optics in data centers," *SIGCOMM Comput. Commun. Rev.*, vol. 40, p. 327–338, Aug. 2010.

[31] J. Shin, E. G. Sirer, H. Weatherspoon, and D. Kirovski, "On the feasibility of completely wirelesss datacenters," *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1666–1679, 2013.

[32] M. Z. Zaaimia, R. Touhami, V. A. Fono, L. Talbi, and M. Nedil, "60 ghz wireless data center channel measurements: Initial results," in *IEEE Int. Conf. on Ultra-WideBand (ICUWB)*, pp. 57–61, Sep. 2014.

[33] W. Zhang, X. Zhou, L. Yang, Z. Zhang, B. Y. Zhao, and H. Zheng, "3d beamforming for wireless data centers," in *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, HotNets-X, (New York, NY, USA), Association for Computing Machinery, 2011.

[34] Y. Katayama, K. Takano, Y. Kohda, N. Ohba, and D. Nakano, "Wireless data center networking with steered-beam mmwave links," in *2011 IEEE Wireless Communications and Networking Conference*, pp. 2179–2184, 2011.

[35] X. Zhou, Z. Zhang, Y. Zhu, Y. Li, S. Kumar, A. Vahdat, B. Y. Zhao, and H. Zheng, "Mirror mirror on the ceiling: Flexible wireless links for data centers," *SIGCOMM Comput. Commun. Rev.*, vol. 42, p. 443–454, Aug. 2012.

[36] J. Y. Shin, D. Kirovski, and D. T. Harper III, "Data center using wireless communication," July 12 2016. US Patent 9,391,716.

[37] H. Vardhan, S.-R. Ryu, B. Banerjee, and R. Prakash, "60ghz wireless links in data center networks," *Computer Networks*, vol. 58, pp. 192–205, 2014.

[38] N. Hamedazimi, Z. Qazi, H. Gupta, V. Sekar, S. R. Das, J. P. Longtin, H. Shah, and A. Tanwer, "Firefly: A reconfigurable wireless data center fabric using free-space optics," *SIGCOMM Comput. Commun. Rev.*, vol. 44, p. 319–330, Aug. 2014.

[39] M. Ghobadi, R. Mahajan, A. Phanishayee, N. Devanur, J. Kulkarni, G. Ranade, P.-A. Blanche, H. Rastegarfar, M. Glick, and D. Kilper, "Projector: Agile reconfigurable data center interconnect," in *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, (New York, NY, USA), p. 216–229, Association for Computing Machinery, 2016.

[40] A. Tomkins, R. A. Aroca, T. Yamamoto, S. T. Nicolson, Y. Doi, and S. P. Voinigescu, "A zero-if 60 ghz 65 nm cmos transceiver with direct bpsk modulation demonstrating up to 6 gb/s data rates over a 2 m wireless link," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 8, pp. 2085–2099, 2009.

[41] C. Marcu, D. Chowdhury, C. Thakkar, J. D. Park, L. K. Kong, M. Tabesh, Y. Wang, B. Afshar, A. Gupta, A. Arbabian, S. Gambini, R. Zamani, E. Alon, and A. M. Niknejad, "A 90 nm cmos low-power 60 ghz transceiver with integrated baseband circuitry," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 12, pp. 3434–3447, 2009.

[42] C. Cheng and A. Zajić, "Characterization of 300 ghz wireless channels for rack-to-rack communications in data centers," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 194–198, 2018.

[43] A. S. Cacciapuoti, K. Sankhe, M. Caleffi, and K. R. Chowdhury, "Beyond 5g: Thz-based medium access protocol for mobile heterogeneous networks," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 110–115, 2018.

[44] A. Verma, P. Ahuja, and A. Neogi, "pmapper: power and migration cost aware application placement in virtualized systems," in *Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware*, pp. 243–264, Springer-Verlag New York, Inc., 2008.

[45] G. Jung, M. A. Hiltunen, K. R. Joshi, R. D. Schlichting, and C. Pu, "Mistral: Dynamically managing power, performance, and adaptation cost in cloud infrastructures," in *2010 IEEE 30th International Conference on Distributed Computing Systems*, pp. 62–73, IEEE, 2010.

[46] Y. Zu, T. Huang, and Y. Zhu, "An efficient power-aware resource scheduling strategy in virtualized datacenters," in *2013 International Conference on Parallel and Distributed Systems*, pp. 110–117, IEEE, 2013.

[47] V. Mann, A. Kumar, P. Dutta, and S. Kalyanaraman, "Vmflow: Leveraging vm mobility to reduce network power costs in data centers," in *International Conference on Research in Networking*, pp. 198–211, Springer, 2011.

[48] D. Huang, D. Yang, H. Zhang, and L. Wu, "Energy-aware virtual machine placement in data centers," in *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 3243–3249, IEEE, 2012.

[49] B. Cao, X. Gao, G. Chen, and Y. Jin, "Nice: network-aware vm consolidation scheme for energy conservation in data centers," in *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, pp. 166–173, IEEE, 2014.

[50] T. C. Ferreto, M. A. Netto, R. N. Calheiros, and C. A. De Rose, "Server consolidation with migration control for virtualized data centers," *Future Generation Computer Systems*, vol. 27, no. 8, pp. 1027–1034, 2011.

[51] G. Sun, D. Liao, D. Zhao, Z. Xu, and H. Yu, "Live migration for multiple correlated virtual machines in cloud-based data centers," *IEEE Transactions on Services Computing*, vol. 11, no. 2, pp. 279–291, 2015.

[52] X. Sun, N. Ansari, and R. Wang, "Optimizing resource utilization of a data center," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2822–2846, 2016.

[53] W. Fang, X. Liang, S. Li, L. Chiaraviglio, and N. Xiong, "Vmplanner: Optimizing virtual machine placement and traffic flow routing to reduce network power costs in cloud data centers," *Computer Networks*, vol. 57, no. 1, pp. 179–196, 2013.

[54] M. Ray, S. Sondur, J. Biswas, A. Pal, and K. Kant, "Opportunistic power savings with coordinated control in data center networks," in *Proceedings of the 19th International Conference on Distributed Computing and Networking*, p. 48, ACM, 2018.

[55] C. Yuan and X. Sun, "Server consolidation based on culture multiple-ant-colony algorithm in cloud computing," *Sensors*, vol. 19, no. 12, p. 2724, 2019.

[56] H. U. Qaiser, G. Shu, and A. W. Malik, "Utilization driven model for server consolidation in cloud data centers," *IEEE Access*, vol. 8, pp. 1998–2007, 2020.

[57] R. W. Ahmad, A. Gani, S. H. A. Hamid, M. Shiraz, A. Yousafzai, and F. Xia, "A survey on virtual machine migration and server consolidation frameworks for cloud data centers," *Journal of network and computer applications*, vol. 52, pp. 11–25, 2015.

[58] G. Padmavathi and M. D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *IJCSIS IJCSIS IJCSIS IJCSIS*, p. 117, 2009.

[59] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen, and J. Cao, "Collaborative network security in multi-tenant data center for cloud computing," *Tsinghua Science and Technology*, vol. 19, no. 1, pp. 82–94, 2014.

[60] C. Franklin Jr and B. Chee, *Securing the Cloud: Security Strategies for the Ubiquitous Data Center*. Auerbach Publications, 2019.

[61] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Sixth International Conference on Semantics, Knowledge and Grids*, pp. 105–112, Nov 2010.

[62] W. A. Arbaugh, "Wireless security is different," *Computer*, vol. 36, no. 8, pp. 99–101, 2003.

[63] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in distributed, grid, mobile, and pervasive computing*, vol. 1, p. 367, 2007.

[64] D.-I. Curiac, "Wireless sensor network security enhancement using directional antennas: State of the art and research challenges," *Sensors*, vol. 16, no. 4, p. 488, 2016.

[65] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[66] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, pp. 1727–1765, Sep. 2016.

[67] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 48–52, Aug 2009.

[68] C. Wang and H. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 5569–5585, Aug 2016.

[69] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "On the security of millimeter wave vehicular communication systems using random antenna subsets," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, pp. 1–5, Sep. 2016.

[70] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 335–343, Sep. 2015.

[71] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 115–119, June 2014.

[72] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2016.

[73] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate ddos attacks on 5g core network slices," in *2019 IEEE Conference on Communications and Network Security (CNS)*, pp. 82–90, 2019.

[74] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, (New York, NY, USA), p. 46–57, Association for Computing Machinery, 2005.

[75] Y. Cai, C. Zhao, Q. Shi, G. Y. Li, and B. Champagne, "Joint beamforming and jamming design for mmwave information surveillance systems," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1410–1425, 2018.

[76] S. G. Umamaheswaran, S. A. Mamun, A. Ganguly, M. Kwon, and A. Kwasinski, "Reducing power consumption of datacenter networks with 60ghz wireless server-to-server links," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, pp. 1–7, 2017.

[77] S. A. Mamun, S. G. Umamaheswaran, A. Ganguly, M. Kwon, and A. Kwasinski, "Performance evaluation of a power-efficient and robust 60 ghz wireless server-to-server datacenter network," *IEEE Transactions on Green Communications and Networking*, vol. 2, pp. 1174–1185, Dec 2018.

[78] J. Niemann, K. Brown, and V. Avelar, "Impact of hot and cold aisle containment on data center temperature and efficiency," *Schneider Electric Data Center Science Center, White Paper*, vol. 135, pp. 1–14, 2011.

[79] T. Matsumura, K. Young, Q. Wen, S. Hanany, H. Ishino, Y. Inoue, M. Hazumi, J. Koch, O. Suttman, and V. Schütz, "Millimeter-wave broadband antireflection coatings using laser ablation of subwavelength structures," *Applied Optics*, vol. 55, no. 13, pp. 3502–3509, 2016.

[80] L. M. Correia and P. O. Frances, "Transmission and isolation of signals in buildings at 60 ghz," in *Proceedings of 6th International Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 3, pp. 1031–, 1995.

[81] "SRTHERMDUCT." `https://www.tripplite.com/smartrack-thermal-duct-kit-for-smartrack-enclosures~SRTHERMDUCT`. (Accessed on 04/04/2021), [Online].

[82] A. Committee *et al.*, "Ashrae tc 9.9 thermal guidelines for data processing enviroments," *USA: American Society of Heating, Refrigerating and Air Conditioning Engineers Inc*, 2011.

[83] D. Makarov, M. Y. Tretyakov, and P. Rosenkranz, "60-ghz oxygen band: Precise experimental profiles and extended absorption modeling in a wide temperature range," *Journal of Quantitative Spectroscopy and Radiative Transfer*, vol. 112, no. 9, pp. 1420–1428, 2011.

[84] "ns-3 network simulator." `https://www.nsnam.org/`. (Accessed on 07/25/2020).

[85] T. Benson, A. Akella, and D. A. Maltz, "Network traffic characteristics of data centers in the wild," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, (New York, NY, USA), p. 267–280, 2010.

[86] Y. Han, J. Yoo, and J. W. Hong, "Poisson shot-noise process based flow-level traffic matrix generation for data center networks," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pp. 450–457, May 2015.

[87] A. Rao, A. Legout, Y.-s. Lim, D. Towsley, C. Barakat, and W. Dabbous, "Network characteristics of video streaming traffic," in *Proceedings of the Seventh COnference on Emerging Networking EXperiments and Technologies*, CoNEXT '11, (New York, NY, USA), Association for Computing Machinery, 2011.

[88] M. Alizadeh, A. Greenberg, D. A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta, and M. Sridharan, "Data center tcp (dctcp)," in *Proceedings of the ACM SIGCOMM 2010 Conference*, pp. 63–74, 2010.

[89] "Cisco nexus 7702 hardware installation guide." `http://www.cisco.com/c/en/us/td/docs/switches/datacenter/hw/nexus7000/installation/guide/b_n7702_hardware_install_guide.pdf`. (Accessed on 04/04/2021), [Online].

[90] "Cisco nexus 9372PX and 9372PX-E NX-OS mode switches hardware installation guide." `http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9372px/guide/b_n9372PX_hardware_install_guide.pdf`. (Accessed on 04/04/2021), [Online].

[91] "Cisco nexus 9508 NX-OS mode switch hardware installation guide." `http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9508_hig/guide/b_n9508_nxos-mode_hardware_install_guide.pdf`. (Accessed on 04/04/2021), [Online].

[92] Silicom, "Silicom PE2G2I35 datasheet." `http://www.silicom-usa.com/wp-content/uploads/2016/08/PE2G2I35-1G-Server-Adapter.pdf`. (Accessed on 04/07/2019).

[93] S. A. Mamun, A. Ganguly, P. P. Markopoulos, M. Kwon, and A. Kwasinski, "Nascon: Network-aware server consolidation for server-centric wireless datacenters," *Sustainable Computing: Informatics and Systems*, vol. 29, p. 100452, 2021.

[94] Y. Fukushima, T. Yokohira, and T. Murase, "Link capacity provisioning and server location decision in server migration service," in *2018 IEEE 7th International Conference on Cloud Networking (CloudNet)*, pp. 1–3, Oct 2018.

[95] Q. Wu, F. Ishikawa, Q. Zhu, and Y. Xia, "Energy and migration cost-aware dynamic virtual machine consolidation in heterogeneous cloud datacenters," *IEEE Transactions on Services Computing*, vol. 12, pp. 550–563, July 2019.

[96] A. Neogi and A. Verma, "Techniques for placing applications in heterogeneous virtualized systems while minimizing power and migration cost," Sept. 13 2016. US Patent 9,442,550.

[97] S. Dutt, "New faster kernighan-lin-type graph-partitioning algorithms," in *Proceedings of 1993 International Conference on Computer Aided Design (ICCAD)*, pp. 370–377, IEEE, 1993.

[98] D. Meisner, B. T. Gold, and T. F. Wenisch, "Powernap: eliminating server idle power," in *ACM sigplan notices*, vol. 44, pp. 205–216, ACM, 2009.

[99] A. Davidson, D. Tarjan, M. Garland, and J. D. Owens, "Efficient parallel merge sort for fixed and variable length keys," in *2012 Innovative Parallel Computing (InPar)*, pp. 1–9, IEEE, 2012.

[100] L. Kleinrock, *Queueing systems, volume 2: Computer applications*, vol. 66. wiley New York, 1976.

[101] SPECpower_ssj2008, "Results for Dell Inc. PowerEdge C5220." `https://www.spec.org/power_ssj2008/results/res2013q2/power_ssj2008-20130402-00601.html`. (Accessed on 04/07/2019).

[102] B. Heller, S. Seetharaman, P. Mahadevan, Y. Yiakoumis, P. Sharma, S. Banerjee, and N. McKeown, "Elastictree: Saving energy in data center networks.," in *Nsdi*, vol. 10, pp. 249–264, 2010.

[103] Cisco, "Cisco data center switches." `https://www.cisco.com/c/en/us/products/switches/data-center-switches/index.html`. (Accessed on 04/07/2019).

[104] A. Devices, "Analog devices HMC6300 and HMC6301 60 GHz millimeter wave transmitter and receiver datasheet." `http://www.analog.com/media/en/technical-documentation/data-sheets/HMC6300.pdf`. (Accessed on 04/07/2019).

[105] A. Chatzieleftheriou, S. Legtchenko, H. Williams, and A. Rowstron, "Larry: Practical network reconfigurability in the data center," in *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pp. 141–156, 2018.

[106] C. Cheng and A. Zajić, "Characterization of 300 ghz wireless channels for rack-to-rack communications in data centers," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 194–198, Sep. 2018.

[107] K. Bilal, O. Khalid, A. Erbad, and S. U. Khan, "Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers," *Computer Networks*, vol. 130, pp. 94–120, 2018.

[108] S. A. Mamun, A. Ganguly, P. P. Markopoulos, A. Kwasinski, and M. Kwon, "Security vulnerabilities of server-centric wireless datacenters," in *2020 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2020.

[109] S. A. Mamun, A. Ganguly, P. P. Markopoulos, A. Kwasinski, and M. Kwon, "What can ail thee: New and old security vulnerabilities of wireless datacenters," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, pp. 1–7, 2020.

[110] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5g cellular: It will work!," *IEEE Access*, vol. 1, pp. 335–349, 2013.

[111] S. Namal, K. Georgantas, and A. Gurtov, "Lightweight authentication and key management on 802.11 with elliptic curve cryptography," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1830–1835, 2013.

[112] G. Joy Persial, M. Prabhu, and R. Shanmugalakshmi, "Side channel attack-survey," *Int. J. Adv. Sci. Res. Rev*, vol. 1, no. 4, pp. 54–57, 2011.

[113] S. Sharafeddine, A. Riedl, J. Glasmann, and J. Totzke, "On traffic characteristics and bandwidth requirements of voice over ip applications," in *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*, pp. 1324–1330 vol.2, 2003.

[114] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, pp. 2027–2051, thirdquarter 2016.

[115] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A sybil attack detection scheme for a forest wildfire monitoring application," *Future Generation Computer Systems*, vol. 80, pp. 613–626, 2018.

[116] M. Alenezi and M. J. Reed, "Methodologies for detecting dos/ddos attacks against network servers," in *The Seventh International Conference on Systems and Networks Communications ICSNC*, pp. 92–98, 2012.

[117] I. Attiya, M. Abd Elaziz, and S. Xiong, "Job scheduling in cloud computing using a modified harris hawks optimization and simulated annealing algorithm," *Computational intelligence and neuroscience*, vol. 2020, 2020.

[118] S. Rommel, T. R. Raddo, U. Johannsen, C. Okonkwo, and I. T. Monroy, "Beyond 5G - wireless data center connectivity," in *Broadband Access Communication Technologies XIII* (B. B. Dingel, K. Tsukamoto, and S. Mikroulis, eds.), vol. 10945, pp. 125 – 133, International Society for Optics and Photonics, SPIE, 2019.

[119] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[120] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[121] Q. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W. Hwang, and Z. Ding, "A survey of multi-access edge computing in 5g and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974–117017, 2020.

[122] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

Appendices

Appendix A

Related Publications

The contributions for each of the research objectives have been published in several peer reviewed conferences and journals. Based on the findings from this research one patent application is filed in US patent office. The details of our research contributions and methodologies can be found from the following conference and journal papers.

A.1 Journal Publications

1. **S. A. Mamun**, A. Ganguly, P. P. Markopoulos, M. Kwon, A. Kwasinski, "NASCon: Network-Aware Server Consolidation for server-centric wireless datacenters," Sustainable Computing: Informatics and Systems, v. 29, p. 100452, Elsevier, 2021. doi: 10.1016/j.suscom.2020.100452

2. **S.A. Mamun**, A. Gilday, A. K. Singh, A. Ganguly, G. V. Merrett, X. Wang, B. M. Al-Hashimi, "Intra- and Inter-Server Smart Task Scheduling for Profit and Energy Optimization of HPC Data Centers," in Journal of Low Power Electronics and Applications. 2020; 10(4):32. doi: 10.3390/jlpea10040032

3. **S. A. Mamun**, S. G. Umamaheswaran, A. Ganguly, M. Kwon and A. Kwasinski, "Performance Evaluation of a Power-Efficient and Robust 60 GHz Wireless Server-to-Server Datacenter Network," in IEEE Transactions on Green Communications and Networking, vol. 2, no. 4, pp. 1174-1185, Dec. 2018, doi: 10.1109/TGCN.2018.2838525.

A.2 Conference Publications

1. **S. A. Mamun**, A. Ganguly, P. P. Markopoulos, A. Kwasinski and M. Kwon, "What Can Ail Thee: New and Old Security Vulnerabilities of Wireless Datacenters," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, Taipei, Taiwan, 2020, pp. 1-7, doi: 10.1109/GLOBECOM42002.2020.9322619.

2. **S. A. Mamun**, A. Ganguly, P. P. Markopoulos, A. Kwasinski and M. Kwon, "Security Vulnerabilities of Server-Centric Wireless Datacenters," 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 2020, pp. 1-9, doi: 10.1109/CNS48642.2020.9162233.

3. **S. A. Mamun**, A. Ganguly, M. Kwon, A. Kwasinski and P. P. Markopoulos, "Network-Aware Server Consolidation for Wireless Data Centers," 2019 10th International Conference on Networks of the Future (NoF), Rome, Italy, 2019, pp. 58-65, doi: 10.1109/NoF47743.2019.9014979.

4. **S. A. Mamun** and A. Ganguly, "Making Cables Disappear: Can Wireless Datacenter be a Reality?," 2018 Ninth International Green and Sustainable Computing Conference (IGSC), Pittsburgh, PA, USA, 2018, pp. 1-2, doi: 10.1109/IGCC.2018.8752167.

5. S. G. Umamaheswaran, **S. A. Mamun**, A. Ganguly, M. Kwon and A. Kwasinski, "Reducing Power Consumption of Datacenter Networks with 60GHz Wireless Server-to-Server Links," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-7, doi: 10.1109/GLOCOM.2017.8254209.

6. M. M. Ahmed, M. S. Shamim, N. Mansoor, **S. A. Mamun** and A. Ganguly, "Increasing interposer utilization: A scalable, energy efficient and high bandwidth multicore-multichip integration solution," 2017 Eighth International Green and Sustainable Computing Conference (IGSC), Orlando, FL, USA, 2017, pp. 1-6, doi: 10.1109/IGCC.2017.8323583.

7. **S. A. Mamun**, S. G. Umamaheswaran, S. S. Chandrasekaran, M. S. Shamim, A. Ganguly and M. Kwon, "An Energy-Efficient, Wireless Top-of-Rack to Top-of-Rack Datacenter Network Using 60GHz Links," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 2017, pp. 458-465, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.74.

A.3 Patent Application

1. A. Ganguly, M. Kwon, A. Kwasinski, **S. A. Mamun**, "Direct Server-to-Server Wireless Data Center Network and Method thereof," US20190327780A1, 2019, (Patent Pending).