Security Vulnerabilities of Server-Centric Wireless Datacenters

Sayed Ashraf Mamun, Amlan Ganguly, Panos P. Markopoulos, Andres Kwasinski and Minseok Kwon

Rochester Institute of Technology
Rochester, NY, USA

Abstract—Wireless datacenter network is an emerging technology. Recent works have shown that by utilizing millimeter wave (mmWave) wireless communication, the power consumption of the networking equipment of datacenters can be reduced drastically. However, security of a datacenter is one of the highest design priorities. Many studies on the security of wired datacenters including identifying the possible threats and solutions have been explored in the literature. On the contrary, being an emerging technology, no study has yet been done on the security for the wireless datacenters. Moreover, being a wireless system, it also inherits most of the threats of a typical wireless system if not all. So, in order to successfully realize wireless datacenter architectures, it is essential to do an extensive investigation of the system from a security perspective. In this paper, we have done an extensive study on the possible threats and their impact on the wireless datacenter network. We showed that eavesdropping, denial of services, and jamming attacks are the most critical security threats for wireless datacenters.

Index Terms—datacenter security, wireless datacenter, wireless security, eavesdropping, DoS attack, jamming attack;

I. INTRODUCTION

Datacenters around the world consume an enormous amount of energy and power, projected to be 140 billion kWh in 2020 [1]. A significant portion of the power consumption is due to the IT equipment consisting of servers and network equipment which contributes more than 60% [2] of the entire power consumed. Novel datacenter network (DCN) technologies, leveraging emerging interconnection paradigms such as millimeter-wave (mmWave) interconnects have been proposed to reduce the power consumption of the networking equipment [3], [4]. Wireless datacenter architectures have been proposed where Top-of-Rack (ToR) switches are interconnected with mmWave links while intra-rack communication is achieved through traditional Ethernet [5]–[7]. Recent work [8], [9] proposed a server-centric wireless DCNs namely server-to-server wireless datacenter network (S2S-WiDCN) for datacenters, where direct wireless links are used for server-to-server communication having the potential to reduce the power consumption of the DCN in an order of magnitude.

Due to the adoption of the upcoming 5G technology and network densification, the number of small datacenters will rise exponentially in the next few years [10] 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 datacenters 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 datacenter.

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. [11], [12]. 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 datacenters 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. In this paper, we have done an in-depth analysis of the possible threats and attacks on the wireless datacenter 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.

II. RELATED WORK

Various designs have been proposed to address DCN design issues such as energy consumption, cabling complexity, scalability, and over-subscription. One popular topology used today in datacenter networks is a fat-tree topology. To address over-subscription and other issues in wired DCNs many alternative DCN architectures have been proposed such as BCube, DCell, DOS, VL2, and Helios [13]. However, these innovations still rely on copper or optical cables and do not mitigate the challenges due to high power consumption, design, and maintenance of a DCN with physical links. To alleviate the issues of DCNs with power-hungry switching fabrics and bundles of cables wireless datacenters with mm-wave interrack links are envisioned in [3], [5], [6]. Most of the recent works on wireless datacenters propose interconnecting entire racks of servers as units with 60GHz wireless links primarily
in order to utilize the commodity Ethernet switching between servers inside individual racks [3]. Phased antenna arrays or directional horn antennas are used to establish wireless links between ToRs in the entire datacenter [6], [7]. Line-of-Sight (LoS) communication paths are necessary between the antennas for reliable communication in a wireless datacenter [6]. Cylindrical or polygonal [4] arrangements of servers are proposed to create LoS wireless links between servers. In [9] a novel wireless DCN architecture, based on 60GHz wireless links between the individual servers of namely, S2S-WiDCN was proposed which drastically reduces power consumption of the network portion of the datacenter while sustaining comparable performance.

Many studies have been done on the security of wired datacenters [14]–[16]. On the contrary, as wireless datacenters are still being an emerging technology, not much study has been done on the security aspects of these types of datacenters. It has also been widely considered that wireless systems are inherently more unsecured than their wired counterparts [17]. 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 [11] 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 [12]. Studies have been done on the security aspect of traditional wireless networks involving lower bandwidth and solutions have been proposed [18]–[20]. 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 [21], [22]. On the contrary, some security related advantage exists because of the high directionality of the antenna arrays in mmWave bands. In [21], 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 [23], 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 [24]. To the best of our knowledge, no work exists on the security of an entirely wireless datacenter which is the gap we attempt to bridge in this paper.

III. SERVER-TO-SERVER WIRELESS DCN

Before discussing the potential security threats on the wireless datacenter, we describe it’s architecture. We choose a server-to-server wireless datacenter architecture [9], which is shown to reduce power consumption compared to traditional wired architectures by up to an order of magnitude.

A. Physical Topology

In the S2S-WiDCN architecture, datacenter 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 only along horizontal lines and vertical planes are used to communicate between any two servers in the three-dimensional space as shown in Fig. 1(a). To achieve this, each server is equipped with two high gain 60 GHz antenna arrays. One of the antennas which are attached on the top of the server is to communicate in the horizontal direction and another one which is on the back of the server projecting out from the rack as shown in Fig. 1(b) is for enabling communication in the vertical plane. This antennas array is capable of beam-steering panning a 60° angle. Therefore, 6 arrays are necessary to cover the 360° panorama to communicate with any other server in the vertical plane. A single array is sufficient in the horizontal plane as no beam-steering is necessary due to the adopted communication and routing strategy discussed next.

B. Routing Mechanism

To avoid interference and obstructions from the rack frames, communications in the horizontal plane are restricted only to a single line between horizontally aligned servers thereby not requiring beam-steering for horizontal communication. A small aperture among servers within a rack is needed to enable LoS among the vertically aligned servers for a linear communication between them [9]. On the other hand, 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 choosing the correct sector out of six and steering its antenna array towards the receiver. These control packets are sent over a separate ISM band. Upon receipt of this control message, a wireless module at the receiver chooses the antenna array in the correct sector out of the set of six and steers that array towards the sending server. All the intra-rack communications in S2S-WiDCN are completed in one hop in the vertical plane whereas inter-rack communication depends on the relative position of the source and destination servers. There are 4 possible routing scenarios in S2S-WiDCN. If the final destination is in the same row as that of the source, communication is achieved over a one-hop path through the vertical plane. If the final destination is in a different row but in the same horizontal line as that of the source, a one-hop path is used along the horizontal line. In all other cases, where the source and destination servers are in different rows and not horizontally aligned, a 2-hop link is established for communication using an intermediate server as shown in Fig. 1(a). IEEE802.11ad [25] standard is adopted here, which allows multiple communication links to be established along the same physical link. This standard defines a physical layer protocol that supports beam-forming, and also supports extremely high data rates through Orthogonal Frequency Division Multiplexing (OFDM) with a maximum achievable data rate of 6.7Gbps.

C. Advantages of S2S-WiDCN Architecture

In [9], it was shown that, with S2S-WiDCN architecture, the power consumption of the network portion of the datacenter can be reduced significantly compared to a conventional fat-tree DCN. Fig. 1(c) shows the comparison of the power consumption of the network portion of a ToR-ToR Wireless DCN (ToR-ToR WiDCN) [7] and S2S-WiDCN normalized to network power consumption of a traditional fat-tree DCN. In ToR-ToR WiDCN architecture, the servers inside a rack are connected through wired line and the ToR switch is equipped with wireless transceiver to maintain inter-rack communication. Additionally, cabling complexity can be reduced significantly with S2S-WiDCN because of the complete elimination of the structured cabling which caused inefficient cooling in the datacenter. However to realize these efficiencies of the wireless DCN this network needs to be secured against all kinds of attacks that are possible on the wireless DCN. In this paper, we will discuss the major security vulnerabilities of S2S-WiDCN architecture.

IV. SECURITY ATTACKS ON S2S-WiDCN DCN

As the S2S-WiDCN datacenter 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. 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. 2 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.

A. 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 [23], the author showed that despite having highly directional transmission, an eavesdropper can successfully intercept a signal by creating virtual periscope. Nevertheless, as the datacenter 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 datacenter premises or outside of the datacenter premises. Based on the location of the eavesdropper, two types of attack models are possible.

1) **External eavesdropper**: In this scenario, the attacker is located outside of the datacenter premises as shown in a blue circle in Fig. 3. In absence of any obstruction, the wireless power received by the external eavesdropper in free space can be calculated using Friis transmission formula,

\[
P_R = \frac{P_T G_T G_{Rc}^2}{(4\pi f R)^2},
\]

where \(P_R\) represents the power received by eavesdropper’s antenna, \(P_T\) is the power transmitted by a legitimate server, \(G_R\) and \(G_T\) represent the respective gain of the receiving and transmitting 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 datacenter. Moreover, the datacenter 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.

2) **Internal Eavesdropper**: Internal Eavesdroppers are the eavesdroppers who are located inside of the datacenter premises. In this attack model, it is considered that servers in the datacenter 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 datacenter 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 datacenter, they would try to strategically attack those servers which have the potential for highest eavesdropping. From the analysis and simulations done in Section V-C1b, 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.

### B. 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.

1) **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 datacenter, 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 datacenter traffic having a higher flow injection rate, but within the normal distribution of the legitimate traffic of datacenter. We define this type of attack as Type-II DoS attack as shown in Fig. 4. 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.

C. 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.

1) Attack Model: The jamming attack can initiate from an external source or any compromised server inside of the network. As the datacenter is in a confined environment, it is unlikely that any external jamming source will have any significant effect on the performance of the datacenter communication as the wireless channels used for the communication utilizes 60GHz which has extremely low penetration capability metal or brick wall. In [26] 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 datacenter. 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° area with the existence of 6 different arrays as discussed in Section III-A. 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.

D. Side-Channel Attacks

A side-channel attack [27] 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 eavesdropping attack.

E. Traffic Analysis Attack

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication, which can be performed even when the messages are encrypted [27]. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. In S2S-WiDCN, all the servers have the potential to become an intermediate node between two server’s communication. Hence any server that has been compromised, can do traffic analysis to some extent. Moreover, any external receiver place inside a datacenter can also be used to carry out a traffic analysis attack.

F. Man in the Middle Attack

A man-in-the-middle attack (MITM) [28] 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 datacenter 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.

G. Sybil Attack

Sybil attack [29] 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 [29], 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.
H. 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.

I. 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.

V. 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 datacenter traffic model and simulation platform in next subsections.

A. Datacenter 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 datacenter traffic for different classes of datacenters is measured in [30]. Using these measured traffic flows, a Poisson shot-noise based model to synthesize datacenter traffic is proposed and verified in [31]. According to [31], 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 [30]. Moreover, it has been observed from the measurement of a variety of datacenters in [30], 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 [30] 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.

B. Simulation Platform
We use the Network Simulator-3 (NS-3) suite [32] 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 datacenter including the 60GHz band and the IEEE802.11ad standard as discussed in [5] 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 [5]. 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 datacenter architecture, we have considered 1.0Gbps links between servers to access switches and 40.0Gbps upper-layer links. We have considered a small datacenter consisting of 800 servers arranged in a 20 × 8 array of racks as [9]. Each of the rack houses 5 servers and occupies an area of 0.6m × 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 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.

C. Performance Evaluation and Analysis
In this section, we evaluate the performance of the wireless datacenter during eavesdropping attack, DoS attack, and jamming attack.

1) Effect of Internal Eavesdropper:
   a) Security vulnerability due to randomly positioned compromised servers: In this attack model, the attacker captures the servers in the datacenter 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 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 $\theta = 15^0$, $\theta = 30^0$, and $\theta = 60^0$ beam-width used by the servers in the datacenter 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. 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$^0$), the total amount of traffic compromised is about 60% of the compromised traffic for wide beam-width (60$^0$) antenna.

b) 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 datacenter, 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. 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 datacenter, 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$^0$, 30$^0$, and 60$^0$ beam-width respectively. The results are also shown in Fig. 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$^0$, up to 33% more flows can be captured by the eavesdropper compared to the antennas having narrow beam-width of 15$^0$.

c) 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 datacenter network architectures for strategically positioned compromised node. In Fig. 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 architecture 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 datacenter 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.

2) Security Vulnerability due to DoS Attack: With the DoS attack, the attacker tries to hamper the performance of the datacenter or disrupt the entire network. As discussed in Section IV-B1, 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 datacenter 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 and regenerated new traffic which represents different types of multimedia traffic and repeats the simulations. The results are shown in Fig. 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.

3) 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. 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.1(a).
layer characteristics like spatial diversity, beamforming, and MIMO, path diversity of the 60GHz and S2S-WiDCN can be leveraged to address a few of the security threats. To mitigate the DoS attack rigorous authentication mechanisms can be implemented. Defense against jamming attack is known to be hard to implement. In the event that a jamming attack is detected, the communication can be deferred for a finite amount of time hoping that the jamming attack will pass through. On the contrary, existing high path diversity of S2S-WiDCN can be leveraged to address a few of the security threats. To overcome the MITM attack and Sybil attack, hello flood attack, sinkhole/wormhole attack, eavesdropping, denial of services, and jamming attacks are the most critical security threats. Man in the middle attack, Sybil attack, hello flood attack, sinkhole/wormhole attack, side-channel attack are among the other possible attacks in the system. In our next phase of research, we will try to address these security threats with possible light-weight solutions which should have minimal effect on the performance. We will also try to leverage the physical characteristics of 60GHz i.e. high directionality, sensitivity to blockage while designing solutions.

VII. CONCLUSIONS

Ensuring data security in the datacenter is extremely important. S2S-WiDCN datacenter can be vulnerable to a variety of different attacks as it uses wireless links for communication. In this paper, we identified the major security vulnerability of an S2S-WiDCN. We have shown that for S2S-WiDCN eavesdropping, denial of services, and jamming attacks are the most critical security threats. Man in the middle attack, Sybil attack, hello flood attack, sinkhole/wormhole attack, side-channel attack are among the other possible attacks in the system. In our next phase of research, we will try to address these security threats with possible light-weight solutions which should have minimal effect on the performance. We will also try to leverage the physical characteristics of 60GHz i.e. high directionality, sensitivity to blockage while designing solutions.

REFERENCES


