584 Paper - 3

Security Vulnerabilities of Server-Centric Wireless Datacenters

Rahul Godugupally

CWID -10470581

1. Summary of fundamental ideas presented in the paper

In this paper, the authors analyze and investigate the security of a server-to-server wireless data center network (S2S-WiDCN). They mention that since this is an emerging technology there have been no studies done previously on the security of wireless data centers. As these are wireless data center architectures contrary to the wired data centers which have been studied extensively, nothing is known about the security of these new wireless architectures.

In this paper, the authors do an extensive security investigation of the system and study their threats and impacts. They say that as these are wireless architectures, they inherit most of the problems, and threats faced by any other wireless systems. As it uses wireless links for communication, they are most vulnerable to eavesdropping, denial of services, and jamming attacks. These 3 attacks are the most severe critical threats to S2S-WiDCN. Among the other possible attacks which could harm the system include Man in the middle attack, Sybil attack, hello flood attack, sinkhole/wormhole attack, side-channel attack.

On top of analyzing the impact on data security, the authors have measured their impact on the performance of the overall network using a network-level simulator, specifically Network Simulator-3 suite. In the end, they address these concerns with lightweight solutions which they claim would not have a severe effect on the performance of the wireless data center. Also, they try to leverage the “physical characteristics of 60GHZ high directionality, sensitivity to blockage while designing solutions” [1] to the threats.

2. Issues paper addresses and how they have been addressed in the past

The paper addresses concerns regarding novel datacenter networks (DCNs) and mentions the high-power consumptions of DCN’s as the sizable portion of the power is due to IT and Networking equipment used by these types of datacenter networks. The paper also considers DCN’s that use emerging technologies for interconnection such as millimeter-wave (mmWave) to reduce power consumption and fat-tree topology, which is one of the more popular topologies used nowadays. Other considerations include BCube, DCell, DOS, VL2, and Helios. But these still rely upon the use of copper or optical cables and do not address the problems faced due to high power consumption, design, and maintenance of a DCN with physical links.

However, the highest potential solution for reducing power consumption was found in server-centric wireless DCN’s namely server-to-server wireless datacenter network (S2S-

WiDCN) based on their previous work from [2] and [3]. The S2S-WiDCN uses direct wireless links for server-to-server communication.

The authors also suggest that with the adoption of 5G technology and due to network densification “the number of small data centers will rise exponentially in the next few years and S2S-WiDCN can be considered as a great candidate for this field.” [1] Also, they mention that due to S2S-WiDCN supporting high data rate exchange through the dense wireless links and highly directional antennas, it can also be adopted to large-scale data centers.

As this architecture is wireless it shares the security aspects of conventional wireless networks such as wireless sensor networks and ad-hoc networks. But it being wireless also has its own advantages such as “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”. [1] Which make them less vulnerable to external eavesdroppers.

Hence, they mention that the security aspect of this technology must be investigated thoroughly along with its impact not only on Data security and integrity but also on its performance.

3. Discussion of core ideas of the paper

The core idea discussed in the paper concerns server-to-server wireless datacenter network (S2S-WiDCN) and its security.

The security of this technology was extensively evaluated to find out the real-world performance and how they stacked up to the wired counterparts. As this technology is wireless, it inherits more threats than a wired DCN. As every server in S2S-WiDCN has direct communication capability this can be compared to a Wireless Sensor Network (WSN). And in fact, many of the security concerns that apply to WSN also apply to S2S-WiDCN. However, the servers in S2S-WiDCN are uniformly arranged and their inter-server communication is done with the help of highly directional antennas which have high speed wireless links. Also, the authors mention that, with the use of directional antennas, the security of the WSN can be enhanced to some extent. Significant secrecy improvement compared to conventional systems could be achieved. However, “eavesdropping is still possible by creating virtual periscope”. [1]

In S2S-WiDCN architecture, the racks are laid out in a conventional rectangular pattern, with aisles running between the rows of racks. Communication is done along Wireless links along horizontal and vertical lines to avoid obstruction. And to achieve this each of the server racks has two high gain 60GHz antennas. The antenna which is attached to the top is used to communicate in the horizontal direction and the antenna which is attached to the back is used to communicate in the vertical direction. In order to avoid interference and obstructions, communications along horizontal planes are restricted to a single line. All the other intra-rack communications are completed in a single hop in the

vertical plane whereas “inter-rack communications depend on the relative position of the source and destination servers. “[1]

There are several advantages to S2S-WiDCN, the first one, of course being it’s significantly reduced power consumption relative to traditional architectures. Secondly, cabling complexity is drastically reduced because of the elimination of cabling which in turn improves the efficiency of cooling in the data center.

The authors then go on to explain the vulnerabilities of S2S-WiDCN by broadly classifying them into two types: Active and Passive. “In passive attacks, the attacker monitors and listens to the communication channel by unauthorized means.” [1] In active attacks on the other hand the attacker not only listens and monitors the communication but also modifies the data.

Passive attacks include eavesdropping and monitoring, traffic analysis, and side-channel attacks. While, active attack includes active eavesdropping, jamming, denial of services, and physical attacks. They concluded that attacks that have the most significant damage to the S2S-WIDCN are eavesdropping, denial of services, and jamming attacks. All the other attacks such as man in the middle attack, Sybil attack, hello flood attack, sinkhole/wormhole attack were classified as an extension of active eavesdropping.

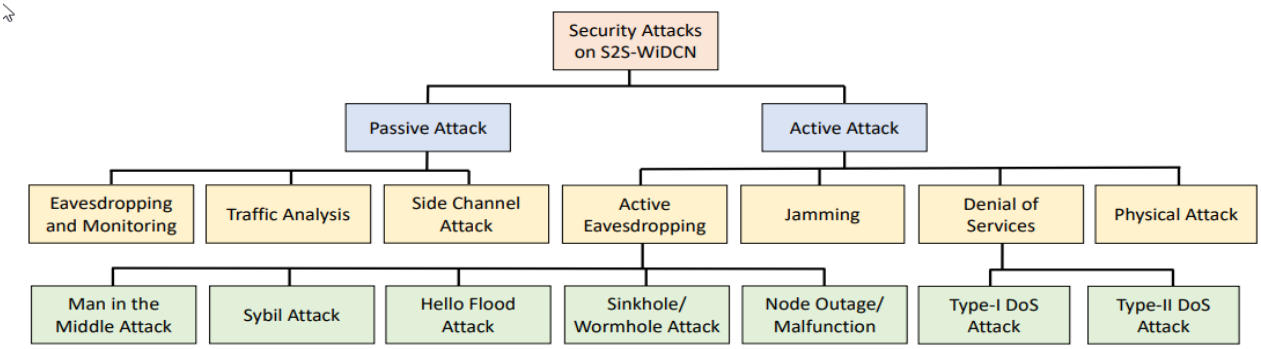

Figure 1: List of possible attacks on S2S-WiDCN [1]

List of Security Attacks on S2S-WIDCN

1. **Eavesdropping Attack:** Widely considered as one of the most common security threats in wireless communications. As S2S-WIDCN utilizes mmWave wireless links for communication that require LoS between transmitter and receiver. And as the datacenter uses 60Ghz wireless links which have low penetration compared to normal 2.4/5 Ghz, the authors argue that this would reduce the possibility of external eavesdropping but would still be vulnerable to internal eavesdropping.
2. **Denial-of-Services Attack:** They conclude that the possibility of Denial of Service in S2S-WiDCN is high as all the servers can communicate amongst each other with one or 2 hops between them with multiple routes being available. For this attack they have assumed that if one server is compromised then it would have the potential to flood the entire network. They give an example of a single malicious

Virtual machine that could significantly downgrade the network performance while being difficult to detect.

3. **Jamming Attack:** The authors mention that due to jamming authorized users are unable to access the data as they are filled with overwhelming noise “As the communication in S2S-WiDCN takes place in an open medium frequency jamming can cause interference with legitimate OFDM channels and cause disruption in the network.” [1]
4. **Side-Channel Attacks:** This is an attack based on information gained from the system through a path not that was not originally designed. The information gained from this attack could be used to carry out other attacks and also for enumerating the datacenter.
5. **Traffic analysis Attack:** This attack involves intercepting and analyzing the messages sent over the network to figure out the information from the patterns in the communication process. The higher number of messages that are analyzed the greater the chance for deducing the traffic. Any server that is compromised in the S2S-WiDCN can become a potential intermediary node and do traffic analysis to an extent.
6. **Man in the Middle Attack:** here the attacker sits in the middle of communication of two nodes who believe that they are directly in contact with each other. As the S2S-WiDCN uses an ISM band control channel that makes use of 2.4/5 GHz frequency the attacker can perform a MitM attack and compromise the integrity of data, monitor what's being sent and even take control of the compromised server.
7. **Sybil Attack:** In this attack a single node duplicates itself and presents itself in multiple locations. With authentication and encryption techniques the Sybil attack can be prevented if the nodes are scattered. The authors argue that, as servers are uniformly positioned in S2S-WiDCN it is unlikely that a sybil attack will cause much disruption in communications.
8. **Hello Flood Attack:** In this attack “an attacker sends and replays hello packets which contain false routing and resource availability information, which can lead other servers trying to utilize that server for routing.” [1] However, in the case of S2S-WiDCN the control information is transmitted over a separate control plane making it secure against this attack.
9. **Sinkhole/Wormhole Attack:** In this attack the attacker tries to attract as much traffic as possible through a compromised server which could lead to dropped packets. In S2S-WiDCN a single compromised server can act as a sinkhole and destroy the communication process.

Lastly, the authors perform a network simulation using Network Simulator-3 to evaluate the performance of S2S-WiDCN networks in the presence of the major vulnerabilities such as eavesdropping, Denial of service and jamming. They then propose solutions which are light weight which do not compromise the performance of the data center. As they mention that there are tradeoffs between security and performance. Also they propose rigorous authentication mechanisms to mitigate the threat of DoS. They suggest the use of existing high path diversity to minimize the effects of jamming attacks.

4. Potential applications of technology presented

The analysis done in the paper can be used for baseline for detecting the security threats faced by server-to-server wireless datacenter network. As the threats are identified their countermeasures can be applied on the data center in order to ensure it is functioning securely.

The S2S-WiDCN can become commonplace in the future due to its lower energy requirements and as it reduces the hassle of cables which in turn provides better cooling solutions to data centers. As more and more small scale data centers start to come up, they could be implemented with S2S-WiDCN.

The technology presented in the paper can also be used to improve the functionality of a data center, by providing better solutions to security problems created by the security threats and also by identifying them quickly.

5. Future directions suggested or ones that you might infer from the topic

The technology presented in the paper gives rise to new age data centers which have minimal use of cables but instead relying on wireless as they are easier to manage and cooler to maintain. These data centers would not require as many cooling solutions and would be efficient in utilization of power compared to traditional data centers.

The technology presented in the paper can also be used to study the possibility of wireless data mining farms or wireless short scale communications networks with the highly directional antennas eliminating the need for chunky cables and improving the power optimization.

It also raises the possibility of wireless replacing existing wired solutions which work well. Not long ago, most solutions used to be wired but with time people are opting the wireless route with wireless charging, Wireless Lan instead of an ethernet cable, one might wonder what is next in the field of wireless communications and what might it replace.

Citations

[1] 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), 2020, pp. 1-9, doi: 10.1109/CNS48642.2020.9162233.

[2] S. G. Umamaheswaran, S. A. Mamun, A. Ganguly, M. Kwon et al., “Reducing power consumption of datacenter networks with 60ghz wireless server-to-server links,” in IEEE GLOBECOM, 2017, pp. 1–7.

[3] S. A. Mamun, S. G. Umamaheswaran, A. Ganguly, M. Kwon et al., “Performance evaluation of a power-efficient and robust 60 ghz wireless server-to-server datacenter network,” IEEE Tran. on Green Communications and Networking, vol. 2, no. 4, pp. 1174–1185, Dec 2018.