Analysis and Detection of DDoS Attacks Targetting Virtualized Servers

Nisar Ahmed, Intesab Hussain sadhayo, Zahid Yousif, Nadeem Naeem, Sajida Parveen

Quaid-e-Awam University of Engineering Science and Technology Nawabshah, Sindh, Pakistan

Abstract

In recent years, virtualization is a fast-growing technology and moving beyond the test and development and manufacture merging to high availability and disaster recovery in big data. Cloud Computing and grid computing solve the increasing computing and storage problems arising in the Internet Age with efficient use of resources, ease of management and efficient power consumption. Therefore, many platforms have become in demand such as VMware ESXi, Microsoft Hyper-V server and Xen Hypervisors .However, the virtualization is facing many security concerns among which Distributed Denial of Service (DDoS) is the major threat in this technological era. DDoS is an attempt of attacking in distributed fashion to make a server's resource unavailable to its legitimate users. It is one of the most severe attacks that threatens many popular Internet based services like e- commerce, e-banking, transportation, medicine and education etc. The aim of this paper is to study the impact of processor exhaustion due to DDoS attacks on virtual server and implement the Snort intrusion detection systems (IDS). The proposed strategy effectively detects DDoS attacks such as TCP SYN and UDP Flood attack based on the threshold limit in the specified time mechanism which gave better results than other state of the art solutions. DDoS attack is generated with the help of LOIC tool to check the processor exhaustion of virtual server at different packet rates and time durations. The experimental results have demonstrated that maximum peak packet rate of TCP SYN is 277143 and UDP DDoS is 168000 at which the server is totally halted. The generated attacks are detected in the form of logs in which source and destination addresses are represented along with port addresses. Furthermore, the Snort IDS tool detects the attack at the early stage. Moreover, it helps to minimize the effect of DDoS attack by alerting the network administrator which facilitates to diagnose the problem.

Key words:

Virtualization, DDoS, TCP SYN flood attack, UDP flood attack, Snort IDS

1. Introduction

In recent years, virtualization is a fast-growing technology in big data, cloud computing and grid computing due to its lower cost, flexible system, efficient use of resources and efficient power consumption. The virtualization creates an abstraction of the computer hardware resources and share to run Multiple OSes on the same physical platform [1]. Virtualization is not magic, but it is the combination of software and hardware that is caused to run multiple Virtual Machines (VMs) simultaneously on one physical machine in which the hypervisor or The VMM (Virtual Machine Monitor) is the controller at the core of virtualization. when multiple Virtual Machines VMs runs on one physical server, prudent monitoring of virtual machines with high security is very crucial. If the intruders launch a DDoS attack by taking the advantages of vulnerabilities in Virtual Machines on virtualized server, all the VMs on the host would suffer from the DDoS attack. The DDoS attack is basically, an attempt of attacking in distribution fashion to make servers resource unavailable to its legitimate users [2]. Moreover; the DDoS attack is the cause to exhaust CPU utilization of virtualized servers during attack which bring down the whole services whether the services are in big data, cloud computing or grid computing. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the most widely used communication protocols to the Internet. In a DDoS attack scenario, TCP SYN flood and UDP flood are the protocol based attack. TCP communication occurs with three-way handshake. In the first phase, client or source sends SYN (synchronization) packet to server and then in second phase, the server responds it by sending SYN-ACK (synchronization- acknowledged) packet to client and at last phase, the client confirms it by sending ack (acknowledged) packet to server [3]. After that data flows in active connection. The hackers take the advantages of the half open connection and send flood of SYN packet attack which may certainly exhaust CPU utilization. In UDP communication, there is no three-way handshake, the data flows in a smooth way. The UDP flood attack is a type of attack in which the enough UDP packets are sent to a victim to slow down or go down its resources [4]. Intrusion Detection System (IDS) is the software for detecting such flooding security threats and monitoring the data packet traffic on the network [5].

In this paper, we evaluate the impact of TCP and UDP flooding DDoS attack on a virtualized server's processor resources and provide detection mechanisms such as open source snort IDS.

The remaining of the paper is structured as follows. In the next section, the problem statement is given followed by at what extent work is done in related work, in section III. A brief description of background is given in section IV. A comprehensive explanation of the proposed work is given

Manuscript received January 5, 2019
Manuscript revised January 20, 2019

in methodology in section V. The evaluation results are presented and discussed in section VI. Finally, we conclude the paper's research contribution and give the future research direction in section VII.

2. Related work

DDoS is a flooding attack to fully exhaust server's resources [6]. The DDoS attack hampers the load on processor of Internet services which turns out the huge business loss [7].

- When any attacker launches the DDoS attack, the victim may face following impact on server,
- To make server's process exhaustion
- To make unavailability of resources of the server to the legitimate users;
- To make server's Bandwidth congestion; and
- Bad QoS of the server

From the above highlighted point, the DDoS attack is creating exhaustion of resources for victims and as a result of huge business losses may occur.

We briefly review some related work in this section.

In [1], paper proposed performance comparison of top three leading virtualization platform such as Microsoft (MS) Hyper-V, VMware ESXi and Xen in a virtual Lab environment. The results concluded that VMware ESXi has great flexibility to implement multiple scenario with varied parameters, in addition to this, it has also easy configuration and implementation options which lead to show the effectiveness of this platform whereas another platform required complex configuration. The user management options to control the multiple virtual servers are more granular and comprehensive. The Hyper-V and Xen have their own advantages in certain scenarios.

In [8], paper focused on studying the effects of TCP SYN attacks on processor performance and in network bandwidth. So, in this study different scenarios based flooding attack is implemented to evaluate the processor and bandwidth power. It can be concluded that, the most significant factor in processor and network performance is the period of the attacks and number of flooding packets used in each attack.

In [9], the paper focused on studying performance results of modern virtualization under TCP SYN DoS attack. The experiments cover all aspects of modern virtualization techniques and inclusively comprehensive set of benchmarks. The experimental results show the great availability of vulnerabilities in modern virtualization: even light attacks can degrade the performance of VMs at much higher rate comparing non-virtualized environment using an equal amount of resources. When the rate of attacks increased the modern virtualization becomes unresponsive to the network.

In [10], the paper designed TCP probing and developed for prevention and detection of the TCP SYN Flood attack. Initially, monitor software the captured packets with SYN field and threshold limit is used to detect malicious packet. This host based intrusion detection architecture uses TCP Probing Reply Acknowledgement Packet method for the detection of TCP SYN Flood attacks. TCP probing has computational cost and overhead.

Thorough review of different literature on modern virtualization and impact of DDoS attack on its processor there has not been found a prominent solution yet. To the best of our knowledge, we are the first to assess the effect of TCP SYN flood attack and UDP flood attack on virtualized server CPU resources and its detection using appropriate snort IDS.

3. Background

This section gives some background on hypervisors, flooding attack tool and the IDS selected for our work.

A. Hypervisors VMware ESXi

VMware ESXi is a Server-side virtualization (known as Type-1 hypervisor) which is implemented without a hosting OS to run multiple computers on single a physical hardware [11]. VMware ESXi is an industry-leading Hypervisor developed by VMware Team. It has Linux Kernel, also known as vmkernel, which is used to load a different kind of virtualization components. On a single VMware ESXi server, different and multiple OS's can be installed and run simultaneously. The virtualization is the nowadays trending platform migrating from physical resources to virtual resources in the technological world. The VMware ESXi is easy to use, flexible and has superior performance [12].

B. LOIC DDoS Tool

Low Orbit Ion Cannon (LOIC) is the GUI based open source software developed by Praetox Technologies to create DDoS attack such as TCP SYN and UDP attack that can exhaust the resources of a victim server [13].

The LOIC DDoS attack needs source URL or IP address along with the port address and attacking service (TCP or UDP). Having filled all the required information in the LOIC GUI field. LOIC starts flooding to the victim server. The TCP and UDP DDoS flooding attack have been generated in the LOIC tool to check the processor exhaustion of a victim server.

C. Snort IDS

The Snort is a lightweight and freely available software which is used to detect malicious network activity and as

result generates alerts against it. The snort is gaining substantial preferences due to its flexibility, performance and effectiveness [14]. The snort is popular and widely used to protect the network of the organization. The snort detects the attacker based on predefined set rules which are easy to write and modify.

4. Implementation

From the related work literature, it is clearly depicted that to solve DDoS attack on virtualized server from the root, there root, there is a novel solution needed. This paper shows the dangerous effect of DDoS attack on virtualized server's resources and proposed a novel solution, which is based on lightweight and free Intrusion Detection System (IDS) software, snort, has been implemented.

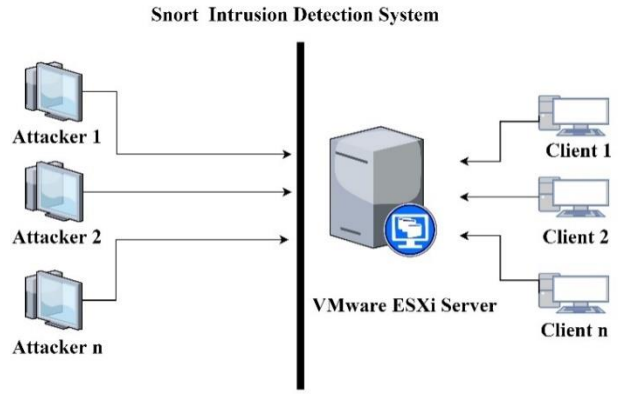

Fig. 1 Model of DDoS attack and its detection

Figure 1 illustrates the working model of DDoS attack and its detection which is implemented in virtual environment. Within it the multiple attackers are generating malicious traffic towards virtualized server. For testing of DDoS attack, Low Orbit Ion Cannon (LOIC) is easy to use and freely available software [15]. The attacker's computers are assumed to be in LOIC DDoS tool. The LOIC DDoS attack needs source URL or IP address along with the port address and attacking service (TCP or UDP) to start flooding to the victim server. Due to the ongoing advanced attacking system, the firewall somehow bypassed. Firewall is the first security defense, but not much capable of securing inside of the network [16]. On the other hand, Snort is famous open source IDS for the detecting attack effectively. Snort analyzes the real-time traffic and compare the packets against one-line rule written by user [17].

The rules can be easily write and modify according need. The Table 1 and Table 2 are the basic structure of snort IDS rules which are divided into rule header and rule option [18].

Table 1: Snort-IDS Rule Header structure

Action	Protocol	Source Address	Source Port	Direction	Destination Address	Destination Port
alert	tcp /udp	any	any	->	192.168.126.135	any

Table 2: Snort-IDS Rule Option structure

Message	Number of Packet	Time	Rule ID
msg:" DDOS attack"	count 1000	5 seconds	10002

From the above Table1 and Table 2, the snort rule line will be as follows;

alert udp any any -> 192.168.126.135 any (msg:" DDOS\ attack"; count 1000, seconds 5; sid: 10002;)

Hence; The alert will be generated by the above rule in Snort IDS, when 1000 UDP packets in 5 seconds with any type of attacking source address is sent from any kind of source port to the destination IP address 192.168.126.135 (VMware ESXi) address with any destination port number. In addition to this, it also depicts the message "DDoS attack" and having the number of rule 10002.For detecting DDoS attack the threshold method is used. If an attacker launches DDoS attack and malicious packets exceed the limit in specified time, then attack is detected.

The VMware ESXi is a Linux based virtualization machine. The latest version of VMware Esxi 6.5.0 has been installed with the hardware configuration 2 x Intel (R) i5-2410M @ 2.30 GHz CPU having 4 GB Memory. After that VMware ESXi is accessed through Secure Shell(SSH) server and esxtop command is executed which shows the CPU utilization in every second. The CPU utilization is at 2% which means the VMware ESXi is at idle state. The IP of VMware ESXi has been targeted along with port address and service (TCP or UDP). To start flooding, two scenarios have been created to testify the tolerance of CPU exhaustion of VMware ESXi.

First Scenario: The service TCP and UDP are set at port 80 (vulnerable port) separately.

Second Scenario: The performance of CPU has been carefully noted and monitor at a different level of attack. The parameters are considering as below;

Time: It is the duration in seconds through which virtualized server is affected

Number of Packets: The number of packets flooded on virtualized server

VMware CPU Exhaustion: Processor exhausted in percentage due to the flooding

Number of Packets /seconds: The number of packets flooded per duration in seconds

5. Results

This section demonstrates the statistical results and its associated graph and then analysis for the detection of distributed denial of service attacks such as TCP SYN Flood attack and UDP Flood attack. The VMware ESXi performance is observed ranges from 2% for before attack. In the first scenario, TCP service is selected in the LOIC tool for flooding on VMware ESXi. The statistical results in Table 3 and its associated graph representation in Figure 2 shows the first attack took 12 seconds to send 13000 packets on virtualized server with the rate 1083 packets per second which turns out the exhausted the server up to 21% and the second attack took 15 seconds to send 32000 packets on virtualized server with the rate 2133 packets per second which turns out the exhausted the server up to 28% and so forth. The last attack took 70 seconds by sending 277143 packets per second to halt the virtualized server. Hence; it can clearly be seen that the packets rate increases with respect to taken time the CPU exhaustion also increases. In addition to this, similarly as we increase the flood attack rate, the increase in CPU usage notifies that virtualized server will keep on degrading as it is going to higher rate. The threshold point at which, virtualized server is totally exhaust that is sending 277143 packets per second for 70 seconds.

Similarly, in the second scenario UDP service is selected in the LOIC tool for flooding on VMware ESXi. The first attack took 4 seconds to send 400000 packets on virtualized server with the rate 100000 packets per second which turns out the exhausted the server up to 25%. And The second attack took 5 seconds to send 560000 packets on virtualized server with the rate 112000 packets per second which turns out the exhausted the server up to 33% and so forth. The last attack took 10 seconds by sending 168000 packets per second to halt the virtualized server. The threshold point at which, virtualized server is totally exhaust that is sending 168000 packets per second for 10 seconds.

Table .3 TCP SYN DDoS Flood Attack

No:	Time(s)	Number of Packets	VMware CPU Exhaustion	Number of Packets / Seconds
1	12	13000	21%	1083
2	15	32000	28%	2133
3	7	72000	47%	10286
4	18	245000	60%	13611
5	35	6820000	86%	194857
6	60	13480000	94%	224667
7	70	19400000	100%	277143

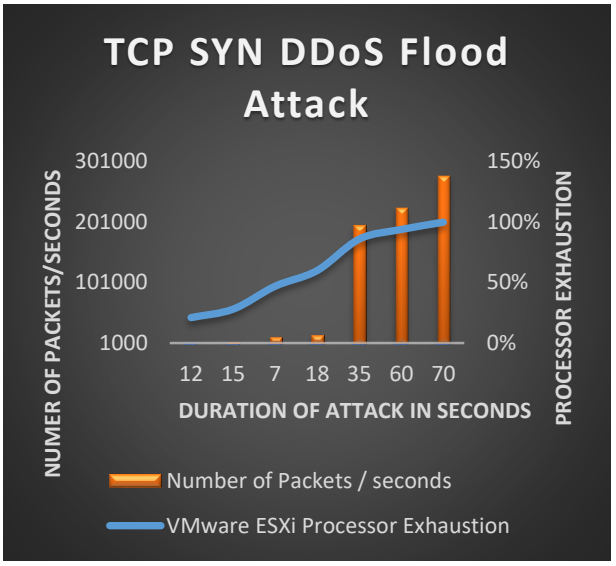

Fig. 2 TCP SYN DDoS Flood Attack

Therefore; From Table 4. The UDP Flood Attack and its associated graph 2 representation show that the packets rate increases with respect to taken time the CPU exhaustion also increases.

Table 4. UDP DDoS Flood Attack

No:	Time(s)	Number of Packets	VMware CPU Exhaustion	Number of Packets / Seconds
1	4	400000	27%	100000
2	5	560000	33%	112000
3	4	670000	59%	167500
4	5	810000	69%	162000
5	6	880000	73%	146667
6	5	980000	84%	196000
7	10	1680000	100%	168000

The comparison of Table 3 and Table 4 clearly show that VMware ESXi is more vulnerable under TCP SYN DDoS attack.

5.1 TCP SYN DDoS flooding attack Detection

In Table 3, the first attack is initiated with the packet rate 1083 for the affected time 12 seconds and the total of 13000 packets sent. By analyzing the first attack from the statistical point of view, we set the threshold for TCP SYN flood that if any attacker sends 100 packets in 5 seconds then attack will be detected by the Snort IDS. Moreover, the massage will appear on the console screen that the attacker is sending floods of packets on virtualized server to exhaust its resources.

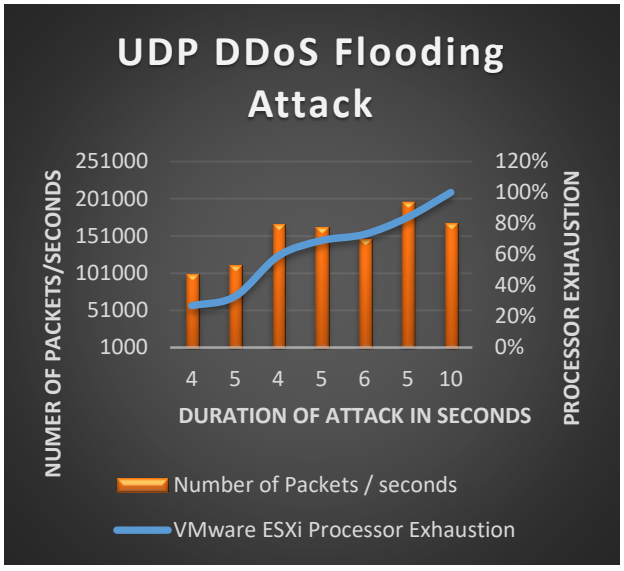

Fig. 3 UDP DDoS Flooding Attack.

Below is the script in snort IDS for detecting TCP SYN DDoS flooding attack

alert tcp any any -> 192.168.126.135 any (flags:S; msg:"\ Possible TCP SYN DDOS Flood Detection"; count 100,\ seconds 10; sid: 10001;)

The alert of message "Possible TCP SYN DDOS Flood Detection" will be generated on the console screen with signature ID:10001 if hundred 100 TCP SYN packets flooded on virtualized server for 10 seconds.

Fig. 4 Snort IDS for detecting TCP SYN DDoS flooding attack

5.2 UDP DDoS flooding attack Detection

In Table 4, the first attack is generated with the packet rate 100000 for the affected time 4 seconds and total of 400000 packets sent. After analyzing the first attack from the statistical point of view, we set the threshold for UDP flood that if any attacker sends 1000 packets in 5 seconds then attack will be detected by the Snort. Moreover, the massage will appear on the console screen that the attacker is sending floods of packets on virtualized server to exhaust its resources.

Below is the script in snort IDS for detecting UDP DdoS flooding attack

alert udp any any -> 192.168.126.135 any (msg:" Possible\ UDP DDOS Flood Detection "; count\ 1000, seconds 5; sid:\ 10002;)

The alert of UDP having message "Possible UDP DDOS Flood Detection" will be generated on the console screen

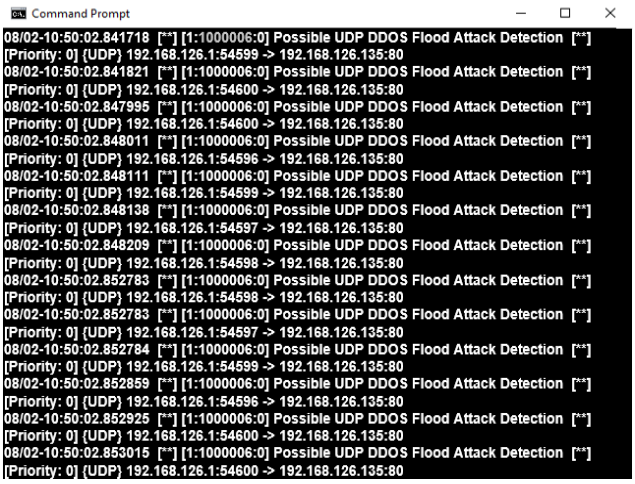

Fig. 5 Snort IDS for detecting UDP DdoS flooding attack

with signature ID:10002 if hundred 1000 UDP packets flooded on virtualized server for 5 seconds.

6. Conclusion and future work

Virtualization is going to be heart of computing technology. This tells the fragility of virtualization with respect to security threats more specifically on one of the devastating DDoS attack. The TCP and UDP are the most prominent communication protocol of the internet. In the paper, we have proposed the effect of TCP SYN and UDP flood attack on virtualized server and a novel DDoS detection. From Table 3 and Table 4, The result is conclusively deduced that if flooding packets rate increase with respect to taken time then processor exhaustion also increases. In addition to this, it is clear from our experiments that VMware Esxi is more vulnerable under UDP DDoS attack because TCP consists of heavyweight header which means it involves more packets transmission. Therefore, server is processing less TCP transmission then UDP. The proposed tool can effectively detect the DDoS attack traffic by alerting the network administrator which

facilitates easy to diagnose the problem. we plan to work with prevention of DDoS attack on virtualized servers.

References

[1] Midhun Babu Tharayanil, Gill Whitney (2015), "Virtualization and Cyber Security: Arming Future Security Practitioners". Trustcom/BigDataSE/ISPA.pp1398-1402, IEEE.

[2] Intesab Hussain, Soufiene Djahel, Zonghua Zhang (2015), " A Comprehensive Study of Flooding Attack Consequences and Countermeasures in Session Initiation Protocol (SIP)", Security And Communication Networks. John Wiley & Sons.Volume8, Issue18, pp 4436-4451

[3] Samad S. Kolahi, Amro A. Alghalbi (2014) , "Performance Comparison of Defense Mechanisms Against TCP SYN Flood DDoS Attack". 6th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops, pp 43-147. IEEE .

[4] Zouheir Trabelsi, Latifa Alketbi, (2013) " Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks",ITiCSE, pp.285-290

[5] Nattawat Khamphakdee, Nunnapus Benjamas, Saiyan Saiyod (2014), "Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection".2nd International Conference on information and Communication Technology.IEEE.

[6] Intesab Hussain, Soufiene Djahelz, Dimitris Geneiatakis (2013) "A Lightweight Countermeasure to Cope with Flooding Attacks Against Session Initiation Protocol" 6th Joint IFIP Wireless and Mobile Networking Conference (WMNC).

[7] Darren Anstee (2016), Denial of service attack data, Arbor Networks Inc.

[8] Abdulaziz Aborujilah, Shahrulniza Musa (2014) "Detecting TCP SYN Based Flooding Attacks by Analyzing CPU and Network Resources Performance",3rd International Conference on Advanced Computer Science Applications and Technologies.

[9] Ryan Shea, Jiangchuan Liu, (2012)" Understanding the Impact of Denial of Service Attacks on Virtual Machines".20th International Workshop on Quality of Service. IEEE.

[10] L. Kavisankar ,C. Chellappan (2011) "A Mitigation model for TCP SYN flooding with IP Spoofing. Proceeding of IEEE International Conference on Recent Trends in Information Technology (ICRTIT),pp. 251-256.

[11] Ammarit Thongthua and Sudsanguan Ngamsuriyaroj,(2016)" Assessment of Hypervisor Vulnerabilities". International Conference on Cloud Computing Research and Innovations, pp.71-77. IEEE.

[12] Hasan Fayyad-Kazan,Luc Perneel and Martin Timmerman(2013),"Benchmarking the Performance of Microsoft Hyper-V server, VMware ESXi and Xen Hypervisors". Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 12, pp.922-933.

[13] Bikram Khadka, Chandana Withana (2015) "Distributed Denial of Service attack on Cloud: Detection and Prevention". IEEE .

[14] Amtul Saboor, Monis Akhlaq (2013), "Experimental Evaluation of Snort against DDoS Attacks under Different Hardware Configurations". 2nd National Conference on Information Assurance (NCIA). PP 31-37. IEEE

[15] Sunny Behal, Krishan Kumar (2017) "Characterization and Comparison of DDoS Attack Tools and Trac Generators - A Review". International Journal of Network Security, Vol.19, No.3, PP.383-393

[16] Akash Garg, Prachi Maheshwari (2016), "Performance Analysis of Snort-based Intrusion Detection", System.3rd International Conference on Advanced Computing and Communication Systems, IEEE .

[17] Tomar Kuldeep, Tyagi S.S(2014)," Overview - Snort Intrusion Detection System in Cloud Environment" International Journal of Information and Computation Technology, PP. 329-334, IJICT

[18] Akash Garg, Prachi Maheshwari (2016) "Performance Analysis of Snort-based Intrusion Detection", System.3rd International Conference on Advanced Computing and Communication Systems, IEEE.