Cyber Security Flood Attacks and Risk Assessment for Internet of Things (IoT) Distributed Systems

Sanjeev Kumar, Adrian Guerrero, Christina Navarro
Cybersecurity Research Lab
Department of Electrical and Computer Engineering
The University of Texas – Rio Grande Valley
Edinburg, TX 78539, USA

2023 IEEE World AI IoT Congress (AIIoT) | 979-8-3503-3761-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/AIIoT58121.2023.10174553

Abstract— **Cyber-attacks continue to create havoc for Internet connected services and systems. Cyber-attacks can compromise not only a single computer system but also a distributed computing system such as Internet of Things (IoT) devices and networks. Distributed Denial of Service (DDoS) based cyber security attacks can have varying adverse impacts on the operation of a computing system. There are different types of DDoS flood attacks found to be commonly used include Ping flood attacks and TCP-SYN flood attacks against distributed systems and IoTs. In this paper, for evaluation purposes, we conducted experiments to measure the impact of these two common flood attacks on the operation of an Internet connected computer system. The impact of flood attacks on the computing system under two flooding mechanisms were measured and compared for risk assessment and risk profiling for AI training for effective protection.**

***Key Terms*— AI, Cybersecurity flood attacks, Distributed IoT systems, Risk assessment.**

I. INTRODUCTION

Today, electronic devices with Internet capabilities have become a necessity in modern society. However, these devices are prone to cyber-security attacks such as the Distributed Denial of Service (DDoS) attacks, which can involve multiple Denial of Service (DoS) agents configured to send attack traffic to a single victim computer or to the entire distributed computer system such as IoT network shown in Figure 1, to exhaust its resources [1-5], [9-16]. Figure 1 depicts the cybersecurity risks due to DDoS based attacks not only for a single computing system but also for a distributed computing system such as IoT system.

Flood attack is a type of DDoS attack where a barrage of certain traffic is sent to the victim computing or IoT system causing exhaustion of computing resources. When the computer system's available resources are exhausted under flood attacks then the victim computing system is unable to deliver intended services. For IoT systems, under such attacks, their availability component of the CIA security triad will be affected, and they will be unable to operate as intended.

The CIA security triad is comprised of three main components, which includes- Confidentiality, Integrity, and Availability. In DDoS attacks, the availability component is affected due to exhaustion of resources of the victim IoT systems, whose performance can be degraded or becomes inoperable, or become unable to deliver the intended quality of service [2-5].

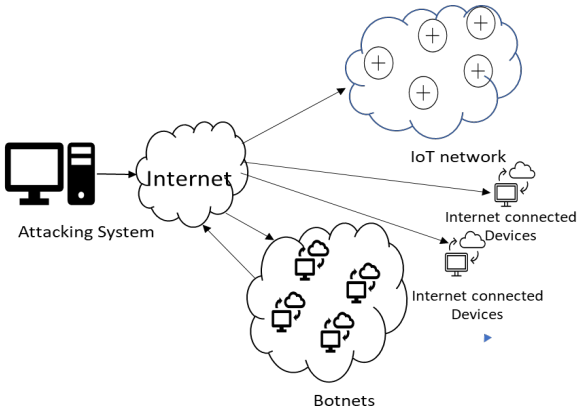

Figure 1: Cybersecurity risks for IoT networks

In this experimental work, a group of simulated botnets were used to simulate DDoS attacks of different types and intensity for comparison purposes and a victim computer system was used to evaluate their impact for comparison purposes. Botnets are a group of Internet connected computers compromised by a security breach (introduced by distribution of malware) where a third party takes over the control of such a group of computers or distributed IoT systems [6]. Then the compromised computers, called bots, are controlled by an attacker to send harmful traffic to a victim computer system which can be a single system or a distributed IoT system. The attacker attempts to exhaust a victim computer's resources to potentially disrupt its normal operation. As a result, a victim computing system becomes inoperable and unavailable to deliver intended services to legitimate users.

II. DDoS Flood Attacks

In this experimental work, two common DDoS flood attacks, namely the Ping flood and TCP-SYN flood attacks were used, and their impacts were measured. A Ping flood attack primarily exploits Internet Control Message Protocol (ICMP) which is one of the commonly used diagnostics tools aiding in network troubleshooting [1] [14]. Figure 2 shows the frame format of ICMP echo request and echo-reply messages.

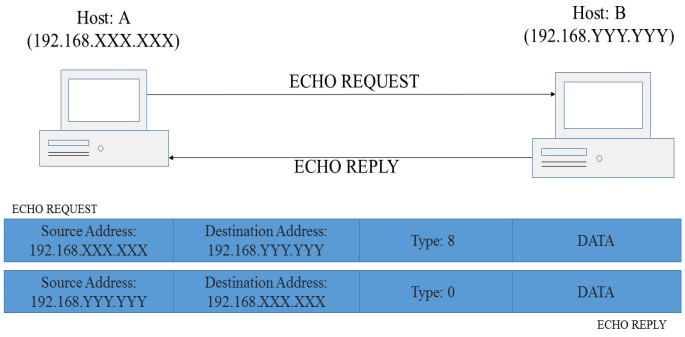

Figure 2: ICMP Echo Request/Reply Message Format

Common ICMP messages known as echo request (Ping) and echo reply allow communication between hosts for inquiries of reachability and packet size in bytes [9]. Additionally, an echo reply is mandatory to be sent for each echo-request received as required by RFC-792 [9].

ICMP messages are commonly exploited by hackers to pose cyber-security attacks on a host or multiple hosts. For instance, Ping flood attacks send an excessive amount of echo request packets to a victim computing system to saturate their capacity. As mentioned before, each request requires a response which further exhausts a victim system of resources to operate properly [12]. Typically, a botnet distributes echo requests to a victim computer, which determines the severity of each DDoS attack.

A TCP-SYN flood attack manipulates the Transmission Control Protocol (TCP) three-way handshake (Figure 3), which is defined as a network communication between two hosts to establish connection between both parties [13]. Essentially, the three-way handshake is an exchange of multiple TCP packets between two hosts as described and shown below [13-14]:

1. Request (TCP-SYN) packet sent from Host A to Host B
2. A new TCP SYN packet and Acknowledgment (SYN-ACK) packets sent from Host B to Host A
3. Final Acknowledgement (ACK) packet sent back to Host A from Host B

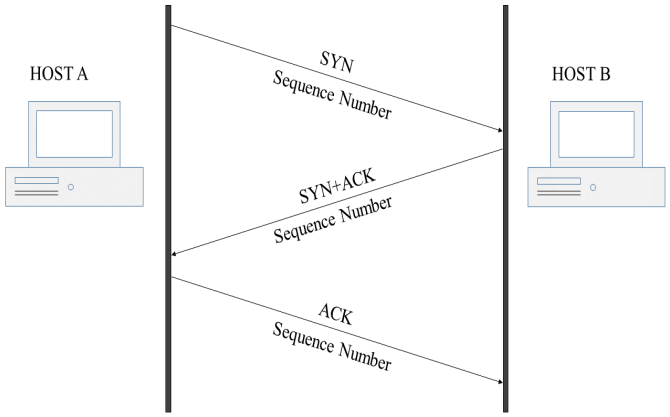

Figure 3: TCP Three-Way Handshake

In TCP-SYN attack, this packet exchange process is manipulated by sending an overwhelming amount of TCP connection requests to a victim host. Furthermore, a victim system is required by RFC-793 to respond to each individual TCP connection request message [8]. For each SYN-ACK packet sent by a system under SYN flood attack, an attacker does not send the final ACK packet creating a half-open connection [13]. Thus, a half open connection is a partial completion of the first two handshakes of the TCP three-way handshake (Figure 3) protocol. Ultimately, a victim computing system under a TCP-SYN flood attack cannot close the connection and keeps it open for some time hoping to receive the final ACK packet required by the three-way handshake [8]. Eventually the connection between the two systems will close by executing a time-out instruction, as described in RFC 793 [8] but it may be too late to avoid the attack. Lastly, the result of a TCP-SYN flood attack is network saturation of a victim system (single system or a distributed IoT system) due to a large number of half-open connections [13].

III. Botnet Size Configuration

In this experiment, a large-scale botnet size was used to simulate Ping and TCP-SYN flood attacks, where botnet size varied for different intensities of an attack. Botnet sizes are configured by manipulating the source Internet Protocol (IP) address of an attack system. Moreover, IP addresses are classified in the following two categories: Classful & Classless Interdomain Routing (CIDR) IP addresses, as described in detail below. A more practical IP address scheme widely used today is CIDR addresses because more address space becomes available by not restricting network or host space to only three different classes [10]. By restricting network or host space, therein lies potentially unused IP address space [10]. CIDR addresses only consider network address and prefix simplifying the addressing itself in comparison to Classful IP addresses [10]. Each class can be used to simulate different botnet sizes. For a large-scale botnet, Class A subnet can be configured to simulate approximately sixteen million compromised hosts [9-10].

IV. Experimental Setup

In this experiment, a DDoS flood attack was simulated in a controlled & closed network environment where DDoS flood attacks utilized Class A botnet size configuration. In this case, for experimentation, the victim system under attack was an Apple iMac with Windows 10 Pro version-1809 installed. Additionally, the victim system had the following specifications:

- 2.5GHz Quad-Core Intel Core i5
- 8GB (two 4GB) of 1333MHz DDR3 Random Access Memory (RAM)
- Network interface bandwidth of 1 Gbps

Figure 4 depicts an experimental configuration for simulation of flood attack traffic under experimentation [9].

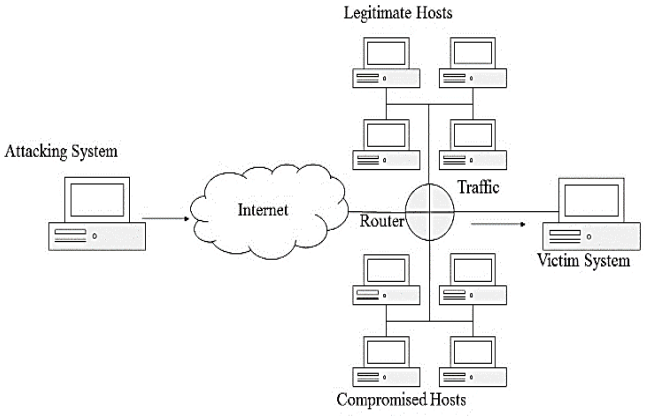

Figure 4: Experimental Setup [9]

The DDoS attacks include a set of simulated hosts with a range of over sixteen million IP address spaces. DDoS attacks implemented for comparing their impact in this experiment are Ping flood and TCP SYN floods which targeted an Apple iMac platform with a Microsoft Windows operating system installed for measurements. Similar impact can be observed with the distributed IoT system if used as a victim system, however here the goal is to rather compare the flood attacks themselves irrespective of the victim system being used.

In each flood attack experimentation, two different types of network traffic are sent to the victim system simultaneously, which are legitimate traffic mixed with attack traffic. In this case, legitimate traffic is defined as host simulations performing multiple requests of a website for reachability. These simulated legitimate hosts send 3000 HTTP transactions per second (Baseline value for the legitimate connections under no attack traffic) to the victim computer system to simulate legitimate traffic. Additionally, the victim system (Apple's iMac) hosts a website originating from a built-in Microsoft Windows service called Internet Information Services. The service uses sub-services called Web Management Tools and World Wide Web Services to support the Web server. The website generated consists of a single webpage simply to provide availability.

To measure the impact of different attacks, attack traffic is generated by a simulated large-scale botnet size of varying attack traffic intensity. Attack traffic is divided into low scale and high scale traffic scenario. A low scale attack refers to an attack traffic bandwidth being less than 20% of the link bandwidth, remaining 80% can be good Internet traffic. The high scale attack refers to the attack traffic that can consume entire link-bandwidth. For the case of low scale attack, attack traffic was sent to the victim system beginning with two percent of the total link bandwidth (1Gbps) and it was increased by two percent until twenty percent of 1Gbps was reached. Furthermore, an additional experiment is conducted where attack traffic intensifies by extending each increment and amounts of data within each increment being sent to the victim system. Essentially, attack traffic was sent beginning with ten percent of the maximum data rate with increments of ten ending with the total link bandwidth. Here we investigate the impact endured by the victim system under low attack traffic and high attack traffic conditions.

All DDoS attacks are simulated to obtain the following information: HTTP transaction rates, overall processor utilization, and available memory under flood attack conditions. Analysis and evaluation of each data set consider the effects of each DDoS flood attack and risk posed on the victim system.

V. Experimental Results

We conducted experiments under Ping and SYN flood attacks in a simulated large-scale botnet configuration. Results presented in this section consist of three different experiments which vary in flood attack type and intensity. Two Ping flood attacks of small-scale and large-scale are sent to the victim system with different attack traffic intensities, as shown in Figures 4 & 5. Also, results of a single SYN flood attack (small scale, lower intensity) on the victim computer system are shown in Figure 4 for comparison purposes. Essentially, in these experiments we intended to measure the impact of these flood attacks on HTTP transaction rates and to find at what intensity these transactions stopped completely. Subsequent paragraphs describe Ping and SYN flood attacks individually then in comparison for an analysis of the data obtained during each experiment. Small-scale attack ranges from 0 to 200Mbps (20% of 1Gbps link bandwidth), whereas the large-scale attack traffic ranges from 0 to 1Gbps i.e., up to 100% of the link bandwidth.

Small-scale Ping flood and TCP-SYN flood attacks:
For small-scale attacks (Figure 5), Ping flood attacks didn't have significant adverse impact on HTTP transactions exchanged with the victim computer system. However, small-scale TCP-SYN flood attack of lower intensity impacted the victim system more so than Ping flood after it exceeded eight percent of total link bandwidth, as shown in Figure 4. For

large-scale attack (Figure 6) shows HTTP transactions exchanged within the experimental system during a Ping flood attack where the attack traffic increased to 1Gbps. Figure 6 shows a steep decline in HTTP transaction rates for large-scale Ping flood attacks starting as the attack increased beyond the 20% of the link bandwidth (i.e., > 200 Mbps) and it resulted in total blocking of HTTP transactions at 1 Gbps. As seen in Figures 5 & 6, the Ping flood attacks show their adverse impact on the HTTP exchanges with the victim computer only under the large-scale attacks, i.e. higher Ping-flood traffic flows.

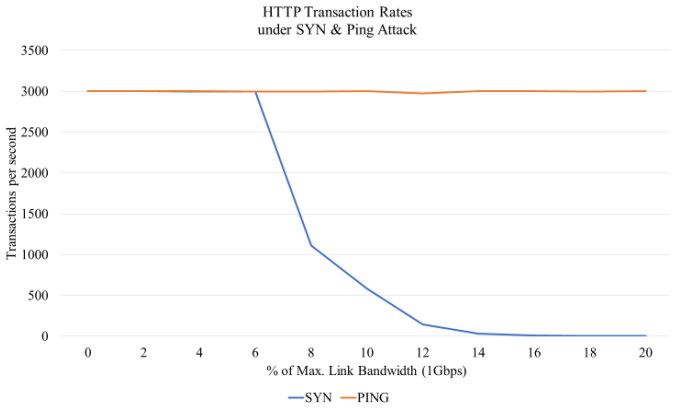

Figure 5: HTTP Transaction Rates measured under Ping and TCP-SYN flood attacks of small-scale load < 20% of link speed.

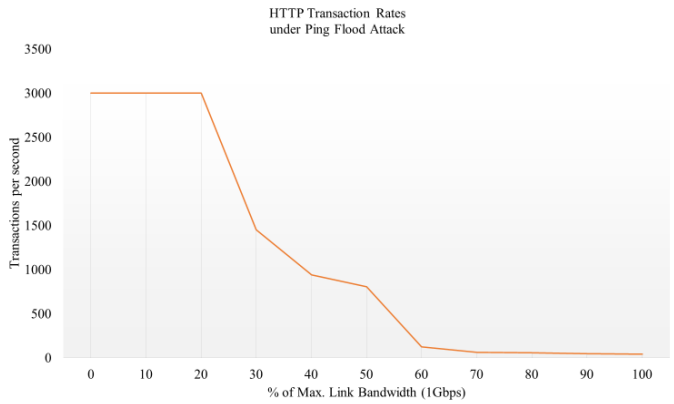

Figure 6: HTTP Transaction Rates measured under Ping flood attack with large-scale load up to 100% of link speed.

We observed the complete loss of HTTP transactions under these flood attacks for both the small-scale (<20% of link speed) and large-scale attacks. The computing system was not able to deliver intended services under these flood attacks. The degree of impact depended on the traffic flow type and flow intensity. There was a complete loss of HTTP transactions (Figure 5) under small-scale TCP-SYN flood attacks (<20% of link speed). A relatively lower rate of 14% of TCP Syn attack traffic flow caused all HTTP connections to be disrupted. However, the HTTP transactions were not affected (Figure 5) by the same small-scale Ping flood attack traffic (< 20% link speed). It took large-scale, higher intensity of Ping flood attack traffic (more than 70% load) to cause complete loss of HTTP transactions (Figure 6).

We investigated what was causing the loss of HTTP transactions under these flood attacks. We measured the memory consumption and the processor utilization under these flood attacks. It was found that the computer system's memory was not affected much by these flood attacks compared to the baseline memory utilization.

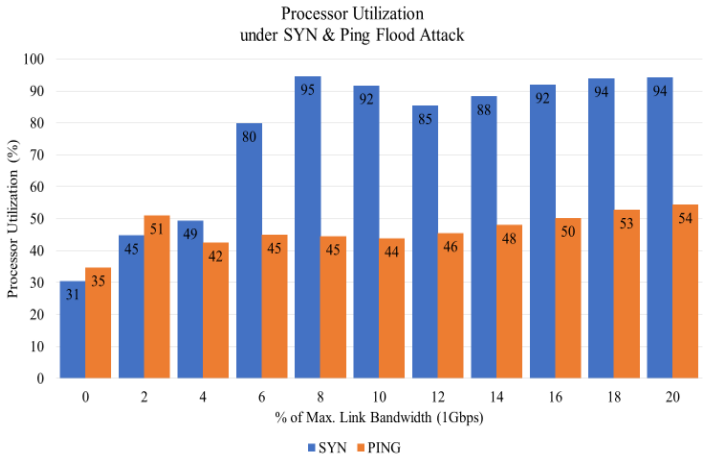

Figure 7: Total processor utilization for small-scale low intensity attacks under Ping floods and TCP-SYN floods.

However, the processor was excessively consumed by these flood attacks (Figure 7) resulting in high processor utilization. Clearly, the cause of loss of HTTP sessions was due to processor exhaustion instead of memory exhaustion hence these flood attacks were processor intensive. It was observed that TCP SYN flood attacks exhausted the processor much more quickly compared to the Ping flood attack for the same traffic intensity. This measurement shows that TCP SYN attack is capable of doing more damage with less traffic intensity, and hence it is assigned a high-risk category based on our risk assessment. Similarly, Ping attack can be assigned a lower risk-level as the damage to computing performance was not affected by small-scale attack traffic. The computing performance started to get affected only when the Ping attack traffic was increased to higher traffic loads (Figure 6).

Based on our experiments we created a risk-assessment profile for these two different traffic flows, Ping traffic and TCP-SYN traffic, and assigned a risk level to them in Table 1.

Risk profiling helps in mitigation of flood attacks. To mitigate these flood attack problems, appropriate Artificial Intelligence (AI) / Machine learning (ML) schemes can be used to design

self-learning systems to detect and prevent cyberattacks on an IoT network [17]. Some of the machine learning schemes [18] used for AI-based cyberattack detection are ensemble learning, inductive learning, artificial neural networks, decision trees, Bayesian networks, naïve Bayes etc. A well-trained AI based Intrusion Prevention System can detect known and unknown attacks (zero-day attacks) based on different traffic flows.

Table 1: Risk assessment for different traffic flows

Traffic flows	Memory Intensive	Processor Intensive	Risk Assessment
Ping traffic flows	No, Memory consumption not impacted	Yes, low processor exhaustion at low traffic (< 20% of link speed)	Low risk
TCP SYN traffic flows	No, Memory consumption not impacted	Yes, high processor exhaustion at low traffic	High risk

Here in this work, we measured and analyzed only two different types of harmful traffic flows that can compromise performance of a distributed computing system or an IoT system. However, there are many more known and unknown flood attacks that can compromise the performance of a computing system or an IoT system. They are not the same in their impact on the computing system. By monitoring different traffic flows, an AI based protection system can automatically create a risk profile for different types of known and unknown flood attacks against an IoT distributed system. Automated risk profiling can help AI based intrusion prevention systems to improve accuracy of detection and effectiveness of mitigation against different types of known and unknown (zero-day) attacks.

VI. Conclusion

Both the Ping flood and TCP SYN flood attacks pose risks to a computer system which may be a single system or a distributed IoT system. It was found that different types of flood attacks pose different levels of risks to the victim computers in delivery of their services. The small-scale TCP-SYN flood attack was found to be capable of causing the complete loss of legitimate good HTTP transactions, whereas the same computer system was not affected by the small-scale Ping flood attacks. The TCP-SYN attack caused more legitimate good connections to be dropped compared to the similar intensity of the PING flood attack. Only the large-scale Ping flood attacks had adverse impact on the computing system. Furthermore, TCP-SYN flood attack was found to exhaust the victim's overall processor much quicker than the Ping flood attack of the same intensity. The TCP-SYN flood attack was more processor intensive causing greater processor exhaustion and higher HTTP-transaction drop rates. These experiments show the fact that all flood attacks are not the same, and different flood attacks have different risk profiles. Risk profiling can help in preventing attacks. AI based prevention systems can take advantage of risk profiling. Traditional non-AI based prevention systems have many false positives, and many false negatives especially for zero-day attacks where attacks go unnoticed by the detection system. AI/ ML based detection and prevention system can use various AI/ML techniques to monitor and analyze traffic to identify anomaly in traffic patterns. AI/ML based detection systems can be trained to automatically create different risk profiles for different traffic flows. Risk assessment will help AI/ML based protection systems to detect attacks much in advance, with greater accuracy, reduce instances of false positives and false negatives for anomaly-based detections, and take automated preventive actions to defend IoT based distributed systems.

ACKNOWLEDGMENTS

The support for this research was provided in part by the US National Science Foundation, Houston Endowment Chair in Science, Math and Technology Fellowship, Benston Jr. Endowment Chair fellowship in Engineering, and in part, the Department of Homeland Security.

REFERENCES

[1] W. Rivas and S. Kumar, "Evaluation of CentOS performance under IoT based DDoS Security Attacks," proceedings of *3rd International Conference on Data Intelligence and Security (ICDIS)*, pp. 64-70, January 2021.

[2] S. Kumar, H. Kumar and G.R. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," proceedings of *IEEE International Conference on Data Intelligence and Security,* vol.2, pp. 5-9, June 2019.

[3] S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, San Jose, CA, July 2007, pp. 25-25.

[4] S. Kumar, "Impact of a Distributed Denial of Service (DDoS) Attack Due to ARP Storm," *Lecture Notes in Computer Science (Book Series -LNCS-3421-Springer Verlag),* pp. 997-1002, April 2005.

[5] S. Kumar and O. Gomez, "Denial of Service Due to Direct and Indirect ARP Storm Attacks in LAN Environment," *Journal of Information Security*, Vol. 1 No. 2, 2010, pp. 88-94. doi: 10.4236/jis.2010.12010

[6] M. Feily, A. Shahrestani and S. Ramadass, "A Survey of Botnet and Botnet Detection," *2009 Third International Conference on*

Emerging Security Information, Systems and Technologies, Athens, Glyfada, 2009, pp. 268-273

[7] Postal, J. (1981) Report for Comments for ICMP, *RFC 792.* http://www.ietf.org/rfc/rfc792.txt

[8] Postal J. (1981) Report for Comments for Transmission Control Protocol, *RFC 793*. https://www.rfc-editor.org/rfc/rfc793.txt

[9] H. A. Herrera, W. R. Rivas and S. Kumar, "Evaluation of Internet Connectivity Under Distributed Denial of Service Attacks from Botnets of Varying Magnitudes," *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, June 2018, pp. 123-126

[10] "IP Addressing and Subnetting for New Users." Cisco, 19 Oct. 2017, www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

[11] Gunnam, G.R. and Kumar, S. (2017) Do ICMP Security Attacks have Same Impact on Servers? *Journal of Information Security*, 8, 274-283. https://doi.org/10.4236/jis.2017.83018

[12] Junior, R. and Kumar, S. (2014) Apple's Lion vs Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks. *Journal of Information Security*, 5, 123-135. doi: 10.4236/jis.2014.53012

[13] Kumar, Sanjeev, and Einar Petana. "Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software." *7th International Conference on Networking* (ICN 2008), 2008, doi:10.1109/icn.2008.77

[14] Petana, Einar, and Sanjeev Kumar. "TCP SYN-Based DDoS Attack on EKG Signals Monitored via a Wireless Sensor Network." *Security and Communication Networks,* vol. 4, no. 12, 2011, pp. 1448–1460., doi:10.1002/sec.275

[15] Surisetty, Sirisha, and Sanjeev Kumar. "Apple's Leopard Versus Microsoft's Windows XP: Experimental Evaluation of Apple's Leopard Operating System with Windows XP-SP2 under Distributed Denial of Service Security Attacks." *Information Security Journal*: A Global Perspective, vol. 20, no. 3, 2011, pp. 163–172., doi:10.1080/19393555.2011.5699

[16] Kumar, Sanjeev. "PING Attack – How Bad Is It?" *Computers & Security,* vol. 25, no. 5, 2006, pp. 332–337., doi:10.1016/j.cose.2005.11.004

[17] Xiao, Wan, Lu, Zhang and Wu, "IoT Security Techniques Based on Machine Learning," *IEEE Signal Processing Mag*. Sept. 2018, pp. 41-49

[18] Ayesha S. Dina, D. Manivannan, "Intrusion detection based on Machine Learning techniques in computer networks," Elsevier *Internet of Things Journal,* Vol.16, December 2021.

Sanjeev Kumar (M'1993–SM'1999) is a professor in the Department of Electrical and Computer engineering at the University of Texas-RGV. He is active in teaching & research in the area of computer network security, IoT, AI/machine learning applications, Cloud Computing, Critical Infrastructure security, Wireless Ad Hoc Networks. Before joining UT-RGV, he worked with the leading Computer Networking companies in the United States. He served as a member of the technical program committee for numerous national and international conferences and served on editorial board of several Journals. He has been awarded US and International patents for his inventions in Internet technologies. He received many teaching excellence awards at his university, including the prestigious UT System Regents' Outstanding Teaching Award (ROTA). He received the Ph.D. degree from Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, North Carolina. He is a senior member of IEEE.

Adrian Guerrero graduated with an MS in Electrical Engineering from the University of Texas- Rio Grande Valley in 2020. His thesis research was in the area of cybersecurity evaluations.

Christina Navarro graduated with an MS in Electrical Engineering from the University of Texas- Rio Grande Valley in 2020. Her thesis research was in the area of cybersecurity evaluations.