http://www.jctjournals.com ISSN(ONLINE):2278 - 3814

Volume-12, Issue-08, August 2023
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-06

A Literature Survey of Distributed Denial of Service (D-DoS) Attack Detection using Machine Learning Approach

[1]Pravin Tukaram Zhunjare, [2]Prof. Lalita B. Randive,
[1]M.Tech Scholar, [2]Assistant Professor ,
[1, 2,]Department of Computer Science and Engineering,
[1, 2]Marathwada Institute of Technology, Aurangabad, M.H., INDIA
[1,2] Dr. Babasaheb Ambedkar Technological University Lonere, Raigad, M.H., INDIA
[1]ptzhunjare@gmail.com, [2]lalita.randive@mit.asia

Abstract—In this paper, we discuss on the nature of the threats posed by Distributed Denial of Service (DDoS) attacks on large networks, such as the Internet, demands effective detection and response methods. These methods must be deployed not only at the edge but also at the core of the network. This paper presents methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. The DDoS attacks show anomalies in the characteristics of the selected packet attributes. The detection accuracy and performance are analyzed using live traffic traces from a variety of network environments ranging from points in the core of the Internet to those inside an edge network. The results indicate that these methods can be effective against current attacks and suggest directions for improving detection of more stealthy attacks. We also describe our detection-response prototype and how the detectors can be extended to make effective response decisions.

Keywords— Internets of Things (IoT), Multi-Access Edge Computing (MEC), Distributed Denial-of-Service (DDoS), Software-Defined Networking (SDN), Network Function Virtualization (NFV), Service An Acknowledgment (ACK), and Transmission Control Protocol (TCP) etc...

I. INTRODUCTION

The advent of 5G networks and IoT infrastructure is expected to foster more steady and trustworthy connections and communications. Many Internets of Things (IoT) technologies will benefit from 5G's new radio access technology because of its zero delay, highly available, and remarkable power.5G-enabled IoT technologies, meanwhile, need not only to boost network speed; they should also maintain security and enhance service dependability. The EU commissioned a study that found the increased reliance on software to power 5G cellular poses security concerns that are "expected to surface or become more apparent." If an assault is undertaken against a 5G network and is successful, it might have serious consequences. This has been understood by hackers who are using new tactics to monetize their attacks by controlling sensitive data, asking for ransom, or making the network unavailable. As a result, 5G network security was particularly vulnerable to attacks from both within and outside the network. Insider players in a network are those who work for the network itself. Insiders in the network might be the cause of data breaches and service tampering, for example 5G enabled IOT applications are expected to suffer from several security issues due to the complexity and expansion of the attack surface. The increasing scale of devices connectivity and interconnectivity along with network slicing will enable a new range of IOT applications. Yet, one of the weak spots in security will be the devices themselves; they can be remotely controlled to form what is known as a botnet to perform serious security attacks. Most of the existing IOT devices were not developed with security as a priority. Intrusion detection approaches may become less accurate and more difficult as the number of data points collected by IOT devices grows dramatically. As a result, it is important to investigate novel approaches to detecting security assaults in 5G networks. As an additional improvement, it would be possible to anticipate network assaults. Because, once we recognize the possibility of attacks, and verify the insufficient protection, faster mitigation and recovery processes can be deployed. Many security threats, most especially DDoS attacks, must be addressed to protect 5G networks. In the present cellular network, there is just one

Copyright © 2023. JCT Publications. All Rights Reserved

service that can be compromised by a DDOS assault (such 4G). On the other hand, 5G networks, if a malicious hacker takes control of a slice and launches a DDOS attack, this could compromise services belonging to the same virtual network.

1.1 An attack-resistant 5G IoT infrastructure

A tiered system to protect 5G networks in the future as part of the Internet of Things. The security mechanisms used in the architecture to detect and recognize attacks in 5G-enabled IoT networks are therefore explained. A Secure 5G Enabled IoT Architecture: An Overview Fig.1 represents the hierarchical 5G enabled IoT security architecture based on distributed multi-access edge computing (MEC). The three phases of this structure are access, MEC, and the cloud. It is the MEC element's job to receive data from the access layer's devices. Computing hardware may take the form of a server, a device that connects devices, or a communication router. All information captured at this tier is sent in real time to gateways connected to the 5G network. High-priority Internet of Things (IoT) applications need instantaneous data transmission, which the 5G network can supply. The gateways' jobs include handling connections between machines and relaying command signals to the right places.

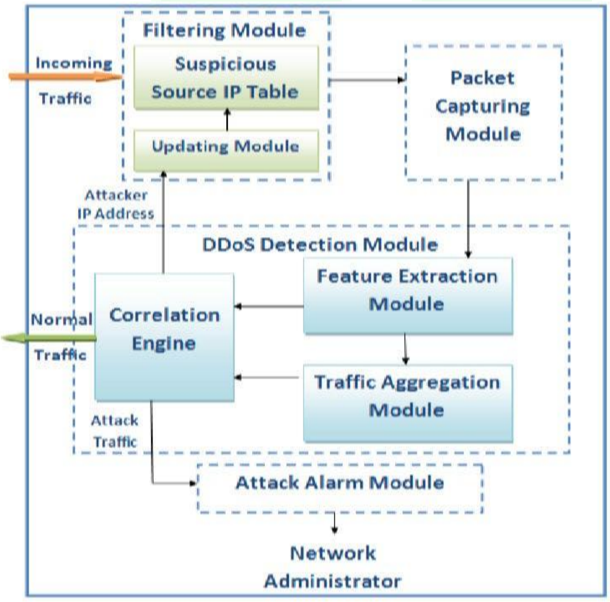

Fig. 1 Entry layer to accept data from the physical universe; MEC layer to identify, recognize, and fight security attacks; this is the architecture for 5G-enabled Internet of Things applications., and cloud layer to store the data.

To ensure system scalability regarding the number of connected devices, new gateways can be dynamically activated and managed independently. Data collection is followed by processing and analysis at the MEC tier, which outsources all calculations from devices to edge servers to compensate for issues like low processing power and excessive latency on the devices themselves. MEC provides a new ecosystem where communications are rapidly performed between networks using MEC hosts. Though, for illustration, MEC hosts are often stationed about a block or two from devices, the latency of their transmissions is often sufficiently low for real-time algorithms to work correctly. In this layer,the goal of setting up 5G portals is to collect data from the access point, analyse it, and then send it to the core network or edge nodes, where it can be used to provide more services Although MEC can process a high amount of traffic, it suffers from security challenges.

II. LITERATURE REVIEW

At present times, the user wants faster data transmission speed and secures services. 5G NR promise to deliver all the basic as well as advanced facilities in contrast to prior. This technology allows users to high-definition and volume data within a second. 5G Technology 5G can handle larger traffic to cover the massive demand of the devices. 5G NR uses mmWave, tiny cells, massive MIMO, beamforming, and full-duplex to achieve this goal. These technologies, however, remain in their infancy and have not been verified.

Marian Gusatuet.al. (2022):- As a 5G-enabled solution, Multi-access Edge Computing (MEC) works to relocate cloud-computing resources closer to the actual consumers. In order to protect 5G MEC networks against Distributed Denial-of-Service (DDoS) attacks, this study explores countermeasures that make advantage of the network's virtualized infrastructure and its management entities. The methods described here are an expansion on research conducted in, and they are geared at mitigating the potential for harm to legitimate traffic in the event of DDoS assaults. Our research backs the concept of using a network flow collector that transmits the data to an anomaly detection system based on AI approaches, and it improves upon prior research by helping to reroute discovered anomalies for isolation to a distinct virtual machine. This virtual machine uses deep packet inspection tools to analyze the traffic and provides services until the final verdict. By separating the bad behavior, we make it less likely that it will spread to the virtual machine that serves normal customers. The MEC architecture's administration entities allow us to create and destroy virtual machines and change various configurations. Hence, If an attack causes the computer that is evaluating the isolated traffic to crash, it won't affect the services for real users [1].

Yea-Sul Kim et.al. (2022):-The ultimate objective with the next 5G cellular networks is to create a low-latency, greater Internet of Things (IoT) ecosystems. Scattered interruption of system (DDoS) attacks on 5G phone carriers may be caused by insecure IoT devices at the Tbps level. The use of machine learning (ML) technologies for autonomous network intrusion detection is thus gaining attraction in 5G networks. We expect that machine learning-based DDoS attack monitoring in a 5G network will be very quick. Because of this, it is feasible to make use of a showcase procedure that may discover characteristics crucial for learning in big datasets while simultaneously decreasing

Copyright © 2023. JCT Publications. All Rights Reserved

computing complexity and increasing speed. The majority of current machine learning (ML) DDoS attack detection technologies are devoted to wired Internet teaching materials. In addition, there is a lack of study on feature engineering for 5G traffic. As a response, our survey involved experimentation with feature selection to hasten the analysis and detection of increased DDoS assaults in real time. based on ML in a 5G core enhance, it's crucial to want an effective feature selection for both training and detection. work environment. The results of the experiment showed that the performance was maintained and improved when the feature selection process was used. In particular, the disparity in temporal difficulty widened significantly as the quantity of a dataset grew. Experiments demonstrate that large-scale DDoS assaults on 5G core networks may be detected in real time using the feature selection approach. This highlights the significance of a noise-free feature set during training and detection, which may be achieved via the feature selection process. Using machine learning to investigate features for identifying network activity transiting the 5G core with low latency, this study has the potential to enhance the efficacy of automated detection technologies for DDoS assaults on 5G networks [2].

Mahmood A. Al-Shareeda et.al., (2022):- Both the public and private transportation sectors place a high value on traffic safety and efficiency. In order to assist drivers and passengers, 5G-enabled vehicular networks may wirelessly share data with one another. Due to the automobile broadcasting the traffic state knowledge, privacy and security are viewed as issues in 5G-enabled vehicular networks. Numerous privacy-preserving and protection strategies have been developed to meet these standards. Since these techniques need complex elliptic curve and bilinear pair cryptography procedures, the performance efficiency in terms of communication and processing costs is inadequate, leading to DoS attacks. In order to address this problem, the authors of this piece suggest a technique for 5G-enabled vehicle networks called Modular Square Root-based Defeat of Service Attacks (MSR-DoS). Our MSR-DoS solution provides unlink ability, traceability, and revocation, as well as assurances for the validity of the source, the integrity of the message, and the privacy of the pseudonym. Burrows-Abadi-Needham (BAN) theory demonstrates that working in our field is risk-free. Analysis of performance shows that the MSR-DoS system uses less money on communication and computation than government tasks. The computational complexity of signing and validating a message is minimized by 99.80% and 98.55%, respectively, using the proposed MSR-DoS method [3].

Hao Wang et.al., (2022):- One of the most distinguishing features of 5G cellular networks is its ultra dense deployment, made possible by mmWave technology. Load balancing across edge nodes is an excellent way to mitigate the effects of a distributed denial of service attack. However, congestion in multiuser and multiage server architectures has received relatively less attention in the majority of previous research. It seems that M/M/1 model users are oblivious to the fact that different scheduling techniques might have different effects on the Markov property of the task arrival process. This book introduces the G/M/1 paradigm to edge server job scheduling for the first time to enhance load balancing amongst edge servers, with the goal of guaranteeing a high quality of experience (QoE) for end users. Metrics are defined for the MAB algorithm framework that measure its level of homeostasis. Each edge node's processing of a particular job and the number of users it is responsible for are considered. We compared its experimental performance on a real-world dataset to that of two reference methods and three state-of-the-art methods. Furthermore, empirical evidence supports the efficiency of this approach [4].

Nashid Shahriar et.al(2021):- When it comes to 5G networks, network slicing is a critical enabling technology since it allows for several virtual networks to exist inside a single physical one. However, the functionality and performance of network slices may be substantially impaired by a Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) assault. To add insult to injury, modern DoS/DDoS attack detection methods rely on data sets gleaned from 5G network simulations rather than actual 5G network slices. To begin, we demonstrate how performance metrics like bandwidth and latency for slice users might be affected by distributed denial-of-service (DDoS) assaults in this research. Then, we provide a new dataset of DoS and DDoS attacks gathered from a hypothetical 5-generation network slicing testing ground. Finally, we showed a deep-learning-based bidirectional LSTM (Long Short Term Memory) model, namely, Slice Secure can detect DoS/DDoS attacks with an accuracy of 99.99% on the newly created data sets for 5G network slices [5].

Vijey Thayananthan. et.al (2021):- The fifth-generation (5G) network supports many systems such as reliable communication in potential applications that require maximum security. Software-Defined Networking (SDN) is advancing because several servers are using different types of Cloud Technology (DC) architectures to target new network topologies. Attackers using Distributed Denial of Service (DDoS). The security of SDN-based 5G technology is problematic and challenging due to DDoS assaults sent by malevolent users. Despite the multitude of solutions to the issue of DDoS attacks in SDN, guarding the SDN controller remains one of the most difficult tasks in the field. Examining the most efficient machine learning (ML) techniques for protecting SDN controllers against DDoS attacks is the focus of this study. Using the ML method, a tunable bandwidth mechanism, and a dynamic threshold approach, we propose a security strategy for the

Copyright © 2023. JCT Publications. All Rights Reserved

present investigation. Since DDoS attacks are a major concern for SDN controllers, the primary focus is on how to best protect against them using a machine-learning-trained model. To better protect the SDN controller and the whole network, the proposed strategy employs the most effective ML techniques currently available. In this method, the Extreme Gradient Boosting (XG Boost) and other ML algorithms were used, which not only enhance the accuracy of the security solutions but also improve the overall network performance [6].

TABLE - I COMPARISON OF DIFFERENT PREVIOUS METHODS

Year/ ref.	Title Name	Method	Result
2022/[01]	methods for preventing distributed denial of service attacks in 5G multi-access edge computing	method	protection against DDOS
2022/[02]	Methods for Detecting 5G Core Network IoT DDoS Attacks Using Optimal Extracted Features	Filter, Wrapper & embedded method	Accuracy 70% to 96%
2022/[03]	The MSR-DoS scheme is a modular way to protect 5G-enabled vehicle networks from DoS attacks. It is based on the square root.	Suggested method	Cost of simulation results
2022/[04]	5GUltra Dense Cellu lar Networks: G/M/1-Based Dos Protection	Off Loading Method	Experimental Result
2021/[05]	Slices ure: dos/ddos Effect and detection in 5G System slices	Suggested method	Accuracy 99.99%
2021/[06]	Utilizing ML to Protect 5G Software Defined Networks	Defense& clustering method	Accuracy 94%

III. TYPES OF DDOS ATTACKS VOLUMETRIC PROTOCOL

It UDP, ICMP, IP, TCP, and HTTP flood attacks, along with their modifications, are just a few of the DDoS attacks that fall under the three umbrellas indicated above. We cover the categories and attack types in depth below.

Volumetric Distributed Denial of Service Attacks: Volumetric DoS attacks work to exceed the capabilities of the targeted resource. Databases may be flooded with queries, networks can't handle the volume of traffic, and servers are overloaded with requests. DDoS assaults are often measured in bits per second, and their purpose is to overload the capacity of the targeted service on the internet.

A. Volumetric DDoS attacks include:- UDP Flood attacks If you want to have a conversation with a server, UDP is not the right technology for you because it does not allow for a two-way connection. While it was waiting for a response from the connected systems, UDP started sending out packets of data.

This feature allows for the optimal conditions for flood assaults, which aim to overwhelm a host by sending an excessive number of packets to its UDP ports. Attackers are aware that when a server receives an Arp request at any port, it must look for an application that corresponds to that port, and that certain protocols will start automated operations inside the server.

The IP address and port number in the datagrams allow intruders to zero in on a specific host on the internet or a local network. The attackers' goal is to flood the server with requests for that process or exhaust the available bandwidth on the network.

B. Protocol DDoS Attacks:- Instead of strictly using sheer volume, protocol DDoS attacks abuse protocols to overwhelm a specific resource, often a server, although firewalls and load balancers may also play a role. These kinds of assaults often have a rate expressed in packets per second.

IP Null attack :- All packets conforming to Internet Protocol version 4 contain headers that should specify if the transport protocol used for that packet is TCP, ICMP, etc. Attackers can get around this by setting the header to a null value, but if the server isn't told to ignore such packages, it will use up more resources trying to figure out how to send them anyway.

TCP Flood attacks:- The Transmission Control Protocol (TCP) relies on three separate data transfers to establish a connection:

SYN:- A packet with a time-stamped sequence number is sent from the requesting node (endpoint or server) to the intended receiver (endpoint).

SYN-ACK:- When the server receives a SYN packet, it sends back a response that includes both the synchronized sequence number and an acknowledgment number (ACK).

ACK:- The requesting device sends a response acknowledgement number (original ACK number + 1) back to the server.

Transmission is ended through a four-part termination sequence consisting of:

FIN:- The requesting device sends a session termination request (FIN) to the server.

Copyright © 2023. JCT Publications. All Rights Reserved

ACK:- The server responds with an ACK response to the requesting device, and the requesting device will wait to receive the FIN packet.
FIN:- The server responds with a FIN packet (may be nearly simultaneous) to the requesting device.

C. Application DDoS Attacks:- Application DDoS attacks target vulnerabilities in applications to cause the application itself to fail. Unlike other attacks that focus on disrupting infrastructure, this attack focuses on the Layer 7 software. However, it can also result in overloaded CPUs or exhausted memory, which affects the server and other applications. A second request is often used as a metric for defining the severity of a distributed denial-of-service attack. Adding an item to a shopping cart or completing a purchase are both computationally intensive operations that may be exploited by sending many requests simultaneously in order to overload the application or the host machine. Other attacks target specific vulnerabilities in software or use **SQL injections** to disrupt databases.

D. Application DDoS attacks with specific names include
HTTP Flood attacks:- HTTP Flood attacks abuse the HTTP commands to attempt to overwhelm websites, the servers that host them, and the bandwidth used to reach them. The bots used in these attacks can send multiple requests in sequence, so the large number of machines in the botnet exponentially increase traffic for the target website.
GET Attacks:- Using a botnet, attackers flood a service with requests for very large files (such as PDFs or films) using HTTP GET.
POST Attacks:- The Transmission Control Protocol (TCP) relies on three separate data transfers to establish a connection.

E. Low and slow POST attacks:- frequently used in conjunction with the R-U-Dead-Yet? (R.U.D.Y.)tool, attackers send HTTP Post requests that indicate they will send large amounts of data but then send tiny bits of data very slowly. As a result, the operation takes up server resources without detecting any DDoS defenses while searching for high-volume threats.

F. Single Session or Single Request Attack*:-* Since many modern anti-DDoS defences are designed to deny huge numbers of incoming packets, attackers are taking advantage of vulnerability in HTTP 1.1 to send multiple requests in a single packet.
G. Fragmented HTTP Flood**:-** Instead of sending large numbers of valid requests, bonnets establish valid HTTP connections and can split the HTTP packets into tiny fragments sent as slowly as the server will allow. This form of low-and-slow attack uses a packet rate that appears to be safe for many DDoS defenses, but the software or server keeps the session active and consumes resources with reserved bandwidth. The Slowworms tool enables this type of attack.

H. Recursive GET Flood:- Attackers attempt to overwhelm servers by requesting long lists of pages or images. The attack appears to be normal browsing behavior, but the botnet simply is chewing up resources that now cannot be used for legitimate traffic.
Random Recursive GET Flood: A variant of the Recursive GET Flood, this attack randomizes the requested pages to avoid detection.

IV. OTHER DDOS ATTACK TYPES

A. Advanced Persistent DoS (APDoS):- Hackers utilize a distributed denial-of-service (DDoS) attack when they aim to do significant harm. It uses a variety of the styles of attacks, such as HTTP flooding, and SYN flooding, and regularly targets multiple attack vectors that send out millions of requests per second. The ability of terrorists to customize methods at any time and create diversions to avoid security measures is a major reason why APDoS attacks can last for weeks. to

B. Multi-Vector Attacks:- DDoS may be caused by many simultaneous assaults launched by the attacker. For example, an adversary may launch a volumetric attack to divert defenses while another botnet launches a reduced HTTP Flood attack.

C. Zero-Day DDoS Attacks:- DDoS attacks may well be carried out by hackers who have found previously unknown flaws in software, networks, or devices. A "zero-day attack" is an attack that takes advantage of a vulnerability that has never been seen before.".

D. Stopping and Preventing DDoS Attacks**:-** DDoS assaults may come in many forms, and they can affect a broad range of services. Teams tasked with security and operations must collaborate to strike a balance between the resource's security and performance requirements. Redundancy will be critical for **defence and recovery from DDoS attacks,** but dedicated attackers have been known to attack multiple web servers simultaneously, so load balancers and redundancy will be insufficient. The defence against these attacks requires an overlapping and supporting combination of device hardening, redundancy, anti-DDoS tools, and anti-DDoS services – and perhaps the support of a DDoS prevention and response service.

V. CONCLUSION

Distributed denial of service (DDoS) attacks on 5G networks pose a serious threat to the availability of essential services. This highlights the need of investigating the effects of such assaults on 5G networks and taking precautions when appropriate.
One of the primary challenges with 5G networks is their high reliance on software-defined networking (SDN) and network function virtualization (NFV) technologies. These technologies make the network more agile and flexible but also increase its attack surface. These technologies are susceptible to Distributed Denial of Service attacks, which may take the network down. Several methods, like as

Copyright © 2023. JCT Publications. All Rights Reserved

traffic filtering, access control, and behavioural analysis, may be used to protect 5G networks against distributed denial of service attacks. It is also crucial to maintain up-to-date security patches monitor network traffic for anomalies, and implement effective response and recovery mechanisms.

REFERENCES

[1] Guşatu, Marian, and Ruxandra F. Olimid. "Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing." In International Conference on Information Technology and Communications Security, pp. 286-295. Springer, Cham, 2022.

[2] Kim, Ye-Eun, Yea-Sul Kim, and Hwankuk Kim. "Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network." Sensors 22, no. 10 (2022): 3819.

[3] Al-Shareeda, Mahmood A., and Selvakumar Manickam. "MSR-DoS: Modular Square Root- based Scheme to Resist Denial of Service (DoS) Attacks in 5G-enabled Vehicular Networks." IEEE Access (2022).

[4] Gao, Qinghang, Hao Wang, Liyong Wan, Jianmao Xiao, and Long Wang. "G/M/1-Based DDoS Attack Mitigation in 5G Ultradense Cellular Networks." Wireless Communications and Mobile Computing 2022 (2022).

[5] Khan, Md Sajid, Behnam Farzaneh, Nashid Shahriar, NiloySaha, and Raouf Boutaba. "SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices.(2021)".

[6] Alamri, Hassan A., VijeyThayananthan, and Javad Yazdani. "Machine Learning for Securing SDN based 5G network." Int. J. Comput. Appl 174, no. 14 (2021): 9-16.

[7] Kim, Youngsoo, Jong Geun Park, and Jong-Hoon Lee. "Security threats in 5G edge computing environments." In 2020 International Conference on Information and Communication Technology Convergence (ICTC), pp. 905-907. IEEE, 2020.

[8] Moudoud, Hajar, Lyes Khoukhi, and Soumaya Cherkaoui. "Prediction and detection of fdia and ddos attacks in 5g enabled iot." IEEE Network 35, no. 2 (2020): 194-201.

[9] Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani. "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy." In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-8. IEEE, 2019.

[10] Ni, Jianbing, Xiaodong Lin, and Xuemin Sherman Shen. "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT." IEEE Journal on Selected Areas in Communications 36, no. 3 (2018): 644-657.

[11] Li, Dong, Chang Yu, Qizhao Zhou, and Junqing Yu. "Using SVM to detect DDoS attack in SDN network." In IOP Conference Series: Materials Science and Engineering, vol. 466, no. 1, p. 012003. IOP Publishing, 2018.

[12] Larijani, Hadi, Jawad Ahmad, and Nhamoinesu Mtetwa. "A novel random neural network based approach for intrusion detection systems." In 2018 10th Computer Science and Electronic Engineering (CEEC), pp. 50-55. IEEE, 2018.

[13] Zhao, S., Li, W., Zia, T., & Zomaya, A. Y. (2017, November). A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (pp. 836-843). IEEE.

[14] Boro, Debojit, and Dhruba K. Bhattacharyya. "DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks." Microsystem Technologies 23 (2017): 593-611.

[15] Azhagiri, M. "Hidden Conditional Random Fields For Intrusion Detection System Using Layered Approach."

[16] Mangaleswaran, M. "Layered Approach for Intrusion Detection System Using Hidden Conditional Random Fields." (2017).

[17] Zantedeschi, Valentina, Maria-Irina Nicolae, and Ambrish Rawat. "Efficient defenses against adversarial attacks." In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, pp. 39-49. 2017.

[18] Boro, Debojit, Himant Basumatary, Tribeni Goswami, and Dhruba K. Bhattacharyya. "UDP flooding attack detection using information metric measure." In Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015 Volume 1, pp. 143-153. Springer Singapore, 2016.

[19] Timotheou, Stelios. "Fast Non-Negative Least-Squares Learning in the Random Neural Network." Probability in the Engineering and Informational Sciences 30, no. 3 (2016): 379-402.

[20] Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "Towards the science of security and privacy in machine learning." arXivpreprintarXiv:1611.03814 (2016).

Copyright © 2023. JCT Publications. All Rights Reserved