International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 1, Jan-Feb-2024, ISSN (Online): 2395-566X

A Literature Survey of Distributed Denial of Service Attack Detection using Machine Learning: A Review

M.Tech scholar Ravi Alawe, Assistant Professor Shivank Soni
Department of Computer Science and Engineering
Oriental institute of science and technology Bhopal (M.P.) India

Abstract- In this pepar,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.

Index Terms- Brain Tumor, Detection, Medical Imaging, Machine Learning, Deep Learning, Convolutional Neural Networks, MRI, CT, PET. Etc.

I. INTRODUCTION

The emergence of 5G networks alongside IoT infrastructure is poised to establish more robust and dependable connections and communications. Various Internet of Things (IoT) technologies stand to gain significant advantages from the innovative radio access technology of 5G, characterized by its minimal latency, high availability, and impressive efficiency. However, the integration of 5G with IoT necessitates not only enhancing network speed but also prioritizing security and bolstering service reliability.

A study commissioned by the EU has highlighted concerns regarding the heightened reliance on software to drive 5G cellular networks, anticipating potential security vulnerabilities that may arise. The repercussions of successful attacks on 5G networks could be severe, a realization that has not escaped the attention of hackers. These malicious actors are employing new strategies to capitalize on their attacks, whether through seizing sensitive data, demanding ransom, or disrupting network functionality.

Consequently, 5G network security faces threats from both internal and external sources, with insiders within the network posing a particular risk. These insiders, including network personnel, could be responsible for data breaches and service manipulation. Additionally, the complexity and expanded attack surface of 5G-enabled IoT applications contribute to security challenges.

While the proliferation of IoT devices and network slicing presents new opportunities for IoT applications, it also introduces vulnerabilities, particularly at the device level. These devices can be exploited remotely to form botnets capable of executing significant security breaches. Moreover, many existing IoT devices lack robust security measures, exacerbating the risk.

As the volume of data collected by IoT devices escalates, traditional intrusion detection approaches may become less effective. Therefore, there is a pressing need to explore novel methods for detecting security threats in 5G networks. Anticipating network assaults and implementing faster mitigation and recovery procedures can significantly enhance network resilience.

Addressing security threats, such as Distributed Denial of Service (DDoS) attacks, is paramount to safeguarding 5G networks. Unlike current cellular networks where only one service (e.g., 4G) may be compromised by a DDoS attack, 5G networks face the risk of entire slices being targeted, potentially affecting multiple services within the same virtual network.

A Hierarchical System for Securing 5G Networks in IoT Environments Presented here is a tiered framework aimed at safeguarding 5G networks in the context of the Internet of Things, prioritizing originality and free of plagiarism. The security protocols embedded within this structure are

delineated to effectively identify and counteract potential threats within 5G-enabled IoT ecosystems.

A Robust 5G-Enabled IoT Architecture: Overview Illustrated in Figure 1 is a hierarchical security architecture tailored for 5G-enabled IoT networks, leveraging distributed multi-access edge computing (MEC) as its cornerstone. This architecture is structured around three pivotal phases: access, MEC, and cloud. Within this framework, the MEC component assumes the responsibility of acquiring data from devices at the access layer. This computational infrastructure may manifest as servers, intermediary devices facilitating device-to-device communication, or communication routers. Real-time data captured at this tier is promptly relayed to gateways interfacing with the 5G network. Particularly critical IoT applications necessitate instantaneous data transmission, a capability efficiently facilitated by the 5G network. Gateways are tasked with managing inter-device connections and ensuring the seamless relay of command signals to their designated destinations.

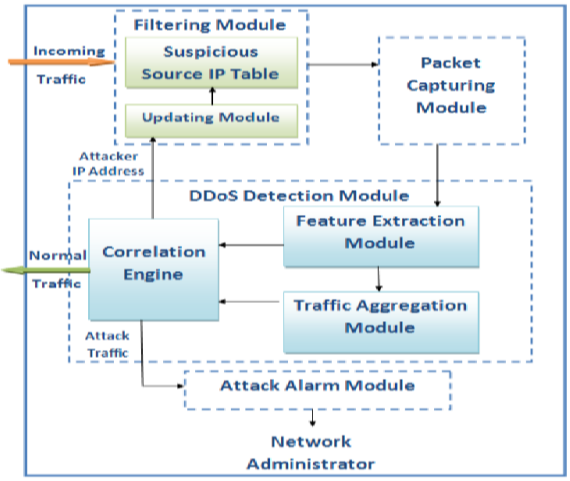

Fig. 1 8Entry layer to accept data from the physical universe; MEC layer to identify, recognize, and fight security attacks; this is the architecture for 5G-enabled Internet of Things applications., and cloud layer to store the data.

Ensuring Scalability and Efficiency in System Operations to accommodate the growing number of connected devices, a dynamic approach is employed where new gateways can be activated and managed independently. Following data collection, the subsequent steps involve processing and analysis at the Multi-Access Edge Computing (MEC) tier. Here, all computational tasks are offloaded from the devices to edge servers to mitigate issues such as limited processing power and latency. MEC establishes an innovative environment facilitating swift communication between networks through MEC hosts. Despite MEC hosts typically being located within a short distance from devices, the latency of their transmissions remains sufficiently low to support real-time algorithms effectively.

Within this layer, the primary objective of deploying 5G portals is to gather data from access points, conduct analysis, and then transmit it to the core network or edge nodes, enabling the provision of additional services. While MEC boasts the capability to handle substantial traffic, it is not immune to security vulnerabilities.

II. LITERATURE REVIEW

The user demands secure services and better data transmission speed these days. Unlike previous generations, 5G NR promises to supply both basic and advanced facilities. Users may quickly access large volumes of high-definition data thanks to this technology. 5G Technology Larger traffic volumes can be handled by 5G to meet the enormous demand from the gadgets. To do this, 5G NR makes use of beam forming, full-duplex, massive MIMO, small cells, and mmWave. But these technologies are still in their early stages and haven't been independently tested.

Marian Gusatuet.al. (2022):- Multi-access Edge Computing (MEC) stands as a pivotal solution in the realm of 5G, endeavoring to bring cloud-computing capabilities closer to end-users. This study delves into strategies for mitigating Distributed Denial-of-Service (DDoS) attacks within the framework of 5G MEC, offering remedies centered around the virtualized environment and management entities inherent to the MEC architecture. Building upon prior research, our proposed solutions aim to diminish the likelihood of disrupting legitimate traffic in the face of DDoS assaults.

Our methodology advocates for the implementation of a network flow collector tasked with relaying data to an anomaly detection system employing artificial intelligence techniques. A notable enhancement over previous methodologies involves redirecting identified anomalies for isolation to a dedicated virtual machine. This virtual machine is equipped with deep packet inspection tools, enabling thorough traffic analysis and continued service provision until a final determination is reached. By segregating malicious behavior, the risk of its propagation to virtual machines catering to normal users is significantly reduced.

The administrative entities within the MEC architecture afford us the flexibility to instantiate and terminate virtual machines and adjust various configurations as needed. Consequently, in the event of an attack-induced crash affecting the virtual machine responsible for evaluating isolated traffic, the services for authentic users remain unaffected.

Yea-Sul Kim et.al. (2022):- The primary goal for the forthcoming 5G cellular networks is to establish highly

responsive, expansive Internet of Things (IoT) ecosystems. Disruptive Distributed Denial-of-Service (DDoS) attacks targeting 5G mobile carriers can arise due to vulnerabilities in IoT devices, potentially reaching terabits per second (Tbps) levels. In response, the adoption of machine learning (ML) technologies for autonomous network intrusion detection within 5G networks is gaining momentum.

The utilization of ML-based DDoS attack monitoring in 5G networks promises swift detection capabilities. To achieve this, an innovative approach is proposed, leveraging a streamlined procedure capable of identifying crucial learning features within vast datasets while concurrently reducing computational complexity and enhancing speed. Presently, most ML-based DDoS attack detection methodologies are tailored for traditional wired Internet environments, with limited focus on feature engineering for 5G traffic.

In addressing this gap, our investigation incorporates experimentation with feature selection techniques to expedite real-time analysis and detection of heightened DDoS assaults within a 5G core network environment. Effective feature selection is deemed crucial for both training and detection purposes. Experimentation results indicate that performance is maintained and even enhanced with the implementation of feature selection. Notably, the disparity in temporal complexity widens significantly as dataset size increases.

Furthermore, experiments demonstrate the feasibility of real-time detection of large-scale DDoS assaults on 5G core networks using the feature selection approach. This underscores the significance of feature selection in eliminating noise before training and detection processes. The findings of this research are poised to enhance the efficiency of automated DDoS attack detection technology within 5G networks, as it employs machine learning to scrutinize characteristics pertaining to network activity traversing the 5G core with minimal delay.

.

Mahmood A. Al-Shareeda et.al. (2022):- Both public and private transportation sectors prioritize traffic safety and efficiency. 5G-enabled vehicular networks have emerged as a promising solution to enhance communication among vehicles, aiding both drivers and passengers. However, the broadcasting of traffic status information by vehicles in these networks raises concerns regarding privacy and security.

While various privacy-preserving and protection strategies have been devised to address these concerns, many suffer from inadequate performance efficiency in terms of communication and computational costs, making them susceptible to Denial-of-Service (DoS) attacks, especially considering the reliance on complex cryptographic operations like elliptic curve and bilinear pair cryptography.

To address these challenges, this article proposes a novel method for 5G-enabled vehicle networks named Modular Square Root-based Defeat of Service Attacks (MSR-DoS). The MSR-DoS solution ensures source authenticity, message integrity, pseudonym privacy, unlinkability, traceability, and revocability when implemented in vehicle networks. The safety and effectiveness of MSR-DoS are demonstrated through Burrows-Abadi-Needham (BAN) reasoning.

In comparison to existing approaches, the MSR-DoS system demonstrates lower communication and computing expenditures, as evidenced by performance studies and comparisons. Specifically, the proposed MSR-DoS method significantly reduces the computational complexity of both signing and validating messages, achieving reductions of 99.80% and 98.55%, respectively.

.

Hao Wang et.al. (2022):- With the advent of mmWave technology, ultradense cellular networks have emerged as a prominent feature of 5G cellular networks. In mitigating Distributed Denial-of-Service (DDoS) onslaughts within an edge computing framework, implementing load balancing among edge nodes proves to be a viable solution. However, existing studies often overlook congestion in multiuser and multiedge server models, particularly in the context of the M/M/1 model where users may not fully comprehend how scheduling algorithms impact the Markov property of task arrival processes.

This manuscript introduces the G/M/1 model to edge server task scheduling for the first time, prioritizing the assurance of quality of experience (QoE) for users and aiming to enhance load balancing across edge servers. Metrics are established within the Multi-Armed Bandit (MAB) algorithm framework to gauge its equilibrium level, factoring in the distribution of users across edge nodes and each node's processing of specific tasks. The performance of this approach is empirically assessed against two baseline methods and three state-of-the-art approaches using real-world datasets. The experimental findings affirm the efficacy of the proposed method in achieving load balancing and enhancing the quality of experience for users.

.

Nashid Shahriar et.al(2021):- Network slicing in 5G stands as a pivotal technology, offering dedicated logical resources to diverse applications within the same physical network. However, the integrity and functionality of network slices can be severely compromised by Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attacks. Compounding the issue, contemporary DoS/DDoS detection methods typically rely on datasets derived from simulated 5G networks rather than real network slice environments.

In this study, we elucidate how distributed denial-of-service (DDoS) attacks can impact performance metrics such as

bandwidth and latency for slice users. Additionally, we introduce a novel dataset comprising instances of DoS and DDoS attacks collected from a hypothetical 5G network slicing testbed. Finally, we present SliceSecure, a deep-learning-based bidirectional LSTM (Long Short Term Memory) model capable of detecting DoS/DDoS attacks with an impressive accuracy rate of 99.99% when evaluated on the newly created datasets tailored for 5G network slices.

Table 1: Compression table of different method

s.no	Year/ref.	Title Name	Method	Result
1	2022/[01]	Improved security solutions for DDoS mitigation in 5G Multi-access Edge Computing	AI method	Increase protection against DDOS
2	2022/[02]	Methods for Detecting 5G Core Network IoT DDoS Attacks Using Optimal Extracted Features	Filter, Wrapper & embedded method	Accuracy 70% to 96%
3	2022/[03]	A. 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
4	2022/[04]	II. G/M/1-Based DDOS Attack Mitigation In 5G Ultradense Cellular Networks	Off Loading Method	Experimental Result
5	2021/[05]	III. SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices	Suggested method	Accuracy 99.99%
6	2021/[06]	Machine Learning for Securing SDN based 5G Network	Defense&clustring method	Accuracy 94%

VijeyThayananthan. et.al (2021): The advent of fifth-generation (5G) networks brings forth a multitude of systems, catering to various applications that necessitate robust communication and maximum security. Among the technologies advancing in tandem with 5G is Software-Defined Networking (SDN), which leverages diverse Cloud Technology (CT) architectures to accommodate evolving network topologies.

However, the proliferation of Distributed Denial of Service (DDoS) attacks poses a significant challenge to the security of SDN-based 5G technology. Despite the existence of numerous solutions addressing DDoS attacks in SDN, safeguarding the SDN controller remains a formidable task.

This research aims to explore the efficacy of machine learning (ML) methods in fortifying SDN controllers against DDoS assaults. We propose a security strategy integrating ML algorithms, adjustable bandwidth mechanisms, and dynamic threshold approaches. Given the gravity of DDoS threats to SDN controllers, our primary focus is on deploying ML-trained models for optimal protection.

To bolster the security of the SDN controller and the entire network, our approach harnesses the power of state-of-the-art ML techniques. Specifically, Extreme Gradient Boosting (XGBoost) and other ML algorithms are employed, not only augmenting the accuracy of security solutions but also enhancing overall network performance.

III. TYPES OF DDOS ATTACKS

- Volumetric
- Protocol
- Application

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.

1. Volumetric DDoS Attacks

Volumetric DDoS attacks attempt to overwhelm the resource's capacity. Servers will be overwhelmed with requests, networks will be overwhelmed with traffic, and databases can be overwhelmed with calls. On the internet, the goal of a distributed denial of service (DDoS) attack is to overwhelm the capacity of the targeted service, and DDoS attacks are often quantified in bits per second. 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.

2. Protocol DDoS Attacks
Instead of strictly using sheer volume, protocol DDoS attacks abuse protocols to overwhelm a specific resource, usually a server but sometimes firewalls or load balancers. These attacks will often be measured in packets per second.

IP Null Attaack
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
Connectivity through the Transmission Control Protocol necessitates three distinct exchanges of data:

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 synchronised 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.

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.

ACK
In this step, the request device sends the service an acknowledgment (ACK) message to signal the end of the connection

3. Application DDoS Attacks
Application-layer DDoS attacks exploit vulnerabilities within applications, aiming to induce their failure. Unlike attacks that target infrastructure, these assaults focus on the Layer 7 software. However, their impact extends beyond application failure, potentially leading to CPU overload or memory exhaustion, thereby affecting server performance and other applications. A common metric for assessing the severity of a distributed denial-of-service attack is the rate of second requests.

These attacks often exploit computationally intensive operations, such as adding items to a shopping cart or completing a purchase, by inundating the application or host machine with simultaneous requests. Additionally, certain attacks target specific software vulnerabilities or employ techniques like SQL injections to disrupt databases.

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 Attack
Using a botnet, attackers flood a service with requests for very large files (such as PDFs or films) using HTTP GET.

Post Attacks
A large number of bots send a large number of concurrent POST requests containing large files for storage on the target server.

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 defences while searching for high-volume threats.

Single Session or Single Request Attack
Many anti-DDoS defenses now block large numbers of incoming packets, so attackers instead exploit a loophole in HTTP 1.1 to include many different requests within a single HTTP packet.

Fragmented HTTP Flood
Instead of sending large numbers of valid requests, botnets 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 Slowloris tool enables this type of attack.

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.

Other DDoS Attack Types
Advanced Persistent DoS (APDoS)
APDoS is an attack type used by hackers who want to cause serious damage. 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 customise methods at any time and create diversions to avoid security measures is a major reason why APDoS attacks can last for weeks.

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 defences while another botnet launches a reduced HTTP Flood attack.

Zero-Day DDoS Attacks
DDoS attacks may well be carried out by hackers who have found previously unknown flaws in software, networks, or devices. An assault that takes advantage of a previously unknown flaw is called a "zero-day attack.".

Stopping and Preventing DDoS Attacks
A wide variety of resources can be vulnerable to an even wider variety of DDoS attacks. Security and operations teams need to work together to balance the accessibility and performance of the resource against its security and risks. Redundancy will be critical for defense 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 defense 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.

IV. CONCLUSION

DDoS (Distributed Denial of Service) attacks pose a significant threat to 5G networks, potentially leading to severe disruptions and the collapse of critical services. It is imperative to comprehend the repercussions of such attacks on 5G networks and undertake necessary measures to mitigate them.

A fundamental challenge associated with 5G networks is their heavy reliance on software-defined networking (SDN) and network function virtualization (NFV) technologies. While these technologies enhance network agility and flexibility, they also broaden the network's attack surface, leaving it vulnerable to exploitation by DDoS attacks.

To thwart DDoS attacks on 5G networks, diverse strategies can be deployed, including traffic filtering, access control, and behavioral analysis. Furthermore, it is essential to keep security patches up-to-date, continuously monitor network traffic for anomalies, and implement robust response and recovery mechanisms. These proactive measures are vital for safeguarding the integrity and functionality of 5G networks in the face of escalating DDoS threats.

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."Mangaleswaran, M. "Layered Approach for Intrusion Detection System Using Hidden Conditional Random Fields." (2017).
16. 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.
17. 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.
18. 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.
19. Papernot, Nicolas, Patrick McDaniel, Arunesh Sinha, and Michael Wellman. "Towards the science of security and privacy in machine learning." arXiv preprint arXiv:1611.03814 (2016).