Enhanced alert generation system with Attacker IP for DOS Attacks

R. Tamilkodi
Professor
Dept. Of CSE(AIML&CS)
Godavari Global University, Rajahmundry, A.P
tamil@giet.ac.in

P. Saroja Rani
Asst Professor
Dept. Of CSE(AIML&CS)
Godavari Institute of Engineering & Technology, Rajahmundry, A.P
saroja@giet.ac.in

L. Ganga Deepthi
UG Student
Dept. of CSE (Cyber Security)
Godavari Institute of Engineering & Technology, Rajahmundry, A.P
deepthilalam13@gmail.com

M. Puri Jagannadh
UG Student
Dept. Of CSE (Cyber Security)
Godavari Institute of Engineering & Technology, Rajahmundry, A.P
purijagannadhmuralasetti13@gmail.com

K. V. Pavan Kumar
UG Student
Dept. Of CSE (Cyber Security)
Godavari Institute of Engineering & Technology, Rajahmundry, A.P
pavankumarkarre143@gmail.com

T. Ravi Teja
UG Student
Dept. Of CSE (Cyber Security)
Godavari Institute of Engineering & Technology, Rajahmundry, A.P
ravitejaravi48903@gmail.com

***Abstract*- The denial of service (DoS) attack carries a significant risk to network security as they can cause major disruptions and financial losses by flooding a network with excessive data. Different approaches can be utilized to carry out these attacks from basic flooding to more complex, distributed methods, and they can target multiple network layers, taking advantage of vulnerabilities to maximize damage. Complex attacks may be difficult for standard detection techniques, which depend on fixed limits, to identify since attackers frequently alter how they overcome fixed defences. Additionally, these techniques may produce false positives, which would result in useless alerts and resource usage. To overcome these obstacles, we have created an improved DoS detection system that uses Pyshark for in-depth packet analysis to keep track of network traffic in real-time. To provide essential data for an immediate reaction, the system observes the attacker's IP address and dynamically modifies its thresholds in response to traffic patterns. Real-time notifications via email containing the attacker's IP address and packet count are provided in the context of a threat detection, allowing for immediate reaction. This method strengthens network security by providing a more effective and rapid protection responses to attacks known as denial-of-service (DoS).**

***Keywords* -DoS attacks, network security, real-time monitoring, packet analysis, Pyshark, attacker IP tracking, network traffic analysis.**

I.INTRODUCTION

In modern times, network security is a top priority for users as well as companies. As our dependency on the internet increases, also rises our risk of different cyberthreats Denial of Service (DoS) assaults are particularly dangerous because they can disrupt critical services, encounter serious financial losses, and cause long-term reputational damage [14,19]. A DoS attack typically operates by overloading a network with an excessive amount of traffic, making it unable to respond to true requests[18] Traditional DoS detection systems, which rely on predefined thresholds and static rules, are excellent at detecting basic attacks but struggle with more complex ones.[10] Attackers are increasingly capable of modifying the strength and pattern of their traffic, making it difficult for traditional systems to detect and respond to these dynamic threats [20]. This drawback shows the need for a more adaptive and intelligent approach to DoS detection.[16] To solve these issues, an improved DoS detection system has been developed that includes dynamic threshold adjustments and real-time network traffic monitoring [12]. This system utilizes Pyshark for accurate packet analysis, allowing possible threats to be detacted accurately.

The system can adapt to changing conditions and detect possible attacks more effectively if it continuously tracks network traffic [21,24]. Along with detecting threats, the system is designed to monitor possible attackers' IP addresses. Whenever it detects a potential DoS attack, it immediately sends alerts via email with important details such as the attacker's IP address and the quantity of packets involved [28]. This real-time connection allows network administrators to respond quickly, minimizing the impact of the attack and ensuring a fast and efficient Défense against the increasing risk of DoS attacks.

II. LITERATURE SURVEY

Denial of Service (DoS) attacks utilize various methods to overwhelm a system or network, causing service disruptions. Several detection techniques have been developed to mitigate these attacks. Packet analysis and anomaly detection are among the most researched approaches, focusing on identifying unusual traffic patterns that signal a potential DoS attack [26]. Below, we summarize different types of DoS attacks, and the detection methods explored in the existing literature.

I. Types of Detection Techniques

KNN-Based DoS Detection: The application of KNN algorithms for detecting DoS attacks over IPv6 networks is examined, showing that classification models can effectively identify attack patterns and protect modern network architectures [1].

SDN DoS Detection: The separation of the control and data planes in software-defined networks (SDN) allows for enhanced traffic management, which is critical for Real-time detection and mitigation of DoS attacks [2, 3].

LAN-Based DDoS Detection: Approaches for spotting and preventing DDoS assaults on local area networks (LAN) are explored, focusing on real-time analysis and rapid response mechanisms to minimize disruption [4].

DoS in Control Systems: Various attack models in control systems are analyzed, offering insight into how DoS attacks compromise system stability and outlining security measures to counteract these threats [5,7].
DoS Detection in IoT Systems: Machine learning in IoT systems for DoS detection is explored, where algorithms analyze traffic to detect patterns associated with attacks and mitigate threats effectively [6, 8].
Application Layer DoS Attacks: Various attack strategies at the application layer are reviewed, along with defense mechanisms that can be implemented to safeguard against service interruptions [9].
DoS Attack in Smart Grids: Research explains the difficulties in identifying and preventing DoS attacks.in smart grids, emphasizing the importance of maintaining communication integrity in critical infrastructure [13, 27, 30].
Cyber-Physical DoS Attack Prevention: Distributed state estimation techniques and active security controls are discussed as methods for countering DoS attacks in cyber-physical systems, ensuring reliable operation [11, 15].

III.EXISTING SYSTEMS

Current systems for Denial of Service (DoS) attack detection and mitigation methods commonly employ signature-based, anomaly-based, and machine learning-driven detection techniques. Signature-based systems focus on recognizing well-known attack patterns, but they frequently have trouble spotting more recent or advanced DoS threats. that may employ unconventional strategies to evade detection.

Anomaly-based detection methods monitor network traffic to identify deviations from normal behaviour. While these systems can adapt to novel attack patterns, they frequently face challenges with high false positive rates, resulting in legitimate traffic being misclassified as malicious. This misclassification can lead to operational disruptions and hinder network performance.

Machine learning-based detection systems have emerged as a more advanced solution, capable of analyzing and classifying traffic patterns in real time. However, these systems typically require significant processing power and large training datasets, which makes them less practical for real-time applications across all contexts.

Despite their strengths, existing systems often lack comprehensive alerting mechanisms and the capability to trace the real-time IP address of the attacker. As a result, notifications could not reach network administrators in a timely manner. about ongoing attacks, which can impede effective response and remediation efforts.

Moreover, current systems face scalability issues as online activity volumes increase, leading to slower detection times and a higher likelihood of missed threats. They also struggle with processing complex data relationships or non-linear patterns, which limits their effectiveness against sophisticated DoS attacks. Existing methods often achieve accuracy percentages ranging from 85% to 92%. However, they frequently encounter high false positive rates and prolonged update cycles, which reduce their overall effectiveness against evolving DoS tactics. The inability to provide timely alerts further hampers network administrators' capacity to respond to emerging threats in a proactive manner.

IV.PROPOSED METHODOLOGY

The proposed strategy introduces a comprehensive framework aimed at enhancing the identification and prevention of Denial of Service (DoS) attacks. by leveraging Python and Pyshark. While existing literature has developed various approaches for handling DoS attacks in complex network environments like IPv6 and Software-Defined Networks (SDN), our approach builds upon these by providing a distributed and reliable detection system that specifically addresses key limitations in traditional methods. By integrating Python's flexibility with Pyshark packet analysis capabilities, Real-time observation is made possible by the system's design of network traffic, facilitating immediate alerts upon detecting suspicious activity. Furthermore, the dynamic tracking of intruder IP addresses offers significant advancement over previous approaches that relied on static entries or manual configurations.

The methodology begins with a deep understanding of DoS attacks, examining various attack vectors, traffic patterns, and their overall significance on network security. This theoretical foundation informs the system's design, ensuring a targeted and precise detection capability.

Pyshark is utilized in conjunction with Python to develop a robust packet capture and analysis system. The system is programmed to filter network packets and flag anomalous traffic patterns that align with typical DoS attack behaviours. This Python-based solution offers adaptability and scalabilities. Facilitating through packet inspection and processing of substantial network traffic

The project setup involves providing a secure virtual framework to defend the host machine during testing. Virtualization technologies such as VMware are used to establish three virtual machines (VMs) that mimic a real-world network setup. These VMs include a Windows machine as the target, a Kali Linux machine simulating the attacker, and an Ubuntu machine serving as the network monitoring system. This virtualized lab allows for thorough and safe experimentation without risking actual network infrastructure.

4.1 Code Execution: The process involves executing the developed Python script within a controlled virtual environment, allowing for ongoing, real-time network traffic monitoring. This script captures additionally analyses the network data, extracting the necessary parameters for efficient identification of DoS (denial of service) assaults.

4.*2.* Detecting DoS Attack: The detection of DOS attack is a critical component of the system. With the use of a Python script's real-time packet analysis features, network traffic is carefully inspected for indications of possible DoS activity. The system identifies suspicious patterns, such as sudden

spikes in packet volume or repeated requests from a single IP address, triggering an alert to notify of the potential threat.

4.3 Tracing the attacker's IP address: In this stage, the alarm message is generated, and the attacker's IP address is recorded. The Python script developed during the earlier phase tracks the source of the Denial of Service (DoS) assault to determine the attacker's IP address, providing critical information for further analysis and response**.**

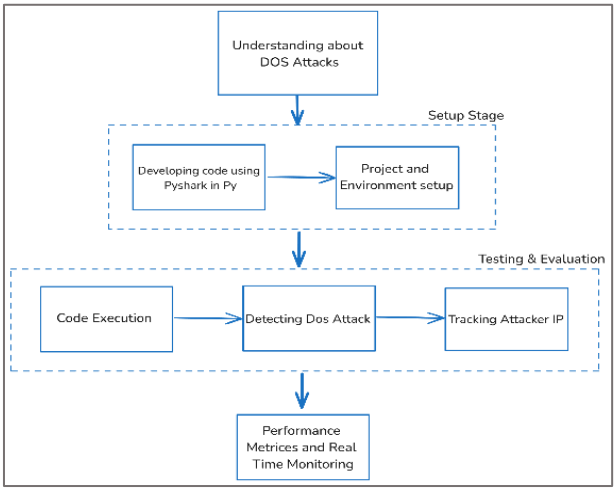

Fig 1. The Proposed system for Dos attack alert generation system

Fig.1 The diagram demonstrates the structure of the proposed system, focusing on how it detects and generates alerts for DoS attacks. detection using Pyshark in Python. It begins with understanding DoS attacks, followed by the setup stage, which involves developing the code and configuring the project environment. The next phase is testing and evaluation, including code execution, detecting DoS attacks, and tracking the attacker's IP. Finally, the process concludes with real-time monitoring to assess the system's capability.

V. EXPERIMENTAL RESULTS

The Experimental setup comprises three virtual machines: Kali Linux that imitate attacks, Windows to act as the victim, and Ubuntu to monitor the network. Ubuntu powers the detection system, and in this virtual lab, controlled studies assess how well the system recognizes and handles denial-of-service (DoS) threats. This setup provides a controlled platform to assess the robustness of the proposed solution.

TESTING: Validating is a crucial phase, particularly when integrating security features like DOS attack Identification technique. here is an organized approach for conducting thorough testing

Step 1: Launch VMware and begin the Ubuntu boot process.
Step 2: Create the Python script and store it to the Ubuntu network monitoring system.
Step 3: Use the command to monitor network traffic by running the script with root capabilities.
Step 4: Launch a terminal with enhanced sudo privileges on Kali Linux, the attacker's computer.
Step 5: Use hping3 or similar tool built for DoS attacks to start a DoS attack against the Windows target.
. as shown in Fig 2.

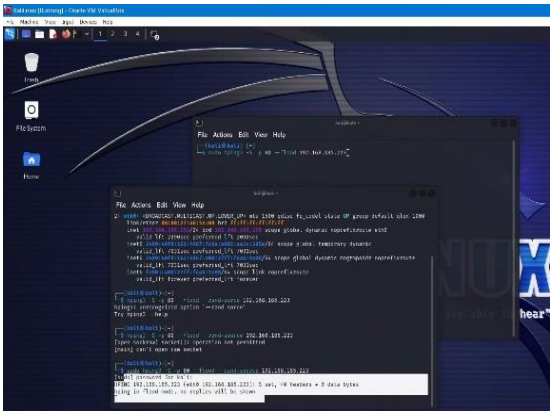

Fig 2: Using hping3 on Kali Linux

-In this research, we used hping3 to generate the DoS attack test traffic

Step 6: Send a flood of packets to the victim machine (Windows) using hping3, targeting a specific port (e.g., port 80) to simulate the DoS attack.as shown in Fig 3.

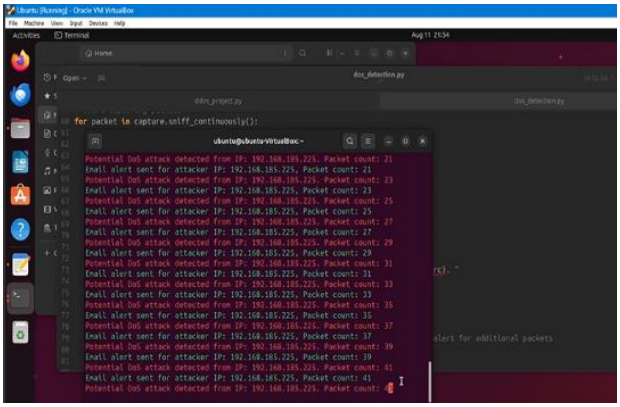

Fig.3: Identifying the Intruder IP in the Ubuntu terminal

Step 7: We continuously monitor Denial of Service (DoS) detection alerts within the Ubuntu terminal, which facilitates the determination of the IP address of the attacker. The output results not only reveal the attacker's IP but also confirm the detection of a potential DoS attack by the mechanism as depicted in Fig.4

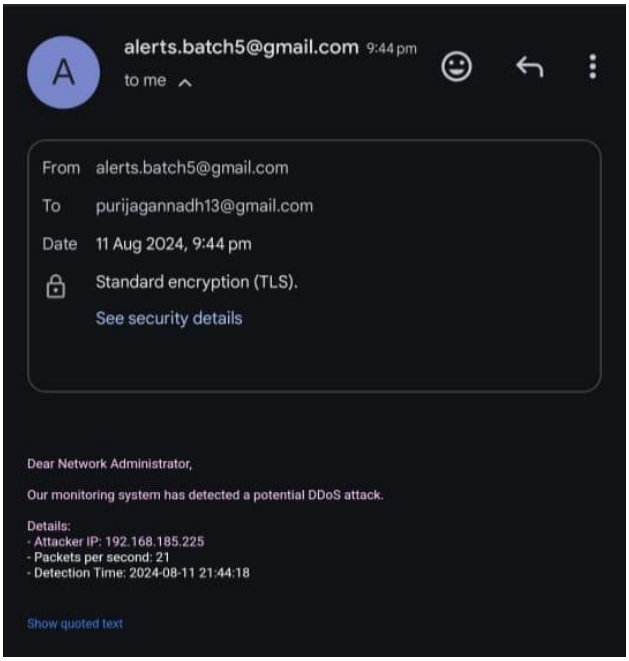

Fig.4 Monitoring system has detected a potential DOS attack # attacker IP address

6. METRICS OF EVALUATION &PERFORMANCE

Assessing this study's efficacy and efficiency is essential to determining its dependability in practical applications. The ratio of successfully discovered DoS incidents to the total number of attack attempts is defined as detection reliability, serving as a measure of the system's capability to accurately identify such threats.

Additionally, detection time refers to the duration it takes for the system to recognize a DoS attack as a threat after its initiation; shorter detection times indicate enhanced response capabilities. The system is also designed to generate real-time alerts, enabling immediate action to be taken in response to detected threats. Furthermore, the system's impact on network resources, including CPU and memory utilization, is evaluated to ensure that it operates smoothly without overloading the network.

Table1: Comparative Analysis Between Existing Systems and Proposed System

FEATURE	EXISTING SYSTEM	PROPOSED SYSTEM
Accuracy	93%	95%
True Positive	78	88
False Positive Rate	10%	2%
False Negative Rate	5%	1%
Cost(USD/month)	100	100
CPU	20%	15%

Table2: The proposed system offers significant improvements over the existing system with a higher accuracy rate of 95% compared to 93%. It reduces the False Positive Rate from 10% to 2% and False Negative Rate from 5% to 1%, ensuring more reliable detection

Table 2: proposed analysis of the Attacker IP Capturing

Metrices	Calculations
True Positives	38
True Negatives	0
False Positives	1
False Negatives	1
Detection Accuracy (TP+TN/TI)x100	94%
Detection Response	Instantly
Attacker IP Capturing Rate (Total Captured/TI)	96%
CPU Utilization	12%
Memory Utilization	28.10%

The Table 2 presents key performance metrics for the DoS attack detection system. With a detection accuracy of 94%, the system promptly responds to attacks while capturing attacker IPs at a 96% rate

CONCLUSION

The Evolution and implementation of the Enhanced DoS Detection with Attacker IP Tracking system yielded positive results in improving network security. Through exhaustive testing and evaluation, the system exhibited reliable detection of DoS attacks by accurately recognizing and tracking abnormal traffic patterns. The functionality to obtain the attacker's IP address, along with provision of real-time alerts, supplies network administrators with crucial information and facilitates rapid responses to emerging threats Moreover, guaranteeing that network performance was unaffected the Enhanced DoS Detection with Attacker IP Tracking system has the potential to evolve into an even more effective and adaptive solution for safeguarding network security and integrity against the increasing landscape of cyber threats.

REFERENCES

[1] Alharbi, Yasser, Ali Alferaidi, Kusum Yadav, Gaurav Dhiman, and Sandeep Kautish. "Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm." *Wireless Communications and Mobile Computing* 2021, no. 1 (2021): 8000869.

[2] Gao, Shang, Zhe Peng, Bin Xiao, Aiqun Hu, Yubo Song, and Kui Ren. "Detection and mitigation of DoS attacks in software defined networks." *IEEE/ACM Transactions on Networking* 28, no. 3 (2020): 1419-1433.

[3] Dobrin, Dobrev, and Avresky Dimiter. "DDoS attack identification based on SDN." In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, pp. 1-8. IEEE, 2021.

[4] Sinha, Somnath, and N. Mahadev Prasad. "Distributed Denial of Service Attack Detection and Prevention in Local Area Network." In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021*, pp. 415-428. Singapore: Springer Nature Singapore, 2022.

[5] Cetinkaya, Ahmet, Hideaki Ishii, and Tomohisa Hayakawa. "An overview on denial-of-service attacks in control systems: Attack models and security analyses." *Entropy* 21, no. 2 (2019): 210.

[6] Syed, Naeem Firdous, Zubair Baig, Ahmed Ibrahim, and Craig Valli. "Denial of service attack detection through machine learning for the IoT." *Journal of Information and Telecommunication* 4, no. 4 (2020): 482-503.

[7] Mihoub, Alaeddine, Ouissem Ben Fredj, Omar Cheikhrouhou, Abdelouahid Derhab, and Moez Krichen. "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques." *Computers & Electrical Engineering* 98 (2022): 107716.

[8] Zhijun, Wu, Li Wenjing, Liu Liang, and Yue Meng. "Low-rate DoS attacks, detection, defense, and challenges: A survey." *IEEE access* 8 (2020): 43920-43943.

[9] Tripathi, Nikhil, and Neminath Hubballi. "Application layer denial-of-service attacks and defense mechanisms: a survey." *ACM Computing Surveys (CSUR)* 54, no. 4 (2021): 1-33.

[10] Sudar, K. Muthamil, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnasamy. "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques." In *2021 international conference on Computer Communication and Informatics (ICCCI)*, pp. 1-5. IEEE, 2021.

[11] Liu, Yan, and Guang-Hong Yang. "Event-triggered distributed state estimation for cyber-physical systems under DoS attacks." *IEEE transactions on cybernetics* 52, no. 5 (2020): 3620-3631.

[12] Bahashwan, Abdullah Ahmed, Mohammed Anbar, and Sabri M. Hanshi. "Overview of IPv6 based DDoS and DoS attacks detection mechanisms." In *Advances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1*, pp. 153-167. Springer Singapore, 2020.

[13] Huseinović, Alvin, Saša Mrdović, Kemal Bicakci, and Suleyman Uludag. "A survey of denial-of-service attacks and solutions in the smart grid." IEEE Access 8 (2020): 177447-177470.

[14] 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.

[15] Li, Tongxiang, Bo Chen, Li Yu, and Wen-An Zhang. "Active security control approach against DoS attacks in cyber-physical systems." IEEE Transactions on Automatic Control 66, no. 9 (2020): 4303-4310.

[16] Iqbal, Ahmed, Shabib Aftab, Israr Ullah, Muhammad Anwaar Saeed, and Arif Husen. "A classification framework to detect DoS attacks." International Journal of Computer Network and Information Security 11, no. 9 (2019): 40-47.

[17] Abughazaleh, Nada, R. Bin, and Mai Btish. "DoS attacks in IoT systems and proposed solutions." Int. J. Comput. Appl 176, no. 33 (2020): 16-19.

[18] Rios, Vinícius De Miranda, Pedro RM Inácio, Damien Magoni, and Mário M. Freire. "Detection and mitigation of low-rate denial-of-service attacks: A survey." IEEE Access 10 (2022): 76648-76668.

[19] Eliyan, Lubna Fayez, and Roberto Di Pietro. "DeMi: A Solution to Detect and Mitigate DoS Attacks in SDN." IEEE Access (2023).

[20] Tian, Jiwei, Buhong Wang, Tengyao Li, Fute Shang, and Kunrui Cao. "Coordinated cyber-physical attacks considering DoS attacks in power systems." International Journal of Robust and Nonlinear Control 30, no. 11 (2020): 4345-4358.

[21] Binu, P. K., Deepak Mohan, and EM Sreerag Haridas. "An sdn-based prototype for dynamic detection and mitigation of dos attacks in iot." In *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 5-10. IEEE, 2021.

[22] Ahuja, Nisha, Gaurav Singal, Debajyoti Mukhopadhyay, and Neeraj Kumar. "Automated DDOS attack detection in software defined networking." *Journal of Network and Computer Applications* 187 (2021): 103108.

[23] Hadi, Raghad Mohammed, Salma Hameedi Abdullah, and Wafaa M. Salih Abedi. "Proposed neural intrusion detection system to detect denial of service attacks in MANETs." *Periodicals of Engineering and Natural Sciences* 10, no. 3 (2022): 70-78.

[24] Li, Tongxin, Yong Wang, Cunming Zou, Yingjie Tian, Lin Zhou, and Yiwen Zhu. "Research on dos attack detection method of modbus tcp in openplc." *Journal of Computer and Communications* 9, no. 07 (2021): 73-90.

[25] Rachmadi, Salman, Satria Mandala, and Dita Oktaria. "Detection of DoS attack using AdaBoost algorithm on IoT system." In *2021 International Conference on Data Science and Its Applications (ICoDSA)*, pp. 28-33. IEEE, 2021

[26] Sambangi, Swathi, and Lakshmeeswari Gondi. "A machine learning approach for dos (distributed denial of service) attack detection using multiple linear regression." In *Proceedings*, vol. 63, no. 1, p. 51. MDPI, 2020.

[27] Zhe, Wang, Cheng Wei, and Li Chunlin. "DoS attack detection model of smart grid based on machine learning method." In *2020 IEEE international conference on power, intelligent computing and systems (ICPICS)*, pp. 735-738. IEEE, 2020.

[28] Salmi, Salim, and Lahcen Oughdir. "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network." *Journal of Big Data* 10, no. 1 (2023): 17.

[29] Wang, Yaqi, Jianquan Lu, and Jinling Liang. "Security control of multiagent systems under denial- of-service attacks." *IEEE Transactions on Cybernetics* 52, no. 6 (2020): 4323-4333.

[30] Zhe, Wang, Cheng Wei, and Li Chunlin. "DoS attack detection model of smart grid based on machine learning method." In *2020 IEEE international conference on power, intelligent computing and systems (ICPICS)*, pp. 735-738. IEEE, 2020.