ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2018.0246

# AN INVESTIGATION OF SECURITY TECHNIQUES FOR CONCEALED DDOS EXPOSURE ATTACKS

**K. Praghash[1], M. Masthan[2] and R. Ravi[3]**

*[1]Department of Information and Communication Engineering, Anna University, Chennai, India*
*[2]Department of Computer Science and Engineering, Manonmaniam Sundaranar University, India*
*[3]Department of Computer Science and Engineering, Francis Xavier Engineering College, India*

*Abstract*

***Due to the influence of the multi-level system, the DDoS became a significant investigation in modern days. This encourages us to reduce the data loss and service overheads. In order to investigate these issues, an investigation of the DDoS attack and their related security techniques were analyzed in this paper. So, in this investigation, various data about the intruders will be collected by employing a secured multi-layered design with nomadic honeypots. Our proposed Subterranean Optimization procedure is utilized to distinguish the gatecrashers in view of the pheromone store on that considered zone. A multi-degree IP log table is utilized to distinguish the gatecrashers at diverse ranges of the device. Once the prompted range is found, the information is sent to multi-degree engineering to restrain the spreading of the stimulated region within the honeypot. This statistics will be dispatched to the honeypot to make a guard framework towards the attackers. The advantage of this proposed strategy is that it gives a complete barrier against DDoS at multilevel without making any overhead.***

*Keywords:*

***DDoS attack, Subterranean Optimization procedure, Service Denial Attacks***

## 1. INTRODUCTION

### 1.1 SERVICE DENIAL ATTACKS

Distributed Denial of service (DDoS) attack is one of the essential security attacks due to its explicit threatening of the balance of the net [1] [4]. DDoS attack is a Denial of carrier (DoS) attacks relying on a distributed, collaborative massive-scale denial of service attacks. DoS attacks might be of one-to-one attack [6]-[9] and have an impact on most effective for the decrease the target computer's configuration or smaller the network bandwidth and will no longer be effective with rapid growth in network technology. DDoS attack replaced the conventional one-way attack with the assist of the community so that a large number of puppet machines are mobilized concurrently to the destination host to attack, attack effect is extremely apparent. Not like DoS, DDoS exploits the massive useful resource asymmetry between the internet and the victim. By means of its many-to-one attack measurement [10] [13], DDoS can block sufferer off-net thereby its protection level come to be inappropriate.

DDoS attack is launched by way of flooding a large number of packets to overwhelm the sufferer with the aid of multiple compromised hosts (attackers) dispersing within the community concurrently. The attack flows with the aid of substantially ingesting target system's bandwidth [11] [12] or key sources preventing provider provision to legitimate users resulting in unauthorized service deny from customers posing a chief safety chance within the network. These days, [14] [16] [19] Botnet is used as an attacking platform to form a large scale of flooding DDoS attacks, attack flows come to be greater disbursed or even greater danger, making it increasingly difficult to be detected correctly [2] [18] [19].

### 1.2 DOCUMENTATION OF SERVICE DENIAL ATTACKS

DDoS attack methods of inherited attack and IP spoofing hardens tracing of attackers to be tough [13]-[15]. DoS mitigation is hard in a disbursed environment, as it is able to be of any shape both ping of death or clone attack. DDoS detection set of rules considered that the detection infrastructure is placed close to saturated hyperlink in the area of the victim, where the detection is easy. Even though it simplifies the detection set of rules, local reaction is useless on the grounds that to be had bandwidth has already been fed on in upstream direction [17].

Detecting DDoS attack at an earlier stage may be very difficult. DDoS attacks are identified if a server or network already down or exhaustion for some time. It is tough to distinguish valid packets on normal visitors and packets dispatched via zombie computers, hence there's a lag in DDoS attack detection. Then again, as a huge number of packets are transmitted, greater time is required to analyze each incoming packet thereby DDoS detection accuracy decreases [18].

Although many efforts have done in attack detection and prevention [3], there may be an adequacy of powerful and green solutions to intercept ongoing attack in a timely fashion, i.e. short sufficient to save your visitors build up from DDOS attack [5].

## 2. PROPOSED SOLUTION

### 2.1 OUTLINE AND STATEMENT OF PROBLEM

In this article, we have suggested an enhanced DDoS detection method, because the net is threatened by using protection attacks like DDoS, it provides an energy to provide a security system for safe conversation. Intrusion detection employs the use of honeypot to fool the intruders and preserve them a long way far from demanding the reliability of a conversation community. An efficient hop with the aid of hop honeypot mechanism is proposed to mitigate spoofing dispensed Denial-of-service attacks. Here, again propagation is finished to hint lower back the root of attacks. In addition, roaming honeypots scheme offer accurate attack signatures. The roaming honeypot on receiving attack packets triggers the activation of a tree of honeypot classes rooted at the honeypot under the attack toward attack resources. To reduce the put-off, progressive lower back-propagation is used to deal with low-rate attacks, which includes on-off attacks with brief bursts. However, there may be no protection machine to guard the honeypots against unknown attacks, fake negatives, fake positives and many others. If an attacker breaks into a honeypot, it'll spoil honey pot connections and make it a bouncer. For adding extra safety to the machine, Our Proposed Sub terrain Optimization rules is used to trace the intruders even as detecting the intrusion. Whilst the attackers found something precious in a root, they frequently use the equal route. Therefore, with the aid of tracing the track at the side of detecting intrusion detection, the honeypot can store the music of attackers. To clear up the hassle of attackers attacking the honeypot, we advise developing a protection gadget for the architecture. Here, we put into effect two technologies within the architecture to save you attackers to make honeypot from attacking different systems by way of user control of the relationship and manipulate of the spread of attacks. Therefore, a bug can be detected as an inflamed honey pot makes a lot of IP desk logs. The site visitors exceeding the restriction is dropped within the latter one. Further, a mechanism for multi-stage logging is used to defend the targeted facts of the attackers in device logs. Consequently, the gadget log records are retained after attacking the honeypots.

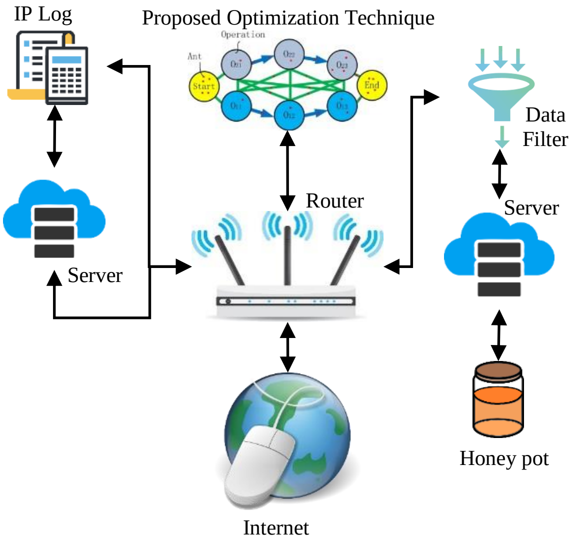

Fig.1. Proposed System Architecture

## 2.2 ASSEMBLY OF CLUSTERING TECHNIQUE

In returned propagation technique, server *S* performs twin movement i.e. server trade between providing service and acting as honeypot based on the timing component. Every server *S* enters a honeypot epoch, once they are scheduled to be inactive. Throughout a honeypot epoch, server *S* assumes that there may be no affordable traffic. As a result, any packet directed for *S* is maximum possibly an attack packet. A honeypot epoch ends as soon as server *S* is available in lively circumstance again. The honeypot epochs are selected based on the coordination between *S* and receiver *R* to keep away from any form of provider interruption. The honeypot epochs are time windows in which a server receives pure attack packets. To pick out the specific intruders and to maintain the file of the affected place the honeypots make use of our proposed sub terrain optimization approach.

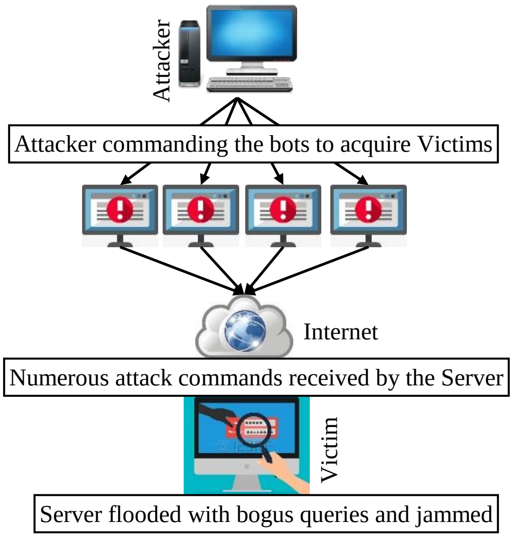
Attacker
Attacker commanding the bots to acquire Victims
Internet
Numerous attack commands received by the Server
Victim
Server flooded with bogus queries and jammed

Fig.2. Denial of Service Attack

## 2.3 OPTIMIZATION

An ant walks randomly on the initial degree. After they locate food and goes back returned to their colony and deposit some pheromone-based on the handed trails. Hence, the last ants can without difficulty discover the route and comply with the tune as opposed to on foot randomly. The deposited pheromone starts off evolved to evaporate. This can lower the enchantment. The navigation approximately the new intrusion could be very tons similar to ant locating meals. In case intruders find something important, then most of them will go to over and over. Else, they may go very rarely or nearly it's going to now not visit non-extensive target once more.

## 2.4 SECURE ARCHITECTURE OF HONEYPOT

If we want to avoid any kind of bug spreading from honeypot to different system within the community, a comfy architecture is proposed. To provide boost security, honeypot structure consists of following two fundamental parts. Data Control Limit: The reason of information manipulate is to limit the spreading of the affected honeypot to complete network machine. Multi-level IP log table: its far use to shield the private statistics about the attackers in device logs.

# 3. SIMULATION RESULTS

The Network Simulator (NS-2) [16] is used to simulate the proposed architecture. In the simulation, 100 nodes are used which are connected together in the simulation region for 10 seconds of simulation time. All nodes have the same transmission range of 250 meters. The Simulation topology is shown in Fig.3.

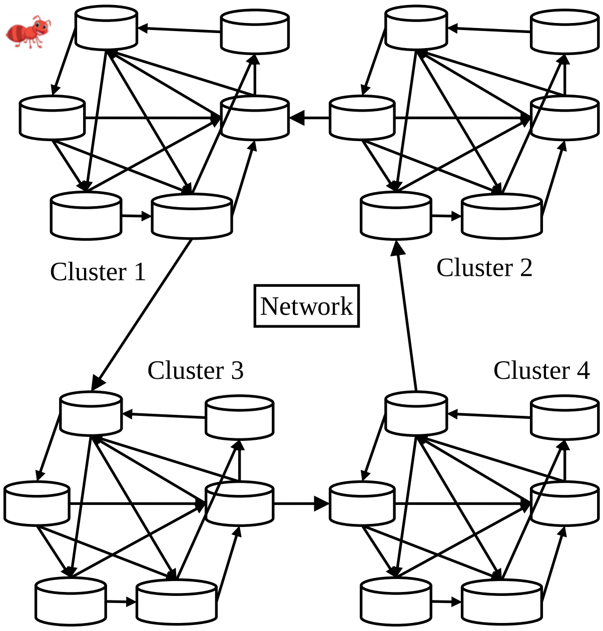

Fig.3. Simulation Topology

## 3.1 PERFORMANCE METRICS AND RESULTS

The proposed Detection technique is as compared with the digital Honeypot technique. The performance is evaluated based totally on average delay, packet delivery ratio, throughput and false-positive rate.

### *3.1.1 Based on Intruders:*

The simulation parameters such as the average delay, throughput, packet delivery ratio and the false positive rate with respect to the number of intruders are discussed below:

*Average Delay*: This graphical representation dealt with the depiction of average delay between the proposed Sub terrain optimization algorithm and the virtual honeypots technique. Here is the graphical representation below in Fig.4, we can clearly see that the delay gets increasing as the number of intruders is increasing. In addition our proposed system.

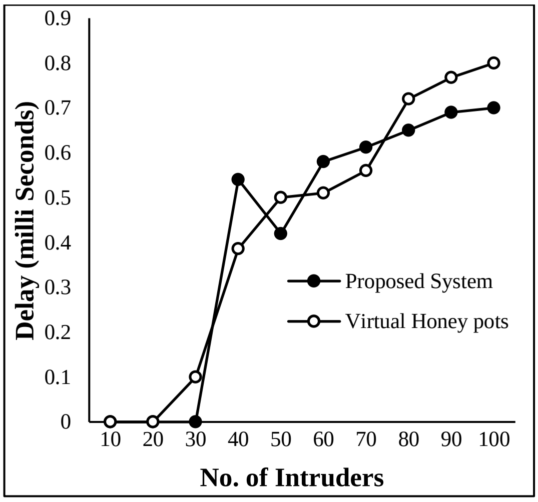

Fig.4. Average Delay

*Packet Delivery Ratio (PDR)*: The Fig.5 states that the packet delivery ratio for the proposed optimization technique is way better than the virtual honeypot that the virtual honeypot nearly went to 20% delivery ration at 100 intruders, while our suggested sub terrain optimization technique will remain, giving a packet delivery ratio of nearly 50% at 100 intruders.

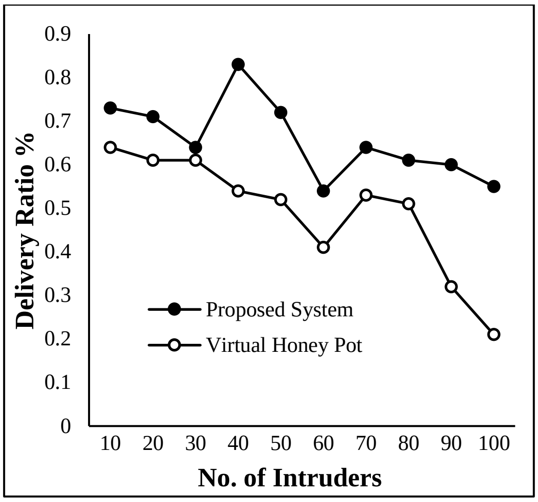

Fig.5. Packet Delivery Ratio

*Throughput*: Here in this graph, the proposed sub terrain optimization outperforms than the virtual honeypot. We can see from the blow Fig.6 that, at the time of 30 intruders the proposed sub terrain a throughput of 86,951 packets per second, while the virtual honeypot having a throughput of 68,569 packets per second.

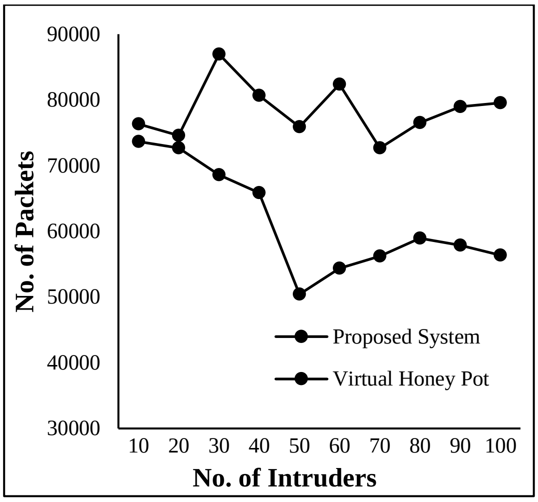

Fig.6. Throughput

*False Positive Rate*: In the Fig.7, the proposed sub terrain optimization technique having a lower false positive rate when compared to the virtual honeypots. The number of intruders and the false positive rate is directly proportional. It is clear from the below graph that our proposed system is efficient than the virtual honeypot and it had the lowest false positive percentage.

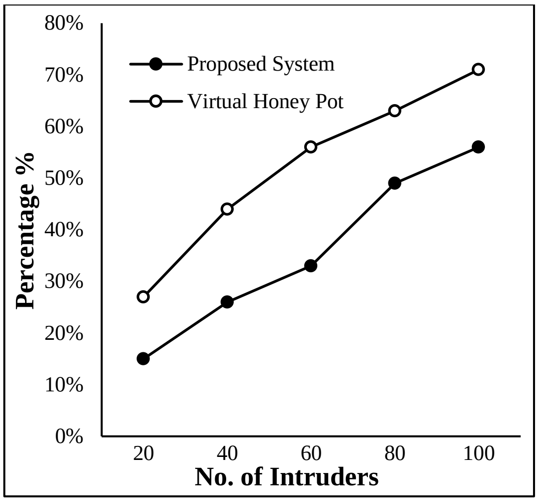

Fig.7. False positive rate

### 3.1.2 *Based on Clustering Level:*

The simulation parameters such as the Average Delay, Throughput, Packet Delivery Ratio and the false positive rate with respect to the level of clustering as level 0, level 1 and level 2 are discussed below:

*Delay*: From the Fig.8, we can clearly say that our proposed technique is having the lesser delay percentage than the virtual honeypot that, at the level 2 of clustering the virtual honeypot is having the delay of 0.458 milliseconds, while the sub-terrain optimization is having only 0.321 milliseconds delay.

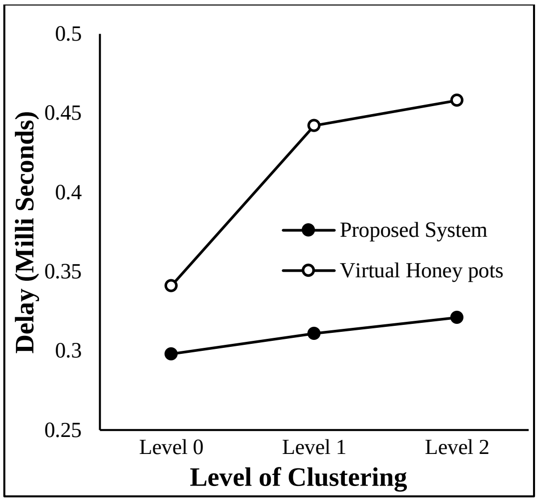

Fig.8. Delay Mean

*Packet Delivery Ratio (PDR)*: In Fig.9, the packet delivery of the two techniques is graphically represented that, at level 2 of clustering the packet delivery ratio degrades to 63.2% for the virtual honeypot, while the packet delivery ratio for the proposed sub terrain optimization is having 73.5% PDR. So, our proposed system is having better efficiency in the packet delivery.

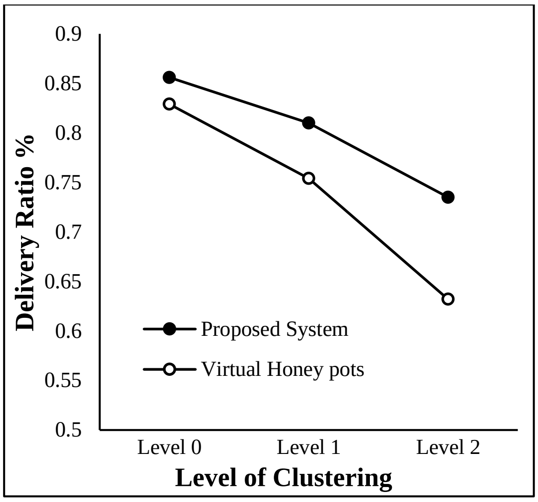

Fig.9. Packet Delivery Ratio

*False Positive Rate*: In the following Fig.10, the False Positive Rate at the clustering level of 2 for the proposed sub terrain optimization clustering is 36%, while the False Positive Rate at the clustering level of 2 for the virtual honeypot is 49%. Hence our proposed sub terrain optimization technique outperforms than the virtual honeypot.

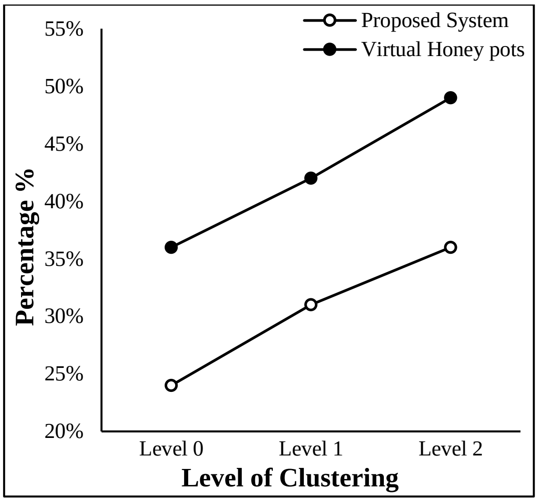

Fig.10. False Positive Rate

## 4. CONCLUSION

This research article proposed a sub-terrain DDoS Detection Technique to exploit the Virtual Honey Pots. Initially, a Virtual Roaming Honey Pot is employed beside the multi-level secure design to gather the knowledge regarding numerous intruders at completely different levels of the network. supported Sub terrain optimization technique, all the knowledge regarding the intruders are collected and sent to the multi-level design to limit any association of the intruders to prevent any unfold of intruders. Multi-level information processing log table is employed to sight the intruders at the completely different level of the network. Once the affected space is found, the knowledge is distributed to multi-level design to limit the dispersion of the affected space. This information is distributed to the network against the intruders. Simulation results show that the projected technique reduces the false positives and will increase the packet delivery magnitude relation and output.

## REFERENCES

[1] A. Masood and J. Jim, "Static Analysis for Web Service Security-Tools and Techniques for a Secure Development Lifecycle", *Proceedings of IEEE International Symposium on Technologies for Homeland Security*, pp. 121-124, 2015.

[2] Jawad Hussain Awan et.al., "Security Strategies to Overcome Cyber Measures, Factors and Barriers", *Engineering Science And Technology International Research Journal*, Vol. 1, No. 1, pp. 51-58, 2017.

[3] M. Dabbagh et al., "Software-Defined Networking Security: Pros and Cons", *IEEE Communications Magazine*, Vol. 53, No. 6, pp. 73-79, 2015.

[4] Kianoosh G. Boroojeni, M. Hadi Amini and S.S. Iyengar, "Overview of the Security and Privacy Issues in Smart Grids", *Proceedings of Smart Grids: Security and Privacy Issues*, pp. 1-16, 2017.

[5] M. Wang and Zheng Yan, "Security in D2D Communications: A Review", *Proceedings of IEEE Trustcom/BigDataSE/ISPA*, pp. 63-69, 2015.

[6] M. Aamir and M.A. Zaidi, "A Survey on DDoS Attack and Defense Strategies: from Traditional Schemes to Current Techniques", *Interdisciplinary Information Sciences*, Vol. 19, No. 2, pp. 173-200, 2013.

[7] Chelsea Montgomery, "New Security for a New Era: An Investigation into Law Enforcement Cybersecurity Threats, Obstacles, and Community Applications", Master Thesis, Department of Science of Cybersecurity, Utica College, 2017

[8] A.B. Fernandes, et al., "Security Issues in Cloud Environments: A Survey", *International Journal of Information Security*, Vol. 13, No. 2, pp.113-120, 2014.

[9] W. Ding, Z. Yan, and R.H. Deng. "A Survey on Future Internet Security Architectures", *IEEE Access*, Vol. 4, pp. 4374-4393, pp. 4374-4393, 2016.

[10] Claude Fachkha, "Security Monitoring of the Cyber Space", Available at: https://arxiv.org/ftp/arxiv/papers/1608/1608.01468.pdf

[11] P. Ravi Kumar, P. Herbert Raj and P. Jelciana, "Exploring Security Issues and Solutions in Cloud Computing Services-A Survey", *Cybernetics and Information Technologies*, Vol. 17, No. 4, pp. 23-31, 2017.

[12] Parnian Najafi Borazjani, "Security Issues in Cloud Computing", *Proceedings of International Conference on Green, Pervasive, and Cloud Computing*, pp. 32-36, 2017.

[13] Mohammad Masdari and Marzie Jalali, "A Survey and Taxonomy of DoS Attacks in Cloud Computing", *Security and Communication Networks*, Vol. 9, No. 16, pp. 3724-3751, 2016.

[14] R. Kavitha and G. Padmavathi, "Advanced Random Time Queue Blocking with Traffic Prediction for Defense of Low-Rate DoS Attacks against Application Servers", *International Journal of Communication Networks and Information Security*, Vol. 9, No. 1, pp. 127-132, 2017.

[15] Ji Min Park, "*Finding Effective Responses against Cyber-Attacks for Divided Nations*", Master Thesis, Naval Postgraduate School, 2015.

[16] Quan Jia, Kun Sun and Angelos Stavrou, "Motag: Moving Target Defense against Internet Denial of Service Attacks", *Proceedings of 22<sup>nd</sup> International Conference on Computer Communications and Networks*, pp. 227-231, 2013.

[17] Sunil Chaudhary, et al., "Applying Finite State Process Algebra to Formally Specify a Computational Model of Security Requirements in the Key2phone-Mobile Access Solution", *Proceedings of International Workshop on Formal Methods for Industrial Critical Systems*, pp. 23-27, 2015.

[18] Karanpreet Singh, Paramvir Singh and Krishan Kumar, "Application Layer HTTP-GET Flood DDoS Attacks: Research Landscape and Challenges", *Computers and Security*, Vol. 65, pp. 344-372, 2017.

[19] Huangxin Wang et al., "A Moving Target DDoS Defense Mechanism", *Computer Communications*, Vol. 46, pp. 10-21, 2014.