Paper Title:
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS DETECTION MECHANISM

Large Scale Paper Link: https://arxiv.org/ftp/arxiv/papers/1201/1201.2007.pdf

****1.1 Motivation/purpose/aims/hypothesis:****
The motivation is to outline a solution to combat Distributed Denial-of-Service (DDoS) attacks, which disrupt online services by overwhelming servers with fake traffic. Traditional congestion-control methods don't work because these attacks come from malicious sources. Therefore, the idea is to equip routers with the ability to detect and discard suspicious traffic by the strategy called pushback. Another approach involves using puzzles to verify if incoming traffic is genuine. By combining these two methods into a new scheme called Router-based Pushback, the aim is to effectively identify and block DDoS attacks.

****1.2 Contribution:****
The contribution of this proposed method is its robust defense mechanism against malicious hosts within the network, particularly targeting the challenging Denial of Service (DoS) attacks. By effectively identifying attacker hosts based on their traffic patterns, the system can swiftly block all traffic originating from these malicious sources. The integration of client puzzles adds an additional layer of validation. The implementation of pushback alleviates the processing workload on intelligent routers by outsourcing puzzle verification to upstream routers. It also ensures that attacker traffic is efficiently intercepted at the network edge, preemptively thwarting denial of service attacks and enhancing the overall security and stability of the network.

****1.3 Methodology:****
The methodology proposed aims to develop a robust defense mechanism against resource consumption attacks, specifically denial of service (DoS) attacks, which flood networks with excessive traffic leading to congestion and service disruptions. The hybrid model combines two key components: a pushback mechanism and client puzzles. Installing intelligent routers across ISP networks which then identify potential attacker hosts and redirect them to upstream routers. Secondly, upstream routers issue puzzles to suspected hosts for validation. Since resource consumption attacks are typically automated and lack human interaction, legitimate hosts can solve these puzzles, distinguishing them from attackers who fail to solve them. This hybrid approach integrates router-based client puzzles at the network edge, enhancing defense capabilities against both DoS and Distributed Denial of Service (DDoS) attacks.

****1.4 Conclusion:****
In conclusion, the paper presents a robust defense against malicious hosts within the network which effectively identifies and blocks attacker hosts based on their traffic behavior. Leveraging client puzzles adds a valuable layer of validation, distinguishing between suspected hosts and legitimate users. Pushback further streamlines the process by redistributing the workload to

upstream routers. Attacker traffic is efficiently blocked by this at the network edge, preemptively thwarting denial of service attacks and ensuring the network's security and stability

****Limitations****

****2.1 First Limitation/Critique:****
While the proposed system demonstrates promising defense capabilities against malicious hosts and effectively identifies attacker traffic it seems that the simulation environment may not fully capture the complexities of real-world network dynamics. Network Simulator models all nodes with identical functionality that potentially oversimplify the diverse roles and behaviors of network components.The behavior of legitimate users and attackers in the simulated environment may not accurately reflect real-world scenarios, potentially limiting the generalizability of the results. Moreover, the traffic generation mechanisms for legitimate users and attackers may not accurately represent their respective behaviors, potentially introducing biases into the simulation results..

****2.2 Second Limitation/Critique:****
The proposed system's reliance on intelligent routers and client puzzles may introduce performance overhead and scalability challenges in large-scale networks. While the pushback mechanism and client puzzles contribute to the system's effectiveness in identifying and mitigating DDoS attacks, their implementation may require significant computational resources and network overhead. Additionally, the effectiveness of client puzzles in differentiating between legitimate users and attackers may be limited in scenarios where attackers employ sophisticated evasion techniques. Therefore, while the proposed system presents a promising approach to DDoS defense, further research and experimentation are necessary to address these limitations and ensure its effectiveness in diverse network environments.

****Synthesis****
The discussion revolves around the development of a defense mechanism against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks within computer networks. The proposed solution integrates client puzzles and pushback mechanisms to identify and mitigate malicious traffic effectively. The simulation of this defense system highlights its potential to reduce the impact of attacks on network resources. But there are some limitations to consider, such as the simplified nature of the simulation environment and potential scalability challenges in real-world implementations. Despite these limitations, the proposed system shows promise in enhancing network security and mitigating the disruptive effects of DoS and DDoS attacks.