

A novel botnet attack detection for IoT.

Problem Statement:

Problem Domain: The problem domain revolves around the security vulnerabilities inherent in Internet of Things (IoT) devices, particularly their susceptibility to botnet attacks.

Description of the Problem: Botnets pose a significant threat to the security and functionality of IoT devices. These attacks involve a network of compromised devices, often recruited through malware, controlled remotely by a malicious actor (botmaster) to perform coordinated actions, such as distributed denial-of-service (DDoS) attacks, data exfiltration, or other malicious activities. Traditional security measures are often insufficient to detect and mitigate botnet attacks targeting IoT devices due to their resource constraints, diverse communication protocols, and heterogeneous nature.

Significance: The proliferation of IoT devices in various domains, including smart homes, healthcare, industrial automation, and smart cities, underscores the critical need for effective botnet attack detection mechanisms. Failure to address this issue exposes these systems to severe security breaches, leading to compromised data integrity, privacy violations, service disruptions, and potentially catastrophic consequences. Furthermore, IoT devices often handle sensitive information and control critical infrastructure, amplifying the urgency of safeguarding them against botnet threats.

Existing Solutions: Existing solutions for botnet detection in IoT environments primarily rely on traditional intrusion detection systems (IDS), anomaly detection techniques, and machine learning algorithms. However, these approaches encounter challenges such as high false positive rates, limited scalability, and the inability to effectively detect sophisticated botnet activities. Additionally, many IoT devices lack the computational resources to support complex security mechanisms, necessitating lightweight and energy-efficient solutions.

Justification for Research: The need for research in novel botnet attack detection mechanisms for IoT is justified by the shortcomings of existing solutions and the evolving landscape of IoT security threats. With the increasing complexity and scale of botnet attacks targeting IoT devices, there is a pressing demand for innovative approaches that can accurately detect and mitigate these threats while minimizing resource overhead and false alarms. Addressing this research gap will not only enhance the resilience of IoT ecosystems against botnet attacks but also contribute to advancing the overall security posture of interconnected systems in the digital age.