CHAPTER 1

INTRODUCTION

1.1 The Emerging Threat of DDoS Attacks for IoT Networks

The quick expansion of the Internet of Things (IoT) linking devices to enhance efficiency also leads to heightened vulnerabilities. Perhaps one of the most critical challenges rising with increasing vulnerability is the DDoS attack. In a DDoS attack, compromised devices-often called bots-sent malicious traffic to overflow the targeted network, breaking its normal operations.

IoT devices are most prone to such attacks due to very low computing capabilities and weak security features. Once such devices come into the hands of attackers, it becomes a tool of immense DDoS attack through botnet and services go totally down with the likelihood of data breaches and financial loss.

1.2 Impact of Real-time Detection and Mitigation

Traditional solutions of IoT security fail to detect most of the DDoS attacks, especially in real time. Most IoT devices tend to be extremely interconnected, with highly dynamic network traffic flows; hence, any type of proactive measure for security should be able to identify and neutralize such threats at the moment they may arise.

Minimizing damage due to DDoS attacks requires real-time detection and mitigation. Malicious traffic overload servers unless acted on in real time, hence resulting in system downtime and decreased performance. This poses the need for highly sophisticated security frameworks that can respond quickly to threats under IoT settings if perpetual service availability is to be sustained.

1.3 Dynamic Fuzz Testing Framework with AI

The framework identifies the limitation that currently exists with IoT security approaches and proposes an AI-driven Dynamic Fuzz Testing framework that incorporates GNNs as a sophisticated solution for real- time DDoS detection and mitigation. Analyzing network traffic patterns, the GNN-based model differentiates between legitimate and malicious traffic, thereby enabling dynamic and accurate threat response capabilities.

It is based on simulations with NS3. Simulations are based on real traffic data and, by virtue of normal and attack conditions, are used in training the model to identify a vast number of attacks. Thus, the robustness in the detection capability is realized. It integrates the model into an IoT network through which continuous monitoring of traffic at the entry points can be done. Malicious sources are identified and blocked without affecting legitimate operations.

1.4 Contribution and Future Prospects

The Dynamic Fuzz Testing framework offers several key contributions to IoT security, which also comprises state-of-the-art DDoS mitigation approaches. First, this approach, in contrast to the traditional methods, poses an AI-driven approach for real-time DDoS detection and mitigation. It uses GNN in such a way that complex patterns and relationships within traffic can be learned by the model, thereby making it more accurate and efficient towards threat detection.

One of the most interesting facts this project demonstrates is the framework's ability to handle high traffic loads, even in complex network topologies, with no loss in overall performance.

The future for the project is to concentrate on improving real-time capabilities within the system, including expanding its scope in attacking scenarios it may address, and adaptive learning to meet emerging threats. The framework can also be used in conjunction with other security tools to develop an all-rounded defense system against IoT networks offering stronger protection against evolving cyber-attacks.