ABSTRACT

The exponential growth in IoT adoptions has brought such networks to be much more vulnerable to Distributed Denial of Service attacks. In the DDoS attack, network performance issues and device vulnerabilities are exploited for inflicting far-reaching disruptions. Traditional IoT security solutions have proven inadequate in detecting and mitigating sophisticated threats in a timely and efficient manner, leaving IoT systems exposed to serious risks. This paper therefore presents an AI-driven security framework to adapt the detection and mitigation approach of DDoS attacks in IoT networks through dynamic fuzz testing and its integration into Graph Neural Networks (GNNs). This approach enables real-time identification and neutralization of malicious activities. The framework leverages the NS3 simulation tool to create realistic and diversified network traffic flows, which are used to train the GNN model. As a result, the model is prepared to handle various traffic patterns and attack scenarios, making it robust against real-world conditions. Once deployed in a live environment, the model monitors network traffic, identifies DDoS attacks, and mitigates them without disrupting legitimate IoT operations. The proposed framework achieved a 74% detection accuracy and a 95% success rate in mitigation during trials, highlighting its scalability and adaptability. This capability ensures that the framework can effectively address present and future IoT security challenges. The integration of AI with dynamic fuzz testing offers comprehensive protection, ensuring the integrity, availability, and reliability of IoT networks, making it an essential component of future IoT architectures by providing high-quality security against evolving DDoS threats.