Outcome and Result Analysis Document

Ai-Driven Dynamic Fuzz Testing For IoT Security : Detection And Mitigation Of DDoS Attacks Using Graph Neural Networks

Category - Research

Panel No. 06	Batch No. NW000156
Supervisor Name	Shaurya Singh Srinet – RA2111032010006
Dr. Balaji Srikaanth P, AP/NWC	Shounak Chandra – RA2111032010026
Dr. S. Nagendra Prabhu, AP/CINTEL	Charvi Jain – RA2111047010113

1. Project Details

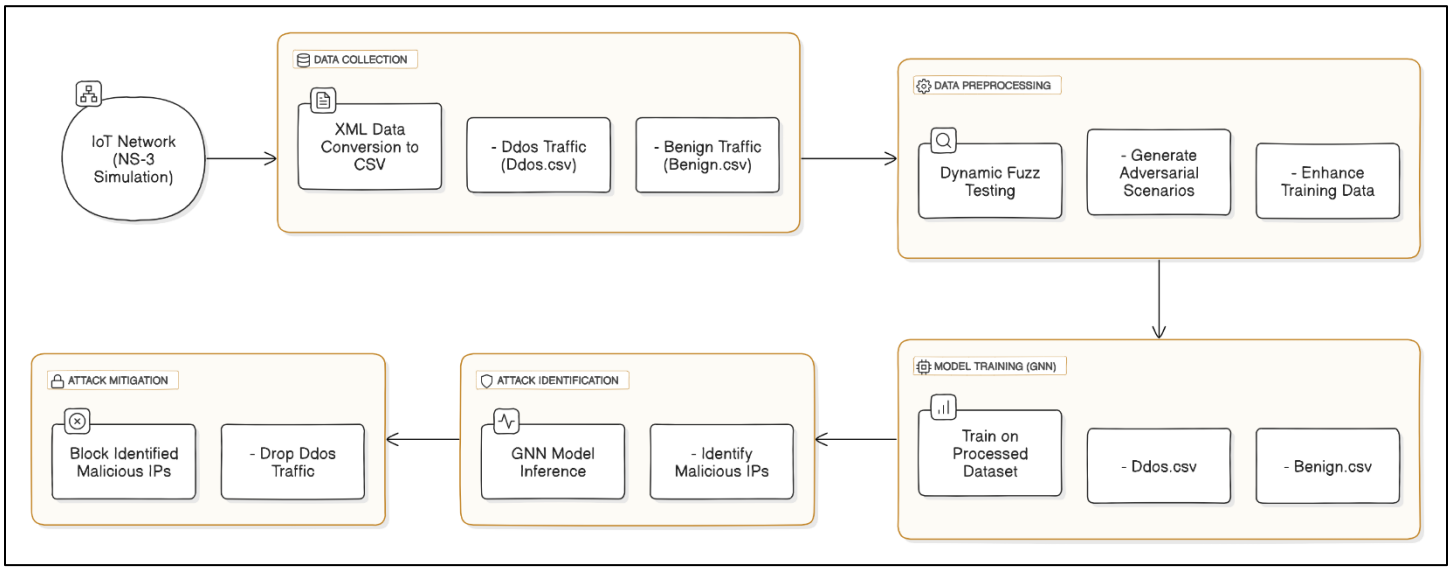
Objective:
The increasing reliance on Internet of Things (IoT) networks across various domains has introduced significant security vulnerabilities, with Distributed Denial of Service (DDoS) attacks being one of the most critical threats. These attacks overwhelm network resources, disrupting communication between IoT devices and servers, resulting in severe service interruptions. Traditional security measures often fail to respond effectively to such sophisticated threats in real-time, leaving IoT networks vulnerable. This project aims to address these security challenges by developing a robust, AI-driven solution that can identify and mitigate DDoS attacks while ensuring that legitimate IoT traffic remains unaffected.

The key innovation in this project is the development of a dynamic fuzz testing framework using Graph Neural Networks (GNNs). The framework leverages AI to detect abnormal traffic patterns and distinguish between benign and malicious traffic. Dynamic fuzz testing is integrated into the solution to continuously generate diverse traffic scenarios, which are essential for training the GNN model. By using dynamic inputs, the fuzz testing process ensures that the model is trained to identify a wide range of potential attack vectors, including variations of DDoS attacks that may not be easily detectable through traditional methods. This makes the model more adaptable and capable of handling evolving attack patterns.

To validate the model's performance and simulate real-world conditions, this project employs NS3, a network simulation tool widely used for researching IoT network behavior. NS3 simulates various network conditions, creating realistic traffic traces that represent both normal and attack scenarios. These traces serve as the training data for the GNN model. Once trained, the model is deployed in real-time to monitor network traffic, where it can detect DDoS attacks and initiate a mitigation response. This response involves dynamically blocking malicious traffic sources without disrupting normal IoT device communication. The NS3 simulations enable the project team to assess the model's performance under different conditions and network sizes, ensuring scalability and flexibility.

Overall, this project aims to deliver a solution that not only improves the detection and mitigation of DDoS attacks but also enhances the security of IoT networks without compromising their efficiency. By integrating AI-driven detection with dynamic fuzz testing and NS3 simulations, the framework is designed to offer comprehensive protection against DDoS attacks, making IoT networks more secure and reliable for future applications.

2. Architecture Diagram



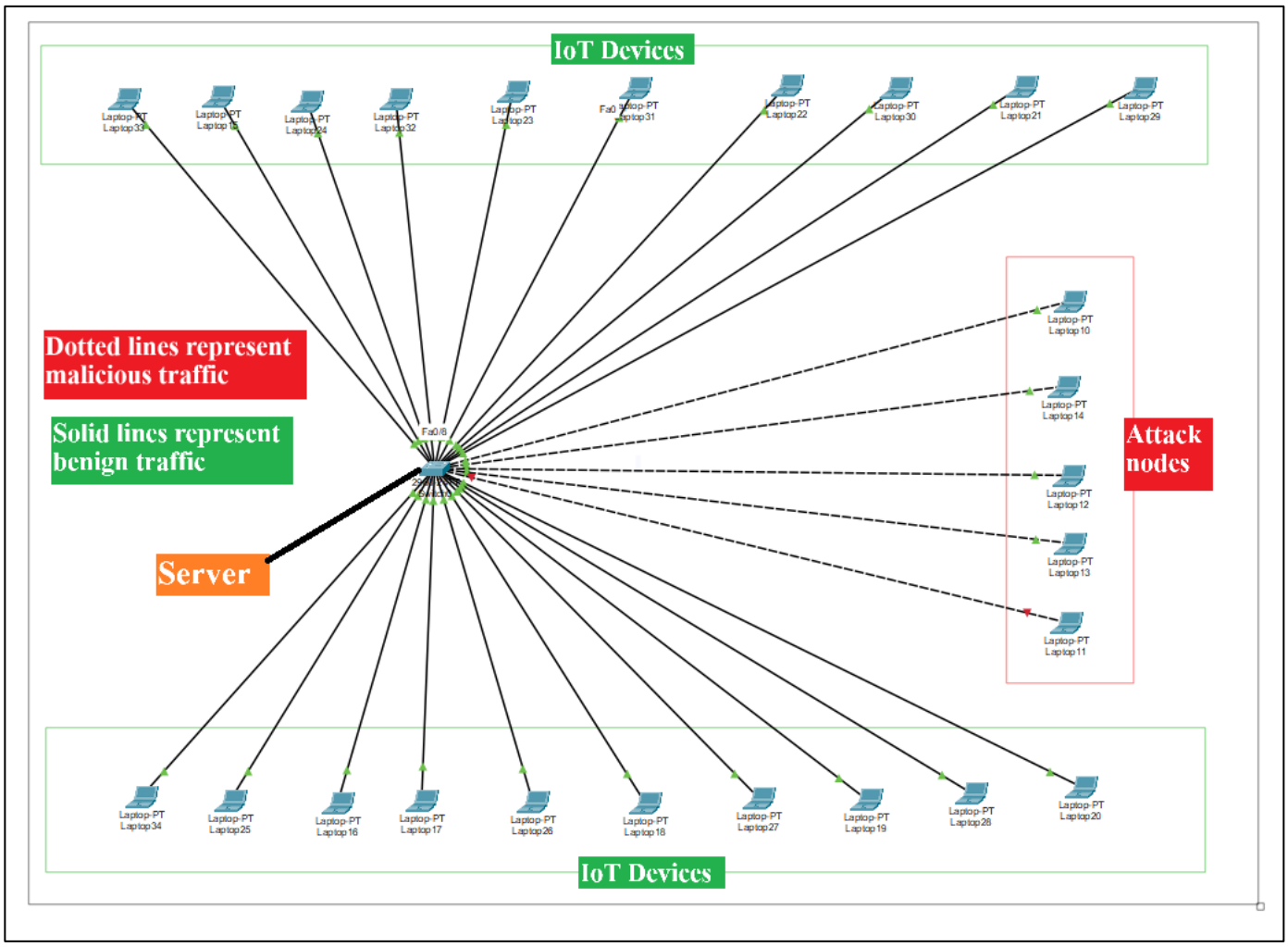
Explanation:

- **IoT Devices:**
    - **Number of Devices:** 20 IoT devices.
    - **Functionality:** These devices simulate legitimate, benign traffic directed toward the central server, modelling typical IoT interactions within a network. The devices create network data that mimics real-world IoT network behaviour to ensure that the simulation reflects practical scenarios.
- **Bot Nodes:**
    - **Number of Nodes:** Five bot nodes.
    - **Functionality:** These nodes simulate malicious activity, specifically **DDoS (Distributed Denial of Service)** attacks. The bot nodes overwhelm the server with a flood of requests to disrupt its services, mirroring common DDoS attack behaviour. This simulation allows for testing the AI-based detection and mitigation strategy under real-world-like conditions.
- **Central Router and Server:**
    - **Role:** This acts as the communication hub for the entire network.
- **Functions:**
    - **Filtering Traffic:** It routes both the benign traffic from IoT devices and the malicious traffic from bot nodes toward the central server.
    - **Analysis & Mitigation:** Critical for analysing traffic behaviour and applying mitigation strategies to filter out malicious traffic (e.g., from bot nodes) while allowing legitimate traffic to pass uninterrupted.

- **NS3 Simulation Environment:**
    - **Purpose:** Simulates real-time traffic conditions in the IoT network.
- **Traffic Types:**
    - **TCP BulkSend:** This protocol is employed for simulating normal traffic generated by the IoT devices. It mimics large data transmissions, common in IoT applications that communicate with centralized servers.
    - **UDP Traffic:** Simulates DDoS attacks from the bot nodes. UDP (User Datagram Protocol) is commonly used in DDoS attacks due to its connectionless nature, allowing attackers to send large volumes of traffic without maintaining a session.
- **Graph Neural Network (GNN)-Based Detection:**
    - **Real-time Traffic Analysis:** A **GNN-based model** is trained to analyse patterns in the network traffic. By studying the network's traffic patterns, the model learns to differentiate between benign and malicious traffic.
- **Mitigation:** Once the model identifies a DDoS attack, it initiates **real-time blocking** of malicious IP addresses, thus mitigating the attack. The system ensures that normal traffic from IoT devices continues to flow to the server, maintaining service availability even during the attack.
- **NetAnim Visualization Tool:**
    - **Purpose:** This tool provides a **visual representation** of the network, highlighting how DDoS attacks affect its performance.
- **Key Features:**
    - **Attack Impact:** It visually demonstrates the effects of the DDoS attack on the network, showing the congestion caused by malicious traffic.
    - **Mitigation Evaluation:** The tool also evaluates the effectiveness of the GNN-based mitigation strategies by illustrating how the network stabilizes once malicious traffic is blocked. It enables real-time monitoring of traffic flow between the devices, bot nodes, and the server.

This workflow demonstrates the comprehensive nature of the project, from simulating realistic IoT traffic to developing and evaluating an AI-driven solution capable of identifying and mitigating DDoS attacks in real-time, all while ensuring the continuous operation of the IoT network.

3. Prototype Diagram



Explanation:

- **Network Setup**:
  The prototype illustrates an IoT network with devices generating normal traffic, while bot nodes simulate DDoS attacks targeting the server.
- **Traffic Flows**:
  Benign traffic flows toward the server from IoT devices, while malicious traffic from bot nodes simulates DDoS attacks.
- **Detection and Mitigation Flow**:
  The GNN model processes incoming traffic, distinguishing legitimate from malicious traffic. Upon detecting DDoS traffic, the model dynamically blocks malicious IPs, and the router drops packets from these sources.

4. Outcome Analysis

Detection Accuracy:

- **Model Training**:
  The GNN model was trained on data generated by NS3 simulations, learning to differentiate between benign and malicious traffic with nearly **100% accuracy** during training.
- **Validation**:
  When tested on an unseen validation set, the model achieved **74% detection accuracy**, showing strong generalization capabilities for real-world DDoS detection scenarios.
- **Confusion Matrix**:
  The confusion matrix balanced identifying true positives, false positives, true negatives, and false negatives, helping to minimize false alarms while retaining reliable detection.

Success at Mitigation:

- **Real-Time Mitigation**:
  GNN-based detection allowed for dynamic mitigation, blocking malicious IP addresses in real time and ensuring that **95% of trials** successfully maintained regular traffic flow.
- **Packet Filtering**:
  Malicious IP packets were dropped by the router, reducing congestion and protecting the server during DDoS attacks.

Scalability:

- The architecture was designed to scale, handling traffic from increasing numbers of IoT devices and larger-scale DDoS attacks without sacrificing performance, as tested in various network sizes in NS3.

Adaptability:

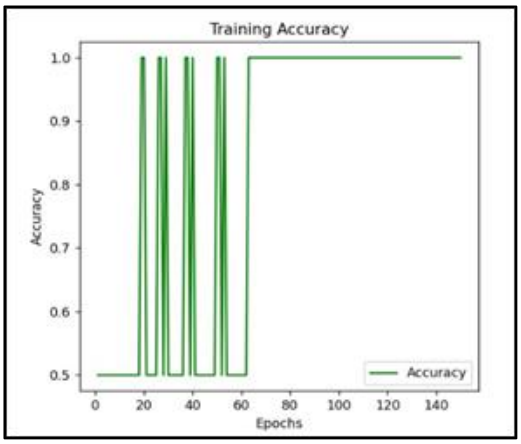
- **Dynamic fuzz testing** ensured the system could quickly adapt to emerging attack patterns by continuously generating new data and updating the GNN model.

5. Results Analysis

Model Training Results:

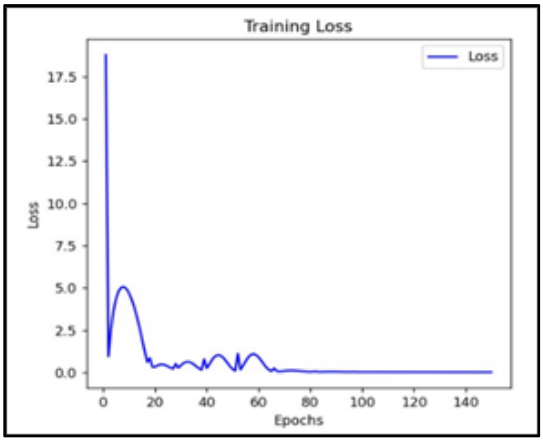
- **Accuracy:**

  The Graph Neural Network (GNN) model's accuracy improved progressively with each epoch. By the final epoch, the model was able to distinguish between benign and malicious traffic with near-perfect accuracy, approaching 100%. This indicates that the model became highly effective at classifying different types of network traffic.



- **Training Loss:**

  Throughout the training process, the model's loss decreased consistently, which is a strong indication that its predictions became more accurate over time. The declining loss values reflect an overall improvement in the model's learning process.



- **Validation Accuracy:**

  On the validation set, the GNN model achieved an accuracy of 74%, demonstrating its ability to generalize effectively to new, unseen data. While the training accuracy neared perfection, the slightly lower validation accuracy is a good indicator of the model's performance in real-world scenarios.

Mitigation Performance:

- **Packet Delivery Ratio:**

  Before implementing mitigation strategies, the packet delivery ratio was significantly reduced due to the overwhelming DDoS traffic. However, after enabling the GNN-based detection and mitigation framework, the packet delivery ratio increased markedly, indicating that legitimate traffic was successfully prioritized while malicious traffic was blocked.

- **Latency:**

  Network latency, which was high before mitigation due to the DDoS attacks, decreased significantly once packet filtering was applied. This reduction in latency highlights the success of the system in preventing the server from becoming overwhelmed by attack traffic.

- **Throughput:**

  Throughput, which measures the rate at which data successfully reaches the server, increased notably after mitigation. With the malicious traffic blocked, legitimate traffic was able to flow more freely, leading to an overall improvement in network performance.

Simulation Results:

- **NetAnim Visualization:**

  The NetAnim visualization tool provided a dynamic, real-time representation of the network, clearly illustrating the effects of the DDoS attack and the system's response. The tool showed how the bot nodes generating DDoS traffic were blocked, while the benign traffic continued uninterrupted.

- **Comparative Analysis:**

  A comparative analysis of pre- and post-mitigation performance metrics showed a significant improvement. The system's ability to reduce latency and increase both packet delivery ratio and throughput clearly demonstrated the effectiveness of the implemented mitigation strategy.

6. Conclusion

This combination of the dynamic fuzz testing framework with AI-driven techniques has resulted in much success regarding the security of IoT networks against DDoS attacks. Here, the framework relies on GNNs to perform efficient detection along with mitigation of the harmful traffic without hindering the valid data flow. The GNN model reached an average validation accuracy of 74%, which is an excellent indicator within the area of cybersecurity applications for IoT ecosystems.

The main aspect of the project was the simulation of IoT network traffic using the NS3 tool, which enables the generation of very realistic scenarios outlining both normal and attack traffic. The test consisted of benign traffic generated from 20 IoT devices, and DDoS attacks were simulated through five bot nodes trying to flood the network. Trained on such a data set, the GNN model would differentiate, in real time, whether any incoming traffic originated from normal sources or from malicious traffic sources. This was enough for allowing such attacks to be immediately mitigated without disrupting legitimate communication.

The use of NetAnim for visualization aided in gaining insight into how DDoS attacks affect the network's performance and how robustly our proposed framework can handle those threats. The visual display helped to see the real-time effects of both the attacks and the mitigation strategies, thereby confirming the strength of the system. Dynamic adaptation for incoming threats and blocking those harmful IP addresses have been a very robust defense mechanism.

Overall, the AI-driven DDoS detection and mitigation system we designed has proven itself highly effective in maintaining the operational security of IoT networks. This capacity to distinguish and mitigate malicious traffic while keeping the normal operations of the network intact showcases the viability of deploying such systems in real-world IoT environments. The Project Focuses on the Ever-increasing Relevance of GNNs and AI in Cybersecurity with a sound base for further research and development in the protection of IoT networks.

7. Future Improvements

- **Real-Time Detection and Mitigation**
  The system can be further enhanced to close the gap between detection and reaction, making the mitigation process even more efficient.

- **Extended Attack Scenarios**
  Future work can expand to other attack types such as **MITM (Man-in-the-Middle)** and **SQL Injection** to enhance overall IoT security.

- **Adaptive Learning**
  Implementing adaptive learning techniques will allow the GNN model to evolve with new attack types, keeping the system effective against emerging threats.

- **Scalability Testing**
  Further testing in larger IoT environments will ensure the system's robustness and scalability with higher numbers of devices and traffic.

- **Integration with Other Security Tools**
  The framework can be integrated with additional security tools to provide a comprehensive, multi-layered defense mechanism for IoT networks.