# CHAPTER 7
# CONCLUSION AND FUTURE ENHANCEMENTS

This chapter summarizes the findings of the project, highlighting the effectiveness of the AI-driven dynamic fuzz testing approach using Graph Neural Networks (GNNs) for DDoS attack detection in IoT networks. It discusses future enhancements needed to improve real-time mitigation, adaptability, and scalability of the system. Key areas for improvement include addressing a wider range of attack scenarios, implementing adaptive learning techniques, and integrating with other security tools. Overall, the chapter emphasizes the project's potential to enhance IoT security in an evolving threat landscape.

## 7.1 Summary of Findings

The novelty AI-driven fuzz testing methodology created dynamic traffic data on the NS3 network simulator. We produced a rich dataset consisting of benign traffic and DDoS attack traffic. We relied on fuzz testing to simulate some variability and predictability of the IoT environment, known for its heterogeneity, limited resources, and susceptibility to a broad range of attacks.

### 7.1.1 AI-Driven Dynamic Fuzz Testing

The module had used AI with Graph Neural Network (GNN) which was intended to identify malicious IoT network traffic patterns. It was understood that traditional learning algorithms would not work great in the case of graph-structured data and represented relationships among the IoT devices, which have thousands of interconnected elements. GNNs instead did very good discoveries of complex relationships and indirect dependencies where it mattered the most in graph-structured data and therefore best suited for IoT applications.

In our system, the GNN was trained on data outputted from the NS3 simulator, which provided it with a controlled testing environment for dynamic traffic scenarios. The model was trained in such a way that it achieved 74% validation accuracy, which is important considering the dynamic nature of IoT traffic. Although there is still room for improvement in this accuracy, it shows that the GNN can generalize well to unseen traffic patterns without overfitting.

This validates the perception that there is a contradiction between the low validation accuracy and nearly perfect training accuracy because of the extreme differences in traffic behavior; most of them are due to differences in devices, protocols, and network configurations.

### 7.1.2 NS3 Simulation and Visualization

The good simulation tool of powerful networking, NS3, was important to mimic real-world conditions of the IoT network. The simulator gave the needed infrastructure to test how well our system could detect and counter DDoS attacks in an environment close to the real world IoT traffic. Using NS3 gives us the chance to create profound patterns in the traffic to see and understand what is happening with malicious traffic, such as increased latency and decreased throughput, on a network.

We also used NetAnim, where we could see the dynamic flow of the traffic through the network in real-time. This is what, therefore, made the visual representation necessary for verification purposes in ascertaining if the strategy was working to curb the malicious transmissions because it provided evidence on how to spot and filter out such malicious traffic. If the GNN had detected an IP address, then NS3 was set to automatically drop all packets coming from that address. This packet-dropping mechanism has significantly reduced network congestion from DDoS traffic, and generally resulted in better overall performance.

### 7.1.3 Countermeasures

To mitigate the attack, the system will identify and drop packets coming from malicious IP addresses. This will successfully reduce the burden on the network, allowing genuine traffic to pass through. For IoT environments, for example, healthcare systems or smart cities, where network reliability is of paramount importance, failure in the network would have critical ramifications.

The packet-dropping mechanism appears to reveal some measurable improvements in network performance metrics. In a DDoS attack, the malicious packets drop served to significantly reduce network congestion and produced increases in throughput and latency correlated with this reduction. Such performance benefits provide evidence for the system's ability to ensure quality of the network despite the attack it may be under. The confusion matrix, a crucial method for measuring classification accuracy in the model, further revealed that the system can classify DDoS traffic with accuracy with minimal false positives and false negatives in the classification decision.

## 7.2 Future Improvement

Although the present system significantly Favors detecting and reducing the destructive nature of DDoS attacks in IoT networks, there are still many improvements that can be applied to further improve the overall performance, adaptability, and scalability factors. Some of the significant areas of improvement in the future are discussed below.

### 7.2.1 Real-time Mitigation

The real-time mitigation capability is one of the most important future development directions. Currently, a time lag exists between malicious traffic detection and incorporation of the strategy for mitigation. Such a delay may severely affect the timely delivery of certain IoT applications such as autonomous vehicles, smart grids, or healthcare systems. A brief network disruption in such applications could provoke catastrophic consequences.

To minimize this latency, the data pipeline of the system may be optimized to speed up the loop of detection to action. The use of edge computing methodologies will allow making decisions closer to the edge network on which the devices of the IoT are located. Since the processes of detection and mitigation can be decentralized, the detection and, hence, the subsequent mitigation could occur through edge devices in near real time too. This would further enhance its efficiency in delivering network performance during attacks.

### 7.2.2 Elaborated Attack Scenarios

Our system now protects against DDoS attacks; however, the IoT networks remain vulnerable to a myriad of cyberattacks including MITM attacks, SQL injection attacks, and data breaches. This definitely increases the utility and flexibility of the system exponentially through the extension into the detection and mitigation of other forms of attacks.

This will entail the design of more sophisticated datasets that capture the traffic patterns pertaining to a broader spectrum of attacks. The developed GNN model would be trained to recognize new patterns, thereby improving its capabilities with respect to a divergent set of threats associated with the IoT network. In addition, the modular architecture allowing for the realization of detection models for various types of attacks might make the system more flexible and adaptive towards new challenges associated with security.

### 7.2.3 Scaling Test

The scalability of an IoT network in a large-scale perspective is going to be one of the critical issues that are meant to be considered practically. All the testing that has been done so far has been within a controlled environment and with very limited devices. In real IoT networks, there might be thousands or millions of devices involved. This would cause a huge traffic, and thus the scalability along with heavy traffic performance needs to be tested in such a scenario for the system.

Future work might be implemented in distributed GNN implementations and the optimization of the packet filtering mechanism to provide effective and efficient operations of the system in high-throughput networks. Further improvement in scalability can also be made using distributed computing techniques such as parallel processing or federated learning in large IoT environments.

### 7.2.4 Adaptive Learning

Another improvement aspect is the adaptation of adaptive learning techniques. In the adaptive nature of an IoT environment, both network behaviour and attack patterns might change drastically. The static model, trained on a single dataset, may not be able to keep up with changes in those dynamics. Online learning techniques or reinforcement learning could be adapted so that the GNN model can keep learning over new data inputs and improve adaptability to changing network conditions. This would mean having detection levels accurate even with new emerging attack vectors in the system. It will also prevent overfitting since the model is going to refresh often with new data rather than sticking to old patterns.

### 7.2.5 Integration of Security Tool

The functionality of the current system can be improved highly. Thus, with integration into other security tools and frameworks, the system can detect and curb DDoS attacks effectively. For example, if the system is combined with IDS, firewalls, and SIEM systems, a more integrated security solution for IoT networks would be produced.

Such integration would, therefore, ensure an all-around approach to IoT security, with real-time monitoring, detection, and mitigation of a wide range of threats in cyber space. Such an integration would easily amalgamate with established infrastructures in real-world environments, providing end-to-end protection for IoT networks.

## 7.3 Conclusion

In conclusion, our dynamic fuzz testing technique based on Graph Neural Networks with simulations in NS3 has been promising as a key for enhancing the security of IoT environments. Here, the ability of the system to detect DDoS attacks with an accuracy of 74% generally indicates its potential utility in practical applications. In addition, the packet-dropping mitigation strategy has shown that it can enhance network performance by maintaining the throughput of the network and reducing the latency in the case of DDoS attacks.

The current system shall provide a good base. A couple of more advancements in the areas of real-time mitigation techniques, attack scenarios to check, scalability testing, adaptive learning, and integration with other security tools would make the system robust, adaptable, and scalable, having the potential for keeping up with the growing complexity and diversity of IoT networks.

Synthesizing advanced AI techniques with traditional network simulation tools presents an incredibly powerful approach toward addressing the challenges posed by security in IoT networks. As IoT networks grow in scale, our ability to protect them from growing sophistication in cyberattacks must keep pace. That is what this project represents in that direction, and the list of future enhancements detailed here paints a clear picture of what needs to be done to further build up the system in terms of effectiveness and resilience.