AI-Driven Dynamic Fuzz Testing for IoT Security: Detection and Mitigation of DDoS Attacks Using Graph Neural Networks

Guide Name	Panel Head
Dr. Balaji Srikaanth P	Dr. Vinoth Kumar S

Faculty Advisor	Project Domain
Dr. G. Suseela	Research

Student(s) Details: Name

1. Shaurya Singh Srinet
2. Shounak Chandra
3. Charvi Jain

Passport size photo(s)



Registration Number(s)

1. RA2111032010006
2. RA2111032010026
3. RA2111047010113

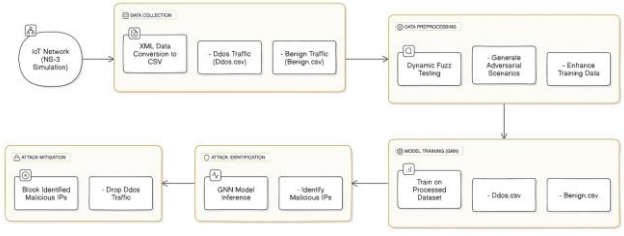
Email ID(s)&Mobile Number(s)

1: sn0273@srmist.edu.in & +919999847323	2: ss4958@srmist.edu.in & +919674617402
3: ca4617@srmist.edu.in & +916239884789	

Abstract

Distributed denial of service (DDoS) attack is one of the security threats brought by the rapid growth of Internet things based on number analysis. Such attacks are capable of severely impacting IoT network capabilities and expose this infrastructure to numerous security problems. Typical security measures seldom stand a chance to detect and suppress such advanced threats in real-time. In this work, we present an AI based security framework called Dynamic Fuzz Test integrated with Graph Neural Networks (GNNs) for detection and mitigation of DDoS attacks in the network. This framework uses NS3 simulations to create realistic network traffic traces, the GNN model is then trained using these data. The trained model is loaded to detect malicious traffic, guaranteeing IoT services of regular operation. Experimental results show that the proposed framework attains effective DDoS attack mitigation without affecting network performance.

Architecture Diagram



Significance of the Project

The project significantly enhances the security of IoT networks by integrating advanced AI techniques with dynamic fuzz testing to detect and mitigate DDoS attacks. By leveraging Graph Neural Networks (GNNs) and realistic network simulations, the project provides a scalable and adaptable solution that not only addresses current IoT security challenges but also prepares the infrastructure for future threats. This approach ensures the integrity, availability, and reliability of IoT systems, making it a crucial advancement in the evolving landscape of cybersecurity.

Conclusion

In conclusion, the proposed AI-driven framework, combining dynamic fuzz testing with GNNs, effectively detects and mitigates DDoS attacks in IoT networks. The framework's ability to distinguish between benign and malicious traffic while maintaining network performance demonstrates its potential as a robust security solution. This project lays the groundwork for future enhancements in IoT security, ensuring that IoT networks remain resilient against emerging threats.

Conference/Journal Publication Details (Mandatory)

4th International Conference on Cognitive & Intelligent Computing India https://sites.google.com/view/iccic2024	11/29/2024	Hyderabad,