CHAPTER 2

LITERATURE SURVEY

2.1 IoT Security Challenges

In the last couple of years, the Internet of Things has been growing with unprecedented growth, turning out to be an enormous and heterogeneous network of devices that communicate and interconnect with each other. Explosive growth has presented big challenges in many areas, especially in terms of security aspects for the devices that work on the edge of networks. These devices, relatively low computational power and often not very secure deployment environments, are inherently prime targets for many attacks, including, but not limited to, DDoS attacks[1].

Research further claims that the diversity among IoT devices- smart home appliances industrial sensors - has brought forth an extremely fractured security landscape. So, most devices have a weak security architecture, but the ones that are even exploitable are the ones that can become a cause of concern. Incidents like the Mirai botnet attack draw attention to the alarm-bells within the community. Obviously, the Mirai attack teaches the world a lesson in the IoT security renaissance as the compromised devices created havoc in multiple services with an alarm for proactive and strong security solutions.

Further observation of the exposed weakness in the IoT network would reveal other types of threat. In this instance, some examples would include unsecured channels of communication. For example, man in the middle attacks where data is intercepted midstream between devices. Often, these results from no encryption or weakly authenticated protocols[2].

Most of the IoT devices are still on old firmware; thus, they will probably expose themselves to risks that could easily be prevented if only the necessary updates were conducted in due time[3]. This irregular pattern of application in the case of IoT introduces a gigantic challenge toward the realization of a safe operational environment. Hence, the right time-by-time working as well as secured devices are one major issue while providing assurance to IoT networks.

2.2 DDoS Attacks on IoT Networks

DDoS attacks currently stand as one of the most effective challenges to any IoT network. DDoS attacks normally overwhelm a network or a service with an intolerable volume of traffic, making it unavailable to legitimate users. IoT architecture encompasses hundreds of thousands of connected devices, thereby easily meeting the definition of DDoS attacks on a large scale[4]. The most vivid example of how malicious elements can misuse these vulnerable devices to orchestrate devastating attacks rendering services paralyzed and even breaking entire networks is the infamous Mirai botnet attack.

In opposition to such an emerging threat, researchers have created several strategies toward mitigating DDoS attacks. Real-time Anomaly detection systems have evolved to monitor network traffic patterns and possibly detect DDoS attacks. These systems use machine learning algorithms, which tell normal from anomalous behavior, hence enable early intervention once unusual traffic patterns are detected. In addition, some network protocols have been designed with the explicit purpose of resisting DDoS attacks; they can tolerate huge amounts of traffic without compromising the quality-of-service[6]. These were quite effective, but indeed scaling them properly across the diversification of IoT devices is a quite challenging task considering their diverse capabilities and constraints.

The methods of DDoS attacks keep evolving with this forcing continued development and refinement in mitigation strategies. While the complexity and interconnectivity are growing in IoT networks, so is the likelihood of coordinated DDoS attacks. Thus, it will be important to let research and practice slightly lead to such emerging threats. Next, academics and industry will work together to build all-encompassing security frameworks that can be dynamic enough to cope with the fluid IoT ecosystem.

2.3 AI-Based IoT Security Solutions

Detection and prevention of DDoS attacks: In the last few years, AI has found significant importance in the domain of IoT security solutions. IoT security solutions based on machine and deep learning are fertile grounds for indicating anomalies in the behavior of the network that forebodes an impending DDoS attack[7].

These systems can be designed to learn and adapt rapidly to newly emerging threats, thus helping to improve the overall security posture of IoT networks by processing vast amounts of data from multiple devices.

Graph Neural Networks (GNNs) is essentially one of the salient strides in this direction: GNNs can be viewed as a strong framework to describe complex relationships among IoT devices and their interactions[8]. The positive features of GNNs allow exact malicious activity determination at complex network structure levels. Handling big-size network data is one salient feature of GNNs that can also capture spatial dependencies among nodes and is suitably adapted to the dynamic environment typically found in IoT applications[9].

This integration pathway of GNNs into the security framework of IoT opens further pathways towards better security. In the process, researchers can use more robust and flexible security solutions in exploiting the power of GNNs, in which these solutions can detect anomalies in networks as well as predict attacks even before they occur. This is preventive and is what builds protection for IoT networks against a constantly changing threat landscape.

2.4 Dynamic Fuzz Testing in IoT Security

Dynamic fuzz testing is known to be a reliable method of vulnerability detection in the internal functions of software components and network protocols. The injection of malformed or unexpected inputs to a system could reveal possible weaknesses attackers can use with malicious intent[11]. Dynamic fuzz testing can serve to be one of the most valuable assessment tools in the context of IoT security in relation to testing the resiliency of IoT devices and networks.

There have been some studies lately trying to extend dynamic fuzz testing in most attack scenarios such as DDoS attacks concerning the robustness of IoT systems in stress situations[12]. Fuzz testing with GNN-based AI models has recently become quite a hot topic as researchers strive to enhance the capabilities of the mechanisms for detecting and mitigating security threats. This synergy allows adaptive runtime assessment of IoT systems and even continuous mechanisms of monitoring and the fast response to any emerging vulnerabilities [12]. It implies the usage of state-of-the-art methodologies in improving the security level of IoT systems against growing threats within a constantly complex cyber landscape.

The infusion of dynamic fuzz testing in the IoT security frameworks would help in terms of vulnerability identification and improvement of the understanding of the attack surface presented by IoT devices. The ever- evolving threat means further development and refinement of fuzzing techniques will be key in continuing to keep IoT networks resilient to diversified attacks.

2.5 NS3 Simulations for IoT Security

NS3 fast is turning out to be the tool of choice in testing IoT security, mainly through the avenue of dynamic fuzz testing and measuring resilience to DDoS attacks. The prospects sired by NS3 simulations allow the researcher to be able to carry controlled experiments on different scenarios that allow simulating how IoT networks behave under different conditions [13]. These include finding if the claimed mitigation strategies are effective and how IoT systems react under stress.

Not long ago, experiments were conducted that integrated dynamic fuzz testing with GNN-based AI models so that the detection strategies employed in the NS3 simulations could be improved [14]. It is so designed that researchers can carry out an elaborate study on the IoT networks, indicating vulnerabilities and the effectiveness of security mechanisms in their existing form. NS3 affords tremendous simulation capabilities for the research to be performed in understanding the security issues of the ecosystem developed in the IoT system.

Simulation insights of NS3 can be used to develop more robust systems for IoT, capable of lasting the threat space for this developing and emerging threat. Along with its rapid growth and wide formation of its ecosystem, a collateral integration of the NS3 simulation tool and the likes would be necessary in developing an effective strategy in safeguarding interconnected devices from possible attacks.