Parvtibai Genba Moze College of

Engineering, Wagholi, Pune.

Department of Computer Engineering

Seminar Synopsis

On topic

DoS / DDoS Attack on IoT Devices

Presented By

Aditya Sachin More

Exam No: 72244658G

Class: TE(Comp)

Guide: Prof. Bharati Bisane. **Sign:**

1. Seminar Title:

"DoS / DDoS Attack on IoT Devices"

2. Seminar Area:

Internet of Things

3. Seminar Guide:

Prof. Bharati Bisane.

4. Technical Keywords:

IoT, DoS, DDoS, Security.

5. Problem Statement

There are many different types of DDoS attacks that can be launched against IoT devices.:

- **Volumetric attacks: -** These attacks involve flooding the target with a large volume of traffic.
- **Protocol attacks: -** These attacks exploit vulnerabilities in specific network protocols.
- **Application-layer attacks: -** These attacks target the application layer of the target's network. For example, an attacker could send a flood of HTTP requests to a web server, causing it to become unavailable.

DDoS attacks on IoT devices can have a significant impact. They can disrupt critical infrastructure, damage businesses, and even cause physical harm. For example, a DDoS attack on a hospital's network could prevent patients from receiving care.

6. Abstract:

Internet of Things (IoT) is an application of the internet correlation with devices that makes human life easy. The need to use (IoT) in our lives makes this field expands every day without stopping. Which would let everything connected to the internet exposure to penetration. As the need for (IoT) devices grows, the horizon of malicious abuse expands.

In this paper, we will study one of the most common violations in IoT devices, which is Distributed Denial of Service (DDoS) attack and study its impact on (IoT) devices in order to be aware to control our utilizations and the need to secure the Internet of Things devices in our lives.

7. Goals and Objectives:

- To deny access to a website or service.
- To overload a network or server, causing it to crash.
- To disrupt or delay a critical operation.
- To damage the reputation of a company or organization.
- To extort money from the victim.

8. Scope

The scope of a DDoS attack on IoT devices can vary depending on the size and complexity of the attack. However, some common factors that can affect the scope of an attack include:

- The number of IoT devices that are infected and controlled by the attacker.
- The bandwidth and resources of the infected devices.
- The type of attack that is being used.

The scope of a DDoS attack on IoT devices can also be affected by the resources of the attacker. A well-funded attacker with access to a large number of infected devices could launch a more powerful attack than a smaller attacker.

The type of attack that is being used can also affect the scope of the attack. A volumetric attack, which involves flooding the target with a large amount of traffic, can have a more significant impact than an application-layer attack, which targets specific vulnerabilities in the target's network.

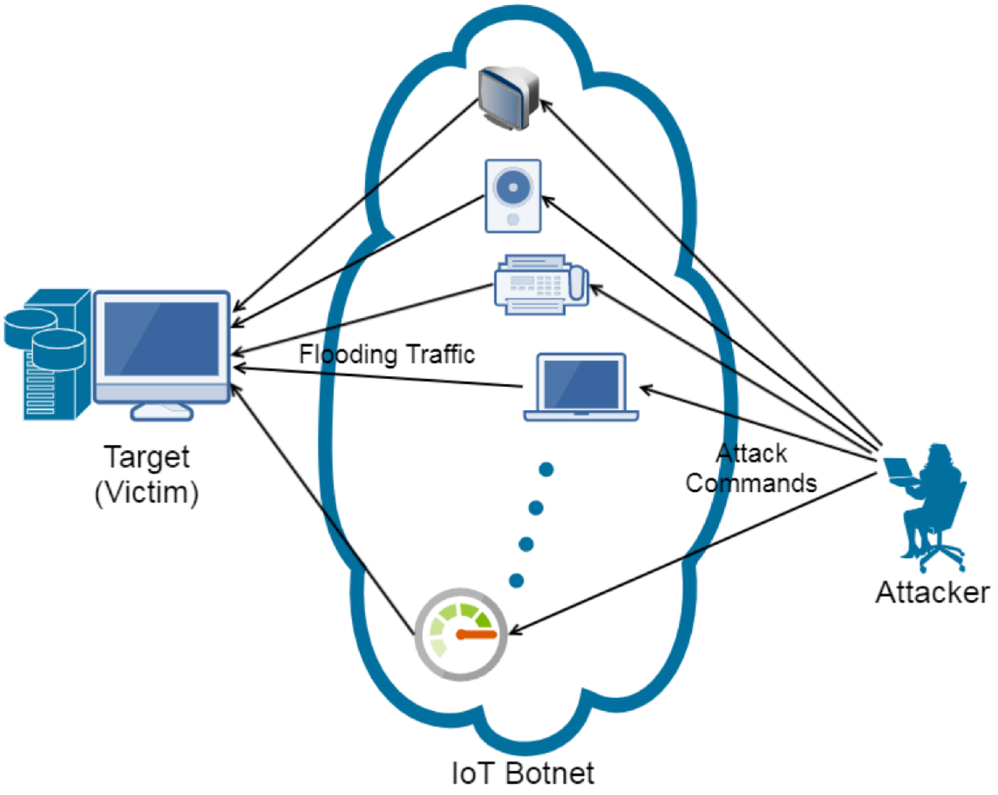
Finally, the target of the attack can also affect the scope of the attack. A critical infrastructure target, such as a power grid or a financial institution, would be more vulnerable to a DDoS attack than a less critical target.

9. Introduction:

Since the Internet of Things began, it has been facing many objections, due to concern about security vulnerabilities. Many violations can occur in hardware, software, operating systems or networks. Hackers have successfully exploited these devices and systems, to access resources, harm these devices and prevent service from legitimate users. In this paper, we will study DDoS attack on IoT devices to get know about what is the mechanism that allows occurring, how to defend our devices from DDoS attack and to be aware to protect systems and devices.

Internet of Things (IoT) is the wireless interconnection of smart devices or things connected over the internet. In recent years, IoT has emerged as a promising technological solution for providing connectivity to myriads of heterogeneous devices across the globe. IoT can help us to access, control and manage these devices to get various functionalities in multiple application scenarios like smart home, smart healthcare, smart transportation, smart industry, etc. It can allow us to automate device control in order to facilitate the ease of device usage, to provide comfort and convenience to human being thus enhancing the overall quality of life.

Denial of service (DoS) attacks and distributed denial of service (DDoS) attacks have been reported as the most common attacks on IoT devices and network [2]. A DoS attack is a malicious attempt done by an attacker using a single source to make a service or network resources inaccessible to legitimate users. When a DoS attack is launched using multiple distributed sources, it is called a DDoS attack.



10. Disadvantages of a DDoS attack on IoT devices:

- Financial loss.
- Damage to reputation.
- Increased security risks.
- Increased costs.

11. Advantages of DDoS Attack Prevention on IoT Devices:

- **Prevention of service disruption.** DDoS attacks can disrupt the availability of critical services, such as power grids, transportation systems, and healthcare systems. By preventing DDoS attacks, organizations can help to ensure that these services are available when they are needed most.
- **Protection of financial assets.** DDoS attacks can also lead to financial losses. For example, a company that is targeted by a DDoS attack may lose revenue if customers are unable to access their website or services. By preventing DDoS attacks, organizations can help to protect their financial assets.
- **Enhancement of reputation**. A DDoS attack can damage a company's reputation. By preventing DDoS attacks, organizations can help to protect their reputation and build trust with customers.
- **Reduction of security risks.** DDoS attacks can also increase the security risks for other devices on the network. By preventing DDoS attacks, organizations can help to reduce these risks and protect their overall security posture.
- **Avoidance of increased costs**. DDoS attacks can lead to increased costs for businesses and organizations. By preventing DDoS attacks, organizations can help to avoid these costs and save money.

12. Conclusion:

Dos/DDoS attacks and security solutions with respect to each IoT layer. It shows that every layer have different vulnerabilities exploited by attackers. Security possible solutions for the networks are also discussed, which makes the IoT network more secure. In order to have strong secure structure, we must take care of security issues for all different layers, not only single one. In other word, securing application layer only will not prevent attackers from hack network layer. As declared earlier, perception layer devices characterized with flexibility and ease of use, for reducing costs. This makes perception layer the most vulnerable layer and require extended research to identify capabilities.

Despite the massive number of DoS/DDoS prevention mechanism given in the literature, they need a lot of work and improvement. Because of IoT applications industry dynamically change. There is massive need to use technologies like machine learning and artificial intelligence to be able to make unified solution against different scenarios with heterogeneous devices, networks, and protocols. Furthermore, users of the applications must be aware of importance of using strong passwords and credentials, and update software as necessary.