Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices

Kavita Sharma, National Institute of Technology, Kurukshetra, India
B. B. Gupta, National Institute of Technology, Kurukshetra, India

ABSTRACT

This article describes how in the summer of 1999, the Computer Incident Advisory Capability first reported about Distributed Denial of Service (DDoS) attack incidents and the nature of Denial of Service (DoS) attacks in a distributed environment that eliminates the availability of resources or data on a computer network. DDoS attack exhausts the network resources and disturbs the legitimate user. This article provides an explanation on DDoS attacks and nature of these attacks against Smartphones and Wi-Fi Technology and presents a taxonomy of various defense mechanisms. The smartphone is chosen for this study, as they have now become a necessity rather than a luxury item for the common people.

KEYWORDS

DDoS, Denial of Service, Denial of Sleep, Network Security, Smartphone

1. INTRODUCTION

Communication is the basic requirement of human beings after air, water, food, clothes, and shelter. As human beings are social animals, they need to communicate. If the history of communication is looked upon, there was only one medium of communication; direct communication where a person communicated with another person present in front of him/her through direct talking. This was followed by exchanging written notes initially in near-by places followed by far-off places through birds like pigeons. They continued up to our recent past, but their mode upgraded by continuously removing associated limitations. Graham Bell changed the field of communication by introducing telephone to the world that revolutionized the communication sector. The telephone was further modified into cellular or mobile phones. Initially, these were only used for communicating voice. However, modern mobile phones are too much different from initial mobile phones. At the same time, computer and laptop industries have grown largely. People started to perceive the need for the computer and mobile phones in daily life. Laptops were developed so that they could be carried from one place to another, but they were still bulky (Zargar, Joshi, & Tipper, 2013).

Therefore, a need was felt to propose several computing features in mobile phones as they can be carried in the pocket easily. Mobiles slowly turned to be a media with much more facilities than simple voice communication devices and were further developed as Smartphone. The smartphone is a huge success to the communication sector, and its variety, sale, and facilities are increasing day-by-day. With an increasing utilization of Smartphone in the public domain, they have become vulnerable to
security attacks. There are many types of security attacks, but we emphasize here on DoS to current two Smartphone operating system iOS and Android (Zargar & Joshi, 2010).

DDoS attack targets that Smartphone a linked to the Internet. This attack generally performed in a group form to a Smartphone and attempt is made to disrupt each other’s operations in the network. These have some common reasons to attack, but the organizations realize its impact only after the attack has occurred. Oftentimes, attacks form a part of cyber crimes where the main aim is to bring down the competitor’s operating system. These attacks can be repelled by analyzing attacker’s nature and the path used by him/her for sending DDoS messages. To combat this problem, many organizations are providing DDoS mitigation & DDoS protection services (Al Quhtani, 2017; Yao, Ruohomaa & Xu, 2012). The target and the solution of DoS attacks are shown in Figure 1.

DDoS is used to interrupt a legitimate user by overwhelming all the resources and bandwidth of the mobile. This is achieved by performing simultaneous attacks from multiple sources.

To launch DDoS attacks (Alomari, Manickam, Gupta, Karuppayah & Alfaris, 2012; Gupta, Misra & Joshi, 2008; Chhabra, Gupta & Almomani, 2013), following two techniques are generally used:

1. **Malford Packets**: In this technique, the attacker sends some malformed packets in the network to perplex the victim.
2. **Interruption**: In this technique, attacker attacks in either of two ways:
   - Exhausting the resources of legitimate users
   - Exhausting the server resources of legitimate users

DDoS attacks are initiated remotely by creating botnet in the network; which further hires zombie (Trojan horse / Worm) to attack the network. Our Contribution to this paper is several. Initially, our main aims to review the recent research work of the DDoS attacks and its defense mechanisms in Smartphone as per today scenario. As cited, there are numerous studies on the DoS attack over

---

**Figure 1. Target and solution of DoS attacks (source: authors’ work)**
Student Support Services
[www.igi-global.com/chapter/student-support-services/44012?camid=4v1a](www.igi-global.com/chapter/student-support-services/44012?camid=4v1a)

Dynamic Maintenance of Service Orchestrations
Manel Fredj, Apostolos Zarras, Nikolaos Georgantas and Valérie Issarny (2011). *Service Intelligence and Service Science: Evolutionary Technologies and Challenges* (pp. 57-78).
[www.igi-global.com/chapter/dynamic-maintenance-service-orchestrations/47356?camid=4v1a](www.igi-global.com/chapter/dynamic-maintenance-service-orchestrations/47356?camid=4v1a)