Mitigate DoS and DDoS Attack in Mobile Ad Hoc Networks

Antonis Michalas, Athens Information Technology, Greece
Nikos Komninos, Athens Information Technology, Greece
Neeli R. Prasad, Aalborg University, Denmark

ABSTRACT
This paper proposes a technique to defeat Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks in Ad Hoc Networks. The technique is divided into two main parts and with game theory and cryptographic puzzles. Introduced first is a new client puzzle to prevent DoS attacks in such networks. The second part presents a multiplayer game that takes place between the nodes of an ad hoc network and based on fundamental principles of game theory. By combining computational problems with puzzles, improvement occurs in the efficiency and latency of the communicating nodes and resistance in DoS and DDoS attacks. Experimental results show the effectiveness of the approach for devices with limited resources and for environments like ad hoc networks where nodes must exchange information quickly.

Keywords: Ad Hoc Networks, Cryptographic Puzzles, Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS) Attack, Game Theory

INTRODUCTION
Denial of Service attacks (DoS) is considered to be one of the most important threats as well as one of the hardest problems in computer security nowadays. The main aim of a DoS attack is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the networks bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients. In general, we can distinguish two different types of DoS attacks: logic attacks and flooding attacks. Until nowadays, there are many security vulnerabilities which an adversary can exploit to launch such an attack.

The enhancement of DoS attack is the so called Distributed Denial of Service (DDoS) attack. In the past years we saw lot of popular sites such as Yahoo, eBay, Amazon, CNN and many more to be under such attacks. DDoS attacks present a significant security threat to corporations, and the threat appears to be growing. On August 6, 2009 the world of Social Networks was under attack, in other words, we were in the middle of a planned attempt to take

DOI: 10.4018/jdcf.2011010102
down two of the world’s most popular social sites: Facebook and Twitter. Even though no user data was at risk, the sites were down for several hours. DDoS, is a relatively simple, yet very powerful technique to attack Internet resources. DDoS attacks add the many - to - one dimension to the DoS problem making the prevention and more difficult and the impact proportionally severe. DDoS exploits the intrinsic weakness of the Internet system architecture, its open resource access model, which paradoxically, also happens to be its greatest advantage (Douligeris, 2004).

One way to categorize DDoS attacks is either as direct or as reflector. In a DDoS attack there is at least an attacker, a victim and an amplifying network. In a direct DDoS attack the invader is able to embed zombie software on a number of sites over the Internet. Frequently, in DDoS attack, two types of zombie machines are concerned, master zombies and slave zombies (Agents / Zombies). The host of both machines has been infected with malicious code. The attacker synchronizes and triggers the master zombies, which in turn coordinate and trigger the slave zombies. The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers (Staling, 2006).

A reflector DDoS attack adds another layer of machines. In this type of attack, the slave zombies construct packets requiring a response that contains the target’s IP address as the source IP address in the packet’s IP header. These packets are sent to uninfected machines known as reflectors. The uninfected machines respond with packets directed at the target machine. A reflector DDoS attack can easily involve more machines and more traffic than a direct DDoS attack and hence be more damaging. Further, tracing back the attack or filtering out the attack packets is more difficult because the attack comes from widely dispersed uninfected machines (Staling, 2006).

A solution to those threats is to authenticate the client before the server commits any resources to it. The problem though is the fact that secure socket layer (SSL) and transport layer security (TLS) protocols allow expensive operations (i.e. such as public key algorithms - RSA) to be performed at the request of unauthenticated clients. So for example if a large site can process around 4000 RSA operations per second and a partial SSL/TLS handshake consumes on average 200 bytes, then all it takes is approximately 800KB / sec. to paralyze the ecommerce site (Dean, 2001). In order to solve such problems, we can make use of cryptographic puzzles and games.

Unlike common wireless networks, ad-hoc networks are characterized by the absence of any existing network infrastructure or centralized administration (decentralized wireless network) as well as the ease and speed of deployment. Such networks are highly dynamic and each node participates in the basic functions of the network like packet forwarding and routing, since there are no routers or access points. Ad-hoc networks can operate in a stand-alone way or can be attached to a larger network.

Protection against DoS and DDoS attacks is a crucial component of any security system. Traditional DoS attacks involve overwhelming a particular host. However, in ad hoc networks, mobility, limited bandwidth, routing functionalities associated with each node, etc. open many new opportunities for launching such attacks. These attacks might be at the routing layer or at the MAC layer (Gupta, 2002).

**Our Contribution**

In this paper we propose two techniques. A new client puzzle to avoid DoS attacks and a multiplayer game in order to prevent DDoS attacks in ad hoc networks, where nodes do not necessarily belong to a single authority and the topology can be altered dynamically.

Our client puzzle solution has the following four attributes:

1) The creation of puzzles is not outsourced to a third entity (decentralized design).
2) The connection initiator is responsible to create and solve the puzzle on the fly.
Tattooing Attack: A New Type of Watermarking Attacks on Image Authentication
www.igi-global.com/article/tattooing-attack/120209?camid=4v1a