CCIT Report #477 March 2004

# Exposing and Eliminating Vulnerabilities to Denial of Service Attacks in Secure Gossip-Based Multicast*

Gal Badishi
*EE Department, Technion*

Idit Keidar
*EE Department, Technion*

Amir Sasson
*CS Department, Technion*

**Abstract**

We propose a framework and methodology for quantifying the effect of denial of service (DoS) attacks on a distributed system. We present a systematic study of the resistance of gossip-based multicast protocols to DoS attacks. We show that even distributed and randomized gossip-based protocols, which eliminate single points of failure, do not necessarily eliminate vulnerabilities to DoS attacks. We propose Drum – a simple gossip-based multicast protocol that eliminates such vulnerabilities. Drum was implemented in Java and tested on a large cluster. We show, using closed-form mathematical analysis, simulations, and empirical tests, that Drum survives severe DoS attacks.

## 1 Introduction

One of the most devastating security threats faced by a distributed system is a *denial of service* (DoS) attack, in which an attacker makes a system unresponsive by forcing it to handle bogus requests that consume all available resources. In a *distributed denial of service* (DDoS) attack, the attacker utilizes multiple computers as the source of a DoS attack, in order to increase the attack strength. In 2003, approximately $42\%$ of U.S. organizations, including government agencies, financial institutions, medical institutions and universities, were faced with DoS attacks [5]. That year, DoS attacks were the second most financially damaging attacks, only short of theft of proprietary information, and far above other attacks [5]. Therefore, coping with DoS attacks is essential when deploying services in a hostile environment such as the Internet [23].

As a first defense, one may protect a system against DoS attacks using network-level mechanisms [4]. However, network-level filters cannot detect DoS attacks at the application level, when the traffic seems legitimate. Even if means are in place to protect against network-level DoS, an attack can still be performed at the application level, as the bandwidth needed to perform such an attack is usually lower. This is especially true if the application performs intensive computations for each message, as occurs, e.g., with secure protocols based on digital signatures. In this paper, we are concerned with DoS attacks on *secure* application-level multicast protocols (such as, e.g., Spinglass [2]), focusing only on the multicast protocol layer.

A DoS attack that targets every process in a large system inevitably causes performance degradation, but also requires vast resources. In order to be effective even with limited resources, attackers target vulnerable parts of the system. For example, consider a tree-based multicast protocol; by targeting a single inner node in the tree, an attacker can effectively partition the multicast group. Hence, eliminating single points of failure is an essential step in constructing protocols that are less vulnerable to DoS attacks.

*A preliminary version of this paper appeared in The IEEE International Conference on Dependable Systems and Networks (DSN) 2004.