CCIT Report #500 August 2004

Silent Attack Hindering in Drum

Gal Badishi[1] Aran Bergman[2] Nadav Lavi[3] Isask'har Walter[4]
Electrical Engineering Department, Technion – Israel Institute of Technology

Abstract

Gossip based multicast is a scalable and reliable protocol for dissemination of information within a group of interconnected users.

Upon receiving or producing a message the process sends (*pushes*) it to a small constant subset of processes which is randomly selected out of the group of members. Some implementations of gossip based multicasts poll a small subset of processes for new information, effectively *pull*ing, instead of *push*ing it. In this manner, each message is eventually delivered to every process, with a high degree of probability [1].

An intrusion-tolerant version of a gossip-based multicast algorithm, developed by G. Badishi, I. Keidar and A. Sasson [2], employs several schemes in order to minimize the effect of DoS attacks on a member.

One possible attack on this protocol is one in which a malicious (or a malfunctioning) process acts normally, but actually does not forward any useful messages, and replies to *pull* requests with null entries, thus affecting the performance of the protocol. In this project we suggest a failure detector for such a malfunction or attack and a way to overcome it.

Introduction

> "This Discourse, of human indifference, it's shouting out its urgently preparing for the worst, this conversation is at an end my brother, and this time the fear is kicking in, my enemy."
>
> - This Discourage. The Silent Attack

Gossip-Based Multicast Algorithms

As described in [1], *gossip-based multicast protocols* are a class of epidemiologic protocols, which have been introduced as an alternative to the "traditional" reliable multicast protocols. The main motivation is to trade the reliability guarantees offered by costly deterministic protocols against probabilistic reliability guarantees, but in return obtain very good scalability and fault-tolerance properties. The reliability of gossip-based protocols suffers lightly as more processes fail. Furthermore, these algorithms are adaptable, meaning that they support dynamic addition and removal of group members and are also relatively easy to implement and deploy.

Decentralization is the key concept underlying the scalability properties of gossip-based broadcast protocols. In contrast to sender-reliable protocols or receiver-reliable protocols, gossip-based multicast protocols are part of the class of peer-to-peer protocols. While retransmission requests in traditional algorithms can be handled by any process but lead to the re-broadcasting of a message, gossip-based protocols rely on interaction between peers.

In typical gossip-based algorithms, messages are disseminated by having every process periodically exchange information with a randomly chosen subset of processes inside the system (*view*). In each gossip-round, a process may send messages to the processes in its view (*push*-based protocols) and may also request messages from processes in the

[1] badishi@techunix.technion.ac.il
[2] aranb@techunix.technion.ac.il
[3] nadavl@techunix.technion.ac.il
[4] zigi@techunix.technion.ac.il