Brief Announcement: 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

Categories and Subject Descriptors: C.2.4 [COMPUTER-COMMUNICATION NETWORKS]: Distributed Systems

General Terms: Reliability, Algorithms

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. As a first defense, one may protect a system against DoS attacks using network-level mechanisms. However, network-level filters cannot detect DoS attacks at the application level, when the traffic seems legitimate.

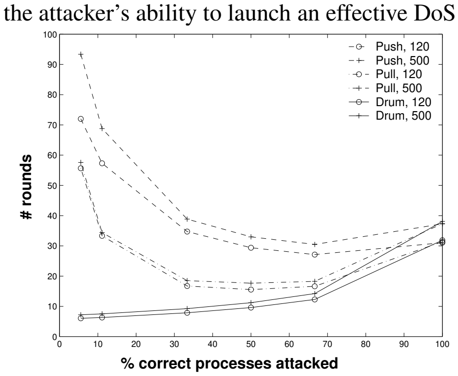
A DoS attack targeting every process in a large system inevitably causes performance degradation, but also requires vast resources. In order to be effective even with limited resources, attackers target vulnerable parts of the system. Hence, eliminating single points of failure is essential when constructing protocols that are less vulnerable to DoS attacks. We focus on gossip-based (epidemic) multicast protocols, which are robust and are known to provide graceful degradation in the face of amounting failures. One may expect that such a system will not be vulnerable to DoS attacks, as it is still effective when many processes fail. Surprisingly, we show that gossip-based protocols can be extremely vulnerable to DoS attacks targeted at a small subset of the processes, since an attacker can effectively isolate a small set of processes from the rest of the group.

To quantify the effects of DoS attacks, we measure their influence on message propagation time and throughput using asymptotic analysis, simulations, and measurements [1].

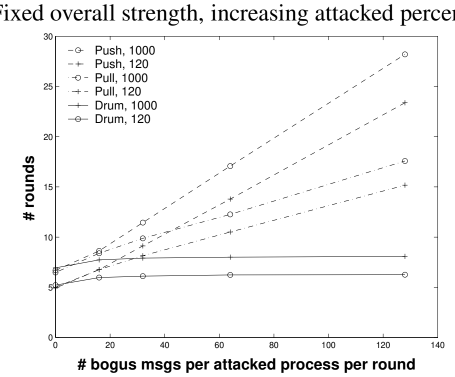
Drum

We next turn to design a protocol that will eliminate vulnerabilities to DoS attacks, i.e., that would not allow an attacker to increase the damage it causes by focusing on a subset of the processes. We are not familiar with any previous protocol that achieves this goal.

We present *Drum* (DoS-Resistant Unforgeable Multicast) [1], a gossip-based multicast protocol, which uses simple ideas to eliminate common vulnerabilities to DoS attacks. Drum uses both the push and pull gossiping techniques in order to resist DoS attacks. Processes attacked via push can still receive messages using pull, and vice versa. In order to realize this, resources are separated and bounded for each operation. Thus, using push does not affect the ability to utilize the pull channels, and vice versa. Finally, well-known ports are only used for communicating control messages, while data messages are sent to random ports in order to further decrease the attacker's ability to launch an effective DoS attack.



(a) Fixed overall strength, increasing attacked percentage.



(b) Fixed attacked percentage, increasing strength.

Figure 1: Average propagation time (simulations).

Evaluation

We show that Drum indeed achieves our design goal: when an adversary has a large sending capacity, its most effective attack against Drum is one that distributes the attacking power as broadly as possible, as illustrated in Figure 1(a). Obviously, performance degradation due to a powerful broad DoS attack is unavoidable for any multicast protocol, and indeed all the tested protocols exhibit the same performance degradation under such an attack.

Additionally, our results show that Drum can withstand severe DoS attacks, where naïve protocols that do not take any measures against DoS attacks completely collapse. E.g., under an attack that focuses on 10% of the processes, Drum's latency and throughput remain *constant* as the attack strength increases, whereas in traditional protocols, the latency grows *linearly* with the attack strength, as can be seen in the simulation results depicted in Figure 1(b).

REFERENCES

[1] G. Badishi, I. Keidar, and A. Sasson. Exposing and eliminating vulnerabilities to denial of service attacks in secure gossip-based multicast. DSN 2004.

PODC'04, July 25–28, 2004, St. John's, Newfoundland, Canada.
ACM 1-58113-802-4/04/0007.