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.

We therefore focus on gossip-based (epidemic) multicast protocols [7, 1, 8, 12, 15, 16, 14], which eliminate single points of failure using redundancy and random choices. Such protocols are robust and have been shown to provide graceful degradation in the face of amounting failures [13, 17]. One may expect that such a system will not suffer from vulnerabilities to DoS attacks, since it can continue to be 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. This occurs because an attacker can effectively isolate a small set of processes from the rest of the group by attacking this set.

To quantify the effects of DoS attacks, we measure their influence on the time it takes to propagate a message to all the processes in the system, as well as on the average throughput processes can receive. We do this using asymptotic analysis, simulations, and measurements.

Having observed the vulnerabilities of traditional protocols, we turn to search for a protocol that will eliminate these vulnerabilities. Specifically, our goal is to design a protocol 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 are familiar with only one previous work, by Minsky and Schneider [22], that deals with DoS attacks on a gossip-based protocol. However, the problem they consider differs from ours in a way that renders their approach inapplicable to our setting (see Section 2), and moreover, they only deal with limited attack strengths.

We present *Drum* (DoS-Resistant Unforgeable Multicast), a gossip-based multicast protocol, which, using a few simple ideas, eliminates common vulnerabilities to DoS attacks. Mathematical analysis and simulations show that Drum indeed achieves our design goal: an attacker cannot substantially hinder Drum's performance by targeting a small subset of the processes. When an adversary has a large sending capacity, its most effective attack against Drum is an all-out attack that distributes the attacking power as broadly as possible. (We concentrate on heavy attacks since they are most damaging, and one can expect them to happen in actual scenarios [28].) Obviously, performance degradation due to a broad all-out DDoS attack is unavoidable for any multicast protocol, and indeed all the tested protocols exhibit the same performance degradation under such a broad attack.

We have implemented Drum in Java and tested it on a on a cluster of workstations. Our measurements validate the analysis and simulation results, and 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, and the throughput continuously degrades.

In summary, this paper makes the following contributions:

- It presents a new framework and methodology for quantifying the effects of DoS attacks. We are not familiar with any previously suggested metrics for DoS-resistance nor with previous attempts to quantify the effect of DoS attacks on a system.
- It uses the new methodology to conduct the first systematic study of the impact of DoS attacks on multicast protocols. This study exposes vulnerabilities in traditional gossip-based protocols.
- It presents Drum, a simple gossip-based multicast protocol that eliminates such vulnerabilities. We believe that the ideas used in Drum can serve to mitigate the effect of DoS attacks on other protocols as well.
- It provides closed-form asymptotic analysis as well as simulations and measurements of gossip-based multicast protocols under DoS attacks varying in strength and extent.

This paper proceeds as follows: Section 2 gives background on gossip-based multicast and related work. Section 3 presents the system model. Section 4 describes Drum. Section 5 presents our evaluation methodology and considered attack models. The following three sections evaluate Drum and compare it to traditional gossip-based protocols using various tools: Section 6 gives closed-form asymptotic latency bounds; Section 7 provides a thorough evaluation using simulations; and Section 8 presents actual latency and throughput measurements. Section 9 evaluates the usefulness of other DoS-mitigation techniques used in Drum. Section 10 overviews a dynamic membership protocol that can be used along with Drum. Section 11 concludes. Appendix A contains some derivations for the asymptotic analysis. Appendix C provides detailed numerical analysis and compares it with the simulation results.

2 Background and Related Work

Gossip-based dissemination [7] is a leading approach in the design of scalable reliable application-level multicast protocols, e.g., [1, 8, 12, 15, 16, 14]. Our work focuses on symmetric gossip-based multicast protocols like lpbcast [8], that do not rely on external mechanisms such as IP multicast.

Such protocols work roughly as follows: Each process locally divides its time into *gossip rounds*; rounds are not synchronized among the processes. In each round, the process randomly selects a small number of processes to gossip with, and tries to exchange information with them. Every piece of information is gossiped for a number of rounds. It has been shown that the propagation time of gossip protocols increases logarithmically with the number of processes [25, 14]. There are two methods for information dissemination: (1) *push*, in which the process sends messages to randomly selected processes; and (2) *pull*, in which the process requests messages from randomly selected processes. Both methods are susceptible to DoS attacks: attacking the incoming push channels of a process may prevent it from receiving valid messages, and attacking a process's incoming pull channels may prevent it from sending messages to valid targets. Some protocols use both methods [7, 14]. Karp et al. showed that combining push and pull allows the use of fewer transmissions to ensure data arrival to all group members [14].

Drum utilizes both methods, and in addition, allocates a bounded amount of resources for each operation (push and pull), so that a DoS attack on one operation does not hamper the other. Such a resource separation approach was also used in COCA [33], for the sake of overcoming DoS attacks on authentication servers. Drum further utilizes randomly selected ports for data transmission, thus making it difficult for an attacker to target these ports. Note that Drum deals with DoS attacks at the application-level, assuming network-level defenses are already in place. Network-level DoS analysis and mitigation has been extensively dealt with [27, 3, 9, 30, 4, 26] but DoS-resistance at the secure multicast service layer has gotten little attention.

Secure gossip-based dissemination protocols were suggested by Malkhi et al. [19, 20, 21]. However, they did not deal with DoS attacks. Follow-up work by Minsky and Schneider [22] suggested a pull-based protocol that can endure limited DoS attacks by bounding the number of accepted requests per round. However, these works solve the *diffusion* problem, in which each message simultaneously originates at more than t correct processes, where up to t processes may suffer Byzantine failures. In contrast, we consider a multicast system where a message originates at a single source. Hence, using a pull-based solution as suggested in [22] does not help in withstanding DoS attacks. Moreover, Minsky and Schneider [22] focus on load rather than DoS attacks; they include only a brief analysis of DoS attacks, under the assumption that no more than t processes perform the attack, and that each of them generates a single message per round (the reception bound is also assumed to be one message per round). In contrast, we focus on substantially more severe attacks, and study how system performance degrades as the attack strength increases.

Here, we focus on DoS attacks in which the attacker sends fabricated application messages. DoS can also be caused by churn, where processes rapidly join and leave [18], thus reducing availability. In Drum, as in other gossip-based protocols, churn has little effect on availability: even when as many as half the processes fail, such protocols can continue to deliver messages reliably and with good quality of service [17]. A DoS attack of another form can be caused by process perturbations, whereby some processes are intermittently unresponsive. The effect of perturbations is analyzed in [1], where it is shown that probabilistic protocols, e.g., gossip-based protocols, solve this problem. We note that our work is the first that we know of that conducts a systematic study of the effect of DoS attacks on message latency.

3 System Model

Drum supports probabilistically reliable multicast [1, 8, 14] among processes that are members of a group. Each message is created by exactly one group member (its *source*). Throughout most of this paper we assume that the multicast group is static. Section 10 suggests a possible solution for dealing with a dynamic group membership.

Like previous gossip protocols [1, 8], we assume that the underlying network is fully-connected. There are no bounds on message delays, i.e., the communication is asynchronous. The link-loss probability is constant, equal for all links, and independent of any other factor. The communication channels are insecure, meaning that senders of incoming messages cannot be reliably identified in a simple manner. However, the data messages' sources (originators) can be identified using standard cryptographic techniques, e.g., [24]. Additionally, some information intended for a specific process may be encrypted using, e.g., a public-key infrastructure.

An adversary can generate fabricated messages and snoop on messages. However, these operations require the adversary to utilize resources. Malicious processes perform DoS attacks on group members. In case these malicious processes are part of the group, they also refrain from forwarding legitimate messages.

We assume that a DoS attack that does not specifically target the random ports does not affect the reception on these port (i.e., the application-level DoS attack does not cause a network-level DoS attack as well).

4 DoS-Resistant Gossip-Based Multicast Protocol

Drum is a simple gossip protocol, which achieves DoS-resistance using a combination of pull and push operations, separate resource bounds for different operations, and the use of random ports in order to reduce the chance of a port being attacked. Each process, p, locally divides its time into rounds. The rounds are not synchronized among the processes. A round is typically in the order of a second, and its duration may vary according to local random choices. Process p holds a list of other processes in the group (maintained by the membership service). Every round, p chooses two small (constant size) random sets of processes from this list, $view_{push}$ and $view_{pull}$, and gossips with them. E.g., when these views consist of two processes each, this corresponds to a combined fan-out of four. In addition, p maintains a message buffer. Process p performs the following operations in each round:

- *Pull-request* – p sends a digest of the messages it has received to the processes in its $view_{pull}$, requesting missing messages. Pull-request messages are sent to a well-known port. The pull-request specifies a randomly selected port on which p will await responses, and p spawns a thread for listening on the chosen port. This thread is terminated after a few rounds.

- *Pull-reply* – in response to pull-request messages arriving on the well-known port, p randomly selects messages that it has and are missing from the received digests, and sends them to the destinations indicated in the requests.
- *Push* – in a traditional push operation, p randomly picks messages from its buffer, and sends them to each target t in its $view_{push}$. In order to avoid wasting bandwidth on messages that t already has, p instead requests t to reply with a message digest, as follows:

  1. p sends a *push-offer* to t, along with a random port on which it waits for a push-reply.
  2. t replies with a *push-reply* to p's random port, containing a digest of the messages t has, and a random port on which t waits for data messages.
  3. If p has messages that are missing from the digest, it chooses a random subset of these, and sends them back to t's randomly chosen port.

  The target process listens on a well-known port for push-offers.

The random ports transmitted during the push and pull operations are encrypted (e.g., using the recipient's public key), in order to prevent an adversary from discovering them. Thus, $|view_{push}| + |view_{pull}|$ encryptions are performed each time these ports are changed.

Upon receiving a new data message, either by push or in response to a pull-request, p first performs some sanity checks. If the message passes these checks, p delivers it to the application and saves it in its message buffer for a number of rounds.

Resource allocation and bounds. In each round, p sends push-offers to all the processes in its $view_{push}$ and pull-requests to all the processes in its $view_{pull}$. If the total number of push-replies and pull-requests that arrive in a round exceeds p's sending capacity, then p equally divides its capacity between sending responses to push-replies and to pull-requests. Likewise, p responds to a bounded number (typically $|view_{push}|$) of push-offers in a round, and if more data messages than it can handle arrive, then p divides its capability for processing incoming data messages equally between messages arriving in response to pull-requests and those arriving in response to push-replies.

At the end of each round, p discards all unread messages from its incoming message buffers. This is important, especially in the presence of DoS attacks, as an attacker can send more messages than p can handle in a round. Since rounds are locally controlled and randomly vary in duration, the attacker cannot "aim" its messages for the beginning of a round. Thus, a bogus message has an equal likelihood of being discarded at the end of the round as an authentic messages does.

Achieving DoS-resistance. We now explain how the combination of push, pull, random port selections, and resource bounds achieves resistance to targeted DoS attacks. A DoS attack can flood a port with fabricated messages. Since the number of messages accepted on each port in a round is bounded, the probability of successfully receiving a given valid message M in a given round is inversely proportional to the total number of messages arriving on the same port as M in that round. Thanks to the separate resource bounds, an attack on one port does not reduce the probability for receiving valid messages on other ports.

In order to prevent a process from *sending* its messages using a *push* operation, one must attack (flood) the push-offer targets, the ports where push-replies are awaited, or the ports where data messages are awaited. However, the push destinations are randomly chosen in each round, and the push-reply and data ports are randomly chosen and encrypted. Thus, the attacker has no way of predicting these choices.

Similarly, in order to prevent a process from *receiving* messages during a *pull* operation, one needs to target the destination of the pull-requests or the ports on which pull-replies arrive. However, the destinations and ports are randomly chosen and the ports are sent encrypted. Thus, using the push operation, Drum achieves resilience to targeted attacks aimed at preventing a process from *sending* messages, and using the pull operation, it withstands attacks that try to prevent a process from *receiving* messages.

5 Evaluation Methodology

The most important contribution of this paper is our thorough evaluation of the impact of various DoS attacks on gossip-based multicast protocols. In addition to examining the effect of DoS on Drum, we also measure the effectiveness of the DoS-mitigating techniques employed by it. We mostly concern ourselves with the benefits of combining both the push and pull methods. We evaluate three protocols: (i) Drum, (ii) *Push*, which uses only push operations, and (iii) *Pull*, which uses only pull operations. Pull and Push are implemented the same way Drum is, with the important measures of bounding the number of messages accepted in each round and using random ports. Thus, in comparing the three protocols, we study the effectiveness of combining push and pull operations under the assumption that these other measures are used. Following that, Section 9 evaluates the effectiveness of the other DoS-mitigation concepts, by comparing Drum's performance to two modified versions of Drum: without resource separation, and without using random ports.

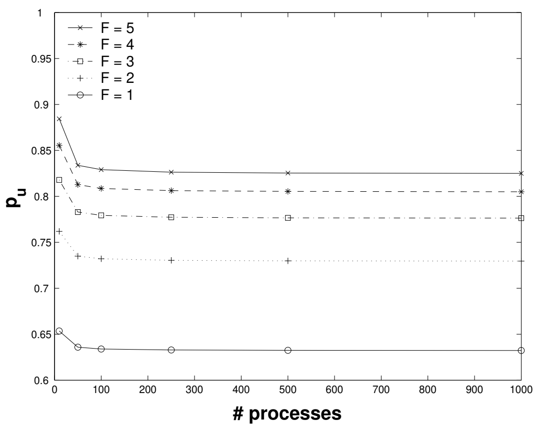
We begin by evaluating the effect that a range of DoS attacks have on message latency using asymptotic mathematical analysis (in Section 6) and simulations (in Section 7). Our simulation results exhibit the trends predicted by the analysis. In Appendix C, we also present detailed mathematical analysis, with results virtually identical to our simulations.

For these evaluations, we make some simplifying assumptions: We consider the propagation of a single message M, and assume that M is never purged from any process's message buffer. We do, however, assume that all the processes have messages other than M in their buffers, and thus all the processes gossip regardless of whether they have M or not. We also assume that when processes send a data message, they send the complete contents of their buffer in a single operation. We model the push operation as performed without push-offers (in Drum and in Push). We assume that the rounds are synchronized, and that the message-delivery latency is smaller than half the gossip period; thus, a process that sends a pull-request receives the pull-reply in the same round. We consider a static group of *n* processes, and assume that every process has complete knowledge of all the other processes in the group. All of these assumptions were made in previous analyses of gossip-based protocols, e.g., [1, 8, 19, 22].

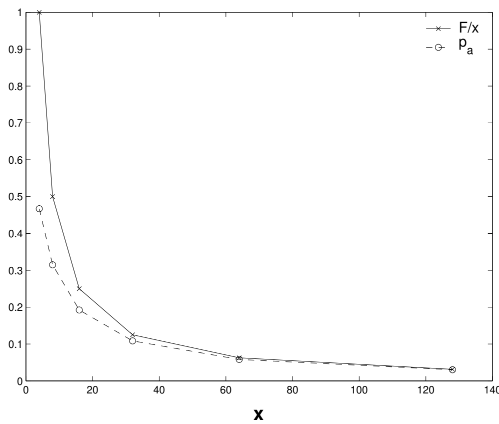
The analysis and simulations measure latency in terms of gossip rounds: we measure M's *propagation time*, which is the expected number of rounds it takes a given protocol to propagate *M* to all (in the closed-form analysis) or to 99% (in the simulations) of the correct processes. We chose a threshold of 99% since *M* may fail to reach some of the correct processes. Note that correct processes can be either attacked or non-attacked. In both cases, they should be able to send and receive dataa messages.

Finally, we turn to measure actual performance on a cluster of workstations (in Section 8). Our goal for this evaluation is twofold: First, we wish to ensure that the simplifying assumptions made in the analysis and simulations have little impact on their results. E.g., in the implementation, rounds are not synchronized and the push-offer mechanism is used (in Drum and in Push). Second, we seek to measure the consequences of DoS attacks not only on actual latency (in msecs.), but also on the throughput of a real system, where multiple messages are sent, and old messages are purged from processes' message buffers.

Attacks. In all of our evaluations, we stage various DoS attacks. In each attack, the adversary focuses on a fraction α of the processes ($0 < \alpha \leq 1$), and sends each of them x fabricated messages per round (in Drum, this means $\frac{x}{2}$ push messages and $\frac{x}{2}$ pull-requests). We denote the total attack strength by $B = x \cdot \alpha \cdot n$. We



(a) p_u as a function of n, for various fan-outs.



(b) p_a vs. $\frac{F}{x}$ for $F = 4$, $n = 1000$.

Figure 1: Actual values of p_u and p_a.

assume that the message source is being attacked (this has no impact on the results of Push). We consider attacks either of a *fixed strength*, where B is fixed and α increases (thus, x decreases); or of *increasing strength*, where either x is fixed and α increases, or vice versa (in both cases, B increases). Examining fixed strength attacks allows us to identify protocol vulnerabilities, e.g., whether an adversary can benefit from targeting a subset of the processes. Increasing strength attacks enable us to assess the protocols' performance degradation due to an increasing attack intensity.

6 Asymptotic Closed-Form Analysis

To simplify the analysis, in this section we assume that all the processes are correct and the DoS attack is launched from outside the system. The protocols use a constant fan-out, F. Every round, each process sends a data message to F processes and accepts data messages from at most F processes. In Drum, F is equally divided between push and pull, e.g., if $F = 4$, then $view_{push} = view_{pull} = 2$, and each process accepts push messages from at most 2 processes and pull-request messages from at most 2 processes in a round. We analyze Drum in Section 6.1, Push in Section 6.2, and Pull in Section 6.3

We denote by p_u the probability of a non-attacked process to accept a valid incoming push or pull-request message sent to it. Similarly, we denote by p_a the probability of an attacked process to accept a valid incoming message. Obviously, p_u is independent of the attack strength. In Appendix A, we give detailed formulas for p_a and p_u, and Lemma 8 shows that $p_u > 0.6$ for all $F \geq 3$. In fact, an exact calculation using the formula in Appendix A shows that $p_u > 0.6$ for all $F \geq 1$, as can be seen in Figure 1(a). Since an attacked process is sent at least x messages in a round, and accepts at most F of them, we get the following coarse bound: $p_a < \frac{F}{x}$. Figure 1(b) shows an example of the numerical calculation of p_a versus $\frac{F}{x}$.

6.1 Drum

We define the *effective expected fan-in*, *I*, to be the average number of valid data messages a process successfully receives in a round. (If the same data message is received from k processes, we count this as k messages.) Likewise, the *effective expected fan-out*, *O*, is the average number of messages that a process sends and are successfully received by their targets in a round.

Let us examine the effect of a DoS attack on O and I, with respect to the push operation (O_{push} and I_{push}, resp.). The probability of an attacked process to receive a push message is p_a. The probability of a non-attacked process to receive a push message is p_u. Therefore, the effective fan-ins I^a_{push} and I^u_{push} of an attacked and non-attacked process (resp.) are:

$$I^a_{push} = F \cdot p_a \quad \text{and} \quad I^u_{push} = F \cdot p_u \tag{1}$$

When αn processes are attacked, the effective fan-outs are:

$$O^a_{push} = O^u_{push} = F \cdot (\alpha \cdot p_a + (1-\alpha) \cdot p_u) \tag{2}$$

Similar arguments apply for the pull opertaion. The probability of an attacked process to receive a pull-request is p_a. The same probability for a non-attacked process is p_u. Receiving pull-requests allows a process to send data messages, and on average, each process receives F pull-requests. Due to the use of random ports, we can assume that each pull-reply is actually being received, and thus, the effective fan-outs are:

$$O^a_{pull} = \quad F \cdot p_a \quad \text{and} \qquad O^u_{pull} = F \cdot p_u \tag{3}$$

$$\tag{4}$$

Receiving data messages requires sending pull-requests. Each round, F pull-requests are being sent. On average, αF of them reach an attacked process and are successfully read with probability p_a, and $(1-\alpha)F$ of those reach a non-attacked process and are succesfully read with probability p_u. Due to the use of random ports, we can assume it makes no difference whether the requesting process is attacked or not. We get the following fan-ins:

$$I^a_{pull} = \quad I^u_{pull} = \quad F \cdot (\alpha \cdot p_a + (1-\alpha) \cdot p_u) \tag{5}$$

In Drum, $O = \frac{1}{2}(O_{push} + O_{pull})$ and $I = \frac{1}{2}(I_{push} + I_{pull})$. Therefore:

$$O^a = I^a = \quad \tfrac{F}{2} \cdot (\alpha \cdot p_a + (1-\alpha)p_u + p_a) \quad = F \cdot (\frac{\alpha+1}{2} \cdot p_a + \frac{1-\alpha}{2} \cdot p_u) \tag{6}$$

$$O^u = I^u = \quad \tfrac{F}{2} \cdot (\alpha \cdot p_a + (1-\alpha)p_u + p_u) \quad = F \cdot (\frac{\alpha}{2} \cdot p_a + \frac{2-\alpha}{2} \cdot p_u) \tag{7}$$

We begin by considering increasing strength attacks. We show that in Drum, an adversary does not gain any significant advantage by increasing its attack strength while focusing on a fixed strict subset of the processes.

Lemma 1. *Fix $\alpha < 1$ and n. Drum's expected propagation time is bounded from above by a constant independent of x.*

Proof. From Equations (6) and (7) we get that for all x, $O^a = I^a > F \cdot \frac{1-\alpha}{2} \cdot p_u$, and $O^u = I^u > F \cdot \frac{2-\alpha}{2} \cdot p_u$. Since p_u is independent of x, and $\alpha < 1$ is fixed, the effective fan-ins and fan-outs of *all* the processes are bounded from below by a constant independent of x. It has been shown that a constant fan-out and a constant group size entail a constant propagation time [25, 14]. Therefore, the propagation time is inevitably bounded from above by a constant independent of x. □

Figure 3(a) in Section 7.2 illustrates this quality of Drum, using simulations.

We now consider attacks where the adversary has a fixed attacking power. In this scenario, the attacker can intensely attack a small group of processes, or perform a moderate attack on a large number of processes. We would like to see which strategy is more beneficial to the attacker. We denote by $c = \frac{B}{F \cdot n} = \frac{\alpha x}{F}$ the attack strength divided by the total system capacity. We show that the adversary's best strategy against Drum is to attack as many processes as it can, i.e., increase α.

Lemma 2. *For $c > 5$, Drum's expected propagation time is monotonically increasing with α.*

Proof. We will show that all the processes' effective fan-ins and fan-outs are monotonically decreasing with α. That is, we want to prove that: $\frac{\mathrm{d}O^a}{\mathrm{d}\alpha} < 0$ and $\frac{\mathrm{d}O^u}{\mathrm{d}\alpha} < 0$. We require the following:

$$\frac{\mathrm{d}O^a}{\mathrm{d}\alpha} = \frac{\mathrm{d}I^a}{\mathrm{d}\alpha} = \frac{F}{2} \cdot \left(p_a + \alpha \frac{\mathrm{d}p_a}{\mathrm{d}\alpha} + \frac{\mathrm{d}p_a}{\mathrm{d}\alpha} - p_u\right) < 0$$
$$p_a + (\alpha+1)\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < p_u$$

Recall that $p_a < \frac{F}{x}$. In Lemma 7 in Appendix A we show that $\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < \frac{F}{\alpha x}$. Bounding the left side of the inequality, we get:

$$p_a + (\alpha+1)\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < \frac{F}{x} + (\alpha+1)\frac{F}{\alpha x} = \frac{F}{\alpha x} \cdot (\alpha + \alpha + 1) = \frac{2\alpha+1}{c} < \frac{3}{c}$$

Thus, our condition holds when $\frac{3}{c} < p_u$, that is, when $c > \frac{3}{p_u}$. Similarly, for the second derivative we get the condition:

$$\frac{\mathrm{d}O^u}{\mathrm{d}\alpha} = \frac{\mathrm{d}I^u}{\mathrm{d}\alpha} = \frac{F}{2} \cdot \left(p_a + \alpha \frac{\mathrm{d}p_a}{\mathrm{d}\alpha} - p_u\right) < 0$$
$$p_a + \alpha\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < p_u$$

Bounding the left side of the inequality, we get:

$$p_a + \alpha\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < \frac{F}{x} + \alpha\frac{F}{\alpha x} = \frac{F}{\alpha x} \cdot (\alpha + \alpha) = \frac{2\alpha}{c} < \frac{2}{c}$$

Thus, we require that $\frac{2}{c} < p_u$, or that $c > \frac{2}{p_u}$. This is already inferred from our previous result. The lemma follows since $p_u > 0.6$. $\square$

This behavior is validated in the simulations in Section 7.3. Moreover, the simulations show that even for much smaller values of c (ranging from 0.25 to 2), Drum's propagation time increases with α (see Figures 7–8).

6.2 Push

We first prove the following simple lemma.

Lemma 3. $\forall a > 0 \quad a < \frac{1}{\ln(1+\frac{1}{a})} < a + 1.$

Proof. We show that $\forall y > 0 \quad \frac{1}{y} < \frac{1}{\ln(1+y)} < \frac{1}{y} + 1.$
Define $h(y) = \ln(1+y) - \frac{y}{1+y}$ and $g(y) = \ln(1+y) - y$. By taking derivatives we get:

$$h'(y) = \frac{1}{1+y} - \left(\frac{1}{1+y} - \frac{y}{(y+1)^2}\right) = \frac{y}{(y+1)^2} > 0, \ \ \forall y > 0,$$
$$g'(y) = \frac{1}{1+y} - 1 < 0, \ \ \forall y > 0.$$

Since $h(0) = g(0) = 0$, $y > \ln(1+y) > \frac{y}{(y+1)}$. Therefore, $\frac{1}{y} < \frac{1}{\ln(1+y)} < \frac{1}{y} + 1$. $\square$

We proceed to show that Push's propagation time is linear in x.

Lemma 4. *The expected propagation time to all processes in Push is bounded from below by:*

$$\frac{\ln n - \ln\left[(1-\alpha)\,n+1\right]}{\ln\left(1+F\alpha p_a\right)}$$

Proof. We prove that the given bound holds even for the case where initially all the non-attacked processes have *M*, in addition to the source (which is attacked). The lemma then follows immediately.

Let $M(k)$ denote the expected number of processes that have *M* at the beginning of round k. In round k, each process having M sends it to F other processes. On average, $F\alpha$ of those are attacked, and each attacked process receives the message with probability p_a. Thus, we get the coarse recursive bound $M(k+1) \leq M(k) + M(k)\cdot F\alpha p_a$ with the initial condition $M(0) = (1-\alpha)n+1$. Thus, $M(k) \leq \left[(1-\alpha)\,n+1\right]\left(1+F\alpha p_a\right)^k$. *M* reaches all the processes when $M(k) \geq n$. The first round number k that satisfies this inequality is the required formula. □

Corollary 1. *Fix α and $n > \frac{1}{\alpha}$. The propagation time of Push increases at least linearly with x.*

Proof. Since α and $n > \frac{1}{\alpha}$ are fixed, the numerator in Lemma 4 is a positive constant. Consider the denominator: since $p_a < \frac{F}{x}$, it holds that $F\cdot\alpha\cdot p_a$ is $O(\frac{1}{x})$. The lemma follows since, by Lemma 3, $\frac{1}{\ln(1+\frac{1}{x})}$ is $\theta(x)$. □

The above corollary explains the trend exhibited by Push in Figure 3(a).

6.3 Pull

We begin by proving the following lemma.

Lemma 5. $\forall b \in \mathbb{N}$ $\frac{x^b}{x^b-(x-F)^b}$ *is* $\Theta(x)$.

Proof. We first show that $\frac{a-1}{b} \leq \frac{a^b}{a^b-(a-1)^b} \leq \frac{a-1}{b}+1$ for every $a > 1$, $b \in \mathbb{N}$.

In order to prove the left inequality, we prove by induction on b that $\frac{b}{a-1} \geq \frac{a^b-(a-1)^b}{a^b}$.
For $b=1$, $\frac{1}{a-1} \geq \frac{1}{a}$ for every $a > 1$. The inductive Step: $\frac{a^{b+1}-(a-1)^{b+1}}{a^{b+1}} = \frac{a(a)^b-(a-1)(a-1)^b}{a(a)^b} = \frac{a^b}{a(a)^b} + \frac{a-1}{a}\frac{a^b-(a-1)^b}{a^b} \leq \frac{1}{a} + \frac{a-1}{a}\frac{b}{a-1} = \frac{1}{a}+\frac{b}{a} = \frac{b+1}{a} \leq \frac{b+1}{a-1}$.

Next, we prove that $\frac{a^b}{a^b-(a-1)^b} \leq \frac{a-1}{b}+1$, i.e., $\frac{(a-1)^b}{a^b-(a-1)^b} \leq \frac{a-1}{b}$. From the inequality $(a)^b \geq (a-1)^b + b(a-1)^{(b-1)}$, we get that $a^b-(a-1)^b \geq b(a-1)^{(b-1)}$. Hence, $\frac{(a-1)^b}{a^b-(a-1)^b} \leq \frac{(a-1)^b}{b(a-1)^{b-1}} = \frac{a-1}{b}$.

Therefore, $\frac{a-1}{b} \leq \frac{a^b}{a^b-(a-1)^b} \leq \frac{a-1}{b}+1$. By substituting $\frac{x}{F}$ for a in the last inequality, we get that $\frac{x-F}{bF} \leq \frac{x^b}{x^b-(x-F)^b} \leq \frac{x-F}{bF}+1$ for every $x > F$. Therefore, $\frac{x^b}{x^b-(x-F)^b}$ is $\Theta(x)$. □

We define $\widetilde{p}$ as probability that M is propagated from the source in a round.

Lemma 6. *Fix α and n. The number of rounds it takes a message to leave the source in Pull grows at least linearly with x.*

Proof. We give a gross over-estimate of $\widetilde{p}$ by assuming that all the other $n-1$ processes choose the source every round. (When fewer processes choose the source, M is *less* likely to leave the source.) Since $p_a < \frac{F}{x}$, $\widetilde{p} < (1 - (\frac{x-F}{x})^{n-1})$. The number of rounds it takes to propagate a message beyond the message source is geometrically distributed with $\widetilde{p}$. Therefore, its expectation is $\frac{1}{\widetilde{p}} > \frac{x^{n-1}}{x^{n-1}-(x-F)^{n-1}}$. Substituting $n-1$ for b in Lemma 5, we get that $\frac{1}{\widetilde{p}}$ is $\Omega(x)$. $\square$

Corollary 2. *Fix α and n. The propagation time of Pull grows at least linearly with x.*

Figure 3(a) illustrates this behavior of Pull.

7 Simulation Results

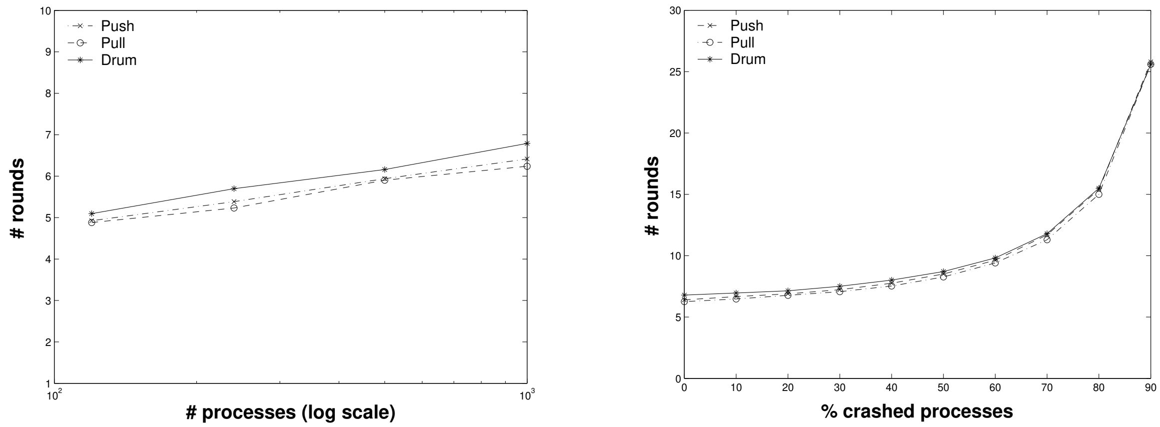
This section presents MATLAB simulations of the three protocols under various DoS attack scenarios. Only one of the group members is a source, with respect to the examined data message M. However, all the group members constantly have messages to send, even if they do not possess M. Each process receives messages from at most $F = 4$ other processes each round (disregarding pull-replies). If more than F processes try to access this process's incoming channels, a random F-sized subset of them is chosen. We consider a link-loss probability of 0.01 on all links and a fan-out of $F = 4$. Rounds are synchronized among all processes. Each data point is averaged over 1000 runs.

In Section 7.1 we consider situations with no DoS attack (either no failures or only crash failures), and validae known results about gossip protocols. We continue in Sections 7.2 and 7.3 by measuring the effect of DoS attacks on the system. In these studies, we assume that 10% of the processes are controlled by the adversary, perform a DoS attack on some correct processes, and do not propagate any valid messages. It is important to realize that the attacking processes do not attack each other, but the correct processes may choose to gossip with these malicious processes. In that case, the gossiped messages will be simply discarded by the attacking processes. We note that, according to our model, malicious group members performing a DoS attack are equivalent to group members suffering crash failures, and an externally-sourced DoS attack of the same strength. As Figure 2(b) shows, the protocols are highly robust to crash failures. Thus, controlling more group members does not grant the adversary with a significant advantage. We measure the propagation times to the correct processes, both attacked and non-attacked. In Section 7.2 we measure the impact of targeted DoS attacks, and in Section 7.3 we examine fixed strength attacks and adversary strategies.

7.1 Validating Known Results

We begin by evaluating the three protocols in a failure-free scenario, and in situations where crash failures occur. We assume that the crashes occur before M is generated, and that the source does not crash. We also assume that the crashes are not detected by the correct processes, i.e., they try to gossip with crashed processes as well.

Our aim is to validate two known results: (1) the propagation time of gossip-based multicast protocols is $O(\log n)$ [25, 14], as can be seen in Figure 2(a), with a logarithmic x-axis; and (2) the performance of such protocols degrades gracefully as crash failures amount [13, 17], as depicted in Figure 2(b)). We can see that Push and Pull slightly outperform Drum in these experiments. This is due to the fact that the bounds on the pull and push channels in Drum are strict, i.e., even if in a specific round no messages have arrived via the push channels, only requests from at most two distinct processes will be handled, although the process is capable of handling four such requests. Conversely, Push and Pull have only one bound, which guarantees

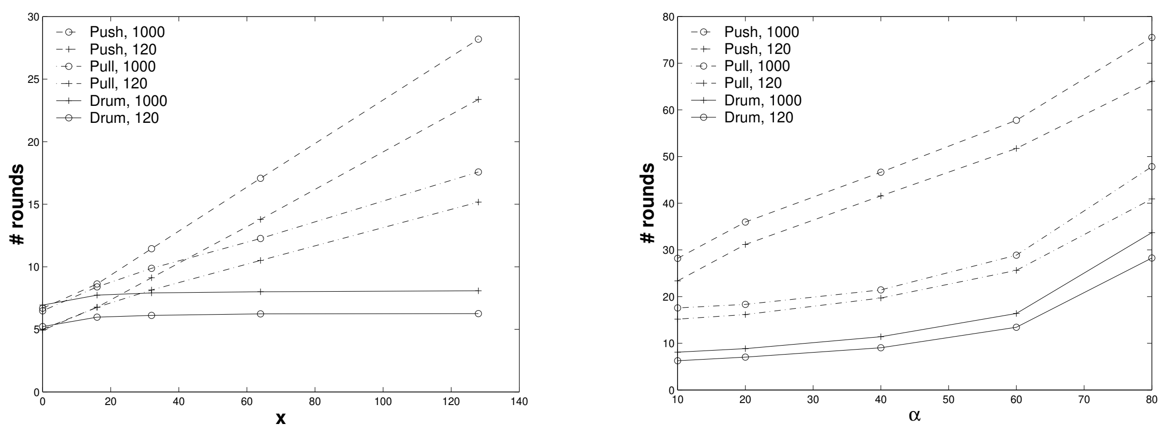


(a) Failure-free operation. (b) Operation with crashed processes, $n = 1000$.

Figure 2: Runs without DoS attack: Average propagation time to 99% of the correct processes (simulations).

that messages won't be discarded if they can be processed. The ability to perform well even when many processes crash stems from the random choice of communication partners each round.

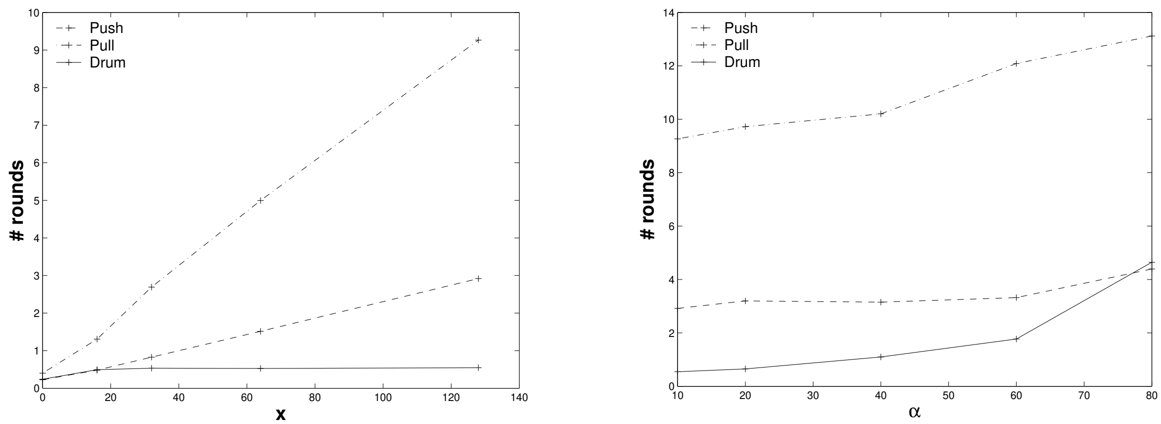
7.2 Targeted DoS Attacks



(a) $\alpha = 10\%$. (b) $x = 128$.

Figure 3: Increasing attack strength: Average propagation time to 99% of the correct processes, $n = 120, 1000$ (simulations).

In this section we consider targeted attacks, where a subset of size αn of the processes is attacked. Figure 3 compares the time it takes *M* to reach 99% of the correct processes for the three protocols under various DoS attacks, with 120 and 1000 processes. Figure 3(a) shows that when 10% of the processes are attacked, the propagation time of both Push and Pull increases linearly with the severity of the attack, while Drum's propagation time is unaffected by the attack strength. This is consistent with the prediction of Lemma 1 and Corollaries 1 and 2. Moreover, the three protocols perform virtually the same without DoS attacks (see the leftmost data point). Figure 3(b) illustrates the propagation time as the percentage of attacked processes (and thus B) increases. The rightmost data point in this figure matches a scenario where



(a) $\alpha = 10\%$. (b) $x = 128$.

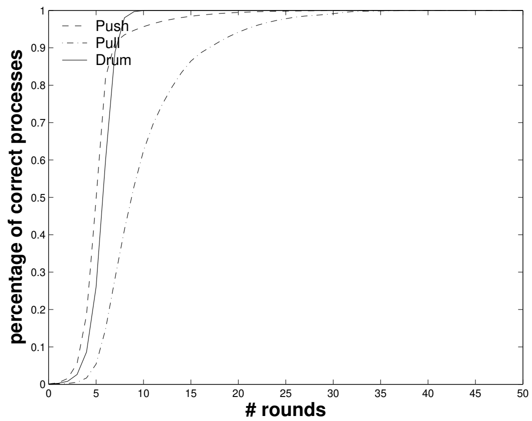
Figure 4: Increasing attack strength: STD of the propagation time to 99% of the correct processes, $n = 1000$ (simulations).

only 10% of the processes are both correct non-attacked. Although the protocols exhibit similar trends, Drum propagates messages much faster than Push and Pull.

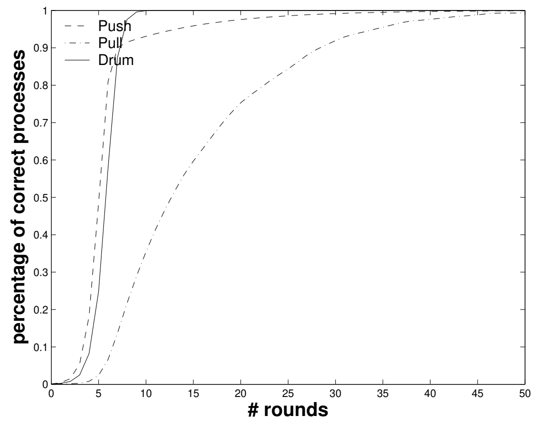
Figure 4 illustrates the *standard deviation* (STD) of the propagation times presented in Figure 3 for $n = 1000$. It shows that for a fixed α, Drum's STD is not affected by the attack strength, whereas the other protocols' STD increases linearly. Furthermore, both Drum and Push exhibit a small STD compared to Pull. E.g., for $\alpha = 10\%$ and $x = 128$, the STDs of Drum and Push are 0.5 and 2.9 rounds (resp.), whereas Pull's STD is 9.3 rounds. Therefore, the bahavior of Drum and Push is more predictable. The high STD of Pull's propagation time is mainly due to the large STD of the number of rounds it takes to propagate *M* beyond the source. The number of rounds it takes to propagate *M* beyond the source is geometrically distributed with $\widetilde{p}$, where $\widetilde{p}$ is the probability to propagate *M* beyond the source in a round. Thus, the STD number of rounds it takes to propagate *M* beyond the source is $\frac{\sqrt{1-\widetilde{p}}}{\widetilde{p}}$. A numerical calculation of $\widetilde{p}$ according to the formula in Appendix B , with $F = 4$ and $x = 128$ yields an STD of 8.17 rounds, which explains Pull's measured STD of 9.3 rounds mentioned above.

Figure 5 illustrates the cumulative distribution function (CDF) of the percentage of correct processes that receive *M* by a given round, under different DoS attacks. As expected, Push propagates *M* to the non-attacked processes very quickly, but takes much longer to propagate it to the attacked processes. Again, we see that Drum significantly outperforms both Push and Pull when a strict subset of the system is attacked.

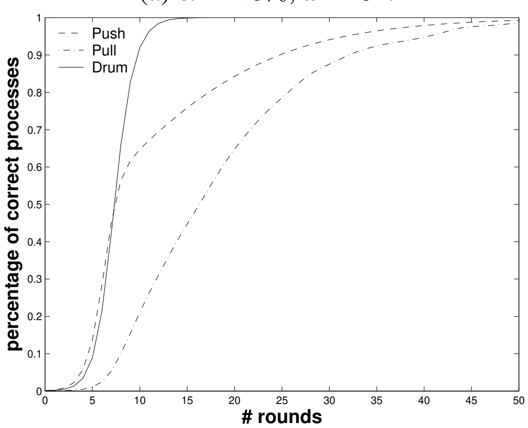
Interestingly, on average, Push propagates *M* to more processes per round than Pull does (see Figure 5), although the average number of rounds Pull takes to propagate M to 99% of the correct processes is smaller than that of Push (see Figure 3). This paradox occurs since, with Pull, there is a non-negligible probability that *M* is delayed at the source for a long time. With $F = 4$ and $x = 128$, the probability for *M* not being propagated beyond the source in 5, 10, and 15 rounds is 0.54, 0.3, and 0.16 resp. (as computed using the formula for $\widetilde{p}$ in Appendix B). Once M reaches one non-attacked process, it quickly propagates to the rest of the processes. Therefore, even if by a certain round k, in most runs, a large percentage of the processes have M, there is still a non-negligible number of runs in which Pull does not reach *any* process (other than the source) by round k. This large difference in the percentage of processes reached has a large impact on the average depicted in Figure 5. In contrast, Push, which reaches all the non-attacked processes quickly in all runs, does not have runs with such low percentages factoring into this average. Nevertheless, Push's average



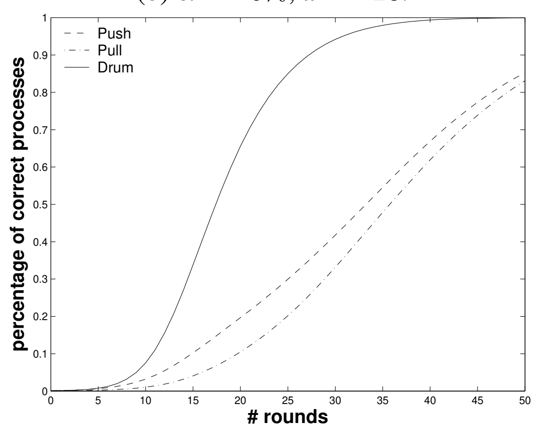
(a) $\alpha = 10\%$, $x = 64$.



(b) $\alpha = 10\%$, $x = 128$.



(c) $\alpha = 40\%$, $x = 128$.



(d) $\alpha = 80\%$, $x = 128$.

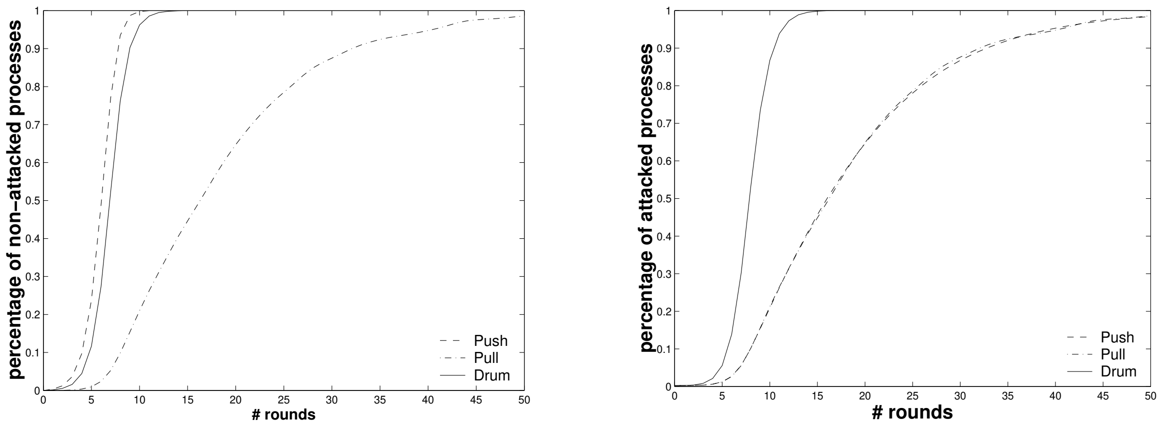
Figure 5: Targeted DoS attacks: CDF: Average percentage of correct processes that receive *M*, $n = 1000$ (simulations).

propagation time to 99% of the correct processes is much higher than Pull's, because Push has to propagate M to *all* the attacked processes, whereas Pull has to propagate M only out of one attacked process.

Figure 6 illustrates this behavior: Figure 6(a) shows that Push propagates M much faster than Pull to the non-attacked processes, while Figure 6(b) indicates that Push and Pull take the same time to propagate M to the attacked processes. Conversely, Drum exhibits fast propagation times both to attacked and non-attacked processes.

7.3 Adversary Strategies

We now evaluate the protocols under a range of attacks with fixed adversary strengths. First, we consider severe attack with $B = 7.2n$ and $B = 36n$ (corresponding to $c = 2$ and $c = 10$, resp.) fabricated messages per round. If the adversary chooses to attack all correct processes, it can send 8 (resp., 40) fabricated messages to each of them in each round, because 90% of the processes are correct. If the adversary instead focuses on 10% of the processes, it can send 72 (resp., 360) fabricated messages per round to each. Figure 7 illustrates the protocols' propagation times with different percentages of attacked processes, for system sizes of 120 and 500. It validates the prediction of Lemma 2, and shows that the most damaging adversary



(a) Non-attacked processes.

(b) Attacked processes.

Figure 6: Propagation to attacked vs. non-attacked processes: CDF: Average percentage of attacked versus non-attacked processes that receive *M*, $n = 1000$, $\alpha = 40\%$, $x = 128$ (simulations).

strategy against Drum is to attack all the correct processes. That is, an adversary cannot "benefit" from focusing its capacity on a small subset of the processes. In contrast, the performance of Push and Pull is seriously hampered when a small subset of the processes is targeted. Not surprisingly, the three protocols perform equally when all correct processes are targeted (see the rightmost data point).

Next, we evaluate Drum under attacks with relatively small adversary powers of $B = 0.9n$, $B = 1.8n$ and $B = 3.6n$ ($c = 0.25$, $c = 0.5$, and $c = 1$, resp.) and also without an attack (as a baseline). As Figure 8 shows, such attacks have little impact on Drum's propagation time.

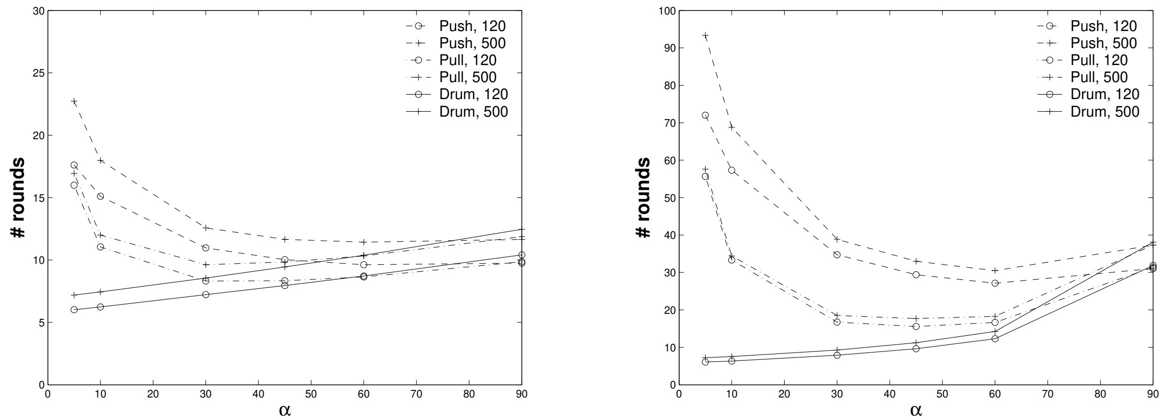
8 Implementation and Measurements

We have implemented Drum, Push, and Pull in Java. The implementations are multithreaded. The operations that occur in a round are not synchronized, e.g., one process might send messages before trying to receive messages in that round, while another might first receive a new message, and then propagate it. We run our experiments on 50 machines at the Emulab testbed [32], on a 100Mbit LAN, where a single process is run on each machine (i.e., $n = 50$). As in the simulations, we designate 10% of the processes as malicious – they do not propagate any messages, and instead perform DoS attacks only on correct processes.

8.1 Validating the Simulation Methodology

Our first goal for these experiments is to validate the simulation methodology. To this end, we experiment with the same settings that were tested in Section 7, first for increasing values of x and $\alpha = 10\%$, and then for $x = 128$ and increasing values of α. As in the simulations, we track the propagation a single data message M, where every process has messages to send, even if it does not hold M. Each data point is averaged over 1000 runs.

Due to the lack of synchronization, messages can be propagated multiple hops in a single round in some situations. We use the following method to count the number of rounds it takes to propagate a message: when a message is created, a round counter is attached to it and initialized to 0. The message source logs the value 0, and immediately increases the round counter to 1. Whenever a process receives a new message,



(a) $B = 7.2n$ ($c = 2$). (b) $B = 36n$ ($c = 10$).

Figure 7: Strong fixed strength attacks: Average propagation time to 99% of the correct processes (simulations).

it logs the message's current round counter. Every round, each process increments the round counters of all the messages in its local buffer.

Figure 9 depicts the results of these experiments, and compares them with the corresponding simulation results. It shows that the experimental results are consistent with the simulation results, indicating that the simplifying assumptions made in the analysis and simulations have negligible effect on the results.

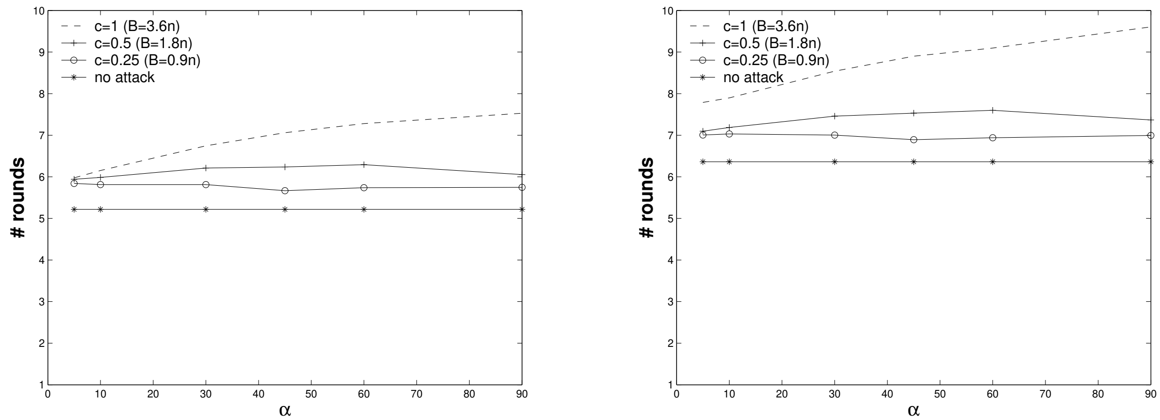
8.2 High Throughput Experiments

We proceed to evaluate the protocols in a realistic setting, where multiple messages are sent, and old messages are purged from processes' buffers. By running on a real network, we can faithfully evaluate latency in milliseconds (instead of rounds), as well as throughput.

In each experiment scenario, a total of $10,000$ messages are sent by a single source, at a rate of 40 messages per second. The average received throughput and latency are measured at the remaining 44 correct processes (recall that 5 of the 50 processes are faulty). The average throughput is calculated ignoring the first and last 5% of the time of each experiment. The round duration is 1 second. Data messages are 50 bytes long. (The evaluation in [8] used a similar transmission rate and similar message sizes.)

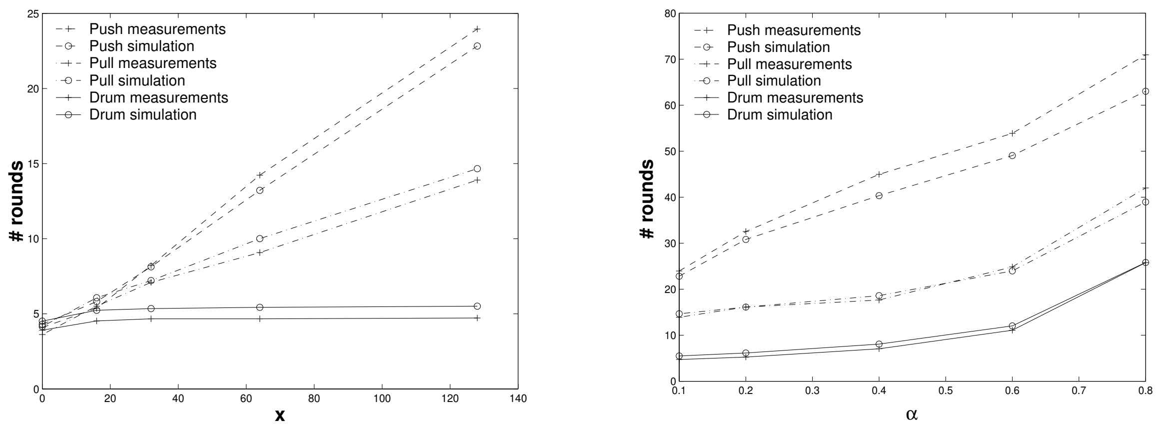
In a practical system, messages cannot reside in local buffers forever, nor can a process send all the messages it ever received in a single round. In our experiments, messages are purged from processes' buffers after 10 rounds, and each process sends at most 80 randomly chosen *new* messages to each of its gossip partners in a round. These are roughly twice the buffer size and sending rate required for the throughput of 40 messages per round in an ideal attack-free setting, since the propagation time in the absence of attacks is about 5 rounds. Due to purging, some messages may fail to reach all the processes. Since we measure throughput at the receiving end, this is reflected by an average throughput lower than the transmission rate (of 40 messages per second).

Figure 10 shows the throughput at the receiving processes for Drum, Push, and Pull, under the same DoS attack scenarios staged above. Figure 10(a) indicates that, as for latency, Drum's throughput is also unaffected by increasing x, while Push shows a slight degradation of throughput, and Pull's throughput decreases dramatically. Figure 10(b) shows that Drum's throughput gracefully degrades as α increases, while Push exhibits a linear degradation, and Pull's throughput is drastically affected for every $\alpha > 0$.



(a) $n = 120$. (b) $n = 500$.

Figure 8: Weak fixed strength attacks: Drum, average propagation time to 99% of the correct processes (simulations).



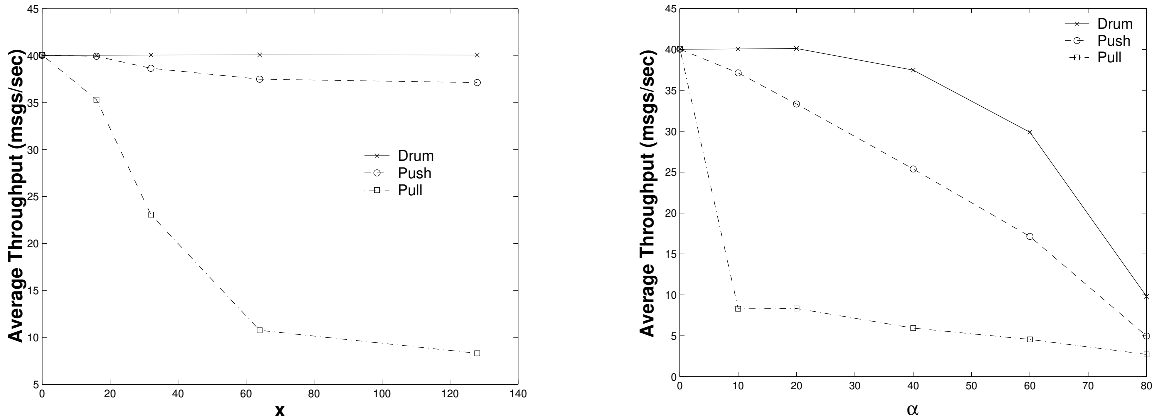
(a) $\alpha = 10\%$. (b) $x = 128$.

Figure 9: Simulations vs. measurements: Average propagation time to 99% of the correct processes, $n = 50$.

Figure 11 depicts the CDF of the average latency of *successfully received* messages in two scenarios. Each data point shows, for a given latency l, the percentage of correct processes for which the average latency does not exceed l. We observe that Push is the fastest in delivering messages to non-attacked processes, but suffers from substantial variation in delivery latency, as messages take a long time to reach the attacked processes. E.g., Figure 11(a) shows that the 4 attacked processes (other than the source) measure an average latency 4 times longer than non-attacked processes. While Pull exhibits almost the same average latency for all the processes, this latency is very long. Drum combines the best of Push and Pull: it delivers messages almost as fast as Push, while maintaining a small variation between attacked and non-attacked processes.

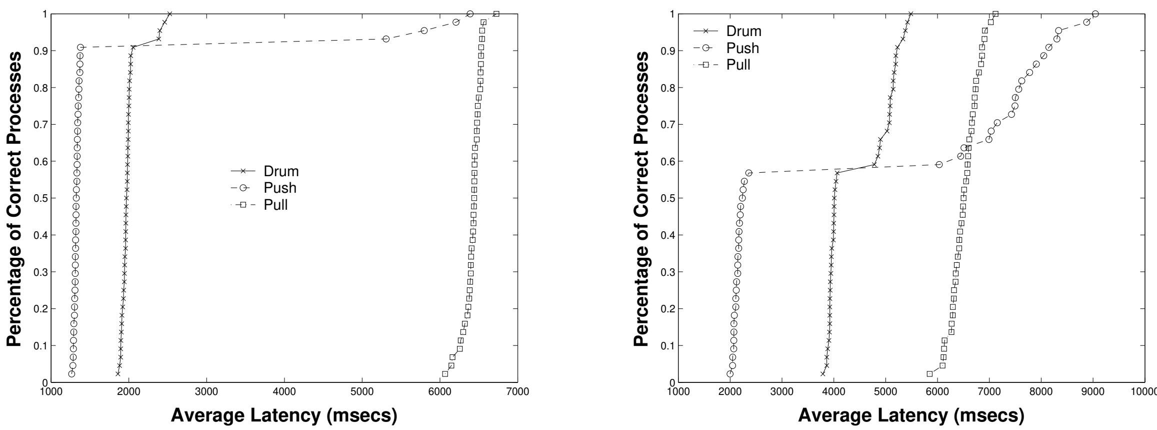
9 Other DoS-Mitigation Methods

Until now, we have evaluated the advantage of combining both the push and pull techniques as a way to mitigate DoS attacks. We now turn to examine the importance of using the other two techniques: utilizing



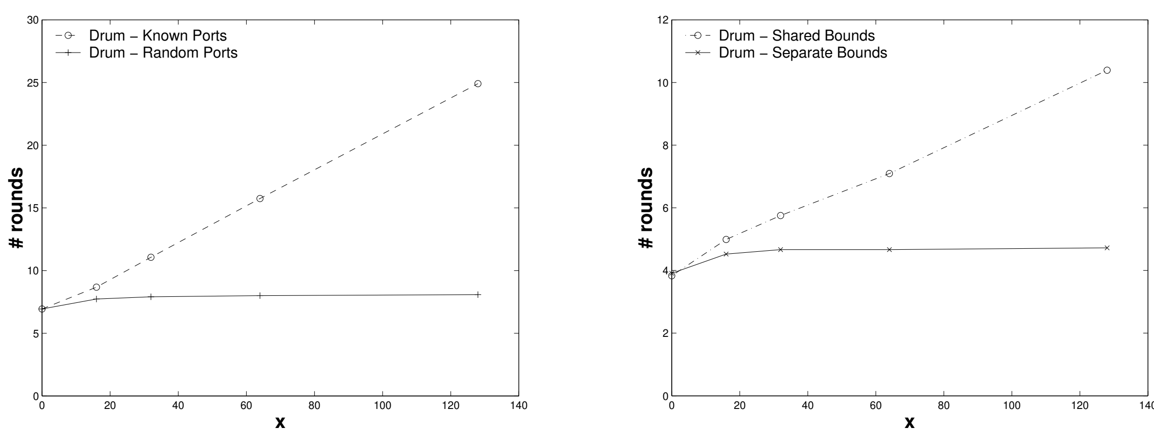
(a) $\alpha = 10\%$.　　(b) $x = 128$.

Figure 10: Increasing attack strength: Average received throughput (measurements).



(a) $\alpha = 10\%$, $x = 128$.　　(b) $\alpha = 40\%$, $x = 128$.

Figure 11: CDF: average latency of received messages (measurements).



(a) $\alpha = 10\%$, $n = 1000$ (simulations).　　(b) $\alpha = 10\%$, $n = 50$ (measurements).

Figure 12: The effect of DoS-mitigation methods on Drum's performance.

random ports whenever possible, and allocating separate resources for orthogonal operations.

In order to evaluate the effectiveness of random ports, we simulate Drum as described in Section 7, with the difference that pull-replies are sent to a well-known port instead of to a random one. The adversary attacks this port by equally dividing its attack strength for the pull channels between the pull-request port and the pull-reply port (i.e., each pull port is attacked with a quarter of the total attack strength). Figure 12(a) presents simulation results comparing Drum's performance with and without the use of random ports, when 10% of the processes are attacked. The results show a linear increase in propagation time for the well-known ports variation of Drum, as the rate of bogus messages each attacked process receives in a round increases. This is in contrast to the propagation time of Drum using random ports, which is bounded by a constant.

When solely using well-known ports, the adversary can attack both pull ports, as well as the push port. A process under attack experiences difficulty receiving messages both via push and through the pull channels, since the push and pull-reply ports are attacked. The same process's ability to send messages is only partly hampered. Although the pull-request port is attacked, the adversary cannot directly affect the process's outgoing push channels.

Next, we measure the effect of resource separation on Drum's performance. To this end, we change Drum's implementation detailed in Section 8. Resources are now combined (i.e., a joint bound on the maximum number of processed messages per round is used) for receiving control messages: pull-requests, push-offers, and push-replies. We do not include the reception of data messages in this bound, since this bound may differ greatly from the bound on control messages in actual scenarios. Figure 12(b) contrasts the measurements of Drum's propagation time with shared bounds against those with separate bounds, when 10% of the processes are attacked. The results indicate a linear degradation of performance as the attack rate increases, when bounds are shared. On the other hand, the unmodified version of Drum is virtually indifferent to the increase in attack strength.

Shared bounds degrade Drum's performance under a DoS attack, since the fabricated control messages sent by the adversary to the well-known push-offer and pull-request ports consume resources that should be used for reading pull-requests, push-offers, and push-replies. The valid control messages are then discarded when resources are exhausted, and the attacked process becomes less responsive.

We conclude that random ports and separate resource bounds are crucial to Drum's ability to cope with DoS attacks.

10 Dynamic Membership

Our analysis and implementation of Drum until this point assumed that the multicast group is composed of a static set of processes. This assumption is in accordance with other studies in the literature [1, 8, 19]. However, in a dynamic environment, the membership information known to each process might not be complete or consistent with the actual group status. Since a process only communicates with processes that are known to be part of the group, a dynamic membership protocol is needed in order to have processes maintain up-to-date and consistent membership information. The membership protocol should also strive to prevent malicious processes from infiltrating the group.

We now sketch out the design of a dynamic membership protocol for Drum, assuming the existence of a *certification authority* (CA). The complete details of the CA are beyond the scope of this paper, but we note that distributed, Byzantine fault-tolerant implementations of CAs exist, e.g., [33, 10]. The membership protocol is layered on top of Drum's multicast protocol, as in [8, 6].

10.1 Outline of the Suggested Dynamic Membership Protocol

In order to join the group, a process must be authorized by the CA. Once the CA authorizes the process according to its credentials, the CA grants the process with a timestamped certificate, which expires (and so must be renewed) after a certain period of time. A process's membership list will never contain processes that do not have a valid certificate. This prevents unauthorized processes from joining the group. Additionally, certificates can be revoked.

The CA provides the newcomer with an initial (not necessarily complete) list of the other processes in the group, and propagates a *log-in* message to the other processes, containing the newly issued certificate.

Whenever a process wishes to log out of the group, it sends a *log-out* request to the CA, which in turn, revokes that process's certificate and forwards the log-out message to the other processes in the group.

The CA may also revoke a process's certificate due to suspicion of malbehavior. In this case, an appropriate message is sent to the processes, in order to remove the process from the group.

The certificates expire after a certain amount of time. When a process's certificate is about to expire, the process must request a new certificate from the CA, or be effectively removed from the group (we assume that the clock drift among group members is small and bounded).

Processes may suffer benign failures, or long delays that affect their responsiveness. In order to prevent situations in which processes try to spread their data through unresponsive processes, a failure detection mechanism is used. From time to time, each process tests the responsiveness of the other processes it communicates with. If a failure is detected, the process stops communicating with the failed process, but does not propagate this information to other processes. Note that this does not affect the status of the slow/failed process as a group member, as it is possible that the process can communicate with other processes.

Each process piggybacks its certificate on top of an outgoing message if it hasn't done so for a relatively long period, or if it has recently joined the system. This way, processes that do not have a complete membership information database are able to authenticate new messages and complete the database.

Actual implementations of the dynamic memberhsip protocol may differ in two parameters: the size of the initial membership information obtained from the servers, and the points in time at which a process piggybacks its certificate on its messages. E.g., piggybacking certificates on all of the messages guarantees that all valid messages will be authenticated.

10.2 The Rational Behind the Suggested Protocol

We now discuss the implications of dynamic membership in general, and particularly in Drum. We present possible problems that can occur and point out the solution provided by the proposed membership protocol:

- **A process may choose as a gossip partner another process that already logged out of the system.** This is exactly the same as trying to perform a gossip operation to a crashed process. We have investigated the effect of crashes and found out that they have little effect on performance (see Figure 2), as also shown in [17]. Eventually, the failure detector will flag the logged-out process as failed, and even this minor performance penalty will be gone.

- **A process may not know of another newly-joined process.** Thus, the probability that a "new" process will be selected as a communication partner by another process in the group is lower than the respective probability for an "old" process. This property is inherent to all of the membership protocols layered on top of gossip-based multicast protocols, e.g., [8, 6]. Since the expected number of rounds to propagate a message to the group members using a gossip-based multicast protocol is logarithmic in the group size, it takes $O(\log n)$ rounds for the log-in message to propagate to all processes and for the process to be known by every other group member [14]. Once this period is over, this difficulty is naturally gone. Specifically, this propertly holds in Drum even under a DoS attack, since Drum succeeds in propagating multicast messages to all the processes under such an attack.

- **Membership information can be fabricated by malicious processes.** This can create inconsistencies in the system, as bogus processes suddenly appear in local membership databases, and valid processes are removed from these databases. Drum solves this problem by guaranteeing that every join/leave/expel message contains a certificate issued by the CA. Since this certificate cannot be forged by a malicious process with high probability, an attacker cannot send valid group management messages. Also, as opposed to some failure detectors [11, 29], with our approach a process's failure detector does not remove another process from the local membership view, based on information received from other processes.

- **The membership protocol might suffer a DoS attack.** Such an attack may cause group management messages not to reach the processes. This is resolved by the mere fact that the dynamic membership protocol operates using Drum's multicast protocol as its transport layer. Since Drum's multicast protocol withstands DoS attacks, so does the membership protocol. Furthermore, a DoS attack on the CA does not hamper communication among processes that have already joined the group.

- **Messages from unknown processes in the group are discarded.** The membership information in Drum is composed of certificates granted by the CA to the processes in the group. These certificates are used in order to validate incoming messages. Thus, if a process is missing from the local membership database, its messages will be discarded. In order to resolve this issue, Drum piggybacks certificates on of data messages.

11 Conclusions

We have conducted the first systematic study of the impact of DoS attacks on multicast protocols, using asymptotic analysis, simulations, and measurements. Our study has exposed weaknesses of traditional gossip-based multicast protocols: Although such protocols are very robust in the face of process crashes, we have shown that they can be extremely vulnerable to DoS attacks. In particular, an attacker with limited attack strength can cause severe performance degradation by focusing on a small subset of the processes.

We have suggested a few simple measures that one can take in order to improve a system's resilience to DoS attacks: (i) combining pull and push operations; (ii) bounding resources separately for each operation; and (iii) random port selection. We have presented Drum, a simple gossip-based multicast protocol that uses these measures in order to eliminate vulnerabilities to DoS attacks. Our closed-form mathematical analysis, simulations, and empirical tests have proven that these measures go a long way in fortifying a system against DoS attacks. We have shown that, as the attack strength increases asymptotically, the most effective attack against Drum is one that divides thhe attack power among all the correct processes in the system. As expected, the inevitable performance degradation due to such a broad attack is identical for all the studied protocols. However, protocols that use only pull or only push operations perform much worse under more focused attacks, which have little influence on Drum.

We expect our proposed methods for mitigating the effect of DoS attacks to be applicable to various other systems operating in different contexts. Specifically, the use of well-known ports should be minimized, and each process should be able to choose some of its communication partners by itself. Our analysis process and its corresponding metric can be used to generally quantify the effect of DoS attacks. We hope that other researchers will be able to apply similar techniques in order to quantitatively analyze their system's resilience to DoS attacks.

Acknowledgments

We thank Aran Bergman and Dahlia Malkhi for many helpful comments and suggestions. We are grateful to the Flux research group at the University of Utah, and especially Mac Newbold, for allowing us to use their network emulation testbed and assisting us with our experiments.

References

[1] K. P. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, and Y. Minsky. Bimodal multicast. *ACM Transactions on Computer Systems (TOCS)*, 17(2):41–88, 1999.

[2] K. P. Birman, R. van Renesse, and W. Vogels. Spinglass: Secure and scalable communications tools for mission-critical computing. In *DARPA International Survivability Conference and Exposition (DISCEX)*, June 2001.

[3] R. K. C. Chang. Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine*, 40:42–51, October 2002.

[4] Cisco Systems. Defining strategies to protect against TCP SYN denial of service attacks. `http://www.cisco.com/warp/public/707/4.html`.

[5] CSI/FBI. Computer crime and security survey, 2003. `http://www.gocsi.com/forms/fbi/pdf.jhtml`.

[6] A. Das, I. Gupta, and A. Motivala. SWIM: Scalable weakly consistent infection-style process group membership protocol. In *The International Conference on Dependable Systems and Networks (DSN)*, pages 303–312, 2002.

[7] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Stuygis, D. Swinehart, and D. Terry. Epidemic algorithms for replicated database maintenance. In *6th ACM Symposium on Principles of Distributed Computing (PODC)*, pages 1–12, 1987.

[8] P. T. Eugster, R. Guerraoui, S. B. Handurukande, A. M. Kermarrec, and P. Kouznetsov. Lightweight probabilistic broadcast. In *The International Conference on Dependable Systems and Networks (DSN)*, 2001.

[9] X. Geng and A. B. Whinston. Defeating distributed denial of service attacks. *IEEE IT Professional*, pages 46–51, July/August 2000.

[10] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold DSS signatures. *Information and Computation*, 164(1):54–84, 2001.

[11] I. Gupta, T. D. Chandra, and G. Goldszmidt. On scalable and efficient distributed failure detectors. In *20th Symposium on Principles of Distributed Computing (PODC 2001)*, August 2001.

[12] I. Gupta, A.-M. Kermarrec, and A. J. Ganesh. Efficient epidemic-style protocols for reliable and scalable multicast. In *21st IEEE International Symposium on Reliable Distributed Systems (SRDS)*, pages 180–189, October 2002.

[13] I. Gupta, R. van Renesse, and K. P. Birman. Scalable fault-tolerant aggregation in large process groups. In *The International Conference on Dependable Systems and Networks (DSN)*, pages 433–442, 2001.

[14] R. M. Karp, C. Schindelhauer, S. Shenker, and B. Vocking. Randomized rumor spreading. In *IEEE Symposium on Foundations of Computer Science*, pages 565–574, 2000.

[15] A.-M. Kermarrec, L. Massouli, and A. J. Ganesh. Probabilistic reliable dissemination in large-scale systems. *IEEE Transactions on Parallel and Distributed Systems*, 14(3):248–258, March 2003.

[16] M. J. Lin and K. Marzullo. Directional gossip: Gossip in a wide area network. In *European Dependable Computing Conference (EDCC)*, pages 364–379, 1999.

[17] M. J. Lin, K. Marzullo, and S. Masini. Gossip versus deterministically constrained flooding on small networks. In *14th International Symposium on DIStributed Computing (DISC)*, pages 253–267, 2000.

[18] P. Linga, I. Gupta, and K. Birman. A churn-resistant peer-to-peer web caching system. *ACM Workshop on Survivable and Self-Regenerative Systems*, October 2003.

[19] D. Malkhi, Y. Mansour, and M. K. Reiter. Diffusion without false rumors: On propagating updates in a Byzantine environment. *Theoretical Computer Science*, 299(1–3):289–306, April 2003.

[20] D. Malkhi, E. Pavlov, and Y. Sella. Optimal unconditional information diffusion. In *15th International Symposium on DIStributed Computing (DISC)*, 2001.

[21] D. Malkhi, M. K. Reiter, O. Rodeh, and Y. Sella. Efficient update diffusion in Byzantine environments. In *20th IEEE International Symposium on Reliable Distributed Systems (SRDS)*, October 2001.

[22] Y. M. Minsky and F. B. Schneider. Tolerating malicious gossip. *Distributed Computing*, 16(1):49–68, February 2003.

[23] D. Moore, G. Voelker, and S. Savage. Inferring Internet denial-of-service activity. In *Proceedings of the 10th USENIX Security Symposium*, pages 9–22, August 2001.

[24] National Institute for Standards and Technology. Digital Signature Standard (DSS). *FIPS Publication 186-2*, October 2001. `http://csrc.nist.gov/publications/fips/`.

[25] B. Pittel. On spreading a rumor. *SIAM Journal on Applied Mathematics*, 47(1):213–223, February 1987.

[26] Riverhead Networks. Products overview. `http://www.riverhead.com/pr/index.html`.

[27] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni. Analysis of a denial of service attack on TCP. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 208–223, May 1997.

[28] S. Staniford, V. Paxson, and N. Weaver. How to own the Internet in your spare time. In *Proceedings of the 11th USENIX Security Symposium*, pages 149–167, August 2002.

[29] R. van Renesse, Y. Minsky, and M. Hayden. A gossip-style failure detection service. TR TR98-1687, Cornell University, Computer Science, May 1998.

[30] J. Wang, L. Lu, and A. A. Chien. Tolerating denial-of-service attacks using overlay networks – impact of overlay network topology. *ACM Workshop on Survivable and Self-Regenerative Systems*, October 2003.

[31] E. W. Weisstein. *CRC Concise Encyclopedia of Mathematics*.

[32] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar. An integrated experimental environment for distributed systems and networks. In *Proc. of the Fifth Symposium on Operating Systems Design and Implementation*, pages 255–270, Boston, MA, Dec. 2002. USENIX Association.

[33] L. Zhou, F. B. Schneider, and R. van Renesse. COCA: A secure distributed online certification authority. *ACM Transactions on Computer Systems*, 20(4):329–368, 2002.

A Calculating p_u and p_a

Suppose process p_i sends a message to process p_j, we want to calculate the probability that process p_j accepts this message. Denote the event "process p_i sends a message to process p_j" by S_{ij}. Assume $n > F$, and define q as the probability that process p_j appears in process p_i's *view*, then:

$$q = 1 - \frac{n-2}{n-1} \cdot \frac{n-3}{n-2} \cdots \frac{n-1-F}{n-F} = 1 - \frac{n-1-F}{n-1} = \frac{F}{n-1}$$

Let Y be the number of valid messages received by p_j in a single round, then:

$$\begin{array}{rrcl} & \Pr(Y \leq 0 \mid S_{ij}) & = & \Pr(Y \geq n \mid S_{ij}) = 0 \\ 0 < y < n & \Pr(Y = y \mid S_{ij}) & = & \binom{n-2}{y-1} q^{y-1}(1-q)^{n-1-y} \end{array}$$

Let p_Y be the probability that a non-attacked process, p_j, discards the message sent by p_i, given S_{ij}, then:

$$p_Y = \begin{cases} 0 & Y \leq F \\ \frac{Y-1}{Y} \cdot \frac{Y-2}{Y-1} \cdots \frac{Y-F}{Y-F+1} = \frac{Y-F}{Y} & Y > F \end{cases}$$

Calculating p_u gives:

$$\begin{aligned} p_u \quad = \quad & 1 - \sum_{y=-\infty}^{\infty} p_y \cdot Pr(Y = y \mid S_{ij}) = \\ & 1 - \sum_{y=F+1}^{n-1} \frac{y-F}{y} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \\ & \sum_{y=1}^{F} \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} + \\ & \sum_{y=F+1}^{n-1} \frac{F}{y} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} \end{aligned} \tag{8}$$

If p_j is attacked with $x \geq F$ messages, we get:

$$p_Y = \frac{Y+x-1}{Y+x} \cdot \frac{Y+x-2}{Y+x-1} \cdots \frac{Y+x-F}{Y+x-F+1} = \frac{Y+x-F}{Y+x}$$

And thus:

$$\begin{aligned} p_a \quad = \quad & 1 - \sum_{y=-\infty}^{\infty} p_y \cdot Pr(Y = y \mid S_{ij}) = \\ & 1 - \sum_{y=1}^{n-1} \frac{y+x-F}{y+x} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \\ & \sum_{y=1}^{n-1} \frac{F}{y+x} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} < \\ & \sum_{y=1}^{n-1} \frac{F}{x} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \frac{F}{x} \end{aligned}$$

Lemma 7. $\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} < \frac{F}{\alpha x}$.

Proof. Calculating the derivatives, we get:

$$\begin{aligned}
\frac{\mathrm{d}p_a}{\mathrm{d}x} &= \sum_{y=1}^{n-1} \frac{\mathrm{d}\frac{F}{y+x}}{\mathrm{d}x} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \\
& \sum_{y=1}^{n-1} \frac{-F}{(y+x)^2} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} \\
\frac{\mathrm{d}x}{\mathrm{d}\alpha} &= \frac{\mathrm{d}\frac{B}{\alpha n}}{\mathrm{d}\alpha} = \frac{-B}{\alpha^2 n} \\
\frac{\mathrm{d}p_a}{\mathrm{d}\alpha} &= \frac{\mathrm{d}p_a}{\mathrm{d}x} \cdot \frac{\mathrm{d}x}{\mathrm{d}\alpha} = \\
& \sum_{y=1}^{n-1} \frac{FB}{\alpha^2 n(y+x)^2} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \\
& \sum_{y=1}^{n-1} \frac{Fx}{\alpha(y+x)^2} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} < \\
& \sum_{y=1}^{n-1} \frac{Fx}{\alpha x^2} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} = \frac{F}{\alpha x}
\end{aligned}$$

□

We now give a bound on p_u.

Lemma 8. $p_u > 0.6$.

Proof. Define:

$$\mu \triangleq E[Y \mid S_{ij}] = \textstyle\sum_{y=1}^{n-1} y \cdot \binom{n-2}{y-1} q^{y-1}(1-q)^{n-1-y} = \frac{n-2}{n-1} \cdot F + 1$$

$$E[Y^2 \mid S_{ij}] = \textstyle\sum_{y=1}^{n-1} y^2 \cdot \binom{n-2}{y-1} q^{y-1}(1-q)^{n-1-y} = \frac{(n-2)(n-3)}{(n-1)^2} \cdot F^2 + 3 \cdot \frac{n-2}{n-1} \cdot F + 1$$

$$\sigma^2 \triangleq Var(Y \mid S_{ij}) = \frac{(n-2)(n-3)}{(n-1)^2} \cdot F^2 + 3 \cdot \frac{n-2}{n-1} \cdot F + 1 - \left(\frac{n-2}{n-1} \cdot F + 1\right)^2 = \frac{n-2}{n-1} \cdot F - \frac{n-2}{(n-1)^2} \cdot F^2$$

By [31], for $n \gg 1$ we get that Y given S_{ij} can be approximated using a normal distribution function, with $\mu = F + 1$ and $\sigma^2 = F$. The cumulative distribution function $D(x)$ is thus given by:

$$D(x) = \tfrac{1}{2} \cdot \left(1 + \operatorname{erf}\left(\tfrac{x-\mu}{\sqrt{2}\sigma}\right)\right) = \tfrac{1}{2} \cdot \left(1 + \operatorname{erf}\left(\tfrac{x-F-1}{\sqrt{2F}}\right)\right) \quad \text{where} \quad \operatorname{erf}(z) = 1 - \frac{2}{\sqrt{\pi}} \int_z^\infty e^{-t^2} \mathrm{d}t$$

From [31] we get the following:

$$\tfrac{1}{x+\sqrt{x^2+2}} < e^{x^2} \textstyle\int_x^\infty e^{-t^2} \mathrm{d}t < \tfrac{1}{x+\sqrt{x^2+\frac{4}{\pi}}}$$

Concluding that:

$$\operatorname{erf}(z) = 1 - \frac{2}{\sqrt{\pi}} \int_z^\infty e^{-t^2} \mathrm{d}t > 1 - \frac{2}{\sqrt{\pi}} \cdot \frac{e^{-z^2}}{z + \sqrt{z^2 + \frac{4}{\pi}}}$$

The first sum in formula 8 is approximated by $D(F)$. Calculating $D(F)$ gives:

$$\begin{aligned} D(F) &= \frac{1}{2}\cdot\left(1+\operatorname{erf}\left(\frac{-1}{\sqrt{2F}}\right)\right) > \frac{1}{2}+\frac{1}{2}\cdot\left(1-\frac{2}{\sqrt{\pi}}\cdot\frac{e^{-\frac{1}{2F}}}{\sqrt{\frac{1}{2F}+\frac{4}{\pi}}-\frac{1}{\sqrt{2F}}}\right) = \\ & 1-\frac{1}{\sqrt{\pi}}\cdot\frac{e^{-\frac{1}{2F}}}{\frac{\sqrt{\pi+8F}}{\sqrt{2\pi F}}-\frac{1}{\sqrt{2F}}} = 1-\sqrt{2}\cdot\frac{\sqrt{F}\cdot e^{-\frac{1}{2F}}}{\sqrt{\pi+8F}+\sqrt{\pi}} \end{aligned}$$

Define:

$$g(F) = \frac{\sqrt{F}\cdot e^{-\frac{1}{2F}}}{\sqrt{\pi+8F}+\sqrt{\pi}}$$

We want to bound D(x) from above by finding for which values of F, $g'(F) < 0$. The denominator of $g'(F)$ is always positive, so we ignore it when calculating the derivative:

$$\left(\frac{e^{-\frac{1}{2F}}}{2\sqrt{F}}+\frac{\sqrt{F}e^{-\frac{1}{2F}}}{2F^2}\right)\left(\sqrt{\pi+8F}-\sqrt{\pi}\right)-\frac{8\sqrt{F}e^{-\frac{1}{2F}}}{2\sqrt{\pi+8F}} < 0$$

$$\frac{F^{\frac{3}{2}}+F^{\frac{1}{2}}}{2F^2}\left(\sqrt{\pi+8F}-\sqrt{\pi}\right)-\frac{8\sqrt{F}e^{-\frac{1}{2F}}}{2\sqrt{\pi+8F}} < 0$$

$$\frac{\left(F^{\frac{3}{2}}+F^{\frac{1}{2}}\right)\left(\sqrt{\pi+8F}-\sqrt{\pi}\right)\sqrt{\pi+8F}-8F^{\frac{5}{2}}}{2F^2\sqrt{\pi+8F}} < 0$$

Once again, the denominator is positive, and we get:

$$\left(F^{\frac{3}{2}}+F^{\frac{1}{2}}\right)\left(\sqrt{\pi+8F}-\sqrt{\pi}\right)\sqrt{\pi+8F}-8F^{\frac{5}{2}} < 0$$

$$\pi+8F-\sqrt{\pi^2+8\pi F}-8F\cdot\left(1-\frac{1}{F+1}\right) < 0$$

$$\frac{8F}{\sqrt{\pi}(F+1)} < \sqrt{\pi+8F}-\sqrt{\pi}$$

Taking derivatives we get:

$$\begin{aligned} \frac{8}{\sqrt{\pi}(F+1)^2} &\overset{?}{<} \frac{8}{2\sqrt{\pi+8F}} \\ 2\sqrt{\pi+8F} &\overset{?}{<} \sqrt{\pi}(F+1)^2 \end{aligned}$$

Clearly, $(F+1)^2$ grows faster than $2\sqrt{\pi+8F}$. Numerically solving for $F=1$ shows that the inequality holds. Thus, it holds for every $F\in\mathbb{N}$. Consequently, we only need to find the first F for which:

$$\frac{8F}{\sqrt{\pi}(F+1)} < \sqrt{\pi+8F}-\sqrt{\pi}$$

A numerical solution for this inequality shows that it first holds for $F=3$. Thus, for $F\geq 3$ we get that $g'(F)<0$, and thus $D(F+1)>D(F)$. Assigning $F=3$ in our previous bound for D(F), we get that for all $F\geq 3$, $D(F)\geq D(3) > 0.3968 \approx 0.4$. Assuming $F\geq 3$, we get:

$$\sum_{y=1}^{F}\binom{n-2}{y-1}\left(\frac{F}{n-1}\right)^{y-1}\left(\frac{n-1-F}{n-1}\right)^{n-1-y} > 0.4$$

Since $D(x)$ is maximal at $x = \mu = F+1$ and symmetric around it, we get the approximation:

$$\sum_{y=F+1}^{2F} \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} > \sum_{y=1}^{F} \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y}$$

And finally, we conclude that:

$$\begin{aligned} p_u \quad = \quad & \sum_{y=1}^{F} \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} + \\ & \sum_{y=F+1}^{n-1} \frac{F}{y} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} > \\ & \frac{2}{5} + \sum_{y=F+1}^{2F} \frac{F}{2F} \cdot \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} > \\ & \frac{2}{5} + \frac{1}{2} \cdot \sum_{y=1}^{F} \binom{n-2}{y-1} \left(\frac{F}{n-1}\right)^{y-1} \left(\frac{n-1-F}{n-1}\right)^{n-1-y} > \\ & \frac{2}{5} + \frac{1}{2} \cdot \frac{2}{5} = \frac{3}{5} \end{aligned}$$

□

B Calculating $\widetilde{p}$

We now compute $\widetilde{p}$, the probability that M is propagated from the source in a round in Pull. Assume $n > F$, and define q as the probability that process p_2 appears in process p_1's $view_{pull}$, then $q = \frac{F}{n-1}$. Let Y be the number of valid pull-requests received in a single round, then:

$$\begin{aligned} & \Pr(Y < 0) &=& \Pr(Y \geq n) = 0 \\ 0 \leq y < n \quad & \Pr(Y = y) &=& \binom{n-1}{y} q^y (1-q)^{n-1-y} \end{aligned}$$

Assume $x \geq F$, and define p_Y as the probability that a valid pull-request is read from the buffer, then:

$$p_Y = 1 - \left(1 - \frac{Y}{Y+x}\right)\left(1 - \frac{Y}{Y+x-1}\right) \cdots \left(1 - \frac{Y}{Y+x-F+1}\right) = 1 - \frac{x! \cdot (Y+x-F)!}{(x-F)! \cdot (Y+x)!}$$

The probability $\widetilde{p}$ that a valid pull-request is read from the buffer, independent of Y, is:

$$\widetilde{p} = \sum_{y=-\infty}^{\infty} p_y \cdot \Pr(Y = y) = \sum_{y=0}^{n-1} \left(1 - \frac{x! \cdot (y+x-F)!}{(x-F)! \cdot (y+x)!}\right) \binom{n-1}{y} \left(\frac{F}{n-1}\right)^y \left(\frac{n-1-F}{n-1}\right)^{n-1-y}$$

C Detailed Analysis

In this section we give a formal analysis of the three protocols in the absence of DoS attacks (failure-free and crash failures) as well as under Dos attacks. In Section C.1, we describe the parameters and notations used in our analysis formulas. In Section C.2, we detail our analysis formulas. In Section C.3, we use these formulas to compute the expected percentage of correct processes that receive *M* for a given round, and compare these results with the simulation results of the previous chapter.

C.1 Definitions

Parameters

- b – number of faulty processes.
- ϵ_{loss} – the link-loss probability. We assume that ϵ_{loss} is equal for all links and independent of any other factor.
- $F_{in-push}$, $F_{in-pull}$ – bounds on the number of process to receive messages from in a round, in a push or a pull (respectively) operation. We fix $F_{in-push} = F_{in-pull} = \frac{F}{2}$ in Drum, $F_{in-push} = F$ in Push, and $F_{in-pull} = F$ in Pull.
- x_{push}, x_{pull} – number of fabricated push or pull (respectively) messages sent to an attacked process in each round. In Drum, $x_{push} = x_{pull} = \frac{x}{2}$, in Push, $x_{push} = x$, and in Pull, $x_{pull} = x$.

Notation

- *p* – the probability that a given correct process, *target*, will receive a gossip message *M* from another given correct process, *sender*, in a certain round. We denote $q = 1 - p$.
- p_{push}, p_{pull} – similar to *p*, but as a result of a push or a pull (respectively) operation.
- d_{push} – the probability that the target will discard the sender's incoming push message due to the bound $F_{in-push}$ on push messages accepted during each round, given that the sender's message reached the target.
- d_{pull} – the probability that the sender will discard the target's incoming pull-request message due to the bound $F_{in-pull}$ on pull-request messages accepted during each round, given that the target's message reached the sender.

  Note that since $F_{in-push}$ and $F_{in-pull}$ are smaller in Drum than in Push and Pull, these evaluate to different values for different protocols.
- S_r – the number of correct processes that have *M* at the beginning of round *r*, $S_r \in [1 \ldots n - b\,]$.

The probability d is similar to $1 - p_u$ computed in Appendix A for the asymptotic analysis, except for the following: (i) $\epsilon_{loss} > 0$, (ii) there are faulty processes ($b > 0$), and (iii) in Drum, the bounds $F_{in-push}$ and $F_{in-pull}$ are tested separately. That is, each processes accepts push messages from at most $F_{in-push}$ processes, and pull-request messages from at most $F_{in-pull}$ processes.

C.2 Formulas

In Section C.2.1, we present the formulas for the case without DoS attacks. In Section C.2.2, we add DoS attacks. In the next section we present the results obtained from both analyses.

C.2.1 Without DoS Attacks

Here, the b faulty processes are crashed – they do not send any messages (when $b = 0$ there is no attack). Our formulas are based on the analysis of a push-based protocol presented in [8].

We first compute d_{push} and d_{pull}. Where d_{push} is the probability that the target will discard the sender's incoming push message, given that the sender's message reached the target, and d_{pull} is the probability that the sender will discard the target's incoming pull-request message, given that the target's message reached the sender. Note that d_{push} (respectively, d_{pull}) depends on the number of messages that the target (respectively, sender) receives in a gossip round, since a process only accepts $F_{in-push}$ (respectively, $F_{in-pull}$) push (respectively, pull-request) messages in each round. The computation of d_{push} is as follows:
Denote the event "sender s chooses target t and the sender's message is not lost" by R_{s-t}. Let Y be the number of valid messages received by the target in a single round, and Z be the number of processes that choose the target in a single round, then:

$$\Pr(Y=y\ ,\ Z=z \mid R_{s-t}) \quad = \quad \binom{n-b-2}{z-1}\left(\frac{|view_{push}|}{n-1}\right)^{z-1}\left(1-\frac{|view_{push}|}{n-1}\right)^{n-b-1-z}\binom{z-1}{y-1}(1-\epsilon_{loss})^{y-1}{\epsilon_{loss}}^{z-y}$$

Where $0 < y \leq z < n-b$. Therefore,

$$\begin{aligned}\Pr(Y=y \mid R_{s-t}) \quad &= \quad \sum_{z}\Pr(Y=y\ ,\ Z=z \mid R_{s-t}) = \\ &\sum_{z=y}^{n-b-1}\binom{n-b-2}{z-1}\left(\frac{|view_{push}|}{n-1}\right)^{z-1}\left(1-\frac{|view_{push}|}{n-1}\right)^{n-b-1-z}\binom{z-1}{y-1}(1-\epsilon_{loss})^{y-1}{\epsilon_{loss}}^{z-y}\end{aligned}$$

Let q_Y be the probability that the target discards the message sent by the sender, given R_{s-t}, then:

$$q_Y = \begin{cases} 0 & Y \leq F_{in-push} \\ \frac{Y-1}{Y}\cdot\frac{Y-2}{Y-1}\cdots\frac{Y-F}{Y-F+1} = \frac{Y-F}{Y} & Y > F_{in-push}\end{cases}$$

Calculating d_{push} gives:

$$d_{push} = \sum_{y} q_y \cdot \Pr(Y=y \mid R_{s-t}) =$$

$$\sum_{y=F_{in-push}+1}^{n-b-1}\frac{y-F_{in-push}}{y}\cdot$$

$$\sum_{z=y}^{n-b-1}\binom{n-b-2}{z-1}\left(\frac{|view_{push}|}{n-1}\right)^{z-1}\left(1-\frac{|view_{push}|}{n-1}\right)^{n-b-1-z}\binom{z-1}{y-1}(1-\epsilon_{loss})^{y-1}(\epsilon_{loss})^{z-y}$$

We compute d_{pull} similarly to the computation of d_{push}, and get the following formula:

$$d_{pull} = \sum_{y} q_y \cdot \Pr(Y=y \mid R_{t-s}) =$$

$$\sum_{y=F_{in-pull}+1}^{n-b-1}\frac{y-F_{in-pull}}{y}\cdot$$

$$\sum_{z=y}^{n-b-1} \binom{n-b-2}{z-1} \left(\frac{|view_{pull}|}{n-1}\right)^{z-1} \left(1-\frac{|view_{pull}|}{n-1}\right)^{n-b-1-z} \binom{z-1}{y-1} (1-\epsilon_{loss})^{y-1} (\epsilon_{loss})^{z-y}$$

We now compute the probabilities p_{push} and p_{pull}. Where p_{push} (respectively, p_{pull}) is the probability that the target will successfully receive a gossip message *M* from the sender, in a certain round, as a result of a push (respectively, pull) operation. The formula for p_{push} includes dependent probabilities. That is,

$$p_{push} = \Pr\left(\begin{array}{c} \textit{sender chooses} \\ \textit{target} \end{array}, \begin{array}{c} \textit{the msg is} \\ \textit{not lost} \end{array}, \begin{array}{c} \textit{target does not} \\ \textit{drop the msg} \end{array} \right) =$$

$$\Pr\left(\begin{array}{c} \textit{sender chooses} \\ \textit{target} \end{array} \right) \Pr\left(\begin{array}{c} \textit{the msg is} \\ \textit{not lost} \end{array} \right) \Pr\left(\begin{array}{c} \textit{target does not} \\ \textit{drop the msg} \end{array} \mid \begin{array}{c} \textit{sender chooses} \\ \textit{target} \end{array}, \begin{array}{c} \textit{the msg is} \\ \textit{not lost} \end{array} \right) =$$

$$(\frac{|view_{push}|}{n-1})(1-\epsilon_{loss})(1-d_{push})$$

The probability p_{pull} is calculated similarly:

$$p_{pull} = (\frac{|view_{pull}|}{n-1})(1-\epsilon_{loss})^2(1-d_{pull})$$

In Push $p = p_{push}$, in Pull $p = p_{pull}$, and in Drum $p = 1-(1-p_{push})(1-p_{pull})$.

Given that *i* correct processes have *M* at the beginning of round r, we define the probability p_{ij} that exactly *j* ($j \geq i$) correct processes have *M* at the beginning of the next round:

$$p_{ij} \triangleq \Pr(S_{r+1} = j | S_r = i)$$

We now approximate p_{ij} as follows[1]:

$$p_{ij} \approx \binom{n-b-i}{j-i} (1-q^i)^{j-i} (q^i)^{n-b-j}$$

S_r is computed recursively as follows:

$$\Pr(S_0 = 1) = 1,$$
$$\Pr(S_{r+1} = j) = \sum_{i \leq j} \Pr(S_r = i) p_{ij}$$

The expected number of correct processes that have *M* at the beginning of each gossip round is then as follows:

$$E(S_r) = \sum_{1 \leq j \leq n-b} \Pr(S_r = j) j$$

[1]This formula gives an over-estimate of p_{ij}, since some of the counted events reflect a situation where a process sends and receives more messages than allowed by the F_{in} and F_{out} bounds. However, the probabilities of these events can be neglected (see [1]).

C.2.2 DoS Attacks

We now add DoS attacks into the mix. For a probability P, we denote by P^a the probability of P when the process is under an attack, and by P^u the case that the process is not under an attack. E.g., d^a_{push} is the probability that an attacked target will discard the sender's incoming push message, and d^u_{push} is the probability that a non-attacked target will discard the sender's incoming push message.

Under a DoS attack, d^u_{push} (respectively d^u_{pull}) is equal to d_{push} (respectively, d_{pull}) as calculated above, whereas the formulas for d^a_{push} and d^a_{pull} also depend on the number of fabricated push or pull-request (respectively) messages sent to an attacked correct process in each round, i.e., x_{push} and x_{pull}. The computation of d^a_{push} is now as follows:
Let $\acute{X}_{push}$ be the number of fabricated push messages that the target receives in a single round, then:

$$\Pr(\acute{X}_{push} = \acute{x}_{push}) = \binom{x_{push}}{\acute{x}_{push}}(1-\epsilon_{loss})^{\acute{x}_{push}}{\epsilon_{loss}}^{x_{push}-\acute{x}_{push}}$$

and

$$q_Y = \begin{cases} 0 & Y + \acute{X}_{push} \leq F_{in-push} \\ \frac{Y+\acute{X}_{push}-F}{Y+\acute{X}_{push}} & Y + \acute{X}_{push} > F_{in-push} \end{cases}$$

Calculating d^a_{push} gives:

$$d^a_{push} = \sum_{y}\sum_{\acute{x}_{push}} q_y \cdot \Pr(\acute{X}_{push} = \acute{x}_{push}) \cdot \Pr(Y = y \mid R_{s-t}) =$$

$$\sum_{y=1}^{n-b-1}\sum_{\acute{x}_{push}=0}^{x_{push}} \max\left\{0, \frac{y+\acute{x}_{push}-F_{in-push}}{y+\acute{x}_{push}}\right\} \cdot \binom{x_{push}}{\acute{x}_{push}} (1-\epsilon_{loss})^{\acute{x}_{push}} \left(\epsilon_{loss}\right)^{x_{push}-\acute{x}_{push}} \cdot$$
$$\sum_{z=y}^{n-b-1}\binom{n-b-2}{z-1}\left(\frac{|view_{push}|}{n-1}\right)^{z-1}\left(1-\frac{|view_{push}|}{n-1}\right)^{n-b-1-z}\binom{z-1}{y-1}(1-\epsilon_{loss})^{y-1}\left(\epsilon_{loss}\right)^{z-y}$$

We compute d^a_{pull} similarly to the computation of d^a_{push}, and get the following formula:

$$d^a_{pull} = \sum_{y}\sum_{\acute{x}_{pull}} q_y \cdot \Pr(\acute{X}_{pull} = \acute{x}_{pull}) \cdot \Pr(Y = y \mid R_{t-s}) =$$

$$\sum_{y=1}^{n-b-1}\sum_{\acute{x}_{pull}=0}^{x_{pull}} \max\left\{0, \frac{y+\acute{x}_{pull}-F_{in-pull}}{y+\acute{x}_{pull}}\right\} \cdot \binom{x_{pull}}{\acute{x}_{pull}} (1-\epsilon_{loss})^{\acute{x}_{pull}} \left(\epsilon_{loss}\right)^{x_{pull}-\acute{x}_{pull}} \cdot$$
$$\sum_{z=y}^{n-b-1}\binom{n-b-2}{z-1}\left(\frac{|view_{pull}|}{n-1}\right)^{z-1}\left(1-\frac{|view_{pull}|}{n-1}\right)^{n-b-1-z}\binom{z-1}{y-1}(1-\epsilon_{loss})^{y-1}\left(\epsilon_{loss}\right)^{z-y}$$

The probabilities p^u_{push} (p^u_{pull}) and p^a_{push} (p^a_{pull}) are computed as follows:

$$p^u_{push} = (\frac{|view_{push}|}{n-1})(1-\epsilon_{loss})(1-d^u_{push}), \quad p^u_{pull} = (\frac{|view_{pull}|}{n-1})(1-\epsilon_{loss})^2(1-d^u_{pull})$$

$$p^a_{push} = (\frac{|view_{push}|}{n-1})(1-\epsilon_{loss})(1-d^a_{push}), \quad p^a_{pull} = (\frac{|view_{pull}|}{n-1})(1-\epsilon_{loss})^2(1-d^a_{pull})$$

Given that i_u and i_a non-attacked and attacked (respectively) correct processes have *M* at the beginning of a round, we can compute the probability q_u^* (respectively q_a^*), that none of these i_u and i_a processes successfully propagate *M* to any other non-attacked (attacked) correct process:
Push:

$$q_u^* = (1 - p_{push}^u)^{i_u + i_a}$$

$$q_a^* = (1 - p_{push}^a)^{i_u + i_a}$$

Pull:

$$q_u^* = q_a^* = (1 - p_{pull}^u)^{i_u} \cdot (1 - p_{pull}^a)^{i_a}$$

Drum:

$$q_u^* = (1 - p_{push}^u)^{i_u + i_a} \cdot (1 - p_{pull}^u)^{i_u} \cdot (1 - p_{pull}^a)^{i_a}$$

$$q_a^* = (1 - p_{push}^a)^{i_u + i_a} \cdot (1 - p_{pull}^u)^{i_u} \cdot (1 - p_{pull}^a)^{i_a}$$

Now we can compute the joint probability $p_{i_u i_a j_u j_a}$ that exactly j_u and j_a ($j_u \geq i_u, j_a \geq i_a$) correct processes have *M* at the beginning of the next round:

$$p_{i_u i_a j_u j_a} \triangleq \Pr(S_{r+1}^u = j_u, S_{r+1}^a = j_a | S_r^u = i_u, S_r^a = i_a) =$$

$$\Pr(S_{r+1}^u = j_u | S_r^u = i_u, S_r^a = i_a) \cdot \Pr(S_{r+1}^a = j_u | S_r^u = i_u, S_r^a = i_a)$$

Where:

$$\Pr(S_{r+1}^u = j_u | S_r^u = i_u, S_r^a = i_a) = \binom{n-b-\alpha n - i_u}{j_u - i_u}(1 - q_u^*)^{j_u - i_u}(q_u^*)^{n-b-\alpha n - j_u}$$

and

$$\Pr(S_{r+1}^a = j_a | S_r^u = i_u, S_r^a = i_a) = \binom{\alpha n - i_a}{j_a - i_a}(1 - q_a^*)^{j_a - i_a}(q_a^*)^{\alpha n - j_a}$$

S_r^u and S_r^a are computed recursively as follows:

$$\Pr(S_0^u = 0, S_0^a = 1) = 1$$

$$\Pr(S_{r+1}^u = j_u, S_{r+1}^a = j_a) = \sum_{0 \leq i_u \leq j_u} \sum_{1 \leq i_a \leq j_a} \Pr(S_r^u = i_u, S_r^a = i_a) p_{i_u i_a j_u j_a}$$

$$\Pr(S_{r+1}^u = j_u) = \sum_{0 \leq j_u \leq n-b-\alpha n} \Pr(S_{r+1}^u = j_u, S_{r+1}^a = j_a)$$

$$\Pr(S_{r+1}^a = j_a) = \sum_{1 \leq j_a \leq \alpha n} \Pr(S_{r+1}^u = j_u, S_{r+1}^a = j_a)$$

The expected number of non-attacked and attacked correct processes that have *M* at the beginning of each round, is calculated as follows:

$$E(S_r^u) = \sum_{0 \leq j_u \leq n-b-\alpha n} \Pr(S_r^u = j_u) j_u$$

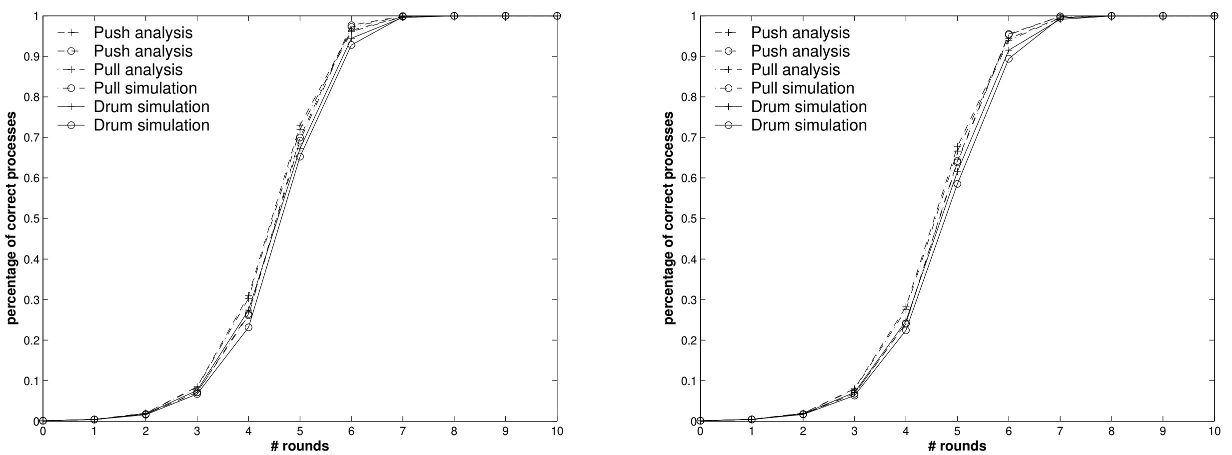
$$E(S_r^a) = \sum_{1 \leq j_a \leq \alpha n} \Pr(S_r^a = j_a) j_a$$

$$E(S_r) = E(S_r^u) + E(S_r^a)$$

C.3 Results

We numerically computed the above formulas using *MATLAB*, with the same parameters used in the simulation presented in the previous chapter. We now compare the analysis results with the results obtained in the simulations.

We show CDFs of the percentage of correct processes that receive *M* by each round. Figure 13 shows the CDFs for failure-free operation (Figure 13 (a)), and for operation with crashed processes (Figure 13 (b)). The analysis and simulation results are almost identical.

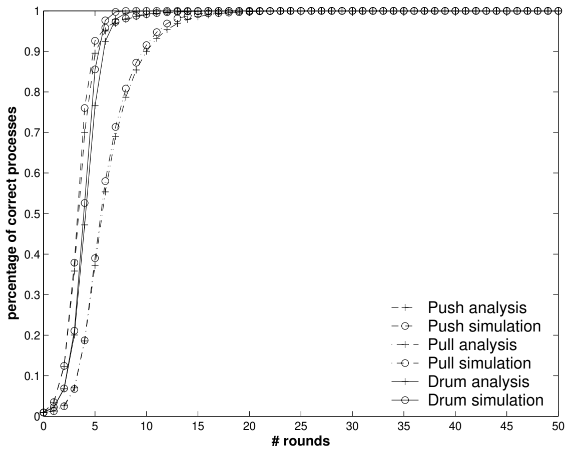


(a) Failure-free operation.

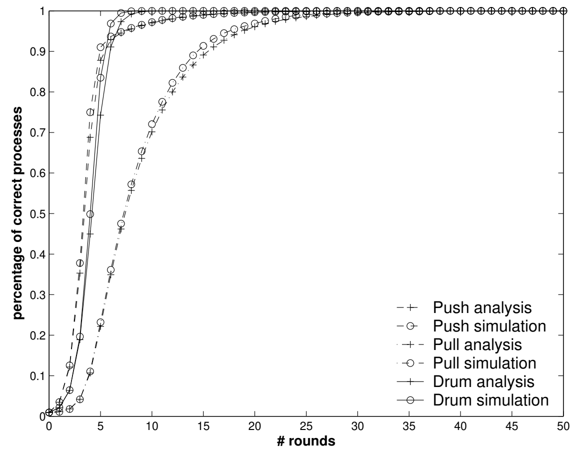
(b) Operation with crashed processes, 10% crashed.

Figure 13: Analysis vs. Simulation: CDFs of percentage of correct processes that receive *M*, $n = 1000$.

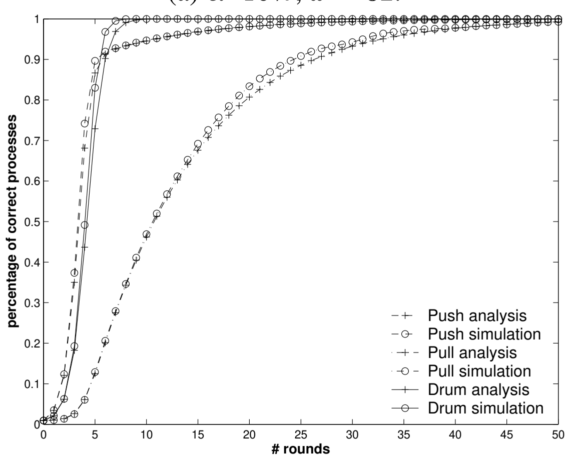
Figure 14 compares our analysis results with the simulation results under various DoS attacks for a system with 120 processes. Again, the analysis and simulation results are virtually the same. Thus, the analysis validates our simulations (and vice versa).



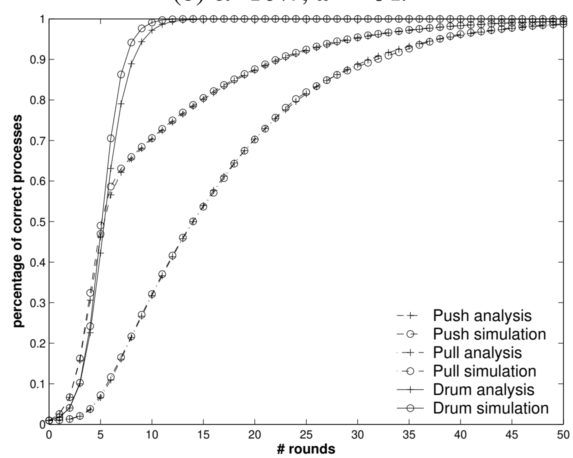
(a) α=10%, $x = 32$.



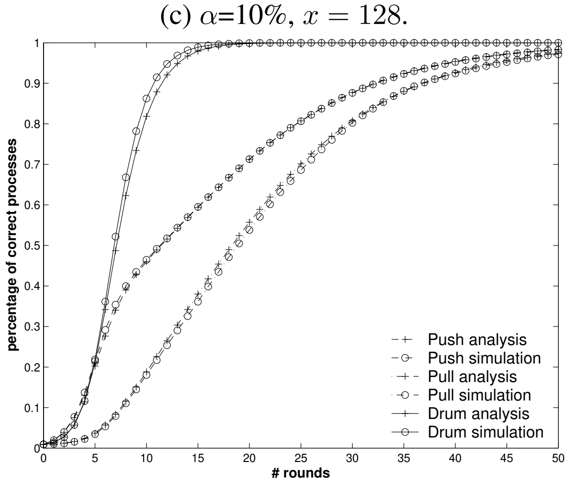
(b) α=10%, $x = 64$.



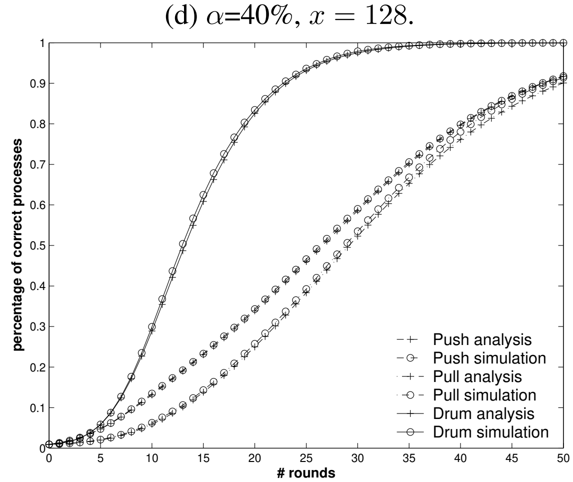
(c) α=10%, $x = 128$.



(d) α=40%, $x = 128$.



(e) α=60%, $x = 128$.



(f) α=80%, $x = 128$.

Figure 14: Analysis vs. Simulation: CDFs of percentage of correct processes that receive *M*, $n = 120$.