Letters to the Editor

Quality of Service

I have read the article “Increasing QoS in Selfish Overlay Networks” from the May/June 2006 issue of Internet Computing magazine and found its conclusions strange.

As Figure 2 implies, using $\beta = 1.0$ gives the best results in terms of number of requests accepted from free-riders and service reliability. This value means that a node builds its reputation using peer testimonials but ignoring its own opinion. In practice, this behavior will make the system vulnerable to a malicious group-of-nodes attack that will let it disconnect any victim node $V$. If the malicious group behaves honestly, then its members will have a high reputation at node $V$. If the malicious group lies to node $V$ of the remaining nodes, then the reputation of those nodes will decrease because $V$ uses peer testimonials and doesn’t use results of its own experience at the evaluation. Eventually, the reputation of bad nodes will dominate that of the remaining nodes. After that, the malicious group could start to behave dishonestly. The reputations of those nodes that testify to the reputation of the malicious group are negligible; therefore, the victim will be unable to learn that it has been deceived. The malicious group will then have a 100 percent share of the network’s bandwidth.

—Alexey Smirnov
Computer Science Department, State University of New York, Stony Brook

Dorgival Guedes and colleagues respond:
In fact, the situation described by the reader is a possible scenario, although it falls beyond the assumptions we adopted in the article. As described in the introduction, we used a noncooperative game model, in which players act independently of each other (that is, in their own self-interests) and don’t use any group strategies. This is the usual behavior of free-riders, which try to extract most of the network for themselves without giving anything in return to any other node. As discussed throughout the paper, the proposed algorithm aims at pinpointing free-riders in the network, and, for this goal, we assume that malicious nodes don’t present other behavior besides that covered in the article.

The reader’s point is, however, very interesting, and relates closely to what we are considering now — the problem of Sybil attacks. In a Sybil attack, a node can enter the network multiple times with different identities, all of which could in turn tell the network that their experiences with the other identities of the same node are always successful. That would cause them all to get highly positive reputations, even if they (actually, the single node with the multiple identities) denied service to the rest of the network. The problem here is the same as in the reader’s question: the joint effect of multiple votes for or against some node’s reputation, orchestrated to get a specific result. Although our model takes into account a node’s personal experience with the nodes that provide testimonials, that’s not enough if a group acts cooperatively.

The exact effect of such cooperative behavior depends on the number of nodes in the group of cheaters in relation to the overall population. If the group is small, their behavior might not be as effective. In this case, the number of fair nodes could be high enough for their votes to outweigh those of the group. However, as the number of cheaters grows, so does their effect on the final outcome. Our model in the article doesn’t consider such scenarios, as we mentioned earlier. We’ve been working on a new model, which extends the pattern of interaction to set rules about when a node should take some other node’s personal experience into consideration, even when $\beta = 1$. Our preliminary results show a much improved behavior, in which the network is able to isolate such groups in cases where the original model fails. As the authors of the original paper on the Sybil attack point out, however, if the group of cooperative cheaters grows, they will always end up overwhelming the others.

Reference

— Email letters to the editor to Rebecca Deuel, rdeuel@computer.org.