# Reliable communication, unreliable networks

August 5 2013, by Larry Hardesty

Now that the Internet's basic protocols are more than 30 years old, network scientists are increasingly turning their attention to ad hoc networks—communications networks set up, on the fly, by wireless devices—where unsolved problems still abound.

Most theoretical analyses of ad hoc networks have assumed that the communications links within the network are stable. But that often isn't the case with real-world wireless devices—as anyone who's used a cellphone knows.

At the Association for Computing Machinery's Symposium on Principles of Distributed Computing in July, past and present researchers from the Theory of Distributed Systems Group at MIT's Computer Science and Artificial Intelligence Laboratory presented a new framework for analyzing ad hoc networks in which the quality of the communications links fluctuates. Within that framework, they provide mathematical bounds on the efficiency with which messages can propagate through the network, and they describe new algorithms that can achieve maximal efficiency.

"There's been a discrepancy between the theory, with its idealized models, and the reality of wireless networks," says Nancy Lynch, the NEC Professor of Software Science and Engineering at MIT and head of the Theory of Distributed Systems Group. "When people start designing theoretical algorithms, they tend to rely too heavily on the specific assumptions of the models. So the algorithms tend to be unrealistic and fragile."

In the past, some researchers have tried to model the unreliability of network links as random fluctuations. "But if you assume real randomness, then you can count on the randomness," Lynch says. "Somehow you can use that in your algorithm. Maybe randomness itself is giving you an assumption that's too strong."

## Adversarial relationships

So Lynch and her coauthors on the new paper—Mohsen Ghaffari, a graduate student in electrical engineering and computer science, and Cal Newport, a former graduate student in Lynch's group who's now an assistant professor of computer science at Georgetown University—instead modeled the fluctuations in the links' quality as the willful manipulations of an "adversary." The adversary can't control all the links in the network: Some will remain up throughout the execution of the communication algorithm. But he can change the bandwidth of the others at will. And the network designer doesn't know in advance which links are reliable and which aren't.

"Your algorithm needs to work for all possible adversaries, some of which are benign and some of which might be doing the worst possible thing for your algorithm," Newport says. "In other words, it needs to work for all possible strategies for controlling the network."

In a paper that appeared two years ago, Newport, Lynch and colleagues assumed a very powerful adversary indeed—one that knew in advance every decision that every node in the network would make while trying to disseminate a message. In that context, they proved, efficient communication is impossible.

In the new paper, they weakened the adversary significantly. He may know exactly how the communications algorithm works, and he may intentionally try to thwart it, but he has to determine his pattern of link manipulation in advance, before the algorithm begins to run. Even this weakened adversary, however, has the potential to be much more disruptive than the types of interference that real-world wireless networks are likely to encounter—such as doors opening and closing, people turning on microwaves, or rain falling.

Lynch, Newport and Ghaffari examined two types of message dissemination. In the first, a single node of the network is trying to broadcast a message to all other nodes. In that case, they found, efficient communication is possible, even in the adversary's presence.

## Geometrical supposition

The second case is that in which a number of nodes are each transmitting messages, and every one of their immediate neighbors has to receive a message from at least one transmitter. As it turns out, many common problems in the analysis of ad hoc networks boil down to this one.

Here, the researchers found that the adversary's presence can thwart efficient communication—but only if the network has an odd shape, in which a central node is connected to many nearby nodes that aren't connected to each other. That type of network layout is improbable in the real world: If two wireless devices are close enough to a third to communicate with it, they're likely to be able to communicate with each other, too.

Once the researchers added another assumption—that two devices connected to a third will at least sometimes be able to establish links with each other, too—efficient communication again becomes possible.

In both cases, the researchers' communication algorithms were able to thwart the adversary by using randomness. One of the problems with designing communications protocols for ad hoc wireless networks is that if two nearby nodes begin transmitting at the same time at the same frequency, they can interfere with each other, preventing either transmission from being received. The best-performing protocols thus assign each node a probability of transmitting during any one round of communication (where a round is defined by the time it takes for a node to send a message to its immediate neighbors).

The MIT researchers' algorithms adhere to this basic scheme—but rather than cycling through a prescribed sequence of steadily shrinking probabilities, they scramble the sequence up. In the case of the local broadcast, each separate message has to have its own unique sequence of probabilities. So clusters of nodes also temporarily elect local leaders that coordinate the probabilities for different transmitters. The researchers were able to show, however, that this extra computation didn't slow communication egregiously.

Provided by Massachusetts Institute of Technology

Citation: Reliable communication, unreliable networks (2013, August 5) retrieved 6 May 2024 from https://phys.org/news/2013-08-reliable-unreliable-networks.html