

Sorting e-mail friends from foes

Identifying networks of mutual friends helps filter out spam.

Philip Ball



Around 60% of all emails are spam.

© Comstock

A simple and easily implemented scheme for combating e-mail spam has been devised by two researchers in the United States.

The technique exploits the structure of social networks to quickly determine whether a given message comes from a friend or a spammer. The method works for only about half of all e-mails received - but in all of those cases, it sorts the mail into the right category¹.

The system sidesteps many of the problems encountered with most available spam filters. It is simple and fast, and seems to never reject legitimate messages under the false impression that they are spam.

P. Oscar Boykin and Vwani Roychowdhury of the University of California, Los Angeles, who devised the system, say their method should prove highly effective when paired up with more sophisticated, but more cumbersome, filtering methods. Such a combination should be able to properly sort all incoming mail.

"It sounds like a perfectly reasonable idea," says Mark Newman, a network specialist at the University of Michigan. "It's clearly based on things we know about, such as the social structure of e-mail networks."

Friends of friends

The war against spam has never looked bleaker - about 60% of all e-mails are spam. At the World Economic Forum in Davos, Switzerland, in January, Microsoft chairman Bill Gates predicted that spam will soon be a thing of the past, thanks to software being developed at his company. But beleaguered computer users are unlikely to believe this until they see it.

Boykin and Roychowdhury decided to tackle the problem by taking advantage of the fact that most people's e-mail comes from a limited social network, and these networks tend to be clustered into clumps where everyone knows each other. If Alice knows and e-mails Bob and Chris, for example, then Bob and Chris are far more likely to know and e-mail each other than if they didn't share a friend in common. E-mails radiating from a spam source don't share this clustering property - the vast majority of recipients don't know each other.

The method effectively turns the spammers' weapon on themselves. The very fact that they can send out so many messages secures their low overall degree of clustering - it's what gives them away.

Problem halved

The e-mail clusters can be mapped out by inspecting the 'from', 'to' and 'cc' fields in a user's inbox. An automated system can quickly build up a blacklist of spammers, as well as a 'whitelist' of approved sources.

Boykin and Roychowdhury found that by quantifying the clustering of incoming e-mails, they could eliminate about 54% of spam. E-mails above a certain 'clustering threshold' are always friendly, and those below a lower threshold are always spam. Messages that fall between these two clustering thresholds are 'don't knows' - the system can't be sure how to classify them. Typically, say the researchers, this applies to about 50% of the mail received.

The remaining half of the e-mail then has to be filtered in a more sophisticated way. But by then the scale of the problem has been cut in half.

References

1. Boykin, P. O. & Roychowdhury, V. Personal email networks: an effective anti-spam tool. *Preprint*, <http://www.arxiv.org/abs/cond-mat/0402143>, (2004).

Nature ISSN 1744-7933 EISSN 1476-4687

[About NPG](#)

[Contact NPG](#)

[Accessibility statement](#)

[Help](#)

[Privacy policy](#)

[Use of cookies](#)

[Legal notice](#)

[Terms](#)

[Naturejobs](#)

[Nature Asia](#)

[Nature Education](#)

[RSS web feeds](#)

[About Nature News](#)

[Nature News Sitemap](#)

Search:

go

© 2016 Macmillan Publishers Limited. All Rights Reserved.

partner of AGORA, HINARI, OARE, INASP, ORCID, CrossRef, COUNTER and COPE