Misinformation diffusing online

July 31 2014

The spread of misinformation through online social networks is becoming an increasingly worrying problem. Researchers in India have now modeled how such fictions and diffuse through those networks. They described details of their research and the taxonomy that could help those who run, regulate and use online social networks better understand how to slow or even prevent the spread of misinformation to the wider public.

Krishna Kumar and G. Geethakumari of the Department of Computer Science and Information Systems, at BITS-Pilani, Hyderabad Campus, in Andhra Pradesh, India, explain how we are increasingly reliant on information we obtain from online sources. However, our implicit faith in the validity of that information can be counterproductive and can make some people and organizations vulnerable to exploitation, perhaps by those spreading the [misinformation](#) and others. The team refers to this as a "semantic attack" and regards it as the "soft underbelly of the internet".

The team suggests that online social networks have added an additional layer of challenges for the detection of such semantic attacks above the conventional world-wide web and other internet services. As such, the rate of diffusion of misinformation can be very rapid as evidenced by recent events driven by panic spreading online regarding so-called "swine" flu in 2009 and a mass exodus from an Asian nation also driven by unnecessary online panic.

As with the transfer of information through any network, the nodes (the

users in a social network) and how they are connected to each other is also critical to the diffusion of misinformation, the researchers report. For example, friendship links on Facebook and the follower/followee relationship on Twitter affect the impact and reach of given updates on those services from particular users.

Connections and connectivity have been well studied in recent years, but the concept of a semantic attack in which misinformation is deliberately seeded into a social network with the aim of affecting the behavior of the maximum number of people possible has only recently emerged as a troubling concept that requires detailed study. While there are firewalls, antivirus programs and other technological diagnostics and defenses to ward off attacks on servers, operating systems and software, defending against the impact of a semantic attack on human emotions and behavior is an entirely different matter.

  More information: *Int. J. Communication Networks and Distributed Systems*, Vol. 13, No. 2, pp.119–143.

Provided by Inderscience Publishers