Ad Hoc and P2P Security

Shiuhpyng W. Shieh
National Chiao Tung University & University of California, Berkeley

Dan S. Wallach
Rice University

When we speak of peer-to-peer (P2P) technologies, we're generally thinking about "overlay networks" built on the existing Internet out of end users' computers. P2P systems today can easily scale to support millions of nodes, cooperatively storing and replicating data in distributed hash tables (DHTs), and letting messages be efficiently routed among network nodes. These underlying techniques enable a growing and exciting array of applications, including distributed data storage, distributed bandwidth sharing, and multicast data distribution. They even give us a chance to rethink low-level network routing protocols. P2P, for example, is about a lot more than pirate downloads – it lets communities of like-minded users pool otherwise wasted resources to achieve robust performance without a costly centralized infrastructure.

Similarly, mobile ad hoc networking and sensor networks have a promising future in which low-cost, lightweight devices with limited computational and battery resources will be able to communicate with each other to form mesh networks. This can enable an extensive array of applications ranging from environmental sensors to devices for emergency communications that work when other wireless infrastructure has been damaged or destroyed. Ad hoc networks could ultimately be used on the battlefield, in forests, or even in outer space.

As the number of individual computing devices and the demand for mobility continue to grow, P2P systems and ad hoc networks will become increasingly popular. Indeed, they are likely to become integral to the future computing and networking infrastructure. P2P systems create application-level virtual networks with their own routing mechanisms; they enable large numbers of computers to share information and resources directly, without dedicated central servers. Ad hoc networks let mobile hosts, mobile devices, and sensor nodes communicate when no fixed infrastructure is available.

Securing P2P Networks

Unfortunately, security concerns have inhibited widespread use of both P2P and ad hoc networks. What happens if some of the nodes in your network are malicious and want to corrupt the network's behavior? Such malice can take various forms, from freeloading to denial-of-service attacks, and without adequate security mechanisms and settings, users are especially vulnerable. Although numerous researchers in both the P2P and ad hoc networking communities have worked on

 Published by the IEEE Computer Society 1089-7801/05/$20.00 © 2005 IEEE

addressing some of these flaws, existing solutions are still quite limited. Solving security problems without being able to trust nodes to operate correctly is quite difficult. Furthermore, without any kind of central, trusted administration, which might be infeasible for some of these networks, these security problems are likely to remain open research problems.

In this Issue

Five interesting articles presented in this special issue of *IEEE Internet Computing* explore several research trends in these areas, including the design of reputation systems, the deployment of trusted computing technologies, the secure construction of overlay routing networks in P2P systems, and the detection of malicious nodes in ad hoc networks.

Girish Suryanarayana, Justin R. Erenkrantz, and Richard N. Taylor address the issue of reputation systems in "An Architectural Approach for Decentralized Trust Management." They present Pace, an architecture-based approach that guides developers in how to incorporate trust models into decentralized applications. Additionally, they survey many of the possible benefits that P2P systems might achieve through the use of reputation systems.

In "Trusted P2P Transactions with Fuzzy Reputation Aggregation," Shanshan Song, Kai Hwang, Runfang Zhou, and Yu-Kwong Kwok also look at the reputation problem in P2P systems. Given that nodes can be malicious, reputation systems can reward good nodes for their behavior as well as let peers detect misbehaving nodes and, presumably, eject them from the network. The authors' FuzzyTrust system tackles the reputation problem using fuzzy logic inferences and storing reputation information in a DHT.

Thomas M. Chen and Varadharajan Venkataramanan look at the problem of malicious node detection in ad hoc networks in "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks." Unlike in P2P systems, nodes in ad hoc networks can speak only to neighbors within radio range (rather than to any node). Individual nodes in the ad hoc network might observe evidence of misbehavior, but the nodes as a group must combine that evidence to create a convincing case that a particular node is malicious. This article presents some formalisms that can help with such determinations.

In "Enhancing Data Authenticity and Integrity in P2P Systems," Xinwen Zhang, Songqing Chen, and Ravi Sandhu look at the application of trusted computing technologies to P2P systems. Such technologies add a variety of new features to computers, such as the ability to securely store cryptographic secrets or even to attest to another computer, over the network, that a particular application and operating system is being used. This article proposes a trusted reference monitor, running on every client, that can digitally sign all network requests such that other P2P nodes can validate that a corrupted P2P application should be ignored by its peers.

Finally, "A Novel Methodology for Constructing Secure Multipath Overlays," by Marc Sánchez Artigas, Pedro García López, and Antonio F. Gómez Skarmeta, focuses on the secure construction of the overlay routing network that underlies most P2P systems. When any node has the potential to be malicious, routing becomes quite fragile given that malicious nodes can misroute any messages that pass through them. Furthermore, any routing update can be corrupted to always refer only to malicious nodes and their coconspirators. This article evaluates *multiple independent path routing* as a technique for increasing the odds that messages will successfully reach destination nodes.

In this special issue, we examine the rapidly expanding fields of P2P and ad hoc networking. These fields clearly introduce several new security challenges, and are especially relevant in light of recent rapid expansion of P2P networking over the Internet. Together, these works present important topics for computer security in these areas, and they might also lead to future development and deployment of efficient and powerful P2P and ad hoc networks.

Shiuhpyng W. Shieh is a professor and former chairman at National Chiao Tung University, President of Chinese Crypto and Information Security Association, and currently a visiting professor at University of California, Berkeley. His research interests include network security, wireless sensor web, and intrusion detection. Shieh has a PhD in electrical and computer engineering from the University of Maryland, College Park. Contact him at ssp@csie.nctu.edu.tw or spshieh@eecs.berkeley.edu.

Dan S. Wallach is an associate professor at Rice University. His research interests include the security of peer-to-peer and distributed systems as well as the security of voting systems. Wallach has a PhD in computer science from Princeton University. He is a member of the IEEE, the ACM, and Usenix. Contact him at dwallach@cs.rice.edu.