Experimental Study of Accountability in Existing Anonymous Networks

PIs: Yingfei Dong, University of Hawaii, yingfei@hawaii.edu NSF1041739
Zhenhai Duan, Florida State University, duan@cs.fsu.edu NSF1041677


Yingfei Dong


Zhenhai Duan

Objectives

- Develop design guidelines for p2p anonymous networks (p2pANs)
- Evaluate the design and implementation choices in existing p2pANs
- Generalize quantitative measures to evaluate the strength of p2pANs
  - not simply attacking them
- Key research issues
  - anonymity strength
  - tradeoffs between anonymity and usability/performance
  - anonymous routing mechanisms

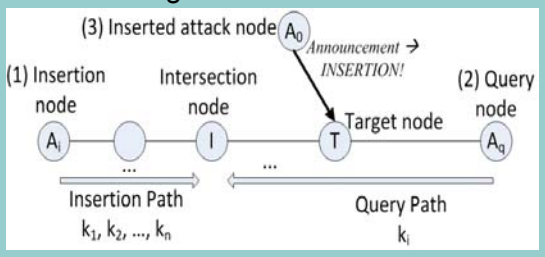
Approach

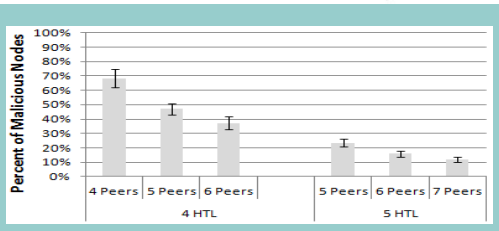
- Analyze Freenet code to identify critical quantitative measures for anonymous systems
- Develop experimental and simulation testbeds for systematically analysis
  - Testbed on VMware private cloud
  - Testbed on Emulab
  - Simulation testbed and system model
  - Graphical analysis tools

Research Highlights

- Identified practical attacks that seriously damage the anonymity strength of Freenet and similar DHT-style systems.
- Developed two effective attacks on Freenet
  - Routing Table Insertion (RTI) attack: insert a malicious peer into a target peer's routing table. A base for many other attacks.
  - Traceback attack: find the origin of a query → break anonymity!
- Freenet responded with a quick fix, 9/11/12
  - https://freenetproject.org/news.html#2012-traceback-attack
  - Long-term solutions under investigation.
- Project Web site
  - http://www.ee.hawaii.edu/~dong/traceback/index.htm

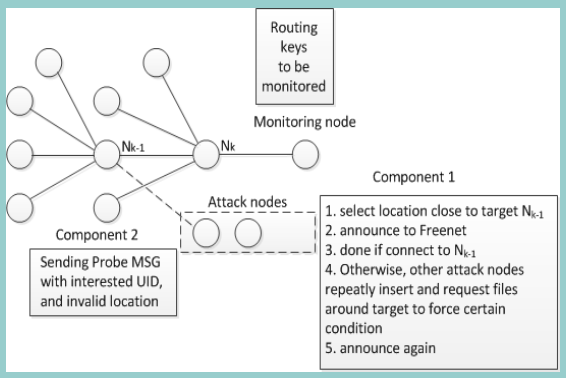
Routing Table Insertion Attack





Attack resources needed to target 100% of nodes in a network, using the attack pairs with the minimum coverage.

Traceback Attack



Find the sender: determine the originating machines of 24% to 43% of messages.

Ongoing work

- Develop generic attacks on p2pANs
- Investigate countermeasures to attacks
  - Preventing attackers from exploiting self-organizing nature of p2pANs
  - Provide good performance with controlled anonymity
- Continuing investigating security of Freenet and other p2pANs such as GNUNet
- Extracting design and development patterns in building strong p2pANs

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD