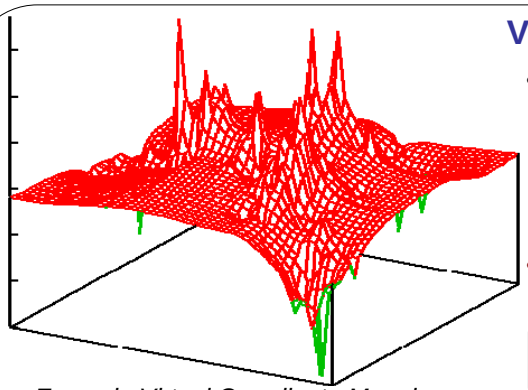
CERIAS

the center for education and research in information assurance and security

On the Accuracy of Decentralized Network Coordinate Systems in Adversarial Networks

David Zage and Cristina Nita-Rotaru

Department of Computer Science and CERIAS, Purdue University



Example Virtual Coordinate Mapping

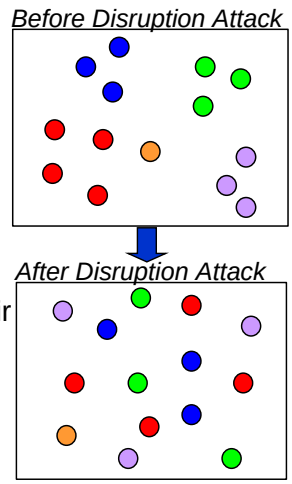
Virtual Coordinate Systems

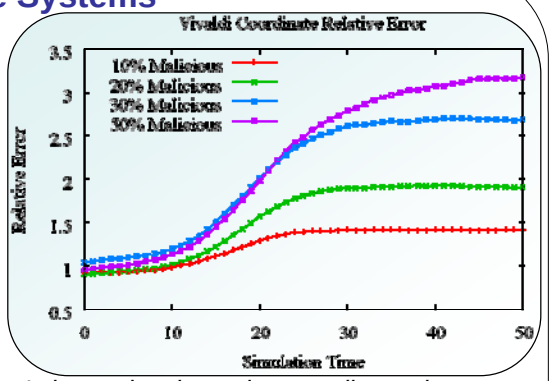
- Many P2P systems optimize their performance based on network topology, including:
  - file download and distribution (BitTorrent, Emule)
  - voice over IP (Skype)
  - video broadcasting (ESM, Coolstreaming, and PPLive).
- **Virtual coordinates** allow hosts to determine the latency to arbitrary hosts without using explicit measurements (periodic probing).

Our Goal - Make virtual coordinate assignment and upkeep robust to malicious attackers.

Insider Attacks on Virtual Coordinate Systems

- **System Design:**
  - Developed to provide accuracy under the assumption nodes are altruistic.
  - Vulnerable to malicious attacks coming from inside the system
- **Attacker capabilities:**
  - A fraction of nodes has access to all data stored on the compromised node
  - Compromised nodes can lie about their coordinates and metrics
- **Results of the attacks:**
  - System instability and coordinate inaccuracy





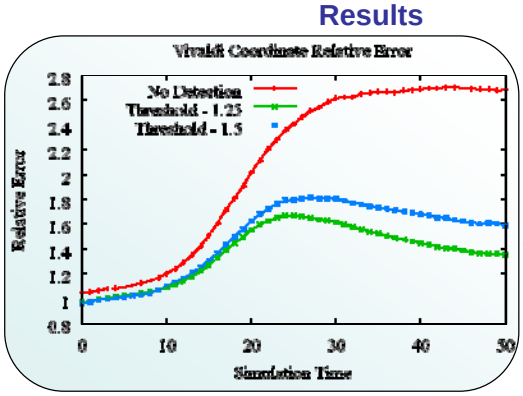
Lying nodes determine coordinate changes and decrease the accuracy in a simulation of the Vivaldi virtual coordinate system over the King data set.

Mitigating Insider Attacks

Defense Mechanisms

- **Reducing incorrect adaptations** – Constrain the ability of an attacker to cause malicious adaptation by using anomaly detection based on a combination of multi-metric correlation and statistical outlier detection.
  - Consistent with what the other nodes have reported
  - Consistent with what it said in the past
- **Increasing stability** – Increase system stability and coordinate accuracy by explicitly integrating defense mechanisms into the adaptation process.

Results



This graph demonstrates the ability of statistical outlier detection in mitigating the effects of 30% malicious nodes in the virtual coordinate system lying about their metrics

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center