

Gaia: A Self-organizing and Self-healing Network Infrastructure

Ben Y. Zhao, <http://current.cs.ucsb.edu>



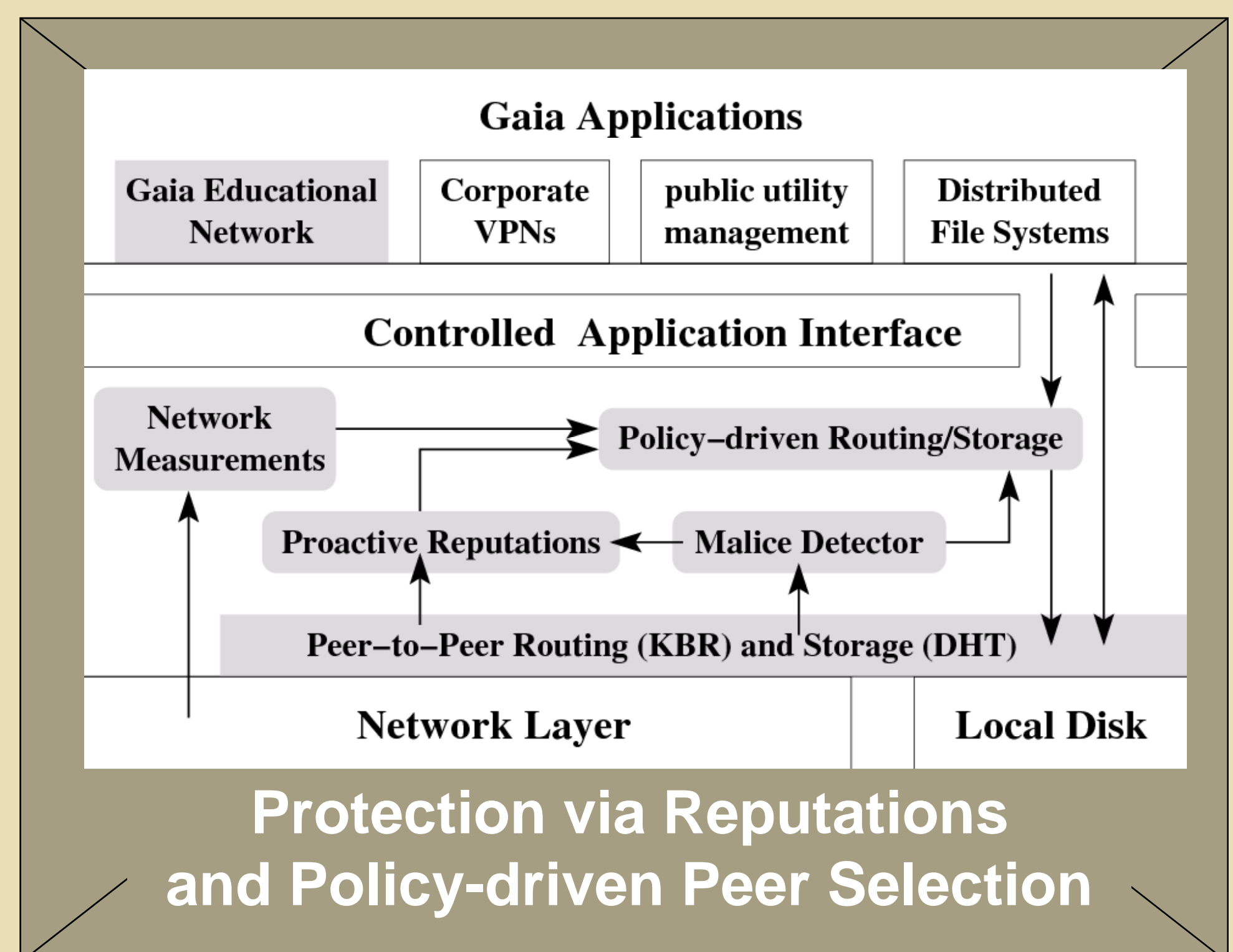
Protecting Network Applications using Reputations and Invariant Checking

Gaia protects applications proactively (reputations) by avoiding untrustworthy peers, and reactively (attack detection) by detecting and marking attackers.

Focus on two goals:

1. Apply use of reputations to nodes in peer-to-peer systems
2. Study invariants of structured overlays to detect anomalous behavior and attacks

Applications like distributed file systems and content delivery networks can proactively avoid peer failures and attacks.



Approach and Impact

New approach

- Reputation reliability metric
- Proactive reputations to probe unknown peers
- Constraint-based attack detection

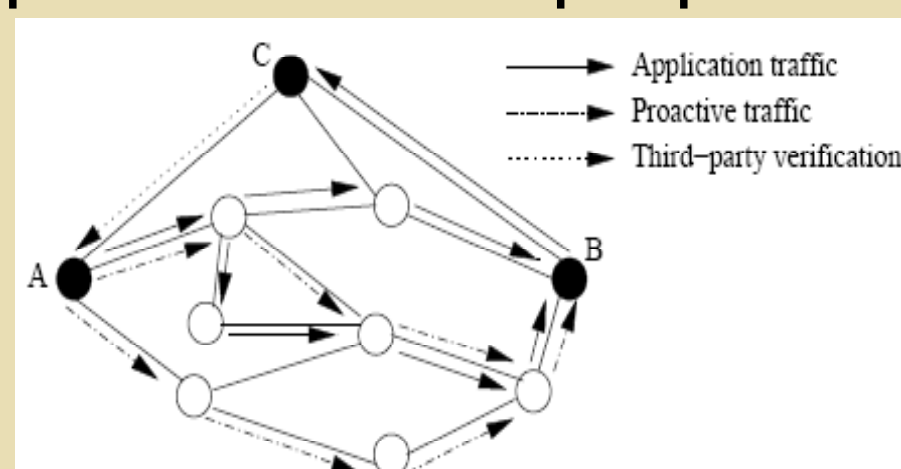
Research Impact

- Predict accuracy of reputation
- More accurate reputations for short lived hosts
- Low cost detection of Identity attacks

Building Reliable Reputation Systems

- Gaia uses reputations to guide policy-driven routing and peer selection
- Challenge: reputations are **not** "reliable" Inaccurate in highly dynamic environments, and fooled by collusion and Sybil attacks
- Approach 1: **reputation reliability metric** Heavily weigh # of peers interacted with, and account for # of total transactions recorded
- Approach 1: **proactive reputations** For peers with unreliable reputations, "test" them with proactive requests for sole purpose of evaluation.

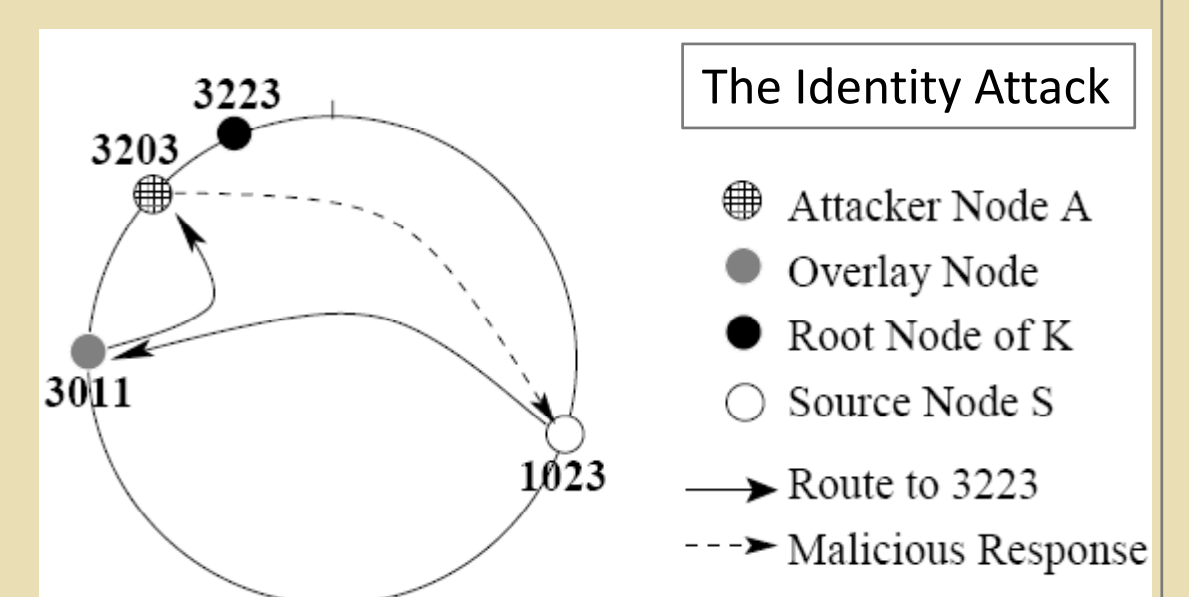
Must make requests anonymous and blend in with normal traffic.



Protecting Overlays from Identity Attacks

- Structured overlays map application components to peer via key-based routing

- KBR messages can be **hijacked** en route



- Attacker controls app component (e.g. X becomes storage manager for file Y)

- Detection via dissemination of **existence proofs** and probabilistic verification. Attackers get negative feedback.

