

Intrusion-Tolerant Dissemination

Kim P. Kihlstrom, Westmont College

<http://starfish.westmont.edu/>



Gossip-Based Communication Protocol for Survivability in Large-Scale Systems

Problem

With increased demand for Web Services has come a heightened need for scalable wide-area communication systems. The need for trust in such systems and the vulnerability of such systems to attack provide motivation to develop protocols that are intrusion-tolerant and able to provide critical services even during an attack or in the presence of arbitrary faults, errors, and accidents.

Starting Point: Gossip-Based Protocol

Scalable

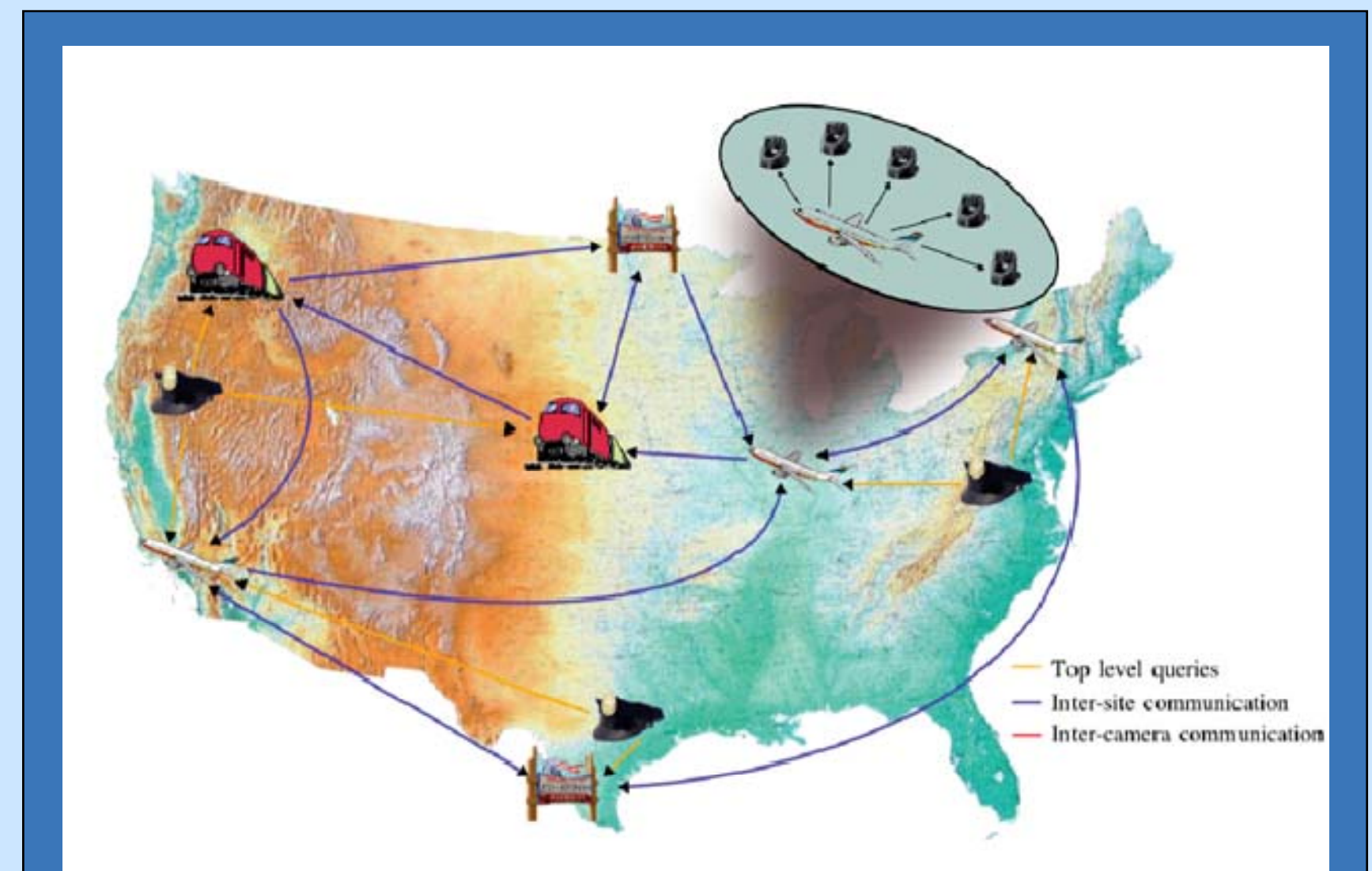
- P2P interaction model
- Self-organizing
- Decentralized
- Size of local view $O(\log N)$

Reliable

- Resilient to link and node crash faults
- Randomized to tolerate random unreliability

End Result: Intrusion-Tolerant Protocol

Developed a new intrusion-tolerant gossip-based communication system that is resilient to arbitrary (Byzantine) faults and malicious attack



Example Application:
National Surveillance System

A national surveillance system such as the one shown above would require a communication protocol that is intrusion-tolerant as well as scalable and reliable.

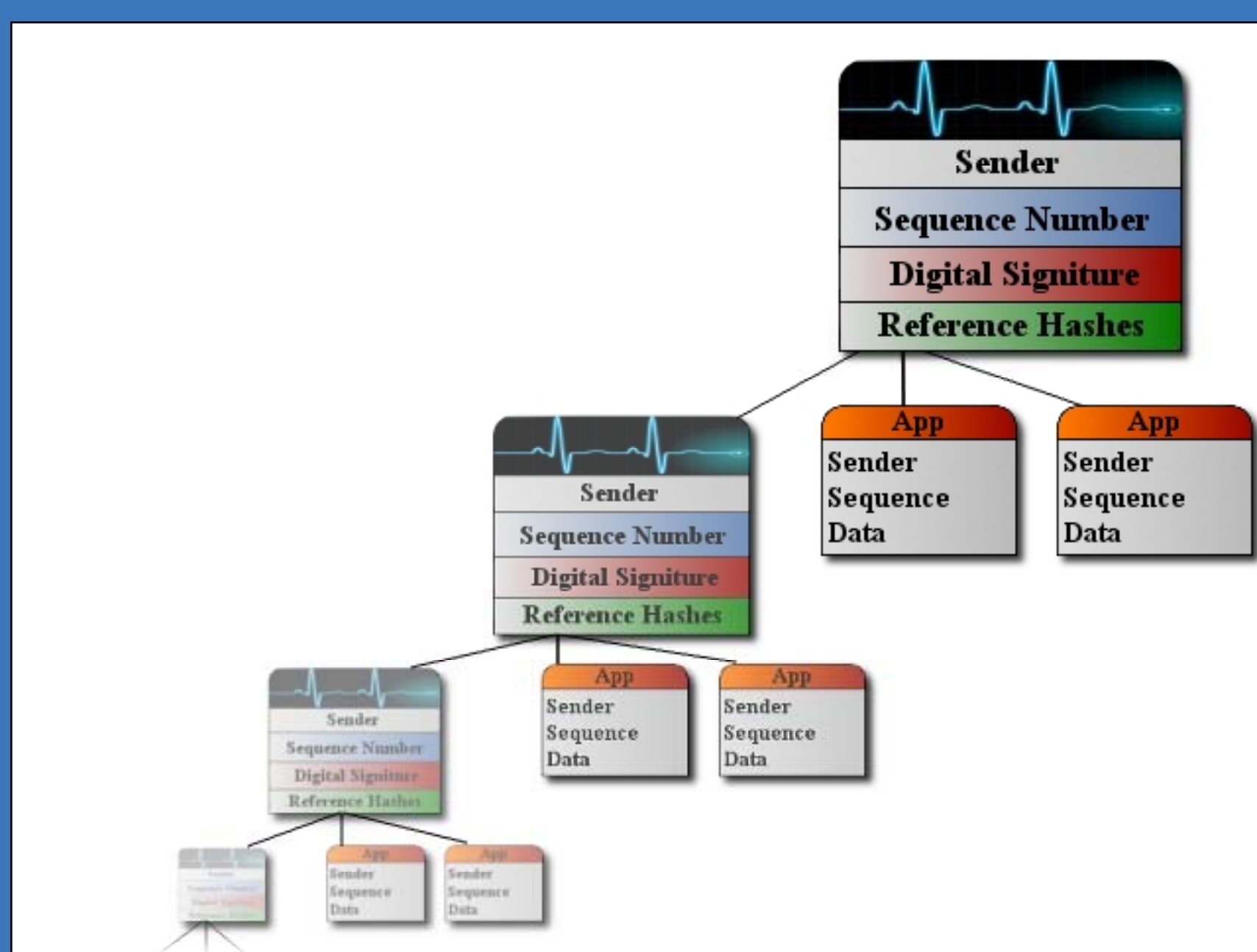
Approach and Impact

Approach

- Modular transformation technique
- Chain of heartbeat messages

Research Impact

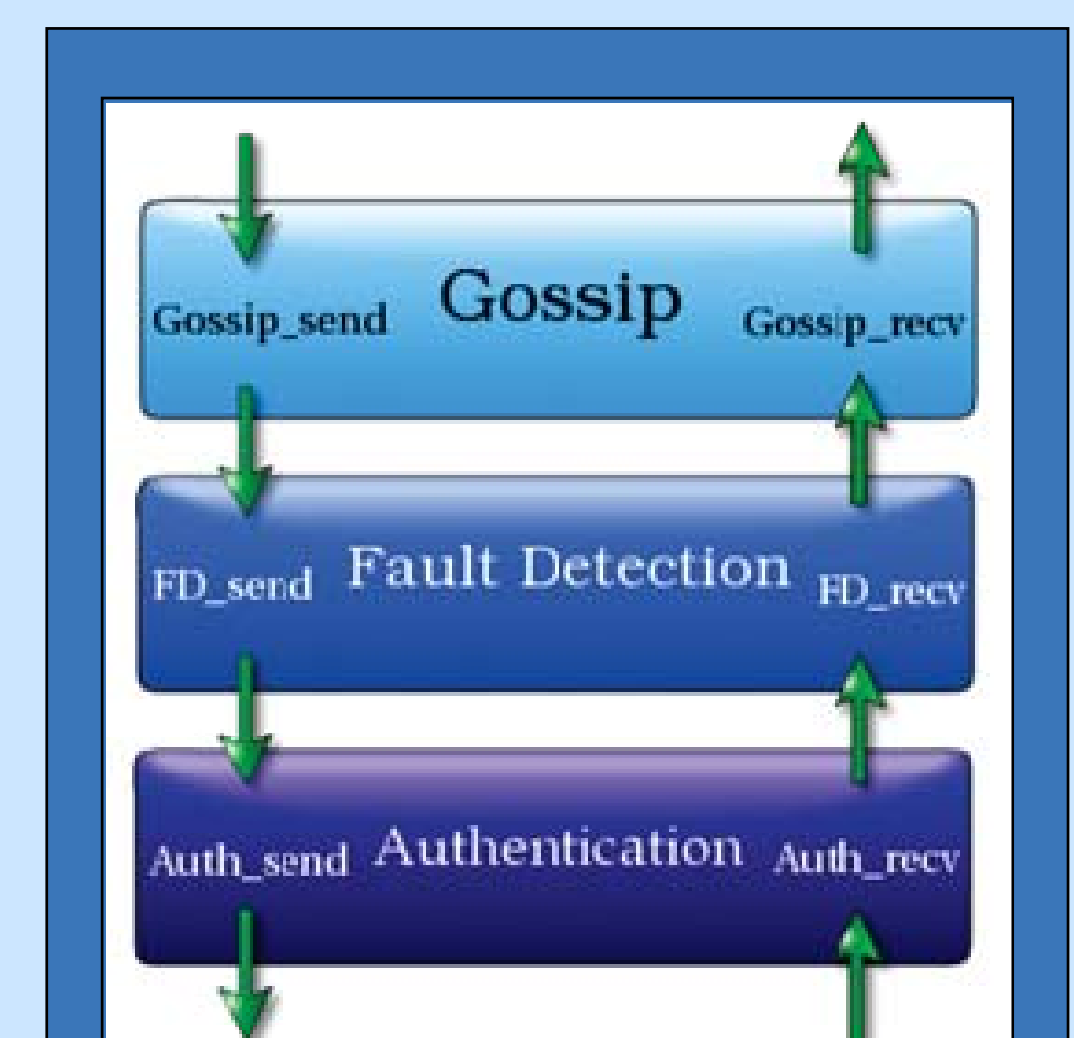
- Crash-tolerant protocol → intrusion-tolerant protocol
- One signature covers many application messages



Chain of Heartbeat Messages

We employed a modular approach to the design, and built on prior work that generalizes the transformation of crash-tolerant protocols to Byzantine-tolerant protocols.

Our protocol avoids the need for signatures on application messages by making use of a novel message chaining technique to achieve efficient and secure message delivery.



Modules