CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Newton Meets Vivaldi:

Securing Virtual Coordinates by Enforcing Physical Laws

Jeff Seibert and Cristina Nita-Rotaru
Department of Computer Science and CERIAS
Purdue University

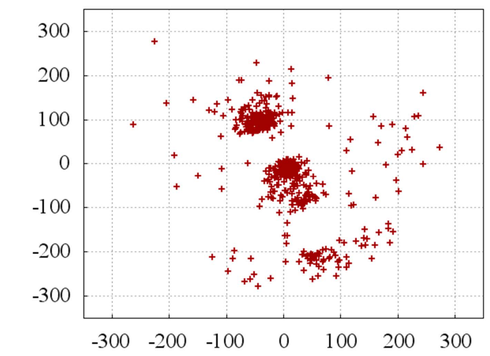
Sheila Becker and Radu State
Interdisciplinary Centre SnT
University of Luxembourg

Virtual Coordinate System (VCS)

Distributed systems can optimize performance by measuring latencies between nodes, but pair-wise measurements do not scale:

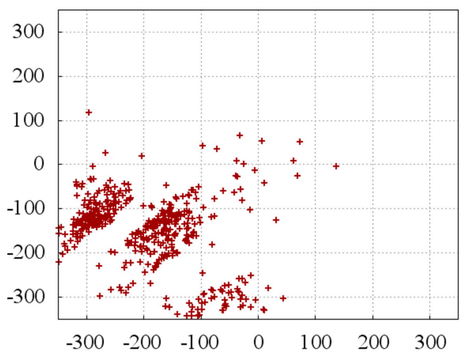
- VCSs embed the Internet onto a coordinate space
- Nodes estimate latencies by calculating the distance between coordinates
- **Vivaldi** is a popular decentralized VCS where nodes are logically connected via a physical spring
- Nodes update their coordinate according to Hooke's law (F=-kx)

Coordinate mappings of 500 nodes running Vivaldi on PlanetLab



Before attack

After frog-boiling attack



Attacks on VCS

Insider attackers can cause other nodes to have bad latency estimations by:

- Lying about their coordinate
- Delaying measurement probes

Previous Defenses and Frog-Boiling Attacks

Previous defense systems (i.e. Anomaly Detection and Voting Schemes) mitigate attacks by learning good behavior over time and discarding bad behavior:

- Frog-Boiling attackers **exploit the learning process** by staying underneath thresholds (which indicate an outlier) by lying by small amounts at a time.
- Previous defenses eventually re-learn bad behavior as good behavior

Newton

- Previous defenses failed because they must learn good behavior
- **Invariants** give us an unchanging standard

Key observation: Vivaldi is based on a physical system and therefore nodes should follow physical laws

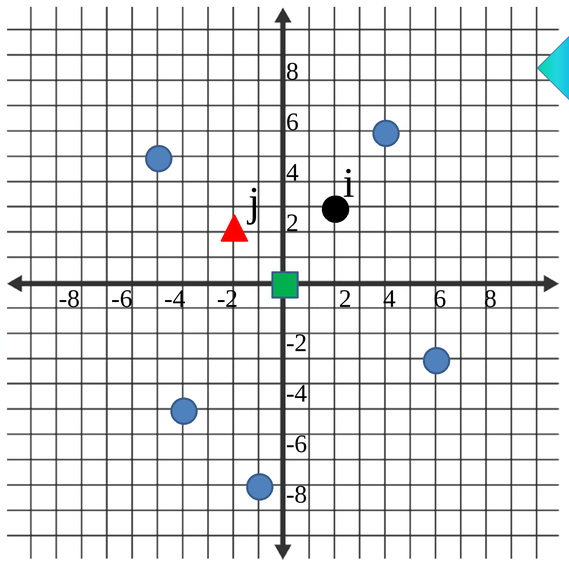
We derive three invariants based on **Newton's three laws of motion**:

- **Invariant 1**: Centroid of coordinates starts and stays at the origin (For every action there is an equal and opposite reaction)
- **Invariant 2**: Physically close nodes experience similar forces (A body stays at rest unless acted upon by an external unbalanced force)
- **Invariant 3**: Nodes will decelerate as their springs come to a resting position (F=ma & F=-kx)

If an attacker causes an invariant to be broken, we can figure out exactly who caused it!

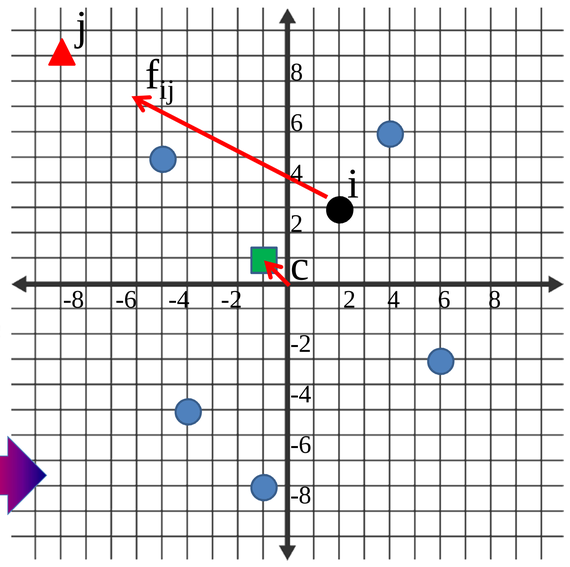
Example of Invariant 1

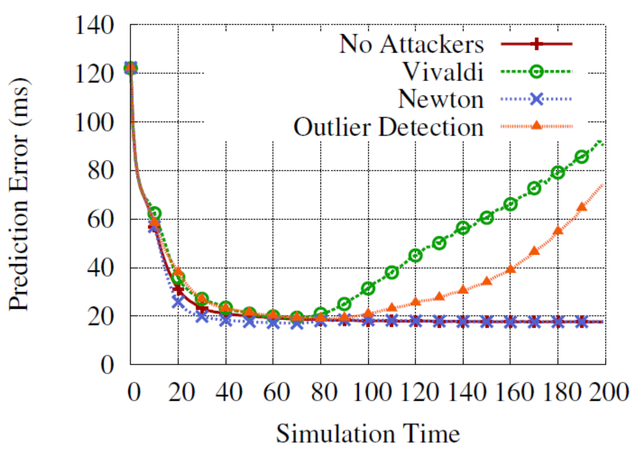
Legend:
Victim
Neighbor
Attacker
Centroid



Before attack, centroid is at the origin

After attacker lies about coordinate, centroid moves the same way attacker does, allowing us to pinpoint the attacker





Simulations results using the King data set with 1740 nodes, with 30% attackers conducting a frog-boiling attack

CERIAS

Discovery Park e-Enterprise Center