Newton Meets Vivaldi: Using Physical Laws to Secure Virtual Coordinate Systems

Jeff Seibert, Cristina Nita-Rotaru
Purdue University
{jcseiber, crisn}@cs.purdue.edu

Sheila Becker, Radu State
University of Luxembourg - SnT
{sheila.becker, radu.state}@uni.lu

1 Introduction

Virtual Coordinate Systems (VCS) have been proposed as an efficient and low cost service to provide network locality estimations by accurately predicting round-trip times (RTT) between arbitrary nodes in a network. Each node measures the RTT to a small number of other nodes and then can estimate the RTT between any two nodes. VCSs assign a set of coordinates to each node based on the estimated RTTs and a distance function. In a distributed and decentralized VCS, like Vivaldi [2], each node maintains and updates its own coordinate by relying on information received from other nodes.

Distributed VCSs have been shown [3] to be extremely vulnerable to insider attacks, where compromised nodes delay measurement probes and lie about their coordinates with the motivation to decrease system performance. As many applications rely on a VCS to build robust services, there have been several proposals to secure them using anomaly detection. However, these schemes are vulnerable to attacks where through small changes attackers make the defense mechanisms to learn malicious behavior as being good behavior. One such attack is the well-known frog-boiling attack where attackers lie by small amounts that accumulate over time and gradually lead to large changes in system performance [1].

2 Description of Newton

A classical approach in designing distributed systems is to use *safety invariants* in order to ensure system correctness. These safety invariants specify states into which the distributed system should never enter. At first glance, VCS do not appear to have such invariants as minimal constraints are imposed. We make the key observation that Vivaldi [2] is built upon an abstraction of a mass-spring system and therefore all nodes must follow physical laws. These laws are universal truths so they represent invariants that all nodes in Vivaldi should globally follow. In particular, we derive three invariants (**IN1**, **IN2**, and **IN3**) that are based on Newton's three laws of motion.

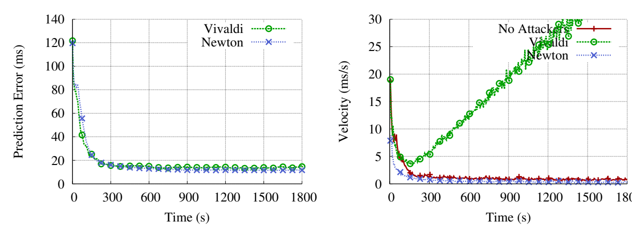
IN1: *If the centroid is not at the origin, then an attacker, has introduced an unbalanced force that has the same direction as a force vector from the origin to the centroid ($\vec{c}$).*

IN2: *Nodes i and k are physically close and if node i experiences a force $\vec{f_{ij}}$ from node j, then node i would expect node k to experience a force from j similar to the vector projection of $\vec{f_{ij}}$ onto the vector $u(x_j - x_k)$.*

IN3: *As the springs in the physical system stabilize and come closer to their rest position, nodes should decelerate and thus also the forces that are applied to them should decrease over time.*

3 Results

We implement Newton, a decentralized VCS which extends Vivaldi to withstand a wide class of insider attacks. When an update sent by a node violates an invariant, the recipient simply discards the update. We run experiments on Planetlab with 500 nodes. In Fig. 1(a) we find that Newton performs 25% better than Vivaldi in benign settings. We also find that Newton is able to mitigate the advanced frog-boiling attack in Fig. 1(b) even under 30% of attackers.



(a) No attack (b) Frog-boiling 30% attackers

Figure 1: PlanetLab results

References

[1] E. Chan-tin, D. Feldman, and Y. Kim. The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems. In *SecureComm*, 2009.

[2] F. Dabek, R. Cox, F. Kaashoek, and R. Morris. Vivaldi: a decentralized network coordinate system. In *Proc. of ACM SIGCOMM*, 2004.

[3] M. A. Kaafar, L. Mathy, T. Turletti, and W. Dabbous. Virtual networks under attack: Disrupting internet coordinate systems. In *Proc. of CoNext*, 2006.