Trust and Observability in Cyber Ecosystems

Ryan Hilger and Steve Simske, Colorado State University

In recent years, the cybersecurity field has become increasingly focused on managing the risk and resilience of ecosystems in response to deepening cyber threats, such as software supply chain attacks and counterfeit electronic parts.

- Exemplified by the push for software bills of materials (SBOM) and software transparency, highlighted by EO 14028, which mandates SBOM use in federal procurement to enhance supply chain trust.
- This research explores the quantification of trust in cyber ecosystems and the impact of ecosystem observability on trust through a novel framework that treats the cyber ecosystem as a collection of linear systems. Internal and external observations of each node facilitate evaluations of node- and network-level trust using a fading memory Kalman filter and a weighted geometric mean. A Monte Carlo analysis is performed to assess framework performance against several different parameters.

Key Concepts:

- Sociotechnical Trust: Sociotechnical trust is neither purely technical nor purely social. It has several attributes key to defining quantitative relationships: subjective, asymmetric, dynamic, measurable, and non-transitive.
- Observability: Feedback that provides insight into a process and refers to the work needed to extract meaning from available data (Woods and Hollnagel, 2006).
- Centralized Trust Calculation: Non-transitive calculation that assumes all nodes can be represented as a set of linear systems that capture the relationships, attributes, third party evidence affecting the node(s) and network, time delay, and variability. The (weighted) geometric mean provides a centralized trust score for the observed ecosystem.

Ecosystem as a Set of Linear Systems – Node Trust

$$T_i = \alpha_i * NE_i + \beta_i * EA_i + \epsilon_i$$

$$\alpha + \beta = 1$$

NE is Node-Based Evidence (Internal), EA is External Assessments

Ecosystem Trust Score by Geometric Mean

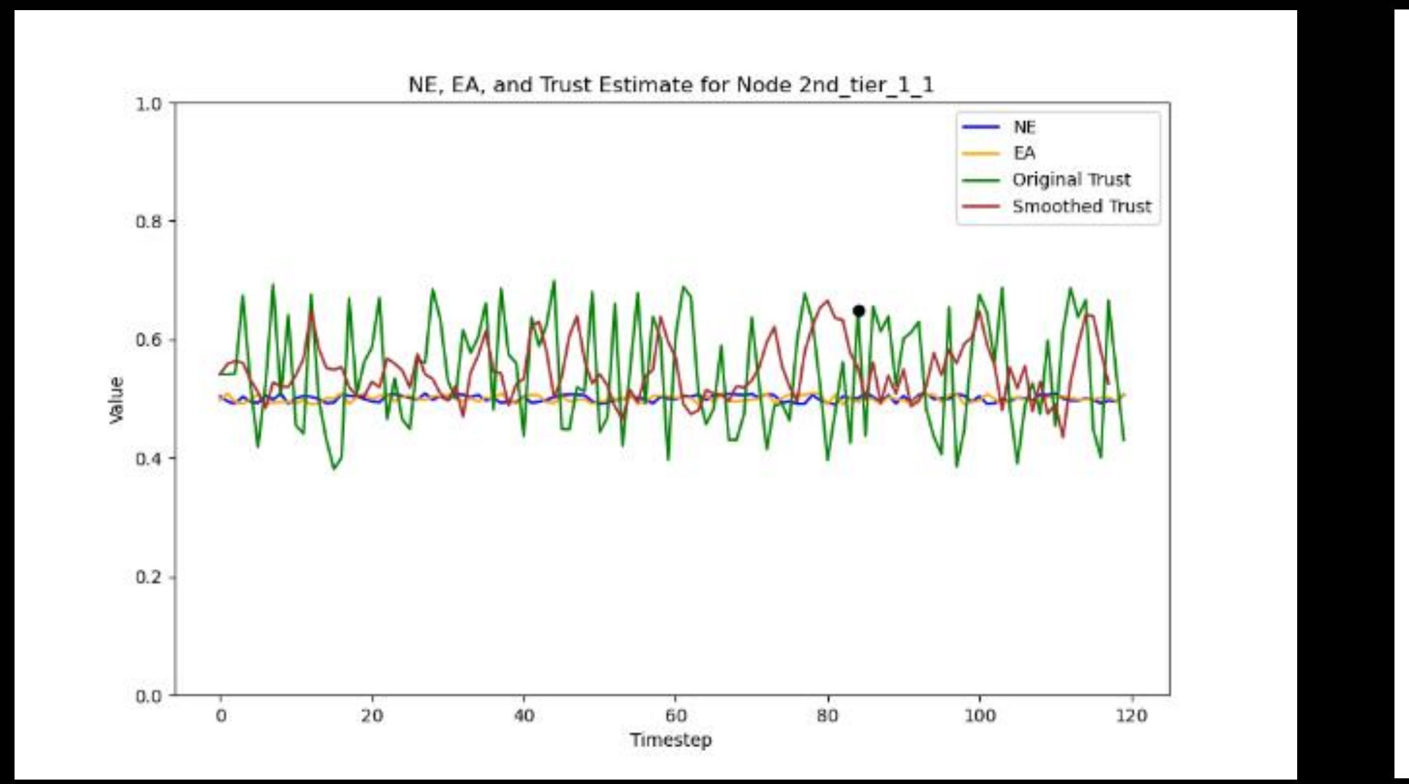
$$EcosystemTrust = (\Pi_{i=0}^{n} T_i * \omega_i)^{\frac{1}{n}}$$

ω_i is the weighting factor for the ith node

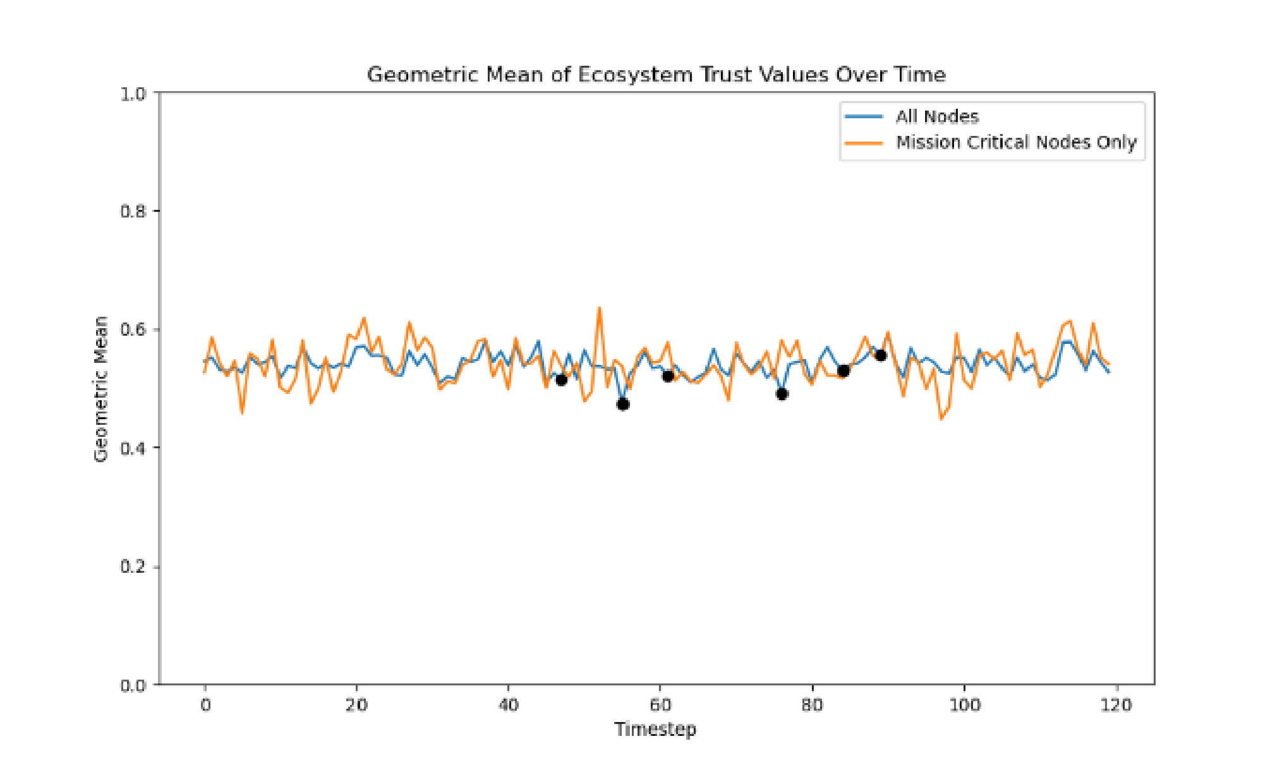
Three Part Experiment: 1) Implementation of the Fading Memory Kalman Filter for each node except the central node, which is assumed to be the organization seeking to observe and assess trust in its cyber ecosystem. Initial process and measurement variances are set high to account for the subjectivity in the model and the measurements. 2) The geometric mean is calculated for all nodes and for node designated "mission critical." 3) A Monte Carlo analysis of 1,000 runs to understand model variability for four different factors: 1) likelihood of a cyber event, 2) the weighting of the NE variable (does internal evidence hold more weight than external), 3) the fading factor for the Kalman filter, and 4) increasing the number of "observations" of the NE parameter.

Experimental Design and Results

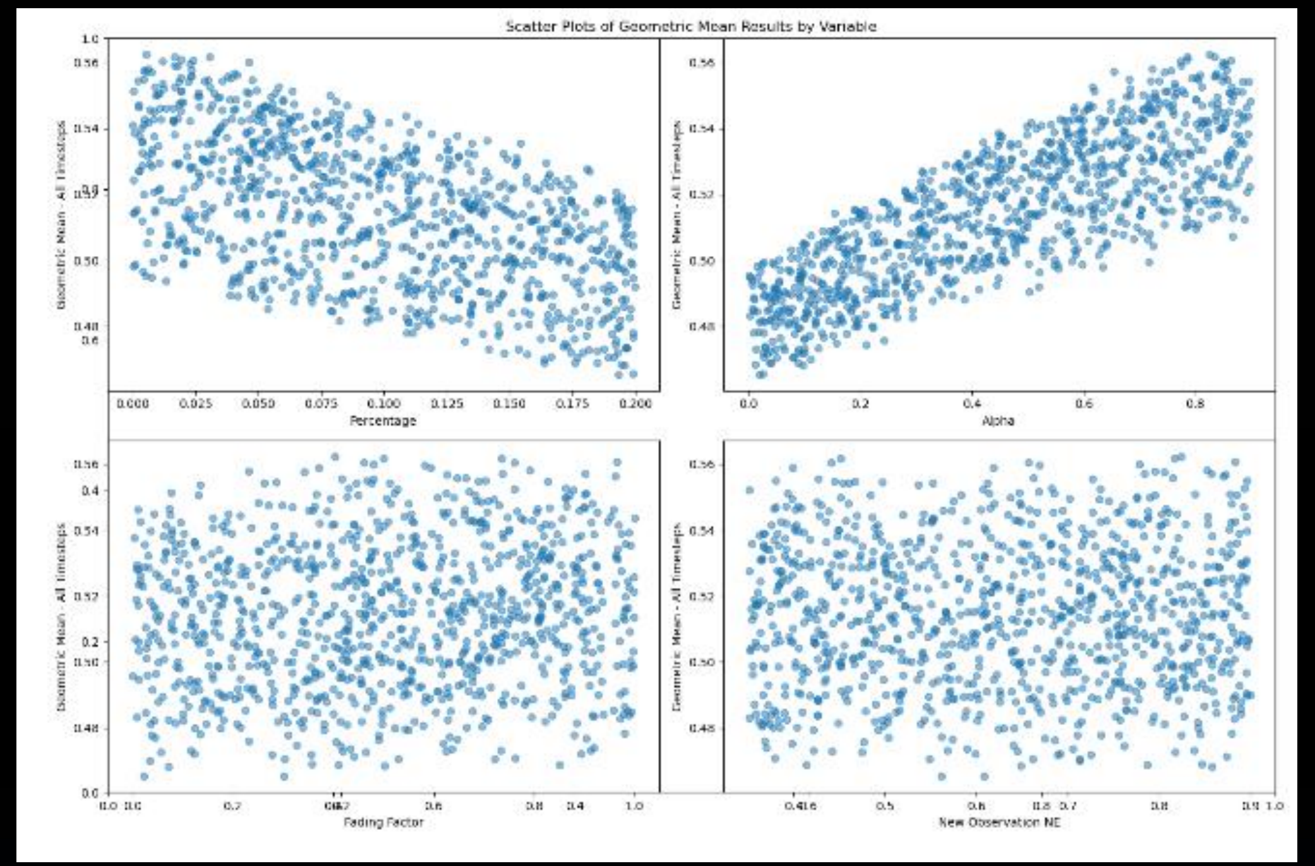
Results: 1) As the incidence of a cyber event goes up, mean ecosystem trust goes down, validating high-level model performance against expectations. 2) Trust increases when there are more NE observations. 3) Fading factor does not have a significant effect. 4) The number of NE observations did not significantly affect trust. Multiple linear regression validated results statistically with R^2 = 0.988 and F-statistic = 1.996e^{4}. Plots below show the results for each of the three parts of the experiment.



Plot of observations of NE, EA, and the trust estimate over time for a single node. Cyber incidents, if they occur, are marked with a black circle.



Geometric mean of ecosystem trust values over time, shown for all nodes (in blue) and for mission critical nodes only (in orange). Cyber incidents are marked with black circles.



Scatter plots of the mean geometric mean for each Monte Carlo simulation performance for each of the four variables.

Future Work and Applications:

- Expand the concept to real-world data sets by leveraging Common Product Enumeration, National Vulnerability Database, and other public data sources to create nominal nodes and real-world attack potential.
- Conduct sensitivity analyses and evaluations of various trust thresholds to determine the best starting points, alarm thresholds, and fading factors.

Computational Cybersecurity in Compromised Environments

2024 Fall Workshop | September 17-19 | SRI International in Menlo Park, CA