# Evidence-Based Trust for Critical-Infrastructure Decision-Making

Yujue Wang, Carl Hauser, Thoshitha Gamage

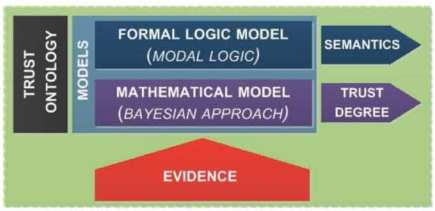
## Goals

- Develop a **Trust Assessment and Management Framework** for large-scale critical infrastructures, such as the power grid, where mutual suspicion between entities often inhibits information sharing
  - Develop a rich, expressive, and unifying formal trust logic to improve critical infrastructures' resilience to physical, epistemic, and attack-based uncertainties
- Instantiate the trust framework in a *wide-area data delivery system* for the power grid
- Explicitly managed trust will:
  - Ensure trusted entity-key bindings in PKI
  - Guarantee that information producers, consumers, and the network adhere to their contracted QoS
  - Enable sensitive information sharing

## Fundamental Questions/Challenges

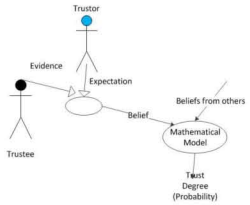
- **The ontology of trust:**
  - Trust is inherently abstract, subjective, and uncertain
  - Trust is multi-faceted and is *belief based on evidence*
  - Diversity of the entities involved makes trust assessment hard
    - Ex. the North American power grid: $n \times 10^5$ devices belonging to $m \times 10^3$ distinct organizations
- **Formal logic models and mathematical models:**
  - Lack of a widely accepted definition of trust
  - Lack of established trust judgment verification techniques
  - Lack of comprehensive mathematical models that are rich in expressiveness

## Research Plan




- Provide a formal definition in the form of a **modal logic model**
  - Extends predicate logic with modality: *necessarily* and *possibly*
  - Principals build *beliefs* based on *evidence* they gather
  - Principals verify the trustworthiness of others by checking if the other's behavior violates its beliefs

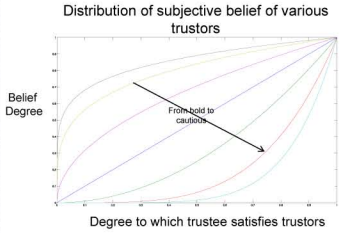
$$\forall x \text{ and } \forall \alpha \; M(\alpha, x) \rightarrow A(\alpha, x);$$
$$\forall x \text{ and } \forall \alpha \; A(\alpha, x) \rightarrow B(\alpha, x);$$
$$(\forall x \; A(\alpha, x), x \rightarrow y) \rightarrow B(\alpha, y);$$
$$T(\alpha, \beta) = \forall x B(\alpha, x), \forall y M(\beta, y), x \wedge y$$

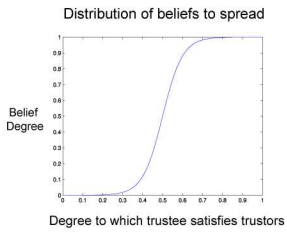



- Provide a framework for trust evaluation in the form of a **mathematical model**
  - Adds *assumptions* to the logic model
    - Logic models are not feasible in practice
- Use probability to express modality: **Bayesian probabilistic model**
  - The *trustor* proposes *expectations*
  - Based on evidence collected, trustor calculates how well the trustee satisfies the expectations and generates its own *beliefs*
  - Make the trust framework deployable in a distributed manner

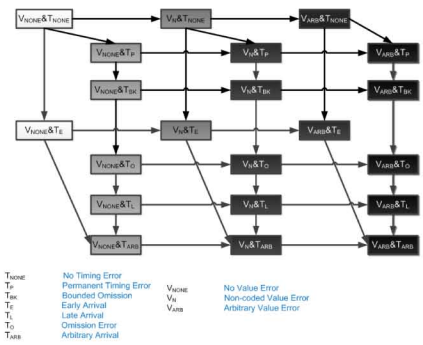
## Research Results

- Trustor's biased belief and belief that spreads




- Possible belief structure for GridStat Subscriber regarding a Publisher [1]




## Broader Impact

- These techniques will be useful for entity authentication. The scheme can help agents involved in an authentication procedure determine whether they locally have enough information to make an authentication decision or if they should refer to others. This reduces the risk of trusting third parties (e.g., CAs) or peers blindly and of making authentication decisions based on partial information.
- With the proposed method, controllers can improve their ability to assess the trustworthiness of data sources.

## Interaction with Other Projects

- In general, our research provides a scheme for solving trust assessment problems. So it is potentially relevant for any projects focused on authentication.
- Specifically, research studying information sharing among devices and systems under the control of diverse stakeholders such as utilities, customers, distributed energy providers and 3rd-party market makers can benefit from our research on assessing and managing trust

## Future Efforts

- More study is required on the *completeness* and *decidability* of our logic model.
- To be useful in practice, our models require calibration in the form of reliability and security metrics. Both general theory and a practical scheme are desired in this area.
- Computing Bayesian statistics is expensive. Explore the feasibility of using *hierarchical trust assessment* to reduce complexity.

### References:

[1] D. Powell, "Failure Mode Assumptions and Assumption Coverage," *Digest of Papers of the 22nd International Symposium on Fault-Tolerant Computing (FTCS-22)*, 1992, pp. 386-395.