# Trust-Based Security Protocols

**Henry Hexmoor, Sandeep Bhattaram, and Seth L. Wilson**
**University of Arkansas**
**Fayetteville, Arkansas 72701**

# Orientation

- AI/agents group working on *knowledge representation and management…*
- Our Primary focus is on design and implementation of socially adept agents…
- “Soft security” as our newest KR&M research area with modest AFOSR funding…

# Orientation and Premise

- Information sharing among disparately-located individuals with security concerns for confidentiality and integrity… sensor networks…
- Existing organizational policies lack in impersonal nature of the work environments and mutuality of trust and respect.
- We are developing trust-based security policies in information sharing that consider “trust” as the key parameter…

# Preliminaries

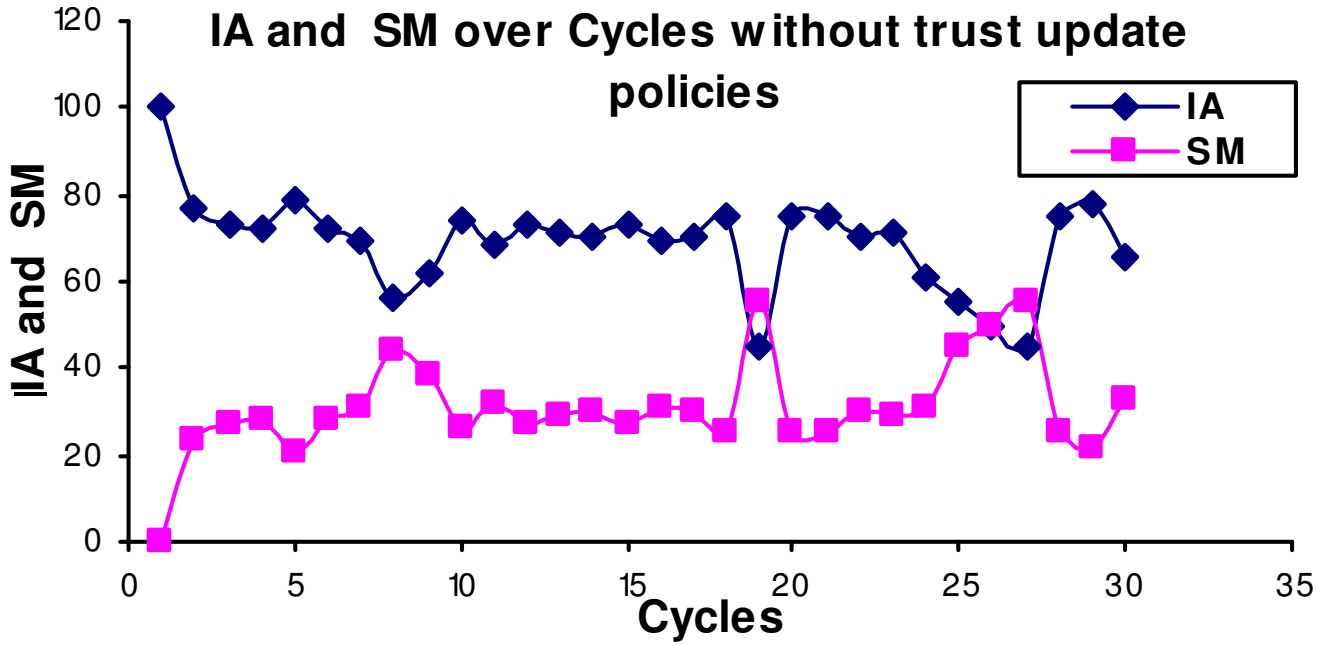
- Interpersonal Trust: Agent *x*'s *trust* in agent *y* is agent *x*'s estimation of the probability that agent *y* will preserve agent *x*'s welfare with regard to actions to be performed
- If a fact initiator agent determines that their trust in a recipient agent does not warrant them to receive the fact, then the recipient agent is considered to be an *unintended receiver*.
- Imagine a DAG of trust, i.e., a trust network…
- *A trust policy* prescribes a trust update policy that regulates changes in interpersonal trust relations in the first order to reduce unintended receivers while increasing the rate of information sharing.
- The larger goal is to establish and maintain enterprise KM regimes and to regulate information sharing topologies…

# Towards System-wide Metrics…

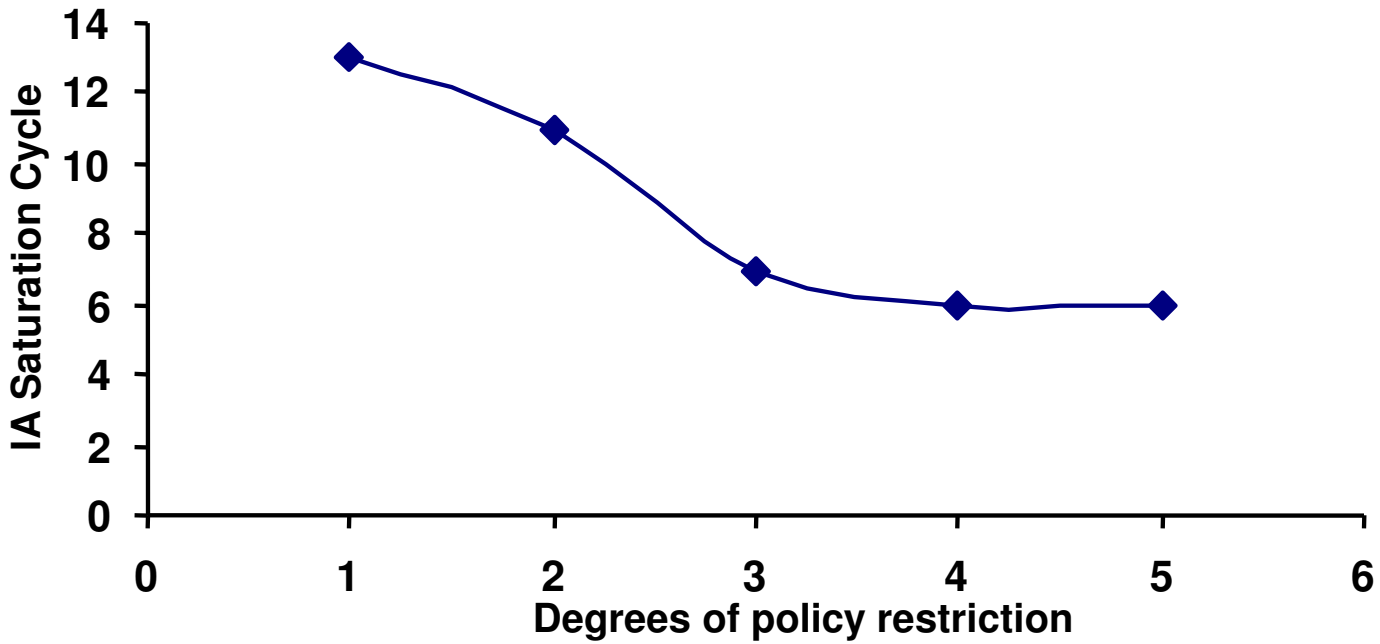
***Information availability*, IA, is the degree to which information is freely available when shared among a group of agents. IA, a system level metric, is the sum of number of satisfied agents and the number of intended receivers expressed as a percentage of the total facts shared.**

***Security Measure*, *SM*, is a system level metric, that measures the number of unintended receivers expressed as a percentage of the total facts shared.**

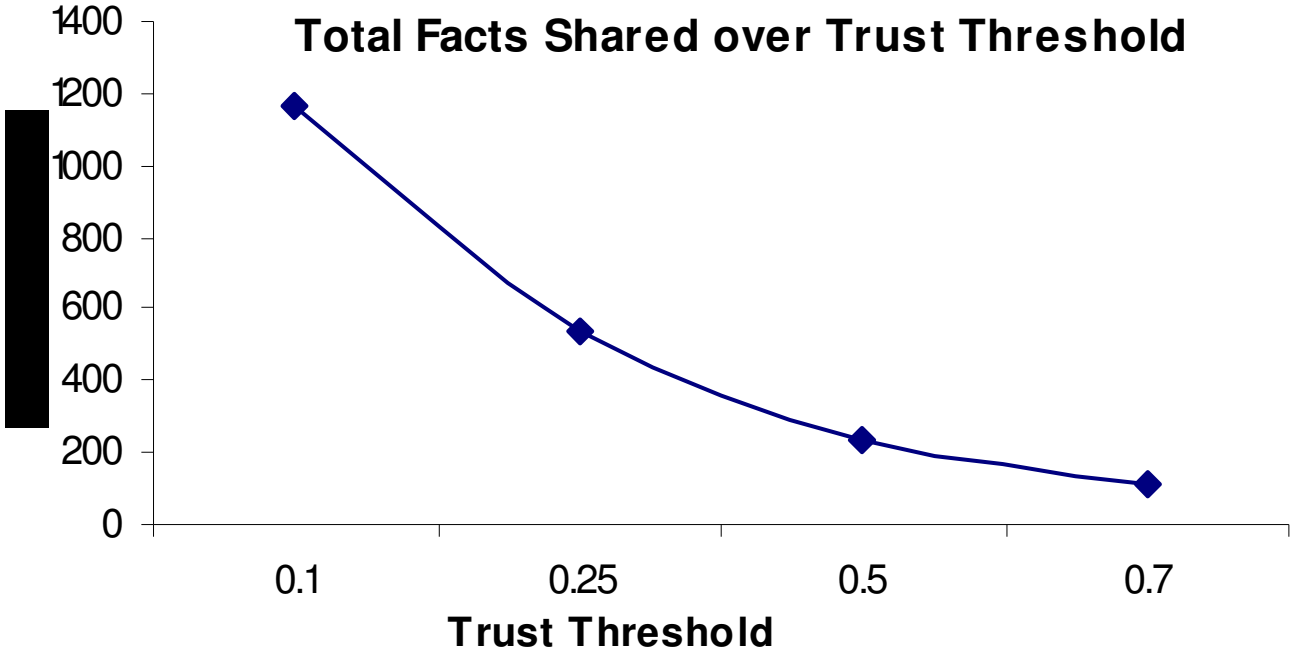
# A simulation with randomized facts and agents…



# A intuitive observation…



# Another observation…



# Conclusion

- The trust-based information sharing model sufficiently and effectively guarantees the high availability of information while limiting security breaches.

- Our simulations have demonstrated that the use of a "soft security" mechanism such as trust is as effective as hard security mechanisms.

- The inherent advantage of our model is in its simplicity, malleability, and scalability.