Resource Integration and Inference in Vanilla World

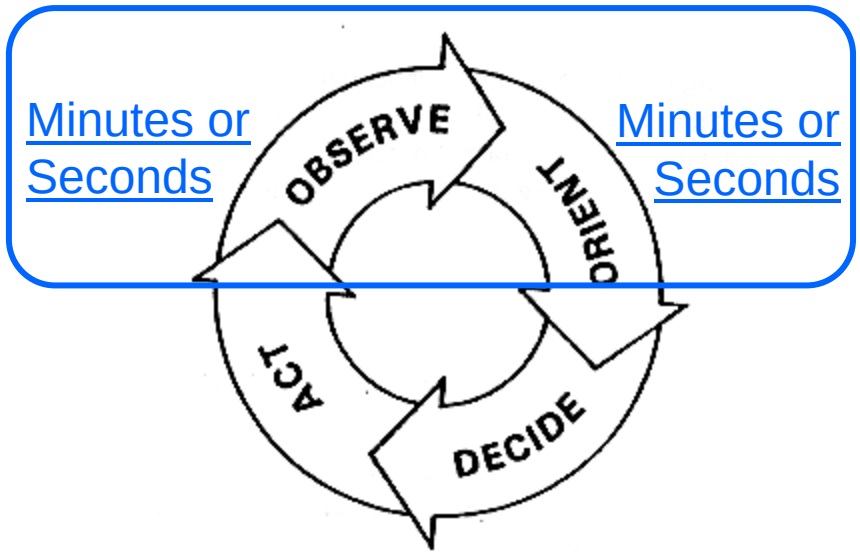
R. Scott Cost, John Cole, Markus Dale, Chris McCubbin, Ronald Mitnick, Dave Scheidt

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Hypothesis

- Information Exists That Can Be Fused to Create R*eal-Time, Actionable T*hreat Assessments and Alerts.
- The Information Necessary to Achieve These Assessments and Alerts is Available from:
  - Strategic Sensors
  - Direct Human Observation
  - Unmanned Sensors
  - Intelligence Data Bases
  - Informal “In-Country” Data Sets
  - Open Source
- As Currently Used This Data Cannot Be Used Fused Rapidly Enough to Provide Tactical Prediction

Blue OODA Loop



Tactical analysis can’t be done by humans *here*.

Design Features

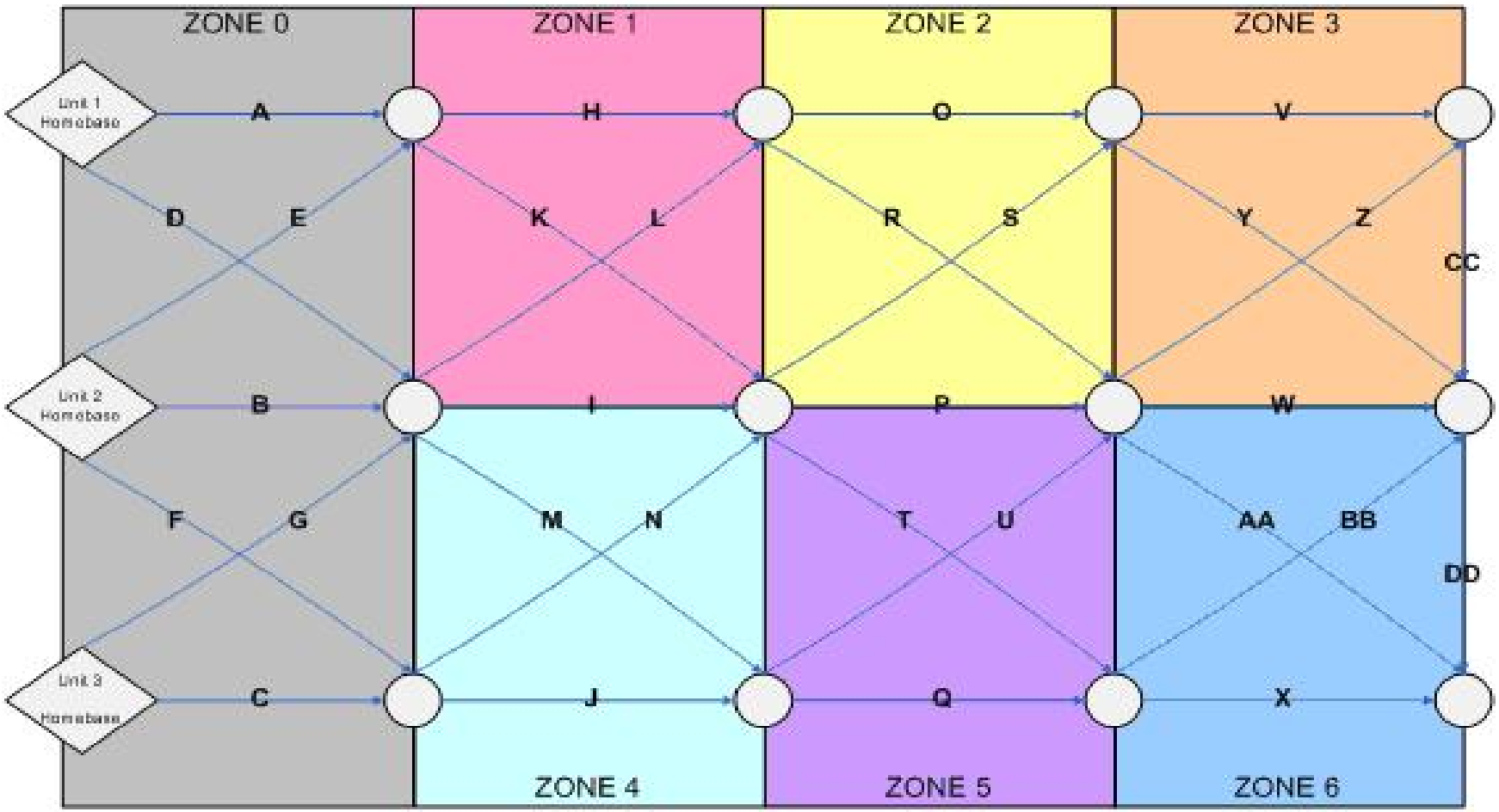
Prototype a Decentralized, Agent-based System With The Following Characteristics:

- Massively Parallel, Addressing Many Users Simultaneously and *Individually*
- Fully Autonomous Threat Assessment
- Real-Time Contextually Aware
- Fusing Information from Diverse Sources
- Adaptive, Incorporating New Users and Changing Information Sources at Run Time
- Lightweight and Easily Understood

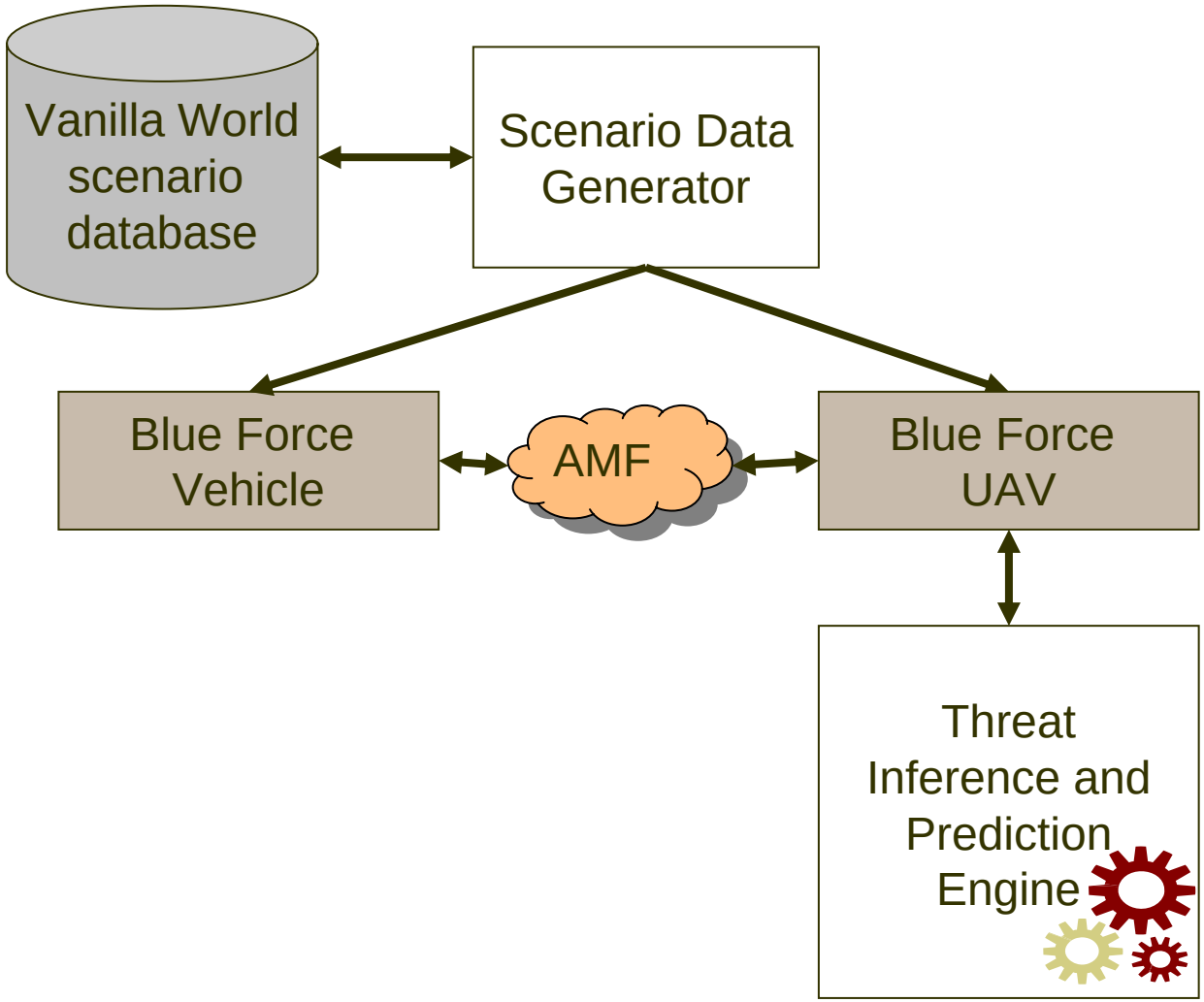
Vanilla World

- Hypothetical Country with undesirable events
- Scenario contains:
  - Patterns of activity leading up to events
  - Significant amount of random “normal” activity
  - 40 days of historical data and 30 days of “real-time” data
  - 2000 non-POI people, 20 POI
- Data Modeled
  - Passenger Aircraft manifests
  - Phone calls (~8500 in last 30 days)
  - HUMINT free-text information
  - Activity reports (digging, emplacement events) (~100 events)
  - Threat events and small arms fire events (~25 events)
  - Events take place in a notional country

Vanilla World Map



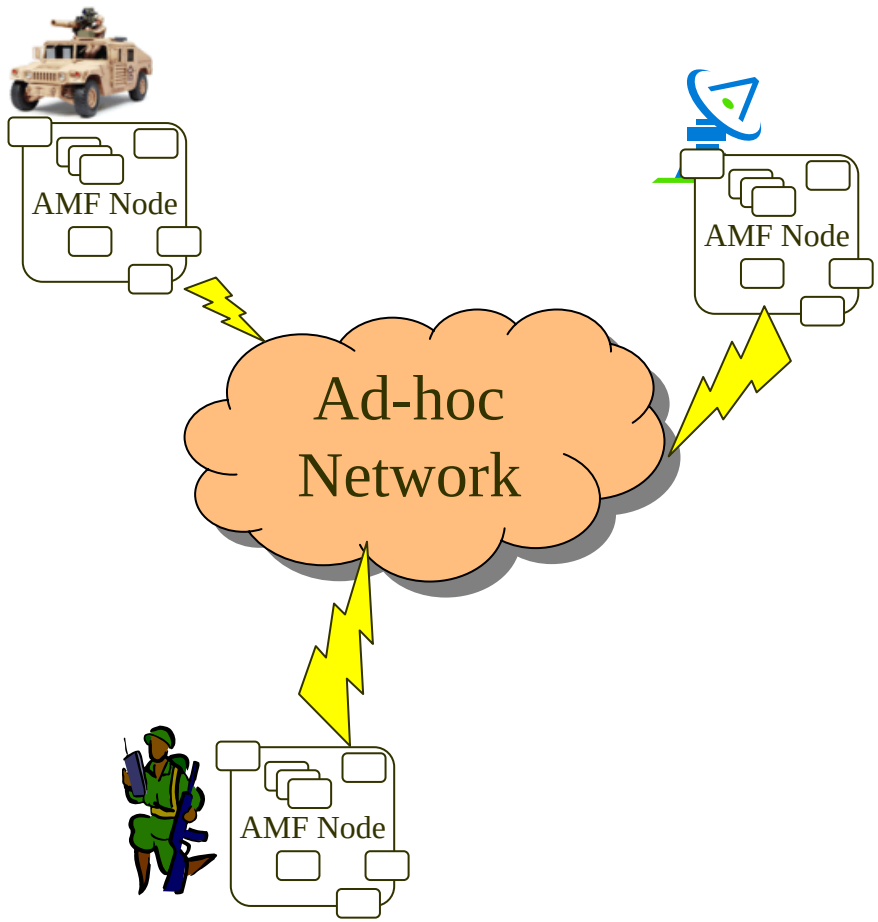
Testbed Architecture



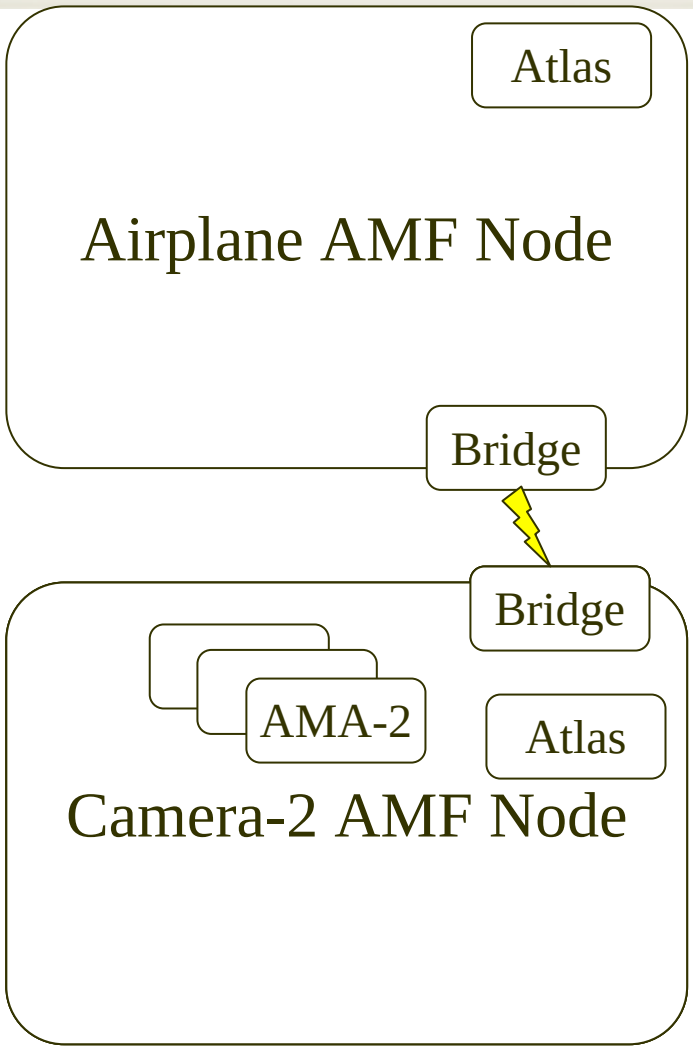
Active Metadata Agents

Design Features

- Agent-Based Architecture
- Discovery – To Support the Incorporation of New Information Providers, Users and Fusion Engines
- Smart Filtering
  - Mission Awareness
  - Threat Awareness
  - Proximal Awareness
  - Temporal Awareness
- Support for Autonomous Data Fusion
- Criticality-Based Information Exchange



AMF Use Case

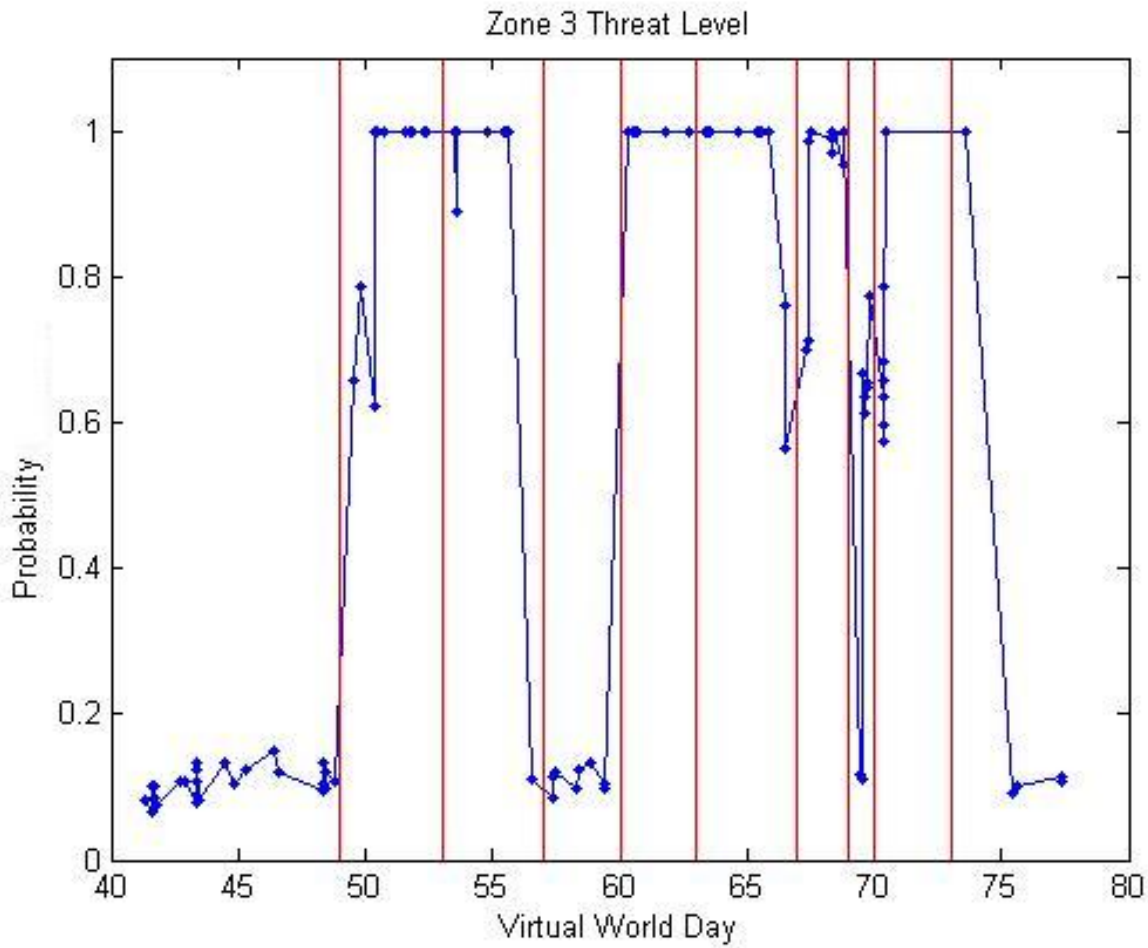

Atlas
Airplane AMF Node
Bridge
Bridge
AMA-2
Atlas
Camera-2 AMF Node


Oahu, Hawaii
"The Aloha Isle"
Kahuku
Laie
Mokuleia
Haleiwa
Makaha
Wahiawa
Mililani
Kahaluu
Kaneohe
Nanakuli
Pearl City
Kailua
Pearl Harbor
Kapolei
Ewa Beach
Honolulu
Waimanalo
Hawaii Kai

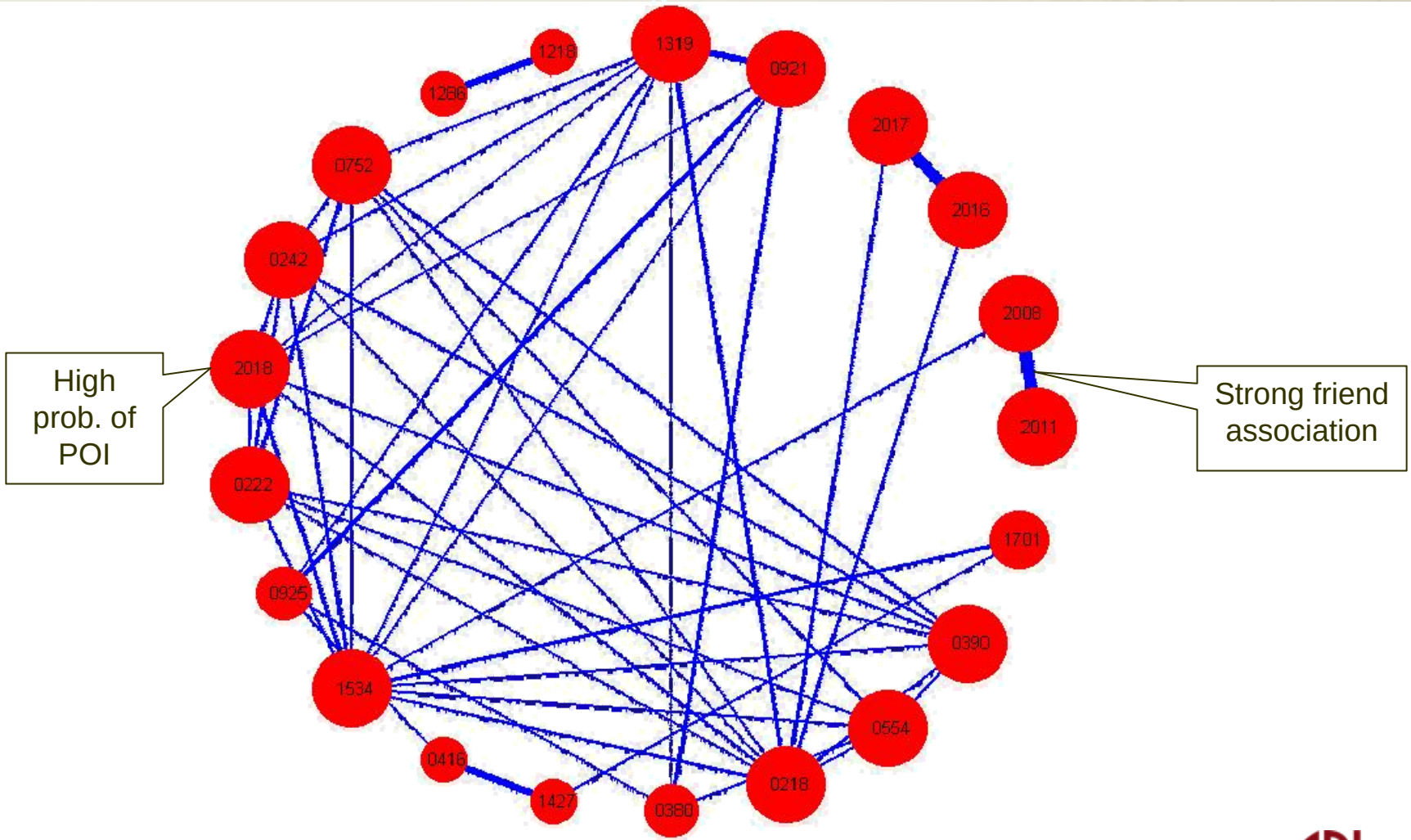
Markov Logic Networks

- We use *Markov Logic Networks* to do inference
  - Hybrid reasoning system combining Markov Networks (probabilistic reasoning) and First Order Logic (deductive reasoning)
- Uses weighted first order logic statements to describe the world
  - Statements may not always hold
- Example of prototype MLN statements:
  - Friends of Persons of Interest are Persons of Interest
    - friends(person1, person2) ^ POI(person2) ~> POI(person1)
  - If a POI dug in a location recently, that location is threatened
    - dig(p, loc, day) ^ POI(p) ^ currentday(today) ^ recent(day, today) ~> threatened(loc)
- Preliminary results: 20% of POIs (4 of 20) are identified vs. 0.5% False Positives (10 of 2000).
- MLN's can also output social network information.

Output of MLN: Threat Level



Output of MLN: Social Networks



Threat Pattern Discovery

- Previous tests used MLN's that were constructed using common sense patterns
- We wish to create a system that can automatically identify existing and novel patterns of threat activity
- Currently applying stochastic optimization techniques to create MLN's that have better results than hand-crafted MLN's.
- Other options include pattern discovery techniques from data mining or other pattern discovery techniques

Options for Future Work

- Improve pattern discovery and pattern recognition Algorithms
- Create distributed pattern discovery and recognition techniques
- Synthesize components into a robust end-to-end solution