Automated Risk Assessment of Sensor Information Disclosure in Coalition Operations

Marco Carvalho, Carlos Perez, and Jeffrey M. Bradshaw

Florida Institute for Human and Machine Cognition (IHMC)
15 SE Osceola Ave., Ocala, FL 34471
http://www.ihmc.us
(850) 202-4446

Marco Carvalho, Ph.D.

- Background:
  - Mechanical Engineering (B.Sc, M.Sc.)
    - Automatic Control Systems and Computation Fluid Dynamics
  - Computer Science (M.Sc., Ph.D.)
    - Machine Learning, Computer Security and Complex Networks
- Current Affiliations
  - Research Scientist at IHMC
  - Graduate Faculty at the Florida Institute of Technology
  - Faculty Member at the Center for Applied Optimization (University of Florida)
- Current Areas of Research
  - Cyber Security and Bio-Inspired Resilience
  - Critical Infrastructure Protection
  - Complex Networks and Distributed Systems
    - Tactical Communication Networks
    - Self-Similarity in Complex Networks
    - Social Network Analysis and Virtual Worlds

Research Team in Ocala, FL

- Marco Carvalho
- Adrian Granados
- Carlos Perez
- Marco Arguedas
- Massimiliano Marcon
- Giacomo Benincasa

- Graduate Students and collaborators
  - UF (Mechanical and Aerospace Engineering, Industrial Engineering, and Computer Science)
  - UF - Center for Applied Optimization (Gainesville, FL)
  - Harris Center for Information Assurance (Melbourne, FL)

What is the Problem?

- A **sensor network** is deployed in an area of interest
- Sensors have different security **classifications,** or classified **capabilities**

- The Problem: How to **provide information** to friends (troops and coalition partners) **while minimizing the risk of disclosing** the presence and/or location of the **classified sensors**?

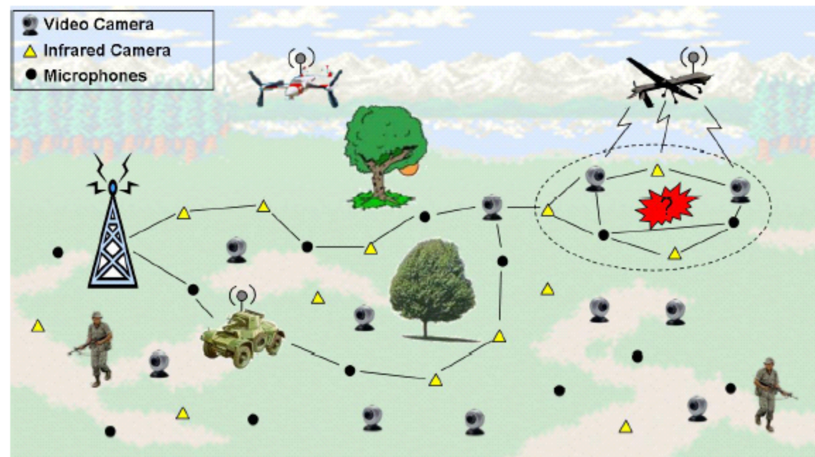


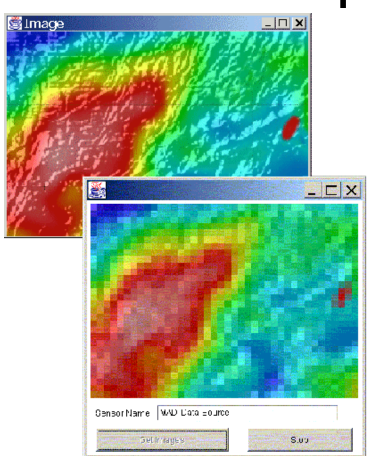
Image src: www.ece.osu.edu/ ~ekici/res_wmsn.html

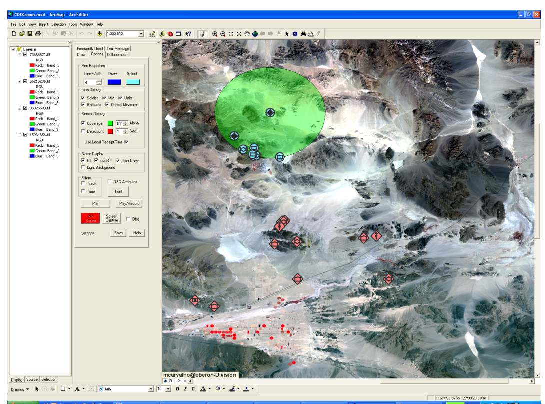
Related Work

- Statistics:
  - Statistical Disclosure Control (SDC)
  - Statistical Disclosure Limitation (SDL)
  - Inference Control
- Data Mining
  - Privacy Preserving Data Mining (PPDM)

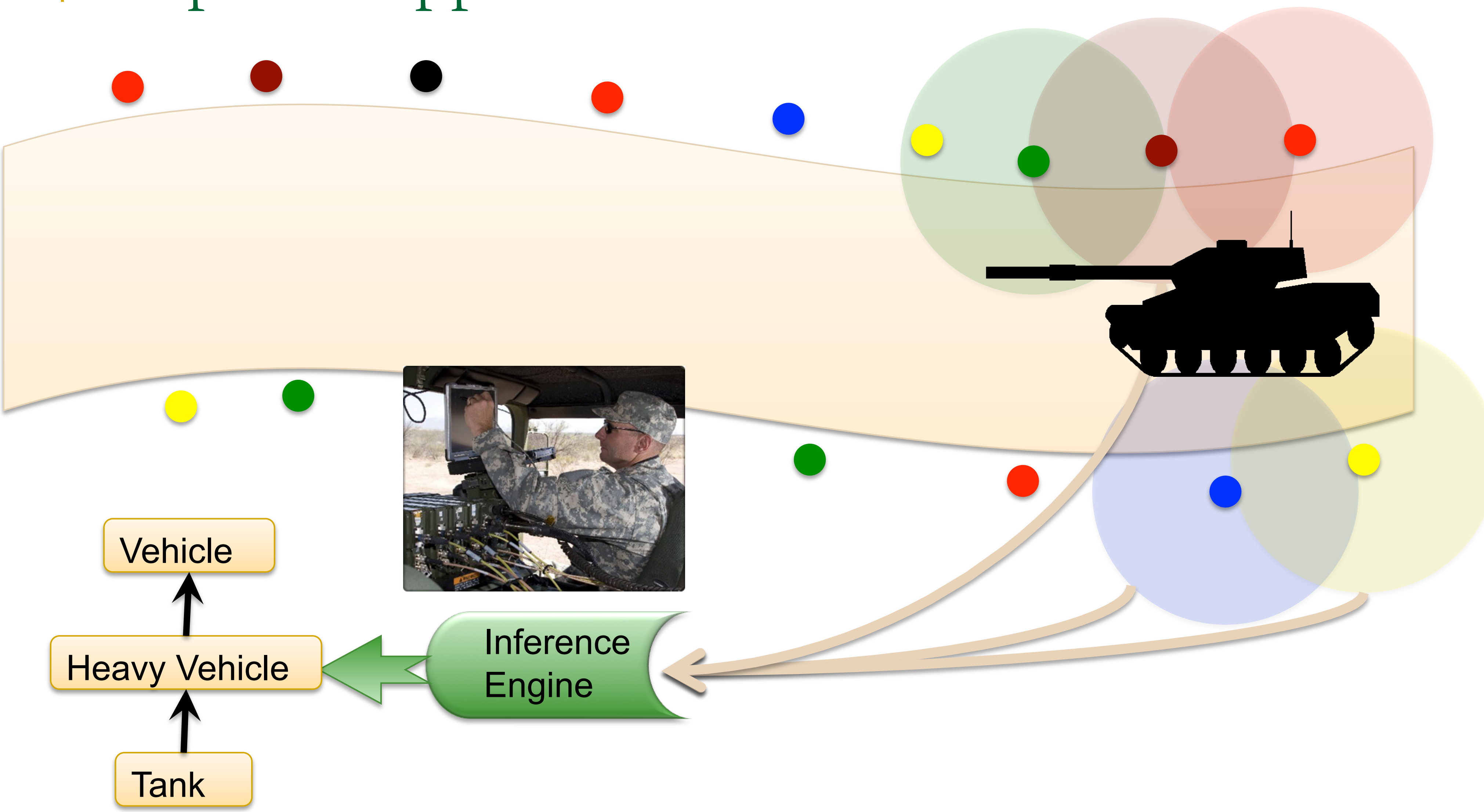
Related Work (cont.)

- ARL Collaborative Technology Alliance
  - Advanced Decision Architectures
    - Policy-governed information exchange
- Information and Sensor Capability Protection
  - Coalition Operations
  - Adversaries in the field, etc.
  - Risk-adaptive access control



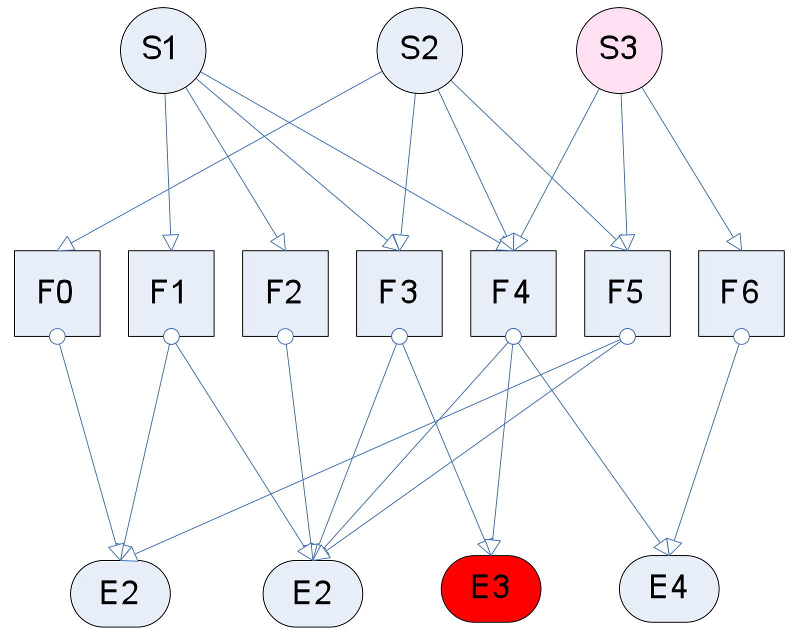


Proposed Approach



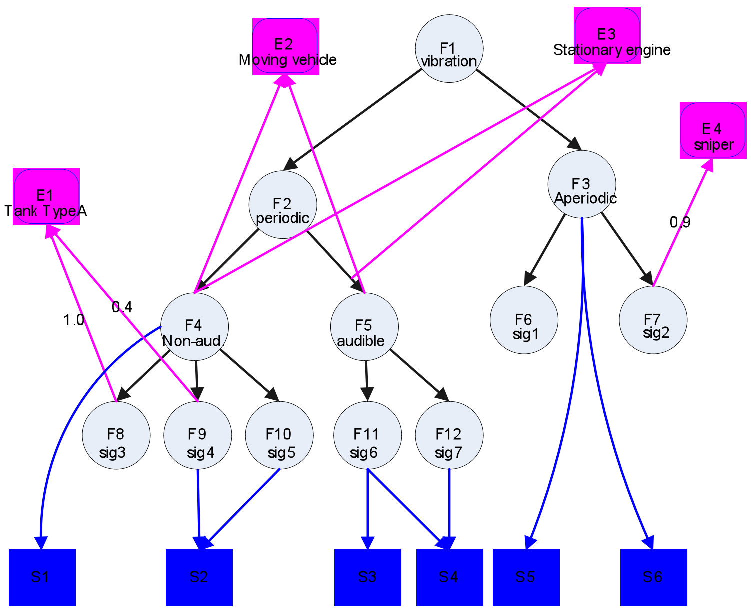
A Simple Example

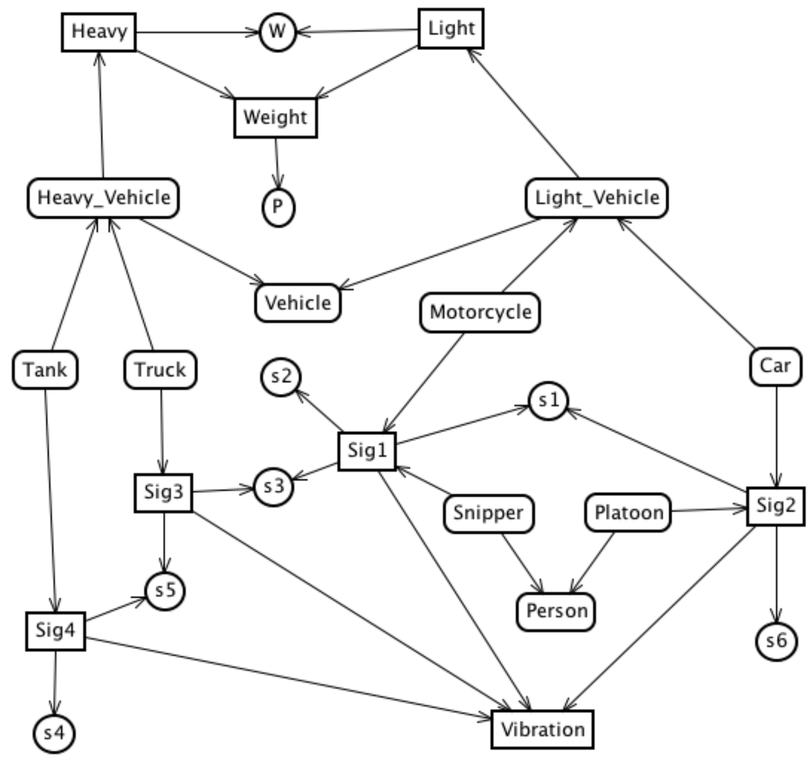
- Reporting E3
  - Ambiguous sources “S2” or “S3”
  - Depending on history of entities previously reported to that soldier, the probability of choosing “S2” is greater than that of choosing “S3”
  - Direct Bayesian inference from the soldier side can be used to estimate the presence of sensor “S3”



A More Complex Scenario

Selective Information Release for Source Protection

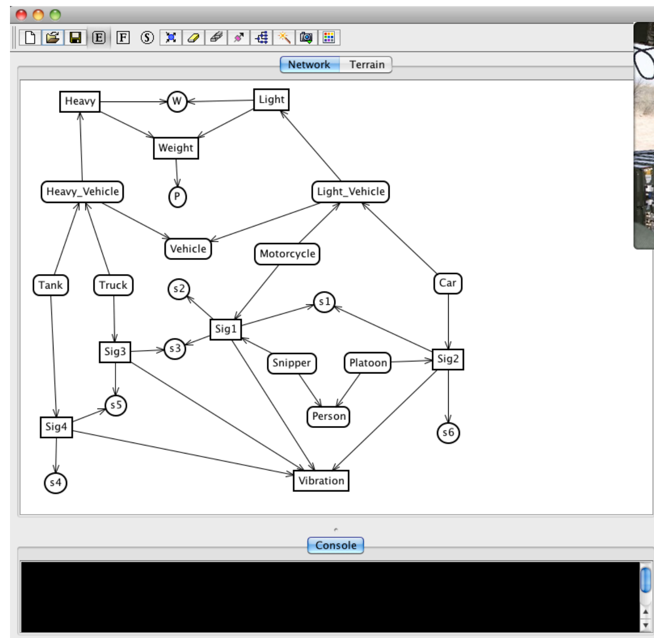


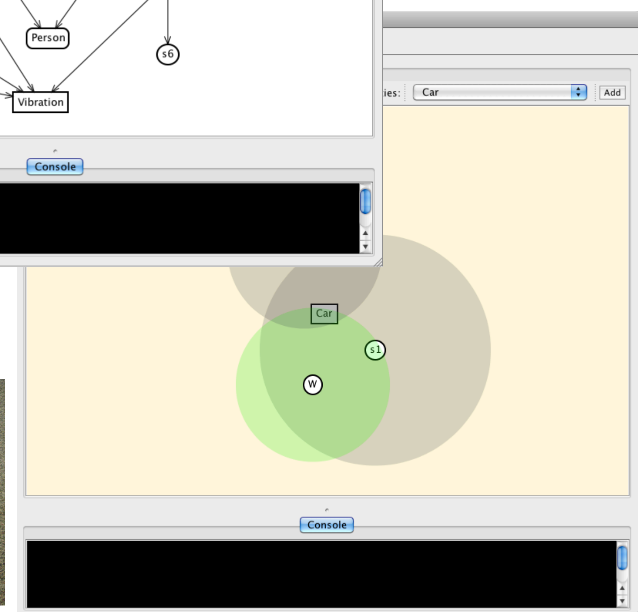


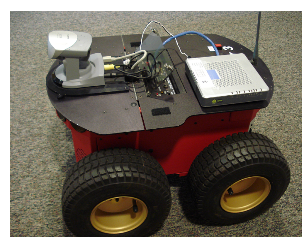
Proposed Solution

- Build an Automatic Source Protection Network (ASPNet), a Bayesian Network that uses an ontology to represent a hierarchy of entities and features

- Use the ASPNet for detecting entities and for assessing the risk of disclosing sensor information using probabilistic inference

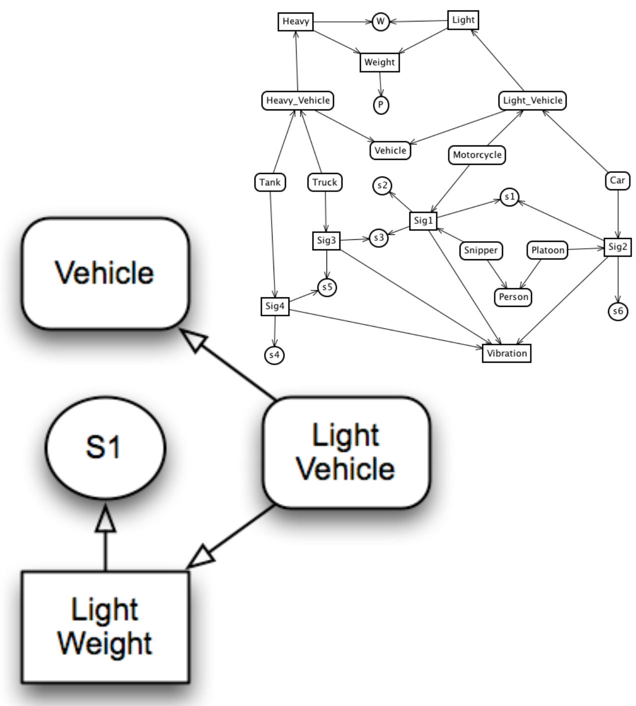




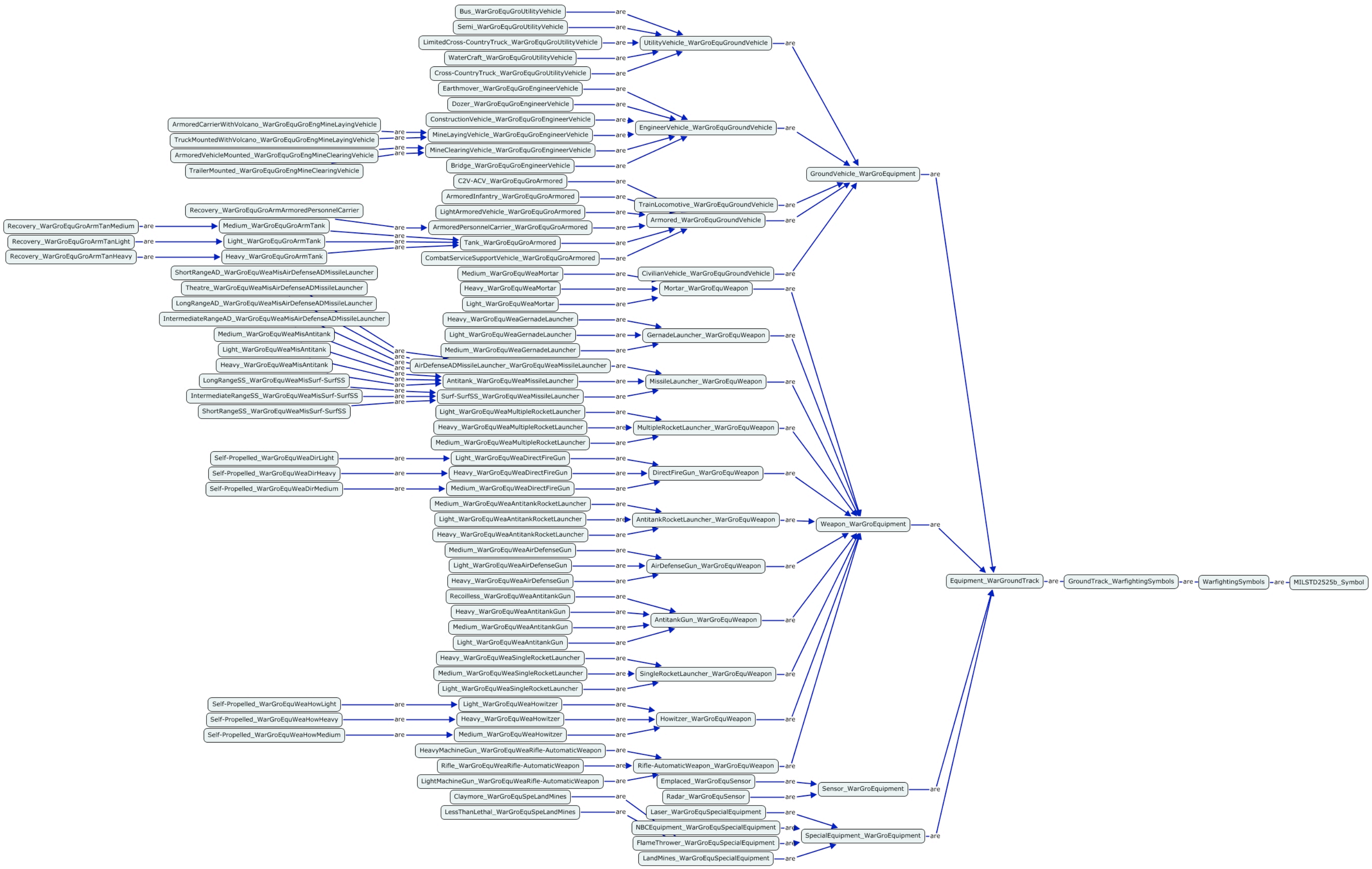


ASPNet Specification

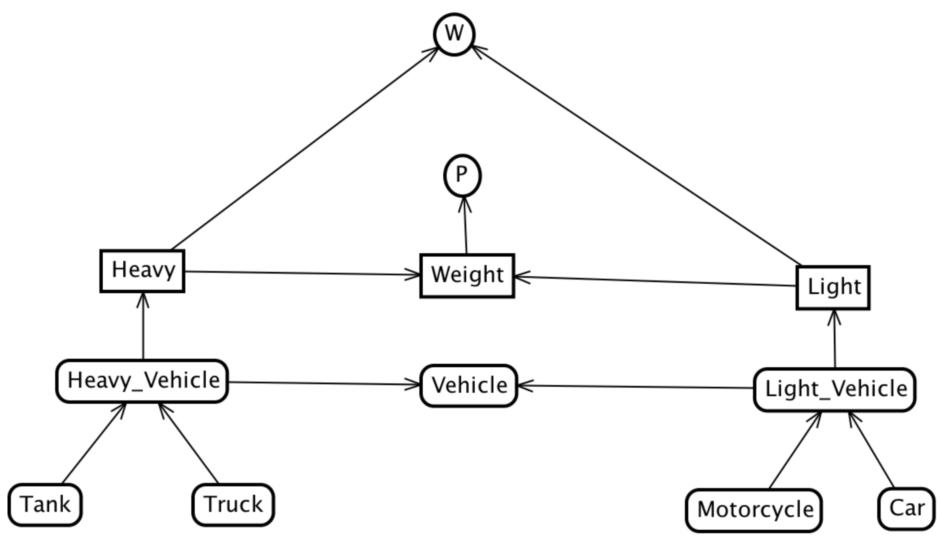
- Bayesian Network
  - Automatically-detected sensor field information, hierarchy of equipment (ontology), and technical database of features and known signatures
- Contains three types of nodes:
  - Entities
  - Features
  - Sensors
- All nodes are binary (true or false)
- Allowed Links:
  - Entities → Parent Entities
  - Entities → Features
  - Features → Parent Features
  - Features → Sensors



Equipment (Entity) Ontology



ASPNet Example

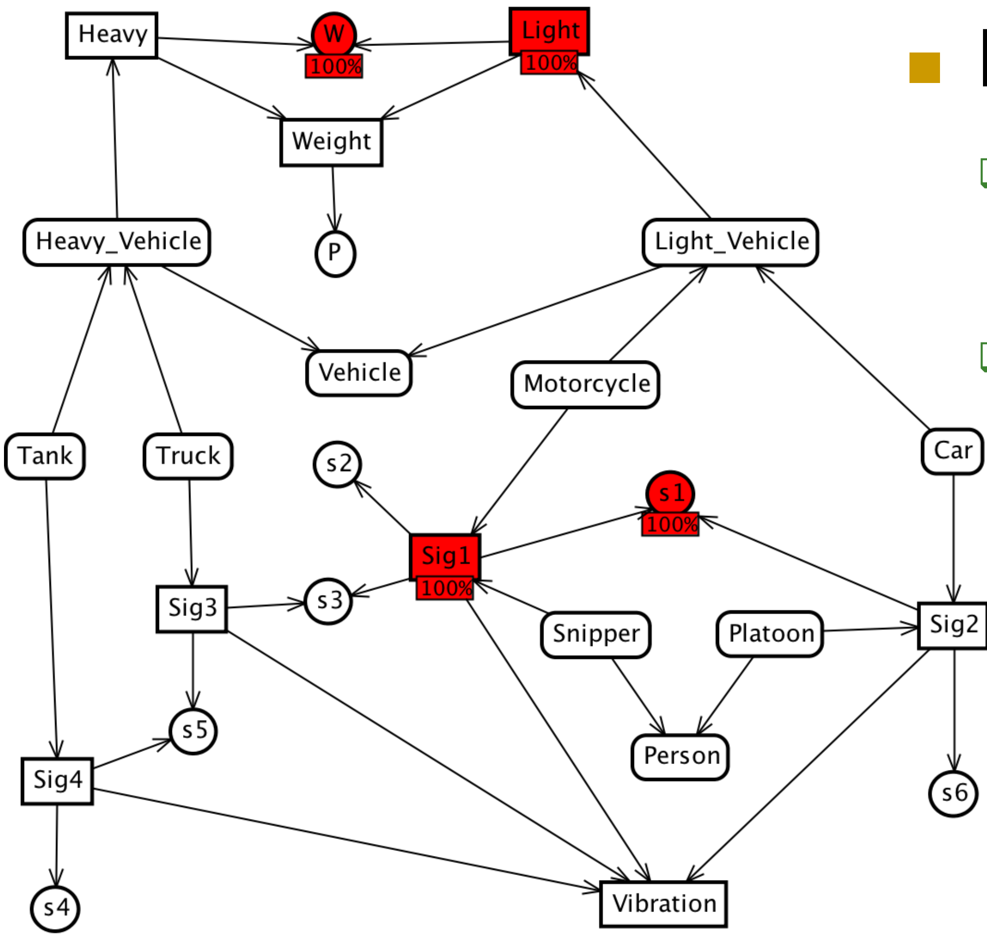


- **Entities:** Vehicle, Heavy_Vehicle, Tank, Truck, Light_Vehicle, Motorcycle, Car
- **Features:** Weight, Heavy, Light
- **Sensors:** W, P

Detecting an Entity

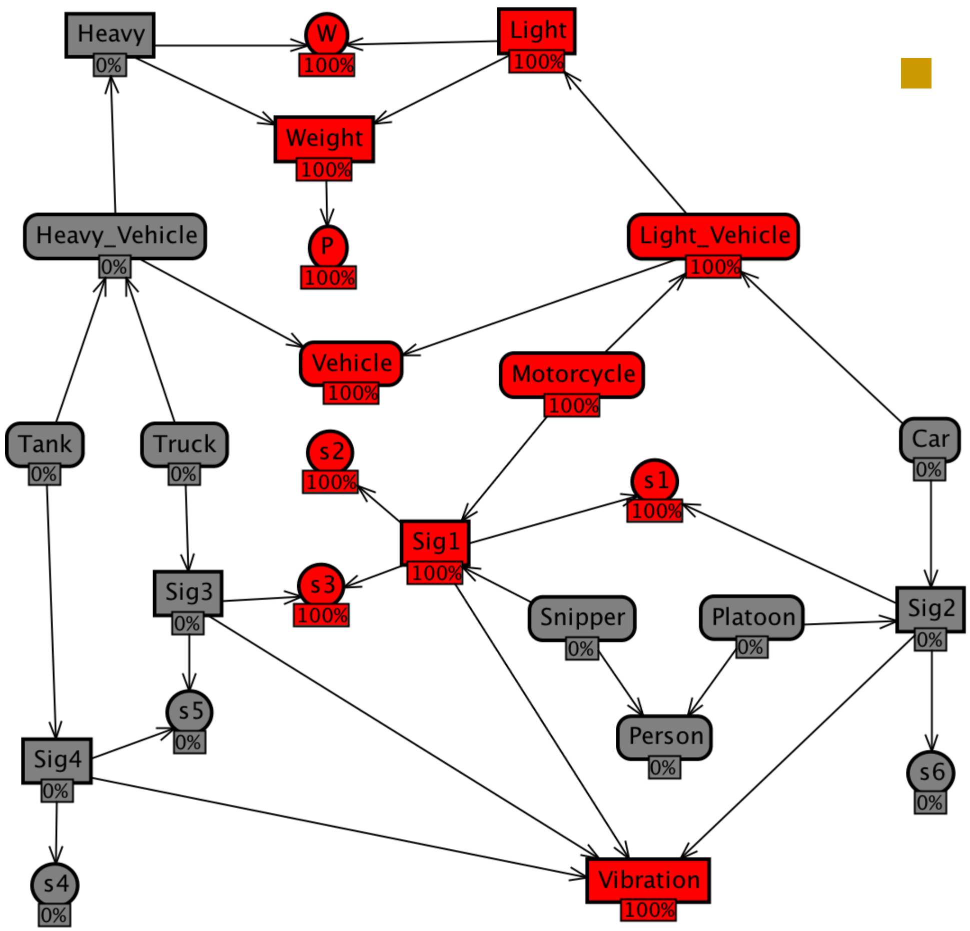
- Gather information provided by the sensors
- Feed that information to the Bayesian Network
- Run an **inference algorithm** over the network
- Pick the entity or entities with **highest probability**

Detection Example



- **Evidence**
  - **W** sensor measured feature **Light**
  - **s1** sensor measured feature **Sig1**

Detection Example (continued)



- **Results of Inference:**
  - The entity is:
    - Vehicle
    - Light_Vehicle
    - Motorcycle

Source Protection Problem

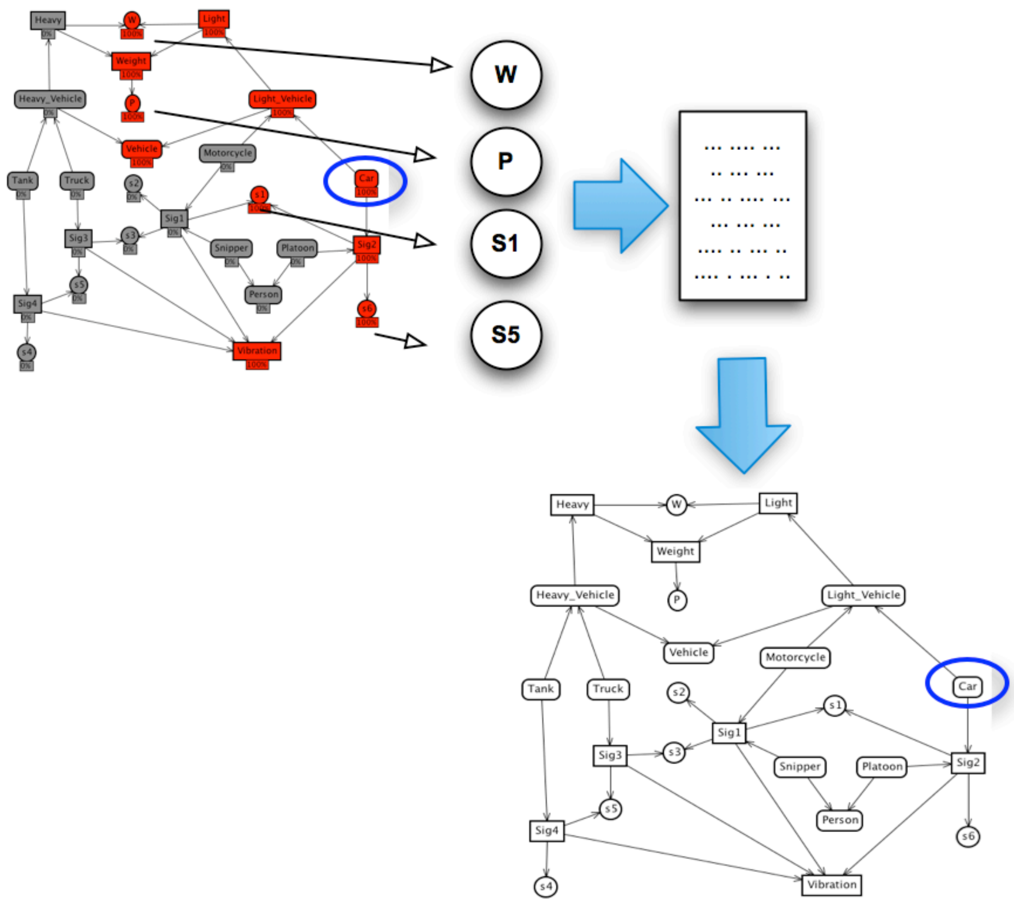
- In the previous example we could disclose to the soldiers that entity is a **Motorcycle**, a **Light_Vehicle** or simply a **Vehicle**
- However, from a **sensor protection** perspective, there is a different risk for each one of these disclosures

Risk of Disclosing a Sensor

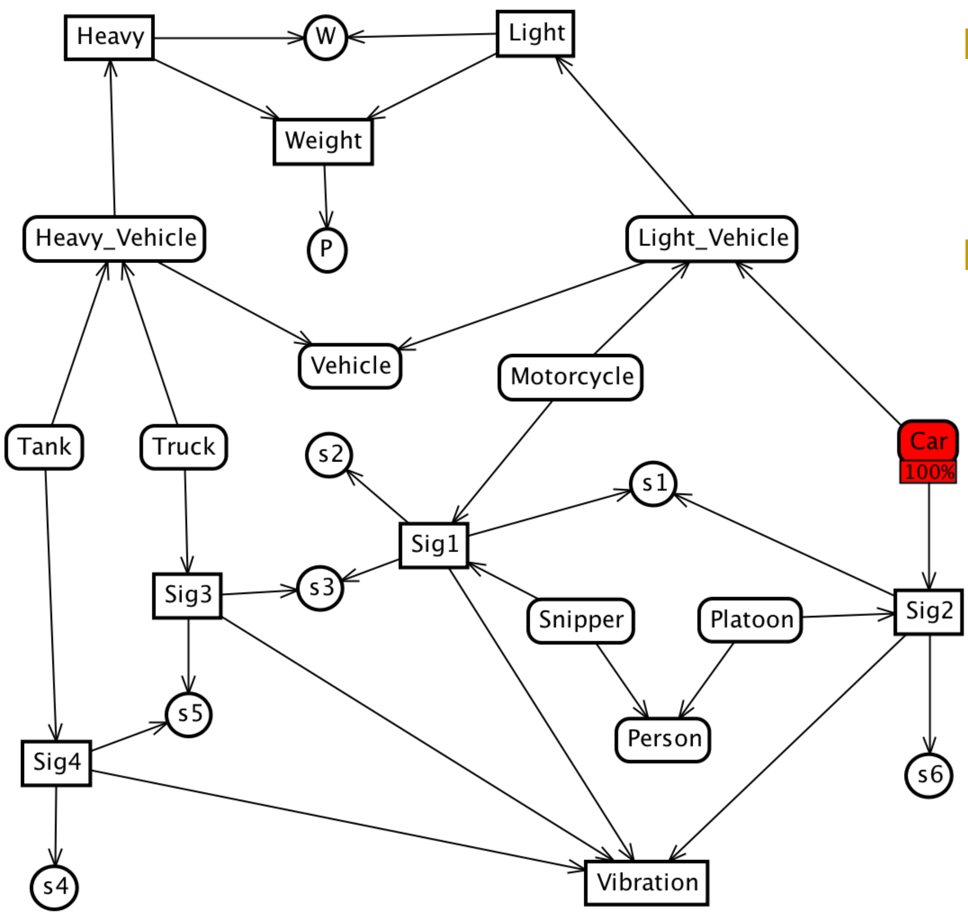
```
Input: N (ASP Network)
Input: e (Entity to be disclosed)
Input: t (Activation threshold)
P ← DoInference(N, {e = true});
F ← {f|f ∈ N ∧ IsFeature(f) ∧ P(f) ≥ t};
S ← {s|s ∈ N ∧ IsSensor(s) ∧ ∃f ∈ F [DetectsFeature(s, f_i)]};
F_s ← {f|f ∈ F ∧ s ∈ S ∧ DetectsFeature(s, f)};
R ← {};
for C ∈ P(S) do
    indexes[1 ... |C|] ← 0;
    i ← 0;
    while C ∉ R ∧ i ≥ 1 do
        s ← C(i);
        indexes[i] ← indexes[i] + 1;
        if indexes[i] ≥ |F_s| then
            indexes[i] ← 0;
            i ← i − 1;
        else
            if i = |C| then
                E ← {};
                for j ∈ {1 ... |C|} do
                    s ← C(j);
                    E ← E ⋃ F_s[indexes[j]];
                end
                P ← DoInference(N, E);
                if P(e) ≥ t then
                    R ← R ⋃ {C};
                end
            else
                i ← i + 1;
            end
        end
    end
end
return R
```

- The risk of disclosing a sensor will be defined as the probability of having used the sensor for detecting the entity
- How is this probability computed?
    - Identify all combinations of sensors that would allow to detect the entity
    - Divide the number of combinations including the sensor by the total number of combinations

Risk Assessment

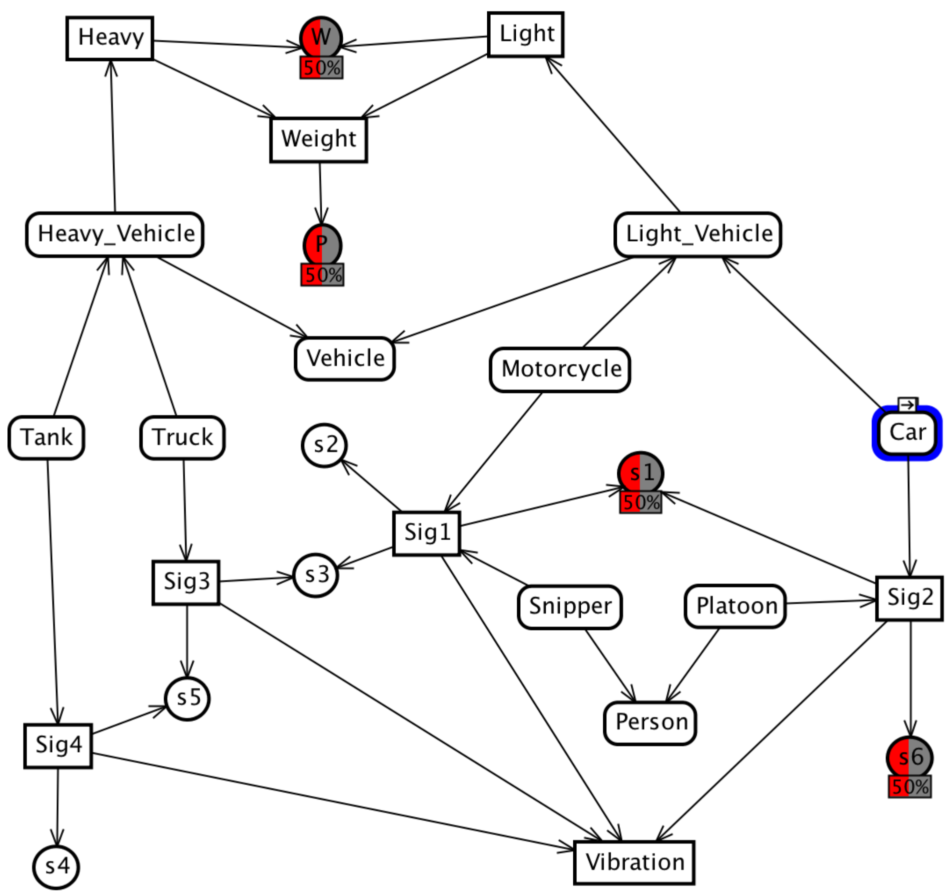


Risk Assessment Example



- Entity to Disclose: **Car**
- Sensor combinations that allow the detection of a **Car:**
  - **{W, s1}**
  - **{W, s6}**
  - **{P, s1}**
  - **{P, s6}**

Risk Assessment Example (continued)



- Sensor combinations:
  - {W, **s1**},
  - {W, s6}
  - {P, **s1**}
  - {P, s6}
- Risk of **s1** = 2 / 4 = 50%

First Evaluation

- **Hypothesis**: Using more abstract ontology classes reduces the risk
- **Evaluation**:
  - Obtained network from Army National Training Center
  - For each child entity, C, assess the risk for each sensor S → Risk(S | C)
  - Then for the parent entity, P, assess the risk for each sensor S → Risk(S | P)
  - Risk(S | C) – Risk(S | P)
  - Average differences

Second Evaluation Using Army National Training Scenario

- **Scenario**: subset of a military exercise dataset from the Army National Training Center
- 161 nodes
  - 51 sensors
    - 18 sensor types
  - 110 entities
    - Ontology has 63 classes of entities

Risk Assessment

Sensor	Entity								
	P07	P0	P	P82	P8	P	4UZ	4U	4
SEH	14.29%	12.50%	8.00%	33.33%	33.33%	8.00%	18.18%	18.18%	16.98%
SQ3IR	14.29%	12.50%	24.00%	33.33%	33.33%	24.00%	36.36%	36.36%	22.64%
SEC	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	18.18%	18.18%	11.32%
SNH	0.00%	0.00%	36.00%	0.00%	0.00%	36.00%	100.00%	100.00%	52.83%
SW	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	7.55%
SQ5	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	9.09%	9.09%	22.64%
SNU	100.00%	87.50%	48.00%	0.00%	0.00%	48.00%	0.00%	0.00%	3.77%
SN8	0.00%	12.50%	4.00%	0.00%	0.00%	4.00%	0.00%	0.00%	0.00%
SW0	0.00%	0.00%	24.00%	100.00%	100.00%	24.00%	0.00%	0.00%	7.55%
SEY2	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	27.27%	27.27%	11.32%
SN9	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.89%
SN90	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.89%
SW3	0.00%	12.50%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	15.09%
SQ3I6	57.14%	50.00%	56.00%	33.33%	33.33%	56.00%	36.36%	36.36%	22.64%
SWP	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	16.98%
SEYO	57.14%	50.00%	16.00%	0.00%	0.00%	16.00%	36.36%	36.36%	37.74%
SWN	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	9.43%
SQ3Z	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	18.18%	18.18%	20.75%

Risk Assessment (continued)

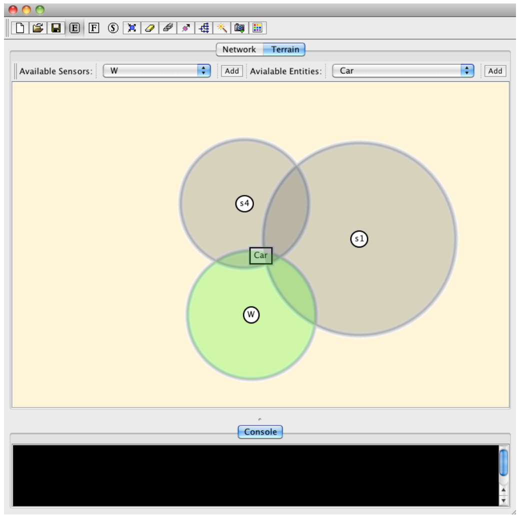
- Using more abstract classes in the ontology only helps to reduce the risk of the sensors involved in discovering the lower level entity type
- It also adds more sensors to the risk assessment, thus increasing the risk of all sensors in general
  - Thus risks of 0% will, in most cases, increase

Risk Assessment

Sensor	Entity								
	P07	P0	P	P82	P8	P	4UZ	4U	4
SEH	14.29%	12.50%	8.00%	33.33%	33.33%	8.00%	18.18%	18.18%	16.98%
SQ3IR	14.29%	12.50%	24.00%	33.33%	33.33%	24.00%	36.36%	36.36%	22.64%
SEC	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	18.18%	18.18%	11.32%
SNH	0.00%	0.00%	36.00%	0.00%	0.00%	36.00%	100.00%	100.00%	52.83%
SW	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	7.55%
SQ5	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	9.09%	9.09%	22.64%
SNU	100.00%	87.50%	48.00%	0.00%	0.00%	48.00%	0.00%	0.00%	3.77%
SN8	0.00%	12.50%	4.00%	0.00%	0.00%	4.00%	0.00%	0.00%	0.00%
SW0	0.00%	0.00%	24.00%	100.00%	100.00%	24.00%	0.00%	0.00%	7.55%
SEY2	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	27.27%	27.27%	11.32%
SN9	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.89%
SN90	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	1.89%
SW3	0.00%	12.50%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	15.09%
SQ3I6	57.14%	50.00%	56.00%	33.33%	33.33%	56.00%	36.36%	36.36%	22.64%
SWP	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	16.98%
SEYO	57.14%	50.00%	16.00%	0.00%	0.00%	16.00%	36.36%	36.36%	37.74%
SWN	0.00%	0.00%	12.00%	0.00%	0.00%	12.00%	0.00%	0.00%	9.43%
SQ3Z	14.29%	12.50%	4.00%	0.00%	0.00%	4.00%	18.18%	18.18%	20.75%

Conclusions and Future Work

- ASP provides sensor disclosure risk estimates for different detections and sensors
- Users can choose explore different hypotheses for information release through the graphical interface
- We are currently adding spatial and temporal reasoning
- The choice of the appropriate level of abstraction for information release is not always intuitive, but it can be facilitated by the proposed approach



Acknowledgments

This work was partially sponsored by the **US Army Research Laboratory** via Cooperative Agreement No. W911NF-07-2-0022, CFDA No. 12.630, and the **US Air Force Research Laboratory** under Cooperative Agreement Number FA8750-07-2-0185

Thank you!

Marco Carvalho
Research Scientist
mcarvalho@ihmc.us
(850) 202-4446

Florida Institute for Human and Machine Cognition (IHMC)
15 SE Osceola Ave.
Ocala, FL 34471
http://www.ihmc.us