

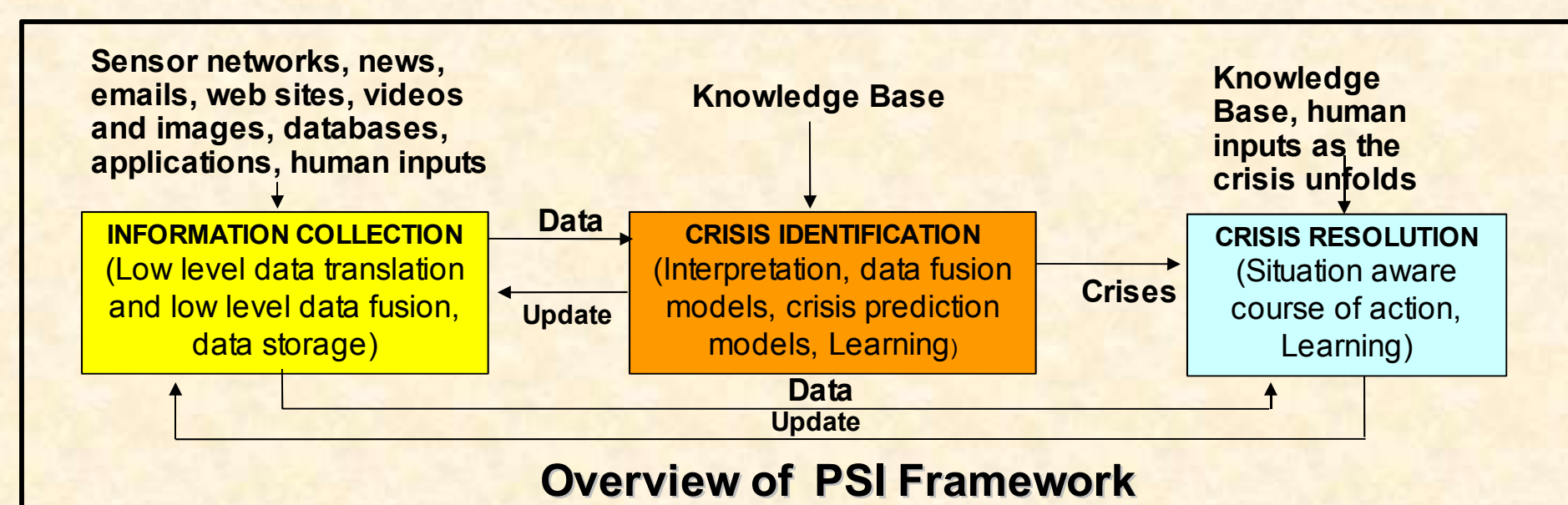
PSI: Pervasively Secure Infrastructures (PSI): Integrating Smart Sensing, Data Mining, Pervasive Networking and Community Computing

<http://crewman.uta.edu/psi>

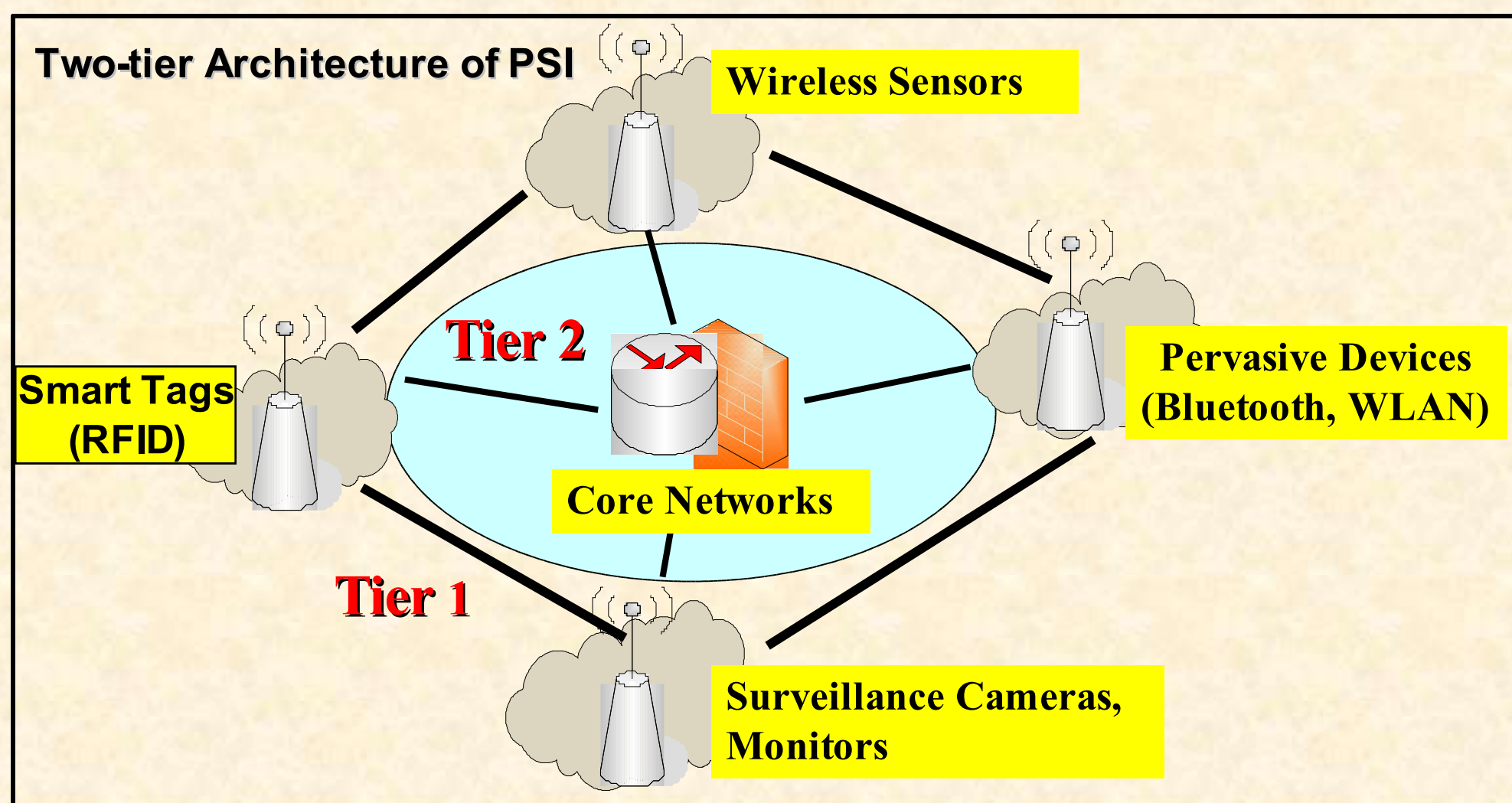
Research Objective

To create a technology-enabled security framework that makes use of smart sensors, wireless networks, data mining, mobile agents and pervasive computing technologies in an integrated, collaborative and distributed manner, with a goal to monitor, prevent and recover from natural and inflicted disasters.

Approach



- Efficient data collection and aggregation from heterogeneous sensors and monitors pervasively
- Novel techniques for real-time, authenticated, and secured information transmission and sharing
- Intelligent situation-awareness through learning, data mining and knowledge discovery techniques
- Community Computing paradigm for adaptability, scalability and dynamic information handling



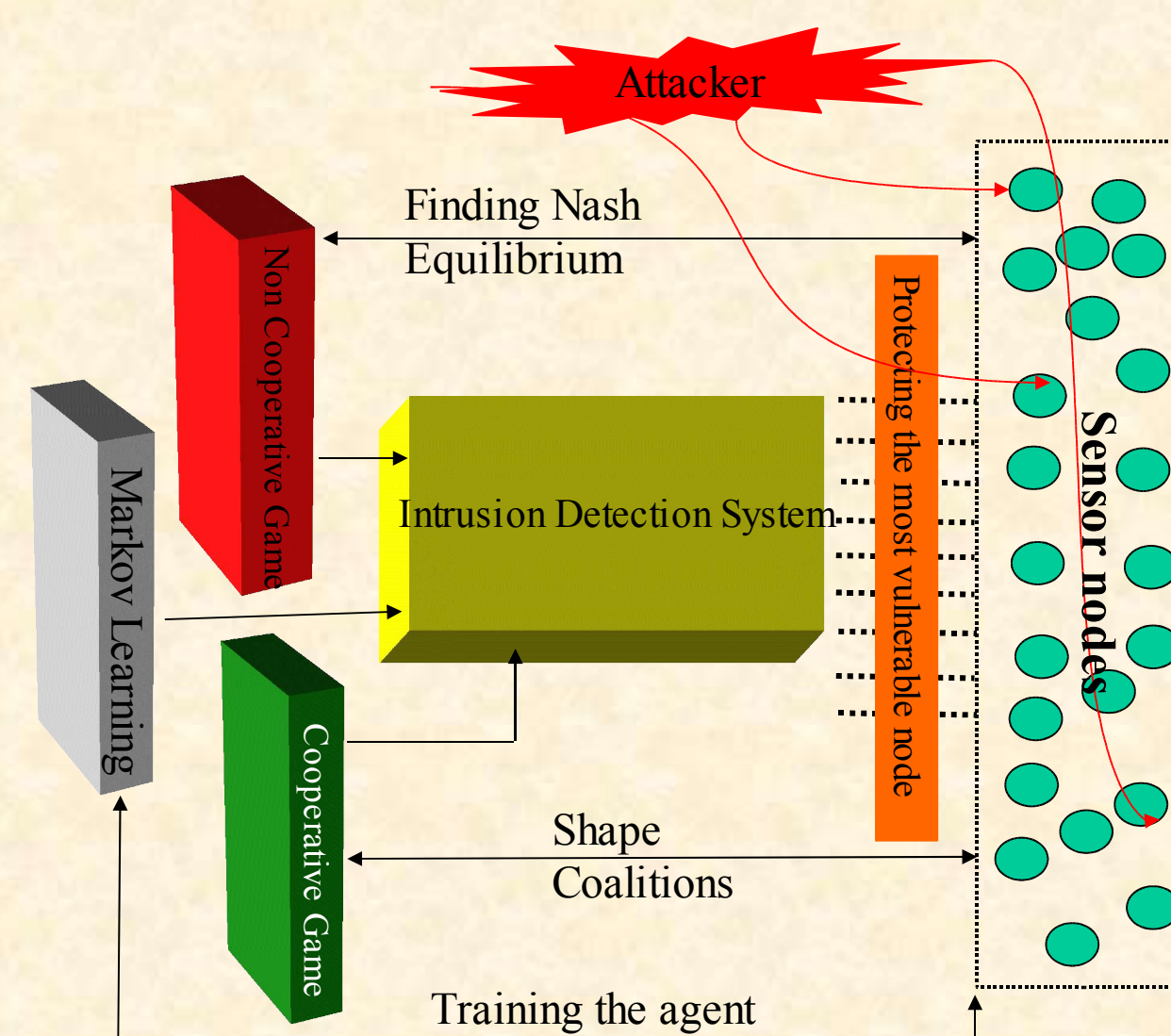
Broader Impact

The PSI framework can be potentially deployed in a variety of safety, security and surveillance instances, including transportation (e.g., air, rail, highway), public utilities (e.g., water, gas, electricity, nuclear, Internet), public or private buildings and gathering places (e.g., airports, train stations, commercial buildings, shopping malls and amusement parks)

Significant Results

Energy-aware Algorithms and Protocols for Sensor Networks

- Data Gathering:** Explores trade-off between data reporting latency and sensing coverage
 - Average data reporting latency is not much affected (< 10%) with 80% sensing coverage
- Clustering:** Uses separate links for control and data collection for delay-adaptive data gathering
 - Up to 70% reduction in transmission distance using sensors with 100 m radio range
- Routing:** Dynamically constructs multiple routes balancing traffic load
 - Much lower sensor failure rate and data delivery latency
- Security:** Game Theoretic Approach to Intrusion Detection (Cooperative and non-cooperative)
 - Average success rate for detecting intrusions is 75% and worst case success rate is 55%

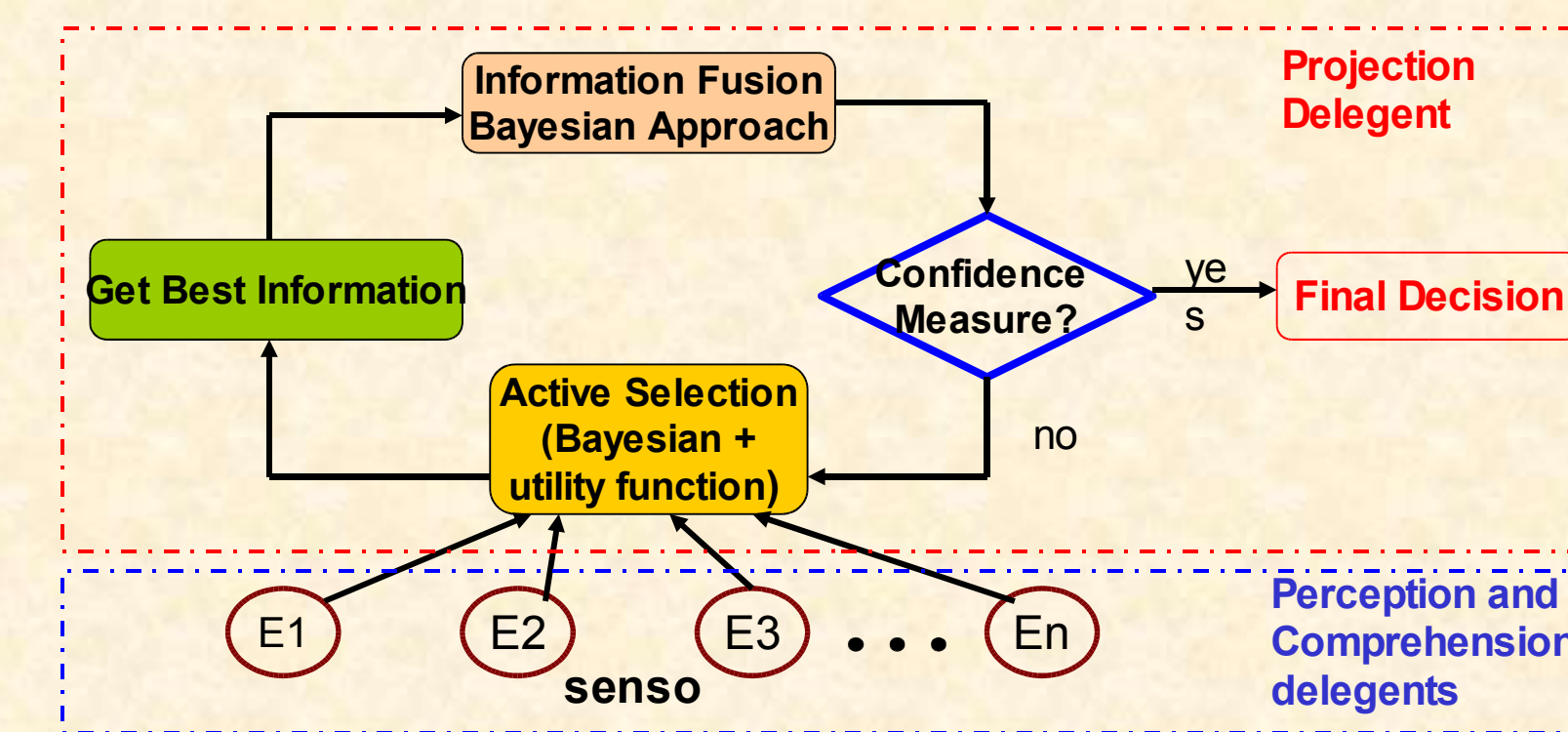


Intrusion Detection using Game Theory

Pervasive Community Computing

Software performing specific activities

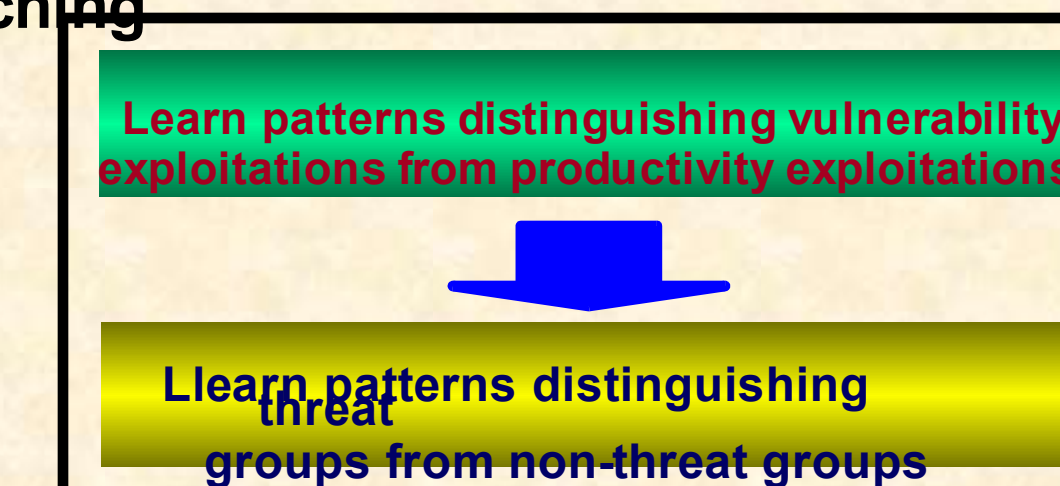
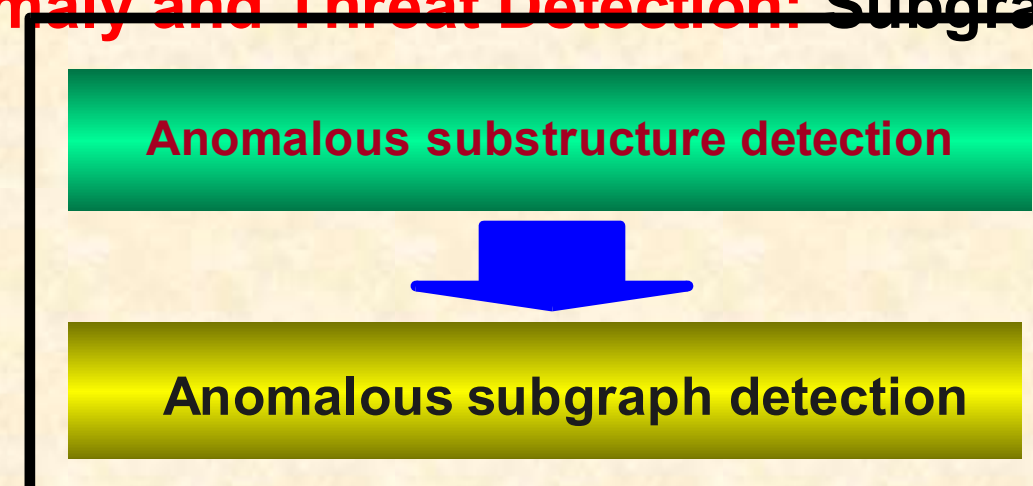
- Information fusion:** Projection delegents



Projection delegent with active information fusion

Graph-based Data Mining (GDM)

- Learning patterns:** Relational data represented as a graph
- Anomaly and Threat Detection:** Subgraph matching



Publications

- A. Agah, S. K. Das and K. Basu, "A Game Theory Based Approach for Security in Sensor Networks", IEEE IPCCC 2004.
- W. Choi and S. K. Das, "Dynamic Path Construction for Route Load Balancing in Sensor Networks", IEEE WCNC 2004.
- S. K. Das, A. Agah and M. Kumar, "Security in Pervasive Computing", Book Chapter, 2004.
- P. De, K. Basu, and S. K. Das, "Ubiquitous Architecture and Protocol for RFID Object Tracking", ACM MobiQuitous 2004.
- A. Tiwari, "Wireless Sensor Networks for Condition Based Maintenance", M.S. Thesis, EE Dept, UT Arlington, May 2004.
- C. Noble and D. Cook, "Graph-based Anomaly Detection," ACM Conf on Knowledge Discovery and Data Mining, 2003.
- L. Holder, D. Cook, J. Noble and M. Mukherjee, "Graph based Relational Learning with Application to Security," 2004.
- M. Kumar, B. A. Shirazi, S. K. Das, "PSI through Community Computing," Workshop on Information Security, 2003.