Simulating Terrorist Threat in the Hats Simulator

Clayton T. Morrison (USC/ISI)
Paul R. Cohen (USC/ISI)
Gary W. King (Umass/Meta!)
Joshua Moody (USC/ISI)
Andrew Hannon (UMass)

http://hats.isi.edu/
Outline

• Introduction
  – Problem domain characteristics

• The Hats Domain
  – Entities, Meetings and Scoring
  – Player actions
  – Meetings planning

• Applications
  – Data generation
  – AIID
  – COLAB
The Hats Problem Domain

- a “society in a box”
- little domain knowledge required
- huge amount of temporal data (data feed, events over time)
- very low signal-to-noise ratio
- requires generating and managing huge number of hypotheses

Find terrorist task forces in the Hats simulator before they can do harm
The Hats Simulator

Hats Simulator
- Meeting Planner
- Scoring

Information Broker
- Cost
- Noise Model

Analyst

Analysis Tools
Hats: Rules of the Game - Entities

- Known terrorists, covert terrorists, benign hats
  - “Terrorist” hats
  - “Unknown” hats

- All hats belong to one or more organizations

- Hats have attributes, attributes are transferable at meetings

- Beacons also have attributes (vulnerabilities)
Hats: Rules of the Game  - Meetings

- All hats go to meetings, all meetings are planned by organization planner (as a part of a task)

- Hats may trade attributes at meetings

- Tasks are planned sequences of meetings designed to bring hats with the appropriate attributes to a target location

- When a collection of terrorist hats with attributes that match vulnerabilities of a beacon (lethal attributes) meet at the beacon, it is attacked
Hats: Rules of the Game - Metrics, Scores

• An *information broker* provides information about hats over time, at a cost (more you pay, better quality info)

• False positives (accusing benign hats) and misses (losing a beacon) are scored

• The goal of the game is to minimize one’s costs
Player Actions

• Pay for information

• Arrest Hats
  Successful if
    (a) hat is a terrorist
    (b) hat is currently part of terrorist taskforce
  Else, false arrest

• Raise beacon Alert Level
When Attack Occurs

IF

• Meeting occurs on beacon
• Meeting is final planned meeting of taskforce
• Meeting participants carry capabilities matching all of the vulnerabilities of beacon
• The taskforce is from a terrorist organization

THEN

Meeting results in beacon being attacked
Terrorist plans

Terrorist organization (known & covert hats)

Non-Terrorist Organization (known, covert & benign)
Terrorist plans

Terrorist organization (known & covert hats)

Non-Terrorist Organization (known, covert & benign)

Task Force

3 May 2005 - http://hats.isi.edu/
Terrorist plans

Terrorist organization (known & covert hats)

Task Force

Target beacon

Non-Terrorist Organization (known, covert & benign)
Terrorist plans

Terrorist organization (known & covert hats)

Non-Terrorist Organization (known, covert & benign)

Task Force

Target beacon

3 May 2005 - http://hats.isi.edu/
Terrorist plans

Terrorist organization (known & covert hats)

Non-Terrorist Organization (known, covert & benign)

Task Force

Target beacon

3 May 2005 - http://hats.isi.edu/
Terrorist plans

Terrorist organization (known & covert hats)

Non-Terrorist Organization (known, covert & benign)

Task Force

Target beacon

3 May 2005 - http://hats.isi.edu/
Terrorist plans

Terrorist organization (known & covert hats)

Task Force

Target beacon

Non-Terrorist Organization (known, covert & benign)
100,000 Hats

3 May 2005 - http://hats.isi.edu/
Implementation

- Hats Code Base
  - developed in Macintosh Common Lisp
  - non-graphical code portable to LispWorks and Franz Allegro (both commercial), and OpenMCL and SBCL (both open source)

- Performance
  - Hats runs a scenario of 100,000 hats for 2000 ticks within a day (roughly 3 ticks/sec without the IB, 2 ticks/sec with the IB)

- Data Export
  - to EAGLE Database (EDB) schema; also export in comma separated value (CSV) and Lisp format
AIID
Architecture for the Interpretation of Intelligence Data

Integrated Interface
(BB Views, Querying, Drilldown)

Blackboard

Actions: Queries, Alerts, Arests
Plans / Threats
Groups / Relational Patterns
Individuals

Control / Agenda

Human Controller
Control Knowledge
Value of Information
Inference Control

Control KS
Control KS
Control KS

Domain KS
Domain KS
Domain KS

Human Analyst
Beacon Alert
Suspicion Scoring
Community Finding

Information Broker

Hats Simulator

3 May 2005 - http://hats.isi.edu/
COLAB

Hats Simulator

Human Analyst

Information Broker

Integrated Interface
(Views, Querying, Drilldown)

Analyst Workspace

Shared Workspace

Services

Beacon Alert

Suspicion

Community Finding

Knowledge Services

Information Broker

Integrated Interface
(Views, Querying, Drilldown)

Analyst Workspace

Shared Workspace

Services

Beacon Alert

Suspicion

Community Finding

Analyst Workspace

Shared Workspace

Knowledge Services

Information Broker

Integrated Interface
(Views, Querying, Drilldown)
COLAB Session: ID032

User: clayton [Modify Profile]
Rating: 60

Browser Interface

Enter Command

(select hats
  from :terrorist-hats
  where (and (near :b012 it)
    (overlap [attributes :b012] it)))

Submit Clear

Space Instance Contents
--------------  -------
:IJARA-WORKSPACE Empty
:FRAGMENTS Empty
:HYPOTHESES 3 instances (1 BEACON; 2 HAT)
:LABELS Empty
:RAW-REPORTS 6 instances (6 BASIC-ENTITY-REPORT)
:REPORTS Empty
:SETS

Done

3 May 2005 - http://hats.isi.edu/
End
# Scores

<table>
<thead>
<tr>
<th>COSTS</th>
<th>The total amount of “algorithmic dollars” spent on information from the information broker</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEACONS ATTACKS</td>
<td>The number of attacks that were planned</td>
</tr>
<tr>
<td>total-potential-attacks</td>
<td>The number of terrorist attacks that succeeded</td>
</tr>
<tr>
<td>beacon-attacks</td>
<td>The number of attacks that were stopped by successful arrests</td>
</tr>
<tr>
<td>beacon-saves</td>
<td></td>
</tr>
<tr>
<td>ARRESTS</td>
<td>The number of arrests that succeeded</td>
</tr>
<tr>
<td>successful-arrests</td>
<td>The number of attempted arrests that did not succeed</td>
</tr>
<tr>
<td>false-arrests</td>
<td></td>
</tr>
<tr>
<td>BEACON ALERTS</td>
<td>The number of alerts at level 1 during which an attack occurred</td>
</tr>
<tr>
<td>level-1-hits</td>
<td>The number of alerts during which no attack occurred</td>
</tr>
<tr>
<td>level-1-false-positives</td>
<td>Same as level-1-hits, but for level-2 alerts</td>
</tr>
<tr>
<td>level-2-hits</td>
<td>Same as level-1-false-positives</td>
</tr>
<tr>
<td>level-2-false-positives</td>
<td></td>
</tr>
</tbody>
</table>
Player Hypotheses

- Kinds of hypotheses
- Different time scales
- Relations between hypotheses
Trellis-authored Hypotheses

- Using Trellis to structure relationships between propositions
Trellis-authored Hypotheses

- Trellis table representation
  - facilitates quick, informative comparison

<table>
<thead>
<tr>
<th>Group</th>
<th>Capability Overlap</th>
<th>Suspicion</th>
<th>Proximity to Beacon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1 Threatens</td>
<td>Overlaps 3/4 Capabilities</td>
<td>Very Suspicious</td>
<td>Near</td>
</tr>
<tr>
<td>Beacon :B012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group 2 Threatens</td>
<td>Overlaps 1/5 Capabilities</td>
<td>Moderate Suspicion</td>
<td>Far</td>
</tr>
<tr>
<td>Beacon :B012</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group 3 Threatens</td>
<td>Overlaps 7/8 Capabilities</td>
<td>Not Suspicious</td>
<td>Far</td>
</tr>
<tr>
<td>Beacon :B012</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AIID

Architecture for the Interpretation of Intelligence Data

Interface to analysts, making this a mixed-initiative system

Integrated Interface
(BB Views, Querying, Drilldown)

Blackboard

Actions: Queries, Alerts, Arrests

Plans / Threats

Groups / Relational Patterns

Individuals

Control / Agenda

Control KS

Analysts’ control guidance

Hypothesis management

Value of Information reasoning

Domain KS

Theory of rational detection schemes

Recognize and learn temporal patterns

Group detection

Suspicion Scoring

Information Broker

Queries

Hats Simulator

Generatively planned behaviors, low domain knowledge, very low signal to noise, large scale, data-feed

3 May 2005 - http://hats.isi.edu/