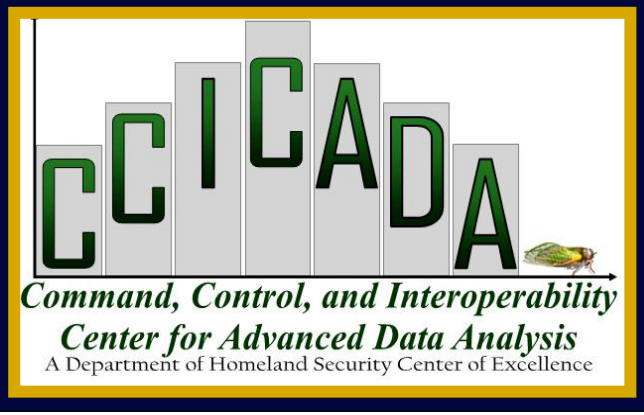
Analytical Approaches to Aviation Security at CCICADA

Command, Control and Interoperability Center for Advanced Data Analysis

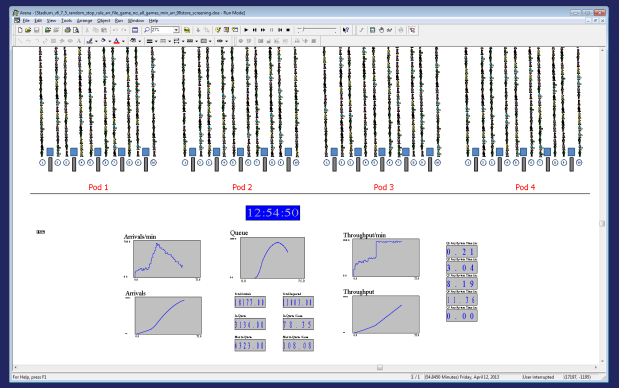
A Department of Homeland Security University Center of Excellence based at Rutgers University

Fred Roberts
Director, CCICADA



Example 1: Stadium Security

- Models for patron inspection – applied at MetLife and other stadiums
- Working with every major sports league:
  - NFL, NBA, MLB, NHL, USLTA, MLS, NASCAR
- Working with venues nationwide
- CCICADA simulation tool allows varying:
  - Patron arrival rates
  - Throughput for WTMDs
  - Timing for secondary screening
  - Varying security settings on WTMDs
  - Randomization of settings, alarms, etc.
- Used to determine:
  - Number WTMDs needed
  - Number screeners needed
  - Number secondary screeners needed
- ***Key observation with implications for the airport of the future: WTMDs "perform" very differently in real-world settings such as outdoors than they do in the lab.***



CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

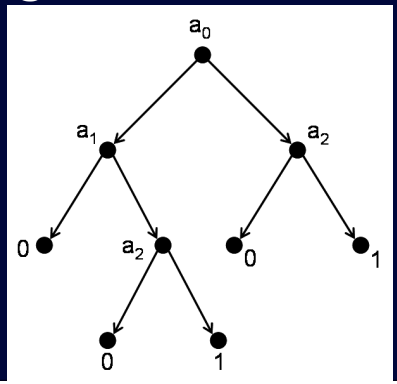
Example 2: Port Authority Bus Terminal

- PABT in NYC: world's busiest bus terminal
- Critical transit facility to move people between NYC and NJ
- Central part of any emergency evacuation scenario for Manhattan
- Terminal faces major crowd management issues:
  - Movement of people through the terminal at high traffic times
  - Overcrowding and crowd management issues during emergency situations
    - Upon reopening after Super Storm Sandy and NYC Blackout, passenger lines extended out into the street.
- ***Key observation: Long queues make people vulnerable to Boston Marathon-type situations***
- CCICADA project: Design a state-of-the-art, 3D agent-based integrated simulation for human crowds and vehicles for the PABT:
  - Pedestrian Movement
  - Pedestrian Movement and 3-D Bus Movement
  - Crowd Simulation/Bus Traffic Management
  - Assist plans for crowd management during reconstruction

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

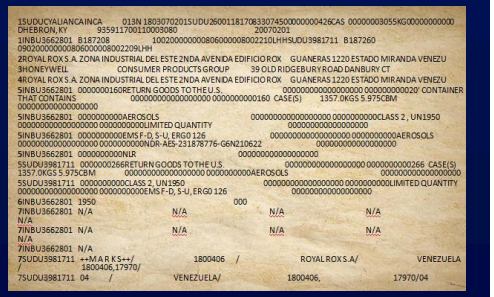
Example 3: Inspection Algorithms

- Work with CBP, Coast Guard
- Stream of containers arrives at a port
- The Decision Maker's Problem:
  - Which to inspect?
  - Which inspections next based on previous results: "sequential diagnosis"
- Approach:
  - Use binary decision trees (BDTs): go left if pass test a_i, right otherwise
  - End with output 0 (pass) or 1 (open the container)
  - Finding the "least cost" binary decision tree is computationally intractable once the number n of types of tests gets too large.
  - Stroud Saeger LANL approach feasible up to n = 4, not n = 5 (Port of LA-Long Beach: n = 5)
- ***Key Observation: Algorithms for inspection are difficult to obtain due to "combinatorial explosion": there are*** 5×10^{18} ***BDTs corresponding to all Boolean decision functions***
- Our results:
  - New search algorithms work for n = 5.
  - Genetics-algorithms search allows us to go to n = 10
  - Our SNSRtree software allows us to go to n = 20 on laptop

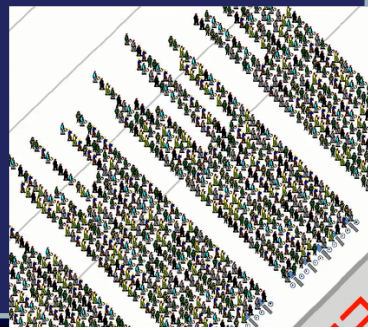


Example 4: Risk Scoring for Containers/Cargo

- Risk assessment a key part of airport security
- Project supported by Domestic Nuclear Detection Office
- Goal: Predict risk score for each container
  - Quantify the likelihood of need for inspection
  - Based on manifest data
- Methods
  - We have developed machine learning algorithms to detect anomalies in manifest data.
    - Text mining on verbiage fields leads to useful characteristics/features.
    - Then regression based on the useful characteristics or "covariates"
    - "Penalized regression" using LASSO and Bayesian Binary Regression software developed by our group gives us a risk score for a container.
    - Looked at manifest data before and after Japanese tsunami. Found significant differences for some features and not for others.
- ***Key observation: Do not depend on just one feature when looking for anomalies***



CCICADA
Command, Control, and Interoperability
Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Example 5: Simulation Models

- Simulation tools used in stadium inspection work – discrete event simulation
- Also used to simulate operations of a port of entry
  - Work with CBP
  - Port of Newark-Elizabeth
  - Led to new ways to measure success of inspection processes
  - Contributed to “outside the box” idea of inspection of containers offsite in warehouses
- Airport Simulation Models:
  - Study arrivals of international passengers at Newark Liberty International Airport
    - With CBP
    - Advance warning of numbers of arriving passengers
    - Division into citizens and non-citizens
    - Modeled passport check lanes; queue lengths
    - Modeled effect of change of number of inspectors, of change in processing time
    - Similar methods applicable to departing passengers
- ***Key Observation: All simulation models involve simplifying assumptions, but allow “what-if” experiments that support planners and policy makers***