Machine Intelligence in Decision-making (MInD)
Automated Generation of CB Attack Engagement Scenario Variants

Nadipuram R. Prasad
Arjun S. Rangamani
Timothy J. Ross
M. M. Reda Taha
Frank Gilfeather

BO05MSB070: Multivariate Decision Support Tool for CB Defense
DTRA University Strategic Partnership
Gold Team
New Orleans Scenario
Fundamental Principles

1. Human decision-making is analogous to finding Order within Chaos
2. Order requires Structure
3. Structure requires Rules for preservation
4. Rules must be learned and applied
5. New Rules are discovered as Information (Data) evolves
Order in Scenario Generation

- Experts match the characteristics of the attacker with postulated attack characteristics to generate engagement scenarios that provide a basis to evaluate the consequences of the attack.

- Base-Case Variants show the effectiveness of mitigating factors on the consequences including the cost of mitigation.

- The set of Base-Case and Variant exemplars provide the means to develop appropriate cost models that can aid in evaluating S&T funding required to mitigate the consequences.

- To preserve “order” in scenario variant generation, a set of Rules governing the relationships between the CB attack Base-Case and Variant exemplars must be “extracted” and “learned” so that many Variants can be generated for further analysis.
Automatic scenario generation is based upon Bose-Einstein’s Large Deviation Theory (LDT).

The fundamental principle of LDT is founded in: “Exponential Asymptotics for Good Sets.”

- What this means is that all sets of new scenario variants must exhibit exponential asymptotic behavior, and satisfy all properties of compact sets.
Exponential Asymptotics

![Graph showing exponential curves with time constants τ=1, τ=2, and τ=5, demonstrating increasing effectiveness of mitigating parameters and a value at 1 time constant](image-url)
Exponential Asymptotics
Exponential Asymptotics
Exemplar Set of Base-Case Engagement Scenario and Variants
Adaptive Network Fuzzy Inference System (ANFIS)

- ANFIS is a set of fuzzy inference rules written in a neural network structure.
- Rules are extracted from exemplar data and learned.
- The resulting fuzzy-neural structure can be used to identify the effectiveness of mitigating factors on the consequences of CB attack scenarios.
Scenario Variant Generation

• Exemplars of scenarios provided by CB Experts are used to train ANFIS rule-based structures and provide the means to generate hundreds and thousands of interpolated scenario variants.

• Large numbers of variants provide the means to Rank the effectiveness of mitigating factors on minimizing the overall consequences, and in identifying the total cost of additional S&T funds required.
Relative Effectiveness Between Base Case Engagement Scenario and Variants

- Human Casualties
  - Max. V0
  - Min. 0
- Remediation Costs
  - Max. V0
  - Min. 0
- Days of Mission Disruption
  - Max. V0
  - Min. 0
- Cost of Additional S&T Dollars
  - Max. V0
  - Min. 0

Relative Effectiveness between Exemplars vs. Time

- Graphs show relative effectiveness changes over time for different scenarios and variables.

Graphs depict:
- Comparison of V0, V1, V2 for different metrics.
- Markers indicating specific values or conditions for each exemplar.
Evolution of Possibility Trees & Engagement Scenario Variants
Fuzzy Inferential Rule-based Model (FIRM)
Scenario Variant Generation Using FIRM

**Attack Variables**
- Perpetrators
- Motivation
- Military Facilities
- Chemical Agent
- Dispersal Mechanism
- Proximity to Civilian Infrastructure
- Air flows
- Access to Offsite Medical Service (Scale 0 - 5)
- Access to Civilian Hazmat response (Scale 0 - 5)

**Attack Mitigating Variables**
- Presence of wall or fence
- Presence of barricaded gates
- Number of armed guards
- Type of Chemical detector
- Range of Detection
- False Positive Rate
- False Negative Rate
- Number of Sensors
- Type of Chemical Prophylaxis
- Risk level of side effects
- Prophylaxis effectiveness
- Number of successive days for treatment
- Minimum number of days between pretreatment cycle
- Number of base personnel receiving prophylaxis normally
- Type of Medical treatment
- Effectiveness of treatment
- Number of medical personnel covered by antidote
- Trained on-site personnel (Scale 0 - 5)

**ANFIS Rulebases for**
- Attacker's Impact (Scale 0 - 1)
- Attack Impact (Scale 0 - 1)

**ANFIS Rulebases for**
- Effectiveness of Perimeter Protection (Scale 0 - 1)
- Effectiveness of Chemical Detector (Scale 0 - 1)
- Effectiveness of Chemical Prophylaxis (Scale 0 - 1)
- Effectiveness of Medical Treatment (Scale 0 - 1)

**Fuzzy Inferential Rule-based Model (FIRM)**
for Chemical Attacks

**ANFIS Rulebases for**
- Geo-Political Impact
- Number of Human Casualties
- Number of days of mission disruption
- Remediation Costs (in millions of US $)
- Cost of additional S&T into CB defensive measures and their deployment

**Evolutionary Computation**
- Rank Ordering

**Chemical Attack Consequence Database**

**Weights of Attack and Attack Mitigating Variables on Effectiveness**
- **Weights of Attack Mitigating Variables Effectiveness on Consequences**
- **Attack and Attacker Impact**
- **Attack Mitigating Variable Effectiveness**
- **Multiplexer**
Learning Systems

(a) Iterated learning through supervision

(b) Iterative learning through evolution
Evolutionary FIRM (E-FIRM)

1. Randomly generated population of Mitigating Variable Sets $M(n,p)$
2. CB Defense Measures ($M$)
3. New Generation of Mitigating Sets
4. ANFIS-Based FIRM
5. Consequences ($C$)
6. Desired Consequences ($C_d$)
7. Fitness Function ($e$)
8. Fitness-based Ranking
9. Selection
10. Crossover & Mutation
11. Elitism

Decision:
- $\text{Is } \text{Abs} \left[ \frac{e(i)}{n} \right] < b$?
  - Yes
  - No

Flowchart:
- Input: Randomly generated population of Mitigating Variable Sets $M(n,p)$
- Process: CB Defense Measures ($M$) → New Generation of Mitigating Sets → ANFIS-Based FIRM → Consequences ($C$) → Desired Consequences ($C_d$) → Fitness Function ($e$) → Fitness-based Ranking
- Output: Selection, Crossover & Mutation, Elitism
Spectrograph of Variant Evolution
Cost Model

\[ [\theta_1, \theta_2] = f[\text{Eff}_1, \text{Eff}_2, \text{Eff}_3, \text{Eff}_4, \text{Eff}_5, \text{Eff}_6, t_1, t_2] \]

\( \theta_1, \theta_2 \) are the Cost of S&T and the Cost of Deployment

\( \text{Eff}_i |_{i=1}^6 \) are the mitigating factor effectiveness

\( t_1, t_2 \) are the time required to achieve the desired effectiveness

This is a nonlinear mapping for which a Radial Basis Function Neural Network with dynamic allocation of neurons has been applied
S&T Cost to minimize Human Casualties based solely upon Expert generated Engagement Scenario exemplars
Advances in 
*CB* Attack Analysis

- It is shown that a “rule-based” inferential method with ability to “learn” CB attack scenarios and consequences, and “evolve”, is necessary for machine intelligence in decision-making (*MInD*) where multitudes of scenario variants can be generated on demand.

- The structure of *MInD* is explored within an evolutionary framework to emulate Human-like learning and decision making for *CB* attack analysis.

- A fuzzy-neural system embedded in the Fuzzy Inferential Rule-based Model (FIRM) exhibits learned decision-making abilities to predict the effectiveness of mitigating factors on consequences.

More …..
Advances in

*CB* Attack Analysis

• An evolutionary structure (E-FIRM) allows the examination of multitudes of mitigating factor variants using FIRM as a kernel to yield a desired set of consequences

• The evolutionary structure allows the formulation of appropriate neural network-based Cost Models that provide a basis for ranking alternatives and for optimizing on the cost of S&T funding and cost of deployment over the desired time horizons
Q & A

Work supported under
BO05MSB070: Multivariate Decision Support Tool for CB Defense,
DTRA University Strategic Partnership, Gold Team

Ram Prasad
Associate Professor, E&CE
Director, RioSoft & RioRoboLab
New Mexico State University, Las Cruces, NM 88003
Email: ramprasad@msn.com