An Outline of the Three-Layer Survivability Analysis Architecture for Information Warfare Research

Sam Ma  Axel Krings  
University of Idaho  
Frederick Sheldon  
Oak Ridge National Laboratory

Outline

- Introduction
- Challenges in Modeling Information Warfare
- Tactical Level Modeling
- Strategic Level Modeling
- Operational Level Modeling
- Summary
What is Strategic Information Warfare (IW)?

- Two fundamental elements manipulated in any warfare are the energy and information.
- What distinguishes Strategic Information Warfare from the traditional use of information in warfare or other digital attacks in some specific domains (such as unauthorized hacking, computer crimes, and economic espionage) lies in:
  Strategic IW is a means for state or non-state actors to achieve objectives by digital attacks on its adversary's centers of gravity (Rattray 2001).
- Centers of Gravity = National Information Infrastructure (NII)
- NII Supports National Critical Infrastructures
- Protection of National Critical Infrastructures needs Survivability Research; Survivability≈Defensive IW.

What is Strategy?

- According to Deibel (2007): “Strategy is a plan for applying resources to achieve objectives.” A nation state has an hierarchy of strategies, from military, grand, national security, foreign affair, national strategy.
- IW strategy should be a subset of military strategy or parallel with it.
- We assume that IW is conducted in an isolated electronic cosmos (e-cosmos).
- Three-layer survivability analysis is an enhanced evolutionary game modeling architecture, enhanced with survival analysis, dynamic hybrid fault models, since evolutionary game theory alone is not sufficient for the problem of survivability or IW.
What are the major challenges in devising IW strategies?

- **Uncertainty** (Unpredictable, latent, Unobserved or Unobservable Risks) = UUUR
- **Vulnerability** (~ fitness, reliability, survivability)
  - Survivability curve is the reliability curve with finite discontinuous points.
- **Deception** As Sun Tzu stated, “All warfare is based on deception.” Deception is particularly striking in IW since it create asymmetric faults.
- **Rationality** (required by traditional game theory)
- **Aggression** (Competition) and **Coalition** (Cooperation).
- All of the above can be time and space dependent. Further, nonlinearity often changes things to counter-intuitive, or even chaotic (catastrophic).

Existing Research: Risk Analysis & Game-Theoretic Modeling.

  - Jormakka & Mölsä (2005) commented: "It seems, however, impossible to assign probabilities to various attack types. … This time dependency associated with lack of knowledge makes building and updating a detailed attack tree practically impossible."
- **Three problems**: Rationality assumption; probability distribution of mixed strategies; and deception.
Overview of the Three-layer Survivability Analysis Architecture

- **Tactical level:** Estimate vulnerability (reliability) and the consequences of UUUR events with survival analysis (SA), competing risks, and multivariate SA.
- **Strategic level:** Core is the dynamic hybrid fault models, which is an evolutionary game system, enhanced by Agreement algorithms and the tactical level models. It derives survivable strategies, deals with time and space dependent vulnerability, deception, and rationality.
- **Operational level:** Hedging and decision-making.

Tactical Level Modeling

States and Failure Behavior of a node in E-Cosmos. (modified from Ma & Krings 2008e)
Why do we use Survival Analysis, rather than the traditional Reliability Analysis?

1. Constant and Homogeneous Failure Rate
2. Binary Failure (Univariate Reliability) vs. Performance Degradation (Multivariate Failure)
4. Observation Censoring
   - Censoring can be left, right, random, interval.
   - Truncation can be left or right, it affects all objects under observation.
   - Censoring is generally unpredictable. e.g., systematic censoring of smoker in clinical trial would affect integrity of results.
5. We take advantages from the “censor-processing” of Survival Analysis to assess the consequences of UUUR Events (Ma 2008)

Survival Analysis, Competing Risks Analysis and Multivariate Survival Analysis (MSA)

- Fundamental Model of Survival Analysis
  Hazard Function $\lambda(t, z)$ is a function of time $t$ and covariate vector $z$:
  $\lambda(t, z) = \lambda_0(t) \exp(z\beta)$, $\lambda$ is a vector of functions in MSA.
  Conditional Survival Functions (on $z$)
  $S(t; z) = [S_0(t)]^{\exp(z\beta)}$, $z$ is the covariate vector or matrix in MSA
- MSA is truly multivariate, has the potential to overcome all four limitations identified previously.
- Use *Shared Frailty* to model the effects of *unobserved* or *unobservable* risks (Frailty=Vulnerability + Risks).
- Competing risks analysis: effects of latent risks.
- Spatial Shared Frailty: vulnerability distribution in space
One Problem, Two Aspects and Two-parts solution.
(1) Agreement Algorithm (Hybrid Faults) Aspect—Time-Dependent Hazard Function
(2) Reliability Analysis—Byzantine Generals Playing Evolutionary Game.

Lamport (1982): Byzantine General Problem: \( n \geq 3m + 1 \)

---

One Problem: Agreement Aspect

- Agreement algorithms focus on reaching agreement in the presence of faults (traitors), e.g., \( N \geq 3m + 1 \). Time notion is ignored largely.
  - it is treated as discrete "rounds", rather than real time.
- Example
  - A bill is presented to Congress. Two opposing sides try to defeat each other.
  - Lobbyists trying to influence the delegates.
  - The bill has to be voted before the end of the summer recess. It is correct to say that 2/3 majority is needed to pass the bill.
  - However, there are time-dependent covariates that influence the delegates.
  - The minds of the delegates may change from day to day.
  - Each delegate has a different “hazard” (fitness) function, which determines how long it takes for an delegate to make his or her mind.
    - \( \lambda(\theta) = f( \text{effort of lobbyist, media influence, constituent, party strategy, ...} ) \)
- The voting result or the agreement should depend on time.
One Problem: Reliability/Vulnerability/Survivability Aspect

- At time of voting counting votes is simple
  - E.g., count 2/3rd majority
- However, assessing probability to reach an agreement each day is not trivial at all!
  \[ \lambda(t) = g[\lambda_i(t)] \text{ or } \lambda(t) = g[\lambda_R(t), \lambda_D(t), \lambda_I(t), z] \], \( z \) could be lobbyists
- What is the form of \( g \)
  - They may be playing “games”, best be described with math games.
  - Simple addition or even complex survival function is not sufficient.
  - Traditional Game is not sufficient because of the rationality limitation.
  - The core of Evolutionary Game is applicable, but it has to be extended.

Two-Parts Solution:

- First part: Time-Dependent Hazard or Survivor Function
  - each general is assigned a time- and covariates dependent hazard function or survivor function.
  - Previous survivor analysis models offer ideal solution.
  \[
  N(t) \geq 3 \times m(t) + 1 \\
  N(t) = N(t - 1) \times S(t | z) \\
  m(t) = m(t - 1) \times S(t | z)
  \]
- Second part: Byzantine Generals Playing Evolutionary Game
  - Evolutionary Game is necessary, but not sufficient.
  - Need to deal with dynamic uncertainty, vulnerability, deception.
  - Need to deal with other strategies such as aggression and coalition.
An example demonstrating DHF

Changes of the Number of “Generals” over Time (Population Dynamics of Total and Traitor Generals) Ma & Krings (2008e, Ma 2008)

Real-time dynamics of the Fault Tolerance Level in Byzantine General Problem. The constraint is dynamically checked. Ma & Krings (2008e, Ma 2008)

Byzantine Generals Playing Evolutionary Game: Inspiration from Evolutionary and Behavior Ecology (Ma 2008, 2009)

- “On the Origin of Species” – Natural Selection or Struggle for Living. Darwin 1859
- “The Decent of Man, and Selection in Relation to Sex” 1871
- “The Expression of the emotions in man and animals” 1872.
- “Altruism”=Cooperation, there are five mechanisms of cooperation in nature: Kin Selection, Direct Reciprocity, Indirect Reciprocity, Graph Selection, and Group Selection. (Hamilton 1963, The Evolution of Altruistic Behavior).
- Evolutionary Game Theory (John Maynard-Smith and George Prince 1973)
- The most famous research now is “Prisoner’s Dilemma (PD) Game (Axelrod & Hamilton 1981), but before PD, there were extensive research in biology already.
- Deception, honesty, or the reliability of animal communication. Handicap Principle (Zahavi 1997). Sir Philip Sydney (SPS) game, which has been used to demonstrate the handicap principle—that animal communication is honest (reliable) as long as the signaling is costly in a proper way.
- Animal Communication Networks (McGregor 2003)
- Reliability Modeling of Animal Communication Networks (Ma 2009)
- 3C=Competition, Cooperation, and Communication vs. War, Peace and Information (Ma 2009)
**Evolutionary Game Theory** = Game Theory + Darwin Evolution + Population Dynamics

Malthusian Population Dynamics
\[
\frac{dN(t)}{dt} = r_m N(t) \quad N(t) = N(0) e^{r_m t}
\]

Logistic Population Dynamics
\[
\frac{dN(t)}{dt} = rN(t) \left(1 - \frac{N(t)}{K}\right) \quad N(t) = \frac{K}{1 + e^{-rt}}
\]

\( r \) is called fitness function

N-strategy system
\[
\frac{dx_i}{dt} = x_i [f_i(x_i) - f(x)]
\]

Constant Failure Rate Model is the Solution of Malthusian model.
\( R(t) = e^{-\lambda t} \)

Failure Rate \( \lambda \) is equivalent to Malthusian - \( r_m \).

Logistic Growth Model can be similarly extended to Reliability model - then \( \lambda \) is not constant.

---

**Enhanced Evolutionary Game Modeling**

“**Byzantine Generals Playing Evolutionary Game**” (Ma 2008)

- “**Byzantine Generals Playing Evolutionary Game**”
- **Node** is evolutionary game player
- **Fitness (payoff)** = **Reliability** = **Survivor** | **Hazard Function**
- **Strategies** = **Behaviors of Nodes** (Attack, Retreat, Benign, Malicious ...)
- **Rationality** is not necessary, since strategy is evolved.
- **Uncertainty** (UUUR) is carried over from tactical level (Survivor ...)
- **Vulnerability** ~ **Reliability** ~ **Fitness**
- **Deception** is detected with **Agreement algorithms** in Dynamic Hybrid Fault models and enforced by the Handicap principle (Ma 2009)
- Evolutionary stable strategies (ESS) are “immune” to both internal mutation and external disturbance.
- **ESS** ~ **Survivable Strategies**.
without UUUR events: reliability = survivability i.e. reliable system is survivable

- With UUUR events: reliability ≠ survivability
  - “Precise” solution is impossible
  - ESS is still assessable, but it cannot be implemented due to the inability to associate real time with ESS.
  - Proposed remedy for inherited difficulties: hedge.
  - Working survivability metric is introduced, which is the reliability with UUUR influences considered, Ru(t).

Operational Level Modeling: Duo of Survivability Metrics (Ma 2008)

- Action Threshold Survivability (TS)
  - TS = Ru(s)

- Expected Survivability (ES)
  - ES = Ru(t), with s < t, s, t are approximate

- The relationship between TS and ES can be approximated by simulation
  - i.e., for specified ES, corresponding ESS can be obtained from the simulation.

- Need to monitor the change of Ru
  - when Ru < Ru(s), action is triggered.
  - The action is taken to assure, e.g., ESS is in place.
  - Future ES(t) is warranted with certain confidence level.

- Multiple TSs may be used to ensure more effective decision-making.