Applying Game Theory to the Domain of Information Warfare

Samuel N. Hamilton, Wendy L. Miller, Allen Ott

ORINCON Information Assurance

O. Sami Saydjari

SRI International

Why Game Theory?

• Provide a different prospective from human analyst by considering millions of possible scenarios, not just the few most probable

• Suggest and explore multiple what-if possibilities, and provide projection based explanations for suggested COAs

<u>Potential Uses</u>

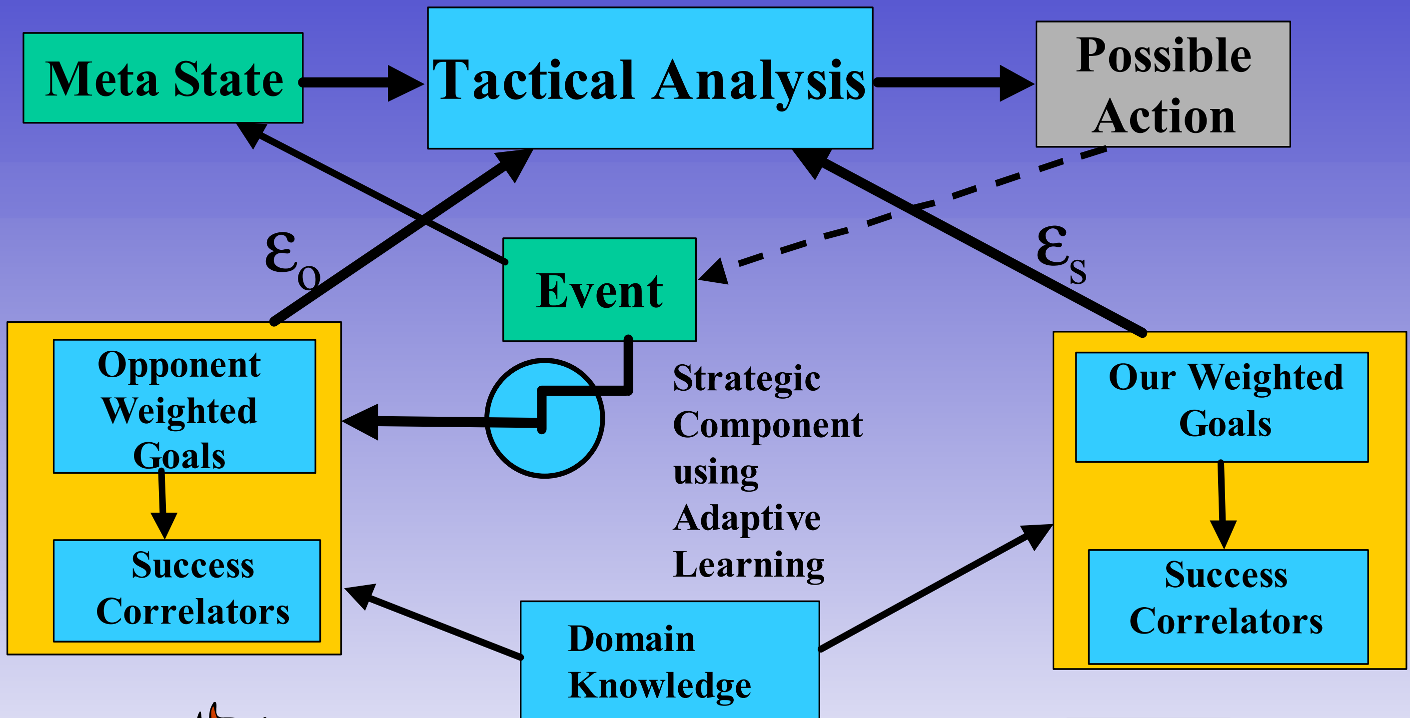
Analysis Tool
Training Tool
Opponent Modeling

ORINCON
INFORMATION ASSURANCE

SRI International

DARPA

Envisioned System Architecture



ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenges in Applying Game Theory to Information Warfare

1. There are limited examples to draw from.
2. Players can make multiple, simultaneous moves.
3. Opponents are under no time control constraints.
4. Opponents may have different end goals from us.
5. The set of known legal moves may change during the game.
6. Opponent resources and end goals may change during the game.
7. Timing for move and state updates is not well defined.

ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Limited Examples

Problem: No Large databases of games between acknowledged masters

Effect: Limits automated evaluation function tuning, makes program validation and testing more difficult

Possible Approaches: deep fast searches reduce the importance of tuned evaluation functions…online learning is also possible but risks leadability

ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Multiple Simultaneous Moves

Problem: Opponent can attack multiple places simultaneously without allowing us to respond

Effect: Potentially explosive move set size

Possible Approaches: redesign null-move searches to allow for opponent-forced null-moves

Challenge: No Time Constraints

Problem: Time constraints are often radically different in this domain than in traditional game tournament conditions

Effect: reduces the effectiveness of broad searches, invalidates depth based opponent modeling literature

Possible Approaches: more selective searches, utilize time intensive hill climbing based opponent modeling

ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Opponent has Different End Goals

Problem: mini-max based approaches assuming $\varepsilon_o = -\varepsilon_s$ lead to poor predictions

Effect: many pruning techniques such as alpha-beta cannot be used, opponent modeling techniques assuming maximum variance invalid

Possible Approaches: prune using iterative, probability based cut-off, use multiple opponent seeds representing traditional adversaries

ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Set of Known Moves may Change

Problem: opponents can do moves not previously considered

Effect: analysis that relies on brute-force calculation to solve troublesome situations is unreliable

Possible Approaches: expand the definition of Quiescence to take into account the fact that opponents are more likely to spring surprises in some situations than others

ORINCON
INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Opponent May Change During Game

Problem: opponent goals, resources, or even identity may change during the course of a game

Effect: no opponent modeling techniques consider this possibility

Possible Approaches: model opponent from multiple starting points, and compare model prediction effectiveness

ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Challenge: Timing not Well Defined

Problem: in most games, moves occur instantaneously…in this domain moves can take a variable amount of time

Effect: Reliance on a fixed time may lead to brittle, dangerous move tree suggestions

Possible Approaches: allow moves multiple probability weighted outcomes with a range of times for completion

ORINCON INFORMATION ASSURANCE

SRI International

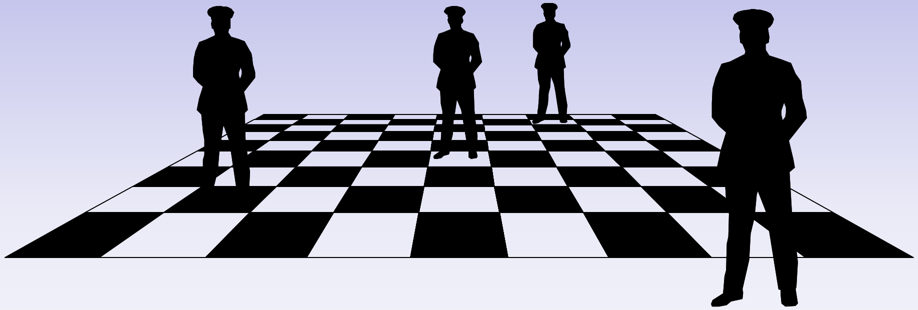
DARPA

Current Project State

1. Working Prototype for New Search

- state representation
- move set
- multiple opponent models
- mission model and evaluation function generation

2. Framework for Genetic Algorithm Based automated opponent model generation



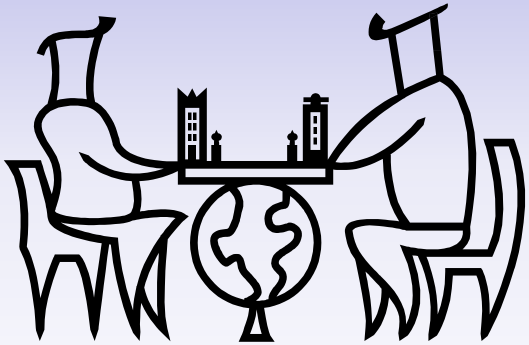
ORINCON INFORMATION ASSURANCE

SRI International

DARPA

Conclusions

- System is quite capable of discovering clever, timing based attacks
- It is crucial to define move set and state representation at the proper granularity level
- There are numerous, segmentable research topics providing a rich area for collaborative works between AI research communities and security research communities



ORINCON INFORMATION ASSURANCE

SRI International

DARPA