CSE468
Information Conflict

Dr Carlo Kopp, MIEEE, MAIAA, PEng
Clayton School of Information Technology,
Monash University, Australia

Background Briefing

Background Briefing (1)

- CSE468 Information Conflict is a 13 week advanced honours level module (2 hr lecture + tutorial per week) providing an introduction to Information Conflict theory.
- The module is unique, *globally*, as it is the first to address this problem area with a mathematically oriented approach, using information theory and game theory to provide models.
- CSE468 was designed and implemented by Dr Carlo Kopp, who was one of the originators of the information theoretical approach to this broader problem area.
- As the module is constructed for 4th year honours undergraduates in computing sciences, much of its focus is on mathematical underpinnings of the area and mathematical modelling of such problems.

Background Briefing (1)

- The module syllabus and structure is oriented to provide students with a robust understanding of the fundamental mathematical models which underpin this research area.
- As strong prerequisite knowledge and understanding of information theory and game theory cannot be assumed, the module provides introductory lectures and tutorials covering these two areas.
- Two thirds of the remaining syllabus deals with a mathematically oriented treatment of key aspects of this area, including the four canonical strategies and application of these to compound strategies and hypergames.
- The remaining syllabus provides an overview of applications, examples and case studies, exploiting the theoretical material covered in preceding lectures.

Module Structure (1)

1. Introduction and overview - Lecture Notes
2. Shannon's information theory concepts - Lecture Notes
3. Basic game theory concepts - Lecture Notes
4. Four canonical strategies of information conflict vs Shannon's information theory - Lecture Notes
5. Compound information conflict strategies and using graphs to model these - Lecture Notes
6. Hypergames vs information conflict strategies - Lecture Notes
7. Evolutionary nature of information conflict and biological examples - Lecture Notes and IWC3 Slides

Module Structure (2)

8. Class I, II, III, IV information warfare, denial of service attack classification; Analysis and modelling of and techniques - Lecture Notes
9. Classical deception techniques, perception management, propaganda, advertising - Lecture Notes
10. Information conflict vs copyright, privacy, spam, espionage, surveillance, hacking and cyberwar, viruses/worms, and identity theft - Lecture Notes
11. Basic concepts and risks in computer security and encryption - Lecture Notes
12. Problems arising in law enforcement and organisational security due to the proliferation of information conflict techniques - Lecture Notes

What is Information Conflict?

- Information Conflict is a more generalised term used to describe what most of the literature calls ‘Information Warfare’, ‘InfoWar’ or ‘IW’.
- Contrary to the common misconception, IW is more than the study of hackers, info-terrorists, applied cryptography, espionage and electromagnetic weapons.
- IW in the broadest sense is the study of how information is exploited or protected in survival contests.
- The ‘exploitation’ aspect is centred on how the use or manipulation of information can be utilised to an advantage.
- The ‘protection’ aspect is centred on how to prevent an opponent from using or manipulating information to an advantage.

Definition – Social Context

- **United States Department of Defense**: *'Information Warfare is any action to Deny, Exploit, Corrupt or Destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions'.*
- This definition describes Information Warfare in terms of 'actions' executed to achieve a sought outcome - denial, exploitation, corruption and destruction of an opponent's 'information' and related functions, and prevention of such 'actions' executed by an opponent.
- This is the most widely used formal definition of what IW is and what it most fundamental aspects are.
- The definition is incomplete and it limitations will be discussed further.

Definition – Scientific Context

- **Kopp and Mills (2002):** *Information Warfare is an evolved survival aid in the biological domain …*
- The argument by evolutionary theorists is that features in a species which improve its probability of individual survival and reproduction will be propagated, at the expense of features which impair individual survival and reproduction. Hypothesis demonstrated by showing:

1. *The species employs one or more than one of the four canonical IW strategies to aid in its survival.*
2. *Multiple species which are not closely related, and preferably exist in diverse environments, employ the same subset of the four canonical strategies to aid in their survival.*
3. *Closely related species exist to the examples found, which do not employ any of the four canonical strategies to aid in their survival*.

Shannon's Information Theory Concepts

- What is ‘information’?
- Information vs data?
- The role of the observer?
- Shannon’s channel capacity theorem
- Shannon’s concept of entropy
- How Shannon applies to real world problems
- Examples

Basic Game Theory Concepts

- What is game theory?
- What is a player?
- Von Neumann and evolution of game theory
- Berne’s psychological game concept
- Metagames – hypergames
- Higher order hypergames
- Ordinal vs cardinal games
- Examples - Prisoner’s dilemma game, iterated PD game, multiplayer PD games
- Examples - The ‘Chicken’ game

Four Canonical Strategies of IW

- Why a fundamental theory?
- Defining the four strategies:
  1. **Denial of Information / Degradation or Destruction**
  2. **Deception and Mimicry / Corruption**
  3. **Disruption and Destruction / Denial [1]**
  4. **Subversion / Denial [2]**
- Shannon vs the four canonical strategies
- Orthogonality properties of the canonical strategies
- Examples of the four canonical strategies

Compound Information Conflict Strategies

- What is a simple strategy?
- What is a compound strategy?
- Graphs vs compound strategies
- State based modelling
- Issues in modelling compound strategies
- Is a strategy being played?
- Examples of compound strategies
- Tutorial – Fortitude deception model

Hypergames vs Information Conflict Strategies

- Hypergames in detail
- Hypergames involving information
- Hypergames and the four canonical strategies
- Analysis of hypergame models for each strategy.
- Examples and case studies

Evolutionary Nature of Information Conflict

- Ideas and concepts in the theory of evolution
- The evolutionary hypothesis for IW in nature
- Examples of each of the strategies as used in nature
- The fallacy of counterarguments
- Information conflict as a natural phenomenon vs a social phenomenon
- Perceptions of information conflict vs the hard facts

Analysis and Modelling of IW

- Models of information conflict
- Applying models to the real world
- Problem issues arising in modelling
- Validating models vs empirical data
- Risks arising in modelling problems

Taxonomy of Information Conflict

- Why a taxonomy?
- Class I information warfare;
- Class II information warfare;
- Class III information warfare;
- Class IV information warfare;
- Denial of service attack classification
- Legal, cultural and political boundaries

Impact of Information Conflict

- Copyright
- Privacy
- Spam
- Espionage
- Surveillance
- Perception management, propaganda, advertising
- Hacking and cyberwar
- Viruses/worms
- Identity theft

Information Conflict vs IT Security/Encryption

- Basic concepts in computer security
- Basic ideas in cryptography
- The context of cryptography and security
- Encryption vs the canonical strategies
- Security vs the canonical strategies

Law Enforcement and Organisational Security

- Law Enforcement vs Organisational Security
- When is IW a criminal offence and when not?
- Problem issues in Law Enforcement
  1. **Identifying attackers**
  2. **Forensics and evidence**
  3. **Legal issues in prosecution**
- Problems in Organisational Security
- Protection of data and secrecy
- Protection of privacy

Reference Sources and Bibliography

- NOTE: There are a limited number of publications available in this area.
- Dorothy E. Denning, Information Warfare and Security, ACM Press (Addison-Wesley), 1999, ISBN 0-201-43303-6.
- Winn Schwartau, Information Warfare: Cyberterrorism : Protecting Your Personal Security in the Electronic Age, New York, NY: Thunder's Mouth Press, 1995, Second Edition.
- Carlo Kopp's publications at http://www.ausairpower.net/iw.html
- In addition, selected research papers will be referenced and discussed throughout the topic.