Cyber Security Defense:

From Moving Target Defense to Cyber Deception

Jie Wu

Temple University

Frontiers in Cyber Security, 2019

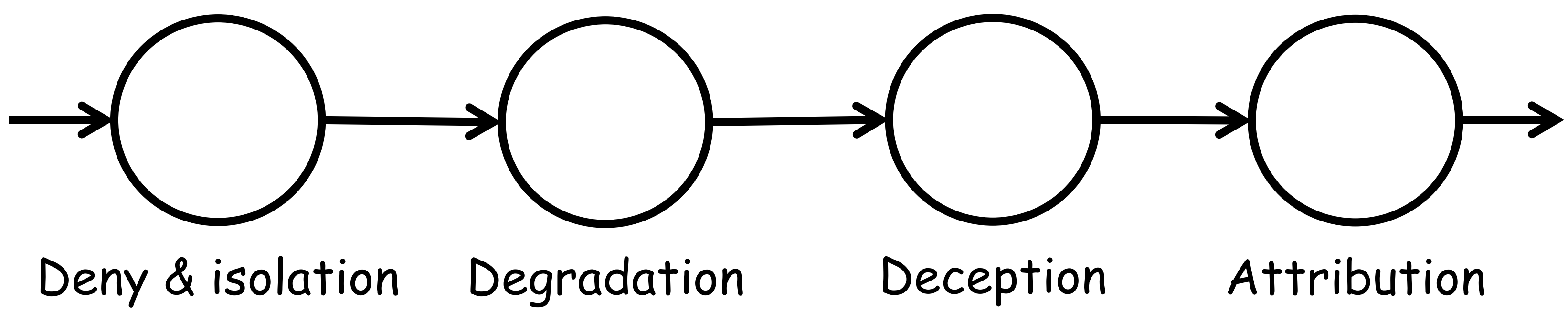
Outline

1. Cyber Security Defense
2. Cyber Deception
3. Honeypots and Honey-X
4. Moving Target Defense
5. Game-Theoretic Approaches
6. Challenges of Cyber Deception
7. Conclusions

1. Cyber Security Defense

- Security: a collection of protection mechanisms
  - Deny and isolation: deny unauthorized access
  - Degradation and obfuscation: slow down once penetrated
  - Negative info and deception: lead attackers stray
  - Attributions and counter-operation: hiking back

Cyber kill-chain

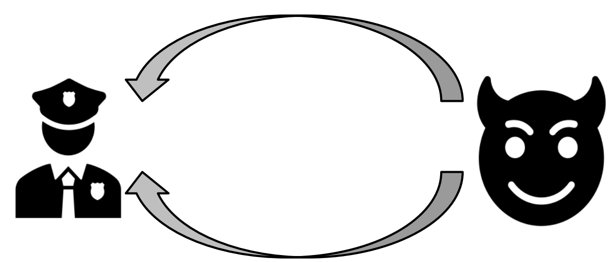


2. Cyber Deception

- The Art of War (孙子兵法)
  - All warfare is based on deception
- Offense vs. Defense
  - Attack is the secret of defense
  - Defense is the planning of an attack

2. Cyber Deception

- Cyber deception
  - Planned actions to mislead/confuse (i.e. trap) attackers
- Goals
  - Complement detection, enhance prevention, and mitigate successful attacks
- Unit and layer
  - Parameter, file, account, profile, …
  - Network, system, application, data, …
- Life cycle of cyber deception
  - Collect knowledge of attacker
  - Implement deception schemes



Adversary Model

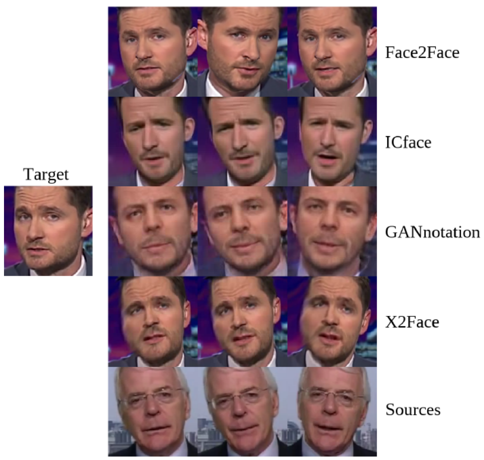
Kerckhoffs' principle: system is public knowledge

- It is unclear how smart an adversary can be
- Traffic analysis challenge: algorithm + big data
  - An adversary can use a sophisticated ML method
  - An adversary can use compressive traffic analysis (CCS 2017)

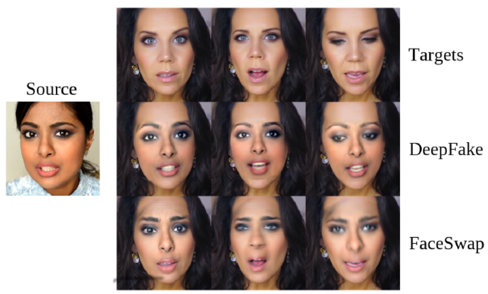
    Perform traffic analysis on compressed features instead of raw data

Deepfake

- Defend against facial forgery

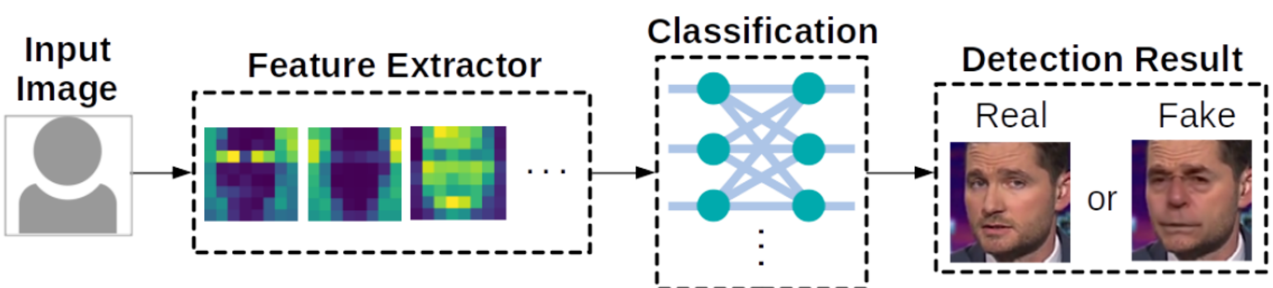


Face reenactment



Face swapping

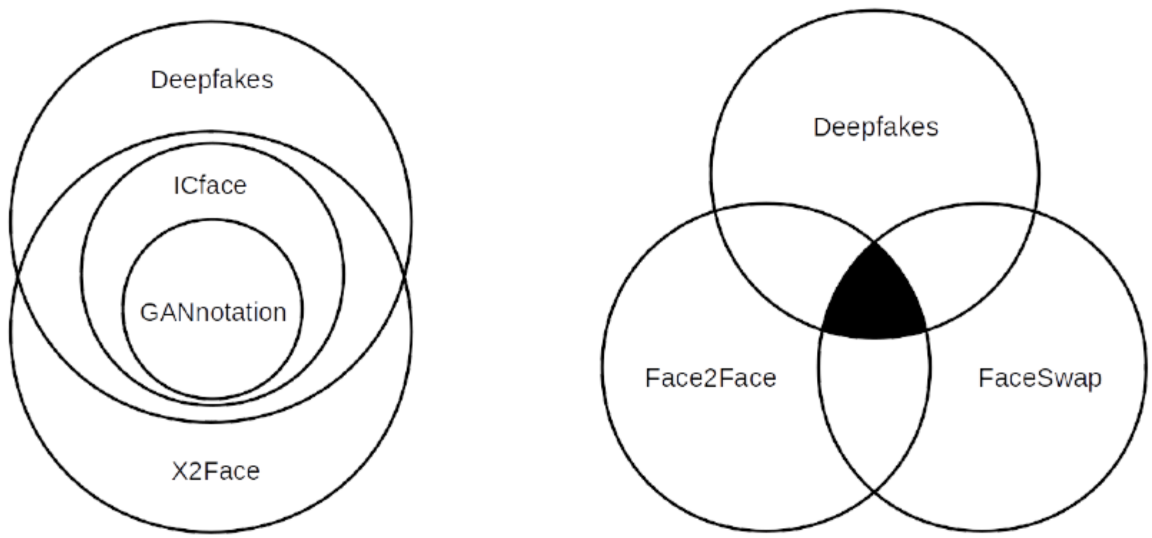
Face2Face, CVPR 2016



Architecture of deepfake defense systems

Deepfake Detection

- Limitation of current defense systems
  - Cannot defend against unseen attack methods
  - Features of different attack methods can be independent

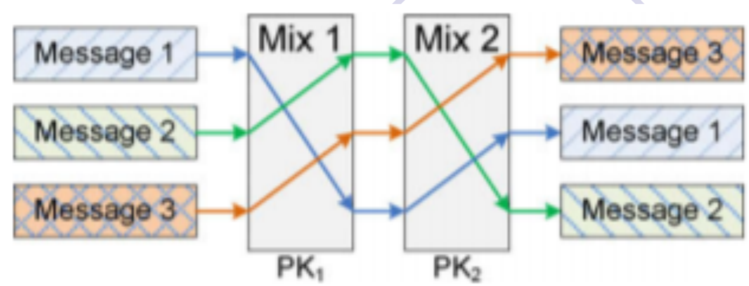


Feature overlap among existing facial forgery techniques [1] (tested on MesoNet)

[1] J. Brockschmidt et al., "On the Generality of Facial Forgery Detection", Proc of REUNS 2019 (Best Paper)

Different Types of Deception

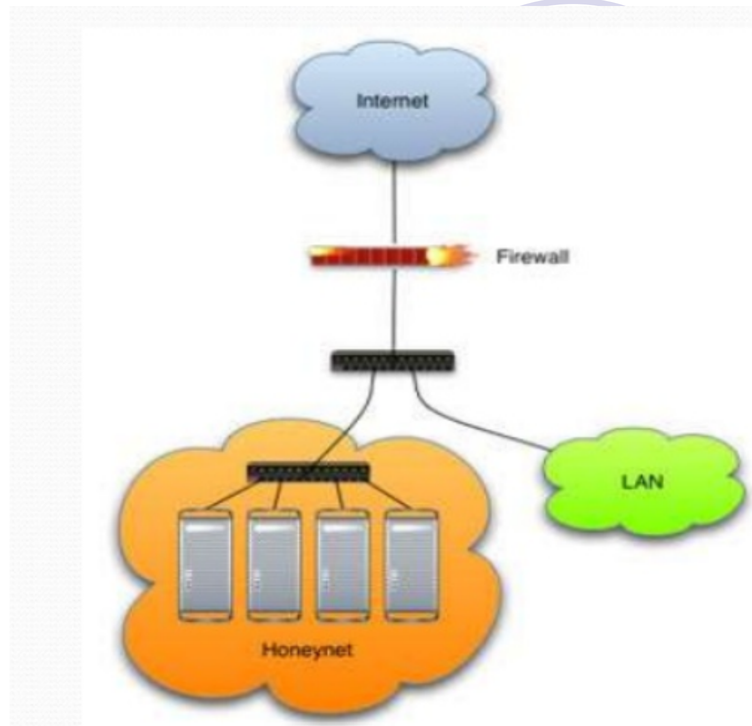
- Perturbation
  - Perturb sensitive data with noises
- Obfuscation
  - Decoy targets and/or reveal useless info
- Mixing
  - Prevent linkability (mixing zone)
- Honey-X
  - Disguise honeypots as real systems
- Moving target defense
  - Change attack surfaces



3. Honeypots and Honey-X

- Honeypots
  - Bears: honey eaters
  - Traps

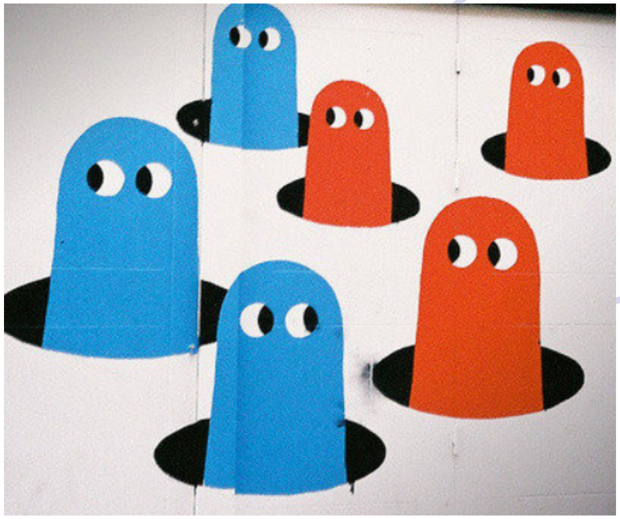
- Honey-X
  - Honeynet: two ore more honeypots on a network
  - Honeyfile, honeyword, …



4. Moving Target Defense (MTD)

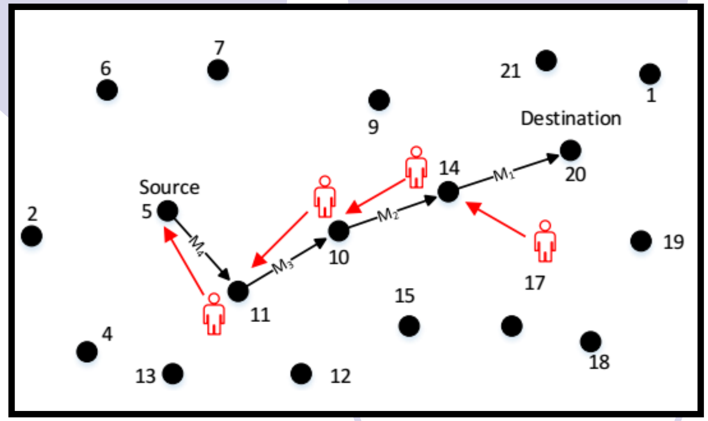
- MTD
  - Controlling change across multiple system dimensions to increase uncertainty and complexity for attackers

- Network: Route change
- Firewall: Policy change
- Host: Address change
- OS: Version/release change

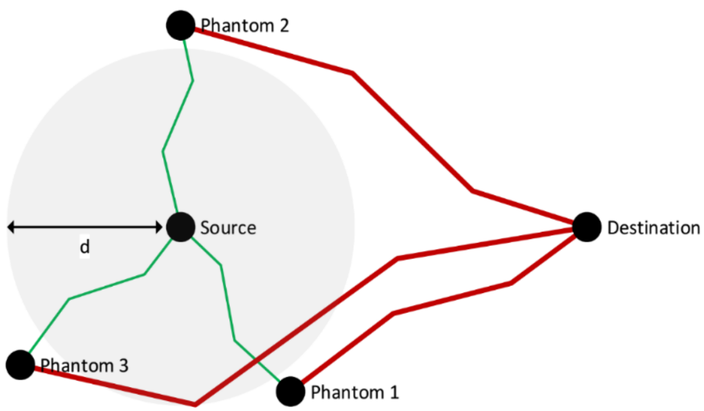


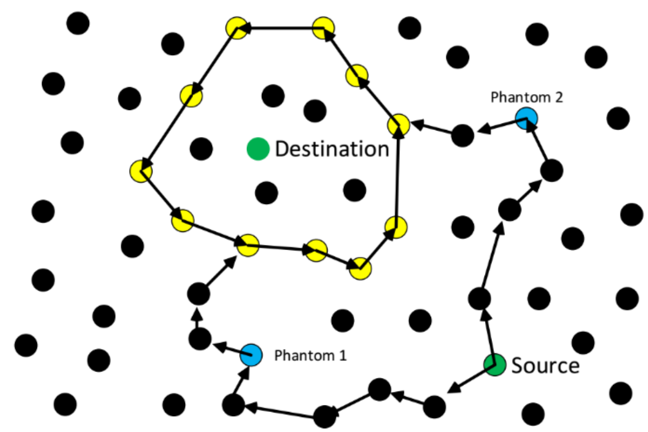
MTD vs. Deception: Intractability

- Source and destination location privacy (Panda-hunter game)



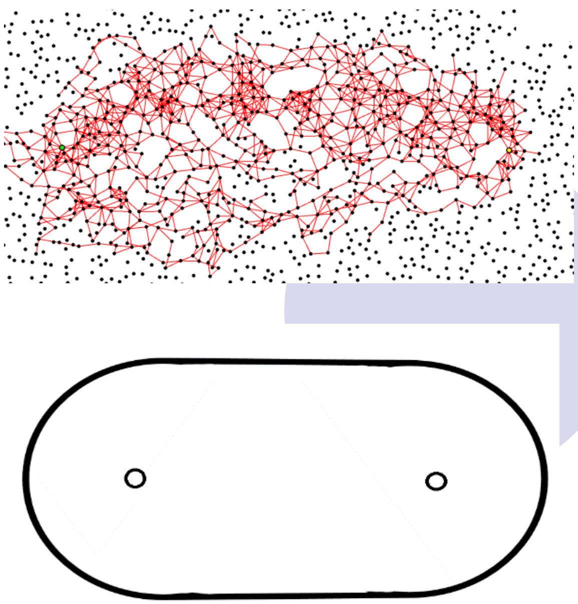
- Phantom/Circular Ring Routing



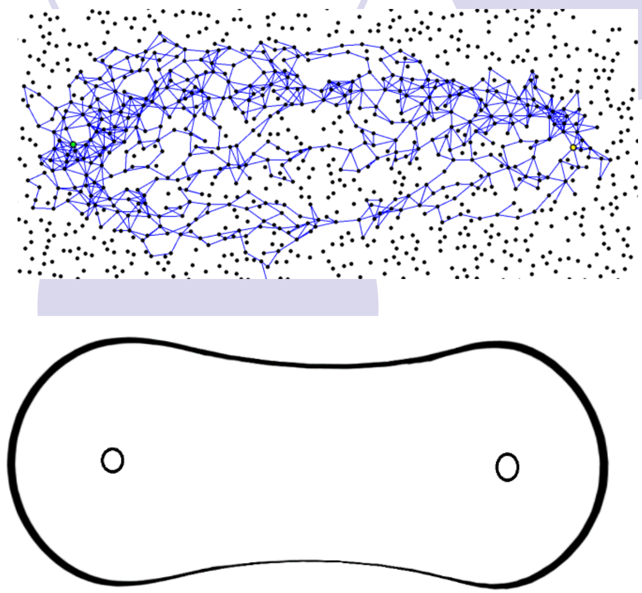


Probabilistic/Controlled Random

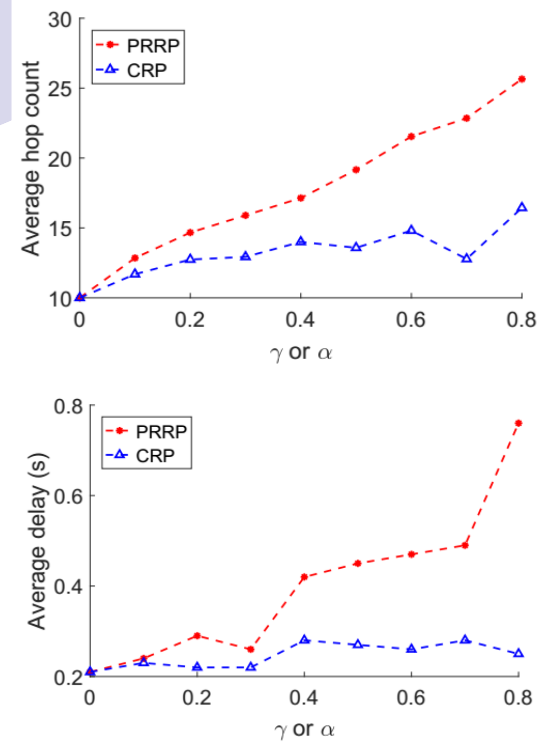
- Performance gain [2]



Probabilistic Random Routing (PRRP)



Controlled Random Routing (CRP)

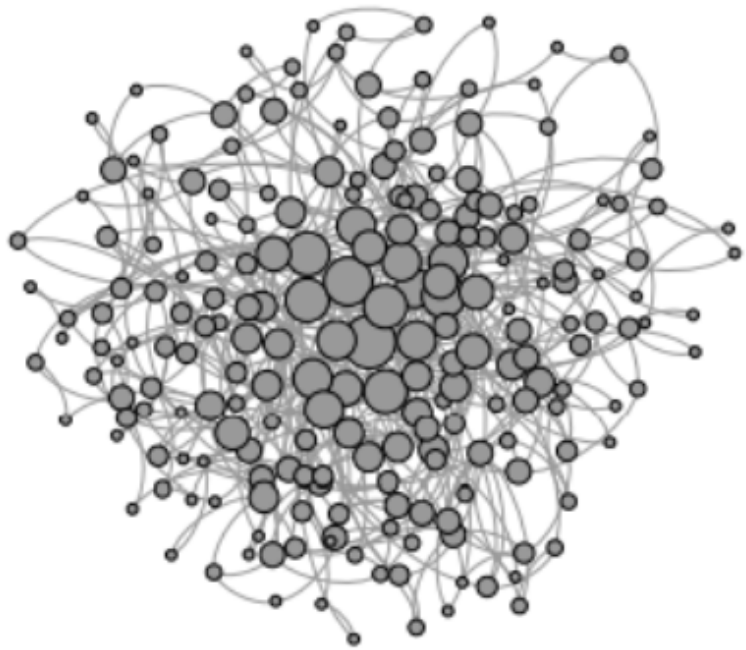


NS3 Simulation

[2] R. Biswas and J. Wu, "Preserving Source and Destination Location Privacy with Controlled Routing Protocol," *IJSN*, 2018

Adaptive Changes

- Hierarchical military command chains
- Network hierarchy
  - SDN controllers: load balance and fault tolerance



Self-Organized Systems

Theory community

- Dijkstra's self-stabilizing system (Dijkstra, 1974)
  - An illegitimate state (caused by some *perturbations*) can be changed back to a legitimate state in a finite number of steps
- *How can we handle the long convergence time that usually occurs in dynamic labeling in a distributed solution?* (ICDCS 2017 [2])

[2] J. Wu, "Uncovering the Useful Structures of Complex Networks in Socially-Rich and Dynamic Environments" *Proc. of IEEE ICDCS*, 2017.

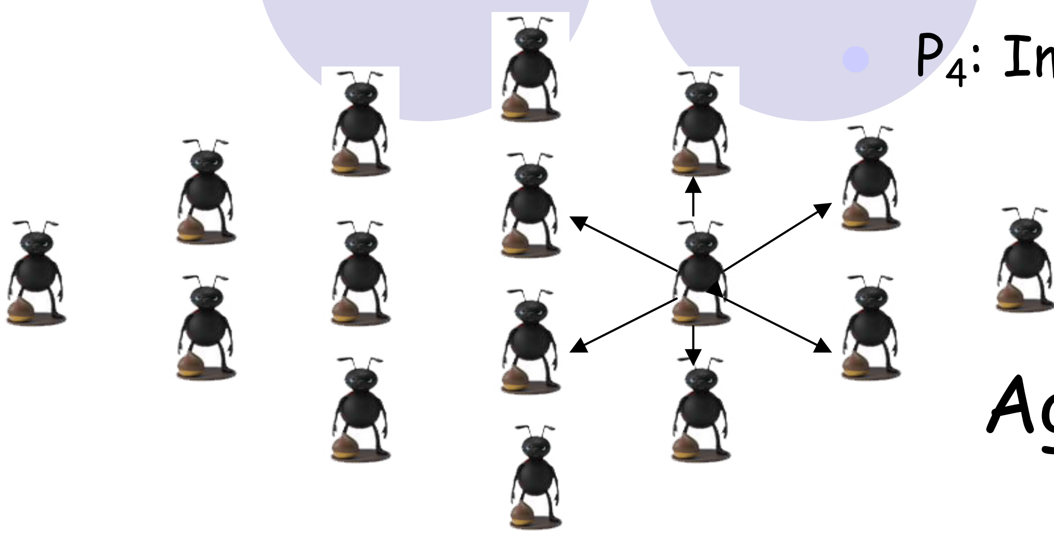
Self-Organizing Solutions

Local decision

- P2P and simple interaction (mostly local and without sequential propagation)

Global functionality

- Adaptive, robust, and scalable

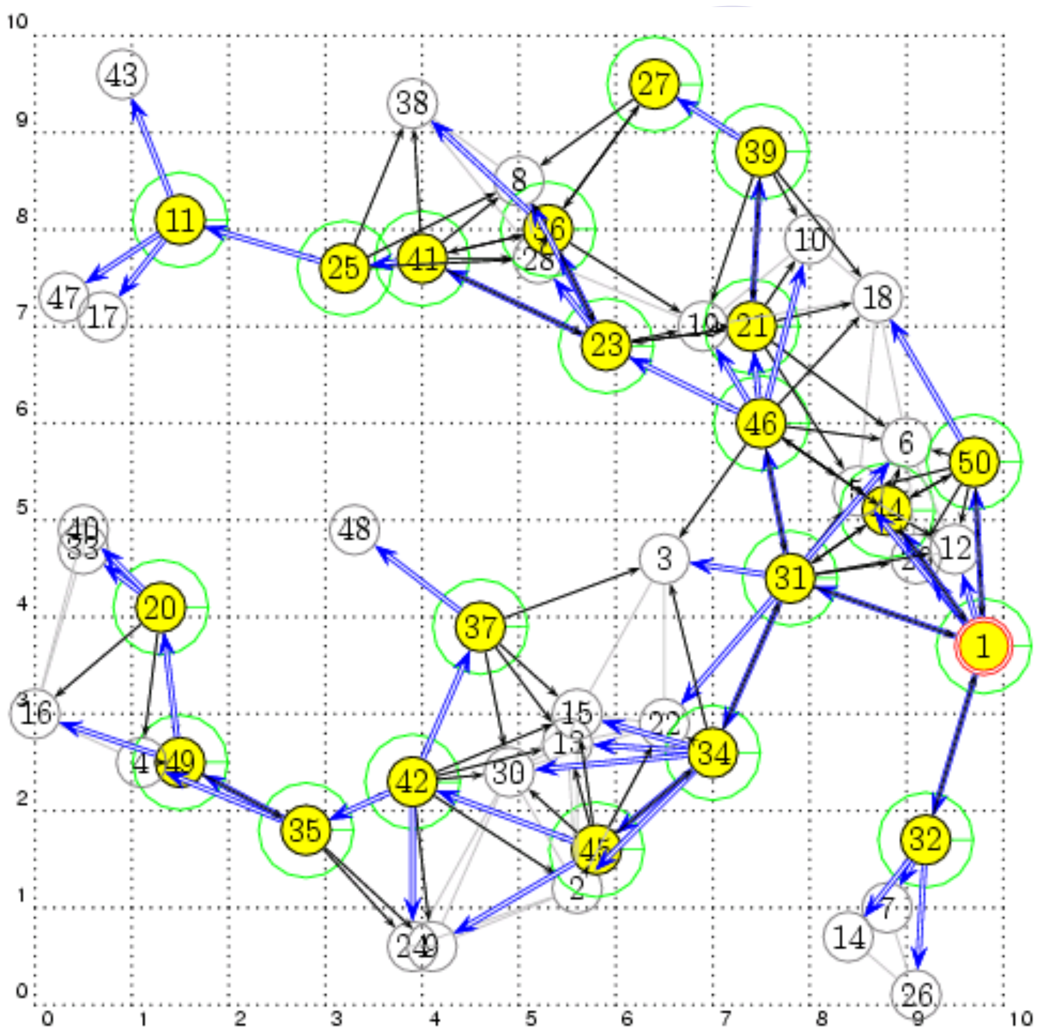


Principles

- P_1: Local interactions with global properties (scalability)
- P_2: Minimization of maintained state (usability)
- P_3: Adaptive to changes (self-healing)
- P_4: Implicit coordination (efficiency)

Agility

MTD Applications



Connected Dominating Set (CDS)

Local decision:

backbone nodes

based on node priority (ID, degree, …)

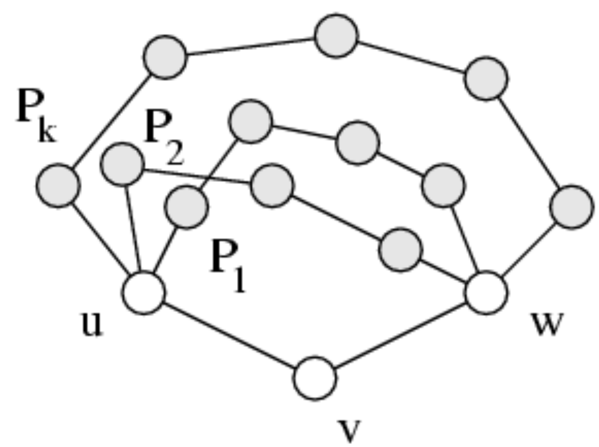
Global properties:

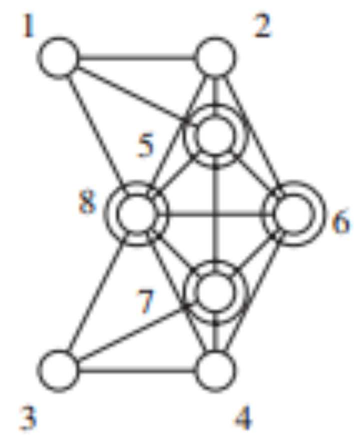
Connectivity

Coverage

Application: Resiliency and Rotation

- Redundancy: *K-connected & K-dominated* [4]
  - Non-backbone node: K node-disjointed paths for any neighbor pairs (for multiple CDS)



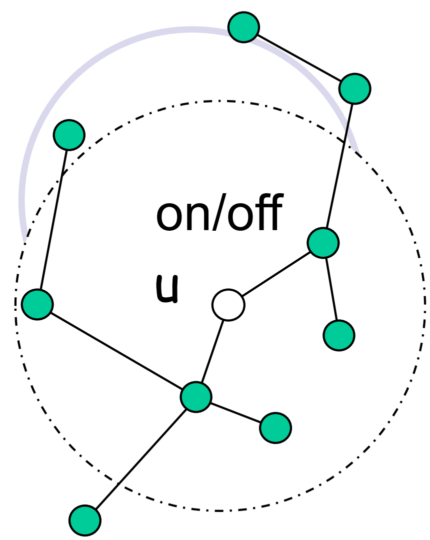


  - Moving target defense (MTD): CDS rotation

[4] F. Dai and J. Wu "On Constructing k-Connected k-Dominating Set in Wireless Networks," *Proc. Of IEEE IPDPS*, 2005

Self-Healing

- *How can we deal with the complexity of building a structure along with a change of topology?* (ICDCS 2017)
- Switched-on/off nodes
  - Status changes in 1-hop/2-hop neighbors only
- Seamless integration in a dynamic network
  - Iterative application of a local solution



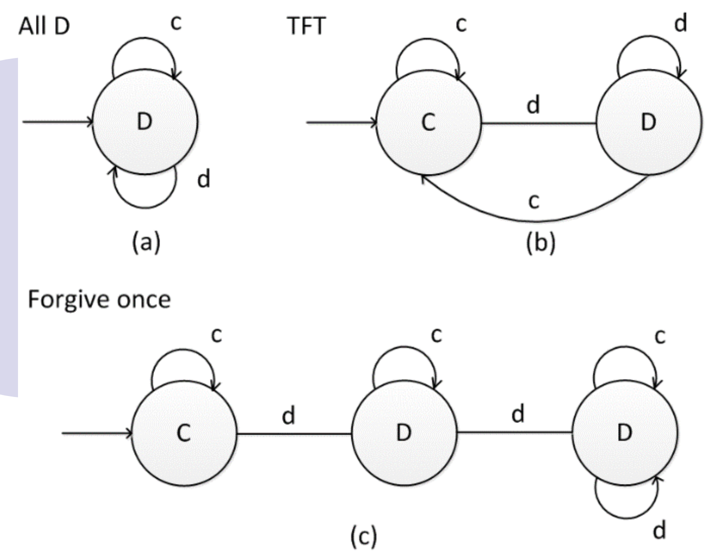
5. Game-Theoretic Approaches

- Nash game
  - Static games and simultaneous move
  - Each player chooses a move which is optimal, given the other player's move
- Stackelberg game
  - Single-shot dynamic game
  - The follower (attacker) moves after observing the leader's (defender) action
- Messaging game
  - Single-shot dynamic game
  - The sender (defender) sends a message (action) to the receiver (attacker). Message may not be the sender's type.

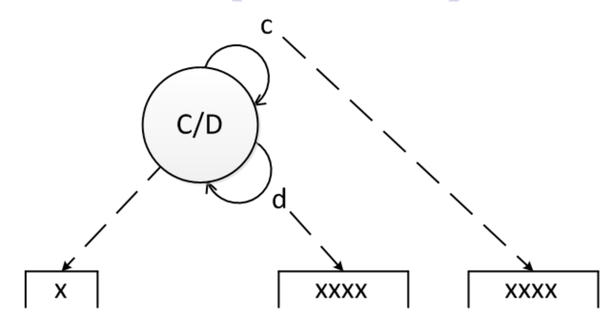
Repeated Nash Game

- Repeated prisoner's dilemma
  - Cooperate (C) or Defecting (D)
  - Payoff metrics between 1 and 2

$$\begin{array}{ccc} & C_2 & D_2 \\ \begin{array}{c} C_1 \\ D_1 \end{array} & \multicolumn{2}{c}{\begin{pmatrix} 3,3 & 0,5 \\ 5,0 & 1,1 \end{pmatrix}} \end{array}$$



- Genetic algorithm (ADS 14)
  - 148 bits for 16 recent states: 9-bit chromosomes
  - Mutation and crossover
- From Moore machine to timed automata
  - Adversary's learning through timing analysis
  - Fitness levels with imperfect information



6. Challenges of Cyber Deception

- Limited Applications
  - Projected market to be $1B by 2020
- Isolation
  - Fully integrated or separated
- Effectiveness
  - How to measure?
- Learning
  - Ability of both attackers & users

Limited Applications

- Still limited in cyber deception, why?
  - Differences: cyber deception vs. deceptions in warfare
    - Domain: cyber vs. physical, social, …
    - Time: different scales, logical clock vs. physical clock (i.e., real time)
    - Space: virtual space vs. physical space
    - Speed: speed of light vs. physical space laws (e.g., movement of a tank)
  - Do not understand the attackers well: known vs. unknown
    - Know your enemies and know yourself
  - How to attract attackers to interact with them in cyberspace?
    - It is relatively easy to engage your enemies in a battle field

Isolation

- Isolation
  - Fake information only for attackers (assuming legitimate users won't visit)
  - Protection layer: detect suspicious users and lead them to fake information

- Feedback to attackers
  - Feedback should be carefully designed in order to prevent the attacker from detecting the deception
    - Increase the level of deception using return partial valuable data
    - Stop deception to avoid exposure of deception schemes

Effectiveness

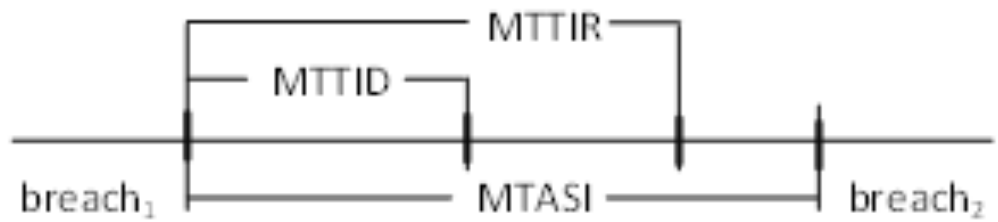
- Key
  - Learn the behavior of the attacker: learning theory
- Effectiveness measurement for attackers
  - Rate frustration in time and cost
- Effectiveness measurement for systems: dependability
  - Time and place of attacker's action
  - How much attacker's resources are wasted (e.g. num. of packets)
  - How long before attacker breaks the system/ stop acting
  - How much valuable data are breached
  - And more…

Measurement

Lord Kelvin: If you cannot measure it, then we cannot improve it

Extended dependability that includes security

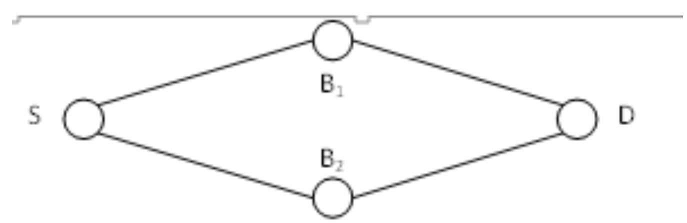
- Mean time between security incidents (MTBSI)
- Mean time to incident discovery (MTTID)
- Mean time to incident recovery (MTTIR)



Performability: work completed before the next security breach

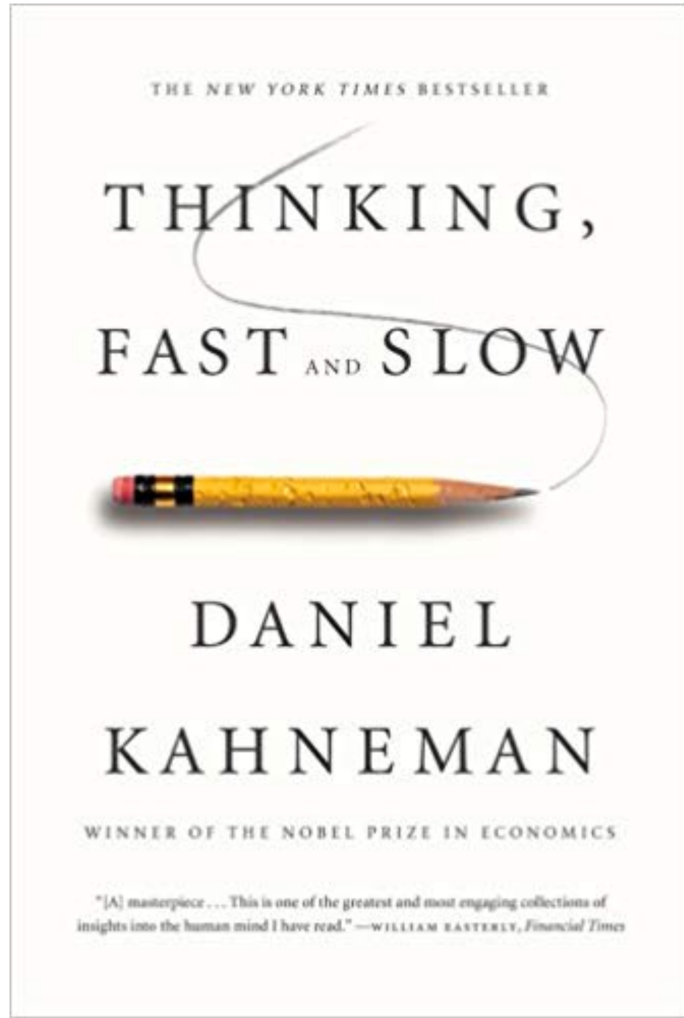
Degradation

- B_1: Level 1 breach, 1,000 hrs
- B_2: Level 4 breach, 5 hrs



Learning: Cognitive Biases

- Deception is strongly relied on human psychology
  - Cognitive biases
- Cultural biases
  - Power Distance Index (PDI)
  - Uncertainty Avoidance (UAI)



Final Thoughts

- Cyber-deception: friend or foe?
- Misinformation vs. disinformation
  - Disinformation is information that is deliberately false or misleading
  - Recent events in HK, Lebanon, Chile, Spain, …
- Challenges
  - Identifying disinformation is not merely about the truth, but about referring the intent (to mislead)

7. Conclusions

- Importance of cyber deception
  - Complement to the existing security methods
- Self-organized design for agility
  - Basic principles and challenges
- Future
  - A better learning model for attackers/users
    - Security vs. ML
  - Science of security (S & P 2017)
    - Induction and deduction

Questions