17. Cyber-Physical Security of Network Systems

金力 Li Jin
li.jin@sjtu.edu.cn
上海交通大学密西根学院
Shanghai Jiao Tong University UM Joint Institute

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Outline

- Background
- Static & sequential games in cyber-physical security
- Dynamic games in cyber-physical security*

Background

- By courtesy of Prof. S. Amin's slides

Network systems

- Transportation
- Water
- Gas
- Power

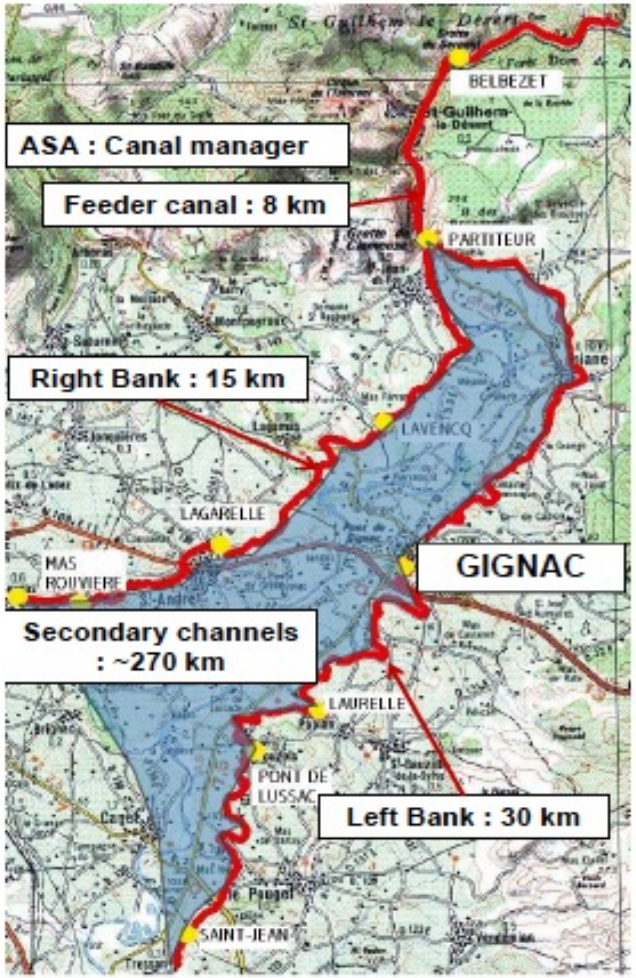
Gignac SCADA system: a 2009 story

SCADA components

- Level & velocity sensors
- PLCs & gate actuators
- Wireless communication

Gignac Le canal victime d'actes de vandalisme à répétition

Depuis le 21 juin, le canal de Gignac est victime d'actes malveillants sur l'ouvrage de l'aqueduc de l'Aurelle (derrière le lagunage de Popian) : effondrement du radier du canal puis dégradation des réparations mises en place (retrait des boulots de serrage, mettant gravement en péril la pérennité de l'aqueduc).
L'ouvrage de l'Aurelle permet la continuité du transport de l'eau vers les parcelles du périmètre irrigué situé sur les communes de Pouzols, Le Pouget, Tressan et Puilacher, soit près de 900 ha, pour lesquels l'apport d'eau estival est essentiel.
Ces agissements ont fait l'objet de constats par les brigades de gendarmerie et de plaintes contre X. Il est à noter que l'intégralité du patrimoine de l'Association syndicale autorisée du canal de Gignac est un ouvrage public, dont la destruction, la dégradation ou la détérioration peuvent faire l'objet de poursuites et être punies de trois ans d'emprisonnement et de 45 000 € d'amende.

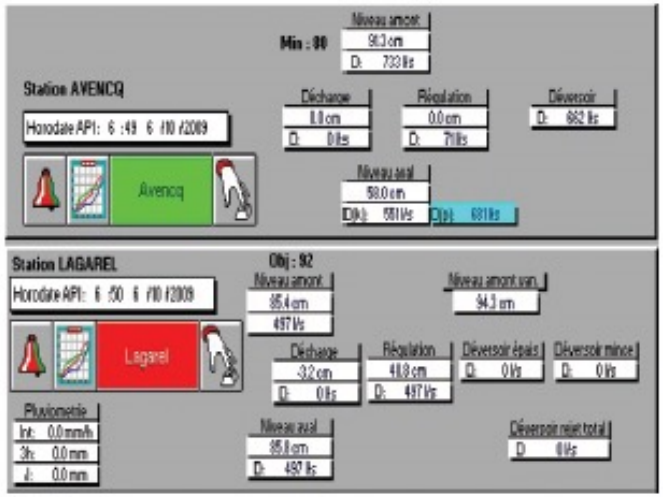


Nominal control objective

Control objective

- Manipulate gate opening
- Control upstream water level
- Reject disturbances (offtake withdrawals)

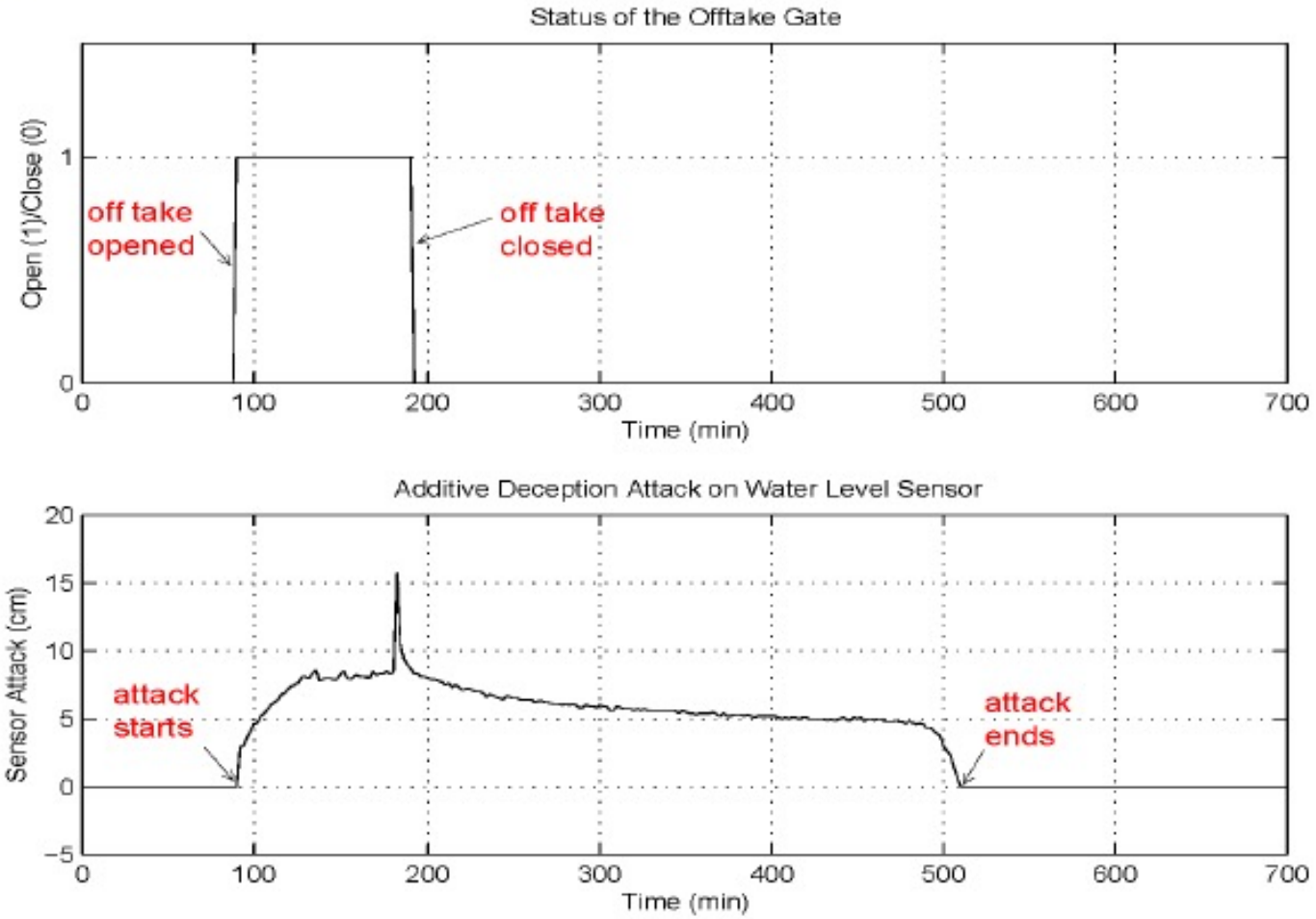
SCADA interface



Avencq cross-regulator

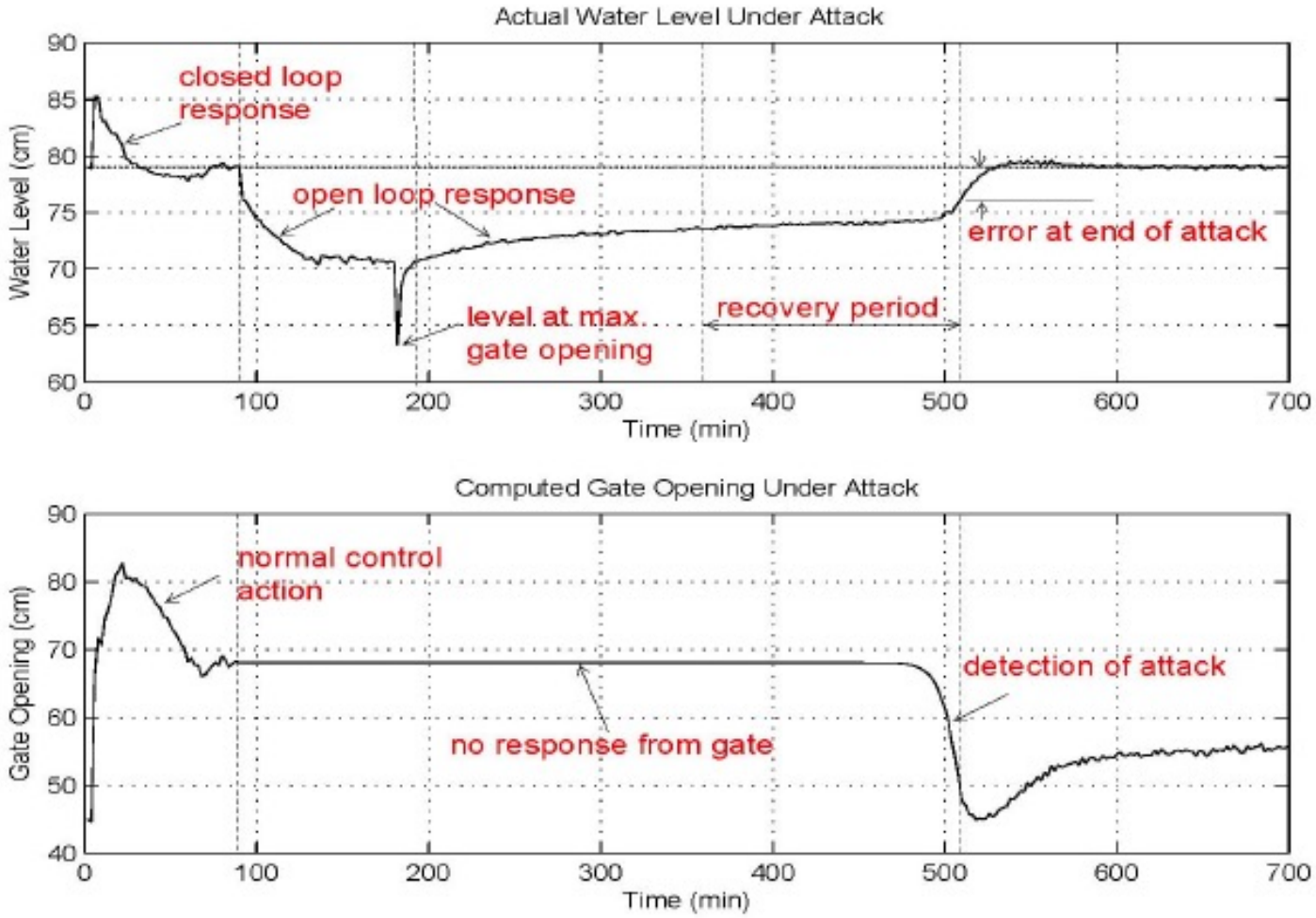
Real test attack

Field operational test (October 12th, 2009)



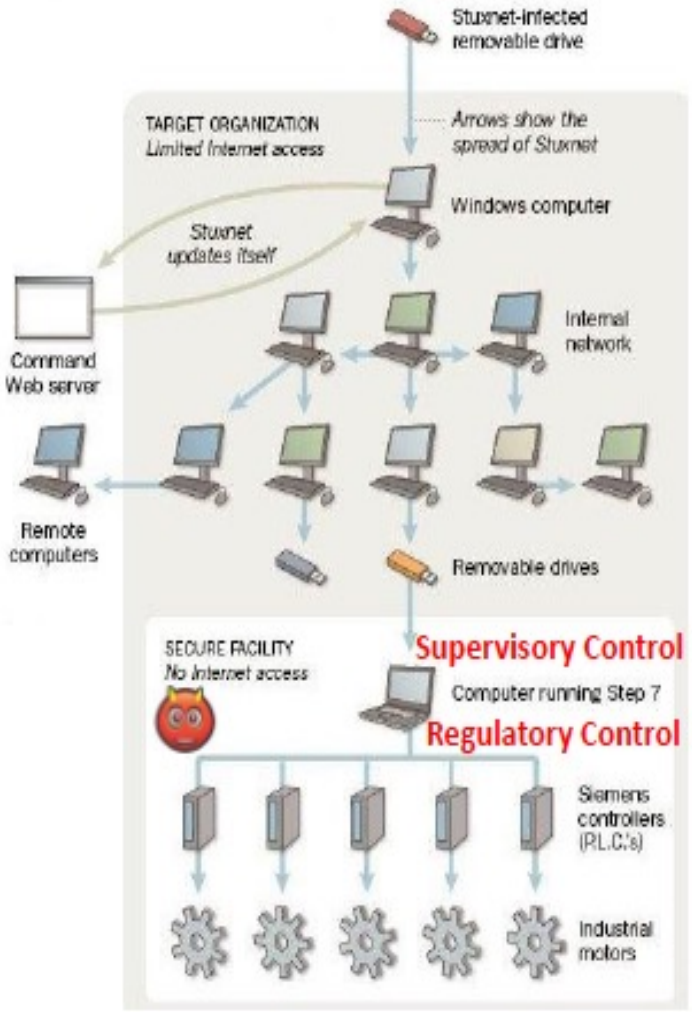
Real test attack

Successful attack



Stuxnet: 2010 - onwards

- Targets supervisory control and data acquisition (SCADA) systems
- 4 zero-day (i.e. vulnerabilities unknown to those who should be interested in its mitigation) exploits
- Antivirus evasion, p-2-p updates
- Reprograms programmable logic controllers (PLC) code
- Deeply involved in world politics...



Source: Symantec, NYT

Real Threats!

In December 2012, the US Department of Homeland Security released a map of approximately 7,200 control system devices that appear to be directly linked to the Internet and are vulnerable to attack.

Intelligent Transportation Systems

Security failures: fake information

- Technion students hacked the Waze GPS app
  - Create fake traffic jams
  - Drivers diverted incorrectly
  - Cause congestion elsewhere
- Problems:
  - No cross-validation of information
  - Traffic managers have no clue about miscommunication by Waze

Security failures: spoofed sensors

- IOActive researchers intruded into traffic sensing system:
  - Spoofed measurements
  - Could induce suboptimal or unsafe decisions by controllers
- Cyber-physical components:
  - Numerous COTS IT components
  - Limited business case for security investments

Another real incident

Los Angeles Times LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH STYLE

L.A. NOW
Southern California -- this just in

« Previous Post | L.A. NOW Home | Next Post »

Engineers who hacked into L.A. traffic signal computer, jamming streets, sentenced

December 1, 2009 | 7:17 am

Two L.A. traffic engineers who pleaded guilty to hacking into the city's signal system and slowing traffic at key intersections as part of a labor protest have been sentenced to two years' probation.

Why game theory

- Since security can always be viewed as a conflict between two opposing objectives, it is quite natural to cast it as a multi-agent decision problem in which the defenders (e.g., system authorities) aim to protect the system against potential attackers.
- However, what makes the analysis of security systems challenging is the fact that most of the recent attacks are highly organized and strategic.
- In other words, the attackers are quite cautious about the potential consequences of their adversarial actions and hence take strategic actions to hide their identities.
- In this regard, game theory, a powerful tool for analyzing strategic multi-agent decision systems, proves quite useful to capture the interactions between security players.

Why game theory?

Multiple decision makers + conflicting objectives

= game theory

Static & sequential games in cyber-physical security

- Wu, M., & Amin, S. (2019). Securing infrastructure facilities: When does proactive defense help? *Dynamic Games and Applications*, *9*(4), 984-1025.

Motivation

- Infrastructure systems are increasingly facing new security threats due to the vulnerabilities of cyber-physical components that support their operation.
- We investigate how the infrastructure operator (defender) should prioritize the investment in securing a set of facilities in order to reduce the impact of a strategic adversary (attacker) who can target a facility to increase the overall usage cost of the system.
- We adopt a game-theoretic approach to model the defender-attacker interaction and study two models:
  1. Normal form game: both players move simultaneously
  2. Sequential game: attacker moves after observing the defender's strategy.

Main challenge of this section

High school math + PhD notations...

Infrastructure facilities

Consider an infrastructure system modeled as a set of components (facilities) E.

Infrastructure facilities

- To defend the system against an external malicious attack, the system operator (defender) can secure one or more facilities in E by investing in appropriate security technology.
- The set of facilities in question can include cyber or physical elements that are crucial to the functioning of the system.
- These facilities are potential targets for a malicious adversary whose goal is to compromise the overall functionality of the system by gaining unauthorized access to certain cyber-physical elements.
- The security technology can be a combination of proactive mechanisms (authentication and access control) or reactive ones (attack detection and response).

Player models

Defender:

- A pure strategy for the defender $s_d \in E$
- Takes values from $S_d = 2^E$ (power set, i.e. set of all subsets of E)
- The cost of securing any facility is $p_d > 0$
- Total defense cost incurred in choosing a pure strategy s_d is $p_d|s_d|$, where $|s_d|$ is the cardinality of s_d (i.e. the # of secured facilities)

Attacker:

- Can either attack a single facility $e \in E$ or launch no attack
- Pure strategy $s_a \in S_a = E \cup \{\emptyset\}$
- Attacking cost $p_a > 0$

Impact of attack

- We assume that prior to the attack, the usage cost of the system is $C_{\emptyset}$.
- This cost represents the level of efficiency with which the defender is able to operate the system for its users.
- A higher usage cost reflects lower efficiency.
- If a facility e is targeted by the attacker but not secured by the defender, we consider that e is compromised and the usage cost of the system changes to $C_e > C_{\emptyset}$.
- Therefore, given any pure strategy profile (s_d, s_a), the usage cost after the attacker–defender interaction, denoted $C(s_d, s_a)$, can be expressed as follows:

$$C(s_d, s_a) = \begin{cases} C_e & \text{if } s_a = e, \text{ and } s_d \neq e, \\ C_{\emptyset} & \text{otherwise.} \end{cases}$$

Normal form game

- Mixed strategy
  - **Defender**: $\sigma_d = \left(\sigma_d(s_d)\right)_{s_d \in S_d} \in \Delta(S_d)$ = probability that the set of secured facilities is s_d
  - **Attacker**:$\sigma_a = \left(\sigma_a(s_a)\right)_{s_a \in S_a} \in \Delta(S_a)$ = probability that the attacker targets at facility $e = s_a$
  - Mixed strategy profile $\sigma = (\sigma_d, \sigma_a)$
- Utilities for a pure strategy profile (s_d, s_a)
  - **Defender**: - usage cost – defense cost

$$u_d(s_d, s_a) = -C(s_d, s_a) - p_d|s_d|$$

  - **Attacker**: usage cost – attack cost

$$u_a(s_d, s_a) = C(s_d, s_a) - p_a \mathbb{I}\{s_a \neq \emptyset\}$$

Normal form game

- For a mixed strategy profile (σ_d, σ_a), expected utilities are

$$U_d(\sigma_d, \sigma_a) = \sum_{s_d \in S_d} \sum_{s_a \in S_a} u_d(s_d, s_a)\sigma_a(s_a)\sigma_d(s_d)$$

$$= -\mathrm{E}_\sigma[C] - p_d \mathrm{E}_{\sigma_d}[|s_d|]$$

$$U_a(\sigma_d, \sigma_a) = \sum_{s_d \in S_d} \sum_{s_a \in S_a} u_a(s_d, s_a)\sigma_a(s_a)\sigma_d(s_d)$$

$$= -\mathrm{E}_\sigma[C] - p_a \mathrm{E}_{\sigma_a}[|s_a|]$$

- Recall law of total expectation...

Equilibrium*

- An equilibrium outcome of the normal for game is defined in the sense of Nash equilibrium (NE).
- A strategy profile $\sigma^* = (\sigma_d^*, \sigma_a^*)$ is an NE if

$$U_d(\sigma_d^*, \sigma_a^*) \geq U_d(\sigma_d, \sigma_a^*), \qquad \forall \sigma_d \in \Delta(S_d)$$
$$U_a(\sigma_d^*, \sigma_a^*) \geq U_d(\sigma_d^*, \sigma_a), \qquad \forall \sigma_a \in \Delta(S_a)$$

- Questions to be asked:
  1. Does an NE exist?
  2. Is the NE unique?
  3. What are the parameter regimes for the equilibrium structure?
  4. How to compute the equilibrium?

Sequential game

- Strategies & utilities: analogous to normal form game
- Main difference:
  - In normal form game, both players move simultaneously
  - In sequential game, defender moves first, and attacker moves second.
- That is, attacker can observe and respond to defender's strategy

$$\sigma_a(\sigma_d) = \sigma(s_a, \sigma_d)_{s_a \in S_a}$$

- $\sigma_a(s_a, \sigma_d)$ = probability that realized action is s_a when defender's strategy is σ_d
- Strategy profile $\sigma = (\sigma_d, \sigma_a(\sigma_d))$

Sequential game*

- For the sequential game, the notion of equilibrium is no longer in the sense of Nash
- Instead, we consider the subgame perfect equilibrium (SPE)
- Also called Stackelberg equilibrium
- Definition:

$$U_d(\sigma_d^*, \sigma_a^*(\sigma_d^*)) \geq U_d(\sigma_d, \sigma_a^*(\sigma_d)),\ \forall \sigma_d \in \Delta(S_d)$$

$$U_a(\sigma_d, \sigma_a^*(\sigma_d)) \geq U_d\big(\sigma_d, \sigma_a(\sigma_d)\big),$$
$$\forall \sigma_a \in \Delta(S_a), \forall \sigma_a(\sigma_d) \in \Delta(S_a)$$

- SPE must exist if we consider mixed strategies.

Summary

- Defender can secure a subset of infrastructure facilities but cannot secure all of them due to budget constraint
- Attacker can compromise up to one facility but cannot compromise more than one due to budget constraint
- Consequently, both players have to select their targets strategically in order to maximize their respective utilities
- At equilibrium, no player can improve its utility by unilaterally vary its action
- In normal form game, neither player can observe the opponent's decision, while in sequential game, attacker can observe defender's action

Dynamic games in cyber-physical security*

- Etesami, S. R., & Başar, T. (2019). Dynamic games in cyber-physical security: An overview. *Dynamic Games and Applications*, *9*(4), 884-913.

Static vs. dynamic security games

- We have seen a static game theoretic formulation of cyber-physical security
- That is, everything is determined at one shot; no strategy evolution and no learning
- Although static game formulations provide good insights into the behavior of security players (and make quite a bit of sense in certain situations), in most cases they fail to capture the crucial dynamic characteristic of security problems
- Security players are repeatedly engaged in a multistage game in which the underlying environment can itself change dynamically over the course of interactions.
- This has motivated more realistic dynamic game formulations

Another motivation: incomplete information

- In fact, studying cyber-security problems using dynamic games becomes even more sophisticated once we account for the information structure.
- This is because in most security problems the defenders and attackers do not have complete information on each other's payoffs, nor are they aware of each others' identities.
- Furthermore, due to limitation of monitoring devices, it is possible that once an attack has occurred, it is not identified by the system.
- As a result, the players may only have partial information about each other's past or current strategies.

Typical dynamic security games

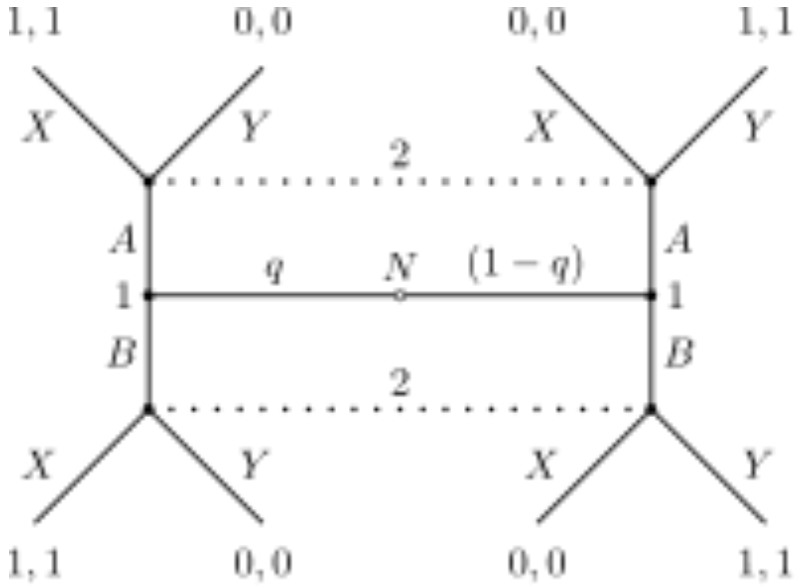
- Signaling games

Signaling games

- In its simplest form, a signaling game is a dynamic Bayesian game with two players (a sender and a receiver) in which the sender has several types which is private to him and determines his payoff function.
- The receiver, however, has only one type, and hence, his payoff is common knowledge to both players. The sender takes an action first by sending a message.
- The receiver observes the sender's message and then takes his action.
- The players then receive some payoffs depending on sender's type and their actions.

Signaling games

- As in many security problems, the defender (receiver) does not have knowledge about the attacker's (sender's) target list, it seems quite reasonable to model the interactions between the attacker and the defender in a security problem using a signaling game



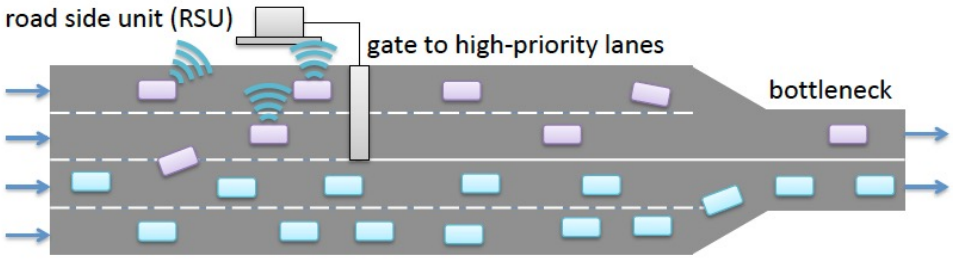
ETC example

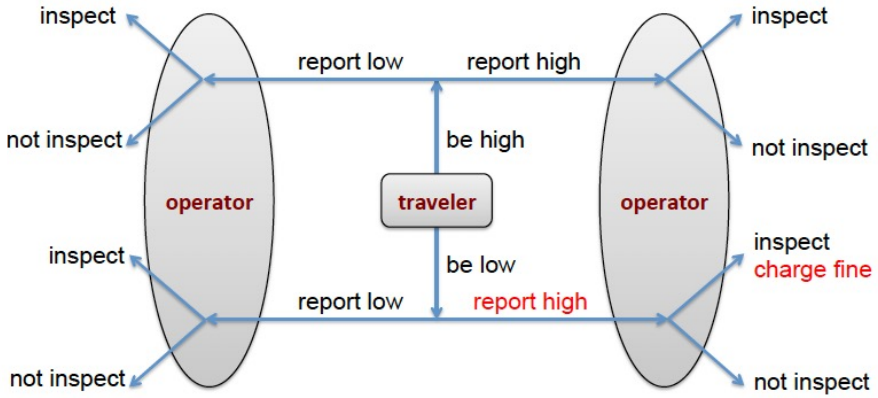
- Electronic toll collection (ETC)
- Security threat: travelers may modify onboard unit to cheat
- Questions:
  - How much incentive for misbehavior?
  - How to address such misbehavior?
- System operator can inspect strategically
  - Activate additional sensing capabilities
  - Costly (hardware, energy, labor…)
- Modeling approach:
  - Queuing model for impact evaluation
  - Game for misbehavior/inspection

(Joint work with Saurabh Amin & Patrick Jaillet @ MIT)

Signaling game

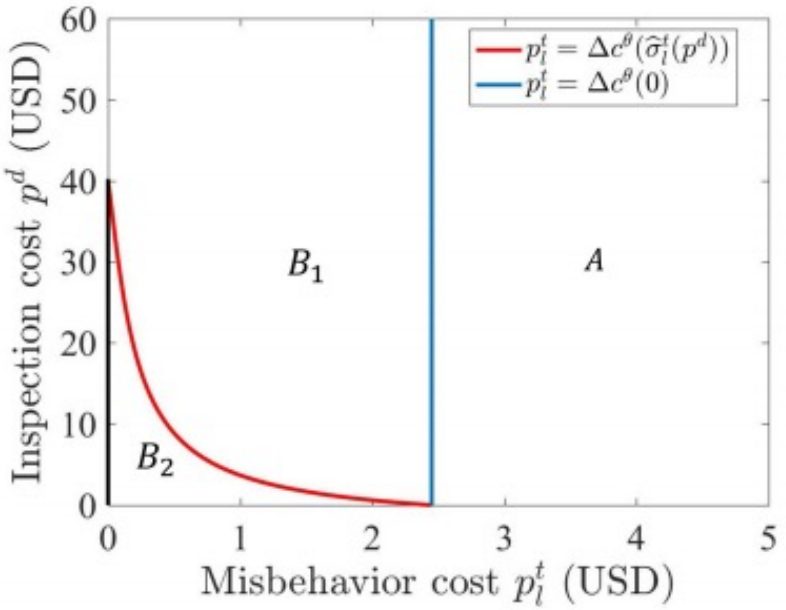
- Setting: tolled (high pr.) & free (low pr.) lanes in parallel
- Player 1: travelers, either paying or not paying toll
  - May misreport (signal) its vehicle type to road-side unit
  - Technological cost for misbehavior
  - Min user travel time + toll + misb. cost
- Player 2: system operator
  - Can inspect a particular traveler
  - Technological cost for inspection
  - Fine on detected misbehaving travelers
  - Min system travel time + insp. cost -fine





Perfect Bayesian equilibirum

- System operator has a prior belief
- System operator updates the belief according to received signal (high/low priority)
- Regimes for PBEs
  - High misbehavior: no misbehavior, no inspection
  - Low misbehavior cost, high inspection cost: misbehavior, no inspection
  - Low misbehavior & inspection cost: no misbehavior, no inspection



- Wu, M., Jin, L., Amin, S. and Jaillet, P., 2018, December. Signaling Game-based Misbehavior Inspection in V2I-enabled Highway Operations. In *2018 IEEE Conference on Decision and Control (CDC)* (pp. 2728-2734). IEEE.

Deception Games

- Deception is a method which can be employed by both attackers and defenders in advanced security problems to make the situation ambiguous, and hence, maximize their payoffs.
- Using deception in security systems makes the situation more complex as now a player relies less on his opponents' strategies in arriving at his decision.
- As discussed in, the information asymmetry in most security problems (e.g., one player may have more information than the other) is one of the main reasons that contributes to players acting deceptively in order to gain advantages.

Honeypot

- In fact, deception can also be used in active cyber defense to manipulate the beliefs of an adversary.
- Perhaps, **honeypot** is one of the most common deception techniques for cyber defense, which is an effective deception mechanism set by the security system to detect, deflect, or counteract attempts of attackers in an information security system
- A honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site and contain information or resources of value to attackers.
- It is actually isolated, monitored, and capable of blocking or analyzing the attackers.

Cascading games

- Cascading failure is a phenomenon in security systems where failure of a subsystem can result in failure of successive subsystems.
- In other words, the failure can propagate over the system once an attack is successful.
- This issue which can put systems at a serious risk, particularly when there are strong interconnections among the subsystems, has been addressed from a dynamic game-theoretic perspective
- Example: network state consists of
  - Susceptible nodes (could be attacked)
  - Infected nodes (already attacked)
  - Dead nodes (already destroyed)

Summary questions

- Why is game theory relevant to cyber-physical security problems?
- What are players, strategies, utilities, and equilibria?