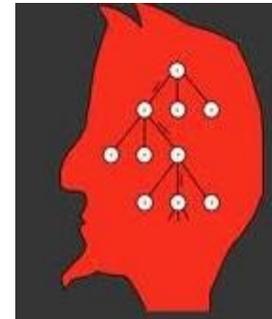
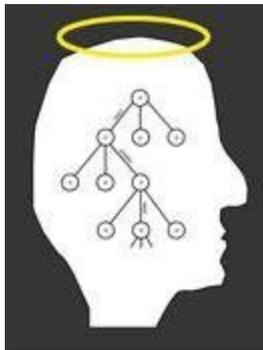


# Game theoretic modeling, analysis, and mitigation of security risks.

Assane Gueye  
NIST/ITL/CCTG, Gaithersberg

NIST ACMD Seminar  
Tuesday, June 7, 2011

[Click to edit Master subtitle style](#)



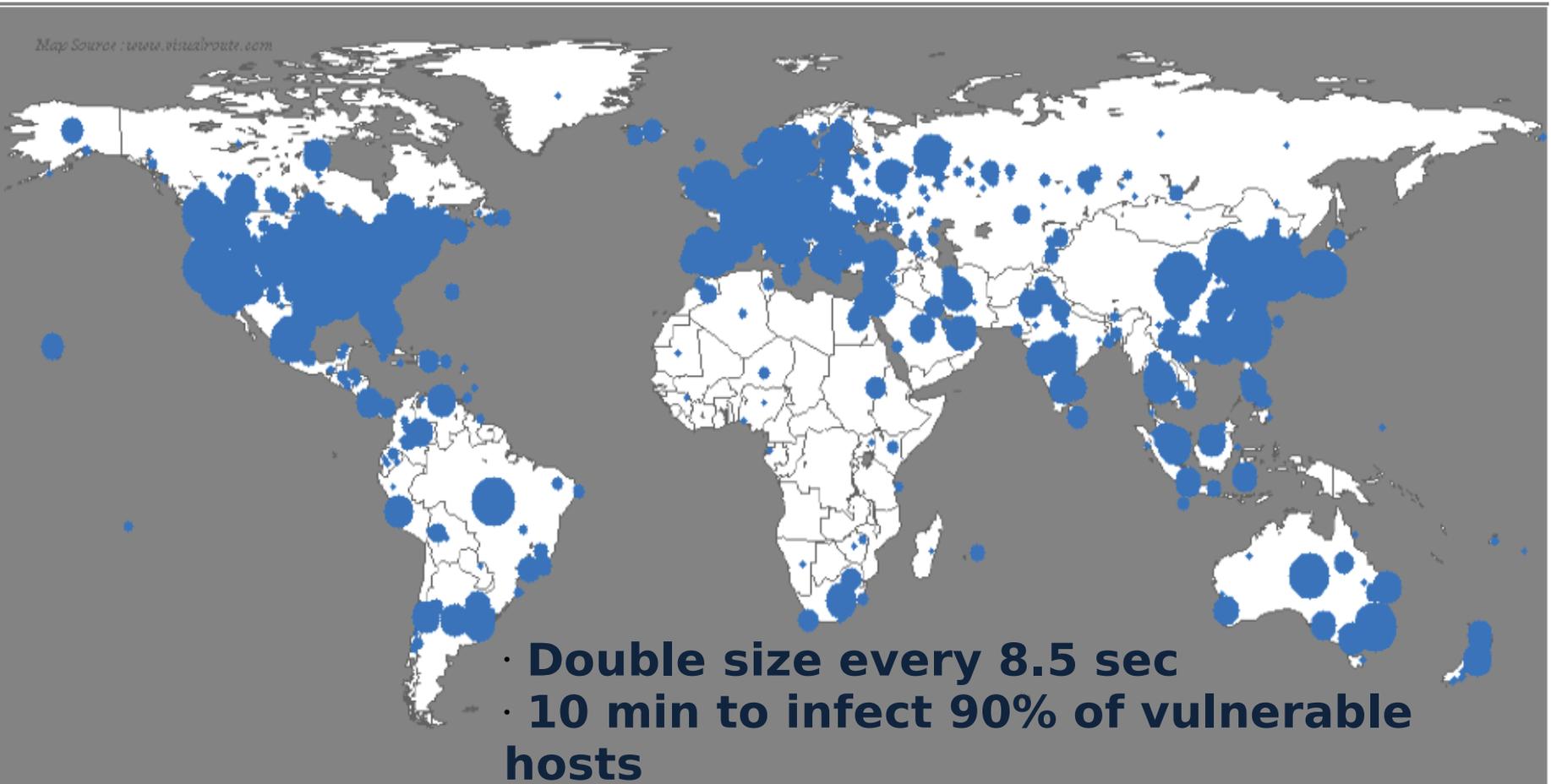
# Outline

1. Motivations
  1. Security
  2. Game Theory for Security
2. Game Theory
  1. History
  2. Game Theory Basics
3. Examples of Communication Security Game Model

# Motivations

# Life just before Slammer 30 minutes later! worm attack

Map Source: [www.visualroute.com](http://www.visualroute.com)



- Double size every 8.5 sec
- 10 min to infect 90% of vulnerable hosts

Sat Jan 25 06:00:00 2003 (UTC)

Number of hosts infected with Sapphire: 7165

Network Outages, cancelled airline flights, ATM failures, <http://www.caida.org>

Copyright (C) 2003 UC Regents

6/11

ATM failures

44

/ 34

TODAY'S NEWS: Sony Unleash 2 PlayStation 3 Exclusives for 2011

WINDOWS GAMES DRIVERS MAC LINUX SCRIPTS MOBILE HANDHELD NEWS

Home > News > Security > Virus alerts

**Virus alerts**

**Before you continue:**  
Run a free scan for Windows errors  
Scan your Windows registry for free with RegistryBooster 2010

**Conficker Worm Infects 3,5 Million Computers**

January 16th, 2009, 11:35 GMT by Lucian Constantin

Researchers from the Finnish security vendor F-Secure, estimate that at least one million computers have been infected by the Conficker worm in a single day. Their worldwide infections count now reads 3,523,230, while other security professionals blame the companies and home users for failing to install the critical patch released by Microsoft.

## Behind The Scenes at Anonymous' Operation Payback

Ernesto

15/11/2010

109

anonymous, Operation Payback

Operation Payback has been without a doubt the longest and most widespread attack on anti-piracy groups, lawyers and lobbyists. Despite the massive media coverage, little is known about the key players who coordinate the operation and DDoS attacks. A relatively small group of people, they are seemingly fuelled by anger, frustration and a strong desire to have their voices heard.

## Storm Worm botnet could be world's most powerful supercomputer

Categories: Botnets, Browsers, Data theft, Exploit code, Firefox, ...

Tags: Operation, Supercomputer, Malware, Worm, Ryan Narain

150 TalkBacks

Nearly nine months after it was first discovered, the Storm Worm Trojan continues to surge, building what experts believe could be the world's most powerful supercomputer.

The Trojan, which uses a myriad of social engineering lures to trick Windows users into downloading malware, has successfully seeded a massive botnet — between one million and 10 million CPUs — producing computing power

## China Cracks Down on Tor Anonymity Network

government for the first time.

By David Talbot

THURSDAY, OCTOBER 15, 2009

For the first time, the Chinese government has attacked one of the best, most secure tools for surfing the Internet anonymously. The clampdown against the tool, called **Tor**, came in the days leading up to the 60th anniversary of China's "national day" on October 1. It is part of a growing trend in which repressive nations orchestrate massive clampdowns during politically sensitive periods, in addition to trying to maintain Internet firewalls year-round.

## Sony Becomes Latest Operation Payback Attack Target

Contributed By: Headlines

**UPDATE:** An article in CIO states: "It get worse: An militant anti-Sony Anonymous offshoot calling its says it's targeting Sony individuals, unearthing em details, then posting them in public spaces. Some sleuthing for information about employees' children hacker complained "No one found ANY info on Stri, reference to Howard Stringer, president and CEO c Corporation). That's more than disturbing, it's repr example of how not to win friends and influence oth undermine your argument by engaging in depravity..."

## Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources, Google, which disclosed on the Gmail

"It was the first time the Chinese government has ever even included Tor in any sort of censorship circumvention effort," says Andrew Lewman, the executive director of Tor Project, the nonprofit that maintains the Tor software and network. "They were so worried about October 1, they went to anything that could possibly circumvent their firewall and blocked it."

Tor is one of several systems that route data through intermediate computers called proxies, thereby circumventing government filters. To anyone watching

## Lockheed Martin Hit By Cyber Attack, Department Of Homeland Security Confirms

LOLITA C. BALDOR | 05/28/11 11:58 PM ET | AP

## Russia accused of unleashing cyberwar to disable Estonia

Parliament, ministries, banks, media targeted

August 11th, 2008

**Coordinated Russian cyber attack in progress**

Posted by Dancho Danchev @ 4:23 pm

Categories: Black Hat, Botnets, Denial of Service, ...

Tags: Security, Cyber Warfare, DDoS, Georgia

62 TalkBacks

In the wake of the Russian-Georgian war, around Russian Internet forums have materialized into a coordinated cyber attack against Georgia's Internet infrastructure. Attacks have already managed to compromise several government web sites, with coordinated DDoS attacks against numerous other Georgian government sites, prompting government to switch to hosting located in the U.S., with Georgia's Ministry of Foreign Affairs undertaking a desperate step in Nisamed2now/AP

Bronze Soldier, the Soviet war memorial removed from Tallinn

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

guardian.co.uk

News | Sport | Comment | Culture | Business | Money | Life & style

News > Politics > Defence policy

## Stuxnet attack forced Britain to rethink the cyber war

virus uniquely programmed to attack Iran's nuclear facility showed power of cyber-weapons had reached chilling new level

Nick Hopkins  
guardian.co.uk, Monday 30 May 2011 21.45 BST  
Article history

CYBERWAR

## COMPUTERWORLD

IDG - verdens største mediehush innen it

SEMINAR & CIO | IT-KARRIERE | IT-HELSE | IT-KURS | IT-STILLING

Online attack hits US government Web sites

A botnet composed of about 50,000 infected computers has been waging a war against U.S. government Web sites and causing headaches for businesses in the U.S. and South Korea.

The attack started Saturday, and security experts have credited it with knocking the Web site of the U.S. Federal Trade Commission (FTC) offline for parts of Monday and Tuesday. Several other government Web sites have also been targeted, including the U.S. Department of Transportation (DOT).

NOMINATE NOW

Latest news from Security

# Who is attacking our communication Systems?

Hacktivists



Hackers



Foreign Governments



Terrorists, Criminal Groups



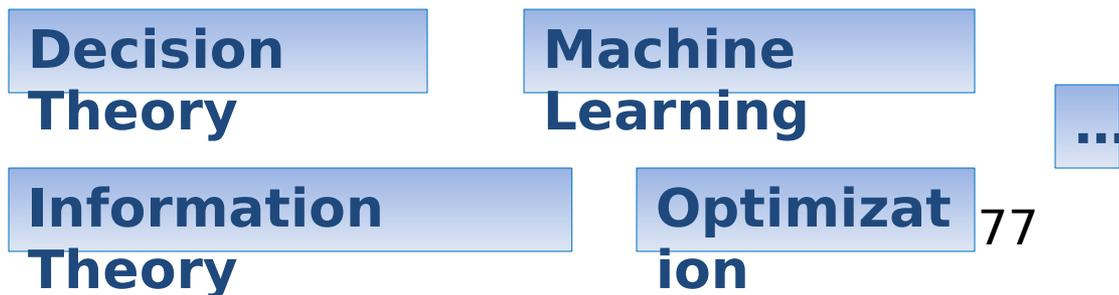
Disgruntled Insiders

# A lot of **good** effort!

- Some practical solutions

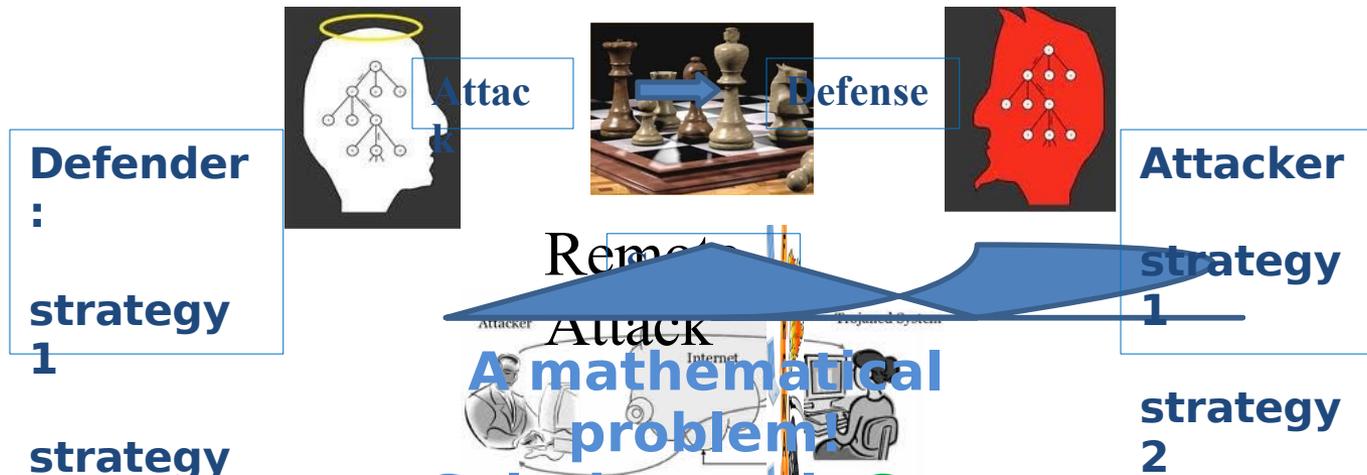


- Some theoretic basis



# Why Game Theory for Security?

Traditional Security Solutions



Predict attacker's behavior, Build defense mechanisms, Compute cost of security, Understand attacker's behavior, etc...

Game Theory also helps:

E.g.: Rate of Port

Scanning

IDS

tuning

Machine Intelligence

...

Conferences (GameSec, GameNets) , Workshops, books, Tutorials,...

This Talk:

How GT can help understand/develop security solutions?

Using illustrative Examples!

# Game Theory

# Game Theory

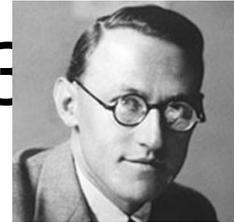


“...Game Theory is designed to address situations in which the outcome of a person’s decision depends not just on how they choose among several options, but also on the choices made by the people they are interacting with...”

“...Game theory is the study of the ways in which *strategic*

# Game Theory: A Little History

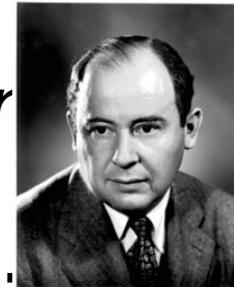
- Cournot (1838), Bertrand (1883)



O. Morgenstern 1902-1977

## Economics

- J. von Neumann, O. Morgenstern (1944)

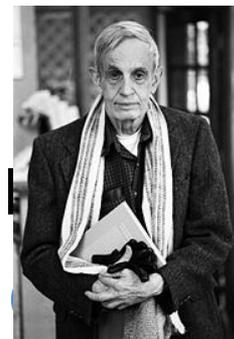


John von Neumann 1903-1957

- *“Theory of Games and Economic Behavior”*

- Existence of mixed strategy in a 2-player game

- J. Nash (1950): Nash Equilibrium



John F. Nash (1928)

- (Nobel Prize in Economic Science

6/7/11

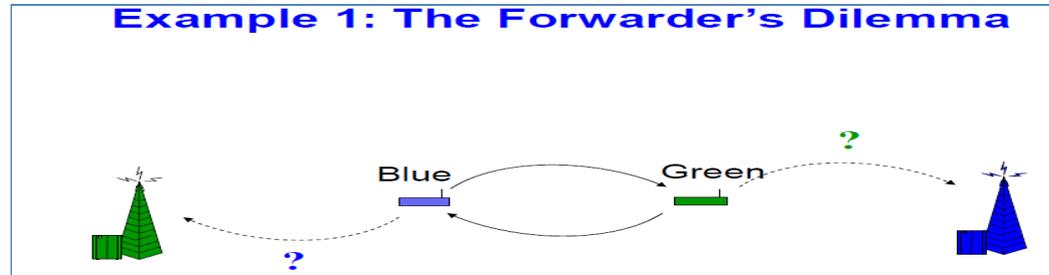
1994)

# Game Theory Basics

- **GAME = (P,A,U)**
  - **Players ( $P_1; \dots ; P_N$ ):** Finite number ( $N \geq 2$ ) of decision makers.
  - **Action sets ( $A_1; \dots ; A_N$ ):** player  $P_i$  has a nonempty set  $A_i$  of actions.
  - **Payoff functions  $u_i : A_1 \times \dots \times A_N : R; i = 1; \dots ; N$**

# Key Concepts

## Example: Forwarder's dilemma



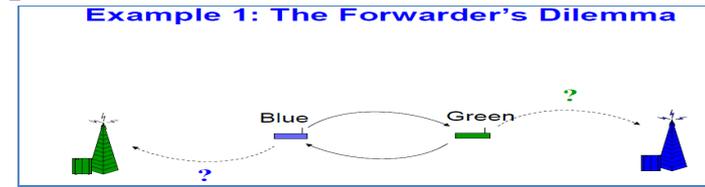
Forwarding has an energy cost of  $c$   
( $c \ll 1$ )

Successfully delivered packet:  
reward of 1

If **Green** drops and **Blue** forwards:

# Key Concepts

## Example: Forwarder's dilemma



Game:

Players: Green, Blue

Actions: Forward (F), Drop (D)

Payoffs:  $(1-c, 1-c)$ ,  $(-c, -c)$ ,  $(-c, 1)$ ,  $(1, -c)$

From a problem to a game

- Users controlling the devices are *rational* (or *selfish*): they try to maximize their benefit
- Game formulation:  $G = (P, S, U)$ 
  - P: set of players
  - S: set of strategy functions
  - U: set of utility functions
- **Strategic-form** representation
  - Reward for packet reaching the destination: 1
  - Cost of packet forwarding:  $c$  ( $0 < c << 1$ )

c)

Matrix rep

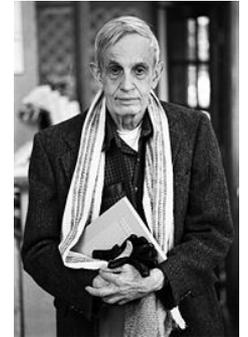
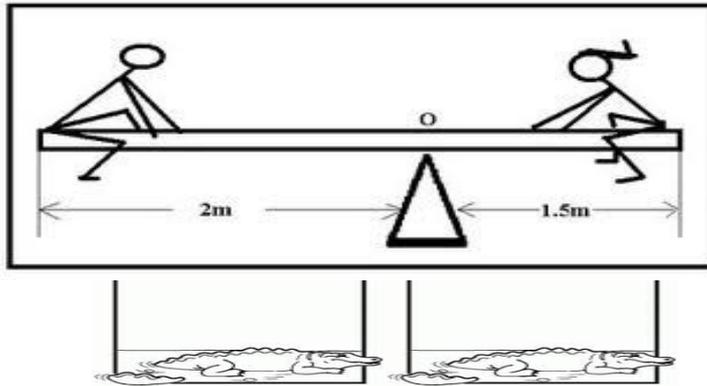
		Green	
		Forward	Drop
Blue	Forward	$(1-c, 1-c)$	$(-c, 1)$
	Drop	$(1, -c)$	$(0, 0)$

Actions of Blue

Reward of Blue

Reward of Green

# Equilibrium Concept



John F. Nash  
(1928)

Nash equilibrium:

“...a solution concept of a game involving two or more players, in which no player has anything to gain by changing his own strategy”

From a problem to a game

- Users controlling the devices are *rational* (or *selfish*): they try to maximize their benefit
- Game formulation:  $G = (P, S, U)$

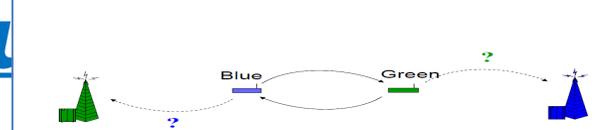
- P: set of players
- S: set of strategy functions
- U: set of utility functions

- Reward for packet reaching the destination: 1
- Cost of packet forwarding:  $c$  ( $0 < c \ll 1$ )

- **Strategic-form** representation

	Green	
Blue	Forward	Drop
Forward	(1-c, 1-c)	(c, 0)
Drop	(1, -c)	(0, 0)

Example 1: The Forwarder's Dilemma



6/7/11

# Other Concepts

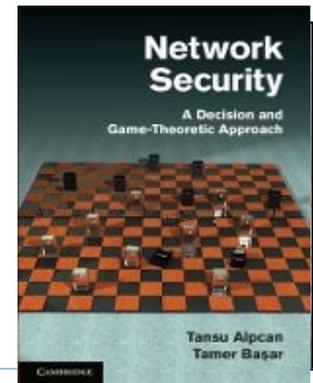
- Cooperative / Non-Cooperative
- Static / dynamic (finite/infinite)
- Complete / Incomplete Information

## Bayesian

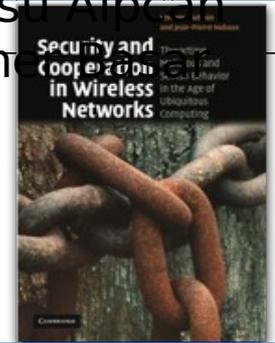
- Zero-Sum, Constant-Sum, Variable-Sum

6/7/11

- Stochastic



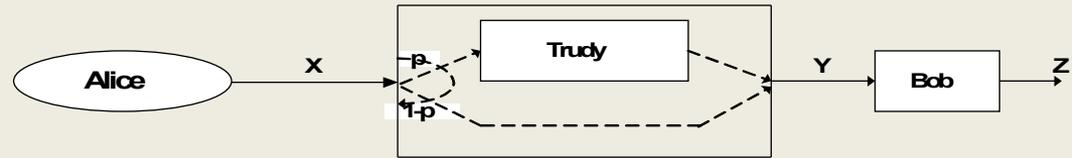
**Game Theory: A Decision and Game Theoretic Approach**  
Tansu Alpcan  
Tamer Başar



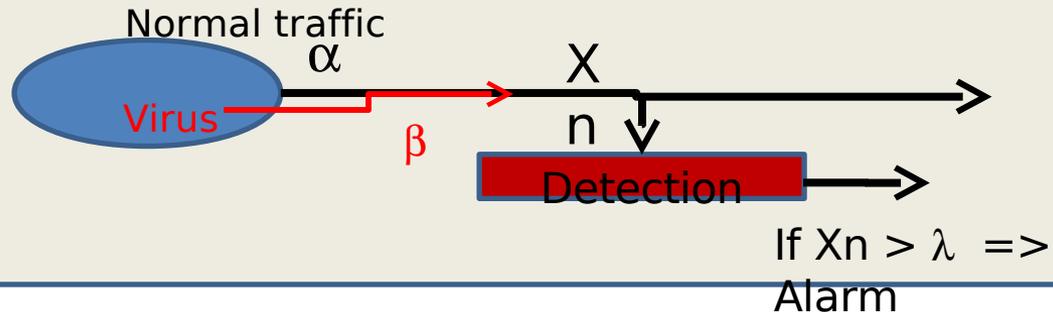
**Security and Cooperation in Wireless Networks**  
Martin J. Osborne  
Alejandro R. Pinto  
Jean-Pierre Auh

# 3 Communication Security Game Models

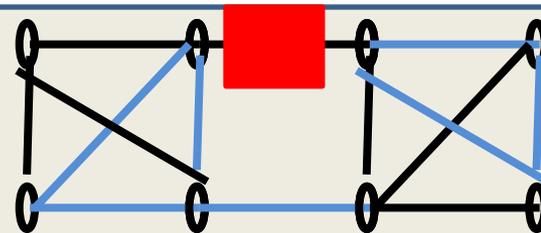
Intruder Game



Intelligent Virus

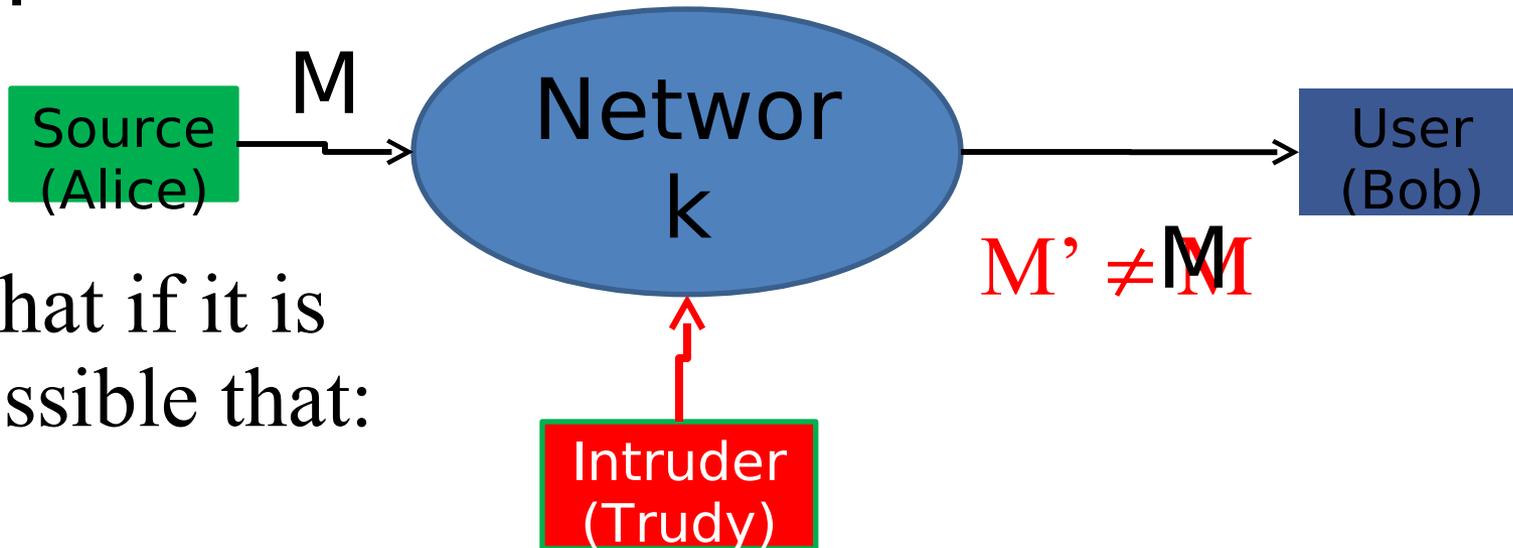


Availability Attack



# Intruder Game

Scenario:



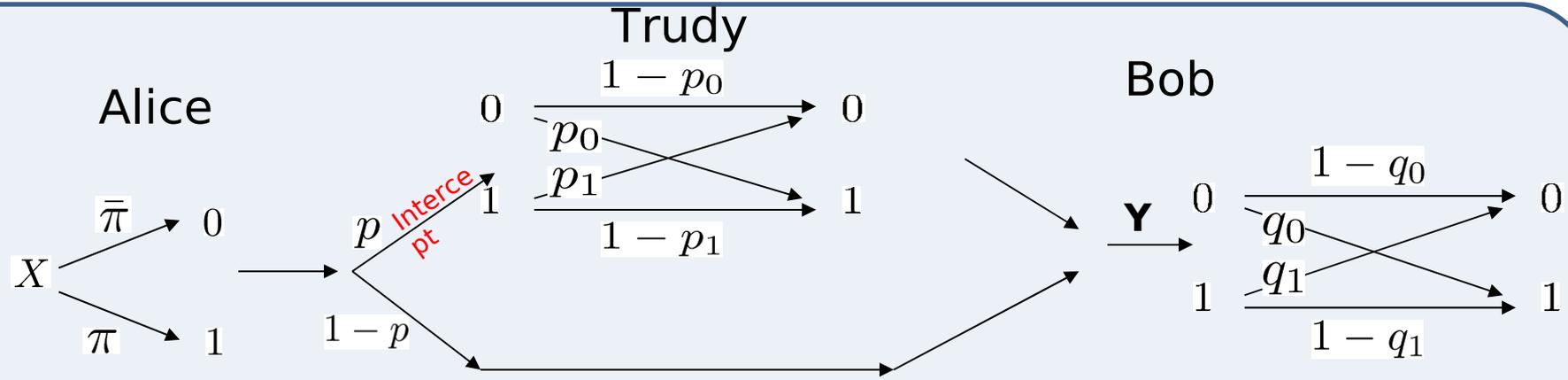
What if it is possible that:

Encryption is not always

practical.

Formulation: Game between Intruder and User

# Intruder Game: Binary



- Strategies (mixed i.e. randomized)

- Trudy:  $(p_0, p_1)$ , Bob:  $(q_0, q_1)$

- Payoffs:

$$\text{Trudy: } \Phi(Z, X) = A * 1_{(Z=1, X=0)} + B * 1_{(Z=0, X=1)}$$

$$\text{Bob: } \Psi(Z, X) = -\Phi(Z, X)$$

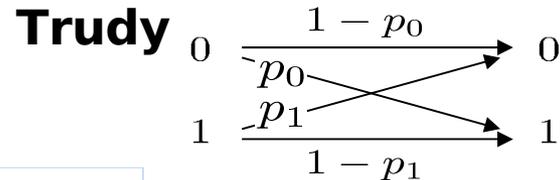
- One shot, simultaneous choice game

- Nash Equilibrium?

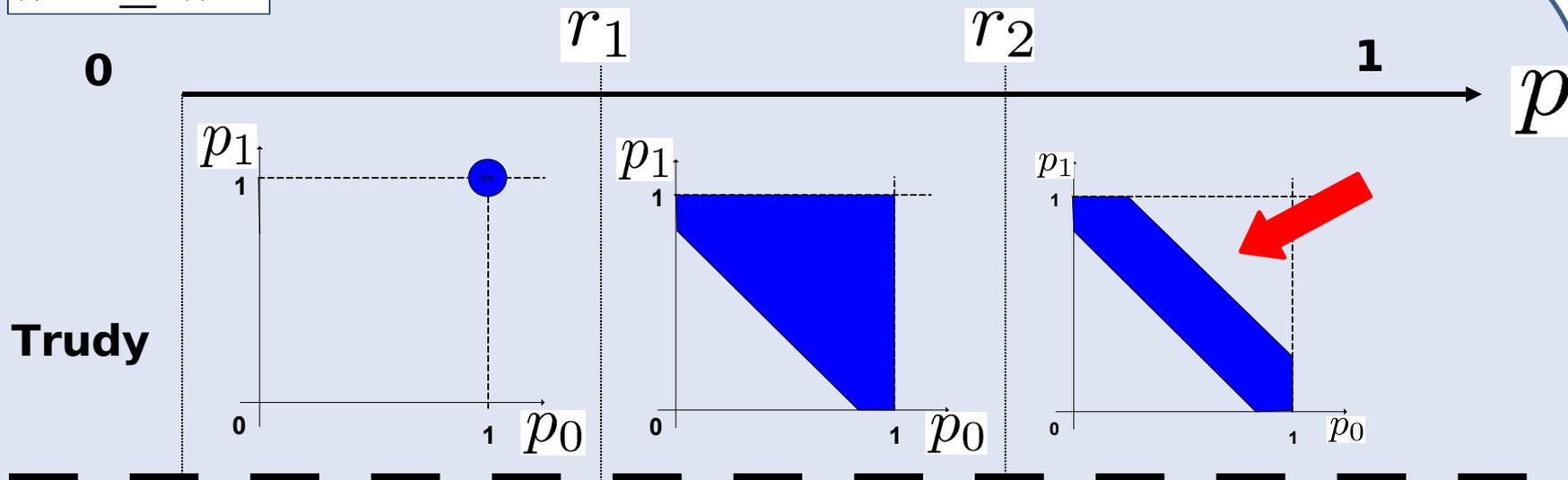
# Intruder game:

## NE

**Payoff**  $\text{Trudy}$ :  $\Phi(Z, X) = A * 1_{(Z=1, X=0)} + B * 1_{(Z=0, X=1)}$



$$\bar{\pi} A \leq \pi B$$



**Bob**

**Always trust**

$$q_0 = q_1 = 0$$

$$\Phi^* = p(\bar{\pi} A + \pi B)$$

**Always decide the less costly hit (1)**

$$q_0 = 1, q_1 = 0$$

$$\Phi^* = \bar{\pi} A$$

**Always decide the less costly hit (1)**

$$q_0 = 1, q_1 = 0$$

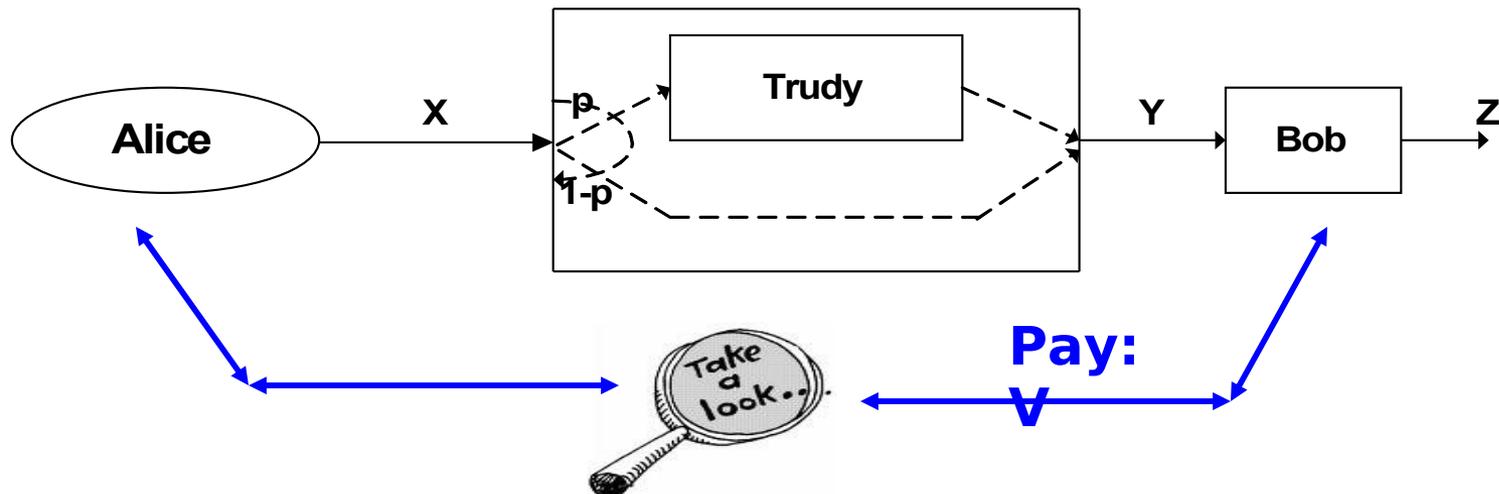
$$\Phi^* = \bar{\pi} A$$

$$r_1 = \frac{\bar{\pi} A}{\bar{\pi} A + \pi B}$$

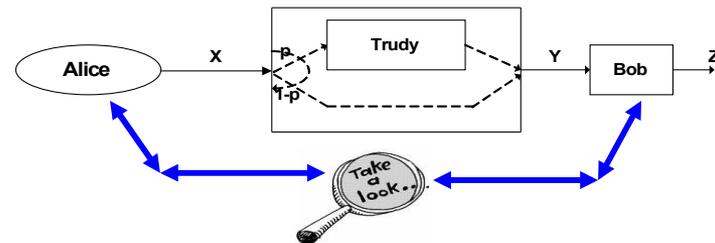
$$r_2 = \frac{\pi B}{\bar{\pi} A + \pi B}$$

# What if the receiver (Bob) can verify the message?

(by paying a cost and using a side secure channel)



# Cost and Reward

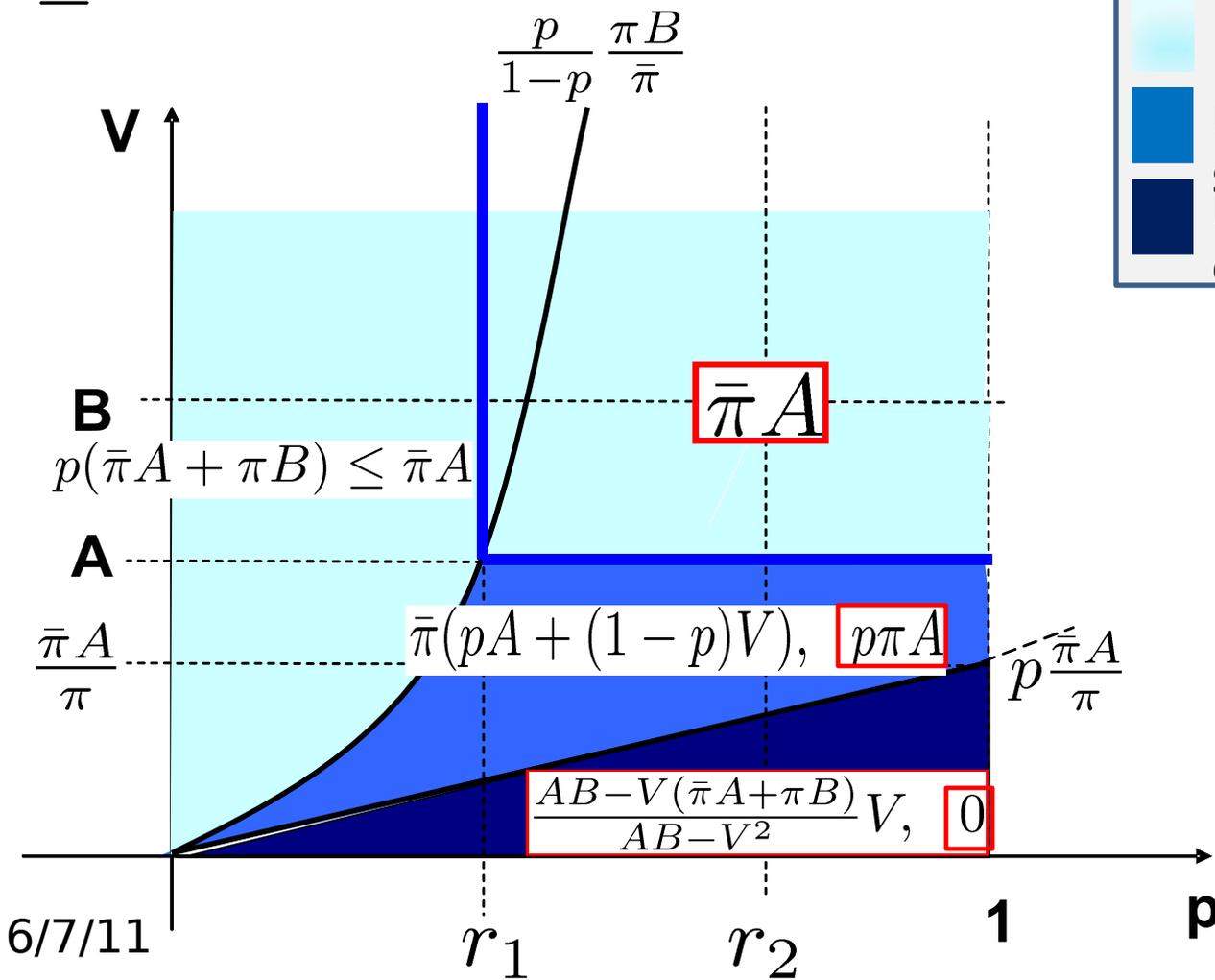


$$\bar{\pi}A \leq \pi B$$

Never use side channel

Use only sometimes

Use more often



**Challenge:**

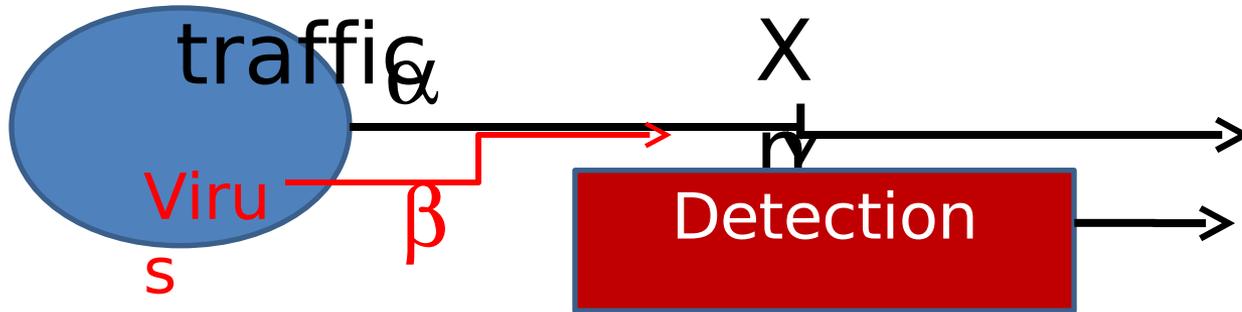
Credible threat

Deter Attacker from attacking

# Intelligent Virus Game

Scenario

o Normal traffic



If  $X_n > \lambda \Rightarrow \text{Alarm}$ .

Assume  $\alpha$

known

**Virus!** choose  $\beta$  to maximize

**infection cost**

**Detection system!** choose  $\lambda$  to

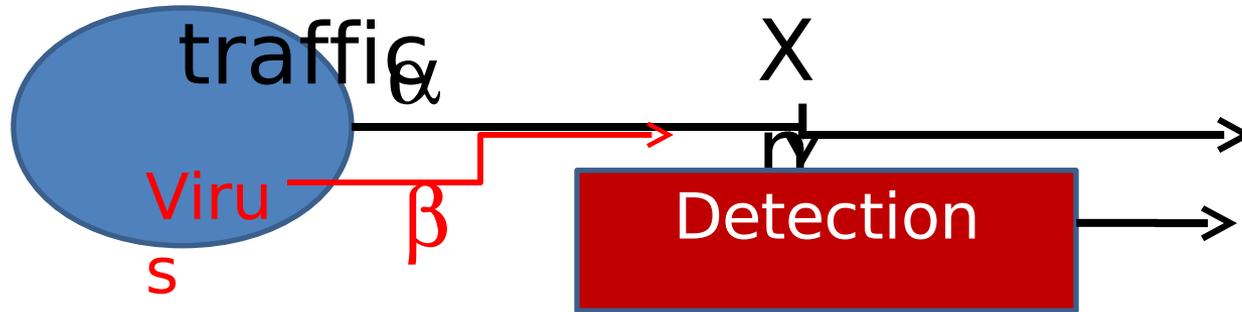
minimize **cost of infection + clean**

**up**

# Intelligent Virus Game (IDS)

Scenario

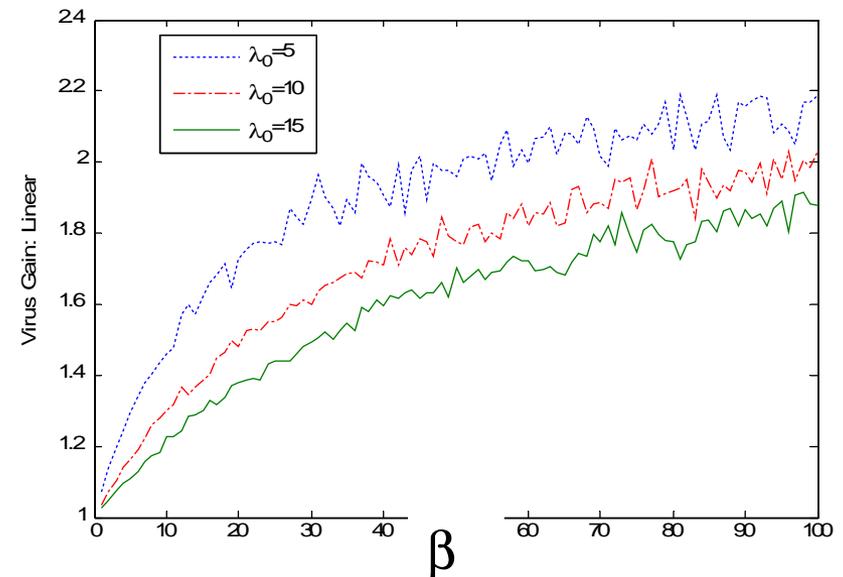
o Normal



If  $X_n > \lambda \Rightarrow \text{Alarm}$ .

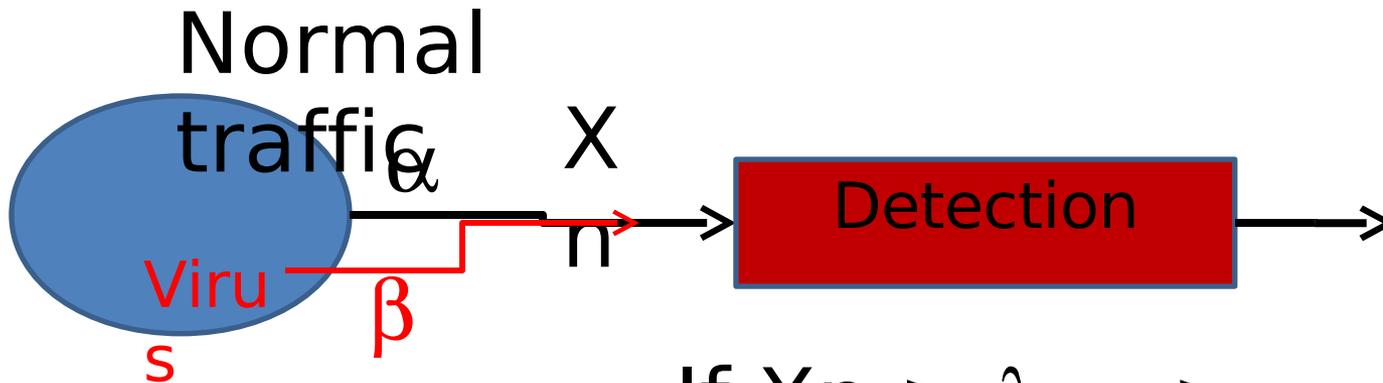
Smart virus designer  
picks  
very large  $\beta$ , so that the  
cost is always high ....  
Regardless of  $\lambda$ !

6/7/11



# Intelligent Virus Game (IPS)

Modified Scenario

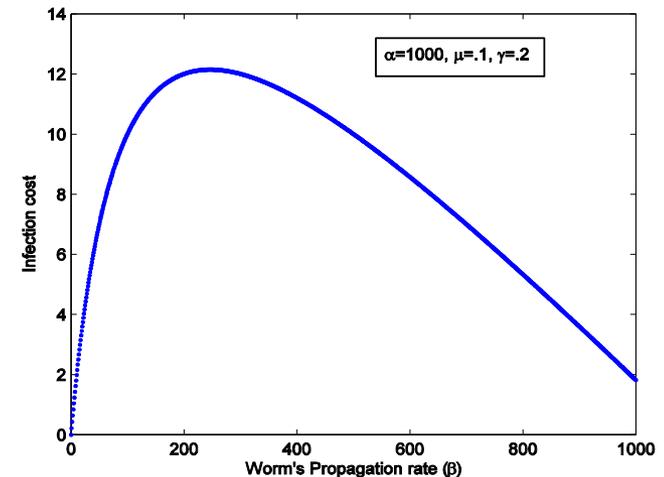


• Detector: buffer traffic and test threshold

- $Xn < \lambda$  process
- If  $Xn > \lambda$  Flush & Alarm

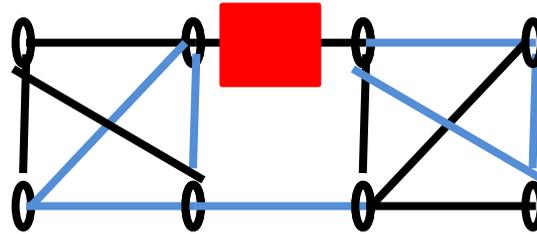
• Game between Virus ( $\beta$ ) and Detect ( $\lambda$ )

( $\lambda$ )<sub>6/7/11</sub>



# Availability Attack Models!

Tree-Link  
Game:



# Model

- Game

- Graph = (nodes  $V$ , links  $\mathbf{E}$ , spanning trees  $\mathbf{T}$ )

- Defender:

chooses  $T \in \mathbf{T}$

- **Attacker:** on  $\mathbf{T}$ , to minimize

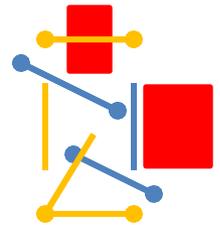
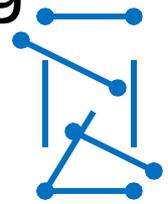
chooses  $e \in \mathbf{E}$  (+ "No Attack")

- **Attacker:** on  $\mathbf{E}$ , to maximize

= Rewards

$$R(\alpha, \beta) = \sum_{e \in \mathbf{E}} \beta_e \left( \sum_{T \in \mathbf{T}} \alpha_T 1_{e \in T} - \mu_e \right)$$

Example



Defender: 0

Attacker: -

$\mu_2$

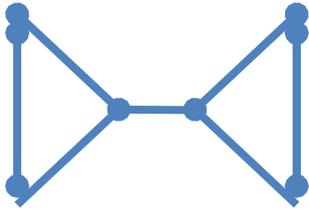
Attacker:

$1 - \mu_1$

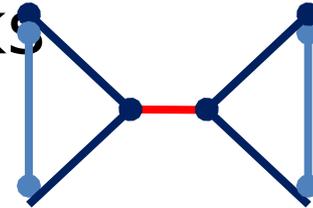
# Let's Play a Game!

Assume: zero attack cost  $\mu_e=0$

Graph

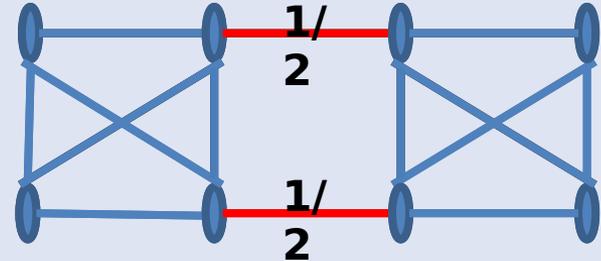
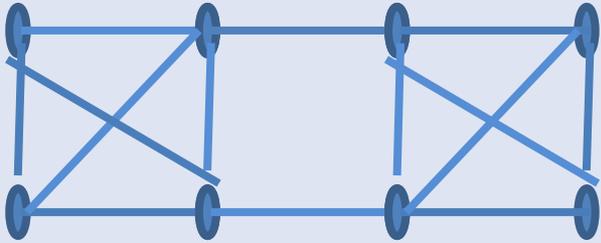


Most vulnerable links



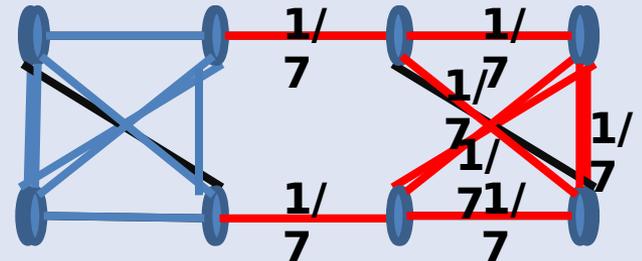
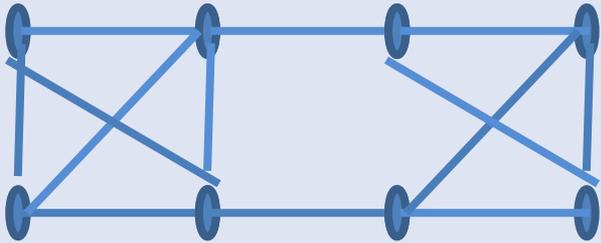
a)

b)



Chance  
 $1/2$

c)



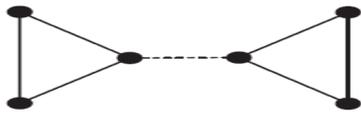
Chance  
 $4/7 > 1/2$

6/7/11

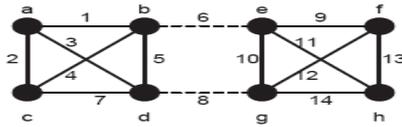
2828

$2/34$

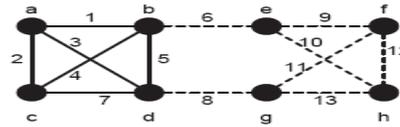
# Critical Subset of Links



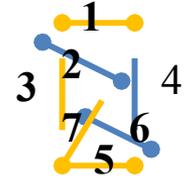
(a) Graph with bridge



(b) Network where minimum cut set is critical



(c) Minimum cut set is not critical



$\chi(G) = 1$

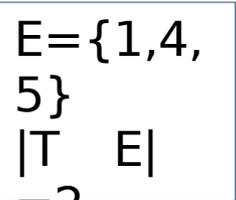
$\chi(G) = 1/2$

$\chi(G) = 4/7$

• **Definition 1&2:** For any nonempty subset  $E \subseteq E$

1.  $M(E) = \min\{|T \cap E|, |T| \}$

(minimum number of links  $E$  has in common with any spanning tree)



$M(E) = 1$

2. Vulnerability of  $E$

$\chi(E) = M(E)/|E|$

$\chi(E) = 1/3$

(minimum fraction of links  $E$  has in common with any spanning tree)

• **Definition 3:** A nonempty subset  $C \subseteq E$  is said to be **critical** if

$\chi(C) = \max_{E \subseteq E} \chi(E)$

( $C$  has maximum vulnerability)

Defender: choose trees that minimally cross **critical** subset of critical subset  $\chi(G) = \chi(C)$  vulnerability

# Critical Subset Attack Theorem

**Theorem 1:** There exists a Nash Equilibrium where

- **Attacker** attacks only the links of a critical set  $C$ , with **equal probabilities**
- **Defender** chooses only spanning trees that have a minimal intersection with  $C$ , and have equal likelihood of using each link of  $C$ , no larger than that of using any link not in  $C$ . [Such a choice is possible.]

There exists a polynomial algorithm to find  $C$  [Cunningham 1982]

Theorem generalizes to a large class of games.

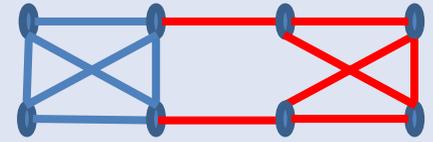
6/7/11

3030

/ 34

# Some implications

Edge-Connectivity is not always the right metric!



If  $v \leq 0$ : Attacker: "No

$$v = \max_{E \in \mathcal{E}} \left( \frac{M(E)}{|E|} - \frac{\mu(E)}{|E|} \right)$$

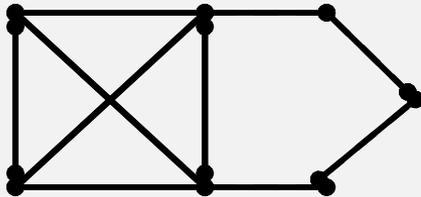
Attack

If can invest to make  $\mu$  high  
 → Deter attacker from attacking  
 • Need to randomize choice of tree

## Network Design

Additional link

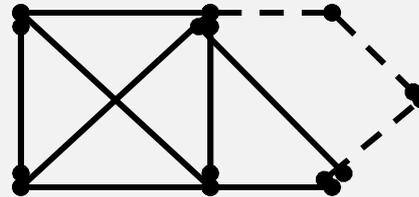
$$v = 3/4$$



a )

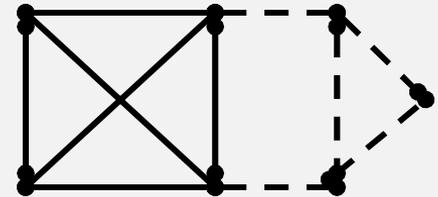
Network in b) is more vulnerable than network in c)

$$v = 2/3$$



b )

$$v = 3/5$$



c )

$$\frac{2}{3} > \frac{3}{5}$$

3131

on

## *Game Theory helps for a better understanding of the Security problem!*

Intruder and Intelligent Virus Games:

- Most aggressive attackers are not the most dangerous ones
- Mechanisms to deter attackers from attacking

Availability Games

- **Critical set**

- Vulnerability ( $\chi(G)$ ): a metric more refined than edge-connectivity
- Analyzing NE helps determine most vulnerable subset of links
- Importance in topology design
- Polynomial-time algorithm to compute critical set

# This is an “young” research field!

- A certain number of issues
  - Costs model
    - Not based on solid ground
  - Mixed strategy equilibrium
    - How to interpret it?
  - Nash equilibrium computation
    - In general difficult to compute

## Game Theory for Airport Security

### ARMOR (LAX)

Airports create security systems and terrorists

seek out breaches.

Placing  
checkpoint



Allocate canine  
units



- Still “theoretic”?

6/7/11

3333

/ 34

# Future Work

- Repeated versions of the games
  - More realistic models
  - Applications: Attack Graphs
- Collaborative Security
  - Team of Attacker vs Team of Defenders
  - Trust and Security
  - Role of Information
- Security of Cloud Computing

Thank you!

Questions?

