ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

GameSec 2010

Designing Network Security and Privacy Mechanisms: How Game Theory Can Help

Jean-Pierre Hubaux
EPFL

With contributions (notably) from
J. Freudiger, H. Manshaei, P. Papadimitratos, M. Poturalski, and M. Raya

Wireless Networks

- Many deployment scenarios
- Spectrum is a scarce resource
  ➔ Potential strategic behavior of individual devices or network operators
- Paradise for game theorists ?

Modern Mobile Phones

Quad band GSM
(850, 900, 1800, 1900 MHz)

GPRS/EDGE/HSDPA

Tri band UMTS/HSDPA
(850, 1900, 2100 MHz)

Soon LTE

GPS + accelerometers

WiFi (802.11b/g)

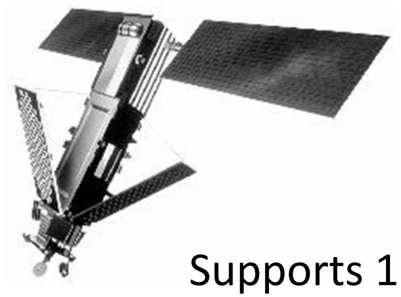
Bluetooth

P2P wireless
- Nokia: NIC
- Qualcomm: Flashlinq
- WiFi-Alliance: Wi-Fi Direct

Wireless Enabled Devices

Satellite Communications

Iridium Satellite



Supports 1100 concurrent phone calls
Orbit altitude: approx. 780 km
Frequency band: 1616-1626.5 MHz
Rate: 25 kBd
FDMA/TDMA

Global Positioning System (GPS)
Orbit altitude: approx. 20,200 km
Frequency: 1575.42 MHz (L1)
Bit-rate: 50 bps
CDMA

Iridium 9505A Satellite Phone

BTCC-45 Bluetooth GPS Receiver

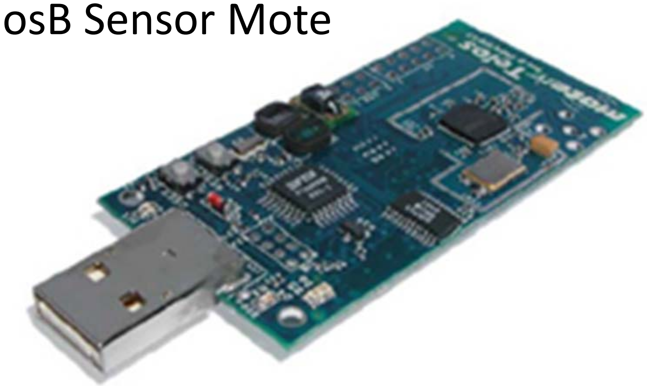
Wireless “Last Mile”: WiMax

WiMAX GP3500-12 omnidirectional antenna
Frequency band: 3400-3600 MHz
Gain: 12 dBi
Impendence: 50 Ω
Power rating: 10 Watt
Vertical beam width: 10°

WiMAX PA3500-18 directional antenna
Frequency band: 3200-3800 MHz
Gain: 12 dBi
Impendence: 50 Ω
Power rating: 10 Watt
Vertical beamwidth: 17°
Horizontal beamwidth: 20°

Wireless Sensors

TelosB Sensor Mote



IEEE 802.15.4 Chipcon Wireless Transceiver
Frequency band: 2.4 to 2.4835 GHz
Data rate: 250 kbps
RF power: -24 dBm to 0 dBm
Receive Sensitivity: -90 dBm (min), -94 dBm (typ)
Range (onboard antenna): 50m indoors / 125m outdoors

Imote2

Cricket Mote

Iris Mote

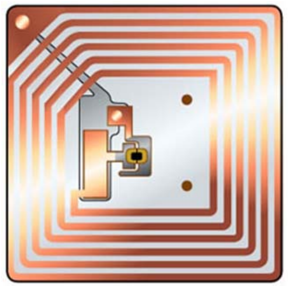
MicaZ

Radio-Frequency Identification (RFID)

SDI 010 RFID Reader

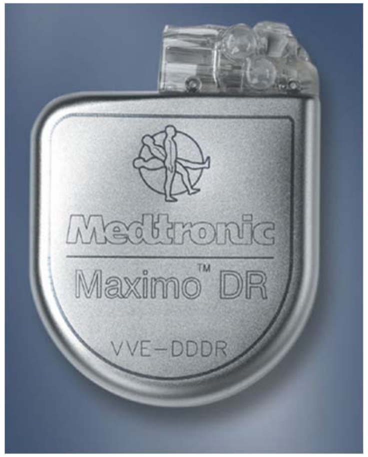
ISO14443-A and B (13.56 MHz)
Operating distance: 1cm
Communication speed: up to 848 Kbit/s

RFID tag



Medical Implants

Implantable Cardioverter Defibrillator (ICD)



Operating frequency: 175kHz
Range: a few centimeters

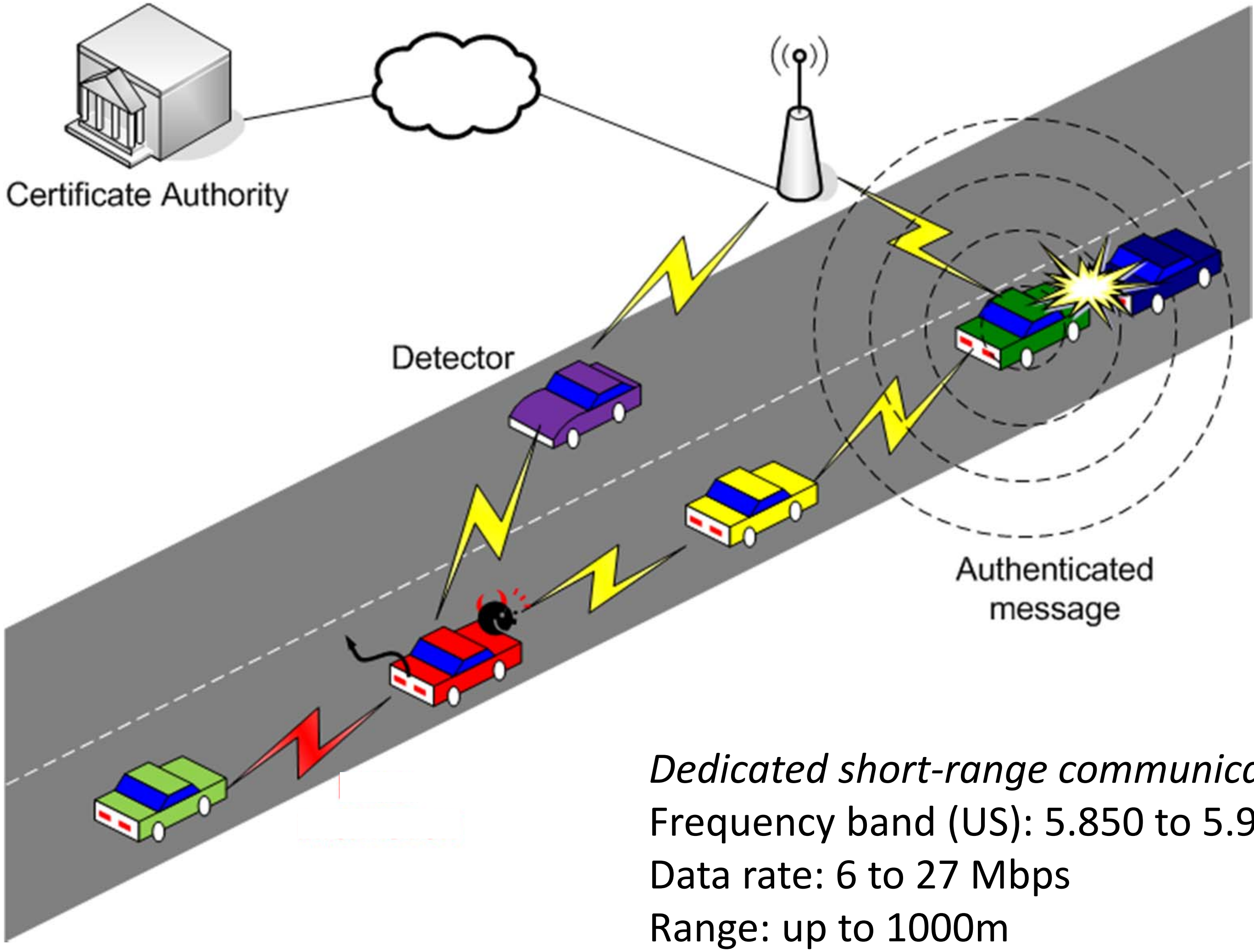
Medical Implant Communication Service (MICS)
Frequency band: 402-405 MHz
Maximum transmit power (EIRP): 25 microwatt
Range: a few meters

Software Defined Radio

Tuning Frequency:
30KHz - 30MHz (continuous)
Tuning Steps:
1/5/10/50/100/500Hz & 1/5/9/10KHz
Antenna Jacket / Impedance:
BNC-socket / 50Ohms
Max. Allowed Antenna Level :
+10dBm typ. / saturation at -15dBm typ.
Noise Floor (0.15-30MHz BW 2.3KHz):
Standard: < -131dBm (0.06µV) typ.
HighIP: < -119dBm (0.25µV) typ.
Frequency Stability (15min. warm-up period):
+/- 1ppm typ.

Application: Cognitive Radios ➔ Dynamic Spectrum Access

Vehicular Communications



Dedicated short-range communications (DSRC)
Frequency band (US): 5.850 to 5.925 GHz
Data rate: 6 to 27 Mbps
Range: up to 1000m

Question

- Would you model wireless devices / network operators by cooperative or non-cooperative games?
- Back to the fundamentals…

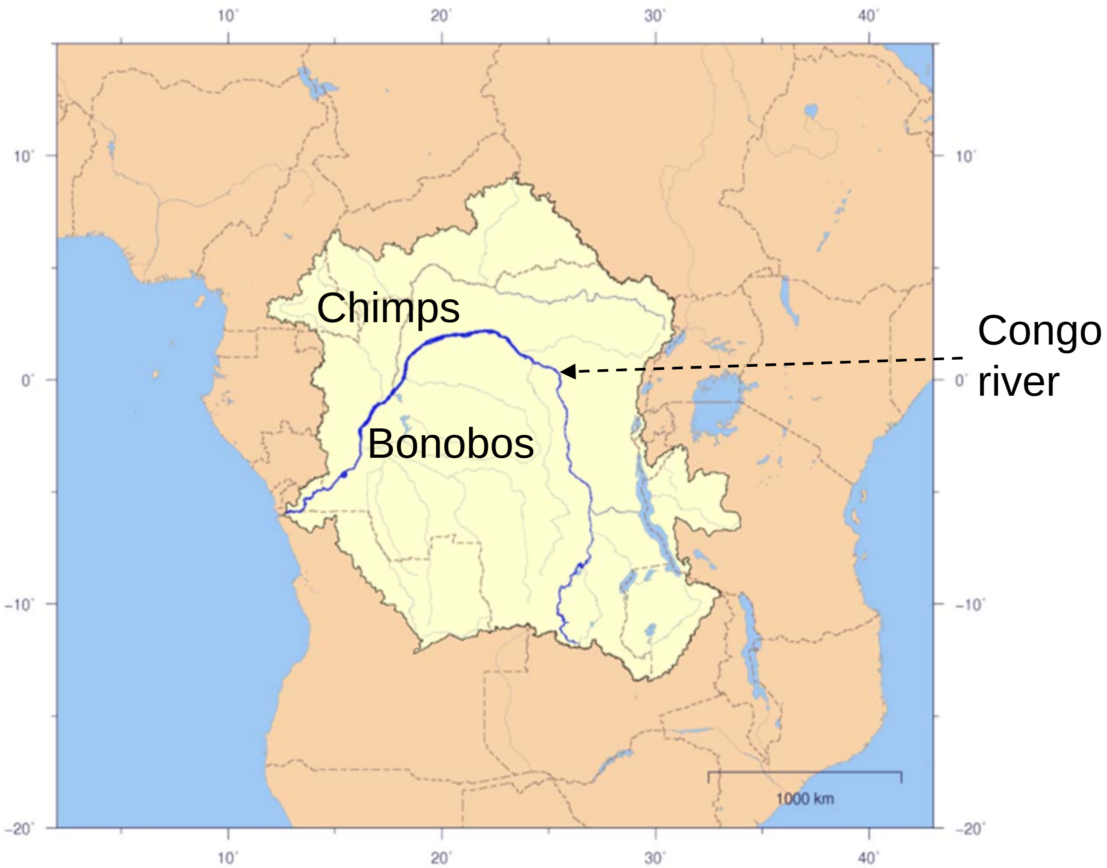
(Non)-Cooperative behavior in wireless networks: bonobos Vs chimps

Chimpanzee
www.ncbi.nlm.nih.gov

Bonobo
www.bio.davidson.edu

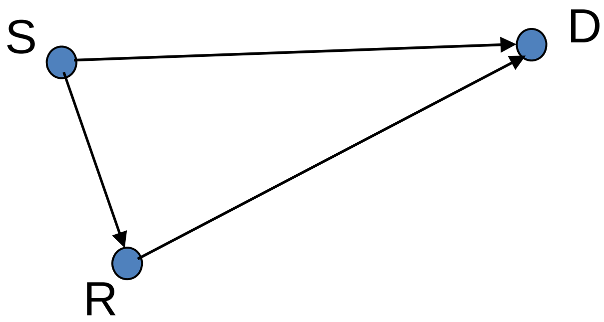
Living places (very simplified)

Cross-layer design…

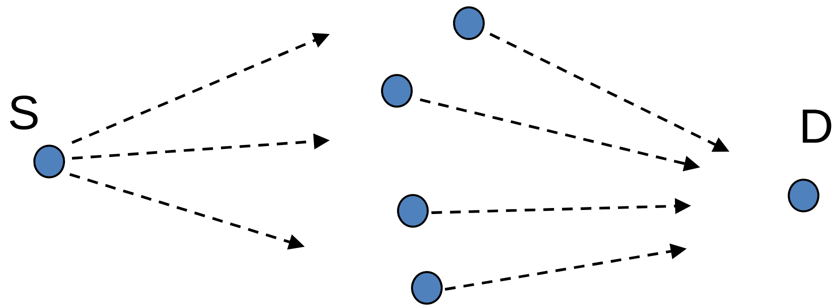


Upper layers (MAC and above)	Non-Cooperative (or “selfish”)
Physical layer	Cooperative

Cooperation between wireless devices (at the physical layer)

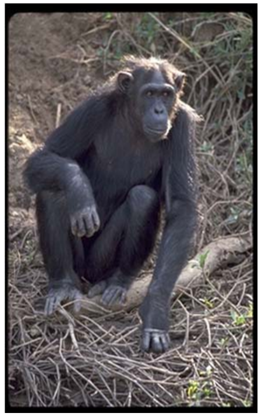


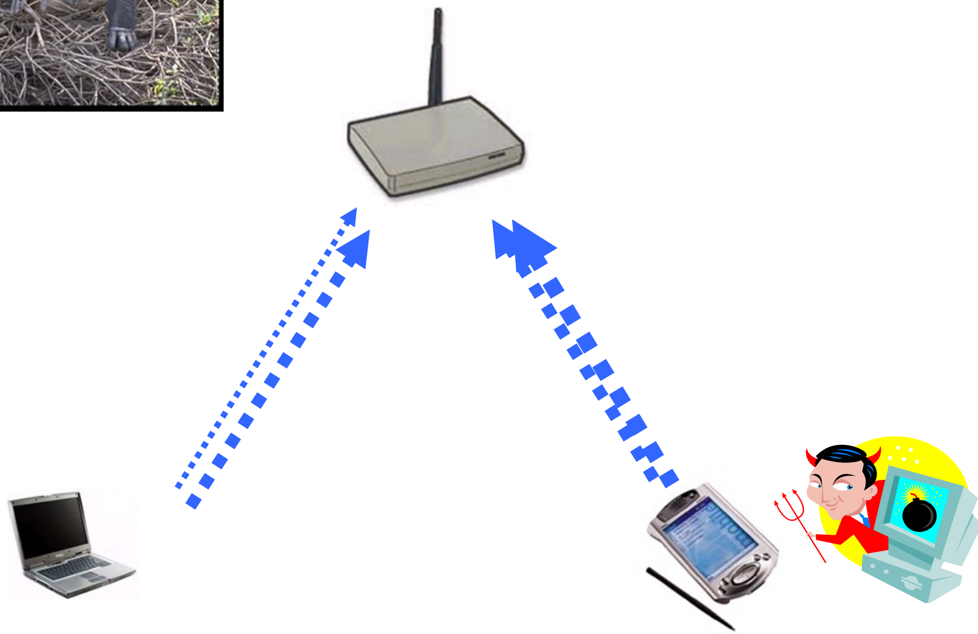
Cooperative relaying



Cooperative beamforming

Non-cooperation between wireless devices (MAC and network layer)



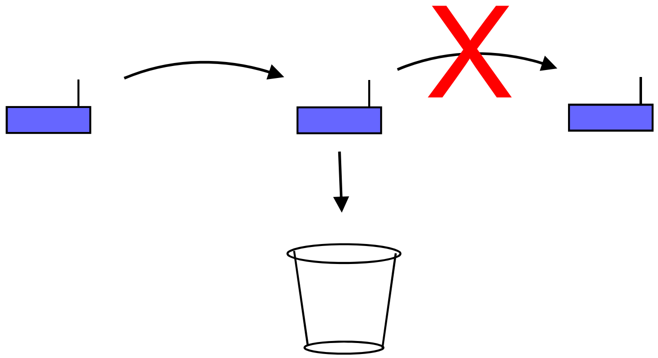


Well-behaved node

Well-behaved node

Cheater

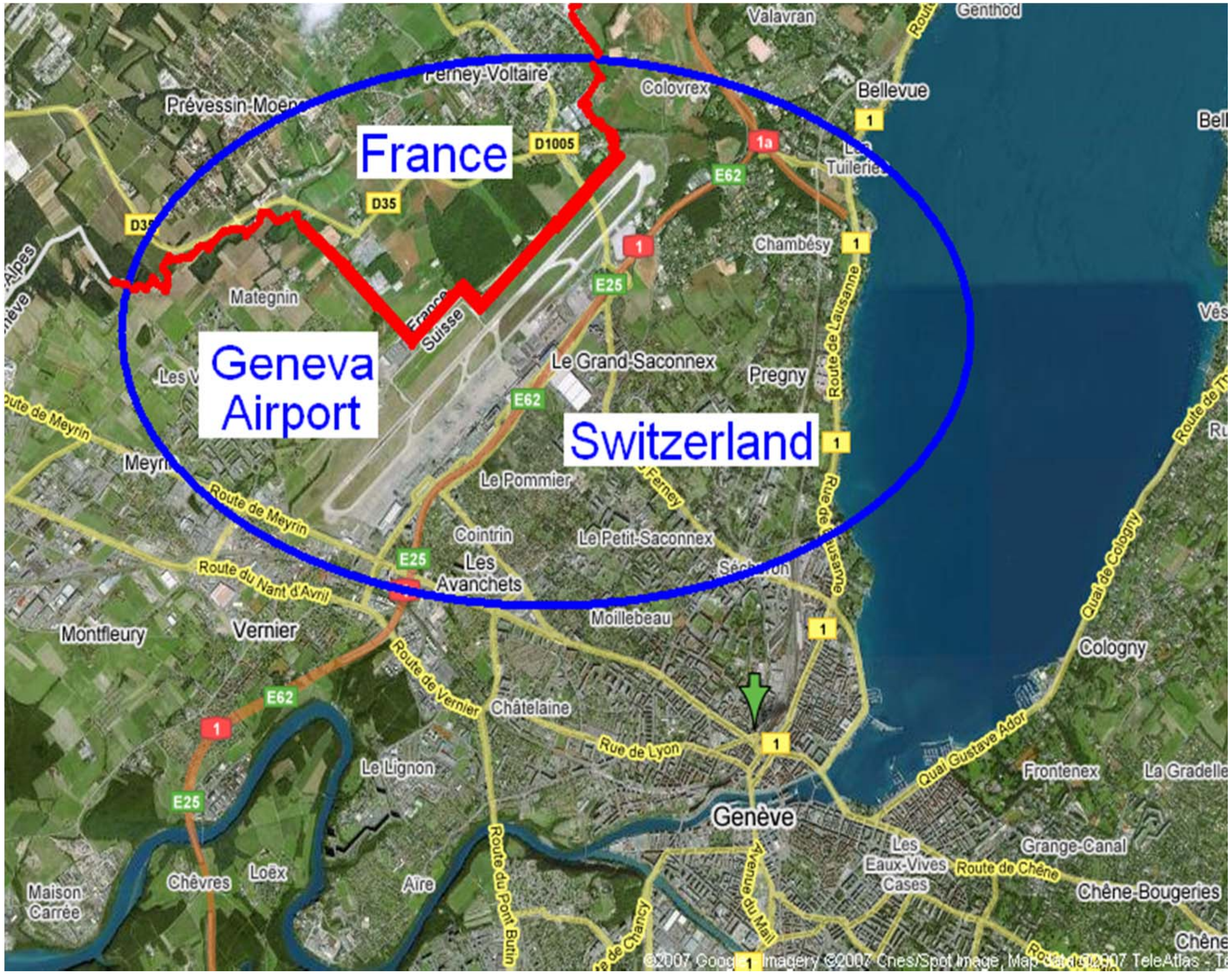
At the MAC layer



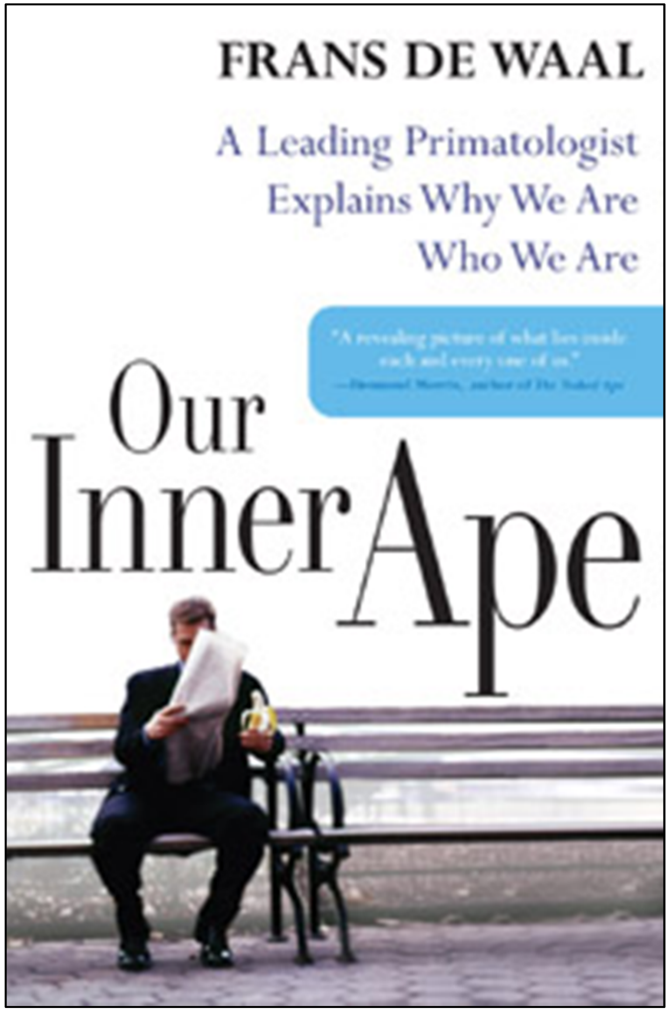
At the network layer

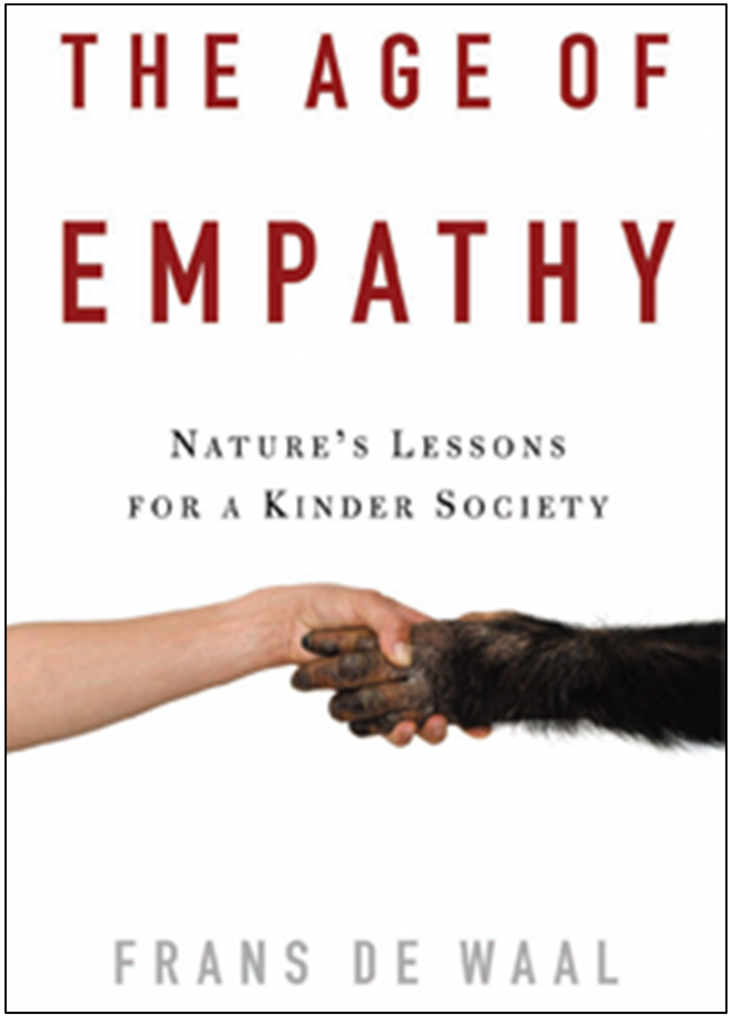
Note: sometimes non-cooperation is assumed at the physical layer; likewise, cooperation is sometimes assumed at the upper layers

(Non-)cooperation between wireless networks: cellular operators in shared spectrum



More on primatology





Dynamic Spectrum Allocation

- Rationale: wireless devices becoming *very* sophisticated
  ➔ ``Command and Control´´ allocation of the spectrum obsolete
  ➔ Less regulation !!!
- Each device / each operator is a selfish agent
- The market determines (in real time) the best usage of the spectrum
- Already a modest realization in the ISM band (for WiFi)
- IEEE DySPAN: Dynamic Spectrum Access Networks
- But isn’t this rather lawyers’ paradise?
- Skepticism of regulators

Vulnerabilities of Wireless Devices…

… to malicious behavior

The New York Times

A Heart Device Is Found Vulnerable to Hacker Attacks

Example in the Internet: viruses

… and to selfish behavior

Power games in shared spectrum (or between cognitive radios)

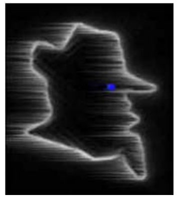
Example in the Internet: spam

Malice Vs Selfishness

- Security/crypto
  - Manichean world
  - Some parties are trusted, some not
  - Attacker's behavior is arbitrary
  - Attacker's model (e.g., Dolev-Yao)
  - Strength of the attacker
- Game theory
  - All players are selfish
  - Payoff / Utility function
  - Strategy space
  - Information
  - Agreements
  - Solution of the game
  - Mechanism design

Who is malicious? Who is selfish?

Harm everyone: viruses,…

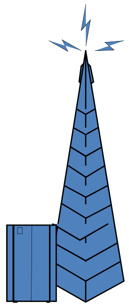


Big brother

Selective harm: DoS,…

Spammer

Cyber-gangster:
phishing attacks,
trojan horses,…



Greedy operator

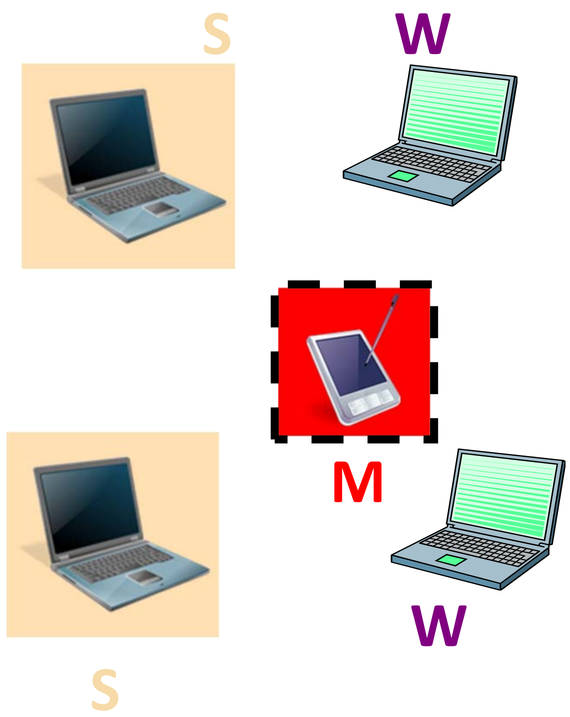
Selfish mobile station

There is no watertight boundary between malice and selfishness
➔ Both security **and** game theory approaches can be useful

Game Theory Applied to Security Problems

- Security of Physical and MAC Layers
- Anonymity and Privacy
- Intrusion Detection Systems
- Security Mechanisms
- Cryptography
- …

Security of Physical and MAC Layers



Players (Ad hoc or Infrastructure mode**):**

1. Well-behaved (W) wireless modes
2. Selfish (S) - higher access probability
3. Malicious (M) - jams other nodes (DoS)

Objective: Find the optimum strategy against M and S nodes

Reward and Cost: Throughput and Energy

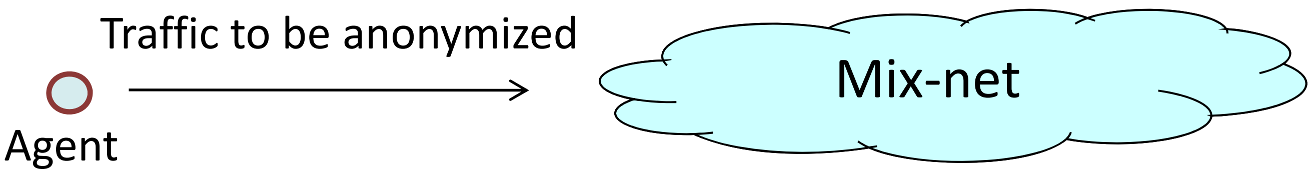
Game model: A power-controlled MAC game solved for Bayesian Nash equilibrium

Game results: Introduce Bayesian learning mechanism to update the type belief in repeated games

Optimal defense mechanisms against denial of service attacks in wireless networks

Y.E. Sagduyu, R. Berry, A. Ephremides, "**MAC games for distributed wireless network security with incomplete information of selfish and malicious user types**," GameNets 2009.

Economics of Anonymity



- Rationale: decentralized anonymity infrastructures still not in wide use today
- In the proposed model, an agent can decide to:
  - act as a simple user (sending her own traffic + possibly dummy traffic)
  - act as a node (receiving and forwarding traffic, keeping messages secret, and possibly creating dummy traffic)
  - send messages through conventional, non-anonymous channels
- Model as a repeated-game, simultaneous-move game
- Global passive adversary

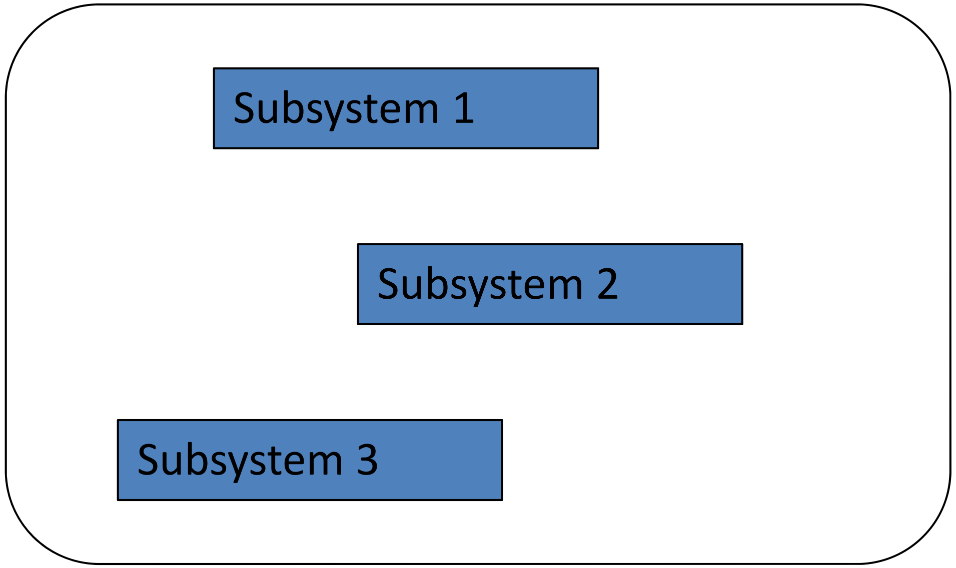
A. Acquisti, R. Dingeldine, P. Syverson. On the economics of anonymity. FC 2003

T. Ngan, R. Dingledine, D. Wallach. Building incentives into Tor. FC2010

N. Zhang et al. gPath: a game-theoretic path selection algrithm to prtect Tor's anonymity GameSec 2010

Intrusion Detection Systems

Attacker



Players: Attacker and IDS
Strategies for attacker: which subsystem(s) to attack
Strategies for defender: how to distribute the defense mechanisms
Payoff functions: based on value of subsystems + protection effort

T. Alpcan and T. Basar, “A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection”, IEEE CDC 2003

Cryptography Vs. Game Theory

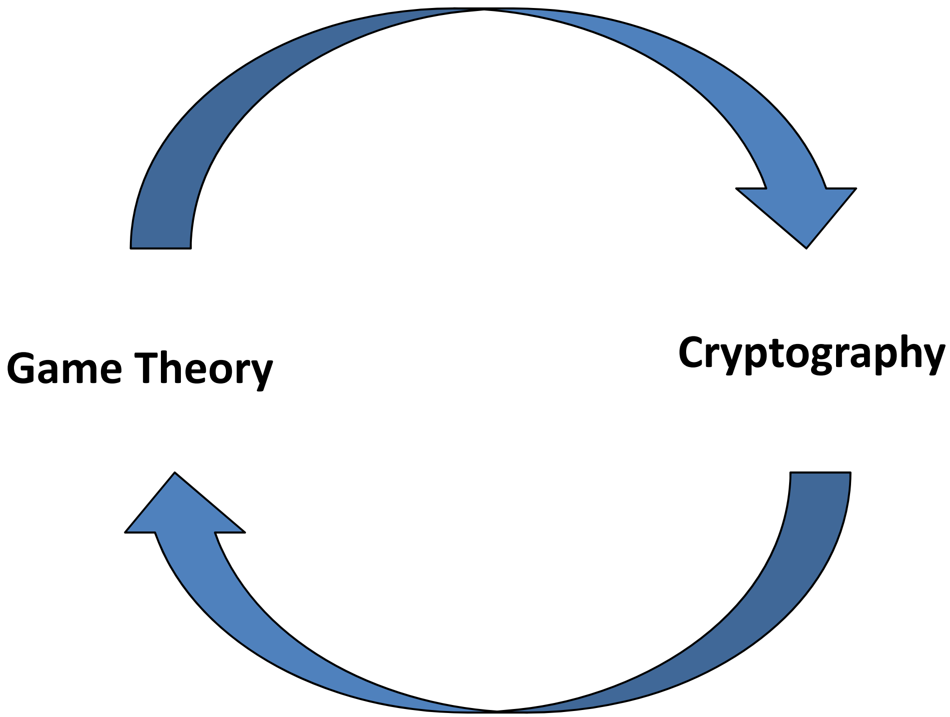
Issue	Cryptography	Game Theory
Incentive	None	Payoff
Players	Totally honest/ malicious	Always rational
Punishing cheaters	Outside the model	Central part
Solution concept	Secure protocol	Equilibrium

Y. Dodis, S. Halevi, T. Rubin. A Cryptographic Solution to a Game Theoretic Problem. Crypto 2000
See also S. Izmalkov, S. Micali, M. Lepinski. Rational Secure Computation and Ideal Mechanism Design, FOCS 2005

Crypto and Game Theory

Design crypto mechanisms with rational players

Example: Rational Secret Sharing and Multi-Party Computation
Halpern and Teague, STOC 2004

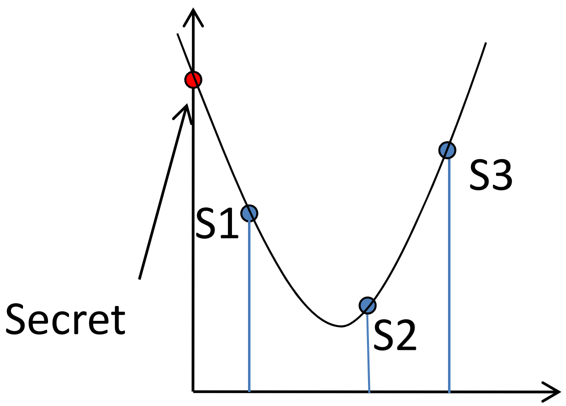


Implement GT mechanisms in a distributed fashion
Example: Mediator (in *correlated equilibria*)
Dodis et al., Crypto 2000

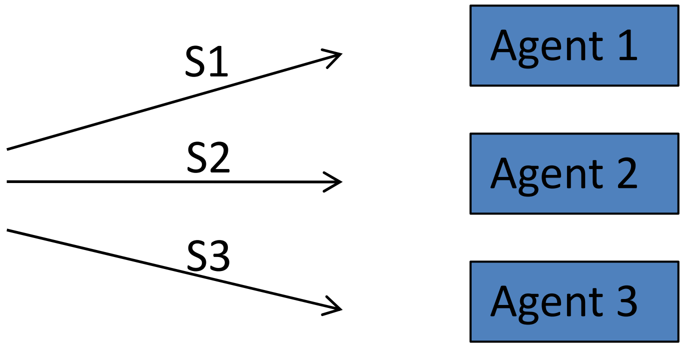
Design of Cryptographic Mechanisms with Rational Players: Secret Sharing

Reminder on secret sharing

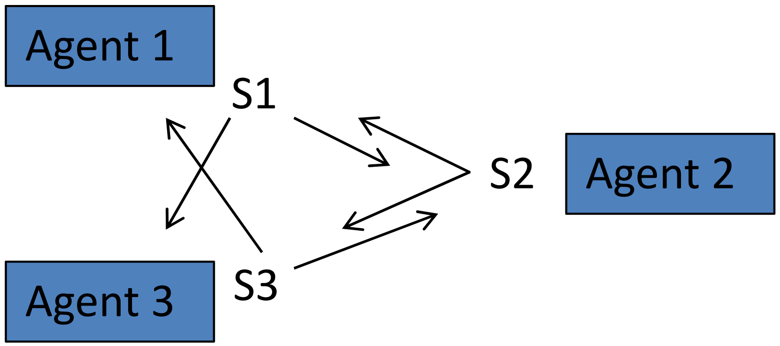
a. Share issuer



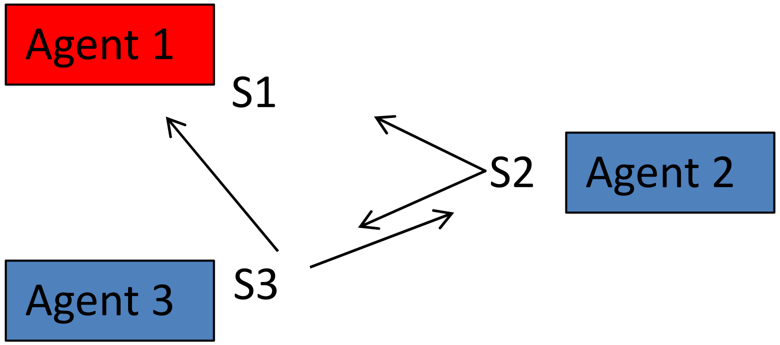
b. Share distribution



c. Secret reconstruction



The Temptation of Selfishness in Secret Sharing



- Agent 1 can reconstruct the secret
- Neither Agent 2 nor Agent 3 can

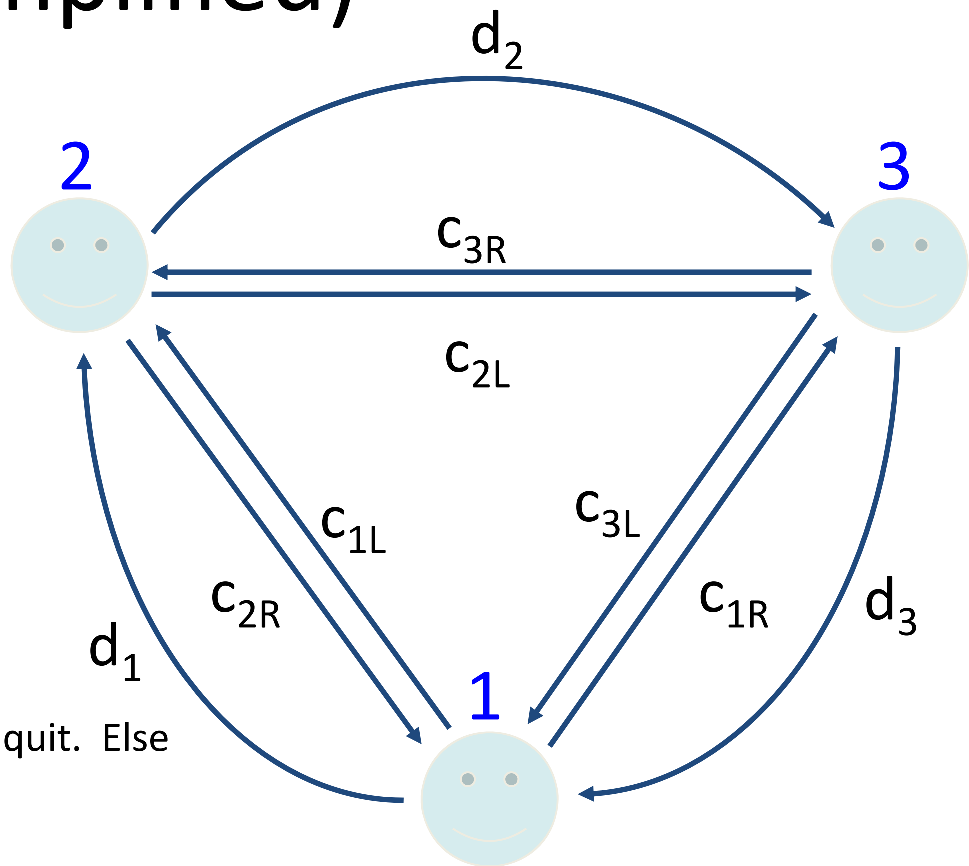
- Model as a game:
  - Player = agent
  - Strategy: To deliver or not one's share (depending on what the other players did)
  - Payoff function:
    - a player prefers getting the secret
    - a player prefers fewer of the other get it

- Impossibility result: there is no simple mechanism that would prevent this
  ➔ Proposed solution: *randomized* mechanism

Randomized Protocol (for 3, simplified)

Protocol for agent 1:

1. Toss coin b1
2. Toss coin c1L
3. Set c1R = b1 ⊕ c1L
4. Send c1L left, c1R right
5. Send d1 = b1 ⊕ c3L left
6. Compute b1⊕b2⊕b3 = b1⊕c2R⊕d3
7. If b1=b1⊕b2⊕b3 = 1, send share.
8. If received shares or detected cheating, quit. Else restart protocol with new share.



Main result: a rational agent will follow the protocol

Courtesy J. Halpern and V. Teague

J. Halpern and V. Teague. Rational Secret Sharing and Multi-Party Computation. STOC 2004

Improving Nash Equilibria (1/2)

		Player 2: Chicken	Player 2: Dare
Player 1	Chicken	4, 4	1, 5
	Dare	5, 1	0, 0

3 Nash equilibria: (D, C), (C, D), (½ D + ½ C, ½ C+ ½ D)

Payoffs: [5, 1] [1, 5] [5/2, 5/2]

The payoff [4, 4] cannot be achieved without a binding contract, because it is not an equilibrium

Possible improvement 1: communication

Toss a fair coin → if Head, play (C, D); if Tail, play (D, C) → average payoff = [3, 3]

Y. Dodis, S. Halevi, and T. Rabin. A Cryptographic solution to a game theoretic problem, Crypto 2000

Improving Nash Equilibria (2/2)

Player 2

Player 1		Chicken	Dare
	Chicken	4, 4	1, 5
	Dare	5, 1	0, 0

Possible improvement 2: Mediator

Introduce an objective chance mechanism: choose V1, V2, or V3 with probability 1/3 each. Then:

- Player 1 is told whether or not V1 was chosen *and nothing else*
- Player 2 is told whether or not V3 was chosen *and nothing else*

If informed that V1 was chosen, Player 1 plays D, otherwise C
If informed that V3 was chosen, Player 2 plays D, otherwise C
→This is a *correlated equilibrium*, with payoff [3 1/3, 3 1/3]
→ It assigns probability 1/3 to (C, C), (C, D), and (D, C) and 0 to (D, D)

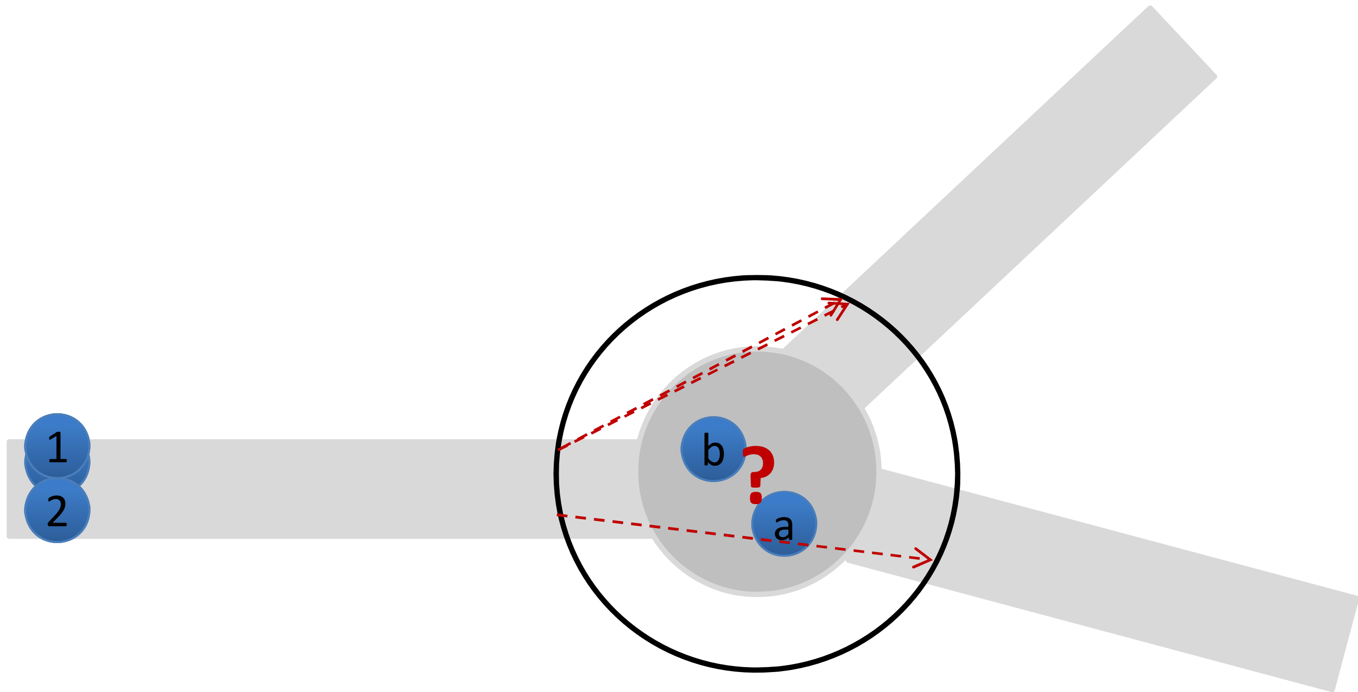
How to **replace the mediator by a crypto protocol**: see Dodis et al.

An Example of Security (or rather, Privacy) Mechanism Modeled by Game Theory:

Cooperative Change of Pseudonyms in Mix Zones

J. Freudiger, H. Manshaei, JP Hubaux, D. Parkes
On Non-Cooperative Location Privacy: A Game-Theoretic Analysis

Location Privacy with Mix Zones



Mix zone

“Costs” generated by Mix Zones

- Turn off transceiver

+

- Routing is difficult

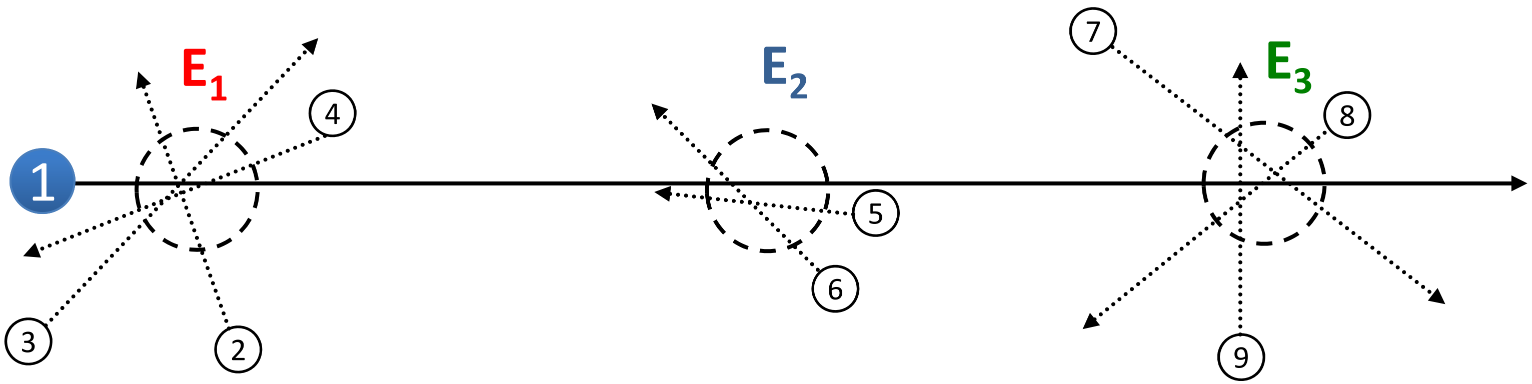
+

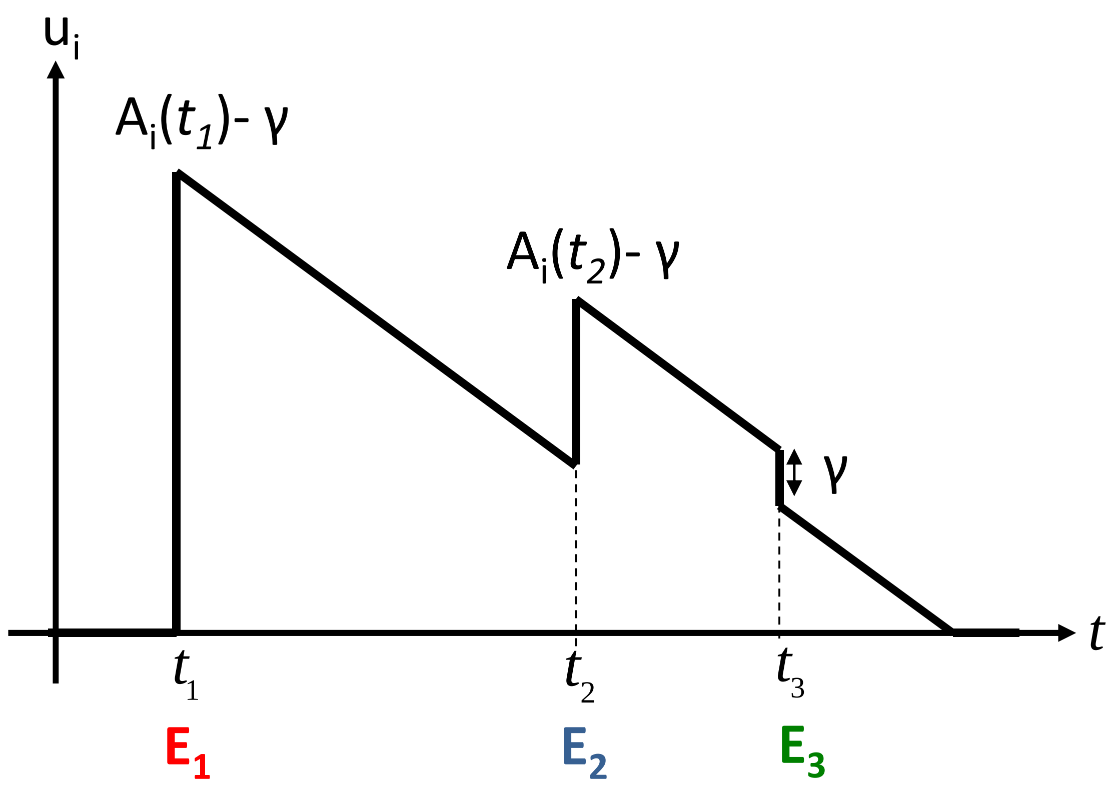
- Load authenticated pseudonyms

=

γ

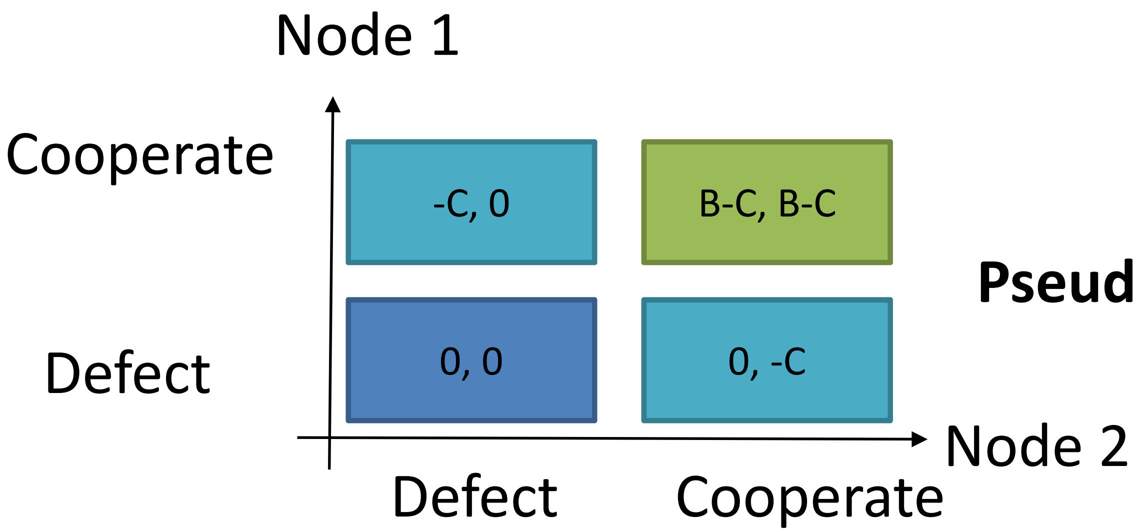
Sequence of Pseudonym Change Games





Non-Cooperative Behavior

- Benefit **B** of mix zone:
  - Location Privacy
- Cost **C** of mix zone :
  - Mobiles must remain silent
  - Mobiles must change their identifier
- Strategies
  - **Cooperate**: Change identifier in the mix zone
  - **Defect**: Do not change
  - Depend on current level of location privacy of nodes



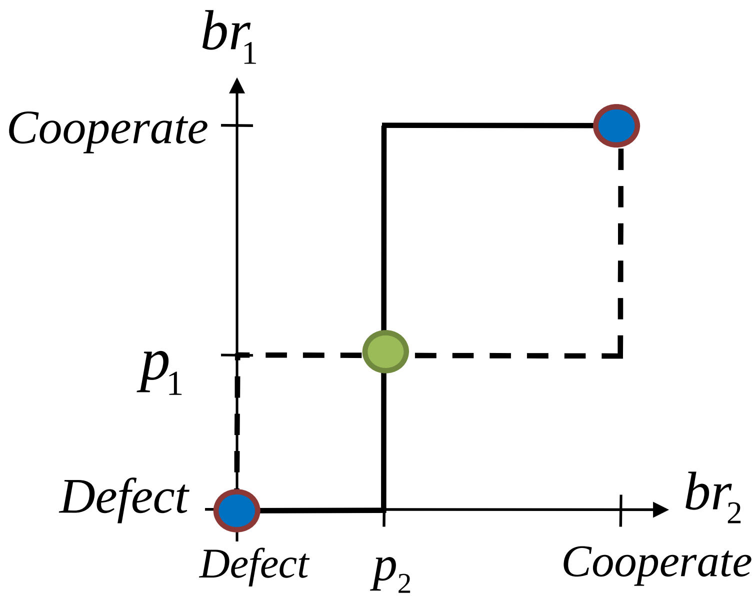
Pseudonym Change Game

Nash Equilibria

Theorem:

The pseudonym change game with complete information has 2 pure strategy Nash equilibria and 1 mixed-strategy Nash equilibrium.

➔ Cooperation cannot be taken for granted



p_i = Pr(node i cooperates)

= pure NE

= mixed NE

- The pseudonym change game is a **coordination game**
  - Mutual gain by making mutually consistent decisions

Overall Conclusion

- Upcoming (wireless) networks bring formidable challenges in terms of malicious and selfish behaviors (including at the physical layer)
- Game theoretic modeling of security mechanisms can help predicting and influencing (by mechanism design) the behavior of the involved parties
- A **lot of work** still needs to be accomplished to establish the credibility of such approaches

http://lca.epfl.ch/gamesec

H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, JP Hubaux
Game Theory Meets Network Security and Privacy
EPFL Tech Report 151965 , Sept. 2010