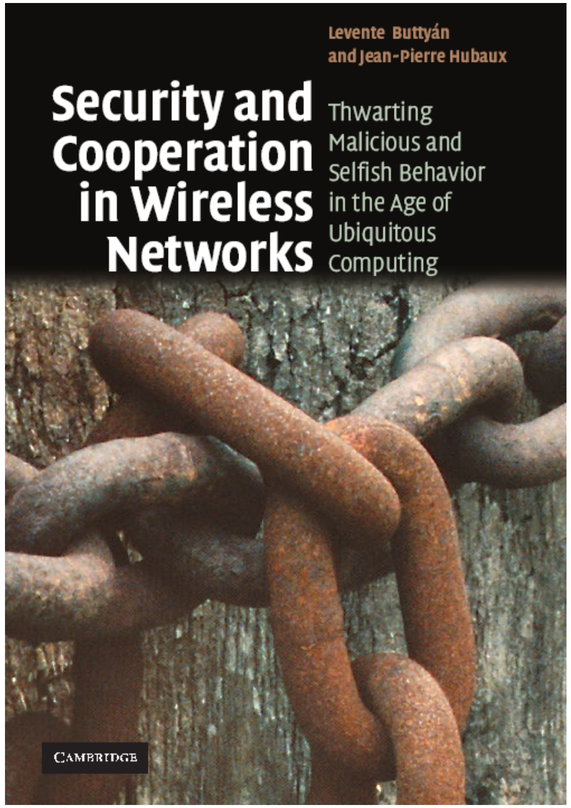
Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com



Security and Cooperation in Wireless Networks

TEXTBOOK REVIEW

http://secowinet.epfl.ch

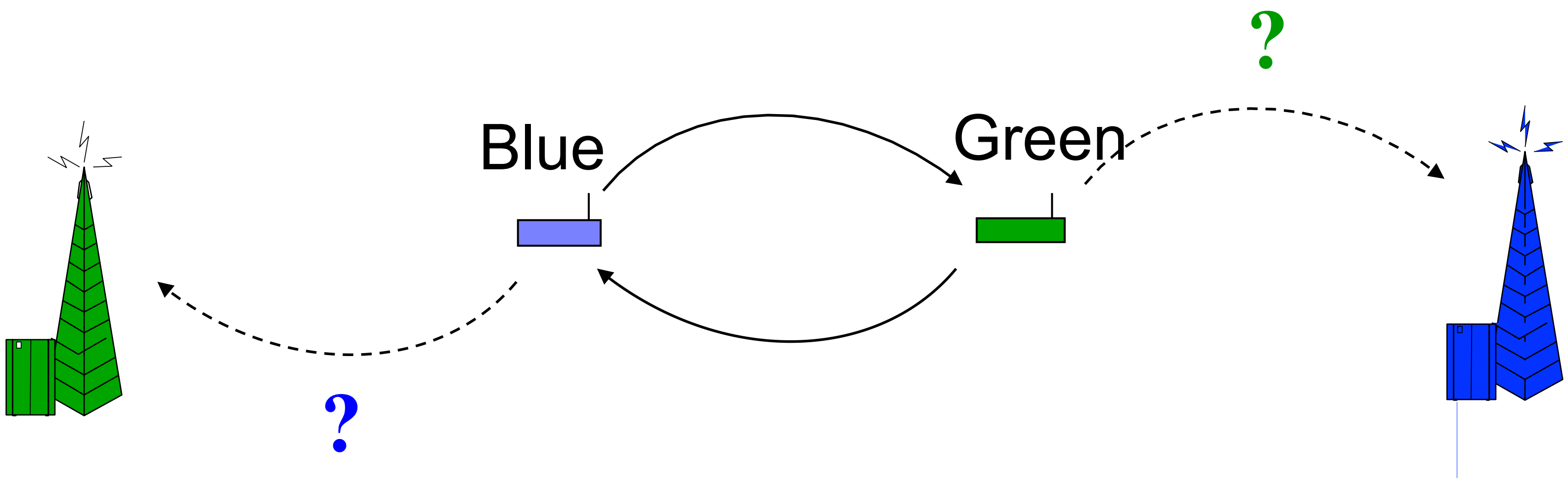
Security and Cooperation in Wireless Networks

1. Introduction
2. Thwarting **malice**: security mechanisms
    2.1 Naming and addressing
    2.2 Establishment of security associations
    2.3 Secure neighbor discovery
    2.4 Secure routing in multi-hop wireless networks
    2.5 Privacy protection
    2.6 Secure positioning
3. Thwarting **selfishness**: behavior enforcement
    3.0 Brief introduction to game theory
    3.1 Enforcing fair bandwidth sharing at the MAC layer
    3.2 Enforcing packet forwarding
    3.3 Wireless operators in a shared spectrum
    3.4 Secure protocols for behavior enforcement

3.0 Brief introduction to Game Theory

- Discipline aiming at modeling situations in which actors have to make decisions which have mutual, **possibly conflicting**, consequences
- Classical applications: **economics**, but also politics and biology
- Example: should a company invest in a new plant, or enter a new market, considering that the **competition** *could* make similar moves?
- Most widespread kind of game: **non-cooperative** (meaning that the players do not attempt to find an agreement about their possible moves)

Example 1:
The Forwarder’s Dilemma



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 << 1)
- ***Strategic-form*** representation

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

Solving the Forwarder's Dilemma (1/2)

Strict dominance: strictly best strategy, for any strategy of the other player(s)

Strategy s_i strictly dominates if

$$u_i(s_i', s_{-i}) < u_i(s_i, s_{-i}), \forall s_{-i} \in S_{-i}, \forall s_i' \in S_i$$

where: $u_i \in U$ utility function of player *i*

$s_{-i} \in S_{-i}$ strategies of all players except player i

In Example 1, strategy Drop ***strictly dominates*** strategy Forward

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

Solving the Forwarder's Dilemma (2/2)

Solution by iterative strict dominance:

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

BUT

Drop ***strictly dominates*** Forward

Forward would result in a ***better outcome***

} Dilemma

Nash equilibrium

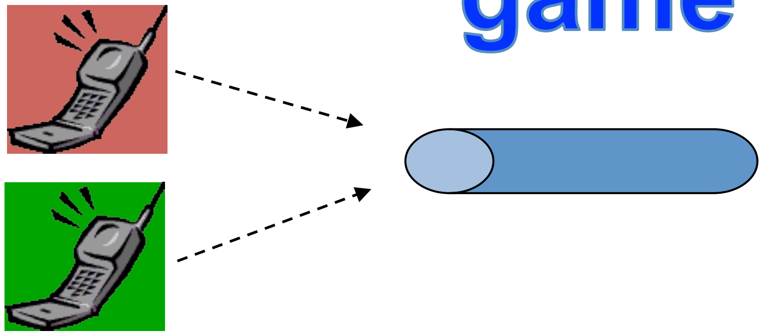
Nash Equilibrium: no player can increase his utility by deviating unilaterally

The Forwarder's Dilemma

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

(Drop, Drop) is the **only** Nash equilibrium of this game

Example 2: The Multiple Access game



Time-division channel

Reward for successful transmission: 1

Cost of transmission: c
(0 < c << 1)

Blue \ Green	Quiet	Transmit
Quiet	(0, 0)	(0, 1-c)
Transmit	(1-c, 0)	(-c, -c)

There is no strictly dominating strategy

There are two Nash equilibria

More on game theory

Pareto-optimality
A strategy profile is Pareto-optimal if the payoff of a player cannot be increased without decreasing the payoff of another player

Properties of Nash equilibria to be investigated:

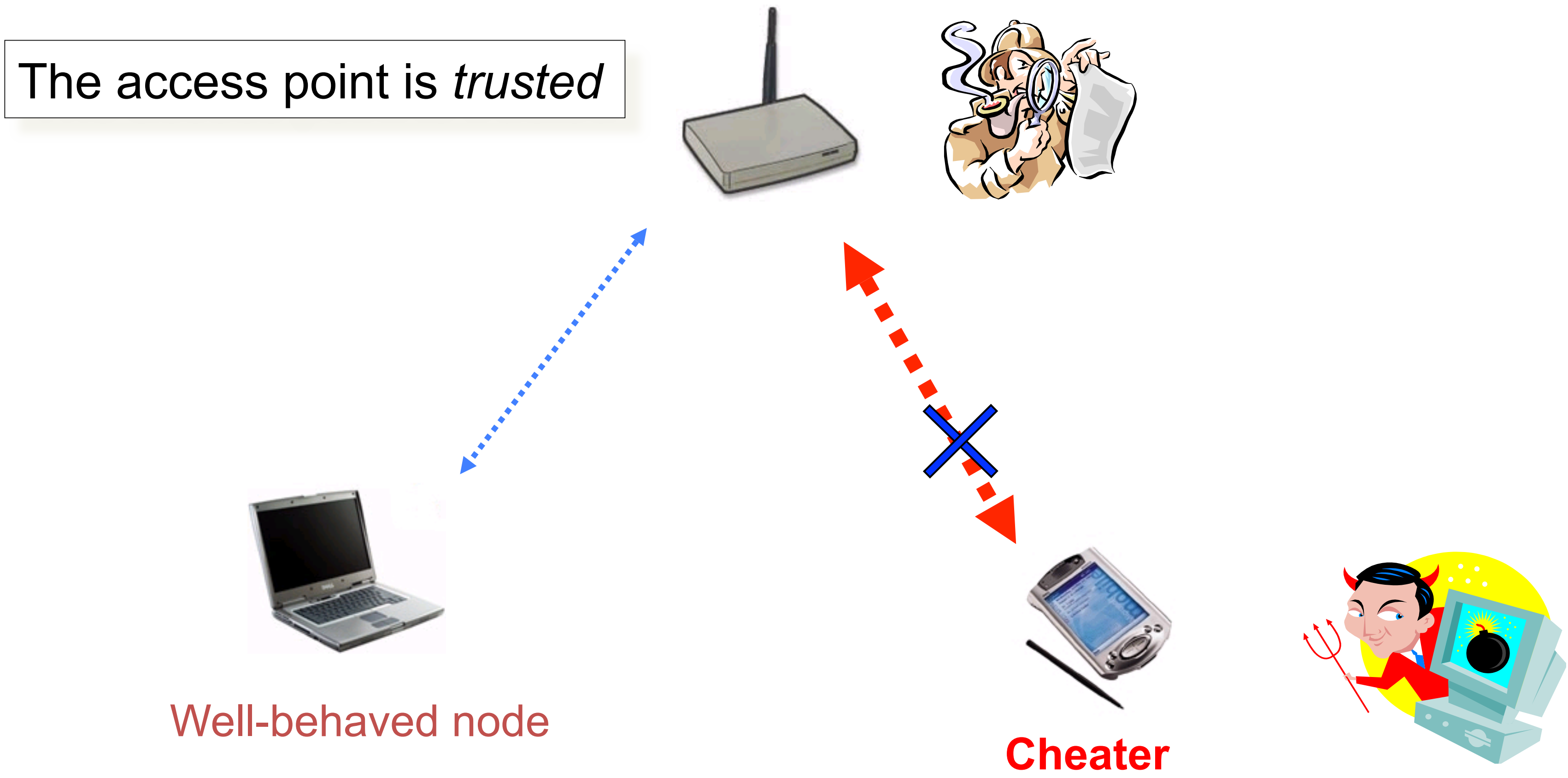
- uniqueness
- efficiency (Pareto-optimality)
- emergence (dynamic games, agreements)

Promising area of application in wireless networks: **cognitive radios, Social Networks,**

Security and Cooperation in Wireless Networks

1. Introduction
2. Thwarting **malice**: security mechanisms
   - 2.1 Naming and addressing
   - 2.2 Establishment of security associations
   - 2.3 Secure neighbor discovery
   - 2.4 Secure routing in multi-hop wireless networks
   - 2.5 Privacy protection
   - 2.6 Secure positioning
3. Thwarting **selfishness**: behavior enforcement
   - 3.0 Brief introduction to game theory
   - 3.1 Enforcing fair bandwidth sharing at the MAC layer
   - 3.2 Enforcing packet forwarding
   - 3.3 Wireless operators in a shared spectrum
   - 3.4 Secure protocols for behavior enforcement

3.1 Enforcing fair bandwidth sharing at the MAC layer

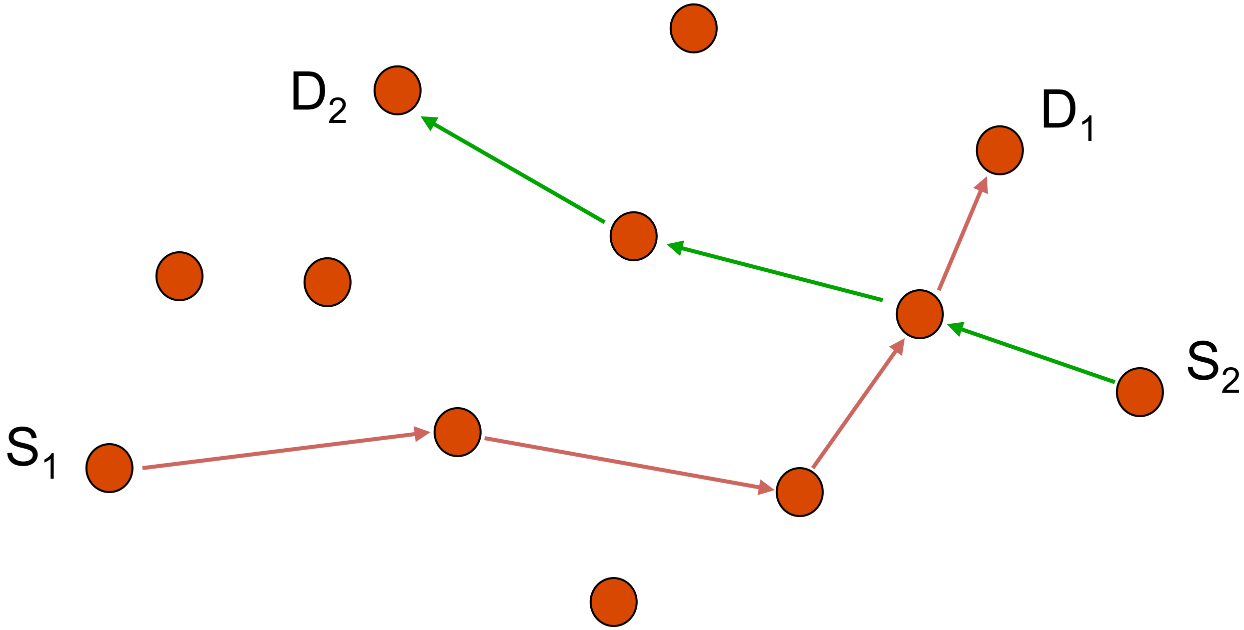


- Kyasanur and Vaidya, *DSN 2003*
- http://domino.epfl.ch
- Cagalj et al., *Infocom 2005* (game theory model for CSMA/CA ad hoc networks)

Security and Cooperation in Wireless Networks

1. Introduction
2. Thwarting **malice**: security mechanisms
    - 2.1 Naming and addressing
    - 2.2 Establishment of security associations
    - 2.3 Secure neighbor discovery
    - 2.4 Secure routing in multi-hop wireless networks
    - 2.5 Privacy protection
    - 2.6 Secure positioning
3. Thwarting **selfishness**: behavior enforcement
    - 3.0 Brief introduction to game theory
    - 3.1 Enforcing fair bandwidth sharing at the MAC layer
    - 3.2 Enforcing packet forwarding
    - 3.3 Wireless operators in a shared spectrum
    - 3.4 Secure protocols for behavior enforcement

3.2 Enforcing packet forwarding

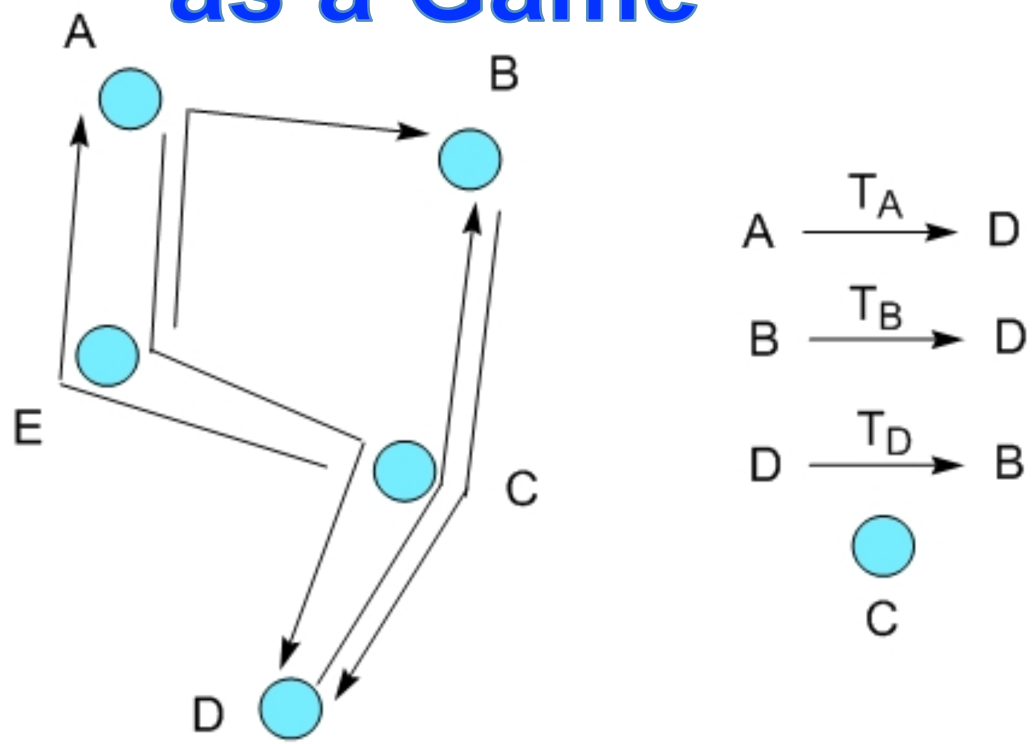


Usually, the devices are assumed to be cooperative.
But what if they are not, and there is no incentive to cooperate?

- V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao, Infocom 2003, IEEE TWC 2005
- M. Felegyhazi, JP Hubaux, and L. Buttyan, Personal Wireless Comm. Workshop 2003, IEEE TMC 2006

Modeling Packet Forwarding as a Game

Player: node



Strategy: cooperation level

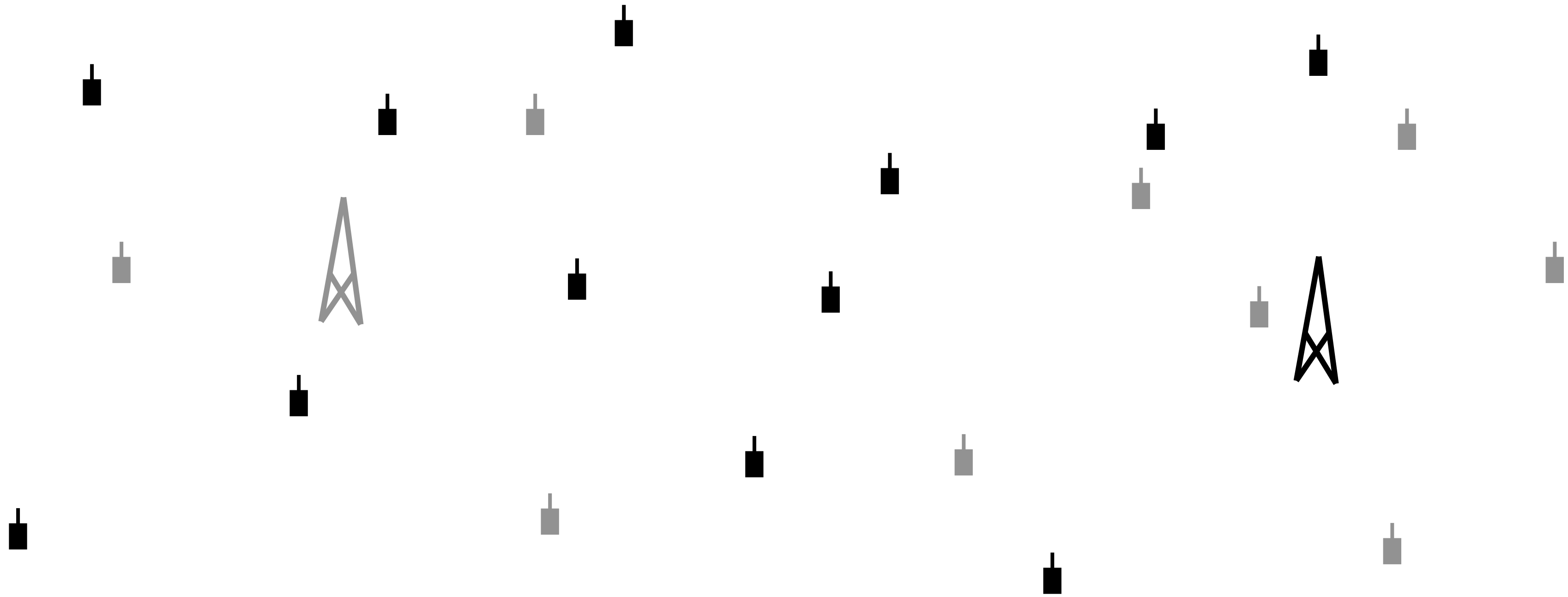
Payoff of node i: proportion of packets sent by node i reaching their destination

Security and Cooperation in Wireless Networks

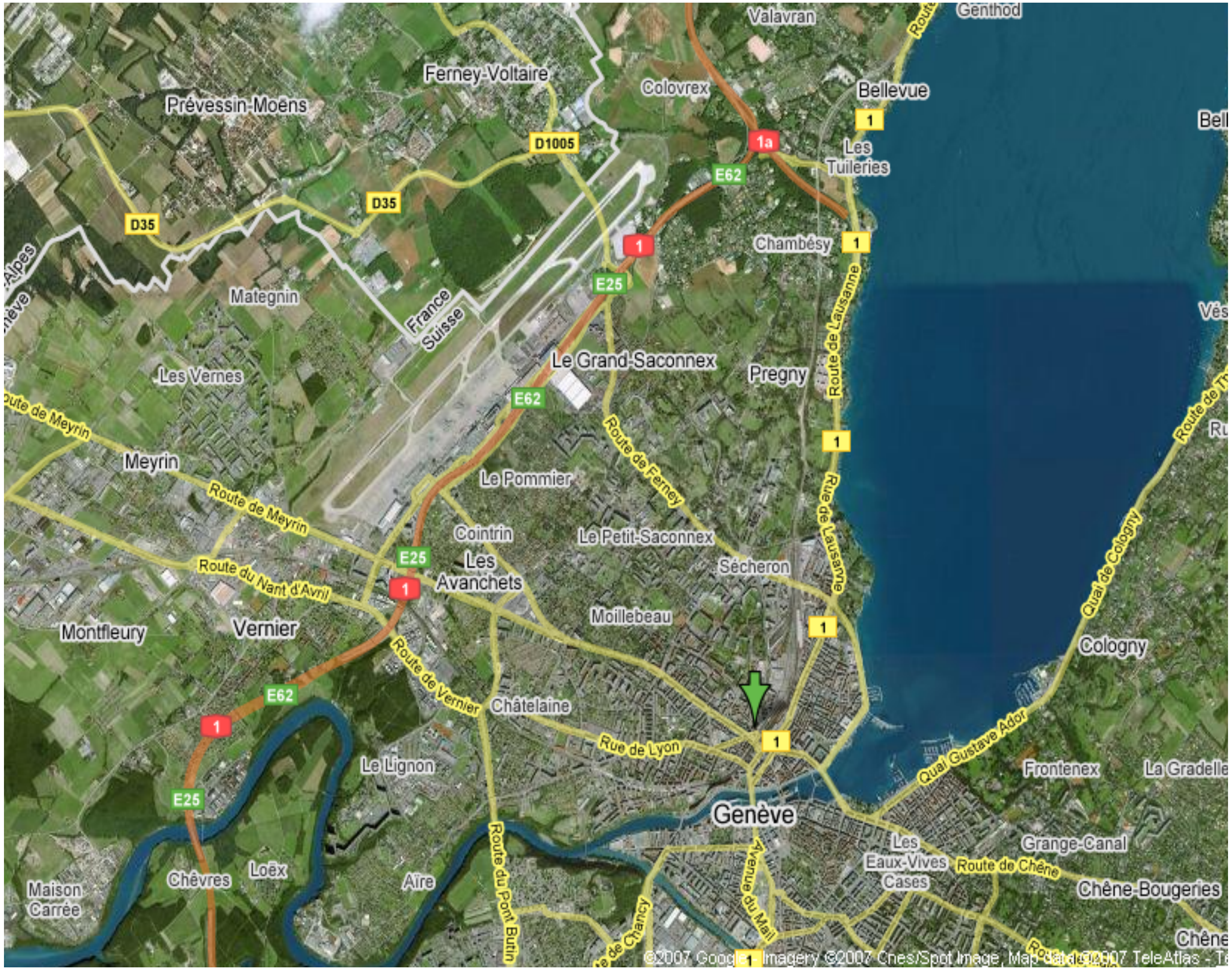
1. Introduction
2. Thwarting **malice**: security mechanisms
    - 2.1 Naming and addressing
    - 2.2 Establishment of security associations
    - 2.3 Secure neighbor discovery
    - 2.4 Secure routing in multi-hop wireless networks
    - 2.5 Privacy protection
    - 2.6 Secure positioning
3. Thwarting **selfishness**: behavior enforcement
    - 3.0 Brief introduction to game theory
    - 3.1 Enforcing fair bandwidth sharing at the MAC layer
    - 3.2 Enforcing packet forwarding
    - 3.3 Wireless operators in a shared spectrum
    - 3.4 Secure protocols for behavior enforcement

3.3 Games between wireless operators Multi-domain sensor networks

- **Typical cooperation:** help in packet forwarding
- Can cooperation emerge spontaneously in multi-domain sensor networks based solely on the self-interest of the sensor operators?

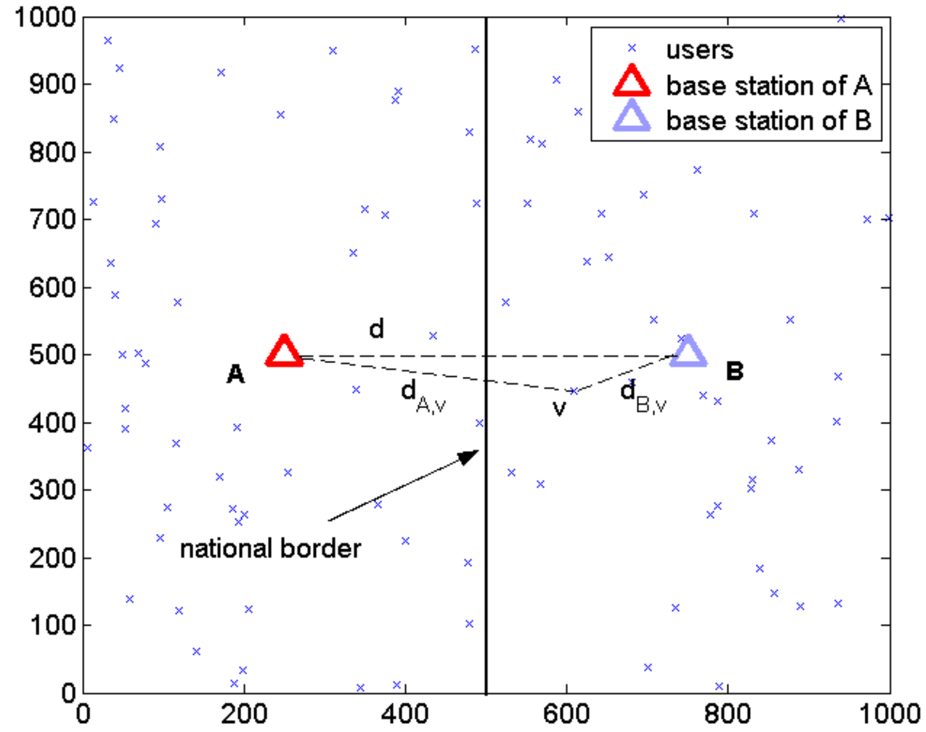


3.3 Border games of cellular operators (1/3)



3.3 Border games of cellular operators (2/3)

- Two CDMA operators: A and B
- Adjust the pilot signals
- Power control game (no power cost):
  - players = operators
  - strategies = pilot powers
  - payoffs = attracted users (best SINR)



Signal-to-interference-plus-noise ratio

$$SINR_{Av}^{pilot} = \frac{G_p^{pilot} \cdot P_A \cdot d_{Av}^{-\alpha}}{N_0 \cdot W + I_{own}^{pilot} + I_{other}^{pilot}}$$

Own-cell interference

$$I_{own}^{pilot} = \varsigma \cdot d_{Av}^{-\alpha} \left(\sum_{w \in M_A} T_{Aw} \right)$$

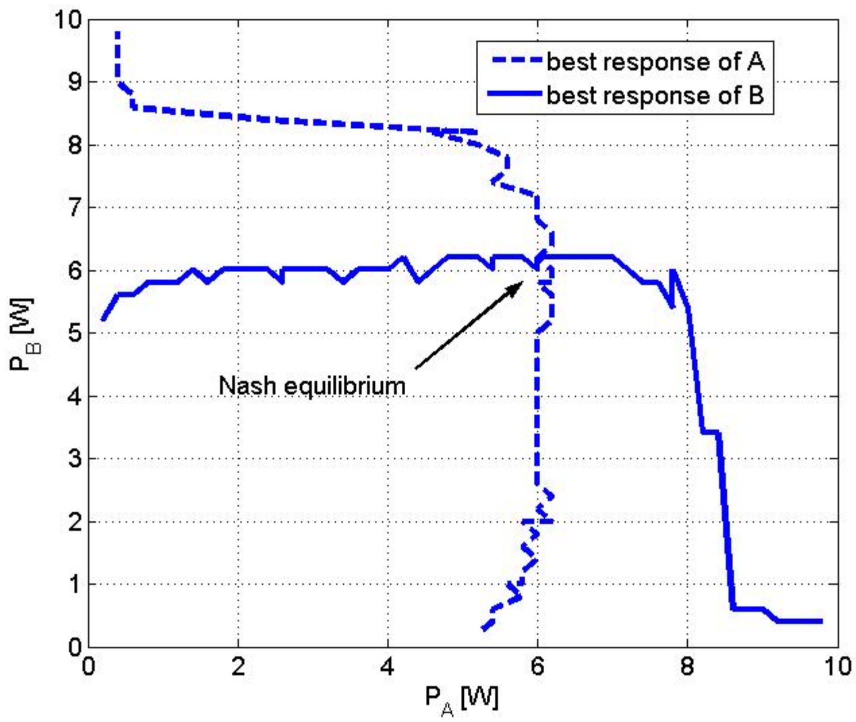
Other-to-own-cell interference

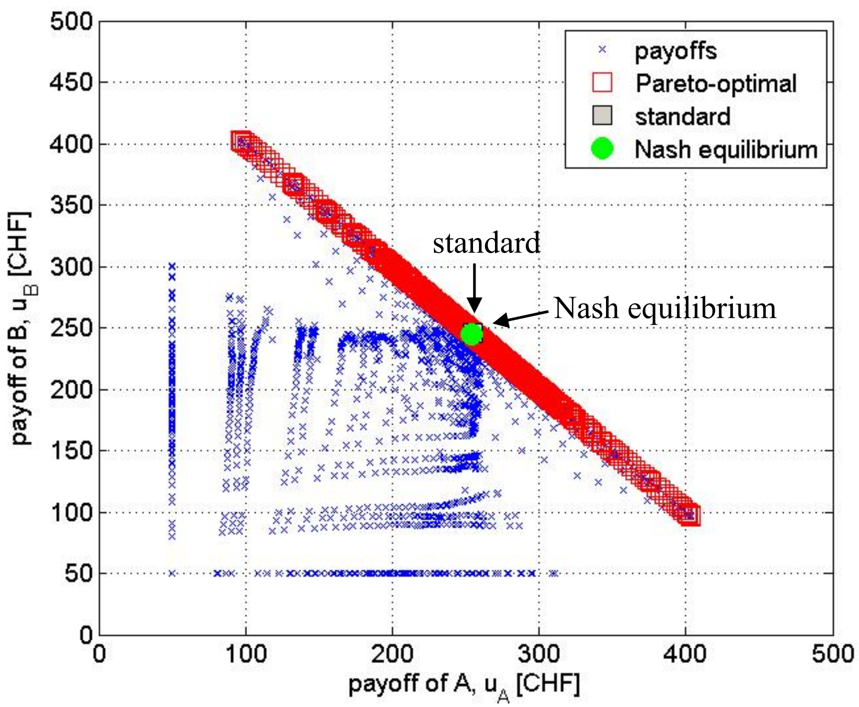
$$I_{other}^{pilot} = \eta \cdot d_{Bv}^{-\alpha} \left(P_B + \sum_{w \in M_B} T_{Bw} \right)$$

where:
- G_p^{pilot} – pilot processing gain
- P_A^p – pilot signal power of BS A
- $d_{Av}^{-\alpha}$ – path loss between A and v
- ς – own-cell interference factor
- η – other-to-own-cell interference factor
- T_{Aw} – traffic signal power assigned to w by BS A
- M_A – set of users attached to BS A

3.3 Border games of cellular operators (3/3)

- Unique and Pareto-optimal Nash equilibrium
- Higher pilot power than in the standard $P^s = 2W$
- 10 users in total





Extended game with power costs = Prisoner's Dilemma

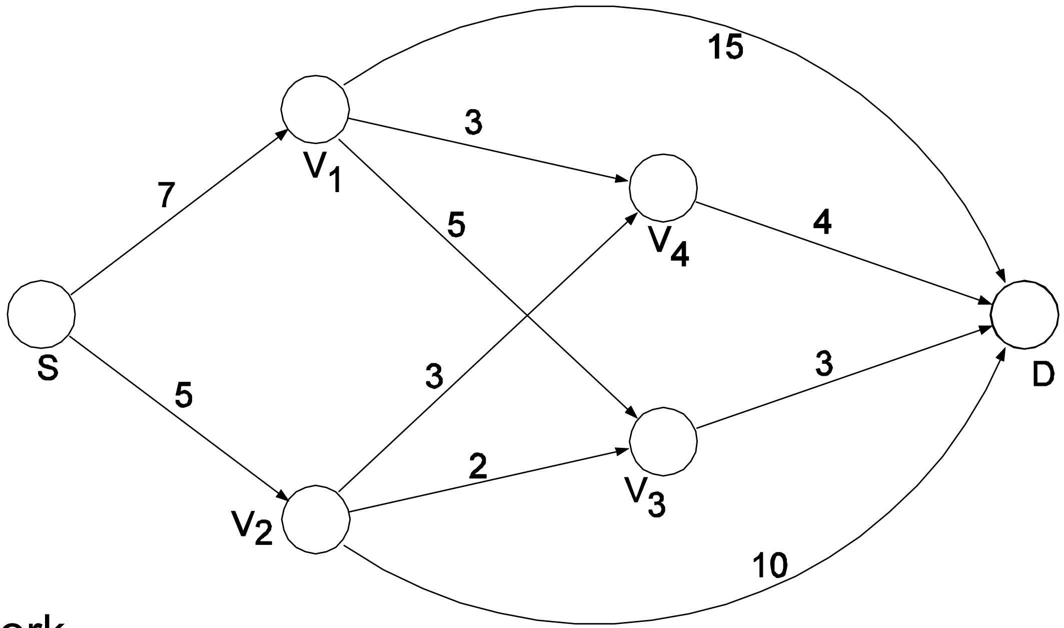
		Player B	
		P^s	P_B^*
Player A	P^s	U, U	$U-\Delta, U+\Delta-C^*$
	P_A^*	$U+\Delta-C^*, U-\Delta$	$U-C^*, U-C^*$

where:

U – fair payoff (half of the users)
Δ – payoff difference by selfish behavior
C* - cost for higher pilot power

Security and Cooperation in Wireless Networks

3.4 Secure protocols for behavior enforcement



- Self-organized ad hoc network
- Investigation of both routing and packet forwarding

S. Zhong, L. E. Li, Y. G. Liu, and Y. R. Yang.
On designing incentive-compatible routing and forwarding protocols in wireless ad hoc networks – an integrated approach using game theoretical and cryptographic techniques
Mobicom 2005

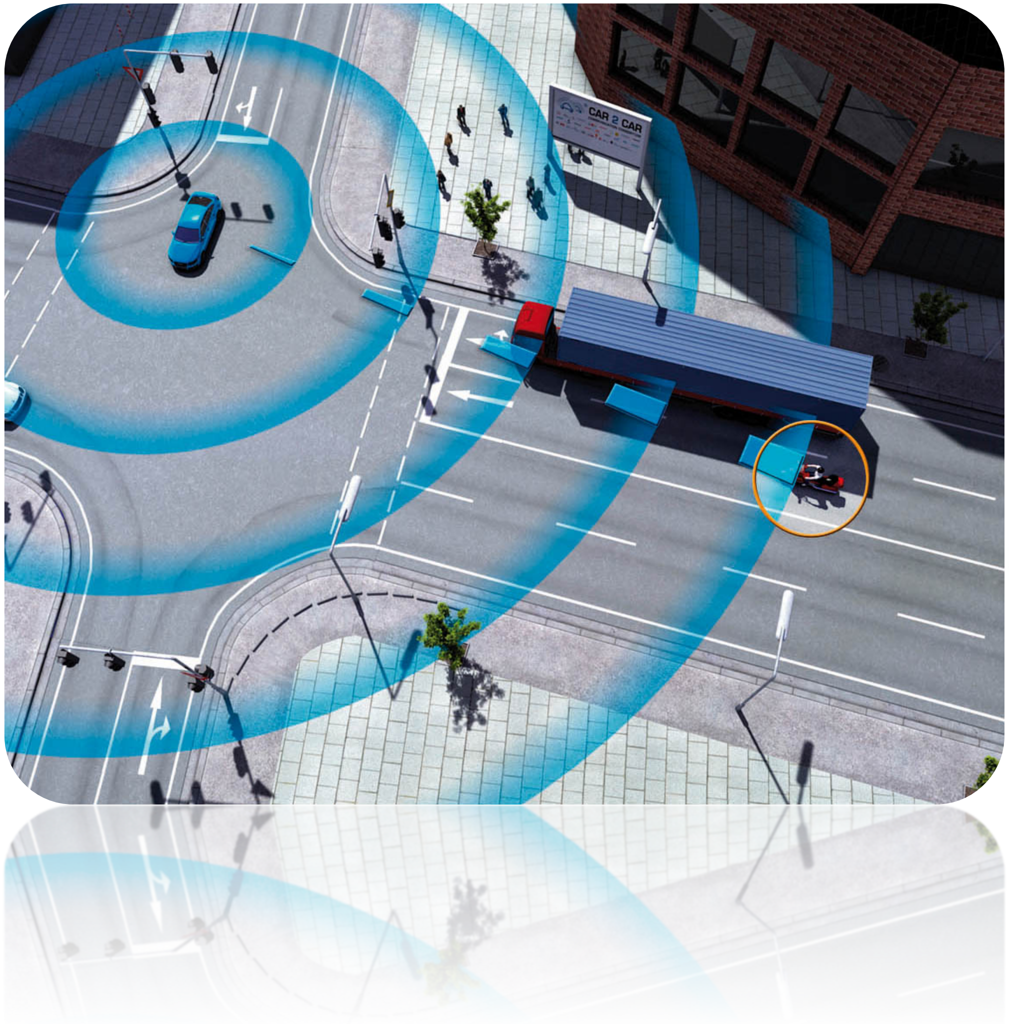
On Non-Cooperative Location Privacy: A Game-theoretic Analysis

Julien Freudiger, Mohammad Hossein Manshaei,
Jean-Pierre Hubaux, and David C. Parkes

CCS 2009

Pervasive Wireless Networks

Vehicular networks



Mobile Social networks

Human sensors

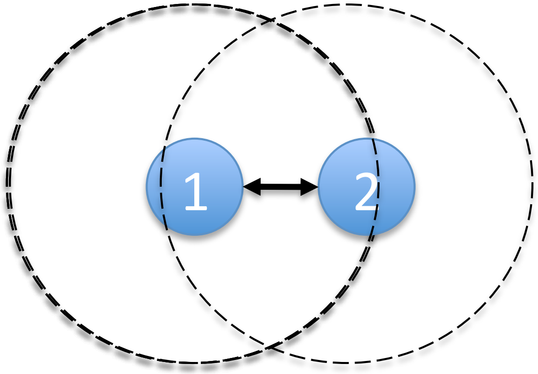
Personal WiFi bubble

New Context-Based Applications

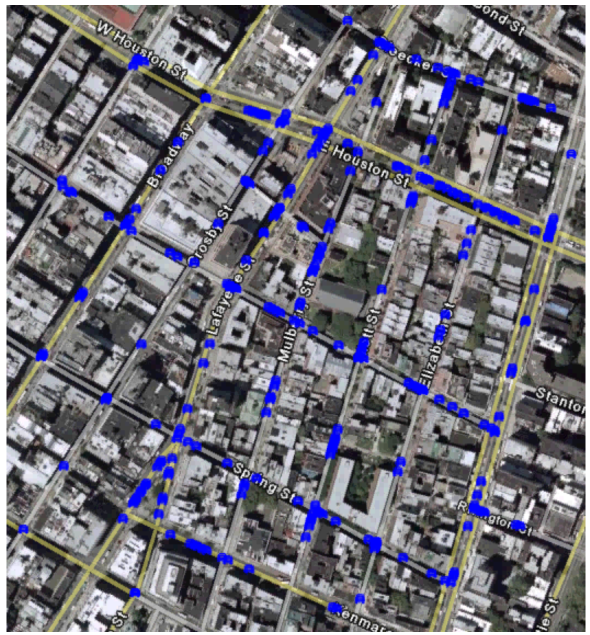
- Search for local services
- Connect with friends and strangers
  - Bluedating, bluelocator, bluetella
  - Aka-Aki
  - Friend finder
- Improve urban mobility
  - Vehicular Networks

Need for Peer-to-Peer Communications

WiFi/Bluetooth enabled

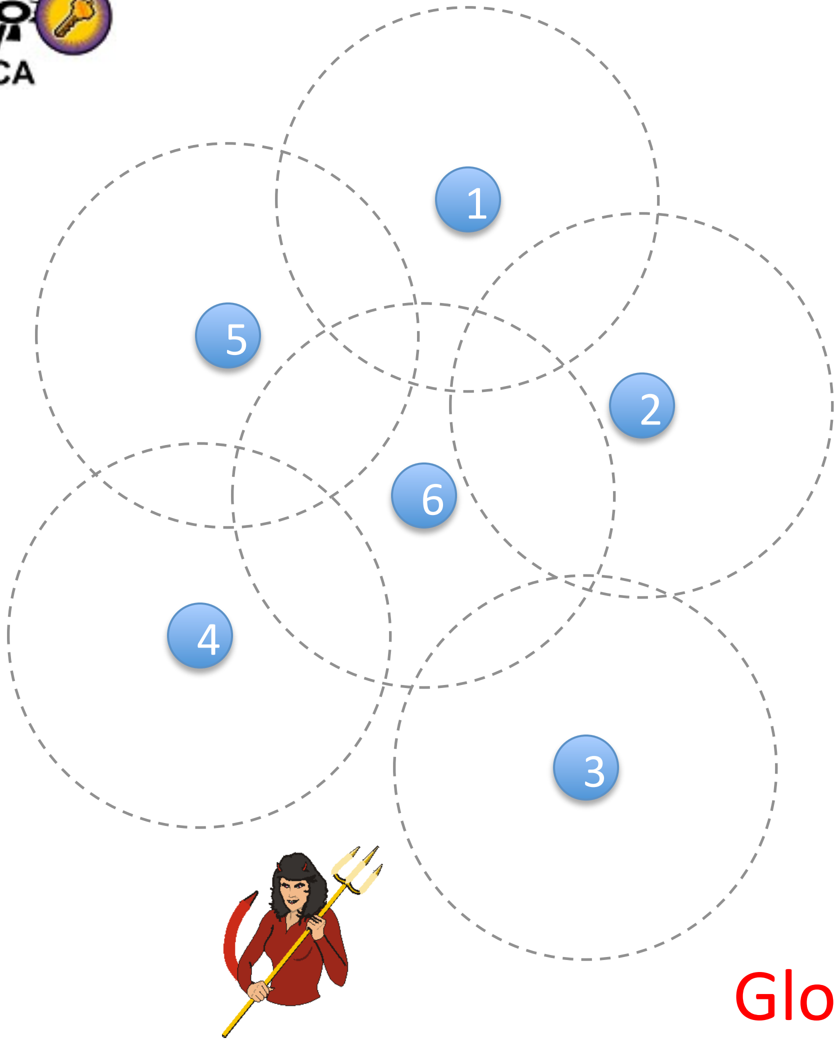


Identifier	Message



Identifier = Pseudonym

System and Threat Model



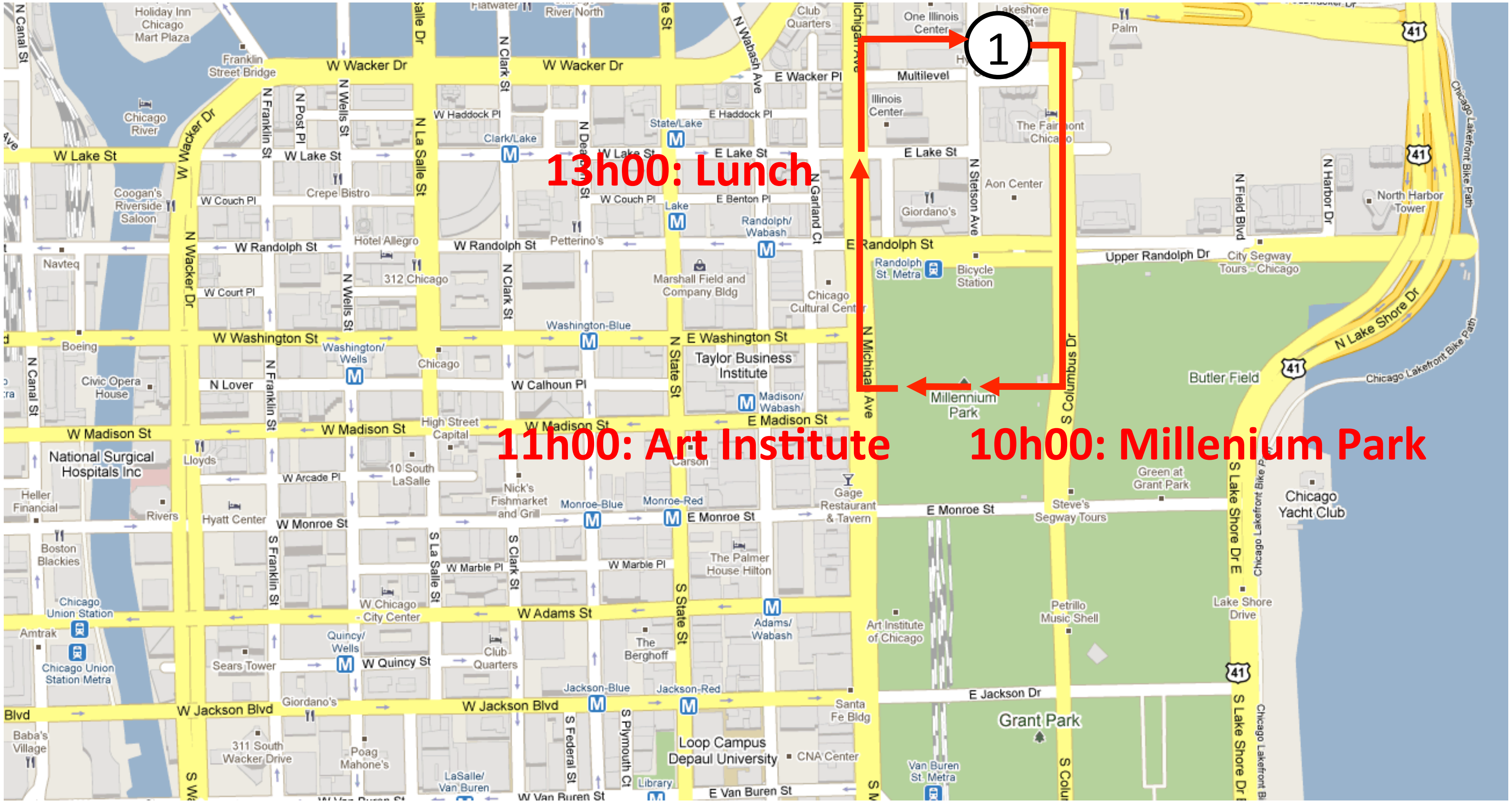
- N mobile nodes
- WiFi/Bluetooth enabled
- Beacons

- Offline CA to provide pseudonyms

Global passive eavesdropper
tracks location of mobile nodes

Location Privacy Problem

Passive adversary monitors identifiers used in peer-to-peer communications



Previous Work

Message

- Pseudonymity is not enough for location privacy [1, 2]
- Removing pseudonyms is not enough as well [3]

Spatio-Temporal correlation of traces

[1] P. Golle and K. Partridge. **On the Anonymity of Home/Work Location Pairs**. Pervasive Computing, 2009

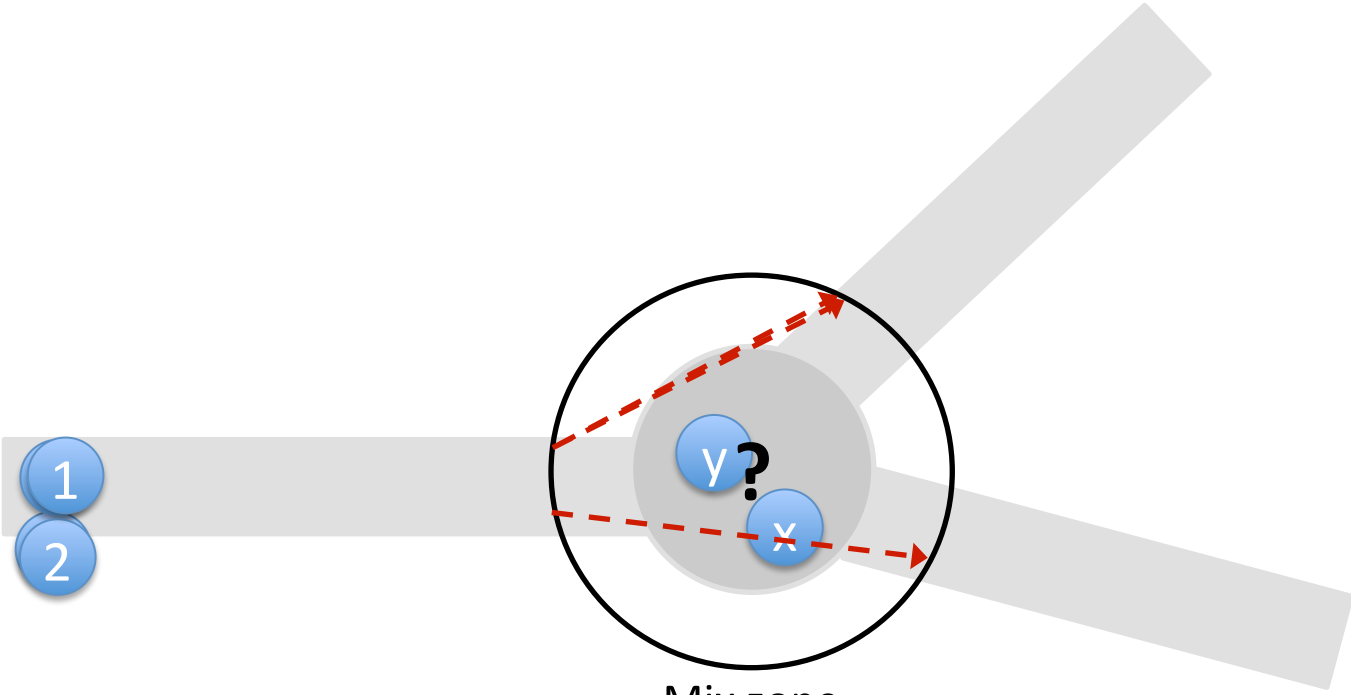
[2] B. Hoh et al. **Enhancing Security & Privacy in Traffic Monitoring Systems**. Pervasive Computing, 2006

[3] B. Hoh and M. Gruteser. **Protecting location privacy through path confusion**. SECURECOMM, 2005

Location Privacy with Mix Zones

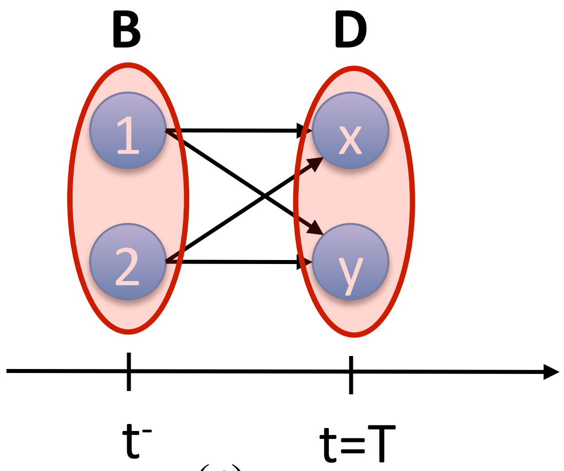
Spatial decorrelation: Remain silent

Temporal decorrelation: Change pseudonym



[1] A. Beresford and F. Stajano. **Mix Zones: user privacy in location aware services**. Percom, 2004

Mix Zone Privacy Gain



$$A_i(T) = -\sum_{d=1}^{n(t)} p_{d|b} \log_2(p_{d|b})$$

$n(t)$ Number of nodes in mix zone

Cost caused by Mix Zones

- Turn off transceiver

+

- Routing is difficult

+

- Load authenticated pseudonyms

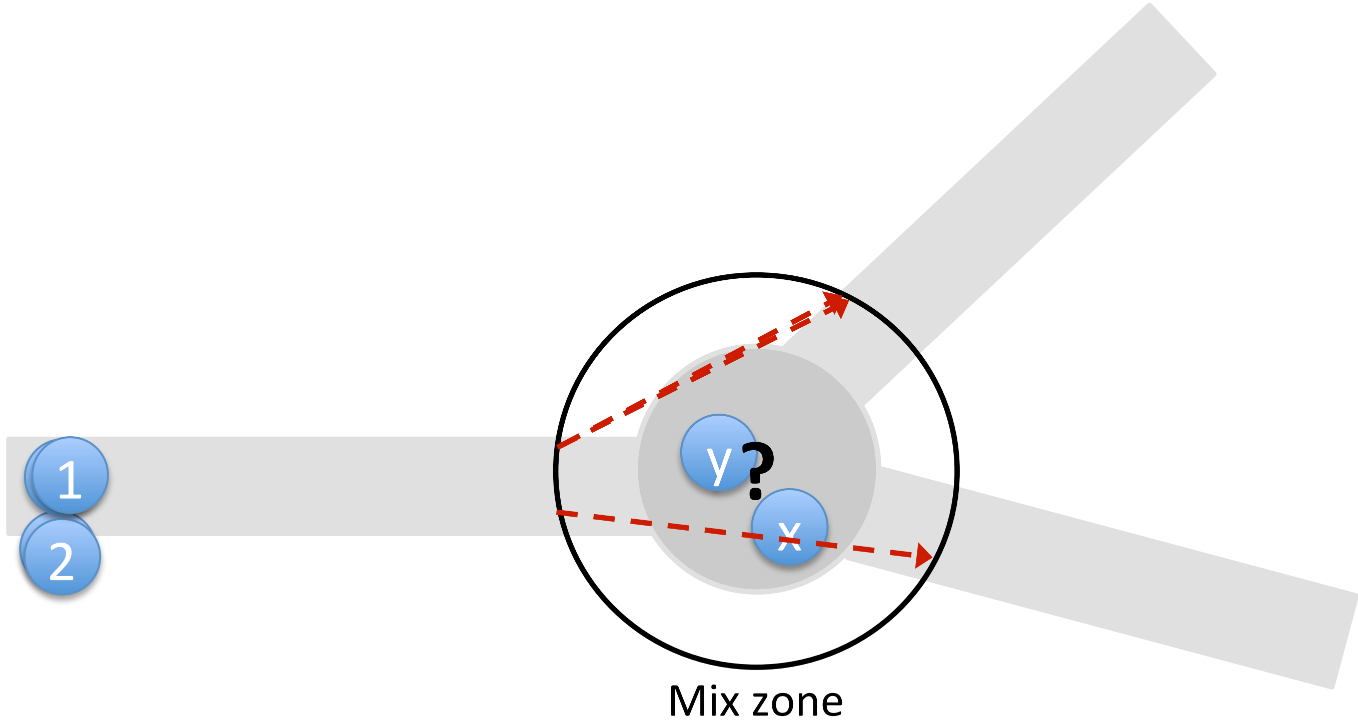
=

γ

Location Privacy with Mix Zones

Spatial decorrelation: Remain silent

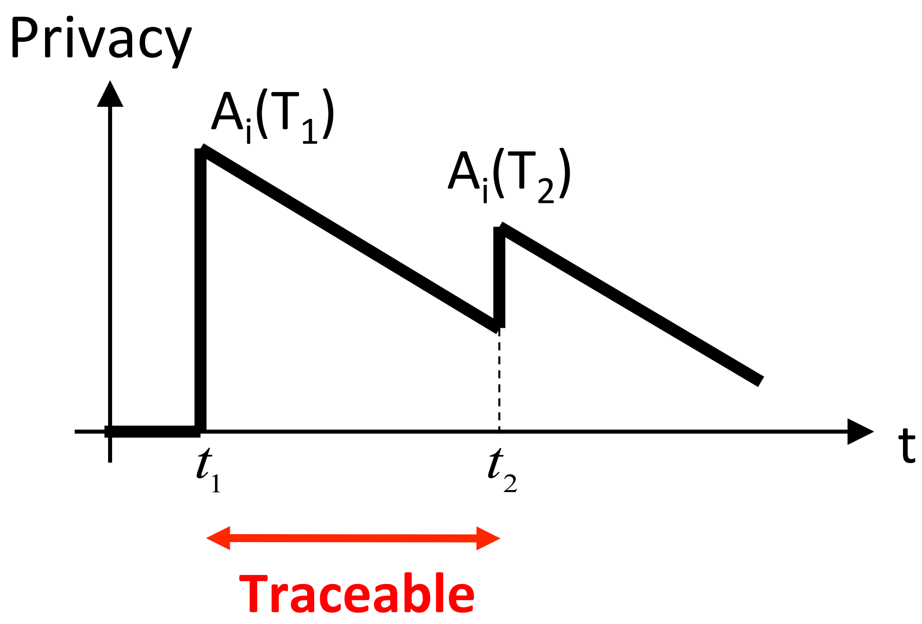
Temporal decorrelation: Change pseudonym



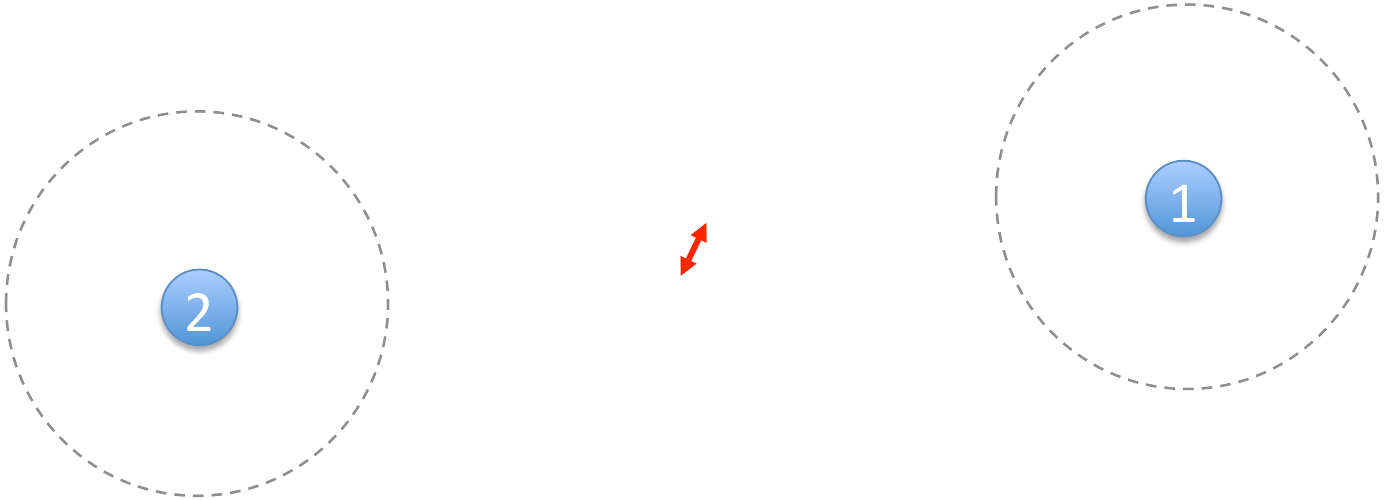
[1] A. Beresford and F. Stajano. **Mix Zones: user privacy in location aware services**. Percom, 2004

User-Centric Location Privacy Model

Privacy = $A_i(T)$ – Privacy Loss



Assumptions



Pseudonym Change game

– Simultaneous decision

– Players want to maximize their payoff

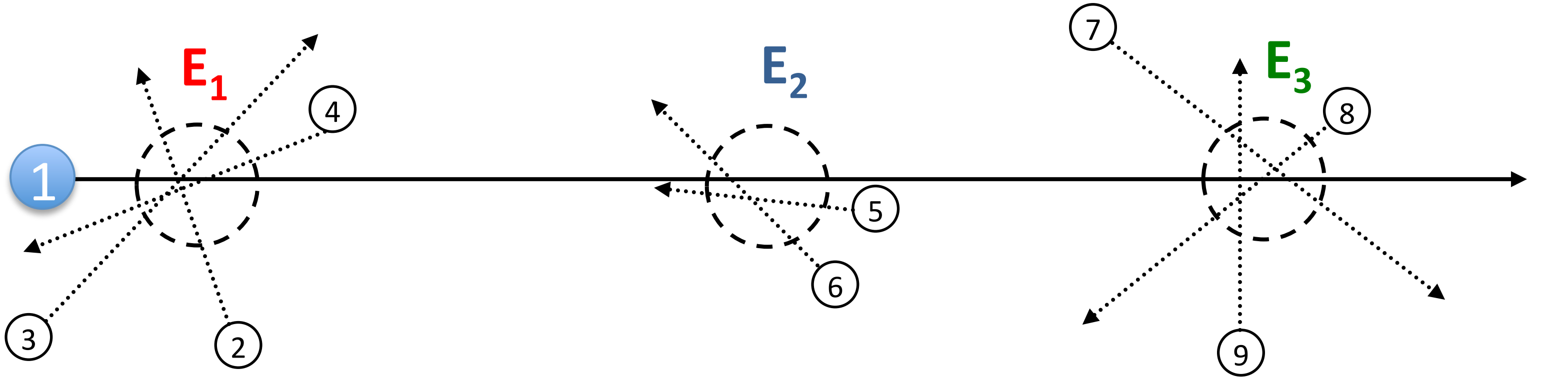
– Consider privacy upperbound $A_i(T) = \log_2(n(t))$

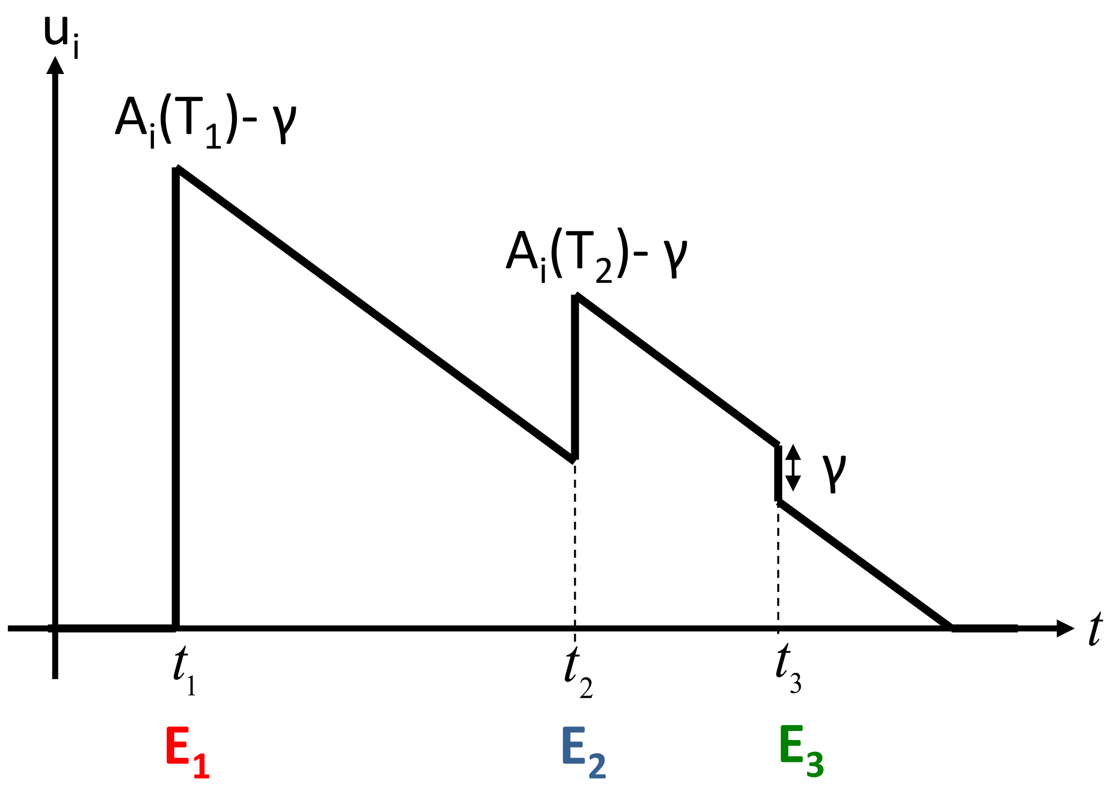
Game Model

- Players
  - Mobile nodes in transmission range
  - There is a game iif $n(t) > 1$

- Strategy
  - Cooperate (**C**) : Change pseudonym
  - Defect (**D**): Do not change pseudonym

Sequence of Pseudonym Change Games





Payoff Function

C

If $(s_i = C) \wedge (n_C(s_{-i}) > 0)$ then

$$T_i^{1} := t$$

$$u_i(t, T_i^{1}, C, s_i) := A_i(T_i^{1}) - \gamma$$

If $(s_i = C) \wedge (n_C(s_{-i}) = 0)$ then

$$u_i(t, T_i^{1}, C, s_i) := \max(0, u_i^{-} - \gamma)$$

D

If $(s_i = D)$, then

$$u_i(t, T_i^{1}, D, s_i) := \max(0, u_i^{-})$$

where $u_i^{-} = A_i(T_i^{1}) - \gamma - \beta_i(t, T_i^{1}) - \gamma\alpha_i(t, T_i^{1})$ the payoff function at the time immediately prior to t

s_{-i} the strategy of the opponents of *i*

$n_C(s_{-i})$ the number of cooperating nodes besides *i*

C-Game

Complete information

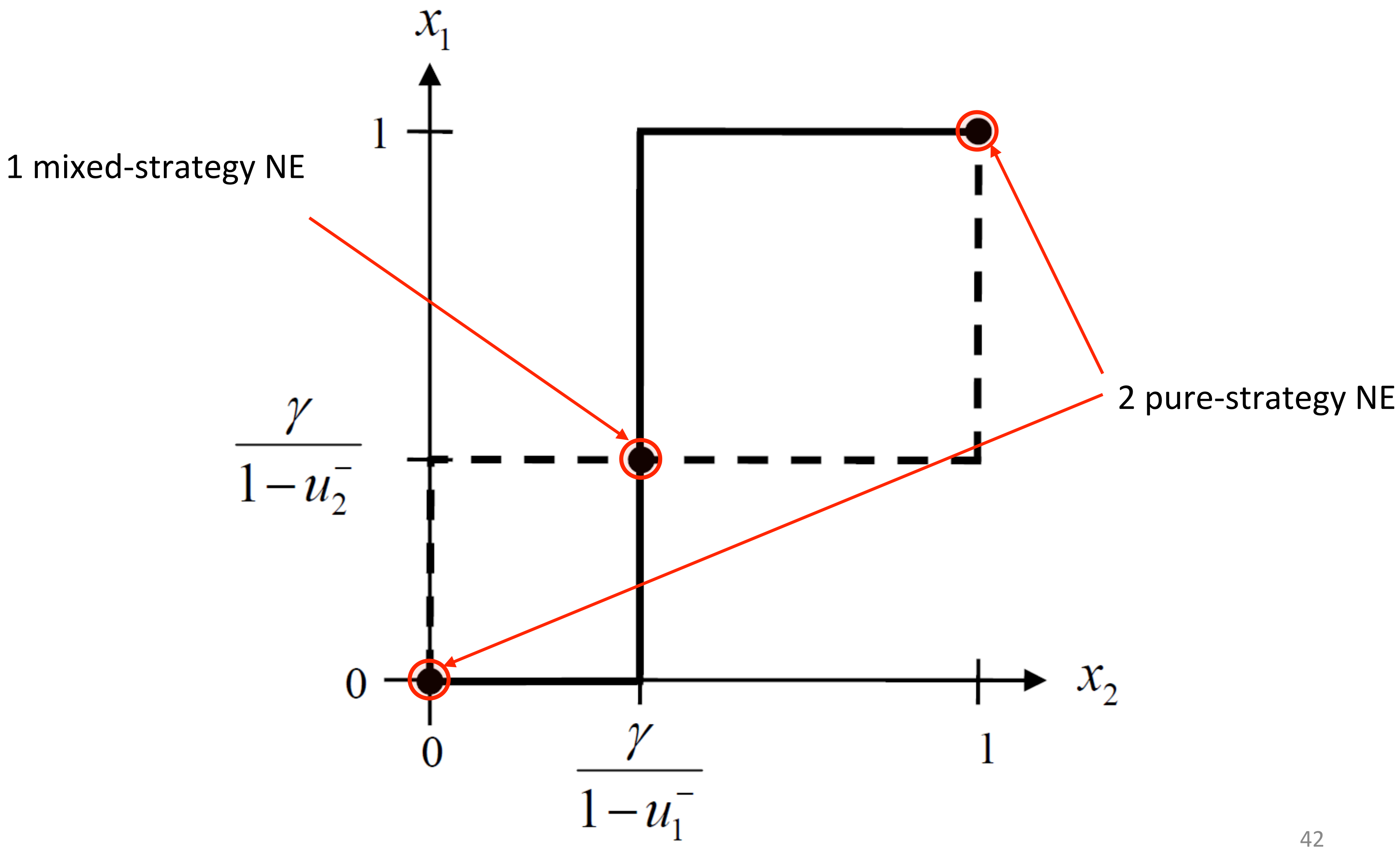
Each player knows the payoff of its opponents

2-Player C-Game

$P_1 \backslash P_2$	C	D
C	$(1-\gamma, 1-\gamma)$	$(u_1^{-} - \gamma, u_2^{-})$
D	$(u_1^{-}, u_2^{-} - \gamma)$	(u_1^{-}, u_2^{-})

Two Nash Equilibria (NE): **(C,C)** & **(D,D)**

Best Response Correspondence



n-Player C-Game

Theorem
The static n-player pseudonym change C-game has **at least 1** and **at most [n/2] Nash equilibria**.

- All Defection is always a NE
- A NE with cooperation exists iif there is a group of *k* users with

$$\log_2(k) - \gamma > u_i^-, \forall i$$ in the group of *k* nodes

C-Game Results

Result 1: high coordination among nodes at NE

- Change pseudonyms only when necessary
- Otherwise defect

I-Game

Incomplete information

Players don’t know the payoff of their opponents

Bayesian Game Theory

Define type of player $\boldsymbol{\theta_i} = \mathbf{u_i^-}$

Predict action of opponents based on pdf over type

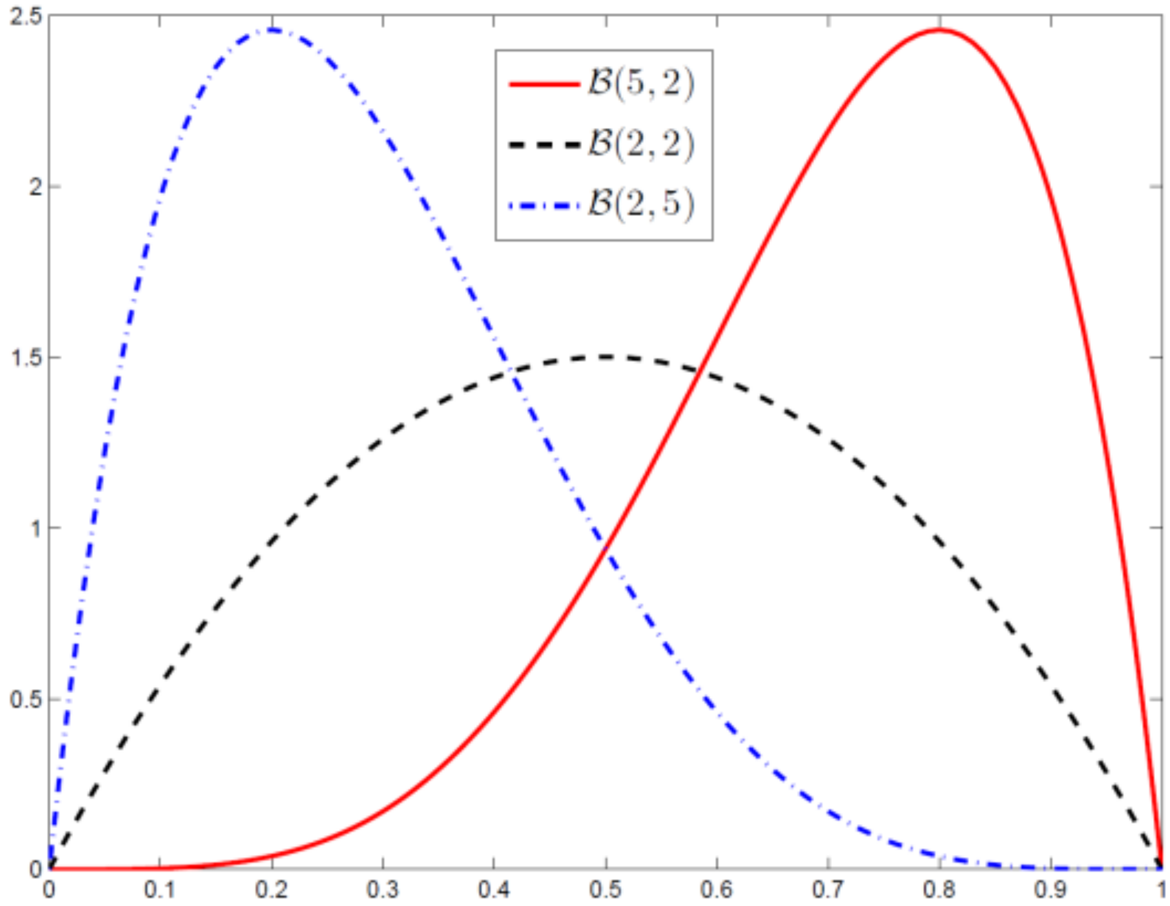
$$f(\theta_i)$$

Environment

Low privacy

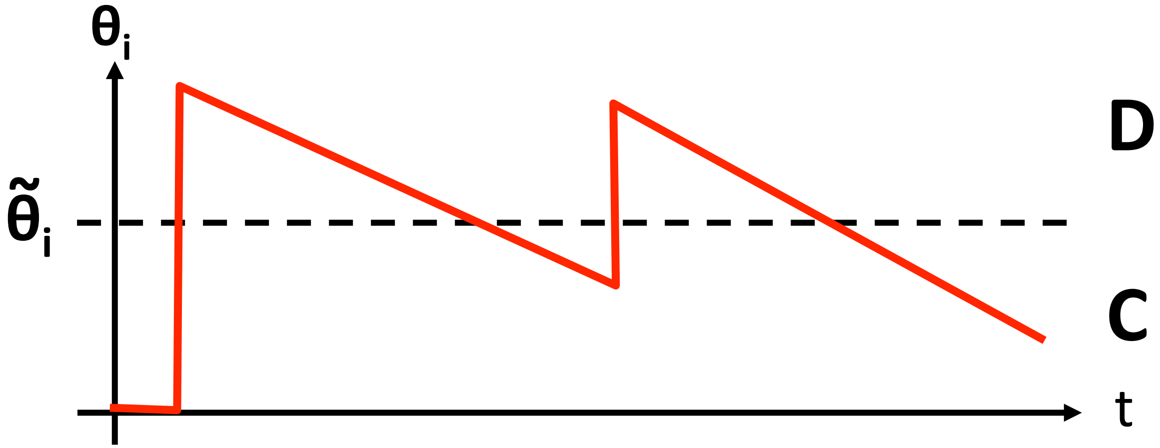
Middle privacy

High privacy



Threshold Strategy

- A threshold determines players' action



- Probability of cooperation is

$$F(\tilde{\theta}_i) = Pr(\theta_i \leq \tilde{\theta}_i) = \int_0^{\tilde{\theta}_i} f(\theta_i) d\theta_i$$

2-Player *I*-Game Bayesian NE

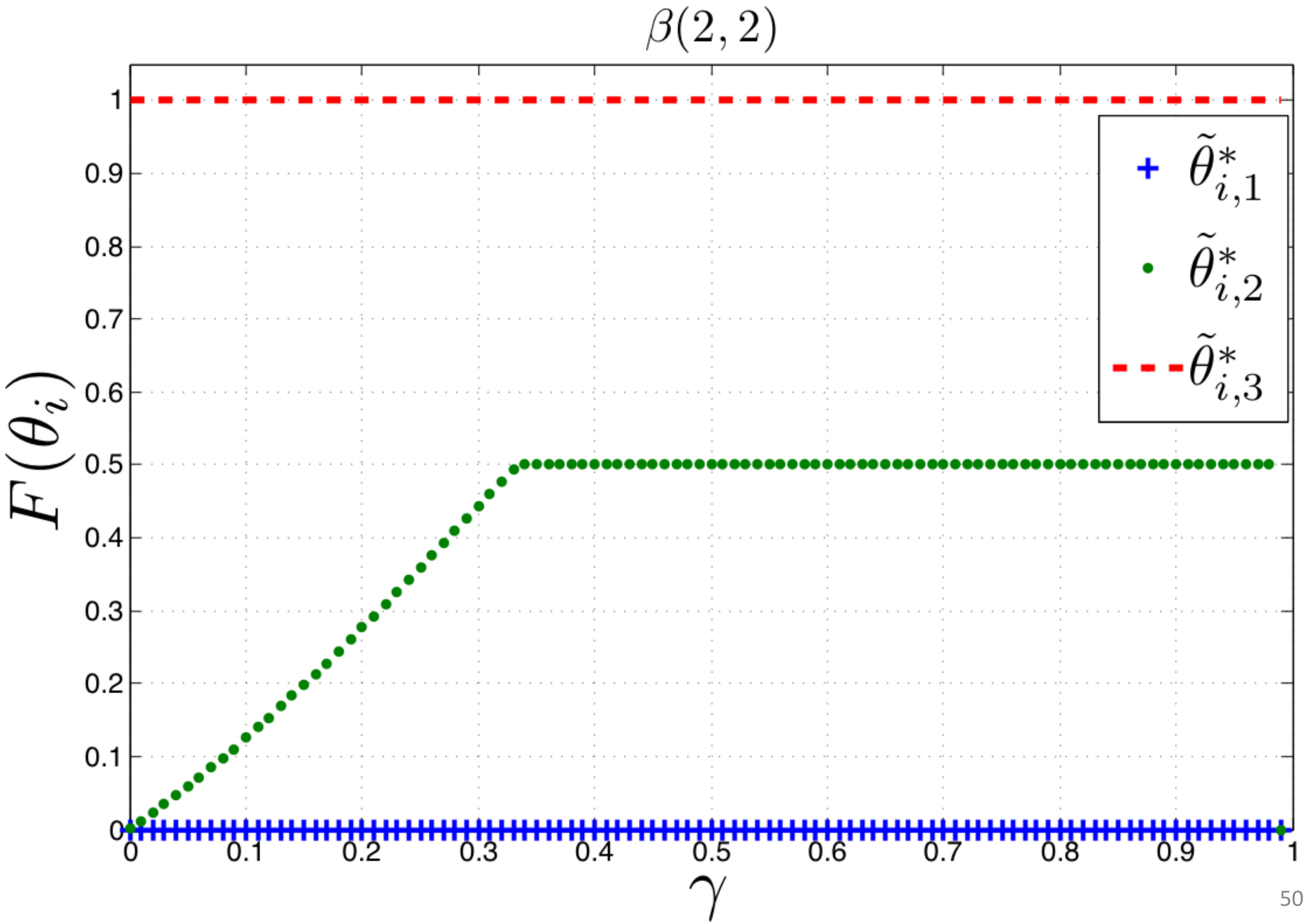
Find threshold $\tilde{\boldsymbol{\theta}}_i^*$ such that

Average utility of cooperation

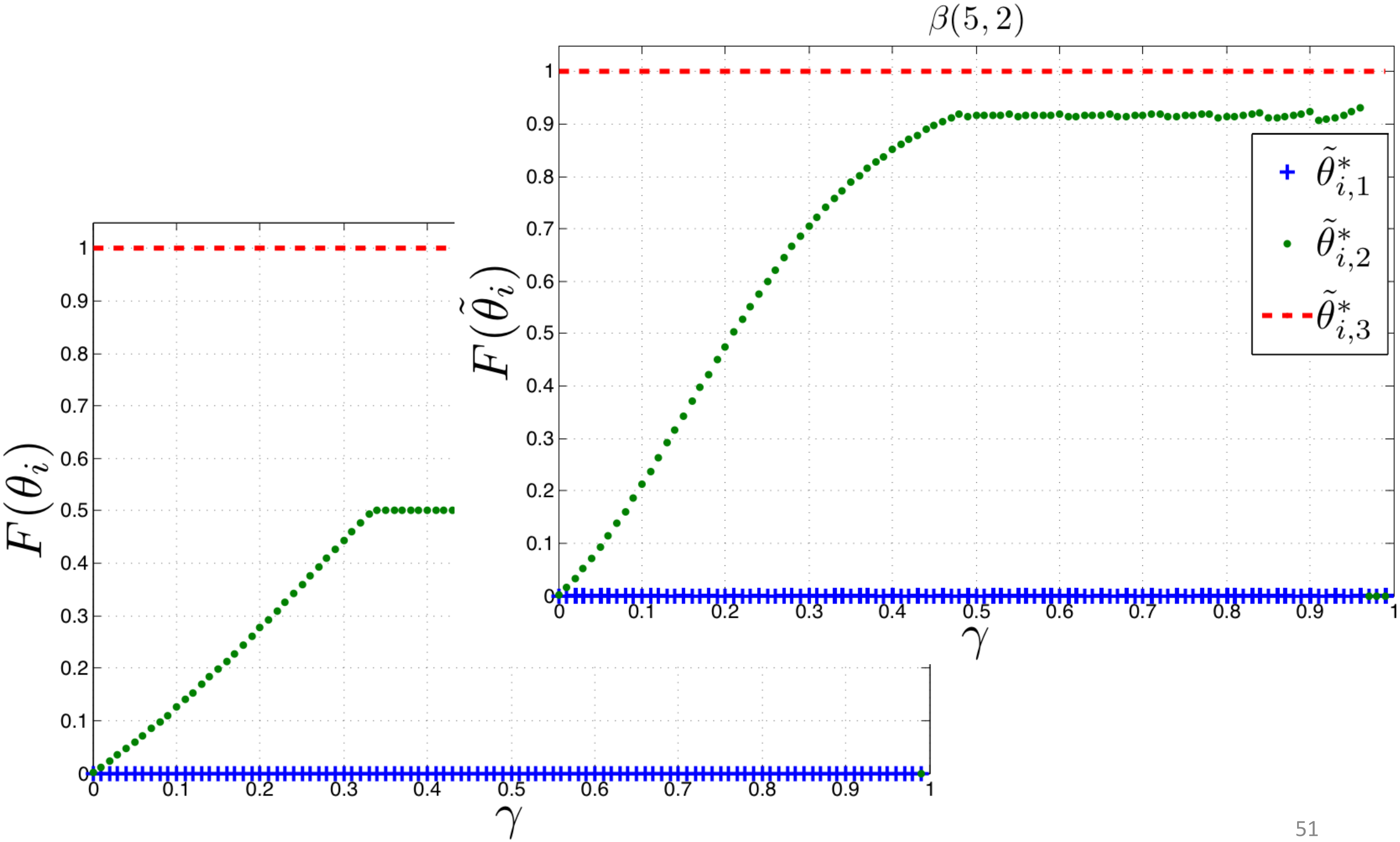
=

Average utility of defection

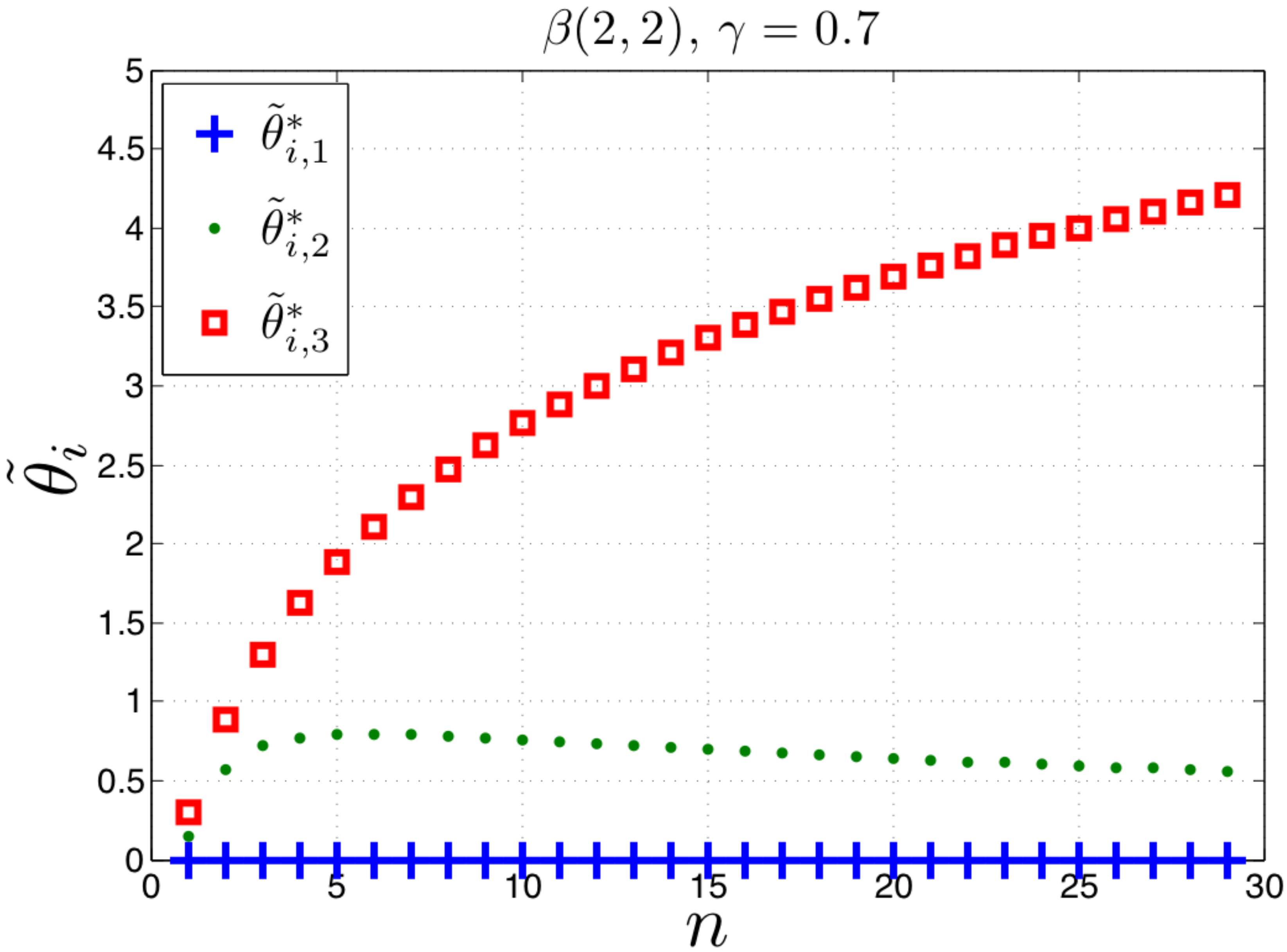
Result 2: Large cost increases cooperation probability.



Result 3: Strategies adapt to your environment.



Result 4: A large number of nodes n provides incentive not to cooperate



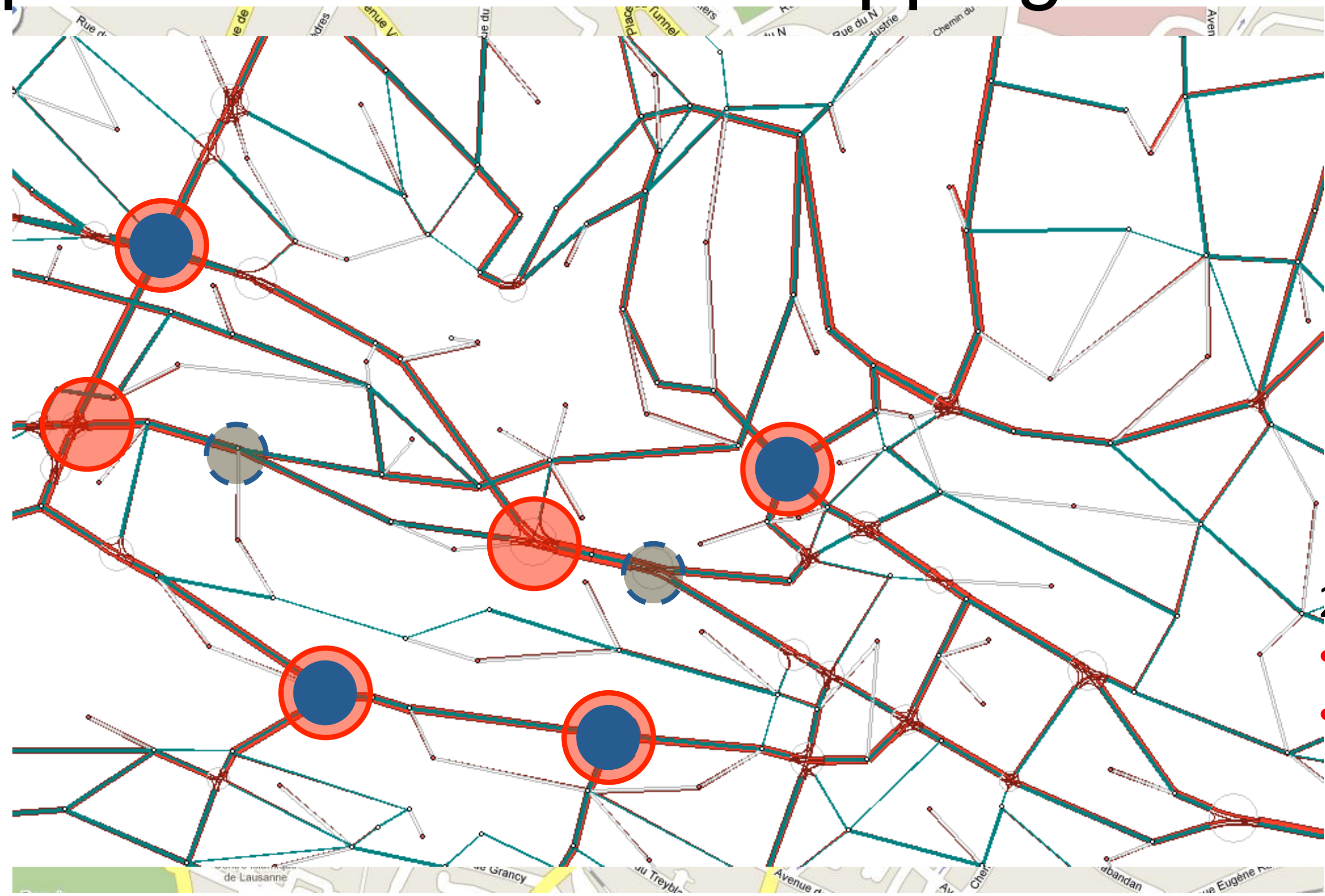
PseudoGame Protocol

Require: Node i knows the probability distribution $f(\theta)$
Require: The current location privacy of node i is u_i^-
1: **if** (Change of velocity within sp_{max}) & (At least one neighbor) **then**
2: Broadcast initiation message to change pseudonym.
3: Goto 6
4: **else**
5: **if** (Receive Initiation message) & (message is valid) **then**
6: $n \Leftarrow estimate(n)$ //Number of neighbors
7: Calculate $\tilde{\theta}_i^*$ as solution of $\sum_{k=0}^{n-1} Pr(K=k) u_i(C, \underline{s}_{-i}) - u_i^- = 0$ wrt $\tilde{\theta}_i$, where $Pr(K=k) \Leftarrow \binom{n}{k} q^k (1-q)^{n-k}$ and $q \Leftarrow \int_0^{\tilde{\theta}_i} f(\theta_i) d\theta_i$
8: **if** $u_i^- \leq \tilde{\theta}_i^*$ **then**
9: Play C
10: Comply with silent period sp_{max}
11: **else**
12: Play D
13: **else**
14: Keep pseudonym

Evaluation of protocols (ns-2, Trans, Implementation, …..)

Tracking Games

Placement of active/passive mix zones versus placement of eavesdropping stations



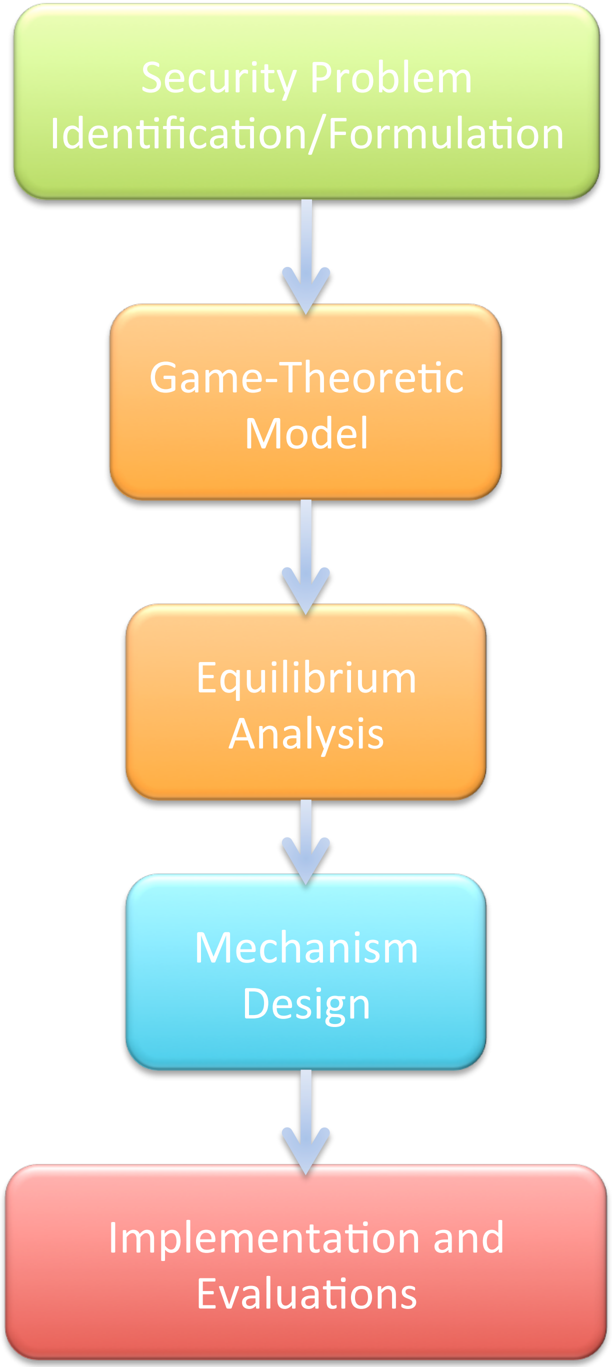
Strategic behaviors of attacker and defenders => **game theory** to model the interactions between players and predict their best strategies

2 knowledge levels

- complete information
- incomplete information

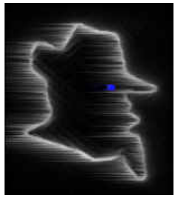
: Eavesdropping station (E)   : Active mix zone (M)   : Passive mix zone (P)

METHODOLOGY



Who is Malicious and Who is Selfish?

Harm everyone: viruses,…

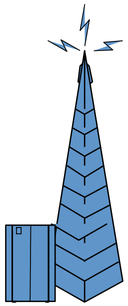


Big brother

Selective harm: DoS,…

Spammer

Cyber-gangster:
phishing attacks,
trojan horses,…



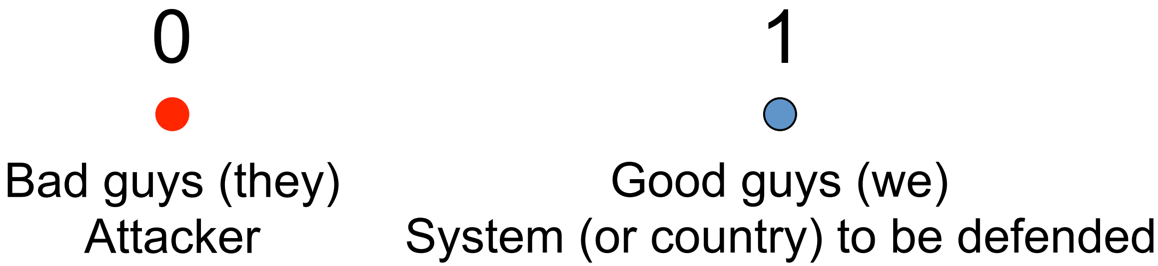
Greedy operator

Selfish mobile station

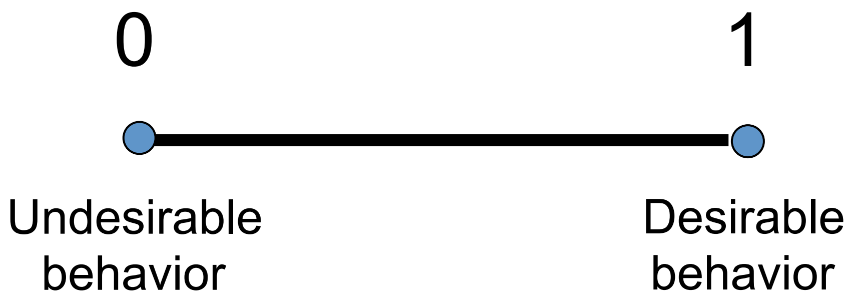
There is no watertight boundary between malice and selfishness
➔ Both security **and** game theory approaches can be useful

From Discrete to Continuous

Warfare-inspired Manichaeism:



The more subtle case of commercial applications:



- Security often needs incentives
- Incentives usually must be secured

Book structure (1/2)

Upcoming wireless networks \ Security and cooperation mechanisms	Naming and addressing	Security associations	Securing neighbor discovery	Secure routing	Privacy	Enforcing fair MAC	Enforcing PKT FWing	Discouraging greedy op.	Behavior enforc.
Small operators, community networks	X	X			X	X		X	X
Cellular operators in shared spectrum	X				X	X		X	X
Mesh networks	X	X	X	X	X	X		X	?
Hybrid ad hoc networks	X	X	X	X	X	X	X	X	X
Self-organized ad hoc networks	X	X	X	X	X	X	X		X
Vehicular networks	X	X	X	X	X	?	?	?	?
Sensor networks	X	X	X	X	X	?		X	?
RFID networks	X	?	X		X				?

Part I (rows) — Part II (Naming and addressing to Privacy) — Part III (Enforcing fair MAC to Behavior enforc.)

Book structure (2/2)

Security | **Cooperation**

12. Behavior enforcement

8. Privacy protection
7. Secure routing
6. Secure neighbor discovery
5. Security associations
4. Naming and addressing

11. Operators in shared spectrum
10. Selfishness in PKT FWing
9. Selfishness at MAC layer

3. Trust
2. Upcoming networks
1. Existing networks

Appendix A: Security and crypto

Appendix B: Game theory

Conclusion

- Upcoming wireless networks bring formidable challenges in terms of security and cooperation
- The proper treatment requires a thorough understanding of upcoming wireless networks, of security, and of game theory