Security and Cooperation in Wireless Networks

Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing

Levente Buttyan and Jean-Pierre Hubaux

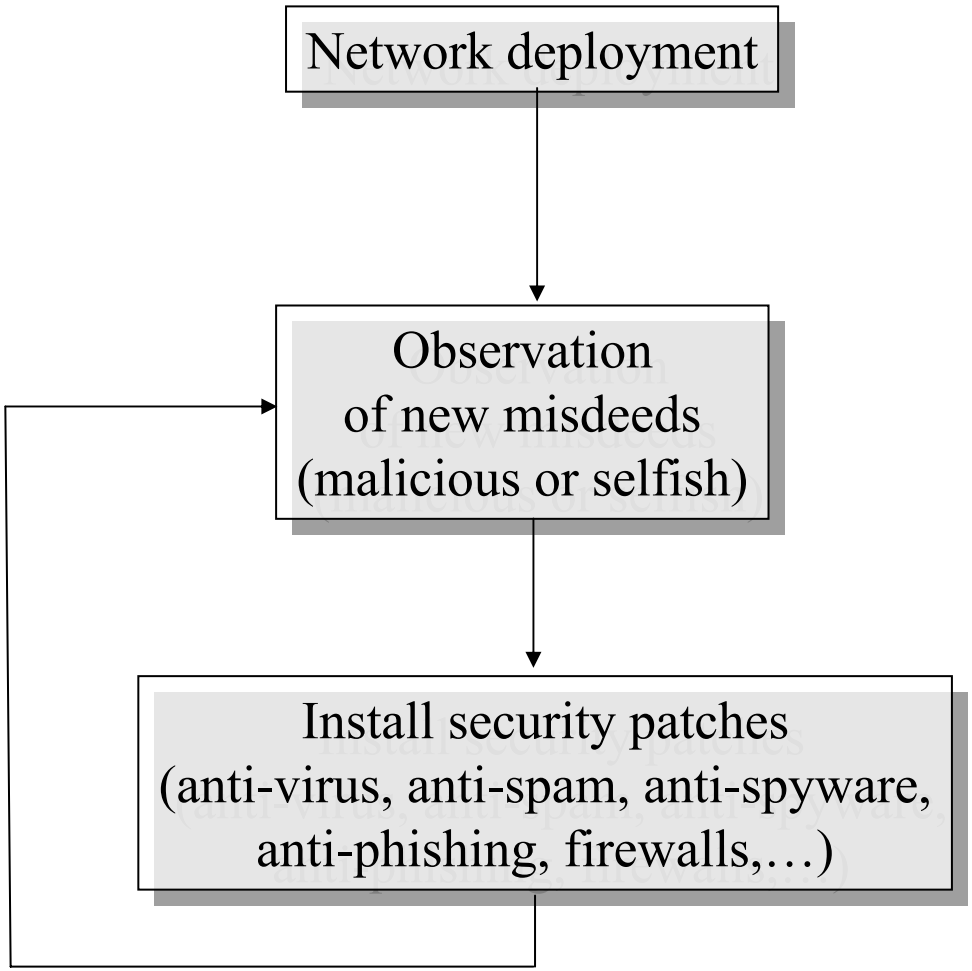
With contributions from N. Ben Salem, M. Cagalj, S. Capkun, M. Felegyhazi, T. Holczer, H. Manshaei, P. Papadimitratos, P. Schaffer, and M. Raya

http://secowinet.epfl.ch

Security and Cooperation in Wireless Networks

1. Introduction
2. Thwarting malicious behavior
3. Thwarting selfish behavior

The Internet : something went wrong



"**The Internet is Broken**"
MIT Technology Review,
Dec. 2005 – Jan. 2006
➔ NSF FIND, GENI, etc.

Where is this going ?

MIT Technology Review,
Dec. 2005 – Jan. 2006

The Economist, April 28, 2007

What if tomorrow's wireless networks are even more unsafe than today's Internet ?

Upcoming wireless networks

- New kinds of networks
  - Personal communications
    - Small operators, community networks
    - Cellular operators in shared spectrum
    - Mesh networks
    - Hybrid ad hoc networks (also called “Multi-hop cellular networks”)
    - “Autonomous” ad hoc networks
    - Personal area networks
  - Vehicular networks
  - Sensor and RFID networks
  - …
- New wireless communication technologies
  - Cognitive radios
  - MIMO
  - Ultra Wide Band
  - Directional antennas
  - …

Upcoming wireless networks

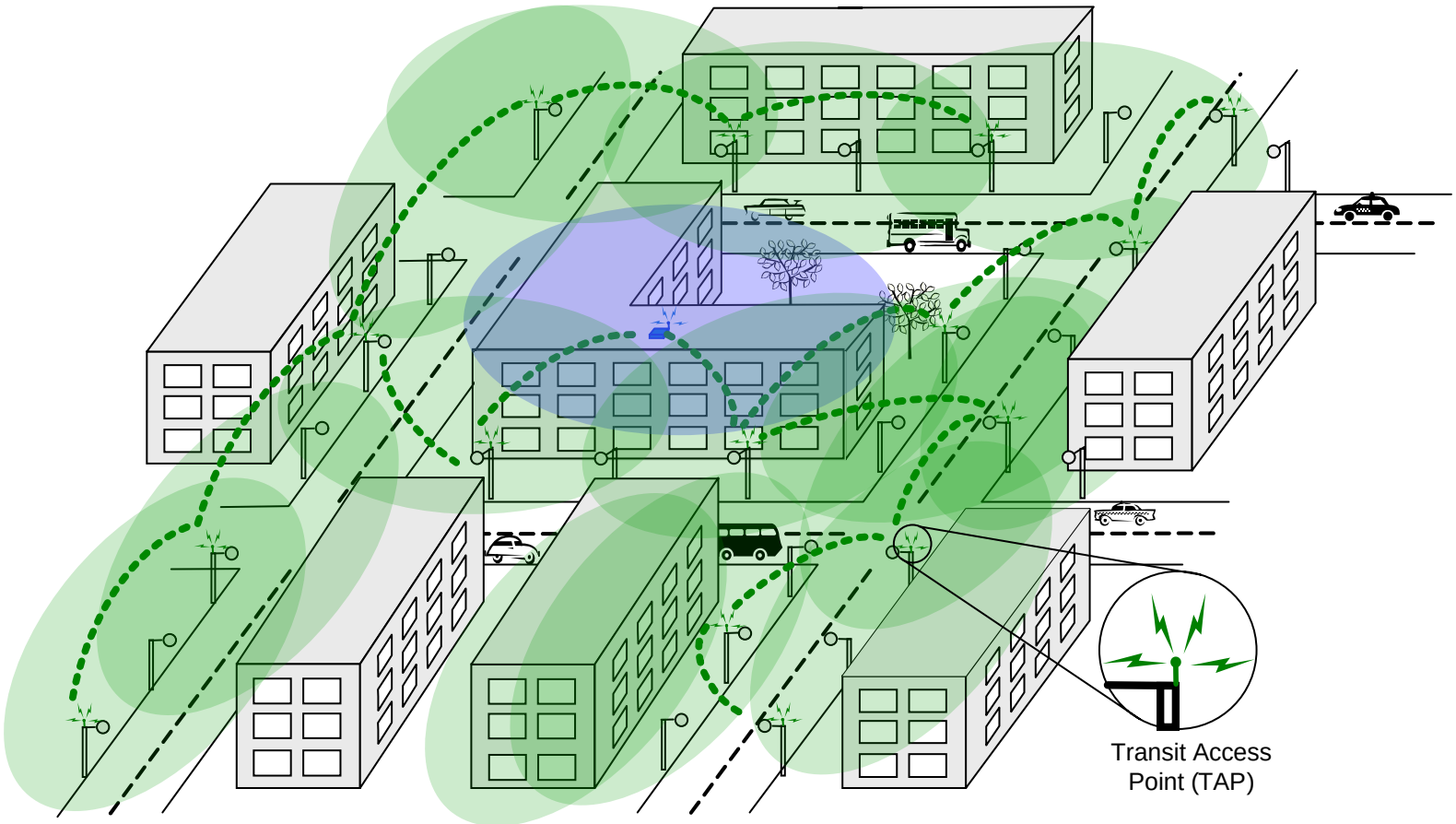
- New kinds of networks
  - Personal communications
    - Small operators, community networks
    - Cellular operators in shared spectrum
    - Mesh networks
    - Hybrid ad hoc networks (also called “Multi-hop cellular networks”)
    - “Autonomous” ad hoc networks
    - Personal area networks
  - Vehicular networks
  - Sensor and RFID networks
  - …
- New wireless communication technologies
  - Cognitive radios
  - MIMO
  - Ultra Wide Band
  - Directional antennas
  - …

Community networks

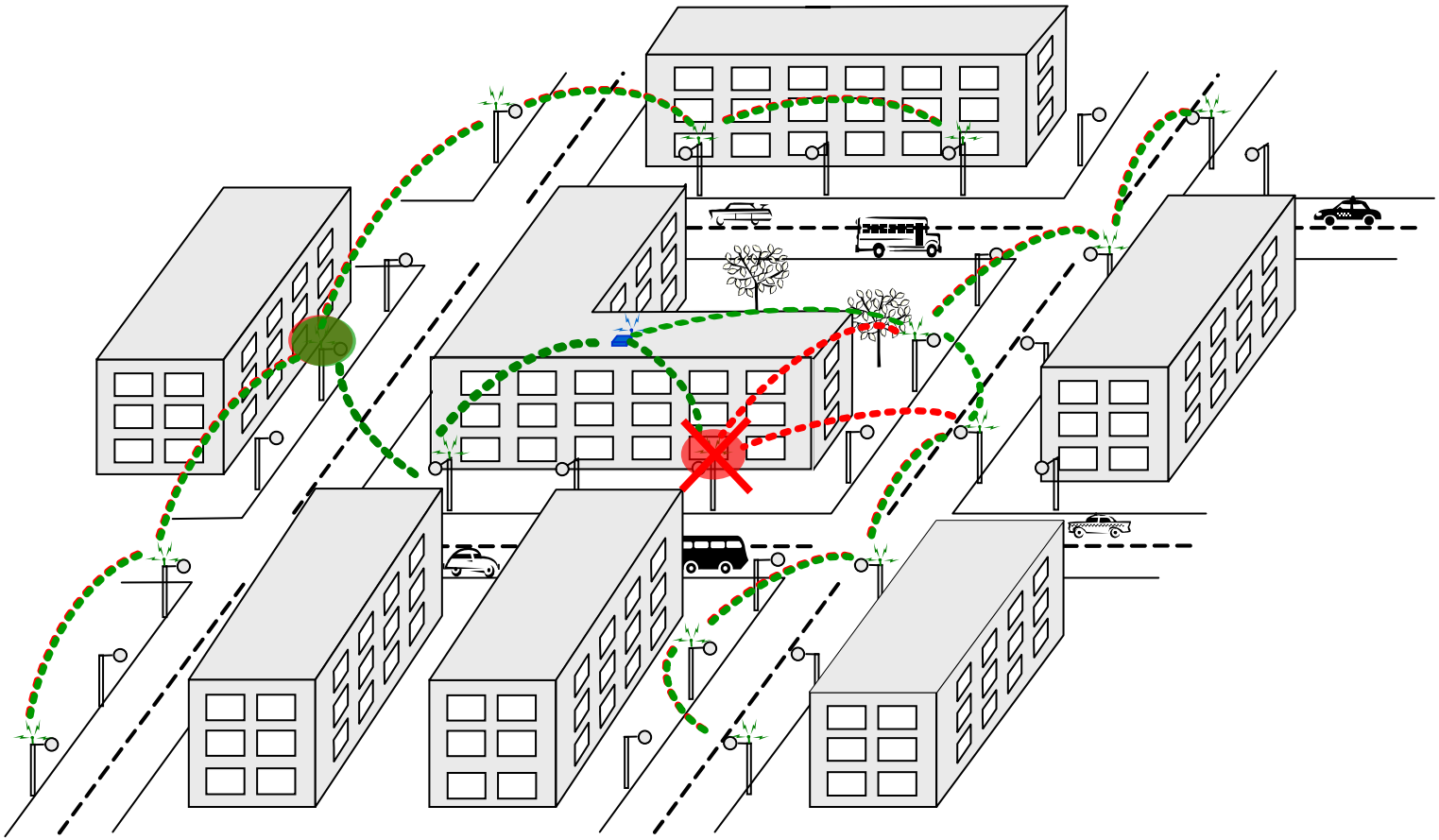
Example: service reciprocation in community networks

- A phenomenon of growing relevance, led by FON, http://en.fon.com/
- FON claims
  - to have raised a total of more than 30M$, notably from Google, Skype, and BT
  - that the number of “Foneros” is around 830’000

Mesh Networks



Mesh Networks: node compromise



Mesh Networks: jamming

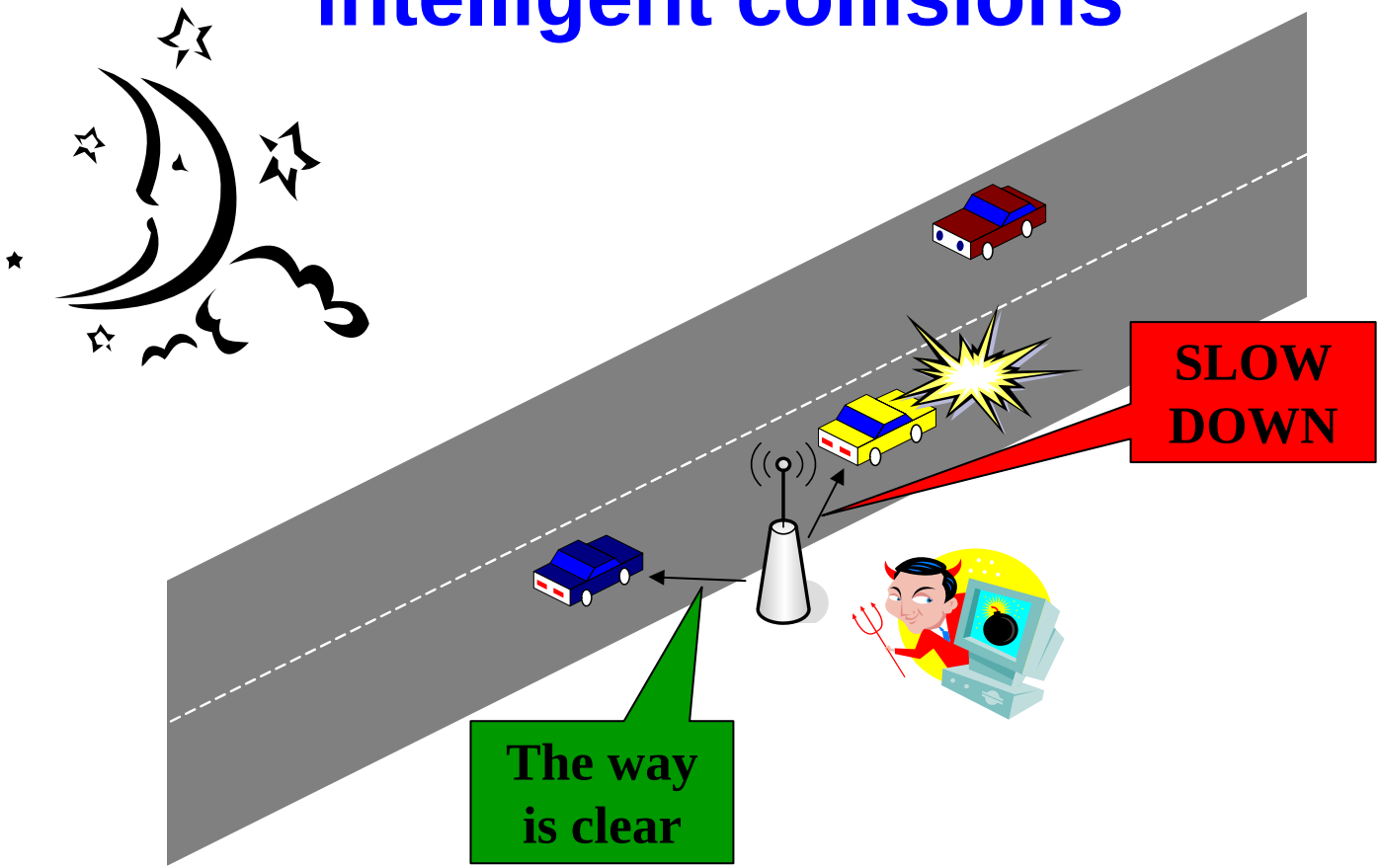
More on mesh networks:

- IEEE Wireless Communications, Special Issue on Wireless Mesh Networking, Vol. 13 No 2, April 2006

Vehicular networks: why?

- Combat the awful side-effects of road traffic
  - In the EU, around 40’000 people die yearly on the roads; more than 1.5 millions are injured
  - Traffic jams generate a tremendous waste of time and of fuel
- Most of these problems can be solved by providing appropriate ***information*** to the driver or to the vehicle

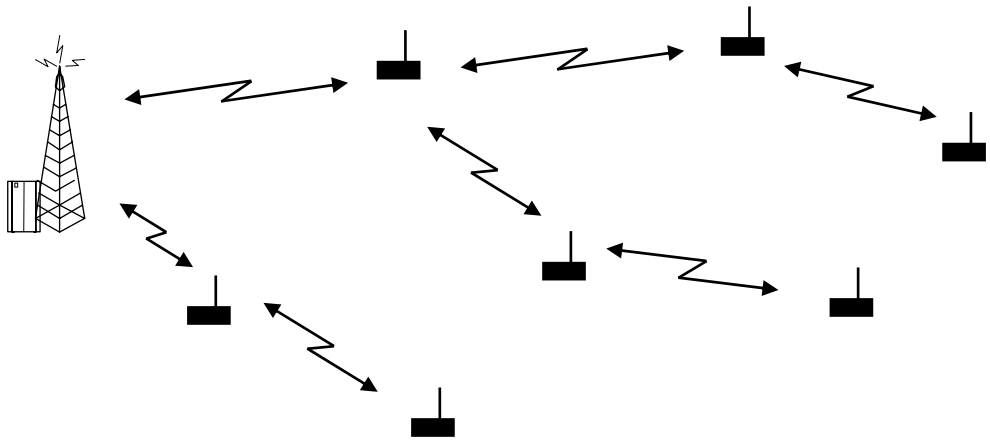
Example of attack : Generate “intelligent collisions”



- All carmakers are working on vehicular comm.
- Vehicular networks will probably be the largest incarnation of **mobile** ad hoc networks

For more information:
http://ivc.epfl.ch
http://www.sevecom.org

Sensor networks

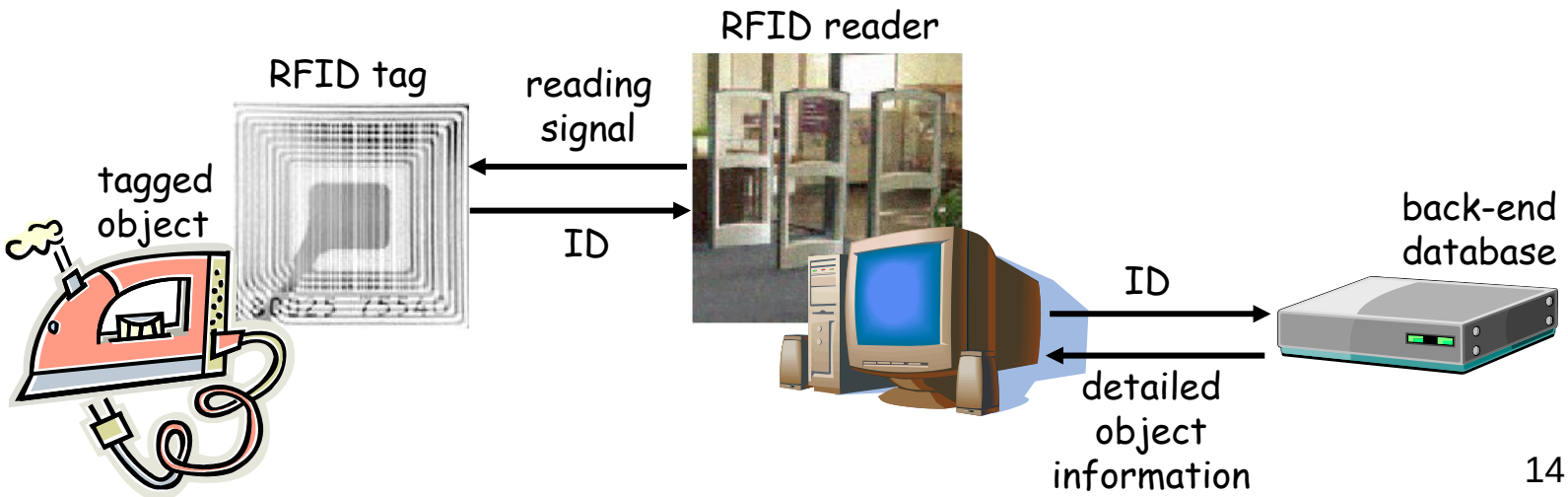


Vulnerabilities:

- Theft ➔ reverse engineered and compromised, replicated
- Limited capabilities ➔ risk of DoS attack, restriction on cryptographic primitives to be used
- Deployment can be random ➔ pre-configuration is difficult
- Unattended ➔ some sensors can be maliciously moved around

RFID

- RFID = Radio-Frequency Identification
- RFID system elements
  - RFID tag + RFID reader + back-end database
- RFID tag = microchip + RF antenna
  - microchip stores data (few hundred bits)
  - Active tags
    - have their own battery → expensive
  - Passive tags
    - powered up by the reader's signal
    - reflect the RF signal of the reader modulated with stored data



Trends and challenges in wireless networks

- From centralized to distributed to self-organized
  ➔ **Security architectures** must be redesigned
- Increasing programmability of the devices
  ➔ increasing **risk of attacks** and of **greedy behavior**
- Growing number of tiny, embedded devices
  ➔ Growing **vulnerability**, new attacks
- From single-hopping to multi-hopping
  ➔ Increasing "**security distance**" between devices and infrastructure, increased **temptation for selfish behavior**
- **Miniaturization** of devices ➔ Limited capabilities
- Pervasiveness ➔ Growing **privacy** concerns

… Yet, mobility and wireless can **facilitate** certain security mechanisms

Grand Research Challenge

Prevent ubiquitous computing from becoming a pervasive nightmare

Reasons to trust organizations and individuals

- Moral values
  - Culture + education, fear of bad reputation
- Experience about a given party
  - Based on previous interactions

} Will lose relevance

- Rule enforcement organization
  - Police or spectrum regulator

→ Scalability challenge

- Usual behavior
  - Based on statistical observation

→ Can be misleading

- Rule enforcement mechanisms
  - Prevent malicious behavior (by appropriate security mechanisms) and encourage cooperative behavior

Upcoming networks vs. mechanisms

Upcoming wireless networks \ Rule enforcement 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				?

Security

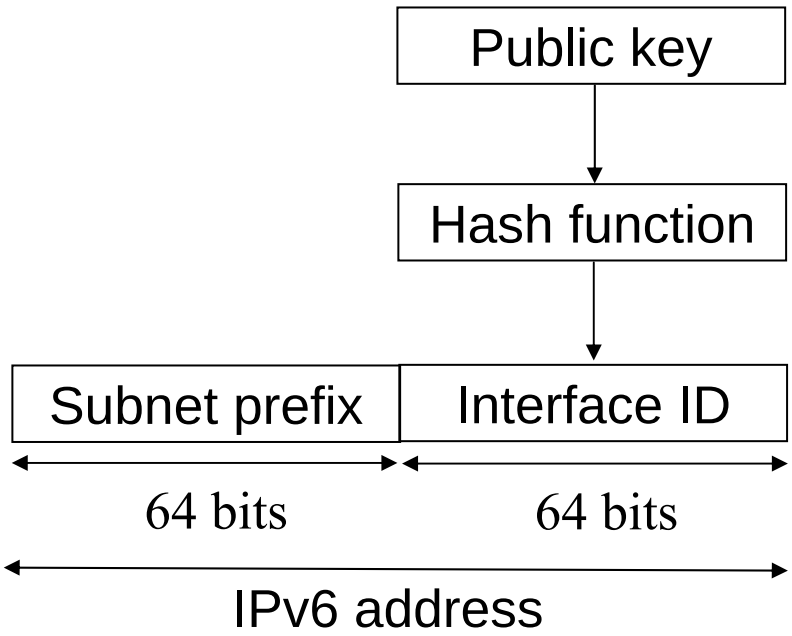
Cooperation

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

2.1 Naming and addressing

- Typical attacks:
  - Sybil: the same node has multiple identities
  - Replication: the attacker captures a node and replicates it
    ➔ several nodes share the same identity
- Distributed protection technique in IPv6: Cryptographically Generated Addresses (T. Aura, 2003; RFC 3972) → only a partial solution to the problem



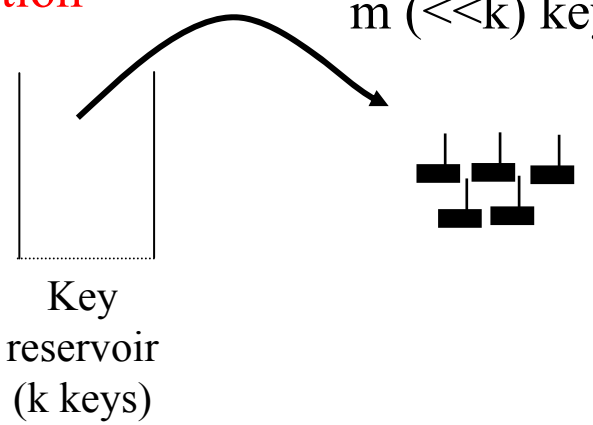
For higher security (hash function output beyond 64 bits), *hash extension* can be used

Parno, Perrig, and Gligor. Detection of **node replication** attacks in sensor networks. *IEEE Symposium on Security and Privacy, 2005*

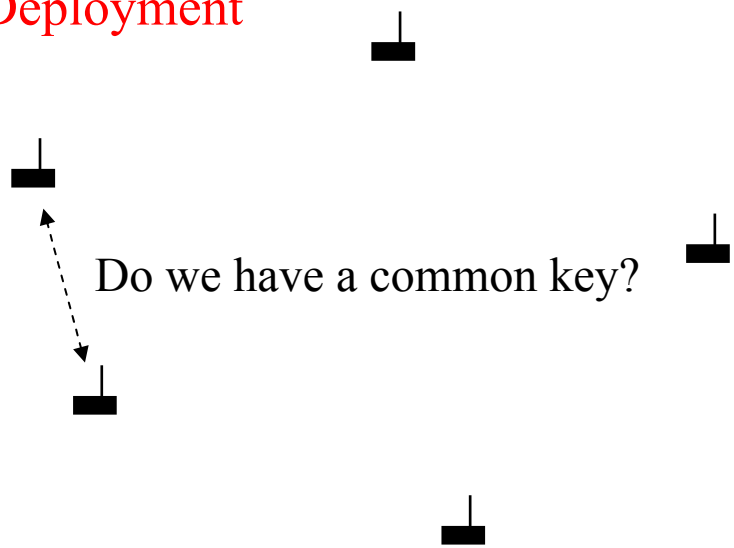
2.2 Pairwise key establishment in sensor networks

1. Initialization

m (<<k) keys in each sensor ("key ring of the node")



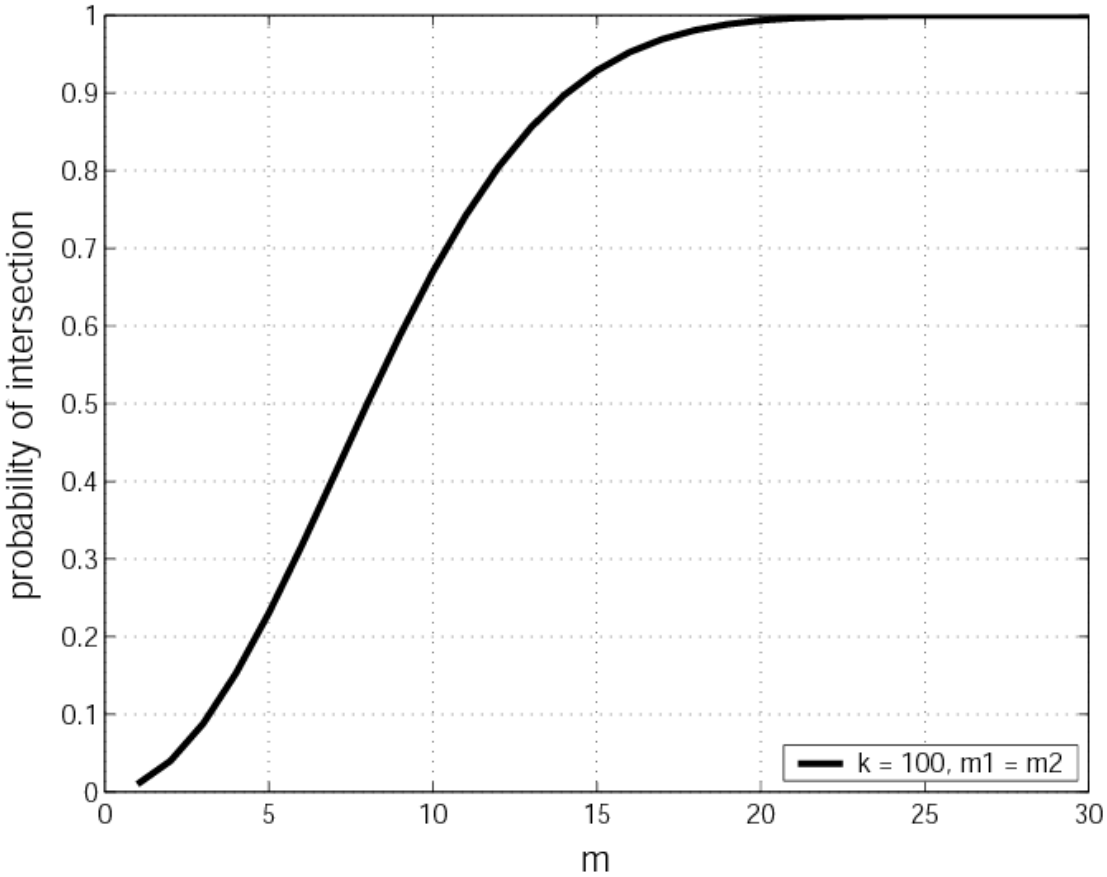
2. Deployment



Probability for any 2 nodes to have a common key:

$$p = 1 - \frac{((k-m)!)^2}{k!(k-2m)!}$$

Probability for two sensors to have a common key

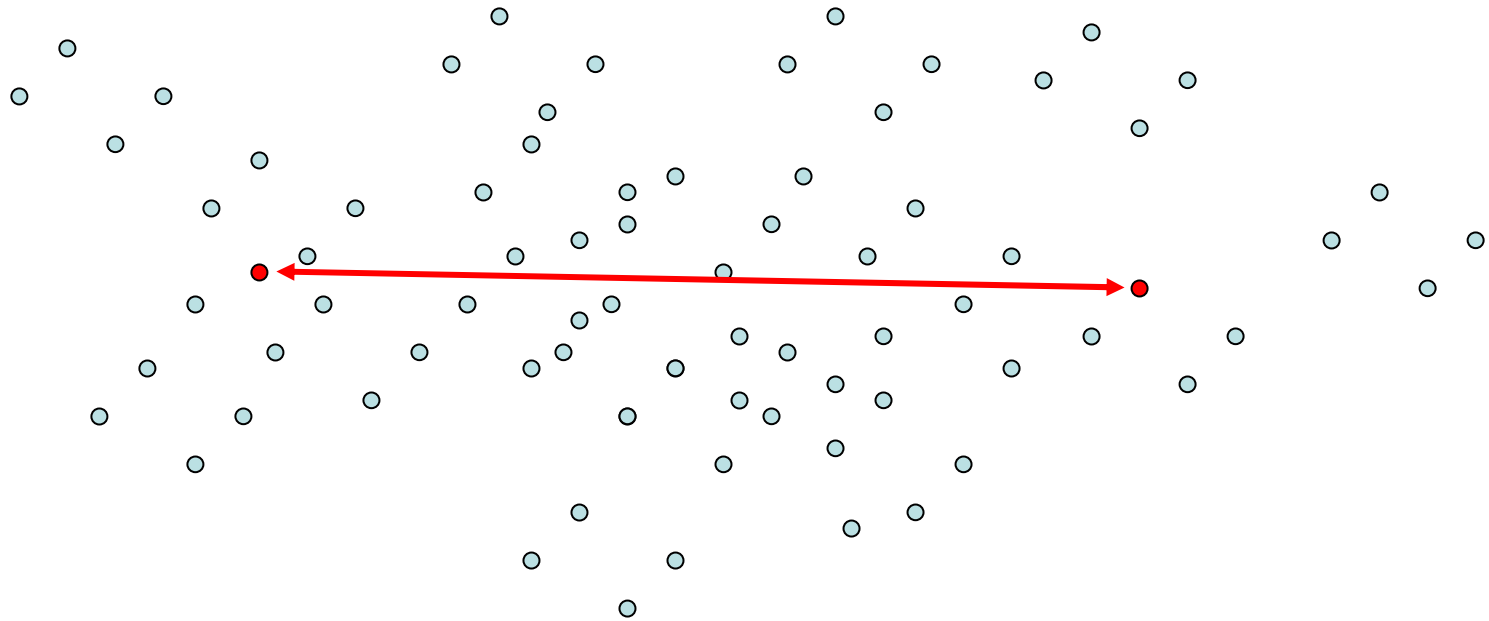


Eschenauer and Gligor, *ACM CCS 2002*

See also:

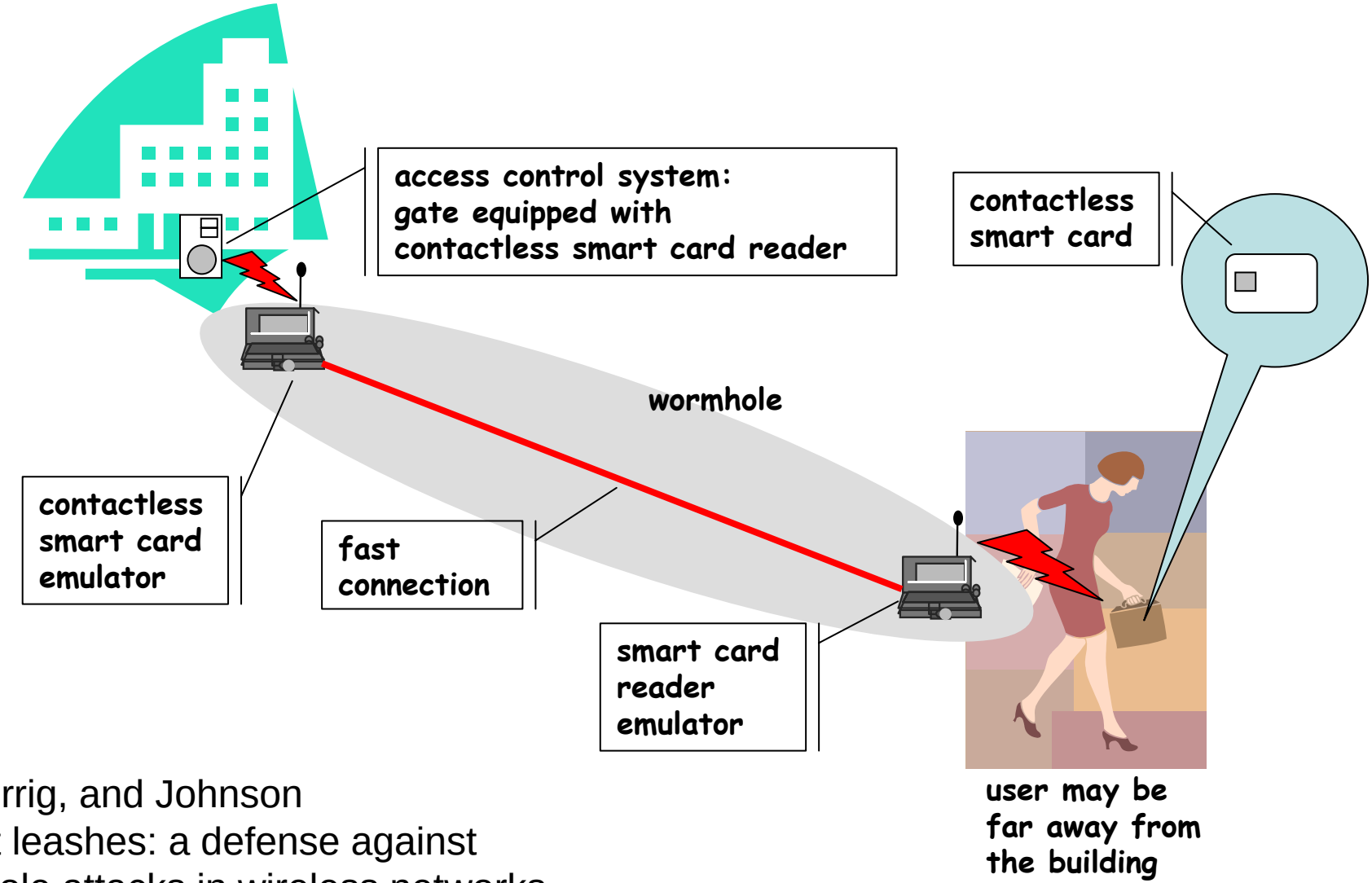
- Karlof, Sastry, Wagner: TinySec, *Sensys 2004*
- Westhoff et al.: On Digital Signatures in Sensor Networks, *ETT 2005*

2.3 Securing Neighbor Discovery: Thwarting Wormholes



- Routing protocols will choose routes that contain wormhole links
  - typically those routes appear to be shorter
  - Many of the routes (e.g., discovered by flooding based routing protocols such as DSR and Ariadne) will go through the wormhole
- The adversary can then monitor traffic or drop packets (DoS)

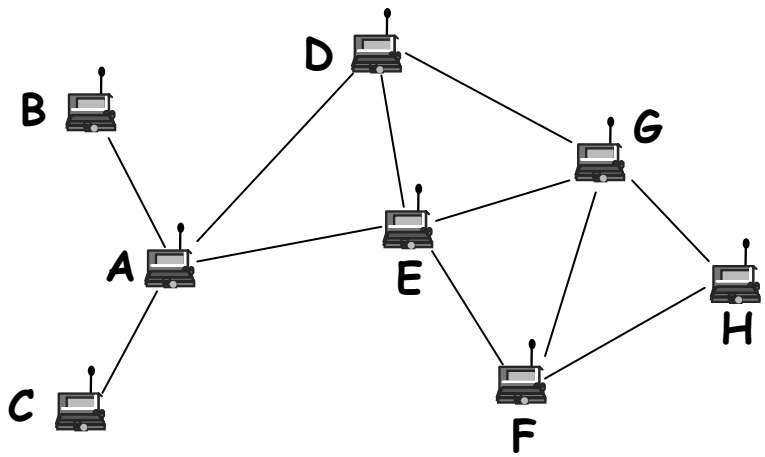
Wormholes are not specific to ad hoc networks



Hu, Perrig, and Johnson
Packet leashes: a defense against wormhole attacks in wireless networks
INFOCOM 2003

2.4 Secure routing in wireless ad hoc networks

Exchange of messages in Dynamic Source Routing (DSR):

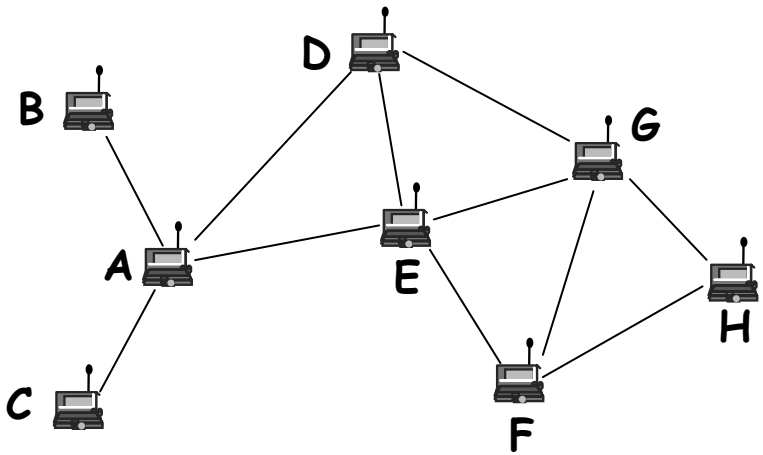


A → *: [req,A,H; -] → B, C, D, E
B → *: [req,A,H; B] → A
C → *: [req,A,H; C] → A
D → *: [req,A,H; D] → A, E, G
E → *: [req,A,H; E] → A, D, G, F
F → *: [req,A,H; E,F] → E, G, H
G → *: [req,A,H; D,G] → D, E, F, H

H → A: [H,F,E,A; rep; E,F]

- Routing disruption attacks
  - routing loop
  - black hole / gray hole
  - partition
  - detour
  - wormhole
- Resource consumption attacks
  - injecting extra data packets in the network
  - injecting extra control packets in the network

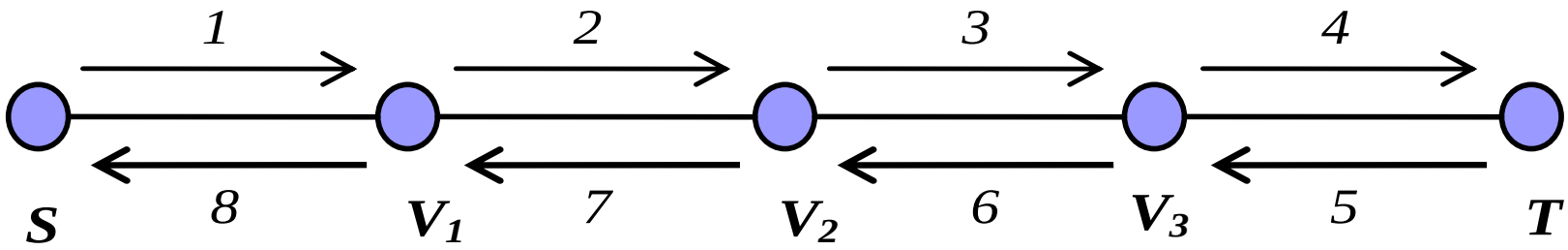
Operation of Ariadne illustrated



A → *: [req, A, H, $MAC_{K_{AH}}$, (), ()]
E → *: [req, A, H, h(E|$MAC_{K_{AH}}$), (E), ($MAC_{K_{E,i}}$)]
F → *: [req, A, H, h(F|h(E|$MAC_{K_{AH}}$)), (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$)]

H → F: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ()]
F → E: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ($K_{F,i}$)]
E → A: [rep, H, A, (E, F), ($MAC_{K_{E,i}}$, $MAC_{K_{F,i}}$), $MAC_{K_{HA}}$, ($K_{F,i}$, $K_{E,i}$)]

Secure route discovery with the Secure Routing Protocol (SRP)



Route Request (*RREQ*): $S, T, Q_{SEQ}, Q_{ID}, MAC(K_{S,T}, S, T, Q_{SEQ}, Q_{ID})$

(1) S broadcasts *RREQ*;
(2) V_1 broadcasts *RREQ*, V_1;
(3) V_2 broadcasts *RREQ*, V_1, V_2;
(4) V_3 broadcasts *RREQ*, V_1, V_2, V_3;

Route Reply (*RREP*): $Q_{ID}, T, V_3, V_2, V_1, S,$
$MAC(K_{S,T}, Q_{ID}, Q_{SEQ}, T, V_3, V_2, V_1, S)$

(5) $T \rightarrow V_3$: *RREP*;
(6) $V_3 \rightarrow V_2$: *RREP*;
(7) $V_2 \rightarrow V_1$: *RREP*;
(8) $V_1 \rightarrow S$: *RREP*;

Q_{SEQ}: Query Sequence Number
Q_{ID} : Query Identifier

More on secure routing

Secure Route Discovery

Hu, Perrig, and Johnson:
Ariadne, Sept. 2002, SEAD, Jun. 2002

Sangrizi, Dahill, Levine, Shields, and Royer: ARAN, Nov. 2002

Papadimitratos and Haas: Secure Routing Protocol (SRP), Jan. 2002

Zapata and Asokan: S-AODV, Sept. 2002

All above proposals are difficult to assess

➔ *G. Ács, L. Buttyán, and I. Vajda*:
Provably Secure On-demand Source Routing
IEEE Transactions on Mobile Computing, Nov. 2006

Secure Data Communication

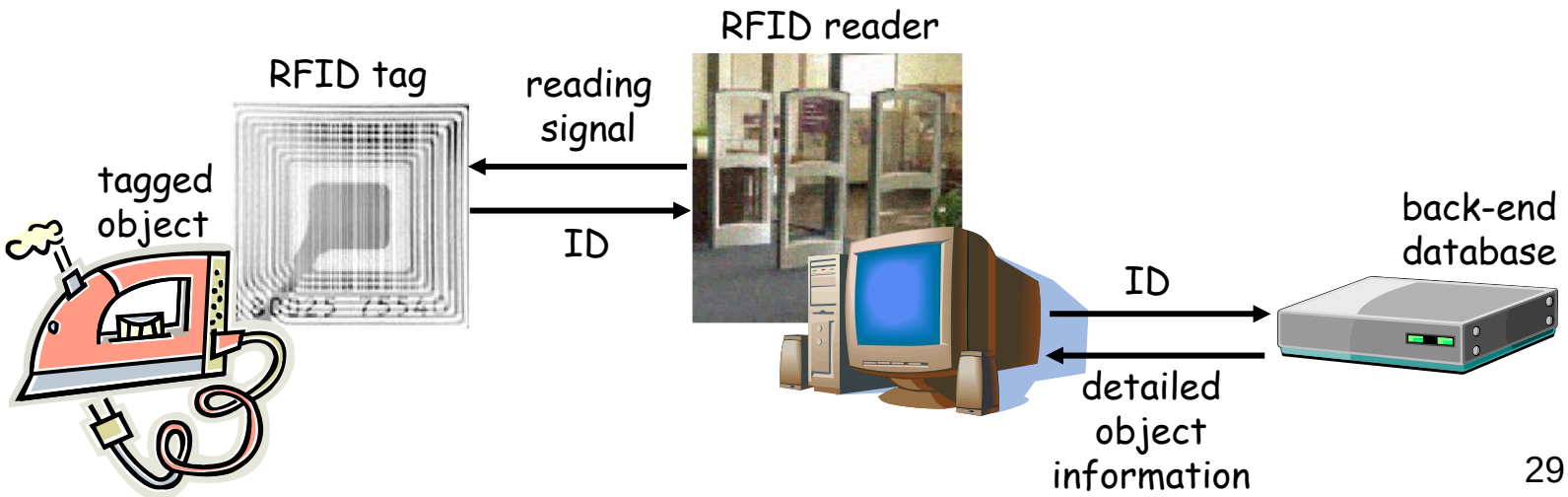
Papadimitratos and Haas: Secure Single Path (SSP) and Secure Multi-path (SMT) protocols, Jul./Sept. 2003, Feb. 2006

Cross-layer attacks

Aad, Hubaux, Knightly:
Jellyfish attacks, 2004

2.5 Privacy: the case of RFID

- RFID = Radio-Frequency Identification
- RFID system elements
  - RFID tag + RFID reader + back-end database
- RFID tag = microchip + RF antenna
  - microchip stores data (few hundred bits)
  - Active tags
    - have their own battery → expensive
  - Passive tags
    - powered up by the reader's signal
    - reflect the RF signal of the reader modulated with stored data

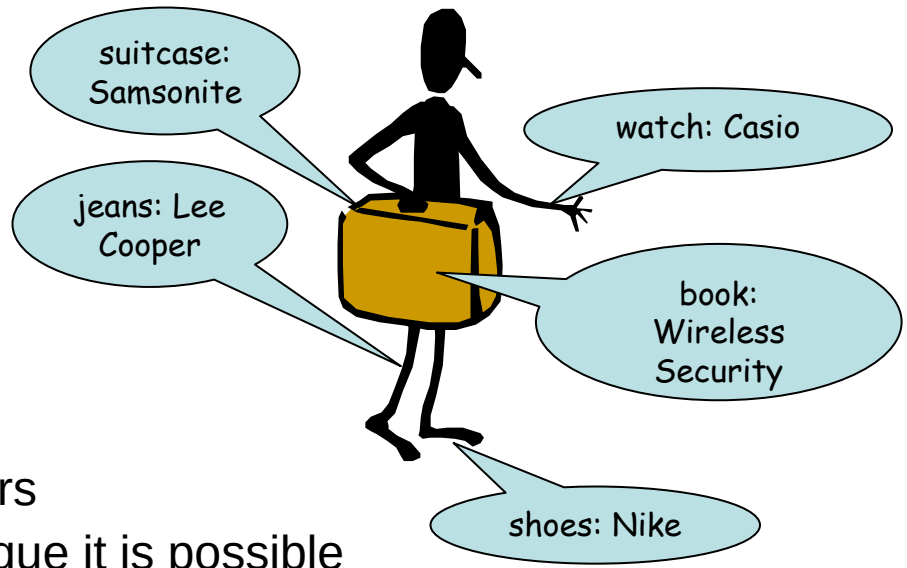


RFID privacy problems

- RFID tags respond to reader's query automatically, without authenticating the reader

→ clandestine scanning of tags is a plausible threat

- Two particular problems:
  1. **Inventorying**: a reader can silently determine what objects a person is carrying
     - books
     - medicaments
     - banknotes
     - underwear
     - …
  2. **Tracking**: set of readers can determine where a given person is located
     - tags emit fixed unique identifiers
     - even if tag response is not unique it is possible to track a set of particular tags



Juels A., RFID Security and Privacy: A Research Survey, *IEEE JSAC, Feb. 2006*

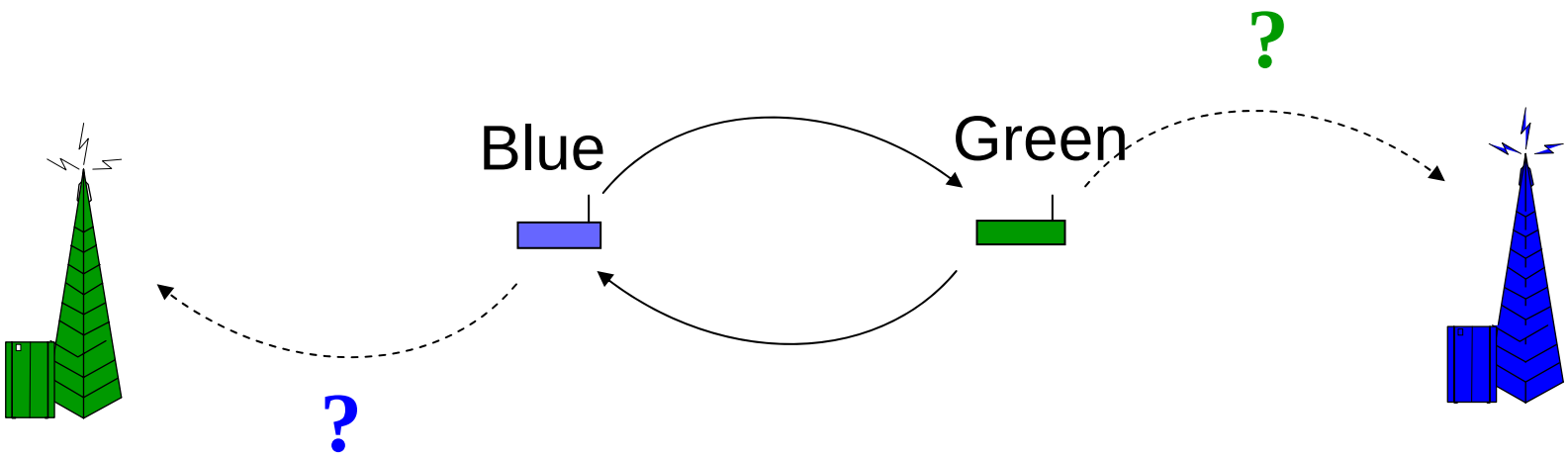
Security and Cooperation in Wireless Ad Hoc Networks

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*

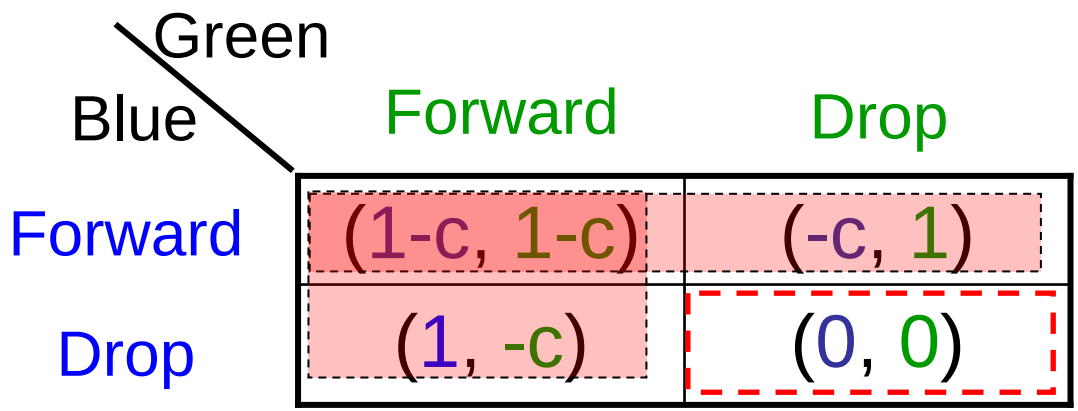
$s_{-i} \in S_{-i}$ strategies of all players except player i

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:



BUT

Drop ***strictly dominates*** Forward

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

} Dilemma

Nash equilibrium

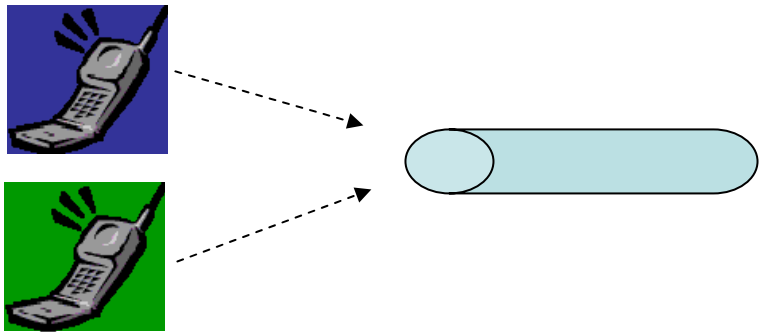
Nash Equilibrium: no player can increase his utility by deviating unilaterally

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



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**

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

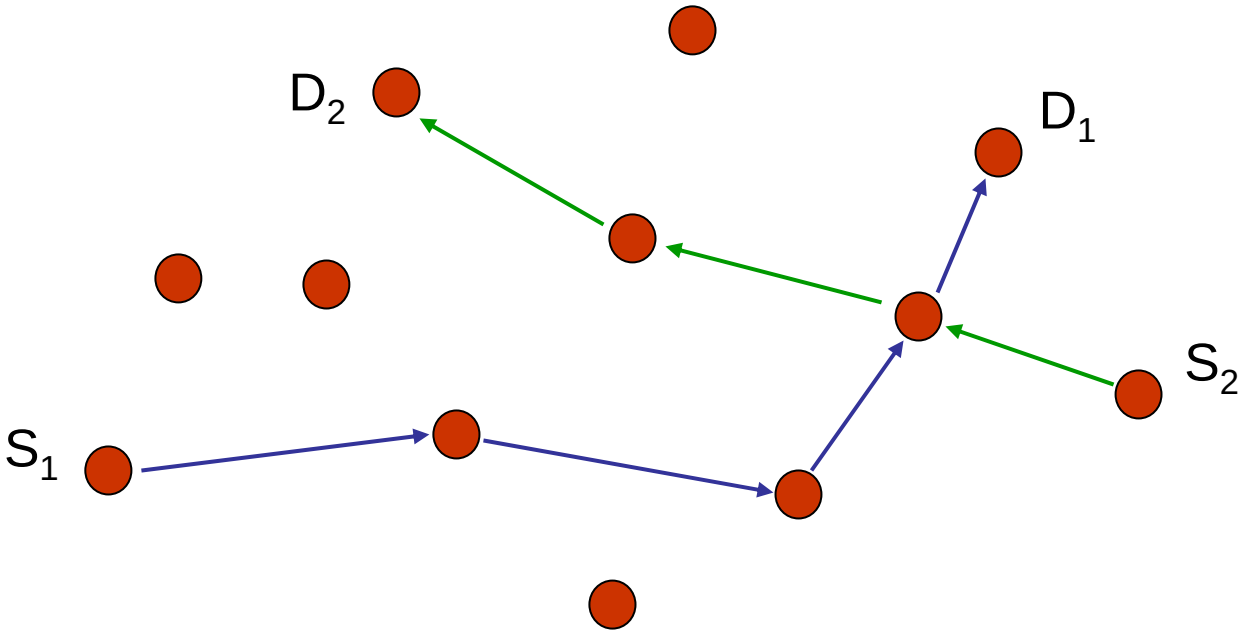
The access point is *trusted*

Well-behaved node

Cheater

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

3.2 Enforcing packet forwarding

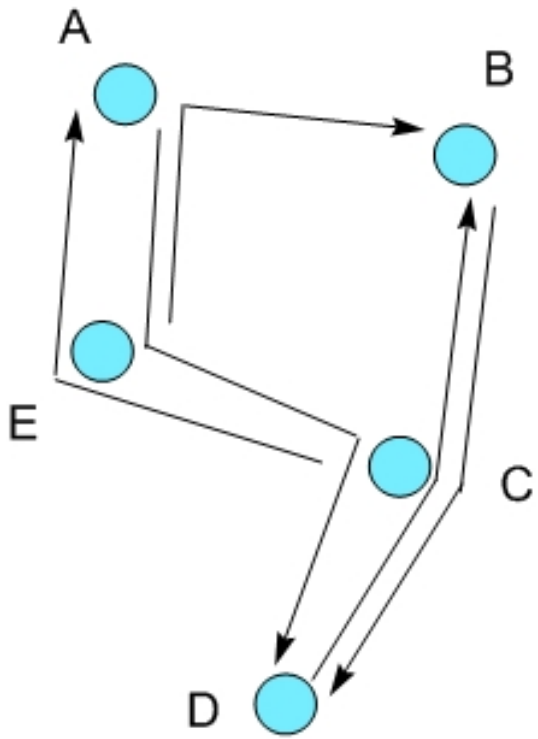


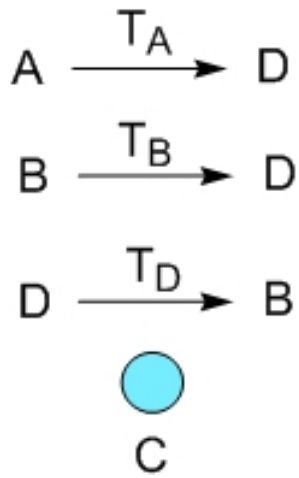
Usually, the devices are assumed to be cooperative.
But what if they are not, and there is no incentive to cooperate?

- 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



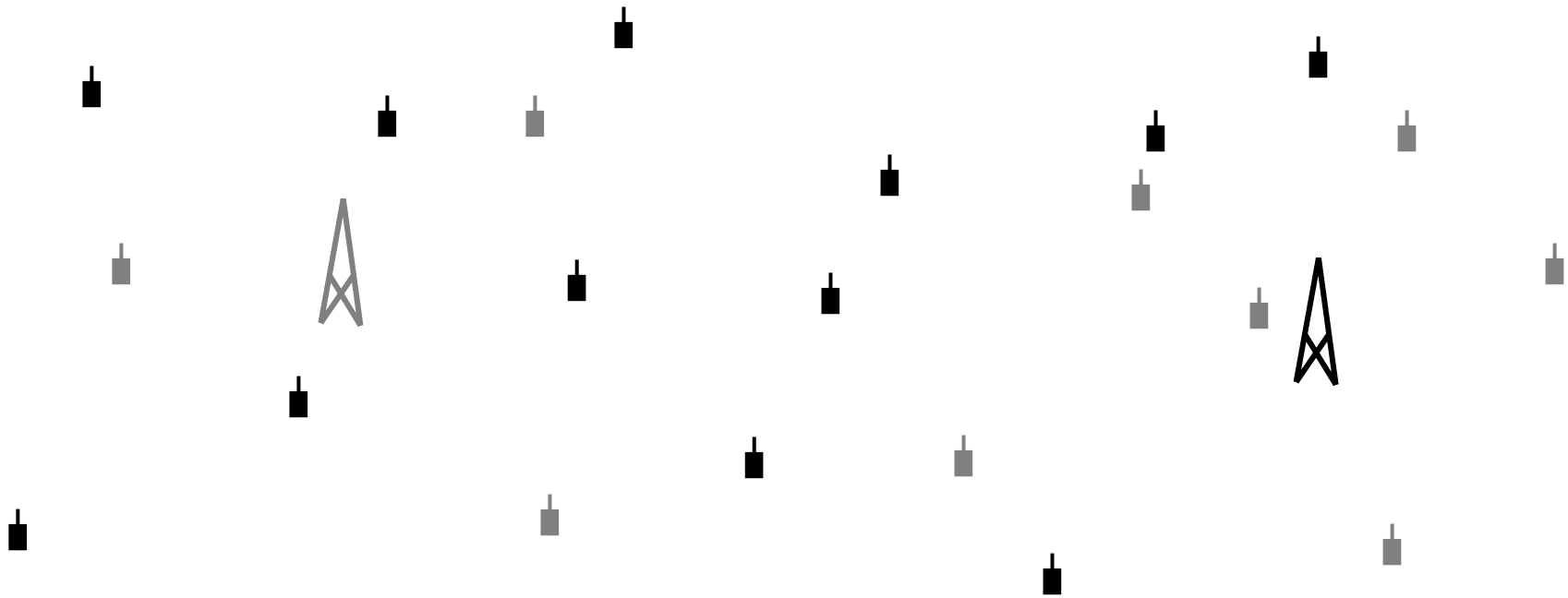


Strategy: cooperation level

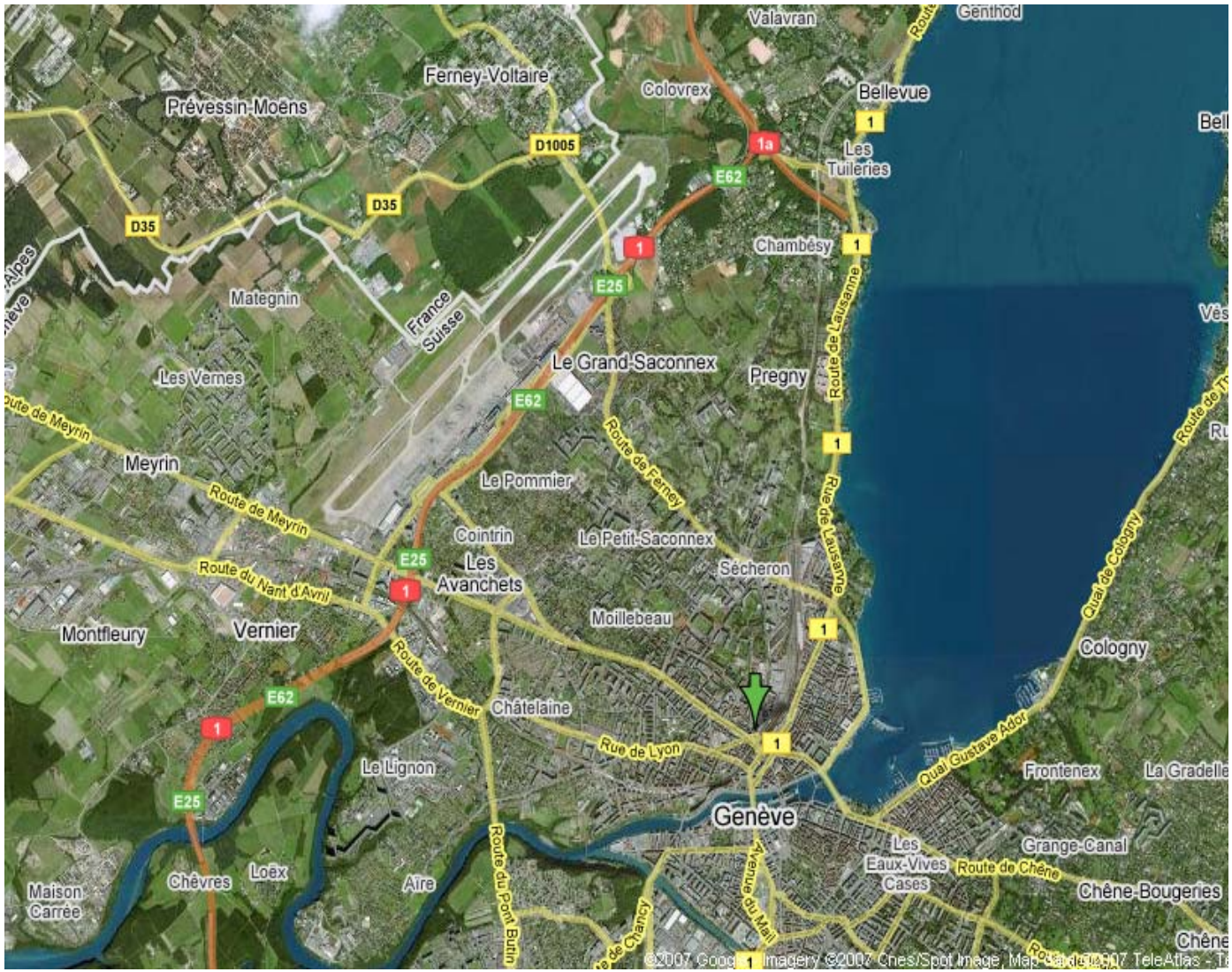
Payoff of node i: proportion of packets sent by node i reaching their destination

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?

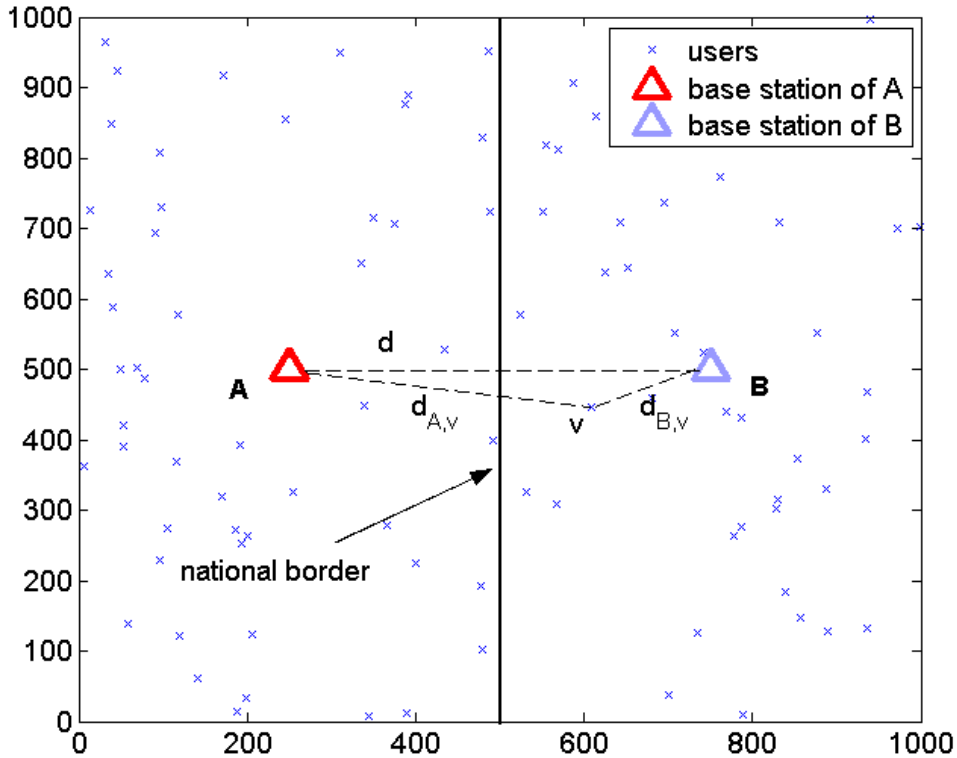


3.3 Border games of cellular operators (1/3)



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

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

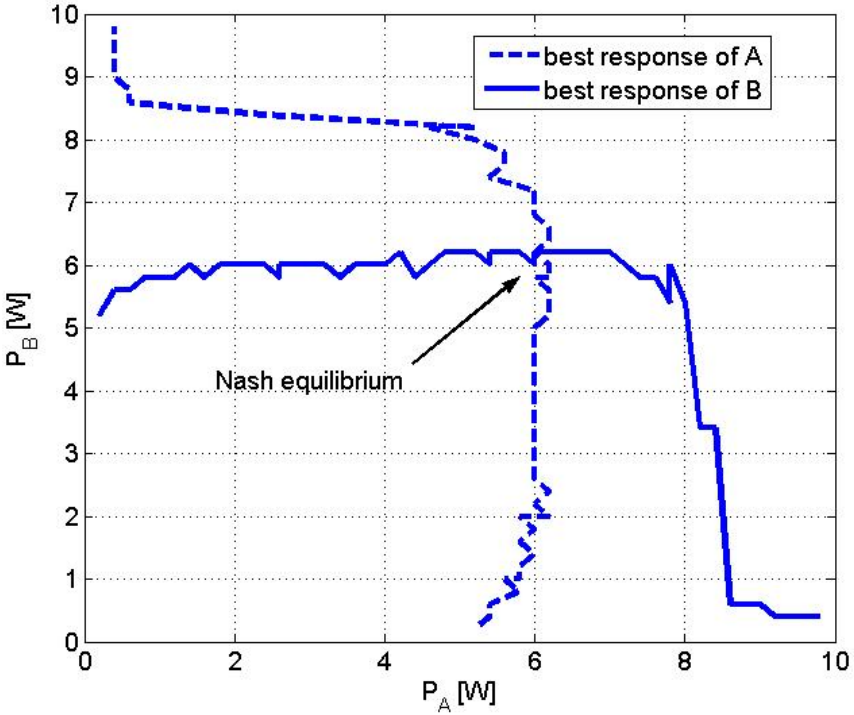
Other-to-own-cell interference

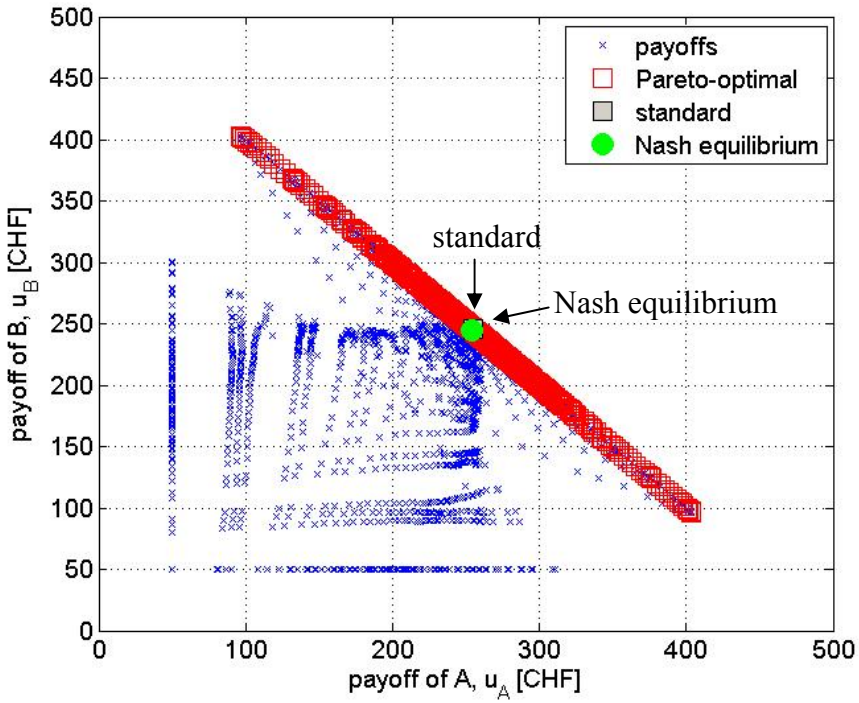
$$I_{other}^{pilot} = \eta \cdot d_{Bv}^{-\alpha} \left(P_B + \sum_{w \in \mathcal{M}_B} T_{Bw} \right)$$

where:
- G_p^{pilot} – pilot processing gain
- P_A – 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
- $\mathcal{M}_A$ – 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





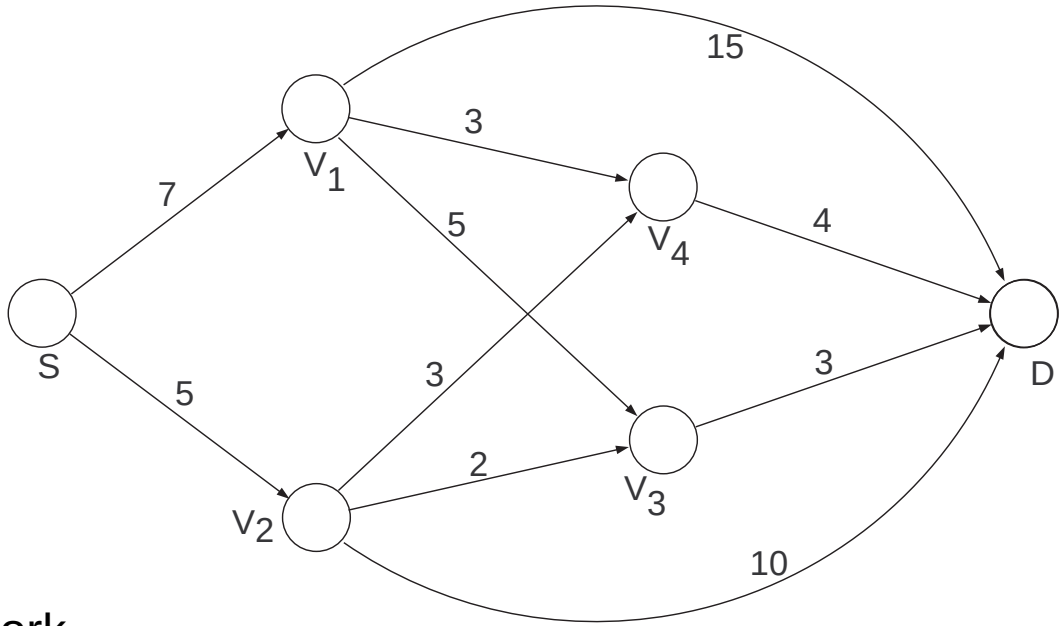
Extended game with power costs = Prisoner's Dilemma

		Player B: P^s	Player B: 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

3.4 Secure protocols for behavior enforcement

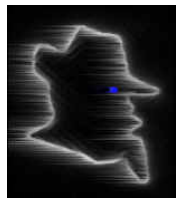


- Self-organized ad hoc network
- Investigation of both routing and packet forwarding

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

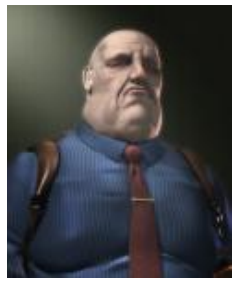
Who is malicious? Who is selfish?

Harm everyone: viruses,…



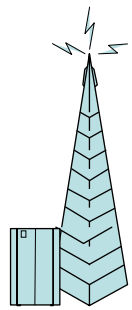
Big brother

Selective harm: DoS,…



Spammer

Cyber-gangster:
phishing attacks,
trojan horses,…



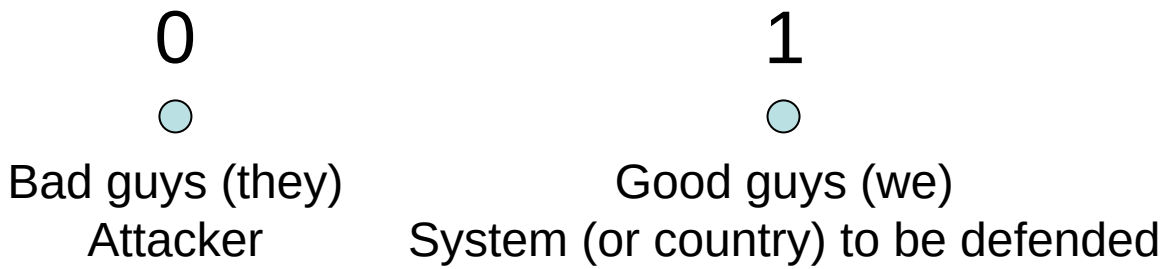
Greedy operator

Selfish mobile station

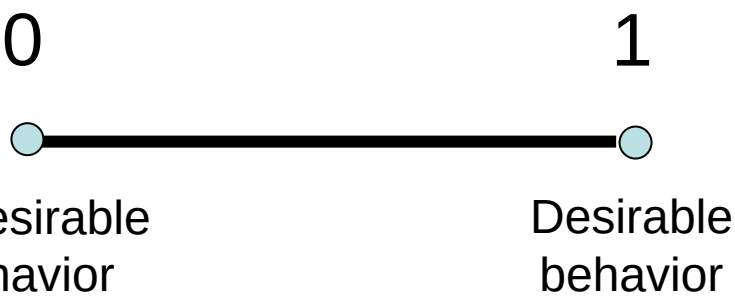
There is no watertight boundary between malice and selfishness
➔ Both security **and** game theory approaches can be useful

From discrete to continuous

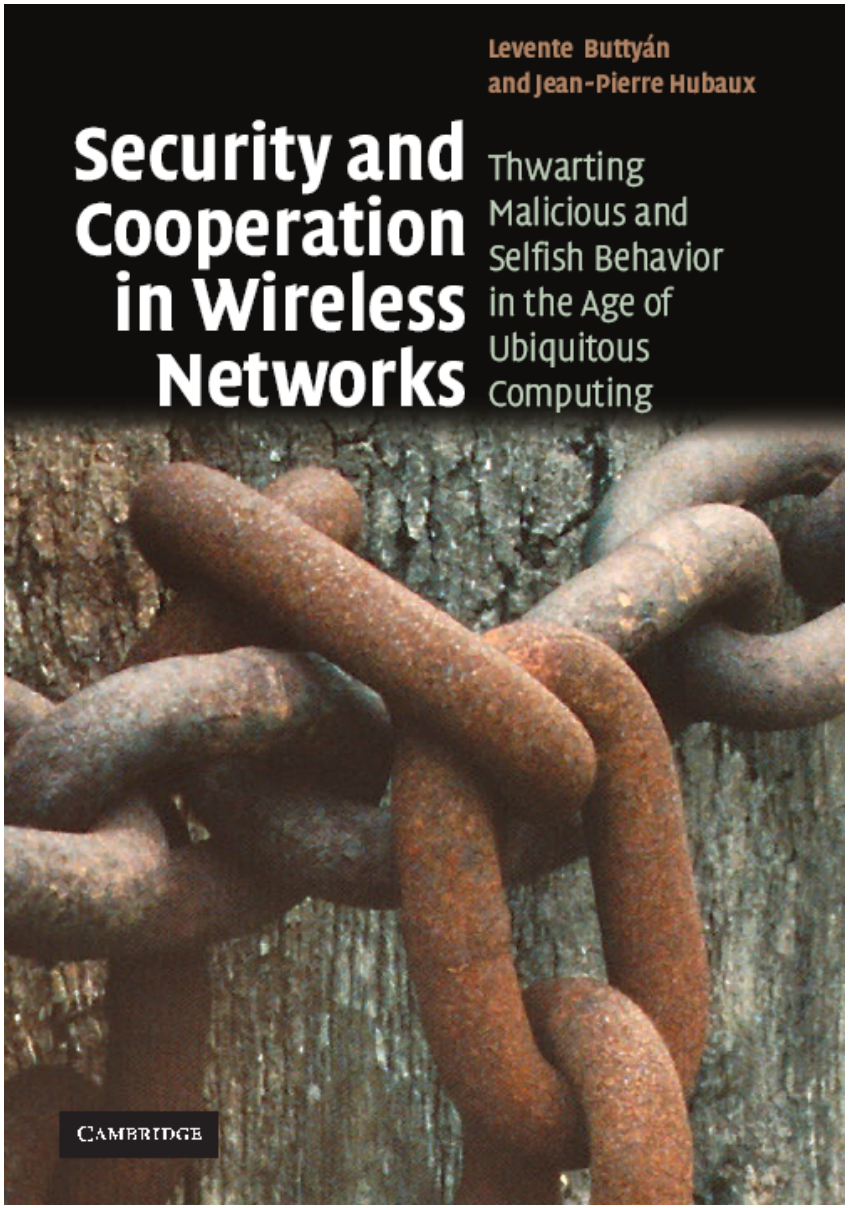
Warfare-inspired Manichaeism:



The more subtle case of commercial applications:



- Security often needs incentives
- Incentives usually must be secured



http://secowinet.epfl.ch

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

Part II

Part III

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

Appendix A: Security and crypto

3. Trust

2. Upcoming networks

1. Existing networks

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

Slides available at http://secowinet.epfl.ch