Security and Cooperation in Wireless Networks

Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing

Jean-Pierre Hubaux
Joint work with
Levente Buttyan

With contributions from N. Ben Salem, M. Cagalj, S. Capkun, M. Felegyhazi, T. Holczer, 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

Network deployment

Observation of new misdeeds (malicious or selfish)

Install security patches (anti-virus, anti-spam, anti-spyware, anti-phishing, firewalls, …)

“The Internet is Broken”
⇒ NSF FIND, GENI, etc.

Where is this going?


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

- Incentive technique based on proof of contribution


- Distributed solution:
  E. Pantelis, A. Frangoudis, and G. Polyzos
  Stimulating Participation in Wireless Community Networks
  INFOCOM 2006

Mesh Networks
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 $\rightarrow$ reverse engineered and compromised, replicated
• Limited capabilities $\rightarrow$ risk of DoS attack, restriction on cryptographic primitives to be used
• Deployment can be random $\rightarrow$ pre-configuration is difficult
• Unattended $\rightarrow$ 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 $\rightarrow$ 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 → Will lose relevance?

• Experience about a given party
  – Based on previous interactions

• Rule enforcement organization
  – Police or spectrum regulator

• 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

<table>
<thead>
<tr>
<th>Upcoming wireless networks</th>
<th>Rule enforcement mechanisms</th>
<th>Naming and addressing</th>
<th>Security associations</th>
<th>Securing neighbor discovery</th>
<th>Secure routing</th>
<th>Privacy</th>
<th>Enforcing fair MAC</th>
<th>Enforcing Pkt F/Wing</th>
<th>Discouraging greedy op.</th>
<th>Behavior enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small operators, community networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Cellular operators in shared spectrum</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Mesh networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Hybrid ad hoc networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Self-organized ad hoc networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Vehicular networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>Sensor networks</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>

Security Cooperation
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))

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

2.2 Pairwise key establishment in sensor networks

1. Initialization

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

Key reservoir (k keys)

2. Deployment

Do we have a common key?

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*
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):

- 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_{KH_A}, (, ,)]
E → *: [req, A, H, h(E|MAC_{KH_A}), (E), (MAC_{KH_E})]
F → *: [req, A, H, h(F|h(E|MAC_{KH_A})), (E, F), (MAC_{KE_F}, MAC_{KF_F})]
H → F: [rep, H, A, (E, F), (MAC_{KE_F}, MAC_{KF_F}), MAC_{KH_A}, (, )]
F → E: [rep, H, A, (E, F), (MAC_{KE_E}, MAC_{KF_E}), MAC_{KH_A}, (K_{E})]
E → A: [rep, H, A, (E, F), (MAC_{KE_F}, MAC_{KF_F}), MAC_{KH_A}, (K_{F}, K_{E})]

A → B: [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, F
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]
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, ...)
(5) T broadcasts RREP; V_3;
(6) V_3 broadcasts RREP; V_2;
(7) V_2 broadcasts RREP; V_1;
(8) V_1 broadcasts RREP; S;

Q_SEQ: Query Sequence Number
Q_ID : Query Identifier

More on secure routing

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

Papadimitratos and Haas: Secure Single Path (SSP) and Secure Multi-path (SMT) protocols,

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

2.6 Secure positioning

http://www.syssec.ethz.ch/research/spot
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: \( \text{1} \)
  • Cost of packet forwarding: \( c \) \((0 < c << 1)\)

• Strategic-form representation

<table>
<thead>
<tr>
<th></th>
<th>Green</th>
<th>Blue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>((1-c, 1-c))</td>
<td>((-c, 1))</td>
</tr>
<tr>
<td>Drop</td>
<td>((1, -c))</td>
<td>((0, 0))</td>
</tr>
</tbody>
</table>

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:
\[
    u_i \in U \quad \text{utility function of player } i
\]
\[
    s_{-i} \in S_{-i} \quad \text{strategies of all players except player } i
\]

In Example 1, strategy Drop strictly dominates strategy Forward

<table>
<thead>
<tr>
<th></th>
<th>Green</th>
<th>Blue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward</td>
<td>((1-c, 1-c))</td>
<td>((-c, 1))</td>
</tr>
<tr>
<td>Drop</td>
<td>((1, -c))</td>
<td>((0, 0))</td>
</tr>
</tbody>
</table>
Solving the Forwarder’s Dilemma (2/2)

Solution by iterative strict dominance:

<table>
<thead>
<tr>
<th></th>
<th>Forward</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>(1-c, 1-c)</td>
<td>(-c, 1)</td>
</tr>
<tr>
<td>Blue</td>
<td>(1, -c)</td>
<td>(0, 0)</td>
</tr>
</tbody>
</table>

BUT Drop \textit{strictly dominates} Forward
Forward would result in a \textit{better outcome}

The Forwarder’s Dilemma

Nash equilibrium

\textbf{Nash Equilibrium}: no player can increase his utility by deviating unilaterally

<table>
<thead>
<tr>
<th></th>
<th>Forward</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>(1-c, 1-c)</td>
<td>(-c, 1)</td>
</tr>
<tr>
<td>Blue</td>
<td>(1, -c)</td>
<td>(0, 0)</td>
</tr>
</tbody>
</table>

(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)

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?


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
Concept of dependency graph

**Dependency:** the benefit of each source is dependent on the behavior of its forwarders

Analytical Results (1/3)

**Theorem 1:** If node $i$ does not have any dependency loops, then its best strategy is AllD.

**Theorem 2:** If node $i$ has only non-reactive dependency loops, then its best strategy is AllD.

**Corollary 1:** If every node plays AllD, it is a Nash-equilibrium.
Analytical results (2/3)

**Theorem 3 (simplified):** Assuming that node \( i \) is a forwarder, its behavior will be cooperative only if it has a dependency loop with each of its sources.

**Corollary 2:** If Theorem 3 holds for every node, it is a Nash-equilibrium.

Example in which Corollary 2 holds:

![Network Diagram](chart.png)

Analytical Results (3/3)

**Theorem 3 (complete):** Assuming that node \( i \) is a forwarder, the best strategy for node \( i \) is TFT, if:

- Node \( i \) has a dependency loop with all of its sources,
- Node \( i \) has a dependency loop with each of its sources,
- \( \frac{b_i(T)}{|F_i|} \cdot T_i \cdot \delta^{d_{\text{src}(r)}} > T_{\text{src}(r)} \cdot C \)

where:

- \( b_i(T) \) – derivative of the benefit function at \( T_i \)
- \( T_i \) – traffic sent by node \( i \)
- \( \delta \) – discounting factor
- \( \text{src}(r) \) – source of a route on which node \( i \) is a forwarder
- \( d_{\text{src}(r)} \) – length of the shortest dependency loop with source \( \text{src}(r) \)
- \( F_i \) – set of routes where node \( i \) is a forwarder
- \( C \) – unit cost of forwarding
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 (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

\[ \text{SINR}_{A\nu}^{\text{pilot}} = \frac{G_p^{\text{pilot}} \cdot P_A \cdot d_{A\nu}^{-n}}{N_0 \cdot W + I_{\text{own}}^{\text{pilot}} + I_{\text{other}}^{\text{pilot}}} \]

Own-cell interference

\[ I_{\text{own}}^{\text{pilot}} = \xi \cdot d_{A\nu}^{-n} \left( \sum_{w \in \mathcal{M}_A} T_{Aw} \right) \]

Other-to-own-cell interference

\[ I_{\text{other}}^{\text{pilot}} = \eta \cdot d_{A\nu}^{-n} \left( P_A + \sum_{w \in \mathcal{M}_A} T_{Aw} \right) \]

where:

- \( G_p^{\text{pilot}} \) - pilot processing gain
- \( P_A^{p} \) - pilot signal power of BS A
- \( d_{A\nu}^{-n} \) - path loss between A and \( \nu \)
- \( \xi \) - own-cell interference factor
- \( \eta \) - 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

- Unique and Pareto-optimal Nash equilibrium
- Higher pilot power than in the standard \( P^A = 2W \)
- 10 users in total

Extended game with power costs = Prisoner’s Dilemma

where:

- \( U \) - fair payoff (half of the users)
- \( \Delta \) - 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

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:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad guys (they)</td>
<td>Good guys (we)</td>
</tr>
<tr>
<td>Attacker</td>
<td>System (or country) to be defended</td>
</tr>
</tbody>
</table>

The more subtle case of commercial applications:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undesirable behavior</td>
<td>Desirable behavior</td>
</tr>
</tbody>
</table>

- Security often needs incentives
- Incentives usually must be secured
### Book structure (1/2)

<table>
<thead>
<tr>
<th>Security and cooperation mechanisms</th>
<th>Upcoming wireless networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small operators, community networks</td>
<td>X</td>
</tr>
<tr>
<td>Cellular operators in shared spectrum</td>
<td>X X</td>
</tr>
<tr>
<td>Mesh networks</td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>Hybrid ad hoc networks</td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>Self-organized ad hoc networks</td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>Vehicular networks</td>
<td>X X X X X X X X X</td>
</tr>
<tr>
<td>Sensor networks</td>
<td>X X X X X X X X X</td>
</tr>
</tbody>
</table>

### Book structure (2/2)

#### Security

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

#### Cooperation

- 12. Behavior enforcement
- 11. Operators in shared spectrum
- 10. Selfishness in PKT FWing
- 9. Selfishness at MAC layer

**Part I**

1. Existing networks

**Part II**

2. Upcoming networks

**Part III**

3. Trust

**Appendix A:** Security and crypto

**Appendix B:** Game theory
Another book:
Cognitive Wireless Networks: Concepts, Methodologies and Visions
- Inspiring the Age of Enlightenment of Wireless Communications –
Edited by Frank H. P. Fitzek and Marcos D. Katz

Part I: Introductory Chapter
Part II: Cooperative Networks: Social, Operational and Communicational Aspects
Part III: Cognitive Networks
Part IV: Marrying Cooperation and Cognition in Wireless Networks
Part V: Methodologies and Tools
Part VI: Visions, Prospects and Emerging Technologies

List of Contributors
Aachen University, Germany
AIST, Japan
Budapest University of Technology and Economics, Hungary
Create-NET, Italy
DcCoMo Euro-Labs, Germany
EPFL, Switzerland
Harvard University, USA
Konica Italia, Italy
KTH, Sweden
MIT, USA
Motorola Labs, France
Oxford University, UK
Stevens Institute of Technology, USA
Technical University of Catalonía, Spain
Technical University of Denmark, Denmark
Universität Duisburg Essen, Germany
Universität Karlsruhe, Germany
University of Aalborg, Denmark
University of Bologna, Italy
University of California at Berkeley, USA
University of California, San Diego, USA
University of Dresden, Germany
University of Paderborn, Germany
University of Padova, Italy
University of Piraeus, Greece
VTT, Finland
WINLAB and Rutgers University, USA
Part V: Methodologies and Tools

1. Cooperation for Cognitive Networks: A Game Theoretic Perspective  
   C. Comaniciu, Stevens Institute of Technology, USA

2. Spectrum Sharing Games of Network Operators and Cognitive Radios  
   (EPFL)

   F. Albiero, VTT, Finland

---

Spectrum sharing games

- Unlicensed Band Devices
  - Heterogeneous wireless systems  
    (University of California at Berkeley)  
  - Wifi Operators (Bell LAB, MIT)
- Cognitive Radios
  - Opportunistic spectrum sharing (UCSB)
  - Auction based spectrum sharing (Northwestern)
- Cellular Operators
  - WAN-WiFi competition/cooperation  
    (University of Texas at Austin)
  - Cellular operators near national borders (EPFL)
  - Cellular operators in shared spectrum (EPFL)
- Licensed Band

---
Panel at Mobicom 2007
(Montreal, September 9 – 15)

Bonobos Vs Chimps: Cooperative and Non-Cooperative Behavior in Wireless Networks

Panelists:
Jean-Pierre Hubaux, EPFL (organizer and moderator)
Ramesh Johari, Stanford University
P. R. Kumar, UIUC
Joseph Mitola, MITRE Corp.
Heather Zheng, UCSB

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