بسم الله الرحمن الرحيم

Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei

manshaei@gmail.com

Teaching Team and Resources

- Instructor:
  - Mohammad Hossein Manshaei
- Course web page available at IUT Web Course (http://ivut.iut.ac.ir/bounce.php?course=765)
  - Slides
  - Ebook
  - Miniprojects
- Any Question: Please drop me an email to make an appointment!

Organization

- Lectures
- Midterm Presentations
  - Short presentation about your project (10 min)
  - Selected topics in security and privacy of wireless networks
- Final Exam
  - Oral + Written
- Mini Projects Report/Presentations
- Grading

Exams and Grading

- Final exam (Oral + Written): 50%
- Midterm Presentation: 10%
- Mini Projects + Presentations: 45%

  - Hence, 5% bonus ☺

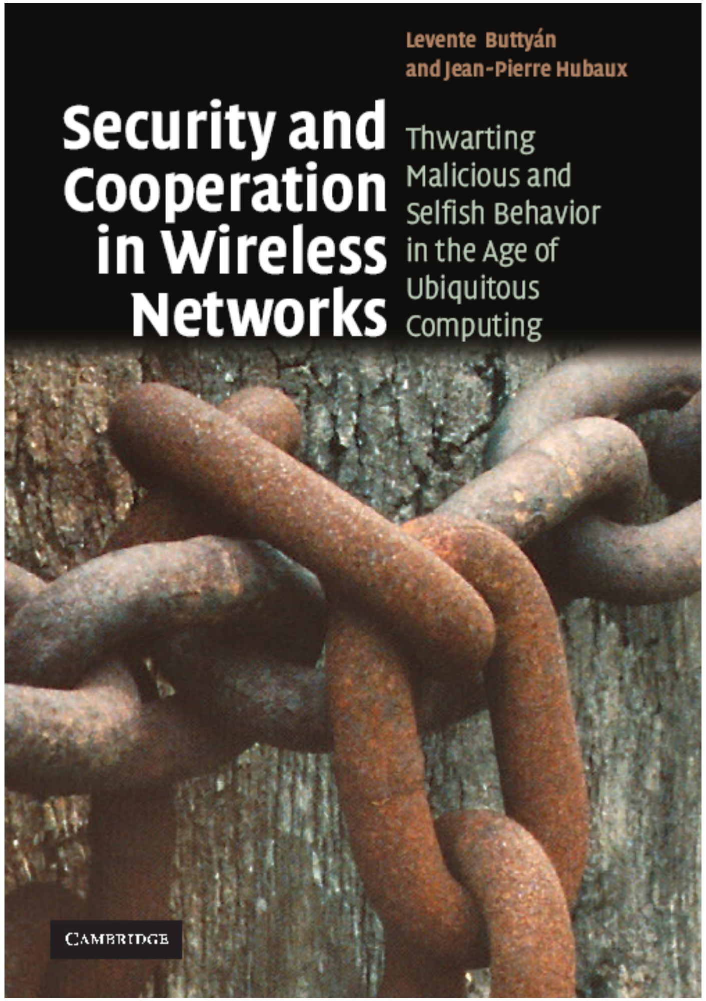
Textbook

Security and Cooperation in Wireless Networks

Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing

Levente Buttyan and Jean-Pierre Hubaux

Cambridge Press
2007


Levente Buttyán and Jean-Pierre Hubaux
Security and Cooperation in Wireless Networks
Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing
CAMBRIDGE

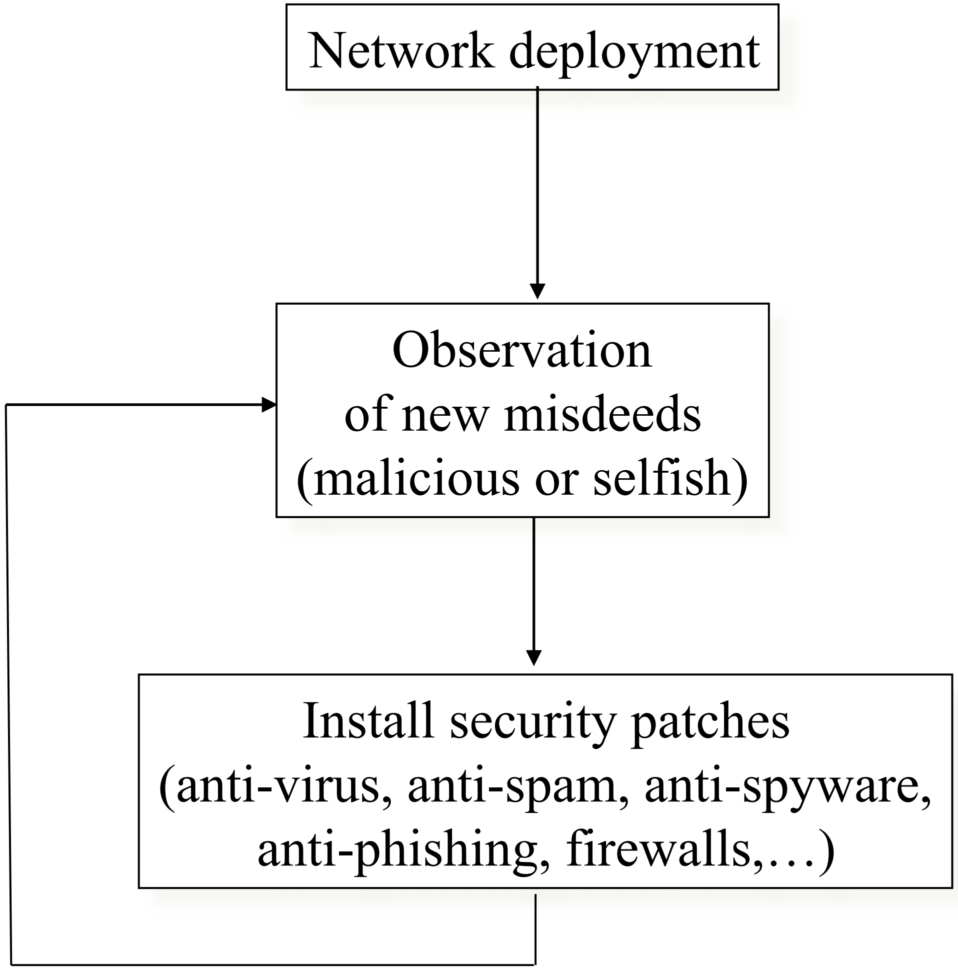
http://secowinet.epfl.ch

Contents:

- Introduction
- Thwarting malicious behavior
- Thwarting selfish behavior

Why Wireless Security and Privacy?

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,…)

EMERGING TECHNOLOGIES AND THEIR IMPACT
December 2005/January 2006
www.technologyreview.com

Imaging Brain Disorders
By Paul Raeburn p70

China's Great Experiment
By Horace Freeland Judson p52

Should You Trust Gmail?
By Simson Garfinkel p76

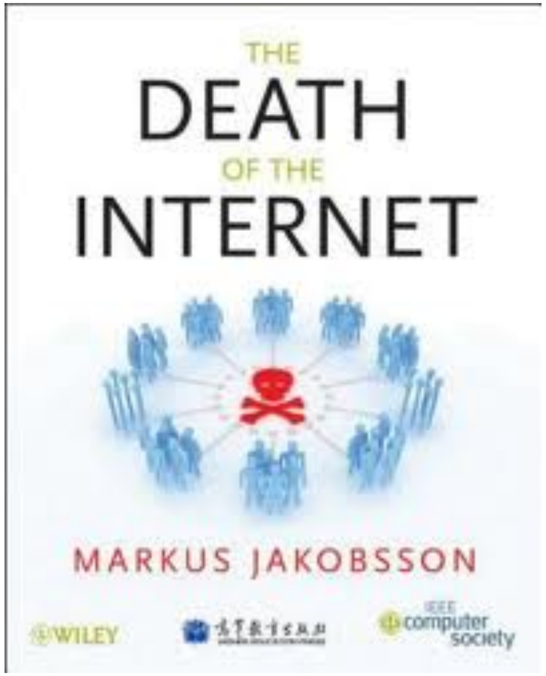
Technology Review
AN MIT ENTERPRISE

The Internet Is Broken
It's time to replace it.
BY DAVID TALBOT
Page 62

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

The Death of the Internet

Markus Jakobsson



Fraud poses a significant threat to the Internet. 1.5% of all online advertisements attempt to spread malware. This lowers the willingness to view or handle advertisements, which will severely affect the structure of the web and its viability. It may also destabilize online commerce. In addition, the Internet is increasingly becoming a weapon for political targets by malicious organizations and governments. This book will examine these and related topics, such as smart phone based web security. This book describes the basic threats to the Internet (loss of trust, loss of advertising revenue, loss of security) and how they are related. It also discusses the primary countermeasures and how to implement them.

Where is this going ?

MIT Technology Review,
Dec. 2005 – Jan. 2006

The Economist, April 28, 2007

The Economist
Meet Britain's next prime minister
Will Africa ever get it right?
In praise of Yeltsin
The world's biggest banking battle
Australia's water crisis
APRIL 28TH–MAY 4TH 2007
www.economist.com
When everything connects
A 14-page special report on the coming wireless revolution

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/SDR
  - LTE
  - MIMO
  - Ultra Wide Band
  - Directional antennas
  - …

Community networks

Example: service reciprocation in community networks

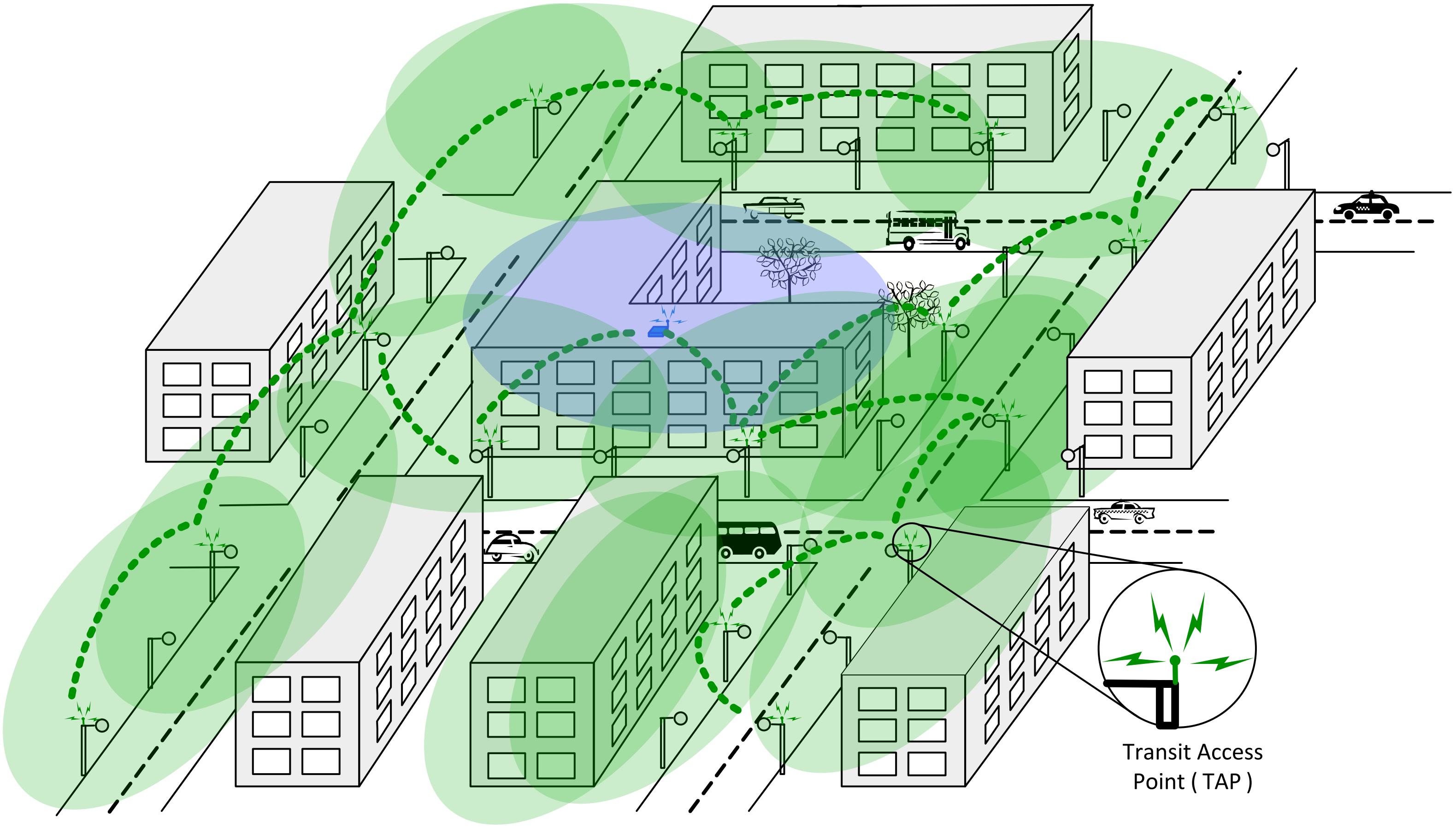
Example: FON

- 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

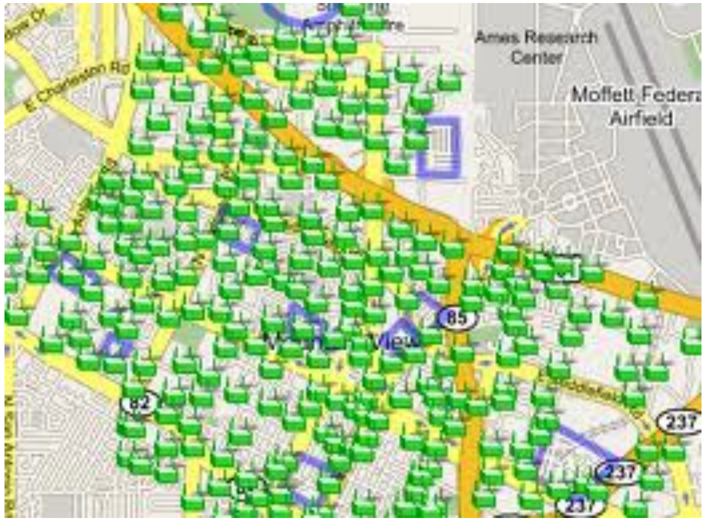
  - That the number of “Foneros” is around 7 millions

Mesh Networks



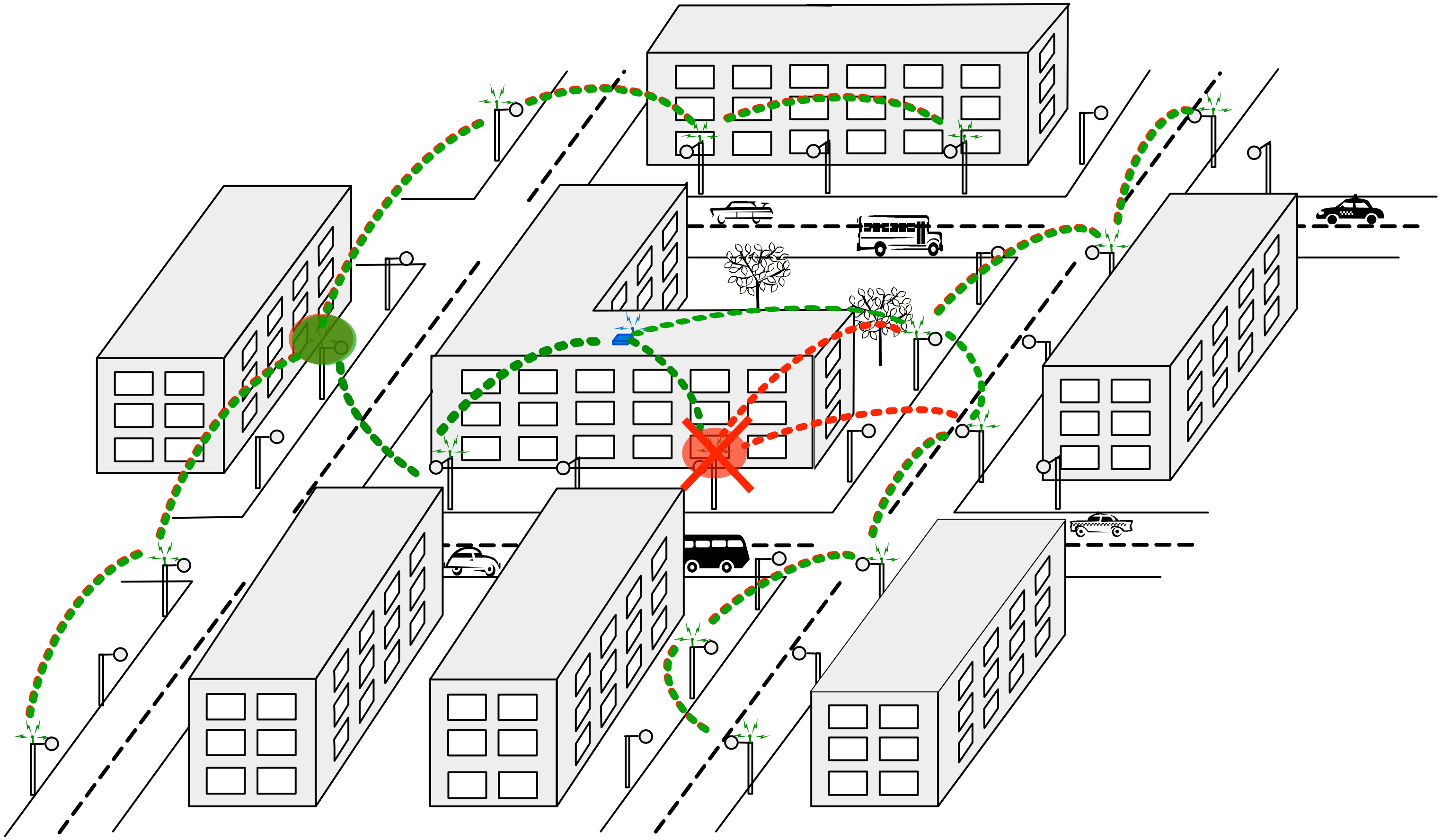
Each node must not only **capture** and **disseminate** its **own data**, but also serve as **a relay for other nodes**, that is, it must collaborate to propagate the data in the network

Example: Mountain View Google

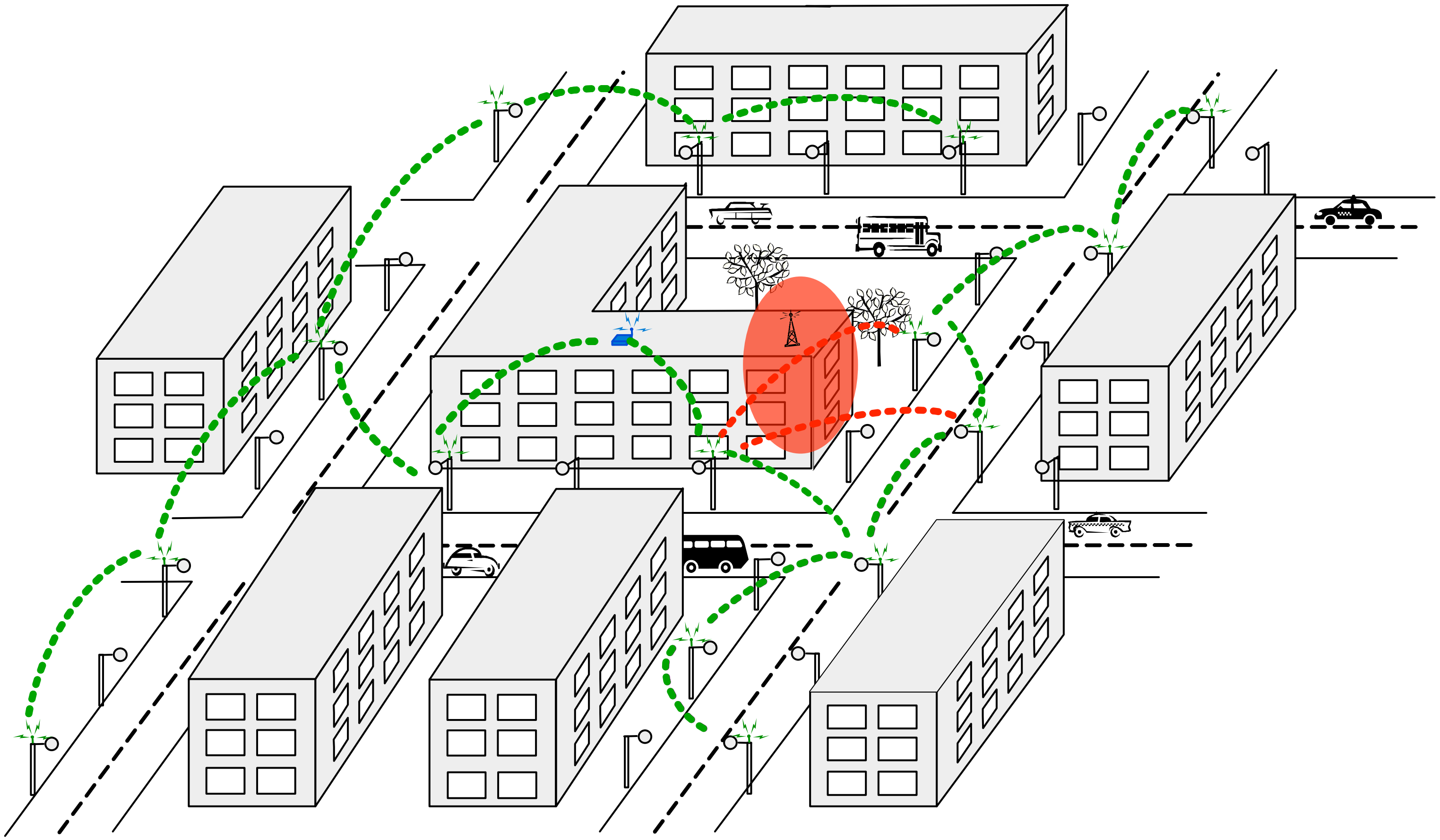


- 500 Tropos Networks MetroMesh routers (2009)
- 95% of the city's area of 12 square miles (31 km^2)
- Google WiFi only requires its end users have a Google Account
- Google offers a free virtual private network (VPN) software client called Google Secure Access (GSA)

Mesh Networks: Node Compromise



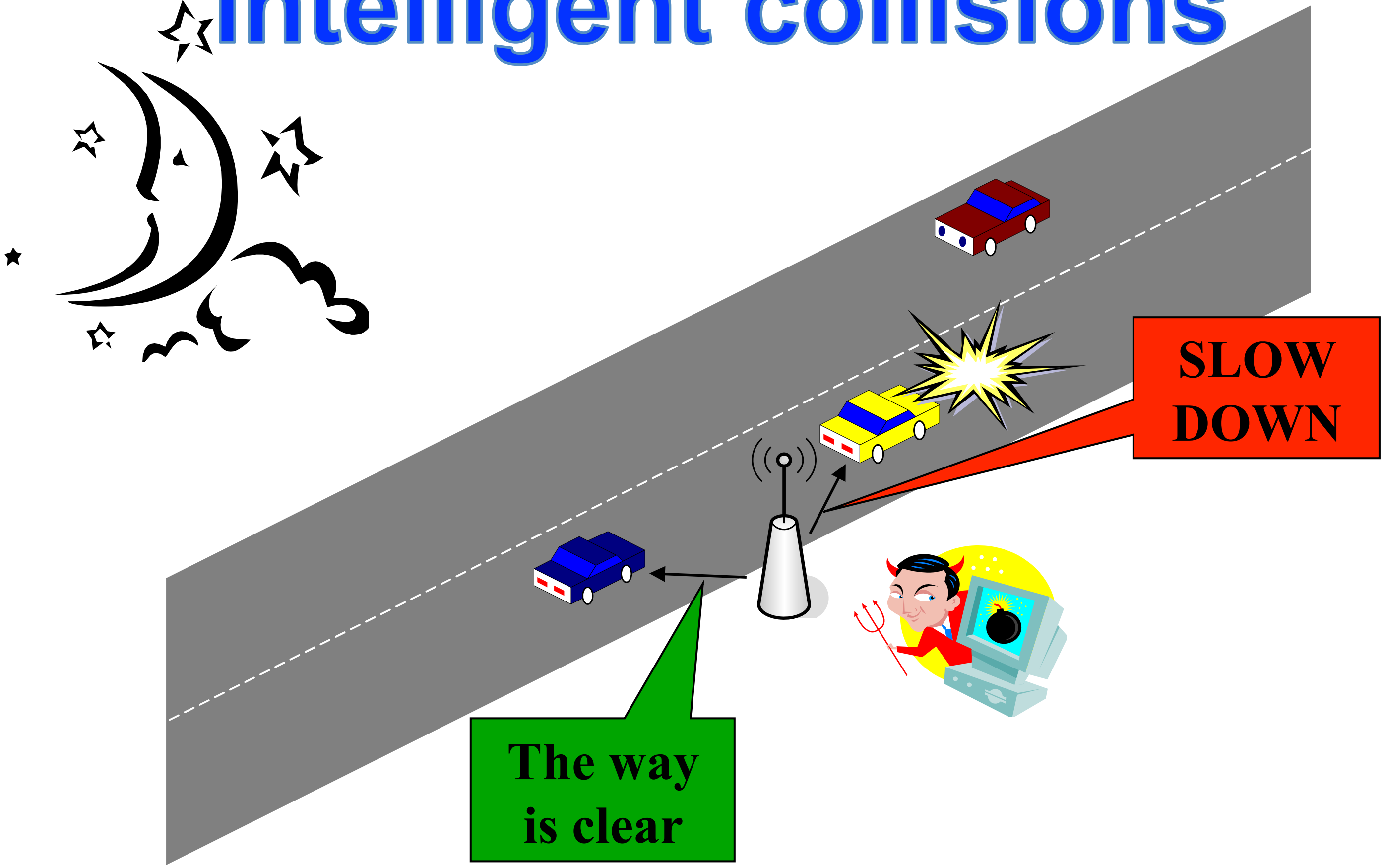
Mesh Networks: Jamming



Vehicular Networks: Why?

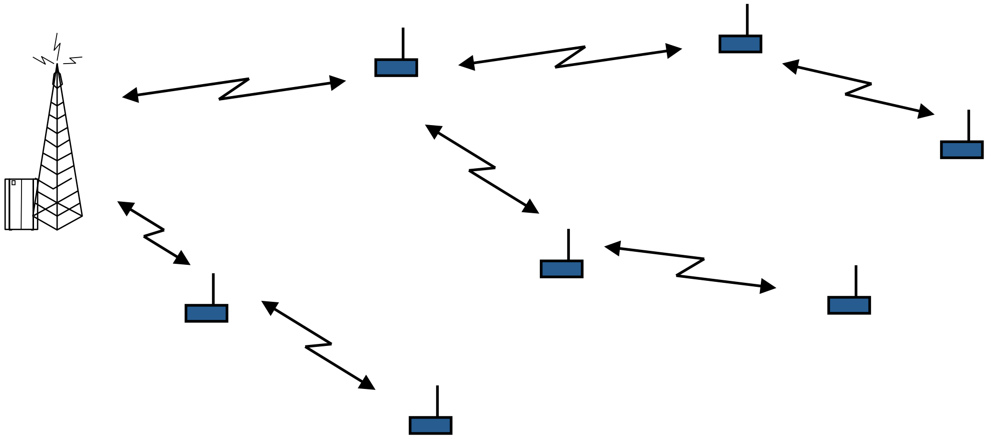
- Combat the awful side-effects of road traffic
  - In the EU, around 40’000 people die yearly on the roads; more than 1.5 millions are injured
  - Traffic jams generate a tremendous waste of time and of fuel
- Most of these problems can be solved by providing appropriate ***information*** to the driver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

Sensor Networks

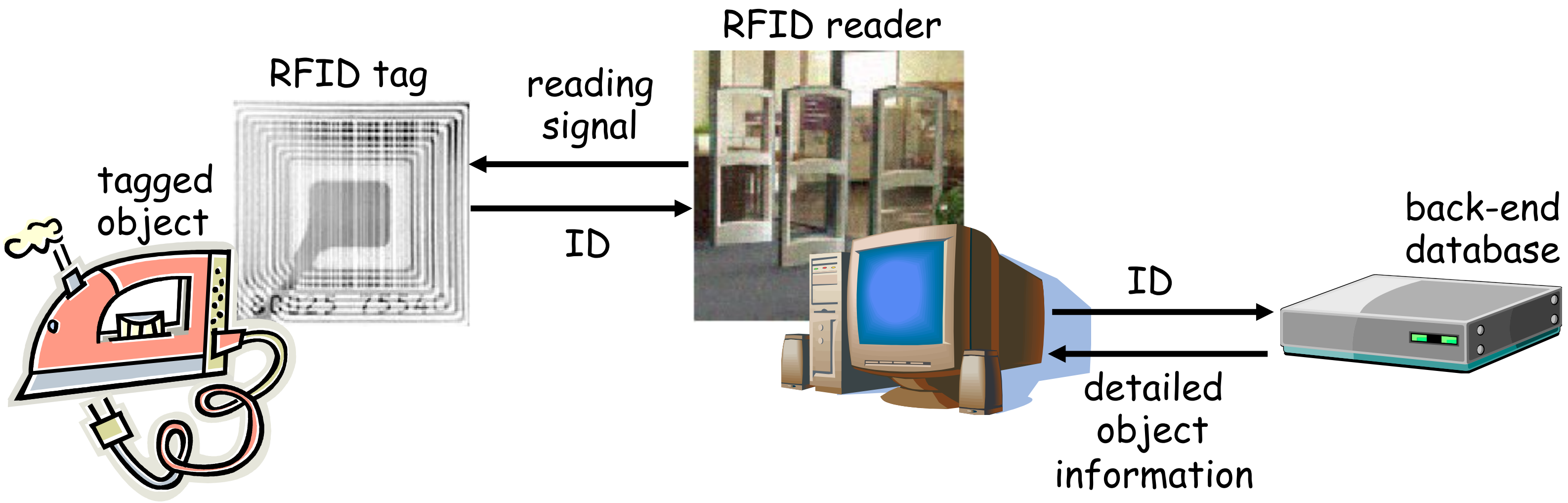


Vulnerabilities:

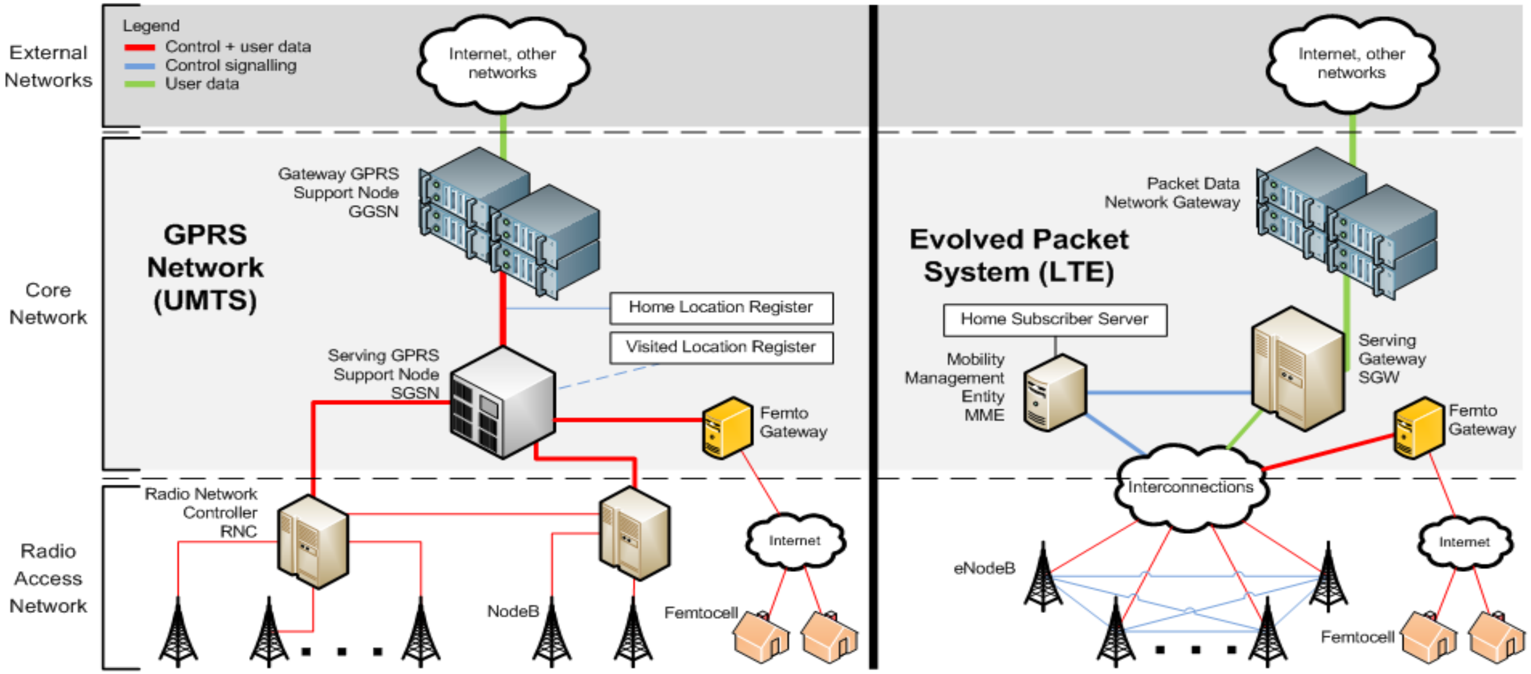
- Theft ➔ reverse engineered and compromised, replicated
- Limited capabilities ➔ risk of DoS attack, restriction on cryptographic primitives to be used
- Deployment can be random ➔ pre-configuration is difficult
- Unattended ➔ some sensors can be maliciously moved around

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



Long Term Evolution (LTE)



iPhone 5
Totally glass capacitive screen on a polycarbonate lightweight body. New design, new core, new camera.
A classic reinvented. Again.
4G LTE
9:42

Lte™

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

… Yet, mobility and wireless can facilitate certain security mechanisms

Let’s review 2 examples!

Physical-layer Identification of RFID Devices

B. Danev, T. S. Heydt-Benjamin, S. Capkun
ETH Zurich, Switzerland
USENIX Security Symposium, 2009

Overview and Motivation

Goal:
Uniquely identify devices based on what they are / what they do.

- Device Identification
  - Logical Layer
  - Physical Layer
- Desirable properties
  - Universality
  - Uniqueness
  - Collectability

Physical Layer Identification

- The main goal is to uniquely characterize a given wireless device
- **Based on physical-layer characteristics exhibited by the device.**
- Physical-layer variations are due to the variability in manufacturing methods and the hardware components used.

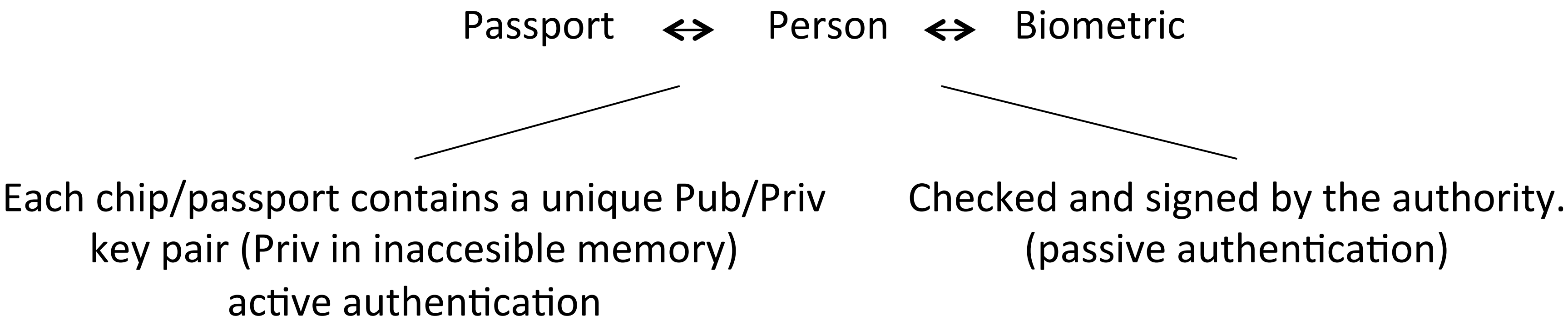
- Reasoning:
  - Hard to change / forge

- Motivation
  - intrusion detection
  - Device cloning detection
  - Message authentication and replay protection
  - Tracking

Problem Statement

– Can we build unique fingerprints of RFID chips?

– *If yes, this could make it more difficult to clone a passport*



Passport ↔ Person ↔ Biometric

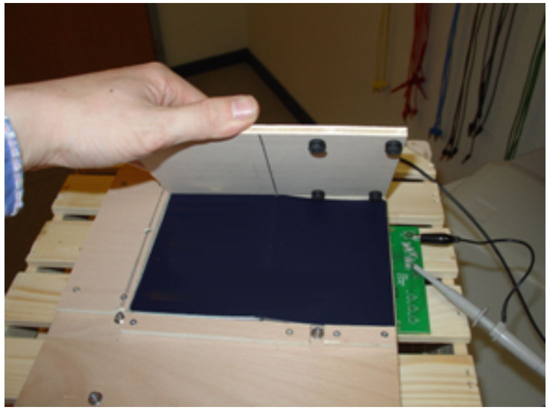
Each chip/passport contains a unique Pub/Priv key pair (Priv in inaccesible memory)
active authentication

Checked and signed by the authority.
(passive authentication)

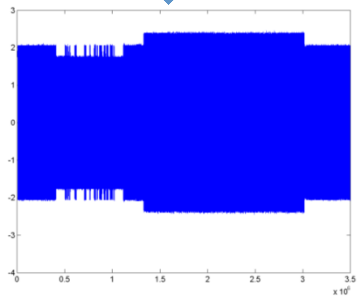
RFID Fingerprinting (1/3)

- Signal Acquisition Setup

Purpose-built HF (13.56MHz) RFID Reader
ISO 14433 Type A and Type B



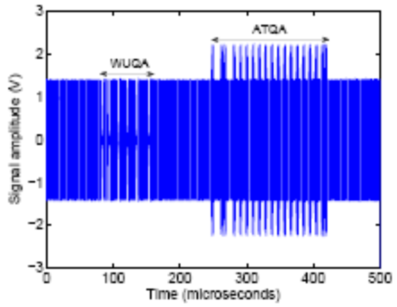
Acquisition antenna setup



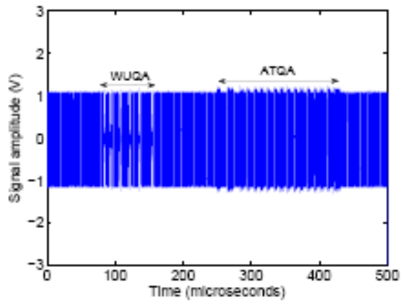
Captured signal transmission

RFID Fingerprinting (2/3)

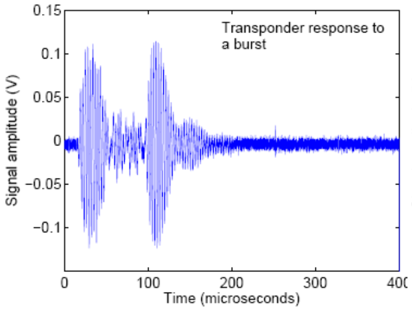
- Experiments performed
  - Experiment 1 (Standard)
    - Fc = 13.56 MHz
  - Experiment 2 (Varied Fc)
    - Fc = 12.86 – 14.36 MHz
  - Experiment 3 (Burst)
    - Sinusoidal burst of RF energy
  - Experiment 4 (Sweep)
    - Sinusoidal frequency sweep of RF energy



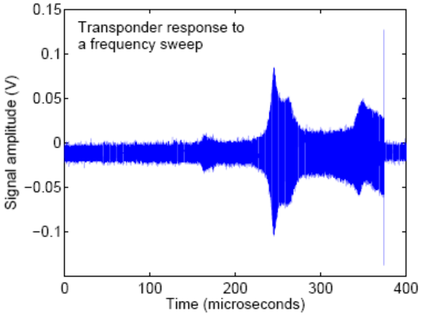
Standard



Varied Fc



Burst

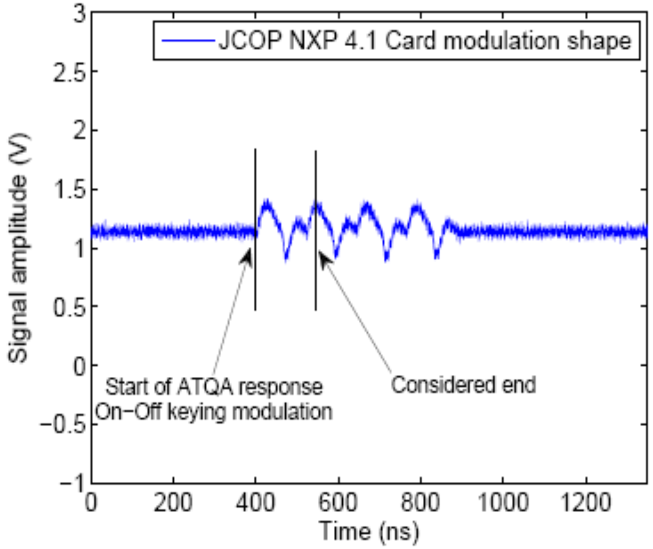


Sweep

RFID Fingerprinting (3/3)

- Timing Features
  - Measuring time between reader query and chip response
  - At different carrier frequency (Fc = 12.86 – 14.36 MHz)

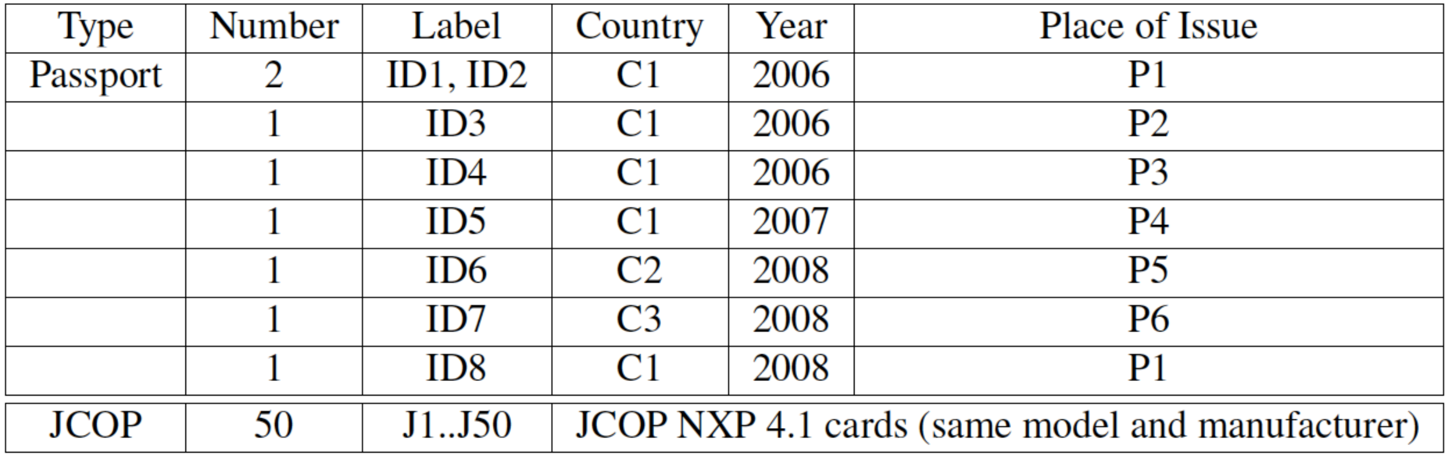
- Modulation-shape Features
  - Type A response is On-Off keying
  - Extract the shape of the On-Off keying by Hilbert transformation



- Spectral Features
  - Extract frequency information
  - Burst and sweep features are selected by means of Fourier transformation and high-dimensional Principal Component Analysis

Experimental Evaluation

- Data Sets: RFID device populations

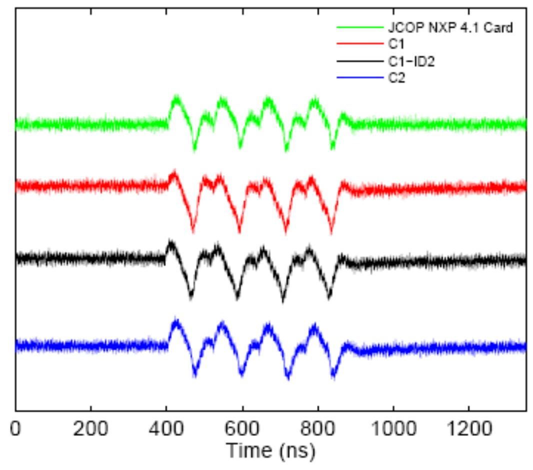


Type	Number	Label	Country	Year	Place of Issue
Passport	2	ID1, ID2	C1	2006	P1
	1	ID3	C1	2006	P2
	1	ID4	C1	2006	P3
	1	ID5	C1	2007	P4
	1	ID6	C2	2008	P5
	1	ID7	C3	2008	P6
	1	ID8	C1	2008	P1
JCOP	50	J1..J50	JCOP NXP 4.1 cards (same model and manufacturer)		

- Evaluating Accuracy
  - Classification (e.g., country of issuance, year, etc)
  - Identification (i.e., identify individual passports)

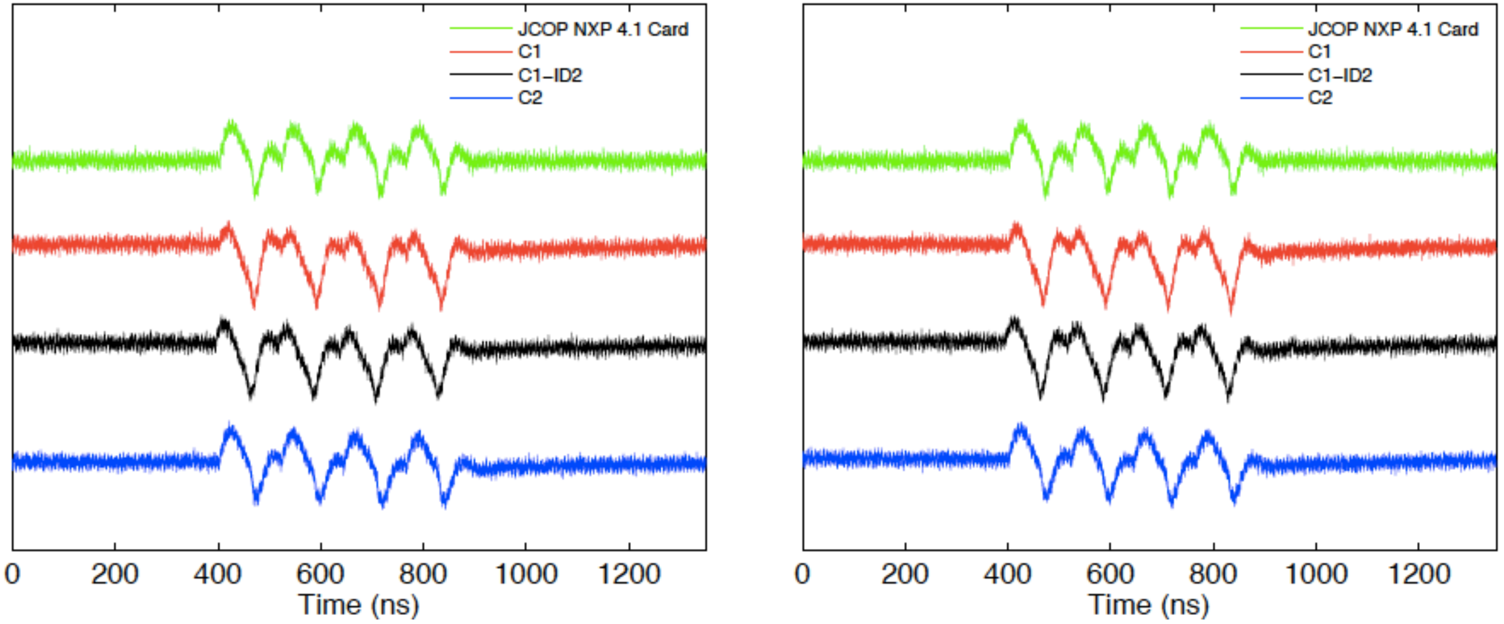
Classification Accuracy

- 4 different classes
  - 8 ePassports from **3** countries + 10 JCOP cards = **4** classes
- Classification accuracy
  - Timing features
    - Very low classification accuracy
    - Each country seems to use RFID chips from same manufacturer. The standard seems well implemented
  - Modulation features
    - High classification accuracy (100%)
    - Different RFID chips?
    - However even passports within same country exhibit differences in the modulation



Classification using Modulation-Shape Features

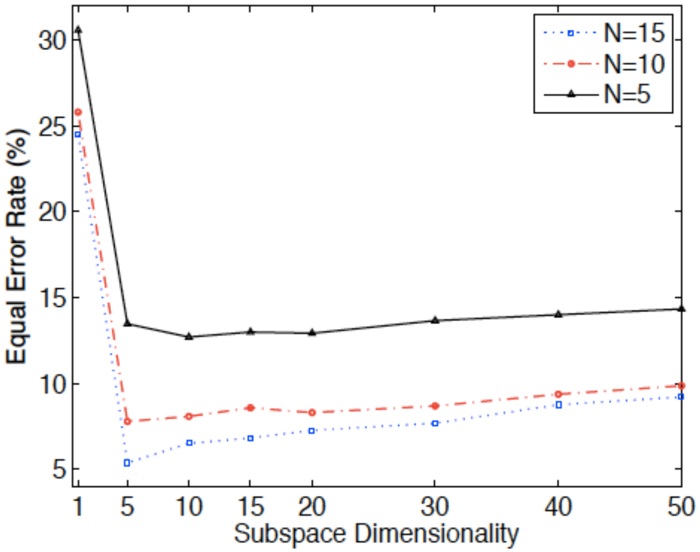
Number of Classes	Class structure	Average Classification Error Rate
3	(C1),(C2),(JCOP)	0%
4	(ID1,ID3,ID4,ID8), (ID2), (ID7), (JCOP)	0%
2	(ID5-C1),(ID6-C3)	0%

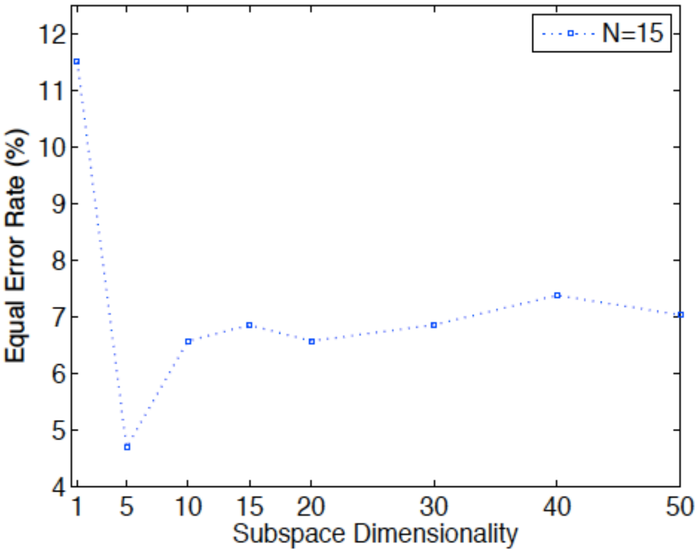


Two-run Experiments

Identification Accuracy(1/2)

- 50 JCOP NXP 41 cards
  - Same model and manufacturer
- Burst and Sweep features
  - Equal Error Rate (EER) = 5% (i.e., 95% accurate identification)





Application to ePassports

- ePassport cloning detection
  - **Scenario 1:** The RFID fingerprint is stored in back-end database
    - Measured before deployment
    - Stored in back-end database, indexed by the ID of the transponder
    - Online verification
  - **Scenario 2:** The RFID fingerprint is stored on the transponder.
    - RFID fingerprint size = 120 bytes.
    - Stored in the chip memory (36/72KB EEPROM in NXP chips)
    - The fingerprint integrity should be ensured, i.e. digitally signed by the document-issuing authority
    - Offline verification
- **Difficulty to circumvent the detection**
  - Obtain the fingerprint template of the passport
  - Produce or find another chip configuration with similar fingerprint

Conclusion

- Active and Passive transponders exhibit unique behavior on the physical layer due to manufacturing variability
- Such variations are inherent to a transponder and are hard to modify at a reasonable cost

Mobility Helps Security in Ad Hoc Networks

Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyàn

4th ACM Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2003)

Does mobility increase or reduce security ?

Mobility is usually perceived as a major security challenge

- Wireless communications
- Unpredictable location of the user/node
- Sporadic availability of the user/node
- Higher vulnerability of the device
- Reduced computing capability of the devices

However, very often, people *gather and move* to increase security

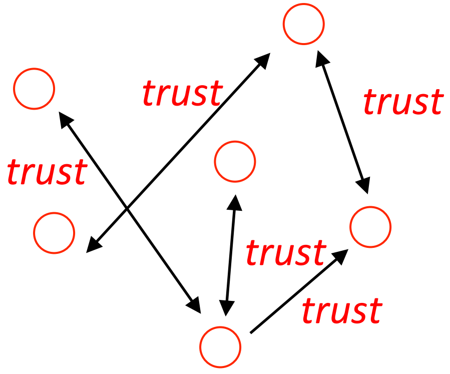
- Face to face meetings
- Transport of assets and documents
- Authentication by physical presence

- In spite of the popularity of PDAs and mobile phones, this mobility has not been exploited to provide digital security
- So far, client-server security has been considered as a priority (e-business)

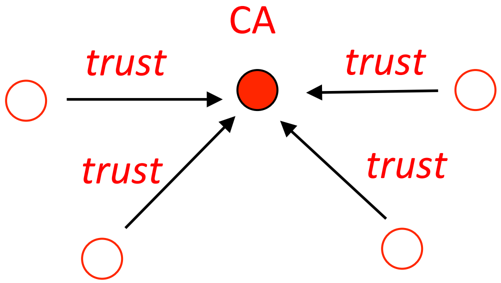
Two Scenarios

- Mobile ad hoc networks with a central authority
    - off-line or on-line authority
    - nodes or authorities generate keys
    - authorities certify keys and node ids
    - authorities control network security settings and membership

- Fully self-organized mobile ad hoc networks
    - no central authority *(not even in the initialization phase !)*
    - each user/node generates its own keys and negotiates keys with other users
    - membership and security controlled by users themselves



Fully self organized



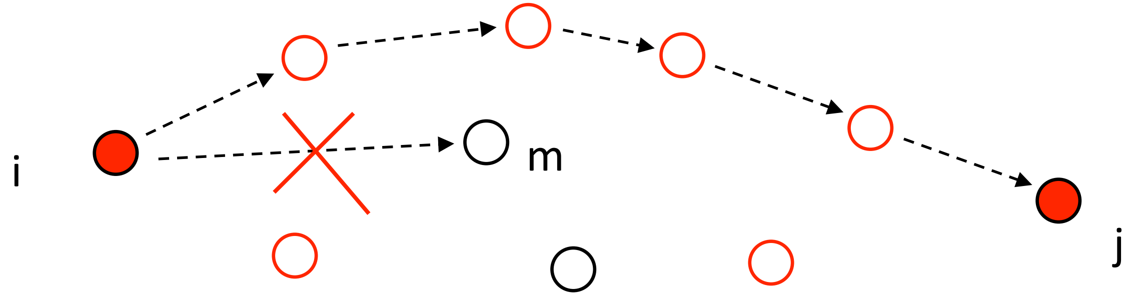
Authority-based

Secure routing requirements and assumptions

- A network controlled by the central authority

- All security associations established between all nodes prior to protocol execution

- The most stringent assumption: Routes are established between nodes with which a source and the destination have security associations



Secure routing proposals

- Securing Ad Hoc Routing Protocols, Zappata, Asokan, WiSe, 2002

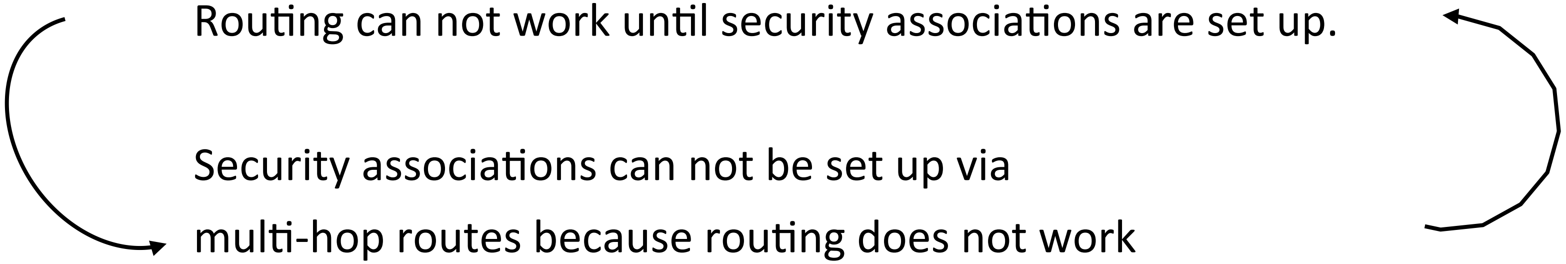
- Ariande, Hu, Perrig, Johnson, MobiCom 2002

- Secure Routing for Ad Hoc Networks, Papadimitratos, Haas CNDS, 2002

- A Secure Routing Protocol for Ad Hoc Networks, Sanzgiri et al. ICNP, 2002

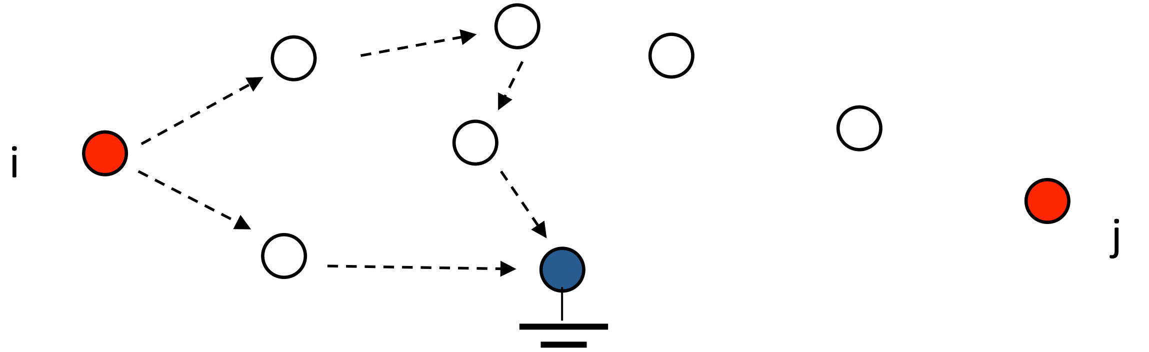
- SEAD, Hu, Perrig, Johnson, WMCSA 2002

Routing – security interdependence



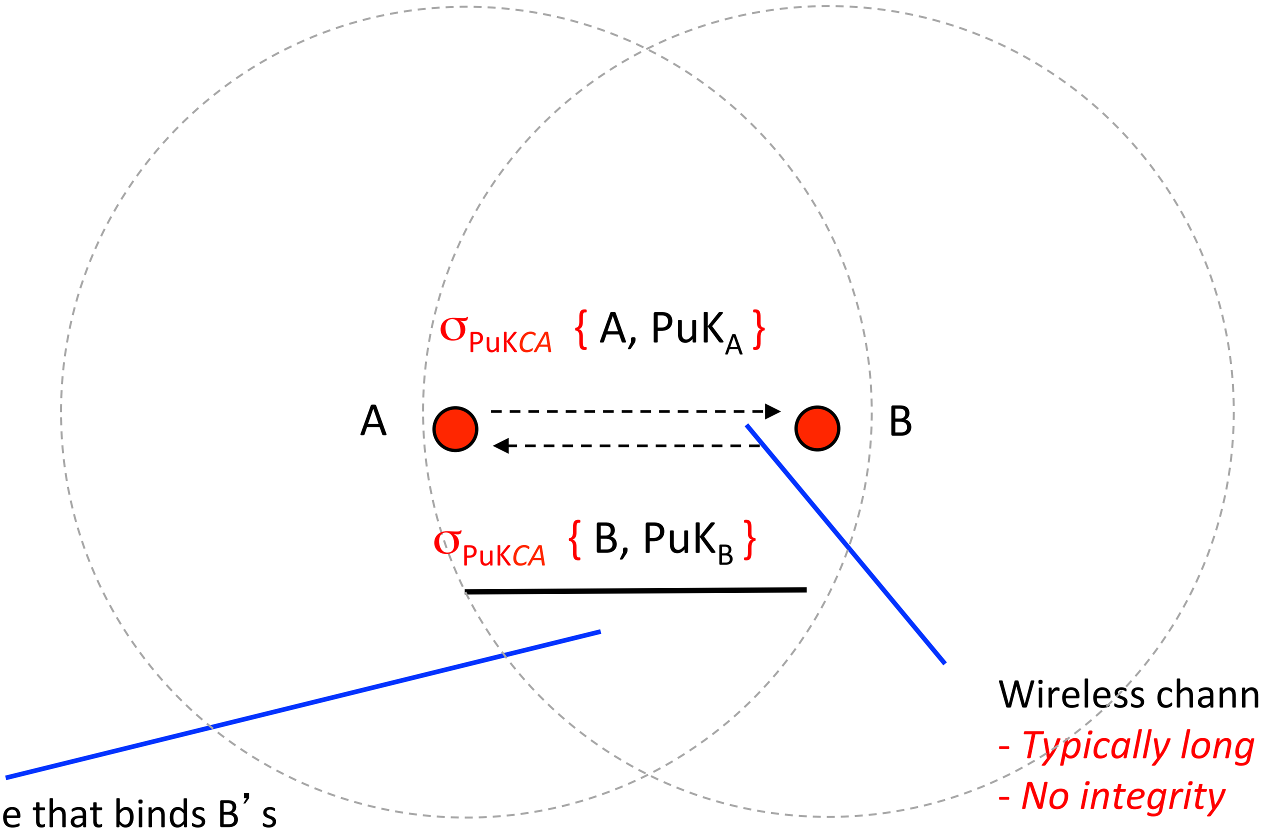
Routing can not work until security associations are set up.

Security associations can not be set up via multi-hop routes because routing does not work



Mobility helps security of routing

- Each node holds a certificate that bind its id with its public key, signed by the CA


σ_{PuKCA} { A, PuK_A }
A
B
σ_{PuKCA} { B, PuK_B }

Wireless channel

- Typically long distance

- No integrity

- No confidentiality

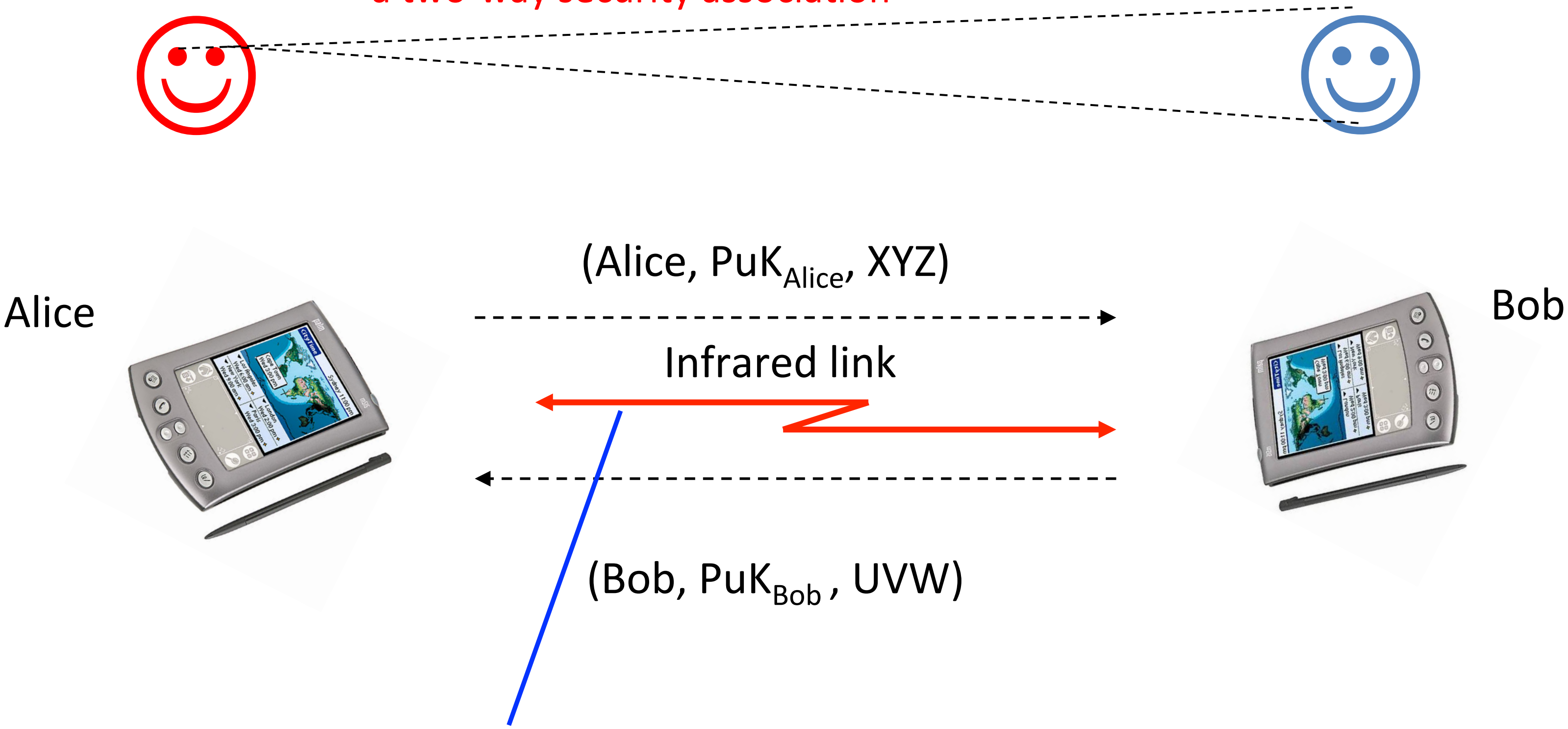
Certificate that binds B' s
Public key with his id,
issued and *signed by the central authority*

Discussion: advantages of the mobility approach (1)

- Mobile ad hoc networks with authority based security systems
    - breaks the routing-security dependence circle
    - automatic establishment of security associations
    - no user involvement
    - associations can be established in power range
    - only off-line authorities are needed
    - straightforward rekeying

Fully self-organized scenario

Visual recognition, conscious establishment of a two-way security association



Alice

(Alice, PuK_{Alice}, XYZ)

Infrared link

(Bob, PuK_{Bob} , UVW)

Bob

Secure side channel

-Typically short distance (a few meters)

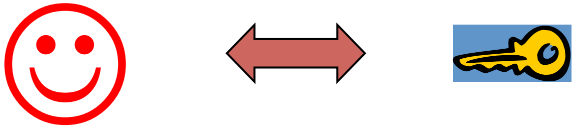
- Line of sight required

- Ensures integrity

- Confidentiality not required

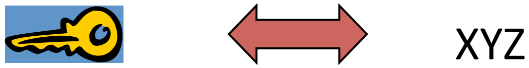
Two binding techniques

Binding of the face or person name with his/her public key



: by the Secure Side Channel,
the Friend mechanism and
the appropriate protocols

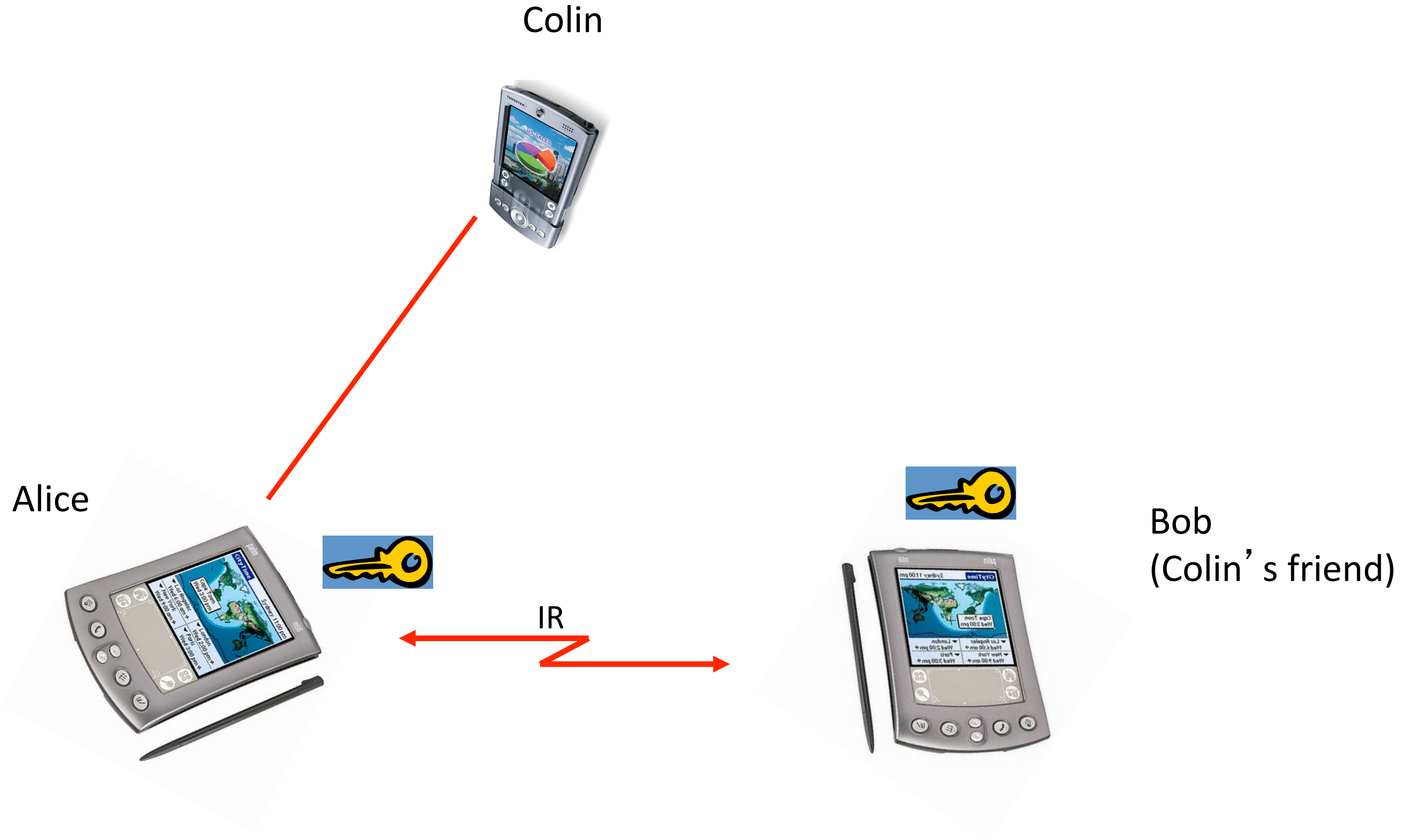
Binding of the public key with the Node-id



: by CAM or SUCV
Assumption: *static* allocation
of the NodeId:
NodeId = h(PuK)

- G. O'Shea and and M. Roe: Child-proof authentication for IPv6 (CAM) ACM Computer Communications Review, April 2001
- G. Montenegro and C. Castelluccia: Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses. NDSS 2002

Friends mechanism



Colin and Bob are *friends*:

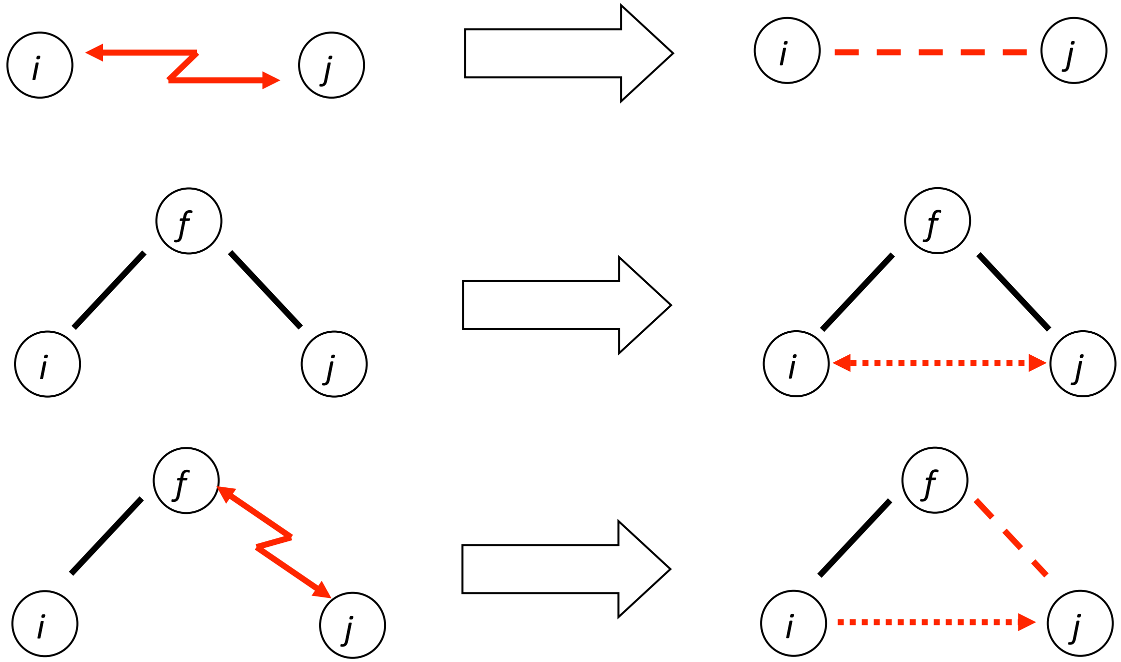
- They have established a Security Association at initialisation
- They faithfully share with each other the Security Associations they have set up with other users

Mechanisms to establish Security Associations

a) Encounter and activation of the SSC

b) Mutual friend

c) Friend + encounter



- ⇄ Exchange of triplets over the secure side channel
- - - - Two-way SA resulting from a physical encounter
- — Friendship : nodes know each others' triplets
- *i* ┈► *j* *i* knows the triplet of *j* ; the triplet has been obtained from a friend of *i*

Note: there is no transitivity of trust (beyond your friends)

Discussion: advantages of the mobility approach (2)

- Fully self-organized mobile ad hoc networks
  - There are no central authorities
  - Each user/node generates its own public/private key pairs
  - (No) trust transitivity
  - Intuitive for users
  - Can be easily implemented (vCard)
  - Useful for setting up security associations for secure routing in smaller networks or peer-to-peer applications
  - Requires some time until network is fully secure
  - User/application oriented

Conclusion

- Mobility can help security in mobile ad hoc networks, from the networking layer up to the applications
- **Mobility "breaks" the security-routing interdependence cycle**
- The pace of establishment of the security associations is strongly influenced by the area size, the number of friends, and the speed of the nodes
- The proposed solution also supports re-keying
- **The proposed solution can easily be implemented with both symmetric and asymmetric crypto**

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 → Scalability challenge
  - Police or spectrum regulator
- Usual behavior → Can be misleading
  - Based on statistical observation
- Rule enforcement mechanisms
  - Prevent malicious behavior (by appropriate security mechanisms) and encourage cooperative behavior

Upcoming Networks vs. Mechanisms

Rule enforcement mechanisms Upcoming wireless networks	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			

Topics and Deadlines!

COURSE PROJECTS

References (To be Reviewed)

- **S&P (Oakland):** IEEE Symposium on Security and Privacy
- **CCS:** ACM Conference on Computer and Communications Security
- **Security:** Usenix Security Symposium
- **NDSS:** ISOC Network and Distributed System Security Symposium
- **WiSec (WiSe,SASN):** ACM Conference on Wireless Network Security Supersedes WiSe (ACM Workshop on Wireless Security) and SASN (ACM Workshop on Security of Ad-Hoc and Sensor Networks)
- **ESORICS:** European Symposium on Research in Computer Security
- **ACSAC:** Annual Computer Security Applications Conference
- **IMC:** Internet Measurement Conference
- **Infocom:** International Conference on Computer Communications
- **MobiCom and MobiHoc**

Important Dates

- **Mehr, 22nd:** Review papers and select your project topic (Please contact me to discuss ASAP)
- **Aban 27th:** Midterm Presentation
- **Azar 25th to Day 4th:** Final Presentation
- **Day 12th:** Report and Final Exam