SPLASH

Securing Adhoc Networks

Eurecom- INRIA - UC Irvine

2003-2006

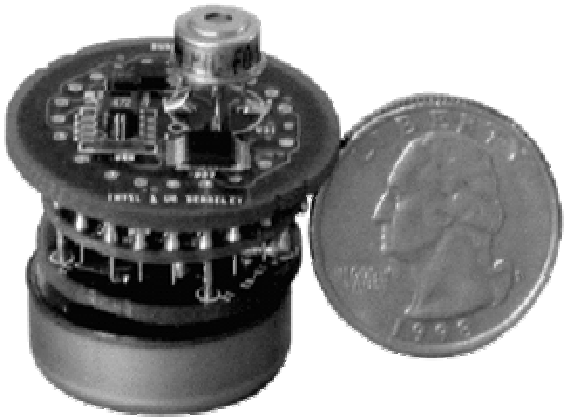
www.**inrialpes**.fr/planete/**splash**.html

Claude Castelluccia

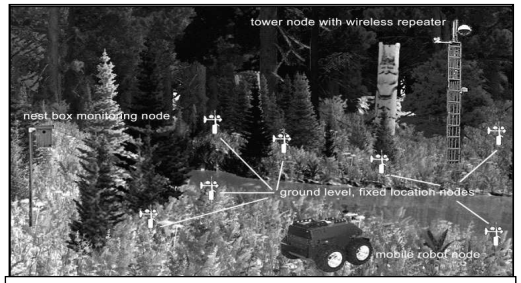
Nov. 2005

The SPLASH Project:
Securing Adhoc Networks

- Adhoc Networks
  - MANET: Mobile Adhoc networks (distributed, no central authority)
  - Wireless Sensor Networks (constraint devices/ one central authority)
- Characteristics
  - Limited CPU/Battery: need light-weight solutions
  - Fully distributed: no Central authority can be assumed



Application Spectrum



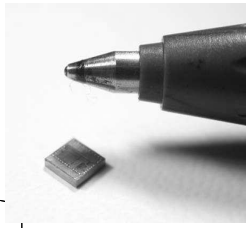
Environmental Monitoring

Interactive VR Game

Wearable Computing

Disaster Recovery

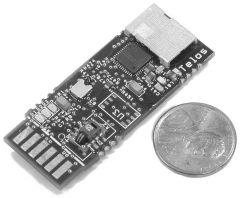
Earth Science & Exploration



Context-Aware Computing

Immerse Environments

Wireless Sensor Networks



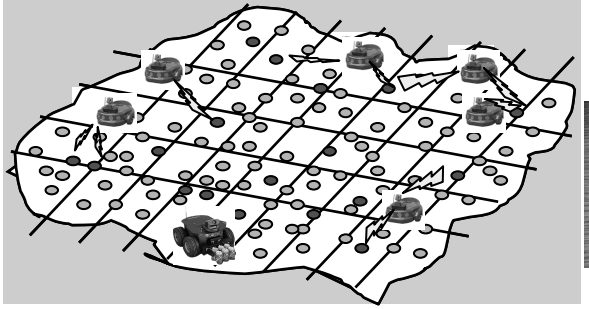
Biological Monitoring

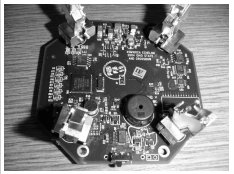
Hazard Detection

Smart Environment

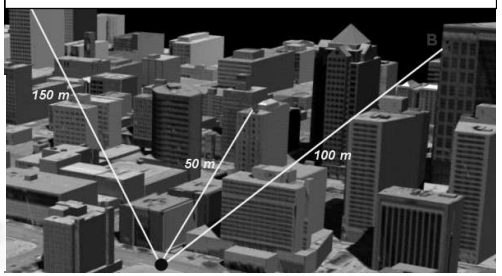
Linear Structure Protection

Military Surveillance

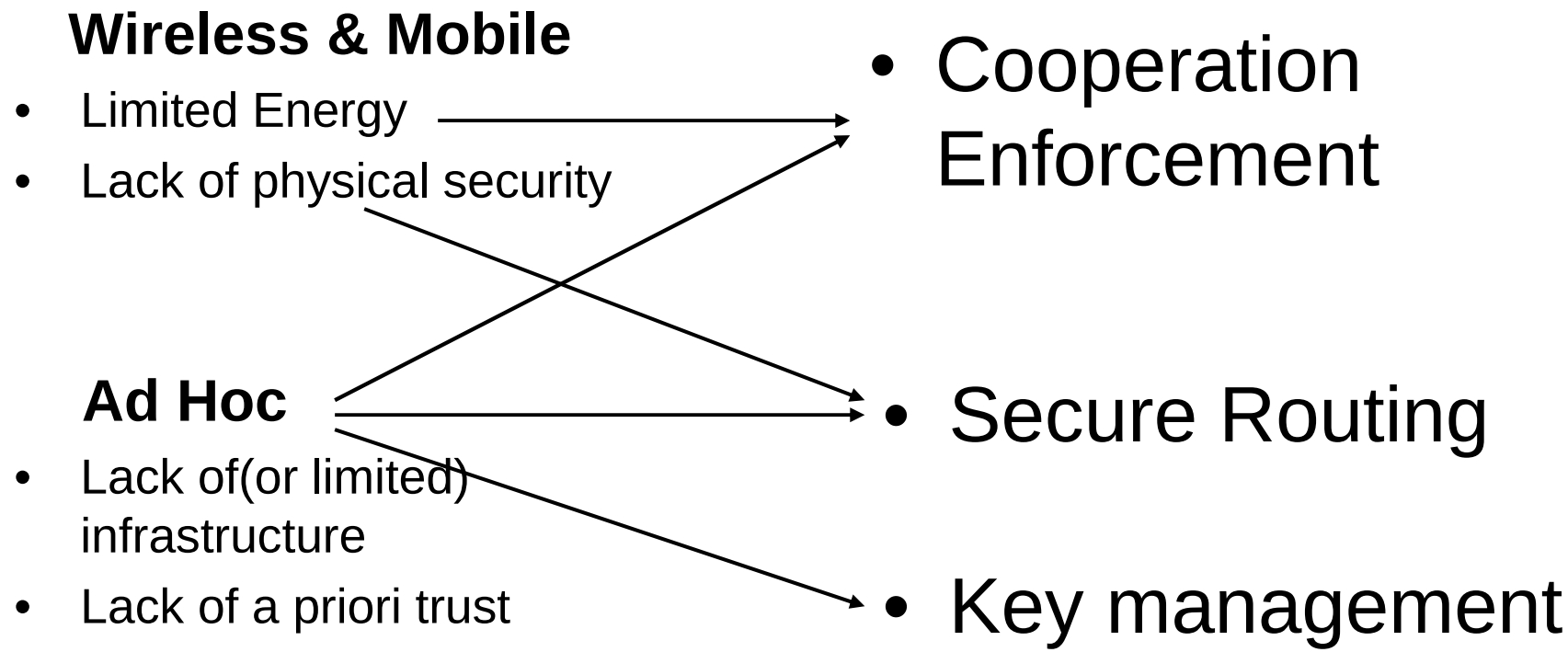




Urban Warfare



MANET Security Requirements



[Recent security solutions for mobile ad hoc networks
In "Ad Hoc Networks" IEEE Press - Wiley Ed]

The SPLASH Project:
Securing Adhoc Networks

- Some of our Research Challenges
  - Efficient and Infrastructure-less Key establishment/pairing
  - Distributed Access Control
  - Collaboration Enforcement
  - Securing Routing Protocols
  - Secure Aggregation
  - Privacy

One example of our results:

Shake Them Up!

ACM Mobysis 2005, Seattle, USA

Shake Them Up!

- In many wireless applications, you need to pair, i.e. establish a shared secret on-the-fly between devices.
- Some devices, such as sensors, have *very limited* CPU, memory and power!
- Standard methods such as the DH key exchange are excluded!
- Examples:

Wireless Thermometer

PDA

Current Solutions

- Public Key Cryptography-based schemes
  - Rely on PK key exchange protocols such as RSA or DH
  - They require to perform CPU-intensive operations such as modular exponentiations with large numbers!
  - Too expensive for sensor devices!
- PIN-based schemes (for ex. Bluetooth)
  - Key derived from a PIN number
  - PIN number is typically entered via an out-of-band channel such as a keyboard.
  - Computationally efficient.
  - …but requires a physical user interface (keyboard) …and most sensors do not have a keyboard L !
  - Security is pretty weak since it depends on the PIN….

Current Solutions (2)

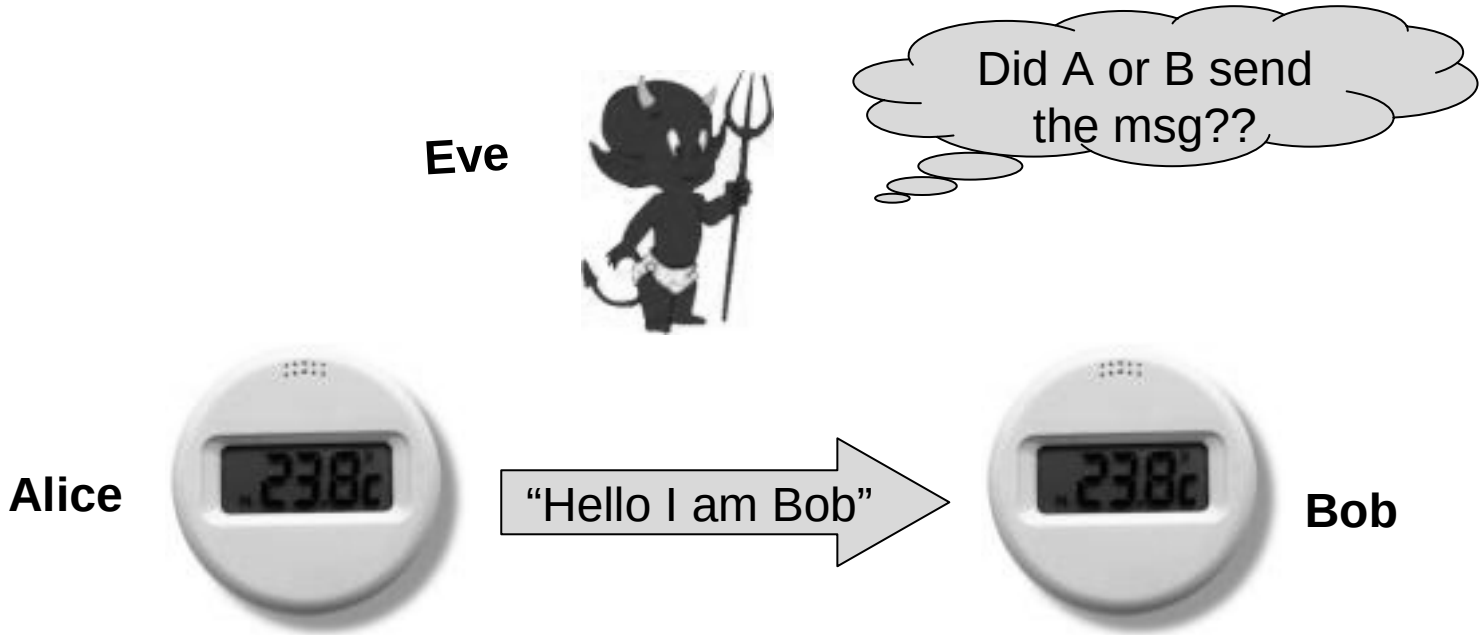
- Physical Contact (imprinting)
  - Stajano and Anderson proposed to establish a key via physical contact by linking devices with a wire….
  - Not always practical and requires additional hardware..
- InfraRed channel
  - IR is difficult to intercept since requires line-of-sight links.
  - But most sensors do not have IR interface!
- Faraday Cage
  - Devices could be placed into a Faraday cage
  - It is clearly impractical to ask users to lug around a metal box ;-)

Our Goals

- Design a secure pairing protocols that:
  - Does not rely on PK cryptography
  - Does not rely on pre-configured information
  - Does not increase the complexity (and cost) of the sensors by requiring additional hardware such as a display, keyboard, IR channel…
  - Does not require special equipements (cable, faraday cage)
- Security Model
  - The protocol must ensure that active or passive attackers do not learn the exchanged key
  - It must provide some DoS protection,i.e. prevent an attacker from disrupting the key exchange and exhausting the devices' resources.

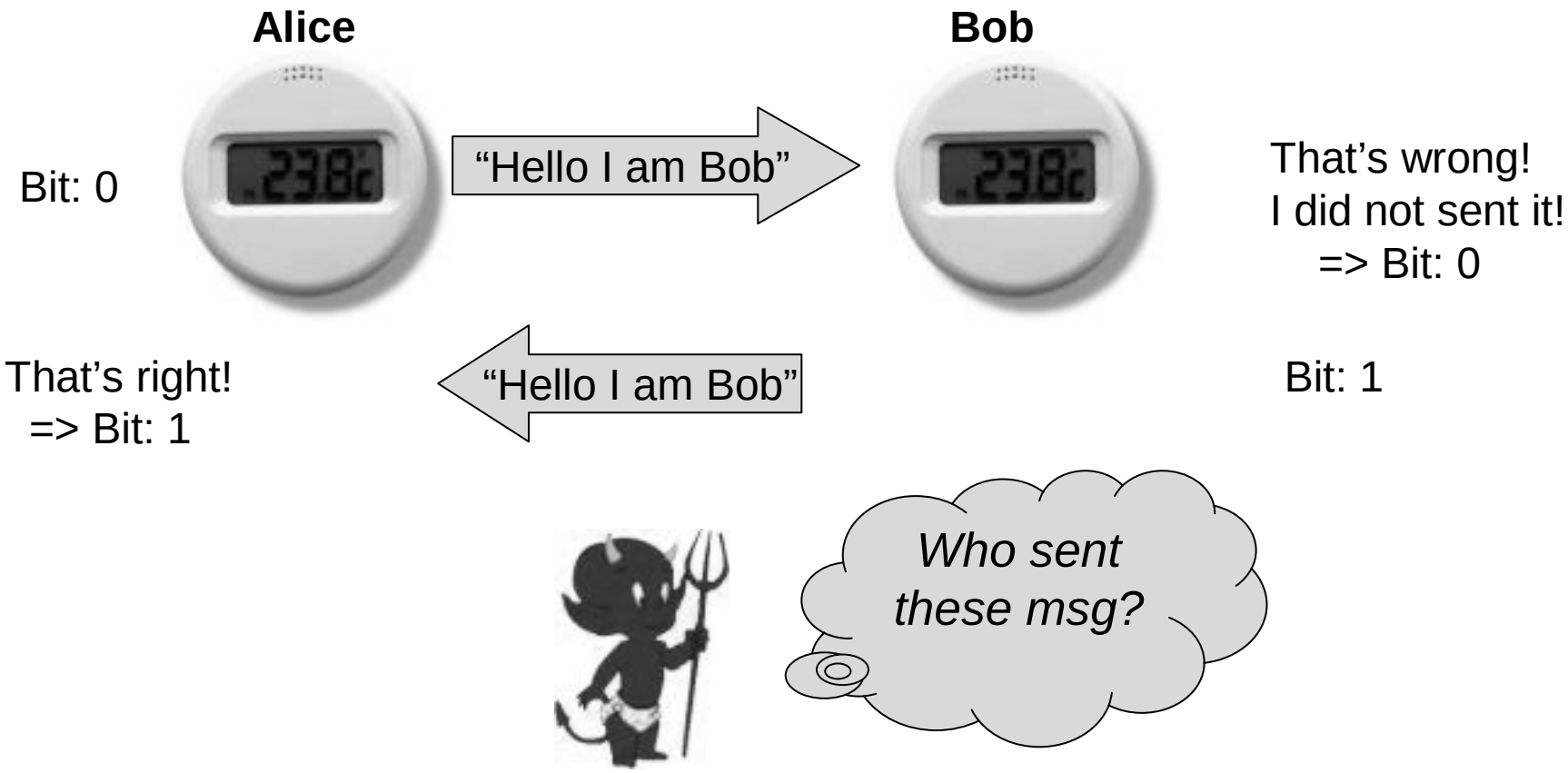
Our solution:
How to exchange one secret bit

- Let’s assume that Alice (A) and Bob (B) communicate over a wireless *anonymous* broadcast channel
  - Eve can read the exchanged packets
  - ...but can not identify the source of the packets.



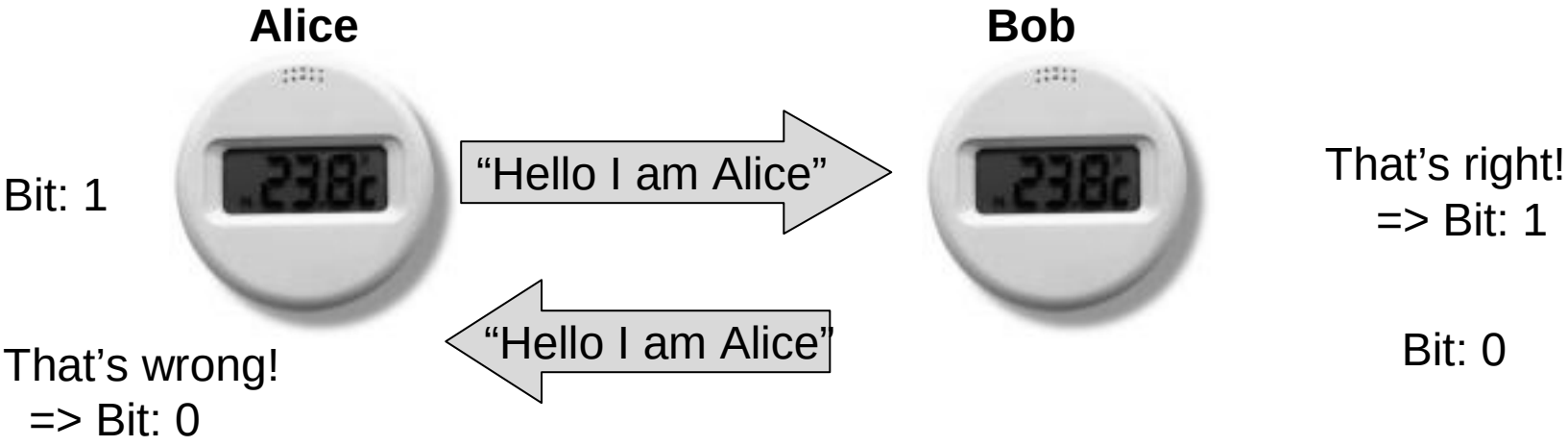
Our solution: How to exchange one secret bit (2)

- Alice and Bob can then use the following algorithm:



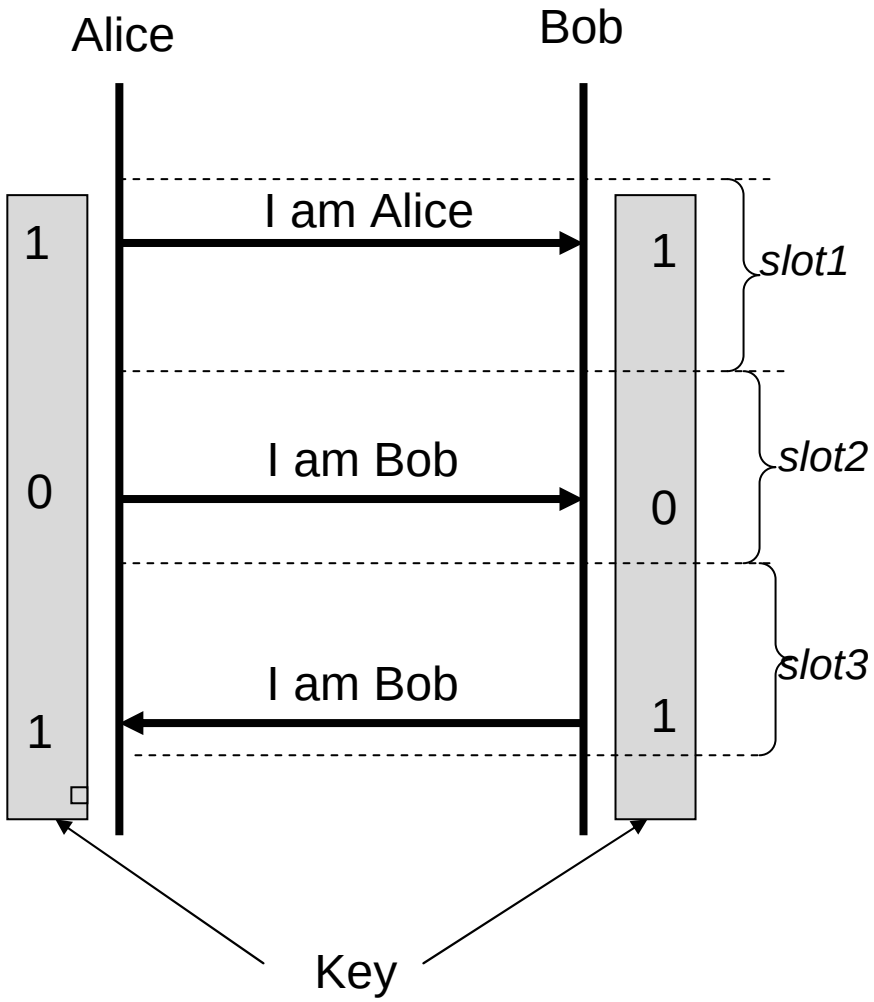
Our solution: How to exchange one secret bit (3)

- Of course the protocol is symmetrical i.e. Alice can also send the bit “1” and Bob the bit “0”



Our solution:
How to exchange a N-bit secret

- We divide the time in N slots.
- During each slot, either A or B sends a message
- The transmission order is random so that Eve can not group the messages together and retrieve the key…!



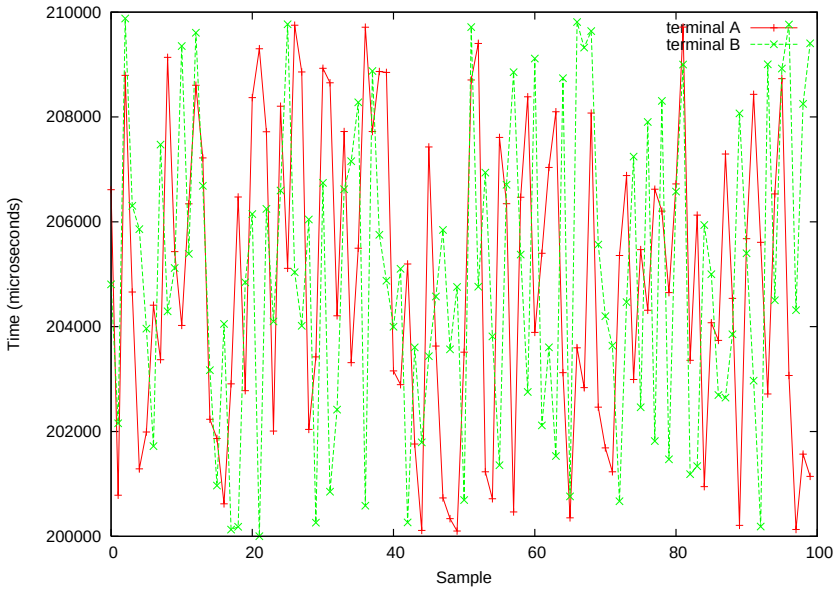
Wireless Anonymous Communication

- We assume source anonymity…
  - Can an 802.11-based system provide source anonymity?
- Eve can potentially identify the real source of the messages
  - Timing information
  - Reception Power
  - Frequency

Wireless Anonymous Communication (2)

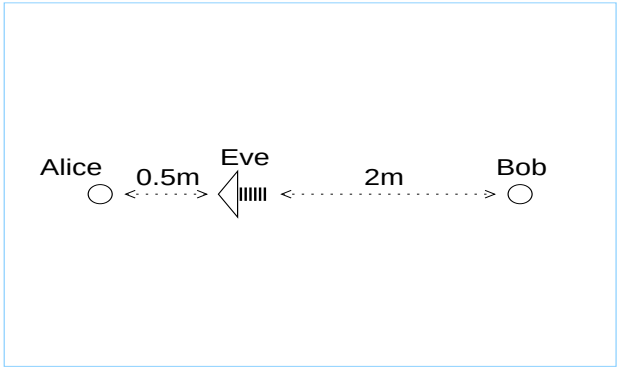
- Timing
  - This is quite trivial in TDMA based scheme since devices always transmit during their allocated slots
  - However Timing does not provide any information if a random access MAC protocol, such as CSMA, is used since each device access the channel at a random time!

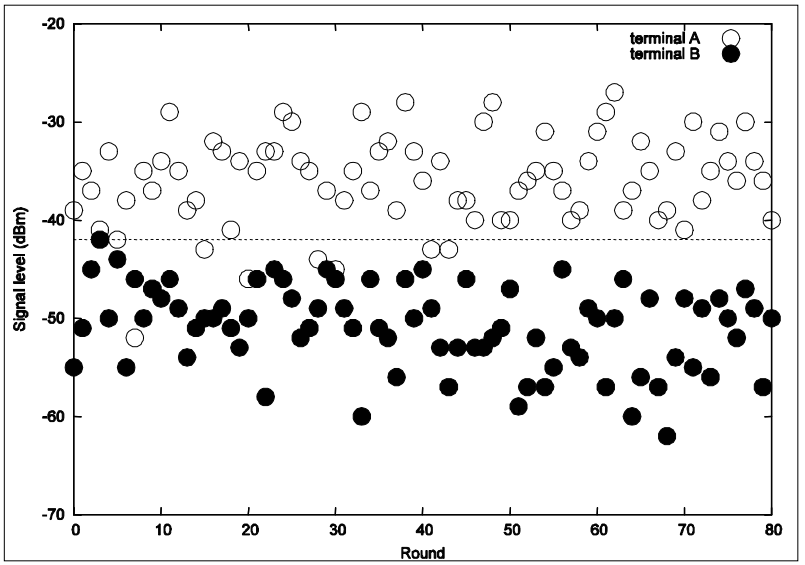
=> Our protocol only works with CSMA-based technologies, such 802.11,802.15.4



Wireless Anonymous Communication (3)

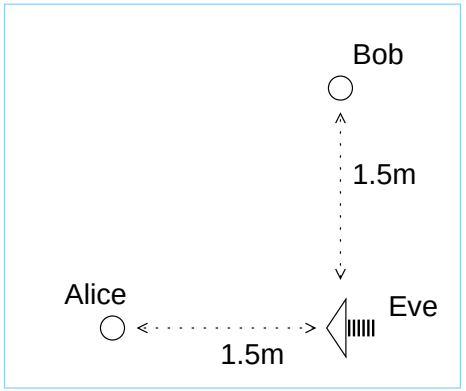
- Reception Power
  - The reception power is defined as $Sr=St.Gt.Gr.K/d^2$
  - If Eve is closer to Alice than Bob, she will receive Alice's message which a higher power!
  - Note: we assume A and B transmit at the same power level.

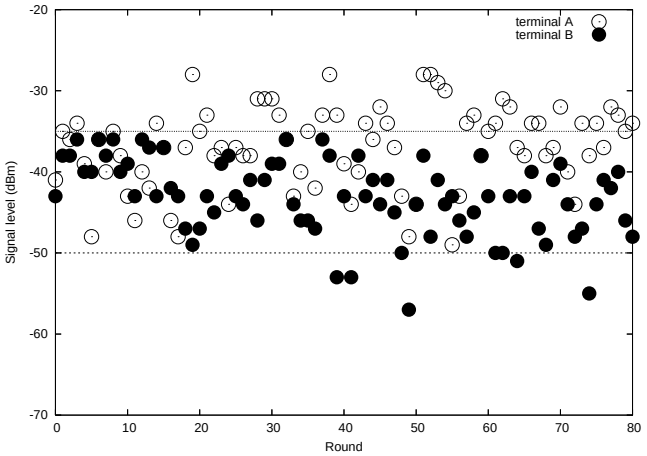




What can be done? (1)

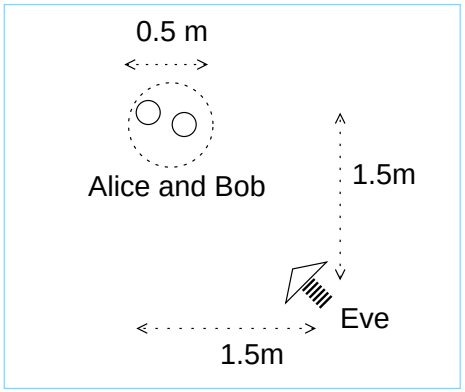
- We can randomly change Alice and Bob's transmission power
  - Some bits will still be revealed
  - If Eve has a directional antenna she can aimed it at one of the devices!

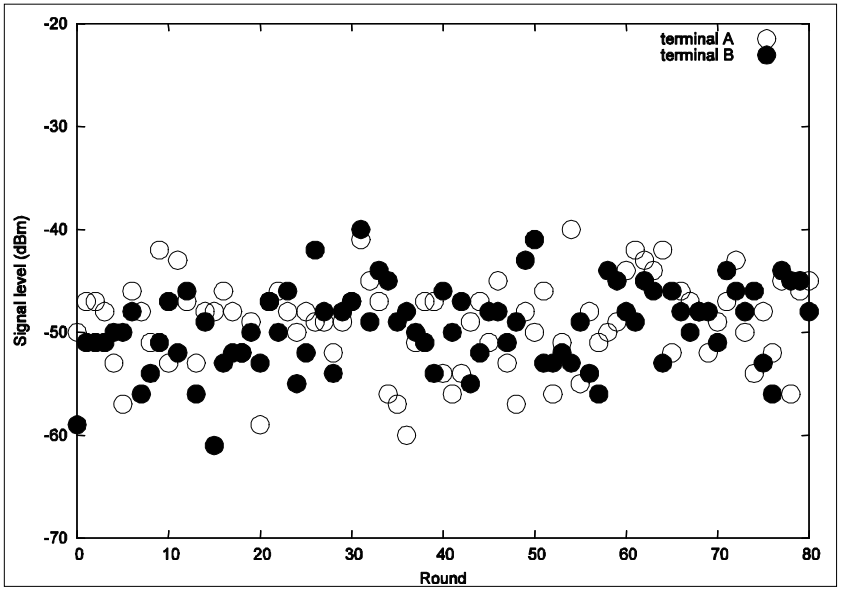




What can be done? (2)

- We can bring the devices together and move them (shake them up) one around the other!
  - The reception power of A's and B's messages will be similar…
  - Eve cannot use a directional antenna since the devices are moving!
- In summary, shaking 2 devices prevents using power to identify source!



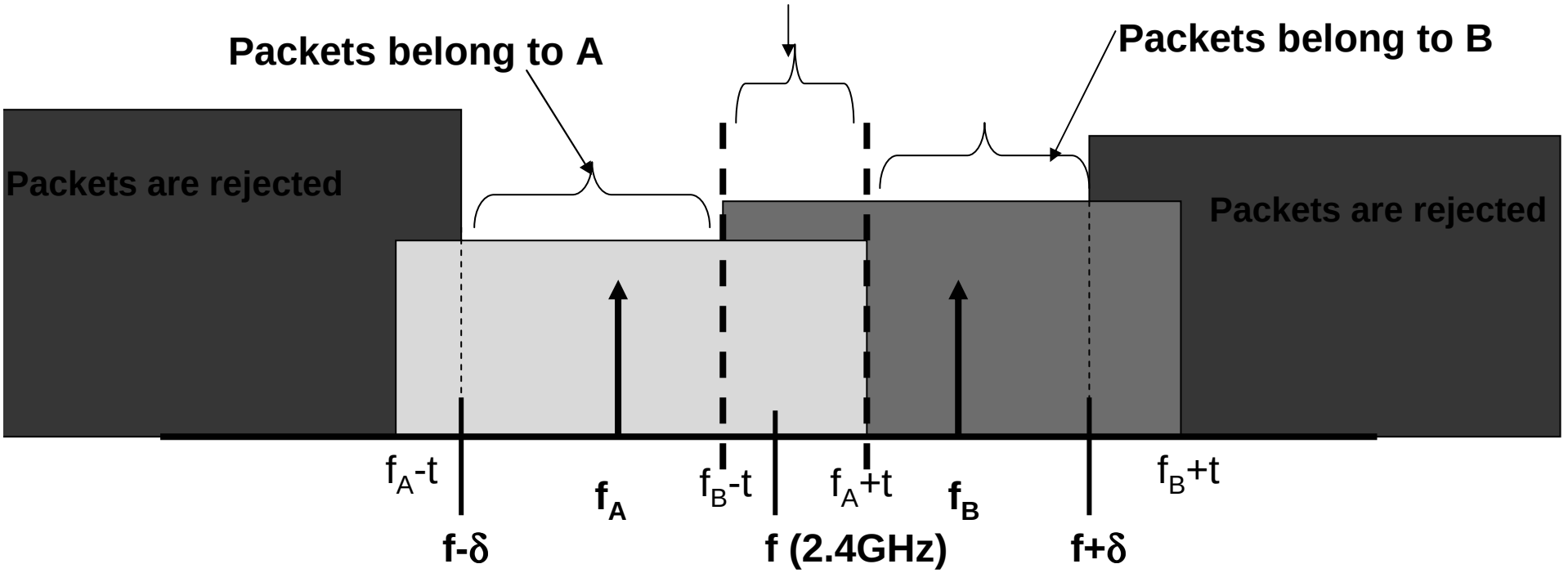


Frequency Fingerprinting

- Even though standard specify one frequency, each device uses a different frequency.
- This difference is due to the crystal oscillator and clock drift, resulting from aging, temperature and so on.
- Typically an error of 25ppm (parts per million) is allowed by the standard.
- So if the transmitting frequency is 2.4GHz, a frequency offset of up to 120kHz is allowed.
- Possibly, a (well-equipped) Eve can use this frequency difference to identify the source and retrieve the secret…

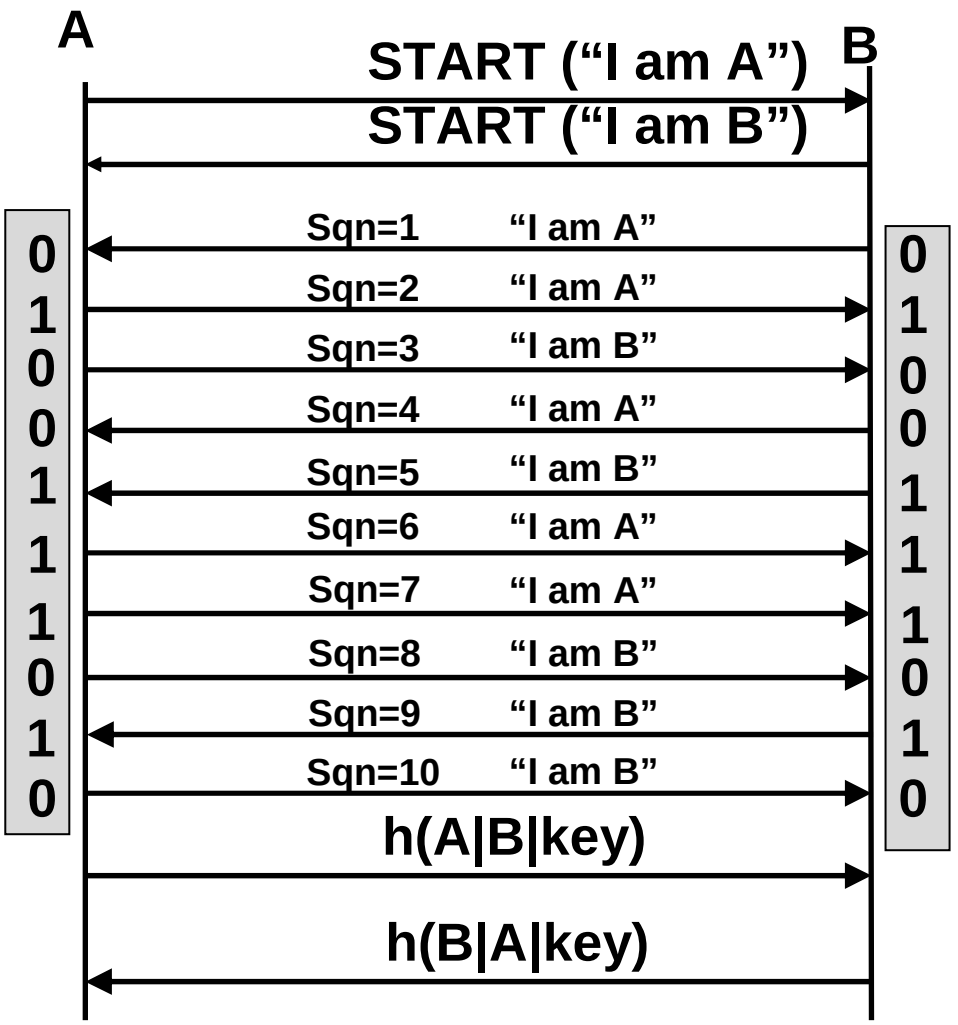
Frequency Fingerprinting (2)

- If you move the devices at a high speed, the doppler effect might solve the problem for you J !
- A more practical solution is to add a random frequency offset so that A and B span over similar frequency ranges.
  - Btw This solution does not require to modify the standard!



The Shake’ em Up protocol (STU)

- We combine the previous protocol with shaking.
- A user that wants to pair to devices A and B
  - Brings the devices together
  - Shakes them up!
  - Triggers the protocol (for example by pushing a bottom on the devices)…



Performance: Energy Consumption

- In STU, each device
  - processes N small messages, where N is # of bits of the secret (total number of bits sent: 2016)
  - …but performs almost no computation.
- In a DH based scheme,
  - each node sends only one large message (>1024 bits)…
  - but performs a lot of computation…i.e. 4.12×10^8 single precision multiplications (if N=72).
- By using the heuristic that transmitting one bit consumes as much energy as executing 800 instructions…
  - we can show (see paper) that our scheme is 100 times more energy efficient than a DH based scheme!
  - Elliptic Curve DH can reduce the communication cost by 5…but our scheme would still be more efficient.

Conclusion

- We’ve presented a key exchange protocol for CPU constrained devices that uses CSMA-based wireless communication.
- We believe this is the first solution that does not rely on cryptography, out-of-band channel or specialized hardware.
  - Very simple and efficient
  - Does not require computation…just transmission and good shaking!
- This is only one example of the ACI SPLASH results

Selected Results in 2005

- Key Establishment
  - ***Shake Them Up!***. ACM/Usenix ***Mobisys'05***
  - ***Self-Configurable Key Pre-distribution Mobile Ad Hoc Networks, IFIP Networking'05***.
  - ***Authentication using ID-based Hash chains***, in submission
- Secure Aggregation
  - ***Efficient Aggregation of Encrypted Data in Wireless Sensor Networks,*** ACM/IEEE ***Mobiquitous*** Conference
  - ***Secure Acknowledgment Aggregation***, ***Computer Networks (Elsevier).***
- Cooperation Enforcement
  - ***Pocket Bluff***, in submission.
  - ***Real life experience of Cooperation Enforcement Based on Reputation (CORE) for MANETs, IEEE REALMAN***
  - **Non cooperative forwarding in ad hoc networks, *IFIP Networking'05***
  - **Some game-theoretic problems in wireless ad hoc networks, *NGI 2005***
  - ***Analysis of coalition formation and cooperation strategies in mobile ad hoc networks, Ad Hoc Networks Journal***
- Secure Routing
  - ***Securing Route Discovery in DSR, ACM/IEEE Mobiquitous'05***
  - **Ad hoc networks security,** Chapter in the book "Handbook of information security"

Diffusion

- We organized:
  - ***ESAS 2005*** (2nd European Workshop on Security and Privacy in Ad hoc and Sensor Network)
    - R. Molva (Eurecom) and G. Tsudik (UCI) were co-chairs
    - C. Castelluccia was in the steering and PC committees.
  - First International Workshop on Trust, Security and Privacy for Ubiquitous Computing (***TSPUC 2005***)
    - R. Molva was co-chair
    - C.Castelluccia, P.Michiardi and G.Tsudik were in the PC
  - First IEEE Conference on Security and Privacy for Emerging Areas in Communication and Networks (***SecureComm'05***)
    - G.Tsudik was co-chair
    - C.Catelluccia, P. Michiardi and R.Molva were in the PC

Future Work

- INRIA will participate to the IST STREP project UbiSen&Sec (Starting 2006)
  - This project is about security in wireless sensor networks
- EURECOM is a partner of two IST FET Projects on Autonomic Computing: HAGGLE and CASCADAS
- We will organize:
  - ESAS'06 (together with ESORICS'06)
  - TSPUC'06
  - SecureComm'06
  - IEEE ICC 2006 Network Security and Information Assurance Symposium

Collaborations within Splash

- The collaboration within the project has been very active
  - C.Castelluccia (INRIA) has spent 2 years at UCI
  - P.Mutaf (INRIA) has moved to Sophia-Antipolis to closely collaborate with Eurecom
  - P. Michiardi, R. Molva (EURECOM) worked with E. Altman (INRIA) on Game theory (2 papers)
  - N.Saxena (UCI) is currently visiting INRIA for 3 months.