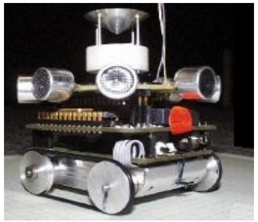
Security and Key Establishment

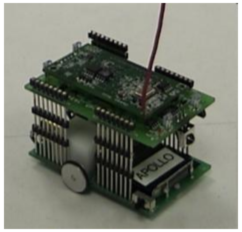
In

Wireless Sensor Networks



Gabriele Oligeri
ISTI – CNR, Pisa

gabriele.oligeri@gmail.com



OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- Well known solutions
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

SENSORS… (1/2)

Iris sensor motes:

- 2.4 GHz IEEE 802.15.4, Tiny Wireless Measurement System
- Designed Specifically for Deeply Embedded Sensor Networks
- 250 kbps, High Data Rate Radio
- Wireless Communications with Every Node as Router Capability
- Outdoor line-of-sight tests have yeilded ranges as far as 500 meters between nodes without amplification
- CPU ATmega1281, 128KB program flash memory, 512KB measurement flash memory, 8KB RAM.

SENSORS… (2/2)

Sensor board:

Expansion Connector for
- ❑ Light
- ❑ Temperature
- ❑ RH
- ❑ Barometric
- ❑ Pressure, Acceleration/Seismic,
- ❑ Acoustic, Magnetic and other

Applications:

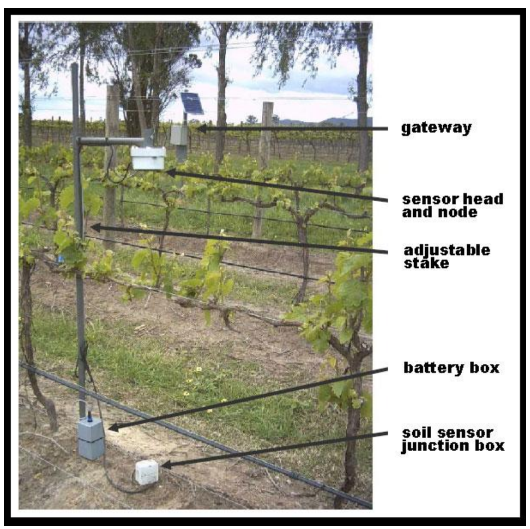
- ❑ Indoor Building Monitoring and Security
- ❑ Acoustic, Video, Vibration and Other High Speed Sensor Data

WSN – APPLICATIONS (1/2)

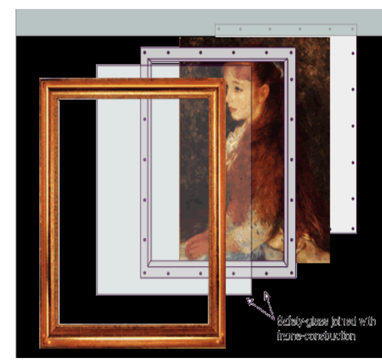
Smart bridges:
- ✓ Vibration recordings of trucks crossing
- ✓ Structural health monitoring

Jindo Bridge – South Korea

Agriculture:
- ✓ Grape networks, Inc, CA, US
- ✓ Save energy and expenses
- ✓ Monitor the effectiveness of water and chemicals



Museum technology:
- ✓ Microclimate framing
- ✓ Protection for precious paintings
- ✓ Temperature and humidity control



WSN – APPLICATIONS – MILITARY (2/2)

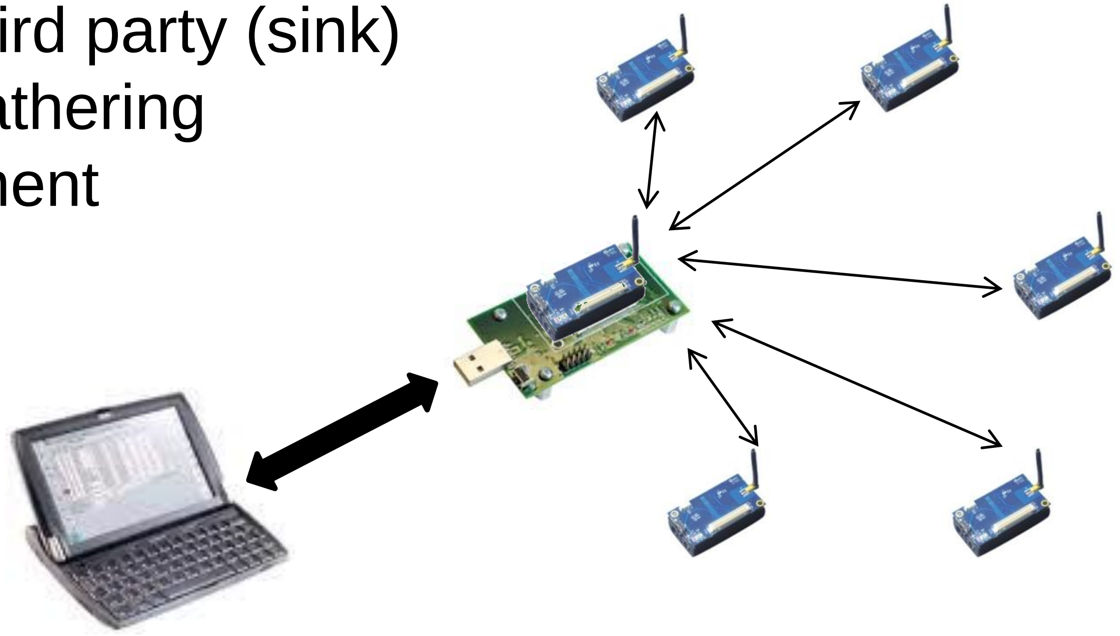
Applications for unmanned vehicles on the ground:

- Area surveillance and monitoring
- Obstacle breaching
- Target acquisition and designation
- Route clearance
- Mine and detection and disposal

ATTENDED OR UNATTENDED… THIS IS THE PROBLEM ! (1/2)

Attended WSNs :

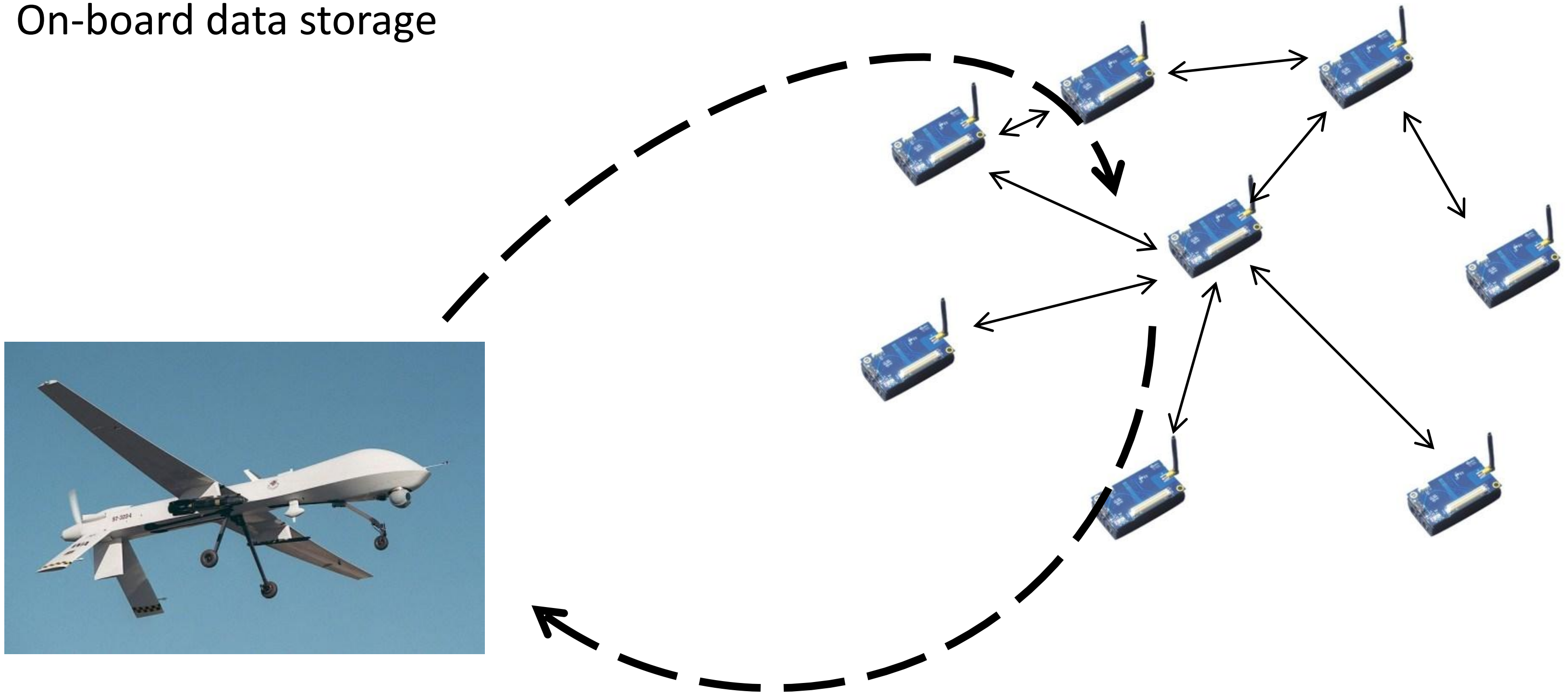
- On-line trusted third party (sink)
- Real-time data gathering
- Sensor management



ATTENDED OR UNATTENDED… THIS IS THE PROBLEM ! (2/2)

UnAttended WSNs :

- **NO** on-line trusted third party
    - ✓ Unpredicatable sink visit frequecy
- On-board data storage



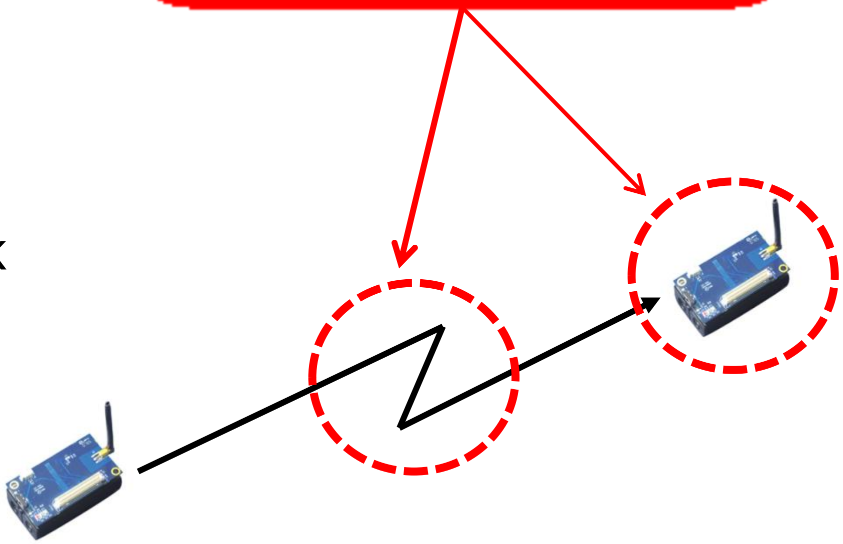
OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- Well known solutions
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

SECURITY ON WSN – WHY ?

- Sensors are cheap and easy to attack
  - No tamper proof hardware
  - No computational power
  - Reduced memory size

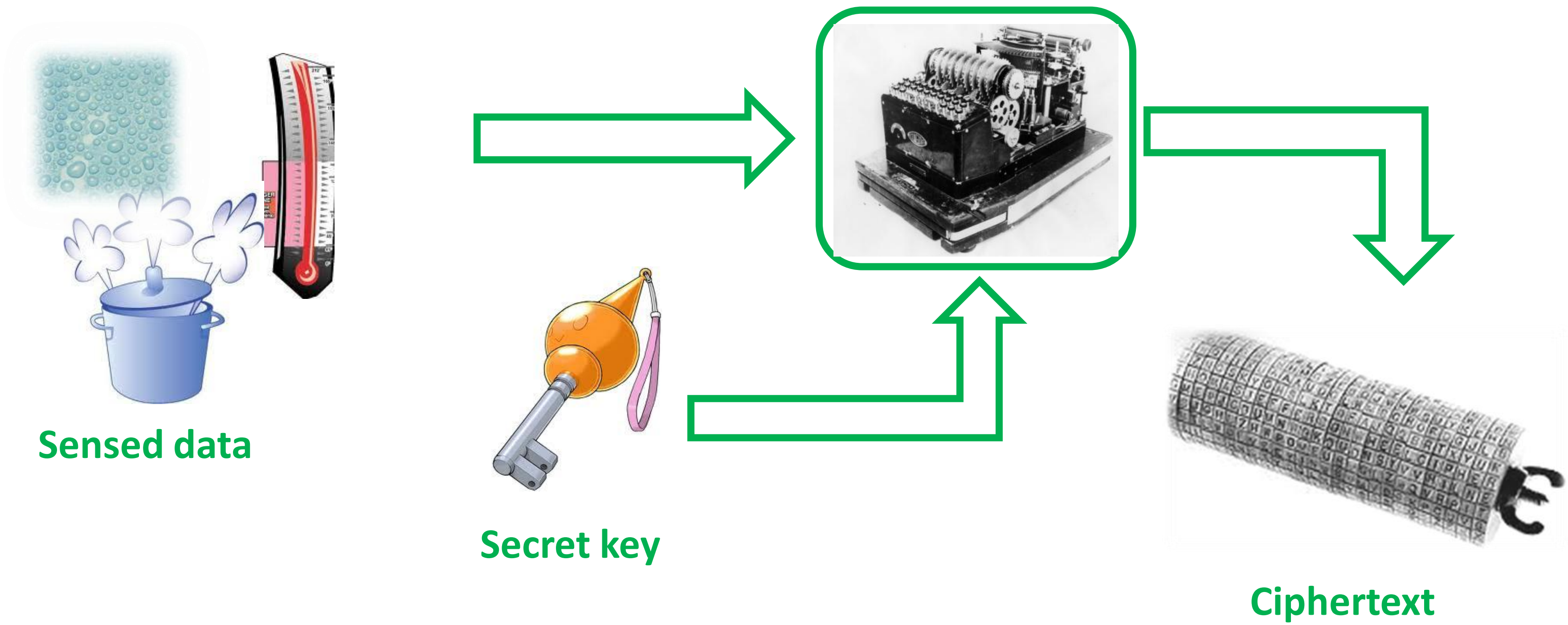
<u>NO strong security guarantees</u>



- Eavesdrop and sell strategy attack
  Sensed data are precious

- Injecting fake values
  Actuators may inhibit damages

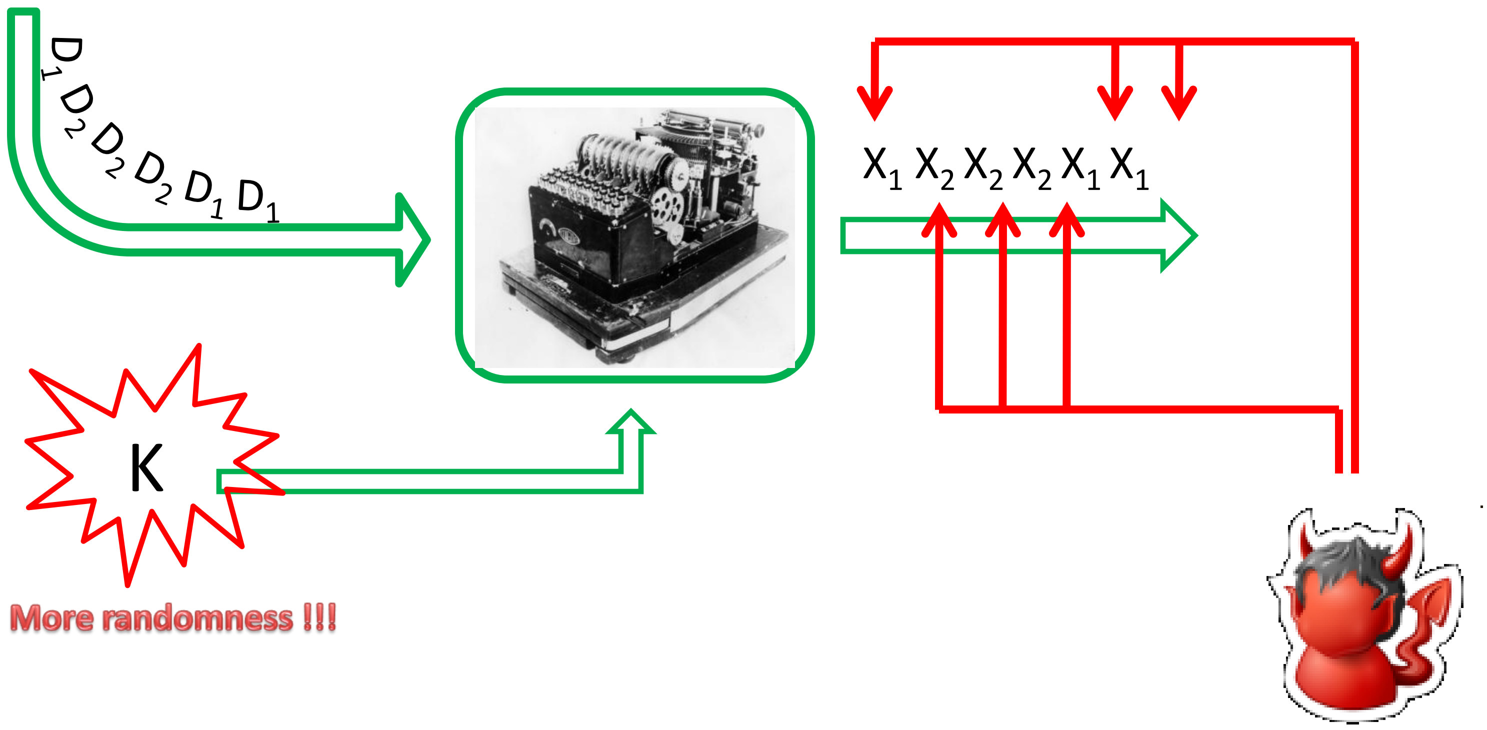
MAKING SENSED DATA SECURE (1/2)



- The secret key allows the parties to understand the meaning of the ciphertext
- How to establish a secret key ?

MAKING SENSED DATA SECURE (2/2)

Symmetric key is nice with sensors …
but there is not enough randomness around !!!



OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- Well known solutions
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

KEY ESTABLISHMENT (1/2)

Establishing a shared secret undergoes to two main problems:

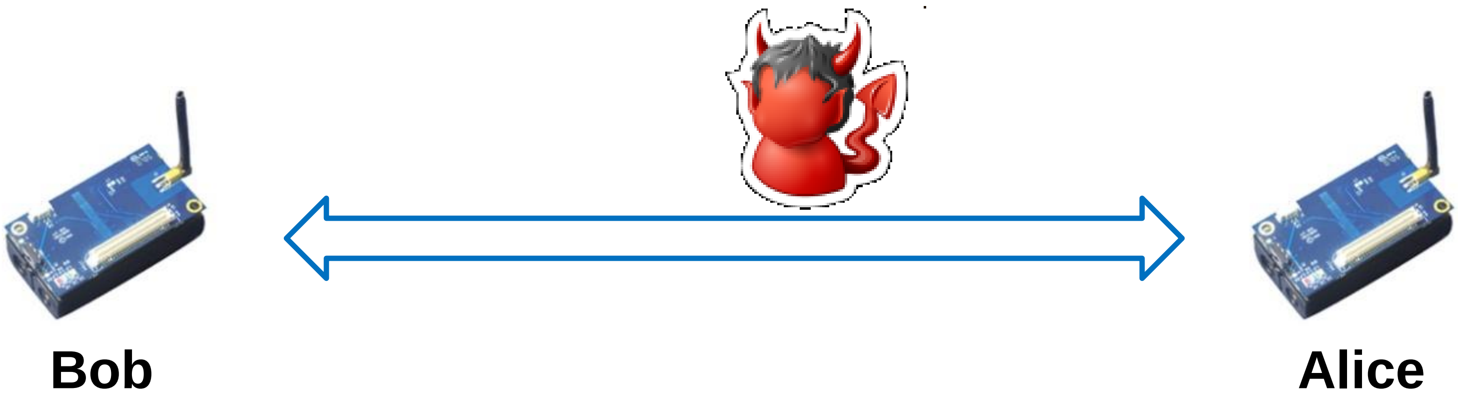
- **Authentication:** Bob is really Bob ?
- **Secret generation**: How to establish a new **safe secret** in a **not-safe** channel ?

KEY ESTABLISHMENT (2/2)

Establishing a shared secret undergoes to two main problems:

- **Authentication:** Bob is really Bob ?

- **Secret generation**: How to establish a new **safe secret** in a **non-safe** channel ?

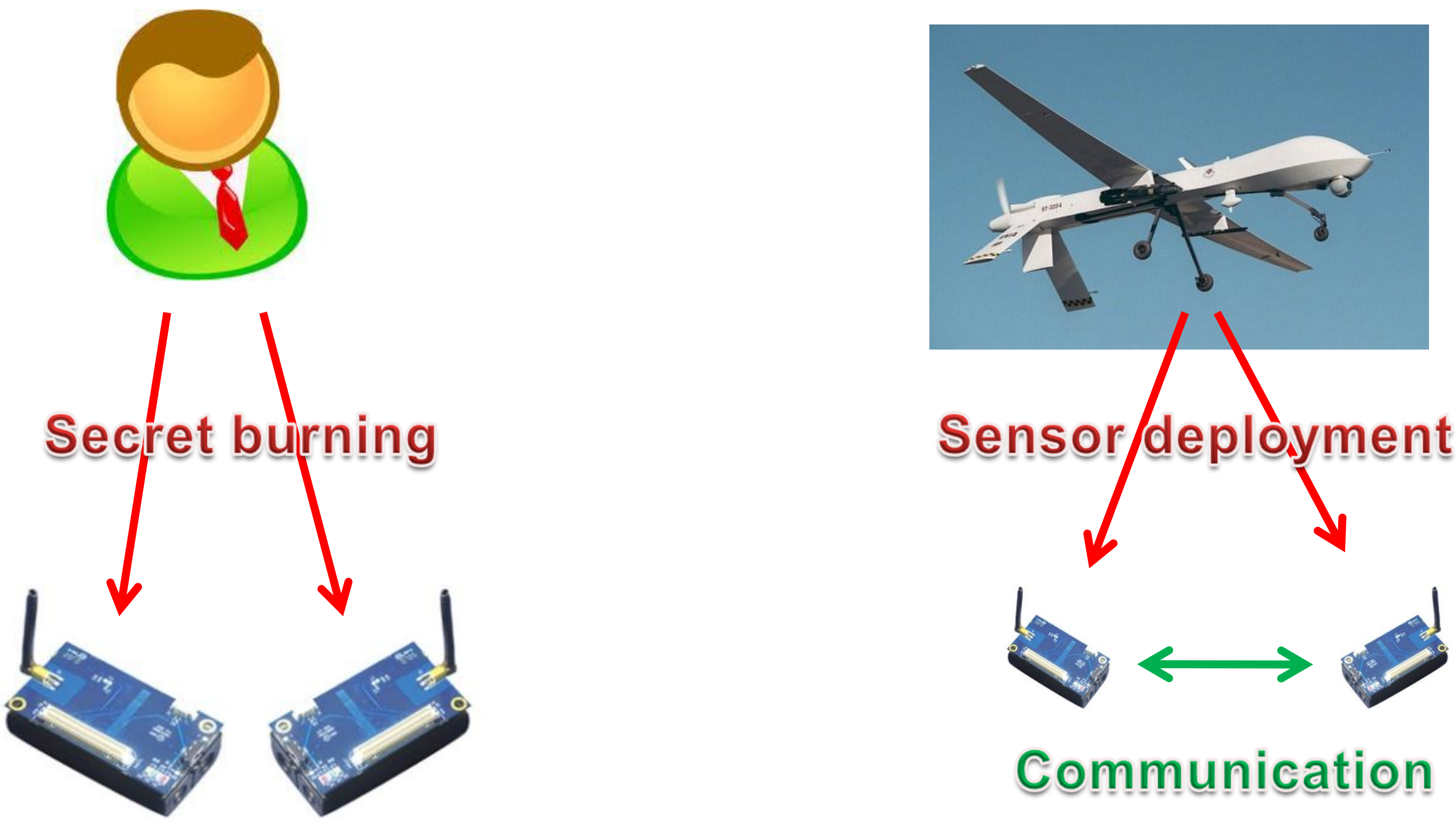


OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- **Well known solutions**
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

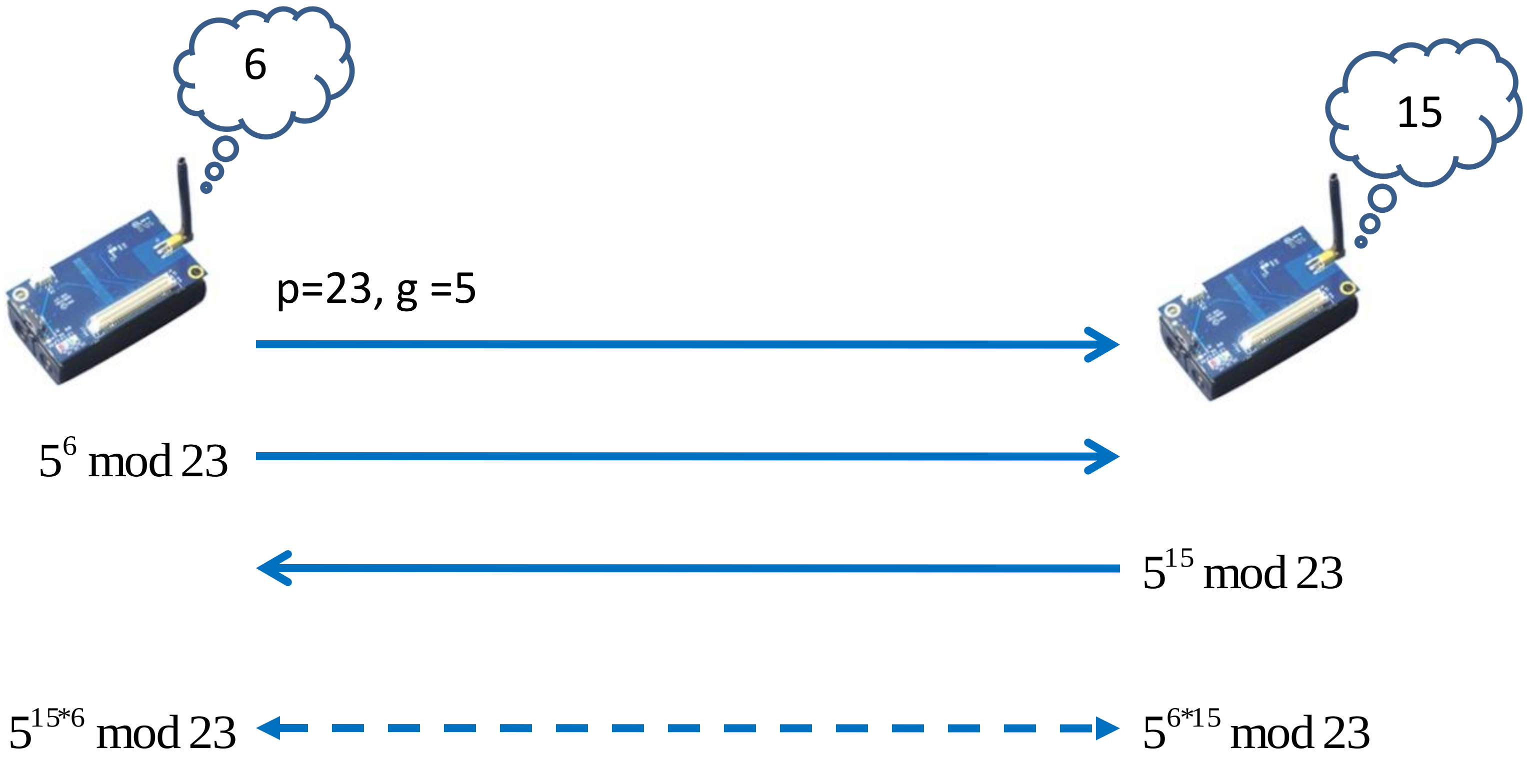
SECRET GENERATION – PIN (1/2)

A pre-shared secret can be burned in the sensors before the WSN deployment.



SECRET GENERATION – DH (2/2)

Diffie-Hellman is a key establishing algorithm



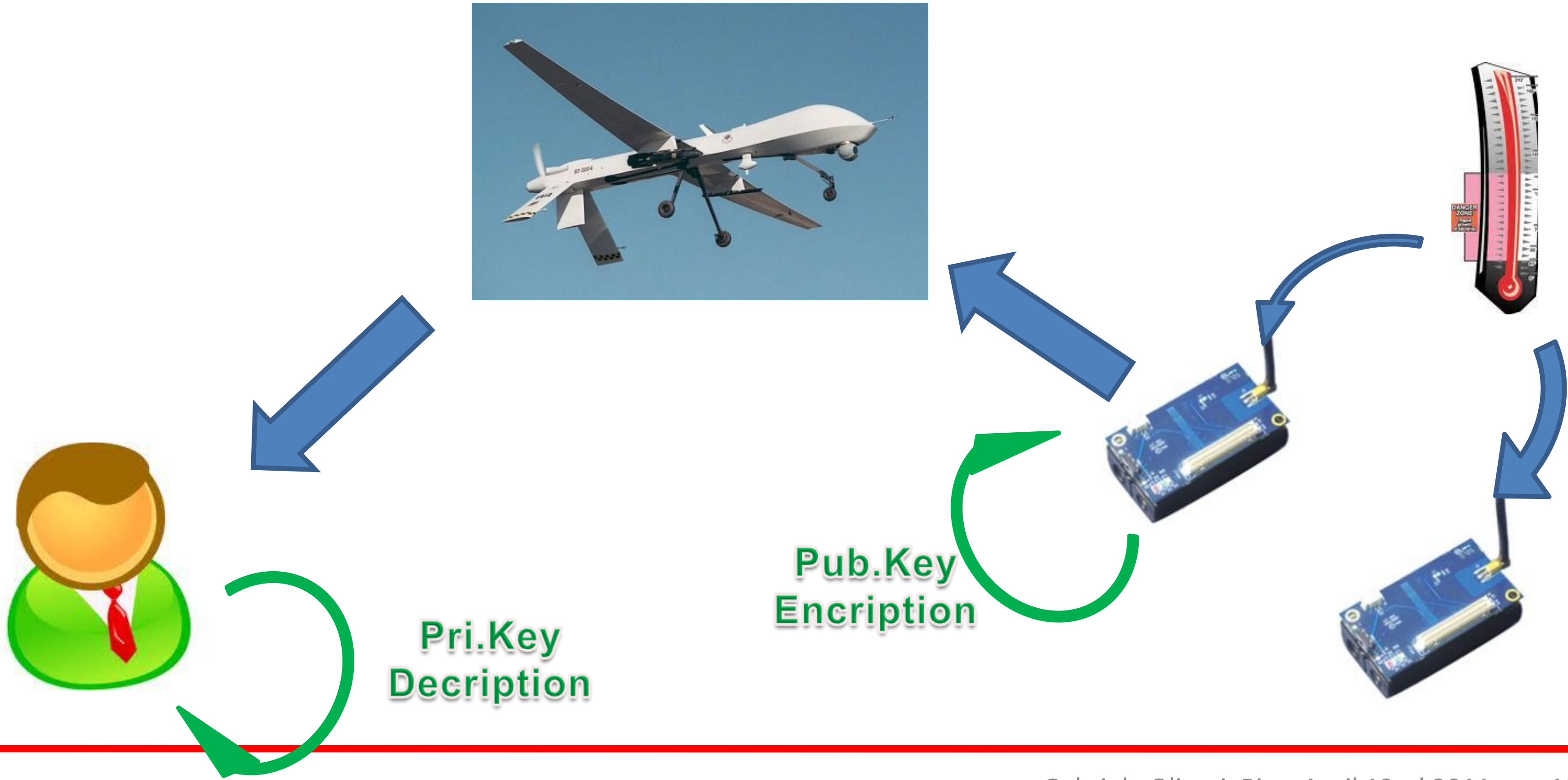
Secret key = 2

$19^a \bmod 23 = 8^b \bmod 23$

AUTHENTICATION - PKI

PKI: public key infrastructure involves the use of the “sink” Public key

- Each sensor encrypts the sensed data with the sink Pub. Key
- Only the Private key owner can access the sensed data



OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- Well known solutions
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

THE BAD GUY… (1/2)

Perfect eavesdropper,
no active behavior.

Active adversary …
but still honest:

- Secrets disclosure
- No code injection

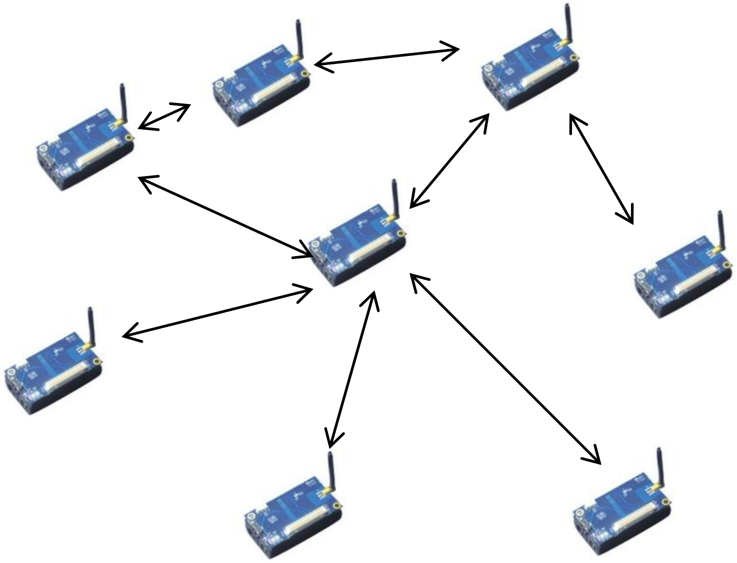
THE BAD GUY… (2/2)

➢ Adversarial model

✓ Honest but curious

✓ She can tamper the sensor but she cannot perform **code injection**, or more generally, change the **sensor behavior**.

– Why ?

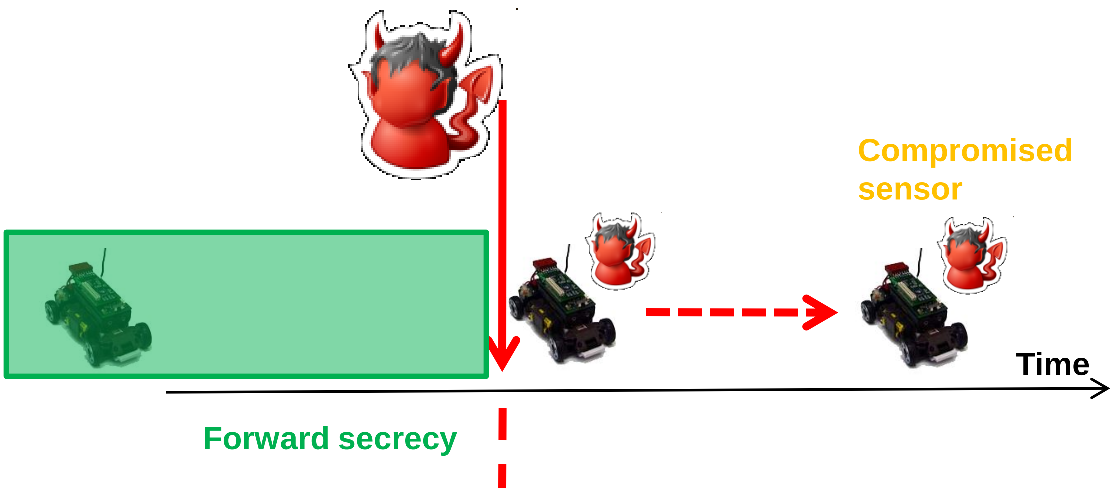


❑ She is interested on the perfect working of the WSN

❑ Overall secrets and data disclosure

FORWARD SECRECY (1/2)

- **Forward secrecy:**
  - Data collected before the compromised event (in the past) must be safe
  - Easy to achieve
  - Periodic one-way secret evolution $K^{r+1}=H(K^r)$
  - Encrypted data in the past is protected by pre-image resistance hash property



FORWARD SECRECY (2/2)

Let the secret key change at each round !

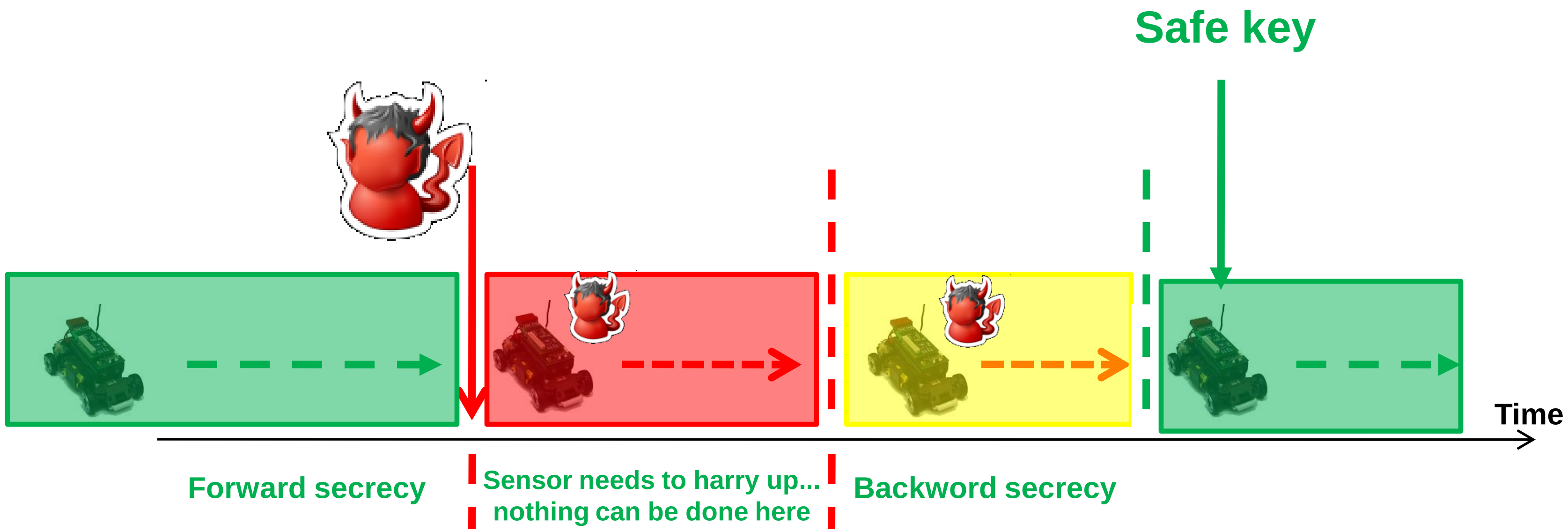
$$K_0 \xrightarrow{H} K_1 \xrightarrow{H} K_2 \xrightarrow{H} K_3 \xrightarrow{H} K_4 \xrightarrow{H}$$

H is a cryptographic hash function:

- It is easy to compute the hash value for any given message.
- It is infeasible to find a message that has a given hash.
- It is infeasible to modify a message without hash being changed.
- It is infeasible to find two different messages with the same hash.

BACKWARD SECRECY

- **Backword secrecy:**
  - Data collected after the compromise event (in the future) must be safe
  - A contribution of secure randomness suffices for intrusion-resilience



WELL KNOWN SOLUTIONS… AND WELL KNOWN ISSUES

PIN : The worst solution… and the most adopted.
Key refreshment does not exist
Forward and backward secrecy are not guaranteed

PKI : Strong key encryption
No entropy if used as stand-alone solution (low forward secrecy)
Backward secrecy is guaranteed

DH : Key refreshment guarantees forward secrecy
Backward secrecy is missing

ISSUES:

- Forward secrecy needs a simple key refreshment algorithm.
- Backward secrecy needs a true random number generator or a "good approximation" of it .

  The generated secret **must** be shared

LET'S GO BACK TO THE PROPOSED ADVERSARIES

How to guarantee forward and backward security with the previously proposed adversaries ?

Perfect eavesdropper, no active behavior.

Active adversary …
but still honest:

- Secrets disclosure
- No code injection

LOOKING FOR RANDOMNESS…

… a simple solution for a pure eavesdropper adversary

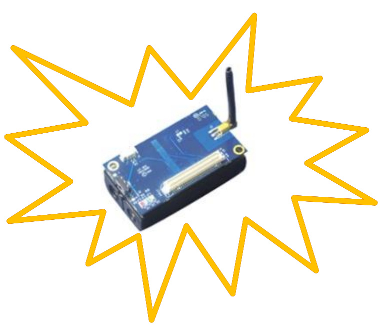
Let the secret key change at each round !

$$K_0 \xrightarrow{H} K_1 \xrightarrow{H} K_2 \xrightarrow{H} K_3 \xrightarrow{H} K_4 \xrightarrow{H}$$

OK !

But what if the adversary gets **more powerful** and takes a screw driver ?

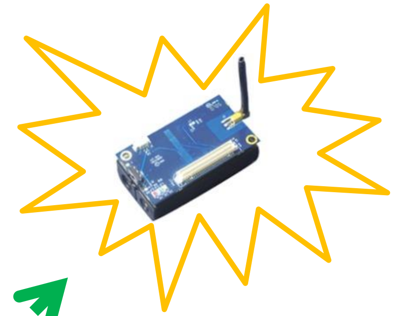
- The adversary will access all the data in the sensor
- All the secrets will be disclosed



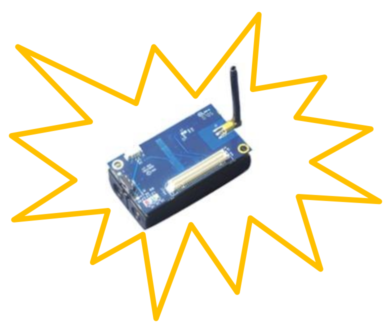
COPING WITH THE SCREW DRIVER... (1/3)

- Adversary
  - ❑ Randomly picks a sensor
  - ❑ Global eavesdropper

- Sensor
  - ❑ Complete secrets disclosure



Need for a new protocol that allows to re-gain secrecy even between **compromised peers** with a **global eavesdropper adversary**.



COPING WITH THE SCREW DRIVER… (2/3)

The question is:

Is there a way to generate a shared secret between two compromised pairs that is unknown to a global eavesdropper adversary ?

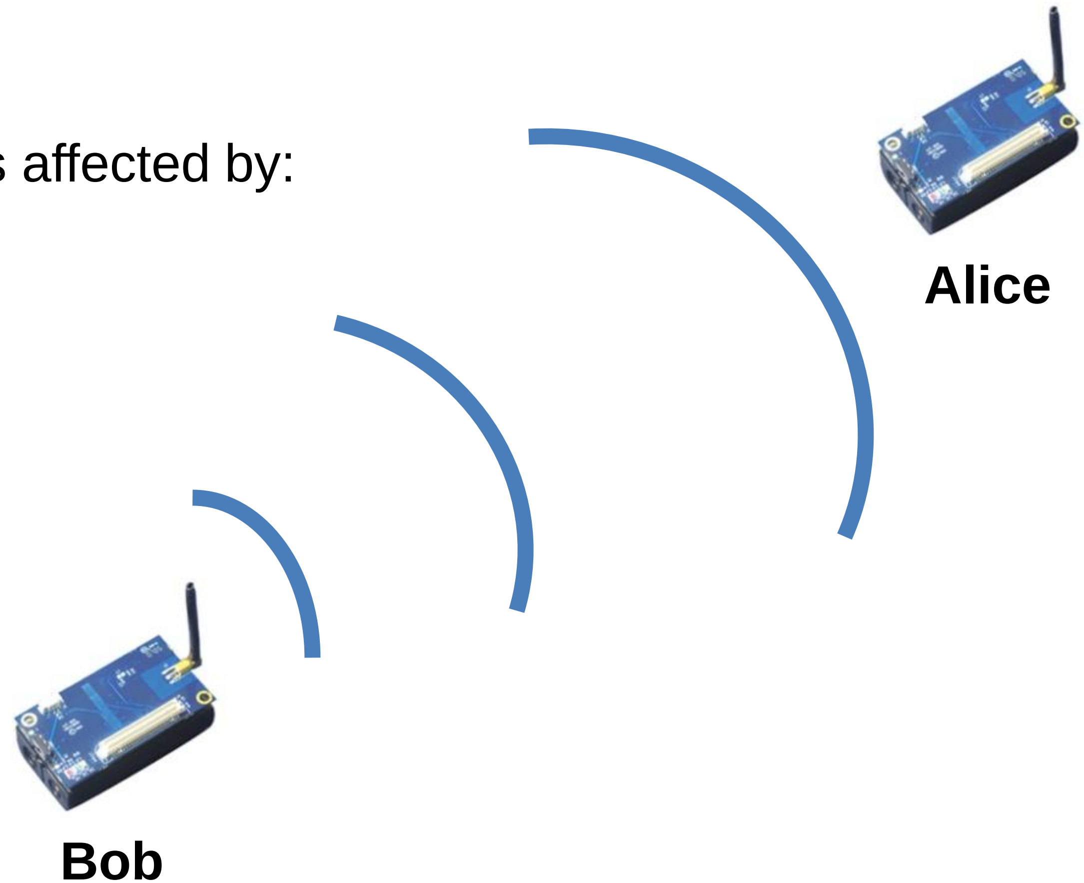
The received signal power may be a possible solution…

RECEIVED SIGNAL POWER - RSS

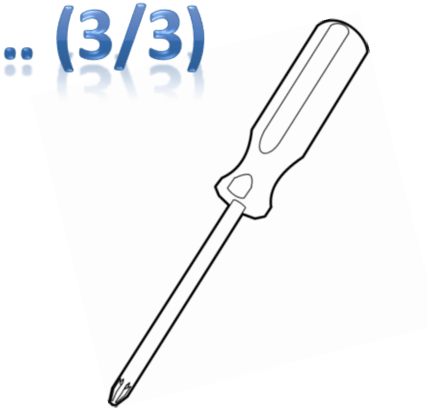
Each device features RSS estimation capability
CSMA cannot work without it

Received signal power is affected by:

- Distance
- Line of sight
- Multipath



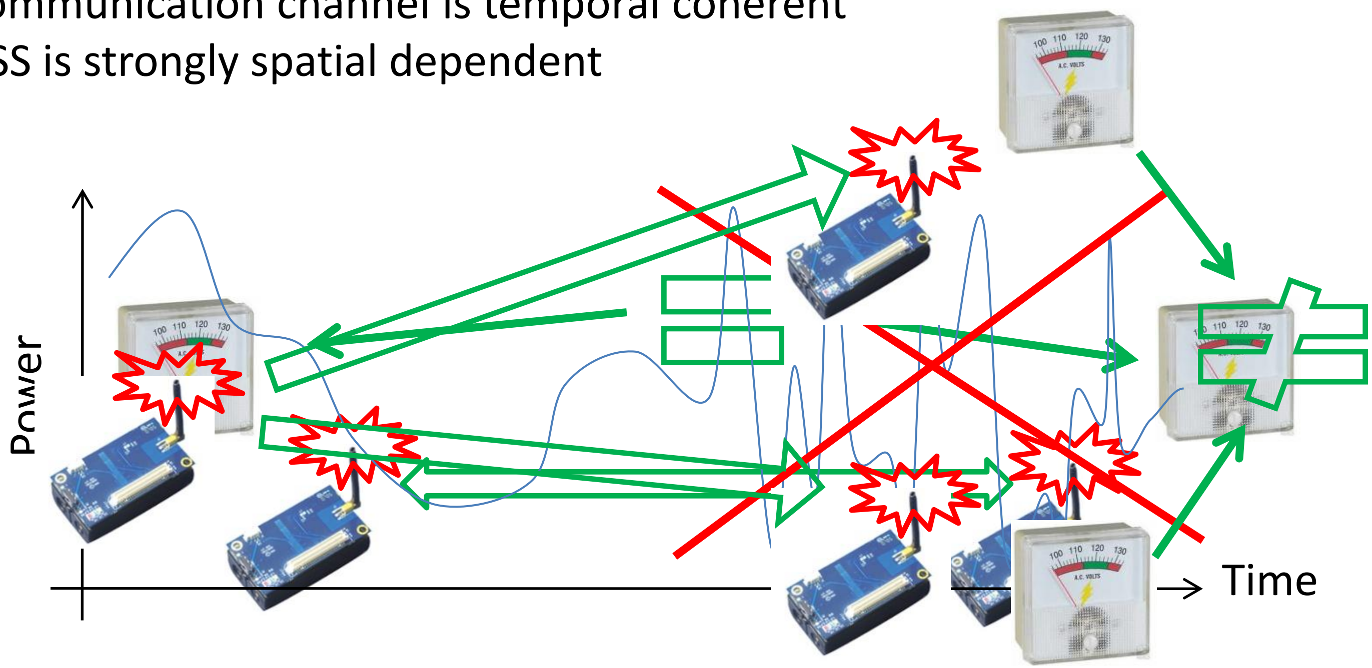
COPING WITH THE SCREW DRIVER… (3/3)



After the secret disclosure, the sensor should be able to regain its secret status in some way.

How to do this ?

Received Signal Strength (RSS) can help us…
- The communication channel is "almost" symmetric
- The communication channel is temporal coherent
- The RSS is strongly spatial dependent



OUTLINE

- Sensors and WSNs
- Security on WSNs
- Key establishment
  - Authentication
  - Secret generation
  - Entropy
- Well known solutions
- Intrusion resilience
  - Adversary models
  - Forward secrecy
  - Backward secrecy
- Alternative solution

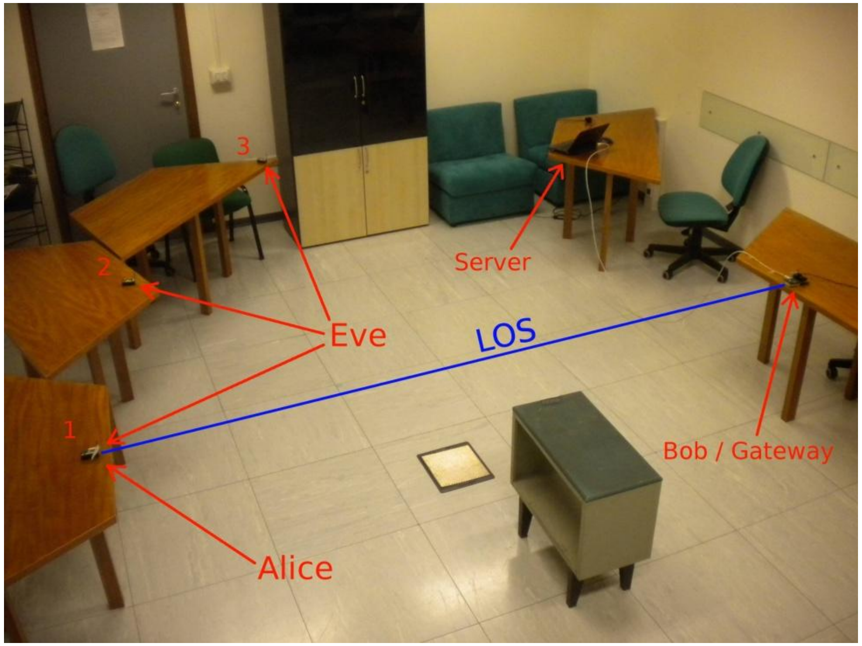
LET'S TAKE A LOOK AT A REAL SCENARIO

Alice wants to agree on a shared secret with Bob

Eve is aware of all the information in the network
- Alice/Bob memory content
- Alice/Bob algorithms

Eve wants to guess the on-going shared secret

How to deal with this scenario ?



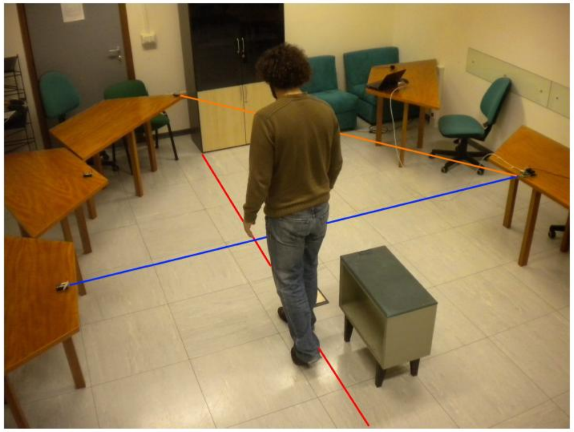
REAL SCENARIO – SIMPLE CUT

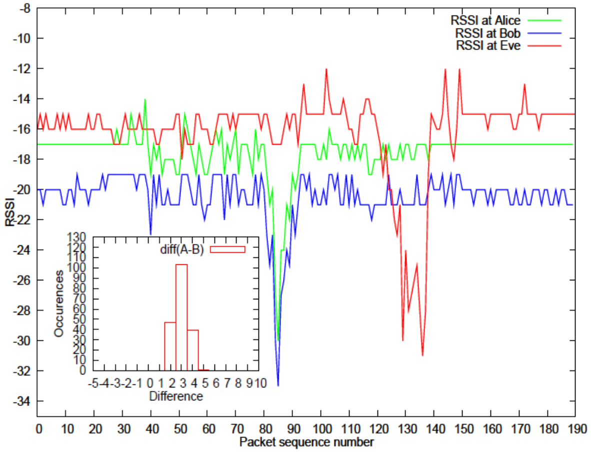
Simple cut of the line-of-sight between Alice and Bob

Alice and Bob experiment almost the same fluctuations during the cut

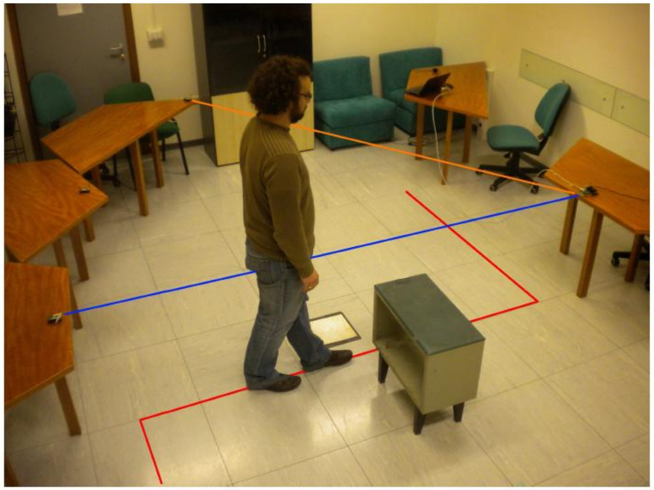
- There is a constant offset between the two RSS values
- There are fast fluctuations that prevent the two signals to be exactly the same

Eve cannot experience the same channel fluctuations due to her position





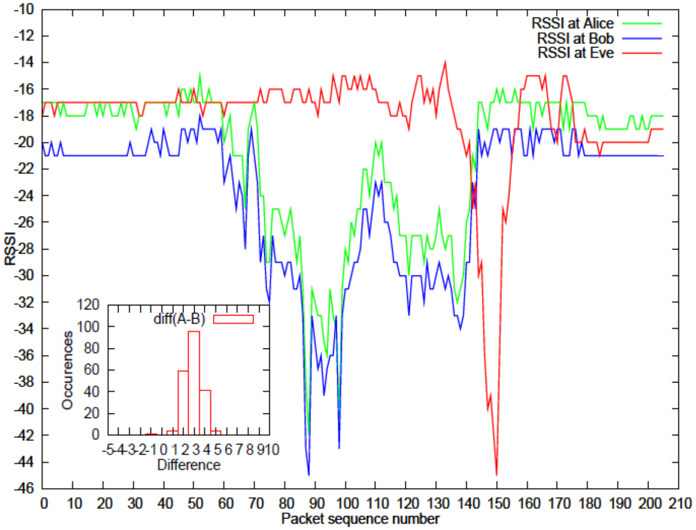
REAL SCENARIO – CROSS WALK



A person cross-walks the line-of-sight between Alice and Bob

Alice and Bob experiment almost the same fluctuations during the cut

- There is a constant offset between the two RSS values
- There are fast fluctuations that prevent the two signals to be exactly the same



Eve cannot experience the same channel fluctuations due to her position

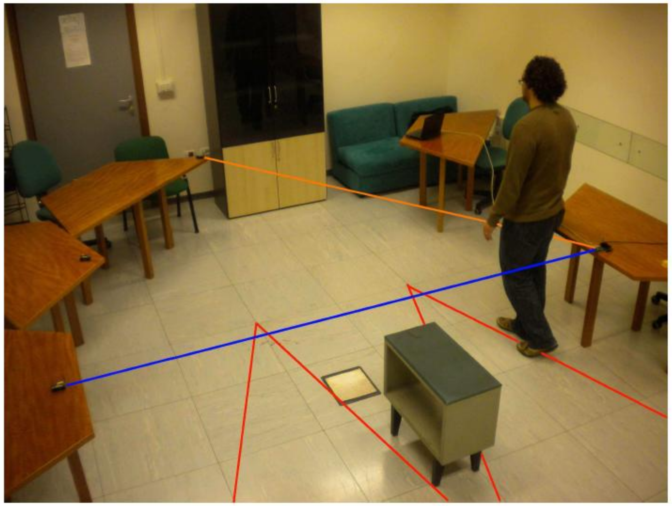
REAL SCENARIO – ZIG ZAG

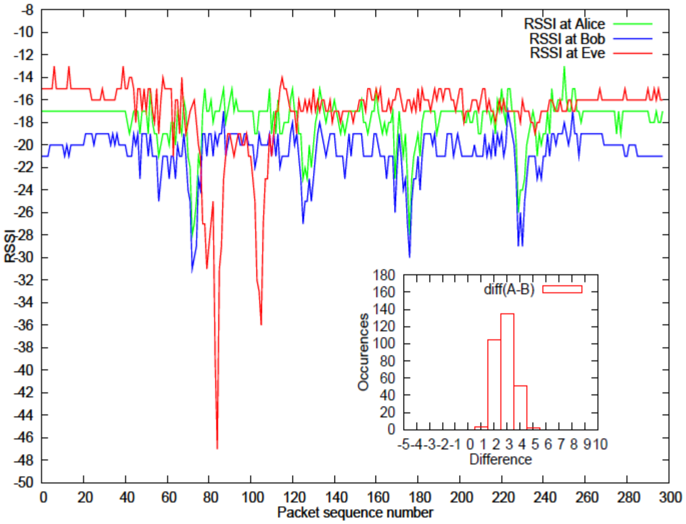
A person performs a zig-zag walk between Alice and Bob

Alice and Bob experiment almost the same fluctuations during the cut

- ❑ There is a constant offset between the two RSS values
- ❑ There are fast fluctuations that prevent the two signals to be exactly the same

Eve cannot experience the same channel fluctuations due to her position





RECEIVED POWER AS A SECRET GENERATOR

The estimates power (RSS) can be used to generate shared secrets between pairs

Fast fluctuations may prevent the agreement…

➢ A correction algorithm is needed

Static/empty environments cannot be considered with this algorithm

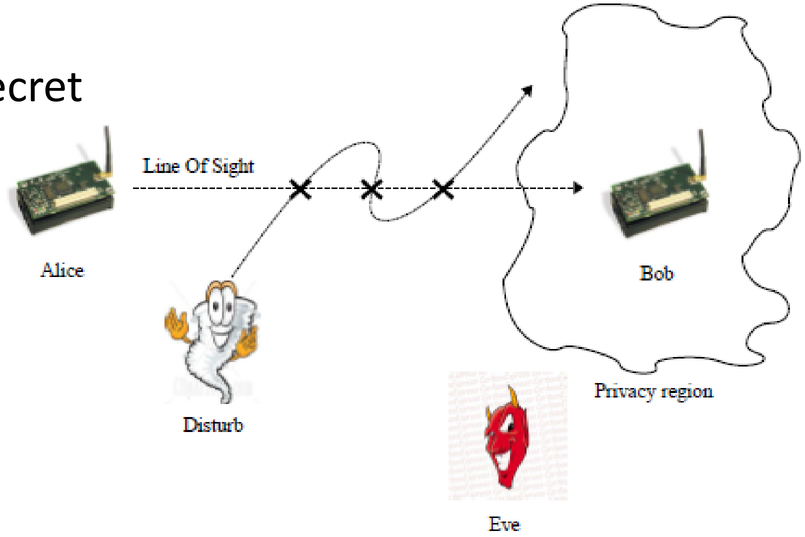
RSS is almost flat in static environments

Eve can easily guess the key

The "perfect" scenario is constituted by:

One or more disturbance events that affect the RSS values at Alice and Bob

A "privacy region" that protects Bob and prevents Eve to guess the on-going secret

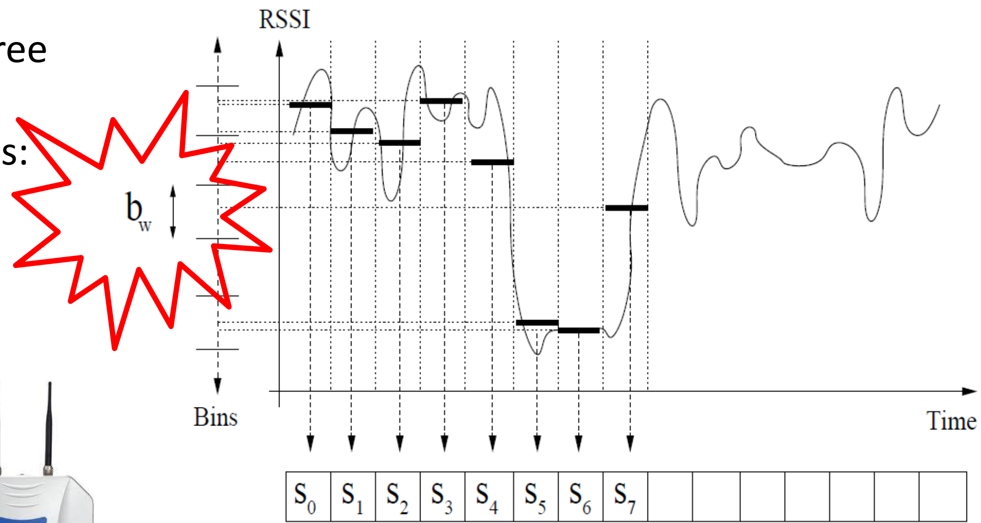


RANDOMNESS HARVESTING

… re-gaining a secret status

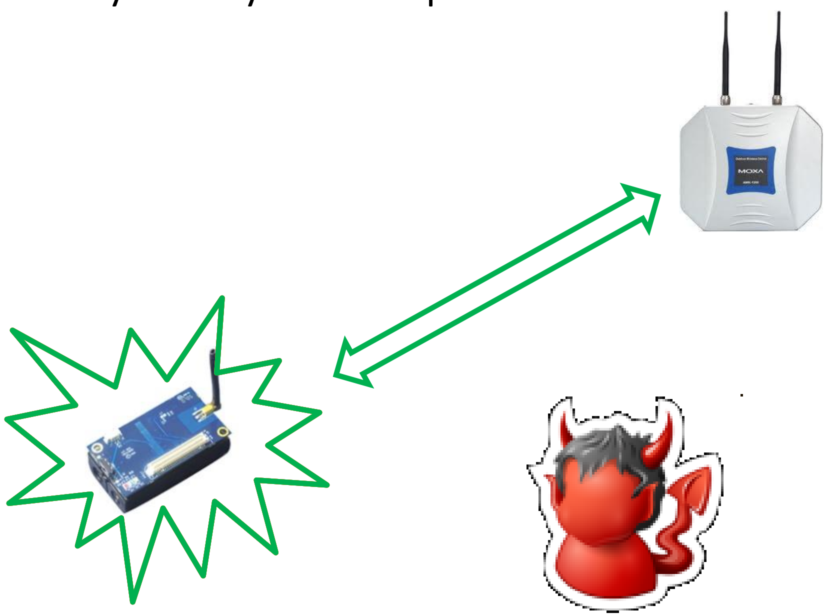
Randomness can be reliably extracted in three steps:

- Cleaning up fluctuations of the RSS values: MEAN
- Translate *w* RSS values to a symbol
- Collect *L* symbols to obtain a key
- Verify the key with the peer



$$\mathcal{A}: \underbrace{\underbrace{r^a_0,\ldots,r^a_{w-1}}_{s_0}\ \underbrace{r^a_w,\ldots,r^a_{2\cdot w-1}}_{s_1}\cdots\underbrace{r^a_{(L-2)\cdot w},\ldots,r^a_{(L-1)\cdot(w-1)}}_{s_{L-1}}}_{\mathcal{K}_1}$$

$$\mathcal{B}^0: \underbrace{\underbrace{r^0_0,\ldots,r^0_{w-1}}_{s_0}\ \underbrace{r^0_w,\ldots,r^0_{2\cdot w-1}}_{s_1}\cdots\underbrace{r^0_{(L-2)\cdot w},\ldots,r^0_{(L-1)\cdot(w-1)}}_{s_{L-1}}}_{\mathcal{K}_1}$$



REAL DEPLOYMENT

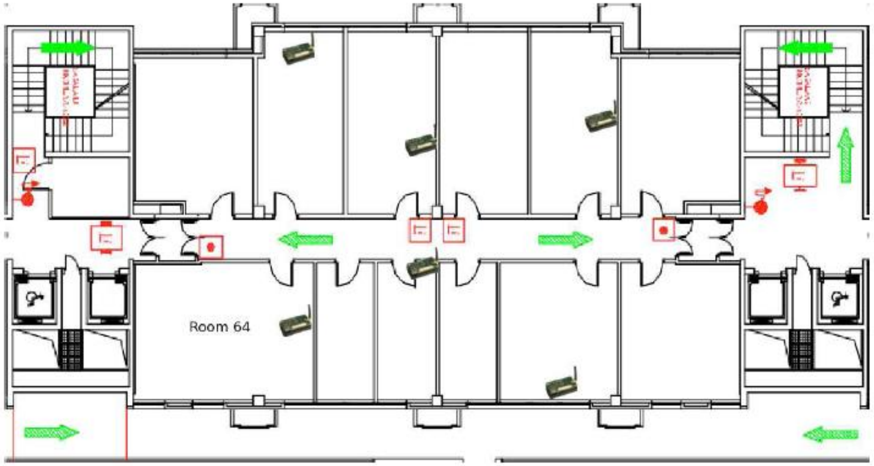
Let's consider a real deployment with:

- 6 anchors
- A mobile user with **Alice on her neck** and **Eve on her wrist**

Anchors:

- Belong to a secure infrastructure .
- Are trusted and can communicate securely among them.
- *E.g.: Eve is interested on compromising Alice and not the anchors.*

Alice wants to pair with one or more anchors

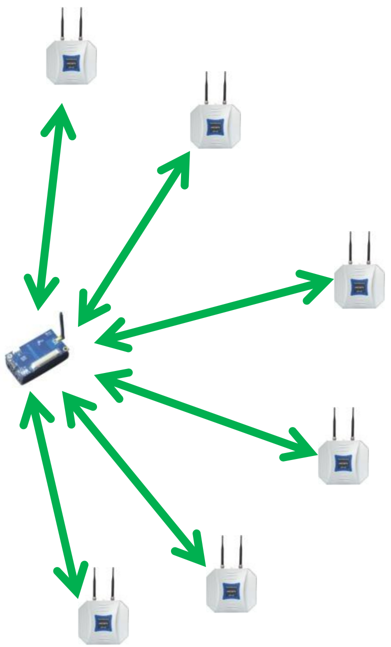


SMART ENVIRONMENT SCENARIO

Baseline scenario

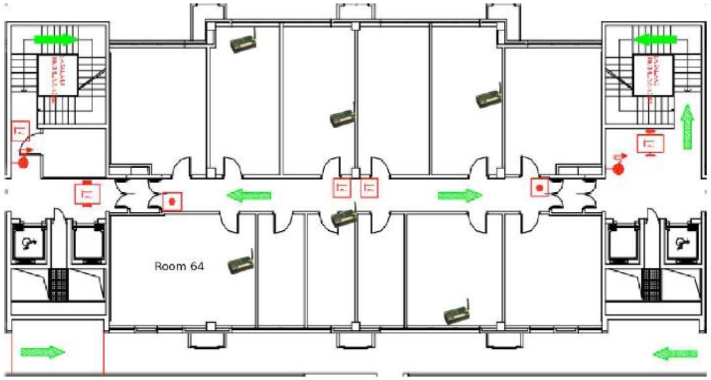
6-anchors scenario

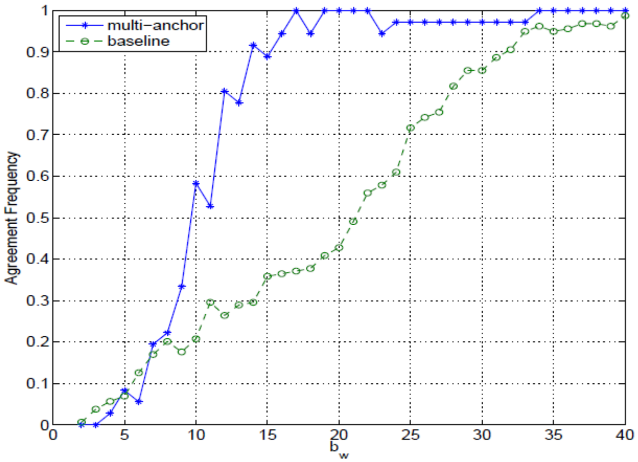
Rounds / Anchors	$0 \ldots Lw-1$	$Lw \ldots 2Lw-1$	$2Lw \ldots 3Lw-1$	$3Lw \ldots 4Lw-1$	$\rightarrow$
$\mathcal{B}^0$	$\mathcal{K}_0^0$	$\mathcal{K}_1^0$	$\mathcal{K}_2^0$	$\mathcal{K}_3^0$	$\ldots$
$\mathcal{B}^1$	$\mathcal{K}_0^1$	$\mathcal{K}_1^1$	$\mathcal{K}_2^1$	$\mathcal{K}_3^1$	$\ldots$
$\mathcal{B}^2$	$\mathcal{K}_0^2$	$\mathcal{K}_1^2$	$\mathcal{K}_2^2$	$\mathcal{K}_3^2$	$\ldots$
$\mathcal{B}^3$	$\mathcal{K}_0^3$	$\mathcal{K}_1^3$	$\mathcal{K}_2^3$	$\mathcal{K}_3^3$	$\ldots$
$\mathcal{B}^4$	$\mathcal{K}_0^4$	$\mathcal{K}_1^4$	$\mathcal{K}_2^4$	$\mathcal{K}_3^4$	$\ldots$
$\mathcal{B}^5$	$\mathcal{K}_0^5$	$\mathcal{K}_1^5$	$\mathcal{K}_2^5$	$\mathcal{K}_3^5$	$\ldots$
Hashing	$\underbrace{}$ $\downarrow$ $H(\circ)$ $\downarrow$	$\underbrace{}$ $\downarrow$ $H(\circ)$ $\downarrow$	$\underbrace{}$ $\downarrow$ $H(\circ)$ $\downarrow$	$\underbrace{}$ $\downarrow$ $H(\circ)$ $\downarrow$	$\ldots$ $\ldots$ $\ldots$ $\ldots$
Session Keys	$\mathbf{K}_1$	$\mathbf{K}_2$	$\mathbf{K}_3$	$\mathbf{K}_4$	$\ldots$

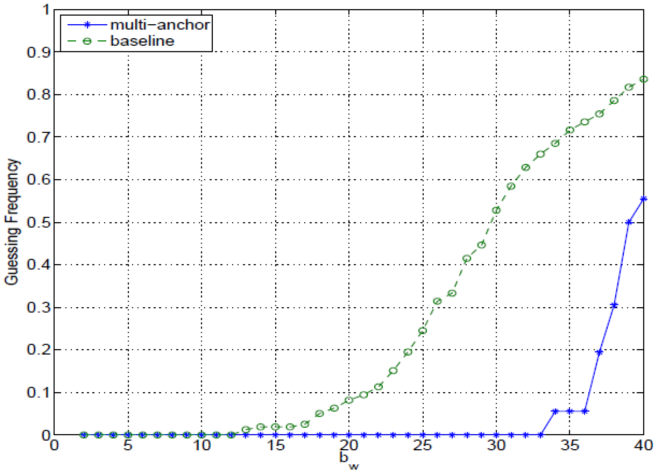


MEASUREMENTS AND PERFORMANCE (1/2)

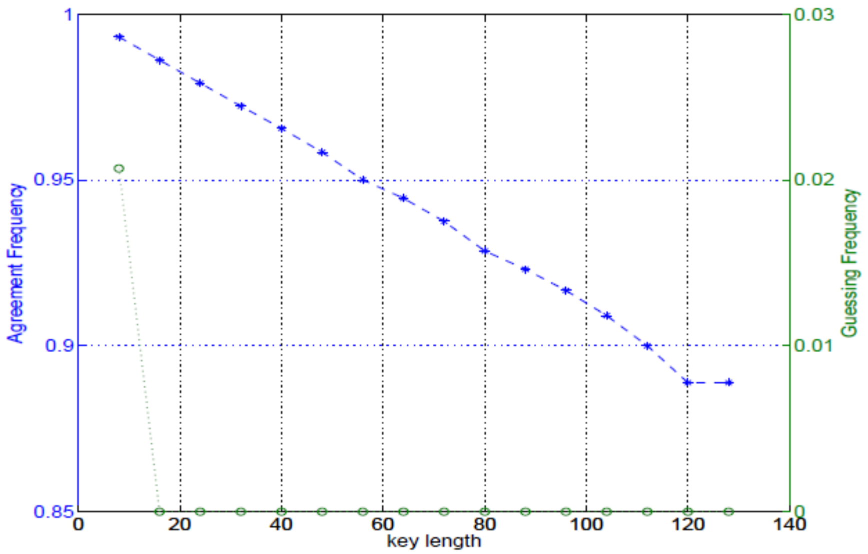
- Indoor scenario with 6-anchors
  - ✓ Office environment during working hours
- Adversary position
  - ✓ Sensor on the neck and adversary on the wrist
- Agreement frequency
  - ✓ Peers experience the same key and commit on it
- Guessing frequency
  - ✓ The adversary is able to guess the key
- Mean computed over the last 5 samples
- Key length 32 bits





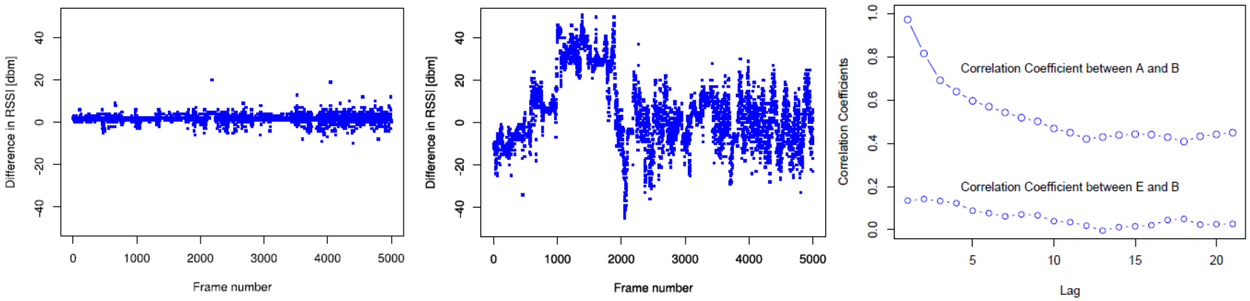


MEASUREMENTS AND PERFORMANCE (2/2)

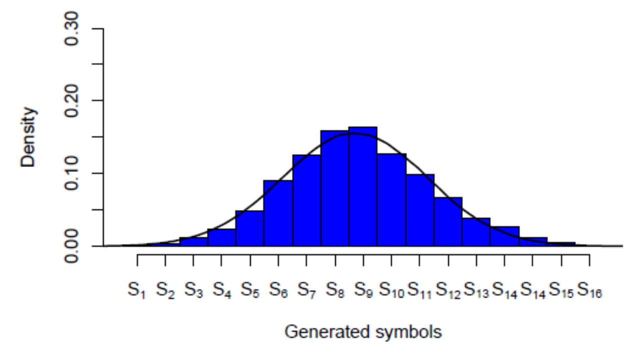


- 6-anchor scenario
- Bin width fixed to 27
- Key length increases security
- Longer keys are more difficult to achieve
- Longer keys are more difficult to guess

HOW SECRET ARE THE SECRET KEYS ?



- RSS values among the peers are well correlated but not between the peer and the adversary.
- Symbols values can be modeled as a Gaussian random variable.
- The entropy of the normal distributions obtained varying b_w is close to a "perfect" uniform distribution.



b_w	2	4	8	16
Normal Distribution	3.39	2.92	1.57	0.98
Uniform Distribution	4	3.16	2.32	1.58

FUTURE WORKS IN SENSORS PAIRING

- Entropy analysis
- Privacy region analysis
- Looking for different algorithms to perform the agreement
- Pairing between smart phones

THE END

Any questions ?