Key-sharing via channel randomness in narrowband body area networks: Is everyday movement sufficient?

Leif W. Hanlen, D. Smith, J. Zhang, D. Lewis

leif.hanlen@nicta.com.au

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

NICTA Members
NICTA Partners

Security for Body-Area Networks

NICTA

Problem

1. *Some devices need extreme security: wireless pace-maker*
2. *Use the randomness of physical channel to generate keys?*
3. *Does normal movement give enough randomness?*

- Motivation
- Background

- Simulation & Experimental setup
- Implications

What this is not

Not interested in HOW to make the keys, just the maximal key length to achieve perfect secrecy

Interlude 1: IEEE 802.15 Task Group-6

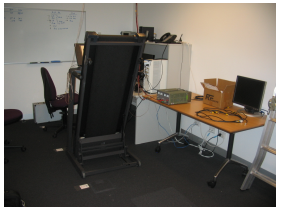
NICTA

- Short range (3m) personal area networking for *Body Area Networking*
- Support for data rates: 10kbps up to 10Mbps
- Ultra-low power
- 256 nodes per pico-net. Up to 10 pico-nets co-located.
- AES style security









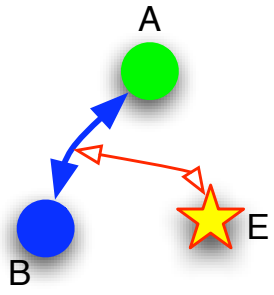
[TG6-08] IEEE802.15-0808-31-05-0006 TG6 Proposal Comparison Criteria

[online] https://mentor.ieee.org/802.15/documents/

How many people fit in a 6m cube?

NICTA

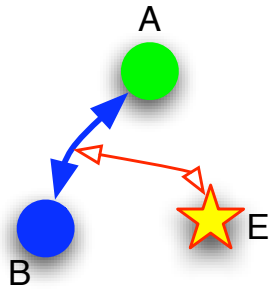
- *Your arm span is approx. 2.5m. how many people are within the 6m x 6m x 6m cube near you* **right now.**
- How certain are you that none those people has a packet sniffer operating on their laptop?
- How happy would you be to trust your pacemaker in this environment?
- Bluetooth devices [10m range] have been "snarfed" at 1.78km
- Alice & Bob are two trusted sensors.
- Eve is not trusted.



  - Uncrackable (perfect) [Information Theoretic]
  - Really hard to crack [Computational]

How many people fit in a 6m cube?

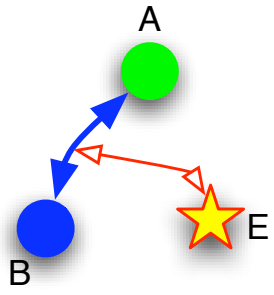
NICTA



- *Your arm span is approx. 2.5m. how many people are within the 6m x 6m x 6m cube near you* **right now.**
- How certain are you that none those people has a packet sniffer operating on their laptop?
- How happy would you be to trust your pacemaker in this environment?
- Bluetooth devices [10m range] have been "snarfed" at 1.78km
- Alice & Bob are two trusted sensors.
- Eve is not trusted.
  - Uncrackable (perfect) [Information Theoretic]
  - Really hard to crack [Computational]

How many people fit in a 6m cube?

NICTA

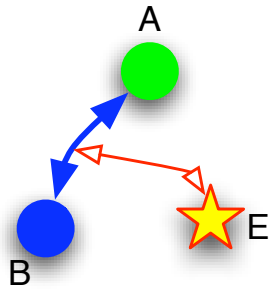


- *Your arm span is approx. 2.5m. how many people are within the 6m x 6m x 6m cube near you* **right now.**
- How certain are you that none those people has a packet sniffer operating on their laptop?
- How happy would you be to trust your pacemaker in this environment?
- Bluetooth devices [10m range] have been "snarfed" at 1.78km
- Alice & Bob are two trusted sensors.
- Eve is not trusted.
  - Uncrackable (perfect) [Information Theoretic]
  - Really hard to crack [Computational]

How many people fit in a 6m cube?

NICTA

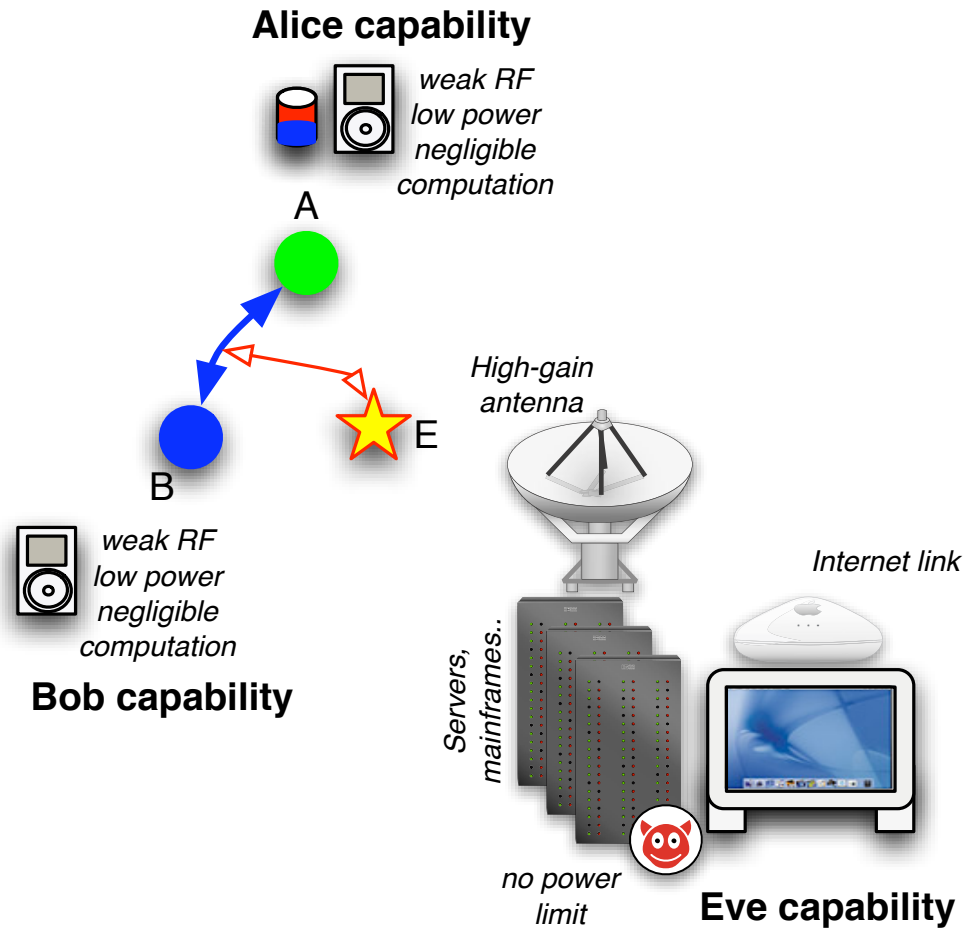
- *Your arm span is approx. 2.5m. how many people are within the 6m x 6m x 6m cube near you* **right now.**
- How certain are you that none those people has a packet sniffer operating on their laptop?
- How happy would you be to trust your pacemaker in this environment?



- Bluetooth devices [10m range] have been "snarfed" at 1.78km
- Alice & Bob are two trusted sensors.
- Eve is not trusted.

  - Uncrackable (perfect) [Information Theoretic]
  - Really hard to crack [Computational]

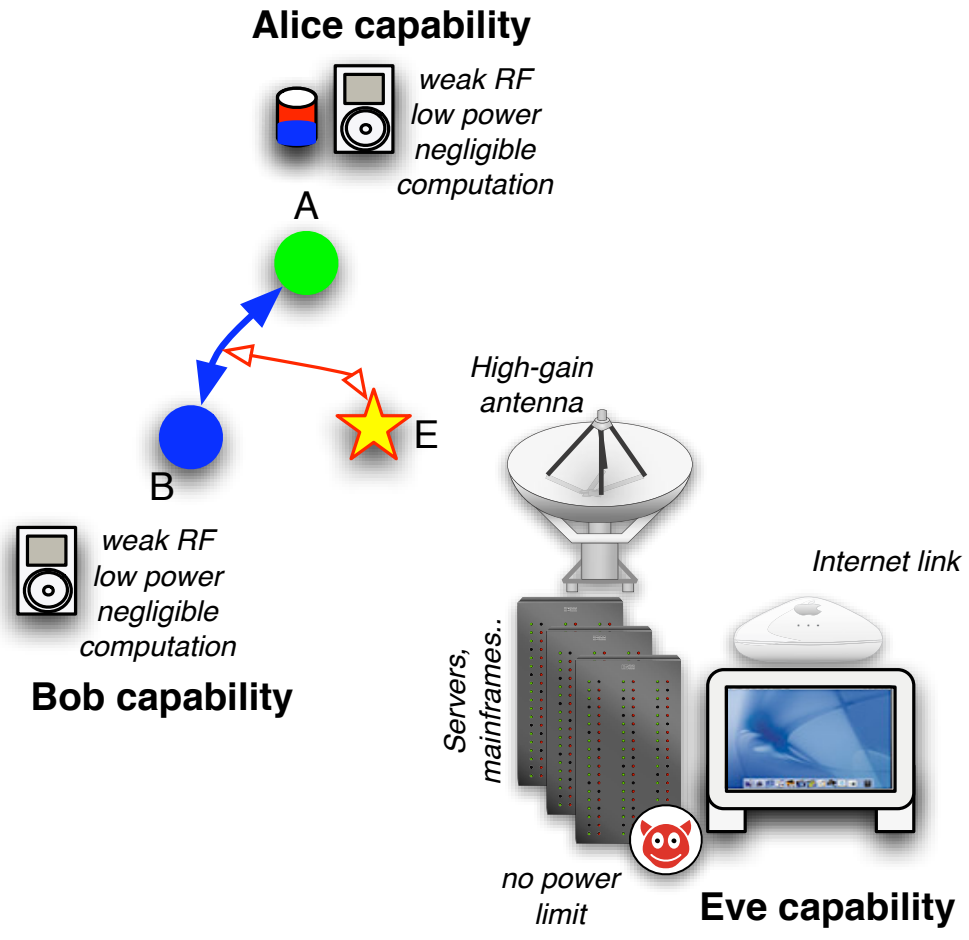
How much effort should we take to stop Alice?



- Eve can spoof, jam, listen
- Eve has unlimited transmit power
- Eve has unlimited computation power

Motivates desire to have perfect secrecy. **BUT.** Can't give everyone individual one-time-pad: use channel randomness instead.

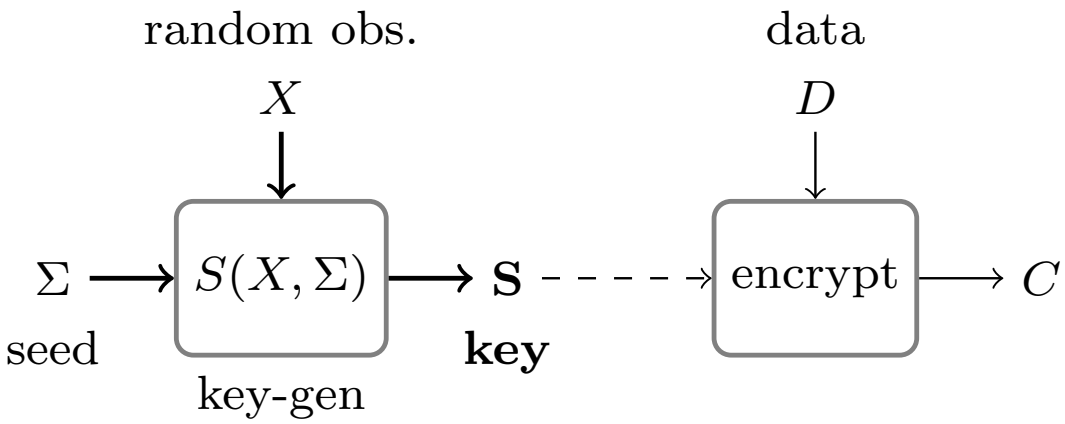
How much effort should we take to stop Alice?



- Eve can spoof, jam, listen
- Eve has unlimited transmit power
- Eve has unlimited computation power

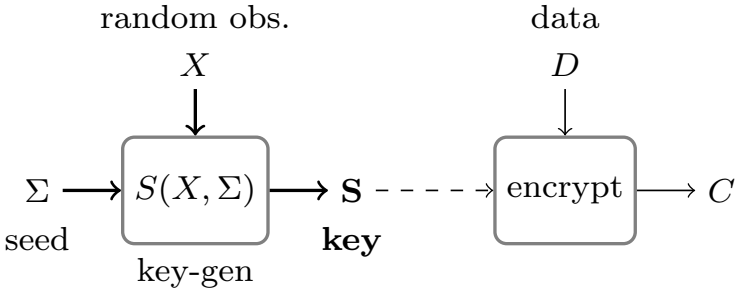
Motivates desire to have perfect secrecy. **BUT.** Can't give everyone individual one-time-pad: use channel randomness instead.

Computational vs Perfect secrecy



Key S, Message data D and coded-message C. S is used to encrypt D via some algorithm (eg. XOR)

Interlude 2: Computational vs Perfect secrecy



Key S, Message data D and coded-message C. S is used to encrypt D via some algorithm (eg. XOR)

Computational secrecy

- $D \mapsto C$ is *hard* to invert
- Weak keys (short S) can be improved by using new keys intermitently [LeonSalas08]

Perfect secrecy

- Based on Shannon [Sha49]
- Entropy of S is larger than entropy of D
- One-time-pad is an example

[LeonSalas08] W. D. Leon-Salas. *Joint encryption/multiple access for body area sensor networks.* Bodynets 2008
[Sha49] C. E. Shannon. *Communication theory of secrecy systems.* May 1949

Design Specification

1. Alice & Bob cannot do much "extra" work for security
2. Alice & Bob cannot have special encryption hardware

- Channel RSSI measurements are implicit in radio designs: can use this at minimal extra implementation cost
- Alice makes channel measurements X
- Bob makes channel measurements Y
- Alice & Bob create common key S, Eve will try to guess this key using measurements Z.

Question

How small must S be so that Eve cannot guess it?
recall: $H(D) \leq H(S)$

Design Specification

NICTA

1. Alice & Bob cannot do much "extra" work for security
2. Alice & Bob cannot have special encryption hardware

- Channel RSSI measurements are implicit in radio designs: can use this at minimal extra implementation cost
- Alice makes channel measurements X
- Bob makes channel measurements Y
- Alice & Bob create common key S, Eve will try to guess this key using measurements Z.

Question

How small must S be so that Eve cannot guess it?

recall: $H(D) \leq H(S)$

Design Specification

NICTA

1. Alice & Bob cannot do much "extra" work for security
2. Alice & Bob cannot have special encryption hardware

- Channel RSSI measurements are implicit in radio designs: can use this at minimal extra implementation cost
- Alice makes channel measurements X
- Bob makes channel measurements Y
- Alice & Bob create common key S, Eve will try to guess this key using measurements Z.

Question

How small must S be so that Eve cannot guess it?

recall: $H(D) \leq H(S)$

Limits to $H(S)$

NICTA

Theorem (Tse etal)

$H(S)$ is upper bounded by denying Eve write-access, and the bound is:

$$H(S) \leq \min\{I(X;Y), I(X;Y|Z)\}$$

Rule-of-thumb first:

1. $I(X;Y) \leq H(X) + H(Y)$ for $X \perp Y$
   - $I(X;Y|Z) \leq H(X|Z) \leq H(X)$
2. $H(S) \leq H(X) \approx H(\text{channel})$

Overbound gives easy relation to entropy of channel

- Channel is stable up to 15ms, fades between -10dB and -70dB [Min08], and has a Weibull distribution.
- $H(S)$ is bounded by 96bps.

[Min08] D. Miniutti etal. *Narrowband channel characterization for body area networks* [IEEE-802.15.08.0421.00.0006]. Jun 2008

Limits to $H(S)$

NICTA

Theorem (Tse etal)

$H(S)$ is upper bounded by denying Eve write-access, and the bound is:

$$H(S) \leq \min\{I(X;Y), I(X;Y|Z)\}$$

Rule-of-thumb first:

1. $I(X;Y) \leq H(X) + H(Y)$ for $X \perp Y$
   - $I(X;Y|Z) \leq H(X|Z) \leq H(X)$
2. $H(S) \leq H(X) \approx H(\text{channel})$

Overbound gives easy relation to entropy of channel

- Channel is stable up to 15ms, fades between -10dB and -70dB [Min08], and has a Weibull distribution.
- $H(S)$ is bounded by 96bps.

[Min08] D. Miniutti etal. *Narrowband channel characterization for body area networks* [IEEE-802.15.08.0421.00.0006]. Jun 2008

Limits to $H(S)$

NICTA

Theorem (Tse etal)

$H(S)$ is upper bounded by denying Eve write-access, and the bound is:

$$H(S) \leq \min\{I(X;Y), I(X;Y|Z)\}$$

Rule-of-thumb first:

1. $I(X;Y) \leq H(X) + H(Y)$ for $X \perp Y$
   - $I(X;Y|Z) \leq H(X|Z) \leq H(X)$
2. $H(S) \leq H(X) \approx H(\text{channel})$

Overbound gives easy relation to entropy of channel

- Channel is stable up to 15ms, fades between -10dB and -70dB [Min08], and has a Weibull distribution.
- $H(S)$ is bounded by 96bps.

[Min08] D. Miniutti etal. *Narrowband channel characterization for body area networks* [IEEE-802.15.08.0421.00.0006]. Jun 2008

Limits to $H(S)$

NICTA

Theorem (Tse etal)

$H(S)$ is upper bounded by denying Eve write-access, and the bound is:

$$H(S) \leq \min\{I(X;Y), I(X;Y|Z)\}$$

Rule-of-thumb first:

1. $I(X;Y) \leq H(X) + H(Y)$ for $X \perp Y$
   - $I(X;Y|Z) \leq H(X|Z) \leq H(X)$
2. $H(S) \leq H(X) \approx H(\text{channel})$

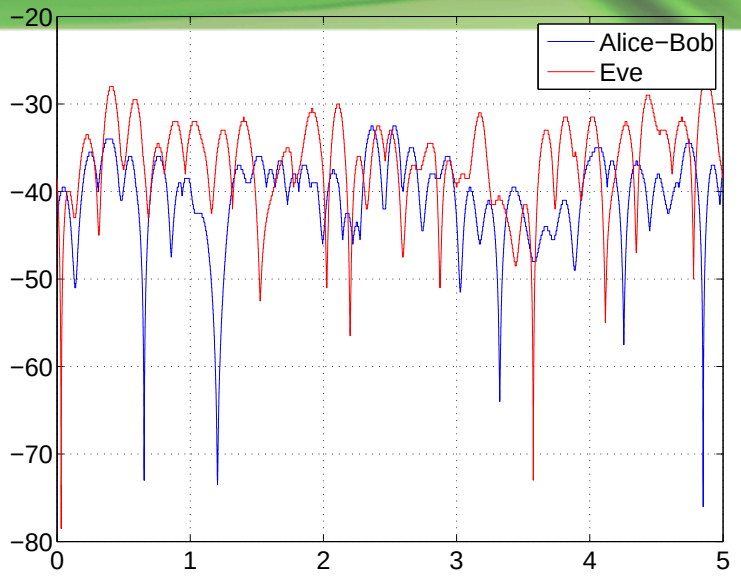
Overbound gives easy relation to entropy of channel

- Channel is stable up to 15ms, fades between -10dB and -70dB [Min08], and has a Weibull distribution.
- $H(S)$ is bounded by 96bps.

[Min08] D. Miniutti etal. *Narrowband channel characterization for body area networks*

[IEEE-802.15.08.0421.00.0006]. Jun 2008

Perfect secrecy

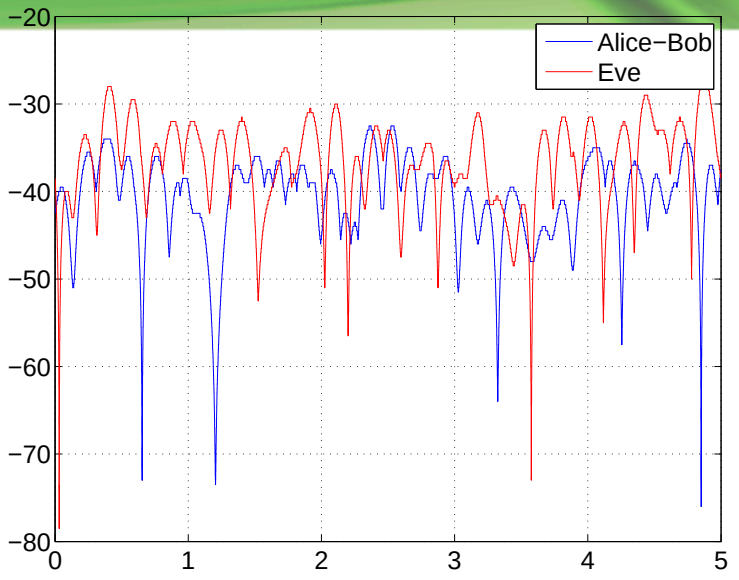


Channel RSSI for Alice-Bob X, and Eve-Bob Z, 5 seconds, using [Smith08]

- The channels Alice-Bob and Bob-Eve are correlated.
- $H(X|Z) \ll H(X)$ implies previous bound is very loose.
- $H(S)$ below 4bps
- *requirement* $H(D) < H(S)$ *is not practical*

[Smith08] D. Smith etal. *Matlab code for generating BAN fading profile.* IEEE-802.15-08-0850-00-0006. Nov 2008

Perfect secrecy



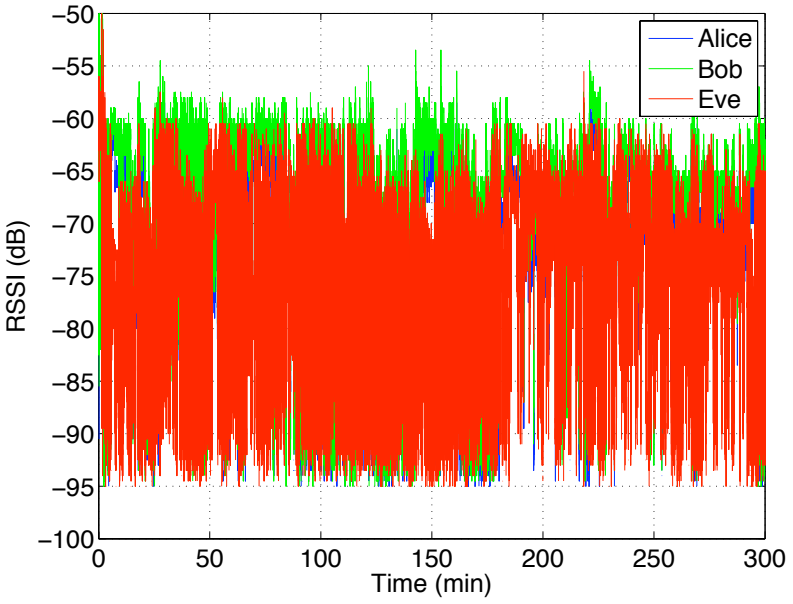
Channel RSSI for Alice-Bob X, and Eve-Bob Z, 5 seconds, using [Smith08]

- The channels Alice-Bob and Bob-Eve are correlated.
- $H(X|Z) \ll H(X)$ implies previous bound is very loose.
- $H(S)$ below 4bps
- *requirement* $H(D) < H(S)$ *is not practical*

[Smith08] D. Smith etal. *Matlab code for generating BAN fading profile.* IEEE-802.15-08-0850-00-0006. Nov 2008

Validation from channel measurements

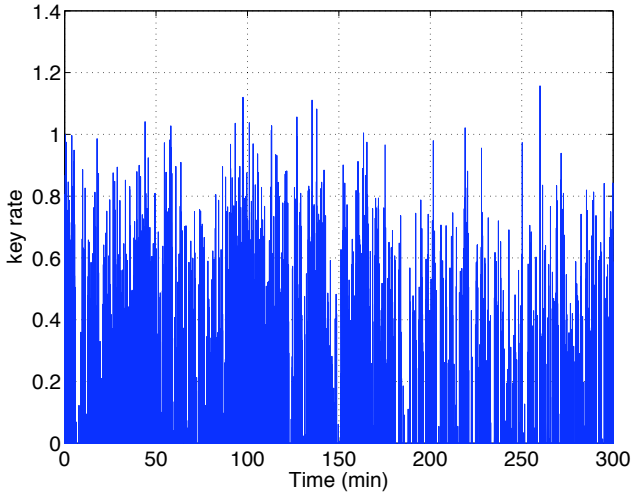
Measurement set-up.
Wearable transceiver using
TI-CC2240 chip



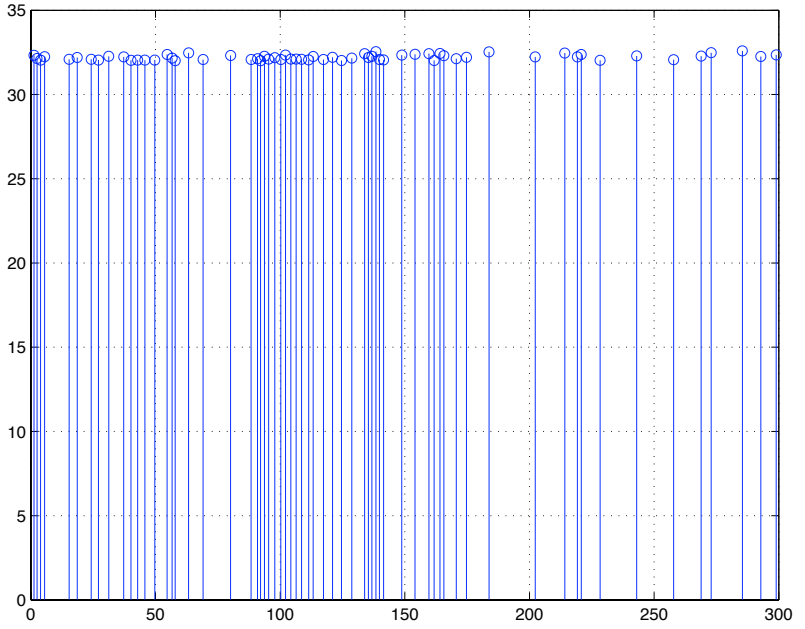
Channel RSSI .

- Here we will use hardware measurements based on TI-C2240 802.15.4 transceiver *de-tuned to 2360MHz*

Channel measurements



Key rate $H(S)$ as function of time.



Time between 32bit secure keys (mins).

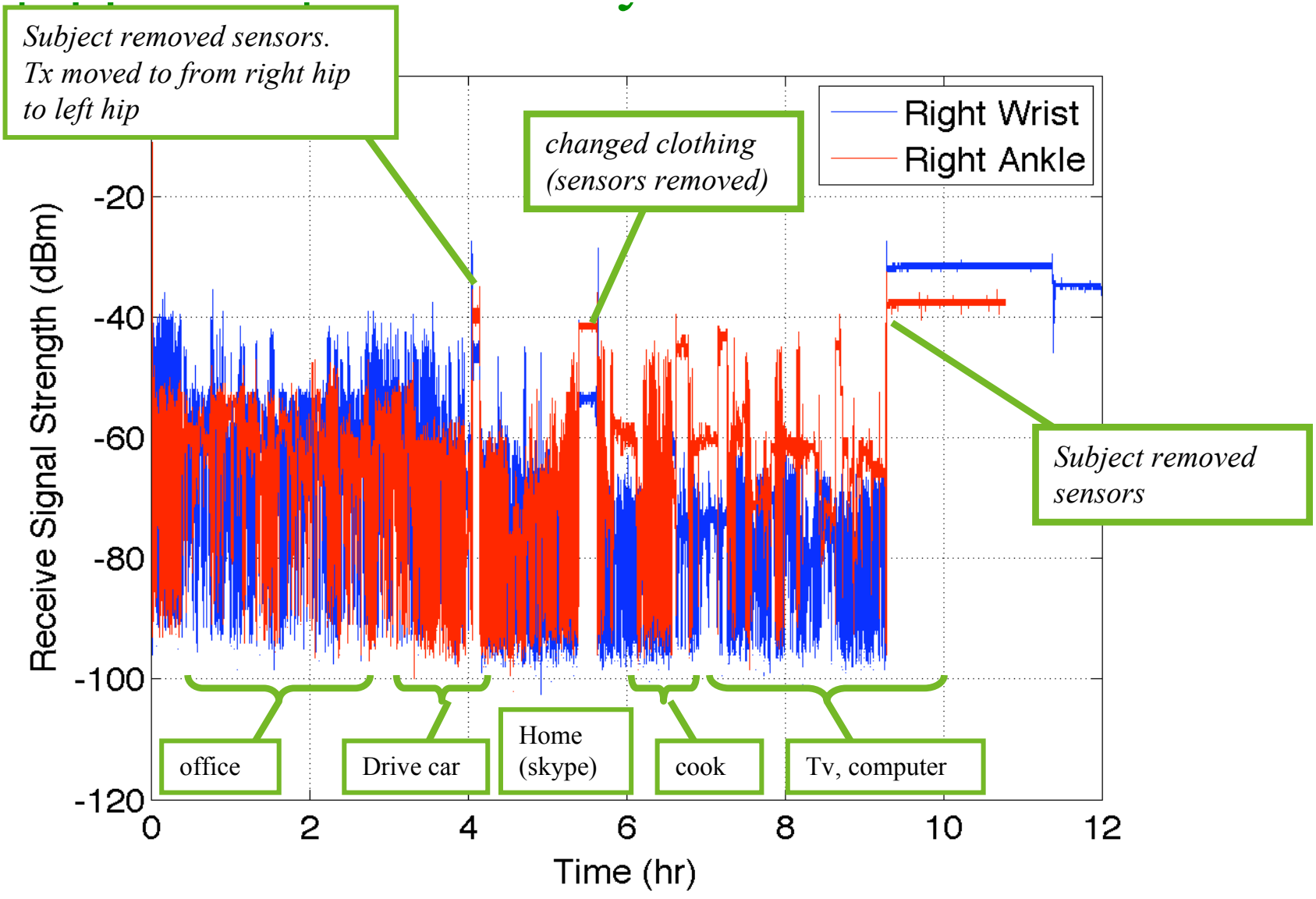
- Alice & Bob can use random process to generate secure 32-bit keys every few minutes
- Apply to cryptography as new key.

Conclusions

NICTA

- Security will be a concern in BAN's (especially when wireless controls actuators)
- Random channel to low rate to generate perfect security (4bps is not practical)
- Can store random bits to generate a "new" 32-bit (or any other length) key every few minutes.

Appendix: Channel dynamics over 10 hours



From NICTA IEEE submission Mar 2009