UNIVERSITY OF OULU


# Watermark-based Secure Communications in Safety-Related Scenarios

**S. Soderi**‡, L. Mucchi*, M. Hämäläinen‡, A. Piva* and J. Iinatti‡

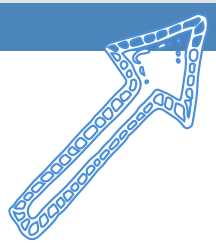
‡*Centre for Wireless Communications, University of Oulu, Oulu, Finland*

**Department of Information Engineering, University of Florence, Florence, Italy*

***SSIE 2016 July 3-9, 2016 – Brixen, Italy.***

CWC Oulu CENTRE FOR WIRELESS COMMUNICATIONS University of Oulu

# Background



## Security main topic


Security Engineering as multidisciplinary field

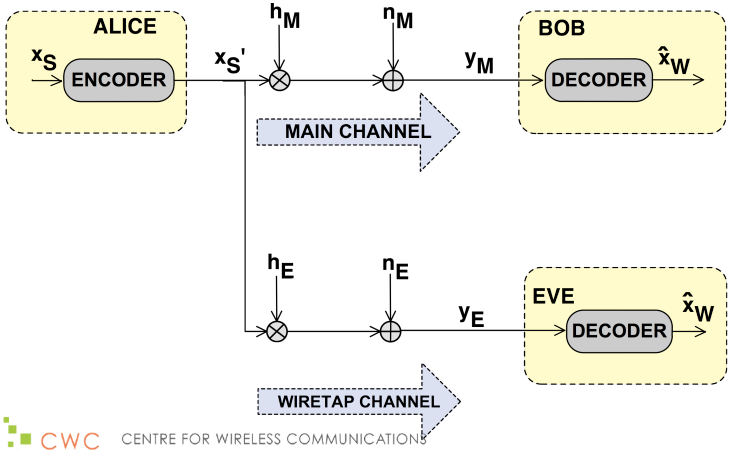
Multi-level analysis of ICT's Security: physical layer, network layer,…

# State of Art: **Phy** **L**ayer **Sec**urity (1/2)

Metrics

- ✧ Shannon – Perfect secrecy $I\left((x_S)^N;(x'_S)^N\right)=0$
  - No mutual info. between $x_S^N$ and $x_S'^N$
- ✧ Maurer – Strong Secrecy $\lim_{N\to\infty} I\left((x_S)^N;(y_E)^N\right)=0$
  - Mutual info. → 0 when N→∞
- ✧ Wyner – Weak Secrecy $\lim_{N\to\infty} \frac{1}{N} I\left((x_S)^N;(y_E)^N\right)=0$
  - The leaked info. is asymptotically 0
  - Definition of Secrecy Capacity ($C_S$)

## Csíszar




## Non-degraded wiretap channel model

- Extends Wyner;
- Bob and Eve have independent channels
  - $C_s$ = 0 when Eve has better Channel.
- Weak secrecy → practical interest;
- Reference model for this research.

# State of Art: **P**hy **L**ayer **Sec**urity (2/2)

## Security Services

Availability
**resources' accessibility** and **usability**.

Integrity
messages are **received as sent** without any **modification**, or **improper information destruction**.

Confidentiality
protect **proprietary information**, implementing **mathematical algorithms** to transform data

Authentication
**two communicating entities are who they claim to be**.

This research
Mitigations against
Confidentiality attacks

## Objective of PLSec

**Reliable** secure communication between Alice and Bob, at a target secure rate, **leaking the least** possible number of bits.

# Context (1/2)

Medical ICT

- Safety-related applications;
- WBAN:
  Worn and Implanted devices to monitor patients' vital signs.

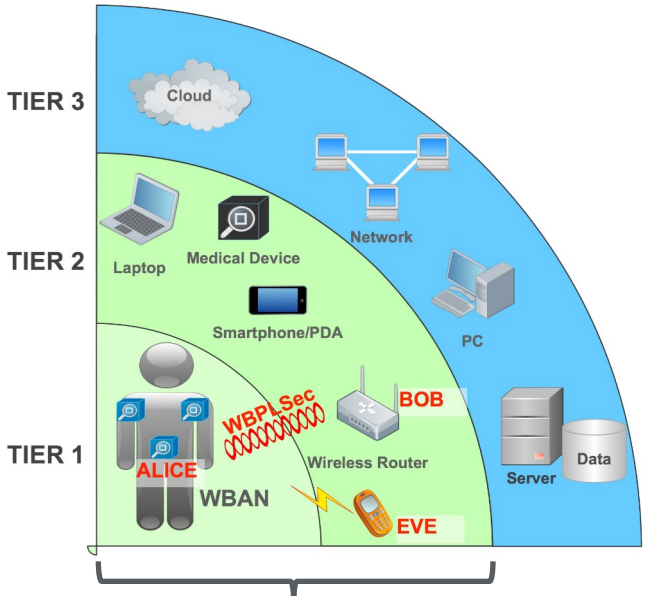
**Hacking Safety systems:**

- Compromise availability (Best Case);
- Fatal accidents to people (Worst Case).

## Risk in Medical ICT

The combination of continuous glucose monitor (CGM) with insulin pump is used for a better diabetics' treatment but, the **wireless link between these medical devices can be attacked** with a high risk for patient's safety.

# Context (2/2)




- ✓ WBAN, physical layer security can provide awesome advantages in terms **of lower number of computations** than cryptography

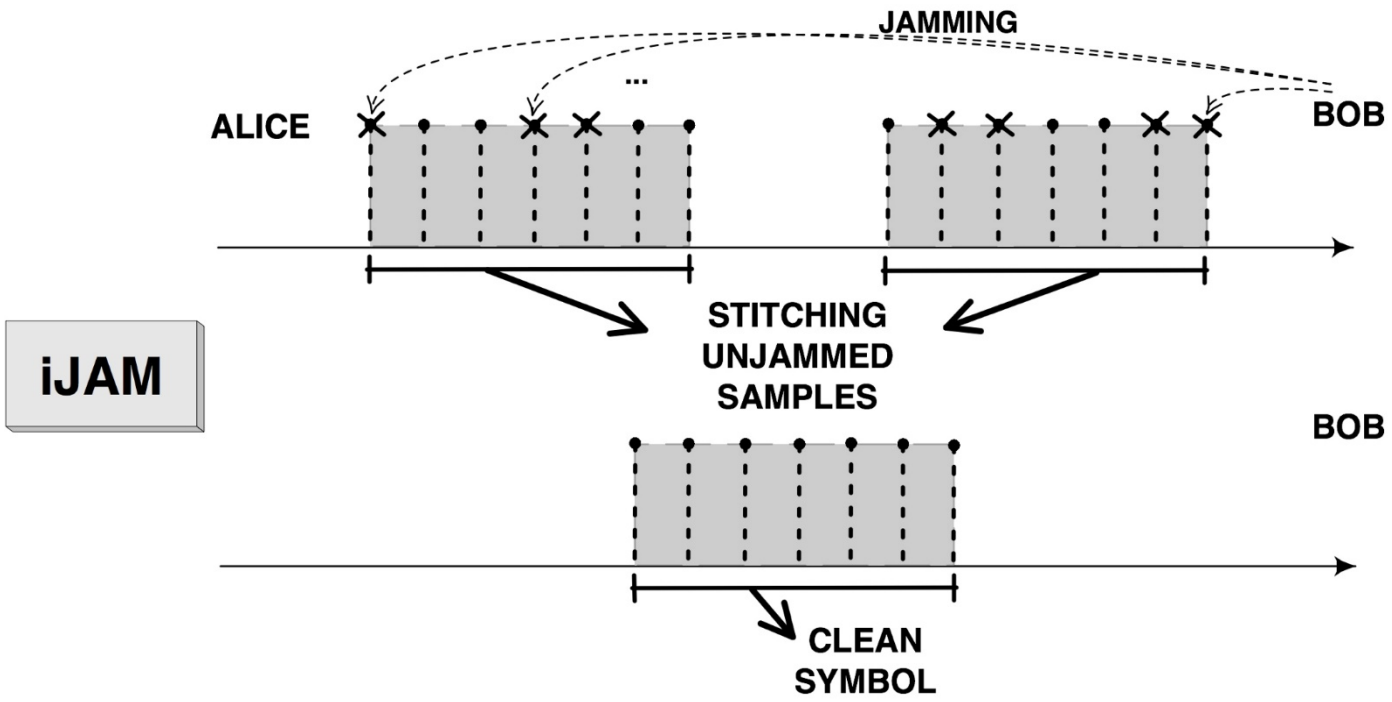
**W**ATERMARK **B**LIND **P**HYSICAL **L**AYER **SEC**URITY (**WBPLSec**)

## Assumptions

- ❑ No assumptions of limited time or power of the attackers;
- ❑ Based on the information leakage concept
  - Weak secrecy (Wyner)
- ❑ Exploit an advantage over the eavesdropper's channel to obtain secrecy capacity > 0

# iJAM

- ✓ In the past years, researchers exploited jamming for network security
- ✓ Recently, a channel independent protocol named **iJAM** (*) was introduced




Same symbol must be transmitted **twice** → data rate is half.

[*] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM,*, April 2011, pp. 1125–1133.

# Research Methods & Results

## *PHY Analysis (1/2)*

Background

Secrecy in communications:

- **cryptography** at upper layers of the OSI model;
- certain one-way functions are **hard to invert**

**Physical-layer security:**

- ✓ Security tech. **embedded** at physical-layer.
- ✓ **Low-power solution**
  - Less computations
- ✓ Implemented exploiting **channel imperfections**.

New transceiver architecture to ensure secure communication combining **watermarking** with **jamming** receiver.

Secrecy at physical-layer from **information theoretic view**:

- Non-degraded wiretap channel;
- Outage probability of $C_S$ as metric.

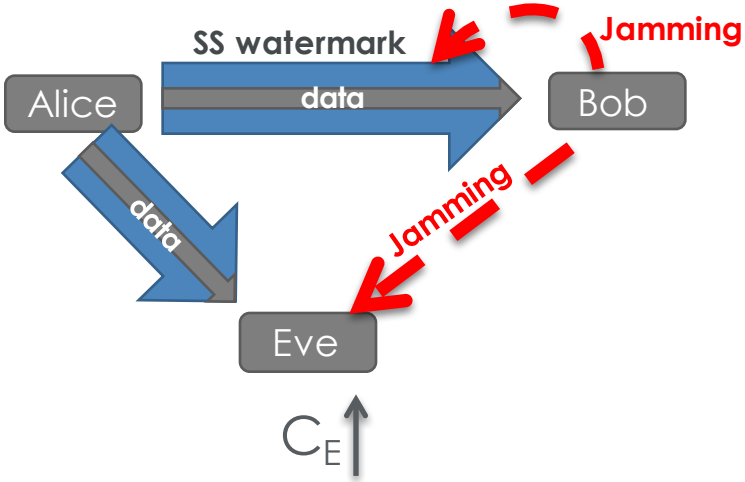
} Alice, Bob and Eve

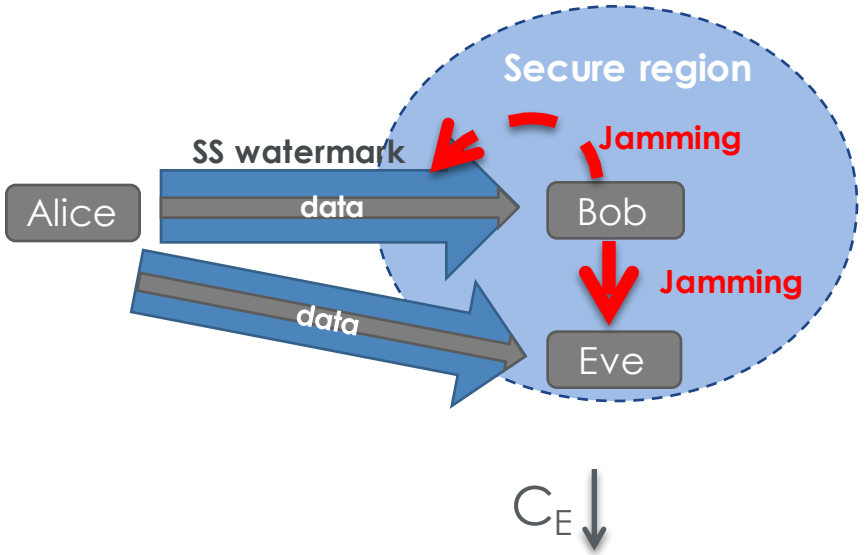
# Research Methods & Results

## *PHY Analysis (2/2) . . .*

**W**atermarked **B**lind **P**hysical **L**ayer **S**ecurity

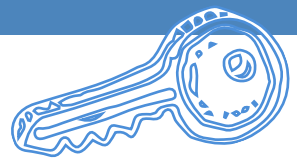
Secure Communication: $C_S = (C_M - C_E) > R_S$




- ✓ WBPLSec send information through two paths
  - SS watermarking extraction gives an advantage over Eve;
  - $C_E$ varies with the distance;
- ✓ Full rate protocol.

# WBPLSec Algorithm



**WBPLSec**
Procedure Physical Layer Security

**SS Watermarking (ALICE):**
A message is first modulated with SS and then embedded into the host signal.

**Jamming Receiver (BOB):**
The receiver jams M samples for each symbol transmitted by Alice.

**Watermark Extraction (BOB):**
The receiver extracts the watermark, i.e. $N_W$ samples with $N_W$>M.

**Symbol Rebuild (BOB):**
Knowing which samples are jammed the receiver, i.e. Bob, is able to rebuild a clean symbol using information contained into the watermark.

**End**

## Data Decomposition Policy

WBPLSec transmits the information through two independent paths:

- The information is sent via a narrowband signal and through the SS watermarked signal.
- The narrowband signal is partially jammed by Bob, but the SS watermark is utilized to re-compose the entire symbol.

# WBPLSec SYSTEM MODEL

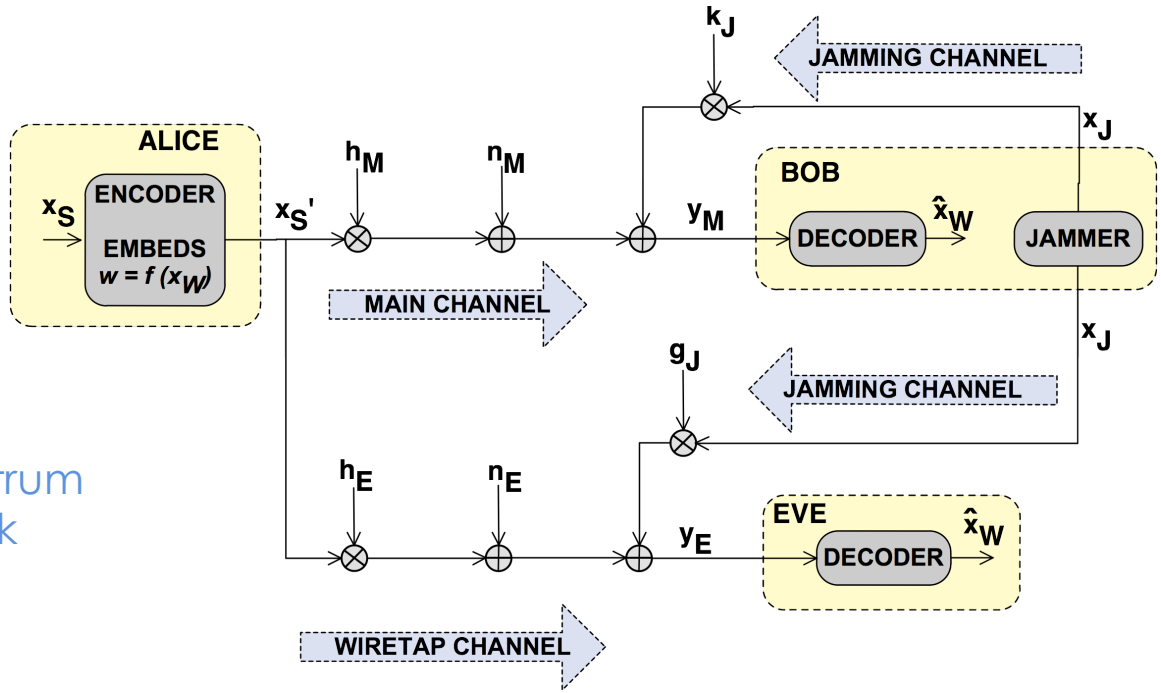
## NON-DEGRADED WIRETAP CHANNEL MODEL WITH JAMMING RECEIVER

WATERMARKING
Cox framework (*)

$$x'_S(i) = x_S(i) + \mu w(i)$$

Spread-Spectrum Watermark

Narrowband

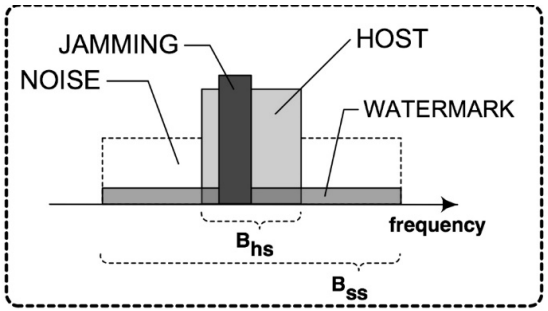



$$y_M(i) = h_M(i)x'_S(i) + k_J(i)x_J(i) + n_M(i)$$

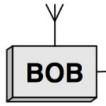
$$y_E(i) = h_E(i)x'_S(i) + g_J(i)x_J(i) + n_E(i)$$

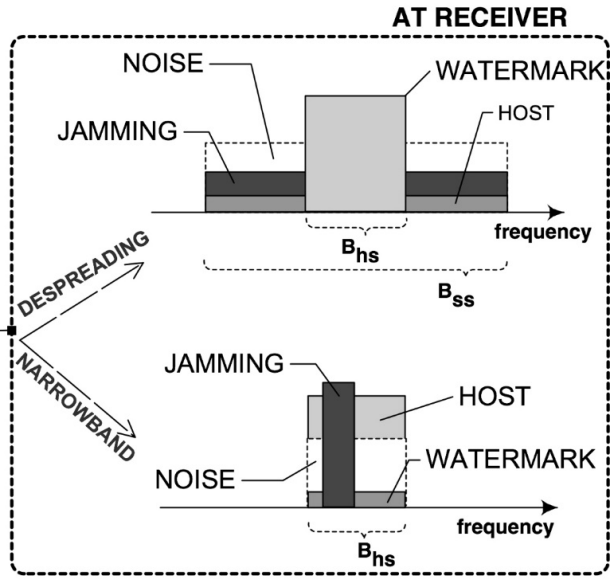

[*] I. J. Cox, M. Miller, and A. McKellips, "Watermarking as communications with side information," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1127–1141, Jul 1999.

# WBPLSec: how it works

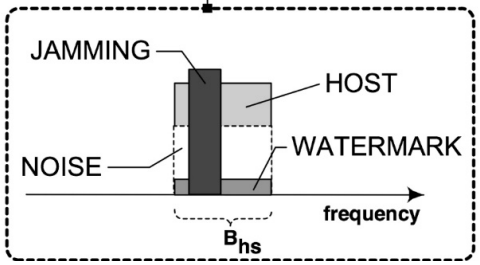











- ✓ Watermark extraction gives an advantage over Eve
- ✓ Data rate is full

$$\gamma_M = \frac{\frac{|h_M|^2 E'_S}{d_{tr}^{2b}}}{N'_0 + |k_J|^2 E_J} = \frac{\alpha\gamma'_{tr}}{1+\tilde{\alpha}\gamma'_{jr}}$$

$$E'_S = E_S + \mu^2 E_W$$

$$\gamma_E = \frac{\frac{|h_E|^2 E_S}{d_{te}^{2b}}}{N'_0 + \frac{|g_J|^2 E_J}{d_{je}^{2b}}} = \frac{\beta\gamma_{te}}{1+\tilde{\beta}\gamma_{je}}$$

- ✧ Secrecy capacity in **case of Gaussian wiretap channel** is bonded to the SNRs of the legitimate and eavesdropper links:

$$C_s = \max\{C_M - C_E, 0\},$$

$$C_M = \frac{1}{2}\log_2(1+\gamma_M)$$

$$C_E = \frac{1}{2}\log_2(1+\gamma_E)$$

# Outage Probability of Secrecy Capacity

**Outage Probability** was defined by Bloch (*)

$$P_{out} = P[C_s < R_s] = P\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < R_s\right] = P\left[\alpha < p(1+\tilde{\alpha}\gamma_{jr}) + q\beta\left(\frac{1+\tilde{\alpha}\gamma_{jr}}{1+\tilde{\beta}\gamma_{je}}\right)\right]$$

In the case of **WBPLSec** follow simple algebra $P_{out}$ can be expressed as follow

$$P_{out} = 1 - \int_0^\infty\!\!\int\!\!\int e^{-p(1+\tilde{\alpha}\gamma_{jr})-q\beta\left(\frac{1+\tilde{\alpha}\gamma_{jr}}{1+\tilde{\beta}\gamma_{je}}\right)} \cdot e^{-\tilde{\alpha}} e^{-\beta} e^{-\tilde{\beta}} d\tilde{\alpha} d\beta d\tilde{\beta} =$$

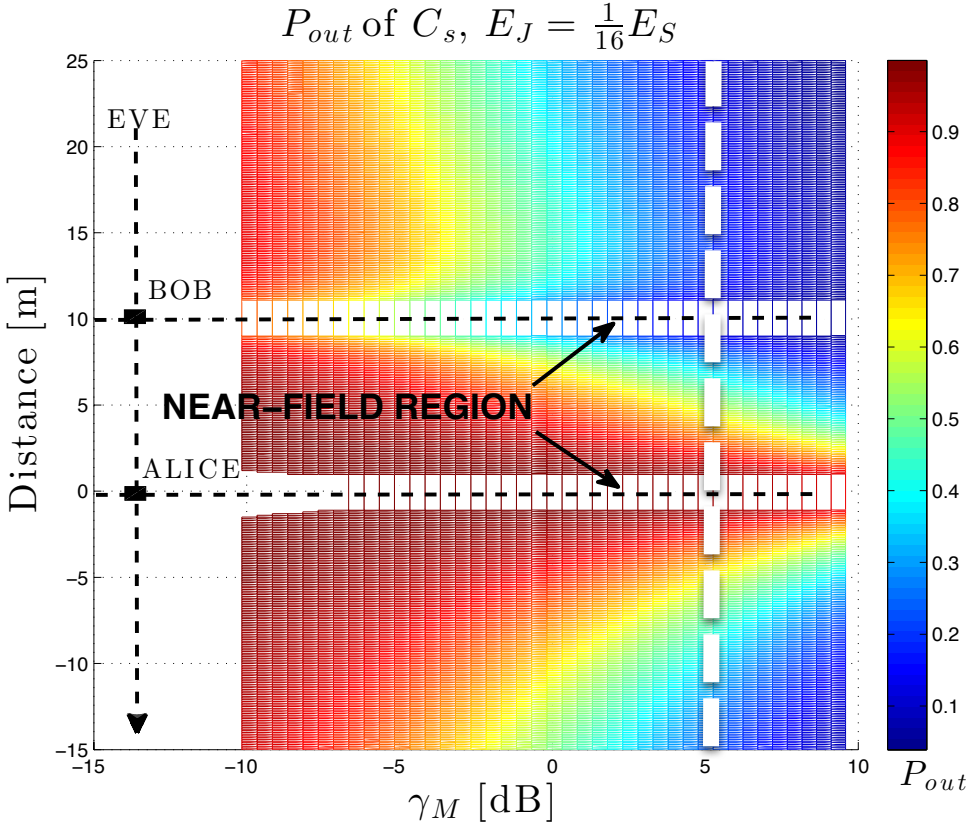
$$= 1 - \frac{1}{(\gamma_{je}\gamma_{jr}p + \gamma_{je} - \gamma_{jr}q)^2} \cdot e^{-p}\left(-q\Omega\left(\frac{q+1}{\gamma_{je}}\right)(\gamma_{je}(\gamma_{jr}p + \gamma_{jr} + 1) - \gamma_{jr}q) - \right.$$

$$\left. \Omega\left(\frac{(q+1)(\gamma_{jr}p+1)}{\gamma_{jr}q}\right)\left(\gamma_{je}\gamma_{jr}p - (\gamma_{je}+1)\gamma_{jr}q + \gamma_{je}\right) + \gamma_{je}(\gamma_{je}\gamma_{jr}p + \gamma_{je} - \gamma_{jr}q)\right)$$

[*] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

# Results

## SECURE REGION AROUND MEDICAL DEVICE, i.e. BOB




Outage probability of $C_s$ versus $\gamma_M$ for different Eve's positions along the line that connects Alice with Bob.

- ✓ Figure depicts a region around Bob, i.e. a medical device, in which the secure communication occurs.
- ✓ The size of this region depends on the acceptable Pout, e.g., when it is lower than 0.3.

*NOTE: EVE cannot be closer than 1 m to both Alice and Bob, because the near-field region limit at 1 m (*) around Alice and Bob was assumed.*


[*] A. Rabbachin, A. Conti, and M. Win, "Intentional Network Interference for Denial of Wireless Eavesdropping," in *2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)*, , Dec 2011, pp. 1–6.

# Discussion & Conclusions

✓ Physical layer security in **wireless health system** was considered because malicious attacks can compromise patients' safety.

**WBPLSec** protocol is developed against information disclosure attacks, such as eavesdropping.

**WBPLSec** attractive solution, compared with encryption, due to limited power and processing capability in WBAN. It is full rate.

The utilization of **WBPLSec** can create a secure region around the legitimate receiver, such as doctor's laptop or other medical devices.


**References:**

① Soderi S, Mucchi L, Hämäläinen M, Piva A & Iinatti J (2016) Watermark–basedsecure communications in safety critical scenarios. 10th International Symposium on Medical Information and Communication Technology (ISMICT'16), 21–23 March 2016.

② Soderi S, Mucchi L, Hämäläinen M, Piva A & Iinatti J (2016) Physical layer security based on spread–spectrum watermarking and jamming receiver. Journal paper under peer review.

UNIVERSITY OF OULU


# Thanks!

Questions?

soderi@ieee.org

# Watermark-based Secure Communications in Safety-Related Scenarios

**S. Soderi**‡, L. Mucchi*, M. Hämäläinen‡, A. Piva* and J. Iinatti‡

‡*Centre for Wireless Communications, University of Oulu, Oulu, Finland*

**Department of Information Engineering, University of Florence, Florence, Italy*

***SSIE 2016 July 3-9, 2016 – Brixen, Italy.***

CWC Oulu CENTRE FOR WIRELESS COMMUNICATIONS University of Oulu

# Backup

# Let's review some concepts

## WLAN

WLANs usually provide the needed connectivity in **public transportation systems**. Many of these systems require high level of safety

## REQs

These WLANs **require high level of safety**. The greater dependence on wireless technologies increases the complexity and exposes them to **security threats**.

## Safety vs Security

**Safety**: Avoids physical harm to humans and things.
**Security**: Applies defenses from malicious attacks.

## Assure & Evaluation

Processes that **assure** and **evaluate Security** are

- Orange Book (1960);
- CC as ISO/IEC15408 (1999);
- FIPS 140-2 (2001),

## Attacks

Security certificates and evaluation have significant **increment** after different terrorist or cyber-attacks occurred in this century

- Stuxnet (2010).
- Duqu(2011).

## New Tech

New technologies brought **prosperity** and **progress** for population, but in some cases these **create also new challenge in the field of security and privacy**. Actually, malwares can affect **critical national infrastructure.**