Physical-layer security: from theory to applications

Consiglio DINFO, 30/01/2020

Lorenzo Mucchi

UNIVERSITÀ DEGLI STUDI FIRENZE

Physical-layer security

- What it is
- Why now
- Practical limits
- New approaches
- Our contribution

Voltone del Podestà, Bologna

"All you need to make a movie is a girl and a gun"

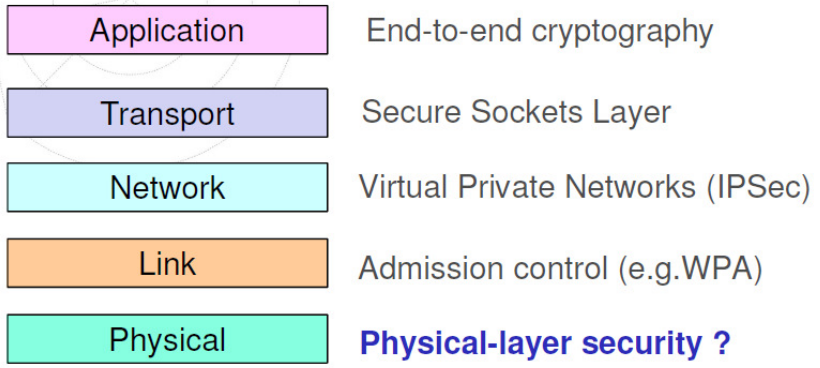
Jean-Luc Godard

"All you need to make info secrecy is a log and a lim"

Sergio Verdù

PhySec: What is it?

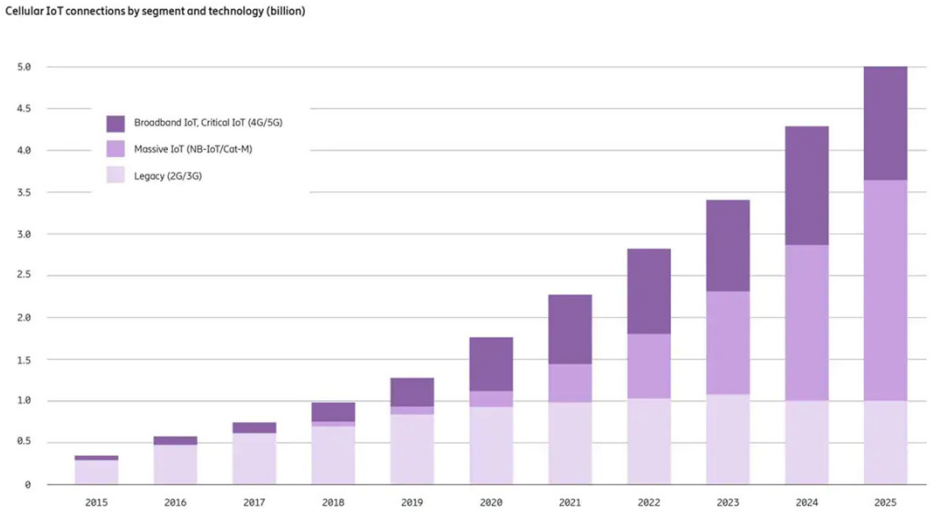
- In traditional systems, reliability is guaranteed by channel coding at the physical layer, while security is ensured by encryption protocols at the upper layers
- Physical layer security aims at exploiting the **randomness** inherent in **noisy** channels to provide an **additional level of protection** at the physical layer
- Nowadays, many results from information theory, signal processing, and cryptography suggest that there is much security to be gained by accounting for the imperfections of the physical layer when designing secure systems



- **Crypto VS PhySec**
  - Crypto: I demodulate, but I don't understand the message
  - PhySec: I don't even demodulate
  - PhySec does not rely on assumtpion of limited computational power of the attacker
  - PhySec: Security can be measured

Why now?

- Computing devices shrinking and becoming more capable
- Networks becoming ubiquitous
- Users becoming more mobile
- Content becoming active
- Context-aware applications and services
- New terminal technologies
- Flexible spectrum management
- Dynamic reconfiguration

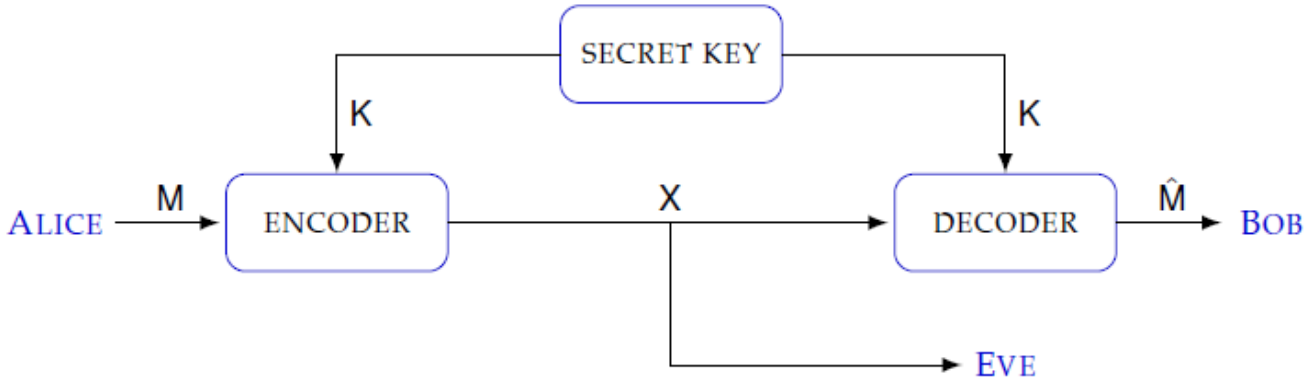


History of PhySec

- Shannon (‘50)
  - Perfect secrecy
  - Noise-free channels (worst case)
- Wyner (‘70)
  - Noise can be useful
  - Wiretap channel
  - Secrecy capacity

- Today
  - Interference can be useful
  - From link to network secrecy
  - How to (practically) implement a PhySec system?

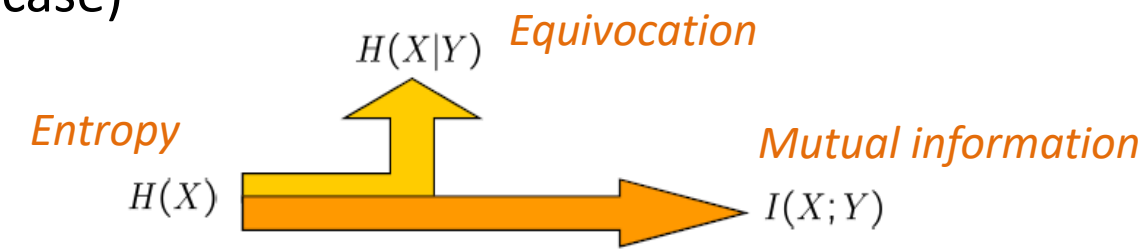
Shannon



- M = message from Alice to Bob
- K = secret key used to encrypt M
  - Common secret between A and B
- X = codeword
- Noise-free channels (worst-case)

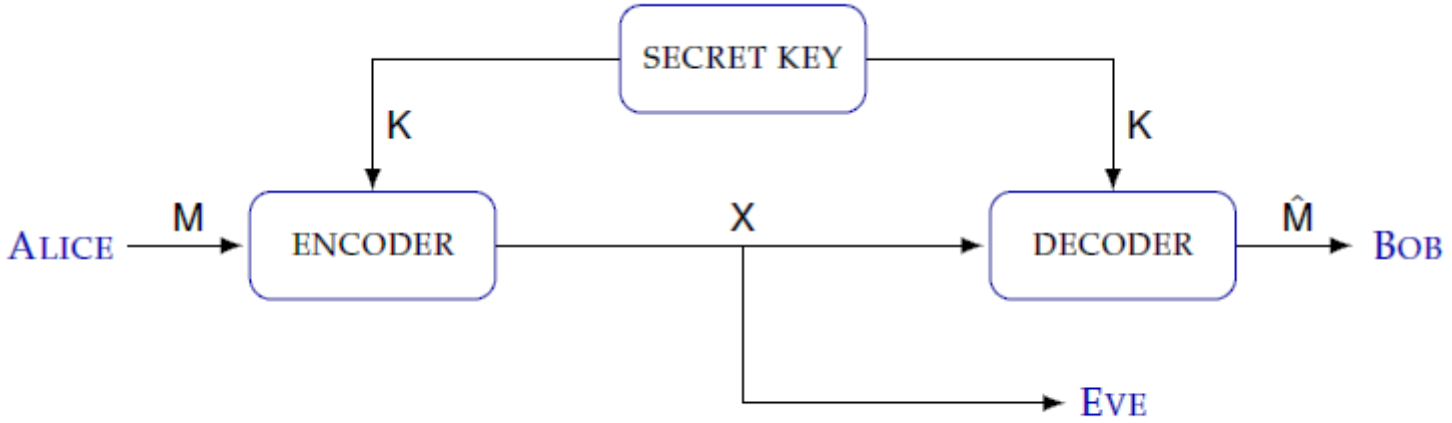
Perfect secrecy: $\mathbb{H}(M|X) = \mathbb{H}(M)$

Necessary condition: $\mathbb{H}(K) \geqslant \mathbb{H}(M)$



$I(X;Y) = H(X) - H(X|Y)$ bit/symbol

Crypto-lemma



If *K* is uniform, then **X = M** $\oplus$ **K** is independent of *M* and uniform

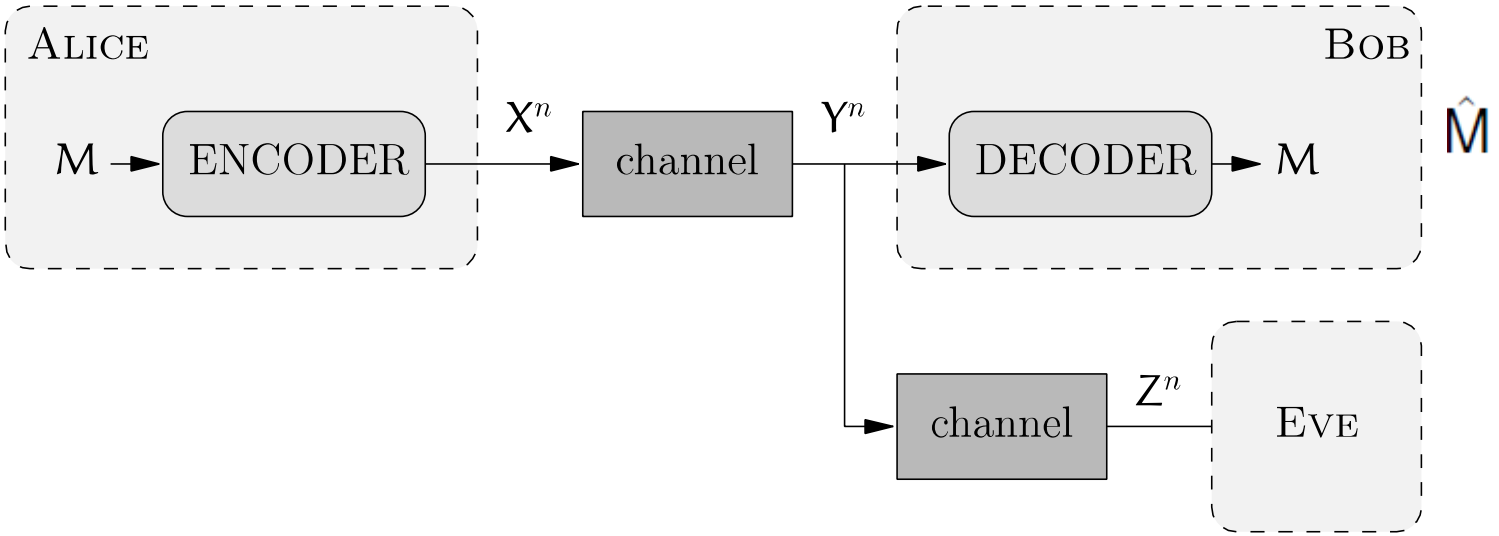
- As many key bits as message bits
- Perfectly uniform key
- Key distribution problem

One-time pad

Bob can recover the message by subtracting (Modulo-|M|) the key K

Eve has mutual information I(M;X) = 0

Wyner



- Channels are noisy
- No a priori common secret

$$(1/n)\mathbb{H}(M|Z^n) \xrightarrow{n\to\infty} (1/n)\mathbb{H}(M)$$

- There exist channel codes asymptotically guaranteeing both an arbitrarily small error probability at the intended receiver and secrecy.

$$P_e(C_n) = \mathbb{P}\{\hat{M} \neq M\} = \varepsilon \qquad \lim_{n\to\infty} I(M, Z^n) = 0$$

- The maximum achiavable transmission rate is called *secrecy capacity*.
- If the observation of the eavesdropper Z^n is noisier than the one of the legitimate receiver Y^n a strictly positive secrecy capacity is achievable.

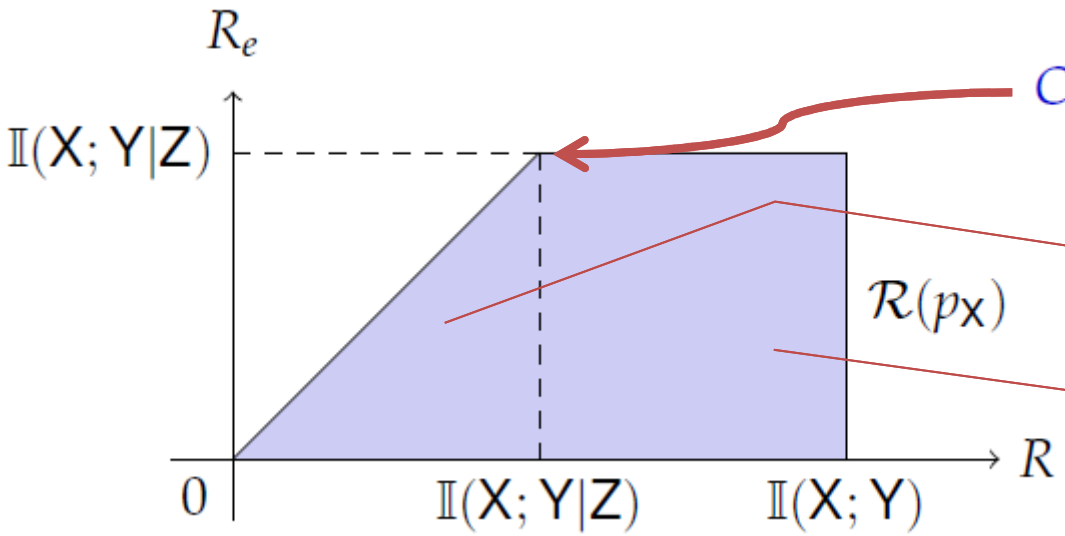
Rate-equivocation region

Theorem (Wyner)

The weak rate-equivocation region of the wiretap channel is given by

$$\mathcal{R} = \bigcup_{p_X} \mathcal{R}(p_X), \quad \textit{where}$$

$$\mathcal{R}(p_X) = \{(R, R_e) \;\; | \;\; 0 \le R_e \le R \le \mathbb{I}(X;Y), \quad 0 \le R_e \le \mathbb{I}(X;Y|Z)\}$$



$C_s^{(s)} = \sup\{R \mid (R,R) \in \mathcal{R}^{(s)}\}$

Full secrecy rate

No secrecy guaranteed for remaining fraction of rate

Secrecy capacity

Corollary

$$C_s = \max_{p_X} \mathbb{I}(X;Y|Z) = \max_{p_X} \left(\mathbb{I}(X;Y) - \mathbb{I}(X;Z)\right)$$

Information rate conveyed to legitimate user

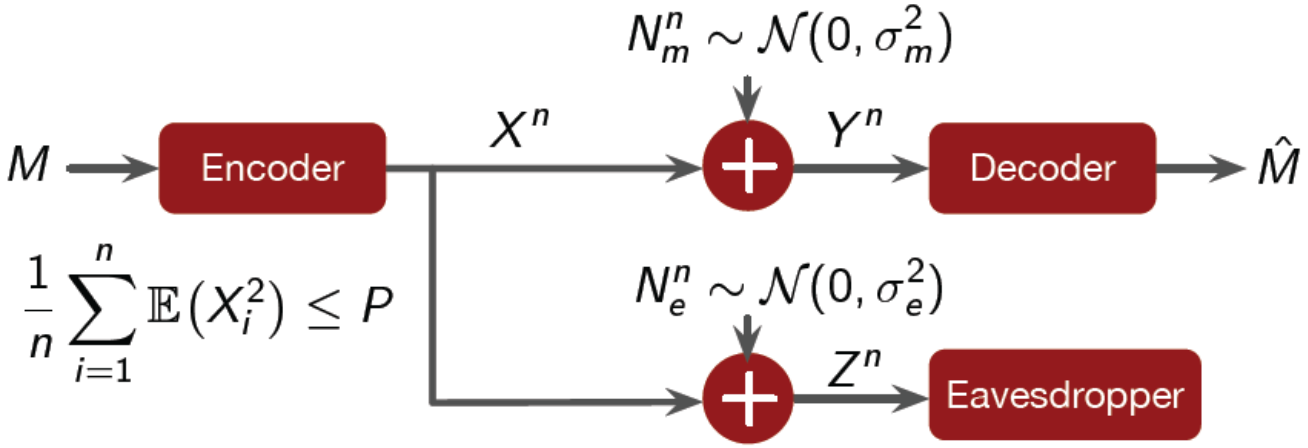
Information rate leaked to the eavesdropper

$$\Rightarrow C_s \geq \max_{p_X} \mathbb{I}(X;Y) - \max_{p_X} \mathbb{I}(X;Z) = C_b - C_e$$

If Z=Y (Eve obtains the same observation of Bob) then I(X;Y|Z)=0 and $C_s = 0$

→ Information-theoretic security cannot be achieved over noiseless channel without secret keys (Shannon)

Secrecy Capacity of Gaussian Channels

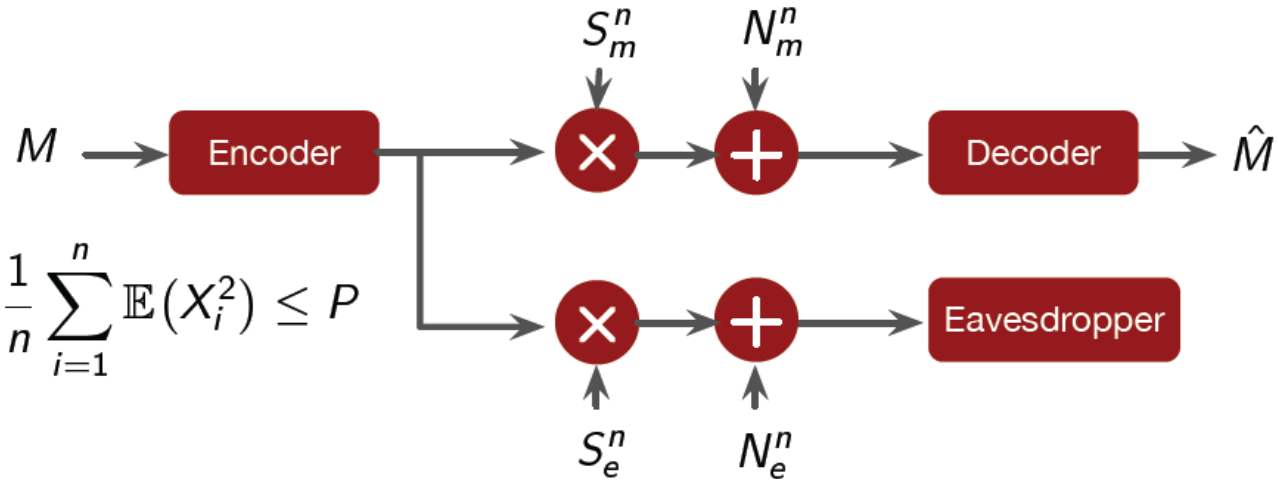


$$C_s^{\mathrm{WT}} = \left\{ \frac{1}{2} \log\left(1 + \frac{P}{\sigma_m^2}\right) - \frac{1}{2} \log\left(1 + \frac{P}{\sigma_e^2}\right) \right\}^+$$

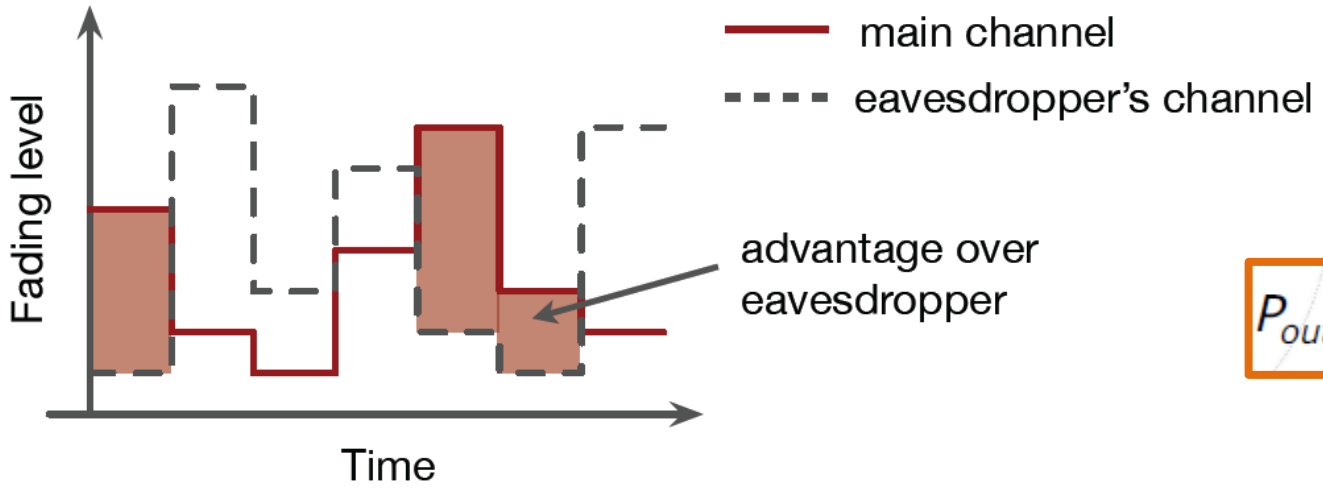
$$\lim_{P \to \infty} C_s = \left(\frac{1}{2} \log \frac{\sigma_e^2}{\sigma_b^2} \right)^+$$

- Unlike the capacity, the secrecy capacity is not unbounded when the Power goes to infinity
- Secure communication is possible only if Bob has a better SNR than Eve.

Fading can be exploited too



- Fading can be exploited in opportunistic way
- Illustration: time variations of fading gains

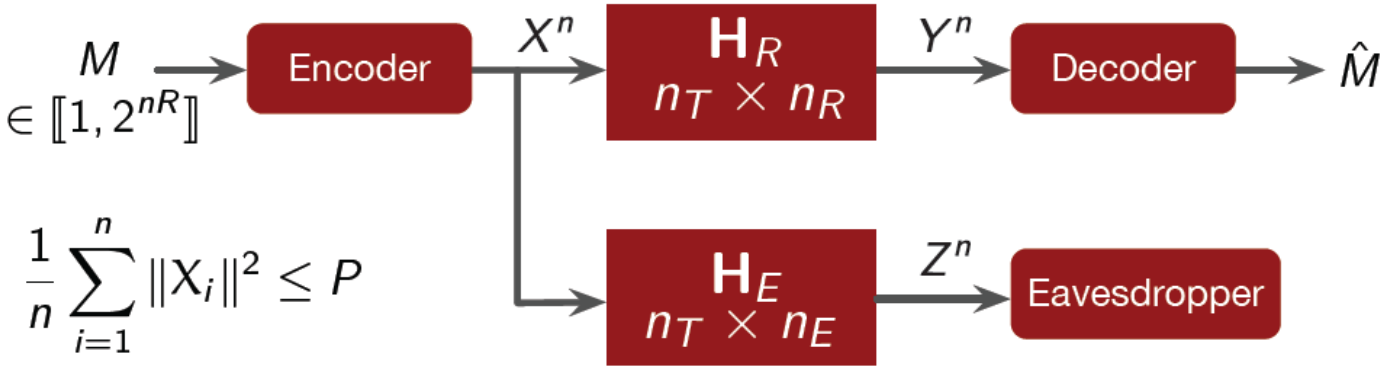


$$P_{out}(R_s) = \Pr(C_s < R_s)$$

Outage probability

- Eavesdropper could have better SNR on average

MIMO



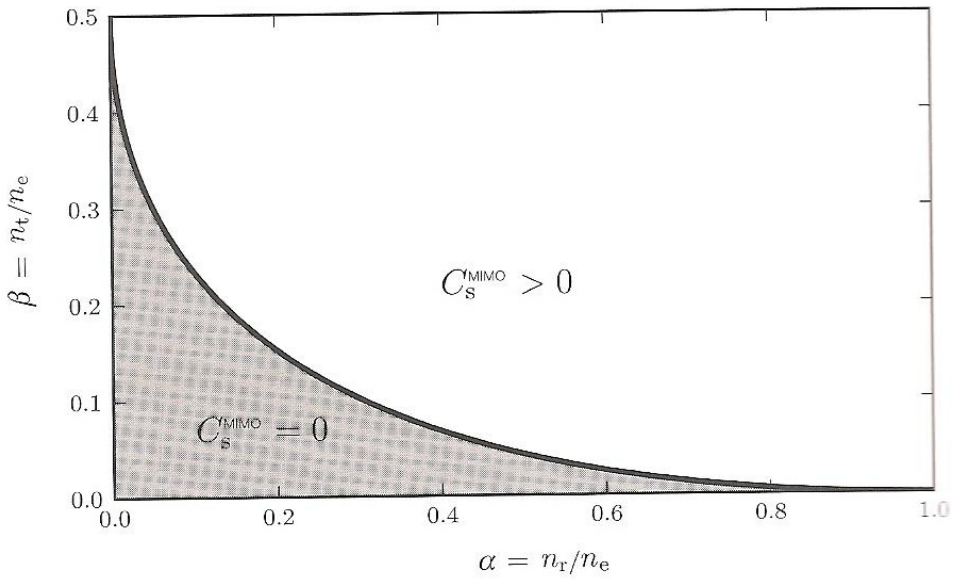
$$C_s = \max_{\mathbf{Q}_X} \left(\log \left| \mathbf{I}_{n_r} + \tfrac{1}{\sigma_b^2} \mathbf{H}_b \mathbf{Q}_X \mathbf{H}_b^H \right| - \log \left| \mathbf{I}_{n_e} + \tfrac{1}{\sigma_e^2} \mathbf{H}_e \mathbf{Q}_X \mathbf{H}_e^H \right| \right),$$

over all the covariance matrices $\mathbf{Q}_X$ *which satisfy the power constraint* $\mathrm{Tr}(\mathbf{Q}_X) \leq P$.

$\sigma_b = \sigma_e = 1$

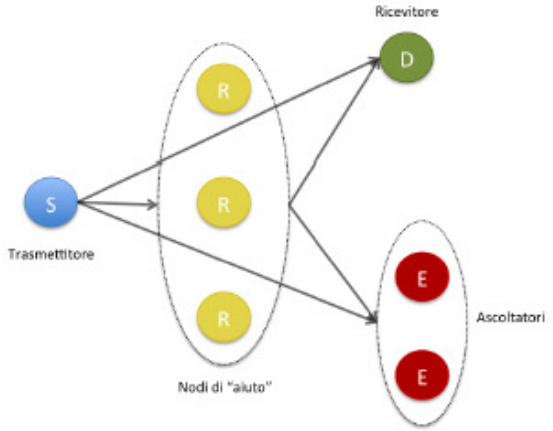
$\mathbf{H}_R$ and $\mathbf{H}_E$ are iid C*N*(0,1)

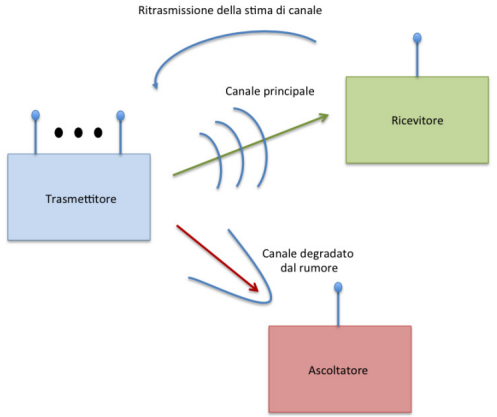
- The secrecy capacity is strictly positive only if Alice can beamform the signals in a direction for which Eve obtains a lower SNR than Bob
- Secrecy capacity is positive as long as Eve does not deploy too many antennas compared to Alice and Bob
  - Single receiving antenna for Bob ($\alpha = 0$):
    Cs > 0 if Eve has fewer than twice as many antennas as Alice
  - Single transmit antenna for Alice ($\beta = 0$):
    Cs > 0 if Eve has fewer antennas than Bob

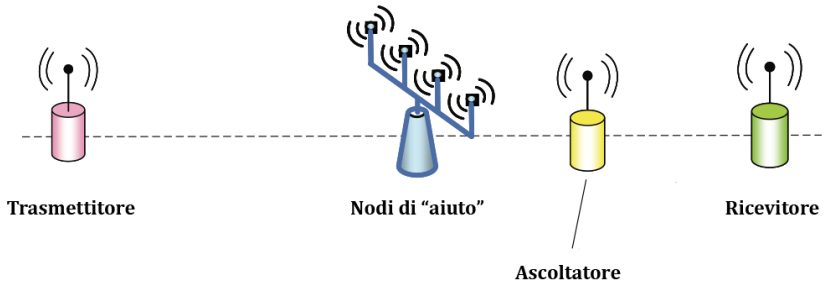


Practical limits of PhySec

- Classical metrics (C_{sec}, P_{out}) designed to quantify security of a single link
- My channel must be better than Eve's one
  - Every method that makes Eve's channel worse can lead to Cs > 0
    - Cooperative relay
    - Artificial noise injection
    - Friendly jamming
    - Game theory
    - …
- (some) Knowledge about Eve is needed (!)
  - Eve is there
  - Eve's channel is known or can be estimated

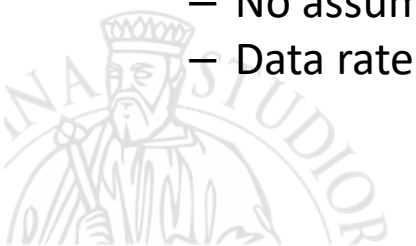






Our contribution

- **Network intrinsic secrecy**
  - Exploit interference
  - New metric for measuring how much secure is a (large) network
  - Only stochastic knowledge of malicious nodes positions
  - Different strategies for optimization (secrecy outage protocol)
- **Secrecy pressure**
  - New metric for measuring how much secure is an arbitrary environment
  - No need to know malicious nodes positions
  - Different strategies for optimization
- **Watermark-based security**
  - Exploit watermark to implement an advantage over Eve
  - No need to know Eve's position
  - Watermark is a common secret
- **Noise-loop modulation**
  - Eavesdropping impossible
  - No assumptions on Eve
  - Data rate is low



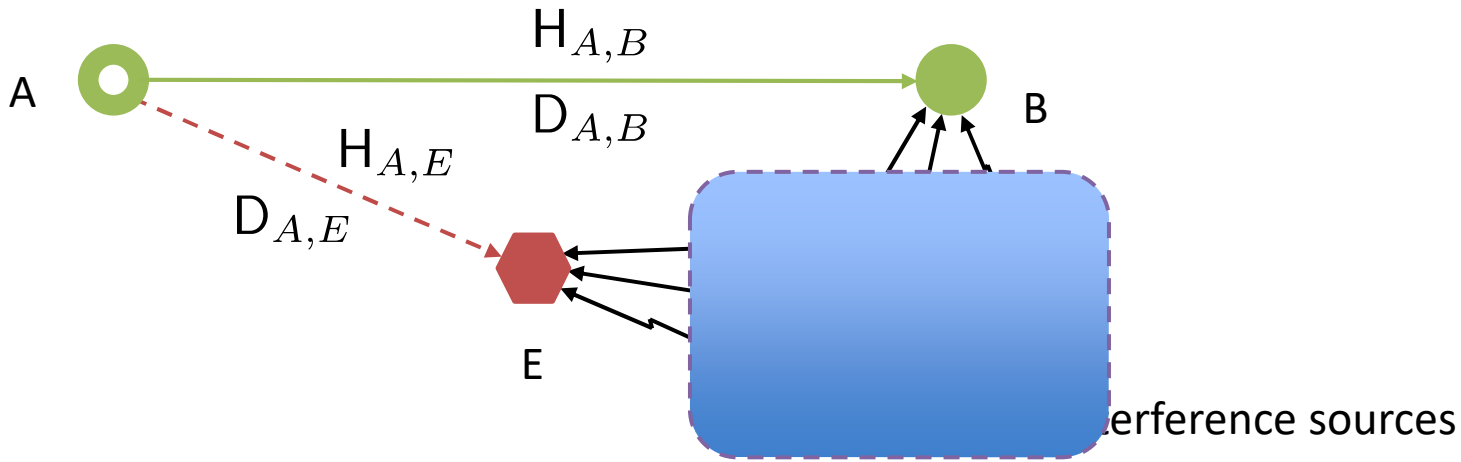
Network intrinsic secrecy

- Interference normally undermines communication reliability
- Interference can help communication confidentiality

Network intrinsic secrecy: information confidentiality achieved by network coordination that exploits the physical characteristics of the communication, e.g.,the interference.

- Secrecy in large-network scenario
- Spatial models for wireless networks
- Network secrecy metric
- How to operate a confidential communication in a large-network

Interference is good



Signal-to-interference-plus-noise ratio: $Z_{u,v} = \frac{P_0 H_{u,v}}{D_{u,v}^{2b}(I_v + N_0)}$ dB

Aggregate interference: $I_v = \sum_{q \in \mathcal{I}_v} \frac{P_0 H_{q,v}}{D_{q,v}^{2b}}$ dB

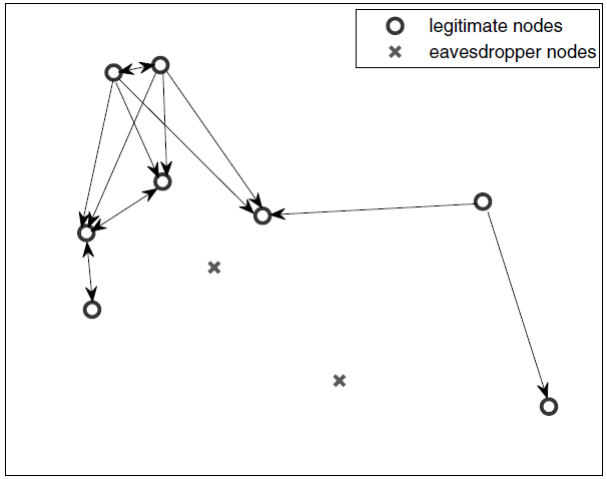
Interferers' set: $\mathcal{I}_v$

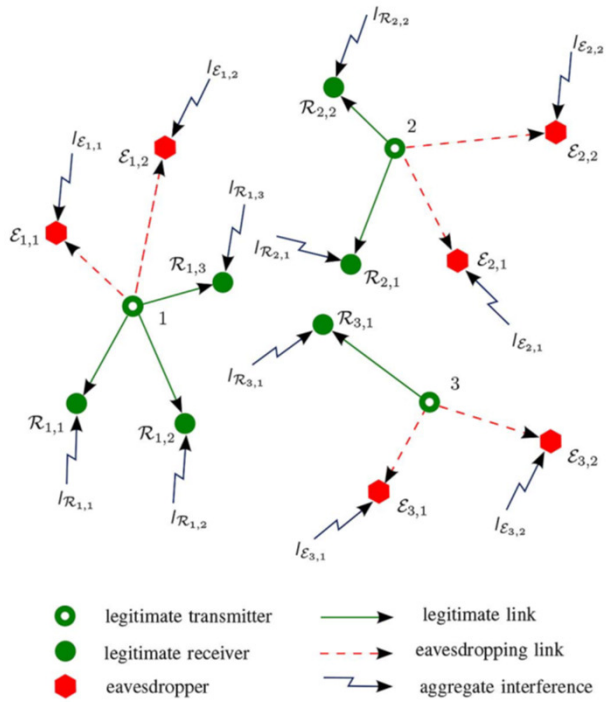
Link capacity: $C_{u,v} = c(Z_{u,v}) = \log_2(1 + Z_{u,v})$ bit/s/Hz

Secrecy capacity: $C_{sec} = C_{A,B} - C_{A,E}$ bit/s/Hz

Stochastic geometry approach

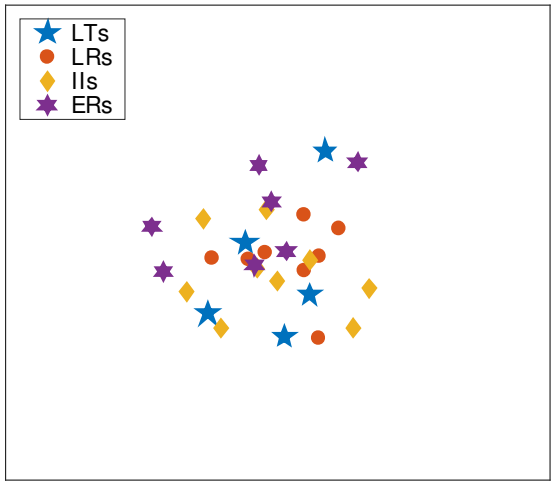
- Legitimate users and the eavesdroppers are **randomly located** over a large geographical area according to some probability distributions.
- The **secrecy graph**, as a graph-theoretic approach, is introduced to study the connectivity properties among the legitimate users of the network.
  - It characterizes the existence of connection with perfect secrecy between any two legitimate users.
- It considers concurrent transmissions between all the legitimate links and gives a mathematically tractable measure on the **achievable network throughput with a given secrecy** requirement.
- The simplest yet most important model in Stochastic Geometry is the **homogenous Poisson point process** (PPP).
  - A homogenous PPP in 2-dimensional space roughly means that all nodes are randomly located inside the network according to a uniform distribution.
  - It is completely characterized by the constant intensity parameter λ.
    - Specifically, the value of λ gives the average number of nodes located inside a unit volume in the n-dimensional space.





Stochastic geometry

- The performance of wireless networks strongly depend on node positions (friends and enemies)
- Node position are subject to uncertainty and thus need to be modeled as a **spatial stochastic process** (point process)
- The secrecy performance of the network varies with the receiver selection policy:
  - nearest neighbor,
  - max SINR or
  - random



$$R = \mathbb{E}_0\{\mathsf{R}_{0,\bar{k},\breve{\imath}}\} = \mathbb{E}_{\mathsf{Z}_{0,\bar{k}}}\left\{\mathbb{E}_{\mathsf{Z}_{0,\breve{\imath}}}\left\{\left[c\left(\mathsf{Z}_{0,\bar{k}}\right) - c\left(\mathsf{Z}_{0,\breve{\imath}}\right)\right]^+\right\}\right\}$$

$$= \int_0^\infty c(y) F_{\mathsf{Z}_{0,\breve{\imath}}}(y) f_{\mathsf{Z}_{0,\bar{k}}}(y) dy \; - \int_0^\infty \int_0^y c(x) f_{\mathsf{Z}_{0,\breve{\imath}}}(x) f_{\mathsf{Z}_{0,\bar{k}}}(y) dx dy$$

$$R_s \leq R_{j,\bar{k},\breve{\imath}} = \left[c(Z_{j,\bar{k}}) - c(Z_{j,\breve{\imath}})\right]^+$$

Secrecy Outage Protocol (SOP)

- Consider a target secret information rate R_s
- A transmitter send such a rate only if the SINR is above a threshold $\mu^\star$ (secrecy protection ratio)
- The probability of such an event to happen is

  Probability to transmit confidential information: $P_{it}(\mu^\star) = \mathbb{P}\{\mathsf{Z}_{j,\bar{k}} \geq \mu^\star\}$

- The threshold $\mu^\star$ is chosen such that the secrecy outage probability P_{so} is below a tolerable value $P_{so}^\star$, i.e.

$$\mu^\star = \arg\max_{\mu \in \mathcal{M}} P_{\mathrm{it}}(\mu) \quad \text{with} \quad \mathcal{M} = \{\mu : P_{so}(\mu) \leq P_{so}^\star\}$$

$$P_{so}(\mu) = \mathbb{P}\{c(\mathsf{Z}_{0,\check{\imath}}) > c(\mathsf{Z}_{0,\bar{k}}) - R_{\mathrm{s}} | \mathsf{Z}_{0,\bar{k}} > \mu\} = \cdots = \frac{1}{1 - F_{\mathsf{Z}_{0,\bar{k}}}(\mu)}$$

$$\times \left[F_{\mathsf{Z}_{0,\bar{k}}}(\mu) F_{\mathsf{Z}_{0,\check{\imath}}}\left(\frac{\mu+1}{2^{R_{\mathrm{s}}}} - 1\right) - F_{\mathsf{Z}_{0,\bar{k}}}(\mu) + \int_{\frac{\mu+1}{2^{R_{\mathrm{s}}}-1}}^{\infty} F_{\mathsf{Z}_{0,\bar{k}}}(2^{R_{\mathrm{s}}}(1+y) - 1) f_{\mathsf{Z}_{0,\check{\imath}}}(y) dy \right]$$

Network secrecy design

Maximum secrecy rate

- Need the global knowledge of the legitimate and eavesdropping network
- Always transmit at a confidential information rate that depends on the instantaneous network condition
- The metrics based on this technique are representative of the network secrecy performance but the communication operation is not practical.

Maximum tolerable SOP

- Need a global knowledge of the legitimate network only, and a stochastic knowledge of the eavesdropping network.
- Transmit confidential information at a fixed rate only if the legitimate channel instantaneous condition is sufficiently favorable.
- It provides a practical and systematic network operation.

- We designed a practical protocol to operate confidential communication assuming only stochastic information about eavesdroppers.
- We showed that is possible to design interfering engineering strategies based on legitimate nodes coordination to impair the eavesdropping channels without damaging the legitimate ones and, hence, maximize the secrecy performance.

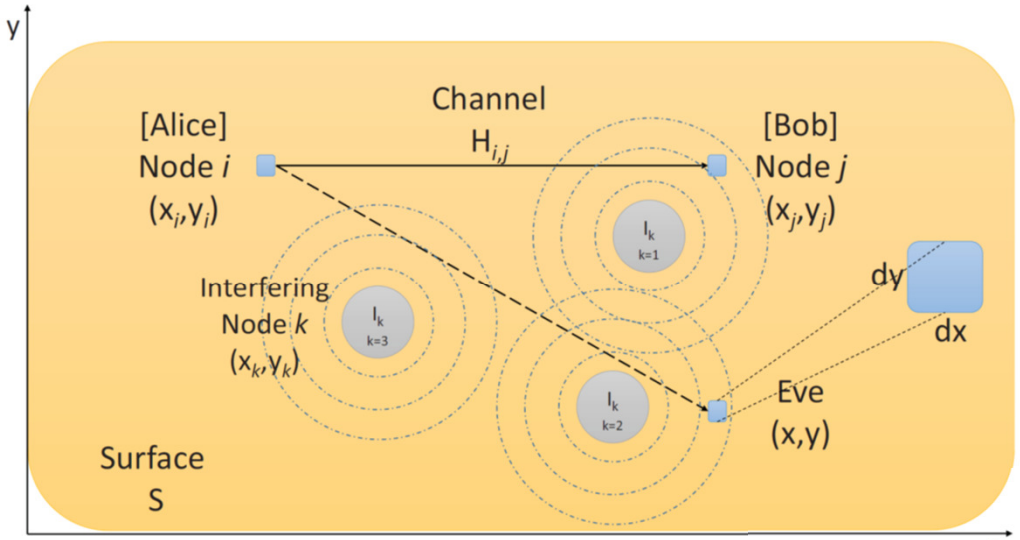
A new metric: the secrecy pressure

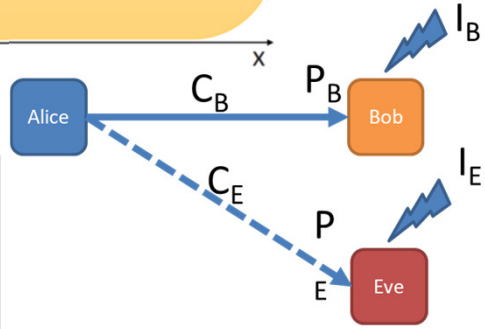
- Secrecy capacity

$$C_B = \frac{1}{2}\log\left(1+\frac{P_B}{N_0+\mathbf{I}_B}\right)$$

$$C_E(x,y) = \frac{1}{2}\log\left(1+\frac{P_E}{N_0+\mathbf{I}_E}\right)$$

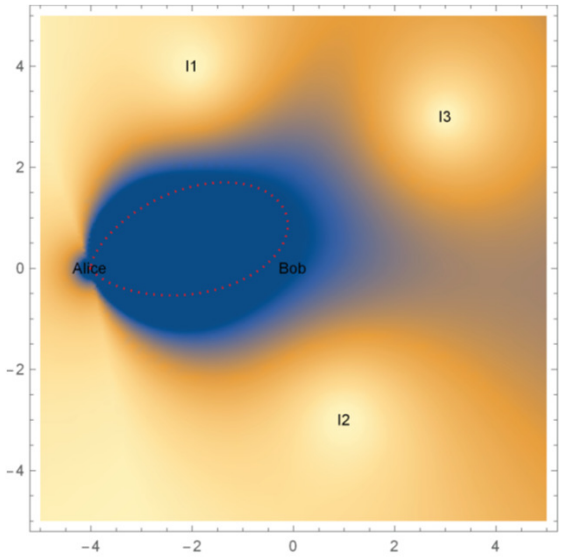
$$\boxed{C_{sec} \geq C_B - C_E}$$



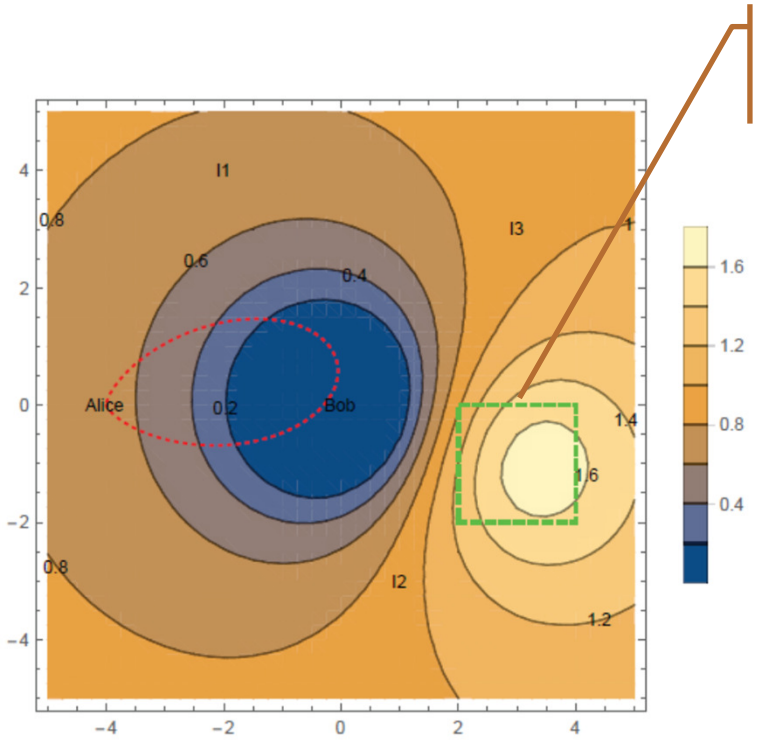


- Secrecy Pressure

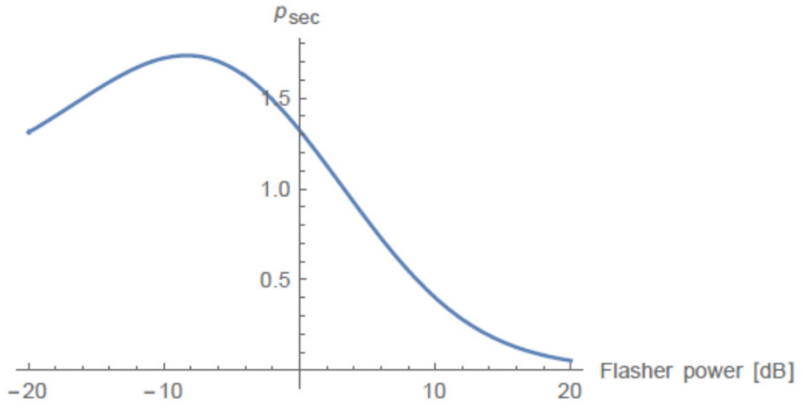
$$\boxed{p_{sec} = \frac{1}{A_S}\iint_S C_{sec}(x,y)dxdy}$$



Optimization: position and power of additional interferer



Secrecy map over the surface S when the optimization problem is solved respect to the **position** of the additional interfering node (flasher).

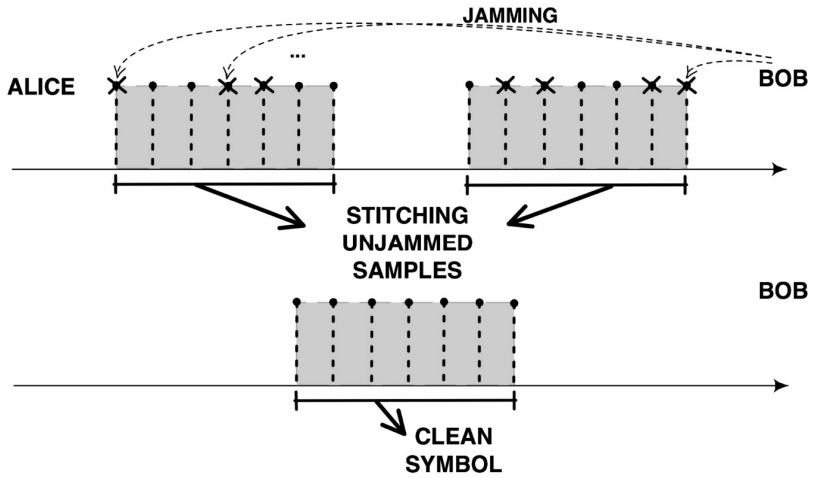


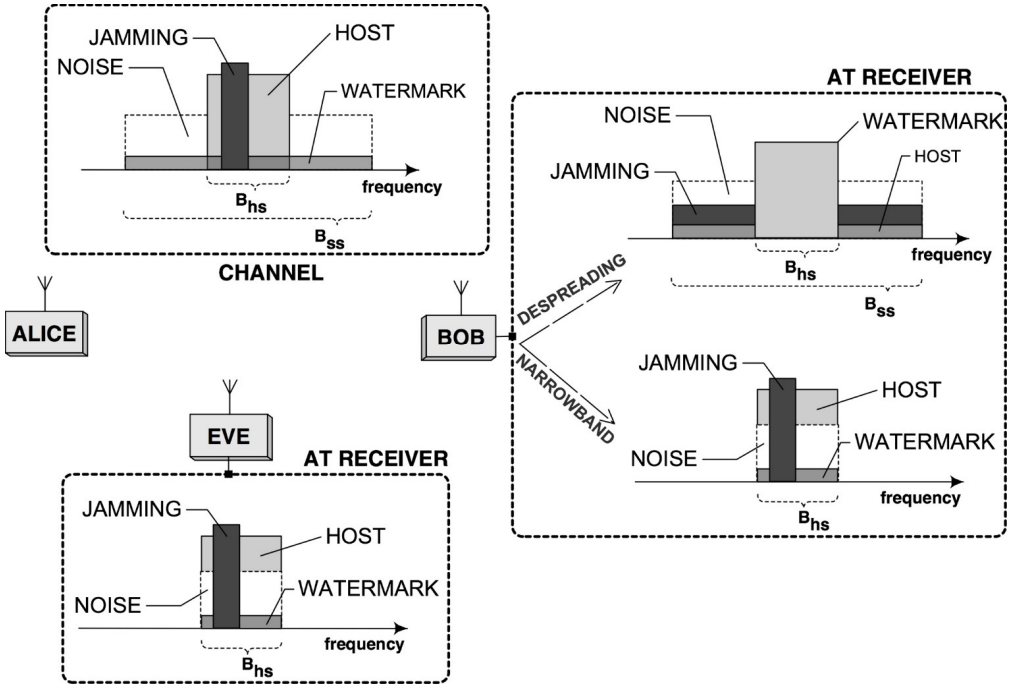
Secrecy map over the surface S when the optimization problem is solved respect to the **power** of the additional interfering node (flasher).

Watermark-based security

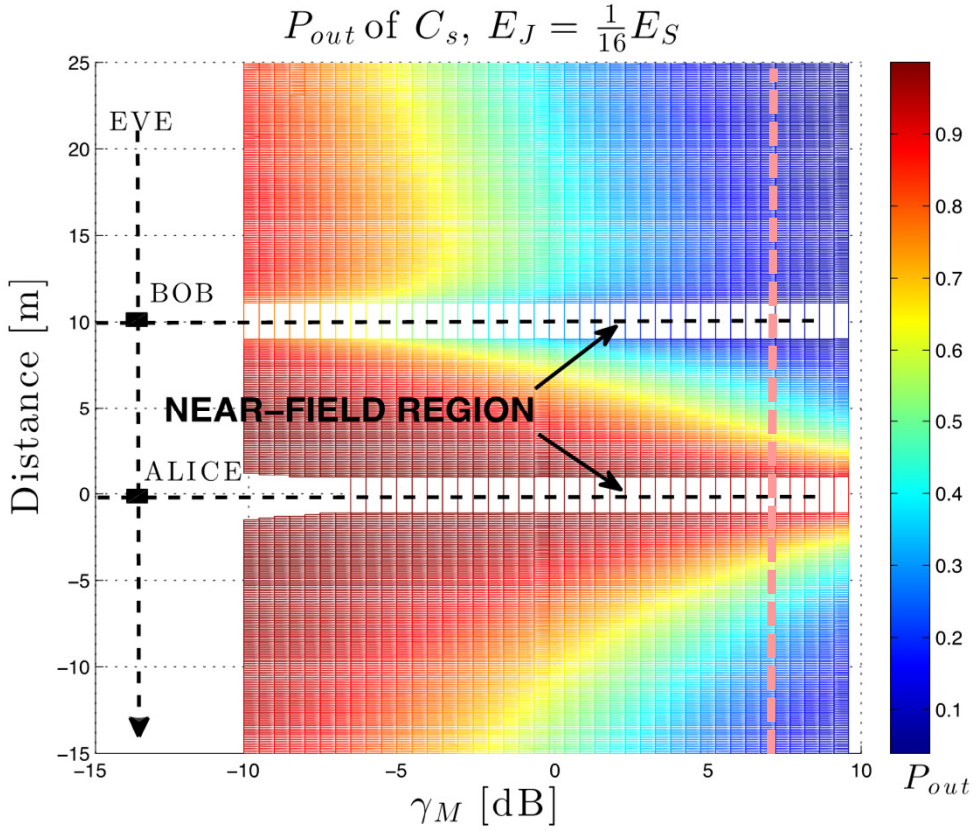
- Spread-spectrum watermark + narrow-band host signal
- Self-jamming at the receiver

- Watermark is used to correct jammed symbols at legitimate receiver
  - Advantage on Eve
- Full secrecy rate
- Watermark is a shared secret





Watermark-based security



Outage probability of C_s versus γ_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.

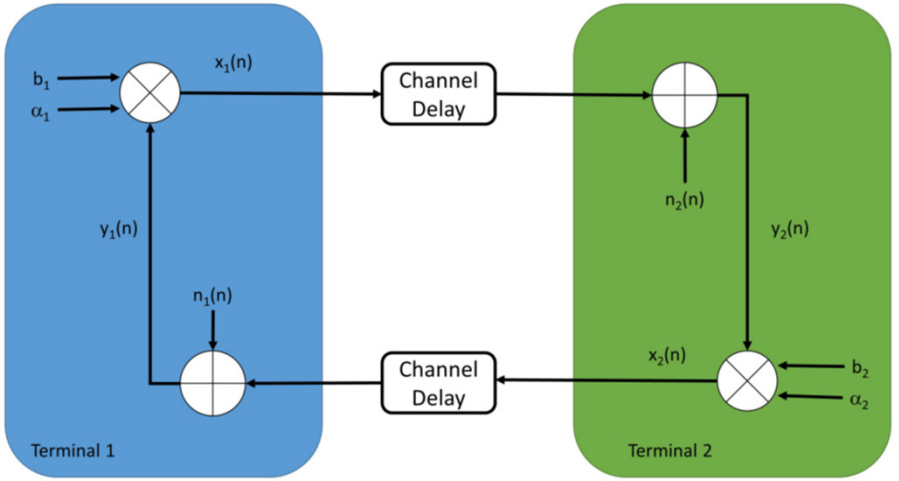
$$P_{out} = 1 - \int_0^{\infty}\!\!\iiint e^{-p(1+\tilde{\alpha}\gamma_{jr})-q\beta\left(\frac{1+\tilde{\alpha}\gamma_{jr}}{1+\tilde{\beta}\gamma_{je}}\right)} \cdot e^{-\tilde{\alpha}} e^{-\beta} e^{-\tilde{\beta}} d\tilde{\alpha} d\beta d\tilde{\beta} =$$

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

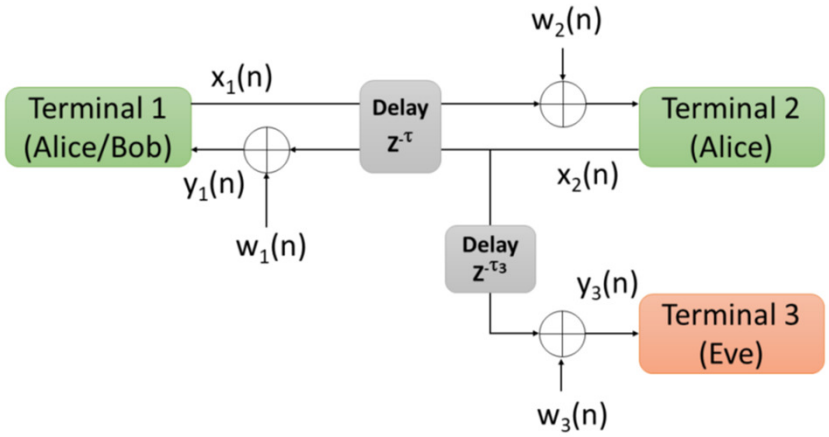
$$\left. \Omega\left(\frac{(q+1)(\gamma_{jr}p+1)}{\gamma_{jr}q}\right)\left(\gamma_{je}\gamma_{jr}p - (\gamma_{je}+1)\gamma_{jr}q + \gamma_{je}\right) + \gamma_{je}(\gamma_{je}\gamma_{jr}p + \gamma_{je} - \gamma_{jr}q)\right)$$

Noise-loop modulation

- Information is modulated with thermal noise
- Closed-loop transmission
  - Low data rate
- Bob can recover information from autocorrelation function
  - To recover one symbol, the other must be known
- Eavesdropping is not possible
  - No HPs on Eve position or conditions



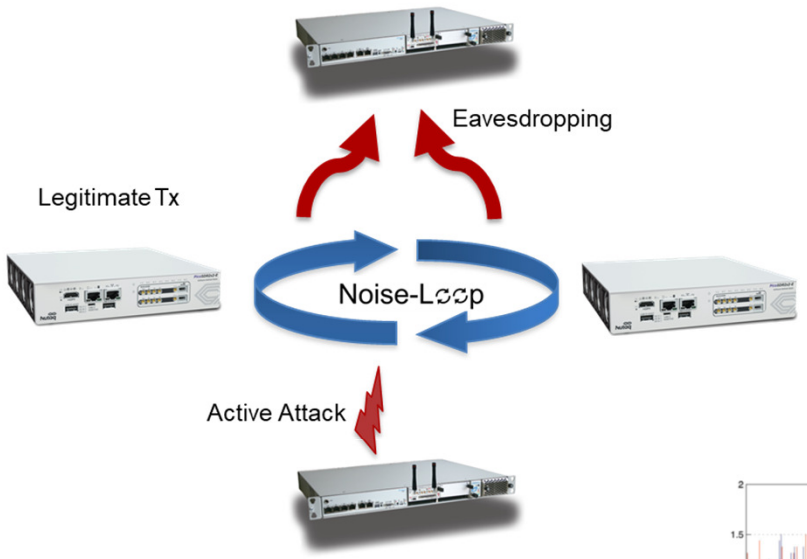
$$y_1(t) = \sum_{j=0}^{\infty} (b_1 b_2 \alpha_1 \alpha_2)^j n_1(t - 2j\tau_p) + \sum_{j=0}^{\infty} (b_1 b_2 \alpha_1 \alpha_2)^j b_2 \alpha_2 n_2(t - (2j+1)\tau_p)$$



$I(b_2; R_{y1}) = 1 \rightarrow$ Reliability

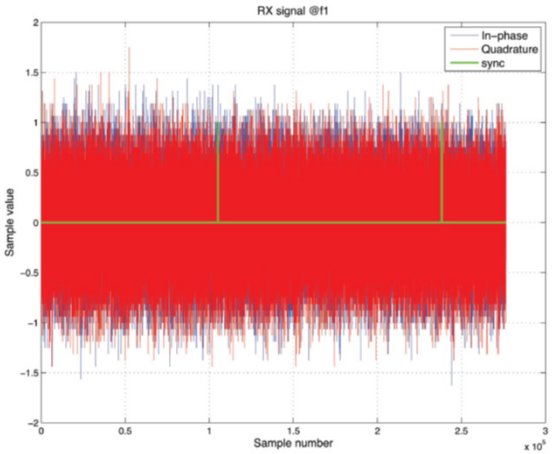
$I(b_2; R_{y3}) = 0 \rightarrow$ Security

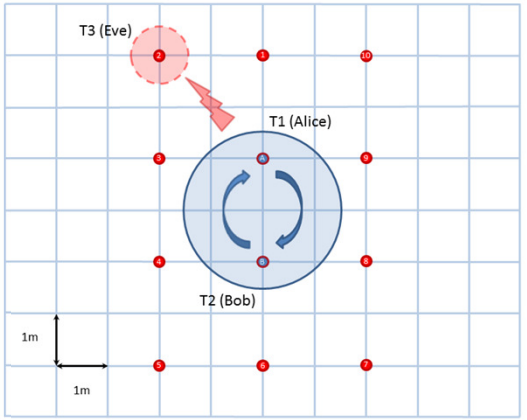
Implementation and testing



Field tests done with the IT Ministry of Defense

Noise-like





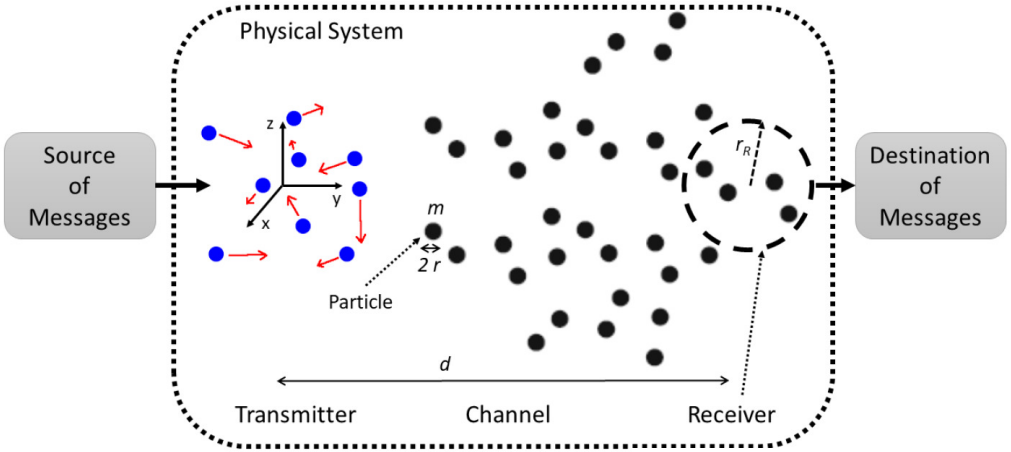
- Eavesdropping is not possible, no matter the computational power of the attacker
- Only low date rate services
- DoS is still possible

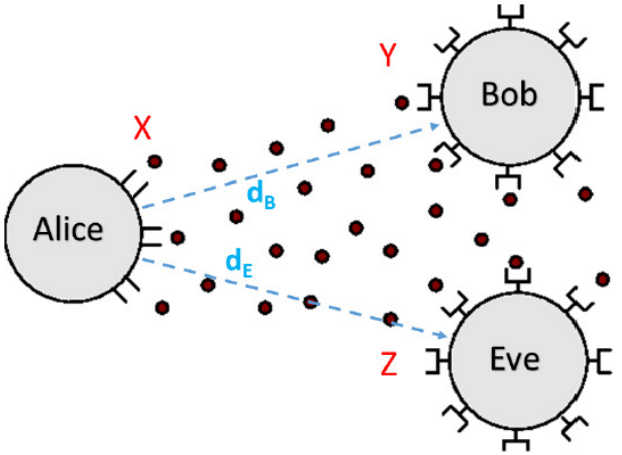
Recent advances

- Security in Molecular Communications
  - Which is the security limit when information is carried by particles?
- Energy cost of PhySec
  - How much energy has to be spent for security?
  - Joint optimization of energy and secrecy
- Resource management to provide PhySec
  - Which is the best association between BSs and UEs if security users are present in the cell?
  - Which is the best resource allocation (time, frequency, space)?
- Anomaly detection
  - How to detect an attack by analysing the physical characteristics of the received signal?

UNIVERSITÀ DEGLI STUDI FIRENZE

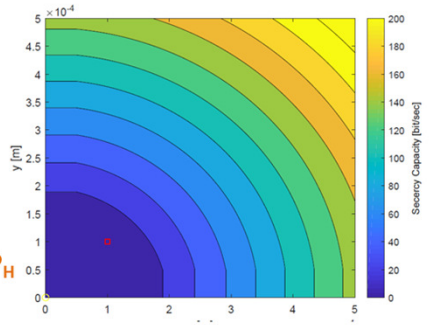
Secrecy Capacity in MolCom



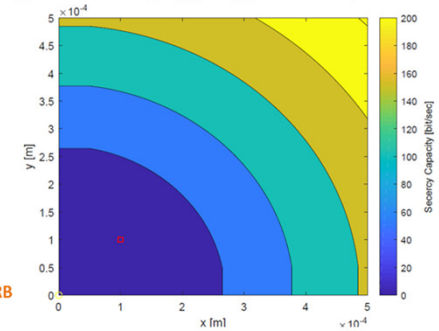


Closed-form mathematical expression of information leakage and secrecy capacity of an MC system based on free molecules diffusion.

P_H = 1e-12 W, r_{RB} = r_{RE} = 10 nm, B=20Hz



P_H = 1e-12 W, r_{RB} = r_{RE} = 10 nm, B=40Hz

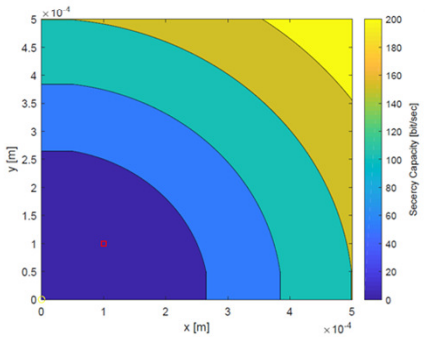


Double P_H

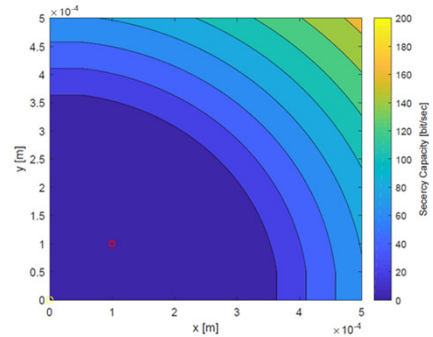
Double B

Double r_{RB}

P_H = 2e-12 W, r_{RB} = r_{RE} = 10 nm, B=20Hz



P_H = 1e-12 W, r_{RB} = 20 nm, r_{RE} = 10 nm, B=20Hz



Applications of PhySec

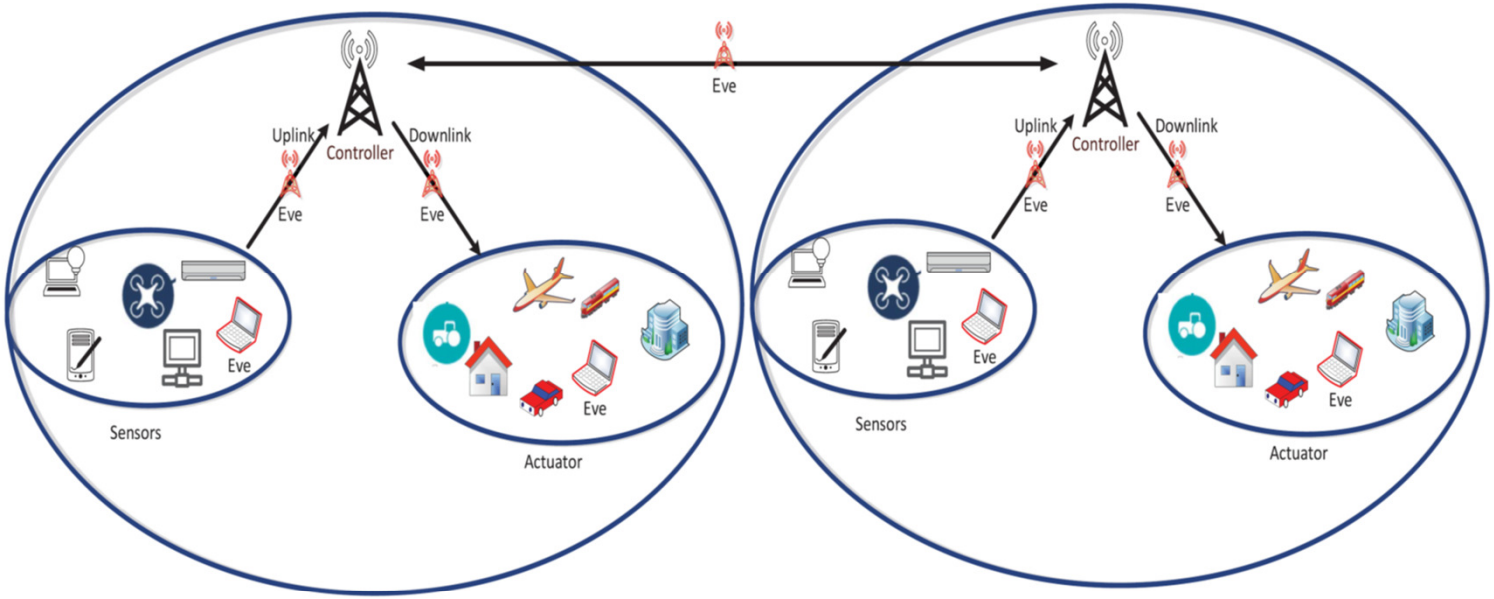
- Where low complex nodes are involved
  - In- and On-Body networks
  - Internet of Bio-Nano-Things
  - Wireless sensors network / IoT / RFID
  - D2D
- Critical services
  - e-payment
  - High sensitive data short-range transfer (e.g. health)
  - Autonomous vehicles / robots

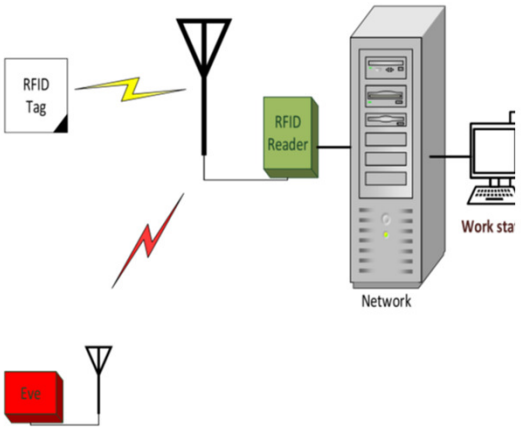
Different types of communication systems
5G mm-Wave
5G Non-Orthogonal-Multiple-Access (NOMA)
Index Modulation Based Systems
Visible Light Communication (VLC)
Smart Grid and Power Line Communication (PLC)
Internet of Things (IoT)
Body Area Networks (BAN) and In-Vivo
Vehicular and VANET
Cognitive Radio (CR)
Radio-Frequency Identification (RFID)
Ultra-Wideband (UWB)
Device-to-Device (D2D)
Unmanned Aerial Vehicle (UAV)

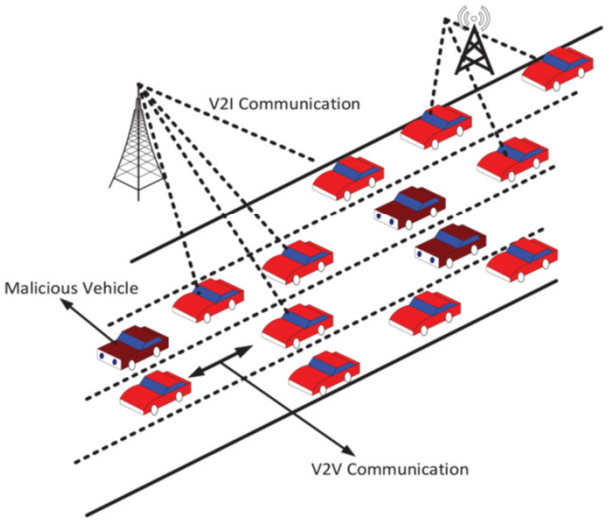
Set of mechanisms that exploit the properties of the physical layer to make an **attacker's job harder**.

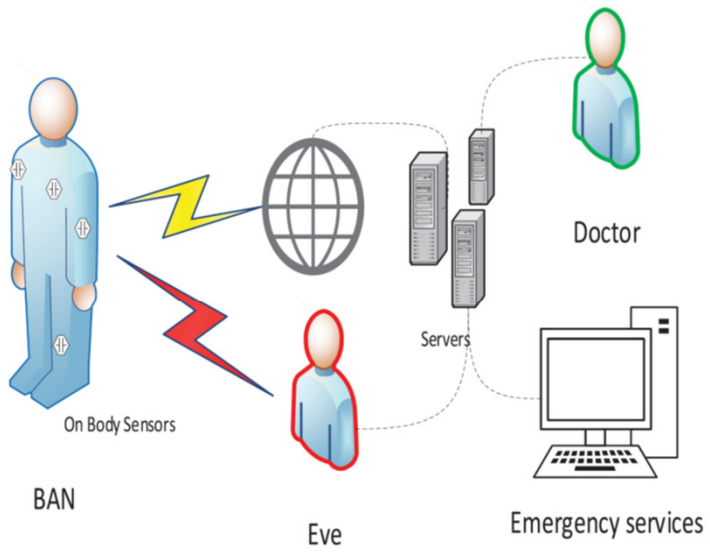
Physical layer security provides an **additional layer of security** which is not yet implemented in communication networks.

Application scenarios









UNIVERSITÀ DEGLI STUDI FIRENZE

(some) Publications

- L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo and M. Pierobon, "Secrecy Capacity and Secure Distance for Diffusion-based Molecular Communication Systems," in IEEE *Access*, Aug. 2019
- G. Chisci, A. Conti, L. Mucchi, and M. Z. Win, "Intrinsic Secrecy in Inhomogeneous Stochastic Networks," IEEE/ACM *Transactions on Networking*, vol. 27, no. 4, Aug. 2019.
- L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, “A new metric for measuring the security of an environment: The secrecy pressure,” IEEE *Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, May 2017.
- S. Soderi, L. Mucchi, M. Hamalainen, A. Piva, and J. Iinatti, ”Physical Layer Security based on Spread- Spectrum Watermarking and Jamming Receiver,” in *Transactions on Emerging Telecommunications Technologies* (ETT), vol. 28, no. 7, pp. 1-13, Dec 2016.
- L. Mucchi, L. Ronga, and G. Chisci, “Noise-loop multiple access,” IEEE *Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8255–8266, Oct 2016.
- T. Pecorella, L. Brilli, and L. Mucchi, “The role of physical layer security in IoT: A novel perspective,” MDPI *Information*, vol. 7, no. 3, pp. 49-66, Sept 2016.
- F. Ciabini, S. Morosi, L. Mucchi, and L. Ronga, "A Metric for Secrecy-Energy Efficiency Tradeoff Evaluation in 3GPP Cellular Networks," MDPI *Information*, vol. 7, no. 4, pp. 60-72, Oct 2016.