6G Research Visions Webinar Series

Research Challenges for Trust, Security and Privacy

Physical-layer Security in 6G Networks

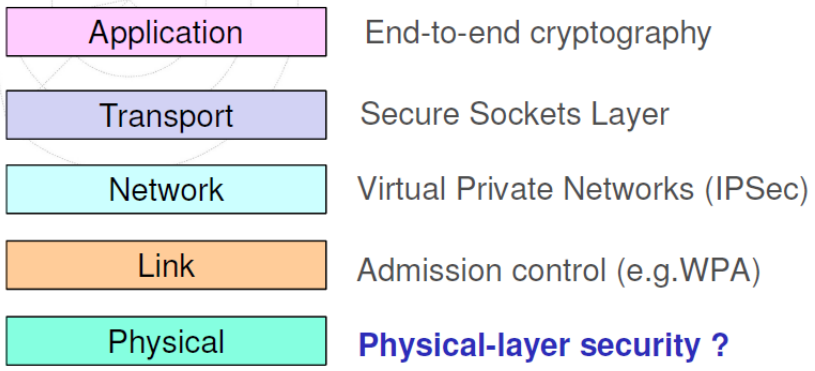
L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, H. Haas,
S. Shahabuddin, J. Bechtold, I. Morales, A. Stoica, G. Abreu

6G Research Visions Webinar Series:
Fundamental Research Challenges for Trust, Security and Privacy: where are we now and what needs to be done to have Trustworthy 6G.

Wednesday 28 October 2020

Why the PhySec?

- New security **challenges** in 6G:
  - How threats can be detected in ultra-dense heterogeneous networks with different levels of nodes complexity?
  - How confidentiality and integrity can be maintained without decreasing the user's experience?
  - How same level of security can be assured over multiple trust domains?
  - How to face the new unprecedent threats opened by AI-based or quantum-based networks?

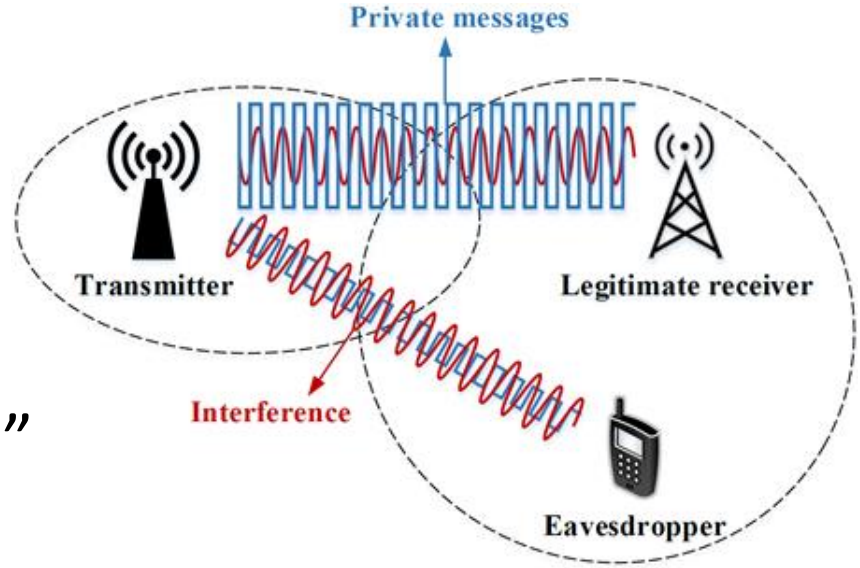


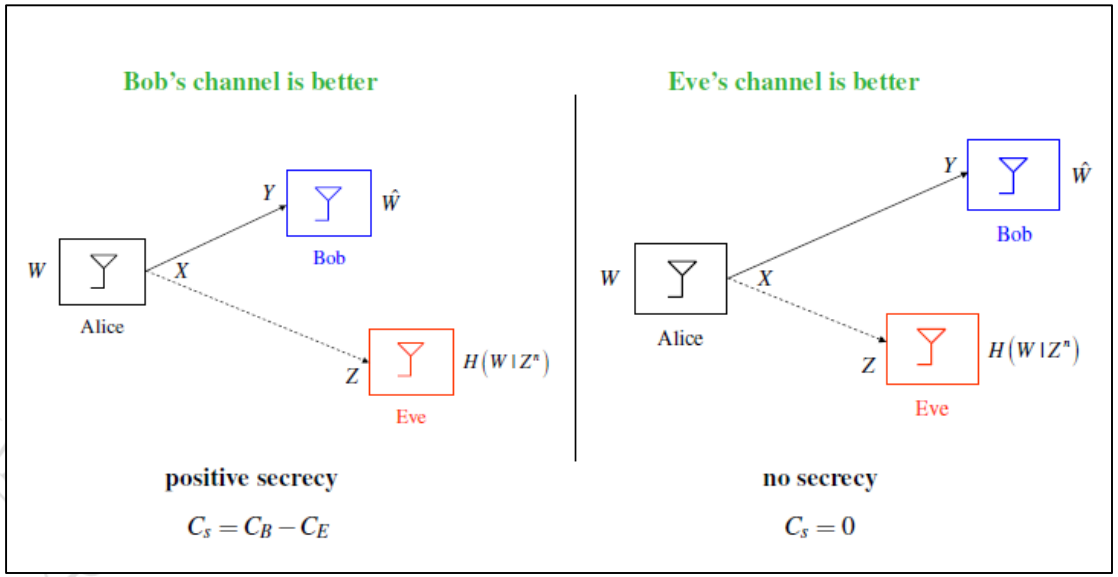
PhySec VS Cryptography

- Physical layer security aims at exploiting the randomness inherent in noisy channels to provide an additional level of protection at the physical layer
- PhySec does not rely on assumtpion of limited computational power of the attacker;
- Physical-layer security is **the first line of defense**, and it can provide security even to low complex nodes in different scenarios;

How it works?

- **Information-theoretic security** can be provided by any techniques which gives an "advantage" over the attacker
  - Exploit randomness
- Make Eve's channel more "noisy"
  - Exploit fading, MIMO, friendly jamming, IRS, coding, …





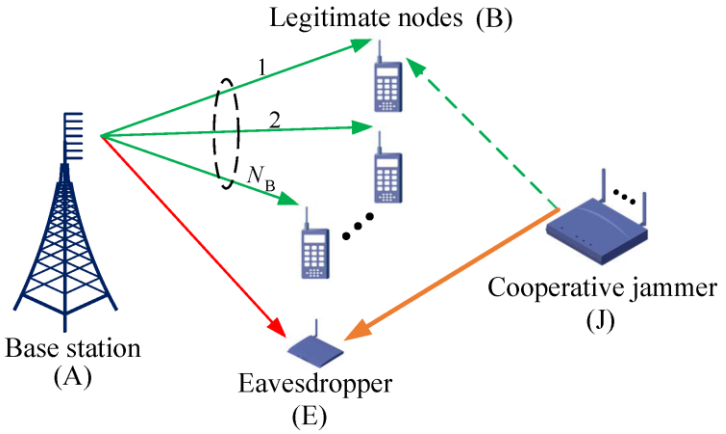
Cs = Cb – Ce

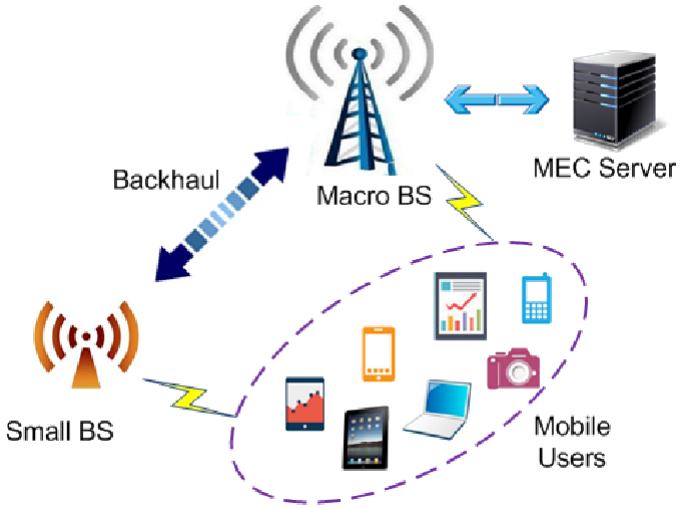
Ce = max I(W; Z)

I(W; Z) = H(W) – H(W|Z)

PhySec techniques

- Signal processing
  - Noisy modulations
- Coding
  - Wiretap codes
- Artificial noise injection
  - Friendly/cooperative jamming
- MIMO/IRS
  - Beamforming destructive signal
- HetNets
  - User/BS association to provide larger area of security
- Visible light communications (VLC)
  - Spatial confinement
- Keys generation



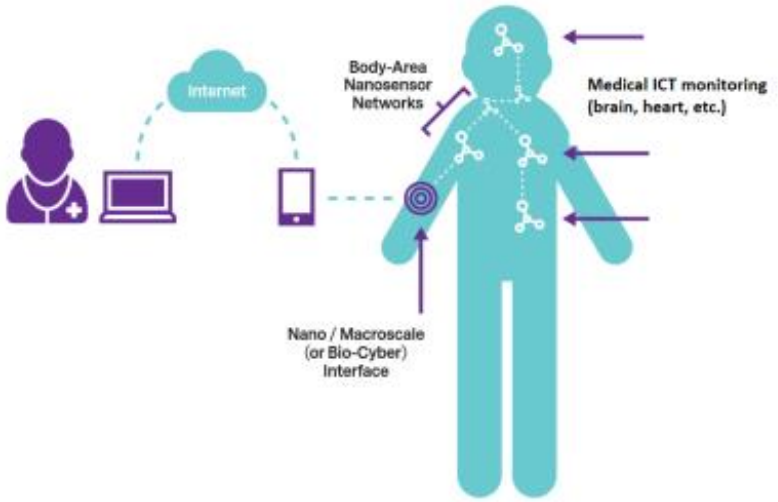


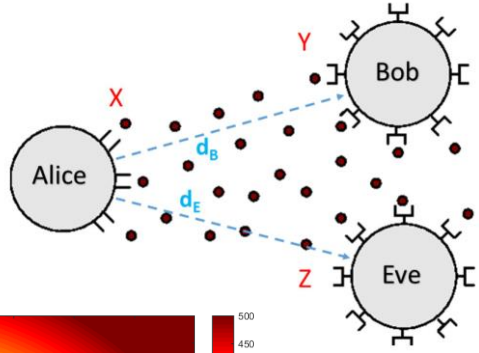
What PhySec can do for 6G?

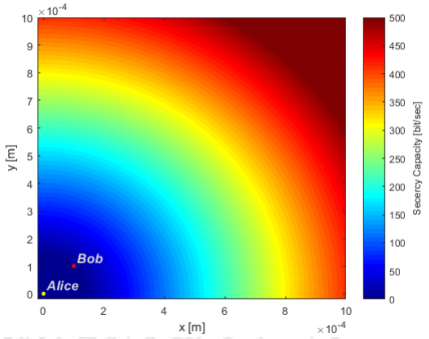
- **For low-resourced devices** (dry and wet nano-scale devices)
  - Signal processing
  - Coding
- **For massive deployed devices with mobility**
  - Massive Cell-Free MIMO
  - Intelligent reflecting surfaces (IRS)
- **For indoor environments**
  - Visible light communications (VLC)
- **For opportunistic/self-organizing networks**
  - Fast generation of PhySec-based crypto-key for symmetric encryption

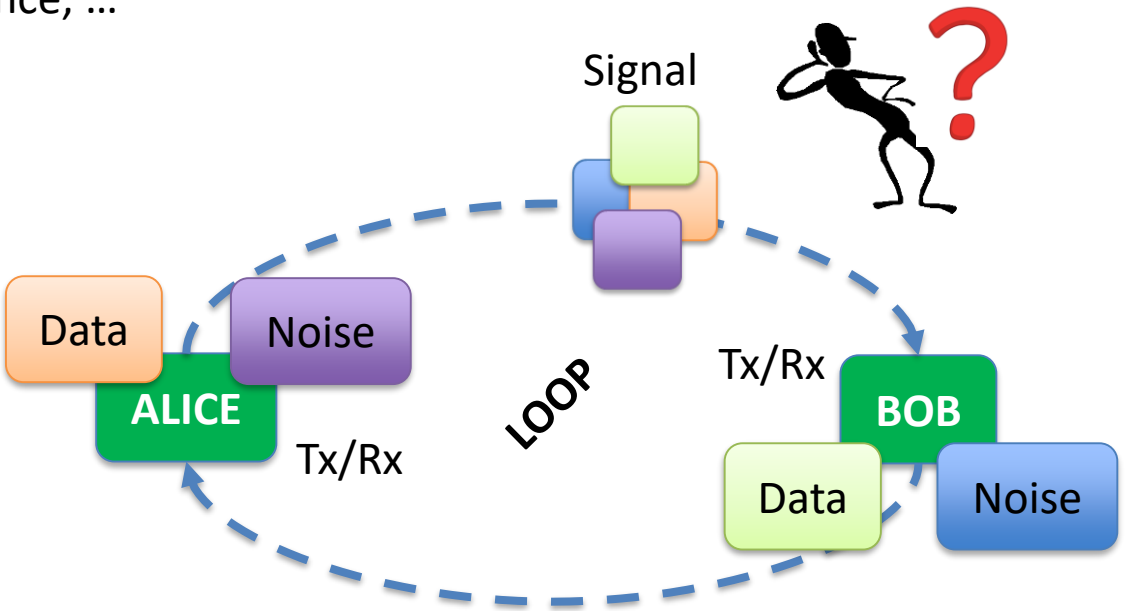
Physical-layer security for extremely low-resourced devices

- The human body will be part of the network architecture (wearable devices, implantable sensors, etc.)
  - Ultra low-resourced devices
  - Bio-nano devices
- Classical cryptography hard to be implemented
- PhySec can help: Noise-loop modulation, Wiretap codes, Secure area/distance, …



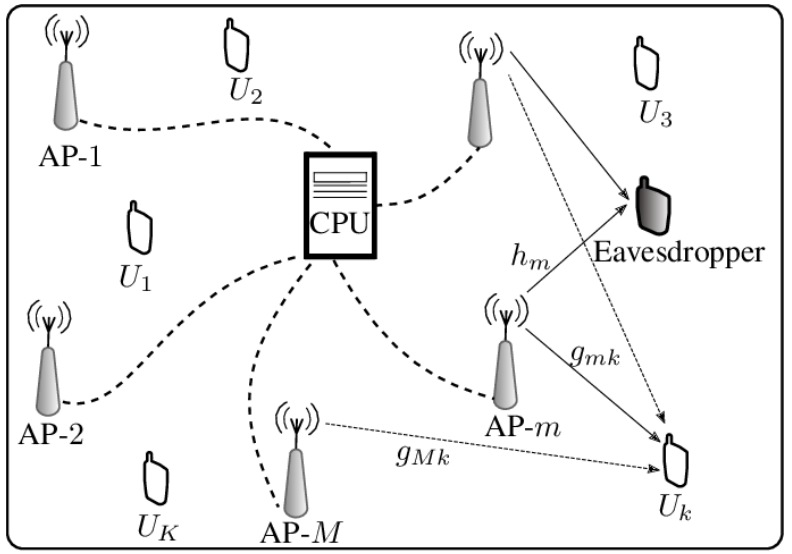


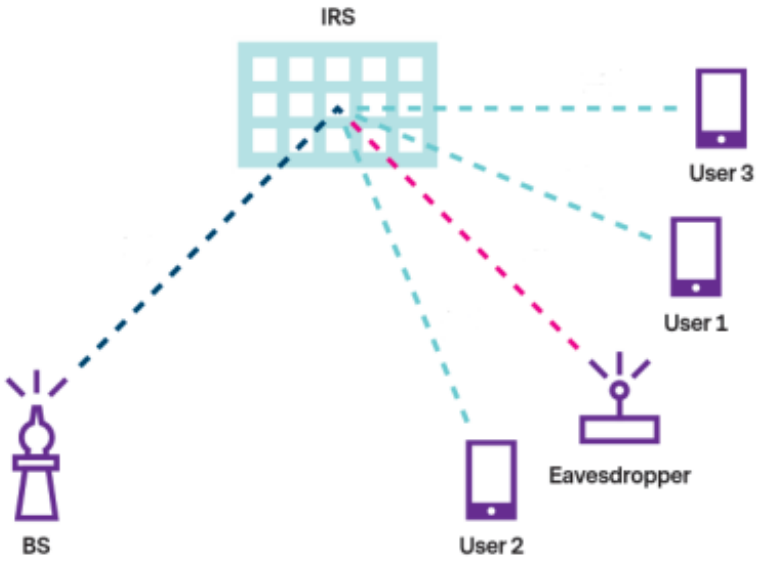




Security of Cell-free Massive MIMO and Intelligent Reflective Surface (IRS)

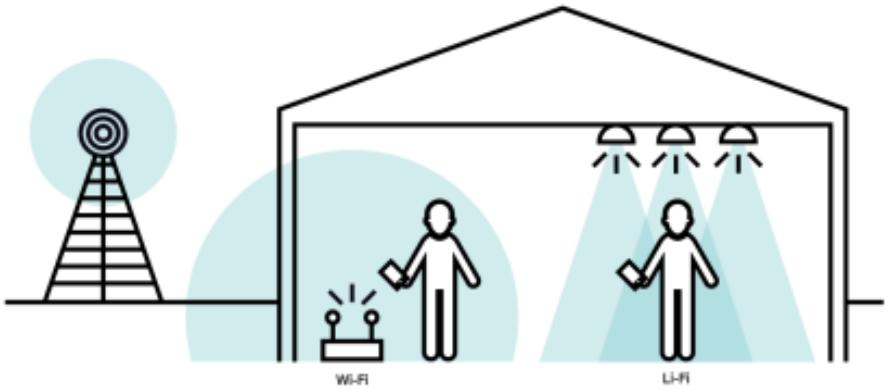
- **Cell-free massive MIMO** is a form of network MIMO where the antennas are not centralized but distributed among different locations
- Signals transmitted from different antennas are sent towards **Intelligent Reflecting Surface (IRS)**, which reflects a beamformed signal towards the user.
- Massive MIMO uses techniques like beamforming and jamming with **artificial noise insertion** to secure physical layer communications.
- IRS can be used in such a scenario to constructively add the **beamformed** signal towards the user and **destructively** add towards the eavesdropper.





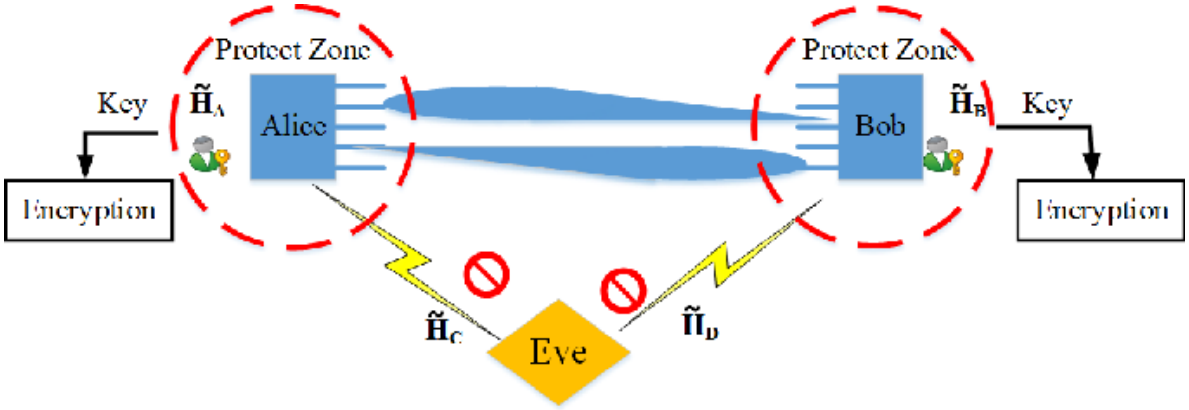
Physical Layer Security using Visible Light Communications in 6G

- **Visible Light Communications** (VLC), offer attractive features such as high capacity, robustness to electromagnetic interference, a high degree of **spatial confinement**, inherent security and unlicensed spectrum
- The key idea behind it is to utilize the intrinsic properties of the VLC channel to realize enhanced physical layer security
- Visible light does not penetrate walls
  - Information can be focused only where needed



Distributed and cooperative PHY-security protocols for 6G networks

- PLS may also exploit the intrinsic characteristics of the wireless channel to **co-generate a cryptographic key** for symmetric encryption
- PHY-based key generation solutions distinguish themselves from traditional key exchange solutions by being **completely decentralized** and not relying on any fixed parameters designed by a particular entity, but rather on the **distributed entropy** source that is the wireless channel
- Such **lightweight** implementations are ideal for networks of resource-constrained devices
- The usage of ML methods in networks with high PHY-Attribute visibility will enable real-time PHY-Layer monitoring and knowledge-based detection, making it highly attractive for leading AI companies to develop Security-as-a-Service (SecaaS) applications



UNIVERSITÀ DEGLI STUDI FIRENZE

Thank you!

- Questions?

- Contact details
  - **Lorenzo Mucchi**, Dept. of Information Engineering, University of Florence, Italy (lorenzo.mucchi@unifi.it)
  - **Erdal Panayirci**, Dept. of Electrical and Electronics Engineering, Kadir Has University, 34083, Istanbul, Turkey (eepanay@khas.edu.tr)
  - **Harald Haas**, LiFi Research and Development Centre, Department of Electronic & Electrical Engineering, University of Strathclyde, 99 George St., Glasgow, G1 1XW, UK. (harald.haas@strath.ac.uk).
  - **Shahriar Shahabuddin**, Mobile Networks, Nokia, Oulu, Finland. (shahriar.shahabuddin@nokia.com)
  - **Jonathan Bechtold, Ivan Morales, Razvan-Andrei Stoica**, WIOsense GmbH & Co. KG, Bremen, Germany. ({j.bechtold, i.morales, r.stoica}@wiosense.de)
  - **Giuseppe Abreu**, Dept. of Electrical Engineering and Computer Science, Jacobs University Bremen, Germany. (g.abreu@jacobs-university.de)