ELEC S425F

Computer and Network Security

Dr. Yaru FU

Hong Kong Metropolitan University

Personal Information:

- Name: Dr. Yaru Fu
- Email: yfu@hkmu.edu.hk
- Office: A0922, Block A, Main Campus
- Homepage: www.hkmu.edu.hk/yfu
- Appointment via Email for discussion or Q&A

My Courses in HKMU

- ELEC S306F Wireless Networks (Aut)
- ELEC S425F Computer and Network Security (Spr)
- MATH S232F Engineering Mathematic II (Spr)
- GEN S100F Mathematics in Daily Life (Aut)

Research Area:

- Wireless Communications and Networking
- Radio Resource Management
- Edge Caching and Computing

Academic Role:

- **Editor**: IEEE Wireless Communications Letters
- **Editor**: IEEE Networking Letters
- **Review Editor**: Frontiers in Communications & Networks
- **PI and Co-I**: RGC-FDS, R&D, RIF

Content

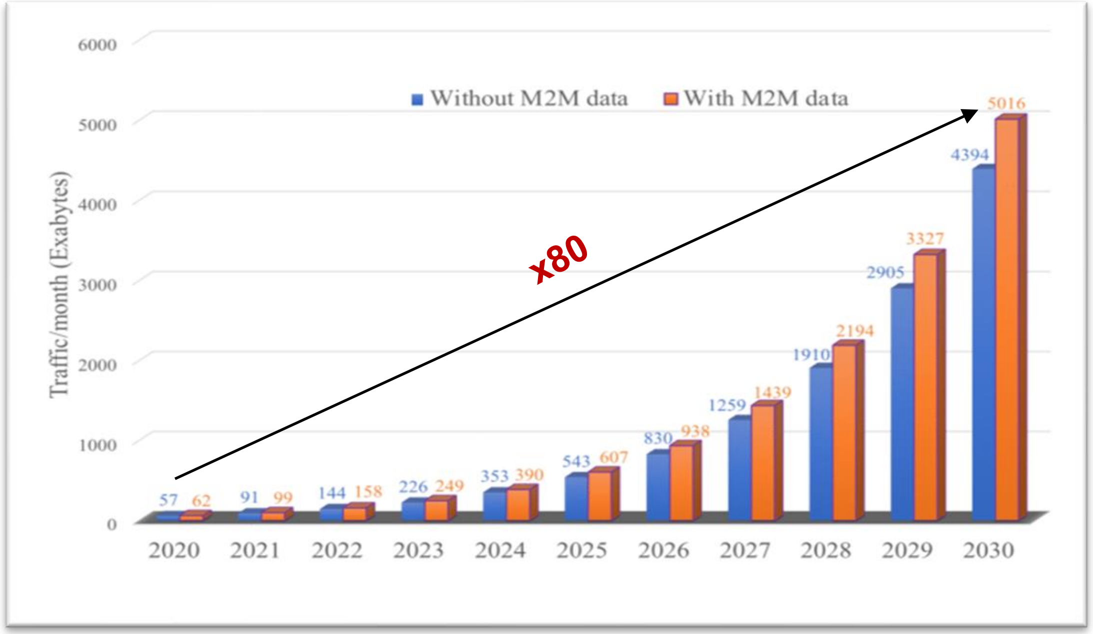
Part A: Physical Layer (PHY) Security in Wireless Communications

Part B: Advanced Technologies of 5G and beyond

Physical Layer (PHY) Security in Wireless Communications

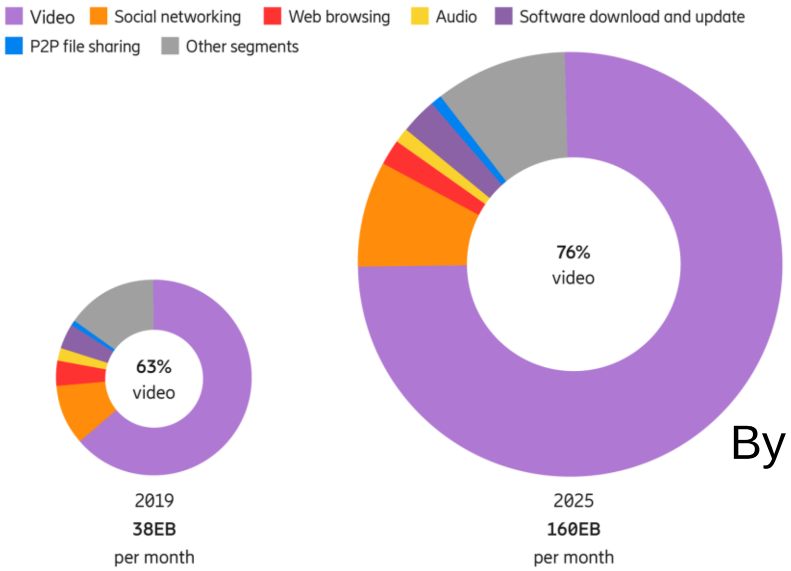
Why Wireless PHY-Security?

- Wireless communication services are enormously increasing due to the spread in wireless devices.
- The surge in wireless data transfer is driven by the huge number of applications customized for mobile users.
- Wireless media is becoming the dominant access for most of the interne-based services, serious security risks appear on the wireless signals because of their broadcasting features.



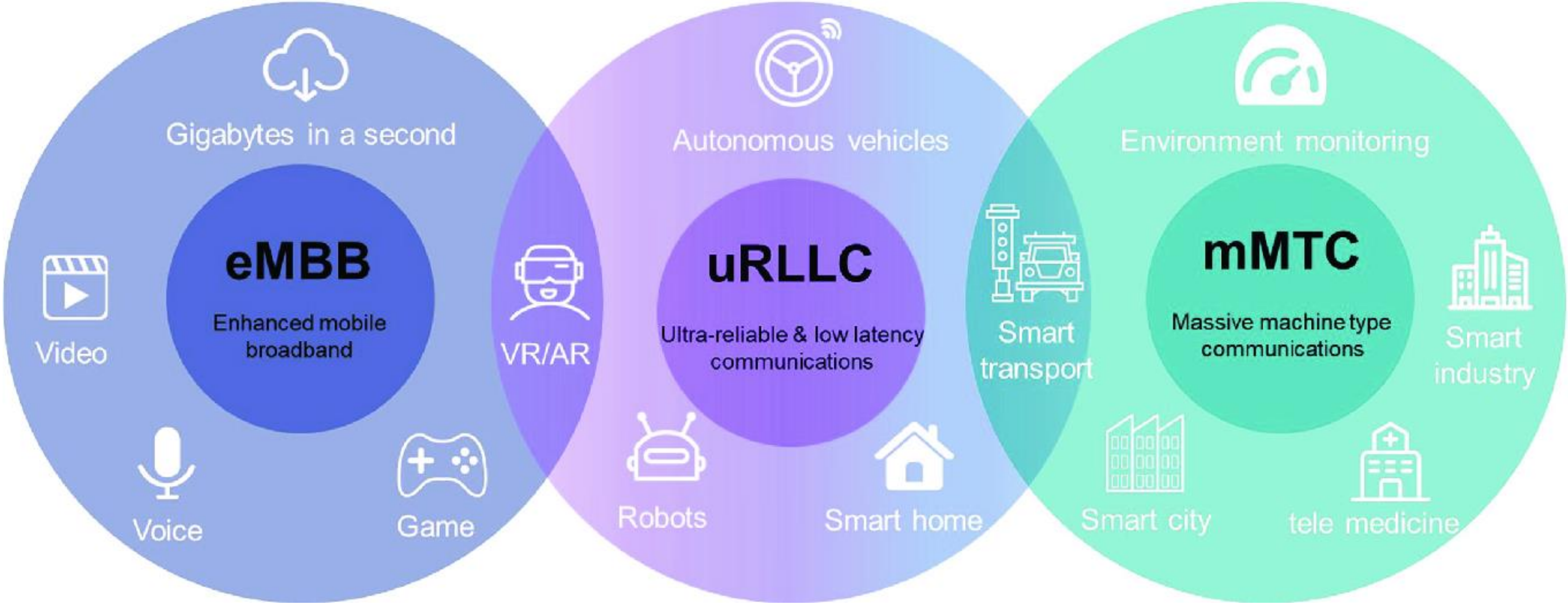
By Cisco

Mobile traffic by application category per month (percent)



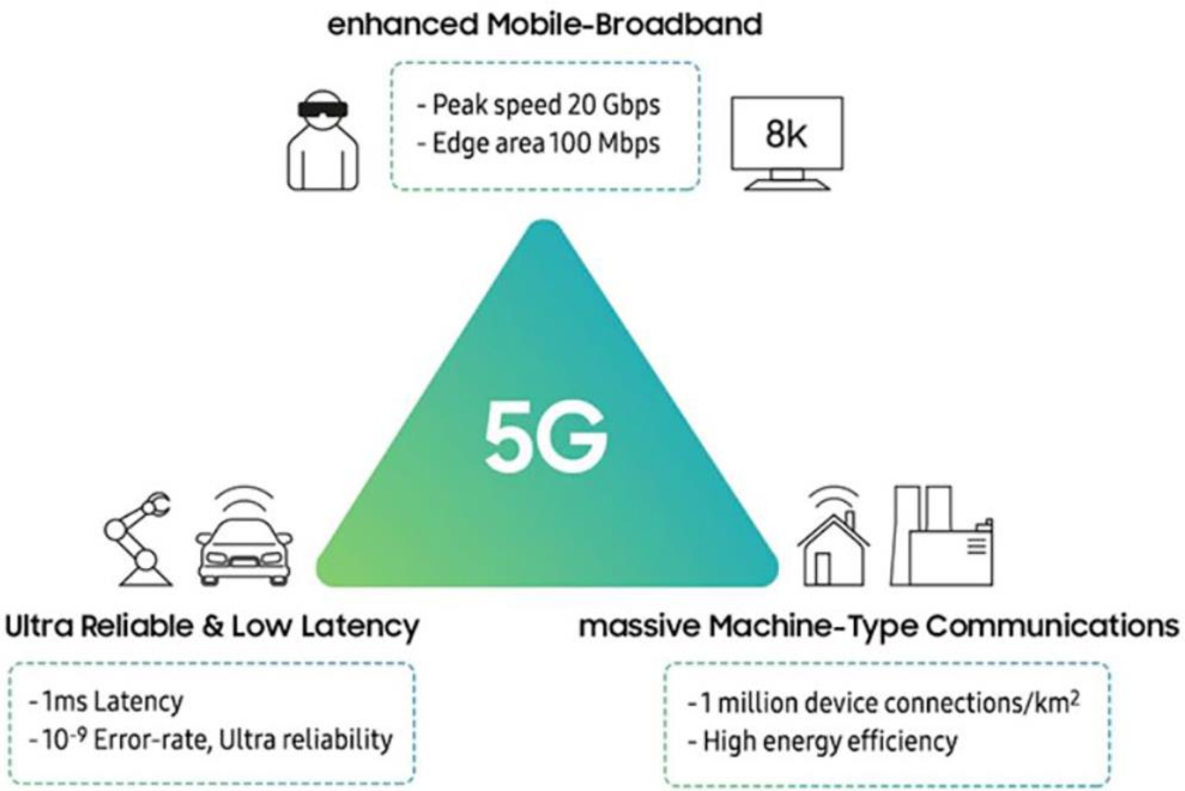
By Ericsson

Physical Layer (PHY) Security in Wireless Communications



Three application scenarios of 5G

Physical Layer (PHY) Security in Wireless Communications


enhanced Mobile-Broadband
- Peak speed 20 Gbps
- Edge area 100 Mbps
8k
5G
Ultra Reliable & Low Latency
- 1ms Latency
- 10^{-9} Error-rate, Ultra reliability
massive Machine-Type Communications
- 1 million device connections/km^2
- High energy efficiency

Three application scenarios of 5G and their requirements

Physical Layer (PHY) Security in Wireless Communications

■ Why Cryptographic approaches are not enough…

- The emergence of new wireless technologies like Internet-of-Things (IoT), massive machine-type communication (mMTC), 5G-Tactile Internet, vehicular communication for autonomous driving, remote surgery, instance control for sensitive IoT actuators, etc, making current encryption-based methods unsuitable since these kind of technology naturally delay-sensitive, power-limited, and processing-restricted.

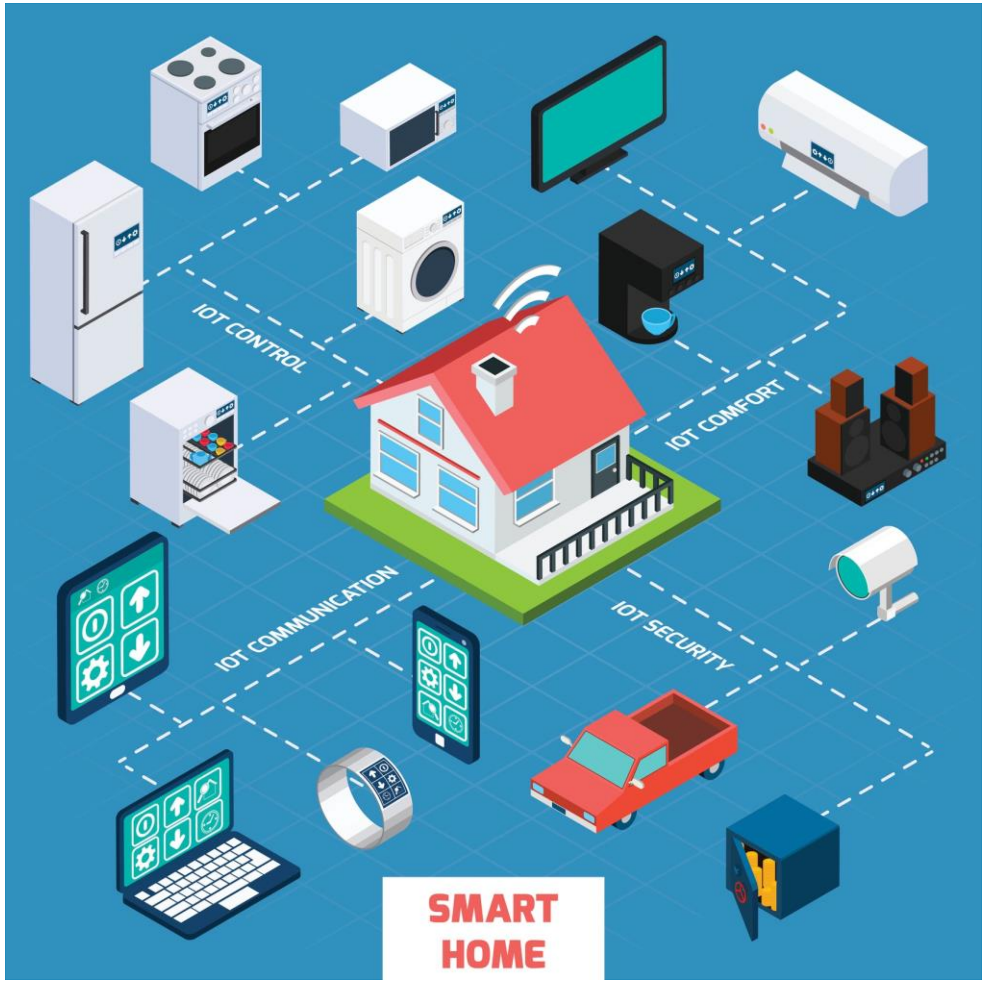
M2M communications

Cryptography is going against the requirements of future services!

Physical Layer (PHY) Security in Wireless Communications

- **Why Cryptographic approaches are not enough…**

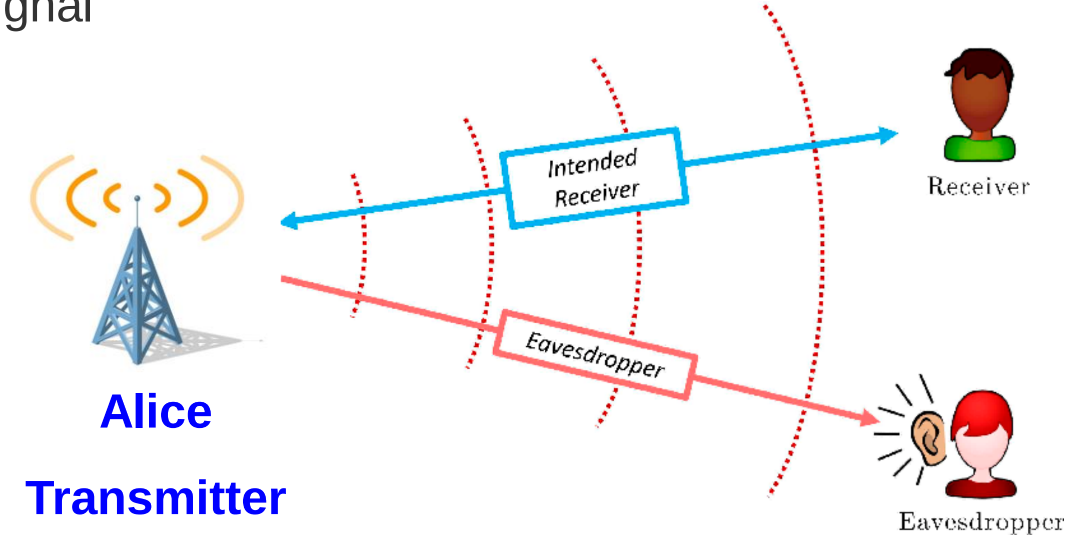
- Moreover, mobile cellular users are anticipated to even be willing and ready to pay extra charges just for the sake of completely ensuring the security of their importance services. Thus, physical security as a service is expected to be one of the future killer applications of mobile service providers, where users can be charged a little more for providing them with strong, perfect secure services.



Physical Layer (PHY) Security in Wireless Communications

■ What is the solution

- New approaches like **physical layer security (PLS)** to secure the transmissions on the signal level instead of the bit level.
  - ✓ Jamming: also known as a denial of service (DoS) is a usual attack against security in the PHY of wireless networks. Sol: frequency hopping, filtering, etc
  - ✓ Eavesdropping: non-authorized users attempt to intercept the confidential information by decoding its received signal



Bob

Legitimate user

Alice

Transmitter

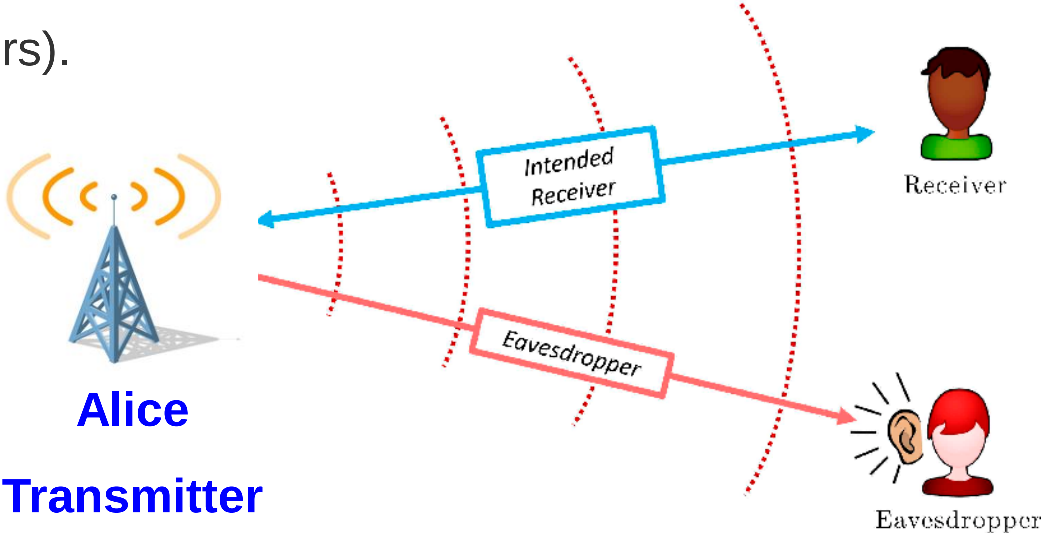
Eve

Non-authorized user

Physical Layer (PHY) Security in Wireless Communications

Physical layer security (PLS)

- PLS has emerged as a novel concept that can **integrate/complement and may even substitute/replace encryption-based schemes**, which suffer from many drawbacks and practical issues in future wireless systems such as IoT. The essential idea of PLS is to utilize the characteristics of the wireless channel including **randomness, spatial decorrelation, TDD reciprocity, diversity**, etc, along with its impairments including **noise, fading, interference, dispersion**, etc, to ensure confidential data transmission to the legitimate users only against unintended receivers (eavesdroppers).



Bob

Legitimate user

Alice

Transmitter

Eve

Non-authorized user

Physical Layer (PHY) Security in Wireless Communications

■ Physical layer security (PLS)

- Randomness
- Spatial decorrelation
- TDD reciprocity
- Diversity
- noise, fading, interference, dispersion

Physical Layer (PHY) Security in Wireless Communications

■ Cryptographic approaches V.S. PLS

- Cryptographic-based methods: Symmetric-key cryptography (issue: key distribution) and public-key cryptography (issue: key generation, replying on mathematical cryptographic algorithm)
  - ✓ Computational complexity – v.s. – level of secrecy
  - ✓ High computing capability, e.g., brute-force attack. ☹ ☹ ☹
- PLS uses the inherent randomness (e.g., noise and fading) of the wireless channel to ensure secure communications in the physical layer
  - ✓ High computing capability. ☺ ☺ ☺

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(1) **Secrecy Capacity *C*s**: The secrecy capacity, *C*s, for a wireless channel is the most used metric in PLS evaluation. *C*s is defined as the capacity difference between the main and wiretap channels. Rigorously speaking, it defines the maximum secret rate at which the secret information reliably recovers at transmitter while remaining unrecoverable at Eve.

$$\begin{aligned} C_{\mathrm{S}} &= \max\{C_{\mathrm{B}} - C_{\mathrm{E}}, 0\} \\ &= \max\{\mathrm{W}\log_2(1+\gamma_{\mathrm{B}}) - \mathrm{W}\log_2(1+\gamma_{\mathrm{E}}), 0\} \end{aligned}$$

where $\gamma_{\mathrm{X}} = \frac{|h_{\mathrm{AX}}|^2 P_{\mathrm{A}}}{N_0}$, depicting the signal-to-noise ratio (SNR), in which X belongs to {B, E}.

In addition, h_{AB} and h_{AE} are the channel coefficients of the main and wiretap channels, respectively. P_A is the transmit power at Alice, N_0 is the average noise power, and C_B and C_E are the capacities of the main and wiretap channels, respectively.

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(2) **Secrecy Outage Probability (SOP)**: The SOP is defined as the probability that the secrecy capacity falls below a target secrecy rate of R_S. In other words, when the current *Cs* is not more than a pre-established target R_S, the secrecy outage happens. This fact means that the current secrecy rate cannot guarantee the security requirement.

$$\begin{aligned}\mathrm{SOP} &= \Pr\left\{C_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}\right) < R_{\mathrm{S}}\right\} \\ &\overset{(a)}{=} \Pr\left\{\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right) < 2^{R_{\mathrm{S}}}\right\} \\ &\overset{(b)}{\geq} \Pr\left\{\frac{\gamma_{\mathrm{B}}}{\gamma_{\mathrm{E}}} < 2^{R_{\mathrm{S}}}\right\}\end{aligned}$$

where Pr {·} denotes probability. The SOP in (a) indicates that whenever $R_S < C_S$, the wiretap channel will be worse than the legitimate channel. So, secure communications are possible. It is worth mentioning that state of the art on PLS's research topic over different types of fading channels focuses on the calculation of (b) due to its simpler mathematical tractability concerning the formulation in (a). Furthermore, the formulation in (b) is well-known as the lower bound of the SOP and represents the ratio of γ_B and γ_E, which can follow any fading distribution.

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(2) **Secrecy Outage Probability (SOP)**:

- it cannot offer any information about the bob’s skill to decode transmitted data successfully, i.e., **transmission reliability**
- it cannot quantify the amount of data leaking to the eavesdroppers when the outage happens, i.e., **transmission security**
- it cannot offer any information about the **eve’s skill to decrypt confidential data** successfully

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(3) **Alternative Secrecy Outage Probability**: Conventional SOP formulation does not distinguish between reliability and security. Therefore, an outage event in SOP can imply either a fault to achieve secrecy or that the transmitted message cannot be successfully decoded by Bob**.**

$$\mathrm{SOP}_{\mathrm{A}} = \mathrm{Pr}\left\{C_{\mathrm{E}} > C_{\mathrm{B}} - R_{\mathrm{S}} | \gamma_{\mathrm{B}} > \mu\right\}$$

where μ is a certain threshold for which allows Alice to **decide whether** (when $\gamma_{B} > \mu$) **or not** (when $\gamma_{B} <= \mu$) **to transmit the information**. Furthermore, this metric is useful when Alice knows Bob’s CSI.

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(4) a. **Average Information Leakage Rate:**

$$R_{\mathrm{L}} = \mathbb{E}\left[\left(1 - \Delta\right) R_{\mathrm{S}}\right] = \left(1 - \bar{\Delta}\right) R_{\mathrm{S}}$$

$$\Delta = \begin{cases} 1, & \text{if } C_{\mathrm{E}} \leq C_{\mathrm{B}} - R_{\mathrm{S}} \\ \left(C_{\mathrm{B}} - C_{\mathrm{E}}\right) / R_{\mathrm{S}}, & \text{if } C_{\mathrm{B}} - R_{\mathrm{S}} < C_{\mathrm{E}} < C_{\mathrm{B}} \\ 0, & \text{if } C_{\mathrm{B}} \leq C_{\mathrm{E}}. \end{cases}$$

This metric explains the amount of data leaking to Eve when an unchanged rate transmission, *R*$_{\mathrm{S}}$, is adopted in the system.

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(4) b. **Generalized Secrecy Outage Probability (GSOP)**: This metric is related to wireless systems with distinct secrecy levels measured in terms of **Eve's capability to decode the confidential information** and is given by

$$\mathrm{GSOP} = \Pr\{\Delta < \theta\}$$

where 0 < θ < 1 represents the minimum reasonable value of the fractional equivocation, and Δ is the fractional equivocation, is a random quantity due to the propagation medium's fading Characteristics. Detail is given as follows:

$$\Delta = \begin{cases} 1, & \text{if } C_{\mathrm{E}} \leq C_{\mathrm{B}} - R_{\mathrm{S}} \\ \left(C_{\mathrm{B}} - C_{\mathrm{E}}\right)/R_{\mathrm{S}}, & \text{if } C_{\mathrm{B}} - R_{\mathrm{S}} < C_{\mathrm{E}} < C_{\mathrm{B}} \\ 0, & \text{if } C_{\mathrm{B}} \leq C_{\mathrm{E}}. \end{cases}$$

Physical Layer (PHY) Security in Wireless Communications

- **PLS Performance Metrics**

(5) **Intercept Probability**: An intercept event happens when the *C*s is negative or falls below 0. This means that the wiretap channel has a better SNR than the legitimate channel. The intercept probability can be formulated as

$$P_{\text{int}} = \Pr\left\{C_{\text{S}}\left(\gamma_{\text{B}}, \gamma_{\text{E}}\right) < 0\right\}$$

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(6) **Probability of Strictly Positive Secrecy Capacity**: The Probability of SPSC is the probability that the *C*s remains higher than 0. This means that secrecy in communication has been attained

$$P_{\mathrm{SPSC}} = \Pr\left\{C_{\mathrm{S}}\left(\gamma_{\mathrm{B}}, \gamma_{\mathrm{E}}\right) > 0\right\}$$

Physical Layer (PHY) Security in Wireless Communications

■ PLS Performance Metrics

(7) **Secrecy Throughput (ST):** ST is a useful metric to assess the secrecy performance of the next wireless communications systems. The ST is defined as confidential data transmission.

$$\eta = p_{tx}(\mu) R_{\mathrm{S}},$$

where $p_{tx}(\mu)$ denotes the probability of success in the transmission, and is given by

$$p_{tx}(\mu) = \Pr\left\{\gamma_{\mathrm{B}} > \mu\right\}.$$

Physical Layer (PHY) Security in Wireless Communications

■ Performance Optimization

- the constraints based on reliability and secrecy requirements
- the availability of Bob’s CSI at Alice

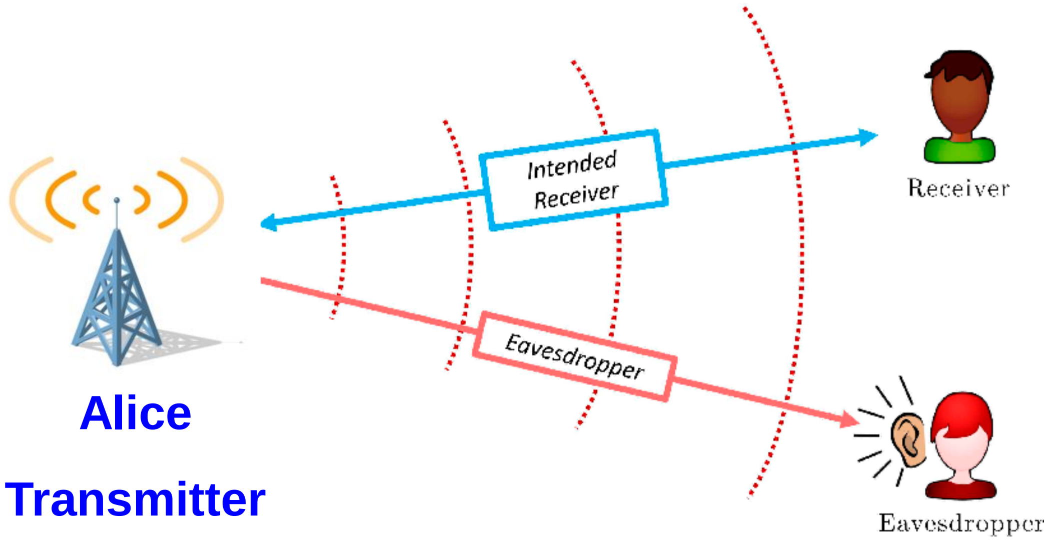
Obj: Maximize ST

$$\begin{aligned} \max_{\mu, R_{\mathrm{S}}} \quad & \eta \\ \text{s.t.} \quad & \mathrm{SOP}_{\mathrm{A}}(\mu, R_{\mathrm{S}}) \leq \epsilon, p_{tx}(\mu) \geq \delta, R_{\mathrm{S}} > 0, \end{aligned}$$

In which the first two conditions denote the reliability and security requirements, respectively.

Physical Layer (PHY) Security in Wireless Communications

Exercise 1: The SNRs of Bob and Eve are 12 dB and 15dB, respectively. The threshold for successful decoding at Bob is 15 dB. In addition, the target secure rate is 1 Mbit/s. Moreover, system bandwidth is 1MHz. Please help Alice to judge whether the secure transmission to Bob can be realized? What if the threshold for successful decoding is 10 dB?



Bob

Legitimate user

Alice

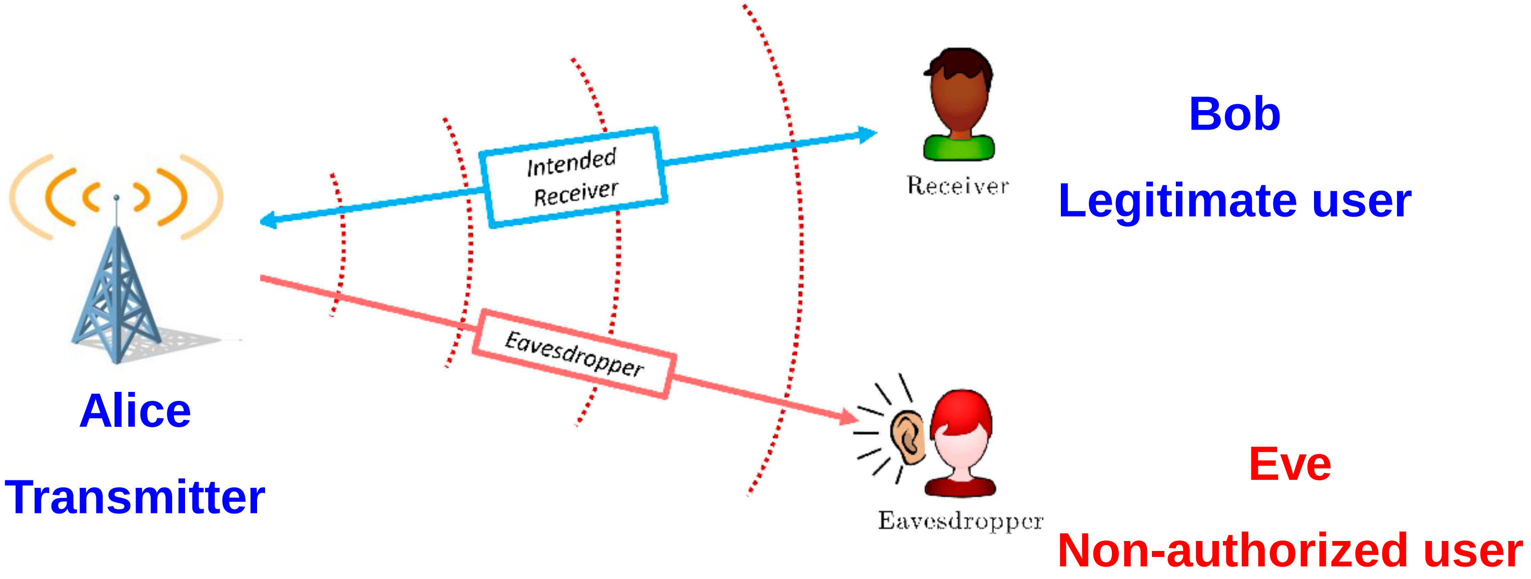
Transmitter

Eve

Non-authorized user

Physical Layer (PHY) Security in Wireless Communications

Exercise 2: The SNRs of Bob and Eve are 15 dB and 12 dB, respectively. The threshold for successful decoding at Bob is 10 dB. In addition, the target secure rate is 1 Mbit/s. Moreover, system bandwidth is 1MHz. Please help Alice to compute whether the secure transmission to Bob can be realized?



Bob

Legitimate user

Alice

Transmitter

Eve

Non-authorized user