Ph.D. **ANNA VALERIA GUGLIELMI**
Supervisor Ph.D. GIULIA CISOTTO
DEI-Unipd

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Protocollo di secret key agreement basato su biometria
per Wireless Body Area Networks

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
ROMA

Padova, 25 Novembre 2020

Borsisti Day 2020

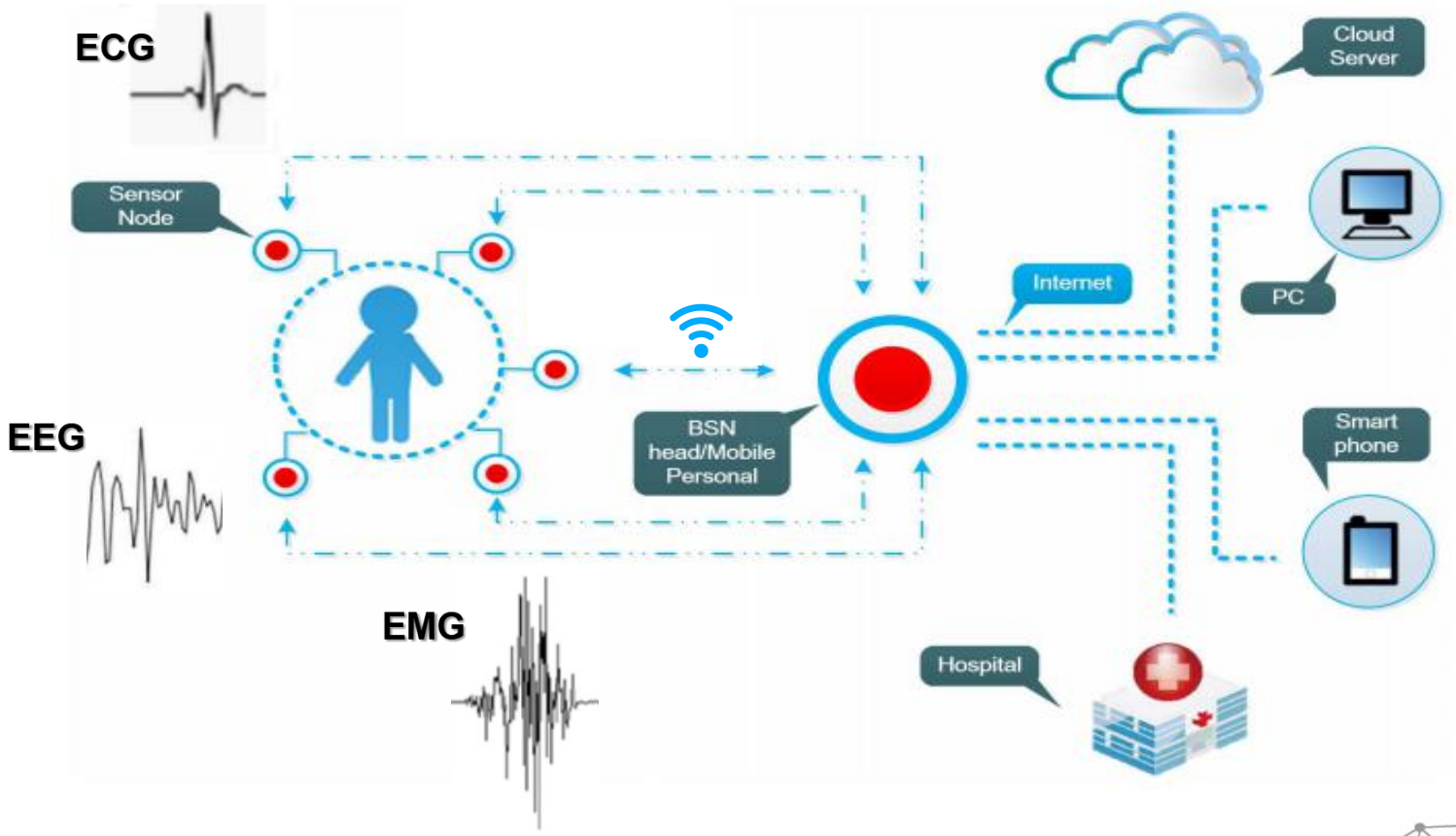
Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

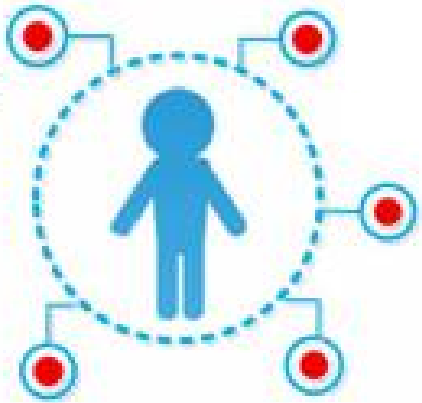
Modello per wireless BAN



Definizione del problema

Scambio sicuro delle informazioni fisiologiche

- privacy dei dati
- autenticazione per accesso ai dati
- integrità dei dati



Contenuti della presentazione

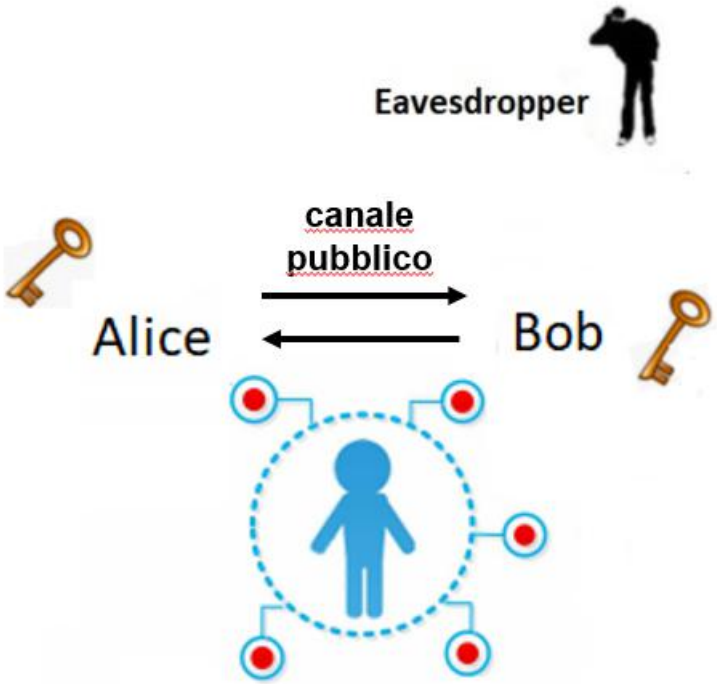
- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Metodi

Schemi di Information-theoretic security

- sistemi basati su third-party key management (letteratura corrente)
- *unconditionally secure* (Novità!)

Metodi

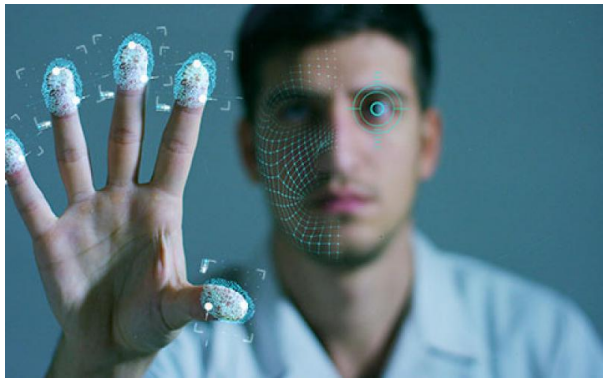


- Valutare il **secret-key rate**
  → massimo rate con cui si può generare una chiave segreta
- Fare **information reconciliation**
  → correzione delle discrepanze tra le misurazioni usate
- Fare **privacy amplification**
  → generazione vera e propria della chiave segreta

Metodi

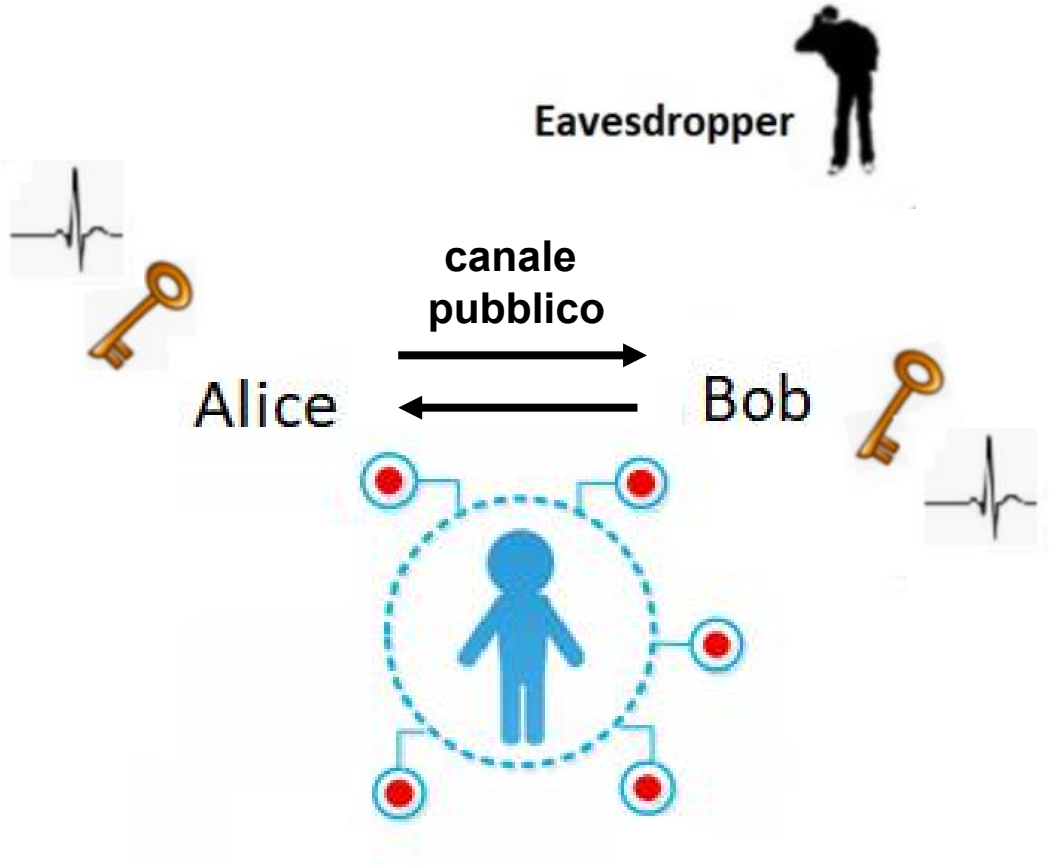
Schemi basati su biometria per la sicurezza

- biometria unimodale statica e multimodale mista



- biometria multimodale dinamica (Novità!)

Scenario per il key-agreement proposto



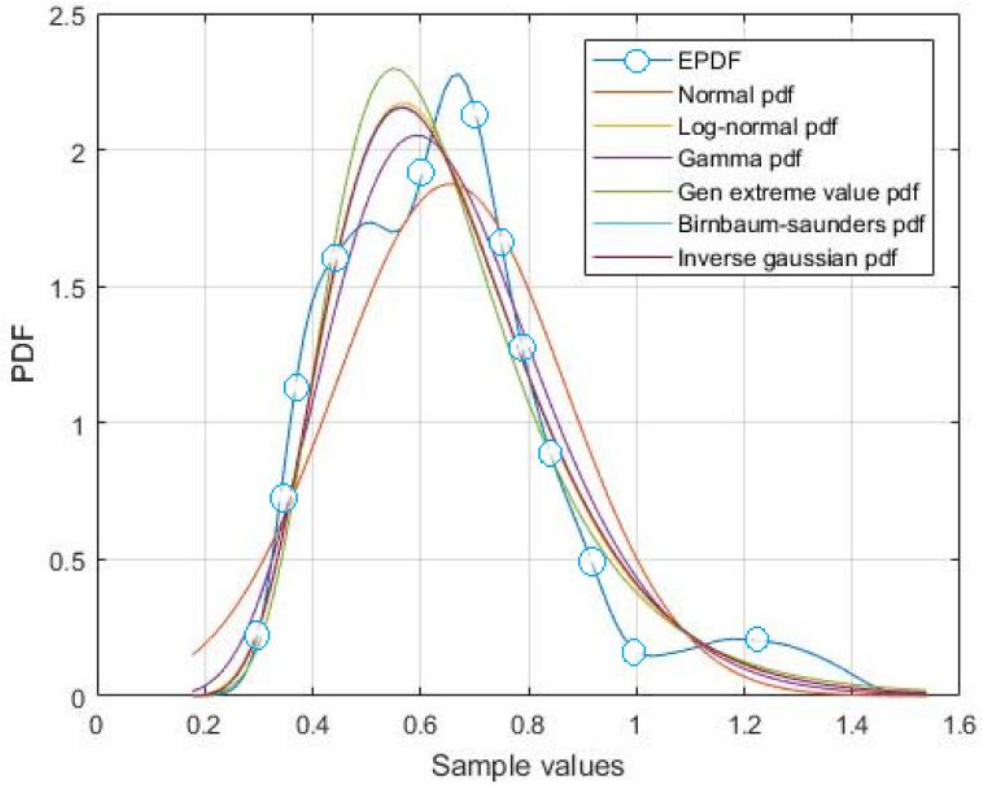
Scopo:

sfruttare variabilità e correlazione dei biosegnali per generare una chiave segreta ignota ad un potenziale attaccante

Contenuti della presentazione

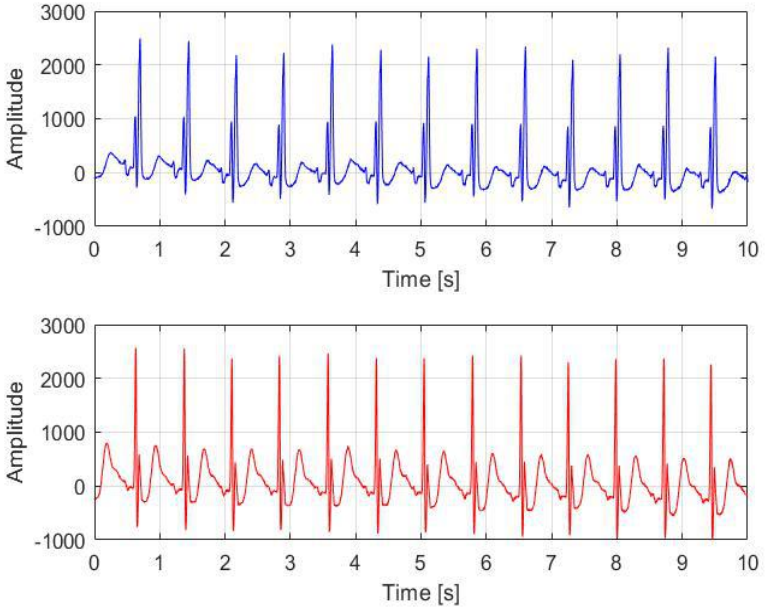
- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Caratterizzazione statistica dei segnali

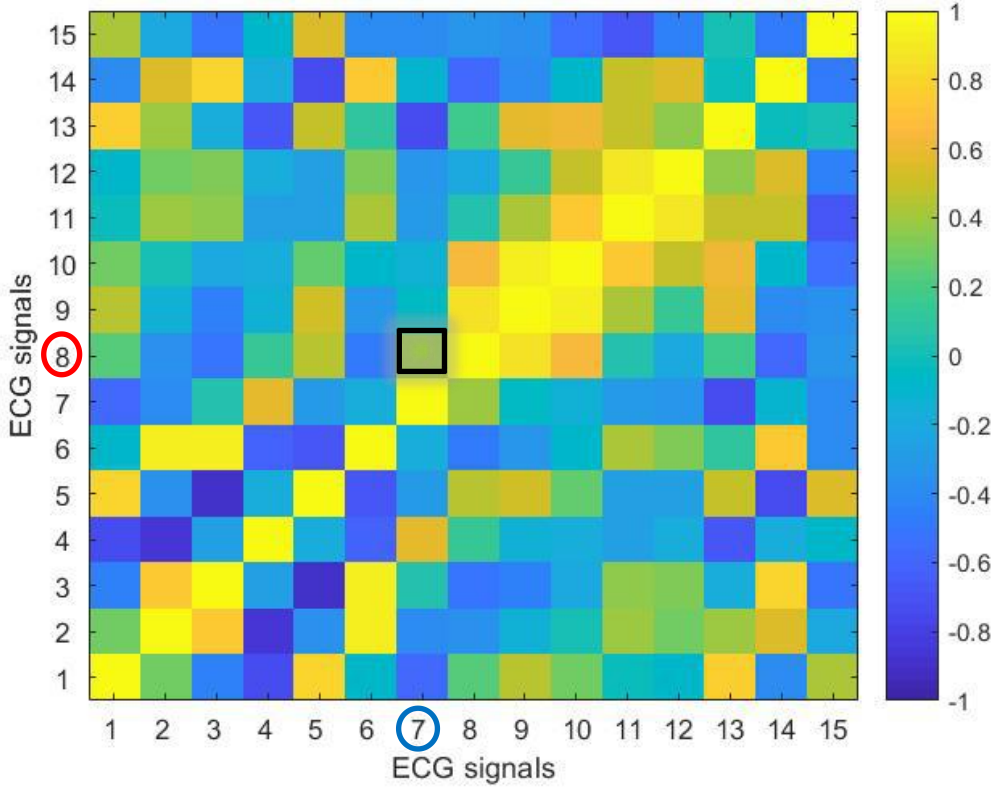


- Non esiste un modello di distribuzione univoco
- Modelli generativi già esistenti per la conoscenza dell'attaccante

Caratterizzazione statistica dei segnali

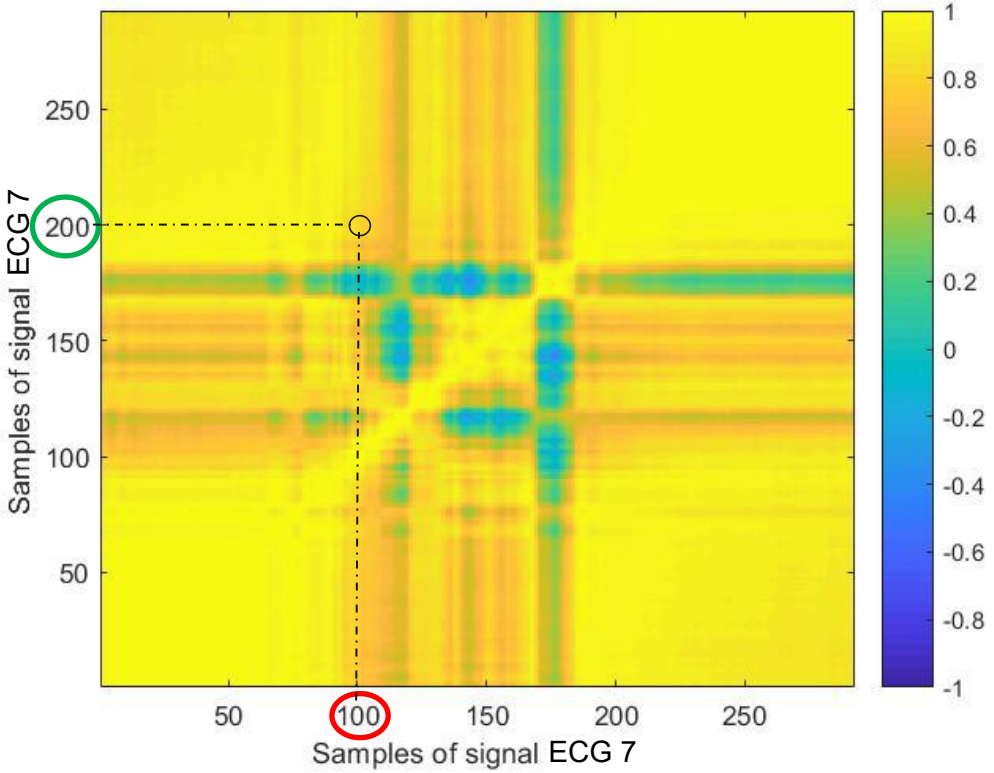


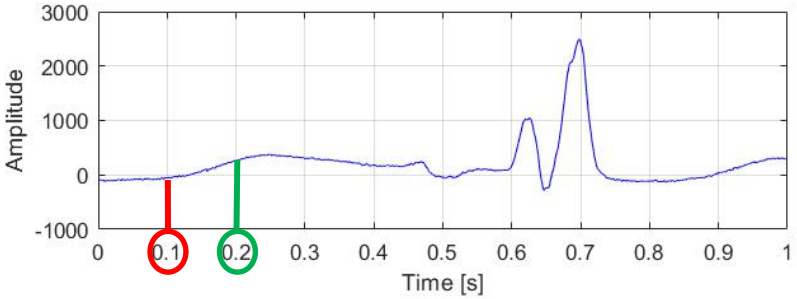
Correlazione spaziale (r)



Caratterizzazione statistica dei segnali

Correlazione temporale (*a*)





Caratterizzazione statistica dei segnali

Per segnali ECG

- alto valore di *r* e di *a*

Analogamente

- per segnali EEG alto valore di *r* e di *a*
- per segnali EMG basso valore di *r* ed alto valore di *a*

Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - ***Stima mutual information rate (MIR)***
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Implicazioni caratterizzazione statistica dei segnali

- Alta correlazione spaziale e bassa correlazione temporale → chiavi segrete "lunghe"
- ECG ed EEG più adatti rispetto ad EMG per la generazione di chiavi segrete
- Entropia significativa e mutua informazione che dipende dallo scenario

Stima mutual information rate

X ed Y segnali biometrici, MIR:

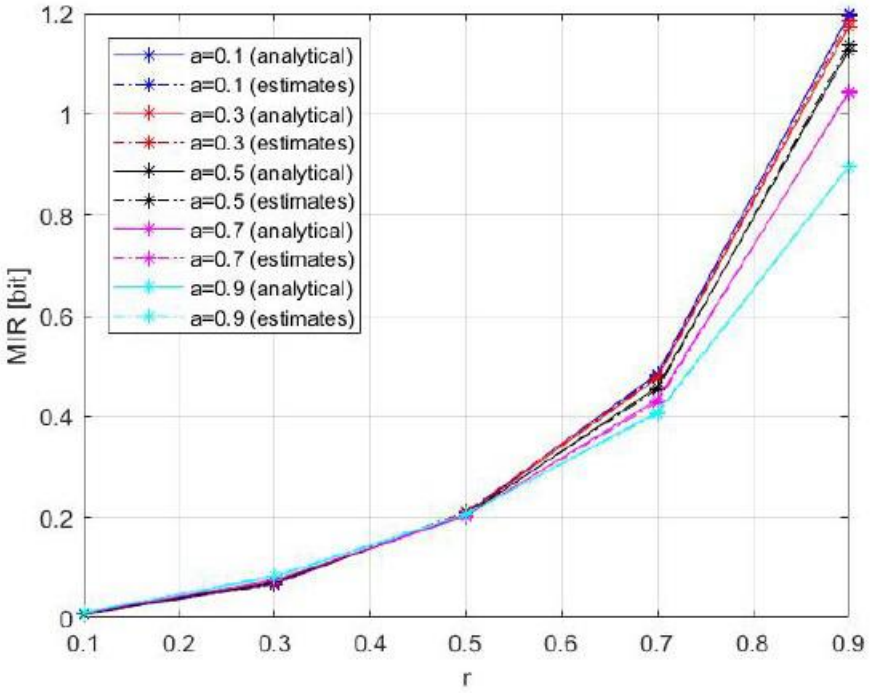
$$I_s(X,Y) = \lim_{K\to\infty} \frac{1}{K} I(x_n, \ldots, x_{n+K-1}; y_n, \ldots, y_{n+K-1}) \leq I(X,Y)$$

Stima del mutual information rate (MIR):

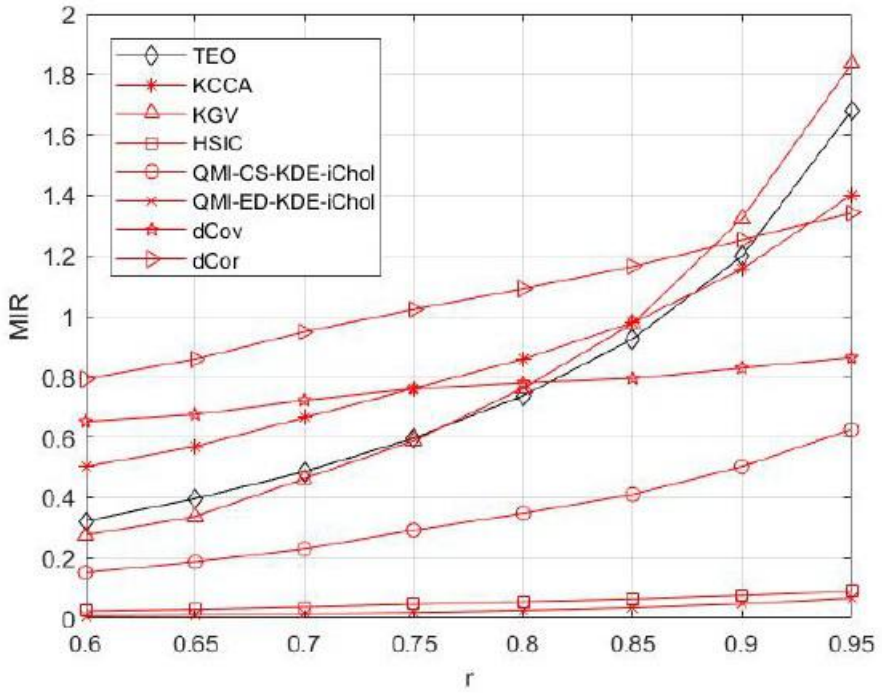
- usando la definizione di entropia differenziale di Shannon
- tramite una valutazione non parametrica basata sui campioni osservati

Stima mutual information rate

Stima tramite entropia differenziale su segnali Gaussiani (K=2)



Stima non-parametrica date le osservazioni su segnali Gaussiani (*a*=0.6 K=2)



Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - ***Valutazione MIR segnali reali***
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Valutazione MIR dati reali

	ch.1-ch.2 KCCA	ch.1-ch.2 KGV	ch.1-ch.2 SvME
K=1	0.0158	0.0098	2.3708
K=2	0.00002	0.00002	5.22
K=3	0.00003	0	3.84
K=4	0	0	2.88
K=5	0	0	2.3
K=6	0	0	1.92

segnali ECG

segnali EEG

	ch.28-ch.31 KCCA	ch.28-ch.31 KGV	ch.28-ch.31 SvME
K=1	0.026	0.0264	2.8123
K=2	0.0004	0.00001	7.96
K=3	0.0001	0.00006	5.54
K=4	0.00005	0.00005	4.15
K=5	0.00004	0.00004	3.32
K=6	0.00003	0.00003	2.77

Valutazione MIR segnali reali

Affidabilità della stima del MIR segnali reali?

Bounds:

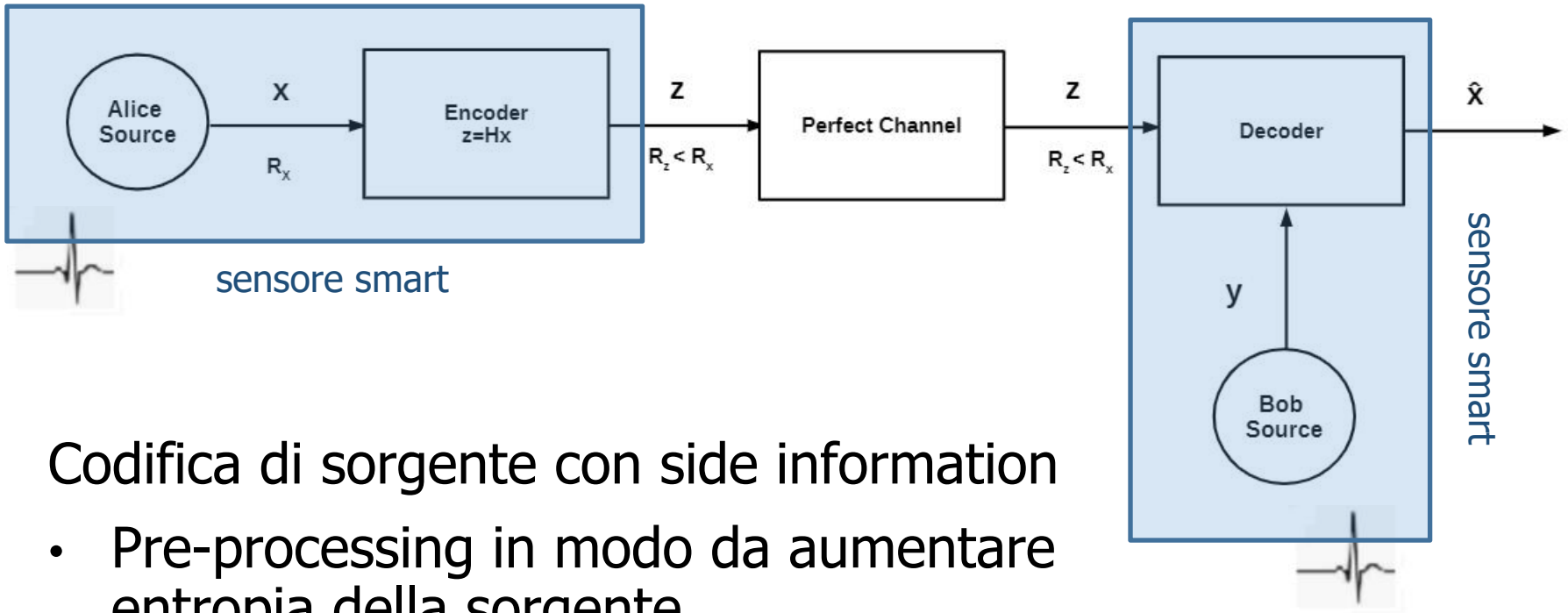
$$\frac{1}{2}\log(|\Sigma|) + \frac{1}{2}(\log(\pi) + 1) \leq I_S(X,Y) \leq I(X,Y)$$

con $\sum$ matrice di covarianza tra X ed Y e π=3.14

Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - ***Implementazione information reconciliation***
- Prospettive future e conclusioni

Implementazione information reconciliation

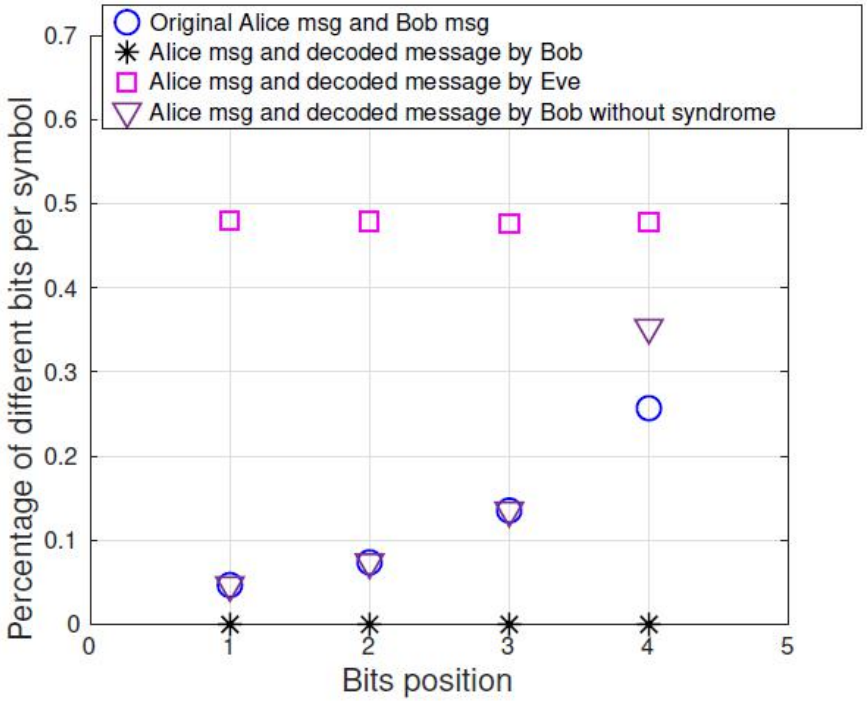


Codifica di sorgente con side information

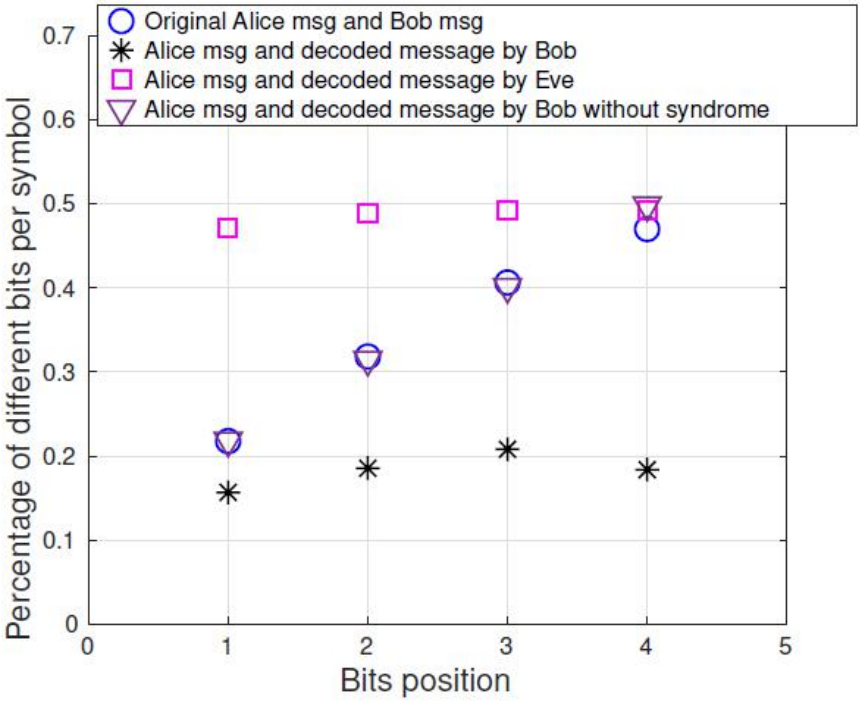
- Pre-processing in modo da aumentare entropia della sorgente
- Codici LDPC con syndrome decoding

Implementazione information reconciliation

Segnali sintetici altamente correlati



Segnali ECG reali



Contenuti della presentazione

- Definizione del problema
- Introduzione agli obiettivi e ai metodi
- Risultati raggiunti
  - *Caratterizzazione statistica dei segnali reali*
  - *Stima mutual information rate (MIR)*
  - *Valutazione MIR segnali reali*
  - *Implementazione information reconciliation*
- Prospettive future e conclusioni

Prospettive future

- **Migliorare information reconciliation** (e.g. LDPC rate e numero di bit in input all'encoder, codici polari)
- **Implementare** uno schema di **privacy amplification**
- Applicazione a **scenario reale** con **smart sensors** commerciali (simulazione e acquisizione di dati fisiologici con sensori off-the-shelf)
- **Confrontare performance** sistema simulato e reale in modo da definire dei **tradeoff** (QoS vs sicurezza)

Conclusioni

- Protocollo **secret-key agreement** in WBAN basato su **segnali biometrici dinamici**
- **Sicurezza by-design** per un sistema **unconditionally secure**
- **Key agreement** sia tra due soli sensori che tra un **gruppo di sensori** della rete
- Estensione ad altri use-case (es., monitoraggio attenzione alla guida, monitoraggio attenzione operai in fabbrica che usano robot/strumentazione rischiosa, etc.)

Grazie per la vostra attenzione!

Contatti:

guglielm@dei.unipd.it
giulia.cisotto@dei.unipd.it