Towards Context Aware 6G Security: New Opportunities and Challenges for Securing the Radio Access

Arsenia (Ersi) Chorti

ETIS UMR 8051, CY Cergy Paris University, ENSEA, CNRS

Wireless World Research Forum 2021, Paris, FR

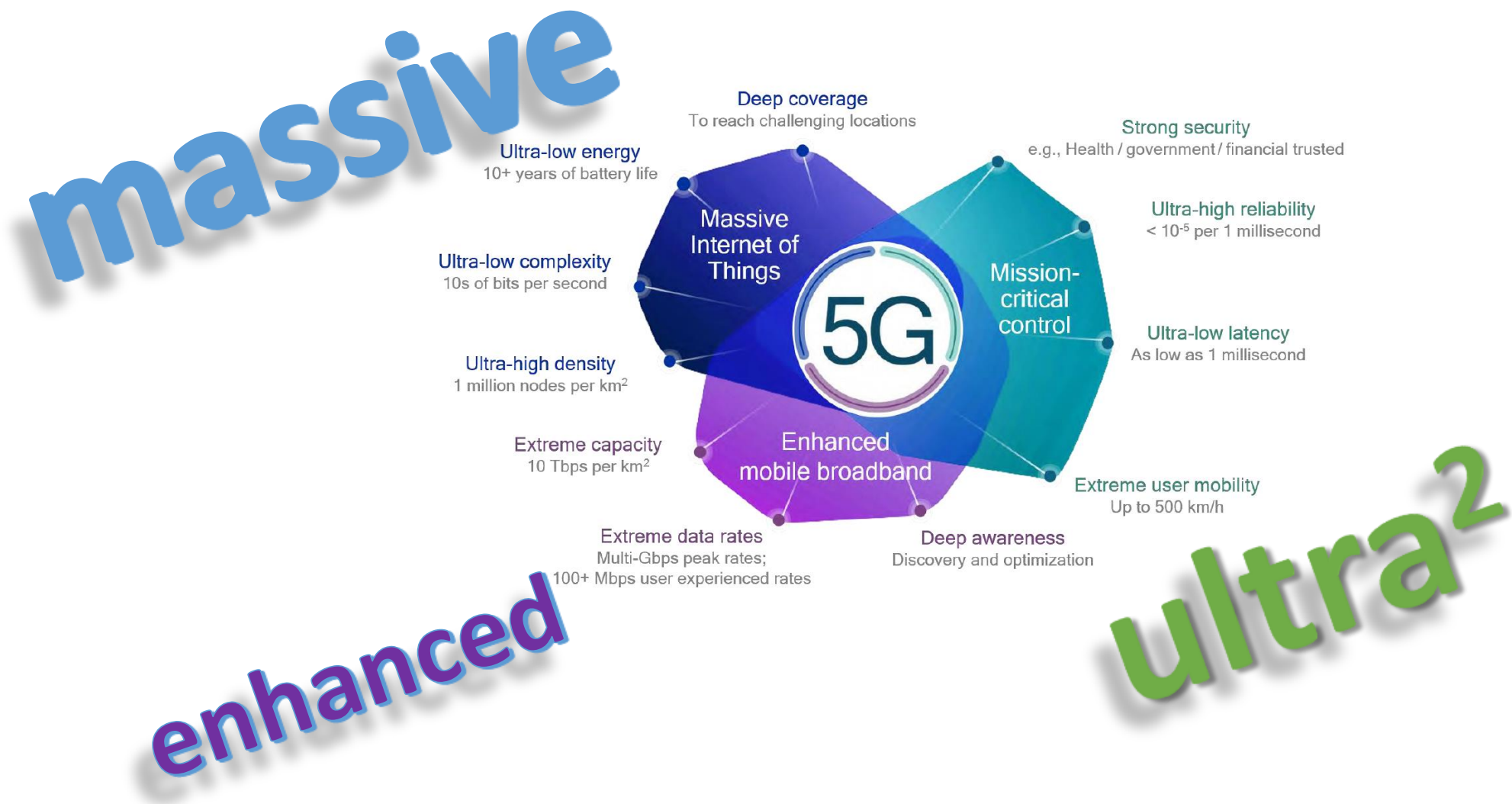
2nd December 2021

Outline

1. 6G security: WHAT are the new challenges? WHY include the PHY?
2. Enabling technologies for the use of physical layer security (PLS) in 6G
3. Examples based on results for authentication, secret key distillation and privacy
4. Conclusions

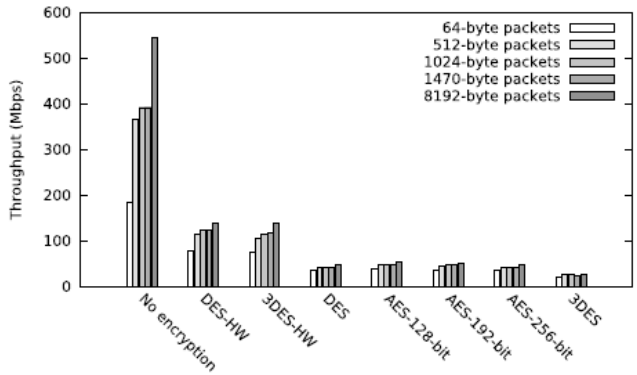
What are the new issues?
Security issues in the B5G evolution...

Securing URLLC and mMTC

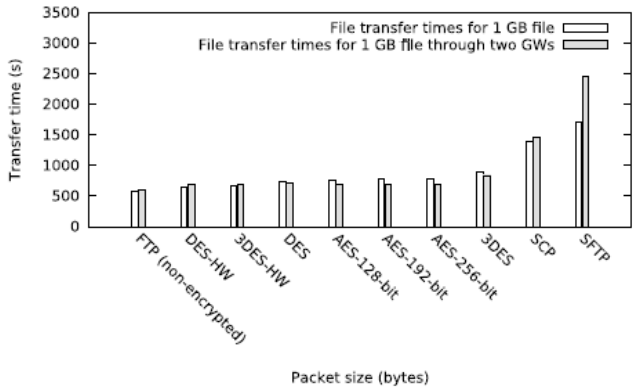


IPSec and (D)TLS for URLLC and mMTC?

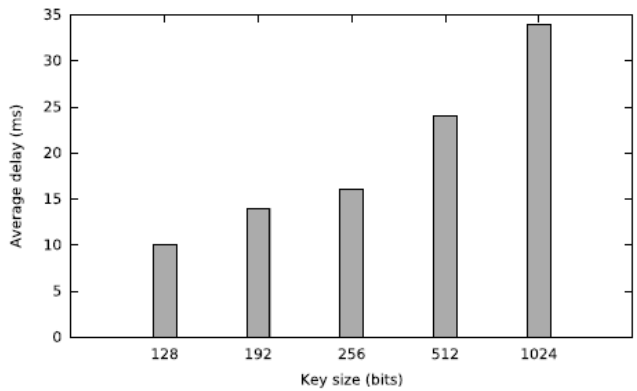
- URLLC security open issues: e.g., $\sim$ 20 msec to verify digital signatures on a vehicle [A. Teniou *et al.*, Security and Privacy, 2018]
- Crypto on constrained IoT devices?



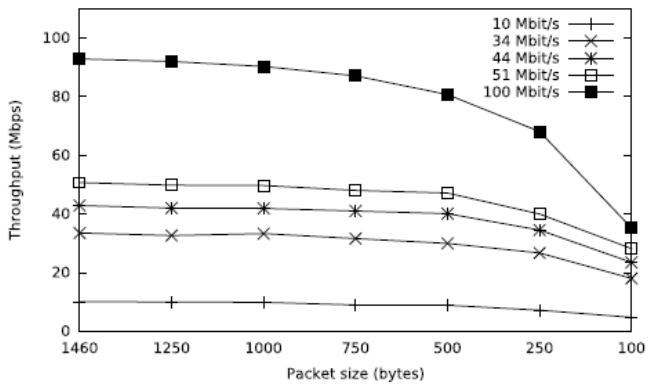
(a) Throughput decreases for stronger cryptographic protocols (e.g., AES > DES).



(b) Transfer time suffers depending on which cryptographic protocol is used.



(c) Average delays for performing cryptographic operations for different crypto-graphic key-sizes in OpenSSL library.



(d) Throughput significantly decreases when IPsec is used for different packet sizes.

[Fadlullah *et al.*, IEEE TWC 2017]

The role of low-end IoT...

Picture taken from BBC News (4th May 2021)

..."He made Belgium bigger and France smaller, it's not a good idea," David Lavaux, mayor of the Belgian village of Erquelinnes, told French TV channel TF1. That sort of move caused a headache between private landowners, he pointed out, let alone neighbouring states...

Other issues

- Quantum computing: popular public key encryption schemes become obsolete
  - Need for lightweight quantum resistant solutions
- Artificial intelligence and machine learning (ML), adversarial ML
- IoT devices produced by many vendors, difficult to normalize

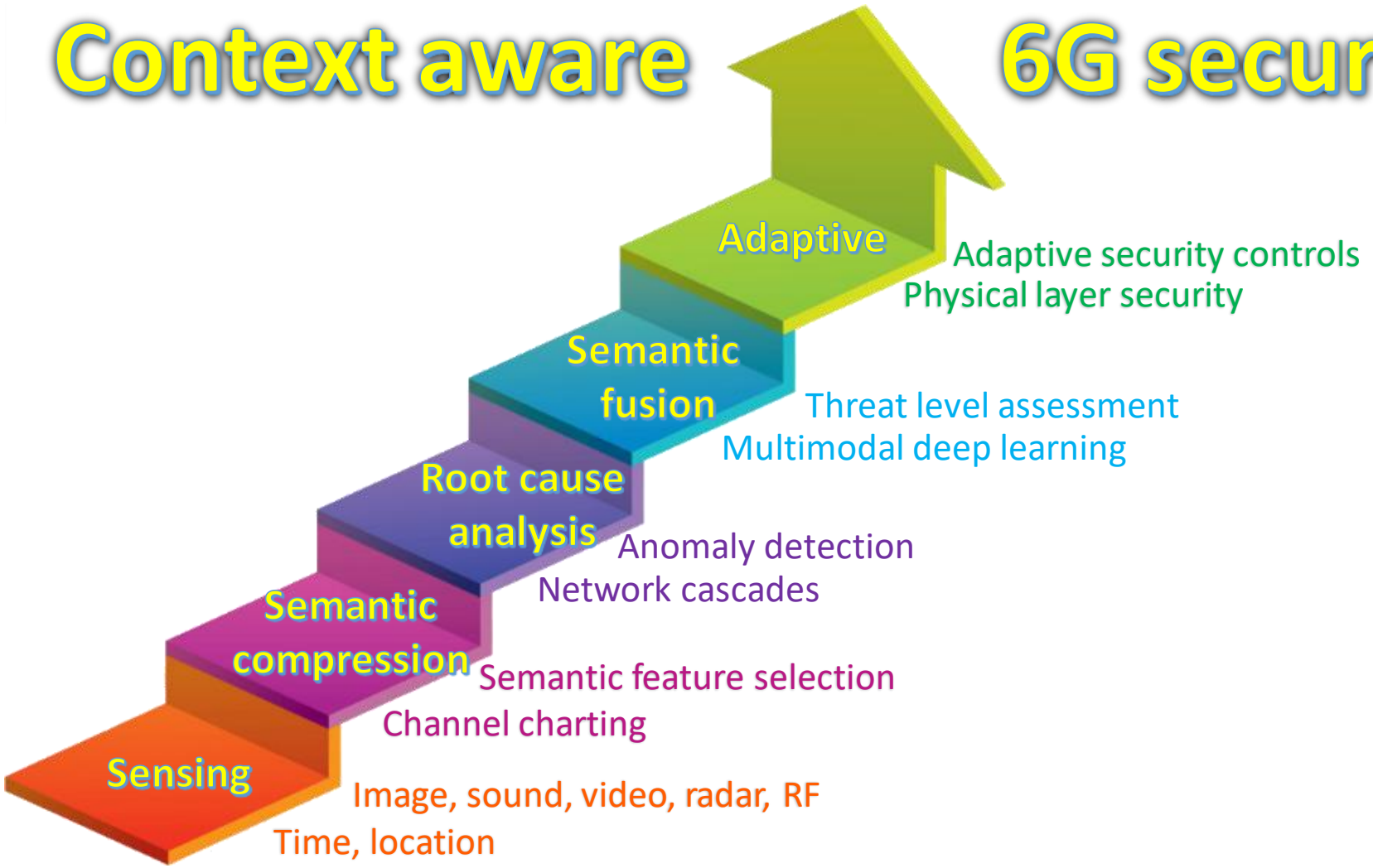
6G security: quality of security (QoSec)

- **QoSec: adaptive security levels**, best effort security
- **Trust! currently zero trust architectures**
  1. How to define other security / trust levels and build adaptive security controls?
  2. How to perform online risk assessment and adaptivity of security controls?

- **Context awareness in cyberphysical systems $\Longrightarrow$ QoSec**

[Chorti, Barreto, Köpsell, Chafii, Sehier, Fettweis, Poor, *Context-Aware Security for 6G Wireless: The Role of Physical Layer Security*, under review at IEEE Std Magazine]

Early proposed roadmap



Physical layer security (PLS) in 6G

PLS technologies of interest for 6G:

1. **Counter-jamming at PHY**, active attacks on PHY
2. **Physical unclonable functions** (PUFs) for device authentication
3. **Localization / RF fingerprinting** as an authentication factor
4. **Secret key generation** (SKG) from shared randomness
5. **Anomaly detection** monitoring hardware
6. **Secrecy codes** for wiretap channels

Why is PLS not included in 5G security standards? Issue 1

First issue: PLS is built on assumptions regarding the adversarial channel conditions, e.g., the secrecy capacity for symmetric channels

$$C_s = [C_m - C_e]^+ \quad (1)$$

$$P_{out}^{(s)} = \mathbb{E}[C_s < \tau] \quad (2)$$

- Many published (celebrated) results rely on specific assumptions regarding the transmission conditions

- Sensing / learning / semantic compression allow overcome this
- In 6G **channel will be learned online (location based)** change approach: instead of channel models, let the data speak!

Why is PLS not included in 5G security standards? Issue 2

Second issue: at finite blocklengths PLS cannot provide guarantees for zero information leakage

- **Can provide privacy guarantees! Pertinent for QoSec**
- Connections with local differential privacy

Why is PLS not included in 5G security standards? Issue 3

Third issue: PLS compromises transmission rates

- No need for high rates! No need for target 0.5 bits/sec/Hz
- Use PLS to distil / distribute keys
- **Hybrid PLS / symmetric crypto systems**: keys can be re-used (256 key bits suffice for roughly a Gigabyte of data)

Added advantage: PLS is trully adpative adjust secrecy outages depending on QoSec level

$$P_{out}^{(s)} = \mathbb{E}[R_s < \tau] \tag{3}$$

Joint Node Authentication and Secret Key Generation

with Drs. Muralikrishnan Srinivasan, Sotiris Skaperas, Mahdi Shakiba Herfeh

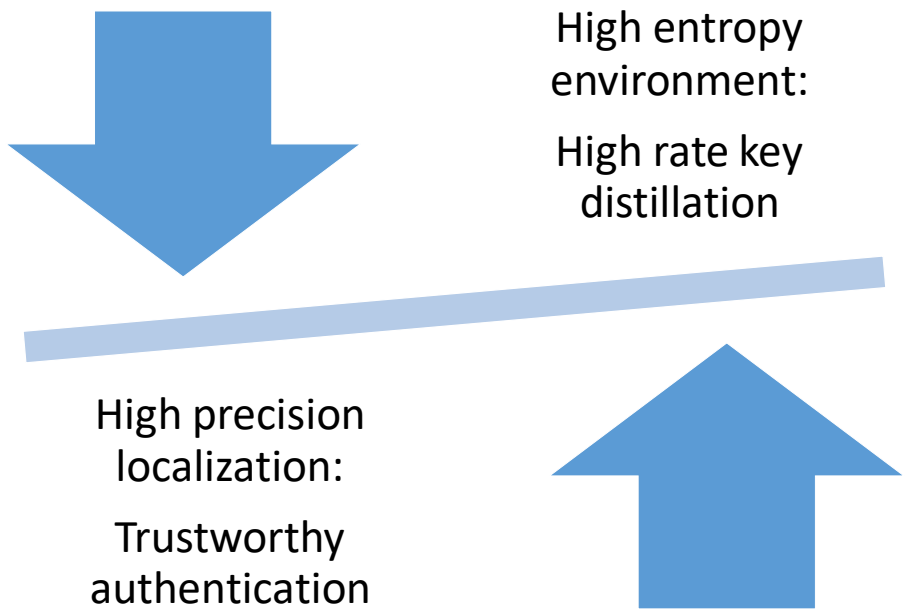


projects: SAFEST (DIM RFSI with Nokia Bell Labs)
ELIOT (ANR PRCI with Univ. Sao Paolo and PUC Rio)
eNiGMA (CYU INEX), PHEBE (CYU INEX)

The dual role of the wireless channel

Wireless coefficients can be used for:

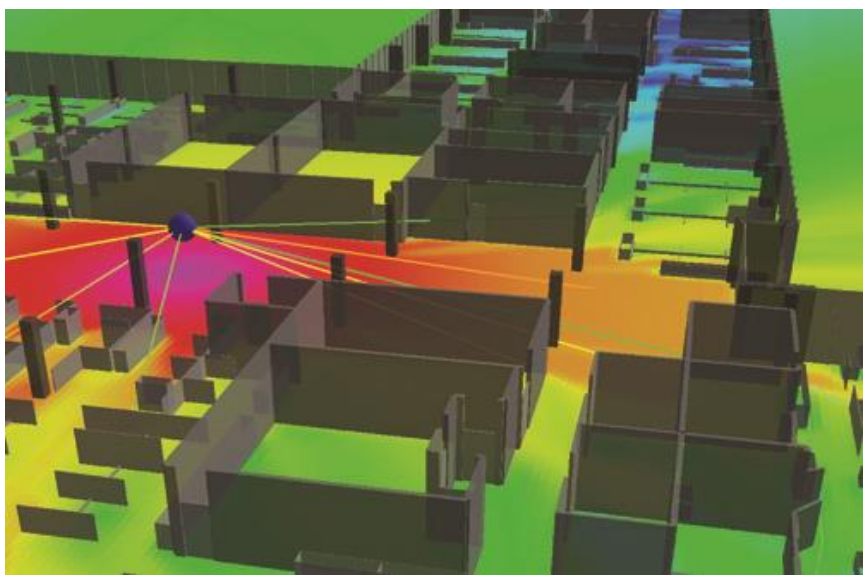
1. Authentication through RF fingerprinting / localization;
2. Symmetric secret key generation (SKG), $\Longrightarrow$ Tx and Rx distil keys from "shared" randomness



Authentication

- *Large scale fading*, i.e., path loss and shadowing
- Related to positioning in a given (static) environment
- Largely predictable can be treated as a source of *uniqueness*

- Key point: need to be able to extract different authentication keys at different locations, separability and reproducability is important

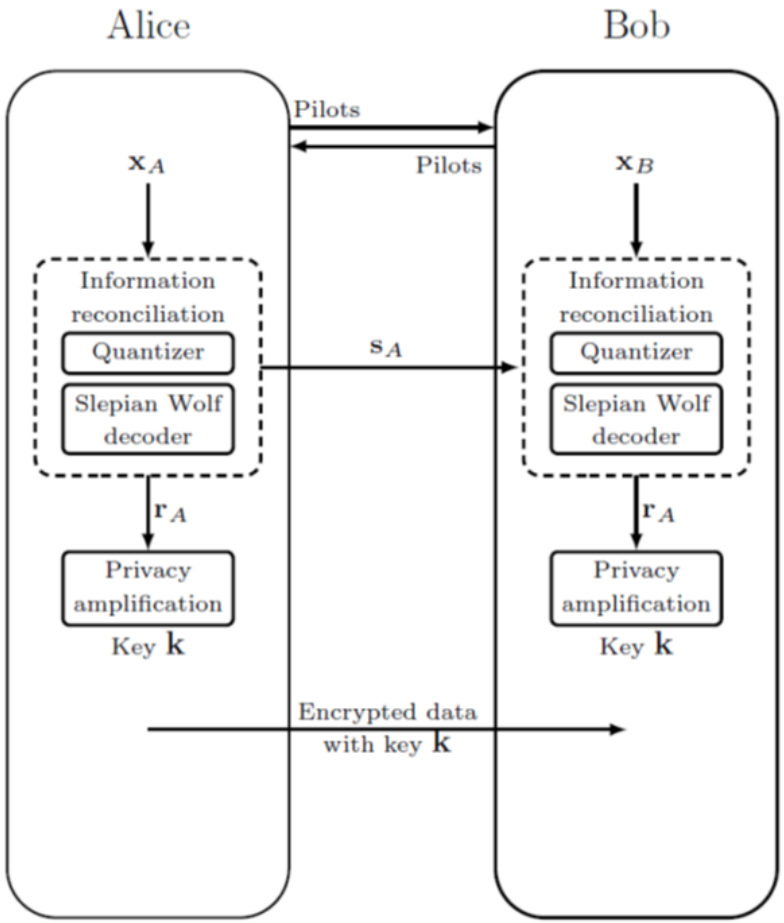


- *Small scale fading* are random variations in channel state information (CSI)
- Treated as a **source of *entropy*** to distil keys from shared randomness

- Concept of "**unpredictability**" is important
- Semantic security: a pseudorandom number generator is "unpredictable" if it can resist next bit predictors

- Straightforward criterion of unpredictability: **independence**

SKG fundamentals



- Quantizer outputs $\mathsf{r}_A = \mathsf{d} \oplus \mathsf{e}_A, \mathsf{r}_B = \mathsf{d} \oplus \mathsf{e}_B$
- Reconciliation: reconstruct r_A from r_B as $\mathsf{r}_A = \mathsf{r}_B \oplus \mathsf{e}_B \oplus \mathsf{e}_A$
  - Channel reciprocity between Tx and Rx: TDD
  - Temporal / spatial / frequency independence

Key goals and methods

1. Disentangle predictable / unpredictable components using *unsupervised learning (PCA / autoencoders (AE))*
   - AE design from trade-off between spatial correlation (SC) between locations and reciprocity between the uplink and downlink components used for SKG

2. Evaluate separability of RF fingerprints in terms of *total variation distance (TVD)* for node-authentication

3. Ongoing work: use (spatial) independence *d-variable Hilbert-Schmidt independence criterion (dHSIC)*

System model

- Quadriga channel models @2.68 GHz
- Single-antenna legitimate nodes and base station (Bob)
- Alices' spatial locations $\{\mathsf{x}_n\}_{n=1}^{N} \in \mathbb{R}^L$ $n = 1, \ldots, N = 400$ where $\{\mathsf{x}_n\}_{n=1}^{N}$ (typically $L = 2$), on a square grid
- $M \times 1$ CSI vectors $\{\boldsymbol{h}_n\}_{n=1}^{N}$ denoted by $\mathcal{H} : \mathbb{R}^L \to \mathbb{C}^M$, where $M = 128$ snapshots in the time domain

Extrapolation of fingerprints using PCA

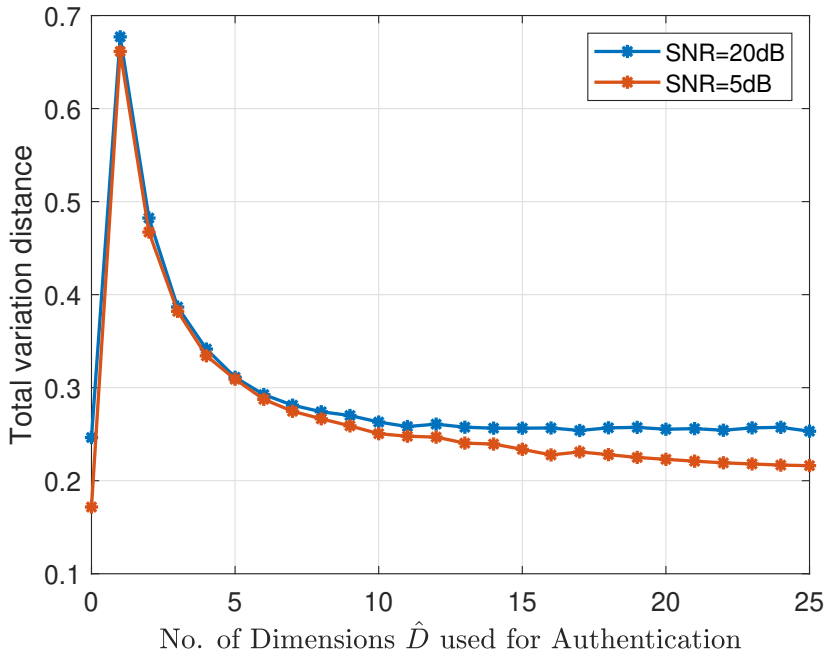
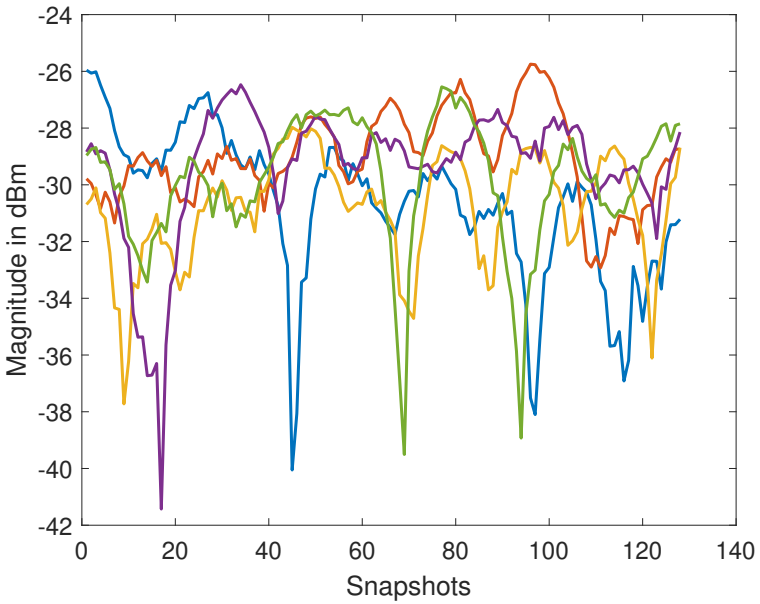


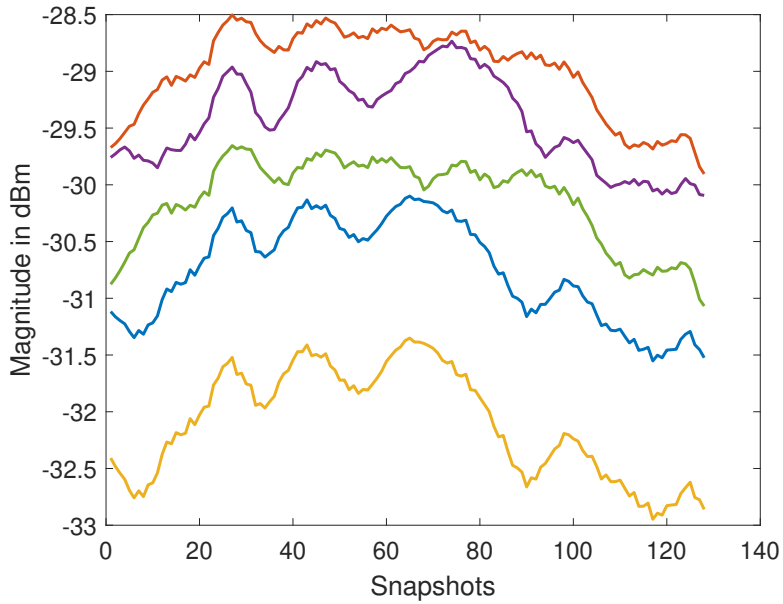
Figure: Total Variation Distance vs $\widehat{D}$

- Picking only the first PCA component provides Alice's best separation from her neighbours based on TVD

Example



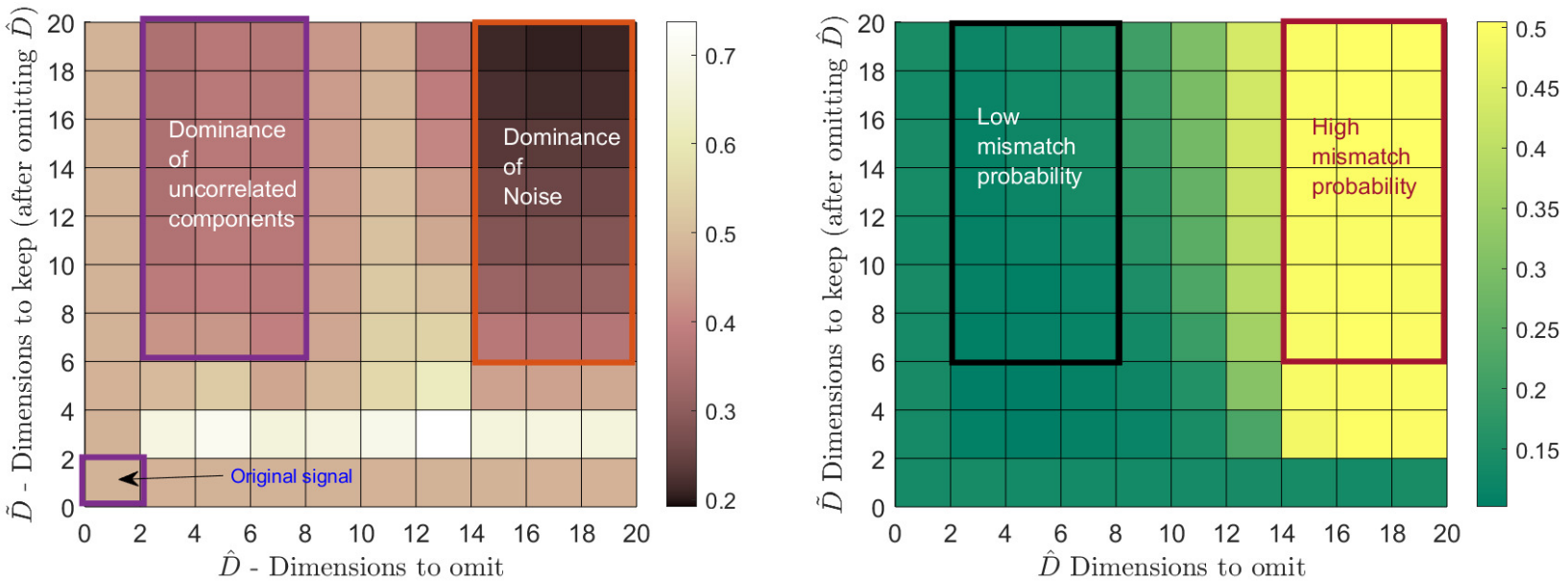
(a) Original signals



(b) Predictable components

Figure: Separability of 6 neighbours for the original signal and the predictable component with $\widehat{D} = 1$ for SNR$=$ 20 dB

Extrapolation of reciprocal and uncorrelated components using PCA

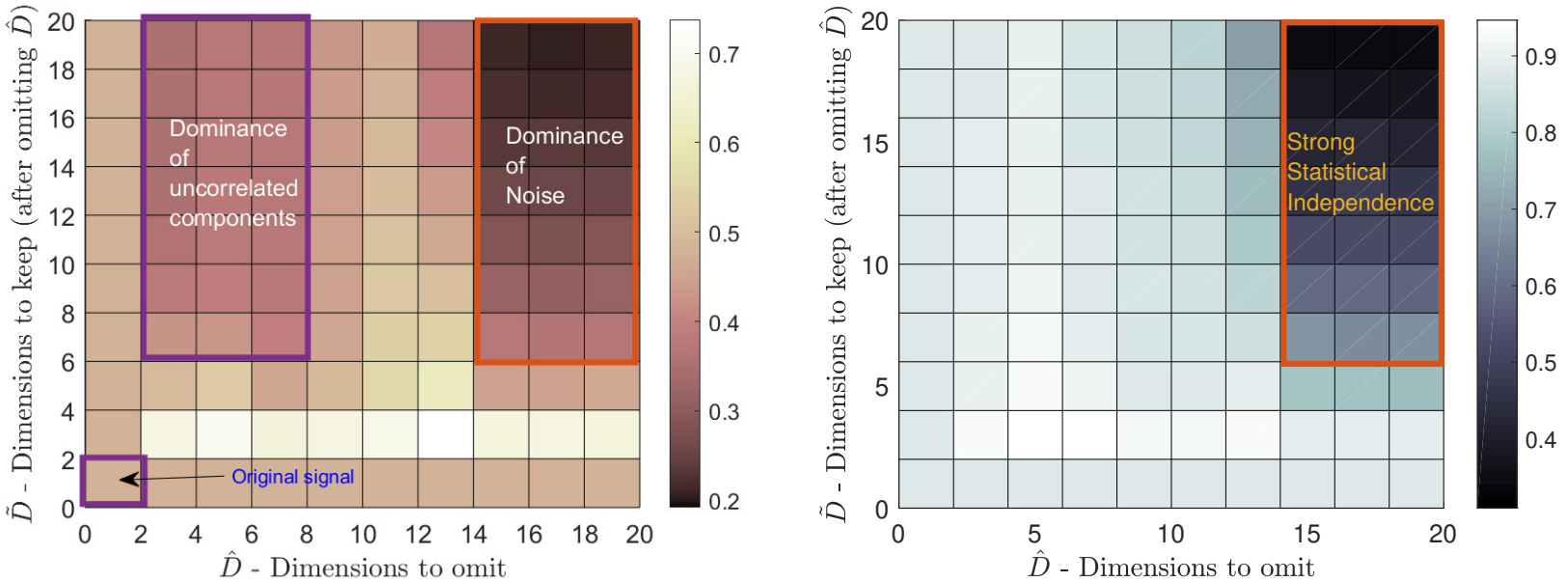


(a) Average CC

(b) Average MP

Figure: Variation of average correlation coefficient (CC) between the locations and their nearest neighbours and the average mismatch probability (MP) between the Alices and Bob, respectively, with respect to the variation in the pair $\{\widehat{D}, \tilde{D}\}$ in steps of 2 for SNR $= 20$ dB

But...



(a) Average CC

(b) Average value of the *dHSIC*

Figure: A trend disimilar to CC is observed in the average *dHSIC* values; independence only for higher values of the pair $\{\widehat{D'}, \tilde{D}\}$ (in the regime "Statistical Independence")

Ongoing work

- Real dataset
- Incorporate dHSIC as the loss function of AE
- Kernel PCA and autoencoders
- Online evaluation of channel statistics

Take away points

- **Securing RAN**: first line of defence for 6G
- **PLS enabled by sensing and AI**: towards context aware security
- **Authentication and key distillation from unsupervised learning**: PCA and AE

IEEE PLS focus group: lay the groundwork for a standardization working group

Steering committee: A. Chorti, A. Yener, M. Bloch, E. Hamad,

Members: Ashutosh Dutta, Parthajit Mohapatra , Pin-Hsun Lin, Muralikrishnan Srinivasan, Vince Poor, Mahdi Shakiba, Nikolaos Pappas, Stefan Köpsell, Marco Baldi, Linda Senigagliesi, Sennur Ulukus, Stefano Tomasin, Rafael, Schaefer, Himanshu Tyagi, Hua Wang, Miroslav Mitev, Jay Prakash, Laura Luzzi, Camilla Hollanti, Eduard Jorswieck, André Noll Barreto, Paul Walther, Muhammad Karam Shehzad

Presented results appear in

1. A. Chorti, A. Noll Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, H.V. Poor, "Context Aware 6G Security, The Role of Physical Layer Security" (major revisions) in IEEE Communications Standards Magazine
2. M. Srinivisan, S. Skaperas, A. Chorti, "On the Use of CSI for the Generation of RF Fingerprints and Secret Keys", in Proc. WSA, Nov. 2021.
3. M. Shakiba Herfeh, A. Chorti, "Comparison of Short Blocklength Slepian Wolf Coding for Reconciliation", in Proc. IEEE SSP, Jul. 2021.
4. M. Shakiba Herfeh, A. Chorti, V.H. Poor, A Review of Recent Results on Physical Layer Security, Springer Nature Jan. 2021.

Thank you!

arsenia.chorti@ensea.fr

Extra slides

Anomaly detection
Centralized and distributed lightweight detection

with G.A.N. Segura and Dr. Cintia Margi

project ELIOT (ANR PRCI with Univ. Sao Paolo and PUC Rio)

Anomaly Detector Using Change Point Theory

Monitor times series for changes in the mean or variance (windows $m = 200$ samples)

Statistical hypothesis test

$$H_0: \quad \mu_1 = ... = \quad \mu_N$$

$$H_1: \quad \mu_1 = \ldots = \mu_{k^*_{off}} \neq \mu_{k^*_{off}+1} = \ldots = \mu_N$$

On-line test statistic $TS_{on}(m, l)$ and threshold $F(m, l)$ => stopping time $\tau(m)$:

$$\tau(m) = \begin{cases} \min\{l \in \mathbb{N} : TS_{on}(m, l) \geqslant F(m, l)\}, \\ \infty, \text{ if } TS_{on}(m, l) < F(m, l) \ \forall l \in \mathbb{N}, \end{cases}$$

On-line CP analysis

- **Test statistic**

$$TS_{on}(m,k) = \frac{1}{\widehat{\Omega}_m}\left(\sum_{i=m+1}^{m+k} X_i - \frac{l}{m}\sum_{i=1}^{m} X_i\right)$$

- **Threshold function**

$$F(m,l) = cv_{on,\alpha}\left(1+\frac{l}{m}\right)\left(\frac{l}{m+l}\right)^{\gamma}, \gamma \in [0,1/2)$$

  - $cv_{on,\alpha}$: derived from the test statistic under H_0 as $m \to \infty$
  - $\lim_{m\to\infty} P\{\tau(m) < \infty | H_0\} = \alpha$, i.e., probability of false alarm asymptotically bounded by α
  - γ: captures trade-off between agility and detection rate

Intrusion detection in IEEE 802.15.4 SD-WSN

SD-WSN network with 36 and 100 IEEE 801.15.4 Tmote sky nodes
Two types of attacks: false flows, false neighbor info

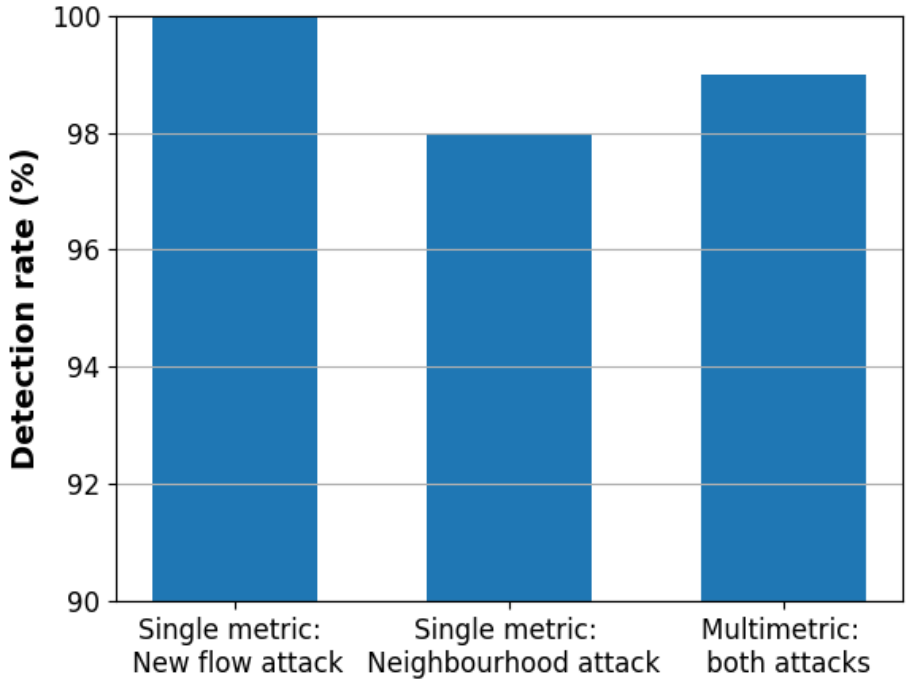
Centralized detection

- Centralized security module on the controler
- Monitor: (i) control overhead (ii) data packets delivery rate
- **Multi-metric** detection

Distributed detection

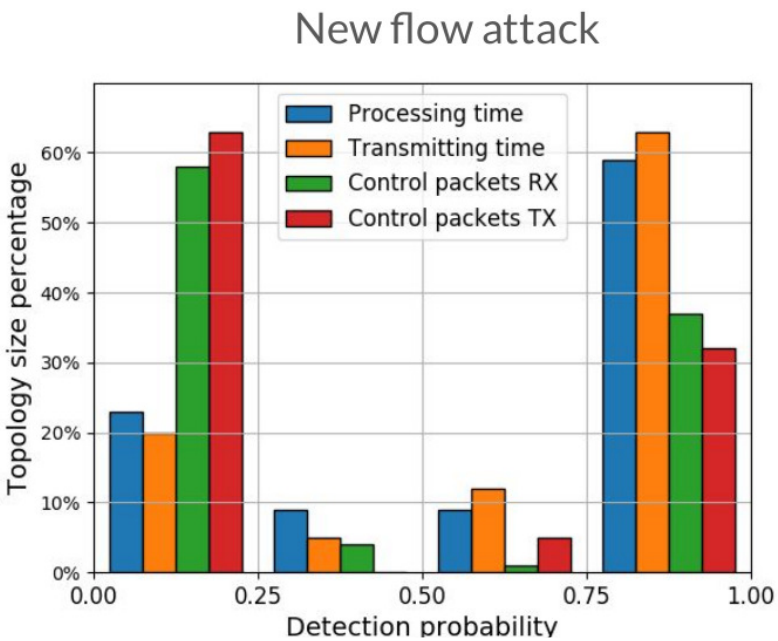
- **Every node** runs a change point detector
- Nodes send alerts to security module

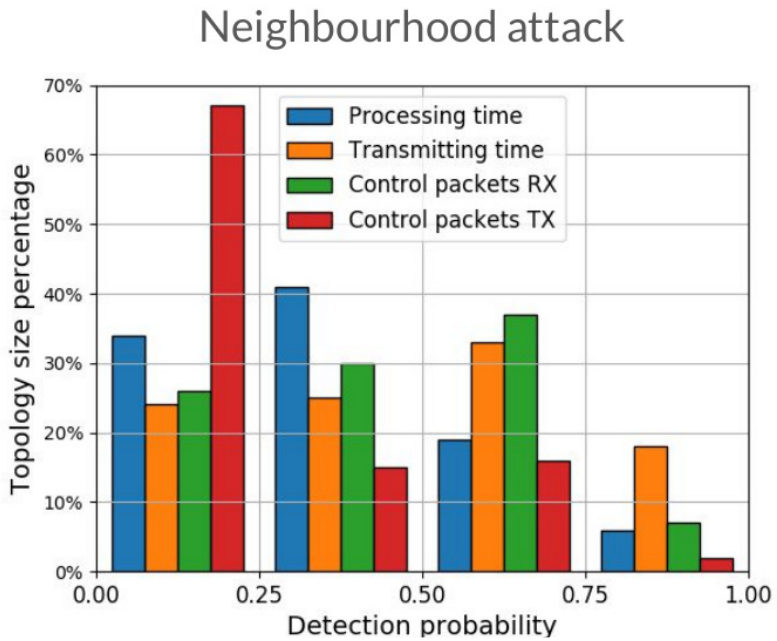
Centralized detection



- Tune sensitivity parameter γ for either agility or precision
- Generic detection rate $> 98\%$
- Type of attack identification rate $> 89\%$

Distributed detection

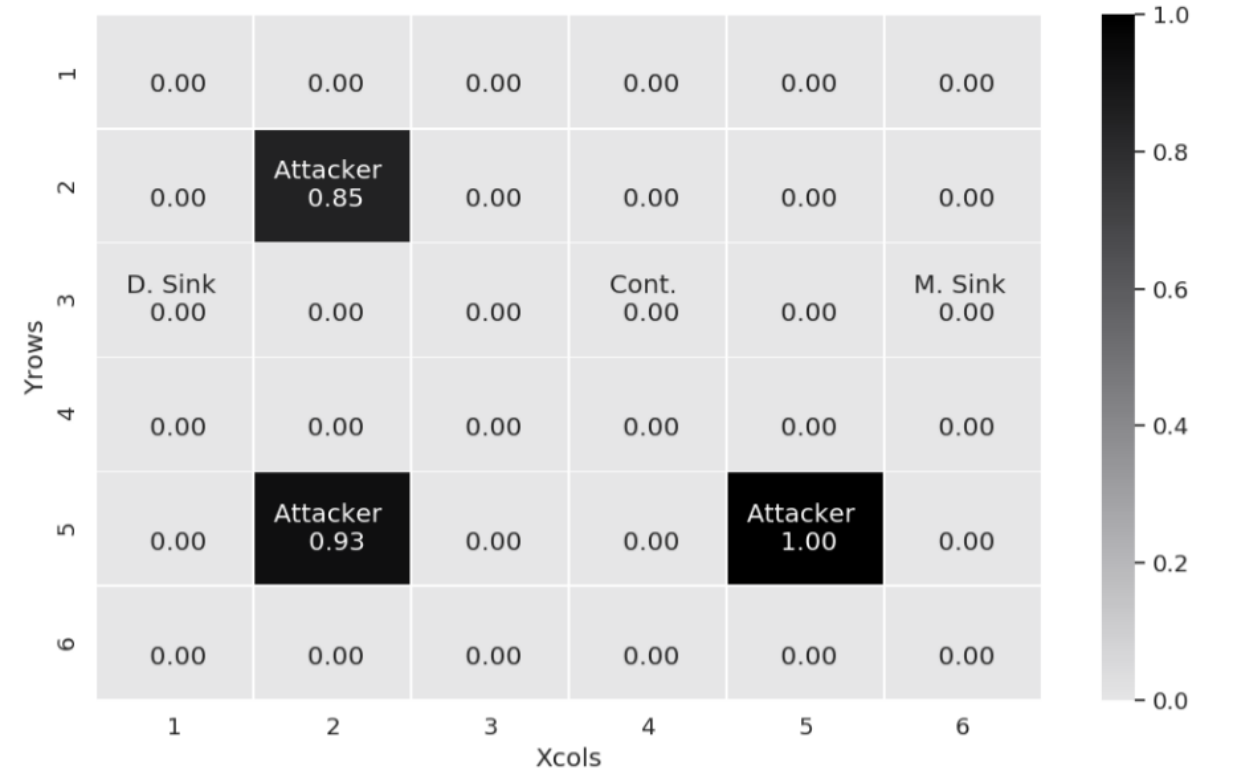




- **New flow attack:** $> 70\%$ detection rate for $> 50\%$ of nodes
- **Neighbourhood attack:** $> 50\%$ detection rate for $> 30\%$ of nodes

Distributed detection: attacker identification

- Individual nodes send alerts to a centralized security module
- Security module matches individual alerts and topology information



Identification probability