Physical Layer Security in a 5G Setting

G. Wunder R. Fritschek R. Khan
Freie Universität Berlin
http://www.mi.fu-berlin.de/en/inf/groups/ag-comm/index.html

in cooperation with Francois Delaveau, Christiane-Laurie Kmeni Ngassa
(both Thales Group, France)

Outline

5G Project Landscape

The Wiretap Scenario - Secrecy Coding & Secret Key Generation

Advanced SKG Setting: Secret keys 'on the fly'

6Doku Demonstrator

Conclusions

Outline

5G Project Landscape

- 5G PPP Phase 1: started July 2015
  - Involved (as PMT): Fantastic-5G ('the' new air interface project beyond LTE)
  - Website: www.fantastic5g.eu
  - Close collaboration with mmMAGIC (>6GHz), 5G NORMA (5G architecture)
  - Altogether 18 projects in first phase
  - All major vendors (Ericsson, Nokia, Huawei etc.) and operators (Orange, DT, TI etc.) involved
- 5G PPP Phase 2: Call Nov. 2016 with 100 Mill Budget!
- Current major events:
  - Workshops at IEEE ICC, IEEE Globebom, EuCNC (EC ICT Flagship)
  - Press releases, IEEE Magazine papers
  - Active in 3GPP Standardization (but very different view in ASIA, USA, and Europe)

5G Security

- Security: 5GPPP '5GEnsure'
- Reference project in 5GPPP for 5G security, privacy and trust
- Produce a 5G security architecture and use cases
- Initial Set of security enablers
- Mainly core network related procedures
  - IoT enablers for AAA
  - Improved identity protection (IMSI, UICC, (V)MNOs etc.)
  - Trust builders, metrics, VNF certification
  - Network virtualization isolation
  - Monitoring tools (access control, bootstrapping etc.)
  - ...

Phase II

- Open consultation on 5G security among stakeholders:
  - Faster handling of security procedures for extremely low latency application
  - Data authenticity, confidentiality and integrity for resource-constrained dives
  - Seamless authentication over multiple devices, access networks, services
  - Protection against DOS attacks to core and radio
  - Security mechanisms for NFV infrastructure
- Remedies (particularly privacy/security trade-offs):
  - Secret sharing (no single point of trust and failure)
  - Practical homomorphic encryption
  - Privacy-preserving profiling
  - IoT: Lightweight encryption
  - IoT: PuFs
  - IoT: Physical layer security

Physical Layer Security: Approaches

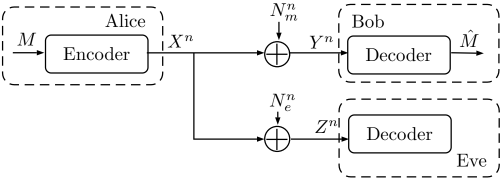
Definition: Physical Layer Security

Security is handled on PHY layer by exploiting PHY layer parameters (e.g. channel, noise, ...) and controlled (of course) by MAC protocol.

- Advantages:
  - Faster procedures: Algorithms run on PHY/MAC level, no packets are given to higher layers
  - Scalable
  - Energy/computation-efficient with lightweight ciphers
  - Improved usability
  - Improved security
  - The 'radio advantage'
  - ...
- Approaches:
  - Secrecy coding
  - Secret key generation
  - Secure pairing

Outline

The Wiretap Scenario



- Alice wants to communicate a message M via X to Bob, and Bob receives $Y = X + N_m$
- But a Wiretapper can see the message through another channel e
- The wiretapper Eve receives $Z = X + N_e$
- Question: Can Alice communicate secretly to Bob?

Secrecy Coding

Definition: Secrecy Capacity

For a $(2^{nR}, n)$ code $\mathcal{C}_n$, which is known by Alice, Bob and Eve

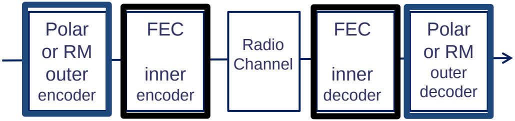
- Code rate: $\frac{1}{n}H(M) = R + \delta$
- Reliability measure: $P_e(\mathcal{C}_n) = \Pr[M \neq \hat{M}|\mathcal{C}_n]$
- Secrecy measure - Equivocation: $H(M|Z^n, \mathcal{C}_n)$ (as high as possible)
- Secrecy measure - Information leakage: $I(M; Z^n|\mathcal{C}_n)$ (as low as possible)

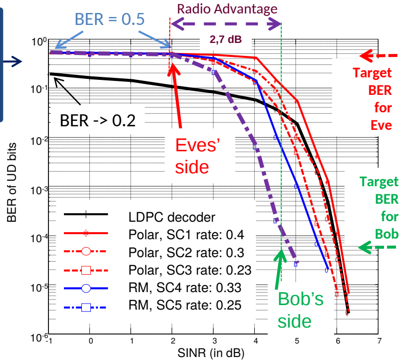
Wyner 75′, Csizar and Körner 78′

$$C_s(P_{YZ|X}) = \max_{P_{UX}}[I(U;Y) - I(U;Z)] \geq \max_{P_X}[I(X;Y) - I(X;Z)]$$

Intuitively: Alice uses 'radio advantage' over Eves channel to send 'perfectly' secured messages to Bob

SC: How to use the Advantage?





- Use concatenation of two codes
- Inner Forward-Error-Correction code (FEC) for sufficient error correction (e.g. LDPC)
- Outer secrecy code to use the advantage of Bob (Polar or Reed-Muller code)
  - Outer code is partitioned into several parts ranked for channel goodness; Good parts are used for information transfer, Eve just gets bad parts

Secrecy Coding - Challenges

- However: SC based on better Channel to Bob

Question 1: Is this a practical requirements?

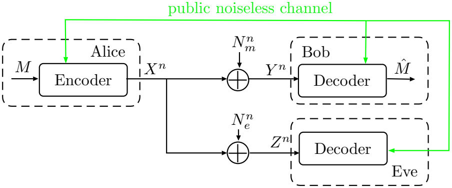
$\rightarrow$ No "warranty" for Alice-to-Bob "radio advantage"!

Question 2: What can we do if Eve got the better channel?

Several other approaches exist to bring physical layer security into practice

- For example:
  - Jamming / alignment strategies [ISIT16-Paper]
  - Channel reciprocity based secret key generation (SKG) schemes [PIMRC16-Paper]

The Wiretap Scenario with Public Discussion



- Public Discussion can be used to transform the channel
- New channel meets previous requirements for Eve
- Paradigm shift: From secrecy capacity to secret key rate

Freie Universität Berlin

Secret Key Generation

Definition: Secret Key Rate

A secret key rate R_s is said to be achievable (for all $\epsilon > 0$) if

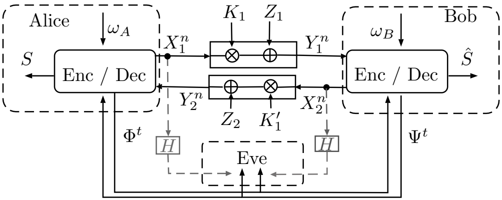
- Alice and Bob agree on the key: $P\{S \neq \hat{S}\} \leq \epsilon$
- While keeping Eve in the dark: $\frac{1}{n} I(S; \text{Eve}) \leq \epsilon$
- But still achieving a key rate: $\frac{1}{n} H(S) \geq R_s - \epsilon$

Maurer, Ahlswede and Csiszar 93′

$$I(X;Y) - \min(I(X;Z), I(Y;Z)) \leq C_s \leq \min(I(X;Y), I(X,Y|Z))$$

Even if Eve got the better channel, using a public channel can ensure secrecy!

Two-way Secret Key Generation



Instead of Secrecy Coding:

- Use two-way communication for key generation and exploit channel entropy
- "Generate" source of common randomness at both terminals
- Extract secret key from common randomness

SKG: Channel reciprocity based key generation

- Fact: Channel gain K_1, K_1' at Alice and Bob is a highly correlated random variable $K_1 \approx K_1'$ (random: due to fading)
- Idea: Send pilot signals and measure the channel gain at Alice and Bob

How to get a key?

- Measured signals get quantized at both terminals
- Alice and Bob reconcile via Public Discussion to agree on a key
- Reconciliation can be done such that Eve gains no knowledge of the key
  - Example: Difference of both msg's viewed as "channel noise impairment"
  - Error correction codes can be used: Alice calculates parity Bits; sends them to Bob so that Bob can reconstruct the same measurement

Drawback:

- Dependent on channel gain randomness: static scenarios yield less key rate

Outline

SKG: Using Local Sources

Channel Model:

$$Y_B = KX_1 + Z_1$$
$$Y_A = KX_2 + Z_2$$

- X_1, X_2 are send codewords and K is the channel gain
- Bob has access to $(KX_1 + Z_1, X_2)$ and Alice to $(KX_2 + Z_2, X_2)$
- Ahlswede & Cszizar: Keyrate $= I(Y_A, X_2; Y_B, X_1)$ (no side-info at Eve)

But

- What is the key rate?
- How to achieve it in practices?
- What about side-information at Eve?

Theorem

The Key-rate for local and global randomness sources is split up in contributions from both.

$$
\begin{aligned}
&I(Y_A, X_1; Y_B, X_2) \\
&= I(X_1; Y_B) + I(Y_A; X_2) + I(Y_A; Y_B | X_2, X_1)
\end{aligned}
$$

- $I(X_1; Y_B)$, $I(Y_A; X_2)$ is the capacity for a non-coherent fading channel
- $I(Y_A; Y_B | X_2, X_1)$ is the key rate for the channel gain randomness conditioned on the input signals
  - Therefore: Exactly the standard achievable key rate!
- Result: Using local and global sources has a positive effect on key rate

SKG: Using Local Sources

Theorem

With input $X_1, X_2 \sim \mathcal{N}(0, P)$, *channel gain* $K \sim \mathcal{N}(0, \sigma_K^2)$ *and noise or estimation error* $Z_1, Z_2 \sim \mathcal{N}(0, \sigma_Z^2)$ *it holds that*

$$
\begin{aligned}
& I(Y_A, X_1; Y_B, X_2) \\
& \geq E_K[\log(1 + \tfrac{|k|^2 P}{\sigma_{\bar{Z}}^2})] \\
& \quad - \tfrac{1}{2} E_{X_1}[\log(1 + \tfrac{|x_1|^2 \sigma_K^2}{\sigma_{\bar{Z}}^2})] - \tfrac{1}{2} E_{X_2}[\log(1 + \tfrac{|x_2|^2 \sigma_K^2}{\sigma_{\bar{Z}}^2})] \\
& \quad + \tfrac{1}{2} E_{X_1, X_2}\left[\log\left(1 + \frac{x_1^2 x_2^2 \sigma_K^4}{(x_1^2 + x_2^2)\sigma_K^2 \sigma_{\bar{Z}}^2 + \sigma_{\bar{Z}}^4}\right)\right]
\end{aligned}
$$

However: No hint on how to achieve it!

Suppose the channel noise is zero:

$$Y'_B = KX_1$$
$$Y'_A = KX_2$$

- Bob has access to (KX_1, X_2) and Alice to (KX_2, X_2)
- Idea: just multiply it, Key$= KX_1X_2$

Noisy channel:

- Ahlswede & Cszizar: Keyrate $= I(Y_AX_1; Y_BX_2)$

But

- Sub-optimal: $I(Y_AX_1; Y_BX_2) \leq I(Y_A, X_2; Y_B, X_1)$ (Due to Fano's Ineq.)
- Hard to actually calculate $I(Y_AX_1; Y_BX_2)$

SKG: lates news - connection to bit vectors

Lets look at $I(Y_A X_1; Y_B X_2)$ and approximate it!

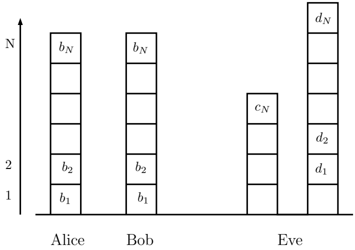
$$Y_B X_2 = K X_1 X_2 + X_2 Z_1$$
$$Y_A X_1 = K X_2 X_1 + X_1 Z_2$$

- Assume that $K = 2^N k$ with $N \in \mathbb{N}$ and $k \in [1, 2)$
- Also assume peak power constraints on X_1, X_2 and Z_1, Z_2 of 1.

$$Y_B X_2 = 2^N k X_1 X_2 + X_2 Z_1$$
$$Y_A X_1 = 2^N k X_2 X_1 + X_1 Z_2$$

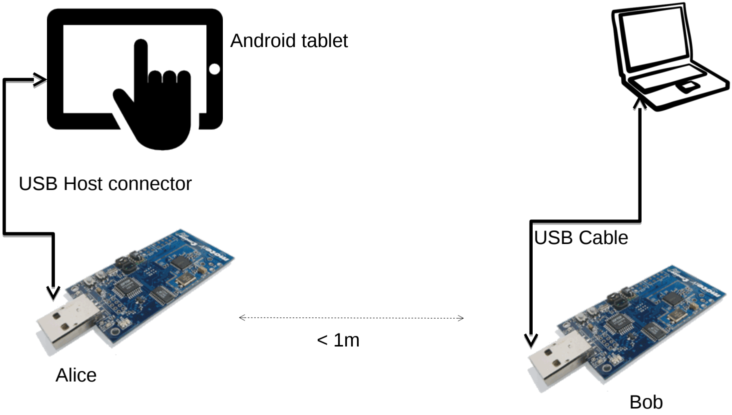
- Use binary expansion on kX_1X_2, $X_2 Z_1$ and $X_1 Z_2$
- Observe that the "coarse" channel gain 2^N shifts $kX_1X_2 = 1.b_1 b_2 \dots b_n$ to the right $2^N k X_1 X_2 = b_N b_{N-1} \dots b_1.b_0 b_{-1}$
- Cut-of at noise level (decimal point) to get deterministic approximation

Resulting Model is deterministic:

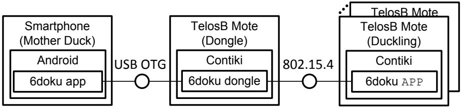


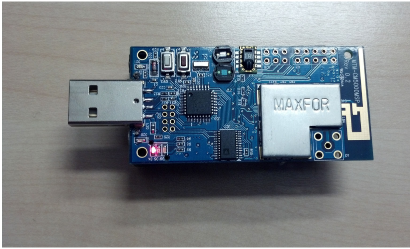
- Due to reciprocity: Same number of bit-levels at Alice & Bob
- New results can be derived in dependence on K, X_1 and X_2
- "Inbuilt" quantization $\rightarrow$ simple key results follow immediately

Implementation:Setup (Hardware)

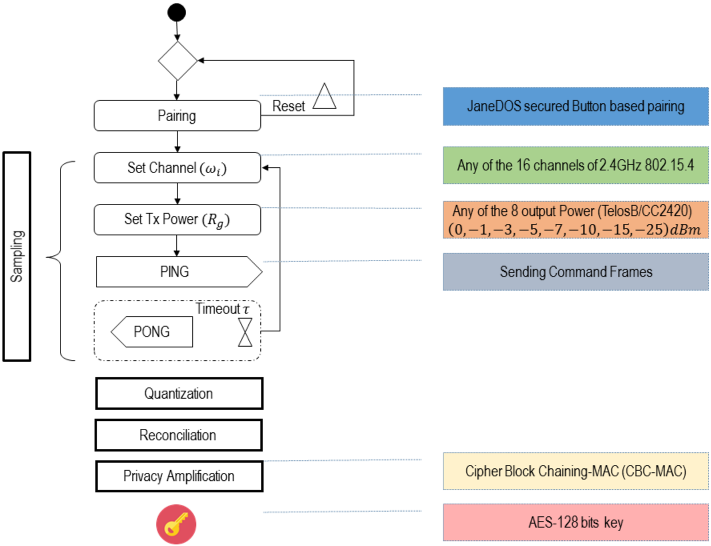


Implementation:Setup (Software)





Implementation:steps



Outline

- Security is a key to the 5G (IoT, Tactile Internet, CPS, SDN etc.) market!
- Research investment on new security (and authentication) schemes highly necessary
- Physical Layer security promising path for 5GPPP Phase II