COMBINING ARTIFICIAL NOISE BEAM FORMING AND CONCATENATED CODING SCHEMES TO EFFECTIVELY SECURE WIRELESS COMMUNICATIONS

SDR'16 Winncomm, Reston, 17 March 2016

Technical Session 8: SDR, CR and DSA Algorithms 2

Eric Nicollet(*)

Christiane Kameni Ngassa(*), François Delaveau(*), Renaud Molière(*), Nir Shapira(**)

(*) Thales Communications & Security; Gennevilliers, France

(**) Nir Shapira (Celeno Communications, Ra'anana, Israel;

E. Nicollet	eric.nicollet@thalesgroup.com	phone : + 33 (0)1 46 13 21 32
R. Moliere	renaud.moliere@thalesgroup.com	phone : + 33 (0)1 41 30 33 60
F. Delaveau	francois.delaveau@thalesgroup.com	phone : + 33 (0)1 46 13 31 32
C. Kameni	christiane.kameni@thalesgroup.com	phone : + 33 (0)1 41 30 30 19

WinnComm USA 2016 – Reston Virginia, 15 - 17th March 2016

Presentation of PHYLAWS project EC FP7 ICT Id-317562

www.phylaws-ict.org

Summary/Agenda

- **Brief introduction to PHYsical Layer SECurity (PHYSEC):**
  - Studied configuration of wireless links
  - Exploiting the multipaths randomness of wireless radio Channel
  - Our Fondamentals - Our current progresses

- **Principle of secrecy coding schemes**
  - Artificial Noise and Beam Forming
  - Secrecy Coding under radio advantage
  - Complete scheme: AN + BF + SC

- **Pre-industrial results of Secrecy coding**
  - Simulation results of Artificial Noise beam forming and Secrecy Coding

- **Conclusion - Technical maturity of**
  Secrecy Coding
  Perspective for other RATs

- **Annex**

Note: This paper is a follow up of Winncomm Munich 2013 and San Diego + Erlangen 2015 papers

"Active and passive eavesdropper threats within public and private civilian networks – Existing and potential future countermeasures – An overview"

"PHYSEC concepts for wireless public networks – introduction, state of the art and perspectives"

"Towards a key-free radio protocol for authentication and security of nodes and terminals in advanced waveforms"

"Physical layer security based protocols to effectively secure wireless communications without key distribution"

Recall of Phylaws' goals and outputs

- **MAIN GOALS:**

  To improve security of wireless links:
  . Radio cell and WLAN
  . Slight to strong mobility (of terminal or scatters)

  To search for key-free solutions based on Physec

  To experiment these solutions <u>in real field</u>

  To search for practical implantations in existing and future public RATs

- **AN ORIGINAL APPROACH:**

  Merging academic and industrial skills on radio-propagation, radio-communications and security.

  Integrating usual hypothesis with return of practical experience

  Considering <u>any kind of threats at physical layer</u>: passive Eve + various active Eve

  <u>Concentrating on signaling and access phases</u> of RATs, and not only on established data links.

PHYLAWS

PHYsical Layer Wireless Security

Project Coordinator:
Thales Communications and Security
François Delaveau
Tel: +33 (0)1 46 43 31 32
Fax: +33 (0)1 46 13 25 55
Email: francois.delaveau@thalesgroup.com
Project website: www.phylaws-ict.org

+ Five Partners:
Institut Mines-Telecom ParisTech (France,
Imperial College of Science, Technology and Medicine (Unted Kingdom),
Teknologian tutkimuskeskus VTT – OY (Finland),
Celeno Communications Israel Ldt (Israël).

Duration 4 years:
November, 2012 – October, 2016

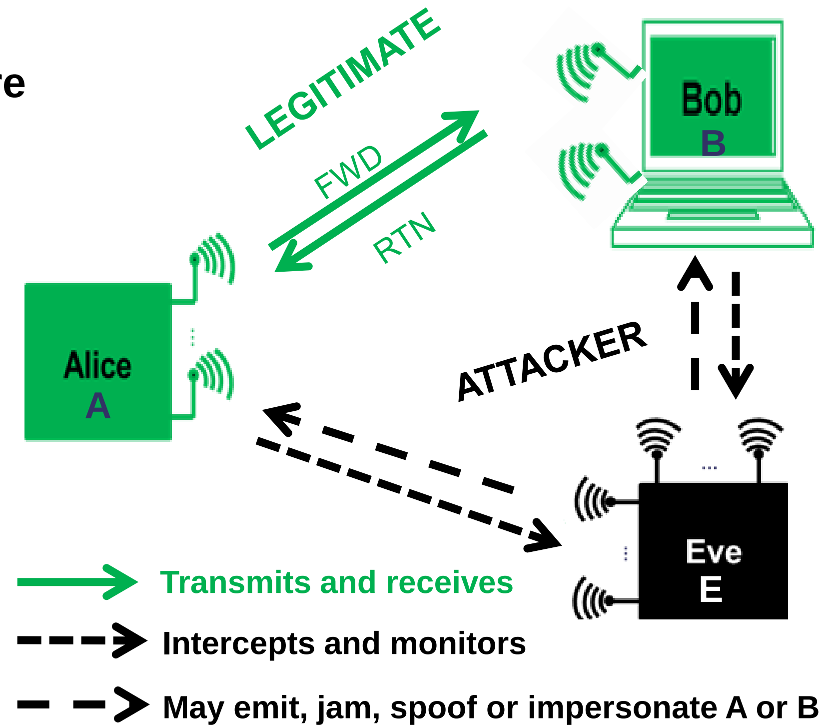
Funding scheme: STREP

Contract Number: CNECT-ICT-317562

Brief introduction to PHYSEC

Studied configuration of wireless links

- **LEGITIMATE links are Alice to/from Bob**
- **EAVESDROPPER and RADIO HACKER links are**
  - Alice to Eve…and even (active) Eve to Alice
  - Bob to Eve… and even (active) Eve to Bob
- **THREAT MODELS**
  - Passive Eve
  - Intelligent (protocol aware) jamming Eve
  - Man in The Middle / Wormhole Eve, etc.



- **Most usual academic hypothesis are:**
  - complete information of Eve about legitimate RATs/waveforms
  - no Information of Eve about legitimate Keys (e.g. Ki Keys on SIM cards)

=> they may be no more valid nowadays especially into public RATs (ex : hacking of Subscriber datat bases)

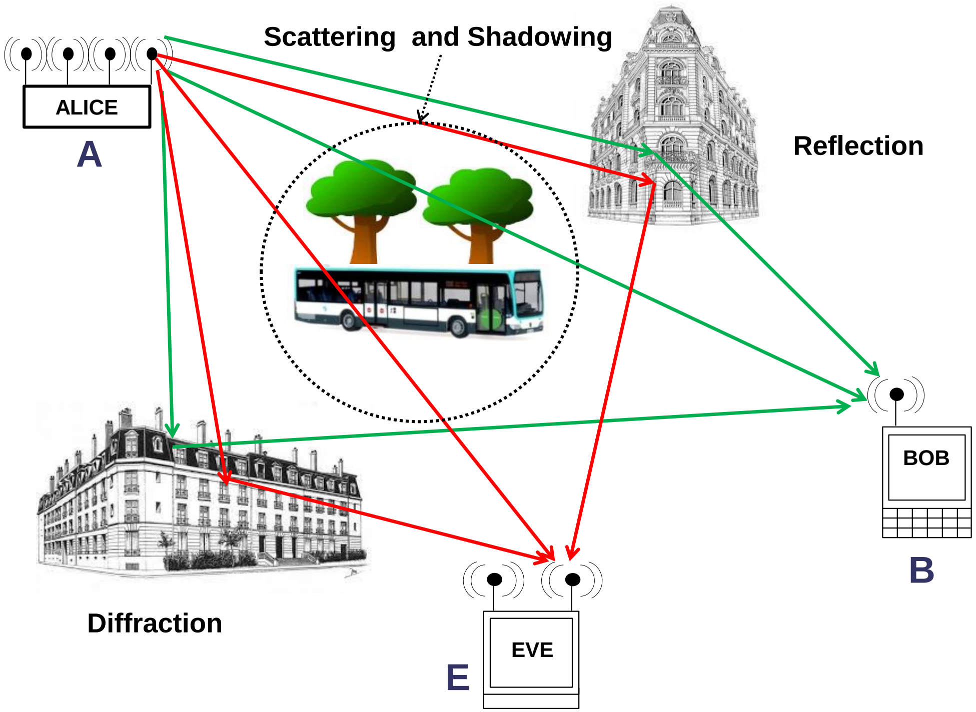
OUR MAIN APPLICATIONS

- **TRANSEC (Transmission Security) is the protection of the transmitted Alice's and Bob's signals face to interception and intrusion attempts of the user receiver (and even jamming and direction finding)**
- **NETSEC (Network Transmission Security) is the protection of the signalling and acces messages of Alice and Bob (usual solutions are authentication and integrity control, sometimes ciphering of signalling in military networks)**
- **COMSEC (Communication Security) is the protection of the data messages of Alice and Bob (voice, sms, mms, high speed data). Most of solutions are based on ciphering+integrity control schemes of signalling and data.**

Brief introduction to PHYSEC
Exploiting the randomness of radiochannel

(Mobile) obstacles between users:

- Multiple paths to reach Bob or Eve
  Reflection, Diffraction, Scattering, Shadowing
- Waveforms received by Bob and Eve have been altered differently
- Apply either to outdoor and indoor



Complex wave propagation + unpredictable scattering objects

- Channel Randomness
- Received waveforms cannot be recovered by computation

At fixed carrier, same angles on obstacles for Alice → Bob and for Bob → Alice

- Same randomness for Alice and Bob
- Channel reciprocity in TDD case

Additional "radio" random for disturbing Eve:

- Alice and Bob Antennas: patterns and orientations
- Artificial noise and Beamforming : SNR advantage to A and B

Used for Secrecy coding

Our Fondamentals = current academic knowledge about PHYSEC:

- Key-less security technique exploiting propagation randomness to establish secret
- Theory is OK since 1980's, academic reasearch is intensive, Applications in realistic radio-environment now exist (IoT in project Prophylaxe, Wireless and WLAN in project Phylaws)

Our current progresses = 3 protection schemes:

Presented Wincomm 2015 San Diego

- Secure Pairing (SP) with Tag Signals (TS) & Interrog. Ackn. Sequences (IASs)
  - ➔ new concepts invented, study in progress.
- Secret Key Generation (SKG)
  - ➔ pre-industrial application to IoT (German project Prophylaxe)
  - ➔ Experimented for WLAN and LTE networks (Phylaws)
- Artificial Noise-Beam Forming (AN-BF) + Secrecy Coding (SC)
  - ➔ Simulation OK, implantation in progress, promises inform. theoretic secrecy

Following slides

Complements on security flaws and threats of public RATs	www.phylaws-ict.org deliverable D2.1.
Complements on legitimate and attacker signals	www.phylaws-ict.org deliverables D2.4, D4.1, D4.3
Fundations of Physical layer security	www.phylaws-ict.org deliverables D2.3, D3.1, D3.2, D3.3
Complements and results about on Physec schemes developed in Phylaws	www.phylaws-ict.org deliverables D2.4, D4.1, D4.2, D4.3, D5.1, D6.1

Prerequisit for secrecy coding schemes

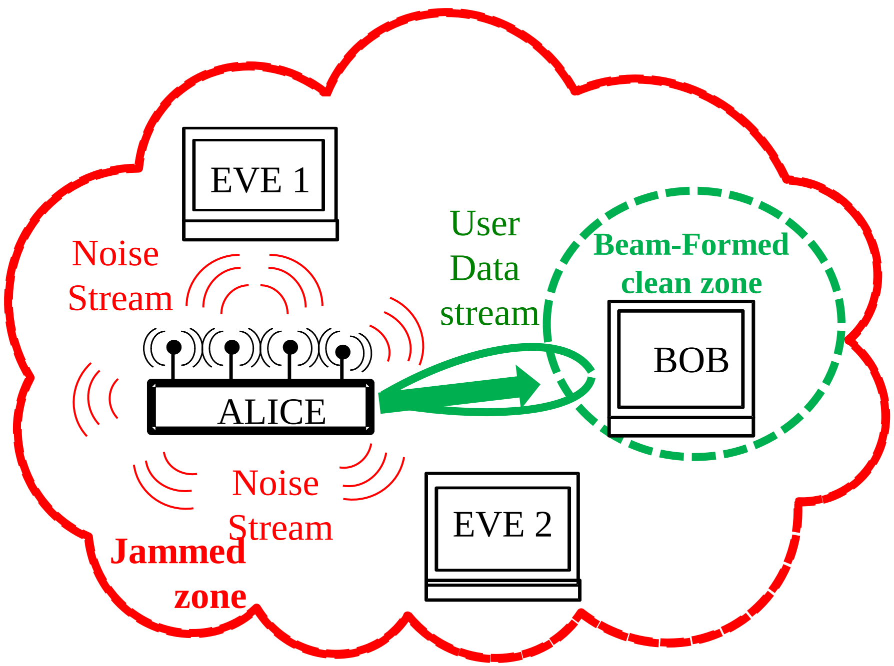
Radio advantage based on Artificial Noise + Beam forming

General principle in MIMO Tx-Rx

1/ Extract the Alice-Bob Channel matrix (CIR) and its orthogonal directions

2/ Transmit noise streams on orthogonal directions. Eve cannot estimate the legitimate CIR, she is thus forced into low Signal to Noise Ratio (SNR).

3/ Beam-form of the Alice-Bob data stream for Bob to maximize link budget.

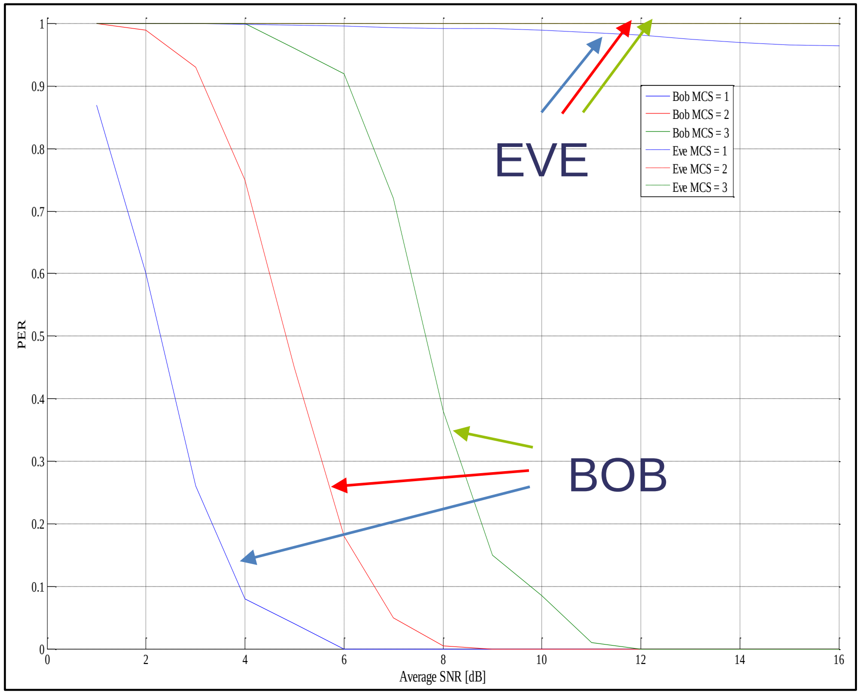


Wifi simulations (Packet error rate)

1/ Alice has four antennas and emits one 802.11n data stream and three noise streams

2/ Bob and Eve have respectively 2 and 4 antennas, with the same receiving capabilities

- Dash line: Packet Error Rate of Eve vs SNR
- Solid line: Packet Error Rate of Bob vs SNR
- Color: Modulation and coding Scheme (MCS)



Principle of secrecy coding schemes

Secrecy Coding under radio advantage

A- Preliminary Radio advantage

- Objective: provide at better capacity at Bob's side than at Eve's side
  - Simple case of AWGN channel

at Bob's Rx   at Eve's Rx

Radio advantage: $(SNR)_{B,dB} - (SNR)_{E,dB}$

Secrecy capacity: C_{SEC}

$$C_{SEC} = \log_2[[1+10^{((SNR)B,dB)/10}]/[1+10^{((SNR)E,dB)/10}]$$

at Bob's Rx   at Eve's Rx

- One practical mean for achieving the radio advantage is Artificial Noise and Beam Forming
  - See the previous slide
  - Eve is forced into low SNR radio because of interfering noise from Alice
  - Thanks for the Beam-Forming, Bob keeps a high SNR radio

B- Objective of the secrecy codes

- correct bit errors between Alice and Bob
- warranty null information leakage towards Eve
- Condition: rate less than C_{SEC}.

C- Practical secrecy coding scheme developed in Phylaws WP4

- Concatenation of two codes
  - A usual Inner FEC Code: able to provide sufficient error correction capability when facing any kind of realistic radio channel
  - An added Outer code (polar or Reed Muller) able to provide secrecy
- The result is a sub-optimal scheme which is close to the optimum.

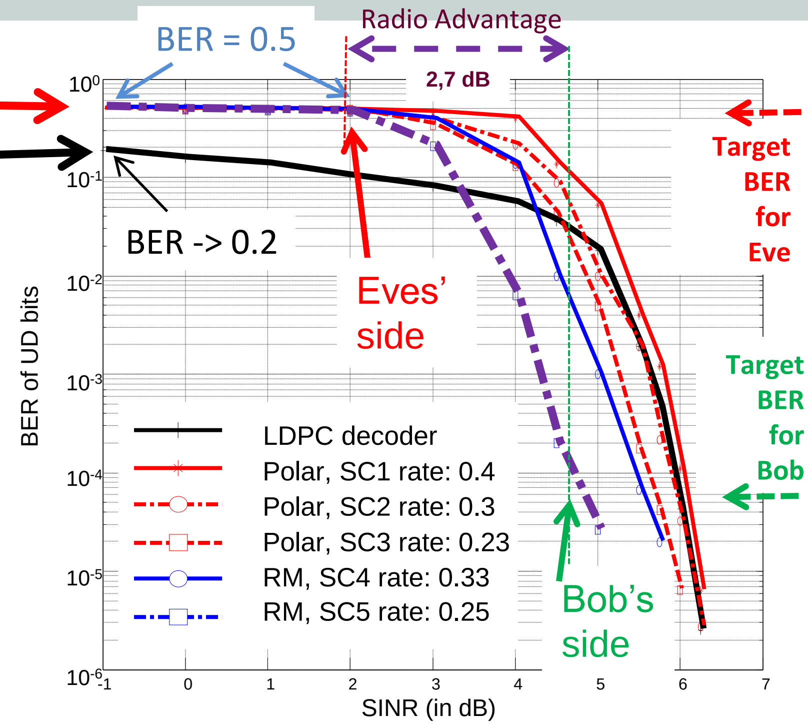
Pre-industrial results of Secrecy Coding

- Simulation results of Artificial Noise Beam Forming and Secrecy Coding

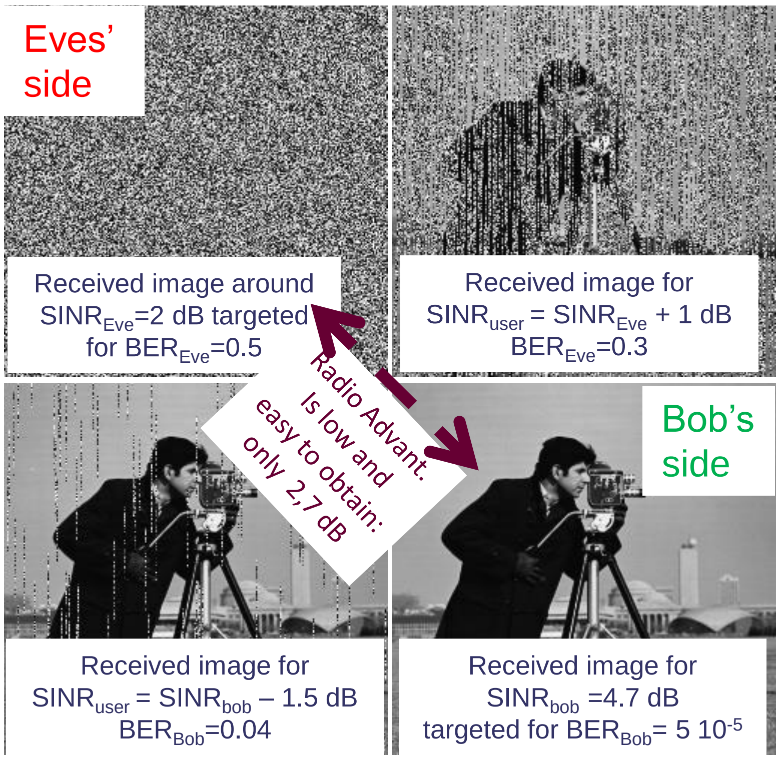
Low $SINR_{Eve}$ ➔ BER = 0.5: no more information leackage

Low $SINR_{Eve}$ ➔ BER = 0.2: information leackage remains

X → Polar or RM outer encoder → FEC inner encoder → Radio Channel → FEC inner decoder → Polar or RM outer decoder → $\hat{X}$



Example with SC 5



Coding schemes	SC 1	SC 2	SC 3	SC 4	SC 5
Inner code	LDPC code of length 1296 and rate 5/6 defined in the 802.11 standard				
Outer code	PC	PC	PC	RMC	RMC
Eves's target rate	**0.1**	**0.1**	**0.1**	**0.05**	**0.05**
Bob's target rate	**0.6**	**0.5**	**0.4**	**0.5**	**0.4**
R bits, UD bits, P bits	102, 512, 410	102, 409, 513	102, 307, 615	56, 430, 538	56, 330, 638
Theoretical Secret rate	0.5	0.4	0.3	0.45	0.35
Secret Bits Rate	**0.4**	**0.33**	**0.24**	**0.33**	**0.25**

Conclusion - Technical maturity of Secrecy Coding Perspective for other RATs

Artifical Noise and BeamForming are mature

- ➔ **Standardization into 802.11ac**
- ➔ **ready now for proposals into LTE releases, IoT & Cellular IoT, 5G, etc.**

and Secrecy Coding is in progress !!

« First » SC schemes for realistic radio communications are proposed and tested

➔ **ready in 2017 for proposals into LTE releases, IoT & Cellular IoT, 5G, Wifi)**

PHYSEC scheme	Technical Status	Requirement	Secrecy efficiency	Application to public Rats
SC - Secrecy Coding	**Schemes now exist** for realistic radio envirT	Controlled Radio (SINR) advantage. (Artificial Noise & Beam Forming)	Controlled with SNR measurT **Ultimate protection**	MIMO Radiocells and WLANs. IoT + M2M

Thank you for your attention

Find more information on our websites
www.phylaws-ict.org

- ZEIT, “Wie Merkels Handy abgehört werden konnte,” 18 12 2014. [Online]. Available: http://www.zeit.de/digital/datenschutz/2014-12/umts-verschluesselung-umgehen-angela-merkel-handy
- Metronews, “Une énorme faille de sécurité permet d'écouter vos appels et de lire vos SMS,” [Online]. Available: http://www.metronews.fr/high-tech/une-enorme-faille-de-securite-permet-d-ecouter-vos-appels-et-de-lire-vos-sms/mnlv!YnqDbOgrtHFYk/
- http://media.ccc.de/browse/congress/2014/31c3_-_6531_-_en_-_saal_6_-_201412272300_-_ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira.html
- https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
- M. Bloch and J. Barros, Physical-Layer Security, Cambridge University Press, 2011.
- J.-C. Belfiore, C. Ling and L. Luzzi, “Lattice codes achieving strong secrecy over the mod-Λ Gaussian channel,” in IEEE International Symposium on Information Theory Proceedings, Cambridge, USA, 2012
- J. W. Wallace and R. K. Sharma, “Automatic secret keys from reciprocal MIMO Wireless channels: measurement and analysis,” *IEEE Transactions on information forensics and security,* vol. 5, no. 3, pp. 381-392, September 2010.
- F. Delaveau, A. Evestti, A. Kotelba, R. Savola and N. Shapira, “Active and passive eavesdropper threats within public and private cililian networks - Existing and potential future countermeasures - An overview,” in Winncomm, Munich, Germany, 2013.
- F. Delaveau, C. Ling, E. Garrido, J.-C. Belfiore and A. Sibile, “Physec concepts for wireless public networks - Intoduction, state of the art, perspectives,” in Winncomm, Munich, Germany, 2013.
- T. Mazloum, F. Mani and A. Sibille, "Analysis of secret key robustness in indoor radio channel measurements," in *IEEE Vehicular Tech. Conf.*, Glasgow, Scotland, 2015.
- X. He, H. Dai, “Is link signature dependable for Wireless Security?” in proceeding IEEE INFOCOM 2013
- Web site of the project Phylaws (Funded by EC-FP7-ICT-2011-8 GN 317562): www.phylaws-ict.org
- Web site of the project Prophylaxe (funded by German BMBF GN 16KIS0005K): www.ict-prophylaxe.de

AN - BF	Artificial Noise – Beam Forming	NETSEC	Network Transmission Security
BCH	Bose Ray-Chaudhuri Hocquenghem	NLOS	Non Line Of Sight
BER	Bit Error Rate	PHYSEC	Physical Layer Security
BTS	Base Transceiver Station	OoM	Order of Magnitude
CIR	Channel Impulse Response	PSS / SSS	Primary Synchr. Sequence / Secondary Synchr. Seq. (LTE)
CFR	Channel Frequency Response	RAT	Radio Access Technology
CQA	Channel Quantization Algorithm	Rx	Receiver
COMSEC	Communication Security	SIM	Subscriber Identity Module – Self Interference Mitigation
CRS	Cell-specific Reference Signal	SISO/SIMO	Single Input Single Output / Single Input Multiple Output
FDD	Frequency Division Duplex	SKG,SC,SP	Secret Key Generation , Secrecy Coding, Secure Pairing
FEC	Forward Error Correction	SNR, SINR	Signal to Noise Ratio, Signal to Noise + Interference Ratio
FuDu	Full Duplex	SS7	Signaling System No.7
GSM	Global System for Mobile communications	STF, LTF	Short Training Field, Long Training Field (Wifi)
IMSI	International Mobile Subscriber Identity	TBD - TBS	To Be Defined - To Be Studied
IoT	Internet of Things	TDD	Time Division Duplex
LDPC	Low Density Parity Check	TMSI	Temporary Mobile Subscriber Identity
LOS	Line Of Sight	TRANSEC	Transmission Security
LTE	Long Term Evolution	Tx	Transmitter
MAC	Media Access Control	UIM	User Identity Module
MISO/MIMO	Multiple Input Single Output / Multiple Input Multiple Output	UMTS	Universal Mobile Telecommunications System
NIST	National Instrument of Standards and Technology		

Complete scheme : AN + BF + SC

Alice
wants to transmit a message B^K

Alice
provides a radio advantage to Bob
(using self interfered tag signals
or artificial noise + Beam Forming)

Alice
encodes B^K using the secrecy coding scheme and sends the message M^N over the modulated signal S

Losses$_{A\rightarrow E}$: mean progataion losses between Alice and Eve
Noise$_{Eve}$: added noise at Eve's receiver

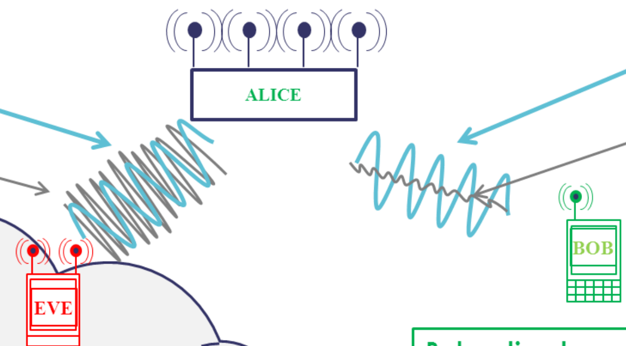
Modulated signal sent by Alide Sig$_{Alice}$

I$_{Eve}$ Strong (intentional) Artificial noise or Self-interference

Losses$_{A\rightarrow B}$: mean progataion losses between Alice and Bob
Noise$_{Bob}$: added noise at Eve's receiver

Modulated signal sent by Alide sig$_{Alice}$

I$_{Bob}$ Very low residue of Artificial Noise or Interference thanks to
- Beam Forming
- Interference mitigation



Eve estimates messages $\hat{M}^N{}_{(Eve)}$ from received signal X$_{Eve}$:

$$X_{Eve} = L_{A\rightarrow E}.(Sig_{Alice}+I_{Eve})+Noise_{Eve}$$

- Eve is in the interfered region and she cannot detect the Alice's signal Sig$_{Alice}$
- Eve as low SINR (=10.log$_{10}$(Power(Sig$_{Alice}$)/Power(I$_{Eve}$+Noise$_{Eve}$)
- Hence Eve decodes $\hat{M}^N{}_{(Eve)}$ with BER = 0.5

Finally: Eve has no information on the transmitted message

Bob estimates messages $\hat{M}^N{}_{(Bob)}$ from received signal X$_{Bob}$:

$$X_{Bob} = L_{A\rightarrow B}.(Sig_{Alice}+I_{Bob})+Noise_{Bob}$$

- Bob is in the clear region or he can detect the Alice Signal.
- Bob has a good SINR (=10.log$_{10}$(Power(Sig$_{Alice}$)/Power(I$_{Bob}$+Noise$_{Bob}$)
- hence Bob decodes $\hat{M}^N{}_{(Bob)}$ with BER = 0

Finally: Bob recovers the transmitted message with no error