Physical layer authentication

Review of physical layer authentication techniques

Ir. Ewan Gencsek

Electromagnetism and Telecommunication Department
Faculty of Engineering
University of Mons

ewan.gencsek@umons.ac.be

April 6, 2023

Outline

1 Introduction

2 Low OSI layers security

3 Physical layer authentication

4 Superimposed-tag authentication

5 Slope authentication

6 Conclusion

Introduction
IoT

My research is about enhancing security at low OSI layers in industrial internet of things (IIoT) field.

IoT characteristics:

- Limited ressources: storage, energy, computation, ...
- Diversity in protocols and in devices
- Profit driven businesses
- Lack of related legislation

From [1, 2, 3]

Introduction

IoT

My research is about enhancing security at low OSI layers in industrial internet of things (IIoT) field.

IoT characteristics:

- Limited ressources: storage, energy, computation, ...
- Diversity in protocols and in devices
- Profit driven businesses
- Lack of related legislation

$\Rightarrow$ Security flaws

From [1, 2, 3]

Introduction

Industrial Internet of Things (IIoT)

IIoT characteristics:

- Sensors
- Controllers
- Production lines
- Used for efficiency and safety

From [1, 2, 3]

Introduction

Industrial Internet of Things (IIoT)

IIoT characteristics:

- Sensors
- Controllers
- Production lines
- Used for efficiency and safety

$\Rightarrow$ We need cybersecurity !!!

From [1, 2, 3]

Why low OSI layers security ?

From [4]

Layer	Protocol data unit (PDU)
Application	Data
Presentation	Data
Session	Data
Transport	Segment, Datagram
Network	Packet
Data link	Frame
Physical	Bit, Symbol

Why low OSI layers security ?

From [4]

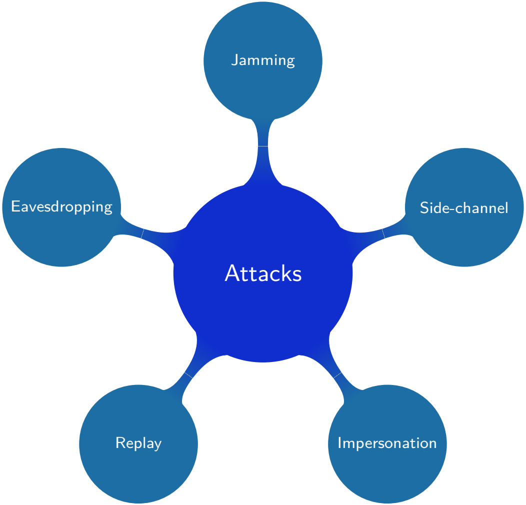
Layer	Protocol data unit (PDU)
Application	Data
Presentation	Data
Session	Data
Transport	Segment, Datagram
Network	Packet
Data link	Frame
Physical	Bit, Symbol

Why low OSI layers security ?

From [4]

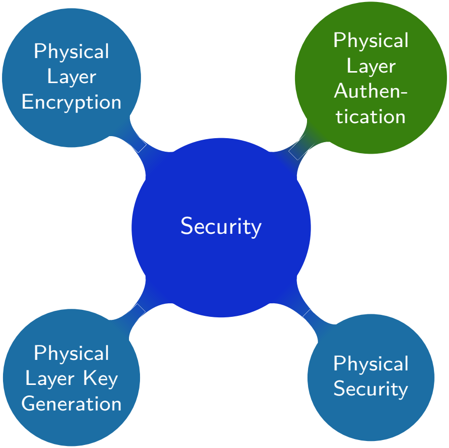
Layer	Protocol data unit (PDU)
Application	Data
Presentation	Data
Session	Data
Transport	Segment, Datagram
Network	Packet
Data link	Frame
Physical	Bit, Symbol

Because there are attacks on low layers ...



From [1, 2, 3]

How to defend against them in PHY layer ?



From [1, 2, 3]

What's physical layer authentication (PLA) ?

From [1]

What's physical layer authentication (PLA) ?

It allows a legitimate receiver to distinguish between a legitimate transmitter and a rogue one [1].

It enables defense against both passive (eavedropping) and active (impersonation) attacks.

It occurs at the physical layer where the unauthenticated signals can be ignored and quickly rejected.

From [1]

PLA should be robust, secure and covert

1. Robustness: The technique should be robust to channel fading and noise effects
   Channel fading: random signal attenuation due to the environment of the communication channel [5].

2. Security: The technique should be resistant to adversary attacks

3. Covertness: Unaware receiver should be able to decode signals sent from an aware transmitter

From [1]

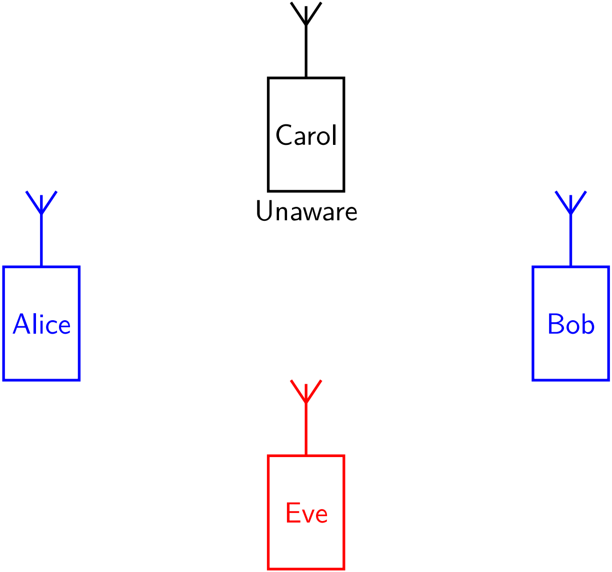
Active or passive PLA ?

1. Passives: use channel and/or device properties to authenticate a transmitter
   * Drawback: sensitive to external variables, e.g. temperature

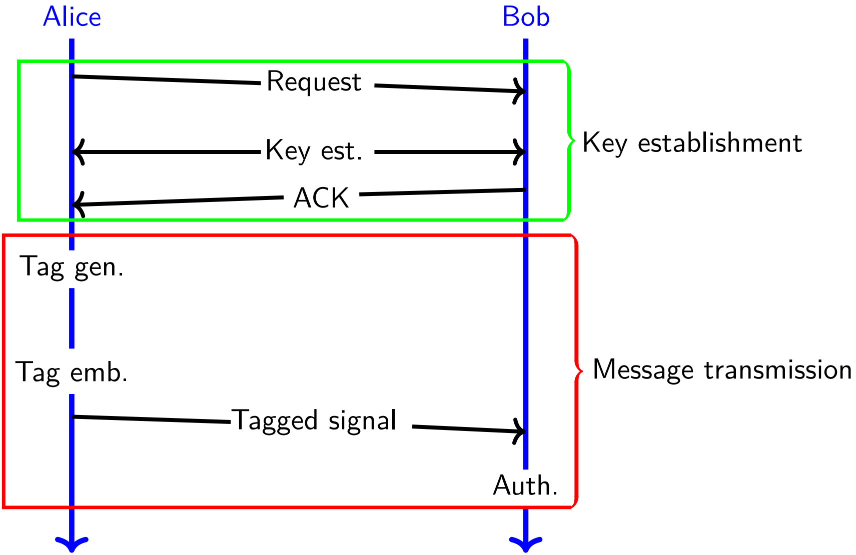
2. Actives: Embbed a "tag" to the signal to authenticate the transmitter
   * if lightweight, this should be useful in industry environment

From [1, 6, 7]

Communication scenario and roles



Key establishment and message transmission stages in active PLA



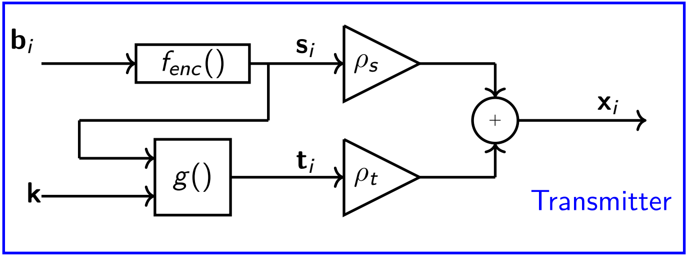
Superimposed-tag transmission (SUP method)

Idea: to send a tag signal simultaneously with the message signal

From [6]

Superimposed-tag transmission (SUP method)

Idea: to send a tag signal simultaneously with the message signal



with

- $\mathbf{b}_i = \{b_1, \ldots, b_L\}_i$ block of L message symbols (i.i.d. RVs);
- $f_{enc}()$ the encoding function and $g()$ the tag generation function;
- ρ_* the energy ratio allocated to the message (ρ_s) and to the tag (ρ_t) $\Rightarrow \rho_s^2 + \rho_t^2 = 1$.

From [6]

Signal reception and estimation

Bob will receive a signal $\mathbf{y}_i$:

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{n}_i$$

- $\mathbf{h}_i$: Rayleigh flat-block fading channel $h_i \sim \mathcal{CN}(0, \sigma_h^2)$
- $\mathbf{n}_i$: white gaussian noise $\mathbf{n}_i = \{n_1, \ldots, n_L\}_i$ where $\{n_k\}_i \sim \mathcal{CN}(0, \sigma_n^2)$

From [6]

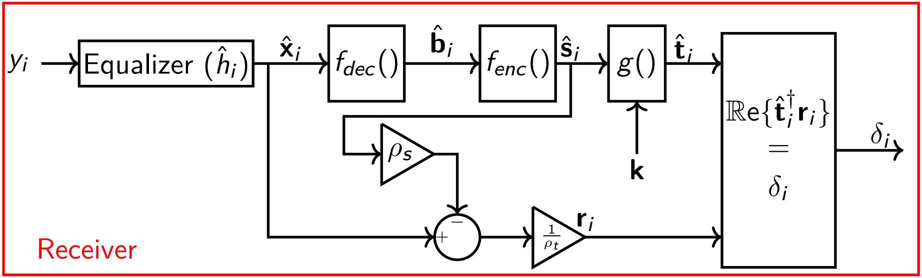
Signal reception and estimation

Bob will receive a signal $\mathbf{y}_i$:

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{n}_i$$

- $\mathbf{h}_i$: Rayleigh flat-block fading channel $h_i \sim \mathcal{CN}(0, \sigma_h^2)$
- $\mathbf{n}_i$: white gaussian noise $\mathbf{n}_i = \{n_1, \ldots, n_L\}_i$ where $\{n_k\}_i \sim \mathcal{CN}(0, \sigma_n^2)$

Bob will compare the estimated tag $\hat{\mathbf{t}}_i$ and a computed residual signal $\mathbf{r}_i = \frac{1}{\rho_t}(\hat{\mathbf{x}}_i - \rho_s \hat{\mathbf{s}}_i)$.



From [6]

Received signal authentication

Received signal authentication

The authentication is a threshold test with hypoteses [8]:

$$H_0: \quad \delta_i \sim \mathcal{N}\left(0, \frac{L}{2\rho_t^2\gamma_i}\right) \quad \rightarrow \mathbf{t}_i \text{ is not present in } \mathbf{r}_i$$

$$H_1: \quad \delta_i \sim \mathcal{N}\left(L, \frac{L}{2\rho_t^2\gamma_i}\right) \quad \rightarrow \mathbf{t}_i \text{ is present in } \mathbf{r}_i$$

- γ_i: instantaneous channel SNR ($= \frac{|h_i|^2}{\sigma_n^2}$)
- $\bar{\gamma}$: average SNR ($= \frac{\sigma_h^2}{\sigma_n^2}$)

Received signal authentication

The authentication is a threshold test with hypoteses [8]:

$$H_0: \quad \delta_i \sim \mathcal{N}\left(0, \frac{L}{2\rho_t^2\gamma_i}\right) \quad \rightarrow \mathbf{t}_i \text{ is not present in } \mathbf{r}_i$$
$$H_1: \quad \delta_i \sim \mathcal{N}\left(L, \frac{L}{2\rho_t^2\gamma_i}\right) \quad \rightarrow \mathbf{t}_i \text{ is present in } \mathbf{r}_i$$

- γ_i: instantaneous channel SNR ($= \frac{|h_i|^2}{\sigma_n^2}$)
- $\bar{\gamma}$: average SNR ($= \frac{\sigma_h^2}{\sigma_n^2}$)

The authentication decision φ_i is then:

$$\varphi_i = \begin{cases} 1, & \delta_i \geqslant \theta_i^0 \\ 0, & \delta_i < \theta_i^0 \end{cases}$$

with θ_i^0 the optimal threshold for a fixed probability of false alarm ϵ_{FA} ($P\{H_0|H_1\}$).

Probability of authentication and simulation

The probability of detection of a randomly chosen block is [8]

$$P_D = \mathbb{E}\{Pr\{\delta_i \geqslant \theta_i^0 | H_1\}\} = \frac{1}{2}\left(1 - \mathrm{sign}(\theta^0 - L)\sqrt{\frac{(\theta^0 - L)^2 \rho_t^2 \bar{\gamma}}{L + (\theta^0 - L)^2 \rho_t^2 \bar{\gamma}}}\right)$$

Probability of authentication and simulation

The pro

$P_D =$

$$\frac{\rho_t^2\bar{\gamma}}{2\rho_t^2\bar{\gamma}}\Bigg)$$

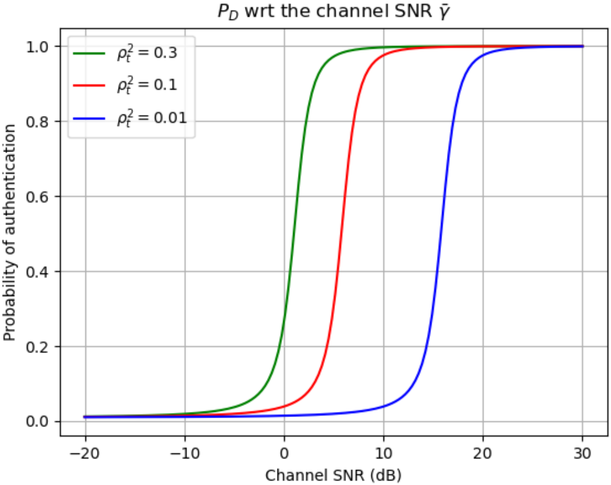


Figure: P_D versus different SNRs for $L = 64$, $\epsilon_{FA} = 0.01$, and different ρ_t^2.

Idea of slope authentication

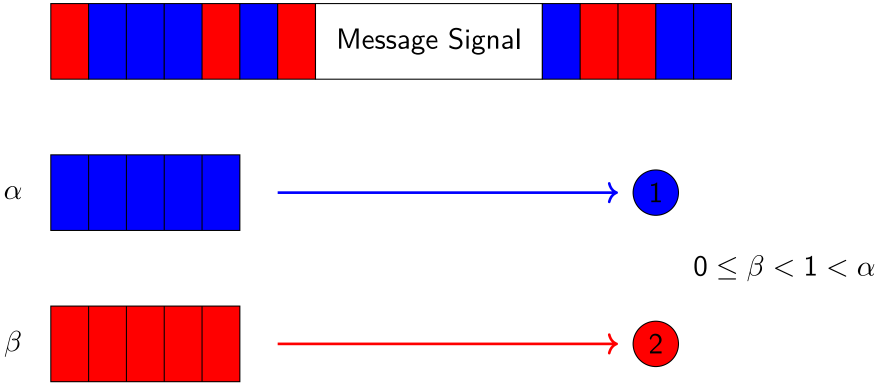
Idea: to divide the message signal into several groups and shuffle the symbols according to the secret key **k**

From [7]

Idea of slope authentication

Idea: to divide the message signal into several groups and shuffle the symbols according to the secret key **k**

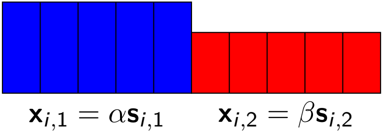
Take the case of two equal groups:



From [7]

Tagged signal transmission and reception

The tag $\mathbf{t}_i = g(\mathbf{p}_i, \mathbf{k})$ ($\mathbf{p}_i$ is the pilot signal) indicates which message signal symbol belongs to which group and is not sent. The tagged signal is constructed as

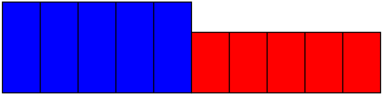


with $\mathbf{s}_{i,*}$ the message signal symbols belonging to the group $*$ and the energy allocation limitation $\frac{\alpha^2}{2} + \frac{\beta^2}{2} = 1$.

From [7]

Tagged signal transmission and reception

The tag $\mathbf{t}_i = g(\mathbf{p}_i, \mathbf{k})$ ($\mathbf{p}_i$ is the pilot signal) indicates which message signal symbol belongs to which group and is not sent. The tagged signal is constructed as



$$\mathbf{x}_{i,1} = \alpha \mathbf{s}_{i,1} \qquad \mathbf{x}_{i,2} = \beta \mathbf{s}_{i,2}$$

with $\mathbf{s}_{i,*}$ the message signal symbols belonging to the group $*$ and the energy allocation limitation $\frac{\alpha^2}{2} + \frac{\beta^2}{2} = 1$.

The received tagged signal: $\mathbf{y}_i = \mathbf{y}_{i,1} | \mathbf{y}_{i,2}$ with $\mathbf{y}_{i,*} = h_i \mathbf{x}_{i,*} + \mathbf{n}_{i,*}$.

Remark: Nakagami-m block-fading channel model [7] ($m = 0.5$, $1 \Leftrightarrow$ one-sided Gaussian distribution, Rayleigh, respectively).

From [7]

Test statistic is the slope between the groups

The hypotheses are different from the SUP method:

$$H_0: \quad \mathbf{y}_i \text{ is a normal signal}$$
$$H_1: \quad \mathbf{y}_i \text{ is a tagged signal}$$

From [7]

Test statistic is the slope between the groups

The hypotheses are different from the SUP method:

$$H_0: \quad \mathbf{y}_i \text{ is a normal signal}$$
$$H_1: \quad \mathbf{y}_i \text{ is a tagged signal}$$

To decide for authtencity of a signal we will compare τ_i to a threshold θ_i as before:

$$\tau_i = \tau_{i,1} - \tau_{i,2}$$

with $\tau_{i,*} = \mathbf{y}_{i,*}^{\dagger}\mathbf{y}_{i,*}$.

From [7]

Test statistic is the slope between the groups

The hypotheses are different from the SUP method:

$$H_0 : \quad \mathbf{y}_i \text{ is a normal signal}$$
$$H_1 : \quad \mathbf{y}_i \text{ is a tagged signal}$$

To decide for authtencity of a signal we will compare τ_i to a threshold θ_i as before:

$$\tau_i = \tau_{i,1} - \tau_{i,2}$$

with $\tau_{i,*} = \mathbf{y}_{i,*}^{\dagger} \mathbf{y}_{i,*}$.

We can see a second advantage of the slope authentication compare to the SUP method: one multiplication instead of channel estimation and demodulation

From [7]

Probability of authentication

The probability of tag detection for the $i th$ block is

$$P_{i,PD} = Q_1\left(\sqrt{\frac{2T_i^2}{\sigma_n^2}}, \sqrt{2\ln\left(\frac{1}{2\epsilon_{FA}}\right)}\right) - \frac{1}{2}e^{\left(\ln\left(\frac{1}{2\epsilon_{FA}}\right) - \frac{T_i^2}{2\sigma_n^2}\right)} Q_1\left(\sqrt{\frac{T_i^2}{\sigma_n^2}}, \sqrt{4\ln\left(\frac{1}{2\epsilon_{FA}}\right)}\right)$$

with Q_1 the first order Marcum Q-function and $T_i = |h_i|^2\left(\alpha^2 - \beta^2\right)$.
Then, for a randomly chosen block, the probability of detection is

$$P_D = \int P_{i,PD} f_\gamma(\gamma) d\gamma$$

with $f_\gamma(\gamma)$ the PDF of channel SNR.

From [7]

Probability of authentication

The probabi

$P_{i,}$

with Q_1 the ... $-\beta^2)$.
Then, for a ... is

with $f_\gamma(\gamma)$ t...

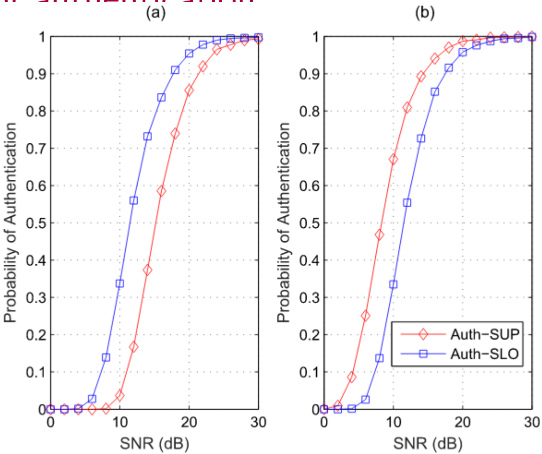


Fig. 6. Authentication probabilities of the Auth-SUP method and the proposed Auth-SLO method considering each block separately with $\varepsilon_{FA} = 0.01$, where the remaining simulation parameters are the same as those of Fig. 5 except (a) $\rho_t = 0.1$, $\beta = 0.9$; (b) $\rho_t = 0.15$, $\beta = 0.9$.

From [7]

BER and channel estimation: superiority of slope method

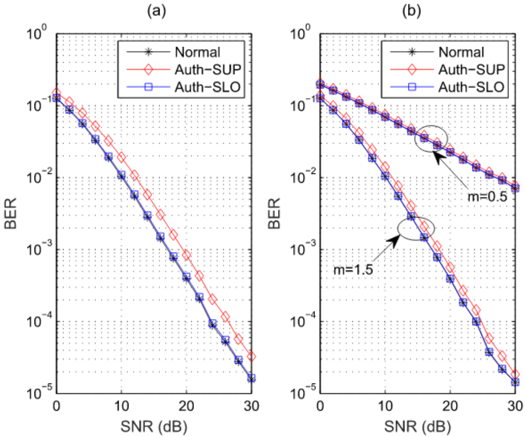


Fig. 5. BER of Carol's receiver for a normal signal, the Auth-SUP method and the proposed Auth-SLO method under Nakagami fading with $m = 1.5$, where the transmit signal is modulated with binary phase-shift keying (BPSK), $L = 2000, f_c = 2\text{GHz}$ and $d = 100\text{m}$. (a) $\rho_t^2 = 0.1$, $\beta = 0.9$; (b) $\rho_t^2 = 0.05$ and $\beta = 0.95$.

BER and channel estimation: superiority of slope method

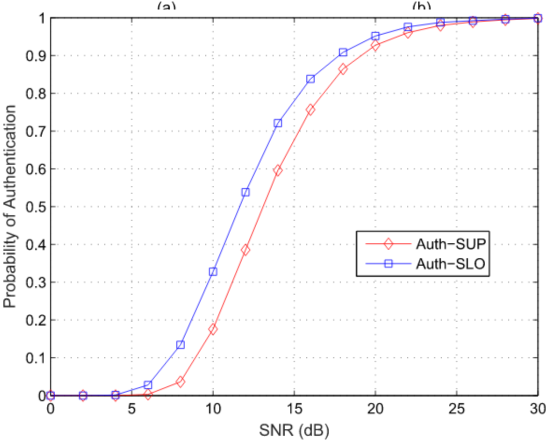


Fig. 9. Authentication probabilities of the Auth-SUP method and the proposed Auth-SLO method considering each block separately with $\varepsilon_{\mathrm{FA}} = 0.01$, where $\hat{h} = h + \tilde{h}$, $\tilde{h} \sim \mathcal{CN}\left(0, \sigma_n^2\right)$ and the remaining simulation parameters are the same as those of Fig. 6(b).

Conclusion

Two methods were presented:

1. Superimposed tag authentication
2. Slope authentication

Both methods are sensible to their parameters (ρ_t and β). Still, the slope method present advantages compared to the SUP method:

- reduced impact at the unaware receiver
- reduced computation complexity

However, I didn't recover the [7] figures. After recovering them, parameter optimization will be done for different IIoT application: simulate an industrial environment and apply PLA methods with specific standard.


CREATE SLIDES
PRESENT SLIDES
END THE PRESENTATION SUCCESSFULLY
QUESTIONS OF THE AUDIENCE

References I

[1] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys And Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[2] C.-K. Wu, *Internet of Things Security*. Springer Singapore, 2021.

[3] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys And Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[4] Wikipedia contributors, "Osi model — Wikipedia, the free encyclopedia," 2022, [Online; accessed 15-November-2022]. [Online]. Available: https://en.wikipedia.org/w/index.php?title=OSI_model&oldid=1116183418

References II

[5] V. Moyeaert and M. Wuilpart, "Advanced communication systems - fading channels modelling for wireless communications," 2020-2021.

[6] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[7] N. Xie and C. Chen, "Slope authentication at the physical layer," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1579–1594, 2018.

[8] N. Xie, C. Chen, and Z. Ming, "Security model of authentication at the physical layer and performance analysis over fading channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 253–268, jan 2021.

Superimposed-tag authentication (SUP) [6]

Definitions and transmitted tagged signal

Idea: to send a tag signal simultaneously with the message signal

Definitions:

- b_i: block of L message symbols $\{b_{i,k}\}$ idependent and identically distributed;
- f_{enc}: encoding function (channel coding, modulation and pulse shaping);
- f_{dec}: decoding function (inverse of f_{enc});
- s_i: message signal ($=f_{enc}(b_i)$);
- t_i: tag signal ($=g(s_i,\mathbf{k})$) with g the tag generation function, e.g. hash function;
- ρ_*: energy allocation for the signal (s) or the tag (t) $\rightarrow \rho_s^2 + \rho_t^2 = 1$.

Alice sends the signal x_i to Bob:

$$x_i = \rho_s s_i + \rho_t t_i$$

Assumptions: $\mathbb{E}\{M_{i,k}\} = 0$; $\mathbb{E}\{|x_{i,k}|^2\} = 1$; $\mathbb{E}\{|M_i|^2\} = L$; $\mathbb{E}\{s_i^\dagger t_i\} = 0$; where M denotes s, t or x; $k = \{1, \ldots, L\}$.

Superimposed-tag authentication (SUP) [6]

Definitions

Idea: to send a tag signal simultaneously with the message signal

Definitions:

- b_i: block of L message symbols $\{b_{i,k}\}$ independent and identically distributed;
- f_{enc}: encoding function (channel coding, modulation and pulse shaping);
- f_{dec}: decoding function (inverse of f_{enc});
- s_i: message signal ($=f_{enc}(b_i)$);
- t_i: tag signal ($=g(s_i,\mathbf{k})$) with g the tag generation function, e.g. hash function;
- ρ_*: energy allocation for the signal (s) or the tag (t) $\rightarrow \rho_s^2 + \rho_t^2 = 1$.

Superimposed-tag authentication (SUP) [6]

Tagged signal and detection

Alice sends the signal x_i to Bob:

$$x_i = \rho_s s_i + \rho_t t_i$$

Bob will receive the signal y_i:

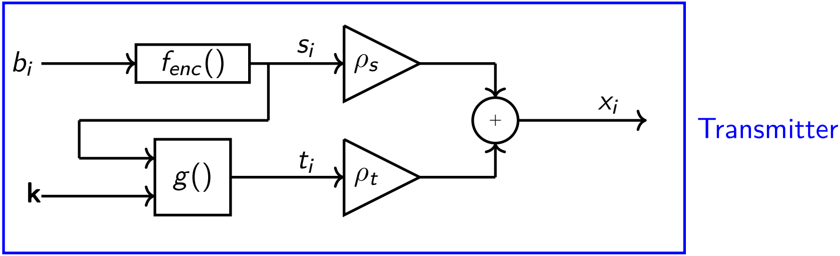
$$y_i = h_i x_i + n_i$$

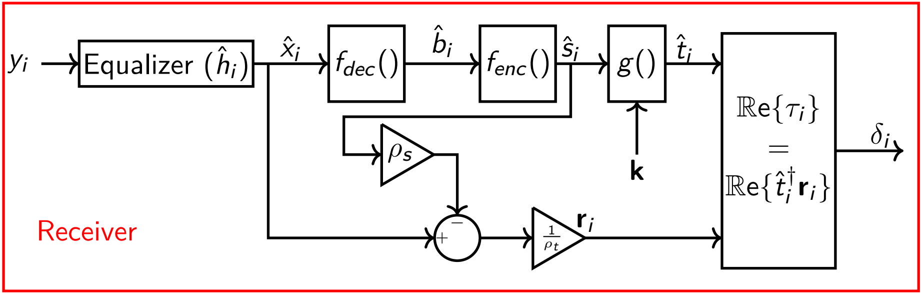
- h_i: Rayleigh flat-block fading channel $h_i \sim \mathcal{CN}(0, \sigma_h^2)$
- n_i: white gaussian noise $n_i = \{n_1, \ldots, n_L\}$ where $n_{i,k} \sim \mathcal{CN}(0, \sigma_n^2)$

Bob will compare the estimated tag $\hat{t}_i$ and a computed residual signal $\mathbf{r}_i = \frac{1}{\rho_t}(\hat{x}_i - \rho_s \hat{s}_i)$.

Superimposed-tag authentication (SUP) [6]

Transmission, reception and authentication block diagrams





Slope authentication [7]

Tagged signal

The tag $t_i = g(p_i,\mathbf{k})$ (p_i is the pilot signal) indicates which message signal symbol belongs to which group and is not sent. The tagged signal is constructed as

$$x_{i,1} = \alpha s_{i,1}$$
$$x_{i,2} = \beta s_{i,2}$$

with $s_{i,*}$ the message signal symbols belonging to the group $*$ and the energy allocation limitation $\frac{\alpha^2}{2} + \frac{\beta^2}{2} = 1$.

The received tagged signal is then:

$$y_{i,1} = h_i x_{i,1} + n_{i,1}$$
$$y_{i,2} = h_i x_{i,2} + n_{i,2}$$

[7] considers Nakagami-m block-fading channel. The Nakagami-m PDF is

$$f_x(x) = \frac{2m^m x^{2m-1}}{\Gamma(m)} e^{(-mx^2)}$$

Slope authentication [7]

Probability of detection

The probability of tag detection for the i*th* block is

$$P_{i,PD} = Q_1\left(\sqrt{\frac{2T_i^2}{\sigma_n^2}}, \sqrt{2\ln\left(\frac{1}{2\epsilon_{FA}}\right)}\right) - \frac{1}{2}e^{\left(\ln\left(\frac{1}{2\epsilon_{FA}}\right)-\frac{T_i^2}{2\sigma_n^2}\right)} Q_1\left(\sqrt{\frac{T_i^2}{\sigma_n^2}}, \sqrt{4\ln\left(\frac{1}{2\epsilon_{FA}}\right)}\right)$$

with Q_1 the first order Marcum Q-function and $T_i = |h_i|^2\left(\alpha^2 - \beta^2\right)$.
Then, for a randomly chosen block, the probability of detection is

$$P_D = \int P_{i,PD} f_\gamma(\gamma) d\gamma$$

with $f_\gamma(\gamma) = \frac{1}{\gamma\Gamma(m)}\left(\frac{m\gamma}{\bar{\gamma}}\right)^m e^{\left(-\frac{m\gamma}{\bar{\gamma}}\right)}$, $\gamma \geq 0$.

Slope authentication [7]

Probability of detection

The probabi

$P_{i,}$

with Q_1 the ... $-\beta^2)$.
Then, for a ... is

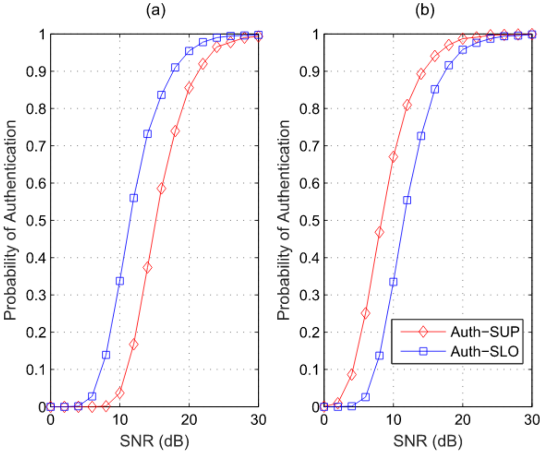


Fig. 6. Authentication probabilities of the Auth-SUP method and the proposed Auth-SLO method considering each block separately with $\varepsilon_{FA} = 0.01$, where the remaining simulation parameters are the same as those of Fig. 5 except (a) $\rho_t = 0.1$, $\beta = 0.9$; (b) $\rho_t = 0.15$, $\beta = 0.9$.

with $f_\gamma(\gamma) =$