URSI GASS 2020
Rome, Italy
29 August - 5 September 2020

Detection of cyber-attacks on Wi-Fi network by classification of spectral data

Jonathan Villain, Virginie Deniau, Anthony Fleury, Christophe Gransart and Eric Pierre Simon

Université Gustave Eiffel

SUMMARY

Introduction

Implementation of jamming an de-authentication attacks

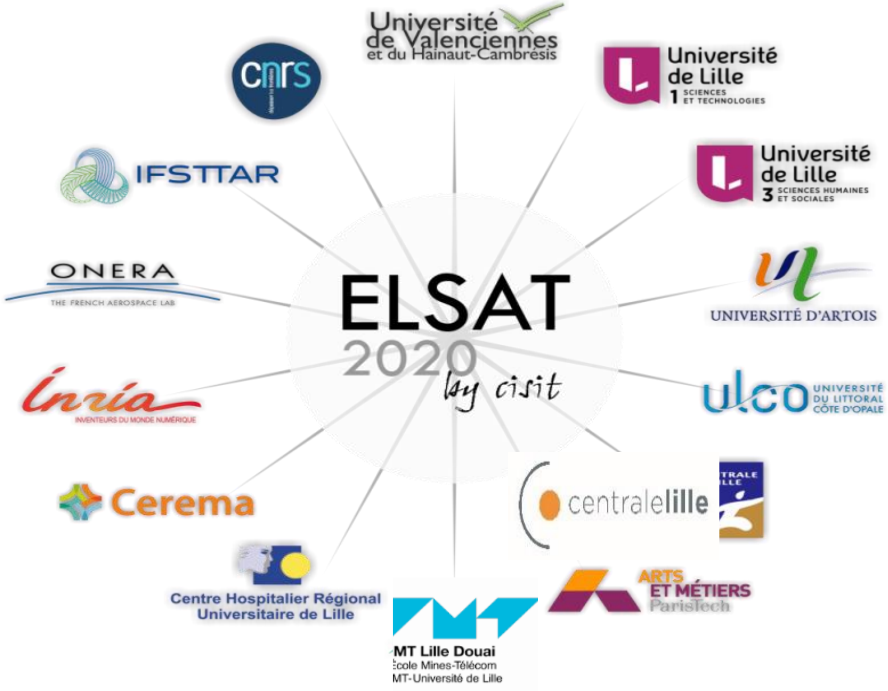
Self Adaptative Kernel Machine (SAKM)

Results

Conclusion

Introduction

- Project co-financed by the European Union through the FEDER, by the state and the region Hauts de France.
  - •320 Research Engineers and Technicians
  - •9 Institutions
  - •5 Research organizations
  - •2 Technology Development Centers
  - •27 Laboratories

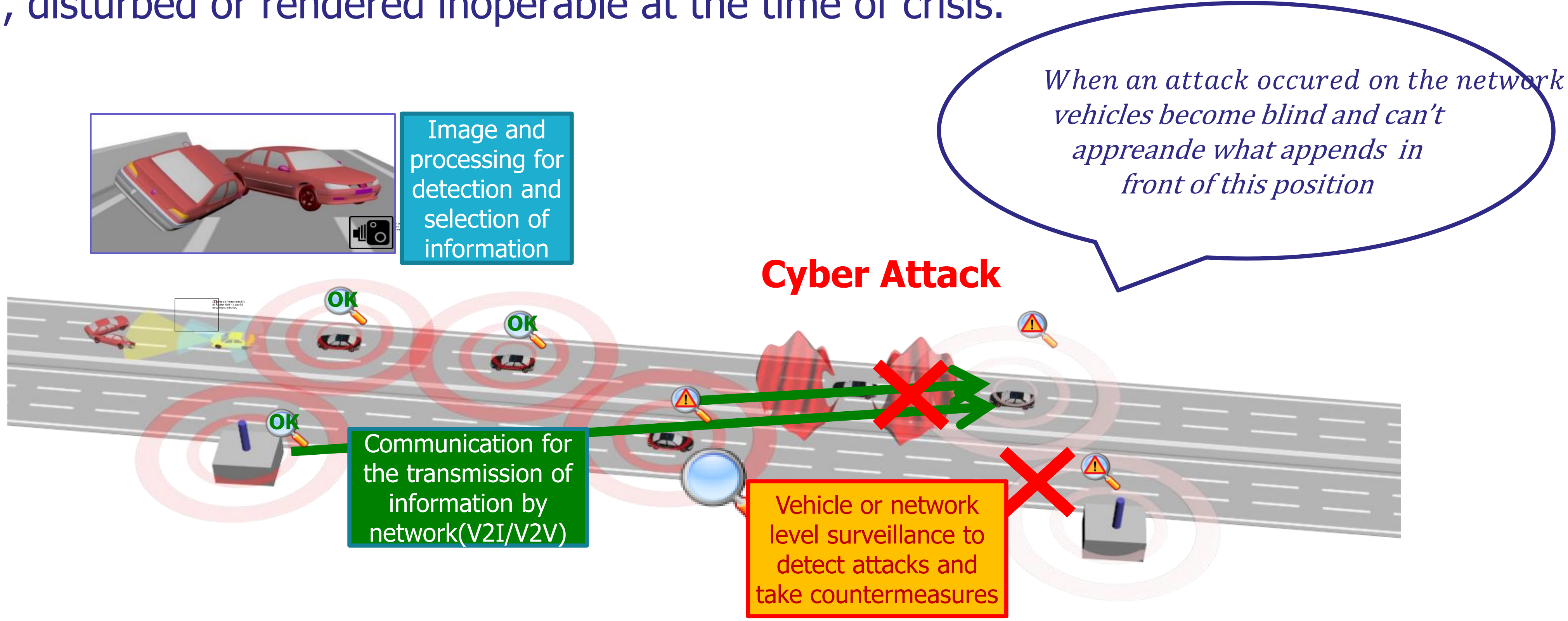


ELSAT 2020 by cisit
cnrs
Université de Valenciennes et du Hainaut-Cambrésis
Université de Lille 1 Sciences et Technologies
Université de Lille 3 Sciences Humaines et Sociales
Université d'Artois
ulco Université du Littoral Côte d'Opale
centralelille
Arts et Métiers ParisTech
IMT Lille Douai École Mines-Télécom IMT-Université de Lille
Centre Hospitalier Régional Universitaire de Lille
Cerema
inria inventeurs du monde numérique
ONERA The French Aerospace Lab
IFSTTAR

- Scientific objectives
  - •OS1- Human in transport and its mobility
  - •OS2 - Mobility Systems Optimization and Logistics
  - •OS3 - New materials and structural concepts
  - •OS4 - Dimensioning and performance of vehicle functions (**SECOURT)**
  - •OS5 - System of mobility and accessibility Sustainable at the crossroads of economic, legal and social
  - •OS6- ICT Innovations and Behavioral Changes

Introduction

The aim of the project is to study communication of information between vehicles and with the infrastructure to secure these communications and verify if they are deliberately attacked, disturbed or rendered inoperable at the time of crisis.



When an attack occured on the network vehicles become blind and can't appreande what appends in front of this position

Image and processing for detection and selection of information

Cyber Attack

Communication for the transmission of information by network(V2I/V2V)

Vehicle or network level surveillance to detect attacks and take countermeasures

Introduction

The aim of the project is to study communication of information between vehicles and with the infrastructure to secure these communications and verify if they are deliberately attacked, disturbed or rendered inoperable at the time of crisis.

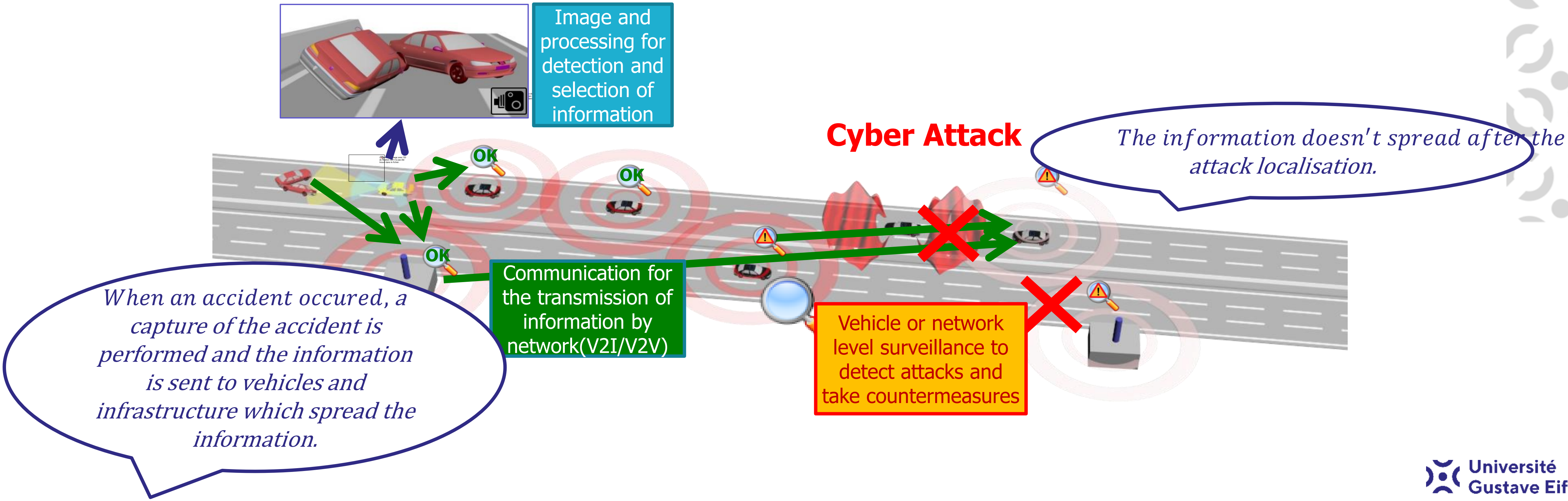


Image and processing for detection and selection of information

Cyber Attack

The information doesn't spread after the attack localisation.

When an accident occured, a capture of the accident is performed and the information is sent to vehicles and infrastructure which spread the information.

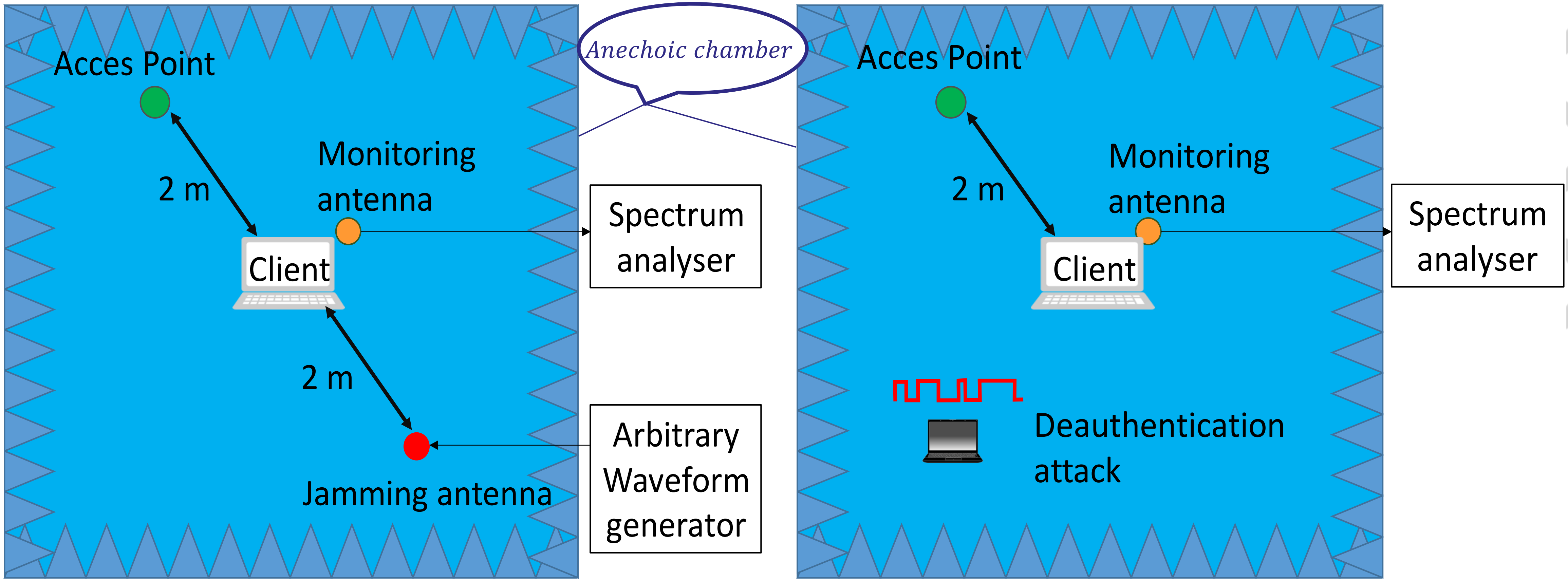
Communication for the transmission of information by network(V2I/V2V)

Vehicle or network level surveillance to detect attacks and take countermeasures

Implementation of jamming and de-authentication frame attacks

- Communication protocol considered:
  - IEEE 802.11n standard which uses the OFDM modulation scheme
  - Used channel was at 2,412GHz (channel 1)
- Spectrum analyzer configuration:
  - frequency range of 40 USD
  - Center frequency of 2,412 GHz
  - Resolution bandwidth of 100 kHz
  - Scan time of 38,2 µs
  - 1601 points per spectra
- Considered attack:
  - Jamming attacks
  - Deauthentication attacks
- Jamming configuration:
  - interference signal that sweeps a frequency band [f1,f2] over a period of time T
  - a frequency band between [2.4; 2.5] GHz in 10µs

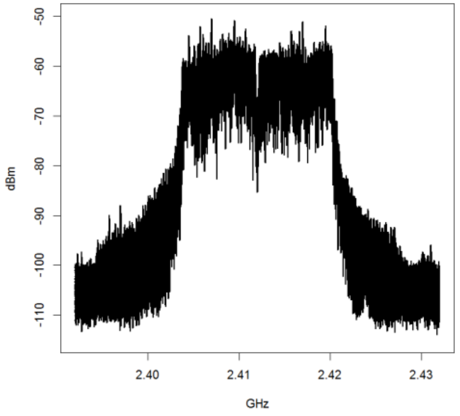
Implementation of jamming and de-authentication frame attacks



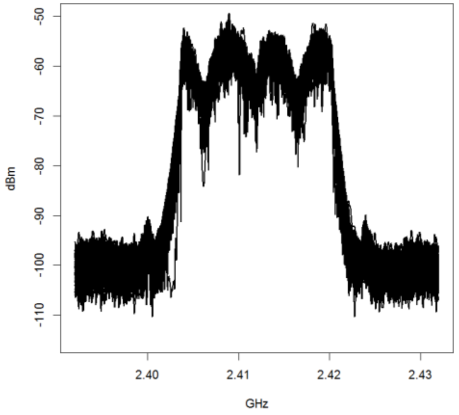
Configuration of the Jamming attack experiments.

Configuration of the De authentication attack experiments.

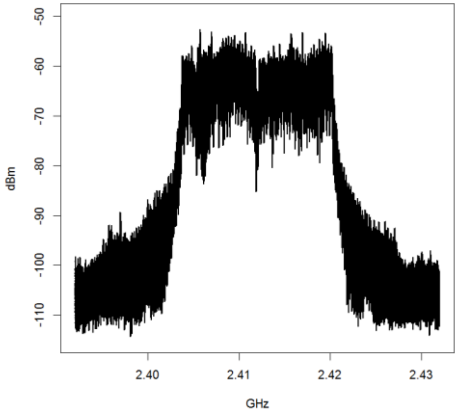
Implementation of jamming and de-authentication frame attacks



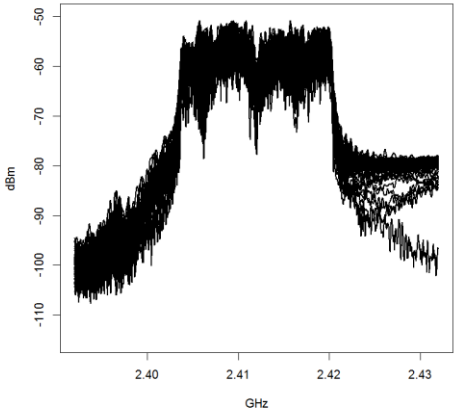
(1) Wi-Fi only



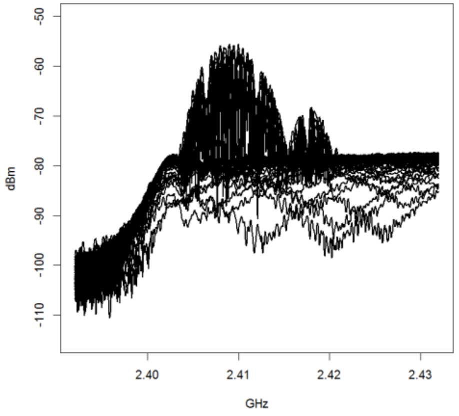
(2) Wi-Fi in the presence of absorbers



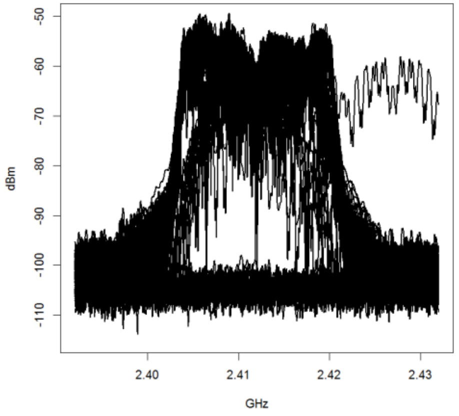
(3) Wi-Fi under jamming without effect



(4) Wi-Fi under jamming with slight effect



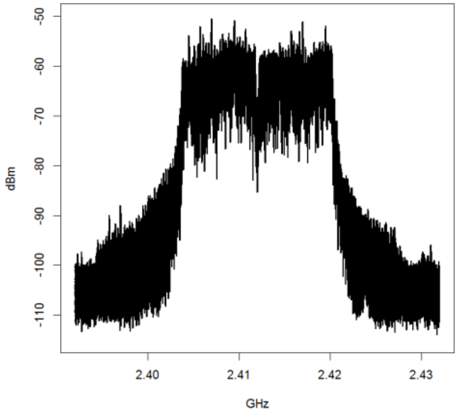
(5) Wi-Fi under jamming at the limit of loss of connection



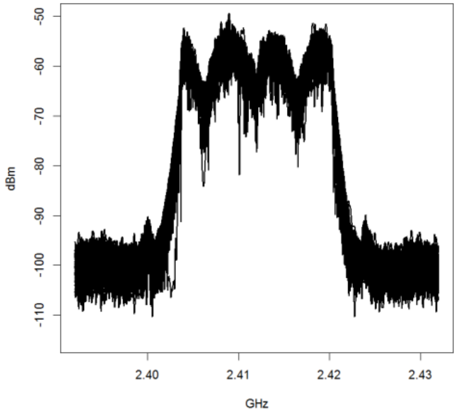
(6) Wi-Fi under de-authentication attack

Université
Gustave Eiffel

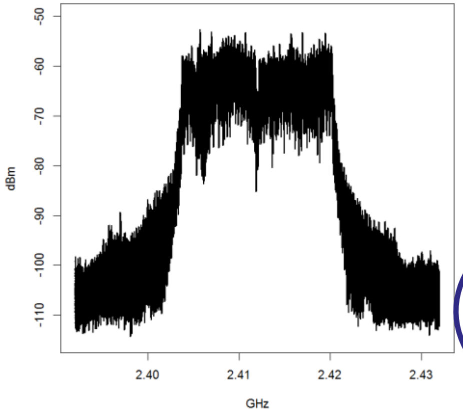
Implementation of jamming and de-authentication frame attacks



(1) Wi-Fi only

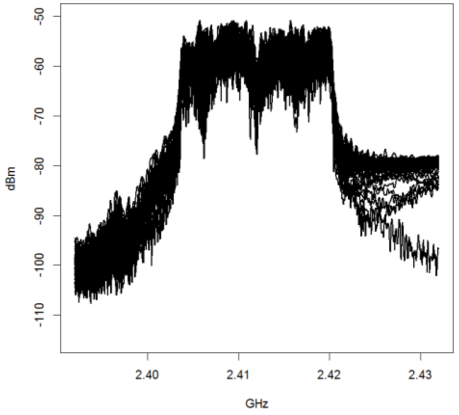


(2) Wi-Fi in the presence of absorbers

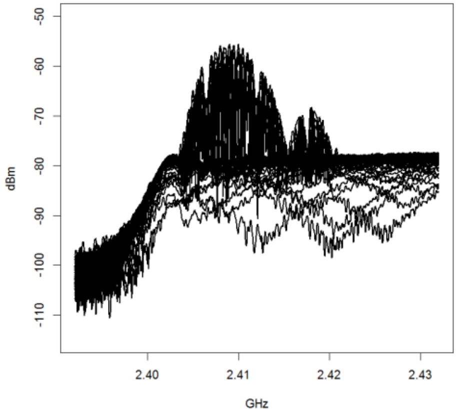


(3) Wi-Fi under jamming without effect

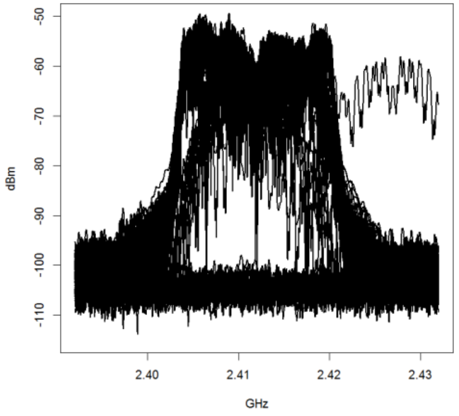
On these figures, 99 spectra of each configuration are represented



(4) Wi-Fi under jamming with slight effect



(5) Wi-Fi under jamming at the limit of loss of connection



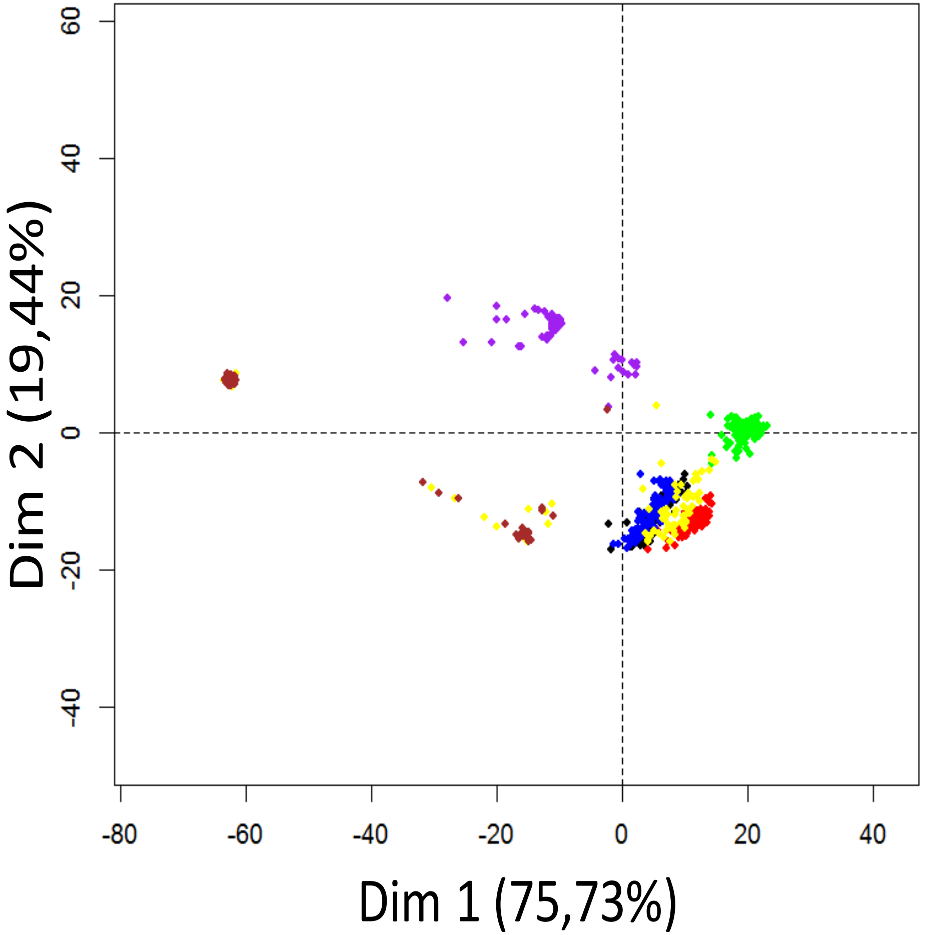
(6) Wi-Fi under de-authentication attack

Université Gustave Eiffel

Principal components analysis representation

- Dim 1 and Dim 2 correspond to the Eigen vector associated to the two highest Eigen values obtained from the correlation matrix.

- 75,73% and 19,44% are the percentage of the data variability explain respectively by the axes Dim 1 and Dim 2



Wi-Fi

With absorbing material

Low jamming – no impact

Jamming with small impact

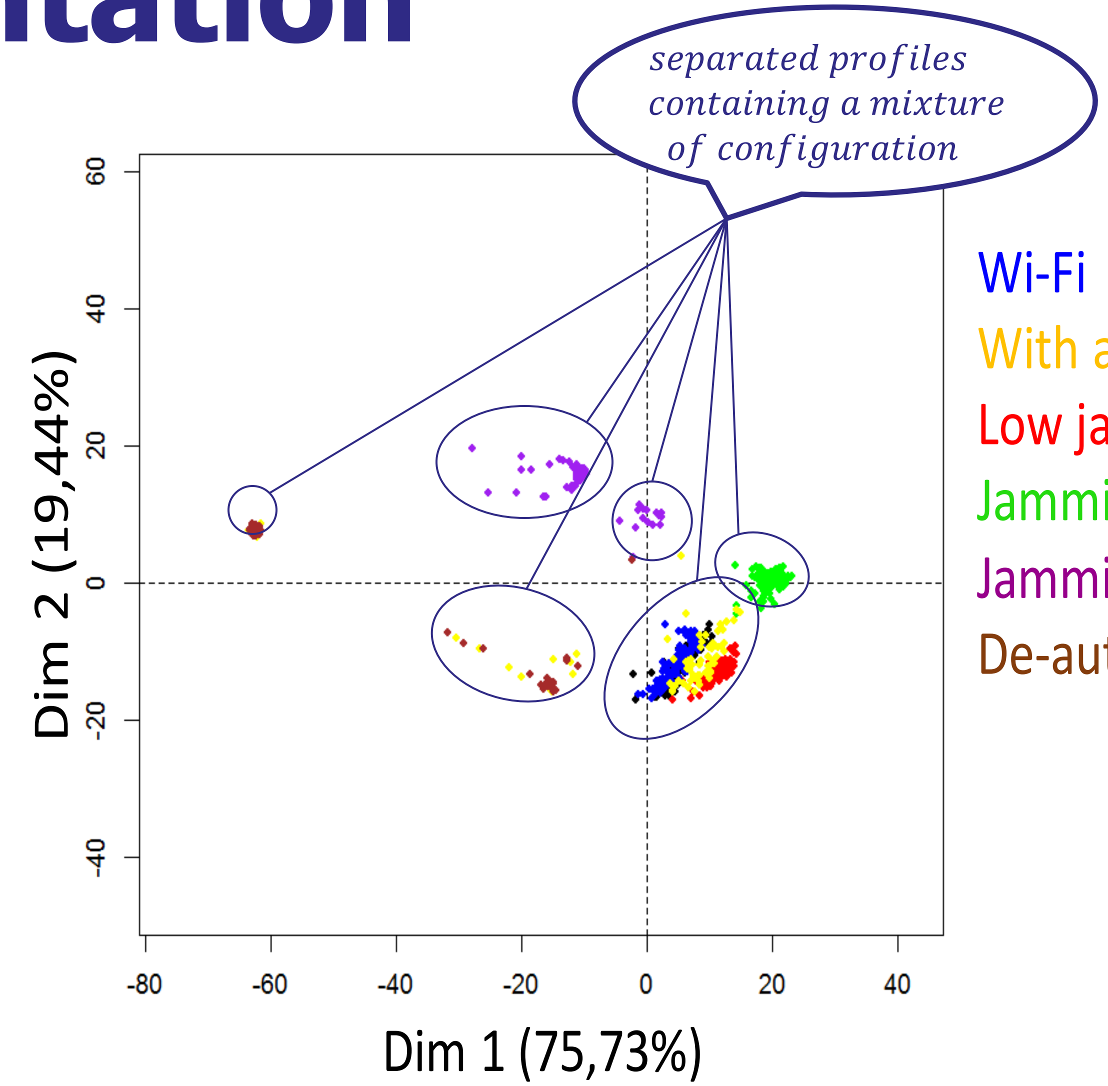
Jamming with significant impact

De-authentication attack

Principal components analysis representation

- Dim 1 and Dim 2 correspond to the Eigen vector associated to the two highest Eigen values obtained from the correlation matrix.

- 75,73% and 19,44% are the percentage of the data variability explain respectively by the axes Dim 1 and Dim 2



separated profiles containing a mixture of configuration

Wi-Fi

With absorbing material

Low jamming – no impact

Jamming with small impact

Jamming with significant impact

De-authentication attack

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$

Algorithm

```
Required: Online data source $X: \rightarrow X_t$
Required: Parameter $\lambda, \eta, \nu, \epsilon_{th}$
Required: Tresholds $\tau, A, N_c, T$
Initialise: $t = 0;\ f_0 = f_0^t = 0;\ C_0 := C_0^t = \emptyset$
While Acquisition $X_t$ do
    Evaluate Kernel Similarity function: $\mu\Phi_{t.m}$
    Determine $\Omega^{win}$
    if Case 1: $\mathrm{card}(\Omega^{win}) = 0$ then
        Creation procedure
    end
    if Case 2: $\mathrm{card}(\Omega^{win}) = 1$ then
        Update procedure
    end
    if Case 3: $\mathrm{card}(\Omega^{win}) > 1$ then
        Fusion procedure
    end
    if  $\mathrm{t} = \mathrm{k}.\mathrm{T}\ (\mathrm{k} \in N)$ then
        Elimination procedure
    end
end
```

t the time

λ the inverse kernel width

η the learning rate

ν the fraction of margin support vector

ϵ_{th} the acceptance treshold

τ the number of terms which will trancate the kernel expension

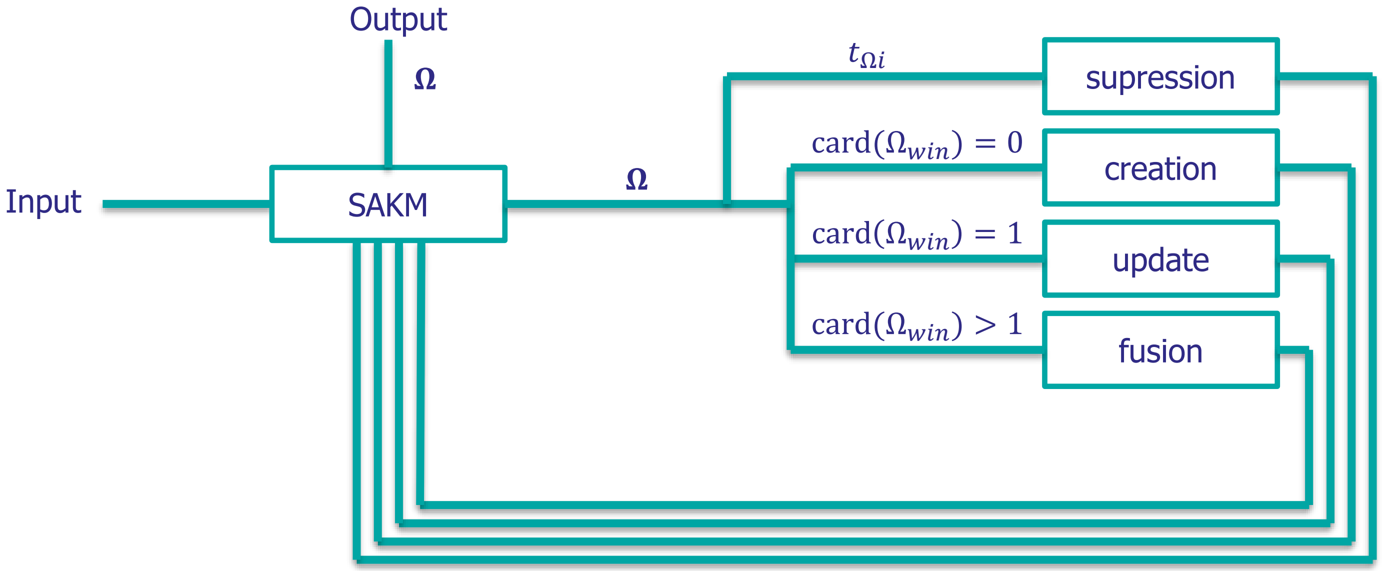
N_c number under which a cluster is inconsistent

T the time after which a cluster with a size lower than N_c is delete

Ω^{win} number of wining cluster

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$

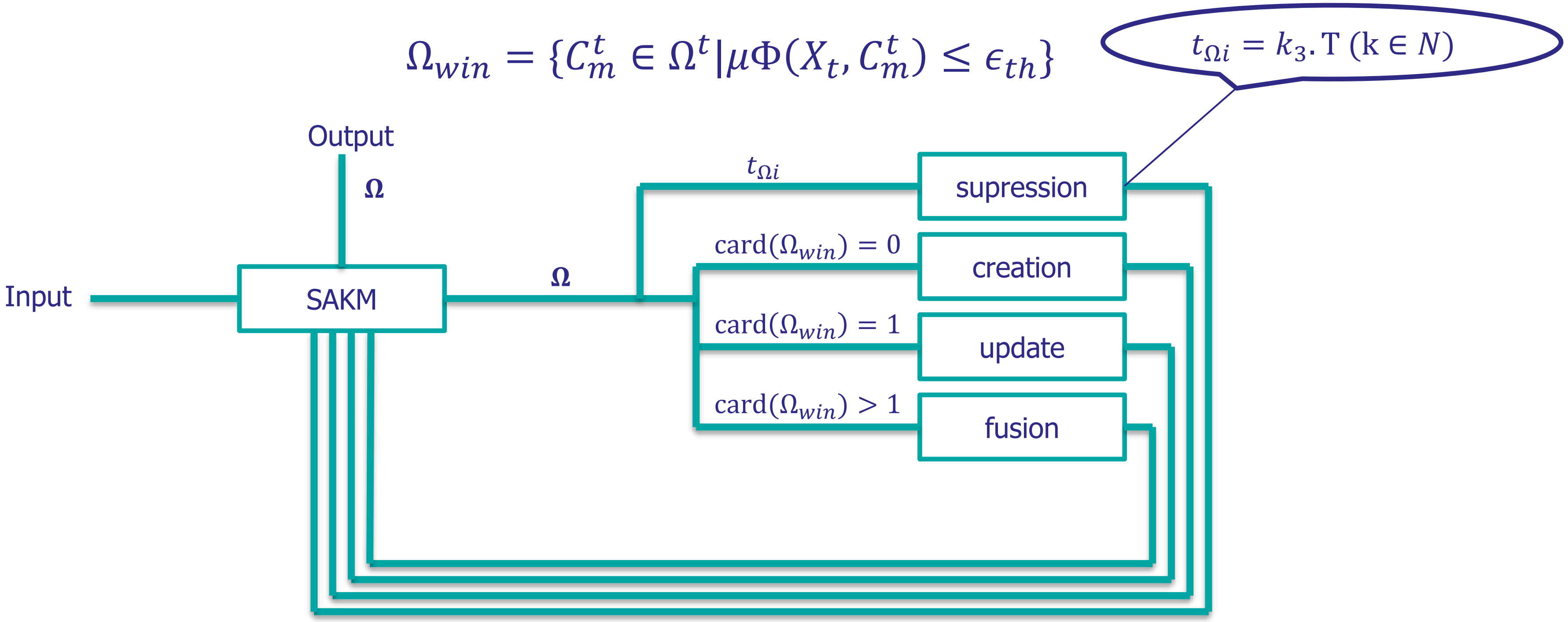


- Limite of SAKM:
  - $\exists \int_{R^p} f(x)\, dx \; \forall \; x \in R^p \; then \; N_c \rightarrow 1$
  - $\nexists \int_{R^p} f(x)\, dx \; \forall \; x \in R^p \; then \; N_c \rightarrow N_{SI}$

  where N_{SI} is the number of interval in which $\int f(x)\, dx$ is defined

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$


$t_{\Omega i} = k_3.\mathrm{T}\ (\mathrm{k} \in N)$
Output
Ω
Input
SAKM
Ω
$t_{\Omega i}$
supression
$\mathrm{card}(\Omega_{win}) = 0$
creation
$\mathrm{card}(\Omega_{win}) = 1$
update
$\mathrm{card}(\Omega_{win}) > 1$
fusion

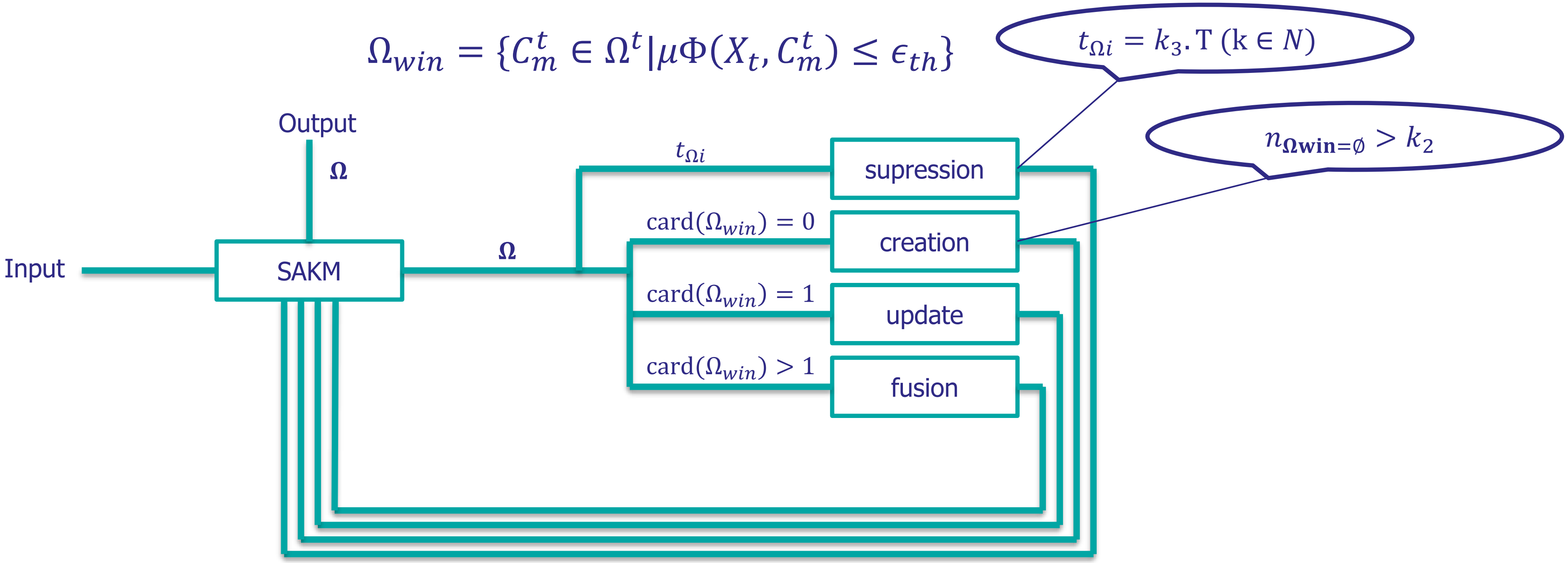
- Limite of SAKM:
  - $\exists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow 1$
  - $\nexists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow N_{SI}$

where N_{SI} is the number of interval in which $\int f(x)\, dx$ is defined

Université Gustave Eiffel

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$



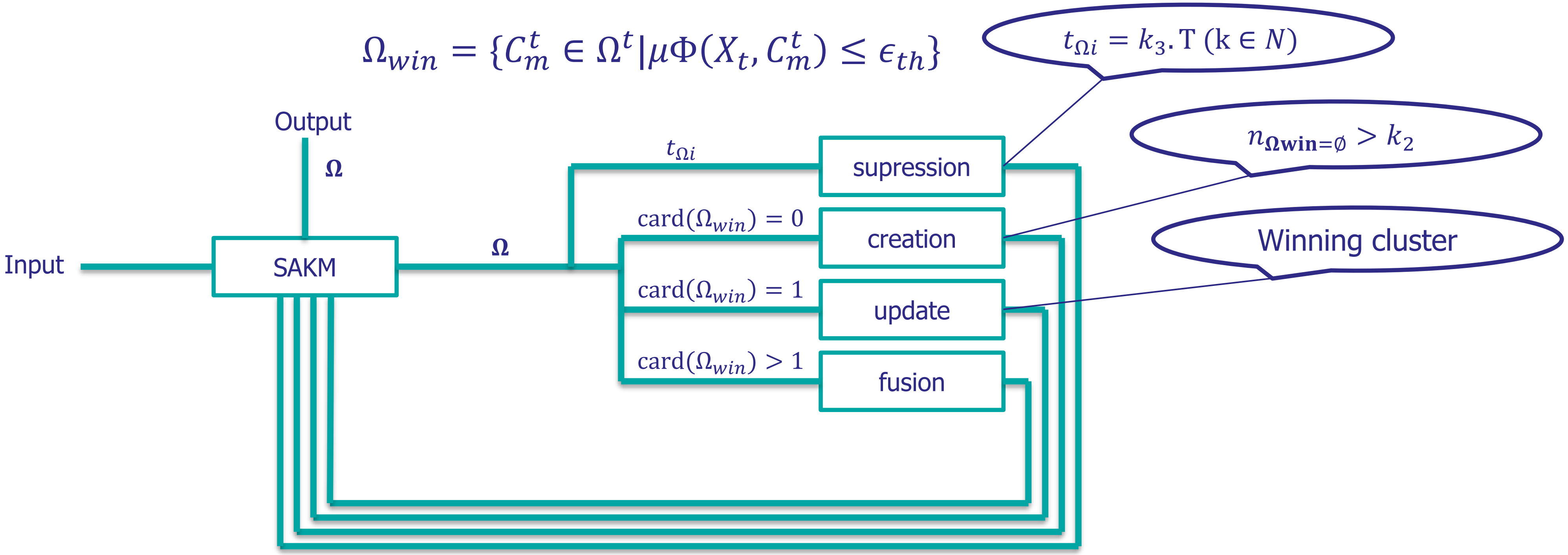
$t_{\Omega i} = k_3.\mathrm{T}\ (\mathrm{k} \in N)$
$n_{\boldsymbol{\Omega}\mathbf{win}=\emptyset} > k_2$
Output
$\boldsymbol{\Omega}$
Input
SAKM
$\boldsymbol{\Omega}$
$t_{\Omega i}$
supression
$\mathrm{card}(\Omega_{win}) = 0$
creation
$\mathrm{card}(\Omega_{win}) = 1$
update
$\mathrm{card}(\Omega_{win}) > 1$
fusion

- Limite of SAKM:
  - $\exists \int_{R^p} f(x)\,dx\ \forall\ x \in R^p\ then\ N_c \rightarrow 1$
  - $\nexists \int_{R^p} f(x)\,dx\ \forall\ x \in R^p\ then\ N_c \rightarrow N_{SI}$

where N_{SI} is the number of interval in which $\int f(x)\,dx$ is defined

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$



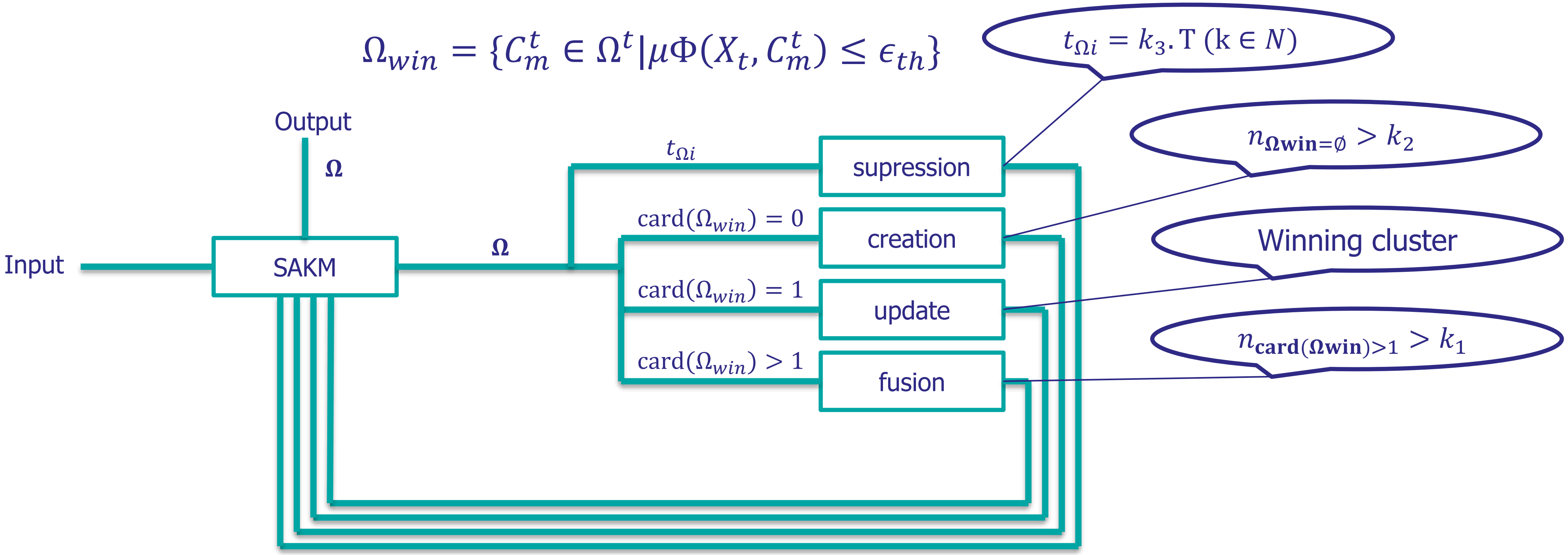
$t_{\Omega i} = k_3.\mathrm{T}\ (\mathrm{k} \in N)$
$n_{\mathbf{\Omega win}=\emptyset} > k_2$
Winning cluster
Output
$\mathbf{\Omega}$
Input
SAKM
$\mathbf{\Omega}$
$t_{\Omega i}$
supression
$\mathrm{card}(\Omega_{win}) = 0$
creation
$\mathrm{card}(\Omega_{win}) = 1$
update
$\mathrm{card}(\Omega_{win}) > 1$
fusion

- Limite of SAKM:
  - $\exists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow 1$
  - $\nexists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow N_{SI}$

where N_{SI} is the number of interval in which $\int f(x)\, dx$ is defined

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$



$t_{\Omega i} = k_3.\mathrm{T}\ (\mathrm{k} \in N)$
$n_{\mathbf{\Omega win=\emptyset}} > k_2$
Winning cluster
$n_{\mathbf{card(\Omega win)>1}} > k_1$
Output
Ω
Input
SAKM
Ω
$t_{\Omega i}$
supression
$\mathrm{card}(\Omega_{win}) = 0$
creation
$\mathrm{card}(\Omega_{win}) = 1$
update
$\mathrm{card}(\Omega_{win}) > 1$
fusion

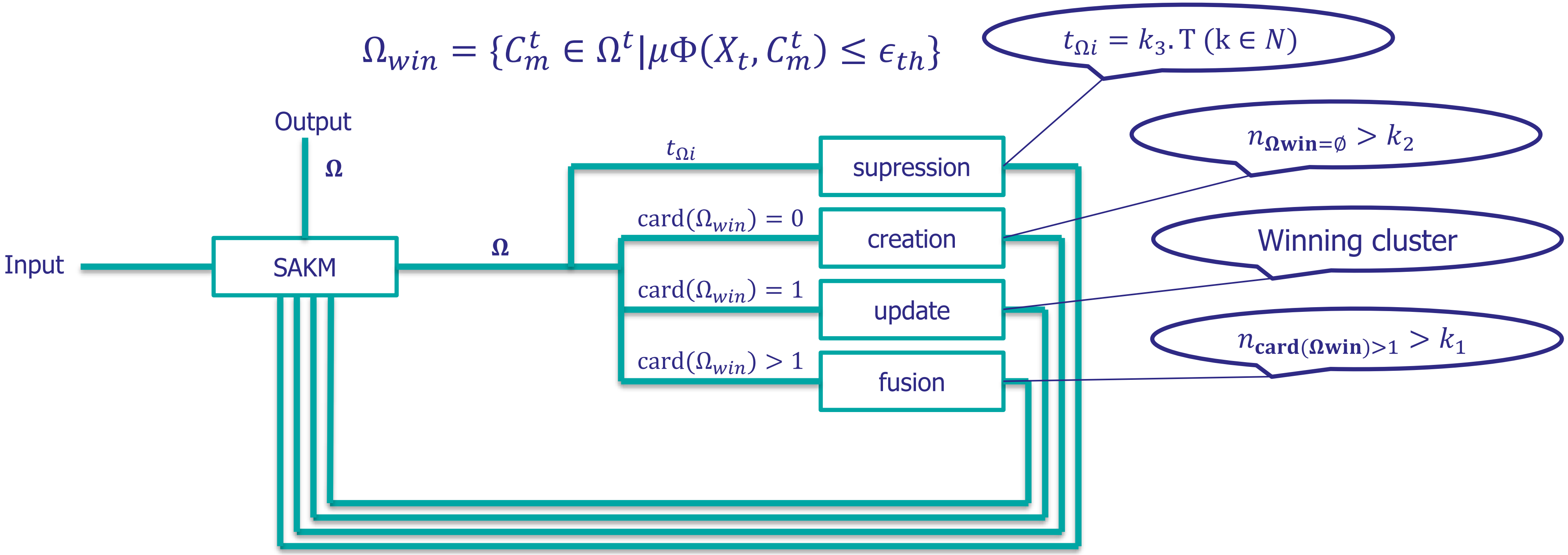
➢ Limite of SAKM:

- $\exists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow 1$
- $\nexists \int_{R^p} f(x)\, dx\ \forall\ x \in R^p\ then\ N_c \rightarrow N_{SI}$

where N_{SI} is the number of interval in which $\int f(x)\, dx$ is defined

Self Adaptative Kernel Machine

$$\Omega_{win} = \{C_m^t \in \Omega^t | \mu\Phi(X_t, C_m^t) \leq \epsilon_{th}\}$$



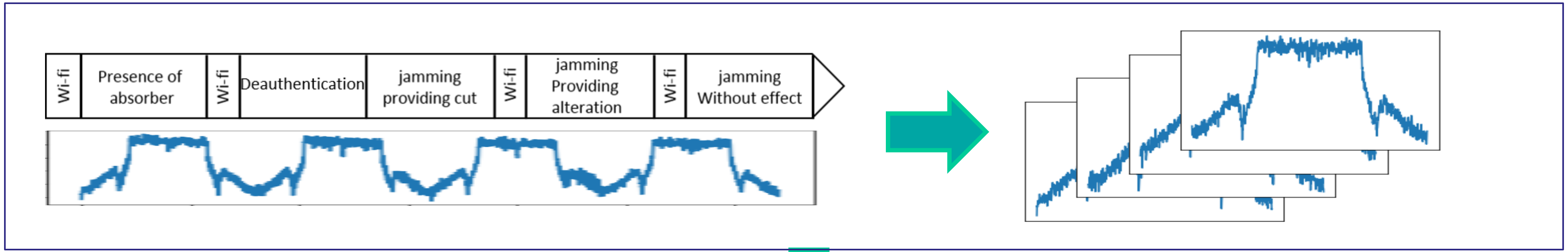
$t_{\Omega i} = k_3.\mathrm{T}\ (\mathrm{k} \in N)$
Output
Ω
Input
SAKM
Ω
$t_{\Omega i}$
supression
$\mathrm{card}(\Omega_{win}) = 0$
creation
$\mathrm{card}(\Omega_{win}) = 1$
update
$\mathrm{card}(\Omega_{win}) > 1$
fusion
$n_{\Omega \mathbf{win}=\emptyset} > k_2$
Winning cluster
$n_{\mathbf{card}(\Omega\mathbf{win})>1} > k_1$

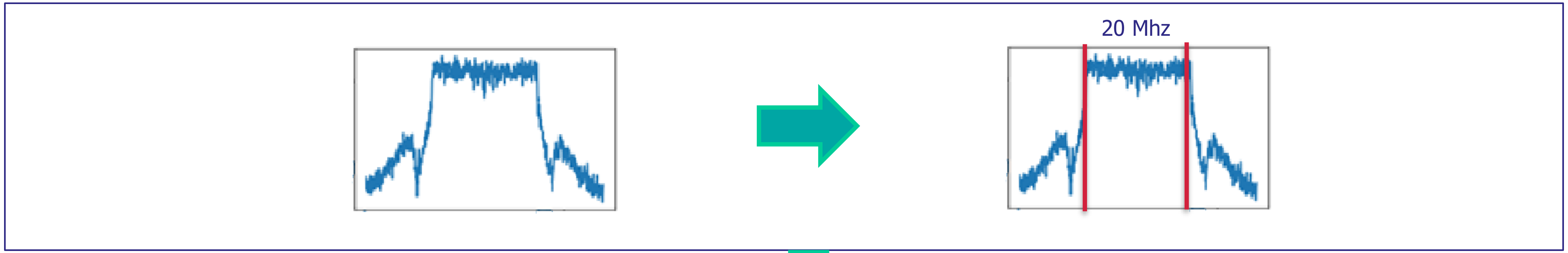
- Limite of SAKM:
  - $\exists \int_{R^p} f(x)\,dx\ \forall\ x \in R^p\ then\ N_c \rightarrow 1$
  - $\nexists \int_{R^p} f(x)\,dx\ \forall\ x \in R^p\ then\ N_c \rightarrow N_{SI}$

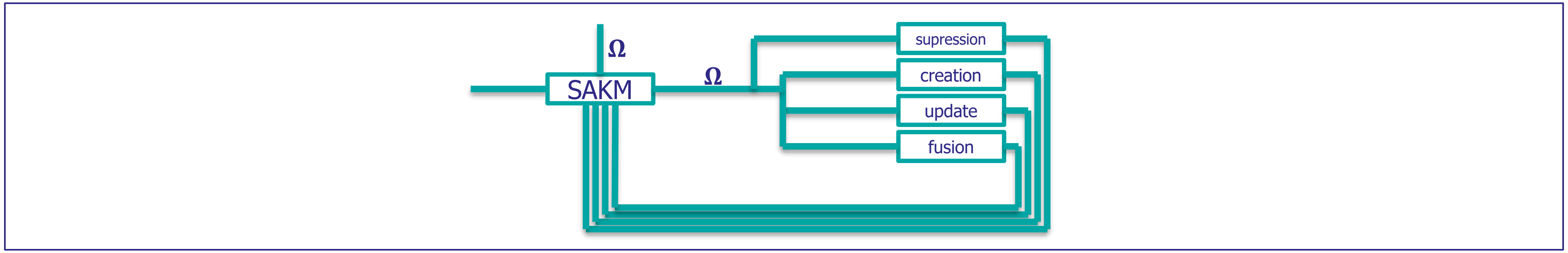
Configuration of the separated profiles

where N_{SI} is the number of interval in which $\int f(x)\,dx$ is defined

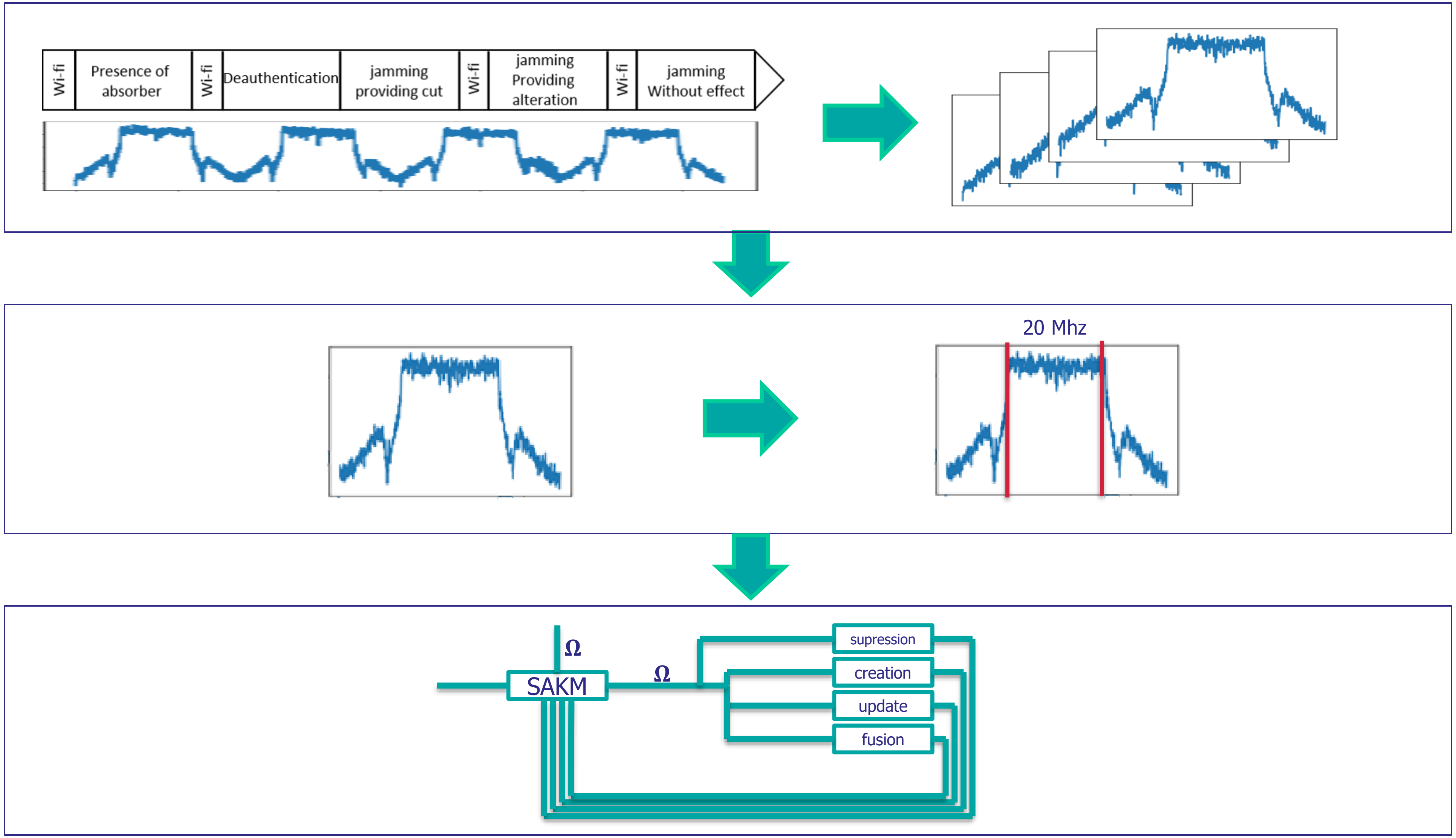
Self Adaptative Kernel Machine





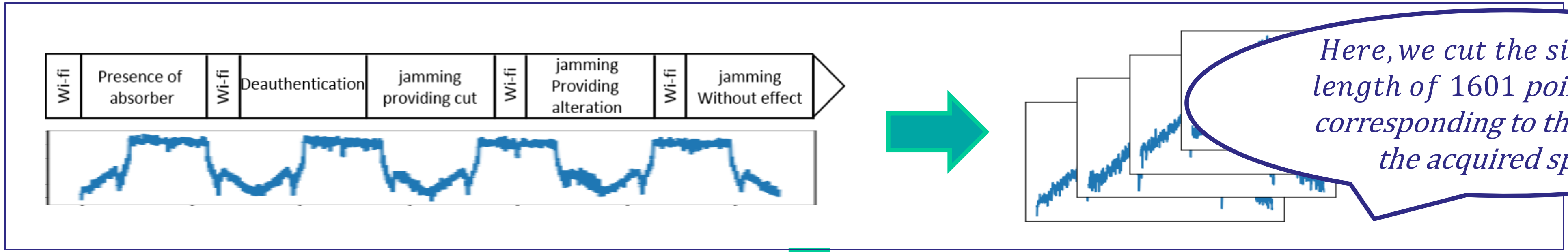


Self Adaptative Kernel Machine

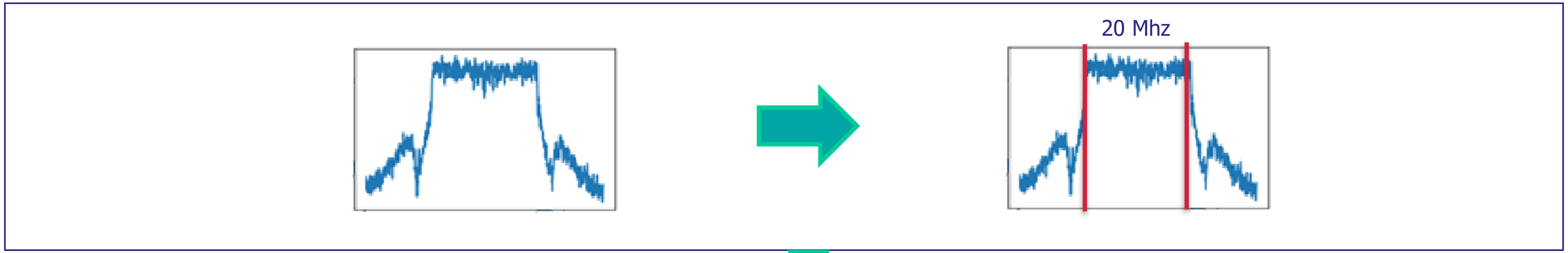


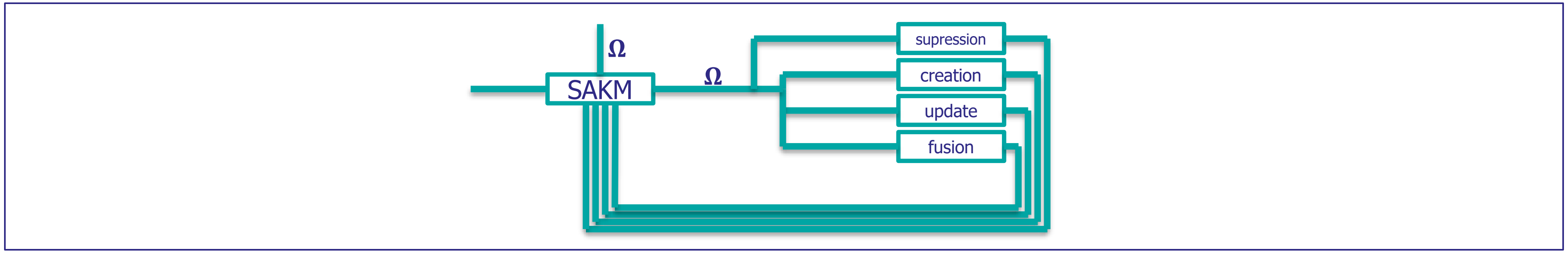
Université Gustave Eiffel

Self Adaptative Kernel Machine

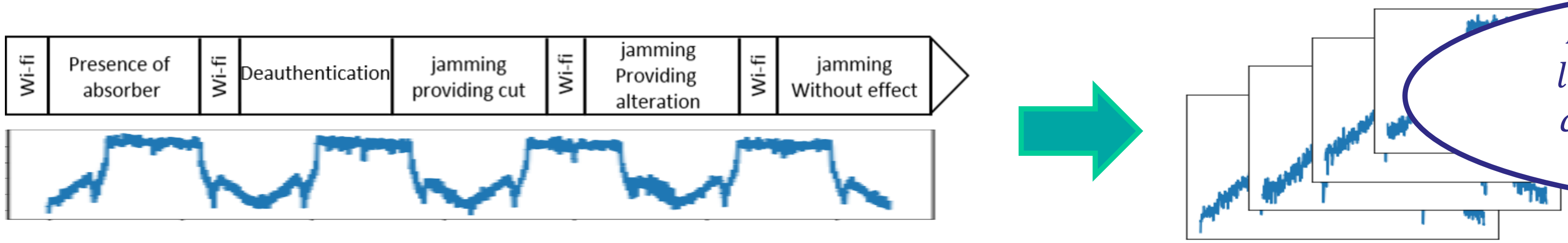


Here, we cut the signal in a length of 1601 points. That's corresponding to the length of the acquired spectra

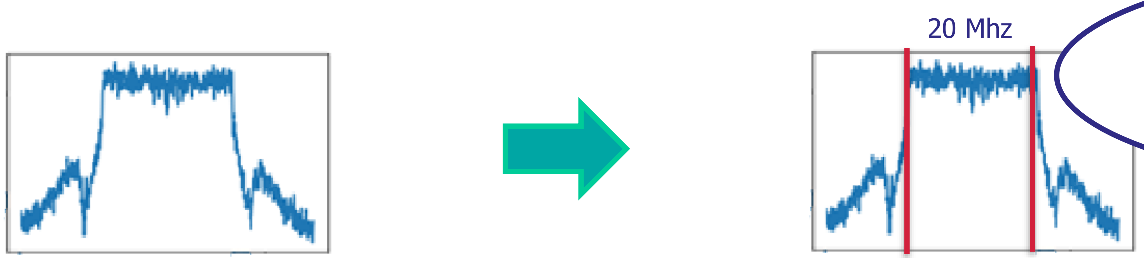




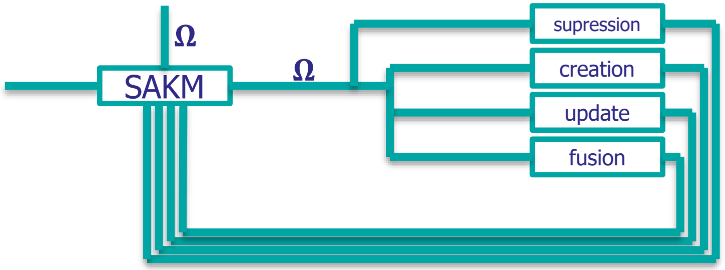
Self Adaptative Kernel Machine



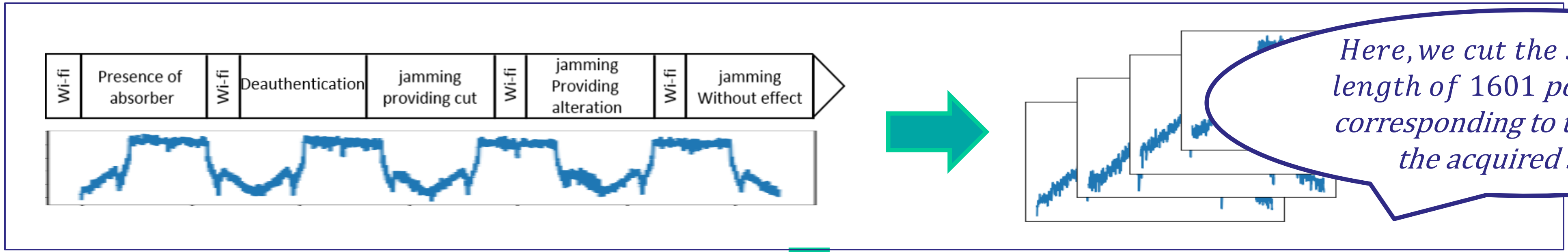
Here,we cut the signal in a length of 1601 points. That’s corresponding to the length of the acquired spectra



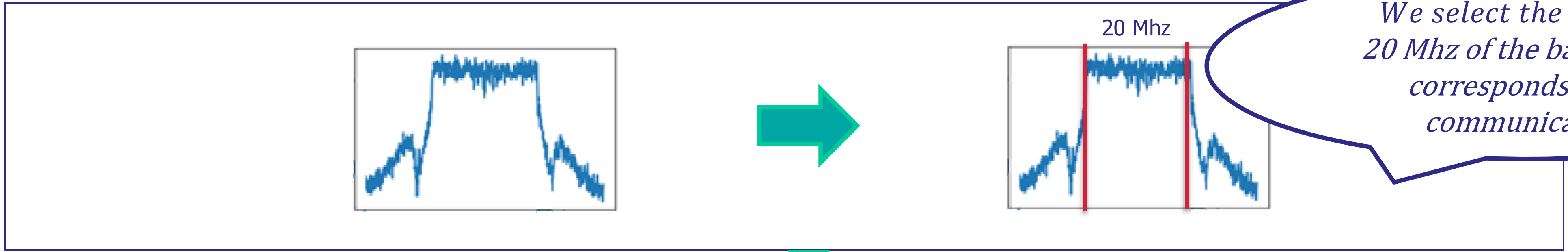
We select the central 20 Mhz of the band which corresponds to the communication.



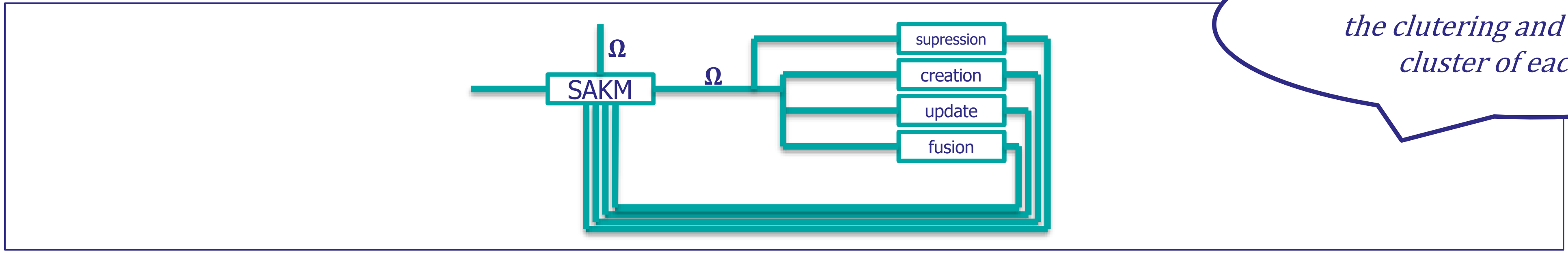
Self Adaptative Kernel Machine



Here, we cut the signal in a length of 1601 points. That's corresponding to the length of the acquired spectra

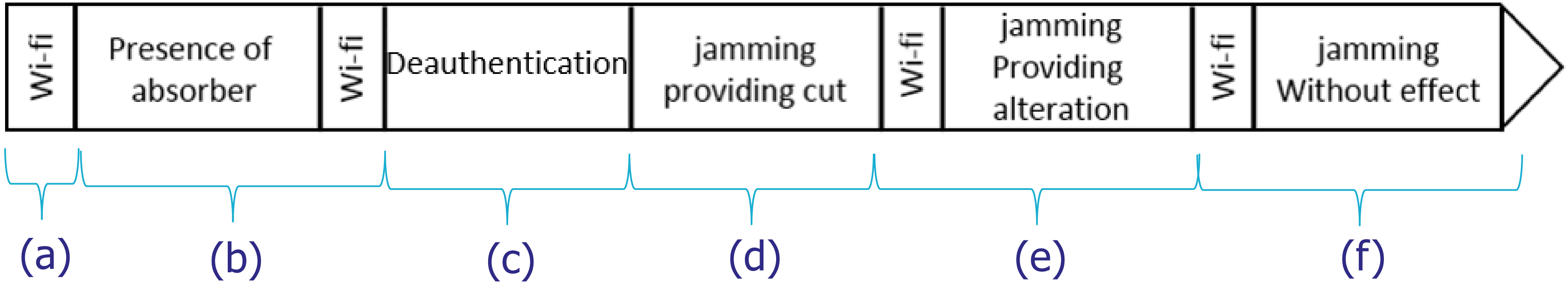


We select the central 20 Mhz of the band which corresponds to the communication.



We run SAKM on the data to perform the clutering and estimate the cluster of each signal.

Results



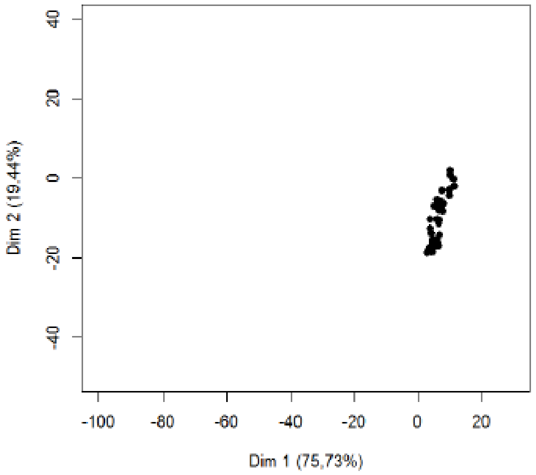
- The timeline represents the different configurations in time applied for the acquisition.

- In the following, we visualize the communication after each step (a), (b), (c), (d), € and (f).

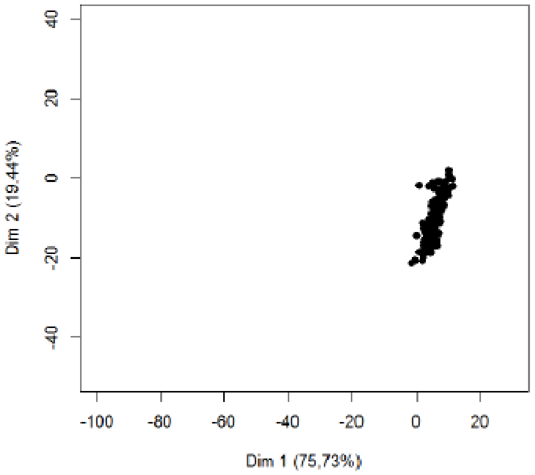
- To visualize the classification we report the data on the two Eigen vectors associated to the two highest Eigen values obtained from the correlation matrix of the central 20Mhz of the communication band.

Results

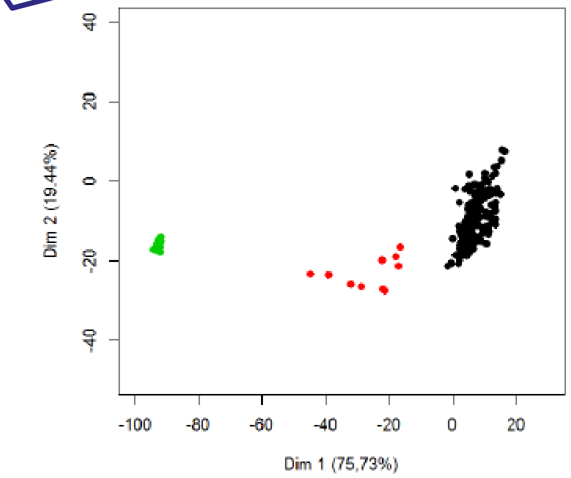
Here the eigen vectors are obtained on the central 20Mhz of the canal band



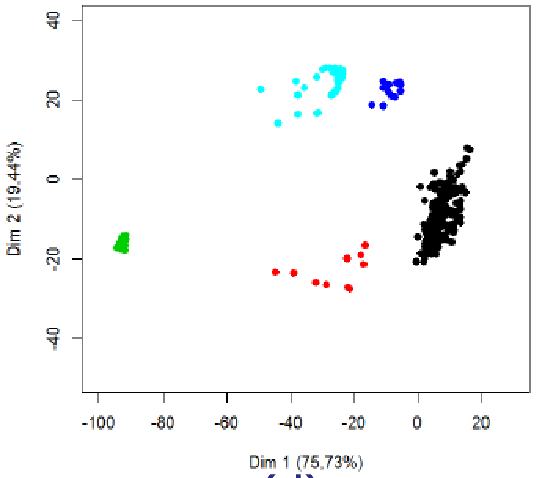
(a)



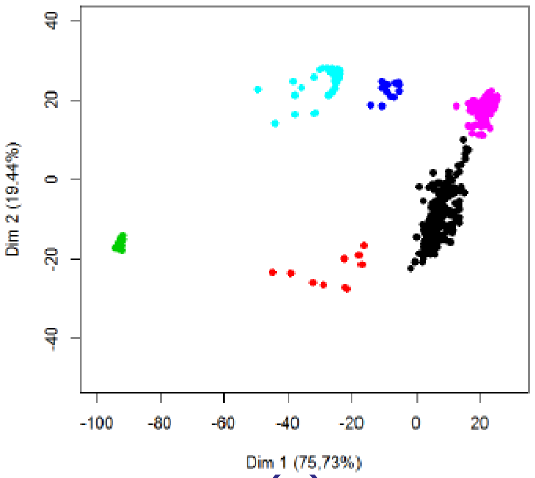
(b)



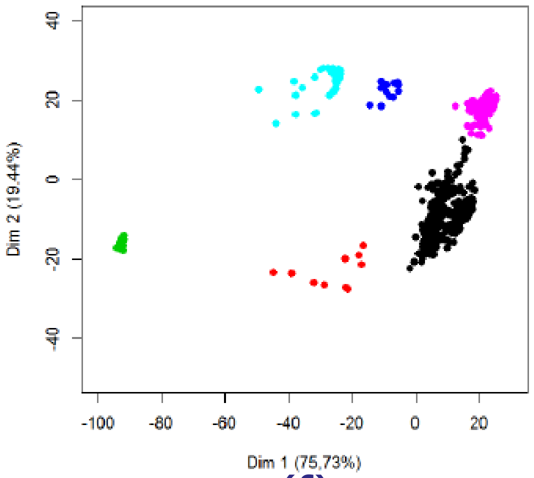
(c)



(d)

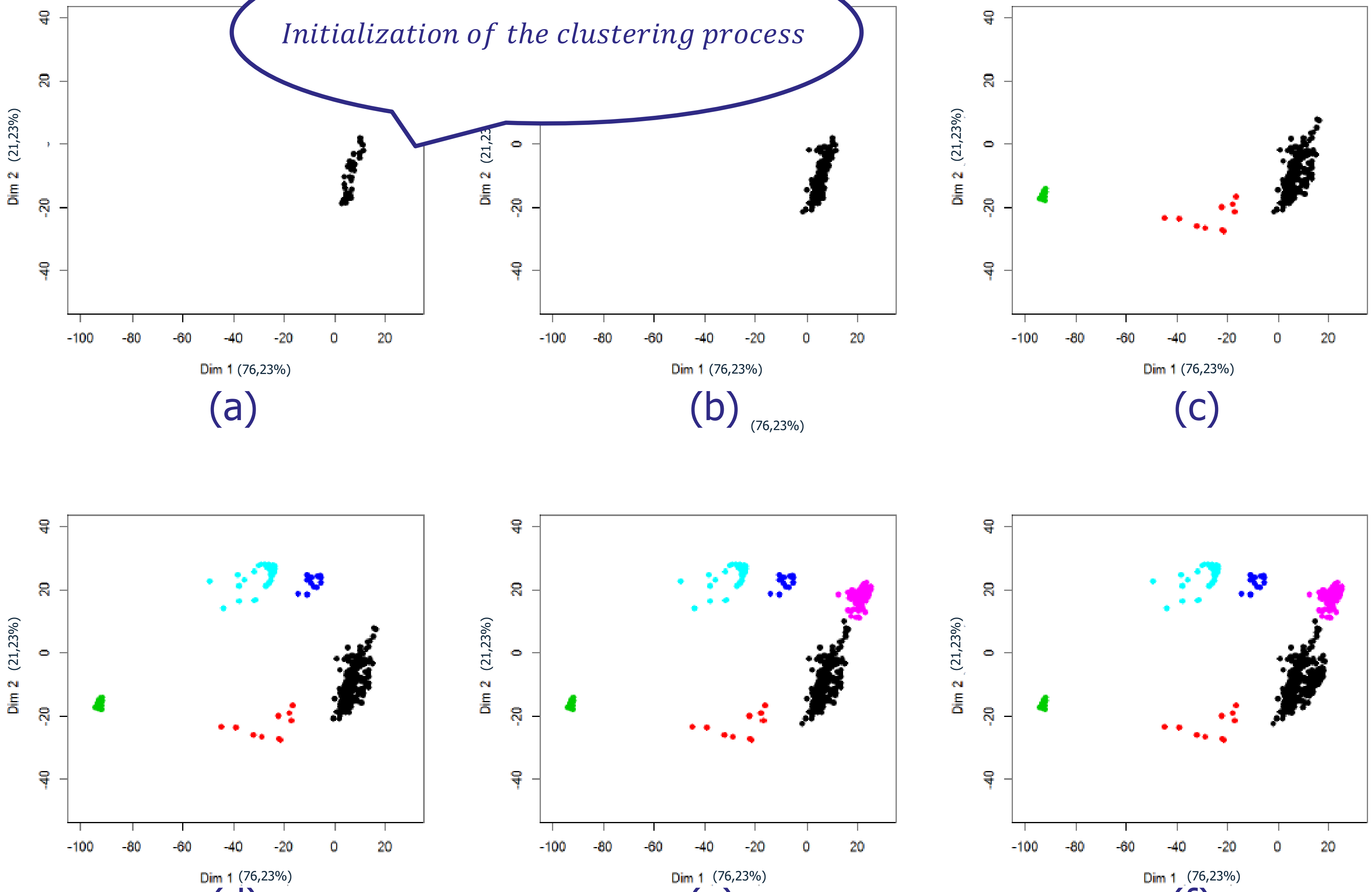


(e)



(f)

Results



Initialization of the clustering process

(a)

(b) (76,23%)

(c)

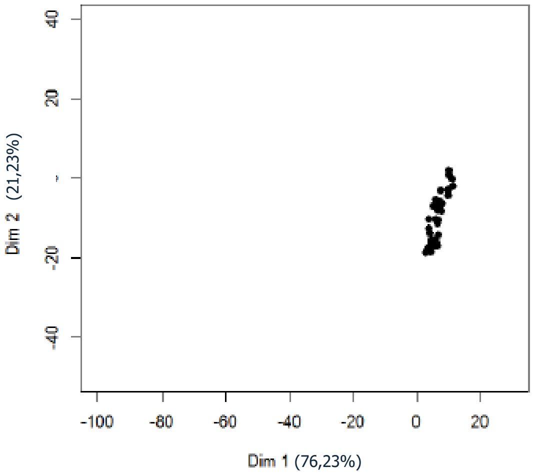
(d)

(e)

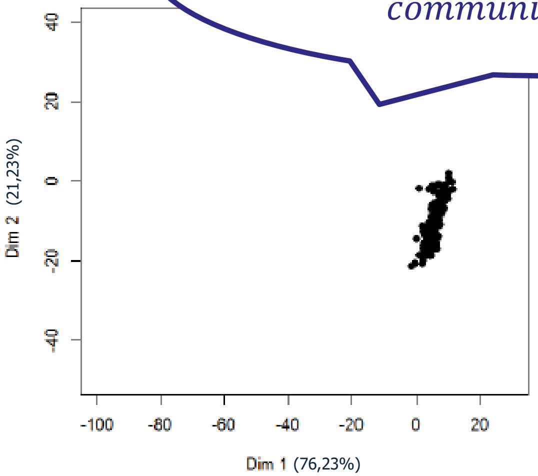
(f)

Results

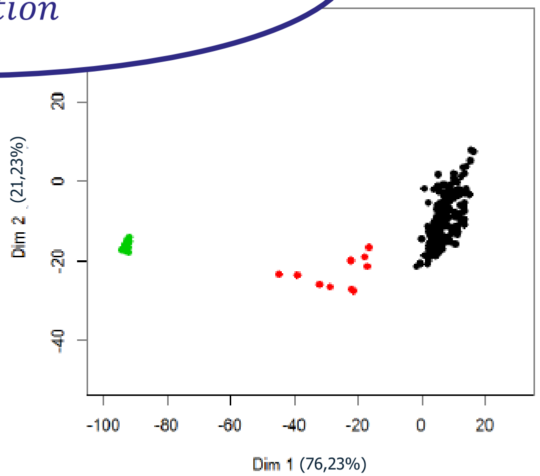
The presence of absorber doesn't impact significantly the communication



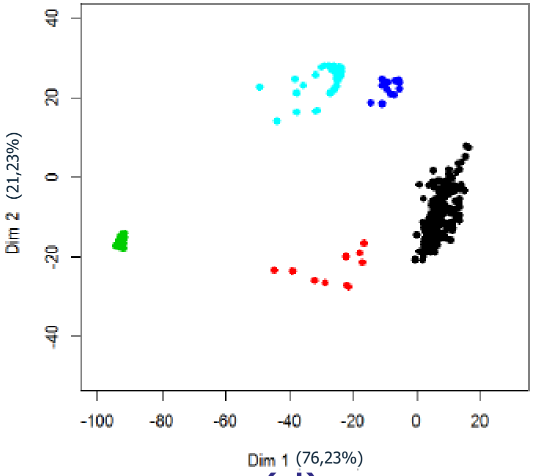
(a)



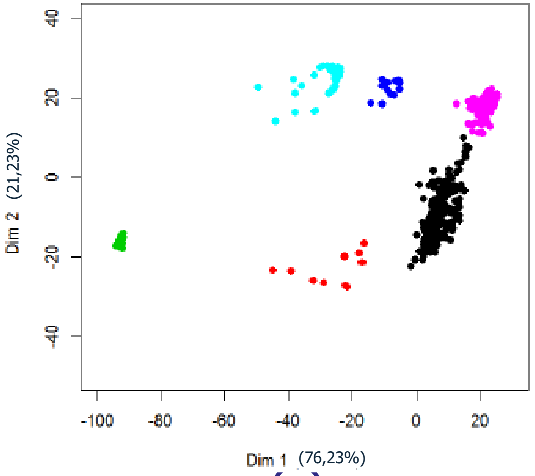
(b) (76,23%)



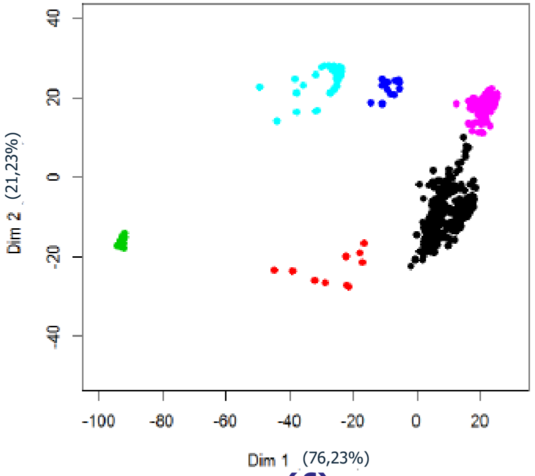
(c)



(d)

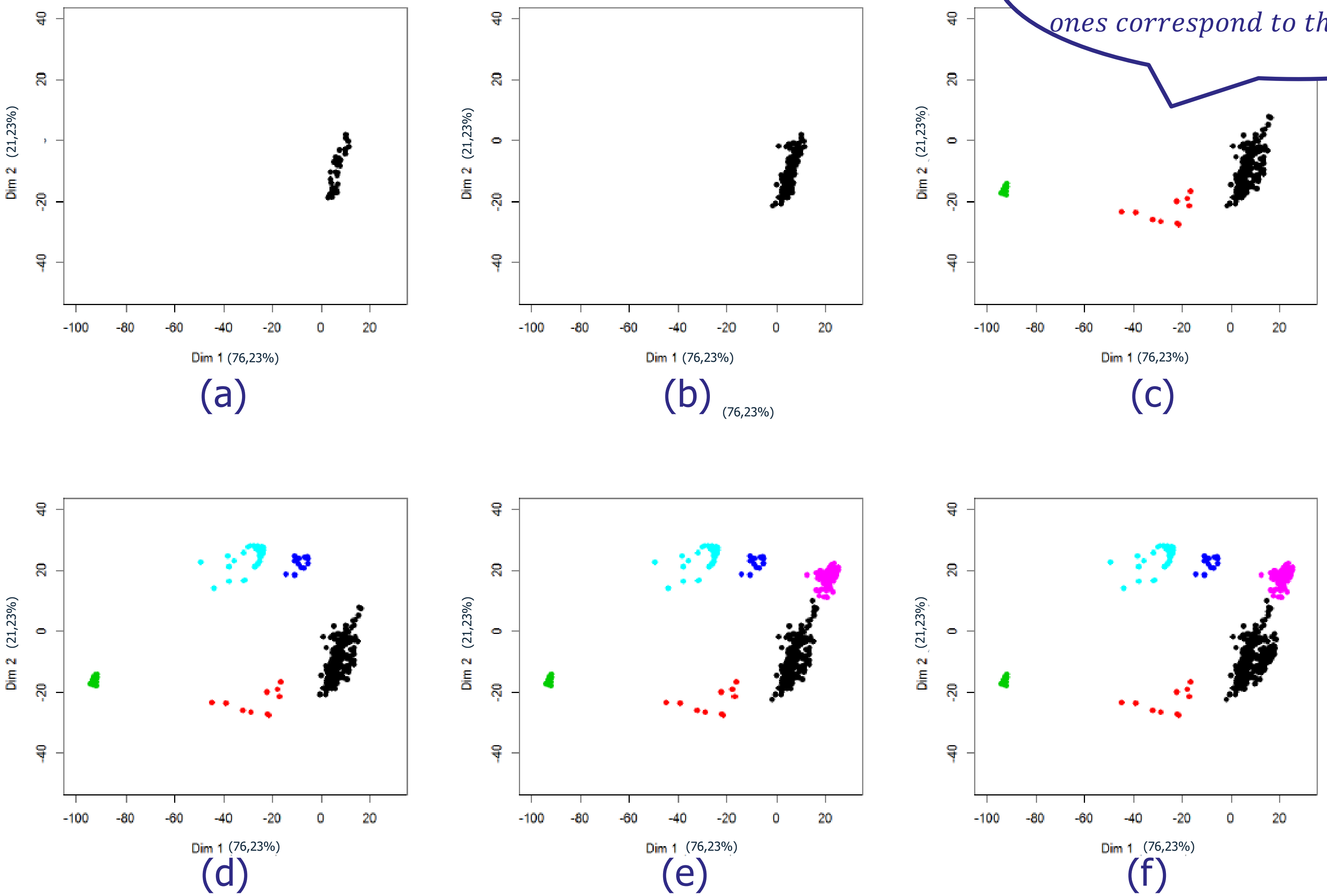


(e)



(f)

Results



(a)

(b)

(c)

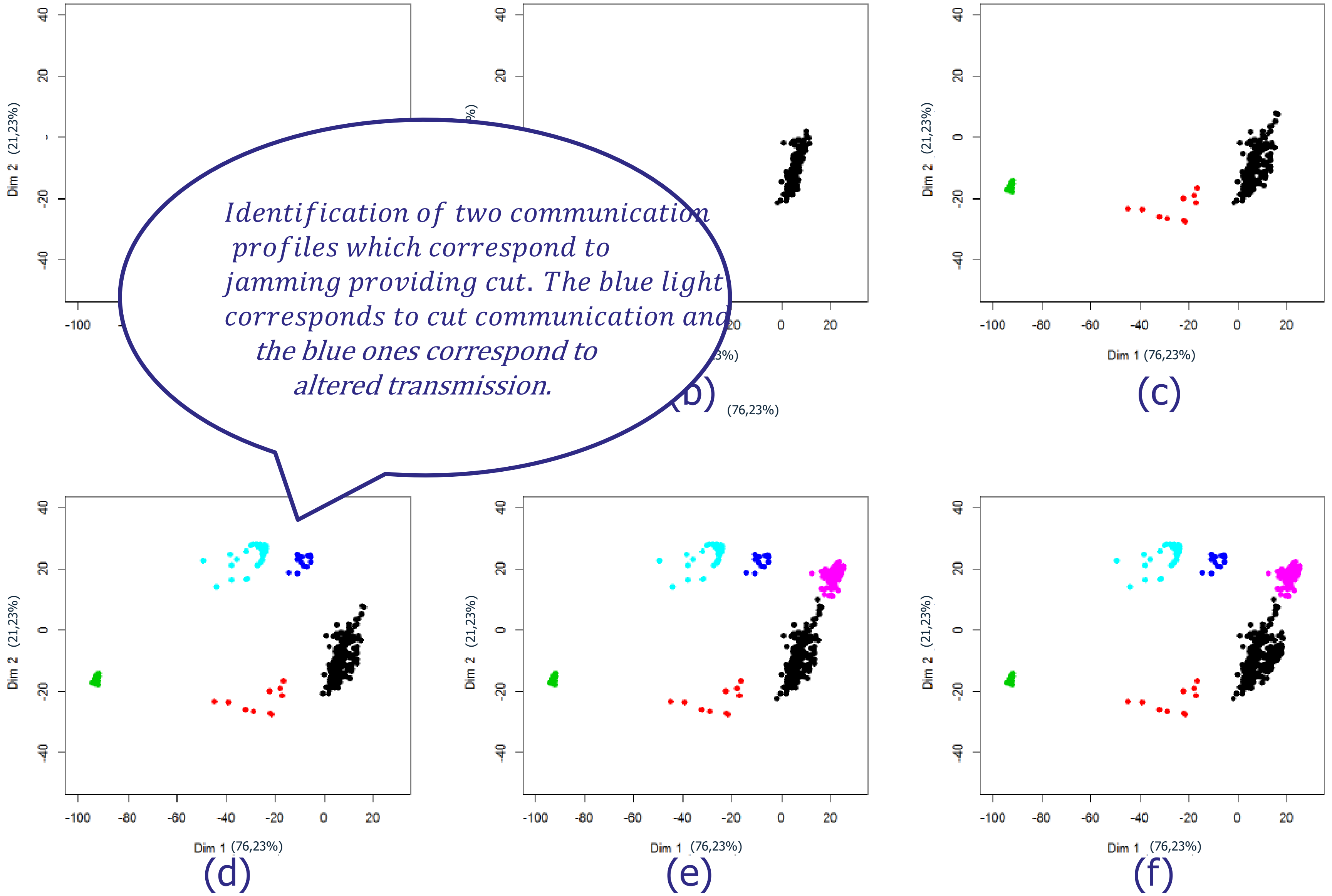
(d)

(e)

(f)

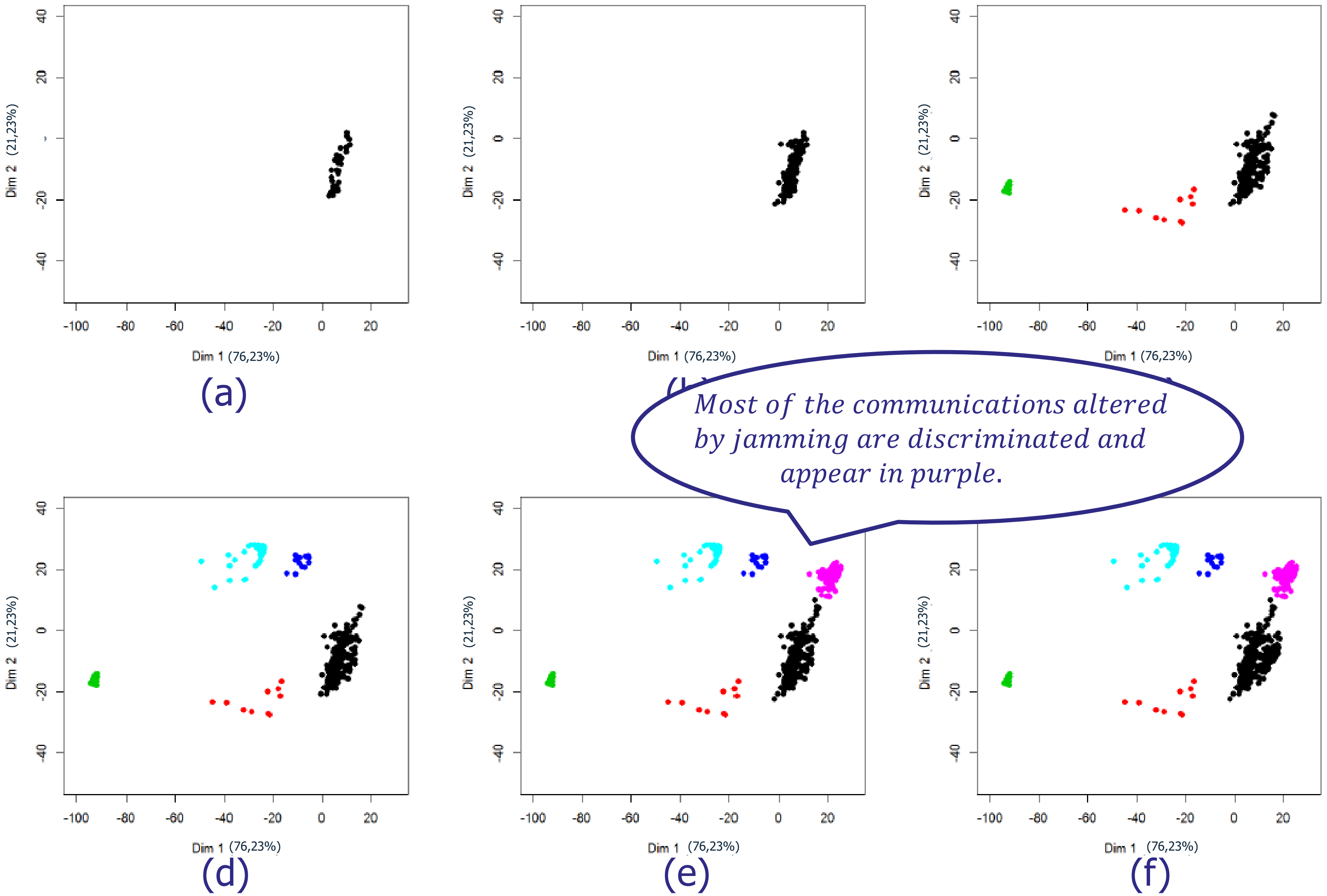
Identification of two communication profiles which correspond to deauthentication attacks. The green ones correspond to the cutting order.

Results



Identification of two communication profiles which correspond to jamming providing cut. The blue light corresponds to cut communication and the blue ones correspond to altered transmission.

Results



(a)

(d)

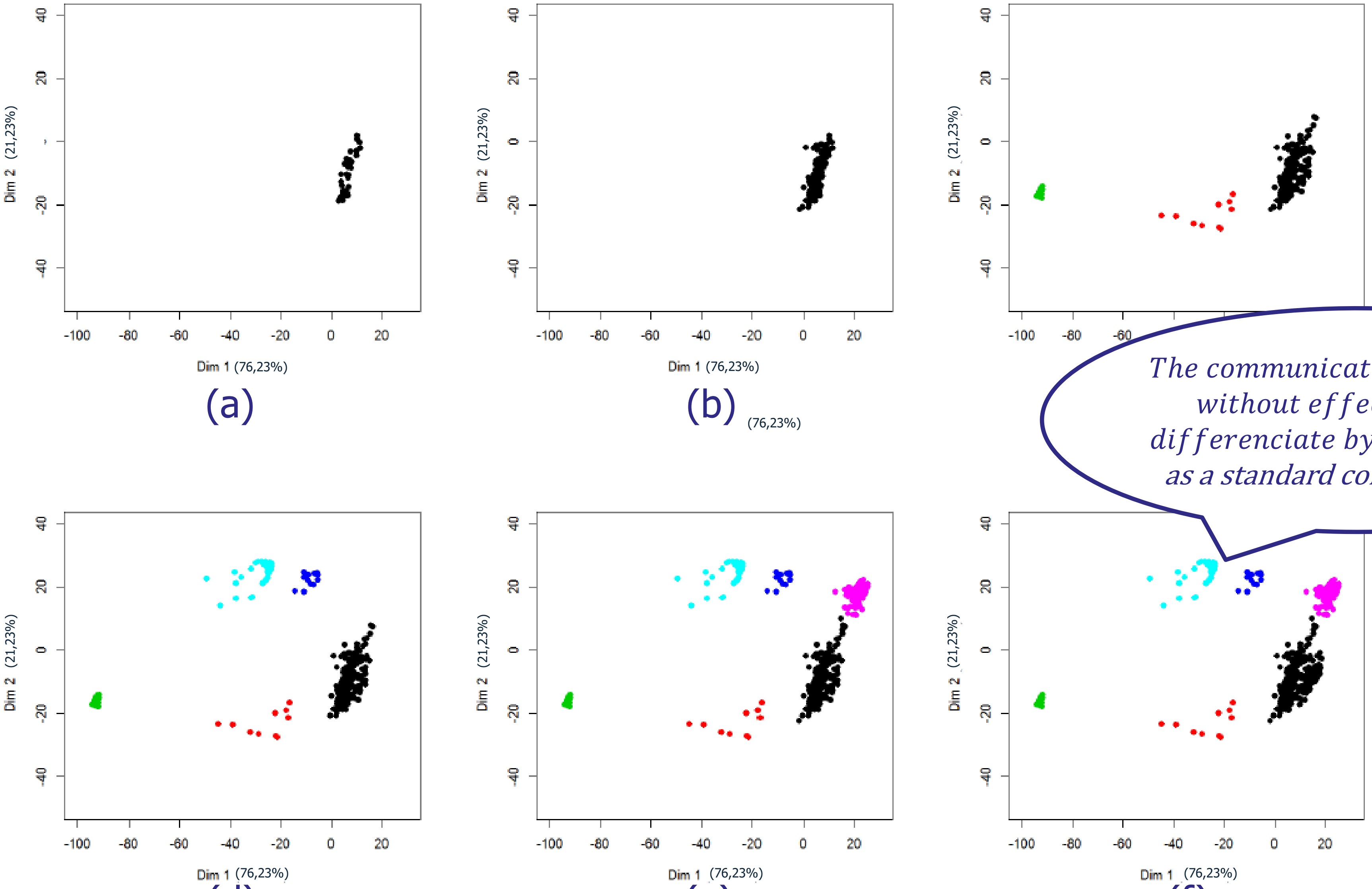
(e)

(f)

Most of the communications altered by jamming are discriminated and appear in purple.

Université Gustave Eiffel

Results



(a)

(b) (76,23%)

(d)

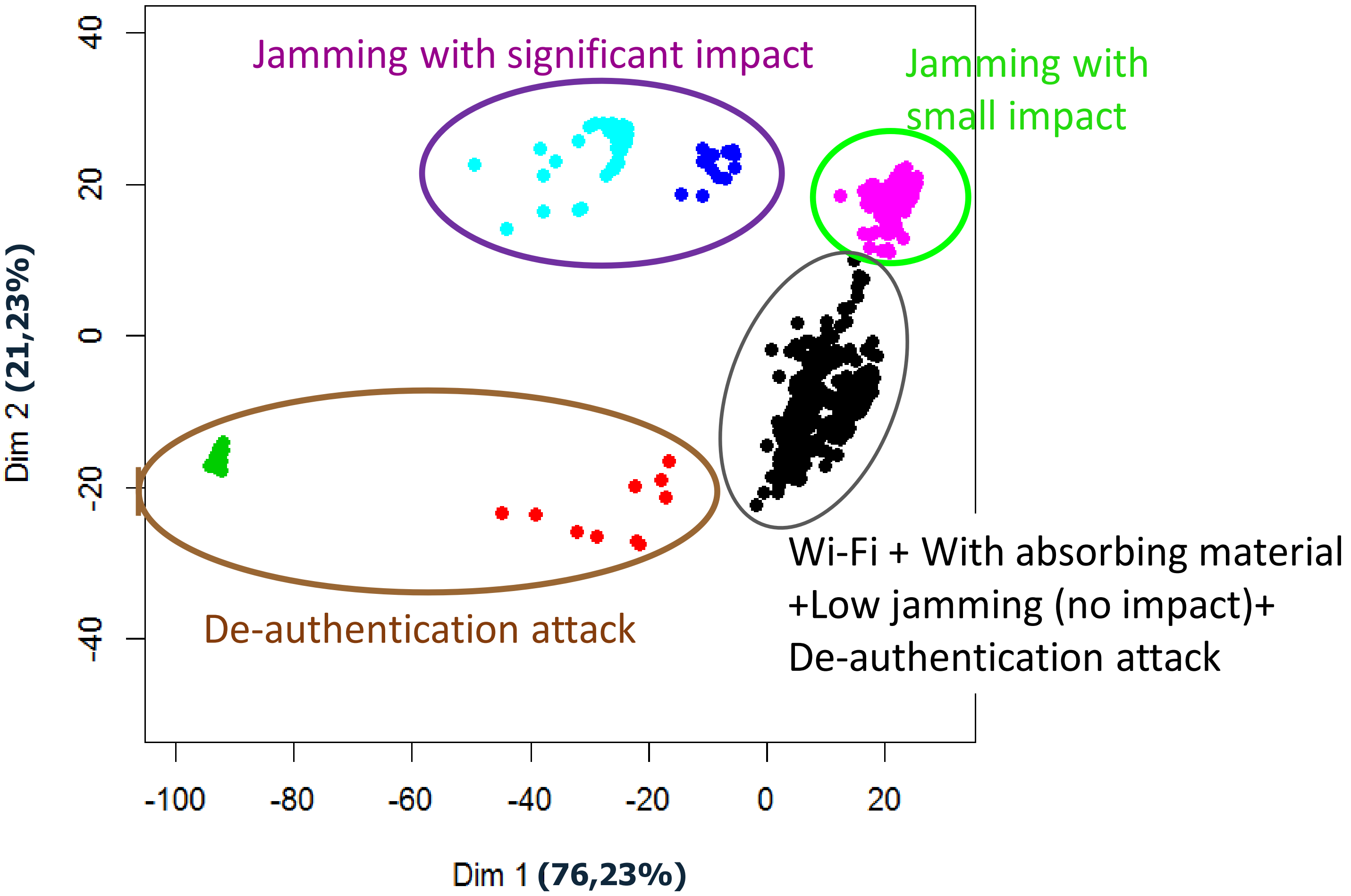
(e)

(f)

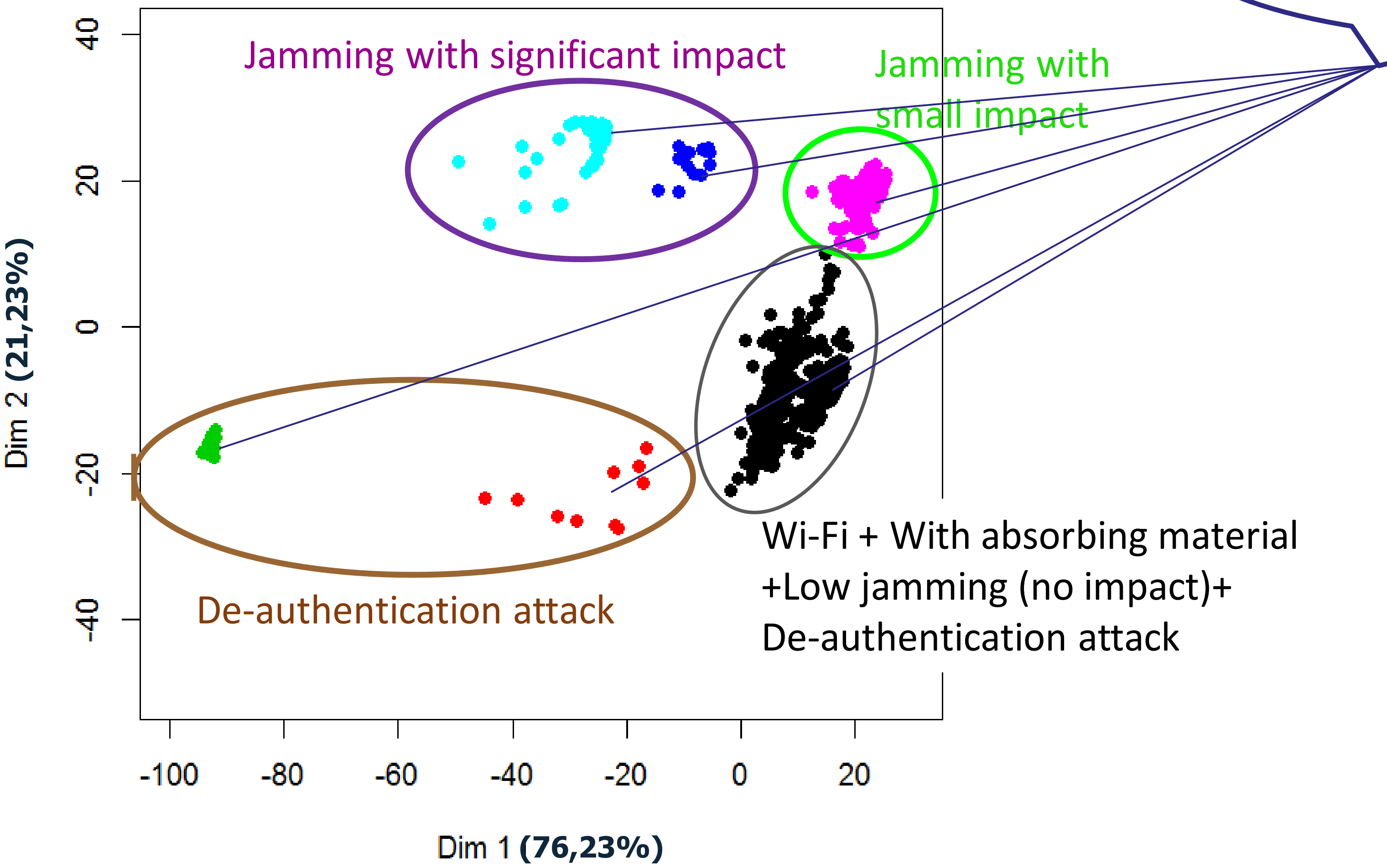
The communication under jamming without effect can't be differenciate by SAKM and appears as a standard communication.

Université Gustave Eiffel

Results


Jamming with significant impact
Jamming with small impact
De-authentication attack
Wi-Fi + With absorbing material +Low jamming (no impact)+ De-authentication attack
Dim 2 (21,23%)
Dim 1 (76,23%)
40
20
0
-20
-40
-100
-80
-60
-40
-20
0
20

Results



The color light blue, blue, purple, Black, red and green correspond to the clusters obtained using SAKM

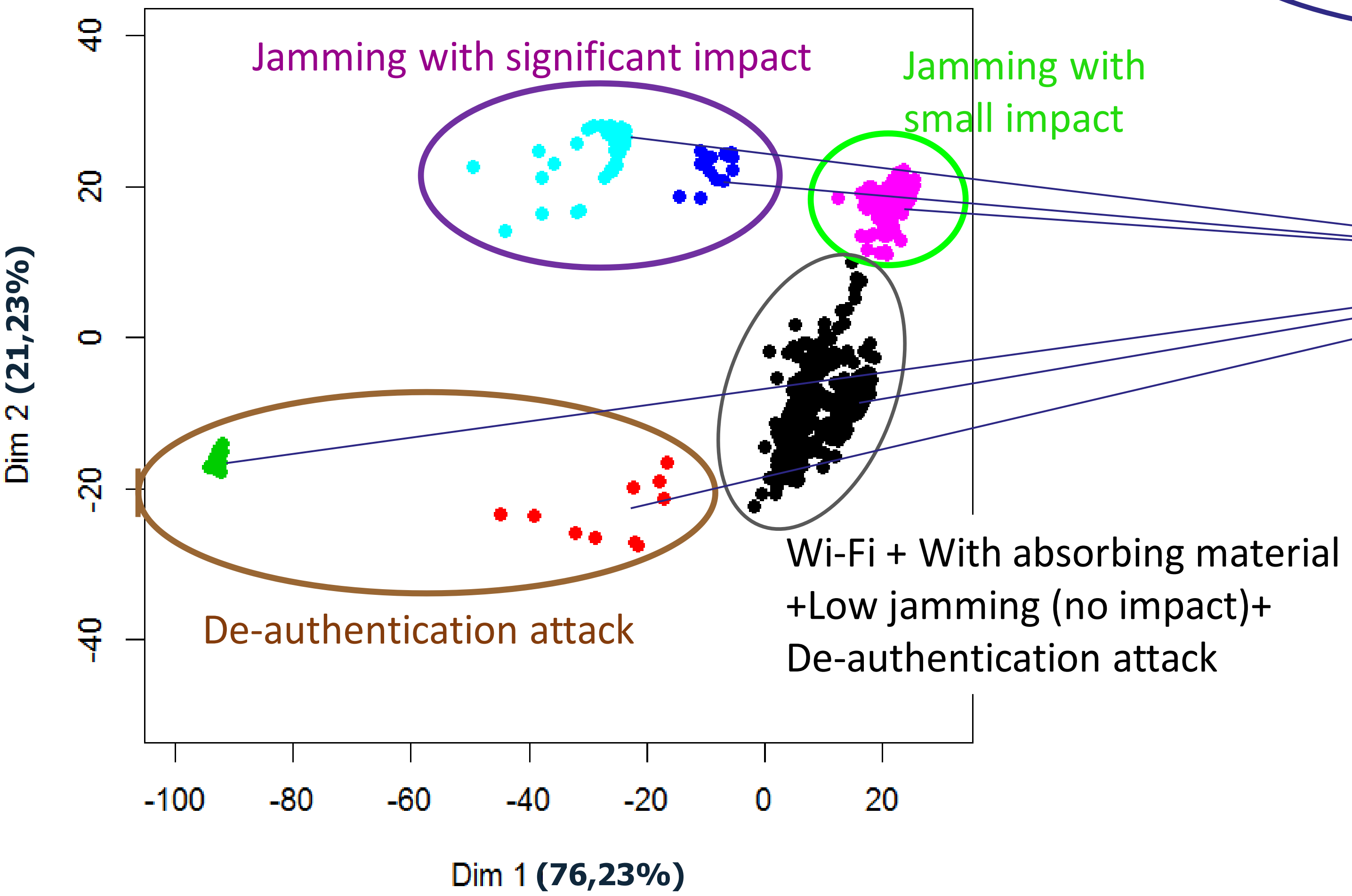
Jamming with significant impact

Jamming with small impact

De-authentication attack

Wi-Fi + With absorbing material +Low jamming (no impact)+ De-authentication attack

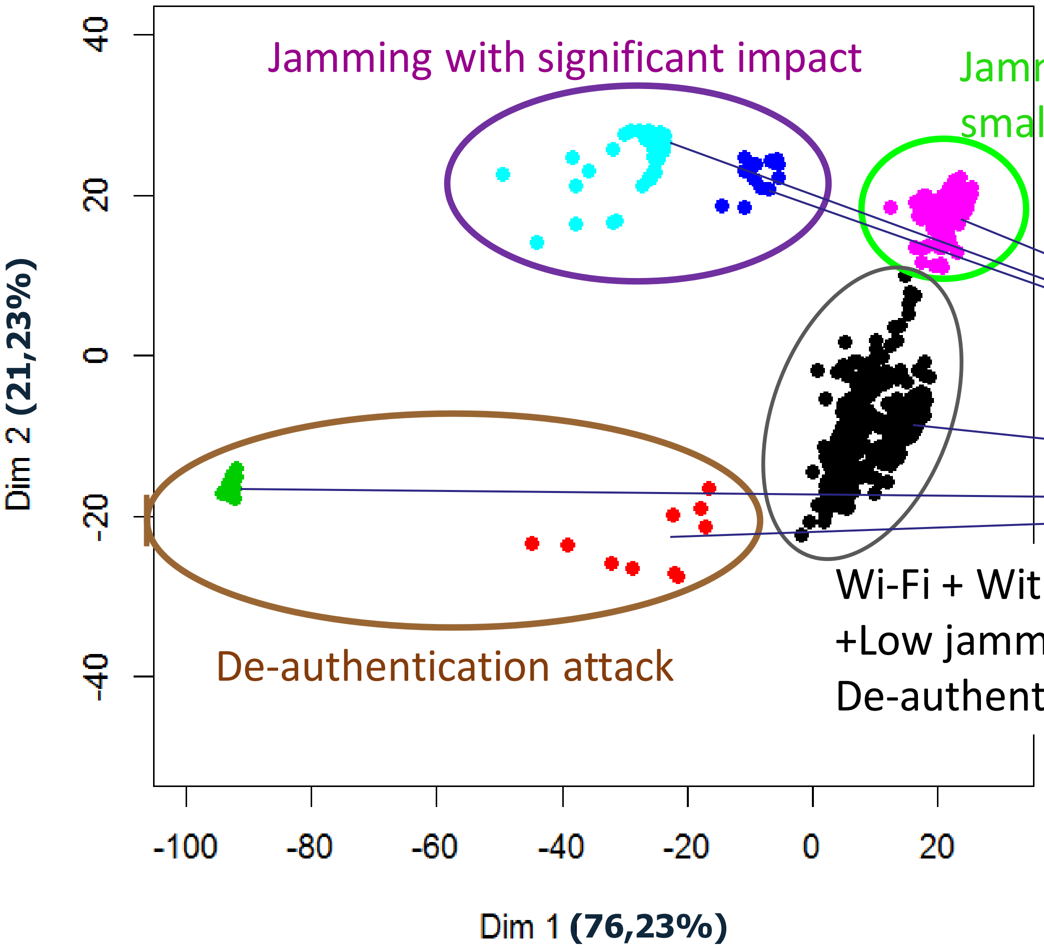
Results



The color light blue, blue, purple, Black, red and green correspond to the clusters obtained using SAKM

These clusters correspond to the expected separated profile visualized on the first PCA representation

Results

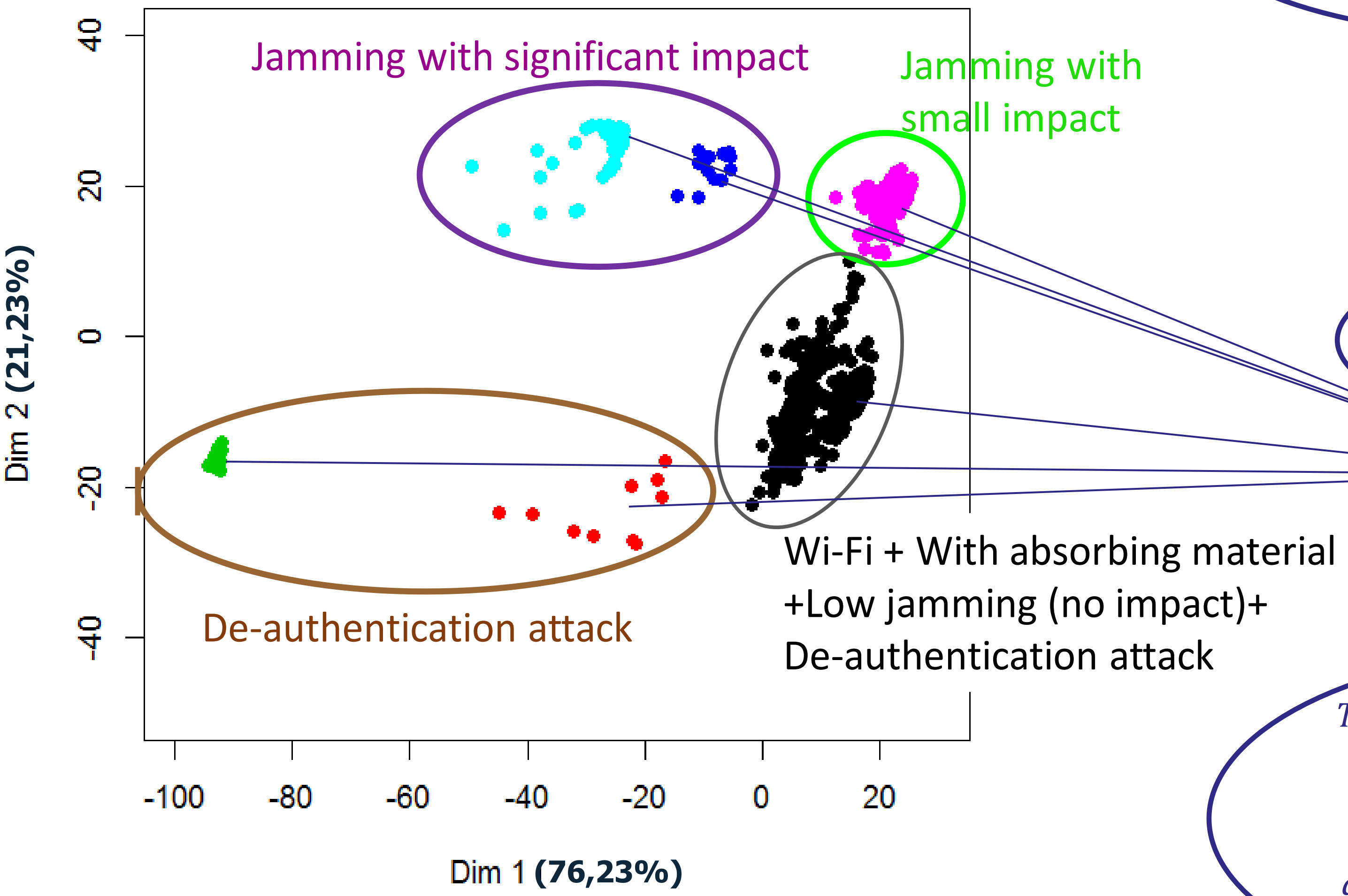


The color light blue, blue, purple, Black, red and green correspond to the clusters obtained using SAKM

These clusters correspond to the expected separated profile visualized on the first PCA representation

These clusters obtained using SAKM are generated without prior learning

Results



The color light blue, blue, purple, Black, red and green correspond to the clusters obtained using SAKM

These clusters correspond to the expected separated profile visualized on the first PCA representation

These clusters obtained using SAKM are generated without prior learning

The adaptive process of SAKM manages the creation of communication profile of separated data but has difficulties facing mixture model of configuration

Self Adaptive Kernel Machine

	Wi-Fi only	Wi-Fi + absorber	Jamming without Effect	Wi-Fi + Jamming with light effect	Wi-Fi + jamming at the limit of connection loss	De-authentication
1 (black)	97	97	92	13	0	12
2 (purple)	0	0	4	86	0	0
3 (blue)	0	0	0	0	22	0
4 (light blue)	0	0	0	0	76	0
5 (red)	2	2	3	0	1	22
6 (green)	0	0	0	0	0	65

Self Adaptive Kernel Machine

	Wi-Fi only	Wi-Fi + absorber	Jamming without Effect	Wi-Fi + Jamming with light effect	Wi-Fi + jamming at the limit of connection loss	De-authentica
1 (black)	97	97	92	13	0	12
2 (purple)	0	0	4	86	0	0
3 (blue)	0	0	0	0	22	0
4 (light blue)	0	0	0	0	76	0
5 (red)	2	2	3	0	1	22
6 (green)	0	0	0	0	0	65

The cluster one contains communication.
The effect of the jamming or the presence of absorber is to low.
The distribution of the data is too close. This proximity conducts to a fusion of this configuration.

Université Gustave Eiffel

Self Adaptive Kernel Machine

	Wi-Fi only	Wi-Fi + absorber	Jamming without Effect	Wi-Fi + Jamming with light effect	Wi-Fi + jamming at the limit of connection loss	De-authentication
1 (black)	97	97	92	13	0	12
2 (purple)	0	0	4	86	0	0
3 (blue)	0	0	0	0	22	0
4 (light blue)	0	0	0	0	76	0
5 (red)	2	2	3	0	1	22
6 (green)	0	0	0	0	0	65

The cluster two contains the communication ligntly affected by a jamming signal. The effect of the jamming is visible on the spectra which are well separated from data present in the cluster one.

Self Adaptive Kernel Machine

	Wi-Fi only	Wi-Fi + absorber	Jamming without Effect	Wi-Fi + Jamming with light effect	Wi-Fi + jamming at the limit of connection loss	De-authentication
1 (black)	97	97	92	13	0	12
2 (purple)	0	0	4	86	0	0
3 (blue)	0	0	0	0	22	0
4 (light blue)	0	0	0	0	76	0
5 (red)	2	2	3	0	1	22
6 (green)	0	0	0	0	0	65

The clusters three and four contain communications affected by a jamming signal. The effect of the jamming is clearly visible. The communication is majoritarly not present in the cluster four and is severly altered in the cluster three.

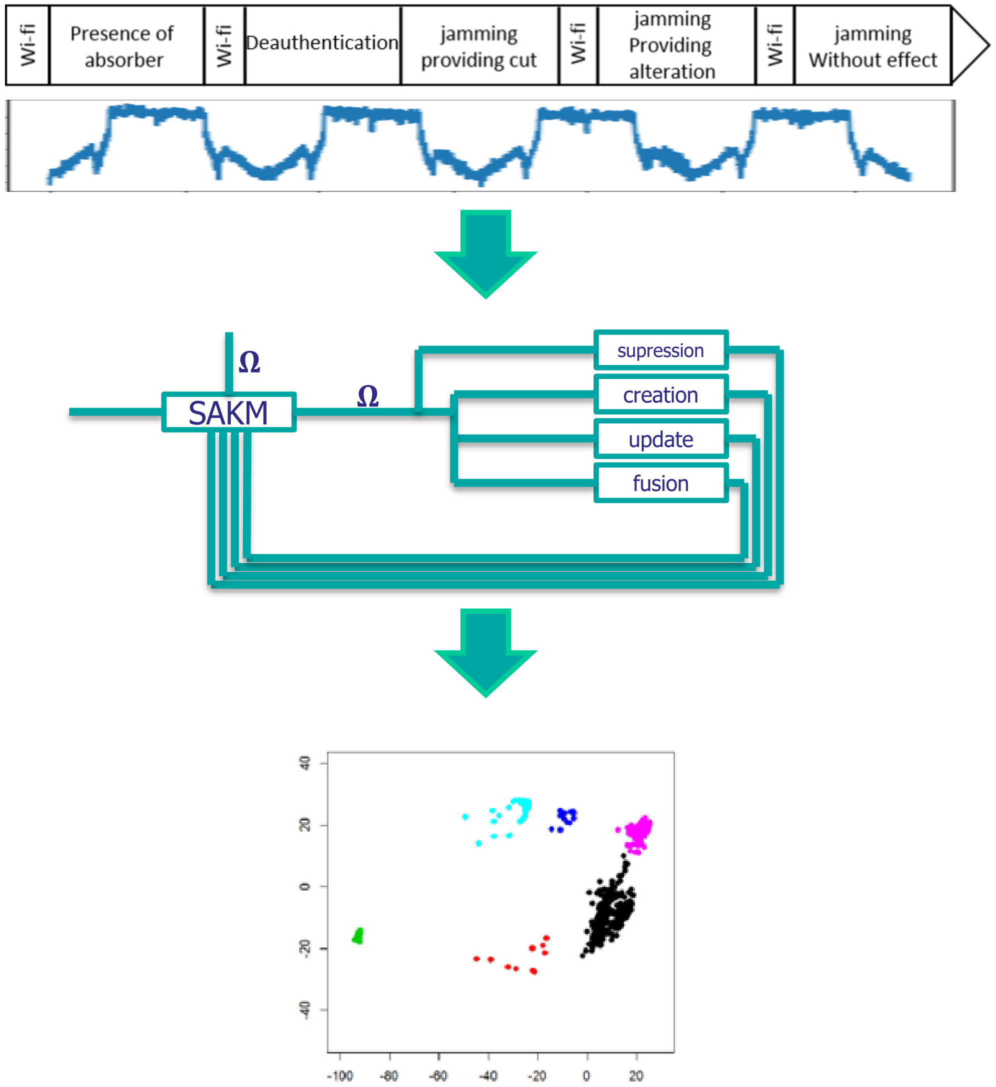
Self Adaptive Kernel Machine

	Wi-Fi only	Wi-Fi + absorber	Jamming without Effect	Wi-Fi + Jamming with light effect	Wi-Fi + jamming at the limit of connection loss	De-authentication
1 (black)	97	97	92	13	0	12
2 (purple)	0	0	4	86	0	0
3 (blue)	0	0	0	0	22	0
4 (light blue)	0	0	0	0	76	0
5 (red)	2	2	3	0	1	22
6 (green)	0	0	0	0	0	65

The clusters five and six contain deauthentication attacks. This repartition of the deauthentication attacks is explain by the attacks protocol. We have in the cluster six the deauthentication order in the cluster five spectra that correspond to an authentication that appears between deauthentication order and in black standard communication.

Université Gustave Eiffel

Conclusion



- ➢ Automatic detection of new profile
- ➢ SAKM is limited and can't discriminate configurations too close. (low jamming attacks and absorbers not detected)
- ➢ Deauthentication attacks and jamming are well detected.
- ➢ In the future :
  - ➢ we will incorporate in this algorithm time correlation to improve these results
  - ➢ study the attack in real environment

Jonathan VILLAIN

Jonathan.villain@ifsttar.fr

+33 6 31 06 18 80

Virginie DENIAU

Virginie.deniau@univ-eiffel.fr

+33 6 02 04 69 53

Université
Gustave Eiffel