

# IoT challenges

## State of the art

Aghiles DJOUDI

PhD student  
LIGM/ESIEE Paris & SIC/ECE Paris

August 28, 2019

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution

# Context

What is IoT ?

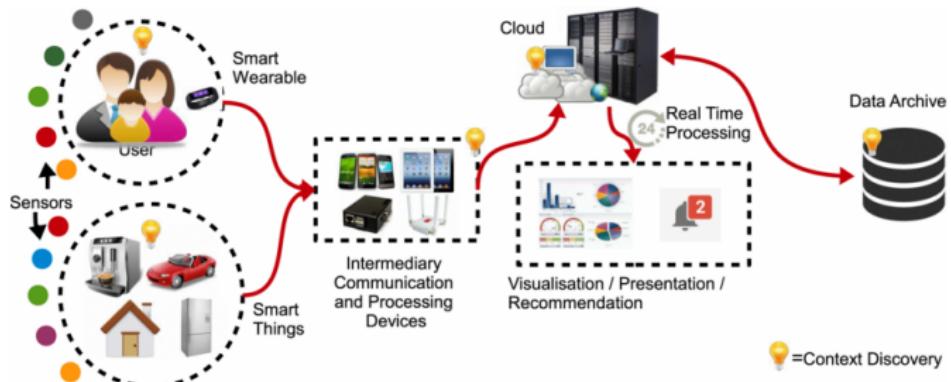


Figure 1: IoT platform.



Figure 2: IoT challenges.

# Problematic

Where is the problem ?

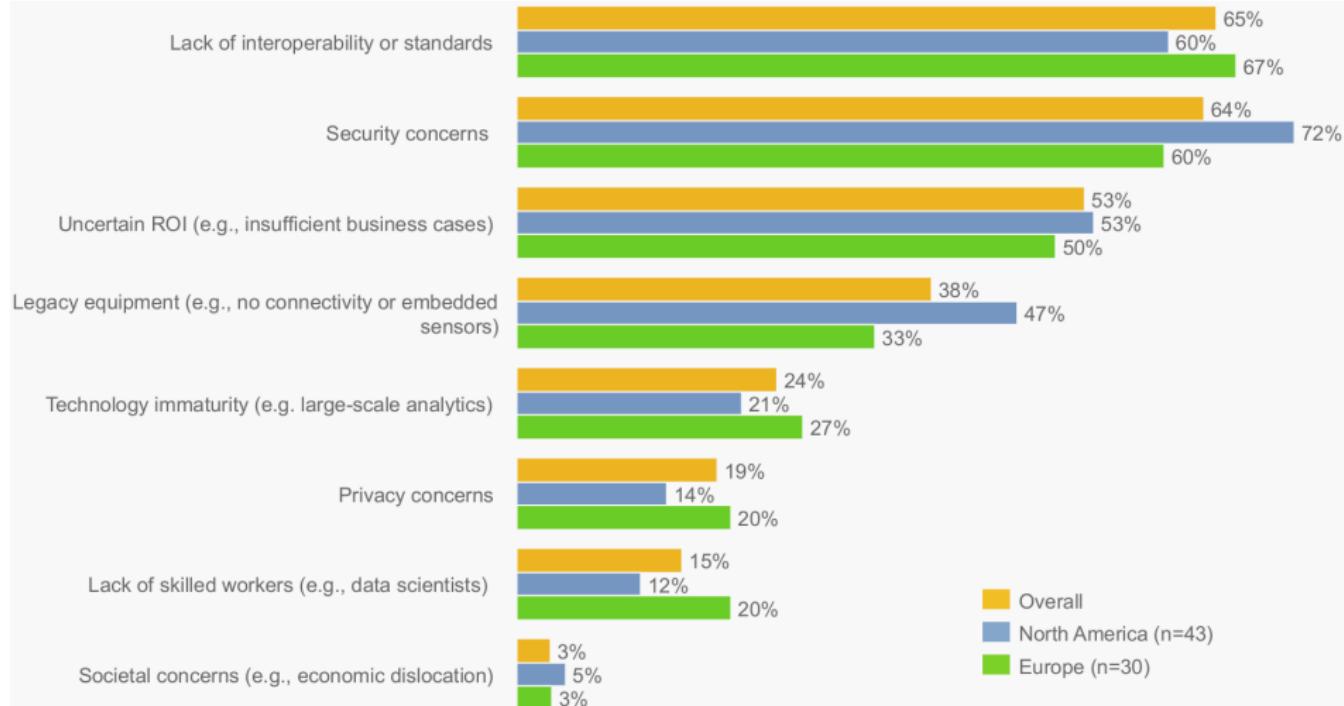


Figure 3: Key barriers in adopting the Industrial Internet [industrialinternetofthings\_executive\_].

# Problematic

Where is the problem ?

- ➡ Some network configuration are static and not adaptive to the application
  - ▶ Decision and optimisation problem..
  - ▶ Various network access
  - ▶ Various configuration of each network access
  - ▶ Lack of selection tools
- ➡ Users have to select the network and the application
  - ▶ How to select the **best** network.
  - ▶ How to select the network required by the application.

# Context

## Introduction

- ▶ IoT Applications
  - ▶ Health care
  - ▶ **Transportation**
  - ▶ Industry
  - ▶ Market
  - ▶ School
  - ▶ Vehicles
  - ▶ Smart Home
  - ▶ Agriculture



Figure ??: IoT Applications

## Problematic

Where is the problem [2] ?

Bandwidth (*BW*) Spreading Factor (*SF*) Coding Rate (*CR*) Transmission Power (*Tx*) Receiver Sensitivity (*RS*) Signal Noise Rate (*SNR*) Data Rate (*DR*) ,Air Time (*AT*), Payload length (*PktL*)

Setting	Values	Rewards	Costs
<i>BW</i>	$7.8 \rightarrow 500\text{kHz}$	<i>DR</i>	<i>RS, Range</i>
<i>SF</i>	$2^6 \rightarrow 2^{12}$	<i>RS, Range</i>	<i>DR, SNR, PktL, Tx</i>
<i>CR</i>	$4/5 \rightarrow 4/8$	Resilience	<i>PktL, Tx, AT</i>
<i>Tx</i>	$-4 \rightarrow 20\text{dBm}$	<i>SNR</i>	<i>Tx</i>

Table 1: [1]

# Technical choice

## Implementation

- ▶ ZOLERTIA RE-MOTE
  - ▶ Low consumption component
  - ▶ ADC port for placing sensors on it
- ▶ CONTIKI OS
  - ▶ Operating system for wireless and low power development
  - ▶ Support for newer standards (6LowPAN, RPL, CoAP, MQTT)
- ▶ 6LowPAN
  - ▶ Based on IPv6 and IEEE 802.15.4
  - ▶ IPv6-based network with low power consumption
  - ▶ Ability to create a mesh network
- ▶ Sending packages
  - ▶ UDP in the 6LowPAN network
  - ▶ MQTT between the cloud platform and the router



# Motivations

Who & why cares with such problems ?

- ➡ a
- ➡ Lake of selective tools
- ➡ How to select the **best** access point

## QoS Analysis

- ➡ a
- ➡ Lake of selective tools
- ➡ How to select the **best** access point

## Threats

- ➡ a
- ➡ Lake of selective tools
- ➡ How to select the **best** access point



Figure 4: Communication diversity.

# Goal

What is the goal ?

- ▶▶ Allow heterogeneous network to communicate
  - ▶▶ QoS Analysis
  - ▶▶ Threats
- 
- ▶ How to select the **best** access point
    - ▶ Allow heterogeneous network to communicate
    - ▶ QoS Analysis
    - ▶ Threats



Figure 5: wsn-IoT.

# Goal

What is the goal ?

- ▶ ▶ Allow heterogeneous network to communicate
- ▶ ▶ QoS Analysis
- ▶ ▶ Threats
  
- ▶ How to select the **best** access point
  - ▶ Allow heterogeneous network to communicate
  - ▶ ▶ QoS Analysis
  - ▶ ▶ Threats



Figure 5: wsn-IoT.

## Map the network to service requirement ?

# Challenges

Where is the difficulty ?

- Reasonable and acceptable delay before the decision appears.
- Cope with the different view points and goals of the operators and the users.
- React to the changing environment conditions.
- Allow any type of inputs and to be applicable to any type of ANs.
- Handle the increasing number of RATs and the large number of criteria.

# Contributions

## Contributions

- ▶ Use cases (Requirements)
  - ▶ Smart building: Videos, Voice, Text.
  - ▶ Smart traffic: Videos, Voice, Text
- ▶ Environments
  - ▶ Rural/Urban
  - ▶ Static/Mobile
  - ▶ Temperature
- ▶ Scenarios
  - ▶ For each application protocol (MQTT, COAP, XMPP)
  - ▶ For each network protocol (Star, Mesh)
  - ▶ For each MAC protocol (LoRaWan, Sigfox, ...)
- ▶ Algorithms
  - ▶ Input:
    - \* Service QoS metrics requirements
    - \* MAC configuration (SF, CR, BW, ...)
    - \* Network QoS metrics
  - ▶ Method:
    - \* MADM, Game, Neural
  - ▶ Outputs:
    - \* Ranked networks

# Contributions

## Contributions

- ▶ Use cases (Requirements)
  - ▶ Smart building: Videos, Voice, Text.
  - ▶ Smart traffic: Videos, Voice, Text
- ▶ Environments
  - ▶ Rural/Urban
  - ▶ Static/Mobile
  - ▶ Temperature
- ▶ Scenarios
  - ▶ For each application protocol (MQTT, COAP, XMPP, ...)
  - ▶ For each network protocol (Star, Mesh)
  - ▶ For each MAC protocol (LoRaWan, Sigfox, ...)
- ▶ Algorithms
  - ▶ Input:
    - \* Service QoS metrics requirements
    - \* MAC configuration (SF, CR, BW, ...)
    - \* Network QoS metrics
  - ▶ Methods:
    - \* MADM, Game, Neural
  - ▶ Outputs:
    - \* Ranked networks

Theoretical, Simulation & Real environment

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  - 1. Related work
  - 2. Contagion process
  - 3. Experimentation
  - 4. Results exploitation
  - 5. Discussion

# Outline

1. Introduction

2. First contribution

3. Second contribution

4. Third contribution

5. Conclusion

6. First contribution

1. Related work
2. Contagion process
3. Experimentation
4. Results exploitation
5. Discussion

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 2: An example table.

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 3: An example table.

# Outline

1. Introduction

2. First contribution

3. Second contribution

4. Third contribution

5. Conclusion

6. First contribution

1. Related work
2. **Contagion process**
3. Experimentation
4. Results exploitation
5. Discussion

... (step 1)

Methods



... (step 2)

Methods



... (step 3)

Methods



... (step 4)

Methods



# Results

## Comparison


Table 4

# Outline

1. Introduction

2. First contribution

3. Second contribution

4. Third contribution

5. Conclusion

6. First contribution

- 1. Related work
- 2. Contagion process
- 3. Experimentation**
- 4. Results exploitation
- 5. Discussion

# Experimentation

## Experimentation

- a
- b

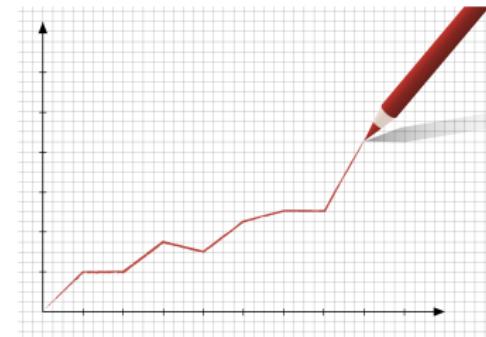


Figure 6: .

# Outline

1. Introduction

2. First contribution

3. Second contribution

4. Third contribution

5. Conclusion

6. First contribution

1. Related work
2. Contagion process
3. Experimentation
- 4. Results exploitation**
5. Discussion

# Results

## Comparison

- a
- b

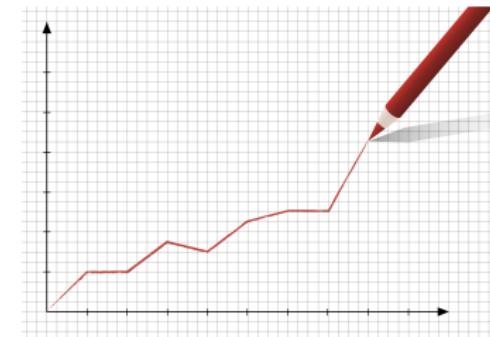


Figure 7: .

# Outline

1. Introduction

**2. First contribution**

3. Second contribution

4. Third contribution

5. Conclusion

6. First contribution

- 1. Related work
- 2. Contagion process
- 3. Experimentation
- 4. Results exploitation
- 5. Discussion**

## Discussion

→ a

→ b

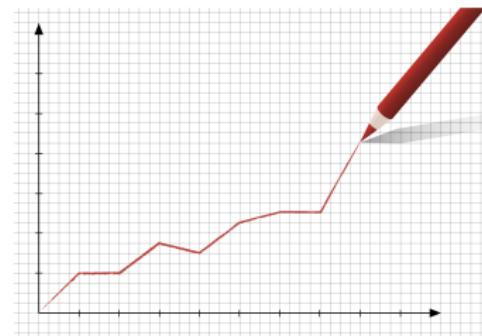


Figure 8: .

# Outline

- 1. Introduction
- 2. First contribution
- 3. Second contribution
  - 1. Related work
  - 2. Contagion process
  - 3. Experimentation
  - 4. Results exploitation
  - 5. Discussion
- 4. Third contribution
- 5. Conclusion
- 6. First contribution

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  - 1. Related work
  - 2. Contagion process
  - 3. Experimentation
  - 4. Results exploitation
  - 5. Discussion

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 5: An example table.

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 6: An example table.

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  1. Related work
  2. **Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion

... (step 2)

Methods



... (step 3)

Methods



... (step 4)

Methods



# Results

## Comparison


Table 7

# Outline

1. Introduction
2. First contribution
3. **Second contribution**
  1. Related work
  2. Contagion process
  3. **Experimentation**
  4. Results exploitation
  5. Discussion
4. Third contribution
5. Conclusion
6. First contribution

# Experimentation

## Experimentation

- a
- b

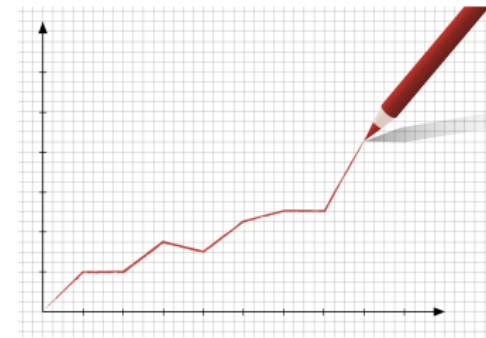


Figure 9: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  1. Related work
  2. Contagion process
  3. Experimentation
  - 4. Results exploitation**
  5. Discussion

## Results

## Comparison

- a  
→ b

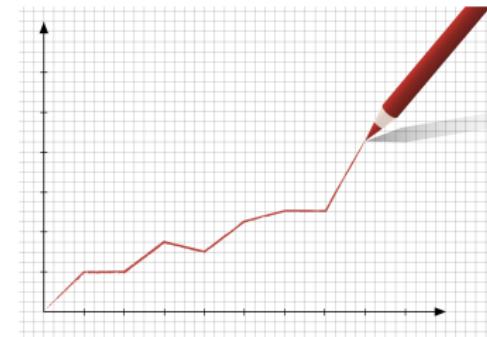


Figure 10: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
  1. Related work
  2. Contagion process
  3. Experimentation
  4. Results exploitation
4. Third contribution
5. Conclusion
6. First contribution

## Discussion

→ a

→ b

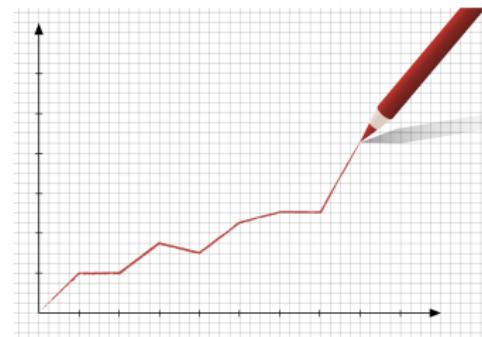


Figure 11: .

# Outline

- 1. Introduction
- 2. First contribution
- 3. Second contribution
- 4. Third contribution
- 5. Conclusion
- 6. First contribution
  - 1. Related work
  - 2. Contagion process
  - 3. Experimentation
  - 4. Results exploitation
  - 5. Discussion

# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  2. Contagion process
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 8: An example table.

## Related work

### Comparison

Paper	A1	A2	A3	A4

Table 9: An example table.

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
  1. Related work
  2. **Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution
  1. Bandit Algorithm
  2. Genetic Algorithm
  3. Marcov chain
  4. Game theory

# Outline

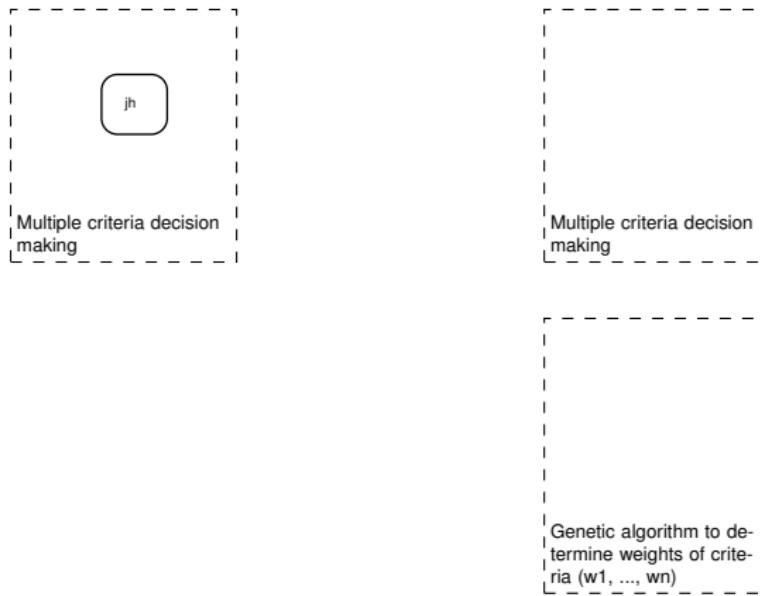
1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  - 2. Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

# Multi-Armed-Bandit Algorithm

## Methods

- Arms:  $K = 1, \dots, K$
- Decision:  $T = 1, \dots, T$
- Reward:  $X_t^k$  with  $\mu_t^k = E [X_t^k]$ 
  - Best reward:  $X_t^*$  with  $\mu_t^* = \max \mu_t^k, k \in K$

# Binary code analysis: Why?



# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  - 2. Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

# Genetic Algorithm

Methods [alkhawiani\_access\_2008a]

- Heterogeneous wireless network: (RAT 1 ,RAT 2 ,...,RAT n)
- Criteria up to i ( $c_1, c_2, \dots, c_i$ ) the operators, the applications, and the network conditions.
- 
- The different sets of scores ( $d_1, d_2, \dots, d_i$ ) are sent to the MCDM in the second component.
- GA component assigns a suitable weight ( $w_1, w_2, \dots, w_i$ )

# Genetic Algorithm

## Methods



→ S = SF12, BW125, 4/8, 17 dBm

→ Input:

→ Problem:  $f(x) = \max(x^2)$ ,  $x \in [0, 32]$

\*  $x_1 : 01101_b$

\*  $x_2 : 11000_b$

\*  $x_3 : 01000_b$

\*  $x_4 : 10011_b$

→ Method: Genetic algorithm

→ Generate a set of random possible solution

→ Test each solution and see how good it is (ranking)

\* Remove some bad solutions

\* Duplicate some good solutions

\* Make small changes to some of them (Crossover, Mutation)

→ Output:

→  $x_1 : 01101$  (169) (14.4)

# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  - 2. Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

# Marcov chain

## Methods

$$V(s, \pi) = \mathbb{E}_s^\pi \left( \sum_{k=0}^{\inf} \gamma^k \cdot r(s_k, a_k) \right), s \in \mathbb{S} \quad (1)$$

$$r(s_k, a_k) = G_k \cdot PRR(a_k) \quad (2)$$

$$\pi^* = \arg \max_{\pi} V(s, \pi) \quad (3)$$

$$PRR = (1 - BER)^L \quad (4)$$

$$BER = 10^{\alpha e^{\beta SNR}} \quad (5)$$

# Marcov chain

## Methods

HGHGJ

$$V(s, \pi) = \mathbb{E}_s^\pi \left( \sum_{k=0}^{\inf} \gamma^k \cdot r(s_k, a_k) \right), s \in \mathbb{S} \quad (1)$$

$$r(s_k, a_k) = G_k \cdot PRR(a_k) \quad (2)$$

$$\pi^* = \arg \max_{\pi} V(s, \pi) \quad (3)$$

$$PRR = (1 - BER)^L \quad (4)$$

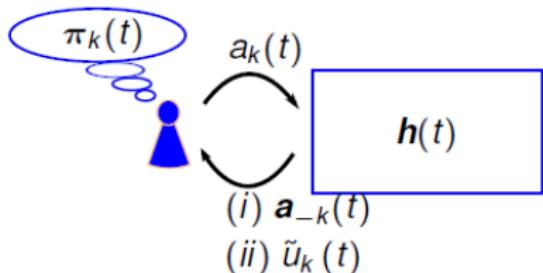
$$BER = 10^{\alpha e^{\beta SNR}} \quad (5)$$

# Marcov chain

## Methods

Learning Iterative Steps:

- **Choose** action  $a_k(t) \sim \pi_k(t)$ .
- **Observe** game outcome, e.g.,  
 $a_{-k}(t)$   
 $u_k(a_k(t), a_{-k}(t))$ .
- **Improve**  $\pi_k(t+1)$ .



Thus, we can expect that:  $\forall k \in \mathcal{K}$ ,

$$\pi_k(t) \xrightarrow{t \rightarrow \infty} \pi_k^* \quad (1)$$

$$\bar{u}_k(\pi_k(t), \pi_{-k}(t)) \xrightarrow{t \rightarrow \infty} \bar{u}_k(\pi_k^*, \pi_{-k}^*) \quad (2)$$

where,  $\pi^* = (\pi_1^*, \dots, \pi_K^*)$  is a NE strategy profile.

Figure 12: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  - 2. Contagion process**
  3. Experimentation
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

# Game theory

## Methods

- ▶ Players:  $K = \{1, \dots, K\}$
- ▶ Strategies:  $S = S_1 \times \dots \times S_K$ 
  - ▶  $S_k$  is the strategy set of the  $k^{\text{th}}$  player.
- ▶ Rewards:  $u_k : S \rightarrow R_+$  and is denoted by  $r_k(s_k, s_{-k})$ 
  - ▶  $s_{-k} = (s_1, \dots, s_{k-1}, s_{k+1}, \dots, s_K) \in S_1 \times \dots \times S_{k-1} \times S_{k+1} \times \dots \times S_K$

... (step 2)

Methods



... (step 3)

Methods



... (step 4)

Methods



# Results

## Comparison


Table 10

# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  2. Contagion process
  - 3. Experimentation**
  4. Results exploitation
  5. Discussion
5. Conclusion
6. First contribution

# Experimentation

## Experimentation

- a
- b

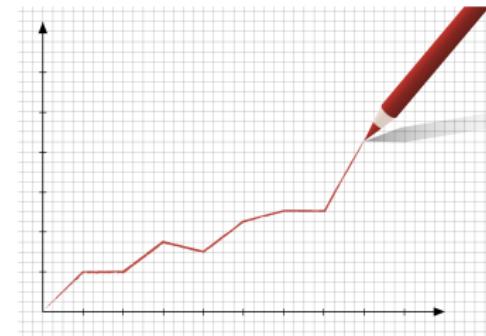


Figure 13: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
  1. Related work
  2. Contagion process
  3. Experimentation
  - 4. Results exploitation**
  5. Discussion
5. Conclusion
6. First contribution

# Results

## Comparison

- a
- b

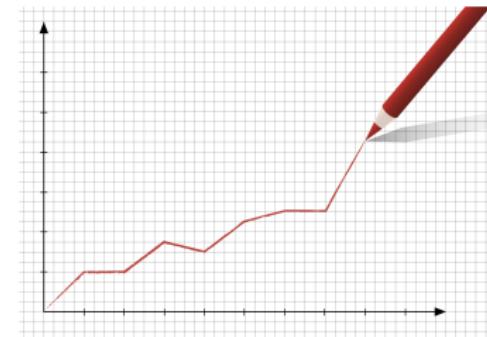


Figure 14: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
- 4. Third contribution**
  1. Related work
  2. Contagion process
  3. Experimentation
  4. Results exploitation
  - 5. Discussion**
5. Conclusion
6. First contribution

## Discussion

→ a

→ b

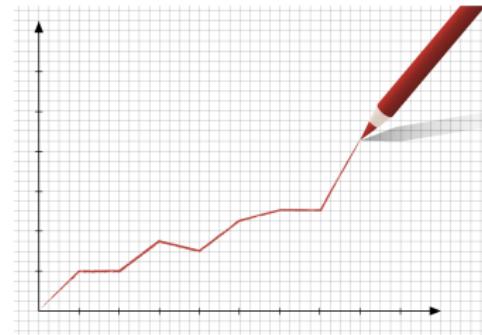


Figure 15: .

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
- 5. Conclusion**
6. First contribution

# Conclusion

Our main goal was



Our main contribution was



Our main results was



# Future Challenges

## Conclusion

Our future goal was



# Future Challenges

## Conclusion

Our future goal was



Thank you !

# Outline

- 1. Introduction
- 2. First contribution
- 3. Second contribution
  - 1. Related work
  - 2. Diffusion process
  - 3. Experimentation
  - 4. Results
  - 5. Discussion
- 4. Third contribution
- 5. Conclusion
- 6. First contribution

# Outline

- 1. Introduction
- 2. First contribution
- 3. Second contribution
- 4. Third contribution
- 5. Conclusion
- 6. First contribution
  - 1. Related work
  - 2. Diffusion process
  - 3. Experimentation
  - 4. Results
  - 5. Discussion

## Related work

### Comparison

Works	Contribution	Goal
[3] Protect U	Classification of interlocutors	Friends lists management
[4] Privacy Wizard	Friends Classification	Permission Configuration
[5] SocialMarket	Common Interests	Assessment of Trust Relationships
[6] PARE	Information Leakage	Evaluation of Information Dissemination
[7] LENS	Spam Protection	Trusted Emitters Evaluation
[8] SocialEmail	Classify msg by paths	Evaluate message reliability
[9] Privacy Index	Visibility, sensitivity	Msg exposure assessment

Table 11: Contributions from existing work.

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  - 1. Related work
  - 2. Diffusion process**
  - 3. Experimentation
  - 4. Results
  - 5. Discussion

# Step 1: Individual vulnerability measurement

## Method

Parameter	Value
Network connection	Private, Public [1:2]
Technology	Ethernet, 5G, 4G, Wifi [1:4]
Operating system	Windows, Unix, Mac [1:3]
Web browser	Firefox, Chrome, Opera, ... [1:10]
Password strength	low, medium, strength [1:3]
Sessions opened	counter [1:10]
TLS version	v1.0, v1.1, v1.2, v1.3 [1:4]

Table 12: Individual Vulnerability parameter

$$Y = \sum_i^n \frac{w * V}{n} \quad (6)$$

- **Y:** Individual vulnerability
- **w:** Weight of each vulnerability
- **V:** Scores mentioned above

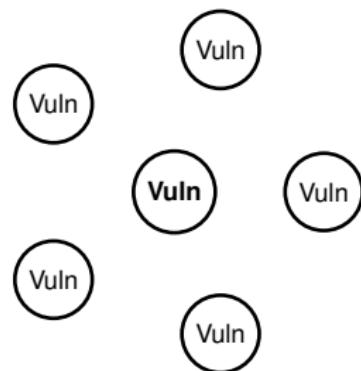


Figure 16: Individual vulnerability level.

## Step 2: Users reputation estimation

### Method

Parameter	Value
Frequency of msg exchanged	continuous
Discussion time	continuous
% of messages exchanged	cipher, signed or clear [1:3]
Message type exchanged	Text, images, videos, script [1:4]

Table 13: Trust grant features

$$\alpha = P(\text{reputation}) = P(X \geq 1) = 1 - (1 - P(\text{trust}))^n \quad (7)$$

- Where,
  - **X**: trust grant, random variable,  $X \sim B(n,p)$
  - **n**: deg(node)
  - **P(X=1)**: The probability of being assigned one trust grant by an interlocutor

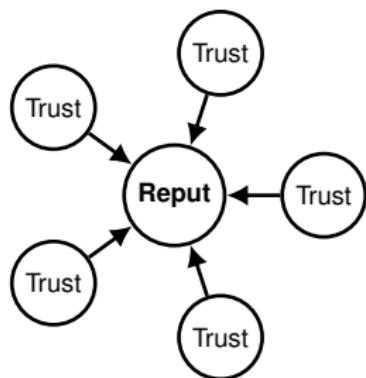


Figure 17: Reputation level.

## Step 3: Social vulnerability measurement

Freidkin's theory of social influence

- Input (Features):

- $Y^{(1)}$  = Vector of the individual vulnerabilities of N users (eq 6)
- $\alpha$  = The level of reputation (influence) of each user (eq 7)
- $M$  = Adjacency matrix  $N \times N$

- Model:

$$Y^{(t)} = \alpha M Y^{(t-1)} + (1 - \alpha) Y^{(t-1)} \quad (8)$$

- Output:

- $Y^{(t)}$  = Vector of the social vulnerabilities of the N users

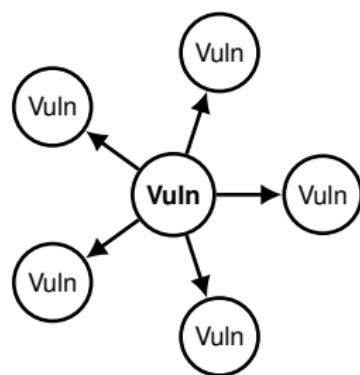


Figure 18: Social vulnerability.

## Step 3: Social vulnerability measurement

Freidkin's theory of social influence

Formal properties of the model:

- When a user's influence is high, the model is reduced to:
  - average vulnerabilities of his friends weighted by their trust levels.

$$Y^{(t)} = \mathbf{1} * \mathbf{M} Y^{(t-1)} + (1 - \mathbf{1}) Y^{(t-1)} \quad (8)$$

$$Y^{(t)} = \mathbf{M} Y^{(t-1)}$$

- In the absence of influence, the model is reduced to:
  - his own vulnerability weighted by the level of mistrust of his friends

$$Y^{(t)} = 0 * \mathbf{M} Y^{(t-1)} + (1 - 0) Y^{(t-1)} \quad (8)$$

$$Y^{(t)} = Y^{(t-1)}$$

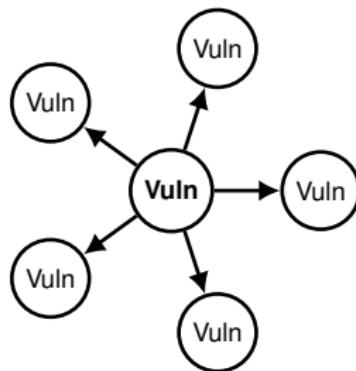


Figure 19: Social vulnerability.



# Outline

- 1. Introduction
- 2. First contribution
- 3. Second contribution
- 4. Third contribution
- 5. Conclusion
- 6. First contribution
  - 1. Related work
  - 2. Diffusion process
  - 3. Experimentation**
  - 4. Results
  - 5. Discussion

# Email datasets

## Experimentation

Parameter	Value
Users	958
Messages	6966
Diameter	958
# of msg on average	2.413361
Msg density	0.00252
Modularity	0.654600
Average distance	3.042114

Table 14: Enron dataset properties.



Figure 20: Enron logo.

Parameter	Value
Users	5885
Messages	26547
Diameter	2096
# of msg on average	9.02192
Msg density	0.001533
Modularity	0.86526
Average distance	3.914097

Table 15: Caliopen dataset properties.



Figure 21: Caliopen logo.

# Outline

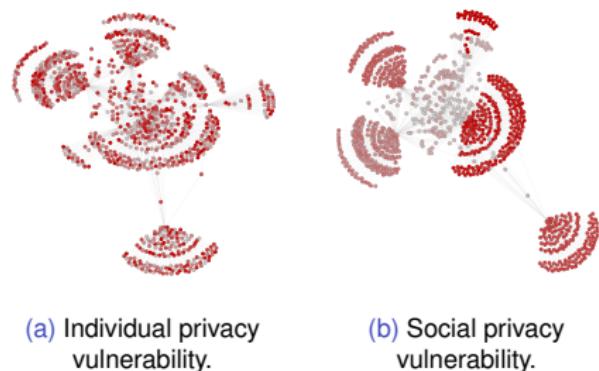
1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  - 1. Related work
  - 2. Diffusion process
  - 3. Experimentation
  - 4. Results**
  - 5. Discussion

# Results

## Comparison

Initial values:

- generated randomly (normal distribution)
- represent individual vulnerabilities.
- dark color = highly infected



Final values:

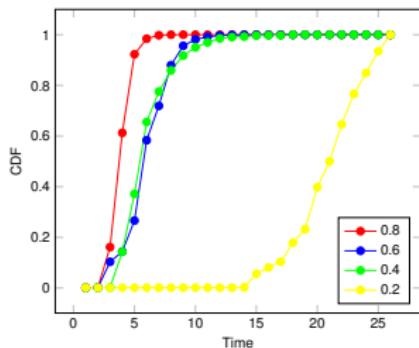
- obtained after convergence.
- represent social vulnerabilities.

Figure 22: Individual & Social privacy vulnerabilities.

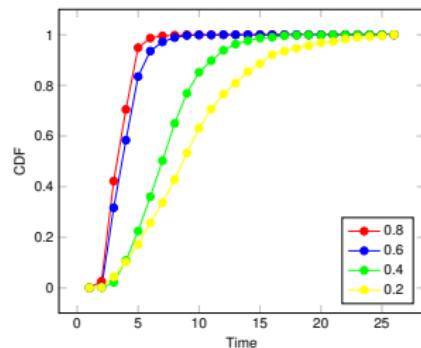
User ID	Individual Vul	Social Vul
34	0.84	0.67
67	0.12	0.87
206	0.76	0.33
588	0.23	0.78

Table 16: Individual and social privacy vulnerabilities.

## Results exploitation



(a) Enron dataset.



(b) Caliopen dataset.

Figure 23: Cumulative distribution function of infected users.

- Figures shows the CDF of the vulnerability diffusion process.
- The vulnerability diffusion process increases as the reputation level of vulnerable users increases.
- Users with high reputation values contribute significantly to the diffusion
  - They spread their vulnerabilities quickly and widely through the network.

## Results exploitation

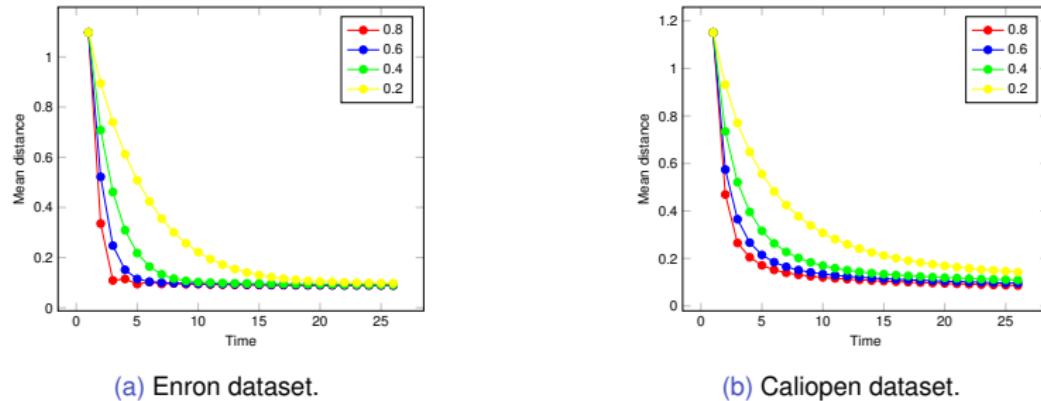


Figure 24: Convergence of the diffusion process.

- ▶ The process converge when the mean distance between social vulnerability scores is the minimum.
- ▶ Assigning trust to vulnerable users allows them to achieve a high level of reputation.
- ▶ Consequently, they infect all other vulnerability values.

# Outline

1. Introduction
2. First contribution
3. Second contribution
4. Third contribution
5. Conclusion
6. First contribution
  - 1. Related work
  - 2. Diffusion process
  - 3. Experimentation
  - 4. Results
  - 5. Discussion**

## Discussion

- ➡ The purpose of this work is to simulate a diffusion process of individual vulnerabilities.
  - ➡ The vulnerability of one user is the vulnerability of all users.
  - ➡ At the end of the diffusion (convergence), all users gets their social vulnerability scores.
- ➡ Future work
  - ➡ To propose mechanisms to improve the reputation of non-vulnerable users.
    - \* Suggest well known interlocutors with acceptable vulnerability scores.
  - ➡ To propose mechanisms to improve the vulnerability of reputed users.
    - \* recommend configurations and softwares.

## Discussion

- ➡ The purpose of this work is to simulate a diffusion process of individual vulnerabilities.
  - ➡ The vulnerability of one user is the vulnerability of all users.
  - ➡ At the end of the diffusion (convergence), all users gets their social vulnerability scores.
- ➡ Future work
  - ➡ To propose mechanisms to improve the reputation of non-vulnerable users.
    - \* Suggest well known interlocutors with acceptable vulnerability scores.
  - ➡ To propose mechanisms to improve the vulnerability of reputed users.
    - \* recommend configurations and softwares.

Thank you

# References

- [1] Marco Cattani, Carlo Boano, and Kay Römer. " An Experimental Evaluation of the Reliability of Lora Long-Range Low-Power Wireless Communication ". In: *Journal of Sensor and Actuator Networks* 6.2 (2017). 00042, p. 7.
- [2] B. Di Martino et al. " Internet of Things Reference Architectures, Security and Interoperability: A Survey ". In: *Internet of Things* 1-2 (Sept. 2018). 00006, pp. 99–112.
- [3] Ala Eddine Gandouz. " PROTECT\_U: Un Systeme Communautaire Pour La Protection Des Usagers de Facebook ". In: (2012). 00001, p. 77.
- [4] Lujun Fang and Kristen LeFevre. " Privacy Wizards for Social Networking Sites ". In: 00397. ACM Press, 2010, p. 351.
- [5] Davide Frey, Arnaud Jégou, and Anne-Marie Kermarrec. " Social Market: Combining Explicit and Implicit Social Networks ". In: *Stabilization, Safety, and Security of Distributed Systems. Symposium on Self-Stabilizing Systems. Lecture Notes in Computer Science*. 00019. Springer, Berlin, Heidelberg, Oct. 10, 2011, pp. 193–207.
- [6] Yongbo Zeng et al. " A Study of Online Social Network Privacy Via the TAPE Framework ". In: *IEEE Journal of Selected Topics in Signal Processing* 9.7 (Oct. 2015). 00003, pp. 1270–1284.
- [7] Sufian Hameed et al. " LENS: Leveraging Social Networking and Trust to Prevent Spam Transmission ". In: *Network Protocols (ICNP), 2011 19th IEEE International Conference On*. 00019. IEEE, 2011, pp. 13–18.
- [8] Thomas Tran, Jeff Rowe, and S. Felix Wu. " Social Email: A Framework and Application for More Socially-Aware Communications ". In: *Social Informatics*. Ed. by Leonard Bolc, Marek Makowski, and Adam Wierzbicki. Vol. 6430. 00000. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 203–215.
- [9] Raj Kumar Nepali and Yong Wang. " SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking ". In: 00021. IEEE, July 2013, pp. 162–166.