IoT challenges

State of the art

Aghiles DJOUDI

PhD student
LIGM/ESIEE Paris & SIC/ECE Paris

August 7, 2019

Outline

Context

What is IoT ?

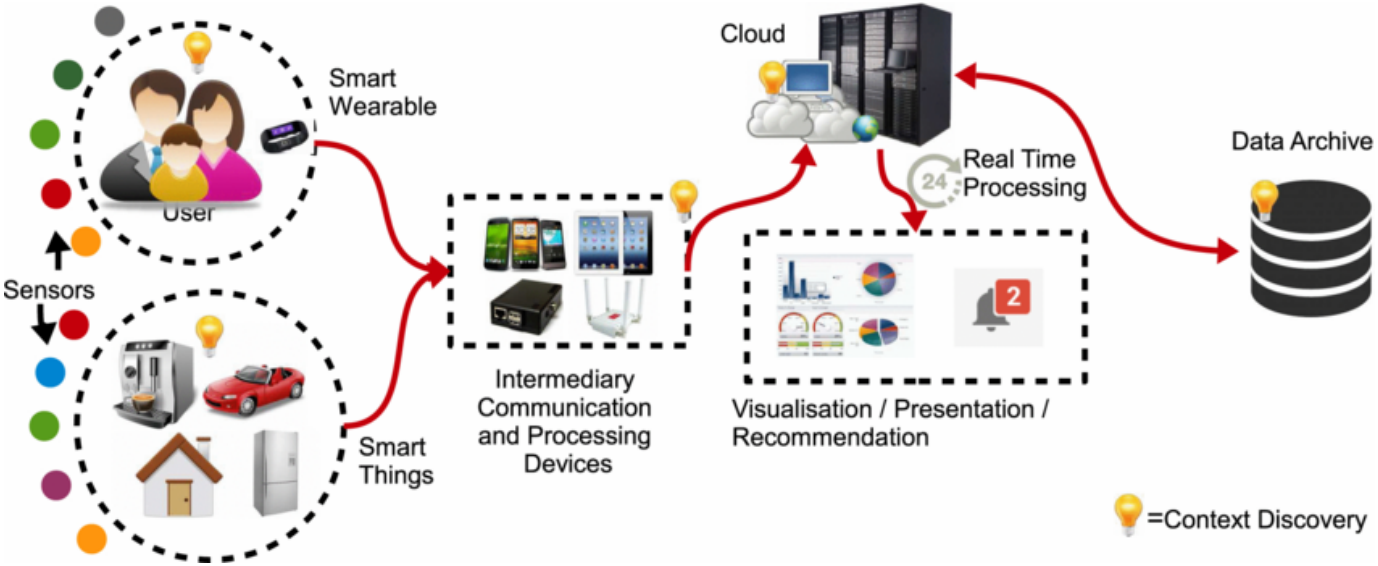


Figure 1: IoT platform.

Figure 2: IoT challenges.

Problematic

Where is the problem ?

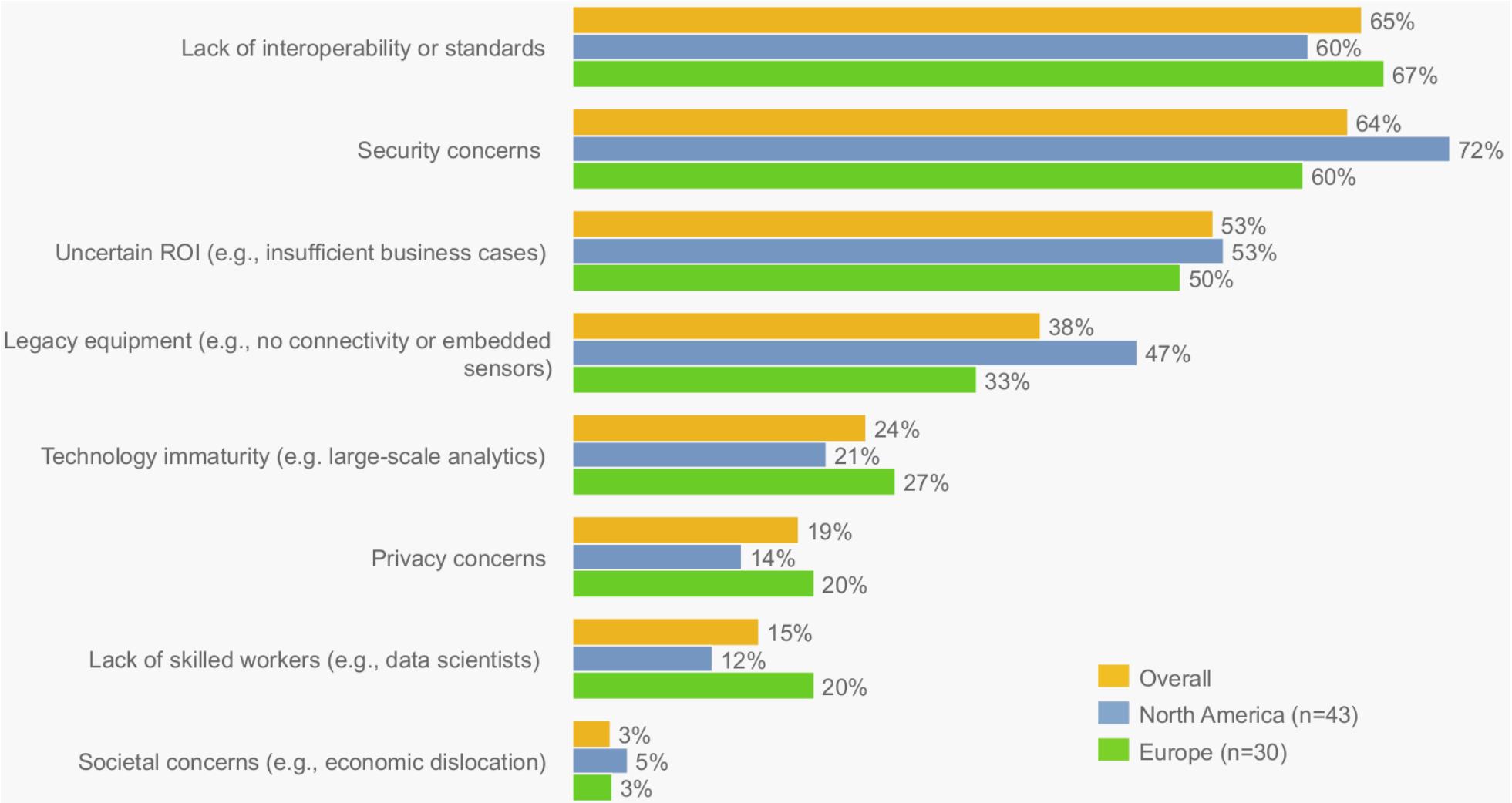


Figure 3: Key barriers in adopting the Industrial Internet [**industrialinternetofthings_executive_**].

Problematic

Where is the problem ?

- Some network configuration are static and not adptive to the application
  - Decision and optimisation problem..
  - Various network acces
  - Various configuration of each network acces
  - Lake 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
  - Scool
  - Vehicles
  - Smart Home
  - Agriculture

Figure ??: IoT Applications

Problematic

Where is the problem [2] ?

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

Setting	**Values**	**Rewards**	**Cost**
BW	$7.8 \rightarrow 500kHz$	*DR*	*RS*, Range.
SF	$2^6 \rightarrow 2^{12}$	*RS*, Range	*DR*, *SNR*, longer packets, *Tx*.
CR	$4/5 \rightarrow 4/8$	Resilience	longer packets, *Tx*, *AT*.
Tx	$-4 \rightarrow 20dBm$	*SNR*	*Tx*

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

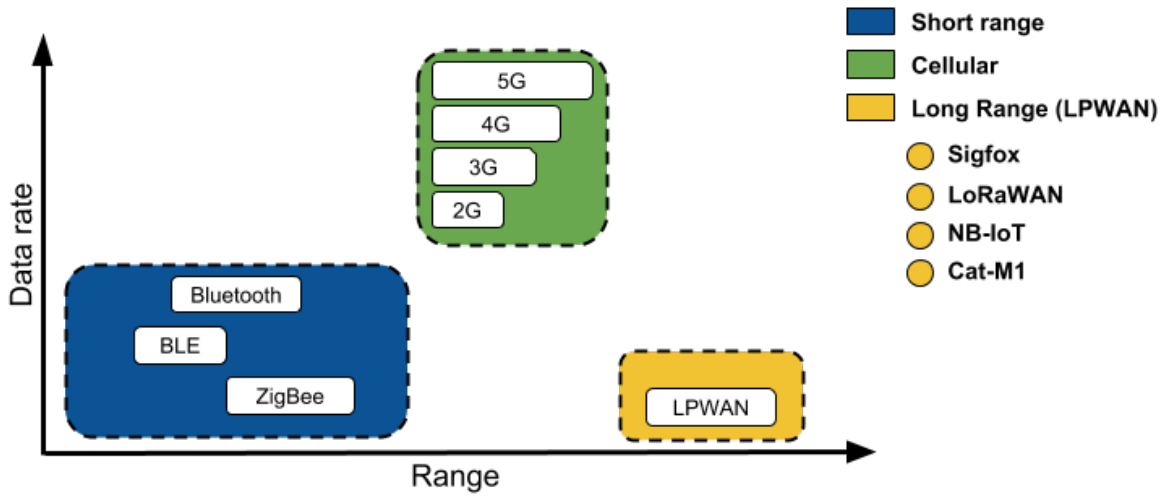


Figure 4: Communication diversity.

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
  - 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 trafic: Videos, Voice, Text
- Environnements
  - Rural/Urban
  - Static/Mobile
  - Tempirature
- Senarios
  - For each application protocol (MQTT, COAP, XMPP)
  - For each network protocol (Start, Mesh)
  - For each MAC protocol (LoraWan, Sigfox, ...)
- Algorithms
  - Input:
    - Service QoS metrics requiremnts
    - 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 trafic: Videos, Voice, Text
- Environnements
  - Rural/Urban
  - Static/Mobile
  - Tempirature
- Senarios
  - For each application protocol (MQTT, COAP, XMPP)
  - For each network protocol (Start, Mesh)
  - For each MAC protocol (LoraWan, Sigfox, ...)
- Algorithms
  - Input:
    - Service QoS metrics requiremnts
    - MAC configuration (SF, CR, BW, ...)
    - Network QoS metrics
  - Method:
    - MADM, Game, Neural
  - Outputs:
    - Ranked networks

Theoretical, Simulation & Real environnement

Outline

Outline

Outline

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

Multi-Armed-Bandit Algorithm

Methods

- Arms: K = 1, ... , K
- Decision: T = 1, ... , T
- Reward: X_t^k with μ_t^k = E $[X_t^k]$
  - Best reward: X_t^* with μ_t^* = max μ_t^k, k∈K

Genetic Algorithm

Methods [**alkhawlani_access_2008a**]

- Heterogeneous wireless network: (RAT 1 ,RAT 2 ,...,RAT n)
- Criteria up to i (c 1 ,c 2 ,...,c i) the operators, the applications, and the network conditions.
-
- The different sets of scores (d 1 , d 2 ,...,d i) are sent to the MCDM in the second component.
- GA component assigns a suitable weight (w 1 ,w 2 ,...,w i)

Marcov chain

Methods

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

$$r(s_k, a_k) = G_k \cdot PRR(a_k) \tag{2}$$

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

$$PRR = (1 - BER)^L \tag{4}$$

$$BER = 10^{\alpha e^{\beta SNR}} \tag{5}$$

Marcov chain

Methods

HGHGJ

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

$$r(s_k, a_k) = G_k \cdot PRR(a_k) \tag{2}$$

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

$$PRR = (1 - BER)^L \tag{4}$$

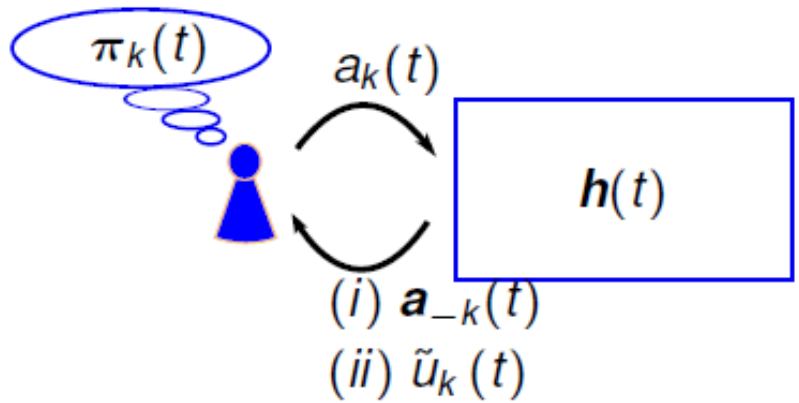
$$BER = 10^{\alpha e^{\beta SNR}} \tag{5}$$

Marcov chain

Methods

Learning Iterative Steps:

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



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

$$\pi_k(t) \overset{t\to\infty}{\longrightarrow} \pi_k^* \tag{1}$$

$$\bar{u}_k(\pi_k(t), \pi_{-k}(t)) \overset{t\to\infty}{\longrightarrow} \bar{u}_k(\pi_k^*, \pi_{-k}^*) \tag{2}$$

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

Figure 6: .

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)
  - x_2: 11000 (576) (49.2)
  - x_3: 01000 (64) (5.5)
  - x_4: 10011 (361) (30.9)

Game theory

Methods

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

... (step 2)

Methods

... (step 3)

Methods

... (step 4)

Methods

➠

➠

Results

Comparison

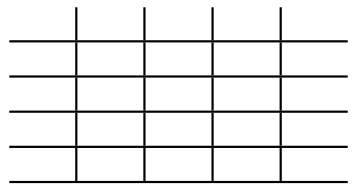


Table 4

Outline

Experimentation

Experimentation

- a
- b

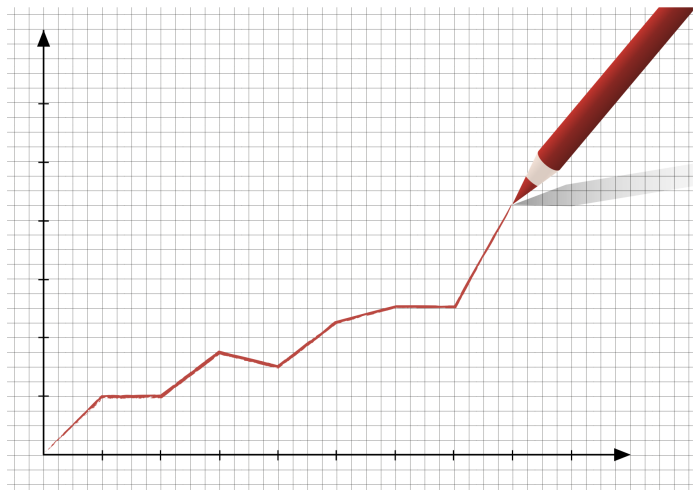


Figure 7: .

Outline

Results

Comparison

- a
- b

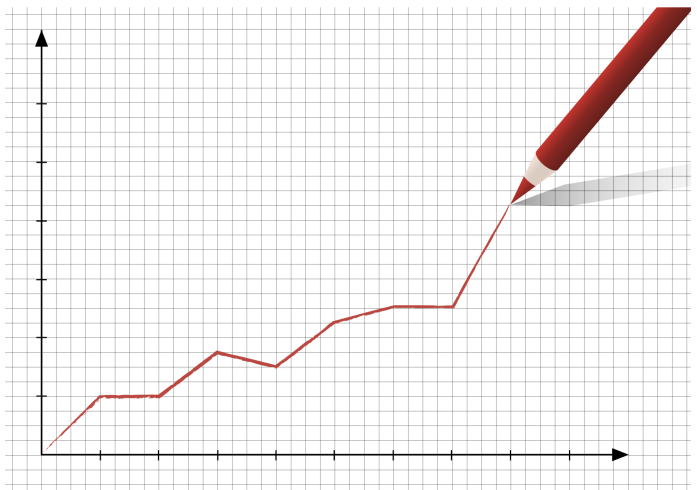


Figure 8: .

Outline

Discussion

- a
- b

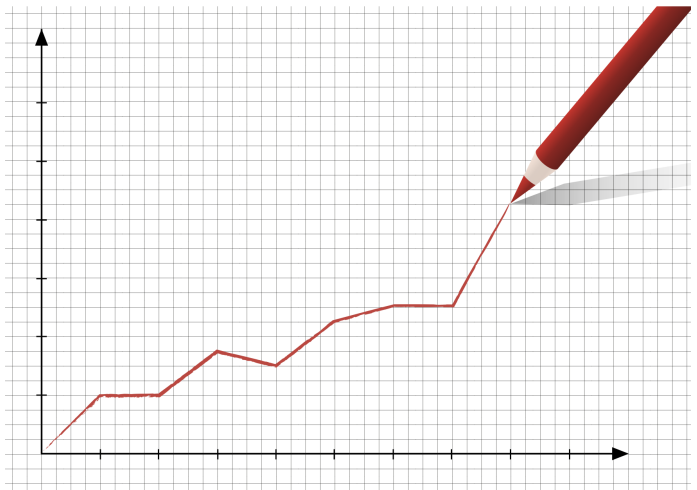


Figure 9: .

Outline

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

	World (2018)	World (2022)	France (2018)
Users	3.8 billion	4.2 billion	25.9 million
Email accounts	4.4 billion	5.6 billion	68 million
Email accounts per user	1.7	1.9	2.1
Emails received each day	281 billion	333 billion	1.4 billion
The email market	9.8 Mrds $	20.4 Mrds $	?

Table 5: Email statistics [**BibEntry2019Mar**].

- Email:
  - More than 50% of the world population use email
  - Usage: 75% personal, 25% professional
- Facebook:
  - 2.2 billion active users (29% worldwide)
  - 10 billion messages are sent every day
  - 8.051 billion $

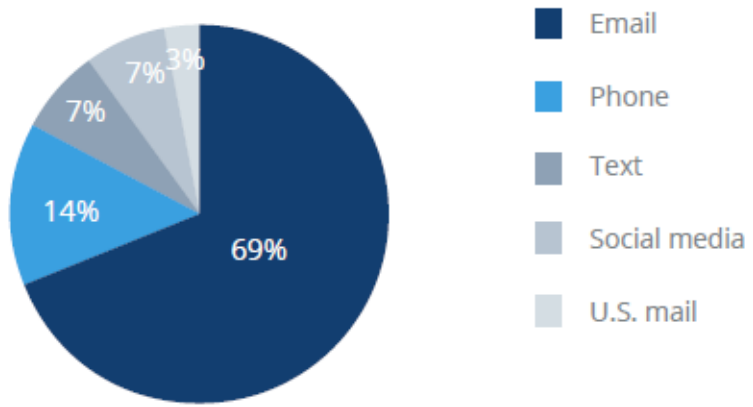


Figure 10: Communication tools [**BibEntry2019Mar**].

Context

Introduction

	World (2018)	World (2022)	France (2018)
Users	3.8 billion	4.2 billion	25.9 million
Email accounts	4.4 billion	5.6 billion	68 million
Email accounts per user	1.7	1.9	2.1
Emails received each day	281 billion	333 billion	1.4 billion
The email market	9.8 Mrds $	20.4 Mrds $	?

Table 12: Email statistics [**BibEntry2019Mar**].

- Email:
  - More than 50% of the world population use email
  - Usage: 75% personal, 25% professional
- Facebook:
  - 2.2 billion active users (29% worldwide)
  - 10 billion messages are sent every day
  - 8.051 billion $

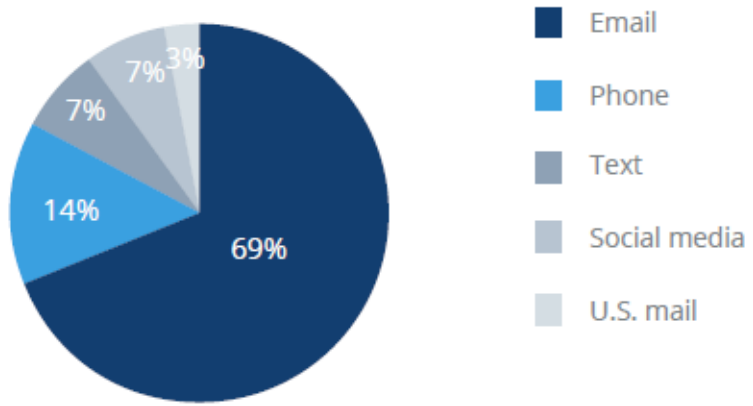


Figure 24: Communication tools [**BibEntry2019Mar**].

Problematic

Introduction

- Privacy issues:

- **External vulnerabilities**
  - Network technologies: 4G, 5G, Wifi, Ethernet.
  - Security protocols: HTTPS, SMTPS, IPsec
- **Internal vulnerabilities**
  - Service providers
    - General Terms and Conditions of Use (GTC)
  - 3^{rd} parties
    - Privacy settings
    - Permission management
  - Users
    - Configuration of user accounts
    - Users list management

Figure 11: Privacy, Am I concerned ?.

Problematic

Introduction

- Privacy issues:

- **External vulnerabilities**
  - Network technologies: 4G, 5G, Wifi, Ethernet.
  - Security protocols: HTTPS, SMTPS, IPsec
- **Internal vulnerabilities**
  - Service providers
    - General Terms and Conditions of Use (GTC)
  - 3^{rd} parties
    - Privacy settings
    - Permission management
  - **Users**
    - **Configuration of user accounts**
    - **Users list management**

Figure 25: Privacy, Am I concerned ?.

Motivation

Introduction

- Give users a way to measure their vulnerabilities
- Help users to better configure their email accounts.
- Alert users of a new vulnerability.
- Make users aware about the level of threat diffusion.

Figure 12: Privacy index [3].

Challenges

Introduction

- Recommend customized security measures
  - New password every time period
  - Secure the exchange with vulnerable accounts
  - Adapt permissions to changes
- Vulnerability measurement of the social environment
  - Measure the level of vulnerability of interactions
  - Measure the level of influence between users.
- Calculate the vulnerability of the message path
  - Identification of MTA servers
  - Assign a trust score to each server
  - Calculate the average confidence of the path.

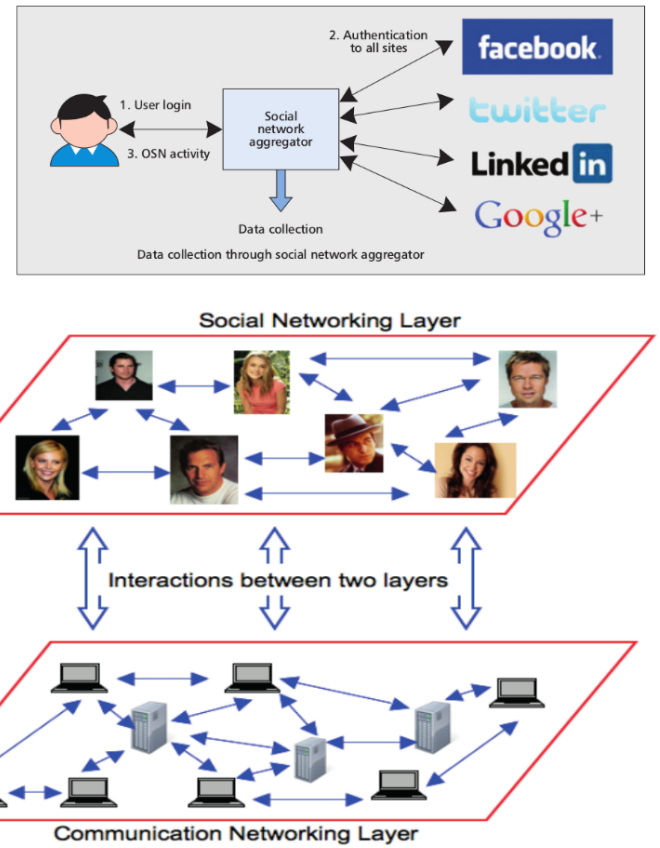


Figure 13: Social interaction.

Challenges

Introduction

- Recommend customized security measures
  - New password every time period
  - Secure the exchange with vulnerable accounts
  - Adapt permissions to changes
- **Vulnerability measurement of the social environment**
  - **Measure the level of vulnerability of interactions**
  - **Measure the level of influence between users**
- Calculate the vulnerability of the message path
  - Identification of MTA servers
  - Assign a trust score to each server
  - Calculate the average confidence of the path.

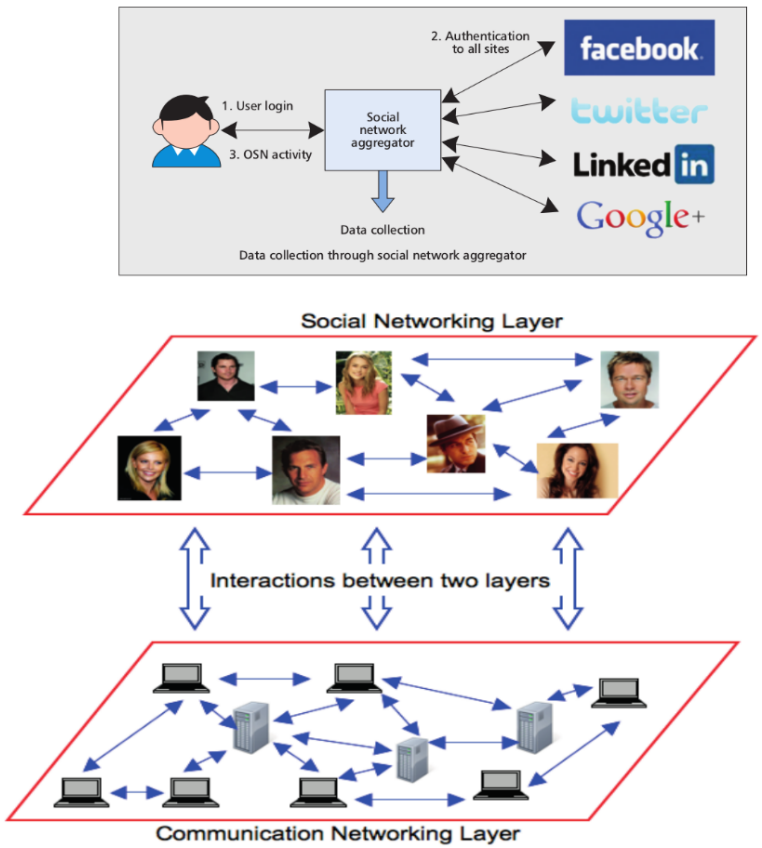


Figure 27: Social interaction.

Contributions

Introduction

- Social vulnerability estimation.
  - Individual vulnerability -> Social vulnerability.
  - Vulnerability diffusion process.
  - Relationship between trust and vulnerability.
  - Data: Enron & Caliopen emails.

Figure 14: The vulnerability of one user is the vulnerability of all users.

Outline

Related work

Comparison

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

Table 6: Contributions from existing work.

Outline

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 7: 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

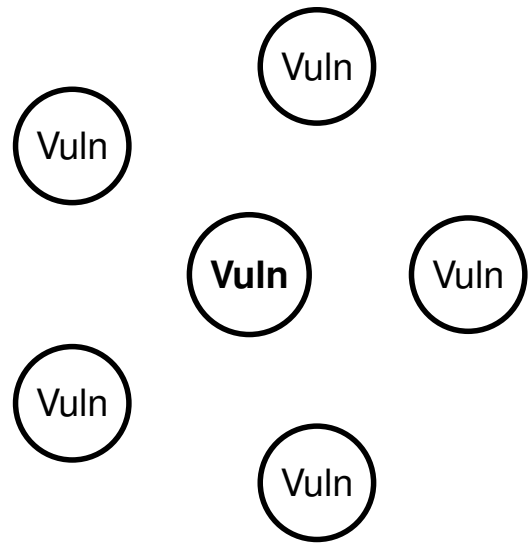


Figure 15: Individual vulnerability level.

Step 2: Users reputation estimation

Method

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

Table 8: Trust grant features

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

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

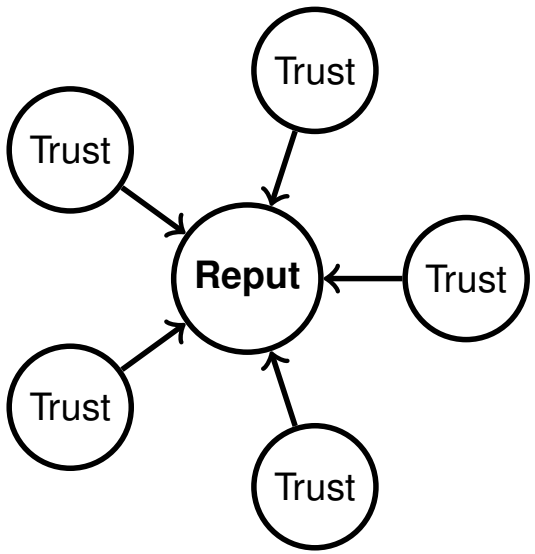


Figure 16: Reputation level.

Step 3: Social vulnerability measurement

Freidkin's theory of social influence

- Input (Features):
  - $Y^{(1)}$ = Vector of the individual vulnerabilities of N users (eq 9)
  - α= The level of reputation (influence) of each user (eq 10)
  - M = Adjacency matrix N x N
- Model:

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

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

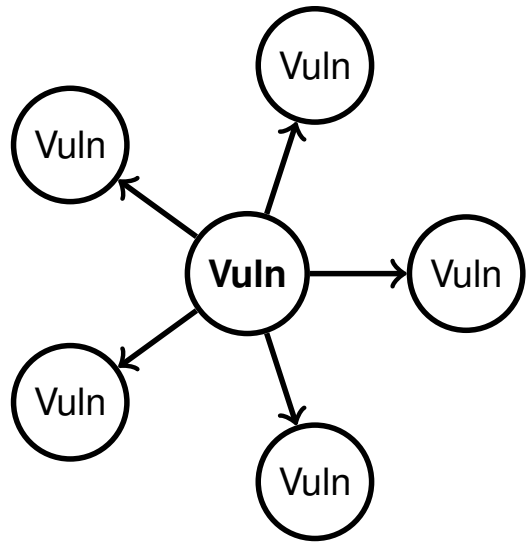


Figure 17: Social vulnerability.

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.

$$Y^{(t)} = 1 * MY^{(t-1)} + (1-1)\,Y^{(t-1)} \tag{11}$$

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

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

$$Y^{(t)} = 0 * MY^{(t-1)} + (1-0)\,Y^{(t-1)} \tag{11}$$

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

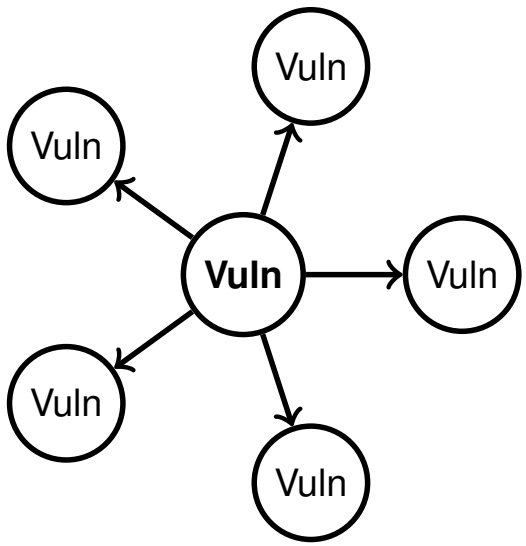


Figure 18: Social vulnerability.

Outline

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 9: Enron dataset properties.

Figure 19: 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 10: Caliopen dataset properties.

Figure 20: Caliopen logo.

Results

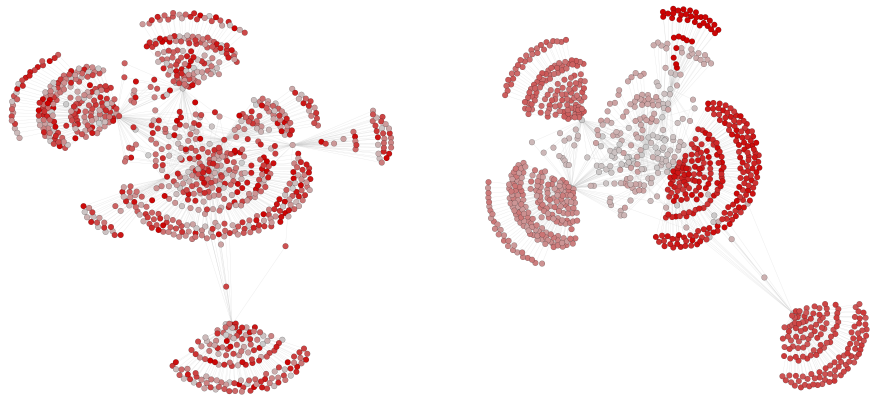
Comparison

Initial values:

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

Final values:

- obtained after convergence.
- represent social vulnerabilities.



(a) Individual privacy vulnerability.

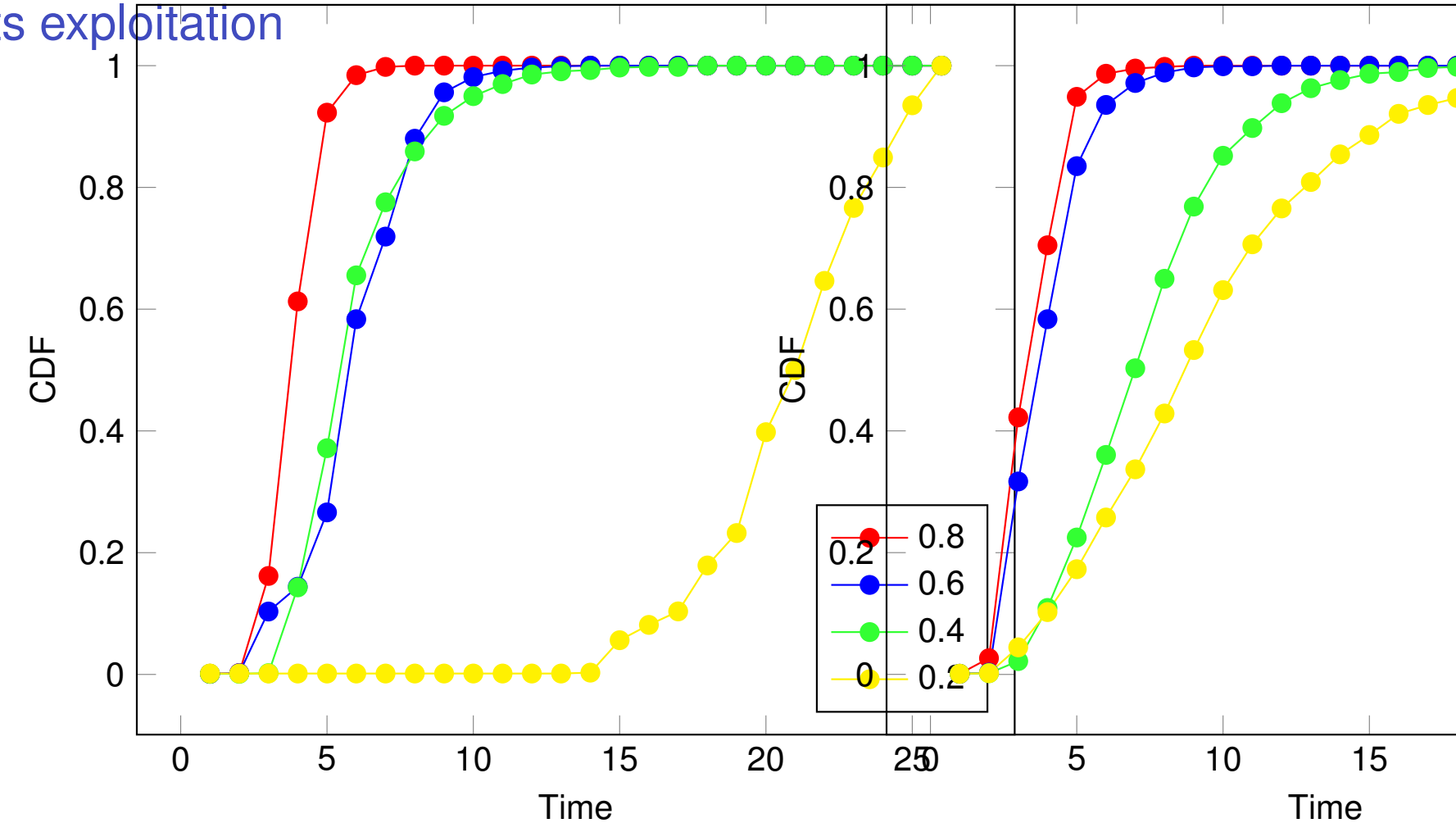
(b) Social privacy vulnerability.

Figure 21: 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 11: Individual and social privacy vulnerabilities.

Results exploitation



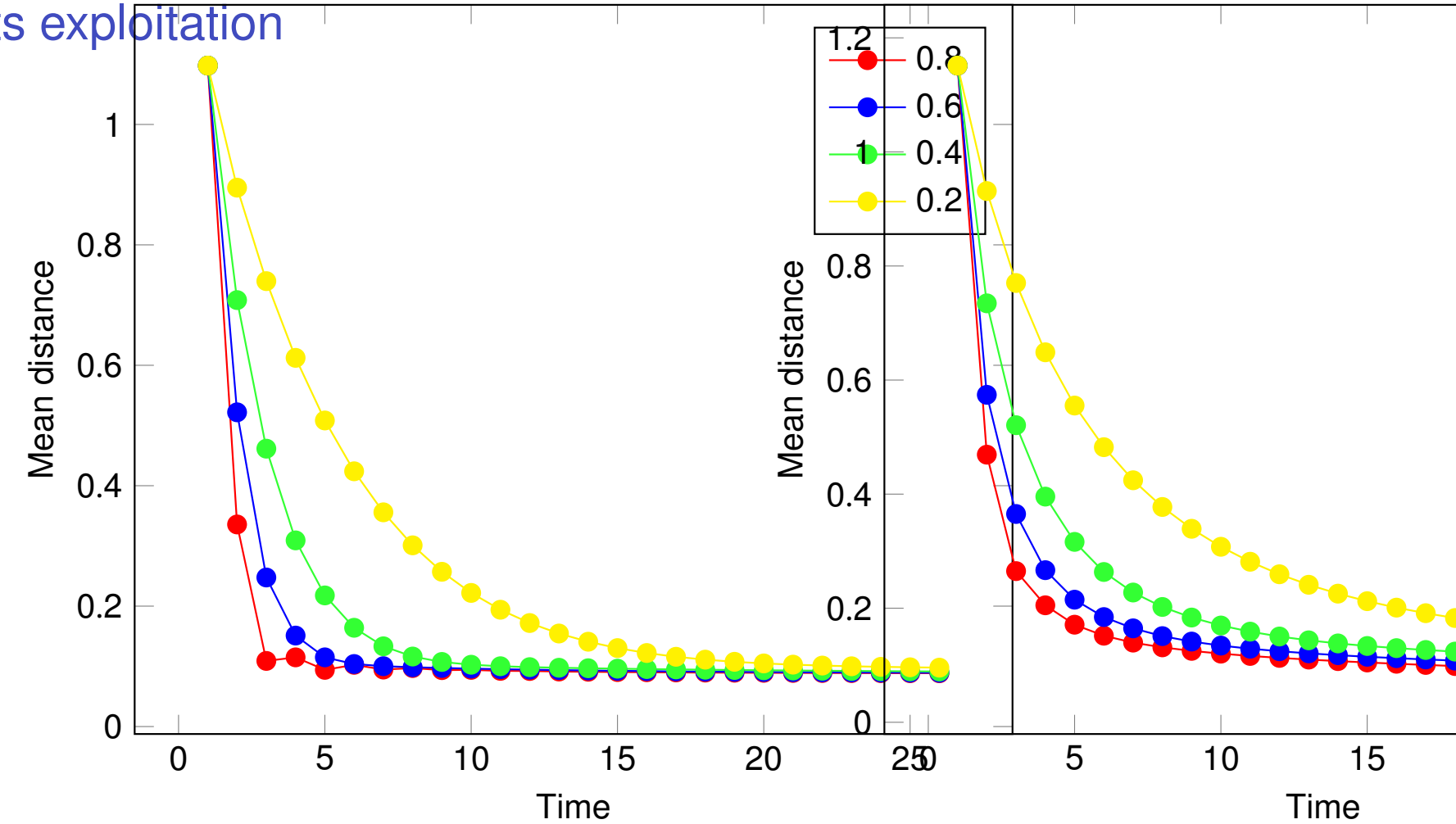
(a) Enron dataset.

(b) Caliopen dataset.

Figure 22: Cumulative distribution function of infected users.

- Figures shows the CDF of the vulnerability diffusion process.

Results exploitation



(a) Enron dataset.

(b) Caliopen dataset.

Figure 23: Convergence of the diffusion process.

- The process converge when the mean distance between social vulnerability scores is the minimum.

Conclusion

- 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.

Conclusion

- 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

Outline

	World (2018)	World (2022)	France (2018)
Users	3.8 billion	4.2 billion	25.9 million
Email accounts	4.4 billion	5.6 billion	68 million
Email accounts per user	1.7	1.9	2.1
Emails received each day	281 billion	333 billion	1.4 billion
The email market	9.8 Mrds $	20.4 Mrds $	?

Table 12: Email statistics [**BibEntry2019Mar**].

- Email:
  - More than 50% of the world population use email
  - Usage: 75% personal, 25% professional
- Facebook:
  - 2.2 billion active users (29% worldwide)
  - 10 billion messages are sent every day
  - 8.051 billion $

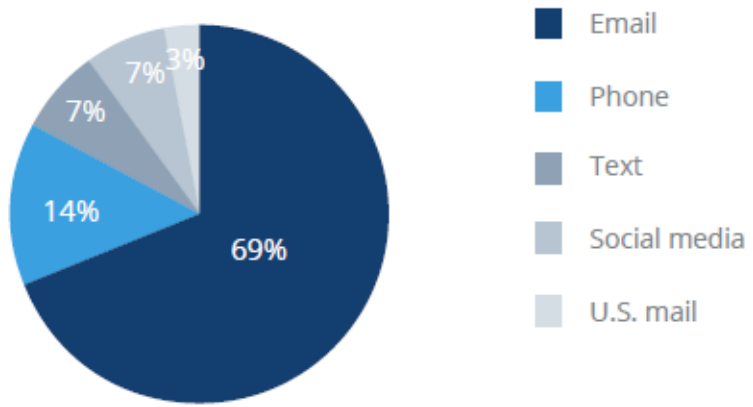


Figure 24: Communication tools [**BibEntry2019Mar**].

	World (2018)	World (2022)	France (2018)
Users	3.8 billion	4.2 billion	25.9 million
Email accounts	4.4 billion	5.6 billion	68 million
Email accounts per user	1.7	1.9	2.1
Emails received each day	281 billion	333 billion	1.4 billion
The email market	9.8 Mrds $	20.4 Mrds $	?

Table 12: Email statistics [**BibEntry2019Mar**].

- Email:
  - More than 50% of the world population use email
  - Usage: 75% personal, 25% professional
- Facebook:
  - 2.2 billion active users (29% worldwide)
  - 10 billion messages are sent every day
  - 8.051 billion $

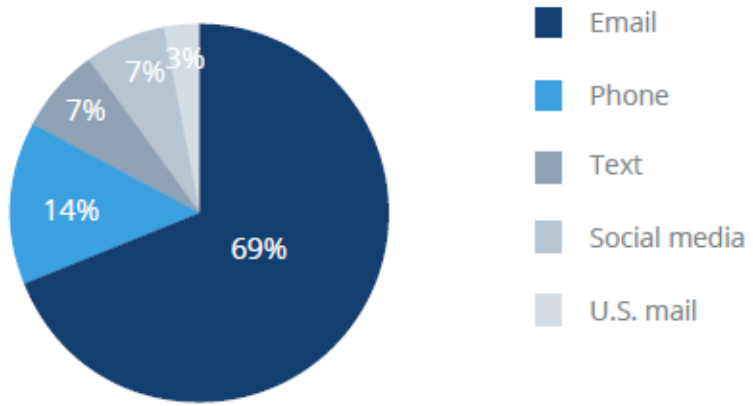


Figure 24: Communication tools [**BibEntry2019Mar**].

- Privacy issues:

- **External vulnerabilities**
  - Network technologies: 4G, 5G, Wifi, Ethernet.
  - Security protocols: HTTPS, SMTPS, IPsec
- **Internal vulnerabilities**
  - Service providers
    - General Terms and Conditions of Use (GTC)
  - 3^{rd} parties
    - Privacy settings
    - Permission management
  - Users
    - Configuration of user accounts
    - Users list management

Figure 25: Privacy, Am I concerned ?.

- Privacy issues:

- **External vulnerabilities**
  - Network technologies: 4G, 5G, Wifi, Ethernet.
  - Security protocols: HTTPS, SMTPS, IPsec
- **Internal vulnerabilities**
  - Service providers
    - General Terms and Conditions of Use (GTC)
  - 3^{rd} parties
    - Privacy settings
    - Permission management
  - **Users**
    - **Configuration of user accounts**
    - **Users list management**

Figure 25: Privacy, Am I concerned ?.

Motivation

Introduction

- Give users a way to measure their vulnerabilities
- Help users to better configure their email accounts.
- Alert users of a new vulnerability.
- Make users aware about the level of threat diffusion.

Figure 26: Privacy index [3].

Challenges

Introduction

- Recommend customized security measures
  - New password every time period
  - Secure the exchange with vulnerable accounts
  - Adapt permissions to changes
- Vulnerability measurement of the social environment
  - Measure the level of vulnerability of interactions
  - Measure the level of influence between users.
- Calculate the vulnerability of the message path
  - Identification of MTA servers
  - Assign a trust score to each server
  - Calculate the average confidence of the path.

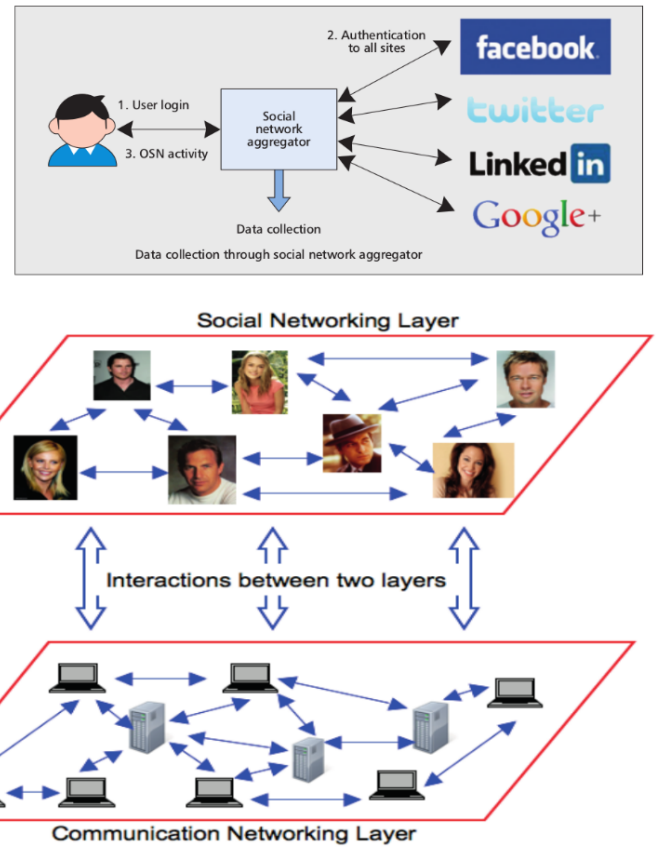


Figure 27: Social interaction.

Challenges

Introduction

- Recommend customized security measures
  - New password every time period
  - Secure the exchange with vulnerable accounts
  - Adapt permissions to changes
- **Vulnerability measurement of the social environment**
  - **Measure the level of vulnerability of interactions**
  - **Measure the level of influence between users**
- Calculate the vulnerability of the message path
  - Identification of MTA servers
  - Assign a trust score to each server
  - Calculate the average confidence of the path.

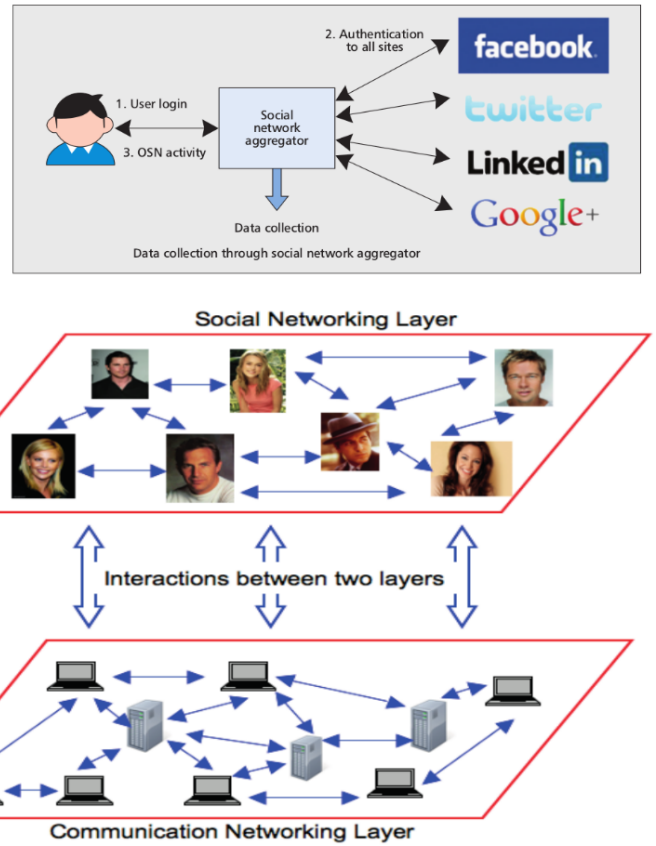


Figure 27: Social interaction.

Contributions

Introduction

- Social vulnerability estimation.
  - Individual vulnerability -> Social vulnerability.
  - Vulnerability diffusion process.
  - Relationship between trust and vulnerability.
  - Data: Enron & Caliopen emails.

Figure 28: The vulnerability of one user is the vulnerability of all users.

Outline

Travaux connexes

Comparaison

Travaux	Contribution	Performance
[4] Protect U	Classification des interlocuteurs	Configuration des listes d'amis
[5] Privacy Wizard	Classification des interlocuteurs	Configuration des permissions
[6] SocialMarket	Intérêt communs	Évaluation des relation de confiance
[7] TAPE	Fuite d'information	Évaluation de la diffusion de l'info
[8] LENS	Protection anti-spam	Évaluation des émetteurs de confiance
[9] SocialEmail	Classer les chemins des msg	Évaluation de la fiabilité du message
[10] Privacy Index	Visibilité, sensibilité	Évaluation de l'exposition des msg

Table 13: Contributions des travaux existants.

Outline

Etape 1: Calcule de la vulnérabilité individuelle

Méthode

- Entrée:
  - Vulnérabilité de la machine utilisée:
    - Connexion réseaux (privé (1) ou publique (2))
    - Type d'architecture: Ethernet, 5G, 4G, Wifi (1:4)
    - Système d'exploitation (Windows, Unix) (1:2)
    - Navigateur web (1:10)
  - Vulnérabilité du compte utilisé
    - Mdp utilisé, mode de récupération des mdp (1:5)
    - Nombre de sessions ouvertes en même temps.(1:nbr)
    - Mode de chiffrement, signature, version TLS
- Sortie:

$$Pi = \sum_{i}^{n} \frac{w * V}{n} \quad (9)$$

  - Pi: Vulnérabilité individuelle
  - w: Poids de chaque vulnérabilité
  - V: Les vulnérabilités cités au dessus

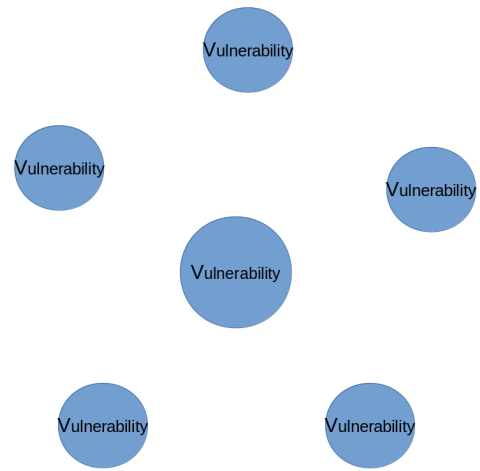


Figure 29: Vulnérabilité individuelle.

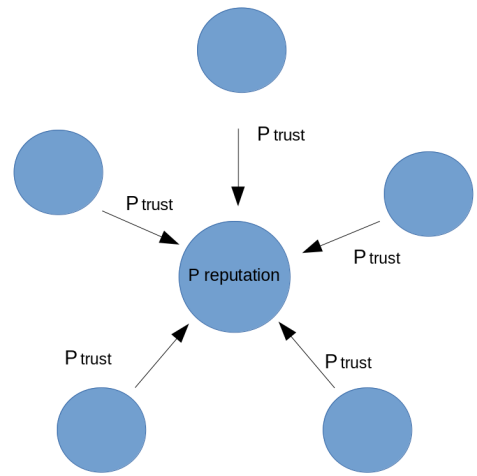
Etape 2: Calcule de la réputation des utilisateurs

Méthode

- Entrée:
  - Fréquence d'utilisation de la messagerie.
  - Horaire, durée des échanges (1:5)
  - % des échanges chiffrés, signés, claires (1:3)
  - Importance des interlocuteurs: Liste favoris (2), noir(1)
  - Type de données: Texte, images, vidéos, script (1:4)
- Méthode:
  - Loi binomiale
- Output:

$$P(reputation) = P(X \geq 1) = 1 - (1 - P(trust))^n \qquad (10)$$

  - Where,
    - X: Niveau de confiance, X ~B(n,p)
    - n: deg(noeud)
    - P(X=1): La probabilité de se faire attribué une confiance par un interlocuteur



P reputation = 1 - (1 - P trust)^n

Figure 30: Niveau de réputation.

Etape 3: Calcule de la vulnérabilité sociale

Théorie de l'influence sociale de Freidkin

- Entrée:
  - $Y^{(1)}$ = Vecteur des vulnérabilités individuelles de N utilisateurs (eq 9)
  - α= Le niveau de réputation (d'influence) de chaque utilisateur (eq 10)
  - M = Matrice d'adjacence N x N
- Modèle:

$$Y^{(t)} = \alpha M Y^{(t-1)} + (1-\alpha) Y^{(t-1)} \qquad (11)$$

- Sortie:
  - $Y^{(t)}$ = Vecteur des vulnérabilités sociales des N utilisateurs

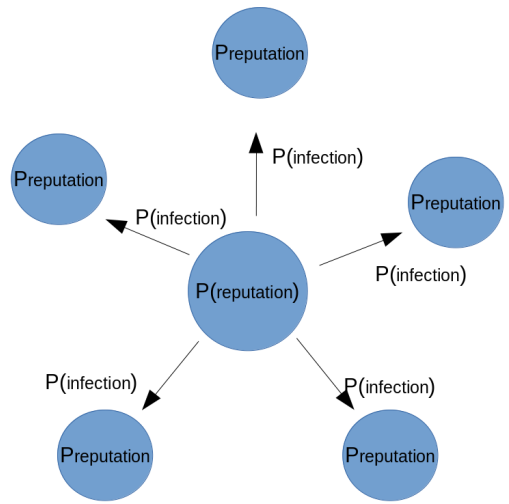


Figure 31: Vulnérabilité Sociale.

Etape 3: Calcule de la vulnérabilité sociale

Théorie de l'influence sociale de Freidkin

Propriétés formelles du modèle:

- Lorsque l'influence d'un utilisateur est élevé, le modèle se réduit aux:
  - vulnérabilités moyennes de ses amis pondérées par leur niveaux de confiances.

$$Y^{(t)} = 1 * MY^{(t-1)} + (1-1)Y^{(t-1)} \quad (11)$$

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

- En absence d'influence, le modèle se réduit à:
  - sa propre vulnérabilité pondérée par le niveau de méfiance de ses amis

$$Y^{(t)} = 0 * MY^{(t-1)} + (1-0)Y^{(t-1)} \quad (11)$$

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

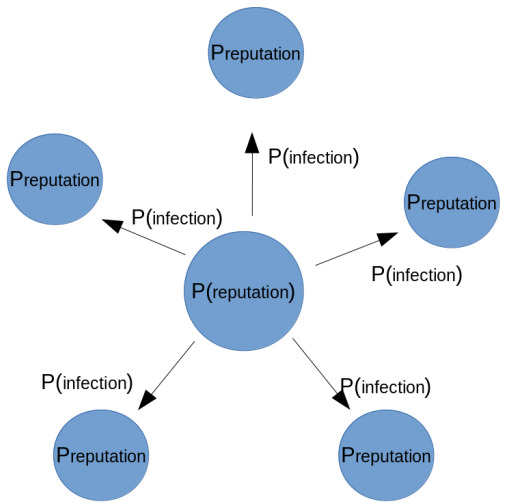


Figure 32: Vulnérabilité sociale.

Outline

Paramètre	Valeur
Utilisateurs	958
Messages	6966
Diamètre	958
# de msg en moyenne	2.413361
Densité des msg	0.00252
Modularité	0.654600
Distance moyenne	3.042114

Table 14: Propriétés des données Enron.

Figure 33: Enron logo.

Paramètre	Valeur
Utilisateurs	5885
Messages	26547
Diamètre	2096
# de msg en moyenne	9.02192
Densité des msg	0.001533
Modularité	0.86526
Distance moyenne	3.914097

Table 15: Propriétés des données Caliopen.

Figure 34: Caliopen logo.

Outline

Résultats

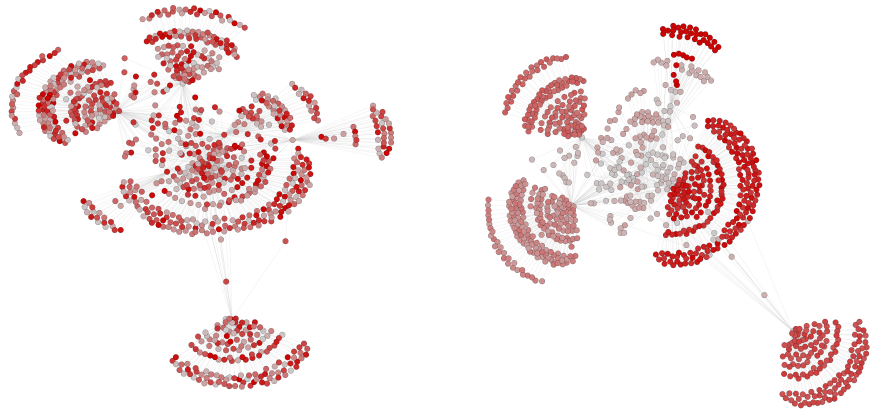
Comparaison

Valeurs initiales:

- générées aléatoirement (distribution normale)
- représentent les vulnérabilités individuelles.
- couleur foncée = vulnérabilité élevé

Valeurs finales:

- obtenu après convergence.
- représentent les vulnérabilités sociales.



(a) Vulnérabilité individuelle.

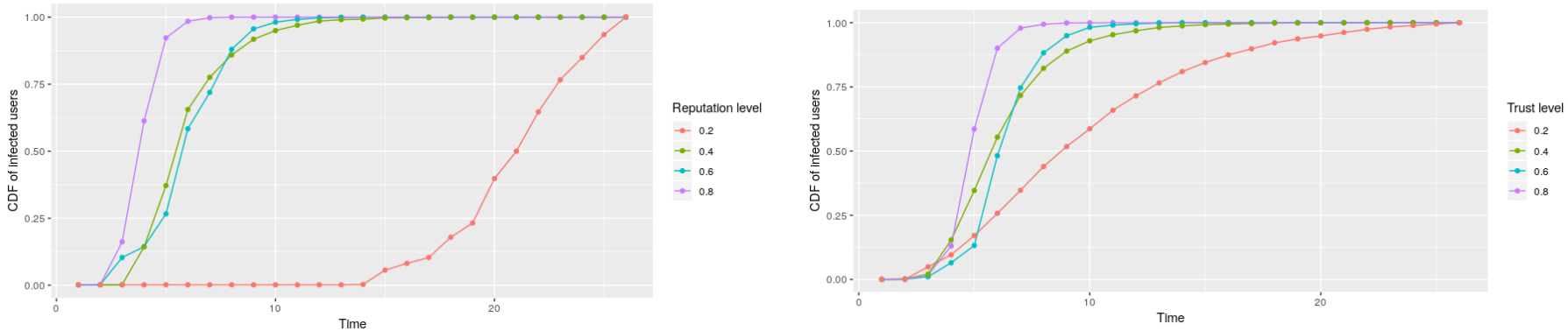
(b) Vulnérabilité Sociale.

Figure 35: Vulnérabilité individuelle & sociale.

User ID	Vul individuel	Vul sociale
34	0.84	0.67
67	0.12	0.87
206	0.76	0.33
588	0.23	0.78

Table 16: Différence entre les vulnérabilités individuelles et sociales en matière de protection de la vie privée.

Exploitation des résultats



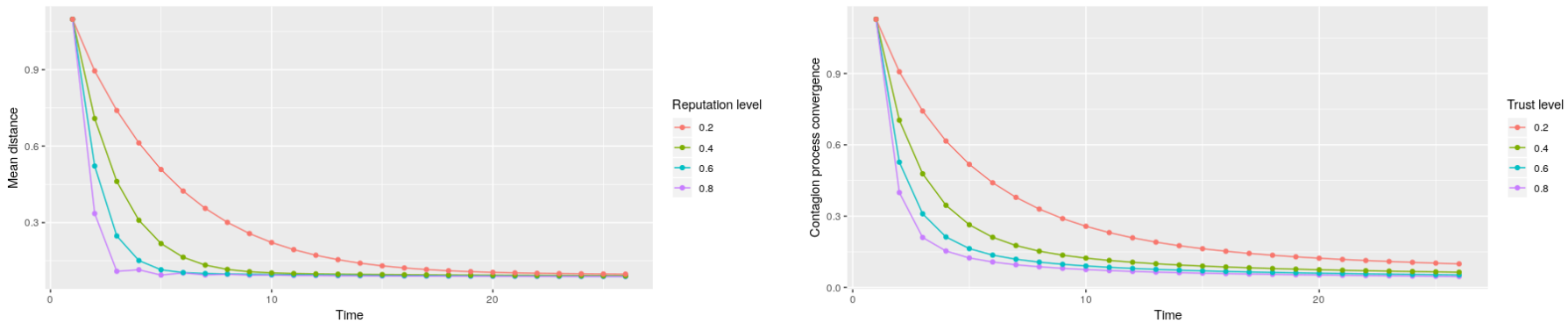
(a) Les données de Enron.

(b) Les données de Caliopen.

Figure 36: Fonction de distribution cumulative des utilisateurs infectés.

- Les utilisateurs avec des valeurs de réputation élevées contribuent considérablement à la diffusion
- Ils diffusent leur vulnérabilités rapidement et largement dans la messagerie.

Exploitation des résultats



(a) Les données de Enron.

(b) Les données de Caliopen.

Figure 37: Convergence du processus de diffusion.

- Attribuer une confiance à des utilisateurs vulnérables leur permet d'obtenir un niveau de réputation élevé.
- Par conséquent, infecter l'ensemble des valeurs de vulnérabilité de la messagerie.

Conclusion

- Le but de ce travail est de simuler un processus de contamination des vulnérabilités individuelles.
  - La vulnérabilité d'un utilisateur est la vulnérabilité de tous.
  - A la fin de la diffusion, tous les utilisateurs auront un indice de vulnérabilité social.
- Travaux futures
  - Proposer des mécanismes pour améliorer la réputation des utilisateurs non-vulnérables.
    - Suggérer des interlocuteurs bien réputés avec des indices de vulnérabilité acceptables.
  - Proposer des mécanismes pour améliorer la vulnérabilité des utilisateurs réputés.
    - Recommander des configurations et des logiciels.

Conclusion

- Le but de ce travail est de simuler un processus de contamination des vulnérabilités individuelles.
  - La vulnérabilité d'un utilisateur est la vulnérabilité de tous.
  - A la fin de la diffusion, tous les utilisateurs auront un indice de vulnérabilité social.
- Travaux futures
  - Proposer des mécanismes pour améliorer la réputation des utilisateurs non-vulnérables.
    - Suggérer des interlocuteurs bien réputés avec des indices de vulnérabilité acceptables.
  - Proposer des mécanismes pour améliorer la vulnérabilité des utilisateurs réputés.
    - Recommander des configurations et des logiciels.

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 (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 (p. 7).

[3] E. Michael Maximilien et al. “ Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform ”. In: *Proceedings of Web*. Vol. 2. 00054. 2009 (p. 48, 72).

[4] Ala Eddine Gandouz. “ PROTECT_U: Un Systeme Communautaire Pour La Protection Des Usagers de Facebook ”. In: (2012). 00001, p. 77 (p. 53, 77).

[5] Lujun Fang and Kristen LeFevre. “ Privacy Wizards for Social Networking Sites ”. In: 00397. ACM Press, 2010, p. 351 (p. 53, 77).

[6] 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 (p. 53, 77).

[7] 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 (p. 53, 77).

[8] 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 (p. 53, 77).

[9] 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 (p. 53, 77).

[10] Raj Kumar Nepali and Yong Wang. “ SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking ”. In: 00021. IEEE, July 2013, pp. 162–166 (p. 53, 77).