Università degli Studi di Firenze

Scuola di Ingegneria

Dipartimento di ingegneria dell'informazione

Fraudsters detection in the international IP telephony market: an approach based on analysis of reputation

Relatore:	**Candidato:**
Ing. Francesco Chiti	Francesco Ermini
Ing. Tommaso Pecorella	

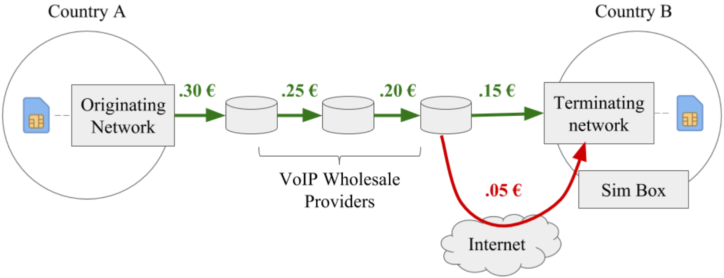
Firenze, 3 aprile 2019

Index

1. Problem
   - Fraud workflow
   - Frauds detection
   - Fraudsters detection
2. Idea
3. Solution
   - Trust Overlay Network
   - Reputation based routing
   - Simulation
4. Results
   - Detection error & delay
   - Benefit costs analysis
5. Conclusion

Fraud workflow

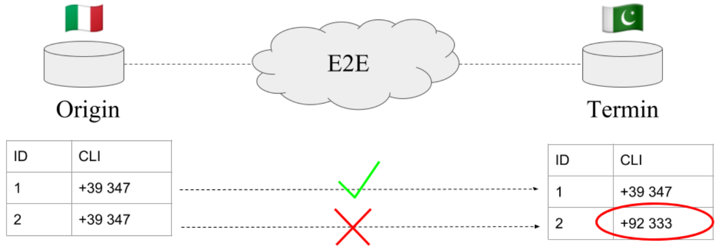
Interconnect bypass fraud



🟩 Legal (white route) 🟥 Fraud (black route)

Fraud detection

Interconnect bypass fraud detection



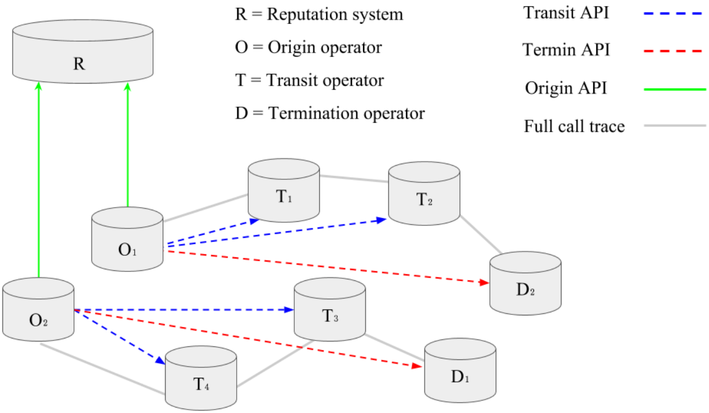
ID	CLI
1	+39 347
2	+39 347

ID	CLI
1	+39 347
2	+92 333

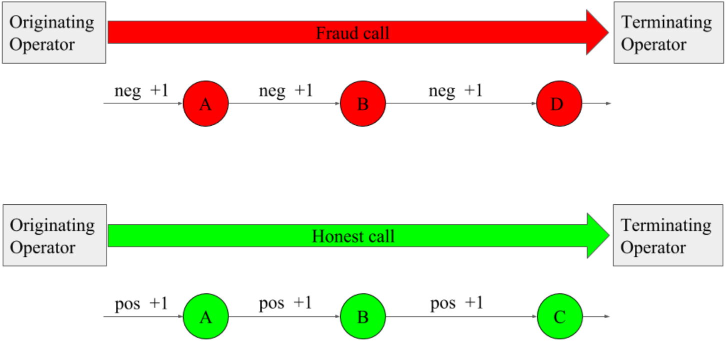
Fraudster detection

1. Lack of transparency in the signaling protocol hides identities of transit operators
2. Absence of proven evidences inhibit pinpointing the truth fraudster (without forensic investigations)

Idea (1): Cooperative design



Idea (2): Guilty assumption & behavioral analysis



Trust Overlay Network (1)

m_{ij} = calls from Telco i to Telco j in period t

$$M_t = \begin{bmatrix} n.a & \begin{pmatrix} pos = 10 \\ neg = 5 \end{pmatrix} & \dots & \begin{pmatrix} pos = 15 \\ neg = 7 \end{pmatrix} \\ \begin{pmatrix} pos = 3 \\ neg = 1 \end{pmatrix} & n.a & \dots & \begin{pmatrix} pos = 0 \\ neg = 0 \end{pmatrix} \\ \vdots & & \ddots & \vdots \\ \begin{pmatrix} pos = 0 \\ neg = 0 \end{pmatrix} & \begin{pmatrix} pos = 0 \\ neg = 0 \end{pmatrix} & \dots & n.a \end{bmatrix}_{N \times N} \tag{1}$$

$$M_t^{'} = \sum_{0 \leq c \leq c_{max}} M_{t-c} \lambda_c \qquad \lambda_c = \frac{c_{max} - c}{c_{max}} \tag{2}$$

Trust Overlay Network (2)

Trust Network Analysis with Subjective Logic[1]

Opinion: $$\omega_x^A \triangleq (b, d, u, a) \qquad \textit{with} \quad b, d, u, a \in [0, 1] \tag{3}$$

$$\omega_x^A = \begin{cases} b = \frac{p}{p+n+2} \\ d = \frac{n}{p+n+2} \\ u = \frac{2}{p+n+2} \\ a = \text{base rate of x} \end{cases}$$

discount: $$\omega_T^{A:B} = \omega_A^T \bigotimes \omega_T^B \tag{4}$$

consensus: $$\omega_F^{A \circ B} = \omega_A^B \bigoplus \omega_F^B \tag{5}$$

[1] Trust Network Analysis with Subjective Logic, Josang, Audun & Hayward, Ross & Pope, Simon. (2006).

Trust Overlay Network (3)

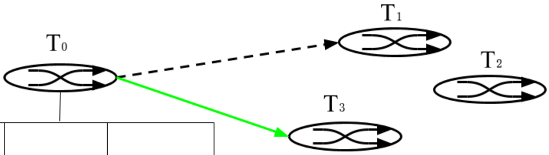
Reputation score of A against B

$$\textbf{Reputation:} \quad R(\omega_A^B) = b + au, \qquad R \in [0, 1.0] \tag{6}$$

$$R(\omega_A^B) = \begin{cases} \text{fraudster} & \textit{if} \quad R < 0.5 \\ \text{honest} & \textit{if} \quad R > 0.8 \\ \text{suspect} & \textit{if} \quad 0.5 < R \leq 0.8 \\ \text{missing} & \textit{if} \quad R = 0.5 \end{cases}$$

Reputation based routing

Telcos with R < 0.5 added to a temporary blacklist

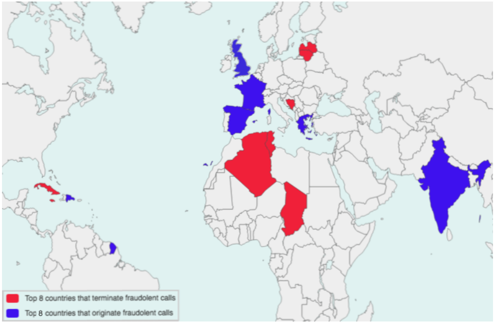


Routing decision	Forward To	Price	Reputation
1°	T_3	0.20 €/min	0.82
2°	T_3	0.25 €/min	0.91
~~3°~~	~~T_2~~	~~0.12 €/min~~	~~0.23~~

▬	Selected LCR route:
🟩	Honest route
🟥	Fraud route
- - - -	Ignored routes

Emulate daily Telcos interconnection

- 145 MOs [2] &
  368 VoIP carriers [3]
  1% Fraudsters
- 3000 daily calls/simbox
  5% Frauds [4]
  240k daily calls rate
- 10% MOs, 5% VoIP carriers cooperate


🟥 Top 8 countries that terminate fraudolent calls
🟦 Top 8 countries that originate fraudolent calls

[1] 2017 Global Fraud Loss Survey, CFCA

[2] ITU, MNC & MCC codes, 2016

[3] voipproviderslist.com

[4] slideshare.net/AkhilRawat/sim-box

Simulation

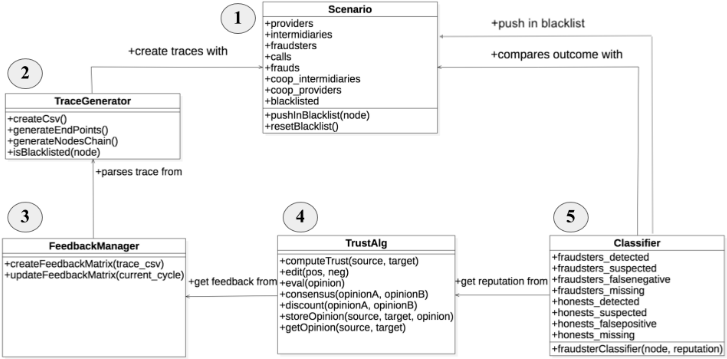


Figure: UML conceptual model

[1] github.com/FrancescoErmini/FraudDetectorSimulator

Detection error & delay

Detection statistics by changing feedback collection period

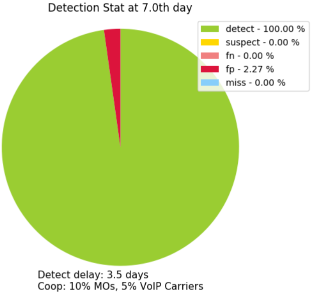


Figure: Less delay, more errors

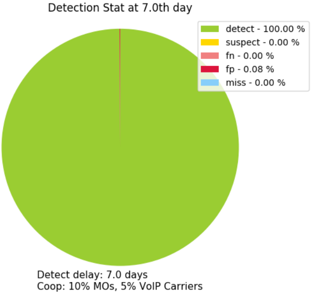
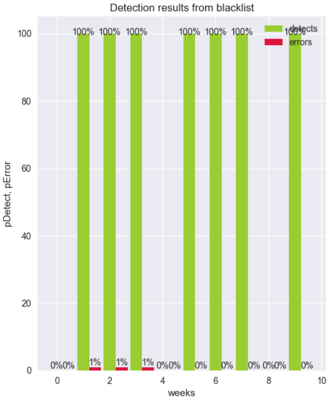
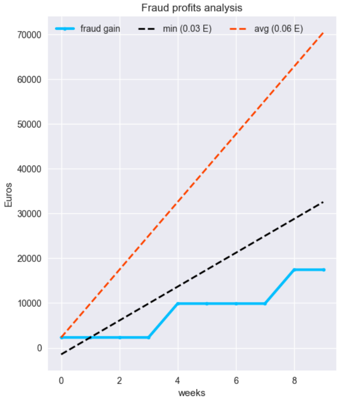


Figure: More delay, less errors

Benefit costs analysis

Evaluate fraud profit loss when blacklisted





Disguised fraud strategy

Detection statistics in case of frauds reduction from 5% to 2.5% (a) and 1% (b)

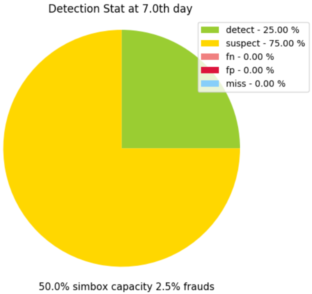


Figure: (a) Partially detected

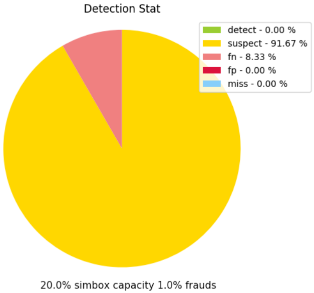
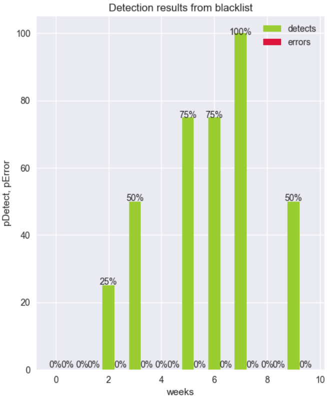
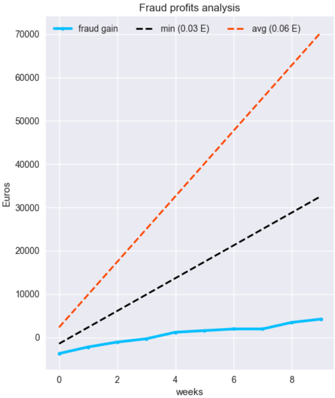


Figure: (b) Fully undetected

Benefit costs analysis with disguised strategy

Evaluate fraud profit loss when blacklisted





Conclusion

Validation in the emulated scenario

- **Detection error:** A priori accusations against honest nodes do not compromise the correct classification.

- **Time delay:** One week delay is acceptable because is the time taken by Telcos to share CDR.

Future directions

Validation in the real scenario

- **Lack of comparison data:** There is a practical difficulty in obtaining call traces (all traces, not only frauds) from multiple Telcos that have some common callID and contains proven fraudsters (Suspended CICs licenses or blacklisted SIP IDs).

Università degli Studi di Firenze

Scuola di Ingegneria

Dipartimento di ingegneria dell'informazione

Fraudsters detection in the international IP telephony market: an approach based on analysis of reputation

Relatore:	**Candidato:**
Ing. Francesco Chiti	Francesco Ermini
Ing. Tommaso Pecorella	

Firenze, 3 aprile 2019