Graph-Based Sybil Detection: a caccia di falsi profili nel grafo di un Social Network

Candidato:

Matteo D'Angelo

Relatori:

Prof. Marco Liverani

Dott. Stefano Guarino

Tesi di Laurea Magistrale in Matematica
Università degli Studi Roma Tre

Anno Accademico 2014/2015

Falsi profili nei Social Network

Nell'ambito dei Social Network, un profilo che non corrisponde alla vera identità di una persona viene tipicamente denominato ***Sybil*** e di conseguenza un attacco basato su falsi profili viene chiamato ***Sybil Attack***.

Perché sono pericolosi i falsi profili?

I falsi profili in un *Social Network* possono essere utilizzati per differenti motivi, tra cui:

- Diffondere *malware* (*i.e.*, programmi creati appositamente al fine di arrecare danni ai sistemi nei quali riescono ad infiltrarsi)
- Diffondere *spam* (*i.e.*, messaggi più o meno diretti che includono link a siti esterni, spesso contenenti malware o pubblicità non desiderata)
- Manipolare votazioni on-line
- Alterare campagne pubblicitarie
- Accedere ad informazioni personali di altri profili
- Danneggiare l'immagine di personaggi o marchi famosi
- . . .

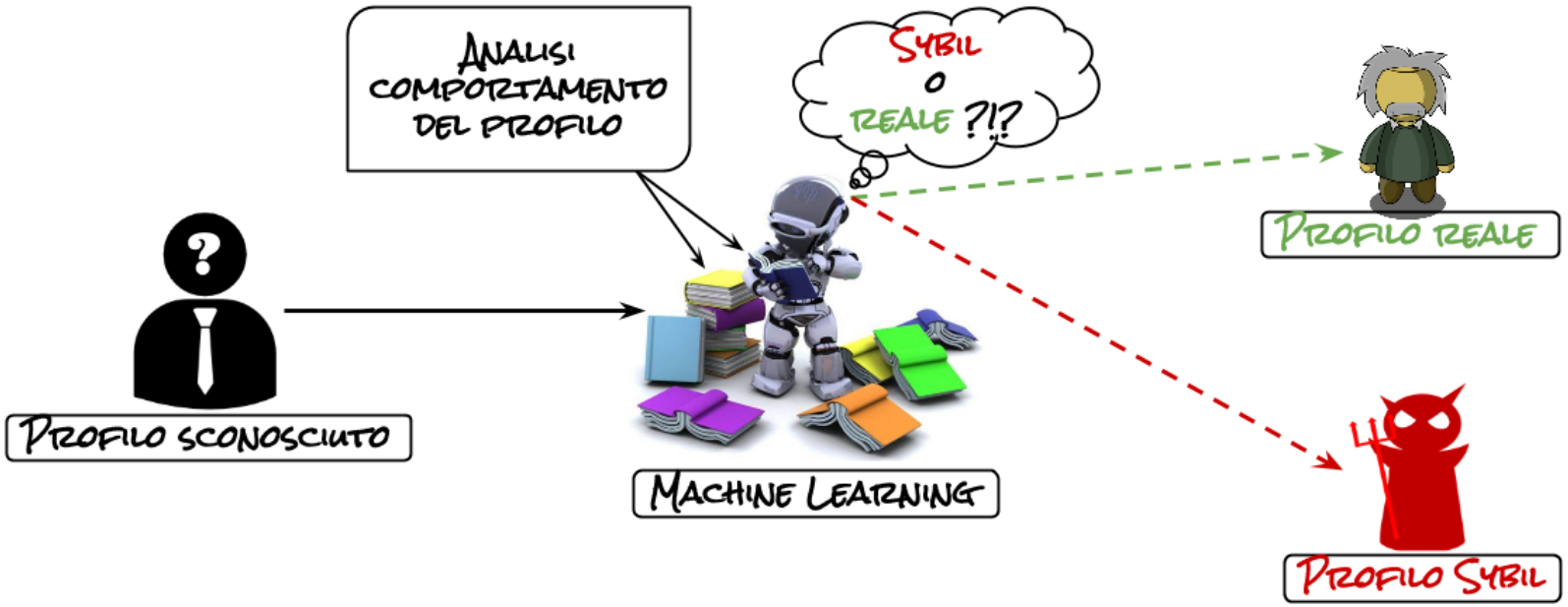
Sybil Detection

Le due principali categorie di schemi utilizzati per contrastare la proliferazione di falsi profili nei Social Network sono:

- Classificatori basati su ***Machine Learning***
- Classificatori basati su ***Grafi***

L'obiettivo comune di entrambi gli approcci è quello di attribuire un punteggio ad ogni profilo che rappresenta la probabilità che essi siano ***onesti*** o ***Sybil***.

Sybil Detection con Machine Learning

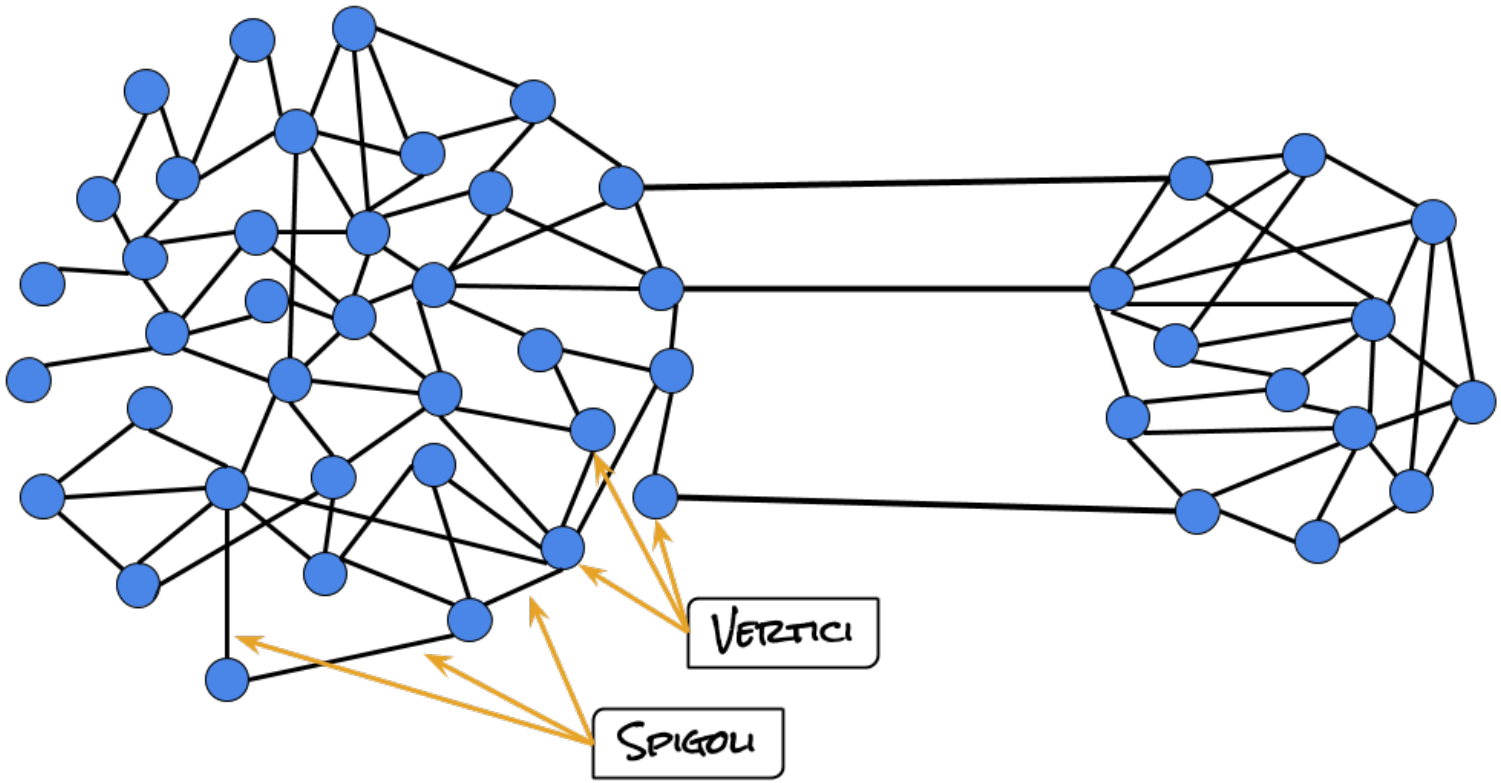


- Numero di *link* per *tweet*
- Numero di caratteri per *tweet*
- Numero di *hashtag* per *tweet*
- Presenza di un volto nella foto del profilo
- Rapporto tra *follower* e *following*
- ...

Graph-Based Sybil Detection

Definizione

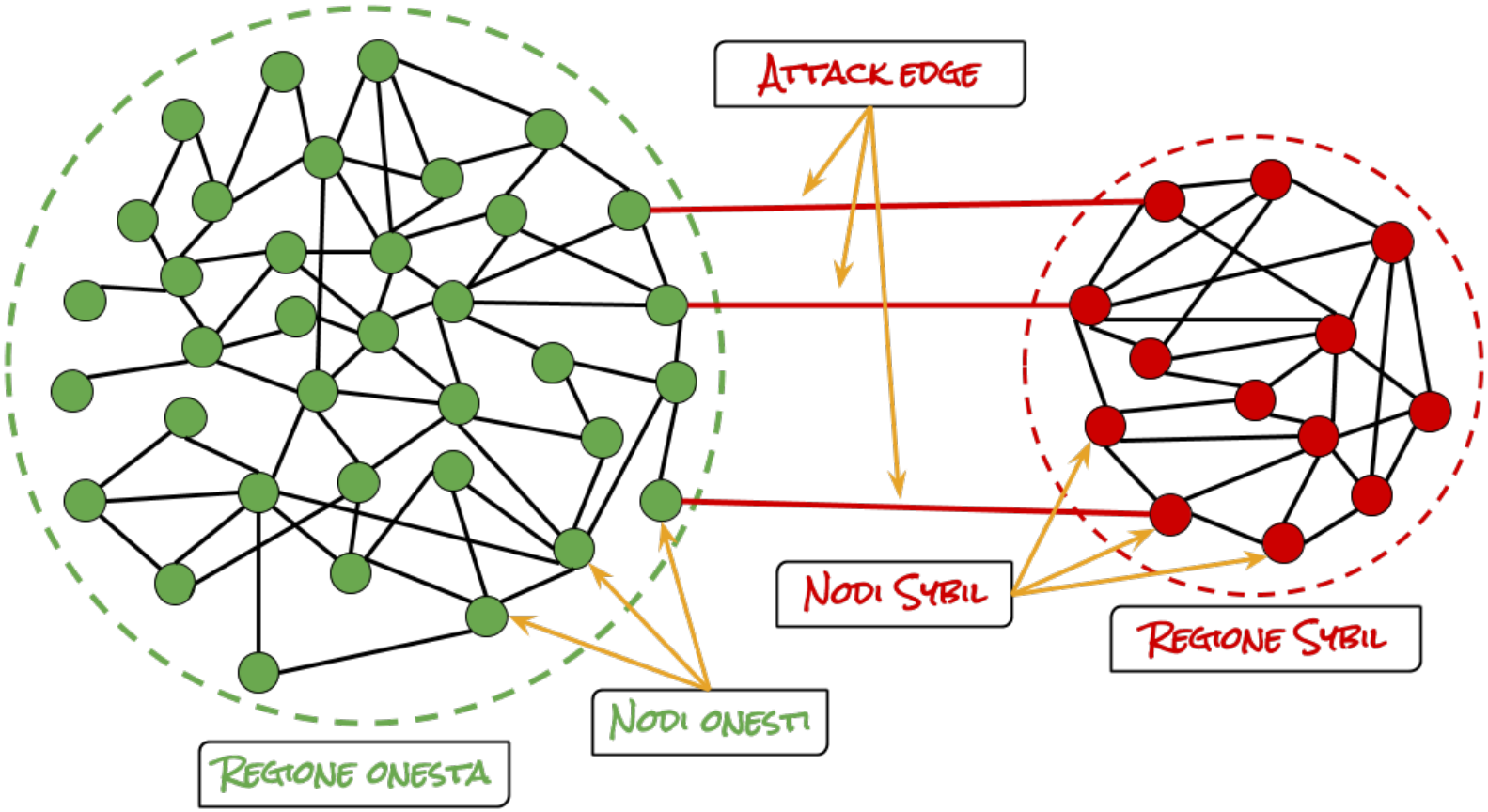
Possiamo definire un Social Network come un ***grafo*** $G = (V, E)$ in cui ogni ***vertice*** o ***nodo*** $v \in V$ rappresenta un'identità "virtuale" e ogni ***spigolo*** $(u, v) \in E$ una ben definita relazione tra le due identità u e v.



Graph-Based Sybil Detection

Definizione

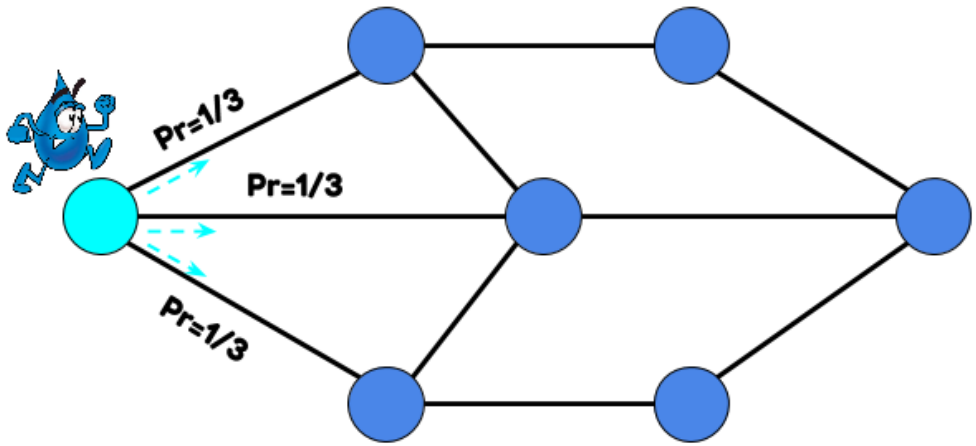
Possiamo definire un Social Network come un ***grafo*** $G = (V, E)$ in cui ogni ***vertice*** o ***nodo*** $v \in V$ rappresenta un'identità "virtuale" e ogni ***spigolo*** $(u, v) \in E$ una ben definita relazione tra le due identità u e v.



Definizione

Una ***random walk*** o ***passeggiata aleatoria*** su un grafo $G = (V, E)$ (costituito da n vertici e m spigoli) è una *catena di Markov* $W = \{w_t\}_{t \geq 0}$ con *spazio degli stati* $V = \{v_1, v_2, \ldots, v_n\}$ e con *matrice di transizione* **P** i cui elementi sono così definiti:

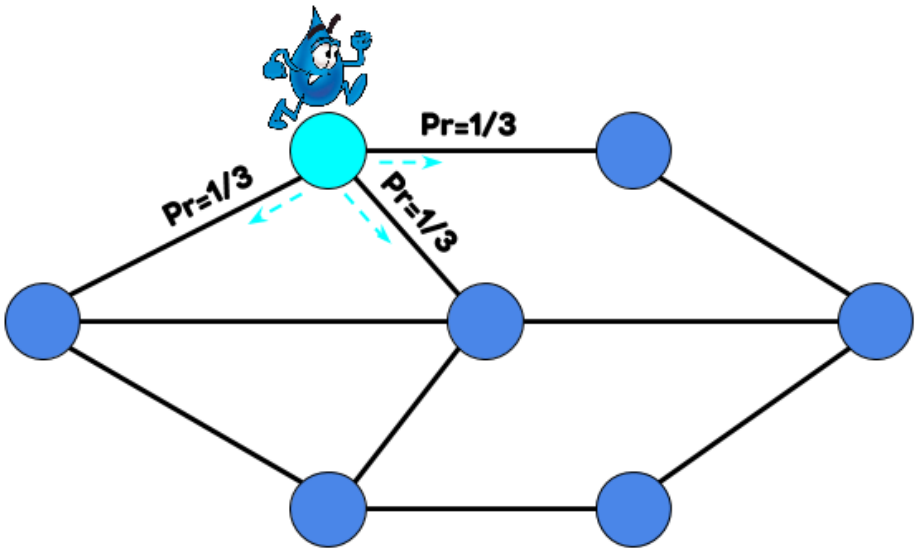
$$P_{i,j} = \begin{cases} \frac{1}{deg(v_i)} & \text{se } (v_i, v_j) \in E \\ 0 & \text{altrimenti} \end{cases}$$



Definizione

Una ***random walk*** o ***passeggiata aleatoria*** su un grafo $G = (V, E)$ (costituito da n vertici e m spigoli) è una *catena di Markov* $W = \{w_t\}_{t \geq 0}$ con *spazio degli stati* $V = \{v_1, v_2, \ldots, v_n\}$ e con *matrice di transizione* **P** i cui elementi sono così definiti:

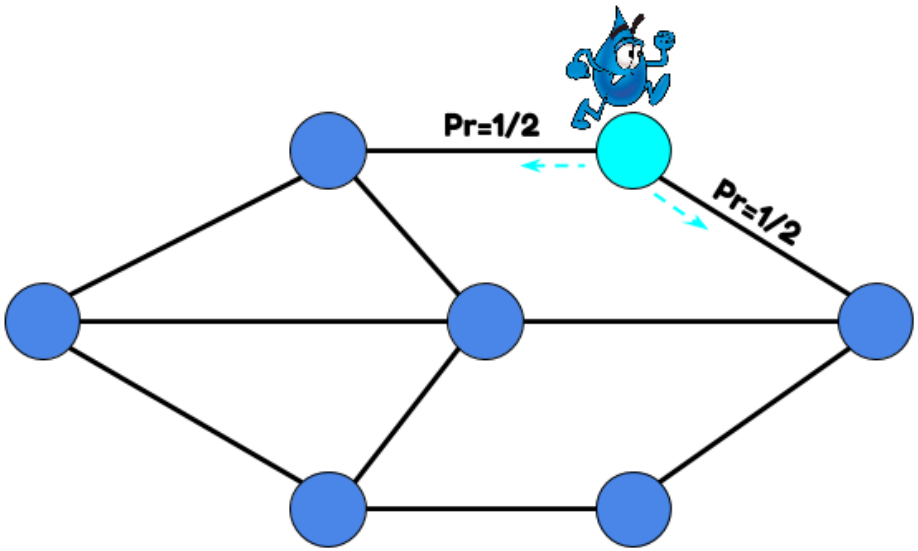
$$P_{i,j} = \begin{cases} \frac{1}{deg(v_i)} & \text{se } (v_i, v_j) \in E \\ 0 & \text{altrimenti} \end{cases}$$



Definizione

Una ***random walk*** o ***passeggiata aleatoria*** su un grafo $G = (V, E)$ (costituito da n vertici e m spigoli) è una *catena di Markov* $W = \{w_t\}_{t \geq 0}$ con *spazio degli stati* $V = \{v_1, v_2, \ldots, v_n\}$ e con *matrice di transizione* **P** i cui elementi sono così definiti:

$$P_{i,j} = \begin{cases} \frac{1}{deg(v_i)} & \text{se } (v_i, v_j) \in E \\ 0 & \text{altrimenti} \end{cases}$$



Definizione

Definiamo la ***distribuzione di probabilità*** della passeggiata aleatoria al tempo t come il vettore $\lambda^{(t)} = (\lambda_1^{(t)}, \ldots, \lambda_n^{(t)})$ in cui l'i-esimo elemento $\left(\lambda_i^{(t)}\right)$ descrive la probabilità che la passeggiata si trovi nel vertice v_i al tempo t.

La ***distribuzione stazionaria*** di una tale passeggiata è definita nel seguente modo:

$$\pi = \left(\frac{deg(v_1)}{2m}, \ldots, \frac{deg(v_n)}{2m} \right)$$

Definizione

Definiamo il ***tempo di mixing*** come il tempo necessario affinché la passeggiata aleatoria raggiunga la distribuzione stazionaria. Formalmente

$$t_{mix} = \min \left\{ t > 0 : d\left(\lambda^{(t)}, \pi\right)_{TV} \leq \frac{c}{n} \right\}$$

Diremo inoltre che la camminata è ***fast-mixing*** se $t_{mix} \in O(\log n)$

La ***conduttanza*** di un grafo descrive la "compattezza" del grafo, ovvero la probabilità che una passeggiata aleatoria su esso raggiunga le parti più isolate. Formalmente, dato un grafo $G = (V, E)$ e $S \subseteq V$ definiamo il *volume* di S come

$$vol(S) = \sum_{v \in S} deg(v)$$

mentre il *taglio* indotto da S come

$$cut(S) = \{ (u, v) \in E : u \in S \text{ e } v \in (V \setminus S) \}$$

Allora la conduttanza indotta dal taglio S è definita come

$$\varphi(S) = \frac{|cut(S)|}{vol(S)}$$

e descrive la "facilità" con cui una passeggiata aleatoria iniziata in S riesca ad uscire da S.

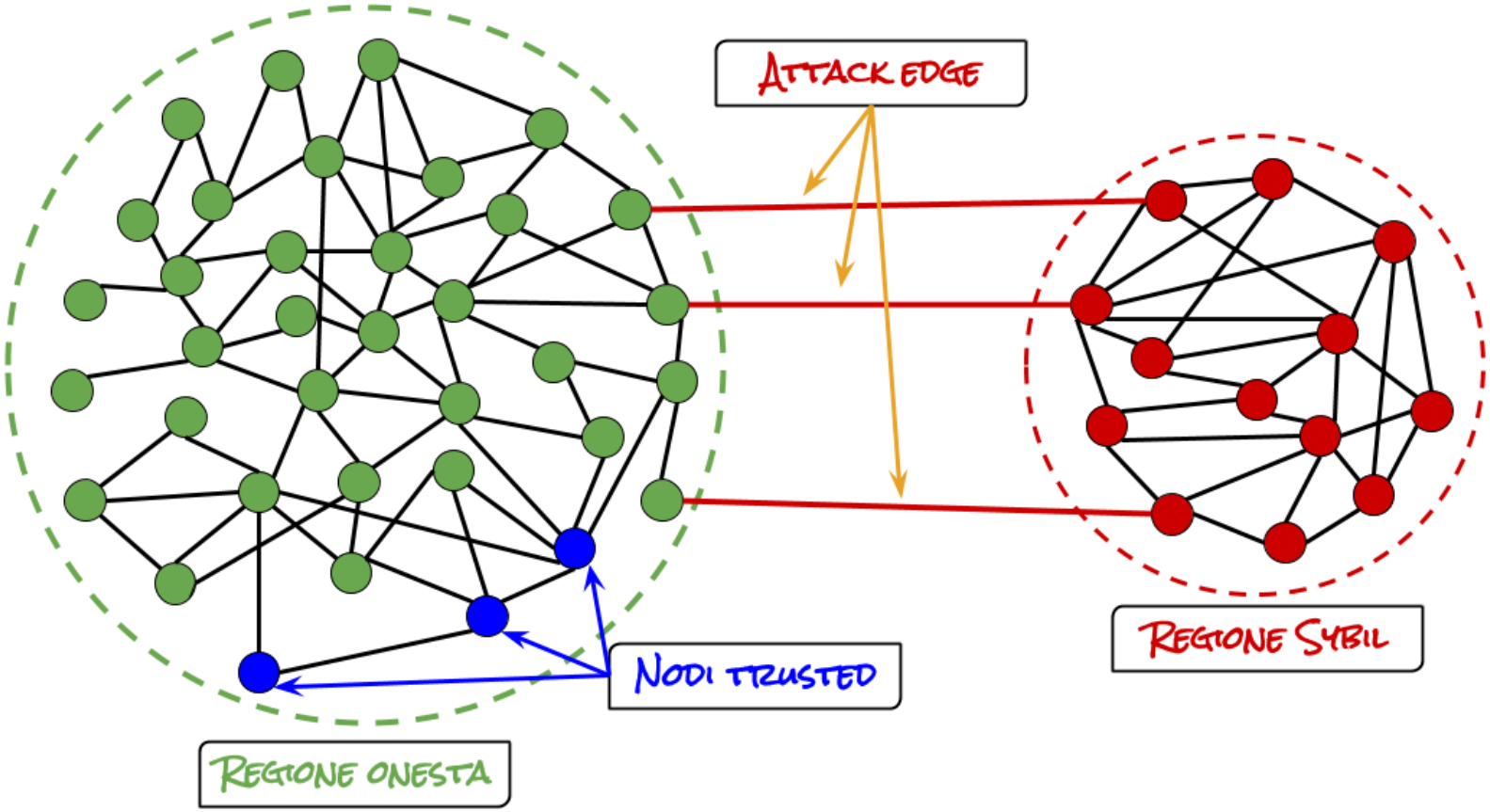
Definizione

La ***conduttanza*** del grafo G è definita come la minima conduttanza su tutti i possibili tagli:

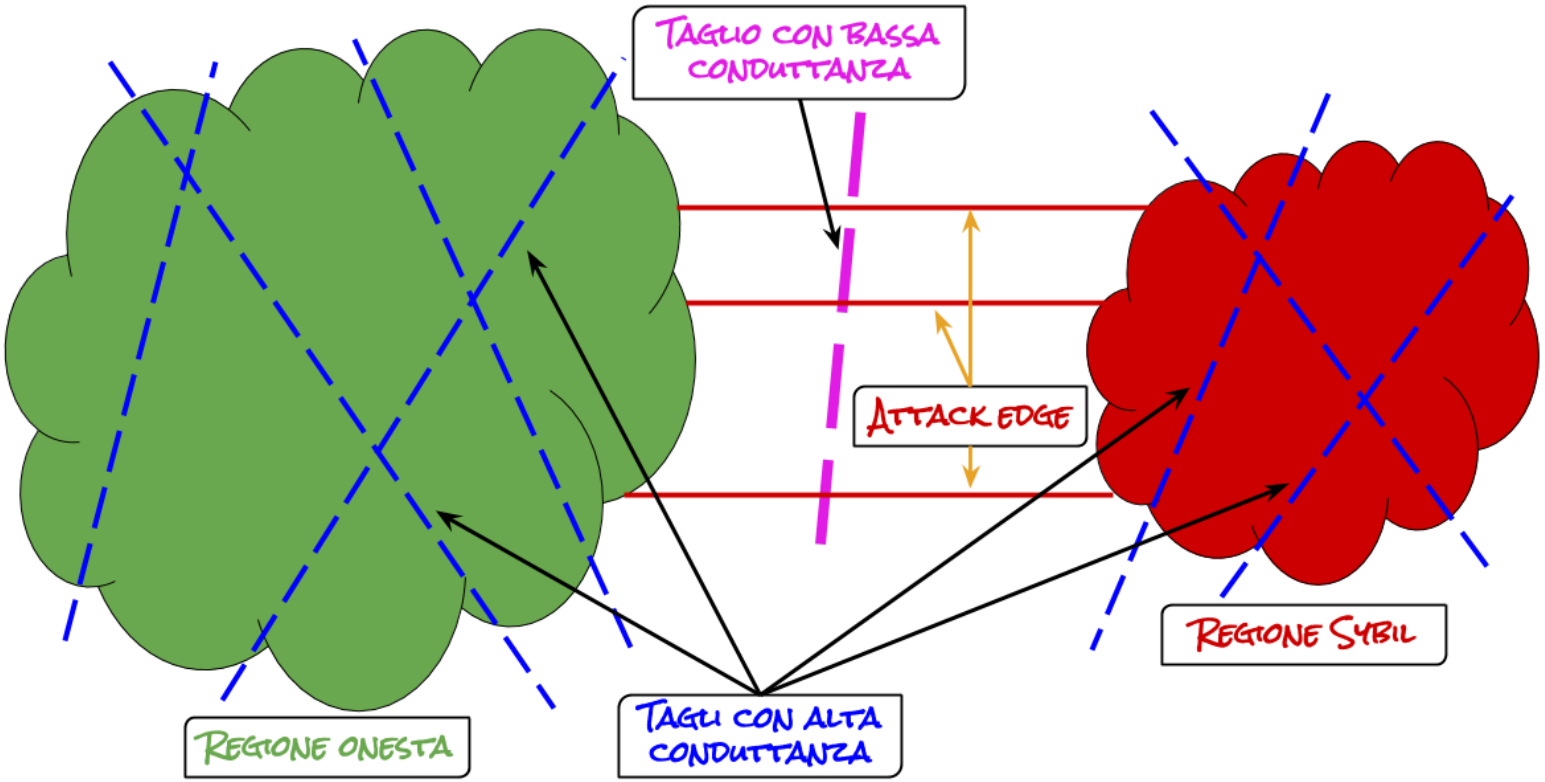
$$\varphi(G) = \min_{S \subseteq V} \varphi(S)$$

Proprietà topologiche

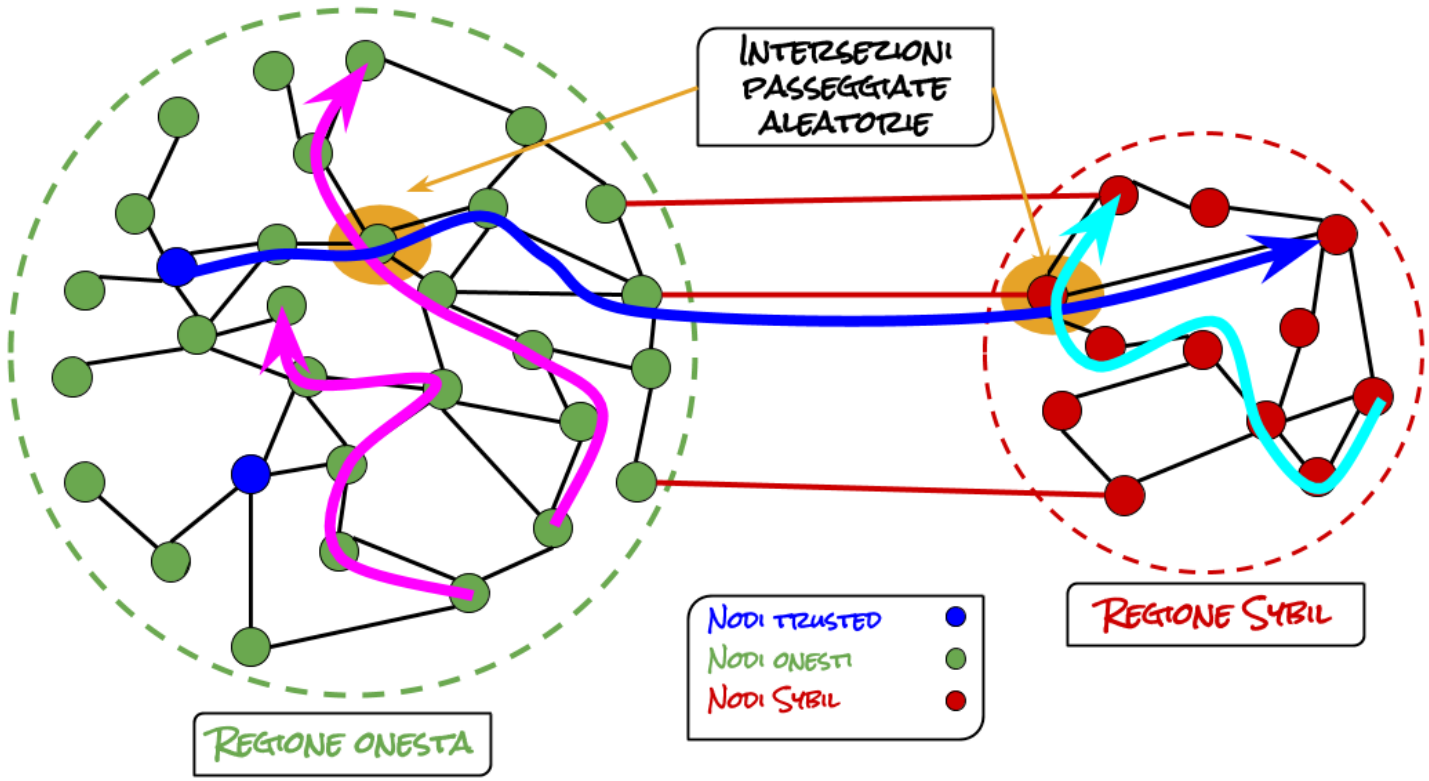
- La regione onesta è ***ben connessa*** e ***fast-mixing***
- Il numero di attack edge è ***basso***
- È sempre possibile identificare uno o più nodi di "fiducia", chiamati ***nodi trusted***, che rompono la simmetria del grafo



L'idea alla base di questi schemi è quella di attribuire un ***valore di ranking*** ad ogni nodo attraverso le ***passeggiate aleatorie***. L'identità di un nodo dipende dal punteggio ottenuto e viene stabilità in base al ***superamento*** di una certa ***soglia***, scelta in maniera tale da minimizzare la conduttanza del taglio indotto dal partizionamento in regione onesta e Sybil.



A causa delle ***smisurate dimensioni*** del grafo che rappresenta un ***Social Network***, non è possibile avere una visione d'insieme di esso e quindi è necessario utilizzare le ***passeggiate aleatorie*** per esplorarlo. Tipicamente vengono realizzate un certo numero di passeggiate di lunghezza $l \in O(\log n)$ e ne vengono considerate le loro intersezioni. Viste le ipotesi sulla struttura del grafo, c'è un alta probabilità che i nodi ***onesti*** ottengano un ***alto punteggio*** e quelli ***Sybil*** un ***basso punteggio***.




Matteo D'Angelo è alla grande.
1 h · Roma ·
GRAZIE PER L'ATTENZIONE!
Mi piace
Commenta
Ti piace.
Scrivi un commento...