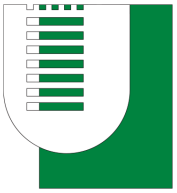

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA

UNIVERSITÀ DEGLI STUDI DI ROMA TOR VERGATA

Corso di Laurea Magistrale in Informatica

A.A. 2022/2023

Tesina: Sicurezza dei Sistemi Informativi

"Social Network Analysis: analisi della rete dei dirottatori responsabili dell'11 Settembre 2001"

Professore

Prof. Maurizio Talamo
Prof. Andrea Dimitri

Studente

Giulia Pascale

"Legami profondi e fidati, non facilmente visibili agli estranei, intrecciavano insieme questa rete terroristica."

Sommario

Lo scopo di questo lavoro sarà quello di fare un approfondimento sull'Analisi delle Social Network e dei suoi concetti. Per farlo si prenderà il lavoro Valdis Krebs nel paper intitolato "Uncloaking Terrorist Networks", in cui si è ricreata la rete sociale che circonda gli eventi tragici dell'11 Settembre 2001, concentrandosi sulla sotto-rete dei 19 dirottatori morti responsabili dell'attentato. Lo scopo di questi studi è quello di tracciare le relazioni tra i dirottatori e ottenere una migliore comprensione dell'organizzazione dietro gli attacchi.

Indice

1 Introduzione alla Social Network Analysis

La Social Network Analysis (SNA) è una metodologia che si occupa di studiare le relazioni sociali tra gli individui o gli enti attraverso l'analisi dei dati di rete.
Questo approccio si basa sulla teoria dei grafi e utilizza concetti e metriche per esplorare la struttura sociale di una rete, come la centralità, la densità, i cluster e le comunità. La teoria dei grafi viene sfruttata per strutturare la Social Network con un grafo in cui i nodi sono individui o organizzazioni e gli archi rappresentano le relazioni sociali fra gli individui.
Inoltre vengono utilizzati tutti gli strumenti della teoria dei grafi, come grado dei nodi, diametro e simili, per studiarne la struttura.
Quindi l'analisi di una social Network permette di evidenziare la struttura gerarchica della rete e altre caratteristiche approfondite in seguito.

Questa metodologia trova spazio anche nelle scienze sociali per via dell'alta componente sociale.

1.1 Applicazioni della SNA

- ***Costruzione di un firewall applicativo***:

  Si hanno due approcci alla sicurezza:

  1. Definizione a priori di regole
  2. Definizione di una condizione di "normalità" e la conseguente definizione di "anomalia"

  Trust

  Dato un grafo diretto aciclico (DAG) $G(V, E)$ che modella una Social Network. Su G è definita una funzione di *Trust Ranking* $r : E \to \{0, 1, ..., 10\}$ dove

$r(u,v), \forall (u,v) \in E$ è un valore di *trust* ad ogni arco diretto.

L'obiettivo è definire una funzione

$$T : V \times V \to \{0, 1, ..., 10\}.$$

Questa funzione rappresenta la *Trust* di un nodo nei confronti di un altro. Si hanno le seguenti caratteristiche:

- $T(u_1, v) \neq T(u_2, v)$, quindi il concetto di *Trust* è **locale** e dipende dai singoli nodi.
- T è definita $\forall u, v \in V$ dove esiste un cammino $path : u \rightsquigarrow \cdots \rightsquigarrow v$. Cioè la *Trust* è un valore definito per tutte le coppie di nodi per cui esiste un cammino che li colleghi e quindi **deriva dai nodi intermedi tra essi**.

Una volta definita la funzione di *Trust* T, vediamo i tre possibili casi:

- $(u, v) \in E$ allora $T(u, v) = r(u, v)$.
- Esiste un unico cammino che unisce $u, v \in V$. Allora

$$T(u, v) = \min\{\text{insieme dei rank associati al path}\}$$

- Esistono più cammini che uniscono $u, v \in V$. Allora $T(u, v)$ è la media pesata con $\left(\frac{1}{n}\right)^{\beta}$ dei T calcolati per ogni path. $\beta \in [0, \infty]$, a seconda del suo valore si può descrivere i valori come pesi tutti uguali ($\beta = 0$) o peso fortemente decrescente al crescere del numero di archi del cammino (con $\beta = \infty$).

Note: la misura non è influenzata dall'ordine dei rank, importa solo qual è il valore del rank minore.

Il concetto di trust può essere applicato nelle social Network nell'ambito della sicurezza informatica e utilizzarlo come base per l'implementazione di un concetto o meccanismo di Authentication.

Ad esempio, possiamo pensare ad una Social Network che modella lo scambio di *e-mail* tra gli utenti. Se una *e-mail* può essere accettata o rigettata, un utente è trust (ci si può fidare) se tutti accettano le sue *e-mail*. L'analisi delle Social Network permette un approccio alla sicurezza bottom up.

- ***Analisi della struttura di una Virtual Organization***:

  Si tratta di rappresentare un'azienda o organizzazione con gli strumenti della teoria dei grafi per poi verificarne i processi e l'adeguatezza. Così facendo è possibile identificare ruoli e dipendenti con relazioni particolari, l'allocazione delle risorse rispetto ad un Task o altro.

- ***Facebook***: è forse la più famosa Social Network della storia che ha il merito di aver portati chiunque sul Web. Su Facebook possono essere fatte analisi globali, riguardanti reti e sottoreti. Ma un altro aspetto interessante è Facebook Ads, uno strumento a disposizione di tutti che permette di usare il Social Network per fare *pubblicità mirata, scalabile nei costi* e di cui si può smettere di usufruire in qualsiasi momento.

- ***SNA come forma di cluster analysis e come strumento esplorativo: il terrorismo***: esiste una parte della letteratura scientifica che si concentra sull'uso della SNA per capire il terrorismo islamico. L'idea è quella di studiare le reti criminali e capire come funzionano e le loro caratteristiche al fine di scovarle prima che commettano crimini. Vedremo in questa tesina di studiare un caso particolare: quello dell'attacco terroristico dell'11 Settembre 2001.

1.2 Node level statistical measures

Le Node level statistical measures (o misure statistiche a livello di nodo) sono misure utilizzate per analizzare e valutare i nodi individuali all'interno di un grafo e quindi di una Social Network. Queste misure forniscono informazioni specifiche sulle caratteristiche o l'importanza di ciascun nodo nel contesto del grafo nel suo insieme. Usate, tra le tante, per scoprire se vi sono nodi con un alto grado di centralità nella rete e se ci sono nodi isolati.

1.2.1 Definizioni preliminari

Definizioni preliminari:

- **Diametro:** massima distanza esistente tra tutti i nodi della rete.
- **Eccentricità:** lunghezza del cammino minimo più lungo. $eccentricità = \max\{d(s, v) : v \in V - s\}$
- **Densità:** rapporto tra il numero di archi presenti nel grafo e il numero di tutti i possibili archi del grafo.
- **Bridge:** arco la cui rimozione disconnette la rete. Sono archi cruciali per l'accesso alle informazioni, in quanto senza di essi una informazione non potrebbe uscire dalla sua componente. In una rete sociale reale è poco probabile che esistano bridge.

1.2.2 Grado (Degree)

Il grado di un nodo $d(u)$ rappresenta il numero di archi che lo collegano ad altri nodi nel grafo. Un nodo con un alto grado ha molte connessioni e possiamo dire genericamente che è importante nel grafo.

1.2.3 Coefficiente di clustering locale

Il coefficiente di clustering locale è una misura della coesione del nodo u all'interno del suo vicinato $N(u)$. Per dirlo in altri termini, è grado di connessione intorno ad un nodo u.

$$c(u) = \frac{|\{(x,y) \in E : x \in N(u) \wedge y \in N(u)\}|}{\binom{N(u)}{2}}$$

Al numeratore abbiamo il numero di coppie di vicini di u che hanno tra di loro un arco. In poche parole si contano il numero di triangoli che incidono su u. Al denominatore abbiamo tutti i possibili triangoli che potrebbero incidere su u.
Possiamo vedere e riferirci al coefficiente di clustering come l'indice di centralità di un nodo.

Analogamente possiamo definire un coefficiente di clustering relativo a un sottoinsieme C di nodi. Ovvero, dato un sottoinsieme $C \subseteq V$ definiamo il coefficiente di clustering di u relativo a C come la quantità:

$$c_C(u) = \frac{|\{(x,y) \in E : x \in N(u) \cap C \wedge y \in N(u) \cap C\}|}{\binom{N(u) \cap C}{2}}$$

Questo valore è: $0 \leq c_C(u) \leq 1$. Più si avvicina a 0 e meno è coeso rispetto a C, più è vicino ad 1 e più è coese in C.

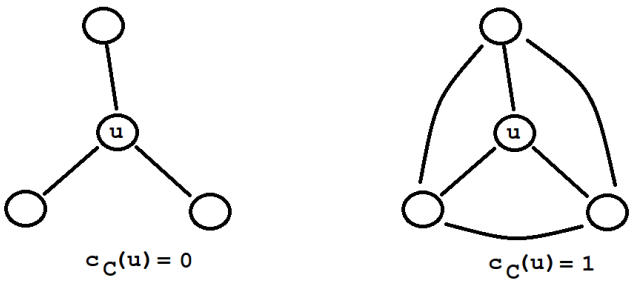

Figura 1: Se $c_C(u) = 0$ la struttura è una stella, se $c_C(u) = 1$ in u incidono tutti i possibili triangoli.

1.2.4 Orizzonte di osservabilità

Questo concetto è stato introdotto da Friendkin nell'ambito delle reti sociali per studiare la diffusione delle opinioni e delle informazioni all'interno di una rete. ([6])
L'idea alla base di questo concetto è che ogni individuo in una rete sociale possiede un certo livello di **influenza** sugli altri individui con cui è collegato. L'orizzonte di osservabilità si riferisce al limite massimo di influenza che un individuo più avere all'interno di una rete. L'orizzonte di osservabilità di un individuo **dipende quindi dalla struttura della rete sociale e dalla posizione di quell'individuo** all'interno della rete. È determinato dalla distanza tra il nodo specifico e gli altri nodi nella rete. La si può anche vedere come la misura della differenza di opinioni tra un nodo e l'altro. Se l'orizzonte di osservabilità di un nodo è ampio, significa che il nodo può influenzare un gran numero di nodi all'interno della rete. Se l'orizzonte di osservabilità è limitato, il nodo ha meno capacità di influenzare gli altri.

1.3 Misure di centralità

In teoria dei grafi e nella Network Analysis, gli indicatori di centralità assegnano numeri o classifiche ai nodi di un grafo in base alla loro posizione nella rete. Ci sono quattro misure di centralità ben note: grado (degree), Betwenness, Closeness e Eigenvector (autovettore), ciascuna con i propri punti di forza e di debolezza.

1.3.1 Degree centrality

La degree centrality è una misura di centralità di un nodo in un grafo, che indica il numero di archi incidenti su quel nodo. In altre parole, la degree centrality di un nodo corrisponde al numero di connessioni che il nodo ha con gli altri nodi nel grafo.

La degree centrality si calcola dividendo il grado del nodo (ovvero il numero di archi incidenti su quel nodo) per il numero massimo di archi possibili tra i nodi del grafo. Il risultato è un valore compreso tra 0 e 1, dove 0 indica un nodo isolato senza connessioni e 1 indica un nodo completamente connesso a tutti gli altri nodi nel grafo.

$$D(v) = \frac{d(v)}{n-1}$$

$\forall v \in V$

1.3.2 Betweenness Centrality

La Betweenness centrality (o centralità di intermediazione) di un nodo misura il numero di volte in cui il nodo si trova lungo il percorso più breve tra due altri nodi nel grafo. Questa misura è utile per identificare i nodi che fungono da ponti o collegamenti critici tra altre parti del grafo. Possiamo vederla come l'*intensità* con la quale un nodo è posto nella rete, il suo grado di intermediazione

$$BW(u) = \sum_{u \neq s \neq t} \frac{\sigma_{(s,t)}(u)}{\sigma_{(s,t)}}$$

dove $\sigma_{(s,t)}$ è il numero di cammini minimi tra i nodi (s,t) e $\sigma_{(s,t)}(u)$ è il numero di cammini minimi tra i nodi (s,t) passanti per il nodo u.

1.3.3 Closeness centrality

La Closeness è la misura della centralità utilizzata per valutare quanto un nodo in un grafo sia vicino agli altri nodi, quanto "veloce" può raggiungere gli altri nodi del grafo.

$$D_c(u) = \frac{1}{\sum_{t \in V} d(u,t)} \forall\, t \in V - u$$

La closeness centrality di un nodo si basa sulla lunghezza media dei cammini più brevi da quel nodo a tutti gli altri nodi del grafo. Un nodo con una closeness centrality più elevata è considerato più centrale, poiché può raggiungere rapidamente un gran numero di altri nodi. Una closeness centrality di 1 indica che il nodo è in grado di raggiungere tutti gli altri nodi in modo immediato, mentre un valore più basso indica che il nodo è più lontano dagli altri nodi.

Ad esempio, in un contesto di una connessione LAN, un valore alto potrebbe averlo l'Amministratore della rete.

1.3.4 Eigenvector Centrality

L'Eigenvector Centrality è una misura di centralità utilizzata per valutare l'importanza o l'influenza di un nodo all'interno di un grafo. Questa misura tiene conto sia del numero di connessioni di un nodo che dell'importanza dei nodi con cui è collegato.

Un nodo è considerato centrale se è collegato ad altri nodi che sono anch'essi considerati centrali, quindi la centralità di un nodo dipende dalla centralità dei suoi vicini. Come suggerisce il nome, per calcolare questa misura occorre fari riferimento agli autovettori e autovalori della matrice di adiacenza del grafo.

2 Articolo Uncloaking Terrorist Networks

Chi ha vissuto l'11 Settembre 2001 è rimasto scioccato e non può non ricordarsene. Nei primi momenti successivi all'attentato, nel continuo flusso di notizie e analisi, spesso veniva ripetuto il concetto di "terrorist network" (rete terroristica), senza però capirne il significato. Inoltre, nessuno riusciva a produrne una rappresentazione visiva.

Il paper intitolato "Uncloaking Terrorist Networks" di Valdis Krebs [[1], [2]], pubblicato su First Monday nel 2002, si concentra sull'analisi delle reti nascoste utilizzando i dati disponibili dalle fonti di notizie sul Web, in particolare giornali come il New York Times, il Wall Street Journal, il Washington Post e il Los Angeles Times. L'autore ha esaminato la rete che circonda gli eventi tragici dell'11 settembre 2001 e, attraverso **dati pubblici**, è stato in grado di mappare una parte della rete centrata sui 19 dirottatori morti. Questa rete (o "la mappatura di questa rete") fornisce alcune informazioni sull'organizzazione terroristica, anche se è incompleta. In sostanza, il paper *si propone di utilizzare le fonti di notizie disponibili al pubblico per mappare le connessioni tra i membri di una rete terroristica.*

L'idea è stata quella di tracciare le relazioni tra i dirottatori responsabili degli attacchi e ottenere una migliore comprensione dell'organizzazione dietro gli attacchi stessi.

2.1 Background dello studio

Prima di entrare nel vivo dello studio, occorre fermarsi a chiarire quali sono state le fonti delle informazioni e qual è stato il background teorico che è stato utilizzato come base per fare successivamente anche le eventuali riflessioni. Le fonti di dati dell'autore sono le informazioni pubblicate su importanti giornali come il New York Times, il Wall Street Journal, il Washington Post e il Los Angeles Times. L'autore ha monitorato l'indagine passo passo ma, com'è facile intuire, in un momento così delicato delle

indagini, gli investigatori non hanno reso note tutte le informazioni pertinenti sulla rete/relazioni e potrebbero addirittura aver diffuso informazioni errate per confondere il nemico. Era chiaro che si sarebbe lavorato con dati incompleti e poco accurati.

Per orientarsi, si è rivolto a lavori precedenti di teorici delle reti sociali che avevano studiato reti segrete, illegali o criminali. La base teorica di questo lavoro si basa su tre articoli fondamentali nell'ambito dello studio delle Social Network di società criminali. Elencati per nome dell'autore o degli autori:

1. ***Malcolm Sparrow*** ([3]) esamina l'applicazione dell'analisi delle reti sociali all'attività criminale. Sparrow descrive tre problemi dell'analisi delle reti criminali che ho presto affrontato.

   - **Incompletezza:** inevitabilmente ci saranno nodi e collegamenti mancanti che gli investigatori non scopriranno.
   - **Confini sfumati:** la difficoltà nel decidere chi includere e chi escludere.
   - **Dinamicità:** queste reti non sono statiche, ma cambiano sempre.

   Invece di considerare la presenza o l'assenza di un legame tra due individui, Sparrow suggerisce di analizzare l'evoluzione della forza di un legame in base al tempo e al compito da svolgere.

2. ***Wayne Baker e Robert Faulkner*** ([4]) hanno suggerito l'utilizzo di dati archivistici per ottenere informazioni sulle relazioni all'interno delle reti illegali.

   Nello specifico, i ricercatori hanno utilizzato principalmente documenti giudiziari e testimonianze giurate come fonti di dati per la loro analisi. Questi documenti comprendevano prove documentali presentate nei procedimenti giudiziari e te-

stimonianze fornite da individui che avevano una conoscenza diretta o erano stati testimoni delle relazioni coinvolte in tali reti illegali.

3. ***Bonnie Erickson*** ([5]) mette in luce l'importanza dei contatti fidati *preesistenti* per il funzionamento efficace di una società segreta. Non a caso, i 19 dirottatori materialmente coinvolti nell'attentato dell'11 Settembre, sembravano far parte di una rete formata mentre completavano l'addestramento terroristico in Afghanistan. Molti di loro erano compagni di scuola di molti anni fa, alcuni avevano vissuto insieme per anni e altri erano legati da vincoli di parentela. ***Legami profondi e fidati, non facilmente visibili agli estranei, intrecciavano insieme questa rete terroristica.***

2.2 Creazione del grafo

Entro una settimana dall'attacco, le informazioni provenienti dall'indagine cominciarono a diventare pubbliche. Il **grafo** è stato costruito ***in modo iterativo***: i vari nodi e legami sono stati aggiunti con cautela a causa del continuo aggiornamento delle informazioni sulle principali fonti di notizie accreditate. Chi ha creato il grafo ha anche tenuto traccia delle fonti di informazioni utilizzate per ogni nodo/legame.

In poco tempo si è saputo chi fossero i 19 dirottatori, la loro nazionalità e su quali aerei viaggiassero. Con queste informazioni, e con quelle sul loro passato che a mano a mano venivano rese pubbliche, si è deciso di mappare i loro legami con 3 livelli di forza (*tie strength*).
La forza del legame (*tie strength*) sarebbe stata in gran parte determinata dalla quantità di tempo trascorso insieme da una coppia di terroristi.

- **Legami forti:** coloro che vivevano insieme o frequentavano la stessa scuola o gli stessi corsi/addestramenti avrebbero avuto i legami più forti. (2.1, Erickson)

- **Legami moderati:** coloro che viaggiavano insieme e partecipavano a incontri insieme.
- **Legami deboli:** coloro che erano registrati come avendo una singola transazione insieme o un incontro occasionale e nessun altro legame,

Nella figura (2) **non** è stata evidenziata la forza del legame.

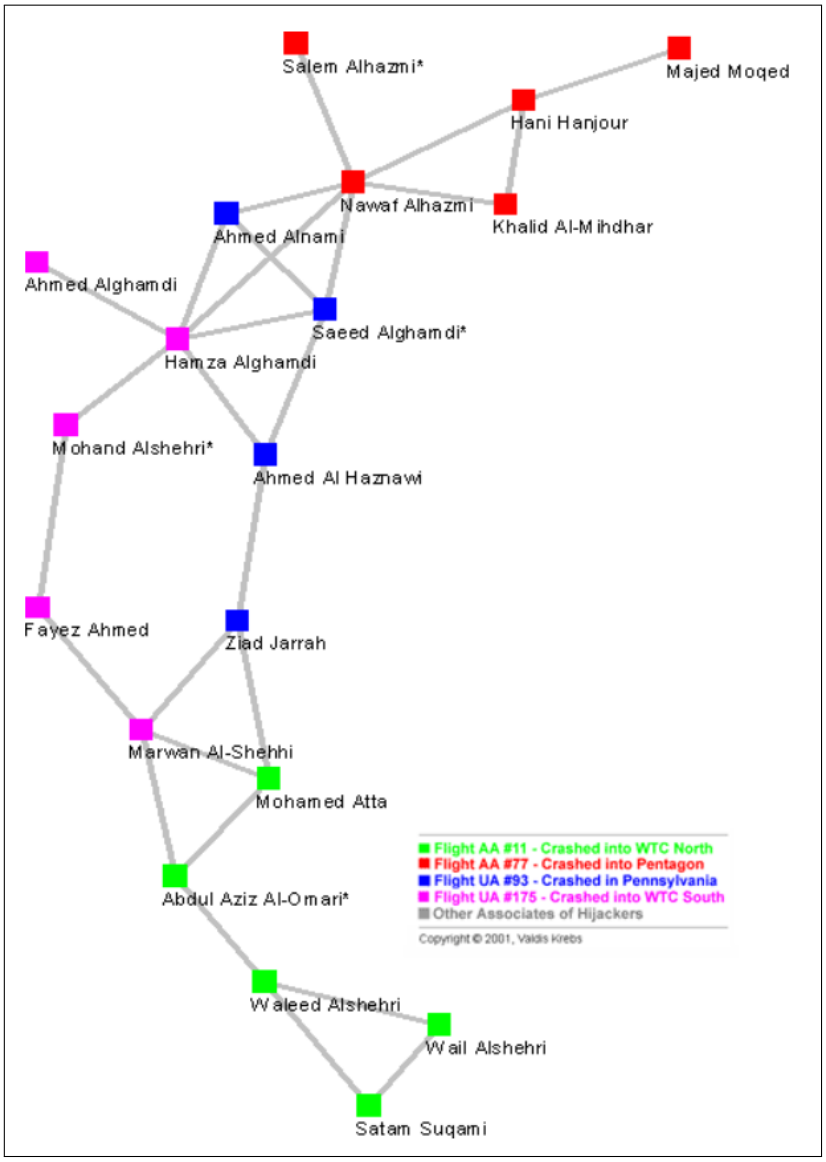

Figura 2: Grafo 19 dirottatori

2.3 Osservazione del grafo

Vediamo ora di fare delle riflessioni e osservazioni sul grafo generato.

2.3.1 Densità e orizzonte di osservabilità

È evidente già ad occhio, che il grafo sia molto sparso e che diversi dirottatori che viaggiavano sullo stesso aereo non hanno legami tra di essi. Molti membri delle squadre sono oltre l'orizzonte di osservabilità (1.2.4) l'uno dall'altro - molti passeggeri sullo stesso volo sono separati da più di due archi.

Osserviamo per esempio nello specifico il sottografo del gruppo di dirottatori che viaggiavano sull'aereo che si è schiantato sul Pentagono.

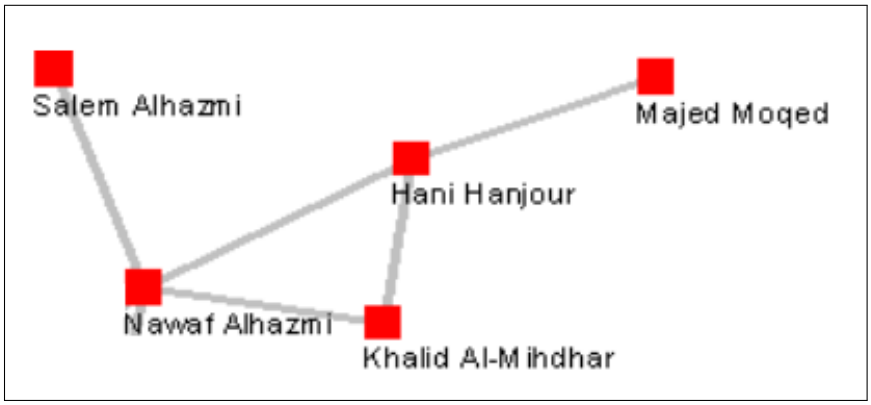

Figura 3: Sotto-rete dei dirottatori responsabili dell'attacco al Pentagono

Due di loro sono separati da più di due passi. Lo stesso discorso lo si può fare su tutti gli altri voli.

Parlando più in generale dell'intera rete dei 19 dirottatori, si può osservare che in questa piccola rete la distanza media tra i nodi è di $4,75$ archi. Alcuni dirottatori sono separati da più di 6 archi.

Strategia

La strategia dietro questa caratteristica della rete dei dirottatori serve per mantenere i membri delle cellule distanti l'uno dall'altro e da altre celle minimizza i danni alla rete nel caso in cui un membro della cellula venga catturato o compromesso in qualche modo.

Osama bin Laden ha descritto questo piano nel suo famigerato video che è stato trovato in Afghanistan. Riguardo la densità dei legami tra i dirottatori dice: *"Coloro che sono stati addestrati a volare non conoscevano gli altri. Un gruppo di persone non conosceva l'altro gruppo."*.

Si può intuire quindi la caratteristica importante delle reti illegali e segrete: ***le reti segrete scambiano l'efficienza per il segreto.***

2.3.2 Come raggiunge i suoi obiettivi una rete segreta? Attuazione dei piani in una rete sparsa e dinamicità

Tuttavia, nonostante la poca densità della rete, i piani devono essere messi in atto. Come raggiunge i suoi obiettivi una rete segreta?

Si è scoperto che venivano organizzati incontri che collegavano parti distanti della rete per coordinare le attività e segnalare i progressi. Dopo il raggiungimento del coordinamento, i collegamenti temporanei diventavano inattivi.
Ad esempio, si ha la conoscenza di un incontro della rete dei dirottatori che ebbe luogo a Las Vegas. Ad onor del vero, l'oggetto di discussione di questo incontro è ancora in dubbio (almeno per il pubblico), come si può leggere in un alcuni articoli recenti ([7]). Questo però non è di fondamentale importanza per questo studio, quello che è interessante è vederne gli effetti sulla rete.

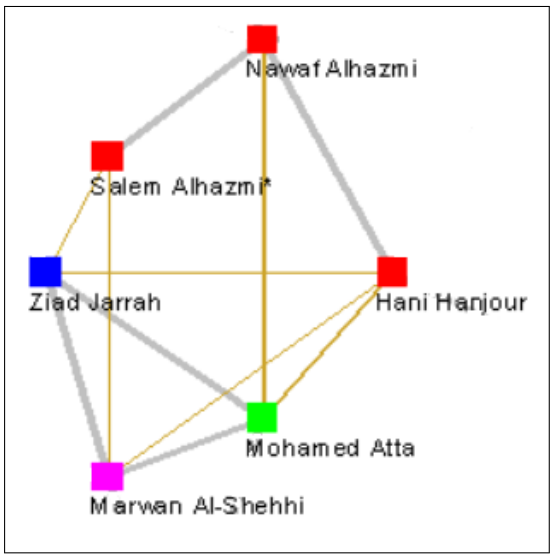

Figura 4: Sotto-rete dell'incontro a Las Vegas prima dell'attentato.

Strategia

Sono state aggiunte temporaneamente 5 shortcuts (scorciatoie) alla rete per facilitare la collaborazione e il coordinamento. Queste scorciatoie hanno ridotto la lunghezza media del percorso nella rete di oltre il 40%, migliorando così il flusso delle informazioni nella rete. Quando la rete viene avvicinata da queste shortcuts, tutti i piloti dell'attentato finiscono in una piccola *clique*, la struttura perfetta per coordinare efficientemente le attività e gli individui coinvolti.

Al fine di facilitare la lettura si riporta la lista dei pilori responsabili:

- Mohamed Atta: pilota (e leader di tutti i dirottatori) che colpì la torre nord del World Trade Center
- Hani Hanjour: pilota che colpì il pentagono
- Ziad Jarrah: pilota dell'aereo che precipitò in Pennsylvania
- Marwan al-Shehhi: pilota che colpì la torre Sud del World Trade Center

Nel dettaglio le metriche prima e dopo l'aggiunta delle shortcuts:

	Clustering Coefficient	Lunghezza media di un cammino
Legami pregressi	0.41	3.51
Legami pregressi + Shortcuts	0.42	2.85

Nota: I dati in questa tabella si riferiscono alla sotto-rete dei 19 dirottatori e non alla rete completa con i 61 associati.

Questo esempio è estremamente interessante perché mette in luce una caratteristica definita da Sparrow (2.1) riguardo le reti illegali e segrete: la ***dinamicità***.

Queste reti non sono statiche, ma possono cambiare sempre.

2.4 Altri associati

Un attentato del genere ha bisogno di molte conoscenze e informazioni, e di un'organizzazione lunga e precisa. I 19 dirottatori non potevano e non hanno agito da soli: avevano altri complici che non sono saliti sugli aerei. Questi complici fungono da canali per il denaro e forniscono anche le competenze e le conoscenze necessarie. Sono stati individuati 61 individui responsabili dell'attentato, tra i 19 dirottatori materiali e altri associati diretti o indiretti.

Di seguito una figura (5) comprendente tutti i 61 individui.

Figura 5: Rete di tutti i responsabili diretti e indiretti dell'11 Settembre.

2.5 Metriche della rete

A posteriori si sa che Mohamed Atta fosse il capo di questa cospirazione, e questa informazione è stata anche confermata dallo stesso Bin Laden in un video.

Questo dato trova riscontro nei valori che si possono trovare riguardo le metriche di centralità della rete. Nel *paper* vengono analizzati tre valori in particolare: *Degrees Centrality, Betweenness e Closeness.* A questi valori ho aggiunto il Degrees e la Eigenvector Centrality per completezza.

Si riporta una visione parziale dei risultati:

Dirottatore	**Degree**	**Degree Centrality**
Mohamed Atta	15	0.25
Marwan Al-Shehhi	12	0.2
Essid Sami Ben Khemail	12	0.2
Nawaf Alhazmi	9	0.15
Ramzi Bin al-Shibh	9	0.15
Djamal Benghal	9	0.15
Ziad Jarrah	8	0.133
Zacarias Moussaoui	8	0.133
Hani Hanjour	7	0.116
Said Bahaji	7	0.116
...	...	...

Betweenness		**Closeness**	
Valore	**Dirottatore**	**Valore**	**Dirottatore**
0.508	Mohamed Atta	0.444	Mohamed Atta
0.256	Essid Sami Ben Khemail	0.379	Marwan Al-Shehhi
0.237	Lofti Raissi	0.375	Ziad Jarrah
0.220	Zacarias Moussaoui	0.375	Lofti Raissi
0.209	Hani Hanjour	0.365	Ramzi Bin al-Shibh
0.141	Nawaf Alhazmi	0.355	Essid Sami Khemail
0.130	Ziad Jarrah	0.352	Zacarias Moussaoui
0.106	Djamal Benghal	0.340	Mustafa al-Hisawi
0.103	Ahmed Al Haznawi	0.338	Imad Eddin Yarkas
0.075	Marwan Al-Shehhi	0.335	Said Bahaji
...	...	...	...

Dirottatore	Eigenvector Centrality
Mohamed Atta	0.438
Marwan Al-Shehhi	0.388
Ramzi Bin al-Shibh	0.342
Ziad Jarrah	0.306
Said Bahaji	0.298
Zakariya Essabar	0.252
Agus Budiman	0.215
Mounir El Motassadeq	0.208
Lofti Raissi	0.171
Mamoun Darkazanli	0.160
...	...

Tutte metriche di rete rivela l'attività di Atta nella rete. La Betweenness misura la sua capacità di accedere agli altri nella rete e monitorare ciò che sta accadendo. La Closeness mostra il suo controllo sul flusso nella rete - svolge il ruolo di intermediario nella rete.

Queste metriche supportano il suo status di leader.

È inoltre interessante notare che il grado medio di questa rete è 4.327. Un valore molto piccolo, rispetto al numero di nodi presenti nella rete. Questo dato rafforza la caratteristica della rete che la vede come poco densa.
Questo e ulteriori valori aggiunti alle metriche del paper sono stati calcolati tramite *Python*, approfonditi nella sezione successiva (3.2).

2.6 Puntualizzazione sulle metriche

Come accennato da Sparrow (in 2.1), una caratteristica importante delle reti criminali è la loro inevitabile **incompletezza**, infatti molto spesso ci saranno nodi e relazioni mancanti che gli investigatori non hanno scoperto. Questa caratteristica molto probabilemente è presente anche in questo studio e nei dati che si hanno a disposizione. Le misure di centralità sono molto sensibili a piccoli cambiamenti nella connettività

della rete. La scoperta di uno o due nuovi cospiratori o la scoperta di nuovi collegamenti tra nodi esistenti possono alterare chi emerge in cima alle misure di centralità. Occorre essere cauti riguardo ai dati incompleti.

3 Applicazioni: Dataset 9/11 HIJACKERS

Online è presente un Dataset contenente la lista di dirottatori che si è reso responsabile in modo diretto o indiretto all'attacco terroristiche dell'11 Settembre. Di seguito le specifiche del Dataset e ulteriori analisi che sono state effettuate nel grafo risultante.

3.1 Specifiche Dataset 9/11 HIJACKERS

[9_11_HIJACKERS_ATTR.csv] .

Nel seguente formato: "", Network Strength, Ties, Las Vegas Meeting

- Network Strength: 1 = Trusted Prior Contacts, 2 = Other Associates
- Ties: 1 = AA #11 WTC North, 2 = AA #77 Pentagon, 3 = UA #93 Pennsylvania, 4 = UA #175 WTC South, 5 = Other Associates
- Las Vegas Meeting: 1 = Attended, 0 = Did Not Attend

Gli archi sono binari e non orientati. Il campo Network Strength associa il valore 1 se si parla di contatti fidati (addestrati insieme, vissuti insieme, transazioni finanziarie, a scuola con, sullo stesso volo), 0 se si parla di altri associati generici. In molti casi ci si riferisce con *Prior Contacts* quando si parla di contatti fidati.

	Network Strength	Ties	Las Vegas Meeting
Dirottatore1			
...			
Dirottatore61			

[9_11_HIJACKERS_PRIORCONTACTS.csv] .

Questo *file CSV* contiene una matrice 19x19 in cui le righe e le colonne corrispondono alle stesse persone. I valori all'interno della matrice sono 0 e 1, che rappresentano l'assenza o la presenza di un arco tra di loro.

Nel seguente formato: "", Dirottatore1, Dirottatore2, ... , Dirottatore19.

	Dirottatore1	Dirottatore2	...	Dirottotare19
Dirottatore1	0	1		1
Dirottatore2	1	0		0
...				
Dirottatore19	0	1		0

- 1 = legame tra dirottatori presente
- 0 = legame tra dirottatori **non** presente

[9_11_HIJACKERS_ASSOCIATES.csv] .

Questo *file CSV* è un'estensione del precedente, infatti contiene una matrice 61x61 in cui le righe e le colonne corrispondono a tutte le persone che hanno contribuito all'attentato dell'11 Settembre, anche quelle che non hanno preso fisicamente parte all'attacco stesso.

I valori all'interno della matrice sono 0 e 1, che rappresentano l'assenza o la presenza di un arco tra di loro.

Nel seguente formato: "", Dirottatore1, Dirottatore2, ... , Dirottatore61.

	Dirottatore1	Dirottatore2	...	Dirottotare61
Dirottatore1	0	1		1
Dirottatore2	1	0		0
...				
Dirottatore61	0	1		0

- 1 = legame tra dirottatori presente
- 0 = legame tra dirottatori **non** presente

3.2 Applicazioni

Di seguito ulteriori metriche calcolate sul grafo.

3.2.1 Strumenti utilizzati

L'implementazione del codice è avvenuta in *Python* mediante l'utilizzo delle seguenti librerie:

- *Pandas*: per analizzare i file *csv* del dataset.
- *Networkx*: per manipolare e analizzare la rete dei terroristi.
- *MatPlotLib*: per disegnare eventualmente i grafi rappresentanti la rete.

3.2.2 Caratteristiche del grafo

Di seguito il codice *Python* per mettere in evidenza caratteristiche elementari della rete.

```
# Stampa il numero di nodi e archi del grafo
print("Numero di nodi:", G.number_of_nodes())
print("Numero di archi:", G.number_of_edges())
numeropossibiliarchi = (G.number_of_nodes() * (G.number_of_nodes() -1
                                    ) )/2
print("Numero di tutti i possibili archi del grafo: ",
                                    numeropossibiliarchi)

#Densita':
densitaG = nx.density(G)
print("Densita' del grafo: ", densit G)

#Grado Medio
average_degree = sum(dict(G.degree()).values()) / len(G)
print("Grado Medio:", average_degree)

#Diametro
diametro = nx.diameter(G)
print("Diametro: ", diametro)
```

3.2.3 Degree e Degree Centrality

Di seguito il codice *Python* per calcolare degree e degree centrality della rete.

```
# Calcola il grado di tutti i nodi
degrees = dict(G.degree())
```

```
# Calcola il grado medio dei nodi
avg_degree = sum(degrees.values()) / len(degrees)

# Ordina i valori del grado dei nodi in ordine decrescente
sorted_degrees = sorted(degrees.items(), key=lambda x: x[1], reverse=
                                    True)

# Stampa il grado dei nodi
for nodo, grado in sorted_degrees:
    print("Nodo:", nodo, "Grado:", grado)

# Stampa il grado medio dei nodi
print("Grado Medio dei Nodi:", avg_degree)
```

```
# Calcola la degree centrality di tutti i nodi
degree_centrality = nx.degree_centrality(G)

# Ordina i valori del grado dei nodi in ordine decrescente
degree_centrality_sorted = sorted(degree_centrality.items(), key=
                                    lambda x: x[1], reverse=True)

# Stampa i primi 10 nodi con la loro degree centrality
for i, (nodo, centrality) in enumerate(degree_centrality_sorted[:10])
                                    :
    print(str(i+1) + ". Nodo: " + str(nodo) + ", Degree Centrality: "
                                        + str(centrality))
```

3.2.4 Betweenness

Di seguito il codice *Python* per calcolare la Betweenness della rete, sia dei nodi che degli archi.

```
node_betweenness = nx.betweenness_centrality(G)

#Ordino i valori di betweenness e li stampo
node_betweenness_sorted = sorted(node_betweenness.items(), key=lambda
                                    x: x[1], reverse = True)
for i, nodo in node_betweenness_sorted:
    print("Il nodo ", i, "ha betweenness: ", nodo)

#Betweenness Centrality degli archi:
edge_betweenness = nx.edge_betweenness_centrality(G)

#Ordino i valori di betweenness e li stampo
edge_betweenness_sorted = sorted(edge_betweenness.items(), key=lambda
                                    x: x[1], reverse = True)
for arco, valore in edge_betweenness_sorted:
    print("L'arco ", arco, "ha betweenness: ", valore)
```

3.2.5 Closeness

Di seguito il codice *Python* per calcolare la Closeness della rete.

```
#Closeness centrality
closenessG = nx.closeness_centrality(G)
print(closenessG)
#Ordino i valori di closeness e li stampo
closeness_sorted = sorted(closenessG.items(), key=lambda x: x[1],
                                    reverse = True)
for nodo, closeness in closeness_sorted:
    print("Il nodo ", nodo, "ha closeness: ", closeness)
```

3.2.6 Eigenvector centrality

```
# Eigenvector_centrality
eigenvector_centrality = nx.eigenvector_centrality(G)

eigenvector_sorted = sorted(eigenvector_centrality.items(), key=
                                    lambda x: x[1], reverse=True)

for nodo, eigenvector in eigenvector_sorted[:10]:
    print("Nodo", nodo, " Eigenvector Centrality: ", eigenvector)
```

4 Conclusioni: preventire o perseguire? Perché è difficile scoprire le reti criminali?

Attualmente, l'analisi delle reti sociali (SNA) viene applicata con maggiore successo per perseguire, piuttosto che prevenire, attività criminali.

Come è stato evidente in questo caso con i dirottatori dell'11 settembre, **una volta che gli investigatori sapevano su chi concentrarsi, le connessioni tra i dirottatori sono state rapide da identificare** e si è potuto scoprire anche diversi associati degli stessi dirottatori.

Occorre fare particolare attenzione al fatto che essere collegati ad un terrorista non prova la colpevolezza, ma invita ad una indagine più approfondita per verificarne eventuali colpevolezze.

Ma quando si vuol fare il contrario, ovvero scoprire prima che sia troppo tardi le reti criminali è molto più difficile. Questo perché, come abbiamo messo in evidenza, **le reti segrete e criminali spesso non si comportano come normali reti sociali.** I criminali non stabiliscono molti legami al di fuori del loro *cluster* immediato, cioè al di fuori della loro cerchia di contatti fidati e in ogni caso quest'ultimi sono pochissimi. Perciò avremo reti poco dense e molto sparse, che privilegiano la segretezza rispetto all'efficienza. Più è inattiva la rete, più è difficile da scoprire.

Addiritura si è scoperto che **non c'erano connessioni tra i membri della rete degli dirottatori e gli estranei**. Spesso si riferiva che gli dirottatori si limitassero a sé stessi: non facevano amicizia al di fuori del cerchio fidato. Raramente interagivano con gli altri nella rete, e spesso uno di loro parlava per tutto il gruppo.

Avendo **obiettivi** da raggiungere, la rete segreta deve essere attiva a volte. È durante questi momenti di maggiore connessione che potrebbero essere più vulnerabili ad essere

scoperti.

La rete degli dirottatori aveva una ***forza nascosta***: una **massiccia ridondanza attraverso contatti fidati** conosciuti in precedenza. Questa caratteristica, più il fatto di essere una rete sparsa, rendevano la rete molto resiliente, infatti qualora uno di loro fosse stato catturato o compromesso, i danni sarebbero stati minimizzati.
Tuttavia, sebbene non conosciamo tutte le connessioni della rete, è possibile notare un ***punto debole***: sembra che molti dei legami fossero concentrati sui piloti, e cioè che quest'ultimi fossero **concentratori di informazioni**. Questo è un movimento rischioso per una rete segreta. Concentrare sia competenze uniche sia connettività negli stessi nodi rende la rete più facile da interrompere una volta scoperta, infatti una volta rimossi questi nodi l'intera rete sarebbe stata "distrutta" e non più capace di operare.

Una possibile **proposta di soluzione**, per interrompere una rete, consiste nel scoprire possibili sospetti mediante il campionamento chiamato snowball sampling, che consiste nel mappare prendere singoli individui e identificare le loro reti personali: vedere a chi portano e dove si sovrappongono. Chiaramente anche condividere le informazioni in proprio possesso con chi sta facendo la stessa investigazione può portare ad avere un quadro più completo.

È evidente come questo sia un ambiente ancora con molte strade da esplorare e molti studi da effettuare.

Riferimenti bibliografici

[1] Valdis Krebs (2002), *Uncloaking Terrorist Networks*, First Monday (First Monday Editorial Group (United States)).

Note: è possibile trovare lo stesso paper sotto il titolo: *"Mapping networks of terrorist cells."*

[2] Valdis Krebs, `http://www.orgnet.com/about.html`

[3] Malcolm K. Sparrow, 1991. *"The application of network analysis to criminal intelligence: An assessment of the prospects"*, Social Networks, volume 13, pp. 251-274

[4] Wayne E. Baker and Robert R. Faulkner, 1993. "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry," American Sociological Review, volume 58, number 6 (December), pp. 837-860

[5] Bonnie H. Erickson, 1981. "Secret Societies and Social Structure," Social Forces, volume 60, number 1 (September), pp. 188-210.

[6] Noah E. Friedkin, 1983. *"Horizons of Observability and Limits of Informal Control in Organizations"*, Social Forces, volume 62, pp. 54-77. (ReserchGate.net: `https://l1nq.com/nSXIH`)

[7] Review-Journal, 7 Settembre 2011, *Theories on why 9/11 hijackers visited Las Vegas*, `https://www.reviewjournal.com/news/theories-on-why-911-hijackers-visited-las-vegas/`