Resilienza ed Infrastrutture Critiche: un nuovo approccio per l'allocazione delle risorse

Autore: Luca Faramondi

Una delle maggiori sfide nella gestione della sicurezza delle infrastrutture critiche è l'individuazione di una politica di allocazione ottimale delle "scarse" risorse per la loro protezione al fine di garantire adeguati livelli di sicurezza e resilienza. In questo contesto, un passo fondamentale è la corretta individuazione di quegli elementi e/o parti dell'infrastruttura che sono maggiormente critici per l'erogazione dei diversi servizi.

Spesso, in ambito scientifico, la ricerca delle criticità di una infrastruttura è superficialmente ridotta alla ricerca di quei nodi della rete che rappresentano gli hub, cioè nodi centrali dal punto di vista topologico e geografico e fortemente connessi con gli altri nodi della rete.

La metodologia proposta in questo articolo vuole riassumere l'approccio studiato presso il laboratorio di sistemi complessi e sicurezza dell'Università Campus Bio-Medico di Roma, che ha come obiettivo l'identificazione di quei nodi di una infrastruttura considerati fondamentali al fine di garantire la connettività tra ogni nodo della rete.

L'approccio applicato dal gruppo di ricerca è basato sull'assunzione della prospettiva di un attaccante, interessato alla distruzione di una rete, il cui comportamento può essere descritto da due regole fondamentali: eseguire un attacco il meno costoso possibile (in termini economici e di risorse impiegate) e massimizzare il danno arrecato all'infrastruttura.

Il problema da risolvere è dunque evidentemente un problema con due obiettivi contrastanti: all'aumentare del costo dell'attacco aumenteranno anche gli effetti negativi dell'attacco, mentre al diminuire delle risorse impiegate diminuiranno i danni arrecati alla rete. Quindi la strategia dell'attaccante si può ricondurre, per semplicità, alla ricerca di quelle azioni di attacco (ovvero target da attaccare) che garantiscano un buon rapporto tra costo dell'azione malevola e danno arrecato all'infrastruttura.

Tale tipologia di problemi è frequentemente affrontata nel contesto della ricerca operativa ed è identificata come *Multi-Objective Optimization Problem*. Una caratteristica di questa classe di problemi è che, in genere, esistono più soluzioni "ottimali", ognuna caratterizzata da un costo più o meno elevato ed un impatto sulla rete più o meno considerevole. Sostanzialmente, quindi, un attaccante ha una moltitudine di possibili target ottimali individuati in funzione della sua propensione ad "investire" risorse nell'attacco ovvero del suo "desiderio" di ottenere un danno elevato nell'infrastruttura.

Negli schemi classici di analisi il difensore, non avendo indicazioni puntuali su quella che sarà la strategia che metterà in atto l'attaccante, effettuerà una valutazione dei possibili target da proteggere sula base di ipotesi (leggi profilazione) su ciò che farà l'attaccante.

Questa soluzione ha però il grosso limite che, qualora le ipotesi sulla strategia che l'attaccante metterà in piedi siano errate, si allochino in modo non adeguato le risorse. In altri termini, nonostante il significativo investimento di risorse nella protezione, l'infrastruttura è ancora molto vulnerabile.

L'analisi che abbiamo proposto cerca di superare questa limitazione. Per fare questo il nostro approccio cerca di considerare, con una visione olistica, tutte le

BIO

Luca Faramondi ricopre attualmente il ruolo di assegnista di ricerca presso il laboratorio "Complex Systems & Security Lab" dell'Università Campus Bio-Medico di Roma ed è docente a contratto del corso di Sistemi di Controllo per l'Automazione Industriale presso l'Università di Cassino e del Lazio Meridionale. L'attività di ricerca riguarda la protezione cyber e fisica delle infrastrutture critiche. Nel 2018 ha vinto il secondo premio del "CIPRNet Young Critis Award, un riconoscimento conferito ai ricercatori sotto i 32 anni che si sono distinti per i loro studi nel campo della sicurezza delle infrastrutture critiche. Dal 2017 è membro dell'IEEE SMC Technical Committee on Homeland Security.

possibili strategie di attacco ottimale. Da un punto di vista matematico, questo vuole dire, considerare tutte le soluzioni ottimali al problema multi obiettivo, ovvero quello che è definito come fronte di Pareto.

L'analisi effettuata terrà quindi in considerazione profili differenti di ipotetici attaccanti con capacità economiche più o meno significative ma sempre interessati al massimizzare il danno arrecato all'infrastruttura con gli strumenti di cui dispongono. In questo modo, l'approccio presentato non vincola in alcun modo, ne suppone a priori, la conoscenza della strategia di attacco se non l'intento di massimizzare il danno arrecato.

L'analisi che proponiamo si basa sulla frequenza con cui ogni nodo della rete risulta coinvolto in differenti piani di attacco nonostante i costi e gli effetti differenti. Tale metrica è stata definita come "indice di criticità del nodo".

L'analisi della distribuzione dei valori della metrica appena definita, ha permesso di identificare i nodi più critici, ovvero più attrattivi dal punto di vista di un attaccante.

Si noti che per poter applicare tale schema di analisi delle vulnerabilità, è necessario quantificare il danno arrecato alla rete nel momento in cui un nodo smette di funzionare perché considerato sotto attacco. Nello specifico, la nostra soluzione suggerisce di definire il danno arrecato in termini di degrado apportato alla connettività della rete nel momento in cui tale elemento smette di funzionare. Il concetto di connettività nel contesto cyber può essere generalizzato e riletto in ottica di collegamento tra due nodi.

L'idea di utilizzare la connettività come indice di impatto dell'attacco sulla rete deriva dal fatto che riteniamo tale caratteristica fondamentale per il funzionamento di una rete di telecomunicazione. In ogni caso l'approccio proposto è personalizzabile definendo nuove misure che descrivano l'effetto dell'attacco sulla rete.

Dal punto di vista matematico, la connettività è espressa in termini di "pairwise connectivity" la quale corrisponde al numero di nodi della rete connessi tra loro mediante un cammino (ovvero un collegamento).

L'obiettivo dell'attaccante, dunque, sarà quello di "spezzare" la rete in più partizioni al fine di non rendere fruibili i servizi che la caratterizzano o rendendo impossibile il raggiungimento di un nodo (server) da parte di un altro nodo (client).

Partendo da questa formulazione, l'azione dell'attaccante e il suo piano di attacco sono modellati come la rimozione di un sottoinsieme di nodi dalla rete con l'obiettivo di minimizzare la connettività con il minimo sforzo economico ed impiego di risorse.

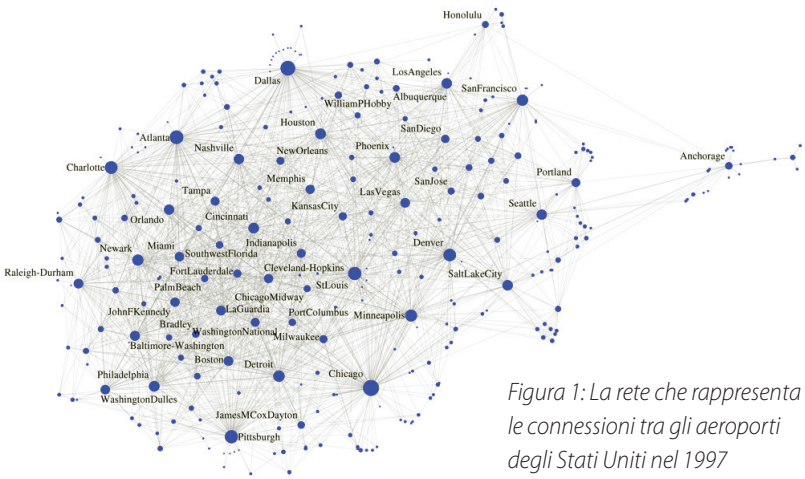

Figura 1: La rete che rappresenta le connessioni tra gli aeroporti degli Stati Uniti nel 1997

All'interno dello stesso studio, al fine di considerare uno scenario più realistico possibile, sono stati anche considerati aspetti legati all'eterogeneità dei nodi della rete e del costo necessario per coinvolgere quest'ultimi in un attacco malevolo.

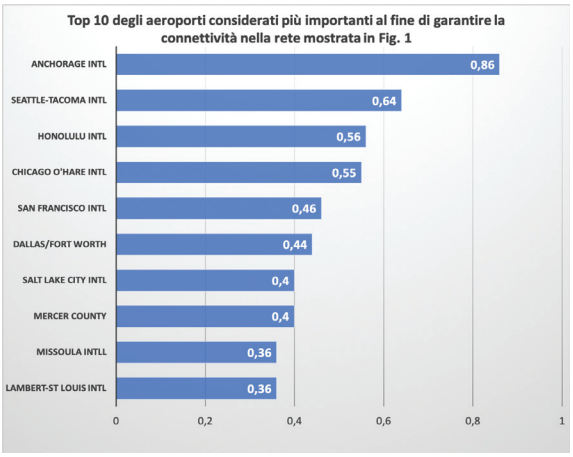

Figura 2 : Top 10 degli aeroporti considerati più importanti

La metodologia proposta è stata testata sulla rete mostrata in Figura 1, la quale rappresenta i voli aerei esistenti tra gli aeroporti degli stati uniti nel 1997. La rete è composta da 332 aeroporti e 4252 voli diretti. Ogni nodo rappresenta un aeroporto ed ogni collegamento l'esistenza di un volo diretto tra due aeroporti. I risultati riportati in Figura 2 evidenziano come nodi più critici della rete gli aeroporti di Anchorage, Seattle ed Honolulu, nonostante non siano gli aeroporti più connessi (cioè con più voli in partenza ed arrivo) ma risultano fondamentali per garantire la connessione tra tutti gli aeroporti del paese. L'andamento dei valori di criticità riportato in Figura 2 rappresenta gli aeroporti più appetibili ed interessanti per un gruppo di attaccanti con preferenze molto diverse tra loro e ne cattura gli aspetti in comune. Un aspetto molto interessante di tale studio è rappresentato dal fatto che un'allocazione di risorse per la protezione dell'infrastruttura, eseguita in maniera proporzionale agli indici appena individuali, incrementa sensibilmente la resilienza del sistema rendendo omogenea la distribuzione dei livelli di criticità tra i diversi nodi della rete.

Possiamo dunque concludere che tale studio intende spostare l'attenzione da quei nodi con funzione di hub centrali e fortemente connessi verso quei nodi che invece hanno la funzione di bridge e che spesso possono essere geograficamente periferici ma fondamentali al fine di garantire la connettività dell'infrastruttura.

Gli sviluppi futuri di tale studio sono mirati alla dimostrazione di come tale metrica possa essere alla base di piani di investimento per attuare politiche di protezione della rete, al fine di rendere l'infrastruttura più resiliente nei confronti di attacchi che mirano alla sospensione dei servizi che erogano. ■