

Game Theory applied to Network Security

Jacek Filipczuk

Giugno 2014

Indice

1	Introduzione	4
1.1	Sicurezza su Reti: Soluzioni attuali	5
1.2	Sicurezza su Reti: miglorie e fattori importanti .	6
2	Teoria dei Giochi	7
2.1	Teoria dei Giochi: Definizioni	7
2.2	Descrizione dei giochi più conosciuti	8
2.2.1	Gioco: Prisoner's Dilemma	8
2.2.2	Gioco: Tragedy of the Commons	11
2.2.3	Giochi di coordinazione	12
2.2.4	Strategie casuali (miste)	14
2.3	Concetti base sulle soluzioni dei giochi	15
2.3.1	Soluzioni con strategia dominante	15
2.3.2	Vickrey Auction: Modellare giochi con so- luzioni a strategia dominante	16
2.3.3	Equilibrio di Nash puro	16
2.3.4	Equilibri di Nash con Strategie Miste . . .	17
2.3.5	Giochi senza Equilibrio di Nash	18
2.3.6	Equilibri correlati	19
2.4	Classificazione dei giochi	20
2.4.1	Classificazione basata sul numero di stati	20
2.4.2	Classificazione basata sull'informazione Per- fetta o Imperfetta	20
2.4.3	Classificazione basata sull'informazione Com- pleta o Incompleta	21

3	Applicazioni alla Sicurezza di Rete	22
3.1	Sicurezza su Reti: Definizioni	22
3.1.1	Applicazioni per la Sicurezza su Reti . .	23
3.2	Classificazione delle Applicazioni alla Sicurezza su Reti	23
3.2.1	Applicazioni per l'analisi degli attacchi e delle difese di una rete	24
3.2.2	Vantaggi e svantaggi delle applicazioni per l'analisi degli attacchi e delle difese di una rete	26
3.3	Classificazione dei Modelli di Gioco	26
3.3.1	Modelli di giochi cooperativi	26
3.3.2	Modelli di giochi non-cooperativi	27
3.3.3	Discussione sulla modellazione dei giochi	30
4	Rilev. dinamica con Giochi Stocastici	32
4.1	Definizione del modello	33
4.2	Simulazione del modello	35
5	Conclusioni	40
6	Bibliografia	41

Capitolo 1

Introduzione

Una delle attività da sempre praticate dall'uomo è la comunicazione, lo scambio di informazioni tra individui. Con l'avvento delle nuove tecnologie la comunicazione si è evoluta e con essa i modi in cui praticarla.

Al giorno d'oggi il tipo di comunicazione più diffuso è quello delle reti internet. Internet infatti non è altro che un'enorme rete di comunicazione (che, da adesso, chiameremo semplicemente rete) che fornisce alle persone un facile accesso alle informazioni e un semplice modo di comunicare. Queste reti offrono notevoli vantaggi agli utenti ma soffrono anche di numerosi problemi di sicurezza come: Attacchi Internet, Cyber crimini, Denial of Service Attacks (DoS), accesso illegale a dati, oscuramento di dati o la loro eliminazione illegale, etc. Gli attacchi di rete possono danneggiare pubbliche istituzioni o entità private causando perdite di denaro, di dati importanti o della loro reputazione [4, 22, 27].

In questo lavoro lo scopo è quello di fornire una visione chiara e dettagliata su una possibile soluzione ai problemi di Sicurezza su Reti, tramite l'applicazione della Teoria dei Giochi. Di seguito una breve panoramica degli argomenti trattati:

Nel **Capitolo 1** viene presentata la situazione attuale dei sistemi e in particolare modo la loro inadeguatezza sotto il punto di vista della sicurezza.

Nel **Capitolo 2** viene spiegata nel dettaglio la Teoria dei Giochi, chiarendo tutte le terminologie usate da questa branca della scienza.

Nel **Capitolo 3** è presente una panoramica sulle attuali soluzioni adottate nella Sicurezza su Reti.

Nel **Capitolo 4** viene presentato un esempio pratico di Teoria dei Giochi applicata alla Sicurezza su Reti.

Infine, nel **Capitolo 5** vengono riassunti i pregi e i difetti dell'uso della Teoria dei Giochi applicata alla Sicurezza su Reti e viene proposto un suo sviluppo futuro.

1.1 Sicurezza su Reti: Soluzioni attuali

Le informazioni, in quanto tali, hanno un certo valore. Se pensiamo, ad esempio, alle informazioni di spostamento delle truppe durante una guerra, o anche solo alla data di uscita di un nuovo prodotto che deve rimpiazzare una vecchia versione dello stesso, ci possiamo rendere conto del loro valore. Per questa ragione le informazioni di valore non possono finire nelle mani di persone sbagliate, devono essere protette in qualche modo. Nasce così la Sicurezza su Reti, che ha lo scopo di proteggere e di rendere sicuro lo scambio di informazioni.

Le soluzioni tradizionali attualmente usate nella Sicurezza su Reti, ormai hanno delle carenze. Queste soluzioni sono implementate impiegando o un sistema di prevenzione, come un firewall, oppure un sistema reattivo, come un programma anti-virus, oppure usando entrambi. In ogni caso questi tipi di soluzioni non sono più sufficienti per avere una protezione della rete adeguata. Sistemi di rilevamento delle intrusioni (IDSs), i quali sono sistemi reattivi, sono diventati un'aggiunta indispensabile per qualsiasi sistema di sicurezza di un'organizzazione. Questa aggiunta è dovuta a un aumento nella tipologia di possibili attacchi di un sistema degli ultimi anni [18]. Un IDS è un sistema software o un hardware usato per monitorare tutto ciò che accade in una rete o un sistema di computer; un IDS è anche sfruttato per analizzare gli eventi monitorati e determinare se è stato compiuto un attacco al sistema. I metodi usati da un IDS per determinare le varie tipologie di attacchi sono ad esempio: Identificazione della firma degli attacchi, Rilevamento di modelli e Analisi statistica[20]. Una volta che l'attacco è stato individuato, viene inviato un messaggio all'amministratore del sistema che provvederà a fermare o almeno mitigare l'attacco. Alcuni IDS sono capaci di reagire ad un attacco rilevato senza contattare l'amministratore [12], questo tipo di sistemi è chiamato Sistema di Prevenzione delle Intrusioni (IPs). I sistemi IDS hanno però due debolezze, non sono molto sofisticati e si basano su schemi creati appositamente e su lavori sperimentali [14]. Per questo motivo hanno bisogno di strumenti di sviluppo adeguati per contrastare i tipi di attacchi più sofisticati.

1.2 Sicurezza su Reti: miglirie e fattori importanti

Molti ricercatori, nell'intento di migliorare la Sicurezza su Reti, hanno proposto approcci basati su modelli di Teoria dei Giochi [21]. La Teoria dei Giochi si concentra su problemi in cui ci sono più giocatori con obbiettivi diversi e che competono gli uni con gli altri, questo approccio può fornire un metodo matematico per analizzare e modellare i problemi di sicurezza riguardanti la rete. Inoltre la Teoria dei Giochi è in grado di analizzare numerosi scenari possibili (fino a centinaia di migliaia) prima di determinare la corretta sequenza di azioni da intraprendere [19]. Tutto questo migliora la capacità e la scelta delle decisioni di un amministratore di rete.

Un altro fattore molto importante che riguarda la sicurezza delle reti è la Misurazione della Sicurezza [1], essa è una valutazione dell'integrità, riservatezza, disponibilità, vulnerabilità e del rischio di un attacco per una rete. La Misurazione della Sicurezza di una rete è una categoria molto ampia che include la misurazione di ogni aspetto della Sicurezza su Reti. La valutazione dei rischi di attacco è una di queste misure [23]. La Misurazione della Sicurezza di una rete comprende le interazioni tra gli attaccanti e i difensori, e il risultato di questa misurazione può essere influenzato dalle loro interazioni. Per esempio, uno dei parametri della valutazione dei rischi di attacco per un sistema di rete è la probabilità di essere attaccati. Siccome le interazioni tra gli attaccanti e i difensori possono essere viste come un gioco, la Teoria dei Giochi può essere applicata a qualsiasi tipo di scenario in modo da predire le azioni degli attaccanti e determinare le decisioni da prendere per i difensori. Ecco perché, per la risoluzione dei problemi di Sicurezza su Reti, sono state proposte soluzioni basate su modelli di Teoria dei Giochi.

Nei seguenti capitoli verranno descritti numerosi concetti della Teoria dei Giochi che sono stati applicati per migliorare la sicurezza di rete. Sarà effettuata una loro classificazione con l'intento di compararli, esprimere i loro limiti e proporre nuovi argomenti di studio basati sulla Teoria dei Giochi. Verrà, inoltre, mostrato con più dettaglio un esempio pratico di una soluzione basata sui modelli di Teoria dei Giochi.

Capitolo 2

Teoria dei Giochi

In questo capitolo verranno spiegate le basi e la terminologia, necessarie per la comprensione della Teoria dei Giochi. Per una spiegazione più dettagliata e formale si rimanda a [13, 15, 6] .

2.1 Teoria dei Giochi: Definizioni

La Teoria dei Giochi è uno strumento matematico usato per la descrizione e la risoluzione dei giochi. La Teoria dei Giochi descrive un gioco definendo le entità (i giocatori) coinvolte, l'ordine in cui le entità eseguono delle azioni, l'insieme delle azioni possibili dalle entità, la conoscenza dei giocatori delle precedenti azioni effettuate da altri giocatori, una conoscenza che viene sfruttata prima che un giocatore esegua un'azione, e la conoscenza della funzione di guadagno di ogni giocatore. Un particolare importante è che la Teoria dei Giochi assume che ogni giocatore sia razionale, ciò comporta che un giocatore esegue sempre le azioni che lo portano ad ottenere il massimo guadagno possibile.

Un gioco include le interazioni tra le entità in qualsiasi situazione, e queste entità devono essere almeno due. Un gioco viene chiamato non-cooperativo se le entità sono in competizione tra loro. Viceversa viene chiamato cooperativo se le entità collaborano.

Nella Teoria dei Giochi gli elementi base necessari per descrivere un gioco sono i seguenti quattro:

Giocatori: Sono le entità coinvolte in un gioco. Queste entità possono essere persone, istituzioni, animali o qualsiasi altre cose che possono interagire tra loro.

Azioni: In ogni turno di un giocatore, lui/lei effettua un'azione. La Teoria dei Giochi assume che ogni giocatore conosce le azioni possibili di tutti gli altri giocatori.

Guadagno: Dopo che tutti i giocatori hanno eseguito le proprie azioni nel gioco, ognuno di loro avrà un ritorno positivo o negativo. Questo ritorno si chiama guadagno.

Strategie: La strategia di un giocatore è il suo piano delle azioni da eseguire basato sulla conoscenza delle azioni precedenti. Le strategie possono essere pure o miste.

La Teoria dei Giochi assume che ogni giocatore sia razionale, per questo motivo il giocatore sceglierà sempre quelle strategie che gli permettono di massimizzare il proprio guadagno in risposta alle strategie di altri giocatori. Questa situazione porta al concetto di Equilibrio in un gioco, che può essere considerato come soluzione del gioco stesso.

Un **Equilibrio** in un gioco è una combinazione delle strategie dei giocatori tale che ogni giocatore esegue le migliori azioni in risposta alle azioni eseguite dagli altri giocatori. Per migliori azioni si intende quelle azioni che portano a massimizzare il guadagno del giocatore. Un **Equilibrio di Nash** [6] è un tipo di equilibrio che può essere applicato per trovare la soluzione di un gioco.

2.2 Descrizione dei giochi più conosciuti

Per poter comprendere meglio la Teoria dei Giochi è opportuno descrivere quelli che sono considerati in letteratura i giochi più conosciuti e studiati dagli scienziati. Di seguito verranno descritti questi giochi con degli esempi di applicazioni reali.

2.2.1 Gioco: Prisoner's Dilemma

La Teoria dei Giochi ha come obiettivo quello di modellare situazioni in cui più partecipanti interagiscono fra di loro e ognuno ha effetto sul risultato dell'altro. Di seguito viene descritto quello che forse è il gioco più studiato e conosciuto nell'ambito della Teoria dei Giochi.

Prisoner's Dilemma

Due prigionieri vengono giudicati per un crimine e ognuno deve scegliere tra confessare il crimine o rimanere in silenzio. Se tutti e due restano in silenzio, le autorità non saranno in grado di confermare le accuse contro di loro e, quindi, i prigionieri passeranno un breve periodo in prigione, ad esempio 2 anni, per offese minori. Se solo uno dei prigionieri confessa, la sua pena sarà ridotta a 1 anno e verrà usato come testimone contro l'altro prigioniero, che riceverà, invece, una condanna a 5 anni di reclusione. Infine se tutti e due confessano il crimine, allora avranno un leggero sconto della pena per aver collaborato con le forze dell'ordine, e passeranno un periodo in prigione di

4 anni ognuno, invece di 5 anni. Si nota subito che ci sono quattro possibili risultati di questo problema, che possono essere riassunti in una matrice due per due, come mostrato di seguito.

		P2	
		Confess	Silent
P1	Confess	4 4	5 1
	Silent	1 5	2 2

Figura 2.1: Prisoner's Dilemma

Ognuno dei due prigionieri P1 e P2 ha due possibili strategie da adottare, quella di confessare e quella di restare in silenzio. Le strategie del prigioniero P1 corrispondono alle righe della matrice mentre quelle del prigioniero P2 corrispondono alle colonne. I valori delle celle della matrice corrispondono al prezzo che i prigionieri devono pagare, cioè gli anni di reclusione, se adottano quelle specifiche strategie. Una matrice di questo tipo viene chiamata “matrice dei costi” perché contiene appunto i costi che devono sostenere i prigionieri per aver scelto una determinata strategia. L'unica soluzione stabile è quando i due prigionieri confessano entrambi, in tutti gli altri casi almeno uno dei due prigionieri può cambiare la propria strategia per migliorare la sua situazione e avere un costo da pagare minore. D'altra parte una soluzione migliore si ha quando nessuno dei due giocatori confessa, ma questa situazione non è stabile perché ognuno dei giocatori è tentato nel cambiare la propria scelta e avere un tempo di reclusione inferiore. Lo scenario modellato dal Dilemma del prigioniero può essere applicato a molteplici situazioni reali, di seguito viene mostrato un esempio di indirizzamento ISP.

Gioco di indirizzamento ISP

ISP che sta per Internet Service Providers, non sono altro che le compagnie che gestiscono il traffico di rete. In questo tipo di problema, il traffico di rete che nasce in un ISP viaggia verso un secondo ISP, e questo genera un certo carico di traffico alla destinazione. Di seguito verrà mostrato come questo

problema risulti essere proprio un Dilemma del prigioniero.

Consideriamo due ISP, come mostrato in figura 2.2, ognuno avente una propria rete. Le due reti possono scambiare dati in due punti di transito, chiamati punti di peer, che saranno chiamati C e S. Nella figura sono presenti anche due coppie di punti sorgente-destinazione s_i e t_i . Supponiamo che l'ISP 1 debba mandare il suo traffico dal punto s_1 , presente nella sua rete, al punto t_1 , presente nell'altra rete. ISP ha due possibili opzioni per poter mandare il suo traffico, e queste opzioni corrispondono ai due punti di peer. Gli ISP di solito si comportano in maniera egoistica e tendono a minimizzare i propri costi, per questo scelgono come punto di peer quello che si trova più vicino, visto che poi il lavoro di indirizzamento verso il nodo destinazione spetta all'altro ISP.

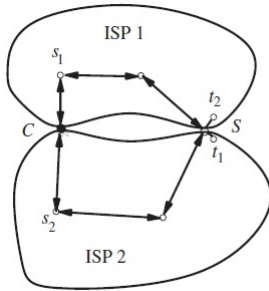


Figura 2.2: Problema dell'indirizzamento tra ISP

Il punto di peer C è quello più vicino, per usarlo l'ISP 1 deve pagare un costo di 1 unità (che corrisponde al mandare il traffico su un arco), invece se vuole usare il punto di peer S deve pagare 2 unità di costo. Da notare che il punto più lontano S è più vicino alla destinazione t_1 , e quindi indirizzare il traffico tramite questo nodo risulta in un costo totale minore. La lunghezza del percorso passando attraverso il punto C è 4 mentre passando attraverso S è 2, questo perché il punto S è molto vicino alla destinazione.

La situazione descritta per l'ISP 1 di indirizzare il traffico dalla sorgente s_1 alla destinazione t_1 è analoga alle scelte del prigioniero nel *Prisoner's Dilemma* perché ci sono due possibili scelte, di cui una è migliore da un punto di vista egoistico, ma danneggia l'altro giocatore. Affinché il gioco dell'indirizzamento risulti uguale al *Prisoner's Dilemma*, supponiamo che ci sia simmetria e che anche l'ISP 2 deve mandare del traffico dalla sorgente s_2 alla destinazione t_2 . Le due scelte dei due ISP portano a un gioco con matrice dei costi uguale a quella presentata nel *Prisoner's Dilemma*.

2.2.2 Gioco: Tragedy of the Commons

La tipologia di giochi che più interessa la Sicurezza su Reti è quella in cui vi sono molti partecipanti che interagiscono tra loro. Di seguito saranno descritti due giochi con più giocatori. Per prima una versione con più giocatori del Prisoner's Dilemma, che viene chiamata Pollution Game, seguita poi dal gioco Tragedy of the Commons.

Pollution Game

Questo gioco non è altro che la versione del Prisoner's Dilemma estesa a più giocatori. Esso è in grado di rappresentare numerosi scenari, e qui verrà applicato al controllo dell'inquinamento. Supponiamo che ci siano n paesi in questo gioco. Per questo modello supponiamo che ogni nazione deve decidere se approvare una legge sull'inquinamento o meno. Supponiamo anche che il controllo dell'inquinamento abbia un costo di 3 per un paese, ma ogni paese che inquina aggiunge un costo di 1 al prezzo che pagano tutti i paesi. Il costo del controllo dell'inquinamento (nell'esempio pari a 3) è decisamente maggiore del costo di 1 che ogni paese paga per essere socialmente irresponsabile.

Supponiamo che k paesi scelgano di non controllare l'inquinamento. Chiamamente il costo che questi paesi devono pagare risulta k . D'altra parte il costo pagato dagli altri $n - k$ paesi è $k + 3$, perché devono pagare il costo del proprio controllo dell'inquinamento. In questo scenario l'unica soluzione stabile è quella in cui nessun paese paga per il controllo dell'inquinamento, e ognuno ha un costo pari a n . Se, invece, ogni paese pagasse il controllo dell'inquinamento, il costo totale da pagare sarebbe solo 3 per ogni paese.

Tragedy of the Commons

Questo gioco verrà descritto nello scenario di condivisione della banda di una rete di collegamento. Supponiamo ci siano n giocatori e ognuno di loro vuole accedere a una risorsa condivisa. Ad esempio, ogni giocatore vuole inviare delle informazioni attraverso un canale di comunicazione condiviso che ha una capacità massima di 1. In questo gioco ogni giocatore avrà un insieme infinito di strategie, la strategia i -esima di un giocatore consiste nel mandare x_i unità di informazione attraverso il canale, con $x_i \in [0, 1]$. Supponiamo che ogni giocatore vorrebbe avere una grossa frazione della larghezza di banda, ma supponiamo anche che la qualità totale del canale peggiora con l'aumentare della banda usata. Questo gioco sarà descritto tramite un semplice modello, sfruttando una funzione di guadagno per ogni insieme di strategie. Se la larghezza di banda totale $\sum_j x_j$ supera la capacità del canale, nessun giocatore ottiene un guadagno. Se $\sum_j x_j < 1$ allora il guadagno per il giocatore i -esimo sarà $x_i(1 - \sum_j x_j)$. Questo modella perfettamente la situazione che è stata rappresentata: il guadagno di un giocatore diminuisce

con l'aumentare della larghezza di banda assegnata, ma aumenta con l'aumentare delle unità di informazione che trasmette, fino a un certo punto.

Per poter capire cosa sono le strategie stabili per un giocatore, è necessario concentrarsi su un singolo giocatore i -esimo, e supporre che il flusso di informazioni trasmesso dagli altri giocatori sia $t = \sum_{j \neq i} x_j < 1$. In questa situazione il giocatore i -esimo deve affrontare un semplice problema di ottimizzazione in cui deve scegliere la propria quantità di informazione da inviare: inviando x unità di informazioni egli avrà un guadagno pari a $x(1 - t - x)$. Se ne ricava che la soluzione ottimale per il giocatore i -esimo è $x = (1 - t)/2$. Un insieme di strategie è detto stabile se ogni giocatore sta eseguendo la strategia migliore per se stesso, conoscendo le strategie giocate dagli altri giocatori. Questa situazione equivale a dire che $t = \sum_{j \neq i} x_j/2$ per tutte le i , che ha come unica soluzione $x_i = 1/(n + 1)$ per tutte le i .

Una soluzione del genere è una tragedia (Tragedy of the Commons) perché il valore totale della soluzione è molto basso. Il guadagno per il giocatore i -esimo è $x_i(1 - \sum_{j \neq i} x_j) = 1/(n + 1)^2$, e quindi la somma dei guadagni di tutti i giocatori è $n/(n + 1)^2 \approx 1/n$. D'altra parte se la larghezza di banda totale usata è $\sum_i x_i = 1/2$ allora il guadagno totale risulta essere $1/4$, cioè approssimativamente $n/4$ volte maggiore. In questo gioco gli n giocatori sovraccaricano la risorsa condivisa e di conseguenza il guadagno totale diminuisce in maniera drastica.

2.2.3 Giochi di coordinazione

Di seguito sarà presentato un esempio di un gioco con più soluzioni stabili, chiamato "Battle of the sexes". Questo gioco, in particolare, è un esempio di un gioco di coordinazione, in cui due giocatori devono scegliere tra due opzioni diverse, e vogliono scegliere la stessa opzione.

I giochi di coordinazione sono naturalmente presenti in numerose situazioni. Un secondo esempio sarà dato di un gioco applicato alla gestione della congestione in un contesto di indirizzamento di rete. In Battle of the sexes, le soluzioni buone sono quelle in cui i due giocatori fanno la stessa scelta, in questo secondo esempio, invece, è il contrario, le soluzioni buone sono quelle in cui i giocatori fanno scelte diverse per non congestionare la rete. Di conseguenza questo tipo di gioco viene chiamato "Gioco di anticoordinazione".

Battle of the sexes

Consideriamo due giocatori, un ragazzo e una ragazza, che devono decidere come spendere il pomeriggio insieme. La coppia tiene in considerazione due possibilità: andare a vedere una partita di baseball o una di softball. Il ragazzo preferisce vedere la partita di baseball mentre la ragazza preferisce quella di softball, ma tutti e due preferiscono passare insieme il pomeriggio

piuttosto che separati. Di seguito viene mostrata la matrice dei costi che rappresenta lo scenario appena descritto.

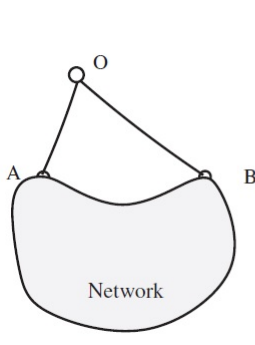
		Boy	
		B	S
Girl	B	6 5	1 1
	S	2 2	5 6

Figura 2.3: Battle of the Sexes

Come si nota, le due soluzioni in cui i giocatori scelgono di vedere cose diverse, non sono stabili perché uno dei due può cambiare la propria scelta e migliorare il proprio guadagno. D'altra parte le due soluzioni rimanenti, riguardanti lo stesso gioco, baseball o softball, sono stabili. Il ragazzo preferisce il primo mentre la ragazza preferisce il secondo.

Routing congestion game

Supponiamo che due flussi di traffico originari del nodo proxy O , devono essere indirizzati nella rete come mostrano in figura 2.4.



		Traffic 1	
		A	B
Traffic 2	A	5 5	2 1
	B	1 2	6 6

Figura 2.4: Routing Congestion Game

Supponiamo anche che il nodo O sia connesso alla rete tramite due punti di connessione A e B , dove A è un punto leggermente più vicino rispetto a B . In ogni caso tutti e due i punti si congestionano facilmente, di conseguenza mandare tutti e due i flussi tramite uno stesso punto causerebbe un notevole ritardo nella trasmissione. In questo gioco il guadagno maggiore si ottiene quando i due flussi di traffico si coordinano e vengono trasmessi attraverso due punti di trasmissione differenti.

Questo scenario viene modellato come se i due flussi di traffico fossero due giocatori. Ogni giocatore ha due possibili strategie da adottare, effettuare l'indirizzamento attraverso il punto A o attraverso il punto B , e questo porta a un totale di quattro diverse possibilità. La matrice dei costi presente in figura 2.4 esprime il costo, espresso come tempo di ritardo, per ogni possibile combinazione delle scelte dei giocatori.

2.2.4 Strategie casuali (miste)

Nei giochi descritti fino ad ora esistevano soluzioni stabili, ovvero soluzioni in cui nessun giocatore voleva cambiare la propria scelta, perché qualsiasi scelta avesse fatto avrebbe diminuito il proprio guadagno. Non tutti i giochi però presentano soluzioni stabili, il seguente ne è un esempio.

Matching pennies

Consideriamo due giocatori, ognuno di loro ha una moneta e a ognuno viene chiesto di scegliere tra due strategie possibili, cioè devono scegliere tra testa (H) e croce (T). Il primo giocatore, diciamo quello della riga nella matrice dei costi, vince se le due monete combaciano, cioè se sono tutte e due testa o croce. L'altro giocatore, invece, vince quando le due monete non combaciano, cioè quando una vale testa e l'altra croce. Questa situazione è espressa dalla matrice dei costi, in cui il valore 1 rappresenta la vincita e il valore -1 la sconfitta.

		2	
		H	T
1	H	-1 1	1 -1
	T	1 -1	-1 1

Figura 2.5: Pennies Game

Come si può facilmente notare questo tipo di gioco non presenta una soluzione stabile. L'unica soluzione ragionevole per i giocatori è quella di effettuare una scelta casuale per contrastare la strategia del giocatore avversario.

2.3 Concetti base sulle soluzioni dei giochi

Di seguito verranno descritti concetti base riguardanti le soluzioni dei giochi descritti in precedenza. Questi concetti vengono usati nella Teoria dei Giochi per studiare i vari modelli di giochi. In particolare verrà data la definizione formale di stabilità che è stata usata in maniera informale fino ad ora per indicare una soluzione stabile in alcuni giochi.

2.3.1 Soluzioni con strategia dominante

Il “Prisoner’s Dilemma” e il “Pollution Game” hanno in comune una determinata proprietà: in questi giochi il giocatore ha un’unica migliore strategia, che risulta indipendente dalle scelte degli altri giocatori. Un gioco avente questa proprietà viene chiamato gioco con *soluzione a strategia dominante*. Diamo ora una definizione formale di strategia dominante. Dato un vettore di strategie $s \in S$ denotiamo con s_i la strategia giocata dal giocatore i -esimo e con s_{-i} il vettore $(n-1)$ -dimensionale delle strategie giocate da tutti gli altri giocatori. Denotiamo anche con $u_i(s)$ il guadagno (o l’utilità) ottenuta dal giocatore i -esimo, che scriveremo anche come $u_i(s_i, s_{-i})$. Sfruttando questo tipo di notazione possiamo dire che un vettore di strategie $s \in S$ è una soluzione a strategia dominante se, per ogni giocatore i e per ogni vettore di strategie alternativo $s' \in S$, si ha

$$u_i(s_i, s'_{-i}) \geq u_i(s'_i, s'_{-i})$$

Bisogna notare che una soluzione a strategia dominante potrebbe non fornire ai giocatori il miglior guadagno possibile. Infatti i giochi *Prisoner’s Dilemma* e *Pollution Game* ne sono un esempio perché è possibile aumentare il guadagno di tutti i giocatori contemporaneamente se non viene usata la strategia dominante.

Avere una singola strategia dominante per ogni giocatore è un vincolo molto forte, e sono veramente pochi i giochi che lo soddisfano. La Teoria dei Giochi studia anche i metodi con i quali poter modellare giochi che abbiano una soluzione a strategia dominante e che questa soluzione porti a dei risultati desiderati. Di seguito viene mostrato un esempio di questo tipo.

2.3.2 Vickrey Auction: Modellare giochi con soluzioni a strategia dominante

Supponiamo di dover creare un'asta per poter vendere un dipinto molto prezioso. Per poter modellare questo scenario tramite un gioco, supponiamo che ogni giocatore i (partecipante all'asta) dia un proprio valore v_i al dipinto. Il guadagno di questo giocatore risulta 0 nel caso in cui perde mentre, nel caso in cui compra il dipinto ad un prezzo p , il suo guadagno è $v_i - p$. La strategia di ogni giocatore consiste semplicemente nel scegliere la propria offerta per acquistare il dipinto, cioè il valore di p . Consideriamo che il gioco che modella questo scenario sia un gioco one-shot e quindi supponiamo che i giocatori devono fare la propria offerta contemporaneamente, metterla in una busta, ad esempio, e successivamente verrà deciso il vincitore del dipinto in base alle offerte presenti nelle buste.

Il modello di gioco più diretto potrebbe essere quello di assegnare il vincitore in base all'offerta più alta presente nelle buste. Questo gioco non ha una soluzione a strategia dominante. La strategia migliore per un giocatore dipende da quello che quel giocatore sa o suppone sulle strategie degli altri giocatori. Per questo motivo decidere la strategia sembra un problema difficile e con risultati imprevedibili.

Il meccanismo di Vickrey, chiamato *second price auction*, evita i problemi riguardanti la scelta dell'offerta da fare per acquistare il dipinto. Come nel modello precedente il dipinto viene dato al giocatore con l'offerta più alta, ma quel giocatore invece di pagare il valore della sua offerta, paga il valore della seconda offerta più alta. Questo particolare modello di gioco della seconda offerta più alta ha un'importante proprietà: la strategia dominante di ogni giocatore è quella di scegliere il suo vero valore personale (v_i) come offerta per l'acquisto del dipinto, indipendentemente dalle scelte effettuate dagli altri giocatori. Bisogna notare che anche se il valore personale di un giocatore è molto alto, quel giocatore pagherà al massimo la seconda offerta più alta.

Notiamo ora altre due proprietà dell'asta di Vickrey. La prima è che forza il gioco verso una soluzione desiderata, ovvero quella in cui è il giocatore con il valore personale più alto a ottenere il dipinto. L'altra proprietà dei giochi con soluzione a strategia dominante, come la *Vickrey Auction*, è che risultano molto semplici da giocare per i giocatori, visto che la strategia di un giocatore è indipendente da quelle degli altri giocatori.

2.3.3 Equilibrio di Nash puro

L'equilibrio di Nash riesce a catturare la nozione di soluzione stabile, quella usata in *Tragedy of the Commons* e *Battle of the Sexes*, una soluzione in cui nessun giocatore è incentivato a cambiare la propria scelta perché non otterrebbe nessun aumento di guadagno.

Un vettore di strategie $s \in S$ viene chiamato un Equilibrio di Nash se per ogni giocatore i e per ogni strategia alternativa $s'_i \in S$ si ha:

$$u_i(s_i, s_{-i}) \geq u_i(s'_i, s_{-i})$$

In altre parole nessun giocatore i può cambiare la sua strategia da s_i a s'_i e di conseguenza incrementare il proprio guadagno, e questo vale quando tutti gli altri giocatori non cambiano le proprie strategie. Questo tipo di soluzione è auto-rafforzativa, ciò vuol dire che una volta che i giocatori hanno scelto una soluzione del genere, sono incentivati a non cambiarla più.

Chiaramente una soluzione a strategia dominante è un Equilibrio di Nash. Inoltre se la soluzione è strettamente dominante, cioè questa scelta incrementa sempre il guadagno finale, allora è anche l'unico Equilibrio di Nash. Bisogna dire, però, che gli Equilibri di Nash non sono unici, infatti nei giochi di coordinazione sono presenti numerosi Equilibri di Nash.

Come detto in precedenza, gli Equilibri di Nash possono non essere ottimi per i giocatori, visto che le soluzioni a strategia dominante sono degli Equilibri di Nash. Nei giochi con multipli Equilibri di Nash, ci possono essere guadagni per i giocatori con valori molto diversi tra un equilibrio e l'altro. In conclusione possiamo dire che la proprietà migliore degli Equilibri di Nash è che sono stabili, ovvero una volta che i giocatori scelgono un Equilibrio di Nash, non sono incentivati a cambiare la propria scelta.

2.3.4 Equilibri di Nash con Strategie Miste

Gli Equilibri di Nash presentati fino ad ora sono chiamati *equilibri a strategia pura*, questo deriva dal fatto che ogni giocatore sceglie in maniera deterministica quale strategia effettuare. Come mostrato in *Matching Pennies*, un gioco non deve per forza possedere alcun equilibrio a strategia pura. Se, per esempio, in *Matching Pennies* ai giocatori viene data la possibilità di scegliere una delle due possibili strategie in maniera casuale, allora si ottiene una soluzione stabile in un certo senso. Il motivo di questo è che il guadagno atteso di ogni giocatore risulta 0 e nessuno di loro può incrementarlo scegliendo delle probabilità diverse.

Quando i giocatori scelgono la propria strategia in maniera casuale, bisogna capire come viene calcolato il guadagno. Un giocatore preferisce avere con grande probabilità un piccolo guadagno positivo, oppure con una piccola probabilità un grande guadagno negativo? Queste ed altre domande portano a una considerazione finale: nella nozione di Equilibri di Nash con Strategie Miste, si suppone che i giocatori sono indifferenti ai rischi, ovvero cercano sempre di massimizzare il guadagno atteso.

Proviamo ora a formalizzare queste strategie casuali, sottolineiamo il fatto che ogni giocatore può scegliere una propria distribuzione di probabilità e sfruttare quella nella scelta della strategia da adottare, una scelta di questo tipo viene chiamata *strategia mista*. Assumiamo che i giocatori scelgono

in maniera indipendente le proprie strategie seguendo la distribuzione di probabilità. Queste scelte indipendenti dei giocatori portano a un vettore s contenente la distribuzione di probabilità delle strategie. Nash ha dimostrato che sotto queste condizioni, ogni gioco avente un numero finito di giocatori, i quali hanno un numero finito di strategie, possiede un Equilibrio di Nash.

2.3.5 Giochi senza Equilibrio di Nash

Nash ha affermato che, nei giochi in cui è presente un numero finito di giocatori e ogni giocatore ha un numero finito di strategie, allora è presente un Equilibrio di Nash in quel gioco. Nel caso in cui invece una di queste due proprietà viene a mancare allora non è sicuro che esista un Equilibrio di Nash. Di seguito viene mostrato un esempio di gioco che non ha un Equilibrio di Nash, il *Pricing Game*.

Pricing Game

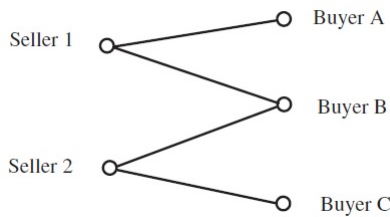


Figura 2.6: Pricing Game

Supponiamo che due giocatori vogliano vendere un prodotto a tre possibili acquirenti come mostrato in figura 2.6. Ogni acquirente vuole comprare una unità del prodotto. Gli acquirenti A e C hanno accesso a un solo venditore, rispettivamente 1 e 2. Mentre l'acquirente B può acquistare il prodotto da uno qualsiasi dei due venditori. Tutti e tre gli acquirenti hanno un budget di 1, vedendola da un'altra prospettiva, il valore che danno al prodotto è pari a 1, quindi se il prodotto costa di più non lo acquisteranno. I venditori giocano il *Pricing Game*, cioè ognuno stabilisce un prezzo p_i nell'intervallo $[0, 1]$. Gli acquirenti A e C comprano, rispettivamente, dai venditori 1 e 2. D'altra parte l'acquirente B compra dal venditore con il prezzo del prodotto minore. Per specificare completamente il gioco bisogna aggiungere qualche altra regola, ad esempio assumiamo che se i due venditori vendono il prodotto allo stesso prezzo, allora l'acquirente B acquista dal venditore 1. Inoltre assumiamo che non ci sono costi di produzione, di conseguenza il guadagno

di un venditore è pari al prezzo di vendita del prodotto che vende.

Una strategia possibile in questo scenario è quella in cui ciascun venditore sceglie come prezzo di vendita $p_i = 1$, in questo modo si garantisce un guadagno di 1 proveniente dall'acquirente che non può scegliere da chi acquistare. Altrimenti i due venditori si possono contendere l'acquirente B. Bisogna specificare però, che un venditore non può scegliere il prezzo in base all'acquirente, una volta scelto il prezzo rimane lo stesso per tutti gli acquirenti. In questo gioco un venditore ha un numero infinito di strategie possibili, perché può scegliere un qualsiasi valore nell'intervallo $[0, 1]$. Gli studi effettuati su questo gioco hanno dimostrato che non vi è presente alcun Equilibrio di Nash, anche se i giocatori usano strategie miste.

Un esempio che non esiste nessun equilibrio è quello in cui uno dei due venditori, supponiamo il venditore 1, scelga come prezzo di vendita $p_1 \geq 1/2$, in questa situazione il venditore 2 potrà sempre scegliere un prezzo tale che $1/2 \leq p_2 < p_1$, il venditore 1 a questo punto può scegliere un altro prezzo che risulti minore di p_2 e questa situazione può continuare all'infinito.

2.3.6 Equilibri correlati

Un ulteriore rilassamento dell'Equilibrio di Nash fu studiato da Aumann, e chiamato *Equilibrio Correlato*. Di seguito viene descritto un gioco che illustra in maniera semplice questo concetto.

Traffic Light

Il gioco che verrà qui descritto tratta di due giocatori che guidano la macchina fino allo stesso incrocio nello stesso tempo. Se tutti e due attraversano l'incrocio, il risultato sarà un tragico incidente stradale. Il gioco è stato modellato da una matrice dei costi in cui: attraversare l'incrocio con successo ha un guadagno pari a 1, non attraversare ha un guadagno pari a 0, mentre un incidente ha un guadagno di -100.

Questo gioco ha tre Equilibri di Nash: due corrispondono al caso in cui una delle due macchine attraversa l'incrocio e l'altra no, mentre il terzo è un equilibrio con strategia mista dove i due giocatori attraversano l'incrocio con una piccola probabilità $\epsilon = 1/100$, e hanno un incidente con probabilità ϵ^2 . I primi due equilibri hanno un guadagno di 1. L'ultimo invece è un equilibrio più giusto, ma ha un guadagno atteso molto basso e inoltre c'è la possibilità di un incidente.

In un Equilibrio di Nash i giocatori scelgono le proprie strategie in maniera indipendente. In un equilibrio correlato, invece, è presente un coordinatore che sceglie le strategie per i giocatori, fermo restando che le strategie scelte sono una soluzione stabile. La richiesta è quella che sia nell'interesse di ogni giocatore effettuare la strategia scelta dal coordinatore. Per esempio, in un equilibrio correlato il coordinatore può scegliere in maniera casuale quale dei

due giocatori debba attraversare l'incrocio. Il giocatore a cui è stato ordinato di non attraversare ottiene un guadagno pari a 0, ma quel giocatore sa che se attraversa l'incrocio causerà un incidente.

2.4 Classificazione dei giochi

Esistono diversi aspetti sui quali è possibile classificare i diversi tipi di giochi. Di seguito saranno mostrati alcuni metodi diversi di classificazione.

2.4.1 Classificazione basata sul numero di stati

Un secondo metodo di classificazione si basa sulla proprietà che un gioco abbia un singolo stato o stati multipli.

Un *gioco Strategico/Statico* è un gioco one-shot nel quale i giocatori eseguono le proprie azioni contemporaneamente. Un gioco Statico può essere visto come un gioco a informazione imperfetta, perchè in ogni situazione un giocatore conosce soltanto le mosse che ha eseguito[13].

Un *gioco Dinamico/Estensivo* è un gioco composto di stati o mosse multiple. Il numero di stati può essere finito o infinito[13].

Un *gioco Stocastico* è un tipo di gioco dinamico in cui c'è uno stato iniziale ed è possibile effettuare una transizione da uno stato all'altro con una certa probabilità; nello stato iniziale i giocatori effettuano delle azioni, ricevono un guadagno ed effettuano una transizione in un altro stato; la transizione avviene con una certa probabilità basata sullo stato corrente e sulle azioni eseguite.

2.4.2 Classificazione basata sull'informazione Perfetta o Imperfetta

Il seguente metodo di classificazione si basa sulla proprietà che un gioco abbia informazione Perfetta o meno.

In un *gioco con Informazione Perfetta* ogni giocatore conosce tutte le azioni precedenti degli altri giocatori nel momento in cui deve scegliere la prossima azione da eseguire. Un esempio di questo tipo di gioco sono gli Scacchi.

In un *gioco con Informazione Imperfetta* almeno un giocatore non conosce tutte le azioni precedenti degli altri giocatori quando deve scegliere la prossima azione da eseguire.

2.4.3 Classificazione basata sull'informazione Completa o Incompleta

Un altro metodo di classificazione si basa sulla proprietà che un gioco abbia informazione completa o meno.

In un *gioco a Informazione Completa* ogni giocatore conosce la funzione di guadagno degli altri giocatori, ovvero conosce il guadagno che un giocatore avrebbe per qualsiasi azione che quel giocatore può eseguire.

In un *gioco a Informazione Incompleta* almeno un giocatore non conosce la funzione di guadagno degli altri giocatori.

In [13], l'autore identifica i giochi a Informazione Incompleta come **Giochi Bayesiani**. Nei giochi Bayesiani il termine “tipo” viene usato per definire l'informazione incompleta. Infatti un giocatore può essere di uno o più tipi. La funzione di guadagno di ogni tipo di giocatore è conosciuta a tutti, l'informazione incompleta sta nel fatto che almeno un giocatore non conosce il tipo di uno o più altri giocatori. L'analisi Bayesiana viene usata per predire le strategie dei giocatori. Un esempio di un Gioco Bayesiano è il gioco dell'asta descritto in [13].

Capitolo 3

Applicazioni alla Sicurezza di Rete

In questo capitolo saranno fornite alcune definizioni di base e sarà effettuata una classificazione delle applicazioni della Teoria dei Giochi alla Sicurezza di Rete.

Il materiale di seguito proposto proviene in gran parte dal lavoro [25] in cui gli argomenti trattati sono affrontati con maggior dettaglio. Per approfondimenti in materia si rimanda a [25].

3.1 Sicurezza su Reti: Definizioni

Nelle Reti spesso vengono discusse le interazioni tra gli attaccanti e i difensori, queste interazioni sono astratte nei seguenti scenari: gli attaccanti eseguono gli attacchi sulla rete o sul sistema di computer, mentre i difensori si difendono da questi attacchi. Di seguito saranno descritti alcuni termini utili alla comprensione di questa astrazione.

Sistema: Nelle Reti, un sistema può essere un nodo, un apparecchio, un host, un software, un processo o una collezione di due o più di questi oggetti.

Attaccante: Qualsiasi persona o cosa che effettua un attacco ad un sistema con l'intento di causare danni o perdite di qualsiasi tipo al sistema o al suo proprietario.

Bersaglio: Il sistema che è stato attaccato o che è a rischio di attacco.

IDS: Un sistema software o hardware usato per monitorare gli eventi che accadono in una Rete, o un sistema di computer, sfruttato per analizzare questi eventi con l'intento di individuare se c'è stato o è in corso un attacco[18]. Negli scenari che saranno descritti, si presuppone che

gli IDS siano senza errori, ovvero segnalano un attacco solo quando questo realmente avviene. Nella realtà invece non è così, infatti un IDS può segnalare un falso attacco o non segnalarne uno.

Sensore Virtuale: Si tratta di un agente software usato per monitorare un sistema e raccogliere dati con lo scopo di migliorare il rilevamento delle intrusioni [28]. I sensori virtuali possono essere considerati come parte degli IDS.

Difensore: Un entità in grado di monitorare gli eventi che accadono in un Bersaglio, analizzandoli, determinando se c'è stato un attacco e rispondendo a quest'ultimo. Un IDS in grado di rispondere a un attacco indipendentemente dall'amministratore del sistema, è considerato un difensore.

3.1.1 Applicazioni per la Sicurezza su Reti

La Sicurezza è un concetto strettamente collegato ad altri, come l'integrità, l'affidabilità o la disponibilità. La misura della sicurezza valuta il livello di sicurezza presente. Esistono numerose metriche per la sicurezza e la misura dell'affidabilità, come il tempo medio di fallimento (MTTF), il tempo medio del primo fallimento (MTFF) [3], il tempo medio tra fallimenti (MTBF) [8], tempo medio al prossimo fallimento, e rischio [23]. Anche il Price of Anarchy (POA) [5] è stato proposto come metrica per valutare l'efficacia di un sistema in termini di sicurezza. Per valutare meglio la sicurezza di una rete è necessario avere una predizione delle azioni dell'attaccante e del difensore. Siccome il processo di interazione tra attaccante e difensore è un gioco, la Teoria dei Giochi può essere applicata per ottenere le predizioni desiderate. Queste predizioni vengono poi usate nel modulo di misurazione con lo scopo di ottenere le giuste metriche di sicurezza e affidabilità.

In [8], ad esempio, le metriche di sicurezza, la MTTF e la MTFF, sono studiate in un sistema di difesa di una rete; questo fornisce un esempio della misura del DNS di un server come caso di studio. La Teoria dei Giochi viene usata per modellare il gioco tra attaccante e difensore e per predire le strategie dei due giocatori. Basandosi sulle strategie predette, viene creata la matrice di transizione di Markov e successivamente questa viene data in input al modulo di misurazione.

3.2 Classificazione delle Applicazioni alla Sicurezza su Reti

Le applicazioni della Teoria dei Giochi nella Sicurezza su Reti possono essere classificate in due grandi categorie come mostrato in figura 3.1 :

- **Applicazioni per l'analisi degli attacchi e delle difese di una rete:** si tratta di modellare le interazioni tra gli attaccanti e i difensori

come un gioco, effettuando la predizione delle azioni degli attaccanti e determinando le strategie di difesa dei difensori.

- **Applicazioni per la Sicurezza su Reti e misura della sua disponibilità:** si tratta di predire le strategie degli attaccanti e dei difensori e valutare la sicurezza del sistema basandosi su queste predizioni.

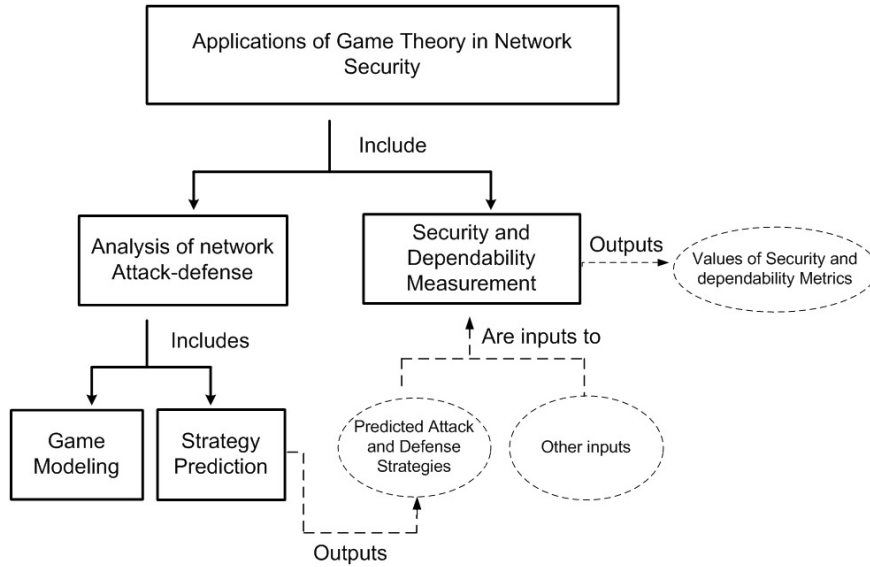


Figura 3.1: Relazioni tra le applicazioni della Teoria dei Giochi alla Sicurezza su Reti

3.2.1 Applicazioni per l'analisi degli attacchi e delle difese di una rete

Come già detto nell'introduzione, le soluzioni tradizionali adottate per la Sicurezza su Reti mostrano le proprie debolezze quando affrontano attaccanti più sofisticati o meglio organizzati. Questo tipo di soluzioni necessitano di un sistema di decisioni quantitativo. La Teoria dei Giochi può essere applicata per creare un tale sistema. Esso include la modellazione, sotto forma di gioco, delle interazioni tra gli attaccanti e i difensori e la predizione delle azioni dei primi e la determinazione delle strategie di difesa dei secondi. Le applicazioni per l'analisi degli attacchi e delle difese di una rete sono formate da due sotto-categorie: 1.a) quelle per l'analisi generale, e 1.b) quelle per l'analisi specializzata. Le due sotto-categorie verranno di seguito descritte.

Applicazioni per l'analisi generale degli attacchi e delle difese di una rete

Nello scenario del problema di questa applicazione, le reti spesso non sono specifiche ma astratte, lo scenario consiste in un attaccante contro un difensore e le azioni dell'attaccante sono quelle di attaccare e di non fare altro. Le azioni del difensore sono di difendere e di non fare altro. Un altro possibile scenario di questo tipo di applicazioni [2] è rappresentato da un difensore che non possiede informazione perfetta sul tipo di un nodo della rete, ovvero non sa se quel nodo è un attaccante o meno e può basarsi soltanto su una propria supposizione. In [2], viene considerato un metodo di rilevazione di intrusioni in una rete mobile ad hoc. In questo scenario, il difensore non sa se il nodo vicino è un attaccante o un utente regolare, per questo deve basarsi su una propria supposizione. Il nodo difensore può scegliere di difendere, non fare nulla, o scegliere casualmente tra una delle due opzioni precedenti. In [7] l'autore analizza quattro scenari competitivi tra due attaccanti e due difensori. Ogni scenario è modellato come un gioco statico con due giocatori e gli autori hanno mostrato come i giocatori sfruttano strategie effettive durante il gioco.

Applicazioni per l'analisi specializzata degli attacchi e delle difese di una rete

La maggior parte delle applicazioni ricade in questa sotto-categoria. I scenari dei problemi di questo tipo di applicazioni possiedono almeno uno dei seguenti elementi: una rete specializzata dove si verificano attacchi, azioni di difesa o attacco più complesse, o multipli livelli di interazione tra i difensori e gli attaccanti.

In [24], gli autori presentano il modello di un approccio alla gestione del rischio di sicurezza. Nel loro approccio considerano l'organizzazione della sicurezza come una combinazione di divisioni differenti. Un esempio da loro proposto è quello di una compagnia che offre servizi video e che era costituita dalle seguenti divisioni: reti centralizzate, infrastrutture TV mobili, amministratori informatici e servizio di supporto, e servizio di video su richiesta. Considerano anche che le risorse di sicurezza, come il budget e gli investimenti in ogni divisione, sono linearmente dipendenti tra di loro, e quindi mettono in risalto le vulnerabilità di ogni divisione. Infine basandosi su queste dipendenze lineari sviluppano dei modelli matematici che descrivono delle tipologie di giochi atte a rappresentare lo scenario.

3.2.2 Vantaggi e svantaggi delle applicazioni per l'analisi degli attacchi e delle difese di una rete

I vantaggi principali dell'applicazione della Teoria dei Giochi alle applicazioni per l'analisi generale degli attacchi e delle difese di una rete sono la semplicità e la facilità di uso. Visto che lo scenario è semplice, l'interazione tra attaccante e difensore può essere modellata tramite un semplice gioco, come quello statico a due giocatori o quello Bayesiano. La Teoria dei Giochi fornisce soluzioni a questo tipo di giochi, di conseguenza è relativamente facile ottenere una soluzione al problema modellato sotto forma di questo tipo di gioco. D'altra parte lo svantaggio maggiore è la sua ineguatezza in scenari più complessi. I vantaggi dell'applicazione della Teoria dei Giochi alle applicazioni per l'analisi specializzata degli attacchi e delle difese delle reti sono la capacità di considerare scenari più complessi e realistici e di descrivere meglio la dinamica delle interazioni. I suoi svantaggi sono la complessità e una possibile mancanza di robustezza. I modelli di gioco usati per questo tipo di analisi sono più complessi di quelli usati per l'analisi generale. La soluzione del gioco non è facile da calcolare e può essere diversa dalla soluzione calcolata teoricamente. Questo può causare una predizione degli attacchi inefficace e portare, quindi, a decisioni difensive errate.

3.3 Classificazione dei Modelli di Gioco

Tutti gli approcci della Teoria dei Giochi alla Sicurezza su Reti richiedono interazioni tra attaccante e difensore, che possono essere modellate come un gioco e quindi risolte usando la Teoria dei Giochi. Di seguito viene presentata una classificazione dei modelli di gioco usati per la modellazione delle interazioni tra attaccanti e difensori. Questi modelli possono essere suddivisi in due classi: modelli di giochi cooperativi e modelli di giochi non-cooperativi, dove quest'ultimi presentano due sotto-classi: giochi statici e giochi dinamici. Questi approcci richiedono, inoltre, la risoluzione del gioco per ottenere la predizione delle strategie usate dagli attaccanti e dai difensori. Passiamo ora alla descrizione dei due modelli di gioco appena nominati.

3.3.1 Modelli di giochi cooperativi

Gli autori di [24] hanno pubblicato il loro lavoro sul rischio della gestione della sicurezza nel 2010, proponendo un modello di gioco cooperativo insieme a un modello non-cooperativo delle relazioni tra le varie divisioni di un'organizzazione di sicurezza. Un'assunzione comune a tutti e due i modelli è quella della dipendenza lineare tra le risorse di sicurezza e le divisioni, e

le vulnerabilità presenti in queste divisioni. Nel modello cooperativo vengono introdotte due matrici, una di influenza positiva e l'altra di influenza negativa. Queste matrici sono basate sulle omonime matrici del modello non-cooperativo e rappresentano le dipendenze tra le risorse di sicurezza e le divisioni, la prima, e le dipendenze tra le vulnerabilità e le divisioni, la seconda. Per poter catturare l'effetto della formazione di una coalizione, qualsiasi coppia di divisioni che si trovano all'interno della stessa coalizione avrà un aumento dell'effetto positivo e una diminuzione di quello negativo rispetto al valore di questi due parametri nel caso le due divisioni non siano nella stessa coalizione. Inoltre per poter catturare il costo della coordinazione all'interno di una coalizione è stata introdotta una funzione costo. Una delle conclusioni più interessanti presentate dagli autori è quella riguardante il gioco cooperativo in cui due coalizioni, formate da più di due divisioni ciascuna, formeranno una nuova coalizione se e soltanto se la funzione costo sarà sotto un certo valore limite.

3.3.2 Modelli di giochi non-cooperativi

Modelli di giochi statici

Tutti i giochi statici sono giochi one-shot di informazione imperfetta, di conseguenza i modelli di giochi statici hanno solo due sotto-classi: giochi statici con informazione completa e giochi statici con informazione incompleta. Nel contesto della Sicurezza su Reti, i modelli di giochi statici con informazione completa vengono usati per analizzare gli scenari in cui sono considerate solo le interazioni tra attaccanti e difensori; nel caso, però, in cui i difensori non sono sempre capaci di distinguere se un determinato nodo è un attaccante o meno, vengono considerate anche le interazioni tra difensori e nodi regolari, di conseguenza i giochi vengono modellati come giochi statici a informazione incompleta. La soluzione ai giochi statici con informazione completa è l'Equilibrio di Nash [6], e la soluzione ai giochi statici con informazione incompleta è l'Equilibrio Bayesiano di Nash [6].

Giochi statici con informazione completa

Il modello non-cooperativo e multi-giocatore presentato in [24] che affronta il rischio di gestione di molteplici divisioni di un'organizzazione di sicurezza, ricade in questa categoria di giochi. Il modello si basa sull'assunzione della dipendenza lineare tra le risorse di sicurezza nelle divisioni e tra le vulnerabilità nelle stesse divisioni, con le dipendenze rappresentate da due matrici: una matrice di influenza positiva e una matrice di influenza negativa. Il guadagno di ogni divisione è la differenza tra la funzione costo del beneficio e quella della minaccia, la prima prende in input la matrice di influenza positiva e le risorse di sicurezza delle divisioni, mentre la seconda prende in

input la matrice di influenza negativa e la vulnerabilità delle divisioni.

Giochi statici con informazione incompleta

Gli autori in [16] hanno proposto un modello di gioco Bayesiano con due giocatori per il problema di una rete con attaccanti e difensori, nel caso in cui i difensori non abbiano informazioni sufficienti per verificare un potenziale attaccante. Questo modello specifica il tipo del potenziale attaccante come «buono,cattivo» e le funzioni di utilità del difensore e dell'attaccante, nel caso in cui sono presenti anche le loro possibili azioni e il tipo dell'attaccante. L'autore conclude affermando che il loro Equilibrio di Nash massimizza l'utilità attesa.

Modelli di giochi dinamici

Nel caso dei modelli di giochi statici applicati alla Sicurezza su Reti, vengono considerate solo le interazioni one-shot tra attaccanti e difensori. D'altra parte nei modelli di giochi dinamici viene considerato un processo multi-livello di interazioni, in cui ad ogni livello gli attaccanti e i difensori eseguono le proprie mosse in risposta alla cronologia dei risultati ottenuti fino a quel momento. I modelli di giochi dinamici applicati alla Sicurezza su Reti sono formati da quattro sotto-classi: quelli con informazione perfetta e completa, quelli con informazione imperfetta e completa, quelli con informazione perfetta e incompleta e quelli con informazione imperfetta e incompleta. Nei modelli con informazione completa vengono considerate solo le interazioni tra attaccanti e difensori con il presupposto che i difensori sono capaci di discriminare gli attaccanti dagli utenti regolari, gli scenari in cui questo presupposto viene a mancare vengono, invece, chiamati a informazione incompleta. Giochi dinamici con informazione perfetta sono tali che in ogni livello di un gioco, i giocatori eseguono le azioni nel loro turno di gioco e, nel momento in cui le eseguono sono a conoscenza della storia passata delle azioni proprie e degli altri giocatori. Altri giochi dinamici in cui i giocatori o eseguono le proprie azioni contemporaneamente o hanno poca informazione sulla storia passata delle azioni eseguite, vengono chiamati giochi a informazione imperfetta. Nella Sicurezza su Reti alcuni aspetti di questi modelli mutano in base a fattori casuali, infatti è possibile che un sistema difensore non si trovi nel suo stato regolare anche se questo non è causato da un attaccante.

Giochi dinamici con informazione completa e perfetta

In [10] gli autori propongono un modello di un gioco con due giocatori a informazione completa e perfetta. Questo gioco è chiamato Gioco di Stackelberg per il rilevamento delle intrusioni in una rete. Nel modello di gioco di Stackelberg gli autori considerano sia il caso in cui è l'attaccante a fare la prima mossa e viene seguito dalla reazione del difensore, sia il caso in cui i due giocatori si scambiano di ruolo. Ogni azione nell'insieme delle azioni di un giocatore è etichettata come azione di attacco o di difesa, e ognuna ha una certa probabilità di essere eseguita sul bersaglio dell'attacco. L'Equilibrio di Nash è usato in tutti e due i casi per stabilire qual'è il ruolo migliore per ogni giocatore. L'Equilibrio di Nash per un gioco di Stackelberg è chiamato anche Equilibrio di Stackelberg.

Giochi dinamici con informazione completa e imperfetta

Gli autori di [8] hanno rappresentato il gioco della sicurezza come un gioco stocastico con due giocatori a somma zero, cioè tra attaccante e difensore. Inoltre gli autori hanno affermato che, anche senza considerare le interazioni tra attaccante e difensore, lo stato del sistema è soggetto a cambiamenti dovuti al suo regolare utilizzo. La matrice di transizione da uno stato all'altro tiene conto, quindi, non solo delle azioni eseguite dai giocatori ma anche degli effetti del normale uso del sistema. Basandosi su quest'idea, il gioco di sicurezza è modellato come segue:

- 1) Identificazione degli elementi del gioco, cioè gli stati che sono vulnerabili agli attacchi.
- 2) Costruzione dell'insieme delle azioni che rappresentano i possibili metodi di attacco e difesa dei due giocatori all'interno del gioco. L'insieme degli stati del gioco stocastico contiene i possibili stati del sistema. L'insieme delle azioni dell'attaccante e del difensore dipendono dallo stato del sistema.
- 3) Per ogni coppia di azioni del difensore e dell'attaccante, determinare le probabilità di transizione da uno stato a un altro.
- 4) Determinare la funzione di guadagno in ogni stato. In ogni stato e per ogni coppia di azioni dei giocatori, la funzione di guadagno dell'attaccante è: un valore fissato sommato al massimo guadagno atteso nella mossa successiva in caso l'azione di attacco abbia successo e ci sia una transizione ad un altro stato del gioco, oppure solo il valore fissato.

Dalle funzioni di guadagno, la dinamica del gioco può essere descritta come segue: l'interazione tra attaccante e difensore nel gioco può cominciare solo

in uno stato vulnerabile; se l'attaccante sceglie di non attaccare o il difensore risponde all'attacco, il gioco termina; se l'attacco ha successo e si ha una transizione in uno stato diverso da quelli vulnerabili, il gioco termina; infine se l'attacco ha successo e si ha una transizione a un altro stato vulnerabile del gioco, il gioco prosegue. La soluzione del gioco è un Equilibrio di Nash per ogni stato del gioco, ma è difficile da ottenere perché la funzione di guadagno non è definita in maniera esplicita.

Giochi dinamici con informazione incompleta e perfetta

Il lavoro descritto in [2] modella la rilevazione delle intrusioni nelle reti wireless ad hoc come un gioco di segnalazione con due giocatori. Nel modello il difensore non ha tutte le informazioni per determinare il tipo del suo avversario, che può essere un attaccante o un nodo regolare. Le azioni possibili per il difensore sono quelle di difendere o di non fare nulla, mentre il suo avversario può attaccare attivamente o agire passivamente se il nodo è un attaccante; d'altra parte, se è un nodo regolare, può attaccare passivamente o agire normalmente. Le strategie ottimali del gioco sono considerate tramite un Equilibrio Bayesiano per un gioco base di segnalazione.

Giochi dinamici con informazione incompleta e imperfetta

In [26], gli autori hanno proposto un gioco Bayesiano per due giocatori a più livelli per modellare il gioco di sicurezza in cui i giocatori hanno informazioni incomplete. La soluzione di quel modello di gioco può essere ottenuta nella maniera seguente: ad ogni stato del gioco, le strategie ottimali dei giocatori per quello stato sono ottenute basandosi sulle supposizioni sul tipo degli avversari; alla fine del turno di azione, ogni giocatore aggiorna la propria supposizione sul tipo del giocatore avversario, basandosi sulle strategie ottimali attuali, la sua supposizione corrente e la storia delle azioni osservate dell'avversario. Per ottenere la soluzione del modello di gioco così strutturato bisogna usare l'Equilibrio Bayesiano Perfetto.

3.3.3 Discussione sulla modellazione dei giochi

Gli studi trattati mostrano che la modellazione della Sicurezza su Reti come gioco è ancora uno schema ad hoc che dipende dallo scenario del problema specifico. I limiti dei modelli di gioco esistenti si possono generalizzare in:

- 1) Mancanza di scalabilità. Come è stato mostrato, la maggior parte dei modelli di giochi per la sicurezza sono giochi a due giocatori; per

lo scenario con più di due giocatori, il modello di gioco usato considera l'insieme degli attaccanti come un unico giocatore e così anche l'insieme dei difensori.

- 2) Il modello statico non è molto realistico nei casi in cui le interazioni tra attaccanti e difensori sono una serie di eventi.
- 3) Il modello stocastico assume sempre che, in ogni stato, il difensore e l'attaccante sono in grado di riconoscere lo stato del sistema senza errori, cosa che non risulta vera in molti casi reali.
- 4) I modelli stocastici assumono anche che gli stati del sistema sono finiti; in realtà gli stati di un sistema sembrano infiniti, anche se in alcuni modelli lo spazio continuo degli stati è stato suddiviso in parti finite.
- 5) Alcuni dei modelli stocastici non sono molto realistici perché assumono che il gioco tra l'attaccante e il difensore è un gioco a somma-zero.

Capitolo 4

Rilevazione dinamica della Sicurezza di Rete basata sulla Teoria dei Giochi Stocastica

Negli ultimi anni la Teoria dei Giochi Stocastica è stata largamente usata nel campo della Sicurezza su Reti [9, 17]. In questo esempio viene usato un gioco stocastico per modellare una situazione di Sicurezza su Reti che aiuta a raggiungere l'obiettivo di ottenere una consapevolezza dinamica quantitativa. Viene costruito un framework di rete, con una parte attaccante e un'altra difendente, e che contiene i comportamenti di tutti e due come mostrato in figura 4.1.

Questo esempio pratico viene affrontato con maggior dettaglio nel lavoro [11] a cui si rimanda per ulteriori approfondimenti.

La figura offre una visione intuitiva sulle interazioni tra gli elementi di gioco e le varie entità della rete di sicurezza. Il sistema di rete con il software di sicurezza installato e le intrusioni sono modellate come i giocatori del gioco, le azioni intraprese dall'attaccante e dal difensore durante l'esecuzione del sistema sono corrispondono alle strategie dei giocatori, infine lo stato del sistema di sicurezza è rappresentato dagli stati sicuri presenti nei punti di Equilibrio di Nash.

Per poter rappresentare al meglio la situazione della rete di sicurezza, bisogna definire le metriche di sicurezza dei servizi offerti dalla rete. Supponiamo ci siano quattro servizi di rete attivi, in particolare WWW, HTTP, FTP e NFS. I loro stati insieme formano lo stato della rete di sicurezza. Le metriche di valutazione di questi servizi sono mostrate in tabella 4.2.

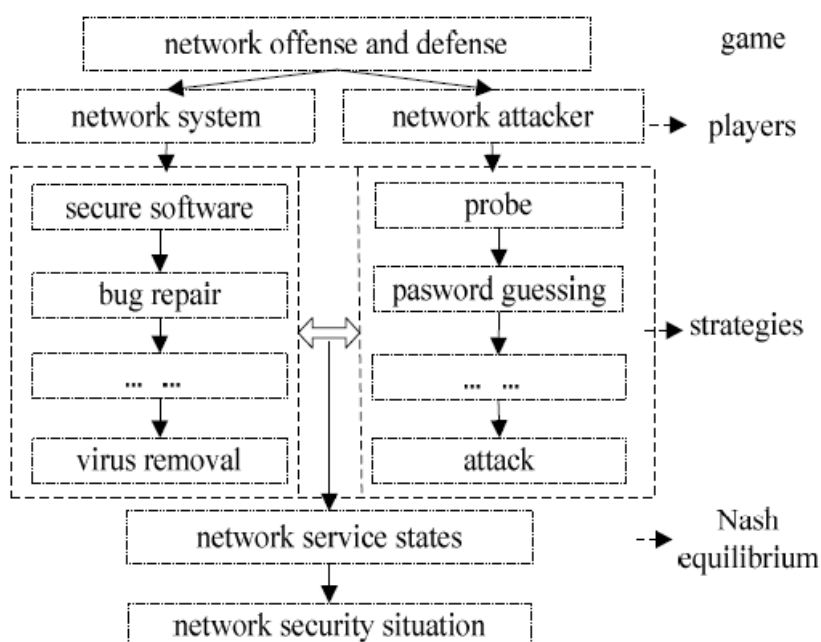


Figura 4.1: Framework della rete con attaccante e difensore

Network Service	Metrics	Result
<i>WWW</i>	service grades	NSS: network security situation
<i>HTTP</i>	availability	
<i>FTP</i>	response time	
<i>NFS</i>	response rate	
	inbound connections	
	outbound connections	
	error connection rate	
	average flow speed	
	flag tags	

Figura 4.2: Metriche dello stato dei servizi della rete

4.1 Definizione del modello

Di seguito verrà introdotto il modello formale di un gioco stocastico, e successivamente verranno specificati meglio i parametri di tale modello.

Un modello di gioco stocastico con due giocatori è, formalmente, una tupla $(S, A^1, A^2, P, U^1, U^2, \beta)$, dove $S = \{s_1, s_2, \dots, s_N\}$ è l'insieme degli stati e $A^k = \{\alpha_1^k, \alpha_2^k, \dots, \alpha_{M^k}^k\}$, $k = 1, 2$, $M^k = |A^k|$ è l'insieme delle azioni del giocatore k -esimo. L'insieme delle azioni del giocatore k nello stato s è un sottoinsieme di A^k , $P : S \times A_1 \times A_2 \times S \rightarrow [0, 1]$ è la probabilità di transizione di stato. Il guadagno di un giocatore k in uno stato mentre esegue azioni viene definito come U^k . Infine β è il fattore di moltiplicazione del guadagno futuro, questo fattore può essere spiegato come segue: nello stato corrente, una transizione di stato ha il suo guadagno pieno, ma il guadagno nell'effettuare un'altra transizione oltre la prima è β volte il guadagno iniziale.

Per poter ottenere dei risultati quantitativi, il gioco stocastico deve essere parametrizzato. Di seguito mostriamo i passi per effettuare questa parametrizzazione.

Passo 1: gli stati della rete di sicurezza sono considerati come gli insiemi degli stati del gioco. Da questo possiamo dire che lo stato della rete di sicurezza al tempo t è rappresentato dagli stati dei servizi di rete, in particolare $S_t = \{S_{WWW}, S_{HTTP}, S_{FTP}, S_{NFS}, S_{attacker}\}$. Mentre lo stato di ogni servizio di rete viene definito come $S_X = \{normal, attacked, hacked\}$. Lo stato *normal* è quello in cui vengono eseguite le normali operazioni del servizio di rete senza nessun attacco, lo stato *attacked* riflette una deviazione dallo stato normale di funzionamento, ma è sempre una situazione interna al servizio e quindi non visibile dall'esterno. Lo stato *hacked* può portare a un'interruzione del servizio di rete, e questo va in conflitto con la funzionalità predefinita del servizio. Lo stato dell'attaccante viene visto come parte dello stato della rete, e può essere definito come $S_{attacker} = \{detected, undetected\}$, questo aiuta a ridefinire il livello di sicurezza totale della rete.

Passo 2: le azioni sono considerate le strategie del gioco. L'insieme delle azioni per ogni giocatore contiene tutte le possibili azioni di attacco che quel giocatore può eseguire, e ogni giocatore può effettuare solo una delle azioni dall'insieme delle azioni. Supponiamo che ogni giocatore può effettuare una sola strategia alla volta, di conseguenza le azioni dei giocatori formano una situazione di gioco, e le coppie di azioni fanno in modo che il sistema transiti da uno stato all'altro in maniera probabilistica. Supponiamo che le azioni un giocatore siano le seguenti:

per un attaccante si ha $A^1 = \{attack, i^{th} network service, continue_attacking, waiting\}$, dove l' i -esimo servizio di rete è numerato 1, 2, 3 e 4 per indicare corrispettivamente i servizi WWW, HTTP, FTP e NFS. Il parametro *continue_attacking* sta a indicare che l'attaccante continua ad effettuare attacchi anche dopo che la sua invasione del servizio ha avuto successo, ad esempio per modificare una pagina internet o rubare dati dopo essere riuscito ad accedere al web server del servizio.

Per il difensore invece si ha $A^2 = \{reboot i^{th} network service, virus - removal, secure software - install, infected_account removal\}$.

Passo 3: probabilità di transizione di stato. In un modello di gioco for-

male, la probabilità di transizione di stato è una funzione che considera le azioni di tutti e due i giocatori. Nel caso in esame, invece, le probabilità di transizione degli stati del sistema sono state scelte principalmente in base all'esperienza di esperti del campo.

Passo 4: costi e guadagno. Per poter modellare le motivazioni dell'attaccante verranno usati i concetti di costo e guadagno. A ogni giocatore viene assegnato un valore relativo a ogni azione, che rappresenta il guadagno ottenuto nell'eseguire quella azione. Per quantificare il costo e il guadagno di ogni giocatore vengono usate le metriche relative al servizio di rete. I concetti di costo e guadagno sono generici, e possono essere specificati a seconda dell'ambiente di utilizzo [9, 17]. In contrasto a quello che viene detto in [9, 17], nell'esempio trattato viene sfruttata l'influenza della sistema di rete, ovvero lo stato dei servizi di rete, per definire la funzione di guadagno di ogni giocatore. In particolare questa funzione di guadagno viene definita come segue:

Guadagno dell'attaccante

$$U^2(\alpha_i^1, \alpha_j^2) = \beta \cdot w(\alpha_j^2) \cdot \epsilon_j \cdot \gamma_j \cdot M'_{jt} - a_0 \quad (4.1)$$

Guadagno del difensore

$$U^1(\alpha_i^1, \alpha_j^2) = \gamma_j \cdot M_{jt} - (\beta \cdot w(\alpha_j^2) \cdot \epsilon_j \cdot \gamma_j \cdot M'_{jt} + d_0) \quad (4.2)$$

Dove $\beta = 1 - M'_{jt}/M_{jt}$ è il tasso di successo degli attacchi, M_{jt} e M'_{jt} sono i tempi di risposta del servizio prima e dopo l'attacco; $w(\alpha^2) \in [0, 1]$ è la probabilità di continuare gli attacchi dopo che un'invasione ha avuto successo; ϵ_j con $j = 1, 2, 3$ è la percentuale di attacchi che mirando la servizio i-esimo; γ_j indica l'importanza del servizio di rete e viene definita in base al numero di richieste effettuate al servizio dagli utenti; a_0 è il costo medio di un attacco per un attaccante, e viene definito come:

$$a_0 = \frac{\sum_t \sum_j (M_{jt} - M'_{jt})}{n} \quad (4.3)$$

dove n sono i tempi di attacco. Infine d_0 è il costo medio di difesa, e viene definito come:

$$d_0 = \frac{\sum_j (M_{jt} - M'_{jt})}{t} \quad (4.4)$$

dove t indica il tempo dell'attacco.

4.2 Simulazione del modello

La situazione della sicurezza di una rete viene osservata attraverso le metriche che descrivono lo stato dei servizi della rete, in punti di Equilibrio di Nash. L'ambiente di simulazione dell'esperimento eseguito è definito come

segue: quattro computer usati rispettivamente come server WWW, server HTTP, server FTP e server NFS. Questi computer sono configurati nello stesso modo dei computer usati dagli utenti. Viene usato anche uno dei migliori software di testing di prestazioni web, chiamato LoadRunner. Questo software viene sfruttato sia per simulare le richieste degli utenti ai servizi di rete, sia per simulare gli attaccanti che vogliono attaccare la rete.

I parametri usati per definire lo stato dei servizi di rete sono quantificati come segue: LoadRunner è usato per inizializzare 200 utenti che effettuano richieste ai servizi di rete. Il numero di connessioni esistenti ai servizi di rete in ogni momento è mostrato nella tabella 4.3, dove sono visualizzate le richieste di tutti e quattro i servizi di rete.

Time	2	4	6	8	10	12	14	16	18	20
WWW	37	105	210	340	524	725	976	1266	1546	1580
HTTP	10	52	128	236	368	528	726	950	1150	1173
FTP	4	32	80	155	240	358	485	627	764	781
NFS	9	27	51	34	80	135	198	270	340	347

Figura 4.3: Numero delle connessioni ai servizi di rete

Considerando i dati in tabella 4.3 definiamo la variabile di accesso come la somma delle connessioni per secondo, possiamo quindi calcolare i seguenti valori $access(WWW) = 79 \text{ times/s}$; $access(HTTP) = 58 \text{ times/s}$; $access(FTP) = 39 \text{ times/s}$; $access(NFS) = 17 \text{ times/s}$. Grazie a questi dati è possibile definire il vettore di importanza in questo esperimento, cioè $\{\gamma_{WWW}, \gamma_{HTTP}, \gamma_{FTP}, \gamma_{NFS}\} = \{0.80, 0.60, 0.40, 0.20\}$.

Gli attacchi a un sistema di rete possono influenzare il normale funzionamento dei servizi di tale rete, e questo si può manifestare, ad esempio, in un ritardo nella risposta da parte di un servizio di rete. LoadRunner viene usato per simulare gli attaccanti che attaccano i server della rete, la durata dell'attacco è di 30 secondi. L'esperimento ha visto due attaccanti separati che attaccavano i server a ritmi differenti, cioè eseguivano prima 80 poi 60, poi 40 e infine 20 attacchi al secondo. Durante l'esperimento viene monitorato lo stato del sistema di rete, i risultati sono mostrati in tabella 4.4.

Dai risultati si evince che il tasso di risposta dei servizi decresce all'aumentare degli attacchi. Col passare del tempo, le risorse del sistema vengono esaurite, e quindi il sistema non ha potuto più rispondere alle richieste

Time	0	3	6	9	12	15	18	21	24	27	30
WWW	80	76	71	60	54	50	46	40	20	3	0
HTTP	60	52	47	43	35	26	24	19	13	2	0
FTP	40	37	30	28	26	20	16	10	4	1	0
NFS	20	16	13	12	12	7	6	1	1	1	0

Figura 4.4: Numero delle richieste soddisfatte dai servizi di rete

di servizio. Grazie all'esperimento è possibile quantificare il guadagno dei giocatori. Sfruttando i dati della tabella 4.4 possiamo calcolare il valore approssimativo di d_0 e a_0 , i valori finali di questi parametri sono: $d_0 = 3.1$ e $a_0 = 4.7$, e il tasso di successo degli attacchi è $\beta = 0.47$.

Nella tabella 4.5 sono mostrati i punti di Equilibrio di Nash del gioco, questi punti sono stati calcolati utilizzando la programmazione non linear di Matlab.

Service States	Atk's Strategy	Def's Strategy
normal	{0.00, 0.00, 1.00}	{0.00, 0.00, 1.00}
http_attacked	{0.25, 0.40, 0.35}	{0.00, 0.30, 0.70}
http_hacked	{0.40, 0.50, 0.10}	{0.20, 0.40, 0.40}
ftp_attacked	{0.25, 0.30, 0.45}	{0.00, 0.30, 0.70}
ftp_hacked	{0.40, 0.50, 0.10}	{0.20, 0.50, 0.30}
nfs_attacked	{0.25, 0.50, 0.25}	{0.00, 0.40, 0.60}
nfs_hacked	{0.25, 0.60, 0.15}	{0.20, 0.50, 0.30}
web_defaced	{0.25, 0.60, 0.15}	{0.00, 0.40, 0.60}
web_sniffer	{0.20, 0.20, 0.60}	{0.00, 1.00, 0.00}
ins_antivirus	{0.00, 0.20, 0.80}	{0.00, 0.00, 1.00}
data_stolen	{0.00, 0.50, 0.50}	{0.00, 0.60, 0.40}
web_hacked	{0.25, 0.60, 0.15}	{0.30, 0.40, 0.30}
service_reboot	{0.10, 0.00, 0.90}	{0.50, 0.30, 0.20}

Figura 4.5: Lista dei punti di Equilibrio di Nash

Dalla tabella è possibile vedere le strategie dell'attaccante e del difensore nei punti di Equilibrio di Nash. Per l'attaccante il vettore della strategia è $\{ attack, i^{th} network service, continue_attacking, waiting \}$ mentre per il difensore è $\{ reboot i^{th} network service, virus-removal, secure software-install, infected_account removal \}$. I valori di questi vettori corrispondono

alle probabilità che le queste azioni vengano eseguite.

Alla fine di questo esperimento i risultati vengono mostrati, ad esempio, all'amministratore di rete sotto forma di grafici. I grafici mostrano le curve che rappresentano il tempo medio di risposta, la velocità media di flusso, e il tasso di errore nella connessione nei punti di Equilibrio di Nash, in cui nessun giocatore ha interesse nel cambiare la propria strategia. In particolare le figure 4.6 e 4.7 mostrano la curva del tempo medio di risposta e la curva del flusso medio in un determinato punto di Equilibrio di Nash. Ci sono però altre metriche che descrivono la situazione di un sistema di servizi come quello illustrato in questo esempio. I due grafici mostrano l'evolversi dello stato della rete di sicurezza.

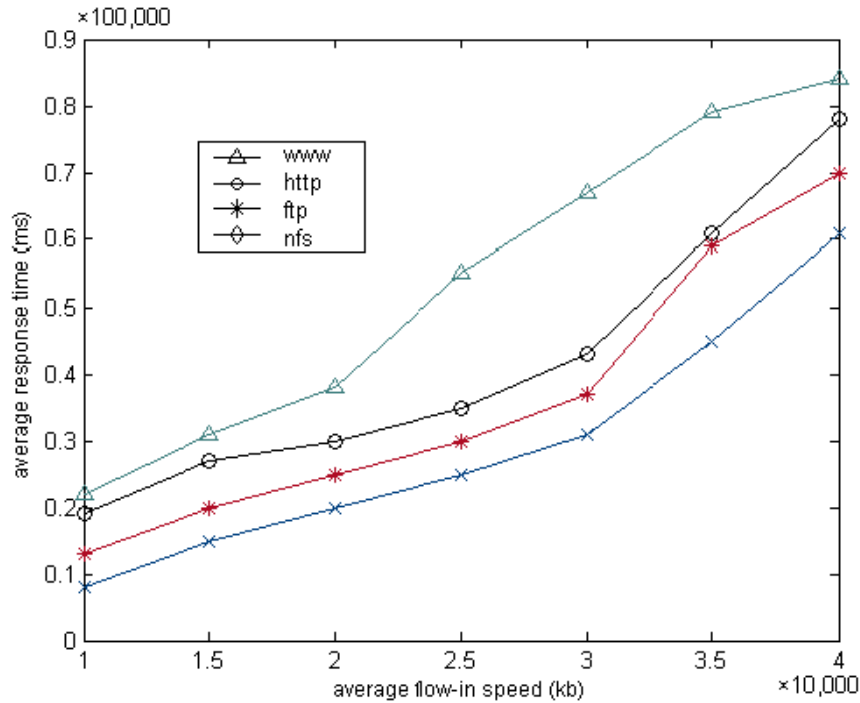


Figura 4.6: Curva del tempo medio di risposta

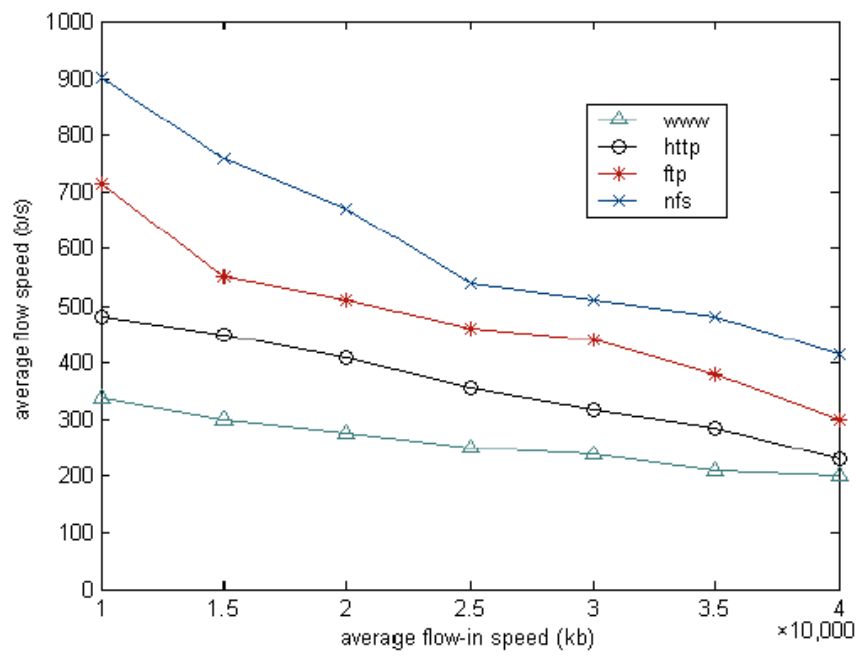


Figura 4.7: Curva del flusso medio

Capitolo 5

Conclusioni

Questo lavoro si propone di essere un punto di riflessione e una classificazione dei vari approcci della Teoria dei Giochi alla Sicurezza su Reti. Nonostante i loro limiti, gli approcci basati sulla Teoria dei Giochi sono degli strumenti potenti per la risoluzione di problemi legati alla Sicurezza su Reti, quest'ultima dovrebbe indirizzare la ricerca sullo studio di nuovi approcci basati sulla Teoria dei Giochi. La classificazione dei giochi e dei modelli proposta dovrebbe sottostare a cambiamenti, visto che, in continuazione, nuovi approcci diventano disponibili. Da questo lavoro i lettori dovrebbero acquisire una panoramica sufficientemente ampia sui vari possibili approcci basati sulla Teoria dei Giochi e sulle possibili direzioni da prendere nel campo della Sicurezza su Reti.

L'esempio descritto in dettaglio mostra uno di questi approcci applicato ad un caso reale, mettendo in evidenza i pregi e i difetti del metodo usato.

In conclusione la Teoria dei Giochi si applica in maniera quasi diretta alle problematiche riguardanti la Sicurezza su Reti tramite numerosi modelli di gioco che possono modellare gli scenari più svariati.

In futuro una direzione di ricerca interessante in questo campo potrebbe essere quella di rendere gli approcci basati sulla Teoria dei Giochi sistematici e modulari in modo da poter suddividere grossi problemi in sotto-problemi di taglia inferiore, risolverli usando uno dei modelli di gioco, e ricomporli, creando così dei modelli di gioco aggregati che riescano a rappresentare scenari ancor più complessi e grandi.

Capitolo 6

Bibliografia

- [1] *Security measurement – white paper.* <http://www.psmc.com/Downloads/TechnologyPapers/SecurityWhitePaperv3.0.pdf>.
- [2] J. Park A. Patcha. *A game theoretic approach to modeling intrusion detection in mobile ad hoc networks.* IEEE workshop on Information Assurance and Security, 2004.
- [3] John A. Buzacot. *Markov approach to finding failure times of repairable systems*, volume R - 19. IEEE Trans. Reliab, 1970.
- [4] Security Focus Bugtraq Vulnerability Notification Database. *Security Focus*. 2009. <http://www.securityfocus.com/archive>.
- [5] C. H. Papadimitriou E. Koutsoupias. *Worst-case equilibria.* Annual Symposium on Theoretical Aspects of Computer Science, 1999.
- [6] R. Gibbons. *Game Theory for Applied Economists.* Princeton University Press, 1992.
- [7] J. V. E. Molsa J. Jormakka. *Modelling information warfare as a game*, volume 4. Journal of Information Warfare, 2005.
- [8] B. Helvik K. Sallhammar, S. Knapskog. *Using stochastic game theory to compute the expected behavior of attackers.* International Symposium on Applications and the Internet Workshops, 2005.
- [9] Jeannette Wing Kong-wei Lye. *Game Strategies in Network Security*, volume 4. Proceedings of the Workshop on Foundations of Computer Security, 2002.
- [10] J. Leneutre L. Chen. *A game theoretical framework on intrusion detection in heterogeneous networks*, volume 4. IEEE Trans. Inf. Forens. Security, 2009.

- [11] W. Huiqiang L. Ying, L. Bingyang. *Dynamic Awareness of Network Security Situation Based on Stochastic Game Theory*. Natural Science Foundation of Harbin, 2009.
- [12] T. Basar M. Bloem, T. Alpcan. *Intrusion response as a resource allocation problem*. IEEE Conference on Decision and Control, 2006.
- [13] A. Rubinstein M. J. Osborne. *A course in game theory*. MIT Press, 1994.
- [14] R. Poovendran M. Li, I. Koutsopoulos. *Optimal jamming attacks and network defense policies in wireless sensor networks*. IEEE International Conference on Computer Communications, 2007.
- [15] G. Owen. *Game Theory*. Academic Press, 3rd edition, 2001.
- [16] M. Yu P. Liu, W. Zang. *Incentive-based modeling and inference of attacker intent, objectives, and strategies*, volume 8. ACM Trans. Information and System Security (TISSEC), 2005.
- [17] Wanyu Zang Peng Liu. *Incentive-based Modeling and Inference of Attacker Intent, Objectives and Strategies*, volume 8. Proceeding of the 10th ACM Conference on Computer and Communication Security, 2003.
- [18] P. Mell. R. Bace. *Intrusion detection systems*. NIST Special Publication on Intrusion Detection Systems. <http://www.snort.org/docs/nist-ids.pdf>.
- [19] A. Ott O. S. Saydjari S. N. Hamilton, W. L. Miller. *The role of game theory in information warfare*. 4th information survivability workshop, 2002. <http://www.cert.org/research/isw/isw2001/papers/index.html>.
- [20] T. Baser T. Alpcan. *A game theoretic analysis of intrusion detection in access control systems*, volume 2. IEEE Conference on Decision and Control, 2004.
- [21] T. Baser T. Alpcan. *An intrusion detection game with limited observations*. 12th Int. Symp. on Dynamic Games and Applications, 2006. <http://www.tansu.alpcan.org/papers/isdg06.pdf>.
- [22] United States Computer Emergency Readiness Team. *US-CERT*. 2009. <http://www.us-cert.gov>.
- [23] H. Wang C. Zheng Y. Ji W. He, C. Xia. *A game theoretical attack-defense model oriented to network security risk assessment*. International Conference on Computer Science and Software Engineering, 2008.

- [24] T. Basar A. Hjørungnes W. Saad, T. Alpcan. *Coalitional game theory for security risk management*. 5th Intl. Conf. on Internet Monitoring and Protection, 2010.
- [25] Y.Xiao X. Liang. *Game Theory for Network Security*, volume 15. IEE Communications Surveys and Tutorials, 2013.
- [26] H. Man Y. Liu, C. Comaniciu. *A bayesian game approach for intrusion detection in wireless ad hoc networks*. Proc. 2006 workshop on Game theory for communications and networks, 2006.
- [27] K. Ghaboosi J. Zhang H. Deng Y. Zhang, Y. Xiao. *A Survey of Cyber Crimes*, volume 5. April 2012. Wiley Journal of Security and Communication Networks.
- [28] D. Zamboni. *Using internal sensors for computer intrusion detection*. Ph.D. dissertation of Purdue University, August 2001.