Università degli Studi di Padova

Dipartimento di Ingegneria dell' Informazione

Laurea Magistrale in Ingegneria delle Telecomunicazioni

Analisi dell'equilibrio nell'applicazione della teoria dei giochi alle strategie di friendly jamming

Laureando

Andrea Baessato

Relatore

Leonardo Badia

8 Luglio 2019

Anno accademico 2018/2019

Questo mio lavoro è dedicato

a tutti quelli che mi hanno sostenuto e

rincuorato lungo tutto questo arduo percorso.

Grazie

Stefania, Carla,

Gabriele, Lisa

Amici tutti

e Yasu.

e soprattutto per chi non c'è

ma è come se fosse sempre con me

Papà e Nonno.

Sommario

Le trasmissioni su reti wireless sono, per loro natura, vulnerabili a diversi tipi di intercettazioni, manomissioni ed interruzioni. Tali problematiche sono inputabili ad attori esterni alla rete stessa ed agiscono, nella maggior parte delle volte, al primo layer del sistema ISO/OSI, ovvero al layer fisico, dove operano i protocolli regolanti i parametri elettromagnetici di una trasmissione tra due nodi e si occupano principalmente della forma e della tensione del segnale, stabilendo, per esempio, le soglie di transizione per i valori logici dei bit trasmessi. Per far fronte alle emergenti sfide riguardanti la sicurezza del layer fisico di trasmissioni wireless implementate in nuove tecnologie, come *WSN* o reti *IoT*, in questo elaborato viene analizzato l'utilizzo del meccanismo denominato *friendly jamming*, il quale, sfruttando nodi addizionali detti *jammer* per la produzione di un segnale d'interferenza artificiale, riesce a evitare eventuali intrusioni da parte di un nodo malevolo e a prevenire eventuali trasmissioni non autorizzate. L'approccio utilizzato per l'analisi è quello della *teoria dei giochi* e punta allo studio del comportamento di jammer ai quali viene messo in opposizione un nodo malevolo *razionale* che tenta di inserirsi nelle trasmissioni di una rete wireless. Vengono analizzate sia la situazione dove al nodo malevolo viene contrapposto un singolo jammer, sia la situazione ove agiscono due jammer consapevoli della presenza l'uno dell'altro.
Con l'analisi dell'andamento del payoff per ogni attore presente in questo modello si cercheranno di ottenere delle *regole empiriche* riguardanti i punti d'equilibrio per poi poter giungere, infine, a conclusioni utili per l'implementazione di nodi funzionanti come *friendly jammers*.

Indice

Capitolo 1

Introduzione

1.1 Motivazioni

È oramai immenso il numero delle tecnologie che al giorno d'oggi sfrutta sistemi di comunicazione wireless ma la crescita di questo tipo di implementazioni non accenna a diminuire.

Le attuali reti dati cellulari risultano essere in grado di supportare un numero di dispositivi interconnessi tra loro contemporaneamente nell'ordine del miliardo, dato comunque che è accreditato dover subire una crescita esponenziale nei prossimi anni [1].

Le nuove implementazioni di tecnologie riguardati l'IoT ed, più nello specifico, il sempre maggior impiego di reti sensoristiche utilizzate nei più disparati campi [2] (dal *militare* [3], dove sono utilizzate per sorveglianza del campo di battaglia e monitoraggio di forze alleate, equipaggiamenti o munizioni, al *socio-sanitario* [4], dove i sensori sono rivolti a fornire un'interfaccia per il

monitoraggio di dati fisiologici riguardanti il paziente, passando per le applicazioni di *domotica domestica* e *commerciale* [5]) ha portato all'attenzione di tutti un problema di tipo progettuale/realizzativo.

Risulta necessario infatti aumentare l'efficienza spettrale, ovvero il rapporto tra velocità di trasmissione e la banda utilizzata, degli attuali sistemi di comunicazione poiché questo approccio è emerso essere l'unico in grado di garantire la trasmissione di una quantità di mole di dati molto grande senza dover investire sull'allargamento della banda effettiva.

Tuttavia, nonostante fosse inizialmente ritenuto di minor importanza rispetto al problema di "sostentamento" di una tale quantità di dati, un altro aspetto delle comunicazioni wireless sta attualmente attirando su di sé l'attenzione di chi si occupa di realizzazione e di gestione di tali reti: *la sicurezza* [6].

Diretta conseguenza di questo sempre maggior livello di connettività, condizione strettamente legata alle tecnologie IoT, e della sempre maggior quantità di servizi accessibili dai nostri dispositivi attraverso una semplice connessione dati (vedasi *internet banking* [7] e *remote control* di sistemi sensibili [8]) è la sempre più grande quantità di informazioni e di dati sensibili che sono potenzialmente disponibili attraverso l'accesso a reti wireless. Questo ha indirettamente portato a un aumento dell'interesse da parte di malintenzionati verso queste infrastrutture e sulla possibilità di carpirne falle o vulnerabilità in grado di garantire accesso a tali informazioni o, nel peggiore dei casi, nel minare completamente il funzionamento della rete stessa. [9]

Tradizionalmente, questo compito, è sempre stato svolto attraverso algoritmi implementati ai livelli superiori del modello ISO/OSI: l'utilizzo di metodi di crittografia (tra cui la crittografia asimmetrica *RSA* [10] e la cifratura a bloc-

chi *AES* [10]) oppure l'utilizzo di una comunicazione cooperativa [11], sono tecniche che, nonostante risultino essere molto efficaci nell'impedire all'eventuale intruso di leggere l'informazione nella sua forma "reale", permettono comunque a quest'ultimo di ricevere il messaggio (il quale risulta essere in una forma diversa, criptato per l'appunto) e di poter successivamente svolgere un lavoro di decriptazione per ottenere il messaggio originale. Le sempre maggiori capacità di calcolo disponibili sul mercato hanno inoltre spinto verso un aumento della complessità dei codici di codifica con l'obiettivo di rendere molto difficile la decrittazione [12]; tali algoritmi però, oltre che inficiare sull'effettivo *throughput* della trasmissione, richiedono, per l'appunto, anche una maggiore complessità computazionale sia per il malintenzionato, ma anche per il trasmettitore ed il ricevitore in gioco [12].

L'approccio alla sicurezza tramite il layer fisico ha quindi ricevuto molte attenzioni poiché considerato un metodo potenzialmente molto efficace per proteggere le comunicazioni che avvengono in una rete wireless senza la necessità di implementazione dei complicati algoritmi sopra citati.

Basandoci su come fisicamente un segnale viene generato e inviato, l'idea fondamentale per mettere in sicurezza una comunicazione tra un nodo trasmettitore A e un nodo ricevente B, è quella di utilizzare le caratteristiche fisiche inerenti al canale di comunicazione stesso, andando a sfruttare un terzo nodo in grado di impedire all'aggressore di ricevere informazioni sufficienti per la decodifica del messaggio [13] [14].

Il dispositivo che, atto alla generazione di un segnale d'*"interferenza amica"* nei confronti del nodo malintenzionato, riesce a garantire un alto livello di sicurezza per la trasmissione è detto *jammer amico* oppure, in inglese, *friendly*

o *cooperative jammer* [11].

1.2 Obiettivi

Gli obiettivi della tesi sono di analizzare lo stato dell'arte riguardante l'approccio alla sicurezza mediante l'utilizzo del fenomeno del friendly jamming e la successiva realizzazione di un simulatore in grado di ricreare molteplici possibili scenari. La successiva analisi dei dati ottenuti dalle simulazioni servirà per identificare dei possibili utili risultati e delle possibili utili conclusioni che possano permettere a questo lavoro di integrarsi e completare quanto di già presente senza dimenticare lo scopo ultimo: la definizione di regole più *"empiriche"* atte a facilitare un'eventuale implementazione reale di un sistema di sicurezza basato sul friendly jamming.

1.3 Organizzazione

La tesi sarà organizzata secondo la seguente struttura. Nel Capitolo 2 verranno analizzati lo stato dell'arte e i già presenti lavori correlati e riguardanti la sicurezza sulle trasmissioni, il jamming ed il friendly jamming dando una panoramica sulla realizzazione di progetti reali.
Nel Capitolo 3 sarà presentato il punto di partenza da cui si è partiti per la realizzazione del nostro simulatore e verificheremo i risultati teorici provenienti dalla teoria dei giochi [15] per le situazioni a noi utili; andremo ad

espandare tali risultati in ambito pratico, analizzando casi particolari e limiti di equilibrio e applicabilità della teoria dei giochi nel successivo Capitolo 4. Nel Capitolo 5 verranno infine presentate le conclusioni, i contributi che questo elaborato ha portato e infine i possibili lavori futuri che potrebbero andare a sviluppare ulteriormente quanto già portato.

Capitolo 2

Stato dell'arte

2.1 Sicurezza nelle trasmissioni

2.1.1 I principi

Il problema della sicurezza in una trasmissione, sia essa cablata oppure wireless, ha da sempre ricoperto un ruolo di estrema importanza.
Nel corso degli ultimi anni infatti, sono stati spesi molti gli sforzi per lo sviluppo e la realizzazione di tecniche in grado di far fronte ad azioni potenzialmente malevole quali *intromissioni, intercettazioni* o *interruzioni* [16].
Al giorno d'oggi sono presenti numerosi metodi crittografici operanti ai livelli superiori del modello ISO/OSI e che permettono di raggiungere standard di sicurezza molto alti ma che, d'altro canto, richiedono livelli di complessità realizzativa ed implementativa molto elevati [17].

La sempre maggior presenza di reti WSN, composte principalmente da sensori, e, più in generale, tutte le reti destinate alle implementazioni riguardati l'IoT, ha però posto un limite operativo all'implementazione di tali tecniche: i dispositivi utilizzati sono, per la maggior parte, alimentati da una fonte di energia limitata e dovranno essere quindi i più semplici e meno energicamente dispendiosi possibile.

Quanto appena dettò però, contrasta pesantemente con la capacità computazionale richiesta per complesse operazioni di crittografia e dal consumo energetico che l'impiego di tali algoritmi richiederebbe [18].

Analizzando il modello ISO/OSI, il livello fisico si pone come obiettivo la trasmissione di un flusso di dati non strutturati in grado di ottenere un livello di sicurezza paragonabile a quello una trasmissione crittografata, attraverso l'utilizzo del solo collegamento fisico mediante il quale viaggiano i segnali elettromagnetici e delle sue proprietà. Esso definisce forma e tensione del segnale ed implementa le procedure meccaniche ed elettroniche necessarie a stabilire, mantenere e disattivare il collegamento fisico. È inoltre l'unico livello che riguarda direttamente l'hardware [19].

Per riuscire quindi a garantire, tramite metodi applicati al livello fisico, una comunicazione tra due nodi nella quale, un'eventuale nodo malevolo frapposto tra trasmettitore e ricevitore che sia in "ascolto", non riesca a carpire le informazioni contenute nel messaggio, nonostante sia anche a conoscenza degli schemi di codifica/decodifica utilizzati, si fa riferimento alle teorie dell'informazione e della sicurezza dei sistemi, entrambe sviluppate da Shannon in [20], e a un parametro SC detto di *secret capacity*.

I primi richiami ed i primi lavori riguardanti tale parametro, rappresentanti

il rapporto di "informazione affidabile" tra trasmettitore e destinatario previsto della comunicazione, ed applicanti le teorie sviluppte da Shannon, si devono ad Aaron Wyner, il quale ipotizzò la possibilità di stabilire una comunicazione con una sicurezza *"almost perfect"* senza far uso di chiavi di codifica private [21].

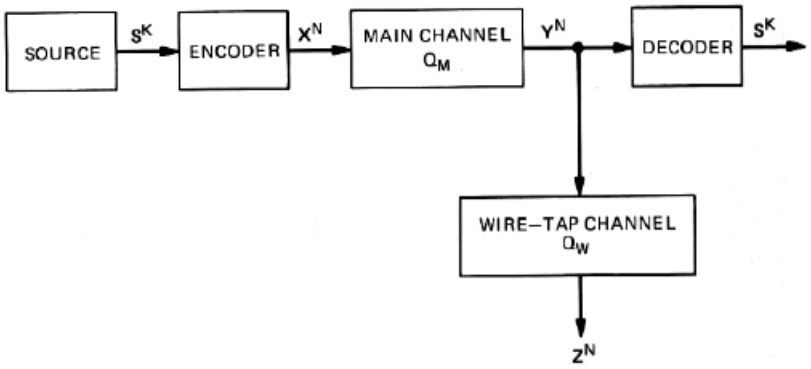


Figura 1: *Caso generale di un canale wire-tapped* [21]

Nel suo articolo Wyner dimostrò che quando il canale tra trasmettitore e nodo aggressore (*wiretap*) risulta essere una versione degradata del canale trasmettitore-ricevitore (*main channel*) è possibile, con probabilità uno, scambiare messaggi perfettamente sicuri ad un bit-rate non nullo.
Le sue affermazioni derivavano dall'osservazione che, sfruttando l'effetto di un segnale di rumore aggiuntivo, era possibile compromettere ciò che veniva ricevuto dal nodo malevolo. Utilizzando una codifica stocastica del segnale [22] e mappando ogni parola del messaggio in una *codeword*, seguendo una distribuzione di probabilità, è possibile massimizzare quindi l'incertezza lato intrusore, andando, dal lato opposto, a massimizzare la sicurezza della trasmissione: anche se in ascolto, un eventuale malintenzionato non riuscirebbe

ad estrarre nessuna informazione dalla sua osservazione del messaggio poiché quello che lui riuscirebbe ad "ascoltare" risulterebbe essere una parte irreversibilmente degradata del segnale originale [23].
Successivamente al lavoro di Wyner, molti altri studi si sono susseguiti con lo scopo di approfondire ed allargare il campo applicativo di tale tecnica.
I primi risultati ottenuti furono l'applicazione di tale approccio per una comunicazione che sfruttasse un medium cablato, del tutto analogo a quello analizzato da Wyner in [21], dove però il rumore aggiunto fosse di tipo Gaussiano (*AWGN: Additive White Gaussian Noise*) [24] [25].
Successivamente, sempre la stessa tecnica, fu estesa a canali definiti "meno rumorosi" e che possedevano quindi una maggiore capacità di trasmissione [26] e a canali contenenti informazioni confidenziali dove, le parti pubbliche, erano inviate in broadcast, ovvero senza interferenza aggiunta, mentre le componenti private al solo ricevitore legittimo tramite l'aggiunta di rumore alla trasmissione [27].

2.1.2 Applicazioni nella tecnologia wireless

Tutti i lavori presentati fino ad ora analizzavano una comunicazione tramite cavi e non espandono lo studio, come richiesto dalla nostra situazione, al caso di trasmissione wireless a causa del fatto che, la maggior parte di essi sono stati pubblicati in un periodo in cui, tale tecnologia, non risultava ancora particolarmente sviluppata.
Nel più recente periodo, tuttavia, sono stati fatti molti sforzi per raggiungere

questo obiettivo iniziando da [28], dove viene dimostrata la possibilità di incrementare la secrecy incorporando la conoscenza della risposta impulsiva del canale alla crittazione, passando per [29] e [30], dove abbiamo l'implementazione di tali principi alle trasmissioni radio, fino a giungere a [31] che studia e presenta un'implementazione *MIMO (Multiple Input Multiple Output)* di un complesso sistema di comunicazione wireless la cui sicurezza è fornita tramite implementazioni al livello fisico.

2.2 Jamming

Il fenomeno del jamming, nelle reti wireless, è definito come l'alterazione della già esistente comunicazione tramite la riduzione del *SNR (Signal to Noise Ratio)* al lato del ricevitore attraverso la trasmissione di un altro segnale wireless d'interferenza [32].

Il jamming differisce dalle classiche interferenze solitamente presenti in una rete, quali potrebbero essere segnali prodotti in bande di frequenza vicine oppure segnali prodotti da nodi appartenenti alla stessa rete che comunicano tra loro, poiché descrive la generazione intenzionale di un segnale wireless, il quale, risulta essere deliberatamente distruttivo per le comunicazioni preesistenti.

L'evoluzione e il sempre maggior impiego di strumenti di sensoristica, per esempio per la realizzazione di reti *WSN (Wireless Sensor Networks)* funzionanti la maggior parte delle volte nella banda delle frequenze license-free *ISM (Industrial Scientific Military*, comprendente anche le frequenze WiFi),

sta ultimamente portando il fenomeno del jamming nuovamente alla ribalta, dato che i dispositivi utilizzati per la realizzazione di tali reti risultano essere, architettetturalmente parlando, molto semplici e quindi facili bersagli di attività illecite [33] il cui scopo è, oltre alla semplice distruzione del segnale, anche la sua manipolazione.

Signals			Effects	
target	attacker's	resulting	signal layer	message layer
———			signal creation/replay	insertion
		———	**annihilation**	deletion
			noise jamming	
			**symbol flipping**	modification
			overshadowing	

Figura 2: *I possibili effetti che una diversa attività di interferenza jammer possono avere sul segnale pre-esistente. Come mostrato negli ultimi due esempi, è possibile, modulando la forma dell'interferenza, distruggere il segnale (annichilendolo o rendendolo troppo rumoroso) oppure modificarne il contenuto [34].*

Un jammer in grado di attaccare una rete WSN e di interromperne completamente la trasmissione d'informazione interna, non risulta, al giorno d'oggi, troppo complesso né da reperire, dato che quasi ogni dispositivo con una scheda RF potrebbe, tramite un'opportuna modifica software, assolvere a tale scopo [35], né da utilizzare, grazie allo sviluppo di software *SDR (Software Designed Radio)*, ovvero di software in grado di impostare e manipolare i diversi parametri relativi ai valori del segnale fisico utilizzato per la trasmessione [36].

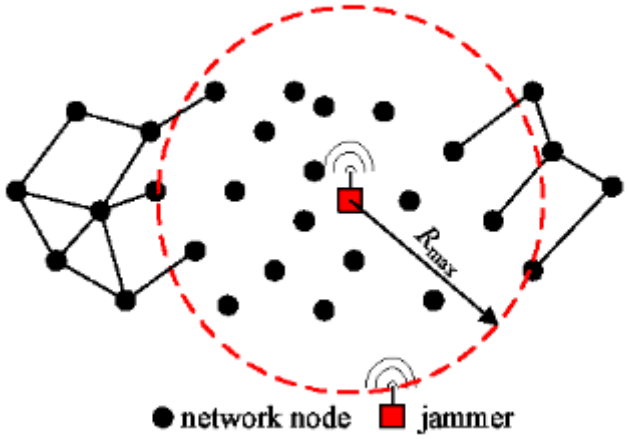


Figura 3: *L'effetto di un jammer su una rete distribuita di sensori. La rete risulta essere divisa in due sottoreti non più comunicanti tra loro.*

A causa dei danni che un jammer può causare ad una rete, l'obiettivo principale, fino a poco tempo fa, era di riuscire ad evitare che un'eventuale azione di jamming potesse compromettere il funzionamento della rete stessa e di implementare dei sistemi di contromisura atti a preservare la trasmissione dei dati.

2.2.1 Tecniche di Jamming

Prima di introdurre i possibili metodi di difesa, risulta molto utile presentare le diverse tipologie di jammer presenti, poichè, a seconda del modo di agire del jammer, varierà anche la miglior tecnica di difesa possibile, detta *best response*, della rete [32]:

- *Jammer Pro-attivi*: trasmettono un segnale d'interferenza sia in presenza di una trasmissione sia con la sua assenza. I pacchetti inviati

sono composti da bit casuali che vengono trasmessi nel singolo e costante canale di operatività del jammer, impedendo a tutti gli altri nodi operanti in quello stesso canale di operare correttamente.

- **Jammer Costanti**: emettono continuamente bit casuali sfruttando le tecniche d'accesso al canale del protocollo *CSMA (Carrier Sense Multiple Access)* per disturbare le comunicazioni. Viene difatti reso impossibile per gli altri nodi comunicare poichè, nel momento di sensing del canale, esso verrà sempre trovato occupato (*busy*) dal segnale di jamming. Questa tipologia di attacco, nonostante sia potenzialmente debilitante per la rete e relativamente semplice da attuare, risulta essere molto inefficiente dal punto di vista energetico oltre che di facile individuazione [37].

- **Jammer "Ingannevoli"**: molto simili ai jammer costanti, i jammer "ingannevoli" si differiscono da quest'ultimi poichè trasmettono continuamente *pacchetti effettivamente validi* [37] facendo credere che sia in atto una reale trasmissione.

  Possiedono le stesse proprietà di inefficienza e di semplicità dei precedenti divenendo però di più difficile individuazione dato che il segnale che trasmettono viene confuso con una reale trasmissione.

- **Jammer Casuali**: trasmettono ad intermittenza sia bit casuali che pacchetti validi nella rete [37] unendo quindi le due tipologie precedenti. Al contrario di esse però, questo jammer, opera secondo degli schemi ideati appositamente per il risparmio energetico: il suo stato cambia continuamente tra *dormiente* ed *attivo*

seguendo una distribuzione utile a massimizzare il suo payoff e minimizzando, nel contempo, il dispendio energetico [32].

- *Jammer Reattivi*: questa tipologia di jammer si attiva ed inizia la sua azione d'interferenza solo quando rileva una comunicazione sopra un certo canale della rete, con lo scopo di comprometterne la riuscita [37]. Tale jammer deve essere in grado di monitorare continuamente lo stato del canale. Questa operazione analogica risulta essere poco efficiente dal punto di vista energetico [33].
  Tuttavia, questo modo di operare rende i jammer reattivi molto più complessi da individuare poichè risulta quasi impossibile determinarne l'effettiva percentuale di attività.

  - **Jammer RTS/CTS**: questi jammer sfruttano il meccanismo utilizzato per ovviare al problema del nodo nascosto nel protocollo wireless 802. Essi si attivano quando individuano un messaggio *RTS (Request to Send)* da parte di un trasmettitore, corrompendone la trasmissione ed impedendo così l'invio da parte del ricevitore del corrispettivo *CTS (Clear to Send)*. Alternativamente può intervenire dopo la ricezione del pacchetto RTS ed impedire la trasmissione del CTS; il risultato, in ogni caso, risulta essere che, per la mancata definizione del canale di trasmissione, il messaggio non sarà inviato [38].

  - **Jammer Data/ACK**: hanno lo scopo di corrompere la trasmissione dell'informazione da parte del trasmettitore oppure, in alternativa, del messaggio di *ACK (Acknowledgement)* da parte del

ricevitore [38]. In entrambe le situazioni tuttavia, sia perché il pacchetto giunge a destinazione corrotto, sia per la mancanza dell'ACK perchè corrotto, la trasmissione dovrà essere effettuata più e più volte, causando così un overflow al buffer del ricevitore.

- *Jammer a Funzione-Specifica*: questa tipologia di jammer è realizzata implementando una funzione pre-determinata: oltre alla caratteristica intrinseca del jammer nell'essere *pro-attivo* oppure *reattivo* infatti, quest'ultimi possono operare su di un singolo canale, per preservare energia, oppure possono agire su molteplici canali contemporaneamente, per massimizzare il proprio payoff. Nel caso in cui agissero su singolo canale tuttavia, quest'ultimo non risulterà fissato, ma potrà variare anch'esso secondo una specifica funzione differenziandoli da quelli semplicemente reattivi [32].

  – **Jammer ad Inseguimento**: salta molto velocemente tra tutti i canali disponibili (nell'ordine di mille volte al secondo) e introduce interferenza su di ognuno per un brevissimo lasso di tempo [39].
  Se, durante la trasmissione, dovesse avvenire un cambio di canale a causa del rilevamento dell'azione del jammer, quest'ultimo analizzerà l'intera banda alla ricerca della nuova frequenza di trasmissione, *inseguendo* il trasmettitore.
  L'azione di intereferenza limitata ad un solo canale per volta rende questo tipo di jamming a "conservazione d'energia" oltre che, proprio a causa dei suoi molteplici salti da un canale all'altro, molto efficace contro certe tipologie di anti-jammer, le quali possiedono

una velocità di switch tra i canali molto minore [32].

- **Jammer Channel-Hopping**: saltano tra un canale ed un altro interferendo in maniera *pro-attiva* [40] [41]. Questo tipo di jammer ha accesso diretto ai canali aggirando l'algoritmo di CSMA e risulta essere invisibile quando compie le azioni di *sensing* del mezzo.
- **Jammer a Rumore-Impulso**: può cambiare il canale d'azione e interferire su diverse bande di frenquenza contemporaneamente e per differenti periodi di tempo, alternando periodi di *sleep* utili per la conservazione dell'energia. Differisce dai jammer proattivi poiché risulta essere in grado di attaccare molti canali, anche contemporaneamente [42].

- *Jammer Smart-Hybrid*: vengono definiti smart poiché molto efficienti dal punto di vista energetico in rapporto all'effetto di interferenza generato. Tale traguardo è raggiunto tramite l'analisi della trasmissione da interrompere, utile per decidere il quantitativo di energia necessario per creare sufficiente interferenza.

  Tale approccio permette inoltre di non utilizzare un quantitativo di energia inutilmente alto e consente la suddivisione della stessa in maniera intelligente tra tutti i canali possibili. La definizione *hybrid* invece deriva dal fatto che possono essere implementati sia in maniera pro-attiva che reattiva [32].

  - **Jammer Channel-Control**: funzionano mirando al canale definito *di controllo*, ovvero quello utilizzato per coordinare le at-

tività della rete [43]. Può generare interferenza sia in modalità pro-attiva che reattiva e può danneggiare la rete fino a renderla completamente inoperativa.

– **Jammer ad Attacco Implicito**: tali jammer, oltre che disabilitare il nodo obiettivo dell'attacco, causano un *denial of service (DoS)* agli altri nodi presenti nella rete [44]. Questo tipo di attacco sfrutta l'algoritmo di adattività utilizzato nelle reti wireless dove gli *AP (Access Points)* comunicano con i nodi più "deboli" riducendone il bit-rate: a causa di questo l'AP spenderà più tempo a comunicare con tali nodi più lenti che, se attaccati, faranno aumentare il tempo speso dall'AP stesso per tentare di comunicare con loro.

– **Jammer "Flow Attacks"**: prevede molteplici jammer che interferiscono con la trasmissione dei pacchetti, riducendo cosi il *packet flow* complessivo. Questi attacchi sono portati utilizzando l'informazione presente nei pacchetti dal network layer [45].

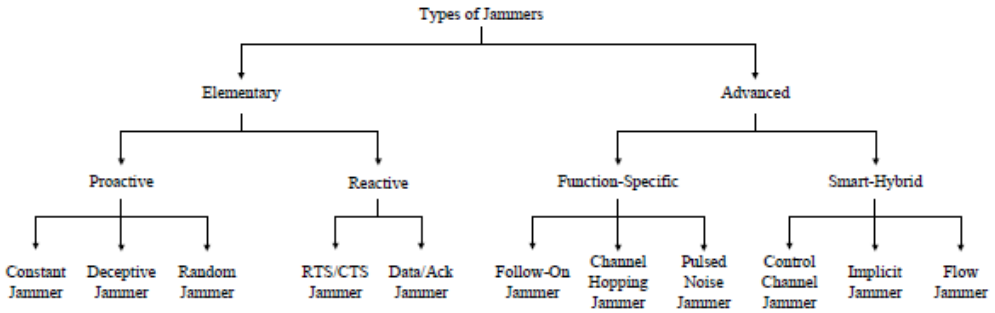


Figura 4: *Sommario delle diverse tipologie di jammer [32].*

2.2.2 Contromisure e rilevamento

Come in precedenza introdotto, le tecniche di anti-jamming dipendono fortemente dalla tipologia di attacco che viene portato alla rete.
Per distinguere più facilmente le successive tipologie di difesa faremo riferimento alla suddivisione mostrata in figura 4 tra jammer *elementari* e jammer *avanzati*.

Difese contro i jammer elementari

Il primo problema da affrontare quando si vuole progettare una difesa contro una potenziale interferenza da parte di un jammer è sicuramente l'individuazione di tale azione malevola all'interno della rete.
L'elemento di individuazione dell'azione di jammer elementari, sia pro-attivi che reattivi, viene fornita dallo "strozzamento" che la banda di trasmissione subisce. Un canale occupato, oltre che dalla trasmissione reale, anche da un segnale di rumore aggiuntivo, subisce infatti una riduzione nella sua effettiva capacità di trasportare l'informazione.
L'utilizzo di una soglia per il *carrier sensing* può quindi risultare molto efficace per la rilevazione di tali tipi di attacco.
Un metodo di rilevazione e mitigazione del problema tramite questo approccio viene proposto in [46], dove un algoritmo mappa la presenza dei nodi e individua, analizzando il numero di tentativi falliti di una trasmissione, la presenza o meno di un jammer. Una volta definita l'area interessata dall'azione d'interferenza, vengono inserite delle nuove entry nelle tabelle di *routing*,

con lo scopo di riuscire a connettere i nodi della rete aggirando i collegamenti operanti in tale zona.

Un altro metodo molto interessante viene proposto in [42], descrivenendo una tecnica operante al terzo livello del protocollo ISO/OSI, ovvero quello di rete: il routing delle informazioni attraverso la network viene definito, di volta in volta, analizzando la probabilità che un collegamento tra un nodo trasmettitore ed un nodo ricevitore stia subendo un'interferenza dovuta ad un jammer. Tale probabilità viene valutata tenendo conto di diverse variabili tra cui *distanza, packet loss, SNR, BER (Bit Error Ratio), RSS (Received Signal Strength)* e PDR.

Sono tuttavia molte altre le metodologie che si sono sviluppate negli anni: dai semplici sistemi che cambiano canale, tra cui [37] [47] [48] [49] [50] [43] o che, se possibile, spostano i nodi al di fuori dell'area influenzata, passando per quelli che utilizzano solamente alcuni dei parametri sopra citati (BER, SNR, RSS, PDR) [37], oppure utilizzando i cosiddetti sistemi *ibridi* [51], fino ad arrivare a vedere una prima applicazione della game theory in ambito sicurezza con [52]: in quest'ultima applicazione si analizza un gioco composto rispettivamente dal jammer e da un "nodo *monitor*" i quali vogliono massimizzare i propri payoff massimizzando, per quanto riguarda il primo, il "danno" procurato alla rete e, dall'altra parte, massimizzando invece il *throughput* della rete.

Difese contro i jammer avanzati

Come descritto in precedenza, i jammer avanzati possono essere del tipo Smart-Hybrid oppure a Funzione-Specifica ed entrambi utilizzano una combinazione di strategie pro-attive e reattive con implementazioni *smart*, atte alla conservazione dell'energia. Risultano quindi essere di più difficile individuazione e, di conseguenza, molto più complessi da contrastare dei jammer ad implementazione elementare.
Alcuni dei più efficaci metodi utili a contrastare questo tipo di attacchi sono:

- **Hermes**: prevede l'implementazione nei nodi della propria rete di uno schema ibrido tra *DSSS (Direct Sequence Spread Spectrum)* e *FHSS (Frequency Hopping Spread Spectrum)* ove il primo viene utilizzato per far si che l'eventuale malintenzionato rilevi la trasmissione come rumore bianco gaussiano mentre il secondo viene utilizzato per cambiare velocemente il canale di trasmissione rendendo inefficaci anche i jammer ad inseguimento [39].

- **MULEPRO**: proposto in [40] e [41], risulta essere un metodo che differisce da tutti gli altri poichè ogni nodo analizza la propria situazione indipendentemente dagli altri: quando un nodo intuisce di essere sotto l'effetto di un jammer (diminuzione dei parametri come throughput e SNR ne possono essere indice) avvia il protocollo *MULEPRO (MUlti-channel Exfiltration PROtocol)*, il quale porta il nodo stesso da un stato *normale*, dove solo il canale comune è utilizzato per le trasmissione, ad uno stato di *exfiltration*. Quando un nodo si trova in quest'ultimo stato, proverà ad inviare i suoi messaggi (compreso un messaggio di controllo

dove afferma la presenza di un'interferenza jammer) trasmettendo su molteplici canali ed utilizzando tutti i routing possibili.

– **FIJI**: in [44] viene proposta una soluzione implementata parzialmente sul driver ed in parte sul modulo dedito alla trasmissione dei dati.
Un AP che utilizzi il sistema *FIJI (Fighting Implicit Jamming)* analizza il ritardo presente su ogni trasmissione di ogni nodo a quest'ultimo collegato e, nel momento in cui viene rilevato un aumento radicale del delay, etichetta il nodo "colpevole" come JAMMED.
Una volta che l'AP ha etichettato un nodo come JAMMED procede diminuendo le risorse che dedica alla comunicazione con quest'ultimo per poi ripristinarle nel caso in cui una situazione di normalità si ripresenti; così facendo si riesce a contrastare in maniera molto efficace molte tipologie di jammer, compresi quelli ad *attacco implicito*.

Considerazioni

Come è possibile osservare, la maggior parte delle contromisure ad azioni di jamming, esclusa la semplice soluzione di "movimento dei nodi fuori dalla zona interessata", presentate precedentemente, sono pensate per operare su reti statiche: il problema di sicurezza relativo alle reti mobili rimane quindi un problema che tutt'ora non presenta soluzioni con una efficacia paragonabile a quelle presenti per le reti cablate.
La problematica di estensione di queste tecniche, anche in ambiente wireless, risiede nel fatto che, una rete dove sia i nodi legittimi di una rete, sia i jammer,

sono liberi di muoversi arbitrariamente andando a modificare path di routing ed aree di interferenza, comporta l'aumento esponenziale della complessità dei modelli da utilizzare, i quali non risultano essere più risolvibili in maniera univoca. Le molteplici caratteristiche intriseche del jammer utilizzato per portare l'attacco alla rete inoltre, rende del tutto impossibile la definizione di una unica strategia di reazione.

2.3 Friendly Jamming

Come precedentemente già affermato, le trasmissioni wireless risultano essere altamente vulnerabili ad intrusioni e/o intercettazioni provenienti da nodi esterni la rete poiché, potenzialmente, ogni dispositivo in grado di sintonizzarsi sulla frequenza utilizzata, può effettivamente interferire con una comunicazione pre-esistente [53].
L'approccio convenzionale utilizzato per proteggere tali reti da eventuali attacchi, si basa su: studi della distribuzione fisica dei nodi della rete, controlli di integrità dei messaggi, autenticazione, controllo dello spettro di comunicazione e, nella maggior parte dei casi, sulla crittografia [54] [55].
L'utilizzo di tali principi è considerato vantaggioso poiché consente la realizzazione di sistemi per la sicurezza astratti dal layer fisico della trasmissione, permettendone quindi l'implementazione in molteplici condizioni e scenari. Tuttavia, tutte le tecniche citate poco fa derivano dall'evoluzione di metodologie che erano inizialmente state formulate per regolare comunicazioni cablate e *point-to-point* e che quindi avevano limiti progettuali e gradi di

libertà diversi da quelli che ci si aspetta possano essere imposti alla realizzazione di una rete wireless [56].

L'ostacolo maggiore che l'implementazione di questi metodi vede nelle reti wireless risiede nel consumo di energia: mentre la maggior parte dei dispositivi utilizzati nelle reti cablate è probabilmente collegata ad una fonte di energia esterna (rete elettrica o generatori) quelli presenti nelle reti wireless sono spesso, per natura stessa della rete, dipendenti da una fonte di energia interna come una batteria.

Dispositivi appartenenti ad una rete wireless, come possono essere sensori di una rete WSN, sono resi solitamente architetturalmente semplici, in maniera tale da limitare il dispendio energetico, poiché, anche la semplice operazione di scambio di chiavi private *necessarie* per l'utilizzo di un algoritmo di crittografia, risulta essere un dispendio energetico quasi insostenibile.

L'importanza nello sviluppare tecniche in grado di ovviare a questi problemi ha quindi assunto sempre una maggiore importanza nel corso degli ultimi anni, fino ad arrivare ai giorni d'oggi dove, una nuova tecnologia, sembra aver attirato su di sé un molta attenzione: il *friendly jamming*.

Il fenomeno dell'interferenza è sempre stato considerato un fenomeno indesiderato in un qualunque tipo di trasmissione, wireless comprese.

Recenti studi hanno tuttavia dimostrato che, un sistema di comunicazione può, dal punto di vista della sicurezza, trarne beneficio se quest'ultima viene generata seguendo alcuni criteri e poi portata secondo dei precisi schemi.

L'idea alla base di questo metodo, consiste nel creare intenzionalmente interferenza utile per mettere il nodo malevolo in una situazione di svantaggio rispetto ai nodi effettivamente appartenenti alla rete, senza tuttavia andare

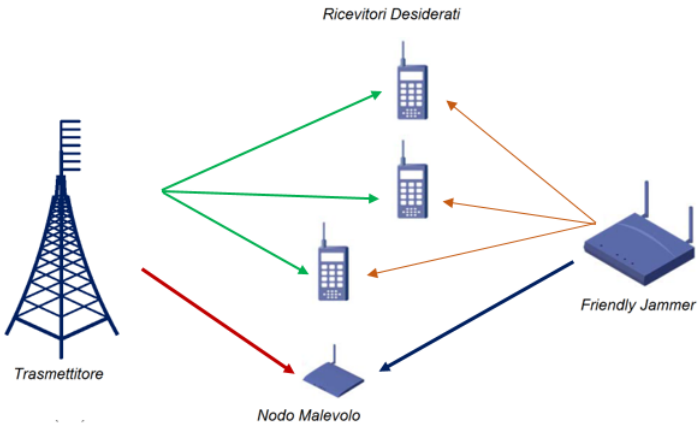


Figura 5: *Principio di funzionamento del friendly jamming dove le frecce verdi indicano la comunicazione lecita, la rossa l'intromissione del nodo malintenzionato (wire-tapped link), la blu l'interferenza generata per disturbare l'azione malevola e l'arancione l'interferenza collaterale del jammer sulla comunicazione reale.[57].*

a compromettere il funzionamento interno della rete stessa.

Per raggiungere tale obiettivo è possibile convertire alcuni nodi alle sole attività di jamming, assegnarvi casualmente alcuni nodi, oppure inserire degli appositi nodi che assolvano tale scopo [58].

2.3.1 Modelli teorici per il friendly jamming

Esistono svariati approcci utili a modellare il fenomeno del friendly jamming, iniziando dai più semplici, i quali considerano solamente la trasmissione malevola tra trasmettitore e nodo intrusore come influenzata dall'aggiunta di rumore da parte del jammer, fino ad arrivare a quelli che analizzano la presenza di molteplici jammer che inficiano sulla qualità del canale di tutte le comunicazioni in *range*.

La valutazione del livello di sicurezza di una trasmissione avviene, in ogni caso, tramite l'utilizzo di alcuni parametri riferiti alla qualità del canale come la *secrecy capacity* oppure la *capacità del canale* stesso [28].

Uno dei modelli più semplici, risultato tuttavia maggiormente interessante nell'analisi iniziale di questa tecnica, risulta essere un gioco composto da tre attori, ovvero il *trasmettitore legittimo* A, il *ricevitore desiderato* B ed il *nodo malevolo* C dove viene idealizzato il fatto che l'azione del jammer infici solamente sulla qualità del collegamento tra A e C [59].

I collegamenti sono rispettivamente chiamati *main channel*, quello tra A e B e, come nel caso presentato in [21], *wire-tap channel.* quello tra A e C.

Utilizzando quanto espresso nel paragrafo 2.1.1, in questa modellizzazione, viene utilizzata come parametro di riferimento la sola *secrecy capacity*, ovvero il massimo valore acquisibile dal parametro del *secrecy rate.*

Tale parametro viene determinato nei casi di riferimento di canali con *AWGN* (*Additive White Gaussian Noise*) e di *Rayleigh Fading.* Quest'ultimo caso tiene in considerazione i canali rappresentati secondo il modello statistico di Rayleigh, il quale afferma che l'intensità di un segnale che ha attraversato un *medium* varia randomicamente seguendo una distribuzione probabilistica, detta anch'essa di Rayleigh.

Utilizzando le seguenti formule sono stati valutati gli andamenti della *secrecy capacity* nei due casi sopra descritti [13]:

$$SC_{s,AWGN} = \left[\frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma_m^2}\right) - \frac{1}{2} \log_2 \left(1 + \frac{P}{\sigma_w^2}\right) \right]^+ \qquad (2.1)$$

$$SC_{s,Ray} = \left[\log_2 \left(1 + \frac{P|h_m|^2}{\sigma_m^2}\right) - \log_2 \left(1 + \frac{P|h_m|^2}{\sigma_w^2}\right) \right]^+ \quad (2.2)$$

dove P è la potenza utilizzata per trasmettere il segnale, σ_m e σ_w sono la potenza del rumore, rispettivamente nel canale principale e del canale wiretapped, h_m e h_w coefficienti di fading nel canale di Rayleigh ed il segno più alla fine delle formule indica $[x]^+ = max(x, 0)$ [59].
Inoltre, per completezza, possono essere ricavate anche le definizioni dei valori del *SNR* sia della trasmissione "reale" verso il nodo B che di quella malevola verso il nodo C, ottenendo:

$$\gamma_m = \frac{P|h_m|^2}{\sigma_m^2} \qquad \gamma_w = \frac{P|h_m|^2}{\sigma_w^2} \quad (2.3)$$

dove γ_m indica il SNR del canale principale mentre γ_w indica l'SNR del canale abusivo.
Confrontando l'andamento dei due secrecy rate, ricavati dalle definizioni in (2.1) e (2.2) e relativi quindi alle due tipologie di canale descritti, otteniamo un andamento come raffigurato in figura 6, dove si osserva che, il parametro medio di SC_s, risulta assumere sempre valori maggiori nel canale affetto da *Rayleigh fading* rispetto a quello ove è presente *Additive White Gaussian Noise.*

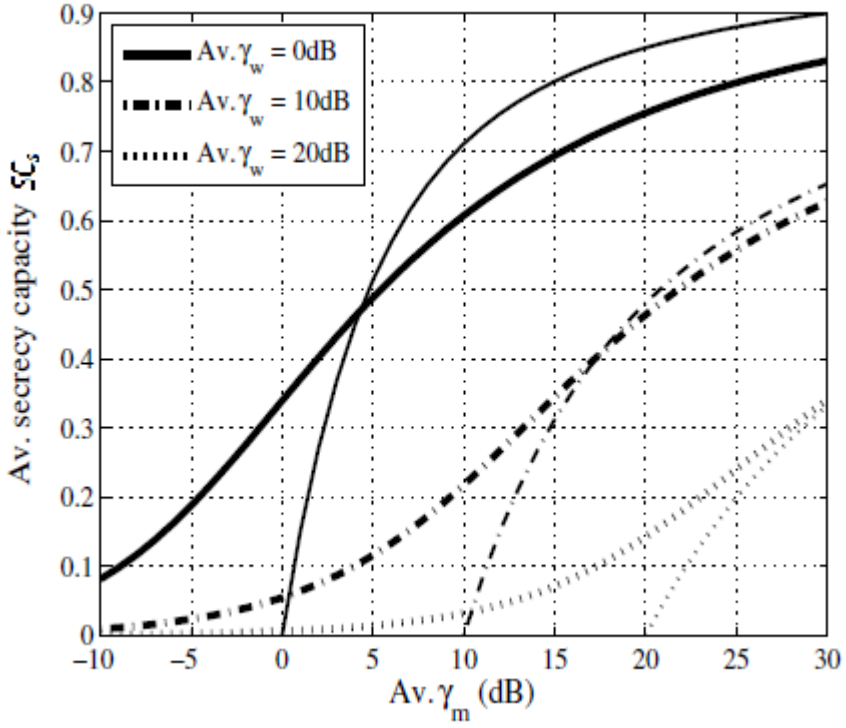


Figura 6: *Andamento della secrecy capacity media rispetto al variare dei valori di SNR γ nel canale principale utlizzando il modello semplificato. Linee spesse sono usate per rappresentare il canale modellato con il modello di Rayleigh mentre linee più sottili per modellizzazione tramite canale AWGN [59].*

Questi andamenti rappresentati in figura 6 ci permettono, nelle limitazioni dovute al modello utilizzato, di affermare che è possibile agire sul livello di sicurezza del segnale, sfruttando le proprietà di *fading* del canale, ovvero quelle riguardanti la sola parte fisica della trasmissione, andando a diminuire l'SNR del canale wire-tapped, il quale risulterà avere sempre un valore di secrecy capacity inferiore a quello del canale principale [59], soddisfacendo così le nostre necessità e garantendo una comunicazione sicura.

Un'analisi più precisa, accurata e realistica di quella precedentemente otte-

nuta utilizzando il modello sopra descritto, può essere ricavata andando ad aumentare la complessità del modello stesso e prendendo in considerazione gli effetti dovuti all'interferenza generata dall'azione del *friendly jammer* su tutti i canali con cui entra in contatto.
Andando quindi a valutare la conseguenza che l'introduzione volontaria di un segnale d'interferenza ha sulle *capacità* di trasmissione, sia del canale primario che del canale wire-tapped, otteniamo le seguenti definizioni:

$$C_m = B\, log_2 \left(1 + \frac{P\, G_m}{\sigma^2 + G_{jm} P_j}\right) \tag{2.4}$$

$$C_w = B\, log_2 \left(1 + \frac{P\, G_w}{\sigma^2 + G_{jw} P_j}\right) \tag{2.5}$$

dove B indica la larghezza di banda, P la potenza di trasmissione dell'effettivo segnale, P_j la potenza del segnale d'interferenza trasmesso dal jammer, G_m e G_w i guadagni del main e del wire-tapped channel, G_{jm} G_{jw} i guadagni relativi alla trasmissione del jammer (anch'essi agenti sia nel canale principale che nel canale non voluto) ed infine σ il rumore termico, considerato per semplicità uguale in entrambi i canali.
Un ulteriore vantaggio di questo modello rispetto a quello precedente consiste nel fatto che, l'eventuale implementazione di molteplici jammer, può essere realizzata andando semplicemente a sostituire, nelle formule (2.4) e (2.5), al posto del singolo effetto, la sommatoria di tutti gli effetti, ottenendo:

$$C_m = B\, log_2 \left(1 + \frac{P\, G_m}{\sigma^2 + \sum_i G_{jmi} P_{ji}}\right) \tag{2.6}$$

$$C_w = B\, log_2 \left(1 + \frac{P\, G_w}{\sigma^2 + \sum_i G_{jwi} P_{ji}}\right) \tag{2.7}$$

Anche in questo secondo modello però, infine, per riuscire a garantire che il nodo malevolo tragga un'informazione mutua nulla dalla comunicazione "catturata", si giunge ad un vincolo sulla secrecy capacity: il trasmettitore dovrà infatti trasmettere il segnale stesso con un valore minimo della SC che, da [23], possiamo definire come:

$$SC_s = [C_m - C_w]^+ \tag{2.8}$$

Dalla (2.8) segue direttamente che, tale valore di SC_s, deve essere strettamente maggiore di zero per poter permettere una comunicazione sicura.
Entrambi i modelli sono riusciti dunque a dimostrare la realizzabilità di quanto teorizzato nel paragrafo 2.3: infatti, tramite l'impiego di un jammer con un segnale d'interferenza generato *ad-hoc* ed utilizzato per danneggiare il canale di una eventuale trasmissione malevola, è possibile degradare il canale di comunicazione abusivo, ottenendo cosi un livello di sicurezza molto alto utilizzando solamente le proprietà fisiche del segnale.

2.3.2 Tipologie di friendly jamming

Abbiamo appena definito il friendly jamming, anche detto *cooperative jamming*, come una tecnica dove viene introdotto del *rumore artificiale*, con lo scopo ultimo di confondere l'eventuale intruso ed impedire quindi che quest'ultimo possa, per esempio, ricavare informazioni *ascoltando* una trasmissione inizialmente non diretta a lui.
Come già visto per le diverse tipologie di jamming *classico*, anche qui è possibile individuare una classificazione dei diversi possibili approcci, i quali però, vengono qui suddivisi per tipologia di segnale d'interferenza generato anziché per principio di funzionamento [60]:

- *Gaussian Noise*: il segnale d'interferenza generato è dello stesso tipo di quello già presente a causa di fonti naturali come le vibrazioni termiche degli atomi in un conduttore oppure lo *shot noise* [61] [62] [63]. È stato inoltre dimostrato in [64] che, l'introduzione di tale interferenza può portare ad ottenere un valore della secrecy rate *positiva* anche quando il canale trasmettitore-ricevitore è peggiore del canale trasmettitore-intruso.

- *Interferenza "ad-priorem"*: il segnale d'interferenza qui generato non possiede uno schema fisso ma è conosciuto a priori dai ricevitori i quali riescono quindi a sottrarne l'effetto sul segnale che effettivamente ricevono [65] [66].

- *Feedback-Based*: questa tecnica sfrutta, per ottenere risultati migliori, un meccanismo fondamentale basato sul *feedback*. Uno scambio tra

due nodi di una chiave di codifica diversa avviene per ogni trasmissione, e un messaggio di feedback viene generato in caso di riuscita/mancata ricezione di quest'ultima. Analizzata isolatamente, questa azione di scambio, non "genera" un livello di secrecy maggiore ma, dato che avviene sotto l'interferenza generata da un jammer, abbassa drasticamente le probabilità per un malintenzionato di riuscire a captare per intero sia tutte le chiavi di codifica che il messaggio correlato [67].

- *Spectrum Leasing*: studiata per la realizzazione su reti dove non è possibile installare dei nodi fissi per la creazione del segnale di jamming, oppure obbligare dei nodi ad utilizzare le loro risorse per il beneficio altrui, sfrutta il paradigma dello *spectrum leasing* [68] per incentivare i nodi ad operare come dei cooperative jammer. L'incoraggiamento avviene tramite la suddivisione della porzione di spettro destinata alla comunicazione in *sotto-canali*, tra loro il più ortogonali possibile, che potranno essere utilizzati da altri nodi per la trasmissione di altri messaggi [69].

Sono in ogni caso molte le tecnologie e/o tecniche utilizzate in congiunzione alla sola generazione di segnali di interferenza. Nella realizzazione di un sistema di friendly jamming, per incrementare le prestazioni ed aumentare la sicurezza, vengono infatti sfruttate *antenne multiple [70], tecniche di beamforming [71] e allocazione di potenza* [72].

Capitolo 3

L'utilizzo della Game Theory

La game theory risulta essere molto utile nello studio di applicazioni riguardanti l'ambito delle telecomunicazioni poiché fornisce strumenti matematici in grado di modellizzare e studiare con precisione le complesse interazioni tra nodi razionali interdipendenti. Recentemente, si è osservata una crescita significativa nelle attività di ricerca che impiegano la game theory per analizzare reti di comunicazione. Il merito di questo incremento è principalmente imputabile alle sempre più impellenti necessità di reti mobili autonome, distribuite e flessibili, nelle quali ogni dispositivo può assumere decisioni razionali ed indipendenti [73].

L'ambito sicurezza non è stato, tuttavia, il primo degli scenari di applicazione alle telecomunicazioni della game theory che, infatti, è stata utilizzata in una moltitudine di studi per l'ottimizzazione delle reti di comunicazione. In [74], un approccio game teorico è stato utilizzato per lo studio di alcune reti wireless cooperative, nelle quali i nodi, basandosi sul principio della *diretta reciprocità* propria delle reti MIMO (*Multiple Input Multiple Output*)

[74], vengono progettati per aiutarsi tra loro. La modellizzazione, avvenuta tramite un *modello dinamico Bayesiano* [75], riusciva a catturare tutti gli aspetti fondamentali e necessari per l'analisi del problema che, in questo caso, presentava un perfetto equilibrio tra *costi e vantaggi.*

In [76], la game theory viene impiegata per lo studio della spartizione dello spectrum e per la stima del *budget* (col fine di bilanciare la richiesta di potenza) in uno scenario più *commerciale* delle risorse di una rete mentre, in [77], si sono valutati sempre tramite un gioco di *Stackelberg* i molteplici problemi presenti nei protocolli *MAC* d'accesso alle reti MIMO.

3.1 Game Theory applicata alla sicurezza

Uno dei più importanti studi riguardanti la sicurezza tramite i principi derivanti dalla game theory si deve a [78] il quale studia il paradigma dello *spectrum leasing* [79] [80].

Il modello proposto viene utilizzato per simulare una situazione in cui dei nodi *non-altruisti* (ovvero che non si occupano "spontaneamente" della sicurezza della rete) vengono incoraggiati ad operare come friendly jammer.

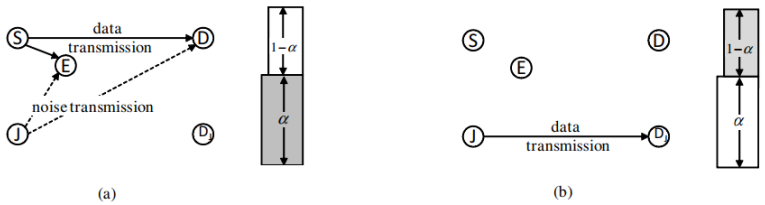


Figura 7: *Esempio di spectrum leasing atto al jamming cooperativo [78].*

La fonte del segnale, S nella figura 7, ricompensa il nodo J, per la sua azione di interferenza amica, utile per evitare che il nodo intruso E possa intercettare la trasmissione diretta a D, garantendogli l'accesso temporaneo al suo canale di trasmissione. Così facendo, S mira a ad ottenere il massimo valore del suo *secrecy rate*, mentre il nodo J ottimizza la sua potenza di trasmissione con lo scopo di massimizzare la quantità di dati che trasmette.
Questa interazione tra *source* e *jammer potenziale* è modellato in un gioco, definito duopolio di Stackelberg [81], dove sono presenti un nodo leader l_1 ed un nodo *inseguitore* l_2, la quale agisce solo dopo aver visto la mossa di l_1.
Più nello specifico, data S fonte del segnale, vuole trasmettere segretamente con il nodo D nonostante la presenza del nodo intrusore E.
A questo punto, il nodo J, viene reclutato come cooperative jammer atto alla generazione di un'interferenza aggiuntiva atta ad aumentare la secrecy rate della trasmissione tra S e D. Definito uno slot di tramissione unitario, solamente una parte α sarà effettivamente utilizzata per la trasmissione $S \to D$, mentre, la restante $1 - \alpha$, viene assegnata come ricompensa al jammer che, a questo punto, effettuerà la trasmissione verso il suo nodo destinatario D_j.
Definendo con β il rapporto tra la *potenza media* utilizzata dal jammer nella fase di interferenza ed in quella di trasmissione, possiamo ricavare la potenza di trasmissione d'equilibrio di questo gioco come:

$$P_J^*(\alpha, \beta) = \left[\frac{1-\alpha}{c \ \ln 2} - \frac{\sigma^2(\alpha\beta + 1 - \alpha)}{h_J} \right]_0^{P_J}$$

dove c è il costo di trasmissione per unità di potenza mentre h_J e σ hanno lo stesso significato spiegato nella sezione 2.3.1.

Uno scenario molto simile a quello appena descritto, viene affrontato in [27] e [82], dove i nodi che decidono di funzionare come jammer vengono ricompensati con un incentivo basato sul credito, a dispetto di un'opportunità di comunicazione.
Un'altra pubblicazione che fa un uso interessante della game theory per l'analisi di reti ove vengono implementati/arruolati nodi utili per aumentare la sicurezza è [15].
Tale studio risulta essere, dal punto di vista implementativo, molto interessante poiché analizza come ricavare le probabilità d'equilibrio ϵ e j, rispettivamente di intrusione del nodo malevolo e di azione difensiva del jammer.
I risultati teorici provenienti da questo articolo risulteranno essere la base di partenza per le analisi che verranno successivamente portate in questo elaborato.

3.2 Verifica dei risultati

Nella realizzazione del nostro simulatore abbiamo preso in considerazione uno scenario astratto dalle proprietà intrisinche dei jammer ed abbiamo sintetizzato l'efficienza di quest'ultimi sotto forma di un unico parametro f, detto *failure rate*. Il valore di f comprende molteplici aspetti, variabili da un tipo di implementazione ad un altra: l'abilità di monitoraggio delle trasmissioni, i pattern dei salti di canale ed i problemi di sincronizzazione sono solo alcune variabili che, in ogni caso, se note, possono essere sintetizzate nell'unico parametro che andremo ad utilizzare [15].
In questo capitolo enunceremo i risultati provenienti dalla *game-theory* in

due casi differenti e verificheremo, tramite l'utilizzo del simulatore, la loro effettiva veridicità. Quanto dimostreremo tramite questa procedura sarà di fondamentale importanza per ottenere i risultati finali.

3.3 Analisi degli scenari

Gli scenari che andremo ad analizzare, riferiti ad una implementazione wireless *locale*, come possono essere dei campus universitari, la quale è messa a rischio da degli attacchi portati da un nodo malevolo esterno, il cui accesso alla rete stessa non dovrebbe essere permesso. Per poter contrastare tali intrusioni, verrà analizzata l'implementazione di uno o più dispositivi jammer atti alla monitorizzazione dei canali di trasmissione. Tali nodi risultano essere in grado, in caso di rilevata attività malevola, di attivarsi per reagire all'intrusione [83]. Per modellare tale scenario utilizzeremo un modello *Entry Game* [84] dato che, quanto accade, può essere riassunto come un modello economico nel quale:

- I jammer spendono ognuno una quantità fissa c per effettuare la loro azione di interferenza;
- Il nodo malevolo spende, per tentare l'intrusione nella rete, la stessa quantità c;
- Nel caso in cui il nodo malevolo riesca ad infiltrarsi con successo, esso riceverà un premio, definito *reward*, rappresentato dal parametro r_m;

– Nel caso in cui i jammer riescano a bloccare l'intrusione riceveranno anch'essi un reward detto r_j e solitamente posto uguale a 1;

– La probabilità che il jammer rilevi l'azione malevola e che, nel tentativo di interromperla, fallisca, è rappresentata dalla *failure rate f.*

3.3.1 Caso d'implementazione singolo jammer

In questo primo caso andremo a prendere in considerazione un gioco, di cui conosciamo tutte le informazioni, tra il jammer N ed il nodo malevolo M. Quest'ultimo tenterà di eseguire delle trasmissioni non autorizzate mentre N monitorerà il canale di comunicazione e cercherà di impedire il successo di tali tentativi.
Definendo in tale maniera il gioco, stiamo assumendo il nodo N come un jammer *reattivo* [35] in grado di rilevare completamente la situazione, ed il nodo M come un nodo malevolo, anch'esso a conoscenza dello stato completo del nostro setup: stiamo quindi affermando che *entrambi i giocatori sono mutualmente a conoscenza dell'avversario e del suo obiettivo* [15].
Ogni nodo tenterà, indipendentemente, di massimizzare il proprio payoff, andando a modificare il proprio comportamento in maniera tale da avere la migliore risposta alla strategia utilizzata dall'avversario.

*Possibili azioni del Jammer **N**:*	**J**: il friendly jammer *genera* interferenza. **A**: il friendly jammer *rimane spento.*
*Possibili azioni del Nodo Malevolo **M**:*	**E**: l'intruso *prova* ad entrare nella rete. **O**: l'intruso *rimane dormiente.*

Tabella 1: *Le possibili azioni che i due attori del nostro gioco possono effettuare.*

Date le possibili azioni nella tabella 1 abbiamo che, per ogni attore, esisterà una *best response* in relazione a ciò che viene giocato dall'avversario: se il nodo malevolo pensa che il jammer sia attivo, la sua miglior risposta risulterà essere **O**, dato che, così agendo, non pagherà il costo della trasmissione, mentre, all'opposto, se pensa che il nodo N sia dormiente gli converrà giocare **E**, ovvero tentare un'intrusione. Analogamente, possiamo andare a definire le best response del jammer in risposta all'azione del nodo malevolo M (**J** in risposta a **E** ed **A** in risposta a **O**), andando a definire per entrambi i nodi, una strategia formata dalla mistura delle loro possibili azioni, in maniera tale da massimizzare il *guadagno* e di minimizzare, nel contempo, i *costi.*
La scelta della strategia da attuare, avviene indipendentemente per ogni giocatore, il che definisce il variare dei loro payoff μ_x per ogni possibile coppia di azioni (n, m).
Possiamo quindi formulare un entry game *statico*, il quale concentri tutte le possibili combinazioni tra questi attori, in una sola iterazione:

		Nodo malevolo M: **E**	Nodo malevolo M: **O**
Jammer N	**J**	$\mu_N = (1-f) - fr - c$ $\mu_M = fr - c$	$\mu_N = -c$ $\mu_M = 0$
	O	$\mu_N = -r$ $\mu_M = r - c$	$\mu_N = 0$ $\mu_M = 0$

Tabella 2: *Tutte le possibili combinazioni di azioni con i loro relativi payoff. Notare che, se il nodo malevolo si inserisce con successo nella rete il suo payoff è pari al reward r meno il costo della trasmissione c, mentre se il jammer si attiva quando è in corso un'intrusione il suo payoff dipende strettamente dalla sua failure rate f.*

Risultati teorici

I risultati mostrati nella tabella 2, ricavati con il valore di r_j fissato a 1, insieme alle considerazioni fatte precedentemente, ci permettono di affermare, utilizzando le definizioni provenienti dalla game theory, che non esiste un *equilibrio di Nash* con *strategia pura.*

Richiamando tuttavia il Teorema di Nash [85], si osserva che deve allora esistere un equilibrio a *strategia mista*, dove N gioca l'azione **J** con probabilità j e l'azione **A** con probabilità $1 - j$ mentre M sceglie **E** con una probabilità ϵ e **O** con $1 - \epsilon$.

Innanzitutto, va fatto notare, che le definzioni inserite nella tabella 2, richiedono una condizione "d'esistenza" per poter essere considerate veritiere:

$$fr \leq c \leq r \quad \rightarrow \quad f \leq \frac{1 + r - c}{1 + r} \tag{3.1}$$

Se la (3.1) non è infatti verificata, la strategia di M diventa ovvia, rendendo **E** oppure **O** azioni dominanti.

Per poter ricavare i valori delle probabilità j ed ϵ in forma chiusa si fa riferimento ad un teorema, derivante dal *Princio di Indifferenza* [85], che attesta l'uguaglianza tra i seguenti valori attesi:

$$\mathbb{E}[\mu_N(0,\epsilon)] = \mathbb{E}[\mu_N(1,\epsilon)] \tag{3.2}$$

$$\mathbb{E}[\mu_M(j,0)] = \mathbb{E}[\mu_M(j,1)] \tag{3.3}$$

Utilizzando questi vincoli stiamo, di fatto, imponendo che, data una probabilità ϵ di trasmettere per M, il payoff atteso di N abbia lo stesso valore sia che quest'ultimo scelga di giocare **J** oppure **A**. Allo stesso tempo stiamo affermando che, data la probabilità j, il payoff di M sia uguale, sia nel caso che giochi **E** sia che scelga **O** [15].

Dallo sviluppo delle (3.2) e (3.3), otteniamo:

$$\epsilon = \frac{c}{(1+r)(1-f)} \tag{3.4}$$

$$j = = \frac{1-c/r}{1-f} \tag{3.5}$$

Questi risultati, come è possibile osservare delle definizioni (3.4) e (3.5), dipendono interamente dai valori assunti dai parametri c, r *e* f utilizzati per modellare la nostra situazione.

Se il costo c aumenta, il nodo M tenderà ad essere *maggiormente attivo* a

causa della diminuzione della probabilità j, dovuta agli alti costi a cui il jammer deve far fronte nel caso decida di intervenire.
Ciò che più sorprende è l'impatto che il reward r ha sulle probabilità dei vari giocatori: all'aumentare del premio per un'intrusione riuscita, la probabilità ϵ del nodo M andrà a diminuire, a causa della maggiore probabilità che si ha nel trovare il jammer acceso (la componente c/r presente al numeratore della definizione di $j \to 0$ se r aumenta).

Risultati sperimentali

Per verificare i valori ottenuti matematicamente in (3.4) e (3.5), si è utilizzato un simulatore progettato in maniera tale da "imitare" la situazione precedentemente descritta del caso a singolo jammer.
L'approccio utilizzato prevede l'esecuzione di un numero molto alto di *giochi single shot* per ogni coppia di probabilità (j, ϵ) dai quali, in base alle azioni che vengono scelte dal nodo N ed il nodo M, si procede con il calcolo delle relative matrici di payoff.
L'algoritmo implementato è stato realizzato con l'obiettivo di raggiungere la massima precisione possibile ed è riassumibile nei seguenti passaggi:

1. Dati i valori operativi *f,r* e *c* si ricavano i valori teorici j_{th} ed ϵ_{th} su cui centrare l'algoritmo

2. Ottenuti (j_{th}, ϵ_{th}) si procede alla definizione di un intervallo centrato su di essi, andando a definire $(j_{th} \pm \Delta j)$ e $(\epsilon_{th} \pm \Delta\epsilon)$

3. Per ogni coppia di valori (j, ϵ) compresi in questo intervallo (presi a valori distanziati da un fattore fisso, definito dalla variabile *step*) ven-

gono giocati un numero T di giochi e viene definito il valore da inserire nella matrice del payoff

4. Per stabilire i valori delle probabilità all'equilibrio si procede analizzando quale sia, per ogni possibile valore j (ϵ), la ϵ (j) tale da massimizzare il payoff del nodo malevolo (jammer).

5. L'andamento delle due probabilità, riportato in un grafico a due dimensioni, presenta un unico punto di interesezione, rappresentante i valori (ϵ, j) relativi all'equilibrio.

Viene qui di seguito riportato un grafico ottenuto da una simulazione effettuata utilizzando l'algoritmo appena descritto dove sono riportati i valori ottenuti:

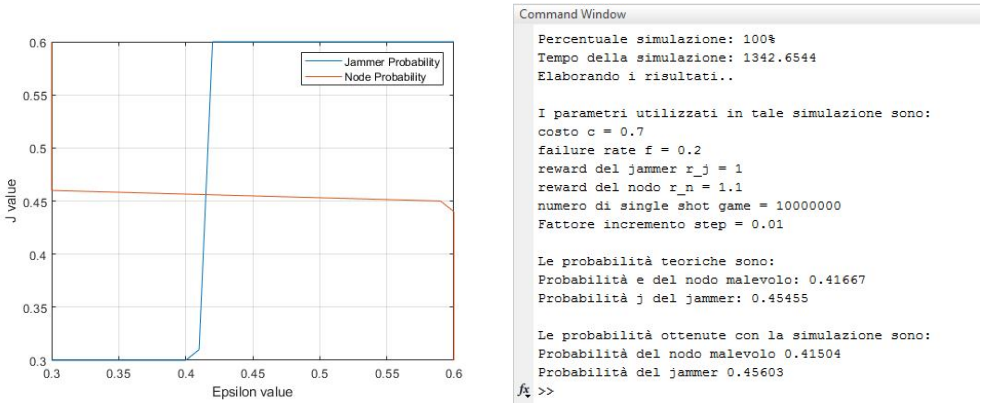


Figura 8: *Esempio di simulazione eseguita con i vettori probabilità centrati intorno ai valori teorici dove sono stati utilizzati $f = 0.2$; $r = 1.1$; $c = 0.7$.*

3.3.2 Caso d'implementazione di due jammer

L'analisi svolta nella sezione precedente può essere estesa al caso di utilizzo di molteplici jammer. Per semplicità di trattazione analizzeremo la situazione comprendente due jammer dato che, l'espansione ad eventuali jammer aggiuntivi, può essere direttamente derivata sfruttando lo stesso tipo di approccio che analizzeremo di seguito.

Gli attori compresi in questo nuovo setup sono i due jammer N_1, N_2 ed il nodo malevolo M i quali, come in occasione del gioco a singolo jammer, hanno come azioni possibili, rispettivamente, **J** ed **A** per N_1 N_2 e **E** ed **O** per M.

I jammer implementati, i quali agiscono con il comune scopo d'impedire l'intrusione del nodo malevolo nella rete, sono detti *strategici*.

Ciò deriva dal fatto che un jammer preferisce, se l'altro è attivo, rimanere dormiente e risparmiare cosi il costo della trasmissione c.

I due jammer in questa simulazione sono considerati tra loro *identici*, ovvero con lo stesso *costo di trasmissione* c e la stessa *failure rate* f.

L'assunzione di un valore di failure rate f unico per i due jammer potrebbe essere, perlomeno, discutibile, in quanto il successo di un'azione d'interferenza dipende da molti fattori tra cui, per esempio, la posizione dei nodi [83]. In ogni caso, il valore di f preso in considerazione in questo elaborato risulta essere una stima media e non il preciso valore di una singola istanza.

Risultati teorici

Per poter ottenere i valori di (ϵ, j) relativi all'Equilibrio di Nash in questa nuova condizione bisogna, prima di tutto, definire la matrice che servirà

per la valutazione dei diversi payoff $\mu_x(n_1, n_2, m)$. La matrice in questione può essere estrapolata espandendo, da due a tre dimensioni, la Tabella 2 ed andando a considerare independente l'azione d'interferenza dei due jammer (quando entrambi sono accesi, il *failure rate* è quindi pari a f^2) [15].
Supponiamo ora di vincolare la nostra situazione all'azione scelta dal nodo N_1. Otteniamo così due possibili scenari:

Caso 1: N_1 gioca **A**, N_2 è l'unico jammer che potenzialmente può opporsi all'intrusore.

		Nodo malevolo M	
		E	**O**
Jammer N_1 N_2	**J**	$\mu_{N_1} = (1-f) - fr$ $\mu_{N_2} = (1-f) - fr - c$ $\mu_M = fr - c$	$\mu_{N_1} = 0$ $\mu_{N_2} = -c$ $\mu_M = 0$
	A	$\mu_{N_1} = -r$ $\mu_{N_2} = -r$ $\mu_M = r - c$	$\mu_{N_1} = 0$ $\mu_{N_2} = 0$ $\mu_M = 0$

Tabella 3: *Payoff calcolati con N_1 spento ed N_2 che varia tra **J** ed **A**.*

Caso 2: N_1 gioca **J**: ho sempre un jammer attivo che "vigila" e, potenzialmente, posso avere due jammer ad opporsi ad eventuali tentativi di intrusione.

		Nodo malevolo M	
		E	**O**
Jammer N_1 N_2	**J**	$\mu_{N_1} = (1-f^2) - fr^2 - c$ $\mu_{N_2} = (1-f^2) - f^2r - c$ $\mu_M = f^2r - c$	$\mu_{N_1} = -c$ $\mu_{N_2} = -c$ $\mu_M = 0$
	A	$\mu_{N_1} = (1-f) - fr - c$ $\mu_{N_2} = (1-f) - fr$ $\mu_M = fr - c$	$\mu_{N_1} = -c$ $\mu_{N_2} = 0$ $\mu_M = 0$

Per poter estrarre in forma chiusa le definizioni di (ϵ, j), come fatto per il caso precedente, si fa uso della *simmetria* dei due jammer ovvero, imponiamo che entrambi giocheranno l'azione **J** con la stessa probabilità j. Così facendo possiamo procedere utilizzando lo stesso teorema sfruttato in 3.1.1, sul nodo M ed ottenendo:

$$\mathbb{E}[\mu_M(j, j, 0)] = \mathbb{E}[\mu_M(j, j, 1)] \tag{3.6}$$

Con l'obiettivo di ricavare dei risultati simili a quelli ottenuti in (3.4)(3.5), calcoliamo il valore del payoff per M, tenendo in considerazione che, come si nota dalla (3.6), esso dipende da *entrambe le azioni scelte dai jammer*, ottenendo:

$$j^2\left(f^2r - c\right) + 2j\left(1-j\right)\left(fr - c\right) + \left(1-j^2\right)\left(r - c\right) = 0$$

da cui:

$$j \quad = \quad \frac{1 - \sqrt{c/r}}{1 - f} \tag{3.7}$$

La definizione appena trovata differisce dalla (3.5) per l'elemento c/r che,

in questa seconda situazione, appare sotto radice quadrata, portando con se alcune considerazioni e variazioni sul comportamento finale in questo secondo caso di molteplici jammer:

- la radice quadrata al numeratore della definizione compare a causa della presenza di due jammer *non coordinati* [86] e porta, dato che solitamente $c/r \leq 1$, ad una diminuzione della probabilità j;
- un valore molto alto del costo di trasmissione porta, contro logica, ad una variazione minima nella funzione (3.7) rispetto alla (3.5). Questo accade a causa del fatto che, i jammer, essendo *non coordinati*, ipotizzano che, con un alto valore di c, l'altro jammer rimanga dormiente [15].

Analogamente a quanto fatto con la probabilità j, vogliamo ricavare una relazione per l'ϵ di quilibrio simile alle (3.4). Per fare questo, applichiamo nuovamente il Teorema dell'Indifferenza alle aspettazioni di entrambi i jammer N_1 N_2:

$$\begin{aligned} \mathbb{E}[\mu_{N_1}(0, j, \epsilon)] &= \mathbb{E}[\mu_{N_1}(1, j, \epsilon)] \\ \mathbb{E}[\mu_{N_1}(0, j, \epsilon)] &= \mathbb{E}[\mu_{N_1}(1, j, \epsilon)] \end{aligned} \tag{3.8}$$

$$\epsilon \quad = \quad \frac{\sqrt{c/r}}{(1-f)(1+r)} \tag{3.9}$$

dove, il c della (3.4), è stato sostituito dallo stesso fattore $\sqrt{c/r}$. Un risultato molto importante, derivante dall'implementazione di due jammer come nello scenario sopra descritto, può essere ottenuto analizzando l'influenza che la presenza di un "nodo alleato" ha sulle scelte operate da un jammer. Andando infatti a valutare l'aspettazione del payoff di ogni singolo jammer si ottiene

che:

$$\mathbb{E}[\mu_{N_i}(j,j,\epsilon)] \quad = \quad \frac{1}{1-f}\left(\frac{\sqrt{cr}}{1+r} - c\right) \tag{3.10}$$

Tale parametro risulta assumere valori positivi se $c < (1+r)^2$ fornendoci le seguenti considerazioni [15]:

- il gioco così descritto presenta una *soglia* $\gamma = r/(1+r)^2$ per il costo di trasmissione. Il payoff dei jammer risulterà essere positivo per valori di $c < \gamma$;
- quanto detto sopra, dovuto al fatto che un jammer può ricevere un *reward* anche rimanendo dormiente, comporta la sostenibilità del gioco da parte dei jammer se il *costo di trasmissione* c risulta essere circa 5 volte inferiore al valore di r_j.

Risultati sperimentali

Come approfondito nella parte teorica e come già fatto nell'analisi dei dati provenienti dalla simulazione del caso a singolo jammer, lo scopo era di valutare i valori dei payoff per ogni singolo attore facente parte dello scenario. L'espansione del modello teorico utilizzo da bidimensionale a tridimensionale è stato quindi implementato nel simulatore stesso il cui scopo rimaneva, in ogni caso, l'imitazione di molti *single shot game*, indispensabili per la valutazione delle varie matrici di payoff: se, mentre nel caso a singolo jammer, ognuno dei due attori presentava una matrice $N \times M$ (dove n ed m erano

determinati da $S_v/step$, con S_v span del vettore di probabilità dell'attore in analisi), in questa versione modificata, ogni attore presentava una matrice $N \times N \times M$.

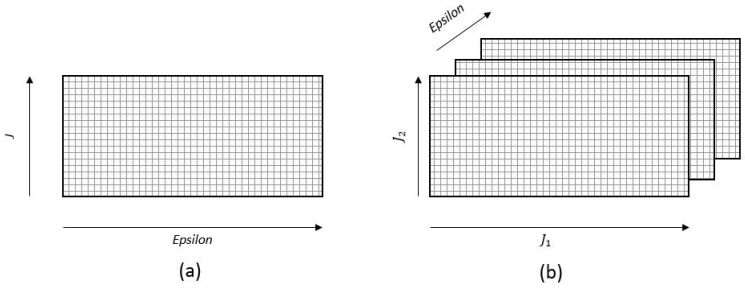


Figura 9: *Le differenze tra le matrici dei payoff tra gioco a singolo (a) ed a doppio (b) jammer.*

L'estensione delle matrici di payoff ha, tuttavia, sortito un effetto negativo sul livello di complessità computazionale richiesta per la simulazione: quanto avevamo precedentemente ottenuto andando a diminuire lo span dei vettori di probabilità di j ed ϵ viene qui perso, andando ad inficiare sulla precisione finale dei risultati.

Considerando la proprietà di simmetria dei jammer introdotto nella situazione descritta precedentemente, i nodi N_1 ed N_2 risultavano giocare l'azione **J** con la stessa probabilità j. Nel ricavare i valori sperimentali delle probabilità d'equilibrio ci siamo quindi limitati alla sola valutazione dei valori presenti nelle *diagonali* delle tabelle formanti la matrice del payoff.

Alcuni risultati delle simulazioni ottenuti sono:

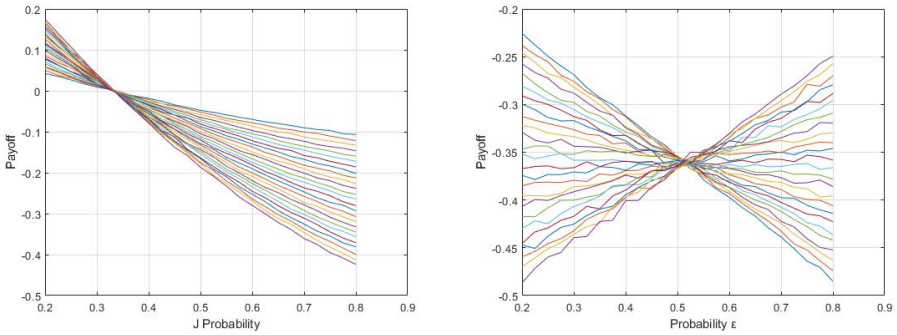


Figura 10: *Simulazione con f=0.2; r=1.3; c=0.7; T=100000; step= 0.25* $(j,\epsilon)_{teor} = (0.333; 0.518)$ $(j,\epsilon)_{sper} = (0.334; 0.511)$

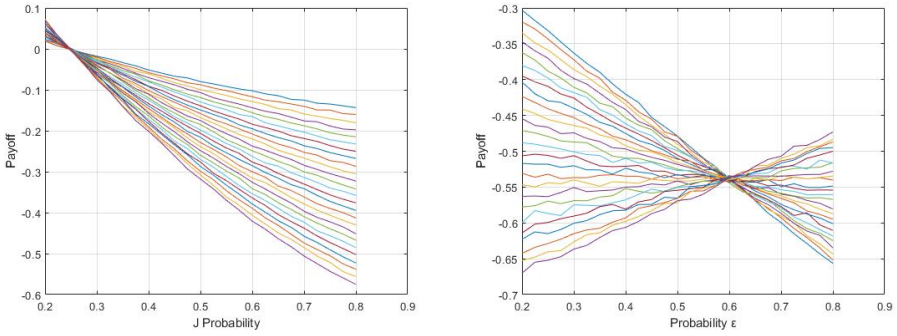


Figura 11: *Simulazione con f=0.2; r=1.4; c=0.9; T=100000; step= 0.25* $(j,\epsilon)_{teor} = (0.248; 0.585)$ $(j,\epsilon)_{sper} = (0.248; 0.595)$

Capitolo 4

Analisi dell'equilibrio

Nella realizzazione del modello game teorico e nel suo successivo impiego per lo studio dell'equilibrio nelle applicazioni delle tecniche di friendly jamming, i parametri presi in considerazione sono stati gli stessi utilizzati nella verifica dei risultati teorici :

- il *costo* di trasmissione $\boldsymbol{c}$, il quale rappresenta il dispendio di risorse di un qualunque nodo intenda effettuare una trasmissione;

- il *reward* del nodo malevolo $\boldsymbol{r_M}$, il quale sintetizza l'eventuale guadagno che, una riuscita intromissione nella comunicazione, porta al nodo malevolo, sia esso dovuto al danno provocato oppure all'intercettazione dell'informazione;

- il *reward* $\boldsymbol{r_J}$, solitamente posto uguale a uno, assegnato ai singoli jammer nel caso di riuscita difesa della rete da un effettivo tentativo di intrusione;

– le probabilità $\boldsymbol{\epsilon}$ e $\boldsymbol{j}$, modellanti, rispettivamente, le attività del nodo malevolo e dei jammer.

Ognuno di questi parametri realizzativi influenza, in maniera differente, il punto d'equilibrio che, un sistema analizzato con i principi precedentemente esposti, raggiunge, sia un termini di probabilità che di payoff dei singoli nodi. La causa di questa forte, ma al contempo, variabile correlazione è da ricercare rispettivamente nelle definizioni *(3.4)* e *(3.5)* per lo scenario a singolo jammer e nelle *(3.7)* e *(3.9)* per quello a due jammer.
A causa di queste relazioni infatti, in ogni set-up preso in considerazione, la variazione di uno di questi parametri, unita alle caratteristiche intrinseche dei dispositivi implementati, produrrà un variazione sulle condizioni di operatività del sistema di diversa entità: osserveremo leggeri spostamenti del punto di equilibrio, completi stravolgimenti di quest'ultimo oppure il raggiungimento di condizioni di lavoro insostenibili per uno degli attori in gioco.

4.1 Variazioni del costo c di trasmissione

Il costo di tramissione c è un parametro che influenza nello stesso modo sia l'azione dei jammer che l'attività del nodo malevolo dato che, un aumento di quest'ultimo, può essere considerato applicato a tutti gli attori in gioco.
Per comprederne meglio la natura, e le motivazioni presenti nella sua presa in considerazione, prendiamo in analisi un semplice scenario di tramissione uni-laterale che ha luogo tra i nodi sensori appartenenti ad una rete *WSN* ed il *gateway* della rete che provvederà poi ad inoltrare l'informazione ricevuta al *server data collector*.

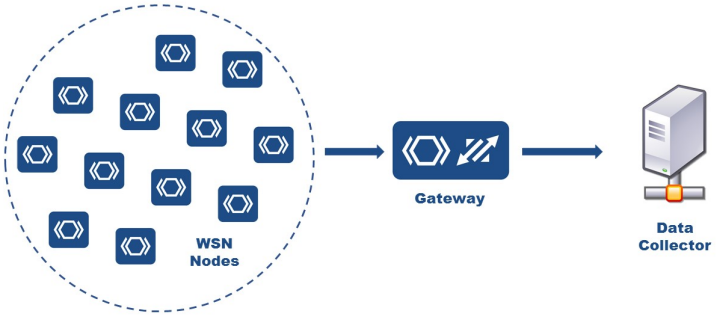


Figura 12: *Rappresentazione dello schema di una rete WSN.*

La generazione e la trasmissione del segnale RF da parte del dispositivo sensoristico, ovvero la parte *analogica* della comunicazione, sono strettamente collegate al consumo energetico di componenti come *amplificatori di potenza* o *sintonizzatori di frequenza* i quali, a differenza delle componenti logiche, comportano un notevole dispendio energetico [33].

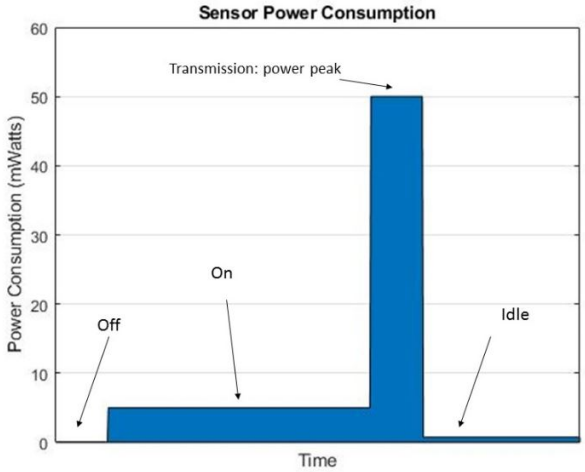


Figura 13: *Grafico rappresentante il consumo di potenza di un sensore [87].*

Data la natura prettamente *fisica* di questa operazione, il dispendio energetico di tutti gli attori presenti nei nostri scenari sono assunti uguali: i jammer ed i nodi malevoli quindi fanno fronte ad un *costo* pari al parametro **c** ogni qualvolta optino, rispettivamente, per un'azione di jamming ed una d'intrusione.

Nelle sottosezioni successive vengono analizzati gli effetti che, la variazione di questo parametro, ha sugli equilibri di scenari differenti, dall'implementazione a singolo jammer a quella a doppio jammer, passando per nodi *intelligenti* che reagiscono a tali variazioni oppure a nodi *statici* che mantengono il loro punto di lavoro nonostante le nuove condizioni operative.

La variazione dei costi di trasmissione per un nodo possono avvenire a causa di svariati motivi, tra cui:

- l'implementazione di protocolli di trasmissione specificatamente progettati, come per esempio il ***Data Transmission Protocol for Sensors Networks*** (D.a.T.) [88], i quali permettono di ridurre, fino quasi a dimezzare, i costi di trasmissione;

- la presenza di un segnale di interferenza agente nella *lof* (line of sight) obbliga, con l'obiettivo di mantenere un dato valore di SNR, a dover trasmettere con una potenza maggiore rispetto a quella precendente, causando un aumento del costo c.

- la non ottimizzazione del flusso di dati oppure la cattiva gestione del canale d'accesso (per esempio dei nodi verso il gateway) può portare ad un aumento del tempo necessario per compiere con successo la trasmissione dei dati, causando quindi un incremento di c.

4.1.1 Implementazione a singolo jammer

Per ottenere i risultati sullo scenario a singolo jammer è stato utilizzato lo stesso simulatore sfruttato per verificare i dati teorici delle *(3.4)* e *(3.5)* nel quale, il valore di c, è stato fatto variare da un valore $c_{min} = 0.3$ ad un valore massimo di $c_{max} = 0.8$, in maniera tale da poterne analizzare gli effetti di variazione su parametri di riferimento come il ***payoff*** e, nel caso di dispositivi intelligenti, anche delle ***probabilità*** ϵ e j.

Prima Simulazione

Reward r	*Failure rate f*	*Costo c minimo*	*Costo c dichiarato*	*Costo c massimo*	Δc	*J Teorico*	ϵ *Teorico*
1.1	*0.2*	*0.3*	*0.7*	*0.8*	*0.05*	*0.45*	*0.42*

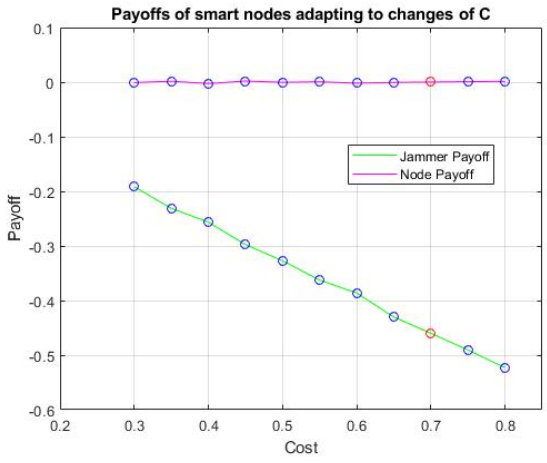


Figura 14: *Evoluzione dei payoff del nodo malevolo e del jammer. Il pallino rosso identifica i valori dei payoff di riferimento.*

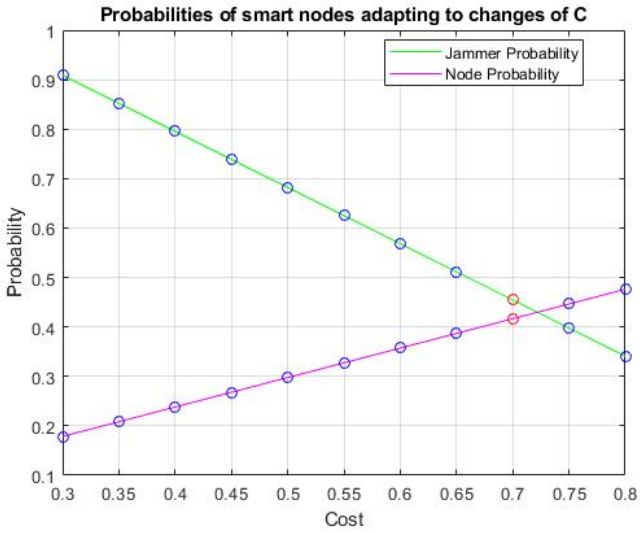


Figura 15: *Evoluzione delle probabilità di equilibrio di attività del nodo malevolo e del jammer. Il pallino rosso identifica i valori di riferimento ottimali delle probabilità.*

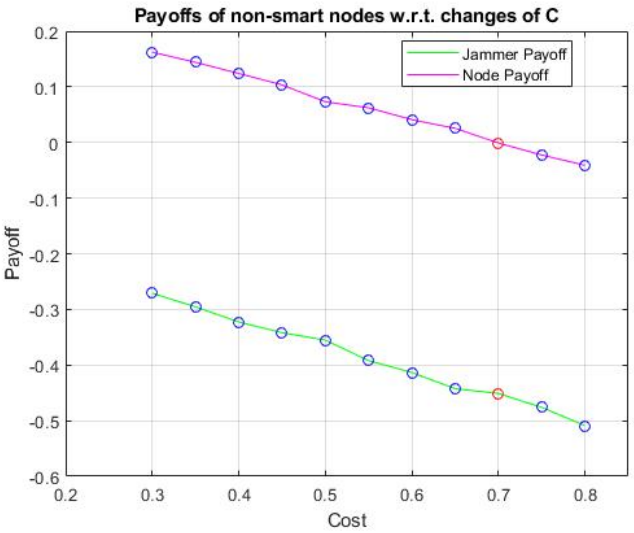


Figura 16: *Evoluzione dei payoff del nodo malevolo e del jammer, al variare del costo c, se quest'ultimi si comportano come dispositivi statici, mantenendo costanti le loro probabilità.*

Seconda Simulazione

Reward r	*Failure rate f*	*Costo c minimo*	*Costo c dichiarato*	*Costo c massimo*	Δc	*J Teorico*	ϵ *Teorico*
0.9	*0.1*	*0.3*	*0.5*	*0.8*	*0.05*	*0.61*	*0.34*

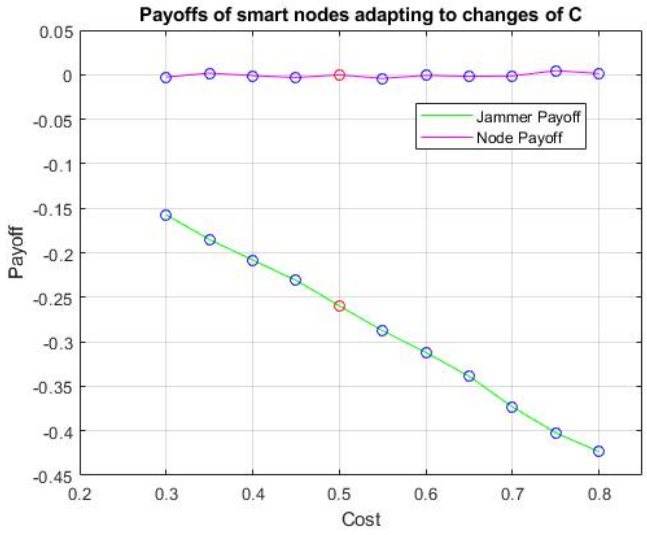


Figura 17: *Evoluzione dei payoff del nodo malevolo e del jammer. Il pallino rosso identifica i valori dei payoff di riferimento.*

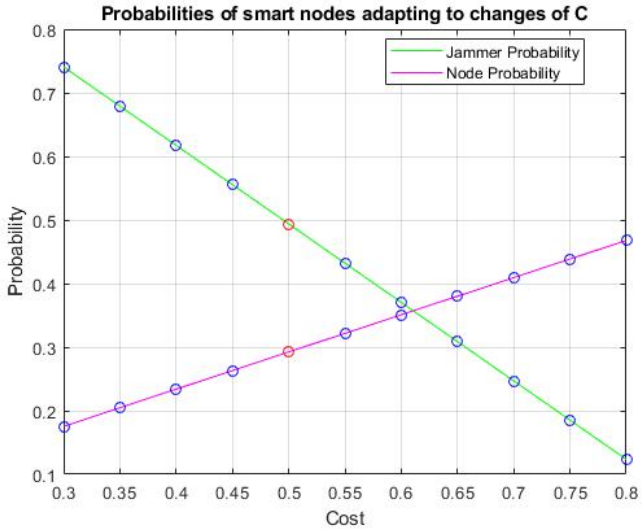


Figura 18: *Evoluzione delle probabilità di equilibrio di attività del nodo malevolo e del jammer. Il pallino rosso identifica i valori di riferimento ottimali delle probabilità.*

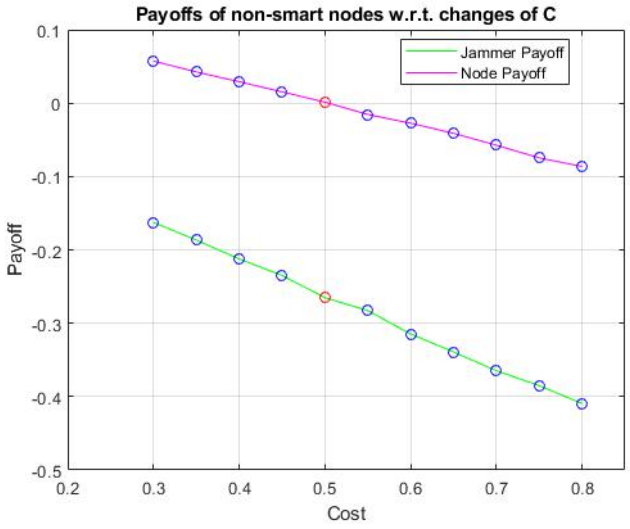


Figura 19: *Evoluzione relativa ai payoff del nodo malevolo e del jammer, al variare del costo c, se quest'ultimi si comportano come dispositivi statici, mantenendo costanti le loro probabilità.*

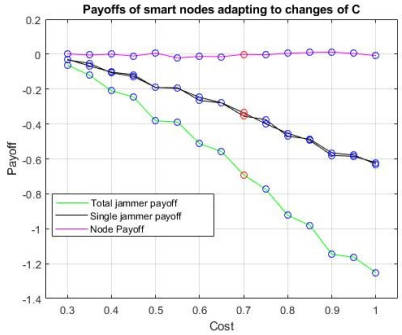
4.1.2 Implementazione a due jammer

Per lo scenario implementativo a due jammer è stato utilizzato lo stesso simulatore impiegato nella verifica dei risultati raffigurati in *(3.7)* e *(3.9)* nel quale il valore del parametro c variava da un valore c_{min} ad un valore c_{max} in maniera tale da poterne analizzare gli effetti sull'equilibrio.

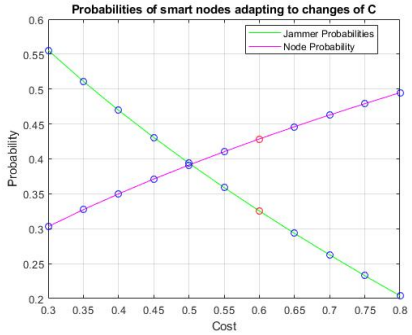
In questo tipo di implementazione, in aggiunta a tutte le casistiche viste nel caso a singolo jammer, viene analizzata anche la possibilità che solamente uno dei due jammer sia reattivo e che quindi, solamente quest'ultimo, possa modificare il proprio comportamento.

Prima Simulazione

Reward r	*Failure rate f*	*Costo c minimo*	*Costo c dichiarato*	*Costo c massimo*	Δc	*J Teorico*	ϵ *Teorico*
1.2	*0.1*	*0.3*	*0.6*	*0.8*	*0.05*	*0.33*	*0.43*

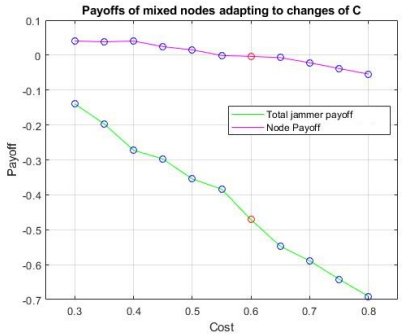


(a) *Evoluzione dei payoff.*

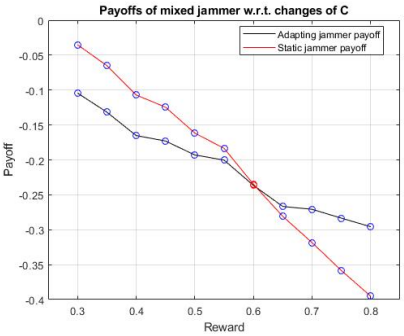


(b) *Evoluzione delle probabilità.*

Figura 20: *Variazioni su nodi smart che si adattano alla variazione di c*



(a) *Evoluzione dei payoff.*



(b) *Evoluzione dei payoff dei singoli jammer.*

Figura 21: *Variazioni dovute alla presenza di un solo jammer adattivo.*

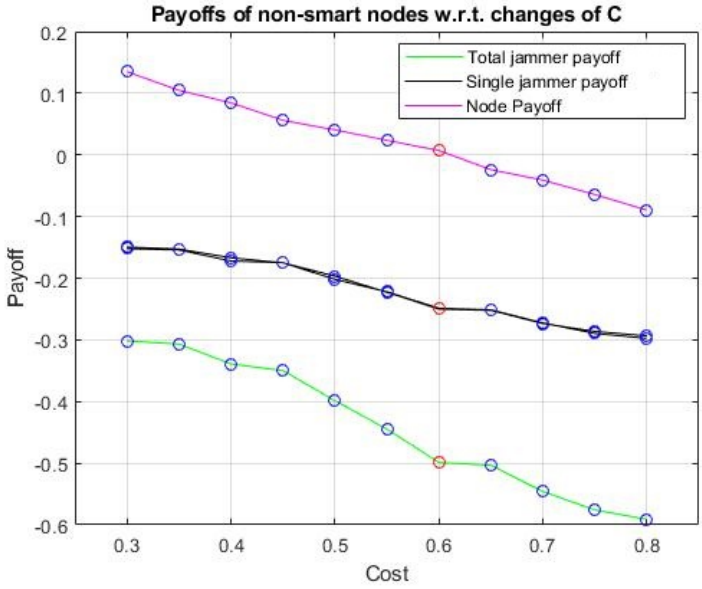
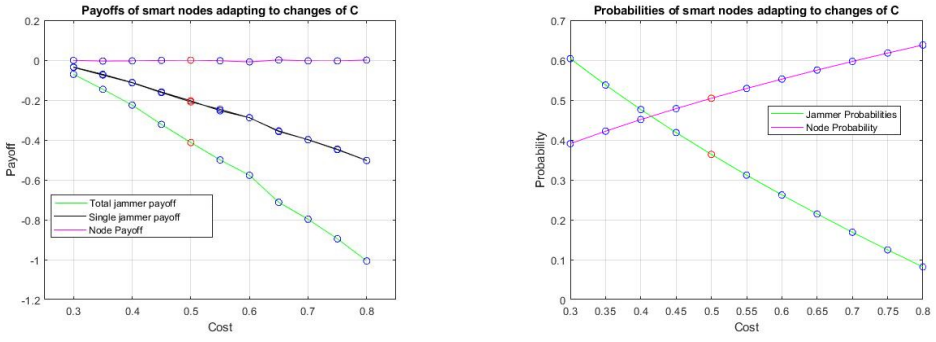


Figura 22: *Valutazione dei payoff nel caso di nodi completamente statici.*

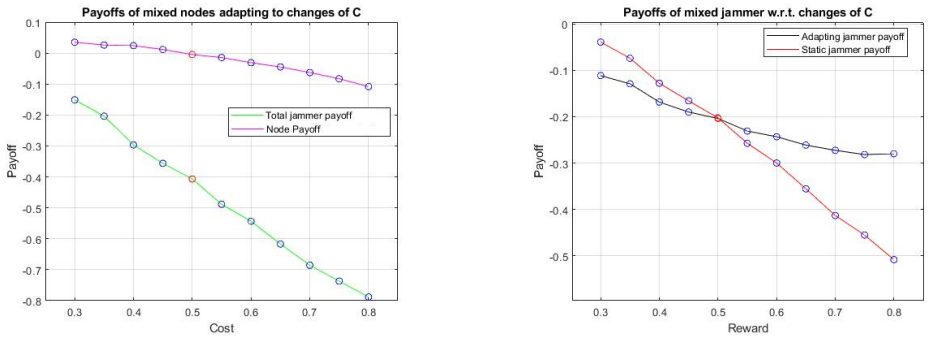
Seconda Simulazione

Reward r	*Failure rate f*	*Costo c minimo*	*Costo c dichiarato*	*Costo c massimo*	Δc	*J Teorico*	ϵ *Teorico*
0.9	*0.3*	*0.3*	*0.5*	*0.8*	*0.05*	*0.36*	*0.50*



(a) *Evoluzione dei payoff.* (b) *Evoluzione delle probabilità.*

Figura 23: *Variazioni su nodi smart che si adattano alla variazione di c*



(a) *Evoluzione dei payoff.*

(b) *Evoluzione dei payoff dei singoli jammer.*

Figura 24: *Variazioni dovute alla presenza di un solo jammer adattivo.*

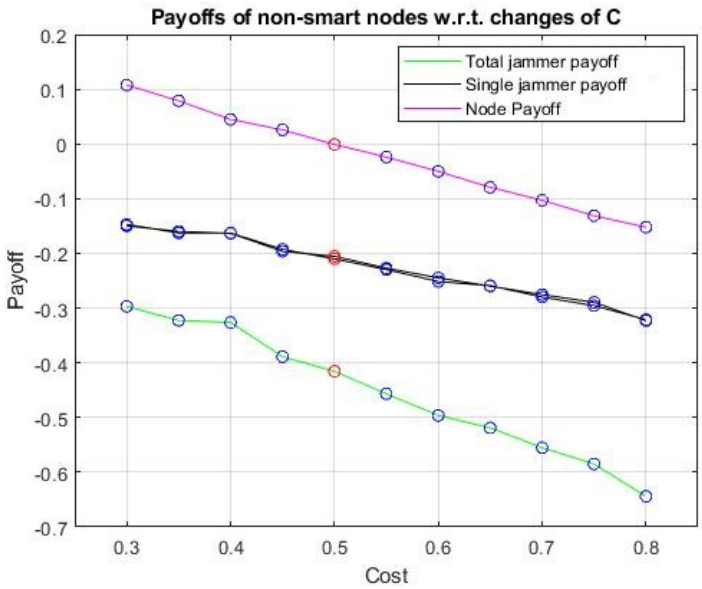


Figura 25: *Valutazione dei payoff nel caso di nodi completamente statici.*

4.2 Variazioni del reward r del nodo malevolo

A differenza di quanto visto con il costo di trasmissione, risulta molto più complesso fornire una definizione unicamente valida di cosa il parametro r_M effettivamente rappresenti.
Dal punto di vista puramente parametrico esso può essere descritto come il *ritorno*, in termini di payoff, che il nodo malevolo M ottiene per ogni trasmissione/intrusione malevola che riesce a compiere con successo.
La natura di questo ritorno però, è da ricercarsi nella tipologia di attività malevola che, grazie a questa trasmissione/intrusione, è stata svolta.
Sono infatti molteplici le motivazioni che possono celarsi dietro un'azione di questo tipo, tra cui:

- ***Denial of Service (DoS)*** [89]: questo tipo di attacco viene portato da un nodo malevolo il cui scopo è quello di saturare le risorse (informatiche e di rete) di un sistema informatico che distribuisce diverse tipologie di servizio.

- ***Injection*** [90]: in questa seconda tipologia di attacchi, lo scopo della trasmissione illecita è quello di aggiungere un flusso esterno di dati nella rete con obiettivo l'inserimento di, per esempio, software malevolo. Nonostante sia oramai molto meno diffuso nelle reti private e/o commerciali (grazie alla protezione delle reti stesse con chiavi d'accesso), rimane un problema di vitale importanza in quelle reti non fornite di una protezione derivante da implementazioni sui layer superiori dello stack ISO/OSI.

- ***Man-In-The-Middle (MitM)*** [91]: un attacco portato secondo quest'approccio prevede che il nodo malevolo si intrometta tra la legittima comunicazione che sta avvenendo tra, per esempio un nodo ed un gateway. Lo scopo è quello di riuscire a sostituirsi ad uno dei due attori originali della rete per poter ricevere e/o inviare informazioni. Ne esistono di varie nature tra cui *IP spoofing, replay* e *session hijacking.*

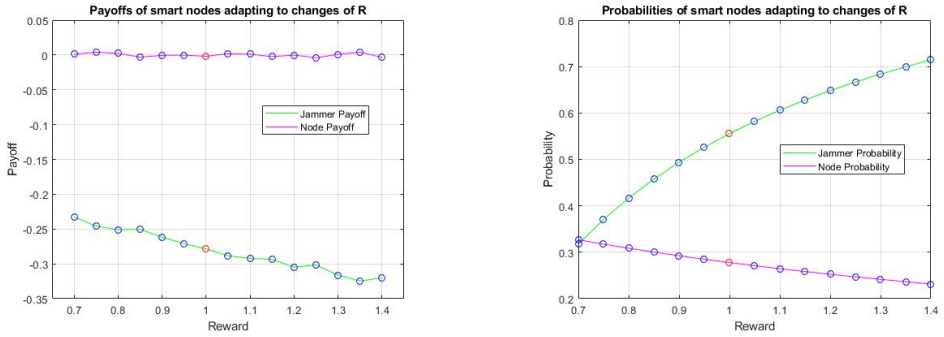
- ***Eavesdropping*** [92]: quest'ultimo tipo risulta essere quello più problematico nelle attuali reti implementate. Esso consiste nel monitoraggio delle informazioni che vengono scambiate dai nodi appartenenti alle reti che, nonostante possano essere protette da chiavi crittografiche, possono sempre essere decifrate in un momento successivo all'intercettazione.

La diversità nelle tipologie di attacco che possono essere portati ad una rete wireless ed i diversi effetti negativi che quest'ultimi comportano rendono, di fatto, impossibile fissare un valore per il coefficiente r che sia standard anche su offensive identiche nella metodologia ma posizionate in lassi temporali differenti. Le informazioni che viaggiano all'interno di una rete possono infatti essere, saltuariamente, di una maggiore importanza rispetto alla media così come la negazione di un servizio può avere effetti diversi a seconda delle richieste e del carico a cui la rete stava facendo fronte nel momento dell'attacco.

4.2.1 Implementazione a singolo jammer

Prima Simulazione

Costo c	*Failure rate f*	*Reward r minimo*	*Reward r stimato*	*Reward r massimo*	Δr	*J Teorico*	ϵ *Teorico*
0.5	*0.1*	*0.7*	*1.0*	*1.4*	*0.05*	*0.56*	*0.28*



(a) *Evoluzione dei payoff.* (b) *Evoluzione delle probabilità.*

Figura 26: *Variazioni su nodi smart che si adattano alla variazione di r*

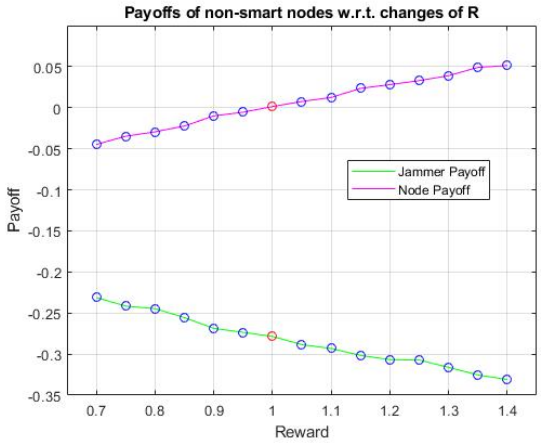
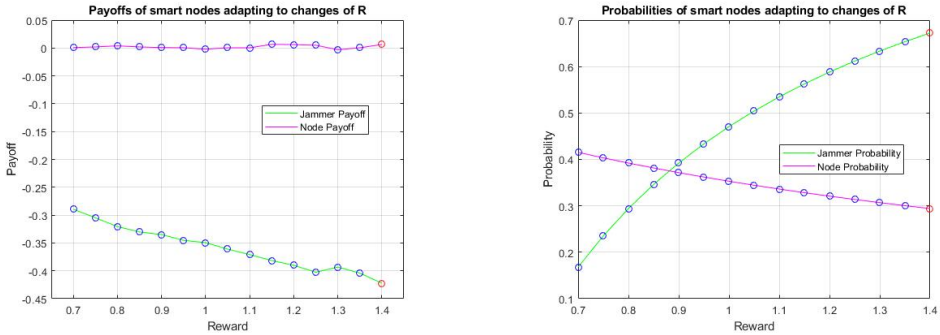


Figura 27: *Variazione del payoff nel caso di nodi statici.*

Seconda Simulazione

Costo c	*Failure rate f*	*Reward r minimo*	*Reward r stimato*	*Reward r massimo*	Δr	*J Teorico*	ϵ *Teorico*
0.8	*0.25*	*0.7*	*1.4*	*1.4*	*0.05*	*0.57*	*0.44*

Tabella 4: *Parametri utilizzati per la seconda simulazione con singolo jammer.*



(a) *Evoluzione dei payoff.* (b) *Evoluzione delle probabilità.*

Figura 28: *Variazioni su nodi smart che si adattano alla variazione di r*

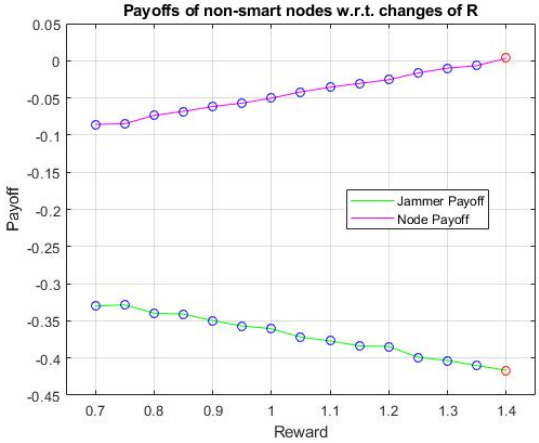
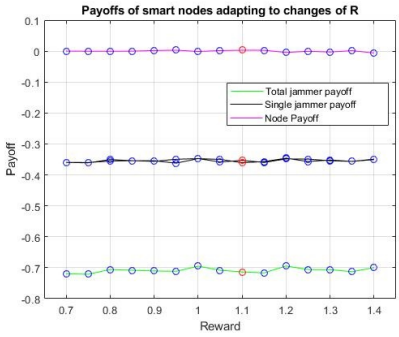


Figura 29: *Variazione del payoff nel caso di nodi statici.*

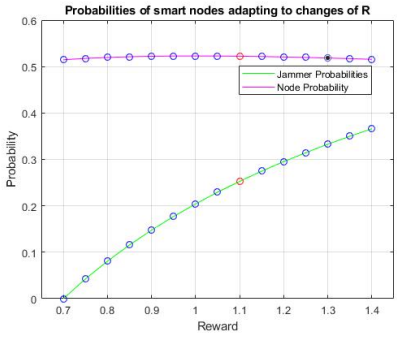
4.2.2 Implementazione a due jammer

Prima Simulazione

Costo c	*Failure rate f*	*Reward r minimo*	*Reward r stimato*	*Reward r massimo*	Δr	*J Teorico*	ϵ *Teorico*
0.7	*0.2*	*0.7*	*1.1*	*1.4*	*0.05*	*0.25*	*0.52*

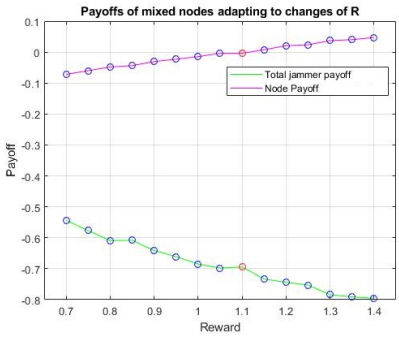


(a) *Evoluzione dei payoff.*

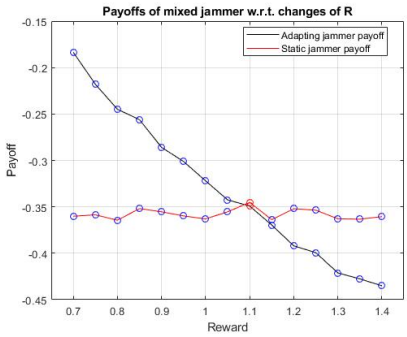


(b) *Evoluzione delle probabilità.*

Figura 30: *Variazioni su nodi smart che si adattano alla variazione di r*



(a) *Evoluzione dei payoff nel caso di un solo jammer adattivo.*



(b) *Andamento dei singoli payoff dei jammer.*

Figura 31: *Variazioni su nodi smart che si adattano alla variazione di r*

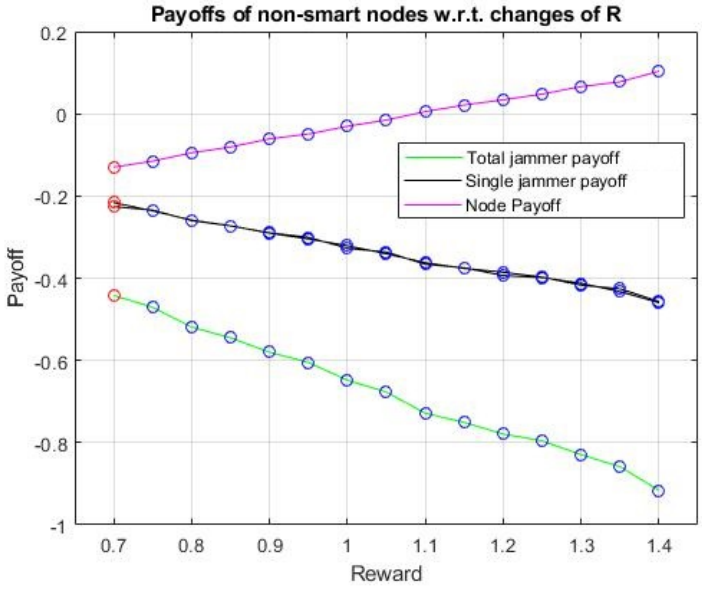
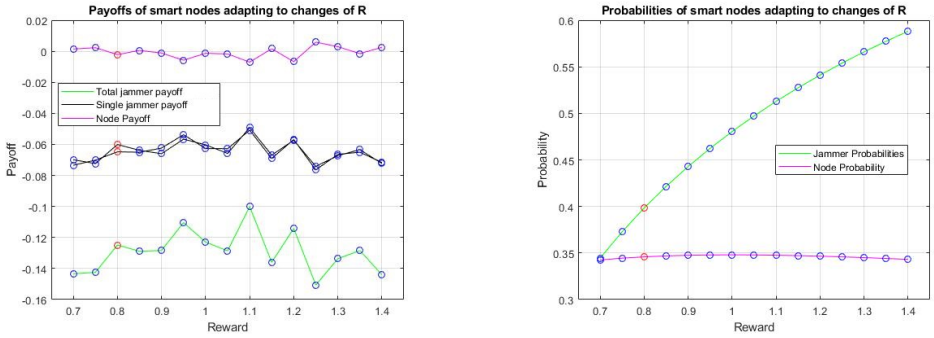


Figura 32: *Valutazione dei payoff nel caso di nodi completamente statici.*

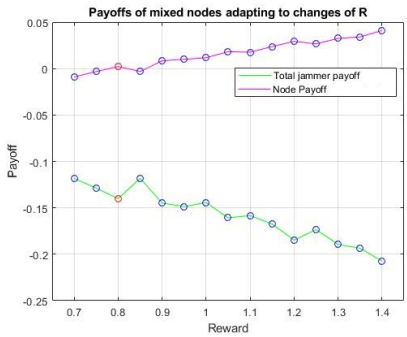
Seconda Simulazione

Costo c	*Failure rate f*	*Reward r minimo*	*Reward r stimato*	*Reward r massimo*	Δr	*J Teorico*	ϵ *Teorico*
0.35	*0.15*	*0.7*	*0.8*	*1.4*	*0.05*	*0.40*	*0.35*

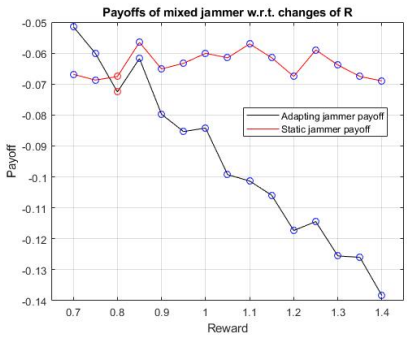


(a) *Evoluzione dei payoff.* (b) *Evoluzione delle probabilità.*

Figura 33: *Variazioni su nodi smart che si adattano alla variazione di r*



(a) *Evoluzione dei payoff nel caso di un solo jammer adattivo.*



(b) *Andamento dei singoli payoff dei jammer.*

Figura 34: *Variazioni su nodi smart che si adattano alla variazione di r*

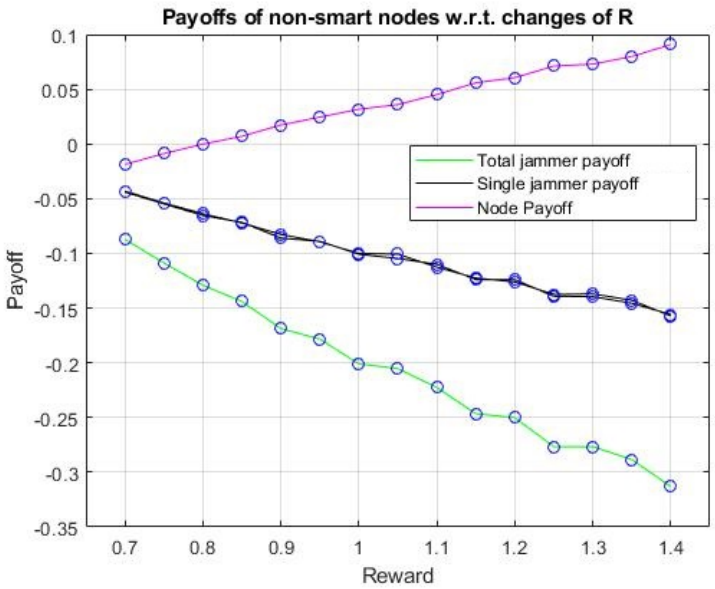


Figura 35: *Valutazione dei payoff nel caso di nodi completamente statici.*

4.3 Variazioni della failure rate *f*

L'analisi del punto di equilibrio al variare della failure rate di uno o più jammer prevede che, nelle implementazioni con molteplici jammer, vengano fatte delle considerazioni sul tipo di realizzazione e installazione fatta.
Un sistema multi-jammer, infatti, può essere concepito in diversi modi che, una volta giunti alla progettazione, si riducono a tre diversi approcci realizzativi, ognuna con i suo vantaggi ed i suoi svantaggi [93]:

- ***Sistema unico o concentrato***: questo sistema risulta essere, dal punto di vista realizzativo, il meno dispendioso, poiché prevede l'implementazione di due componenti analogiche RF su di un singolo dispositivo. In altre parole, utilizzare questo approccio può essere paragonato all'impiego di due antenne collegate allo stesso jammer, le quali vengono orientate in maniera tale da massimizzare il loro range di copertura.
  I vantaggi di questo modus operandi sono, come detto, di natura economica (necessito di una sola componente computazionale) ma anche di *reattività* del sistema. Essendo le due antenne implementate sullo stesso core operazionale, l'aumento del valore della failure rate di una delle due è automaticamente conosciuta anche dall'altra, la quale può quindi reagire per bilanciare gli effetti.
  Gli aspetti negativi sono invece da ricercare nella flessibilità del sistema che, essendo indivisibile, potrebbe incorrere in problemi di copertura dell'intera rete a causa dell'impossibilità nel posizionare le due antenne in posizioni diverse.

- ***Sistema completamente distribuito***: antitesi del sistema unico, questo approccio prevede l'utilizzo di due jammer distinti non comunicanti e non coordinati tra loro. La semplicità implementativa (non si necessita di nessun tipo di algoritmo di bilanciamento) contrasta però con i seri problemi di sostenibilità dell'intero sistema quando, uno dei due jammer si trovi a fronteggiare un aumento della sua failure rate che, per natura stessa dei dispositivi, non può essere notificata all'altro jammer.

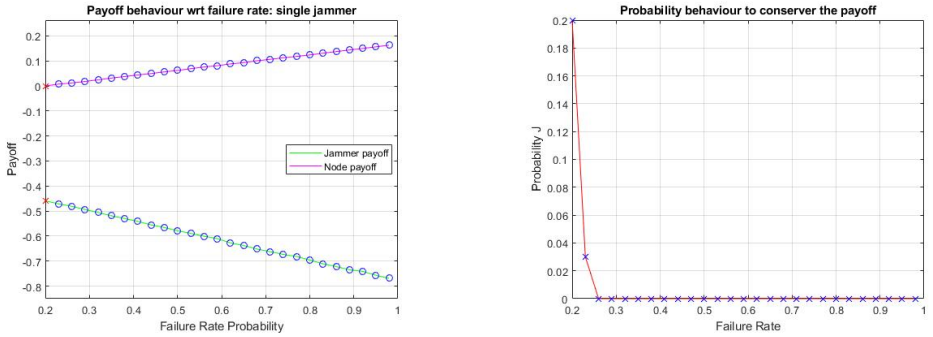
- ***Sistema parzialmente distribuito***: questa proposta è un ibrido tra le due tipologie viste in precedenza. I due jammer risultano essere distinti e posizionati in maniera tale da offrire la maggiore copertura possibile ma sono in grado di comunicare tra loro in caso di necessità. Dato che la comunicazione tra J_1 e J_2 comporta comunque un costo di trasmissione c, al jammer che subisce un peggioramento della failure rate converrà comunicare tale variazione solamente se, rispetto alle condizioni normali, la perdita stimata in fatto di payoff superi tale valore. Successivamente, se si opta per la comunicazione, il jammer non influenzato modificherà il suo comportamento per bilanciare gli effetti che, la variazione di f sull'altro nodo jammer, sta causando.

4.3.1 Implementazione a singolo jammer

In questa casistica, a differenza di quanto visto precedentemente, verranno presentati l'andamento del payoff al variare del parametro f, nell'ipotesi di nodi statici, e l'*operational window* del sistema. Quando il sistema implementa nodi adattivi e si trova in una situazione di normalità, infatti, opererà in una situazione di equilibrio che, anche con l'aumentare della probabilità di fallimento, cercherà di mantenere: il secondo grafico che verrà qui riportato sarà indicativo di quanto fare possa il singolo jammer, senza variazione di altri parametri se non la sua probabilità j, per mantenere il suo valore ottimale di payoff.

Prima Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
1.1	*0.7*	*0.2*	*0.98*	*0.03*	*0.61*	*0.34*



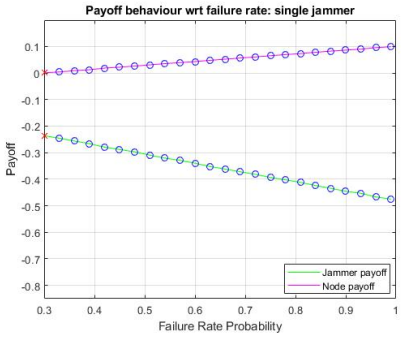
(a) *Evoluzione dei payoff nel caso di nodi statici.*

(b) *Finestra di operatività del jammer.*

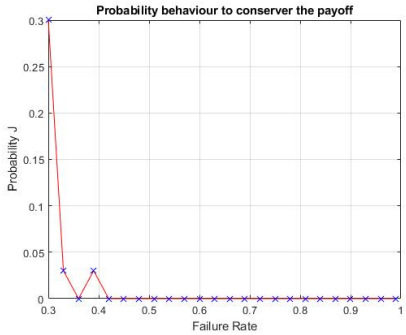
Figura 36: *Risultati evoluzione payoff e operational window del jammer.*

Seconda Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
0.7	*0.4*	*0.3*	*0.99*	*0.03*	*0.35*	*0.44*



(a) *Evoluzione dei payoff nel caso di nodi statici.*



(b) *Finestra di operatività del jammer.*

Figura 37: *Risultati evoluzione payoff e operational window del jammer.*

4.3.2 Implementazione a due jammer

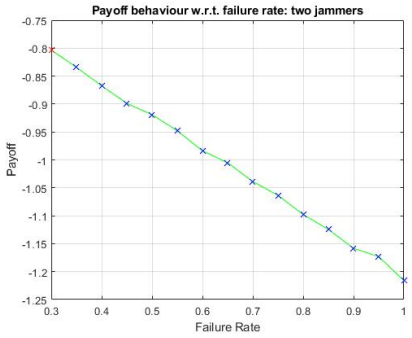
Come detto precedentemente, nell'implementazione a due jammer con failure rate f variabile, esistono principalmente tre diversi tipi di approccio che vengono qui analizzati singolarmente per ottenere dei risultati il più accurati possibile.

Nella realizzazione di tutti i possibili scenari è stata presa come assunzione la tesi che, i due jammer utilizzati, fossero inizialmente simmetrici, ovvero che presentassero lo stesso costo di trasmissione c e la stessa failure rate f.

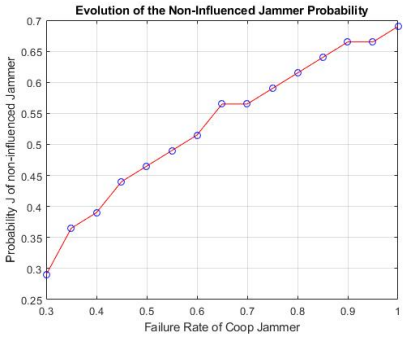
Caso completamente distribuito

Prima Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
1.1	*0.7*	*0.2*	*1*	*0.05*	*0.25*	*0.52*



(a) *Evoluzione dei payoff nel caso di nodi statici.*

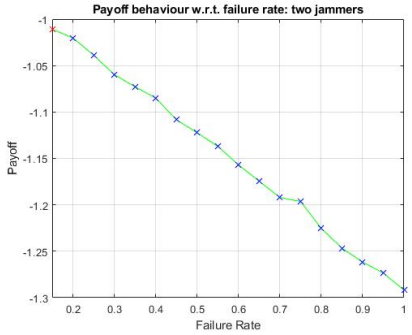


(b) *Evoluzione della probabilità del jammer non influenzato.*

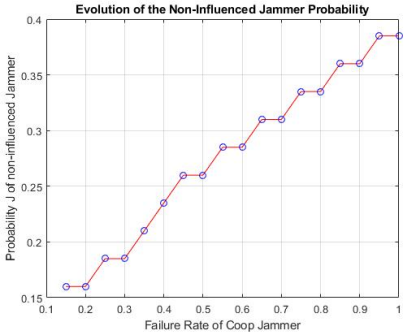
Figura 38: *Risultati evoluzione payoff ed evoluzione della probabilità del jammer non influenzato se dovesse compensare il deficit proveniente dall'altro jammer.*

Seconda Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
1.2	*0.9*	*0.15*	*1*	*0.05*	*0.16*	*0.56*



(a) *Evoluzione dei payoff nel caso di nodi statici.*



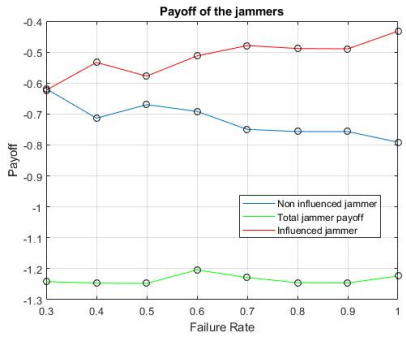
(b) *Evoluzione della probabilità del jammer non influenzato.*

Figura 39: *Risultati evoluzione payoff ed evoluzione della probabilità del jammer non influenzato se dovesse compensare il deficit proveniente dall'altro jammer.*

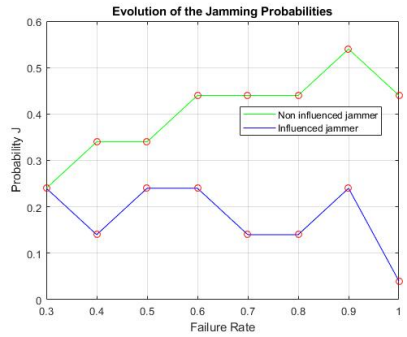
Caso concentrato

Prima Simulazione

Reward r	***Costo c***	***Failure rate dichiarata***	***Failure rate massima***	Δf	***J Teorico***	ϵ ***Teorico***
1.3	*0.9*	*0.3*	*1*	*0.1*	*0.24*	*0.67*



(a) *Evoluzione dei payoff nel caso jammer implementati insieme e che si adattano.*

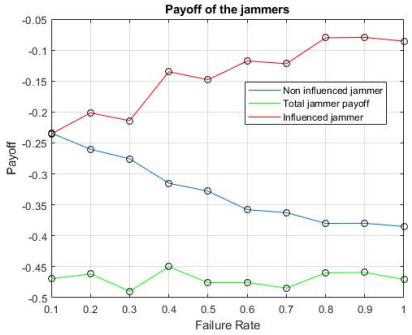


(b) *Evoluzione delle probabilità j_1 e j_2.*

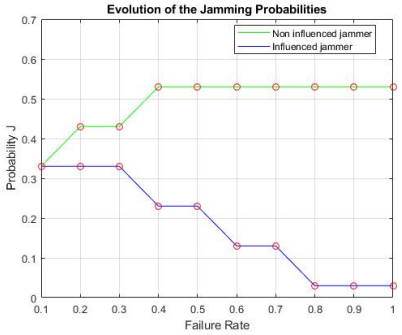
Figura 40: *Evoluzione dei payoff e della coppia di probabilità* $(j_1, j_2($.

Seconda Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
1.2	*0.6*	*0.1*	*1*	*0.1*	*0.33*	*0.43*



(a) *Evoluzione dei payoff nel caso jammer implementati insieme e che si adattano.*



(b) *Evoluzione delle probabilità* j_1 *e* j_2.

Figura 41: *Evoluzione dei payoff e della coppia di probabilità*$(j_1, j_2($.

Caso ibrido

Prima Simulazione

Reward r	*Costo c*	*Failure rate dichiarata*	*Failure rate massima*	Δf	*J Teorico*	ϵ *Teorico*
1.1	*0.7*	*0.2*	*1*	*0.05*	*0.25*	*0.52*

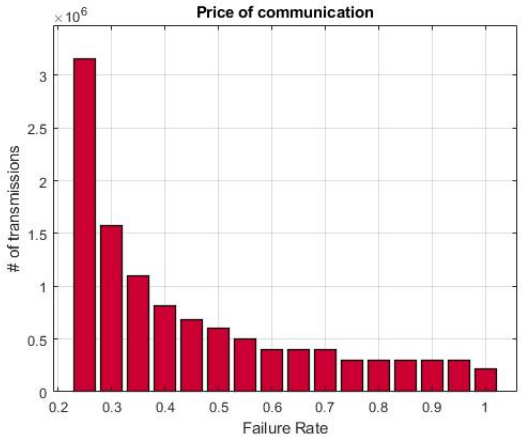


Figura 42: *Numero medio di trasmissioni dopo le quali la variazione di f viene comunicata.*

Seconda Simulazione

Reward r	***Costo c***	***Failure rate dichiarata***	***Failure rate massima***	Δf	***J Teorico***	ϵ ***Teorico***
1	*0.5*	*0.35*	*1*	*0.05*	*0.45*	*0.54*

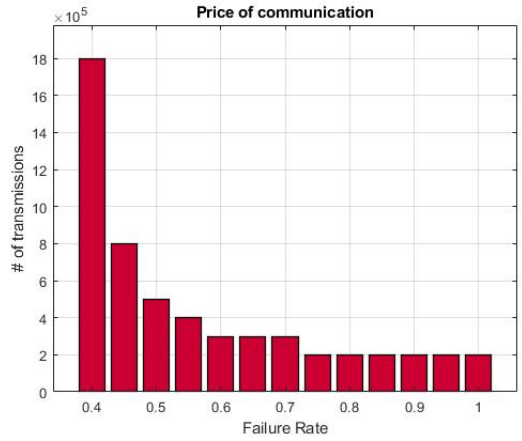


Figura 43: *Numero medio di trasmissioni dopo le quali la variazione di f viene comunicata.*

4.4 Raggiungimento del punto di equilibrio

Fino ad ora abbiamo analizzato gli effetti che, variazioni dei parametri fondamentali del sistema, hanno sul payoff, sulle probabilità e, in generale, sulle considerazioni di operatività in cui il sistema operava prima di essere perturbato.

Un altro fondamentale aspetto del punto di equilibrio risulta essere il tempo necessario a raggiungerlo partendo da valori iniziali di ϵ e j diversi: è stato quindi analizzato il numero di cicli necessari a un jammer che viene inserito in una rete dove inizialmente il nodo malevolo, non avendo nodi oppositori, compie un'azione di intromissione con probabilità $\epsilon = 1$.

I risultati ottenuti e mostrati, sono ovviamente molto legati all'algoritmo implementato dai nodi per modellarne il comportamento quando, analizzando il proprio payoff, quest'ultimi notassero una variazione delle condizioni di operatività. Per quanto riguarda l'approccio che è stato scelto, possiamo suddividere l'algoritmo in quattro principali fasi:

1. ***Prima parte: pre-accensione del jammer***:

   1.a) Il *nodo malevolo* rileva che, ad ogni suo tentativo di intrusione, dato che nel nostro modello il nodo M non è caratterizzato da una failure rate, ottiene un payoff pari alla sua differenza tra il parametro r ed il costo di trasmissione $c \Longrightarrow \epsilon = 1$.

   1.b) Il *jammer* può essere considerato, in questa fase, come installato ed operante ma con una probabilità di compiere l'azione di jamming nulla ($j = 0$).

1.c) Viene valutato il payoff del jammer in queste condizioni, ovvero con $\epsilon = 1$ e $j = 0$ ed utilizzato come riferimento. In queste condizioni ovviamente, anche il nodo malevolo ha un suo valore di payoff che potremmo definire "di riferimento".

2. ***Seconda parte: iniziale adattamento***:

2.a) La probabilità j viene incrementata di un valore fisso, denominata come j *step*. A questo punto, per un lasso temporale definito dal numero di giochi presi in considerazione (variabile *update*), viene valutato il payoff del jammer e paragonato con quello di riferimento rilevato nel punto *(1.c)*, aprendo a due possibili scenari:

- Il payoff ottenuto nel punto (*2.a*) è maggiore rispetto a quello ricavato nel punto (*1.c*) $\Longrightarrow$ aggiorno il valore di payoff di riferimento con questo appena ottenuto ed imposto j uguale al valore di j step.
- Il payoff ottenuto nel punto (*2.a*) è minore rispetto a quello ricavato nel punto (*1.c*) $\Longrightarrow$ non aggiorno il valore di payoff di riferimento con questo appena ottenuto e mantengo j uguale al valore predecente.

2.b) Con il valore di j aggiornato (oppure rimasto invariato, a seconda dell'opzione del punto precedente) il nodo malevolo osserva che, il proprio payoff potrebbe subire una diminuzione a causa dell'azione del jammer. Esso procederà allora con lo stesso approccio,

abbassando la sua ϵ e confrontando i valori di payoff ottenuti con questa nuova probabilità con quello precedente di riferimento.

- Il payoff ottenuto nel punto (*2.b*) è maggiore rispetto a quello ricavato nel punto (*1.c*) $\Longrightarrow$ aggiorno il valore di payoff di riferimento con questo appena ottenuto ed imposto ϵ uguale al valore di ϵ - ϵ_{step}.
- Il payoff ottenuto nel punto (*2.a*) è minore rispetto a quello ricavato nel punto (*1.c*) $\Longrightarrow$ non aggiorno il valore di payoff di riferimento con questo appena ottenuto e mantengo ϵ uguale al valore predecente.

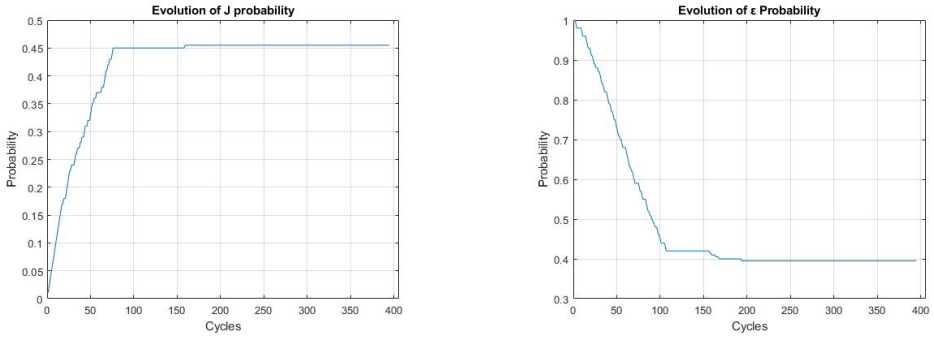
3. ***Terza parte: raggiungimento dell'equilibrio***: questa fase, risulta essere la principale e, parlando dal punto di vista realizzativo, si riduce alla applicazione ripetitiva di quanto descritto nel punto *(2)*. Le probabilità vengono quindi aggiornate ogni qualvolta un attore rilevi che il proprio payoff sarebbe maggiore con la nuova probabilità.
   Questa segmento di algoritmo si conclude quando per un numero di cicli, impostato a 50 nel simulatore, non avvengono aggiornamenti.

4. ***Quarte parte: perfezionamento dell'equilibrio***: In questa sezione viene nuovamente ripreso quanto accade nel punto *(2.b)* con la variazione dei parametri di ($j_{step}, \epsilon_{step}$) che, nell'implementazione utilizzata per la simulazione venivano dimezzati rispetto al valore iniziale. L'algoritmo, per poter fornire un risultato, esce dopo 200 cicli senza aggiornamento ma, in una realizzazione reale, continuerebbe nel suo ciclo di modifica delle probabilità.

4.4.1 Implementazione a singolo jammer

Prima Simulazione

Costo c	*Reward r*	*Failure Rate f*	*Update*	*Step J*	*Step ϵ*	*ϵ Teorico*	*j Teorico*
0.7	*1.1*	*0.2*	*1000*	*0.01*	*0.01*	*0.42*	*0.45*

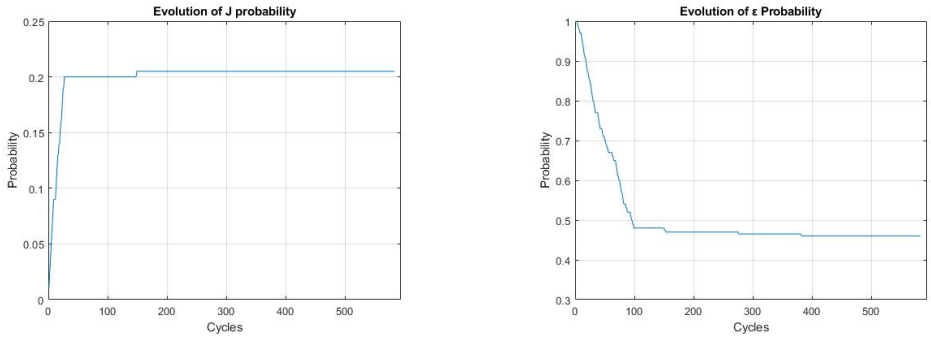


(a) *Evoluzione della probabilità j.* (b) *Evoluzione delle probabilità ϵ.*

Figura 44: *Evoluzione delle probabilità tramite l'utilizzo dell'algoritmo sopra descritto.*

Seconda Simulazione

Costo c	*Reward r*	*Failure Rate f*	*Update*	*Step J*	*Step ϵ*	*ϵ Teorico*	*j Teorico*
0.9	*1.1*	*0.1*	*1000*	*0.01*	*0.01*	*0.48*	*0.21*



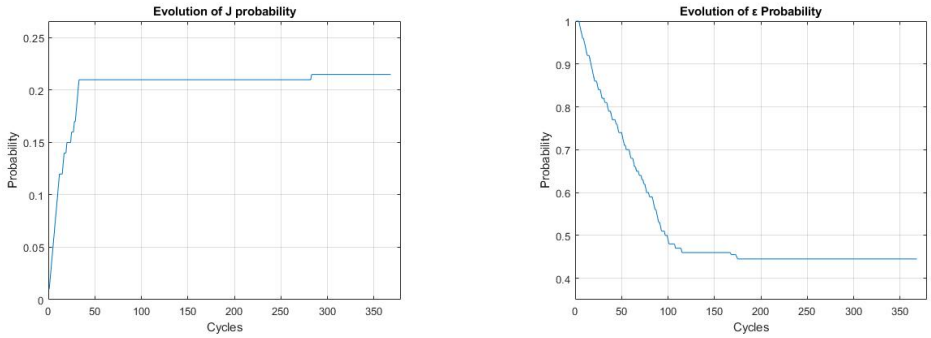
(a) *Evoluzione della probabilità j.* (b) *Evoluzione delle probabilità ϵ.*

Figura 45: *Evoluzione delle probabilità tramite l'utilizzo dell'algoritmo sopra descritto.*

4.4.2 Implementazione a due jammer

Prima Simulazione

Costo c	***Reward r***	***Failure Rate f***	***Update***	***Step J***	***Step ϵ***	***ϵ Teorico***	***j Teorico***
0.6	*0.9*	*0.15*	*1000*	*0.01*	*0.01*	*0.46*	*0.22*

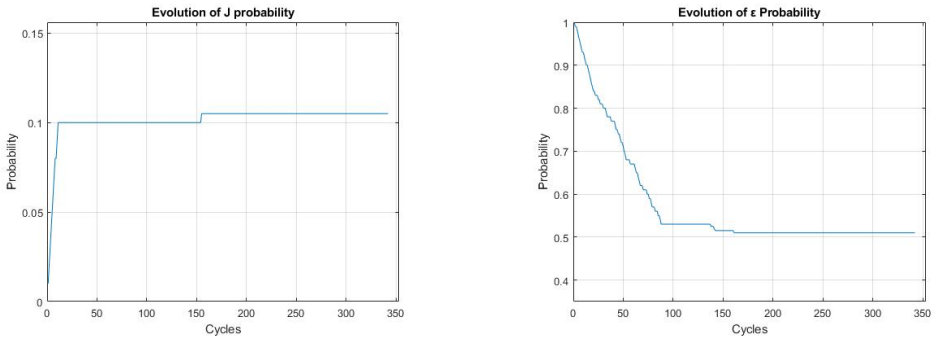


(a) *Evoluzione della probabilità j.* (b) *Evoluzione delle probabilità ϵ.*

Figura 46: *Evoluzione delle probabilità tramite l'utilizzo dell'algoritmo sopra descritto.*

Seconda Simulazione

Costo c	***Reward r***	***Failure Rate f***	***Update***	***Step J***	***Step ϵ***	***ϵ Teorico***	***j Teorico***
0.9	*1.1*	*0.1*	*1000*	*0.01*	*0.01*	*0.53*	*0.11*



(a) *Evoluzione della probabilità j.* (b) *Evoluzione delle probabilità ϵ.*

Figura 47: *Evoluzione delle probabilità tramite l'utilizzo dell'algoritmo sopra descritto.*

Capitolo 5

Conclusioni e lavori futuri

Il lavoro svolto ci ha permesso di osservare molteplici aspetti relativi all'equilibrio nell'applicazione della teoria dei giochi alle strategie di friendly jamming, siano esse implementate attraverso l'utilizzo di un singolo jammer o di una coppia di jammer (l'estensione ad eventualmente un numero maggiore di jammer risulta essere comunque ottenibile utilizzando lo stesso approccio utilizzato per passare da uno a due, passando ovviamente dalla dimensione n alla dimensione $n+1$).
Innanzitutto, tramite l'utilizzo del simulatore, abbiamo ottenuto i risultati mostrati nelle sezioni (3.3.1) e (3.3.2) dove rispettivamente:

- per la realizzazione a singolo jammer abbiamo dimostrato che i valori teorici ottenuti dalle *(3.4)* e *(3.5)* sono verificati con, in media, un distaccamento massimo dei risultati sperimentali, che può essere assunto circa pari allo 0.4% .

- per l'utilizzo dei due jammer, i dati teorici provenienti dalle *(3.7)* e

(3.9), sono sperimentalmente verificati con una variazione che si assesta intorno all'*1.5*% (va preso in considerazione che, per ragioni di tempistiche computazionali, il valore della variabile T nel simulatore era un ordine di grandezza inferiore rispetto al valore utilizzato nel caso a singolo jammer).

Raggiungimento dell'equilibrio

Confermato quindi che i risultati teorici fossero corretti, abbiamo analizzato l'evoluzione di uno scenario in cui un jammer venga inserito in una rete soggetta ad intrusioni da parte di un nodo malevolo.

Lo scopo di tale simulazione era di ottenere le tempistiche necessarie per riuscire a raggiungere, da parte di nodi intelligenti, la situazione di equilibrio. Assunti i valori come nella sezione *(4.4)*, è stato quindi analizzato il numero medio di cicli utili per raggiungere le relative probabilità di equilibrio partendo dalla peggiore situazione possibile, ovvero quella con $j = 0$ e $\epsilon = 1$. Andando ad osservare i risultati ottenuti da molteplici simulazioni, considerando l'algoritmo implementato e la varianza dovuta alle possibili diverse combinazioni dei parametri, possiamo concludere che:

– Il numero di cicli necessari per raggiungere il punto di equilibrio del sistema è fortemente legato al valore del parametro c.

  Se infatti quest'ultimo scende al di sotto di una certa soglia alla quale, sempre basandoci sulle simulazioni svolte, possiamo assegnare un valore uguale a 0.5, il numero di cicli necessari diverge fino a raggiungere valori oltre 100000. Tale problema è arginabile andando ad aumentare il valore di j *step*, causando però, al contempo, una diminuzione della

precisione con cui avvicinarsi al valore di probabilità teorico.

– Il numero medio di cicli necessari per raggiungere il valore di probabilità teorico (o, nel caso sia risultato necessario aumentare il valore di j step, arrivare ad un suo prossimo equivalente) si è concentrato, per quanto riguarda le simulazioni a singolo jammer, su valori compresi tra $370 \div 550$ mentre, per implementazioni a doppio jammer, ci si aggira intorno ai $290 \div 360$ cicli.

  Il valore di stabilità viene quindi raggiunto, in generale, con una velocità molto superiore nelle implementazioni a due jammer. Questa conclusione è verificabile paragonando i risultati della seconda simulazione effettuata per il primo jammer (figura *48*) con quelli ottenuti nella seconda a doppio jammer (figura *50*)dove i paremetri utilizzati sono esattamente gli stessi.

Ricordando che, per ogni ciclo, nel simulatore, era necessario "registrare" il risultato di un numero di giochi pari alla variabile *update*, nel nostro caso abbiamo che, per raggiungere il punto di operatività migliore, saranno necessari $370 \div 550 \times update = 370000 \div 550000$ giochi per il singolo jammer e $290000 \div 360000$ giochi per un sistema con doppio jammer.

Nelle sezioni (4.1), (4.2) e (4.3) è stata inoltre valutata la robustezza di tale punto operativo, ovvero quanto le variazioni dei parametri *c, r* ed *f*, influiscano su di un sistema che, prima di tali perturbazioni, risulti operante nel punto di equilibrio. Sono quindi stati fatti variare a giro i parametri

del sistema, andando a valutare come tali variazioni andavano ad inficiare su valori di *payoff* e *probabilità* dei diversi nodi in molteplici scenari, dal caso a nodi intelligenti ed "adattivi" fino a quello di nodi completamente statici.

Variazioni del costo di trasmissione c

Il variare del parametro c influsice maggiormente sui valori di payoff e probabilità dei jammer rispetto a quanto non faccia su quelli relativi al nodo malevolo. Nelle figure *17* e *20* per il singolo jammer e nelle figure *23.a* e *26.a* per la realizzazione a due jammer, è possibile osservare che, in presenza di nodi intelligenti ed adattivi, all'eventuale aumento di c, il nodo malevolo risponde incrementando la propria probabilità ϵ e mantendo un payoff costante mediamente nullo mentre, i jammer, subiscono un decremento del proprio payoff a causa della marcata diminuzione della probabilità j. La variazione percentuale di queste probabilità è, in generale, più marcata per quanto riguarda j, ma risulta molto spesso inferiore al 2% per ogni incremento di $\Delta\, c = 0.05$.

L'analisi con jammer misti, svolta per le implementazioni a doppio jammer (figure *24* e *27*), dimostra che, nonostante si faccia ovviamente fronte, a causa del jammer non adattivo, ad un costo di trasmissione medio maggiore, è possibile andare a ridurre il payoff del nodo malevolo, il quale supponendo un comportamento intelligente di entrambi jammer, aumenta la sua probabilità di intrusione.

Va comunque detto che, se l'intrusore rilevasse questa anomalia comportamentale, il suo eventuale adattamento causerebbe una perdita per i jammer, in termini di payoff, molto maggiore rispetto alla situazione precedente.

Nella più semplice situazione in cui nessun attore in gioco sia intelligente, e che quindi nessuno di essi modifichi il proprio comportamento, si avrà una generale diminuzione dei payoff medi di entità comunque maggiore per i jammer.

Variazioni del reward r_M

Gli effetti che le varizioni del parametro r hanno sulle condizioni di equilibrio del sistema possono sembrare, nel complessivo, molto meno marcate di quanto non lo fossero quelle dovute all'alterazione del parametro c.

Iniziando ad analizzare gli effetti sulle realizzazioni a singolo jammer, possiamo osservare che, nelle figure *29.a* e *31.a* rappresentanti l'utilizzo di nodi adattivi, grazie alla diminuzione della probabilità ϵ, il nodo malevolo è in grado di mantenere il proprio payoff medio nullo (questo a causa dell'indifferenza presente nel caso in cui esso scelga l'azione **O**) mentre, anche in questo caso, il payoff del jammer tende a diminuire.

I risultati sembrerebbero dunque ricalcare quelli già visti per la variazione di c e, dal punto di vista puramente numerico, possono essere considerati, nonostante la diminuzione del payoff del jammer sia in questo caso molto meno marcata, comparabili.

Analizzando però, con le figure *29.b* e *31.b*, l'andamento delle probabilità, possiamo notare come la natura di questa variazione sia profondamente diversa da quella rappresentata dalle figure *18* e *21* poichè, in questo caso, vi è un'inversione nei comportamenti delle probabilità stesse:

- La probabilità ϵ subisce una leggera diminuzione, assumibile nell'ordine del 1.2% per ogni incremento $\Delta\, r = 0.05$

– L'effetto sulla probabilità j è invece molto più importante, dato che, per ogni incremento $\Delta\, r = 0.05$, essa subisce in incremento che molte volte supera il 3%, andando a definire una forte dipendenza tra il parametro r e la probabilità j.

Nel caso di utilizzo di nodi statici invece, l'aumento di r ed il mancato "aggiustamento" delle probabilità vede, come mostrato nelle figure *30* e *32*, un incremento del payoff dell'intrusore a fronte di una diminuzione di quello relativo ai jammer.
Nelle implementazioni a doppio jammer, gli effetti appena descritti, possono essere generalizzati, facendo però alcune opportune osservazioni:

– Come mostrato in figura *33.a* e *36.a*, successivamente all'implementazione del secondo jammer, è possibile, andando ad adattare la probabilità j, mantere costante il payoff complessivo dei jammer evitando, dall'altro lato, un aumento di quello relativo al nodo intrusore.

– Vi è un aumento della probabilità j molto meno marcato rispetto al caso a singolo jammer mentre, l'andamento della probabilità ϵ, può essere considerato quasi costante nell'arco della simulazione.

– La realizzazione a jammer misti mostra che, nel caso in cui il nodo supponga entrambi i suoi oppositori adattivi ed intelligenti, si possa ottenere un guadagno in termini di payoff complessivo. Il nodo malevolo, infatti, supponendo di trovare *entrambi* i jammer attivi con una probabilità maggiore (vedi figure *33.b* e *36.b*), abbasserà la sua ϵ, riducendo il numero di tentativi di intrusione. Va detto che, come analizzato per

il caso misto di variazione di c, se il nodo intrusore percepisse questo comportamento e reagisse di conseguenza si avrebbe un aumento delle intrusioni che hanno successo.

Variazioni della failure rate *f*

Nell'analisi svolta per la variazione di f abbiamo studiato un aspetto che, nelle altre casistiche, non era possibile andare ad analizzare: l'*operational window* del jammer.

Mentre nelle figure *39.a* e *40.a* viene riportato l'andamento dei payoff dei vari nodi all'aumentare del parametro f (i quali, ovviamente, vedono un incremento del payoff del nodo intrusore ed una diminuzione di quello relativo al jammer) nelle figure *39.b* e *40.b* viene mostrato, sempre all'aumentare di f, come può reagire, in termini di variazione di probabilità j, un singolo jammer, per tentare di mantenere costante il suo valore di payoff.

Ciò che si evince dall'analisi di tali finestre di operabilità è che, un leggero aumento della failure rate, rende di fatto impossibile, per il jammer, operare sui parametri d'equilibrio, rendendo quest'ultimo molto sensibile e poco robusto alle variazioni di questo parametro.

Per quanto riguarda le implementazioni a doppio jammer invece, l'analisi è stata suddivisa in tre parti:

- Nell'opzione ***completamente distribuita***, la mancanza di comunicazione tra i due jammer causa una grande diminuzione del payoff che, analizzando le figure *41.a* e *42.a*, è attestabile nell'ordine del $35\% \div 50\%$.

Le figure adiacenti, ovvero le *41.b* e *42.b* mostrano come, la probabilità del jammer non influenzato dall'incremento di f, dovrebbe variare per cercare di compensare le perdite dovute al condizionamento dell'altro jammer.

– Nella seconda opzione, ovvero quella ***concentrata***, possiamo notare, osservando le immagini *43.a* e *44.a*, come, al contrario del punto precedente, riusciamo a mantenere il valore complessivo del payoff attorno a quello d'equilibrio, grazie alla diminuzione della probabilità del nodo influenzato ed all'aumento di quella del jammer operante normalmente (figure *43.b* e *44.b*).

  La probabilità j_2 subisce quidni una dimunizione costante e tende ad annullarsi in punti che, ovviamente, dipendono dal valore degli altri parametri, ma che generalmente si assestano su $f = 0.8 \div 1$.

– Nella realizzazione ***ibrida*** invece, figure *45* e *46*, viene mostrato come, nel caso in cui sia prevista la possibilità di comunicazione tra due jammer nell'eventualità di variazioni dei parametri di funzionamento, questa non sia sempre conveniente.

  Prendendo in analisi la sola figure *45* infatti salta subito all'occhio come, se la failure rate del jammer influenzato, superi il 30% (dato che la f dichiarata fosse del 20%), molto probabilmente, in termini di payoff, mi convenga comunicare la mia nuova situazione in maniera tale da poter aggiustare le probabilità j_1 e j_2 come avviene nel caso concentrato.

Considerazioni

Riassumendo tutto quello detto precedentemente, possiamo quindi dire che, il punto di equilibrio che si raggiunge in un sistema di friendly jamming a cui viene applicata la teoria dei giochi, risponde in maniera profondamente diversa a seconda del parametro che andiamo a modificare.

Una variazione del parametro r causerà un'ampia ed immediata variazione della probabilità j mentre una variazione di c influenzerà, in maniera circa paragonabile, tutti i nodi in gioco. Per quanto riguarda la probabilità di fallimento del jammer f, essa risulta essere probabilmente il punto di maggiore fragilità nei sistemi implementanti il singolo jammer i quali, anche in seguito a una leggera variazione, perdono la possibilità di operare al migliore dei modi.

Tuttavia, molti aspetti di quanto detto, soprattutto per il raggiungimento dell'equilibrio, dipende in maniera molto stretta, dal tipo approccio utilizzato o di algoritmo che si è pensato ed implementato.

Uno studio di ottimizzazione di questi algoritmi, l'espansione ad un numero maggiore di jammer, l'apertura alla possibile presenza di molteplici nodi intrusori coordinati tra loro e la possibilità che l'azione malevola venga svolta in alternanza ad azioni legittime e da nodi effettivamente facenti parte delle rete vengono lasciati come possibili sviluppi futuri ad espansione di questo operato.

Bibliografia

[1] Elmustafa S.A.A., Zeinab K.A.M, *Internet of Things Applications, Challenges and Related Future Technologies.* 2017.

[2] *"The Evolution of Wireless Sensor Networks"*. Silicon Laboratories Inc, 2013.

[3] Johnsen F.T, Zielinski Z., Wrona K., Suri N., *Application of IoT in military operations in a smart city.* Maggio 2018.

[4] Baker S., Xiang W., Atkinson I.M., *Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities.* Novembre 2017.

[5] F. C., *"An Introduction to Wireless Sensor Networks"*. Royal Institute of Technology, Settembre 2014.

[6] Drugarin C.V.A., *Data security in wireless networks.* 40th Symposium on Advanced Engineering and Applied Management.

[7] Alghazo J., Kazimi Z., Latif G., *Cyber security analysis of internet banking in emerging countries: User and bank perspectives.* IEEE International Conference on Engineering Technologies and Applied Sciences.

[8] Tyagi N.,Joshi A., Singh S., *A Comparative Approach to Remote Home Security System Based on Wireless System Network and GSM.* International Journal of Scientific and Engineering Researchs.

[9] Check Point Software Technologies LTD, *2019 Security Report.* Check Point Research.

[10] Diffie W., Hellman M., *"New directions in cryptography"*. IEEE Trans. Inf. Theory, Novembre 1976.

[11] Makda S., Choudhary A., Raman N., Korakis T., Tao Z., Panwar S., *"Security Implications of Cooperative Communications in Wireless Networks"*. IEEE Sarnoff Symposium, Maggio 2008.

[12] Singh G., Supriya S., *"A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security"*. International Journal of Computer Applications, Aprile 2013.

[13] Bloch M., Barros J., Rodrigues M.R.D., McLaughlin S.W., *"Wireless information theoretic security"*. IEEE Trans. Inf. Theory, Giugno 2008.

[14] Shannon C.E., *"Communication theory of secrecy systems"*. Bell System Technical Journal, Aprile 1949.

[15] Badia L., Gringoli F.,, *"A Game of One/Two Strategic Friendly Jammers versus a Malicious Strategic Node"*. IEEE Networking Letters, Gennaio 2019.

[16] Konakalla A., Veeranki B., *Evolution of Security Attacks and Security Technology*. International Journal of Computer Science and Mobile Computing.

[17] Delfs H., Knebl H., *"Introduction to Cryptography vol. 2"*. 2004.

[18] Patel S.T., Mistry N.H., *"A survey: Lightweight cryptography in WSN"*. 2015 International Conference on Communication Networks (ICCN), 2015.

[19] Sechi M., *"Il modello ISO/OSI"*. 2014.

[20] Shannon C.E., *"Communication theory of secrecy systems"*. Bell System Technical Journal, Aprile 1949.

[21] Wyner A., *"The Wired-Tap Channel"*. Bell System Technical Journal, 1975.

[22] Luttrell S.P., *"A User's Guide to Stochastic Encoder/Decoders"*. 1987.

[23] Zhu H., Ninoslav N., Debbah M., Hjorungnes A., *"Physical Layer Security Game: How to Date a Girl with Her Boyfriend on the Same Table"*. IEEE International Conference on Game Theory for Networks, 2009.

[24] Leungh-Yan-Cheon S.K., Hellman M.E., *"The Gaussian Wire-Tap Channel"*. Bell System Technical Journal, 1978.

[25] Gopala P.K., Lai L., Gamal H.E., *"On the secrecy capacity of fading channels"*. IEEE Trans. Inf. Theory, Ottobre 2008.

[26] Csiszar I., Korner J., *"Broadcast channels with confidential messages"*. IEEE Trans. Inf. Theory, Maggio 1978.

[27] Han Z., Marina N., Debbah M., Hjorungnes A., *"Physical layer security game: interaction between source, eavesdropper, and friendly jammer"*. EURASIP J. Wireless Commun. and Netw., Marzo 2009.

[28] Hassan A.A., Hershey J.E., Yarlagadda R., *"Unconventional cryptographic keying variable management"*. IEEE Trans. on Communications, Gennaio 1995.

[29] Hassan, A.A., Hershey J.E., Stark W.E., Chennakeshu S., *Cryptographic key agreement for mobile radio"*. Digital Signal Processing, Academic Press, 2006.

[30] Hassan A.A., Chennakeshu S., Koorapaty H., *"Secure information transmission for mobile radio"*. IEEE Communications Letters, Febbraio 2000.

[31] Hero A.O., *"Secure Space-Time Communication"*. IEEE Transactions on Information Theory, Marzo 2003.

[32] Grover K., Lim A., Yang Q., *"Jamming and Anti-jamming Techniques in Wireless Networks: A Survey"*. Int. J. Ad Hoc and Ubiquitous Computing, 2014.

[33] Baessato A., *"Internet Delle Cose e WiFi Passivo: Tutto puo' essere collegato"*. Universita' degli Studi di Padova, 2016.

[34] Tippenhauer N.O., Capkun S., Popper C., Daven B., *"Investigation of Signal and Message Manipulations on the Wireless Channel"*. ESORICS 2011: 16th European Symposium on Research in Computer Security, 2011.

[35] Schulz M., Gringoli F., Koch M., Steinmetzer D., Hollick M., *"Massive Reactive Smartphone-Based Jamming using Arbitrary Waveforms and Adaptive Power Control"*. Association for Computing Machinery, Giugno 2017.

[36] Mpitziopoulos A., Gavalas D., Konstantopoulos C., Pantziou G., *"A Survey on Jamming Attacks and Countermeasures in WSNs"*. IEEE Communication Surveys and Tutorials, 2009.

[37] Xu W., Trappe W., Zhang Y., Wood T., *"The feasibility of launching and detecting jamming attacks in wireless networks."*. ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2005.

[38] Pelechrinis K., Iliofotou M., Krishnamurthy S., *"Denial of service attacks in wireless networks: The case of jammers."*. IEEE Communications Surveys Tutorials 13, 2011.

[39] Mpitziopoulos A., Gavals D., Pantziou G., *"Defending wireless sensor networks from jamming attacks."*. IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007.

[40] Alfie G., Simon R., *"A multi-channel defense against jamming attacks in wireless sensor networks."*. Proceedings of the 3rd ACMWorkshop on QoS and Security for Wireless and Mobile Networks, 2007.

[41] Alfie G., Simon R., *"MULEPRO: a multi- channel response to jamming attacks in wireless sensor networks."*. Wireless Communications and Mobile Computing, 2010.

[42] Muraeleedharan R., Osadeiw L.A., *"Jamming attack detection and countermeasures in wireless sensor network using ant system"*. SPIE the International Society for Optical Engineering, 2006.

[43] Lazos L., Liu S., Krunz M., *"Mitigating control- channel jamming attacks in multi-channel ad hoc networks."*. Proceedings of the 2nd ACM Conference on Wireless Network Security, 2009.

[44] Brousis I., Pelechrinis K., Syrivelis D., Krishnamurthy S.V., Tassiulas L., *"FIJI: Fighting implicit jamming in 802.11 WLANs."*. Security and Privacy in Communication Networks, 2009.

[45] Tague P., Slater D., Poovendra R., Noubir G., *"Linear programming models for jamming attacks on network traffic flows."*. 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008.

[46] Wood A., Stankovic J., Son S., *"JAM: a jammed-area mapping service for sensor networks."*. 24th IEEE Real-Time Systems Symposium, 2003.

[47] Wang H., Zhang L., Li T., Tugnait J., *"Spectrally efficient jamming mitigation based on code-controlled frequency hopping."*. IEEE Transactions on Wireless Communications 10, 2011.

[48] Gummadi R., Wethreall D., Greenstein B., Sesham S., *"Understanding and mitigating the impact of RF interference on 802.11 networks."*. Proceedings of the 2007 Conference on Applications, technologies, architectures, and protocols for computer communications, 2007.

[49] Navda V., Bohra A., Ganguly S., Rubenstein D., *"Using channel hopping to increase 802.11 resilience to jamming attacks."*. IEEE Transactions on Wireless Communications 10, 2007.

[50] Khattab S., Mosse D., Melhem R., *"Jamming mitigation in multi-radio wireless networks: Reactive or proactive?"*. Proceedings of the 4th International Conference on Security and privacy in communication networks, 2008.

[51] Jain S.K., Garg K., *"A hybrid model of defense techniques against base station jamming attack in wireless sensor networks."*. Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, 2009.

[52] Thamilarasu G., Sridhar R., *"Game theoretic modeling of jamming attacks in ad hoc networks"*. Internatonal Conference on Computer Communications and Networks, 2009.

[53] Hong Y.-W. P., Lan P.-C., Kou J., *"Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems."*. Springer Publishing Company Incorporated, 2013.

[54] Lou W., Ren K., *"Security, privacy, and accountability in wireless access networks."*. IEEE Wireless Communication, 2009.

[55] Shiu Y.-S., Chang S.Y., Wu H.-C., Huang S.-H., Chen H.-H., *"Physical layer security in wireless networks: a tutorial."*. IEEE Wireless Communication, 2011.

[56] Martinovic I.,Pichota P., Schmitt J.B., *"Jamming for Good: A Fresh Approach to Authentic Communication in WSNs"*. ACM Pubblication, 2009.

[57] Yang M., Zhang B., Huang Y., Yang N., Guo D., Gao B., *"Secure Multiuser Communications in Wireless Sensor Networks with TAS and Cooperative Jamming."*. Sensors Pubblications, 2016.

[58] Park K.-H., Wang T., Alouini M.-S., *"On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming."*. IEEE J. Selected Areas in Communication, 2013.

[59] Atallah M., Kaddoum, G., Kong L., *"A Survey on Cooperative Jamming Applied to Physical Layer Security."*. IEEE International Conference on Ubiquitous Wireless Broadband, 2015.

[60] Long H., Xiang W., Wang J., Wang W., Zhang Y., *"Cooperative jamming and power allocation with untrusty two-way relay nodes."*. Commun. IET, Settembre 2014.

[61] Bassilly R., Ulukus S., *"Deaf Cooperation and Relay Selection Strategies for Secure Communication in Multiple Relay Networks."*. IEEE Transaction on Signal Processing, Marzo 2013.

[62] Zhang R., Song L., Han Z., Jiao B., *"Distributed coalition formation of relay and friendly jammers for secure cooperative networks."*. IEEE Int. Conf. Commun., Giugno 2011.

[63] He W., Yener A., *"The role of feedback in two-way secure communications."*. IEEE Trans. Inform. Theory, Dicembre 2013.

[64] Tang X., Liu R., Spasojevic P., Poor H. V., *"Interference-assisted secret communication."*. IEEE Trans. Inform. Theory, Maggio 2008.

[65] Long H., Xiang W., Wang J., Wang W., Zhang Y., *"Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems."*. IEEE Wireless Commun. and Networking Conf., Aprile 2013.

[66] Dong L., Yousefi'zadeh H., Jafarkhani H., *"Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper."*. IEEE Int. Conf. Commun, Giugno 2011.

[67] Pierrot A., Bloch M., *"Strongly secure communications over the two-way wiretap channel."*. IEEE Trans. Inform. Forensics and Security, Giugno 2011.

[68] Stanojev I., Simeone O., Spagnolini U., Bar-Ness Y., *"Cooperative ARQ via Auction-Based Spectrum Leasing."*. IEEE Transactions on Communications, Luglio 2010.

[69] Stanojev I., Yener A., *"Recruiting Multi-Antenna Transmitters as Cooperative Jammers: An Auction-Theoretic Approach."*. Forty-Ninth Annual Allerton Conference, Settembre 2011.

[70] Chen X.,Kwan D.W.Ng., Gerstacker W.H., Chen H-H., *A Survey on Multiple-Antenna Techniques for Physical Layer Security.* IEEE Communications Surveys and Tutorials.

[71] Zhang Y., *Wireless Security with Beamforming Technique.* Cornell University.

[72] Guo H., Yang Z., Zhang L., Zhu J., Zou Y., *Optimal Power Allocation for Physical-Layer Security Using Joint Relay and Jammer Selection.* 2016 IEEE Global Communications Conference.

[73] Han Z., Niyato D., Saad W., Basar T., HjÃ¸rungnes A., *"Game Theory in Wireless and Communication Networks: Theory, Models and Applications."*. Cambridge University Press, 2010.

[74] Dehnie S., Memon N., *"Modeling Misbehavior in Cooperative Diversity: A Dynamic Game Approach."*. Journal on Advances in Signal Processing, Gennaio 2009.

[75] Kreps D., Wilson R., *Sequential equilibra.* Econometrica.

[76] Ling M.-H., Tsai J.-F., Yinyu Y., *"Budget Allocation in a Competitive Communication Spectrum Economy."*. Journal on Advances in Signal Processing, Gennaio 2009.

[77] Park J., Van Der Schaar M., *"Stackelberg Contention Games in Multiuser Networks."*. Journal on Advances in Signal Processing, Febbraio 2009.

[78] Stanojev I., *"Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming."*. IEEE Trans. Commun., Gennaio 2013.

[79] Simeone O., Stanojev I., Savazzi S., Bar-Ness Y., Spagnolini U., Pickholtz R., *"Spectrum leasing to cooperating secondary ad hoc networks."*. IEEE J. Sel. Areas Commun., Gennaio 2008.

[80] Stanojev I., Simeone O., Spagnolini U., Bar-Ness Y., Pickholtz R., *"Cooperative ARQ via auction-based spectrum leasing."*. IEEE Trans. Commun., Gennaio 2010.

[81] Osborne M. J., Rubenstein A., *"A Course in Game Theory."*. MIT Press, 1994.

[82] Han Z., Marina N., Debbah M., Hjorungnes A., *"Improved wireless secrecy capacity using distributed auction theory."*. Proc. 2009 International Conf. Mobile Ad-hoc Sensor Netw., 2009.

[83] Berger D.S., Gringoli F., Facchi N., Martinovic I., Schmitt J.B, *"Friendly jamming on access points: Analysis and real-world measurements."*. IEEE Trans. Wireless Commu., 2016.

[84] Teng F., Guo D., Honig M.L., *"Sharing of unlicensed spectrum by strategic operators."*. IEEE J. Sel. Areas Commun., 2017.

[85] Osborne M., *"An introduction to game theory"*. Oxford University Press., 2009.

[86] Guglielmi A.V., Badia L., *"Bayesian game analysis of a queueing system with multiple candidate servers."*. Proc. IEEE CAMAD, 2015.

[87] Boisseau S., G. Despesse G., Ahmed Seddik B., *Electrostatic Conversion for Vibration Energy Harvesting.* 2012.

[88] Idrees A.K., Salman M.A., *Data Transmission Protocol for Reducing the Energy Consumption in Wireless Sensor Networks.* 2018.

[89] Mahjabin T.,Xiao Y., Sun G., Jiang W., *A survey of distributed denial-of-service attack, prevention, and mitigation techniques.* International Journal of Distributed Sensor Networks.

[90] Elshazly K., Fouad Y., Saleh M., Sewisy A., *A Survey of SQL Injection Attack Detection and Prevention.* Journal of Computer and Communications.

[91] Jain K.M., Jain M.V., Borade J.L., *A Survey on Man in the Middle Attack.* International Journal of Science Technology and Engineering.

[92] Santhi G., Sowmiya R., *A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks.* International Journal of Computer Applications.

[93] Martin-Flatin J.P., Znaty S., Hubaux J.P, *A Survey of Distributed Network and Systems Management Paradigms.* Swiss Federal Institute of Technology Lausanne.