ALMA MATER STUDIORUM
UNIVERSITA' DI BOLOGNA

SECONDA FACOLTA' DI INGEGNERIA
CON SEDE A CESENA

CORSO DI LAUREA IN INGEGNERIA
ELETTRONICA E TELECOMUNICAZIONI

Generazione di chiavi sicure in Reti wireless

TESI DI LAUREA
IN
Elaborazione dei Segnali

CANDIDATO
Marco Zoli

RELATORE
Chiar.mo Prof. Davide Dardari
CORRELATORE
Chiar.mo Prof. Gianni Pasolini

ANNO ACCADEMICO 2011/2012

SESSIONE II

Alla mia famiglia, ai miei compagni di studio e alla mia dolce Nicole

INDICE

INTRODUZIONE

"Il problema fondamentale della comunicazione è la riproduzione esatta o approssimativa in un certo punto dello spazio di un messaggio selezionato in un altro diverso punto"

C.E. Shannon (1948) [4]

Al giorno d'oggi il vasto universo delle tecnologie di telecomunicazioni, dette anche ICT **(Information and Communication Technologies),** occupano indubbiamente un ruolo fondamentale nella vita quotidiana e nella moderna società. A partire dagli anni '60 abbiamo assistito ad un enorme progresso scientifico nel campo dell'elettronica e dell'informatica tanto che ora le relazioni interpersonali, il mondo del lavoro e persino le arti musicali o visive ne sono così irreversibilmente influenzate da costituirne parte integrante. La possibilità di accedere da casa a qualunque documento nel mondo o la facilità nel dialogare con altre persone a chilometri di distanza, grazie all'uso di Internet per esempio, hanno portato alcuni giornalisti, filosofi e sociologi a definire questi anni in cui viviamo come **Information Age** [4] o Network Society [6]. Così come l'invenzione della macchina a vapore innescò il decollo dell'era industriale ad esempio, un profondo cambiamento mondiale iniziò con lo sviluppo del computer e con la diffusione delle reti di calcolatori e continua inarrestabilmente tutt'ora. In particolare possiamo evidenziare, a prescindere dal design, dalla marca, dal produttore o dall'età ciò che davvero contraddistingue intrinsecamente la vasta gamma dei diversi sistemi elettronici: il flusso di trasformazione dei dati, ovvero il concatenarsi e/o il ripetersi di alcuni processi essenziali: Acquisizione, Memorizzazione, Elaborazione, Comunicazione. L'elemento principale dell'intero processo risiede nel concetto di informazione, che fu per primo ideato e studiato da Claude Elwood Shannon negli anni '40 e '50, fondando così la Teoria dell'Informazione, su cui oggi si basano la codifica di canale, la codifica di linea e la compressione dati. Risulta facile, ora, comprende quanto sia importante e necessario salvaguardare l'integrità e la riservatezza dell'informazione da entità estranee nemiche, attraverso l'impiego della **crittografia,** ovvero la scienza che tratta lo studio del celare un determinato messaggio.

Dopo diversi secoli di aspre battaglie tra Criptoanalisti e Crittografi (citiamo ad esempio gli sforzi da parte del gruppo inglese di Bletchley Park per scoprire il funzionamento della macchina Enigma del Terzo Reich durante la Seconda Guerra Mondiale [5]) disponiamo oggi dei migliori sistemi per la sicurezza, che garantiscono un ottimo livello di privacy nella comunicazione. Poiché la maggior parte di questi, però, sfrutta la matematica dei moduli o dei fattori primi, un set di parametri con elevate cifre numeriche e l'ipotesi basilare di condivisione a priori di una dato comune indispensabile (ovvero la chiave), è oggi più che mai viva la necessità di ricercare nuovi approcci crittografici che, utilizzando limitate risorse di calcolo e di memoria, siano meglio adatti alle **telecomunicazione wireless,** in cui i terminali radio sono spesso lontani, mobili e di piccole dimensioni. In questo ampio contesto ho cercato di condurre uno studio appropriato per indagare sulle qualità e sulla versatilità di una delle più diffuse tecniche di sicurezza, proposte attualmente in letteratura. Ho organizzato il lavoro in questo modo : dapprima ho delineato gli aspetti teorici fondamentali, tra cui la caratterizzazione del canale radio come fonte di informazione casuale oppure il Teorema di Reciprocità della tratta radio, in seguito ho effettuato alcune sperimentazioni, per valutare la reale efficacia del critto-sistema, in campo pratico, utilizzando come Hardware alcuni nodi Zigbee della Texas Instruments. I risultati complessivamente sono stati soddisfacenti e rappresentano, sicuramente, un'ulteriore conferma delle potenzialità future di queste nuove tecniche di sicurezza nell'ambito delle reti di telecomunicazioni.

CAPITOLO 1
TIPICO SCENARIO NELL'AMBITO DELLA SICUREZZA

Nel mondo della crittografia la maggior parte delle possibili situazioni viene spesso sintetizzata nell'interazione di sole tre entità, denominate per semplicità **Alice , Bob ed Eva,** come rappresentato di seguito in Figura 1:

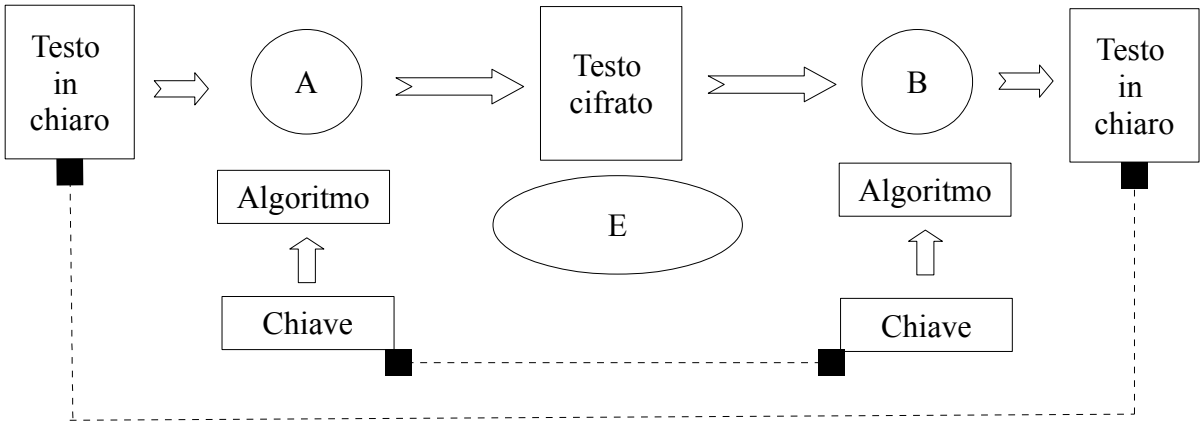


Fig.1 Tipico scenario crittografico con Alice, Bob ed Eva

Il collegamento tra Alice e Bob deve essere mantenuto il più possibile al riparo da attacchi di vario genere da parte di Eva, che potrebbe cercare di captare o alterare il contenuto dei messaggi intromettendosi nel canale di comunicazione. Per far questo è necessario un **algoritmo di sicurezza**, ovvero un insieme di determinate operazioni e funzioni matematiche, che, in fase di cifratura, a partire da un testo in chiaro e da una chiave (precedentemente condivisa tra Alice e Bob) generi un testo cifrato, mentre, in fase di decifrazione, a partire dal testo cifrato stesso e dalla stessa chiave di sicurezza, recuperi il testo in chiaro iniziale. Si può notare in Figura come sia di fondamentale importanza instaurare un protocollo comune tra le estremità della comunicazione, denominati A e B, che includa e definisca l'utilizzazione dell'algoritmo e della chiave del processo crittografico. Complessivamente , quindi, tutte le informazioni che transitano sul canale sono così inaccessibili a chiunque non sia coinvolto nella comunicazione, non essendo solitamente a conoscenza della **chiave**. Quest'ultima, infatti, così chiamata perché utilizzata nel processo crittografico così come normalmente per sbloccare e bloccare porte o lucchetti, può essere una qualsiasi informazione alfanumerica e, in particolare, in questo scenario simmetrico deve essere identica sia per l'entità in trasmissione che quella in ricezione. Anche se, banalmente, la sicurezza del procedimento potrebbe essere attribuita

al fatto di mantenere celato l'algoritmo crittografico, trascurando inizialmente la qualità della chiave, il principio cardine della crittografia, formulato da Kerchoffs nel 1883 [5], afferma che: “ La sicurezza di un critto-sistema non deve dipendere dal tener celato il critto-algoritmo. La sicurezza dipenderà solo dal tener celata la chiave”. Passando in secondo piano lo studio di un efficace algoritmo di elaborazione, nasce, così, la necessità di risolvere uno dei più affascinanti problemi logici-matematici: **lo scambio delle chiavi:** Alice e Bob prima di poter trasmettersi informazioni al sicuro, devono, paradossalmente, concordare una chiave preoccupandosi proprio di evitare attacchi esterni condotti da Eva, senza aver avuto però la possibilità di un precedente mutuo accordo. Appare ovvio che se le entità sono vincolate in posizioni lontane o hanno limitate risorse di comunicazione la questione risulta abbastanza critica e di fondamentale importanza per la totalità del critto-sistema. Alcuni risultati [2], inoltre, hanno dimostrato che due entità in dialogo tra loro non riescono a condividere, con un' alta ed arbitraria probabilità di successo, un oggetto comune se non scambiano qualche informazione nel canale di comunicazione e non corrono, perciò, il rischio di esposizione ai tentativi di corruzione da parte di entità sconosciute. Meccanismi numerici che costruiscono un modello ottimo capace di sciogliere il nodo dello scambio di chiavi sono oggi ampiamente utilizzati nella Rete. Citiamo per esempio l'algoritmo **Diffie Hellman Merkle** a chiavi simmetriche oppure quello RSA a chiavi asimmetriche (esistono cioè una chiave pubblica e una privata per ogni entità) ideato da **Rivest Shamir Adleman**. Questi algoritmi oltre a sfruttare alcune speciali funzioni matematiche, che permettono la produzione di una chiave nota ad Alice e Bob, ma non a Eva, si basano essenzialmente sulla casualità della chiave, cioè sulla estrema difficoltà di indovinarla, anche conoscendo esattamente l'algoritmo di cifratura. Il numero e l'andamento di bit o di simboli all'interno della chiave sono le uniche caratteristiche che contraddistinguono la sicurezza del sistema, in quanto determinano le probabilità di successo e la durata temporale d'esecuzione dell'attacco condotto di Eva.

CAPITOLO 2
IL CANALE RADIO COME MEZZO DI GENERAZIONE DI CHIAVI

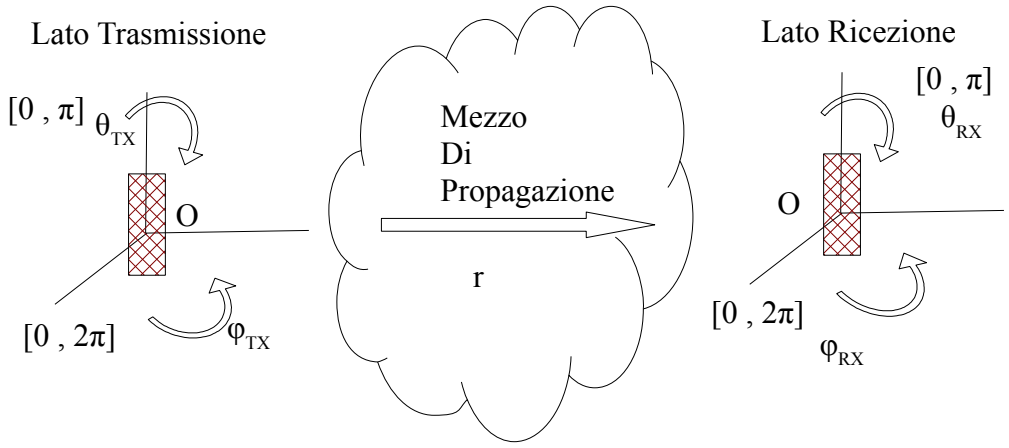


Fig.2 Rappresentazione del collegamento radio

Sfruttando la propagazione delle onde elettromagnetiche in un mezzo fisico riusciamo a trasmettere informazione tra due o più punti lontani tra loro. Se la trasmissione avviene in modo guidato il mezzo di propagazione è costituito da cavi, guide d'onda, linee di trasmissione o fibre ottiche, altrimenti se il mezzo di propagazione è composto dall'aria o dal vuoto stesso, la comunicazione avviene in modo **wireless** mediante l'utilizzo di antenne, ovvero trasduttori elettromagnetici, come mostrato in Figura 2, dove compare una schema di principio della tratta radio in spazio aperto con dettagli sui sistemi di riferimento sferici adottati nel centro di fase delle antenne. Se in primo luogo, la principale caratteristica delle onde di espandersi alla velocità della luce, o meno, in tutto lo spazio circostante è uno degli aspetti positivi, ed anche eccezionali, della propagazione libera, dal punto di vista della sicurezza diventa, invece, un elemento decisamente sfavorevole, in quanto chiunque è in grado, con la giusta attrezzatura, di captare i segnali elettromagnetici che transitano sul canale radio. E' sufficiente pensare alla radio usata sia per diffondere la musica, sia per le comunicazioni delle operazioni militari. Ciononostante il **canale radio**, inteso come entità fisica che caratterizza nel dominio del tempo e nel dominio delle frequenze la propagazione dei segnali, svela interessanti caratteristiche della sua intrinseca natura che permettono la costruzione di algoritmi per la generazione e la condivisione di chiavi ad un livello Fisico, cioè relativo alla Propagazione di onde Elettromagnetiche e non a livello Applicazione.

Teorema di Reciprocità:

Con riferimento alla Figura 3 sottostante, date due entità A e B elettromagnetiche caratterizzate da densità volumetriche di correnti elettriche o magnetiche (cioè le antenne) e contenute in uno spazio, il cui volume è occupato da un mezzo lineare, stazionario, non dispersivo (cioè l'aria o il vuoto), delimitato da una superficie con le relative condizioni al contorno di radiazione (cioè una regione illimitata aperta), il Teorema di Reciprocità afferma che la reazione, intesa come variazione della densità di corrente secondo le **leggi di Maxwel**l, (cioè il cambiamento del segnale registrato) dell'entità A, al campo elettromagnetico emesso dall'entità B, coincide con quella dell'entità B, rispetto al campo elettromagnetico generato dall'entità A.

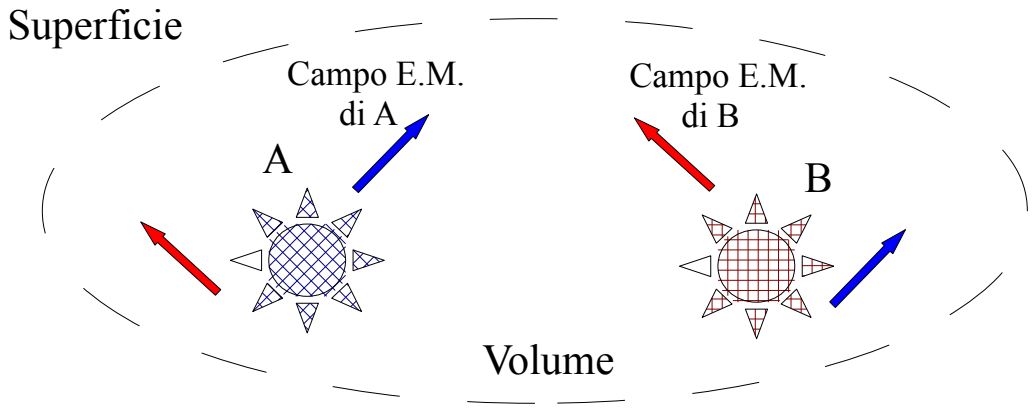


Fig.3 Illustrazione del Teorema di Reciprocità

In conclusione, sotto opportune condizioni, sussiste **l'intercambiabilità** tra due distinte sorgenti elettromagnetiche, in quanto ciò che "sente" il nodo A ad un estremo del canale radio coincide con quanto "sente" il nodo B dall'altro, anche se si scambiano la posizione.
Sebbene questo sia dimostrato dal punto di vista teorico e possa costituire le fondamenta di un possibile protocollo di generazione e di scambio chiavi, nel caso reale, è opportuno dover introdurre ulteriori fattori che completano il modello matematico-fisico di propagazione:

Il rumore:

Il rumore, indicato molto spesso con la sigla AWGN cioè **Additive White Gaussian Noise** [7] è descritto in termini probabilistici da una funzione gaussiana di densità di probabilità a valor medio nullo e viene spesso, in fase di analisi di un sistema elettromagnetico,

aggiunto artificialmente al segnale utile nel canale radio. Secondo l'effetto Johnson [7] il rumore negli apparati deriva dall'agitazione atomica o molecolare degli elementi, che compongono i metalli o i semiconduttori utilizzati negli apparati, e per questo motivo non può essere eliminato del tutto dai sistemi di telecomunicazione, ma solamente limitato con opportuni filtri. Dal punto di vista fisico il rumore altera tutti i segnali in gioco nella trasmissione, in modo completamente casuale e quindi può essere trattato analiticamente solamente dal punto di vista statistico. Per il nostro scopo risulta quindi un elemento assai dannoso che rappresenta la causa dei maggiori problemi tra nodo A e nodo B.

Multipath Propagation and Fading:

Un altro fattore correttivo è espresso dagli effetti, a volte disastrosi, della propagazione multipercorso ovvero **Multipath propagation**. Quando in fase di trasmissione moduliamo una certa sequenza di bit ad una certa frequenza portante e immettiamo tutto nel canale radio, in realtà dal punto di vista fisico attraverso l'antenna generiamo una serie di pacchetti di onde che si propagano nello spazio e nel tempo. A seconda, ad esempio, del rapporto che intercorre tra le dimensioni degli oggetti circostanti e la lunghezza d'onda del tono sinusoidale della portante avvengono complessi fenomeni di propagazione: diffusione, riflessione, rifrazione, assorbimento ecc.. che vanno ad alterare significativamente il segnale originario, in fase di ricezione. In conclusione possiamo affermare che l'ambiente, in cui avviene la comunicazione, influenza in modo preponderante la forma e la natura dei segnali, sia nel tempo, in quanto assistiamo ad una serie di echi e sovrapposizioni del segnale, sia in frequenza, in quanto assistiamo ad un cambiamento di fase e a possibili interferenze distruttive.

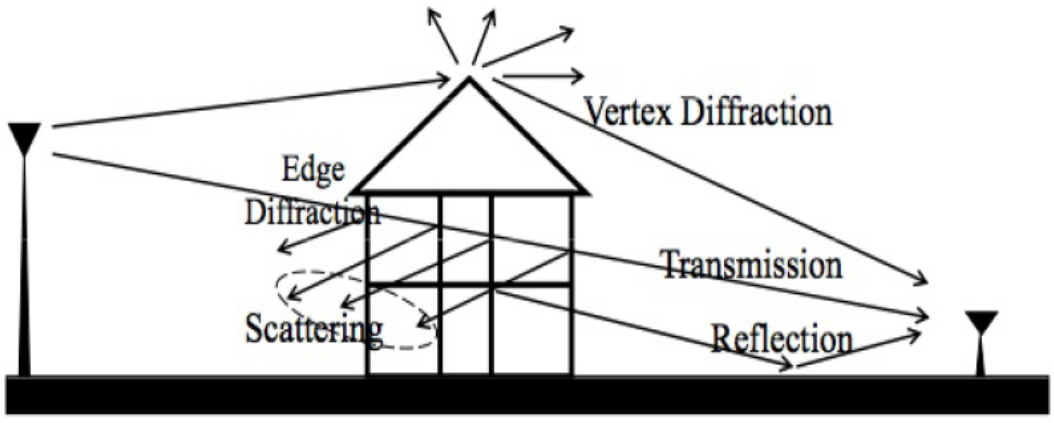


Fig.4 Esempio degli effetti del Multipath Propagation

Il canale radio, inoltre, non può essere considerato sempre stazionario e nemmeno statico: ad esempio possiamo condurre un esperimento in cui trasmettendo da un terminale base un segnale di test, prima fissiamo un punto nello spazio e così otteniamo oscillazioni del segnale ricevuto nel corso del tempo, poi, dualmente, fissiamo un'istante preciso nel tempo e osserviamo variazioni del segnale ricevuto nello spazio considerato. Se in aggiunta i nodi wireless, si muovono ad una certa velocità, la questione si complica ancora di più: la durata temporale del segnale deve essere molto minore del **Tempo di coerenza del canale**, così da poter considerare approssimativamente stazionario il canale stesso, rispetto alle variazioni dovute all'effetto Doppler. Da un punto di vista sistemistico, quindi, un'ulteriore importante fattore da considerare è la funzione di trasferimento del canale di propagazione che varia sia nel tempo che in frequenza, facendo così registrare informazioni differenti in luoghi e secondi diversi, così come mostrato nella Figura 5 seguente:

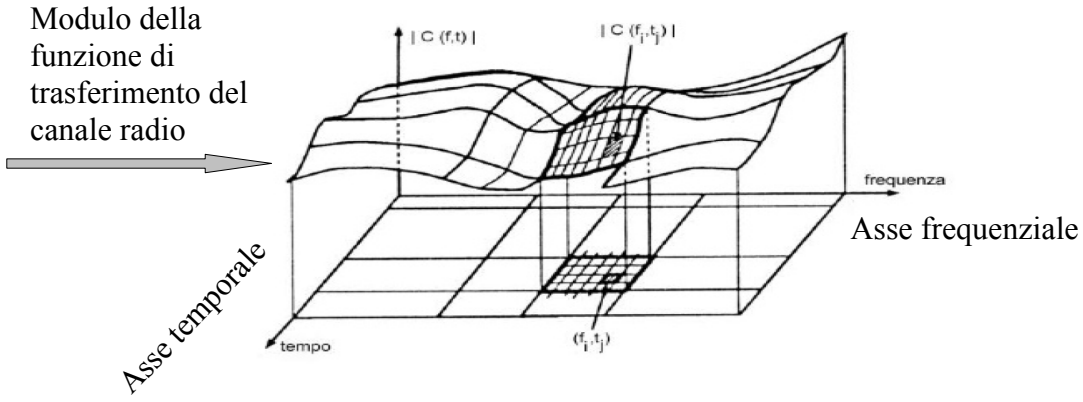


Fig.5 Fluttuazioni del canale radio

Correlazione spaziale dei canali:

L'ultimo fattore è formato dalla correlazione statistica tra i canali radio presenti nello scenario. E' dimostrato [1] che una qualsiasi entità nemica E situata ad una distanza maggiore almeno una semilunghezza d'onda dall'entità A o B riceverà un segnale **statisticamente indipendente** dagli altri, perché derivante da un distinto canale di propagazione, che, per quanto detto precedentemente, sarà caratterizzato da variazioni temporali e spaziali dissimili da quelle riscontrabili nel canale principale tra A e B.

In conclusione possiamo ora interpretare il canale radio come una fonte di informazione e sfruttare la sua natura non deterministica per estrapolare una chiave di sicurezza da utilizzare per instaurare poi una comunicazione priva di minacce. Così come è stato fatto per la **tecnologia MIMO**, invece che cercare di lottare assiduamente contro le avversità del mondo elettromagnetico, si cerca di studiare in quale modo si possano utilizzare al meglio le avanzate proprietà della propagazione per aumentare la qualità del collegamento, la bit rate o ad esempio come in questo caso la sicurezza nelle reti wireless.

CAPITOLO 3
PROCEDIMENTO DI GENERAZIONE DI CHIAVI

Diversi approcci sono stati condotti in letteratura per ideare e mettere in pratica un possibile protocollo che risolva adeguatamente lo scambio di chiavi tra due o più entità wireless. La maggior parte di essi riguarda la misurazione di un parametro, molto comune negli apparati di reti wireless, cioè RSSI ovvero **Received Signal Strength Indicator** che indica, con valori numerici interi, codificati con 8 bit unsigned, dell'ordine dei milliWatt ed espressi in dB, il valor medio del livello di potenza del segnale ricevuto durante una certa finestra temporale, proporzionale a multipli del tempo di simbolo. Così come delineato in [1], il protocollo comune, adottato da alcuni studi in letteratura, si suddivide in tre parti: Fase uno: Collezione dei valori RSSI attraverso il canale radio, Fase due: Elaborazione dei valori tramite un preciso algoritmo reso pubblico, Fase tre: Riconciliazione delle chiavi o Correzione degli errori.

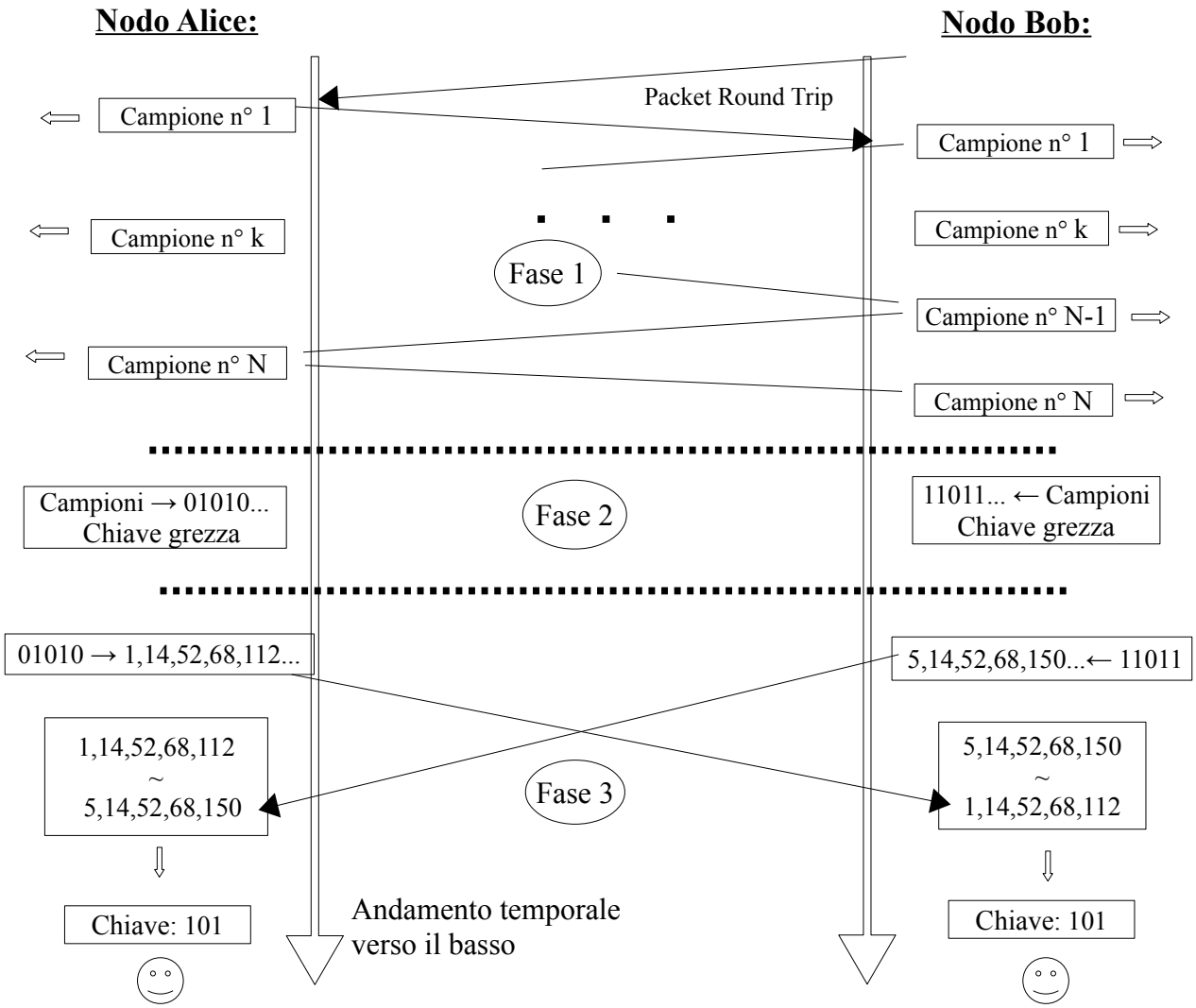


Fig.6 Schema di principio del procedimento di generazione chiavi

Descrizione del protocollo di generazione chiavi con riferimento alla Figura 6:

La prima fase è quella più critica, poiché se i nodi A e B avessero il clock di sistema ben sincronizzato tra di loro e potessero comunicare in modo full duplex, si scambierebbero una serie di pacchetti prova (non importa in questo contesto il loro contenuto informativo) ad un passo temporale preciso e collezionerebbero così una sequenza identica, a meno del rumore, di valori RSSI nel tempo. Eva, di nascosto, seguirebbe la stessa procedura con l'intento di captare gli stessi valori di RSSI di Alice o di Bob, ma essendo fisicamente distinta dai due nodi principali, la sua sequenza di campioni RSSI sarebbe totalmente diversa e, per di più, sfasata nel tempo. E' proprio questo, in particolare, il cuore del meccanismo fisico utilizzato per compiere lo scambio di chiavi dai lavori in letteratura, ad esempio [2],[3], in quanto si verificano sia una precisa reciprocità tra i valori di A e B, grazie al **sincronismo** e all'assenza di ritardi, sia una profonda **incorrelazione** tra i campioni di Alice ed Eva e quelli di Bob ed Eva, dovuta all'indipendenza statistica delle variazioni di Fading dei canali radio in gioco, come precedentemente esposto.

In seguito, passando alla fase due, eseguendo un semplice algoritmo ogni nodo potrebbe estrapolare, a seconda dell'andamento nel tempo dei campioni RSSI, una sequenza di bit per comporre una chiave grezza, che dovrebbe essere il più possibile pseudo-casuale. Per far questo, ad esempio vedi [3], si possono utilizzare due **soglie orizzontali** che formino una fascia di valori centrata sul valore medio dei valori RSSI, in modo da suddividere nettamente tre regioni mutualmente esclusive: quando il RSSI campione in esame è superiore alla soglia superiore vi si associa nella chiave grezza un bit '1', se invece è inferiore alla soglia inferiore allora un bit '0', altrimenti, se cade all'interno della suddetta fascia, viene scartato dall'algoritmo. Per una data lunghezza di chiave, inizialmente la soglia superiore si posiziona alla pari del campione RSSI di valore massimo e quella inferiore alla pari del campione RSSI di valore minimo, poi, gradualmente, ad ogni ciclo di iterazione della funzione di quantizzazione, si diminuiscono i parametri “alpha”, restringendo conseguentemente la fascia di esclusione, in modo da effettuare progressivi tentativi di quantizzazione, fino al raggiungimento del numero di bit sufficienti. La calibrazione del posizionamento delle soglie avviene come mostrato nelle seguenti equazioni:

Valor medio temporale del vettore RSSI è indicato con l'operatore E [] (Expected Value), in figura è rappresentato dalla riga orizzontale tratteggiata rossa al centro dell'immagine. Deviazione standard del vettore RSSI è indicato da STD [] (Standard Deviation), non compare direttamente in figura anche se stabilisce l'ampiezza delle soglie.

Upper Threshold = E[RSSI] + (Alpha_UT * STD[RSSI])
Lower Threshold = E[RSSI] - (Alpha_LT * STD[RSSI])

In figura sono entrambe rappresentate dalle righe orizzontali tratteggiate nere, la soglia superiore al di sopra del valor medio e quella inferiore al di sotto.

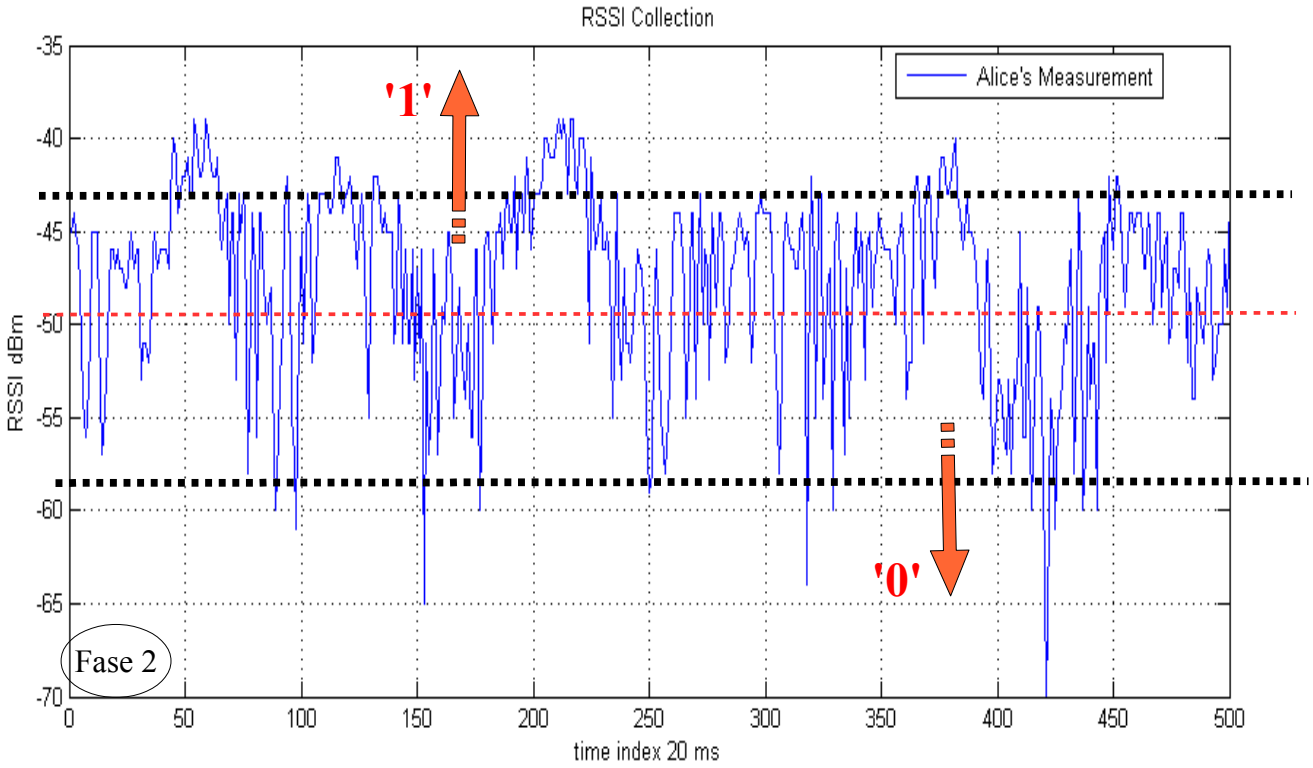


Fig.7 Rappresentazione delle fase di quantizzazione dei campioni RSSI

Effettuando questa sorta di clipping della curva tracciata dai valori RSSI collezionati, si cerca di avere bit il più possibile incorrelati tra loro perché, essendo relativi a livelli di potenza molto distanti, risalgono a istanti di campionamento in cui il canale radio assumevano connotati diversi per via del Multipath Fading. Purtroppo bisogna far fronte anche ad un **compromesso**: se si desidera aumentare il numero di bit necessari per comporre la chiave è sufficiente, come precedentemente affermato, restringere l'ampiezza

della fascia di esclusione e lasciar libertà alla funzione di quantizzazione di generare più bit dai campioni RSSI, anche se, così facendo, si riduce il margine di indipendenza statistica dei bit stessi. Insomma questo si traduce o in una chiave corta e molto casuale, oppure lunga e più facilmente predicibile.

Infine, nella terza fase, come rappresentato in Figura 6, Alice e Bob possono scambiarsi, per correggere eventuali imprecisioni, un semplice vettore contenente gli indici di posizione dei campioni RSSI utilizzati nel processo di quantizzazione. Ogni nodo, poi, confrontando quest'ultimo dato con il proprio vettore di indici dei campioni RSSI collezionati, sarà in grado di delineare un sotto-elenco di indici dei campioni RSSI in comune. In questo modo i bit della chiave grezza, a cui corrispondono campioni RSSI diversi tra Alice e Bob, vengono scartati, mentre i restanti formano la chiave definitiva di sicurezza . Anche se può sembrare una mossa falsa dal punto di vista della sicurezza, Eva catturando il pacchetto contenente il vettore di riconciliazione dei bit, entrerebbe in possesso solo di informazioni in merito alla posizione temporale dei campioni RSSI utilizzati per la chiave e non del valore binario, a loro associato.

Parametri di valutazione del procedimento:
In conclusione le **figure di merito** da considerare, come evidenziato da [1], per valutare la qualità dell'intero procedimento sono essenzialmente quattro:

La frequenza relativa di concordare (**Key Agreement Rate**) una chiave da parte di Alice e Bob calcolata semplicemente come il rapporto dei casi favorevoli, in cui la chiave di Alice coincide con quella di Bob, rispetto a tutti i casi considerati. Idealmente pari al 100%.

La frequenza relativa di rubare la chiave (**Key Attack Rate**) da parte di Eva “ascoltando” Alice o Bob, calcolata semplicemente come il rapporto dei casi favorevoli, in cui la chiave di Eva coincide con quella di Bob o di Alice, rispetto a tutti i casi considerati. Idealmente pari allo 0%

La qualità della Casualità (**Key bit Randomness**) della chiave concordata, calcolata attraverso alcune funzioni di test ricavate dalla pubblicazione [8]:

1) Frequency Monobit Test: il numero di bit '1' nella chiave dovrebbe corrispondere al numero dei bit '0', così da poter stimare una di funzione di massa di probabilità del 50% per entrambi i valori discreti.
2) Frequency Test within a Block: ripeto esattamente il test precedente a diversi sotto-blocchi di lunghezza prefissata dell'intera chiave così da valutarne la casualità parziale.
3) Runs Test: scorrendo l'intera chiave conteggio il numero di parole di bit composte da 'k' bit adiacenti dello stesso valore binario. Se il numero di parole di '1' è identico a quello delle parole di '0', al variare della lunghezza 'k' della parola di bit, allora la pseudo-casualità è confermata dal test.
4) Autocorrelation Function Test: la funzione di autocorrelazione a tempo discreto dei bit della chiave deve tendere ad una delta di dirac nell'origine, cioè assumere un valore unitario all'istante zero e un valore nullo in tutti gli altri casi di valutazione.
5) Discrete Fourier Transform Test: se la chiave è composta da pattern di bit qualsiasi, che però si ripetono in modo periodico, la qualità di pseudo-casualità viene meno perché vi è correlazione tra i diversi bit e risulta molto più facile individuare la struttura della chiave. Questa singolarità è ben visibile nel dominio delle frequenze attraverso il calcolo della DFT della chiave, dopo essere stata mappata in modo simmetrico, cioè ad un bit '1' corrisponde un valore di +1 e ad un bit '0' corrisponde un valore di -1. Se la stima dello spettro gode di caratteristiche simili al noto spettro bianco del rumore AWGN allora risulta confermata la casualità della chiave.

La bit rate di generazione (**Key bit Generation Rate**), ovvero il numero di bit concordati nell'unità di tempo all'uscita dell'intero processo. Quest'ultimo parametro serve sopratutto a valutare il tempo massimo richiesto dall'intero procedimento prima di poter adoperare la chiave di sicurezza.

Di seguito propongo 3 esempi applicativi delle funzioni di test di casualità esposte sopra:
Esempio uno:
La chiave gode di pseudo-casualità ed è quindi confermata da tutte le funzioni test:
Chiave di sicurezza: dal bit numero 1 al 25: 01001 01110 00111 01010 01001
dal bit numero 26 al 50: 10001 10011 10001 01100 11101

Test uno: In totale: 25 bit a '1' e 25 bit a '0'
Esito positivo

Test due: Prendendo blocchi da 25 bit ad esempio
(cioè dividendo la chiave a metà)
Parte iniziale: 12 bit a '1' e 13 bit a '0',
Parte finale: 13 bit a '1' e 12 bit a '0'
Esito positivo

Test tre: Considerando sequenza di 2 bit e da 3 bit ad esempio
8 coppie di bit a '1' e 8 coppie di bit a '0',
3 tris di bit a '1' e 2 tris di bit a '0'
Esito positivo

Test quattro: Esito positivo

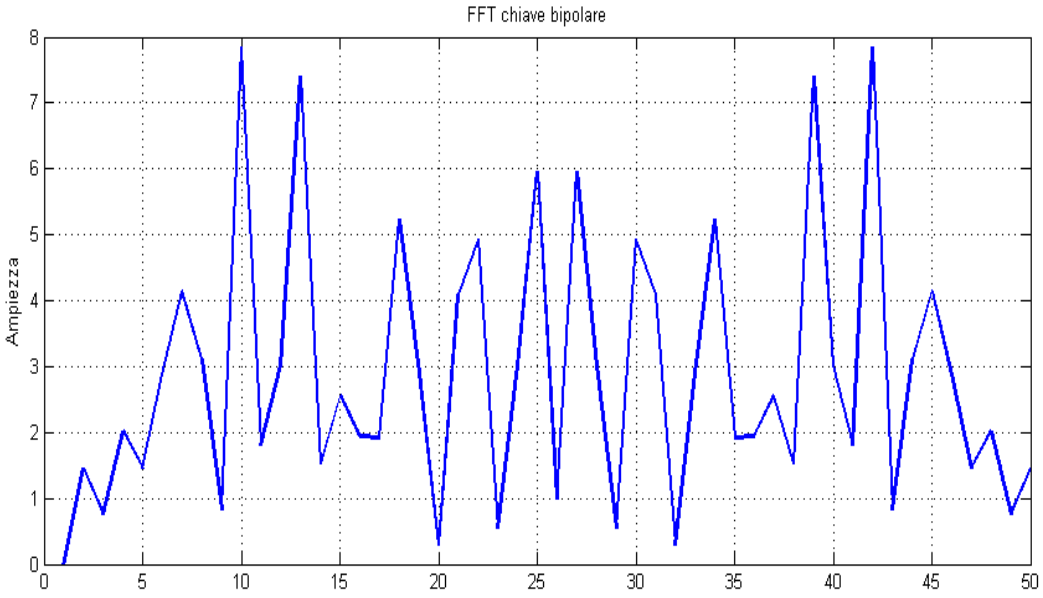


Fig.8a Grafico in frequenza della chiave dell'esempio uno

Esempio due. La chiave non è per niente casuale e viene bocciata da tutti i test:

Chiave di sicurezza: da 1 a 25: 11111 11111 11111 00000 00000
da 26 a 50: 00000 00000 00000 00000 11111

Test uno: In totale: 15 bit a '1' e 30 bit a '0'
Esito negativo

Test due: Prendendo blocchi da 25 bit ad esempio.
(cioè dividendo la chiave a metà)

Parte iniziale: 15 bit a '1' e 10 bit a '0',

Parte finale: 5 bit a '1' e 20 bit a '0'

Esito negativo

Test tre: Considerando sequenza di 2 bit e da 3 bit ad esempio

16 coppie di bit '1' e 24 coppie di bit '0',

12 tris di bit '1' e 18 tris di bit '0'

Esito negativo

Test quattro: Esito negativo

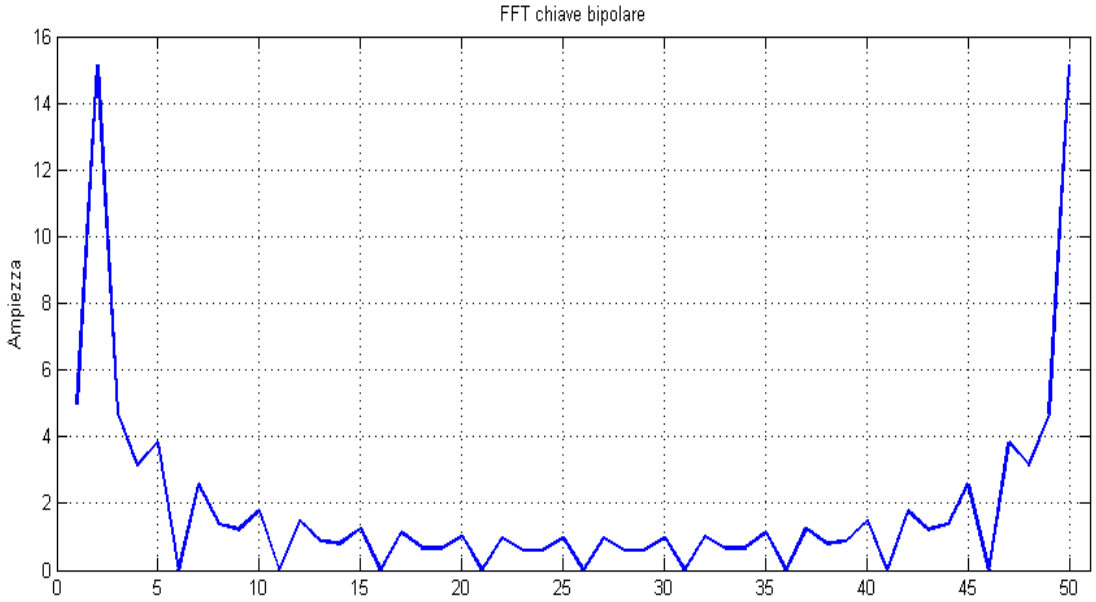


Fig.8b Grafico in frequenza della chiave dell'esempio due

Esempio tre. La chiave può sembrare casuale dal numero di '1' e '0', ma invece è periodica:

Chiave di sicurezza: da 1 a 25: 10110 01101 10110 01101 10110

da 26 a 50: 01101 10110 01101 10110 01101

Test uno: In totale: 30 bit a '1' e 20 bit a '0'

Esito negativo

Test due: Prendendo blocchi da 25 bit ad esempio

(cioè dividendo la chiave a metà)

Parte iniziale: 15 bit a '1' e 10 bit a '0',

Parte finale: 15 bit a '1' e 10 bit a '0'

Esito negativo

Test tre: Considerando sequenza di 2 bit

10 coppie di bit '1' e 0 coppie di bit '0'

Esito negativo

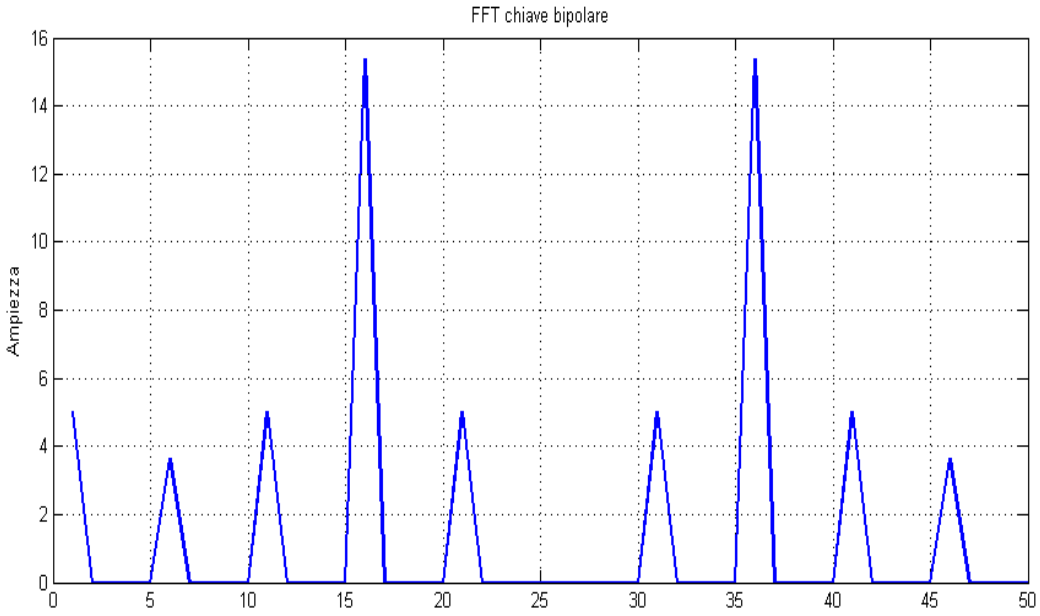


Fig.8c Grafico in frequenza della chiave dell'esempio tre

Confrontando i risultati grafici del Test numero quattro dei tre esempi di chiavi di sicurezza di cui sopra:

In figura 8a si può notare che l'escursione dei valori in frequenza della prima chiave sia molto limitata in ampiezza. La forma d'onda è infatti molto simile a quella del rumore.

A parte la presenza di un picco iniziale verso l'alto dovuto alla sequenza iniziale di bit '1', l'escursione in ampiezza dei campioni DFT in Figura 8b è molto contenuta. Il basso valore di quasi la totalità dei campioni indica un buon numero di bit adiacenti '0' nella chiave.

Molto rilevante per lo scopo del Test quattro appare il grafico in Figura 8c. La presenza di un notevole picco verso l'alto, rispetto al valore medio di tutti i campioni DFT, segnala che un pattern di bit viene ripetuto all'interno della chiave stessa.

CAPITOLO 4
HARDWARE E SOFTWARE UTILIZZATO

Con il termine **Wireless Sensor Network** si intende una nuova concezione di tecnologie ICT che unendo vari elementi di elettronica, sensori, reti di calcolatori e telecomunicazioni wireless riesce a dar vita ad un piccolo insieme di nodi autonomi in comunicazione tra loro capaci di svolgere svariati compiti ed adattarsi a diversi ambienti, come in Figura 9. Le molteplici aree di applicazione possono essere il campo medico, il monitoraggio ambientale, la prevenzione di eventi sismici o climatici, controllo per l'efficienza energetica, la sicurezza di infrastrutture, la rintracciabilità di persone o animali ecc...

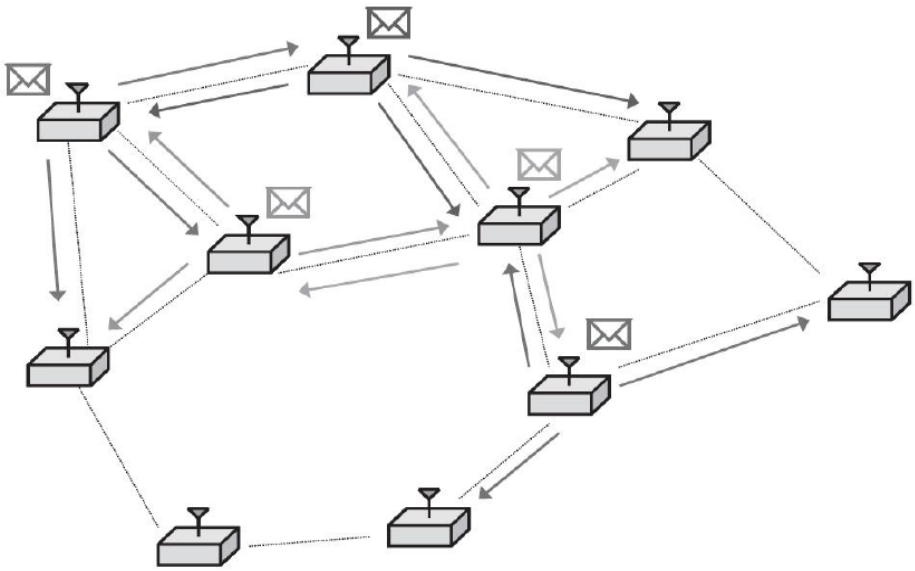


Fig.9 Esempio astratto del flusso di pacchetti dati all'interno di un WSN.

Diversi dispositivi sono oggi disponibili sul mercato e si distinguono essenzialmente per le loro caratteristiche tecniche: ad esempio, l'utilizzo della frequenza 2.4 Ghz della banda ISM per le modulazioni standard oppure l'utilizzo della tecnologia UltraWideBand come forma di comunicazione. Gli standard che stanno alla base di questi prodotti, spesso denominati **Zigbee**, sono IEEE di 802.15.4, vedi Figura 10, e 802.15.4a e stanno all'interno della grande gruppo IEEE 802 per le reti Internet e Wireless. Le principali caratteristiche comuni a quasi tutti i nodi WSN, al di là dell'architettura interna, sono:

Bassa velocità di trasmissione (< Megabit / sec)

Breve raggio di copertura (< 500m)

Potenza di trasmissione limitata (al max 0.5 mWatt)

Buona sensibilità in ricezione (al max -85dBm)

Basso consumo sia in modalità operativa che in standby (< 30 milliAmpere)

Basso costo commerciale

Piccole dimensioni (< 30 cm)

Diverse tipologie di rete possibili

Instradamento a commutazione di pacchetto (Abilitazione al Routing)

Meccanismi di gestione Accesso Canale (strato MAC)

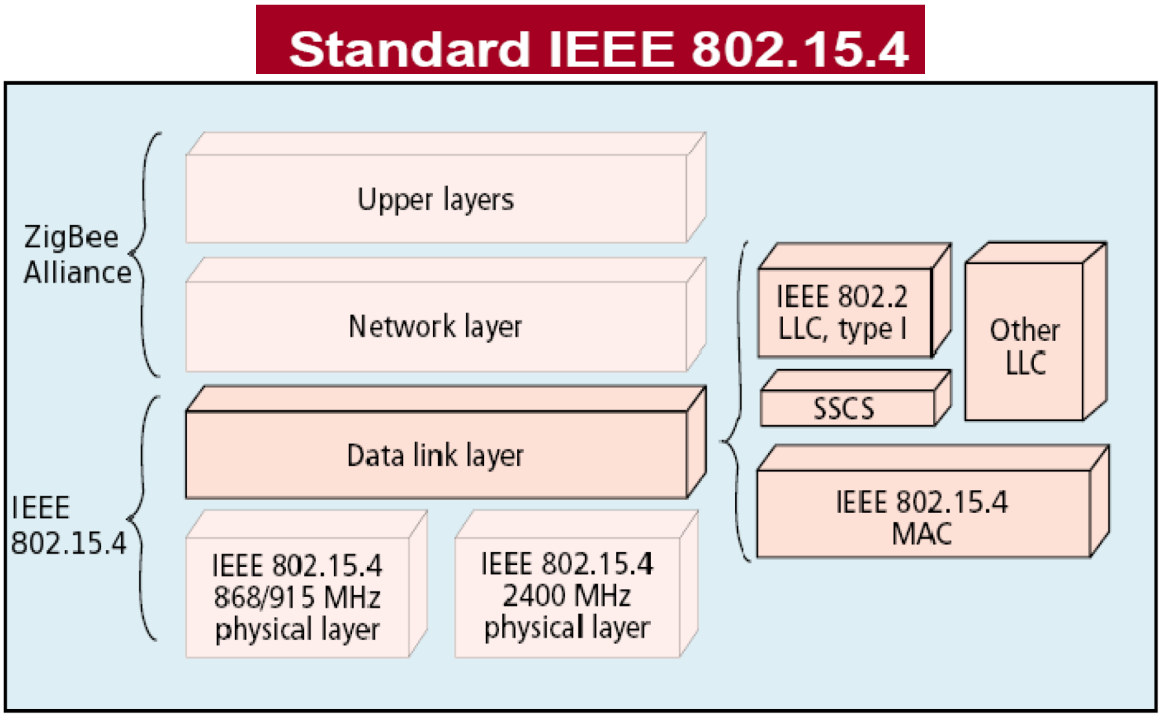


Fig.10 Stack del protocollo IEEE 802.15.4

Più in dettaglio ho utilizzato per la parte pratica il **kit CC2430** della Chipcon, Texas Instruments. Come mostrato in Figura 11, compone di schede singole dei nodi (DevelopmentBoard) e schede piattaforma (SmartRF04EvaluationBoard) di interfacciamento con il computer per l'analisi del traffico di pacchetti o il debugging dei protocolli implementati. Ho utilizzato il software IAR Embedded Workbench per la programmazione dei microcontrollori dei nodi e infine il tool Packet Sniffer messo a disposizione dalla TI, per collezionare e memorizzare i dati delle misure effettuate.

Fig.11 Presentazione del Kit Chipcon CC2430

L'architettura del Chip CC2430 si compone di numerosi elementi, vedi Figura 12:

Memoria RAM da 8KB e Memoria non volatile di tipo Flash da 128KB
DMA e Memory Arbitrator per la gestione della memoria
Interfacce per protocolli di comunicazione standard come ad esempio USART
CPU 8051 come unità di calcolo
Controlli per la gestione delle risorse di alimentazione e della modalità di funzionamento
Oscillatori al quarzo per generazione del clock di sistema

L'architettura del blocco radio, in particolare, rappresentato in Figura 13, si compone di:
Blocco processore del meccanismo CSMA/CA
Blocchi sommatori e produttori (mixer) e registri a scorrimento
Blocchi Analog to Digital and Digital to Analog Conversion
Blocco di modulazione e demodulazione

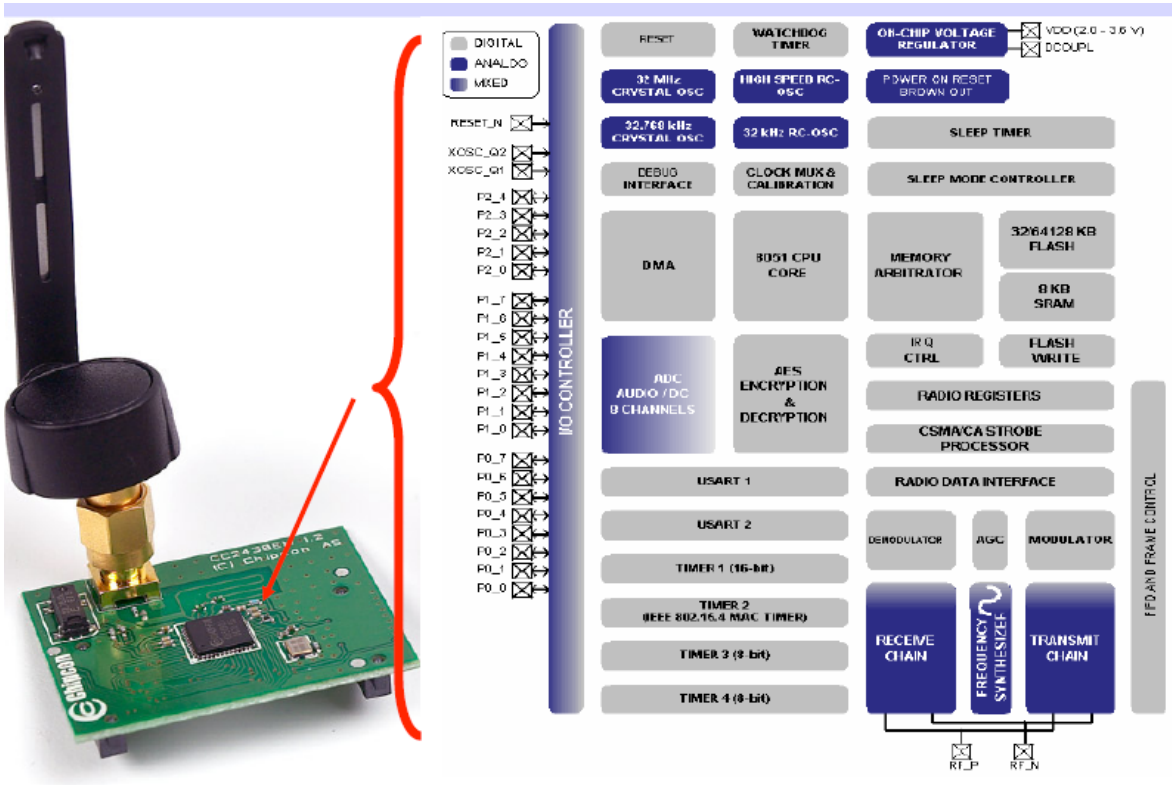


Fig.12
Architettura interna del chip CC2430 dei nodi Zigbee

CC2430 chip RADIO

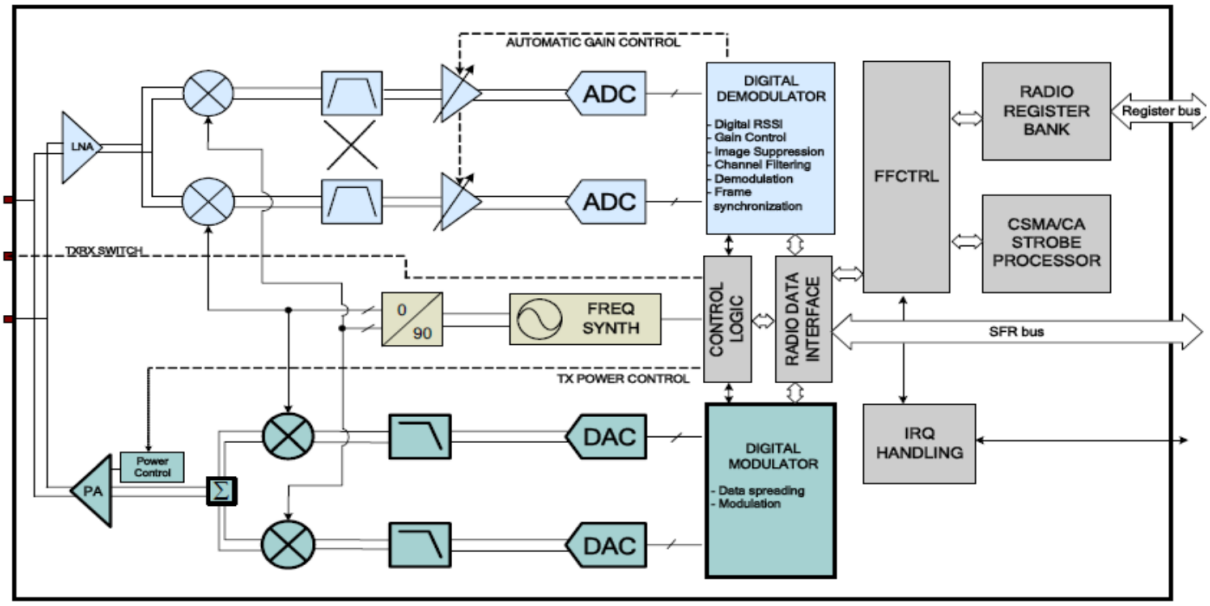


Fig.13
Struttura interna del blocco relativo all'elaborazione a radio frequenza

CAPITOLO 5
PROTOCOLLO DI RACCOLTA MISURE

La configurazione dei nodi Alice, Bob ed Eva utilizzata per la raccolta misure è stata la seguente:

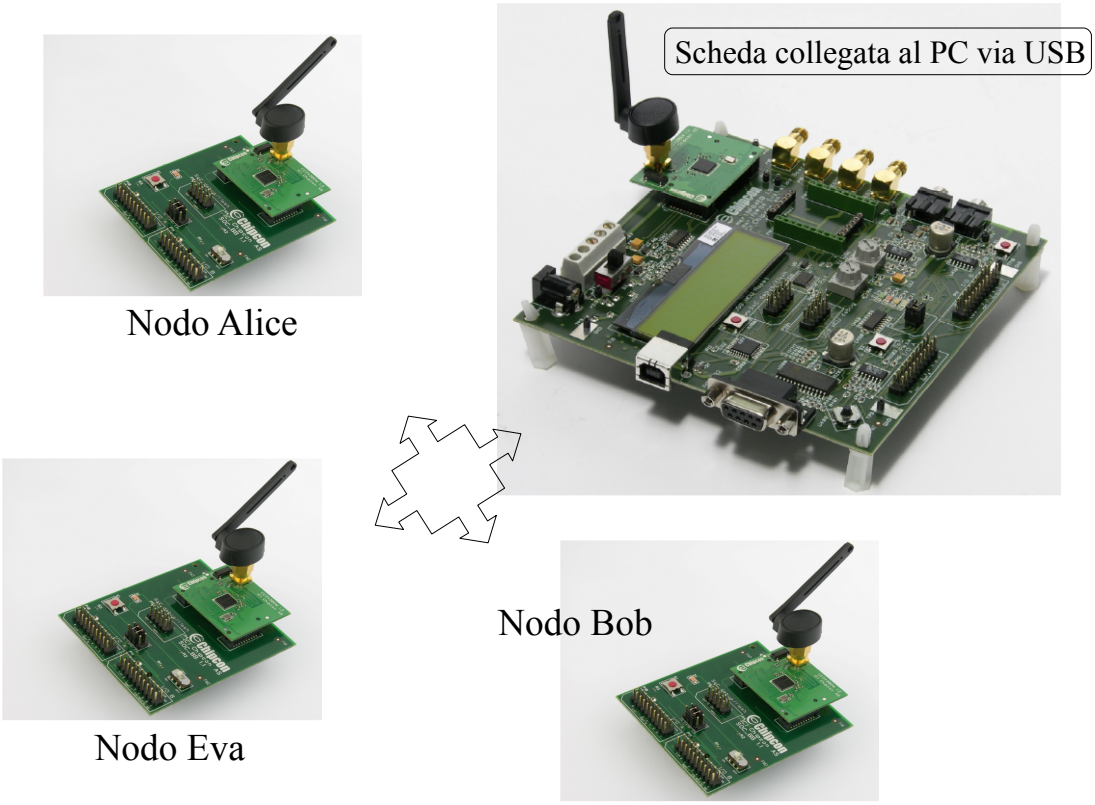


Fig.15
Configurazione dei nodi Zigbee in fase di misurazione

Il **protocollo** a livello applicativo è il seguente:

1) Posizionamento manuale di 3 + 1 nodi Zigbee nell'ambiente di misurazione.

2) Accensione manuale dei nodi Alice, Bob, Eva.

3) Inizializzazione dei nodi e relativa associazione.

4) Alla scadenza di un timer di alcuni secondi, Bob crea un pacchetto standard e lo invia in modalità broadcast, cioè non specificando un indirizzo preciso per il destinatario. Crea

inoltre un parametro interno che conteggi il numero dei pacchetti trasmessi. Poi si mette in attesa.

5) Eva colleziona tutti i pacchetti di passaggio, senza aver la possibilità però di interferire attivamente o di fare jamming nel canale radio. Crea due buffer distinti in memoria RAM e vi inserisce i valori di RSSI registrati ad ogni pacchetto ricevuto da Alice o da Bob. Crea anch'essa un contatore per il numero dei pacchetti, sia per quelli provenienti da Alice che da Bob.

6) Alice, non appena ricevuto il pacchetto di Bob, incrementa il proprio contatore di pacchetti e registra in memoria RAM il livello di RSSI associato al messaggio corrente. Infine trasmette lo stesso pacchetto indietro a Bob. Poi si mette in attesa del successivo.

7) Bob ricevuto il pacchetto di Alice, incrementa il contatore di pacchetti e memorizza anche lui il valore di RSSI associato. Poi aspetta un intervallo di 20 millisecondi prima di trasmettere un altro pacchetto, per lasciare il tempo minimo di elaborazione dati sia ad Alice che ad Eva. In alcune misure l'intervallo è stato portato a 30 millisecondi.

Per chiarezza, ciò che importa per la questione inerente la reciprocità tra Alice e Bob non è tanto l'intervallo temporale tra un pacchetto e il successivo trasmessi da Bob, ma il il lasso di tempo che intercorre tra il pacchetto di Bob e la contro-risposta di Alice.

8) Il procedimento di scambio pacchetti viene iterato in questa modalità “Master (Bob) Slave (Alice)” finché tutti i contatori di numerazione pacchetti non raggiungono il valore di 500 campioni RSSI.

9) Ogni nodo in gioco, infine, preleva 100 valori di RSSI alla volta dai buffer della RAM e li trasmette al nodo ausiliario di riferimento che li memorizza nel PC in modo definitivo.

Prendendo in considerazione le ipotesi e gli aspetti dei precedenti capitoli, elenco qui di seguito una serie di problemi che ho riscontrato implementando il protocollo di generazione di chiavi con i nodi Zigbee:

La comunicazione avviene sempre in modalità **half duplex** e quindi l'esatto sincronismo tra Alice e Bob non può essere raggiunto. Inoltre a seguito di un eventuale errata numerazione dei pacchetti scambiati, per via di eventuali problemi nel canale radio, perdite di Ack o ritrasmissioni di pacchetti dati, spesso si presenta un **progressivo disallineamento temporale** tra i valori RSSI collezionati nel corso dello scambio di pacchetti. Vedi come esempio le Figura 16 e 17. Nell'implementazione SW del codice del protocollo, infatti, per semplicità, ho inserito un meccanismo di controllo che non risolvesse del tutto, come ad esempio nel protocollo TCP di livello Trasporto, i vari problemi di alterazione della numerazione in ordine cronologico dei 500 valori RSSI, ma che si limitasse, solo, a garantire la sequenzialità dei campioni raccolti. Ciononostante, nella totalità dei casi non è stato necessario regolamentare l'accesso al canale dei vari nodi a livello MAC, in quanto per questo scopo è stato sufficiente il ben noto meccanismo **CSMA-CA** (Carrier Sense Multiple Access with Collision Avoidance).

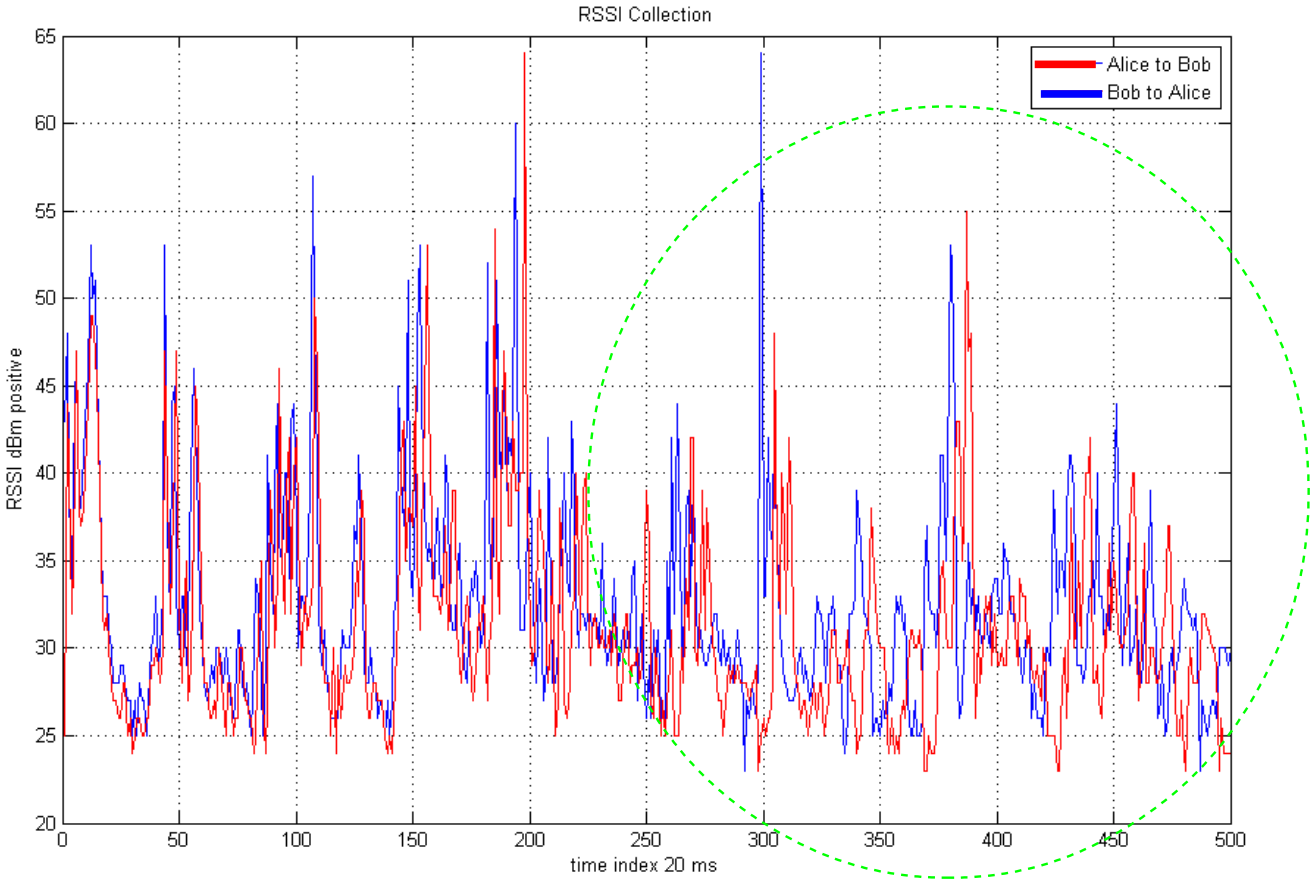


Fig.16
Esempio di disallineamento temporale dei campioni di Alice e di Bob

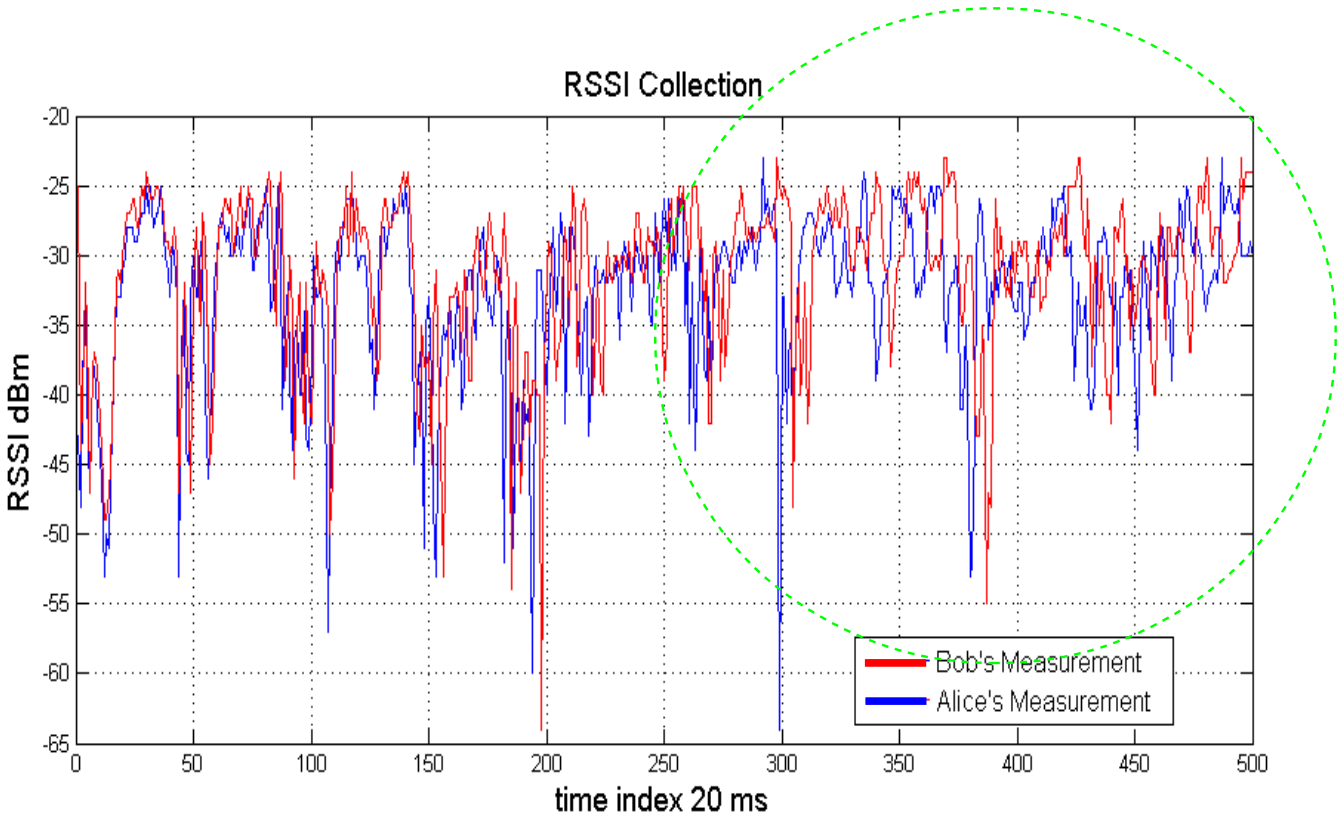


Fig.17
Altro esempio di disallineamento temporale dei campioni di Alice e di Bob

Il tempo di reazione con cui il nodo Alice riesce a rispondere prontamente al messaggio di Bob è abbastanza limitato e per via del tempo di accesso alla memoria, dell'elaborazione dati e della gestione dei messaggi di Acknowledgment, non può scende sotto il **1millisecondo ,** come mostrato in Figura 18. In particolare si denota che i campioni di Bob, per come è progettato lo scambio di pacchetti, sono posizionati qualche millisecondo di tempo dopo il corrispondente valore di Alice. Lo stesso vale per Eva ma in quel caso risulta una condizione positiva per la sicurezza. Questo risultato va a compromettere la reciprocità del canale e il soddisfacimento del vincolo dato dal tempo di coerenza per alte velocità.

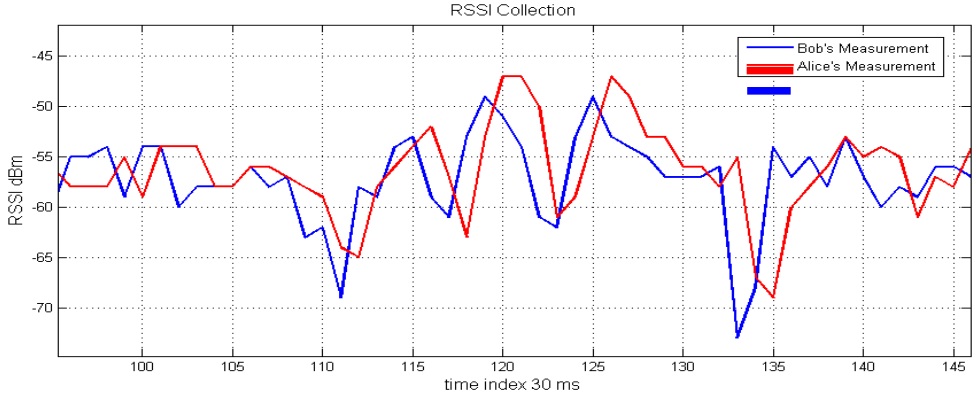


Fig.18 Esempio di sfasamento temporale dovuto alla comunicazione Half Duplex

Il payload (cioè il carico di dati contenuto in ogni pacchetto) non può superare i 100 byte. Per questo motivo i nodi nello scenario alla fine del processo riportano i dati al nodo referente sotto forma di 5 pacchetti da 100 valori RSSI ciascuno. Dal punto di vista delle prestazioni questo vincolo ha limitato il numero di campioni misurabili realisticamente.

Così come proposto da [3],[2] ho suddiviso l'insieme di misure possibili in diversi scenari per poter evidenziare le diverse conseguenze nei casi reali di funzionamento:

> **Scenari con nodi statici o in movimento:** le variazioni dei valori RSSI nel tempo raccolte nel caso in ci sia uno o più nodi in movimento, essendo più accentuate e ricche come contenuto informativo, per via degli aspetti complessi della propagazione, offrono un'ottima predisposizione all'algoritmo di quantizzazione ai fini di una chiave pseudo-random, mentre nel caso statico ho riscontrato che, nella quasi totalità dei casi, i cambiamenti nel tempo dei campioni sono dovuti principalmente al rumore e alle interferenze e quindi non utili ai fini della generazione delle chiavi.

Esempio in caso statico

Esempio in caso dinamico

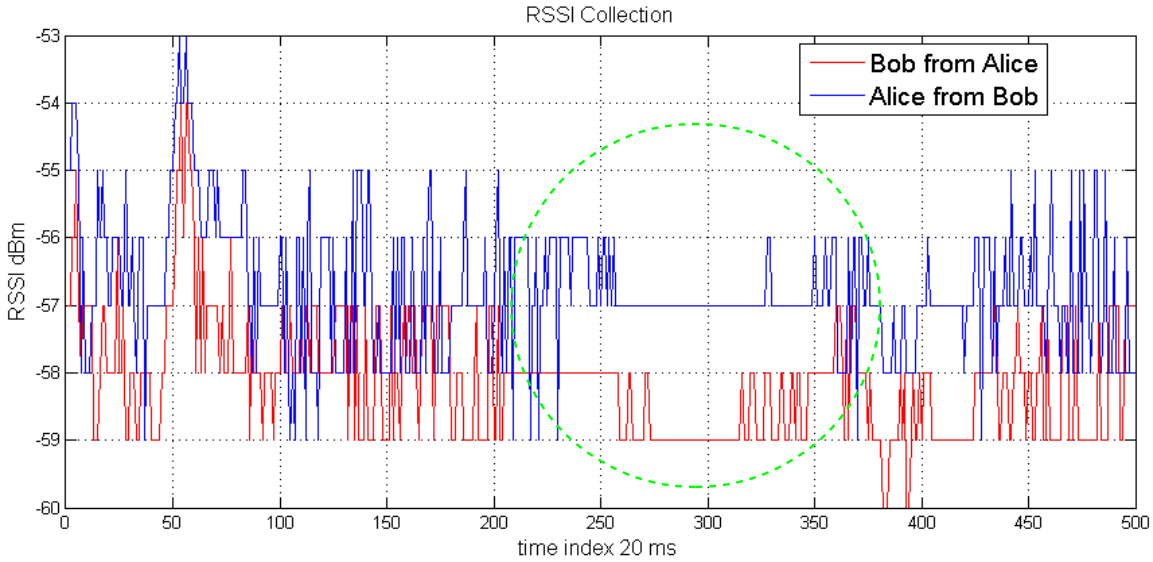


Fig.19 Andamento nel tempo dei campioni RSSI in scenario statico

Nella Figura 19 si può notare nel cerchio verde come vi sia pochissima variazione in ampiezza dei valori di potenza registrati in questo scenario, dove i nodi sono fermi.

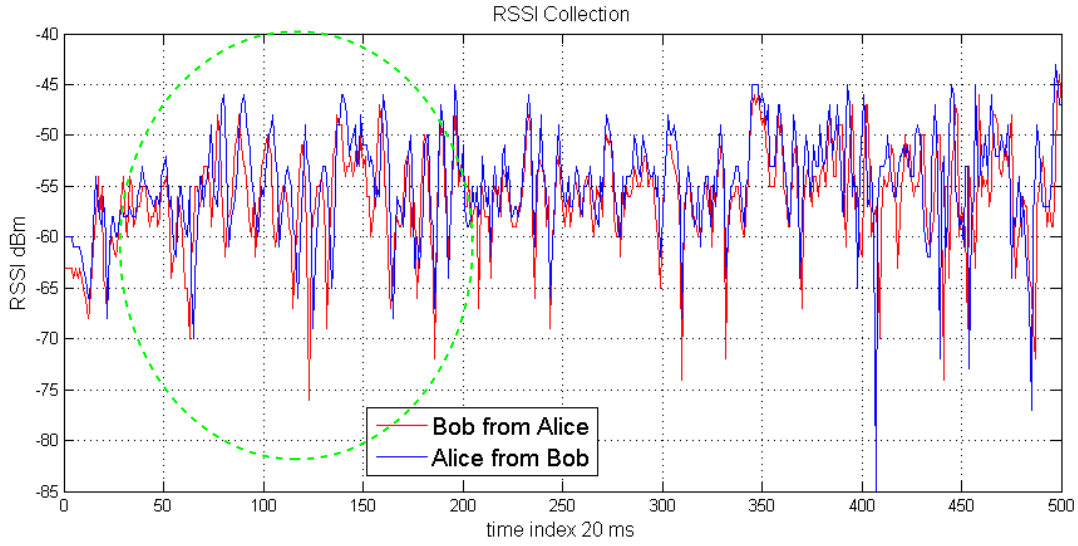
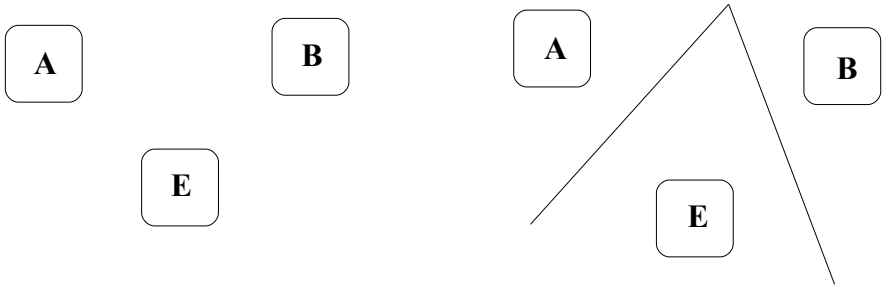


Fig.20 Andamento nel tempo dei campioni RSSI in scenario in movimento

In Figura 20 si può notare nel cerchio verde che l'escursione in ampiezza è di circa 30dBm e che la quasi perfetta reciprocità tra i campioni di Alice e di Bob porta a delle curve molto simili per tutto l'intervallo di osservazione.

> Con o senza linea di vista: il termine LOS, LineOfSight, indica la visibilità tra le entità radio, cioè se tracciando una retta geometrica passante per i punti di fase delle antenne incontriamo o meno ostacoli. Ovviamente nel caso NLOS la propagazione risulta più complicata e questo spesso si traduce sia in uno svantaggio per Eva, sia in una minore reciprocità tra Alice e Bob.



Esempio in caso LOS Esempio in caso NLOS

In Figura 21 si può notare nel cerchio verde come vi sia un'ottima reciprocità tra Alice e Bob, in quanto i campioni raccolti differiscono di pochi livelli di RSSI tra loro, nonostante le grandi variazioni di ampiezza dovute alle variazioni del canale radio.

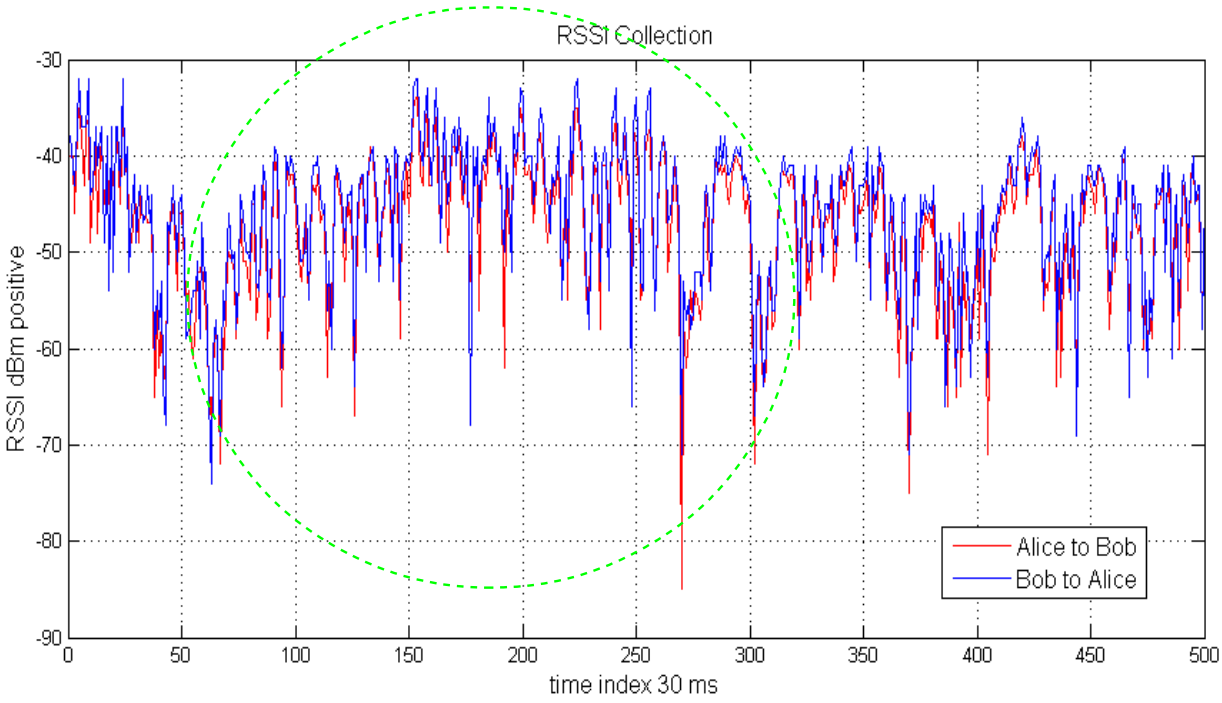


Fig.21 Andamento nel tempo dei campioni RSSI in scenario LOS

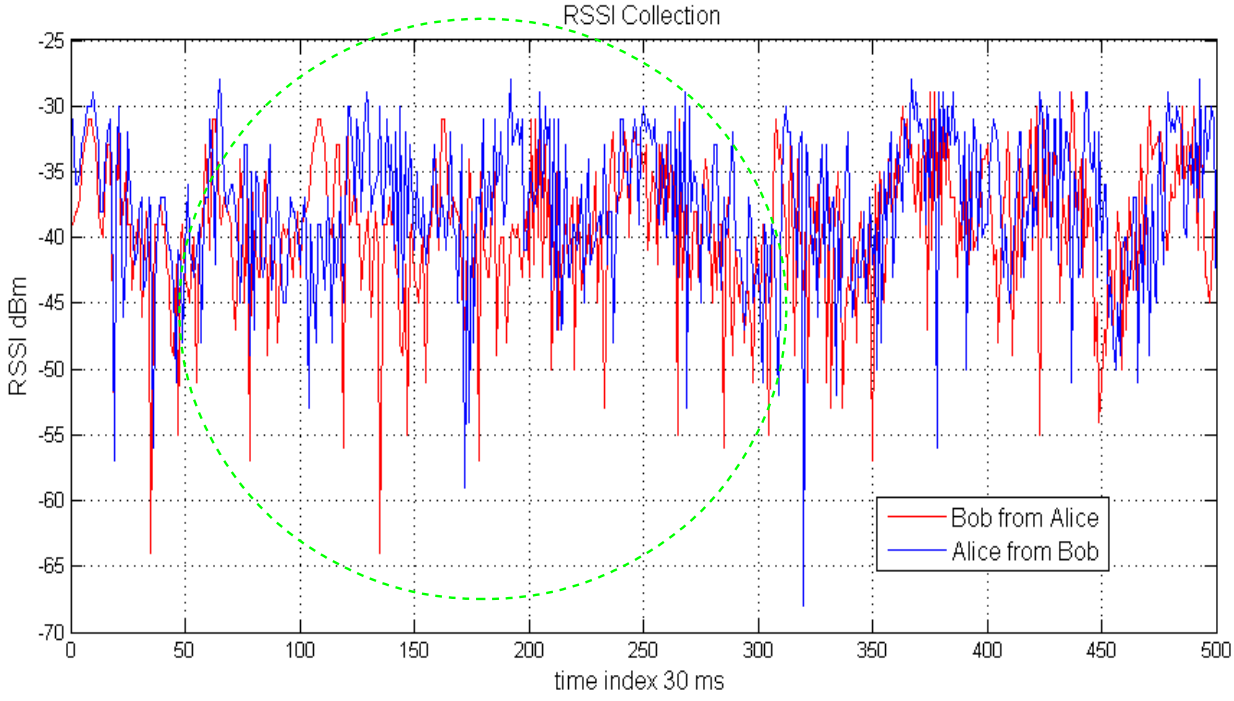


Fig.22 Andamento nel tempo dei campioni RSSI in scenario NLOS

In Figura 22 si può notare nel cerchio verde come vi siano grosse differenze tra i valori registrati da Alice e Bob dovuti alle caratteristiche dell'ambiente NLOS.

> Alice e Bob vicini, Eva lontana: Questa situazione rappresenta il caso migliore perché Eva è svantaggiata dalla distanza di alcuni metri, mentre Alice e Bob comunicano molto vicini.

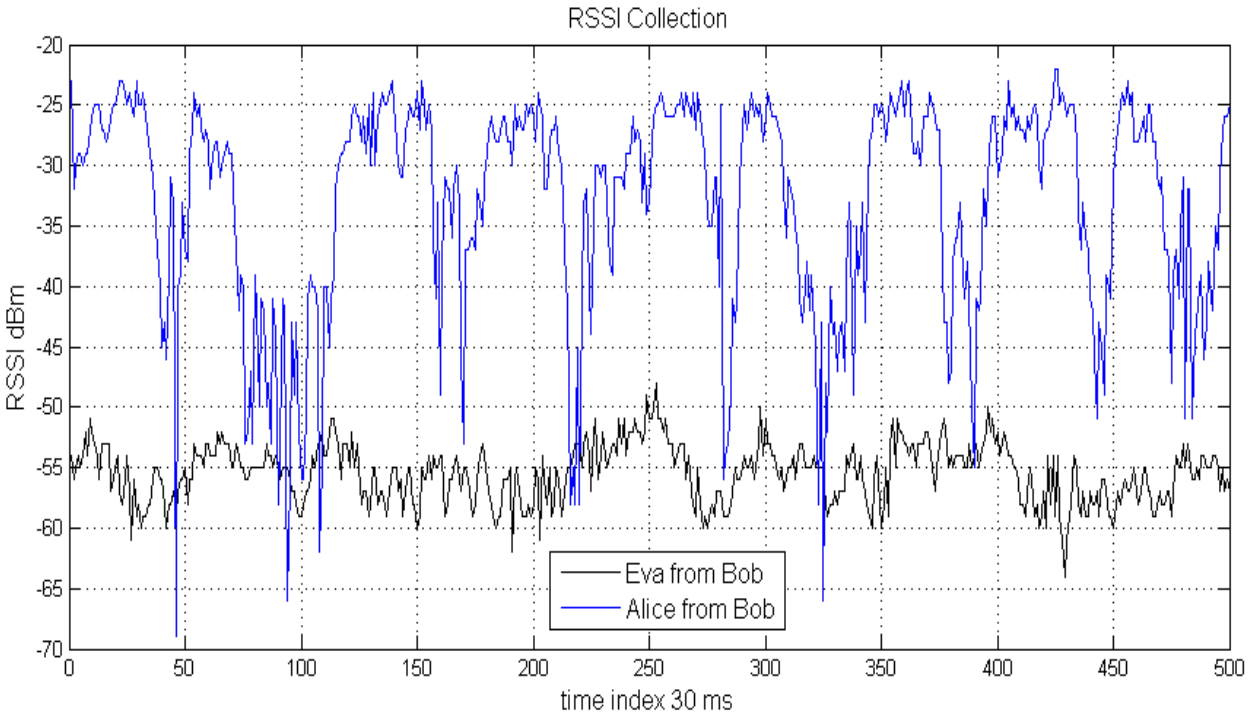


Fig.23 Andamento nel tempo dei campioni RSSI in scenario Alice Bob vicini, Eva lontana. Confronto tra campioni di Alice ed Eva

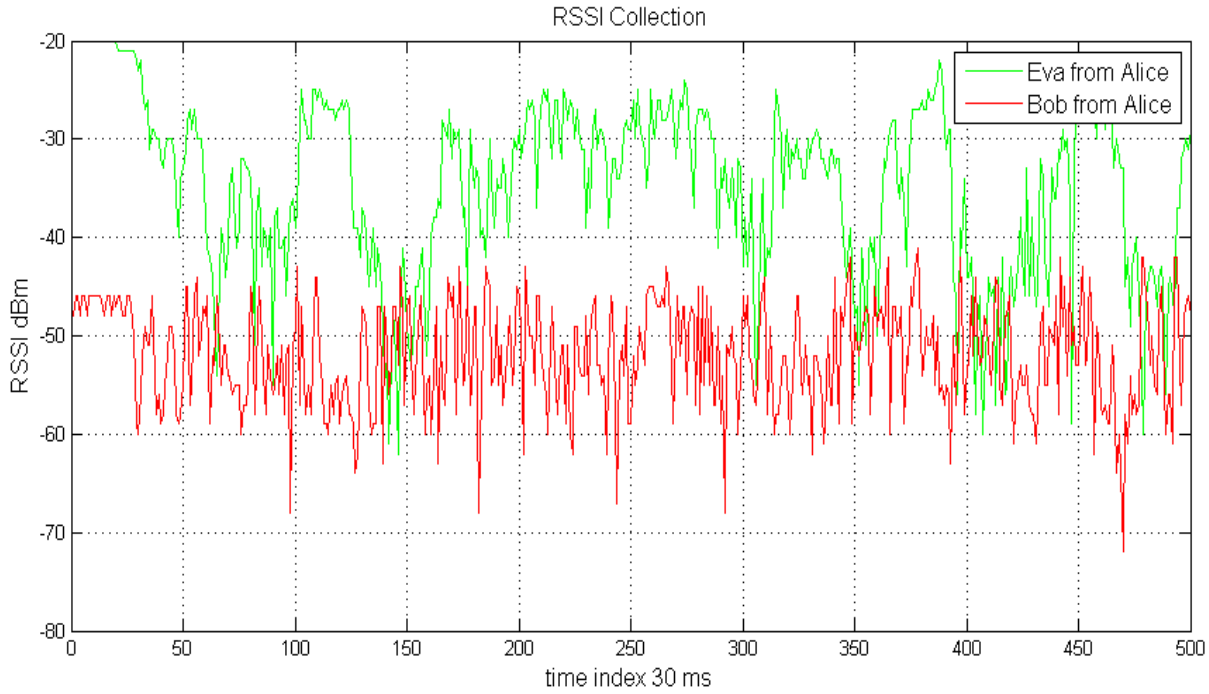


Fig.24 Andamento nel tempo dei campioni RSSI in scenario Alice Bob vicini, Eva lontana. Confronto tra campioni di Bob ed Eva

Nelle figure 23 e 24 si può notare facilmente la totale incorrelazione degli andamenti temporali dei campioni RSSI tra Alice, Bob ed Eva. A prescindere dal valor medio di potenza registrato da Eva, i suoi valori RSSI non seguono mai le oscillazioni, verso l'alto verso il basso, dei campioni di Alice o di Bob.

>Alice ed Eva vicini, Bob lontano: Al contrario questa situazione rappresenta il caso peggiore, perché Eva, trovandosi molto vicino ad Alice, all'interno del cerchio di raggio di circa 6.125 cm, pari alla semilunghezza d'onda della portante attorno ai 2.4Ghz, dovrebbe aver ottime possibilità di captare le stesse informazioni RSSI di Alice. I risultati sperimentali però confermano la totale incapacità di Eva in questo.

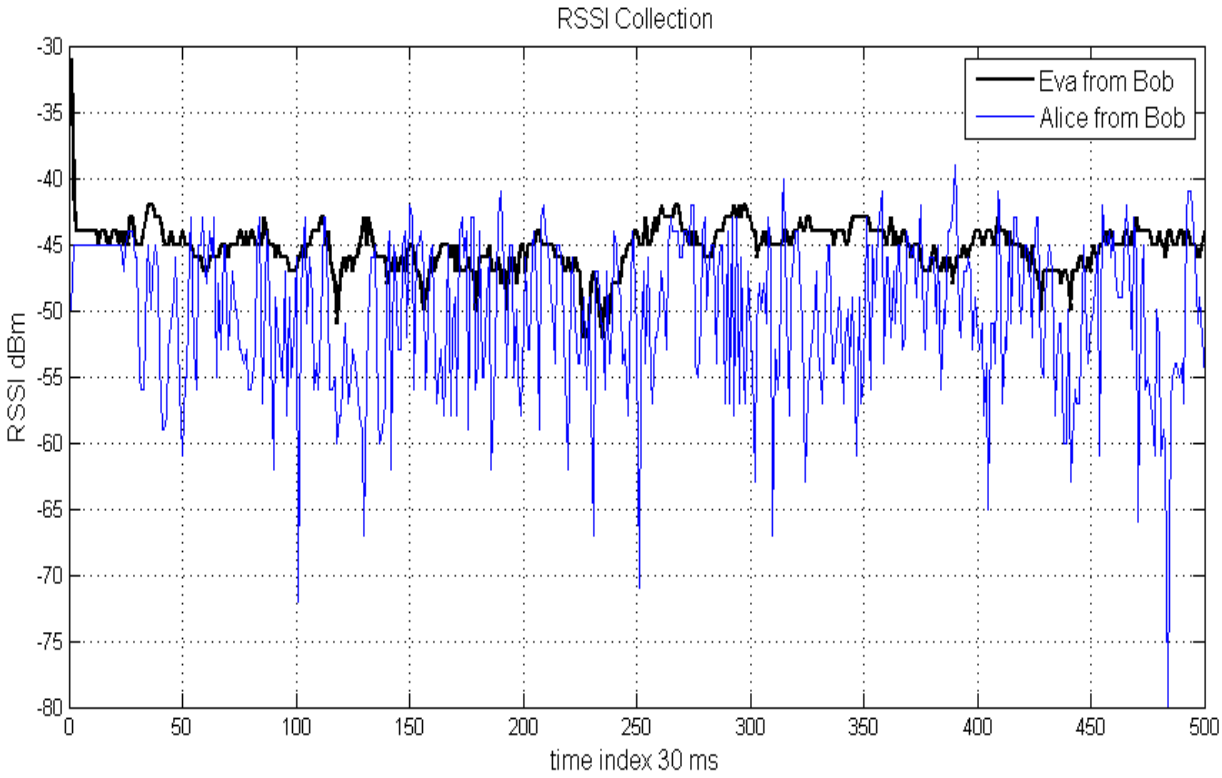


Fig.25 Andamento nel tempo dei campioni RSSI in scenario Alice Eva vicini, Bob lontana. Confronto tra campioni di Alice ed Eva

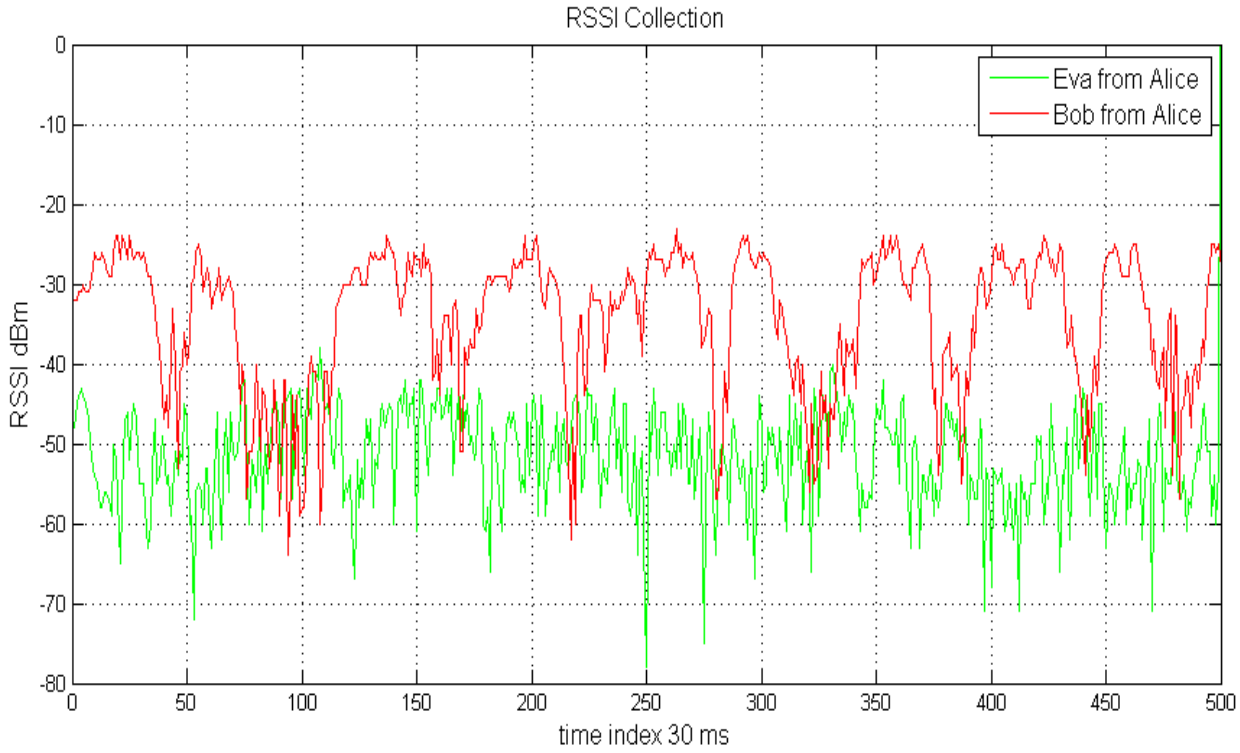
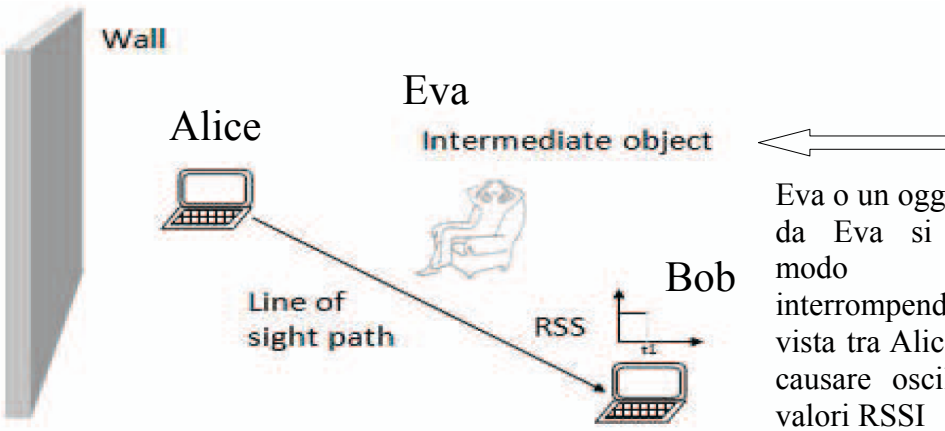


Fig.26 Andamento nel tempo dei campioni RSSI in scenario Alice Eva vicini, Bob lontana. Confronto tra campioni di Bob ed Eva

Nelle figure 25 e 26 si può notare facilmente la totale incorrelazione degli andamenti temporali dei campioni RSSI tra Alice, Bob ed Eva. A prescindere dal valor medio di potenza registrato da Eva, i suoi valori RSSI non seguono mai le oscillazioni, verso l'alto verso il basso, dei campioni di Alice o di Bob, nonostante Eva stessa sia fisicamente posizionata vicino al nodo Alice.

> **Alice e Bob sotto attacco di Eva:** prendendo ispirazione da [3], ho cercato di riprodurre uno scenario in cui Eva si limiti ad introdurre un oggetto in movimento periodico sulla linea di vista tra Alice e Bob in modo da modificare, senza creare interferenze E.M. dirette, l'andamento dei valori RSSI collezionati in modo predicibile.



Eva o un oggetto pilotato da Eva si muove in modo periodico interrompendo la linea di vista tra Alice e Bob per causare oscillazioni nei valori RSSI

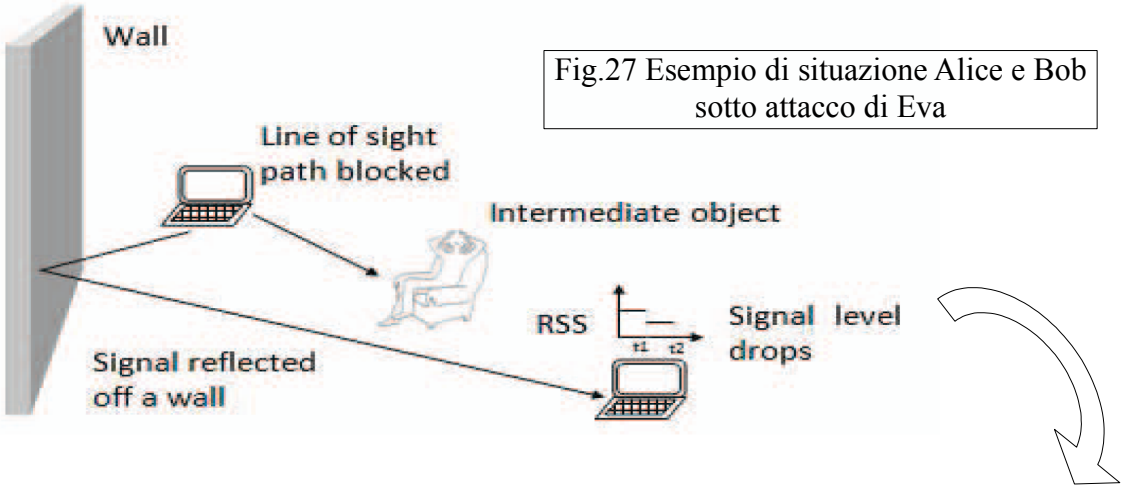


Fig.27 Esempio di situazione Alice e Bob sotto attacco di Eva

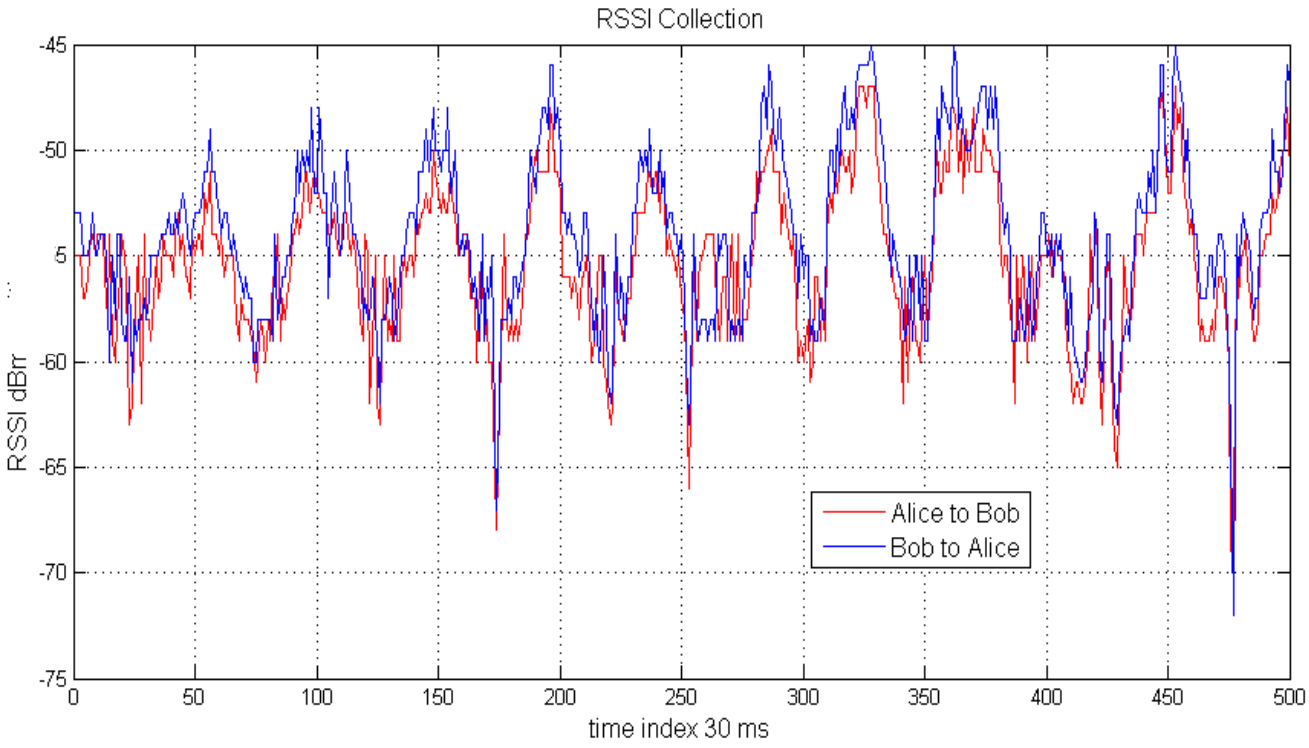
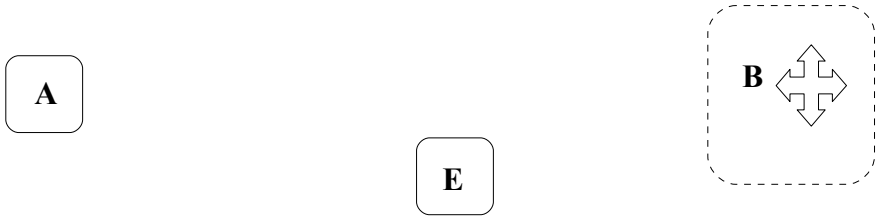


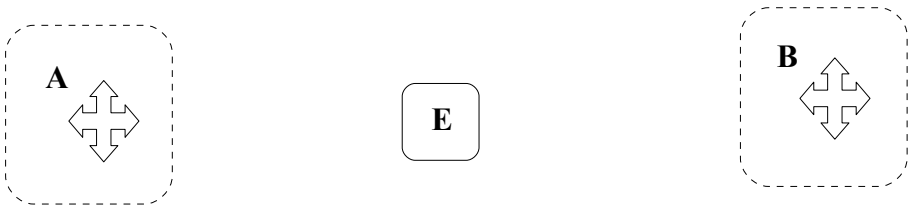
Fig.28 Esempio di oscillazioni temporali dei valori RSSI dovute all'attacco di Eva

> Scenari con misure ripetute: per ottenere dei risultati statisticamente significativi ho iterato per 10 volte lo stesso tipo di misura di tre scenari molto promettenti. Certamente si potrebbero ottenere risultati molto più precisi aumentando il numero di casi ripetuti, in fase di simulazione del sistema.

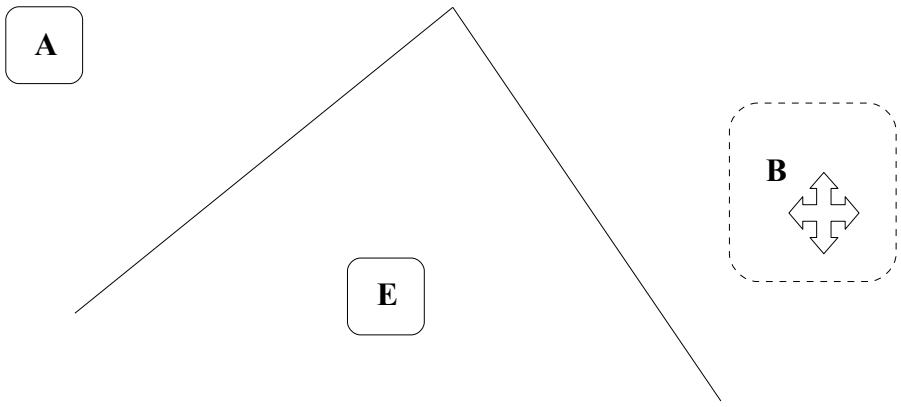
In particolare:
Scenario in cui i nodi si trovano nel raggio di 2-3m in modalità LOS e Bob viene spostato a velocità di camminata, circa 30-40 cm al secondo:



Scenario in cui i nodi si trovano nel raggio di 2-3m in modalità LOS e sia Alice che Bob vengono messi in movimento a velocità di camminata , circa 30-40 cm al secondo:



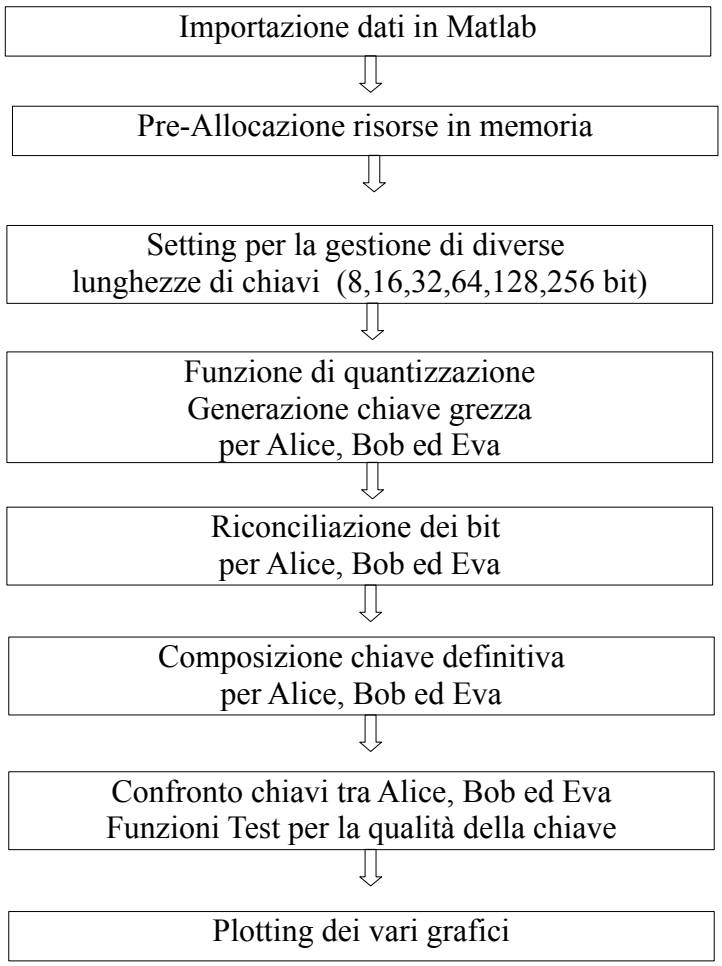
Scenario in cui i nodi si trovano nel raggio di 3-5m in modalità NLOS e Bob viene spostato a velocità di camminata, circa 30-40 cm al secondo:



CAPITOLO 6
ELABORAZIONE DATI IN AMBIENTE MATLAB

Una volta raccolti i quattro vettori (RSSI di Alice, RSSI di Bob, RSSI di Eva from Alice ed RSSI di Eva from Bob) contenenti ognuno 500 campioni RSSI, ho utilizzato per comodità l'ambiente SW Matlab per la restante parte del protocollo, precedentemente descritto. Anche se nel caso più reale possibile sarebbero dovuto essere i nodi Zigbee stessi, a terminare le operazioni necessarie alla generazione della chiave, i risultati non sarebbero cambiati, perché gli unici fattori, positivi o negativi, che influenzano il processo, sono racchiusi nei valori RSSI misurati. Ancora una volta si presuppone che Eva sia a conoscenza dell'intero processo di elaborazione dati e quindi agisca parallelamente a quanto fanno Alice e Bob per la loro sicurezza.

Schema di flusso del programma di analisi delle misure:



Vale la pena citare il tentativo di porre rimedio allo sfasamento temporale tra gli andamenti di campioni RSSI, ad esempio, andando traslare rigidamente indietro di qualche millisec il vettore relativo alle misure di Bob rispetto a quello di Alice. Purtroppo però come evidenziato in precedenza i ritardi non sono uniformi lungo tutta la finestra temporale e quindi sarebbe necessario elaborare una funzione apposita che individui i disallineamenti e li corregga prima della chiamata della funzione di quantizzazione.

L' intervento aggiuntivo che ho dovuto condurre rispetto all'idea di base dei casi [2],[3], è stato quello di eliminare dalla chiave grezza, alcune **lunghe sequenze di bit** adiacenti e tutti uguali tra loro, che venivano estratte a partire dalla quantizzazione di un insieme di campioni RSSI appartenenti ad un unico picco di livello di potenza verso l'altro o il basso. Come mostrato di seguito:

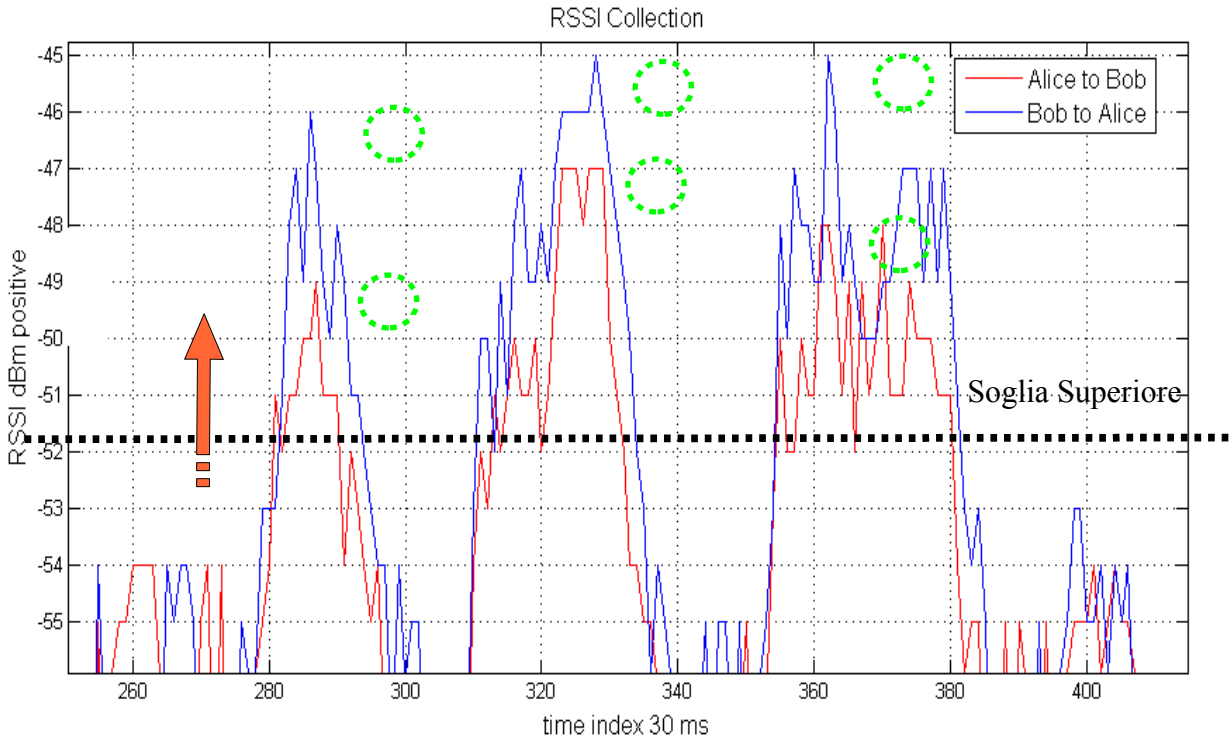


Fig.29 Esempio di esecuzione della funzione di eliminazione di lunghe sequenze di bit

Prima sequenza: 111111 1 1111111

Seconda sequenza: 1111111 1 111111

Terza sequenza: 111111 1 11111111111111

In particolare, il suddetto problema è stato risolto selezionando dalle sequenze di bit uguali, (in questo caso sono tutti '1', ma vale la stessa questione analogamente per i picchi verso il basso con bit a '0'), il singolo bit a cui corrisponde il campione RSSI con maggior valore in dBm, in Figura 29 è marcato in verde. Poiché all'interno dell'esecuzione della funzione di quantizzazione ho diverse iterazioni in cui gradualmente avvicino le soglie di quantizzazione al valor medio temporale, come spiegato nel capitolo 3, i campioni RSSI con valore molto alto,(o molto basso), sono i primi ad essere quantizzati e quindi sono i candidati ottimali per generare bit per la chiave grezza, in quanto rappresentativi dell'intero gruppo del picco. Questo metodo è applicato sia da Alice che da Bob, che da Eva e, come si può notare con i piccoli cerchi verdi in figura, è progetto al meglio per avere più probabilità di concordare la chiave di sicurezza, senza alterarne le caratteristiche di pseudo-casualità.

CAPITOLO 7
RISULTATI

Le seguenti frequenze relative fanno riferimento a scenari tra loro eterogenei, a volte con pochi casi considerati in totale e con una diversa appartenenza temporale. Per questo sono valori indicativi e relativi al lavoro condotto:

Frequenza di concordare una chiave tra Alice e Bob in tutti i casi =	25/100	~25%
Frequenza di attacco da parte di Eva in tutti i casi =	0/100	~0%
Frequenza di concordare una chiave negli scenari statici =	8/50	~16%
Frequenza negli scenari dove Alice e Bob sono sotto attacco=	2/6	~33%
Frequenza negli scenari LOS =	4/25	~16%
Frequenza negli scenari NLOS =	4/26	~15%
Frequenza di concordare una chiave negli scenari in movimento =	18/50	~26%
Frequenza negli scenari dove Alice e Bob sono sotto attacco=	2/4	~50%
Frequenza negli scenari LOS =	12/31	~39%
Frequenza negli scenari NLOS =	6/19	~32%

Le seguenti frequenza relative, invece, sono frutto di un set di 10 misure identiche ripetute in momenti temporali vicini e nello stesso ambiente. Hanno perciò una validità diversa.

Frequenza di concordare una chiave negli scenari con misure ripetute=	10/30	~33%
Frequenza negli scenari della serie 2-3m LOS =	5/10	~50%
Frequenza negli scenari della serie 3-5m NLOS=	2/10	~20%
Frequenza negli scenari della serie 2-3m LOS (in questo caso sia Alice che Bob sono in movimento)=	3/10	~30%

Complessivamente la frequenza media di concordare la chiave di sicurezza è stimata al 20-25%. Nei casi favorevoli come scenari in movimento LOS essa può raggiungere anche il 35%, mentre nei casi sfavorevoli come scenari di tipo NLOS statici al contrario può sfiorare anche il 10%.

Le caratteristiche principali del concetto di generazione di chiavi di sicurezza a livello fisico sono stati raggiunte pienamente e i risultati dell'intero lavoro confermano le grosse potenzialità di questo nuovo approccio. I risultati grafici e numerici ottenuti dall'elaborazione dati della sperimentazione si conciliano molto bene con le aspettative teoriche delineate nei primi capitoli. Uno degli **aspetti più incoraggianti** dei risultati, infatti, è composto, in primo luogo, dal fatto che la reciprocità tra Alice e Bob, nonostante i limiti del Hardware di cui sopra, sia stata rispettata in quasi tutti gli scenari, escludendo in questo contesto l'insieme di scenari statici di poca importanza per i nostri scopi, e in secondo luogo dal fatto che, in nessun caso, Eva sia riuscita a rubare la chiave di Alice e Bob, utilizzando i propri valori RSSI misurati. Questo vale anche in ambienti sfavorevoli, dove Eva ed Alice erano molto vicini a discapito di Bob e quindi, complessivamente, risulta giustificata la validità teorica del processo. Appare, inoltre, molto evidente dal punto di vista visivo, come sia presente la non correlazione tra i canali Eva-Bob o Eva-Alice e il canale Alice-Bob:

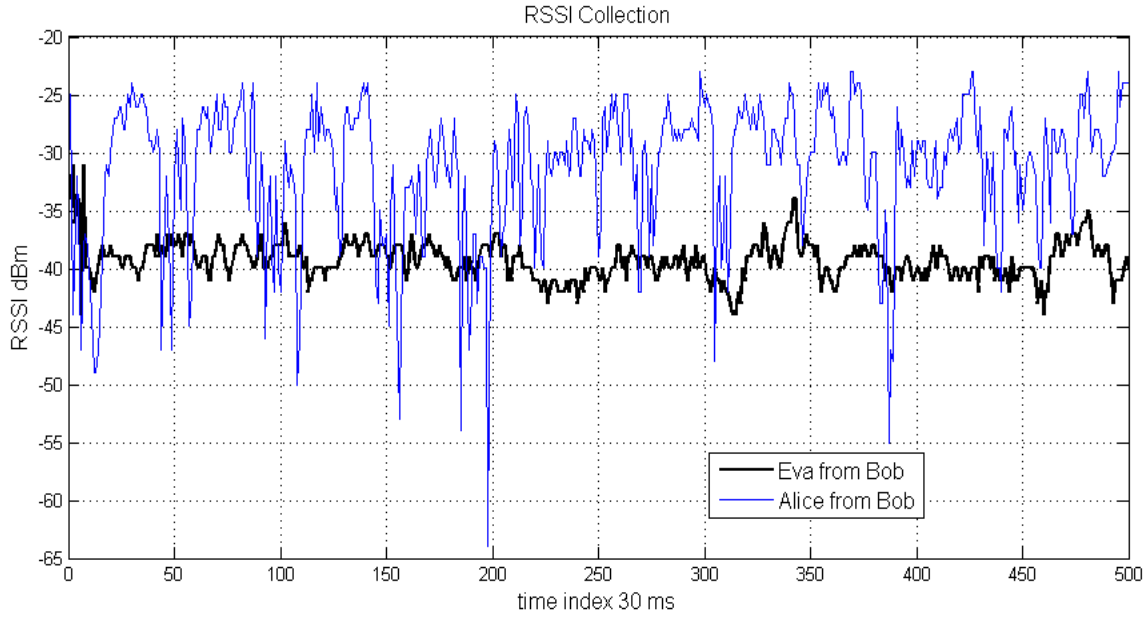


Fig.30 Esempio di incorrelazione temporale dei valori RSSI tra Alice e Eva

Nelle figure 30 e 31 si può notare facilmente la totale incorrelazione degli andamenti temporali dei campioni RSSI tra Alice, Bob ed Eva. A prescindere dal valor medio di potenza registrato da Eva, i suoi valori RSSI non seguono mai le oscillazioni, verso l'alto verso il basso, dei campioni di Alice o di Bob.

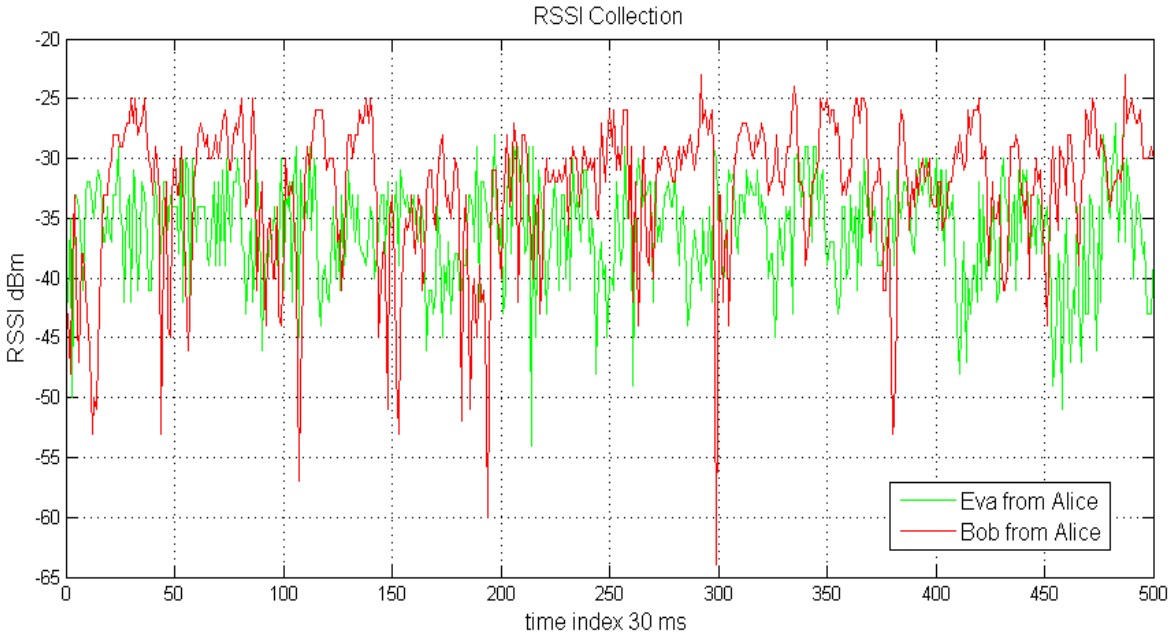


Fig.31 Esempio di incorrelazione temporale dei valori RSSI tra Bob e Eva

Per quanto riguarda la struttura delle chiavi definitive, i risultati finali sono, invece, meno entusiasmanti. Nella quasi totalità dei casi le chiavi concordate tra Alice e Bob sono quelle di minor lunghezza, cioè 8, 16, 32 bit. In aggiunta, nonostante il processo di eliminazione di blocchi di bit contigui all'interno della funzione di quantizzazione, la distribuzione di bit '1' e bit '0' all'interno delle chiavi non è del tutto omogenea, cioè vi compaiono comunque sequenze del tipo '1111111111', '0000000000' relative al susseguirsi di una serie di piccoli picchi di RSSI tra loro vicini.

Un altro importante problema è costituito dalla difficoltà dell'algoritmo nel creare **chiavi lunghe**. Mediamente, anche in assenza di accordo tra Alice e Bob, non è stato possibile estrarre più di 100-150 bit dai campioni RSSI. Le cause più comuni di questa mancanza sono da individuare nei seguenti elementi:

I valori di RSSI sono troppo pochi. Velocizzando lo scambio di pacchetti e collezionando un maggior numero di campioni l'algoritmo di quantizzazione potrebbe scegliere tra un maggior insieme di valori e avere più possibilità di raggiungere la lunghezza prestabilita per la chiave.

I valori RSSI misurati hanno poca dinamica rispetto al loro valor medio e quindi

l'algoritmo di quantizzazione non può ridurre la fascia di estrazione in modo adeguato. Gli scenari migliori in questo contesto sono quelli in movimento con lunghe distanze tra i nodi Zigbee.

Complessivamente quindi otteniamo una serie di chiavi abbastanza corte e non del tutto pseudo-casuali.

Infine non bisogna dimenticare di considerare anche il tempo necessario allo svolgimento di tutto processo di generazione chiavi: trascurando il tempo di elaborazione dati effettuato in Matlab, sicuramente al di sotto dell'ordine di centinaia di millisecondi, e considerati i dettagli, sopra esposti, in merito al protocollo di scambio pacchetti di misura, il procedimento può impiegare persino dai 10 ai 15 secondi per la raccolta di 500 campioni. Appare indiscutibile che sia un intervallo di tempo eccessivamente grande per essere adatto ad una situazione reale.

CAPITOLO 8
CONCLUSIONI

Anche se si può ammettere che i risultati riscontati in questo lavoro non sono del tutto soddisfacenti, per via di una lunga serie di problemi spiegati nei precedenti capitoli, nei diversi lavori in letteratura, dove spesso si fa un largo uso di complicati strumenti matematici per manipolare le misure, l'esito dell'intero processo è di gran lunga molto promettente: la frequenza relativa di successo nel concordare la chiave riesce ad arrivare persino al 90% e la chiave stessa gode di una buona pseudo-casualità, sempre in ambienti simili a quelli utilizzati in questa sede. Vale la pena, quindi, impegnarsi in futuro nel cercare di utilizzare più risorse, sia di calcolo sia di precisione Hardware, ad esempio una maggior accuratezza proprio nel parametro indicatore RSS porterebbe un vantaggio significativo, al fine di innalzare la frequenza relativa di accordo della chiave dal valore di **20% circa** ottenuto in questa esperienza. Parallelamente si potrebbero investigare diverse strategie di elaborazione e raccolta dati: ad esempio sfruttare la selettività in frequenza del canale invece che osservare l'andamento dei valori RSSI nel tempo, oppure passare alla tecnologia Ultra Wide Band, per riuscire così a poter applicare in modo ottimale il procedimento di generazione e scambio chiavi anche a scenari statici o molto complicati. In conclusione la generazione di chiavi di sicurezza a livello fisico, in confronto ai metodi crittografici tradizionali, risulta ideale per le reti wireless poiché permette una facile implementazione, una notevole flessibilità e un'ottima prospettiva di successo.

ELENCO FIGURE

BIBLIOGRAFIA

[1] “Secret Key Generation Exploiting Channel Characteristics in Wireless Communication”
Kui Ren, Hai Su, Qian Wang, Illinois Institute of Tecnology
IEEE Wireless Communication 2011

[2] “High Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements”
N. Patwari, J. Croft, S. Jana, S. K. Kasera
IEEE Transaction on Mobile Computing 2010

[3] “Secret Key Extraction from Wireless Signal Strength in Real Environment”
S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy
IEEE Transaction on Mobile Computing 2012

[4]”The Information”
James Gleick. Fourth Estate.

[5]”Codici e Segreti”
Simon Singh. Saggi BUR.

[6] “The Theory of The Network Society”
M.Castells. Blackwell Publisher.

[7] “Comunicazioni elettriche”,
A.Calandrino, M. Chiani. Pitagora Editrice.

[8] “A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications ”
National Institute of Standards and Technology 2010