Università di Padova

**Facoltà di Ingegneria**

**Corso di Laurea Triennale in Ingegneria Dell'Informazione**

# Sicurezza delle reti di tipo IEEE 802.11

Autore:
Ongaro Nicolò

Relatore:
Lorenzo Vangelista

# Indice

Le reti vengono comunemente oggi utilizzate all'interno degli ambienti più diversi. Con il diffondersi di internet e dei numerosi servizi che questo offre, sempre più, all'interno delle reti, vengono trasmessi dati di natura confidenziale senza la preoccupazione che i mezzi adottati siano del tutto sicuri. In questa tesi si mira a dimostrare che la sicurezza in questo ambito non è un fattore scontato e che molto si è dovuto fare prima di raggiungere un buon livello in questo senso. Verranno prese in analisi le reti wireless basate sullo standard IEEE 802.11 in quanto le più diffuse al giorno d'oggi, se ne vedranno le caratteristiche principali e fino a che punto possono essere considerate sicure.

# 1. Introduzione alle reti wireless

Negli ultimi 8 anni, la mobilità è stata uno dei principali obbiettivi per qualsiasi tipo di tecnologia. I metodi tradizionali di comunicazione, in particolare, si sono rivelati inadeguati nei confronti delle nostre abitudini di tutti i giorni. Se un utente è costretto a collegarsi alla rete tramite dei cavi fisici la sua mobilità ne risulta largamente limitata. La connetività wireless permette di superare queste restrizioni rendendo più flessibili le reti che ne fanno uso.
Spesso cablare un intero edificio, soprattutto se vecchio, può rivelarsi estremamente problematico e in alcuni edifici storici le leggi di preservazione non permetterebbero mai l'installazione di una tradizionale rete LAN su cavo. Un sistema wireless, in questo e in molti altri casi, offre non solo un'estrema praticità ma anche nuove tipologie di soluzioni che spesso risultano essere anche le più praticabili. I costi delle strumentazioni wireless sono diminuiti costantemente negli ultimi anni e spesso ormai il loro impiego costituisce la soluzione migliore anche dal punto di vista economico.
Le reti wireless usano un certo numero di stazioni per connettere gli utenti a una rete. La parte infrastrutturale di una rete wireless rimane qualitativamente la stessa sia che vi sia un solo utente sia che ce ne siano migliaia. Per offrire questo servizio in una data area è necessario solamente un access point e una antenna adeguatamente posizionata. Una volta che la rete è stata configurata correttamente, nuovi utenti si possono collegare e scollegare in qualunque momento in modo del tutto dinamico. Con una semplice e breve procedura di autenticazione chiunque, se autorizzato, può entrare a far parte della rete a tutti gli effetti senza bisogno di ulteriori cavi o dispositivi. Ovviamente a seconda dell'area che è necessario coprire e dal numero di utenti che si vogliono servire l'infrastruttra necessaria dovrà essere adeguatamente progettata e correttamente riscalata per garantire una buona qualità del servizio.
Fra le numerose tecnologie wireless quella basata sullo standard IEEE 802.11 è stata sicuramente quella ad avere il piu grande successo. Lo standard IEEE 802.11 è conosciuto con numerosi nomi, da alcuni è chiamato "wireless Ethernet" per sottolineare la stretta parentela che lo lega allo standard Ethernet (802.3) su cavo mentre dalla maggior parte è conosciuto semplicemente come Wi-Fi (*wireless fidelity*). E' da ricordare tuttavia che questo nome, sebbene il più diffuso, si riferisce in realtà ad un programma di certificazione di qualità proposto dalla WECA (Wireless Ethernet Compatibility Alliance, rinominata in seguito Wi-Fi Alliance) e non allo standard in sé. I produttori di hardware wireless basati sullo standard IEEE 802.11, devono sottoporre quindi i loro prodotti ai test della WECA se vogliono poter essere autorizzati a utilizzare il marchio Wi-Fi.

**Figura 1: Logo del Wi-Fi**

In realtà la tecnologia Ethernet è solo superficialmente simile al IEEE 802.11, su quest'ultimo infatti si sono dovuti fare grandi sforzi e numerosi cambiamenti per adattare e integrare il wireless con l'Ethernet stesso. All'hardware IEEE 802.11 è assegnato un indirizzo MAC a 48 bit e da questo la rete, in realtà, non è capace di distingue una comune interfaccia Ethernet da un'interfaccia wireless in quanto, effettivamente, per ogni uso pratico fare una simile distinzione non è necessaria. L'assegnamento dell'indirizzo MAC, infatti, viene fatto per l'IEEE 802.11 dallo stesso pool di indirizzi che viene assegnato anche all'hardware Ethernet così che in una rete dove ci siano

contemporaneamente interfacce wireless e su cavo non ci siano mai due utenti indistinguibili. Come in tutte le reti IEEE 802, l'indirizzo MAC è fissato per ogni diversa macchina e nella tabella ARP di ogni nodo compaiono senza distinzione le assegnazioni dell'indirizzo IP per l'una e per l'altra tipologia di interfaccia.

# 2. Lo standard IEEE 802.11

## 2.1 La famiglia IEEE 802

In realtà la stretta relazione che intercorre fra l'802.11 e l'Ethernet si riscontra in tutta la famiglia IEEE 802 che comprende una serie di specifiche e protocolli appositamente studiati per le tecnologie LAN (*local area network*). Gli standard IEEE 802 si riferiscono alla gestione degli ultimi due livelli del modello OSI: il physical layer e il data link layer. Il data link layer, o più precisamente la sua componente MAC (*medium access control*), si occupa di definire un set di regole per l'accesso condiviso degli utenti alla rete, mentre i dettagli sull'effettivo invio e ricezione dei dati è lasciato al physical layer. Caratteristiche specifiche di ogni implementazione del IEEE 802 sono indicate da un secondo numero di catalogazione. Per esempio le specifiche 802.3 si riferiscono a una rete CSMA/CD indicata spesso con il nome di Ethernet, mentre lo standard 802.5 si occupa di reti di tipo token ring.
Ciò che rende diverso l'IEEE 802.11 rispetto a tutte le altre implementazioni delle stessa famiglia è innanzi tutto il physical layer (PHY), la cui gestione appare piuttosto complessa se paragonata a tutte le altre dell' IEEE 802. L'utilizzo di onde radio come mezzo fisico, infatti, non poteva che appesantire la componente PHY, che nell'802.11 è divisa in due generici settori o *sublayers*: il PLCP *(Physical Layer Convergence Procedure*) e il PMD (*Physical Medium Dependent*). Il primo ha il compito di interagire direttamente con il layer MAC soprastante e mappa i dati da questo generati (detti *MAC protocol data unit*, o MPDU) in frame che possano essere adeguatamente inoltrati attraverso il mezzo. Il PMD si occupa infine di tradurre i dati in segnale svolgendo le operazioni di modulazione e demodulazione.
Infine all'interno dello standard IEEE 802.11 si possono fare ulteriori distinzioni. I prodotti basati su questa tecnologia furono realizzati inizialmente nel 1997. Il primo standard 802.11 prevedeva, oltre alla tipica interfaccia RF, anche una seconda basata sugli infrarossi (IR) che però non fu mai realmente impiegata. Poteva inoltre usare due diverse tecnologie di propagazione del segnale denominate *frequency hopping* (FH) e *direct sequence* (DS), entrambe molto semplici e capaci di garantire velocità non superiori ai 2 Mbps. Nel 1999, il team che si occupava dell'IEEE 802.11 riuscì a realizzare delle interfacce radio più veloci e a concludere nello stesso anno le operazioni per la pubblicazione di due nuovi standard: l'802.11a e l'802.11b. L'802.11a utilizza una terza e nuova tecnologia di modulazione del segnale chiamata *orthogonal frequency division multiplexing* (OFDM) e nonostante potesse raggiungere velocità paragonabili a quelle delle reti Ethernet più veloci, non ebbe mai il successo che venne dato invece all’802.11b e tutt'oggi è impiegato principalmente negli Stati Uniti. L’802.11b invece, anche se più lento, ebbe molto più successo e fu all’epoca subito visto come lo standard definitivo vista la sua enorme e veloce diffusione.
Nella seguente tabella sono elencate le principali versioni dello standard 802.11 e le loro caratteristiche peculiari.

| **Standard IEEE** | **Velocità** | **Frequenza** | **Dettagli** |
|---|---|---|---|
| 802.11 | 1-2 Mbps | 2.4 GHz | Il primo standard (1997). Supportava due diverse tecnologie di modulazione FH e DS. |

| | | | |
|---|---|---|---|
| 802.11a | Fino a 54 Mbps | 5 GHz | Secondo standard (1999), utilizzato ufficialmente solo a partire dal 2000. Implementa la tecnologia OFDM. Le frequenze di cui fa uso sono tuttora riservate in alcuni paesi. |
| 802.11b | 5.5-11 Mbps | 2.4 GHz | Sviluppato contemporaneamente all'802.11a (1999). Ha riscosso molto successo dovuto al drastico incremento del throughput che ha saputo apportare e al relativo basso costo del hardware di cui fa uso. |
| 802.11g | Fino a 54 Mbps | 2.4 GHz | Standard ufficializzato nel 2003. E' completamente compatibile con l'802.11b a patto di limitarne la velocità che, normalmente, risulta essere superiore a quella di quest'ultimo. Il suo successo è dovuto in parte alla Apple che per prima ha voluto pubblicizzarlo e utilizzarlo per il suo hardware. |
| 802.11i | Fino a 54 Mbps | 2.4 GHz | Creato allo scopo di risolvere i problemi di sicurezza dai quali le precedenti reti erano afflitte. Molti dei protocolli di sicurezza che qui sono stati introdotti sono oggi diventati di comune uso. |
| 802.11n | Fino a 150 Mbps per ogni singolo stream | 2.4 e 5 GHz | Standard risalente al 2009. Sviluppato per permettere la realizzazione di reti wireless capaci di coprire intere città. Supporta l'utilizzo di antenne multiple (multiple-input multiple-output, o MIMO) e quindi la gestione contemporanea di più flussi (stream) permettendo così di raggiungere velocità di trasmissione molto elevate. |

## 2.2 Il sistema wireless


**Figura 2: Esempio di rete 802.11**

Una tipica rete IEEE 802.11 può essere strutturata, come vedremo, in diversi modi. In ogni rete tuttavia le componenti principali che si possono distinguere sono quattro:

- Stazioni:

Le reti vengono costruite per permettere innanzitutto lo scambio di dati fra le stazioni. Le stazioni sono nodi terminali con capacità computazionale e dotati di interfacce wireless. Tipicamente si tratta di computer portatili, cellulari e palmari, tuttavia nulla vieta di collegare anche le stazioni non mobili come computer desktop alla rete wireless. Anche se quest'ultime, in genere, non hanno nessun vantaggio ad avere un collegamento wireless, spesso si rivela meno costoso dotare questi terminali di interfaccia Wi-Fi piuttosto che farli raggiungere da un cavo.

- Access points (AP):

I dati (o frames) in una rete 802.11 devono essere prima elaborati adeguatamente prima che possano essere inviati al resto del mondo. La funzione più importante gestita da un access point è proprio quella di ricevere i dati wireless e svolgere l'operazione detta *wireless-to-wired bridging* che rende trasparente al sistema di distribuzione su cavo il momentaneo passaggio dei dati attraverso il mezzo wireless.

- Sistema di distribuzione:

Quando più access point sono connessi fra loro a coprire una vasta area, è necessario garantire loro la possibilità di scambiarsi dei dati. Il sistema di distribuzione (*distribution system*) è la componente logica del IEEE 802.11 usata proprio per permettere la comunicazione fra gli access point che in

questo modo possono sia scambiarsi fra loro utili informazioni di servizio relative agli utenti, che inoltrare correttamente i dati fra due stazioni che non sono raggiungibili da uno stesso AP. Lo standard non specifica nessuna tecnologia in particolare per il sistema di distribuzione. Nella maggior parte dei prodotti commerciali, questo sistema è implementato tramite una rete di supporto (o *backbone network*) che permette il bridging fra i vari access point che così possono comunicare fra loro. Per la backbone network è in genere comunemente impiegato l'Ethernet.

- Mezzo di trasmissione:

I dati che vengono trasmessi fra una stazione e un access point viaggiano attreaverso un mezzo wireless. A supporto delle reti IEEE 802.11 sono stati sviluppati e standardizzati diversi sistemi di trasmissione wireless, sia a infrarosso che a radio frequenze. Queste ultime si sono dimostrate le più versatili e sono oggi quelle di gran lunga più utilizzate.

## 2.3 Tipologie di rete

In una rete IEEE 802.11 l'insieme dei nodi capaci di comunicare fra loro è detto *basic service set* (BSS). La comunicazione avviene entro un'area dai confini non ben definiti chiamata *basic service area* (BSA) la cui estensione è funzione delle caratteristiche di propagazione del mezzo e dalla potenza impiegata dai nodi. Quando una stazione si trova all'interno della BSA può comunicare con le altre all'interno della stessa e può essere considerato a tutti gli effetti parte della rete.

### 2.3.1 BSS indipendente

Ci sono diverse tipologie di configurazioni possibili per una rete, la più semplice è sicuramente quella costutita da una rete indipendente o indipendent BSS (IBSS). Le stazioni in una rete indipendente comunicano direttamente fra loro e devono quindi rientrare nella stessa area di servizio. La più piccola rete IEEE 802.11 è una IBSS comprendente solamente due stazioni. Tipicamente questo tipo di reti viene insatallato sempre fra un numero ristretto di stazioni e solo per brevi periodi di tempo, come soluzione temporanea. Un tipico utilizzo è quello di sfruttare, magari durante una conferenza, una rete di questo tipo per condividere dei dati con i presenti che si trovano tutti all'interno di una stessa stanza. Alla fine della conferenza la rete viene disciolta. Dato il suo utilizzo e la sua praticità spesso questo tipo di rete viene chiamato BSS ad hoc o più semplicemente "rete ad hoc".

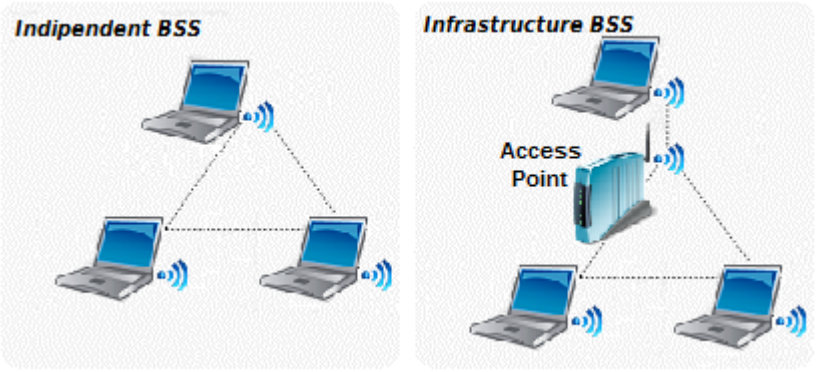



**Figura 3: IBSS e BSS indipendente**

### 2.3.2 BSS a infrastruttura

Quando la rete è supportata dall'utilizzo di un access point si parla invece di rete a infrastruttura (infrastructure BSS). Tutti i dati inviati all'interno della rete, compresi quelli scambiati fra due stazioni nella stessa area di servizio, devono in questo caso passare attraverso l'access point. Se una stazione mobile all'interno di una rete a infrastruttura deve comunicare con una seconda stazione, i dati sono quindi costretti a fare due "salti" (hop), ovvero a passare attraverso un terzo nodo. Una stazione che ha bisogno di comunicare si rivolge così sempre all'access point e sarà poi questo a inoltrare i dati correttamente al destinatario. Delegando interamete la consegna dei frames all'access point si può, per una rete ad infrastruttura, ridefinire l'area di servizio come l'insieme dei punti nei quali e possibile comunicare direttamente con l'access point. A prima vista potrebbe sembrare un sistema piuttosto inefficiente poichè effetivamente si utilizzano più risorse del necessario e i dati inviati risentono di un maggiore ritardo, tuttavia ci sono dei vantaggi molto significativi. Il primo vantaggio è che dal momento in cui la comunicazione con un access point è garantita non ci sono più restrizioni sulla distanza fra una stazione e l'altra, la comunicazione avviene solo con l'access

point e non c'è bisogno di tener traccia di tutte le altre stazioni nell'area, cosa che per un cellulare, ad esempio, potrebbe essere piuttosto gravoso. Inoltre gli access point sono costantemente collegati all'alimentazione, cosa che non si può dire per le stazioni, che essendo in genere mobili, funzionano spesso grazie a una batteria. Alcune interfacce wireless sfruttano ciò per poter adottare strategie di risparmio energetico che permettono loro, se opportuno, di spegnersi automaticamente dopo aver inviato i dati. Gli access point riconoscono quando una stazione si trova in risparmio energetico e memorizzano all'interno di un buffer i dati destinati a queste stazioni, in attesa che si riattivino. In questo modo le stazioni sono libere di spegnersi per risparmiare energia e riattivarsi solamente quando c'è una buona probabilità che nel buffer dell'access point ci sia qualcosa da ricevere.
In una rete a infrastruttura, le stazioni devono rivolgersi agli access point anche per ottenere il permesso ad accedere al servizio. Il processo con il quale una stazione entra a far parte di una rete IEEE 802.11 è detto processo di associazione ed equivale dal punto di vista logico a collegare fisicamente il cavo di rete di una Ethernet, una stazione può associarsi sempre con un solo access point. Da parte loro gli access point possono ovviamente consentire o negare l'accesso alla rete basandosi esclusivamente sul contenuto della richiesta di associazione. Lo standard IEEE 802.11 non definisce nessun limite a quante stazioni un access point può servire, tuttavia ogni implementazione possiede ovviamente un tetto massimo sopra il quale la qualità del servizio inizia a deteriorarsi. Nella pratica le trasmissioni wireless presentano una forte ridondanza nei dati che vengono inviati per far fronte all'alta probabilità di errori nella ricezione del segnale radio, cosa che si traduce, in termini tecnici, in un throughput relativamente basso, motivo per il quale si tende in genere piuttosto a limitare il numero di stazioni su una rete Wi-Fi.

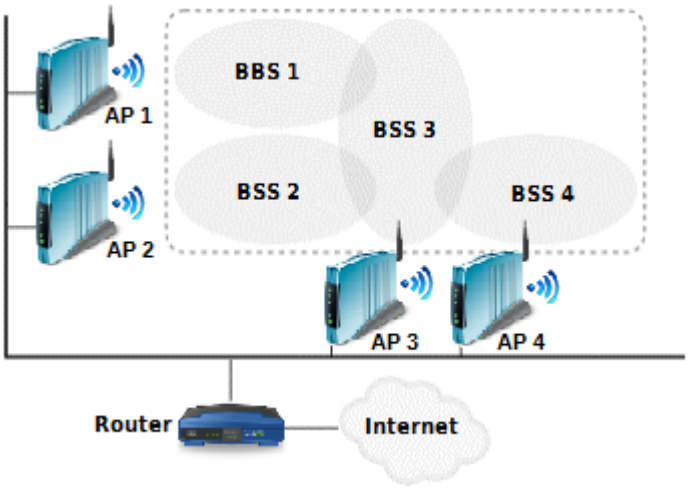



**Figura 4: Extended Service Set (ESS)**

### 2.3.3 Extended Service Set

Una BSS può coprire un intera casa o ufficio, ma non di certo aree più vaste. Lo standard stesso prevede reti di di grandezza arbitraria create collegando fra loro, grazie a un'adeguata backbone network, più BSS a formare una extended service set (ESS). L'area di copertura è l'unione di quelle fornite dalle singole BSS, tenendo presente però che, per garantire continuità di servizio a una stazione in movimento, è necessario che queste abbiano adeguate intersezioni (Figura 4). Ovviamente gli access point, grazie alla possibilità di comunicare fra loro, possono eseguire l'operazione di bridging fra le varie BSS permettendo lo scambio di dati fra le varie stazioni all'interno dell'intera ESS. Questo tipo di rete è la più completa e generica implementazione supportata dalla documentazione ufficiale dello standard IEEE 802.11. La presenza di un router collegato alla backbone network permette di usare un singolo indirizzo MAC per inoltrare e ricevere dati da e verso l'esterno della rete qualora le stazioni lo richiedessero. Il router non è a conoscenza della posizione delle varie stazioni ne dalla loro esistenza, si affida solamente agli access point per svolgere la sua funzione.

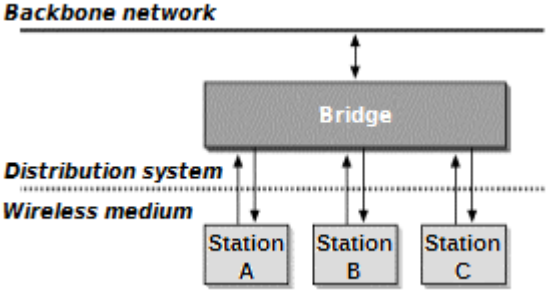



**Figura 5 : Il wireless-to-wired bridging**

Quando un frame giunge al sistema di distribuzione questo viene inoltrato, a seconda dei casi, verso l'esterno della rete oppure, se il destinatario è una stazione raggiungibile localmente, verso l'access point relativo alla BSS in questo si trova. In quest'ultimo caso l'AP si occuperà del passaggio finale del dato verso tale stazione mobile. La capacità di scegliere il corretto access point a cui inoltrare i singoli frames è da imputare agli AP stessi, questi infatti tengono

traccia della BSS a cui appartiene ogni stazione all'interno della ESS e condividono tali informazioni fra loro. La maggior parte degli access point attualmente in commercio possiedono almeno un interfaccia wireless ed una Ethernet. Tramite la porta Ethernet è possibile collegare l'AP ad una rete preesistente, mentre la parte wireless può essere vista come un estensione di questa rete. E' sotto questo punto di vista che si può dire che un access point svolge semplicemente un operazione di bridging fra due reti. Va infine detto che i più moderni AP sono oggi capaci di attuare un bridge wireless, ovvero di utilizzare la stessa interfaccia Wi-Fi per comunicare sia con le stazioni che con gli altri AP, cosa che nello standard IEEE 802.11 viene effettivamente proposta come possibile soluzione. In questo caso la distinzione di una backbone network è da considerarsi solo di tipo logico.

# 3. Il MAC IEEE 802.11

## 3.1 Controllo dell'accesso al mezzo

La parte chiave dello standard IEEE 802.11 è il MAC, ovvero la gestione e il controllo delle trasmissioni radio. Proprio come l'Ethernet l'IEEE 802.11 utilizza il sistema CSMA (*carrier sense multiple access*) per il controllo dell'accesso al mezzo, non è presente dunque un controller centralizzato e di conseguenza ogni stazione decide da se quando trasmette e quando non farlo. Le principali differenze rispetto agli altri standard IEEE 802 che vedremo derivano tutte dal particolare mezzo di trasmissione utilizzato.

### 3.1.1 Difficoltà di implementazione

Le onde radio risultano essere molto più inaffidabili rispetto al cavo. Nonostante si sia cercato di utilizzare una banda ristretta rimangono comunque numerosi i fattori per nulla trascurabili di rumore e di interferenza, dovuti anche al fatto che le frequenze utilizzate fanno parte di bande libere e senza licenza (bande ISM) utilizzate anche da molti altri apparecchi wireless molto comuni. Inoltre bisogna tener conto che una rete wireless è facilmente soggetta a veloci mutazioni: una stazione che ad un tratto si sposta in un'area irragiungibile, causa l'improvvisa sparizione di un nodo e dunque ulteriori possibili problemi di trasmissione. Per questi motivi su reti wireless, a differenza dell'Ethernet che utilizza il collision detection (CSMA/CD), si preferisce, per irrobustire il sistema, usare il "*collision avoidance*" (CSMA/CA), nonché un sistema di acknowledgment che prevede che la ricezione di ciascun frame debba essere confermata dal destinatario con un apposito segnale (ACK). La sequenza di trasmissione frame-ACK è cosiderata in questo caso atomica, ovvero costituisce la più piccola operazione elementare che si posssa avere su una rete.

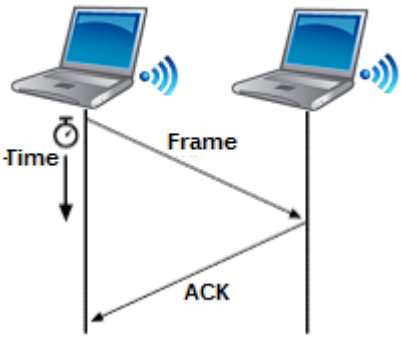


**Figura 6: Operazione atomica Frame-ACK**

Come vedremo, il protocollo CSMA (*Carrier Sense Multiple Access*) utilizzato dall'IEEE 802.11 viene in genere implementato in modo diverso da come si fa su reti Ethernet in quanto, se così non fosse, insorgerebbe il famoso problema del "nodo nascosto". Il sistema CSMA classico è stato creato per collegamenti via cavo e si basa sulla capacità dei nodi di capire in ciascun istante se il mezzo è libero o meno e di conseguenza se è possibile servirsene o se bisogna attendere. Questo presuppone che ciascun nodo sia capace di intercettare il segnale inviato da ciascun altro

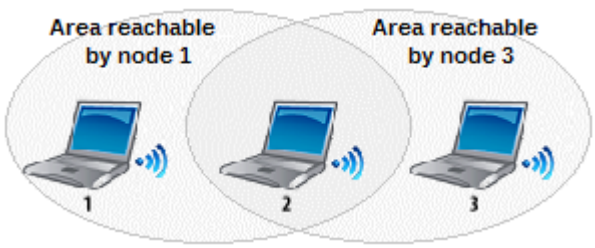


**Figura 7: Il problema del "nodo nascosto"**

nodo, cosa che purtroppo non è sempre vera nelle reti wireless. L'accessibilità è garanatita dalla raggiungibilità dell'access point e non delle altre stazioni, perciò, in [Figura 7], possiamo presupporre tutte e tre le stazioni all'interno della stassa rete. Tuttavia, in realtà, il nodo 1, pur essendo in grado di "sentire" il 2, non è capace di raggiungere il nodo 3 e stessa cosa vale per il nodo 3 stesso, relativamente ai nodi 1 e 2. Ciò significa che sia il nodo 1 che il 3 non trasmetteranno quando il canale verrà utilizzato dal nodo 2 poichè ne sarebbero consci e attenderebbero per evitare una sicura collisione, tuttavia non avranno alcuna possibilità di evitare una possibile collisione fra loro stessi. Si dice che dal punto di vista del nodo 1 il 3 è un nodo nascosto (*hidden node*) e viceversa. Per risolvere questo problema in realtà esiste una soluzione suggerita dallo stesso standard 802.11, ovvero quella di usare altri due segnali di controllo detti *request to send* (RTS) e *clear to send* (CTS). In [Figura 8] è raffiguarata una rete che utilizza questo metodo. Il nodo 1, dovendo comunicare con il 2, invia innanzitutto un frame RTS per avvisare che, a breve, sarà suo intento trasmettere. Questo segnale non solo richiama l'attenzione del destinatario ma avvisa anche tutti gli altri nodi raggiungibili dal nodo 1 che il mezzo sarà momentaneamente occupato. Il nodo 2 ricevendo il segnale RTS risponde con un frame CTS per dire di aver colto la richiesta e di essere pronto allo scambio di dati. Quest'ultimo segnale, come quello RTS, blocca infine tutti i nodi raggiungibili dal nodo 2 con il risultato finale che ogni trasmissione che mai avrebbe potuto interferire con l'invio dei dati è stata sicuramente annullata. Lo scambio procede quindi normalmente con l'invio del frame dati e il successivo ACK. Questo metodo seppur efficace aggiunge ulteriore latenza ed è utilizzato solamente in reti con grande capacità oppure solo nello scambio di frame particolarmente grandi.

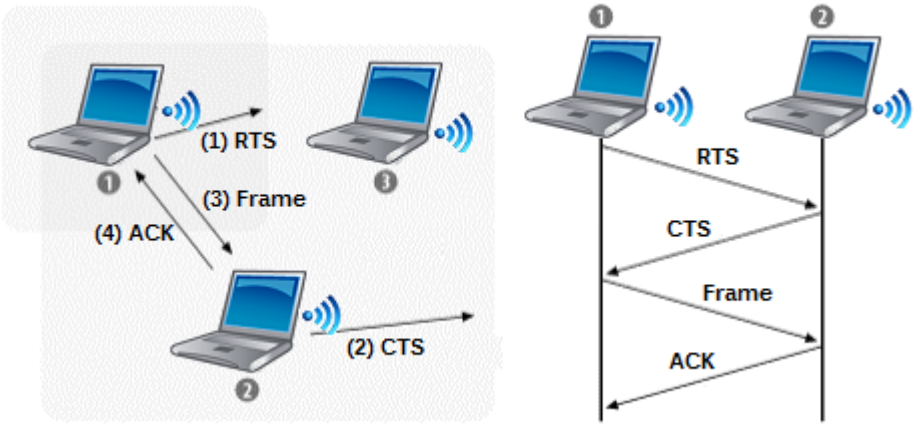


**Figura 8: Utilizzo dei segnali RTS e CTS**

### 3.1.2 CSMA

Ci sono due funzioni che compaiono nella documentazione dello standard IEEE 802.11 in grado di percepire se il canale è occupato: il *physical carrier sensing* e il *virtual carrier sensing*. La prima cerca effettivamente di intercettare sul mezzo il segnale provenienete dall'eventuale nodo che sta occuapando il canale. Tuttavia, come abbiamo visto, questa soffre del problema del nodo nascosto, senza contare che la sua implementazione su ricevitori che, in genere, non sono in grado di trasmettere e ricevere contemporaneamente risulta complicato. Nelle applicazioni reali è preferibile invece l'uso del *virtual carrier sensing* che prevede l'aggiunta, all'interno dei frame stessi, di un campo detto *network allocation vector* (NAV) che permette a un nodo qualsiasi di riservare il canale per un periodo di tempo fissato. Una stazione che deve trasmettere può settare il NAV al tempo per il quale si aspetta di utilizzare il mezzo, comprendendo ogni segnale di controllo necessario a concludere l'operazione. Gli altri nodi ricevono questo valore all'interno dei classici frame e sanno così quanto devono aspettare prima di poter trasmettere nuovamente. Quando il NAV assume il valore 0 indica che il canale è libero.
In [Figura 9] è mostrato come si può utilizzare il NAV per impedire l'interruzione della trasmissione di un frame. Il valore NAV in questo esempio viene inviato all'interno dei frame di RTS e CTS. All'inizio, il nodo che vuole comunicare riserva il canale per tutto il tempo necessario stimato per riuscire a inviare il frame ed averne la conferma di corretta ricezione tramite il segnale di ACK. Il nodo interessato fa poi la stessa cosa tramite il segnale CTS, idealmente settando il NAV allo stesso punto del suo interlocutore. A questo punto, ancora una volta, tutti i nodi raggiungibili sia da l'uno

che dall'altro nodo fra i quali avviene la comunicazione sono stati avvertiti che il canale è occupato per un dato periodo di tempo nel quale non sarà quindi più necessario svolgere l'operazione di carrier sensing. Ogni nodo tiene il conteggio del tempo e, quando questo arriva a 0, possono iniziare nuovamente a contendersi il canale.
Nel diagramma temporale di [Figura 9] compaiono anche gli spazi interframe SIFS (*short interframe space*) e DIFS (*DCF interframe space*). Quando un nodo avverte il canale occupato, secondo le specifiche CSMA, questo deve attendere un certo periodo di tempo (detto di backoff) prima di poter provare a trasmettere nuovamente. Questo lasso di tempo varia dal SIFS, più breve, al DIFS, più lungo. Questa differenza è utile per creare due diversi livelli di priorità: i frame con priorità maggiore, in genere quelli con funzione di controllo (come RTS, CTS e ACK nel esempio precedente), per essere trasmessi dovranno, dopo che il canale si è liberato, attendere solo un breve

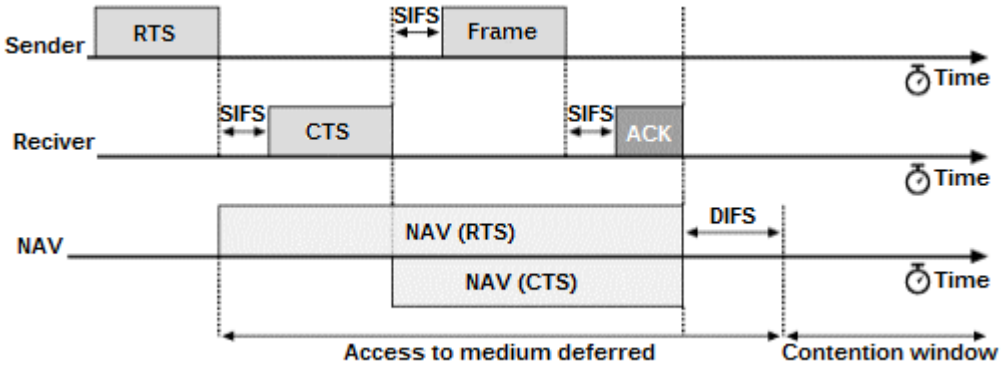



**Figura 9: Diagramma temporale di un possibile utilizzo del NAV**

periodo di tempo (pari al SIFS) avendo così la possibilità di potersi riservare il canale in anticipo rispetto alle altre trasmissioni secondarie in attesa, che invece devono aspettare un tempo maggiore (pari al DIFS). Esiste infine anche l'EIFS (*extended interframe space*), riservato alle ritrasmissioni di frame la cui consegna già una volta non è andata a buon fine, questo intervallo di tempo varia a seconda della priorità che si vuole dare a queste operazioni.

## 3.2 Il frame MAC

Ogni livello del modello OSI utilizza una sua specifica terminologia, così come al network layer il singolo elemento di dato viene in genere, per tipiche reti TCP/IP, chiamato "pacchetto" (*packet*) a livello MAC si utilizza il termine "frammento" (*frame*). E' da tener presente però che i due termini non sono sinonimi in quanto in realtà il frame consiste dell'intero pacchetto IP o di una sua parte (nel caso in cui fosse stato necessario frammentarlo) al quale sono state aggiunte ulteriori informazioni necessarie al corretto invio del dato secondo un meccanismo comunemente detto di “incapsulamento”. In [Figura 10] è raffigurato il frame MAC completo di una rete IEEE 802.11, i

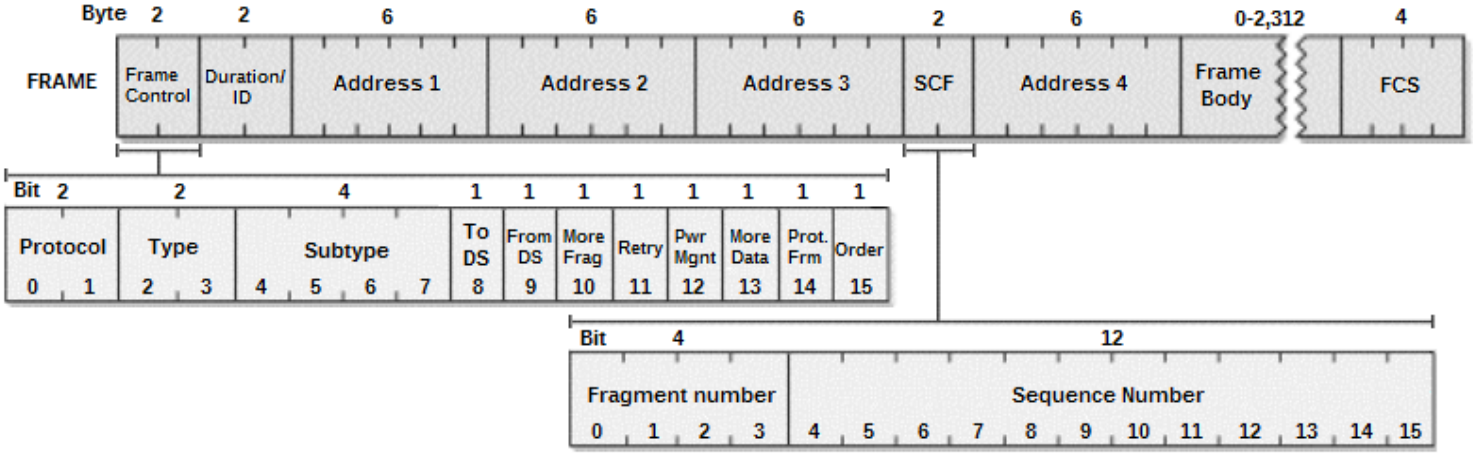



**Figura 10: Struttura di un frame MAC IEEE 802.11 completo**

bit vengono inviati da sinistra verso destra mentre i bit più significativi sono gli ultimi. Per "completo" si intende dire che alcuni dei campi che vi compaiono sono presenti in certi tipi di frame ma potrebbero anche non esserlo in altri.

### 3.2.1 Frame Control

Il primo campo e detto "frame control", è costituito dai primi due byte del frame e contiene molte informazioni sulla rete e sulla tipologia di dato trasportato. Di questi 16 bit si distingue:

- bit 0-1 (*protocol*): contiene la versione del MAC utilizzata.
- bit 2-3 e 4-7 (*type* e *subtype*): contengono il tipo e il sottotipo a cui appartiene il frame. Per un segnale di acknowledgment ad esempio il campo type è settato a 01, a indicare che si tratta di un frame di controllo, mentre il sottotipo sarà 1101 a specificare che nel particolare si tratta proprio di un frame ACK.
- bit 8 e 9 (FromDS e ToDS): indicano la tipologia del nodo di partenza (FromDS) e del nodo destinatario (ToDS) , un 1 indica l'infrastruttura mentre uno 0 indica una stazione. Ad esempio un frame con FromDS settato a 0 e ToDS a 1 è stato inviato da una stazione ed è destinato all'infrastruttura, ovvero ad un access point. Frame con entrambi i parametri a 0 viaggiano invece direttamente fra due stazioni, cosa che accade nelle sole reti ad hoc.
- bit 10 (*More fragments*): a volte i pacchetti IP sono talmente grandi che il MAC preferisce dividerli e inviarli in più frame. Un 1 in questo campo indica un frammento non terminale di un pacchetto.
- bit 11 (*Retry*): un 1 in questo campo indica che il frame è già stato inviato una volta ed è stato ora ritrasmesso. Può aiutare il nodo ricevente a eliminare possibili frame doppi.
- bit 12 (*Power management*): le stazioni mobili sono in genere alimentate a batteria e utilizzano spesso tecniche di risparmio energetico che consentono loro di disabilitare parte delle funzioni dell'interfaccia wireless. Se queste non si aspettano di ricevere dati nell'immediato poterebbero voler disabilitare momentaneamete la ricezione del segnale. Settando a 1 questo campo in un frame, posso comunicare ad un access point l'intento di entrare in risparmio energetico appena conclusa l'azione corrente. Un access point, sapendo una stazione in risparmio energetico, è in grado di mantenere all'inerno di un buffer i dati destinati a questa in attesa che si riattivi. Avendo in genere gli access point alimentazione diretta, i frame da loro inviati hanno sempre questo campo a 0.
- bit 13 (*More data*): un access point può segnalare a una stazione che dopo il frame corrente ce ne sono altri nel buffer a lei indirizzati ponendo a 1 questo flag. Una stazione può decidere eventualmente di mettersi in modalità di risparmio energetico leggendo il valore 0 in questo campo.
- bit 14 (*Protected frame*): se posto a 1 indica che il frame è stato sottoposto a un sistema di criptaggio dei dati come ad esempio il WEP (*wired equivalnet privacy*).
- bit 15 (*Order*): un 1 in questo campo indica che i frame vengono trasmessi in ordine.

### 3.2.2 Il campo Duration/ID

Il terzo e quarto byte del frame MAC costituiscono il duration/ID field che può principalmente due diverse funzioni. La prima e più comune di queste è quella di ospitare il valore del NAV. Quando l'ultimo dei 16 bit è 0, infatti, il campo viene interpretato dai nodi che ricevono il frame come il tempo in microsecondi al quale aggiornare il periodo di inaccessibilità del canale.

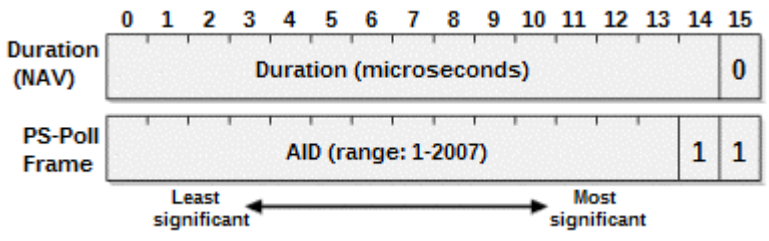



**Figura 11: Diverso utilizzo del campo per NAV e AID**

Un ulteriore utilizzo di questo campo è invece riservato ai speciali frame PS-Poll. Questo segnale può essere, in alcuni casi, utlizzato dalle stazioni che fanno uso di modalità di risparmio energetico. Al loro "risveglio" queste stazioni posso inviare un frame PS-Poll all'access point con il quale

richiedono l'invio dei dati accumulati nel buffer. A questo scopo il frame deve contenere per sicurezza anche l'ID di assosiazione o *association ID* (AID). In questo caso entrambi gli ultimi due bit, il 14 e il 15, sono settati a 1 e l'AID può assumere qualsiasi valore fra 1 e 2.007. I valori fra 2.008 e 16.383 sono riservati e non vengono utilizzati.

### 3.2.3 Indirizzi MAC

All'interno di un frame posso comparire fino a quattro campi di indirizzi. Gli indirizzi MAC seguono lo standard imposto a tutte le reti della famiglia IEEE 802. Dei 48 bit che li compongono il primo ha un significato speciale: uno 0 indica che si fa riferimento a un singolo nodo, mentre un 1 fa riferimento a un indirizzo di tipo multicast. Un indirizzo composto di soli 1 indica l'intera rete è costituisce quindi l'indirizzo di broadcast. Gli indirizzi che possono comparire all'interno di un frame sono i seguenti:

- Indirizzo del destinatario (*destination address*): il destinatario è il nodo che si occuperà di estrarre dal frame il pacchetto per mandarlo al soprastante network layer.
- Indirizzo del ricevitore (*receiver address*): tipicamente è il primo indirizzo a comparire nel frame. Per definizione il ricevitore è quel nodo che si occuperà di ricevere il segnale radio per poi ricavarne il frame che gli è stato inviato. Il ricevitore può eventualmente coincide con il destinatario.
- Indirizzo della sorgente (*source address*): l'indirizzo del nodo che ha creato il frame.
- Indirizzo del trasmettitore (*transmitter address*): in genere, all'interno del frame, compare subito dopo l'indirizzo del ricevitore. Fra trasmettitore e sorgente esiste l'analoga relazione che sussiste fra ricevitore e destinatario. Il trasmettitore è responsabile dell'immissione del frame sul canale e può eventualmente coincidere con la sorgente.
- BSSID (*Basic service set ID*): per identificare diverse LAN wireless nella stessa area, le singole stazioni possono essere esplicitamente assegnate alle diverse BSS tramite il BSSID. In una BSS a infrastruttura il BSSID è l'indirizzo MAC del access point mentre in una rete ad hoc è un indirizzo generato casualmente e con il primo bit sempre a 1 (per non rischiare conflitti). Un frame con BSSID costituito da soli 1 è indirizzato a tutte le reti ed è detto broadcast BSSID. Gli unici frame che posso usare questo indirizzo sono quelli relativi ai segnali di *probe request*, quelli cioè che le stazioni non ancora associate a nessuna rete inviano in broadcast per avere informazioni sulle eventuali BSS accessibili nella sua zona.

Il numero di indirizzi presenti in un frame non dipende solo dalla tipologia di rete ma varia anche da frame a frame. Il più delle volte sono presenti solo i primi tre inidrizzi raffigurati in [Figura 10], il quarto è utilizzato solo nelle reti a *wireless bridge*.

### 3.2.4 I dati

Ciò che interessa direttamente i dati trasportati dal frame si trova negli ultimi 12 byte, dei quali i primi due costituiscono il *sequence control field* che contiene un identificativo univoco del dato stesso. In particolare quattro bit sono qui dedicati all'indicizzazione dei frammenti apparteneti originariamente a uno stesso pacchetto. Un dato che giunge al MAC dal livello superiore può quindi essere suddiviso in non più di 16 parti che vengono indicizzate a partire da 0. Per ogni intero pacchetto trasmesso invece cambia il *sequence number* a cui sono dedicati i 12 bit successivi. Frammenti dello stesso pacchetto hanno quindi stesso *sequence number* e sono distinguibili e ordinabili per *fragment number*. Ovviamente, per non fare confusione, i frame che vengono ritrasmessi mantengono inalterati entrambi questi due byte.

Lo spazio dedicato al corpo del frame è variabile e dipende dalla grandezza del pacchetto di network layer originario e dal livello di frammentazione applicato dal MAC. Il corpo, in genere, può contenere fino a 2.312 byte, tuttavia certe reti che utilizzano algoritmi di criptaggio dei dati potrebbero dover supportare una lunghezza leggermente superiore per far spazio ad un eventuale overhead, mentre altre ancora potrebbero avere invece volutamente imposto limiti più restrittivi. La

correttezza dei dati ricevuti è garantita dagli ultimi 4 byte del frame che costituiscono il *frame check sequence* (FCS). Il valore di questo campo è ricavabile matematicamente dai bit del resto del frame, il ricevitore è così in grado di ricalcolarlo e di confrontarlo con quello ricevuto. Se il confronto va a buon fine significa che con molta probabilità il frame è stato inviato correttamente, il dato viene preso per valido e, dopo aver inviato il segnale di positive acknowledgement, viene inoltrato al livello OSI superiore. Nelle reti IEEE 802.11, nel caso in cui il check fallisca, il dato viene semplicemente scartato, non è previsto l'invio di un negative acknowledgment (NAK). I nodi ritrasmettono automaticamente se, dopo un tempo fissato dall'invio del frame, non hanno ancora ricevuto nessun ACK. Gli access point che devono modificare il frame per adattarlo a un'altra rete, sono ovviamente tenuti, dopo il primo check e la modifica, anche a ricalcolare il nuovo FCS è sostituirlo.

# 4. Sicurezza delle reti IEEE 802.11

Nelle reti wireless le trasmissioni radio da punto a punto avvengono in modo tale che possano essere ricevute in tutte le direzioni, entro un area sufficentemente grande. In realtà l'esatta posizione relativa di due nodi che comunicano direttamente fra loro in una stessa rete non è mai conosciuta, si sa solo che questi sono sufficentemente vicini per captare l'uno il segnale dell'altro. Altre stazioni all'interno della stessa area, normalmente, non ricevono i dati solo perchè sono state configurate in modo tale che i frame con indirizzo di destinazione diverso dal loro vengano ignorati. Una delle principali problematiche riscontrare durate lo sviluppo dello standard IEEE 802.11 è stato proprio quello di impedire l'eventualità che qualcuno, pur non appartenendo alla rete, potesse accedere alle informazioni che vi viaggiavano. Una prima soluzione fu data dall'introduzione di un opzionale standard di criptaggio chiamato *Wired Equivalent Privacy* (WEP). Nel 2001 fu, tuttavia, dimostrata ufficialmente la debolezza del sistema WEP e da allora seguirono, come vedremo, diverse sue evoluzioni.

## 4.1 WEP

### 4.1.1 Crittografia

Per proteggere i dati, l'802.11 iniziò a far uso, per lo standard WEP, di un sistema di criptaggio denominato RC4. Si tratta in particolare di uno *stream cipher* in quanto, come altri algoritmi, fa uso di una sequenza di bit detta *keystream* che, combinata con il messaggio da proteggere, permette di ottenere i dati cifrati. Per recuperare il messaggio originale dal testo cifrato è necessario possedere il keystream usato per il criptaggio. L'RC4, in particolare, utilizza l'operatore OR esclusivo (XOR) sui singoli bit per combinare il keystream con i dati e ottenerene così la versione criptata. In questo modo il destinatario non dovrà far altro che ripetere la stessa operazione, questa volta fra dato criptato e keystream per riottenere il messaggio originale [Figura 12].

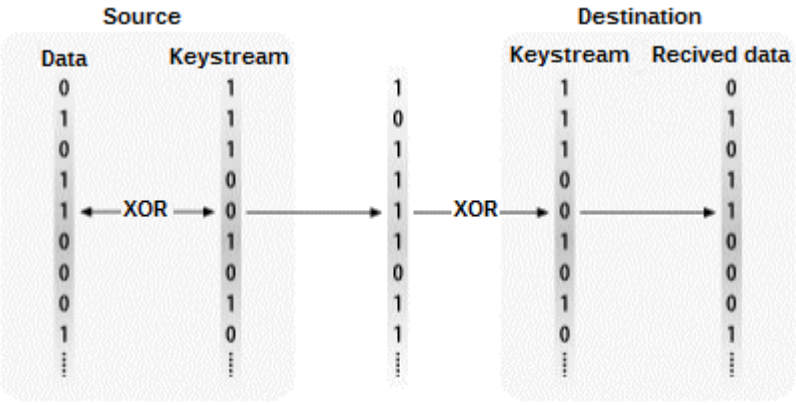



**Figura 12: Algoritmo di cifratura RC4**

Quello che viene chiesto di ricordare all'utente è ovviamente una singola parola chiave (o password) dalla quale poi si ricava ogni volta uno pseudo-random keystream della stessa lunghezza del messagio da criptare. Affinchè la

comunicazione funzioni entrambi gli interlocutori devono quindi utilizzare sia la stessa parola chiave che lo stesso algoritmo di generazione del keystream. Il fatto che la chiave venga espansa in una sequenza il più casuale possibile è di estrema importanza per l'effettiva sicurezza che si vuole garantire. L'unico metodo di criptaggio che si può dimostrare matematicamente essere immune a molte tipologie di attacco deriva infatti dall'utilizzo di un keystream generato in modo totalmente casuale. Generare una sequenza totalmente casuale è tuttavia molto più difficile di quanto si possa credere, basti pensare che tutto ciò che deriva da un algoritmo, per sua natura, già non può essere definito casuale. Un keystream generato senza nessun preciso algoritmo dovrebbe poi necessariamente essere distribuito fra gli utenti in quanto questi non avrebbero nessun modo di ricalcolarlo e il problema, a quel punto, diverrebbe la creazione di un sistema di distribuzione perfettamente sicuro. Per questi motivi le sequenze utilizzate, in realtà, non sono mai totalmente casuali e vengono invece dette "pseudo-random" in quanto, per questo tipo di applicazioni, permettono comunque di ottenere buoni risultati.

### 4.1.2 Il processo WEP

Nonostante si sia dimostrato inadeguato, il WEP è ancora utilizzato da molti cellulari e palmari che non siano di ultima generazione. Anche con la consapevolezza della sua debolezza, per molto si è continuato a far affidamento sul WEP in quanto, a differenza dei suoi successori, è più semplice da implementare e richiede una potenza di calcolo minore. Per certe applicazioni dunque, rimane la soluzione migliore, se non l'unica possibile.

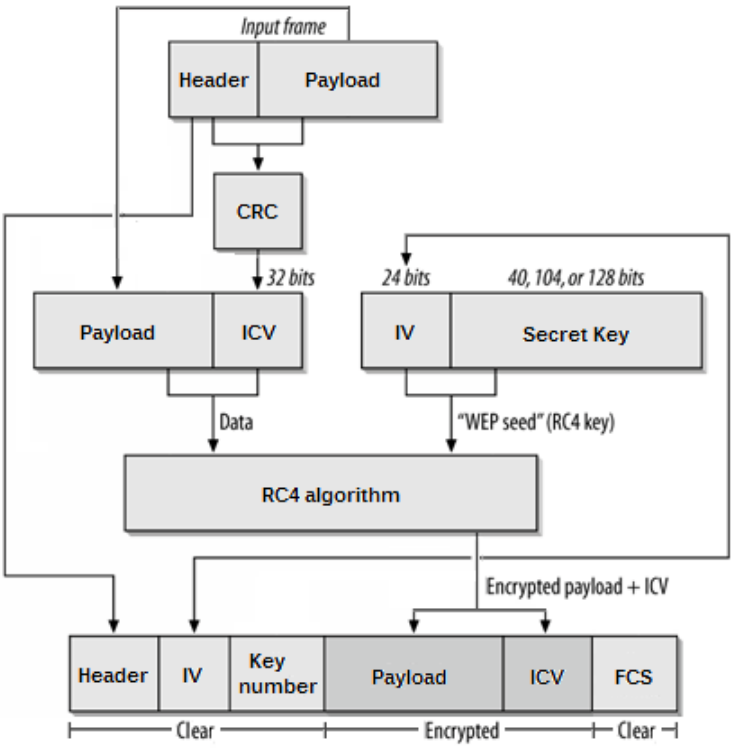



**Figura 13: Il processo WEP**

La procedura di criptaggio prevede innanzitutto il calcolo di un *integrity check value* (ICV) di tutto il frame, che permetterà al momento della decriptazione di controllare l'integrità dei dati. In particolare, l'ICV utilizzato dal WEP è un *Cyclic Redundancy Check* (CRC). A questo punto, dal frame viene estratta la parte proveniente dal layer superiore (*payload*) e ne viene concatenato l'ICV appena calcolato per ottenere il dato che verrà effettivamente protetto. Il keystream necessario all'algoritmo RC4 viene invece espanso da una sequenza detta chiave RC4 (*RC4 key*) ottenuta dalla concatenazione di un *initialization vector* (IV) di 3 byte con una parola chiave (*secret key*) che, invece, può avere una lunghezza variabile di 5, 13 o 16 byte. L'algoritmo di generazione del keystream, in realtà, produce sempre la stessa sequenza per una data chiave e una data lunghezza del dato da proteggere ed è per questo che per ogni frame viene preposta alla parola chiave un IV, ovvero una sequenza pseudo-random di 24 bit. Con l'utilizzo dell'algoritmo RC4 i dati vengono criptati e il frame può quindi essere riassemblato. All'header MAC originale viene apposto un WEP header formato dall'IV e dal key number. L'IV servirà al destinatario per assemblare la chiave RC4 con cui generare il corretto keystream mentre il key number indica quale parola chiave è stata utilizzata. Il WEP, infatti, prevede l'utilizzo di fino a 4 parole chiave diverse e il key number permette di specificare quale è stata usata per il frame corrente. Al header WEP segue poi il risultato dell'operazione di cifratura a cui, per finire, viene apposto l'FCS calcolato, come abbiamo visto, sull'intero frame.

### 4.1.3 I problemi del WEP

Nel 2001, Scott Fluhrer, Itsik Mantin, e Adi Shamir pubblicarono un articolo intitolato "Weaknesses in the Key Scheduling Algorithm of RC4" che fece emergere una debolezza riguardante proprio l'algoritmo di generazione del keystream (detto appunto *Key Scheduling Algorithm*). Alla fine di questo articolo vi è anche la descrizione teorica di un possibile attacco a un rete che sfrutta le loro scoperte e permette di risalire alla parola chiave WEP tramite la cattura dei frame criptati. Come abbiamo visto, il dato che viene criptato è composto dal payload MAC e dal ICV. I primi bit del payload costituiscono un particolare header (*SNAP header*) che viene aggiunto dal layer LLC e poi successivamente incapsulato nel frame del sottostante layer MAC. Purtroppo il primo byte di questo header è notoriamente sempre 0xAA. Il primo byte del dato è quindi conosciuto e avendo a disposizione anche la sua versione criptata che viaggia nel frame, possiamo, tramite l'XOR ricavare anche il primo byte del keystream. Questo fatto ha portato alla luce una particolare classe di IV che appaiono nella forma b+3:FF:n, detti *weak IVs*. Nella notazione usata in questi casi, i byte vengono scritti in forma esadecimale e separati l'uno dall'altro dai due punti. Gli IV detti "deboli" sono quindi quelli formati da un primo byte pari a b+3, dove b è un valore che vedremo più tardi, da un secondo byte pari a 0xFF, ovvero al byte di soli 1 e da un terzo byte che può assumere qualsiasi valore n. La particolarità di questi IV è che danno informazioni su particolari byte della chiave RC4. La parte della chiave RC4 di maggior interesse è quella dopo il terzo byte in quanto costituisce la vera password (*secret key*) che gli utenti usano per collegarsi alla rete, indichiamo dunque con "b" l'indice, a partire da 0, dei byte di questa password. Con b=1 indichiamo ad esempio il secondo byte della password, ovvero il quinto byte dell'intera chiave RC4. Gli IV nella forma 4:FF:n (b+3=4, b=1), sono quindi IV deboli e possono essere usati per ricavare informazioni sul secondo byte (b=1) della password.
Lo studio compiuto da Fluhrer, Mantin e Shamir è interamente basato su calcoli statistici. Ciò che notarono fu l'esistenza di una notevole correlazione fra i byte della password e una particolare classe di IV. Il metodo da loro proposto consiste nel collezionare un gran numero di frame alla ricerca degli IV deboli. Secondo quanto da loro stimato, 60 diversi IV deboli relativi allo stesso byte permettono già di stimare correttamente tale byte. Questo studio è stato in seguito enormemente ampliato e si sono trovati nuove classi di IV sfruttabili. Oggi, per una tipica password WEP di 40 bit, il 5% degli IV è considerato debole e il processo di cattura dei frame necessario al recupero dell'intera parola chiave richiede, per una rete mediamente attiva, solo pochi minuti.

## 4.2 Standard di sicurezza IEEE 802.11i

Il team che si occupò di stabilire lo standard IEEE 802.11i fu incaricato di risolvere definitivamente i problemi legati alla sicurezza nelle reti wireless. In sostituzione al WEP furono sviluppati in contemporanea due nuovi protocolli: il *Temporal Key Integrity Protocol* (TKIP) e il *Counter Mode with CBC-MAC Protocol* (CCMP). Dato che la conclusione dei lavori era stata rinviata più volte la Wi-Fi Alliance fu autorizzata al rilascio di uno standard commerciale chiamato *Wi-Fi Protected Access* (WPA), basato sulla versione non definitiva del TKIP. Il WPA2 invece include anche il CCMP ed è basato sullo standard finale IEEE 802.11i.

### 4.2.1 Gestione delle chiavi

Un primo miglioramento è stato fatto sulla gestione delle chiavi, per la quale è stato definito un set di procedure che va sotto il nome di *Robust Security Network* (RSN). Ciò che si è voluto fare è per prima cosa evitare il più possibile di utilizzare direttamente la chiave principale (*master key*), in modo da diminuire le occasioni in cui questa possa essere scoperta. In secondo luogo, si è deciso di usare più chiavi, ciascuna con il suo specifico scopo, in modo tale che, anche se ne venisse scoperta una, non sarebbe comunque possibile l'accesso completo alla rete.

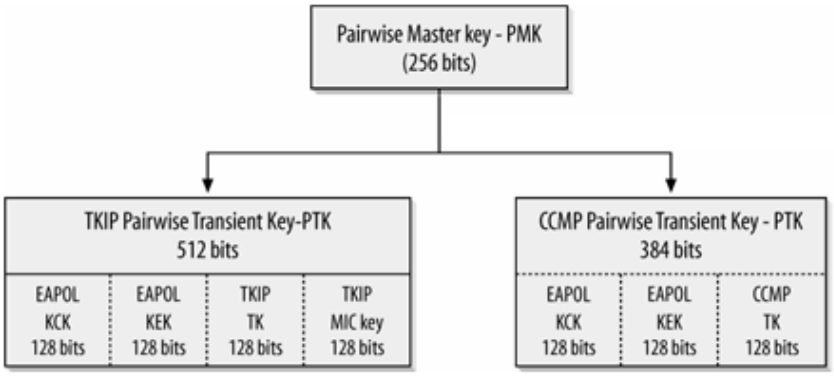



**Figura 13: Espansione della master key per TKIP e CCMP**

Le chiavi utilizzate dalla rete sono suddivise in due gruppi. Le *pairwise keys* sono destinate a proteggere il traffico fra una stazione e un AP, mentre le *group keys* proteggono le trasmissioni broadcast e multicast da un AP verso le relative stazioni associate. Entrambi gli standard TKIP e CCMP che vedremo in seguito ottengono tutte le chiavi di cui hanno bisogno espandendole con un particolare algoritmo dalla master key. In figura è rappresentato come il TKIP e il CCMP espandono la master key (che in questo contesto è anche detta *pairwaise master key*, o PMK) per ottenere l'intero set delle pairwise keys. Nel caso del TKIP, dalla master key di 256 bit si ottiene una seconda chiave di 512 bit detta *pairwise transient key* (PTK). Suddividendo la PTK in blocchi da 128 bit si ottengono infine le 4 chiavi dette pairwise keys. Le prime due, *EAPOL Key Confirmation Key* (KCK) e *EAPOL Key Encryption Key* (KEK), sono usate sia dal TKIP che dal CCMP e vengono utilizzate per la sicurezza dei pacchetti EAP (*Extensible Authentication Protocol*) ovvero per trasmissioni di tipo request-response impiegate per specifiche procedure di autenticazione. Le altre due sono invece la *temporal key* (TK) e la MIC key (usata solamente dal TKIP), vengono utilizzate per la sicurezza di tutte le altre tipologie di frame e il loro utilizzo lo vedremo più avanti, separatamente per TKIP e CCMP.

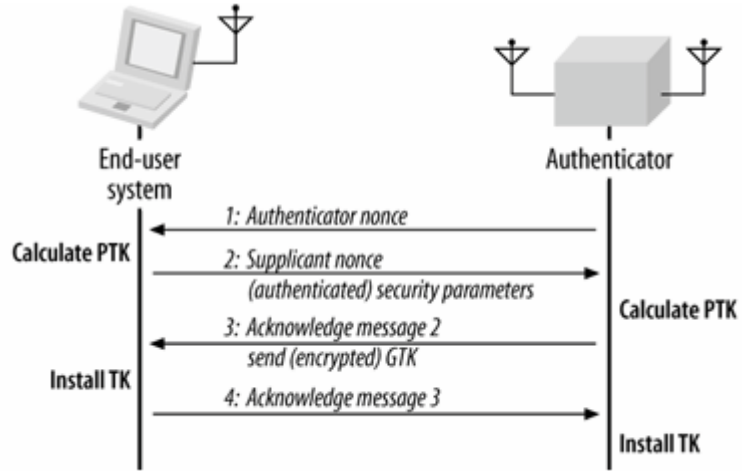



**Figura 14: Four-way handshake**

Con questo sistema, non solo la master key non viene mai utilizzata direttamente, ma c'è anche la possibilità di derivare le chiavi necessarie in qualsiasi modo, cambiarle a intervalli regolari e persino crearne di specifiche per ogni singola stazione. Il procedimento con il quale una stazione si accorda con un access point sul modo di espandere la master key è detto *handshake* e fa parte dei metodi implementati dal protocollo EAP. Le pairwise keys e le group keys vengono definite tramite due diversi handshake, in particolare il processo di aggiornamento delle pairwise keys è detto *four-way handshake*. Come suggerisce il nome, il procedimento consiste nello scambio di 4 pacchetti EAPOL (*EAP Over LAN*). Il primo di questi è inviato dall'access point verso la stazione con la quale è necessario definire o aggiornare le chiavi e contiene un semplice *nonce*, ovvero una sequenza casuale di bit. La stazione interessata è così in grado di calcolare l'intero set delle pairwaise keys (ovvero la *transient key*) usando come input la master key di cui è in possesso, l'indirizzo MAC suo e dell'access point, il *nonce* che ha appena ricevuto e un secondo nonce che calcolerà personalmente. Con il secondo pacchetto la stazione invia all'access point il secondo nonce e una copia dei dati della sua associazione, il tutto autenticato da un integrity check del messaggio, calcolato utilizzando la nuova KCK appena ricavata. Ora l'AP, con il secondo nonce, può espandere allo stesso modo le chiavi e verificare che anche la stazione lo abbia fatto correttamente verificando che l'integrity check sia stata calcolato con la KCK corretta. Il terzo pacchetto informa la stazione che il procedimento è andato a buon fine e consegna una copia della corrente group transient key, il tutto criptato con l'uso della KEK e autenticato tramite integrity check con la KCK. Infine l'ultimo pacchetto, autenticato come al solito, indica che le nuove chiavi sono ora operative.

### 4.2.2 TKIP

Il TKIP (Temporal Key Integrity Protocol) fu sviluppato come una prima soluzione alla debolezza del sistema WEP. Questo nuovo protocollo costituisce un semplice miglioramento della procedura WEP in quanto le meccaniche base di quest'ultimo rimangono invariate. All'epoca era necessario infatti trovare una soluzione velocemente e si è voluto quindi sviluppare qualcosa che potesse essere implementato immediatamente sull'hardware che era già in commercio.

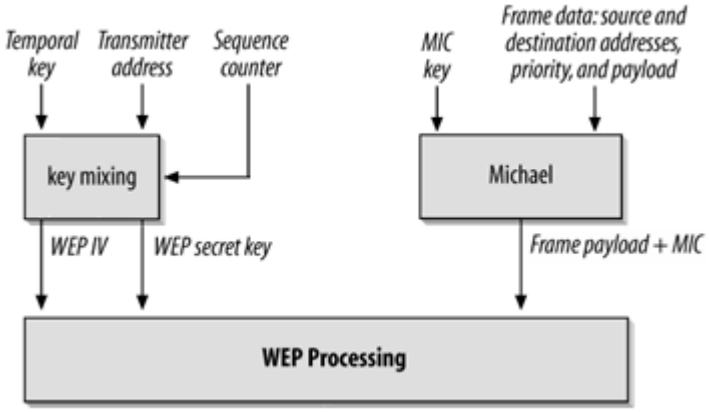



**Figura 15: Il processo TKIP**

I principali miglioramenti apportati, oltre al già discusso sistema RSN, sono l'introduzione del *sequence counter* e di un nuovo algoritmo per l'integrity check chiamato Michael. Il sequence number numera i frame trasmessi fra due nodi e impedisce che qualche stazione possa "imbrogliare" la rete catturando dei pacchetti e ritrasmettendoli così come sono in un secondo momento (*replay attack*). I numeri sono assegnati a ogni frame consecutivamente a partire da un valore iniziale che viene resettato ogni qualvolta le chiavi vengono aggiornate. Tramite un processo detto *key mixing*, il TKIP calcola un IV e una parola chiave WEP diversi per ogni frame, a partire dalla temporal key (una delle pairwise keys), dall'indirizzo del trasmettitore e dal sequence counter. L'IV in particolare è costituito questa volta da 48 bit invece che da 24 e viene strutturato in modo tale da evitare la generazione di chiavi RC4 deboli. In seguito, tramite l'algoritmo Michael, viene prodotto, con l'utilizzo della MIC key, del payload e degli indirizzi MAC di sorgente e destinazione, il *Message Integrity Check* (MIC), più robusto del CRC e calcolabile con semplici operazioni sui bit. A questo punto il payload affiancato al MIC costituisce il nuovo dato da criptare e assieme al IV e alla parola chiave viene dato in input al processo WEP che abbiamo precedentemente descritto. La struttura del frame finale rimane dunque invariata e le funzioni aggiuntive, come quelle relative all'algoritmo Michael, pur aggiungendo carico computazionale sono realizzabili tramite operazioni già supportate dall'hardware WEP.

### 4.2.3 CCMP

A differenza del TKIP, il CCMP (Counter Mode with CBC-MAC Protocol) è stato ideato come standard di sicurezza definitivo e pensato per l'hardware di nuova generazione. Utilizza un nuovo algoritmo di cifratura detto *Advanced Encryption Standard* (AES) impiegato anche dal U.S. National Security Agency. A differenza del RC4 l'AES trasforma i dati tramite una chiave agendo separatamente su singoli blocchi di bit. L'AES supporta vari formati, ma per l'802.11i si è scelto l'uso chiavi e blocchi entrambi di 128 bit. Il TKIP è stato costruito su una base non robusta e per evitare che questo possa vanificare ulteriori sforzi in questo senso, il CCMP presenta invece un sistema totalmente rinnovato. Il nuovo processo prevede innanzi tutto il calcolato sull'header MAC dell'*Additional Authentication Data* (AAD). L'header in questione non può essere criptato in alcun modo poiché contiene informazioni necessarie all'invio del frame sul mezzo che devono quindi poter esser lette chiaramente. L'AAD permette, però, di controllare che le parti principali di queste informazioni non vengano alterate durante la trasmissione. In particolare protegge gli indirizzi MAC principali, il sequence number (all'interno del SCF) e buona parte del frame control (protocol version, type, e i bit To/From DS, more fragments e order). Un header CCMP viene poi formato tramite il *packet number* e il *key ID*. Il key ID, come il key number per il WEP, specifica quale master key è stata impiegata (è possibile specificare fino a 6 diverse chiavi) mentre il packet number ha lo stesso scopo del sequence counter che abbiamo visto nel TKIP, numera sequenzialmente ogni trasmissione fra una coppia di nodi in modo univoco durante l'uso di una stessa transient key ma il suo valore non aumenta per frame che vengono ritrasmessi (il sequence

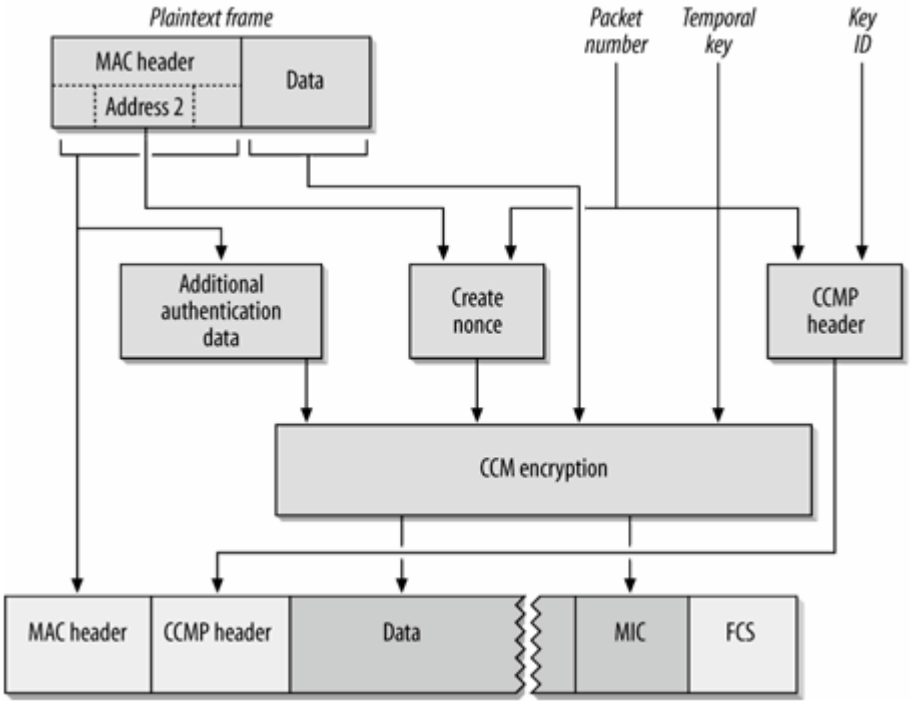



**Figura 16: Processo CCMP**

counter in questo caso invece incrementerebbe).
A questo punto è possibile procedere con il criptaggio dei dati, ovvero alla "CCM encryption". Con CCM (Counter with CBC-MAC) ci si riferisce ad un sistema che, con l'utilizzo di una singola chiave, provvede contemporaneamente sia all'autenticazione che al criptaggio dei dati. La "CCM mode" (da cui il nome del protocollo CCMP) è utilizzabile solo in coppia con un algoritmo di cifratura "a blocchi" (nel nostro caso AES-128 bit). Gli input a questo sistema sono i dati (payload), la temporal key (dalle pairwise keys), l'AAD e un nonce. Quest'ultimo viene generato in modo tale che uno stesso suo valore non venga mai usato due volte con la stessa temporal key. Poiché due frame, se indirizzati a due nodi diversi, possono avere lo stesso packet number, per il calcolo del nonce è quindi richiesto in input anche l'indirizzo del trasmettitore. Il prodotto della cifratura CCM, come anticipato, comprende sia i dati criptati che un MIC (Message Integrity Check) per l'autenticazione degli stessi. Come ultima cosa, il frame viene riassemblato con l'introduzione del header CCMP e, come di consueto, ne viene calcolato l'FCS (anch'esso inserito all'interno del frame).

# 5. Test pratici di sicurezza

Dopo quanto abbiamo visto finora sulla sicurezza dell'IEEE 802.11, proveremo ora a vedere cosa realmente può fare una stazione per accedere a una rete senza averne l'autorizzazione. Per fare questo ci serviremo della suite open source aircrack-ng, un insieme di programmi che permette la cattura e l'invio di pacchetti senza nessun tipo di restrizione. Utilizzeremo un access point e due PC per simulare l'ambiente che ci interessa. Una prima generica stazione sarà collegata tramite l'AP a una rete appositamente creata, mentre una seconda sarà posizionata in modo tale da poter intercettare chiaramente le trasmissioni all'interno della rete ma senza farne parte. Ipotizzeremo di avere il controllo della stazione non associata sulla quale è presente il sistema operativo ubuntu 12.0 e la suite aircrack-ng installata. Come primo cosa vedremo l'applicazione del metodo di Fluhrer,

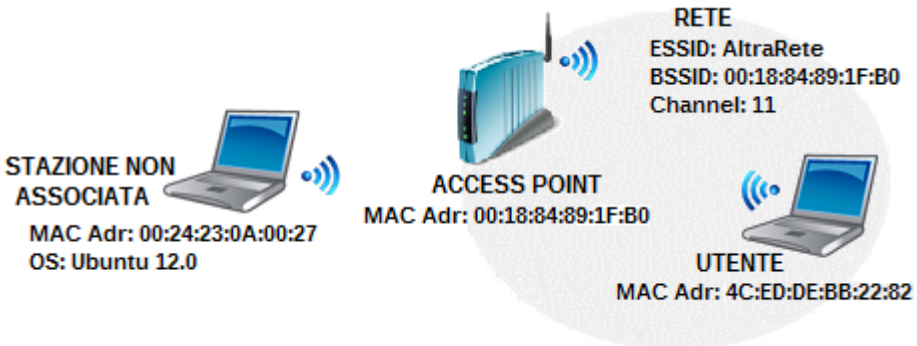



**Figura 17: L'ambiente simulato per i test**

Mantin e Shamir (FMS) per riuscire a recuperare la password della rete nel caso in cui questa sia protetta dal protocollo WEP che ricordiamo non essere più utilizzato proprio per la sua debolezza. Infine vedremo il caso in cui la rete utilizzi il sistema WPA-PSK largamente usato sia in ambito domestico che aziendale. Quest'ultimo protocollo è tutt'oggi un sistema di sicurezza robusto e ci limiteremo quindi a descrivere un teorico attacco a questo tipo di rete.

## 5.1 WEP

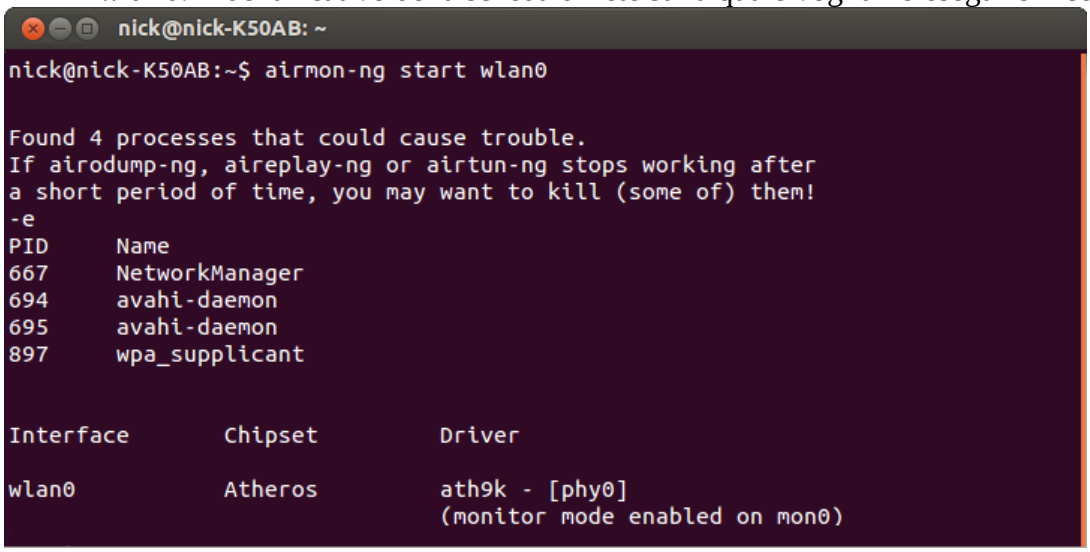
Fra le tante cose, aircrack-ng implementa un adattamento del metodo FMS (migliorato e ottimizzato) per riuscire a risalire alla parola chiave WEP tramite la cattura dei pacchetti criptati. Con ciascun IV debole in suo possesso assegna un "voto" a un particolare byte in modo tale che, fra questi, quelli che alla fine totalizzeranno un numero maggiore di voti avranno una maggior probabilità di far parte della password. Per aumentare le possibilità di successo, non vengono presi in considerazione solo i valori più probabili ma anche quelli che hanno totalizzato un numero di voti che risulta comunque relativamente alto. Vengono quindi verificate tutte le chiavi ricavate da tutte le combinazioni dei byte che sono ritenuti potenzialmente validi. Questo metodo può essere considerato un ibrido fra quello di natura statistica che abbiamo visto e il metodo detto di *brute force* che consiste invece nel tentare tutte le soluzioni possibili. Il compromesso fra le due strategie è dato dal *fudge factor* il cui significato lo vedremo a breve.

1.Innanzitutto è necessario impostare la scheda di rete wireless in *monitor mode*, questo ci permetterà di metterci in ascolto di tutte le trasmissioni Wi-Fi che viaggiano attorno a noi, a prescindere dalla loro provenienza. Per fare questo eseguiamo tramite shell unix il comando:

```
airmon-ng start wlan0
```

Con questo richiamiamo il programma airmon-ng che si trova nella suite di aircrack specificando i seguenti parametri:

- **start**: con questo chiediamo di abilitare la monitor mode su un interfaccia wireless. Allo stesso modo il parametro stop permette di ripristinare la normale *managed mode*.
- **wlan0**: l'identificativo della scheda di rete sulla quale vogliamo eseguire il comando.



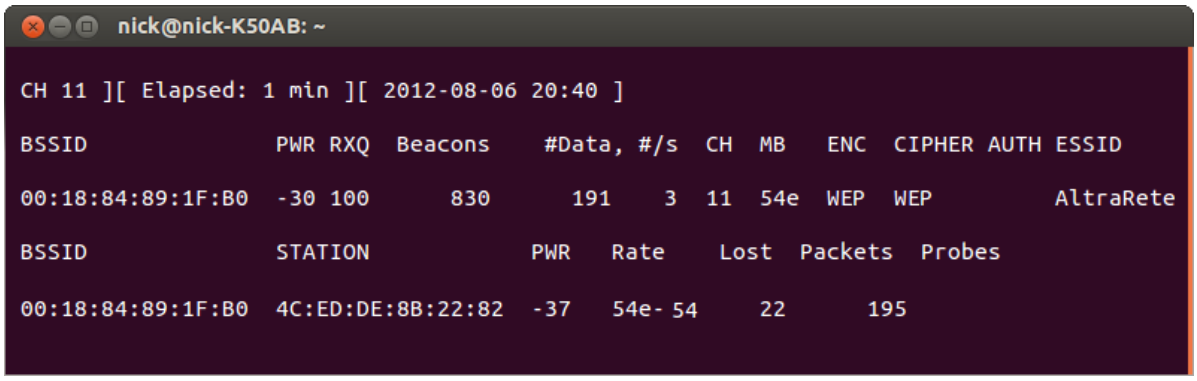

L'output ci informa che la monitor mode è stata abilitata su una periferica virtuale "mon0" appena creata. D'ora in avanti al posto di wlan0 useremo quindi mon0. Il programma ci avvisa inoltre che in caso di problemi potrebbe essere necessario terminare momentaneamente alcuni processi in quanto potrebbero impegnare la periferica wireless.

2. A questo punto è necessario iniziare a catturare i pacchetti. Per fare questo ci serviamo di una seconda applicazione della suite chiamata airodump-ng in grado di salvare i pacchetti all'interno di un file. Dato che siamo interessati ai dati di una rete in particolare, ne specifichiamo il BSSID e il canale che utilizza in modo da ignorare trasmissioni estranee. Eseguiamo quindi il seguente comando:

```
airodump-ng -c 11 --bssid 00:18:84:89:1F:B0 -w pkt mon0
```

Nel particolare i parametri che vi compaiono sono:

- **-c 11**: specifica il canale sul quale raccogliere i pacchetti. In questo caso 11.
- **--bssid 00:18:84:89:1F:B0**: specifica il BSSID dell'unica rete di cui vogliamo i pacchetti. In questi casi il BSSID coincide con l'indirizzo MAC dell'access point.
- **-w pkt**: "pkt" sarà il prefisso comune ai file in cui verranno salvati i dati raccolti.
- **mon0**: l'identificativo della scheda di rete da usare. Indichiamo la periferica virtuale mon0 appena creata, attualmente in monitor mode.




Come volevamo, compare la sola rete a cui siamo interessati ("AltraRete") e tutte e sole le stazioni che vi fanno parte (in questo caso c'è un unico utente). Per la rete sono rese disponibili le seguenti informazioni:

- BSSID: indirizzo di identificazione della BSS.
- PWR: la potenza con cui ci giunge il segnale dell'access point in dB.
- RXQ: *receive quality*. Percentuale di pacchetti catturati negli ultimi 10 secondi.
- Beacons: sono pacchetti che l'AP manda alle stazioni per informarle della presenza di una rete e delle modalità con cui è possibile collegarsi a questa. Molte delle informazioni che il programma riporta, come il canale o il nome della rete, derivano dalla lettura di questi pacchetti. Il numero sotto questa colonna indica quanti beacons sono stati ricevuti.
- #Data: numero di pacchetti catturati finora.
- #/s: pacchetti al secondo che vengono catturati, valore calcolato sugli ultimi 10 secondi.
- CH: il numero del canale (*channel*) sul quale si trova la rete.
- MB: velocità massima supportata dall'access point. Il valore 54 in questo caso indica che è evidentemente supportato l'IEEE 802.11g mentre la "e" vicino al numero indica che l'AP fa uso del QoS (*Quality of Service*).
- ENC: lo standard di sicurezza di cui fa uso la rete. WEP, WPA o WPA2.
- CHIPHER: in questo caso viene riportato nuovamente WEP in quanto il sistema è già ben definito. Per WPA e WPA2 verrebbe per esempio specificato l'utilizzo del TKIP o del CCMP.
- AUTH: modalità di autenticazione. Il WEP non usa l'RSN perciò il campo è lasciato vuoto.
- ESSID: nome della rete.

Mentre per quanto riguarda le stazioni:

- BSSID: indirizzo di identificazione della BSS a cui è associata la stazione.
- STATION: indirizzo MAC della stazione.

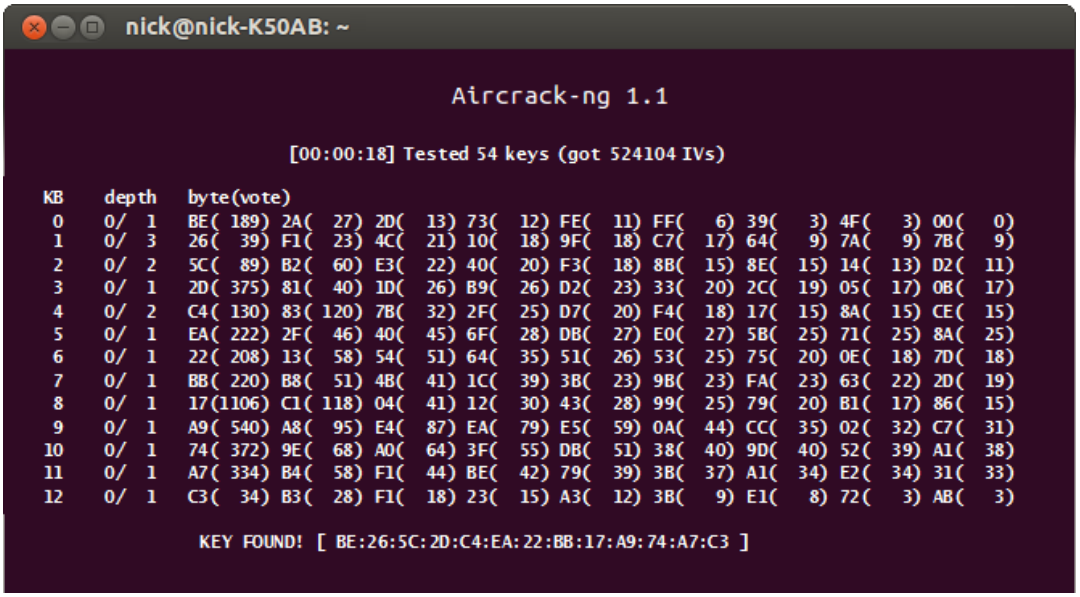
- PWR: potenza del segnale della stazione in dB.
- Rate: sono le velocità di trasmissione dal AP verso la stazione e dalla stazione verso l'AP separate da "-". In questo caso entrambe le velocità sono di 54 Mbit/s.
- Lost: il numero di pacchetti che non siamo riusciti a catturare basandosi sul valore del sequence number all'interno dei frame.
- Packets: il numero di pacchetti inviati dalla stazione.
- Probes: i segnali di probe request sono usati dalle stazioni per sollecitare gli AP a inviare le informazioni per l'accesso alla rete. Il programma utilizza questi frame per sapere se una stazione non ancora associata sta cercando di collegarsi a qualche rete. Sotto questa colonna vengono riportati gli ESSID delle reti alle quali la stazione ha inviato un segnale di probe. In questo caso l'utente era già collegato e quindi non è stato catturato nessun frame di questo tipo.

3. Quando verranno catturati abbastanza pacchetti non rimarrà che analizzare gli IV. Tramite aircrack-ng eseguiamo:

```
aircrack-ng -f 2 -b 00:18:84:89:1F:B0 pkt*.cap
```

dove:

- **-f 3**: imposta il valore del fudge factor a 2.
- **-b 00:18:84:89:1F:B0**: nel caso in cui fossero stati catturati all'interno degli stessi file dati relativi a reti diverse è necessario specificare il BSSID che ci interessa. Nel nostro caso la cattura era già stata limitata ad una sola rete perciò avremmo potuto non specificare questo parametro.
- **pkt*.cap**: con questo indichiamo che i file contenenti i frame raccolti sono hanno prefisso comune "pkt" e estensione ".cap".




Ogni riga fa riferimento a un key byte (KB) della password. Per spiegare come il programma procede e come viene influenzato dal fudge factor, prendiamo come esempio la riga dell'output relativa al key byte 1. Vengono riportati i possibili valori di questo byte e fra parentesi il numero di voti che ciascuno di questi ha accumulato dall'analisi degli IV catturati. Il valore del byte 1 più probabile è dunque 26 poiché ha accumulato il maggior numero di voti per questo byte (39 voti). Il programma divide il numero di questi voti per il fudge factor:
39/2=19.5
Saranno considerati perciò validi e da testare tutti i valori del byte che hanno ricevuto un numero di voti maggiore o uguale a 19.5, ovvero in questo caso i tre valori 26, F1 e 4C. Per il byte 1 si ha

quindi una profondità (*depth*) totale di 3. Il programma, sotto la colonna "depth" riporta il valore "0/3" a significare che in quell'istante, per quel specifico byte, sta per il momento prendendo in considerazione il primo valore dei tre possibili. Nel nostro esempio la chiave è stata trovata dopo soli 18 secondi ed è riportata dal programma in forma esadecimale.

## 5.2 WPA-PSK

Abbiamo visto che il sistema RSN impiegato nei protocolli di sicurezza WPA/WPA2 fa uso di chiavi temporanee per criptare i frame. Cercare di risalire a queste, oltre a risultare più difficile, non permetterebbe comunque l'accesso alla rete. La Wi-Fi Alliance ha rilasciato due tipologie di WPA il WPA-PSK e il WPA-Enterprise. Queste variano sulla metodologia con la quale le stazioni vengono autorizzate all'accesso alla rete. Il WPA-Enterprise prevede a questo scopo un server dedicato che attraverso un complesso scambio di certificati TLS (*Transport Layer Security*) può autorizzare o meno una stazione che ha richiesto l'associazione. Ovviamente questo sistema viene utilizzato solo per reti di grandi dimensioni, per tutte le altre è invece largamente usato il più semplice WPA-PSK (o WPA-Personal). Il sistema PSK (*Pre-Shared Key*) prevede semplicemente che ogni stazione ricavi dal ESSID della rete e da una password (la parola chiave che l'utente deve ricordare per collegarsi alla rete) la master key con la quale potrà portare a termine correttamente il processo di handshake con l'AP e di conseguenza essere ammesso alla rete. In quest'ultimo caso però, se il four-way handshake viene catturato, è possibile, tramite un approccio di tipo brute force, provare a risalire alla password. Fortunatamente, per far fronte a questo problema lo standard WPA impone che la lunghezza della password non sia inferiore a 8 caratteri, cosa che effettivamente rende la procedura di brute force quasi impraticabile. Quello che vedremo è quindi solo un attacco teorico: ci limiteremo a catturare il four-way handshake e a scopo dimostrativo verificheremo se la password è una parola italiana di senso compiuto.

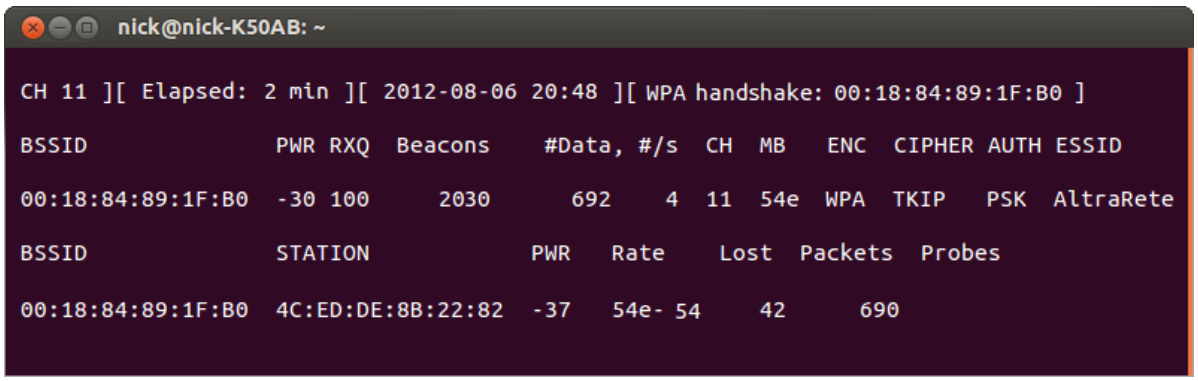
1. Dobbiamo ancora una volta metterci nelle condizioni di poter catturare i pacchetti perciò ripercorriamo i punti 1 e 2 della precedente dimostrazione. A questo punto stiamo nuovamente salvando i dati all'interno di un file ma quello a cui siamo veramente interessati sono i pacchetti EAP del four-way handshake. Per non interrompere la cattura, apriamo una nuova shell e usiamo il programma aireplay-ng della suite aircrack-ng per inviare alla stazione collegata alla rete un falso pacchetto di deautenticazione. In questo modo costringeremo l'utente a ripetere il processo di handshake e noi saremo pronti a catturare i pacchetti. Eseguiamo su una seconda shell il seguente comando:

```
aireplay-ng -0 1 -a 00:18:84:89:1F:B0 -c 4C:ED:DE:8B:22:82 mon0
```

dove abbiamo specificato i seguenti parametri:

- **-0**: il programma aireplay-ng è in grado di creare ogni tipo di frame 802.11 e di inviarlo a una qualunque stazione senza alcuna restrizione. Con "0" indichiamo che siamo interessati a un frame di deautenticazione.
- **1**: il numero di frame che vogliamo mandare.
- **-a 00:18:84:89:1F:B0**: indirizzo MAC dell'AP. La stazione deve credere che il frame provenga dall'access point.
- **-c 4C:ED:DE:8B:22:82**: indirizzo MAC della stazione a cui mandare il frame e che quindi vogliamo deautenticare.
- **mon0**: la periferica wireless virtuale.

A questo punto la stazione dopo esser stata deautenticata si ricollegherà automaticamente alla rete e sulla prima shell possiamo vedere il seguente risultato:



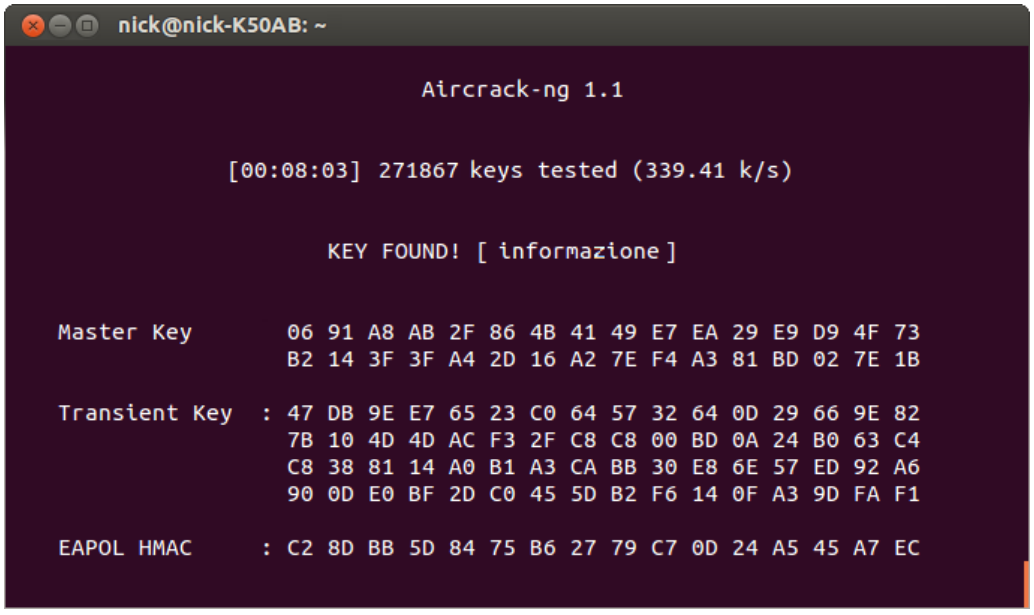

In alto a destra possiamo leggere "WPA handshake: 00:18:84:89:1F:B0" a indicare che fra i dati raccolti siamo riusciti a catturare anche un four-way handshake valido. Notiamo anche che la rete è stata identificata correttamente come protetta da WPA-PSK TKIP.

2. Possiamo ora provare a ricavare la password. Per fare questo useremo il file di testo "wordlist.txt" contenete tutte le parole italiane di senso compiuto. Affinché la password venga trovata dovrà essere una parola contenuta nel nostro file. Eseguiamo il seguente comando:

```
aircrack-ng -w wordlist.txt -b 00:18:84:89:1F:B0 pkt*.cap
```

I parametri sono:

- **-w wordlist.txt**: il file contenete le parole chiave che volgiamo verificare.
- **-b 00:18:84:89:1F:B0**: BSSID della rete.
- **pkt*.cap**: specifica i file dove sono stati salvati i dati. Devono contenere un four-way handshake valido.




Per ogni parola all'interno del file wordlist.txt il programma calcola quale sarebbe la relativa master key, la espande nella transient key e infine ricava il four-way handshake. Se questo risulta uguale all'handshake originale che abbiamo catturato significa che la password è quella giusta altrimenti ripete l'operazione dall'inizio con la parola successiva. Nel nostro esempio la password era "informazione" ed è stata trovata dopo poco più di 8 minuti.

# Conclusioni

Si sono presentate le problematiche e le difficoltà che stanno dietro ai sistemi di sicurezza di una rete dando un'idea della delicatezza della questione. L'ultimo capitolo, in particolare, dimostra come sia possibile, anche senza particolari conoscenze, sfruttare con semplicità anche una piccola debolezza per agire in modo scorretto nei confronti di una rete con l'aiuto di un software che implementi i giusti algoritmi. Basta dunque un piccolo errore nella progettazione di un protocollo di sicurezza per renderlo completamente inaffidabile.

# Bibliografia


- «Aircrack-ng Main Documentation.» s.d. http://www.aircrack-ng.org/documentation.html.

- Gast, Matthew S. *802.11 Wireless Networks: The Definitive Guide.* O'Reilly, 2005.

- «IEEE Standard 802.11i Amendment 6: MAC Security Enhancements.» s.d. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf.

- «The State of Wi-Fi Security.» (white paper) s.d. http://www.wi-fi.org/knowledge-center/white-papers/state-wi-fi%C2%AE-security-wi-fi-certified%E2%84%A2-wpa2%E2%84%A2-delivers-advanced.