

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

CORSO DI LAUREA IN SCIENZE DI INTERNET

SISTEMI E RETI WIRELESS

PROF. LUCIANO BONONI

SEMINARIO

RETI VEICOLARI

- STANDARD

IEEE 1609.4

Marilena Mordenti

Matr. 0000353069

INDICE

Introduzione	3
1. Mobile Ad-Hoc Network	3
2. Vehicular Ad-Hoc Network	4
2.1. Dispositivi	4
2.2. Applicazioni	6
3. Dedicated Short Range Communication	7
4. Standard Wireless Access in Vehicular Environments	9
4.1. IEEE Std 802.11p	12
4.1.1. Sottolivello MAC	13
4.1.2. Basic Service Set	13
4.1.3. Wildcard BSSID e WAVE BSS	15
4.1.4. Livello PHY	15
4.2. IEEE Std 1609.1	19
4.3. IEEE Std 1609.2	20
4.4. IEEE Std 1609.3	21
5. IEEE Std 1609.4	23
5.1. Modello di riferimento	23
5.2. Vista sui servizi	24
6. Data Plane services	26
6.1. Channel coordination	27
6.2. Channel Routing	28
6.3. Priorità utente	31
7. Management plane services	33
7.1. Sincronizzazione multicanale	33
7.1.1. Informazioni di temporizzazione	33
7.1.2. Tolleranza di sincronizzazione	35
7.2. Accesso al canale	36
7.2.1. Accesso alternato	36
7.2.2. Accesso SCH immediato	36
7.2.3. Accesso SCH esteso	36
7.2.4. Rilascio del canale	36
7.3. Vendor Specific Action frames	39
7.4. Altri servizi IEEE 802.11	41
7.5. MIB manutenzione	41
7.6. Reindirizzamento	42
8. Le primitive dello standard IEEE 1609.4	42
CONCLUSIONI	44
BIBLIOGRAFIA	45

Introduzione

In questo elaborato verrà trattata una sottocategoria delle Mobile ad-hoc network (MANET), denominata Vehicular Ad-Hoc Network (VANET). Le reti VANET trovano importante utilizzo in una vasta gamma di applicazioni in ambiente di trasporto, comprese innanzitutto la sicurezza dei veicoli e la gestione del traffico. Si dirà delle frequenze Dedicated Short Range Communication (DSRC) assegnate e degli standard dell'Institute of Electrical and Electronics Engineers (IEEE) denominati Wireless Access in Vehicular Environments (WAVE). La figura sottostante evidenzia, nell'ambito delle attuali tecnologie wireless, la caratterizzazione delle reti veicolari trattate:

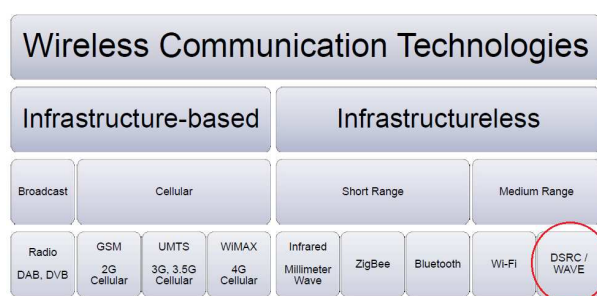


Fig.1 – Tecnologie wireless

Gli standard WAVE sono IEEE 802.11p e la famiglia degli IEEE 1609 che definiscono architettura, modello di comunicazione, struttura di gestione, meccanismi di sicurezza e di accesso al canale per comunicazioni wireless in ambiente veicolare. Tra questi standard sarà trattato in maniera particolare lo standard IEEE 1609.4 che definisce la coordinazione multicanale delle comunicazioni.

1. Mobile Ad-Hoc Network

Le reti mobili ad hoc (MANET) sono costituite da un insieme di terminali in grado di organizzarsi dinamicamente in rete senza alcun contributo da parte di una infrastruttura preesistente. La trasmissione effettuata da un nodo mobile viene ricevuta da tutti i nodi nel suo raggio di trasmissione a causa della diffusione broadcast delle comunicazione wireless. A causa della mobilità degli host, ognuno di essi deve essere dotato di un sistema autonomo e di una funzione di instradamento senza appoggiarsi ad una infrastruttura staticamente stabilita o a una gestione centralizzata. I nodi possono spostarsi arbitrariamente e la comunicazione può essere attivata o disattivata senza avvisare gli altri nodi. Con una rete ad hoc si evitano i costi ed i tempi di installazione associati ad una rete dotata di infrastruttura in quanto può essere facilmente disinstallata o riconfigurata e può presentare grande robustezza grazie alla sua natura distribuita e all'assenza di punti centralizzati che possono andare fuori servizio.

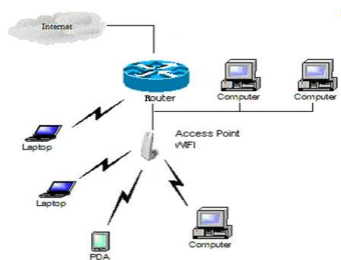


Fig. 2 – Rete wireless basata su infrastruttura



Fig. 3 - Manet: i nodi si collegano dinamicamente senza infrastruttura preesistente

2. Vehicular Ad-Hoc Network

Le Vehicular ad-Hoc network (VANET) sono una sottocategoria delle reti MANET. Si tratta di reti che usano i veicoli come nodi, per creare una rete mobile. Si basano sulla comunicazione cooperativa tra nodi paritetici, senza la necessità di infrastrutture di rete preesistenti e formano configurazioni dinamiche (ad-hoc). I nodi veicolari, attraverso l'uso di sistemi di posizionamento, come il GPS (sistema di posizionamento e navigazione satellitare) e l'uso di mappe dettagliate, possono disporre di una buona conoscenza del territorio circostante. Inoltre i movimenti dei veicoli sono strutturati e vincolati dalla rete viaria. Obiettivi primari sono lo sviluppo di applicazioni distribuite per incrementare la sicurezza ed il comfort di viaggio. Ogni veicolo può trasmettere, ricevere ed inoltrare messaggi, come avvisi di incidente, allarmi stradali e informazioni sul traffico ad altri veicoli o anche a base-station fisse. Le VANET si differenziano dalle MANET principalmente per la velocità di spostamento dei nodi, che generano continuamente diversi scenari e per il rapido mutamento della topologia delle reti. Le reti veicolari inoltre consentono un maggiore impiego di risorse hardware rispetto alla MANET infatti i dispositivi sono alimentati tramite la batteria della vettura, in questo modo la priorità può essere focalizzata sulle performance e non sul consumo energetico, inoltre consentono di immagazzinare i dati in dispositivi di massa sia lato client sia su un eventuale server a cui inviare informazioni.

2.1. Dispositivi

Un sistema di comunicazioni interveicolare è tipicamente caratterizzato da dispositivi montati in ogni veicolo e dispositivi presenti lungo le strade. Le Road Side Unit (RSU) sono di solito installate in pali della luce, semafori, segnaletica stradale, e così via. Le On Board Unit (OBU) sono invece montate nei veicoli e possono funzionare in movimento.

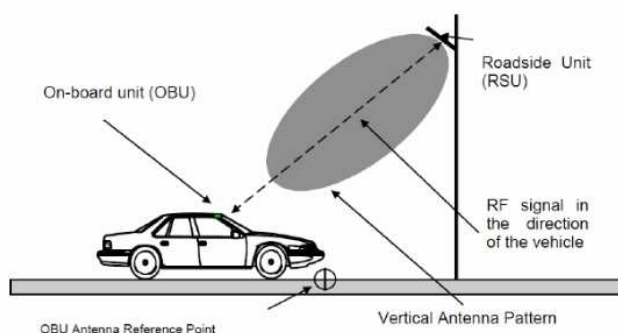


Fig. 4 - On Board Unit (OBU) e Road Side Unit (RSU)

Nella figura sono mostrate le On Board Unit (OBU) cioè i dispositivi montati sui veicoli che sono responsabili delle comunicazioni che avvengono tra due o più veicoli (Vehicle-to-Vehicle communication [V2V]) e delle comunicazioni tra il veicolo e le stazioni radio ai lati della strada (Vehicle-to-Infrastructure communication [V2I] o Vehicle-to-Road Side Unit [V2R]).

Le funzioni di un dispositivo OBU sono:

- fornire una connessione wireless
- eseguire il routing ad hoc geografico
- controllare la congestione della rete
- trasferire in maniera affidabile e sicura i messaggi
- supportare la mobilità per il protocollo IP

Le stazioni radio poste lungo le strade sono chiamate Road Side Unit (RSU) e possono essere installate in una qualsiasi utile collocazione (es. edifici, semafori ...). Sono dotate di un dispositivo di rete per supportare comunicazioni con gli OBU e con altri dispositivi per la comunicazione con altre infrastrutture di rete.

Le principali funzioni di un RSU sono:

- estendere la rete ad hoc tra veicoli inoltrando i dati ad altri veicoli che sopraggiungono
- inoltrare informazioni di sicurezza a tutti i veicoli nel range di copertura
- cooperare con le altre stazioni RSU per scambio di informazioni di sicurezza.
- fornire connettività internet alle OBU.

Nella figura successiva sono evidenziate le tipologie di comunicazione tipiche di una rete Vanet.

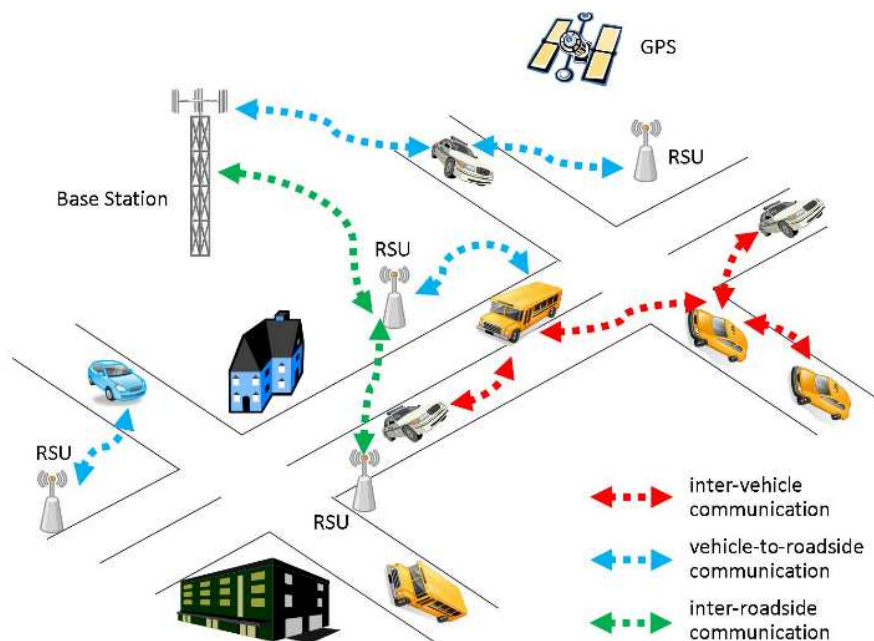


Fig. 5 - Vehicular Ad Hoc Networks

2.2. Applicazioni

La funzione principale delle reti veicolari è lo sviluppo di applicazioni distribuite e pubbliche orientate alla sicurezza stradale e al miglioramento delle condizioni del traffico. La figura sottostante mostra un tipico esempio di utilizzo delle comunicazioni veicolari in caso di incidente.

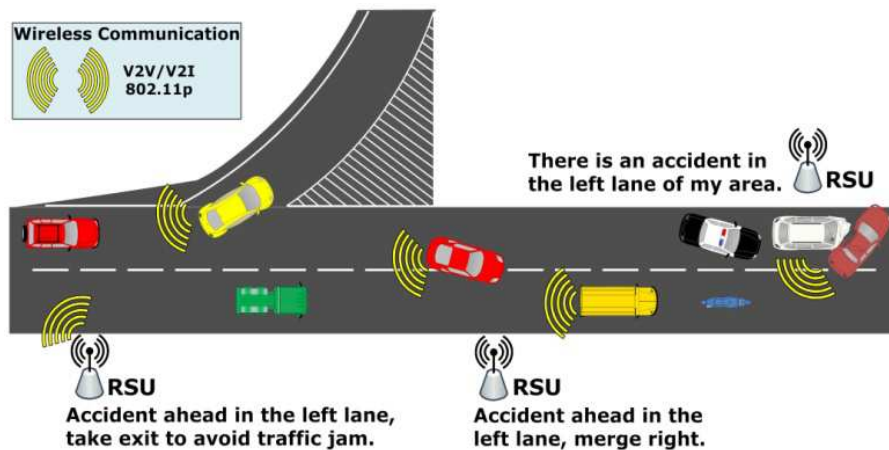


Fig. 6 - Vehicular Ad Hoc Networks: segnalazione di incidente ai veicoli vicini

Queste alcune delle materie di interesse per l'impiego delle comunicazioni veicolari:

- Sicurezza stradale: i veicoli che scoprono un pericolo imminente come un ostacolo ne possono informare gli altri. I sensori elettronici di ogni vettura sono in grado di rilevare cambiamenti improvvisi del percorso o della velocità e inviare un messaggio appropriato ai vicini. Nei sistemi più avanzati, è possibile che il sistema possa decidere quale veicolo ha il diritto di passare prima e segnalarlo a tutti gli altri.
- Gestione del traffico: utile alle autorità per gestire il flusso del traffico e fornire una risposta in tempo reale alle congestioni. Le autorità titolate alla regolamentazione della viabilità possono cambiare le regole del traffico in base ad una situazione specifica e gestire ad esempio limiti di velocità variabile, semafori adattabili, segnalazioni per passaggio ambulanze, etc....
- Assistenza alla guida: le roadside units possono fornire agli automobilisti informazioni che li supportino nel controllo del veicolo. Anche in assenza di roadside units, i veicoli stessi possono essere in grado di emettere avvertimenti come l'altezza di un ponte o di un tunnel.
- Operazioni di polizia: le forze dell'ordine possono usare le comunicazioni veicolari in diversi modi come sorveglianza stradale o avvertenze per limiti di velocità.
- Pagamenti elettronici, al fine di evitare congestioni causate da code per pagamento pedaggi oppure parcheggi con variazione dei prezzi per i giorni feriali, nei weekend e nelle ore di punta.
- Direzione e ottimizzazione dei percorsi: per raggiungere una destinazione vi sono di solito molti percorsi alternativi. Con un sistema di raccolta informazioni rilevanti si possono trovare i migliori percorsi in termini di tempo di viaggio, costo (dei pedaggio o del carburante).

- Informazioni di viaggio: in una città sconosciuta i conducenti di veicoli possono essere aiutati a trovare informazioni rilevanti sui servizi disponibili con mappe e indicazioni ad esempio sull'allocazione delle postazioni di rifornimento carburante.
- Autostrade automatizzate: non ancora realizzabili, ma è comunque un'applicazione interessante. In teoria nelle strade le auto sarebbero in grado di viaggiare senza l'aiuto dei loro conducenti attraverso la cooperazione tra veicoli. Ad esempio, ciascun veicolo conosce la velocità e la direzione di marcia dei veicoli vicini attraverso una comunicazione con loro. Lo stato viene aggiornato frequentemente, quindi ogni veicolo è in grado di prevedere il futuro in merito al tempo necessario ed è in grado di prendere decisioni appropriate in momento opportuno. Poiché autostrade automatiche non sono limitate dal tempo di risposta umana, ipoteticamente sarebbero possibili velocità molto più elevate.
- Servizi di informazione generale: come molte altre reti di comunicazione, le reti veicolari possono essere utilizzate per ottenere vari contenuti e servizi (anche non direttamente correlati alla viabilità).
- Infine, nel caso in cui i nodi veicolari siano collegati ad Internet, virtualmente ogni applicazione che viene attualmente utilizzata in Internet troverà il suo impiego in ambienti veicolari.

3. Dedicated Short Range Communication

Già nel 1991 il congresso degli Stati Uniti d'America promosse un programma chiamato Intelligent Vehicle Highway Systems (IVHS), in materia di sviluppo di ITS (Intelligent Transportation System) i cui obiettivi principali erano quelli di aumentare la sicurezza stradale, evitare le congestioni del traffico e ridurre l'inquinamento. Venne intuito che le comunicazioni wireless erano il fondamento su cui si potevano basare la maggior parte dei servizi ITS. All'epoca, le poche applicazioni esistenti, come ad esempio il pagamento automatizzato dei pedaggi (Telepass), utilizzavano uno spettro tra 902MHz e 928MHz ma purtroppo questa porzione di spettro era troppo stretta e affollata per poterla sfruttare con nuovi servizi ITS.

Di conseguenza, nel 1997, i vari enti interessati allo sviluppo presentarono una petizione alla Federal Communication Commission (FCC), l'autorità amministrativa indipendente incaricata di tutti gli usi dello spettro radio negli USA, per ottenere 75MHz di banda allocati attorno ai 5.9GHz con l'obiettivo di utilizzare questo spettro per le comunicazioni ITS.

Nel 1999 la FCC ha riservato sette canali da 10 Mhz nella banda dei 5.9 Ghz (5.855-5.925) denominata DSRC (Dedicated Short Range Communication) ad uso esclusivo delle comunicazioni veicolari.

Il 17 dicembre 2003 la Commissione ha adottato una relazione d'ordine che stabilisce norme di licenza e di servizio per DSRC nella banda 5,850-5,925 GHz (5.9 GHz). Il servizio prevede l'utilizzo della banda DSRC per comunicazioni V2V (interveicolari) e V2I (veicolo – infrastruttura) contribuendo a proteggere la sicurezza dei passeggeri. L'uso della banda è altresì concesso a soggetti non pubblici per comunicazioni DSRC commerciali o private.

Lo spettro di 75 MHz nella banda ITS 5.9 GHz è diviso in sette canali da 10MHz l'uno, come mostrato nella Fig. 7, distinti in canali di servizio denominati Service Channel (SCH) e un canale, il 178, denominato Control Channel (CCH) riservato esclusivamente alle comunicazioni di sicurezza.

Caratterizzazione dei Control Channels (CCHs):

- Messaggi broadcast
- Frame di dimensioni ridotte e di alta priorità
- Comunicazioni critiche con basse latenze
- Inizializzazione di comunicazione bidirezionale su canali SCH
- Parametri del canale con valori fissati a priori

Circa il Service Channel (SCH):

- Comunicazione bidirezionale tra RSU e OBU o tra gli OBU
- Per applicazioni specifiche, per es pedaggi, accessi ad Internet
- Diverse applicazioni possono essere eseguite in parallelo su più canali di servizio differenti
- Richiede l'esistenza di un Basic Service Set Wave (WBSS - "Ad-hoc group", descritto più avanti in questo elaborato) prima dell'utilizzo del SCH
- I parametri del canale possono essere modificati.

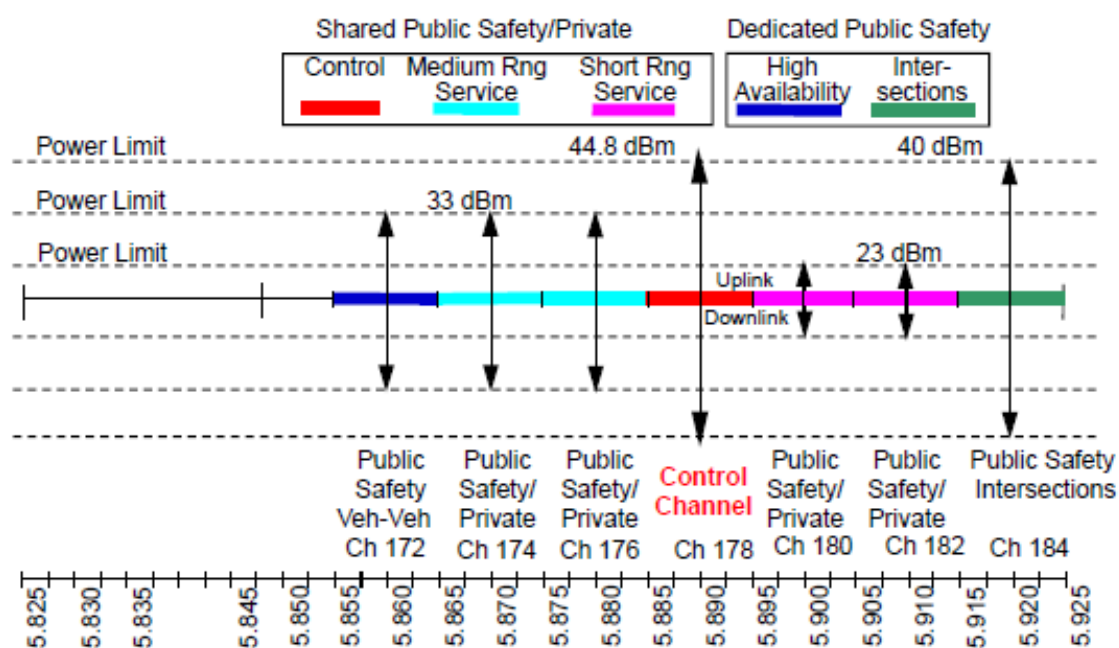


Fig. 7 - Spettro della banda DSRC da 5,9 GHz negli Stati Uniti

Per quanto riguarda la situazione europea, nel 2008 l'Electronic Communications Committee (ECC) ha assegnato (ECC/DEC/(08)01) una parte della banda 5,9 GHz per le infrastrutture di comunicazione per le applicazioni stradali prioritarie di sicurezza e interveicoli.

L'intenzione è che la compatibilità con gli Stati Uniti sarà garantita anche se l'assegnazione non è esattamente la stessa, le frequenze saranno sufficientemente vicino da consentire l'utilizzo della stessa antenna e trasmettitore / ricevitore: sono stati riservati cinque canali da 10 Mhz nella stessa banda (5.875-5.925 Ghz). ECC emette quindi una raccomandazione (ECC/REC/(08)01) che designa le frequenze da 5.855 a 5.875 Ghz per applicazioni non di sicurezza nell'ambito degli ITS. La massima potenza irradiata è limitata a 23 dBm/MHz, ed in totale non deve eccedere i 33 dBm.

non-safety		Road Safety and traffic efficiency	Control Channel	Critical road safety	Route safety and traffic efficiency	
CH172	CH174	CH176	CH178	CH180	CH182	CH184
5.86	5.87	5.88	5.89	5.90	5.91	5.92 (GHz)
Raccomandata		Banda designata per ITS			Estensione futura	

Fig. 8 - Spettro della banda DSRC da 5,9 GHz in Europa

4. Standard Wireless Access in Vehicular Environments

Le comunicazioni wireless in ambienti veicolari hanno necessità di collegare tra loro:

- Roadside units distanti fino a 1000 metri l'uno dall'altro
- Roadside units e veicoli (V2I) che si muovono a velocità variabili
- Veicoli e veicoli (V2V) che si muovono a velocità elevate (fino a 140 km / h)

Si richiedono quindi requisiti specifici nei sistemi di comunicazione wireless. La necessità di utilizzare applicazioni in materia di sicurezza non può tollerare ritardi nell'abilitazione alla comunicazione con altri veicoli incontrati sulla strada. Allo stesso modo, anche le applicazioni non di sicurezza stradale richiedono l'installazione di efficienti collegamenti con le roadside unit per la fornitura di servizi a causa del tempo limitato in cui il veicolo potrebbe restare nell'area di copertura data la rapidità di movimenti e le situazioni ambientali sempre diverse.

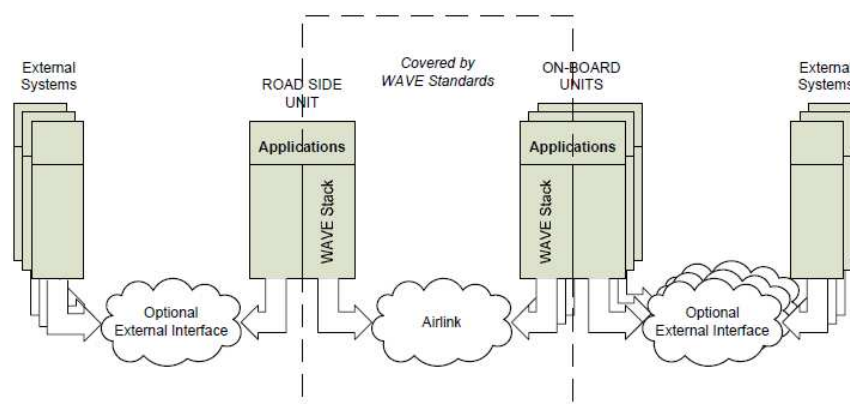


Fig. 9 – L'area trattata degli standard WAVE

Data la particolarità di tale comunicazione, si valutò definire uno standard innanzitutto per quanto riguardava il livello fisico (PHY) e il livello MAC.

Negli Stati Uniti, lo sforzo iniziale fu un progetto mirato alla standardizzazione della tecnologia radio DSRC nel gruppo di lavoro 2313 dell'ASTM (American Section of the International Association for Testing Materials). Nel 2004 un gruppo di ricercatori di IEEE prese in mano il progetto iniziato e cominciò a sviluppare una versione dello standard 802.11 contenente specifiche sulle applicazioni veicolari: il documento è conosciuto come 802.11p.

Un altro gruppo di ricercatori IEEE, conosciuto come gruppo 1609, si impegnò a sviluppare le specifiche per completare anche gli altri livelli della pila protocollare.

Nel complesso i protocolli IEEE 802.11p e la famiglia degli IEEE 1609, che ricoprono l'ambito delle comunicazioni interveicolari (VANET), sono conosciuti come Wireless Access in Vehicular Environments (WAVE).

Lo stack protocollare ISO/OSI e il modello WAVE si differenziano sotto diversi aspetti:

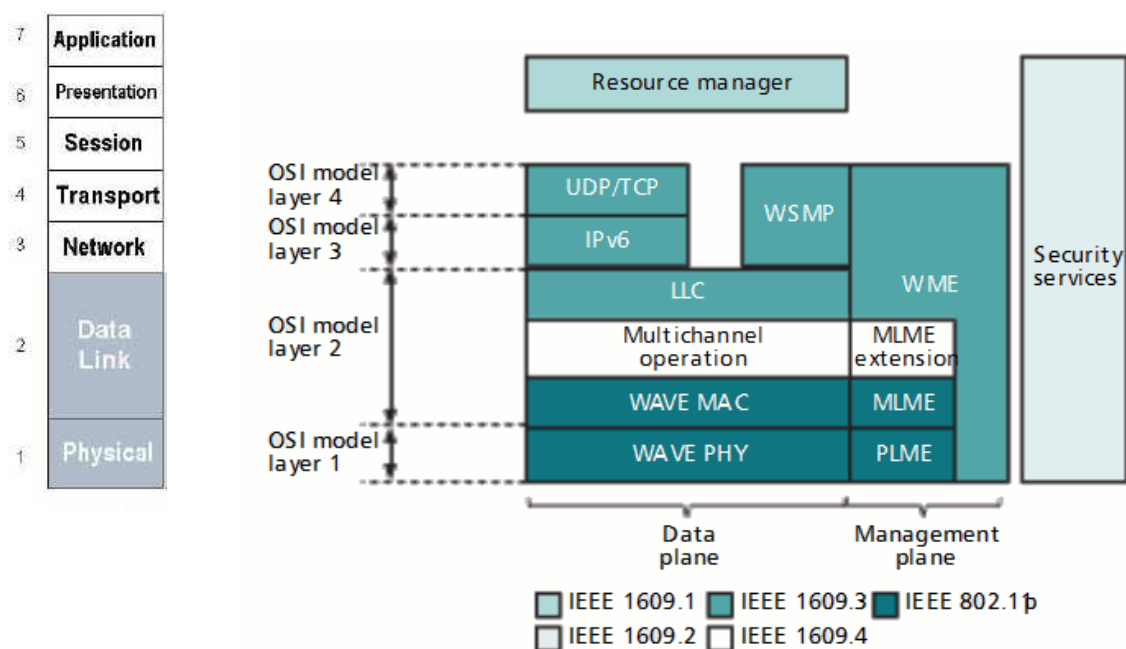


Fig. 10 – Modello ISO/OSI e Modello WAVE

Innanzitutto il modello WAVE non specifica i layers sessione, presentazione e gli strati applicativi, tuttavia introduce il blocco Resource Manager e Security Services.

A livello rete sono supportati Internet Protocol ver. 6 (IPv6) e Wave Short-Message Protocol (WSMP). La ragione della presenza di due protocolli deriva dalla necessità di far fronte a diverse esigenze: da un lato gli scambi ad alta priorità e le comunicazioni time-sensitive e dall'altro transazioni meno esigenti per applicazioni che utilizzano Transmission Control Protocol (TCP) o User Datagram Protocol (UDP). WSMP consente di inviare piccoli messaggi e controllare direttamente alcuni parametri della risorsa radio per massimizzare la probabilità che tutte le parti

coinvolte riceveranno i messaggi in tempo. Tuttavia WSMP non è sufficiente per supportare le applicazioni tipiche di Internet, comunque necessarie per attrarre gli investimenti privati tali da contribuire a diffondere tale tecnologia e ridurre il costo di implementazione dei sistemi: di qui l'inclusione di IPv6.

WAVE si basa sullo standard IEEE 802.11, che specifica il primo e parte del secondo layer dello stack protocollare, tuttavia, come detto, l'ambiente di elevata mobilità ha portato alla creazione dello standard IEEE 802.11p. Questo standard specifica non solo la trasmissione di dati, ma anche le funzioni di gestione associate al livello corrispondente: il Physical Layer Management Entity (PLME) e il MAC layer management entity (MLME).

Lo stack protocollare WAVE comprende un substrato a livello due della pila OSI, dedicato al controllo delle operazioni multicanale. Questo sottolivello, comprese le funzioni di gestione associate, è specificato in IEEE 1609.4. La parte restante del livello due OSI (Logical Link Control [LLC]) segue lo standard IEEE 802.2.

A livello degli strati OSI tre e quattro, IEEE 1609.3 specifica WSMP e spiega come integrare IPv6, UDP e TCP nel sistema. Inoltre IEEE 1609.3 definisce una serie di funzioni di gestione definite Wave Management Entity che devono essere utilizzate per fornire i servizi di rete.

I restanti due blocchi: resource manager e security services non si adattano facilmente alla struttura a strati del modello OSI. Essi sono rispettivamente trattati in IEEE 1609.1 e IEEE 1609.2.

La tabella sottostante riporta i protocolli e gli standard specifici per le comunicazioni Wave.

Protocols	Standard document	Purpose of the standard	OSI model layer numbers
WAVE PHY and MAC	IEEE 802.11p	Specifies the PHY and MAC functions required of an IEEE 802.11 device to work in the rapidly varying vehicular environment	1 and 2
Multichannel operation	IEEE 1601.4	Provides enhancements to the IEEE 802.11p MAC to support multichannel operation	2
WAVE networking services	IEEE 1609.3	Provides addressing and routing services within a WAVE system	2, 3, and 4
WAVE resource manager	IEEE 1609.1	Describes an application that allows the interaction of OBUs with limited computing resources and complex processes running outside the OBUs in order to give the impression that the processes are running in the OBUs	N/A
WAVE security services	IEEE 1609.2	Covers the format of secure messages and their processing	N/A

Fig.11 – Panoramica degli standard WAVE

Oltre a quelli mostrati, da ricordare anche IEEE Std 1609.11™-2010 (Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems [ITS]) che definisce i servizi e formati per i messaggi sicuri necessari per supportare il servizio di pagamenti elettronici.

Nei prossimi paragrafi si parlerà degli standard IEEE 802.11p, 1609.1-2-3 e si tratterà poi in maniera specifica IEEE 1609.4.

4.1. Standard IEEE 802.11p — Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications — Wireless Access in Vehicular Environments

Lo standard IEEE 802.11p per reti wireless in ambienti veicolari definisce le funzioni e i servizi delle stazioni WAVE e le tecniche del segnale e le interfacce tra il livello fisico e MAC.

L'immagine sottostante mostra una panoramica della famiglia 802 nell'ambito del modello (OSI).

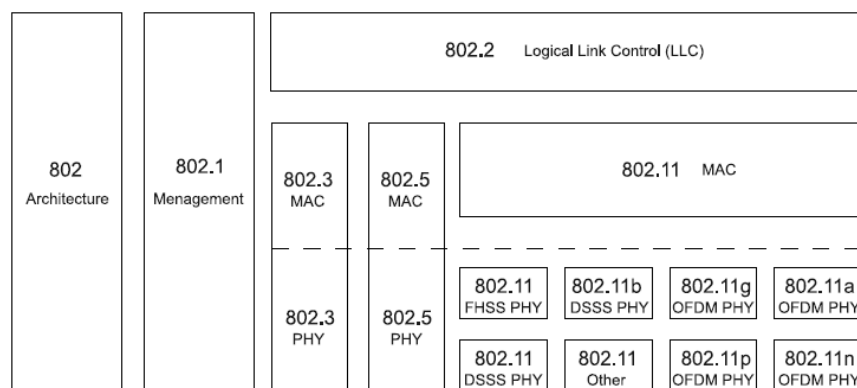
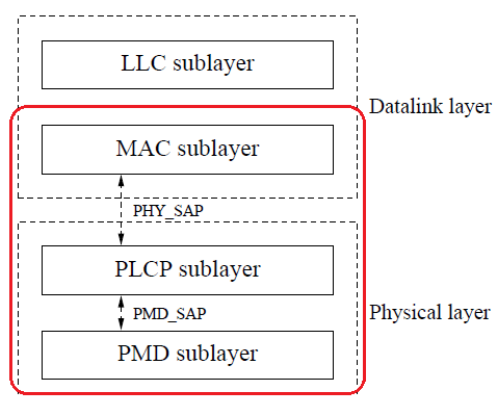


Fig.12 – Gli standard della famiglia 802

L'emendamento 802.11p è stato definito per gestire:

- lunghe distanze tra i dispositivi (fino a 1000 m)
- l'elevata velocità dei veicoli
- l'ambiente multipath estremo (che può provocare problemi di riflessione del segnale con ritardi prolungati);
- la necessità di gestire molteplici sovrapposizioni di reti ad-hoc, mantenendo elevato il livello di qualità del servizio;
- la natura e la particolarità delle applicazioni veicolari che devono essere supportate.



MAC: Medium Access Control - controllo di accesso al mezzo (banda occupata dalla trasmissione)

Strato fisico: Immediatamente sotto allo strato MAC e diviso in due substrati:

- PLCP: physical layer convergence procedure (sincronizzazione)
- PMD: physical medium dependent (è il vero e proprio canale)

Fig.13 – In evidenza i sottolivelli trattati da IEEE 802.11p.

IEEE 802.11p definisce i requisiti del sottolivello MAC e del livello fisico e si basa su:

- IEEE 802.11a PHY: modulazione OFDM
- IEEE 802.11 MAC: CSMA/CA
- IEEE 802.11e MAC: gestione della qualità del servizio.

4.1.1. Sottolivello MAC

802.11 MAC si occupa dell'organizzazione delle comunicazioni al fine di stabilire e mantenere un gruppo cooperativo chiamato Basic Service Set (BSS). Le postazioni possono liberamente comunicare tra loro all'interno del gruppo, ma tutte le trasmissioni provenienti dall'esterno vengono filtrate. Lo scopo principale dell'emendamento IEEE 802.11p a livello MAC è quello di consentire la creazione di un gruppo di comunicazione senza gran parte dell'overhead tipicamente necessario in IEEE 802.11. In altre parole, il focus è sulla semplificazione delle operazioni di BSS in maniera veramente ad hoc per l'utilizzo veicolare.

4.1.2. Basic Service Set

Il MAC 802.11 supporta due diversi framework: a infrastruttura e "Ad-hoc". Un'infrastruttura Basic Service Set (BSS) è un gruppo di stazioni IEEE 802.11 collegate ad un Access Point (AP) e configurate per comunicare con altre stazioni con collegamenti wireless. Il meccanismo di BSS controlla l'accesso alle risorse e ai servizi dell'AP e consente inoltre di filtrare le trasmissioni radio provenienti da sorgenti estranee nelle vicinanze. Una stazione wireless ascolta prima il beacon da un AP e poi si unisce al BSS attraverso una serie di passaggi interattivi, inclusi autenticazione e associazione.

La modalità operativa ad-hoc (chiamata anche *peer-to-peer mode*), definita sempre nell'abito di IEEE 802.11, consente alle stazioni di formare un Independent Basic Service Set (IBSS): una stazione wireless si assume le responsabilità di un AP; tali responsabilità includono l'esecuzione periodica del processo di beaconing e l'autenticazione di nuovi membri.

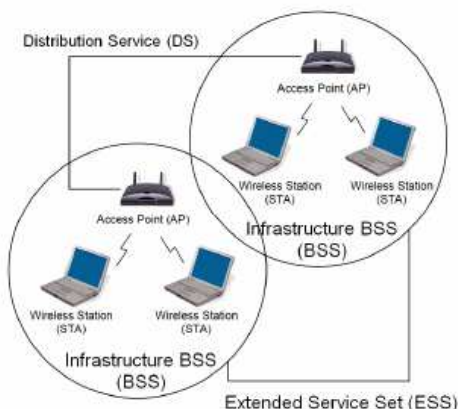


Fig. 14 - IEEE 802.11: Basic service set

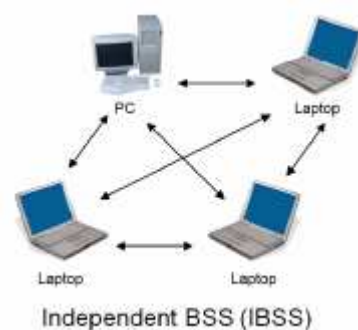


Fig. 15 - IEEE 802.11: ad hoc network

Un BSS è noto agli utenti attraverso l'individuazione del SSID (Service Set Identifier) che corrisponde al nome dell'AP al quale è possibile connettersi. Il livello MAC di una stazione, al ricevimento di un frame dal PHY, utilizza il contenuto dei campi Address per eseguire il matching dell'indirizzo. Se il campo contiene un gruppo di indirizzi (per esempio, un indirizzo broadcast), il BSSID viene confrontato per garantire che il broadcast o il multicast originato da una stazione sia nello stesso BSS.

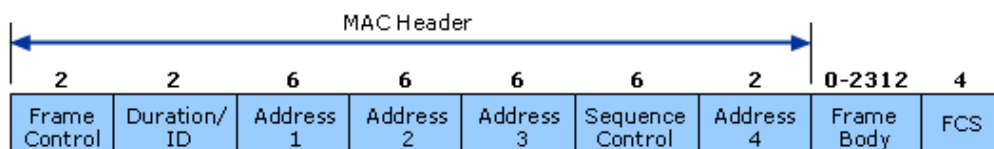


Fig. 16- 802.11 MAC Frame Format

Ogni data frame IEEE 802.11 include 4 campi indirizzo, a seconda del tipo di frame, i campi indirizzo potranno contenere una combinazione dei seguenti tipi di indirizzi:

- Basic Service Set Identifier (BSSID) - identifica in modo univoco ogni BSS. Quando il frame proviene da una stazione in infrastruttura BSS, il BSSID è l'indirizzo MAC del punto di accesso. Quando il frame proviene da una stazione in una IBSS, il BSSID è generato in modo casuale dalla stazione che ha avviato il IBSS.
- Destination Address (DA) - indica l'indirizzo MAC della destinazione finale del frame.
- Source Address (SA) - indica l'indirizzo MAC del sorgente originale che ha inizialmente creato e trasmesso il frame.
- Receiver Address (RA) - indica l'indirizzo MAC della stazione immediatamente successiva per la ricezione del frame.
- Transmitter Address (TA) - indica l'indirizzo MAC della stazione che ha trasmesso il frame sul supporto wireless.

Il campo Frame Control, mostrato nella figura seguente, contiene informazioni di controllo utilizzate per definire il tipo di frame 802.11 MAC e fornire le informazioni necessarie per capire come elaborare il frame MAC.

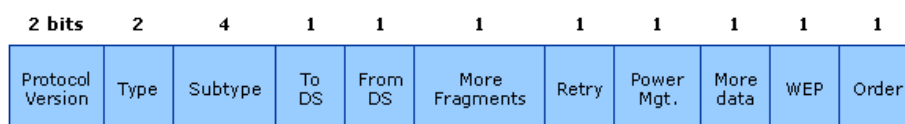


Fig. 17 - 802.11 MAC Header Frame Format

I sottocampi del Frame Control:

- Protocol Version - fornisce la versione corrente del protocollo 802.11 utilizzato. Le stazioni riceventi utilizzano questo valore per sapere se la versione del protocollo è supportato.
- Type and Subtype - determinano la funzione del frame. Ci sono tre diversi tipi di frame: control, data e management. Ogni sottotipo determina la specifica funzione di svolgere per il suo associato tipo di frame.
- To DS e From DS - indicano se il frame sta per uscire dal DS (sistema distribuito), e viene usato solo in frame di dati di stazioni associate con un AP.
- More Fragments - indica se ci sono ulteriori frammenti successivi di quel frame.
- Retry - indica se il frame è stato ritrasmesso.
- Power Management - indica se la stazione trasmittente è in modalità attiva o modalità di risparmio energetico.
- More Data - indica ad una stazione in modalità di risparmio energetico che l'AP ha più frames da inviare. E' anche usato per gli AP per indicare che seguirà la trasmissione di frames supplementari.
- WEP - indica se la crittografia e autenticazione vengono utilizzati o meno nel frame.
- Order - indica che tutti i data frame ricevuti devono essere elaborati in ordine.

4.1.3. Wildcard BSSID e WAVE BSS

Le attività di IEEE 802.11 MAC, come sopra descritto, sono troppo dispendiose in termini di tempo per essere adottate nell'approccio WAVE in quanto le comunicazioni veicolari di sicurezza richiedono capacità di scambio veloce di dati e non è possibile effettuare scansione dei canali per reperire il beacon di un BSS e, successivamente, l'esecuzione di handshakes multipli per stabilire le comunicazioni. Si pensi, ad esempio, ad uno scenario in cui un veicolo incontra un altro veicolo sulla strada proveniente dalla direzione opposta: a seconda della dinamica dei veicoli, il tempo disponibile per le comunicazioni può essere estremamente breve. Pertanto, è essenziale, per tutte le comunicazioni IEEE 802.11p, essere per default nello stesso canale e configurato con lo stesso BSSID per consentire le comunicazioni di sicurezza.

Un emendamento fondamentale introdotto da IEEE 802.11p è il termine "modalità WAVE". Ogni stazione WAVE è autorizzata a trasmettere e ricevere data frame con il *wildcard BSSID* e senza la necessità di appartenere, a priori, ad una BSS di qualsiasi tipo. Ciò significa che due veicoli possono immediatamente comunicare tra loro quando si incontrano senza overhead aggiuntivo perché operano nello stesso canale utilizzando il *wildcard BSSID*.

Anche per le comunicazioni e i servizi non di sicurezza, l'overhead della tradizionale impostazione BSS possono essere troppo costosi. Un veicolo si avvicina ad una road site unit che offre, ad esempio un servizio di download di mappe digitali, non è possibile attendere i tanti secondi che sono in genere necessari in una configurazione convenzionale ad connessione WiFi, perché il tempo totale in cui questo veicolo resta nell'area di copertura potrebbe essere molto breve.

Lo standard WAVE introduce un nuovo tipo di BSS: WBSS (WAVE BSS). Una stazione forma una WBSS innanzitutto trasmettendo un beacon di richiesta. La richiesta parte dagli stati protocollari superiori e contiene tutte le informazioni necessarie alle stazioni riceventi per capire il tipo di servizio offerto dalla WBSS così da poter decidere se aderire o meno ed inoltre contiene anche tutte le informazioni necessarie per autoconfigurarsi come stazione appartenente alla WBSS. Questo approccio offre overhead estremamente ridotti per la creazione di una rete tra veicoli evitando processi di associazione e autenticazione. Inoltre se una stazione si è già configurata per appartenere ad una WBSS può ancora ricevere frames da altre stazioni con il wildcard BSSID.

Il livello MAC di 802.11p ha queste caratteristiche fondamentali:

- Non sono eseguite scansioni alla ricerca di Access Point.
- Non si effettuano associazione e autenticazione delle stazioni.
- Qualunque stazione in WAVE mode può comunicare con qualunque altra sintonizzata sul suo stesso canale, indicando un wildcard BSSID con i campi "To DS" e "From DS" impostati a 0, questo permette lo scambio diretto di informazioni di sicurezza.
- Un WAVE BSS (WBSS) è un tipo di BSS costituito da un insieme di stazioni cooperanti in modalità WAVE che comunicano utilizzando un BSSID comune. Un WBSS viene inizializzato quando una stazione in modalità WAVE invia un Beacon WAVE, che include tutte le informazioni necessarie ad un ricevente per aderire. Nel Beacon sono indicati i servizi offerti ed un nome BSSID casuale che identifica il WBSS, chi riceve il Beacon può decidere di aderire al WBSS. Anche se una stazione aderisce ad un WBSS, può continuare ad usare il BSSID wildcard per segnalare eventi di sicurezza a tutti.
- Una stazione si unisce a una WBSS quando è configurata per inviare e ricevere data frame con il BSSID definito per quel WBSS. Al contrario, esso cessa di appartenere ad un WBSS quando il suo MAC interrompe l'invio e la ricezione di frame che utilizzano il BSSID di quel WBSS.
- Una stazione non può essere membro di più di un WBSS contemporaneamente e non può far parte di un infrastruttura BSS o IBSS.
- Un WBSS cessa di esistere quando non ha membri. La stazione che lo ha avviato non è diversa da qualsiasi altro membro dopo la costituzione di un WBSS. Pertanto, un WBSS può continuare anche se la stazione che lo ha avviato cessa di essere un membro.

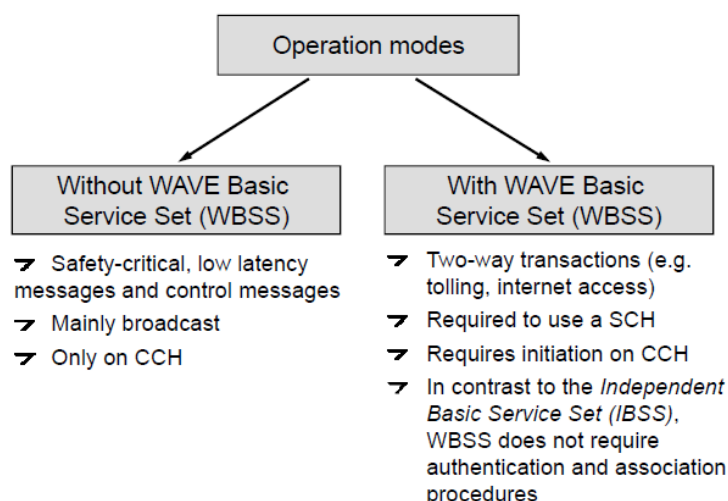


Fig. 18 – Modalità operative di 802.11p MAC

4.1.4. - Livello PHY

Il segnale radio è prodotto dai chipset già sviluppati per realizzare il segnale 802.11a con modulazione Orthogonal Frequency Division Modulation (OFDM) modificandone però alcuni parametri.

La modulazione OFDM è di tipo MCM (Multi Carrier Modulation) in quanto flussi di dati ad alto bit rate vengono modulati separatamente su un insieme di carrier multipli, in questo modo si ottiene un valore di bit rate aggregato, somma di tutti i bit codificati su tutti i carrier. L'utilizzo di carrier multipli, ognuno dei quali a banda stretta (narrow band), permettono di ridurre il symbol rate su ognuno dei carrier, senza ridurre (globalmente) il bit rate trasportato. Il vantaggio derivato dal symbol rate più basso, è la possibilità di separare (temporalmente) un simbolo dall'altro, avendo a disposizione più tempo per separarli e più tempo per elaborarli, dando più accuratezza al tentativo di interpretazione che viene fatto a scapito, eventualmente, dell'errore sul canale (maggiore affidabilità della tecnologia di comunicazione che, tendenzialmente, sbaglia meno i simboli e, quindi i bit). Nelle trasmissioni terrestri in generale esistono più percorsi di propagazione possibili per il segnale tra l'antenna trasmittente e quella ricevente. Il percorso più breve è quello diretto, o in visibilità (LOS), ma ne esistono anche molti altri che sono il risultato dei "rimbalzi" delle onde elettromagnetiche su ostacoli riflettenti che circondano l'area di copertura del segnale. Quando si è in queste condizioni si parla di propagazione multicammino (*multipath*) e il risultato è che al ricevitore giungono più copie ritardate nel tempo dello stesso segnale, ognuna con ampiezza e fase diversa rispetto a quella che perviene tramite il cammino diretto. Uno degli obiettivi primari del sistema di modulazione digitale OFDM è proprio quello di poter funzionare bene anche in condizioni di propagazione multicammino.

Caratteristica fondamentale della modulazione OFDM è inoltre l'ortogonalità delle portanti che consente di garantire un'efficienza spettrale comparabile con quella di una trasmissione numerica analogica su portante singola, in quanto consente di sovrapporre parzialmente le bande delle varie

componenti del multiplex, senza avere interferenza tra le portanti: i dati vengono trasmessi in parallelo all'interno di ogni sottoportante, senza necessitare di uno spazio fra l'una e l'altra ma, anzi, permettendo l'overlapping. Mentre le classiche Frequency Division Multiplexing richiedono gli spazi di guardia, in OFDM il segnale ricevuto viene ricostruito anche se le sottoportanti si sovrappongono.

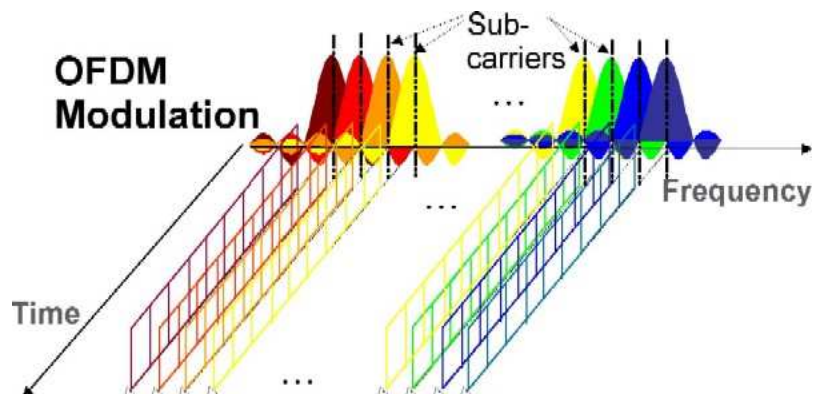


Fig. 19 – Modulazione OFDM

I 75 MHz del canale DSRC sono distinti in sette sottocanali da 10 MHz. Ogni sottoportante è distante dall'altra 156.25 kHz.

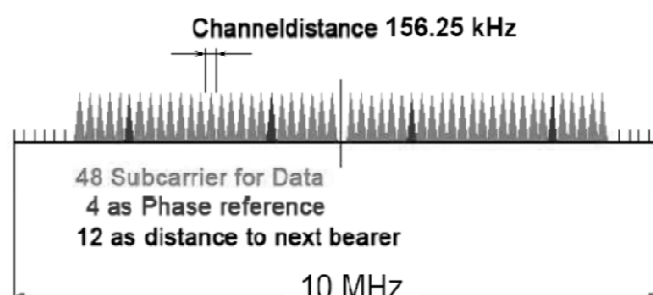


Figura 20 - 10 MHz di un canale DSRC

Nelle sottoportanti possono essere utilizzate diverse tecniche di modulazione come ad esempio le modulazioni QAM (Quadrature Amplitude Modulation) che combinano la modulazione sia dell'ampiezza che della fase del segnale in ogni simbolo trasmesso).

	IEEE 802.11a	IEEE 802.11p	
Data rate	6, 9, 12, 18, 24, 36, 48, 54 Mbps	3, 4.5, 6, 9, 12, 18, 24, 27 Mbps	
Modulation	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM	BPSK OFDM QPSK OFDM 16-QAM OFDM 64-QAM OFDM	Longer guard period → Less Inter-symbol Interference → Better resistance against multipath error
# of subcarriers	52 net	52 net	
OFDM Symbol Duration	4.0 μ s	8.0 μ s	Re-order of sub-carriers → Better multipath mitigation
Guard Period	0.8 μ s	1.6 μ s	
Occupied bandwidth	20 MHz	10 MHz	Dedicated frequency band → Less Co-Channel Interference
Frequency	5 GHz ISM band	5.850-5.925 GHz	

Figura 21 - IEEE 802.11a e 802.11p a confronto

Come evidenziato in Fig. 21, IEEE 802.11p PHY raddoppia le costanti temporali in modo da dimezzare la banda occupata a 10 Mhz e raddoppiare il tempo di guardia tra simboli OFDM, così da evitare l'interferenza intersimbolica dovuta all'aumentata dispersione temporale causata dalla mobilità. La massima potenza irradiata aumenta fino a 2 Watt, con portata fino ad 1 Km. Il livello effettivo può essere variato dagli strati superiori per ogni pacchetto, su di una dinamica di 30 dB.

Occorre notare che mentre IEEE 802.11p descrive come le comunicazioni avvengono su ogni singolo canale dello spettro DSRC, un sistema completo di comunicazione per WAVE deve includere il supporto per le operazioni multi-canale, la sicurezza, e altre operazioni necessarie agli strati protocollari superiori, queste problematiche sono affrontate dagli standard IEEE 1609.

4.2. IEEE Std 1609.1™- 2006 — Wireless Access in Vehicular Environments (WAVE) — Resource Manager

Questo standard definisce i componenti WAVE, le interfacce e le risorse, i formati dei messaggi e di memorizzazione e i dispositivi supportati dagli OBU.

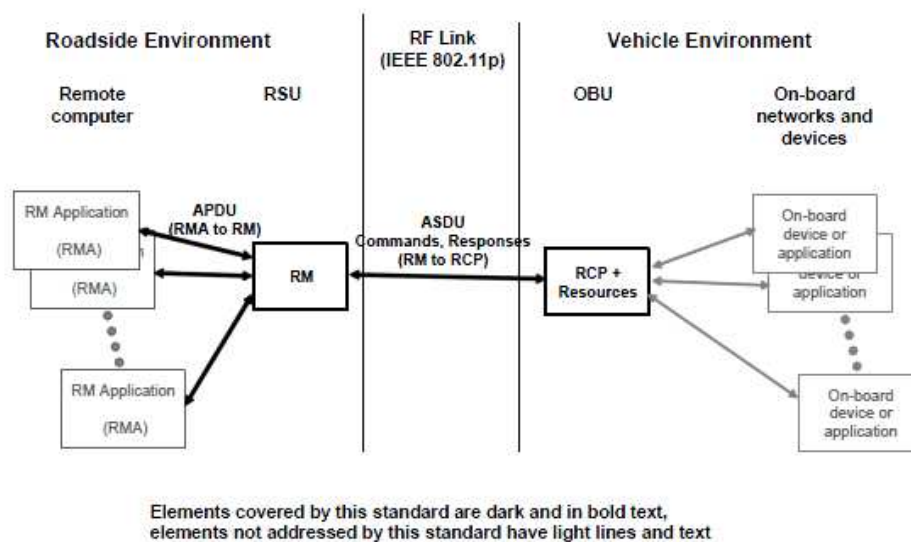


Fig. 22 – std. IEEE 1609.1

Gli OBU possono decidere di utilizzare i servizi forniti da applicazioni installate in unità lontane dalle RSU. Gli OBU ospitano un'applicazione (Command Processor Resource, o RCP), che utilizza il servizio. Terze parti (lontane dalla RSU) ospiteranno altre applicazioni (Resource Manager Application, o RMA) che forniscono i servizi. Le RSU ospitano un'applicazione (Resource Manager, o RM) che funge da middle-man tra gli RCP e gli RMA. Questo standard specifica la RM e la RCP. In particolare descrive come avviene la multiplazione delle richieste RM da molteplici RMA, ciascuno dei quali è in comunicazione con più OBU che ospitano un RCP.

Lo scopo della comunicazione è quello di fornire l'accesso RMA alle "risorse", come memoria, interfacce utente e interfacce ad altre OBU controllate dal RCP, in maniera consistente, interoperabile e puntuale per soddisfare le richieste RMA.

4.3. IEEE Std 1609.2™— 2006 — IEEE Trial-Use Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages

Le applicazioni WAVE possono essere soggette a vincoli di sicurezza elevati a causa della loro vasta gamma di operazioni supportate e della diversità delle esigenze. Da un lato ci sono le applicazioni legate alla sicurezza stradale che sono time-critical, pertanto, l'overhead delle comunicazioni deve essere ridotto al minimo. Dall'altro alcune applicazioni hanno un pubblico potenziale di migliaia di veicoli, di conseguenza i meccanismi utilizzati per autenticare i messaggi devono essere il più flessibili e scalabili possibile. Resta, in ogni caso, fondamentale proteggere i messaggi dalle intercettazioni, sostituzioni, alterazioni e duplicazioni e al contempo fornire, ai proprietari dell'informazione, il diritto alla privacy per evitare perdite dei dati personali, identificazione o recepimento delle informazioni da parte di device non autorizzati.

Nello standard IEEE 1609.2, troviamo i servizi di sicurezza che vengono utilizzati all'interno dello stack protocollare al fine di definire i formati sicuri per la gestione dei messaggi e delle applicazioni consentendo l'elaborazione di tali messaggi protetti.

Sono previsti meccanismi per autenticare i messaggi di gestione WAVE, per autenticare i messaggi che non richiedono l'anonimato, per crittografare i messaggi per un destinatario conosciuto.

I meccanismi previsti, che includono la crittografia con chiave pubblica, sono tali da consentire riservatezza (crittografia di un messaggio per un destinatario specifico evita l'intercettazione o la modifica di un messaggio), autenticità (conferma di provenienza del messaggio) e integrità (la conferma che il messaggio non è stato alterato in transito consente di evitare di ingannare il destinatario ad accettare il contenuto dei messaggi errati).

I meccanismi di crittografia utilizzati, che forniscono la maggior parte di questi requisiti di sicurezza sono gli algoritmi simmetrici (a chiave segreta), gli algoritmi asimmetrici (a chiave pubblica) e funzioni di hash.

Nel sistema WAVE, un provider offre un servizio mediante WAVE Service Announcement (WSA), ed annuncia la disponibilità di un Basic Service Set WAVE (WBSS). Se un utente stabilisce che uno dei servizi offerti è di interesse, si può unire alla WBSS, così da utilizzare il servizio desiderato. I WSA sono formati per proteggere gli utenti contro le potenziali entrate in WBSS non validi, in altre parole dall'evitare di rispondere a WSA che non sono stati inviati da parte dei fornitori validi. WAVE Management Entity (WME) e l'entità sul provider che genera, e sull'utente che processa, il WSA.

4.4. IEEE Std 1609.3™— 2010 — IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services

Nello standard IEEE 1609.3 vengono definite le specifiche per i servizi dei livelli rete e trasporto, inclusi indirizzamento e instradamento, e per funzioni associate alla LLC (Logical Link Control).

Possiamo funzionalmente dividere i servizi di rete in due gruppi:

- Data-plane services, la cui funzione è quella di trasportare il traffico;
- Management-plane services, che si occupano della configurazione e della manutenzione del sistema.

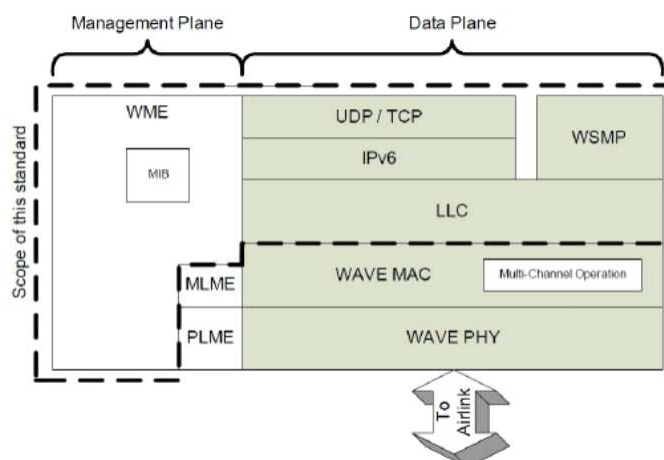


Fig. 23 – Modello di riferimento Std IEEE 1609.3 (l'area tratteggiata è trattata dallo standard)

In merito ai Data plane services, l'architettura WAVE supporta due stack di protocollo: IPv6 e WSMP. Entrambi operano in cima a un singolo strato LLC. Questa configurazione duale serve per ospitare comunicazioni ad alta priorità e time-sensitive, attraverso WSMP (Wave Short-Message Protocol), che consente alle applicazioni di controllare canale e potenza di trasmissione, così come transazioni meno impegnative (tramite UDP/TCP/IP). I dispositivi devono implementare IPv6, come specificato nella RFC 2460, UDP come definito nella RFC 768 e TCP secondo RFC 793.

I produttori sono liberi di implementare altre raccomandazioni Internet Engineering Task Force (IETF), purché non ostacolino l'interoperabilità con altri dispositivi WAVE.

I servizi Management Plane sono noti come Wave Management Entity (WME) e comprendono:

- Application registration: tutte le applicazioni che si aspettano di utilizzare i servizi di rete prima devono necessariamente registrarsi con la WME. Ogni applicazione si registra con un unico provider server identifier (PSID).
- Gestione WBSS: I WME è incaricato di avviare un WBSS per conto di qualsiasi applicazione che fornisce un servizio. Questo può richiedere una o più delle seguenti operazioni:
 - Collegamento stabile

- Aggiunta o la rimozione delle applicazioni dalle WBSS dinamiche
- Inclusione (lato provider) e il recupero (lato utente) di credenziali di sicurezza
- Cessazione WBSS
- Mantenimento dello status di ogni applicazione nel contesto di una particolare WBSS.
- Monitoraggio utilizzo del canale: anche se lo standard non specifica come farlo, definisce che la WME tenga traccia delle modalità di utilizzo di SCH in modo che possa scegliere un canale che ha meno probabilità di essere congestionato quando si deve stabilire una WBSS.
- Configurazione IPv6: questo servizio permette di gestire i collegamenti locali, gli indirizzi globali e multicast IPv6 dell'unità.
- Monitoraggio Received channel power indicator (RCPI): qualsiasi applicazione può interrogare un dispositivo remoto sulla forza del segnale ricevuto. Il WME invia la richiesta corrispondente al nome dell'applicazione. MLME (MAC Sublayer Management Entity) e non WME è l'unità remota che risponde a questa richiesta.
- Mantenimento Management Information Base (MIB): WME mantiene un MIB che contiene le informazioni collegate al sistema e all'applicazione. Le informazioni relative al sistema includono informazioni di rete (router, gateway, Domain Name Service), indirizzi (ad esempio indirizzi MAC locali), e altri valori, come la registrazione delle porte e la lunghezza massima WSM. Le informazioni relative all'applicazione comprendono informazioni sui canali e sul livello di potenza di trasmissione.

5. IEEE Std 1609.4™_2010 — IEEE Standard for Wireless Access in Vehicular Environments (WAVE) — Multi-channel Operation

Scopo di questo standard è curare gli arricchimenti al MAC 802.11 per operare in modalità WAVE, permettendo il coordinamento e la gestione dei diversi canali, inoltre offrire un collegamento logico agli strati protocollari superiori senza preoccuparsi di come avviene lo scambio di informazioni a livello fisico. Un dispositivo WAVE deve disporre di un'architettura in grado di supportare un canale di controllo (CCH) e canali multipli di servizio (CSH). Il coordinamento dei canali è un miglioramento di IEEE 802.11 MAC e interagisce con IEEE 802.2 LLC e IEEE 802.11 PHY.

Lo scopo di questo standard è la definizione delle specifiche funzionali e dei servizi del sottolivello MAC che supportano la connettività multi-canale wireless tra device IEEE 802.11 WAVE .

La finalità consiste nell'attivare efficaci meccanismi che controllano le operazioni di trasferimento dati dei livelli superiori su più canali, senza richiedere la conoscenza dei dettagli del layer fisico, e descrivere le operazioni di routing e switching multi-canale per diversi scenari.

5.1. Modello di riferimento

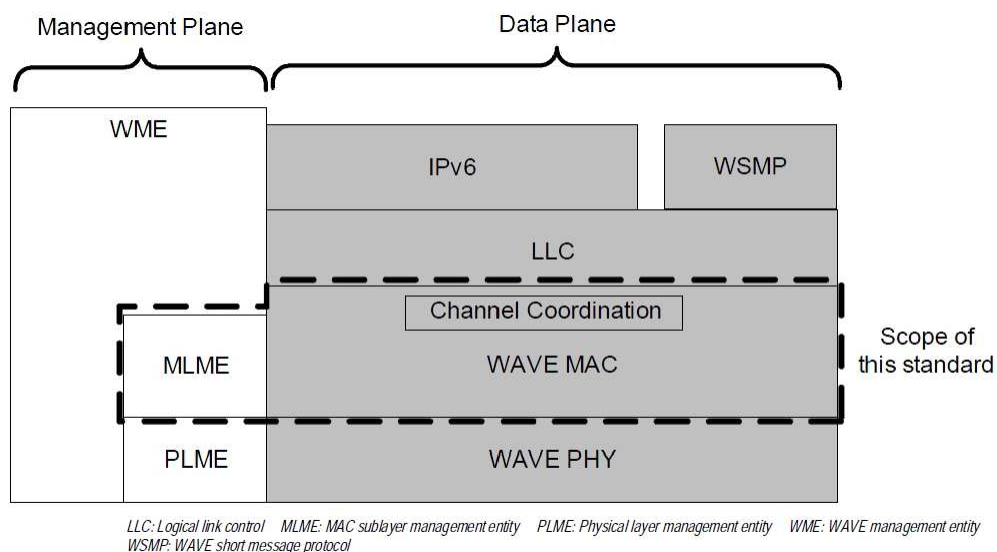


Fig. 24 – Reference model std. IEEE 1609.4

Wave supporta i trasferimenti di dati basati sia su IP che su WSMP (specificato in IEEE Std 1609.3), anche se i singoli dispositivi potrebbero supportare solo uno dei due protocollo di rete. Il coordinamento del canale è un insieme di miglioramenti al IEEE 802.11 MAC e interagisce rispettivamente con lo strato LLC (IEEE 802.2) e il livello fisico (IEEE 802.11p). Wave Management entity (WME) e servizi di rete corrispondenti sono specificati in IEEE 1609.3. I servizi di sicurezza WAVE sono specificati in IEEE 1609.2.

I livelli MAC e PHY concettualmente comprendono due entità di gestione, chiamate rispettivamente MAC Sublayer Management Entity (MLME) e PHY Layer Management Entity (PLME). Queste due

entità forniscono le interfacce per gli altri livelli attraverso le quali le funzioni di gestione possono essere invocate. Le interazioni tra le varie entità avvengono attraverso Service Access Point (SAPs) attraverso i quali vengono scambiate primitive definite.

La figura successiva mostra come, ai fini della descrizione della funzionalità specificate in questo standard, MAC layer management entity (MLME) sia divisa in due parti: le estensioni WAVE MAC management specificate in questo documento e MLME specificato dallo standard IEEE 802.11. Tutte le primitive specificate in questo standard hanno il prefisso MLMEX per agevolare l'identificazione.

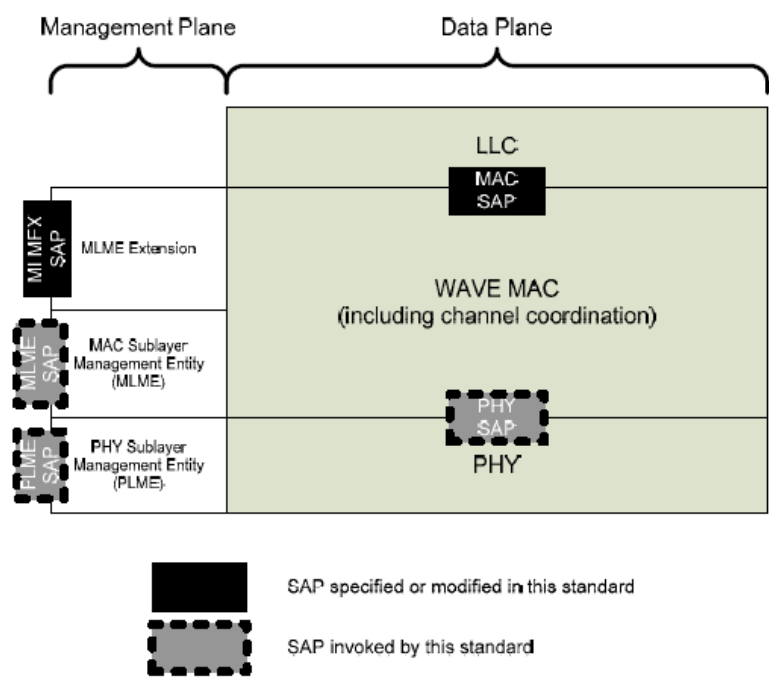


Fig. 25 – Interfacce SAP rilevanti in questo standard

5.2. Vista sui servizi

I servizi forniti da questo standard sono utilizzati per gestire il coordinamento dei canali e per supportare la consegna dei MAC Service data unit (MSDU) e si distinguono in Data Plane services e Management Plane services.

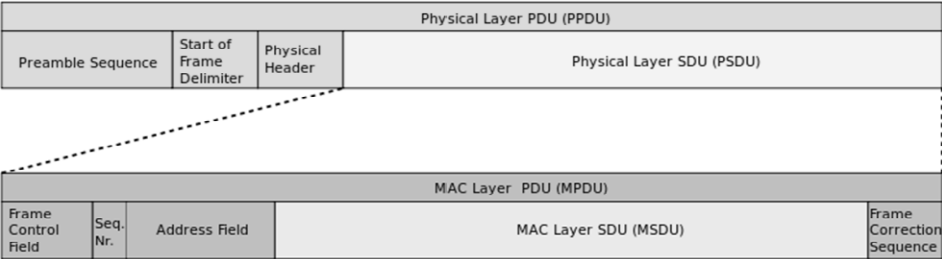


Fig. 26 – MAC Service data unit (MSDU)

DATA PLANE SERVICES:

I servizi forniti da MLME (MAC sublayer management entity) comprendono:

- Coordinazione del canale: il sottolivello MAC coordina gli intervalli del canale in modo che i pacchetti vengano trasmessi sul canale al momento giusto.
- Channel Routing: il sottolivello MAC gestisce in entrata e in uscita i dati di livello superiore. Questa specifica include il routing dei pacchetti dall'LLC (Logica Link Control) al canale designato e il setting di parametri, come ad esempio la potenza, per le trasmissioni WAVE.
- Priorità utente: WAVE supporta una varietà di applicazioni di sicurezza e non di sicurezza con un massimo di otto livelli di priorità come definito nello standard IEEE 802.11. L'utilizzo della priorità utente (UP) delle categorie di accesso collegate (AC) supporta la qualità del servizio utilizzando le funzionalità Enhanced Distributed Channel Access (EDCA) definite in IEEE 802.11.

MANAGEMENT PLANE SERVICES:

I servizi di gestione forniti da MLME comprendono:

- Sincronizzazione multi-canale: MLME utilizza le informazioni derivate localmente e ricevute attraverso l'etere per fornire una funzione di sincronizzazione con l'obiettivo di allineare gli intervalli del canale tra i dispositivi di comunicazione WAVE. MLME consente di generare frames timing advertisement (TA) per distribuire informazioni di temporizzazione e di monitorare i TA frames ricevuti.
- Accesso al canale: MLME controlla l'accesso agli specifici canali radio sulla base delle richieste di comunicazione ricevute da WME.
- Vendor Specific Action frames - MLME accetta in ingresso frame VSA (Vendor Specific Action) e li passa alla WME; MLME genera anche frames VSA per la trasmissione su richiesta della WME.
- Altri servizi IEEE 802.11: MLME consente l'accesso ai servizi IEEE 802.11, che possono essere invocati per un singolo canale.
- Mantenimento MIB: MLME tiene un Management Information Base (MIB) che contiene la configurazione e le informazioni di stato.
- Reindirizzamento - MLME permette di modificare l'indirizzo del dispositivo per gestire pseudonimi.

Nei paragrafi successivi verranno più dettagliatamente trattati i servizi descritti in IEEE 1609.4.

6. Data Plane services

I dispositivi WAVE comunicano al di fuori del contesto di un BSS, come specificato in IEEE 802.11p.

Questo design architetturale di riferimento viene utilizzato per specificare le operazioni di coordinamento del canale, accodamento e attribuzione di priorità ai dati, routing.

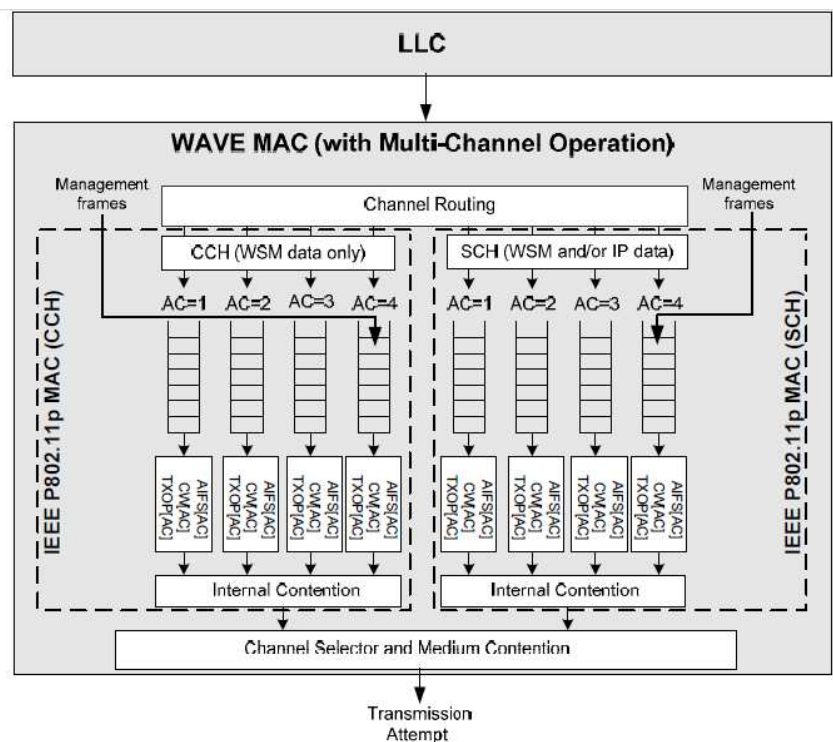


Fig. 27 –Architettura interna del MAC WAVE con coordinamento dell'accesso al canale

Un'entità MAC WAVE utilizza una o più istanze dell'entità sottolivello MAC specificato in IEEE 802.11, come modificata dalla IEEE Std 802.11p, per operare al di fuori del contesto di un basic service set con le estensioni definite in questo standard.

Sono definiti due percorsi distinti di accessi ai canali: di servizio (SCH) e di controllo (CCH), all'interno di ognuno, le priorità vengono attribuite secondo le categorie di accesso (direttamente correlata alla priorità utente), come indicato dalle code in Fig. 27, che forniscono parametri di trasmissione e contesa diversi per diversi livelli di priorità dei data frame.

Ci sono tre tipi di informazioni scambiate sul media WAVE: management frames, data frames e control frames.

I control frames possono essere utilizzati per IEEE 802.11 e non sono trattati in questo standard.

I principali management frames sono il frame TA (timing advertisement), utilizzato per distribuire informazioni di sincronizzazione temporale e il frame VSA (Wave service advertisement) utilizzato per lo scambio di informazioni di gestione, entrambi trattati in IEEE 802.11p. I frames VSA e TA possono essere trasmessi su ogni canale.

Per gli scambi di dati ai layer superiori, WAVE supporta sia il WSMP che IPv6. Per riconoscere pacchetti che gli vengono passati dallo strato LLC, ne verifica l'header, in particolare il campo EtherType che assume diverso valore a seconda si tratti di un pacchetto IP o WSMP: i frame di dati contenenti WSM possono essere scambiati tra dispositivi sia sul CCH che sul SCH, tuttavia, frame di dati contenenti datagrammi IP sono ammessi solo sui canali di servizio.

6.1. Channel coordination

Il coordinamento del canale è progettato per supportare l'alternarsi di operazioni concorrenti su CCH e su SCH. Ciò consente, ad esempio, ad un singolo dispositivo fisico di accedere a dati ad alta priorità e gestire il traffico durante l'intervallo CCH, così come l'elevato traffico durante l'intervallo SCH. La figura successiva illustra due esempi di accesso al canale: accesso continuo, che non richiede coordinamento del canale, e l'accesso alternato, che richiede un coordinamento del canale. La funzione di coordinamento dei canali inoltre assicura che i pacchetti vengano trasmessi sul canale RF desiderato.

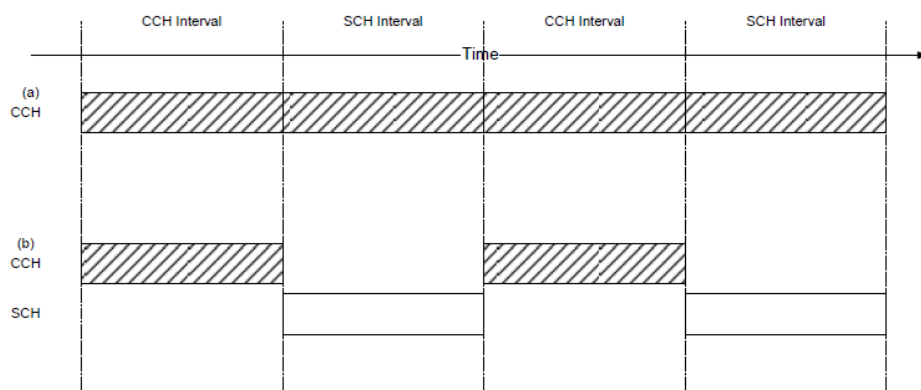


Fig. 28 – Esempio di accesso al canale: (a) continuo e (b) alternato

Nella figura successiva è dettagliato l'accesso alternato al canale con gli intervalli di sincronizzazione e i suoi componenti CCH intervals e SCH intervals:

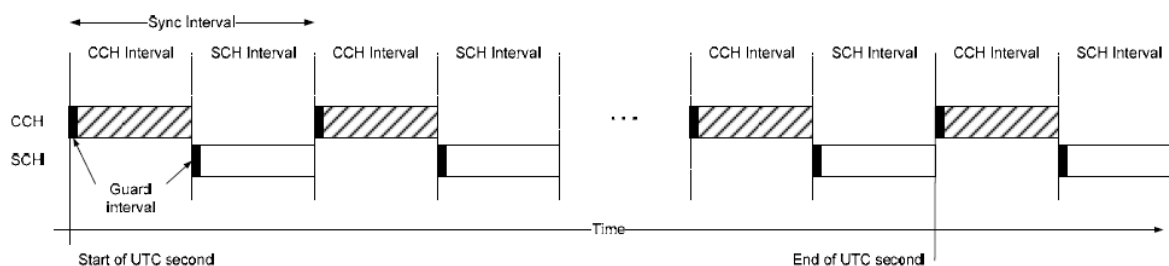


Fig. 29 - Sync interval, guard interval, CCH interval, and SCH interval

La durata degli intervalli CCH e SCH, definiti dallo standard sono memorizzati negli attributi MIB (management information base). CchInterval e SchInterval rispettivamente, ed i valori di questi attributi sommati è pari alla lunghezza dell'intervallo di sincronizzazione. Coordinated Universal Time (UTC) definisce la base temporale comune per la coordinazione del canale.

All'inizio di ogni intervallo di canale (CCH interval o SCH interval) c'è un intervallo di guardia, usato per tenere conto di imprecisioni temporali e di switching tra i diversi dispositivi.

Characteristic	Value
<i>OperatingClass</i> (CCH)	17
<i>ChannelNumber</i> (CCH)	178
<i>CchInterval</i>	50 ms
<i>SchInterval</i>	50 ms
<i>SyncTolerance</i>	2 ms
<i>MaxChSwitchTime</i>	2 ms

Fig. 30 - Parametri coordinamento canale

Un dispositivo WAVE deve supportare i seguenti tipi di frame IEEE 802.11:

- Management frame di tipo Timing Advertisement
- Management frame di tipo Action con sottotipo Vendor Specific
- Data frame, per il trasporto WSM
- Data frame, per il trasporto IP

I frames delle tipologie dette potrebbero essere trasmessi sia nell'intervallo CCH che nell'intervallo SCH ad esclusione dei pacchetti IP che non devono essere trasmessi sul CCH ma possono essere trasmessi solo su SCH. I controlli supportati e i canali di servizio sono identificati nella MIB. Altri tipi di frame possono essere trasmessi sia su CCH che su SCH.

6.2. Channel Routing

Il numero di canali disponibili per l'utilizzo dal dispositivo sono elencati nel MIB nell'attributo ChannelSetTable (come specificato in IEEE 802.11p). Il sottolivello MAC riceve i dati per la trasmissione dal sottolivello LLC nella forma di MA-UNITDATA.requests per i dati IP oppure MA-UNITDATA.requests per i dati WSMP, come illustrato nella due figure successive.

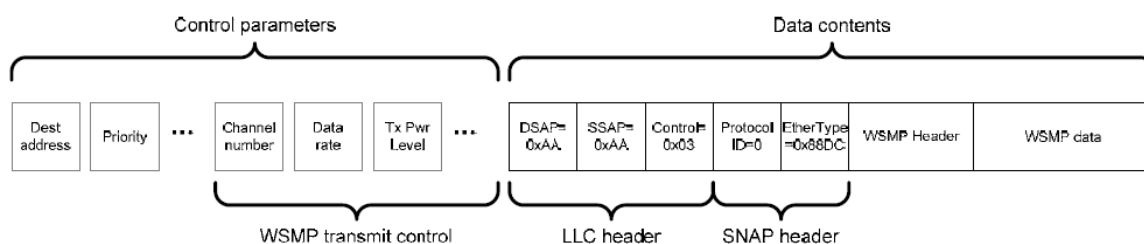


Fig. 31 - MA-UNITDATA.req fields for WSMP data

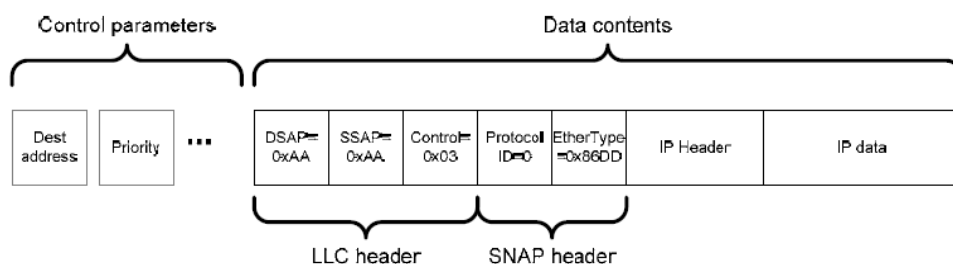


Fig. 32 - MA-UNITDATA.req fields for IP data

I frame dei protocolli IP o WSMP si distinguono anche attraverso il campo Ethertype del subnetwork Access Protocol (SNAP). Per i messaggi WSM il canale, la potenza di trasmissione e il data rate vengono impostato da livelli più alti a seconda dei messaggi. Per datagrammi IP, il canale, la potenza trasmissiva e il data rate da utilizzare è memorizzato nel profilo trasmettitore.

In Fig. 31 sono mostrati i contenuti del MA-UNITDATA.request dall'LLC al MAC per dati WSMP. Ethertype viene passato al MAC nell'intestazione SNAP. Il numero di canale, la velocità di trasmissione dati (data rate), potenza di trasmissione, indirizzo MAC di destinazione e la priorità vengono passati al MAC tramite parametri nella MAUNITDATA.request. Un esempio simile per dati IP è mostrato in Fig. 32.

Un dispositivo di trasmissione WAVE deve supportare il traffico WSMP, il traffico IP, o entrambi.

Un esempio di flusso di processo di trasmissione da LLC a PHY, specificato nello standard IEEE 802.11 è illustrato nella figura successiva. Il MAC controlla il data rate e il livello di potenza utilizzata dal PHY tramite valori nel TXVECTOR del PHY-TXSTART.request.

Per le specifiche IEEE Std 802.11 relative alle procedure Transmit Power Control, MLME impedisce alla potenza di trasmissione di superare la potenza massima consentita. La potenza massima consentita per un canale è definita in IEEE 1609.3 MIB nell'attributo UserAvailableTransmitPowerLevel o in ProviderChannelInfoTransmitPowerLevel.

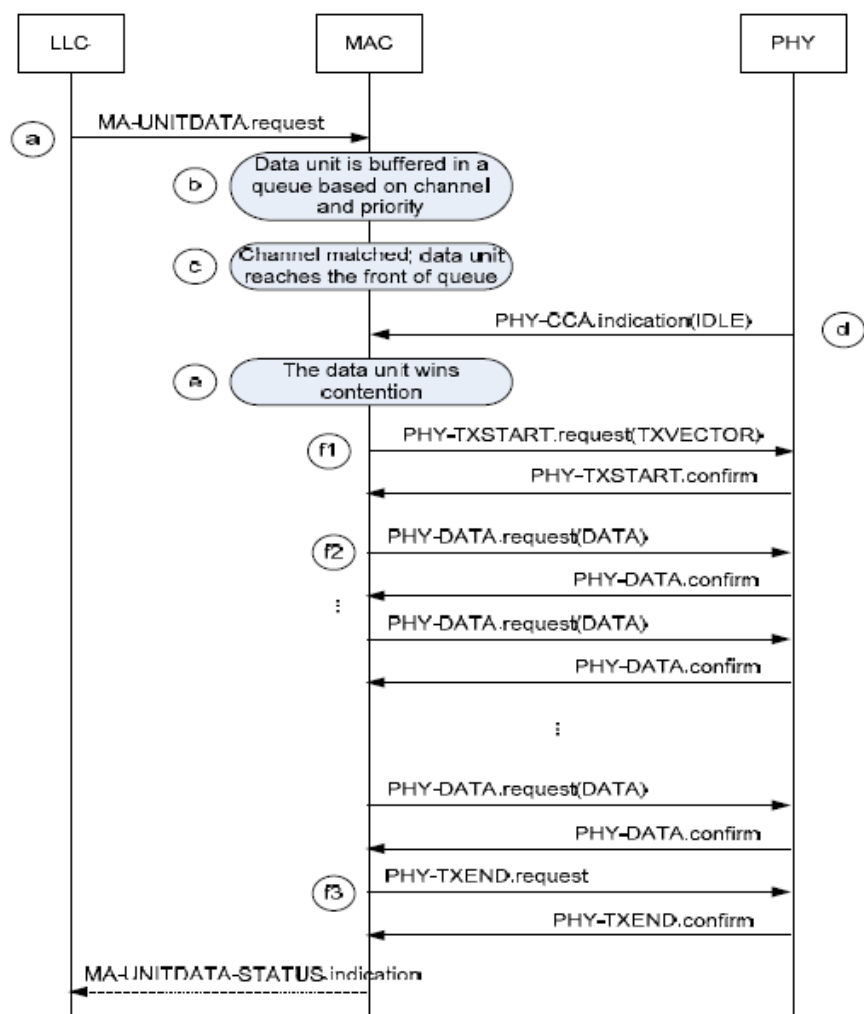


Fig. 33 - Esempio di flusso del processo di trasmissione

- a) LLC passa un MSDU (MAC service data unit) al MAC tramite un MA-UNITDATA.request o MA-UNITDATA.request.
- b) Le funzioni di routing del MAC esaminano il campo Ethertype della MSDU:
- 1) Se il campo Ethertype indica WSMP, il MAC assegna MSDU alla categoria di accesso basata sulla priorità utente dal MA-UNITDATA.request. Il MAC combina MSDU con le informazioni del protocollo MAC per formare una MPDU (*Fig. 27*) e pone l'MPDU in una coda appropriata per la categoria di accesso assegnata e il parametro del canale passato nella primitiva.
 - 2) Se il campo Ethertype indica IP, il MAC assegna MSDU ad una categoria di accesso in base alla priorità dell'utente. Il MAC combina MSDU con le informazioni del protocollo MAC per formare un MPDU e inserisce l'MPDU in una coda appropriata per la categoria di accesso assegnata l'SCH ottenuto dal profilo trasmettitore.
- c) L'insieme di code di dati associato al canale corrente è identificato.
- 1) Se il frame contiene un WSM, allora vengono utilizzati la potenza di trasmissione e il data rate ricevuti nel MA-UNITDATA.request.
 - 2) Se Ethertype contiene un datagramma IP, allora la potenza di trasmissione e data rate utilizzati sono quelli memorizzati nell'attributo MIB TransmitterProfileTable.
- d) Il livello PHY segnala un canale chiaro al MAC mediante emissione del PHY-CCA.indication (IDLE).
- e) Il MAC seleziona l'MPDU che vince la contesa interna sul canale corrente tramite EDCA (Enhanced distributed channel access).
- f) I valori del livello di potenza e data rate sono impostati in un TXVECTOR. La procedura per trasferire un MPDU tra il MAC e PHY:
- 1) Il MAC emette un PHY-TXSTART.request (TXVECTOR) al PHY. Al MAC viene restituita conferma dopo il PHY ha impostato il livello di potenza desiderato e il data rate..
 - 2) I dati vengono poi scambiati tra MAC e PHY attraverso una serie di primitive PHY-DATA.REQUEST (DATA) emesse dal MAC e primitive di PHY-DATA.confirm emesse dal PHY.
 - 3) Dopo la trasmissione del bit finale dell'ultimo ottetto MPDU, la trasmissione viene interrotta dal MAC attraverso la primitiva PHY-TXEND.request.
- g) Se la trasmissione di un MPDU non è terminata quando l'intervallo canale corrente termina, la trasmissione può essere annullata dal MAC attraverso la primitiva PHY-TXEND.request. Questa risoluzione anticipata può essere evitata tramite l'attuazione di alcune misure di salvaguardia in particolare:
- 1) Prima di consegnare un MSDU al PHY, il MAC invia un PLME-TXTIME.request e il PHY restituisce un PLME-TXTIME.confirm con il tempo di trasmissione desiderata.
 - 2) Se il tempo di trasmissione richiesta supera la durata residua dell'intervallo canale, l'MSDU dovrebbe essere accodato nel sottolivello MAC fino al ritorno della disponibilità del canale.

Per quanto riguarda invece le operazioni di ricezione, Quando il MAC riceve un MPDU, estrae il MSDU e lo passa al LLC. Si utilizza un primitiva MA-UNITDATA.indication indipendentemente dal fatto che il frame contenga un WSM o un pacchetto IPv6. Se il PHY è in fase di ricezione di un frame di dati quando avviene uno switching di canale, provocando un'interruzione della ricezione, il PHY segnala un PHY-RXEND.indication (RXERROR = CarrierLost) al sottolivello MAC (come specificato in IEEE 802.11) e il corrispondente frame incompleto viene scartato dal MAC.

Per WSMP, la primitiva MA-UNITDATA.request, definita in 802.11, è estesa nello standard IEEE 1609.4 per permettere al livello superiore di controllare i parametri di trasmissione PHY per ogni singolo pacchetto e comprende: Channel Identifier, Data Rate, TxPwr_Level e Expiry Time. Al ricevimento di questa primitiva, l'entità sottolivello MAC determina se la richiesta può essere soddisfatta secondo i parametri richiesti: il MAC deve instradare il pacchetto verso una appropriata coda in base al Channel Identifier e alla priorità. Il pacchetto dati non è accodato per la trasmissione nel caso in cui Channel Identifier non si riferisca ad un canale valido. Se la richiesta può essere soddisfatta, il MAC sublayer entity, passa il frame formattato correttamente ai livelli inferiori e ne dà notizia all'LLC con una primitiva MA-UNITDATA.confirm che indica lo stato di trasmissione effettuato con successo. Se una richiesta non può essere soddisfatta viene scartata e se ne dà comunicazione a LLC utilizzando, anche in questo caso, la primitiva MAUNITDATA.confirm che descrive perché il MAC non è stato in grado di soddisfarla.

Per l'invio di datagrammi IP occorre che nell'attributo MIB TransmitterProfileTable sia registrato un profilo trasmettitore tramite un MLMEX-REGISTERTXPROFILE.request o altro meccanismo. Il profilo trasmettitore contiene il numero SCH, il livello di potenza e il data rate. La priorità è fissata dal livello superiore per ciascuna MSDU. Quando il pacchetto IP viene passato in un MA-UNITDATA.request dall'LLC al MAC, il MAC deve passare il pacchetto alla coda corrispondente al SCH e alla priorità richiesta. Se non c'è nessun profilo trasmettitore registrato per il SCH, o se l'MLME non fornisce accesso al SCH, i dati devono essere scartati.

La trasmissioni dei management frame deve essere controllata attraverso i parametri di data rate e potenza presenti nell'attributo MIB ChannelSetTable per il canale.

6.3. Priorità utente

Il MAC WAVE implementa lo schema di accesso al mezzo EDCA (Enhanced Distributed Channel Access) definito in 802.11. L'architettura generale della definizione di priorità d'accesso per la trasmissione dei dati è illustrata in Fig. 27.

Quando un MA-UNITDATA.request o un MA-UNITDATA.request arriva al sottolivello MAC ed è stato completato l'appropriato instradamento sul canale (SCH o CCH), il MAC deve accodare i frames mappandoli in base alla priorità utente (UP con range da 0 a 7) nelle access category (AC) e access category index (ACI, range 0 a 3).

Le AC assumono un valore in un range da 1 a 4: 4=AC_VO – voce, 3=AC_VI – video, 2=AC_BE – best effort, 1=AC_BK – background.

I management frames sono assegnati al più alto AC (cioè 4).

Ogni AC ha una funzione indipendente di accesso al canale, con priorità regolata da appropriati parametri EDCA. I valori del set di parametri WAVE EDCA è diverso dal predefinito specificato in IEEE Std 802.11 e sono descritti di seguito:

- Arbitration inter-frame space (AIFS): l'intervallo di tempo minimo dal momento in cui canale è inattivo a quando inizia la trasmissione di un frame.
- Contention Window (CW): un intervallo da cui si ricava un numero casuale per l'attuazione del meccanismo di back-off di trasmissione casuale (random transmit back-off mechanism).
- Limite Trasmission Opportunity (TXOP): il tempo di durata massimo (in millisecondi) per i quali una stazione può trasmettere dopo aver ottenuto un TXOP. Se il limite TXOP è 0, è consentita solo la trasmissione di un singolo MPDU.

L'algoritmo interno di contesa secondo IEEE 802.11 calcola il tempo di back-off in modo indipendente per ciascun AC basato sui 3 parametri di accesso detti. L'AC con il più piccolo back-off vince la contesa interna (internal contention) tra le code, poi dovrà affrontare la contesa del mezzo (medium contention).

Il set di parametri predefiniti EDCA in IEEE Std 802.11p è ottimizzato per il trasferimento dei messaggi brevi ed è consigliato per essere utilizzato quando si opera sul CCH.

I pacchetti di dati IP, WSMP, così come i management frames, sono consentiti su SCH. Su un SCH, se viene ricevuto un insieme di parametri EDCA in MLMEX-SCHSTART.request, questo set di parametri sarà usato per trasmissioni su questo SCH, altrimenti deve essere utilizzato il set di parametri predefinito EDCA specificato in IEEE 802.11p.

ACI	AC	CWmin	CWmax	AIFSN	TXOP Limit OFDM PHY
1	Background	CWmin	CWmax	9	0
0	Best effort	$(CWmin + 1)/2 - 1$	CWmin	6	0
2	Video	$(CWmin + 1)/4 - 1$	$(CWmin + 1)/2 - 1$	3	0
3	Voice	$(CWmin + 1)/4 - 1$	$(CWmin + 1)/2 - 1$	2	0

Fig. 34 – Parametri EDCA IEEE 802.11p per CCH

ACI	AC	CWmin	CWmax	AIFSN	TXOP Limit OFDM/ CCK-OFDM PHY
1	Background	CWmin	CWmax	7	0
0	Best Effort	CWmin	CWmax	3	0
2	Video	$(CWmin + 1)/2 - 1$	CWmin	2	0
3	Voice	$(CWmin + 1)/4 - 1$	$(CWmin + 1)/2 - 1$	2	0

Fig. 35 – Parametri EDCA IEEE 802.11p per SCH

7. Management plane services

Questo standard specifica un'estensione del MAC sublayer management entity (MLME) specificato in IEEE Std 802.11 e IEEE Std 802.11p. Esso comprende la sincronizzazione temporale e le funzionalità di accesso al canale a sostegno del coordinamento del canale, nonché la trasmissione periodica di management frames.

7.1. Sincronizzazione multicanale

La funzione di sincronizzazione, necessaria per consentire ai dispositivi WAVE di eseguire il coordinamento del canale (di cui al paragrafo 6.1), utilizza UTC (Coordinated Universal Time) come tempo di riferimento base. UTC è definito in ITU-R TF.460 e può essere ottenuto da diverse fonti tra cui Global Positioning System (GPS). I ricevitori GPS forniscono tipicamente un impulso al secondo (PPS), con un errore inferiore a 100 ns, e questi segnali possono essere utilizzati per la temporizzazione e sincronizzazione.

I dispositivi senza una sorgente locale di temporizzazione possono acquisire informazioni di temporizzazione via etere da altri dispositivi WAVE. In tal caso essi utilizzano il campo Timestamp e le informazioni ricevute nei frames Time Advertisement come input nella stima del tempo UTC.

Timestamp indica il valore della timing synchronization function (TSF) del trasmettitore.

Il valore del temporizzatore TSF è un intero modulo 2^{64} , incrementato in unità di microsecondi.

Le informazioni di temporizzazione utilizzate per la sincronizzazione possono essere derivate da informazioni ricevute da altri dispositivi o possono essere ottenute da un riferimento temporale locale.

MLME mantiene una stima del tempo UTC usato per la coordinazione del canale. La funzione di gestione della temporizzazione dalla quale deriva la stima UTC può essere interna o esterna a MLME. Una funzione di gestione dei tempi esterna può impostare la stima di MLME UTC attraverso MLME-SETUTCTIME.request.

Quando esegue la sincronizzazione, MLME si sincronizza al tempo UTC attraverso l'implementazione di uno stimatore del tempo UTC e uno stimatore della deviazione standard dell'errore nella stima del tempo UTC in modo da includere l'effetto delle eventuali distorsioni nella stima del tempo.

7.1.1. Informazioni di temporizzazione

Le informazioni di temporizzazione, che sono trasportate attraverso un Timing Advertisement frame, possono essere utilizzate dai destinatari per stimare il tempo UTC. Questo frame è costituito da 3 sottocampi: Timer Capabilities, Time Value e Time Error (come specificato in IEEE 802.11p). Il destinatario del frame TA può usare il Timestamp, il Time Value e il Time Error, insieme con il tempo TSF locale per determinare il rapporto tra UTC e l'ora TSF che può quindi essere utilizzato con tempo locale TSF per fornire una stima di UTC in qualsiasi momento.

Quando chi trasmette non dispone di una stima di tempo valida allora il Time Value deve essere impostato a zero e Time Error è fissato al suo valore massimo. Quando una fonte di tempo UTC di qualità superiore diventa disponibile, il sorgente e la sua varianza di errore possono essere utilizzati dallo stimatore UTC. Il valore del Time Error (cioè, l'incertezza nella stima del Time Value), è generalmente una funzione di vari fattori ambientali e di attuazione che possono variare nel tempo.

Spedire TA frame è opzionale, al ricevimento di un MLMEX-TA.request, MLME può generare la primitiva MLME-TIMING_ADVERTISEMENT.request al rate indicato in Repeat Rate in MLMEX-TA.request (Fig. 36). I frames Timing Advertisement devono essere trasmessi nel canale e nell'intervallo di canale indicato in MLMEX-TA.request. Se una funzione di gestione del tempo è esterna, esso è fornito a MLME in the MLMEXTA.request; altrimenti è lo stesso MLME che lo calcola.

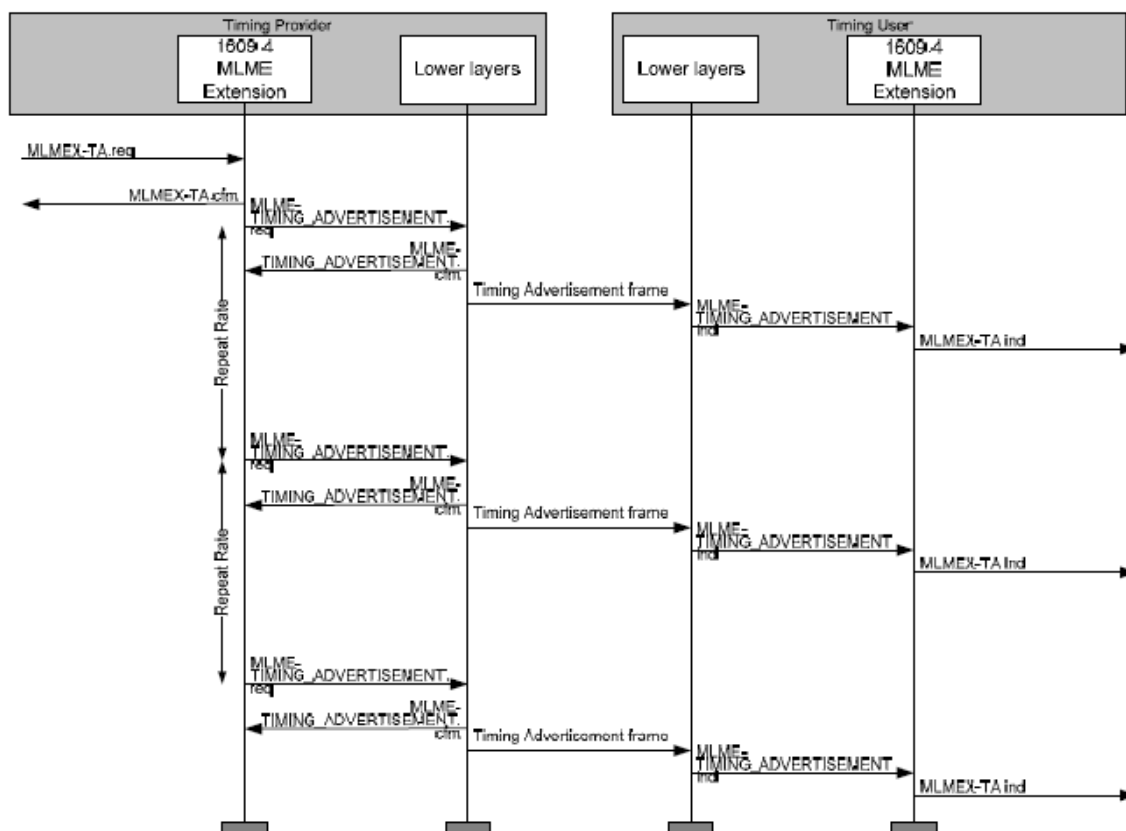


Fig. 36 – Trasmissione informazioni di temporizzazione

7.1.2. Tolleranza di sincronizzazione

Ogni intervallo CCH e SCH include un intervallo iniziale di guardia, come mostrato in *Fig. 29*, costituito dalla somma dei parametri MIB SyncTolerance e MaxChSwitchTime.

$\text{SyncTolerance} / 2$ è il valore utilizzato per determinare se un dispositivo WAVE è sincronizzato con UTC o meno.

MaxChSwitchTime è il tempo massimo consentito, per ogni dispositivo WAVE con sincronizzazione multicanale, per cambiare canale.

Durante l'intervallo di guardia, il dispositivo PHY potrebbe non essere disponibile per la comunicazione oppure potrebbe essere in uno stato di transizione tra i canali. All'inizio di un intervallo di guardia, le attività MAC sul canale precedente deve essere sospesa, al termine dell'intervallo di guardia, le attività di accesso prioritarie sul canale successivo devono essere iniziate, o riprese se sono state sospese.

Per evitare che piu' switching device tentino di trasmettere contemporaneamente alla fine di un intervallo di guardia, viene segnalato il supporto occupato durante l'intervallo di guardia in modo che tutti i tentativi di trasmissione siano soggetti ad un back-off casuale all'inizio di ciascun intervallo di canale.

In *Fig. 37* sono illustrate le componenti dell'intervallo di guardia. MaxChSwitchTime rappresenta il momento in cui il dispositivo non è utilizzabile, incapace di trasmettere o ricevere. SyncTolerance / 2 tiene conto del fatto che dispositivi di comunicazione possono non essere esattamente allineati nel tempo. La ricezione tuttavia può avvenire durante gli intervalli di tolleranza, ma la trasmissione può essere effettuata solo di fuori dell'intervallo di guardia.

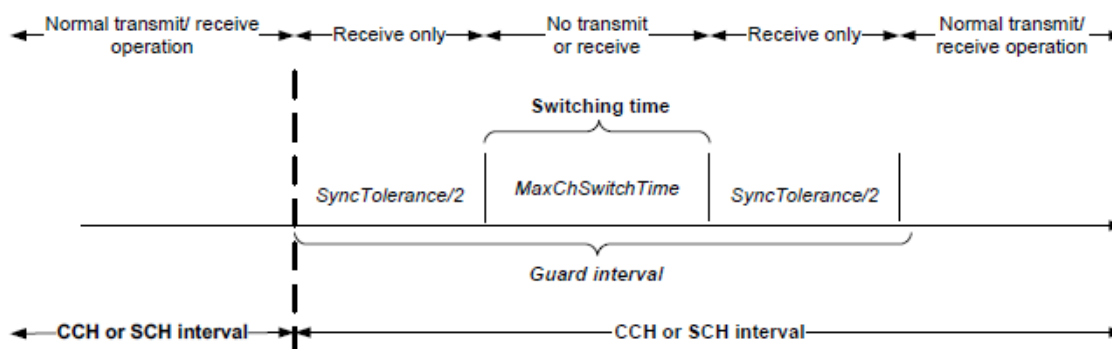


Fig. 37 – Intervallo di guardia, tolleranza di sincronizzazione e tempo max di switch canale

Un dispositivo WAVE deve essere sincronizzato con UTC se tre volte il valore del suo Time Error è inferiore a $\text{SyncTolerance} / 2$. Quando non è sincronizzato con UTC, MLME non fornisce accesso alternato ai canali (o accesso immediato al canale quando viene utilizzato senza accesso esteso) come specificato successivamente nella definizione di accesso al canale.

7.2. Accesso al canale

Come detto, MLME fornisce l'accesso a specifici canali sotto il controllo della WME. Le opzioni di accesso al canale includono l'accesso continuo, l'accesso alternato al canale SCH e CCH, l'accesso immediato SCH e l'accesso esteso SCH, come illustrato in Fig. 38.

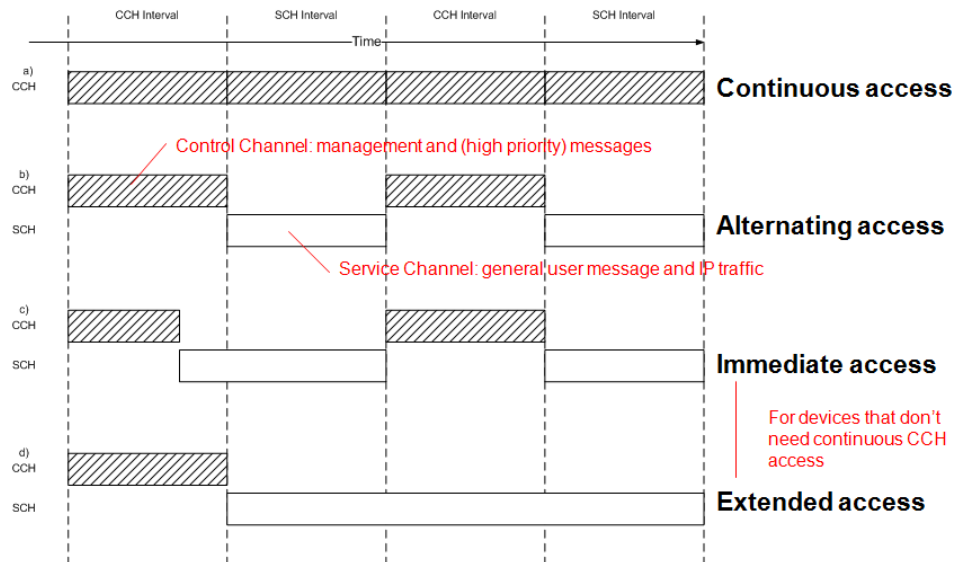


Fig. 38 – Possibilità accesso al canale: (a) continuo, (b) alternato, (c) immediato e (d) esteso

Il servizio di accesso al canale consente ai livelli più alti di scambiare dati su un canale di servizio designato. Le operazioni di accesso al canale sono specificate qui nel contesto dei singoli dispositivi fisici.

MLME effettua il cambio del canale inviando (come da IEEE 802.11) un PLME-SET.request con dot11CurrentFrequency settato con il canale desiderato.

Inoltre, se i canali attuali e quelli nuovi hanno diversi *Channel Starting Frequency* o *Channel Spacing*, MLME invia un PLME-SET.request che setta l'impostazione dot11ChannelStartingFactor e/o dot11PhyOFDMChannelWidth.

7.2.1. Accesso alternato

Al ricevimento della MLMEX-SCHSTART.req, MLME deve iniziare a fornire l'accesso al numero di canale richiesto.

Se non è diversamente indicato da ExtendedAccess, all'inizio di ogni intervallo CCH, MLME invia un PLME-SET.request con dot11CurrentFrequency uguale al numero di canale CCH come determinato dall'attributo MIB ChannelSetTable.

Se non diversamente indicato da ImmediateAccess o ExtendedAccess, all'inizio di ogni intervallo SCH, MLME invia un PLME-SET.request con dot11CurrentFrequency pari alla numero del canale dalla MLMEX-SCHSTART.request (Fig. 39).

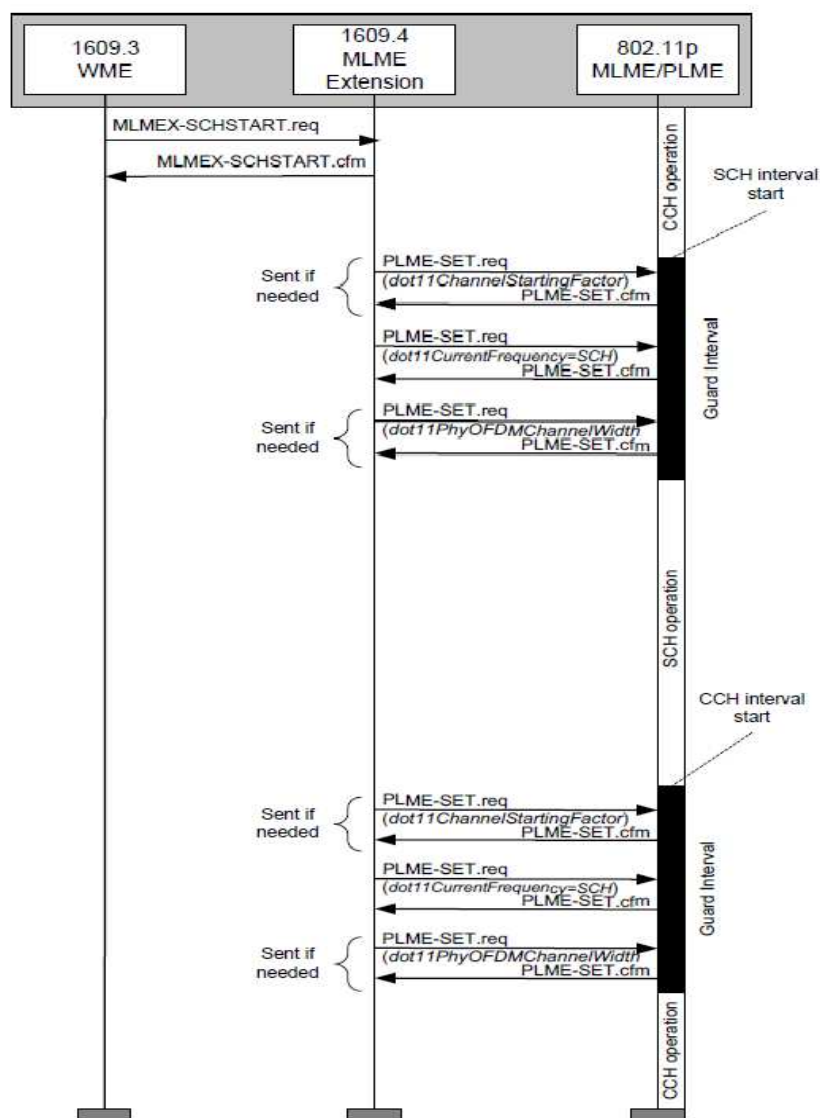


Fig. 39 - Accesso alternato al canale

7.2.2. Accesso SCH immediato

Consente l'accesso immediato alle comunicazioni su SCH senza attendere il prossimo intervallo SCH. Al ricevimento della `MLMEX-SCHSTART.request` con `ImmediateAccess` settato a `True`, MLME deve fornire l'accesso al canale indicato in `Channel Number`: appena possibile, MLME invia un `PLME-SET.request` con `dot11CurrentFrequency` uguale al numero del canale dalla `MLMEX-SCHSTART.request`.

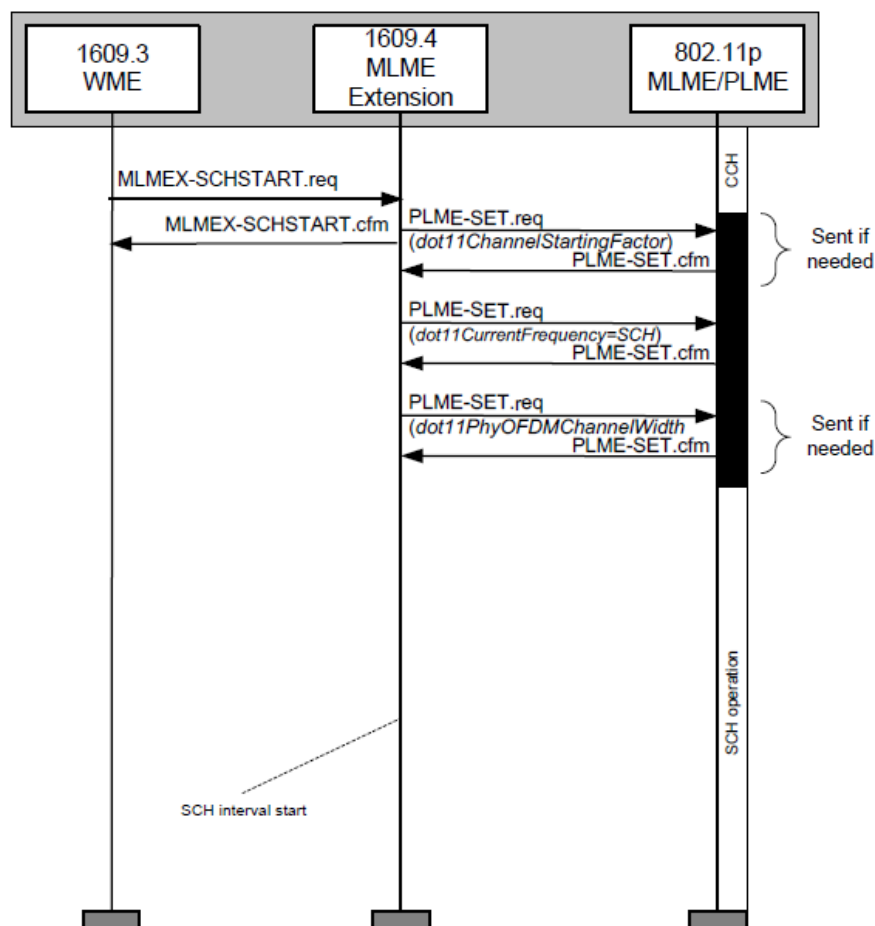


Fig. 40 - Accesso immediato a SCH

7.2.3. Accesso a SCH esteso

Consente l'accesso alle comunicazioni su SCH senza pause per l'accesso CCH. Al ricevimento della MLME-SCHSTART.request con ExtendedAccess > di 0, la MLME deve cominciare a fornire l'accesso al numero del canale indicato come segue. Il MLME invia un PLME-SET.request con l'insieme dot11CurrentFrequency pari al numero del canale dal MLME-SCHSTART.req come illustrato nella figura sotto. A meno che non si riceva una nuova MLME-SCHSTART.request o un MLME-SCHEND.request, MLME non invia più PLME-SET.requests per un periodo di intervalli di canale ExtendedAccess, trascorso questo tempo, MLME torna all'accesso alternato o continuo a seconda dei casi.

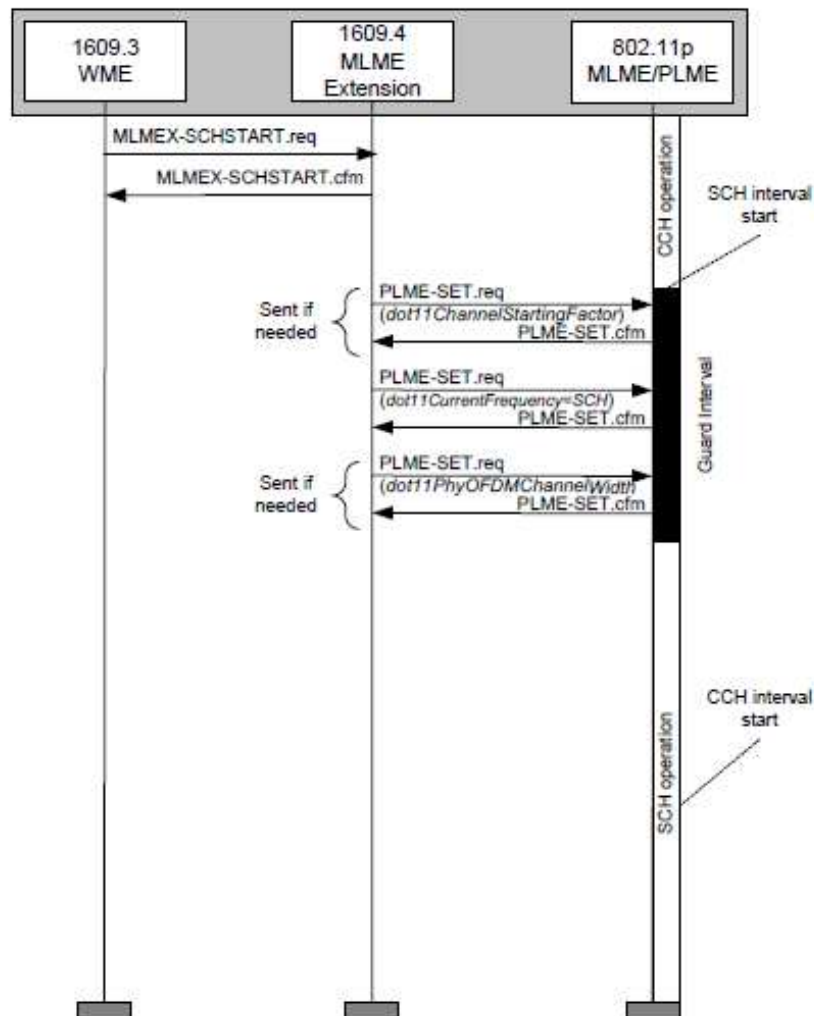


Fig. 41 - Accesso SCH esteso

7.2.4. Rilascio del canale

Al ricevimento della MLMEX-SCHEND.request, MLME cessa di fornire l'accesso al Channel Number in questo modo: MLME invia un PLME-SET.request con dot11CurrentFrequency pari al CCH come determinato dall' attributo MIB ChannelSetTable. Se MLME rilascia unilateralmente un SCH (ad esempio, a causa della perdita di sincronizzazione), invia un MLMEX-SCHEND.indication per indicare il motivo.

7.3. Vendor Specific Action frames

La trasmissione di VSA è opzionale. La ricezione di un MLMEX-VSA.request fa sì che IEEE 1609.4 MLME inizi a generale trasmissioni di frames VSA come segue. Se è indicato l'indirizzo MAC di destinazione nella MLMEX-VSA.request allora utilizza un indirizzo unicast: MLME genera una primitiva MLME-VSPECIFIC.request, altrimenti, MLME genera un numero di primitive MLMEVSPECIFIC.request al Repeat Rate ricevuto nel MLMEX-VSA.request (Fig. 44).

I parametri di MLME-VSPECIFIC.request vengono impostati:

Parameter	Value
<i>PeerMacAddress</i>	Set to the <i>Destination MAC Address</i> from the MLME-VSA.request.
<i>Organization Identifier</i>	Set as specified in the text that follows the table.
<i>Vendor Specific Content</i>	Set to the <i>Vendor Specific Content</i> field from the MLME-VSA.request.

Fig. 43 - parametri MLME-VSPECIFIC.request

Organization Identifier è impostato con l'identificatore di organizzazione dal MLME-VSA.request, se presente.

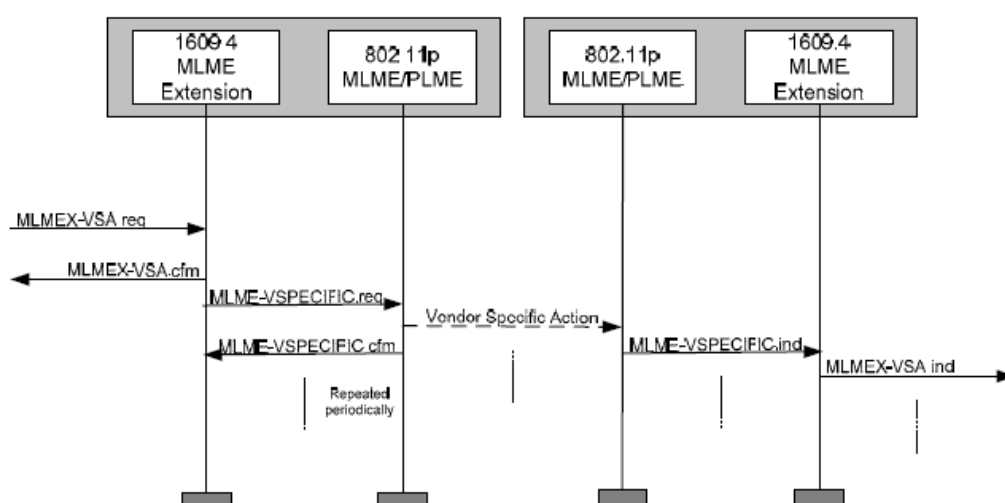


Fig. 44 - Trasmissione e consegna VSA

Durante la generazione di VSA ripetuti, al ricevimento di un MLME-VSAEND.request, la MLME cessa di generare MLME-VSPECIFIC.requests. Se il MLME sta generando diversi VSA, occorre sia implementato uno specifico meccanismo per identificare quale VSA viene terminata.

Dal lato ricezione occorre dire che è opzionale processare VSA ricevuti. Il ricevimento di frame d'azione specifici del fornitore è indicato a MLME attraverso MLME-VSPECIFIC.indication (IEEE 802.11). MLME a sua volta genera un MLME-VSA.indication. Al ricevimento di un MLME-VSPECIFIC.indication, per le implementazioni che supportano questa funzione, MLME genera un MLME-VSA.indication come specificato nella tabella.

Parameter	Value
<i>Source MAC Address</i>	Set to the <i>PeerMACAddress</i> from the MLME-VSPECIFIC.indication.
<i>Vendor Specific Content</i>	<i>VendorSpecificContent</i> from the MLME-VSPECIFIC.indication.
<i>RCPI</i>	Set to Received Channel Power Indicator (<i>RCPI</i>) in the MLME-VSPECIFIC.indication.
<i>Channel Identifier</i>	The channel on which the frame was received.
<i>Management ID</i>	Set to 4 least significant bits of <i>Organization Identifier</i> in the MLME-VSPECIFIC.indication. <i>Management ID</i> values are specified in IEEE P1609.0.

Fig. 45 – Parametri di MLME-VSA.indication

7.4. Altri servizi IEEE 802.11

MLME può supportare l'invio di primitive che invocano specifici servizi IEEE 802.11. Questo permette ad una entità esterna di attivare la trasmissione di un frame di gestione, come quelli utilizzati per la valutazione della qualità collegamento su un canale specifico. Al ricevimento di un MLME-SendPrimitive.req, l'IEEE 1609.4 MLME genera la primitiva di richiesta del servizio IEEE 802.11 indicato. La figura successiva mostra un esempio di questa possibilità nel caso di una IEEE 802,11 Measurement Request, e il suo rapporto risultante.

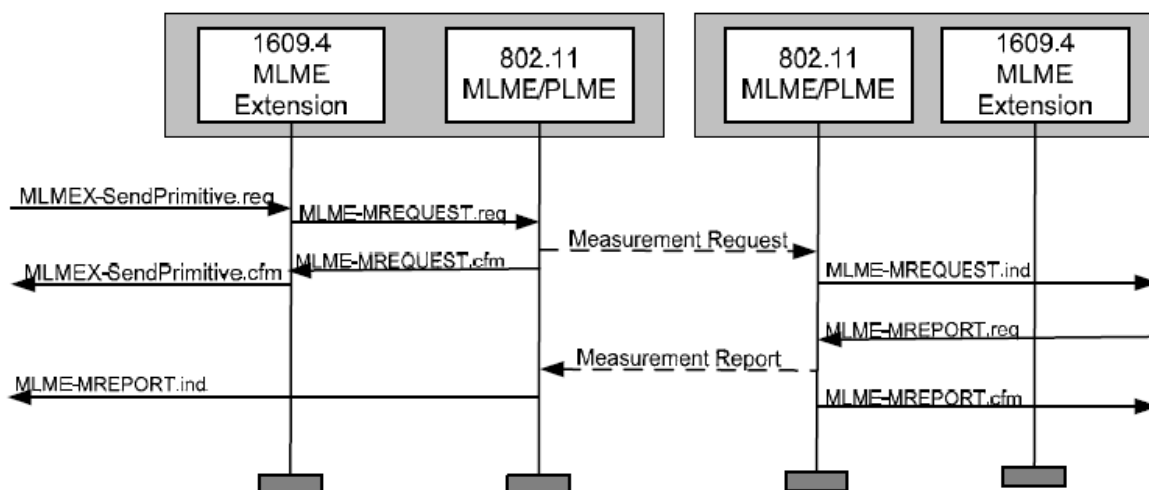


Fig. 46 – Esempio di chiamata IEEE 802.11 management frame

7.5. MIB manutenzione

In un dispositivo WAVE gestito, MLME tiene un Management Information Base (MIB) che contiene le informazioni di configurazione e le informazioni di stato. Il MIB è accessibile ai più alti livelli tramite le primitive, specificate in IEEE 802.11, MLME-Get e Set-MLME. Inoltre, il dispositivo può supportare altri MIB (ad esempio, MIB che contengono informazioni specifiche del fornitore).

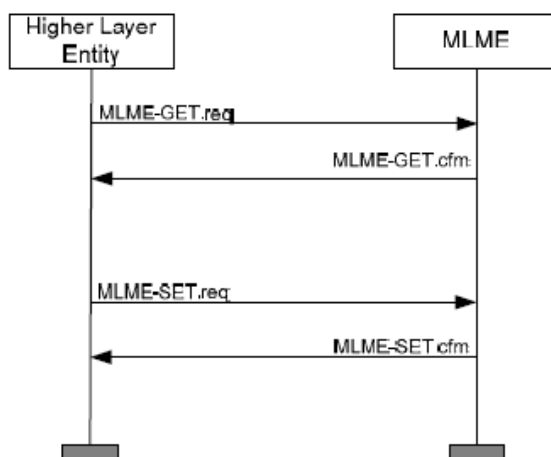


Fig. 47 – Flusso di comunicazioni per accedere al MIB

7.6. Reindirizzamento

A sostegno della pseudonimia, un dispositivo può supportare una funzione di reindirizzamento. Al ricevimento di un MLMEXAddressChange.request, MLME deve reimpostare l'indirizzo MAC del dispositivo su un nuovo valore. Se un MLMEXAddressChange.request include MAC Address, tale valore viene utilizzato come nuovo indirizzo, altrimenti, viene utilizzato un indirizzo scelto a caso. L'indirizzo scelto è un indirizzo gestito localmente come definito dallo standard IEEE 802. Si noti che un cambio di indirizzo può interrompere tutte le comunicazioni in corso.

8. Le primitive dello standard IEEE 1609.4

In Fig. 48 sono elencate le primitive trattate in questo standard: primitive già definite negli standard IEEE 802.11 e IEEE 802.11p e primitive qui definite, che costituiscono le estensioni MLME di cui si è parlato ampiamente nei paragrafi precedenti

SAP	Primitive	Specified in
MLME extension	MLMEX-TA	IEEE Std 1609.4
	MLMEX-TAEND	IEEE Std 1609.4
	MLMEX-VSA	IEEE Std 1609.4
	MLMEX-VSAEND	IEEE Std 1609.4
	MLMEX-SCHSTART	IEEE Std 1609.4
	MLMEX-SCHEND	IEEE Std 1609.4
	MLMEX-REGISTERTXPROFILE	IEEE Std 1609.4
	MLMEX-DELETETXPROFILE	IEEE Std 1609.4
	MLMEX-CANCELTX	IEEE Std 1609.4
	MLMEX-GETUTCTIME	IEEE Std 1609.4
	MLMEX-AddressChange	IEEE Std 1609.4
	MLMEX-SendPrimitive	IEEE Std 1609.4
MLME	MLME-GET	IEEE Std 802.11
	MLME-SET	IEEE Std 802.11
	MLME-VSPECIFIC	IEEE Std 802.11
	MLME-TIMING_ADVERTISEMENT	IEEE Std 802.11p
	MLME-GETTSFTIME	IEEE Std 802.11p
PLME	All	IEEE Std 802.11
MAC	MA-UNITDATA	IEEE Std 802.11
	MA-UNITDATAx	IEEE Std 1609.4
PHY	All	IEEE Std 802.11

Fig. 48 – Primitive nello standard IEEE 1609.4

Si descriverà ora brevemente la caratterizzazione delle primitive di questo standard:

- MLMEX-TA e MLMEX-TAEND attengono alla trasmissione e ricezione di informazioni di temporizzazione (Fig. 37).
- MLMEX-VSA e MLMEX-VSAEND sono relativi alle trasmissioni di vendor specific action frames (Fig. 44).
- MLMEX-SCHSTART e MLMEX-SCHEND per l'accesso al canale (Paragrafo 7.2)
- MLMEX-REGISTERTXPROFILE e MLMEX-DELETETXPROFILE per la registrazione e la cancellazione di un profilo trasmettitore per le comunicazioni ip-based (Paragrafo 6.2)
- MLMEX-CANCELTX è utilizzato per annullare tutte le trasmissioni di una categoria di accesso di un particolare per canale.

- MLMEX-GETUTCTIME meccanismo usato per chiedere e settare il valore della stima del tempo UTC.
- MLMEX-AddressChange gestire il campo immediato dell'indirizzo MAC (paragrafo 7.6)
- MLMEX-SendPrimitive specificatamente per richiedere una primitiva IEEE 802.11.

Le primitive MA-UNITDATA sono definite per consentire ai livelli più alti della pila protocollare di controllare le caratteristiche della trasmissione di pacchetti WSMP (paragrafo 6.2).

CONCLUSIONI

Le reti veicolari consentono l'implementazione di una miriade di applicazioni legate alla sicurezza stradale, alla gestione del traffico, alla fornitura di servizi di supporto ai conducenti dei veicoli e ai passeggeri, oltre che ai pedoni. I primi esempi di tali applicazioni sono certamente i sistemi automatici di esazione pedaggi e i sistemi di assistenza al conducente.

L'interesse per i "Sistemi di Trasporto Intelligenti" sono supportati da sforzi coordinati per la standardizzazione e la formazione di consorzi e altri enti governativi e industriali che mirano a definirne i principi, le linee guida e i requisiti necessari al fine di trovare soluzioni per i sistemi di comunicazione che riguardano principalmente i veicoli e gli utenti all'interno dei veicoli.

Negli Stati Uniti, gli sforzi di ricerca scientifici, industriali e governativi hanno creato importanti opportunità in progetti come *US IntelliDrive (sm)*, *CAMP/VSC-2*; *CICAS*, *SafeTrip21* e *California PATH*. I protocolli standard per reti veicolari utilizzati in tali progetti, ad eccezione del *SafeTrip21*, sono gli standard WAVE.

In Giappone molti progetti e programmi in materia ITS hanno portato alla creazione di infrastrutture di rete veicolari, come la realizzazione di *ETC (Electronic Toll Collection)* che utilizza la banda DSRC. Nel 2008 circa 20 milioni di veicoli erano equipaggiati con *OBU ETC*.

In Europa, in materia di comunicazione veicolare sono in corso di definizione architetture per comunicazioni veicolari, come ad esempio *Continuous Air-interface Long and Medium range (CALM)*, per definire un insieme di protocolli di comunicazione e interfacce wireless per una varietà di scenari, con molteplici modalità di comunicazione e metodi di trasmissioni, tra cui DSRC WAVE.

BIBLIOGRAFIA

- Research and Innovative Technology Administration (RITA) – Department of Transportation's "IEEE1609 - Family of Standards for Wireless Access in Vehicular Environment(WAVE) ", [http://www.standards.its.dot.gov/fact_sheet.asp?f=80].
- Federal Communication Commission, agency of the United States government [http://wireless.fcc.gov/services/index.htm?job=service_home&id=dedicated_src].
- Dr. Guillermo Acosta, Professor Roberto A. Uzcategu , "The WAVE Solution – Coming Soon to a Car Near You: Wireless Access", October 2011 [http://www.slideshare.net/gamarun/wave-tutorial].
- Roberto A. Uzcátegui, Universidad Nacional Experimental Politécnica "Antonio José de Sucre" and Guillermo Acosta-Marum, Georgia Institute of Technology, "WAVE: A Tutorial", April 2009 [http://www.slideshare.net/gamarun/wave-a-tutorial].
- Gerald D. Conover, "ITS Car to Car Communications Standards", NIST-CDV Workshop on ITS, September 29, 2010 [http://gsi.nist.gov/global/docs/sit/ 2010/its/GConoverFriday.pdf].
- Shahzad A. Malik, Madad Ali Shah, Shahid A. Khan, M. Jahanzeb, Umar Farooq, M. Adnan Khan, "Performance Evaluation of IEEE 802.11p MAC Protocol for VANETs", Australian Journal of Basic and Applied Sciences, 4(8): 4089-4098, 2010 ISSN 1991-8178 © 2010, INSInet Publication [http://www.insipub.com/ajbas/2010/4089-4098.pdf]
- Alastair Malarky, MARK IV IVHS, Markiv, "1609.1", 30 september 2007, [http://www.ieeevtc.org/plenaries/vtc2007fall/33.pdf].
- TechnoCom, "The WAVE Communications Stack: IEEE 802.11p, 1609.4 and, 1609.3", September, 2007 [http://www.ieeevtc.org/plenaries/vtc2007fall/34.pdf].
- Yi Wang, Akram Ahmed, Bhaskar Krishnamachari and Konstantinos Psounis - Viterbi School of Engineering, University of Southern California, "IEEE 802.11p performance evaluation and protocol enhancement", Proceedings of the 2008 IEEE International Conference on Vehicular Electronics and Safety Columbus, OH, USA. September 22-24, 2008.
- Abdel Kader Mokaddem, RENAULT , ITS - "Car to Car Communications at 5,9 GHz -Workshop on Spectrum Requirement" -For Road Safety -Brussels, February 2006 [http://ec.europa.eu/information_society/activities/esafety/doc/esafety_2006/spectrum_28feb2006/7_c2c_eu_workshop_280206_v1.pdf].
- University of Waterloo – Canada, Broadband Communications Research (BBCR) Group, July 2012 [http://bbcr.uwaterloo.ca/~slcesped/vanet/index.html].
- Dar, K. and Bakhouya, M. and Gaber, J. and Wack, M. and Lorenz, P., "Wireless Communication Technologies for ITS Applications," IEEE Communications Magazine, vol. 48 (5), pp. 156-162, May 2010.

- Rashid A. Saeed¹, Amran Bin Hj Naemat, Azrin Bin Aris, Ir. Mat Khamis, Mat Kamil Bin Awang, “*Evaluation of the IEEE 802.11p-based TDMA MAC Method for Road Side-to-Vehicle Communications*”, International Journal of Network and Mobile Technologies- ISSN 1832-6758 Electronic Version - VOL 1 / ISSUE 2 / NOVEMBER 2010 - © 2010 INTI University College [<http://www.ijnmt.com/JournalPapers/Vol1No2/P7Vol1No2.pdf>].
- T.M. Kurihara, Chair, IEEE 1609 WG, William Whyte, “*Security Innovation. IEEE Standards Association (IEEE SA) - ITS Standards*”, 3rd ETSI TC-ITS Workshop 9-11 February 2011 – Venice [http://docbox.etsi.org/workshop/2011/201102_ITSWORKSHOP/08_INTERNATIONAL_ITS_STANDARDIZATION/IEEE_KURIHARA.pdf].
- Daniel Jiang, Luca Delgrossi, “*IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments*”, Mercedes-Benz Research & Development North America, Inc. , February 2012 [<http://wenku.baidu.com/view/786af922ccbff121dd3683d7.html>].
- Alessandro Falaschi, seminario Vehicular Ad Hoc Networks – Mobilità sostenibile - Regione Lazio, Dicembre 2009 [http://infocom.uniroma1.it/alef/seminario_vanet.pdf].
- Wikipedia <http://en.wikipedia.org/> .
- IEEE 1609 Working Group Public [http://vii.path.berkeley.edu/1609_wave/]
- Institute of Electrical and Electronics Engineers:
 - IEEE Std 802.11™ - 2012 (Revision of IEEE Std 802.11-2007) *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 29 March 2012.
 - IEEE Std 1609.1™ - 2006 - *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager*, 13 October 2006.
 - IEEE Std 1609.2™ - 2006 - *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments- Security Services for Applications and Management Messages*, 6 July 2006.
 - IEEE Std 1609.3™ - 2010 (Corrigendum to IEEE Std 1609.3-2010), *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Networking Services*, 13 July 2012.
 - IEEE Std 1609.4™ - 2010 (Revision of IEEE Std 1609.4-2006), “*IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Multi-channel*”, 7 February 2011.
 - IEEE-SA 1609 WG - Dedicated Short Range Communication Working Group.