Attività formativa: tesina

PROTOCOLLI DI TRASMISSIONE PER RETI VEICOLARI

Laureando: Diego Chinellato

Relatore: Andrea Zanella

Corso di laurea in Ingegneria delle Telecomunicazioni

Data: 26/4/2010

Anno accademico 2009/2010

Indice

Sommario

Negli ultimi anni si stanno studiando delle tecniche per aumentare la sicurezza durante la guida. L'idea che risale a quasi due decenni fa, è di trovare un modo per far comunicare tra loro i veicoli arrivando ad ottenere uno scambio continuo di informazioni per garantire una maggior sicurezza degli utenti della strada. In ordine con la trattazione verranno fornite prima le nozioni di base sulle comunicazioni interveicolari con relative spiegazioni dei vari impieghi e delle varie modalità di comunicazione, successivamente si passerà ad una trattazione più approfondita del livello fisico e MAC del protocollo di comunicazione proposto per tali servizi.

I. Introduzione

Il traffico stradale è in costante aumento in tutto il mondo come conseguenza di una crescente motorizzazione, urbanizzazione e della crescita demografica, nonché di un sostanziale cambiamento della densità di popolazione. In Italia oggigiorno le grandi città come Napoli Milano e Torino, sono quelle a maggior densità di popolazione nelle quali il problema del traffico è una realtà quotidiana. Recenti studi hanno fatto sapere che l'Italia gode del primato del numero di auto per abitante che sono ben 60 ogni 100 abitanti. L'alta densità automobilistica mette inevitabilmente a dura prova la rete di strade e autostrade presenti nella nostra penisola, provocando a volte disagi dovuti a congestioni del traffico, con conseguenti code spesso inevitabili. Oltre al traffico potremmo trovare molti altri problemi connessi alla grande massa di veicoli che si muovono ogni giorno sulle strade come, ad esempio, gli incidenti. È risaputo ormai che gli incidenti stradali sono dovuti principalmente a comportamenti scorretti del conducente e, in minoranza, ad altri fattori come, ad esempio, lo stato delle infrastrutture o avarie ai veicoli. Anche per questi motivi già due decenni fa si cominciò a pensare a una qualche soluzione per far fronte al problema. Più precisamente a partire dal 1991 il congresso degli Stati Uniti d`America nell' Intermodal Surface Transportation Efficiency Act (ISTEA), creò un programma chiamato Intelligent Vehicle Highway Systems (IVHS) i cui obbiettivi principali erano quelli di aumentare la sicurezza stradale, evitare le congestioni del traffico e ridurre l'inquinamento per salvaguardare i combustibili fossili destinati all'esaurimento. La responsabilità per il programma fu assegnata

alla U.S. Department of Trasportation (DOT) il quale chiese la consulenza della Intelligent Transportation Society of America (ITSA) per l'assegnazione del progetto. Nel 1996, DOT, ITSA e varie altre società interessate al progetto avevano sviluppato una struttura con le linee fondamentali che definivano i servizi IVHS o servizi di Intelligence Trasportation System (ITS) come sono chiamati oggi. Conosciuta come National Intelligent Transportation Systems Architecture (NITSA), questa struttura fu di riferimento per le molteplici iniziative di ITS nel corso dei tredici anni successivi. Fin dall'inizio, NITSA mostrò 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 dei pedaggi automatizzato (tipo Telepass), utilizzavano uno spettro tra 902MHz e 928MHz; purtroppo questa porzione di spettro era troppo stretta e affollata per poterla sfruttare con servizi di comunicazioni IVHS. Di conseguenza nel 1997 l'ITSA fece una petizione alla Federal Communication Commission (FCC) per ottenere 75MHz di banda allocati attorno a 5.9GHz con l'obbiettivo di utilizzare questo spettro per le Dedicated Short Range Communication (DSRC) per ITS. La FCC accettò la richiesta nell'ottobre del 1999 assegnando 75MHz di banda tra 5.85GHz e 5.925GHz a DSRC per ITS. Nel luglio del 2002, l'ITSA influenzò la commissione dell'FCC per quanto riguardavano le licenze, le norme e le possibili applicazioni dei servizi che potevano fornire le comunicazioni ITS-DSRC. L'ITSA consigliò l'adozione di uno standard unico per quanto riguardava il livello fisico (PHY) e il livello MAC e propose uno sviluppo in collaborazione con la American Society for Testing and Materials (ASTM) basando lo sviluppo su IEEE 802.11. La FCC accettò ufficialmente la proposta negli anni tra il 2003-2004. Nel 2004 un gruppo di ricercatori di IEEE prese in mano il progetto iniziato da ASTM e cominciò a sviluppare una versione dello standard 802.11 contenente nozioni sulle applicazioni veicolari. Il documento è conosciuto come 802.11p. Un altro gruppo di ricercatori di IEEE (conosciuto come gruppo 1609) era impegnato a sviluppare specifiche per completare anche gli altri livelli del protocollo. Oggi lo standard IEEE1609 è composto di quattro documenti IEEE1609.1, IEEE1609.2, IEEE1609.3 e IEEE1609.4.

Nel complesso i protocolli IEEE802.11 e IEEE1609.1-2-3-4 che ricoprono l'ambito delle comunicazioni interveicolari sono conosciuti come Wireless Access in Vehicular Environments (WAVE) e su questo argomento si articoleranno i prossimi paragrafi, con particolare attenzione per gli strati protocollari PHY e MAC.

II. Scenari di applicazione

Un sistema di comunicazioni interveicolare richiede un dispositivo montato in ogni veicolo e dei dispositivi presenti lungo le strade. I primi, chiamati On Board Unit (OBU), sono responsabili delle comunicazioni che avvengono tra due o più veicoli, Vehicle-to-Vehicle communication (V2V), e delle comunicazioni con le stazioni radio ai lati della strada, Vehicle-to-Infrastructure communication (V2I). Queste unità devono essere dotate di almeno un dispositivo di rete per le comunicazioni a corto raggio DSRC che viene utilizzato per inviare, ricevere e inoltrare informazioni di sicurezza ad altri veicoli. Inoltre gli OBU possono essere equipaggiati con altri dispositivi di rete per comunicazioni non inerenti alla sicurezza basate sugli standard 802.11a/b/g/n.
Le funzioni di un dispositivo OBU sono:

- fornire una connessione wireless
- eseguire il routing ad hoc geografico
- controllo della congestione della rete (Vehicular Ad hoc NETwork)
- trasferimento affidabile e sicuro di messaggi
- supporto alla mobilità per il protocollo IP

I dispositivi posti lungo le strade sono chiamati Road Side Unit (RSU) e possono essere installati in un qualsiasi posto utile come ristoranti, distributori di carburante, semafori. Sono dotati di un dispositivo di rete per supportare comunicazioni DSRC basato sullo standard 802.11p e di altri dispositivi per la comunicazione con la rete di infrastrutture. Le principali funzioni di un RSU sono:

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

Possiamo ora analizzare i vantaggi che portano l'utilizzo di questi sistemi a partire dal settore della sicurezza attiva, tema attuale molto importante per passare poi all'utilizzo nella gestione del traffico e infine all'uso di questi sistemi per applicazioni internet.

Prevenzione della collisione

Le cause tipiche di tamponamenti tra veicoli sono la distrazione dei conducenti o la frenata improvvisa del veicolo che ci precede. Questi inconvenienti possono essere evitati quando siamo in presenza di veicoli che durante la marcia comunicano tra loro scambiandosi informazioni sulla propria posizione, velocità e direzione. Ogni veicolo tiene monitorato il comportamento del proprio conducente, la propria posizione e il comportamento di tutti i veicoli nelle vicinanze. Quando il veicolo rileva che ci potrebbe essere un pericolo imminente avverte il guidatore con un segnale visivo o uditivo così il conducente avrà abbastanza tempo per poter intervenire. In aggiunta a questo sistema che prevede comunicazioni wireless possiamo affiancare l'utilizzo di sensori per identificare veicoli che non sono dotati di sistemi di comunicazioni interveicolari.

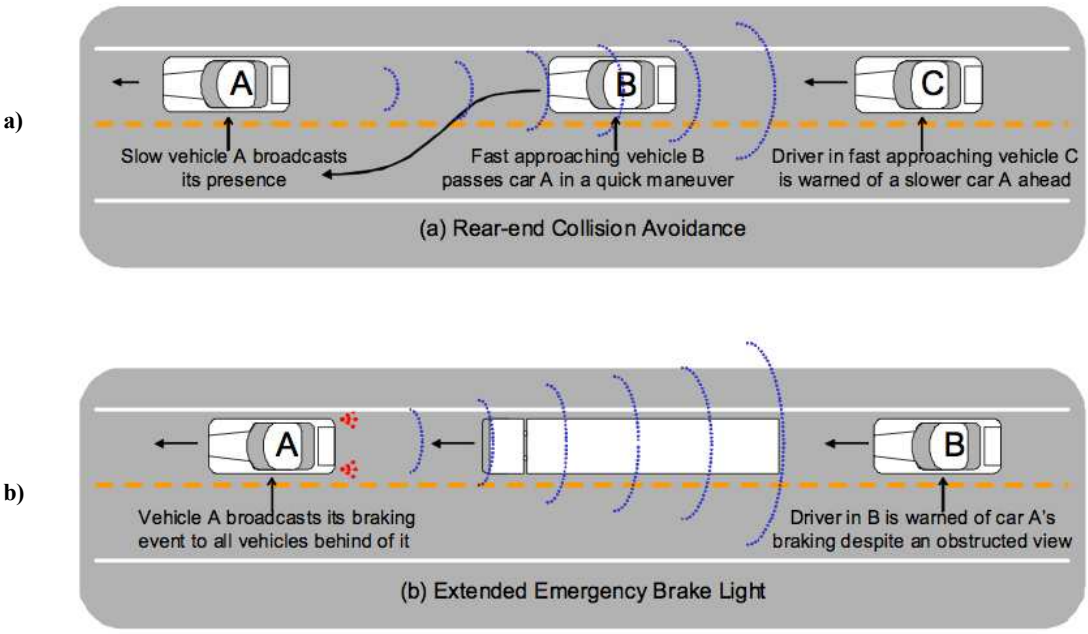


Figura 1 - Esempio di applicazioni delle comunicazioni interveicolari [3]: a) veicolo A avanza lentamente nella corsia di marcia b) frenata improvvisa del veicolo A

Avvertimento pre-crash

L'avvertimento pre-crash è un possibile utilizzo delle comunicazioni veicolari; serve per ottimizzare l'utilizzo dei sistemi di protezione dei passeggeri in caso di collisione imminente e inevitabile. Quando uno o più veicoli si trovano in una situazione in cui la prevenzione non è sufficiente ad evitare lo scontro si passa ad una fase successiva di utilizzo ottimale delle risorse di sicurezza passiva presenti nel veicolo. I mezzi che stanno per essere coinvolti nello scontro scambiano informazioni in modo veloce e affidabile sulla posizione del veicolo

rispetto agli altri e sulle sue dimensioni. Questo scambio di informazioni supplementari permette di utilizzare al meglio air bag, pre-tensionatori delle cinture di sicurezza e paraurti allungabili.

Segnalazione di zone pericolose

Le notifiche che avvertono la presenza di elementi pericolosi sulla strada sfrutta la rete formata dai veicoli presenti nei dintorni. I veicoli scambiano informazioni utili tra loro come la presenza di manto stradale scivoloso, o di qualche ostacolo. Questo scambio di messaggi tra veicoli è reso possibile grazie all'utilizzo di sensori già esistenti su molti veicoli, come l'Elettronic Stability Program meglio conosciuto come ESP. Tutti i veicoli che ricevono le informazioni possono avvertire il proprio conducente o ottimizzare automaticamente l'assetto del veicolo. Le informazioni utili possono essere inoltrate di veicolo in veicolo per avvertire anche quelli che sopraggiungeranno nel tratto di strada pericoloso.

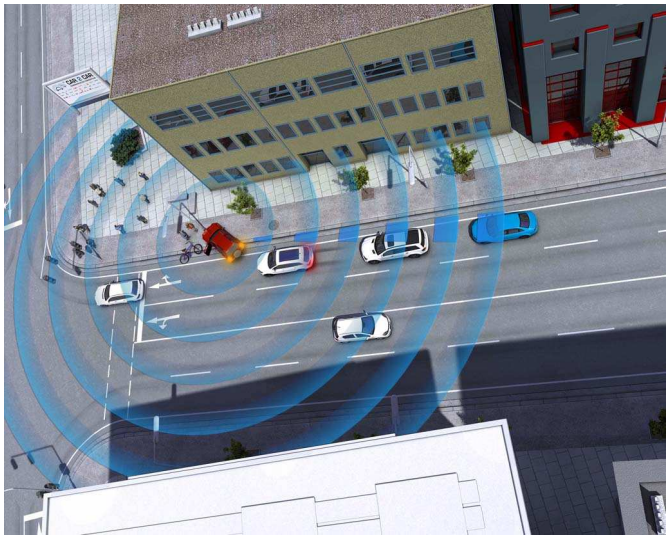


Figura 2 - Esempio di avvertimento zona pericolosa [9]

Gestione del traffico

Gli utilizzi delle comunicazioni veicolari per la gestione del traffico sono quelle che hanno lo scopo di migliorare l'efficienza della rete di trasposto automobilistica con il duplice vantaggio di fornire informazioni utili sia ai veicoli che vi transitano che ai proprietari della rete (ad esempio nelle autostrade). Un sistema di trasporto più efficiente riduce i ritardi negli spostamenti ed evita congestioni del traffico grazie al costante scambio di informazioni tra più

veicoli (comunicazioni V2V) e tra veicoli e stazioni apposite poste ai lati delle strade (comunicazioni V2I). Il proprietario della rete di trasporto rileva le informazioni che i veicoli in transito si scambiano per prevenire eventuali congestioni. Tutti questi dati raccolti (che possono interessare anche una vasta area geografica) vengono poi elaborati e ritrasmessi dalle stazioni radio (RSUs) poste ai bordi delle carreggiate verso i dispositivi presenti nelle auto (OBUs) informando il conducente sulle condizioni del traffico e sugli eventuali percorsi alternativi da seguire. Un'altra applicazione molto utile per gestire il traffico in città consiste nell'utilizzare questo tipo di comunicazioni per informare i conducenti dei veicoli della velocità ottimale da tenere per avere un'alta probabilità che il semaforo che si trova lungo il percorso sia verde al nostro attraversamento. Questo ha un'immediata conseguenza nel favorire lo smaltimento del traffico e ridurre il più possibile il consumo di ogni veicolo. In fig.3 possiamo vedere un esempio di scenario cittadino in cui una via è bloccata perciò tutti i veicoli che si accingono ad imboccarla vengono preventivamente avvisati e viene consigliato loro un percorso alternativo da seguire (evidenziato in verde).

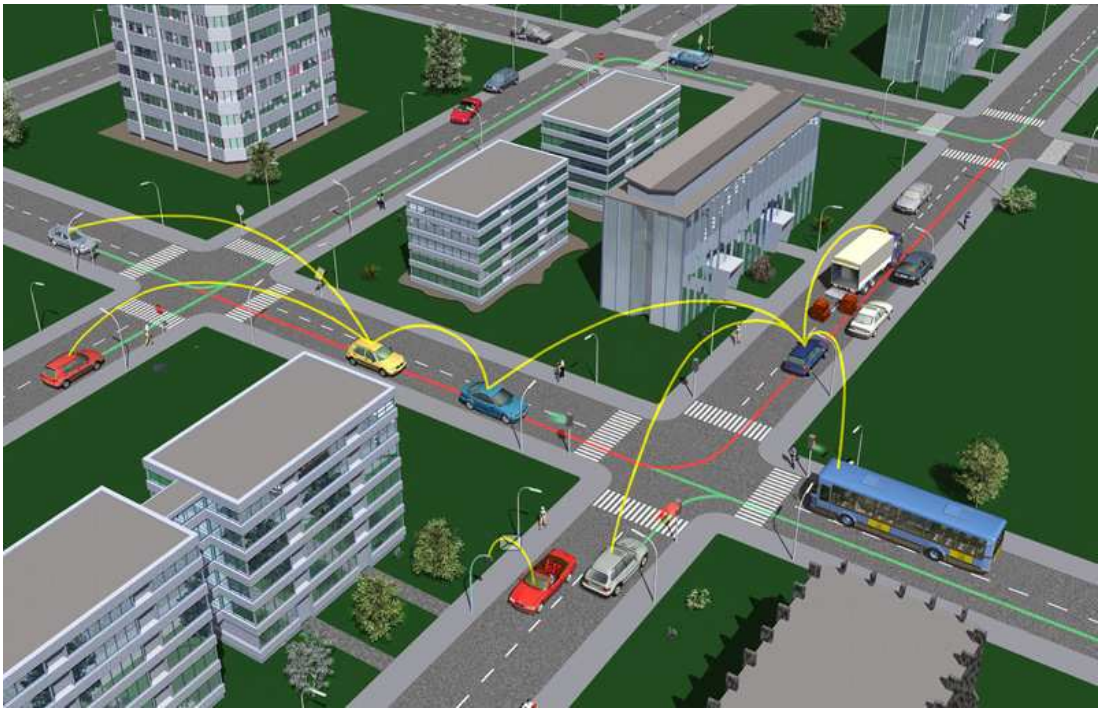


Figura 3 - Esempio di scenario urbano con strada bloccata [9]

Accesso a Internet

Esistono molte altre applicazioni che sono complementari a quelle per la sicurezza e la gestione del traffico come la possibilità di navigare in internet dalla propria auto attraverso le

comunicazioni V2I permettendo l'utilizzo di tutte quelle applicazioni basate sul protocollo IP. Le stazioni radio base RSU fungono da gateway per l'accesso alla rete internet mantenendo una connessione stabile con il veicolo. Questo è possibile perché viene eseguito un instradamento dei pacchetti IP cosiddetto “multi-hop”: il veicolo muovendosi interagisce con diversi RSU posti lungo il suo percorso ma questa tecnica è trasparente ai livelli protocollari superiori che vedono comunque una connessione Internet stabile. Sfruttando una connessione di questo tipo, le stazioni RSU possono trasmettere a tutti i veicoli in zona qualsiasi tipo di informazioni, come la disponibilità di alberghi, ristoranti, stazioni di rifornimento e i relativi prezzi nonché recapiti telefonici e qualsiasi altra informazione utile. Infine un'ulteriore applicazione può essere, in caso di avaria del veicolo, la trasmissione di informazioni necessarie all'officina meccanica autorizzata più vicina per intervenire nel minor tempo possibile.

III. Architettura del sistema

Canale radio dedicato per DSRC

Tutte le applicazioni appena descritte utilizzano lo spettro DSRC che va dai 5.85GHz ai 5.925GHz con centro banda a 5.9GHz.

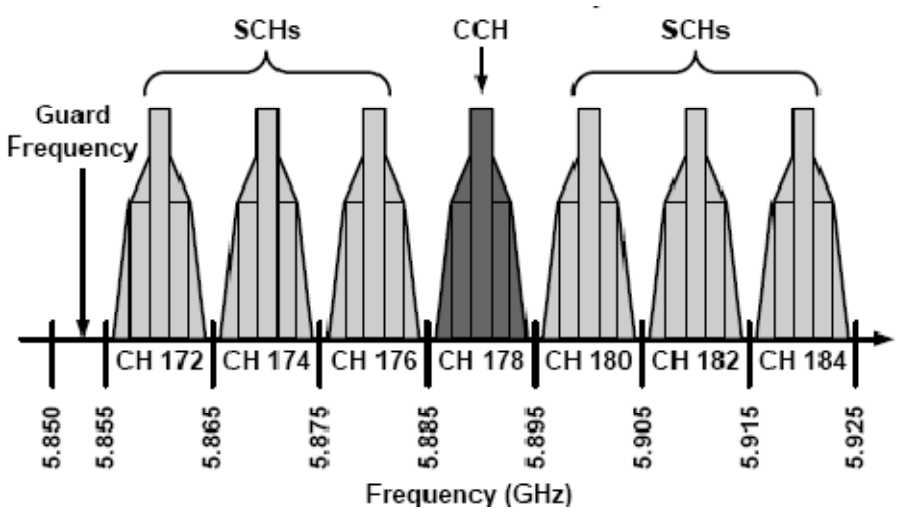


Figura 4- canale dedicato per le DSRC

Questi 75MHz sono suddivisi in sette sottocanali da 10MHz l'uno. Il canale 178 è il Control Channel (CCH) riservato esclusivamente alle comunicazioni di sicurezza. I canali restanti denominati Service Channel (SCH) sono utilizzati anche per altre applicazioni. La banda DSRC è con licenza e non deve essere confusa con la banda senza licenze a 900MHz, 2.4GHz e 5GHz. Queste bande libere da licenze hanno reso possibile lo sviluppo di sistemi come WiFi e Bluetooth. La banda DSRC rispetto alle altre prive di licenza è regolata da diverse norme come l'utilizzo di un determinato standard. In Europa si stanno accordando per allocare 30MHz di banda alla frequenza di 5GHz per le comunicazioni interveicolari, come è già stato fatto negli USA.

Architettura del protocollo per DSRC

Lo standard per DSRC è essenzialmente un aggiustamento ad hoc dello standard 802.11 finalizzato a ridurre il più possibile le dimensioni del pacchetto da inviare tramite il collegamento radio. Nella famiglia IEEE 802.11, il protocollo per le DSRC è meglio conosciuto come IEEE802.11p Wireless Access in Vehicular Environments (WAVE).

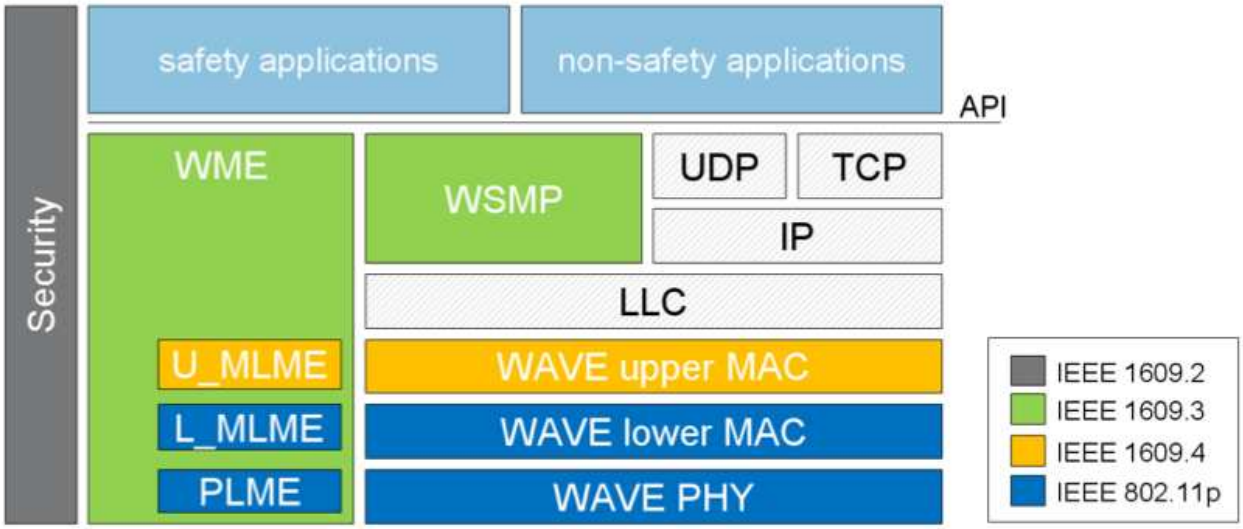


Figura 5 - Stack protocollare per comunicazioni DSRC [3]

Questo standard si occupa di descrivere le funzioni e i servizi richiesti per operare in rapidità scambiando messaggi senza avere a disposizione un Basic Service Set come avviene utilizzando lo standard IEEE802.11. Inoltre definisce le tecniche di segnalazione e le funzioni di interfaccia che sono controllate dal livello MAC. La pila protocollare che definisce lo standard per le comunicazioni interveicolari è composto da diversi protocolli oltre a 802.11p dei quali verrà fornita solo una breve spiegazione.

IEEE1609.1 è lo standard che definisce:

- i componenti di WAVE
- le interfacce e le risorse
- i formati dei messaggi e di memorizzazione
- i dispositivi che equipaggiano gli OBU

IEEE1609.2 è lo standard che definisce:

- i formati sicuri di messaggio e la loro elaborazione
- le circostanze in cui usare gli scambi sicuri di messaggi

IEEE1609.3 è lo standard che definisce:

- i servizi offerti dagli strati di rete e di trasporto, inclusi indirizzamento e instradamento, in supporto agli scambi sicuri
- il WAVE Short Messages Protocol (WSMP), una efficiente alternativa ad IP che permette alle applicazioni di controllare canale e potenza di trasmissione

IEEE1609.4 è lo standard che definisce:

- gli arricchimenti al MAC 802.11 per operare in modalità WAVE, permettendo il coordinamento e la gestione dei diversi canali
- offre un collegamento logico agli strati protocollari superiori senza preoccuparsi di come avviene lo scambio di informazioni a livello fisico.

IEEE802.11p è lo standard che definisce:

- le funzioni e i servizi richiesti dalle stazioni WAVE per operare in un ambiente che varia spesso e rapidamente scambiando messaggi senza la necessità di creare una BSS
- le tecniche di segnalazione e le funzioni di interfaccia che sono controllate dal livello MAC

Funzioni del livello MAC

Come abbiamo detto nel paragrafo precedente lo standard IEEE 802.11p è basato sul già esistente e collaudato IEEE 802.11, con alcune modifiche per essere applicato alle comunicazioni veicolari. Nella strato protocollare MAC di 802.11 il principio di funzionamento si basa sullo scambio di informazioni preliminari per stabilire e mantenere una connessione sicura. L'idea proposta da IEEE802.11p è riuscire a creare una comunicazione molto efficiente senza il pesante overhead tipicamente presente in 802.11 MAC e questo a vantaggio della velocità di trasmissione per l'utilizzo nelle reti veicolari. Una rete basata sullo standard IEEE802.11 è chiamata Basic Service Set e si compone di un certo numero di stazioni wireless e di un Access Point (AP). Per stabilire la connessione è necessario effettuare l'autenticazione e l'associazione e questo comporta lo scambio di messaggi denominati Beacon. Una BSS è riconosciuta dall'utente grazie al Service Set Identification (SSID) che corrisponde al nome visualizzato quando andiamo a connettere il computer alla rete. Il SSID non deve essere confuso con il Basic SSID (BSSID) che corrisponde al nome con cui la rete è riconosciuta a livello MAC. Ogni BSS ha un unico BSSID a livello mondiale che, nelle reti basate sullo standard IEEE 802.11, è l'indirizzo MAC dell'AP. Nelle reti “ad hoc” l'indirizzo IBSS viene fornito dall'amministratore locale di quella rete, ad esempio da uno dei computer. Il filtraggio degli indirizzi BSSID a livello MAC è il metodo per riconoscere mittente e destinatario in ogni BSS.

La Fig.6 mostra il formato di un pacchetto dati dello standard 802.11, che è composto da quattro campi di indirizzo, rispettivamente Source Address (SA), Destination Address (DA), Transmitting Station Address (TA), Receiving Station Address (RA). Come possiamo notare

dalla fig.6 i campi indirizzo sono composti da 6 ottetti, perciò abbiamo uno spazio di indirizzamento di $2^{48} \simeq 2.81 \cdot 10^{14}$unità. Questo perché ogni campo *address* deve essere in grado di identificare qualsiasi indirizzo MAC, unico a livello mondiale.

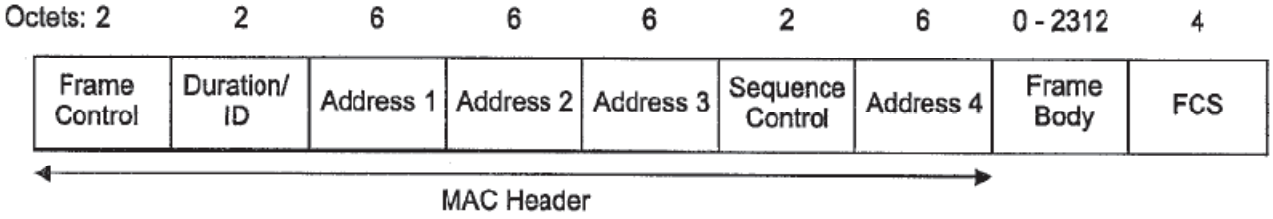


Figura 6-datagramma di 802.11 [6]

Le operazioni di autenticazione e associazione sono troppo onerose per essere adottate in IEEE 802.11p. Le comunicazioni tra veicoli richiedono, soprattutto in caso di comunicazioni di sicurezza, la capacità di scambiare dati rapidamente, il che rende inefficiente la procedura di adesione utilizzata in 802.11. Pertanto è essenziale per tutti i dispositivi basati su 802.11p essere settati sullo stesso canale e configurati con lo stesso indirizzo MAC (BSSID). La novità introdotta da IEEE802.11p WAVE è proprio il termine WAVE che sta ad indicare la configurazione della stazione radio in "modalità WAVE". Questa permette alla stazione di trasmettere e ricevere pacchetti di dati senza la necessità di appartenere ad una determinata BSS. Ugualmente, per le comunicazioni non legate alla sicurezza, l'overhead di una tradizionale BSS è troppo dispendioso per questo in 802.11p viene introdotto un nuovo concetto di BSS: il Wave BSS (WBSS). Una stazione forma una WBSS utilizzando un pacchetto di richiesta denominato *Beacon*; a sua volta la stazione ricevente diffonde il messaggio di beacon a stazioni radio vicine in modo tale da espandere la WBSS. La richiesta di creare una WBSS viene 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. In caso di adesione, nel pacchetto di richiesta sono contenute anche tutte le informazioni necessarie per auto configurarsi come stazione della WBSS. Notiamo che questa procedura di interazione è molto veloce perché permette di creare una connessione stabile tra più unità semplicemente con lo scambio di un pacchetto (beacon) di richiesta e non c'è bisogno di ulteriori interazioni per completare il processo di adesione. Questo approccio offre overhead estremamente ridotti per la creazione di una rete tra veicoli evitando processi di associazione e autenticazione. Per far funzionare correttamente la rete servono ulteriori meccanismi gestiti a livelli superiori, ad esempio garantire la sicurezza della trasmissione, ma questi esulano dallo scopo della trattazione dello standard 802.11p.

Nelle applicazioni per la sicurezza è supportato da tutte le stazioni l'utilizzo dell'indirizzo speciale BSSID (wildcard BSSID). Questo significa che se un veicolo facente parte di una

WSSB deve trasmettere una segnalazione per la sicurezza, può inviare il pacchetto con l'indirizzo speciale in modo che questo sia ricevuto da tutti i veicoli nei dintorni, anche se non compresi nella sua WSSB. Allo stesso modo veicoli che ricevono pacchetti con l'indirizzo speciale BSSID possono utilizzarlo anche se non facenti parte delle WSSB della stazione trasmittente. I pacchetti che possono essere trasmessi anche alle unità al di fuori della propria WBSS vengono ricevuti solo se contengono l'indirizzo speciale BSSID perché, in genere, ogni stazione a livello MAC filtra i pacchetti ricevuti conservando solamente quelli provenienti dalla stessa WSSB a cui appartiene la stazione ricevente.

Le innovazioni principali a livello MAC sono:

- una stazione in modalità WAVE può inviare e ricevere pacchetti dati con indirizzo speciale BSSID indipendentemente dal fatto di essere o meno membro della stessa WBSS.
- Una WBSS è un tipo di BSS che consiste in una serie di stazioni (veicoli) che cooperano tra loro in modalità WAVE e che comunicano utilizzando uno stesso indirizzo BSSID. Una WBSS è inizializzata quando una stazione in modalità WAVE invia un "WAVE beacon" nel quale include tutte le informazioni necessarie perché il ricevitore si configuri alla WBSS.
- Un stazione entra a far parte di una WBSS quando è configurata per inviare e ricevere pacchetti con indirizzo BSSID definiti per quella WBSS. Viceversa cessa di far parte di una WBSS quando il livello MAC interrompe la ricezione e l'invio di pacchetti dati contenenti l'indirizzo BSSID di quella WBSS.
- Una stazione non può essere membro di più di una WBSS contemporaneamente.
- Una WBSS cessa di esistere quando non ci sono membri che la compongono. Inoltre la prima unità che richiede la creazione della WBSS invia un messaggio che è uguale a quello che utilizzano poi tutti gli altri veicoli quindi quando il primo membro che ha generato la richiesta di formare la WBSS si dissocia, quest'ultima continua ad esistere.

Funzioni del livello fisico

A livello fisico la filosofia di 802.11p è quella di apportare cambiamenti minimi rispetto alla già esistente 802.11 PHY in modo da ottimizzare quest'ultima per l'utilizzo nelle reti veicolari. Questo approccio è fattibile perché IEEE 802.11a opera alla frequenza di 5 GHz e non è difficile configurarlo per renderlo operativo a 5.9 GHz. Mentre gli aggiornamenti a livello

MAC sono relativamente semplici, richiedendo solo un aggiornamento software, gli aggiornamenti a livello fisico sono più complicati per cui si è cercato il più possibile di sfruttare 802.11a per evitare di creare una nuova tecnologia di collegamento radio. IEEE 802.11p è essenzialmente basato sulla tecnica di modulazione OFDM con una larghezza di banda del canale di 10MHz anziché i 20MHz di 802.11a. Il motivo principale di questa scelta è ridurre gli effetti di rumore introdotti dal canale radio.

IV. Modalità di comunicazione

Un aspetto molto importante per le comunicazioni veicolari è la velocità di spostamento dei nodi che vogliono comunicare. Si passa da situazioni in cui l'unità è ferma, come nel caso delle RSU fissata a bordo strada, a situazioni in cui i veicoli viaggiano a velocità molto elevate, ad esempio nelle autostrade. Le alte velocità dei veicoli portano a una riduzione del tempo in cui essi sono in copertura di un'altra OBU o di una RSU: ad esempio, due automobili che viaggiano in direzioni opposte a una velocità di 90Km/h e con antenna tale da avere un raggio di copertura di 300m, hanno solamente 12 secondi utili per la comunicazione. Inoltre, ad alte velocità il ricetrasmettitore di ogni veicolo si trova a far fronte all'effetto Doppler. Questo effetto fisico genera uno scostamento della frequenza del segnale ricevuto rispetto a quello trasmesso di un valore che dipende dalla velocità relativa dei veicoli e dalla frequenza del segnale originario.

$$\Delta f \cong \pm f_0 \frac{v}{c}$$

Ad esempio se un veicolo che trasmette segnali a frequenza di 5.9 GHz viaggia ad una velocità di 100 Km/h la variazione di frequenza del segnale ricevuto da un'unità ferma in un certo punto sarà

$$\Delta f \cong \pm 5.9 \times 10^9 \frac{27.8}{3 \times 10^8} \cong 546.73 Hz$$

Diversamente, quando i veicoli sono fermi o viaggiano a velocità molto basse la topologia della rete è molto stabile. Il grafico in fig.7a mette a confronto la durata del collegamento radio con la portata dell'antenna e possiamo notare che la durata media dei collegamenti che si instaurano con tutti i veicoli durante il percorso (sia nella stessa direzione di marcia che opposta) è di circa 17s. In fig.7b viene messa a confronto la capacità dei vari nodi di comunicare tra loro (connettività) in funzione della portata delle antenne dei veicoli.

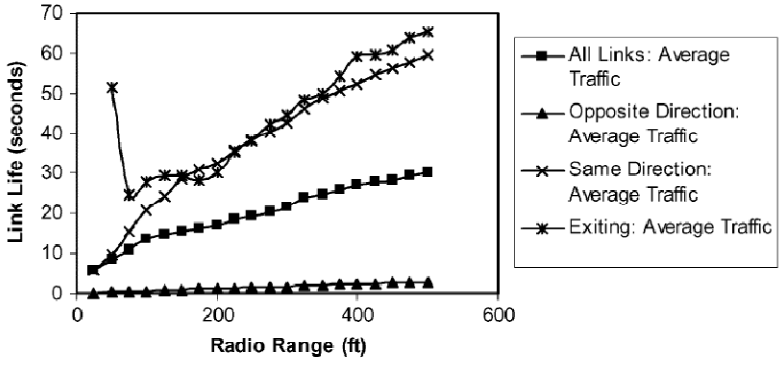


Figura 7 a - Durata del collegamento radio in funzione della portata dell'antenna [12]

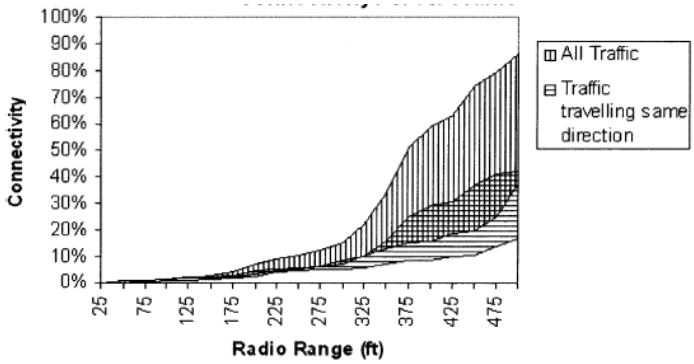


Figura 7b - Connettività in funzione della portata dell'antenna [12]

I veicoli in genere non si muovono casualmente, essendo vincolati a rimanere nel tracciato stradale in entrambi i sensi di marcia. Le uniche variazioni di traiettoria dei veicoli sono agli incroci o alle rotatorie. Vengono distinti tre diversi tipi di strade:

Le strade di città, dove il traffico è intenso e ci sono numerosi incroci. Inoltre le costruzioni presenti ai lati delle strade spesso limitano le comunicazioni radio. Le strade fuori città invece hanno una bassa densità di veicoli sfavorendo la formazione di eventuali reti che in città possono formarsi con più facilità. Le autostrade invece sono con traffico variabile ma ad alta velocità. La direzione dei veicoli è pressoché costante e in queste situazioni si possono formare reti tra unità che viaggiano nella stessa direzione come si può valutare anche dai grafici in fig.7.

La densità dei nodi presenti nelle strade rappresenta un'altra proprietà delle reti veicolari. Non è difficile immaginare che il numero di veicoli presenti nell'area coperta dall'antenna di una OBU può variare da zero a più di un centinaio; basti pensare che con la portata dell'antenna di 300m in una situazione di traffico congestionato su un'autostrada a quattro corsie può portare rapidamente il numero di veicoli nel range di trasmissione di ogni OBU a più di un centinaio di unità. In caso di basse densità di veicoli un messaggio può essere continuamente ripetuto finché non si incrocia un altro veicolo che lo riceverà correttamente. Nelle situazioni di alta densità invece si deve regolare la ripetizione dei messaggi altrimenti si rischia la saturazione del canale di trasmissione. La densità dei nodi non dipende essenzialmente dal tipo di strada (come la velocità) ma dalle fasce orarie; in orari di punta il traffico sarà più intenso mentre durante la notte circoleranno molti meno veicoli per le strade.

Si è visto nel capitolo II che le applicazioni per le reti veicolari sono molteplici ma le caratteristiche della rete le rendono talvolta di difficile applicazione. Tuttavia la maggior parte

delle applicazioni si appoggia su dei metodi di comunicazione di base; questi metodi non fanno riferimento alle tecnologie di comunicazione, semplicemente richiedono la possibilità di comunicazioni di tipo *broadcast* e *unicast*. Su questi modi elementari di comunicazioni potranno essere basate tutte le applicazioni attuali e future.

Beaconing

I messaggi di Beacon vengono inviati da tutti i veicoli alle unità limitrofe ad intervalli regolari compresi tra 0.1s e 1s. Questi messaggi hanno una dimensione di 8 byte e possono contenere l'identità del veicolo, la posizione, la direzione e la velocità nonché messaggi derivanti da qualche sensore attivo. Inoltre i beacon concorrono alla consapevolezza cooperativa cioè prima di inviare nuovi beacon ogni veicolo elabora i dati ricevuti dai veicoli adiacenti modificando i parametri del prossimo messaggio da inviare se necessario. I messaggi sono inviati nel canale in modalità broadcast a tutti i veicoli che rientrano nella portata dell'antenna. Solitamente questi messaggi vengono inoltrati a intervalli temporali costanti ma potrebbe accadere che a causa di un evento come un incidente questi vengano inoltrati al di fuori dell'intervallo periodico regolare. I beacon, essendo informazioni aggiuntive, hanno la priorità più bassa tra tutti i tipi di messaggi che possono essere inviati nel canale radio.

Esempi di applicazioni che utilizzano questo sistema di comunicazione sono:

- Assistente di svolta a sinistra
- Cooperazione con altri veicoli per adattare la velocità di marcia

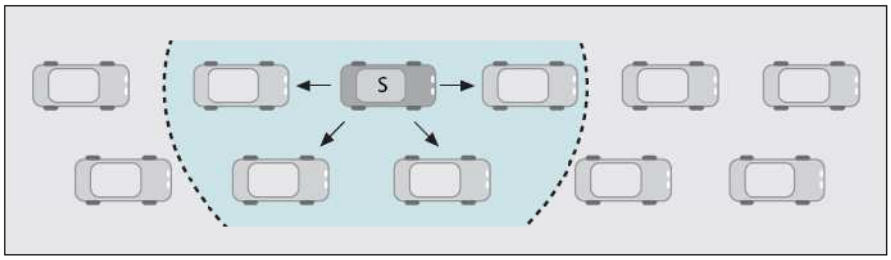


Figura 8 - Beaconing, messaggi periodici inviati in Broadcast [8]

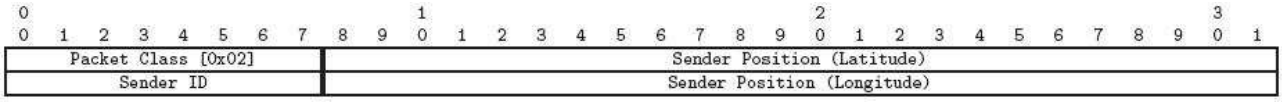


Figura 9 - Header di un Beacon [12]

Geobroadcast

Consiste nell'immediato invio di informazioni in una determinata area per informare i veicoli in quella zona di eventi improvvisi e condizioni anomale. Il mittente seleziona la zona dove destinare le informazioni e inserisce questa informazione all'interno del messaggio. Questo viene inviato in modalità broadcast a tutti i veicoli che si trovano nel range di trasmissione. A sua volta tutti i ricevitori che si trovano coinvolti (e che rientrano nell'area specificata) inoltrano, se necessario, il messaggio in broadcast. I messaggi in geobroadcast non sono inviati continuamente come i beacon, ma solamente all'occorrenza. La priorità dei messaggi è maggiore di quella dei Beacon.
Esempi di applicazioni che utilizzano questo sistema di comunicazione sono:

- Avvisi di lavori in corso sulla carreggiata
- Avvisi di incidente

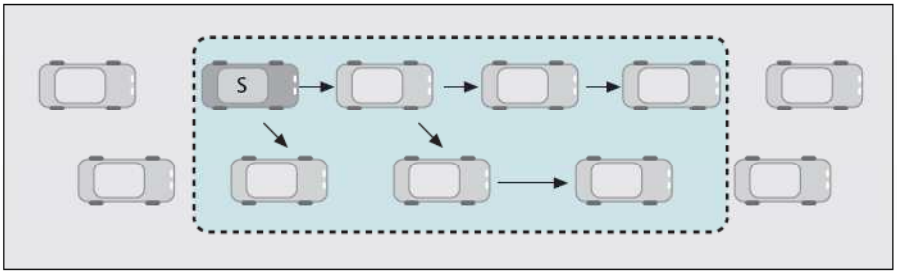


Figura 10 - Esempio di Geobroadcast inizializzato dal veicolo S e destinato ai veicoli nell'area tratteggiata [8]

Unicast Routing

In questo caso la rete veicolare viene utilizzata per recapitare dei messaggi ad un unico destinatario (unicast), cioè instaurare un collegamento punto-punto tra due veicoli. Per effettuare una comunicazione di questo tipo il nodo mittente deve avere l'informazione sulla posizione del veicolo destinatario perché quest'ultimo durante la trasmissione dei dati può muoversi. A tal fine ogni veicolo contiene in memoria una tabella (*neighbor table*) nella quale sono registrate le identità dei nodi vicini e la loro posizione fornita tramite GPS. Le tabelle vengono aggiornate di continuo in base alle informazioni presenti nei messaggi di beacon. Perciò il veicolo che trasmette in base alla posizione del veicolo destinatario decide a quale unità adiacente affidare il trasposto del messaggio. I messaggi di questo tipo possono essere unidirezionali o bidirezionali e nel secondo caso viene richiesta una comunicazione *connection-oriented* a differenza di molte applicazioni per la sicurezza nelle quali si usa una

comunicazione unidirezionale. Solitamente i messaggi unicast non sono messaggi legati alla sicurezza perciò hanno una minore priorità rispetto a questi.
Esempi di applicazioni che utilizzano questo sistema di comunicazione sono:

- Notifica di incidente ad un centralino di gestione del traffico

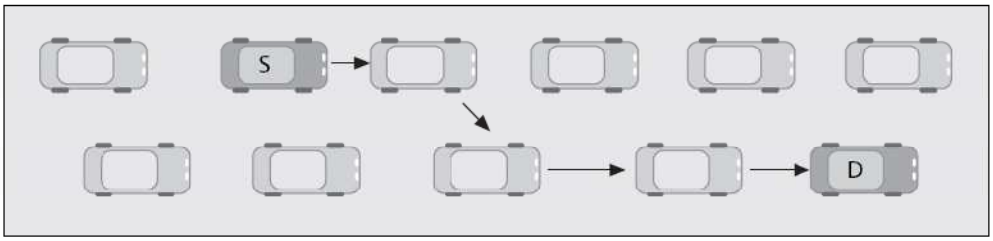
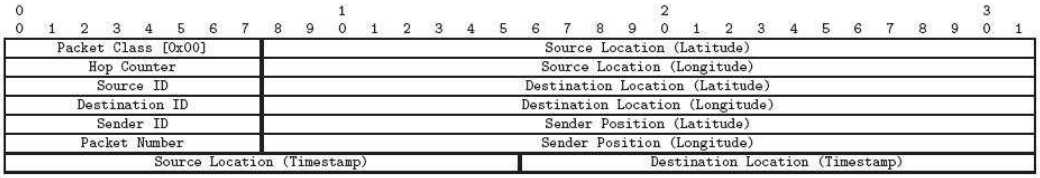


Figura 11 - Esempio di Unicast Routing inizializzato dal veicolo S e destinato al veicolo D [8]



Packet Class [0x00]	Source Location (Latitude)
Hop Counter	Source Location (Longitude)
Source ID	Destination Location (Latitude)
Destination ID	Destination Location (Longitude)
Sender ID	Sender Position (Latitude)
Packet Number	Sender Position (Longitude)
Source Location (Timestamp)	Destination Location (Timestamp)

Figura 12 - Header di un pacchetto dati Unicast [12]

Diffusione di informazioni (*information dissemination*)

Questo tipo di comunicazioni hanno lo scopo di mantenere vivo uno scambio di informazioni per prolungati periodi di tempo mantenendo informati anche veicoli che sopraggiungono in tempi successivi. Ogni messaggio viene memorizzato e inoltrato (tecnica *store-and-forward*) dai vari nodi e ad ognuno viene assegnata una priorità per evitare di sovraccaricare il canale trasmissivo.
Esempi di applicazioni che utilizzano questo sistema di comunicazione sono:

- avvisi di avvicinamento di ambulanze
- avvisi di condizioni anomale della strada

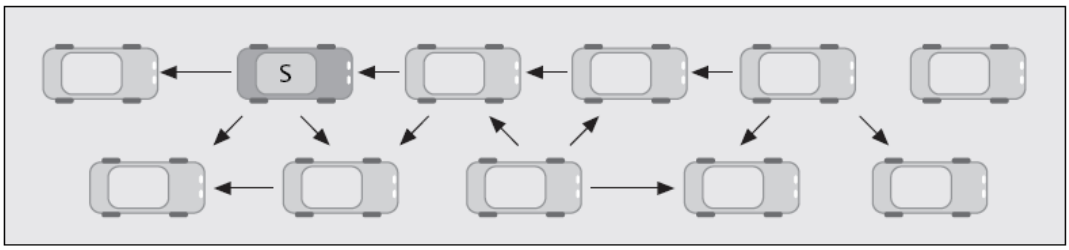


Figura 13 - Esempio di information dissemination [8]

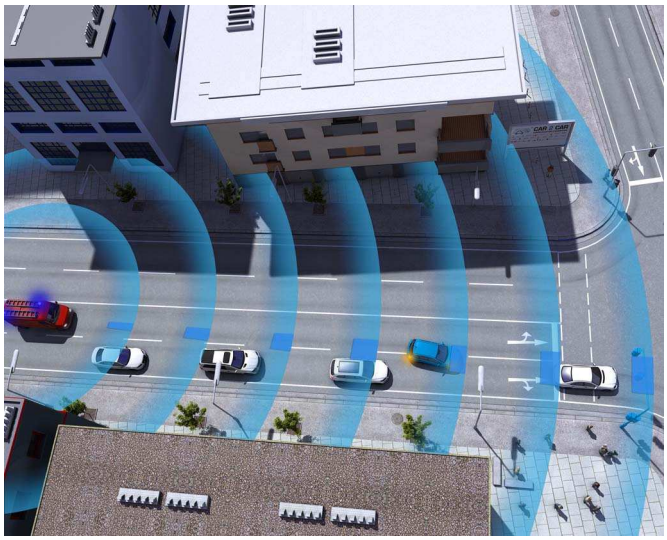


Figura 14 - Esempio di avviso avvicinamento mezzi di soccorso [9]

Aggregazione di informazioni (*information aggregation*)

In questo metodo di comunicazione i dati ricevuti via radio dai veicoli vengono ricevuti ed elaborati piuttosto che inoltrati direttamente come accadeva nella diffusione di informazioni. Ha l'obbiettivo di ridurre il sovraccarico del canale trasmissivo quando un evento viene notificato da più veicoli. Inoltre la collaborazione cooperativa tra le varie unità fa si che ad ogni messaggio ricevuto si arricchiscano le conoscenze di ogni veicolo sullo stato di quelli adiacenti. In altre parole, ogni messaggio ricevuto viene elaborato e in base ai dati ricevuti viene deciso cosa inviare alle altre unità circostanti. L'invio di questo tipo di messaggi può avvenire a intervalli temporali definiti o su richiesta da parte di qualche unità. Un tipo di comunicazione come questo non può essere utilizzato da applicazioni che sono sensibili ai tempi di consegna dei messaggi, come applicazioni di sicurezza.

Esempi di applicazioni che utilizzano questo sistema di comunicazione sono:

- Gestione intelligente del flusso di traffico
- Servizio di individuazione parcheggio

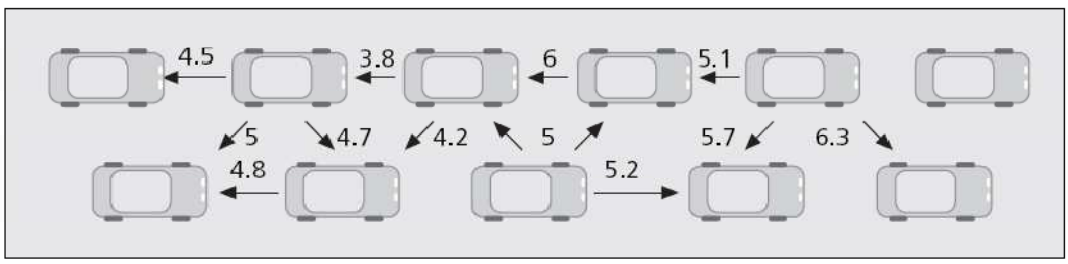


Figura 15 - Esempio di information aggregation [8]

V. Livello fisico 802.11p

Modulazione OFDM

Il livello fisico di 802.11p è basato essenzialmente sullo standard IEEE 802.11a con delle modifiche per meglio adattarsi alle condizioni di utilizzo. La modulazione utilizzata è l'Orthogonal Frequency Division Modulation (OFDM) basata su FDM per suddividere i 75 MHz del canale in sette sottocanali da 10 MHz. Su ognuno di questi è utilizzata una modulazione discreta multi tono (DMT). Come possiamo notare dalla figura sottostante ogni sottoportante è distanziata di 156.25 kHz. L'intervallo di guardia tra i canali è invece pari a 12*156.25 kHz = 1.875 MHz.

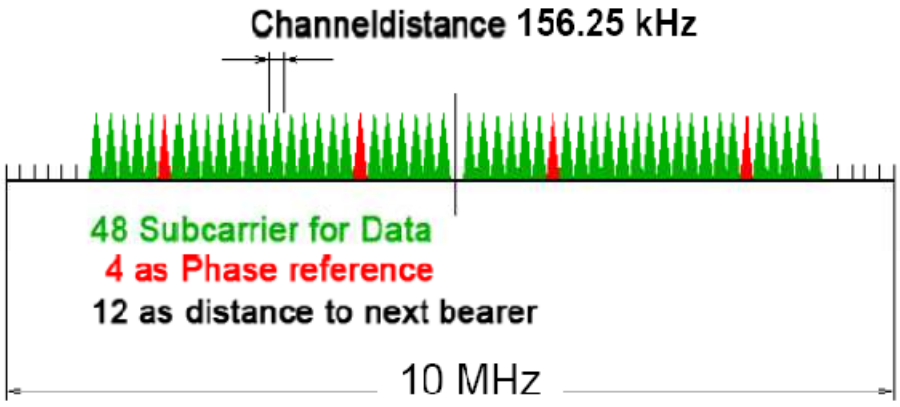


Figura 16 - Conformazione sottocanali SCH e CCH [10]

Ogni sottoportante è modulata con delle tecniche di modulazione tradizionali tipo QAM o PSK, ognuna con bassa frequenza di simbolo (symbol rate), ma la velocità di trasmissione totale è paragonabile ad una modulazione a singola portante sulla larghezza di banda di 10 MHz. Il vantaggio principale della modulazione OFDM è la sua adattabilità alle condizioni del canale radio dovute, ad esempio, all'attenuazione alle varie frequenze e ai fenomeni di fading causati dai cammini multipli delle onde radio, senza ricorrere all'uso di filtri equalizzatori. L'equalizzazione del canale avviene in modo molto più semplice perché nell'intervallo di frequenze interessate da una sottoportante, ovvero 156.25 kHz, la risposta impulsiva del canale può essere equalizzata molto più facilmente piuttosto che su canale unico da 10 MHz con alta frequenza di bit. Inoltre la bassa frequenza di simbolo di ogni sottocanale rende il sistema molto più resistente ai fenomeni di interferenza intersimbolica (ISI), diminuendo la probabilità d'errore. Nella tabella di fig.17 vengono messe a confronto le varie tecniche di modulazione che possono essere utilizzate nelle varie sottoportanti. Per

frequenze molto disturbate converrà utilizzare modulazioni che portano poca informazione, come la BPSK, perché il rumore introdotto potrebbe causare interferenze non correggibili dal ricevitore. Per frequenze in cui il canale presenta una risposta impulsiva meno disturbata (idealmente costante) si possono utilizzare modulazioni che riescono a portare molta informazione come la 64-QAM.

Data Rate, Mbits/s for WAVE*	Modulation	Coding Rate, (R)	Coded Bits per Subcarrier, (N_{BPSC})	Coded Bits per OFDM Symbol, (N_{CBPS})	Data Bits per OFDM Symbol, (N_{DBPS})
3	BPSK	1/2	1	48	24
4.5	BPSK	3/4	1	48	36
6	QPSK	1/2	2	96	48
9	QPSK	3/4	2	96	72
12	16-QAM	1/2	4	192	96
18	16-QAM	3/4	4	192	144
24	64-QAM	2/3	6	288	192
27	64-QAM	3/4	6	288	216

Figura 17 - Modulazioni applicabili con tecnica OFDM su standard 802.11p [10]

Oltre a questi fattori si può variare, a parità di modulazione, il Coding Rate cioè il rapporto tra il numero di bit d'informazione (utili) e il numero di bit inviati nel canale. Questo parametro è il complementare della frazione di bit di codifica nel pacchetto. Ad esempio possiamo notare come nella 64-QAM con Coding Rate $\frac{2}{3}$ si riesca ad ottenere un throughput di 24Mbps contro i 27Mbps raggiungibili con Coding Rate $\frac{3}{4}$.

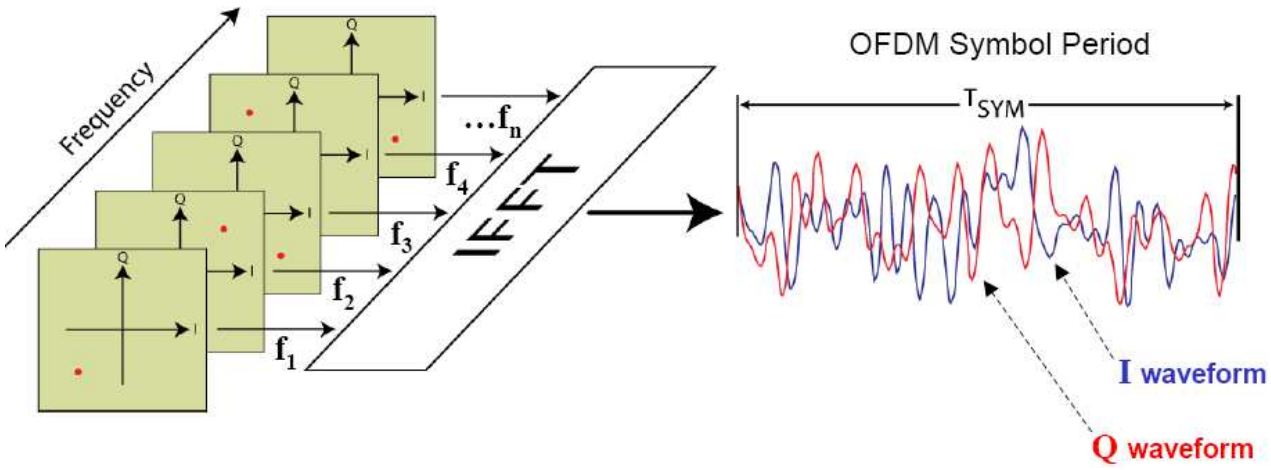


Figura 18 - Schema concettuale modulazione OFDM

Le sottoportanti nella modulazione OFDM sono rese ortogonali tra loro, il che significa che i segnali trasportati su ogni portante non andranno a disturbarsi l'uno l'altro, non richiedendo quindi la banda di guardia tra un sottocanale e l'altro. La progettazione del trasmettitore e ricevitore è quindi semplificata dove non sono necessari dei filtri come nella tradizionale FDM. Uno dei più importanti problemi delle comunicazioni radio è il ritardo introdotto dai cammini multipli (*multi-path*). Questo problema causa interferenza intersimbolica e la tecnica OFDM offre una valida soluzione a questo inconveniente. A differenza di 802.11°, in 802.11p è stata raddoppiata la durata dei simboli OFDM e di conseguenza è stato raddoppiato il periodo di guardia tra simboli differenti. Se i ritardo di un simbolo supera l'intervallo di guardia per una frazione piccola di tempo tra l' 1% e il 10%, il segnale può ancora essere recuperato. Se invece supera il 10% la decodifica può essere gravemente affetta da errori e l'interferenza intersimbolica è inevitabile. Questi rimedi però portano ad un abbassamento della velocità di trasmissione; le differenze tra i due standard sono riassunte nella tabella in fig.19.

	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
Error Correction Coding	Convolutional Coding with K=7	Convolutional Coding with K=7
Coding Rate	1/2, 2/3, 3/4	1/2, 2/3, 3/4
# of subcarriers	52 net	52 net
OFDM Symbol Duration	4.0 μs	8.0 μs
Guard Period	0.8 μs	1.6 μs
Occupied bandwidth	20 MHz	10 MHz
Frequency	5 GHz ISM band	5.850-5.925 GHz

Figura 19 - Confronto standard 802.11a e 802.11p [10]

Controllo della potenza di trasmissione D-FPAV

La potenza di trasmissione nelle comunicazioni wireless è un fattore molto importante in quanto da essa dipende la buona riuscita della comunicazione tra trasmittente e ricevente. Nel nostro caso la potenza di trasmissione gioca un ruolo fondamentale perché permette di coprire

una zona più o meno vasta quando si vogliono trasmettere dei messaggi ad altri veicoli. A questo proposito possiamo pensare che i vari veicoli possano utilizzare una potenza di trasmissione a seconda della distanza da coprire con la trasmissione fino ai 1000m di portata consentiti dallo standard 802.11p. Possiamo notare nel grafico di fig. 20 la probabilità che un messaggio sia ricevuto correttamente da un'unità in relazione alla distanza tra trasmettitore e ricevitore. La distanza tra i due determina la potenza di trasmissione, ovvero più la distanza è elevata più potenza dovrà essere utilizzata per inviare correttamente il messaggio. In particolare questo grafico da un'idea di come si comporta il trasferimento di messaggi di beacon in un contesto autostradale con bassa densità di veicoli e con rate di beacon generati pari a 10 pacchetti/s.

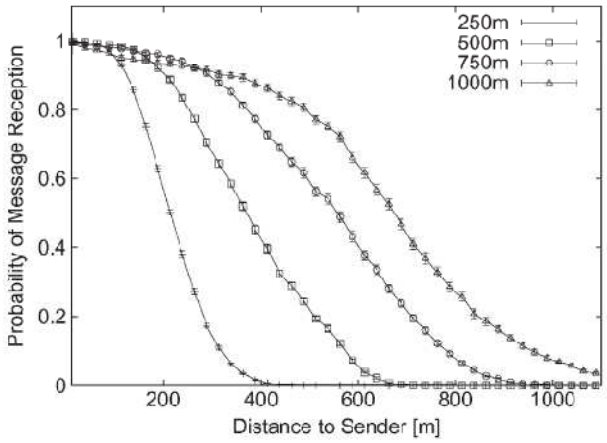


Figura 20 - Probabilità di corretta ricezione Beacon con densità 36 veicoli/Km [11]

Quando la densità di veicoli comincia a crescere è inevitabile che, utilizzando potenze di trasmissione costanti, si vengano a creare maggiori interferenze. Lo dimostra il grafico in fig. 21 che valuta, come nel caso precedente, la probabilità di corretta ricezione in funzione della distanza tra ricevitore e trasmettitore in un contesto autostradale con densità di veicoli quasi doppia rispetto alla precedente.

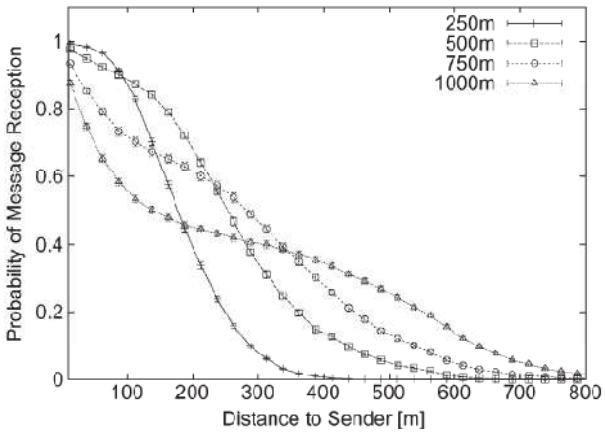


Figura 21 - Probabilità di corretta ricezione Beacon con densità 66 veicoli/Km [11]

Possiamo notare una netta diminuzione della probabilità di corretta ricezione dei pacchetti poiché, con una densità maggiore di veicoli, l'interferenza procura effetti indesiderati. Utilizzando la massima potenza di trasmissione possiamo vedere che se il ricevente si trova ad una distanza di 200 m, la probabilità di corretta ricezione scende ad ½ . Si nota quindi che ogni veicolo necessita di un sistema di controllo della potenza di trasmissione per cercare, anche in condizioni di alta densità di traffico, di mantenere quanto più alta possibile la probabilità di corretta ricezione dei dati. Per questo esiste un algoritmo che viene eseguito da ogni veicolo denominato D-FPAV (Distribuited Fair Power Adjustment for Vehicular environments) per controllare il carico del mezzo trasmissivo dovuto alla trasmissione di beacon, rendere equo in termini di potenza di trasmissione l'accesso al canale da parte di tutte le unità e dare una priorità maggiore a messaggi legati alla sicurezza. L'algoritmo si basa sulla conoscenza delle informazioni portate dai beacon tipo posizione, velocità e direzione fornite da tutte le unità che rientrano nella portata di interferenza massima (CSmax); ogni nodo scambia informazioni di questo tipo con tutti i nodi vicini in modo che ognuno abbia sempre il quadro generale sulla posizione dei vicini (e vicini dei vicini) completo e aggiornato. Sulla base di queste informazioni l'algoritmo FPAV calcola la potenza di trasmissione da utilizzare per ridurre il più possibile la portata d'interferenza e inserisce questa stima della potenza nei successivi beacon da inviare. Contemporaneamente ogni stazione riceve i beacon dei propri vicini con allegati i valori consigliati di potenza da utilizzare. Alla fine ogni nodo sceglierà la potenza di trasmissione da utilizzare come la minima tra quelle calcolate da se stesso con l'algoritmo FPAV e quelle consigliate dai vicini. In fig.20 possiamo notare l'algoritmo D-FPAV.

Algorithm D-FPAV: (algorithm for node u_i)
INPUT: geographical positions of all nodes in $CS_{MAX}(i)$
OUTPUT: a power setting $PA(i)$ for node u_i, such that the resulting power assignment is an optimal solution to BMMTxP

1. Based on the geographical positions of all nodes in $CS_{MAX}(i)$, use FPAV to compute the maximum common transmit power level P_i s.t. the MBL threshold is not violated at any node in $CS_{MAX}(i)$
2a. Disseminate P_i to all nodes in $CS_{MAX}(i)$
2b. Collect the power level values computed by nodes u_j such that $u_i \in CS_{MAX}(j)$ and store the received values in P_j
3. Assign the final power level: $PA(i) = \min\{P_i, \min_{j:u_i \in CS_{MAX}(j)}\{P_j\}\}$

Figura 22 - Algoritmo D-FPAV per il controllo della potenza di trasmissione [11]

Con l'utilizzo di questo algoritmo si è dimostrato [11] che la riduzione delle collisioni è notevole, a discapito però della distanza massima di trasmissione. Infatti possiamo notare nel

grafico di fig. 23 che con questo tipo di controllo la distanza massima raggiungibile è attorno ai 350 m. Il vantaggio è tutto per le comunicazioni su distanze brevi perché, come si può notare, fino ai 100 m le probabilità di corretta ricezione sono più alte di quelle ottenute senza l'ausilio del D-FPAV.

Da notare che per l'utilizzo di questo algoritmo è necessario aggiungere ai beacon un overhead per portare le informazioni relative alla potenza consigliata. Queste informazioni aggiuntive possono essere inviate ogni beacon (1over1), un beacon ogni cinque (1over5) e un beacon ogni dieci (1over10). Queste diverse frequenze di aggiornamento della potenza stimata portano, da un lato, ad avere un aggiornamento frequente della situazione, ma dall'altro tendono a saturare maggiormente il canale a causa dell'overhead sui vari beacon. Il giusto compromesso sta nel inviare un beacon esteso ogni dieci beacon (1over10) e si può notare dal grafico di fig. 23 che questa soluzione porta, a parità di distanza, ad una probabilità di corretta ricezione maggiore.

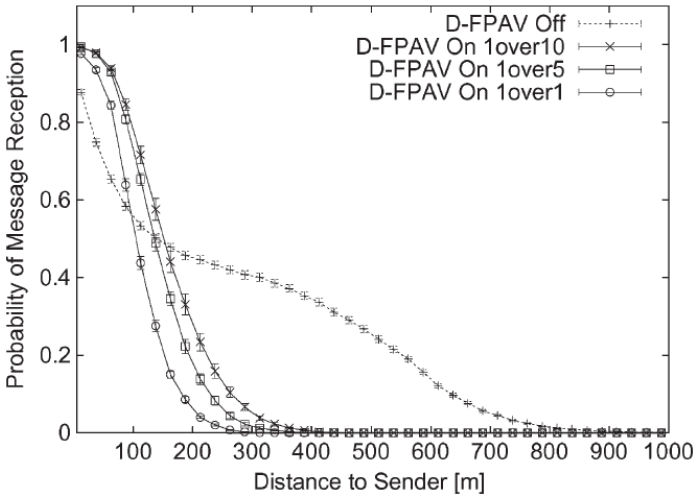


Figura 23 - Probabilità di corretta ricezione con e senza l'utilizzo di D-FPAV [11]

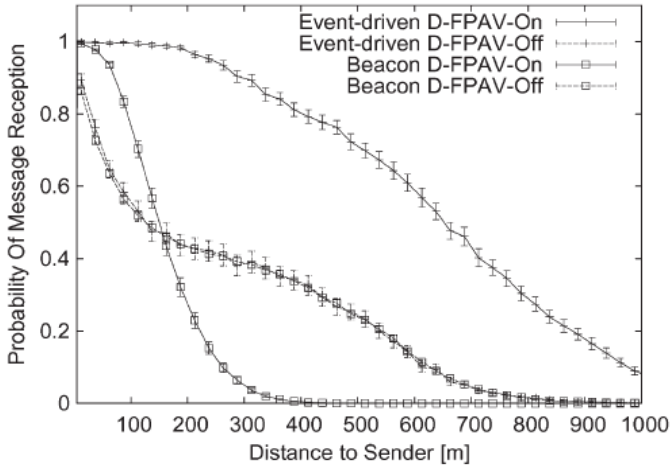


Figura 24 - Probabilità di corretta ricezione di beacon e messaggi d'emergenza con e senza D-FPAV [11]

L’algoritmo D-FPAV migliora la trasmissione dei beacon entro una distanza di 160 m [11]; questa distanza è ritenuta accettabile perché si pensa che in uno scenario reale i veicoli che si trovano a 160 m si possano considerare abbastanza distanti e le informazioni che possono inviare sono comunque di minor importanza rispetto ai beacon dei veicoli più vicini e ai messaggi di emergenza.

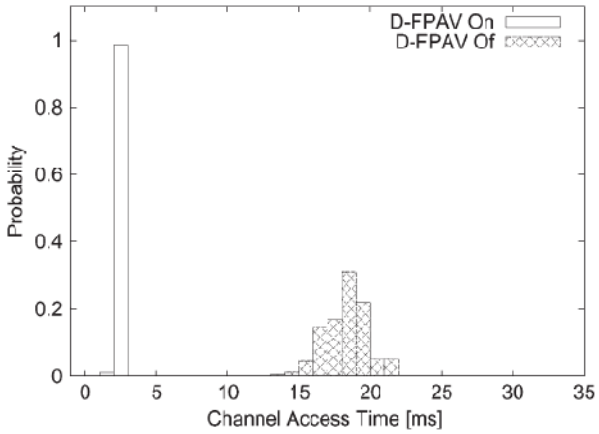


Figura 25 - Tempo di accesso al canale con e senza D-FPAV

Un altro aspetto importante dell’utilizzo del controllo della potenza di trasmissione è il tempo di accesso al canale: il tempo medio per l’accesso al canale senza l’utilizzo del D-FPAV è di 17.5 ms contro gli 1.1 ms utilizzando l’algoritmo [11]. Questo perché se tutti i veicoli controllano la loro potenza di trasmissione, la portata di interferenza di ognuno è ridotta al minimo e quando qualche unità intende accedere al mezzo e si mette in ascolto della portante, con molta probabilità troverà il canale libero e potrà trasmettere.

VI. Livello Medium Access Control (MAC): 802.11p e 1609.4

Accesso al mezzo con CSMA/CA

Lo strato MAC implementa lo schema di accesso al mezzo Enhanced Distributed Channel Access (EDCA), derivato dallo standard IEEE802.11e e QoS. Questo meccanismo è basato sulla tecnica Carrier Sense Multiple Access con Collision Avoidance (CSMA/CA) nella quale tutte le stazioni sono in competizione per l'accesso al canale (sistema Best Effort). Una stazione che vuole trasmettere inizia ascoltando il canale; se il canale è occupato viene attivato un timer di durata casuale (tempo di backoff) che viene decrementato durante i periodi di inattività del canale e mantenuto costante quando il canale è occupato da trasmissioni. Quando il timer arriva a zero la stazione esegue un altro tentativo di ascolto: se il canale è occupato si ripete la procedura precedente, se è libero prenota la trasmissione e attende un altro istante. Se il canale continua ad essere libero significa che non ci sono altre prenotazioni quindi trasmette. L'intervallo di tempo che intercorre tra quando la stazione ascolta il canale a quando trasmette i propri dati è chiamato Distributed Interframe Spacing time (DIFS). In fig. 26 possiamo notare le fasi della tecnica base CSMA/CA. SISF è il tempo che intercorre tra la ricezione di un pacchetto e l'invio del pacchetto di riscontro (ACK) da parte del ricevente. In tutto il periodo in cui il canale è occupato, compreso il tempo del SIFS e il DIFS successivo ad ogni trasmissione, il contatore del tempo di backoff delle stazioni rimane "congelato".

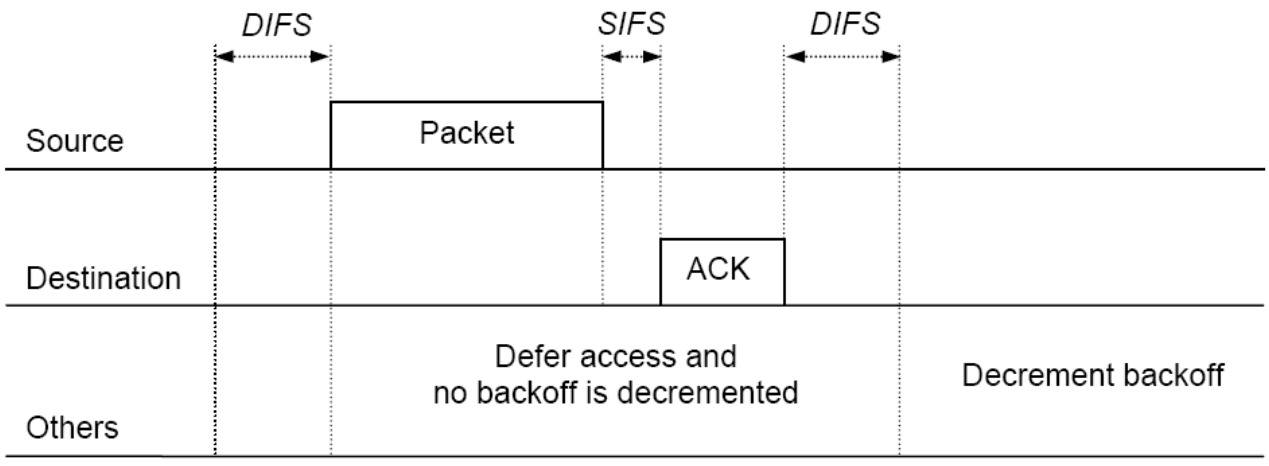


Figura 26 - Fasi del CSMA/CA [13]

Di questa tecnica di accesso al mezzo esistono due metodi di ascolto del canale: uno fisico e l'altro virtuale. Nel primo, *physical carrier sensing*, lo stato del canale viene deciso sulla base dell'energia rilevata dall'antenna. Il secondo metodo di ascolto del canale si dice *virtual carrier sensing* ed è basato su una tecnica di prenotazione. Il mittente ascolta la portante e se questa è libera per un tempo pari a DIFS invia un pacchetto di controllo chiamato Request To Send (RTS). Dopo un SIFS il destinatario risponde con un pacchetto Clear To Send (CTS). Le altre stazioni che ricevono i pacchetti di RTS e CTS evitano di occupare il canale nell'intervallo successivo. La trasmissione dei dati può quindi iniziare dopo un SIFS dalla ricezione del CTS.

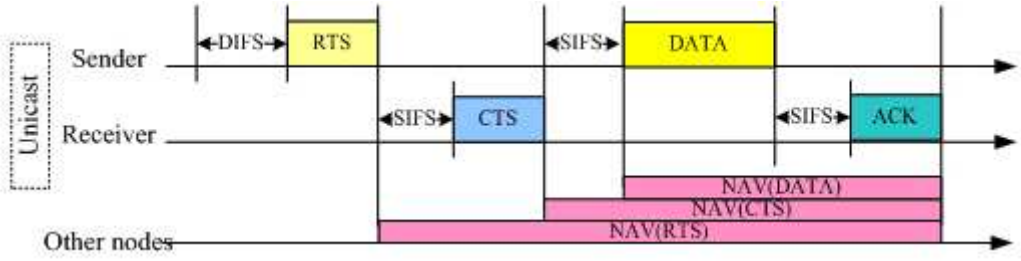


Figura 27 - Sistema RTS/CTS per trasmissioni Unicast

Questa tecnica di ascolto del canale, più onerosa rispetto alla *physical carrier sensing* è utilizzata solamente per comunicazioni nel canale di servizio (SCH) quindi in tutte le trasmissioni che non hanno una priorità elevata (comunicazioni non legate alla sicurezza) tra OBU e RSU o anche tra OBU e OBU.

In entrambi i casi, *physical carrier sensing* e *virtual carrier sensing*, la dimensione della finestra di backoff è una variabile aleatoria uniforme nell'intervallo [0, CW] dove CW è la Contention Window che aumenta ogni qual volta avviene una collisione. La finestra CW può assumere dei valori tra un minimo CWmin ed un valore massimo CWmax. L'incremento della finestra è utile quando ci sono diverse stazioni radio che vogliono trasmettere sullo stesso canale e con un valore ampio di CW si può fare in modo che le collisioni diminuiscano. Dopo una trasmissione avvenuta con successo la finestra CW viene riportata al valore iniziale Cwmin. Per garantire che la trasmissione avvenga con successo lo strato MAC implementa un protocollo di ARQ Stop&Wait. Dopo ogni trasmissione, il trasmettitore resta in attesa di ricevere il pacchetto di riscontro ACK che conferma l'avvenuta ricezione del datagramma da parte del ricevitore. Perché questo meccanismo ARQ funzioni è necessario che i pacchetti inviati siano numerati in modo da riconoscere quali eventuali pacchetti non sono arrivati a destinazione. A questo proposito possiamo notare in fig. 12 un Byte riservato al numero del pacchetto (Sequence Number).

In fig. 28 possiamo notare le differenze tra gli standard 802.11a e 802.11p; l'aumento del tempo di slot e del tempo di SIFS nello standard 802.11p consente di ridurre gli errori di interferenza intersimbolica dovuti ai cammini multipli dei segnali radio.

	IEEE 802.11a	IEEE 802.11p
Slot time	9 μs	13 μs
SIFS time	16 μs	32 μs
CW_{min}	15	15
CW_{max}	1023	1023

Figura 28 - Confronto tra 802.11a e 802.11p [10]

Il servizio di conferma della trasmissione ACK è fornito dal livello MAC solo a comunicazioni di tipo unicast, mentre per comunicazioni di tipo broadcast questo servizio non viene fornito.

Gestione priorità EDCA

Lo strato MAC, e precisamente lo strato superiore del livello MAC di fig.5 si occupa del coordinamento degli accessi ai canali sia di servizio (SCH) che di controllo (CCH). Sopra a questo strato esistono applicazioni che creano datagrammi di tipo IP o WSMP che sono quelli utilizzati nelle comunicazioni tra veicoli. Perché possano coesistere più applicazioni sopra lo stesso livello MAC è necessario da parte di quest'ultimo poter riconoscere i pacchetti che gli vengono passati dagli strati superiori. A questo fine l'header dei pacchetti che vengono passati dallo strato LLC al MAC contiene un campo di 2 Byte, denominato *EtherType* o *802.2 header*.

Il campo *802.2 header* assume il valore

- 0x86DD nel caso il pacchetto sia di tipo IP
- 0x88DC nel caso il pacchetto sia di tipo WSMP

802.2 header	IP or WSMP header	IP or WSMP data

Figura 29 - MSDU passate tra LLC e MAC [4]

Quando una MSDU è passata dal livello Logical Link Control (LLC) a livello MAC, questo esamina il campo EtherType per capire se il pacchetto è di tipo IP o WSMP. Nel primo caso il pacchetto viene indirizzato verso le quattro code della parte destra di fig.30 che gestiscono l'accesso al canale di servizio (SCH), poiché i pacchetti di tipo IP possono essere inviati solamente utilizzando i canali SCH. Nel secondo caso invece, a seconda del tipo di messaggio usato (beacon, messaggi di sicurezza, ecc…), il pacchetto viene indirizzato verso la parte che si occupa della gestione dell'unico canale di controllo (CCH) o verso la parte che si occupa della gestione degli SCH.

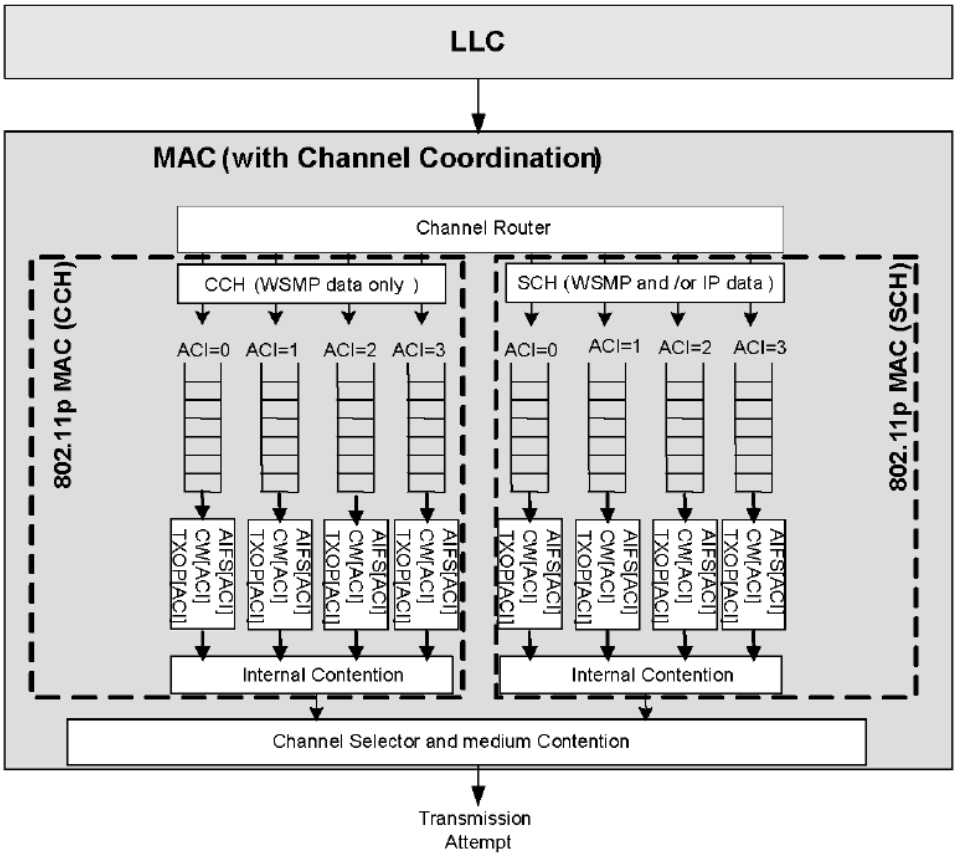


Figura 30 - Architettura livello MAC con coordinamento dell'accesso al canale [4]

Inoltre la gestione dei pacchetti è eseguita tenendo conto della priorità delle informazioni da inviare. A questo proposito esistono quattro categorie d'accesso (AC): background, best effort, video, voice traffic. Ad ogni categoria d'accesso viene riservata una coda. La priorità maggiore è quella della classe Voice Traffic. Una volta che il livello MAC ha letto il contenuto del campo *802.2 header* del pacchetto che ha ricevuto dallo strato LLC va a leggere il campo *IP o WSMP header*. Nel caso di un datagramma WSM sono contenute le informazioni sul numero del canale (*channel*), la potenza di trasmissione (*power*) e il rate di trasmissione (*Data rate*).

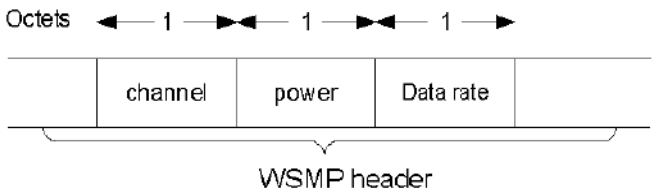


Figura 31 - Porzione di header usata per il controllo dei parametri di trasmissione del livello PHY [4]

Nel campo *channel* è indicata la coda per quel pacchetto, nel campo *power* è contenuta l'informazione della potenza di trasmissione e nel campo *data rate* il rate da utilizzare ovvero il tipo di modulazione da utilizzare. Il pacchetto verrà scartato qualora contenesse un indirizzo di *channel* non valido.

Se il pacchetto ricevuto è di tipo IP nel corrispondente header sono contenute le stesse informazioni con in più il campo campo denominato *adaptable* nel quale è specificato se la potenza e la velocità di trasmissione possono essere adattate alle condizioni del canale.

Il pacchetto IP verrà scartato nel caso in cui il veicolo trasmittente non sia un membro della stessa WBSS del ricevente perché solo se ne fa parte può avvenire la trasmissione (ad esempio una WBSS tra OBU e RSU).

La gestione della priorità dei messaggi da trasmettere avviene successivamente sulla base del meccanismo EDCA. Dopo aver superato la prima fase di instradamento verso i canali SCH o il canale CCH vengono assegnati ai vari pacchetti degli indici di categoria d'accesso (ACI) a seconda dell'informazione fornita dal campo *channel*. Ad ogni categoria d'accesso (AC) vengono assegnati dei parametri:

- Arbitration Inter-Frame Space (AIFS): minimo intervallo di tempo che intercorre tra quando il canale si libera a quando inizia una trasmissione.
- Contention Windows (CW): intervallo nel quale viene scelto il numero casuale che realizza il meccanismo di back-off.
- Transmit Opportunities (TXOP): tempo massimo in millisecondi entro il quale una certa stazione può trasmettere.

Un algoritmo interno calcola il tempo di back-off in modo indipendente per ogni categoria d'accesso, basandosi esclusivamente sui tre parametri appena descritti. La categoria d'accesso con il minor tempo di back-off vince la competizione interna (*internal contention*) tra le code dopodiché dovrà affrontare la contesa del mezzo (*medium contention*). Questi passaggi avvengono sia per i pacchetti indirizzati al CCH che per quelli indirizzati al SCH come mostrato in fig. 32.

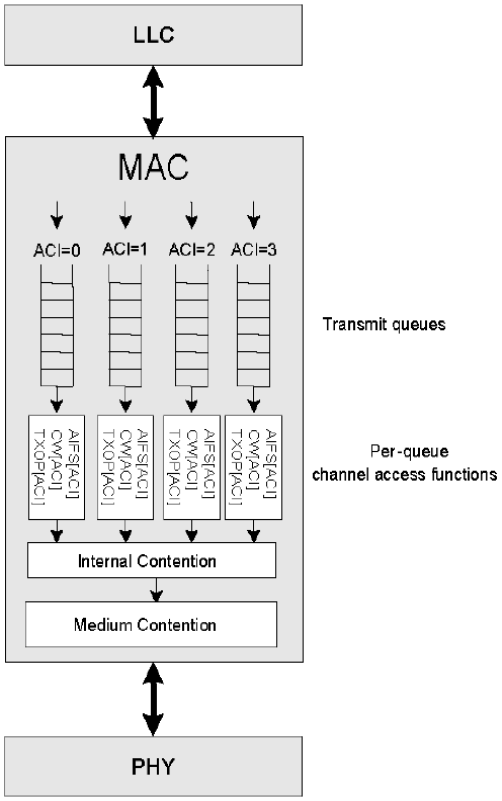


Figura 32 - Accesso con priorità in ogni canale [4]

Nelle tabelle di fig. 33 e fig. 34 possiamo notare i parametri EDCA che vengono settati rispettivamente per il canale di controllo e per il canale di servizio. Da notare che l'intervallo CWmax-CWmin è massimo per pacchetti che hanno priorità bassa (AC = 1) mentre è minimo per i pacchetti che hanno priorità alta (AC = 3). Inoltre anche il tempo AIFSN è minimo per la classe 3 e massimo per la classe 1; tutto questo allo scopo di evitare il più possibile i conflitti durante la competizione interna privilegiando i pacchetti con priorità alta che sono quelli legati alla sicurezza di guida. L'intervallo di tempo TXOP è per entrambi i canali e per tutte le classi pari a zero e ciò significa che ogni pacchetto può essere inviato una sola volta nel canale. Il valore di aCWmin e aCWmax per il calcolo di CWmin e CWmax è rispettivamente di 15 e 1023.

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

Figura 33 - Parametri EDCA usati nel CCH [4]

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

Figura 34 - Parametri EDCA usati nel SCH [4]

Nella fig. 35 possiamo vedere l'aumento esponenziale della CW all'aumentare del numero di tentativi di trasmissione falliti. La relazione che lega il valore di CW ad ogni ritrasmissione è:

$$CW(n+1) = min\{CW_{max}\,, 2 \cdot [CW(n)+1] - 1\}$$

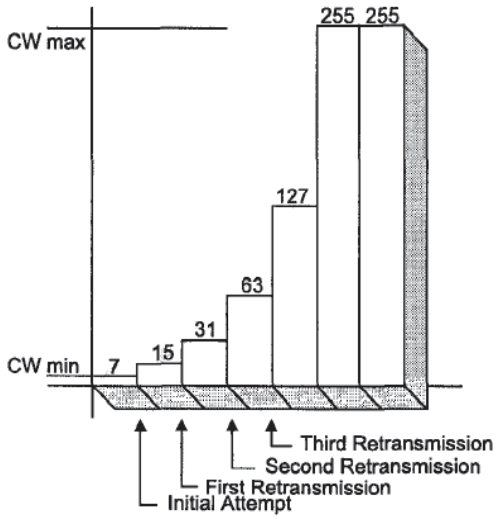


Figura 35 - Espansione della CW all'aumentare del numero di ritrasmissioni [6]

Il canale nel quale vengono trasmessi i datagrammi deve essere coordinato perché le varie unità non sono in grado simultaneamente di monitorare il canale di controllo CCH e trasmettere sui canali di servizio SCH. Tutti i dispositivi devono monitorare il CCH durante l'intervallo di tempo dedicato perché nel caso ci siano in coda messaggi ad alta priorità, questi devono essere trasmessi eventualmente anche durante l'intervallo di tempo dedicato al SCH. Quando una stazione si aggiunge ad una WBSS è necessaria la sincronizzazione e il

coordinamento del canale per permettere a tutte le unità di monitorare il CCH durante il periodo opportuno. Per questo tutte le unità sono sincronizzate temporalmente sullo stesso riferimento (ad esempio GPS) ed ogni intervallo sia CCH che SCH dura 50 ms. Tra un intervallo e l'altro c'è un periodo di guardia che di default vale 4 ms per sopperire ad eventuali ritardi di trasmissione ed errori di sincronizzazione.

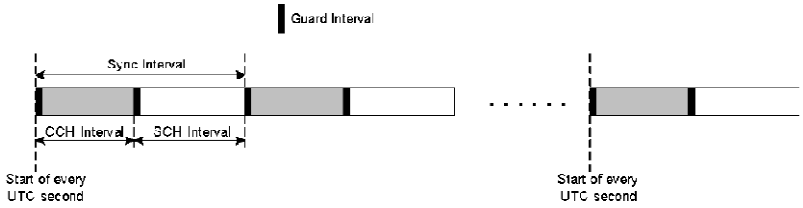


Figura 36 - Intervalli temporali dedicati al CCH e al SCH [4]

Ad ogni trasmissione vengono eseguite le seguenti operazioni:
Il livello LLC passa al livello MAC la MSDU. Il Channel Router del livello MAC controlla il campo EtherType del pacchetto dove è indicata la tipologia del protocollo: WSMP o IP. Se siamo di fronte ad un pacchetto WSMP viene controllato il numero di canale nel WSMP header (perché possono essere trasmessi sia nel CCH che nel SCH) e in base a questo il pacchetto viene indirizzato su una delle code del canale CCH o SCH a seconda del numero di canale e dell'indice della categoria d'accesso (ACI). Il pacchetto viene scartato se il numero del canale non dovesse essere valido. Se il pacchetto è di tipo IP invece viene indirizzato direttamente ad una delle quattro code del canale SCH. Ora tutti i pacchetti sono accodati nelle relative code e il livello MAC sceglie la MSDU che vince la contesa interna, sceglie quindi il pacchetto a cui era stato assegnato il minor tempo di back-off e riesamina nuovamente il campo EtherType. Ora il livello MAC legge i campi di WSMP o IP header relativi al rate di trasmissione e alla potenza di trasmissione da applicare al pacchetto in esame. Da questo momento in poi il livello MAC comunica con il livello fisico:

- il livello fisico avvisa il MAC della presenza del canale libero con la primitiva PHY-CCA.indication(IDLE)
- il MAC risponde con la primitiva PHY-TXSTART.request(TXVECTOR) finalizzata a settare i parametri di potenza e velocità di trasmissione del livello fisico
- il livello MAC chiede al livello fisico il tempo impiegato per trasmettere il pacchetto con la primitiva PHY-TXTIME.request e il livello fisico risponde con la primitiva PHY-TXTIME.confirm. Se questo tempo supera il tempo residuo dell'intervallo di canale (CCH intervall o SCH interval) il pacchetto viene memorizzato temporaneamente per poi essere trasmesso all'inizio del successivo intervallo di canale. Altrimenti, nella condizione migliore si passa al punto successivo.

- inizia lo scambio dell'intero pacchetto tra MAC e PHY con un susseguirsi di primitive del tipo PHY-DATA.request(DATA) rilasciate dal MAC e PHY-DATA.confirm rilasciate dal livello fisico a conferma del corretto trasferimento al destinatario
- finito il trasferimento dell'intero pacchetto il livello MAC termina il collegamento con la primitiva PHY-TXEND.request

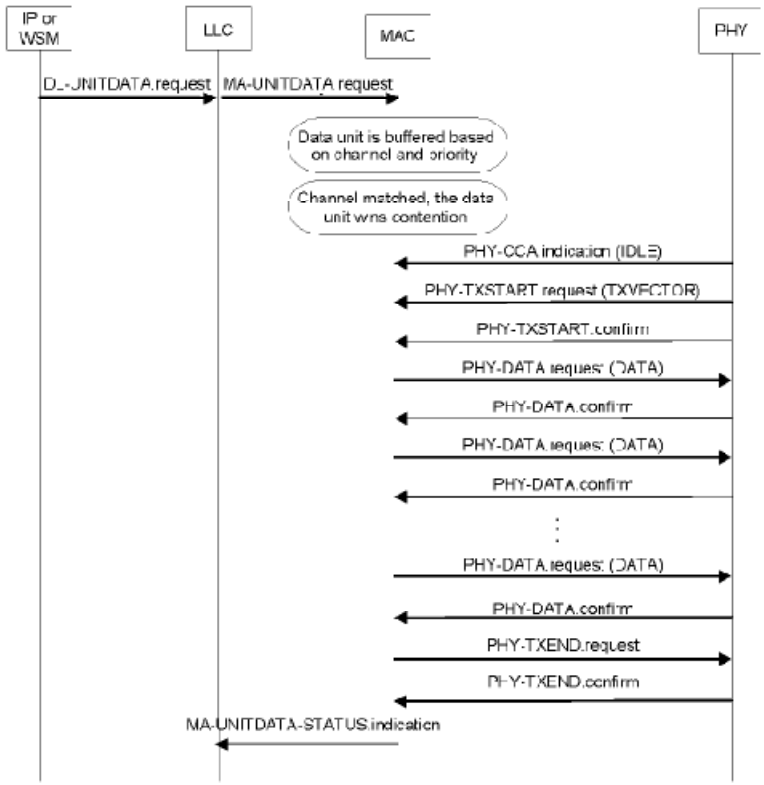


Figura 37 - flusso del processo di trasmissione [4]

da notare che nel caso peggiore il campo dati di una MSDU contiene al massimo 2312 Byte il che equivale a dire che alla minima velocità di trasmissione ci vogliono

$$t_{max} = \frac{2312 * 8}{R_{min}} = \frac{2312 * 8}{3Mbps} \cong 6.20ms$$

Perciò in un intervallo SCH o CCH possono essere inviati al più

$$N = \frac{Channel\ interval}{t_{max}} = \frac{50ms}{6.2ms} \cong 8$$

Pacchetti di dimensione massima.

VII. Conclusioni

Lo standard WAVE è il candidato nel futuro per le comunicazioni DSRC e sarà completato nei prossimi mesi. Questo standard che oggi è ancora sottoforma di bozza verrà sicuramente migliorato e molte case automobilistiche all'avanguardia stanno già sperimentando diverse applicazioni sulle proprie autovetture. Tutta la trattazione fatta finora fa riferimento alla situazione americana dove già da diverso tempo è stata allocata la banda per DSRC. In Europa la situazione deve ancora essere definita ma già si stanno facendo diverse prove pratiche per prepararsi all'applicazione di questi sistemi di comunicazione che incrementeranno notevolmente la sicurezza su strada e non solo. Nel capitolo V si è vista l'utilità del controllo della potenza, senza il quale in situazioni di traffico elevato diventa difficile trasmettere con successo. Questo però è solamente una proposta che poi potrebbe venire presa in considerazione dalla comunità IEEE e standardizzata nel prossimo aggiornamento dello standard 802.11p. Nel capitolo VI si è visto come ai vari tipi di messaggi, che vengono inviati nel canale, possano venire assegnate diverse classi alle quali corrisponde una priorità diversa. La priorità dei messaggi viene assegnata dagli strati protocollari superiori a seconda che il messaggio sia per la sicurezza (ACI = 3) o per altri scopi (ACI = 0,1,2). Perché possa venire attuato il progetto di poter equipaggiare tutte le autovetture con questi nuovi sistemi bisogna trovare i finanziamenti per poterlo fare. Ecco che le comunicazioni basate sul protocollo IP giocano un ruolo fondamentale perché permetterebbero a qualsiasi attività commerciale di farsi indirettamente pubblicità all'interno di ogni veicolo. Questo è a vantaggio sia dell'utente che disporrà di tutte le informazioni necessarie sia all'attività commerciale che ne trarrà beneficio. Questi scopi che sicuramente sono meno importanti di quelli per la sicurezza permetterebbero un rapido decollo di questo sistema. Tutte le informazioni riportate in questa tesi sono riferite ad un aggiornamento dello standard 802.11p del novembre 2006 mentre per quanto riguarda lo standard 1609.4 è già in forma definitiva.

Bibliografia

[1] IEEE Communication magazine Maggio 2009 – "WAVE: a tutorial" pp.126-133

[2] IEEE P802.11p/D2.0, "Draft Amendment to Standard for Information Technology – Telecommunications and information exchange between systems – Local and Metropolitan networks – specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment : Wireless Access in Vehicular Environments" 2006

[3] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," IEEE Vehicular Technology Conference, (VTC Spring 2008), pp. 2036–2040, May 2008.

[4] IEEE 1609.4 "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation", [Online] http://www.ieee.org/index.html

[5] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," in *Proc. IEEE VTC'07*, pp. 2199-2203, Sept. 2007.

[6] IEEE 802.11a "Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 1: High-speed Physical Layer in the 5 GHz band"

[7] IEEE 802.11e "Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements."

[8] E. Schoch, F. Kargl, M. Weber, T. Leinmüller, "Communication Patterns in VANETs", IEEE Communications Magazine, November 2008, pp.119-125

[9] "Car 2 Car Communication Consortium Manifesto" [Online]. http://www.car-2-car.org/

[10] T. Strang, M. Röckl, V2X communication protocols, Innsbruck University

[11] M. Torrent-Moreno, J. Mittag, P. Santi, H. Hartenstein: Vehicle-to-Vehicle Communication: "Fair Transmit Power Control for Safety-Critical Information" , IEEE Tr. on Vehicular Technology, Sept. 2009, pp 3684-3703

[12] Walter Franz, Hannes Hartenstein, Martin Mauve "Inter-Vehicle Communication Based on Ad Hoc Networking Principles. The FleetNet Project", [Online] http://digbib.ubka.uni-karlsruhe.de/volltexte/1000003684

[13] K. Bilstrup, E. Uhlemann and E. G. Ström, "Medium Access Control in Vehicular Networks Based on the Upcoming IEEE 802.11p Standard," *in Proceedings of. World Congress on ITS*, New York City, NY, Nov. 2008, 12 pages," 2008.