CAR ACCIDENT DETECTION AND COLLITION AVOIDANCE

Docenti: Prof.Ing. L.A. Grieco, Ing. P. Boccadoro

Corso di laurea in Ingegneria dell'Automazione
Esame di Internet of Things

Studenti:
Brandi Antonio
Comitangelo Giuseppe
Zitoli Vladimir

Sommario

Introduzione

Nell'ambito della sicurezza stradale, sarebbe ideale poter minimizzare il numero delle vittime in seguito ad un incidente. L'obiettivo del progetto è stato, quindi, quello di creare un sistema di telecomunicazioni che permetta, una volta rilevato un incidente, di comunicarlo all'ospedale più vicino e nel contempo alle auto circostanti.

In questo progetto, è stato realizzato un modello in scala di un tratto stradale servendoci di:

- N° 2 di macchine telecomandate;
- N° 4 di sensori di distanza;
- N°2 di accelerometri;
- N° 5 di antenne NRF24L01+;
- N°3 di Arduino Uno;
- N° 2 di Arduino Nano.

Ciascuna macchina comunica con un'antenna posta sul ciglio della strada e, non appena è coinvolta in un incidente, manda un messaggio di allarme all'antenna. Quest'ultima, quindi, inoltra il messaggio all'ospedale se quest'ultimo è visibile dall'antenna o, altrimenti, lo inoltra alle antenne vicine le quali provvederanno a far giungere il messaggio a destinazione.

Per evitare zone di buio, le antenne sono poste ad una distanza tale da coprire tutta la carreggiata. Dato che in questa configurazione si creano zone in cui i raggi d'azione di due o più antenne si sovrappongono, nel caso in cui l'incidente viene rilevato da più antenne, il messaggio verrà inviato ad una sola antenna scelta in maniera casuale dall'autoveicolo.

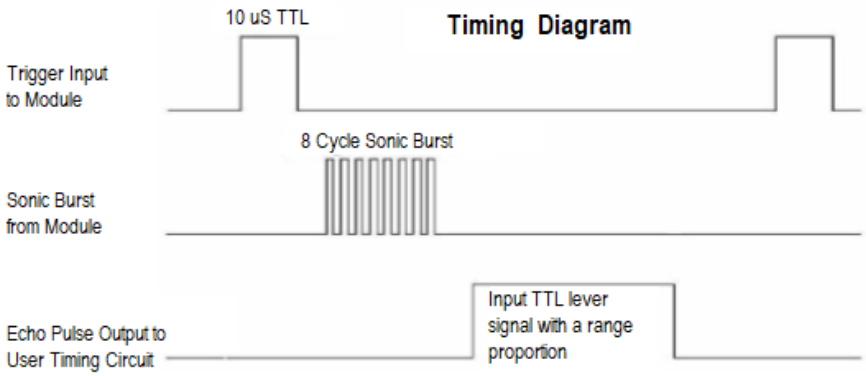
Di seguito verranno illustrate le caratteristiche salienti di ciascun dispositivo utilizzato e la pila protocollare usata nel progetto in scala.

1. Materiale utilizzato

1.1 Sensori di distanza

I sensori di distanza utilizzati nel progetto sono i sensori ULTRASONIC RANGING MODULE HC-SR04. Tali sensori sono in grado di fornire il valore della distanza di un oggetto con un'accuratezza di 3mm.

Il diagramma temporale è riportato in basso: viene inizialmente portato a livello logico alto il pin TRIGGER per almeno 10µs. Al termina di questa fase il modulo automaticamente invia un'onda acustica alla frequenza di 40 kHz e si pone in ascolto di un segnale ad onda quadra di ritorno. Durante questa fase, il modulo aspetta un segnale di eco. Se questo arriva, si calcola la distanza dell'oggetto su cui è stato riflesso il segnale mediante la seguente formula: $d = \frac{t*v}{2}$, con t=tempo di attesa dell'eco, v=velocità del segnale (≈340m/s).



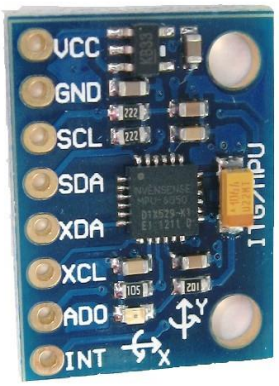
1.2 Accelerometro

L'accelerometro utilizzato per il progetto è stato l'accelerometro MPU 6050.

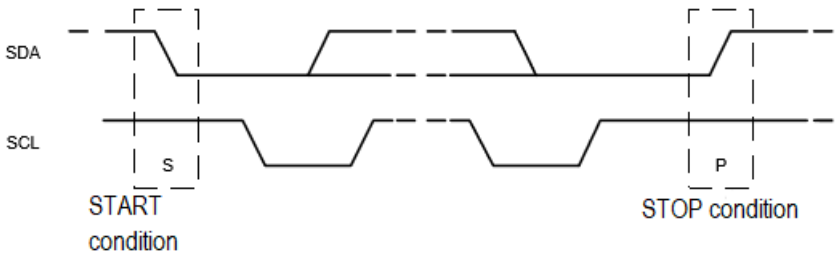
Tale accelerometro contiene, in un singolo integrato, un accelerometro MEMS a 3 assi ed un giroscopio MEMS a 3 assi in modo tale da poter calcolare sia le accelerazioni lineari che angolari. Le caratteristiche salienti di tale accelerometro sono:

- Range di misura dell'accelerazione lineare di $\pm 2g$, $\pm 4g$, $\pm 8g$ e $\pm 16g$;
- Convertitore A/D integrato a 16 bit sia per la rilevazione dell'accelerazione lineare che angolare, e quindi misura molto accurata dell'accelerazione del dispositivo;
- Comunicazione mediante protocollo I²C;
- Alimentazione nominale di 3.6 mA per il giroscopio e di 500µA per l'accelerometro lineare;
- Range di tensione di lavoro [2.375-3.46]V

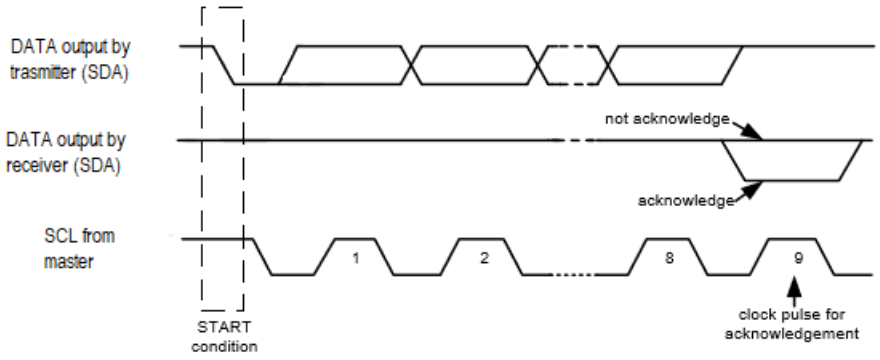
La comunicazione I²C avviene mediante la trasmissione di messaggi lunghi 8 bit. Non ci sono restrizioni riguardo il numero di byte che il master e lo slave si possono trasmettere. Ciascun byte trasferito è seguito da un segnale di acknowledge (ACK). Il segnale di ACK è generato dal ricevitore (in genere lo slave) facendo passare da alto a basso il livello di tensione corrispondente al pin SDA (Serial Data) e lasciandolo basso per un certo periodo. Se lo slave è occupato e non può trasmettere o ricevere alcun dato, esso può forzare il master a non trasmettere nulla ponendo il segnale di clock (SCL) al livello logico basso.



La comunicazione inizia quando il master impone la condizione di partenza (START, S) ponendo il segnale sulla linea SDA da alto a basso mentre il segnale di clock è alto. La comunicazione termina, invece, quando il master impone la condizione di stop (P), definito ponendo il livello logico della linea SDA da basso a alto mentre il segnale di clock è alto.

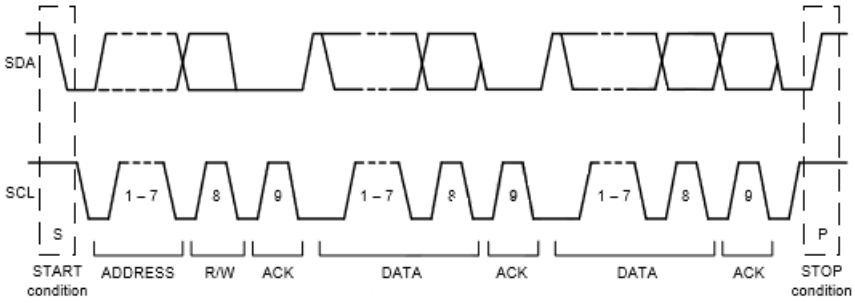


Dopo aver impostato le condizioni di partenza, il master invia un indirizzo di 7 bit, rappresentante lo slave con cui vuole comunicare, seguito dall'ottavo bit che indica se l'operazione che deve eseguire lo slave è di lettura (R) o scrittura (W).



Successivamente, il master rilascia la linea SDA e aspetta il segnale di ACK. In seguito alla ricezione dell'ACK, inizia lo scambio di dato tra master e slave e ciascun byte è seguito sempre da un ACK. Al termine della comunicazione il master impone la condizione di stop.

Se il master deve scrivere dei dati salvati in un determinato registro dello slave, dopo il 9° colpo di clock (corrispondente alla ricezione dell'ACK) il master invia allo slave l'indirizzo del registro con cui vuole interagire. Se invece esso vuole leggere, dopo il 9° colpo di clock rimane in ascolto per ricevere i dati fino a quando non invia un segnale di not acknowledge (NACK).



Master	S	AD+W		RA		S	AD+R			NACK	P
Slave			ACK		ACK			ACK	DATA		

Master	S	AD+W		RA		DATA		P
Slave			ACK		ACK		ACK	

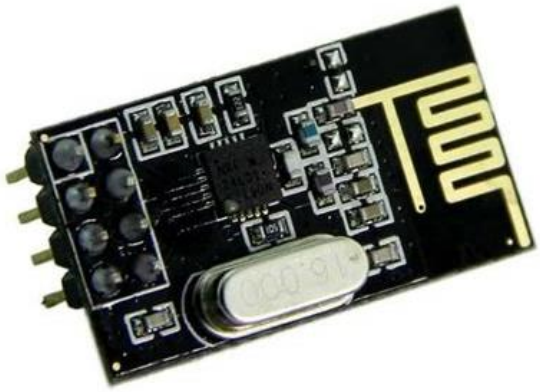
1.3 Antenna

Per il nostro progetto ci siamo serviti anche di 5 antenne nRF24L01+.

nRF24L01+ è un ricetrasmettitore a chip singolo da 2.4GHz con un motore di protocollo in banda base incorporato (Enhanced ShockBurst ™), adatto per applicazioni wireless a bassissima potenza. Il nRF24L01 + è progettato per funzionare nella banda di frequenza ISM mondiale a 2.400 - 2.4835 GHz.

Per progettare un sistema radio con nRF24L01 +, c'è semplicemente bisogno di un MCU (microcontrollore) e alcuni componenti passivi esterni.

nRF24L01 + è compatibile drop-in con nRF24L01 e compatibile on-air con nRF2401A, nRF2402, nRF24E1 e nRF24E2.



Le caratteristiche salienti che appartengono a questa famiglia di antenne sono:

- Banda ISM di lavoro: 2.4 GHz
- Range di tensione di funzionamento: 1.9 ÷ 3.6 V
- Corrente assorbita: 26µA (stand-by), 11.3mA (RX), 13.5 mA (TX)
- Gestione automatica dei pacchetti
- Ogni antenna nRF24L01+ può ascoltare contemporaneamente fino a 6 trasmettitori
- Compatibilità con NRF24L01
- Basso costo BOM (Bill Of Material, componenti del materiale)
- Velocità operativa (max) 2Mbps
- Regolatore di tensione integrato
- Altre funzioni: comunicazione Multi-point a 125 canali, salto di frequenza, anti-interferenza, modulazione GFSK
- Rilevamento errori CRC
- Dimensioni: 29 x 15 x 12mm
- Peso 3g
- Payload massimo trasportabile 32 bytes

Il funzionamento dell'antenna avviene mediante l'ausilio di 8 pin:

1. GND: massa
2. VCC: tensione alimentazione
3. CE: abilitazione al chip di attivare la modalità di trasmissione o ricezione
4. CSN: SPI chip select
5. SCK: SPI clock
6. MOSI: SPI slave data input: è la linea in uscita dal master ed in entrata negli slaves.
7. MISO: SPI slave data output: è la linea in ingresso al master ed in uscita dagli slaves.
8. IRQ: interrupt mascherabili (solitamente i meno utilizzati, in modo che il loro rumore non causi problemi)

Il protocollo di comunicazione utilizzato dall'antenna è il SPI (Serial Peripheral Interface). Similmente al protocollo I²C, la trasmissione avviene tra un dispositivo detto master ed uno o più slave. Il master controlla il bus, cioè ne prende possesso così da evitare che altri dispositivi slaves possano utilizzarlo mentre questo è occupato. Ogni dispositivo slave è collegato ad un pin con il segnale CS (Chip Select) del dispositivo master. Il dispositivo master dovrà avere un numero di pin CS pari al numero di dispositivi slaves collegati. Dunque abilitando un determinato pin CSi, verrà attivato lo slave corrispondente a tale pin. In definitiva ogni slave si collega al dispositivo master indipendentemente dagli altri e ciò rende tale protocollo molto più veloce rispetto al protocollo I²C. D'altra parte, è necessario che il dispositivo master abbia un numero di pin CS pari al numero di slave da coordinare. La comunicazione tra master e slave avviene seguendo nell'ordine le seguenti operazioni:

1. Il dispositivo master, nel caso in cui il dispositivo slave sia controllato singolarmente, seleziona lo slave con cui comunicare settando il segnale CS corrispondente al livello logico basso (logica 0-Attiva);
2. Il master invia il segnale di clock, configurandolo ad una frequenza tale che tutti i dispositivi possano supportarlo;
3. Ad ogni ciclo di clock avviene la comunicazione: il master invia il primo bit del dato attraverso il canale MOSI, insieme al segnale di clock;
4. Il dispositivo slave riceverà il segnale di clock e il primo bit sul canale MOSI, interpretandolo come l'inizio della comunicazione. In contemporanea invierà un altro dato sul canale MISO.

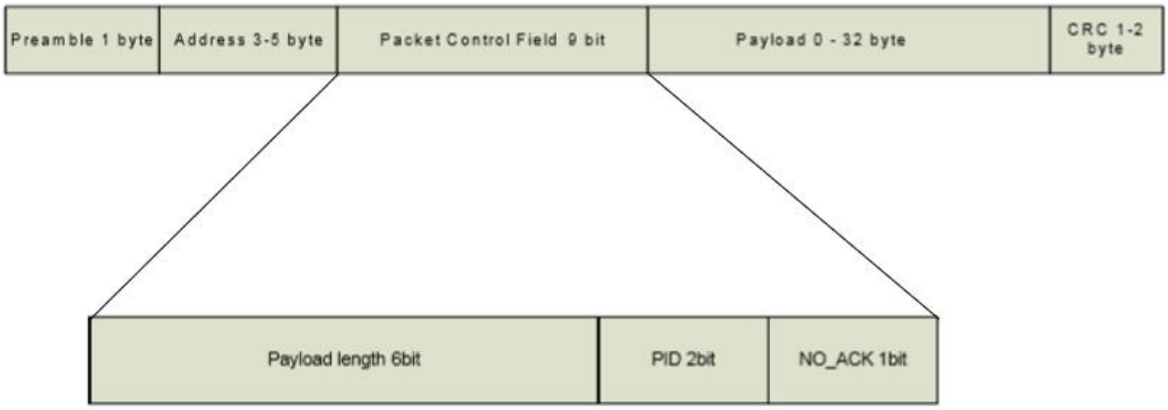
Come è possibile intuire, un altro vantaggio tipico della comunicazione SPI è la possibilità di essere full-duplex.

L'antenna può trovarsi in tre differenti modalità:

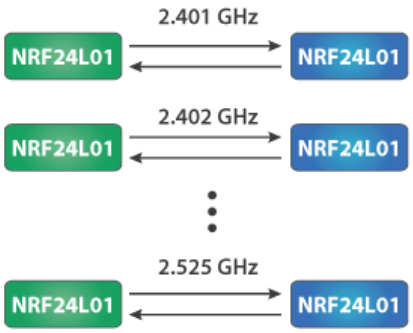
- STAND-BY: Il dispositivo entra nella modalità di stand-by quando il livello di tensione posto sul pin CE è basso oppure quando il livello di tensione sul pin CE è mantenuto alto ma il buffer di trasmissione (FIFO TX) è vuoto. In quest'ultimo caso la modalità di stand-by termina non appena c'è qualche dato da inviare.
- RICEZIONE: La modalità di ricezione è attiva quando l'antenna viene utilizzata come ricevitore. Per entrare in questa modalità, essa deve avere il livello di tensione sul pin CE settato alto. In modalità di ricezione il ricevitore demodula il segnale dal canale RF e cerca costantemente un pacchetto valido. Se viene trovato un pacchetto valido, il payload del pacchetto viene caricato in uno slot libero del buffer FIFO RX. Se questo buffer è pieno, il pacchetto ricevuto verrà scartato. L'antenna rimane in modalità di ricezione finché l'MCU non la configura in modalità standby o in modalità di spegnimento. Tuttavia, se le funzionalità del protocollo automatico sono abilitate, l'antenna può entrare in altre modalità automaticamente.
- TRASMISSIONE: La modalità di trasmissione è attiva quando l'antenna deve trasmettere dati. Per entrare in questa modalità l'antenna deve avere almeno un payload nella pila TX FIFO e un impulso alto in CE per più di 10µs. nRF24L01+ rimane in modalità di trasmissione finché c'è un pacchetto da trasmettere. Se CE= 0, l'antenna torna in modalità standby. Se CE=1, lo stato della pila TX FIFO determina la prossima azione: se la pila non è vuota l'antenna rimane in trasmissione altrimenti torna in modalità standby.

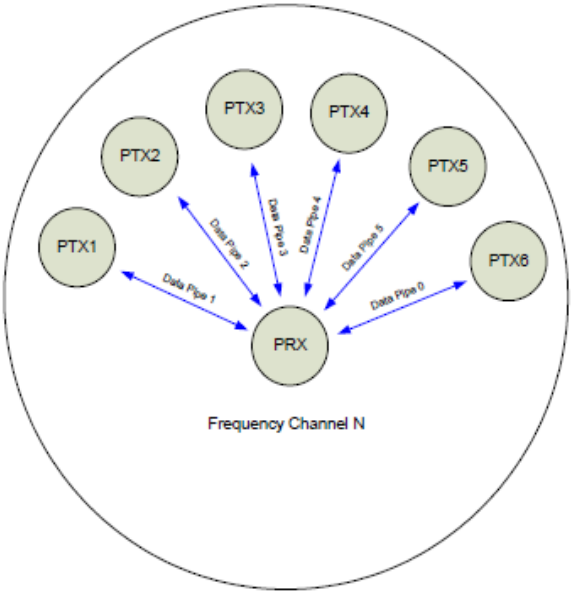
I frame utilizzati per la trasmissione dei dati sono caratterizzati dai seguenti campi:

- PREAMBLE (1 byte): Sequenza di 8 bit usata per sincronizzare il demodulatore del ricevitore per poter leggere l'informazione. Può assumere il valore di 0x01:0x01:0x01:0x01 o di 0xAA:0xAA:0xAA:0xAA in base al primo bit dell'indirizzo (se esso è 0 allora verrà utilizzato automaticamente il primo byte altrimenti verrà utilizzato il secondo).
- ADDRESS (3-5 byte): Indirizzo del ricevitore
- PACKET CONTROL FIELD (9 bit): Tale campo è caratterizzato da tre sub-campi:
    - PAYLOAD LENGHT (6 bit): Indica la lunghezza del payload in byte (da 0 a 32 bytes)
    - PID (Packet Identification, 2 bit): Indica se il frame ricevuto è un frame nuovo o un frame ritrasmesso.
    - NO_ACK (1 bit): Questo flag è usato per indicare se è attivo l'auto acknowledgement.
- PAYLOAD (0-32 bytes)
- CRC (1-2 bytes): Meccanismo di rilevamento degli errori di trasmissione. Esso è calcolato in base ai bit che compongono i campi address, Packet Control Field e Payload.



Una delle caratteristiche principali di questa famiglia di antenne è la possibilità di poter comunicare con più dispositivi contemporaneamente (modalità Multiceiver). Infatti il modulo nRF24L01+ può utilizzare 125 differenti canali per la comunicazione tra trasmettitore e ricevitore, il che permette di poter utilizzare fino a 125 coppie di trasmettore-ricevitore che lavorano in maniera indipendente tra di loro. Inoltre per ciascun canale il ricevitore (PRX, primary receiver) può ricevere dati da 6 differenti trasmettitori (PTX, primary trasmitter) come mostrato in figura utilizzando 6 indirizzi diversi, uno per ciascun trasmettitore.

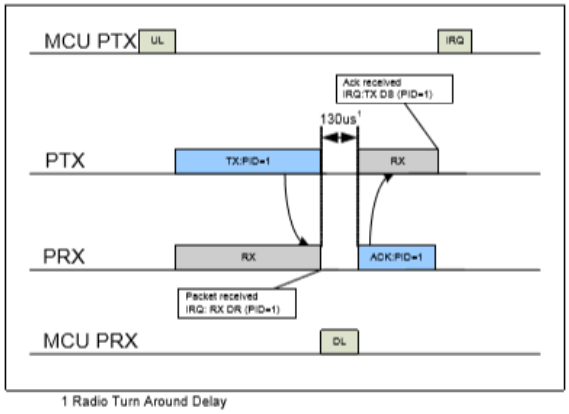




Le antenne PTX possono trasmettere simultaneamente ma l'antenna PRX può ricevere i pacchetti uno per volta. L'indirizzo identificato da pipe 0 è composto da 5 byte diversi tra loro, mentre gli altri condividono i primi 4 byte significativi e si differenziano per l'ultimo.

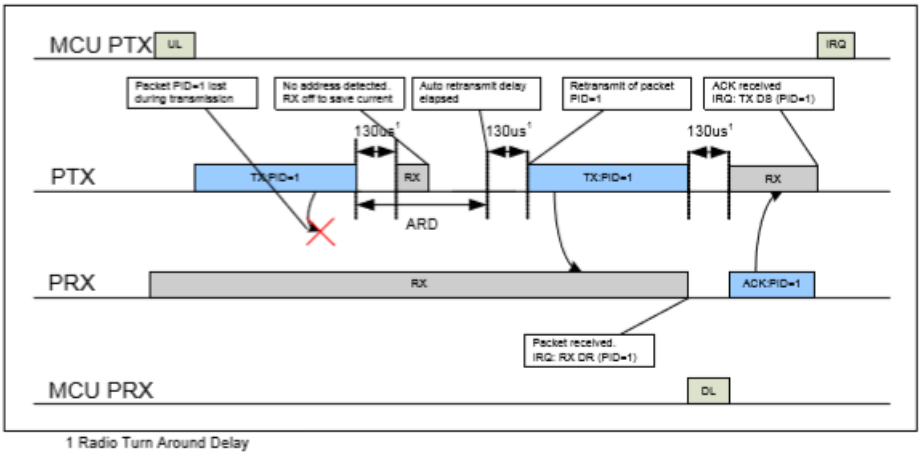
	Byte 4	Byte 3	Byte 2	Byte 1	Byte 0
Data pipe 0 (RX_ADDR_P0)	0xE7	0xD3	0xF0	0x35	0x77
Data pipe 1 (RX_ADDR_P1)	0xC2	0xC2	0xC2	0xC2	**0xC2**
Data pipe 2 (RX_ADDR_P2)	0xC2	0xC2	0xC2	0xC2	**0xC3**
Data pipe 3 (RX_ADDR_P3)	0xC2	0xC2	0xC2	0xC2	**0xC4**
Data pipe 4 (RX_ADDR_P4)	0xC2	0xC2	0xC2	0xC2	**0xC5**
Data pipe 5 (RX_ADDR_P5)	0xC2	0xC2	0xC2	0xC2	**0xC6**

Di seguito è rappresentato il meccanismo di auto acknowledgement. Nel caso di singola trasmissione con ricezione dell'ACK, dopo che il pacchetto è stato trasmesso dal PTX e ricevuto dal PRX quest'ultimo invia un messaggio di ACK al PTX



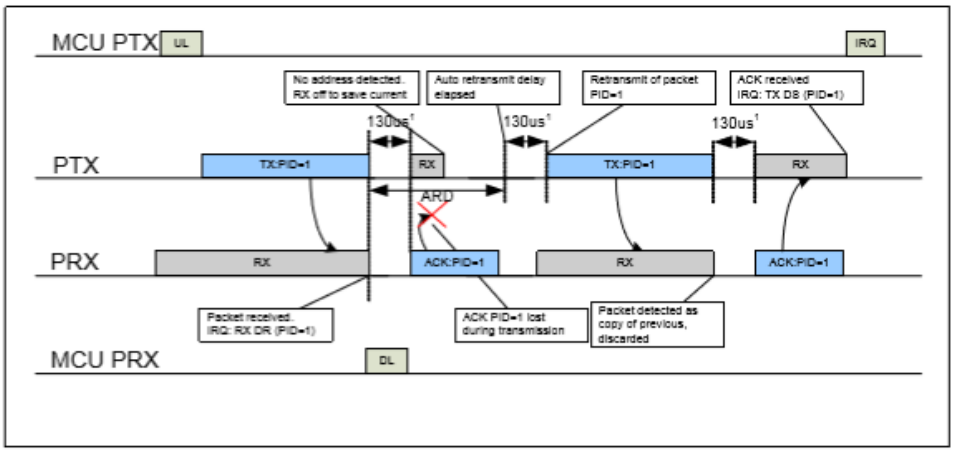
1 Radio Turn Around Delay

Se, invece, il pacchetto si perde durante la trasmissione, esso viene ritrasmesso solo dopo che il PTX non riceve l'ACK entro un certo periodo di tempo.



1 Radio Turn Around Delay

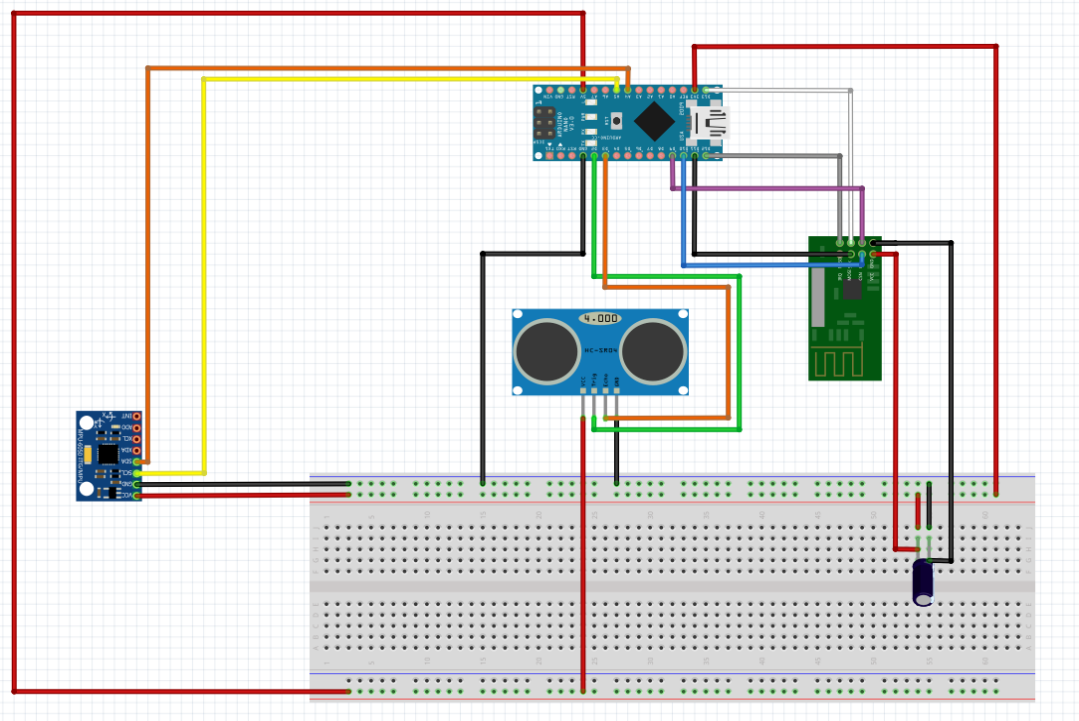
Infine, si può verificare lo scenario in cui il pacchetto di ACK viene perso. In questo caso il PTX ritrasmette il dato ma il PRX, una volta verificato che si tratta di una copia di un pacchetto già ricevuto, lo scarta e rinvia l'ACK.



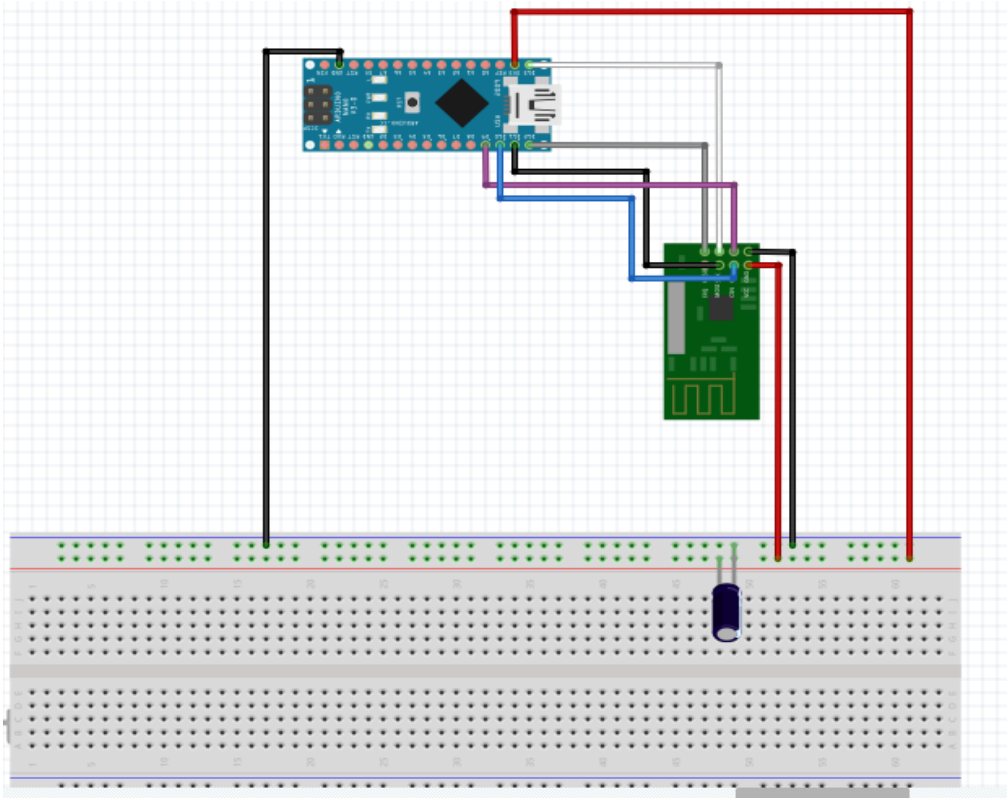
1 Radio Turn Around Delay

1.4 Circuito

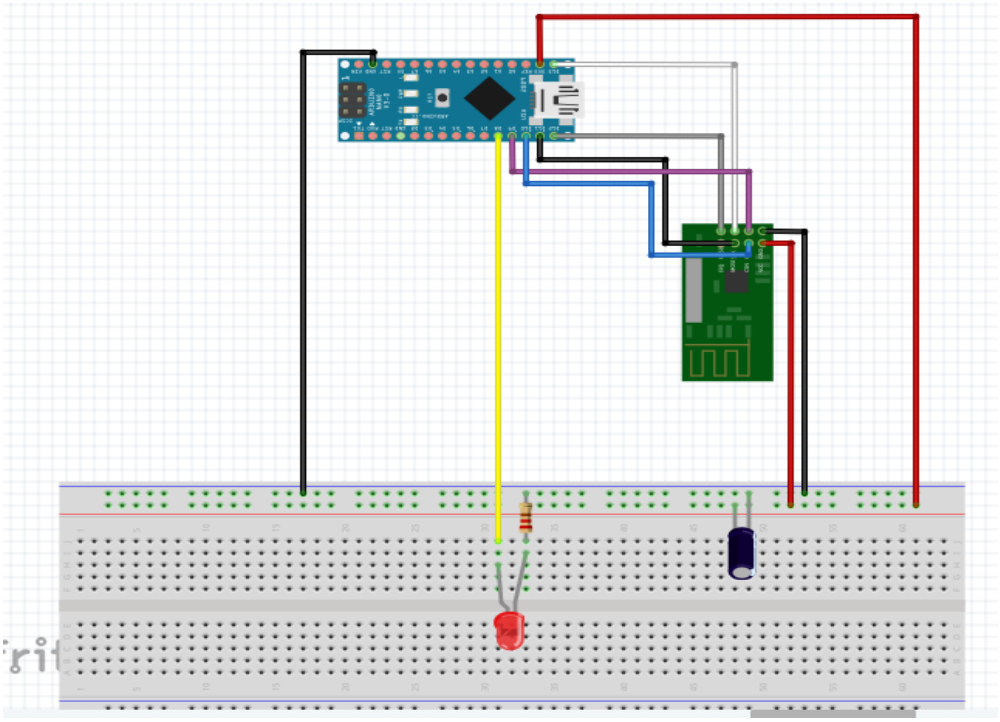
Nel nostro progetto in scala sono stati utilizzati i seguenti circuiti.



AUTOMOBILE



ANTENNA BORDO STRADA



OSPEDALE

Com’è possibile notare, è stato posto un condensatore da 100µF ai capi dell’antenna per stabilizzare la tensione.

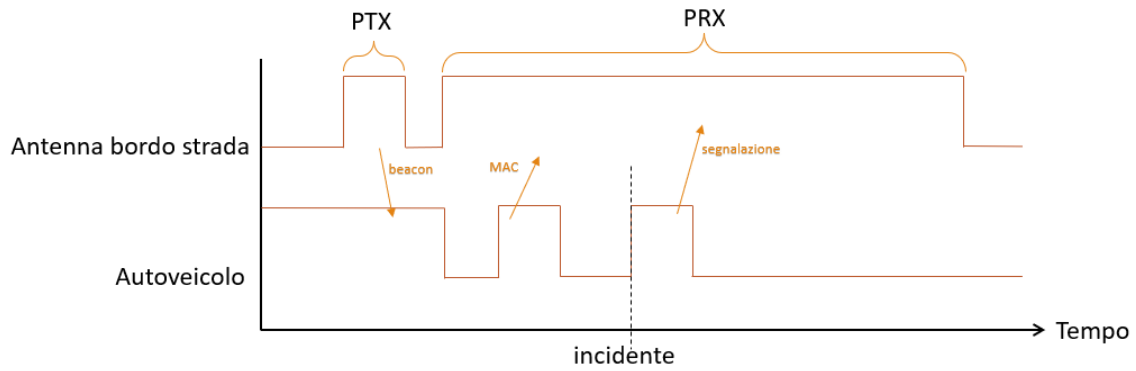
2. Analisi del progetto

Per realizzare il progetto in scala sono stati utilizzati:

- 2 macchinine telecomandate su cui sono stati montati per ciascuna un accelerometro, due sensori di distanza ed un'antenna
- 2 antenne che rappresentano l'antenna bordo strada ed una che rappresenta l'ospedale

Ciascuna antenna bordo strada invia periodicamente dei messaggi di beacon a tutte le automobili presenti nel suo range di copertura. Le automobili che ricevono il beacon rispondono all'antenna inviando il loro indirizzo MAC. Tale indirizzo viene inserito nella MAC TABLE dell'antenna e rimane memorizzato in essa per 10 cicli, in questo modo l'antenna conosce le automobili presenti nella sua regione di copertura così da poter comunicare in unicast con ciascuna di esse all'occorrenza. Se nel frattempo la macchina non risponde più ai messaggi di beacon, il suo indirizzo MAC scade e viene eliminato dalla MAC TABLE.

In caso di incidente la macchina invia un messaggio di allarme all'antenna con la quale ha comunicato fino a quel momento. Quest'ultima inoltra il messaggio in broadcast a tutte le automobili vicine al fine di evitare ulteriori incidenti ed alle antenne vicine affinché esse lo possano inoltrare all'ospedale più vicino (processo di flooding). Per evitare zone di buio le antenne sono poste in modo tale che parte dei loro range si sovrappongano. In questo modo, però, può capitare che una automobile si trovi in questa zona di interdizione, dove cioè viene coperta da due diverse antenne. In questo caso si è deciso di inviare il messaggio di allarme solo ad una delle due antenne e la scelta è effettuata in modo casuale.



Di seguito si è analizzato lo stack protocollare proposto per il funzionamento del progetto.

A livello 2 è stato utilizzato RFID per l'identificazione delle macchine e la comunicazione tra macchine e antenna.

A livello 3 si è pensato di utilizzare iPv6 perché in questo modo ad ogni macchina è possibile associare un indirizzo IP univoco e garantire una più efficiente gestione del pacchetto. Tuttavia, poiché le antenne utilizzate possono trasmettere al più 32 byte di payload di livello 2, è stato utilizzato iPv4 che riesce a garantire un header più piccolo. L'header di livello 3 è stato settato come rappresentato in tabella.

Per quanto concerne la comunicazione dell'incidente, si è deciso di comunicarlo mediante processo di flooding.

<table>
<tr><td>version:
0100</td><td>Header Lenght:
0101</td><td>Tos:
00000000</td><td colspan="2">Total Lenght:
0000000000011011</td></tr>
<tr><td colspan="3">Identification:
00000000</td><td>Flags:
010</td><td>Fragment Offset:
0000000000000</td></tr>
<tr><td colspan="2">Time to live:
00000110</td><td>Protocol:
00000110</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

3. Sviluppi futuri

Nel progetto presentato sono state proposte soluzioni ideali solo per un modello in scala del dispositivo. Risulta, dunque, necessario dover proporre una soluzione per un possibile utilizzo su scala reale.

Una possibile soluzione per la comunicazione tra veicolo ed antenna bordo strada è quella di utilizzare la tecnologia basata sulle reti VANET (**v**ehicular **a**d hoc **net**work).

Una rete VANET permette ai veicoli di comunicare tra loro oppure con infrastrutture stradali munite di sensori. Una rete veicolare è composta da dispositivi a bordo dei veicoli denominati OBU (On Board Unit) e opzionalmente, da dispositivi fissi installati ai margini della strada denominati RSU (Road Side Unit). Le entità appartenenti ad una rete VANET possono comunicare in diversi modi:

- V2V (Vehicle-to-Vehicle) per la propagazione del warning: Ci sono situazioni in cui è necessario inviare un messaggio a un veicolo specifico oppure ad un gruppo di essi. Ad esempio, quando viene rilevato un incidente, è necessario inviare un messaggio di avviso ai veicoli in arrivo per aumentare la sicurezza del traffico.

- V2V (Vehicle-to-Vehicle) per la comunicazione di gruppo: Solo i veicoli dotati di alcune caratteristiche possono partecipare a questa comunicazione. Queste caratteristiche possono essere statiche (ad esempio veicoli della stessa impresa) o dinamiche (ad esempio veicoli sulla stessa area in un intervallo di tempo).

- V2V (Vehicle-to-Vehicle) per beaconing: I messaggi beacon vengono inviati periodicamente ai veicoli vicini. I beacon vengono inviati solo ai veicoli comunicanti 1-hop, cioè non vengono inoltrati. In realtà, sono utili per il routing di protocolli, in quanto consentono ai veicoli di scoprire il migliore vicino per indirizzare un messaggio.

- I2V/V2I (Vehicle to Infrastructure) per warning: Questi messaggi vengono inviati dall'infrastruttura (tramite RSU) o da un veicolo quando viene rilevato un pericolo potenziale. Sono utili per migliorare la sicurezza stradale. Ad esempio, un'infrastruttura potrebbe inviare un messaggio ad un veicolo che si avvicina ad un incrocio quando potrebbe verificarsi una possibile collisione.

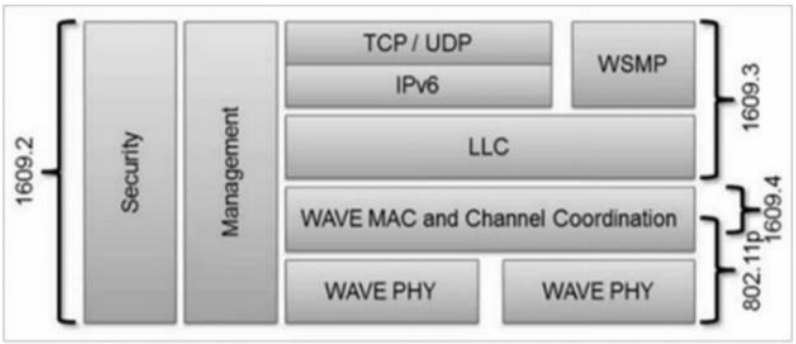
Le applicazioni relative alle reti veicolari possono essere di quattro tipi:

1. Informazioni generali: Servizi per i quali la perdita di messaggi non rappresenta nessun tipo di problema.
2. Informazioni di sicurezza: Servizi per i quali è fondamentale non perdere dei messaggi per non compromettere la sicurezza della guida.
3. Controllo del tragitto individuale: Servizi utili a migliorare la sicurezza alla guida.

4. Controllo del tragitto di gruppo: Servizi che cercano di regolare il flusso generale dei veicoli.

Lo standard su cui è basata la tecnologia VANET è chiamato **WAVE** (**W**ireless **A**ccess for **V**ehicular **E**nvironments) o anche **IEEE 802.11p.**

Lo standard 802.11p viene approvato dall'IEEE nel giugno del 2010 con lo scopo di rendere il livello fisico e MAC di 802.11 idonei alla comunicazione tra veicoli. Queste estensioni derivano dal fatto che due OBU oppure un OBU e un RSU hanno la necessità di completare uno scambio di dati in tempi brevi. In 802.11, in modalità infrastruttura, una stazione deve autenticarsi e associarsi ad un Access Point prima di poter inviare i propri dati, in modalità ad hoc, le due stazioni devono associarsi a Service Set Identifier (SSID) e Basic Service Set Indetifier (BSSID) comuni prima di poter scambiare dati. Entrambe le procedure implicano un tempo di esecuzione superiore al tempo disponibile di una rete veicolare. In 802.11p viene introdotta una modalità che consente a due stazioni di poter comunicare direttamente tra loro, anche se non fanno parte dello stesso BSS o IBSS, eliminando le procedure di associazione e autenticazione. In questo modo, il livello MAC non può utilizzare gli algoritmi di cifratura per verificare le credenziali delle altre stazioni. Dato che l'integrità dei dati trasmessi è un requisito fondamentale per le VANET, l'autenticazione viene gestita dai livelli superiori attraverso lo standard 1609.

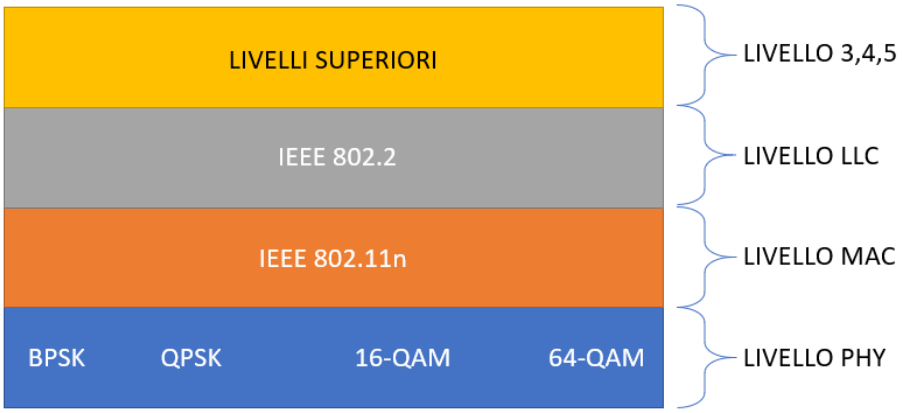


Per quanto concerne invece la comunicazione tra antenne bordo strada, è possibile utilizzare uno degli standard della IEEE 802.11, come ad esempio lo standard **IEEE 802.11n**.

Le caratteristiche salienti di questo standard sono le seguenti:

- Data rate 600Mbps
- Operante ad una frequenza di 2.4 GHz o 5 GHz
- Tecnologia MIMO, che permette l'utilizzo di più antenne per trasmettere e ricevere dati

- Modulazione utilizzate BPSK, QPSK, 16-QAM, 64-QAM



Il vantaggio nell'utilizzo di tale soluzione è quello di usare uno standard (IEEE 802.11p) che è stato ideato per la comunicazione tra veicoli e tra veicoli ed antenne. In questo modo è possibile utilizzare questa soluzione non solo per segnalare un incidente ma anche per scambiare informazioni utili quali condizioni del traffico, condizioni stradali ed avvisi di vario genere. D'altra parte tale soluzione presenta l'inconveniente di essere limitata sul range di comunicazione: infatti ciascun veicolo può comunicare solo fino a 250m con l'antenna in condizioni ottimali e ciascuna antenna non può essere distante più di 100m circa dall'altra per poter inoltrare il segnale dell'incidente.

Un'altra soluzione è rappresentata dallo standard **IEEE 802.16e** che deriva da IEEE 802.16 (WiMax) ma adattato ai dispositivi mobili (Mobile WiMax).

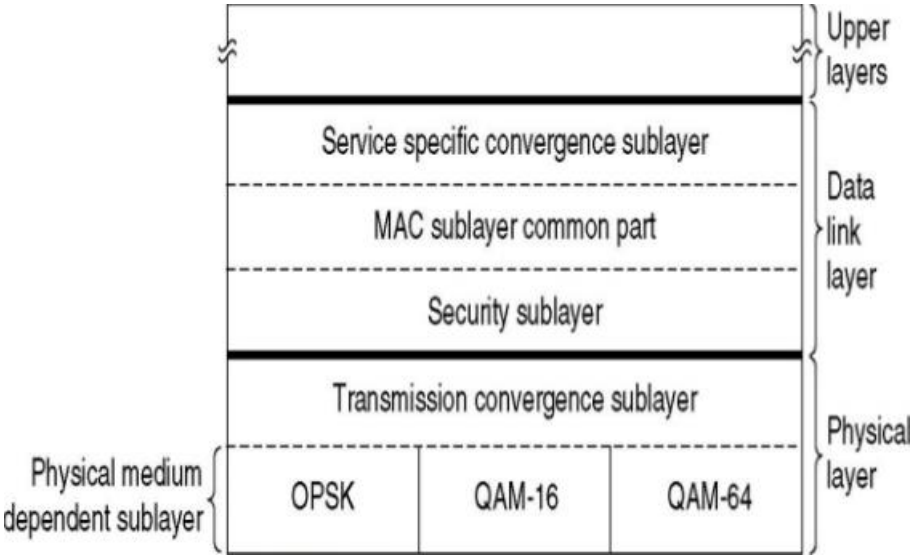
Le caratteristiche principali dello standard IEEE 802.16e sono le seguenti:

- Frequenza di trasmissione 3.5 Ghz (in Europa)
- Raggio di copertura delle celle variabile fino a 56 km con antenne omnidirezionali.
- Operante anche in condizioni di scarsa visibilità (NLOS, Non-Line of Sight)
- Bit Rate di 16Mbps
- Modulazione OFDMA
- Larghezza di banda variabile da 1.5MHz a 20MHz

I dispositivi compongono una rete WiMax sono due: la Base Station (BS) e le Subscriber Station (SS). Il ruolo principale svolto dalla BS è quello di allocare la banda necessaria alle varie SS, ricevere i segnali inviati dalle SS connesse, rigenerare il segnale ricevuto e ritrasmetterlo verso la destinazione. Una BS quindi avrà un numero variabile di SS connesse e sarà a sua volta connessa ad altre BS che gestiscono aree diverse. Quindi, come è intuitivo pensare, nel nostro progetto le SS sono rappresentate dai veicoli mentre le BS sono rappresentate dalle antenne. Collegando più Base Station si possono ottenere reti anche di grosse dimensioni e, dato che una BS gestirà solo una

parte della rete, in caso di malfunzionamenti o guasti rimarrà isolata solo una parte della rete e non la rete nella sua totalità.

Il protocol stack dello standard WiMax presenta gli stessi livelli dello stack TCP/IP ma in più presenta un *sottolivello di convergenza alla trasmissione* a livello fisico ed un *sottolivello di convergenza al servizio* con un *sottolivello di sicurezza* a livello MAC.



A livello fisico, il WiMax può presentare tre differenti tipi di modulazione del segnale (QPSK, 16-QAM, 64-QAM).

Per quanto concerne l'autenticazione, ogni SS di una rete WiMax possiede un certificato digitale che contiene la chiave pubblica assegnata a quel particolare client e il MAC address della scheda di rete presente nel dispositivo. Sostanzialmente quando un client richiede l'accesso alla BS quest'ultima controllerà il certificato digitale del client e se lo ritiene valido, ovvero se il MAC address dell'SS che richiede l'accesso è presente nell'archivio dei client autorizzati nella BS, il terminale viene autenticato nella rete e viene deciso quanta banda riservargli.

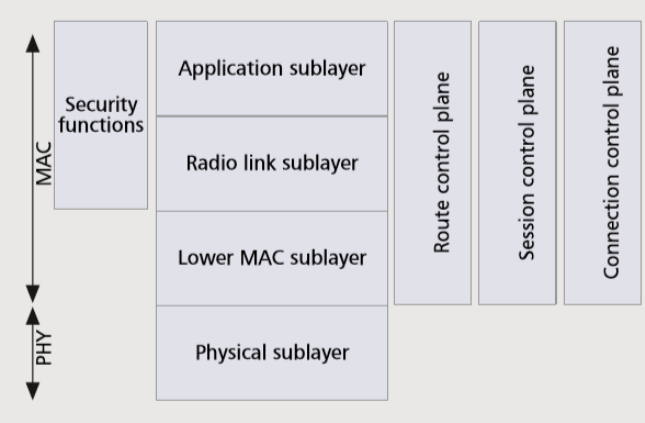
Il processo di autenticazione in WiMax è abbastanza complesso in quanto richiede la generazione di più chiavi e dell'invio di diversi pacchetto prima di una reale connessione di una SS ad una rete. Questa complessità di autenticazione è uno dei punti di forza di questo standard per la sicurezza di autenticazione e confidenzialità dei pacchetti scambiati, ma nel contempo rappresenta un punto di debolezza in quanto c'è il rischio che il veicolo possa subire un incidente durante l'autenticazione e quindi che il segnale non arrivi all'antenna.

Una delle caratteristiche principali di una rete WiMax è quella di funzionare, in maniera abbastanza affidabile, in condizioni di NLOS (Non Line Of Sight) ovvero funzionare quando tra due BS, che vogliono comunicare tra loro, ci sono grossi ostacoli che non

consentono di "vedersi". La continuità di funzionamento è stata raggiunta grazie all'uso della tecnica OFDMA. La tecnologia OFDMA è un'evoluzione della tecnologia OFDM la quale si basa sul principio di dividere i dati da trasmettere in sotto-flussi trasmissivi su portanti separate in frequenza ed in questo modo viene evitata l'interferenza tra i vari flussi trasmissivi.

Complessivamente, quindi, lo standard IEEE 802.16e riesce a superare gli ostacoli presenti nello standard IEEE 802.11/802.11p in quanto permette una trasmissione sicura ed efficace anche a diversi km di distanza tra auto ed antenna. Naturalmente in presenza dell'incidente l'auto dev'essere in grado di mandare la propria posizione all'antenna. Lo svantaggio più evidente è quello inerente all'eccessivo tempo di autenticazione del veicolo.

Infine, un'ultima soluzione è rappresentata dallo standard **IEEE 802.20** o **Mobile Broadband Wireless Access (MBWA)**, che rappresenta una valida alternativa al Mobile WiMax in quanto è adatto per la comunicazione tra dispositivi fissi e mobili. Tale standard è molto simile a quello appena visto: anche qui sono definiti una stazione base (AN, Access Network) ed un dispositivo che comunica con essa (TA Terminal Access). I livelli PHY e MAC tipici di tale standard sono organizzati come mostrato in figura.



Il livello fisico fornisce la struttura del canale, la potenza in uscita, il tipo di modulazione e le specifiche di codifica.

Il livello MAC fornisce cinque tipi di servizi:

- Servizi di controllo delle rotte (Route Control Plane): per il controllo, creazione ed eliminazione delle rotte;
- Servizi di controllo della sessione (Session Control Plane): per la configurazione dei protocolli e definizione dei parametri interni alla comunicazione tra AN e AT;

- Servizi di controllo della connessione (Connection Control Plane): per la creazione della connessione wireless tra nodi e servizi di manutenzione della stessa;
- Servizi di sicurezza (Security functions): per la crittografia dei messaggi;

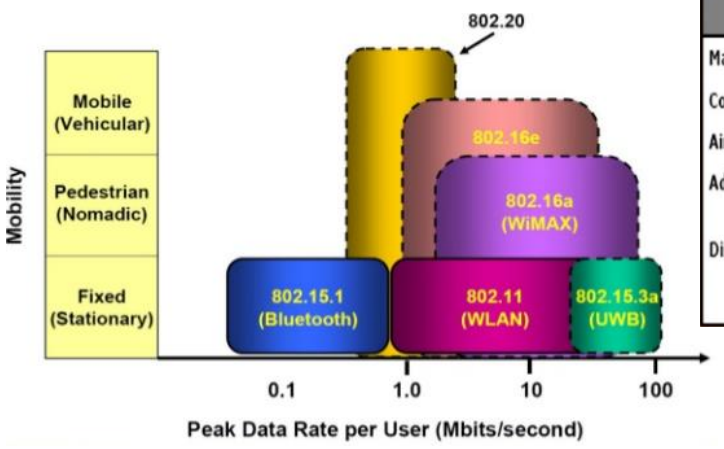
Esso è organizzato in tre sottolivelli.

- Il sottolivello LOWER MAC definisce le procedure usate per ricevere e trasmettere bit in base al livello fisico.
- Il sottolivello RADIO LINK definisce i protocolli che forniscono servizi ai livelli superiori come sicurezza dei frame, multiplexing e le varie specifiche di QoS.
- Il sottolivello APPLICATION fornisce molteplici protocolli per supportare la comunicazione tra un AN ed un AT. Inoltre, specifica il protocollo IRTP (InterRoute Transport Protocol) per il trasporto di pacchetti da e verso altri nodi. Per supportare requisiti funzionali per la privacy, autenticazione dei dispositivi e per le autorizzazioni a determinati servizi, il sottolivello di application include anche il protocollo EAP (Extensible Authentication Protocol). Infine, il livello application supporta il protocollo IP (sia IPv4 che IPv6) a livello 3.

Le caratteristiche principali di questo protocollo sono:

- Frequenza massima di lavoro 3.5GHz
- Larghezza di banda di 1.25MHz, 5MHz e 10MHz
- Funzionante con dispositivi mobili fino ad una velocità di 250 km/h
- Adatto per vaste aree geografiche
- Coesistenza con altre tecnologie
- Sicurezza

In definitiva, tale standard risulta essere il più adatto per la comunicazione tra veicoli ed antenne (range di copertura più ampio, velocità dei dispositivi mobili più elevata) ma presenta lo stesso svantaggio dello standard Mobile WiMax: infatti anche questo standard risulta essere molto sicuro ma nel contempo richiede un tempo di accesso

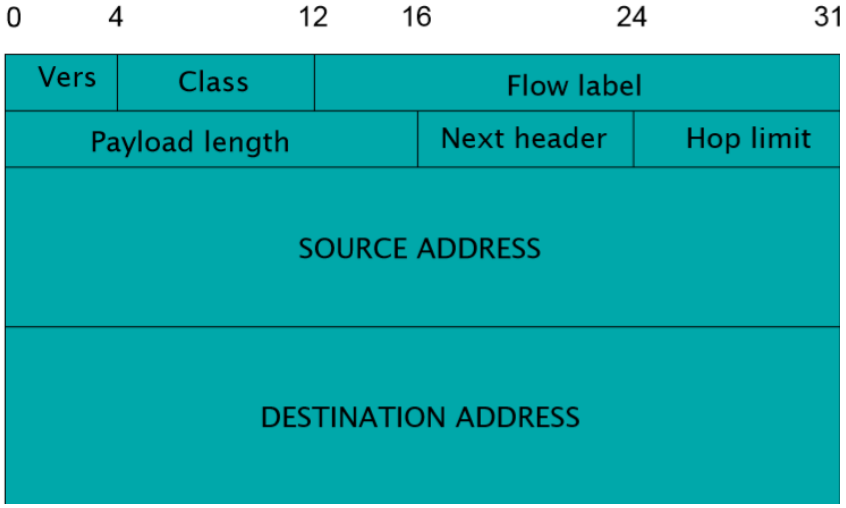


	3G	Wi-Fi: 802.11	WiMAX: 802.16	Mobile-Fi: 802.20
Max speed	2Mbps	54Mbps	100Mbps	16Mbps
Coverage	Several miles	300 feet	50 miles	Several miles
Airwave	Licensed	Unlicensed	Either	Licensed
Advantages	Range, mobility	Speed, price	Speed, range	Speed, mobility
Disadvantages	Slow, expensive	Short range	Interference issues?	High price

alla rete più lungo. Inoltre quest'ultimo risulta essere anche il più costoso standard dei tre proposti.

Per quanto concerne il livello di rete, tutte le soluzioni proposte sono in grado di supportare a livello 3 il protocollo IPv6. Quest'ultimo risulta essere il più adatto a questo tipo di progetto in quanto presenta i seguenti vantaggi:

- Possibilità di assegnare indirizzi IP statici a ciascuna macchina (esistono $3.4*10^{38}$ indirizzi)
- Possibilità di essere usato anche nelle reti IPv4
- Gestione più efficiente dei pacchetti (no fragmentation, ICMP con nuove funzionalità, nuove tecniche di routing)
- Gestione della sicurezza dei pacchetti a livello di rete (protocollo IPsec)



Avendo proposto OSPF come protocollo di routing per IPv4, è analogamente possibile utilizzare OSPFv3 come protocollo di routing per IPv6.