

---

## Indice

Introduzione .....	I
Capitolo 1. Le Reti Wireless e lo Standard 802.11p .....	1
1.1 Le Reti Wireless .....	1
1.2 IEEE 802.11 .....	7
1.3 IEEE 802.11p .....	16
1.3.1 Standard IEEE 1609.4 .....	19
1.3.2 Standard WAVE .....	22
Capitolo2. Le VANET, il MAC e il Routing .....	24
2.1 Le VANET .....	24
2.1.1 DSRC .....	29
2.2. Il livello MAC .....	33
2.3 Il Routing .....	45
2.3.1 Topology Based Routing Protocols .....	47
2.3.2 Position Based Routing Protocols .....	50
Capitolo 3. Protocolli ed Algoritmi MAC .....	59
3.1 ALOHA puro .....	62
3.1.1 RR-ALOHA .....	62
3.2 CSMA e CSMA-CD .....	64
3.3 SRMA .....	64
3.3.1 SOTDMA .....	65
3.3.2 COMB .....	66
3.4 MACA .....	73
3.5 MC-MAC, BTMA e FPRP .....	74
3.6 AD-HOC MAC .....	75

---

3.7 D-MAC .....	76
3.8 Distributed Ad-Hoc Multi Channel Coordination Scheme .....	78
3.8.1 V-MESH .....	78
3.9 Centralized Ad-Hoc Multi Channel Coordination Scheme .....	79
3.9.1 DCAP .....	79
3.10 Protocolli MAC Multicanale .....	79
3.11 Protocolli MAC Multicanale per Reti Ad-Hoc .....	80
3.11.1 DYNAMMA, SNMS e CAM-MAC .....	80
3.12 Multi-Channel MAC Protocols For VANET .....	82
3.12.1 VMMAC (VANET Multicanale MAC) .....	83
3.12.2 DMMAC .....	84
3.12.3 RAMC .....	86
3.12.4 CMMP .....	86
3.13 PCF .....	88
3.14 EDCF .....	89
3.14.1 I protocolli PCF ed EDCF messi a confronto .....	91
Capitolo 4. Analisi e Campagna di Simulazioni .....	94
4.1 Il simulatore OMNet++ .....	94
4.2 Veins .....	99
4.3 SUMO .....	102
4.4 Importazione della mappa .....	105
4.5 Risultati della campagna di simulazioni .....	108
Conclusioni .....	133
Bibliografia .....	136

---

## Introduzione

Nel campo dell'Informatica, delle Telecomunicazioni e delle Radiocomunicazioni la comunicazione senza aiuto di fili e cablaggio (in inglese definito come *wireless*) [1] consente la comunicazione tra dispositivi elettronici che non hanno bisogno di cavi come invece succede per le reti cablate (definite come *wired*). Questo tipo di rete viene definita come *Rete Wireless* e i rispettivi dispositivi di comunicazione atti a mettere in opera tale rete vengono anch'essi denominati dispositivi *wireless*. In sostituzione dei cavi vengono utilizzate le onde radio a bassa potenza, la radiazione infrarossa, il laser oppure i dispositivi *Bluetooth*. Grazie al progresso tecnologico in atto le Reti Wireless vengono utilizzate ed impiegate per un crescente numero di attività, specialmente riguardanti le imprese, ma non solo: basti pensare al largo impiego delle installazioni delle suddette reti nelle università, negli uffici e strutture pubbliche, negli hotel e negli aeroporti. Grazie anche all'abbattimento dei costi, i quali qualche anno fa risultavano eccessivi, le Reti Wireless hanno fatto il loro ingresso anche nella quotidianità familiare delle case, consentendo così la condivisione dei dati tra i computer della famiglia e l'accesso ad *Internet*. La tecnologia *wireless* è considerata il futuro della connettività se si considerano il *Wi-Fi*, il *Wi-MAX* ed il *4G*. I sistemi di comunicazione *wireless* sono composti da un trasmettitore, atto a trasmettere il segnale radio ed un ricevitore, atto a ricevere il segnale radio emanato, entrambi elementi addetti all'irradiazione elettromagnetica; essi possono essere antenne, laser oppure foto-rivelatori e le frequenze elettromagnetiche che vengono utilizzate per la comunicazione variano a seconda dello standard che viene utilizzato, implementando una trasmissione che può avvenire in modalità monodirezionale, bidirezionale *half-duplex* e bidirezionale *full-duplex*.

---

La motivazione più considerevole per la quale si decide di installare una Rete Wireless è rappresentata proprio dall'abolizione del cablaggio che in alcuni casi può risultare molto fastidioso a causa del sovraccarico di fili dei dispositivi a corto raggio, ma soprattutto a causa dei costi onerosi per quanto riguarda principalmente la messa in posa delle portanti fisiche delle reti informatiche di medio/lungo raggio: infatti un dispositivo *wireless*, grazie alla ricetrasmisione di onde radio, riesce a ricoprire una zona di utenza molto più ampia ad un costo di messa in opera decisamente più economico. Inoltre la tecnologia *wireless* consente non solo di risolvere il problema del cablaggio, ma permette anche la mobilità utente del servizio all'interno delle reti radiomobili; un esempio di questo campo di applicazione possono essere le reti cellulari. Sono presenti comunque degli svantaggi rispetto alle reti cablate, quali una Qualità del Servizio (definita come QoS, abbreviativo di *Quality of Service*) inferiore, delle problematiche relative alla sicurezza della comunicazione oppure all'eventuale inquinamento elettromagnetico.

Le Reti Wireless possono appartenere a diverse tipologie [1]:

- ✓ Reti WPAN (abbreviativo di *Wireless Personal Area Network*), ovvero delle reti a livello domestico;
- ✓ Reti WLAN (abbreviativo di *Wireless Local Area Network*), ovvero delle reti locali senza fili e che quindi non necessitano di cavi per collegare gli *host* della rete tra di loro e ad Internet, conosciute anche come reti Wi-Fi;
- ✓ Reti WAN (abbreviativo di *Wide Area Network*), conosciute anche come reti geografiche, ovvero una tipologia di rete che ha un'estensione territoriale pari ad una o più regioni geografiche e che risulta superiore sia a quella della rete locale che a quella della rete metropolitana;
- ✓ Reti BWA (abbreviativo di *Broadband Wireless Access*), ovvero una famiglia di tecnologie il cui scopo è quello di fornire accesso ad Internet ad alta velocità

---

di trasmissione e *wireless* su grandi aree, che sta conoscendo grande diffusione grazie alla tecnologia Wi-MAX;

- ✓ Reti Cellulari Radiomobili, come ad esempio il GSM (abbreviativo di *Global System for Mobile Communications*), il GPRS (abbreviativo di *General Packet Radio Service*), l'EDGE (abbreviativo di *Enhanced Data rates for GSM Evolution*), l'UMTS (abbreviativo di *Universal Mobile Telecommunications System*) e l'HSPA (abbreviativo di *High Speed Packet Access*);
- ✓ Reti Satellitari.

I principali standard ai quali le Reti Wireless si riferiscono sono:

- ✓ Standard *Bluetooth* per la connessione computer-periferiche (usato anche per connessioni tra telefoni cellulari);
- ✓ Standard IEEE 802.11 per le reti WLAN e le reti Wi-Fi;
- ✓ Standard IEEE 802.16 per le reti metropolitane WMAN;
- ✓ Il GPRS e l'EDGE per la trasmissione dati sulla rete telefonica cellulare GSM;
- ✓ L'HSDPA per la trasmissione di dati ad alta velocità su reti cellulari radiomobili.

Lo Standard 802.11p [2] [3] [4] [5] è un emendamento approvato come evoluzione dello Standard 802.11 atto a definire miglioramenti necessari a supportare le applicazioni ITS (abbreviativo di *Intelligent Transportation Systems*) e per standardizzare i prodotti commercializzati sotto la categoria di dispositivi Wi-Fi. Tutto ciò include lo scambio di dati tra i veicoli e le infrastrutture stradali nelle reti veicolari ad alta velocità nell'intorno della frequenza dei 5.9 GHz (più esattamente si tratta dell'intervallo dei 5,85 GHz – 5.925 GHz). Inoltre pone le basi sulle quali si fonda lo Standard 1609.4 [6]. Lo Standard 802.11p è stato pensato proprio per le comunicazioni a corto raggio dello Standard DSRC [7] (abbreviativo di *Dedicated Short-Range Communications*) che descrive l'architettura delle comunicazioni utilizzate nelle reti veicolari per applicazioni quali il pagamento dei pedaggi, i servizi di

---

sicurezza dei veicoli e le trasmissioni inter-veicolari. Lo scopo ultimo di questo standard è l'implementazione di una grande rete che consente la comunicazione tra i veicoli e tra veicolo e vari punti di accesso stradale. Dal momento che la comunicazione tra i veicoli e l'infrastruttura stradale può essere di breve durata, l'emendamento 802.11p definisce un metodo atto a scambiare i dati attraverso quel rapido collegamento prescindendo dalla necessità di stabilire una connessione di base attraverso un *set* di servizi di base (*Basic Service Set*, abbreviato in BSS), proprio dello Standard 802.11, e quindi, senza la necessità di attendere che le procedure di associazione e di autenticazione siano completate prima di scambiare dati; a tale scopo le stazioni radio ed i veicoli che appartengono alla categoria 802.11p utilizzano un BSSID (abbreviativo di *Basic Service Set Identification*) all'interno dell'intestazione dei *frame* che vengono scambiati nella rete, offrendo la possibilità di iniziare ad inviare e tramettere messaggi appena i veicoli raggiungono quel canale di comunicazione. Tutto ciò comporta che i meccanismi di autenticazione e riservatezza dei dati offerti dallo Standard 802.11 non possono essere utilizzati in questo scenario, delegando agli strati superiori l'implementazione di tali funzionalità. Inoltre viene introdotto un nuovo *frame* di gestione per la sincronizzazione temporale delle stazioni attraverso un riferimento temporale comune.

Lo standard 802.11p viene utilizzato principalmente nelle comunicazioni delle reti veicolari. Una rete VANET [8] (abbreviativo di *Vehicular Ad-Hoc Network*) utilizza le automobili che si muovono in una mappa stabilita come nodi mobili per creare una rete. In una VANET ogni vettura rappresenta un *router wireless* denominato "nodo" e viene consentita la connessione di autovetture a distanza di circa 100 – 300 metri l'una dall'altra creando una rete ad ampia gamma. I veicoli possono entrare oppure abbandonare la rete in base al campo di copertura del segnale; inoltre le comunicazioni sono prettamente rappresentate da messaggi relativi alla sicurezza stradale. Le reti VANET si differenziano dalle reti MANET

---

(abbreviativo di *Mobile Ad-Hoc Network*) dal fatto che i nodi della rete, ovvero i veicoli, non si muovono a caso, ma il loro comportamento tende ad essere organizzato in una precisa porzione di mappa seguendo strade asfaltate. Inoltre le interazioni con le apparecchiature stradali possono essere altresì determinate in modo preciso ed organizzato. Le reti VANET si avvalgono di molteplici tecnologie di *net-working* che vengono integrate per un miglior funzionamento, quali il Wi-Fi, lo standard IEEE 802.11p, lo standard WAVE [9] (abbreviativo di *Wireless Access for Vehicular Environments*), lo standard IEEE 1609.4, il Wi-MAX, il *Bluetooth* ed altri. Le comunicazioni in una rete VANET possono avvenire tra i veicoli (*vehicle-to-vehicle* abbreviato in V2V) oppure tra un veicolo e un dispositivo di controllo stradale (*vehicle-to-infrastructure* abbreviato in V2I). Tutto ciò si basa sulla consapevolezza della poca sicurezza sulle strade e sulla determinazione di riuscire a porre rimedio. L'idea di base è proprio la comunicazione fra i veicoli riuscendo ad ottenere uno scambio continuo di informazioni atto a garantire una maggior sicurezza degli utenti della strada.

Per poter garantire una trasmissione efficiente, si ha bisogno di uno strato MAC [4] [5] (abbreviativo di *Medium Access Control*) in modo tale da poter garantire alle stazioni che vogliono trasmettere una comunicazione veloce ed efficace. Lo strato MAC implementa uno schema di accesso al mezzo di tipo EDCA (abbreviativo di *Enhanced Distributed Channel Access*) basato sulla tecnica del CSMA/CA (abbreviativo di *Carrier Sense Multiple Access con Collision Avoidance*) nella quale le stazioni sono in competizione per l'accesso al canale condiviso. Una stazione che ha intenzione di trasmettere, inizia ascoltando il canale: se risulta occupato viene attivato un timer (tempo di *backoff*) che viene decrementato nei periodi di inattività del canale e mantenuto costante nel momento in cui il canale è occupato da trasmissioni. Quando il timer arriva a zero, la stazione ascolta nuovamente il canale: se lo trova nuovamente occupato ripete la procedura precedente, altrimenti prenota la trasmissione ed attende un altro istante; se il canale continua ad essere

---

libero può tranquillamente trasmettere. Per poter “ascoltare” il canale vi sono due metodi: il *physical carrier sensing* (nel quale lo stato del canale è deciso sulla base dell’energia rilevata dall’antenna) e il *virtual carrier sensing* (basato su una tecnica di prenotazione che risulta più onerosa rispetto a quella fisica). Inoltre il livello MAC per comunicazioni *unicast* garantisce il servizio di conferma della trasmissione tramite pacchetti di tipo ACK. Al livello MAC pervengono dagli strati superiori datagrammi di tipo diverso (IP oppure WSMP) da smistare nelle code dei due diversi canali (di servizio SCH oppure di controllo CCH) in base alla priorità che è stata assegnata loro; sono presenti quattro categorie di accesso (*Access Category*, abbreviato in AC): *background*, *best effort*, *video* e *voice traffic*. Inoltre tutti i dispositivi hanno l’obbligo di monitorare il canale di controllo (CCH) anche durante l’intervallo di tempo dedicato al canale di servizio (SCH) poiché i pacchetti presenti nella sua coda con alta priorità devono essere trasmessi immediatamente. Nel momento in cui una nuova stazione si aggiunge alla rete, si rende necessaria la sincronizzazione ed il coordinamento del canale per monitorare il CCH durante il periodo opportuno e per permettere a tutte le unità di sincronizzarsi temporalmente sullo stesso riferimento. Per sopperire ad eventuali ritardi di trasmissione oppure ad errori di sincronizzazione, si è reso utile un periodo di guardia con valore di *default* di 4 msec.

La progettazione di un livello MAC applicato alle reti *ad-hoc* [11] [12] [13], ovvero le reti MANET ma soprattutto le reti VANET, che sia efficiente ed affidabile viene considerata ancora una sfida. Infatti il livello MAC è deputato all’utilizzazione efficiente del mezzo trasmissivo condiviso, ossia alla risoluzione di tutti i conflitti e le collisioni tra le trasmissioni dei nodi che usufruiscono dello stesso mezzo di comunicazione. L’interesse di diversi studiosi di tutto il mondo per questo tipo di problematiche [14] è cresciuto negli anni grazie soprattutto alle molteplici ed utilissime applicazioni di sicurezza stradale che sarebbero capaci di diminuire significativamente il numero di incidenti sulle strade. Tutto ciò tuttavia

---

implica una maggiore efficienza della comunicazione *wireless* facendo fronte al superamento di comportamenti imprevedibili del canale condiviso, al controllo delle rapide modifiche della topologia della rete ed alla rigorosa tempistica della comunicazione degli eventi. Quest'ultimo requisito risulta molto importante e fondamentale nel momento in cui si ha il bisogno di comunicare immediatamente un'imminente situazione pericolosa prima che si verifichi in modo da evitarla; tutto ciò classifica questo tipo di comunicazione come un sistema *real-time*. Comunicare un messaggio in tempo reale non necessita obbligatoriamente di un alto tasso di trasmissione oppure di un basso ritardo, bensì richiede un sistema prevedibile che sia in grado di consegnare il messaggio prima della sua scadenza, dal momento che in un sistema a tempo reale tutte le informazioni pervenute dopo il *deadline* sono inutili ed implicano inoltre gravi conseguenze per il traffico ed il sistema di sicurezza. La maggior parte dei protocolli [15] presenti in letteratura concepiti per le reti VANET è suddivisa in tre grandi gruppi: protocolli di tipo TDMA (abbreviativo di *Time Division Multiple Access*), ovvero a divisione di tempo; protocolli di tipo FDMA (abbreviativo di *Frequency Division Multiple Access*), ovvero a divisione di frequenza; infine protocolli di tipo CDMA (abbreviativo di *Code Division Multiple Access*), ovvero a divisione di codice. Inoltre si è dovuto sviluppare protocolli capaci di superare il problema delle collisioni derivanti dall'utilizzo di un unico canale MAC, formalizzando e delineando due schemi di coordinazione multicanale: *Distributed* e *Centralized Ad-Hoc* [12]. Questa linea di studio ha aperto la strada per lo sviluppo di diversi protocolli MAC multicanale.

Un protocollo di *routing* [10] governa la maniera in cui due nodi comunicano tra di loro effettuando uno scambio di informazioni, comprese la procedura di creazione di un percorso, le decisioni di inoltramento (*forwarding*), di mantenimento della comunicazione e del recupero della caduta di connessione. Vengono classificati in due grandi categorie: protocolli di *routing* basati sulla Topologia (ulteriormente classificati in *Proactive* e *Reactive*) e protocolli di *routing* basati sulla Posizione. I

---

protocolli di tipo *Proactive* sono basati su algoritmi di ricerca del percorso più breve prelevando e studiando tutte le informazioni ricevute dai nodi connessi alla rete memorizzate in tabelle condivise; ogni qual volta si verifica un cambiamento riguardante la topologia della rete, ogni nodo deve aggiornare la sua tabella ed inoltrarla. Viceversa, i protocolli di tipo *Reactive* (chiamati anche *on demand*) iniziano la scoperta del cammino solo nel momento in cui i nodi hanno bisogno di comunicare con gli altri nodi della rete. Il Capitolo 3 presenterà alcuni protocolli di *routing* proposti in letteratura introdotti nelle MANET, ma utilizzati ed ottimizzati per le reti VANET, prestando attenzione sul loro funzionamento e i loro aspetti positivi e negativi che variano in base alle caratteristiche della rete considerata.

Nel Capitolo 4 verranno presentate quattro diverse campagne di simulazioni per valutare il comportamento del protocollo MAC relativo allo Standard 1609.4. Sarà utilizzato l'ambiente di simulazione OMNet++ (abbreviativo di *Objective Modular Network Testbed* in C++) [16] [17], ovvero un simulatore *open source* ad eventi discreti, scritto in C++ e nato nel 2003. Questo *software* per la simulazione sarà integrato da altri due *framework* in modo da funzionare in maniera complementare e sincrona: Veins [18] (abbreviativo di *Vehicles in Network Simulation*) (un *framework open source* per l'esecuzione di simulazioni in ambienti di reti veicolari *Inter-Vehicular Communication*) e SUMO [19] (abbreviativo di *Simulation of Urban Mobility*, un pacchetto di simulazione del traffico stradale *open-source* e *portable*). In un primo momento si procederà con la sostituzione della mappa di *default* presente in OMNet++ con un'altra estratta da una porzione di mappa appartenente al centro di Cosenza; in un secondo momento e come accennato in precedenza, verranno portate avanti quattro tipi di campagne di simulazioni differenti:

- ✓ La prima campagna di simulazioni effettuata su quindici *route* (strade) caricate nel simulatore singolarmente, scelte in modo *random* e processate al variare del numero di nodi (100 nodi, 200 nodi, 300 nodi, 400 nodi e 500 nodi);

- 
- ✓ La seconda campagna di simulazioni effettuata su quindici coppie di *route* (strade), scelte ed accoppiate in modo *random* e processate al variare del numero di nodi (100 nodi, 200 nodi, 300 nodi, 400 nodi e 500 nodi);
  - ✓ La terza campagna di simulazioni effettuata su quindici combinazioni di tre *route* (strade), scelte ed abbinate in modo *random* e processate al variare del numero di nodi (100 nodi, 200 nodi, 300 nodi, 400 nodi e 500 nodi);
  - ✓ Un'ultima campagna di simulazioni effettuata su quindici *route* (strade) caricate nel simulatore singolarmente, scelte in modo *random* con numero di nodi fissato e processate al variare del valore del *bit rate* (18 Mbps e 6 Mbps).

Al termine di ogni campagna di simulazioni verranno poi presentati, studiati ed argomentati svariati grafici riportanti l'andamento di diversi parametri che spiegheranno meglio il comportamento del protocollo: *Sent Packets* (numero di pacchetti totali inviati correttamente), *Total Lost Packets* (numero totale dei pacchetti andati persi), *RXTX Lost Packets* (numero di pacchetti andati persi poiché sono stati ricevuti nel momento in cui il nodo stava trasmettendo il suo pacchetto), *SNIR Lost Packets* (numero di pacchetti scartati a causa di errori di *bit* riscontrati all'interno del *frame*), *Times Into Backoff* (numero di volte in cui il nodo è incorso nel tempo di *backoff*), *Slots Backoff* (numero di tutti gli *slot* di attesa a causa della pausa durante il tempo di *backoff*) ed infine *Total Busy Time* (tempo totale in cui il nodo, ascoltando il canale, lo ha trovato occupato). Saranno in seguito portate avanti delle tesi, avvalorate dall'andamento dei valori medi riscontrati dei parametri elencati.