ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA
SEDE DI CESENA
SCUOLA DI INGEGNERIA E ARCHITETTURA
CORSO DI LAUREA IN INGEGNERIA ELETTRONICA, INFORMATICA E DELLE TELECOMUNICAZIONI

INTERNET DEI VEICOLI, UN NUOVO PARADIGMA PER UNA MOBILITÀ INTELLIGENTE E AUTONOMA

Elaborato nel corso di:
Sistemi Distribuiti

Relatore:
Prof. Andrea Omicini

Presentata da:
Matteo Pasolini

Sessione III

Anno Accademico 2014/2015

Abstract

Grazie al continuo affinamento dell'elettronica di consumo e delle tecnologie di telecomunicazione, ad oggi sempre più *cose* sono dotate di capacità sensoriali, computazionali e comunicative, si parla così di Internet delle cose e di oggetti *smart*.

Lo scopo di questo elaborato è quello di approfondire e illustrare questo nuovo paradigma nell'ambito dell'automotive, evidenziandone caratteristiche, potenzialità e limiti. Ci riferiremo quindi più specificatamente al concetto di **Internet dei veicoli** per una gestione ottimale della mobilità su strada.

Parleremo di questa tecnologia non solo per il supporto che può dare alla guida manuale, ma anche in funzione del concetto di **guida autonoma**, di come quest'ultima beneficerà di un'interconnessione capillare di tutti gli utenti, i veicoli e le infrastrutture presenti sulla strada, il tutto in un'ottica cooperativa. Illustreremo quali sono le principali sfide per raggiungere uno scenario del genere e quali potrebbero essere le implicazioni più rilevanti.

Parole chiave: Internet of Vehicles, Intelligent Transportation System, Autonomous Driving, Mobility-as-a-Service, Internet of Things

Indice

Capitolo 1

Introduzione

Al giorno d'oggi siamo soliti definire *intelligenti* moltissimi degli oggetti di cui facciamo uso quotidianamente, basti pensare ai computer, ai telefoni cellulari o ai tablet, fino ad arrivare – in tempi ancora più recenti – a elettrodomestici, infrastrutture e persino mezzi di trasporto. Ma qual è il comune denominatore che accomuna tutte queste cose attribuendogli *intelligenza*?

La capacità fondamentale che caratterizza un oggetto cosiddetto *smart* è la possibilità di scambiare informazioni con altri oggetti che hanno la stessa capacità, al fine di arrivare a poter compiere azioni che singolarmente non avrebbero avuto l'abilità di svolgere. Si viene così a creare un **meccanismo di interazione** che apre le porte a tantissime nuove possibilità, il cui più grosso limite è probabilmente solo la fantasia.

Nell'ambito della domotica questa possibilità si traduce nella cooperazione tra classi eterogenee di oggetti ed elettrodomestici; la comunicazione, per esempio, tra l'impianto di climatizzazione e uno smartphone apre gli utenti a servizi nuovi. Il climatizzatore potrebbe venire a sapere dal telefono che ci fa da sveglia l'orario in cui ci alzeremo e sarà in grado di preparare autonomamente ed efficientemente stanze e servizi di cui avremo bisogno. Grazie al GPS integrato nello smartphone potrebbe anche riuscire proattivamente a capire che stiamo per tornare a casa, facendoci già trovare un clima ideale.

Questi tipi di servizi, senza un contatto tra i vari device, sarebbero possibili solo con l'intervento attivo delle persone.

Anche nell'ambito dell'**automotive**, su cui incentreremo questo elaborato, la possibilità di una comunicazione pervasiva apre la strada a moltissime opportunità che potrebbero anche cambiare radicalmente la mobilità su strada come la intendiamo oggi.

1.1 Quotidianità ai tempi dell'Internet dei veicoli

Monica è in procinto di uscire di casa per andare alla presentazione di un libro nella biblioteca della sua città. Tramite uno qualsiasi dei suoi terminali decide quindi di prenotare un veicolo che la venga a prendere, dato che non può andarci a piedi e i mezzi pubblici le sono scomodi da prendere in questo momento. Nel giro di qualche minuto riceve una notifica che la informa che il veicolo libero più vicino è arrivato sotto casa sua e che può salirci immediatamente. Una volta salita in macchina, Monica deve solo comunicare la sua destinazione, tramite messaggio vocale o digitandola manualmente sul display della vettura. A quel punto il veicolo parte autonomamente nella direzione da lei scelta.

Durante il viaggio, Monica può tranquillamente mettersi a leggere oppure chattare/telefonare, l'automobile è perfettamente in grado di gestire tutte le situazioni. Ad un certo punto, però, l'automobile apprende da alcuni veicoli provenienti dalla direzione opposta che una delle strade per arrivare alla biblioteca è chiusa per lavori; a questo punto il veicolo riformulerà l'itinerario con un percorso che non comprenda quella strada. Questo inconveniente si risolverà in maniera del tutto trasparente per Monica e dal suo punto di vista il viaggio proseguirà come se la deviazione non ci fosse nemmeno stata.

Una volta arrivata di fronte all'ingresso della biblioteca, Monica scende semplicemente dal veicolo e, senza minimamente preoccuparsi di posteggi o

pagamenti – visto che si tratta di un servizio pubblico in abbonamento – va alla presentazione del libro. A questo punto il veicolo è di nuovo libero e pronto per andare a servire un altro utente nelle vicinanze come Monica che ha fatto richiesta di un'automobile per spostarsi.

Terminata la presentazione del libro, Monica non deve far altro che fare richiesta col suo smartphone per un altro veicolo che la riporti a casa o dovunque altro lei voglia. Se preferisse viaggiare in compagnia potrebbe anche prenotare assieme a delle amiche un'automobile, che, una volta impostato un itinerario a più fermate, provvederà a riaccompagnarle tutte a casa.

Questo rappresenta uno degli scenari ideali a cui la ricerca scientifica e tecnologica in questo ambito vorrebbe arrivare.

1.2 Cosa affronteremo

Nel prossimo capitolo introdurremo il concetto di Internet delle cose e illustreremo brevemente il suo attuale stato dell'arte.

Nel terzo capitolo introdurremo invece l'Internet dei veicoli e daremo un'idea dei servizi che può offrire e delle sue caratteristiche.

Nel capitolo 4 vedremo più specificatamente metodi e paradigmi con cui i vari veicoli su strada potranno/dovranno comunicare, inoltre presenteremo alcuni dei più rilevanti sistemi sperimentali di supporto alla mobilità intelligente (simulati e/o svolti su strada).

Il capitolo 5 verterà sul concetto di *guida autonoma* e, dopo aver illustrato le principali tappe storiche che hanno portato alle attuali tecnologie a riguardo, vedremo il suo possibile impatto tecnologico e sociale.

Infine, nel capitolo 6, discuteremo sulle principali questioni concernenti la sicurezza informatica e la privacy degli utenti che una comunicazione pervasiva dei veicoli pone.

Capitolo 2

Internet of Things: breve panoramica

Cosa si intende quando si parla di *Internet of Things* (IoT)? Ad oggi l'impiego dell'elettronica è diventato pervasivo e il perfezionamento delle tecnologie di telecomunicazione sta rendendo sempre più semplice ed economico integrarle in tutte le *cose*. Possiamo parlare di IoT quando abbiamo un vero e proprio network di oggetti fisici; tra questi non ci sono solamente i classici device come smartphone, tablet e pc tramite i quali siamo quotidianamente abituati ad avere accesso alla rete internet, ma tutti (o quasi) gli oggetti e i servizi di cui disponiamo tutti i giorni.

I domini di applicazione di questo attuale paradigma possono essere i più disparati e l'obiettivo di ingegneri e infrastrutture è quello di assicurare una buona integrazione orizzontale tra di loro. La domotica è sicuramente uno di quelli più iconici, ma per esempio anche servizi pubblici come scuole e la sanità potranno godere di grandi miglioramenti grazie ad una connessione così capillare. Anche in ambito produttivo le possibilità sono moltissime, sia nel settore primario con un'agricoltura più avanzata, sia in quello secondario grazie a industrie e fabbriche molto più efficienti, sia nel terziario dove un'organizzazione automatica o semi-automatica di tutti i vari processi gestionali

rende più efficaci i loro servizi.

Come scritto nel capitolo precedente, ciò che contraddistingue un oggetto comune da uno *intelligente* è la capacità di quest'ultimo di collezionare informazioni sul mondo attorno a sé e potersele scambiare, in funzione di precisi scopi, con oggetti della sua stessa classe e/o di classi differenti [7].

2.1 Elementi che costituiscono l'IoT

Per rendersi conto in maniera migliore del reale significato dell'IoT, è opportuno illustrare schematicamente i sei principali macro-elementi che costituiscono il cuore del suo funzionamento. In figura 2.1 vediamo questi sei blocchi che formano l'IoT: identificazione, sensazione, comunicazione, elaborazione, servizi e semantica [11].

Figura 2.1: Struttura logica dell'IoT. Immagine tratta da [11].

Bisogna tenere conto del fatto che gli standard per realizzare tutti i vari blocchi sono eterogenei, quindi, se si vuol fare in modo che l'IoT diventi pervasivo, è necessario che tutte le varie tecnologie utilizzate siano interoperabili tra di loro, o tramite la definizione di standard unici e precisi oppure tramite la realizzazione di opportuni middleware di supporto.

Identification

La parte di identificazione di oggetti e risorse nel cloud è cruciale, perché rende possibile rivolgervisi univocamente selezionando con precisione i servi-

zi desiderati. Ogni *oggetto* deve avere un *Object ID* e un indirizzo ben precisi; da sottolineare la loro distinzione, dato che l'indirizzo li identifica univocamente nella rete globale, mentre l'ID è il nome dell'oggetto all'interno del suo particolare contesto, quindi non è globalmente univoco (per es., mi rivolgo ad un particolare sensore di temperatura come T_1).

Un esempio di struttura per gli indirizzi pubblici di tutti gli oggetti può essere il classico IPv4 o IPv6 (quest'ultimo molto probabilmente necessario visto l'enorme numero di indirizzi IP necessari).

Sensing

Per riuscire ad avere quel livello di *context-awareness* necessario a poter svolgere le proprie funzioni, gli oggetti devono poter "leggere" autonomamente il mondo esterno, in altre parole devono essere dotati di veri e propri sensi. I sensori sono quei dispositivi che rendono possibile questo, assorbono segnali dall'ambiente fisico reale e li traducono in segnali digitali interpretabili ed elaborabili dall'unità di calcolo integrata. Termometri, odometri, accelerometri, ecc. sono tutti esempi di sensori.

Le informazioni così raccolte, che saranno successivamente analizzate ed elaborate (*Computation*), verranno immagazzinate in database interni oppure in rete nel cloud.

Communication

Lo scambio di tali dati tramite l'interazione – sia diretta che indiretta – con gli altri oggetti è chiaramente fondamentale in un'ottica di cooperazione, perché permette di accedere a dati raccolti che sono inaccessibili ai sensori del singolo oggetto, che però sono necessari in fase decisionale (*Semantics*).

Alcune delle tecnologie che possono soddisfare quest'importante requisito sono WI-FI, bluetooth oppure la rete LTE; anche il protocollo NFC è adatto in molti scenari. In generale le tecnologie di *Radio-Frequency IDentifica-*

tion (RFID) sono particolarmente indicate per l'IoT e permettono anche una comunicazione decentralizzata peer-to-peer, particolarmente indicata, come vedremo, per il settore dell'automotive.

Computation

Questa parte è resa possibile grazie all'avanzamento dell'elettronica di consumo, che ha reso possibile un'economica integrazione di microcontrollori e microprocessori all'interno degli oggetti, basti pensare a prodotti altamente modulari e adattabili come Arduino o Raspberry Pi. La capacità computazionale è in grado di conferire un certo livello di autonomia alle *cose* che la possiedono.

L'utilizzo di unità di calcolo integrate rende vitale anche l'utilizzo di sistemi operativi adeguati ai particolari scopi. In ambito IoT sono particolarmente adatti i cosiddetti sistemi operativi real-time (RTOS), altamente indicati per gli utilizzi critici e costanti richiesti in molte situazioni (si pensi all'ambito medico). Verranno quindi sviluppate applicazioni *RTOS-based*. Qualche esempio di RTOS è *Contiki*, *LiteOS*, *TinyOS* o lo stesso *Android*.

Anche le piattaforme cloud costituiscono una parte molto importante nella computazione. Questi supporti permettono agli *smart-object* di condividere i loro dati (raccolti e/o elaborati) in un "terreno comune", facilitandone così la propagazione in tempo reale, utile sia per gli utenti finali che per i big data. Due esempi di piattaforme cloud esistenti pensate per l'ioT sono *Nimbits* e *Hadoop*.

Services

I servizi rappresentano le "funzioni" dell'IoT, ovvero gli effetti di questo paradigma sulle applicazioni offerte. Possono essere schematicamente raggruppati in quattro categorie astratte principali:

- *Identity-related Services*: sono i servizi più basilari ed utilizzati a loro volta da altri servizi; permettono di mappare univocamente gli oggetti fisici ai corrispettivi oggetti logici virtuali, permettendo alle varie applicazioni di interagire con un oggetto fisico senza equivoci. In altre parole, conferiscono un'identità alle *cose*.

- *Information Aggregation Services*: raccolgono, raggruppano e riassumono tutti i dati provenienti dai sensori integrati negli oggetti. Conferendo una struttura a tutti i dati "grezzi" si rendono possibili le successive elaborazioni e sfruttamenti di tali informazioni.

- *Collaborative-Aware Services*: questi tipi di servizi sfruttano i dati ordinati dai servizi del tipo precedente utilizzandoli per elaborare decisioni e reagire in maniera opportuna.

- *Ubiquitous Services*: qui siamo al livello più alto, i servizi di questo tipo coordinano a loro volta quelli del tipo precedente stabilendo in maniera intelligente *come*, *dove* e *quando* utilizzarli.

Le principali applicazioni sono molteplici. Le cosiddette *smart-home* sono un chiaro esempio di ciò di cui parliamo, ma anche nell'ambito infrastrutturale vi è terreno fertile per questa tecnologia, con le *smart-buildings* (si pensi alla gestione e coordinazione di un condominio o di un gruppo di strutture). L'ambito dei trasporti rappresenta un altro esempio di applicazione dell'internet delle cose, col concetto di *Intelligent Transportation System* (ITS) – di cui parleremo nel prossimo capitolo. Oltre alla gestione di strutture e veicoli vi può essere anche una gestione di macchine industriali, dove una cooperazione nelle fabbriche tra macchinari intelligenti potrebbe incidere moltissimo nel settore manifatturiero. Un altro ambito, come già precedentemente menzionato è quello sanitario oppure anche quello energetico (*smart-grids*).

Grazie ad un'adeguata integrazione orizzontale tra tutte queste possibili applicazioni dell'internet delle cose, avremo delle vere e proprie città autono-

me e intelligenti (*smart-city*), dove la qualità della vita potrebbe aumentare significativamente.

Semantics

La semantica è quell'abilità dell'IoT di estrarre una conoscenza utile e mirata dalle informazioni prodotte dai vari device. La si può vedere come il cervello dell'IoT, è quel blocco che prende le decisioni facendo le giuste richieste contattando le risorse opportune, riconosce, analizza e interpreta i dati di cui si è in possesso dando un senso alle decisioni, fornendo così i servizi giusti al momento giusto e nella maniera più efficiente possibile.

A supporto di ciò è necessario l'utilizzo di tecnologie di web semantico come *Resource Description Framework* (RDF), *Web Ontology Language* (OWL) o *Efficient XML Interchange* (EXI).

Capitolo 3

Dall'Internet of Things all'Internet of Vehicles

Come facilmente immaginabile anche da coloro che non sono "addetti ai lavori", l'internet delle cose invade – e in futuro è fisiologico che lo farà sempre di più – anche il mondo della mobilità su strada, coinvolgendo non solamente i dispositivi collegati ai veicoli (come tablet, smartphone, navigatori satellitari, ecc.) ma anche i veicoli stessi e l'intera infrastruttura stradale cui usufruiamo quotidianamente per muoverci. Rendere ordinato, efficiente e sicuro questo "naturale" processo evolutivo non è un obiettivo banale e bisogna innanzitutto analizzare a fondo il problema e porsi le seguenti questioni. Il paradigma dell'Internet of Things, così come lo concepiamo oggi, è già integralmente adatto al mondo della mobilità su strada? Fornisce già tutti gli strumenti concettuali e tecnici necessari allo sviluppo di un'infrastruttura stradale soddisfacente e sicura? Oppure è necessario riarchitettare alcuni concetti e aggiungere supporto alla risoluzione di, fino ad oggi, inedite tipologie di problemi?

3.1 Concetto di Intelligent Transportation System

L'esponenziale sviluppo tecnologico nel campo dell'elettronica di consumo e delle telecomunicazioni ha spalancato la porta a molti ambiti di studio; uno di questi è l'*Intelligent Transportation System* (ITS), ovvero Sistema di Trasporto Intelligente, con cui si intende proprio l'integrazione di moderne tecnologie dell'ingegneria delle telecomunicazioni all'ingegneria dei trasporti [6]. Tale integrazione è una rivoluzione per la mobilità, in quanto dà strumenti inediti per una gestione molto più raffinata di numerosi problemi riguardanti la mobilità stradale.

Già dopo un primissimo lavoro di fantasia, non è difficile immaginare le potenziali conseguenze positive che potrebbero avere sulla gestione del traffico tecniche come simulazione e monitoraggio in tempo reale del flusso globale dei veicoli, comunicazione reattiva e proattiva tra i veicoli stessi (e con l'infrastruttura stradale) e condivisione di informazioni sempre in tempo reale. Gli effetti di una migliore gestione del traffico non si limitano solamente ad una (perlomeno potenziale) diminuzione del tempo di percorrenza medio, ma anche ad un conseguente risparmio energetico, ad una più efficace pianificazione di interventi sul traffico e sulla strada sia a breve termine che a medio/lungo termine, ad una migliore sicurezza di tutti gli utenti della strada, ad una migliorata gestione delle emergenze, ecc.; sono tutti aspetti che vedremo più specificatamente anche in seguito.

Uno scenario del genere non è semplicemente desiderabile, è addirittura necessario considerata l'attuale trend di crescita demografica monotòna e di emergenza ecologica. Oltre ai benefici bisogna sottolineare che l'ITS ripropone anche ai veicoli tutti gli apert(issim)i problemi di sicurezza informatica e di privacy propri della rete.

3.2 Perché l'Internet dei veicoli?

Viviamo in un momento storico in cui gli oggetti cosiddetti *smart* costituiscono una presenza pervasiva nelle nostre vite. Come detto nel capitolo 2, quando si parla di oggetti intelligenti, si parla di dispositivi, elettrodomestici o altro dotati della capacità di comunicare, ma non solo, sono anche dotati di sensori con cui sono in grado di interpretare, secondo un certo linguaggio, l'ambiente esterno, inoltre sono dotati di microprocessori integrati, quindi sono anche in grado di elaborarle queste informazioni per poi condividerle con i loro "simili" e/o con opportuni middleware di supporto [12].

Nell'ambito della mobilità stradale possiamo identificare questi oggetti intelligenti nei veicoli stessi e negli oggetti che costituiscono l'infrastruttura stradale, come un semaforo o, più genericamente, un data-center adibito all'elaborazione e propagazione di informazioni ai veicoli, oppure un server centrale. In questo scenario, l'ambito di studio al quale ci stiamo riferendo non è più semplicemente l'Internet of Things, ma l'*Internet of Vehicles* (IoV). Vedremo nel prossimo capitolo, tramite l'analisi di alcuni primi prototipi di infrastruttura e protocolli di comunicazione attualmente già esistenti e testati, che ci saranno molte situazioni di rilevanza quotidiana che richiederanno necessariamente soluzioni ad hoc.

Ma Perché tutto questo? Tendenzialmente, quando è possibile realizzare una cosa di solito, prima o poi, viene realizzata. Ma quali sono i principali ambiti di ricerca che davvero costituiscono specificatamente la ragion d'esistere di questo nuovo concetto di mobilità? Vediamone alcuni di seguito.

3.2.1 Gestione del flusso veicolare

Fino ad ora una gestione davvero efficiente del traffico non è mai stata realmente possibile, in primis perché una rilevazione in real-time del flusso veicolare senza le attuali tecnologie di telecomunicazione è estremamente difficoltosa; alcune soluzioni praticate sono state (e talvolta sono tuttora) sensori

sulla pavimentazione stradale oppure videocamere posizionate in punti strategici, ma si tratta di metodi dalla limitata efficacia, oltre che molto onerosi. Fondamentale anche la capacità di coordinazione ad ampio raggio tra i vari attori che, nell'attuale realtà quotidiana, è molto rudimentale; i principali metodi sono cartelli luminosi, notiziari, guide o, alla meglio, navigatori satellitari dalle informazioni perlopiù statiche; con soluzioni di questo tipo vi è l'inconveniente che vengono inoltrate le stesse indicazioni a tutti i veicoli, non facendo altro che spostare un ingorgo da una parte all'altra, invece di distribuirlo [13].

L'obiettivo è arrivare ad una situazione in cui tutti i veicoli riescano ad ottenere una visione ad ampio raggio – seppur sempre limitata alla propria macro-zona geografica di interesse – della situazione stradale e che ognuno di loro possa venir informato in tempo reale di ogni nuovo evento d'interesse, in modo che possa indipendentemente decidere la maniera migliore per muoversi. Un esempio di ciò potrebbe essere la scelta del percorso in quel momento più conveniente per arrivare da un punto A a un punto B; i percorsi potrebbero essere molteplici e il miglior modo di scegliere è farlo dinamicamente, non staticamente, analizzando man mano la quantità di traffico presente su un percorso piuttosto che su un altro, ma per farlo è necessario raccogliere, elaborare e condividere informazioni sul flusso in tempo reale.

3.2.2 Monitoraggio dell'ordine stradale

Ad oggi il controllo proattivo della strada è molto limitato e sempre a carico di pochi attori predisposti, la chiave è dunque che tutti i veicoli mettano a disposizione i loro sensi per ottenere risultati sia quantitativamente che qualitativamente migliori. A tale scopo viene molto utile lo sfruttamento coordinato dei molteplici sensori di cui sono (e saranno sempre più) dotati i veicoli e le infrastrutture [13].

Un esempio di possibile scenario potrebbe essere quello della prevenzione di un atto criminale o un attentato terroristico; in caso di conoscenza del

fatto che determinati veicoli o individui siano in procinto di attaccare un determinato luogo, ai veicoli casualmente circolanti attorno a quella zona potrebbe venir assegnato il compito di videoregistrare sequenze, raccogliere metadati e di condividere il tutto in un predeterminato spazio cloud. Le videoregistrazioni sarebbero molto utili, talvolta fondamentali, anche nelle indagini di ricostruzione di incidenti, ma in questo caso sarebbe necessario che tutti i veicoli registrino e raccolgano informazioni costantemente.

Eventuali raccolte dati così massive, però, sollevano notevoli questioni sulla privacy. E' importante che tali dati vengano sfruttati solamente in casi di stretta necessità (certezza di attacchi in corso o indagini DOPO gli incidenti, come detto prima). Fino ad allora, per esempio, i dati potrebbero venir mantenuti solo per un certo periodo di tempo (quindi quelli vecchi verrebbero eliminati, se inutilizzati) e rimanere opportunamente crittografati offline sulla memoria di massa dei singoli veicoli con opportune (e possibilmente effimere) chiavi private di cifratura generate in locale, quindi conoscibili solamente dal veicolo stesso, in questo modo rimarrebbero opportunamente decentralizzati fino a che un'autorità certificata – magari decentralizzata a sua volta, distribuire un tale potere è importante per prevenire abusi – non comunichi al veicolo di decifrare e di consegnare quelli inerenti un determinato luogo ad una determinata ora.

Vi potrebbero comunque essere anche tipologie di informazioni non sensibili ma utili al monitoraggio stradale, in questo caso sarebbe utile che tali informazioni venissero efficientemente condivise in tempo reale. Vedremo più specificatamente nel capitolo 6 come potrebbero venir tecnicamente gestiti scenari di questo tipo.

3.2.3 Gestione delle emergenze

Un concetto come l'IoV renderebbe molto più semplice anche la gestione e la coordinazione di situazioni di emergenza. Un esempio potrebbe essere l'improvvisa inagibilità di una porzione di strada oppure la necessità di lasciarne

di libera a forze dell'ordine, ambulanze, vigili del fuoco, ecc.

Nello scenario che ci prefiggiamo di raggiungere, grazie all'ordinata applicazione delle nuove tecnologie, un cambiamento imprevisto della situazione diventa molto meno rischioso e molto più coordinabile rispetto ad ora per gli utenti della strada.

3.2.4 Assistenza alla guida

Le automobili di nuova generazione sono quasi tutte dotate di numerosi dispositivi di supporto alla guida, rendendole in un certo senso auto a guida semi-automatica; non si tratta quindi di un ambito di ricerca propriamente nuovo ma, con l'aumentare di sensori integrati e il rapido affinarsi di nuovi e adatti protocolli dei comunicazione ad hoc, nel breve termine diventerà un problema sempre più complesso e rilevante.

Influire sul veicolo per perfezionare lo stile di guida dell'uomo può avere effetti positivi sia sulla sicurezza (prevenire colpi di sonno, scoraggiare una guida indisciplinata, rimediare a distrazioni, ecc.) che sull'inquinamento (un uso ottimale del gas, del freno e soprattutto del cambio hanno un impatto non trascurabile sul consumo di carburante, sull'usura del veicolo e sulla sua longevità).

3.3 Comunicazione tra veicoli e concetto di Vehicular Cloud

Fino ad ora abbiamo sottolineato l'importanza di una buona coordinazione tra i vari attori per svariate finalità. I veicoli sono entità in grado di collezionare grandi quantità di dati con grande accuratezza, se consideriamo quindi tutti quelli in circolazione ci ritroviamo a che fare con un bacino sconfinato di informazioni da gestire. Ma come rendere possibile un'efficiente comuni-

cazione? Quali protocolli e tecnologie potrebbero venir sfruttati/architettati per raggiungere l'obiettivo?

Una possibile prima soluzione potrebbe essere che ogni singolo attore venga dotato di un indirizzo IP e che si interfacci pubblicamente a internet [12]; rete e spazi cloud centrali opportunamente preposti sia all'elaborazione che alla diffusione di dati (concetto di *Internet Cloud*) potrebbero rappresentare un possibile middleware per lo scambio di informazioni; ma quanto sarebbe ottimale una soluzione di questo tipo?

La verità è che la maggior parte delle informazioni e dei metadati collezionati dalle automobili hanno una rilevanza esclusivamente locale; ad esempio un'automobile che sta circolando a Milano non avrà interesse (e non sarebbe auspicabile che lo avesse) né trarrà beneficio dalla possibilità di accedere ad informazioni riguardanti il traffico di Roma. Anzi, molti dati hanno una rilevanza addirittura su una scala dell'ordine dei metri (incidente più avanti, ingorgo, mezzo di soccorso nei paraggi, auto in panne, segnale stradale, ecc.). Oltre alla rilevanza geografica bisogna considerare anche la rilevanza temporale. Eventi riguardanti il traffico, lo stato della strada, ecc. per loro natura vengono continuamente rinnovati e diventano obsoleti in tempi nell'ordine delle ore e talvolta addirittura dei minuti o dei secondi.

In uno scenario del genere, cose come frequenza di ricerca delle informazioni da parte dei milioni di client, tempo di upload/download, latenza, costi e altissima richiesta di risorse computazionali ai server per l'elaborazione di dati in tempo reale possono diventare gravosi per l'Internet Cloud, rendendolo una soluzione probabilmente poco efficiente, poco scalabile o, in determinate zone, addirittura non attuabile.

Data la circoscritta rilevanza delle informazioni potrebbe essere una scelta intelligente mantenerle, elaborarle e diffonderle direttamente all'interno della zona in cui vengono raccolte e richieste, sfruttando così direttamente le risorse computazionali dei veicoli, evitando di viaggiare costantemente su internet in server centrali; in questo modo, una volta progettato un buon

metodo di ricerca e di archiviazione dei dati, non avremo gli inconvenienti di cui parlato sopra. Si parla quindi di *Vehicular Cloud* [13] che, una volta affiancato all'Internet Cloud e scelto dinamicamente il metodo più conveniente per performare le singole richieste, può essere in grado di sostenere l'ingente reticolo di scambio di informazioni, aumentando in maniera decisiva la scalabilità dell'intera infrastruttura.

Per sostenere un modello di coordinazione e di gestione così decentralizzato, è necessario un paradigma di comunicazione che lo sia altrettanto; il modello peer-to-peer (P2P) è una possibile soluzione. Con opportuni adattamenti potrebbe essere di grande importanza riuscire a progettare un protocollo di comunicazione specifico per i veicoli, quindi un modello *vehicle-to-vehicle* (V2V) in modo che due mezzi possano scambiare dati tra loro senza la necessità di intermediari fisici. Con lo stesso criterio si potrebbe rendere possibile l'interazione indipendente anche tra il veicolo e l'infrastruttura stradale (ad esempio un'unità di calcolo stradale, un segnale, ecc.), si parla dunque anche di comunicazione *vehicle-to-infrastructure* (V2I). Parleremo meglio dei metodi di comunicazione e di gestione delle informazioni scambiate nel capitolo successivo.

Capitolo 4

Comunicazione inter-veicolare e soluzioni sperimentate

Abbiamo parlato della necessità di una forma di cooperazione tra i veicoli circolanti su strada. Nel corso del capitolo illustreremo un modo per indicizzare e ricercare i dati scambiati che, invece che basarsi sul loro indirizzo fisico si basa sul contenuto dei dati stessi. Inoltre vedremo alcuni esempi concreti, seppur sperimentali, di sistemi di supporto al paradigma dell'*Internet of Vehicles*.

4.1 Concetto di Content-Centric Network

Sebbene ad oggi molti veicoli comunichino (anche) attraverso server centralizzati, la comunicazione diretta peer-to-peer rappresenta un'alternativa per contesti mobili e real-time come quello della mobilità stradale. Come brevemente accennato alla fine dello scorso capitolo, nell'ambito stradale si parla di comunicazione *vehicle-to-vehicle* (V2V) e *vehicle-to-infrastructure* (V2I), ovvero uno scambio diretto di dati tra veicoli e data-center o stazioni fisse poste lungo le strade a supporto della comunicazione (*Road Side Units*, RSU), come si vede in figura 4.1.

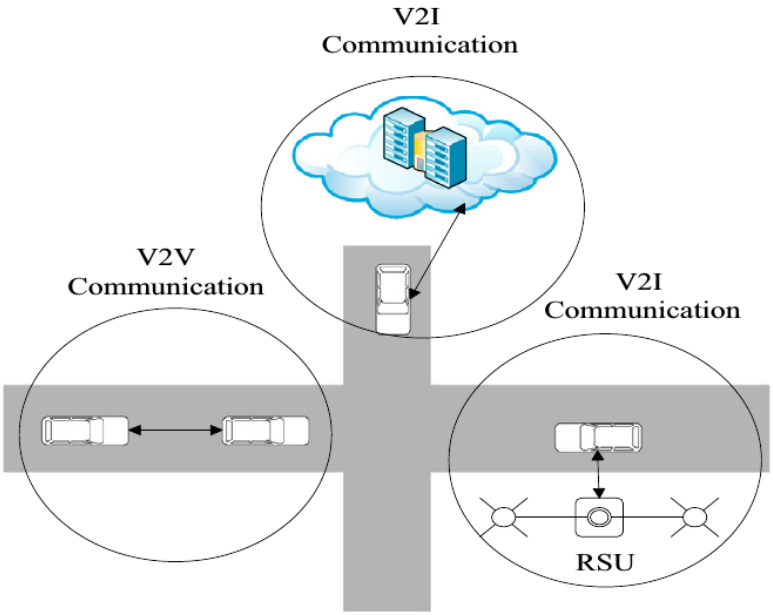

Figura 4.1: Comunicazione peer-to-peer tra veicoli e infrastrutture. Immagine tratta da [19]

Pensando ad un modello di telecomunicazione così decentralizzato ci si accorge che sfruttare l'attuale modello infrastrutturale basato sugli indirizzi IP – quindi sulla posizione fisica del dato – probabilmente non è la soluzione ottimale e nemmeno la più scalabile. Il numero degli indirizzi IP necessari sarebbe enorme e la complessità del routing dei dati aumenterebbe notevolmente, minando così anche la stabilità dell'infrastruttura. Bisogna anche considerare che parliamo di veicoli, quindi di entità mobili, la richiesta di informazioni basate su un indirizzo fisico sarebbe estremamente sconveniente.

Si propone l'introduzione di un nuovo approccio per il routing dei dati, basato non più sulla loro posizione (indirizzo IP) ma sul loro nome e/o contenuto, questo nuovo approccio è chiamato *Named-Data Networking* (NDN) oppure anche *Content-Centrinc Networking* (CCN) e sembra particolarmente adatto per il mondo dell'Internet of Vehicles [18]. La comunicazione, in

un contesto NDN, è interamente gestita dal richiedente, che invia tramite broadcast un *Interest*, ovvero un pacchetto contenente il nome preciso che identifichi il dato (o i dati) cercato. Un tale approccio è molto più adatto al contesto, visto che il consumatore non ha bisogno di sapere né dove questo dato si trovi né l'identità di chi glielo fa avere; si tratta di un intelligente disaccoppiamento tra contenuto e locazione. Per funzionare, però, è necessario un efficiente, ben studiato e soprattutto standard protocollo di naming dei dati, in modo che siano sempre univocamente identificabili (qualora esistano, ovviamente).

Come mostrato in figura 4.2, i veicoli possono assumere sostanzialmente tre tipi di ruoli: publisher, muli e consumatori; ogni veicolo può svolgerne anche più di uno contemporaneamente [18]. Il publisher (1) è rappresentato da ogni entità che elabora e produce un'informazione a partire dai propri sensori (o da dati arrivati da altri), questo dato rimane poi cachato in un database interno e mantenuto disponibile per essere distribuito in caso di ricezione di opportuni *Interest*. Molti veicoli e soprattutto molte unità stradali fisse poste a loro supporto (RSU), oltre ad essere publisher possono essere anche muli (2), ovvero entità che, secondo le proprie capacità, raccolgono e cachano indistintamente dati provenienti dagli altri altri veicoli oltre ai propri. Anche se tali dati non sono utili a loro, i muli contribuiscono comunque ad estendere la reperibilità e la longevità delle informazioni prodotte, si tratta dunque di un ruolo di importanza critica. Il consumatore (3) è colui che ha bisogno di un dato che non possiede, eseguendo quindi un broadcast con pacchetti di interesse contenenti il nome del dato desiderato, rimane in attesa di un'eventuale risposta. Ogni dato ricevuto sarà poi visualizzato ai passeggeri, se necessario (4).

Prima abbiamo accennato della necessità di un protocollo di naming condiviso, ma quali sono le caratteristiche generali che dovrebbe avere? Innanzitutto, pur non essendo basato sulla locazione fisica come per gli indirizzi IP, dovrebbe comunque avere un range geografico, quindi dal nome si dovrebbe riuscire ad identificare perlomeno la macrozona all'interno della quale

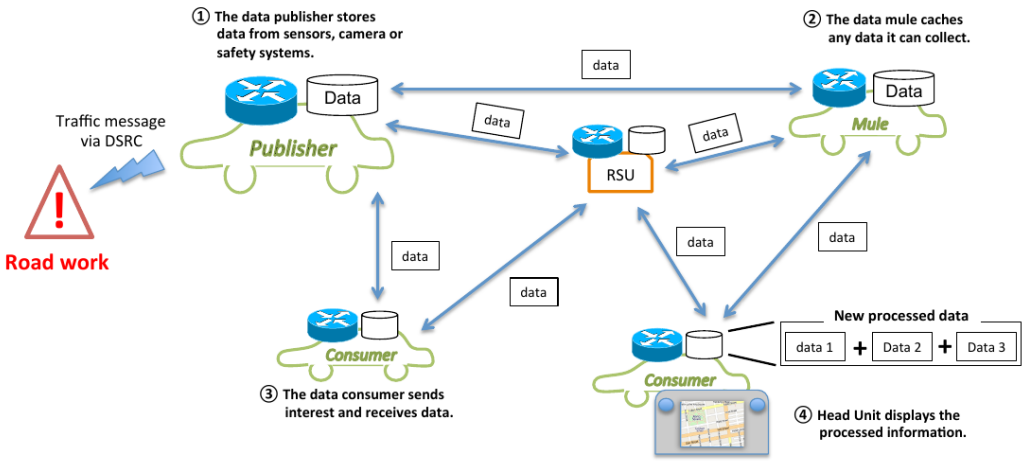

Figura 4.2: Ruoli e interazioni tra i vari attori in un NDN. Immagine tratta da [18].

si vuole trovare il dato. Considerando che moltissime informazioni riguardanti gli eventi del traffico sono destinate a diventare obsolete nel giro di ore/minuti/secondi, anche un range temporale dovrebbe essere chiaramente espresso, ad esempio tramite l'utilizzo di timestamp. Per evitare la ricezione di repliche dello stesso dato – visto che potrebbe essere in possesso di più veicoli – si potrebbero utilizzare degli opportuni filtri di esclusione o tabelle aggiornate dinamicamente. Bisogna considerare che tutti i possibili dati interscambiabili sono molto diversi tra di loro e potrebbero servire per molti tipi di applicazioni differenti; potrebbe essere una scelta intelligente prevedere strutture di naming specifiche per applicazioni specifiche. Un'altra questione riguarda la sicurezza, ovvero il difendersi da publisher malevoli; sarebbe opportuno poter verificare l'autenticità delle informazioni proteggendo al contempo l'identità e la privacy del veicolo [18].

Vediamo quale potrebbe essere un esempio di stringa che identifichi univocamente un'informazione. Supponiamo che al nostro veicolo interessi venire a conoscenza del livello di scorrimento del traffico (calcolabile in base alla velo-

città media tenuta dai veicoli) lungo l'autostrada 101, lato nord, tra la 400a e la 410a sezione tra le 12:00 e le 13:00 del 6 dicembre 2011, il relativo pacchetto di *Interest* diffuso tramite broadcast dovrebbe contenere una stringa di questo tipo: `/traffic/Highway101/north/[400,410]/[1323201600,1323205200]/speed/19375887`

Fino a questo momento abbiamo parlato di modalità di richiesta e di scambio delle informazioni, ma in realtà i dati possono essere di varia natura, non sarebbe praticabile se tutti venissero trattati alla stessa maniera. I dati potrebbero venir suddivisi in tre macro-gruppi: dati pubblici, dati pubblici non condivisibili e dati privati.

L'architettura sopra descritta si adatta molto bene al primo tipo, di cui l'esempio della velocità lungo l'autostrada 101 rappresenta un buon esempio. Un esempio per il secondo tipo, invece, potrebbe essere un video di grandi dimensioni prodotto da un veicolo; considerato il contesto altamente mobile sarebbe notevolmente difficoltoso ed alto rischio failure l'affidarsi integralmente ad uno scambio V2V/V2I per questi file, lo scambio richiederebbe tempo e molte risorse, in questo caso una soluzione ibrida con server centralizzati, nonostante le latenze, produrrebbe probabilmente risultati migliori. Il terzo tipo di informazione (i dati privati) richiederebbe invece modalità di scambio differenti; in questo caso non si tratterebbe di richiedere genericamente informazioni che chiunque potrebbe avere, ma dati specifici ad attori specifici. Nel caso di chat tra due utenti è per esempio necessario che i veicoli comunicanti siano reciprocamente a conoscenza dell'identità di colui con cui stanno comunicando, cosa non strettamente necessaria per i dati pubblici [21].

4.2 MobEyes

MobEyes è uno dei primi sofisticati supporti al monitoraggio urbano proattivo. Il progetto si basa sull'idea principale di sfruttare il moto dei veicoli per diffondere opportunisticamente piccoli riepiloghi (*summary*) di dati e meta-

dati raccolti in un determinato lasso di tempo (nell'ordine dei secondi) in una determinata area. L'obiettivo è dunque di rendere facile, efficiente e veloce la cooperazione e la comunicazione nel traffico servendosi del traffico stesso [17].

Una delle più interessanti caratteristiche che rendono questo supporto particolarmente solido è la sua natura completamente distribuita; raccolta, elaborazione, richiesta e diffusione di dati avvengono integralmente sulle singole vetture, vi è completa indipendenza da strutture centrali, rendendo così molto difficile e costoso per un potenziale attaccante interrompere il monitoraggio. Un tipico caso d'uso è la ricostruzione di un crimine tramite la raccolta di tutti i dati generati dai veicoli in un preciso momento e luogo. Ciò richiede quindi che entità autorizzate all'accesso dei dati massivamente generati (come agenti di polizia) facciano posteriormente richiesta delle informazioni cui sono interessati.

Ma qual è l'architettura di *MobEyes*? Possiamo vederla in figura 4.3. Ogni veicolo raccoglie dati "grezzi" tramite i propri sensori, li elabora e li spedisce autonomamente. Il componente che si occupa di elaborare questi dati grezzi raccolti dall'esterno si chiama *MobEyes Data Processor* (MDP), un'unità di calcolo preposta appositamente per questo scopo. Il MDP ha accesso ai dati – mantenuti nell'apposito database *Raw Data Storage* – comunicando opportunamente con i sensori dell'automobile tramite un'interfaccia standard chiamata *MobEyes Sensor Interface* (MSI). Una volta prodotti i riepiloghi – risiedenti in un altro database ad hoc, il *Summary Database* – interviene il componente chiave dell'intera infrastruttura, che si occupa del fondamentale compito di diffondere opportunisticamente e/o di fare richiesta dei riepiloghi prodotti dal MDP, il *MobEyes Diffusion/Harvesting Processor* (MDHP).

Il caso d'uso prima menzionato mette in evidenza i due principali protocolli di comunicazione delle informazioni previsti dal MDHP, ovvero quello di diffusione dei riepiloghi (*summary diffusion*) e quello di raccolta dei riepiloghi (*summary harvesting*). Nel primo caso i veicoli raccolgono tramite

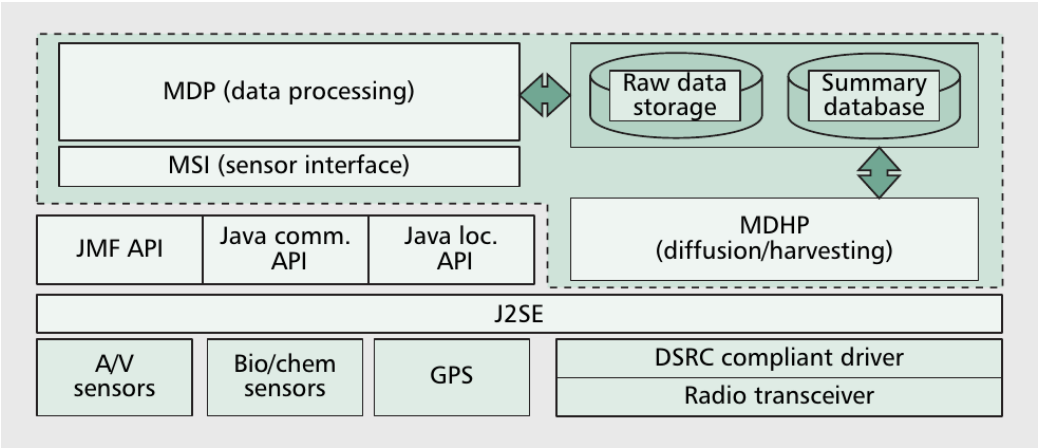

Figura 4.3: Schema ad alto livello dell'architettura di *MobEyes*. Immagine tratta da [17].

i loro sensori, elaborano grazie alle loro capacità computazionali e producono in maniera del tutto indipendente pacchetti di dati che riassumono l'environment locale in cui si trovano/si sono trovati. Questi pacchetti – che possono eventualmente raggruppare più riepiloghi assieme, in modo da coprire un lasso di tempo più lungo – vengono continuativamente diffusi ai veicoli attorno (*periodic advertisement*), dai quali poi sono raccolti, immagazzinati nell'opportuno database interno (*Summary Database*) e utilizzati a loro volta dagli stessi come ulteriore fonte di informazione per produrre i loro. Nel momento in cui ci sarà la necessità di sfruttare queste informazioni, inizierà il processo di raccolta delle stesse (fase di *harvesting*), ma solo da parte di entità autorizzate, come le forze dell'ordine. Queste ultime saranno interessate verosimilmente solo ai riepiloghi che sono stati prodotti più recentemente (nell'ipotesi che un'indagine sia ragionevolmente tempestiva), quindi andranno fisicamente nelle zone di interesse ed eseguiranno dei broadcast con le query di richiesta dei pacchetti cercati (*event-driven advertisement*).

Un aspetto da considerare durante il processo di raccolta è che più veicoli incontrati avranno lo stesso pacchetto, quindi il "veicolo agente" potrebbe

ritrovarsi a ricevere molte repliche dei vari riepiloghi. Una soluzione sarebbe di tenere dinamicamente conto dei pacchetti ricevuti e di quelli mancanti e aggiornare opportunamente il broadcast con la nuova query di richiesta man mano che vengono raccolti; una volta ottenuti tutti i pacchetti cercati il processo termina. Si tenga conto che la presenza contemporanea di più agenti che cooperano potrebbe facilitare, velocizzare ed estendere il perimetro dell'indagine. Vi sono necessarie anche misure di sicurezza per proteggersi da eventuali avversari che potrebbero tentare malevoli invii di falsi riepiloghi; ad esempio si potrebbe utilizzare un sistema a chiave pubblica e privata in modo che i pacchetti viaggino cifrati e opportunamente autenticati tramite firma; lo stesso può valere per i broadcast di richiesta da parte degli agenti, ma sulla sicurezza delle comunicazioni con veicoli e infrastrutture parleremo più specificatamente nel capitolo 6.

L'efficacia e la fattibilità del supporto offerto da *MobEyes* è stato testato simulando opportunamente un contesto stradale comprensivo di un'area urbana di Westwood (Los Angeles, USA) di superficie 2.400 per 2.400 metri. I risultati mostrano, come facilmente pronosticabile, che le prestazioni, la scalabilità e la stabilità dell'infrastruttura dipendono da parametri fisici come ad esempio il numero di automobili in circolazione, dall'ampiezza del raggio di comunicazione dei singoli veicoli e dalla gittata delle comunicazioni – ad esempio, se un veicolo/agente B facesse da ripetitore ad un veicolo/agente A, riportando i suoi riepiloghi/richieste ad altri veicoli/agenti, la gittata della comunicazione aumenterebbe di un livello; se a loro volta questi altri veicoli/agenti propagassero lo stesso broadcast ad altri ancora aumenterebbe di un altro livello e così via.

Un aumento di questi parametri porterebbe ad una diminuzione della latenza di comunicazione e ad un aumento di scalabilità, a fronte però di un maggiore costo, complessità, overhead e di una potenziale diminuzione di stabilità. In generale, nel contesto considerato, si è evinto che è possibile raggiungere buoni risultati e una sufficiente scalabilità con livelli di complessità e di costi relativamente bassi; ad esempio, come si illustra in figura 4.4,

con 3 agenti in presenza di 300 veicoli con un raggio radio di comunicazione compreso tra i 100 e i 300 metri si sono ottenuti risultati nel complesso promettenti [17].

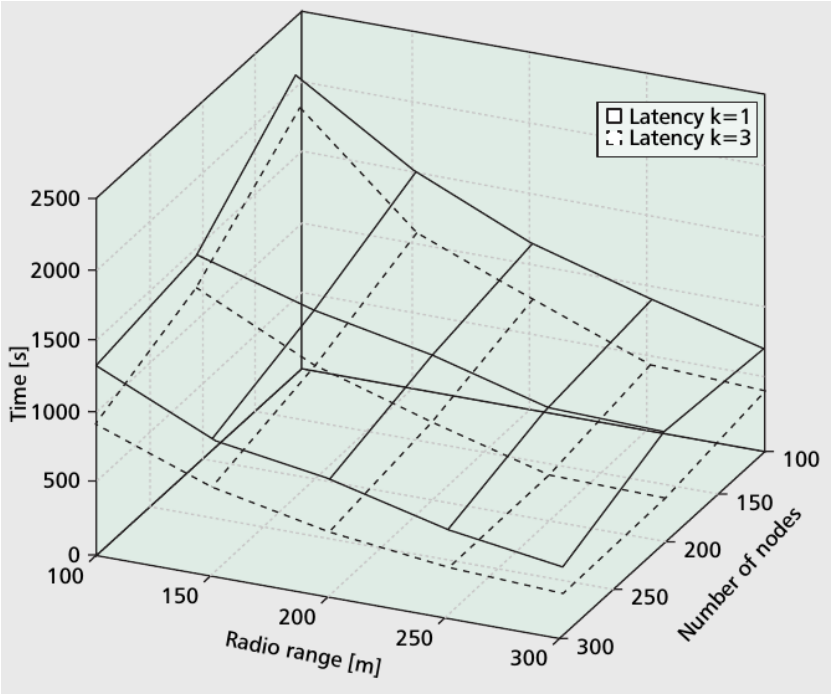

Figura 4.4: Tempi medi di collezione di tutti i pacchetti da parte di *MobEyes*. Immagine tratta da [17].

MobEyes si è dimostrato un sistema potenzialmente molto potente in contesti urbani, ma potrebbe esserlo considerevolmente meno al di fuori delle città. Il motivo principale è che l'intera infrastruttura si basa su uno scambio di informazioni del tutto decentralizzato, non ci sono quindi entità centrali a cui affidare le informazioni raccolte in caso di insufficiente possibilità di interazione, dato che i dati vengono consegnati solo tramite un incontro fisico (entro il reciproco raggio radio) con gli agenti o gli altri veicoli. L'indagine e il monitoraggio di zone periferiche poco trafficate potrebbe quindi essere un problema per svariate ragioni; innanzitutto, visto lo scarso

afflusso di veicoli in tali zone, vi sarebbero numerosi intervalli di tempo non coperti, rendendo così eventuali indagini incomplete, inoltre, anche ammesso che tutti i riepiloghi interessati esistano, sarebbero molto rari dato che sarebbero posseduti solamente da un numero esiguo di vetture, diminuirebbero quindi considerevolmente le probabilità per gli agenti di raccoglierli tutti.

4.3 CarTorrent

Come *MobEyes*, *CarTorrent* rappresenta un altro sistema di supporto alla mobilità che si basa su un approccio peer-to-peer. Anche questo progetto nasce con l'assunto che il classico modello di scambio client-server non sia ottimale per lo scopo e che un network realizzato ad-hoc per i veicoli (*vehicular ad hoc network*, VANET) si debba basare su un modello decentralizzato.

CarTorrent propone un metodo di scambio dei dati sul modello BitTorrent, ovvero le informazioni vengono suddivise in pacchetti e disseminate tramite broadcast; ogni veicolo deve anche poter essere in grado di ottenere la topologia dei nodi locali e poter essere informato della disponibilità dei pacchetti interessati. Per esempio, sarebbe auspicabile che se un veicolo avesse bisogno di un pacchetto che è posseduto da due nodi differenti, questo lo ottenga preferibilmente da quello più in prossimità [16].

Vediamo com'è l'architettura software del sistema *CarTorrent*, in figura 4.5 lo schema. Supponiamo che un *Client* A voglia condividere un file; questo verrà opportunamente suddiviso in pacchetti dal componente *FileSplitter* e nel frattempo il thread *SendGossipThread* propagherà periodicamente dei gossip per informare gli altri client della disponibilità, della struttura e della topologia del file. Un altro Client B, una volta ricevuto il gossip tramite il thread periodico *RecvGossipThread*, lo manterrà e lo gestirà tramite il componente *CarTorrent File Manager*. Una volta preso atto che alcuni dei pacchetti posseduti da A possono interessargli, B – tramite opportuni algoritmi – invierà una precisa richiesta grazie al thread *SendPacketThread*,

che il destinatario ascolterà grazie a *RecvPacketThread* e che, tramite *AODV* (che si interfaccia all'hardware di comunicazione), soddisferà. Sempre tramite *RecvPacketThread*, B riceverà i pacchetti richiesti. Il *File Manager* è quel componente che ha il compito di mantenere aggiornato lo stato e la topologia di ogni pacchetto posseduto, conseguentemente stabilisce quali e di quanti ha ancora bisogno. Il thread *ListenThread* si occupa invece di gestire tutte le richieste di connessione che il client riceve man mano e di smistarle ai vari *RecvPacketThread* [16].

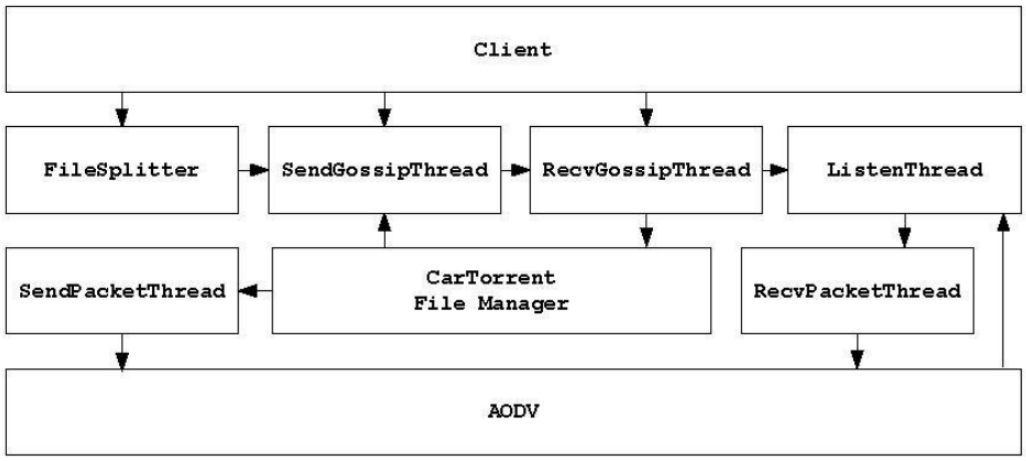

Figura 4.5: Modello di interazione tra le varie parti del sistema. Immagine tratta da [16].

CarTorrent è stato sottoposto a due tipi di esperimenti. Nel primo lo scenario è un semplice parcheggio in cui due computer portatili statici cercano di comunicare. Nel secondo esperimento si è testata la comunicazione tra due automobili – con all'interno gli stessi portatili – in movimento in direzione opposta su un tratto di strada lungo 1 km. Nei risultati si prenderanno in considerazione valori come il goodput per ogni pacchetto, la sua distribuzione e le dimensioni dei singoli pacchetti. Nel parcheggio, in cui non erano presenti interferenze esterne, è stato provato lo scambio di un file di 25 MB via TCP

suddiviso in pacchetti di uguali dimensioni, dapprima di 64 kB per pacchetto, poi di 128. Su strada, invece, a metà del chilometro da percorrere dalle due automobili è posto un access point di supporto alla comunicazione, che funge da ulteriore entità cui si può fare richiesta o inviare informazioni; anche qui si è testato il trasferimento del medesimo file suddiviso nelle medesime modalità di prima.

Nel primo esperimento si può notare dalla figura 4.6 che il goodput aumenta col crescere della dimensione dei singoli pacchetti, questo è dovuto principalmente dal fatto che abbiamo una connessione di tipo TCP/IP; il miglioramento, tuttavia, è via via sempre minore, questo perché pacchetti più grandi sono maggiormente suscettibili a failure e quindi a ritrasmissione, oltre che maggiormente frammentabili (perché più grandi). I goodput medi sono stati di 5,279 Mbps e 5,677 Mbps rispettivamente per i pacchetti da 64 kB e da 128 kB.

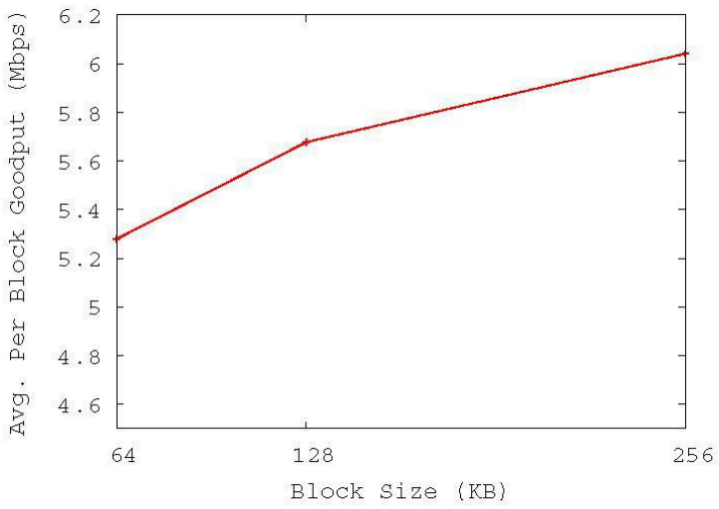

Figura 4.6: Trend di crescita del goodput medio all'aumentare della dimensione dei pacchetti. Immagine tratta da [16].

Nel secondo più rilevante esperimento le difficoltà sono state prevedibil-

mente maggiori. Innanzitutto le interferenze esterne hanno peggiorato la qualità del segnale, inoltre ci sono stati dei momenti in cui, nonostante il buon segnale, i download non avvenivano perché nessuno era ancora in possesso dei pacchetti richiesti; c'è stato anche un momento in cui il download era bloccato perché i *RecvPacketThread* erano tutti occupati. Nonostante questo, i goodput medi con i pacchetti da 64 kB e da 128 kB sono stati rispettivamente 3,777 Mbps e 3,920 Mbps, mediamente 1,5 Mb in meno rispetto al test statico. Un altro aspetto emerso è che il protocollo di file-sharing BitTorrent non è sufficientemente scalabile per un VANET, questo per il fatto che non è pensato per un contesto mobile, ma per una topologia statica (o comunque quasi statica) come lo è il traffico internet. Un metodo più efficiente di raccolta e diffusione dei pacchetti in un contesto dinamico è probabilmente l'adozione della strategia *Rarest-Closest First*, dove viene data la precedenza ai pacchetti più rari e al contempo geograficamente più vicini [16].

4.4 CarSpeak

CarSpeak, di cui parleremo più brevemente, è uno dei primi supporti alla comunicazione inter-veicolare pensato principalmente per la guida senza conducente. L'obiettivo di *CarSpeak* è di permettere una completa condivisione delle capacità sensoriali dei veicoli; l'idea è che il singolo mezzo debba avere la possibilità di usufruire dei dati raccolti dai sensori dei veicoli vicini esattamente come se fossero i suoi.

Per lo scambio delle informazioni viene adottato uno scalabile design *Content-Centric*. Gli oggetti delle informazioni con cui opera il sistema sono rappresentati da regioni di spazio. *CarSpeak* suddivide ricorsivamente lo spazio in tanti cubi, ognuno dei quali si riferisce ad una sua precisa porzione. La struttura dati utilizzata è un Octree (figura 4.7), in cui ogni nodo rappresenta un cubo e ogni sotto-nodo rappresenta un maggior livello di dettaglio (un "sotto-cubo") del nodo padre. In questo modo è possibile riferirsi

univocamente a tutte le possibili porzioni di spazio con il livello di "zoom" desiderato [15].

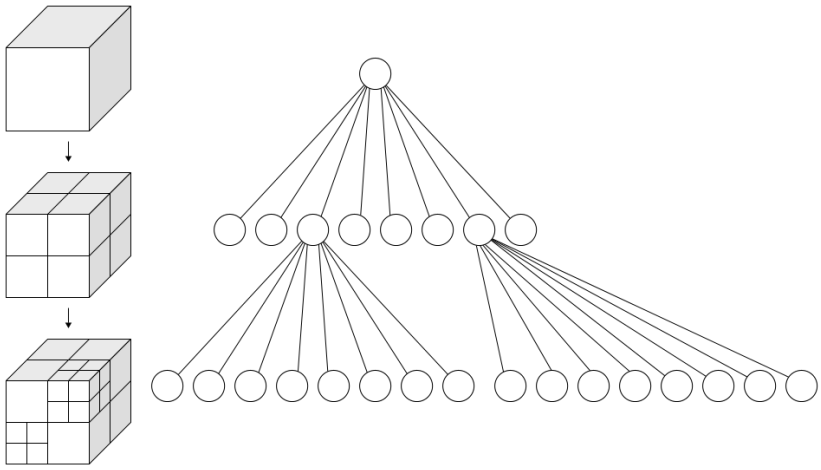

Figura 4.7: Trasposizione grafica di un Octree. Immagine tratta da Wikimedia Commons.

Per rendere possibile ciò, *CarSpeak* utilizza un protocollo di naming che supporti la rappresentazione delle informazioni a più risoluzioni, chiamato *Octree naming system*. Ogni cubo può trovarsi in tre stati possibili: occupato (se sono presenti dati utili al suo interno), libero (se non ci sono) e sconosciuto (se non è possibile stabilirlo con certezza); un cubo si considera occupato se almeno uno dei suoi figli è occupato, ogni spazio viene dunque rappresentato con $8^L - 1$ cubi, con L che rappresenta il numero dei "piani" utilizzati dall'octree (ad esempio, nella figura 4.7 avevamo tre cubi con L rispettivamente uguale a 1, a 2 e a 3).

Un fatto da tenere in considerazione con questo design è la ridondanza; tendenzialmente i cubi segnati come liberi tendono ad essere molto più numerosi e collocati in gruppo, specialmente nelle zone di scarso interesse. Nel momento della trasmissione delle informazioni può essere utile l'utilizzo di algoritmi di compressione che riducano questa ridondanza evitando di

trasmettere necessariamente tutti i valori di tutti i cubi di una certa zona; per esempio trasmettendo solamente una porzione strategica di zeri (ovvero di cubi vuoti), da cui sia possibile indurre che anche quelli attorno lo siano, renderebbe comunque chiaro al destinatario l'ambiente e al contempo alleggerirebbe il carico di lavoro. Ovviamente facendo ciò ci si espone maggiormente al rischio d'errore, ma è possibile arrivare a buoni compromessi.

Il protocollo *CarSpeak* è stato sperimentato in due fasi; dapprima in un percorso di laboratorio controllato, infine in un ambiente aperto con pericoli reali e meno prevedibili (come ad esempio l'attraversamento improvviso della carreggiata da parte di un pedone). In entrambi i casi ha ottenuto risultati migliori rispetto al classico protocollo 802.11. I tempi di reazione dei veicoli agli ostacoli, anche improvvisi, si è dimostrato mediamente inferiore, questo grazie al fatto che ogni veicolo poteva usufruire anche dei sensori dei vicini diminuendo (o del tutto annullando) così i propri angoli ciechi; inoltre l'efficiente compressione dei dati e la buona resistenza agli errori ha garantito prestazioni elevate.

Per un maggior livello di dettaglio sia sull'architettura che sui risultati degli esperimenti, rimando a [15].

Capitolo 5

L'Internet of Vehicles in uno scenario di automobili a guida autonoma e futuro della mobilità

I recenti sviluppi nel campo delle telecomunicazioni e dei sistemi embedded hanno cambiato il tradizionale punto di vista con cui concepivamo la mobilità, ovvero il pensare un veicolo come un'estensione del corpo dell'uomo, come un sistema asservito ai suoi sensi e comandi. Oggi il mezzo di trasporto (così come l'infrastruttura stradale) è una ricca fonte di informazioni che lui stesso ha assorbito dall'esterno tramite i molteplici sensori di cui è munito, ciò lo ha reso abile ad assistere ed estendere spazialmente i sensi del guidatore per una navigazione più sicura, un miglior controllo dell'inquinamento e una miglior valutazione del traffico.

Il prossimo imminente passo evolutivo del mezzo di trasporto consiste nel prendere direttamente il controllo della navigazione, non limitandosi solamente ad assistere la guida; ciò è possibile grazie ai veicoli a guida autonoma (*Autonomous Vehicle*, AUV), le cui applicazioni si baseranno su un approccio

cooperativo. Si tratta di una tecnologia che imprimerà notevoli cambiamenti, sia dal punto di vista tecnologico che sociale che (forse soprattutto) culturale.

5.1 Momenti significativi nella storia degli AUV

Vediamo in breve quali sono stati i tentativi e gli esperimenti più rilevanti che costituiscono la storia degli AUV, che per primi hanno esplorato il concetto di veicolo senza conducente e gettato le basi per la ricerca in questo campo [5].

5.1.1 Secolo XX

I primissimi esperimenti volti all'automatizzazione dell'automobile risalgono agli anni '20. Il primo veicolo a raggiungere buoni risultati è stato Linrrican Wonder, una Chandler del 1926 radiocontrollata, cui è stata installata un'antenna collegata all'impianto elettrico, potendo così quindi essere controllata dall'esterno. Durante l'esperimento la Chandler ha viaggiato senza il supporto attivo di un conducente grazie ad un secondo veicolo che la seguiva, il quale era in grado di dare comandi via radio a Linrrican Wonder, che riceveva ed attuava tramite l'antenna installata.

Qualche decennio più avanti, nel 1953, RCA Labs, in collaborazione con General Motors, è riuscita a costruire un modello sperimentale di automobile controllata tramite cavi posti sulla pavimentazione del laboratorio di sviluppo. Cinque anni più avanti, RCA è riuscita a portare questo risultato anche fuori dal laboratorio, allestendo un percorso in linea retta di circa 120 metri appena fuori la città di Lincoln (Nebraska, USA). Il sistema richiedeva che sotto tutta la pavimentazione stradale fossero presenti dei circuiti rivelatori in grado di comandare tutti i veicoli circolanti. Già in questi anni il concetto di automobile senza conducente iniziò ad inserirsi nella cultura popolare e ci furono già i primi manifesti pubblicitari, come si vede in figura 5.1.

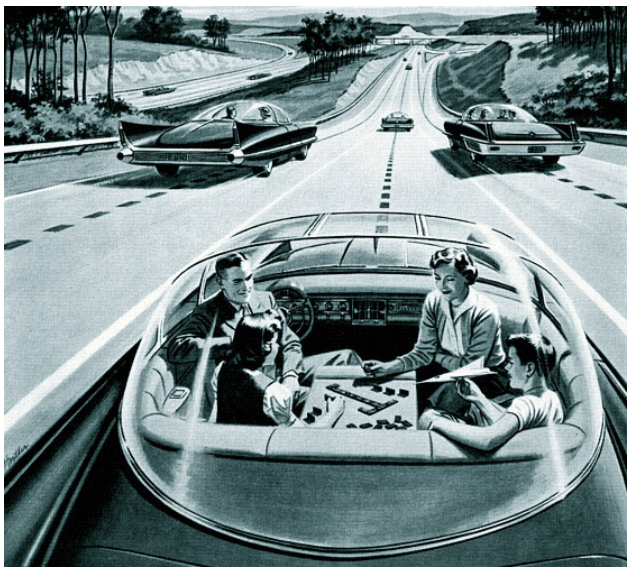

Figura 5.1: Uno dei primi manifesti a portare all'attanzione il concetto di guada autonoma. Immagine tratta da [5].

Dal 1960 si pensava che il controllo elettronico da parte della strada sui veicoli fosse il modello del futuro tanto che, in vista di questa tecnologia, il *Bureau of Public Roads* americano considerò la ristrutturazione di una serie di strade principali per inserire il supporto al controllo elettronico dei veicoli. Si prevedeva l'inizio della commercializzazione delle automobili sfruttanti questa tecnologia entro il 1975. Anche in Europa, nel Regno Unito, sempre negli anni '60, si facevano test con automobili controllate elettronicamente dalla pavimentazione stradale; un esperimento di successo vide una Citroën DS viaggiare costantemente e stabilmente a 130 km/h. Nonostante la ricerca verso questa tecnologia di cablaggio stradale fosse continuata fino al decennio successivo, a metà degli anni '70, in seguito a diverse valutazioni costi-benefici (l'ingente costo sarebbe stato del tutto rimborsato solo a partire dal terzo millennio a patto di ridurre gli incidenti del 40% e di ricoprire almeno il 50% dell'intera rete stradale), furono ritirati i finanziamenti necessari a renderla massiva.

Nel corso degli anni '80, Ernst Dickmanns e il suo team di ricerca dell'università di Monaco progettarono per Mercedes-Benz il primo furgone robotico in grado di viaggiare autonomamente su strada alla velocità di 63 km/h, a patto però di essere in assenza di traffico.

Lo stesso periodo ha visto la realizzazione di un altro notevole progetto finanziato dalla *Defense Advanced Research Projects Agency* (DARPA), l'*Autonomous Land Vehicle* (ALV), che per primo ha dimostrato la potenzialità di tecnologie come LIDAR e visione artificiale nell'ambito della mobilità autonoma, riuscendo a viaggiare in maniera promettente ad una velocità massima di 31 km/h. Nel 1989, la *Carnegie Mellon University* di Pittsburgh (Pennsylvania, USA) ha per prima sperimentato lo sfruttamento di reti neurali, tecnologia chiave anche per le strategie di controllo attuali.

Negli Stati Uniti, nel 1991, passò una legge che incaricò lo *United States Department of Transportation* (USDOT) a mostrare la fattibilità di un'infrastruttura autostradale di trasporto del tutto automatizzata entro il 1997. Il progetto è stato svolto in collaborazione con molti partner (tra cui GM), fino a che, nel 1997, un'autostrada di San Diego (California, USA) non ha visto il traffico di 20 veicoli sperimentali – tra cui automobili, autobus e camion – senza conducente.

Il 1994 fu un anno che vide in azione due dei prototipi più avanzati e pionieristici mai visti sino a quel momento. Si tratta di *VaMP* e di *VITA-2* da parte di Mercedes-Benz e della *Bundeswehr University of Munich*, le prime automobili in grado di viaggiare senza intervento umano, in condizioni di traffico intenso e per lunghe distanze. Il notevole esperimento ha visto il completamento di un trafficato percorso autostradale di circa 1.000 km (una distanza enorme, sino a quel momento) alla canonica velocità di 130 km/h, dimostrando ottime capacità di destreggiamento e riuscendo a completare efficacemente e in sicurezza persino sorpassi e cambi di corsia [10].

Un altro interessante esperimento fu svolto sempre dalla *Carnegie Mellon University* col progetto *Navlab*, nel 1995. Avendo percorso ben 5.000 km, si

tratta del primo viaggio coast-to-coast degli Stati Uniti per un'automobile senza guidatore. Nonostante questo, bisogna sottolineare che l'automobile utilizzata non era completamente autonoma ma semi-autonoma, dato che acceleratore e freni erano controllati manualmente (principalmente per motivi di sicurezza dei collaudatori), ma lo sterzo era del tutto controllato da reti neurali. Da sottolineare, però, che per il 98,2% del tempo e delle situazioni non c'è mai stato bisogno di un significativo intervento umano per quei compiti che il prototipo era in grado di svolgere autonomamente, un risultato incoraggiante.

Un prototipo simile, ma questa volta completamente autonomo, è stato realizzato anche in Italia all'*Università degli Studi di Parma* nel 1996, in cui un modello di Lancia Thema ha percorso con successo in sei giorni un tratto autostradale di ben 1.900 km in presenza di traffico, riuscendo a mantenere una velocità media di 90 km/h. L'automobile ha avuto bisogno del supporto attivo dei collaudatori solamente per il 6% del tempo. Fatto notevole è che per muoversi ha avuto bisogno solamente di alcune economiche videocamere e dell'elaborazione di algoritmi stereoscopici in tempo reale per "capire" dove si trovasse.

5.1.2 Terzo millennio

All'inizio degli anni 2000, il governo statunitense ha finanziato un progetto denominato *Demo III* per lo sviluppo di mezzi autonomi ad uso militare in grado di percorrere anche percorsi ostili e lontani da ambienti urbani e asfaltati. Il prototipo adottava il modello architetturale *Real-time Control System* (RCS) che provvede non solo al controllo del singolo veicolo, ma è uno dei primi in grado di imbastire una forma di coordinazione tra più veicoli.

Nel 2005, in Olanda divenne operativo su strada il mini-autobus *Park-Shuttle*, in figura 5.2, uno dei primi mezzi di trasporto pubblico senza bisogno di un conducente. Si tratta di una primissima forma di mobilità on-demand ed è stato progettato per percorrere itinerari fissi in ambienti urbani [8].

Figura 5.2: Parkshuttle. Immagine tratta da [5].

Alla fine del 2008, la compagnia canadese Rio Tinto Alcan decise di adottare i mezzi a guida autonoma anche per scopi non finalizzati al trasporto di persone, cominciando a testare in ambito minerario il primo sistema autonomo di trasporto di minerali commerciale al mondo, col suo *Komatsu Autonomous Haulage System*. L'azienda registrò numerosi benefici dall'adozione di questa nuova tecnologia, tra cui migliori standard di salute per gli operai, miglior sicurezza sul lavoro e maggior produttività.

Nel 2009, sebbene lo annunciò pubblicamente solo alcuni anni più tardi, fece il suo ingresso nello sviluppo dei mezzi a guida autonoma anche Google, iniziando lo sviluppo di quella che sarà la *Google Car* (figura 5.3).

Sicuramente degno di nota uno dei più grandi test svolti sino a quel momento è stato condotto con successo da *VisLab*, un progetto capitanato dal professor Alberto Broggi dell'*Università degli studi di Parma*, che, nel 2010, ha visto completare con successo il primo viaggio intercontinentale mai compiuto da auto a guida autonoma. Partiti da Parma ed arrivati con

Figura 5.3: Google Car. Immagine tratta da [3].

successo a Shanghai, i prototipi hanno percorso all'incirca ben 16.000 km in oltre tre mesi di viaggio su strade eterogenee e con livelli di traffico variabili.

Il primo maggio del 2012, Google svolse uno dei primi test pubblici per il suo prototipo, percorrendo un percorso di 22 km nella città di Las Vegas (Nevada, USA), non testando però ostacoli come rotonde, passaggi a livello o zone ad alta criticità pedonale (come scuole e asili).

Il 12 luglio del 2013, sempre *VisLab* effettuò un altro esperimento molto importante; il veicolo *BRAiVE* è stato il primo a raggiungere risultati così importanti, riuscendo a completare con successo nella città di Parma un itinerario urbano ad alto coefficiente di difficoltà. I prototipi hanno superato in sicurezza pericoli quotidiani come semafori, rotonde, attraversamenti pedonali e dossi, per la prima volta il tutto completamente senza intervento umano [9].

Nell'agosto del 2013, anche Daimler, con la collaborazione del *Karlsruhe Institute of Technology* (Germania), ha svolto un esperimento simile, riuscendo a far percorrere ad una Mercedes Classe S un percorso urbano di 100 km che andava dalla città di Mannheim alla città di Pforzheim. Nello stesso

mese, anche Nissan ha annunciato la sue presenza nello sviluppo di una propria tecnologia di self-driving, che sarà poi applicata l'anno successivo su una Nissan Leaf elettrica come dimostrazione. Ha anche annunciato che avrebbe cominciato a rendere disponibili al pubblico i suoi modelli di AUV a partire dal 2020.

A gennaio del 2014, compare finalmente il primo modello di veicolo senza conducente disponibile per la vendita commerciale. Si tratta di *Navia* da parte della francese Induct Technology, un minibus elettrico a 10 posti che, equipaggiato con quattro LIDAR e camere ottiche stereoscopiche, è in grado di muoversi autonomamente ad una velocità massima di 20 km/h. E' stato testato e viene utilizzato in alcuni poli universitari di Svizzera, Regno Unito e Singapore. Sempre nel corso del 2014, anche Google ha annunciato pubblicamente i suoi prototipi in sviluppo da anni, inoltre c'è stata anche la presentazione del primo modello a guida autonoma da parte di Tesla Motors, con la sua Model S (in figura 5.4), la prima in grado di poter ricevere aggiornamenti del proprio software nel corso del tempo, aumentando man mano le proprie abilità. Questa tecnologia da parte di Tesla, chiamata *AutoPilot*, è stata annunciata per metà del 2015.

Figura 5.4: Tesla Model S. Immagine tratta da [5]

A luglio del 2015, Google ha ufficialmente annunciato i risultati dei suoi

test nel corso dei sei anni precedenti. Il capo-progetto Chris Urmson ha rivelato che le Google Car hanno avuto un totale di 14 incidenti su più di tre milioni di chilometri percorsi. Da sottolineare che tutti gli incidenti subiti sono stati colpa delle automobili incontrate guidate manualmente, la maggior parte dei quali sono stati tamponamenti.

Sebbene non ci siano mai state conferme ufficiali, anche Apple sembra intenzionata ad entrare nel mercato dell'automotive con un veicolo elettrico [1].

5.2 Principali caratteristiche degli AUV e caso d'uso

MobEyes, *CarTorrent* e *CarSpeak* sono degli ottimi esempi dell'approccio cooperativo che avevamo menzionato prima; in un sistema di trasporto intelligente i veicoli si scambiano continuamente messaggi con informazioni riguardanti lo stato del traffico, della strada, ecc. in modo da mantenere una visione il più possibile completa del contesto. Questa collaborazione nel processare e diffondere i dati sensoriali agli altri sarà in assoluto uno dei punti chiave del concetto di guida autonoma.

Oltre ai veicoli anche la strada e gli oggetti che vi si trovano sopra, come ad esempio unità fisse poste ai margini delle strade in supporto ai veicoli in movimento (RSU), costituiranno quel reticolato dinamico che va a formare il cloud dei veicoli; in questo senso lo si può definire come un'istanza del concetto di Internet of Vehicles, che, assieme al cloud, provvede a fornire i protocolli e i servizi necessari alla griglia di veicoli per viaggiare efficientemente e in sicurezza [14].

Non è complicato immaginare che sarà proprio la guida autonoma (*Autonomous Driving*) ad essere uno dei maggiori beneficiari di questa architettura altamente "sociale", dato che un sistema avanzato di guida autonoma ha bisogno di costruire dettagliate mappe del traffico su varie scale e in tempo reale,

questo principalmente per evitare gli ostacoli e per identificare il percorso migliore da percorrere a seconda della situazione.

Un esempio di scenario avanzato di guida senza conducente può essere quello rappresentato in figura 5.5, in cui sia veicoli che RSU cooperano per stabilire e mantenere una volatile e locale piattaforma cloud virtuale [14].

Inizialmente vi sarà una fase di *discovery* delle risorse sensoriali e computazionali – ovvero veicoli e RSU disponibili – in grado di estendere il raggio di controllo (*context awareness*) oltre i singoli veicoli. Vi sarà un veicolo leader (in questo caso, supponiamo, V_1) che assumerà il ruolo di organizzatore del cloud inviando espliciti "inviti" a far parte della struttura del cloud a veicoli e RSU attorno. Una volta ricevute le risposte il leader seleziona i candidati più strategici (in questo caso, ad esempio, il veicolo V_2 e una videocamera stradale RC_1) provvedendo così alla formazione del cloud.

A questo punto V_1 si preoccupa di assegnare le varie mansioni agli altri veicoli, come ad esempio il raccogliere immagini aggiornate della zona. Una volta che il leader ha ottenuto ed elaborato i dati utili (indichiamo questo contenuto come C_1) vi è una fase di *sharing* di tali dati a tutti i membri facenti parte del network in quel momento. Il veicolo leader può anche delegare altri veicoli o unità (in questo caso V_4) a mantenere disponibili le informazioni per un futuro riutilizzo (*caching*). Ad esempio nuovi veicoli, come V_6 e V_7, potrebbe eseguire un broadcast di richiesta per C_1, a quel punto V_4 sarebbe in grado di soddisfare le due richieste senza bisogno di contattare V_1.

Il leader, oltre al ruolo di organizzatore, ha anche il compito di mantenere il cloud sempre funzionante; ad esempio uno dei membri precedentemente selezionati potrebbe dover abbandonare il suo ruolo, a quel punto V_1 seleziona un sostituto, scegliendo il più opportuno tra quelli da cui aveva ricevuto riposta nella fase di *discovery*, a quel punto provvederà a riassegnare i compiti che spettavano al precedente membro e aggiornerà la tabella dei membri.

Una volta che i suoi servizi non saranno più utili, il veicolo leader invierà un messaggio di rilascio ai veicoli che formavano la struttura assieme a lui

(in questo caso V_2 e RC_1), a quel punto il cloud e i suoi servizi smetteranno di esistere e i veicoli coinvolti potranno andare a costituire o ad usufruire di altri cloud.

Da sottolineare che la comunicazione tra le varie parti del cloud è tutta di tipo peer-to-peer (V2V e V2I).

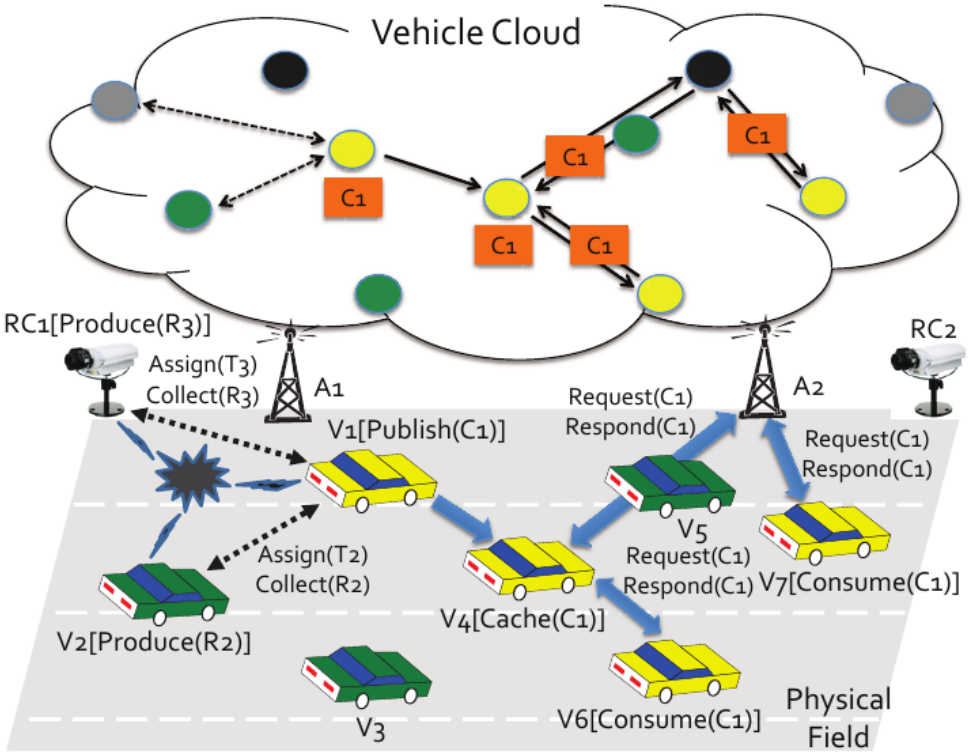

Figura 5.5: Un esempio di cloud di veicoli. Immagine tratta da [14].

5.2.1 Le principali sfide per la diffusione degli AUV

Il passaggio dalla guida manuale assistita alla guida autonoma porta con sé numerose nuove sfide. Nonostante la questione sulla gestione della quantità

massiva di dati generati dai molteplici sensori di cui sono equipaggiati i veicoli sia già stata affrontata, diventa ancora più critica nel caso di automobili senza controllo umano. Nei casi di indecisione potrebbe volerci un tempo non trascurabile e non innocuo prima che l'uomo riprenda completamente il controllo della vettura e ciò diventerebbe ancora più critico con automobili completamente autonome, in fondo uno dei grandi vantaggi di questa tecnologia è permettere alle persone di viaggiare in macchina esattamente come se fossero su un treno, un autobus o un taxi.

Ma vediamo quali sono alcune delle sfide principali per poter realmente portare su scala mondiale questa potenzialmente rivoluzionaria tecnologia [14].

Applicazione di un Named-Data Network

Abbiamo già sottolineato nello scorso capitolo l'importanza di un *Named-Data Network* per la mobilità intelligente, ma anche questa sfida diventa ancora più delicata se parliamo di AUV, dato che parliamo di mezzi che, senza guidatore, devono fare affidamento totale ai dati generati dai sensori. Trovare quelli giusti in un volume potenzialmente sconfinato di informazioni e in tempo reale diventa un pre-requisito, non semplicemente una "caratteristica in più".

Allarmi e segnali

Sebbene i sensori facciano gran parte del lavoro necessario a rendere possibile una navigazione autonoma, da soli potrebbero non essere sufficienti a garantire totale sicurezza in situazioni dove la velocità di crociera e la densità dei veicoli sono particolarmente elevate.

In caso di emergenza in testa ad una coda, come un tamponamento, la comunicazione V2V in real-time diventa molto importante per i veicoli più indietro, in quanto potrebbe evitare pericolose reazioni a catena e dareb-

be la possibilità di cambiare in anticipo il proprio comportamento, come ad esempio la velocità o addirittura l'itinerario, prima che la sicurezza sia compromessa. Bisogna anche sottolineare che in situazioni come queste un sistema automatico di rilevazione dei pericoli sarebbe molto più reattivo di qualsiasi guidatore umano e soprattutto non avrebbe modo di subire cali di prestazioni dovuti a distrazioni, fatica, stanchezza, alterazioni e svariate altre comuni cause di incidente.

Recupero in caso di failure delle infrastrutture

Come facilmente prevedibile, il concetto di guida autonoma è fortemente legato all'infrastruttura, dalla quale dipende. Per esempio, la comunicazione diretta con gli altri veicoli, l'accesso ai dati delle unità stradali o l'accesso alla rete globale tramite connessione WI-FI o LTE sono requisiti di primaria importanza per l'efficienza e la sicurezza degli AUV.

In caso di failure dell'intero sistema, per esempio dovuto ad un disastro naturale, vi è uno spazio temporale critico compreso tra l'avvenimento del disastro e il momento in cui i veicoli possano fermarsi. Durante quest'arco di tempo è importante che i veicoli riescano almeno temporaneamente a gestire la situazione e a muoversi avvalendosi unicamente delle proprie singole capacità sensoriali, senza dunque cooperare con gli altri, questo almeno fino a quando il veicolo non sarà in grado di fermarsi in totale sicurezza (o eventualmente fino a che una persona a bordo non sia pronta a prendere manualmente il totale comando dell'automobile, se possibile).

Nonostante le failure, sarebbe comunque auspicabile che una forma di comunicazione diretta V2V rimanesse ugualmente disponibile.

Condivisione di file e multimedia

Lo scambio e il download di file multimediali ha due principali finalità. La prima è la condivisione di eventi riguardanti il traffico, la seconda è puramente

ricreativa.

Nel primo caso, la propagazione di immagini chiave, come un incidente o altri avvenimenti rilevanti, è molto importante per il monitoraggio stradale, oltre ad essere informazioni utili anche ai veicoli diretti in quella direzione. Per esempio un veicolo, nel percorrere il suo itinerario, può costantemente fare richiesta della situazione aggiornata delle strade che dovrà percorrere; nel caso dovessero arrivargli messaggi con immagini (o metadati) di percorsi inagibili, questo potrà decidere in anticipo quale strategia adottare. Come già detto, per questo tipo di scambi è opportuno adottare una comunicazione peer-to-peer, dato che latenze e volume dei dati renderebbero non scalabile e poco performante una comunicazione centralizzata su server remoti.

Nel secondo caso, il download di file multimediali da internet come musica, film, videogiochi, ecc. è funzionale al comfort e all'intrattenimento dei passeggeri. Rappresenta inoltre una strategia di marketing chiave per i veicoli a guida autonoma.

Concorrenza spettro dei segnali

La comunicazione massiccia e ininterrotta tra i veicoli richiederà all'infrastruttura di telecomunicazione uno spettro notevolmente grande per poter sostenere lo scenario futuro.

Attualmente non è detto che lo stato attuale delle tecnologie di *dedicated short-range communication* (DSRC) sia pronto per farcela, soprattutto in una prospettiva di crescita continua dell'utilizzo di tale tipo di comunicazione in ambito stradale. Gli scenari più critici sono ovviamente quelli in cui ci si ritrova in zone ad alta densità di popolazione, dove il livello di congestione è elevato e dove la propagazione del segnale deve vedersela con una massiccia concorrenza da parte degli altri veicoli e un ingente rumore esterno.

Una prima ipotesi per far fronte a tale problema è quella di servirsi anche dello spettro del WI-FI, andando a competere così con l'infrastruttura residenziale, tutto ciò in una modalità di condivisione dinamica dello spettro.

Abbiamo sottolineato più volte l'importanza dello scambio reciproco di informazioni, quindi questa si presenta come una questione di importanza non irrilevante per la fattibilità della guida autonoma.

Virtualizzazione

Si tratta di un altro aspetto importante per questa tecnologia, dato che permette ai veicoli di usufruire dei servizi di supporto offerti dall'internet cloud. In un'ottica collaborativa può essere molto utile avere la possibilità di sfruttare potenze computazionali remote molto più potenti della propria unità di elaborazione interna, come per processi di data-mining.

Un esempio di utilizzo potrebbe essere quello del riconoscimento di un veicolo sospetto; il processare immagini e la consultazione di database online richiede uno sforzo computazionale e di rete potenzialmente molto elevato, quindi, una volta svolte le operazioni preliminari in locale (come la raccolta di immagini), l'esportare trasparentemente parte del carico di lavoro all'esterno potrebbe rappresentare un notevole incremento di efficienza, sia per il processo che per il veicolo stesso, che nel frattempo può svolgere altre attività.

Sicurezza

Anche qui abbiamo a che fare con un aspetto chiave che sarà cruciale per il destino di questa tecnologia. Questioni come privacy, confidenzialità, autenticazione, protezione da DDoS, prevenzione attacchi MiTM, ecc. erano già di fondamentale importanza anche nell'ambito della guida assistita. Con gli AUV, oltre a riconfermarsi vitali, la sicurezza informatica diventa ancora più critica, visto che stiamo parlando di affidare la guida fisica di un mezzo di trasporto (con all'interno potenzialmente decine di persone) ad un computer collegato in rete ad altri computer analoghi.

Un nefasto scenario da prevenire, molto più pericoloso per gli AUV rispetto alle auto guidate manualmente, è quello in cui un malintenzionato riesca a prendere il controllo remoto di componenti chiave dell'automobile, quale acceleratore, sterzo e/o freni, oppure quello in cui riesca a modificare la destinazione del veicolo. Ciò può dare una chiara idea della priorità di questo ambito di ricerca.

Una prima forma di prevenzione potrebbe consistere nello strutturare gli accessi alle varie parti del veicolo secondo predeterminate gerarchie di permessi e in funzione di certi eventi. Per esempio le comuni automobili avranno solamente il minimo grado di privilegio nei confronti dei loro pari, potendo accedere in sola lettura ai dati strettamente necessari – e il più impersonali possibile – per un'efficiente e sicura coordinazione. Mentre invece veicoli come quelli delle forze dell'ordine oppure veicoli di soccorso, opportunamente autenticati, potranno avere un livello di privilegio più elevato, potendo impartire ai comuni AUV comandi funzionali per esempio alla cattura di un malvivente o al soccorso medico.

Parleremo un po' più approfonditamente dell'importante ambito della sicurezza informatica nel corso del capitolo 6.

5.2.2 Implicazioni, legislazioni e concetto di Mobility-as-a-Service

La diffusione del paradigma della mobilità autonoma non avrà conseguenze puramente tecnologiche, ma inciderà radicalmente sulla vita quotidiana delle persone. Impieghiamo negli spostamenti una considerevole parte del nostro tempo, delle nostre risorse e delle nostre energie, quindi un impiego massivo di questo sistema avrà certamente importanti implicazioni sociali, economiche, ecologiche e addirittura di natura etica. Vediamo di seguito una serie di possibili pro e contro di questa tecnologia [2].

Implicazioni potenzialmente positive

Uno dei vantaggi più lampanti nell'utilizzo di un robot alla guida di un veicolo è la completa assenza del fattore "errore umano". Si stima che circa il 90% dei sinistri sia imputabile ad una non corretta condotta dei guidatori. Condotta aggressiva e guida distratta sono i principali nemici della sicurezza fisica degli utenti della strada; si pensi a situazioni come un mancato mantenimento della distanza di sicurezza e le a volte inevitabili distrazioni dovute anche a fattori esterni alla guida. Un robot non solo sarebbe sostanzialmente programmato per seguire alla lettera il codice della strada, ma sarebbe anche esente da qualsiasi tipo di calo di prestazioni; diminuzione dei tempi di reazione, stanchezza, distrazione, ebbrezza, stordimento da droghe, ecc. non avrebbero più influenza sulla guida, quindi sulla sicurezza pubblica.

Come abbondantemente illustrato in precedenza, l'abbondanza di sensori presenti nell'automobile apre a numerosi vantaggi. La comunicazione attiva tra i veicoli in movimento permette in primis una gestione migliore del traffico, con relativi effetti su tempi di percorrenza, congestioni ed inquinamento. Bisogna anche considerare che, grazie a questa maggior "coscienza" dell'ambiente esterno da parte dei veicoli, anche i furti saranno notevolmente più complessi da portare a termine con successo.

Con la diminuzione di incidenti e furti, calerebbero drasticamente gli eventi indesiderati per le compagnie assicuratrici, è verosimile ritenere che, diminuendo i rimborsi erogati, anche i premi assicurativi subirebbero delle diminuzioni in favore dei clienti. Oltre a questo, anche gli interventi delle forze dell'ordine in caso di sinistri calerebbero sensibilmente, con conseguente risparmio sulla spesa pubblica.

Arrivati in un'ipotetica situazione in cui tutti i veicoli circolanti rispettino scrupolosamente il codice della strada, sarebbe possibile rivedere anche i limiti di velocità e le distanze di sicurezza. Tali valori sono calcolati tenendo conto del cervello umano e dei limiti dei suoi riflessi, in modo che rispettandoli sia possibile reagire in sufficiente sicurezza in quasi tutte le situazioni. Ma

in un contesto dove il tempo di reazione ad un imprevisto cala drasticamente (perché eseguito da una macchina e non da un cervello umano) sarebbe possibile ricalcolare questi valori a tutto vantaggio dei passeggeri, che potrebbero godere di una maggiore efficienza negli spostamenti e di una diminuzione del tempo di percorrenza senza incidere negativamente sulla sicurezza fisica.

Con l'impiego massivo dei robot alla guida sarebbe anche possibile ripensare la segnaletica stradale, dato che la maggior parte delle informazioni necessarie verrebbero apprese tramite comunicazione elettronica diretta con altre automobili, RSU o server centrali.

Un'altra importante implicazione è la seguente. Le persone sarebbero, in prospettiva, del tutto sollevate da qualsiasi onere che richieda un veicolo su strada al guidare, ciò significa che potrebbero dedicarsi ad altre attività, esattamente come se fossero su un mezzo pubblico, ciò a vantaggio di produttività e riposo; gli "ex-guidatori" sarebbero inoltre liberati dal lavoro nervoso – talvolta davvero massiccio in zone altamente congestionate – che richiede la conduzione di un veicolo. Non è un aspetto secondario considerando che i brevi/medi viaggi in macchina occupano mediamente una finestra di tempo non trascurabile nell'arco della giornata delle persone.

Implicazioni potenzialmente negative

Nonostante i grandi vantaggi, ci sono anche numerosi ostacoli da gestire, di ogni tipo.

Innanzitutto, per un funzionamento sempre corretto, i veicoli hanno bisogno di software perfettamente stabile ed affidabile. Vista la sua complessità è un compito della massima responsabilità e ad elevato coefficiente di difficoltà, dato che bug, vulnerabilità e attacchi malevoli potrebbero costituire un grande pericolo per i passeggeri.

Un altro aspetto ancora tutto da perfezionare è il seguente; questo tipo di tecnologia mostra risultati e livelli di stabilità e sicurezza soddisfacenti, ma tutto questo in condizioni meteorologiche favorevoli. La capacità di sensori

ed attuatori di saper resistere a disturbi come pioggia intensa, nebbia fitta, neve, venti forti, ecc. è al momento ancora tutto da affinare [4].

Molti prototipi attualmente funzionanti (sebbene non tutti) dipendono da mappe sempre perfettamente aggiornate e dall'alto livello di dettaglio, mantenerle tali è un compito oneroso e non sempre fattibile. Laddove non lo sia sarebbe auspicabile che le automobili siano comunque in grado di orientarsi sulla base di sensori e comunicazione.

Tutti i cambiamenti e le novità esposte sino ad ora richiedono notevoli cambiamenti – talvolta pure ricostruzioni – dell'intera infrastruttura stradale pubblica e privata per poter funzionare in maniera ottimale. Come ben si può immaginare, si tratta di un obiettivo molto grande che richiede costi gravosi sia in termini economici che di tempo. Tutto questo richiede la notevole capacità da parte di governi, legislatori, imprenditori e persino normali cittadini di prendere importanti e onerose decisioni a lungo/lunghissimo termine.

Ma gli ostacoli non sono solamente di natura prettamente tecnologica e infrastrutturale. Dal punto di vista legale, ad esempio, ci sono ancora molti punti aperti. In caso di incidente, come si stabilirebbero le responsabilità? Senza un quadro normativo stabilito in maniera chiara e univocamente interpretabile, ai primi incidenti potrebbero partire subito costose controversie; il prodotto, a quel punto, potrebbe venire probabilmente ritirato per timore di eccessive spese legali da parte dei manifatturieri.

Bisogna ricordarsi che un AUV si attiene perfettamente ai limiti stabiliti, tuttavia se il guidatore avesse la possibilità di passare ai comandi manuali (come potrebbe servire in situazioni d'emergenza), potrebbe violare il codice della strada e causare un incidente. In questo caso come sarebbero distribuite le responsabilità? Oppure il guidatore potrebbe essere passato ai comandi manuali per compensare un comportamento erroneo della vettura, ma non esserci riuscito e aver causato un incidente. Di chi sarebbe la colpa? Le questioni legali non sono meno prioritarie della tecnologia stessa.

Non da sottovalutare nemmeno le barriere psicologiche che molte persone avranno; anche essendo consapevoli che statisticamente la macchina è mediamente più sicura dell'essere umano, affidarsi completamente ad un robot è difficile per moltissime persone. Consideriamo, inoltre, che un AUV sbaglia in maniere completamente differenti dalle persone, quindi gli incidenti sarebbero probabilmente dovuti a situazioni che un guidatore umano avrebbe saputo gestire e la macchina no; sebbene siano numericamente (molto) minori, questo fatto quasi certamente creerà istintivamente delle resistenze nell'opinione pubblica.

Il passaggio da un parco di veicoli non-autonomi ad uno di veicoli autonomi sarà ovviamente graduale. Durante il potenzialmente lungo processo questi due tipi di veicoli – con distribuzioni via via differenti – dovranno coesistere, questo significa che gli AUV dovranno saper affrontare situazioni impreviste con un sufficiente livello di sicurezza. Tali imprevisti sono sostanzialmente dovuti all'assenza di garanzia che il guidatore umano seguirà alla lettera le regole della strada, oltre al fatto che un buon numero di automobili circolanti non saranno di ultima generazione, quindi incapaci di comunicare e cooperare attivamente con le altre.

Un ulteriore dibattito lo si potrebbe fare su una potenziale perdita della privacy dovuta proprio alla massiccia comunicazione; ogni itinerario, spostamento, targa e persino viso è potenzialmente tracciabile e incrociabile con le informazioni degli altri, ciò è vero anche più in generale per l'Internet of Things.

Un delicato problema molto attuale è quello del pericolo terrorismo. Un veicolo in movimento ha il potenziale per diventare una bomba in movimento; in realtà ciò è già tecnicamente possibile, ma l'eventualità che i veicoli possano viaggiare senza conducenti potrebbe rappresentare una facilitazione o un incentivo per qualche malintenzionato. Va però anche sottolineato che un veicolo autonomo più difficilmente riuscirà a rimanere completamente autonomo e dipendente alla volontà del proprietario, Grazie ad un miglior *context-awareness* da parte dei veicoli stessi, trasportare materiale pericoloso

potrebbe diventare ancora più arduo.

Un'altra delicata situazione su cui riflettere è quando un veicolo guidato da un robot non ha modo di poter evitare, per esempio, un investimento mortale. Consideriamo un nefasto scenario in cui un'automobile senza conducente, impossibilitata ad arrestarsi in tempo, sia costretta a scegliere tra due direzioni entrambe occupate da pedoni; come agire in questi casi? Si tratta sostanzialmente di decidere chi è "meno peggio" investire e, potenzialmente, uccidere. Ma secondo quale criterio? Minimizzare il numero delle vittime è forse una soluzione considerabile, ma non è una decisione scontata, si tratta di una questione etica molto complessa e tutt'altro che secondaria. Inoltre, chi deciderà come i veicoli dovranno reagire? Sarà una scelta a discrezione del costruttore o ci sarà una regolamentazione comune? E' una questione che, sebbene si riferisca ad eventualità probabilmente molto rare, è ancora molto aperta e prioritaria.

Consideriamo ora un paio di questioni che guardano al lungo termine, quando gli AUV costituiranno la grande maggioranza del parco veicoli circolante. Verosimilmente, la grande maggioranza degli utenti viaggeranno per tutto il loro tempo (o comunque per la maggior parte) esclusivamente come passeggeri, è lecito quindi considerare che, nonostante un addestramento su come guidare manualmente un veicolo lo riceveranno comunque, avranno lo stesso un'esperienza molto ridotta nella conduzione manuale di un veicolo; siccome, come già detto, in alcune rare e imprevedibili situazioni d'emergenza potrebbe essere necessario il controllo umano, l'inesperienza potrebbe costituire un ostacolo.

Un'altra notevole questione da considerare è la seguente. Attualmente moltissimi mestieri si basano sulla conduzione manuale di veicoli; tassisti, autisti, camionisti e piloti, sono mestieri destinati a diventare non più richiesti. L'automatizzazione del trasporto di persone e merci diminuirà (seppur gradualmente) in maniera non trascurabile la capacità occupazionale della società, proprio per questo è facile prevedere che ci saranno moltissime resistenze a riguardo; è quindi fondamentale che economicamente, politicamente,

socialmente e culturalmente questa questione venga pianificata e gestita nella maniera più saggia possibile.

Concetto di Mobility-as-a-Service

Nel 1948, a Zurigo (Svizzera), è nato il primissimo concetto di automobile condivisa, col programma di carsharing *Selbstfahrergenossenschaft*. Da allora, fino ad oggi, è sempre stato un modello di nicchia per lo spostamento in automobile, solitamente ci si affida a mezzi pubblici come autobus e treni, ma l'idea e il bisogno del mezzo di proprietà sono stati e sono tuttora il paradigma dominante. Sebbene negli ultimi tempi il carsharing sia un modello di mobilità in crescita, come evolverà grazie all'arrivo dei veicoli senza conducente?

La vera grande rivoluzione che, in prospettiva, potrebbero portare i veicoli a guida autonoma è la graduale diminuzione del bisogno del mezzo di proprietà. Questo è particolarmente vero già oggi nei grandi centri abitati, in cui la densità di mezzi pubblici è particolarmente elevata; i residenti di tali zone, avendo tutti i servizi maggiormente a portata di mano e potendo fare affidamento su frequenti autobus e metropolitane, sentono il reale bisogno di un mezzo privato meno frequentemente. Dall'altra parte, coloro che risiedono in zone non centrali, come periferie, campagne o montagna, dove i servizi sono meno presenti e i mezzi pubblici molto meno frequenti e comodi da prendere, non avranno altre alternative che utilizzare un mezzo di proprietà ogni volta che dovranno uscire di casa. L'enorme potenziale che si porta dietro questa tecnologia è l'ampliamento del raggio d'azione del mezzo pubblico. Si immagini uno scenario in cui l'automobile diventi essa stessa un mezzo condiviso utilizzabile a chiamata e che la sua disponibilità diventi capillare. Ad oggi un simile modello è già adottato dai taxi o da aziende come Uber: chiamata di un mezzo, comunicazione della destinazione, pagamento una volta raggiunta, mezzo disponibile per qualcun altro.

L'utilizzo degli AUV ha però ulteriori vantaggi; l'assenza di un conducente

rappresenterebbe una notevole diminuzione dei costi sia di gestione che per l'utente finale, rendendo il servizio molto più accessibile. Inoltre, grazie alla sua grande efficienza nel coordinarsi con gli altri AUV, la tempestività e la disponibilità del servizio aumenterebbero considerevolmente.

Stiamo entrando nell'era del *Mobility-as-a-Service* (MaaS) e la sua diffusione ha il potenziale per rendere il mezzo pubblico capillarmente accessibile anche nelle zone non centrali e per renderlo facilmente disponibile per molte più persone contemporaneamente. Ciò porterebbe, nel complesso, ad un bisogno sempre minore del bisogno di un mezzo di proprietà per muoversi.

Uno dei principali problemi del concetto di mezzo di proprietà è che probabilmente presto sarà destinato a diventare insostenibile; la popolazione in grado di acquistare un mezzo proprio è in costante aumento e, conseguentemente, lo è anche la densità del traffico; ciò porta ad un aumento costante del numero di veicoli presenti su strada, presentando notevoli problemi di spazio, efficienza e anche di emissioni inquinanti. Un altro aspetto da considerare è la notevole inefficienza del mezzo ad uso della singola persona. Si stima che mediamente oltre il 90% del tempo di vita di un'automobile questa rimanga spenta e inutilizzata; ciò è verosimile se si considera che il tempo che passiamo alla guida è comunque una parte relativamente piccola nell'arco della giornata. Grazie al paradigma dell'automobile condivisa, un mezzo resterebbe in movimento per quasi il 100% del proprio ciclo di vita, ciò renderebbe quindi possibile una drastica riduzione del numero di veicoli presenti sul territorio, i vantaggi sarebbero molteplici.

Si pensi inoltre alla notevole quantità di spazio urbano necessaria all'alloggiamento di tutti i mezzi di trasporto; se tutti i veicoli rimanessero in costante movimento, oltre a servirne molti meno (dato che uno può servire molte persone consecutivamente), sarebbero necessari molti meno parcheggi, spazio che potrebbe essere riutilizzato in maniera più proficua al benessere collettivo. Una gestione particolarmente efficiente del ridimensionato parco mezzi avrebbe anche effetti positivi sulla vivibilità dello spazio pubblico, sulla sicurezza, sul monitoraggio dei veicoli e sull'ecologia, oltre probabilmente

a costi più abbordabili per gestori e utenti.

Il concetto di MaaS rappresenta anche un nuovo modello di business che, grazie ad abbonamenti o pagamenti sul posto, potrebbe rendere la mobilità più facile ed accessibile per tutti. In uno scenario ideale, con un semplice smartphone e una connessione internet, chiunque potrebbe richiedere un passaggio al veicolo autonomo libero più vicino, il quale lo verrà a prendere e lo porterà a destinazione; una volta arrivato l'utente scenderà senza minimamente preoccuparsi del posteggio, mentre l'automobile andrà a soddisfare la richiesta dell'utente successivo.

Capitolo 6

Sicurezza e privacy

L'Internet dei veicoli è un modo di concepire l'internet al servizio della mobilità con un grandissimo potenziale; come abbiamo visto sono tantissimi gli scenari e le tecnologie nuove in grado di cambiare anche radicalmente il modo di intendere la mobilità, ma per far sì che ciò avvenga è necessario che problemi come sicurezza informatica e privacy vengano opportunamente affrontati e che siano integrati by design alle nuove tecnologie.

Il mondo sta diventando e diventerà sempre più interconnesso, ciò purtroppo non è funzionale solamente alle buone idee ma introduce anche numerosi nuovi metodi e opportunità di cattivi utilizzi da parte di malintenzionati o autorità poco democratiche. Trovare un modo per utilizzare la crittografia in maniera che sia contemporaneamente efficace, trasparente e scalabile è necessario. In un contesto del genere, inoltre, gli attaccanti hanno dei vantaggi rispetto ad un contesto tradizionale; tanto per cominciare veicoli attaccanti e utenti normali utilizzano la stessa infrastruttura fisica, dato che viaggeranno sulla stessa strada, senza contare che identificare univocamente da dove venga l'attacco è reso notevolmente più difficoltoso dal contesto altamente mobile e dinamico.

6.1 Attacchi malevoli: quali, come e perché

Quali potrebbero essere i principali obiettivi di un attacco malevolo? Principalmente tre [20]:

- avere accesso ad informazioni riservate o di valore all'interno del *Vehicular Cloud* (VC);
- poter compromettere l'integrità delle informazioni alle quali si ha accesso, minando così la sicurezza degli altri utenti a proprio vantaggio;
- poter prendere il controllo di altre entità, come veicoli, RSU o intere infrastrutture e server centrali.

Vediamo in principio come potrebbe svolgersi un attacco: una volta individuato un veicolo target ed essendosi posizionati nelle sue vicinanze, l'attaccante cercherà di individuare e di localizzare, rifacendosi alla topologia del VC, il servizio di cui sta usufruendo il target; a questo punto l'attaccante proverà a fare richieste per accedere alle stesse applicazioni e, tramite lo sfruttamento di eventuali vulnerabilità, cercherà di aumentare i suoi privilegi per accrescere il suo controllo sul veicolo target.

Vediamo ora quali sono le più comuni minacce cui anche l'IoV è suscettibile:

- ***Spoofing***: si tratta di una modalità di attacco in cui un utente cerca di appropriarsi dell'identità di un altro utente in modo da far credere agli altri di essere quella persona; l'esempio più comune di un attacco di questo tipo è il *Man-in-The-Middle* (MiTM) mentre Alice e Bob comunicano, in cui l'attaccante riesce a far credere a Bob di essere Alice e ad Alice di essere Bob, in questo modo è perfettamente in grado di accedere in chiaro ai loro messaggi.
- ***Tampering***: oltre al semplice accesso ad informazioni non autorizzate, l'attaccante è anche in grado di manipolarle e comprometterne l'integrità.

- ***Repudiation***: se questo tipo di attacco è in atto, il malintenzionato è in grado di agire sul sistema e sui dati senza lasciare alcuna traccia, log o persino di lasciarne di false.

- ***Information disclosure***: l'attaccante è in grado di sfruttare parti vulnerabili del sistema tramite le quali riesce ad ottenere informazioni sensibili quali dati personali, identità o informazioni critiche riguardanti lo stato del VC.

- ***Denial of service***: classica pratica con la quale si cerca di sovraccaricare il provider di un servizio o applicazione consumando tutte le sue risorse, ad esempio inviando un massiccio numero di richieste in modo che non sia più in grado di offrire il suo servizio a nessun altro.

- ***Privilege escalation***: tramite lo sfruttamento di bachi del sistema, il malintenzionato acquisisce il controllo di risorse normalmente non autorizzate ad un normale utente o applicazione, ciò lo mette nella situazione di poter compiere azioni impreviste e potenzialmente pericolose.

Ragionando sulla sicurezza di un'infrastruttura il cui funzionamento si basa sullo scambio di messaggi, possiamo distinguerne principalmente di due tipi: messaggi funzionali alla cooperazione e alla sicurezza e messaggi confidenziali [20].

Per il primo tipo abbiamo sostanzialmente tre livelli di criticità; al livello uno abbiamo scambi di informazioni non sensibili, quali la segnalazione di ostacoli ad altri veicoli, presenza di un ingorgo, ecc.; al livello due abbiamo messaggi della stessa natura ma urgenti e necessari entro un certo lasso di tempo; al livello tre abbiamo messaggi critici, a volte non ridondanti, necessari a stabilire responsabilità e dinamiche in situazioni gravi quali incidenti o atti criminali. In tutti e tre i casi la privacy e l'identità della sorgente del dato dovrebbe essere protetta e accedibile solamente da autorità certificate.

Per quanto riguarda i messaggi privati è opportuno che mittente e destinatario possano verificare esattamente quale sia la reciproca identità – nei messaggi del tipo precedente, specialmente se si adotta un paradigma content-centric, questo non era strettamente necessario, era sufficiente certificare la bontà e l'autenticità del contenuto del messaggio. Un modello di scambio con chiave pubblica e chiave privata con crittografia e firma del messaggio (in stile PGP) è dunque strettamente consigliato allo scopo.

6.2 Autenticazione

In quasi tutte le situazioni ha un'importanza fondamentale la corretta autenticazione degli utenti, quindi dei nodi. Per ottenerla ci possono essere varie strategie, come per esempio la titolarità di una qualche identità o di un token, oppure la conoscenza di una qualche informazione (come una password o un PIN o la corretta risposta ad una qualche domanda personale); un altro metodo più moderno per identificare un utente è lo sfruttamento della biometria (firma, impronta digitale, viso, voce, ecc.).

Bisogna tenere presente che il contesto altamente mobile dei nodi può rendere difficoltosa l'autenticazione di dati che si basano sulla localizzazione delle informazioni, come ad esempio un messaggio di allarme per l'ubicazione di un incidente o la denuncia di qualche tipo di azione illegale. Anche i limiti puramente fisici potrebbero costituire un problema da affrontare, dato il rischio failure dovuto alla velocità e al relativamente stretto raggio di trasmissione da parte dei veicoli. Un'altra questione ancora è l'aggiornamento di token e chiavi di identificazione; non è affatto scontato che tutti i veicoli siano utilizzati costantemente e sempre in movimento, in tal caso gli sarebbe impossibile poter aggiornare tempestivamente le proprie chiavi (oltre alle identità degli altri).

Un'ulteriore sfida nel processo di autenticazione di un veicolo o di un conducente (passeggero, se parliamo di AUV) è quella della preservazione

della sua privacy; la sua reale identità potrebbe venire rimpiazzata da qualche pseudonimo, in questo caso però il processo vede una difficoltà in più, dato che in caso di alcuni tipi di eventi è necessario poter risalire all'identità del guidatore. Per mediare a questo inconveniente si potrebbe pensare di istituire un servizio denominato *Pseudonymization Service Center* [20], una struttura sicura e certificata che solo lei sia in grado di associare uno pseudonimo alla reale identità del guidatore. Per maggior sicurezza gli pseudonimi potrebbero essere effimeri e periodicamente rinnovati.

Oltre all'autenticazione dei singoli veicoli è fondamentale anche l'autenticazione dei provider e dei servizi pubblici a cui si rifanno molte delle applicazioni al servizio di guidatori/AUV e passeggeri. Innanzitutto tutti i veicoli dovrebbero poter aver modo di verificare univocamente le identità dei provider a cui stanno chiedendo servizi, specialmente quelli governativi cui vengono comunicate informazioni sensibili e dal valore legale (numero dell'assicurazione, targa, identità del proprietario, ecc.).

Nel processo di verifica dell'identità bisogna anche tenere conto del fatto che, per natura di molti tipi di applicazioni e per la struttura spesso decentralizzata della comunicazione, i nodi quasi mai comunicano direttamente con la struttura fisica cui sono interessati; come si vede in figura 6.1, molti nodi vengono coinvolti nella trasmissione di un dato, come gli altri utenti, le RSU, infrastrutture intermedie e altro.

6.2.1 Autenticazione geografica

Per incrementare l'affidabilità dell'autenticazione e la confidenzialità dei messaggi scambiati, ci sono alcune situazioni in cui al classico schema con coppie di chiavi si può pensare di affiancare un meccanismo di sicurezza *location-based*. Le informazioni verrebbero ulteriormente criptate con una chiave pubblica corrispondente alla locazione fisica presunta del destinatario, quindi i dati così inviati potranno essere letti solamente se quest'ultimo si trova effettivamente all'interno della zona geografica di cui il mittente ha scelto la

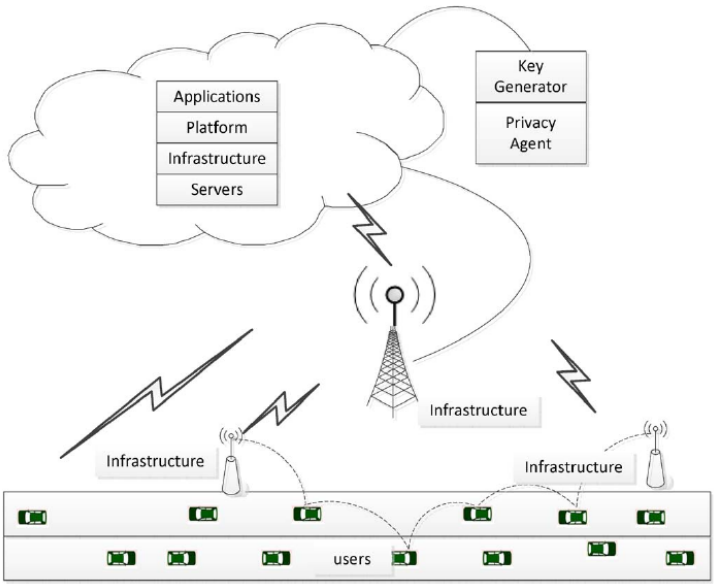

Figura 6.1: La comunicazione tra due nodi è quasi sempre indiretta. Immagine tratta da [20].

chiave. Una volta che il destinatario ha decifrato il dato con la corretta "chiave geografica", potrà normalmente utilizzare la sua personale chiave privata per accedere al testo in chiaro [20].

In uno scenario simile, se anche un attaccante malauguratamente riuscisse ad entrare in possesso della chiave privata di un veicolo target per intercettare le sue comunicazioni, sarebbe anche costretto a trovarsi fisicamente dove si trova lui per poter accedere ad un ciphertext interpretabile. Per esempio, come si vede in figura 6.2, se il veicolo a provasse a mandare un messaggio (che passa attraverso molti nodi) al veicolo g e uno tra b, c, d ed e fosse in possesso della sua personale chiave privata, il messaggio sarebbe comunque al sicuro, perché prima di poterla sfruttare dovrebbero trovarsi all'interno della zona target. Solamente f sarebbe potenzialmente in grado di offendere, perché molto vicino alla zona geografica interessata.

Figura 6.2: Autenticazione *location-based*. Immagine tratta da [20].

Questo modello, in grado di rendere alcuni tipi di attacco più impegnativi e costosi, è utilizzabile solamente a patto di riuscire ad assicurare l'effettivo utilizzo delle chiavi di decifratura solamente all'interno di una data zona e nelle situazioni in cui la locazione geografica del destinatario è nota e sufficientemente statica.

6.3 Gestione di chiavi e certificati

La gestione delle chiavi rappresenta un punto cruciale per la sicurezza del cloud dei veicoli. Innanzitutto tutte devono essere generate seguendo algoritmi standard e dalla comprovata affidabilità (l'adozione di algoritmi e software liberi e open-source è probabilmente una buona idea), inoltre devono poter essere univocamente associabili ad un nodo. Per questo compito sarebbe opportuno assegnare ad un'ulteriore autorità certificata (o, ancora meglio, ad un insieme di autorità certificate) il compito di creazione e di mantenimento di un'infrastruttura distribuita, ma comune, che funga da *Certificate Authority* (CA), chiamata *Public Key Infrastructure* (PKI) [20].

Di particolare importanza è che la generazione delle coppie di chiavi avvenga esclusivamente a bordo del veicolo, in modo che le chiavi private non escano mai dal device a cui serviranno (in questo caso il veicolo stesso); esse oltre ad essere, come detto, uniche e univoche dovranno avere una data superata la quale non siano più valide e sia necessario generarne di nuove. Il ricambio periodico è un buon modo per limitare eventuali danni dovuti ad attacchi che abbiano avuto successo nel furto della chiave privata; in questo modo il ladro potrà accedere e/o intercettare dati privati solo entro un ristretto lasso di tempo, mantenendo così al sicuro le comunicazioni passate e quelle future (concetto di *Forward Secrecy*). Utilizzando invece un'unica statica chiave per ogni veicolo si renderebbe molto meno costoso – quindi si incentiverebbe – il furto integrale di informazioni non autorizzate.

Nonostante la generazione in locale delle chiavi è però necessario che CA fidate riconoscano ufficialmente le chiavi pubbliche certificandole. Il certificato verrebbe assegnato seguendo uno schema di questo tipo:

$cert_i[pub_i] = pub_i|sig_{pri_{CA_j}}(pub_i|ID_{CA_j})$

Il certificato con cui una CA j vuole riconoscere valore ufficiale alla chiave pubblica pub_i, generata dal veicolo i, è denominato $cert_i$. L'identità della CA è rappresentata invece da ID_{CA_j}. Per apporre con la sua firma lo speciale messaggio $pub_i|ID_{CA_j}$, la CA utilizza la sua chiave privata pri_{CA_j}. Per una più approfondita analisi dell'algoritmo matematico di firma digitale rimando a [20].

Un altro aspetto fondamentale nell'amministrazione delle chiavi, oltre alla loro generazione e verifica, è la revoca. Nonostante la loro natura effimera, è importante procedere subito con una loro revoca se si hanno motivi di pensare che siano state compromesse. Un certificato di revoca non serve solamente al veicolo stesso che poi genererà nuove chiavi, ma è necessario per far sì che anche la PKI e gli altri utenti non comunichino più col veicolo fin tanto che possiede una chiave pubblica compromessa.

Capitolo 7

Conclusioni

Siamo partiti illustrando in breve il concetto di *Internet of things*, delle caratteristiche che possiede e alcune delle sue possibili applicazioni. Una di queste, molto importante, è l'automotive, dove questo nuovo concetto può portare ad una rivoluzione importante.

Abbiamo introdotto quindi i concetti di *Internet of Vehicles* e di *Intelligent Transportation System* e menzionato alcuni degli scenari di utilizzo. Una buona e scalabile comunicazione tra i vari attori è fondamentale, abbiamo quindi parlato di metodi di comunicazione decentralizzati, peer-to-peer e di maniere di indicizzazione dei dati non basate sulla locazione, ma sul contenuto del dato stesso. Sono stati inoltre presentati alcuni esperimenti concreti di supporti alla guida intelligente e autonoma.

La guida autonoma è e sarà una tecnologia che sfrutterà intimamente il concetto di IoV e, dopo averne menzionato le principali tappe storiche, abbiamo parlato delle principali sfide che vanno affrontate per portare all'utilizzo massimo i veicoli senza conducente, sia da un punto di vista tecnologico che da un punto di vista sociale.

Infine, abbiamo illustrato l'importante ambito della sicurezza informatica e della privacy, delle nuove e più rilevanti questioni che una mobilità sempre più interconnessa presenta, di come sia fondamentale impedire che una

tecnologia così potente sia sfruttata per fare danni.

Per il futuro, i problemi da risolvere e le questioni aperte sono ancora molteplici, ma i risultati prodotti sino ad ora sono molto promettenti dal punto di vista tecnologico e la situazione fa pensare che un giorno potremo realisticamente arrivare ad usufruire quotidianamente di questa tecnologia. Il percorso non sarà breve, né improvviso, il passaggio alla guida autonoma sarà molto graduale e richiederà ancora alcuni decenni, ma è probabile che un giorno ripenseremo alla mobilità come la intendiamo oggi (automobile guidata manualmente, mezzo di proprietà, incidenti dovuti ad errori umani, parcheggio, ecc.) come ad un ricordo.

Bibliografia

[1] Apple electric car project. https://en.wikipedia.org/wiki/Apple_electric_car_project.

[2] Autonomous car. https://en.wikipedia.org/wiki/Autonomous_car.

[3] Google self-driving car. https://en.wikipedia.org/wiki/Google_self-driving_car.

[4] Hidden obstacles for google's self-driving cars. https://www.technologyreview.com/s/530276/hidden-obstacles-for-googles-self-driving-cars/.

[5] History of autonomous car. https://en.wikipedia.org/wiki/History_of_autonomous_car.

[6] Intelligent transportation system. https://it.wikipedia.org/wiki/Intelligent_transportation_system.

[7] Internet of things. https://en.wikipedia.org/wiki/Internet_of_Things.

[8] Park shuttle automated driverless vehicle pilot project. https://faculty.washington.edu/jbs/itrans/parkshut.htm.

[9] Proud-car test 2013. http://vislab.it/proud/.

[10] Vamp. https://en.wikipedia.org/wiki/VaMP.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.

[12] G. Dimitrakopoulos. Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 145–151, Aug 2011.

[13] M. Gerla. Vehicular cloud computing. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean*, pages 152–155, June 2012.

[14] M. Gerla, Eun-Kyu Lee, G. Pau, and Uichin Lee. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pages 241–246, March 2014.

[15] Swarun Kumar, Lixin Shi, Nabeel Ahmed, Stephanie Gil, Dina Katabi, and Daniela Rus. Carspeak: A content-centric network for autonomous driving. In *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '12, pages 259–270, New York, NY, USA, 2012. ACM.

[16] K. C. Lee, S. h. Lee, R. Cheung, U. Lee, and M. Gerla. First experience with cartorrent in a real vehicular ad hoc network testbed. In *2007 Mobile Networking for Vehicular Environments*, pages 109–114, May 2007.

[17] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi. Mobeyes: smart mobs for urban monitoring with a vehicular sensor network. *IEEE Wireless Communications*, 13(5):52–57, October 2006.

[18] L. Wang, R. Wakikawa, R. Kuntz, R. Vuyyuru, and L. Zhang. Data naming in vehicle-to-vehicle communications. In *Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on*, pages 328–333, March 2012.

[19] Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, and Rajkumar Buyya. A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, 40:325 – 344, 2014.

[20] G. Yan, D. Wen, S. Olariu, and M. C. Weigle. Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, 14(1):284–294, March 2013.

[21] Y. T. Yu, T. Punihaole, M. Gerla, and M. Y. Sanadidi. Content routing in the vehicle cloud. In *MILITARY COMMUNICATIONS CONFERENCE, 2012 - MILCOM 2012*, pages 1–6, Oct 2012.