Università degli Studi di Torino

Dipartimento di informatica

Tesi di Laurea Triennale in Informatica

Analisi dei Protocolli di Comunicazione nelle applicazioni di sicurezza stradale per veicoli autonomi

Relatore:

Prof: Paolo Castagno

Candidato:

Mirko Vanzetto

ANNO ACCADEMICO 2023/2024

Non c'è niente di più tragico di un talento sprecato.
Puoi avere tutto il talento del mondo, ma se non fai la cosa giusta,
non succede niente.

Abstract

La diffusione delle tecnologie per veicoli autonomi e sistemi Vehicle-to-Everything (V2X) rappresenta una rivoluzione nel settore della mobilità, con l'obiettivo di aumentare la sicurezza stradale e ottimizzare la gestione del traffico. Tuttavia, l'efficacia di tali sistemi dipende in modo critico dalla capacità di comunicare informazioni accurate e in tempo reale tra i diversi attori coinvolti, specialmente in scenari altamente dinamici come l'attraversamento pedonale. Questo studio si concentra sull'analisi della latenza nella disseminazione delle informazioni all'interno di una rete V2X durante un caso di studio che prevede l'interazione tra veicoli autonomi, pedoni e un faro intelligente situato presso un incrocio. Il lavoro è strutturato attorno a diversi protocolli di comunicazione principali: trasmissione diretta tra pedone e veicoli, comunicazione centralizzata mediata dal faro, e approcci distribuiti in cui i veicoli collaborano per condividere le informazioni. Attraverso un emulatore sviluppato con tecnologie come Docker e Tailscale, è stato possibile simulare un ambiente realistico e dinamico in cui veicoli e pedoni si connettono e disconnettono dalla rete in modo intermittente. La simulazione include anche un modello di coda M/M/1 per rappresentare i ritardi di elaborazione e trasmissione, fornendo un'analisi quantitativa delle prestazioni dei diversi protocolli.

I risultati evidenziano l'impatto della latenza di disseminazione sull'accuratezza delle informazioni e sulla sicurezza complessiva del sistema. La valutazione si è focalizzata sul tempo medio di latenza e sulla probabilità di disseminazione di informazioni errate, due metriche fondamentali per determinare l'affidabilità dei protocolli adottati. Inoltre, si discute il ruolo etico delle decisioni prese dai veicoli autonomi in situazioni critiche, come la scelta di dare priorità a un pedone rispetto a un altro sulla base di parametri eticamente discutibili.

Questo lavoro contribuisce alla comprensione delle sfide legate alla progettazione di reti V2X affidabili e fornisce spunti per migliorare la gestione delle comunicazioni in scenari di attraversamento pedonale, con implicazioni dirette per la sicurezza e l'etica dei sistemi di guida autonoma. Le conclusioni offrono una visione integrata delle problematiche tecniche ed etiche, sottolineando la necessità di soluzioni che bilancino prestazioni tecnologiche e responsabilità sociale.

Dichiaro di essere responsabile del contenuto dell'elaborato che presento al fine del conseguimento del titolo, di non avere plagiato in tutto o in parte il lavoro prodotto da altri e di aver citato le fonti originali in modo congruente alle normative vigenti in materia di plagio e di diritto d'autore. Sono inoltre consapevole che nel caso la mia dichiarazione risultasse mendace, potrei incorrere nelle sanzioni previste dalla legge e la mia ammissione alla prova finale potrebbe essere negata.

Indice

Capitolo 1

Introduzione

L'avvento delle auto a guida autonoma rappresenta una delle rivoluzioni tecnologiche più significative del nostro tempo. Questa innovazione promette di trasformare radicalmente il modo in cui viviamo, lavoriamo e ci spostiamo, portando benefici quali la riduzione degli incidenti stradali, l'ottimizzazione del traffico e una maggiore efficienza energetica. Tuttavia, con l'adozione crescente di veicoli autonomi, emergono anche nuove sfide tecniche ed etiche.

In particolare, il problema della sicurezza nei casi di attraversamento pedonale solleva questioni critiche. La capacità delle auto autonome di rilevare e reagire prontamente alla presenza di un pedone rappresenta una sfida non solo tecnologica, ma anche morale. È infatti più grave un errore commesso da un'auto autonoma, dotata di sistemi avanzati con margini di errore minimi, rispetto a un incidente causato da un conducente umano in stato di ebbrezza, la cui probabilità di errore è intrinsecamente più elevata. La corretta comunicazione dei dati tra i diversi attori coinvolti – auto, pedoni e infrastrutture – è cruciale per ridurre al minimo il rischio di incidenti e garantire la sicurezza di tutti gli utenti della strada.

Questa tesi si focalizza sullo scenario di attraversamento pedonale come caso di studio per esplorare e valutare le dinamiche di comunicazione Vehicle-to-Everything. L'obiettivo è analizzare e confrontare differenti protocolli di comunicazione in un contesto dinamico e ad alta variabilità, al fine di comprendere l'impatto della latenza e della disseminazione delle informazioni sulla sicurezza stradale. Inoltre, si affronta la questione dell'accuratezza dei dati trasmessi, valutando il rischio derivante dalla diffusione di informazioni incorrette all'interno della rete.

Capitolo 2

Architettura del Sistema

2.1 Introduzione

L'architettura del sistema rappresenta gli elementi che sono parte del sistema che si vogliono studiare o progettare e definisce ruoli ed interazioni tra vari elementi.
Essa prevede un modello di comunicazione distribuita e centralizzata che coinvolge tre principali entità: il faro, le auto autonome e i pedoni. Queste entità interagiscono all'interno di una rete overlay dedicata, progettata per garantire una comunicazione sicura, scalabile e affidabile in scenari di incrocio stradale e non. L'uso di un'architettura dedicata per ogni incrocio permette di minimizzare la latenza e migliorare l'efficienza della gestione delle comunicazioni.

2.2 Architettura dell'infrastruttura di gestione di un incrocio intelligente

2.2.1 Faro Intelligente (beacon)

Il faro svolge un ruolo cruciale all'interno dell'architettura del sistema, fungendo da nodo centrale che gestisce sia la rete di comunicazione sia il coordinamento tra i vari attori coinvolti, ossia le auto e i pedoni. La sua funzione principale è quella di gestire le comunicazioni tra questi attori, agendo come punto di interfaccia tra le auto in movimento e i pedoni che stanno attraversando la strada. In questo contesto, il faro si occupa anche di raccogliere le richieste di attraversamento inviate dai pedoni, assicurandosi che ogni richiesta venga trattata tempestivamente e con la giusta priorità.

Oltre a raccogliere e smistare le informazioni tra i vari soggetti, il faro è responsabile anche del calcolo delle informazioni necessarie per migliorare le prestazioni generali del sistema, come la latenza media delle comunicazioni tra i veicoli e i pedoni. Questi dati vengono salvati per permettere un'analisi continua del sistema e per ottimizzare il flusso di traffico. Per garantire che il traffico venga gestito in modo efficiente, il faro implementa anche algoritmi di prioritizzazione, i quali stabiliscono l'ordine in cui le comunicazioni devono essere inviate e ricevute, in base alle posizioni dei veicoli, ai tempi di arrivo e alle esigenze di sicurezza del sistema.

Un aspetto fondamentale del faro è l'utilizzo di una coda **M/M/1** [12] per gestire le richieste. La coda M/M/1 è un modello di teoria delle code che prevede:

- **Un unico server**: Il faro gestisce una richiesta alla volta.
- **Arrivi Markoviani**: Le richieste arrivano in modo casuale, seguendo una distribuzione di Poisson.
- **Tempo di servizio esponenziale**: Ogni richiesta richiede un tempo medio di servizio R, con una variabilità intrinseca esponenziale.

Il comportamento esponenziale del ritardo rende il sistema sensibile alla congestione. Quando il numero di richieste aumenta, il tempo medio di attesa W_q nella coda cresce in modo non lineare, ed è dato dalla formula:

$$W_q = \frac{\lambda}{\mu(\mu - \lambda)} \tag{2.1}$$

dove:

- λ è il tasso medio di arrivo delle richieste,
- μ è il tasso medio di servizio (inverso del tempo di servizio R).

Il faro deve affrontare la sfida di bilanciare il traffico delle richieste in modo da evitare congestioni e ritardi eccessivi nel sistema. A tal fine, vengono adottate diverse strategie di ottimizzazione. Una delle principali tecniche utilizzate è l'impiego di code a priorità, che consente di gestire le richieste più urgenti prima di altre, assicurando che le situazioni critiche vengano trattate tempestivamente. Inoltre, per distribuire equamente il carico di rete, il sistema può fare ricorso al load balancing, ossia l'assegnazione delle richieste a più fari, in modo da evitare il sovraccarico di un singolo nodo. Infine, vengono utilizzati modelli predittivi che permettono di stimare in anticipo il carico di rete, ottimizzando la gestione delle richieste e garantendo che il sistema rimanga reattivo e scalabile anche sotto carichi elevati.

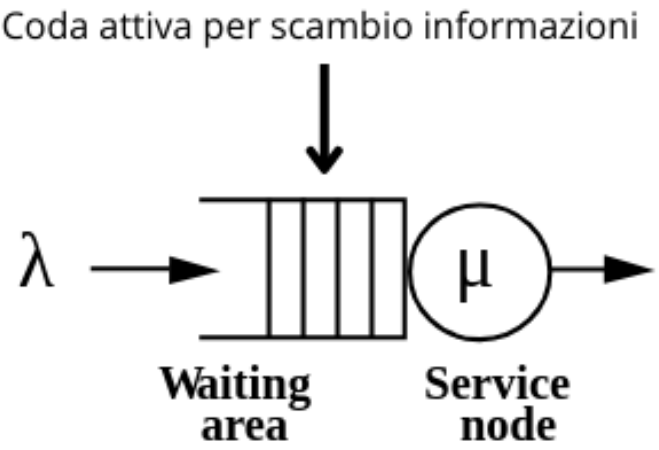

Figura 2.1: Rappresentazione grafica della coda M/M/1 utilizzata dal faro per la gestione delle richieste. Fonte: [3].

2.2.2 Auto Autonome

Le auto autonome svolgono un ruolo fondamentale nel sistema, fungendo da nodi mobili che interagiscono non solo con il faro, ma anche, in alcuni casi, direttamente tra di loro. La loro principale responsabilità consiste nella ricezione delle notifiche inviate dal faro, come ad esempio l'avviso della presenza di pedoni. Queste informazioni permettono alle auto di adattarsi tempestivamente all'ambiente circostante. Inoltre, le auto sono responsabili di comunicare il loro stato al faro, fornendo aggiornamenti relativi alla loro posizione, velocità e altri parametri rilevanti, al fine di mantenere la rete sempre aggiornata.

Le auto autonome devono anche reagire prontamente agli eventi in tempo reale, come fermarsi per consentire l'attraversamento dei pedoni o rispettare le precedenze in base alle regole del traffico. In scenari critici, le auto possono comunicare direttamente tra loro, riducendo la dipendenza dal faro e garantendo una risposta più rapida in caso di emergenza. Inoltre, l'adozione di protocolli di emergenza consente alle auto di continuare a operare in modo sicuro anche in caso di guasti alla rete principale, assicurando che la sicurezza degli utenti della strada non venga compromessa in nessuna circostanza.

2.2.3 Pedone

Il pedone rappresenta una figura vulnerabile all'interno dell'architettura, ma il suo ruolo è cruciale per garantire la sicurezza stradale. Una delle sue funzioni principali è l'invio delle richieste di attraversamento al faro, che segnala la sua intenzione di attraversare la strada. A seconda del tipo di protocollo in uso, il pedone può anche comunicare direttamente con le auto, trasmettendo informazioni vitali per la sua sicurezza.

Prima di procedere nell'attraversamento, il pedone riceve conferme o notifiche dal faro, che gli indicano quando è sicuro attraversare. In alcuni scenari, il pedone può anche interagire con altri pedoni per scambiarsi informazioni sulla situazione del traffico o sulla sicurezza dell'attraversamento, rafforzando così la cooperazione tra le diverse entità presenti nell'ecosistema di traffico e sicurezza stradale.

2.2.4 Overlay Network

L'overlay network rappresenta l'infrastruttura fondamentale che consente la comunicazione tra tutte le entità coinvolte nel sistema, inclusi il faro, le auto e i pedoni. Ogni incrocio stradale è dotato di una rete overlay dedicata, progettata per rispondere a specifiche esigenze di comunicazione tra i vari nodi. Una delle principali caratteristiche di questa rete è la **scalabilità**, che consente di gestire un numero variabile di nodi, come le auto e i pedoni, senza compromettere la qualità del servizio. Questo permette alla rete di adattarsi dinamicamente alle variazioni nel numero di entità in movimento, mantenendo alta l'efficienza delle comunicazioni.

Un altro elemento cruciale è la **sicurezza**: l'uso di protocolli di rete sicuri garantisce che le informazioni sensibili, come la posizione delle auto e le richieste di attraversamento dei pedoni, siano protette da accessi non autorizzati. Questo livello di sicurezza è essenziale per prevenire potenziali attacchi e garantire la privacy delle comunicazioni tra i vari attori. Infine, la **affidabilità** dell'overlay network è assicurata dalla sua progettazione con ridondanza integrata, che permette di minimizzare i rischi legati alla perdita di informazioni causata da disconnessioni temporanee o malfunzionamenti dei nodi, garantendo una comunicazione continua e stabile.

Figura 2.2: Rappresentazione grafica dell'overlay network applicato ad incroci con fari.

Tuttavia, in scenari extraurbani o in contesti privi di infrastrutture stradali avanzate, le auto possono comunicare direttamente tra loro senza la necessità di un faro centrale. In queste situazioni, ogni veicolo agisce come nodo della rete, scambiando informazioni con i veicoli vicini per gestire autonomamente le interazioni e le precedenze. Una delle principali caratteristiche di questa configurazione è la **comunicazione peer-to-peer**, che consente alle auto di utilizzare protocolli di rete diretti per inviare e ricevere dati in tempo reale, senza la necessità di intermediari. Questo approccio riduce la dipendenza da un'infrastruttura centrale e permette alle auto di comunicare in modo efficiente anche in ambienti con limitata connettività.

Inoltre, la rete è in grado di adattarsi dinamicamente alle condizioni del traffico e alla densità veicolare, creando connessioni temporanee tra veicoli vicini. Questo tipo di **gestione dinamica della rete** assicura che ogni auto possa ricevere e inviare informazioni pertinenti in base alla sua posizione e al flusso del traffico, migliorando la reattività del sistema in tempo reale. Infine, in assenza di un faro, le auto si affidano a una **affidabilità decentralizzata** tramite l'uso di algoritmi distribuiti che permettono di evitare collisioni e di garantire un flusso di traffico sicuro, mantenendo comunque l'efficienza e la sicurezza nelle interazioni tra i veicoli.

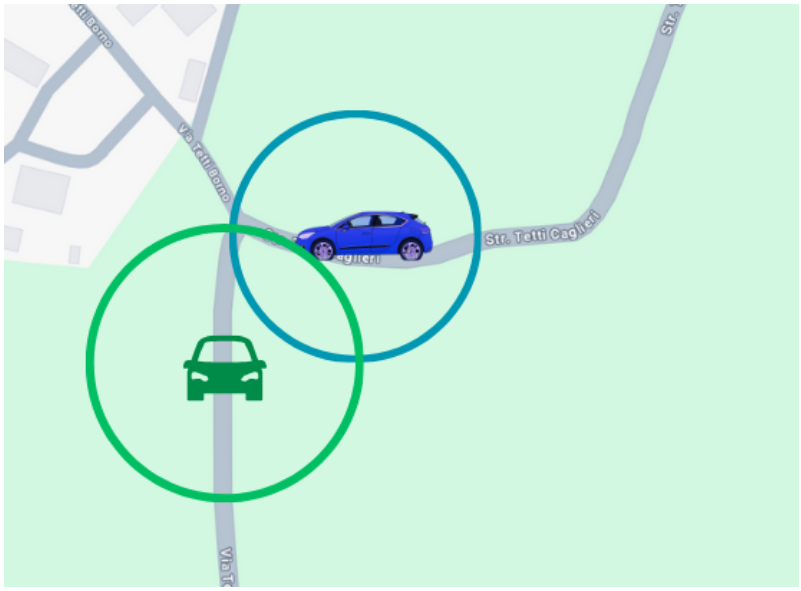

Figura 2.3: Rappresentazione grafica dell'overlay network in contesti senza faro, con comunicazione diretta tra veicoli.

La rete overlay è progettata per essere isolata per ogni incrocio, ma anche interconnessa all'interno di una rete più ampia, in cui le auto possono migrare tra diverse reti overlay senza perdere la capacità di comunicare tra loro.

2.2.5 Relazioni tra le Entità

Le relazioni tra faro, auto e pedoni all'interno dell'overlay network si sviluppano in un contesto collaborativo e dinamico. Il **faro** assume il ruolo di coordinatore centrale, raccogliendo informazioni sia dalle auto che dai pedoni per gestire le comunicazioni in modo efficace e tempestivo. **Le auto**, da parte loro, inviano periodicamente dati al faro, aggiornando lo stato della rete, e reagiscono ai comandi ricevuti per adattarsi alle condizioni del traffico o per rispondere a situazioni di emergenza.

I **pedoni**, sebbene interagiscano principalmente con il faro per inviare le richieste di attraversamento e ricevere notifiche, in alcuni protocolli avanzati possono anche comunicare direttamente con le auto, migliorando così l'efficienza della gestione del traffico in scenari specifici. Infine, la **rete overlay** gioca un ruolo cruciale nel garantire la ridondanza e la resilienza del sistema. Questa architettura consente agli incroci di funzionare autonomamente, mantenendo l'affidabilità delle comunicazioni anche in presenza di guasti o disconnessioni temporanee. ete overlay garantisce ridondanza e resilienza, permettendo agli incroci di funzionare autonomamente.

Nota bibliografica: Per ulteriori informazioni sulle reti overlay e sulle code M/M/1, si rimanda a [8, 12].

Capitolo 3

Applicazione in Campo Reale

3.1 Introduzione

L'implementazione del sistema di comunicazione V2X in un contesto reale richiede un'infrastruttura solida e scalabile, capace di gestire un'elevata quantità di veicoli, pedoni e incroci in tempo reale. Questo capitolo analizza come ogni auto, pedone e infrastruttura stradale possa interagire all'interno di una rete globale, garantendo sicurezza, affidabilità e interoperabilità tra le diverse entità.

3.2 Struttura della Rete e Identificativi dei Veicoli

Per garantire un funzionamento sicuro ed efficiente, ogni veicolo deve essere dotato di un *identificativo univoco (UUID)* che consente di riconoscerlo all'interno della rete. Inoltre, il sistema utilizza *chiavi crittografiche e certificati digitali* per autenticare ogni dispositivo e prevenire accessi non autorizzati.

- Ogni auto riceve una chiave di accesso per connettersi alla rete V2X.
- Gli incroci e i fari intelligenti verificano la validità della chiave prima di permettere la comunicazione.
- L'infrastruttura supporta l'aggiornamento dinamico delle chiavi per mantenere la sicurezza nel tempo.

Questa strategia consente di creare una rete autenticata e sicura, riducendo il rischio di attacchi informatici e garantendo che solo entità verificate possano accedere al sistema.

3.2.1 Gestione delle Overlay Network

L'architettura proposta si fonda su una rete globale V2X, che è suddivisa in overlay network locali. Ogni overlay network locale è dedicato alla gestione di un incrocio o di una specifica area della strada, con l'obiettivo di ottimizzare le comunicazioni e garantire la sicurezza. In questo scenario, ogni incrocio funziona come una rete isolata, gestita da un faro intelligente che coordina le comunicazioni tra tutti gli attori coinvolti. La rete è progettata per essere dinamica e flessibile: le auto possono entrare e uscire dalle diverse reti overlay senza compromettere la loro capacità di

comunicare. Questo consente un flusso continuo di informazioni anche quando i veicoli si spostano da un incrocio all'altro.

Inoltre, quando le auto si trovano nelle vicinanze, è possibile che queste comunichino direttamente tra loro, riducendo così la dipendenza dai fari e migliorando l'efficienza della rete. Questa comunicazione peer-to-peer contribuisce a una gestione del traffico più fluida e a una riduzione dei tempi di attesa, aumentando la sicurezza in tempo reale.

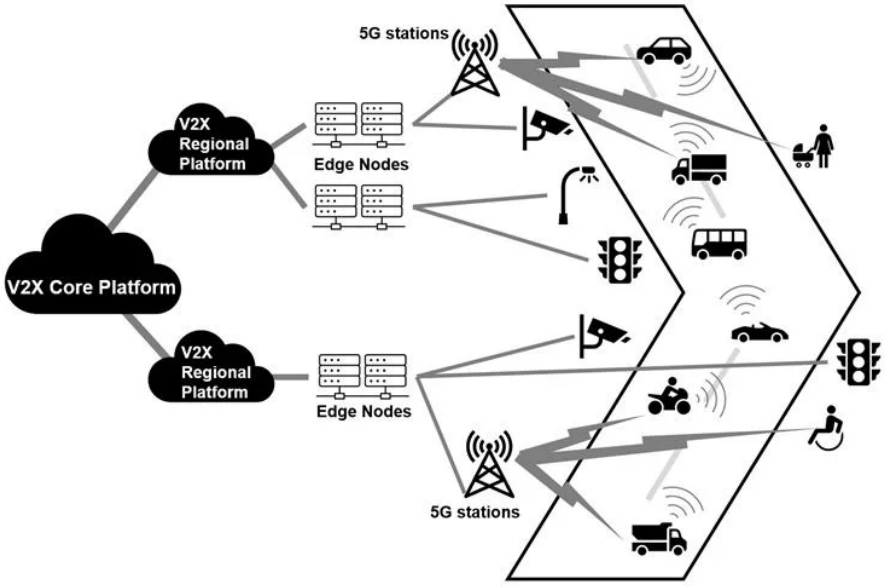

Figura 3.1: Schema della rete globale V2X [7].

3.2.2 Comunicazione tra Auto, Pedoni e Incroci

Uno degli aspetti più innovativi dell'implementazione proposta è l'integrazione dei pedoni nella rete V2X. Questo obiettivo viene raggiunto attraverso diverse tecnologie, tra cui dispositivi mobili o wearable in grado di trasmettere la posizione del pedone e l'intenzione di attraversare. Tali dispositivi permettono al pedone di inviare informazioni rilevanti, che vengono raccolte dalla rete e utilizzate per garantire un attraversamento sicuro. Inoltre, sensori stradali posizionati lungo il percorso dei pedoni possono rilevare la loro presenza e comunicare direttamente con le auto in avvicinamento, avvisando i conducenti della situazione.

La rete consente anche un'interazione diretta tra i pedoni e i veicoli autonomi. Questo è particolarmente utile in scenari complessi, dove la gestione dell'interazione tra pedoni e auto è cruciale per garantire la sicurezza. Ad esempio, i veicoli autonomi possono ricevere informazioni in tempo reale sulle intenzioni di attraversamento dei pedoni e fermarsi di conseguenza, evitando potenziali incidenti.

Un altro aspetto fondamentale della rete è la gestione della priorità per i veicoli speciali, come le ambulanze o altri mezzi di emergenza. La rete V2X consente a questi veicoli di ricevere priorità in caso di necessità, grazie a protocolli di priorità implementati all'interno delle overlay network. Questo permette una gestione ottimale del traffico in situazioni critiche, riducendo i tempi di intervento e garantendo una risposta più rapida in caso di emergenza.

3.3 Sicurezza e Resilienza della Rete

Per garantire l'affidabilità e la sicurezza della rete, sono stati implementati diversi livelli di protezione. In primo luogo, la **crittografia end-to-end** è utilizzata per proteggere le comunicazioni tra veicoli e infrastrutture. Questo meccanismo assicura che le informazioni scambiate tra i nodi della rete siano cifrate, impedendo a eventuali attaccanti di intercettare o manipolare i dati in transito. La crittografia garantisce la riservatezza e l'integrità delle informazioni sensibili, come la posizione dei veicoli e le intenzioni di attraversamento dei pedoni, assicurando che solo i destinatari autorizzati possano accedere ai dati.

In aggiunta, è stato previsto un sistema di **rilevamento delle intrusioni**, progettato per identificare tempestivamente eventuali tentativi di accesso non autorizzato alla rete. Questo sistema monitora costantemente l'attività sulla rete e segnala comportamenti sospetti, permettendo una rapida risposta in caso di minacce. L'introduzione di questo strato di protezione aiuta a prevenire attacchi da parte di attori maligni che potrebbero compromettere la funzionalità della rete o compromettere la sicurezza delle comunicazioni.

Infine, la **resilienza del sistema** è garantita tramite **failover e ridondanza**, che assicurano che la rete continui a funzionare anche in caso di guasti o disconnessioni di alcuni dei suoi componenti. La ridondanza è progettata per garantire che, in caso di malfunzionamenti hardware o interruzioni nelle comunicazioni, il sistema possa rimanere operativo, reindirizzando automaticamente il traffico verso percorsi alternativi. Questo approccio riduce al minimo il rischio di interruzioni del servizio e aumenta la continuità operativa della rete.

In sintesi, queste misure di sicurezza e resilienza sono fondamentali per garantire che il sistema possa operare in modo continuo e affidabile, proteggendo le comunicazioni e minimizzando i rischi di compromissione della sicurezza. La combinazione di crittografia, rilevamento delle intrusioni e failover contribuisce a rendere la rete sicura e resistente a minacce esterne e guasti interni.

Nota bibliografica: Per un approfondimento sull'implementazione della tecnologia V2X nelle infrastrutture urbane, si rimanda a [8, 10, 16].

3.4 Aspetti Etici e Difficoltà Sociali

L'implementazione di veicoli autonomi e sistemi di comunicazione V2X solleva numerose questioni etiche e sociali che devono essere affrontate prima di un'adozione su larga scala. Sebbene la tecnologia offra enormi potenziali benefici, tra cui la riduzione degli incidenti stradali e un traffico più efficiente, vi sono anche implicazioni morali, legali e sociali che necessitano di un'analisi approfondita.

3.4.1 Dilemmi Etici nell'Automazione Stradale

Uno degli aspetti più complessi legati all'introduzione dei veicoli autonomi riguarda la gestione delle situazioni di emergenza, in cui questi veicoli devono prendere decisioni che potrebbero coinvolgere vite umane. Tra i principali dilemmi etici, uno dei più discussi è la **scelta tra vite umane**. In scenari inevitabili, come in situazioni di frenata d'emergenza, l'auto potrebbe trovarsi di fronte alla necessità di scegliere tra investire un pedone o mettere a rischio i passeggeri a bordo. La domanda che sorge è: quale decisione dovrebbe prendere un'auto autonoma in tali circostanze? Questa scelta dipenderebbe da fattori morali, giuridici e tecnologici che necessitano di un'attenta considerazione.

Un altro dilemma riguarda la **valutazione morale degli individui**. In base ai dati raccolti, un sistema di intelligenza artificiale potrebbe teoricamente decidere chi salvare in base a fattori come età, stato di salute o conformità alle norme stradali. Ma è giusto che un algoritmo, e non un essere umano, prenda queste decisioni vitali? Questo solleva preoccupazioni etiche sul ruolo dell'intelligenza artificiale nelle scelte morali, specialmente in scenari ad alto rischio.

Un'ulteriore questione riguarda la **responsabilità legale**. Se un'auto autonoma è coinvolta in un incidente, chi è responsabile? È il produttore del veicolo, il programmatore che ha scritto il software, o il proprietario del veicolo? La mancanza di una chiara definizione delle responsabilità giuridiche in questi casi potrebbe portare a complicazioni legali e incertezze su chi dovrebbe rispondere in caso di danni.

Questi dilemmi etici richiedono un ampio dibattito pubblico, regolamenti chiari e un aggiornamento continuo delle normative, per evitare ambiguità giuridiche e garantire che la tecnologia venga utilizzata in modo equo e responsabile.

3.4.2 Accettazione Sociale e Fiducia nella Tecnologia

Nonostante i rapidi progressi tecnologici, la società potrebbe non essere ancora completamente pronta ad accettare l'introduzione dei veicoli autonomi e dei sistemi V2X. Un ostacolo significativo è la **diffidenza nella tecnologia**. Le persone potrebbero essere riluttanti a fidarsi di un sistema automatizzato che gestisce la propria sicurezza stradale. La paura che la tecnologia possa fallire in situazioni critiche o che non possa prendere decisioni adeguate in tempo reale potrebbe rallentare l'adozione su larga scala.

Un altro fattore che potrebbe influenzare l'accettazione della tecnologia è la **disparità di accesso alla tecnologia**. Sebbene i veicoli autonomi possano apportare significativi benefici in termini di sicurezza e efficienza, l'adozione di massa potrebbe creare una divisione tra chi può permettersi veicoli autonomi e chi è costretto a dipendere dai mezzi di trasporto tradizionali. Questa disuguaglianza potrebbe accentuare

il divario socioeconomico, limitando i benefici della tecnologia a determinate fasce della popolazione.

Inoltre, la **resistenza normativa** è un altro ostacolo importante. Molti paesi hanno leggi obsolete che non contemplano la guida autonoma, il che rallenta l'adozione di questi sistemi. Le normative attuali potrebbero non essere adeguate a gestire le complessità legate ai veicoli autonomi, creando incertezze legali e regolamentari. La necessità di aggiornare e armonizzare le leggi a livello globale è cruciale per una transizione efficace verso la mobilità autonoma.

3.4.3 Impatto sul Lavoro e sull'Economia

L'introduzione di veicoli autonomi potrebbe avere un impatto significativo sul mercato del lavoro, specialmente nei settori dei trasporti e della logistica. Da un lato, l'automazione potrebbe comportare una **perdita di posti di lavoro**. Ad esempio, i conducenti di taxi, camionisti e addetti alla logistica potrebbero essere sostituiti da sistemi automatizzati, creando disoccupazione in alcuni settori. Questo fenomeno potrebbe richiedere interventi in ambito formativo e di riqualificazione professionale per mitigare gli effetti negativi sull'occupazione.

D'altro canto, la diffusione della tecnologia potrebbe anche generare **nuove opportunità lavorative**. L'adozione dei veicoli autonomi aumenterà la domanda di ingegneri software, esperti di intelligenza artificiale, e tecnici specializzati nella manutenzione dei veicoli autonomi. Questi nuovi lavori potrebbero rispondere a un bisogno crescente di competenze tecniche avanzate, stimolando la crescita di nuovi settori industriali.

Tuttavia, l'adozione di veicoli autonomi potrebbe comportare anche **costi elevati**, limitando inizialmente l'accesso a queste tecnologie. Le grandi aziende e i consumatori con disponibilità economiche superiori potrebbero essere i primi a beneficiare della tecnologia, mentre piccole imprese e individui meno abbienti potrebbero rimanere esclusi, aggravando il divario socioeconomico.

3.4.4 Regolamentazione e Normative Future

Per garantire un'implementazione etica e socialmente sostenibile della tecnologia, è necessario sviluppare normative adeguate che affrontino diverse questioni cruciali. Una priorità è la definizione di **standard di sicurezza obbligatori** per i veicoli autonomi. Questi standard dovrebbero stabilire requisiti tecnici minimi per garantire che i veicoli autonomi operino in sicurezza in ogni scenario, proteggendo la vita degli utenti della strada e prevenendo incidenti.

Un altro punto cruciale riguarda la **regolamentazione delle responsabilità** in caso di incidente. È fondamentale definire chiaramente chi sia legalmente responsabile quando un'auto autonoma è coinvolta in un incidente, sia essa il produttore, il programmatore o il proprietario del veicolo. Senza regole chiare, potrebbero sorgere conflitti legali che ostacolano l'adozione e l'integrazione della tecnologia.

Inoltre, è necessario creare **framework normativi** che garantiscano che l'intelligenza artificiale prenda decisioni conformi ai principi etici. Questo implica la creazione di linee guida su come i veicoli autonomi dovrebbero comportarsi in situazioni morali complesse, come quelle legate alla scelta tra vite umane, garantendo che l'IA rispetti valori condivisi dalla società.

Infine, le normative dovrebbero includere misure per ridurre il **divario sociale** nell'accesso alla tecnologia, garantendo che i benefici dei veicoli autonomi siano distribuiti in modo equo, senza escludere le fasce più vulnerabili della popolazione.

3.4.5 Conclusione

L'adozione di veicoli autonomi e della tecnologia V2X può portare benefici significativi in termini di sicurezza stradale ed efficienza del traffico. Tuttavia, per garantire una transizione equa e sostenibile, è fondamentale affrontare le implicazioni etiche e sociali di questa rivoluzione tecnologica. Un dibattito interdisciplinare tra ingegneri, eticisti, legislatori e la società civile sarà essenziale per costruire un futuro in cui l'automazione stradale sia accettata e regolamentata in modo responsabile.
Nota bibliografica: Per un approfondimento sui dilemmi etici dell'intelligenza artificiale nei trasporti autonomi, si rimanda a [13, 1, 5].

Capitolo 4

Protocolli di Comunicazione

4.1 Introduzione

L'efficacia della gestione del traffico in un ambiente di veicoli autonomi dipende fortemente dalla capacità di comunicazione tra le entità coinvolte. In questo contesto, i protocolli di comunicazione rappresentano la base per garantire un'interazione efficiente tra pedoni, veicoli e infrastrutture stradali. L'obiettivo principale è minimizzare i tempi di latenza, migliorare la sicurezza dell'attraversamento e garantire l'affidabilità delle informazioni trasmesse.

I protocolli di comunicazione adottati in questo studio si suddividono in due principali categorie:

- **Trasmissione diretta**: la comunicazione avviene direttamente tra il pedone e le auto, con un intervento limitato del faro per la raccolta delle informazioni iniziali.
- **Comunicazione centralizzata**: il faro agisce da intermediario, gestendo la comunicazione tra il pedone e le auto in maniera sequenziale.

L'analisi dei protocolli segue una progressione logica, partendo da soluzioni semplici e passando gradualmente a schemi più sofisticati, che introducono nuove problematiche e soluzioni per gestire la comunicazione in un ambiente reale. Inizialmente, il pedone comunica direttamente con le auto, con una latenza minima ma senza garanzie di affidabilità. Successivamente, il faro viene introdotto come nodo centrale, migliorando la coordinazione ma aumentando la latenza dovuta alla gestione delle code. Infine, i protocolli più avanzati cercano di bilanciare efficienza e affidabilità, adottando modelli di comunicazione distribuita o ibrida.

Le sezioni seguenti analizzano nel dettaglio i protocolli implementati, evidenziandone il funzionamento, le metriche di valutazione e le problematiche riscontrate.

4.2 Protocollo 1: Direct Transmission

4.2.1 Descrizione del Protocollo

Il **Protocollo Direct Transmission** prevede una comunicazione diretta tra il pedone e le auto, mediata inizialmente dal faro per la sola fase di raccolta degli indirizzi IP. Una volta ottenuti gli IP, il pedone comunica direttamente con le auto in arrivo per segnalare l'inizio e la fine dell'attraversamento.

Il faro utilizza una coda **M/M/1** [12] per processare le richieste di IP, introducendo un ritardo cumulativo proporzionale al numero di auto presenti. Questo tipo di coda è caratterizzato da un tempo di servizio esponenziale, il che significa che all'aumentare del numero di auto nella rete, il ritardo cresce rapidamente, potenzialmente generando congestione e rallentamenti nel sistema.

L'attesa attiva dovuta al recupero delle informazioni da parte del faro prima della comunicazione introduce un ritardo complessivo pari a:

$$T = R \cdot N \tag{4.1}$$

dove:

- N è il numero di auto presenti nella rete,
- R è il ritardo medio per comunicazione, il quale varia in funzione del livello di congestionamento della coda del faro.

La prima auto riceve il messaggio a:

$$T = R \cdot N + R \tag{4.2}$$

Nota bibliografica: Per un'analisi più dettagliata sulle code **M/M/1**, si rimanda a [12].

4.2.2 Funzionamento

Il funzionamento del protocollo può essere descritto come segue:

1. Il pedone comunica la sua presenza al faro.
2. Il faro recupera gli indirizzi IP delle auto presenti in rete:
   - A $t = 0$, il faro comunica con l'auto 1 (tempo $t = R$).
   - A $t = R$, comunica con l'auto 2 (tempo $t = R$).
   - A $t = (N - 1)R$, comunica con l'auto N.
3. Il faro restituisce l'elenco degli IP al pedone.
4. Il pedone comunica direttamente con le auto:
   - Invia un segnale di "inizio attraversamento" in broadcast.
   - Invia un segnale di "fine attraversamento" al termine.

4.2.3 Schema del Protocollo

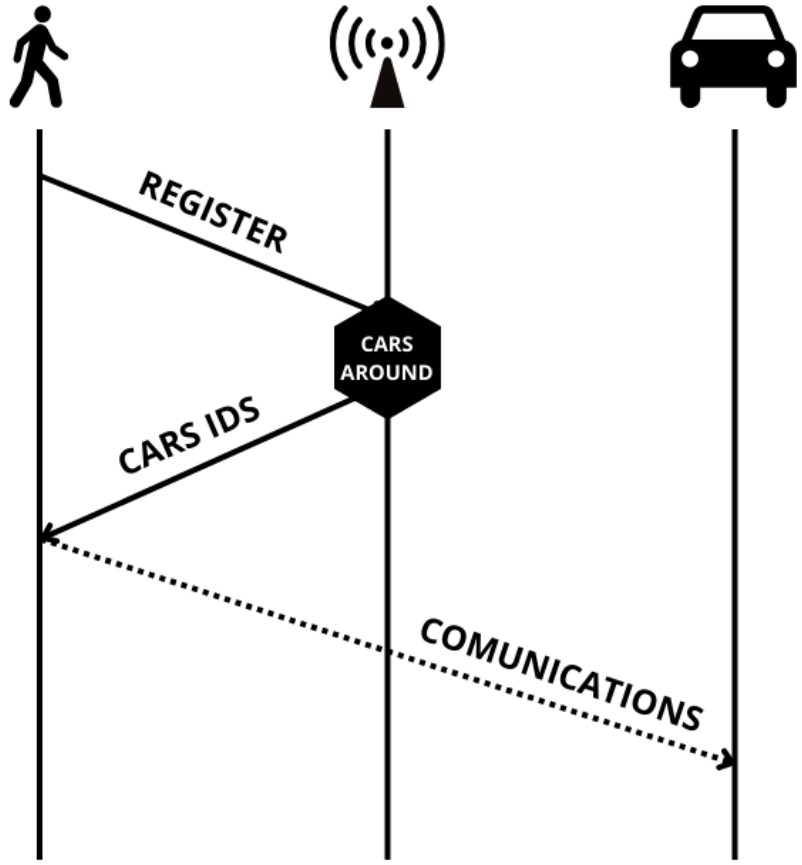

Figura 4.1: Schema del funzionamento del Protocollo 1.

4.2.4 Schema Dettagliato del Protocollo di Attraversamento

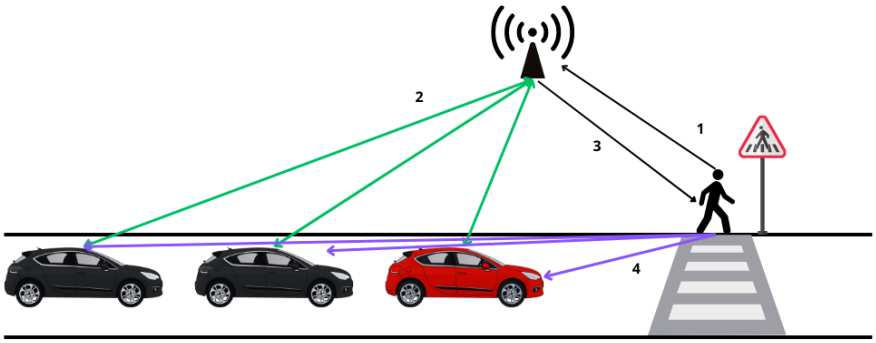

Figura 4.2: Schema del Protocollo di Attraversamento 1.

4.2.5 Problemi Identificati

Il protocollo presenta i seguenti problemi:

- **Latenza elevata**: Il tempo di attesa per ottenere gli IP è proporzionale al numero di auto nella rete. Questo significa che, in scenari con un elevato numero di veicoli, il pedone potrebbe dover attendere un tempo significativo prima che la comunicazione avvenga, riducendo l'efficacia del protocollo.
- **Congestione della rete**: Poiché il faro gestisce ogni richiesta individualmente e in sequenza, un aumento del numero di auto può portare a una saturazione della coda, aumentando il ritardo totale del sistema.
- **Informazioni obsolete**: Le auto che entrano nella rete dopo la fase di raccolta degli IP non vengono incluse nella comunicazione del pedone. Questo può portare a situazioni in cui un'auto, che non è stata informata della presenza del pedone, continua a muoversi, aumentando il rischio di collisione.

4.2.6 Formula della Latenza

La latenza totale del protocollo è calcolata come:

$$T = N \cdot R + R \tag{4.3}$$

dove:

- N è il numero di auto nella rete.
- R è il ritardo medio per comunicazione.

L'aumento della latenza con il numero di auto evidenzia un problema di scalabilità: in un ambiente urbano con un elevato numero di veicoli autonomi, il protocollo può risultare inefficace. Inoltre, il ritardo aggiuntivo per ogni richiesta, derivante dall'accodamento, può portare a tempi di reazione troppo lunghi per garantire un attraversamento sicuro ed efficiente.

4.3 Protocollo 2: Comunicazione da parte del faro

4.3.1 Descrizione del Protocollo

Il **Protocollo 2** introduce un primo livello di centralizzazione della comunicazione, rispetto alla trasmissione diretta del Protocollo 1. In questo caso, il pedone, arrivato all'attraversamento, comunica la propria presenza al faro e ne segnala l'intenzione di attraversare. Il faro, che mantiene un registro delle auto attive nella rete e del loro ordine di arrivo, si occupa di inoltrare l'informazione alle auto una per volta.

L'introduzione di un nodo centrale migliora la gestione della comunicazione, riducendo il rischio che alcuni veicoli non ricevano il segnale del pedone. Tuttavia, questo approccio comporta un incremento della latenza, poiché la trasmissione avviene in modo sequenziale. Il faro utilizza una coda di gestione in ordine **FIFO** (First-In, First-Out) [12] per elaborare le comunicazioni con i veicoli.

Il tempo totale di comunicazione risulta essere:

$$T = R \cdot (N - 1) + R \tag{4.4}$$

dove:

- N è il numero totale di auto in attesa della comunicazione.
- R è il ritardo medio di trasmissione del messaggio.

La comunicazione sequenziale introduce un ritardo cumulativo: se il tempo di trasmissione medio R è elevato e il numero di auto N cresce, il sistema può diventare poco reattivo, con un impatto significativo sulla fluidità del traffico.

4.3.2 Funzionamento

Il protocollo segue i seguenti passaggi:

1. A $t = 0$, il pedone comunica al faro la sua presenza e volontà di attraversare.

2. A $t = 0$, il faro comunica con la prima auto in coda (tempo di trasmissione $t = R$).

3. A $t = R$, il faro comunica con la seconda auto (tempo di trasmissione $t = R$).

4. Il processo continua fino a raggiungere l'ultima auto presente nella rete.

L'utilizzo di una coda FIFO assicura che le auto vengano informate nell'ordine in cui sono entrate nella rete, ma aumenta il tempo necessario per notificare tutti i veicoli.

4.3.3 Schema del Protocollo

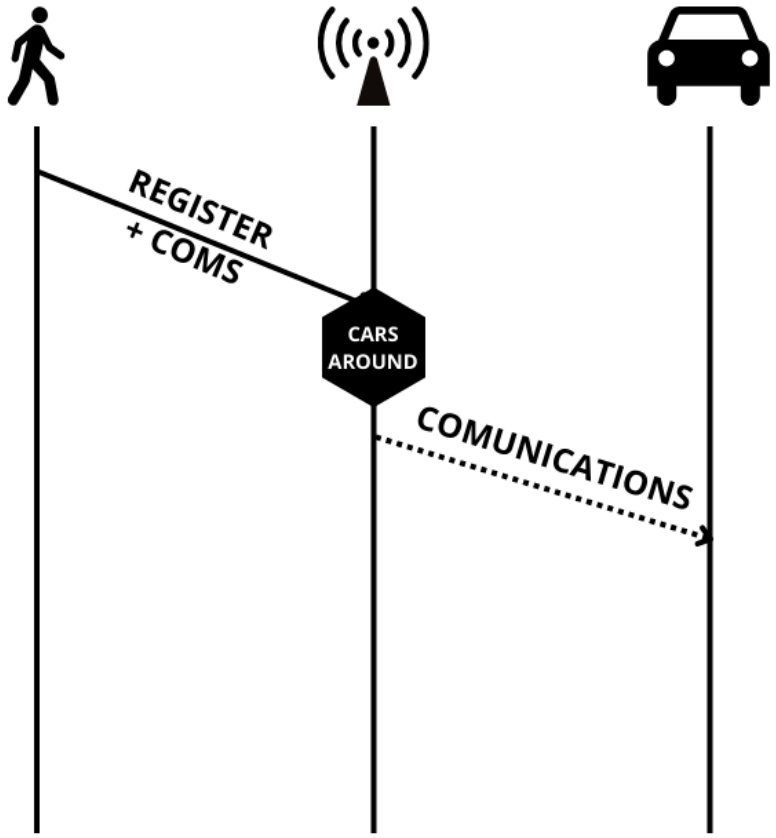

Figura 4.3: Schema del funzionamento del Protocollo 2.

4.3.4 Schema Dettagliato del Protocollo di Attraversamento

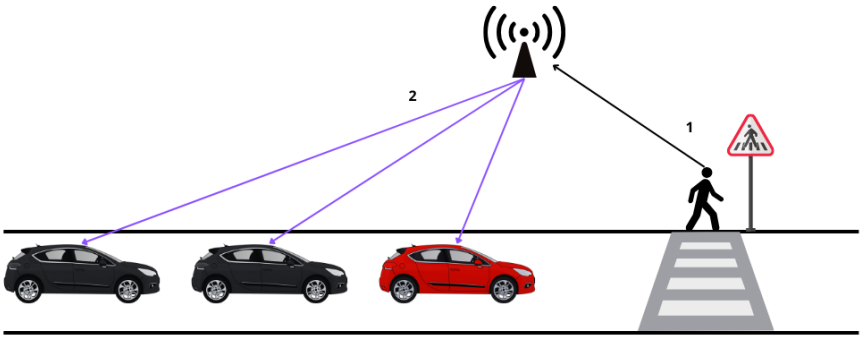

Figura 4.4: Schema del Protocollo di Attraversamento 2.

4.3.5 Problemi Identificati

Il protocollo presenta le seguenti criticità:

- **Ritardo proporzionale al numero di auto**: Poiché la comunicazione avviene in modo sequenziale, la latenza totale è proporzionale a N. Se il numero di auto è elevato, il tempo necessario per informare tutti i veicoli può superare i tempi di reazione ideali per evitare incidenti.
- **Dipendenza dalla coda**: L'accumulo di richieste nel faro può portare a un aumento del tempo di attesa per ogni auto. Se il sistema è congestionato, il tempo di elaborazione di ogni richiesta può aumentare ulteriormente, amplificando il problema.
- **Possibile perdita di sincronia**: Se un'auto entra nella rete dopo che il faro ha iniziato la trasmissione della sequenza, potrebbe non ricevere il messaggio di avviso dell'attraversamento, generando potenziali rischi per la sicurezza del pedone.

Questi problemi emergono dalla centralizzazione della comunicazione nel faro. Se da un lato questo garantisce che ogni auto riceva l'informazione, dall'altro introduce un collo di bottiglia nella trasmissione, rallentando il sistema all'aumentare del numero di auto. Il protocollo funziona bene in scenari con un numero limitato di veicoli, ma potrebbe risultare inefficiente in condizioni di traffico intenso.

4.3.6 Formula della Latenza

Il tempo totale necessario per notificare tutte le auto è:

$$T = (N - 1) \cdot R + R \tag{4.5}$$

dove:

- N è il numero di auto nella rete.
- R è il ritardo medio di trasmissione per ogni comunicazione.

Rispetto al Protocollo 1, questo schema garantisce che tutte le auto ricevano l'informazione, evitando il problema delle **informazioni obsolete**. Tuttavia, la latenza più elevata può compromettere l'efficacia del sistema in scenari reali con un elevato numero di veicoli.

4.4 Protocollo 3: Comunicazione Diretta Auto-Auto

4.4.1 Descrizione del Protocollo

Il **Protocollo 3** introduce un modello di comunicazione completamente distribuito, eliminando la necessità di un nodo centrale come il faro. In questo scenario, il pedone interagisce direttamente con la prima auto in arrivo utilizzando una connessione wireless a corto raggio, come il **Bluetooth** o protocolli V2X basati su **Dedicated Short-Range Communications (DSRC)** [11]. L'auto che riceve il segnale dal pedone diventa responsabile della propagazione dell'informazione alle altre auto nella rete locale.

Questa soluzione rappresenta un'evoluzione significativa rispetto ai protocolli precedenti: mentre il **Protocollo 1** soffriva di problemi di latenza a causa della raccolta IP gestita dal faro e il **Protocollo 2** introduceva un ritardo sequenziale dovuto alla trasmissione centralizzata, il Protocollo 3 elimina il collo di bottiglia del faro e sfrutta un modello **auto-auto (V2V, Vehicle-to-Vehicle)**. Le auto mantengono costantemente una tabella locale aggiornata con lo stato delle altre vetture nella loro zona, permettendo una trasmissione dell'informazione in parallelo.

4.4.2 Funzionamento

Il protocollo segue i seguenti passaggi:

1. Il pedone arriva all'attraversamento e comunica via wireless (es. Bluetooth, DSRC) con la prima auto in arrivo.

2. L'auto 1 riceve il segnale e lo trasmette immediatamente alle altre auto vicine utilizzando la comunicazione diretta V2V.

3. Poiché le auto condividono costantemente informazioni sul traffico tra loro, ciascuna auto aggiorna il proprio stato e si ferma se necessario.

4. Al termine dell'attraversamento, l'auto 1 trasmette il segnale di completamento alle altre auto, che possono riprendere il movimento.

L'assenza di un nodo centrale permette alle auto di aggiornarsi tra loro in tempo reale, riducendo drasticamente il ritardo nella trasmissione dell'informazione rispetto ai protocolli precedenti.

4.4.3 Schema del Protocollo

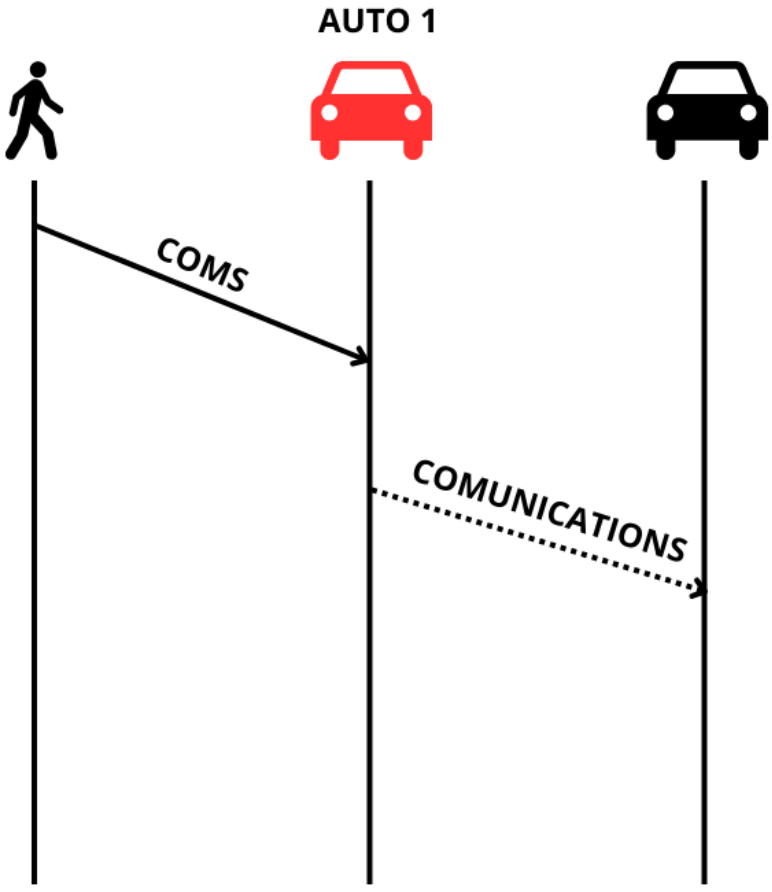

Figura 4.5: Schema del funzionamento del Protocollo 3.

4.4.4 Schema Dettagliato del Protocollo di Attraversamento

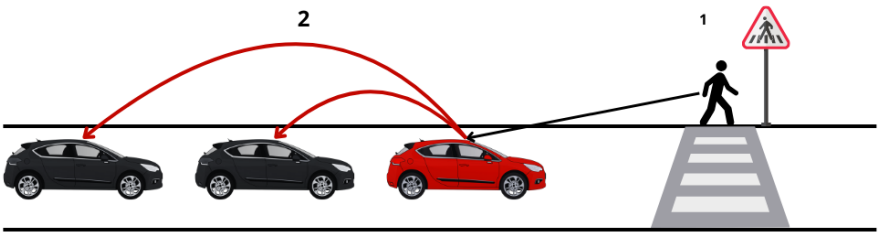

Figura 4.6: Schema del Protocollo di Attraversamento 3.

4.4.5 Vantaggi e Problemi Identificati

Rispetto ai protocolli precedenti, questo metodo offre diversi vantaggi:

- **Riduzione della latenza**: Eliminando il faro come nodo centrale, il ritardo di comunicazione è drasticamente ridotto, poiché l'informazione viene trasmessa in parallelo invece che in sequenza.

- **Migliore scalabilità**: Il sistema può adattarsi più facilmente all'aumento del numero di auto, evitando la congestione tipica di un sistema centralizzato come quello del Protocollo 2.

- **Flessibilità**: Il protocollo può funzionare anche in assenza di infrastrutture fisse, come in strade extraurbane o in situazioni di emergenza.

Tuttavia, questa decentralizzazione introduce anche alcune problematiche:

- **Affidabilità del segnale wireless**: La comunicazione basata su Bluetooth o DSRC può essere soggetta a interferenze o avere un raggio limitato, rendendo la propagazione del messaggio meno affidabile rispetto a un sistema centralizzato con il faro.

- **Coerenza delle informazioni**: Poiché la comunicazione avviene in modo distribuito, potrebbero verificarsi discrepanze nei tempi di aggiornamento dello stato tra le auto, con il rischio che alcune vetture non ricevano in tempo reale l'informazione sull'attraversamento del pedone.

- **Dipendenza dalla prima auto**: Se la prima auto non è in grado di inoltrare correttamente il messaggio (ad esempio per un guasto o una connessione instabile), la comunicazione potrebbe non raggiungere le altre vetture, compromettendo la sicurezza dell'attraversamento.

Rispetto ai protocolli precedenti, il Protocollo 3 introduce una maggiore velocità nella trasmissione dell'informazione ma richiede un'infrastruttura di comunicazione V2V affidabile per funzionare correttamente.

4.4.6 Formula della Latenza

Poiché la comunicazione avviene in parallelo tra le auto, senza la necessità di un intermediario centrale, la latenza complessiva è significativamente ridotta e può essere approssimata come:

$$T = R_{wireless} \tag{4.6}$$

dove:

- $R_{wireless}$ è il ritardo medio di trasmissione del segnale wireless tra le auto.

A differenza del Protocollo 2, in cui la latenza cresce linearmente con il numero di auto, nel Protocollo 3 la latenza rimane bassa grazie alla propagazione parallela. Tuttavia, la qualità della comunicazione dipende fortemente dall'affidabilità della rete V2V.

4.5 Protocollo 4: Comunicazione Faro-Centralizzata con Broadcast

4.5.1 Descrizione del Protocollo

Il **Protocollo 4** introduce un modello di comunicazione **semi-centralizzato**, combinando i vantaggi della comunicazione diretta tra auto e pedone con la coordinazione di un nodo centrale, il faro.
In questo scenario, il pedone comunica con la prima auto in arrivo utilizzando una connessione wireless a corto raggio, come il **Bluetooth** o il **DSRC**.
L'auto che riceve il segnale dal pedone inoltra immediatamente l'informazione al faro. Il faro, a sua volta, diffonde il messaggio a tutte le auto nelle vicinanze tramite un messaggio in broadcast.

Rispetto al **Protocollo 3**, che si basava esclusivamente sulla comunicazione diretta tra auto (**V2V**), il Protocollo 4 reintroduce un elemento di centralizzazione per migliorare l'affidabilità e garantire che tutte le auto ricevano l'informazione simultaneamente. Questo riduce il rischio di perdita o incoerenza delle informazioni, ma introduce una latenza aggiuntiva dovuta al passaggio attraverso il faro.

4.5.2 Funzionamento

Il protocollo segue i seguenti passaggi:

1. **Il pedone arriva all'attraversamento e comunica via wireless** (es. Bluetooth, DSRC) con la prima auto in arrivo.

2. **L'auto 1 riceve il segnale e lo trasmette immediatamente al faro.**

3. **Il faro**, una volta ricevuta l'informazione, **invia un messaggio in broadcast a tutte le auto** nella zona, informandole della presenza del pedone.

   Le auto ricevono il messaggio e aggiornano il proprio stato, fermandosi se necessario.

   Una volta completato l'attraversamento, il faro invia un segnale di ripresa del traffico a tutte le auto.

Questo meccanismo garantisce che tutte le auto nella zona ricevano contemporaneamente l'informazione, riducendo i rischi di ritardi o incongruenze nella rete.

4.5.3 Schema del Protocollo

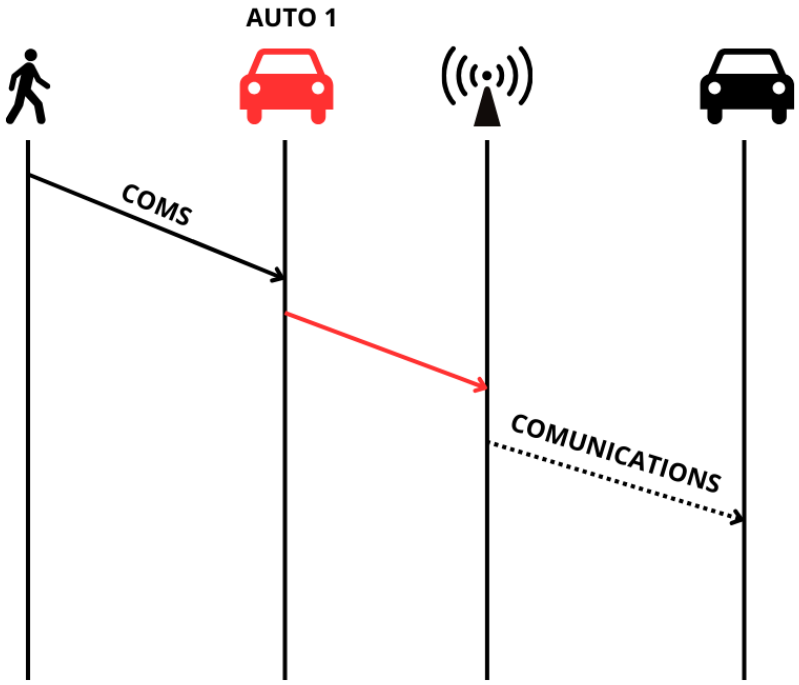

Figura 4.7: Schema dettagliato del Protocollo 4: Comunicazione diretta tra pedone e auto 1, con successivo inoltro al faro e broadcast verso le auto.

4.5.4 Schema Dettagliato del Protocollo di Attraversamento

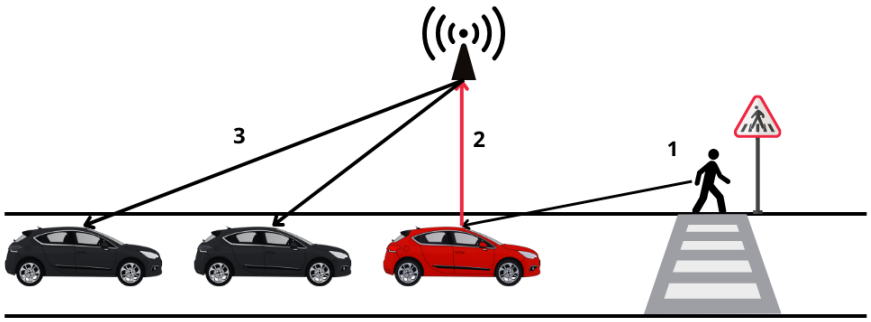

Figura 4.8: Rappresentazione grafica del Protocollo 4: il pedone comunica con l'auto 1, che inoltra l'informazione al faro, il quale la trasmette alle altre auto.

4.5.5 Vantaggi e Problemi Identificati

Rispetto ai protocolli precedenti, questo metodo offre diversi vantaggi:

- **Riduzione del carico di comunicazione sulle auto**: A differenza del Protocollo 3, in cui le auto devono propagare autonomamente l'informazione tra loro, il Protocollo 4 centralizza questa operazione nel faro, semplificando la gestione della rete.
- **Maggiore affidabilità della trasmissione**: La presenza del faro garantisce che tutte le auto ricevano l'informazione senza dipendere esclusivamente dalla propagazione V2V, che potrebbe essere soggetta a interferenze o ritardi.
- **Sincronizzazione globale delle auto**: Poiché il faro invia il messaggio in broadcast, tutte le auto ricevono l'informazione simultaneamente, evitando discrepanze nei tempi di ricezione.
- **Riduzione della latenza per la prima auto**: L'auto 1 riceve l'informazione immediatamente dal pedone e può reagire senza dover aspettare che altre auto confermino il messaggio.

Tuttavia, il protocollo introduce alcune limitazioni:

- **Latenza introdotta dal faro**: Poiché il messaggio deve essere trasmesso dall'auto 1 al faro e poi dal faro a tutte le auto, si introduce un ritardo aggiuntivo rispetto alla propagazione diretta auto-auto del Protocollo 3.
- **Dipendenza dal faro**: Se il faro non è disponibile o ha un carico elevato, la trasmissione dell'informazione potrebbe essere ritardata o interrotta.
- **Affidabilità della comunicazione wireless**: La trasmissione iniziale tra pedone e auto 1, così come l'invio del messaggio da parte del faro, dipendono dalla qualità del segnale wireless, che può essere influenzato da ostacoli fisici o interferenze elettromagnetiche.

4.5.6 Formula della Latenza

La latenza totale del protocollo è determinata dalla somma dei ritardi di trasmissione tra i vari attori coinvolti:

$$T = R_{ped-auto} + R_{auto-faro} + R_{faro-broadcast} \tag{4.7}$$

dove:

- $R_{ped-auto}$ è il ritardo medio di trasmissione tra il pedone e l'auto 1.
- $R_{auto-faro}$ è il ritardo medio di trasmissione tra l'auto 1 e il faro.
- $R_{faro-broadcast}$ è il ritardo medio di propagazione del segnale dal faro alle auto.

Rispetto al **Protocollo 3**, in cui le auto comunicano direttamente tra loro senza un nodo centrale, il Protocollo 4 introduce un ritardo aggiuntivo dovuto al passaggio attraverso il faro. Tuttavia, questa architettura migliora la sincronizzazione globale delle informazioni e riduce il rischio di mancata ricezione del messaggio da parte di alcune auto.

Nota bibliografica: Per approfondimenti sulle tecnologie di comunicazione V2V e V2X, si rimanda a [11, 9].

Capitolo 5

Emulazione del Sistema

5.1 Introduzione

L'emulazione del sistema descritta in questo capitolo ha l'obiettivo di simulare un ambiente complesso in cui un incrocio intelligente gestisce la comunicazione tra auto, pedoni e un faro intelligente. L'intento è quello di replicare un sistema che permette alle auto di reagire in tempo reale alla presenza di pedoni, migliorando la sicurezza stradale attraverso un flusso continuo e sicuro di informazioni.
L'emulazione vuole esplorare come le comunicazioni crittografate possano essere gestite in tempo reale tra i dispositivi, come le auto reagiscano ai segnali inviati dal faro e come i pedoni possano interagire con il traffico in modo sicuro. Viene inoltre testata la capacità del sistema di scalare e adattarsi a scenari complessi, come l'ingresso e l'uscita delle auto dalla rete, la gestione della sicurezza tramite certificati digitali, e la gestione dinamica del traffico, inclusi i tempi di attesa e le risposte delle auto durante l'attraversamento dei pedoni. In sostanza, l'emulazione ha lo scopo di verificare e validare le performance del sistema in un contesto che replica fedelmente l'interazione tra le varie entità.

L'emulazione del sistema è stata realizzata con un'infrastruttura software che replica il comportamento di un incrocio intelligente, utilizzando tecnologie come **Tailscale**, **Netcat** e **Docker** per gestire la rete, la comunicazione e la virtualizzazione delle entità coinvolte. Questo capitolo descrive i dettagli tecnici dell'implementazione, i meccanismi di sicurezza adottati e le strategie per la simulazione di un ambiente realistico.

5.2 Gestione della Rete con Tailscale

Tailscale è stato utilizzato per creare un'**overlay network sicura** che consente alle auto, ai pedoni e al faro di comunicare tra loro in modo affidabile e crittografato.

Un **overlay network** è una rete virtuale che si costruisce sopra un'altra rete fisica o esistente, creando una sorta di "strato" aggiuntivo che permette di gestire la comunicazione tra i dispositivi in modo più flessibile, sicuro o efficiente. In altre parole, l'overlay network non si preoccupa della topologia fisica sottostante (come la rete locale o Internet), ma costruisce una propria rete logica, che può seguire una struttura completamente diversa.

Nel contesto di Tailscale, un overlay network è stato utilizzato per creare una rete privata sicura tra le entità coinvolte nel sistema (auto, pedoni, faro), indipendente-

mente dalla rete fisica su cui si trovano. Tailscale, basato su WireGuard, fornisce una crittografia end-to-end e permette a ciascun dispositivo di comunicare direttamente con gli altri attraverso questa rete sicura, senza necessità di configurare manualmente firewall o altre misure di sicurezza. In pratica, ogni entità nel sistema diventa un nodo di questa rete virtuale, connessa tramite chiavi crittografiche e certificati, e la comunicazione avviene attraverso canali protetti che impediscono accessi non autorizzati.

Questo tipo di rete è particolarmente utile per creare sistemi distribuiti in cui la sicurezza, la privacy e la gestione delle comunicazioni tra dispositivi sono cruciali, come nel caso di un incrocio intelligente dove il traffico di dati tra auto, pedoni e il faro deve essere protetto da attacchi esterni e garantire l'affidabilità delle informazioni.

5.2.1 Autenticazione e Sicurezza con WireGuard e Certificati Digitali

Tailscale sfrutta il protocollo **WireGuard** per la crittografia e la protezione delle comunicazioni. Ogni entità del sistema (auto, pedone, faro) utilizza **chiavi di autenticazione** e **certificati digitali** per accedere alla rete. Questo garantisce che solo dispositivi autorizzati possano partecipare alle comunicazioni.

- **Autenticazione delle auto:** Ogni auto deve presentare un certificato digitale valido per connettersi alla rete dell'incrocio.
- **Verifica del faro:** Il faro verifica l'identità di ogni utente prima di accettare la comunicazione.
- **Sicurezza crittografica:** Le comunicazioni tra le entità avvengono con cifratura end-to-end tramite WireGuard, garantendo protezione contro intercettazioni e manomissioni.

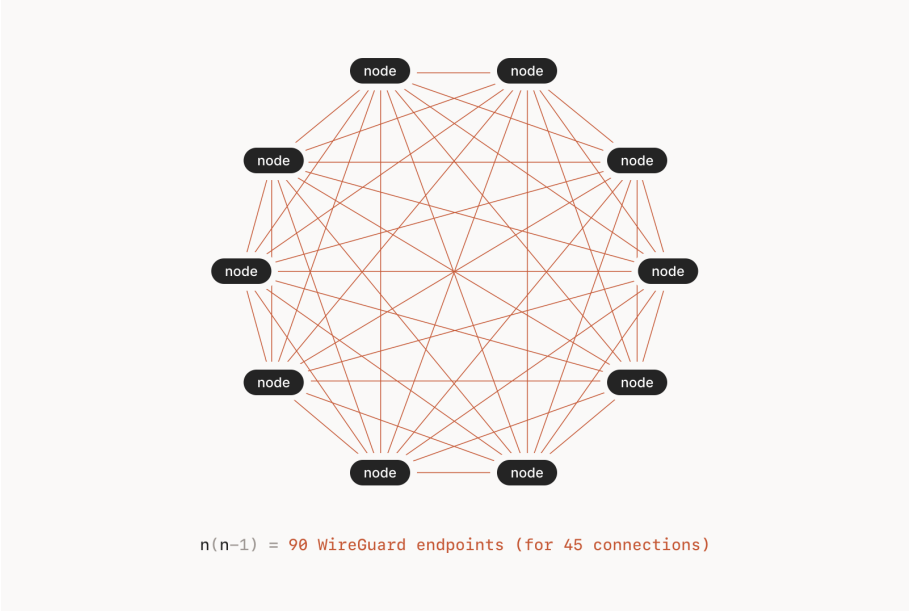

Figura 5.1: Schema della rete gestita con Tailscale.

5.3 Comunicazione tra le Entità con Netcat

Netcat è stato impiegato per la trasmissione dei messaggi tra le auto, il faro e il pedone. Si tratta di un **tool di basso livello** per la comunicazione in rete, utile per testare lo scambio di messaggi in scenari simulati.

5.3.1 Struttura della Comunicazione

Ogni entità nel sistema apre una connessione su una porta specifica:

- Il faro **ascolta su una porta predefinita** per ricevere le richieste di attraversamento dai pedoni e inoltrarle alle auto.
- Le auto **ricevono le notifiche** dal faro e dai pedoni e regolano la loro velocità di conseguenza.
- I pedoni **inviamo un segnale di attraversamento** utilizzando Netcat verso il faro o direttamente alle auto, a seconda del protocollo adottato.

5.3.2 Esempio di comunicazione

Un'auto che riceve un segnale di attraversamento dal pedone:

```
nc -l -p 8000
# Output atteso: "Pedone sta attraversando"
```

Invio di un messaggio di attraversamento da parte del pedone:

```
echo "Pedone sta attraversando" | nc 192.168.1.10 8000
```

5.4 Virtualizzazione con Docker

Docker è stato utilizzato per simulare più auto, il faro e il pedone in un ambiente controllato. Ogni entità è eseguita in un container separato per replicare la scalabilità e la dinamicità del sistema reale.

5.4.1 Struttura dei Container

- **Container Faro:** Coordina le comunicazioni tra pedoni e auto.
- **Container Auto:** Riceve notifiche e interagisce con il faro e i pedoni.
- **Container Pedone:** Simula il comportamento di attraversamento e invia segnali agli altri attori.

Esempio di creazione di un container Docker:

```
docker run -d --name car1 --hostname car1 --cap-add NET_ADMIN
--device /dev/net/tun --network tailscale-network -e
TAILSCALE_AUTHKEY=tskey-auth-keyOfTheNode car
```

5.5 Funzionamento del Programma

Il programma è organizzato in moduli separati per ciascun attore, con la logica implementata in script **Bash**. Ogni attore segue un ciclo operativo basato sugli eventi che riceve:

- Il **faro** riceve richieste e gestisce le comunicazioni con la coda M/M/1.
- Le **auto** attendono segnali dal faro o dai pedoni e agiscono di conseguenza.
- Il **pedone** simula l'attraversamento e notifica le altre entità.

Esempio di codice per dle richieste nel faro nel protocollo 4:

```
while true; do
    echo -e "${CYAN}Faro in attesa di messaggi da car...${NC}"

    # Ascolta i messaggi da car1 sulla porta 12347
    MESSAGE=$(nc -l -p 12347)
    if [ ! -z "$MESSAGE" ]; then
        echo -e "${YELLOW}Messaggio ricevuto da car1: $MESSAGE${NC}"

        # Recupera l'IP di car1
        CAR1_IP=$(tailscale status | grep 'car1' | awk '{print $1}')

        # Invia il messaggio a tutte le altre auto
        invia_a_tutte_le_auto_escluse_car1 "$MESSAGE" "$CAR1_IP"
    fi
done
```

5.6 Esempio di Log dell'Emulazione

L'emulazione ha permesso di testare diversi scenari di traffico, verificando il flusso delle comunicazioni tra il pedone, il faro e le auto. Qui sono riportati alcuni estratti dei log generati durante l'esecuzione del sistema, evidenziando i messaggi scambiati tra le entità.

Pedone:
2024-11-14 14:58:11 Sono al semaforo...
2024-11-14 14:58:16 IP delle auto ricevuti: 100.91.211.29, 100.81.119.104

Faro:
2024-11-14 14:58:03 Faro in attesa di ricevere dati...
2024-11-14 14:58:16 Messaggio ricevuto dal pedone: Sono al semaforo, dammi gli IP delle auto - Timestamp: 2024-11-14 13:58:11 - IP pedone: 100.122.22.62
2024-11-14 14:58:16 Messaggio inviato al pedone (100.122.22.62): IP delle auto: 100.91.211.29, 100.81.119.104

Comunicazione del Faro alle Auto:
2024-11-14 14:58:26 Messaggio inviato all'auto 100.91.211.29: Pedone sta attraversando - Timestamp: 2024-11-14 13:58:26
2024-11-14 14:58:26 Messaggio inviato all'auto 100.81.119.104: Pedone sta attraversando - Timestamp: 2024-11-14 13:58:26

L'uso di Docker ha garantito la scalabilità della simulazione, mentre Netcat ha dimostrato di essere un metodo efficace per la comunicazione a bassa latenza. La sicurezza della rete è stata assicurata dall'uso di Tailscale, che ha impedito accessi non autorizzati alle comunicazioni tra le entità.

Nota bibliografica: Per approfondimenti sulle tecnologie impiegate, si rimanda a [15, 6, 2, 4, 14].

Capitolo 6

Analisi e Confronto dei Protocolli di Comunicazione

6.1 Introduzione

L'analisi dei protocolli di comunicazione adottati in questo studio è fondamentale per valutare l'efficacia dei metodi utilizzati nel ridurre la latenza e nel migliorare la sicurezza degli utenti deboli della strada, come i pedoni, in un contesto urbano. Lo scenario considerato coinvolge un sistema di comunicazione tra auto, pedoni e un faro intelligente in un incrocio, dove la sicurezza è garantita dalla corretta gestione della comunicazione tra i vari attori del sistema. In questo scenario, la gestione dei flussi di dati in tempo reale è essenziale per evitare situazioni pericolose, come la mancata rilevazione di un pedone che sta attraversando la strada.

Per eseguire una valutazione precisa dei protocolli di comunicazione, è stato preso in considerazione un numero variabile di auto, da 1 a 15, che partecipano alla comunicazione con il faro, simulando condizioni di traffico diverse. La latenza di comunicazione è stata ipotizzata essere intorno ai $\pm$100ms, con una connessione wireless di qualità medio/buona, che è rappresentativa di una connessione tipica in ambienti urbani congestionati. Questo intervallo di latenza è importante per testare la reattività e l'affidabilità del sistema, in particolare durante le situazioni di alta densità di traffico.

Ogni protocollo di comunicazione verrà valutato in base alla sua capacità di ridurre la latenza, alla sua resilienza in ambienti congestionati e alla sua tolleranza ai guasti. In questa sezione, verranno confrontati i quattro protocolli precedentemente definiti, con particolare attenzione alla latenza introdotta, alla capacità di gestire le comunicazioni in scenari di traffico variabile e alla resilienza in caso di malfunzionamenti o perdite di pacchetti.

6.2 Raccolta Dati e Metodologia di Analisi

Per misurare l'efficacia di ogni protocollo, sono stati raccolti dati sulle latenze di comunicazione in diversi scenari di traffico. Le metriche principali prese in considerazione includono:

- **Tempo di risposta** T: intervallo tra l'invio della richiesta da parte del pedone e la ricezione della conferma da parte dell'auto.

- **Numero di veicoli coinvolti** N: quantità di auto che devono ricevere l'informazione.
- **Influenza della coda** W_q: impatto della gestione delle richieste da parte del faro sulle latenze di trasmissione.
- **Scalabilità**: capacità del protocollo di gestire un aumento del numero di auto senza degrado delle prestazioni.
- **Fault tolerance**: resilienza del protocollo in caso di malfunzionamenti o perdita di pacchetti di comunicazione.

6.3 Parametri di Misurazione

La latenza totale del sistema viene calcolata come:

$$T_{totale} = T_{arrivo_info} - T_{invio_info} \tag{6.1}$$

dove:

- T_{invio_info} è il tempo in cui l'informazione viene inviata dal pedone o dal faro.
- T_{arrivo_info} è il tempo in cui l'informazione raggiunge l'auto destinataria.
- La differenza tra i due valori rappresenta il ritardo effettivo del sistema.

Inoltre, possiamo espandere il calcolo dettagliando i contributi:

$$T_{totale} = T_{iniziale} + T_{propagazione} + W_q \tag{6.2}$$

dove:

- $T_{iniziale}$ è il tempo impiegato dal sistema per elaborare e avviare la trasmissione dell'informazione.
- $T_{propagazione}$ è il tempo di trasmissione del segnale nella rete.
- W_q è il tempo di attesa nella coda del faro (quando presente), che dipende dalla congestione della rete.

6.4 Confronto delle Prestazioni tra i Protocolli

I quattro protocolli sono stati analizzati sulla base delle latenze di comunicazione in diversi scenari. I risultati sono riportati nei seguenti grafici.

6.4.1 Protocollo 1: Comunicazione Diretta Pedone-Auto via Faro

- **Vantaggi**: Struttura semplice, adatta a scenari con basso traffico.
- **Svantaggi**: Ritardo cumulativo dovuto alla coda FIFO nel faro.

Se il pedone invia la comunicazione ma il faro impiega troppo tempo a recuperare le informazioni delle auto, potrebbe accadere che il pedone abbia già attraversato o, nel peggiore dei casi, un'auto non abbia il tempo sufficiente per frenare.

$$T_{P1} = N \cdot R + R \tag{6.3}$$

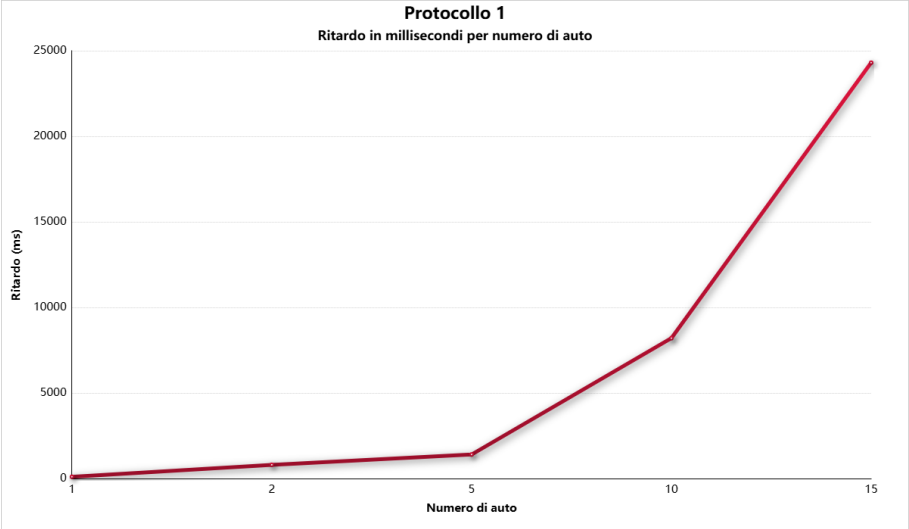

Figura 6.1: Analisi della latenza del Protocollo 1.

6.4.2 Protocollo 2: Comunicazione Centralizzata via Faro

- **Vantaggi**: Ritardo ridotto rispetto al Protocollo 1 grazie alla gestione sequenziale delle comunicazioni da parte del faro.
- **Svantaggi**: Dipendenza dal faro, che diventa un potenziale punto critico.

Se il faro è congestionato, l'ultima auto in coda riceverà l'informazione con un ritardo considerevole, riducendo il margine di sicurezza.

$$T_{P2} = (N - 1) \cdot R + R \tag{6.4}$$

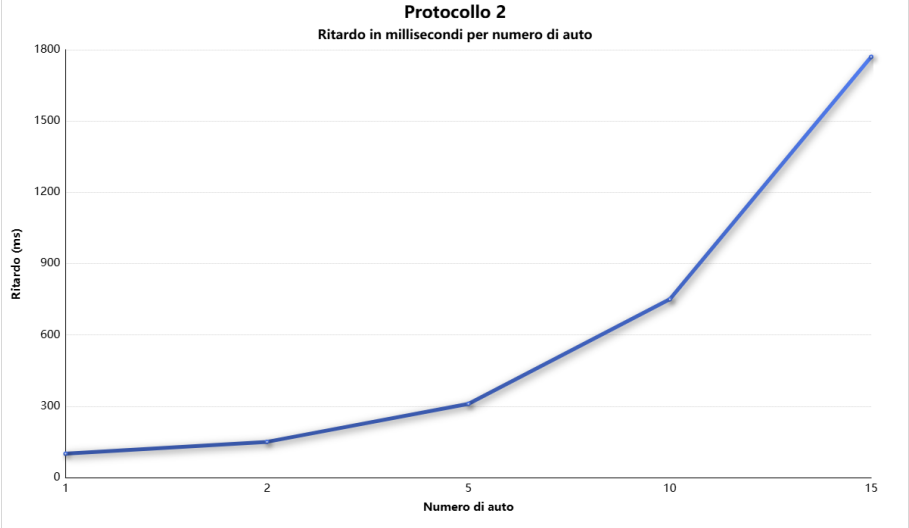

Figura 6.2: Analisi della latenza del Protocollo 2.

6.4.3 Protocollo 3: Comunicazione Auto-Auto (V2V)

- **Vantaggi**: Comunicazione diretta tra le auto, riduzione della latenza complessiva.
- **Svantaggi**: Possibili problemi di coerenza delle informazioni in caso di perdita di pacchetti.
  Possibile non conoscenza di tutte le auto presenti, con conseguente problema di diffusione dell'informazione

Grazie alla trasmissione diretta V2V, il tempo di propagazione 'e ridotto rispetto agli altri protocolli, avendo un ritardo di comunicazione lineare.

$$T_{P3} = R_{wireless} \tag{6.5}$$

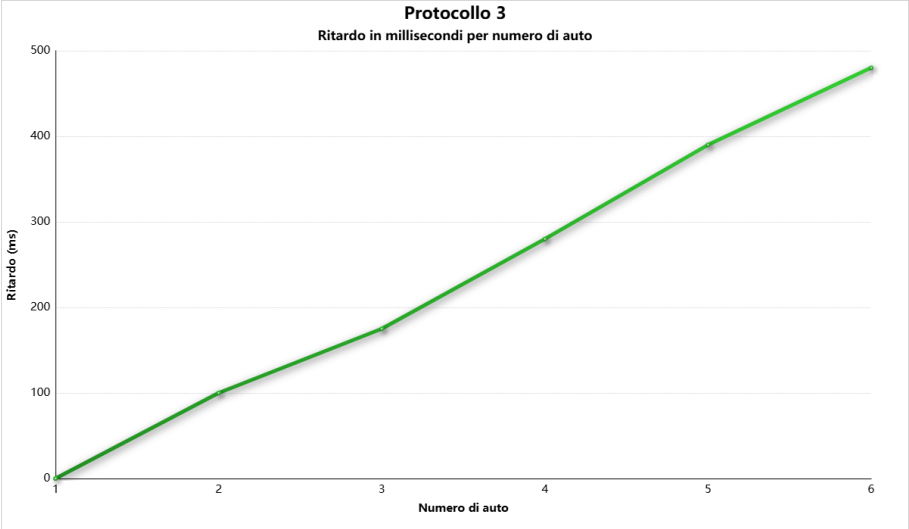

Figura 6.3: Analisi della latenza del Protocollo 3.

6.4.4 Protocollo 4: Comunicazione Faro con Broadcast

- **Vantaggi**: Maggiore affidabilità, riduzione del rischio che un'auto perda il messaggio.
  Auto più vicina al pedone con ritardo quasi assente.
- **Svantaggi**: Dipendenza dal faro, che potrebbe introdurre ritardi in caso di congestione.

Il faro trasmette a tutte le auto l'attraversamento del pedone; la prima auto ricevendo l'informazione diretta dal pedone, riesce a ridurre a quasi 0, il ritardo. Risulta essere una versione migliorata del protocollo 2.

$$T_{P4} = R_{wireless} + W_q \tag{6.6}$$

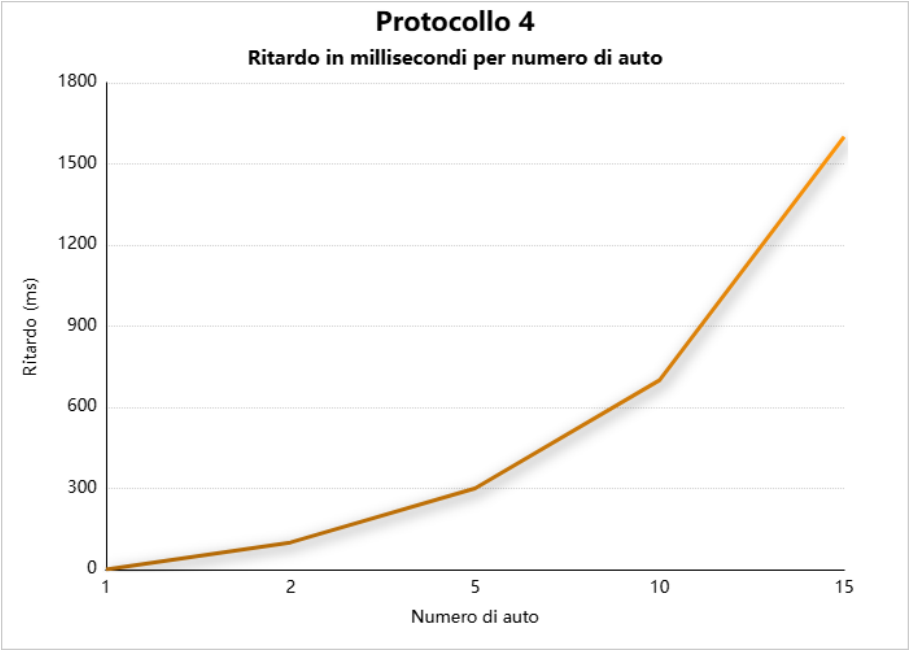

Figura 6.4: Analisi della latenza del Protocollo 4.

6.5 Affidabilità e Fault Tolerance

I protocolli sono stati confrontati in termini di tolleranza ai guasti:

- **Protocollo 1 e 2**: Forte dipendenza dal faro, che può diventare un punto critico in caso di guasti.
- **Protocollo 3**: Maggiore resilienza, poiché la comunicazione auto-auto riduce la dipendenza da un nodo centrale.
- **Protocollo 4**: Equilibrio tra affidabilità e velocità, grazie all'uso del faro per la diffusione dei messaggi. Il protocollo 4 garantisce la possibilità di passare al metodo di comuncazione del protocollo 3.

6.6 Formula del Ritardo Massimo Ammissibile

La determinazione del **ritardo massimo ammissibile** è un aspetto critico nella progettazione di sistemi di attraversamento sicuri. Se il tempo di risposta complessivo di un protocollo supera questo valore, si entra in una zona di rischio in cui le auto potrebbero non avere il tempo sufficiente per frenare e fermarsi in sicurezza prima di raggiungere il pedone.

6.6.1 Definizione del Ritardo Massimo

Il ritardo massimo ammissibile $\Delta T_{ritardomax}$ viene calcolato come:

$$\Delta T_{ritardomax} = T_{arrivo} - T_{frenata} \tag{6.8}$$

dove:

- T_{arrivo} è il tempo che un'auto impiega per raggiungere il punto di attraversamento dal momento in cui il pedone invia il segnale.
- $T_{frenata}$ è il tempo necessario all'auto per fermarsi completamente una volta ricevuta la comunicazione.

6.6.2 Calcolo dei Tempi

Il tempo di arrivo di un'auto dipende dalla velocità e dalla distanza dall'incrocio:

$$T_{arrivo} = \frac{D}{V} \tag{6.9}$$

dove:

- D è la distanza dell'auto dal punto di attraversamento (in metri).
- V è la velocità dell'auto (in metri al secondo).

Il tempo di frenata, invece, dipende dalla decelerazione media del veicolo:

$$T_{frenata} = \frac{V}{a} \tag{6.10}$$

dove:

- a è la decelerazione media dell'auto (tipicamente 8 m/s^2 per un'auto moderna su asfalto asciutto).

6.6.3 Analisi del Margine di Sicurezza

Affinché un'auto possa fermarsi in tempo, è necessario che:

$$T_{comunicazione} + T_{reazione} < \Delta T_{ritardomax} \tag{6.11}$$

dove:

- $T_{comunicazione}$ è il tempo necessario affinché il pedone comunichi l'attraversamento alle auto.
- $T_{reazione}$ è il tempo di elaborazione della comunicazione e attuazione della frenata (stimato tra 0.5 e 1 secondo per i veicoli autonomi).

Se questa condizione non viene rispettata, aumenta il rischio che l'auto non riesca a fermarsi in tempo, con conseguente impatto sulla sicurezza dell'attraversamento.

6.6.4 Apprendimento Automatico per l'Ottimizzazione della Velocità

Un sistema avanzato di **machine learning** potrebbe essere implementato per migliorare la sicurezza stradale attraverso l'auto-adattamento della velocità dei veicoli autonomi. Il sistema imparerebbe a moderare la velocità in zone ad alto rischio di ritardo comunicativo, basandosi su dati storici e analisi delle condizioni della rete.

Raccolta dati e identificazione dei punti critici

Ogni veicolo autonomo potrebbe raccogliere dati relativi ai ritardi nelle comunicazioni e alla frequenza degli attraversamenti pedonali, al fine di individuare potenziali criticità nel sistema. L'analisi si concentrerebbe sul tempo medio di latenza nelle interazioni con il faro e i pedoni, sulla ricorrenza degli attraversamenti in specifici punti della rete stradale e sulla presenza di frenate improvvise richieste in determinate aree.

L'aggregazione di queste informazioni consentirebbe di identificare tratti stradali in cui il rischio di superamento del ritardo massimo ammissibile risulta particolarmente elevato, permettendo così l'implementazione di strategie di ottimizzazione mirate per migliorare l'efficienza e la sicurezza del sistema.

Regolazione automatica della velocità

Un modello predittivo potrebbe stimare in tempo reale il rischio di dover frenare improvvisamente e adattare di conseguenza la velocità del veicolo. Il comportamento potrebbe essere regolato come segue:

$$V_{ottimale} = V_{base} \cdot \left(1 - \frac{T_{storicoritardo}}{T_{ritardomax}}\right) \tag{6.12}$$

dove:

- $V_{ottimale}$ è la velocità adattata per migliorare la sicurezza.
- V_{base} è la velocità normale su quel tratto di strada.

- $T_{storicoritardo}$ è il valore medio del ritardo di comunicazione registrato in passato.
- $T_{ritardomax}$ è il ritardo massimo ammissibile per evitare incidenti.

In aree con ritardi elevati, la velocità del veicolo verrebbe ridotta in modo dinamico per aumentare il margine di sicurezza e garantire il tempo sufficiente per reagire.

6.6.5 Schema Visivo

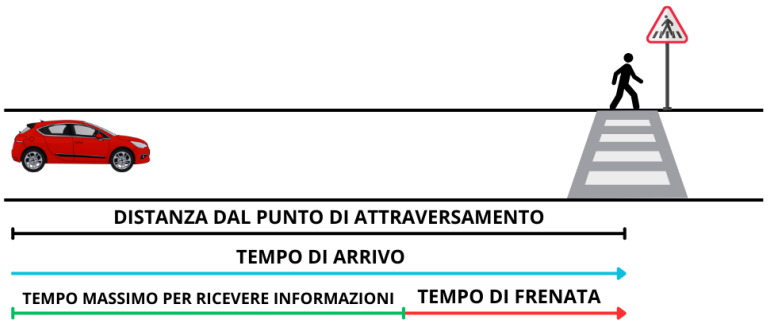

Figura 6.5: Schema del ritardo massimo ammissibile

6.6.6 Risultati e Considerazioni

Dai dati raccolti, si osserva che protocolli con comunicazione diretta tra auto (come il Protocollo 3) riducono significativamente il tempo di comunicazione $T_{comunicazione}$, aumentando la probabilità di rispettare la soglia di sicurezza. Al contrario, protocolli che coinvolgono un intermediario centralizzato (Protocollo 1 e 2) introducono latenze superiori, riducendo il margine di sicurezza.
Il protocollo 4 presenta il miglior compromesso tra sicurezza, velocità, stabilità e adattamento.

Conclusione: la scelta del protocollo incide direttamente sulla sicurezza dell'attraversamento. Protocolli con latenza inferiore garantiscono una maggiore affidabilità nella prevenzione di incidenti, rispettando il ritardo massimo ammissibile.

.

Nota bibliografica: Per ulteriori dettagli sulle misurazioni, si rimanda a [9, 12].

Capitolo 7

Conclusioni

Lo studio condotto in questa tesi ha analizzato l'interazione tra veicoli autonomi, pedoni e infrastrutture stradali in scenari di attraversamento, evidenziando le criticità della comunicazione nei sistemi Vehicle-to-Everything (V2X). L'implementazione di protocolli di comunicazione differenti ha permesso di valutare come la latenza e l'affidabilità influenzino la sicurezza stradale e l'efficienza del traffico.

L'emulazione del sistema ha evidenziato che le soluzioni centralizzate, pur garantendo un maggiore controllo sulle informazioni, soffrono di colli di bottiglia dovuti all'accumulo di richieste, mentre i modelli distribuiti riducono la latenza ma possono introdurre problemi di coerenza delle informazioni. In particolare, il **Protocollo 3 (Comunicazione Diretta Auto-Auto)** ha dimostrato tempi di risposta più rapidi grazie alla propagazione parallela, mentre il **Protocollo 4 (Comunicazione Faro con Broadcast)** ha migliorato l'affidabilità della trasmissione garantendo una sincronizzazione globale.

I risultati ottenuti confermano che non esiste un'unica soluzione ottimale, ma la scelta del protocollo deve essere adattata alle esigenze specifiche del contesto di applicazione. Scenari con elevata densità di traffico potrebbero beneficiare di approcci ibridi che combinano comunicazione diretta tra veicoli e una supervisione centrale per garantire la coerenza dei dati.

Infine, questo lavoro apre la strada a futuri sviluppi nell'ambito della comunicazione V2X, come l'integrazione di tecniche di apprendimento automatico per l'ottimizzazione dei tempi di risposta o l'uso di reti neurali per la predizione del comportamento dei pedoni. Inoltre, ulteriori ricerche potrebbero esplorare l'implementazione su larga scala di queste soluzioni in ambienti reali, valutando l'efficacia dei protocolli in scenari urbani complessi.

L'adozione di soluzioni efficaci per la comunicazione tra veicoli autonomi e pedoni sarà cruciale per garantire la sicurezza e l'affidabilità delle future infrastrutture stradali intelligenti.

Bibliografia

[1] Jean-François Bonnefon, Azim Shariff, and Iyad Rahwan. The social dilemma of autonomous vehicles. *Science*, 352(6293):1573–1576, 2016.

[2] GNU Netcat Contributors. Netcat user guide, 2024.

[3] Wikipedia contributors. M/m/1 queue — wikipedia, the free encyclopedia, 2024. Accessed: 2024-02-04.

[4] Jason A. Donenfeld. Wireguard: Fast, modern, secure vpn tunnel, 2024. Accessed: 2024-02-06.

[5] Noah J. Goodall. Machine ethics and automated vehicles. *Road Vehicle Automation*, pages 93–102, 2014.

[6] Docker Inc. Docker documentation, 2024.

[7] GlobalSpec Insights. Network architecture essentials for v2x, 2021. Accessed: 2024-02-06.

[8] Georgios Karagiannis, Ozan Altintas, Eran Ekici, Günter Heijenk, Babak Jarupan, Kenichi Lin, and Timothy Taleb. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys Tutorials*, 13(4):584–616, 2015.

[9] Georgios Karagiannis and et al. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys Tutorials*, 13(4):584–616, 2011.

[10] John B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[11] John B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[12] Leonard Kleinrock. *Queueing Systems, Volume 1: Theory*. Wiley-Interscience, New York, 1975.

[13] Patrick Lin. Why ethics matters for autonomous cars. *Autonomous Driving*, pages 69–85, 2016.

[14] Jens B. Schuerz and Wolfgang J. W. Jansen. *Digital Certificates: An Introduction to Public Key Infrastructure*. Springer, 2020.

[15] Tailscale. Tailscale documentation, 2024.

[16] Haibo Zhou, Ruiliang Chen, Lei Xu, and Michel Kadoch. V2x communication for future intelligent transportation systems. *Wireless Communications and Mobile Computing*, 2012:1–10, 2012.

Grazie.

Una parola così semplice e così poco usata, contenente tanto significato.
Sono grato a tutte le persone che in questi anni mi hanno fatto crescere, facendomi capire cosa voglio e soprattutto cosa non voglio essere nella mia vita.
Grazie a Mirko, per non essersi mai arreso, puntando sempre al meglio nonostante le tante cause di stress.
Per non esserti mai fermato.
Non volevi continuare, eppure facendolo sembrare facile, hai vinto.
Grazie alla mia famiglia, per avermi regalato le console, facendomi appassionare al mondo virtuale e informatico.
Per avermi insegnato dei valori non indifferenti.
Grazie a tutti gli amici, che hanno reso più serene le giornate, con cui ho vissuto esperienze e momenti indimenticabili.