Gestione della Reputazione nelle Reti Veicolari per la Diffusione Affidabile degli Eventi

Tesi di Laurea Magistrale in Ingegneria Informatica

Antonio Virga

Relatore: Prof.ssa Alessandra De Paola

Correlatori: Ing. Vincenzo Agate

UNIVERSITÀ DEGLI STUDI DI PALERMO
DIPARTIMENTO DI INGEGNERIA

LAUREA MAGISTRALE IN INGEGNERIA INFORMATICA

GESTIONE DELLA REPUTAZIONE NELLE RETI VEICOLARI PER LA DIFFUSIONE AFFIDABILE DEGLI EVENTI

Tesi di Laurea di
Antonio Virga

Relatore:
Prof.ssa Alessandra De Paola

Correlatore:
Prof. Vincenzo Agate

Abstract

I progressi tecnologici nel settore automobilistico e nei paradigmi di comunicazione tra veicoli promettono l'implementazione di servizi sempre più avanzati per rendere la guida più sicura e consapevole di eventi come la congestione del traffico e i pericoli stradali. Tuttavia, l'efficacia di questi servizi si basa sull'assunzione che nel contesto delle VANET (Vehicular Ad Hoc Networks) una rete di veicoli possa essere connessa a un'infrastruttura più complessa, utilizzando diverse Road Side Unit (RSU) per raggiungere obiettivi specifici. Questa ipotesi non sempre può essere soddisfatta nella pratica a causa di vincoli economici e ambientali che limitano la distribuzione di RSU. Inoltre, il rilevamento e la diffusione di informazioni affidabili sugli eventi stradali sono di fondamentale importanza per evitare situazioni spiacevoli e potenzialmente pericolose, causate dalla diffusione di falsi messaggi da parte di veicoli inaffidabili o intenzionalmente manomessi. Al fine di affrontare queste sfide, la presente tesi propone un sistema innovativo di rilevamento degli eventi che si basa sulla diffusione affidabile dei dati nelle VANET, sfruttando un meccanismo di reputazione e fiducia completamente distribuito, senza l'ausilio di un'infrastruttura fissa lungo le strade, consentendo così una maggiore flessibilità e scalabilità del sistema. La valutazione sperimentale dimostra la robustezza del sistema nel contrastare la presenza di veicoli fraudolenti o che forniscono informazioni inaccurate, confermando la sua capacità di fornire informazioni affidabili sugli eventi stradali.

Contents

1 Introduzione **3**

1.1 Motivazioni 4

1.2 Struttura della tesi 4

2 Stato dell'arte **7**

2.1 VANET: caratteristiche 8

2.2 VANET: componenti 9

2.3 Dedicated Short-Range Communications 10

2.4 Comunicazione 13

2.5 Data Dissemination 15

2.6 Population Protocol 24

2.7 Sistemi di gestione della fiducia-reputazione 27

3 Sistema proposto **32**

3.1 Architettura multi livello 32

3.2 Sensing layer 32

3.3 Communication Layer 32

3.4 Modello di reputazione 33

3.5 Modello di diffusione dei dati 33

3.6 Application layer 33

4 Valutazione sperimentale **34**

4.1 Ambiente di simulazione 34

4.2 Metriche di valutazione 34

4.3 Calibrazione delle scelte progettuali 34

4.4 Impostazione sperimentale 35
4.5 Risultati sperimentali 35

5 Conclusioni **36**

Elenco delle figure **39**

Elenco delle tabelle **40**

Bibliography **41**

Chapter 1

Introduzione

Il filone di ricerca delle VANET (Vehicular Ad Hoc Networks) risulta essere tra i più studiati dalla comunità scientifica, con un interesse fortemente cresciuto negli ultimi anni, grazie alla sua promessa di rivoluzionare il settore del Intelligent Transport System [1] attraverso la comunicazione tra veicoli e l'infrastruttura di supporto.
Il crescente numero di veicoli, d'altro canto, ha portato ad un aumento sostanziale di incidenti e inquinamento atmosferico. I problemi elencati costituiscono solo una parte delle molteplici sfide che le reti VANET risolvono con efficacia. Attraverso l'uso di tecnologie wireless per abilitare le comunicazioni, le VANET offrono una vasta gamma di applicazioni con lo scopo di migliorare la sicurezza stradale, l'efficienza e l'esperienza degli utenti, consentendo una migliore gestione del traffico, la prevenzione degli incidenti e la riduzione delle emissioni.
Tra gli aspetti chiave che caratterizzano le VANET vi è la loro capacità di fornire una comunicazione efficiente ed affidabile in ambienti particolari caratterizzati da alta mobilità. La Data Dissemination tra veicoli e tra veicoli ed infrastrutture richiede protocolli di routing appositamente progettati per affrontare le sfide di questo contesto dinamico e volatile. Inoltre, la sicurezza delle comunicazioni nelle VANET è un fattore critico da considerare, poiché l'accesso a informazioni sensibili, la protezione dei dati degli utenti e l'affidabilità delle informazioni ricevute sono aspetti di fondamentale importanza. Pertanto, lo sviluppo di protocolli di sicurezza efficaci, meccanismi di autenticazione e sistemi di gestione della reputazione diventano un'area di ricerca fondamentale nel contesto delle VANET.

1.1 Motivazioni

Le comunicazioni Vehicle-to-Vehicle (V2V) e Vehicle-to-Infrastructure (V2I) sono componenti fondamentali dei Sistemi di Trasporto Intelligenti (ITS) al fine di migliorare la qualità del servizio (QoS), come la sicurezza e l'efficienza del traffico veicolare [2, 3]. Questi due paradigmi di comunicazione VANET, nonostante le loro profonde differenze, mirano a abilitare servizi avanzati come l'analisi della congestione, la gestione del traffico, la prevenzione delle collisioni, la guida cooperativa e le applicazioni di comfort/infotainment [4].

Nel V2I, l'interazione tra i veicoli si basa sulla presenza di un'infrastruttura statica, quindi la comunicazione avviene tra le unità di bordo (OBUs) installate nei veicoli e le unità stradali (RSUs) che fanno parte dell'infrastruttura statica. La necessità di questa infrastruttura è la principale limitazione di questo paradigma, in quanto potrebbe non essere sempre presente per molteplici ragioni, incluse l'impatto ambientale o il costo eccessivo.

Pertanto, è di fondamentale importanza esplorare soluzioni efficienti e affidabili per garantire servizi avanzati negli scenari V2V. Una delle principali sfide in questo scenario è garantire l'affidabilità delle comunicazioni, che può essere influenzata da vari fattori fisici come la velocità del veicolo, l'elevata densità del traffico e la presenza di ostacoli fisici.

Molti lavori presenti in letteratura cercano di risolvere questo problema attraverso la progettazione di protocolli efficienti di diffusione dei dati [5]. Tuttavia, questo approccio non è sufficiente, poiché in un ambiente completamente distribuito, senza alcun controllo sulla qualità dei dati scambiati, informazioni false potrebbero essere diffuse a causa di errori dei sensori o opportunamente falsificate da nodi maligni che partecipano alla rete. Per questi motivi, la fiducia e la reputazione diventano essenziali per valutare l'affidabilità dei dati ricevuti e dei nodi di rete [6, 7]. Tuttavia, i sistemi esistenti di gestione della reputazione sono inadeguati per scenari come le reti veicolari a causa dell'alta mobilità dei nodi e della necessità di elaborare richieste di valutazione della fiducia in modo tempestivo per mantenere le operazioni di rete [8].

1.2 Struttura della tesi

Per superare tali limitazioni, il lavoro di tesi propone un architettura multi livello distribuita in cui vi è implementato un modello di comunicazione V2V basato su un Population Protocol one-way [9], che utilizza un sistema di gestione della reputazione per attribuire maggiore importanza ai dati inviati dagli utenti fidati e migliorare così la QoI complessiva [10]. Tale architettura

determina accuratamente valori di fiducia sugli eventi scambiati durante le comunicazioni. Per ottenere con accuratezza questi valori di fiducia vengono calcolati valori di reputazione per tutti i nodi che costituiscono la rete. Questi valori di reputazione sono calcolati localmente in ogni nodo, tenendo conto dello storico di comunicazione. Pertanto, i valori di reputazione determinati da un veicolo specifico sono opportunamente aggregati al fine di calcolare la fiducia per ogni evento ricevuto. Le prestazioni dell'architettura proposta, che ha il compito di gestire comunicazioni efficienti ed affidabili, sono state investigate in termini di accuratezza della rilevazione di comportamenti malevoli e della sua resistenza ad attacchi di diffusione di informazioni errate. I principali contributi della tesi sono riassunti come segue:

- è stato ideato un sistema di diffusione degli eventi efficiente, in grado di diffondere in tempi ragionevoli la conoscenza locale di ogni nodo;
- è stato ideato un modello per il calcolo di fiducia distribuito che associa ad ogni evento ricevuto un valore di fiducia ponderando i valori di reputazione dei nodi che partecipano alla comunicazione. Le reputazioni dei nodi vengono determinate sulla base della fiducia locale e con lo storico di comunicazione;
- è stato sviluppato un meccanismo a soglia di fiducia in grado di scartare gli eventi incerti, e di segnalare con un sistema di feedback gli eventi ritenuti malevoli;
- è stata condotta un'ampia valutazione sperimentale stressando il modello con attacchi di disseminazione di false informazioni al crescere del numero di nodi malevoli nella comunicazione. I risultati mostrano che la soluzione proposta qui è resistente ad attacchi da parte di utenti maligni organizzati in gruppi che agiscono simultaneamente per danneggiare il sistema.

Il lavoro di tesi è stato strutturato in 5 capitoli.

- In questo primo capitolo, è stata presentata un descrizione dello scenario oggetto del lavoro di tesi, presentando le problematiche che caratterizzano quest'ambiente.
- Il capitolo 2 presenta le caratteristiche principali delle VANET, affrontando una panoramica delle varie tecniche di Data Dissemination e dei sistemi di gestione della reputazione. Introduce il modello matematico relativo ai Population Protocol. Approfondisce quindi lo stato dell'arte facendo riferimento ad alcuni sistemi proposti in letteratura.

- Il capitolo 3 è dedicato alla descrizione dell'architettura proposta per far fronte ai problemi di efficienza e affidabilità nella comunicazione.
- Il capitolo 4 descrive la valutazione sperimentale condotta sul modello. Inizialmente mostra il processo che a condotto alle scelte progettuali del sistema, e successivamente valuta l'efficienza del sistema in scenari realistici.
- Infine, il capitolo 5 riassume gli obiettivi raggiunti e pone dei riferimenti su futuri lavori di approfondimento e miglioramento del sistema.

Chapter 2

Stato dell'arte

Nelle reti VANET, per mantenere elevati valori di QoS nelle possibili applicazioni, diventa di fondamentale importanza un'efficiente rete per la distribuzione delle informazioni [11]. In questa tipologia di reti la diffusione dei dati viene effettuata tramite tre differenti comunicazioni dirette: da veicolo a veicolo (V2V), da veicolo a infrastruttura (V2I) o da infrastruttura a veicolo (I2V), come mostrato in Fig. 2.1. In questa figura, le comunicazioni V2V, V2I e I2V avvengono all'interno dell'intervallo di comunicazione delle RSU (Road-Side Unit) e OBU (On-Board Unit). Oggi molti dei veicoli moderni sono dotati di centinaia di sensori che generano un'enorme quantità di dati. Questi devono essere raccolti e analizzati per garantire il corretto funzionamento delle varie applicazioni smart [12], [13]. I sensori a bordo del veicolo a loro volta devono comunicare tra loro attraverso tecnologie come Bluetooth, ZigBee, Radio Frequency Identification (RFID), banda ultra larga (UWB) e onde millimetriche. Un problema ancora presente in questi scenari e la gestione affidabile delle comunicazioni. L'obbiettivo di questo capitolo è quello di analizzare le sfide uniche e le strategie utilizzate per garantire la consegna efficiente ed affidabile delle informazioni.
In particolare presenta:

- una panoramica sulle reti VANET evidenziando le sfide che le caratterizzano;
- la definizione dello standard di comunicazione con le diverse tipologie presenti nelle scenario delle reti veicolari;
- le tecniche di data dissemination e sistemi di gestione della reputazione presenti in letteratura.

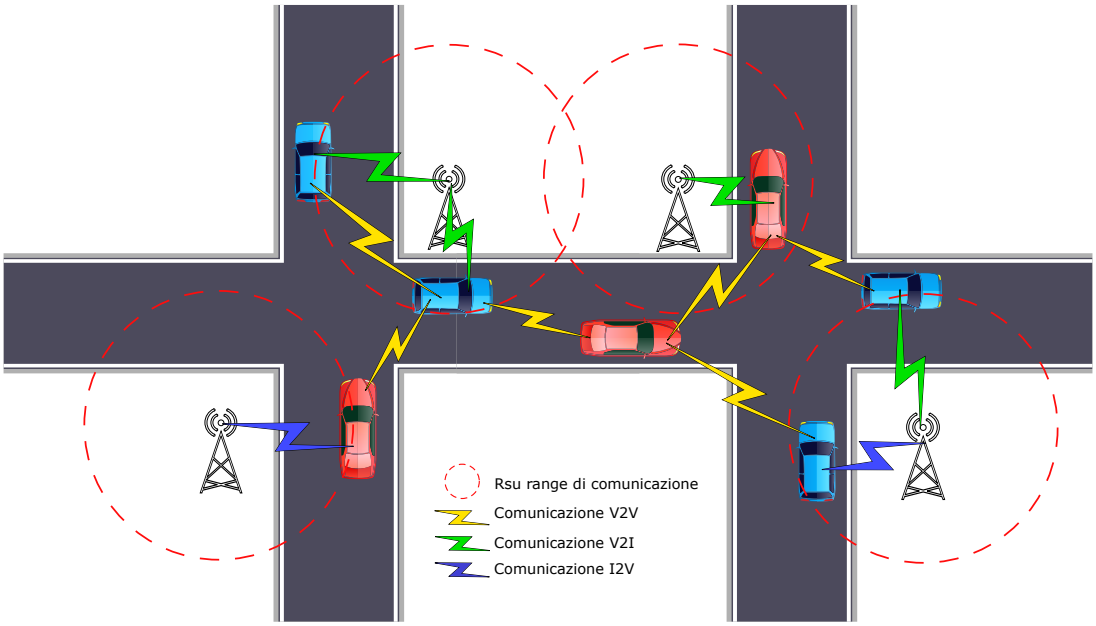

Figure 2.1: Struttura della rete VANET.

2.1 VANET: caratteristiche

Le VANET inizialmente considerate come una sotto categoria delle reti MANET (Mobile Ad-hoc Network), sono diventate un campo di studio assestante per le loro sfide uniche che le differenziano dalle reti mobili [13]. Volendo effettuare un analisi comparativa fra le due tipologie di reti, gli aspetti principali in cui differisco sono:

- *velocità di spostamento dei nodi*: nelle reti MANET, la velocità di spostamento dei nodi, che sono dispositivi mobili, è determinata dall'azione umana, conferendo loro una bassa mobilità. Al contrario, nelle VANET, la velocità di spostamento dei nodi dipende dalla velocità del veicolo, introducendo così delle complessità nella gestione della rete. Questa situazione rappresenta una sfida per gli algoritmi di routing poiché i nodi (veicoli), in movimento ad alta velocità, modificano frequentemente le connessioni nella rete, richiedendo un maggiore sforzo computazionale;

- *topologia di rete*: le reti MANET sono caratterizzate da una topologia di rete dinamica e autoconfigurante, poiché i nodi possono entrare o uscire dalla rete in qualsiasi momento. Al contrario, nelle VANET, la topologia di rete è strettamente legata alla disposizione dei veicoli sulla strada;

- *distribuzione dei nodi*: nei sistemi VANET, è possibile osservare una distribuzione più densa dei nodi rispetto a un contesto MANET convenzionale. Di conseguenza, si verifica un incremento della probabilità che i veicoli all'interno della rete formino gruppi ravvicinati. Tale caratteristica è vantaggiosa in quanto contribuisce ad alleviare le difficoltà legate all'instaurazione di connessioni locali;

- *energia*: la mancanza di dipendenza dalla batteria rappresenta una caratteristica distintiva dei sistemi VANET, poiché elimina la preoccupazione riguardante la disconnessione improvvisa dei nodi a causa dell'esaurimento dell'energia.

Come risultato, è stato sviluppato il campo delle reti veicolari ad hoc (VANET) per affrontare i specifici aspetti unici che caratterizzano questo ambiente. In breve, le VANET possono essere considerate reti wireless composte da nodi veicolari che formano in modo spontaneo la struttura della rete.

2.2 VANET: componenti

Nell'ambito delle VANET, vengono utilizzati diversi dispositivi hardware che svolgono un ruolo cruciale nel garantire una comunicazione efficiente e sicura tra i veicoli e infrastrutture stradali. Ognuno di questi componenti ha il compito specifico di fornire funzionalità essenziali per il funzionamento delle reti VANET. Nelle sezioni seguenti, segue una breve panoramica sulle componenti principali che costituiscono le VANET.

2.2.1 Road-Side Unit

La Roadside Unit (RSU) è un dispositivo hardware che funge da ponte all'interno delle reti VANET installato lungo le infrastrutture stradali o in luoghi dedicati come ad esempio in corrispondenza di incroci o in prossimità di parcheggi. Grazie alla loro posizione strategica consente le comunicazione V2I (Vehicle-to-Infrastructure) e tra veicoli e RSU. L'RSU è dotata di un scheda di rete che permette la comunicazione dedicata a corto raggio implementando lo standard IEEE 802.11p. Le RSU hanno i compiti principali di:

- estendere il raggio di comunicazione della rete scambiando informazioni provenienti delle OBU con altre RSU dislocate nella rete così da raggiungere aree più esterne;

- gestire le comunicazioni I2V (Infrastructure-to-Vehicle) così da diffondere ai nodi informazioni provenienti dall'infrastruttura;
- fornire connettività Internet alle OBU.

2.2.2 On-Board Unit

L'On-Board Unit (OBU) è un dispositivo hardware solitamente installato su ogni veicolo all'interno di una rete VANET. L'OBU ha il compito di raccogliere e trasmettere informazioni. Il principale compito è quello di scambiare informazioni con altri veicoli e con l'infrastruttura tramite le RSU incontrate nelle strade. Per eseguire le comunicazioni implementa un interfaccia di rete che sfrutta la tecnoligia wireless basato sullo standard IEEE 802.11p. Talvolta viene anche dotato di altro hardware che gli permette di comunicare tramite tecnologia GSM, UMTS, 4G oppure 5G, al fine di fornire dei servizi aggiuntivi.

2.2.3 Application Unit

L'AU (Application Unit) è il dispositivo equipaggiato all'interno del veicolo che ha la capacità di processare tutte quelle informazioni ottenute tramite comunicazione dell'OBU per eseguire quelle applicazioni fornite dal provider. L'AU può essere un dispositivo dedicato come centraline aggiuntive di gestine dell'auto o un normale dispositivo come un assistente digitale personale. L'AU può essere connesso all'OBU tramite una connessione cablata o wireless e può risiedere con l'OBU in un singola unità fisica.

2.3 Dedicated Short-Range Communications

Dedicated Short-Range Communications (DSRC) è una tecnologia di comunicazione wireless progettata per consentire la comunicazione a corto raggio tra veicoli e infrastrutture stradali. Questa nasce quando, la Federal Communication Commission (FCC) degli Stati Uniti ha riservato 75 MHz di spettro nella banda a $5,9$ GHz da utilizzare esclusivamente per le comunicazioni di tipo Vehicle-to-Vehicle e Vehicle-to-Infrastructure [14, 15]. Lo standard viene definito da tre enti quali:

- IEEE (Institute of Electrical and Electronics Engineers): Lo standard IEEE 802.11p definisce la specifica tecnica per il livello fisico di DSRC come mostrato in Fig. 2.3. IEEE

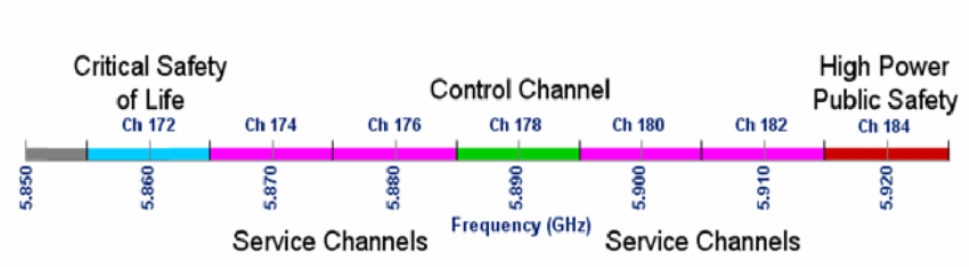

Figure 2.2: Banda e canali dello spettro DSRC negli Stati Uniti. (Immagine tratta da [14])

802.11p fa parte della famiglia di standard Wi-Fi e fornisce una base per le comunicazioni V2V e V2I;

- SAE (Society of Automotive Engineers): SAE ha sviluppato lo standard J2735, che definisce il formato dei messaggi di sicurezza veicolare trasmessi tramite DSRC. Questo standard specifica la struttura e il contenuto delle informazioni scambiate tra i veicoli e le infrastrutture stradali;

- ETSI (European Telecommunications Standards Institute): L'ETSI ha contribuito alla standardizzazione di DSRC per il contesto europeo. Lo standard ETSI EN 302 571 definisce i requisiti tecnici e le caratteristiche operative per l'uso di DSRC in Europa, compresi gli aspetti relativi alle frequenze e alla coesistenza con altri sistemi di comunicazione.

Una rappresentazione dello spettro DSRC è mostrata in Fig. 2.2, questa è suddivvisa in sette canali larghi 10 MHz ciascuno. Nella definizione dei canali questi sono stati raggruppati per servizi che offrono, in particolare: il canale 178 che corrisponde al canale di controllo (CCH), è riservato solo alle comunicazioni di sicurezza, i due canali 172, 184 sono riservati ad usi speciali, mentre il resto sono canali corrispondono a canali di servizio (SCH) disponibili per qualsiasi tipo di applicazioni. Lo spettro è stato suddiviso in canali da 10 MHz, piuttosto che da 20 MHz, poiché questo nasce con lo scopo di gestire più applicazioni in parallelo e quindi di ridurre la congestione dei canali di comunicazione a disposizione.

Analizzando lo stack del protocollo per la comunicazione DSRC mostrato in Fig. 2.3, troviamo una rappresentazione dei vari livelli protocollari con i relativi standard associati. In particolare, partendo dal basso, nel livello fisico (PHY) e MAC, lo standard DSRC utilizza IEEE 802.11p Wireless Access for Vehicular Environments (WAVE). Al centro dello stack, DSRC utilizza una serie di standard che fanno parte della famiglia dall'IEEE 1609 Working Group:

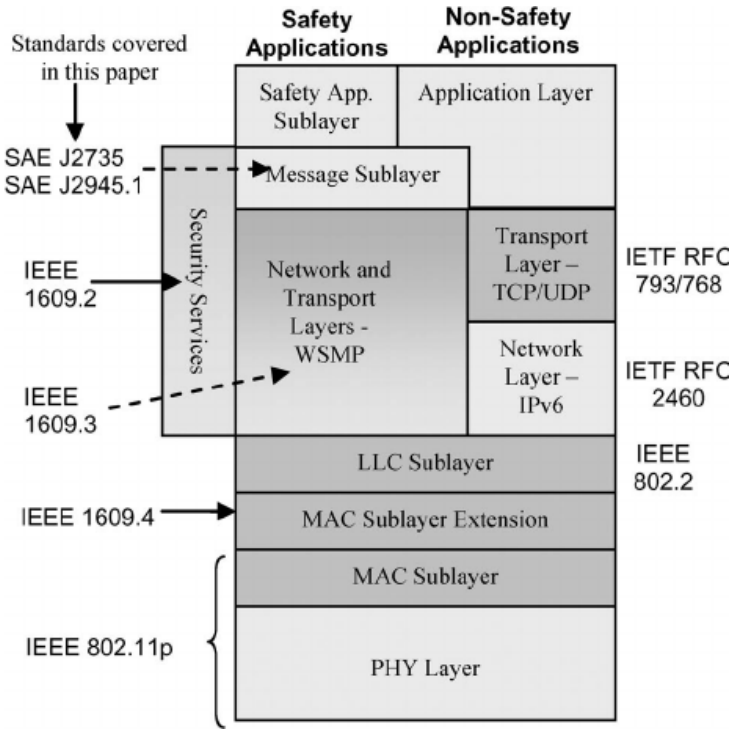

Figure 2.3: Stack protocollare DSRC. (Immagine tratta da [15])

- *1609.4*: utilizzato per il Channel Switching, definisce il livello di interfaccia di rete (Network Interface Layer) per le comunicazioni DSRC. Questo standard specifica le regole di accesso al canale, il formato dei pacchetti di dati ed i meccanismi di sicurezza per consentire la comunicazione V2V e V2I affidabili;

- *1609.3*: utilizzato per il livello rete e di trasporto. Questo standard fornisce le specifiche per il routing dei pacchetti e la rilevamento dei nodi di rete;

- *1609.2*: utilizzato per i servizi di sicurezza, è uno standard che definisce il livello di gestione della sicurezza (Security Management Layer) per le comunicazioni DSRC. In particolare stabilisce le specifiche per la gestione delle chiavi di crittografia, l'autenticazione delle entità, l'autorizzazione e l'integrità dei dati trasmessi.

Nella figura in questione sono mostrati anche protocolli noti come IPv6, UDP e TCP, anch'essi supportati dallo standard DSRC. Tuttavia, tali protocolli sono rappresentati esclusivamente per completezza, in quanto il protocollo WSMP risulta essere il più utilizzato nei livelli rete e trasporto. In fine nella figura, vi è lo standard SAE J2735 Message Set Dictionary che specifica

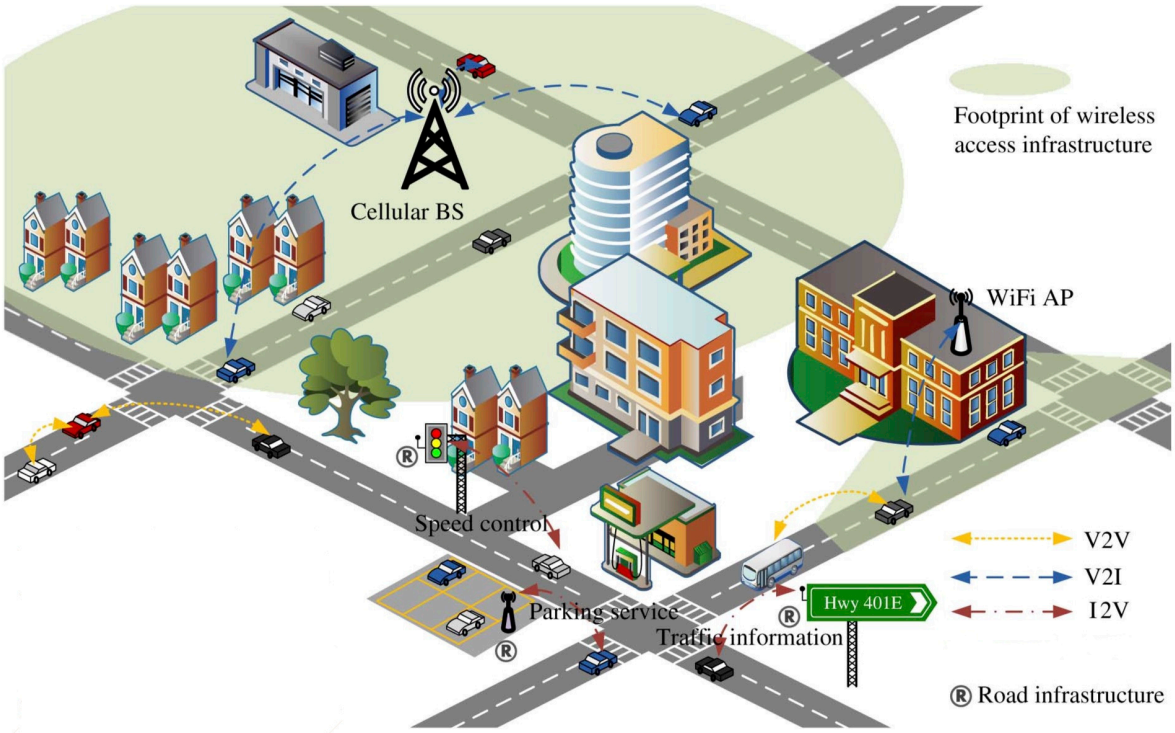

Figure 2.4: Comunicazioni nelle VANET.

la struttura e i formati dei messaggi che possono essere generati e vengono supportati dalle varie applicazioni per le VANET. Tra le varie tipologie di messaggi definiti in J2735 possiamo trovare: messaggi per la sicurezza stradale (BSM), messaggi generici e messaggi di allerta per i casi di emergenza (EVAM).

2.4 Comunicazione

Come già anticipato le reti VANET sono caratterizzate da elevata mobilità dei nodi e dalla topologia della rete altamente dinamica. Per far fronte a queste caratteristiche sono state proposte due tecnologie innovative che hanno lo scopo di cambiare il sistema di trasporto attuale. Nella figura 2.4 sono illustrati alcuni possibili scenari di comunicazione veicolare.

La tecnologia V2V (Vehicle-to-Vehicle), che in figura è rappresentata in giallo, mette in comunicazione i nodi della rete direttamente senza l'ausilio di componenti terze. L'obbiettivo principale di questa tecnologia è quello di scambiare, in maniera repentina, tutte quelle informazioni utili

alle applicazioni di sicurezza stradale così da migliorare la viabilità della strada. Attraverso le comunicazioni V2V i nodi nella rete possono organizzarsi in strutture completamente o parzialmente connesse come mostrato nelle figure 2.5, 2.6. Dove nella prima figura, ogni nodo può inviare messaggi a tutti i nodi raggiungibili dal suo range di comunicazione, mentre nel secondo caso, si formano dei collegamenti ridotti, sulla base di diverse caratteristiche, come la vicinanza, topologia o frequenza di condivisione delle informazioni. Attraverso queste topologie di connessioni, i nodi delle reti che vengono formate, possono scambiare informazioni o con i nodi vicini direttamente connessi tramite protocollo a singolo hop, oppure sfruttando uno dei diversi percorsi disponibili, formanti dalla struttura sparsa della rete, così da raggiungere il nodo di destinazione.
Con questa tecnologia, i nodi non fanno affidamento su nessuna stazione base (RSU) per la generazione dei percorsi di routing per la diffusione delle informazioni. Invece, i singoli nodi si inoltrano reciprocamente i pacchetti, permettendo una comunicazione fluida e indipendente. In questa rete gli agenti possono muoversi in maniera casuale e organizzarsi arbitrariamente, sebbene la topologia vari rapidamente e in modo imprevedibile.
Un vantaggio significativo di questa tecnologia che sfrutta solo le comunicazioni V2V, è che permette ai nodi di comunicare in qualsiasi condizione stradale, senza dover dipendere da infrastrutture che potrebbero non essere presenti in diversi contesti stradali.
Tuttavia, è importante considerare anche alcuni svantaggi derivanti da questa indipendenza. Ad esempio, potrebbe portare a congestione della rete come il fenomeno del broadcast storm [16], soprattutto nelle aree con una densità elevata di nodi, a causa dell'assenza di un'entità centralizzata che gestisca l'inoltro delle informazioni.

A differenza delle comunicazioni V2V, precedentemente descritte, la tecnologia V2I consente ai veicoli in transito di interfacciarsi con l'infrastruttura fissa a bordo della strada, (rappresentata in figura 2.4 da connesioni di colore rosso/blu). Quest'infrastruttura può essere distribuita in componenti stradali quali semafori, telecamere, lampioni e segnaletica verticale. Con l'ausilio di questa tecnologia le informazioni vengono trasmesse dagli elementi dell'infrastruttura al veicolo, o viceversa, attraverso una rete ad-hoc. Grazie alle comunicazioni V2I lo scenario degli ITS può acquisire dati da zone differenti della rete così da fornire agli utenti finali consigli in tempo reale, quali informazioni su viabilità, congestione del traffico, eventuali incidenti o disponibilità di parcheggi. Nonostante il vantaggio di raggiungere più nodi in posizioni differenti della rete, tra le principali limitazioni di questa tecnologia vi è il posizionamento e la manutenzione delle componenti fisse, infatti le RSU devono essere installate in modo uniforme

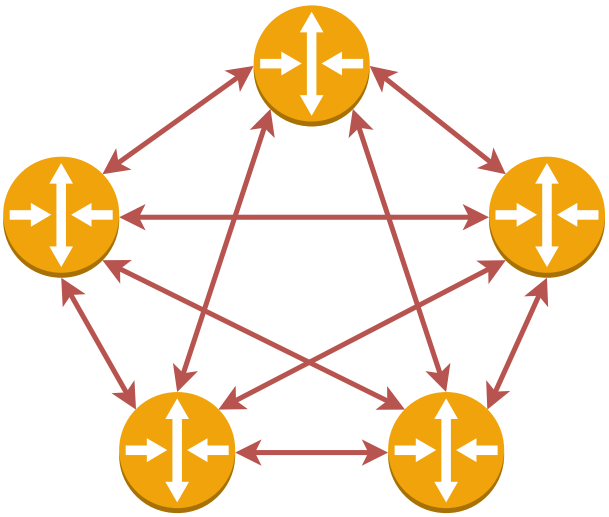

Figure 2.5: Struttura di una rete fully connected generata con comunicazione V2V.

nella rete per garantire una raggiungibilità a tutti i veicoli partecipanti alle comunicazioni.

2.5 Data Dissemination

La Data Dissemination è una componete cruciale nelle VANET, può essere usata per migliorare le applicazioni di sicurezza stradale, ottimizzare le prestazioni dei trasporti e creare reti per la pubblicizzazione locale e servizi di intrattenimento [17]. Data l'ampia gamma di applicazioni in cui è possibile usufruirne, la letteratura è ricca di numerosi articoli che trattano la Data Dissemination, evidenziando l'ampio interesse da parte della comunità accademica verso questa tematica nel contesto delle reti VANET. Prima di entrare nel dettaglio delle strategie di data dissemination presenti in letteratura, è importante comprendere gli obiettivi e le sfide che stimolano questo processo. Tra gli obiettivi comuni della data dissemination nelle reti VANET vi sono [18, 19]:

1. consegna affidabile dei dati: garantisce che i dati vengano inviati e ricevuti correttamente tra i veicoli, impedendo errori di trasmissione e corruzione delle informazioni. Questo richiede che siano implementate strategie e protocolli in grado di superare le sfide introdotte dalla elevata mobilità dei veicoli e dalla connettività intermittente dei nodi;

2. basso ritardo di consegna: ridurre il ritardo tra la generazione dei dati e la loro ricezione da

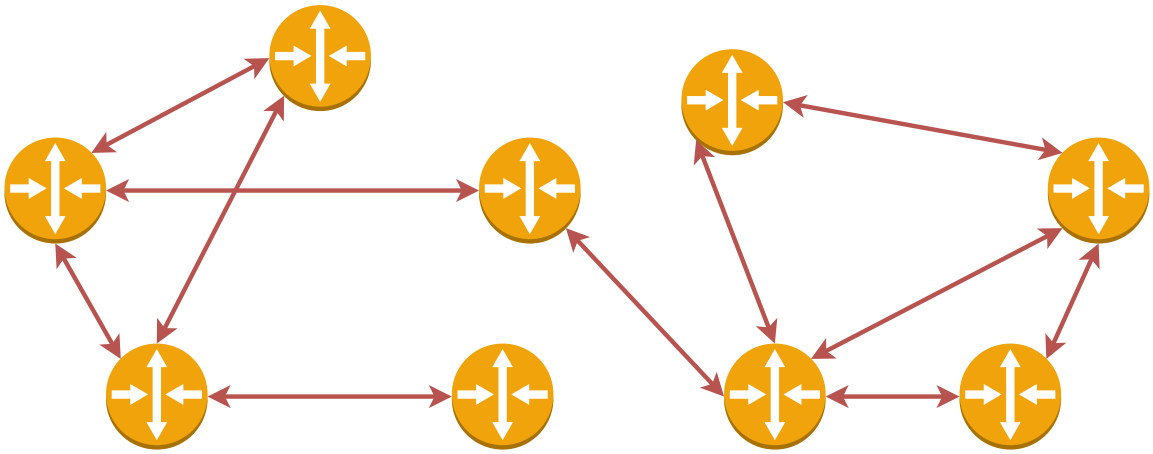

Figure 2.6: Struttura di una rete sparsa generata con comunicazione V2V.

parte dei veicoli destinatari, così da massimizzare l'efficienza e il QoS delle applicazioni che dipendono da tali informazioni;

3. utilizzo efficiente delle risorse: ottimizzare l'utilizzo delle risorse di rete, come la larghezza di banda e le risorse energetiche dei veicoli. Le tecniche di data dissemination devono essere progettate per ridurre al minimo il consumo di risorse e la congestione nella rete, garantendo al contempo una rapida e affidabile diffusione delle informazioni.

Come sopra citato i ricercatori nel campo delle VANET devono far fronte a diverse sfide per garantire una diffusione efficace dei dati. Alcune delle principali sfide sono:

1. realizzazione di applicazioni in real-time: il settore della mobilità è caratterizzato dall'importanza dello sviluppo di applicazioni in tempo reale. Tuttavia, risulta complesso avvisare veicoli circostanti nel momento opportuno, specialmente quando i dati scambiati sono utili per applicazioni di sicurezza con bassi tempi di validità o di utilità;

2. topologia altamente variabile: la topologia in una rete VANET cambia frequentemente a causa dell'elevata mobilità dei veicoli e delle interazioni tra di essi. I veicoli si muovono rapidamente e seguono percorsi imprevedibili, il che rende difficile prevedere la loro posizione e stabilire connessioni stabili per la trasmissione dei dati;

3. gestione delle connessioni instabili: a causa della mobilità dei veicoli, la connettività di rete può essere intermittente. È necessario sviluppare meccanismi di routing e strategie di

Data Dissemination che possano gestire la connettività instabile e garantire la consegna dei dati.

I ricercatori in letteratura hanno sviluppato diversi modelli efficienti di Data Dissemination nelle VANET, questi posso essere racchiusi in 5 macro categorie [20]: *Delay-Based Data Dissemination*, *Probability-Based Data Dissemination*, C*luster-Based Data Dissemination*, *Geocast-Based Data Dissemination* e *Hybrid-Based Data Dissemination*.
Prima di entrare nel dettaglio di queste categorie e importante sottolineare un'altra caratteristica cruciale per l'inoltro dei dati, ossia gli approcci di routing. Le tecniche di routing possono essere distinte in routing proattivo e routing reattivo [21]:

- Routing Proattivo: prevede la creazione e il mantenimento di tabelle di routing complete che devono essere aggiornate in ogni nodo della rete. Queste tabelle contengono informazioni sulle rotte che i dati devono seguire per raggiungere i nodi della rete;
- Routing Reattivo: determina il percorso dei pacchetti solo quando avviene una richiesta di transazione. In particolare, se un nodo desidera inoltrare un pacchetto, deve prima eseguire una fase di ricerca per determinare il percorso che i dati dovranno seguire.

2.5.1 Delay-Based Data Dissemination

Gli approcci di Data Dissemination orientati sul ritardo nascono con lo scopo di ridurre i tempi di trasmissione così da garantire la consegna efficiente dei dati, evitando la formazione del fenomeno del *Broadcast Storm* [16]. Il broadcast storm si manifesta all'interno di una rete quando numerosi nodi trasmettono contemporaneamente un elevato numero di pacchetti broadcast, così da causare congestione nella rete, collisioni di pacchetti e un utilizzo eccessivo delle risorse, con conseguente diminuzione generale delle prestazioni complessive. Le tecniche basate sul ritardo, per il loro funzionamento, considerano i ritardi di trasmissione e la connettività intermittente, caratteristiche tipiche delle reti VANET. Il funzionamento generale di questi sistemi può essere riassunto come segue [22, 23]:

- il nodo mittente crea un messaggio, e lo trasmette ad ogni singolo nodo del vicinato;
- i nodi riceventi avviano un timer che dipende da diversi fattori come: la distanza dal mittente, la portata di trasmissione, la velocità del veicolo del mittente, ecc;

- il veicolo con il valore più basso del timer ritrasmetterà il messaggio, allo stesso modo i restanti veicoli, con timer attivi per lo stesso messaggio fermeranno la ritrasmissione del messaggio.

Tuttavia, il problema principale di questa categoria è la definizione del timer di attesa appropriato, cioè in base a quali criteri e con quale tecnica. Considerando i lavori presenti in letteratura possiamo distinguere due tecniche di assegnazione del timer per mitigare il broadcast storm:

- **tecnica a slot** [24]: in questa tecnica, il tempo di trasmissione viene suddiviso in slot di tempo discreti, dove tutti i veicoli appartenenti allo stesso slot avranno assegnato lo stesso timer. La suddivisione degli slot ai nodi può dipendere da vari fattori come la distanza dal nodo mittente, la direzione che dovrà seguire il messaggio e dalla densità dei nodi presenti nella rete. Tale approccio richiede una sincronizzazione accurata tra i veicoli per garantire che ciascun nodo trasmetta nel suo slot di tempo assegnato. La mancanza di sincronizzazione accurata può portare a problemi come collisioni di pacchetti, sovrapposizione di trasmissioni o sottoutilizzo del canale. Se i nodi non trasmettono in maniera sincronizzata durante i loro slot di tempo assegnati, potrebbe verificarsi una congestione di rete o addirittura la mancata consegna dei pacchetti. Tuttavia, la sincronizzazione richiede un meccanismo affidabile per la distribuzione di clock comuni tra i nodi, e ciò aumenta la complessità computazionale del sistema;

- **tecnica continua** [25]: nella tecnica continua, il timer di attesa viene assegnato a ciascun veicolo ricevente in base alla sua distanza dal veicolo mittente. In genere, al nodo più lontano viene assegnato il tempo più breve per migliorare la propagazione dei dati nella direzione del messaggio. Per effettuare l'inoltro dei messaggi i nodi monitorano l'utilizzo del canale e cercano di evitare le collisioni ritardando la trasmissione in caso di congestione di rete. Questa tecnica si basa su algoritmi di accesso al canale come il protocollo Code Division Multiple Access (CDMA) o il protocollo Frequency Division Multiple Access (FDMA) per consentire una gestione efficiente delle trasmissioni broadcast. Tuttavia, la tecnica continua presenta anche alcune sfide. Poiché i nodi trasmettono in modo asincrono, ci può essere un rischio maggiore di collisioni di pacchetti, specialmente quando diversi nodi decidono di trasmettere contemporaneamente. Questo approccio offre una maggiore adattabilità al carico di traffico e alle condizioni del canale, ma richiede meccanismi di gestione e di rilevamento delle collisioni per evitare il deterioramento delle prestazioni a causa delle collisioni di pacchetti.

2.5.2 Probability-Based Data Dissemination

Come già accennato nei paragrafi precedenti, nelle VANET è fondamentale ottimizzare la trasmissione dei dati per garantire che le informazioni vengano diffuse in modo efficiente e tempestivo nella rete. Nella letteratura esistente, sono stati suggeriti diversi metodi di dissemination per le VANET, dove il flooding è la tecnica di trasmissione più comune. In questo approccio, quando un veicolo riceve un pacchetto, lo ritrasmette tempestivamente in rete a tutti i nodi vicini. Questo negli scenari delle reti veicolari si traduce nel problema del broadcast storm [55]. Una delle soluzioni adottate che ha lo scopo di ridurre questo fenomeno è la Probability-Based Data Dissemination [56]. L'obiettivo principale della probability-based data dissemination è massimizzare l'utilizzo delle risorse di rete e migliorare l'efficienza complessiva della trasmissione dei dati. Se i messaggi vengono trasmessi solo a un sottoinsieme selezionato di veicoli destinatari, la quantità di dati trasmessi e l'overhead di rete possono essere ridotti, consentendo un utilizzo più efficiente della larghezza di banda e dell'energia disponibili.
Nelle prime soluzioni proposte, i nodi della rete definiscono in maniera statica i valori di probabilità di inoltro per decidere la ritrasmissione del messaggio [57]. In questi schemi, i destinatari inoltrano i pacchetti a loro volta con una probabilità precalcolata così da ridurre la ridondanza delle informazioni. La probabilità di inoltro viene calcolata in base a diversi parametri, come la distanza tra mittente e destinatario, la densità della rete, l'orientamento del veicolo. In generale, nei sistemi appena descritti la probabilità aumenta in modo esponenziale al crescere della distanza tra mittente e destinatario, cosicché la ritrasmissione sia concentrata principalmente sui nodi di confine.
La semplice soluzione di considerare probabilità statiche non è adeguata in scenari complessi, quando nodi vicini trasmettono le stesse informazioni. Esistono soluzioni che basano l'inoltro dei dati su contatori o densità dei nodi. Esempi di queste soluzioni sono:

- *Adaptive Information Dissemination (AID)* [58]: in questo lavoro gli autori propongono un approccio che tiene conto di un *contatore* per calcolare la probabilità di inoltro delle informazioni. Nello specifico viene calcolato un punteggio (ridondanza dai vicini), che dipende dalla quantità di pacchetti simili ricevuti in un determinato periodo di tempo e dai loro parametri locali. Un punteggio alto implica che vi sia una ritrasmissione minima dell'informazione, ed aumenta di conseguenza la probabilità per quel nodo di inoltrare il messaggio. Al contrario, un punteggio basso, riduce la probabilità di trasmissione;

- *Dynamic Hybrid Broadcasting Protocol (DHBP)* [59]: in questo documento, la dissemi-

nazione delle informazione viene eseguita in base ad un valore di probabilità calcolato da una funzione decisionale (DMF). Questo valore dipende da vari fattori, come la priorità del messaggio, la distanza tra il nodo di inoltro e la posizione dell'incidente e il conteggio dei messaggi ricevuti durante il tempo di valutazione. Quando la priorità del messaggio raggiunge lo zero o la distanza o il numero di messaggi supera una soglia predefinita, il nodo di inoltro interrompe la ritrasmissione;

- *Density-Aware Probabilistic Interest Forwarding (DAPIF)* [61]: con questo metodo, la probabilità di inoltro dipende dalla densità dei veicoli vicini quando viene ricevuto un pacchetto di dati. Per stimare il valore di densità, viene proposto un metodo di approssimazione della densità locale utilizzando i beacon, che la determina senza conoscere la posizione esatta dei veicoli.

Anche se i metodi di Data Dissemination basati sulla probabilità offrono vantaggi significativi nel risolvere la congestione e il broadcast storm, questi soffrono di alcuni problemi che dipendono dalla stima delle probabilità di invio. In generale queste tecniche si basano sulle informazioni locali dei veicoli, tuttavia, la disponibilità e l'accuratezza di queste informazioni possono essere influenzate da vari fattori, come la scarsità dei dati, l'affidabilità delle misurazioni o la mancanza di comunicazione con i nodi circostanti. Ciò potrebbe compromettere l'efficacia e l'adattabilità dei metodi. La mobilità dei veicoli può causare variazioni rapide nella topologia di rete, rendendo difficile la selezione dei destinatari ottimali. I metodi di diffusione adattiva delle informazioni richiedono la definizione di parametri per prendere decisioni di inoltro o ritrasmissione. Tuttavia, determinare in modo accurato tali parametri può essere complesso e soggetto a variazioni nelle condizioni di rete e nei requisiti delle applicazioni.

2.5.3 Cluster-Based Data Dissemination

In letteratura sono presenti tecniche di Data Dissemination che nascono con lo scopo di ottimizzare il carico e il traffico sulla rete. Come analizzato nelle sezioni precedenti, i nodi nelle VANET sono caratterizzati da connettività dinamica e funzionalità auto-organizzanti [39]. Tuttavia, a causa della mobilità estremamente elevata dei veicoli, la topologia cambia frequentemente. Questo comporta una riduzione del tempo di vita della connessioni aumentando l'overhead per i protocolli di routing. La soluzione più comune adottata per tale problema è la formazione di reti basate su cluster di veicoli [38] che prevedono la creazione di gruppi

ridotti di veicoli chiamati cluster. Per comunicare tra loro i nodi sfruttano due diversi tipi di protocolli di routing dipendenti dai destinatari della comunicazione: se la comunicazione deve avvenire all'interno del cluster di appartenenza allora utilizzano un routing "diretto" di tipo proattivo, viceversa, se la comunicazione è diretta a membri di cluster differenti questa richiede la creazione di un'infrastruttura di rete virtuale, ed in questo caso vengono utilizzati protocolli di routing di tipo reattivo. Il processo di clustering nelle VANET è la fase cruciale che consiste nell'organizzare i veicoli in gruppi basati su alcune regole o criteri distinti, quali la separazione tra i nodi, la velocità, la direzione, piani di viaggio condivisi, ecc, questo facilita la costruzione di reti gerarchiche. Nella Figura 2.7 è rappresentata una tipica struttura generata dal processo di clustering. Come si può notare i nodi vengono suddivisi in diversi gruppi virtuali, racchiusi in figura da cerchi tratteggiati. In questa tipologia di rete, i nodi possono assumere differenti ruoli come: *Cluster Head*, *Cluster Member* o *Cluster Gateway*.

- **Cluster Head** (CH): è il nodo responsabile della comunicazione all'interno di un cluster. Il CH ha il compito di assegnare la larghezza di banda e di coordinare i membri del cluster. In letteratura sono presenti varie tecniche per la selezione ottimale del CH;
- **Cluster Member** (CM): è un nodo ordinario all'interno di un cluster, gli unici collegamenti che può sfruttare sono quelli all'interno del cluster stesso;
- **Cluster Gateway** (GW): è il nodo che ha il compito di condividere le informazione tra i cluster. Inoltre, se due cluster vicini si sovrappongono, i GW sono i nodi si trovi tra due cluster, essi sono capaci di ascoltare i pacchetti trasmessi da entrambi CH, così da facilitare la diffusione inter-cluster.

Questo metodo di Data Disseminantion può essere appropriato in ambienti in cui vi sono necessarie esigenze di scalabilità, o la topologia della strada obbliga in maniera rigorosa i percorsi dei veicoli, quali autostrade. Quindi, l'obiettivo delle architetture basate su cluster è quello di ridurre il carico complessivo e migliorare l'efficienza delle comunicazioni tra nodi, sfruttando la struttura gerarchica dei nodi e la creazioni di reti virtuali così gestire in modo efficiente la Data Disseminantion. Secondo [40] i protocolli di routing basati sul clustering nelle VANET hanno bisogno di servizi diversi o complessi, per determinare i nodi all'interno di un determinato cluster. Inoltre, non è presente in letteratura un algoritmo di clustering globale per la formazione dei cluster. Quindi per gli obbiettivi imposti nella tesi, questa tecnica risulta essere posso adatta rispetto al modello basato sui Population Protocol.

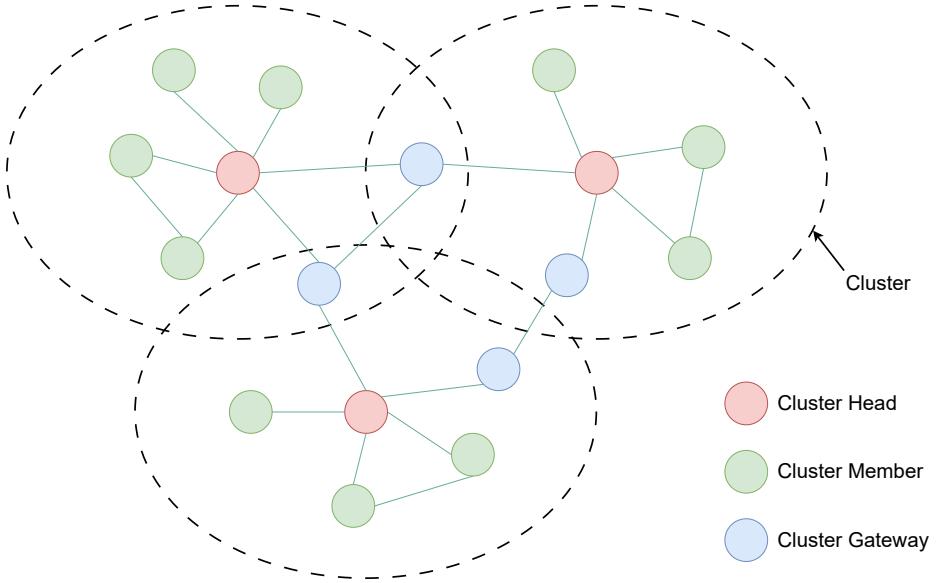

Figure 2.7: Struttura di una rete a Cluster.

2.5.4 Geocast-Based Data Dissemination

Molte applicazioni, specialmente quelle di sicurezza, richiedono che la Data Dissemination avvenga ad un gruppo di veicoli, e non ad un singolo nodo come avviene negli scambi unicast [36]. Pertanto, gli schemi multicast o broadcast diventano più efficienti in queste circostanze. Una specializzazione del problema può essere effettuata per quelle applicazioni come: avvisi di sicurezza del veicolo stesso, messaggi di avviso di collisione/incidente, questi normalmente sono di interesse per tutti quei veicoli presenti nella stessa area. In questi casi, abbiamo bisogno di protocolli che implementano la Data Dissemination in zone geograficamente ben definite. Una soluzione al problema è il geocast, una variante del multicast, che specifica una posizione geografica come posizione di destinazione. Quindi a differenza degli schemi multicast, i destinatari delle informazioni sono l'insieme dei nodi all'interno di un'area specifica. In altre parole, se un nodo si trova all'interno della regione geocast in un determinato momento, diventerà automaticamente uno dei nodi riceventi. In letteratura sono presenti diversi schemi che mirano ad implementare l'approccio geocast. Tra le prime soluzioni vi è lo schema *Location-Based Multicast (LBM)*, un metodo di flooding che limita lo spazio di inoltro dei pacchetti. In questo schema tutti i nodi appartenenti alla zona di inoltro, tra la sorgente e la zona di destinazione, sono responsabili dell'inoltro dei pacchetti. Il semplice flooding effettuato da questo schema e da i vari che ne derivano, comporta ritardi dovuti alle collisioni, poiché l'inoltro dei messaggi

non è controllato, ogni veicolo ricevente ritrasmette il messaggio a tutti i suoi vicini, generando un problema di broadcast storm.
Gli autori di [37] hanno presentato diversi approcci per il routing geocast efficiente tra cui:

- protocollo *Inter-Vehicular Geocast (IVG)*: lo scopo di IVG è quello di diffondere informazioni solo ai nodi presenti in una zona a rischio, a causa di pericoli stradali. Per raggiungere questo obiettivo, il protocollo seleziona dei *relay* tra i veicoli posizionati nell'area designata. Le zone a rischio vengono determinate tenendo conto della posizione degli ostacoli sulla strada e delle direzioni di guida che i nodi assumono. Nello specifico il protocollo nasce per la segnalazione di incidenti in autostrada, nel caso in cui si verifichi quest'evento, il veicolo danneggiato invia un messaggio a tutti i suoi vicini e questi avranno il compito di determinare la zona a rischio e i nodi *relay*;

- protocollo *Distributed Robust Geocast (DRG)*: questo protocollo basa l'inoltro delle informazioni sulla base di due zone geografiche. Determina una zona di rilevanza, detta ZOR, nella quale i messaggi di sicurezza sono ancora validi, ed una zona di inoltro (ZOF), della quale viene eletto un nodo relay scegliendolo tra i nodi più distanti;

- *Trajectory Based Dissemination (TBD)*: questo è un algoritmo di routing orientato ai beacon geocast. In questo algoritmo, i veicoli aggiornano le loro posizioni attraverso la rete cellulare così da costruire una conoscenza della distribuzione dei nodi all'interno della rete. La sorgente, per inviare il messaggio geocast, converte quindi la rete ottenuta in zone di dimensione pari al raggio di trasmissione, determina la densità all'interno di ogni zona dai messaggi beacon scambiati, così da selezionare il percorso che dovrà seguire il messaggio.

2.5.5 Hybrid-Based Data Dissemination

La Hybrid-Based Data Dissemination è una strategia di distribuzione dei dati che combina le diverse modalità definite precedentemente al fine di ottimizzare l'efficienza e la scalabilità della comunicazione. In letteratura sono presenti molti lavori che sfruttano le potenzialità di questi metodi [62, 63]. Proponendo soluzioni come la combinazione dell'approccio Cluster-Based con il Probability-Based, per la costruzione di una rete gerarchica dove si limita l'inoltro delle informazioni ridondanti, o attraverso l'uso di approcci come Delay e Probability-Based così da migliorare il rapporto di consegna dei pacchetti riducendo il ritardo nelle comunicazioni.

Negli approcci ibridi, è importante riconoscere che i vantaggi presenti comportano anche l'inclusione dei loro svantaggi associati:

- l'implementazione di un sistema ibrido può essere complessa e richiedere una gestione accurata. È necessario coordinare e sincronizzare le diverse modalità di trasmissione, adattandole dinamicamente in base alle condizioni di rete e ai requisiti dei dati;
- l'utilizzo di un approccio ibrido può introdurre un overhead aggiuntivo nella comunicazione. Ad esempio, l'uso di trasmissione multicast può richiedere la duplicazione dei pacchetti per raggiungere più destinazioni, aumentando il carico di rete;
- l'utilizzo di diverse modalità di trasmissione può portare alla necessità di implementare protocolli di routing ad hoc. Questi protocolli possono essere più complessi rispetto a quelli utilizzati in sistemi di diffusione dei dati più semplici. La progettazione e l'implementazione di tali protocolli può risultare una sfida piuttosto complessa.

2.6 Population Protocol

I Population Protocol (PP) [35] sono definiti come sistemi costituiti da un gran numero di semplici agenti identici, che interagiscono in modo casuale e aggiornano il proprio stato seguendo semplici regole. Una definizione formale che ricorre comunemente in letteratura è la seguente: *i population protocol sono un insieme di agenti in movimento che interagiscono tra loro per eseguire un processo computazionale* [9, 33, 32]. Inoltre, il paradigma dei population protocol può essere utilizzato per modellare reti ad-hoc di dispositivi mobili.
Volendo analizzare nel dettaglio il modello dei PP possiamo elencare le seguenti caratteristiche principali:

- **agenti anonimi**: gli agenti che compongono il modello sono nodi indistinguibili di una rete a stati finiti, programmati in modo identico che spesso vengono inizializzati con valori di default;
- **computazione**: l'aggiornamento dello stato per ogni nodo avviene tramite interazione diretta sfruttando delle tabelle di transizione. Gli agenti, nel modello matematico, non inviano messaggi né condividono memoria, mantenendo il meccanismo di interazione astratto.

- **scheduler imparziale**: le interazioni tra gli agenti avvengono in modo imprevedibile, i quali hanno scarso controllo sulla scelta dell'agente col quale interagire. In questo scenario gli agenti devono adattarsi a situazioni imprevedibili in cui gli incontri sono governati da regole o restrizioni esterne;
- **variabili distribuite**: l'input di un population protocol è distribuito nello stato iniziale dell'intera popolazione, allo stesso modo, l'output viene distribuito tra tutti gli agenti;
- **terminazione del processo**: gli agenti nei population protocol non sono in grado determinare quando il loro processo computazionale ha terminato, invece, gli output degli agenti devono convergere dopo un certo tempo finito a un valore comune e corretto.

Date le caratteristiche sopra elencate, ad ogni passo in cui si effettua un processo computazionale, viene selezionato un numero fisso di agenti in modo non deterministico e l'aggiornamento dei loro stati avviene attraverso una funzione di transizione congiunta. In generale, gli agenti in un population protocol seguono delle regole locali che determinano il loro comportamento in base alle informazioni disponibili. Attraverso l'interazione ripetuta tra gli agenti, il modello si evolve fino al raggiungimento di uno *Stato Globale*. In questo contesto, lo stato globale rappresenta l'informazione complessiva sullo stato del sistema, ottenuta aggregando le conoscenze individuali degli agenti contenute nei loro stati. Poiché gli agenti sono anonimi e quelli aventi gli stessi stati sono identici, lo stato globale di un processo computazionale è determinato solo dal contenuto dello stato locale di ogni agente e questo prende il nome di *configurazione* [34], la quale può essere rappresentata come un vettore di tutti gli stati degli agenti appartenenti al quel processo. L'esecuzione di un protocollo procede dalla configurazione iniziale, attraverso le interazioni tra gli agenti, con la generazione di infinite configurazioni. Lo scopo dell'esecuzione dei population protocol è quello di raggiungere la convergenza tra gli stati degli agenti così da produrre l'output corretto.
Le interazioni che svolgono gli agenti nei PP, come detto precedentemente, vengono gestite da un meccanismo di schedulazione che deve rispettare un vincolo detto *fairness condition* (vincolo di equità). Questo vincolo garantisce che gli agenti della popolazione abbiano le stesse probabilità di partecipare alle interazioni così che il protocollo faccia progressi in modo bilanciato. Il meccanismo di schedulazione, in questo modo, deve garantire che nessun agente venga ignorato durante le interazioni. In pratica, il vincolo di equità richiede che ogni agente abbia la possibilità di interagire con altri agenti nel corso del tempo, senza favoritismi o discriminazioni.

Ciò garantisce una distribuzione equa delle risorse e una partecipazione equa di tutti gli agenti, promuovendo l'efficienza e la correttezza del population protocol.

2.6.1 Population Protocol base

Nella letteratura sono stati proposti diversi modelli di PP che si distinguono dal modello base per quanto riguarda gli attori coinvolti o al meccanismo che determina le interazioni.
Il modello base può essere descritto formalmente da i seguenti parametri: Q, Σ, ι, ω, δ. Dove:

- Q: corrisponde all'insieme di possibili stati che gli agenti possono assumere;
- Σ: è un alfabeto finito di possibili valori di input;
- ι: è la funzione di inizializzazione degli agenti che, preso in input un simbolo da Σ inizializza l'agente con uno stato contenuto in Q;
- ω: è detta funzione di output, che mappa ogni stato appartenente a Q con uno dei possibili valori di output. Questo valore rappresenta il risultato raggiunto dall'agente durante l'esecuzione del processo;
- δ: la funzione di transizione che mette in relazione una coppia di stati di agenti che hanno interagito, causando il passaggio di stato.

2.6.2 Population Protocol one-way

Una delle varianti proposte in letteratura per i sistemi di population protocol utilizza come forma di comunicazione il paradigma one-way, analogo ai modelli tradizionali di comunicazione asincrona basati sullo scambio di messaggi [9]. Nei popupation protocol di base, si presume che due agenti per poter eseguire la propria funzione di transazione, devono effettuare uno scambio reciproco dello stato, ciò può avvenire solo sfruttando una comunicazione bidirezionale tra i due agenti. Nei sistemi di tipo one-way, le interazioni tra gli agenti, possono essere suddivise in due step: eventi di invio e eventi di ricezione, che coinvolgono al più un singolo agente. Questi modelli potrebbero essere più adeguati per la rappresentazione della comunicazione nelle reti distribuite quali reti di sensori, reti MANET e VANET, in cui la comunicazione radio potrebbe non essere sempre bidirezionale, anche tra agenti prossimi. Quindi, con la comunicazione unidirezionale, solo il ricevente apprende informazioni dallo stato del mittente, non avviene il

viceversa.
Il ricevente è in grado di ottenere lo stato del mittente, mentre il mittente non ha accesso alle informazioni sullo stato del ricevente. Esistono due modelli principali che descrivono questa comunicazione: il *modello di trasmissione* e il *modello di osservazione*. Nel modello di trasmissione, il mittente è consapevole dell'avvenuta interazione e può aggiornare il proprio stato, quindi può applicare la funzione di transizione, anche se questa non dipende dallo stato del nodo ricevente. Nel modello di osservazione, invece, il ricevente osserva passivamente lo stato del mittente. Un altro aspetto da considerare è se l'interazione avviene in modo istantaneo o richiede un certo intervallo di tempo anche in questo caso possiamo distinguere due casi: *modello a trasmissione immediata* e *modello a trasmissione ritardata*. Nei modelli a trasmissione immediata, l'interazione si verifica istantaneamente, senza ritardi significativi, questi sono i modelli più simili al population protocol base dove gli eventi di invio e ricezione avvengono contemporaneamente. Tale tipologia gestisce meglio le interazioni tra agenti. Al contrario, nei modelli a trasmissione ritardata, l'interazione richiede un intervallo di tempo specificato, ma i riceventi possono rifiutare i messaggi in arrivo così da non essere congestionati da messaggi.

2.7 Sistemi di gestione della fiducia-reputazione

Le VANET, come già anticipato precedentemente, sono reti costituite da un gran numero di veicoli che cooperano scambiandosi informazioni. Questa cooperazione è utile per migliorare la sicurezza stradale, il comfort e i servizi di infotainment. Nelle sezioni precedenti sono già stati presentati diversi lavori che mostrano schemi efficienti per la diffusione di informazioni. Tuttavia, la natura aperta e non affidabile di queste reti presenta sfide significative che devono essere affrontate per garantire sicurezza nelle informazioni scambiate tra i veicoli. In particolare, un problema reale diventa la gestione dei dati inaffidabili, cioè quelli raccolti da utenti che hanno sensori imprecisi o rumorosi o, nel peggiore dei casi, esibiscono deliberatamente un comportamento malevolo (ad esempio, inviando false informazioni al sistema per compromettere il servizio) [10]. Negli scenari distribuiti tradizionali, le tecniche di gestione della fiducia basate sulla reputazione degli utenti o sulla fiducia nei dati che condividono sono state sempre più utilizzate per gestire gli utenti non affidabili. Tali meccanismi consentono di tenere conto della storia delle precedenti transazioni con gli attori della comunicazione per valutare l'affidabilità delle informazioni appena diffuse. La fiducia può essere considerata come un attributo multidimensionale associato a un'entità o ad un informazione e può utilizzato per decidere se considerarla

o meno affidabile [41].

La presente sezione si concentra sull'analisi delle tecniche e degli algoritmi utilizzati nei sistemi di gestione della fiducia e reputazione nelle reti veicolari. Saranno mostrate le diverse metodologie e strategie utilizzate per la gestione della reputazione diversificando in base al target del sistema, fornendo un'analisi delle loro caratteristiche, vantaggi e limitazioni.

2.7.1 Sistemi di gestione della fiducia Entity-based

I sistemi di gestione della fiducia di tipo Entity-based associano il concetto di fiducia ai soli nodi della rete. Il loro obbiettivo è valutare l'affidabilità dei nodi che partecipano ai processi di rounting. In questo modo sono capaci di riconoscere nodi malevoli tra e partecipanti e decidere se escluderli dalla rete o isolati. Alcuni di questi approcci, presenti nella letteratura si basano principalmente su metriche di reputazione. Pertanto, per calcolare il valore di fiducia di un nodo, questi si basano principalmente su metriche legate alla conoscenza passata, come l'esperienza del nodo nel tempo in relazione al comportamento percepito e alle attività, e sulle raccomandazioni scambiate tra le diverse entità. Altri lavori invece, oltre alle metriche basate sulla reputazione, considerano il fattore di similarità. Quest'ultimo si riferisce alle entità che hanno le stesse proprietà, come ad esempio nodi appartenenti allo stesso cluster in un protocollo di tipo Cluster-based Data Dissemination.

Tra i vari lavori presenti in letteratura vengono riportati alcuni esempi: gli autori di [42] propongono un modello di fiducia che utilizza la fiducia diretta basata su fattori quali la velocità di consegna dei pacchetti (PDR) e il ritardo medio di consegna (ADD). Questi fattori, che indicano le caratteristiche fisiche delle comunicazioni e dei collegamenti di rete, sono utilizzati indirettamente per calcolare la fiducia di un nodo.

Un esempio di approccio basato sulla similarità è presentato dagli autori in [43]. L'obbiettivo del loro lavoro è quello di riuscire a individuare l'iniezione di falsi messaggi di eventi di sicurezza provenienti da veicoli anomali. Per valutare le somiglianza, sfruttano i messaggi beacon inviati dai nodi, così da analizzare i loro valori di velocità e posizione.

Alcune tecniche di gestione della fiducia per scenari autostradali sono state affrontate dagli autori in [70] dove propongono REPLACE, uno schema di raccomandazione affidabile basato sulla fiducia del servizio di platooning. È un modello di guida in cui veicoli con obiettivi comuni si muovono in modo cooperativo. L'obiettivo finale di REPLACE è quello di raccomandare un leader di plotone affidabile per il servizio di platooning. Il modello REPLACE utilizza un sis-

tema di reputazione centralizzato per calcolare i punteggi sfruttando i feedback degli utenti. Per mitigare il potenziale impatto dei feedback provenienti da nodi maligni, gli autori propongono un algoritmo di filtraggio iterativo. La sicurezza del sistema proposto si basa su tecniche crittografiche come la crittografia a chiave pubblica e l'accordo sulla chiave di sessione tra veicoli e RSU. Tuttavia, come nella maggior parte dei meccanismi di gestione della fiducia centralizzati che sfruttano tecniche crittografiche, è necessario uno sforzo infrastrutturale. Di conseguenza, i valori di fiducia vengono aggiornati iterativamente dal server e poi distribuiti.

2.7.2 Data-based trust management

Analizzando gli approcci di tipo Data-based, la fiducia è legata al contenuto del messaggio scambiato. Questo vuol dire che il valore di fiducia dipende sull'autenticità e qualità dei dati e non sulla reputazione dell'agente che li ha generati [44]. Alcuni modelli di fiducia, per valutare la trust del dato scambiato, si basano sull'utilità del suo contenuto informativo. L'utilità è considerata come l'unità di misura che specifica il valore di un evento rispetto ad un altro ricevuto nello stesso contesto. In letteratura vi sono sistemi che valutano questa metrica sfruttando caratteristiche dell'evento comunicato come il tempo, la vicinanza, la categoria e il ruolo del nodo [45]. Pertanto, i sistemi di gestione della fiducia Data-based possono essere distinti in metodi orientati alle informazioni e metodi orientati agli eventi.
Un altro aspetto considerato per valutare la fiducia del contenuto dei dati è la similarità. Inizialmente, la similarità si riferisce alla corrispondenza dei contenuti dei dati scambiati, ad esempio in termini di tempo e vicinanza. Questo approccio aiuta a ridurre la quantità di dati trasmessi e assicura che siano diffusi solo contenuti utili. Tuttavia, con questo modello di valutazione, non è possibile valutare l'affidabilità di ogni parte dei messaggi scambiati.

Gli autori di [48] hanno presentato uno schema per rilevare i nodi maligni nelle VANET che sfrutta la similarità dei messaggi. L'idea generale è che ogni nodo ha il compito di calcolare una metrica che indica le caratteristiche generali dell'andamento del veicolo (velocità, posizione e informazioni sul traffico circostante), questa viene indicata come *valore di flusso*. Ottenuto tale valore, ogni nodo lo inoltra ai veicoli vicini, così da confrontarsi con il vicinato. Quando riceve un messaggio (contenente un valore di flusso), il veicolo lo confronta con il valore da esso calcolato. Successivamente, il contenuto del messaggio ricevuto sarà preso in considerazione solo se il valore di flusso del nodo sorgente è simile a quello del nodo destinatario e rispetta il modello di traffico veicolare. Viceversa, segnalerà il nodo mittente come malevolo.

Gli autori in [52] hanno presentato una tecnica di gestione della fiducia per la rilevazione delle intrusioni nelle VANET. In questo approccio, la valutazione della fiducia viene determinata per ogni messaggio ricevuto riguardante un evento specifico. Queste misurazioni vengono effettuate su parametri come la posizione dell'evento, il tempo di generazione dei dati e la correttezza della posizione del nodo mittente. Lo schema valuta la correttezza della posizione con algoritmi che sfruttano misure come la distanza e il tempo di invio. Questo schema introduce un grande ritardo nella comunicazione che non è accettabile per le applicazioni di sicurezza VANET.

Considerando questi aspetti nei modelli che sfruttano solo le informazioni scambiate, si può affermare che la scarsità dei dati, uno degli aspetti presenti nelle VANET, rappresenta il principale problema per questa classe di approcci. Ciò significa che può essere difficile ottenere una quantità sufficiente di dati affidabili per supportare le decisioni o le azioni basate sui dati.

2.7.3 Sistemi di gestione della fiducia Hybrid-based

I sistemi di gestione della fiducia di tipo Hybrid-based si basano sulla fiducia sia dell'entità sia dei dati scambiati, per un calcolo della fiducia più efficiente. L'obbiettivo è quello di sfruttare l'affidabilità dell'entità per la valutazione del valore di fiducia dei dati, inoltre, vengono anche sfruttate tecniche di raccomandazione per valutate la fiducia del contenuto dei dati che è stato valutato come affidabile da entità fidate. Tra i lavori presenti in fiducia vengono presentati i seguenti lavori:

in [53], gli autori propongono uno schema di gestione della fiducia resistente agli attacchi (ART) che mira a valutare l'affidabilità dei nodi e dei messaggi per far fronte agli attacchi nelle VANET. L'affidabilità dei dati è stimata sulla base dei dati raccolti da più veicoli. Mentre, l'affidabilità di un nodo è misurata in base alla sua fiducia funzionale (cioè la probabilità che un nodo soddisfi la sua funzionalità) e alla fiducia nelle raccomandazioni (cioè la probabilità che le raccomandazioni di un nodo siano affidabili).

Un framework che ha il compito di stimare la densità del traffico, di calcolare la fiducia tra le entità e di distribuire i nodi maligni in una rete è stato proposto in [54]. Questi nodi possono essere esclusi dalla rete sfruttando diverse metriche di fiducia, ad esempio la fiducia basata su RSU, eventi, fiducia diretta e indiretta. Il meccanismo di diffusione utilizzato prevede uno scambio periodico di valori di fiducia globali, aggiungendo nuovi campi ai messaggi dei beacon. Tuttavia, gli autori ipotizzano che i nodi maligni nella rete abbiano sempre un comportamento disonesto, ma questo potrebbe non essere probabile in un ambiente reale.

Il recente lavoro proposto in [69] sfrutta le tecniche di clustering per eleggere un cluster head (CH) responsabile dell'invio di informazioni attendibili nella rete. Purtroppo, il principale svantaggio di questo approccio è la possibilità di eleggere CH disonesti quando la maggioranza dei nodi è disonesta [68].

A differenza di altri lavori proposti nella letteratura recente che basano il meccanismo di controllo della QoS su un'infrastruttura o su entità fidate che potrebbero non essere sempre disponibili, nell'approccio multilivello proposto la comunicazione è realizzata in modo completamente distribuito attraverso un sistema basato su Population Protocol in cui le informazioni sugli eventi vengono diffuse solo dopo essere state opportunamente filtrate da un modulo di reputazione. Il meccanismo di reputazione sfrutta sia le informazioni acquisite direttamente attraverso il livello sensoriale, sia le informazioni di riferimento opportunamente ponderate. Nella sezione sperimentale, oltre a dimostrare l'efficacia dell'approccio, verranno misurate anche le prestazioni del sistema in scenari di attacco diversi e gradualmente crescenti.

Chapter 3

Sistema proposto

In questa capitolo viene presentata l'architettura del sistema, che ha il compito di diffondere informazioni tra i nodi di una rete VANET al fine di garantire la fruizione di servizi utili all'utente. L'architettura sfrutta i population protocol e solamente le comunicazioni V2V per effettuare la Data Dissemination, inoltre, all'interno del sistema viene impiegato un modello di reputazione distribuito al fine di valutare l'affidabilità delle informazioni condivise tra i partecipanti della rete VANET. Tale modello di reputazione consente di stimare l'affidabilità dei veicoli stessi, contribuendo a una valutazione più accurata delle informazioni trasmesse da essi.

3.1 Architettura multi livello

OMISSISS

3.2 Sensing layer

OMISSIS

3.3 Communication Layer

OMISSIS

3.4 Modello di reputazione

OMISSIS

3.5 Modello di diffusione dei dati

OMISSIS

3.6 Application layer

OMISSIS

Chapter 4

Valutazione sperimentale

Questa capitolo è dedicato all'illustrazione dei risultati ottenuti dalla valutazione sperimentale della soluzione proposta. Attraverso questa valutazione, si dimostra che la soluzione è adeguata per facilitare e rendere affidabile la diffusione di eventi utili in scenari veicolari. Inoltre, si evince che la soluzione dimostra resilienza anche in presenza di attacchi alla sicurezza effettuati da nodi organizzati opportunisticamente per danneggiare il sistema.
La valutazione sperimentale è stata condotta attraverso l'ambiente di simulazione VEINS. Durante queste simulazioni, sono stati considerati fattori come la densità del traffico, la velocità dei veicoli e la distribuzione degli eventi nello scenario.

4.1 Ambiente di simulazione

OMISSIS

4.2 Metriche di valutazione

OMISSIS

4.3 Calibrazione delle scelte progettuali

OMISSIS

4.4 Impostazione sperimentale

OMISSIS

4.5 Risultati sperimentali

OMISSIS

Chapter 5

Conclusioni

Con la progressiva diffusione delle moderne smart city, i sistemi di trasporto intelligenti sono diventati una componente principale per la gestione intelligente dei veicoli. Questi sistemi stanno diventando sempre più importanti in quanto cercano di migliorare la viabilità delle strade con l'obiettivo di garantire la sicurezza nelle strade. Inoltre, consentono l'interazione dei veicoli con diverse entità stradali e con altri veicoli tramite comunicazione Vehicle-to-Infrastructure e Vehicle-to-Vehicle, così da facilitare l'implementazione di applicazioni veicolari sia critiche come le applicazioni di sicurezza, che non critiche, come l'infotainment. Tuttavia, a causa delle caratteristiche peculiari delle reti veicolari, le entità che ne fanno parte sono estremamente vulnerabili e soggette a un'ampia gamma di potenziali attacchi. Per tali motivi l'obiettivo principale è garantire comunicazioni efficienti ed affidabili all'interno della rete veicolari. Per fare ciò, è necessario implementare misure di sicurezza che possano rilevare e prevenire gli attacchi, garantendo al contempo un funzionamento efficiente e affidabile del sistema.

Per raggiungere tali obiettivi questo lavoro di tesi propone uno schema di rilevamento e diffusione degli eventi affidabile per le VANET basato sui Population Protocol e su un sistema di gestione della reputazione. Nello schema proposto, l'affidabilità degli eventi e dei nodi viene valutata utilizzando due metriche distinte, rispettivamente la fiducia locale negli eventi e la reputazione dei nodi. La fiducia locale negli eventi viene utilizzata per valutare l'affidabilità degli eventi ricevuti dai veicoli nella rete. Inoltre, la reputazione dei nodi indica l'affidabilità dei nodi all'interno delle VANET. Nel sistema proposto, la gestione della reputazione è completamente distribuita sui veicoli e non dipende dalla topologia della rete e dalla densità delle RSU distribuite nella rete. Per convalidare e valutare le prestazioni del sistema, sono stati condotti diversi

esperimenti che hanno dimostrato che il sistema proposto è in grado di discriminare gli eventi dannosi generati e propagati da gruppi di veicoli organizzati per rendere l'attacco più efficace in un tempo ragionevole.

Mentre le tecniche di Data Dissemination negli ambienti distribuiti sono state ampiamente studiate, i sistemi di gestione della reputazione totalmente distribuiti rappresentano uno scenario in continua evoluzione. Di conseguenza, i potenziali lavori futuri riguardano le sfide ancora aperte relativi nei modelli di fiducia per le reti veicolari, tra le quali:

- *soglie di fiducia adattive*: i sistemi di gestione della fiducia esistenti, come quello proposto, utilizzano soglie per distinguere nodi o informazioni malevoli da quelli benigni. Nei lavori esistenti in letteratura, i ricercatori si sono principalmente concentrati sull'utilizzo di soglie statiche per questo scopo. Lo stesso approccio è stato utilizzato nel lavoro di tesi proposto. Tuttavia come implementazione futura, è importante considerare la possibilità di sviluppare un meccanismo che renda il calcolo della soglia di fiducia adattivo con l'obiettivo di identificare accuratamente, in diversi scenari stradali, nodi ed informazioni malevoli;

- *durata del punteggio di reputazione di un nodo*: nel sistema proposto i veicoli all'interno della rete memorizzano i valori di reputazione dei nodi vicini con cui interagiscono lungo il loro percorso. La quantità di informazioni che riescono a mantenere è limitata e constante. Questo dipende dall'uso di una memoria che mantiene i dati di interazione relativi all'ultima finestra temporale T. Tuttavia, data la natura estremamente dinamica delle reti veicolari, i nodi potrebbero entrare in contatto con un gran numero di veicoli vicini, rendendo impraticabile per ciascun di essi memorizzare e aggiornare la reputazione dei vari veicoli con cui hanno interagito in passato. In particolare, l'aggiornamento dei valori di reputazione richiede di determinare la durata degli stessi per ogni nodo, e servono tecniche di decadimento dopo un determinato intervallo di tempo, specialmente quando non vi è alcuna nuova interazione col nodo in esame. Pertanto, sono utili meccanismi intelligenti in grado di calcolare la durata della reputazione dinamicamente e individuare la percentuale di decadimento della reputazione sulla base delle interazioni passate;

- *sistema di raccomandazione*: il sistema di gestione della fiducia proposto sfrutta la conoscenza locale per calcolare le metriche utili a valutare le informazioni diffuse, non avviene quindi alcuno scambio diretto dei valori di reputazione calcolati tra gli agenti. Tuttavia, in una versione futura del sistema, si potrebbe prevedere l'implementazione di uno

scambio dei valori di reputazione tra gli agenti stessi, che consentirebbe una diffusione degli eventi accompagnati dai loro valori di incertezza.

List of Figures

2.1 Struttura della rete VANET. 8
2.2 Banda e canali dello spettro DSRC negli Stati Uniti. 11
2.3 Stack protocollare DSRC. 12
2.4 Comunicazioni nelle VANET. 13
2.5 Struttura di una rete fully connected generata con comunicazione V2V. 15
2.6 Struttura di una rete sparsa generata con comunicazione V2V. 16
2.7 Struttura di una rete a Cluster. 22

List of Tables

Bibliografia

[1] T. S. Darwish and K. A. Bakar. "Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues". In: *IEEE Access* 6 (2018), pp. 15679–15701.

[2] M. S. Anwer and C. Guy. "A survey of VANET technologies". In: *Journal of Emerging Trends in Computing and Information Sciences* 5.9 (2014), pp. 661–671.

[3] F. Belamri, S. Boulfekhar, and D. Aissani. "A survey on QoS routing protocols in Vehicular Ad Hoc Network (VANET)". In: *Telecommunication Systems* 78.1 (2021), pp. 117–153.

[4] S. Singh and S. Agrawal. "VANET routing protocols: Issues and challenges". In: *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (2014), pp. 1–5.

[5] T. Nadeem, P. Shankar, and L. Iftode. "A comparative study of data dissemination models for VANETs". In: *2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*. IEEE. 2006, pp. 1–10.

[6] V. Agate, A. De Paola, G. Lo Re, and M. Morana. "A platform for the evaluation of distributed reputation algorithms". In: *2018 IEEE/ACM 22nd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*. IEEE. 2018, pp. 1–8.

[7] X. Huang, R. Yu, J. Kang, and Y. Zhang. "Distributed reputation management for secure and efficient vehicular edge computing and networks". In: *IEEE Access* 5 (2017), pp. 25408–25420.

[8] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni. "Trust management for vehicular networks: An adversary-oriented overview". In: *IEEE Access* 4 (2016), pp. 9293–9307.

[9] J. Aspnes and E. Ruppert. “An introduction to population protocols”. In: *Middleware for Network Eccentric and Mobile Applications* (2009), pp. 97–120.

[10] V. Agate, A. De Paola, G. Lo Re, and M. Morana. “A simulation software for the evaluation of vulnerabilities in reputation management systems”. In: *ACM Transactions on Computer Systems (TOCS)* 37.1-4 (2021), pp. 1–30.

[11] S. Abduljabbar Rashid, l. Audah, M. Maad Hamdi, and S. Alani. “An Overview on Quality of Service and Data Dissemination in VANETs”. In: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2020, pp. 1–5.

[12] M. M. Rathore, S. Attique Shah, A. Awad, D. Shukla, S. Vimal, and A. Paul. “A cyber-physical system and graph-based approach for transportation management in smart cities”. In: *Sustainability* 13.14 (2021), p. 7606.

[13] M. Lee and T. Atkison. “Vanet applications: Past, present, and future”. In: *Vehicular Communications* 28 (2021), p. 100310.

[14] D. Jiang and L. Delgrossi. “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments”. In: *VTC Spring 2008 - IEEE Vehicular Technology Conference*. 2008, pp. 2036–2040.

[15] J. B. Kenney. “Dedicated Short-Range Communications (DSRC) Standards in the United States”. In: *Proceedings of the IEEE* 99.7 (2011), pp. 1162–1182.

[16] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar. “Broadcasting in VANET”. In: *2007 mobile networking for vehicular environments*. IEEE. 2007, pp. 7–12.

[17] M. M. Hamdi, O. A. R. Al-Dosary, O. A. S. Alrawi, A. S. Mustafa, M. S. Abood, and M. S. Noori. “An overview of challenges for data dissemination and routing protocols in VANETs”. In: *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. 2021, pp. 1–6.

[18] S. Yousefi, M. S. Mousavi, and M. Fathy. “Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives”. In: *2006 6th International Conference on ITS Telecommunications*. 2006, pp. 761–766.

[19] H. Shahwani, S. A. Shah, M. Ashraf, M. Akram, J. P. Jeong, and J. Shin. "A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks". In: *Vehicular Communications* 34 (2022), p. 100420.

[20] S. Bayan and U. Mohammad. "A Survey of Data Dissemination Schemes in Secure Inter-Vehicle Communications". In: *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 2023, pp. 1224–1230.

[21] P. K. Shrivastava and L. Vishwamitra. "Comparative analysis of proactive and reactive routing protocols in VANET environment". In: *Measurement: Sensors* 16 (2021), p. 100051.

[22] A. T. Akabane, R. W. Pazzi, E. R. Madeira, and L. A. Villas. "Carro: A context-awareness protocol for data dissemination in urban and highway scenarios". In: *2016 8th IEEE Latin-American Conference on Communications (LATINCOM)*. IEEE. 2016, pp. 1–6.

[23] J. B. D. da Costa, A. M. de Souza, D. Rosário, E. Cerqueira, and L. A. Villas. "Efficient data dissemination protocol based on complex networks' metrics for urban vehicular networks". In: *Journal of Internet Services and Applications* 10 (2019), pp. 1–13.

[24] M. Chaqfeh, A. Lakas, and I. Jawhar. "A survey on data dissemination in vehicular ad hoc networks". In: *Vehicular Communications* 1.4 (2014), pp. 214–225.

[25] I. Achour, T. Bejaoui, A. Busson, and S. Tabbane. "Delay-based strategy for safety message dissemination in Vehicular Ad hoc NETworks: Slotted or continuous?" In: *2016 international wireless communications and mobile computing conference (IWCMC)*. IEEE. 2016, pp. 268–274.

[26] V. Agate, A. R. Khamesi, S. Silvestri, and S. Gaglio. "Enabling peer-to-peer User-Preference-Aware Energy Sharing Through Reinforcement Learning". In: *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. 2020.

[27] V. Agate, F. Concone, and P. Ferraro. "A Resilient Smart Architecture for Road Surface Condition Monitoring". In: *The Proceedings of the International Conference on Smart City Applications*. Springer. 2021, pp. 199–209.

[28] P. Ferraro and G. Lo Re. "Designing ontology-driven recommender systems for tourism". In: *Advances onto the Internet of Things*. Springer, 2014, pp. 339–352.

[29] C. Sommer, R. German, and F. Dressler. "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis". In: *IEEE Transactions on Mobile Computing (TMC)* 10.1 (2011), pp. 3–15.

[30] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner. "Microscopic traffic simulation using sumo". In: *2018 21st international conference on intelligent transportation systems (ITSC)*. IEEE. 2018, pp. 2575–2582.

[31] A. Varga and R. Hornig. "An overview of the OMNeT++ simulation environment". In: *1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*. 2010.

[32] O. Michail, I. Chatzigiannakis, and P. G. Spirakis. "Mediated population protocols". In: *Theoretical Computer Science* 412.22 (2011), pp. 2434–2450.

[33] D. Alistarh, R. Gelashvili, and M. Vojnović. "Fast and exact majority in population protocols". In: *Proceedings of the 2015 ACM Symposium on Principles of Distributed Computing*. 2015, pp. 47–56.

[34] J. Esparza, P. Ganty, J. Leroux, and R. Majumdar. "Verification of population protocols". In: *Acta Informatica* 54.2 (2017), pp. 191–215.

[35] D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, and R. Peralta. "Computation in networks of passively mobile finite-state sensors". In: *Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing*. 2004, pp. 290–299.

[36] J. Chennikara-Varghese, W. Chen, O. Altintas, and S. Cai. "Survey of Routing Protocols for Inter-Vehicle Communications". In: *2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking e Services*. 2006, pp. 1–5.

[37] S. Allal and S. Boudjit. "Geocast routing protocols for vanets: Survey and guidelines". In: *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. IEEE. 2012, pp. 323–328.

[38] A. Abuashour and M. Kadoch. "Performance Improvement of Cluster-Based Routing Protocol in VANET". In: *IEEE Access* 5 (2017), pp. 15354–15371.

[39] S. T. Hasson and A. T. Abbas. “A clustering approach to model the data dissemination in VANETs”. In: *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*. IEEE. 2021, pp. 337–342.

[40] A. Srivastava, N. Bagga, and M. Rakhra. “Analysis of Cluster-Based and Position-based Routing Protocol in VANET”. In: *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 2021, pp. 1–5.

[41] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato. “A Survey of Trust and Reputation Management Systems in Wireless Communications”. In: *Proceedings of the IEEE* 98.10 (2010), pp. 1755–1772.

[42] S. Tan, X. Li, and Q. Dong. “A trust management system for securing data plane of ad-hoc networks”. In: *IEEE Transactions on Vehicular Technology* 65.9 (2015), pp. 7579–7592.

[43] H. Al Falasi and N. Mohamed. “Similarity-based trust management system for detecting fake safety messages in vanets”. In: *Internet of Vehicles-Safe and Intelligent Mobility: Second International Conference, IOV 2015, Chengdu, China, December 19-21, 2015, Proceedings 2*. Springer. 2015, pp. 273–284.

[44] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee, and S. Mandala. “Trust management in vehicular ad hoc network: a systematic review”. In: *EURASIP Journal on Wireless Communications and Networking* 2015 (2015), pp. 1–22.

[45] J. Zhang. “A Survey on Trust Management for VANETs”. In: *2011 IEEE International Conference on Advanced Information Networking and Applications*. 2011, pp. 105–112.

[46] V. Agate, A. De Paola, G. Lo Re, and M. Morana. “Vulnerability Evaluation of Distributed Reputation Management Systems”. In: *InfQ 2016 - New Frontiers in Quantitative Methods in Informatics*. ICST, Brussels, Belgium: ICST, 2016, pp. 1–8.

[47] V. Agate, A. De Paola, G. Lo Re, and M. Morana. “A simulation framework for evaluating distributed reputation management systems”. In: *Distributed Computing and Artificial Intelligence, 13th International Conference*. Springer. 2016, pp. 247–254.

[48] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan. “Data-centric rogue node detection in VANETs”. In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE. 2014, pp. 398–405.

[49] A. De Paola, P. Ferraro, S. Gaglio, G. Lo Re, and S. K. Das. "An adaptive bayesian system for context-aware data fusion in smart environments". In: *IEEE Transactions on Mobile Computing* 16.6 (2016), pp. 1502–1515.

[50] V. Agate, P. Ferraro, and S. Gaglio. "A Cognitive Architecture for Ambient Intelligence Systems". In: *AIC*. 2018, pp. 52–58.

[51] V. Agate, A. De Paola, S. Gaglio, G. Lo Re, and M. Morana. "A framework for parallel assessment of reputation management systems". In: *Proceedings of the 17th International Conference on Computer Systems and Technologies 2016*. 2016, pp. 121–128.

[52] R. A. Shaikh and A. S. Alzahrani. "Intrusion-aware trust model for vehicular ad hoc networks". In: *Security and communication networks* 7.11 (2014), pp. 1652–1669.

[53] W. Li and H. Song. "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks". In: *IEEE transactions on intelligent transportation systems* 17.4 (2015), pp. 960–969.

[54] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni. "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS". In: *Computer Communications* 93 (2016), pp. 68–83.

[55] S. Latif, S. Mahfooz, B. Jan, N. Ahmad, Y. Cao, and M. Asif. "A comparative study of scenario-driven multi-hop broadcast protocols for VANETs". In: *Vehicular Communications* 12 (2018), pp. 88–109.

[56] A. Srivastava, A. Prakash, and R. Tripathi. "Fuzzy-based beaconless probabilistic broadcasting for information dissemination in urban VANET". In: *Ad Hoc Networks* 108 (2020), p. 102285.

[57] L. Zhou. "NPPB: A broadcast scheme in dense VANETs". In: *Information Technology J.* 9.2 (2010), pp. 247–256.

[58] M. Bakhouya, J. Gaber, and P. Lorenz. "An adaptive approach for information dissemination in vehicular ad hoc networks". In: *Journal of Network and Computer Applications* 34.6 (2011), pp. 1971–1978.

[59] A. Naja, M. Boulmalf, and M. Essaaidi. "A distributed priority-based rebroadcasting protocol for VANETs: mitigating the storm problem". In: *Mobile Networks and Applications* 24 (2019), pp. 1555–1568.

[60] V. Agate, F. M. D'Anna, A. De Paola, P. Ferraro, G. Lo Re, and M. Morana. "A Behavior-Based Intrusion Detection System Using Ensemble Learning Techniques." In: *ITASEC*. 2022.

[61] R. Tizvar and M. Abbaspour. "A density-aware probabilistic interest forwarding method for content-centric vehicular networks". In: *Vehicular Communications* 23 (2020), p. 100216.

[62] J. Sospeter, D. Wu, S. Hussain, and T. Tesfa. "An effective and efficient adaptive probability data dissemination protocol in VANET". In: *Data* 4.1 (2018), p. 1.

[63] L. Liu, C. Chen, T. Qiu, M. Zhang, S. Li, and B. Zhou. "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs". In: *Vehicular Communications* 13 (2018), pp. 78–88.

[64] A. Timilsina, A. R. Khamesi, V. Agate, and S. Silvestri. "A Reinforcement Learning Approach for User Preference-aware Energy Sharing Systems". In: *IEEE Transactions on Green Communications and Networking* (2021).

[65] A. De Paola, P. Ferraro, S. Gaglio, G. Lo Re, M. Morana, M. Ortolani, and D. Peri. "A context-aware system for ambient assisted living". In: *International Conference on Ubiquitous Computing and Ambient Intelligence*. Springer. 2017, pp. 426–438.

[66] A. De Paola, P. Ferraro, G. Lo Re, M. Morana, and M. Ortolani. "A fog-based hybrid intelligent system for energy saving in smart buildings". In: *Journal of Ambient Intelligence and Humanized Computing* 11.7 (2020), pp. 2793–2807.

[67] V. Agate, A. De Paola, P. Ferraro, G. Lo Re, and M. Morana. "SecureBallot: A secure open source e-Voting system". In: *Journal of Network and Computer Applications* 191 (2021).

[68] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu. "NOTRINO: A NOvel Hybrid TRust Management Scheme for INternet-of-Vehicles". In: *IEEE Transactions on Vehicular Technology* 70.9 (2021), pp. 9244–9257.

[69] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui. "A Hybrid Trust Management Heuristic for VANETs". In: *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. 2019, pp. 748–752.

[70] H. Hu, R. Lu, Z. Zhang, and J. Shao. "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET". In: *IEEE Transactions on Vehicular Technology* 66.2 (2016), pp. 1786–1797.

[71] A. Bordonaro, A. De Paola, and G. Lo Re. "VPP: A Communication Schema for Population Protocols in VANET". In: *2021 20th International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS)*. 2021, pp. 11–18.

[72] N. Khatri, S. Lee, A. Mateen, and S. Y. Nam. "Event Message Clustering Algorithm for Selection of Majority Message in VANETs". In: *IEEE Access* 11 (2023), pp. 14621–14635.

[73] R. Hussain, J. Lee, and S. Zeadally. "Trust in VANET: A survey of current solutions and future research opportunities". In: *IEEE transactions on intelligent transportation systems* 22.5 (2020), pp. 2553–2571.

[74] V. Agate, F. Concone, A. De Paola, P. Ferraro, G. Lo Re, and M. Morana. "Bayesian Modeling for Differential Cryptanalysis of Block Ciphers: A DES Instance". In: *IEEE Access* 11 (2023), pp. 4809–4820.

[75] V. Agate, S. Drago, P. Ferraro, and G. Lo Re. "Anomaly Detection for Reoccurring Concept Drift in Smart Environments". In: *2022 18th International Conference on Mobility, Sensing and Networking (MSN)*. IEEE. 2022, pp. 113–120.

[76] V. Agate, A. De Paola, G. Lo Re, and M. Morana. "DRESS: A Distributed RMS Evaluation Simulation Software". In: *International Journal of Intelligent Information Technologies (IJIIT)* 16.3 (2020), pp. 1–18.

[77] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti. "VANet security challenges and solutions: A survey". In: *Vehicular Communications* 7 (2017), pp. 7–20.

[78] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan. "A comprehensive survey on vehicular ad hoc network". In: *Journal of network and computer applications* 37 (2014), pp. 380–392.

[79] D. M. Powers. "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation". In: *arXiv preprint arXiv:2010.16061* (2020).

[80] A. Bordonaro, F. Concone, A. De Paola, G. Lo Re, and S. K. Das. “Modeling Efficient and Effective Communications in VANET through Population Protocols”. In: *2021 IEEE International Conference on Smart Computing (SMARTCOMP)*. 2021, pp. 305–310.

[81] C. Crapanzano, F. Milazzo, A. De Paola, and G. Lo Re. “Reputation management for distributed service-oriented architectures”. In: *2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems Workshop*. IEEE. 2010, pp. 160–165.