Sicurezza in ambito automotive: vulnerabilità, minacce, attacchi e possibili contromisure

Università degli Studi di Verona

08 Febbraio 2024

Marco Deano, Mattia Bernardi

Indice

1 Introduzione

2 Attacchi al sistema di Infotainment

3 Attacchi al sistema di road safety

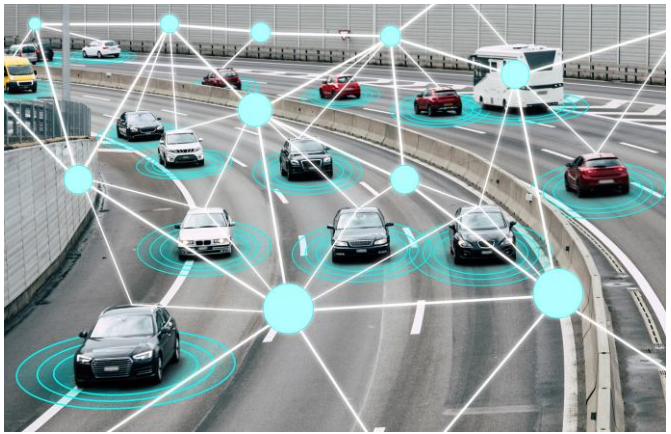
4 Conclusioni

Introduzione

Negli ultimi anni, il settore dei trasporti ha vissuto una profonda rivoluzione grazie alle auto a guida autonoma, conosciute come **CAV** (**Connected and Autonomous Vehicles**)

Erroneamente a quanto si potrebbe pensare, tale rivoluzioni non riguarda solamente l'introduzione di nuovi veicoli, ma comprende anche l'utilizzo di:

- Tecnologie innovative;
- Strategie di sicurezza;
- Nuovi meccanismi di gestione delle infrastrutture stradali.



Si ottiene, allora, un nuovo **complesso ecosistema tecnologico**, che porta con sé **vantaggi** e **minacce**.

Importanza delle auto a guida autonoma

Le auto a guida autonoma promettono di:

- Prevenire gli incidenti stradali;
- Migliorare l'esperienza di guida;
- Migliorare l'accessibilità al trasporto;
- Migliorare l'efficienza del trasporto.

Promettono, quindi, di **rivoluzionare il settore del trasporto**

Per riuscire a fare tutto ciò, sarà ovviamente necessario l'introduzione di:

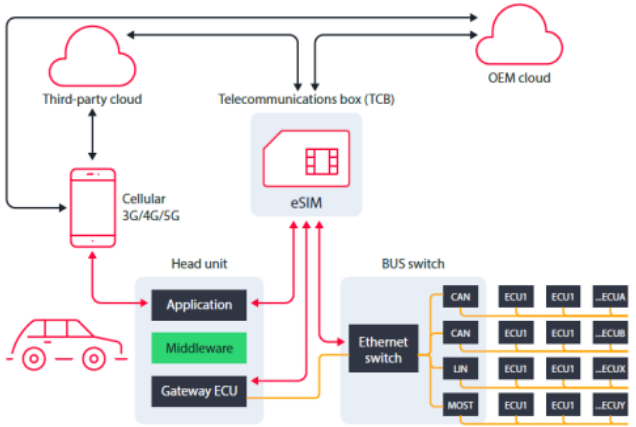
- Sistemi avanzati di assistenza alla guida (**ADAS**);
- Tecnologie di parcheggio automatico;
- Applicazioni di controllo del traffico;
- Applicazioni di sicurezza stradale.

Comportano i vantaggi visti sopra, ma anche **minacce, come gli attacchi informatici da parte di virus, bug e hacker**

Ecosistema delle auto a guida autonoma

La visione astratta dell'ecosistema di un CAV la possiamo osservare nell'immagine riportata sotto, in cui abbiamo:

- **Head unit**, la quale:
  - Supporta l'esecuzione di diverse applicazioni;
  - Ha un livello middleware → estrae i dettagli E/E (Elettrici ed elettronici) del veicolo e comunica con l'ECU gateway → facilita lo scambio di dati e informazioni tra le varie unità di controllo del veicolo.



- **Bus switch** → instrada i pacchetti verso le corrette centraline di destinazione;
- **eSIM**→ grazie ad essa, le app possono comunicare con:
  - **OEM Cloud** → piattaforma cloud, che fornisce servizi specifici del produttore automobilistico;
  - **Third-party Cloud** (Netflix, Google).
- **Cellulari**→ le app di terze parti svolgono un ruolo fondamentale nell'esperienza di guida.

Minacce e requisiti di sicurezza

Sicurezza e qualità del traffico stradale si basano molto sulle comunicazioni wireless

Diversi tipi di minacce possono interferire con il sistema stradale

In Europa si sta diffondendo lo standard **ETSI ITS**, che ha come requisiti di sicurezza:

- Autenticazione
- Integrità dei dati
- Privacy e anonimato
- Disponibilità
- Tracciabilità e revoca
- Autorizzazione
- Non ripudio
- Robustezza contro attacchi esterni

ITS components	Possible threats	Direct impact	Hazardous situations created
Infrastructure sign	Change/ add/ remove road signs (e.g., speed limit, messages)	False/ No reaction,	Traffic disturbance, collision, and congestions
Radar/Camera	Creating blind spot and presenting false image	False reaction	Driver disturbance
GPS	Spoofing and jamming	Inaccurate location information and wrong maneuver	Traffic disturbance and crash hazard
In-vehicle devices	Malware and head unit attack	Depends on malware capability	Serious traffic congestions and driver/traffic disturbance
Acoustic sensors	Interference and fake sound	False positive/negative obstacle detection and sensor malfunction	Traffic disturbance and low/high speed crash
Lidar	Jamming and smart material (absorbent, reflective)	False detection and degraded Lidar performance	Loss of situation awareness and traffic disturbance
In-vehicle sensors	Eavesdropping and malware	Privacy leak, reverse engineering and false message generation	Traffic disturbance, disabling vehicle automation service and accident
Infrastructure (RSU)	Denial of Service and fake WSA (RSA, SPAT)	Wrong notification to driver, wrong detection and no information for ITS	Traffic disturbance, safety issues and critical incident

Attacchi recenti nel mondo automotive

Molti test preliminari, hanno messo in luce possibili attacchi a vari componenti delle **CAV**:

- LiDAR
- GPS
- Messaggi di warnings
- Monitoraggio dei propulsori

Esempi di attacchi

- Attacco malware nel 2011 ad una Chevrolet Chevy Malibu → manipolazione della radio tramite una vulnerabilità Bluetooth ed iniezione di codice che bloccò il sistema di frenata
- Attacco man-in-the-middle nel 2015 ad una Jeep Cherokee → modifica dei messaggi tra le centraline e i freni, lo sterzo e l'acceleratore
- Attacco Sybil nel 2018 ad un'auto di Google → falsi nodi hanno inviato informazioni fuorvianti sulla posizione e sulle condizioni del traffico

Attacchi al sistema di Infotainment

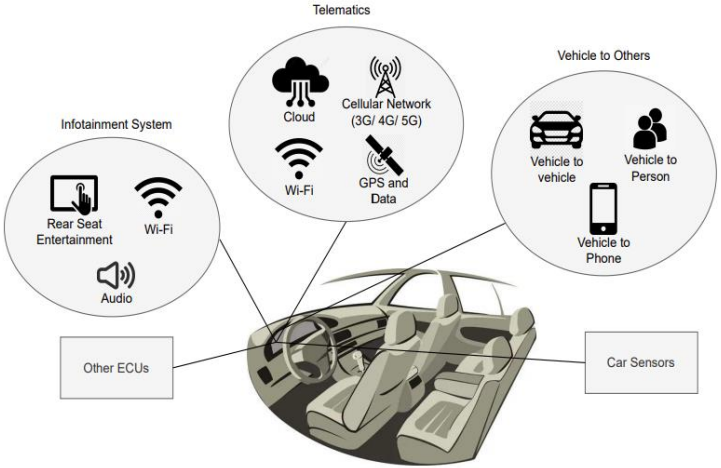
L’integrazione di un sistema di **Infotainment High-Performance Computing** (**HPC**) all’interno delle automobili moderne, comporta diversi servizi:

- Navigazione GPS;
- Assistenza alla guida;
- Integrazione con lo smartphone;
- Accesso a varie informazioni (dato che il veicolo è sempre connesso a Internet);
- Aggiornamenti software (in questo modo i produttori possono correggere bug e aggiungere nuove funzionalità).

L'interconnessione dei servizi con le automobili aumenta le vulnerabilità della sicurezza e infatti, sempre più frequentemente si verificano incidenti di hacking delle auto.

Questo ha portato ad una **maggiore attenzione verso la sicurezza del veicolo**, anche perché quest'ultimo è connesso ad una rete complessa, composta da:

- **Internet** → permette aggiornamenti della navigazione (in tempo reale del veicolo), servizi di streaming e aggiornamenti software;
- **Reti interne del veicolo** (**VAN**) → collegano le ECU (unità di controllo elettronico) del veicolo e quindi assicurano uno scambio di dati efficiente;
- **Reti di telecomunicazione** → permettono di effettuare la diagnostica remota del veicolo e la sua localizzazione;
- **Sensori dell'auto**;
- **Tecnologia wireless** (Wi-Fi) → utilizzata per creare una connessione tra il veicolo e i dispositivi esterni o per accedere a risorse online.



Infotainment e OBP apps

Per rimanere al passo con lo sviluppo dell'elettronica di consumo, le case automobilistiche hanno introdotto **applicazioni di Infotainment**, utilizzando maggiormente lo standard aperto **Android Auto** → ha come conseguenza diretta, un approccio maggiormente flessibile e di facile interazione con dispositivi Android di terze parti. Questo introduce le seguenti minacce:

Tecnica d'attacco	Descrizione
Virus/Malware	Utilizzo non autorizzato delle funzioni di infotainment attraverso l'impersonificazione o attacchi ai bug.
Autenticazione	Le informazioni inerenti al veicolo vengono rubate o mascherate per un utilizzo illegale.
Impostazione illegale	I dati del veicolo vengono compromessi attraverso impersonificazione o attacchi ai bug.
Informazioni false	Le app dannose inviano messaggi falsi al sistema di infotainment, al fine di ingannare il conducente o eseguire delle azioni illegali.
Jamming	Le app dannose ottengono il controllo del percorso di comunicazione, dirottano le comunicazioni regolari e si mescolano con quelle illegali.
Tracciamento	Gli attaccanti ottengono illegalmente informazioni sul veicolo e tracciano le informazioni sullo stato del veicolo come velocità, posizione e destinazione.
Distrazioni del conducente	Le app dannose distraggono il conducente visualizzando immagini o riproducendo audio o video.

Oltre alle applicazioni di Infotainment, abbiamo anche le **applicazioni OBD-II**, utilizzate per scaricare dati diagnostici e per eseguire test sull'autovettura. Precedentemente queste applicazioni venivano installate su dispositivi specifici, mentre ora vengono installate sugli smartphone personali. Questo crea altri rischi di sicurezza:

Tecnica d'attacco	Descrizione
CAN Injection	Gli attaccanti inviano messaggi CAN (Controller Area Network) modificati per eseguire operazioni pericolose.
Compromissione del dispositivo OBD-II	Gli attaccanti utilizzano un dispositivo OBD non sicuro per assumere il controllo di componenti cruciali dell'auto.
Bluebugging	Gli attaccanti prendono il controllo del dispositivo OBD quando non è collegato al dispositivo del proprietario e accedono a componenti cruciali dell'auto.
Violazione della privacy	Gli attaccanti utilizzano i dispositivi OBD per attaccare i dispositivi mobile dell'auto e rubare i dati personali.
Tracciamento	Gli attaccanti ottengono illegalmente le informazioni del veicolo e ne tracciano lo stato.

Esempio di attacco (MirrorLink)

Recentemente sono emersi diversi protocolli standardizzati per consentire una connettività fluida e senza interruzioni (nella trasmissione dei dati) tra gli smartphone e i sistemi di Infotainment delle auto, come ad esempio:

- Android Auto;
- Apple CarPlay;
- MirrorLink → l'obiettivo principale è quello di offrire all'utente la possibilità di utilizzare le applicazioni del proprio smartphone (ad esempio, le applicazioni di navigazione) sullo schermo più grande del sistema di Infotainment, invece di acquistare un **IVI** (**In-Vehicle Infotainment**) più costoso con connettività Internet e applicazioni integrate.

Al fine di analizzare in maniera dettagliata il protocollo MirrorLink, nel nostro documento abbiamo sviscerato 3 punti fondamentali:

1. **Analisi di sicurezza del protocollo e le modalità di implementazione**;
2. Analisi di sicurezza delle parti critiche dell'applicazione IVI MirrorLink;
3. Dimostrare le vulnerabilità dell'implementazione dell'applicazione IVI MirrorLink.

Analisi del software

Al fine di individuare potenziali vulnerabilità (sfruttabili dall'attaccante), sono state eseguite **delle analisi statiche** e **dinamiche** sul protocollo MirrorLink. In particolare, l'analisi statica ha evidenziate le seguenti vulnerabilità:

- ***Send2Micon*** e ***SendMsg*** → funzioni che consentono l'invio di byte di dati su un CAN tramite il controllore Micom CAN del IVI, senza adeguati controlli o restrizioni;
- **Controllore Micom CAN** → limita le comunicazioni dell'IVI ad altri dispositivi con lo stesso CAN ed in particolar modo, l'attaccante potrebbe aggiornare il firmware Micom (con dei metodi noti), ottenendo la possibilità di inviare messaggi arbitrari sul CAN;
- **Vulnerabilità nell'aggiornamento del firmware Micom**;
- **Vulnerabilità nel codice sorgente** → il firmware e le DLL IVI (Dynamic Link Libraries In-Vehicle Infotainment) sono scritte in C++.

L'analisi dinamica, invece, ha evidenziato che **non esiste un controllo dei limiti** o **un altro meccanismo di protezione** → per esempio, si è dimostrato che andando in Heap overflow, si riusciva a riservare spazio sull'Heap per iniettare codice maligno.

Modellazione delle minacce

La modellazione delle minacce è un metodo per identificare e priorizzare i pericoli legati al sistema, al fine di **sviluppare delle contromisure efficaci contro le minacce**. Il modello utilizzato è **STRIDE**, mentre i rischi sono stati valutati utilizzando:

- **SAHARA** → combina 3 parametri, al fine di determinare un **livello di sicurezza** (**SecL**). In particolare i 3 parametri sono:
  - **R** → risorse;
  - **K** → competenze necessarie per l'esecuzione della minaccia;
  - **T** → criticità della minaccia.

R	K	T			
		0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

- **DREAD** → calcola il rischio come: ***Rischio = (D + R + E + A + D)***

  D → danno; **R** → riproducibilità **A** → utenti colpiti;

  E → sfruttabilità; **D** → scopribilità.

Una volta modellate le minacce (con i meccanismi visti precedentemente), al fine di garantire la sicurezza e l'integrità del sistema e proteggerlo da potenziali compromissioni, vengono adottate una serie di meccanismi di difesa:

STRIDE Category	Threat Details	Mitigation
Spoofing	Adversary pretends to be a legitimate user or system	Multi-factor authentication [50–52], Biometric authentication [53,54]
Tampering	Adversary modifies data or software without authorization	Encryption [55], Digital signature [56]
Repudiation	Adversary denies responsibility for actions they have taken	Logging and auditing mechanisms to track and trace user actions [57]
Information Disclosure	Adversary gains access to sensitive information	Access controls and permissions to limit access to sensitive data [58,59]
Denial of Service	Adversary prevents legitimate users from accessing a system or service	Rate limiting and load balancing to distribute traffic across multiple servers [60,61]
Elevation of Privilege	Adversary gains higher levels of access than they are authorized to have	Secure coding practices [62], User activity monitoring and logging to detect potential privilege escalation attempts [63]

Attacchi alla connettività Bluetooth

Le automobili moderne sono dotate di funzioni di connettività per migliorare il comfort dell'utente. Il Bluetooth è una di queste tecnologie di comunicazione, che viene utilizzata per accoppiare un dispositivo personale con l'unità di Infotainment dell'automobile.

La sicurezza Bluetooth prevede l'**autenticazione**, l'**autorizzazione** e la **crittografia** basati sulla premessa che **l'utente si fida del dispositivo con il quale sta accoppiando il suo dispositivo personale**. Tuttavia, questo presupposto non può essere sempre vero con le unità IVI nei veicoli, soprattutto quelli gestiti da più utenti. Un utente malintenzionato potrebbe manipolare l'unità IVI e compromettere furtivamente la privacy dell'utente.

Quando l'utente accoppia il proprio telefono con il sistema IVI tramite Bluetooth per applicazioni hands-free (chiamate, intrattenimento) le loro informazioni personali vengono sincronizzate con l'unità IVI. L'attaccante può recuperare queste informazioni memorizzate attraverso una connessione cablata con il veicolo (USB) o attraverso una connessione wireless (Wi-Fi).

I dati (contatti personali, messaggi e registri delle chiamate**) recuperati dall'attaccante, attraverso le opzioni dello sviluppatore, non sono crittografati**.

Possibili contromisure

- Controllare se le opzioni dello sviluppatore sono abilitate nell'unità IVI. Se le opzioni dello sviluppatore sono abilitate, informare l'utente e richiedergli un ulteriore consenso;
- Controllare frequentemente lo stato del Bluetooth;
- Implementare in meccanismo di autenticazione più robusto per la connessione Bluetooth tra smartphone e sistema IVI;
- Implementare delle politiche di accesso basate sulla posizione del veicolo;
- Monitorare l'integrità del sistema IVI e avvertire l'utente in caso di attività sospette.

Attacchi ai sistemi di «road safety»

Fondamentale garantire la sicurezza dei passeggeri nelle strade

Implementazione di "applicazioni" che permettono di migliorare la **sicurezza stradale**:

- Sistemi **LiDAR**
- **GPS**
- Comunicazioni **V2X**
- Reti **VANET**

Anche queste tecnologie non sono esenti da vulnerabilità

Attacco/danno a questi sistemi → grave pericolo per i passeggeri

Attacchi ai sistemi LiDAR

Cosa sono i LiDAR? → Sensori per la creazione di mappe 3D dell'ambiente circostante

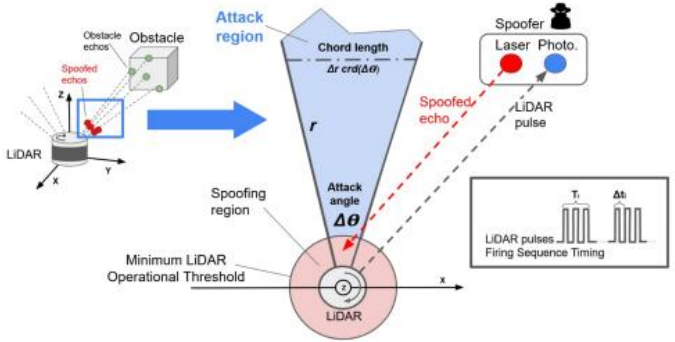
Utilizzano ottiche di alta qualità e hardware meccanici rotanti a cui vengono integrate delle coppie diodo-fotodiodo che permettono l'invio/recezione di raggi laser per il **rilevamento di eventuali ostacoli nei pressi della strada**

Attacco proof-of-concept contro il sistema LiDAR

L'obiettivo è quello di forzare l'eliminazione dei punti di nuvola tramite invio di **echi** (laser) falsi

Funziona perchè:

- I sistemi LiDAR danno priorità agli echi con intensità maggiore
- I sistemi LiDAR filtrano i punti di nuvola più vicini



Contromisure proposte contro gli attacchi ai sistemi LiDAR

- **FSD** (Fake Shadow Detection): consiste nell'identificare le regioni d'ombra presenti nel terreno e successivamente confrontarle con le ombre previste degli oggetti rilevati dal LiDAR.

➢ Molto sofisticata e precisa ma difficile da attuare

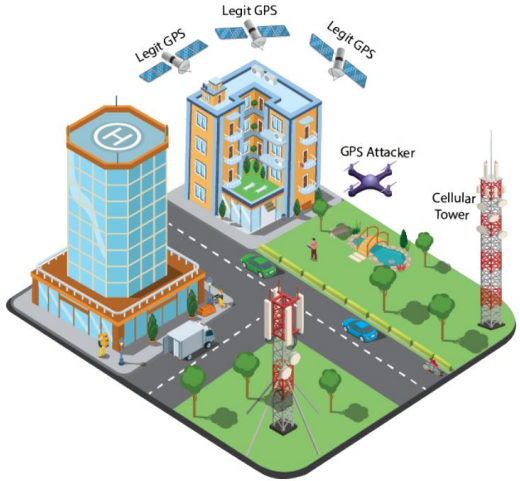
- **Interpolazione dei punti di nuvola**: consiste nel calcolare i valori di tutti i punti di nuvola nella scena, ordinarli e collocarli in una ipotetica mappa 3D; tutti i punti di nuvola mancanti in un certo angolo orizzontale (1°-2°), corrisponderanno a degli ostacoli mancanti

➢ Misura molto più semplice ed efficace

Possibili altre contromisure contro gli attacchi ai sistemi LiDAR

- Protezione fisica dei sensori del LiDAR
- Posizionare il LiDAR in punti strategici
- Utilizzare tipi diversi di sensori
- Protocolli di crittografia

Attacchi ai sistemi GPS



GPS → Standard di navigazione satellitare aperto che sfrutta i segnali ricevuti dai satelliti
Fondamentale per il corretto funzionamento dei veicoli autonomi

Tipi di attacchi ai sistemi GPS:

- **Jamming**: interruzione della comunicazione tra dispositivi GPS
- **Spoofing**: generazione di segnali falsi (i segnali GPS non sono autenticati)

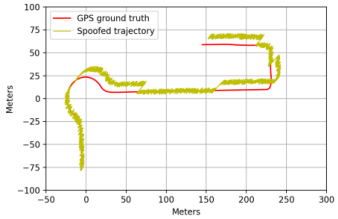
Contromisura proposta per gli attacchi ai sistemi GPS

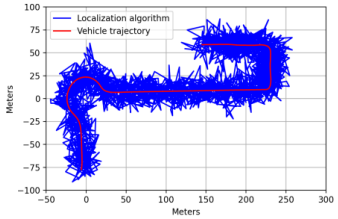
3 fasi:

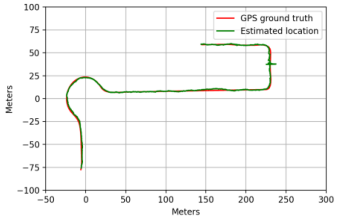
1. Fase di Previsione: tramite sensori di bordo, viene predetta la posizione $\hat{p}_{k+1} = [\hat{x}_{k+1}, \hat{y}_{k+1}]$ data la posizione precedente $p_k = [x_k, y_k]$
2. Fase di Aggiornamento: viene calcolata la posizione $p_{k+1}^{L} = [x_{k+1}^{L}, y_{k+1}^{L}]$ (calcolata tramite dispositivo specializzato), per stimare la posizione raffinata di $\hat{p}_{k+1}$
3. Fase di Attack Detection: la posizione GPS $p_{k+1}^{G} = [x_{k+1}^{G}, y_{k+1}^{G}]$, fornita dal ricevitore GPS del veicolo, viene confrontata con $\hat{p}_{k+1}$

Analisi critica sulla metodologia proposta

- Strategia robusta e funzionante







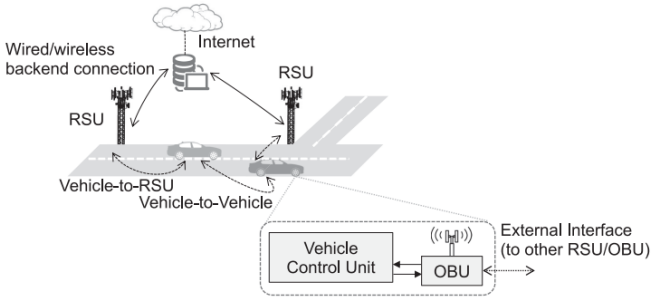
- Necessita di una notevole potenza di calcolo
- Troppo dipendente da segnali provenienti da infrastrutture esterne

Possibili altre contromisure contro gli attacchi ai sistemi GPS

- **Crittografia** a livello militare
- Implementazione di **firmware sicuri**
- Utilizzo di **filtri anti-spoofing**
- Sfruttare la **presenza di altri veicoli** e i segnali provenienti da essi

Attacchi alle comunicazioni V2X

Migliorano la sicurezza e l'efficienza del traffico tramite **scambio di info in tempo reale** tra macchine, pedoni, strade ed infrastrutture



Tipi di attacchi alle comunicazioni **V2X**:

- **Denial of Services**
- **Sybil**
- **Iniezione di dati falsi**

Contromisure proposte per gli attacchi alle comunicazioni V2X

- Infrastruttura a chiave pubblica (**PKI**)
- Meccanismi di **watchdog** per gli attacchi di DoS
- Utilizzo di **timestamp** per i messaggi spediti per gli attacchi di Sybil
- Utilizzo di un entità **CoE** (Certainty Of Event), calcolato combinando dati provenienti da varie fonti
- **Tecniche statistiche**

Analisi critica sulle metodologie proposte

- L'utilizzo di un **infrastruttura a chiave pubblica** (**PKI**), è una pratica comune e robusta; di contro però richiede una gestione complessa di tutta l'infrastruttura e un utilizzo di risorse significative
- I **meccanismi di watchdog** sono sicuramente semplici da implementare, però c'è il rischio di avere falsi positivi
- L'utilizzo di **timestamp** integrati nei messaggi spediti, è molto economico perché non sfrutta nessuna infrastruttura, macome nel caso dei watchdog c'è possibilità di avere falsi positivi
- La metodologia che sfrutta l'entità **CoE**, ed il meccanismo che sfrutta le tecniche statistiche, sono molto flessibili e possono contribuire a rendere il sistema più resistente agli attacchi mirati

Possibile altra contromisura contro gli attacchi alle comunicazioni V2X

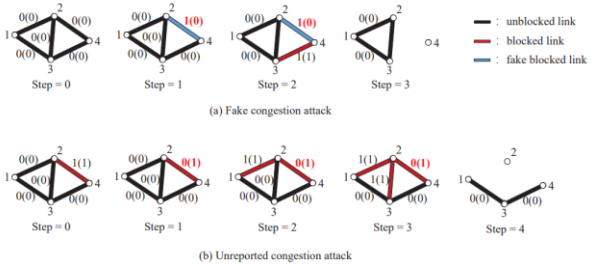
➢ Tutte le entità fisiche hanno **risorse limitate** → "programmi" computazionali per testare le risorse a disposizione di ogni auto

Attacchi alle reti VANET

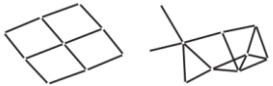
Cosa sono le reti VANET? → Reti ad-hoc create per migliorare la **sicurezza e la gestione del traffico**
Sono reti che si basano molto sulla comunicazione peer-to-peer

Tipi di attacchi alle reti **VANET**:

- Attacchi di **impersonification** and **masquerade**
- Attacchi di **timing**
- **Illusion attacks**
- Attacchi **black hole**



Conseguenze dovute agli attacchi alle reti VANET



➢ Rappresentiamo la rete stradale come un **grafo**

Consideriamo 2 classi di attacchi (che comprendono le tipologie citate sopra):

- **Fake congestion pollution** → sono più minacciosi in una rete eterogenea: le prestazioni del sistema diminuiscono della metà quando viene attaccato il 15% dei collegamenti
- **Unreported congestion pollution** → sono più pericolosi nella rete a griglia: le prestazioni del sistema diminuiscono della metà quando viene attaccato il 30% dei collegamenti

Contromisure proposte per gli attacchi alle reti VANET

- L'utilizzo di un **infrastruttura a chiave pubblica** (**PKI**)
- **TPM** (Trusted Platform Module), utilizzato contro attacchi di timing, è un **componente hardware che può calcolare l'hash** sul firmware, sull'avvio del SO o altri componenti critici
- **PVN** (Plausibility Validation Network), utilizzato per gli attacchi di illusion, **sfrutta i dati in ingresso** dalle RSU e da vari sensori **per determinare se un dato messaggio sia affidabile o meno**
- Utilizzo di **protocolli di instradamento dei pacchetti che considerino più di un percorso possibile**, contro gli + attacchi black hole)
- Utilizzo di un **protocollo di comunicazione anonimo per la privacy**

Analisi critica sulle metodologie proposte

- **TMP** → offre funzionalità di sicurezza avanzate
- **PVN** → è un approccio innovativo e proattivo; però l'utilizzo di infrastrutture aumenta molto la complessità di calcolo
- **Protocolli di instradamento** per gli attacchi di black hole → complessità computazionale elevata

Conclusioni

- Costo elevato per il mantenimento/manutenzione delle infrastrutture "side road"
- Elevata dipendenza da queste infrastrutture
- Sistemi di sicurezza attuali sono ancora in fase di evoluzione
- Necessità di una maggior consapevolezza da parte degli utenti

GRAZIE PER L'ATTENZIONE

Ingegneria e scienze informatiche - Università degli Studi di Verona
08 Febbraio 2024

Marco Deano, Mattia Bernardi