Tecniche di Lightweight Cryptography applicate in ambito Automotive

Candidato: Carmine Vincenzo *Russo*
Relatore: Prof. Arcangelo *Castiglione*

12 Dicembre 2019

Università degli studi di Salerno

Obiettivi

Obiettivi

Esaminiamo la rete di comunicazione interna dei veicoli, denominata CAN-bus

Obiettivi

Esaminiamo la rete di comunicazione interna dei veicoli, denominata CAN-bus, ne abbiamo analizzato le vulnerabilità ed ipotizzato come metterla in sicurezza attraverso algoritmi di cifratura Lightweight.

Focalizzando poi l'attenzione sulla latenza introdotta da tali algoritmi.

Introduzione

Stato dell'arte

L'industria automobilistica negli ultimi anni si è avvicinata sempre di più al mondo dell'informatica

Stato dell'arte

L'industria automobilistica negli ultimi anni si è avvicinata sempre di più al mondo dell'informatica, utilizzando tecnologie quali:

- Internet of Things
- Sistemi Cloud ed Ibridi
- Intelligenza Artificiale

Stato dell'arte

L'industria automobilistica negli ultimi anni si è avvicinata sempre di più al mondo dell'informatica, utilizzando tecnologie quali:

- Internet of Things
- Sistemi Cloud ed Ibridi
- Intelligenza Artificiale

Trasformando i veicoli in veri e propri sistemi informatici connessi.

Stato dell'arte

Tale progresso impone di mettere in sicurezza i veicoli.

Stato dell'arte

Tale progresso impone di mettere in sicurezza i veicoli.
Non più come semplici mezzi di trasporto,

Stato dell'arte

Tale progresso impone di mettere in sicurezza i veicoli.
Non più come semplici mezzi di trasporto, ma come un qualsiasi sistema informatico che dispone di connettività.

Stato dell'arte

Tale progresso impone di mettere in sicurezza i veicoli.
Non più come semplici mezzi di trasporto, ma come un qualsiasi sistema informatico che dispone di connettività.

Focalizzando l'attenzione sulla sicurezza del veicolo dal punto di vista informatico.

Connettività

La connettività introduce nuove funzionalità di Infotainment, come il Wi-Fi a bordo, e di sicurezza, come assistenza stradale immediata e diagnostica in remoto.

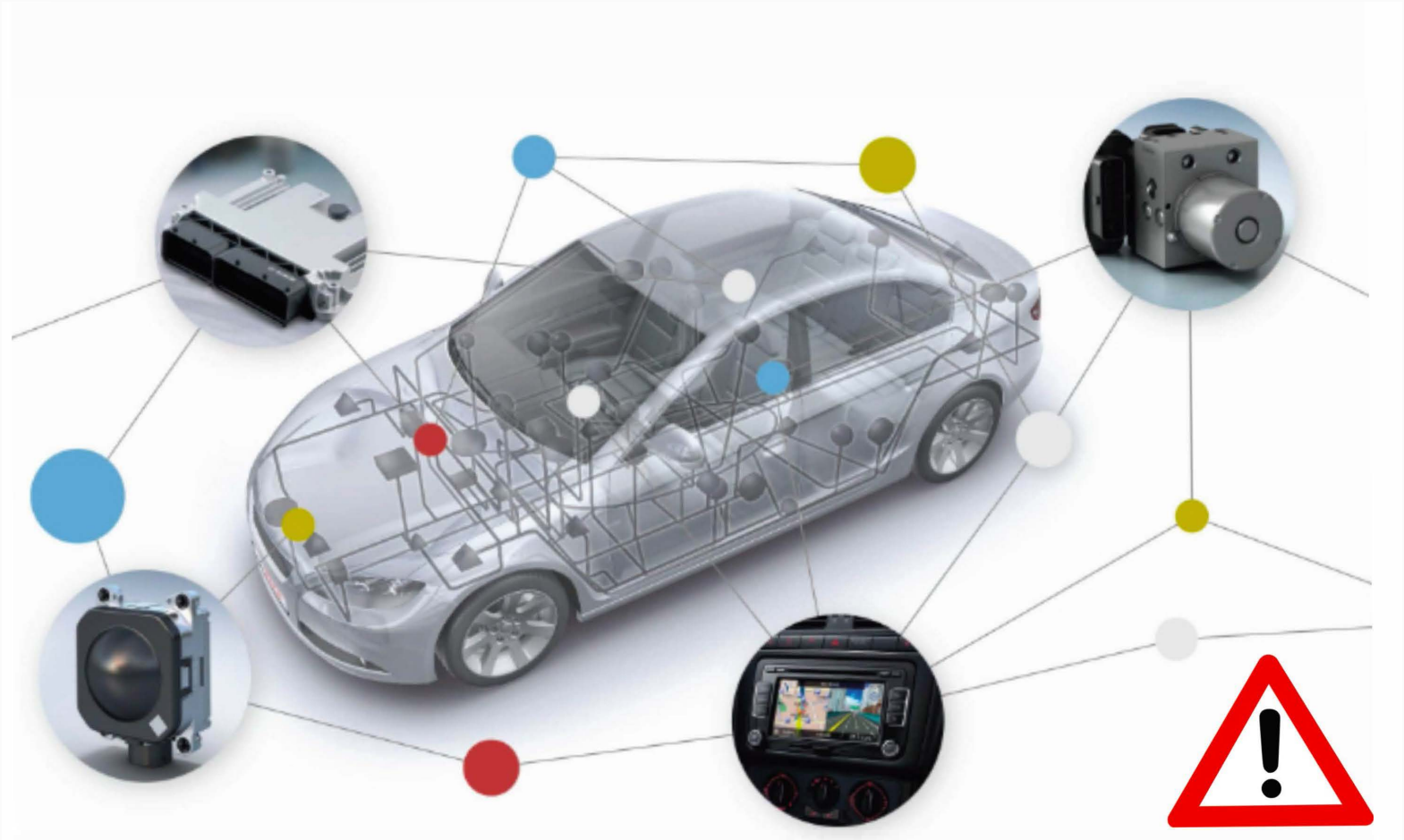
Connettività

La connettività introduce nuove funzionalità di Infotainment, come il Wi-Fi a bordo, e di sicurezza, come assistenza stradale immediata e diagnostica in remoto.

Allo stesso tempo, introduce nuovi pericoli e vulnerabilità.

Vulnerabilità

La criticità più grande si è rivelata essere il Controller Area Network bus (CAN-bus).



Protocollo CAN-bus

Standard

Il protocollo CAN-bus, nato negli anni '80 ma ancora tutt'oggi soggetto a continue modifiche, nasce con un preciso scopo:

Standard

Il protocollo CAN-bus, nato negli anni '80 ma ancora tutt'oggi soggetto a continue modifiche, nasce con un preciso scopo:

"Proporre un meccanismo arbitrario non distruttivo per garantire l'invio di messaggi con priorità alta senza alcun ritardo."

Protocollo CAN-bus

Tale scopo è raggiunto attraverso comunicazioni molto efficienti, che avvengono in Broadcast ed in chiaro sulla rete.
Tutti i dati sulla rete vengono trasmessi sotto forma di messaggi.

Trasmissione dei messaggi

I messaggi trasmessi possono essere di 4 tipologie:

- Data Frame
- Remote Frame
- Error Frame
- Overload Frame

Sicurezza del protocollo

Il protocollo CAN-bus, così come ideato, è vulnerabile ad attacchi Man-in-the-middle, dato che tutti i messaggi sono trasmessi in chiaro.

Sicurezza del protocollo

Il protocollo CAN-bus, così come ideato, è vulnerabile ad attacchi Man-in-the-middle, dato che tutti i messaggi sono trasmessi in chiaro.

Tale problematica, trascurabile in passato,

Sicurezza del protocollo

Il protocollo CAN-bus, così come ideato, è vulnerabile ad attacchi Man-in-the-middle, dato che tutti i messaggi sono trasmessi in chiaro.

Tale problematica, trascurabile in passato, nell'era dei veicoli connessi e raggiungibili tramite Internet rappresenta un serio rischio per la sicurezza.

Soluzione Proposta

Proposta

Avendo constatato che la problematica risiede nella trasmissione di dati in chiaro, si propone di cifrare i messaggi in maniera non invasiva e con il minimo impatto prestazionale sul protocollo CAN-bus.

Proposta

Avendo constatato che la problematica risiede nella trasmissione di dati in chiaro, si propone di cifrare i messaggi in maniera non invasiva e con il minimo impatto prestazionale sul protocollo CAN-bus.

Focalizzando l'attenzione sui Data Frame, tramite algoritmi di cifratura *Lightweight*, puntiamo a limitare la possibilità di attacchi al protocollo.

Lightweight Cryptography

Abbiamo deciso di utilizzare i seguenti algoritmi di cifratura:

- PRESENT
- SIMON
- SPECK

Cifrari a blocchi, con blocco dati di 64 bit e chiavi di varie lunghezze.

Implementazione della Soluzione Proposta

Implementazione della Soluzione Proposta

Per lo sviluppo e l'implementazione della nostra proposta, abbiamo utilizzato il sistema operativo Automotive Grade Linux ed i suoi strumenti di sviluppo.

Utilizzando AGL su un Raspberry Pi3 per ricreare l'ambiente limitato di un veicolo connesso.

Implementazione della Soluzione Proposta

AGL è un progetto *open source* nato per proporre un sistema di riferimento per i veicoli connessi.

Implementazione della Soluzione Proposta

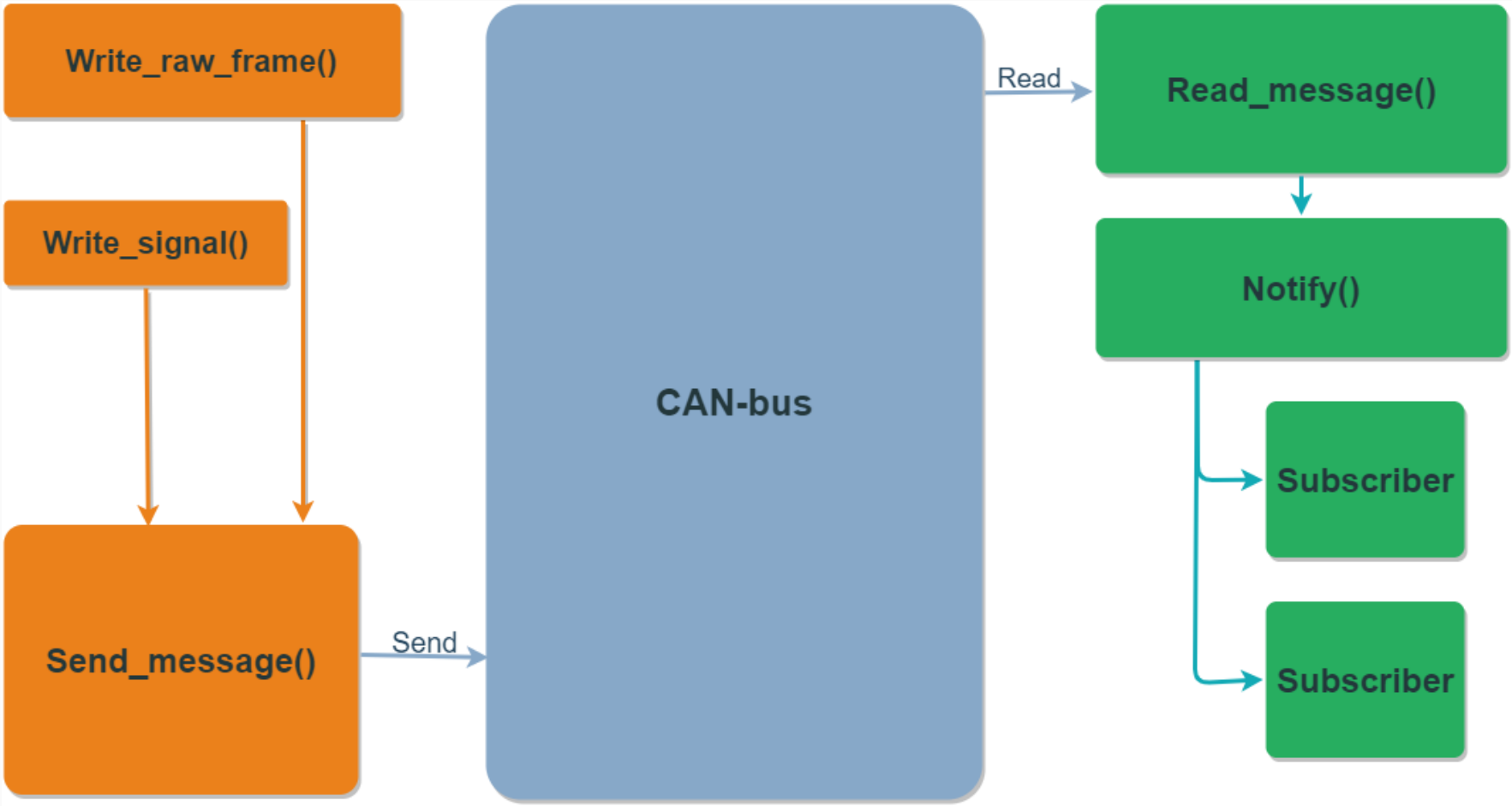
AGL è un progetto *open source* nato per proporre un sistema di riferimento per i veicoli connessi.
Ci ha fornito gli strumenti necessari per simulare il funzionamento del protocollo CAN-bus ed implementare la nostra proposta.

Architettura della Soluzione Proposta

Simulato il funzionamento del CAN-bus, ci siamo concentrati sul comprendere ed individuare come i messaggi vengono creati ed inviati sul mezzo di comunicazione.

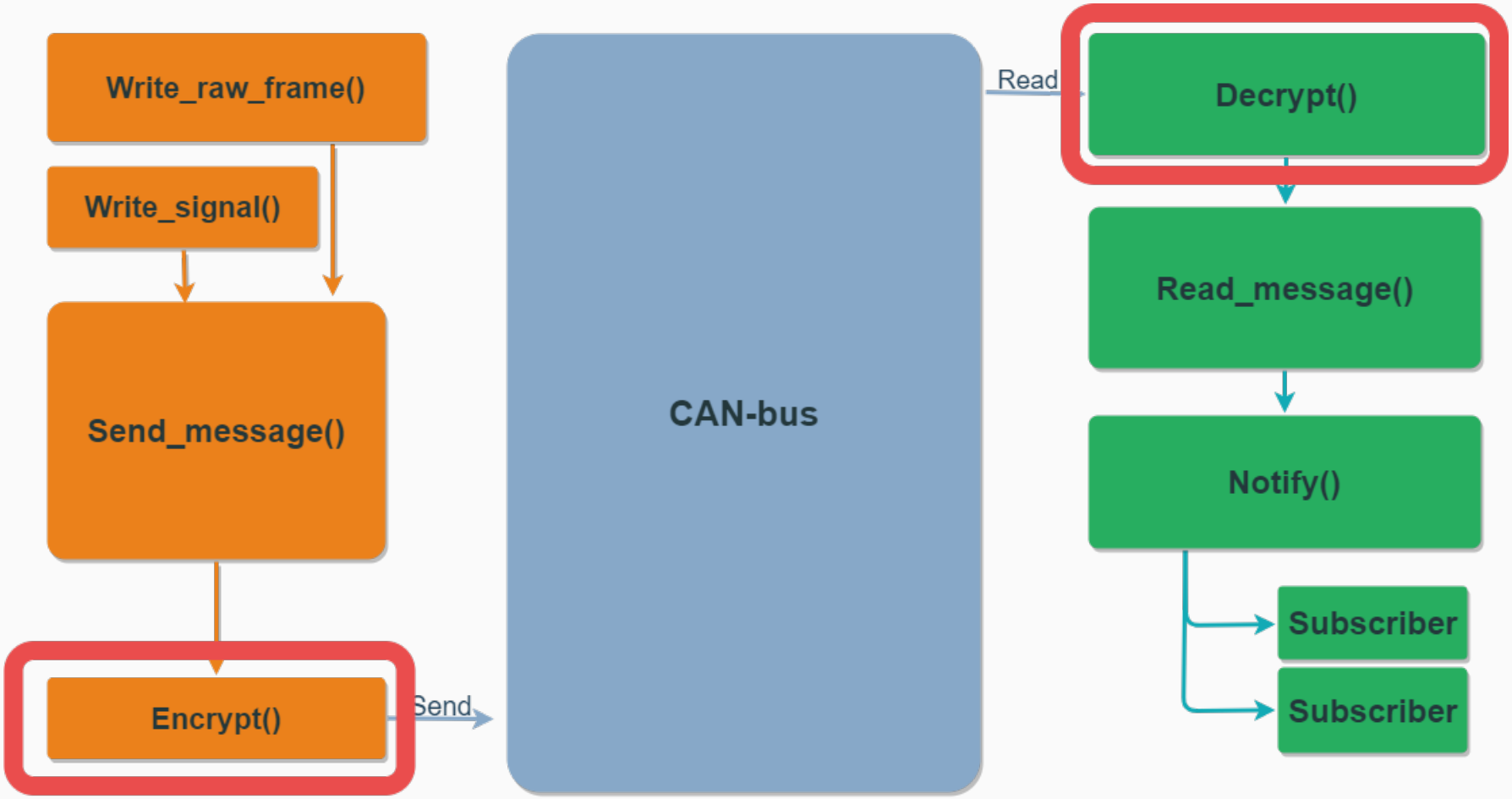
Architettura della Soluzione Proposta

Siamo dunque risaliti alla seguente struttura:



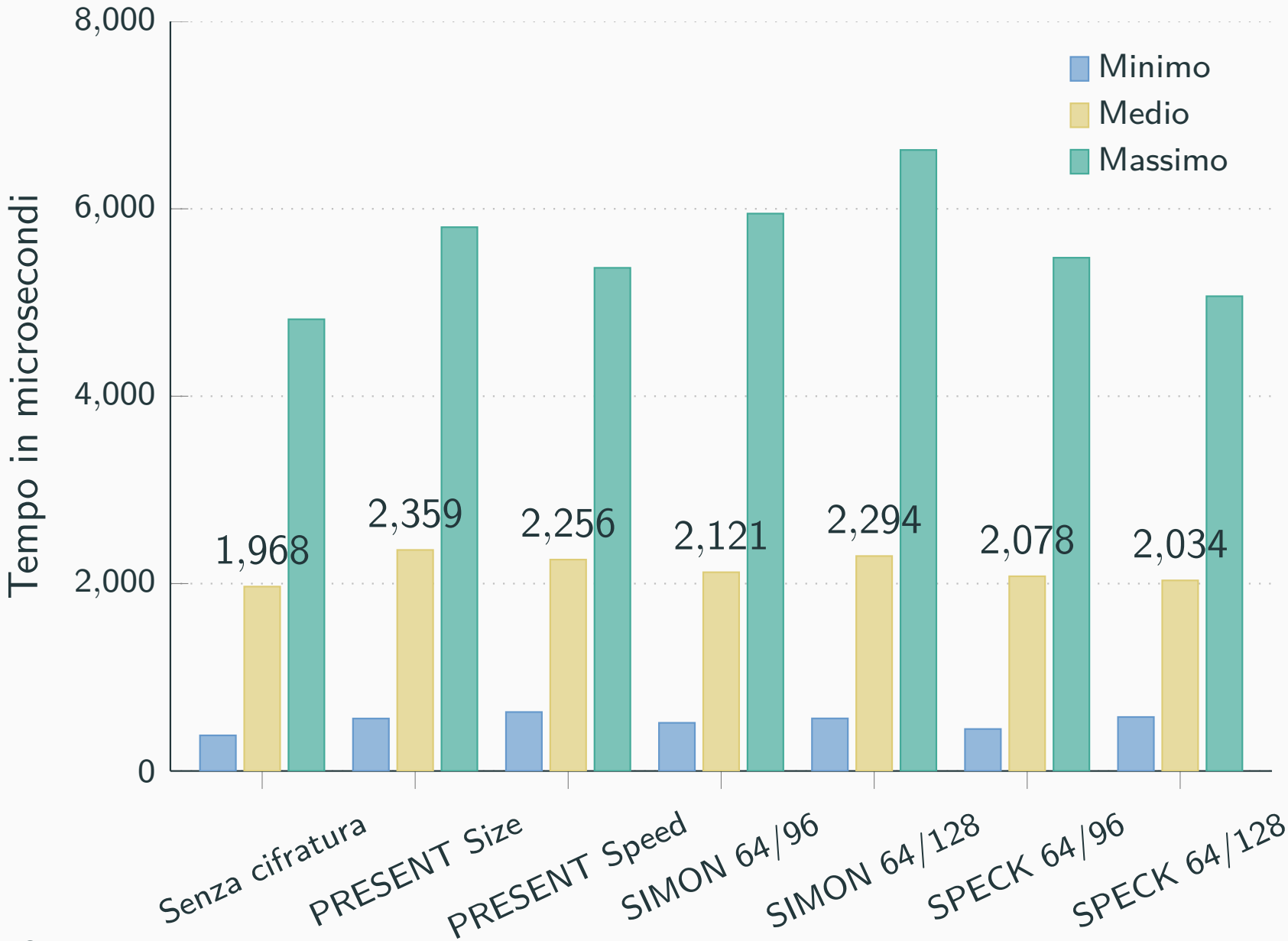
Architettura della Soluzione Proposta

Potendo individuare il punto esatto in cui introdurre le funzionalità di cifratura e deciratura.



Risultati Sperimentali

Risultati Sperimentali



Risultati Sperimentali - Considerazioni

Le modalità di cifratura introducono una latenza che varia tra i 66us ed i 391us.

SPECK 64 128 risulta essere il più performante, mentre entrambe le modalità di PRESENT risultano essere tra le più lente.

Risultati Sperimentali - Considerazioni

Velocità	66us	391us
50 Km/h	0.9 mm	5.4 mm
100 Km/h	1.8 mm	10.8 mm
150 Km/h	2.7 mm	16.3 mm
200 Km/h	3.6 mm	21.7 mm
250 Km/h	4.6 mm	27.1 mm

Table 1: Spazio percorso prima di iniziare la frenata con la latenza introdotta valutando varie velocità.

Conclusioni e Sviluppi Futuri

Conclusioni

I risultati ottenuti hanno un impatto minimo sul sistema e mostrano come l'introduzione di uno strato di cifratura possa essere una soluzione efficace per mitigare le vulnerabilità del protocollo CAN-bus.

Sviluppi Futuri

Come sviluppi futuri potrebbero essere effettuate ulteriori ricerche riguardo:

- La possibilità di implementare la soluzione da noi proposta su Hardware meno performante
- La possibilità di utilizzare altri Lightweight Cipher selezionati dal NIST nell'ambito del Lightweight Cryptography (LWC) Standardization contest.

Grazie per l'attenzione!