Interfaccia wifi a crittografia avanzata per la ricarica automatica di autoveicoli elettrici

SAPIENZA
UNIVERSITÀ DI ROMA

Corso di laurea in Ingegneria dell'Informazione

Laureando:
Gianluca Grasso
 # matricola: 1494995

Relatore:
Alessandro Falaschi

Anno Accademico
2018/2019

Indice

Introduzione - Mobilità elettrica

Cos’è e che vantaggi porta ?

È un tipo di mobilità incentrata sull’uso di energie rinnovabili, e fa della sostenibilità uno dei suoi vantaggi fondamentali.

Quali sono i pro e contro di una vettura elettrica ?

Pro:

- È più efficiente e inquina meno
- Ha costi di manutenzione e percorrenza più bassi
- È più longeva

Contro:

- È più costosa
- Attualmente solo il 30% dell’elettricità prodotta proviene da fonti rinnovabili
- La ricarica è lunga

Introduzione - Stato dell’arte

Come si ricarica oggi un’automobile elettrica ?

Attualmente la ricarica viene effettuata così

Il conducente dovrà parcheggiare, scendere dall’auto attaccare il cavo di alimentazione e successivamente pagare.

Introduzione - Soluzione

Selezionare per scrivere o eliminare il sottotitolo

Soluzione:

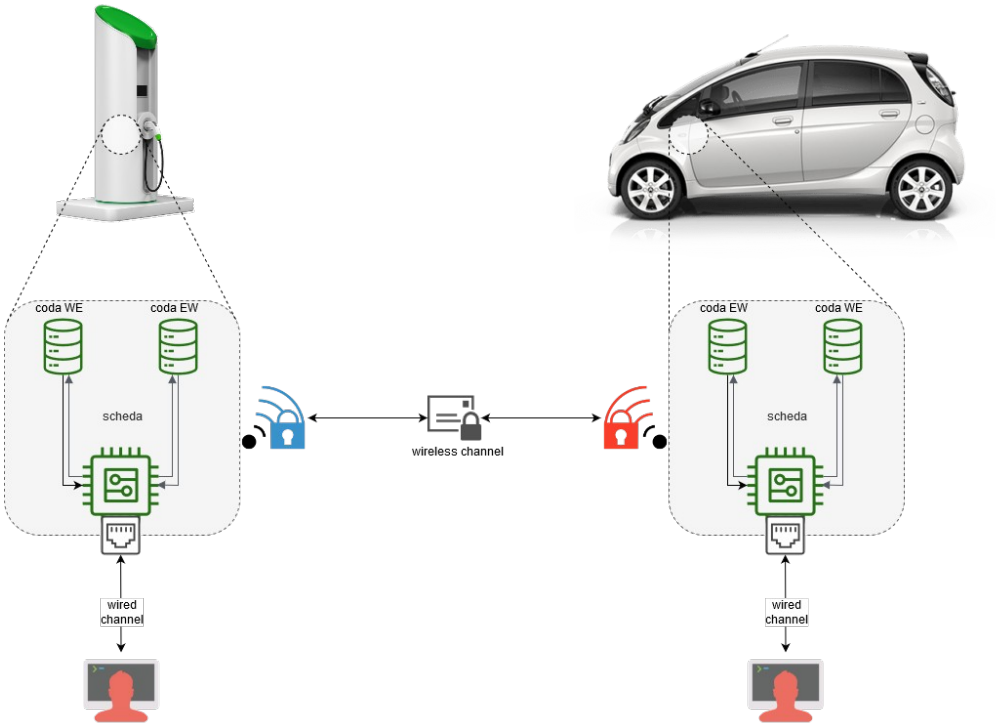
Si potrebbe automatizzare la procedura di ricarica attraverso l'utilizzo sia per le comunicazioni che per la trasmissione di energia delle onde elettromagnetiche.

La comunicazione attraverso wifi

La ricarica attraverso l'induzione

Architettura

Scambio dati tra attori



La comunicazione per mezzo del wireless è implementata sugli attori coinvolti attraverso l'installazione di una board.

La comunicazione dovrà garantire:

- Sicurezza
- Affidabilità

Architettura - Scheda

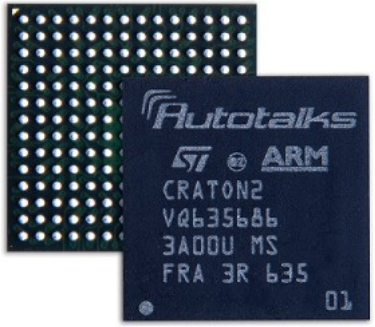
Board utilizzata

È stata utilizzata una board di sviluppo dalle seguenti caratteristiche:

- Dual 802.11p
- V2x communications
- On-board gps
- Cryptographic hardware acceleration
- CAN FD interface

Architettura - Scheda

System on Chip



Il cuore della board è rappresentato dal SoC «Craton2» che al suo interno implementa 2 core ARM cortex a7 e un modulo per l'accelerazione hardware della crittografia complessa in tempi brevi.

La gestione della comunicazione attraverso l'802.11p è invece esterna al Soc, ed è affidata ad un chip presente sulla board «pluton2», che ne implementa lo stack .

Architettura – Wifi

IEEE 802.11p

La board attraverso il modem «pluton2» implementa le comunicazioni VANET V2X attraverso lo stack IEEE 802.11p.

Inoltre, supporta IEEE 802.11a/b/g/n/ac, abilitando il servizio WIFI all'esterno del veicolo per servizi supplementari. Può supportare due antenne per un'installazione flessibile, e può persino supportare il funzionamento simultaneo dei canali (WIFI standard e 11p).

Architettura – Crittografia

Elliptic Curve Integrated Encription Scheme

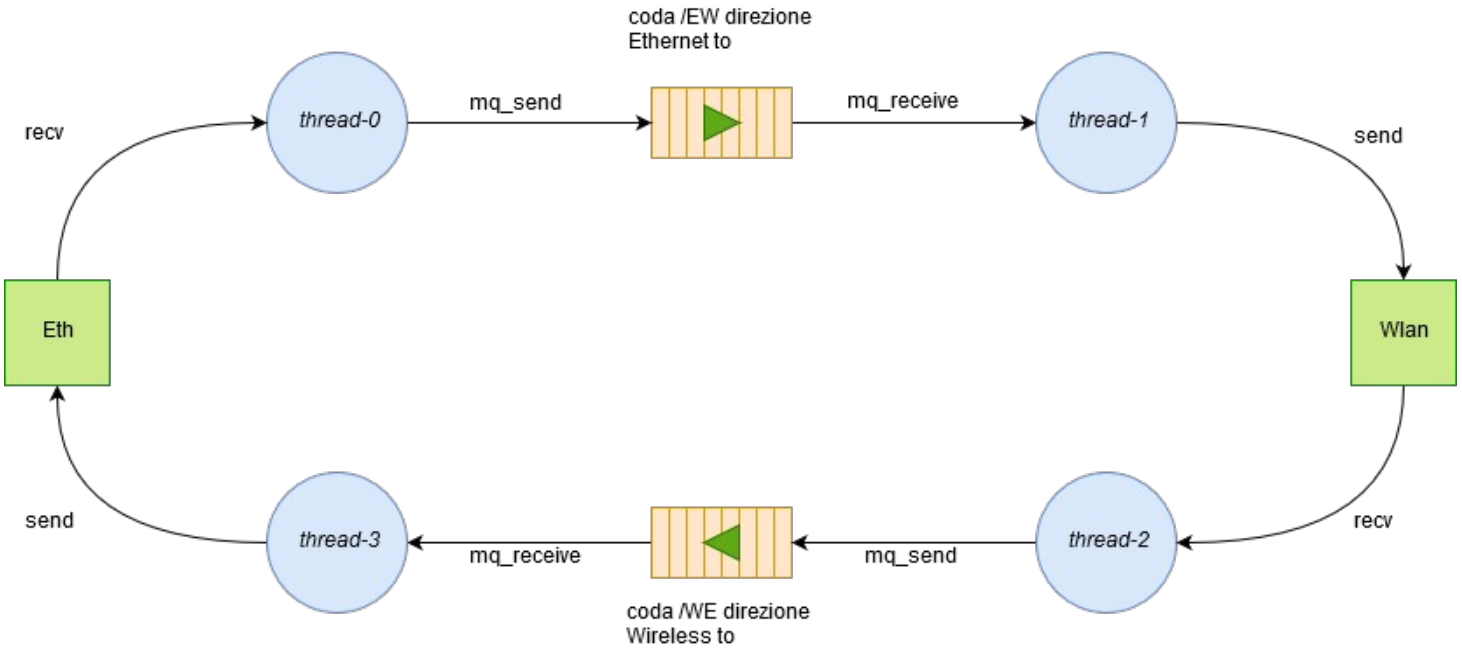
La crittografia è affidata ad un famoso e annoverato schema crittografico ibrido che combina innumerevoli sottoschemi crittografici traendo da ognuno di essi dei vantaggi.

Lo schema utilizza sia schemi a chiave simmetrica che asimmetrica, di quest'ultimi utilizza però un implementazione differente dal classico RSA poiché utilizza le più efficienti curve ellittiche «ECC»

Inoltre lo schema implementa anche una firma digitale, che accompagnerà il messaggio e consentirà al destinatario di validare quanto ricevuto.

Implementazione
Architettura software

L’implementazione software di una board è sintetizzata nel seguente schema:



Implementazione

Code e Thread

L'architettura software progettata è formata da due flussi di esecuzione uguali e opposti nel verso, che interconnettono le interfacce come delle autostrade.

Ogni interfaccia è ascoltata da 2 istanze diverse con compiti diversi, la prima legge mentre la seconda scrive. Le due metà del grafico ciascuna delle quali rappresenta un'interfaccia dialogano per mezzo di code con il fine di rendere questa comunicazione asincrona.

Sebbene le 2 interfacce siano gestite in egual modo, quella wireless si differenzia per avere in più delle chiamate all'hardware crittografico e quindi cifrare le comunicazioni.

Il diagramma completo è dunque composto da 4 thread e 2 code

Implementazione

Perché multi-thread e non multi-processo ?

L’esecuzione parallela è possibile in 2 modi:

- Multi-processo
- Multi-thread

In questo progetto è stata utilizzata l’esecuzione parallela di tipo multi-thread, benché non sia la più performante è sicuramente la più semplice da implementare e gestire poiché a memoria condivisa.

Implementazione

Gestione delle interfacce

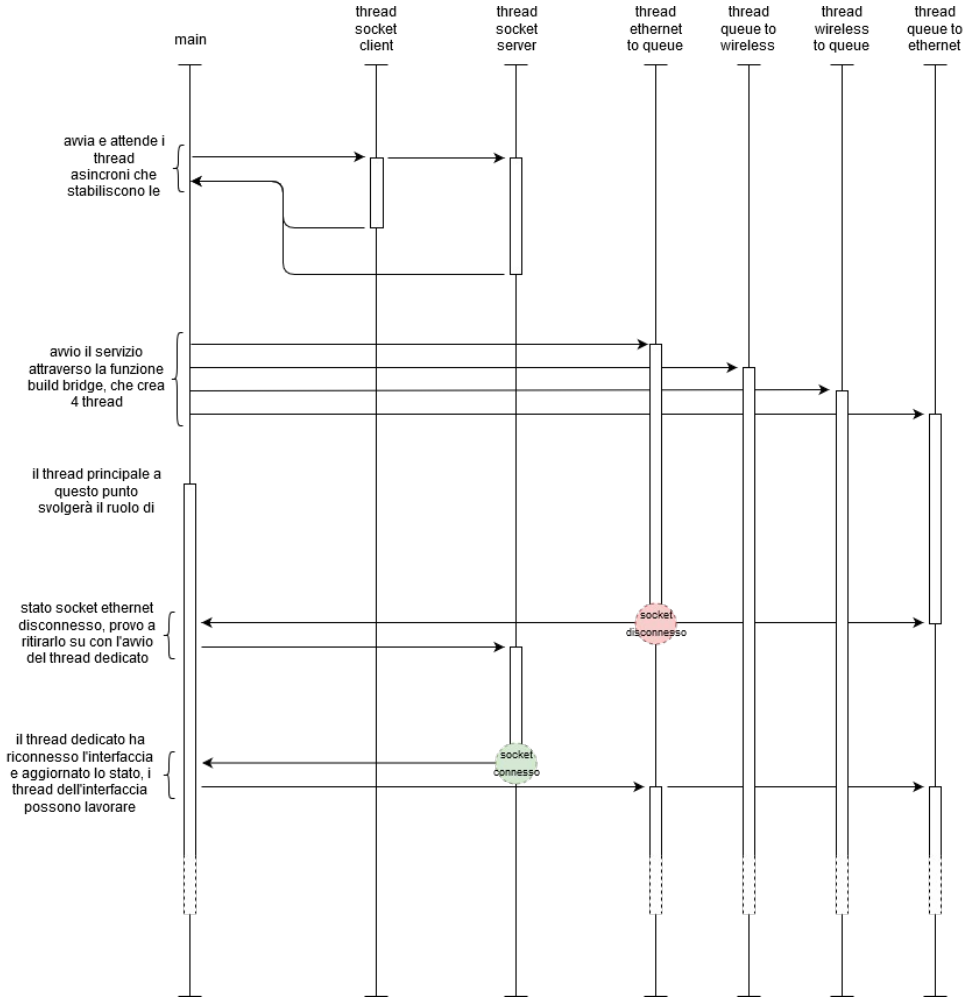
Poiché le interfacce di rete della board potrebbero disconnettersi in un qualsiasi momento, è stato implementato un meccanismo di recupero attraverso un watchdog di controllo delle connessioni.

Il watchdog controllerà ogni 5 secondi lo stato delle connessioni attraverso la memoria condivisa di ogni thread.

Le code in caso di disconnessione permettono di non perdere i dati, in attesa che la connessione venga ristabilita.

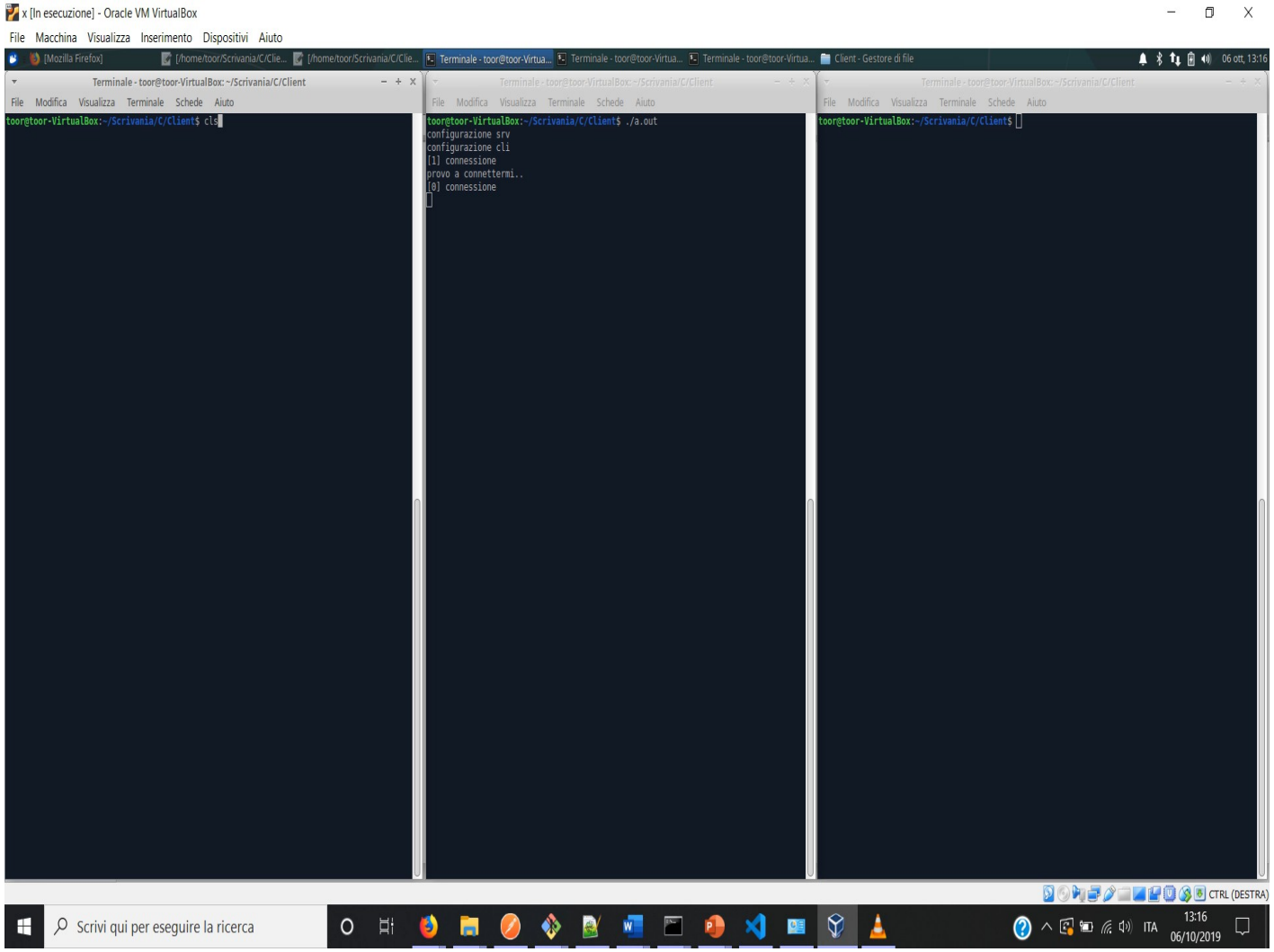
Implementazione

Diagramma temporale



Nella Figura a lato è mostrato un esempio di diagramma temporale per meglio comprendere il comportamento software progettato

Demo


x [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Terminale - toor@toor-VirtualBox: ~/Scrivania/C/Client
toor@toor-VirtualBox:~/Scrivania/C/Client$ cls
toor@toor-VirtualBox:~/Scrivania/C/Client$ ./a.out
configurazione srv
configurazione cli
[1] connessione
provo a connettermi..
[0] connessione
toor@toor-VirtualBox:~/Scrivania/C/Client$
Scrivi qui per eseguire la ricerca
ITA
13:16
06/10/2019

Sviluppi futuri (Conclusione)

- Sviluppo reti 5g
- Riduzione dipendenza combustibili fossili e maggior energia proveniente da fonti rinnovabili
- Implementazione gps attraverso galileo