UNIVERSITÀ
DI PARMA

Dipartimento di Ingegneria e Architettura

Corso di Laurea in Ingegneria Informatica, Elettronica e delle Telecomunicazioni

---

Aggiornamento delle Root Key per Applicazioni IoT Basate su LoRaWAN

Root Keys Update for LoRaWAN-Based IoT Applications

Relatore:
Chiar.mo Prof. Michele Amoretti

Tesi di Laurea di:
Alessandro Pindozzi

Correlatore:
Prof. Luca Veltri

ANNO ACCADEMICO 2020/2021

Quando si parla di IoT (Internet of Things) si fa riferimento all'interconnessione e allo scambio di dati tra dispositivi/sensori. I dispositivi in questione sono tutti gli oggetti intelligenti che ci circondano nelle attività quotidiane. Essi devono essere in grado di comunicare tra loro a grandi distanze e con uno consumo di energia più basso possibile. Per questo motivo utilizzano un modello di comunicazione wireless detto LPWAN (Low Power Wide Area Network). Tra le reti LPWAN una delle più promettenti è LoRa.

Sviluppato da Semtech Inc., LoRa è uno strato fisico la comunicazione a lungo raggio che usa una particolare tecnica di modulazione, chiamata CSS (Chrip Spread Spectrum). Il protocollo di comunicazione e l'architettura di sistema per la rete sono invece definiti da LoRaWAN, la quale quindi ha più influenza nel determinare la durata della batteria di un nodo, la capacità della rete, la qualità del servizio, la sicurezza e la varietà di applicazioni servite dalla rete. Proprio sull'aspetto di sicurezza ci si focalizza in questa Tesi, il cui fine è quello di trovare un meccanismo che possa compensare una delle vulnerabilità di LoRaWAN.

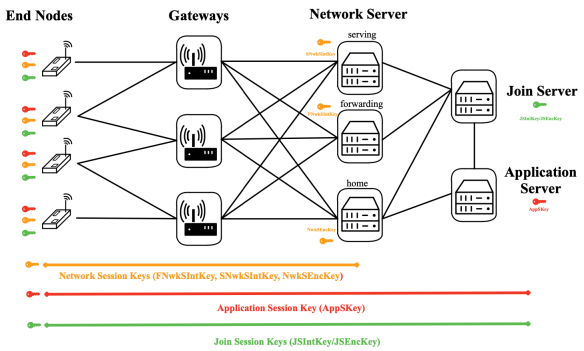

Figura 1: Architettura di rete LoRaWAN e distribuzione di chiavi

Nella Fig. 1 viene mostrata l'architettura di una rete LoRaWAN, quali sono le parti che la compongono e in che maniera vengono distribuite le chiavi.

Un dispositivo finale che si connette a una rete LoRaWAN tramite un Network Server, scambia messaggi di Join Request e Join Accept con il Join Server. Solo dopo che il join ha avuto successo e che quindi vengono generate le chiavi di sessione che permettono di criptare il payload dei messaggi, il dispositivo può comunicare con l'Application Server. Tutte le chiavi di

sessione sono derivate dalle root key (NwkKey e AppKey) le quali vengono installate in fase di fabbricazione nei dispositivi e rimangano invariate per tutto il loro ciclo di vita. Proprio questo aspetto viene considerato come una delle falle di sicurezza di LoRaWAN, ed è bene che vengano utilizzati meccanismi di memorizzazione sicuri per queste root key.

Il progetto di Tesi ha come fine quello di creare un sistema di aggiornamento dinamico delle root key, così che le chiavi di sessione siano sempre derivate da root key differenti. Per realizzare questo progetto si sono utilizzati dei dispositivi virtuali, sia end device che gateway, e una piattaforma di backend TTN (The Things Network), che fornisce un Network Server gratuito per formare la propria rete LoRaWAN. Inoltre essa espone anche un API che permette di interagire con i dispositivi dall'esterno.

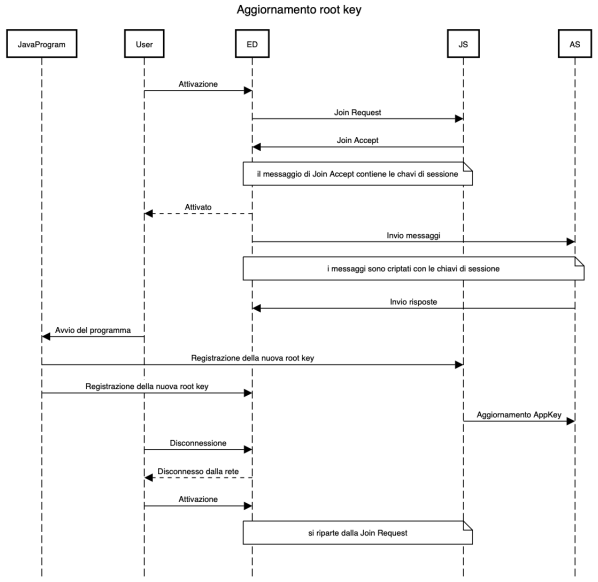

Figura 2: Sequence diagram del sistema realizzato per l'aggiornamento delle root key

La Fig. 2 mostra il sequence diagram che descrive le varie fasi e operazioni del sistema realizzato. Infatti, proprio grazie all'API di TTN, inviando richieste HTTP, è possibile aggiornare le AppKey dei dispositivi registrati sulla piattaforma TTN. Più precisamente una richiesta PUT permette di registrare i nuovi valori della chiave sul Join Server. Sfruttando questo aspetto, e modificando anche il valore delle chiavi a livello locale, quindi sul file di configurazione dei dispositivi, si ottiene una root key AppKey sempre diversa dalla quale, ogni qualvolta si effettua il re-join, vengono derivate delle chiavi di sessione nuove. Infatti le chiavi di sessione vengono create ogni volta che il dispositivo si connette alla rete, quindi ogni qualvolta viene effettuato il join. Nel sistema realizzato questo passaggio (disconnettere il dispositivo dalla rete e riconnetterlo) deve essere fatto manualmente, sebbene possa essere reso automatico grazie al software del dispositivo virtuale.

Cambiando periodicamente le root key, si hanno due diverse possibilità. O si semplifica l'implementazione e si riducono i costi hardware dei dispositivi in quanto non occorrono metodi di salvataggio sicuri delle chiavi radici, proprio perché esse vengono aggiornate, o si fa uso di questi sistemi di archiviazione sicura insieme al re-keying progettato, aggiungendo così un ulteriore livello alla sicurezza.

Ci sono diverse possibili strade che possono essere percorse per portare avanti questo progetto. Una possibile evoluzione del sistema realizzato prevede l'automatizzaione del re-join, quindi fare in modo che questo non debba essere fatto manualmente. Oppure si possono utilizzare dispositivi fisici, e non virtuali. Infine un'interessante evoluzione potrebbe consistere in un meccanismo che rigeneri le chiavi di sessione senza necessità di effettuare il re-join.

In conclusione si può affermare che questo sistema si prefigura come un buon punto di partenza per apportare migliorie di sicurezza al protocollo LoRaWAN.