PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4479 di Lunedì 03 giugno 2019

La security nelle reti in tecnologia 5GV

Uno studio sostenuto dalla National Security Agency fa il punto della situazione fa il punto sul livello di sicurezza e protezione dei dati della recente tecnologia 5G.

L'imminente entrata in funzione della più recente tecnologia di trasmissione dati via radio, chiamata 5G, ha destato, in molti esperti, preoccupazioni in merito a livello di sicurezza e protezione dei dati, che questa tecnologia offre. Uno studio sostenuto dalla National Security Agency fa il punto della situazione.

In questo primo articolo viene trattato l'aspetto afferente alla security; la protezione dei dati sarà oggetto di un secondo documento.

La crescita vertiginosa del numero di apparati che devono scambiarsi dati tramite reti senza fili ha portato ad un altrettanto rapido sviluppo di nuove tecnologie di comunicazione. Queste nuove tecnologie sono classificate con l'acronimo LTE (Long Term Evolution), che è impiegato per indicare la tecnologia successiva al diffuso standard di radiocomunicazione mobile UMTS (Universal Mobile Telecommunications System). Questa tecnologia è stata introdotta per far fronte alla crescita repentina del traffico mobile di dati che, sinora, è raddoppiato a livello mondiale a ritmo quasi annuale.

La tecnologia LTE include un'interfaccia radio ottimizzata per la radiocomunicazione mobile, già impiegata con profitto nelle reti per la radiodiffusione digitale terrestre. Il suo utilizzo comporta la riorganizzazione delle stazioni esistenti, l'allestimento di stazioni di base supplementari e nuovi terminali (cellulari, tablet, PC, modem, router). Fra le caratteristiche distintive di questa tecnologia vi è una maggiore velocità di trasmissione nell'interfaccia radio tra la stazione di base e il terminale. In questo modo aumenta la capacità di trasmissione della rete mobile, è possibile servire un maggior numero di utenti o fornire velocità più elevate. Tra l'altro, la riduzione dell'intervallo di trasmissione dati (latenza) migliora considerevolmente la reattività della rete. Inoltre, rispetto allo standard UMTS, la tecnologia LTE richiede un minor consumo di energia da parte del terminale e consente dunque di prolungare i tempi di attività del servizio dati.

I problemi di sicurezza della trasmissione, in questa nuova tecnologia, sono accresciuti dal fatto che essa prevede l'interconnessione di miliardi di apparati di piccola dimensione e modesta capacità di elaborazione, spesso contrassegnati con l'acronimo IoT- Internet of Things. Questi dispositivi dispongono di ridotte sorgenti di alimentazione e di ridotte capacità di calcolo e non sono quindi in grado di gestire in modo efficiente ed efficace protocolli crittografici evoluti. Inoltre questi dispositivi possono comunicare contemporaneamente dall'uno all'altro, oppure tramite nodi di rete, oppure infine tramite cloud.

Un ultimo requisito, richiesto a questa nuova rete, è la bassa latenza di trasmissione, che viene ottenuta con velocità estremamente elevate, in modo da consentire ai veicoli autonomi di interagire tempestivamente con le informazioni che provengono dal campo.

La soluzione di questi problemi pone sfide significative sia ai responsabili della security di rete, per l'intero tratto di collegamento tra trasmettitore e ricevitore-*end to end security,* sia per i tutori della protezione dei dati in transito.

Cominciamo ad analizzare la struttura della rete 5G, che è sostanzialmente diversa da una rete 4G.

Nelle precedenti architetture di rete vi era un punto centrale di controllo con piena autorità per effettuare il monitoraggio e la gestione della sicurezza. Vi sono strutture chiamate osservatori, che tengono sotto controllo il traffico in rete e riferiscono al punto centrale di controllo, che assume decisioni afferenti alla sicurezza, con una visione globale del traffico in rete.

Questo modello non è applicabile alle reti 5G.

Il numero spaventoso di utenze collegate infatti renderebbe improponibile il monitoraggio centralizzato dei collegamenti e quindi decisioni afferenti alla sicurezza devono essere decentrate. La mancanza di un punto centrale di controllo e monitoraggio rappresenta una area critica, dal punto di vista della sicurezza, ma d'altro canto ad oggi non è possibile trovare altre soluzioni, che non prevedano la distribuzione delle funzioni sicurezza nell'intera rete. Gli obiettivi primari di questa nuova architettura, che prevedono la comunicazione da macchina a macchina, una comunicazione a bassissima latenza ed alta affidabilità, rappresentano caratteristiche di rete che possono essere in contrasto fra di loro.

La soluzione fino adesso attuata, in reti 4G e 5G, è la generazione di chiavi criptografiche simmetriche, condivise fra i gestori della rete e la SIM posta nell'apparato telefonico o nella macchina, che deve comunicare.

Nelle architetture 4G questa generazione di chiavi e scambio fra le controparti richiede lo scambio di numerosi messaggi e questa soluzione non è compatibile con la rete 5G, perché la quantità di messaggi in transito avrebbe un effetto negativo sulla velocità di rete. Una ipotesi di soluzione, già proposta, prevede che la banda radio, riservata ai collegamenti 5G, venga suddivisa in sotto bande, destinate ai vari servizi di comunicazione, prima illustrati. Tuttavia questa soluzione contrasta con le esigenze di allocazione dinamica delle frequenze disponibili, proprio per mantenere estremamente elevato il reato di trasmissione dei dati, in funzione del numero degli utenti e dei tipi di messaggi da scambiare.

Come accennato in precedenza, la necessità di eliminare un'autorità centrale di autentica delle controparti, che è resa purtroppo necessaria dalle diverse esigenze dell'architettura di comunicazione della rete 5G, pone problemi non indifferenti.

Ad esempio, il fatto di utilizzare delle piccole celle, che lavorano secondo scenari diversi, fa sì che le verifiche di sicurezza siano delegate alla periferia e non controllate centralmente. D'altro canto, appare chiaro che l'utilizzo di piccole cellule allevia di molto il traffico complessivo in rete, perché non si impegnano risorse, che devono coprire ampie superfici geografiche, per trasmettere dati, che interessano solo apparati posti l'uno a breve distanza dell'altro.

Ecco la ragione perché la migrazione da una struttura centralizzata ad una struttura decentrata, in cui gli apparati comunicano direttamente fra di loro, rappresenta una soluzione pressoché ideale, almeno dal punto di vista dell'efficienza delle trasmissioni.

D'altro canto, come accennato in precedenza, le risorse di calcolo disponibili in piccoli apparati, tipici della rete IoT, impediscono l'utilizzo di sofisticate e sicure architetture.

Per contro, l'eccessivo frazionamento delle sottoreti di collegamento può portare ad una possibilità di geolocalizzare gli apparati con una precisione oggi inconcepibile, a livello di metri, se non proprio di centimetri.

I progettisti di queste reti, per risolvere almeno in parte questi problemi, hanno fatto ricorso ai cosiddetti SDN - software defined networks. Si tratta di architetture di rete oltremodo agili, basate su protocolli aperti, che separano le funzioni di controllo di rete, come ad esempio lo smistamento ed il filtro dei messaggi, dall'hardware che effettua il trattamento dei pacchetti di dati. La rete viene pertanto suddivisa in strati separati: lo strato dei dati, lo strato di controllo e lo strato applicativo.

Infine, tutte queste architetture sicurezza devono essere sviluppate partendo dal fatto che, anche se le reti 4G potranno essere successivamente migliorate, alla fine l'unica rete dominante, in tutto il mondo, sarà una rete 5G, che opera secondo standard di interoperabilità e che coprirà tutte le comunicazioni mobili, dalla più lenta alla più rapida.

Se si pensa che queste reti devono consentire una trasmissione di dati ad almeno 10 gigabit per secondo, per poter trasmettere in tempo reale le immagini radiografiche catturate da un ospedale alla rete di consulenti, ci si rende conto che si sta parlando di un obiettivo estremamente ambizioso.

Aggiungendo a queste considerazioni quelle afferenti alla capacità di collegare, con bassa latenza, fino a 10 miliardi di apparati, sparpagliati nel mondo, appare evidente che gli attuali protocolli di sicurezza delle reti 4G non possono essere trasferiti nelle reti 5G, che hanno bisogno di una progettazione innovativa e dedicata.

Adalberto Biasiotti

www.puntosicuro.it