Cooperative Communications with Confidential Messages

Risultati in breve

Uno scambio di dati sicuro nelle reti ad hoc

La cooperazione tra i nodi di una rete senza fili potrebbe trasformare questa risorsa in uno strumento vulnerabile e suscettibile agli attacchi. Scienziati finanziati dall'UE hanno analizzato questi problemi di sicurezza per le reti ad hoc.

ECONOMIA DIGITALE

© Thinkstock

In un futuro non troppo lontano, si prevede che le reti senza fili tradizionali verranno sostituite da quelle decentralizzate, che sono caratterizzate dalla presenza di vari terminali mobili che si collegano e scollegano continuamente dalla rete. La progettazione di tali sistemi fa emergere una questione importante relativa all'affidabilità degli scambi di dati riservati tra nodi di reti attendibili.

Il progetto CCCM ("Cooperative communications with confidential messages") è stato incentrato sull'aumento dei livelli di sicurezza nelle reti ad hoc, nelle quali l'eterogeneità dei nodi non garantisce scambi di chiavi crittografiche con un livello di segretezza assoluto. L'idea di base dell'iniziativa consisteva nella progettazione di una rete in cui i dati vengono trasmessi dal nodo di origine al nodo di destinazione con una potenza minima. In senso lato, questa soluzione dovrebbe proteggere le reti da nodi dannosi che ricevono dati non destinati a loro.

Al fine di aumentare il rendimento, altri utenti sarebbero in grado di cooperare con il mittente. Partendo da una potenza specifica, gli scienziati hanno tentato di ottimizzare l'affidabilità e il rendimento delle reti senza fili ad hoc preservando, nel contempo, la riservatezza delle comunicazioni.

Gli esperti hanno rilevato un miglioramento della sicurezza complessiva delle reti garantito dai nodi cooperativi grazie alla loro capacità di fungere da relè o di inviare interferenze agli intercettatori (jammer). Fatta eccezione per le controparti mobili, questi nodi si presterebbero a essere fissati, consentendo in tal modo alle reti delle infrastrutture gestite di potenziare la sicurezza delle trasmissioni. Nello specifico, si è assistito a un potenziamento del rendimento in termini di segretezza nel corso della modellizzazione della rete ad hoc in un traliccio quadrato.

Gli scienziati hanno inoltre scoperto la possibilità di preservare la riservatezza dei dati provenienti da nodi intermedi. L'utilità di tale sistema si concretizzava nella sua capacità di garantire trasmissioni sicure attraverso nodi cooperativi non attendibili. In tali casi, l'utilizzo di questi nodi come jammer si è rivelato più efficace rispetto alle controparti a relè.

Un'altra parte del progetto è stata incentrata sulla combinazione di un livello di segretezza informativo-teorico e un sistema di riservatezza crittografico tradizionale. Partendo da tali presupposti, gli esperti hanno utilizzato collegamenti perfettamente sicuri supportati da nodi cooperativi per lo scambio di chiavi segrete tra parti legittime, che ha garantito un aumento del rendimento in termini di segretezza.

I risultati del progetto offrono nuove possibilità nell'ambito delle comunicazioni cooperative. Nello specifico, accanto alle reti ad hoc mobili, anche la segretezza informativa-teorica potrebbe avere utili risvolti in un'ampia gamma di settori, tra cui le comunicazioni a corto raggio e le reti di identificazione a radiofrequenze, i sistemi di codifica delle reti, la sicurezza dei social network e la privacy nelle reti intelligenti.

Parole chiave

Dati sicuri | scambio di dati | rete ad hoc | reti senza fili | dati riservati | nodi di rete | comunicazioni cooperative | crittografico | nodo cooperativo | jammer | trasmissione sicura | rendimento in termini di segretezza | informativo-teorico

Informazioni relative al progetto

CCCM

ID dell'accordo di sovvenzione: 237669

Progetto chiuso

Data di avvio
1 Dicembre 2009

Data di completamento
31 Maggio 2013

Finanziato da
Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Costo totale
€ 251 049,26

Contributo UE
€ 251 049,26

Coordinato da
ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE
Switzerland

Ultimo aggiornamento: 22 Gennaio 2015

Permalink: https://cordis.europa.eu/article/id/151935-secure-data-exchange-in-adhoc-networks/it