

Le reti mobili ad hoc: una nuova sfida per la sicurezza

Alessandro Ghioni, Davide Cerri

La grande diffusione delle reti radiomobili cellulari per fornire connettività a livello geografico e la crescente diffusione delle reti basate sullo standard Wi-Fi per fornire connettività a livello locale stanno rendendo sempre più indispensabile, e in qualche modo scontata, la percezione degli utenti di poter essere sempre collegati a sorgenti di informazioni, o a servizi disponibili all'interno di uffici o di aree pubbliche. Le infrastrutture di comunicazione usate per questi scopi si fondano su uno schema gerarchico, in cui sono presenti punti d'accesso centralizzati che fanno da "collettore" per l'accesso degli utenti. La comunità scientifica sta però studiando soluzioni che vadano oltre la necessità di una infrastruttura fissa e predeterminata: si tratta delle cosiddette *reti ad hoc*, e in particolare delle reti mobili ad hoc (*MANET* – Mobile Ad hoc NETWORKS). Questo modo destrutturato di interconnettere sistemi può permettere di utilizzare servizi distribuiti anche quando le infrastrutture fisse siano danneggiate (pensiamo ad applicazioni per la protezione civile), inaccessibili, sovraccariche, inesistenti (in questo caso, potrebbero essere interessanti ambiti applicativi quali il monitoraggio del territorio o la classificazione di beni culturali) o semplicemente costose. Le reti ad hoc hanno una loro naturale applicazione in contesti di comunicazione "spontanea", quando gruppi di persone, dotate di terminali come PC portatili, PDA, smartphone, si trovano fisicamente nello stesso luogo e hanno l'esigenza di comunicare tra loro, senza doversi necessariamente appoggiare su un'infrastruttura di rete esistente fornita da terzi. Spingendosi un po' più in là con l'immaginazione, si arriva agli scenari di "ubiquitous computing", in cui sistemi e applicazioni che si trovano in un certo luogo si possono autoorganizzare per offrire servizi in modo trasparente agli utenti.

Dal punto di vista della sicurezza, le reti mobili ad hoc presentano i problemi di base che affliggono qualunque infrastruttura di rete wireless, connessi all'intrinseca debolezza di questo tipo di mezzo di comunicazione, come la facilità di interagire con la rete e di intercettare le informazioni in transito, o la possibilità di portare attacchi denial of service disturbando il segnale a livello fisico. Oltre a questi, tuttavia, le MANET presentano problemi di sicurezza nuovi e particolari, legati alla loro natura di sistemi aperti e collaborativi.

Routing e sicurezza Per realizzare una MANET con le attuali tecnologie è sufficiente, per esempio, essere provvisti di laptop o PDA equipaggiati con una scheda Wi-Fi configurata in modalità ad hoc. In questo caso è possibile realizzare una rete mobile ad hoc in cui ogni nodo è in grado di comunicare con quelli che sono in diretta visibilità radio. Una direzione interessante sulla quale la comunità scientifica sta lavorando è quella di rendere

“*multihop*” la rete che così si crea, in modo che i nodi che non sono in diretta visibilità radio possano comunque comunicare tra di loro appoggiandosi su quelli che si trovano sul percorso. In una MANET multihop il terminale di ciascun utente svolge sia il ruolo di host che di router; di fatto, si crea una rete “collaborativa” in cui, se un nodo vuole comunicare con un altro ma non è possibile una comunicazione radio diretta tra i due, magari per qualche ostacolo o per la distanza, un altro nodo che si trovi in una posizione intermedia si fa carico di inoltrare i messaggi tra il mittente e il destinatario. Per rendere multihop una MANET è necessario adottare *protocolli di routing* specificatamente studiati, in grado di gestire la variabilità dei percorsi di instradamento che si creano (i nodi si muovono, e la topologia può cambiare di continuo) senza però sovraccaricare la rete.

Ad oggi, i quattro protocolli di routing per reti ad hoc in fase di standardizzazione in IETF¹ (AODV, DSR, OLSR e TBRPF) hanno come obiettivo primario le prestazioni della rete, e non si preoccupano degli aspetti di sicurezza. C’è però da considerare il fatto che, in una rete aperta che basa il proprio funzionamento sulla collaborazione “volontaria” tra i nodi, il problema della sicurezza non è secondario a quello delle prestazioni, se si vuole ottenere una certa robustezza dell’infrastruttura. In queste reti, infatti, tutti i nodi partecipano alle operazioni di routing, per cui potrebbe essere sufficiente anche un solo nodo che si comporti in maniera non corretta per danneggiare seriamente l’operatività della rete. A testimonianza di questo, molti studi, articoli e proposte stanno nascendo per aggiungere funzionalità di sicurezza ai protocolli sopra elencati, o per proporre altri in cui la sicurezza sia un fattore considerato sin dalla prima fase di progettazione.

Gli attacchi più probabili al routing di una MANET sono quelli in cui un nodo che voglia minare il corretto funzionamento delle operazioni di instradamento dei pacchetti sfrutti i messaggi previsti dal protocollo in modo da veicolare informazioni fasulle circa la topologia di rete, col fine di escludere qualche nodo, compromettere la disponibilità della rete, o deviare alcuni percorsi per diventare “collettore” delle informazioni in transito. Due sono i tipi di soluzioni in fase di studio per difendersi da attacchi di questo tipo: utilizzare meccanismi per garantire l’autenticità e l’integrità dei messaggi di routing (per lo più facendo ricorso a firme digitali) e sfruttare la natura broadcast del mezzo trasmissivo usato (il canale radio) per far sì che ciascun nodo possa controllare e verificare il comportamento dei suoi vicini. Entrambe le tecniche possono risultare onerose dal punto di vista delle prestazioni della rete e dei nodi. Infatti, in uno scenario come quello delle MANET, si suppone che i terminali non siano particolarmente potenti (tendenzialmente, si tratta di PDA), e il fatto che siano continuamente impegnati in operazioni di routing riduce la potenza disponibile per le applicazioni, e la durata delle batterie. Aggiungere operazioni di firma (e conseguente verifica) dei messaggi, oppure spendere tempo, risorse e batteria per controllare le operazioni compiute dai vicini, tende ad aggravare questa già scarsa disponibilità di risorse. Proprio per questi motivi, sono allo studio tecniche e protocolli in cui le operazioni sopra descritte vengono usate nel modo meno invasivo e oneroso possibile. La sfida, come spesso accade, sta nel coniugare le prestazioni con la sicurezza dell’infrastruttura, in presenza di risorse limitate.

¹Reperibili sul sito del MANET working group: <http://www.ietf.org/html.charters/manet-charter.htm>

La distribuzione di credenziali e il problema della fiducia La verifica di messaggi di routing correttamente firmati, o il controllo sul comportamento di altri nodi, pone un altro problema: quello dell'identificazione dei nodi partecipanti. Per poter identificare con certezza un terminale nella rete non è possibile utilizzare l'indirizzo MAC o l'indirizzo IP, facilmente falsificabili. È necessario considerare l'utilizzo di identità crittografiche, che peraltro possono essere adottate per molteplici scopi, oltre quello di autenticare messaggi di routing. Il problema, in questo caso, risiede nel meccanismo di distribuzione e verifica delle identità crittografiche.

Si possono fare due considerazioni sullo scenario in cui si prevede che le MANET verranno usate: in generale, si tratterà spesso di un ambiente aperto, collaborativo, a cui chiunque sia dotato di un terminale adeguato potrebbe partecipare per dare il suo contributo al miglior funzionamento della rete. È anche vero, però, che nella maggior parte dei casi la MANET sarà popolata da un nucleo stabile di persone, riunite in un certo luogo per uno scopo preciso, e che in massima parte si conoscono. Dalla prima considerazione discende che è desiderabile mantenere e incoraggiare l'ingresso di nuovi utenti nella MANET, mentre dalla seconda deriva il fatto che la presenza di un nucleo "fidato" di utenti può essere sfruttata per distribuire credenziali di accesso ai nuovi arrivati.

Resta il problema di come distribuire queste credenziali. La MANET è per sua natura un ambiente decentralizzato, per cui un paradigma centralizzato come quello delle classiche PKI non sembra la scelta migliore. In uno scenario del genere infatti non sarebbe corretto che un singolo nodo facesse da autorità di certificazione, in quanto potrebbe in certi casi essere irraggiungibile, ma soprattutto potrebbe non esistere alcun nodo che "abbia titolo" per svolgere questa funzione; inoltre non sarebbe corretto appoggiarsi a una o più autorità esterne alla MANET, in quanto questa si comporta in generale come un ambiente autonomo. Si sfocia quindi in problemi che hanno a che vedere con la distribuzione di credenziali e la creazione di rapporti di fiducia all'interno di un gruppo. Un approccio promettente è quello delle *PKI distribuite*, in cui la chiave crittografica di una Certification Authority distribuita viene divisa su più nodi (che potrebbero essere i componenti del "nucleo fidato" sopra citato). Quando deve essere rilasciato un certificato digitale a un nuovo nodo, è sufficiente che questo venga firmato da un sottoinsieme degli appartenenti al nucleo, e ciò è possibile mediante tecniche di "crittografia a soglia". In questo modo è possibile sia evitare che la radice della PKI risieda su un solo nodo, che potrebbe anche essere non raggiungibile, sia permettere che l'accesso al gruppo da parte di un nuovo utente sia subordinato alla volontà di un sottoinsieme di nodi di rilasciargli una credenziale per l'accesso. Dopodiché, quando un nodo è in possesso di una credenziale che lo identifica, è sempre possibile da parte di altri nodi (o di gruppi di utenti) riconoscere eventuali comportamenti scorretti da questo tenuti, e potenzialmente notificarlo ad altri. Si può quindi arrivare ad aspetti di creazione e distribuzione della reputazione, tipici delle reti peer-to-peer. Questa non è una coincidenza, ma è dovuta alla similitudine architetturale tra una MANET (una rete in cui i dispositivi si parlano "direttamente", senza che nessuno sia un punto d'accesso privilegiato) e il paradigma peer-to-peer (che permette alle applicazioni di organizzare una cosiddetta rete "overlay", alla quale ciascun utente può partecipare senza dover passare per punti di accesso centralizzati). Problemi di distribuzione e creazione della reputazione nelle reti P2P sono attualmente allo studio,

ed è possibile una futura estensione anche al mondo delle MANET delle soluzioni che verranno adottate.

Un'altra idea interessante per scambiare credenziali digitali tra utenti partecipanti a una rete ad hoc è quella nota col nome di “*resurrecting duckling*”². Nello schema a “*resurrecting duckling*” si parte dal presupposto che i partecipanti alla MANET si trovino contemporaneamente in un preciso luogo fisico. Si sfrutta questo fatto facendo in modo che i partecipanti possano scambiarsi chiavi crittografiche attraverso un canale di diretto contatto tra i loro dispositivi, come un'interfaccia a infrarossi, conoscendosi di persona e basandosi sulla fiducia che essi hanno nel mondo reale. Si tratta quindi di un modello adottabile in piccoli gruppi di utenti, tra di loro tutti fidati (non è infatti un modello per distribuire fiducia, ma solo per scambiare materiale crittografico). Si pensi a una piccola squadra che debba effettuare rilevazioni di qualche tipo sul territorio: all'inizio delle operazioni i partecipanti potrebbero effettuare una “sincronizzazione” dei palmari per evitare che, una volta distribuiti sul territorio, qualcuno possa intromettersi nella MANET da loro realizzata.

In conclusione, buona parte dell'attuale studio sulle MANET è ancora focalizzata sul modo più efficiente per costituire e far funzionare la rete mobile ad hoc. I molteplici campi di applicazione fanno però pensare che il futuro successo di questa tecnologia sarà legato anche a come e se saranno risolte le sfide che un contesto di questo tipo pone sul versante della sicurezza a tutti i livelli dello stack protocollare, a partire dalla protezione dei messaggi che devono costruire e rendere operativa la rete, fino alla creazione di gruppi di utenti identificabili e fidati.

²<http://www-lce.eng.cam.ac.uk/~fms27/duckling/>