Reti Mobili Ad Hoc (Parte II): Aspetti "Sociali"

Date : 26 gennaio 2018

Sommario

Le reti di comunicazione mobili wireless sono diventate parte integrante della nostra società, migliorando notevolmente le capacità di comunicazione, estendendola a qualsiasi ora e luogo e fornendo connettività senza bisogno di un'infrastruttura sottostante. Nella prima parte dell'articolo è stato esaminato il recente settore delle Reti Mobili Ad Hoc (MANET — Mobile Ad Hoc Network), con particolare riferimento agli aspetti architetturali e di sicurezza. In questa seconda parte sono approfonditi gli aspetti rilevanti per l'affermazione del paradigma delle MANET dal punto di vista "sociale" degli incentivi economici per i nodi della rete che ne stimolino la diffusione e l'utilizzo.

Architetture distribuite

Come già osservato nella prima parte, Internet rappresenta l'ambiente informatico più "distribuito" oggi conosciuto, in particolare grazie alla sua architettura aperta. Nuove direzioni di ricerca nella progettazione dei protocolli per reti distribuite si avvalgono di concetti e strumenti della teoria dei giochi: da questa prospettiva, i protocolli sono visti come giochi, con i giocatori rappresentati dai nodi della rete; ogni nodo (agente) ha una propria funzione di utilità, come il flusso di rete (da massimizzare) o il consumo energetico (da minimizzare). Questo approccio (come vedremo nelle sezioni successive) è il punto di vista naturale e più interessante di un'architettura informatica distribuita.

In una rete distribuita, gli agenti utilizzano quindi un protocollo secondo le regole specificate dal protocollo stesso. Tuttavia, tale ipotesi non sempre si applica come quando, ad es. nel caso di Internet, la rete è gestita e utilizzata da soggetti economici diversi, con possibili interessi in conflitto. In altre parole, l'assunto non è ragionevole quando gli agenti che partecipano al protocollo possono agire egoisticamente con l'obiettivo di migliorare qualche utilità personale. L'esempio evidente è un insieme di router in un dato dominio che decidono di non inoltrare il traffico Internet diretto verso domini appartenenti a organizzazioni concorrenti.

In presenza di agenti egoisti, selfish, la progettazione dei protocolli di rete diventa un compito molto più difficile. In realtà, è più di questo: l'influenza dei fattori socioeconomici richiede un

approccio completamente nuovo alla comprensione e alla progettazione di reti aperte mobili. Citando un autore influente nella comunità teorica dell'informatica "gli strumenti matematici e le intuizioni più appropriate per comprendere Internet possono derivare da una fusione di idee algoritmiche con concetti e tecniche dell'economia matematica e della teoria dei giochi" [14].

Questo nuovo approccio può essere sintetizzato brevemente come segue. Prima di tutto, il protocollo e tutti gli agenti che eventualmente partecipano al protocollo definiscono un gioco; questo implica che ogni agente ha la propria funzione di utilità. Secondo questo scenario, un primo obiettivo è la comprensione del costo sociale dell'egoismo. In altre parole, data la misura delle prestazioni complessive del protocollo (questa può essere una funzione globale, come ad esempio il ritardo medio da punto a punto generato da qualsiasi messaggio che viaggia sulla rete), si vuole capire quanto male, rispetto alle prestazioni ottimali ideali, la rete si comporti a causa dell'egoismo di alcuni (vedi ad esempio [15]). Un obiettivo complementare è la progettazione di protocolli che mirano a raggiungere alcuni obiettivi sociali attraverso le proprietà di razionalità e veridicità (che verranno definite nelle sezioni successive). Quest'ultimo è un obiettivo di lunga data nel campo della progettazione architetturale [12].

Nel prosieguo vengono analizzati gli aspetti di sicurezza e i concetti e gli strumenti della teoria dei giochi applicata alle architetture e protocolli di una rete. Successivamente sono descritte più dettagliatamente le strutture di rete distribuite e i protocolli di routing adottati nelle MANET e le prospettive future nel settore.

Sicurezza

Una questione importante riguardante le reti è la minaccia alla sicurezza. Le reti senza fili utilizzano onde radio (segnali elettromagnetici) che provocano un fenomeno di irradiazione nell'area interessata: i segnali che consentono le connessioni di rete superano i confini dell'area di rete, raggiungendo i luoghi circostanti nonostante una perdita proporzionale alla distanza. Questa "trasmissione" involontaria rende possibile l'accesso alla rete non solo al personale autorizzato, ma anche a tutti i vicini[1]. Ma gli stessi problemi di sicurezza si riscontrano anche nelle reti wireless ad hoc (multi-hop): come può essere sicuro un nodo che il suo traffico in uscita non venga intercettato o manomesso? Da un punto di vista puramente crittografico, i servizi di rete ad hoc non implicano problemi "nuovi": l'autenticazione, la riservatezza e l'integrità sono problemi già riscontrati in molte altre reti di comunicazione pubbliche. Ma in una rete wireless ad hoc, la fiducia diventa un problema chiave [10].

Poiché il mezzo di comunicazione (radio) non può essere affidabile (essendo intrinsecamente non protetto, come visto in precedenza), la crittografia è una scelta obbligata, basata sulle chiavi crittografiche utilizzate. Quindi, l'idea di base è quella di creare relazioni di fiducia ("trusted") tra le chiavi senza una CA (Certification Authority) emittente esterna.

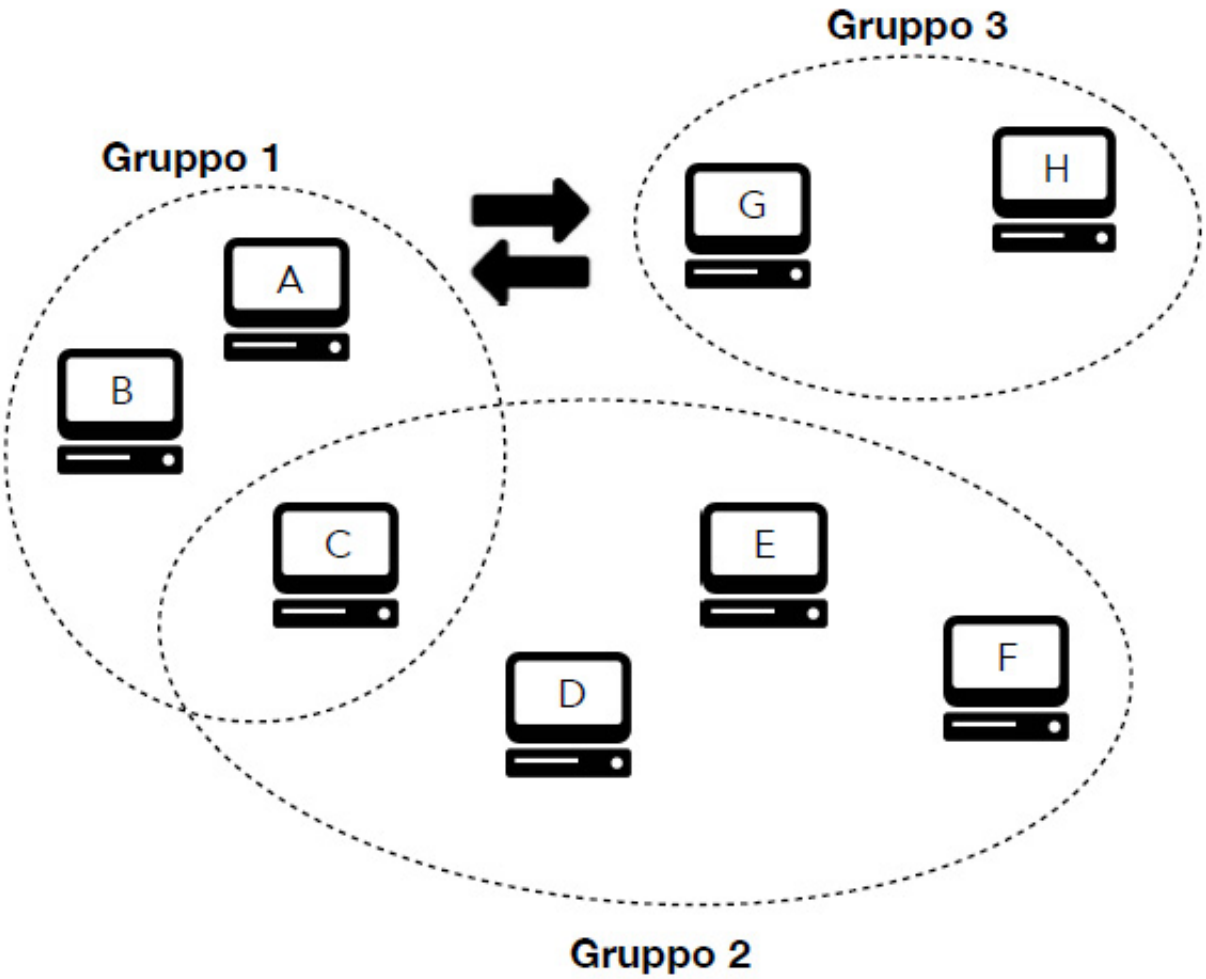

Figura 1: Relazioni di fiducia.

Infatti, una rete ad hoc wireless deriva da nodi con connessione spontanea e mobile, e non vi è alcuna garanzia per un nodo di ottenere chiavi pubbliche fidate da altri nodi, né possono esibire certificati di terzi. Tuttavia, se è consentita la delega fiduciaria internodo, i nodi che hanno già stabilito rapporti di fiducia possono estendere questo privilegio ad altri membri del gruppo: vediamo in dettaglio come funziona.

Il metodo si basa su un sistema PKI (Infrastruttura a chiave pubblica). Supponiamo che tutti i nodi abbiano una connettività reciproca (ad esempio attraverso un protocollo di routing reattivo), come mostrato in fig. 1.

1. Inizialmente, il nodo A assume il ruolo di nodo server nella procedura di delega fiduciaria e avvia il processo di fiducia trasmettendo un messaggio di avvio alla rete. Ogni nodo che riceve tale messaggio ne inoltra un altro contenente il set di chiavi pubbliche fidate. Il nodo A può così stabilire una mappa delle relazioni di fiducia e identificarle. In fig. 4 i gruppi di nodi 1, 2 e 3 partecipano alla catena fiduciaria.

2. Tutti i nodi nel gruppo 2 partecipano indirettamente al rapporto di fiducia con A (attraverso il nodo C). Il nodo A può così raccogliere le chiavi firmate ricevute dal gruppo 2 tramite il nodo C. I nodi nel gruppo 3, invece, non hanno rapporti di fiducia con il nodo A. Tuttavia, una relazione di fiducia tra il nodo G (appartenente al gruppo 3) e A può essere creata "manualmente" per mezzo dello scambio di chiavi fidate.
3. Il nodo A può quindi raccogliere le chiavi firmate ricevute dal gruppo 3 attraverso il nodo G.

Ora il nodo A è pronto ad inoltrare un messaggio alla rete contenente tutte le chiavi firmate raccolte. Questa procedura crea relazioni di fiducia tra i nodi nei tre gruppi e forma un nuovo gruppo di fiducia (trusted group).

Problematiche strategiche nelle reti mobili ad hoc

Come già evidenziato nell'introduzione, cresce l’interesse della comunità informatica a formulare nuovi protocolli (o per lo meno a comprendere il comportamento dei protocolli attualmente in uso) nell'ipotesi di comportamento strategico dei nodi della rete. Nel caso delle reti ad hoc, tuttavia, sono noti pochissimi risultati, che si applicano quasi sempre al routing.

Come esempio di comportamento strategico, un nodo può decidere di non inoltrare il traffico di altri nodi, poiché durante la trasmissione di un messaggio un nodo consuma relativamente più energia che durante i periodi di inattività. Naturalmente, se la maggior parte dei nodi agisce in questo modo, non è possibile il traffico multi-hop. Tuttavia, senza cooperazione, lo scenario informatico distribuito descritto alla fine della sezione precedente (solo per fare un esempio) non può verificarsi in quanto non è economicamente fattibile [11]. L’attenzione di un numero crescente di ricercatori si sta quindi concentrando sulla progettazione di protocolli per reti ad hoc utilizzando gli strumenti della teoria dei giochi e della progettazione di meccanismi (mechanism design). Due proprietà sono particolarmente ricercate: la razionalità (rationality) e la veridicità (truthfulness). Secondo la prima, un agente è sempre motivato a partecipare al gioco (cioè al protocollo), dal momento che la sua utilità non può diminuire come risultato della partecipazione. Veridicità significa che la strategia migliore (cioè quella che massimizza la sua utilità) per un agente è quella di comportarsi secondo il protocollo. A tal fine, si possono prevedere alcune forme di incentivo per motivare i giocatori ad agire in modo veritiero. Ovviamente, se gli agenti sono razionali e veritieri, il protocollo raggiungerà alcuni obiettivi sociali (come la creazione di rotte end-to-end efficienti per tutte le possibili coppie di nodi). Nelle sezioni successive vengono discusse alcune idee pratiche per lo sviluppo di un protocollo di routing veritiero, su cui si basano le future direzioni di ricerca.

Come già accennato, ci sono pochissimi risultati che affrontano il problema del comportamento strategico nelle reti ad hoc wireless. A livello di rotte, sono stati proposti protocolli per l’istituzione di rotte tra coppie di nodi utilizzando pagamenti incentivanti per motivare i nodi intermedi ad agire lealmente [2, 3, 4, 5, 6, 7, 8, 13, 17]. In particolare il lavoro di Anderegg ed Eidenbenz [2] ha introdotto il primo protocollo di routing veritiero. Anche questo protocollo presenta tuttavia una serie di lacune: è caratterizzato da un elevato carico di comunicazione e, cosa ancora più importante, non gode della proprietà di razionalità.

Per quanto riguarda gli altri protocolli, e le applicazioni, soggetti a potenziale manipolazione strategica, non è noto in letteratura alcun risultato significativo.

Obiettivi "sociali"

Gli obiettivi di ricerca nell'ambito del comportamento "sociale" dei nodi di una rete mobile riflettono quelli generali introdotti nella prima parte, che caratterizzano il nuovo scenario per la comprensione e la progettazione di reti aperte. Prima di tutto occorre capire, rispetto ad alcuni potenziali scenari applicativi per reti ad hoc, sotto quali condizioni i protocolli "classici" noti garantiscono il raggiungimento degli obiettivi sociali richiesti. Questo tipo di analisi è stata fatta con riferimento ad alcuni protocolli Internet, come il routing BGP [1]. Le seguenti domande sono di interesse per la ricerca attuale e futura:

- In quale scenario (ad es. modello di traffico, payoff di nodo, ecc.) possiamo evitare la formazione di coalizioni, cioè la formazione di sottoinsiemi di nodi che possono aumentare il loro payoff separandosi dal resto della rete?
- Nel caso negativo, alcuni meccanismi di pagamento relativamente semplici possono contribuire a spingere l'attività della rete verso risultati socialmente migliori?

È probabile che, in molti scenari potenziali, i protocolli noti per le reti ad hoc non godano delle proprietà di razionalità e veridicità. Il secondo (e più ambizioso) quesito è orientato alla progettazione di nuovi protocolli resilienti alle manipolazioni strategiche. Come indicato nella sezione precedente, esistono già alcune proposte per il livello di instradamento, anche se finora non è noto alcun protocollo che implementi le strategie delineate. Tuttavia, vanno analizzate le questioni strategiche anche a livello topologico (per quanto ci risulta, l'unico risultato in questo settore è dovuto a Eidenbenz, Kumar e Zust [9]) e a livello applicativo.

Problemi e prospettive

Consideriamo alcuni protocolli e schemi che, meglio di altri (a nostro avviso), cercano di risolvere il comportamento strategico dei nodi.

Ad hoc VCG

Ad hoc VCG è un protocollo di routing progettato pensando alla teoria dei giochi e ai principi del "mechanism design": si basa sul comportamento "veritiero" dei nodi [2]. Quasi tutti i protocolli di routing si basano sul presupposto che tutti i dispositivi presenti in una rete ad hoc siano cooperativi: in particolare, si suppone che ogni nodo sia disposto a trasmettere dati per conto di altri dispositivi. Se da un lato l'ipotesi della cooperatività può sembrare ragionevole in alcuni contesti, dall'altro la cooperazione non può certo essere ipotizzata in una rete ad hoc più generale. Infatti, l'inoltro dei pacchetti per conto di altri nodi della rete implica un consumo energetico, e in un caso estremo un nodo della rete potrebbe trovarsi nella situazione di non avere più l'energia della batteria disponibile, anche se non ha mai inviato o ricevuto alcun messaggio! Se i nodi di rete non sono gestiti da un'entità centrale (come, invece, i telefoni cellulari GSM) ma sono agenti indipendenti e orientati al profitto, saranno sicuramente "egoisti".

Il protocollo VCG intende affrontare questo problema e vuole raggiungere due obiettivi: l'efficienza economica e la veridicità. Per raggiungere l'efficienza dei costi i progettisti hanno iniziato con il concetto di efficienza energetica, che rappresenta una pietra miliare nella progettazione di diversi protocolli di routing: un protocollo con efficienza energetica assicura infatti che i pacchetti raggiungano i nodi target attraverso il percorso di minor consumo energetico. L'energia totale consumata sarà data dalla somma dei singoli consumi delle connessioni tra il mittente e i nodi intermedi. In una situazione ideale, un nodo intermedio dovrebbe utilizzare un livello di emissione di energia appena sufficiente per raggiungere il nodo successivo più vicino. Per fare questo, il protocollo Ad hoc VCG utilizza un meccanismo di controllo dell'energia che inizia con l'invio, da parte del nodo emittente, di un pacchetto contenente, nell'header, la potenza di emissione utilizzata; grazie a questo trucco, il nodo ricevente conosce il livello minimo di energia necessario per comunicare con il nodo emittente, ed è in grado di confrontare il livello di energia effettivo con quello stimato: se il primo supera il secondo, il nodo ricevente invierà al nodo emittente un pacchetto contenente l'esatto livello di energia necessario per raggiungerlo, riducendo così i consumi energetici in eccesso.

L'efficienza energetica è un obiettivo auspicabile solo da un punto di vista della rete globale, meno da una prospettiva di nodo "egoista". Infatti, se un nodo viene spesso coinvolto nell'inoltro dei pacchetti per conto di altri nodi della rete, sarà certo che è sul percorso più efficiente dal punto di vista energetico, ma vedrà rapidamente svanire la carica della batteria semplicemente servendo le trasmissioni di altri nodi. Allora tenderà probabilmente a sembrare "morto" in modo da smettere di inoltrare messaggi per conto di altri nodi. Questo comportamento non cooperativo rappresenta il problema fondamentale in quasi tutte le reti ad hoc in cui i nodi mirano a massimizzare il proprio profitto, e può essere un serio ostacolo alla loro diffusione.

I ricercatori del protocollo Ad hoc VCG propongono di utilizzare il costo dell'energia c = costo unitario di trasmissione dell'energia (in dollari/Watt): si tratta di un costo unitario e, se un nodo impiega un consumo energetico P, richiederà una ricompensa (payoff) pari a c·P. D'altra parte, se un nodo non ottiene una ricompensa adeguata che copra i suoi costi, allora si limiterà a negare l'inoltro dei pacchetti. Un'altra idea è quella di dichiarare anche la potenza del segnale ricevuto rispetto ai nodi vicini, ma questo può portare a comportamenti scorretti tendenti ad ottenere rendimenti più elevati attraverso dichiarazioni "false": per risolvere questo problema, è stato proposto uno schema di ricompensa che scoraggia le frodi pagando i nodi tanto quanto dovrebbero essere pagati attraverso dichiarazioni sleali. Per un nodo intermedio vi che si trova sul percorso più breve tra un nodo mittente S e una destinazione D, la ricompensa totale Mi corrisponde alla somma dei costi di trasmissione dichiarati, più un supplemento Ei = C+i ? C?i [2]. Il regime di "ricompensa" è definito in modo da fornire ai nodi lo stesso importo, indipendentemente dai costi di instradamento dichiarati.

Il comportamento strategico dei nodi

Per risolvere il problema del comportamento strategico dei nodi è stato proposto uno schema di partecipazione economica, chiamato Ad Hoc Participation Economy Scheme (APE). Questo schema richiede che tutti i nodi di una MANET siano forzati ad inoltrare pacchetti di altri nodi e ricompensati con "moneta virtuale"; tale schema considera l'energia della batteria come un

bene fisico, quantificabile in termini di moneta virtuale. Ogni nodo può virtualmente "stampare" la propria moneta e ne sarà responsabile nei confronti di speciali nodi banchieri: in questo scenario, tutti i nodi sono obbligati ad offrire servizi alla rete per mantenere un saldo positivo. Un nodo banchiere è un nodo speciale di cui si fidano tutti gli altri nodi che partecipano alla rete: svolge la maggior parte dei controlli di sicurezza e tiene traccia di tutti i conti dei singoli nodi. L'invio delle informazioni di pagamento ai nodi banchieri è l'unico modo per ottenere la conferma del pagamento, e ogni nodo sceglie casualmente i tempi di trasmissione in modo da non rendere la rete congestionata.

Prima che i nodi siano attivi nel routing devono essere conosciuti ai nodi banchieri: APE adotta uno schema di autenticazione simile a quello utilizzato nel World Wide Web. Ogni nodo coinvolto avrà un ID digitale "firmato" dal nodo banchiere, dimostrandone l'identità attraverso una chiave pubblica. Tale ID digitale deve essere ottenuto da un'entità esterna al sistema: in tal modo, esso fornirà anche un'autenticazione affidabile internodo. Dopo aver ricevuto le informazioni sui pagamenti, il nodo banchiere la ritrasmette ai nodi di addebito: alla loro conferma, i pagamenti saranno accreditati ai beneficiari, con la cancellazione delle informazioni sui pagamenti dai nodi creditori e debitori. In seguito, quando tutte le informazioni su un particolare nodo saranno consolidate, il nodo banchiere verificherà il beneficiario per ottenere la corretta quantità di denaro virtuale: se non c'è differenza tra il traffico totale inoltrato e il pagamento ricevuto, tali informazioni saranno definitivamente rimosse anche dalla memoria del nodo banchiere.

Tale schema può essere oggi ad esempio implementato mediante la tecnologia blockchain[16], la stessa alla base della diffusione dei Bitcoin.

SPRITE

Un altro schema semplice a prova di cheat-proof è lo SPRITE [17], basato su incentivi per i nodi che partecipano all'attività di routing. L'architettura di sistema di SPRITE è costituita da un Credit Clearance Service (CCS) e da una serie di nodi mobili, dotati di interfacce di rete attraverso le quali è possibile inviare e ricevere messaggi in ambienti wireless utilizzando, ad esempio, GPRS/UMTS/LTE su ampia scala e standard 802.11 o Bluetooth in un'area limitata. Ogni nodo dovrebbe avere un digital ID ottenuto da una CA e il mittente conosce l'intero percorso verso la destinazione attraverso un protocollo di routing ad hoc basato su DSR. Quando un nodo trasmette i propri messaggi perde credito (o moneta virtuale), che viene utilizzato per coprire i costi dei nodi intermedi di inoltro dei pacchetti. D'altra parte, quando un nodo inoltra pacchetti per conto di altri riceve credito per poter inviare i propri messaggi. Ci sono due modi in cui un nodo può ottenere più credito:

1. acquistando moneta virtuale a un tasso di cambio variabile basato sulle prestazioni del sistema;
2. inoltrando messaggi per conto di altri nodi, e ssendo quest'ultimo il metodo preferito.

Nel sistema SPRITE, per ottenere crediti un nodo deve comunicare a CCS quali messaggi ha inoltrato. SPRITE mira a prevenire comportamenti fraudolenti e a promuovere la cooperazione tra i nodi della rete: per raggiungere questi obiettivi, il sistema non si occupa di pagamenti

equilibrati, cioè non richiede che il debito totale del mittente equivalga al credito totale dei nodi intermedi ricevuto per la loro attività di inoltro. Infatti, per evitare comportamenti fraudolenti, il mittente è debitore CCS di un importo superiore a quello dovuto ai nodi intermedi; solo in un secondo tempo il credito eccedente sarà ripartito uniformemente tra i nodi o darà un credito fisso a ciascun nodo. Questa procedura dovrebbe evitare comportamenti scorretti.

Conclusioni

Quindi, sintetizzando la discussione precedente, è possibile trarre alcune conclusioni che mettono in luce i principali problemi e orientamenti tecnologici:

- i nodi dovrebbero dichiarare il loro costo unitario di energia per ottenere un percorso efficiente, in modo che il protocollo raggiunga l'efficienza economica e la veridicità (tutti i "player" utilizzano una strategia dominante);
- le sessioni devono essere ragionevolmente lunghe per ridurre al minimo l'overhead della fase di ricerca del percorso;
- future direzioni di ricerca verso le reti mobili ad hoc considerano una distribuzione nota dei tipi di nodo oppure una parziale violazione locale dei requisiti di efficienza economica e veridicità;
- esiste un grave problema nel caso di una "coalizione di secessione" composta da più di un nodo;
- i protocolli di instradamento possono essere integrati con l'adozione di regimi di pagamento quali moneta virtuale (Sprite [17], Nuglet [8]) e nodi banchieri (APE [13]);
- sono necessari maggiori sforzi di ricerca nel campo degli aspetti algoritmici e della veridicità;
- la teoria dei giochi e il "mechanism design" possono aiutare a risolvere i problemi ancora aperti nella progettazione del routing della rete.

Riferimenti bibliografici

- [1] Agarwal, R., and Ergun, Ö. Mechanism design for a multicommodity flow game in service network alliances. Operations Research Letters 36, 5 (2008), 520–524.
- [2] Anderegg, L., and Eidenbenz, S. Ad hoc-vcg: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In Proc. ACM Mobicom (2003), pp. 245–259.
- [3] Buchegger, S. Performance analysis of the confidant protocol: Cooperation of nodes-fairness in distributed ad-hoc netwoks. MobiHoc 2002, Lausanne (2002).
- [4] Buchegger, S., and Le Boudec, J.-Y. Cooperative routing in mobile ad-hoc networks: Current efforts against malice and selfishness. In Mobile Internet Workshop. Informatik 2002. (2002), no. LCA-CONF-2002-022.
- [5] Buchegger, S., and Le Boudec, J.-Y. Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In Parallel, Distribu- ted and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on (2002), IEEE, pp. 403–410.
- [6] Buttyán, L., and Hubaux, J.-P. Enforcing service availability in mobile ad-hoc wans.

In Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing (2000), IEEE Press, pp. 87–96.
- [7] Buttyán, L., and Hubaux, J.-P. Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications 8, 5 (2003), 579–592.
- [8] Buttyán, L., and Hubaux, J.-P. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM Mobile Networks & Applications 8 (October 2003).
- [9] Eidenbenz, S., Kumar, V., and Zust, S. Equilibria in topology control games for ad hoc networks. Mobile Networks and Applications 11, 2 (2006), 143–159.
- [10] Frodigh, M., Johansson, P., and Larsson, P. Wireless ad hoc networking: the art of networking without a network. Ericsson review 4, 4 (2000), 249.
- [11] Mas-Colell, A., Whinston, M. D., Green, J. R., et al. Microeconomic theory, vol. 1. Oxford university press New York, 1995.
- [12] Nisan, N., and Ronen, A. Algorithmic mechanism design. In Proceedings of the thirty-first annual ACM symposium on Theory of computing (1999), ACM, pp. 129– 140.
- [13] Obreiter, P., and Nimis, J. A taxonomy of incentive patterns. In International Workshop on Agents and P2P Computing (2003), Springer, Berlin, Heidelberg, pp. 89–100.
- [14] Papadimitriou, C. Algorithms, games, and the internet. In Proceedings of the thirty-third annual ACM symposium on Theory of computing (2001), ACM, pp. 749–753.
- [15] Roughgarden, T., and Tardos, É. How bad is selfish routing? Journal of the ACM (JACM) 49, 2 (2002), 236–259.
- [16] Wright, A., and De Filippi, P. Decentralized blockchain technology and the rise of lex cryptographia.
- [17] Zhong, S., Chen, J., and Yang, Y. R. Sprite: A simple, cheat-proof, credit- based system for mobile ad-hoc networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (2003), vol. 3, IEEE, pp. 1987–1997.

Note

[1] Come viene fatto nel "Warchalcking" o "Noderunner" da hacker alla ricerca di nodi di rete wireless accessibili, contrassegnando le zone non protette con i tradizionali segnali in gesso

[2] Dove C+i è il costo totale del percorso più breve (shortest path) tra i nodi S e D compreso vi, mentre C?i è il costo totale del percorso più breve tra S e D senza vi.

A cura di: **Crescenzio Gallo, Michele Perilli, Michelangelo de Bonis**
Università di Foggia