Bluetooth, Wi-Fi, TCP senza fili
Dottorato 2004

Agenda delle lezioni

Posizione originaria: <http://fly.isti.cnr.it/didattica/dottorato/wireless04.html>.

Una panoramica sui protocolli Wi-Fi e Bluetooth si trova nell'articolo *Bluetooth and Wi-Fi wireless protocols: a survey and a comparison*, basato sulla tesi di laurea *Confronto fra due protocolli per reti Wireless: IEEE 802.11 e Bluetooth*, che comprende una descrizione dei protocolli e un glossario dei numerosi acronimi adottati nella descrizione dei protocolli.

Protocollo IEEE 802.15.1 (Bluetooth)

- Presentazione dell'articolo succitato.
- Una vecchia presentazione dell'architettura dello standard Bluetooth.
- La pagina del gruppo di lavoro sullo standard IEEE 802.15.

Protocollo IEEE 802.11 (Wi-Fi)

- Questa è una recente presentazione molto ben fatta e ampia, sono 97 lucidi che descrivono anche i numerosi emendamenti allo standard 802.11 del 1997.
- Una breve discussione del throughput ottenibile da una rete 802.11b, con chiare illustrazioni degli header ad ogni livello.
- Questa è una presentazione centrata sulla codifica e acquisizione.
- La pagina del gruppo di lavoro sullo standard IEEE 802.11.

TCP su wireless

Una panoramica sulle varie tecniche usate per migliorare le prestazioni del TCP su link radio si trova su Enhancing wireless Internet performance (PDF). È anche consigliata la lettura di RFC 3135: *Performance enhancing proxies intended to mitigate link-related degradations.*

- Il meccanismo di Fast Retransmit, utilizzato nella variante Reno del TCP che è descritta in *RFC 2581: TCP congestion control*, allevia i problemi derivanti da perdite occasionali. Il meccanismo consente il recupero di un pacchetto perduto per ogni RTT, a prezzo di un dimezzamento della finestra di trasmissione. Più di una perdita in un RTT possono causare un timeout.
- Questo meccanismo è perfezionato nella variante del TCP che è descritta in *RFC 2582: The NewReno modification to TCP's Fast Recovery algorithm*, che è quella comunemente usata nei moderni sistemi operativi. NewReno può recuperare più perdite avvenute nella stessa finestra di trasmissione, al ritmo di una per RTT.
- Perché il Fast Retransmit funzioni, la finestra di trasmissione deve essere lunga alemno quattro pacchetti. Il meccanismo di Limited Transfer (RCF 3042), ancora poco usato, permette di beneficiare degli effetti del Fast Retransmit anche con finestre più piccole, basandosi sullo stesso principio di *conservazione dei pacchetti*.
- Un ulteriore miglioramento consiste nell'uso dell'opzione SACK (RFC 2018) o D-SACK (RFC 2883), grazie alle quali è possibile recuperare un maggior numero di pacchetti peduti in una finestra di

trasmissione.

- È da notare che, benché il ritardo connesso al link wireless terrestre sia molto piccolo per i protocolli che abbiamo esaminato (Wi-Fi e Bluetooth), il tempo di RTT riguarda l'intero percorso fra i nodi terminali, e non è generalmente trascurabile.
- I protocolli wireless usati su link con bassi ritardi, come Bluetooth e Wi-Fi, utilizzano spesso tecniche di ARQ (automatic repeat request), cioè ritrasmettono i pacchetti perduti un certo numero di volte prima di considerarli perduti. Questa tecnica agisce sotto il livello del TCP, ed è efficace quando le perdite di pacchetti sono poco correlate ed il ritardo sul link è piccolo, ma se queste condizioni non sono soddisfatte ha l'effetto di rallentare i meccanismi di recupero del TCP. Una tecnica analoga per la correzione di errore sotto il TCP è la forward erasure correction (FZC).
- Explicit Loss Notification (ELN) è una tecnica che comunica al mittente i numeri dei paccehtti persi per errore sul canale. Necessita di una stazione base wireless che conosca il TCP, in maniera da identificare i pacchetti mancanti e accendere un apposito bit sugli ack che richiedono la trasmissione di un pacchetto perso per errore sul link. Per distinguere gli errori dalla congestione, la stazione base deve conoscere la coda del trasmettitore, e sapere che non era piena quando il pacchetto mancante doveva essere trasmesso. Chi riceve una ELN ritrasmette il pacchetot senza ridurre la finestra di trasmissione.
- Sono state proposte numerose varianti di questa tecnica, per esempio EBSN (explicit bad state notification) cambia il timeout, delayed duplicate acks (DDA) usa la rilevazione di due dupack per attivare una ritrasmissione a livello di link.
- L'opzione HACK, proposta in versione estesa in *An adaptive TCP protocol for lossy mobile environment*, permetterebbe di identificare i pacchetti perduti, ma suppone che i pacchetti con CRC errato siano consegnati al destinatario.
- Il protocollo I-TCP: *Indirect TCP for mobile hosts* è un esempio di applicazione del *proxying*, o *splitting*, una tecnica che non mantiene la semantica end-to-end, perché crea dei pacchetti di ack quando ancora il pacchetto dati non è stato ricevuto dal nodo destinatario. Il protocollo I-TCP crea due connessioni TCP separate, e richiede modifiche al TCP sui nodi wireless. L'implementazione proposta è interamente in spazio utente. Sono stati proposti approcci analoghi che usano un protocollo apposito per la parte senza fili. La stessa tecnica era anche chiamata *spoofing*, termine oggi usato più frequentemente per indicare un tipo di attacco TCP.
- Il protocollo *Snoop*, descritto nell'articolo Improving TCP/IP Performance over Wireless Networks è un esempio di applicazione di *snooping*, una tecnica che mantiene la semantica end-to-end del protocollo TCP. Quando vede un ack duplicato, indice di un pacchetto perso, intercetta l'ack e non lo prosegue, ma piuttosto ritrasmette al destinatario il pacchetto perduto. Solo quando gli ack sono in sequenza vengono proseguiti. In tal modo la trasmissione viene rallentata quel tanto che basta per ritrasmettere i pacchetti perduti, ma il TCP mittente vede solo un ritardo, non vede pacchetti perduti, e quindi non dimezza la propria finestra di trasmissione. I ritardi sono tarati in modo da non indurre un timeout nel mittente TCP. Il protocollo è implementato nei nodi gateway fra la rete cablata e quella radio, e non tocca i nodi terminali. Analoghe proprietà ha il protocollo WTCP.
- Alcuni protocolli manipolano gli ack, ritmandoli e manipolando la finestra di ricezione, in modo da controllare il flusso sia in termini di velocità sia in termini di regolarità.
- Sia le tecniche di splitting sia quelle di snooping permettono di nacondere al mittente una temporanea perdita di connettività dovuta a roaming o caduta del link. Per sospendere le trasmissioni del mittente basta inviargli una ack con la finestra di ricezione posta a zero. Se non c'è splitting, l'ack verrà clonato dall'ultimo ack; è possibile far funzionare questo sistema in entrambe le direzioni usando una coppia di PEP, oppure, come fa M-TCP, sospendendo tutti i timer sul TCP che gira sul nodo mobile.
- Il difetto principale dei PEP è che non funzionano per traffico che usa cifratura end-to-end (IPsec). Altri difetti possibili dei PEP comprendono impossibilità di usare mezzi diagnostici per la verifica della connettività, complicazione della gestione della mobilità, mancato funzionamento nel caso di routing asimmetrico, complicazione della gestione della qualità del servizio, limiti al numero di connessioni gestibili dai nodi intermedi. Nel caso di proxy, si perde la semantica end-to-end, con l'aggiunta un terzo punto vulnerabile alla connessione, oltre ai due nodi terminali. Questo non è un problema nel caso in cui il nodo su cui è implementato il PEP è comunque un passaggio obbligato per ogni connessione fra i nodi terminali.