



APPLICAZIONE DEI MECCANISMI DHT NELL' AMBITO DELLE RETI AZIENDALI

Relatore: Prof. LUCA VELTRI
Correlatore: Ing. NATALYA FEDOTOVA

Tesi di laurea di:
STEFANO FANTI

Anno Accademico 2005-2006

Sempre un maggior numero di organizzazioni aziendali dipendono dalle loro computer network per gestire e realizzare il loro business. Ogni azienda, di medie e grandi dimensioni, deve quindi possedere un'infrastruttura informatica che le consenta di reperire e produrre dati velocemente, in modo semplice e in totale sicurezza. Sempre più aziende accumulano ingenti quantità di dati nei loro database e sempre più si rendono conto che la produttività può essere aumentata rendendo queste informazioni maggiormente accessibili ai dipendenti, in accordo con una politica di attribuzione di differenti privilegi di accesso ai dati agli utenti dei vari dipartimenti aziendali.

Per loro natura i database aziendali, grandi o piccoli, presentano una *struttura centralizzata* che, sebbene rappresenti il modo più intuitivo di organizzare una enterprise network, non rappresenta un metodo così sicuro, scalabile ed economico come invece ci si aspetterebbe. Il sistema client/server presente nelle connessioni tra i terminali di una rete aziendale centralizzata e il data center, presenta alcuni problemi critici per il buon funzionamento della rete, dal punto di vista dell'efficienza e della sicurezza: la presenza di un *singolo point of failure* sia in termini di guasti sia di attacchi volontari (in quanto i server centrali sono gli unici responsabili dell'archiviazione delle risorse), la riduzione della larghezza di banda e un aumento del tempo di accesso alle risorse qualora molti client richiedano un accesso simultaneo ad esse. A questi si sommano altre problematiche come la ridotta scalabilità nel caso di una crescita delle dimensioni dell'azienda, i costi di amministrazione e mantenimento delle strutture dedicate allo storage e infine l'elevata esposizione agli attacchi.

L'obiettivo di questo lavoro di tesi consiste nell'offrire una soluzione ai problemi derivanti dall'utilizzo di una struttura centralizzata nelle reti aziendali, con particolare riferimento al livello di sicurezza e all'efficienza dello storage e del backup delle risorse.

Per risolvere questi problemi si è pensato di applicare alla enterprise network una *struttura decentralizzata* di archiviazione e scambio dei dati, tipica dei sistemi di condivisione peer-to-peer, che sfrutta le risorse collettive di tutti i terminali della rete. In questo modo si riesce a creare uno storage system sicuro e affidabile, che offre alla enterprise network tutti i servizi di cui questa già disponeva in ambito centralizzato, ma con un notevole miglioramento in termini di resistenza agli attacchi e a malfunzionamenti. L'azienda ha così la certezza e la sicurezza che le risorse saranno ospitate presso l'enorme spazio disco distribuito presente complessivamente tra tutti i terminali della propria rete, risolvendo così problemi (come il packet filtering e attacchi di tipo Denial of Service) legati all'outsourcing della memorizzazione dei dati.

Per quanto riguarda l'organizzazione del lavoro svolto, sono state inizialmente descritte le caratteristiche generali delle reti aziendali e i problemi presenti nelle reti centralizzate. Dopo la presentazione dei sistemi peer-to-peer esistenti, ci si focalizza sulle *overlay network di tipo strutturato*, che utilizzano un metodo di indicizzazione dei contenuti basato sulle *Distributed Hash Table* (DHT), e in particolare si studia il protocollo di *Kademlia*, che si ritiene costituisca il punto di partenza più adatto per l'applicazione dei meccanismi DHT nell'ambito delle reti aziendali.

Per meglio adattare le funzionalità offerte da questo sistema di condivisione dati, sono state effettuate alcune *modifiche al protocollo di Kademlia*, con lo scopo soprattutto di poter assegnare in modo semplice differenti privilegi di accesso alle risorse ai diversi utenti, e di migliorare il grado di sicurezza della rete. Le modifiche più rilevanti riguardano in particolare: l'introduzione di un prefisso di lunghezza variabile all'interno dell'identificativo di ogni nodo e chiave (per adattare il protocollo a situazioni reali in ambito aziendale), la creazione di una gerarchia di privilegi posseduti dai singoli nodi per quanto riguarda l'accesso alle risorse, l'introduzione di un modello di memorizzazione "ad albero" (che semplifica l'attività di storage) e l'introduzione di un "backup a chiave complementare" (che ha lo scopo di rendere immune la rete da attacchi di tipo Denial of Service).

Sulla base delle considerazioni esposte nel corso della trattazione, si può affermare che il principale obiettivo di questo studio è stato raggiunto. E' stata infatti realizzata una struttura di rete aziendale completamente distribuita (basata sull'algoritmo di routing e di memorizzazione dei dati adottato in Kademlia) che è caratterizzata da un *livello di sicurezza della rete notevolmente aumentato* rispetto a quello presente nel modello centralizzato attualmente adottato dalle enterprise network. Nel modello che è stato realizzato, tutti i nodi della rete hanno le stesse funzioni, responsabilità e caratteristiche, sia in termini di storage, sia di banda assegnata, sia di probabilità di essere soggetti ad attacchi.

L'applicazione dei meccanismi DHT nell'ambito delle reti aziendali ha permesso di ottenere un sistema di memorizzazione e ricerca dei dati più flessibile, sicuro, robusto ed economico rispetto a quello di tipo centralizzato, e tale da adattarsi ai cambiamenti organizzativi interni all'azienda senza la necessità di alcuna modifica strutturale per quanto riguarda l'archiviazione delle risorse.