Rețea de comunicații anonime criptate pe infrastructură peer-to-peer

Sergiu Gabriel Silca

Rezumat

Lucrarea de față presupune construirea unei rețele distribuite P2P (Peer-to-Peer) ce are ca scop posibilitatea navigării pe internet în mod anonim. Păstrarea anonimității se realizează prin metode specifice de rutare ce facilitează ascunderea identității unui nod în rețea.

Aplicația se adresează tuturor celor care doresc să își păstreze identitatea și comunicațiile pe internet ascunse. Exemple de utilizatori pot fi: jurnaliști, activiști, cetățeni al unui stat totalitar, hack-eri etc.

Limbajul ce stă la baza implementării proiectului este C#. Arhitectura folosită este Peer-to-Peer, unde același proiect software rulează pe mai multe mașini având același comportament. O componentă importantă în cadrul unui sistem distribuit este comunicația. Comunicația dintre nodurile rețelei este realizată prin intermediul socket-urilor. Acestea folosesc pentru transmiterea mesajelor protocolul TCP/IP.

Având în vedere că un nod trebuie să fie atât client cât și server s-a folosit la bază arhitectura Client – Server. Nodul folosește pentru a comunica propria implementare de protocol. Se reușește astfel decuplarea dintre o conexiune din partea browser-ului și una din partea unui nod din rețea. Pe lângă acest aspect, protocolul ajută în special la rutarea pachetelor în rețea prin specificarea nodului ce urmează să primească mesajul.

Proiectul practic este împărțit în două componente principale: serverul de administrare a nodurilor din rețea și aplicația P2P, ce rulează pe mai multe mașini.

Serverul de administrare a nodurilor, după cum se poate deduce din nume, se ocupă de managementul nodurilor din rețea. Fiecare nod ce dorește participarea la rețea este nevoit să se adreseze serverului printr-o cerere de participare. Informațiile legate de rețea sunt reținute cu ajutorul unei baze de date MySQL.

A doua componentă, aplicația P2P, are ca scop rutarea pachetelor în rețea. Tehnica folosită este „onion routing”, ce presupune încapsularea mesajelor, ce vor fi trimise, în straturi criptate cu cheile publice a nodurilor prin care vor trece. Fiecare nod, prin care trece mesajul criptat, va decripta câte un strat până la ultimul nod din rută. Prin decriptare nodul află cui trebuie să trimită mai departe mesajul. În acest fel expeditorul rămâne anonim deoarece fiecare intermediar cunoaște doar adresa nodurilor precedente și următoare.