V dnešní době se architektura určitých typů služeb jako jsou distribuované výpočty, distribuovaná úložiště nebo sítě pro distribuci obsahu, posouvá od tradičního modelu klient-server k více škálovatelnému a robustnějšímu P2P modelu. V takto složitém, anonymním a otevřeném systému je ale velice komplikované zajistit alespoň základní míru zabezpečení. Největší hrozbu představují útočníci, kteří dokáží spolupracovat a s použitím sofistikovaných strategií se snaží obejít stávající bezpečnostní systémy. Jako obrana proti těmto uživatelům vznikly takzvané systémy na řízení důvěry v P2P sítích. Nicméně jejich účinnost právě proti sofistikovaným strategiím není dostatečně ověřena.

V této práci jsme navrhli nový systém pro řízení důvěry s názvem BubbleTrust a vyvinuli simulační framework P2PTrustSim pro testování různých systémů na řízení důvěry a libovolné strategii používané útočníky. Navržený framework definuje několik kriterií, která pomohou vyhodnotit úspěšnost dané strategie oproti zkoumanému systému. V rámci simulací jsme testovali čtyři systémy jež reprezentují současné hlavní přístupy k řízení důvěry a BubbleTrust.