View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Creative Repository of Electro-Communications

修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　情報システム学研究科　　情報ネットワークシステム学専攻 博士前期課程		
氏　　名	任　杰	学籍番号	1052020
論 文 題 目	カウツグラフを用いた匿名通信の安全性向上		

要　　旨

近年，インターネットの急速な発展と伴い，通信情報の不正利用も問題になる．特に，行政 や医療など高度の機密性が求められる情報の保護は注目を浴びている．通信の内容を暗号化によって隠すなけではなく，送信者と受信者の身分と関連性を秘匿する匿名通信が必要になる.

1997年にSyversonらが提案したオニオンルーティンング方式は，代表的な匿名通信方式である．2004年にDingledineによって，Torというオニオンルーティング方式を基づいた匿名通信システムが生まれた．しかし，Torでは，ルーティング情報の配布はサーバーですべて処理して，その負担が著しく大きい.

この問題を解決する為に，DHT（分散ハッシュテーブル）を利用して，サーバーの負担を分散してルーティング情報の配布する方法が多数提案された．一方，従来からDHTに対する攻撃も匿名通信システムの脅威になる．Nambiarらが提案したSalsaでは，ノードが複数経路で検索を行う方法でルーティング攻撃を抑える．しかし，それはDoS攻撃を受けやすい．また，Mittalらは影(shadow)というノードが情報に署名を与える方法をShadowwalkerで提案した．検索を行うノードが署名を利用して手にした情報を認証することができる．しかし，エクリプス攻撃にはまだ弱いと指摘される．これらの匿名通信システムで利用されるDHTはノードの隣接関係が弱く，攻撃者に利用され，攻撃の標的になることがある.

そこで本研究では，カウツグラフをベースにしたSKYというDHTを利用する．カウツグラフでは，ノードの隣接関係が明確である．この性質を用いて，Shadowwalkerの他のノードが署名を与える方法を元にして，同一のメッセージにの対する各署名の間に関連性をつける．この方法で，ルーティング攻撃，DoS攻撃及びエクリプス攻撃を抑える．また，本システムにおいて，これらの攻撃が成功しにくいことをを示した.