研究・技術シーズ集
ピックアップ

8

匿名通信　3-Mode Net

多重ループバック

インターネット上での通信の匿名化技術

河野　和宏
社会安全学部　安全マネジメント学科

Point1　本研究の概要

　インターネット上で投票や遠隔医療、オークションなどのサービスを安心して利用するためには、匿名性やプライバシの十分な確保が不可欠です。本技術では、匿名通信3-Mode Netを解析手法を応用し、暗号化処理が不要の3つの動作を中継ノードが確率的に選択することで、送受信者双方を秘匿可能とすることができます。

Point2　応用可能な分野

オンラインショッピングなどのような通信内容の秘匿が求められるサービスや、電子投票や医療相談などのような通信内容の秘匿だけでなく、誰と誰が通信しているかを秘匿することが要求されるサービスに展開が可能です。

Point3　連携を希望する業種等

　国内におけるパーソナル情報市場の市場は、金融・保険業、小売業、宿泊・旅行業、通信と続きますが、上記、応用可能な分野に関連すれば業種は問いません。

詳細な研究・技術シーズは次のページへ

情報通信

インターネット上での通信の匿名化技術

用途・応用分野

・インターネット通信における送受信者の秘匿が必要なサービス
・電子投票などのプライバシー保護が必要とされる通信サービス

本技術の特徴・従来技術との比較

・暗号化を利用せずに送受信者の匿名性を担保するあらたな匿名通信システムを実現
・多重暗号化により送受信者の匿名性を担保する通信システム（Onion RoutingやTorが代表）と比べて、中継ノードの暗号化処理負担の軽減やネットワークへの負荷の軽減が可能
・確率を用いて送信者の匿名性を担保する通信システム（Crowds）の欠点である、受信者の匿名性が担保可能

技術の概要

○通信の匿名化の方法
　複数の中継地点（中継ノード）を介して送信者から受信者にメッセージが届くようにする
○本技術での実現方法
　暗号化処理が不要の3つの動作を中継ノードが確率的に選択することで、送受信者双方を秘匿可能にする
　本技術の元となる匿名通信3-Mode Netを解析手法を応用[3]

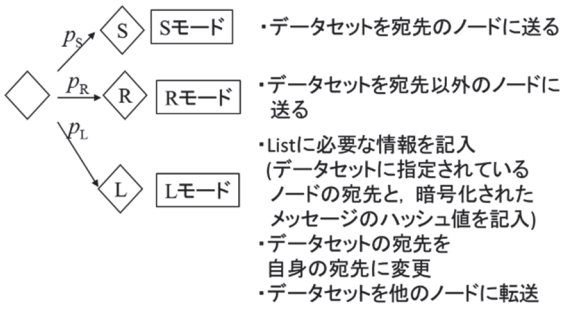

図1：中継ノードの行動 [1]

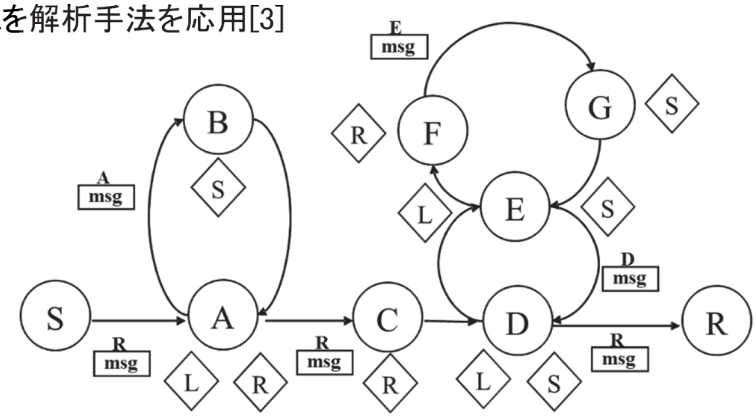

図2：動作例 [1]

特許・論文

1. 河野和宏，″インターネット上で匿名性を有するサービスを実現するために，″ 社会安全学研究，no. 1，pp. 13-26，2011.
2. K. Kono, S. Nakano, Y. Ito, and N. Babaguchi, ″Anonymous Communication System Based on Multiple Loopbacks,″ Journal of Information Assurance and Security, 8 pages, online published 2011.
3. K. Kono, S. Nakano, Y. Ito, and N. Babaguchi, ″Theoretical Analysis of the Performance of Anonymous Communication System 3-Mode Net,″ IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E93-A, no. 7, pp. 1338-1345, 2010.

研究者

河野　和宏
社会安全学部　安全マネジメント学科
河野研究室

お問合わせ先
関西大学 社会連携部 産学官連携センター
TEL：06-6368-1245
MAIL：sangakukan-mm@ml.kandai.jp