様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　24　年　　5 月　　30 日現在

機関番号：34416
研究種目：研究活動スタート支援
研究期間：2010～2011
課題番号：22860070
研究課題名（和文）
個人情報保護のための匿名性を有するシステムの開発
研究課題名（英文）
Network System with Anonymity for Protecting Personal Information
研究代表者
河野　和宏　（KOUNO　KAZUHIRO）
関西大学・社会安全学部・助教
研究者番号：　60581238

研究成果の概要（和文）：
本研究では，匿名性に関わるシステム，特に匿名通信方式 3-Mode Net の解析および 3-Mode Net の改良手法を提案した．3-Mode Net の解析では，ランダムウォーク理論を用いて 3-Mode Net における中継ノード数や暗号化処理回数に加え，送信者および受信者の匿名性を定量的に評価した．また，3-Mode Net の改良型である多重ループバックを用いた方式を提案し，多重暗号化を用いない方式に変更することに成功した．さらに，3-Mode Net の実装や匿名認証・匿名署名方式などの他の匿名性を有するシステムとの関連性も検討した．

研究成果の概要（英文）：
This study proposed a system with anonymity, in particular anonymous communication system 3-Mode Net. This study analyzed the performance of 3-Mode Net and proposed a new version of 3-Mode Net. We evaluated the number of relay nodes, the number of encryption, sender anonymity, and receiver anonymity of 3-Mode Net by using random walk theory. We also proposed a new anonymous communication system based on multiple loopbacks, which used no multiple encryption. In addition, we implement 3-Mode Net, and consider the relationships between 3-Mode Net and other systems with anonymity, such as anonymous authentication and anonymous signature.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,250,000	375,000	1,625,000
2011 年度	1,150,000	345,000	1,495,000
年度			
年度			
年度			
総　計	2,400,000	720,000	3,120,000

研究分野：工学
科研費の分科・細目：通信・ネットワーク工学
キーワード：ネットワーク、セキュア・ネットワーク、匿名性

１．研究開始当初の背景

近年，インターネット上で通信する際に，お互いのプライバシーをどのように保護するかが問題となっている．メッセージの内容を暗号化するセキュリティ技術では，通信内容の秘匿が可能であるが，IP アドレスやメールアドレスは秘匿されておらず，医療相談や電子投票，内部告発などの高い匿名性が必要となるサービスを提供する場合，既存のセ

キュリティ技術では対応が難しい．そこで本研究では，送受信者のプライバシーを保護可能な通信システムの開発，特に 1)匿名通信方式 3-Mode Net の解析・改良，2)匿名認証方式・匿名署名方式などの匿名通信方式以外の匿名方式の検討を目的とする．

２．研究の目的

研究段階において，3-Mode Net には，主に以下の問題点が知られていた．

(1) 中継ノード数，暗号化処理回数，送信者および受信者の匿名性の度合いが定量的に評価されていない．
(2) 実装されていない．

また，一般に公開鍵を用いた暗号化には時間がかかるため，計算量の観点から考慮すると，多重暗号化は行わない方が良いといえる．そのため，3-Mode Net を以下の通りの方式に変更する．

(3) 3-Mode Net を改良し，多重暗号化を用いない匿名通信方式へと変更する．

その他，3-Mode Net を含め匿名通信方式全般に関する問題点についても考察する．

(4) 3-Mode Net を用いた具体的なシナリオや他の匿名性を有する方式（匿名認証方式・匿名署名方式）との整合性を検討する．

以上の 4 点を研究の目的とする．

３．研究の方法

(1) 3-Mode Net は，初期暗号化多重度を k とすると，図 1 の通り，通信されるたびに，その多重度が増減され，最終的に多重度が 0 になると，受信者にメッセージが届けられるというモデルで表すことができる．つまり，3-Mode Net はランダムウォークのモデルで表すことができる．そのため，ランダムウォークの一般的な性質を調査した後，確率母関数を用いて理論値を導出した．

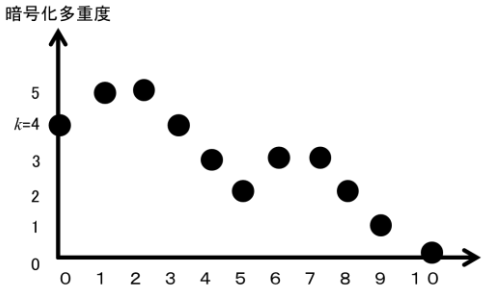

図 1：3-Mode Net のモデル化

匿名性の評価については，Crowd と呼ばれる匿名通信方式で使われている匿名性の指標を参考にし，ノードの結託（複数のノードが協力してメッセージの送受信者を特定する行為）に対する送信者の匿名性を解析した．さらに，メッセージの受信者の匿名性については，Crowd では受信者の匿名性がないという性質上，指標が定義されていなかったため，指標の定義から行った後，受信者の匿名性を解析した．

(2) 実装し，通信時間に関する実験を行った．実装に際しては，C#を用いた．実験には，8 台のパソコンを用いた．ネットワークについては，物理トポロジの関連からはハブを中心として全てのノードをスター型に接続し，論理トポロジの観点からはフルメッシュ型となるように構築した．

(3) 3-Mode Net では，多重暗号化を用いることにより，メッセージの宛先が変化する枠組みを用意していた．提案手法では，多重暗号化の代わりに，List（中継ノードがメッセージの宛先を記録したもの）とループバック（メッセージが自身に戻ってくること）の仕組みを導入し，多重暗号化を行う動作の代わりにループバックを行う動作（L モード）へ変更することにより，多重暗号化を用いない方式へと改良した（図２参照）．

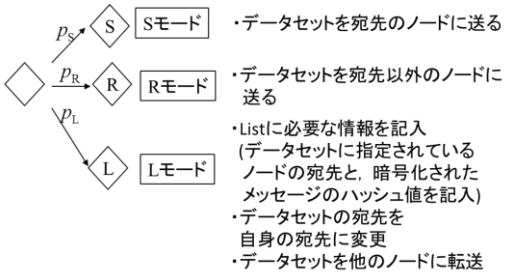

図２：多重暗号化を用いない改良手法

(4) 匿名認証方式・匿名署名方式に関する他の論文を調査した後，3-Mode Net との関連性を考察した．また，シナリオについては，ユーザがどのような利用体系を求めているかを考慮した後，そのシナリオに向けて 3-Mode Net はどのようにあるべきかを考察した．

４．研究成果

(1) 中継ノード数，暗号化処理回数については，確率分布，平均値，分散の理論値を導出した．なお，確率分布から平均値および分散を計算するために，確率母関数を用いた．また，送信者および受信者の匿名性についても，定義式から計算していく上で，確率母関数を用いることによ

り，送信者および受信者が特定される確率を導出した．その後，3-Mode Net における動作選択の確率を変化させた結果（図３および図４）および，得られた各理論値を解析した結果，以下のことが示された．

- 中継ノード数とノードの結託に対する送受信者の匿名性都の間には，トレードオフがある．
- 中継ノード数の期待値を一定にしたまま，分散を小さくした場合，暗号化処理回数の平均値は小さくなり，送信者の匿名性も保証されるが，受信者の匿名性は失われる．
- 多重暗号化の初期値は，中継ノード数・暗号化処理回数・送信者の匿名性には強い影響を与えるが，受信者の匿名性には影響は少ない．

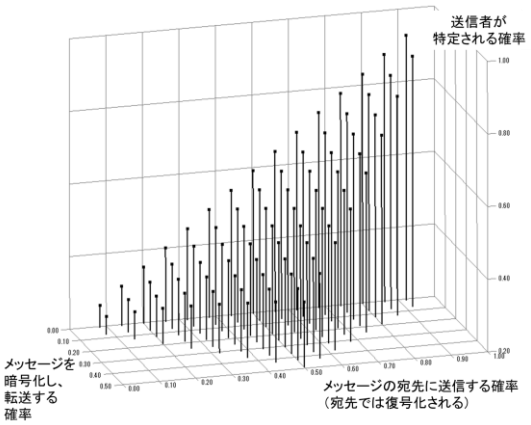

図３：送信者の匿名性

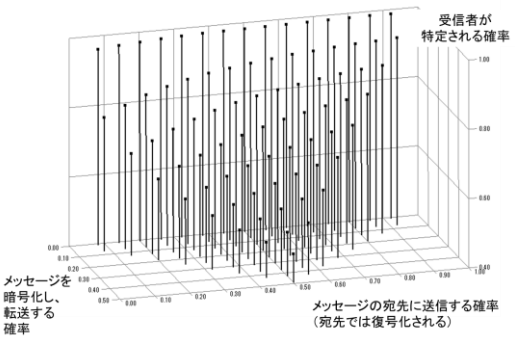

図４：受信者の匿名性

(2) 実験では，3-Mode Net の他に，それまでに提案されている 3 つの改良型 3-Mode Net の比較・検討を行った．その結果，通信時間および中継ノード数の観点から，最初は 3-Mode Net の動作を行い，途中で Onion Routing（匿名通信方式の一種）に動作を変更する方式（3MN with OR）が，通信時間が短く，かつ 3-Mode Net の大きな問題点の１つである中継ノード数に上限がないという問題点を解決しているため，最も有効な手法であることが分かった（図５参照）．

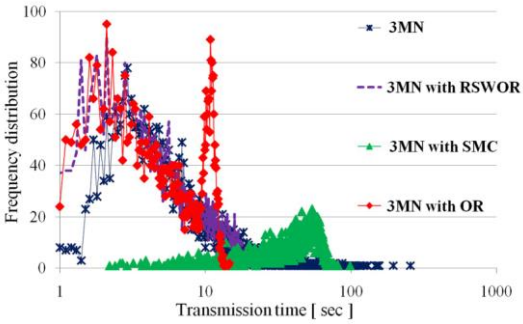

図５：通信時間の度数分布

(3) 3-Mode Net の枠組みを基本的に変えないまま，多重暗号化を用いない方式へと改良した．ここで，3-Mode Net とどのような違いがあるかを表１に示す．表１に示す通り，中継ノード数に関しては，3-Mode Net と同様の結果となるが，多重暗号化を一切用いていないため，暗号化処理の回数だけ，通信時間が早くなり，中継ノード数への負荷も低くなると想定される．

表１：3-Mode Net と提案手法との比較

	3-Mode Net	提案手法
送信者の匿名性	あり	あり
受信者の匿名性	あり	あり
中継ノード数	少ない	少ない
多重暗号化処理	必要	不必要
計算負荷	高い	低い
メッセージサイズ	変化する	変化しない
トラフィック量	多い	少ない
記憶媒体	不必要	必要

(4) シナリオについては，メールサービスや電子掲示板・SNS・チャット，オンラインショッピング・オークションの匿名化について考察した．特に，オンラインショッピングについては，商品の購入や受け取りが問題となるが，電子マネーの利用，コンビニエンスストアなどの購入者と関係がない場所での受け取りにより，可能となることを示した．
他の匿名性を有するシステムとの関連については，各方式が独立しているため，複数の匿名性を有するシステムを同時に使用した場合，どちらか一方が低い匿名性しか提供されなければ，意味をなさなくなるという問題点を指摘した．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 4 件）

1. 河野和宏, “東日本大震災から考える情報セキュリティ”, 社会安全学研究, No. 2, pp. 42-43, 2012. ＜査読無＞
2. K. Kono, S. Nakano, Y. Ito, and N. Babaguchi, “Anonymous Communication System Based on Multiple Loopbacks”, Journal of Information Assurance and Security, Vol. 6, No. 2, pp. 124-131, 2011. ＜査読有＞
3. 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. ＜査読有＞
4. K. Kono, S. Nakano, Y. Ito, and N. Babaguchi, “Theoretical Analysis of the Performance of Anonymous Communication System 3-Mode Net”, IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E93-A, No. 7, pp. 1338-1345, 2010. ＜査読有＞

〔学会発表〕（計 4 件）

1. 中村公美, 河野和宏, 伊藤義道, 馬場口登, “マルチタッチアクションを用いたタブレット型端末の所有者認証”, 電子情報通信学会 2012 年総合大会, D-210-6, p. 230, 2012 年 3 月 20 日, 岡山大学. ＜査読無＞
2. 中埜伸乃佑, 河野和宏, 伊藤義道, 馬場口登, “匿名通信方式 3-Mode Net における中継ノード数の低減手法”, 2011 年暗号と情報セキュリティシンポジウム（SCIS2011）, 8 ページ, 2011 年 1 月 26 日, リーガロイヤルホテル小倉（福岡）. ＜査読無＞
3. 河野和宏, 中埜伸乃佑, 伊藤義道, 馬場口登, “匿名通信方式 3-Mode Net におけるノードの結託に対する送受信者の匿名性の解析”, 2011 年暗号と情報セキュリティシンポジウム（SCIS2011）, 8 ページ, 2011 年 1 月 26 日, リーガロイヤルホテル小倉（福岡）. ＜査読無＞
4. K. Kono, Y. Ito, and N. Babaguchi, “Anonymous Communication System Using Probabilistic Choice of Actions and Multiple Loopbacks”, Proc. 6th International Conference on Information Assurance and Security, pp. 210-215, August 24, 2010, Atlanta, USA. ＜査読有＞

〔その他〕
ホームページ等
http://gakujo.kansai-u.ac.jp/profile/ja/948609f23C190ebfI.08927bG90.html

６．研究組織
(1)研究代表者

河野　和宏（KOUNO KAZUHIRO）
関西大学・社会安全学部・助教
研究者番号：60581238