様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　１日現在

機関番号：13903
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：20500064
研究課題名（和文）安全で実用的な匿名通信の実現

研究課題名（英文）Realization of Secure and Practical Anonymous Communication System

研究代表者
斎藤　彰一（SAITO SHOICHI）
名古屋工業大学・大学院工学研究科・准教授
研究者番号：70304186

研究成果の概要（和文）：
本研究では，多重暗号と多段中継を用いた低遅延型匿名通信システムにおける安全性の向上と実用性の向上を目指し，匿名通信システム Bifrost を開発した．Bifrost は，匿名性の向上と多重暗号処理のコストを軽減する方式を実現し，安全性と実用性を向上させることに成功した．さらに，研究期間後半には，ID ベース暗号を匿名通信システムに応用する方法を考案し，ディレクトリサーバを匿名通信システムから取り除くことに成功した．これにより，ディレクトリサーバによる匿名性の低下とスケーラビリティの低下を取り除き，実用性を向上させた．しかし，悪用時の匿名性解除方式を新たな提案するには至らず，既存の解除方式を適用するに止まった．

研究成果の概要（英文）：
In this research, we developed a novel anonymous communication system Bifrost to improve safety and practicality of low-latency anonymous communication systems with multiple-encryptions and multistage-relay. Bifrost can realize improving anonymity and reducing costs of multiple-encryptions and succeed in improving safety and practicality. Moreover, we proposed a new method applying ID-based encryption to anonymous communication systems and succeeded in removing directory servers from them. Therefore a decline in anonymity and scalability by directory servers is removed and practicality is improved. However we cannot present a novel method revoking anonymity of a sender when it abused anonymity. Our system just uses an existing revoking method.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,200,000	360,000	1,560,000
2009 年度	1,100,000	330,000	1,430,000
2010 年度	700,000	210,000	910,000
総　計	3,000,000	900,000	3,900,000

研究分野：システムソフトウェア
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワークセキュリティ技術，匿名通信，オーバレイネットワーク

１．研究開始当初の背景

匿名通信の研究はすでに行われている．しかし，理論的積み上げの研究も多く，実用に耐えうる方式はまだない．本研究では，安全性と実用性の高い匿名通信方式の実装を行う．

また，匿名通信は公的機関や人権擁護団体に対する訴えを，告発者の身元と訴え先を第三者から隠したまま可能にする．内部告発者の保護を目的とした公益通報者保護法が

2006 年 4 月より施行されており，匿名通信は今後社会的なニーズが大きく増加するシステムである．

２．研究の目的

本研究では，P2P ネットワークによる安全性と実用性を有する匿名通信路を実現する．安全性とは，参加ノードの結託による攻撃に耐えうる匿名性，名前検索時における匿名性，匿名の悪用に対する悪用者の特定機能をそれぞれ有すること．実用性とは，十分なスケーラビリティ，動的なネットワーク構造の変化に耐えうるノード管理手法，問題のない通信速度を有することである．

３．研究の方法

匿名通信路の基盤となる DHT には現在主流である Chord を用いる．研究初期には，匿名通信路のための詳細な検討期間を設ける．

本研究の開発には，OverlayWeaver を用いる．OverlayWeaver は，分散ハッシュテーブルを用いたオーバレイネットワーク環境を構築できるツールキットである．これにより，複雑な分散ハッシュテーブルを新たに構築することなしに，主目的である匿名通信システムの開発に着手することが可能となる．

評価には，所属機関の教育用計算機システムと，導入した計算機クラスタによるローカルネットワーク環境による実機評価を行う．さらに，インターネットにおける広域分散実験環境である PlanetLab を利用した実機評価を行う．これらにより，実用性のある匿名通信路の実現を目指す．ローカルネットワーク環境では，基本的な動作確認を行うとともに，通信遅延時間や計算機性能が均一であることを利用した，基本性能評価を実施する．PlanetLab では，全世界のノードで匿名通信網を構築し，インターネット環境における通信時間などの性能評価を行う．

４．研究成果

本研究の成果として，以下を上げる．

(1) ID ベース暗号を用いた匿名通信方式の実現と，これによるスケーラビリティと安全性を向上した．
(2) 匿名性向上ための中継ノード数の増加に伴う暗号化コストの増加を，分散ハッシュテーブルを用いた経路制御により軽減した．

本研究における最大の成果は，(1)にある ID ベース暗号を匿名通信システムに利用する方式を提案し，それにより安全性と実用性（スケーラビリティ）の向上を実現したことである．ID ベース暗号とは，任意の ID（文字列）を基に公開鍵と秘密鍵が生成可能な公開鍵暗号システムである．ID ベース暗号は，通常，システム内の ID 管理が信用できる場合に用いられてきており，匿名通信システムのような参加者の ID が不明確なシステムへの適用は行われてこなかった．本研究では，参加者の ID を厳密に管理することで，参加各ノードによる参加済みノードの ID が推測できると考えた．これを応用することで，従来の匿名通信システムでは不可欠だがスケーラビリティの低下を招く原因とされたディレクトリサーバを，匿名通信システムから取り除くことが可能であると考え，この考えに基づく匿名通信システムを開発した．

ディレクトリサーバを使用しない匿名通信システムは，現在の匿名通信システム研究において重要なテーマの一つである．従来の匿名通信システムでは，参加済みノード一覧を取得するためと，暗号化を行うための公開鍵を取得するためにディレクトリサーバが必要である．参加ノードは，匿名通信路を構築するために，ディレクトリサーバからノード一覧や個々の公開鍵を入手する必要がある．ノード一覧は，ノードの参加や離脱が発生する度に，参加全ノードのノード一覧を更新する必要がある．この入手や配布は大きな負担となり，スケーラビリティを低下させ実用的なシステム構築を阻害する．また，参加ノードの情報を入手するためや他ノードの公開鍵を入手するためにディレクトリサーバを検索した場合，検索ノードがどのようなノードを匿名通信路に使用しようとしているかが，ディレクトリサーバに漏洩することになる．ディレクトリサーバを信頼することができたとしても，コンピュータウィルスや管理者の操作ミスによる情報漏洩の危険性はなくならない．そこで，匿名通信システムの研究においては，ディレクトリサーバを設置しない方法の研究が盛んに行われている．

本研究では，ID ベース暗号を用いることで，まったく新しい方法によるディレクトリサーバを用いない匿名通信システムを実現した．ID ベース暗号を使用するためには，使用中の ID が明確になればよい．しかし，そのためにディレクトリサーバを使用すると匿名性が低下する．そこで，ノードを配置するすべての ID を事前に決定し，その ID 群にランダム順で参加ノードを割り当てる方式を考案した．この方法とは，隣接する ID の間隔を等間隔になるように割り当てることである．つまり，任意の部分 ID 空間において割り当て済み ID の密度が均一になるように割り当てを行う（図 1 参照）．これにより，各ノードは隣接ノードの ID を調べて近隣の ID 密度を求めるだけで，システム全体における ID 密度，つまり割り当て状況を知ることができる．これにより，ディレクトリサーバ

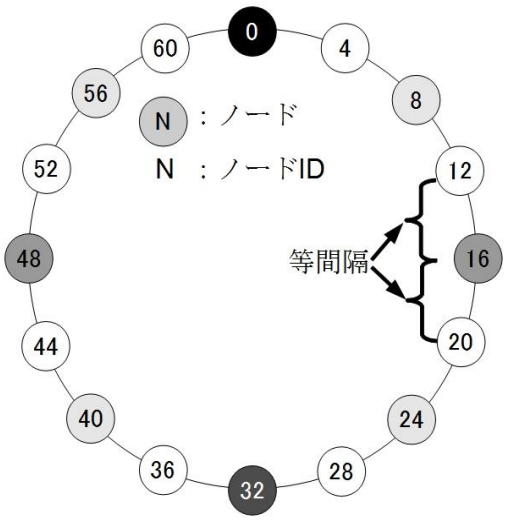

図 1 ノード ID の割り当て方式

を用いることなしに，おおよそのシステム全体の ID 使用状況を知ることができる．もちろん，1 つの間違いもない使用状況を知ることはできない．しかし，匿名通信路構築に必要なノード数には十分な ID 数を知ることができる．さらに，ID ベース暗号の ID から公開鍵を求めることができるという性質から，新たな負荷なしに公開鍵を求めることができる．このようにして求めたノード ID と公開鍵により，匿名通信路構築が可能となる．本方式の成果は，雑誌論文①と学会発表①で発表を行った．特に学会発表①では，学生論文賞を受賞した．

研究成果(2)は，匿名通信における最大の負荷である暗号化コストを軽減させ，実用性を向上させた．多くの匿名通信システムでは，多数のノードを経由して受信ノードと通信する「多段中継」が使用される．多段中継により，受信ノードは，送信ノードを特定する情報（IP アドレスとポート番号）を得ることができなくなる．しかし，中継する各ノードに，送信ノードと受信ノードと通信内容が漏れることを防がなければならない．そのために，各中継ノードは，中継するすべてのメッセージをあらかじめ送信ノードに指定された鍵を用いて復号する．この時，復号することによって次に中継するノードを得ることができる．これにより，各中継ノードは，自身の前後 2 ノード以外を知ることなしに，メッセージを中継することが可能となる．これを多重暗号方式という．

多重暗号方式では，各中継ノードがメッセージを復号・暗号化するため，中継コストが大きい．そのため，多数の中継ノードを経由するような匿名通信路を構築すると，経路途中での暗号化処理のために，大きな通信遅延が発生し実用性を低下させる．そこで，本研究成果では，暗号処理を増やすことなく中継ノードを増加させる方式を実現した．

提案方式では，一部の中継ノードのみが復号できる匿名通信路構築メッセージを用いる．復号ができた中継ノードは，通常の多重暗号方式と同様に，指定された次の中継ノードにメッセージを中継する．ここで，復号できないノードは，復号することなしに分散ハッシュテーブルの successor node に中継する．つまり，復号できない中継ノードが続く間は分散ハッシュテーブル上で連続する中継ノード群を通過し，復号できた中継ノードが離れた中継ノード群に送信する方式である．この「復号できない連続する中継ノード群」を「受信エリア」という．以上より，匿名通信路の一部のみが暗号化処理を行うだけとなり，匿名通信路全体における暗号化処理の負荷が軽減される．言い換えれば，少ない暗号化処理により，多数の中継ノードを利用できる．結果，実用性の向上と匿名性の向上の双方が実現できる．さらに，この方式では，中継に参加するノードを送信ノードが送信前に計画することが可能となることを利用して，計画された匿名通信路の途中に受信ノードを配置することが可能である．これにより，匿名通信に対するタイミング解析攻撃に対する耐性を向上させ，安全性・匿名性を向上させる．

次に，匿名性の悪用防止について述べる．悪用防止のために悪用者の特定機能は，匿名通信が正常に利用されるために必要な機構であると考える．本研究においても，研究目的にあげており，課題の一つである．そこで，既存研究である千田らの研究[1]について調査を行った．この研究では，匿名路を構築する各参加ノードが，直前のノードの IP アドレスを暗号化してメッセージに含めることで，受信者に中継ノードを伝達する．ただし，受信者はこの暗号を復号することはできない．匿名で行われた通信に問題がある場合は，匿名通信システムを監視する第三者機関にその旨とメッセージを提出する．第三者機関では，匿名性解除の妥当性を検証する．妥当であると判断した場合は，提出を受けたメッセージを復号し，中継したノードの IP アドレスを特定するという手順である．この研究は，各ノードが，通信に必ず必要で，かつ偽装が困難な IP アドレスを通信相手が記録することで，通信した事実を確認することが可能である．この方式を，我々の実現匿名通信システムに適用した．

さらに，この方式の課題である暗号化の負荷を軽減する試みを行った．我々の提案方式では，受信エリアでは分散ハッシュテーブルにおける静的な通信路を通過することを利用して，受信エリア内では IP アドレスの記録を行わない方式を実現した．これにより，IP アドレス記録のための暗号化処理コスト

が軽減した．しかし，受信エリア中の通信記録は，分散ハッシュテーブルへの参加記録のみとなるため，送信者特定の厳密性は低下している．実用的かつ厳密な悪用者の特定機能の実現は，今後の課題である．

[1] 千田浩司,小宮輝之,林徹,匿名性確保と不正者追跡の両立が可能な通信方式,情報処理学会論文誌,Vol.45,No.8,pp.1873-1880 (2004).

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 2 件）

① Hiroyuki Tanaka, Shoichi Saito, and Hiroshi Matsuo, Removing Directory Servers from Anonymous Communication Systems using ID-Based Encryption to Improve Scalability, Proceedings of the World Congress on Internet Security 2011 (WorldCIS-2011), 査読有, 2011, 93-98.
② Masaki Kondo, Shoichi Saito, Kiyohisa Ishiguro, Hiroyuki Tanaka, and Hiroshi Matsuo, Bifrost: A Novel Anonymous Communication System with DHT, Proceedings of Parallel and Distributed Computing, Applications and Technologies, 査読有, 2009, 324-329.

〔学会発表〕（計 5 件）

① 田中寛之，齋藤彰一，松尾啓志，ID ベース暗号の匿名通信への応用，情報処理学会 コンピュータセキュリティシンポジウム 2010，2010 年 10 月 20 日，岡山市.
② 田中寛之，石黒聖久，近藤正基，齋藤彰一，松尾啓志，通信用公開鍵配布機能と並列送信機能を有する匿名通信方式の提案と評価，情報処理学会 コンピュータセキュリティシンポジウム 2009，2009 年 10 月 28 日，富山市.
③ 石黒聖久，田中寛之，近藤正基，齋藤彰一，松尾啓志，匿名通信路のノード離脱に対する通信路継続方式，情報処理学会 コンピュータセキュリティシンポジウム 2009，2009 年 10 月 28 日，富山市.
④ 近藤正基，田中寛之，齋藤彰一，松尾啓志，分散ハッシュテーブルによるノード管理を行う匿名通信方式の設計と実装，情報処理学会 システムソフトウェアとオペレーティングシステム研究会，2009 年 4 月 23 日，那覇市.
⑤ 近藤正基，齋藤彰一，松尾啓志，DHT を用いた双方向匿名通進路の提案，情報処理学会 コンピュータセキュリティ研究会，2008 年 7 月 25 日，福岡市.

〔図書〕（計 0 件）
〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕
・学会発表論文①は，当該シンポジウムにおいて学生論文賞を受賞した.

６．研究組織
(1)研究代表者
斎藤　彰一（SAITO SHOICHI）
名古屋工業大学・大学院工学研究科・准教授
研究者番号：70304186

(2)研究分担者
松尾　啓志（MATSUO HIROSHI）
名古屋工業大学・大学院工学研究科・教授
研究者番号：00219396