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１５日現在

機関番号：31302
研究種目：若手研究（B）
研究期間：2008～2010
課題番号：20700069
研究課題名（和文）　利便性・匿名性に優れたセキュアでスケーラブルな P2P ネットワーク

研究課題名（英文）　Secure and Scalable P2P Network with Usability and Anonymity

研究代表者
武田　敦志（TAKEDA ATSUSHI）
東北学院大学・教養学部・講師
研究者番号：90424001

研究成果の概要（和文）：
安全な P2P ネットワークを構築するための分散型認証手法 HDAM の安全性・信頼性に関する理論研究とシミュレーションによる評価を行い，従来手法に比べて半分以下のメモリ量・通信データ量で安全で利便性の高い P2P ネットワークを構築できることを確認した．また，HDAM の技術を効果的に利用した分散型公開鍵認証基盤 HDPKI を構築し，利便性・スケーラビリティに優れた公開鍵の分散管理が可能であることを示した．

研究成果の概要（英文）：
I studied a theory of a distributed authentication method named HDAM which is used for building a safe P2P network, and I evaluated HDAM through simulations. The results showed that required memory size and communication overhead of a P2P network with HDAM is much less than required memory size and communication overhead of conventional methods. Moreover, I built a distributed public key infrastructure named HDPKI which is based on an algorithm of HDAM. This study showed that HDPKI provides distributed managing service of public keys which is scalable and easy to use.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,100,000	330,000	1,430,000
2009 年度	700,000	210,000	910,000
2010 年度	600,000	180,000	780,000
年度			
年度			
総　計	2,400,000	720,000	3,120,000

研究分野：　総合領域
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：　オーバーレイネットワーク，P2P ネットワーク

１．研究開始当初の背景

最も普及している認証手法として，認証局と呼ばれるサーバを介してノードの認証を行う PKI が存在する．しかし，PKI で認証を行うためには利用者の情報を登録したサーバを用意する必要があるため，PKI を P2P ネットワークに適用すると P2P ネットワークの特徴である利便性・匿名性が失われる可能性がある．一方，サーバを必要としない認証手法として PGP や Self-Organized Public-Key

Management などが提案されている．しかし，これらの手法は認証に必要な情報を無計画に収集し，それぞれのノードに多くのメモリ量と通信データ量を必要とするため，スケーラビリティに問題がある．このように，利便性・匿名性・スケーラビリティに優れた既存の認証手法は存在しない．

２．研究の目的

P2P ネットワークは利便性・匿名性などに優れたコンピュータネットワークであるが，その一方で信頼性に乏しいという問題がある．そこで本研究では，サーバを必要としない分散認証手法 HDAM の研究・開発を行うことにより，利便性・匿名性・スケーラビリティに優れたセキュアな P2P ネットワークの実現を目指す．また，HDAM を導入した P2P ネットワークのアプリケーションの開発を通じて，スケーラビリティ・利便性・匿名性に優れた安全な P2P ネットワークを活用した新しい高度な情報通信サービスを模索する．

平成 19 年度までに信頼の輪と分散ハッシュテーブルを用いた新しい分散認証手法 Hash-based Distributed Authentication Method (HDAM) の基礎的研究を行った．HDAM では信頼の輪を用いてサーバを必要としない分散認証を行うことにより，利便性・匿名性に優れた認証システムを提供する．さらに，分散ハッシュテーブルを用いて効果的に認証情報を分散させることにより，スケーラビリティに優れた効率的な認証システムの運用を実現する．本研究ではこれらの成果を引き継ぎ，HDAM を用いたセキュアで利便性・匿名性に優れたセキュアでスケーラブルな P2P ネットワークの実現を目指す．

３．研究の方法

平成 19 年度までに，HDAM の基本コンセプトを提案し，そのスケーラビリティを検証した．平成 20 年度以降は HDAM の安全性・信頼性を理論的に証明し，HDAM を P2P ネットワークに適用することにより，実ネットワーク上に利便性・匿名性に優れたセキュアでスケーラブルな P2P ネットワークを実現することを目指す．また，大規模な仮想ネットワークや大規模な実ネットワークを用いた評価を行う．具体的には，HDAM の安全性・信頼性に関する理論と実環境への適用方法を確立するため，以下の計画に従って研究を進める．

(1) 安全性・信頼性に関する理論とシミュレーションによる評価（平成 20 年度）
  ① HDAM の安全性・信頼性に関する理論の構築
  ② 数万ノードからなる仮想ネットワークでのシミュレーションを通じた評価

(2) 認証プラットフォームとアプリケーションの開発（平成 21 年度）
  ① HDAM を運用するための認証プラットフォームの設計と開発
  ② HDAM を利用したアプリケーションの開発と運用

(3) 実ネットワークを用いた実験と総合評価（平成 22 年度）
  ① 数百ノードからなる実ネットワークでの実験を通じた評価
  ② 総合評価

４．研究成果

上記計画に基づいた研究を進め，以下の成果を得た．平成 20 年度から 22 年度までに，これらの研究成果に関する 2 個の学術論文と 3 個の国際会議論文を発表し，5 個の国内学会で発表を行い，1 個の論文賞を受賞した．

(1) 安全性・信頼性に関する理論とシミュレーションによる評価（平成 20 年度）

平成 20 年度には，新たな分散型認証手法 HDAM の安全性・信頼性に関する理論研究とシミュレーションによる評価を行った．HDAM は分散ハッシュテーブルを用いて公開鍵を分散管理するため，従来手法に比べて利便性・匿名性・スケーラビリティに優れた認証手法である．HDAM の安全性・信頼性に関する理論研究では，HDAM で用いる分散ハッシュテーブルに冗長性を持たせるためのアルゴリズムを設計し，このアルゴリズムにより安全性の向上が可能であることを示した．また，HDAM のシミュレーションにおいては，HDAM のスケーラビリティが既存手法に比べて大幅に優れていることを検証し，安全性向上のための冗長性を導入したとしても従来手法より十分に少ないメモリ量・通信データ量で安全なネットワークを構築できることを確認した．以上より，新しい分散型認証手法 HDAM の安全性・信頼性・スケーラビリティを明らかにし，HDAM の理論的基礎を確立した．

(2) 認証プラットフォームとアプリケーションの開発（平成 21 年度）

平成 21 年度には，ユビキタス環境における認証プラットフォームである分散型公開鍵認証基盤 HDPKI (Hash-based Distributed Public Key Infrastructure) の設計と，HDPKI の性能評価を行った．HDPKI は，HDAM の技術を効果的に利用することにより，匿名性・利便性・スケーラビリティに優れた公開鍵の分散管理を実現する．また，HDPKI では，マルチパスメカニズムを導入することにより，公開鍵管理の信頼性の向上を実現した．さらに，

シミュレータを用いた性能評価により，HDPKI が従来手法よりスケーラビリティに優れた手法であることを確認した，マルチパスメカニズムを導入したことにより信頼性の向上を実現していることを確認した．以上より，永続的なサーバを必要としない認証プラットフォームである HDPKI の設計と開発に成功した．

(3) 実ネットワークを用いた実験と総合評価（平成 22 年度）

平成 22 年度には，平成 21 年度までの成果に基づき，HDPKI の性能及び安全性の評価を行った．特に，複数経路を介した安全な認証方法の再設計・再評価を行い，悪意のある利用者が含まれる環境においても高い認証成功率を維持できることを検証した．また，平成 22 年度までの研究開発を通じて，安全な P2P ネットワークを利用した新たなユビキタスサービス「Socio-familiar Personalized サービス」の着想を得た．この新たなユビキタスサービスについては，平成 23 年度以降に学術論文等を通じて発表する予定である．また，HDPKI の開発を通じて，既存の構造型 P2P ネットワークの問題点を発見し，その問題の解決法を発見した．この知見を反映させた新たな構造型 P2P ネットワーク「Waon」の設計を行い，その基礎理論をまとめた論文により第 18 回マルチメディア通信と分散処理ワークショップ優秀論文賞を受賞した．

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 5 件）

(1) Atushi Takeda, Takuma Oide and Akiko Takahashi, "New Structured P2P Network with Dynamic Load Balancing Scheme", Proceeding of the 25th International Conference on Advanced Information Networking and Applications - Workshops (AINAW2011), 査読有, 2011 年, pp. 108-113

(2) Atushi Takeda, Seiya Nakayama, Gen Kitagata, Debasish Chakraborty, Kazuo Hashimoto, and Norio Shiratori, "Hash-based Distributed Public Key Infrastructure for Ubiquitous Environments", Proceedings of the 4th International Conference on Complex, Intelligent Computing and Information Systems (CISIS2010), 査読有, 2010 年, pp. 337-344.

(3) Atushi Takeda, Debasish Chakraborty, Gen Kitagata, Kazuo Hashimoto and Norio Shiratori, "Proposal and Performance Evaluation of Hash-based Authentication for P2P Network", IPSJ Journal, 査読有, vol. 50, no. 2, 2009 年, pp. 737-749.

(4) Atushi Takeda, Debasish Chakraborty, Gen Kitagata, Kazuo Hashimoto and Norio Shiratori, "A New Scalable Distributed Authentication for P2P Network and its Performance Evaluation", WSEAS Transactions on COMPUTERS, 査読有, vol. 7, 2008 年, pp. 1628-1637.

(5) Atushi Takeda, Debasish Chakraborty, Gen Kitagata, Kazuo Hashimoto and Norio Shiratori, "A New Scalable Distributed Authentication for P2P Network and its Performance Evaluation", Proceedings of the 12th WSEAS International Conference on Computers, 査読有, 2008 年, pp. 536-541.

〔学会発表〕（計 5 件）

(1) 武田 敦志, 生出 拓馬, 高橋 晶子, "構造型 P2P ネットワークにおける動的負荷分散法", 第 18 回マルチメディア通信と分散処理ワークショップ（優秀論文賞を受賞）, 2010 年 10 月 28 日, 宮崎県 青島サンクマール

(2) 武田 敦志, 中山 誠也, デバシシュチャクラボルティ, 北形 元, 橋本 和夫, 白鳥 則郎, "オーバーレイネットワークのセキュリティに関する研究開発", 第 8 回情報科学技術フォーラム (FIT2009) (デモ展示), 2009 年 9 月 2 日～4 日, 東北工業大学.

(3) 武田 敦志, 中山 誠也, デバシシュチャクラボルティ, 北形 元, 橋本 和夫, 白鳥 則郎, "ユビキタスコンピューティング環境のための分散型公開鍵認証基盤の設計", マルチメディア, 分散, 協調とモバイルシンポジウム (DICOMO 2009), 2009 年 7 月 9 日, 大分県 別府温泉 杉乃井ホテル.

(4) 武田 敦志, チャクラボルティ デバシシュ, 北形 元, 橋本 和夫, 白鳥 則郎, "分散ハッシュテーブルを用いた公開鍵管理手法の設計と評価", 第 16 回マルチメディア通信と分散処理ワークショップ, 2008 年 12 月 10 日, 山口県萩市 萩本陣.

(5) 武田 敦志, チャクラボルティ デバシシュ, 北形 元, 白鳥 則郎, "P2P ネットワークのための分散型認証システムの設計", 第 135 回 DPS 研究会, 2008 年 6 月 19 日, 会津大学.

〔その他〕
(1) 優秀論文賞受賞，第18回 マルチメディア通信と分散処理ワークショップ(DPSWS2010)，2010年10月28日，宮崎県 青島サンクマール

(2) 東北学院大学内に設置されているWebサーバ(下記URL)において研究成果を公開予定
http://takeda.cs.tohoku-gakuin.ac.jp/

6．研究組織
(1)研究代表者
武田　敦志　(TAKEDA ATSUSHI)
東北学院大学，教養学部，講師
研究者番号：90424001

(2)研究分担者
なし

(3)連携研究者
なし