様式 C-7-2

自己評価報告書

平成２３年４月２８日現在

機関番号：14301
研究種目：基盤研究(B)
研究期間：2008～2012
課題番号：20300028
研究課題名（和文）　HIP に基づく開放型ユビキタスネットワークアーキテクチャ

研究課題名（英文）　Open Ubiquitous Network Architecture based on Host Identity Protocol

研究代表者
岡部寿男（OKABE YASUO）
京都大学・学術情報メディアセンター・教授
研究者番号：20204018

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：モバイルネットワーク技術、Host Identity Protocol、ユビキタスネットワーク、セキュリティ、プライバシ保護、位置情報、Security Assertion Markup Language

１．研究計画の概要

ユビキタス時代においては，あらゆるモノにネットワーク機能が具備され、だれもがいたるところで自在にネットワークが使えることが期待される。そのようなネットワークが社会の隅々まで通信事業者(Internet Service Provider; ISP) によって整備されることは困難であることを踏まえ、今日一般家庭でも当たり前になりつつあるブロードバンドネットワーク環境を、無線 LAN などのネットワークを介して、ネットワークの元々の設置者とは別の不特定の利用者が、本来の設置目的とは別の目的にも活用できるようにするのが、開放型ユビキタスネットワークアーキテクチャの考え方である。本研究課題では、このようなネットワークにおけるセキュリティとプライバシ、特に「いつ・だれが・どこに」居たかの位置情報に関するプライバシ（ロケーションプライバシ）の課題を、IP アドレスに代わる新しいアドレス体系として注目され IETF で標準化が進められている HIP (Host Identity Proctocol) を用いて解決する。

２．研究の進捗状況

本研究において解決すべき具体的課題は以下の通りである。

(1) HIP を単純に適用することでは、利用者や通信相手が誰であるかという情報がネットワークアクセスの提供者から秘匿できず、誰がいつどこでネットワークを使ったかというロケーションプライバシの保護が脆弱であること。
(2) ネットワークの元々の設置者が不特定の利用者にネットワークアクセスを提供するにあたって認証に負担がかからないようにしなければならないこと。またネットワークアクセス提供者が悪意を持っていても盗聴や改竄が不可能なように十分な強度で暗号化されていること
(3) 利用者が誰であるのかはネットワークアクセスの提供者は知りえない一方で、不正アクセス等や著作権侵害などのインシデントが発生した場合には、利用者を（第三者に立証できる形で）特定できなければならないこと

このうち(1)に関しては、BLIND と呼ばれる手法を HIP に適用することで解決できた。オリジナルの BLIND はモビリティには非対応であったのを、HIP におけるモビリティサポートと組み合わせて用いることができるように改良した。この成果は IEEE/IPSJ SAINT2009 国際会議において発表した。また電子情報通信学会インターネットアーキテクチャ研究会より 2008 年度 IA 研究賞を受賞している。

(2)に関しては、古典的な radius 連携を用いた方式や VPN を用いた方式についてまず検討を進め、残された課題を HIP を用いることで解決するアプローチを取っている。特に VPN により認証と暗号化を行うみあこネット方式は HI で認証を行い IPsec で暗号化を行う HIP と共通点が多いことから基本アーキテクチャとして考えている。成果としてはみあこネット方式に関する論文が電子情報通信学会論文誌に掲載された他、eduroam アカウント連携などについて学会で発表している。

(3)に関しては、Web サービスにおける Identity Provider (IdP) と Service Provider(SP) のモデルを適用し、ネットワー

クアクセスの提供者、ネットワークアクセスの利用者、および通信相手に対し、一定レベルの匿名性を保ちつつIdPがある種の身元保証を行うモデルを提案している。インシデント対応のためにネットワークアクセスの提供者がどのようなログを保存しておく必要があるかについて検討を進めている。

３．現在までの達成度

②おおむね順調に進展している。

上記項目で示したように、ロケーションプライバシの保護については提案している方式が学会で評価を得るなど、順調であると言える。

４．今後の研究の推進方策

本研究課題は、平成 24 年度が最終年度となる。平成 23 年度中にアーキテクチャを確立するとともに必要な要素技術を完成させ、平成 24 年度には実証実験や標準化活動が行えるようにしたい。

５． 代表的な研究成果

（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 3 件）

1. 大平健司、住岡敦史、北岡有喜、古村隆明、藤川賢治、岡部寿男,“公衆無線インターネットサービス「みあこネット」の設計と運用”, 電子情報通信学会論文誌， vol.J93-B,no.5， 2010，pp.759-768
2. 古村隆明・岡部寿男・中村素典, “SAML 連携を用いてロケーションプライバシを守る eduroam アカウント利用方式”, 信学技報, vol. 109, no. 438, IA2009-109, pp. 153-158, 2010 年 3 月.
3. 前川慶司, 岡部寿男,Host Identity Protocol を用いたロケーションプライバシを有する匿名移動通信,信学技報, vol. 108, no. 275, IA2008-43, pp. 13-17, 2008 年 11 月.（2009 年 5 月に電子情報通信学会 2008 年度 IA 研究賞を受賞）

〔学会発表〕（計 5 件）

1. Keiji Maekawa, Yasuo Okabe, “An Enhanced Location Privacy Framework with Mobility Using Host Identity Protocol”, The 2009 International Symposium on Applications and the Internet (SAINT2009), pp. 23-29, Seattle, USA, 20 - 24 July 2009.
2. Toshiyuki Kataoka, Takeshi Nishimura, Masaki Shimaoka, Kazutsuna Yamaji, Motonori Nakamura, Noboru Sonehara, Yasuo Okabe, “Leveraging PKI in SAML2.0 Federation for Enhanced Discovery Service”, The Third Workshop on Middleware Architecture in the Internet (MidArc2009) (held as a part of SAINT2009), Seattle, USA, 20 - 24 July 2009.
3. Kenji Ohira, Yasuo Okabe, “Host-Centric Site-Exit Router Selection in IPv6 Site Multihoming Environment”, 1st International Workshop on Protocols and Applications with Multi-Homing Support (PAMS 2011), Singapore, pp. 696-703, March 22-25, 2011.
4. 岡部寿男・古村隆明, “商用公衆無線インターネットサービスのキャンパスネットワークへの展開”, 日本学術振興会産学協力研究委員会インターネット技術第 163 委員会(ITRC) 第 28 回研究会, 2010 年 11 月.
5. Yasuo Okabe, “Cross-layer Support for Multihoming toward Truly Resilient Future Internet”, 2010 Northeastern Asian Symposium on ICT: Next Generation Network and Network Security (Xi'an,China), Sept. 2010.

〔図書〕（計 0 件）

〔その他〕

ホームページ

http://www.net.ist.i.kyoto-u.ac.jp/ja/index.php?%CF%C0%CA%B8