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　4 月　26 日現在

機関番号：34315
研究種目：若手研究（Ｂ）
研究期間：2009～2011
課題番号：21700089
研究課題名：（和文）信頼度に基づく端末認証技術を利用した安全なモバイルアドホックネットワーク構成法
研究課題名：(英文)　Secure Ad-hoc Network Construction Method Exploiting Trust-based Node Authentication
研究代表者
野口　拓（NOGUTI　TAKU）
立命館大学・情報理工学部・助教
研究番号：00388133

研究成果の概要（和文）：
アドホックネットワークに端末信頼度に基づく端末認証機能を追加し，高信頼・高安全なアドホックネットワークを構築するセキュリティ技術の開発を行った．具体的には，まずネットワーク監視に基づく端末信頼度評価技術および端末認証技術を開発し，続いて，ネットワークコーディングおよび端末位置情報を用いた端末情報収集プロセスの最適化を行った．さらに，ユニキャスト複数配信とマルチキャスト配信を併用した制御情報配信の最適化も行った．提案手法の性能評価を行い，安全なアドホックネットワークを構成できることを明らかにした．

研究成果の概要（英文）：
A constructing method of secure and reliable ad hoc networks was developed by exploiting trust-based node authentication. Our main contributions are as follows: first, we developed the node evaluation and the node authentication mechanisms based on network monitoring. Second, we optimized node information gathering process by exploiting network coding and node location information. Third, we optimized delivery of control information for virtual certificate authority services by using both multiple unicast transmissions and multicast transmission. Our simulation results show that the proposed method can construct secure and reliable ad hoc networks.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	**1,200,000**	**360,000**	**1,560,000**
2010 年度	**900,000**	**270,000**	**1,170,000**
2011 年度	**1,100,000**	**330,000**	**1,430,000**
年度			
年度			
総　計	**3,200,000**	**960,000**	**4,160,000**

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：アドホックネットワーク，マルチキャスト，セキュア/ネットワーク，高信頼性ネットワーク

１．研究開始当初の背景

固定の基地局やアクセスポイントなどのインフラを必要とせず，各端末が相互に無線接続されることでネットワークを形成するアドホックネットワークは，場所の制約を受けずに柔軟にネットワークを形成できる．インフラレスで容易に敷設可能であるという特長を活かし，大災害発生時の安否情報や被災状況の通知，イベント会場での情報配信などがその具体的アプリケーションとして検討されている．近年，アドホックネットワークに対する潜在的な需要を受け，実用化に向けた研究開発が各国で精力的に進められており，MAC プロトコル，経路制御プロトコルおよびトランスポートプロトコルについての多くの提案・評価報告がなされている．従来研究の大部分はアドホックネットワークが誠実な端末によって構成され，ネットワークに対する不正な攻撃が存在しないことを暗に仮定しているため，これらの研究成果を導入する際には，安全なアドホックネットワークが構築されていることが必須の条件となる．しかしながら，送受信者以外の第三者がデータ中継に介在し，誰もが傍受可能な無線通信によってデータが伝送されるアドホックネットワークは，本質的に安全性の低い脆弱なシステムであり，なりすましやデータの改竄・盗聴，中継データの故意による廃棄などの不正行為が容易である．不正行為の存在するアドホックネットワークにおいては，安全面を考慮していない従来方式の大部分は正しく機能しないと考えられる．アドホックネットワークにおける不正攻撃の大部分は，端末認証技術の導入によって防ぐことが可能であるが，インターネットに接続されていないスタンドアロン型アドホックネットワークにおいては，既存のセキュリティインフラ（PKI, Housley et al., 1999, RFC2459）を利用できないため，従来の公開鍵暗号や電子署名を用いた端末認証を行う事が困難である．

２．研究の目的

本研究の目的は，インターネットへの接続点を持たないスタンドアロン型アドホックネットワークにおいて，正規の受信者以外の端末によるなりすまし，データの盗聴，改竄および故意廃棄を防ぐ安全なアドホックネットワークを構築することである．そこで本研究では，スタンドアロン型アドホックネットワークにおいて端末認証を行うための公開鍵認証技術および端末信頼度評価技術について重点的に検討を行った．具体的には，以下の３つの研究課題に対して研究を遂行した．

(1) ネットワーク監視に基づく端末信頼度評価技術および端末認証技術の開発
(2) ネットワークコーディングおよび端末位置情報を用いた端末情報収集プロセス最適化手法の開発
(3) ユニキャスト複数配信とマルチキャスト配信を併用した制御情報配信の最適化手法の開発

３．研究の方法

(1) アドホックネットワークでは，無線通信が用いられるため，その同報性を利用すれば，自身の周囲に存在する端末の通信状況を把握することは比較的容易である．本研究では，この無線通信の同報性を利用して傍受した隣接端末の送受信情報を元に，隣接端末の信頼度を評価する方式を提案した．提案方式では，アドホックネットワーク構成端末の責務であるデータ中継処理を隣接端末が適切に行っているかどうかを監視し，さらに周囲の端末が送受信している公開鍵証明書情報を収集し，これらの情報を元に端末信頼度を定量評価する．提案方式は，個々の端末が周囲に存在する他端末を監視・評価する分散制御のアプローチであり，ネットワーク形状が変化しやすいアドホックネットワークに適した方式である． さらに，本方式で取得した端末信頼度情報に基づいて仮想認証局を構成し，この認証局を利用してスタンドアロン型アドホックネットワークにおいて，公開鍵による端末認証を実現する方式を提案した．計算機シミュレーションを行い，悪意を持つ不正端末が存在時の安全性に関する性能評価を行った．

(2) 上記(1)で開発した端末認証技術では，各端末は，自身が他端末の信頼度情報および公開鍵情報を周囲の端末と定期的に交換し，端末認証に必要な他端末情報を収集する．この収集プロセスにおける発生トラヒックを最小化するため，各端末の位置情報を利用して，収集プロセスで不必要な情報交換がなされるのを防ぎ，さらにネットワークコーディングを用いた高効率ブロードキャスト通信を行うことで，ネットワーク負荷の観点から収集プロセスの最適化を行った．さらに，計算機シミュレーションによる性能評価を行い，提案手法の有効性を定量的に検証した．

(3) 本研究で提案する端末認証方式においては，複数の端末が仮想認証局を構成し認証機能を提供する．仮想認証局の構成端末群は仮想認証局を維持するための制御情報を定期的に交換する．この制御情報の交換プロセスで発生するトラヒックを最小化するため，

端末位置情報に基づいてユニキャスト複数配信とマルチキャスト配信を組み合わせて用いる通信経路最適化手法を提案した．また，計算機シミュレーションによる性能評価を行い，本最適化手法の有効性を定量的に検証した．

４．研究成果

(1)本研究課題で提案するネットワーク監視に基づく端末信頼度評価技術では，各端末が自身の隣接端末の通信状況を監視し，さらに周囲で交換される公開鍵証明書を収集する．この監視・収集結果に基づいて隣接端末の信頼度評価を分散的に行う．さらに，信頼度の高い端末群が仮想的に１つの認証局として機能し，一定数以上のグループメンバ端末から同意を得た端末に対して公開鍵証明書を発行する．本方式では，なりすましを行うために不正な公開鍵証明書を発行する不正端末が存在する場合でも，端末信頼度評価と仮想認証局機能によって不正な公開鍵証明書を排除し，正しい端末認証が可能となる．この点を検証するため，計算機シミュレーションを行い，提案方式が既存方式と比較して高い安全性を有することを確認した．提案方式と既存方式（確率的減衰モデル）の正当結合率特性を図１に示す．正当結合率とは，公開鍵と所有者を正しく紐付けできた数／紐付けを行った総数であり，端末認証が正しく行われているかを表す尺度である．また，図１においてグラフの横軸は不正な証明書を発行する不正端末数を表している．

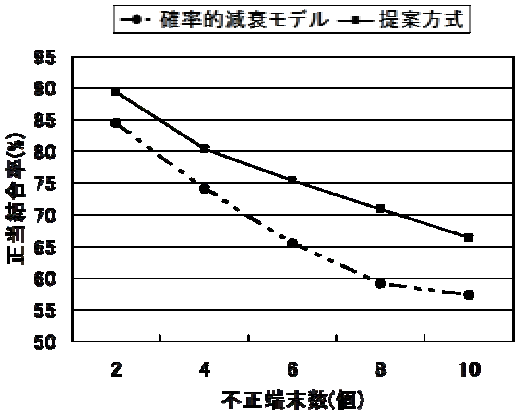

図１：正当結合率特性

図１より，提案方式は既存方式（確率的減衰モデル）と比較して，高い正当結合率を実現できている．特に，不正端末数が多い状況下においては，約 10%の改善が見られることがわかった．

(2) 上記(1)で提案した端末認証方式においては，端末認証に必要な他端末情報を収集する際のトラヒック負荷がネットワークを圧迫し，他のトラヒックに多大な悪影響を与える．そこで，本研究課題では，端末位置情報とネットワークコーディングを用いた高効率ブロードキャスト通信を用いて，ネットワーク負荷の観点から収集プロセスの最適化を行った．本最適化手法によってネットワーク負荷が軽減されていることを検証するため，計算機シミュレーションを行い，提案方式と既存方式の性能比較を行った．提案方式（AMSNC）と既存方式（Flooding, Aggregation）のネットワーク負荷特性を図２に示す．図２においてグラフの縦軸はネットワーク内で中継されたパケット数，横軸は中継されるパケットのサイズを表している．

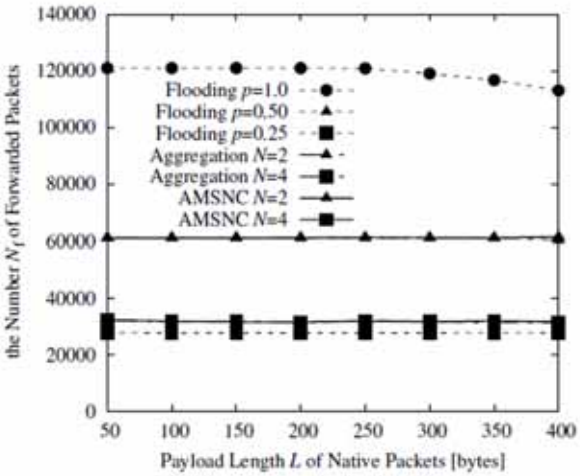

図２：ネットワーク負荷特性

図２より，提案方式は，既存方式と比較してネットワーク負荷を 40%以上軽減できることを明らかにした．

(3) 上記(1)で提案した端末認証方式においては，仮想認証局の構成端末群は仮想認証局を維持するための制御情報を定期的に交換する必要がある．この制御情報の交換は構成端末群内での一対多通信となるため，マルチキャスト通信を用いられる．この交換プロセスで発生するトラヒックを最小化するためユニキャスト複数配信とマルチキャスト配信を組み合わせて用い，さらに２つの配信法で用いられる通信経路を端末位置に基づいて最適化する手法を提案した．本最適化手法の有効性を検証するため，計算機シミュレーションによる性能評価を行った．図３は，ユニキャスト複数配信（AODV）とマルチキャスト配信（ODMRP）におけるデータパケット（仮想認証局機能用制御情報）と制御パケット（経路制御用情報）が全トラヒックに占めるバイト量を示している．図３より，受信ノード数（仮想認証局の構成端末数）が小さい場

合は，ユニキャスト複数配信を用い，受信ノード数が多い状況下では，マルチキャスト配信を用いて仮想認証局機能用制御情報を配信することで，制御情報交換プロセスの通信トラヒックを最小化できることがわかる．

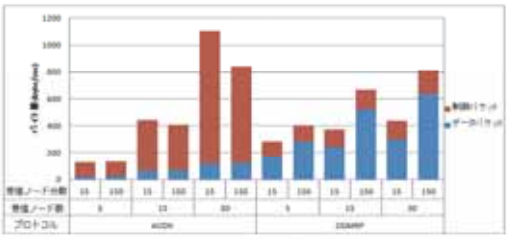

図 3：全トラヒックに占めるバイト量特性

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 13 件）

① 日比野裕，野口拓，川合誠，``アドホックネットワークにおけるユニキャスト複数配信とマルチキャスト配信との性能比較 ”，情報処理学会研究報告，Vol. 2012-MBL-61, No. 39, 2012 年 3 月，査読無.
② 三輪祐太，野口拓，川合誠，``Bluetooth で構成したアドホックネットワークの特性 ”，情報処理学会研究報告，Vol. 2012-MBL-61, No. 40, 2012 年 3 月，査読無.
③ 北川大智，野口拓，川合誠，`` Android 端末を用いたアドホックネットワーク上に実装した Web アクセスシステム ”，情報処理学会研究報告，Vol. 2012-MBL-61, No. 42, 2012 年 3 月，査読無.
④ Keisuke Minami, Takahiro Matsuda, Tetsuya Takine, Taku Noguchi, ``Asynchronous Multiple Source Network Coding for Wireless Broadcasting”, American Institute of Mathematical Sciences (AIMS) Journal, Numerical Algebra, Control and Optimization, Vol.1, No.4, pp.577-592, Dec. 2011，査読有.
⑤ Takahiro Matsuda, Taku Noguchi, Tetsuya Takine, ``Survey of Network Coding and Its Applications”, IEICE Transactions on Communications, Vol.E94-B, No.3, pp.698 -717, Mar. 2011，査読有.
⑥ Nguyen Kim Giang，野口拓，川合誠，`` ZigBee センサーネットワークにおける受信信号強度を用いた位置推定手法に関する一検討 ”，2011 年電子情報通信学会総合大会, B-20-3, p. 598, 2011 年 3 月，査読無.
⑦ 三輪祐太, 谷英紀, 野口拓, 川合誠, `` iPod touch アドホックネットワーク上に実装した簡易型 AODV の特性 ”, 2010 年電子情報通信学会ソサエティ大会, B-21-9, p. 409, 2010 年 9 月，査読無.
⑧ 神田景太，野口拓，川合誠，``カメラの遠隔操作機能を有する画像収集アドホックネットワークの構成と特性 ”, 情報処理学会第 72 回全国大会，4ZD-9，pp. 3-543-544， 2010 年 3 月，査読無.
⑨ 立山崇之，野口拓，川合誠，``アドホックネットワークにおける相互評価された端末信頼度を考慮する分散型公開鍵認証方式 ”，情報処理学会第 72 回全国大会, 5ZD-7, pp. 3-607-608, 2010 年 3 月，査読無.
⑩ 星野豊，野口拓，川合誠，``適応型ネットワークコーディングを用いたアドホックマルチキャストネットワーク ”, 情報処理学会第 72 回全国大会，6ZD-9，pp. 3-557-558, 2010 年 3 月，査読無.
⑪ 河内洋介，野口拓，川合誠，``送信者認証を用いた安全なアドホックネットワークルーチングプロトコル", 電子情報通信学会論文誌レター論文，Vol.J92-B,No.12,pp.1844-1847,Dec. 2009，査読有.
⑫ 滝口隆樹，野口拓，川合誠，``接続安定性に基づくアドホックオーバーレイマルチキャストツリー構築法", 電子情報通信学会論文誌レター論文， Vol.J92-B, No.10， pp.1712-1715, Oct. 2009，査読有.
⑬ 南圭祐，野口拓，松田崇弘，滝根哲哉，`` マルチソースネットワークコーディングを用いた無線ブロードキャストの性能改善 ”，信学技報，Vol. 109，No. 37, IN2009-2, pp. 7-12, 2009 年 5 月，査読無.

〔学会発表〕（計 0 件）

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者

野口　拓（NOGUCHI　TAKU）
立命館大学・情報理工学部・助教
研究者番号：00388133