社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－MBL－39 (5)
2006－ITS－27 (5)
2006／11／16

アドホックネットワークにおける PKI 証明書連鎖発見問題について

安田 侑八 † 毛利 寿志 † 高田 喜朗 † 関 浩之 †
† 奈良先端科学技術大学院大学 情報科学研究科
630-0192 奈良県生駒市高山町 8916-5
E-mail:† {ikuya-y, hisas-mo, y-takata, seki}@is.naist.jp

あらまし アドホックネットワークでは，一般的な PKI システムで用いられるような信頼できる認証局やレポジトリを仮定できない．そこで通信域内の各ノードが互いに自律的に証明書を発行できる web-of-trust 型 PKI システムが研究されている．このシステムはネットワークトポロジが変化するアドホックネットワークにおいて有用であるが，認証に必要な証明書が手元にない場合，認証相手までの証明書連鎖を発見しなければならないという問題点がある．本稿ではこのシステムを重み付き有向グラフで形式化し，分散アルゴリズムを用いて証明書連鎖発見問題を解決する新たな方式を提案する．また通信量の評価指標を提案し，それに従って既存研究と提案手法の通信量を比較する．
キーワード アドホックネットワーク，PKI，証明書連鎖，通信量，分散アルゴリズム

PKI Certificate Chain Finding Problem for Ad Hoc Networks

Ikuya YASUDA †, Hisashi MOHRI †, Yoshiaki TAKATA †, Hiroyuki SEKI †
†Graduate School of Information Science
Nara Institute of Science and Technology
Takayama 8916-5, Ikoma, Nara, 630-0192 Japan
E-mail:†{ikuya-y, hisas-mo, y-takata, seki}@is.naist.jp

Abstract In an ad hoc network, we cannot assume a trusted certification authority and a centralized repository that are used in ordinary PKI systems. Hence several studies have been done on a PKI system of web-of-trust type in which each node within communication range can issue certificates with each other in a self-organizing manner. This system is useful for ad hoc networks whose topology can change, but it has a problem that nodes without certificates necessary for authentication need to find a certificate chain to the target node. In this paper, we model this system as a weighted directed graph and formally define the certificate chain finding problem, and we propose a new method based on distributed algorithms that solves the problem. Furthermore, we propose a measure of communication cost, and according to the measure, we compare our method with an existing method.
Key Words Ad hoc networks, PKI, certificate chain, communication cost, distributed algorithms

1 はじめに

アドホックネットワークは，固定された基盤に頼らない自律したネットワークのことであり [5]，その特性のため既存のセキュリティ技術をそのまま適用できない．既存のセキュリティ技術の代表的なものに公開鍵基盤 (PKI)[11] があるが，これを導入する場合，認証局の存在を仮定するのが一般的である．しかしアドホックネットワークの移動性や自律性などにより，既存の認証局を利用できない．ネットワーク内の特定のノードを認証局

として仮定する方法も考えられているが，認証局となったノードの移動性や悪意あるノードからの攻撃により，認証局の機能が損なわれる可能性が大きい．そのため，アドホックネットワークにおいて認証局の存在を仮定することは適当でない [8]．そこで，各ノードが自律的に証明書を発行する web-of-trust 型 PKI システムに着目する．このシステムにおいては，ノードが各自で証明書保管庫 (レポジトリ) を保有するという新たな方式も研究されており [1, 9]，本研究でもこの方式を用いる．しかしこの方式には，認証の際に必要となる証明書が自身のレポジトリにない場合，相手ノードまでの証明書連鎖を発見しなければならないという問題がある．

証明書連鎖とは，PKI の公開鍵認証における推移律のことである．PKI では，自身や認証局など，公開鍵を予め確実に取得できているノード (これらを信頼点と呼ぶ) の公開鍵を用いて，通信したい相手の公開鍵の有効性を検証する．これを公開鍵の認証という．ここで，認証を行うノードを**認証要求ノード**，通信相手を**最終被認証ノード**と呼ぶ．さらに，信頼点が通信相手の公開鍵に直接署名していなくても，証明書連鎖が存在すればその連鎖を通して公開鍵の認証が可能である．すなわち認証要求ノードは，最初に信頼点を信頼し，次に信頼点に署名された公開鍵の持ち主を信頼する．この関係を繰り返し適用し，結果的に最終被認証ノードまでの証明書連鎖を見つけることができれば認証は成功したといえる．通常のネットワークのようにレポジトリを集中管理している場合には，その中から証明書連鎖を見つけるだけでよいが，アドホックネットワークのようにレポジトリを分散管理している場合には，証明書連鎖の発見は容易でない．

本稿では，アドホックネットワークにおける証明書連鎖発見問題の新たな解法を提案する．まず問題を明確にするために，アドホックネットワークにおける web-of-trust 型 PKI システムを，重み付き有向グラフで形式化する．さらに，アドホックネットワークにおける証明書連鎖発見問題を有向グラフ上のノード間のパスを発見する問題と見なし，この問題を経路情報に関する分散アルゴリズムを用いて効率よく発見する方式を提案する．具体的には，証明書連鎖発見問題を**証明書連鎖探索段階**と**証明書連鎖収集段階**に分け，探索段階では**生成木を構成する分散アルゴリズム**を用いて連鎖を探索し，収集段階では実際に認証要求ノードへ証明書を添付して送信する．また，本稿では，提案手法についての評価も合わせて行う．既存研究では，証明書サイズなどパケットサイズを考慮した評価方法が行われていないため，まず我々の考える問題に沿った評価指標を提案し，さらにこの評価指標に従って既存研究と提案手法それぞれの評価と比較を行う．

2 アドホックネットワークにおける証明書連鎖発見問題

ここでは，本稿で扱う証明書連鎖発見問題を定義する．そのためにまず PKI 信頼モデルについて説明し，次にアドホックネットワークへの PKI 技術の適用方法を述べる．その後で，アドホックネットワークにおける証明書連鎖発見問題を定義する．

2.1 PKI の概要と PKI 信頼モデル

PKI システムとは，あるノードの公開鍵などの情報に別のノードが署名を施した公開鍵証明書を用いるセキュリティ基盤である [11]．公開鍵暗号を用いる場合，有効性が確実な公開鍵を取得する必要がある．PKI システムでは信頼点 (認証要求ノード自身や認証局など) の公開鍵を用いて各証明書に含まれる公開鍵の有効性を検証する．さらに，以下に述べるように，PKI システムでは公開鍵の有効性検証に関する推移律が成り立つと仮定することで，直接信頼点が通信相手の公開鍵に署名していなくても，間接的に通信相手の公開鍵の有効性を確認できる．すなわち，通信相手の公開鍵の有効性検証を行う認証要求ノードは，まず信頼点を信頼し，次に信頼点に署名された公開鍵の持ち主を信頼する．この関係を繰り返し適用し，結果的に最終被認証ノードまでの証明書連鎖を見つけることができれば，認証要求ノードは最終被認証ノードの公開鍵の有効性を検証できる．

また，あるネットワークにおける証明書の発行関係を表したものは信頼モデルと呼ばれる [4]．一般に信頼モデルは有向グラフで表現され，各頂点はノード，各有向辺は証明書の発行関係に対応し，有向辺 $\langle u, v \rangle$ は，ノード u がノード v の公開鍵証明書の発行者であることを表す．信頼モデルは，全ノードが信頼する認証局 (証明書発行機関) を仮定する階層型信頼モデルと，PGP[7] をはじめとする認証局を仮定しない web-of-trust 型信頼モデルに大別される [2]．アドホックネットワークで PKI システムを構築する場合，閾値署名などを用いて認証局を仮定する手法も存在するが [6, 8]，その多くはネットワーク内のある特定のノードに認証局の機能を持たせる方式であり，攻撃対象が限定されるという問題の根本的な解決には至っていない．よって，一般的には認証局を

仮定しない web-of-trust 型信頼モデルの方がアドホックネットワークに適していると考える．ゆえに本研究では web-of-trust 型信頼モデルを適用する．

2.2 アドホックネットワークへの PKI 技術の適用

web-of-trust 型信頼モデルをアドホックネットワークへ適用するためには，証明書レポジトリの運用方法を考えなければならない [1]．通常のネットワークにおけるレポジトリの管理は，信頼できる第三者が行っていることが多い．しかしアドホックネットワークの場合，信頼できる第三者機関を仮定できない．このような問題に対して，[1] では各ノードがレポジトリを持つようなアドホックネットワークのための PKI モデルを提案している．しかし，「レポジトリにはできるだけ多くの証明書を集める」という方針のため，証明書の収集に通信量が大きくかかるという問題があった．

[1] における問題を解決するために，北田らは次のような方針に基づく証明書の管理方法を提案している [9]．

- 各ノードは，自身が他のノードに署名した証明書，または自身の公開鍵に対して他のノードが署名した証明書のみをレポジトリに保管する．

このように，レポジトリに保管する証明書を制限することにより，証明書の収集に必要な通信量を削減することができる．ただし北田らのモデルでは，通信相手の公開鍵を検証するために，毎回証明書連鎖をネットワーク全体から探さなければならないという新たな問題が発生する．この問題を，**アドホックネットワークにおける証明書連鎖発見問題**と呼ぶ．

定義 1 アドホックネットワークにおける証明書連鎖発見問題

アドホックネットワークにおいて，各ノードがレポジトリを持ち，さらに自身に関する証明書のみを保管する web-of-trust 型信頼モデルに基づく PKI システムを仮定する．このとき，認証要求ノードが最終被認証ノードまでの証明書連鎖を発見し，連鎖上の各証明書を収集するという問題を，証明書連鎖発見問題という．

3 既存研究: 北田方式

2.2 節で述べた証明書連鎖発見問題に対して，北田方式ではまず認証要求ノードがネットワーク全体に対して証明書連鎖の探索を行うためのプロトコル ASNS を提案している．ASNS の動作は以下の通り．

- 認証要求ノードは自身が証明書を発行したノード全員に探索パケット p を送信．
- 探索パケット p を受け取った各ノード v は，
  - p の送信者が予め自身 (v) に発行した証明書を p に添付．さらに p の宛先を v が証明書を発行したすべてのノードとして，p を送信．
  - ただし，v が最終被認証ノードに証明書を発行している場合，同様に証明書を p に添付するが最終被認証ノードにのみ p を送信 (ユニキャスト)．
- 同一の探索パケットを受け取ったノードは，二回目以降受信した探索パケットを破棄．

各ノードが同一のパケットを二回目以降破棄することによって，通信路を流れるパケット数は辺数の線形オーダとなる．

また，ASNS によって最終被認証ノードに集められた証明書連鎖中の各証明書が，最終被認証ノードから認証要求ノードへユニキャストされることによって，認証要求ノードは必要とするすべての証明書を入手できる．

しかし，アドホックネットワークのような分散ネットワークでは，一度の探索プロトコルによって (すぐに証明書連鎖が見つかったとしても) ネットワーク全体に探索パケットが到達しなければプロトコルは完了しない．そのような環境で証明書を探索パケットに添付するような ASNS では，通信量が大きくかかってしまう．このような点から，証明書連鎖発見問題をより小さい通信量で効率よく解く新たな方式が必要である．

4 提案手法

まず，前提としてアドホックネットワークにおける web-of-trust 型 PKI システムの形式化を行う．その上で，効率よく証明書連鎖を発見する方式を提案する．本稿では，無駄な証明書の添付を避けるため，**証明書連鎖探索段階**と**証明書収集段階**の二段階に分けて，アドホックネットワークにおける証明書連鎖発見問題を解決する．

4.1 アドホックネットワークにおける web-of-trust 型信頼モデルの形式化

ここでは証明書連鎖発見問題を明確にするため，アドホックネットワークにおける web-of-trust 型信頼モデルの形式化を行う．

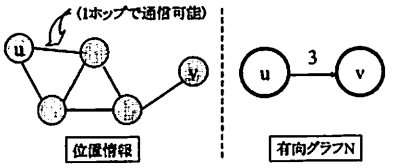

図 1　物理的なネットワークと重み付き有向グラフ N との関係

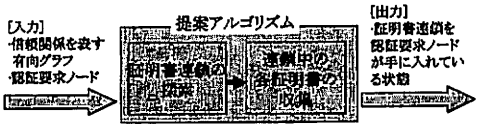

図 2　提案手法の概要

定義 2 信頼モデルの形式化

アドホックネットワークにおける web-of-trust 型信頼モデルを重み付き有向グラフ $N = (V, E, \phi)$ とする．

ここで，

- V：ノードの集合．
- E：有向辺の集合．
- ϕ：有向辺から非負整数への重み関数．

信頼モデル上で有向辺が存在したとしても，物理的にその 2 ノードが隣接している (直接通信できる) とは限らない．そこで，信頼モデル中の各有向辺 $\langle u, v\rangle$ の重み $\phi(\langle u, v\rangle)$ は，物理的な距離 (最小ホップ数) を表すとする (図 1)．なお，ここでは簡単のため，有向グラフ N 中の V は，アドホックネットワークを構成する全ノードの集合と同一であると仮定する．

4.2　効率よく証明書連鎖を発見する方式の提案

3 節で述べたように，北田方式では，証明書連鎖の探索時に証明書を添付してブロードキャストしている．しかし，これでは関係のないノードにも証明書が添付されたパケットが配送されることになり，ネットワーク全体の通信量も大きくなってしまう．そこで本研究では，証明書連鎖探索段階と証明書収集段階の二段階に分けて証明書連鎖発見問題を考え，この問題に対するより効率の良い解法を提案する (図 2)．

■証明書連鎖探索段階　ネットワークの各ノードはルーティングプロトコルなどを参照することにより，他の各ノードまでの距離を参照できると仮定する．しかし，信頼モデルについては自身に関する証明書発行関係のみ分かっている．証明書連鎖を探索する問題は，このような状況で認証要求ノードが最終被認証ノードまでの証明書連鎖を見つけるという問題である．また認証要求ノードにとって，すべての証明書連鎖を見つける必要はなく，有効な連鎖を 1 つでも見つけられれば認証に足りる．

本研究では，上記の問題を解く方法として，有向グラフ N 上における**認証要求ノードを根とした生成木 (spanning tree) を構成する分散アルゴリズム**を使用する．すなわち，認証要求ノードは，最終被認証ノードまでの証明書連鎖を知りたいとき，生成木を構成する分散アルゴリズム [3] を使用し，有向グラフ N 上で自身を根とする生成木を構成する．生成木を構成する一般的な分散アルゴリズムでは，通信計算量が $O(|E|)$ であることが知られている [3]．ここで，$|E|$ は有向辺の集合 E の要素数を表す．

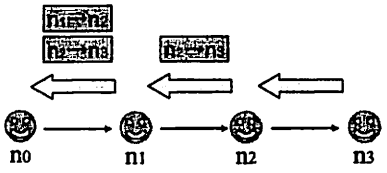

図 3　証明書連鎖収集方式

■証明書収集段階　証明書連鎖探索段階が終了したとき，各ノードは生成木の根ノード (認証要求ノード) と自身の親子関係のみを知っており，この段階では認証要求ノードはまだ生成木全体を把握できていない．証明書を収集する問題は，このような状況で認証要求ノードが先の証明書連鎖探索段階で求めた証明書連鎖中のすべての証明書を取得するという問題に帰着できる．

本研究では上記の問題の解法として，最終被認証ノードから順番に必要な証明書を添付して認証要求ノードまで順次パケットを返信していくという方式を提案する (図 3)．ここでは，連鎖中の全証明書を入手しようとする認証要求ノードは，最終被認証ノードまでの連鎖の経路は知らないが，連鎖中の各ノードは経路における直接の親ノードを知っていることを利用する．証明書連鎖探索段階が終了したとき，証明書連鎖中の各ノードは以下のように振る舞う．

- 最終被認証ノードは，直接の親に返信パケットを送信．
- 返信パケットを受け取った各ノードは，証明書連鎖

に必要な証明書を添付し，宛先を自身の直接の親として送信．

上記の操作を繰り返すことにより，最終的に認証要求ノードに返信パケットが到達するとき，認証要求ノードは証明書連鎖中の全証明書を受け取ることができる．

5 評価

ここでは評価指標の定義を行い，それに基づいて北田方式と提案方式の評価を行う．具体的には，定義した評価指標に基づき，各方式の通信量を算出しそれらの比較を行う．またその結果より，提案方式の方が北田方式に比べて通信量が抑えられることを示す．

5.1 通信量の定義

本研究における通信量の定義に入る前に，北田方式で用いられている通信量の定義に触れる．北田方式における通信量はメッセージ数 (パケット数) で定義されており，パケットに証明書が 10 枚添付されていても 1 枚添付されていても，一度に送信できればメッセージ数は同じ 1 となる．この評価法では証明書のサイズや枚数が考慮されておらず，現実的ではない．そこで本研究では，より現実的な通信環境を考慮し，**メッセージ量の点から通信量を定義する**．メッセージ量は証明書のサイズや枚数により変化する．そのため，添付される証明書の枚数が多くなる程通信量は大きくなる．

ここでの通信量を数式で示すと，以下の通りになる．ただし，ネットワークにおける任意の有向辺を e とおく．

$$\sum_{\text{有向辺}\ e} \{e\text{を流れるメッセージ量} \times \phi(e)\}$$

5.2 北田方式の評価

北田方式では証明書の探索に生成木を構成する分散アルゴリズムを使用している．認証要求ノードを根ノードとし，最終被認証ノードを探索しながら生成木は構成されていく．証明書連鎖の探索が終了しても，連鎖に関係のないノードはそのことを知らないため，パケットはネットワーク上を流れ続ける．結果，存在する証明書連鎖の長さよりも構成される生成木の高さの方が長くなる場合が起こる．つまり以下のような関係が成り立つ．

$$\text{証明書連鎖の長さ} \leq \text{生成木の高さ}$$

通信量の評価においては，証明書連鎖の長さが生成木の高さと等しいと仮定している．すなわち，証明書連鎖の長さの上界に基づいて評価する．この仮定は 5.3 節においても同様である．

北田方式は証明書連鎖の探索と同時に証明書の添付も行っている．またパケットが最終被認証ノードに到達すると，添付されてきた全ての証明書がユニキャストで認証要求ノードに送られる．このときの通信量は次式の通り．

$$\text{[探索]} \qquad S_1(k) = n\sum_{i=1}^{k}\{Crt(i-1)+1\}m^i$$

$$\text{[収集]} \qquad C_1(k) = n(k \times Crt + 1)$$

n は平均ホップ数，m は有向グラフ上の平均次数，Crt は証明書サイズを表す．

■証明書探索段階　認証要求ノードは，最初に有向グラフ上の子ノードに向けて探索を要求する信号 (パケット) を送信する．このとき証明書は添付されていない．次にそのパケットを受信したノードは，送られてきたパケットに自らに対して発行された証明書を添付し，次のノードへ送信する．このように，認証ノードが見つかる度に証明書が次々と添付されていき探索が進んでいく．中括弧内の $+1$ は信号の送信に必要な通信量である．

■証明書収集段階　添付されてきたすべての証明書と最終被認証ノードに対して発行された証明書が認証要求ノードへ送られる．そのため，木の高さと同じ枚数分だけの証明書が添付されている．また括弧内の $+1$ は探索時と同じく，パケットを送信するのに必要な通信量である．

5.3 提案方式の評価

提案方式は北田方式と同じく生成木を構成しながら探索を行っている．しかし北田方式と異なり，パケットに証明書を添付しない．そのため，証明書の収集は探索した連鎖を遡りながら順次行っていく．この方式における通信量は次の通り．

$$\text{[探索]} \qquad S_2(k) = \sum_{i=1}^{k} m^i$$

$$\text{[収集]} \qquad C_2(k) = n\sum_{i=1}^{k}\{Crt(i-1)+1\}$$

北田方式と同じく，n は平均ホップ数，m は有向グラ

フ上の平均次数，Crt は証明書サイズを表す．

■証明書探索段階　各ノードは証明書の添付を行わず，探索を知らせる信号のみを送信する．よって探索時の通信量は，有向グラフ上の平均次数を等比とした級数になる．

■証明書収集段階　探索が終了すると，最終被認証ノードは証明書収集の開始を知らせる返信パケットを連鎖中の親ノードへ向けて送信する．そのパケットを受信した親ノードは，自身が最終被認証ノード (子ノード) へ発行した証明書をパケットに添付し，またさらに自身の親ノードへパケットを送信する．このように最終被認証ノードから返信されたパケットは，証明書連鎖を遡りながら順次証明書を添付していく．結果的に認証要求ノードは，(木の高さ -1) 枚の証明書を受け取る．そして最後に自身が子ノードへ発行した証明書を合わせると，連鎖中の全ての証明書が集まる．式中の中括弧の中の $+1$ は，パケットの送信に必要な通信量である．

5.4　通信量の比較

次に，北田方式と提案方式それぞれの通信量を比較する．

数式中の級数を計算し，北田方式と提案方式の通信量における比を求めた．結果は次の通りである．

$$\frac{S_1(k)+C_1(k)}{S_2(k)+C_2(k)} = \frac{O(k\cdot Crt\cdot m^{k+2})}{O(m^{k+1})} = O(k\cdot Crt\cdot m)$$

提案方式に比べ，北田方式を用いた方が通信量が大きくなることがわかる．

以下では，5.2 節と 5.3 節の各数式に具体的に数値を代入して比較と解析を行う．代入する数値は，$n=4$, $m=4$, $Crt=1024$(ビット) とする．$n=4$, $m=4$ は北田方式において，証明書連鎖を構築するのに妥当な値として挙げられているものを用いた．また証明書サイズの 1024 ビットは，RSA 暗号で比較的安全とされる値である．

通信量のグラフ結果は，図 4(証明書連鎖の探索にかかる通信量)，図 5(証明書の収集にかかる通信量)，図 6(全通信量) の通り．

図 4 から，提案方式の方が北田方式に比べて証明書連鎖の探索にかかる通信量を低く抑えていることがわかる．提案方式の場合パケットに証明書を添付せずに信号のみを送信するため，メッセージ量が小さくなるからである．

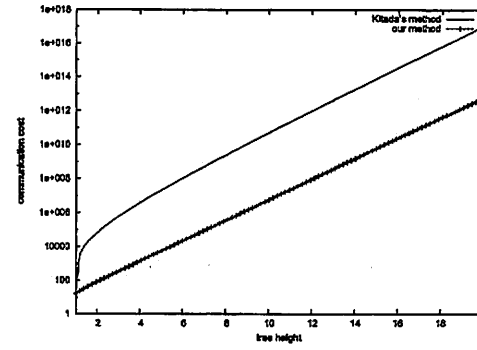

図 4　探索にかかる通信量の比較

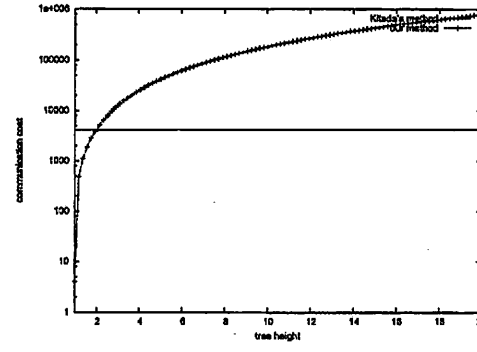

図 5　収集にかかる通信量の比較

また，図 5 では，木の高さが 3 以上のとき北田方式の方が通信量が小さくなっている．北田方式の場合，探索が終了した時点で最終被認証ノードに連鎖中の全証明書が集まっており，それを一度に認証要求ノードへユニキャストするだけでよい．しかし提案方式では，連鎖を遡りながら証明書を集めていかなければならず，一度にユニキャストする方法よりも物理的な通信距離が累積するため，より通信量が必要になる．こうした結果から，北田方式に比べて提案方式の通信量が比較的大きくなっている．

次に探索と収集両方の通信量を足し合わせた結果を比較する (図 6)．木の高さ (ノード数) に関わらず提案方式の方が常に通信量を低く抑えられており，証明書連鎖を発見し連鎖中のすべての証明書を集めてくるという証明書連鎖発見問題において，提案方式の方が北田方式に比べ優れているといえる．

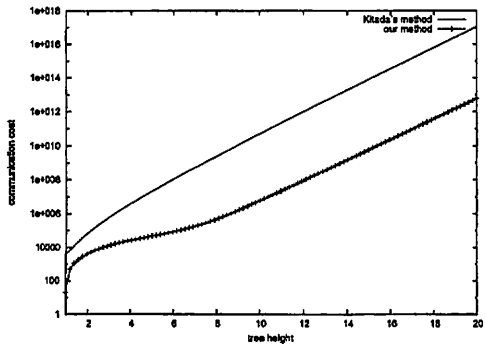

図 6　全通信量の比較

6　提案方式の改良

6.1　改良 1

ここでは提案方式の改良として新たな方式を提案する．提案方式では生成木を構成する分散アルゴリズム [3, 10] を用いて証明書連鎖の探索を行っていたが，改良 1 では最短経路木を構成するアルゴリズムを用いる．有向辺の重み (ホップ数) を基に最短経路木を構成し，認証要求ノードから最終被認証ノードまでの最短な証明書連鎖を探索する．この方式の利点は，証明書収集において連鎖中のすべての証明書を最短経路で集めることができる点である．そのため，生成木 (4 節) に比べ証明書収集段階における通信量を抑えることができる．逆にこの方式の欠点は，生成木に比べ木の構成にかかる通信量が大きくなることである．そのため頻繁に信頼関係が変化し木の構成回数が多くなる場合にはこの方式は不利になる．

6.2　改良 2

さらに改良 1 とは独立に別の改良として，証明書収集段階の改良も考えられる．提案方式のような最終被認証ノードから順番に証明書を添付しながら認証要求ノードまで順次返信していく方式では，認証要求ノードは一度に必要な証明書をすべて受け取ることができる反面，添付された証明書がすべての中間ノードを経由するために通信量が大きくかかってしまう．しかし，証明書連鎖探索段階が終了した時点では，どのパスが認証要求ノードの求める証明書連鎖かわからない．そこで，改良 2 では探索段階が終了したとき，証明書連鎖中の各ノードは以下のように振る舞うとする (図 7)．

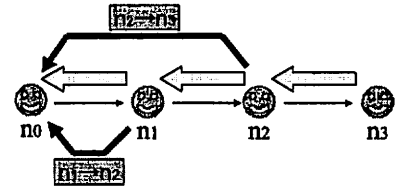

図 7　証明書連鎖収集方式

- 最終被認証ノードは，直接の親に返信パケットを送信．
- 返信パケットを受け取ったノードは，証明書連鎖に必要な証明書 (自身が子に発行した証明書) を直接認証要求ノードにユニキャストし，さらに自身の直接の親 u に対して，u が証明書連鎖中にいることを知らせるための返信パケットを送信．

上記の操作を繰り返すことにより，最終的に認証要求ノードに返信パケットが到達すれば，認証要求ノードは証明書連鎖中の全証明書を各中間ノードからユニキャストされて受け取ることができる．

7　おわりに

アドホックネットワークにおける PKI 証明書連鎖発見問題に対する新たな解法と，その改良法を提案した．最初に，アドホックネットワークにおける web-of-trust 型 PKI システムを重み付き有向グラフで形式化し，アドホックネットワークにおける証明書連鎖発見問題を，先に形式化した有向グラフ上のノード間のパスを発見する問題と見なした．そして，生成木を構成する分散アルゴリズムを用いてこの問題を効率よく解く方式を提案した．既存手法である北田方式では，証明書連鎖の探索段階で証明書を添付しているため，証明書連鎖に関係のない余計な証明書も通信路を流れてしまう欠点があった．その点，本研究の提案方式では，探索段階において証明書連鎖の探索のみを行い，証明書の収集に工夫を行うことで，より通信量を抑えた解法となっている．

本稿では，通信量の評価を行い既存手法と提案手法とを比較した．今後の課題として，提案手法と既存手法についてそれぞれシミュレーションを行い，それらの比較を行うことが考えられる．また 6 節で挙げた 2 つの改良案の解析を行い，他の方式との比較を行うことも今後の課題の一つである．さらに，アドホックネットワークにおける PKI システムのモデル化そのものについて，

Capkun らのモデル [1] と北田モデル [9] を組み合わせた，新しいモデルの検討も行う予定である．

参考文献

[1] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, 2003, Vol.2, No.2, pp.52–64, 2003.

[2] C. R. Davis, "A Localized Trust Management Scheme for Ad Hoc Networks," IEEE International Conference on Networking (ICN), pp.671–675, 2004.

[3] N. A. Lynch, "Distributed Algorithms," Morgan Kaufmann Publishers, 1996.

[4] R. Perlman, "An Overview of PKI Trust Models," IEEE Network, Vol.13, No.6, pp.38–43, 1999.

[5] C. K. Toh, "Ad-Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall, 2001.

[6] S. Yu and R. Kravets, "Composite Key Management for Ad Hoc Networks," IEEE Annual International Conference on Mobile and Ubiquitous Systems: Networks and Services (Mobiquitous), pp.52–61, 2004.

[7] P. Zimmermann, "The Official PGP User's Guide." MIT Press, 1995.

[8] L. Zhou and Z. J. Haas, "Securing Ad Hoc Network," IEEE Network, Vol.13, No.6, pp.24–30, 1999.

[9] 北田, 荒川, 竹森, 渡邊, 笹瀬, "無線アドホックネットワークに適したルーティング情報を用いたオンデマンド公開鍵分散管理方式," 電子情報通信学会論文誌, Vol.J88-D1, No.10, pp.1571–1583, 2005.

[10] 三浦, 増澤, 都倉, "距離に応じた計算量で最短経路木を求める分散アルゴリズム," 電子情報通信学会論文誌, Vol.J77-D1, No.1, pp.21–32, 1994.

[11] 情報処理推進機構セキュリティセンター, "PKI 関連技術解説,"
http://www.ipa.go.jp/security/pki/index.html