論　文

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

北田　夕子[†]　荒川　豊[†]　竹森　敬祐[††]　渡邊　晃[†††]
笹瀬　巌[†]

On Demand Distributed Public Key Management Using Routing Information for Wireless Ad Hoc Networks

Yuko KITADA[†], Yutaka ARAKAWA[†], Keisuke TAKEMORI[††], Akira WATANABE[†††], and Iwao SASASE[†]

あらまし　インターネットに接続点を持たない独立した無線アドホックネットワークでは信頼できる既存の認証局 (CA:Certificate Authority) を利用できないため，各ノードが独自に証明書を発行・管理する公開鍵証明書分散管理方式が提案されている．しかし，この方式は，各ノードが全証明書を収集するため，メモリ消費量の増加や失効証明書リストの管理などの問題がある．そこで本論文では，従来方式の課題を解決するために，各ノードは自身に対して発行された証明書のみを持っておき，認証要求が発生した時点で，認証したいノードまでの証明書を収集して信頼の輪を構築するオンデマンド公開鍵証明書分散管理方式を提案する．証明書の収集には，被認証ノードに関わるルーティングテーブル情報を付加してブロードキャストすることで，ブロードキャストが直接届かない被認証ノードも一括して探索することができるアドホック一括ノード探索プロトコル (ASNS:Adhoc Simultaneous Nodes Search) を提案する．提案プロトコルにより，提案方式は，認証に必要な証明書のみを収集するため，ノードのメモリ消費量を削減でき，かつ失効証明書リストの確認処理が不要になる．計算機シミュレーションにより，信頼の輪の構築成功率，信頼の輪を構築するために必要なノード数，および信頼の輪の構築に必要な通信量について評価を行い，ノード密度の低いアドホックネットワーク環境に有利であることを示す．

キーワード　無線アドホックネットワーク，公開鍵基盤，信頼の輪，分散管理

1. まえがき

公開鍵基盤 (PKI:Public Key Infrastructure) [1] を用いることで，認証や情報の秘匿および完全性の保証といった高度なセキュリティサービスを提供できる．PKI では，ノードが生成した公開鍵の正当性を証明するために，公開鍵に対して公開鍵証明書 [2] を発行している．この公開鍵証明書を発行・管理する機関は認証局 (CA:Certificate Authority) と呼ばれる．

昨今，電波の届く範囲内のノードがお互いに協調してパケットを中継する無線アドホックネットワーク [3]〜[7] が注目されている．不特定多数のノードが参加する無線アドホックネットワークの場合，通信相手の認証は重要な課題である．無線アドホックネットワークの環境として，既存の CA を利用できる場合，CA を用いた個人認証ができる．しかし，無線アドホックネットワーク内の 1 つのノードがある既存の CA に認証してもらっている際，他の全ノードがそのノードを信頼しようとする場合，全員が失効証明書リストが格納されているリポジトリサーバにアクセスする必要がある．もし 1 ノードでもインターネットの接続環境がなくリポジトリサーバにアクセスすることが出来なければ，認証は行えない．さらに，ノードが無線アドホックネットワークを構築しようとした場合，常に周囲にアクセスポイントがあるとは限らない．そこで，

[†] 慶應義塾大学理工学部情報工学科, 神奈川県
Department of Information and Computer Science, Keio University, Yokohama, 223-8522 Japan
[††] 株式会社 KDDI 研究所, 埼玉県
KDDI R&D Laboratories, Inc., Saitama, 356-8502 Japan
[†††] 名城大学理工学部情報工学科, 愛知県
Department of Information and Computer Science, Meijo University, Aichi, 468-8502 Japan

本論文では，アドホックネットワーク内のあるノードが，周囲にアクセスポイントがなく，インターネットにオンラインで直接通信できない環境を想定する．このようなネットワークにおいて信頼の輪を用いることで相手認証を行う手法として，各ノードが独自に証明書を発行・管理する公開鍵証明書分散管理方式が提案されている [8]．この方式では，各ノードが独自の判断で信頼する他ノードの公開鍵に対し公開鍵証明書を発行している．各ノードは自身に発行された公開鍵証明書をメモリに格納し，リポジトリを構築する．そして，電波の届く範囲内にいるノードとリポジトリを定期的に交換することで，ネットワーク内の全ての証明書を収集している．ノードは通信相手の公開鍵の正当性を確認したい場合，リポジトリから通信相手までの信頼の輪を構築して，その正当性を検証することになる．しかしながら，この方式では，リポジトリ内の証明書を用いて信頼の輪を構築するため，証明書を収集し始めた初期段階において，格納されている証明書が少なく認証に失敗する確率が高くなる問題や，全てのノードの証明書を収集するまでに多大な時間を要するという問題がある．また，時間を掛けて収集した証明書の有効性を検証しなければならず，証明書を発行したノードに対してその有効性を確認する失効証明書リスト [9], [10] の要求処理も必要になる．さらに，メモリ容量が制限されている移動端末がある中，収集する証明書が増加するとともに，リポジトリの管理に必要なメモリ使用量も増加する問題がある．

そこで本研究では，従来方式の課題を解決するために，各ノードは自身に対して発行された証明書のみをリポジトリに格納しておき，認証要求が発生した時点で通信相手ノードまでの信頼の輪を他ノードと協調して構築するオンデマンド公開鍵証明書分散管理方式を提案する．提案方式では，被認証ノードに関わるルーティングテーブルの情報を付加したパケット (以下探索パケット) をブロードキャストすることにより，信頼の輪の構築に必要なノードだけが探索パケットの中継や信頼の輪の構築に参加するアドホック一括ノード探索プロトコル (ASNS:Adhoc Simultaneous Nodes Search) を新たに導入する．ASNS は 1 回の探索処理で信頼の輪を構築することが可能であり，無駄なトラヒックが発生しない方式である．また，オンデマンドで信頼の輪を構築するため，メモリ使用量を軽減できることや，有効な証明書を収集するために失効証明書リストの確認処理が不要になるなどの優位性を持つ．計算機シミュレーションにより，提案方式に関する基本特性として，信頼の輪の構築成功率および信頼の輪を構築するために必要なノード数について評価を行い，各ノードが他ノードに対して公開鍵証明書を最低 1 枚発行し，自身の公開鍵に対しては他ノードから最低 1 枚発行されるという条件下においては，1 ノードあたり約 4 ノードの証明書を発行しあうことで，確実に信頼の輪を構築することができることを示す．また，通信量に関する評価を行い，特にノード密度の低いアドホックネットワーク環境に有利であることを示す．

以下，**2.** において，従来の公開鍵証明書分散管理方式を示す．**3.** で提案方式の動作について述べ，**4.** で特性評価を行う．最後に **5.** で結論を述べる．

2. 従来の公開鍵証明書分散管理方式

CA を利用できない無線アドホックネットワークにおいて，各ノードが独自に証明書を発行・管理し信頼の輪を用いることで相手認証を行う公開鍵証明書分散管理方式が提案されている [8]．図 1 に従来方式の公開鍵証明書分散管理方式を示す．○がノードを示し，矢印がノード間の信頼関係を示す．例えば，ノード 1 により署名されたノード 2 の公開鍵証明書は 1 → 2 と表現する．この証明書にはノード 2 の公開鍵とノード 1 による署名が含まれている．以下の説明においても，同様の証明書の表現方法を用いる．以下，通信開始ノードを認証ノード，通信相手ノードを最終被認証ノードと呼ぶ．さらにノードから信頼されているノードをそのノードの被認証ノードと呼ぶ．図 1 において，認証ノード 1 が信頼関係を直接結んでいない最終被認証ノード 4 の認証を行いたいものとする．図中の表に，認証ノード 1 がネットワーク内の全証明書を集め終わった定常状態におけるリポジトリ内の証明書の状態を示す．

2.1 認証動作における初期段階

step1) 公開鍵生成

各ノードは公開鍵と秘密鍵のペアを作成する．

step2) 公開鍵証明書発行・格納

各ノードは，知識や経験といった独自の判断で信頼する他ノードの公開鍵に対し公開鍵証明書を発行する．また，自身が発行した証明書，および発行された証明書を，メモリやハードディスク上に構築したリポジトリで管理する．

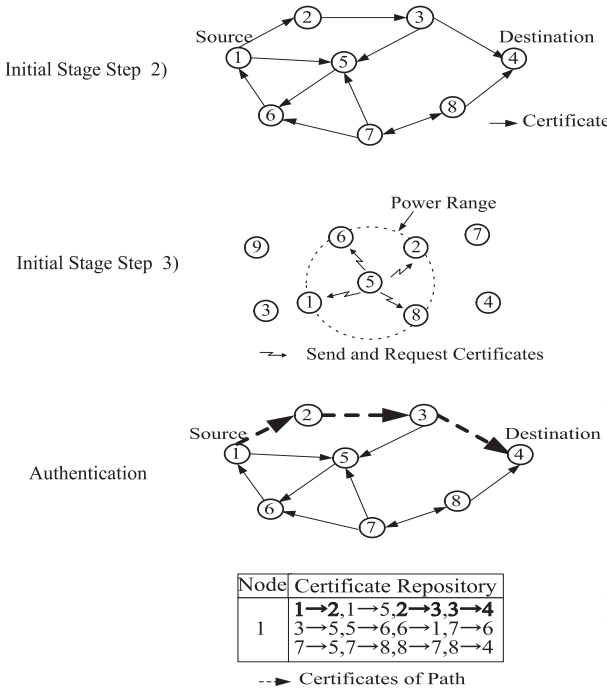

図 1　従来方式の公開鍵証明書分散管理方式
Fig. 1　Conventional distributed public key management.

step3) リポジトリ交換

アドホックネットワークに参加しているノードは，電波の届く範囲内にいるノードと，互いのリポジトリを交換しあう．この処理を繰り返すことで，最終的に全てのノードのリポジトリを収集する．

2.2　信頼の輪の構築

認証ノードは，最終被認証ノードまでの信頼の輪を構築する証明書を自身のリポジトリから探索する．その結果，最終被認証ノード 4 までの信頼の輪が 1 → 2 → 3 → 4 と繋がることがわかる．このため，従来方式は，いったん全証明書を格納してからは信頼の輪が短時間で探索可能である．一方，定常状態に満たない段階では，証明書の収集が満足ではなく，信頼の輪を構築するのに必要な証明書がその時点のリポジトリに存在しない場合がある．この場合，認証ノードと最終被認証ノードの間に実際には信頼の輪が存在するにもかかわらず認証に失敗する．

2.3　信頼の輪の確認

認証ノード 1 は信頼の輪を構築するノードの公開鍵の正当性および証明書の有効性を確認するために以下の処理が必要になる．

2.3.1　公開鍵の正当性確認

公開鍵の正当性を確認するために，その公開鍵に対する電子署名を確認する．認証ノード 1 は，信頼の輪 (1 → 2 → 3 → 4) より，最終被認証ノード 4 の公開鍵に対する署名者はノード 3 であることがわかる．そこでノード 3 の署名をノード 3 の公開鍵を用いて復号化し，公開鍵で解いた情報が正しいことを確認する．正しい場合には，認証ノード 1 は公開鍵 4 の正当性を確認することができる．同様にして，信頼の輪を構築する残りの公開鍵 3 および公開鍵 2 の正当性も確認する．

2.3.2　証明書の有効性確認

証明書が有効期限内であるにも関わらず，秘密鍵を紛失し第三者に悪用されることが予測される場合や，証明書に記載した事項が変化した場合など，その証明書を利用できなくする必要がある．そのため，ノードは自身が格納する全証明書のうち無効な証明書の一覧を記載する失効証明書リストを管理する．信頼の輪を構成する証明書の有効性を確認するためには，この失効証明書リストを検証する必要がある．ノードは失効証明書リスト内の情報を常に最新に保つために，証明書を発行した全ノードに対して定期的に証明書の有効性を確認し，失効証明書リストを更新する必要がある．最終的に，信頼の輪を構築する全証明書が失効証明書リストに存在しない場合，信頼の輪が有効であると判断する．

2.4　従来方式の課題

従来方式では，リポジトリに格納されている証明書が少ない場合，認証に失敗する確率が高い．また，ノードがネットワーク内の全証明書を収集するまでには多大な時間を要する．例えば，従来方式では，ノード数が 100，証明書数が 600 枚で構成されるアドホックネットワークにおいて，リポジトリ交換の間隔を 60 秒とすると，1 ノードが全証明書を収集するために要する時間は約 10000 秒になることが報告されている [8]．ノード数が多い大規模ネットワークになると，この時間は指数関数的に増加する．また，収集する証明書が増加するとともに，リポジトリに必要なメモリ使用量も増加する．移動端末の中にはメモリ量が制約されているものもあり，リポジトリに保有する証明書

数の増大は大きな課題となる．さらに，この方式では，証明書の有効性を確認するために，証明書を発行した全ノードに対し証明書の有効性を定期的に確認し，失効証明書リストを更新する処理負荷の問題もある．

3. オンデマンド分散管理方式の提案

本論文では，従来方式の課題を解決するために，各ノードは自身に対して発行された証明書のみをリポジトリに格納しておき，認証要求が発生した時点で最終被認証ノードまでの信頼の輪を構築することで，全証明書を保持不要となるオンデマンド公開鍵証明書分散管理方式を提案する．信頼の輪を構築するために，ルーティングテーブル情報を付加して探索パケットをブロードキャストすることで，ブロードキャストが直接届かない被認証ノードも一括して探索可能な ASNS を提案する．

3.1 認証動作における初期段階

step1 公開鍵生成

従来方式と同様である．

step2 公開鍵証明書発行・格納

公開鍵証明書発行の発行処理は従来方式と同様である．証明書の管理については，他ノードから発行された自身への証明書のみをリポジトリに格納する．これは，ノードが発行した証明書にはそのノードの署名が含まれており，自身の秘密鍵で署名の有効性を確認できるため，発行した証明書を格納する必要はない．ただし，各ノードは発行した相手ノードの情報のみを記憶しておく．

step3 リポジトリ交換

本提案方式では，他ノードから発行された自身への証明書のみをリポジトリに格納するため，全証明書をリポジトリで管理しない．よって，本ステップは不要である．

3.2 信頼の輪の構築

信頼の輪を構築するためには，まず各ノードのルーティング情報をあらかじめ知っておく必要がある．そこで，提案方式において前提とするアドホックルーティングプロトコルについて述べ，次にそのプロトコルを利用した提案プロトコルについて述べる．

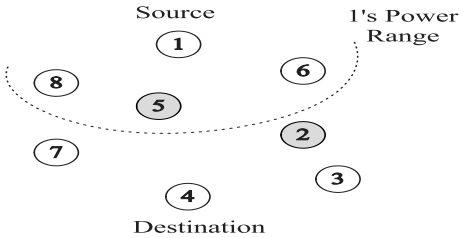

図 2 提案方式における物理的なノードの配置例
Fig. 2 Eaxmple of a physical topology in the proposed system.

3.2.1 前提とするアドホックルーティングプロトコル

無線アドホックネットワークにおけるルーティングプロトコルには，Proactive 型プロトコル [11]〜[15] がある．Proactive 型は定期的に経路情報をノード同士で交換し合うことで，ルーティング情報を収集してルーティングテーブルを常に全ノードが持つようにする．ASNS では信頼の輪に加わる被認証ノードを一括して探索するためにブロードキャストパケットにルーティングテーブル情報を付加する．このため，ASNS では，各ノードが自身のルーティングテーブルを常に保持する必要があり，アドホックネットワークルーティングプロトコルとして Proactive 型ルーティングプロトコルの利用を前提とする．

3.2.2 アドホック一括ノード探索プロトコル

図 2 に提案方式における物理的なノードの配置例を示す．ここで，ノード間の信頼関係は図 1 と同様とし，認証ノード 1 が直接信頼関係を結んでいない最終被認証ノード 4 の認証を行いたいものとする．図 1 より，認証ノード 1 が信頼しているノードはノード 2 と 5 である．図 2 の場合，ノード 1 の被認証ノード 5 は認証ノード 1 の電波の届く範囲内に存在するため探索パケットを受信し，信頼の輪の構築に参加する．しかしながら，被認証ノード 2 は認証ノード 1 の電波範囲外に存在するため，探索パケットを受け取ることができない．

そこで，ASNS では，被認証ノードの探索パケットにアドホックネットワークのルーティングテーブル情報を付加してこれをブロードキャストすることで，認証ノードの電波範囲外に存在するノードに対しても探索パケットを到達させる．ここではノード 6 が探索パケットを更に中継することにより，ノード 1 からの探

索パケットがノード 2 に届けられ，ノード 2 は信頼の輪の構築に参加することができる．

3.2.3 探索パケットの内容

図 3 に ASNS における被認証ノードを探索するためのパケットである探索パケットの内容および各ノードが保持するルーティングテーブルの内容を示す．ここで，1 等の数値はノード識別子を示す．探索パケットには以下の情報フィールドが付加される．

- Authnode：認証ノードフィールド．認証する側のノードの ID(IDentification) を示す．
- Authednode：最終被認証ノードフィールド．最終的に認証されるノードの ID を示す．

各ノードが保持するルーティングテーブルは，宛先ノード情報である DestinationHost の IP アドレスと，宛先ノードに到達するための次ホップノード情報である NextHopHost の IP アドレスから構成される．テーブル上のハイフン “—” は電波の届く範囲内に存在することを示す．探索パケットには，各ノードが保持するルーティングテーブル情報のうち被認証ノードに対応するルーティングテーブル情報を付加する．

図 3(1) に，認証ノード 1 が送信する探索パケットを示す．認証ノードフィールドがノード 1，最終被認証ノードフィールドがノード 4 という情報が付加されている．認証ノード 1 が信頼している被認証ノードはノード 2 とノード 5 であるため，図 3(1) における認証ノード 1 のルーティングテーブル情報のうち DestinationHost がノード 2 とノード 5 に対応するルーティングテーブル情報が付加される．図 3(2) 以降は図 4 と対比させながら説明する．

3.2.4 往路構築

図 4 に，提案方式における認証方法を示す．提案方式における各ノードがリポジトリ内に格納する証明書の表現方法は図 1 と同様である．図 4(1) において，認証ノード 1 が探索パケットのブロードキャストを行った結果，電波の届く範囲内に存在する全ノード (ノード 5,6,8) がこのパケットを受信する．ノード 5 は被認証ノード，ノード 6 はルーティングテーブル情報の nexthop にあたるノードである．それ以外のノード (図の例ではノード 8) は信頼の輪の構築には関与しないので，受信した探索パケットを無視する．図 4 における探索パケット上の×印は，ノードがパケットを無視することを示す．ノードが，探索パケットを受信した場合，自身が探索パケットの発信元であるか確かめるため，探索パケットの Authnode フィールドを参照する．参照した際，自身が探索パケットの発信元であり中継ノードではない場合，ノードはその探索パケットを無視する．一方，自身が探索パケットの発信元ではなく中継ノードである場合，ノードは中継ノードとしての役割を果たす．また，自身が探索パケットの発信元でありかつ中継ノードである場合は，中継ノードとしての役割を果たす．また，自身が発信元でも中継ノードでもない場合，そのノードは信頼の輪の構築に参加する必要がないため，探索パケットを無視する．

(a) 被認証ノードの動作

探索パケットを受信した被認証ノードは，探索パケットの最終被認証ノードフィールドが自身でない場合，パケットに自身の証明書を付加し，ルーティングテーブル情報の部分を自身が信頼するノードのルーティングテーブル情報に書き換え，さらに探索パケットをブロードキャストする．被認証ノードのうち，自身が信頼するノードに最終被認証ノードが存在するノードは，パケットに自身の証明書を付加し，最終被認証ノードに探索パケットをユニキャストする．

図 4(2) において，探索パケットを受信した被認証ノード 5 は，自身の信頼するノードがノード 6 であることから図 3(2) のように探索パケット情報を書き換え，ノード 1 と同様に探索パケットをブロードキャストする．

(b) 中継ノードの動作

探索パケットを受信したルーティングテーブル情報の nexthop にあたるノードは，パケットのルーティングテーブル情報を自身が中継する被認証ノードのルーティングテーブル情報に書き換え，さらに探索パケットをブロードキャストする．

図 4(3) において，探索パケットを受信したルーティングテーブル情報の nexthop にあたるノード 6 は，自身が被認証ノード 2 の中継ノードであると認識し，図 3(3) のように自身のルーティングテーブルのノード 2 に対応する部分を付加し，ノード 1 と同様に探索パケットをブロードキャストする．これにより，認証ノード 1 の電波範囲外に存在するノード 1 の被認証ノード 2 にも，探索パケットを届けることが可能になる．ノード 2 は，ノード 5 と同様に被認証ノードとしての動作を行う．

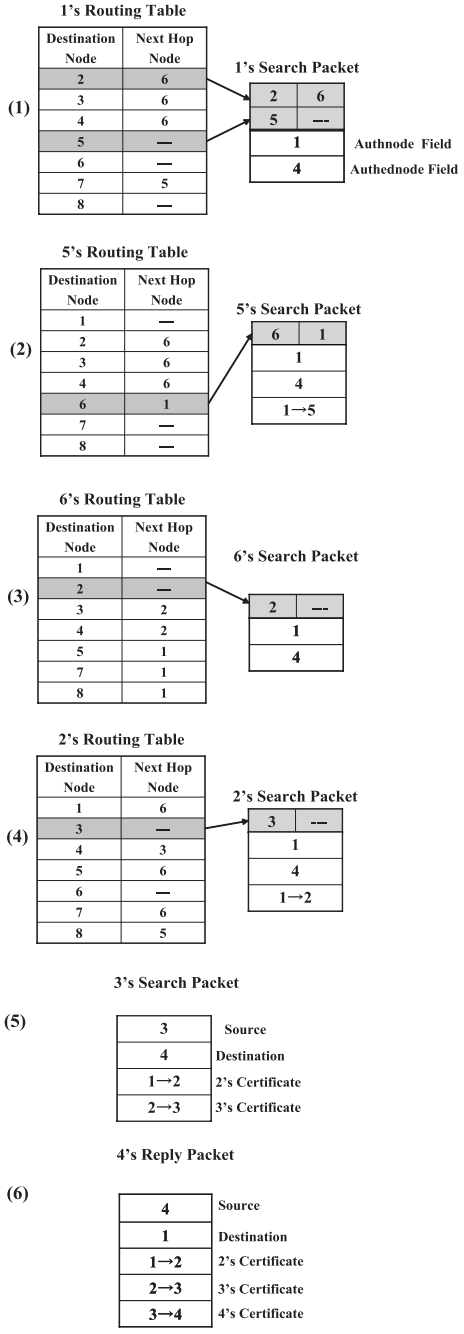

図 3　提案方式における探索パケットの内容およびルーティングテーブル内容

Fig. 3　Content of a search packet and a routing table.

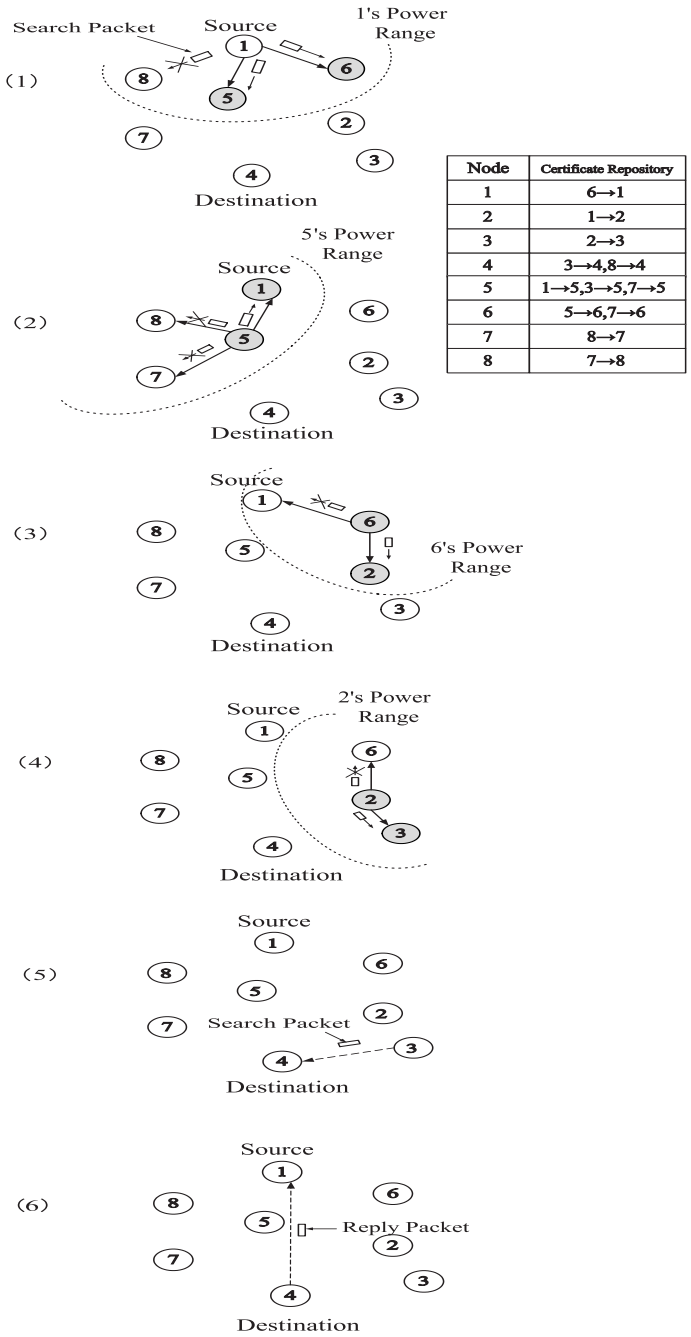

図 4　提案方式における認証方法

Fig. 4　Authentication in the proposed system.

ASNS において，自身が信頼するノードが既に探索を行っていた場合，証明書の探索を繰り返す冗長な処理となる．また，最終被認証ノードを発見できない場合，無限に探索を行ってしまう危険性がある．そこで，ASNS では，証明書の探索を繰り返さないため

に，ノードが探索パケットを受信した際，自身が被認証ノードならば二回目以降の探索パケットは棄却する．一方，自身が中継ノードである場合は，信頼の輪の構築関係に関わることは一切せず，二回目以降も探索パケットを棄却することなく，中継ノードとしての役割を果たす．これにより，ASNS は，無駄な探索を行う必要がない．そのため，提案方式では，同じノードの信頼関係において繰り返し探索パケットが転送されることはない．さらに，最終被認証ノードが見つからない場合でも，無限に探索を行わずに探索を収束させることが可能になる．

3.2.5 復路構築

最終被認証ノードは，信頼の輪に関わったノードの全証明書が付加されている返信パケットを認証ノードに返信する．この際，ノード 3 は，最終被認証ノード 4 に対し証明書を発行しているため，最終被認証ノード 4 に自身の証明書を付加した探索パケット (図 3(5)) を図 4(5) のようにユニキャストする．図 4(6) において最終被認証ノード 4 は，ノード 3 が送信した探索パケットを参照し，自身が最終被認証ノードであるため，自身の証明書を付加し，図 3(6) のように 1 → 2，2 → 3 および 3 → 4 の証明書が付加された返信パケットを認証ノード 1 にユニキャストで返信する．認証ノード 1 はこの返信パケットの情報から，信頼の輪を構築するために必要な全証明書を獲得することができる．

3.2.6 信頼の輪が成立しない場合の最終被認証ノードおよび認証ノードの処理

提案方式において，ノードの信頼関係によっては信頼の輪が成立せず，認証が成り立たない場合がある．また，ネットワークにおけるノードの陳腐化や輻輳により被認証ノードに探索パケットが届かず，信頼の輪を構築できない場合がある．そのため，提案方式では信頼の輪の構築処理にタイムアウトを設ける．例えばタイムアウトの値として，ネットワークにおける最大ホップ数を 10 ホップ，各中継ノードおよび被認証ノードでの最大処理時間を 0.2 秒と考え，余裕をもってタイムアウトの値を 3 秒とする．認証ノードは，信頼の輪を構築し始めてから 3 秒たっても最終被認証ノードから応答がない場合，リトライを行うことにする．リトライでは信頼の輪を構築する際の動作を繰り返す．Proactive 型の代表である TBRPF では，隣接ノード同士でパケットを交換しあう間隔が 5 秒と規定されていることから [15]，例えばリトライを 2 回繰り返す場合には，その間にルーティグテーブルの情報が更新され，信頼の輪構築が成功する可能性が高くなる．また，信頼の輪は複数本存在する可能性があり，どれか一本が回復すれば認証が成功する．認証ノードは，リトライをしても返信パケットを受信しなかった場合，認証不成立とみなす．

提案方式では，信頼の輪はどれか一つが繋がればよいため，最終被認証ノードは最初に受信した探索パケットに対してのみ，認証ノードに対して返信パケットを送信し，それ以降に受信する他の探索パケットを無視する．また，認証ノードに返信パケットが届かず，認証ノードがリトライした場合を考慮し，最終被認証ノードにもタイムアウトを設ける．タイムアウトの値を最終被認証ノードが最初に探索パケットを受信してから 3 秒とする．タイムアウトになった場合，最終被認証ノードは信頼の輪の処理を完了する．信頼の輪が成立しない場合，最終被認証ノードは探索パケットを受信することがないため，何も行わない．

3.3 信頼の輪の確認

認証ノード 1 は信頼の輪を構築するノードの公開鍵の正当性を確認する必要がある．確認方法は 2.3 と同様である．ここで，証明書の有効性の確認については，信頼の輪の構築をオンデマンドで実施しているため，その時点での有効な証明書のみを獲得しており，失効証明書リストの確認処理が不要になる．これにより，インターネットに接続点を持たず独立した無線アドホックネットワークにおいて，CA により発行された失効証明書リストを確認できずとも確実にノード同士の認証を行うことが可能になる．さらに，ノードは，信頼していたノードを信頼しなくなる場合，信頼の輪の構築に参加しない．つまり，無効な証明書が存在する場合，一つ手前のノードが信頼の輪の構築に参加しないことで，有効な証明書のみを集めることができる．このことより，提案方式は，証明書の有効性が頻繁に更新されるようなアドホックネットワーク環境に有利である．

提案方式では，オンデマンドでその都度信頼の輪を構築するため認証が成功後収集した証明書は，不要になり次第削除する．

4. 特性評価

4.1 従来方式と提案方式の処理の比較

表 1 に従来方式と提案方式の処理の比較を示す．全証明書を収集するためにリポジトリ交換を定期的に行う従来方式に比べて，提案方式は信頼の輪に必要な証明書をオンデマンドで収集するため，リポジトリ交換が不要になる．ネットワーク内の全公開鍵証明書数を X 枚，ノード数を N とした場合，従来方式は定常状態において各ノードは最大 X 枚格納するのに対し，提案方式は平均 X/N 枚格納すればよい．つまり提案方式では，ノード数が増加しても保持すべき証明書数は自身に発行された証明書だけでよいので，消費するメモリ量を削減できる．また，失効証明書リストを定期的に更新するための管理が必要な従来方式に比べて，提案方式は認証要求が発生した時点の証明書を獲得することで有効な証明書のみを集めることになり，失効証明書リストの管理が不要になる．しかしながら，提案方式は，探索パケットに被認証ノードに対応するルーティング情報を付加しているため，信頼の輪の構築とルーティングが従属しており，ノードの陳腐化により，期待する被認証ノードに探索パケットがうまく届かず，信頼の輪が構築できないことがある．さらに，ある程度時間が経てば多くの証明書情報を収集できる従来方式に比べて，オンデマンドで信頼の輪を構築する提案方式の場合は，ノードの陳腐化率に左右されるため，信頼の輪の構築成功率が低くなる．また，従来方式は全ての証明書を収集できた状態では信頼の輪を短時間で探索できるのに対して，提案方式は必要になった時点で証明書情報を収集して信頼の輪を構築するため，収集に時間がかかるという欠点もある．

表 1　従来方式と提案方式の処理の比較
Table 1　Comparison of the conventional system and our proposed system.

評価項目	従来方式	提案方式
全証明書の事前収集	必要	不要
証明書収集方法	定期収集	オンデマンド
認証のためのメモリ量	全証明書保持 X 枚分	自身の証明書のみ保持 X/N 枚分
失効証明書リストの管理	必要	不要
ルーティングプロトコルに依存	しない	する

4.2 提案方式の基本特性

信頼の輪を構築するときの基本特性として，信頼の輪の構築成功率および信頼の輪を構築するために必要なノード数について，計算機シミュレーションにより評価する．このときの条件として，各ノードは他ノードに対して公開鍵証明書を最低 1 枚発行し，自身の公開鍵に対しては他ノードから最低 1 枚発行されることにする．さらに，認証ノードと被認証ノードを無作為に 2 ノード選択し，信頼の輪を構築する試行を 10000 回繰り返す．ここで，1 ノードあたりの信頼ノード数は一様分布とする．また，下位レイヤでのルーティングプロトコルは，ノードの陳腐化や輻輳によるパケット棄却は起こらず，完全に動作すると仮定する．以降の評価においては，図 10 を除いてノードの陳腐化率は 0 とする．

4.2.1 信頼の輪の構築成功率

図 5 に，1 ノードあたりの平均信頼ノード数に対する信頼の輪の構築成功率を示す．図より，ノード数が 100 の場合においても，1 ノードが少なくとも平均 4 ノード信頼することで確実に信頼の輪を構築できることがわかる．これより，以後の計算機シミュレーションは 1 ノードが平均 4 ノード信頼するシステムを想定する．

4.2.2 信頼の輪の平均パス長

図 6 に，1 ノードあたりの平均信頼ノード数に対する信頼の輪の平均パス長を示す．ここで，パス長とは，信頼の輪を構築するノードを結ぶリンク数を示す．また，平均パス長とは，すべての認証ノードと最終被認証ノードのペアの信頼の輪のうち，最短のパス長の平均を取ったものとする．提案方式では，探索パケットに制限ホップ数フィールドを設けなくても，各ノード

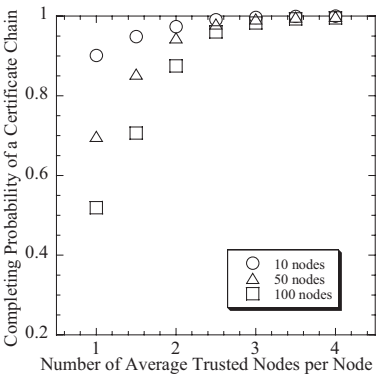

図 5　信頼の輪の構築成功率
Fig. 5　Completing probability of a certificate chain.

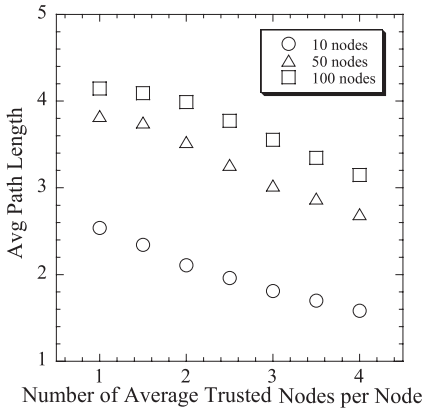

図 6　信頼の輪の平均パス長
Fig. 6　Average path length.

が他ノードに対して公開鍵証明書を最低 1 枚発行し，自身の公開鍵に対しては他ノードから最低 1 枚発行されるという条件下においては，信頼の輪の構築成功率が 1 となる平均信頼ノード数は 4 であり，平均すると 4 ノード以下で信頼の輪が繋がることがわかる．

4.3　通 信 量

ここでは，提案方式における通信量を評価する．通信量を評価するにあたり，まず始めにアドホックネットワークの基本特性である通信成功確率および平均ホップ数を評価する．

4.3.1　通信量評価におけるシミュレーション条件

提案方式において一回の認証でネットワーク上に流れる総パケット数を通信量と定義する．この際，復路構築の際に発生する通信量は，ユニキャストの 1 パケットのみでありネットワークに与える影響が少ないため，シミュレーションには含めないことにする．また，ノードの物理的配置を考慮した場合の一つの送信ノードから受信ノードまでのホップ数を平均したものを平均ホップ数と定義する．ただし，認証ノードが送信した探索パケットが宛先ノードに達するまでに経由したノード数に，認証ノードの分として 1 を足した値をホップ数と定義する．すなわち，認証ノードの電波範囲内に存在するノードに到達するためのホップ数は 1，中継ノードを 1 台中継した場合のホップ数は 2 となる．平均ホップ数は，あるノードから被認証ノードまでのホップ数の平均とする．表 2 にシミュレーション諸元を示す．通信成功確率特性，平均ホップ数特性の評価においては，ノードをランダムに配置することを 10000 回繰り返し，その平均値を用いる．

4.3.2　通信成功確率および平均ホップ数

図 7 に通信成功確率を示す．この際，横軸は，シミュレーション領域の各辺の長さを示す．例えば，横軸 100m の場合，100m × 100m 四方のシミュレーション領域中に，該当するノード数が存在することを意味する．図より，シミュレーション領域が広く，かつノード数が少ない場合には，通信成功確率が低下することがわかる．通信成功確率が低いと無線アドホックネットワーク自体が成り立たない．これは提案方式に限らず，proactive 型ルーティングプロトコルを用いた場合の無線アドホックネットワークの特性といえる．よって，以下の評価では各ノードにおいて通信成功確率が 0.9 以上のシミュレーション領域について検討する．具体的には，20 ノードではシミュレーション領域の一辺が 300m 以下，40 ノードでは 400m 以下，60 ノードでは 500m 以下，100 ノードでは 600m 以下がシステムが成り立つ範囲である．
次に，平均ホップ数を図 8 に示す．プロットが途中で途絶えているのは，上述のシミュレーション領域のプロットしか記載していないためである．図よりシステムが成り立つ領域ではノード数が平均ホップ数にあまり影響を与えていないが，ノード数が多い程ホップ数も少なくなり，トラヒック的に有利であることがわかる．これは，ノード数が多い方がより適切な位置にある中継ノードを選択できる可能性が高くなるためである．また，図より平均ホップ数はシミュレーション領域に比例に近い関係にあることがわかる．これは無線アドホックネットワーク全体の特性である．

4.3.3　平均通信量

1 ノードが認証を行う際に発生する総パケット数である通信量 Ts の評価式を以下に示す．

$$Ts = \{1 + m \times (n-1)\} \times (N-1) \qquad (1)$$

ここで N はアドホックネットワーク内の全ノード数であり，m は 1 ノードあたりの信頼ノード数，n は平均ホップ数である．ASNS プロトコルは，探索パケットを受信した各ノードは自身が信頼している全ノードを探索するため，通信量は 1 ノードの信頼ノード数と平均ホップ数を掛け合わせた値となる．ここで，平均

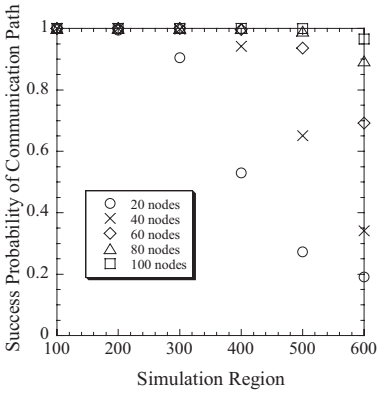

図 7　通信成功確率
Fig. 7　Success probability of communication path.

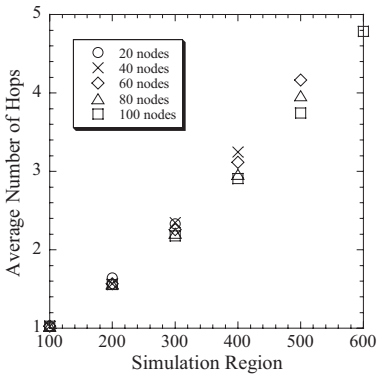

図 8　平均ホップ数
Fig. 8　Average number of hops.

ホップ数はノードの物理的配置を考慮したものであり，探索パケットを転送した中継ノードも 1 ホップとしてカウントする．1 ノードあたりの信頼ノード数 m と平均ホップ数 n を掛け合わせたものを探索パケットが中継ノードを経由するために生じる通信量と定義することで，中継ノードを経由するために生じる通信量も含んだものとなっている．この際，各ノードはブロードキャストを行うため，1 ホップ目の全中継ノードには，1 回のブロードキャストで探索パケットを届けることができる．そのため，掛け合わせる際の平均ホップ数から 1 を引いている．掛け合わせた結果に足す 1 がブロードキャストパケットに相当する．また，式 (1) において，1+m × (n-1) は，一つのノードが自身の全被認証ノードまで探索パケットを到達させるために発生する通信量となる．ここで，探索パケットがあるノードからある被認証ノードに届く間の中継ノード数は，平均ホップ数と仮定する．アドホックネットワーク全体において発生する通信量は，全ノードから最終被認証ノードを引いたノード数 (N-1) を掛け合わせることで求めることができる．本論文では，各ノードが既に持っているルーティングテーブル情報を参照して効率的に信頼の輪を構築する手法を提案しており，ルーティングテーブルの更新のための通信と信頼の輪の構築のための通信を独立して取り扱っている．このため，信頼の輪の構築成功率を高めるために，ルーティングテーブルを頻繁に更新する制御は行っておらず，本論文で評価している通信量にはルーティングテーブルの更新のための通信は含まれていない．

図 9 に平均通信量を示す．図より，アドホックネットワークシステムが成り立つ範囲内ではノード数の少ない程探索に関わるパケットが少なくてすむことがわかる．また，ノード数が多い場合においては，探索に関わる通信量も増加する．これらのことから，提案方式は，ノード密度の低いアドホックネットワーク環境に有利である．

4.3.4　従来方式と提案方式の平均通信量の比較

従来方式では，収集したネットワーク内の全証明書のうち，信頼の輪の構築において使用頻度が高く有効性の確認が必要な証明書を特定証明書と呼ぶ．各ノードは，特定証明書を発行したノードに対して，ユニキャストで定期的に有効性を確認する．この処理を「特定証明書のアップデート」と呼ぶ．従来方式は，定期的にリポジトリ交換するための通信および特定の証明書をアップデートするための通信が発生する．一方，提案方式は，オンデマンドで信頼の輪を構築するため

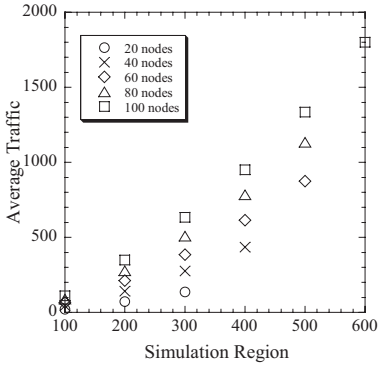

図 9　平均通信量
Fig. 9　Average traffic.

定期的な通信は発生せず，一回の認証において図 9 のような通信量が発生する．

従来方式において，アドホックネットワーク内ノード数を 100，リポジトリ交換と特定証明書のアップデートは同時に行われると仮定する．例として，リポジトリ交換と特定証明書のアップデートの間隔が 1 分および特定証明書が 4 枚の場合の従来方式の通信量は約 900/分（リポジトリ交換により発生する通信量は，全ノードがブロードキャストでパケットを 1 つずつ送信するため，100/分となる．また，アップデートにより発生する通信量は，ユニキャストで特定証明書の発行者に対して有効性を確認するために発生するパケットとその返信のために発生するパケットが存在するため，100 × 4 × 2=800/分となる.），間隔が 2 分および特定証明書が 4 枚の場合の通信量は約 450/分 (間隔が 1 分の通信量の半分) となる．また，間隔が 1 分で特定証明書の枚数が 8 枚の場合の通信量は約 1700/分，間隔が 2 分で特定証明書の枚数が 8 枚の場合の通信量は約 850/分となる．この際，従来方式におけるパケットサイズは提案方式と同じと仮定する．一方，提案方式の平均通信量は，図 9 より，例として，ノード数 100 の場合，シミュレーション領域の一辺が 350m では約 850，一辺が 600m では約 1800 であることがわかる．そのため，一辺が 350m では，30 秒に一回ノード認証要求が発生すると，平均通信量として，間隔が 1 分および特定証明書の枚数が 8 の場合の従来方式と同等になる．

従来方式における通信量は，特定証明書の枚数およびリポジトリ交換と特定証明書のアップデートの間隔に依存する．一方，提案方式は認証要求の発生間隔に依存する．つまり，従来方式は，特定証明書の枚数が少なく，リポジトリ交換およびアップデートの間隔が長い場合に有利であり，提案方式は，認証要求の発生間隔が長い場合に有利である．

4.4 ノードが陳腐化した場合における信頼の輪の構築成功率

陳腐化とは，ルーティングテーブルの情報が古く，誤った経路情報を保持している状態を意味する．本論文ではあるノードのエントリのうち一部でも誤りがある場合，そのノードを陳腐化したノードと見なす．本シミュレーションでは，全ノードに対する陳腐化したノードの割合をノードの陳腐化率と呼ぶ．そして，提案方式のノードが陳腐化した場合における信頼の輪の構築成功率に関して評価を行う．図 10 に，ノードの陳腐化率に対する信頼の輪の構築成功率を示す．陳腐化する可能性のあるノードとしては，中継ノードと被認証ノードを含む．アドホックネットワーク内の全ノード数を 100 とする．図より，ノードの陳腐化率が 0.3 以下であれば，信頼の輪の構築成功率がほぼ 1 となることがわかる．ここで [15] では，各ノードのルーティングテーブル更新間隔として 5 秒が例示されており，ノードの移動特性にも依存するが，5 秒間に陳腐化してしまうノードの割合が 0.3 を超える場合は極めて小さいと考えられるため，ノードの陳腐化率に対する信頼の輪の構築成功率については妥当な特性が得られていると見なすことができる．これは，信頼の輪が複数本存在する可能性があるためである．シミュレーション領域が大きいほど，構築成功率が下がるが，これは，平均ホップ数が大きくなるため，中継ノードの陳腐化による影響が大きくなるためである．

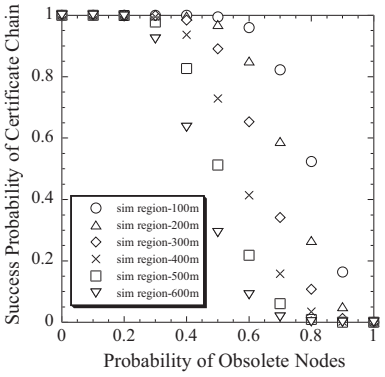

図 10　ノードが陳腐化した場合の信頼の輪の構築成功率
Fig. 10　Success probability of certificate chain in case of obsolete nodes.

5. 結　　論

本論文では，インターネットに接続点をもたない独立した無線アドホックネットワークにおいて，各ノードは自分に対して発行された証明書のみを持っておき，認証要求が発生した時点で，認証したいノードまでの証明書を収集して信頼の輪を構築するオンデマンド公開鍵証明書分散管理方式を提案した．証明書の収集には，被認証ノードに関わるアドホックネットワークのルーティングテーブル情報を付加してブロードキャストすることで，信頼の輪に加わる複数の被認証ノードを一括して探索するアドホック一括ノード探索プロト

コル (ASNS:Adhoc Simultaneous Nodes Search) を提案した．提案方式は，認証に必要な証明書のみを，要求が発生した時点で収集するため，ノードのメモリ消費量を削減でき，かつ失効証明書リストの確認処理が不要になる．これにより，インターネットに接続点を持たない独立した無線アドホックネットワークにおいても，確実にノード同士の認証を行うことができる．計算機シミュレーションにより，提案方式に関する基本特性として，信頼の輪の構築成功率および信頼の輪を構築するために必要なノード数について評価を行い，各ノードが他ノードに対して公開鍵証明書を最低 1 枚発行し，自身の公開鍵に対しては他ノードから最低 1 枚発行されるという条件下においては，1 ノードあたり約 4 ノードの証明書を発行しあうことで，信頼の輪を高い確率で構築できることを確認した．このときの信頼の輪の構築に必要な証明書数は 3 つから 4 つ程度であり，少ない数で構築できている．また，信頼の輪の構築に必要な通信量についても評価を行い，特にノード密度の低いアドホックネットワーク環境に有利であることを確認した．提案方式は，下位レイヤのルーティングプロトコルに従属している．そこで，ルーティングプロトコルの動作に直接依存しないものの，ノードの移動性に対する影響を考察できるように，ノードの移動に起因するノードの陳腐化率を変化させた特性評価を行った．

6. 謝　　辞

本研究は，文部科学省 COE「アクセス網高度化光電子デバイス」プログラム，及び KDDI との共同研究によって行われた．関係者各位に深謝する．

文　　献

[1] IETF, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,” RFC3280, April 2002.
[2] IETF, “RFC 3281 An Internet Attribute Certificate Profile for Authorization,” April 2002.
[3] S.Corson and J.Macker, “Mobile ad hoc networking(MANET): Routing protocl performance issues and evaluation consideration,” IETF RFC25010,Jan,1999.
[4] Mobile Ad-hoc Networks(manet)Charter, http://www.ietf.org/html.charters/manet-charter.html.
[5] C.E. Perkins, *Ad Hoc Networking*. Addison Wesley Professional, Dec. 2000.
[6] J.Jubin and J.D. Turnow, “The DARPA Packet Radio Project,” *Proc.IEEE*, 1987, vol,75,pp.21-32,Jan.
[7] 間瀬憲一，中野敬介，仙石正和，篠田庄司，“アドホックネットワーク,”，vol.84, no.2, pp.127-134, Feb.2001 電子情報通信学会誌.
[8] Srdjan Capkun,Levente Buttyan,and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Moblie Ad Hoc Networks,” IEEE Transactions on MOBILE COMPUTING,vol.2,No.2,JANUARY-MARCH 2003,p52-64.
[9] “ITU-T Recommendation X.509: Information Technology - Open Systems Interconnection- The Directory: Public-Key and Attribute Certificate Frameworks,” ITU-T, March 2000.
[10] R.Housley, W.Ford, W.Polk, D.Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” RFC-2459, January 1999.
[11] C.E.Perkins and P.Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” Comput.Commun.Rev, pp.234-244,1994.
[12] S.Murthy and J.J.Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks,” ACM MONET Journal, pp.183-197,1996.
[13] C.-C. Chiang, H.-K. Wu, W.Liu, and M.Gerla, “Routing in clustered mutihop, mobile wireless networks with fading channel,” Proceedings of IEEE SIngapore International Conference on Networks(SICON’97),1997 Apr, pp.197-211.
[14] P.Jacquet, P. Muhlethaler, A.Qayyum, A. Laouiti, L.Viennot, and T.Clausen, “Optimized link state routing protocol,” Internet-draft, draft-ietf-manet-olsr-02.txt,2000.
[15] R.Ogier, “Topology Dissemination Based on Reverse-Path Forwarding(TBRPF),” IETFRFC 3684.

（平成 xx 年 xx 月 xx 日受付）

北田　夕子　（学生員）

平 16 慶大・理工・情報卒．現在，同大大学院修士課程在学中．主として，インターネットセキュリティに関する研究に従事．

荒川　　豊　（学生員）

平 13 慶大・理工・情報卒．平 15 同大大学院修士課程了．現在，慶大大学院博士課程在学中．主として，通信ネットワーク及びインターネットセキュリティに関する研究に従事．IEEE，情報処理学会各会員．

竹森　敬祐　（正員）

平 6 慶大・理工・電気卒．平 8 同大大学院修士課程了，同年 KDD(株) 入社．平 16 同大大学院博士課程了，現在に至る．主として，通信ネットワーク及びインターネットセキュリティに関する研究に従事．平 14 年度本会学術奨励賞受賞．情報処理学会各会員．

渡邊　　晃　（正員）

昭 49 慶大・理工・電気卒．昭 51 同大大学院修士課程了，同年三菱電機 (株) コンピュータ製作所入社後，LAN システムの開発・設計に従事．平 3 同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティなどの研究に従事．工博．平 14 名城大学理工学部教授．IEEE，情報処理学会各会員．

笹瀬　　巌　（正員）

昭 54 慶大・工・電気卒．昭 59 同大大学院博士課程了．同年オタワ大・理工・電気・ポストドクトラルフェロー，昭 60 同大学講師．昭 61 慶大・理工・電気助手，昭 63 同大専任講師，平 4 同助教授，平 11 同大・理工・情報・教授，現在に至る．主として，ディジタル通信，通信ネットワーク，光通信理論，マイクロ波通信，非線形通信システム，通信理論，符号理論，インターネットセキュリティに関する研究に従事．工博．昭 59 年度 IEEE COM．SOC．学生論文賞．昭 62 年第 3 回井上研究奨励賞受賞，昭 63 第 1 回安藤博記学術奨励賞，昭 63 篠原記念学術奨励賞，平 8 年度本会交換システム研究会優秀論文賞受賞．IEEE Senior Member，情報理論とその応用学会，情報処理学会各会員．

Abstract In this paper, we propose on-demand distributed public-key management to construct a public-key infrastructure for wireless ad hoc networks not connected to the Internet. The proposed system collects certificates of certificate chains only when a node wants to authenticate the others. Each node holds in her local repository only the certificates issued to herself. To collect certificates for certificate chain efficiently, we propose Adhoc Simultaneous Nodes Search protocol, which can search chained nodes using broadcast packets and the contents of routing tables. The proposed system can reduce node's memory size, shorten the initial convergence time, and also it does not need certificate revocation list for authentication. With a computer simulation, we show basic characteristics of success probability of certificate chains and average shortest path length for the system. Also we show overall traffic when the node collects certificates, and show an advantage condition for the proposed system.

Key words Wireless ad hoc network Public Key Infrastructure Certificate Path Distributed management