情報処理学会研究報告
IPSJ SIG Technical Report

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

無線アドホックネットワークにおける属性証明書を用いた通信経路の信頼度評価法

井上　慎一郎[†1,†2]　菅谷　直史[†1]　石井　方邦[†1]
谷田貝　健[†1]　笹瀬　巌[†1]

概要：無線アドホックネットワーク (MANET : Mobile Ad-Hoc Network) は，ネットワークを管理する第三者機関の設置は期待できないために，意図的にパケット内容を改ざんしたり，パケットの転送を行わなかったりする悪意あるノードが存在する可能性がある．MANET には基地局等のインフラがなくマルチホップ通信を行う必要があるため，上記のような悪意あるノードが中継ノードとなることは十分に考えられ，よって通信経路の信頼性の評価が重要となる．このような課題に対して，ノードの信頼度をもとに通信経路を評価する方式が提案されているが，信頼度の改ざんや，他のノードへのなりすましという問題には対処できていない．そこで本論文では，公開鍵証明書に付随する属性証明書を用いた通信経路の信頼度評価法を提案する．ノードの信頼度を属性証明書を用いて共有することで，改ざん検知となりすまし検知が可能となり，また経路作成を担う送信者は中継ノード候補から属性証明書の回収を行うことで，通信経路の評価を行う．最後に，証明書の検証成功率を評価することで，本提案方式の有効性を示す．

Trust Level Evaluation for Communication Paths in MANETs Using Attribute Certificate

Shinichiro Inoue,[†1,†2] Naofumi Sugaya,[†1]
Masakuni Ishii,[†1] Takeshi Yatagai[†1]
and Iwao Sasase [†1]

Since Mobile Ad hoc NETwork(MANET) is a distributed and self-organized network which closely depends on cooperation among mobile nodes, it needs to be considered the existence of malicious nodes that intentionally modify data of packets or do not forward packets. Recently, due to evade those malicious nodes in communication routes, a number of trust-based secure routing protocols have been proposed. However, two problems are remained in trust sharing or reporting phase in these schemes. One problem is that trust itself might be modified. The other problem is that a node might impersonate other nodes. In this paper, we propose a scheme to evaluate trust level of communication paths in MANETs using Attribute Certificate(ACs). By using ACs, it enables to detect if trust has been modified, and if a node has impersonated other nodes. Moreover, our proposed scheme is able to not only increase security level, but also share trust effectively using ACs in a witty way.

1. はじめに

近年，ユビキタス社会を支える技術として，ノード同士が協調し合い自立分散的に柔軟なネットワークを構築する無線アドホックネットワーク (MANET: Mobile Ad-Hoc Network) が注目されている 1)．自律分散制御に基づく MANET は，拡張性や耐障害性に優れ，例えばノード数が常時変化している場合においてもネットワークの維持が可能であり，また，中継ノードとして選択されていたノードが電力不足等で使用できなくなる場合においても，他のノードが新たな中継ノードとなることにより通信の再開が可能である，といった特徴を持つ．これらの特徴を生かし，MANET は基地局等のインフラがない災害現場やイベント会場において，ノード同士が即興でネットワークを構築し，情報の収集や管理を行う，といった使用方法が期待されている．

MANET は不特定多数のノードによって構成され，さらにネットワークの管理を行う第三者機関の設置は期待できない．よって，そのような MANET において通信を行う場合，まず考えられる課題は，通信相手ノードは本当に自身が想定している相手ノードであるのかどうかである．ノードは他のノードに容易になりすますことが可能であり，想定していない相手ノードと通信をしてしまうことも十分に考えられる．そこで，このような課題に対して，MANET において相手ノード認証を行う方式が提案されている 2)．2) は MANET における公開鍵分散管理方式であり，各ノードが独自に公開鍵証明書を発行して，その管理を行い，信頼の輪を構築することで相手ノード認証を行う方式である．2) を用いることで，想定する相手ノードの正当な公開鍵を入手することができ，公開鍵暗号通信が可能となるため，想定している相手ノードとのみ情報のやり取りを行うことができる．

しかしながら，基地局等のインフラを持たない自律分散型ネットワークである MANET

†1 慶應義塾大学理工学部情報工学科
†2 inoue@sasase.ics.keio.ac.jp

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

において，電波範囲外にいる相手ノードと通信を行う場合は，他のノードが中継ノードとなることによって可能となるマルチホップ通信を行う必要がある．様々なノードが中継ノードとなるマルチホップ通信において課題となるのが，通信経路に対する信頼性である．不特定多数のノードが参加する MANET において，ネットワークを混乱させるために，パケット内容の改ざんを意図的に行うノードや，電力消費を抑制するために，受信したパケットの転送を行わないといった悪意あるノードが存在し，このようなノードが中継ノードとなる場合もあると考えられる．これらのノードはネットワーク内に誤った情報をもたらし，またスループットの大幅な低下といった問題を引き起こす可能性がある．よって，MANET において送信者と受信者間に提供される経路がどの程度信頼のおける経路であるのかどうかの検証として，通信経路の信頼度評価を行う必要がある．近年，このような課題に対して，各ノードがパケットを改ざんすることなく、正しく転送していることを示す指標として信頼度を導入し，各ノードの信頼度にもとづき，通信経路全体の信頼度の評価を行うことで，上記のような悪意あるノードを回避する方式が提案されている 3)4)．3)4) では，初めに，各ノードは，自身の電波範囲内に存在する近隣ノードがパケット内容を改ざんすることなく転送を行っているかどうか，また転送すべきパケットをドロップしていないかどうか，という通信における振る舞いを監視し，その近隣ノードに対して信頼度を算出する．そして，通信要求が生じた場合，各ノードの信頼度をノード間で共有し，信頼度の高いノードや通信経路を選択することで信頼度の低い悪意あるノードを回避している．

従来，2) のような相手ノード認証に関する研究と，3)4) のような通信経路の信頼性に関する研究はそれぞれ個別に取り扱われており，そのため 3)4) においては 2) で提案されている MANET における公開鍵分散管理方式を用いていない．よって，3)4) は以下にあげる 2 つの問題には対処できていないと考えられる．1 つ目の問題は，ネットワーク内における信頼度の改ざんに対する問題である．悪意あるノードが存在する MANET において，パケット内に記載された信頼度の値そのものの改ざんは容易に考えられる攻撃であり，この攻撃に対して信頼度が改ざんされたかどうかを確かめる改ざん検知の仕組みが必要となる．2 つ目の問題は，他のノードへのなりすましである．ノードの信頼度にもとづき通信経路を評価した上で，実際に用いる経路を決定しているのであるが，悪意あるノードが他のノードになりすまし，自身にとって都合の良い信頼度を通知することが可能である．よって，その問題に対処するために，なりすまし検知の仕組みが必要となる．

そこで本論文では，上記の 2 つの問題を解決するために，2) で提案されている方式を 3)4) の方式に取り入れた新たな通信経路の信頼度評価法の検討を行う．本方式は，ノードの動作を明確にするために，通信要求が生じていない場合のオフライン状態と，通信要求が生じている場合のオンライン状態の 2 つの状態に分ける．まず，オフライン状態においてノードは，従来方式と同様に近隣ノードに対して信頼度を算出した後、信頼度を記入した属性証明書をその近隣ノードに発行する．一方，属性証明書を発行されたノードは，その属性証明書を収集，保持したままネットワーク内を移動する．そしてオンライン状態では，経路作成を担うノードは通信相手までの経路を複数取得しつつ各ノードから属性証明書を回収し，各属性証明書の検証を経て，最終的に通信経路の信頼度の評価と経路の選択を行う．また，証明書の検証成功率を評価することで，本提案方式の有効性を示す．

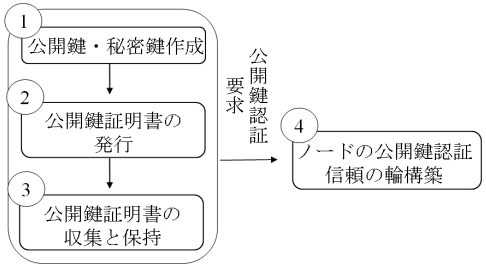

図 1 MANET における公開鍵分散管理方式 2)

以降，2 章では MANET において他ノードの公開鍵の認証を行う公開鍵分散管理方式ついて説明する．3 章では信頼度共有を行う従来方式を取り上げ，その問題点についてまとめる．そして，4 章では提案方式について述べる．5 章では提案方式の評価を行い，最後に，6 章で本稿をまとめる．

2. MANET における公開鍵分散管理方式 2)

本章では，MANET における公開鍵分散管理方式 2) についての概要を説明する．2) は，CA(Certificate Authority) のような信頼のおける第三者機関の設置が困難である MANET において，各ノードの公開鍵を分散管理し，さらに他のノードの公開鍵認証を行う方式である．この方式により，MANET 内において見ず知らずのノードの公開鍵の正当性を保証することができ，そのため，通信相手ノードの認証が可能となる．図 1 に方式 2) の流れを示す．以下，図 1 を用い，公開鍵作成から，他のノードの公開鍵認証に至るまでの概要を述べる．

1. 各ノードは自身で公開鍵と秘密鍵の作成を行う．

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

2. 各ノードは自身の知識や経験に基づき，信頼できるノードの公開鍵に対して公開鍵証明書を発行する．以降，ノード A がノード B に対して発行する公開鍵証明書を A → B と表記する．

3. 各ノードは自身に対して発行された公開鍵証明書のみを保持する．

4. 各ノードは自身に対して発行された公開鍵証明書のみ保持しているため，認証要求が生じた時点でネットワーク内から信頼の輪構築のために必要な公開鍵証明書の収集を行い，認証ノードから被認証ノードまで信頼の輪を構築することで公開鍵認証を行う．ここで，信頼の輪とは，見ず知らずの相手の認証を行うために，信頼できる第 3 者を利用するものであり，例えばノード A はノード B の公開鍵に対して公開鍵証明書を発行し，ノード B はノード C の公開鍵に対して公開鍵証明書を発行している場合，A → B → C と繋がり，結果ノード A はノード C の公開鍵の正当性を間接的に確認することが可能である，というものである．もし，認証ノードから被認証ノードまでこのような信頼の輪が構築できた場合，認証ノードは被認証ノードの公開鍵の正当性を保証できたと言える．

以上が公開鍵分散管理方式の概要であり，信頼の輪を構築することで，MANET 内において見ず知らずのノードの公開鍵の正当性を保証することが可能となる．

3. 通信経路評価法の関連研究

本章では，通信経路の信頼度を評価するために信頼度を共有する方式 3)4) について述べる．3) は近隣ノードに対して算出した信頼度を RREQ(Route REQest) パケットを用いてネットワーク内に広めていく方式であり，AODV を応用した方式である．一方 4) は近隣ノードではないノードの信頼度を取得するための方式を提案しており，信頼度共有のためだけに特別なパケットである TREQ(Trust Request) を用いて行われる．以下，各方式について述べ，3.3 でこれらの方式における問題点についてまとめる．

3.1 AODV-REX(AODV-Reputation EXtention) 3)

一般的な AODV では，送信者は受信者までの経路作成のために，RREQ パケットのフラッディングを行い，中継ノードはそのパケットの転送を行う．3) はその AODV の性質を利用し，制御パケットである RREQ パケットを用いて信頼度の共有を行う方式である．送信者は RREQ パケットに自身の近隣ノードに対して算出した信頼度をその近隣ノードの ID と共にパケットに記入した上でフラッディングを行う．一方，RREQ パケットを受信した中継ノードは，自身の近隣ノードに関する信頼度が記入されていないかを調べ，記入されている場合は，その値を抽出する．次に，その中継ノードは自身がその近隣ノードに対して算出していた信頼度と先ほど抽出した信頼度を総合し，その近隣ノードへの新たな信頼度を決定する．同時に，新たに決定した値を，抽出した信頼度があったフィールドへ上書きし，RREQ パケットの転送を行う．したがって，3) は算出した信頼度の共有を，AODV における経路作成と同時に終了することが可能であるという利点を有する．

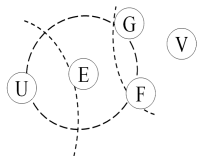

図 2 ノード配置例

3.2 Getting rust of a remote node 4)

しかしながら，近隣ノードではないノードの信頼度を知りたい場合は，ノード監視を行うことによる信頼度の取得は不可能である．そこで 4) は信頼度を知りたいノードの近隣ノードに対して算出した信頼度を TREQ パケットを用いて問い合わせる手法を提案している．図 2 にノードの配置例を示す．図 2 において，ノード U が近隣ノードではないノード V の信頼度を取得したい場合，ノード V を宛先ノードとして TREQ パケットをブロードキャストを行う．まもなくして，ノード F と G はこの TREQ パケットを受信し，パケットの宛先ノードが自身の近隣ノードであることが分かる．そこで，ノード F と G はノード V に対して算出した信頼度をノード U に返信する．この方式により，近隣ノードではないノードの信頼度を取得することが可能となる．

3.3 問 題 点

従来，2) のような相手ノード認証に関する研究と，3)4) のような通信経路の信頼性に関する研究はそれぞれ個別に取り扱われており，そのため 3)4) においては 2) で提案されている MANET における公開鍵分散管理方式を用いていない．よって，3)4) は以下にあげる 2 つの問題には対処できていないと考えられる．1 つ目の問題は，ネットワーク内における信頼度の改ざんに対する問題である．悪意あるノードが存在する MANET において，パケット内に記載された信頼度の値そのものの改ざんは容易に考えられる攻撃であり，この攻撃に対して信頼度が改ざんされたかどうかを確かめる改ざん検知の仕組みが必要となる．2 つ目の問題は，他のノードへのなりすましである．ノードの信頼度にもとづき通信経路を評価した上で，実際に用いる経路を決定しているのであるが，悪意あるノードが他のノードになり

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

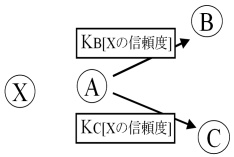

図 3 公開鍵を用いた共有法

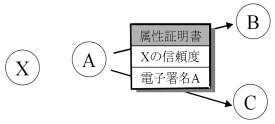

図 4 属性証明書を用いた共有法

すまし，自身にとって都合の良い信頼度を通知することが可能である．よって，その問題に対処するために，なりすまし検知の仕組みが必要となる．

4. 属性証明書を用いた通信経路の信頼度評価法

本節では 3.3 で述べた 2 つの問題を解決するために，2) で提案されている方式を 3)4) の方式に取り入れた新たな通信経路の信頼度評価法の検討を行う．まず 2) を用いた場合に実現できることは，通信相手ノードの認証と，認証によって正当性が保証された公開鍵による公開鍵暗号通信である．図 3 に，ノード A がノード X に関する信頼度をノード B，C に通知する様子を示す．ここで，図 3 における，K_B と K_C はそれぞれノード B，C の公開鍵である．2) を用いて考えられる信頼度の通知手段について，図 1 を用いて説明する．まず，ノード A はノード X を監視後，算出した信頼度を 2) を用いて入手したノード B，C の正当な公開鍵を用いて暗号化する．そして，暗号化した信頼度をノード B，ノード C に対して個別に送信する．しかしながら，このやり取りで保証される要素は，ノード A は確かにノード B，C と通信をしているということと，X の信頼度はネットワーク内において盗聴されないということの 2 点のみであり，逆に，ノード B，C から見れば，送信者は確かにノード A であるということと，信頼度は改ざんされていない，ということの 2 点を保証する手法とはなっていない．さらに，ノード B やノード C のようなノードが増加した場合，ノード A は毎回各ノードの公開鍵を用いて暗号化を行い，暗号化された信頼度を各ノードに送信しなければならないという問題も考えられる．

次に，ノード B，C が送信者はノード A であるということを確信でき，またノード A の役割を軽減できるような手法として考えられるのは，電子署名の付加された証明書を用いて信頼度を通知する手法である．この電子署名により可能となることは，送信者のなりすまし検知と，電子署名と共に送信されてきた情報の改ざん検知である．つまり，図 3 の場合，ノード A がノード X の信頼度と共に電子署名を付加した証明書をノード B，C に送信すると，ノード B，C は送信者が確かにノード A であるのかどうかという検証と，受信した信頼度がネットワーク内において改ざんされなかったどうかの検証が可能となる．このような証明書としてまず考えられる証明書が公開鍵証明書である．公開鍵証明書はノードの公開鍵の正当性を保証するための証明書であり，公開鍵証明書に信頼度を付加して通知を行うことは確かに可能である．しかし，信頼度自体の性質上，公開鍵証明書を用いることには問題がある．それは，信頼度が悪意あるノードの振る舞いにより常時変化するものであり，よって信頼度を付加した証明書を頻繁に失効させ，更新を行う必要がある．一方で，公開鍵証明書は信頼のおける機関が発行を行い，有効期限は一般に長く，失効や更新を頻繁に行う証明書ではないということである．つまり，有効期限の観点からすると，信頼度の性質と公開鍵証明書の性質は相反する性質であるという問題である．そこで，信頼度の有効期限の条件を満足し，さらに電子署名が付加された証明書として考えられるのが公開鍵証明書に付随した属性証明書であり，本論文において信頼度の通知や通信経路の信頼度評価を行うために用いる証明書である．これは，属性証明書が秘密鍵を持つユーザであれば容易に生成可能な証明書であり，この性質が信頼度の有効期限の条件を満足するためである．さらに，その正当性は公開鍵証明書による公開鍵の検証を以って保証される．図 4 にノード A がノード X に関する信頼度を，属性証明書を用いてノード B，C に通知する様子を示す．ノード A はノード X の信頼度と共に自身の秘密鍵によって作成した電子署名を付加した属性証明書をノード B，C に送信する．一方，この属性証明書を受信したノード B，C は 2) を用いて，ノードの A の正当な公開鍵を取得し，電子署名の検証を行うことで，信頼度の改ざん検知，さらに送信者がノード A であるというノードのなりすまし検知が可能となる．以下，従来方式では問題であった信頼度の改ざんと，ノードのなりすましという問題を解決するために，属性証明書を用いた通信経路の信頼度の評価法について述べる．初めに，提案方式の概要を述べ，次に属性証明書を用いた通信経路の評価法，さらに用いる属性証明書のサイズに関する検討を行う．

本方式は，ノードの動作を明確にするために，通信要求が生じていないオフライン状態と，通信要求が生じた場合のオンライン状態の 2 つの状態に分けて考える．まず，オフライン状態においてノードは，従来方式と同様の信頼度算出法を用い近隣ノードに対して信頼度を算出した後、信頼度を記入した属性証明書をその近隣ノードに発行する．一方，属性証明書を発行されたノードは，その属性証明書を収集，保持したままネットワーク内を移動する．そしてオンライン状態では，経路作成を行うノードは通信相手までの経路を複数取得しつつ各ノードから属性証明書を回収し，各属性証明書の検証を経て，最終的に通信経路の信頼度を評価と経路の選択を行う．

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

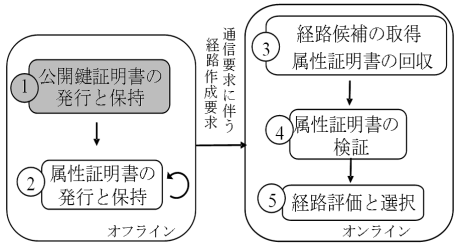

図 5 提案方式のフローチャート
ただし，陰部分は方式 2)

図 6 属性証明書の例

4.1 提案モデル

図 5 に提案方式における経路作成に至るまでのフローチャートを示す．図 5 で示す番号 1〜5 は本文での 4.1.1〜4.1.5 に対応する．

4.1.1 公開鍵証明書の発行と保持

オフライン状態において，各ノードは信頼するノードの公開鍵に対して公開鍵証明書の発行を行う．さらに，自身の公開鍵に対して発行された公開鍵証明書を収集し，それを保持する．これは，以下で示す属性証明書の検証を行うために，その属性証明書の発行者の正当な公開鍵が必要であり，2) 方式に従って，ノードが独自に生成した公開鍵を信頼の輪を構築することで認証するためである．

4.1.2 属性証明書の発行と保持

従来方式では，近隣ノードに対して算出した信頼度をその近隣ノードに知らせるという手法は取っていない．ここで，信頼度を算出するノードを算出ノード，また監視され信頼度を算出されるノードを被算出ノードと呼ぶことにすると，被算出ノードは自身の信頼度を知らないままネットワーク内を移動するということである．被算出ノードに信頼度を知らせると，例えば，悪意あるノードは個々の算出ノードに対してその振る舞い方を変化させ，自身に都合の良い信頼度を取得できるのではないか，という議論がある 3)．しかし，この手法には以下にあげる 2 つの問題が考えられる．1 つ目の問題は，ノード移動後，自身に対して算出された信頼度を新たな近隣ノードに示すことができないことである．つまり，算出ノードから見れば，自身の電波範囲内に新たに移動してきたノードの信頼度を取得するためには，毎回一定時間そのノードの振る舞いを監視しなければならない．2 つ目の問題は，算出ノードにおいて，算出した信頼度を用いない場合があるということである．通信が生じた場合，通信経路の信頼度評価を行うために信頼度が必要となるが，信頼度を算出した後，必ずしもノードの物理的な配置が変化する前に通信が発生するとは限らない．もし通信が発生しなければ，算出した信頼度は無駄となってしまうことも十分に考えられる．そこで，提案方式では上記の 2 つの問題に対して，被算出ノードに信頼度を知らせるという手法を取ることとする．まず，各ノードは近隣ノードの監視を行い，信頼度を算出後，被算出ノードに対して，算出した信頼度を記入した属性証明書の発行を行う．この発行が信頼度を知らせるということであり，被算出ノードは自身に対して発行された属性証明書を保持する．この手法により，上記の 1 つ目の問題に対しては，被算出ノードは移動直後も保持する属性証明書を以って，自身に対して算出された信頼度を示すことが可能であり，逆に算出ノードにとっては，毎回信頼度を算出することなく，他の算出ノードが算出した信頼度を利用することが可能となるという利点を有する．2 つ目の問題に対しても，被算出ノードが自身に対して算出された信頼度を保持して移動するため，信頼度が無駄になることはないと考えられる．

図 6 にノード A がノード B に対して発行した属性証明書の例を示す．以下，ノード A がノード B への信頼度算出後，ノード B に対して発行する属性証明書の作成法について述べる．まず，発行者 (A) は自身の ID と，発行先 (B) の ID を記入し，有効期限の設定を行う．これは，信頼度が悪意あるノードの振舞い方により常時変化し，ゆえに，ある時刻における信頼度を一定時間後には無効とするためである．次に，発行者 (A) は発行先 (B) に対して算出した信頼度を記入する．最後に，上記の内容 (発行者 ID，発行先 ID，有効期限，信頼度) を発行者 (A) の秘密鍵により暗号化し，ハッシュ関数からハッシュ値を取得する．それを電子署名 (A) とし，付加する．以上が属性証明書の作成法であり，各ノードは近隣ノードに対して算出した信頼度を記入した属性証明書を発行する．一方，属性証明書を発行されたノードはこれを保持し，ネットワーク内を移動することとなる．近隣ノードへの信頼度算出と，属性証明書の発行，さらに発行された属性証明書の保持を各ノードはオフライン状態においてネットワークを移動しながら行うこととなる．

4.1.3 属性証明書の回収

本節以降は，経路の作成要求が生じた場合のオンライン状態におけるノードの動作について述べる．MANET においては様々なルーティングプロトコルが提案されているが，本論文ではその中でも最も基本的な DSR(Dynamic Source Routing) 5) をベースにし，属性証明書の扱い方について検討を行う．通信要求が生じた場合，通信経路の作成を担う送信者は，初めに，どの経路が信頼度が高く，悪意あるノードを含まない経路であるのかを検証するために，各ノードが保持する属性証明書の回収を行う必要がある．この回収方法は主に 3 パターン考えられる．1 つ目の手法は，オフライン状態において，常に他のノードと保持す

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

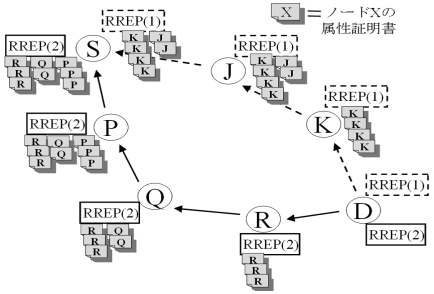

図 7 属性証明書の回収例

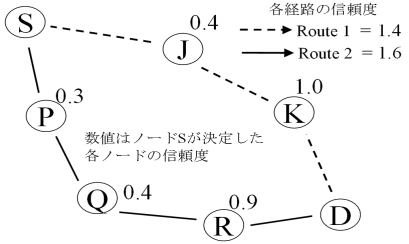

図 8 通信経路の信頼度評価と選択

る属性証明書を交換し合うという手法である．これにより，送信者は通信直前に信頼度を知りたいノードから属性証明書を回収する必要がなくなる．しかし，通信に伴いノードの信頼度を知りたい場合，信頼度を知りたいノードに対して発行された属性証明書を保持していない可能性，さらに不必要な属性証明書を保持してしまう可能性が考えられる．2 つ目の手法は，通信直前であるオンライン状態に，信頼度を知りたいノードから属性証明書を回収する手法である．この手法は，必要な時に必要なものだけを，というオンデマンドの考えにもとづく手法であり，不必要な属性証明書の交換を避けることができる一方で，遅延が発生するものと考えられる．3 つ目の手法は，上記の 2 つの手法のハイブリッド手法である．オフライン状態では有効期限の比較的新しい属性証明書のみを交換しておき，オンライン状態では不足している属性証明書のみを回収するという手法である．本論文では，2 つ目の手法に注目し，DSR の性質を上手く利用することで，遅延なく DSR と同様の動作のなかで属性証明書を回収する手法を検討する．

一般的に DSR は送信者が目的ノードまでの経路を作成するために RREQ パケットをブロードキャストし，最終的に目的ノードは複数の RREQ を受信し，それぞれの RREQ に対して RREP(Route REPly) パケットを返信することとなる．図 7 に RREP パケットを用いた属性証明書の回収法について示す．図 7 においてノード S は送信者であり，ノード D は目的ノードであるとする．ノード D は複数の RREQ パケットを受信後，それぞれの RREQ パケットに対して RREP パケットの返信を行う．この RREP パケットは最終的にノード S に届くのであるが，その際，各中継ノードは自身が保持する属性証明書をその RREP パケットに随時付加した上で転送を行う．この手法により，ノード S は各通信経路を構成する中継ノードが保持する属性証明書の回収を完了し，一般的な DSR の動作のなかで，属性証明書の回収を行うことができる．

4.1.4 属性証明書の検証

回収した属性証明書の検証とは，属性証明書の内容がネットワーク内において改ざんされなかったかどうかの改ざん検知，さらに，あるノードが他のノードになりすまして属性証明書の発行を行っていないかのなりすまし検知を行うことであり，属性証明書の正当性を保証するための検証である．ここで，検証を行うノード (検証ノード) が図 6 に示すノード B が保持している属性証明書を回収したとして，その検証法について示す．

初めに，検証ノードは属性証明書に記入されている発行者 (A) の正当な公開鍵を事前に取得する必要がある．これは属性証明書の発行者 (A) 自身の秘密鍵で作成された電子署名 (A) を復号するためである．取得した公開鍵の正当性は 2) を用いて，検証ノードから発行者 (A) までの信頼の輪の構築により認証される．もしここで信頼の輪を築くことができれば，公開鍵認証は成功し，よって属性証明書の検証を行うことができる．しかし，信頼の輪の構築に失敗すれば，取得した公開鍵が発行者の正当な公開鍵であるという保証はないため，その属性証明書の検証に失敗する．次に，検証ノードは取得した正当な公開鍵を用いて電子署名 (A) の復号を行う．ここで，復号により得られるハッシュ値を HASH-1 とする．また，検証ノードは属性証明書の内容からハッシュ値を算出する．ここで，得られるハッシュ値を HASH-2 とする．最後に，上記で得た 2 つのハッシュ値を比較し，同じであれば，改ざんや，なりすましはなかったと判断し，この属性証明書を正当な属性証明書とする．逆に，2 つの値が異なれば，その属性証明書を無効とする．以上が，検証ノードが行う検証動作であり，正当であると判断された属性証明書に記入されている信頼度を用いて，以下の通信経路の信頼度評価と選択を行う．

4.1.5 経路の信頼度評価と選択

送信者は，複数の通信経路候補の信頼度を評価し，最終的に経路を 1 つ選択することとなる．まず，送信者は前述の検証を行い，正当性が保証された属性証明書の信頼度を用いて，各ノードの信頼度を決定する．次に，決定した各ノードの信頼度から値を合計することで経路自体の信頼度を決定する．最終的に信頼度の高い経路を通信経路として選択する．図 8 に，経路評価と選択を行う例を示す．図 8 に示すように，ノード S は各中継ノードの信頼度を決定した後，それらを合計することで経路自体の信頼度を決定し，信頼度の高い経路を通信経路として選択する．しかし，この段階における信頼度の扱い方や，信頼度の表現の方法には，ただ単に信頼度を合計したものを経路の信頼度にしても良いのであるかということと，このような評価法を取る場合において信頼度を 1.0〜0.0 間で表現することが妥当であ

Vol.2009-SE-164 No.17
Vol.2009-EMB-13 No.17
Vol.2009-CSEC-45 No.17
2009/5/29

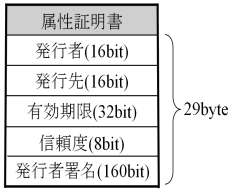

図 9 属性証明書のサイズ

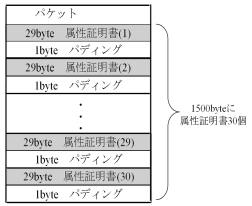

図 10 属性証明書を運ぶパケットの例

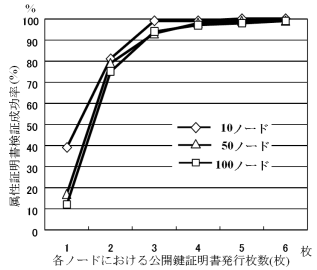

図 11 属性証明書の検証成功率

るのかどうかという課題がある．また，提案方式では属性証明書を RREP パケットに付加する手法で回収を行うため，属性証明書のサイズに関する検討を行う必要がある．

4.2 提案方式における属性証明書サイズ

本節では，提案方式で用いる属性証明書のサイズに関する検討を行う．提案方式は従来方式と異なり属性証明書を用いて信頼度の共有を行っているために，そのサイズはネットワークにおける通信量を考慮する上で重要な検討事項となる．図 9 に提案方式における属性証明書のサイズを示す．まず発行者，発行先の項目は 16bit とする．これは，災害現場，またイベント会場での使用を想定した場合，約 6 万ノード数分確保すれば十分であろうという理由による．次に，有効期限は UNIX 時刻を用い設定を行うため 32bit とする．信頼度を表すには，8bit で十分と考え，最後に発行者署名は SHA-1 から出力されるハッシュ値を用いるため 160bit とする．以上が，提案方式における属性証明書であり，1 枚のサイズを 29byte とすることができる．図 10 に提案方式における属性証明書の回収を行う際のパケットの構成図を示す．上記より属性証明書のサイズを 29byte と決定したため，1byte のパディングを考慮すると，1 パケットに最大で 30 枚の属性証明書の格納が可能となる．つまり，図 7 で示した回収手法はネットワークに負荷をかけない手法であると言える．

5. 評価:属性証明書検証成功率

計算機シミュレーションにより，公開鍵証明書の発行数に基づく属性証明書の検証成功率の評価を行う．シミュレーション諸元は，ノードの移動モデルはランダムウェイポイントモデル，範囲は 1000m × 1000m，ノードの電波範囲は 250m とする．図 11 に，各ノードにおける公開鍵証明書発行数に対する属性証明書の検証性効率を示す．横軸は，各ノードにおける公開鍵証明書発行数である．いずれのノード数の場合においても，各ノードが平均 3 個のノードの公開鍵を信頼して，公開鍵証明書の発行を行えば，90%の確率で属性証明書の検証が行えることがわかる．特に，100 ノードの場合，平均 6 個のノードの公開鍵を信頼して公開鍵証明書の発行を行えば，検証率はほぼ 100%であり，通信経路の信頼度評価を行うための属性証明書の検証は確実に行うことができると考えられる．

6. 結　　論

本論文では，公開鍵証明書に付随する属性証明書を用いた通信経路の信頼度評価法を提案した．属性証明書に信頼度を記入し，ネットワーク内で共有することで，改ざん検知や，なりすまし検知を行うことが可能となり，さらに通信経路の信頼度評価を行うための属性証明書の回収手法について検討を行った．計算機シミュレーションにより，属性証明書の検証成功率を示し，提案方式の有効性を示した．今後の課題として，提案方式によって選択された通信経路のホップ数と，DSR を用いた場合に選択される通信経路のホップ数の比較を行うことで，遅延に関する考察のみでなく，通信経路の信頼度を最終的に評価する段階における，信頼度の扱い方についての考察があげられる．また，本論文で示した属性証明書の 3 つの回収方法につていの検討を行い，どのようなネットワーク状態である場合，どの手法が有効であるのかの検討も行う予定である．

謝辞 本論文の一部はグローバル COE プログラム「アクセス空間支援基盤技術の高度国際連携」により行われた．また，本研究を進めるにあたり，有益な助言を頂いた KDDI 研究所の竹森敬祐氏，磯原隆将氏に，深く感謝する．

参 考 文 献

1) S. Corson, J. Macker,“ Mobile ad hoc networking(MANET): Routing protocol performance issues and evaluation consideration ”, IET-FRFC25010, January 1999.
2) 北田夕子, 荒川豊, 竹森敬祐, 渡邊晃, 笹瀬巌,“ 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 ”, vol103 , no.692, pp255-258, Mar 2004 電子情報通信学会論文誌
3) F. Oliviero, S.P. Romano, “ A Reputation-based Metric for Secure Routing in Wireless Mesh Networks ”, IEEE GLOBECOM 2008, pp.1-5, Nov 2008.
4) P. Veeraraghavan, V. Limaye, “ Trust in mobile ad hoc networks ”, IEEE ICT-MICC 2007, pp.330-334, May 2007.
5) D.B. Johnson,“ Routing in Ad Hoc Networks of Mobile Hosts ”, Proceedings of the Workshop on Mobile Computing Systems and Applications, IEEE Computer Society, Santa Cruz, CA, pp. 158-163, December 1994.