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

立山 崇之　　野口 拓　　川合 誠
立命館大学理工学研究科

1 はじめに

固定インフラを必要とせず無線端末同士でネットワークを形成するアドホックネットワークは, ユビキタス社会への貢献が期待される一方で, ルーティングプロトコルや電力効率, セキュリティといった様々な課題に直面している. アドホックネットワークのセキュリティ分野の課題の 1 つに公開鍵認証の問題がある. アドホックネットワークにおける公開鍵認証には, 従来の CA(Certificate Authority) といった一点集中型の認証局を用いることは困難であり, 分散型の公開鍵認証方式が必要とされている. これまでいくつかのアドホックネットワーク向けの分散型公開鍵認証方式が提案されてきたが, その多くが公開鍵管理に参加する端末の信頼関係を基盤とし, 各端末が不正をしないことを前提としているため, 不正を行う端末が存在する状況ではうまく機能しない.[1]

本稿では相互評価された端末信頼度を考慮する公開鍵認証方式について述べ, その性能を高めるための他端末評価機能の提案を行い, ネットワークシミュレータを用いて検討を行った結果を報告する.

2 関連研究

分散型の公開鍵認証方式の 1 つに証明書連鎖 [2] がある. 証明書連鎖は,CA のような一点集中型の認証局を用いることなく, 各端末が他の端末の公開鍵についての公開鍵証明書を自律的に発行・交換し, 集めた証明書をチェーンのようにたどることで他の端末の公開鍵認証を行う方式である. 図 1 に証明書連鎖の例を示す.

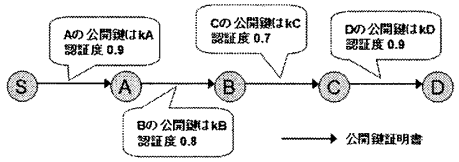


図 1: 証明書連鎖

公開鍵証明書には証明書の発行者, 鍵の所有者, 公開鍵認証度などの情報が含まれており, 証明書連鎖の始点端末からみた終点端末の公開鍵認証度は, 証明書連鎖に含まれる公開鍵証明書の公開鍵認証度の積によって求められる. 図 1 の例では, 端末 S から見た端末 D の公開鍵の認証度は $0.9\times0.8\times0.7\times0.9 = 0.4536$ となる.ネットワーク中に不正な証明書を発行する端末が存在すると, 証明書連鎖に不正な証明書が含まれる可能性があり, 証明書連鎖がうまく機能せず認証が失敗してしまうという問題点がある.またその場合, 証明書連鎖に不正な証明書が含まれるかどうかを見分けることはできない [1].

CKM(Composite Key Management)[1] は, 証明書連鎖と仮想 CA[3] とを統合した公開鍵管理方式である. CKM では証明書連鎖の正当性がチェーンの長さによって変わる確率的減衰モデルが提案されている.CKM の確率的減衰モデルを用いた証明書連鎖では, ネットワーク内の端末が悪意がある確率 p(ここで $0 \leqq p \leqq 1$) を減衰定数として与えると, 長さ d の証明書連鎖が正当である確率は $(1-p)^{d-1}$ で表される.ある端末を対象とする長さ n の証明書連鎖に含まれる各証明書の認証度の値を $(V_1, V_2, \cdots, V_n)$ とすると, その証明書連鎖が示す対象端末の公開鍵の認証度は $V_1 \times V_2 \times \cdots_n \times (1-p)^{n-1}$ となる.CKM の確率的減衰モデルを用いた証明書連鎖は, 正当な証明書連鎖でも長さが長ければ, 認証度は低くなり, 逆に不正な証明書連鎖でも, 長さが短ければ認証度は高くなる. その結果, 不当な証明書連鎖の情報に基づき, 誤った公開鍵認証をしてしまう可能性があり, 証明書連鎖の問題点を完全に解決したとはいえない.

3 提案方式

本章では信頼証明書を導入することで個々の端末の信頼度の違いを考慮する公開鍵認証方式 [4] について述べ, 本方式の性能向上の方法として, 信頼度不明な端末および不正端末に与える信頼度の値の適切な設定と, 他端末評価という考え方を提案し, それについて述べる.

3.1 信頼証明書を用いた公開鍵認証

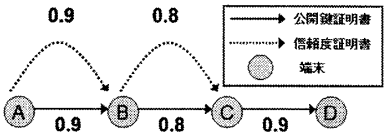


図 2: 信頼証明書を用いた公開鍵認証方式

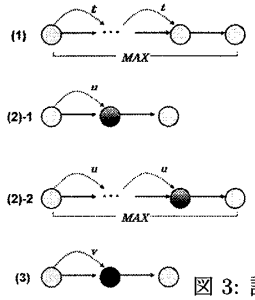
図 2 は信頼証明書を用いた公開鍵認証方式のシステムモデルで, 実線矢印は証明書連鎖と同等の公開鍵証明書を表し, 点線矢印は信頼証明書を表している. 信頼証明書には証明書の発行者, 対象者, 信頼度などの情報が含まれており, 信頼度は発行者から見た対象者の振る舞いの信頼度を数値化 (0.0〜1.0) したものを表す. 例えば A と B の間の点線矢印は A が発行した,B を対象とする信頼度 0.9 の信頼証明書を表す. 本方式において, ある端末を対象とする長さ n の証明書連鎖に含まれる各公開鍵証明書の公開鍵認証度を $(V_1, V_2, \cdots, V_n)$, 各信頼証明書の信頼度を $(T_1, T_2, \cdots, T_{n-1})$ とすると, その証明書連鎖が示す対象端末の公開鍵の認証度は $V_1 \times T_1 \times V_2 \times T_2 \times \cdots \times V_{n-1} \times T_{n-1} \times V_n$ となる.

不正な証明書を発行する端末の信頼度を低くすることで, 不正な端末が参加している証明書連鎖は長さが短くても認証度は低くなる. 本方式では, 対象とする端末までの証明書連鎖の中で, 最も認証度の高い証明書連鎖の情報を元に, 端末とその公開鍵の紐付けを行う.

3.2 信頼度不明な端末および不正端末に与える信頼度

3.1 で述べた方式では,(a) 正当な証明書のみで構成され, 信頼証明書がすべて存在する証明書連鎖,(b) 信頼証明書が欠けている証明書連鎖,(c) 不正な証明書を含み, その発行者である不正端末を対象とする信頼証明書が存在する証明書連鎖, という 3 つのパターンが考えられる. このとき証明書連鎖の認証度の大小関係は,「(c)<(b)<(a)」の関係を満たすことが望ましい. それぞれの証明書連鎖の例と各パラメータを図 3 に示す.

"Distributed Public-Key Authentication Using Mutually Evaluated Terminal Trustworthiness in Ad-Hoc Networks"
Takayuki Tateyama　Taku Noguchi　Makoto Kawai
Graduate School of Science and Engineering, Ritsumeikan University



○	正当であることがわかっている端末
●	信頼度不明の端末
●	不正であることが分かっている不正端末
MAX	証明書連鎖の最長限度
c_1	公開鍵証明書の取りうる認証度の最大値
c_2	公開鍵証明書の取りうる認証度の最小値
t	正当な端末に発行する信頼証明書が取りうる信頼度の最小値
u	信頼度が不明な端末に与える信頼度
v	不正な端末に与える信頼度
d	証明書連鎖に含まれる公開鍵証明書の数

図 3: 証明書連鎖の例

ここでまず「(b)<(a)」の関係について考える. (a) の認証度が最小となるのは図 3 の (1) のように,d=MAX となる場合である (認証度:$c_2^{MAX} \times t^{MAX-1}$).($b$) の認証度が最大となるのは図 3 の (2) − 1 のように,$d = 2$ の場合である (認証度 :$c_1^2 \times u$).したがって,「$c_1^2 \times u < c_2^{MAX} \times t^{MAX-1}$」となる. 次に「(c)<(b)」の関係について考える.(b) の認証度が最小となるのは図 3 の (2) − 2 のように,$d = MAX$ の場合である (認証度 : $c_2^{MAX} \times u^{MAX-1}$).($c$) の認証度が最大となるのは図 3 の (3) のように,$d = 2$ の場合である (認証度 : $c_1^2 \times v$).したがって,「$c_1^2 \times v < c_2^{MAX} \times u^{MAX-1}$」となる.

それぞれのパラメータに本研究で設定している値を代入して (MAX=10,c_1=0.9,c_2=0.7,t=0.7) 計算すると,u<0.0138,v<2.6358×10^{-17} となる. これに基づき, 本研究では信頼度が不明な端末に与える信頼度の値を 0.013, 不正な証明書を発行する端末に与える信頼度の値を 2.635×10^{-17} と設定する.

3.3 他端末評価

信頼証明書を用いる公開鍵認証方式において, 先述の「(a) 正当な証明書のみで構成され, 信頼証明書がすべて存在する証明書連鎖」が多いほど, 正しい公開鍵認証を行うことができる. ここでは他端末の信頼度をより多く知る方法として, 集めた公開鍵証明書をチェックして信頼度を査定する 2 つの方法を提案する.

3.3.1 自分自身を対象とする公開鍵証明書をチェック

集めた公開鍵証明書の中で, 自分自身を対象とする証明書に注目し, 鍵情報と発行者を調べる. もし正しい鍵情報を含んでいれば, 発行者を正当な端末であると評価し, 誤った鍵情報を含んでいれば, その発行者を不正端末であると評価する.

自分自身の公開鍵の情報は分かっているため, 査定を誤ることは無い.

3.3.2 他端末を対象とする公開鍵証明書をチェック

集めた公開鍵証明書の中で, 他端末を対象とする証明書に注目し, 鍵情報と発行者を調べる. その端末のものとされている鍵候補の中で, 最も証明書が多い鍵を鍵情報として含む証明書の発行者を正当な端末であると評価し, 他の鍵情報を含む証明書の発行者を不正端末であると評価する.

多数決的に査定を行うため, 鍵候補の中で, 誤った鍵の証明書が最も多ければ, 査定を誤ってしまう.

4 計算機シミュレーションによる性能評価

CKM の確率的減衰モデルを用いた証明書連鎖を比較対象とし, 信頼証明書を用いた公開鍵認証方式の「他端末評価機能無し」と「他端末評価機能有り」の性能を, ネットワークシミュレータ JiST/SWANS[5] を用いて検討を行った. 本シミュレーションでは前提条件として端末利用者間の友好関係をあらかじめ設定し, 不当な証明書を発行する端末（不正端末）の数を変化させ, それに応じた正当結合率（「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」）と, シミュレーション全体における紐付け結果の内訳を測定した. 本シミュレーションにおけるそれぞれの方式の紐付け総数はほぼ同数である. また, 本シミュレーションでは, 不正な証明書を発行する端末（不正端末）をネットワーク中に存在させている. 正当な端末および不正端末の動作は過去のシミュレーション [4] と同様である. 表 1 にシミュレーション環境を示す.

表 1: シミュレーション環境

試行回数	各100回
シミュレーション時間	900s
総端末数	50個
端末帯域	1MByte/s
フィールドサイズ	1000m× 1000m
初期配置	Grid
移動性	RandomWayPoint (no pause)
移動速度	5m/s
通信可能範囲	半径100m
証明書交換条件	通信可能範囲に25秒以上滞在
1端末の友好関係数	20個
不正端末数	2, 4, 6, 8, 10個

4.1 信頼度の値

信頼証明書を用いた公開鍵認証方式の「他端末評価有り」では, 各端末は証明書連鎖の認証度計算に必要な自身以外の全端末の信頼度を次の手順で再評価する. (1). 自分自身を対象とする公開鍵証明書チェックにおいて正当であると評価されている端末に対しては, その端末の信頼度を 1, 不正端末だと評価されている端末に対しては, その信頼度を 2.635×10^{-17} とする. (2). 手順 (1) で再評価できない端末に対しては, 他端末を対象とする公開鍵証明書チェックにおける評価に基づき手順 (1) と同様の処理を行う. (3). 手順 (2) でも再評価できない端末に対しては, 信頼度の再評価を行わない (この場合,「他端末評価無し」と同様の値となる).

4.2 シミュレーション結果

図 4 に測定した正当結合率を示す. どの状況でも,CKM の証明書連鎖に比べて信頼証明書を用いた公開鍵認証方式の方が高い正当結合率を示し, 他端末評価機能有りの方がより高い正当結合率を示すという結果になった. 図 5 に紐付け結果の内訳を示す. 信頼証明書を用いた公開鍵認証方式に他端末評価機能を実装することで, 正当な証明書連鎖が存在していて紐付け失敗するケースが減少するという結果になった.

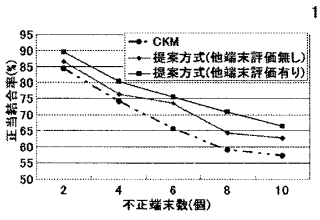


図 4: 正当結合率

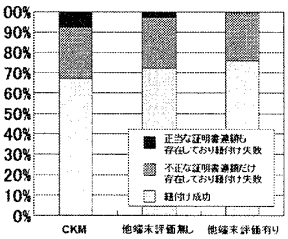


図 5: 紐付け結果

5 まとめ

本稿では, 相互評価された端末の信頼度を考慮した公開鍵認証方式, および他端末評価機能の提案を行った. シミュレーションによる検討の結果,CKM の確率的減衰モデルよりも信頼証明書を用いた公開鍵認証方式が高い正当結合率を実現し, さらに他端末評価機能を実装することで, 正当な証明書連鎖が存在し認証失敗となるケースを減少させ, より高い正当結合率を実現することを確認した.

参考文献

[1] Seung Yi et al. ,"Composite Key Management for Ad Hoc Networks", MobiQuitous2004, pp.52-61,2004.

[2] Srdjan Capkun et al. ,"Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE TMC,Vol.2,No.1,2003.

[3] Bing Wu et al. , "Secure and efficient key management in mobile ad hoc networks", IEEE Network, pp.288-295,2005.

[4] 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端末の信頼度を考慮した分散型公開鍵管理方式", 情報処理学会第 71 回全国大会, pp.385-386,2009.

[5] http://jist.ece.cornell.edu/.