マルチホップセルラネットワークにおけるインセンティブ機能およびPKI補助機能の統合

安齋 潤[†,††] 松本 勉[†]

マルチホップ通信では，ノードがルータ機能を持つ．このようなマルチホップ通信を用いたアドホックネットワークやマルチホップセルラネットワークのセキュリティ課題として，Public Key Infrastructure が必ずしも有効でない場合があること，また各ノードが必ずしもデータ転送に協調しないことが，従来は個別に研究されてきた．これらの課題が相互に関連していることを指摘し，これらを統合的に解決する汎用性の高いセキュリティ機構を提案する．

Integration of the Incentive and the PKI-supporting Mechanism on Multi-hop Cellular Networks

Jun Anzai[†,††] and Tsutomu Matsumoto[†]

As networks using multi-hop there are ad-hoc networks and multi-hoc cellular networks. Those networks have two problems, PKI is not always available and nodes do not always cooperate to forward data. In this paper, we indicate a relation between the problems, and propose security mechanism that can unitedly solve the problems.

1. はじめに

1.1 マルチホップ通信によるネットワーク

マルチホップ通信は送信端末から受信端末へ経路上の転送端末がバケツリレー式にデータを転送する方式である．これを用いたネットワークとして，**アドホックネットワーク**（アドホックネットと呼ぶ）や**マルチホップセルラネットワーク**（セルラネットと呼ぶ）が存在する．

アドホックネット（**図 1**）は，無線端末（ノードと呼ぶ）の集合から自立的に形成されたネットワークであり，バックボーンインフラ（BI と呼ぶ）を介さずにノードが相互に接続して網目のように通信する．BI が不要，短距離通信とトラフィック分散による周波数帯域の有効利用，無線エリアが拡大容易なことを主な特徴とする．

セルラネット（**図 2**）は，プロバイダが提供するアクセスポイント（AP と呼ぶ）を介して BI に接続する無線 LAN スポットサービスや基地局を介して BI に接続する携帯電話等のネットワークと，アドホックネットを結合したネットワークである．ここで，BI とノード間の通信はマルチホップにより実現される．既存網を利用しつつ，アドホックネットの特徴を取り入れたとネットワークと考えられる．本論文でセルラネットは次の前提を持つ：

- 無線 LAN スポットサービスと携帯電話を想定する．
- ノードはつねにステーションに接続できるとは限らない．
- ノード間通信は必ずしもステーションを経由しなくてよい（AP と基地局を総称してステーションと呼ぶ）．
- ステーションを経由する場合，ステーション以降の通信網がマルチホップ通信をサポートする必要はない．

1.2 マルチホップ通信のセキュリティ課題

本論文では，セキュリティ課題として知られるノード間認証，セキュアルーティング[1),12)]，ノード間協調等のうち，ノード間認証とノード間協調に着目する．

《PKI 補助機能》

一般に不特定多数のエンティティ間認証に PKI（Public Key Infrastructure）を用いるが，次の理由により，想定するネットワークでは必ずしも有効でない．

- ノードは，リソースが少ないため，複数回の証

† 横浜国立大学
Yokohama National University
†† パナソニック MSE 株式会社
Panasonic Mobile & System Engineering Co., Ltd.

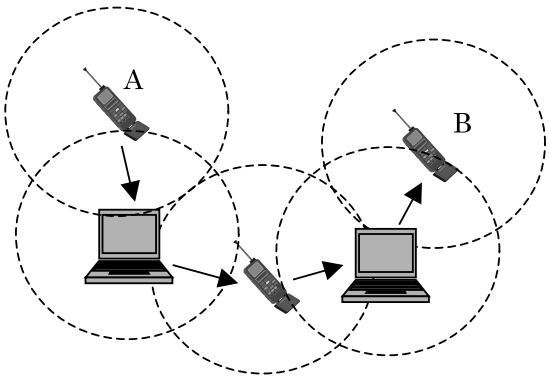

図 1 アドホックネットワークにおけるノード A からノード B へのマルチホップ通信
Fig. 1 Communications from node A to node B in ad-hoc networks.

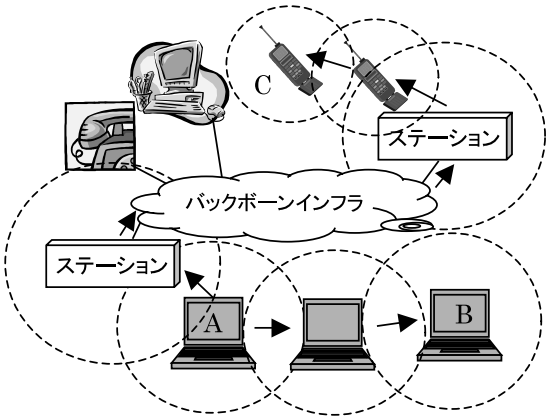

図 2 マルチホップセルラネットワークにおけるノード A からノード B とノード C へのマルチホップ通信
Fig. 2 Communications from node A to node B and node C in multi-hop cellular networks.

明書検証やディジタル署名生成は負荷が大きい，また不特定多数のノード認証に必要な種類の CA（Certificate Authority）証明書の保持も困難である．

- 証明書の発行や管理に CA を利用できない場合がある（ただし，セルラネットでは他ネットワークとの連携を考慮しなければ CA は必ずしも必要ではない）．

以上を解決するため，リソースに余裕があるノードが他ノードに対して証明書の代理検証，証明書の提供，および証明書の発行を行う PKI 補助機能が存在する．

《インセンティブ機能》

マルチホップ通信では，ノードがデータ転送を行う必要がある．しかし，ノードはバッテリ駆動であり，電力を消費する処理への協力に積極的でないと予想される（バッテリ問題は燃料電池により解決する可能性もあるが，本論文では未解決問題として扱う）．そのため，ノードの協調を促すために協調に対して報酬を与え，非協調対して罰を与えるインセンティブ機能が存在する．報酬を数値（Reward Point: RP と呼ぶ）として表し，RP をサービスと交換する方式が多く検討されている．

1.3 関 連 研 究

アドホックネットに PKI を適用する研究を紹介する．論文 4)，6) に PGP（Pretty Good Privacy）と同様に知り合いを信頼する方式が提案されている．PGP との違いは公開鍵ディレクトリを用いず，各ノードが自身の証明書を発行管理・配送すること，ノード間で証明書を交換することである．全処理を行うノードに負荷が集中することが課題である．一方，特権的なノードのグループを信頼する方式[10),16),17)] も提案されている．CA の秘密鍵を特権的なノードが分散保持し，一定数以上の秘密鍵を用いると証明書の発行・配布が可能となる．ノードは複数の特権的なノードへ接続が必要なことが課題である．ノードグループを信頼する方式[15)] も提案されている．ノード自身で検証困難な証明書の信頼性を同報でグループに問い合わせる．通信量の増加や，問合せ結果の安全な判断方式に課題が残る．

次に，インセンティブ機能の研究を示す．論文 2)，3) にアドホックネットを想定し，信頼の仮定を耐タンパモジュール TRM（Tamper Resistant Module）におく方式が提案されている．TRM で管理する RP を転送時に増加し，逆にデータ送信時に減少し，転送先 TRM が転送を検査して転送元に対して RP を送る．送り方が不明確なこと，高機能な TRM が必要となることが課題である．一方，セルラネットを想定した共通鍵暗号ベースの方式[8),14)] が提案されている．基地局で各ノードの RP 口座を管理する．各ノードは基地局とセッション確立後，送信データに MAC（Message Authentication Code）を付け，それを基地局経由時に検査することで送信・転送ノードを特定し，送信ノードの RP を転送ノードに移動する．基地局から受信ノードへの転送時は，受信ノードが基地局へ受信通知を行う．ノードの負荷が小さくて済む反面，必ずノード間通信が基地局を経由することおよび，通過するノードを明示的に示して中継するソースルーティング方式を前提とするため，ルーティングに自由度が少ないことが課題である．特に基地局へつねに接続できるとは限らないセルラネットではこれらの前提は妥当とはいえない．

また，公開鍵暗号ベースでアドホックネットを想定した方式[18] が提案されている．データに添付した送信ノードの署名を，転送時に転送ノードが，受信時に受信ノードが検証する．受信ノードが署名を TTP（Trusted Third Party）に送り，TTP が送信ノードから転送ノードへと RP を移す．TTP の仮定や，ノードが転送ごとに署名検証することが課題である．暗号に代わり監視を用いたルーティング方式[1),12)] が提案されている．ノードがデータ転送を監視し，転送しないノードを検出し，再送信時に当該ノードをルートから外す仕組みのため，インセンティブ機能に使える（監視結果を元に RP を転送ノードに発行すればよい）．しかしながら，監視は負荷が大きく，多くのシステムではノードによる監視を想定することは現実的ではないと考えられる．

1.4 本論文の概要

従来方式では，PKI 補助・インセンティブ機能は別々に議論され，同時に両機能を適用する検討は行われていない．しかし，インセンティブ機能を実現するために PKI を前提とする方式があり，逆に PKI 補助機能においてノードの協調を前提とする方式もある．つまり，両機能は互いに補完関係の場合がある．この場合，PKI 補助機能のどの部分にインセンティブ機能が必要であるのか，インセンティブ機能に必要な PKI 補助機能とは何であるのか，について同時に検討することが重要である．本論文では，セルラネットにおいて仲介ノードと呼ぶ特権ノードが PKI 補助・インセンティブ機能を同時提供する方式を提案する．従来方式[8),14)] と異なり，ルーティングの自由度が高いことを特徴とする．

以降，2 章において提案機構のシステム構成と設計方針を示し，3 章において提案機構の詳細を説明し，4 章において提案機構の性能と安全性の評価を行う．

2. システム構成と設計方針

2.1 システム構成

提案機構は，以下のエンティティから構成される：

ノード：マルチホップ通信機能を有する無線端末である．任意のノード証明書（とその秘密鍵），任意の CA 証明書，および耐タンパモジュール TRM を有する．本論文では TRM として SIM（Subscriber Identity Mo-dule）等の IC カードを想定し，Card と表記する．仲介ノード以外のノードを示す場合，一般ノードと呼ぶ．

仲介ノード：システム管理者の発行する代理証明書（とその秘密鍵），任意のノード証明書（とその秘密鍵），複数のシステム管理者証明書のうち少なくとも 1 つを検証可能な CA 証明書および TRM を有するノードである．なお，代理証明書とは，システム管理者がノードを仲介ノードとして認定したことを示す有効期間の短い（たとえば 1 日程度）証明書である．

仲介ノードは一般ノードよりリソースを要求されるため，主にノート PC を，一般ノードは携帯電話や PDA を想定する．ともにマルチホップ通信可能な無線通信技術 Bluetooth，UWB，IEEE802.11 等を備える．

システム管理者：セルラネットの管理者であり，M と表記する．無線 LAN スポットサービスや携帯電話サービスを提供するキャリアを想定する．ほぼすべての CA 証明書を有する．また，全ノードが信頼する．

ステーション：無線 LAN スポットサービスのアクセスポイントや携帯電話の基地局の総称である．本論文では，システム管理者，カード発行者と合わせてバックボーンインフラ BI の一部として扱う．

カード発行者：TRM である Card（またはそのアプリケーション）の発行・管理者であり，C と表記する．Card 内の RP を増加する権限を有する．なお，システム管理者と同一でもよい．また，全エンティティが信頼する．

2.2 設 計 方 針

提案機構は，論文 8)，14)，18) の方式と異なり，信頼できる中央機関に代わり，仲介ノードが PKI 補助・インセンティブ機能を同時に提供する．このようなアプローチにより，以下の目標を実現するように設計を行う：

(1) 送受信メッセージが必ずしも BI を経由する必要がない．そのため，ルーティングの自由度が高い．

(2) 機能を個別に提供する場合に比べて初期設定や不正検出・防止機能の重複を削減でき，かつ個々の機能に対する不正ノードおよびその情報を一括的に扱うことにより，安全性が向上する．

(1) を実現するため，インセンティブに関する検証を BI が直接かつリアルタイムに行わずに済ます必要があり，PKI を用いて仲介ノードを実現する．PKI 補助機能の実現に必要となるインセンティブ機能と，インセンティブ機能の実現に必要となる PKI 補助機能を明確にする．

さらに，提案機構は以下の性質を満たす設計とする：

接続性：証明書の検証処理を高確率で実行できる．

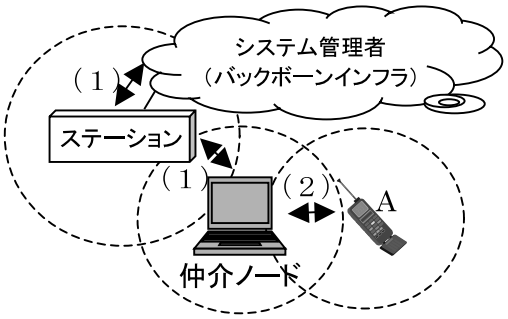

図 3 システム管理者による仲介ノードの認定（1），およびノード A の仲介ノードへの登録（2）
Fig. 3 A system manager authorizes on intervener (1), and the intervener registers node A (2).

効率性：システムに対するオーバヘッドが少ない．
検証性：不正を検出できる．
結託耐性：結託によりシステムの秘密が漏洩しない．
追跡性：不正ノードを特定できる．

3. 提 案 機 構

提案機構を，PKI 補助・インセンティブ機能に共通の準備フェーズ，PKI 補助機能，およびインセンティブ機能に分けて説明する．以下の記号を説明に用いる：

H(·)： 暗号学的に安全な一方向性ハッシュ関数．
HMAC(·)： 暗号学的に安全な MAC 関数．
ID_A： エンティティA の ID．
$\theta(\mathbf{a},\mathbf{b},\mathbf{c})$： Reward Point を表すデータ．a がエンティティの ID，b がポイント数，c が Out の場合は Card からの出力，In の場合は入力を表す．c の未記載は Card 内に存在する状態を示す．
$AInfo_{AB}$： エンティティA からエンティティB に送る認証情報であり，A と B の共通鍵 $CKey_{AB}$ と ID，認証対象情報を入力とする HMAC の出力．A は認証情報の生成ごとに 16 バイト程度の乱数を生成し，これを認証対象情報に含め，この乱数を B に送る．特に記載のないとき，認証情報の検証に失敗した場合に B は処理を終了する．

3.1 準備フェーズ

提案機構では，ノードが仲介ノード j としてシステム管理者 M に認定され，j へ他ノードが登録を行う（**図 3**）．その後，j が登録済みのノードに対して PKI 補助機能およびインセンティブ機能の提供を行う．

《仲介ノードの認定》

Step1：ノード i はリソース情報 $RInfo_i$，これに対して，自身の証明書 $Cert_i$ に対応する秘密鍵 $SKey_i$ を用いて生成したディジタル署名 Sig_i を M へ送る．なお，$RInfo_i$ は i が公開可能なスペック（例：CPU，メモリサイズ，HD 容量），保持する CA 証明書の Subject のリスト，自身の証明書 $Cert_i$ を少なくとも含む．

Step2：M は Sig_i を検証し，$RInfo_i$ に基づき代理証明書☆$PCert_i$ と譲渡情報☆☆$TInfo_i$ を発行し，共通鍵 $CKey_{Mi}$ を生成する．$PCert_i$ とその秘密鍵 $PSKey_i$ と $TInfo_i$ とこれらに対する署名 Sig_M（自身の証明書 $Cert_M$ に対応する秘密鍵 $SKey_M$ により生成）を $CKey_{Mi}$ により暗号化した暗号文 $Enc1_M$，$CKey_{Mi}$ を $Cert_i$ の公開鍵により暗号化した $Enc2_M$ を i に送る．なお，$TInfo_i$ は M が i に対して提供する PKI 関連情報であり，具体的には $RInfo_i$ に基づき i が扱える量だけ，M の証明書，各種 CA 証明書，CRL，不正ノードのブラックリストを含む．

Step3：i は $Cert_i$ に対応する秘密鍵 $SKey_i$ で $Enc2_M$ を，$CKey_{Mi}$ で $Enc1_M$ を復号する．Sig_M を検証し，成功時は復号した情報を受け入れ，失敗時は拒否する．

《仲介ノードへの登録》

仲介ノード j への登録とは，ノード k と j が相互認証を行い，共通鍵を共有することを意味する．

Step1：k はリソース情報 $RInfo_k$，これに対して，自身の証明書 $Cert_k$ に対応する秘密鍵 $SKey_k$ を用いて生成したディジタル署名 Sig_k を j へ送る．なお，Step2 で発行される一時ノード証明書 $TCert_k$ を取得済みの場合は $Cert_k$ に代えて $TCert_k$ を使用し，一方，j は $Cert_k$ を提示された場合には $TCert_k$ を発行する．ここで，$TCert_k$ とは，仲介ノードが自身の代理証明書により，一般ノードに対して自身に登録済みであることを証明するために発行する証明書である．

Step2：j は Sig_k を検証☆☆☆し，一時ノード証明書 $TCert_k$（とその秘密鍵 $TSKey_k$），共通鍵 $CKey_{jk}$ を生成し，これらに対して $RInfo_k$ に基づき選択した代理証明書 $PCert_j$ に対応する秘密鍵 $PSKey_j$ により署名 Sig_j を生成する．Sig_j と $TCert_k$ と $TSKey_k$ を $CKey_{jk}$ で暗号化した暗号文 $Enc1_j$，$CKey_{jk}$ を

☆ M は各 CA に対応した $PCert_i$ を発行できるため，$RInfo_i$ に基づき i が扱える枚数分だけ，各 CA に対応した $PCert_i$ を発行する．
☆☆ 仲介ノード間の連携が可能な場合，他の仲介ノードの位置情報，保持する証明書の Subject のリスト，仲介ノード間の共通鍵 $CKey_I$ を少なくとも含む．
☆☆☆ j は検証に必要な CA 証明書を保持しない場合，仲介ノード間の連携を想定するモデル（仲介ノード間共通鍵 $CKey_{all}$ を仮定）では，他仲介ノードに $CKey_{all}$ を用いて CA 証明書の提供を依頼できる．

$Cert_k$ の公開鍵で暗号化した暗号文 $Enc2_j$，$PCert_j$ を k へ送る．

Step3：k は $SKey_k$ で $Enc1_j$ を，$CKey_{jk}$ で $Enc2_j$ を復号して Sig_j を検証し，成功時にのみ受領する．なお，k が検証可能な CA 証明書を保持しない場合，相互認証済みの他ノードに CA 証明書の提供を依頼できる．

一時ノード証明書は，上位 CA がシステム管理者となっているため，任意の CA が発行する証明書と比べて，他の仲介ノードが検証できる可能性が高い．

仲介ノード j はノードに提供したサービスに応じて RP をシステム管理者 M から受け取る．j はサービス提供時にノードから認証情報を受信するが，これが一定量となった際，その検証に必要な共通鍵とともに M へ送る．M はこれらを検証し，成功時にカード発行者 C からサービスに応じた RP の発行を受けて RP を j へ送る．

仲介ノード間通信を想定できる場合，仲介ノード認定時に，M は仲介ノード間共通鍵と他仲介ノード情報を仲介ノードに提供し，仲介ノードはそれらを利用することで，一般ノード登録時の成功確率の向上および，他仲介ノードへ登録済みノードと，自身に登録済みのノードとの相互認証および鍵共有☆が可能となる．

3.2 PKI 補助機能

提案機構は PKI 補助機能として，証明書の代理検証，証明書の発行，公開鍵ディレクトリ（証明書の提供機能）をサポートする．なお，代理検証・発行に関しては，具体的な利用方法を提案するため，ノード間の相互認証および鍵共有プロトコルに適用した形で説明する．

《相互認証および鍵共有の補助》

仲介ノード j を介し，登録済みノード A，B の相互認証および鍵共有（**図 4**）を共通鍵暗号で実現する☆．

Step1：A は乱数 $Rand_A$ 生成し，処理開始要求として $ID_A \| Rand_A$ を B に送る．ここで，$\|$ は連結を示す．

Step2：B は Step1 の処理開始要求に応じる場合は乱数 $Rand_B$ を生成し，$ID_B \| Rand_B$ を A に送る．

Step3：A は $Rand_A$，ID_B，それらを対象とする $AInfo_{Aj}$，ID_A，ID_j を j に送る．

☆ A と B がそれぞれ別の仲介ノード E と F に登録されている場合，Step3，4 をそれぞれ登録している E と F に対して行い，E と F はそれぞれが得た乱数を交換して，認証情報を検証し，成功時は E と F が $CKey_{AB}$ の生成に必要な情報を交換する．なお，E と F 間通信の認証と暗号化には仲介ノード間共通鍵 $CKey_{all}$ を用いる．

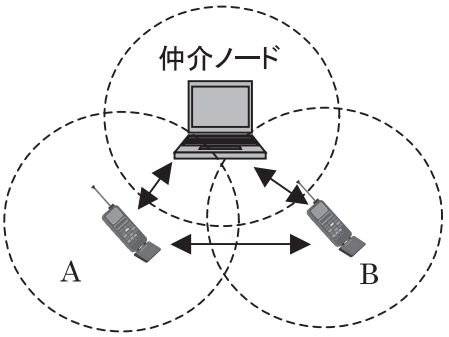

図 4 PKI 補助機能における仲介ノードによるノード A と B への相互認証および鍵共有の補助

Fig. 4 An intervener authenticates node A and node B, the intervener shares a key with the nodes as a PKI-supporting mechanism.

Step4： B は $Rand_B$，ID_A，それを対象とする $AInfo_{Bj}$，ID_B，ID_j を j に送る．

Step5：j は $AInfo_{Aj}$，$AInfo_{Bj}$ を $CKey_{jA}$，$CKey_{jB}$ で検証し，$Rand_A \| Rand_B$ を対象とする $AInfo_{jA}$，$CKey_{jA}$ により共通鍵 $CKey_{AB}$ を暗号化した暗号文 Enc_{jA}，ID_j，ID_A を A へ送る．$Rand_A \| Rand_B$ を対象とする $AInfo_{jB}$，$CKey_{jB}$ を用いて共通鍵 $CKey_{AB}$ を暗号化した暗号文 Enc_{jB}，ID_j，ID_B を B へ送る．

Step6：A と B は，各々$CKey_{jA}$，$CKey_{jB}$ により $AInfo_{jA}$，$AInfo_{jB}$ を検証し，成功時のみ各々 $CKey_{jA}$，$CKey_{jB}$ により Enc_{jA}，Enc_{jB} を復号し，それぞれ $CKey_{AB}$ を得る．

《公開鍵ディレクトリサービス》

仲介ノード j へ登録済みのノード i に対し，j が保有する PKI 関連情報（証明書等）を提供する機能である．

Step1：i は請求 List（証明書の Subject リスト等），それを対象とする $AInfo_{ij}$，ID_i，ID_j を j に送る．

Step2：j は $AInfo_{ij}$ を検証し，請求 List に対応する情報 $PKIInfo_j$，それを対象とする $AInfo_{ji}$，ID_j，ID_i を i へ送る．

Step3：i は $AInfo_{ji}$ を検証し，成功時のみ $PKIInfo_j$ を受け入れる．ただし，対価の RP を提供済みで，$PKIInfo_j$ が請求 List の内容と異なる場合は M へ通知する．

3.3 インセンティブ機能

インセンティブ機能の前提となる TRM である Card の RP 管理と，機能モデルを説明する．各ノードが登録する仲介ノードと RP を仲介する仲介ノードは異なって構わないが，簡単化のためにいずれも j と記載する．

《TRM（Card）における RP 管理》

ノード i は $Card_i$ を有し，$Card_i$ の $\theta(i, Y)$ から $X(\leqq Y)$ ポイントの $\theta(i, X, Out)$ を引き出せる．このとき，$Card_i$ は $\theta(i, Y)$ を X ポイント減少する（$\theta(i, (Y-X)$ となる）．一方，カード発行者 C のみが $Card_i$ の $\theta(i, Y)$ を L ポイント増加する情報 $\theta(i, L, In)$ を生成できる．ここで，$Card_i$ と C は共通鍵 $CKey_{iC}$ を共有し，$\theta(i, X, Out)$ と $\theta(i, L, In)$ の生成と検証に $CKey_{iC}$ を用いる．$Card_i$ は $CKey_{iC}$ により生成されない $\theta(i, L, In)$ を拒絶する．PR を再利用されないために，電子マネー等で行われているように，C において二重使用の検査を行うものとする．

《相互通信モデル》

公開鍵ディレクトリサービス等の請求ノード R に対して提供ノード P が機能を提供するモデルである．R がノードまたは証明書等を P に求め，P が請求された証明書等を R に与え，R は対価として RP を P に与える．なお，R と P は相互認証済みで共通鍵 $CKey_{PR}$ を共有する．

Step1：R は請求 List，それを対象とする $AInfo_{RP}$，ID_R，ID_P を P へ送る．なお，請求 List は証明書であれば Subject を含み，他のブラックリスト等のデータを請求する場合は，それらの名称を含むものとする．

Step2：P は $AInfo_{RP}$ を検証し，提供可能 List，それを対象とする $AInfo_{PR}$，ID_P，ID_R，R へ送る．なお，提供可能 List は請求リストのうち提供可能な証明書の Subject 等を含むリストである．

Step3：R は $AInfo_{PR}$ を検証し，提供可能 List を確認し，$Card_R$ から提供可能 List に応じたポイント T の $\theta(R, T, Out)$ を引き出し，$\theta(R, T, Out)$，それを対象とする $AInfo_{RP}$，ID_R，ID_P を P に送る．なお，データに応じたポイントは事前に決定し，これをノードは仲介ノードを介してシステム管理者 M から受け取り済みとする．

Step4：P は $AInfo_{RP}$ を検証し，提供可能 List に対応するデータのうち保有するデータ，それを対象とする $AInfo_{PR}$，ID_P，ID_R，を R へ送り，$\theta(R, T, Out)$，それを対象とする $AInfo_{Pj}$，ID_P，ID_j を j へ送る☆．

Step5：R は $AInfo_{PR}$ を検証し，データを受領する．

Step6：j は $AInfo_{Pj}$ を検証し，$\theta(R, T, Out)$，それを対象とする $AInfo_{jM}$，ID_j，ID_M を M に送る☆．

Step7：M は $AInfo_{jM}$ を検証し，$\theta(R, T, Out)$ をカード発行者 C に送り，C から $\theta(P, T, In)$ の発行を受け，$\theta(P, T, In)$，それを対象とする $AInfo_{Mj}$，ID_M，ID_j を j に送る．ただし，C は $\theta(R, T, Out)$ が不正なことを検知した場合は M に通知する．

Step8：j は $AInfo_{Mj}$ を検証し，$\theta(P, T, In)$，それを対象とする $AInfo_{jP}$，ID_j，ID_P を P に送る．

Step9：P は $AInfo_{jP}$ を検証し，$\theta(P, T, In)$ を $Card_P$ に入力し，$\theta(P, Y)$ を増加させる（$\theta(P, (Y+T))$ となる）．

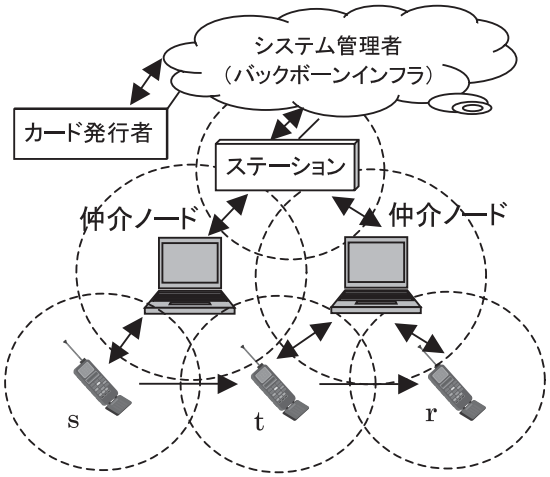

図 5 インセンティブ機能の一方向通信モデル：ノード s からノード t を経由したノード r への送信

Fig. 5 A one-way communication model of an incentive mechanism: Transmission from node s to node r via node t.

《一方向通信モデル》

送信ノード s が対価として RP を添付したメッセージ Message の転送を転送ノード t に求め，t が受信ノード r へ転送を行い，r が RP を仲介ノード j に送付することで，t が RP を得るモデル（**図 5**）である．これは Packet Purse Model[2] とほぼ同じであるが，「事前に r までのホップ数が不明な☆☆ために添付する RP が確定困難」という問題[2] を解決するため，提案機構は，s が平均的に予想されるホップ数に $+\alpha$ を加えたポイント W を添付し，余りの RP を j 経由で s へ返却する RP 返却機能，s と r 間でのメッセージ認証・暗号化機能☆☆☆を備える．s と r 間は相互認証済み，かつ共通鍵 $CKey_{sr}$ を共有済み．簡単化のため，転送ノードが 1 台の場合を説明する．

Step1：s は $Card_s$ からポイント W の $\theta(s, W, Out)$

☆ 受信後即送信せず，一定量 RP が貯まってから一括請求する．

☆☆ たとえば DSR[9] はメッセージ送信前にホップ数が決定しているが，AODV[13] のように事前に決定できないものもある．

☆☆☆ 共通鍵暗号としてブロック暗号，ストリーム暗号のどちらを用いるかは，インセンティブ機能の本質でないためスコープ外とする．

を引き出す．Message を暗号化した暗号文 Enc_s とハッシュ値 $Hash_s$（$= H(Enc_s)$）を生成し，$ID_s \| ID_t \| ID_r \| Hash_s \| \theta(s, W, Out) \| W$ を $Header_s$ とし，$Header_s$，それを対象とする $AInfo_{sj}$ と $AInfo_{sr}$，Enc_s を t へ送る．

Step2：t は $H(Enc_s)$ を計算し，$Hash_s$ と等しいことを検証し，$W \leftarrow W-1$ とし，$D_s \| ID_t \| ID_r \| Hash_s \| \theta(s, W, Out) \| W$ を $Header_t$ とし，$Header_t$，それを対象とする $AInfo_{tj}$，$AInfo_{sj}$，$AInfo_{sr}$，Enc_s を r へ送る☆．なお，転送ノードが複数の場合，r に代えて次転送ノード宛てに送信し，次ノードが r になるまで Step2 を繰り返す．

Step3：r は $H(Enc_s)$ を計算し，$Hash_s$ と等しいことおよび $AInfo_{sr}$ を検証し，Message を復号し，$ID_s \| ID_t \| ID_r \| Hash_s \| \theta(s, W, Out) \| W$ を $Header_r$ とし，$Header_r$，それを対象とする $AInfo_{rj}$，$AInfo_{sj}$，$AInfo_{tj}$ を j へ送る．

Step4：j は $AInfo_{sj}$ と $AInfo_{tj}$ と $AInfo_{rj}$ を検証し，$ID_s \| ID_t \| ID_r \| ID_j \| Hash_s \| \theta(s, W, Out)$ を $Header_j$ とし，$Header_j$，それを対象とする $AInfo_{jM}$ を M へ送る．

Step5：M は $AInfo_{jM}$ を検証し，$\theta(s, W, Out)$ を C へ送り，$\theta(t, W_t, In)$ と $\theta(r, W_r, In)$ と $\theta(s, W_s, In)$ ☆☆の発行を受ける．なお，$W = W_t + W_r + W_s$ とする．C は $AInfo_{jM}$ および $\theta(s, W, Out)$ が不正の場合は発行しない．次に，$ID_M \| ID_j \| \theta(t, W_t, In) \| \theta(r, W_r, In) \| \theta(s, W_s, In)$，それを対象とする $AInfo_{Mj}$ を j へ送る．

Step6：j は $AInfo_{Mj}$ を検証し，$ID_j \| ID_t \| \theta(t, W_t, In)$ とそれを対象とする $AInfo_{jt}$，$ID_j \| ID_r \| \theta(r, W_r, In)$ とそれを対象とする $AInfo_{jr}$，$ID_j \| ID_s \| \theta(s, W_s, In)$ とそれを対象とする $AInfo_{js}$ をそれぞれ t，r，s へ送る．

Step7：t，r，s はそれぞれ $AInfo_{jt}$，$AInfo_{jr}$，$AInfo_{js}$ を検証し，$\theta(t, W_t, In)$，$\theta(r, W_r, In)$，$\theta(s, W_s, In)$ を，それぞれ $Card_t$，$Card_r$，$Card_s$ へ入力し，各 Card の保存する RP を増加させる．

転送ノード t が次ノードへ転送ができない場合，添付の RP と認証情報を，仲介ノード j 経由でシステム管理者 M へ送信する．M はそれらを検証後，RP の一部とその残りをカード発行者により，それぞれ t と送信ノード s が扱える形に変換してもらい，それぞれを j 経由で t と s へ送ることで，RP の紛失を防ぐことができる．

ノード s，t，r が仲介ノード j に認証情報を送る Step において s，t，r と j 間の通信がマルチホップである場合，認証情報を提出するモチベーションを高めるため，システム管理者は RP 返却機能を用いて s，r，t が認証情報の送信に要した RP を返却する．

3.4 その他の機能

PKI 補助機能における不正ノード情報および，インセンティブ機能における認証情報は，仲介ノード等を介してシステム管理者 M に集約される．M は両機能に対する不正ノードを検出・特定後，安全性向上のために共通ブラックリストを生成し，これを仲介ノード経由で一般ノードに配布し，各ノードがリストに掲載されたノードとの接続を拒否することで，不正ノードを排除する．

仲介ノード j への登録時に，j はオンラインで CRL（Certificate Revocation List）を検査できないため，RP の請求時に，j は M に検証済みノード証明書を提出し，M が CRL を検査して該当する場合は，j と該当証明書に対応するノードと相互認証を行ったノードへ CRL を検査した結果を通知する．M はつねに CRL 検査が可能である．M は TTP であり，その証明書の失効する可能性が低く，j は M の証明書を CRL により検査しない．

4. 評　　価

4.1 目標達成の確認

2.2 節の目標が達成されていることを確認する：

(1) PKI により実現した仲介ノード経由でバックボーンインフラ BI が不正ノード情報と認証情報を収集するため，メッセージが BI を経由する必要がなく，ルーティング方式も限定しないため自由度が高い．

(2) 両機能に必要な仲介ノードへの登録は一括で可能であり，仲介ノードを介した不正ノード情報と認証情報収集・ブラックリスト生成機能も共用できる．また，両機能のブラックリスト共用により，不正ノード情報を効率的に配布し，安全性が向上する．

以上より，提案機構は 2 つの目標を達成している．また，PKI 補助機能に必要なインセンティブ機能として，仲介ノード等の検証時に必要な情報の入手に利用可能な相互通信モデルを，インセンティブ機能に必

☆ ステーション以降のネットワークがマルチホップ通信に対応していない場合（固定電話網等）はインセンティブ機能が不要となるため，M にて直接 Step5 と同様に RP の清算処理を実施する．

☆☆ システムにおいて事前に決定された W_t と W_r を W から引いた残りのポイントとなるため，存在しない場合もありえる．ただし，残りポイントが負の値になることは想定しない．

要な PKI 補助機能として，一方向通信モデルの送信ノードと受信ノードの事前鍵共有に必要な相互認証および鍵共有の補助機能を用意し，必要な機能を明確にした．

4.2 性質満足の確認

2.2 節の性質が満たされていることを確認する．

4.2.1 性　　能

《接続性》

PKI 補助機能の有無ごとに，検証処理が実行可能な確率（実行確率 P）を算出し，比較する．実行確率は証明書の検証に必要な CA 証明書を保持または入手可能であり，検証処理が実行できる確率を示す．ノード A と B の相互認証（実行確率を P_{AB} とする）は，システム管理者 M と仲介ノード E の相互認証（P_{ME}），M と仲介ノード F の相互認証（P_{MF}），E と A の相互認証（P_{EA}），F と B の相互認証（P_{FB}）に分けられる．検討を簡単にするため，E と F，A と B のリソースが等しいとし，それぞれを j，i で表し，P_{Mj} ($= P_{ME} = P_{MF}$)，P_{ji} ($= P_{EA} = P_{FB}$) とすることで，P_{AB} を P_{Mj} と P_{ji} で表す．P_{Mj} は M が j の証明書を検証する確率（$P1_{Mj}$）と，j が M の証明書を検証する確率（$P2_{jM}$）に分けられる．P_{ji} は j が i の証明書を検証する確率（$P1_{ji}$）と i が j の証明書を検証する確率（$P2_{ij}$）に分けられる．以上より，P_{AB} は次式で表せる．

$$P_{AB} = P_{Mj}^2 \times P_{ji}^2 = P1_{Mj}^2 \times P2_{jM}^2 \times P1_{ji}^2 \times P2_{ij}^2$$

2 章の定義より $P1_{Mj} = P2_{jM} = 1$．また，$P1_{ji}$ は次の理由によりほぼ確率 1 と期待する．(1) j は多くリソースを有する．(2) i は他の仲介ノードから一時ノード証明書を発行されている可能性がある．(3) j は他の仲介ノードから CA 証明書の提供を受けられる可能性がある．よって，$P_{AB} \fallingdotseq P2_{ij}^2$ となり，P_{AB} は $P2_{ij}^2$ に帰着する．

一方，PKI 補助機能がない場合の実行確率は，A が B の証明書を検証する場合の実行確率 P_{AB}' と等しい．つまり，P_{AB}' は B 以外に検証対象ノードを変更できないために実行確率が固定的に決定するのに対し，$P2_{ij}$ は異なる仲介ノードを選択すること，および i が認証済みの他ノードから CA 証明書の入手が期待でき，P_{AB}' より実行確率を向上できる．以上より接続性を満たす．

《効率性》

提案機構と，同様にセルラネットを想定し，効率性の高い方式[14] を**表 1** に比較する．頻繁に行われるメッセージの転送時に 1 メッセージに追加するデータ量と，各ノードの総演算量，受信ノードからシステム管理者への完了通知のデータ量とその生成に必要な演算量を比較する．方式 14) は 1 セッションごとにセッション確立処理を，提案機構はシステム使用開始時に仲介ノードへの登録処理を要するが，これらは実施回数が異なると予想され，比較しない．方式 14) に合わせて，一方向性ハッシュ関数の出力は 16 Byte，ID は 4 Byte，カウンタは 2 Byte とする．なお，F を転送ノード数，1 メッセージの総パケット数を U とする．RP については HMAC により生成されると想定して 16 Byte として扱う．

表 1 提案機構と方式 14) の通信量・演算量比較
Table 1 Comparisons between our proposed scheme and a scheme 14).

		メッセージに追加されるデータ量 [Byte/Message]	メッセージ転送に要する総演算量 [ハッシュ回数/Message]
転送処理	提案機構	79+21F	5+2F
	方式[14]	22U	U
完了処理	提案機構	77+21F	4
	方式[14]	38U	U

表 1 より大きなサイズのメッセージを送る場合は提案機構が有利となり，ホップ数の大きくなるノードと通信する場合は方式 14) が有利となることが分かる．一般に通信量は年々大きくなることと，ホップ数の多い場合はステーションを利用可能な場合もあることから，提案機構の方が有利といえる．また，提案機構はルーティング方式への依存を避けるためセッション層での実装を想定し，方式 14) はルーティング方式に依存するためネットワーク層での実装と予想される．セキュリティ機能は，ルーティング方式の確定後に追加されることが多く，セッション層を想定する方が実用的である．

4.3 安　全　性

攻撃者を以下の目的を持つノードと定義する：

- RP を不正取得する，または RP を不正に払わない．
- 他ノードに対する RP の取得妨害．
- 任意のノードまたはステーションへのなりすまし．
- 不正なノード間協調の拒否．

攻撃者は通信の盗聴と任意データの送信が可能だが，Card および BI への攻撃は困難であるとする．

《検証性》

仲介ノードの認定および仲介ノードへの登録は，PKI による相互認証を行い，その公開鍵を用いて共通鍵を共有するため，なりすましや共通鍵の不正取得は困難である．PKI 補助機能は，前記共通鍵により相互認証

表 2 攻撃の検出に必要な AInfo と Header の種類
Table 2 Kinds of AInfo and Header to detect attaks.

攻撃＼ログ				攻撃の検出に使用可能な AInfo と Header		
種別	内容	被害ノード	攻撃ノード	送信ノード	転送ノード	受信ノード
不正な RP 取得	非存在メッセージに対する RP の請求	送信ノード	転送ノード	○	○	○
			受信ノード	○	○	×
			転送・受信ノード	○	×	×
	メッセージを転送せずに RP を請求	送信ノード	転送ノード	○	○	○
			受信ノード	そもそも転送しない		
			転送・受信ノード	○	○	×
RP 取得妨害	認証情報を削除	転送ノード	送信ノード	認証情報を削除困難		
			転送ノード	×	○	×
			受信ノード	×	○	×
RP を不払い	不正な RP を添付	転送・受信ノード	送信ノード	カード発行者により不正 RP を検出可能		
転送を不正に停止	メッセージを転送しない	送信ノード	転送ノード	×	○	×
	RP と，対応する認証情報を削除	送信ノード	転送ノード	×	○	×

と新規共通鍵の共有を行うため，同様になりすましや新規共通鍵の不正取得は困難である．なお，通信時に共通鍵が正しいことは確認可能なため，別途確認処理は設けないが，容易に追加可能である．また，公開鍵ディレクトリサービスでは，要求と異なる情報が提供された場合，システム管理者 M へ通知される．

相互通信モデルでは，提供ノード P が請求ノード R から RP を受信後に請求されたデータを提供しない場合と，P が受信した RP が不正の場合がある．前者は P が仲介ノード j 経由で M へ不正を通報でき，後者は M からカード発行者へ PR を送る際に不正を検出できる．

一方向通信モデルでは，M が送信ノード s，転送ノード t，受信ノード r から収集したログ（Header, AInfo）を，対応する共通鍵を用いて比較し，不正を検出できる．

表 2 に想定する攻撃と，攻撃検出に必要なログを示す．攻撃が検出可能なときは○を，困難なときは×を記す．表 2 より提案機構が検出性を満たす（想定する全攻撃を防ぐ）には，デフォルトの受信ノードのログと別に，送信ノードと転送ノードのログを収集する必要があることが分かる．また，提案機構はルーティングの自由度が高く，RP 取得のみを目的として不必要にルートに入り，中継ノードとして RP を蓄積する攻撃が考えられる．しかしながら，この攻撃において不正な中継ノードは通常のコスト（CPU パワーおよび電力の消費）で RP を取得しているため，提案機構で想定する程度の RP の価値では，攻撃のモチベーションは高くないと予想される．ただし，より高い価値を RP に与える場合は，同様の攻撃を検出する方式 5), 7) 等を利用して防御する必要がある．

《結託耐性》

ノードはシステムの秘密情報を持たず，かつノードの秘密鍵は他ノードの秘密鍵と関連性がなく，結託によりシステム全体をブレイクするのに必要な情報量は増加しない．以上より，提案機構は結託耐性を持つ．

《追跡性》

提案機構は仲介ノードへの登録が必要であるため，基本的には不正ノードを事後に追跡できる．仲介ノード自体はシステム管理者へ登録されるため，不正仲介ノードも追跡できる．ただし，転送ノードとして仲介ノードが不参加のメッセージ転送において，転送ノードが転送メッセージを改ざんした場合，その転送ノードと次の転送ノードのどちらが攻撃者か区別できない．しかしながら，攻撃者が 2 回以上攻撃を繰り返した場合は，攻撃者は候補として 2 回以上追跡されることになり，その候補は攻撃者である疑いが大幅に高まっていく．したがって，十分に攻撃の抑止効果が期待できる．

4.4 他方式との比較

提案機構はインセンティブ・PKI 補助の両機能の補完関係を考慮して設計された唯一の方式のため，機能ごとに他方式との比較を行う．ここで，論文 X) に示される方式を方式 X) と表記する．また，提案機構以外にセルラネットに適用可能な PKI 補助機構が存在しないため，公平性を期すためにサーバ—クライアントモデルにおいてよく知られた方式 11) も比較の対象とする．

《PKI 補助機能の比較》

表 3 より，提案機構は，すべての機能を満足し，かつ一般ノードへの負荷も小さいため，セルラネットが想定可能な場合は従来方式より優れていることが分かる．

《インセンティブ機能の比較》

表 4 より，提案機構は，ノード自身がポイントを管理でき，かつルーティング方式に依存しないことが分かる．また PKI を利用できるため，他ネットワークへの接続が容易であり，他方式より汎用性に優れる．一方，処理負荷は，PKI と共通鍵暗号のハイブリッド使用により，PKI のみを使用した方式や，監視を行う方式と比較して少ない．

表 3 提案機構と他方式の PKI 補助機能の比較
Table 3 A comparison between our proposed scheme and other PKI-supporting mechanisms.

	機能			性能		
	証明書		認証補助	システム	処理主体	一般ノードの処理負荷
	発行管理	配送				
提案機構	○	○	○	セルラネット	特権ノード	特権ノードが処理するため小さい
方式[11]	×	×	○	サーバークライアント	サーバ	サーバが処理するため小さい
方式[4] 方式[6]	○	○	○	アドホックネット	一般ノード	一般ノードが処理するため大きい
方式[10] 方式[16] 方式[17]	○	○	×	アドホックネット	特権ノード	複数特権ノードに接続が必要なため大きい
方式[15]	×	×	○	アドホックネット	一般ノード	他ノード集合への同報通信が頻発するため大きい

表 4 提案機構と他方式のインセンティブ機能の比較
Table 4 A comparison between our proposed scheme and other incentive mechanisms.

	システム	ポイント保管場所	負荷を決定する技術	ルーティング方式
提案機構	セルラネット	TRM	PKI と共通鍵暗号の併用	制限無し
方式[2] 方式[3]	アドホックネット	TRM	TRM	不明
方式[8] 方式[14]	セルラネット（制約あり）	口座	共通鍵暗号	ソースルーティング
方式[18]	アドホックネット	不明	PKI	ソースルーティング
方式[1] 方式[12]	アドホックネット		監視	ソースルーティング

5. ま と め

本論文では，マルチホップセルラネットワークに適した，インセンティブ機能と PKI 補助機能を同時に提供するセキュリティ機構を提案した．提案機構は，仲介ノードにより，従来は個別に研究されてきたインセンティブ・PKI 補助の両機能を統合的に提供することが可能であり，かつ従来方式と比較してルーティングの自由度が高いことを特徴とするものである．

参 考 文 献

1) Buchegger, S. and Boudec, J.Y.L.: Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in dynamic ad-hoc networks, *Proc. IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing*, IEEE (2002).
2) Buttyan, L. and Hubaux, J.P.: Enforcing service availability in mobile ad-hoc WANs, *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing* (2000).
3) Buttyan, L. and Hubaux, J.P.: Stimulating cooperation in self-organizing mobile ad hoc networks, *ACM Journal for Mobile Networks, special issue on Mobile Ad Hoc Networks* (2002).
4) Capkun, S., Buttyan, L. and Hubaux, J.P.: Self-Organized Public-Key Management for Mobile Ad-Hoc Networks—Abstract, *Report on a Working Session on Security in Wireless Ad Hoc Networks, ACM Mobile Computing and Communications Review* (*MC2R*), Vol.6, No.4 (2002).
5) Capkun, S., Buttyan, L. and Hubaux, J.P.: SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks, *ACM Workshop on Security of Ad Hoc and Sensor Networks* (*SASN '03*) (2003).
6) Hubaux, J.P., Buttyan, L. and Capkun, S.: The Quest for Security in Mobile Ad Hoc Networks, *Proc. ACM Symposium on Mobile Ad Hoc Networking and Computing* (2001).
7) Hu, Y.C., Perrig, A. and Johnson, D.B.: Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, *Proc. 2nd ACM Workshop on Wireless Security* (2003).
8) Jakobsson, M., Hubaux, J.P. and Buttyan, L.: A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, *Proc. 7th International Financial Cryptography Conference* (2003).
9) Johnson, D.B., Maltz, D.A. and Hu, Y.-C.: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), ITERNET-DRAFT, draft-ietf-manet-dsr-09.txt, IETF MANET Working Group (April 2003).
10) Kong, J., Zerfos, P., Luo, H., Lu, S. and Zhang, L.: Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks, *Proc. 9th International Conference on Network Protocols* (*ICNP*) (2001).
11) Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP, RFC2560, IETF Network Working Group (1999).
12) Marti, S., Giuli, T., Lai, K. and Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks, *Proc. 6th International Conference on Mobile Computing and Networking 2000* (2000).
13) Perkins, C., Belding-Royer, E. and Das, S.: Ad hoc On-Demand Distance Vector (AODV) Routing, RFC3561, IETF Network Working Group (2003).

14) Salem, N.B., Buttyan, L., Hubaux, J.P. and Jakobsson, M.: A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular NetWorks, *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing* (2003).
15) Weimerskirch, A. and Thonet, G.: A Distributed Light-Weight Authentication Model for Ad-hoc Networks, *Information Security and Cryptology-ICISC2001* (2001).
16) Yi, S. and Kravets, R.: Key Management for Heterogeneous Ad Hoc Wireless Networks, Technical Report UIUCDCS-R-2002-2290/UILU-ENG-2002-1734, University of Illinois at Urbana-Champaign (2002).
17) Zhou, L. and Haas, Z.: Securing Ad Hoc Networks, *IEEE Network*, Vol.13, No.6, pp.24–30 (1999).
18) Zhong, S., Yang, Y.R. and Chen, J.: Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad Hoc Networks, Technical Report Yale/DCS/TR1235, Department of Computer Science, Yale University (2002).

(平成 16 年 3 月 31 日受付)
(平成 16 年 10 月 4 日採録)

安齋 潤

平成 8 年東海大学工学部通信工学科卒業．同年松下通信工業株式会社入社（現パナソニックモバイルコミュニケーションズ株式会社）．平成 14 年 10 月より横浜国立大学環境情報学府博士後期課程在学．平成 15 年よりパナソニック MSE 株式会社へ出向．携帯電話のセキュリティソフトウェアの開発に従事．電子情報通信学会会員．

松本 勉

昭和 61 年 3 月東京大学大学院博士課程（電子工学）修了．工学博士．同年横浜国立大学工学部専任講師．現在，同大学大学院環境情報研究院教授．昭和 56 年より，暗号・電子署名のアルゴリズムとプロトコル，ディジタル証拠性，耐タンパソフトウェア，情報ハイディング，ネットワークセキュリティ，認証方式，バイオメトリクス，人工物メトリクス等の各種情報セキュリティ技術の研究教育とその実応用に力を注ぐ．昭和 57 年に「明るい暗号研究会」を数人の仲間とともに創り研究をはじめた．国際暗号学会 IACR 理事．CRYPTREC 暗号モジュール委員会委員長．電子情報通信学会より「情報セキュリティの基礎理論」への貢献に関して業績賞を受賞．