6 情報共有空間のためのモバイルアドホックネットワーク

高橋　修　公立はこだて未来大学

はじめに

移動する情報機器による情報共有空間の通信の基盤となるモバイルアドホックネットワークについて解説する．街角やイベント会場，あるいは渋滞中の車同士で携帯電話やPDAなどの携帯端末を持ち運びながら，いつでも，どこでも，誰とでも通信を行ったり，あるいは災害などにより通信インフラが利用できなくなった時の緊急通信手段として，モバイルアドホックネットワークが重要な役割を果たすと期待されている．

本稿では，モバイルアドホックネットワークで情報共有する場合にネットワーク構成方式として，モバイルアドホックネットワークのためのルーティングプロトコルの特徴と代表的なルーティングプロトコルについて解説する．さらに，普及する上で避けて通れない重要なセキュリティ課題として，アドホックネットワークに特有な脅威とその対策について体系的に解説するとともに，最近の研究動向についても紹介する．

情報共有空間のための モバイルアドホックネットワーク

モバイルアドホックネットワークは，無線通信とネットワーキングの能力を備えた複数の端末から構成される．それらの端末は，その無線範囲内の端末や無線範囲外の端末と通信が可能である．後者の場合，送信されたパケットは，複数の端末によって中継され宛先まで届けられる（マルチホップ通信）．各端末は，新たにネットワークに参加したり，移動により無線範囲から離れたり，電力切れ，あるいは異常終了などに伴い離脱したりして，「その場限り」の通信を実現することによって情報共有空間を形成する．

このように，モバイルアドホックネットワークを利用すると，固定の無線基地局，電話線や固定ルータなどの通信インフラを必要とせずに，端末だけで情報共有空間をいつでもどこでも手軽に形成できるのが特徴である．モバイルアドホックネットワークにより情報共有空間を形成するためには，以下の2つが重要な技術課題となる（図-1）．

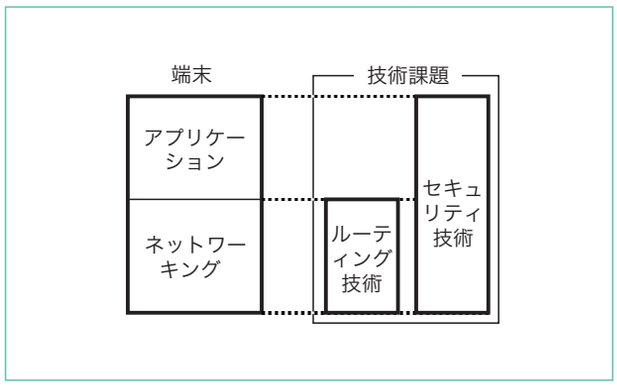


図-1　モバイルアドホックネットワークによる情報共有空間の実現課題

(1) モバイルアドホックネットワークのルーティングプロトコル

モバイルアドホックネットワークでは，端末は絶えず移動などによりネットワークへの参加／離脱を行うため，情報共有空間を形成する端末は，他の端末を検出して通信に必要なハンドシェイクや，リンクの接続性を反映して経路情報を変化させなければならないためルーティングプロトコルに工夫が必要である．

(2) モバイルアドホックネットワークセキュリティ

管理運用面から見たモバイルアドホックネットワークは，

1) 電波を利用しているため，情報は無線到達範囲内で傍受可能であること
2) その場限りのネットワークであるので一般に管理者はいないこと
3) パケットを中継するのは，第三者（他人）であること

が特徴となり，情報共有空間を形成するためには新しい観点からのセキュリティ対策が必要である．

以下では，アドホックネットワークのルーティングプロトコルとセキュリティの技術動向について概説する．

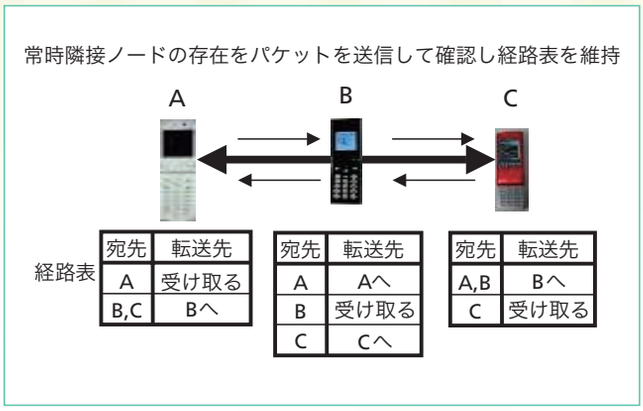


図 -2　プロアクティブ型ルーティングプロトコル

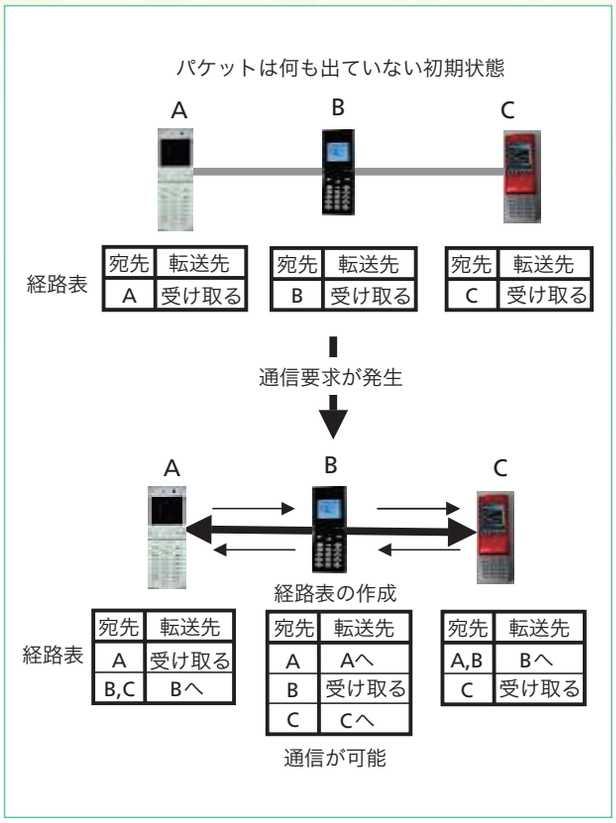


図 -3　リアクティブ型ルーティングプロトコル

モバイルアドホックネットワークのルーティングプロトコル

●概要

モバイルアドホックネットワークに利用されるルーティングプロトコルの特徴は，有線ネットワークのルーティングプロトコルと違って，隣接に存在する端末が不明なために宛先（目的）端末までのルートを探す必要があること，またモバイル端末は時間とともに移動するためいったん設定したルート上の端末が時間とともに変更するところにある．モバイルアドホックネットワークのためのルーティングプロトコルには，通信路の設定方式によりプロアクティブ型，リアクティブ型，およびそれらの混合型に分類できる．

プロアクティブ型のプロトコルは，モバイルアドホックネットワーク上の各々の端末から他のすべての端末への，矛盾のない最新のルーティング情報をあらかじめ維持する（図 -2）．このため，各端末はルーティング情報を格納するための経路表（テーブル）を 1 つ以上持ち，端末が移動する等によってネットワークの構造（トポロジ）が変化するのに伴って，ネットワーク全体の経路情報を各端末相互間で送受信することによってルーティング情報を更新する．このため，テーブル駆動型プロトコルともいわれる．

リアクティブ型ルーティングプロトコルは，送信元端末が要求したときのみ経路を作成する．送信元が宛先端末への経路が必要になったときに，経路を探査し，いったん経路が発見，確立されると，宛先への経路は不用になるまで，何らかの手段でその経路を維持する（図 -3）．このため，リアクティブ型プロトコルは，オンデマンド型プロトコルともいわれる．

さらに，ハイブリッド型ルーティングプロトコルは，上記 2 方式を組み合わせて，時間的あるいは，空間的に使い分ける方式である．

これらのルーティングプロトコルは，端末数や，端末密度，端末の移動速度などにより適用領域があり，たとえば，リアクティブ型のプロトコルは，定期的な制御オーバーヘッドは発生しないため，大規模かつ低密度で端末の移動速度が遅いネットワークに適している．現在のところ，まだあらゆる状況に効率よく適用できる万能なプロトコルはまだ存在していない．また，モバイルアドホックネットワークのためのルーティングプロトコルの標準化は，IETF（Internet Engineering Task Force）で検討されており，RFC（Request For Comment）となっているものもあるが，いずれもまだ“実験的”なものであり，検討が継続されている．

●プロアクティブ型プロトコル

プロアクティブ型プロトコルの代表的なプロトコルとして，IETF で標準化されている OLSR（Optimized Link State Routing Protocol）[1] がある．OLSR で定義されるパケットには，HELLO メッセージ，TC（Topology Control）メッセージなどがある．HELLO メッセージは，ネットワーク内で各端末の持つ情報の交換を目的として，隣接端末間で定期的に送受信され，周辺情報の収集に使用される．具体的には，各端末で管理されているローカルリンク情報（リンク集合，隣接端末集合，など）を構

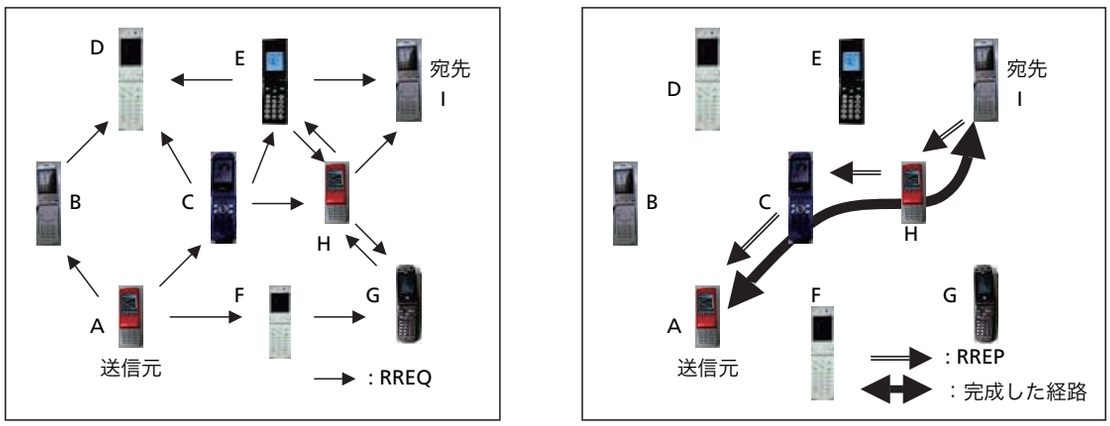


図 -4　AODV における経路の設定（通常動作）

築するために，隣接端末間で互いに自端末の情報を交換する．このメッセージにより，自分の周辺にどんな端末がいるのかを把握することが可能となる．また，TC メッセージは，HELLO メッセージで収集したローカルリンク情報を，各端末がネットワーク全体の他端末にフラッデング（一斉配信）することによって，ネットワーク全体のトポロジを知らせるために使用される．各端末は，受信したトポロジ情報を基にして実際の通信経路（最短路）を計算し，経路表を作成する．

また，OLSR では，MPR（MultiPoint Relay）集合という端末の集合を定義し，MPR のみがフラッディングを行うことで，無駄な再送信端末数を削減することによって効率的に行うことを可能としているのが特徴である．

●リアクティブ型プロトコル

リアクティブ型プロトコルの代表的なプロトコルとして，IETF で標準化されている AODV（Ad hoc On-Demand Distance Vector（AODV）Routing）[2] がある．AODV で定義されている制御メッセージには，RREQ（Route Request），RREP（Route Reply）メッセージ，RERR（Route Error）などがある．また，OLSR と同様の HELLO メッセージが RREP メッセージの 1 つ（オプション）として定義されている．RREQ メッセージは，新しい送信先への経路が必要になったとき，その経路を見つけるために送信（フラッディング）される．目的（宛先）の端末に RREQ メッセージが届くと，目的端末は RREP メッセージを送信元に送信（ユニキャスト）する．RREP メッセージの転送には，双方向の経路を作成するため，RREQ メッセージの転送時に作られた経路が用いられる．これらのメッセージのやりとりによって，中間に位置する端末の経路表に，送信元と宛先の経路情報が作成され，以降はこの経路表を利用してルーティングが可能となる（図 -4）．

RREQ メッセージは，ネットワークにフラッディングされるが，OLSR と同様に効率的に行うための工夫がしてある．具体的には，目的の端末がすぐ近くにいるかもしれないので，最初は再転送するホップ数を制限することで探索範囲を限定し，それで見つからなかった場合には徐々に探索する範囲を広げていく“expanding ring serch”という方式を採用している．

モバイルアドホックネットワークのセキュリティ

●アドホックネットワークに特徴的な脅威

モバイルアドホックネットワークの運用管理面では，1）傍受されやすいこと，2）ネットワークの管理者はいないこと，3）第三者（他人）経由でパケットが中継されること，が特徴になり，それらを考慮してセキュリティを検討する必要がある．上記のうち，1）に関する事項は，暗号技術を送受信者相互間で適用すれば解決可能であるが，2），3）に関しては，ルーティングプロトコルに密接に関連し，やっかいな問題となる．本章では，モバイルアドホックルーティングプロトコルに関する攻撃方法とそれに対する防御方式を中心に基本方式や研究動向について概説する．

●脅威とその検出・防御

モバイルアドホックネットワークを利用して，情報共

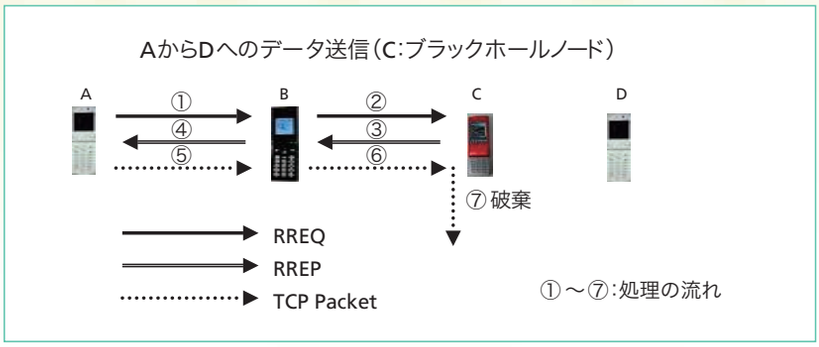


図 -5　ブラックホール攻撃の実際の動作例（AODV）

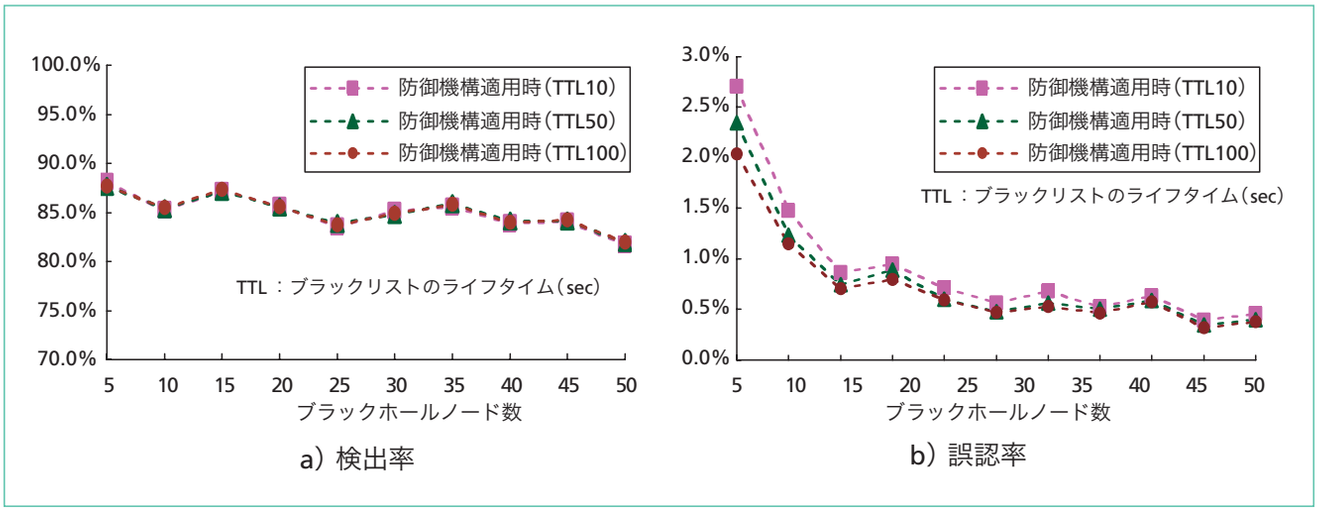


図 -6　ブラックリストによる検出能力評価結果例（AODV）

有空間を構築する際に脅威となる攻撃方法とその検出・防御方式をその特性から大きく 4 つに分けて概説する．

(1) 経路表攻撃

攻撃者はある端末になりすまし，経路表を構成するための制御情報を送受信するメッセージ（たとえば，OLSR なら TC メッセージ，AODV ならば HELLO メッセージ）を偽造して送ることによって，受信端末側に不正な経路表を作成させ，ルートを破壊することによって通信不能とする [3]．

防御方法は，パケットをすべて暗号化したり，すべてのパケットにディジタル署名を付与することによって可能であるが，PKI 基盤をモバイルアドホックネットワークに導入することは現実的には困難である．厳密な方法ではないが，たとえば TCP の ACK パケットのような End-End レベルの情報を利用したり，あるいは，端末ごとに評価関数（信頼度）を定義して，域値以下の信頼度と評価されている端末は，ルートから除外する方式などがある [3]．

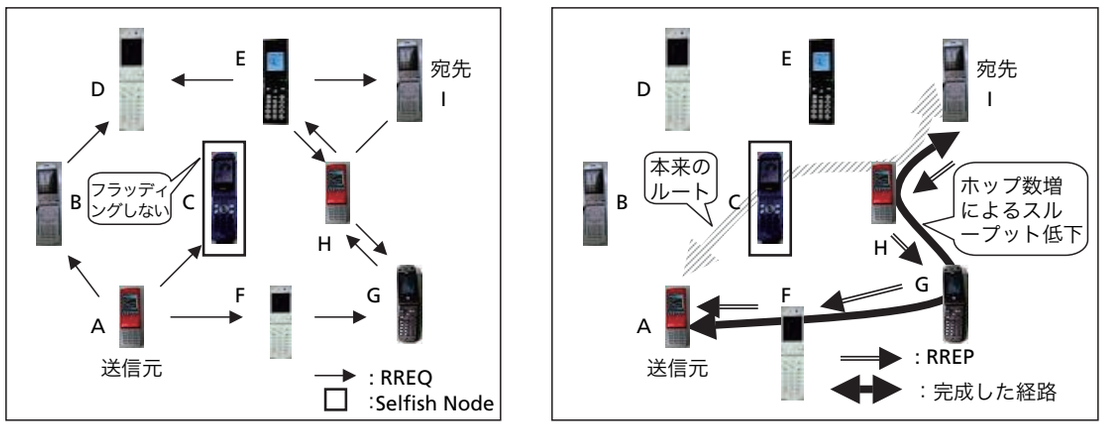
(2) 落とし穴攻撃

攻撃者が隣接端末に対し，自分を中継するようなルートの構築／再構築を促すようにして，何らかのかたちで攻撃者が送受信端末間のルートを構成する中継端末として加わり，情報パケットを破棄したり，改ざんしたりする攻撃である．たとえば，AODV のような距離ベクトルを利用するルーティングプロトコルの場合は，ホップカウントを詐称し，偽の RREP を送信することで実現できる．典型的には，すべてのパケットを破棄するブラックホール攻撃 [4]（図 -5），選択的に破棄するグレーホール攻撃，複数の攻撃端末が共謀して外部リンクにデータを転送するワームホール攻撃 [5] などが知られている．

防御方式としては，ルート上の各端末が攻撃特有の行動（たとえば，RREP の送信方法）を監視し，異常を検出した端末が，何らかのかたちで他の端末か送信元端末に報告し，攻撃端末を避けるようにルートの再設定を行う方式など [4), 6] と，ルート上の各端末は通信ログ情報を送信元端末に送り，これらの統計情報から送信元端末が攻撃端末を検出し，攻撃端末を避けるようルートの再設定を行う方式など [3] がある．前者の方式の 1 つで，ブラックリストにより動作パターンを特定して検出した場合のシミュレーションによる評価例を図 -6 に示す [4]．

(3) セルフィッシュ動作攻撃

パッシブな攻撃方法で，攻撃者は，自身のバッテリや



a）RREQメッセージのフラッディング　　b）RREPメッセージの返信

図 -7　AODV における経路の設定（C が Selfish Node 動作）

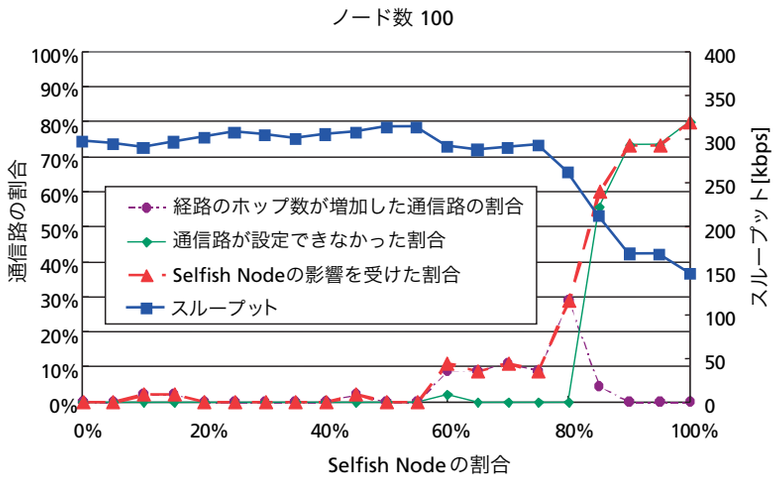


図 -8
Selfish Node のネットワークへの影響評価例（AODV）

計算資源の節約のため，自分自身が送受信先となるパケットは扱うが，それ以外のルート検索や中継処理を行わない攻撃である（図 -7）．この場合，代替ルートが見つからず通信ができないか，迂回する代わりのルートが見つかるが最適ルートではないためスループットが低下する可能性がある（図 -8）[7]．

攻撃端末に対して周囲の端末がパケットを監視し，攻撃の特徴（たとえば，AODV の場合 RREQ を中継しているか否か）を検出し，落とし穴攻撃と同様の方式で防御することが可能である [7]．

（4）その他

上記以外に，特定のパケットを複製／改変などして周辺の端末へブロードキャスト（たとえば，AODV の場合，架空の宛先への RREQ メッセージのブロードキャスト）することによって，大量のパケットをネットワーク内に発生させ，通信不能に陥れたり，特定の端末に大量のパケットを送信したりするリソース攻撃がある．

これに対する抜本的な防御方法はないが，物理的にパケットフィルタリングをしたり，一定時間内に特定の端末からのパケット数を制限するなどの方法が考えられる．また，IPsec（Security Architecture for Internet Protocol）のようにセキュリティを考慮したセキュアなモバイルアドホックルーティングプロトコルを新たに設計する研究も進められている [8]．

●今後の展望

攻撃に対する検出・防御方式は，まだ特定のルーティングプロトコルごとに研究されている状況であり，あらゆる攻撃に万能なセキュアなルーティングプロトコルはまだ実用的なものはない．さらに，今後もいろいろな攻撃法が提案される可能性があり，攻撃とその対策は「いたちごっこ」状態となろう．

また，署名や認証を行うためには，公開鍵暗号方式が必要になるが，公開鍵の証明書の配布方式が課題となる．そのため，メールアドレスなどの well-known 情報を公開鍵に使用できる ID ベース暗号が上手く利用できるかもしれない．

モバイルアドホックネットワークによる情報共有空間の利用の仕方によって，信頼性に対する要求条件が異なると思われるので，完全なトラストモデルはいらないが，たとえばお互いを評価し合うことで，そこそこの信頼感を実現する方式も有効であると思われる．

おわりに

モバイルアドホックネットワークは，通信インフラを必要とせずに端末同士が協力しあってその場限りのネットワークを構築することが可能であり，コミュニティなどによる情報共有空間の形成を始めとして，災害により通信インフラが破壊された場合の代替通信手段としても利用することが可能であり，将来有望な通信手段となることが期待されている．このために，モバイルアドホックネットワークのルーティングプロトコルとセキュリティに関する研究の進展が望まれている．

参考文献

1) RFC 3626 : Optimized Link State Routing Protocol (OLSR) (Oct. 2003).
2) RFC 3561 : Ad hoc On-Demand Distance Vector (AODV) Routing (July 2003).
3) Yu, W., Sun, Y. and Liu, K. J. R : HADOF : Defense Against Routing Disruptions in Mobile Ad Hoc Networks, IEEE INFOCM 2005, pp.1252-1261 (Mar. 2005).
4) 森　郁海，横山　信，高木　剛，山崎憲一，高橋　修：アドホックネットワークにおけるブラックホール攻撃に対する防御法と提案と実装・評価，情報処理学会研究報告 (ISSN 0919-6072)，Vol.2006, No.120, pp.47-52 (Nov. 2006).
5) Hu, Y. -C., Perrig, A. and Johnson, D.B. : Packet Leashes : A Defense against Wormhole Attacks in Wireless Networks, IEEE INFOCOM 2003, pp.1976-1986 (Mar. 2003).
6) Marti, S., Giuli, T. J., Lai, K. and Baker, M. : Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, ACM MobiCom (Aug. 2000).
7) Yokoyama, S., Nakane, Y., Takahashi, O. and Miyamoto, E. : Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods, Proc. on MDM2006 Workshop FMUIT, pp.49-54 (May 2006).
8) Hu, Y.-C., Johnson, D. B. and Perrig, A. : SEAD : Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Ad Hoc Networks Journal, Vol.1, pp.175-192 (2003).

(平成 18 年 12 月 25 日受付)

高橋　修（正会員）
osamu@fun.ac.jp

1975 年北海道大学大学院工学研究科修了．同年電電公社（現 NTT）横須賀電気通信研究所入所．NTT ドコモを経て 2004 年より公立はこだて未来大学教授．博士（工学）．本会業績賞．本会フェロー．電子情報通信学会，IEEE 各会員．