社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＭＢＬ－37（12）
2006／5／18

アドホックネットワークにおける Power Off Attack とその対策

鈴木 俊博† 小林 基成† カーン アシック† 森田 正範†

†（株）NTT ドコモ ネットワーク研究所 〒239-8536 神奈川県横須賀市光の丘 3-5
E-mail: †{toshi, kobayashi, ashiq-khan, morita}@netlab.nttdocomo.co.jp

あらまし アドホックネットワーク上で安全で確実な通信を実現するためにルーティング・パケット転送技術のセキュア化，鍵管理方式等様々な研究が行われている．それらが想定している攻撃は，プログラムコードやルーティング情報の改ざんを前提としており，それらを対象とした研究成果や，対タンパー性の向上，セルラネットワークからの管理・制御により，発生する可能性が制限される．そのような状況においても，ユーザが利己的に端末の電源を落とすことにより期待するネットワーク性能を得られないリスクが存在し，それらは既存の研究では対処することが出来ない．本稿では，ユーザが利己的に端末の電源を落とすことによる攻撃，*power Off Attack* の影響とそれに対応する方式について提案し，シミュレーションによりその優位性を示す．

キーワード アドホックネットワーク，セキュリティ，ルーティング，電源管理

Power Off Attack and its Remedy for Mobile Ad hoc Networks

Toshihiro SUZUKI† Motonari KOBAYASHI† Ashiq KHAN† and Masanori MORITA†

† Network Laboratories, NTT DoCoMo, Inc. 3-5 Hikarino-oka, Yokosuka, Kanagawa, 239-8536 Japan
E-mail: †{toshi, kobayashi, ashiq-khan, morita}@netlab.nttdocomo.co.jp

Abstract To realize a secure, reliable communications in mobile ad hoc networks, various researches, such as secure routing, secure packet forwarding, or key management technologies, are being done. The security attack in these related works are assumed by modified program codes or routing information and resolved by various related works and controlled from a core network in integrated networks. This paper defines a new realistic and practical security attack, *power off attack*, which turn off his terminals selfishly, and evaluates the influence from it. Additionally, and this paper propose a solution against *power off attack* and show the effectiveness of it.

Keyword Ad hoc networks, Security, Routing, Power management

1. はじめに

アドホックネットワークの登場により，公衆網における通信形態が，信頼されたキャリアを介しラスト 1 ホップのみが無線である通信形態から，エンド端末以外の不特定多数の第三者を介した無線マルチホップ通信形態に変化し，第三者の協力が通信成立の必要条件となる．第三者を介することにより通信への様々な攻撃が想定されネットワークセキュリティ研究への関心が高くなっている[1]．具体的には，*black hole* [2] や *wormhole* [3]などの攻撃を想定し，それらの攻撃に対して，ルーティング技術のセキュア化を実現する Secure AODV(SAODV) [4]，Secure Routing Protocol(SRP) [5]，Authenticated routing for ad hoc networks(ARAN) [6]，Secure Link-State Protocol(SLSP) [7]，アドホックネットワーク上での鍵管理方式である Simple Ad hoc Key Management(SAKM) [8]等，様々な研究が行われている．そのようなセキュリティに関する研究成果や，CAN [9]をはじめとするなどのセルラネットワークとの統合したアドホックネットワーク[9-12]では管理や制御が容易に実現可能であり，コード改竄の防止，通信相手の認証，盗聴対策のためのデータの暗号化等が実現され，アドホックネットワーク上での安全な通信が期待される．以上の通り，通信のセキュア化を実現する様々な研究がなされているが，想定している攻撃は，プログラムコードやルーティング情報等の改竄を前提としており，大多数の一般ユーザでは動作し得ないモデルである．また，ユーザが利己的に電源を落とすとネットワーク内の中継端末が減少してしまうため，関連研究の方式においてもネットワーク性能の低下が懸念される．

本論文では，一般ユーザが行いうる，ユーザ自身の通信時のみ電源を投入しそれ以外では利己的に電源を落とす動作，*power off attack* を定義し，その攻撃によるネットワーク性能低下の防止，及び通信の公平性確保の困難性を示す．さらに，*power off attack* の影響を低減するために，ルーティングと電源管理機能の連携の必要性と方式を提案する．

以下，2 節にて想定する利己的動作，*power off attack* とその影響を示し，3 節にてルーティングと電源管理機能との連携について述べる．4 節では連携方式の有

効性をシミュレーション評価により示す.

2. Power Off Attack

2.1. Power Off Attack の定義

関連研究では，*black hole*，*wormhole*，及び利己的動作など様々な攻撃を想定している[1]．*black hole* ではデータパケットを攻撃ノードに誘導しパケットを破棄，*wormhole* では複数攻撃ノード間をトンネリングによりルーティングの正常動作を妨げることを想定している．利己的動作は，データ転送の利己的動作を想定しており，制御信号は通常通り処理を行うが，バッテリ消費を避けるなどの目的によりデータパケットの転送を拒否する動作である．これらの動作はプログラムコードやルーティング情報の改ざんを伴うため，一部のユーザに限られるものであり，大部分のユーザでは想定し得ない動作であると考えられる．また，SU 対策を含めたアドホックネットワーク上での安全で確実な通信を実現を目指した様々な研究成果や，固定網からの管理・制御により，コード改竄の防止，通信相手の認証，盗聴対策のためのデータの暗号化等が実現され，アドホックネットワーク上での安全な通信が期待される．

本論文では，そのような状況においても発生しうる利己的電源断，*power off attack* を定義する．*power off attack* は，コード改竄等を必要せず，ユーザ自身が通信を行う時のみ電源を投入し，それ以外では電源を落とす，もしくは，通信機能をオフにする動作であり，電源が投入されている時は通常動作を行う．コード改竄等を必要としないため一般ユーザも SU になるおそれがある．*power off attack* を行う SU が増えてきた場合，パケットを中継する端末数が減少してしまうためネットワーク性能への影響が懸念される．

2.2. Power Off Attack の影響

power off attack がネットワークへ与える影響をシミュレーションにより評価した．

2.2.1. シミュレーションモデル

ネットワーク内の全ユーザ数及び *power off attack* を行う利己的ユーザ(Selfish User: SU)数，セッションモデルを変化させた時のパケット到達率をシミュレーションにより評価した.エリアサイズは 1500×1500[m^2]，ルーティングプロトコルは AODV[13]，MAC プロトコルは 802.11b，移動モデルは歩行程度の移動，具体的には Random Way Point(Pause time = 0[s]，speed = 0.5～2.1[m/s])とし，トラヒックは VoIP を想定し，1 セッションあたり 500～2500UDP パケット 200[byte]，パケット発生間隔 20[ms]，セッション発生間隔を各ユーザ独立に 200～1000[s] にランダムで発生させ，シミュレーション時間は 1000[s]とした．SU の動作は，自身のパケットを送信する時のみ電源を投入し，それ以外の時には電源を落とすとモデル化とした．すなわち，自身がパケット送信している間は通常の動作を行い，それ以外は全くパケットを中継しない．なお，シミュレーションツールには QualNet[14]を使用し，結果はサンプル数 10 の平均値を採用した．

2.2.2. ユーザ数の影響

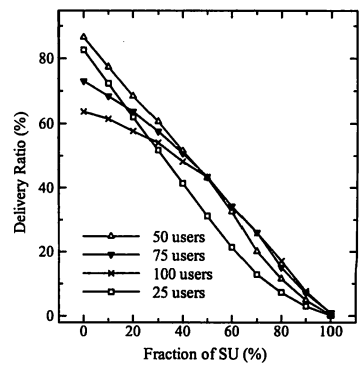

図 1　ユーザ数を変化させた時のパケット到達率

図 1 は，セッションモデルを固定(セッション発生間隔：600[s]，セッション内 UDP 数：1500)し，SU 割合を変化させた時の，ネットワーク内のユーザ数 4 パターン(25, 50, 75, 100)におけるパケット到達率を示している．図に示す通り，ユーザ数に関わらず SU 割合が増加するとパケット到達率が急激に低下している．特に，SU 割合が 30%を超える条件下ではユーザ数 25 の場合は，低いパケット到達率を示している．これは，低ユーザ密度の場合，代替ルートが確保できず通信が完了しないセッションが増えるのに対し，高ユーザ密度の場合は，代替ルートの存在により通信が継続されるためである．また，各ユーザ数での全パケット到達率の平均が，ユーザ数 25 の時が 35.1%，50 の時 41.6%，75 の時 40.1%，100 の時 37.7%となっており，ユーザ数 50 の時が最も高いパケット到達率を示している．これは，ユーザ数 75 及び 100 では，高ユーザ密度のためにコリジョンが発生しパケット到達率の低下を導いているためである．このような事象に対しては，盛んに研究されている制御信号の低減手法やセンサーネットワークで検討されている省電力ルーティング等を用いることで対処することが可能である．なお，各ユーザはランダムに相手先を選択するモデルであり，SU 割合が増加すると相手先として電源を落としている SU を選択する確率が増加するため，それによるパケット到達率低下もある．

2.2.3. セッション発生間隔の影響

図 2 は，セッションセッション内 UDP 数を 1500，ネットワーク内ユーザ数を 50 と固定し，SU 割合を変化させた時の，セッション発生間隔 5 パターン(200, 400, 600, 800, 1000)におけるパケット到達率を示している．図に示す通り，セッション発生間隔に関わらず SU 割合が増加するとパケット到達率が急激に低下している．特に，セッション発生間隔 200 時は，SU 割合が 0%においても低いパケット到達率を示している．これは，セッション発生間隔が短く結果として電源が投入されているユーザ数が増加し，2.2.2 節にて示した高ユーザ密度時と同様，コリジョンの発生に起因する．

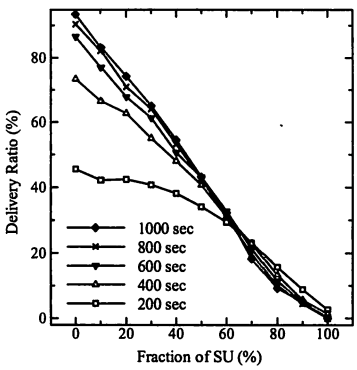

図 2　ｾｯｼｮﾝ発生間隔を変化させた時のﾊﾟｹｯﾄ到達率

2.2.4. セッション時間の影響

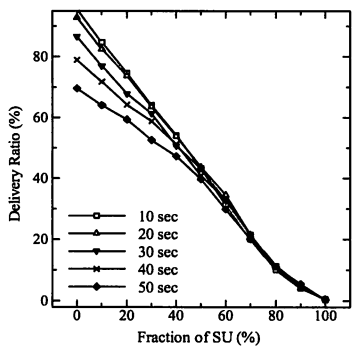

図 3　ｾｯｼｮﾝ時間を変化させた時のﾊﾟｹｯﾄ到達率

図 3 は，セッション発生間隔を 600，ネットワーク内ユーザ数を 50 と固定し，SU 割合を変化させた時の，セッション時間 5 パターン(10(セッション内 UDP 数：(500), 20(1000), 30(1500), 40(2000), 50(2500))におけるパケット到達率を示している．図に示す通り，セッション時間に関わらず SU 割合が増加するとパケット到達率が急激に低下している．各セッション時間での全パケット到達率の平均が，セッション時間 10 の時が 43.85%, 20 の時 43.79%, 30 の時 41.5%, 40 の時 39.7%, 50 の時 36.3%となっており，セッション時間 10 の時が最も高いパケット到達率を示している．これは，セッション時間の増加によりコリジョンの発生確率が上昇するためである．

2.3. 考察

2.2.2 節から 2.2.4 節に示したとおり，ネットワーク内のユーザ数やセッションモデルに関わらず power off attack のネットワーク性能へ与える影響は顕著である．原因は大きく 2 つ存在する．1 つは，電源投入ユーザ数の低下により利用できるルート数が減少し，そのルート上での輻輳や，そもそもルートを確保できない問題である．具体的には，ある時刻における電源が投入され有効なユーザ数は以下(1)のように表せ，SU 割合，及びセッション間隔の増加，セッション時間の減少によりネットワーク内のユーザ数に対して稼動ユーザ数が低くなってしまい，影響を大きく受ける傾向となる．

$$
\begin{aligned}
&\textit{稼動ユーザ数}\\
&= \textit{CU 数＋電源投入中の SU 数}\\
&= \textit{User (1 – Su) + User*Su(Vol / Int)} \qquad \cdots \quad (1)
\end{aligned}
$$

ネットワーク内ユーザ数: User
SU 割合: Su
セッション間隔: Int
セッション時間: Vol

2 つ目の原因は，アクティブルート上のユーザが利己的に電源を落とすことにより通信が途中で切断されることに起因しており，そのためのルート切り替え時に発生するパケットロスや，通信の中断に陥ってしまうにより性能が低下する．

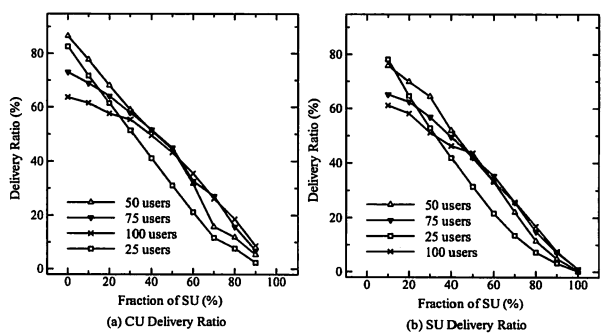

図 4　ユーザ数を変化させた時のパケット到達率

図 4，5，及び 6 は，2.2.2 節から 2.2.4 節のそれぞれ同様の環境下での，SU でなく常に電源を投入し協調的に動作するユーザ(Cooperative User: CU)が発信したセ

ッションのパケット到達率(a)，SU が発信した到達率(b)を示している．図 4～6 に示すとおり，ネットワーク全体のスループット同様 CU 発のパケット到達率も SU の影響を大きく受けていることが確認できる．また，SU 発と CU 発のパケット到達率に大きな差がなく，通信の公平性の観点からも *power off attack* の問題である．

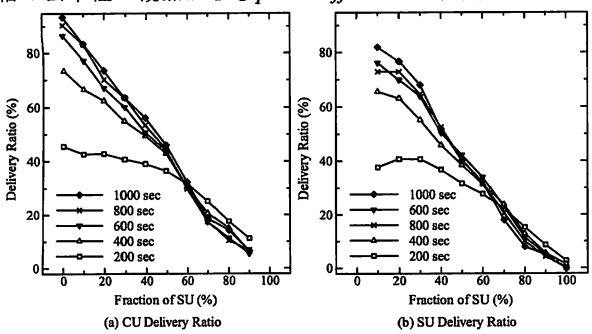

図 5　ｾｯｼｮﾝ発生間隔を変化させた時のﾊﾟｹｯﾄ到達率

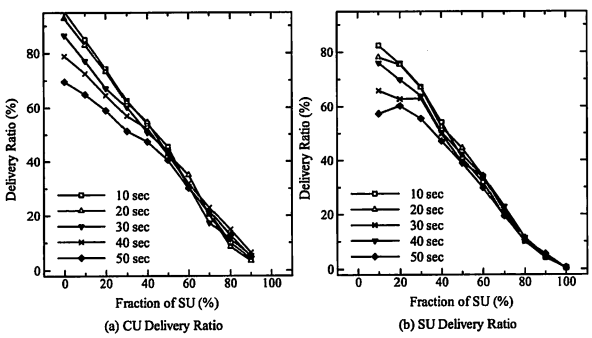

図 6　ｾｯｼｮﾝ時間を変化させた時のﾊﾟｹｯﾄ到達率

以上の通り，*power off attack* はモデルに関わらずネットワーク性能低下と通信の不公平性の問題を発生させており，解決すべき非常に重要な課題である．

3. ルーティングと電源管理機能の連携

Power off attack による影響を解決するためには，2.3 節に示した原因，稼動ユーザ数低減，及びアクティブルートの切断への対策が必要である．本稿では，本対策のためにルーティングと電源管理機能の連携を提案する．稼動ユーザ数低減に対しては，利己的な電源断を制約することにより対処が期待できる．本稿では特に，アクティブルート切断への対策について説明する．

3.1. 提案方式

アクティブルート切断による通信の中断は，SU がパケット中継動作中にもかかわらず，利己的に電源を落とせてしまうことに起因している．したがって，本稿ではパケット中継動作中，すなわちルート保持中に，電源断要求の受付を拒否し，パケット中継動作完了後に電源断を実施する．処理フローは図 7 の通りとなる．本方式により，アクティブルート中断の回避が期待できる．

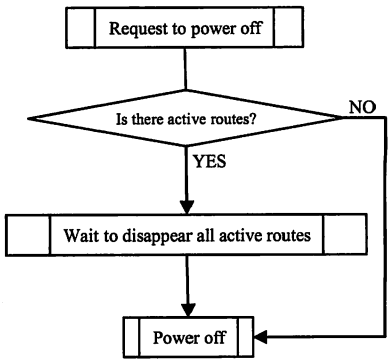

図 7　提案方式の処理フロー

4. シミュレーション評価

シミュレーションモデルは 2.2.1 節のモデルを踏襲し，ネットワーク内の全ユーザ数を 50，セッション時間を 30 秒(1500UDP パケット)，セッション発生間隔を 600 秒と固定し，利己的ユーザ(Selfish User: SU)数を変化させた時のパケット到達率をシミュレーションにより評価し，提案方式，ルート上のユーザの電源断を制限する方式の効果を確認した．なお，ルート保持の確認は 1 秒毎にルーティングテーブルを確認するモデルとした．

4.1. 提案方式の効果

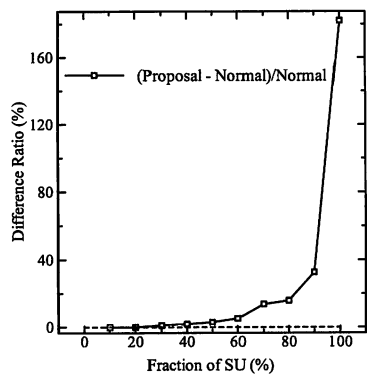

図 8　提案方式によるパケット到達率の増加率

図 8 は，提案方式を導入しない方式に対する，提案方式，ルート上のユーザの電源断を制限する方式におけるパケット到達率の増加率を示している．図に示すとおり，SU 割合に関わらず提案方式の効果が確認でき，その効果は平均 25.5%である．なお，SU 割合が増加する毎に大きな効果が確認できるのは，図 1～6 に示すと

おり，パケット到達率が非常に小さく相対的に向上しているためである．

図 9 は，提案方式を導入したことによりアクティブルートの切断を回避できた回数を示しており，その平均は 22.7 回である．また，SU 割合が 70%をピークに高い数字を示しているのは，稼動している全ユーザに締める SU の割合が高く，SU が中継ルートとして選択されているケースが多いためである．全体的に回避回数が少ないのは，本評価モデルでは，SU が中継ノードとし選択されアクティブルートが SU の電源断により切断されてしまうケースが少なくためであり，それに伴い，図 8 に示すとおりのパケット到達率向上にとどまっている．しかし，より大規模なネットワークやセッション時間が長く，SU が通常動作し中継ルートとして選択されるケースが増えてくる場合には，効果が上がってくると想定される．また，本稿では *power off attack* の動作を，通信中のみ電源を投入し，それ以外では完全に電源断する動作をモデリングしたが，ユーザの自己都合により様々な電源断モデルが想定され，SU が中継ルートとして選択されるケースが増え，提案方式の効果が上がることも期待できる．

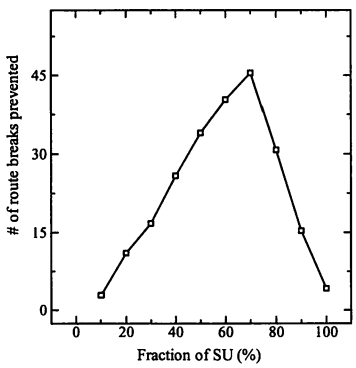

図 9　提案方式によるルート切断回避回数

以上の通り，提案方式の効果が認められ，稼動ユーザ数低減を回避する方式と連携させることにより更なる効果が期待できる．

5. おわりに

本稿では，利己的電源動作，*power off attack* を定義しその影響を示した．シミュレーション評価により，ユーザ数，セッションモデルに関わらず *power off attack* を行う利己的ユーザ(Selfish User: SU)がネットワーク内に増加するほどネットワーク性能が低下し，通信の公平性確保が困難であることを示した．*power off attack* の影響は，電源が投入されているユーザ数の減少により使用可能ルート数が限られてしまう問題と，パケットを中継しているユーザが電源断によりルートが切断されてしまう問題により発生する．また，本稿では，*power off attack* の対策としてルーティングと電源管理機能の連携の可能性を示した．具体的には，アクティブルートを保持し中継動作中のユーザの電源断を制限することで 25.5%の性能向上をシミュレーション評価により示した．今後は，電源が投入されているユーザ数を増加させるための方式を含む詳細な方式検討等を実施予定である．

文　献

[1] P. G. Argyroudis, and D. O'Mahony, 'Secure Routing for Mobile Ad hoc Networks', *IEEE Communications Surveys & Tutorials*, pp.02-21, Third Quarter 2005.

[2] R. Perlman, 'Network Layer Protocols with Byzantine Robustness', *Ph.D. Dissertation, MIT/LCS/TR-429*, October 1998.

[3] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, 'SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks', *Mobile Computing Systems and Applications*, pp.3-13, June 2002.

[4] Manel Guerrero Zapata, 'Secure Ad hoc On-Demand Distance Vector (SAODV) Routing', *Internet Draft: draft-guerrero-manet-saodv-05.txt*, February. 2006.

[5] P. Papadimitratos, and Z. J. Haas, 'Secure Routing for Mobile Ad hoc Networks', *Communication Networks and Distributed Systems, Modeling and Simulation Conf.*, pp.27-31, January 2002.

[6] K. Sanzgiri, and B. Dahill, 'A Secure Routing Protocol for Ad hoc Networks', *Proceedings of International Conference Network Protocol*, pp.78-87, 2002.

[7] P. Papadimitratos, and Z. J. Haas, 'Secure Link State Routing for Mobile Ad Hoc Networks', *Application and the Internet Workshps*, pp.379-383, January 2003.

[8] Manel Guerrero Zapata, 'Simple Ad hoc Key Management (SAKM)', *Internet Draft: draft-guerrero-manet-sakm-00.txs*, February. 2006.

[9] 森田，鈴木，ラタポン，小林，" セルラネットワークのカバレッジと通信キャパシティを拡大するキャリアアドホックネットワーク "，信学技法，AN2005, 2005.1

[10] H. Luo, R. Ramjee, L. Li, and S. Lu, 'UCAN: A Unified Cellular and Ad-Hoc Network Architecture', *ACM MOBICOM*, pp.353-367, September 2003.

[11] H-Y. Wei, and R. Gitlin, 'Two-Hop-Relay Architecture for Next-Generation WWAN/WLAN Integration', *IEEE Wireless Communications*, Vol. 11, No. 2, pp.24-30, April 2004.

[12] Y. Lin, and Y. Hsu, 'Multi-Hop Cellular: A New Architecture for Wireless Communications', *IEEE INFOCOM 2000*, March, pp.1273-1282, March 2000.

[13] C. Perkins, E. Belding-Royer, and S. Das, 'Ad hoc On-Demand Distance Vector (AODV) Routing', *RFC3561*, October. 2003.

[14] Scalable Network Technologies, Inc., QualNet Network Simulator, http://www.scalable-networks.com/