高セキュリティと低オーバヘッドを実現するIoT物理レイヤセキュリティ

代表研究者　　杉　浦　慎　哉　　東京大学　　生産技術研究所　　准教授

1 概要

本研究調査の目的は信号処理によるワイヤレス分散ネットワークにおける情報セキュリティ向上である。ワイヤレス通信の分野では、不正なノードがデータを盗聴できない伝搬路を構成することで情報理論的に通信の秘匿性が保証される物理レイヤセキュリティ技術が注目を集めている[1]．本技術の起源は 1975 年の Wyner によるワイヤタップ通信路の研究[2]にさかのぼるが，暗号技術の発展により長く研究がされてこなかった．しかしながら，近年の中継ノードを用いた協調通信技術や信号処理技術（中継ノード選択，協調ビームフォーミング，協調ジャミング等）[3,4]の進展により，伝搬路を能動的に制御することが可能となり物理レイヤセキュリティ技術が鋭意研究されるようになった．さらに，中継ノードにデータバッファを用いた協調通信が注目されている[5-7].この技術は中継ノードのもつバッファを利用することで柔軟な送信リンク選択が可能となり，高い信頼性を実現することができる．これらの物理レイヤセキュリティ，および，バッファ利用無線分散システム両技術を活用することで，高いセキュリティと信頼性を同時に実現することが期待できる．本研究では，複数のデータバッファを備えた中継ノードによる２ホップ通信を対象として，新たなアイデアを考案し，その性能向上を確認した．特に，中継バッファを利用した物理レイヤセキュリティにおいて,これまで使われてこなかったブロードキャスト伝搬路特有の自由度を活用するプロトコルを開発した．その効果として，秘密伝送容量を向上しながら，パケット遅延の低減を図った．ここでは特に，従来方式が単一中継リンクの選択に限定しているのに対して，複数のリンクを含むリンクサブセットを同時利用できるようプロトコルを設計した．具体的には，リンク選択をブロードキャストフェーズと中継フェーズの２フェーズに分け，ブロードキャストフェーズでは陽にリンク選択を行わず，電波のブロードキャスト性を利用して一定レベル以上の品質のリンクをすべて活用することを特徴とする．システムのセキュリティ，パケット遅延，オーバヘッドの性能を評価するための基本的な数値解析フレームワークを構築し，提案方式によるセキュリティ性能向上を明らかにした．

2 中継ノードのデータバッファを利用したセキュア協調通信

2-1 提案方式のシステムモデル

図１に提案するセキュア協調通信方式のシステムモデルを示す．２ホップの協調通信ネットワークを考える．構成ノードとして，送信元ノード，宛先ノード，複数の中継ノード，および，盗聴ノードがあるものとする．送信元ノードと宛先ノード間には直接リンクは存在せず，中継ノードを経由してのみパケットを伝達できるものとする．盗聴ノードは送信元ノードと中継ノードのパケットを盗聴可能であるとする．ワイヤレス通信で一般的な半二重通信を仮定し，中継ノードでは各スロットでパケットの送信または受信のどちらかが可能であるとする．各リンク間のチャネル係数は独立同分布のレイリーフェージングとする．中継ノードはそれぞれサイズ L のデータバッファを備えており，first-in first-out (FIFO) 方式でパケットを中継する．データバッファとチャネル係数は中央制御局である宛先ノードに集められる．すべての受信ノードで decode-and-forward (DF) 方式を仮定しており，伝送レートがチャネル容量を上回らない限り復号に成功するものとする．さらに，秘密レートは盗聴ノードがパケットを復号できない最大レートを意味する．ここでは，半二重通信を仮定しており，秘密レートは 1/2 の係数が付加されているものとする[8]．また，ターゲットレートは送信元ノードから宛先ノードまで各ノードで固定とする．したがって，ターゲットレートが秘密レートを下回るときには，当該パケットは盗聴ノードにパケットを復号されることなく，対象とするノードに送信成功する．一方，そうでない場合には，送信イベントは不稼働であるとする．なお，想定しているシナリオでは，送信ノードの電力消費を低減するために，ターゲットレートが秘密レートを下回らない程度に送信電力を低下させることが可能である．

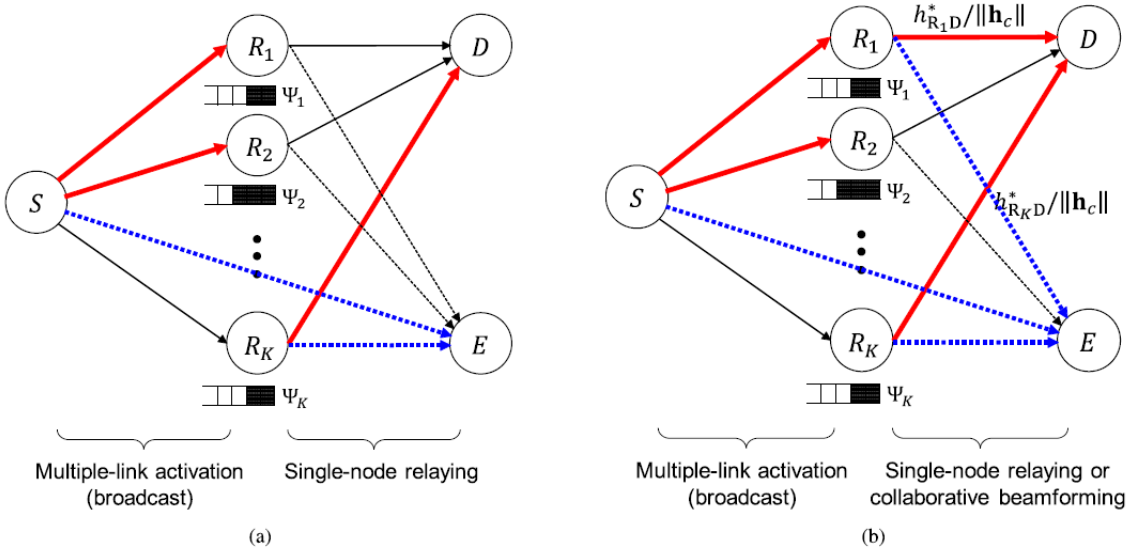

図１．提案方式のシステムモデル：(a)ブロードキャストフェーズ，(b)中継フェーズ．
（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

基本的に，提案プロトコルは文献[9]の Max-ratio 法と同様にして中継ノード選択は送信先ノードの伝搬路係数と盗聴ノードへの伝搬路係数の比を最大化するように行われる．しかしながら，提案方式の新規な点として以下の二点があげられる．

- 中継ノードのバッファのオーバーフローと空状態を避けるために，バッファの状態に応じたリンク選択が行われる．これにより，最大リンク選択数，つまり，ダイバーシティー次数を高く維持することができる．
- 電波伝搬のブロードキャスト性を活用することにより，複数の送信元－中継ノード間リンクを同時に選択することができるようにプロトコルが設計されている．

提案のリンク選択アルゴリズムでは，中央制御ノードがすべての中継ノードバッファ状態を得たうえで，一つの送信元－中継ノード間リンク，複数の一つの送信元－中継ノード間リンク，または，一つの中継ノード－宛先ノード間リンクが各タイムスロットで選択される．まず，各リンクが不稼働な状態になっているか確認される．そして，表１に従ってバッファ状態から不稼働ではない各リンクの優先度が計算される[10]．特に，Level 1 から Level 3 までの三段階に分類される．この分類により，中継ノードのバッファ状態がオーバーフローや空の状態にならないように制御される．

ここまでで，各リンクの優先度が決定されたので，図２で示される提案のアルゴリズムによってリンクが選択される．Level 3 の送信元－中継ノード間リンクが存在する場合には，Level 3 と Level 2 の送信元－中継ノード間リンクがすべて選択される．このとき，送信元ノードから送信されたパケットは選択された中継ノードすべてのバッファにコピーされることになる．また，Level 3 の送信元－中継ノード間リンクが存在せず，Level 3 の中継ノード－宛先ノード間リンクが存在する場合には，もっとも高い秘密レートに対応する Level 3 の中継ノード－宛先ノード間リンク一つが選択される．このとき，宛先ノードがパケットの復号

表１．各リンクの優先分類．（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

TABLE I
PRIORITY CLASSIFICATIONS OF AVAILABLE SR AND RD LINKS

Priority	Level 1 (Low)	Level 2 (Medium)	Level 3 (High)
SR links	$\Psi_k = L-1$	$1 < \Psi_k < L-1$	$\Psi_k = 0, 1$
RD links	$\Psi_k = 1$	$1 < \Psi_k < \xi$	$\Psi_k \geq \xi$

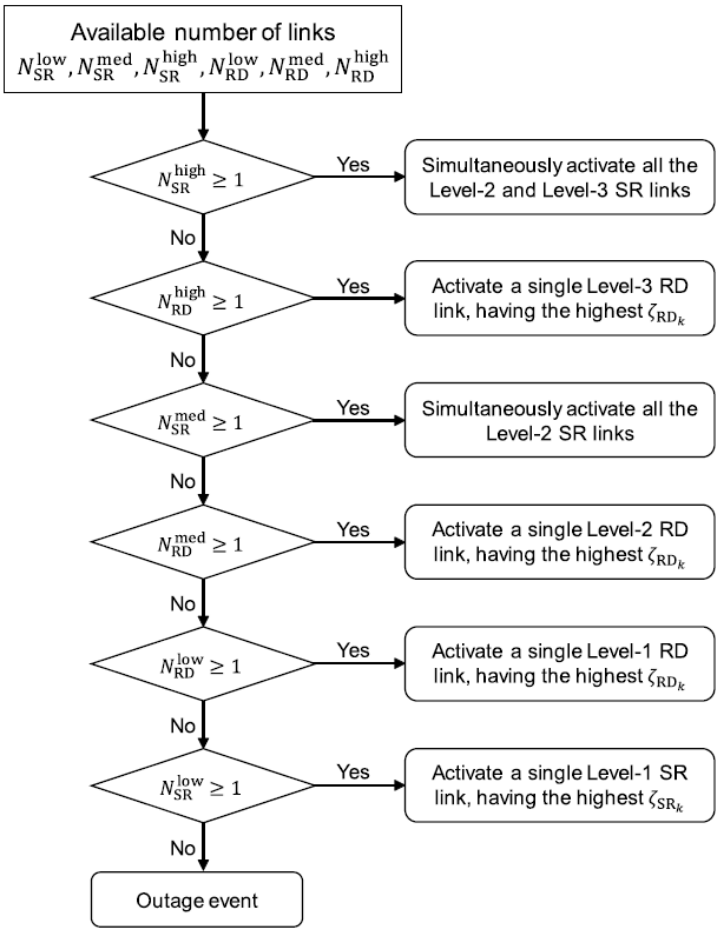

図２．フローダイアグラム．（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

に成功したら，Acknowledgement (ACK) パケットをすべての中継ノードに送り，中継ノードではそのパケットをバッファから削除する．そのほか，Level 2 の送信元－中継ノード間リンクが存在し，Level 3 の送信元－中継ノード間リンクと Level 3 の中継ノード－宛先ノード間リンクが存在しない場合には，すべての Level 2 の送信元－中継ノード間リンクが選択させる．さらに，Level 2 の中継ノード－宛先ノード間リンクが存在し，Level 2 以上の送信元－中継ノード間リンクと Level 3 の中継ノード－宛先ノード間リンクが存在しない場合には，もっとも高い秘密レートに対応する Level 2 の中継ノード－宛先ノード間リンク一つが選択される．もし上記のいずれの場合にも当てはまらないときは，Level 1 のリンクのみしか存在しないことになる．Level 1 の中継ノード－宛先ノード間リンクが存在する場合には，もっとも高い秘密レートに対応する Level 1 の中継ノード－宛先ノード間リンク一つが選択される．そうでない場合には，もっとも高い秘密レートに対応する Level 1 の送信元－中継ノード間リンク一つが選択される．

上記の提案アルゴリズムの理論解はバッファ状態のマルコフ連鎖に基づくフレームワークで導出することができる．詳しくは文献[8]を参考にされたい．

3 性能解析

本章では，モンテカルロシミュレーションによる提案方式の数値解析結果を示す．数値解析に用いた基本的なシステムパラメータを表２に示す．ここでは，シミュレーションごとに 10^4 フレームを計算し，各フレームで 10^5 パケットを生成した．敷値レベルは 2 に固定した．ベンチマークとして，Max-ratio 法[9]を考えた．簡単のため，送信元－中継ノード間リンクと中継ノード－宛先ノード間リンクの平均信号対雑音電力比 (Signal-to-noise ratio; SNR) が等しい対称チャネルシナリオを考えた．

表２．数値解析に用いた基本パラメータ
（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

Number of Monte Carlo simulatoins	10^4
Frame length	10^5 packets
Channels	Symmetric Rayleigh fading
SNR	$\gamma_{\mathrm{SR}} = \gamma_{\mathrm{RD}} = \gamma_{\mathrm{RR}} = [20, 40]$ dB
SNR ratios of SR and SE links	$\zeta_{\mathrm{SR}_k} = [1, 5]$
SNR ratios of RD and RE links	$\zeta_{\mathrm{R}_k\mathrm{D}} = [1, 5]$
SNR ratios of DR and DE links	$\zeta_{\mathrm{DE}} = [1, 5]$
Thresholding parameter	$\xi = 2$
Target secrecy rate	$r_{\mathrm{sc}} \in [0.1, 3.0]$
Number of relay nodes	$K \in [2, 20]$
Buffer size	$L = 5$

図３に提案方式（Proposed w/o beamforming）の秘密不稼働率を示す．また，本報告書では割愛したが，提案方式に協調ビームフォーミングを用いた改良方式（Proposed with beamforming）[8]もプロットした．中継ノード数とバッファサイズをそれぞれ(K, L)=(3,5)と設定した．秘密レートを 0.1 bps/Hz から 3.0 bps/Hz まで変化させた．平均 SNR を 40 dB に固定した．図３より，２種類の提案方式はほぼ同程度の性能を示し，全領域でベンチマークである Max-ratio 法を大きく上回る性能を示した．特に，低秘密レート領域でその利得が大きかった．

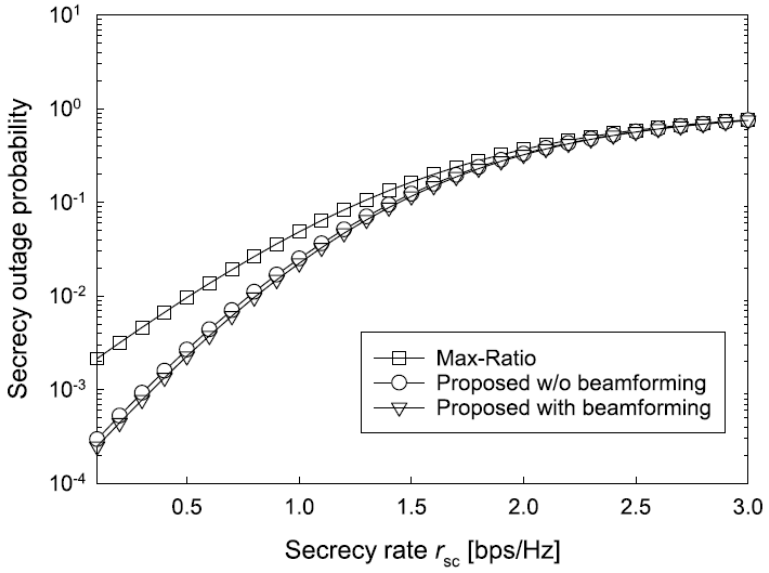

図３．秘密不稼働率と秘密レート．(K, L) =(3,5)，SNR = 40 dB.
（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

図４に秘密不稼働率と中継ノード数 Kの関係を調べた．特に，中継ノード数を 2 から 20 まで変化させたときの，秘密不稼働率をプロットした．このとき，バッファサイズは 5 に固定し，平均 SNR は 40 dB，秘密レートは 1 bps/Hz とした．図４より，提案方式は Max-ratio 法と比べて，優れた秘密不稼働率を示すことがわかった．特に，中継ノード数が増加するにつれ，その利得は増加した．

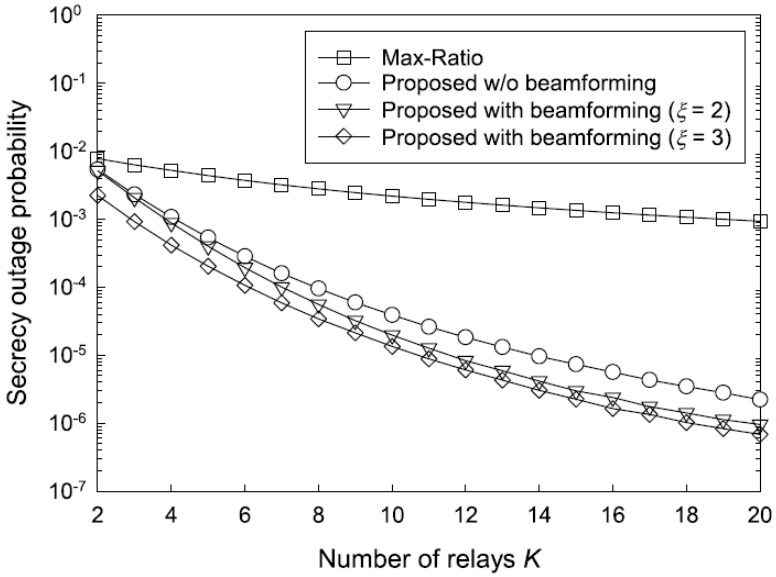

図４．秘密不稼働率と中継ノード数．L = 5, SNR = 40 dB, 秘密レート 1 bps/Hz.
（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

図５に平均パケット遅延を示す.バッファサイズをL=5, 平均SNRを40 dBとして,秘密レートを0.1 bps/Hzから3.0 bps/Hz まで変化させた．図５(a)は中継ノード数が 3, 図５(b)は中継ノード数５の結果を示している．図５より，すべての秘密容量の領域において，提案方式の平均パケット遅延は従来手法である Max-ratio 法よりも大きく低い値を示した.さらに,秘密レートを増加させるとその利得幅は増大することがわかった.

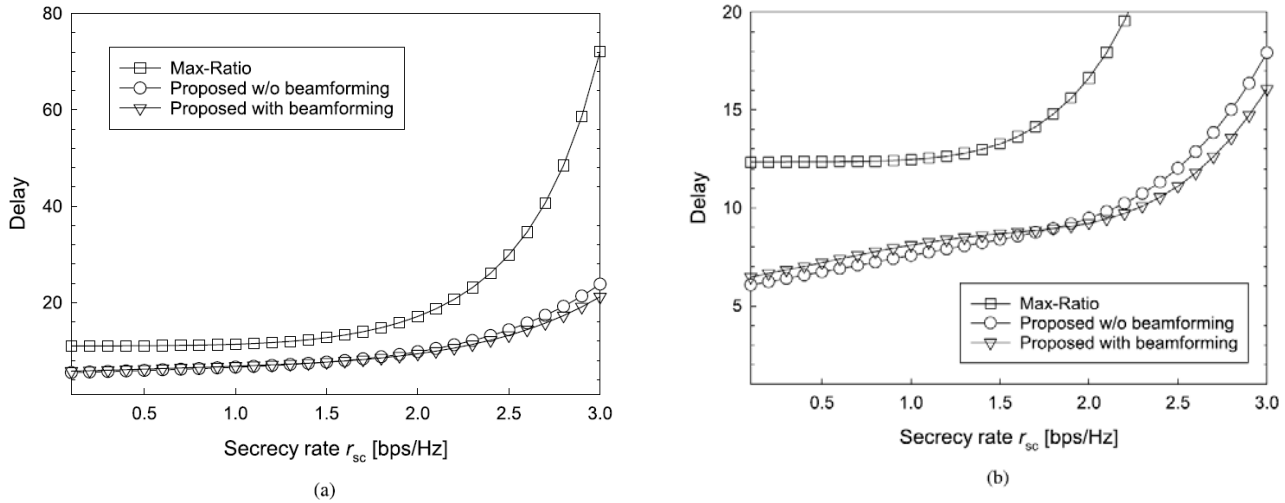

図５．平均パケット遅．バッファサイズ L = 5, SNR = 40 dB, 秘密レート 0.1～3.0 bps/Hz:
(a)中継ノード数 3, (b)中継ノード数 5.
（©IEEE. Reprinted, with permission, from [8] Nakai and Sugiura.）

4 まとめ

本研究では，中継ノードにデータバッファを備えた２ホップ協調通信システムを対象として，秘匿性と遅延特性を向上させた新しいプロトコルを提案した．特に，宛先ノードと中継ノード間の伝搬路のブロードキ

ャスト性を利用することにより，従来方式に新しい設計の自由度を追加した．数値解析により，提案方式の性能向上を定量的に示した．

【参考文献】

[1]. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[2]. A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3]. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[4]. J. Li, A. P. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[5]. B. Xia, Y. Fan, J. Thompson, and H. V. Poor, “Buffering in a threenode relay network,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[6]. A. Ikhlef, D. S. Michalopoulos, and R. Schober, “Max-max relay selection for relays with buffers,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, Mar. 2012.

[7]. I. Krikidis, T. Charalambous, and J. S. Thompson, “Buffer-aided relay selection for cooperative diversity systems without delay constraints,” *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

[8]. R. Nakai and S. Sugiura, "Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 431-444, Feb. 2019.

[9]. G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, “Max-ratio relay selection in secure buffer-aided cooperative wireless networks,” *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[10].R. Nakai, M. Oiwa, K. Lee, and S. Sugiura, “Generalized buffer-state-based relay selection with collaborative beamforming,” IEEE Trans. Veh. Technol., vol. 67, no. 2, pp. 1245–1257, Feb. 2018.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming	IEEE Transactions on Information Forensics and Security	2019 年 2 月
バッファ状態に基づく中継ノード同時利用による物理レイヤセキュリティ	電子情報通信学会総合大会	2018 年 3 月
中継ノード間干渉を考慮したバッファ利用全二重協調通信	電子情報通信学会ソサエティ大会	2018 年 9 月