様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　１５　日現在

機関番号：　３３９０３
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１０３

研究課題名（和文）無線伝送路特性を利用するアナログセキュリティネットワークの開発

研究課題名（英文）Development of a channel state based analog secure network

研究代表者
内藤　克浩（Naito, Katsuhiro）

愛知工業大学・情報科学部・准教授

研究者番号：８０３７８３１４

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：本研究では、プレ等化技術を活用するセキュア通信を実現するため、伝送路状態に基づいた無線通信技術を提案した。本研究では、一般的な無線通信環境では、多数のマルチパス信号を受信する点に着目する。提案方式の送信端末は、送受信端末間の伝送路状態に最適化した信号をプレ等化技術により送信する。そのため、想定した伝送路状態である受信端末のみが送信端末からの信号を高品質に受信可能となり、受信信号の復調にも成功する。結果として、盗聴端末は異なる場所では伝送路状態が異なるため、受信信号の等化を行うことができず、受信信号の復調に失敗する。数値例より、一般的な伝搬環境において、セキュア通信を実現可能であることを示した。

研究成果の概要（英文）：This research proposed a new channel state based a secure wireless communication mechanism to realize secure communication with a pre-equalization function in a physical layer. We focused on practical wireless communication environment, where multi-path signals are received at a receiver. The transmitter of the proposed scheme transmits an optimized signal to a receiver with pre-equalizing the signal according to the channel state between the transmitter and the receiver. Therefore, only the receiver that has the same channel state for the pre-equalizing can obtain the high quality signal from the transmitter, and can demodulate the signal correctly. As a result, eavesdroppers around the transmitter cannot equalize the received signal before a demodulation process for the received signal because they exist at a different place of the receiver. The numerical results show that the proposed scheme can realize secure communication in typical wireless channel models.

研究分野：　モバイルネットワーク

キーワード：　無線通信技術　モバイルネットワーク　変復調技術　セキュア通信　セキュリティ

１．研究開始当初の背景

無線通信におけるブロードキャスト性は，セキュリティ技術と併用しない限り，安全ではないことが以前より指摘されている．そのため，無線信号が到達する範囲に存在する盗聴者は，発見されるリスクなく無線信号を傍受可能であり，伝送されている情報も確認可能である．無線通信では，データリンク層・ネットワーク層などの上位層において暗号化による対策が行われるのが一般的である．一方で，暗号化を採用するためには，暗号鍵を端末間で共有する手段が必要である．無線通信上で暗号鍵の共有を行うためには，暗号鍵を安全に配布，管理する枠組みが必要となるが，無線通信のブロードキャスト性により，実現は困難である．そこで，物理層の特性に着目することにより，物理層において所望の端末のみで復調が可能となるセキュリティ技術を実現する試みが進められている

２．研究の目的

本研究では、より安全な無線通信技術を実現するため、物理層においてセキュリティを実現する手段を開発する。提案手法では、既存手法とは異なり、既存機器の設計を大きく変更するのではなく、無線伝搬環境をセキュリティの鍵として活用する方式を提案する。

３．研究の方法

本研究では，現実の通信環境はAWGN(Additive White Gaussian Noise)環境のように安定した環境ではなく，多数のマルチパス波が存在するため，無線伝送路特性が場所により大きく異なることに着目する．無線伝送路特性は，場所が通信で利用する無線信号の半波長以上異なれば，一般的には独立して変化すると言われている．また，一般的な無線通信システムでは，このような無線伝送路特性の影響を受信側で取り除く等化処理を行うことにより，正しい復調処理を実現している．そのため，所望の受信端末のみが無線伝送路特性の影響を取り除くことが可能である一方，他端末は無線伝送路特性の影響を取り除けない方式が実現されれば，物理層による安全性を改善可能と考える．

４．研究成果

(1)　概要

本研究で提案する無線伝送路特性を鍵として利用するセキュア通信方式は，無線通信性能を特徴づける無線伝送路特性に着目したものである．一般に，端末間の無線伝送路特性は，同一周波数，同一時間では同一のものとなり，端末間の双方向通信は同一の無線伝送路特性の影響を受ける．一方，端末位置が通信周波数の半波長以上離れている場合，無線伝送路特性が全く異なるという独立性を持つ．そのため，受信端末とは異なる場所に存在する盗聴端末は，異なる無線伝送路特性の影響を受けた無線信号を受信することとなる．

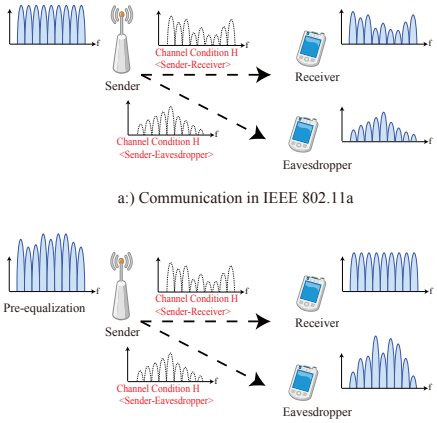

図１ 提案方式の通信概要

図１に提案するプレ等化技術を用いるセキュア通信方式の概要を示す．本システムでは，無線 LAN 基地局などと通信する複数の端末を想定する．本図では，基地局である送信端末が受信端末と通信をしており，盗聴端末が送信端末と受信端末の通信内容の傍受を試みている．

図１(a)で示される一般的な無線 LAN システムなどでは，送信端末は一般的な OFDM 信号を送信する．また，受信端末では，既知のパイロット信号を用いることにより無線伝送路特性の推定を行う．次に，受信端末により推定された無線伝送路特性を用いて受信信号を等化することにより，送信時とほぼ同様の信号を復元し，復調により情報を取得している．

図１(b)で示される提案方式では，通信中の端末移動が少ない準静止環境を想定する．準静止環境では，送信端末と受信端末間の無線伝送路特性の時間変動は極めて少なくなるため，パケット転送の直前に無線伝送路の推定を行うことで，無線伝送路特性の推定値と実際のパケット転送時の無線伝送路特性はほぼ一致する．また，送信端末から受信端末宛の通信と受信端末から送信端末宛の通信では，同一周波数を利用している場合，無線伝送路特性は同一のものとなる．そこで，送信端末と受信端末間であらかじめ無線伝送路特性を推定することにより，送信端末は所望の受信端末までの無線伝送路特性を考慮した送信信号を送信する．このような処理をプレ等化処理と呼び，プレ等化処理された送信信号は，無線伝送路の影響を受けることにより，所望の受信端末のみで復調可能な信号となる．結果として，受信端末は正常に復調処理が可能となる一方，盗聴端末は異なる無線伝送路の影響を受ける上，プレ等化処理で利用した無線伝送路特性も不明なため，受信時に等化処理を行うこともできず，復調処理に失敗する．

(2)　システムモデル

IEEE 802.11a のフレーム構造では，ショートプリアンブル，ロングプリアンブルに続き，OFDM シンボルが繰り返し送信される．また，プリアンブルの次の OFDM シンボルのみ制御情報が含まれており，その後の OFDM はペイロードデータが含まれている．提案方式のシステムにおいても，IEEE 802.11a と同一のフレーム構造を想定する．

図 3 に提案方式の通信モデルを示す．提案方式は IEEE 802.11a などの OFDM を利用する通信システムを想定する．OFDM を利用するシステムでは，送信データ系列を周波数方向にマッピングし，1 次変調を行う．また，データパケットの送信前に交換される制御パケットを利用して，伝送路特性を推定し，推定した伝送路特性を用いてプレ等化処理を行う．その後，IFFT(Inverse Fast Fourier Transform)を利用することにより，時間方向の信号を生成し，一般の OFDM システムと同様にガードインターバル(GI)を付加して送信を行う．

受信処理では，IEEE 802.11a と同様に，ショートプリアンブルを用いることで，AGC(Automatic Gain Control)の調整，信号検出，タイミング推定，周波数オフセット推定を行う．また，ロングプリアンブルを用いて，より正確なタイミング推定と周波数オフセット推定を行う．既存の IEEE 802.11a と異なる点は，既存方式では，ロングプリアンブルに含まれる既知のパイロットを利用して伝送路特性を推定し，推定した伝送路特性を利用して等化処理してから復調処理を行う．一方，提案方式の場合，送信時に伝送路特性に合わせてプレ等化処理を行っているため，受信時の等化処理は必要なく，直接復調処理を行う点である．なお，プレ等化処理をするのは，ペイロードデータを搬送するサブキャリア部だけであり，既知信号が含まれるパイロット用のサブキャリアにはプレ等化処理を行わない．また，上記のプリアンブルは標準のものを利用するため，ペイロード受信前に行われる信号検出，タイミング推定，周波数オフセット推定などの処理は同一である．

なお，受信端末と異なる位置に存在する盗聴端末には，プレ等化処理された信号が自らの無線伝送路を通して受信される．そのため，正確な復調処理を行うためには，プレ等化処理で利用した無線伝送路特性と，自らの無線伝送路特性が必要となる．しかし，プレ等化処理で利用した無線伝送路特性は知ることができないため，等化処理に失敗し，復調処理をしたとしても，多くのデータは誤りとなる．

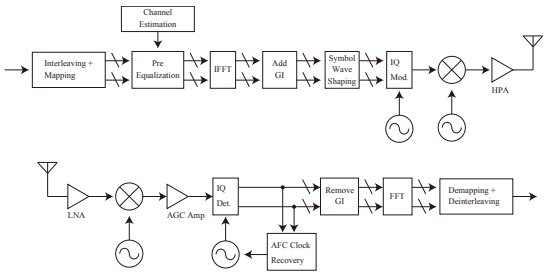

図 2 提案方式のシステムモデル

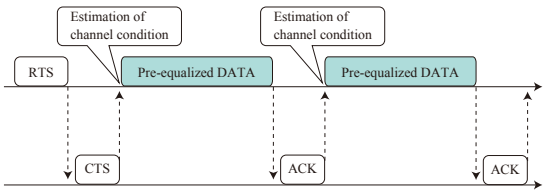

図 3 提案方式の通信シグナリング

(3) 通信シグナリング

提案方式では，プレ等化処理を行うために送信端末が無線伝送路特性を予め知る必要がある．一般に無線伝送路特性は準静止環境においても，ゆっくりと時間的に変化しており，プレ等化処理を行う直前の無線伝送路特性の推定が必要である．図 4 は，RTS/CTS の機構を活用した無線伝送路特性を行う通信シグナリングである．提案方式の通信シグナリングでは，無線伝送路特性が不明な場合，RTS/CTS の通信を行うことにより，送信端末は CTS パケットを用いて無線伝送路を推定する．また，推定した無線伝送路特性を用いて，データパケットのデータサブキャリアのプレ等化処理を行う．なお，連続的にデータパケットを送信可能な場合は，データパケットの確認応答(ACK)パケットを用いて，無線伝送路特性を改めて推定することにより，最新の無線伝送路特性を取得する．なお，RTS，CTS，ACK パケットは IEEE 802.11a に準拠したパケットを想定しており，データパケットのみプレ等化処理を行う．

(4)　数値例

提案方式の有効性を検討するため，Matlab による数値シミュレーションによる評価を実施した．無線システムとしては，IEEE 802.11a を想定し，図 2 に示す，IEEE 802.11a のフレーム構造を利用した．そのため，送信信号のフレームには，ブリアンブル部とペイロード部が含まれている．また，64 本のサブキャリアの内，48 本をデータ伝送に利用し，4 本はパイロット信号用に利用した．なお，12 本はゼロパディングが挿入されるため，利用していない．プレ等化処理はデータ伝送用のサブキャリアのみに適用し，受信側ではパイロット信号を利用した等化処理は行わない実装とした．チャネルモデルとしては，Joint Technical Committee (JTC)により提案されたアン

テナ高が低い場合の室内及び屋外の伝送路モデルと一般的なマルチパス環境をモデル化した Rayleigh Fading 環境を用いた. なお, 利用したチャネルモデルでは, マルチパスの最大遅延量が GI 長より少ない環境である. また, シミュレーション諸元を表 1 に示す.

図 4 にプレ等化技術を利用することで, 受信側では等化処理を行わない, 提案方式のビット誤り率特性を示す. 本図の性能は所望の受信端末のビット誤り率を示すため, 低いビット誤り率が要求される. 結果より, 多くのチャネルモデルは類似した特性を持つことが確認される. また, JTC Indoor residential A のみは, ビット誤り率特性が極めてよいことも確認できる.

図 5 に提案方式の盗聴端末のビット誤り率特性を示す. 提案方式では, 盗聴端末はプリアンブル部などを用いることにより, 送信端末と盗聴端末間及び受信端末と盗聴端末間の伝送路特性の推定は可能である. しかし, 送信端末と受信端末間の伝送路特性は, 物理的に受信端末に近づかなければ推定が困難である. 結果として, すべてのチャネルモデルにおいて, ビット誤り率がほぼ 0.5 となることが確認できる. つまり, 盗聴端末が得られる情報量もほぼ 0 であることを示し, 提案方式の有効性を確認できる.

表 1 シミュレーション諸元

Simulator	Matlab 2015b
Number of trials	10000
Communication device	IEEE802.11a
Number of symbols in a frame	10
Modulation scheme	QPSK
Number of FFT points	64
Number of data sub-carriers	48
Number of pilot subcarriers	4
Number of zero padding	12
Guard Interval	16 (0.8 [μs])
Bandwidth	20 [MHz]
Frequency	5.2 [GHz]
Channel model	JTC · Indoor residential A · Indoor office A · Indoor commercial A · Outdoor urban low-rise areas Low antenna A · Outdoor residential areas Low antenna A Rayleigh fading (Multi-path: 4)
Speed	1km/h

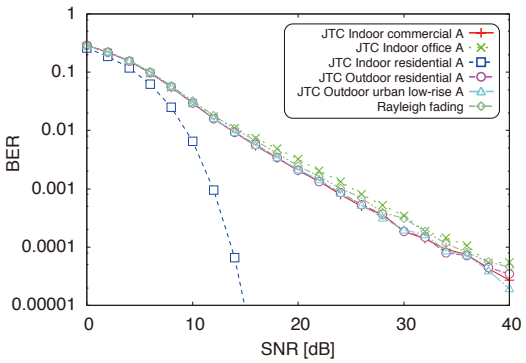

図 4 ビット誤り率（目的端末）

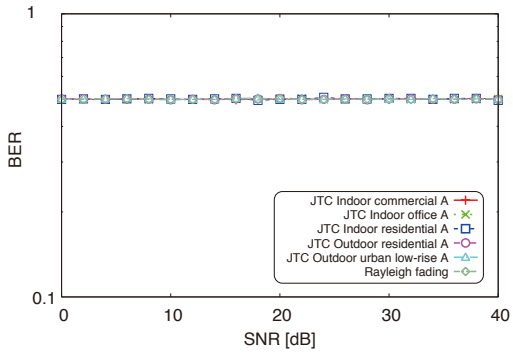

図 5 ビット誤り率（盗聴端末）

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 33 件）

- Tanairat Mata, Katsuhiro Naito, Pisit Boonsrimuang, Kazuo Mori, and Hideo Kobayashi: Proposal of Channel Estimation Method for Bi-directional OFDM Based ANC in Higher Time-varying Fading Channel, The IEEE 79th Vehicular Technology Conference (IEEE VTC 2014-Spring), May 2014.（査読有）（2014/5/18-21・ソウル・韓国）
- Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Cooperative Broadcast Scheme for VANETs in OFDM Wireless Networks, Cybernetics and Information Technologies, Systems and Applications (CITSA 2014), July 2014.（査読有）（2014/7/15-18・オーランド・米国）
- Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Cooperative Broadcast Scheme for VANETs in OFDM Wireless Networks, Cybernetics and Information Technologies, Systems and Applications (CITSA 2014), July 2014.（査読有）（2014/7/15-18・オーランド・米国）
- Katsuhiro Naito, Keisuke Sugita, Yuta Inoue, Kazuo Mori and Hideo Kobayashi: Implementation of IPv4/IPv6 Translation Mechanisms for BIS and NAT64 Router, Cybernetics and Information Technologies, Systems and Applications (CITSA 2014), July 2014.（査読有）（2014/7/15-18・オーランド・米国）

- Hiroki Sakakibara, Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Proposal of ML Demodulation Method for OFDM without GI in Time-varying Fading Channel, IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium 2014 (APWCS 2014), August 2014. (査読有) (2014/8/28-29・高雄・台湾)
- Naoto Kitajima, Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Decision Aided ML Channel Estimation Method for OFDM in High Time-varying Fading Channel, IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium 2014 (APWCS 2014), August 2014. (査読有) (2014/8/28-29・高雄・台湾)
- Quan Ji, Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Proposal of Adaptive Modulation and Frame Size for OFDM Systems in Time-varying Channel, IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium 2014 (APWCS 2014), August 2014. (査読有) (2014/8/28-29・高雄・台湾)
- Katsuhiro Naito, Fumihito Sugihara, Hiroshi Nodo, Masanori Kako, Tatsuya Hirose, Hidekazu Suzuki, Akira Watanabe, Kazuo Mori, and Hideo Kobayashi: Implementation of smartphone applications supporting end-to-end communication, International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2014), December 2014. (査読有) (2014/12/2-5・ロンドン・英国)
- Jae-Han Lim, Katsuhiro Naito, Ji-Hoon Yun, Danijela Cabric, Mario Gerla: Safety Message Dissemination in NLOS Environments of Intersection using TV White Space, IEEE International Conference on Computing, Networking and Communications 2015, February 2015. (査読有) (2015/2/16-19・アナハイム・米国)
- Jae-Han Lim, Katsuhiro Naito, Ji-Hoon Yun, Mario Gerla: Revisiting Overlapped Channels: Efficient Broadcast in Multi-channel Wireless Networks, IEEE INFOCOM 2015, April. 2015. (査読有) (2015/4/26-5/1・香港・香港)
- Katsuhiro Naito, Kento Nakanishi, Kazuo Mori, and Hideo Kobayashi: Implementation of tree-based data collection scheme for Arduino-compatible board, The 8th International KES Conference on INTELLIGENT INTERACTIVE MULTIMEDIA: SYSTEMS AND SERVICES, June 2015. (査読有) (2015/6/17-19・ソレント・イタリア)
- Katsuhiro Naito, Kazuo Mori, and Hideo Kobayashi, Implementation of agricultural sensor network systems based on Arduino based microcomputer board with Bluetooth Low Energy, The 8th International Multi-Conference on Engineering and Technological Innovation: IMETI 2015, June 2015. (査読有) 2015/7/12-15・オーランド・米国)
- Katsuhiro Naito, Kenta Nakanishi, Kazuo Mori, and Hideo Kobayashi: Implementation of maintenance system based on Bluetooth Low Energy for hermetic inline amplifiers in CATV networks, The 8th International Multi-Conference on Engineering and Technological Innovation: IMETI 2015, June 2015. (査読有) (2015/7/12-15・オーランド・米国)
- Fumihito Sugihara, Katsuhiro Naito, Hidekazu Suzuki, Akira Watanabe, Kazuo Mori, Hideo Kobayashi: Proposal of cooperative operation framework for M2M systems, The 12th IEEE Asia Pacific Wireless Communications Symposium: IEEE VTS APWCS 2015, August 2015. (査読有) (2015/8/19-21・シンガポール・シンガポール)
- Kohei Tanaka, Fumihito Sugihara, Katsuhiro Naito, Hidekazu Suzuki, and Akira Watanabe: Design of an application based IP mobility scheme on Linux systems, IWIN (International Workshop on Informatics) 2015, September 2015. (査読有) (2015/9/6-9・アムステルダム・オランダ)
- Takamasa Mizukami, Katsuhiro Naito, Chiaki Doi, Tomohiro Nakagawa, Ken Ohta, Hiroshi Inamura, Takaaki Hishida, and Tadanori Mizuno: Evaluation of Unconscious Participatory Sensing System with iOS devices, IWIN (International Workshop on Informatics) 2015, September 2015. (査読有) (2015/9/6-9・アムステルダム・オランダ)
- Takuya Wada, Tomoya Ogawa, Katsuhiro Naito: Prototype implementation of a field monitoring and control system, International Symposium on EcoTopia Science 2015, November 2015. (査読有) (2015/11/27-29・名古屋・日本)

- Katsuhiro Naito, Kazuo Mori and Hideo Kobayashi: Feasible cooperative communication with IEEE 802.11a based devices for multi-hop networks, The 13th Annual IEEE Consumer Communications & Networking Conference CCNC 2016, Future Internet Architecture for Developing Regions, January 2016. (査読有) (2016/1/8-11・ラスベガス・米国)
- Katsuyuki Tanaka and Katsuhiro Naito : Demonstration: Implementation of unconscious bus location sensing system with smartphone devices and beacon devices, The 13th Annual IEEE Consumer Communications & Networking Conference CCNC 2016, January 2016. (査読有) (2016/1/8-11・ラスベガス・米国)
- Katsuhiro Naito, Hiroki Sakakibara, Yosuke Mukai, Kazuo Mori and Hideo Kobayashi: Channel state based secure wireless communication, IEEE Infocom 2016 MiseNet Workshop, April 2016. (査読有) (2016/4/10-15・サンフランシスコ・米国)
- Katsuhiro Naito, Kenta Nakanishi, Kazuo Mori, and Hideo Kobayashi: Implementation of maintenance system based on Bluetooth Low Energy for hermetic inline amplifiers in CATV networks, Journal on Systemics, Cybernetics and Informatics: JSCI, Vol. 14, No. 1, pp. 55-60, April 2016. (査読有)
- Katsuhiro Naito, Shunsuke Tani and Daichi Takai: Implementation of mobile sensing platform with a tree based sensor network, The 9th International KES Conference on INTELLIGENT INTERACTIVE MULTIMEDIA: SYSTEMS AND SERVICES, June 2016. (査読有) (2016/6/15-17・テネリフェ・スペイン)
- Takuya Wada and Katsuhiro Naito: Prototype implementation of actuator sensor network for agricultural usages, The 9th International KES Conference on INTELLIGENT INTERACTIVE MULTIMEDIA: SYSTEMS AND SERVICES, June 2016. (査読有) (2016/6/15-17・テネリフェ・スペイン)
- Tomoya Ogawa and Katsuhiro Naito: Development of multi-hop field sensor networks with Arduino board, The 9th International KES Conference on INTELLIGENT INTERACTIVE MULTIMEDIA: SYSTEMS AND SERVICES, June 2016. (査読有) (2016/6/15-17・テネリフェ・スペイン)
- Katsuhiro Naito, Shunsuke Tani and Daichi Takai: Development of a bus location system on a multi-hop network with IEEE 802.15.4 based wireless system-on-a-chip, The 10th International Multi-Conference on Society, Cybernetics and Informatics: IMSCI 2016, July 2016. (査読有) (2016/7/5-8・オーランド・米国)
- Jae-Han Lim, Katsuhiro Naito, Ji-Hoon Yun and Mario Gerla: Exploiting Overlapped Bands for Efficient Broadcast in Multi-channel Wireless Networks, IEEE Transactions on Vehicular Technology Vol. 66 No. 5, pp. 4355-4370, 2016. (査読有)
- Takamasa Mizukami, Katsuhiro Naito, Chiaki Doi, Ken Ohta, Hiroshi Inamura, Takaaki Hishida, and Tadanori Mizuno: Evaluation About the Feasibility of an Unconscious Participatory Sensing System with iOS Devices, International Journal of Informatics Society, vol.8, 2016. (査読有)
- Kohei Tanaka, Fumihito Sugihara, Katsuhiro Naito, Hidekazu Suzuki, Akira Watanabe: Design of an Application Based IP Mobility Scheme on Linux Systems, International Journal of Informatics Society, vol.8, 2016. (査読有)

〔学会発表〕(計６件)

- 内藤 克浩, 榊原 寛紀, 向井 洋介, 森香津夫, 小林 英雄: 無線伝送路情報を鍵として利用するセキュア通信方式の基礎研究, IPSJ MBL 研究会 2015-DPS-163, 2015. (2015/5/28-29・宮古島マリンターミナル・沖縄県・宮古島市)

〔その他〕

ホームページ: http://www.pluslab.org

６．研究組織

(1)研究代表者

内藤 克浩 (NAITO KATSUHIRO)

愛知工業大学 情報科学部

准教授

研究者番号：80378314

(2)研究分担者

なし

(3)連携研究者

なし

(4)研究協力者

なし