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

令和　３ 年　 ６ 月　 １ 日現在

機関番号：３４３１０
研究種目：若手研究(B)
研究期間：2017～2020
課題番号：１７Ｋ１２６７９

研究課題名（和文）劣通信環境における攻撃耐性を備えた高信頼通信システムの構築

研究課題名（英文）Consideration of Reliable Communication Systems in Poor Communication Environments

研究代表者
木村　共孝（Kimura, Tomotaka）

同志社大学・理工学部・准教授

研究者番号：２０７５６３８２

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究は，劣通信環境における攻撃耐性を備えた次世代通信システムの構築を目的とした．近年，通信インフラのない劣通信環境における通信技術の研究が盛んに行われているが，これまでの研究ではネットワークを破壊するような攻撃に対する対策が不十分であった．そこで，本研究では，劣通信環境で発生する特有の攻撃を複数想定し，それらの攻撃の特性を理論解析によって明らかにした．さらに，これらの解析に基づいた対抗策を提案した．

研究成果の学術的意義や社会的意義
本研究では，劣通信環境において発生する独自の攻撃に対する対抗策を提案した．これらの攻撃に対する対抗策の確立によって劣通信環境における通信が安全に行えるようになるため，本研究の社会的意義は高い．また，劣通信環境下における複数の攻撃に対する理論解析によってこれらの攻撃の特性を明らかにしている．さらに，シミュレーション実験により，提案手法の有効性を示しており，学術的意義は高い．

研究成果の概要（英文）：The purpose of this study is to construct a reliable communication system in poor communication environments. In recent years, communication technologies for poor communication environments without communication infrastructure have been extensively studied, but these previous research has been insufficient in countermeasures against attacks that can destroy networks. In this study, we assumed several unique attacks that occur in poor communication environments, and clarified the characteristics of these attacks using theoretical analysis. Furthermore, we proposed countermeasures based on these analyses.

研究分野：通信ネットワーク工学

キーワード：劣通信環境　セキュリティ対策　DTN　蓄積運搬転送

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

大規模な災害の発生によって通信インフラが破壊され，日常で使用されている携帯電話やインターネットなどは全く利用できなくなる危険性があることが，2011 年の東日本大震災で浮き彫りになった．災害直後に被災状況を正確に把握することは救助活動や避難誘導を行う上で極めて重要であるため，通信インフラを必要とせず，端末同士が互いの通信半径内に入った際に情報転送を行うすれ違い通信技術の研究開発が活発に進められている．

既存のすれ違い通信技術はすべての端末が協力的・善意的であることを前提として設計されているため，ネットワークを破壊する攻撃に脆弱である．脆弱性を解消するにはインターネットにおけるセキュリティ対策を用いれば良いように思えるが，端末の密度が疎な劣通信環境では，常時接続できるサーバや認証局が存在しておらず，その適用は困難である．よって，信頼度の高い情報収集を実現するには，劣通信環境下に適したセキュリティ対策の確立が必要不可欠である．ネットワークへの攻撃がシステム性能に大きな影響をおよぼすことが明らかであるにも関わらず，これまで劣通信環境において発生する特有の攻撃についてほとんど議論されていなかった．

２．研究の目的

本研究は，劣通信環境における攻撃耐性を備えた次世代通信システムの構築を目的とした．近年，大規模災害の発生時など通信インフラのない劣通信環境における通信技術の研究が盛んに行われているが，　これまでの研究ではすべての端末が協力的であることを前提としており，ネットワークを破壊するような攻撃をほとんど考慮していない．しかし，実際には，ネットワーク内に攻撃を仕掛ける端末が潜んでいる恐れがあり，劣通信環境下における既存技術は攻撃に極めて脆弱である．そこで，本研究では，劣通信環境で発生する特有の攻撃を複数想定し，それらの対策を提案することで,攻撃耐性を備えた高信頼･高セキュアな通信システムの確立を目指し，研究を遂行してきた．

３．研究の方法

本研究では，研究目的達成のために，三つの攻撃（a）アンチパケット偽造攻撃の対策，(b)フラッディング攻撃，(c)フェイクメッセージ攻撃に着目し，それぞれの攻撃の特徴を明らかにするために，マルコフ解析などの理論解析を行った．さらに，この解析の結果に基づき，対抗策を検討した．

(a)　多くのすれ違い通信技術では宛先へ情報を伝達しやすくするために複製を用いた冗長化を行うが，伝達後も複数の端末が情報の複製を持ち続けることとなる．これらの不要な情報を削除するために，宛先は『アンチパケット』と呼ばれるパケットを伝達直後にブロードキャストを行う．アンチパケットを受け取った端末がその情報をもっていれば削除を行う．アンチパケット偽造攻撃では，この仕組みを悪用し，宛先に情報が伝達されていないにも関わらず，偽造アンチパケットを拡散することでネットワーク内から情報を消滅させることを狙う．情報の消滅を防ぐには，攻撃を検知する方法や，攻撃端末の特定法を考えなければならない．攻撃端末を特定できれば，その端末からのアンチパケットを破棄することによって攻撃を防ぐことができるため，攻撃端末特定方法を考案した．

(b) フラッディング攻撃はネットワーク資源を枯渇させることを目的として，攻撃端末が無用な情報を生成し，その情報の複製をまきちらす攻撃である．一般に，すれ違い通信はネットワーク資源の乏しい劣通信環境下で用いられるため，フラッデイング攻撃をくわえられれば即座にネットワーク資源が枯渇する．資源の枯渇を防ぐには，攻撃による転送量の増加の特性を明らかにし，その特性に基づく攻撃検知法や攻撃端末特定法を考える必要がある．フラッディング攻撃を仕掛けている端末を突き止めることができれば，その端末からの情報の複製を転送しないことで攻撃に対処できるため，攻撃端末の特定方法を検討した．

(c) フェイクメッセージ攻撃では，悪意を持つ攻撃端末が受信したメッセージを改ざんし，その改竄されたフェイクメッセージを拡散する．フェイクメッセージを受け取った中継端末は受信したメッセージが改竄されているか否かを判断する手段を持たないため，中継端末には悪意がないにも関わらず，フェイクメッセージの転送を行う．さらに，宛先端末もフェイクメッセージを判別する手段を持たないため，フェイクメッセージを正常なメッセージとみなして受信する．このようなフェイクメッセージ攻撃に対抗するために，メッセージのハッシュ値を用いた手法を検討した．送信元端末はメッセージを生成すると同時に，ハッシュ値の情報を含んだハッシュパケットを生成する．送信元端末は別の端末と遭遇すると，メッセージとハッシュパケットのいずれか一つを確率的に転送する．

４．研究成果

以下，それぞれの攻撃に対する研究成果を述べる．

(a)アンチパケット偽造攻撃の対策

アンチパケット偽造攻撃の対策として，既存の VACCINE 回復手法を改良し，VACCINE-HR 回復手法を提案した．VACCIN-HR 回復手法は，メッセージ及びアンチパケットの送信などの端末間での手続きは VACCINE 回復手法と同一であり，変更点はアンチパケットのフォーマットと端末内部での処理のみである．VACCIN-HR では，アンチパケットに転送履歴というそのアンチパケットがどの端末を経由して転送されてきたかを示すフィールドを追加する．一方，各端末はメッセージ毎に他端末が持つアンチパケットの転送履歴を収集し，その情報に基づきアンチパケット偽造攻撃を行った端末の候補を抽出して，それらの候補にスコアを加算する．この動作を異なるメッセージに対して繰り返すと，最終的に攻撃端末に対するスコアが正常端末に対するものより大きくなり，攻撃端末の検出が可能となる．転送グラフが有効木になる場合の攻撃検出アルゴリズムとして Algorithm-T，閉路を含む転送履歴がある場合の攻撃検出アルゴリズムとして Algorithm-C をそれぞれ提案した．

表 1: アルゴリズム駆動回数 (宛先端末，10,000 メッセージ)

| 偽造長 $l$ | 攻撃非発生 | 見逃し | Algorithm-T | Algorithm-C |
|---|---|---|---|---|
| 2 | 2307 | 0 | 6252 | 1441 |
| 3 | 2307 | 3047 | 710 | 3936 |
| 4 | 2307 | 2781 | 35 | 4877 |
| 5 | 2307 | 2347 | 0 | 5346 |
| 6 | 2307 | 2046 | 0 | 5647 |
| 10 | 2307 | 1394 | 0 | 6299 |
| 15 | 2307 | 1028 | 0 | 6665 |
| 20 | 2307 | 821 | 0 | 6872 |
| 25 | 2307 | 704 | 0 | 6989 |
| 29 | 2307 | 638 | 0 | 7055 |

表 1 は，宛先端末 D のアルゴリズム実行回数を示している．10,000 個のメッセージのうち，表中の「攻撃非発生」は攻撃を受けなかったメッセージ数，「見逃し」は攻撃が開始されたにも関わらずアルゴリズムが駆動しなかったメッセージ数，「Algorithm-T」と「Algorithm-C」は，攻撃が開始されたメッセージについて，それぞれのアルゴリズムが駆動された回数である．偽造履歴が長くなるに従い，見逃しと Algorithm-T の実行割合は減少する．特に，偽造長が 3 以上の場合には，オリジナルの偽造履歴と偶然同じ正規の転送が発生しなければ転送グラフは有向木にならない．したがって，偽造履歴が長くなるほど，Algorithm-T が実行される割合は小さくなる．なお，この実験では，偽造長が 5 以上については，攻撃が発生したという条件で履歴グラフが有向木になることはなかった．偽造履歴が長くなるに従って Algorithm-C の実行割合が増加するのは，偽造履歴が長いほど閉路が発生しやすくなるためである．

表 2 は，10,000 個のメッセージに対する攻撃端末候補の抽出が終了した後のスコアベクトルを示している．表 2 のいずれにおいても，正常端末と比較して，攻撃端末の累積スコア $x_V^{(M)}$ は非常に大きくなっており，攻撃端末を検出できており，有効な手法であることを示した．

表 2：スコアベクトル $x_V$

| 偽造履歴 | 端末 V | $x_V^{(S)}$ | $x_V^{(D)}$ | $x_V^{(M)}$ | $x_V^{(4)}$ | $x_V^{(5)}$ | $x_V^{(6)}$ | $x_V^{(7)}$ | $x_V^{(8)}$ | $x_V^{(9)}$ | ⋯ | $x_V^{(30)}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D-M | $V = D$ | 0 | 0 | 6371.3 | 50.9 | 53.4 | 47.1 | 49.9 | 42.2 | 48.4 | ⋯ | 46.6 |
| | $V \in \mathcal{N} \setminus \{D\}$ | 0 | 0 | 739.2 | 27.3 | 27.4 | 23.7 | 26.6 | 18.6 | 23.3 | ⋯ | 24.1 |
| D-4-M | $V \in \mathcal{N}$ | 0 | 0 | 1843.3 | 0 | 75.3 | 86.9 | 82.8 | 79.8 | 79.9 | ⋯ | 82.3 |
| D-4-5-6-7-M | $V \in \mathcal{N}$ | 0 | 0 | 2496.2 | 0 | 0 | 0 | 0 | 138.1 | 137.5 | ⋯ | 140.8 |

(b) フラッディング攻撃の対策

フラッディング攻撃を防ぐために，各端末が独自に，他の端末から受信するメッセージ数をカウントし，スコアを算出することで，攻撃端末を検出するという手法を提案した．提案手法では，ネットワーク全体として共通の不審端末を検出するのではなく，各端末が自律分散的に不審端末を検出する．

図 1 はある端末が算出した他の端末 $k$ についての合計スコアを示している．不審端末である ID が 0 の端末のスコアが他の端末よりも大きくなっていることが確認できる．したがって，提案手法によって得られたスコアを比較することで，不審端末を検出でき，提案手法が有効であることが分かった．

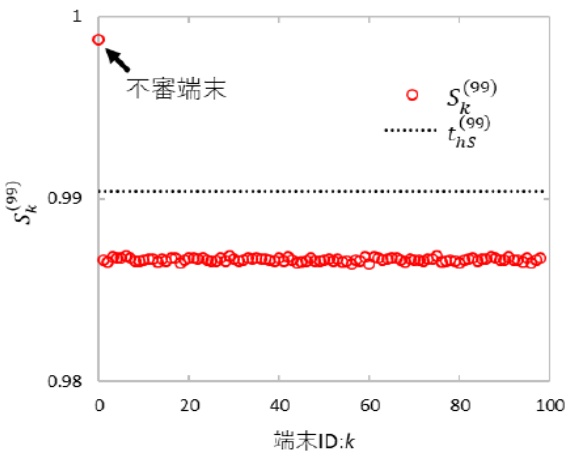


図 1：フラッディング対策法を用いたスコア

(c) フェイクメッセージ攻撃の対策

フィクメッセージ攻撃を防ぐために，ハッシュ関数を用いた対策法を提案した．フェイクメッセージ攻撃の発生を検知するために，送信元端末はメッセージを生成する度に，そのメッセージのハッシュ値を作成する．送信端末が未保持端末と遭遇した際には，メッセージ，もしくは，ハッシュ値のいずれか一つを確率的に転送する．ここで，メッセージを選択する確率を$r$ $(0 < r < 1)$，ハッシュ値を選択する確率を$1 - r$ とする．したがって，(p, q) 感染型ルーチング方式でメッセージ転送を行う場合，メッセージは確率 $rq$で転送され，ハッシュ値は確率$(1-r)q$ で転送される．メッセージとハッシュ値のいずれか一つを持つ中継端末が他の端末と遭遇した際には，保持している情報を確率$p$で転送する．両方を持つ場合，送信元端末と同様に，メッセージを確率$rp$ で，ハッシュ値を確率$(1 - r)p$ で転送する．このようなハッシュ値の転送を行うことによって，受信先端末にメッセージとハッシュ値の両方が配送された場合，正しいメッセージを受信したことが確認できる．さらに，受信先端末がフェイクメッセージとハッシュ値を受信した場合，受信端末はフェイクメッセージのハッシュ値を計算し，ハッシュ値と一致しないため，メッセージの改ざんを検知することができる．

図 2 はポアソン過程に従って端末間の遭遇が発生するシナリオにおける攻撃端末数に対する配送確率の変化を示している．“Legitimate” は正常なメッセージとハッシュ値の組，“Fake” はフェイクメッセージとフェイクハッシュ値の組“Detection” はフェイク検知確率をそれぞれ表している．性能比較のため，“w/o Proposal” は提案手法を用いず，攻撃対策を行わない場合の結果を示している．攻撃端末数の増加に伴い，正常な組の配送確率が減少している．さらに，偽造された組の配送確率はいずれの攻撃端末数に対しても非常に小さいため，提案手法が有効に働いていることが分かる．

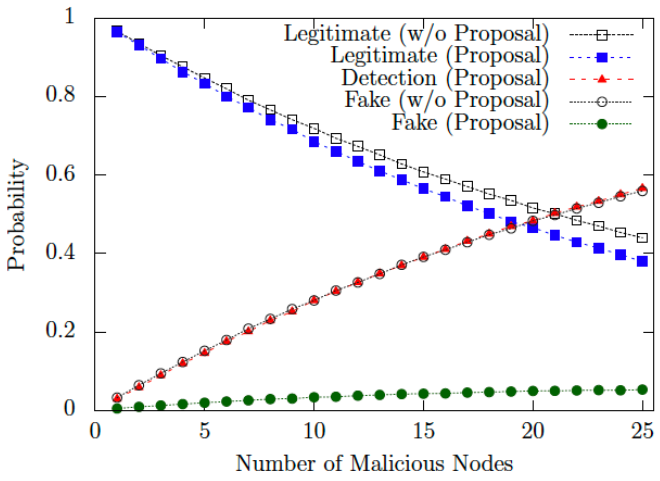


図 2: 配送確率の変化（ポアソン遭遇）

図 3 はリアルトレースデータを用いたシナリオにおける攻撃端末数に対する配送確率の変化を示している．リアルトレースデータを用いた現実に近い遭遇に対しても，提案手法を用いることで偽造された組の配送確率はいずれの攻撃端末数に対しても小さくなっている．したがって，現実的な状況においても提案手法の有効性を示せた．

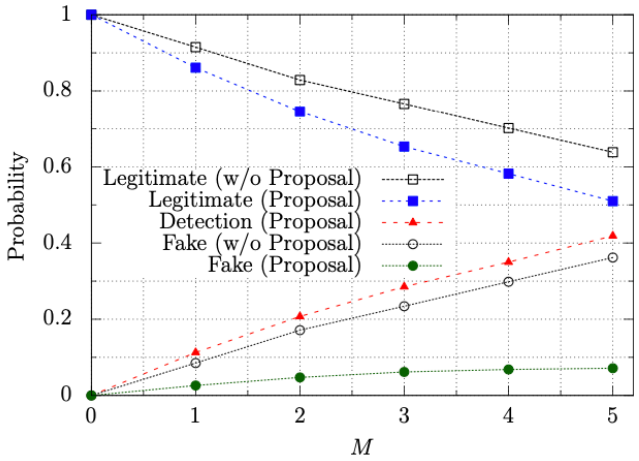


図 3: 配送確率の変化（リアルトレース）

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

| | |
|---|---|
| １．著者名<br>Tomotaka Kimura, Premachandra Chinthaka | ４．巻<br>98 |
| ２．論文標題<br>Suppressive Fair Buffer Management Policy for Intermittently Connected Mobile Ad Hoc Networks | ５．発行年<br>2017年 |
| ３．雑誌名<br>Wireless Personal Communications | ６．最初と最後の頁<br>613～627 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/s11277-017-4886-8 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Inoue Yoshiaki、Kimura Tomotaka | ４．巻<br>39 |
| ２．論文標題<br>Age-Effective Information Updating Over Intermittently Connected MANETs | ５．発行年<br>2021年 |
| ３．雑誌名<br>IEEE Journal on Selected Areas in Communications | ６．最初と最後の頁<br>1293～1308 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/JSAC.2021.3065031 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

〔学会発表〕　計21件（うち招待講演　0件／うち国際学会　7件）

| |
|---|
| １．発表者名<br>Y. Shimizu, T. Kimura, and J. Cheng |
| ２．発表標題<br>Detection Method Against Fake Message Attacks in Sparse Mobile Ad-Hoc Networks |
| ３．学会等名<br>IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2019)（国際学会） |
| ４．発表年<br>2019年 |

| |
|---|
| １．発表者名<br>A. Osamura, T. Kimura, and J. Cheng |
| ２．発表標題<br>Partial Access for LDPC-Coded-IDMA Systems |
| ３．学会等名<br>IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC2019)（国際学会） |
| ４．発表年<br>2019年 |

１．発表者名
T. Idezuka, T. Kimura, K. Hirata, and M. Muraguchi

２．発表標題
Malicious node detection method against message flooding attacks in aparse mobile ad-hoc networks

３．学会等名
Fifteenth International Conference on Wireless and Mobile Communications (ICWMC 2019)（国際学会）

４．発表年
2019年

１．発表者名
T. Kimura, A. Noguchi, K. Hirata, and M. Muraguchi

２．発表標題
Trajectory estimation method using sparsely deployed anchor nodes

３．学会等名
IEEE International Conference on Consumer Electronics - Taiwan (IEEE ICCE-TW 2019)（国際学会）

４．発表年
2019年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
機械学習を用いたネットワーク異常検知システムの脆弱性の評価

３．学会等名
電気学会通信研究会

４．発表年
2020年

１．発表者名
清水裕貴，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網におけるフェイクメッセージ攻撃に対する検知手法の性能評価

３．学会等名
電子情報通信学会コミュニケーションクオリティ研究会

４．発表年
2019年

１．発表者名
木村共孝，野口晃，平田孝志，村口正弘

２．発表標題
疎に配置されたアンカーノードを用いた移動軌跡の推定法

３．学会等名
電子情報通信学会コミュニケーションクオリティ研究会

４．発表年
2019年

１．発表者名
清水裕貴，木村共孝，程俊

２．発表標題
Convolutional Neural Networksを用いた通信ネットワークの頑強性推定

３．学会等名
電子情報通信学会 超知性ネットワーキングに関する分野横断型研究会

４．発表年
2019年

１．発表者名
小川侑治，木村共孝，程俊

２．発表標題
機械学習を用いたネットワーク異常検知システムの脆弱性の評価

３．学会等名
電子情報通信学会 超知性ネットワーキングに関する分野横断型研究会

４．発表年
2019年

１．発表者名
清水裕貴，木村共孝，程俊

２．発表標題
疎密度モバイルアドホック網におけるホップ回数を用いたフェイクメッセージ攻撃の対策

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会

４．発表年
2019年

１．発表者名
Takuya Idezuka, Tomotaka Kimura, Masahiro Muraguchi

２．発表標題
Behavior Analysis of Flooding Attacks in Sparse Mobile Ad-Hoc Networks

３．学会等名
2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2018年

１．発表者名
Tomotaka Kimura, Chinthaka Premachandra

２．発表標題
Aggressive Recovery Scheme for Multicast Communication in Intermittently Connected Mobile Ad-Hoc Networks

３．学会等名
33rd International Conference on Information Networking (ICOIN 2019)（国際学会）

４．発表年
2019年

１．発表者名
清水裕貴，木村共孝，程 俊

２．発表標題
疎密度モバイルアドホック網におけるフェイクメッセージ攻撃の検知手法

３．学会等名
電子情報通信学会 ネットワークシステム研究会

４．発表年
2019年

１．発表者名
木村共孝，白石航輝，平栗健史

２．発表標題
ドローンメッシュネットワークにおけるアンテナの指向性を考慮した経路選択の検討

３．学会等名
電子情報通信学会 コミュニケーションクオリティ研究会

４．発表年
2019年

１．発表者名
雑賀大輔，木村共孝，滝根哲哉

２．発表標題
VACCINE-HR：疎密度MANETにおけるアンチパケット偽造攻撃対策

３．学会等名
電子情報通信学会 コミュニケーションクオリティ研究会

４．発表年
2018年

１．発表者名
可香谷昌人，木村共孝，平田孝志，村口正弘

２．発表標題
受信信号強度を考慮したマルコフ近似によるアクセスポイント選択法

３．学会等名
電気学会 通信研究会

４．発表年
2018年

１．発表者名
出塚拓也，木村共孝，平田孝志，村口正弘

２．発表標題
疎密度モバイルアドホック網におけるメッセージフラッディングの検出手法

３．学会等名
電気学会 通信研究会

４．発表年
2018年

１．発表者名
出塚拓也，木村共孝，村口正弘

２．発表標題
疎密度モバイルアドホックネットワークにおけるメッセージフラッディングの分析

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会（MIKA2018）

４．発表年
2018年

| |
|---|
| １．発表者名<br>木村 共孝，村口 正弘 |
| ２．発表標題<br>疎密度モバイルアドホックネットワークにおけるフラッディング攻撃の分析 |
| ３．学会等名<br>電子情報通信学会コミュニケーションクオリティ研究会 |
| ４．発表年<br>2017年 |

| |
|---|
| １．発表者名<br>Tomotaka Kimura, Masahiro Muraguchi |
| ２．発表標題<br>Buffer Management Policy Based on Message Rarity for Store-Carry-Forward Routing |
| ３．学会等名<br>Asia-Pacific Conference on Communications (APCC2017)（国際学会） |
| ４．発表年<br>2017年 |

| |
|---|
| １．発表者名<br>長久保智子，木村共孝，程　俊 |
| ２．発表標題<br>疎密度モバイルアドホック網における正常転送回数を用いたフェイクメッセージ攻撃の対策 |
| ３．学会等名<br>電気学会通信研究会 |
| ４．発表年<br>2021年 |

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 |
| --- | --- |