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　５ 年　 ６ 月 １５ 日現在

機関番号：２０１０３
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１７７２

研究課題名（和文）モバイルエッジコンピューティングにおける分散同期型攻撃の特性に関する研究

研究課題名（英文）A Study on Distributed Synchronous Attacks in Mobile Edge Computing

研究代表者
稲村　浩（Inamura, Hiroshi）

公立はこだて未来大学・システム情報科学部・教授

研究者番号：２０７８０２３２

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：高度化し悪質化の兆しのある分散同期型攻撃について、特に低量DoS/DDoS攻撃に関する実践的な知見を蓄積することを目的とする。LDDoSはDDoSと異なり遥かに低量の攻撃トラフィックを用い、 多数のノードが同期して攻撃を行うことで検知のしにくさを企図した攻撃手法である。その適用性や攻撃特性、分散攻撃を実現するMirai等のIoTマルウェアの特性を明らかにするために、特定が未知のボトルネックリンクに対する低量DoSによる攻撃戦略の明確化、分散攻撃に必要なボットネットを構築するIoTマルウェアの分類問題への攻撃可能性、短時間転送を標的とした低量DoS攻撃の検討の3つの課題について検討した。

研究成果の学術的意義や社会的意義
リモートワークが社会的に活用される昨今，サテライトオフィスや家庭ネットワークでも重要な業務が実施されることが想定される.モバイル端末での個々の遠隔業務や，PC 等で運用される SSL/TLS VPN を対象としたリモートエントランス経路そのものを狙い，Low-rate DoS攻撃の攻撃効果による QoS の低下によって目的のサービスを許容できない水準まで低下させることで業務の妨害を図るといった攻撃シナリオを検討した。さらに分散同期型攻撃に参加する可能性のある、管理されていないIoTデバイスの悪用対策のために重要なマルウェアの分析手法への攻撃の可能性についても議論した。

研究成果の概要（英文）：The purpose of this study is to accumulate practical knowledge on distributed synchronous attacks, especially Low-rate DoS/DDoS attacks, which are becoming more sophisticated and malicious. LDDoS is an attack method that uses a lower volume of attack traffic than DDoS and attempts to make it difficult to detect by synchronizing many nodes. To clarify its applicability, attack characteristics, and characteristics of IoT malware such as Mirai that realize distributed attacks, we clarified the attack strategy using Low-rate DoS attacks against bottleneck links whose characteristics are unknown, the possibility of attacking the classification problem of IoT malware that builds botnets necessary for distributed attacks, and the possibility of attacking low-volume DoS targeting short-time transmission.

研究分野：情報ネットワーク

キーワード：Network Security　Low-rate DoS　IoT malware　TCP

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

IoT デバイスが活用されるモバイルエッジコンピューティングでは、多数のノードが地理的に分散した運用形態を前提している。本研究課題では分散同期型攻撃を、ネットワークに分散して存在する悪意のあるノードが特定の対象に向けて同期し協調した攻撃を行うことと定義する。分散同期型攻撃の代表的な例として DDoS がある。昨今の事例ではマルウェアとして Mirai による Dyn への DDoS 攻撃が有名である。2016 年 10 月に発生した、DNS サーバープロバイダである Dyn 社への DDoS 攻撃では、十分に管理されていない IoT デバイスによるボットネットが利用され史上最大規模である 620Gbps の攻撃が観測された。管理されていない IoT デバイスの現状把握については様々な取り組みが成されている。我々は最近、その可能性と実現性が指摘され研究が始まっている Low rate DDoS(LDDoS) に着目する。LDDoS は DDoS と異なり遥かに低量の攻撃トラフィックを用い、多数のノードが同期して攻撃を行うことで検知のしにくさを企図した攻撃手法である。分散同期型攻撃と括った場合、攻撃成立のための要求条件において LDDoS は DDoS と丁度、対角線上の位置付けになる。すなわち、要求される攻撃ノードの同期のタイミングの厳密さにおいて DDoS < LDDoS であるのに対して要求される攻撃トラフィックの量は DDoS >> LDDoS という関係にある。

LDDoS 攻撃の原理となる LDoS 攻撃が Kuzmanovic らによって提案されている。これは、TCP 通信に対する攻撃手法であり、ラウンドトリップタイム(RTT)程度の幅の短時間のバースト攻撃トラフィックと無通信が周期 T で繰り返される矩形波状のトラフィックを再送タイムアウトの長さ(RTO)に重なるように連続で送信することで、対象の TCP コネクションに再送タイムアウトを継続させ、通信がほぼできない状態にする攻撃である。LDDoS 攻撃は、LDoS 攻撃に必要なバースト通信を複数の攻撃元ホストから分割して送信し、攻撃対象ホストで集約することで LDoS バーストを発生させる攻撃である。この手法により単一のバースト通信は小さくて済むため、通常のトラフィックとの判別が難しくなる。既存手法の有効性はネットワークシミュレータ上で明らかにされているが、実践的な知見が求められている。まず実際のネットワーク機材による実験環境において LDDoS の実現可能性を確認し、その攻撃の構成要件を得て、それらの充足を防ぐシステムの機能を設計するために、これまで我々が検討してきた IoT デバイス間の同期の抑止についての知見が活用できるのではないかという着想を得た。

２．研究の目的

本研究課題では、高度化し悪質化の兆しのある分散同期型攻撃について、特に低量 DoS/DDoS 攻撃に関する実践的な知見を蓄積することを目的とする。その適用性や攻撃特性、分散攻撃を実現する Mirai 等の IoT マルウェアの特性を明らかにするために、以下の 3 つの課題について検討し明らかにする。

① 特定が未知のボトルネックリンクに対する低量 DoS による攻撃戦略の明確化
② 分散攻撃に必要なボットネットを構築する IoT マルウェアの分類問題への攻撃可能性
③ 短時間転送を標的とした低量 DoS 攻撃の検討

３．研究の方法

① 特定が未知のボトルネックリンクに対する低量 DoS による攻撃戦略の明確化

Shrew 攻撃を成功させるためには、送信する攻撃パルスの合計ピークレートが標的ネットワークのボトルネックリンク帯域幅以上の値に設定される必要がある。これを言い換えると、現実の攻撃シナリオにおいて、攻撃者が標的 TCP フローの経路上のボトルネックリンク帯域幅をあらかじめ知っていることが必要であることを意味する。しかし、現実の攻撃シナリオにおいて、攻撃者が常に標的ボトルネックリンクのパラメータを熟知しているとは限らない。そこで、攻撃パルスのパラメータの中で最も重要なパルスレートに関連するボトルネックリンクの帯域幅とバッファサイズが攻撃者に未知の場合を想定し、観測に基づいた攻撃強度の自動最適化のための LDDoS 攻撃戦略を提案する。提案戦略は、ボットネットによって自動化されることを想定しており、ネットワークパラメータが未知のボトルネックリンクに対して有効な攻撃パルスレートの最適化を、ステルス性を維持しながら行うことを目的とする。ステルス性とは、必要十分な攻撃トラフィックのみをネットワーク内に存在させ検知を防止することで得られる攻撃の隠蔽性を指す。

② 分散攻撃に必要なボットネットを構築する IoT マルウェアの分類問題への攻撃可能性

公開されたソースコードを使用した亜種生成により IoT マルウェアが急増している。人手による解析は時間がかかるため、マルウェアの亜種の増加は解析者の負担を増加させる。この問題に対して、マルウェアファミリの分類が有用である。マルウェアファミリとは、マルウェアのオリジナルと亜種をグループ化したものである。同じファミリに属するマルウェアは機能が類似しているため、新たな解析を行う必要性が薄い。解析を行う場合でも、オリジナルや他の亜種の解析結果を参考にできるため、少ない解析で済み解析者の負担軽減ができる。

IoT マルウェアの分類では、マルウェアの画像化による分類手法が役立つ。多くの IoT マルウェアは静的リンクであり、シンボル情報も削除されている。そのため、Windows で行われるような、リンクされたライブラリ関数によるマルウェア分類手法などを用いることができない。リンクされた関数の情報を使用しない分類手法は複数提案されているが、画像化による分類手法は従来手法と比較して高い精度が得られる報告があり、IoT マルウェア の分類に適していると考えられる。画像化による分類手法は、マルウェアのバイナリ変更の影響を受ける。そのため、プログラムの動作が変わらないバイナリ変更は画像化による分類手法への攻撃手法と考えることができる。このようなバイナリ変更の手段として、ソースコードの難読化処理を検討する。マルウェアファミリの分類に対して攻撃を受けた場合、新たに検出された全てのマルウェアの亜種に対して解析を 行う必要があり、解析者の負担が増大しマルウェアの急増に対応できない。マルウェアの画像化による分類手法の精度向上のためには、上記のような今後想定される攻撃に対する対処を検討しておくことが重要である。本研究では、ソースコードに施す難読化を攻撃手法として想定し、その効果と対処を検討する。

③ 短時間転送を標的とした低量 DoS 攻撃の検討

近年、マイクロサービスアーキテクチャの普及や通信速度の向上により、対話型トランザクションなどで発生する短時間転送が多く行われている。これに伴い、短時間転送に対する安全性の提供が要求されている。サイバー攻撃の 1 つとして、パルス形状の攻撃トラフィックを用いることで平均帯域利用率が低 い Low-rate DoS(LDoS)攻撃が議論されている。LDoS 攻撃に関する既存研究では、FTP などを用いた大容量のデータ転送時に発生する長時間転送を攻撃対象としていた。LDoS 攻撃はパルス形状の攻撃トラフィックを用いるため、転送時間が短い場合には攻撃パルスが攻撃対象トラフィックと衝突する確率が低くなる事が想定される。本研究では、gRPC を用いた短時間で転送が終了する短時間通信を攻撃対象とし、LDoS 攻撃の 1 つである Shrew 手法を用いた攻撃手法の実現性を示す。

４．研究成果

① 特定が未知のボトルネックリンクに対する低量 DoS による攻撃戦略の明確化

従来研究では議論されていなかった LDDoS における攻撃強度の決定について攻撃効果計測と攻撃を一体化した適応的な制御方法の提案を行った(図 1 参照)。具体的には以下の通りである。

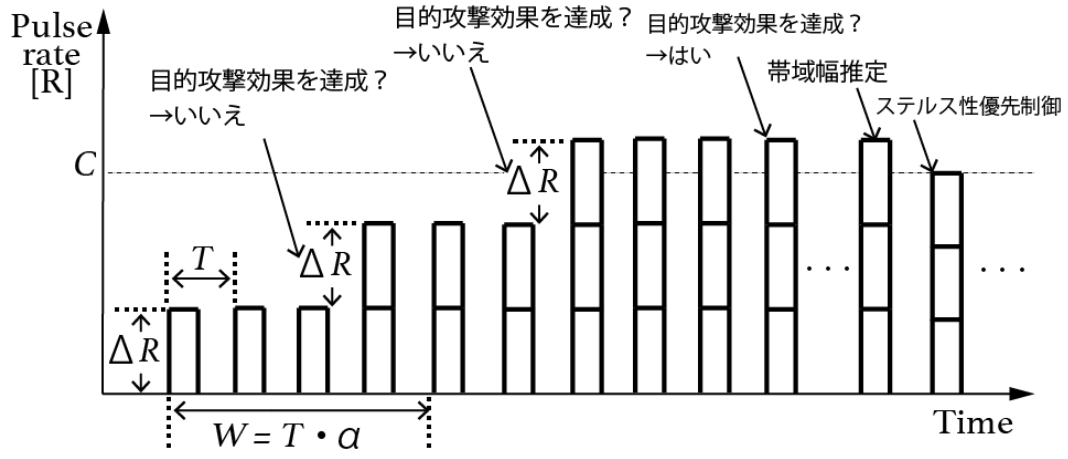


図 1. 提案戦略によるパルスレートの増減

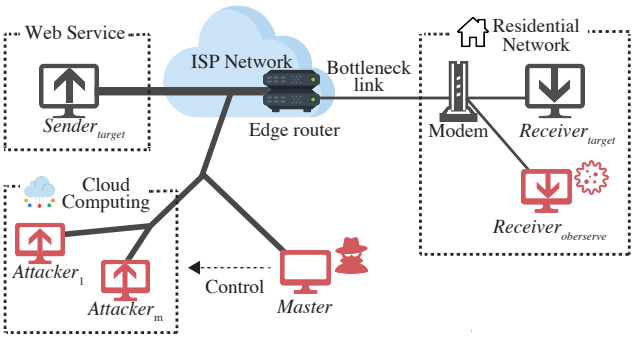


図 2.　攻撃シナリオの適用例

(1)　標的 TCP フローと競合する観測 TCP フローから攻撃効果を推定することで、特性が未知のボトルネックリンクに対して、自動でパルスレートの最適化を行い、攻撃者が指定した値まで標的 TCP の品質を低下させることが可能であることを示した。3 つの異なるパラメータによるシミュレーションシナリオ(図 2 参照)において、本提案手法による攻撃効果を優先した攻撃を行ったことでボトルネックリンク使用率を 44% ~ 45%に低下させ、500kbps の目標帯域幅を十分下回る平均スループットまで対象の通信を抑制できることを確認した。しかし攻撃フローの帯域使用率は 43% ~ 45%となっておりステルス性の低下が見られた。

(2)標的ネットワークに送信されたパルスレートを観測することで、ボトルネックリンク帯域幅を推定し、ボトルネックリンクの特性が未知の場合においてもステルス性の高い LDDoS 攻撃が実行可能であることを示した。前項と同様のパラメータによるシミュレーションシナリオにおいて、本提案手法のステルス性を優先とする攻撃を行ったことで攻撃フローの帯域使用率を 30%に留め、ボトルネックリンク使用率を 35% ~ 55% まで低下させ LDoS 攻撃の原理的な成功を確認した。ただし設定した 500kbps の目標帯域幅を下回ることは確認できなかった。

(3)提案戦略の対策として、既存研究の手法を援用してボトルネックリンクのバッファサイズを大きく設定することを提案し、攻撃下でバッファサイズを一時的に通常の 2 倍に設定することで、攻撃パルスが過剰に送信されステルス性を失うことを示した。この対策の実現において考慮すべき前提について議論した。

④　分散攻撃に必要なボットネットを構築する IoT マルウェアの分類問題への攻撃可能性

ソースコードへの難読化処理による画像分類手法への攻撃の概要を図 3 に示す。マルウェアの画像分類手法では収集したマルウェアを画像化し、CNN(Convolutional Neural Network)による深層学習により分類を行う。この 画像分類手法への攻撃方法として、Obfuscator-LLVM によるソースコードへの難読化処理を用いてマルウェアを生成する。難読化されたマルウェアはバイナリ表現が変化しているため、画像化するとオリジナルのマルウェアと視覚的な違いが生まれる。攻撃の実装方法では収集したマルウェアのテストデータを難読化されたマルウェアのバイナリ画像と入れ替えることで検証を行う。難読化処理による画像分類手法への攻撃有効性が確認された場合、難読化を施したサンプルを用いた訓練を行うことで対処を試みる。

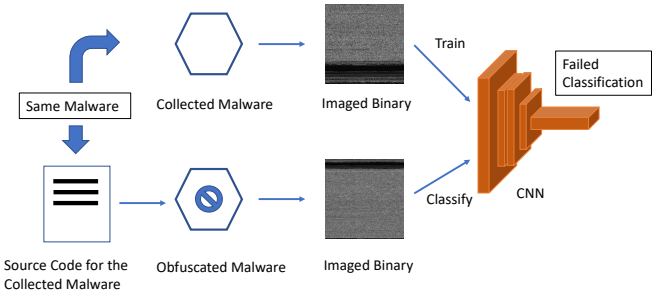
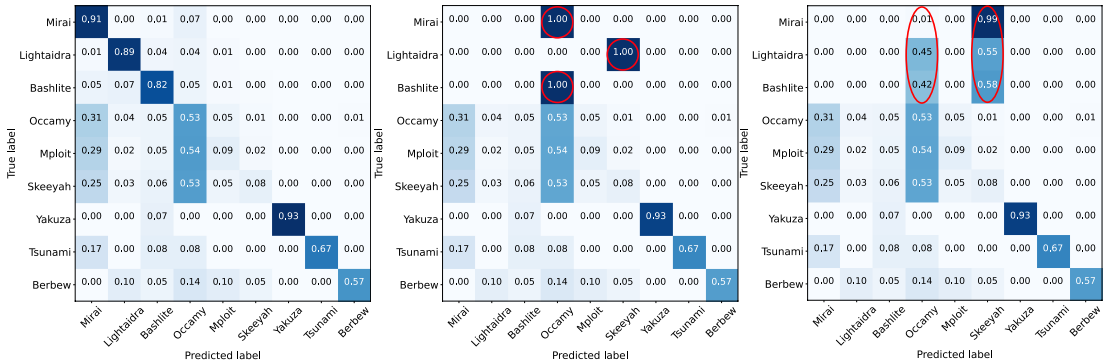


図 3　攻撃の概要

Original の分類結果と clang による攻撃及び clang + oLLVM による攻撃を比較すると(図 4 参照)、攻撃したマルウェアファミリである Mirai、Lightaidra、Bashlite が全て誤分類されていることが分かる。clang を用いた攻撃効果が認められることから、LLVM を通したセクション再配置の効果が大きいと考えられる。Clang による攻撃はランダム性がないため全て同じファミリに分類されているが、oLLVM による難読化は毎回異なるバイナリが生成されるため、バイナリによって分類されるファミリが変化している。本実験では、コンパイル時に適用する難読化処理が IoT マルウェアの画像分類手法への単純な攻撃として一定の効果を持ち得ることが確認できた。マルウェアの画像化による分類手法の精度向上のためには、このような想定される攻撃への対処が必要である。



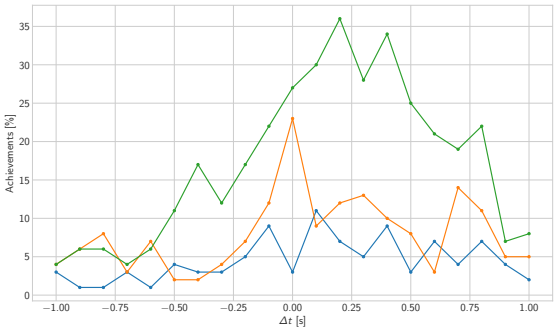
Original の分類結果　　Clang による攻撃　　Clang+oLLVM による攻撃

図 4. マルウェアファミリ分類結果のヒートマップ

本稿では、ソースコードに施す難読化処理によるマルウェアの画像分類手法への攻撃効果及び難読化を施したサンプルを用いた訓練による対処を示した。難読化なしの収集したマルウェアを用いて画像分類器を作成し、攻撃手法として難読化を施したマルウェアを分類させたところ、攻撃対象のマルウェアファミリである Mirai、Lightaidra、Bashlite は全て誤分類された。この手法に対処するため難読化を施したサンプルを用いたマルウェアの画像分類器を作成し、約 60%以上の精度で分類可能であることを確認した。コンパイル時に適用する難読化処理は IoT マルウェアの画像分類手法への単純な攻撃として一定の効果を持ち得た。この攻撃は難読化を施したサンプルを用いた訓練により対処可能なため、画像分類に基づく分類器を用いる際には予め難読化を施したサンプルを用いて訓練させることを考慮すべきである。

② 短時間転送を標的とした低量 DoS 攻撃の検討

短時間転送に対して Shrew 手法を用いる場合、攻撃対象トラフィックに攻撃開始タイミングを合わせることができるかが課題となる。しかしながら、現実世界に存在する攻撃対象の環境を考えると、正確な攻撃開始タイミングを推定できるよう通信を監視することは難しい。本研究では、



従来の Shrew 手法では対応が難しかった短時間で転送が終了する短時間通信に対して、初期パルス幅を拡大し攻撃開始タイミングの誤差許容性能を向上させる Fawe-Shrew 手法を提案した。初期パルスによる攻撃成功後は RTO 処理が発生するため、minRT O 秒間隔での短時間パルスによる攻撃という従来の Shrew 手法と同様の攻撃を行う。これにより、ステルス性を維持したまま短時間転送

図 5. 攻撃タイミング誤差 Δt における目標攻撃効果の達成率

表 1. 初期パルス幅ごとの許容誤差性能

初期パルス幅 L_i	Δt_{min}	Δt_{max}	許容誤差性能 D
0.3	0.10	0.10	0.00
0.5	−0.10	0.70	0.80
1.0	−0.40	0.80	1.20

に対しての攻撃効果を高めることが可能となる。Fawe-Shrew 手法の誤差許容性能を検証するため、従来の Shrew 手法である初期 パルス幅 Li = 0.3 と、拡大した初期パルス幅 Li = 0.5、1.0 の 3 パターンにおいて、攻撃開始タイミングと攻撃対象トラフィックの転送開始タイミングをずらし、目標攻撃効果 E > 70 % の達成率を用いて評価した(図 5、表 1 参照)。評価結果より、提案した Fawe-Shrew 手法に初期パルス幅を拡大することで、攻撃開始タイミングの誤差許容性能を向上可能であることが明らかとなった。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1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 髙橋 佑太、稲村 浩、中村 嘉隆	４．巻 64
２．論文標題 特性が未知のボトルネックリンクに対する低レートDDoS攻撃の戦略	５．発行年 2023年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 465～477
掲載論文のDOI（デジタルオブジェクト識別子） 10.20729/00224259	査読の有無 有
オープンアクセス 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 －

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 佐藤大介，稲村浩，中村嘉隆
２．発表標題 Robust WREDによるLow-rate Shrew DoS攻撃に 対する保護緩和機構の提案
３．学会等名 情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2021）シンポジウム論文集，pp.90-97
４．発表年 2021年

１．発表者名 佐藤隼斗，稲村浩，石田繁巳，中村嘉隆
２．発表標題 IoTマルウェアの画像分類手法への 難読化による攻撃の試み
３．学会等名 情報処理学会研究報告，Vol.2021-MBL-101，No.22，pp.1-6
４．発表年 2021年

１．発表者名 久末瑠紅，稲村浩，石田繁巳，中村嘉隆
２．発表標題 gRPC通信に対するLow-rate DoS攻撃 の試み
３．学会等名 情報処理学会第84回全国大会講演論文集，Vol.2022，pp.3_391-3_392
４．発表年 2022年

１．発表者名
Yuta Takahashi, Hiroshi Inamura, Yoshitaka Nakamura

２．発表標題
A Low-rate DDoS strategy for unknown bottleneck link characteristics

３．学会等名
International Workshop on Pervasive Information Flow (PerFlow'21) in conjunction with PerCom 2021, pp.508-513, March 2021, Virtually Kassel, Germany.（国際学会）

４．発表年
2021年

１．発表者名
髙橋佑太，稲村浩，中村嘉隆

２．発表標題
特性が未知のボトルネックリンクに対して有効なLow-rate DDoS攻撃戦略の検討

３．学会等名
情報処理学会研究報告，Vol.2020-MBL-97，No.4，pp.1-9，2020年11月

４．発表年
2020年

１．発表者名
佐藤大介，稲村浩，中村嘉隆

２．発表標題
WREDに対する高いIP Precedenceを用いたLDoS攻撃の分析

３．学会等名
情報処理学会第83回全国大会講演論文集，Vol.2021，pp.3_269-3_270，2021年3月.

４．発表年
2021年

１．発表者名
Hayato Sato, Hiroshi Inamura, Shigemi Ishida, and Yoshitaka Nakamura

２．発表標題
Plain source code obfuscation as an effective attack method on IoT malware image classification

３．学会等名
Proceedings of the 2023 IEEE Computer Society Signature Conference on Computers, Software, and Applications (COMPSAC2023), June 2023, Torino, Italy. (to appear)（国際学会）

４．発表年
2023年

１．発表者名 川内谷玲己斗，久末瑠紅，稲村浩，石田繁巳，中村嘉隆
２．発表標題 QUIC通信に対するLDoS攻撃の可能性の検討
３．学会等名 情報処理学会第85回全国大会講演論文集，Vol.2023，pp.3_409-3_410，2023年3月
４．発表年 2023年

１．発表者名 久末瑠紅，稲村浩，石田繁巳，中村嘉隆
２．発表標題 攻撃タイミングの誤差を許容する短時間通信向けLow-rate DoS攻撃の提案
３．学会等名 マルチメディア，分散，協調とモバイル（DICOMO2022）シンポジウム論文集，pp.1497-1504，2022年7月
４．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （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