情報処理学会論文誌 Vol.60 No.12 2245–2258 (Dec. 2019)

モバイルネットワークにおける異常フローの分散管理遮断方式

鈴木 敏明[1,a)] 梶原 貴利[2] 本橋 知子[3] 小村 和司[2]

受付日 2019年3月8日, 採録日 2019年9月11日

概要：近年，自動車等の多様な移動体が通信ネットワークに接続され，通信ネットワークを経由した管理やサービスの提供が進展している．一方，通信ネットワークにおいては，アプリケーションサービス等を提供するサーバに対して，遠隔の端末から多数の不要データを送信することにより，通信ネットワークにおける帯域不足を誘発する等のサイバー攻撃が発生している．従来は，固定端末等からのサイバー攻撃が主であった．今後は，移動体を対象としたサイバー攻撃対応が望まれる．本論文では，異常フローを送信する移動体の基地局間移動を対象とし，移動後においても遅滞なく異常フローの遮断継続が可能な方式を提案する．提案方式では，複数の基地局が存在する領域をリージョンとして管理し，リージョン単位にゲートウェイで異常フローを遮断する．特に，異常フローを送信する移動体が接続する基地局エリアに対して隣接する基地局エリアすべてに遮断を設定する．また，各リージョンに設置した管理サーバが遮断情報を共有する分散型のネットワーク管理により，隣接リージョンに対しても遮断の設定が実行される．これにより，異常フローを送信する移動体が基地局間を移動するようなモバイルネットワークに対して，遅滞のない異常フロー遮断が可能となる．

キーワード：サイバー攻撃，異常フロー遮断，分散型ネットワーク管理，モバイルネットワーク

Distributed Management for Abnormal Flow in Mobile Network

Toshiaki Suzuki[1,a)] Takatoshi Kajiwara[2] Tomoko Motohashi[3] Kazushi Komura[2]

Received: March 8, 2019, Accepted: September 11, 2019

Abstract: Lately, a variety of mobile objects such as cars have been connected to a communications network. In addition, a diversity of services that are provided by way of a communications network have been popular. On the other hand, number of cyber-attack that causes lack of bandwidth in the communications network by sending many abnormal data flows from a remote terminal to a server providing application services has been increasing. Conventionally, cyber-attack was mainly made from/to fixed terminal. The cyber-security involving mobile objects is expected in future. In this paper, a novel scheme to dicard abnormal flows sent by a mobile object moving between base stations is proposed. In the proposed scheme, multiple base station areas are managed as a region. In each region, a gateway that connects all base stations discards abnormal flows. Specifically, configurations to discard abnormal flows are set in all base station areas in the region where a mobile object sends abnormal flows. These configurations are shared with neighbor regions by exchanging information between region management servers. Therefore, abnormal flows are timely dicarded even if a mobile objet sending them moves between base station areas.

Keywords: cyber-attack, abnormal flow discarding, distributed network management, mobile network

[1] 株式会社日立製作所研究開発グループ
Research & Development Group, Hitachi Ltd., Kokubunji, Tokyo 185–8601, Japan
[2] 株式会社日立製作所 IoT・クラウドサービス事業部
IoT & Cloud Services Business Division, Hitachi, Ltd., Yokohama, Kanagawa 240–0005, Japan
[3] 株式会社日立製作所 IoT・クラウドサービス事業部
IoT & Cloud Services Business Division, Hitachi, Ltd., Shinagawa, Tokyo 140–8573, Japan
[a)] toshiaki.suzuki.cs@hitachi.com

1. はじめに

近年，携帯電話のほか，パーソナルコンピュータやタブレット端末，ゲーム機，また自動車等の多様な移動体が通信ネットワークに接続され，通信ネットワークを経由した管理やサービスの提供が進展している．たとえば，通信ネットワークを介した管理として，遠隔からの自動車状態管理等があげられる．また，将来的には通信ネットワークを介した遠隔運転制御が想定されている．高速移動する自動車に対して遠隔からの制御を実施するためには，低遅延かつ安定した帯域を有するネットワーク接続が必要になると考えられ，そのような高品質な通信環境を提供する通信ネットワークが必要とされている．

一方，通信ネットワークにおいては，アプリケーションサービス等を提供するサーバに対して，遠隔の端末から多数の不要データを送信することにより，通信ネットワークにおける帯域不足を誘発，あるいはサーバにおける処理を過負荷とすることにより，アプリケーションサービスの提供不全を発生させる等のサイバー攻撃が発生している．また近年では，通信ネットワークを介して遠隔から自動車を不正制御可能な事例が検出され，自動車および通信ネットワークにおけるセキュリティ対策が望まれている．特に，自動車が遠隔から不正制御される場合，あるいは通信不全により遠隔制御が不能になった場合の被害は甚大になる可能性が高いため，自動車等を接続する通信ネットワークにおいては，サイバー攻撃への耐性が必要とされている．

これまでの通信ネットワークにおいては，アプリケーションサービスやコンテンツ等を提供する静的なサーバへのサイバー攻撃が主流となっており，それらに対するセキュリティ対策技術やシステムの開発が多数実施 [1], [2], [3] されてきた．しかし，今後は，移動体へのサイバー攻撃，あるいは移動体からのサイバー攻撃が増加すると想定され，移動体を中心としたサイバー攻撃対策が必要である．たとえば，通信ネットワークに接続した自動車から多数の異常フローを送信するといったように，アプリケーションサービスを提供するサーバへのサイバー攻撃等が想定される．そのため，今後は高速な移動体の考慮が必要であり，それらの移動に依存することなく，サイバー攻撃の遮断を継続して実行可能な通信ネットワークの実現が必要とされる．

本論文では，異常フローを送信する移動体の基地局間移動を対象とし，移動後においても遅滞なく異常フローの遮断継続が可能な方式を提案する．

以降の構成は，以下のとおりである．2 章において関連研究について述べる．3 章では，対象とするシステム構成と課題，および対応方針について述べる．4 章では，ハンドオーバに対応する異常フローの遮断方式を提案する．5 章では提案方式について評価を行い，6 章において結論を述べる．

2. 関連研究

サイバーセキュリティ関連として，多数の研究が実施されている．たとえば，DoS/DDoS（Denial of Service attack/Distributed DoS）を対象とした研究 [4], [5] が実施されている．対策方式としては，ネットワークドメインに不整合な IP アドレスを有するパケットを制御する，あるいは，過去の伝送履歴に対して想定されない IP（Internet Protocol）アドレスを有するパケットを制御する等，様々に研究が実施されている．

また，センサからのデータ収集において，整合性のないデータ挿入が行われる状況に対するサイバーセキュリティについても研究 [6], [7], [8] が精力的に実施されている．

さらに，データマイニングや機械学習を用いた侵入検知等についても研究 [9] が実施されている．たとえば，サイバー攻撃における特徴をベースとして検知する方式や，通常と異なる異常レベルにより検知する方式等，多数の研究が調査・報告されている．

一方，サイバーアタックに対する検知や防御技術の研究のほか，サイバーセキュリティに対する人材育成等のためのテストベッドの研究 [10] も推進されている．

上記で紹介した関連研究では，主にサイバー攻撃を実行する側，およびアタックされる側が物理的に移動しない，静的な状況を主な対象とした研究となっている．本論文では，サイバー攻撃を実行する側等が物理的に移動し，かつ攻撃を継続するような動的な状況を対象としている．具体的には，異常フローを送信する移動体が，基地局エリアをハンドオーバしながらサイバー攻撃を継続するような状況を対象としている．このような設定の下，本論文では，ハンドオーバに追随して，異常フローの遮断継続が可能なシステムについて提案する．

3. 対象システムの課題と対応方針

3.1 対象システム

図 1 に，対象とするネットワークシステムの構成を示

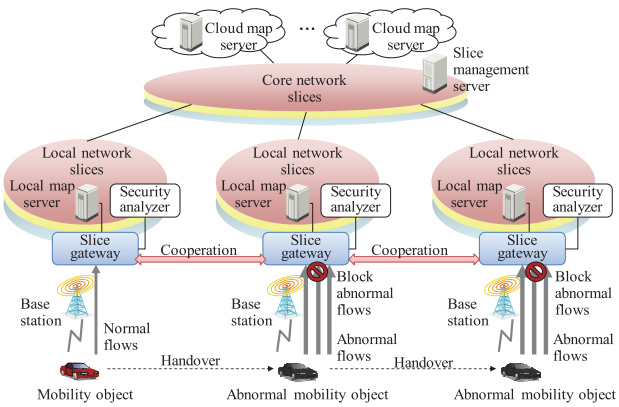

図 1 対象とするネットワークシステム
Fig. 1 Target network system.

す．本システムは，自律走行する自動車等の移動体に対して，ネットワークを介して地図や道路状況等の情報を提供することにより，移動体は受信した情報を活用し，より安定した自律的な走行を実現するシステムである．また，コアネットワークおよびローカルネットワークの物理的なリソースを論理的に分割管理した仮想ネットワーク（ネットワークスライス）をスライス管理サーバにより管理・形成し，サービスごとに異なるネットワークスライスで収容することにより，サービス間の影響を遮断するシステムである．

目標とするシステムは，無線接続を提供するローカルネットワークと，ローカルネットワーク間を接続するコアネットワークとから構成される．コアネットワークに接続されたクラウドでは，移動体に対して提供する地図情報のオリジナルデータを保持する地図情報サーバが存在する．一方，ローカルネットワーク側には，地図情報の配信遅延を削減するため，クラウド内の地図情報サーバから複製した地図情報を保持するローカルな地図情報サーバが存在する．移動体は，基地局間をハンドオーバし，ローカルに存在する地図情報サーバより地図情報を受信し，安定した自律走行を実現する．

本システムでは，移動体がウィルス等に感染し，異常なデータフローを多数送信するサイバー攻撃等を開始した場合に，その異常なデータフローをハンドオーバに追随して遮断することを目的としている．本システムでは，移動体から送信される地図情報要求等のデータフローおよび地図情報サーバから送信されるデータフローのすべてが，ローカルネットワーク内のセキュリティ機器により異常なデータフローか否かが分析される．分析の結果として異常なフローと判定された場合には，移動体を接続しているスライスゲートウェイで，その異常なデータフローを遮断する．

正常な移動体の場合は，移動する位置情報を取得管理することで，移動の方向性を把握，あるいは推測することが可能である．一方，異常フローを送信する移動体の場合は，位置を特定されないようにするため等，意図的に位置情報を提供しない可能性が考えられ，位置情報を取得することが困難と想定されるため，移動体から位置情報を取得せずに，ハンドオーバに追随した異常フローの遮断を目的とする．

本論文では，検出した異常フローに対して，発信源である移動体がハンドオーバしても追随して遮断する機能を主な対象とし，データフローの異常性判断は対象外とするが，閾値超え等により，異常なデータフローを検出する方法等が可能である．異常フローの検出については，関連研究の章で紹介した技術の利用が可能である．

3.2 異常フロー遮断における課題

図 1 に示したネットワークシステムにおいて，異常フローを遮断するためには，異常フロー検出後において，異常フローを送信する移動体がハンドオーバした場合においても追随した遮断の継続が必要である．ハンドオーバする移動体からの異常フロー遮断を実行するにあたり，第 1 の課題として，異常フローデータを受信するネットワークノード（スライスゲートウェイ）に対して，ハンドオーバに対して遅滞なく遮断の設定を実行する必要がある．また，第 2 の課題として，全国レベルでの移動に対応して遮断を可能とするためには，遮断管理においてスケーラビリティを有する必要がある．

3.3 スライスゲートウェイにおける遮断課題と対応方針

近年の無線ネットワークでは，携帯端末向けモバイルネットワーク，無線 LAN（Local Area Network），LPWA（Low Power Wide Area）等の多様なネットワークが存在し，また混在しており，異常フローの遮断を実行するためには，各移動体が各種の無線基地局を介して接続するスライスゲートウェイに対して適切な遮断設定が必要である．**表 1** に，対応策の比較表を示す．移動体からの異常フロー，特にマルウェア等に感染したアプリケーションからの異常フローを送信元 IP アドレス等を指定して遮断する方式として，移動体が接続するスライスゲートウェイの接続ポート単独に対して遮断設定を実行する「接続ポート遮断型」と，移動体が存在する領域（リージョン）内の基地局等を接続しているスライスゲートウェイの全ポートに対して遮断設定を実行する「リージョン遮断型」が想定される．

接続ポート遮断型では，移動体のハンドオーバに対応して遮断を継続するためには，正確に移動体の移動先を予測して，該当するスライスゲートウェイのポートに対して異常フローを指定して遮断の設定を実行する必要がある．一方，移動体の接続ポートを特定して遮断するため，遮断の設定先は 1 カ所となる．ただし，移動体の予測を失敗した場合，移動先ではないポートに対して遮断の設定を実施してしまい，結果として遮断を失敗する可能性があると推定される．

リージョン遮断型では，移動体が接続する基地局を含めたリージョン内スライスゲートウェイの全ポートに対して

表 1 異常フローに対する遮断方式比較
Table 1 Comparison of discarding methods for abnormal flow.

	Port type	Region type
Discard granularity	Network port	Region
Moving prediction	Use	No use
Discard request	1	1
Discard area	1	Number of areas
Miss-configuration potential	Large	Small
Overall judgment	-	Promising

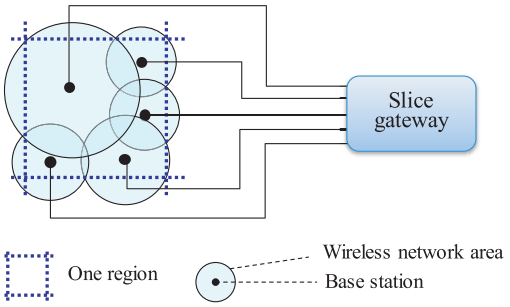

図 2 リージョンと無線ネットワークの関係
Fig. 2 Relation between a region and wireless network areas.

異常フローを指定して遮断設定を実行するため，移動体の正確な移動先予測を実行する必要がない．リージョンと複数無線ネットワークの関係を，**図 2** に示す．図に示されるように，リージョンの領域内に存在する基地局は，統合的に遮断の設定と解除が管理される．そのため，大小様々な接続エリアを有する基地局やアクセスポイントが存在，あるいは追加される場合においても，リージョンとして統一管理することで，遮断の設定と解除が可能である．この方式では，ハンドオーバが発生した場合において，異常フローを送信する移動体の移動方向を正確に予測しないため，移動先の候補となるリージョンに対して遮断の設定が要求されると，リージョン内の基地局を接続するすべてのポートに対して遮断の設定が実行される．そのため，広範囲にわたって遮断の設定が実行され，遮断失敗の可能性は微小となる．

接続ポート遮断型とリージョン遮断型とを比較した場合，異常フローを送信する移動体のハンドオーバに追随して遮断を継続する必要性を考慮すると，リージョン遮断型が有望と考えられる．

3.4 全国レベルでのハンドオーバ課題と対応方針

全国レベルでのハンドオーバに対応して，異常フローの遮断を継続実行するためには，広域移動および多数の移動体に対して遮断を管理する，スケーラブルな遮断管理機構が必要である．**表 2** に，対応策の比較表を示す．日本全土等の全国レベルの領域を移動対象として，異常フローを送信する移動体を単一の管理サーバ（スライス管理サーバ）で管理する「集中管理型」と，複数の管理サーバが連携して管理する「分散管理型」が想定される．

集中管理型では，たとえば倉庫内の異常な移動体管理といった小規模な場合には，単独のスライス管理サーバで移動体を管理するため，管理が容易になると推定される．一方，日本全土に存在するような多数の車両を管理するような多数移動体管理においては，単独のスライス管理サーバでは対応が困難であり，複数のスライス管理サーバが必要と想定される．この場合，1 台のスライスゲートに対して複数台のスライス管理サーバが接続される構成となる．異常フローを送信する移動体の識別子に応じて担当するスライス管理サーバを固定し，かつ異常フローを送信する移動体の接続を検知したスライスゲートウェイから，その移動体の遮断等を担当するスライス管理サーバへ接続情報（識別子）を通知するためには，識別子に基づいて担当するスライス管理サーバを選択する機能（レイヤ 7 ロードバランサ装置等）が各スライスゲートウェイに必要である．そのため，稼動装置増加にともなう管理負荷の増大化やコスト増が大幅に発生する．また，特定の領域から異常フロー遮断の機能を開始し，その領域を拡大する場合，領域内に存在する移動体数が増加するため，より高性能なスライス管理サーバを用いる，あるいは各スライス管理サーバが担当する移動体数を削減する等の設定の変更が必要となる．さらに，管理移動体数の拡張性については，移動体増加にともないロードバランスするスライス管理サーバが増加し，多数存在するレイヤ 7 ロードバランサに対して，設定の変更を行う必要がある．

表 2 異常フロー遮断の管理方式比較
Table 2 Comparison of management methods for configuration of abnormal flow discarding.

	Centralized management	Distributed management
Management of small-sized field	Easy	Complex
Management of many objects	Multiple management servers with multiple load balancers	Management based on small-sized field
Management scalability based on the size of discarding field	Server scale up or decreasing of the number of management object for each management server	Increasing of the number of management servers for a new field
Expandability of the number of management objects	Add a new management server and configure all slice gateways to connect it	Add a new management server and configure one slice gateway to connect it
Overall judgment	-	Promising

分散管理型では，移動体数や領域が小規模な場合において，複数のスライス管理サーバが連携する必要があり，異常フロー遮断の管理が，集中管理型に比較し複雑になる．一方，多数の車両を管理するような多数移動体管理においては，各スライス管理サーバが管理を担当する領域を細分化することにより対応が可能となる．また，異常フローを遮断する領域を拡大する場合，拡大した領域に新たなスライス管理サーバを追加することにより，容易に対応が可能である．さらに，管理移動体数の拡張性については，各スライス管理サーバが遮断を設定するスライスゲートウェイとの対応が固定的であり，スライス管理サーバが増加した場合に，関係する少数のスライスゲートウェイに対してのみ設定を変更することで対応が可能である．

異常フローの管理方式として，集中管理型と分散管理型とを比較した場合，管理する移動体や領域が小規模な場合は，集中管理型で対応が可能であるが，大規模な場合や規

模の拡大が発生するような場合は，少ない設定変更で対応が可能な分散管理型が有望と考えられる．

4. 異常フロー遮断システムの提案

4.1 異常フロー遮断システムの構成

本システムでは，異常フローを送信する移動体は，リージョン間移動に対しても送信元 IP ドレス，あるいは無線利用のための契約上の識別子等により識別が可能なことを前提としている．また，複数の無線基地局エリアから構成されるリージョン間を移動するような長距離移動に対して，電源を停止する等により，無線接続をせず移動する場合のような送信元 IP アドレスが変更される場合は，新たな異常フローとして検出することを前提としている．

提案する異常フロー遮断システムの構成を，**図 3** に示す．図においては，原理説明のために一次元方向におけるリージョン配置を想定したが，実際のシステムでは，二次元の格子状にリージョンが構成され，異常フローを送信する移動体のリージョン間移動に連動して，異常フロー遮断の設定が管理される．

提案システムでは，異常フローの遮断を管理する管理サーバ（ローカルスライス管理サーバ）が，リージョンごとに設置される．ここでリージョンは，モバイルネットワークの基地局やアクセスポイントを介して無線接続が可能なエリアを複数含む領域として構成される．提案するシステムでは，動的に追加される基地局等に影響を受けないようにするため，特定の区画（緯度，経度等により規定）によりリージョンを指定する．そのため，追加された基地局等の存在位置により，所属するリージョンが自動的に決定される．異常フローを遮断するスライスゲートウェイは，ローカルスライス管理サーバ同様に，各リージョンに設置され，リージョン内に存在する基地局等を複数接続収容する．また，異常フローを検出するセキュリティアナライザも，各リージョンに設置される．

提案システムでは，リージョン 1 に属する移動体からのデータフローがセキュリティアナライザ 1 に転送され，異常フローが送信されているか否かが判定される．異常フローの検出は，一例として帯域に関する閾値により判定される．セキュリティアナライザ 1 で異常フローが検出されると，その情報がスライスゲートウェイ 1 を経由してローカルスライス管理サーバ 1 へ伝達される．ローカルスライス管理サーバ 1 は，異常フローの情報を受信すると，自身が管理するリージョン 1 内に存在するスライスゲートウェイ 1 に対して，異常フローを遮断する設定を実行するよう要求，および隣接するリージョン 2 を管理するスライス管理サーバ 2 に対して異常フローを遮断する設定を要求する．異常フローの遮断設定要求を受信したスライスゲートウェイ 1 は，基地局等を接続しているすべてのポートに対して，指定された異常フローの遮断設定を実行する．また，異常フローの遮断設定要求を受信したスライス管理サーバ 2 は，自身が管理するリージョン 2 内のスライスゲートウェイ 2 に対して異常フローを遮断する設定を要求する．異常フローの遮断設定要求を受信したスライスゲートウェイ 2 は，自リージョンにおいて基地局等を接続しているすべてのポートに対して，指定された異常フローの遮断設定を実行する．

異常フローを送信する移動体がハンドオーバにより隣接リージョン 2 へ移動した場合は，移動先のリージョン 2 に存在するスライスゲートウェイ 2 により，リージョン 2 への接続が検知される．また，検知した移動体の情報は，ローカルスライス管理サーバ 2 へ通知される．ローカルスライス管理サーバ 2 は，さらに隣接するリージョン 3 を管理するスライス管理サーバ 3 に対して，異常フローを遮断する設定を要求する．異常フローの遮断設定要求を受信したスライス管理サーバ 3 は，自身が管理するリージョン 3 内のスライスゲートウェイ 3 に対して異常フローを遮断する設定を要求する．異常フローの遮断設定要求を受信したスライスゲートウェイ 3 は，自リージョンにおいて基地局等を接続しているすべてのポートに対して，指定された異常フローの遮断設定を実行する．

異常フローを送信する移動体がハンドオーバにより隣接リージョン 3 へ移動した場合は，移動先のリージョン 3 に存在するスライスゲートウェイ 3 により，リージョン 3 への接続が検知される．また，検知した移動体の情報は，ローカルスライス管理サーバ 3 へ通知される．ローカルスライス管理サーバ 3 は，さらに隣接するリージョンが存在しないため，異常フローの遮断を要求する通知は実行しない．一方，異常フローを送信する移動体がリージョン 3 に接続となったため，リージョン 2 は隣接リージョンとなるが，リージョン 1 は隣接リージョンとならないため，リージョン 1 を管理するローカルスライス管理サーバ 1 に対して，ローカルスライス管理サーバ 3 は，異常フロー遮断の設定を解除するよう要求する．ローカルスライス管理サーバ 1 は，スライスゲートウェイ 1 に対して，異常フロー遮断の設定を解除するよう要求する．スライスゲートウェイ

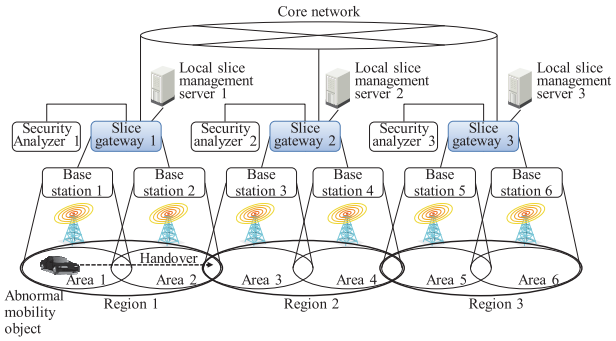

図 3 異常フロー廃棄システム
Fig. 3 Proposed system to discard abnormal flow.

1は，自リージョンにおいて基地局等を接続しているすべてのポートに対して，異常フロー遮断の設定を解除する．このように，異常フローを送信する移動体が接続するリージョンに隣接しないリージョンにおいては，遮断の設定を解除することにより，遮断リストの膨張抑制が可能となる．

4.2 異常フロー遮断の複数ローカルスライス管理サーバによる分散管理

ローカルスライス管理サーバが，他のローカルスライス管理サーバと連携して，異常フロー遮断を実行するためのフローチャートを，**図 4** に示す．ローカルスライス管理サーバは，異常フローの遮断管理を開始すると，リージョン構成や他のローカルスライス管理サーバのアドレス等の初期情報を，人としてのシステム全体の管理者から受け付けて登録する．初期設定が完了すると，3つの処理を並列で実行する．

第1の処理（左側の処理フロー）として，ローカルスライス管理サーバは，セキュリティアナライザより異常フローの検知情報を受信したかを監視する．異常フローの検知情報を受信した場合，リージョン内において異常フローの遮断設定を実行するスライスゲートウェイに対して，異常フロー遮断の実行を要求する．また，隣接するリージョンを管理するローカルスライス管理サーバすべて（図3の場合は，隣接1台）に対して，異常フロー遮断の設定を要求する．

第2の処理（中央の処理フロー）として，ローカルスライス管理サーバは，異常フローを送信する移動体の接続情報（送信元IPアドレスおよび受信ポートに基づくリージョン識別番号）をスライスゲートウェイから受信したかを監視する．異常フローを送信する移動体の接続情報を受信した場合，その接続情報をローカルスライス管理サーバ内のメモリに登録する．その後，異常フローを送信する移動体が，他のリージョンから移動してきたかを判定する．移動してきた場合は，新たに遮断を実行すべきリージョンと，遮断を解除すべきリージョンを特定し，該当するリージョンを管理するローカルスライス管理サーバに対して，異常フローの遮断，あるいは解除を要求する．

第3の処理（右側の処理フロー）として，他のローカルスライス管理サーバより異常フロー遮断の設定，あるいは解除の要求を受信したか否かを監視する．異常フロー遮断の設定，あるいは解除要求を受信した場合は，異常フローの遮断，あるいは解除設定を実行するスライスゲートウェイを選択して，異常フロー遮断の実行，あるいは解除を要求する．

上記の遮断設定管理では，異常フローを送信する移動体が検出されている場合の処理になる．一方，移動体において通信用の電源が停止となった場合や電波が届かない地点へ移動した場合は，別の処理が必要になる．たとえば，無線接続のために払い出された送信元IPアドレスの有効期間をタイマ等で管理し，その払い出された送信元IPアドレスが無効となった場合に，該当する送信元IPアドレスに対する遮断を解除する等の処理が必要となる．本処理については，将来的な拡張機能と想定している．

4.3 スライスゲートウェイにおける異常フロー遮断管理

スライスゲートウェイが，ローカルスライス管理サーバと連携して，異常フロー遮断を管理するためのフローチャートを，**図 5** に示す．スライスゲートウェイは，異常フローの遮断制御を開始すると，セキュリティアナライザ

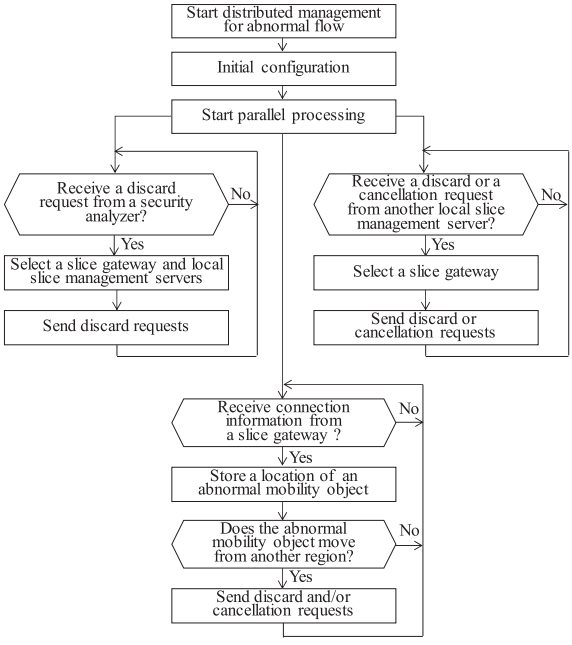

図 4 異常フローの分散管理
Fig. 4 Distributed management for abnormal flow.

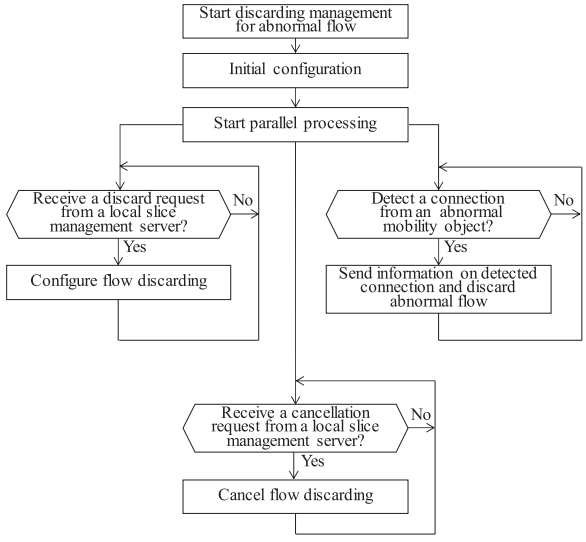

図 5 スライスゲートウェイにおける異常フロー遮断管理
Fig. 5 Abnormal flow management on a slice gateway.

へのデータ転送や，ローカルスライス管理サーバのアドレス等の初期情報を，管理者から受け付けて登録する．初期設定が完了すると，3 つの処理を並列で実行する．

第 1 の処理（左側の処理フロー）として，ローカルスライス管理サーバより，異常フローの遮断要求を受信したかを監視する．異常フローの遮断要求を受信した場合，各スライスゲートウェイが担当するリージョン内に存在するエリア（基地局等）を接続するポートに対して，該当する異常フローの遮断を設定する．本処理において，複数の基地局エリアを有する領域をリージョンとして設定し，異常フローを送信する移動体が存在するリージョンに対して，隣接するリージョンに先回りして異常フローの遮断設定を実行する．これにより，異常フローを送信する移動体は，短時間において基地局エリア間を移動可能であるが，リージョン間移動は不可となり，かつ隣接リージョンに異常フロー遮断が設定されているため，該当移動体のリージョン間移動に対して，遅滞のない異常フロー遮断が可能となる．

第 2 の処理（中央の処理フロー）として，ローカルスライス管理サーバより，異常フローの遮断解除要求を受信したかを監視する．異常フローの遮断解除要求を受信した場合，各スライスゲートウェイが担当するリージョン内に存在するエリア（基地局等）を接続するポートに対して，該当する異常フローの遮断解除を設定する．

第 3 の処理（右側の処理フロー）として，異常フローを送信する移動体の接続を監視する．具体的には，スライスゲートウェイを経由するデータフローに対して，遮断を設定している異常フローに該当するかを監視する．異常フローとして登録されたデータフローを検出すると，異常フローを送信する移動体の接続情報（送信元 IP アドレスおよび受信ポートに基づくリージョン識別番号）を，ローカルスライス管理サーバへ通知する．また，通知後に，該当する異常フローの遮断を実行する．

4.4 移動履歴に基づく異常フロー遮断管理

移動体のリージョン間移動に基づいた，異常フローの遮断管理方式を，**図 6** に示す．図中の左側（Before moving）における格子は，一例としての 5 × 5 のリージョン構成を示している．ここで，異常フローを送信する移動体が，格子状の中央のリージョン（緑色）で検出された場合を起点として，リージョン間移動履歴に基づいた異常フローの遮断制御を示す．中央のリージョンに隣接するリージョン（灰色：1 次隣接リージョン）では，移動体が移動する可能性があるため，異常フローの遮断が設定される．一方，中央のリージョンに隣接しないリージョン（白色：2 次隣接リージョン）では，異常フローの遮断は設定されない．ここでリージョンは，複数の無線エリアを包含する規模の領域に設定される．そのため，異常フローを送信する移動体は，瞬時にはリージョン間を移動することが不可となる想定をしている．

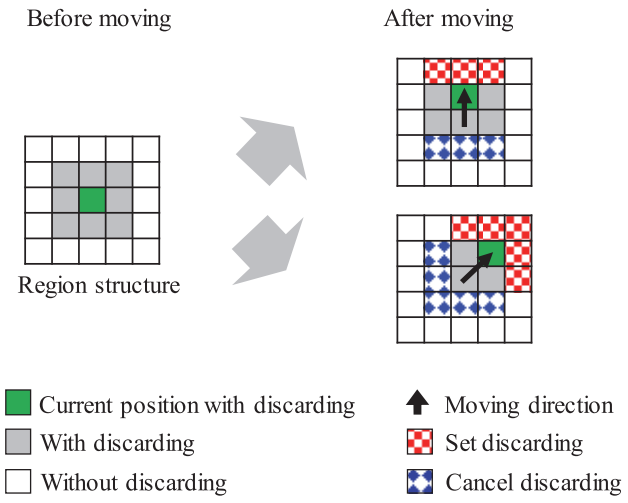

図 6 移動履歴に基づいた異常フロー遮断管理
Fig. 6 Discard management based on moving history.

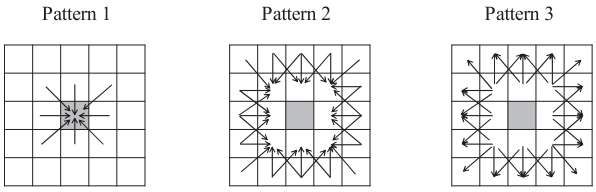

図 7 ローカルスライス管理サーバ間連携による異常フロー遮断管理
Fig. 7 Discard management between local slice management servers.

リージョンの構成を格子状としたことにより，図中の右側（After moving）に示したように，異常フローを送信する移動体は，縦横方向への移動と斜め方向への移動に大別される．縦横方向に移動する場合は，図の右上に示されように，リージョン間移動後に，新たに隣接する 3 つのリージョン（赤色■：1 次隣接リージョン）に対して遮断の設定が実行される．また，リージョン間移動により隣接しなくなった 3 つのリージョン（青色◆：2 次隣接リージョン）に対しては，遮断の解除が実行される．一方，斜め方向に移動する場合は，図の右下に示されように，リージョン間移動後に，新たに隣接する 5 つのリージョン（赤色■：1 次隣接リージョン）に対して遮断の設定が実行され，また，隣接しなくなった 5 つのリージョン（青色◆：2 次隣接リージョン）に対して遮断の解除が実行される．

4.5 ローカルスライス管理サーバ間連携による異常フロー遮断管理

移動体のリージョン間移動に基づいた，ローカルスライス管理サーバ間における遮断管理機構を，**図 7** に示す．遮断の設定および解除が発生するパターンとして，3 種類が想定される．

第 1 のパターンは，異常フローを送信する移動体が，隣接リージョン（1 次隣接リージョン）からローカルスライ

ス管理サーバ自身が管理するリージョン（灰色のリージョン）へ移動した場合の遮断設定と，解除設定である．移動体のリージョン間移動にともない，新たに隣接となる 1 次隣接リージョンを管理するローカルスライス管理サーバに対して，異常フローの遮断設定を要求する．また，隣接しなくなったリージョン（2 次隣接リージョン）を管理するローカルスライス管理サーバに対して，異常フローの遮断解除を要求する．

第 2 のパターンは，異常フローを送信する移動体が，間にリージョンを挟んで隣接するリージョン（2 次隣接リージョン）から，1 次隣接リージョンに移動した場合である．この場合，1 次隣接リージョンを管理するローカルスライス管理サーバより，遮断設定の要求を受信し，自身が管理するリージョンに対して，遮断の設定を実行する．

第 3 のパターンは，異常フローを送信する移動体が，1 次隣接リージョンから 2 次隣接リージョンに移動する場合である．この場合，2 次隣接リージョンを管理するローカルスライス管理サーバより，遮断設定の解除要求を受信し，自身が管理するリージョンに対して，遮断の解除を実行する．

5. 提案システムの評価と結果

5.1 評価概要

本評価では，日本国内に存在する車両総数を想定して，発生した異常フローの遮断性能を評価する．具体的には，対象とする車両総数規模として 8,000 万台 [11]，および制御対象としての面積を 378,000 km^2 [12] とした場合について評価する．前記想定では，平均の車両密度は約 212 台/km^2 となるため，評価では，相当する 250 台/km^2 を用いて実施する方針とした．

図 8 に，評価システムのイメージを示す．異常フローの遮断を管理する提案システムは，分散管理型であり，異常フローを発生する車両が存在するリージョンに隣接するリージョン（1 次隣接リージョン）に対して遮断の設定を行い，隣接しなくなったリージョン（2 次隣接リージョン）に対しては，遮断の解除を行う．そのため，着目しているリージョンを基軸として，2 次隣接リージョンまでの車両移動に対して遮断と解除を模擬可能な，縦方向 5 リージョン，横方向 5 リージョンとなる，計 25 リージョンの構成に対して評価を行う．本構成において，密度 250 台/km^2 の車両における異常フローの遮断と解除が可能であれば，結果として国内全土における異常フローの管理が可能と想定される．このとき，たとえば，リージョンの 1 辺が 10 km の場合，面積は 100 km^2 となり，リージョン内に 25,000 台の車両が存在することになる．そして，25,000 台の車両が存在する領域に対してリージョンを構成する場合，日本全国でローカルスライス管理サーバが，3,200 台存在する構成となる．

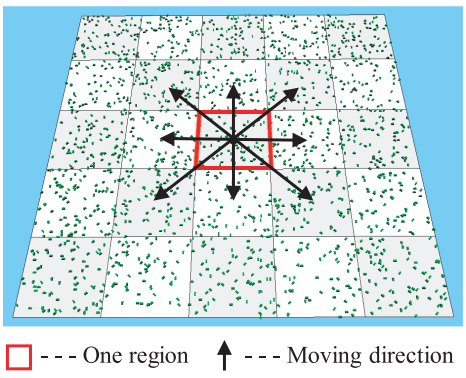

図 8 評価システムイメージ
Fig. 8 Evaluation system image.

上記の車両密度設定では平均密度への対応であり，都市部における車両集中を考慮した場合は，その対応が必要である．たとえば，1,000 台/km^2 を想定した場合，250 台/km^2 に対して，車両数が 4 倍となる．この場合，リージョンのサイズ（面積）を，1/4 にするような区分けを実行する．たとえば，リージョンの 1 辺を 1/2 にする区分けになる．そのため，25,000 台の車両が存在するような面積に対して，リージョンを構成するような区分けが実行される．本区分けでは，結果として同様に日本全国において，3,200 台のローカルスライス管理サーバが存在することになる．

また，車両の密度と移動速度には密接な関係がある．たとえば，都市部における車両集中の状態では，密度が増加しているため，移動速度が減少することになる．このような密度と移動速度の変化を考慮して，車両の密度と速度の積に対する性能評価を評価項目として含める．具体的には，リージョンの 1 辺の長さを 10 km とし，車両密度と移動速度の積を，4,000～20,000 と変更して評価する方針とした．車両密度と移動速度の積が 20,000 の場合，たとえば車両の速度が 10 km/h であれば，密度が 2,000 台/km^2 に相当し，車両の速度が 100 km/h であれば，密度が 200 台/km^2 に相当する．

一方，車両の稼働率に関しては，ある地域および時間帯において 100%稼働している場合や，10%しか稼働していないような状況が想定される．ここで，システムとして安定稼働させる場合，より負荷の高い状態への対応が必要と考えられ，100%稼働に対して評価を実施する方針とした．

評価システムでは，**表 3** に示した物理サーバ上に，ロー

表 3 サーバ仕様
Table 3 Specifications of a server.

#	Item	Specification
1	CPU	2.6GHz, 28cores
2	Memory	48GByte
3	Storage	1TByte

カルスライス管理サーバ，スライスゲートウェイ，および車両としての移動機能をすべて実装し，仮想空間上においてリアルタイムに稼働を行い評価を実施した．具体的には，リージョン内に対象とする車両をランダムに配備し，縦横方向と斜め方向に移動する車両数を均等に配備した．また，評価時のパラメータとして設定した移動速度に応じて縦横，および斜め方向の移動を行い，25 リージョンの端点に到達した場合は，反対側のリージョンの端点から再び移動する処理を行い，車両の移動を模擬した．

5.2 評価項目

具体的な評価では，以下に示す 5 種類の評価設定において，異常フローを送信する車両のリージョン間移動にともない発生する遮断と解除の通信回数により評価を行う．

- **評価 1：車両移動に追随した遮断と解除の設定評価**
  提案システムにおいて，異常フローを送信する移動体の存在するリージョンおよび隣接リージョンに対して，遮断の設定が実行されているかを評価する．
- **評価 2：提案方式と集中管理方式との性能比較評価**
  提案システム（分散管理方式）の性能を評価するため，集中管理方式において発生する通信回数との比較を行う．
- **評価 3：異常フロー発生量に対する分散管理の性能評価**
  異常フローの発生量として，1 台のローカルスライス管理サーバが管理するリージョンのサイズ，および異常フローを発生する車両の比率を変更して発生する通信回数を評価する．
- **評価 4：車両の密度と速度の積を一定にした場合の分散管理の処理数評価**
  車両の速度が増加すると必要な車間距離が増加するため，密度が減少する．そこで，密度と速度の積が一定となる複数の状態に対して，リージョンのサイズを変更して発生する通信回数を評価する．
- **評価 5：車両の密度と速度の積に対する分散管理の性能評価**
  車両密度と速度の積値，および異常フローの発生率を変更して，発生する通信回数を評価する．

5.3 提案システム評価

5.3.1 車両移動に追随した遮断と解除の設定評価

異常フローを送信する車両のリージョン間移動に追随した異常フロー遮断と解除の評価結果を，**図 9** に示す．図中において，着目している車両は黒色点で表示されている．左図では，中央のリージョンにおいて異常フローを送信する車両が存在する状況を示している．着目している車両が存在するリージョンおよび 1 次隣接リージョン（紫色表示）においては，異常フロー遮断が設定されている．一方，2 次隣接するリージョンに対しては，着色されておらず，遮断の設定がされていない状況を示している．

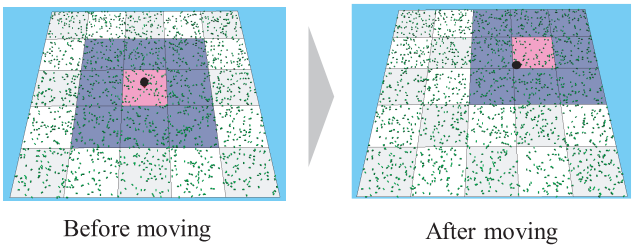

図 9 車両移動に追随した遮断設定
Fig. 9 Abnormal flow discarding according to mobility.

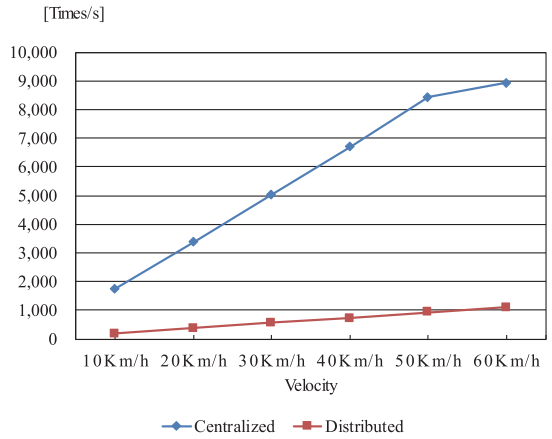

図 10 集中管理型と分散管理型のスライス管理サーバ処理数比較
Fig. 10 Slice management server processing load comparison between centralized and distributed management.

一方，右図では，異常フローを送信する車両が，中央のリージョン（Before moving）から右上のリージョンへ移動（After moving）した状況を示している．異常フローを送信する車両が移動したことにより，遮断設定をしている 1 次隣接リージョンもあわせて移動していることが検証された．また，1 次隣接しなくなったリージョンにおいては，紫色表示されなくなり，遮断設定が解除されていることを検証した．なお，異常フローを送信する他の車両に対しても，遮断の実行が同時に実行されていることを検証している．これにより，異常フローを送信する車両がリージョン間移動した場合に，その移動に追随して遮断の設定と解除が実行されていることが検証された．

5.3.2 提案方式と集中管理方式との性能比較評価

スライス管理サーバ 1 台あたりにおける，提案方式（分散管理方式）と集中管理方式との性能の比較結果を**図 10** に示す．図中の横軸は，車両の移動速度であり，縦軸はスライス管理サーバが必要とする 1 秒間あたりの通信の処理回数を表している．本評価では，車両密度 250 台/km^2，異常フローを送信する車両の比率 100%，リージョンの 1 辺を 10 km，リージョン数 25 の設定の下，移動速度を変化させて，すべての車両を対象として評価を実施した．そのため，提案方式では，25,000 台を対象として制御を行い，集中管理方式では，625,000 台を対象として制御が必要である．

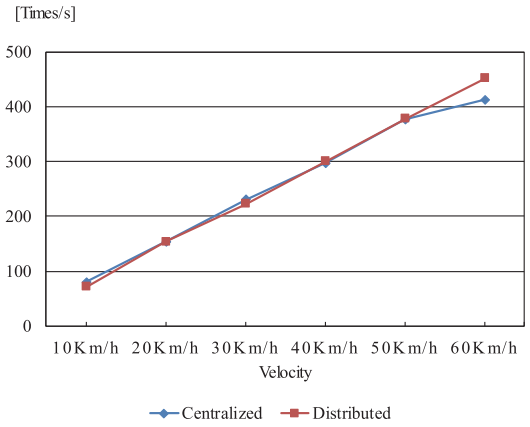

図 11 集中管理型と分散管理型のスライスゲートウェイ処理数比較
Fig. 11 Slice gateway processing load comparison between centralized and distributed management.

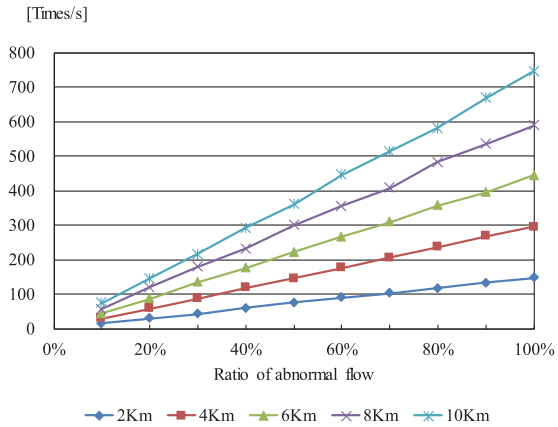

図 12 異常フロー発生率に対するローカルスライス管理サーバの処理数
Fig. 12 Processing load of a local slice management server for ratio of abnormal flow.

評価結果として，車両の移動速度が 50 km/h である場合，集中管理方式では，1 秒間あたり 8,428 回の通信が複数のスライスゲートウェイ間に必要である．一方，提案方式では，1 秒間あたり 930 回の通信が他のローカルスライス管理サーバやスライスゲートウェイ間に必要である．車両の移動速度が 60 km/h の場合，集中管理方式では処理が飽和している．一方，提案方式では，1,104 回の通信が 1 秒間あたり必要であるが，遮断の設定制御が完了している．この結果より，60 万台規模の車両を対象とした場合，集中管理方式に比較し，提案方式は約 1/9 の処理量で対応が可能である．

本評価システムの構成では，管理する車両の台数が 62.5 万台および移動速度が 50 km/h 以内の場合，集中管理方式でも対応が可能である．集中管理方式では，管理サーバが 1 台のため，提案方式に比較してコスト面や運用管理の点で有利である．一方，管理する車両の台数が 62.5 万台および移動速度が 60 km/h の状況では，集中管理方式では処理が飽和しはじめており，分散管理方式が有望である．

スライスゲートウェイにおける提案方式（分散管理方式）と集中管理方式との性能の比較結果を**図 11** に示す．図中の横軸は，車両の移動速度であり，縦軸はスライスゲートウェイが必要とする 1 秒間あたりの通信の処理回数を表している．スライスゲートウェイは，1 リージョンあたり 1 台配備しており，集中管理方式と分散管理方式の何れにおいても，リージョン内の 25,000 台の車両に対して制御が必要である．

集中管理方式と分散管理方式の結果が同様の結果となっており，おおむね重なって表示されている．結果として，集中管理方式と分散管理方式のいずれの場合においても，スライスゲートウェイは，車両の移動速度が，50 km/h である場合，1 秒間あたり 377 回の通信がスライス管理サーバとの間に必要である．一方，車両の移動速度が 60 km/h の場合，集中管理方式において処理が飽和している．

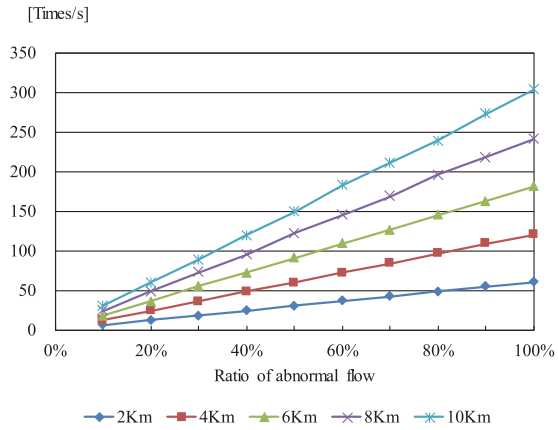

図 13 異常フロー発生率に対するスライスゲートウェイの処理回数
Fig. 13 Processing load of a slice gateway for ratio of abnoraml flow.

評価結果より，スライスゲートウェイにおける必要な通信回数に関しては，集中管理方式と分散管理方式において大きな差がない．しかし，車両の移動速度が 50 km/h を超える状況では，集中管理方式において処理が飽和している．

以上の評価結果より，スライスゲートウェイにおける処理に差はないが，スライス管理サーバにおける必要な通信回数に関しては，分散管理方式は，集中管理方式に比較して処理負荷が約 1/9 であり，有効性が高い．

5.3.3 異常フロー発生量に対する分散管理の性能評価

異常フローを送信する車両の比率およびリージョンサイズに対する，異常フロー遮断のためのローカルスライス管理サーバおよびスライスゲートウェイの処理負荷における評価結果を，**図 12** および**図 13** に示す．本評価では，密度 250 台/km^2，車両の移動速度 40 km/h，リージョン数 25 の設定を用いている．図中の横軸は異常フローを送信する車両の比率を表し，縦軸は 1 秒間あたりの必要な通信回数を示している．また，本評価では，リージョンの 1 辺の長さを 2 km～10 km と変更して評価している．

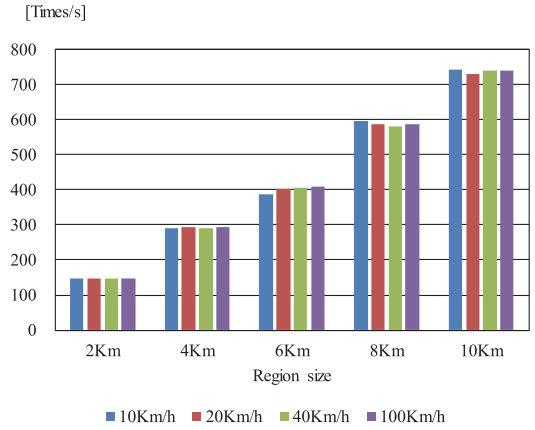

図 14 車両速度とリージョンサイズに対するローカルスライス管理サーバの処理数

Fig. 14 Processing load of a local slice management server for velocity and the size of region.

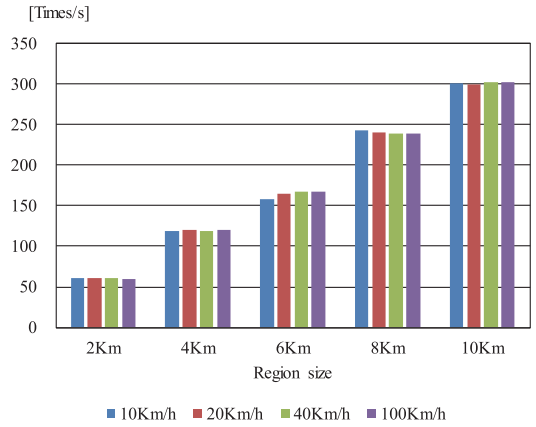

図 15 車両速度とリージョンサイズに対するスライスゲートウェイの処理回数

Fig. 15 Processing load of a slice gateway for velocity and the size of region.

図 12 の評価結果より，ローカルスライス管理サーバの通信負荷は，異常フローを送信する車両数比率の変化，およびリージョンの 1 辺の長さの変化に対して，おおむね線形に上昇することが検証された．特に，リージョンの 1 辺が 10 km の場合，1 秒間あたり 747 回の通信が必要であった．

図 13 の評価結果より，スライスゲートウェイの通信負荷は，異常フローを送信する車両数比率の変化，およびリージョンの 1 辺の長さの変化に対して，おおむね線形に上昇することが検証された．また，リージョンの 1 辺が 10 km の場合，1 秒間あたり 304 回の通信が必要であった．

5.3.4 車両の密度と速度の積を一定にした場合の分散管理の処理数評価

本評価では，車両の密度と速度の積を一定にした場合において，異常フローの遮断制御に必要な 1 秒間あたりの通信回数を，車両の速度を 10 km/h～100 km/h と変更して評価した．具体的には，車両の密度と速度の積として，10,000 を設定している．そのため，車両の速度が 10 km/h の場合は，車両の密度が 1,000 台/km^2 となっている．また，車両の速度が 100 km/h の場合は，車両の密度が 100 台/km^2 となっている．たとえば，速度が 100 km/h の場合に，車間距離として約 100 m を考えた場合，進行方向に対して 1 km あたりに約 10 台となる．また，進行方向と直角な方向に対しては，100 m 置きに 1 台存在するとした場合，1 km あたりに 10 台となり，100 台/km^2 の状況に相当する．また，本評価では，リージョンの 1 辺の長さを 2 km～10 km と変更して評価している．ローカルスライス管理サーバとスライスゲートウェイにおける評価結果を，**図 14** および**図 15** に示す．

図 14 の評価結果より，ローカルスライス管理サーバの通信負荷は，車両の速度が増加しても，それに対して密度が減少するため，リージョンサイズが変化しない場合，結果として異常フロー遮断に必要な通信回数が変化しないことが検証された．一方，リージョンサイズが増加する場合には，そのリージョン内に存在する車両数が増加するため，必要な通信回数は増加するが，リージョンサイズが異なる場合においても，車両の速度に依存せず必要な通信回数が一定であることが検証された．

図 15 の評価結果より，スライスゲートウェイの通信負荷は，車両の速度が増加しても，それに対して密度が減少するため，リージョンサイズが変化しない場合，結果として異常フロー遮断に必要な通信回数が変化しないことが検証された．一方，リージョンサイズが増加する場合には，必要な通信回数は増加するが，リージョンサイズが異なる場合においても，車両の速度に依存せず必要な通信回数が一定であることが検証された．

5.3.5 車両の密度と速度の積に対する分散管理の性能評価

本評価では，車両密度と速度の積の値を変更して，異常フロー遮断制御に必要な 1 秒間あたりの通信回数を評価した．具体的には，リージョンの 1 辺の長さを 10 km とし，車両密度と速度の積を，4,000～20,000 と変更して評価した．また，異常フローを送信する車両の比率を 10%～100%と変更して評価した．車両密度と速度の積が 20,000 の場合，たとえば車両の速度が 10 km/h であれば，密度が 2,000 台/km^2 に相当し，車両の速度が 100 km/h であれば，密度が 200 台/km^2 に相当する．ローカルスライス管理サーバとスライスゲートウェイにおける評価結果を，**図 16** および**図 17** に示す．

図 16 の評価結果より，ローカルスライス管理サーバの通信負荷は，車両密度と速度の積，および異常フロー送信車両の比率に比例して増加することが検証された．特に，ローカルスライス管理サーバは，車両密度と速度の積が 20,000 であり，かつ異常フロー送信車両の比率が 100%の場合，1 秒間あたり 1,468 回の通信が他のローカルスライス管理サーバおよびスライスゲートウェイと必要であった．

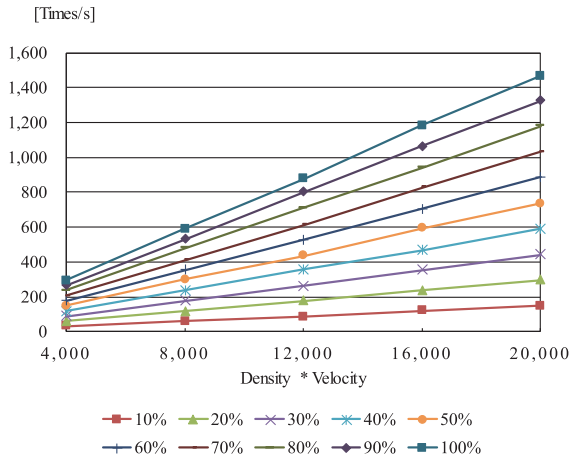

図 16 車両密度と速度の積値に対するローカルスライス管理サーバの処理数

Fig. 16 Processing load of a local slice management server for product of object density and the velocity.

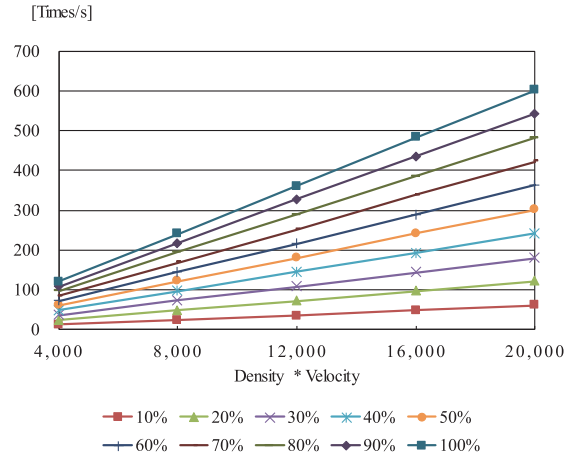

図 17 車両密度と速度の積値に対するスライスゲートウェイの処理数

Fig. 17 Processing load of a slice gateway for product of object density and the velocity.

図 17 の評価結果より，スライスゲートウェイの通信負荷は，車両密度と速度の積，および異常フロー送信車両の比率に比例して増加することが検証された．特に，スライスゲートウェイは，車両密度と速度の積が 20,000，かつ異常フロー送信車両の比率が 100%の場合，1 秒間あたり 603 回の通信がローカルスライス管理サーバと必要であった．

以上の評価結果より，シミュレーション上においては，車両密度と速度の積が 20,000 の場合にも対応が可能なことを検証した．具体的には，車両の速度が 10 km/h で密度が 2,000 台/km^2，また車両の速度が 100 km/h で密度が 200 台/km^2 の状態に対して，対応が可能なことを検証した．

5.4 考察

図 10 の評価結果より，リージョンの 1 辺が 10 km，車両密度が 250 台/km^2，および 25 リージョン構成の場合において，異常フロー遮断制御における提案方式（分散管理方式）は，集中管理方式に比較し，約 9 倍遮断が可能なことが検証された．提案方式では，1 次および 2 次隣接するリージョンのローカルスライス管理サーバとの間においてのみ，異常フロー遮断制御の設定，および解除のための通信が必要である．そして，3 次隣接以上のローカルスライス管理サーバとの間には，遮断制御のための通信が不要である．そのため，25 のリージョン構成ではなく，管理すべき車両台数やリージョン数に合わせてローカルスライス管理サーバを増加することにより，より広域への対応が可能である．結果として，国内に存在する 8,000 万台規模の車両，および 378,000 km^2 への対応が可能である．

一方，集中管理方式では，リージョン構成に関係なく，存在する車両すべてに対して管理する必要がある．車両として 625,000 台が存在し，すべての車両が異常フローを送信した場合に他のサービスに影響を及ぼさないためには，1 秒間あたり 8,428 回の通信が必要である．そのため，国内に存在する 8,000 万台規模の車両に対応することは，困難と想定される．ただし，管理すべき車両を固定し，ロードバランサと組み合わせてシステムとして構成することが考えられる．しかし，その場合には，管理する車両が増加するたびに，全国に配備されたすべてのロードバランサへの設定変更が必要であり，管理負荷が非常に高いと考えられる．

分散管理型の提案方式では，新たに管理が必要な領域が増加した場合に，その領域に対してリージョンを構成してローカルスライス管理サーバを配置し，2 次隣接するリージョンを管理するローカルスライス管理サーバに対して，リージョン構成の変更を設定することで対応が可能となる．そのため，ロードバランサを用いた方式に比較しても，分散管理型の提案方式は有望である．

通信ネットワーク上において異常なフローを遮断することは，通信帯域の有効利用につながるため，絶え間なく監視して制御することが重要と考えられる．提案した分散型の管理方式では，ローカルスライス管理サーバは独立に稼働するため，不具合が発生したリージョン以外では異常フローの遮断管理が継続されるため，可用性の観点で高められる可能性があると思われる．

6. おわりに

本論文では，異常フローを送信する移動体が基地局間を移動した際にも，リージョン間移動履歴に基づき，移動先の基地局に対して先回りして遮断の設定を可能とする，分散管理型の異常フロー管理方式を提案した．提案方式では，複数の基地局が配備される領域をリージョンとして管理し，リージョン単位に遮断を制御することにより，移動体が接続する各基地局エリアに対して隣接する基地局エリアすべてに遮断が設定される．そのため，異常フローを送

信する移動体が，どのような方向に移動しても，移動先の基地局エリアに対して遮断の設定が先回りして実行される．これにより，異常フローを送信する移動体が基地局間を移動するようなモバイルネットワークに対して，遅滞のない異常フロー遮断が可能である．

提案した分散管理方式に対して，性能の評価を実施した．その結果，1台のローカルスライス管理サーバの管理範囲であるリージョンに対して，1辺が10 kmであり，車両の密度と速度の積が20,000の場合において，1秒間あたり1,468回の通信で，異常フロー遮断がすべての車両に対して可能となることを検証した．具体的には，車両の速度が10 km/hの場合には，密度が2,000台/km^{2}に相当し，あるいは，車両の速度が100 km/hの場合には，密度が200台/km^{2}に相当する状況に対して，速度と密度の関係が変動する場合にも対応が可能なことをシミュレーションで検証した．

今後は，ローカルスライス管理サーバとスライスゲートウェイ間の接続を，実際の通信ネットワークを用いて構成し，より実際のシステムに近い構成において評価を行う予定である．また，電源停止等により異常フローを送信する移動体が存在しなくなった場合，遮断設定を自動解除する機能，および複数の基地局にリージョンをまたいでつながる場合への対応機能を追加し，実用性を高める予定である．さらに，一部の装置に不具合が発生した場合等の高信頼化対応についてもエンハンスする予定である．

謝辞 本研究の一部は，総務省の委託研究「自律型モビリティシステム（自動走行技術，自動制御技術等）の開発・実証 I自律型モビリティシステムの高信頼化に係る技術の確立」および「膨大な数の自律型モビリティシステムを支える多様な状況に応じた周波数有効利用技術の研究開発技術（課題ウ）大量の異常通信の検知・抑制による高信頼化技術」の一環として実施された．

参考文献

[1] Cisco Systems, Inc.：Cisco ASR 9000 vDDoS 攻撃対策ソリューション，入手先 ⟨https://www.cisco.com/c/ja_jp/products/collateral/routers/asr-9000-series-aggregation-services-routers/solution-overview-c22-736143.html⟩（参照 2019-03-01）．

[2] Akamai Technologies：Akamai によるサービス妨害攻撃の阻止，入手先 ⟨https://www.akamai.com/jp/ja/resources/denial-of-service-attacks-dos.jsp⟩（参照 2019-03-01）．

[3] 富士通株式会社：FENICS インターネットサービス 帯域確保型専用線 IP 接続サービス DDoS 対策サービス，入手先 ⟨http://www.fujitsu.com/jp/services/infrastructure/network/internet/internet-ip/service/⟩（参照 2019-03-01）．

[4] Zhang, C.: DOS Attack Analysis and Study of New Measures to Prevent, *2011 International Conference on Intelligence Science and Information Engineering*, pp.426–429 (2011).

[5] Deepika, M. and Monika, S.: DDoS Attack Prevention and Mitigation Techniques - A Review, *International Journal of Computer Applications* (*0975–8887*), Vol.67, No.19, pp.21–24 (2013).

[6] Minsu, J. et al.: Adaptive transient fault model for sensor attack detection, *2016 IEEE 4th International Conference on Cyber-Physical Systems, Networks, and Applications* (*CPSNA*), pp.59–65 (2016).

[7] Yanpeng, G. and Xiaohua, G.: Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks, *IEEE Trans. Signal and Information Processing over Networks*, Vol.4, No.1, pp.48–59 (2018).

[8] Kang, Y. et al.: Enhanced Resilient Sensor Attack Detection Using Fusion Interval and Measurement History, *2018 International Conference on Hardware/Software Codesign and System Synthesis* (*CODES+ISSS*) (2018).

[9] Anna, L.B. and Erhan, G.: A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, *IEEE Communications Surveys & Tutorials*, Vol.18, No.2, pp.1153–1176 Secondquarter (2016).

[10] Maximilian, F., Maria, L. and Timea, P.: Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education, *2017 IEEE 15th Intl. Conf. Dependable, Autonomic and Secure Computing, 15th Intl. Conf. Pervasive Intelligence and Computing, 3rd Intl. Conf. Big Data Intelligence and Computing and Cyber Science and Technology Congress* (*DASC/PiCom/DataCom/CyberSciTech*), pp.38–46 (2017).

[11] 一般財団法人自動車検査登録情報協会：わが国の自動車保有動向，入手先 ⟨https://www.airia.or.jp/publish/statistics/trend.html⟩（参照 2019-03-01）．

[12] 外務省：日本の領土をめぐる情勢，入手先 ⟨http://www.mofa.go.jp/mofaj/territory/page1w_000011.html⟩（参照 2019-03-01）．

鈴木 敏明

1990年東京理科大学理工学部卒業．1992年同大学大学院修士課程修了．同年（株）日立製作所入社．以来，臨場感映像通信システム，アクティブネットワーク，省電力クラウドシステム，モバイルネットワーク管理システムの研究開発に従事．電子情報通信学会会員．

梶原 貴利

1992年久留米高専・電気工学科卒業．同年（株）日立製作所入社．以来，交換機システム，アクセスサーバ装置のソフトウェア開発に従事．

本橋 知子

1999 年東京工業大学理学部卒業．2001 年同大学大学院修士課程修了．同年（株）日立製作所入社．以来，アクセス・ネットワーク，モバイルネットワーク管理システムの開発に従事．

小村 和司

1988 年慶應義塾大学理工学部卒業．同年（株）日立製作所入社．以来，通信事業者向けの交換機システム，移動体通信システム，インターネットワークシステム，モビリティシステムの研究開発，多言語音声翻訳システムの実証に従事．電子情報通信学会，日本機械学会各会員．