氏名（本籍地）	佐藤（さとう） 彰洋（あきひろ）
学位の種類	博　士（情報科学）
学位記番号	情　博　第　５０５　号
学位授与年月日	平成２３年　３月２５日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	ユビキタス情報環境におけるネットワーク情報の分析法に関する研究
論文審査委員	（主査）東北大学教授　木下　哲男
	東北大学教授　鈴木　陽一　　東北大学教授　加藤　寧
	東北大学准教授　北形　元

論文内容の要旨

信頼性の高いユビキタス情報環境を実現するためには，ネットワーク情報を分析することで，管理対象のネットワーク内で発生する障害や攻撃などの出来事を把握して対処する必要がある．効率的なネットワーク情報の分析の実現するために重要な概念がイベントである．管理者は，通常と異なるネットワーク情報の変化をイベントとして検出し，そのイベントに関連する範囲のネットワーク情報を分析することで，発生原因を特定する．しかしながら，従来の分析法では，ユビキタス情報環境において必要不可欠な性質である，移動透過性，および高速大容量性を有するネットワークに対応できておらず，それらの確立が期待されている．

本研究の目的は，ユビキタス情報環境における，ネットワークの運用管理のための，ネットワーク情報の分析に関する基盤技術の構成とする．これは，ユビキタス情報社会の到来を見据えたものである．特に，ユビキタス情報環境において重要な要素となることが予想される，移動透過ネットワーク，および高速大容量ネットワークにおける問題を解決するため，本研究の研究課題として，(T1)移動透過ネットワークにおけるネットワーク情報の分析の効率化，(T2)高速大容量ネットワークにおけるネットワーク情報の分析の効率化，の２点を設定する．

課題(T1)で挙げられる移動透過ネットワークでは，管理主体の異なるネットワーク，すなわち複数の管理ドメインにわたる通信が発生するため，収集可能な個々のノードに関するネットワーク情報が制限される．そのため，イベントの検出が困難となり，ネットワーク情報を効率的に分析することができないことが問題となる．本論文では，第 2 章において収集可能なネットワーク情報に含まれる，イベントの検出に効果的なフローの変化点の判別とそれに基づく部分フローの選択を実現する，推移部分フロー選択手法を提案し，その解決を図る．

課題(T2)で挙げられる高速大容量ネットワークでは，多量のノードによる通信が頻繁に発生するため，管理ドメインで収集可能なネットワーク情報が膨大な量になる．そのため，特に多量のイベントが検出された場合，ネットワーク情報を効率的に分析することができないことが問題となる．本論文

では，第3章において，検出された膨大な量のイベントを比較することにより，発生原因が異なるイベントのみを選択を実現する，イベント分析価値評価手法を提案し，その解決を図る．

第2章　移動透過ネットワークに適したネットワーク情報の分析法

移動透過ネットワークは，接続するネットワークの変更時においても，ノード間の通信を維持できる性質を持つ．すなわち，ユーザの移動や状況の変化に応じて物理的に接続しているネットワークを変更すること，かつ変更時においてもユーザが継続的に情報サービスを利用することが可能となる．移動透過ネットワークを実現するための技術として，Mobile IPv6 (MIP6)，Network Mobility (NEMO)，IP Multimedia Subsystem (IMS)が注目されており，それらに関する研究が盛んに行われている．

移動透過ネットワークの運用管理において，個々のノードに関するネットワーク情報の分析により，管理者が注目するトラフィックの発生を検出することが重要となる．その実現のために，トラフィック分類手法が提案されている．この手法は，ネットワーク情報に基づいてP2Pなどの組織のポリシーに違反するトラフィックの発生をイベントとして検出し，それらを対応するクラス毎に分類する，イベント検出手法の一種である．クラスの例としては，アプリケーション毎，およびバルクデータやリアルタイムデータに代表されるトラフィックの種類毎などが挙げられる．これらの分類結果は，管理者によるネットワークの使用状況の把握やトラフィックの制御に用いられる．トラフィック分類手法は，利用するネットワーク情報により，(1)パケットの情報に基づく手法，(2)フローの情報に基づく手法に大別される．フローの情報に基づくトラフィック分類手法は，機械学習と先頭部分フローの特徴を利用した分類を行う．先頭部分フローとは，ノード間におけるアプリケーションの通信から切出される最初の連続したNパケットであり，特徴とはフローを構成する個々のパケットから計測可能な統計的特徴である．

しかしながら，ノードが通信の途中に移動することを想定している移動透過ネットワークでは，管理主体の異なるネットワークにわたる通信が発生するため，ノードに関する収集可能なネットワーク情報が制限される．具体的には，ノードが他のドメインから管理ドメインに移動した場合，管理ドメインでは，ノードが移動してくる以前のネットワーク情報，すなわち先頭部分フローの特徴を計測することができない．そのため，移動透過ネットワークにおいてフローの情報に基づくトラフィック分類手法を適用することが困難となる．幾つかの分類手法ではその問題の解決を試みているが，それらの手法はバルクデータ，低ビットレートリアルタイムデータ，および高ビットレートリアルタイムデータなどの粒度の荒いトラフィックの分類や，ゲームアプリケーションなどの非常に限定されたトラフィックの分類のみにしか対応できていない．すなわち，一般的なアプリケーションに対応可能な先頭部分フローに依存しないトラフィックの分類の実現が望まれている．

本章では，これらの問題点を解決するため，まず各アプリケーションが複数のタスクの組み合わせにより構成されることを明らかにし，そのタスクを考慮して部分フローの特徴の分析した．分析の結果から，大きく分けて，次に示す2つの知見を得た．(1)トラフィックの分類におけるタスクの推移点から得られる部分フローの有効性，(2)フローにおける推移点の判別と部分フローの選択方法．それらの知見に基づいて，収集可能なネットワーク情報に含まれる，トラフィックの分類に効果的なフローの変化点，すなわち推移点の判別とそれに基づく部分フローの選択を実現する，推移部分フロー選択手法を提案した．また，プロトタイプシステムを用いた実験と評価を通じて，提案手法により，移動透過ネットワークにおいて一般的なアプリケーションのトラフィックを高精度で分類できることを示

した.

第3章 高速大容量ネットワークに適したネットワーク情報の分析法

高速大容量ネットワークは，単位時間当たりに膨大な量の情報を処理できる性質を持つ．遍在する多種多様のノードによる位置や周辺の状況などの実時間性が要求されるコンテクスト，および音声や映像などの大容量性が要求されるコンテンツの交換により，それらを利用した高度な情報サービスの実現が期待できる．高速大容量ネットワークを実現するための技術として，フォトニックネットワークや光無線通信などが注目されており，それらに関する研究が盛んに行われている．

高速大容量ネットワークの運用管理において，ネットワーク全体に関するネットワーク情報の分析により，機器の障害や外部からの攻撃など，管理ドメイン内で発生する出来事を把握することが重要となる．その実現のために，異常検出手法が提案されている．この手法は，正常時と現在のネットワーク情報の差違に基づいて，管理ドメインにおける様々な出来事の発生をイベントとして検出する．管理者はそのイベントを分析，すなわちイベントに関連する範囲のネットワーク情報を分析することで，その発生原因を特定し必要に応じて対処する．

しかしながら，高速大容量ネットワークでは，管理ドメインで収集されるネットワーク情報が膨大になるため，個々のイベントの分析における管理者の作業負担が増大する．それに加えて，多量のイベントが検出された場合，管理者が全てのイベントを分析することが困難となる．そのため，イベントの分析を効率化する手法の実現が望まれている．

本章では，既存の異常検出手法により検出された多量のイベントに対し，管理者による効率的なイベントの分析を支援する「イベント分析価値評価手法」を提案する．本手法の特徴は，イベント時のトラフィックが持つ情報量に基づき，イベントの分析価値を与え，管理者が分析を行うべきか否かの判断基準とすることである．これにより，多量のイベントが検出され，全てのイベントを分析しきれない場合に，発生原因が異なるイベントのみを選択することで，管理者が分析するイベントの数を大幅に抑制することができる．プロトタイプシステムを用いた実験と評価を通じて，提案手法により導出された分析価値に基づいてイベントを選択することで，希少なイベントを見逃すことや，類似したイベントを何度も分析することなく，その発生原因を効率良く特定できることを示した．

第4章 結論

本論文では，推移部分フロー選択手法とイベント分析価値評価手法の提案により，ノードに対する移動性・遍在性の付与に不可欠である，移動透過ネットワーク，および高速大容量ネットワークにおけるネットワーク情報の効率的な分析を実現した．これらの成果は，ユビキタス情報社会の到来に向けた，信頼性の高いユビキタス情報環境を支える，ネットワークの運用管理の発展に貢献するものである．

今後の課題としては，ユビキタス情報環境におけるネットワーク情報の収集や評価，ネットワークに対する操作の効率化・高度化を目指す．

論文審査結果の要旨

信頼性の高いユビキタス情報環境を実現する上で、その基盤となるネットワークから得られる運用情報を分析し、ネットワーク内で発生する障害や攻撃などの事象を把握することが重要である。ネットワーク管理者がこうした事象を把握しようとする場合、その手段としてイベントを定義し、ネットワーク情報の異常な変化をイベントとして検出し、その原因を特定することが必要となる。しかし、現状では、ユビキタス情報環境向きネットワークにおける重要な性質である移動透過性や高速大容量性を考慮した分析手法は確立されていない。そこで著者は、この問題に着目し、ユビキタス情報環境向きのネットワークを対象としたネットワーク情報の分析手法について詳細に検討した。本論文は、その成果をまとめたもので、全編4 章から成る。

第1 章は序論である。

第2 章では、移動透過性を有するネットワークにおける分析法について検討している。このタイプのネットワークでは、ノードが管理主体の異なるネットワーク間を移動して、複数の管理ドメインにまたがる通信が発生し、個々のノードで収集可能なネットワーク情報も制限されるため、個々のノードに関するイベント検出が困難となる。この問題に対処するため、収集可能なネットワーク情報に含まれるフローの変化点を判別してイベントを抽出する推移部分フロー選択手法を提案し、実験によりその有効性を確認した。これは移動透過性を有するネットワークの特性を考慮したイベント検出手法として有用な提案である。

第3 章では、高速大容量ネットワークに適した分析法について検討している。このタイプのネットワークでは、管理ドメインで提供される種々の情報サービスを多数のノードが利用するため、収集可能なネットワーク情報や検出されるイベント数が膨大となり、これら全てを分析対象とすることが困難となる。そこで、検出されたイベントの特徴解析によるランク付けを行い、分析対象とすべきイベントの選択を効率的に行うイベント分析価値評価手法を提案し、実験を通してその効果を確認した。これは、高速大容量ネットワークにおける効率的なイベント検出を実現する上で有用な手法であり高く評価される。

第4 章は結論である。

以上要するに本論文は、ユビキタス情報環境におけるネットワークの特性を考慮したイベント検出のための新しい手法を与えたものであり、ネットワーク運用管理技術、ならびに情報基礎科学の発展に寄与するところが少なくない。

よって、本論文は、博士（情報科学）の学位論文として合格と認める。