（様式 5）

指導教員 承認印	

平成　27 年　2 月　12 日

学位（博士）論文の和文要旨

論文提出者	工学府博士後期課程　　電子情報工学専攻 平成　24 年度入学 学籍番号　12834305　　氏名　　宮田　宏　　印
主指導教員 氏　　名	並木　美太郎　教授
論 文 題 目	A Study on Real-time Communications Management Based on Packet Propagation Time Monitoring and Hop-by-Hop Packet Authentication for Process Automation （パケット伝達時間監視と Hop-by-Hop パケット認証に基づくプロセス オートメーション向け実時間通信管理に関する研究）

論文要旨

本論文は，プラント内の施設間に敷設される産業用 Backhaul と呼ばれるネットワークを用いたプロセスオートメーションを可能とするため，信頼の高い実時間通信を管理するための研究について述べる．既存研究においても実時間通信を提供する事を目的としたものが存在する．しかしながら，そのほとんどがネットワーク機器の設定を行なうものの，実時間通信の確認を行なわない．またネットワーク機器が実時間通信を偽装したパケットを検出できないため，攻撃者が実時間通信を阻害する事が可能である．本研究では，パケット伝達時間の測定を含む「実時間通信確認機能」と「実時間通信偽装防止機能」という二つの機能を提供する事で，これらの問題を解決し，実時間通信を管理する事を可能とした．

第 1 章では，背景を説明する．プラントの中では機能階層毎に実時間通信が異なる．その中で，生産プロセスを制御や監視を行なう Level1，2 の通信に強く実時間通信が求められる(PID 制御では 0.3 秒周期，操作・監視端末では 1 秒の反応時間)．また，プラントにおいてはプラント敷地内に分散した施設を産業用 Backhaul で接続し，生産プロセスに関わる Level1,2 の通信をこの上で行ないたいという要求がある．したがって，産業用 Backhaul は，実時間通信を提供する必要がある．一方で，産業用 Backhaul を利用する実時間通信は静的なものに加え動的なものが現れてきていること，プラントもサイバー攻撃の対象となっていることなどから，トラフィックの特性や攻撃の危険性を考慮し，実時間通信を保証する事が求められる．以上をふまえ，本研究では「産業用 Backhaul を用いた PA を実現す

るために高信頼の実時間通信を提供する方式を明らかにする」ことを目的とする.

第２章では，既存研究を示し，本研究の目的を達成するための阻害要因を分析し対応状況を示す．実時間通信を保証するためには，「1.帯域制御機能」「2.帯域割り当て機能」「3.実時間通信評価機能」「4.帯域不正予約防止機能」「5.実時間通信偽装防止機能」の五つの機能が必要である．既存の研究では，これらの機能のうち「3.実時間通信評価機能」と「5.実時間通信偽装防止機能」を十分に提供できない事を示した.

第３章では，本研究の位置づけを明確にし，課題と目標を示す．本研究では，目的を達成するために既存研究では提供されていない「実時間通信評価機能を提供する」「実時間通信偽装防止機能を提供する」の二点を主要課題と定義する．本研究では，これらの課題を解決するためにそれぞれ，「パケット伝達時間に基づく実時間通信管理方式」，「パケットを中間機器で認証し送信 Queue を保護する方式」の開発を目標とする.

第４章では，「パケット伝達時間に基づく実時間通信管理方式」を実現するための提案を示す(文献[2][4]).提案方式は OpenFlow を基に設計を行なった．本提案方式はネットワーク機器の送信 Queue に割当てられた帯域の利用状況の観察に加え，パケットの伝達時間を観察することで，タイムアウトの発生を検出・予測し，適切に帯域の割当量を変更する．試作，評価により，帯域使用量と，パケット伝達時間の二つの監視機能が相互に補完関係となり，動的な通信に対しても実時間通信を提供できる事を確認できた．本提案方式により，「パケット伝達時間に基づく実時間通信管理」を実現可能とした.

第５章では，「パケットを中間機器で認証し送信 Queue を保護する方式」を実現するために，まず QoS Spoofing 攻撃が可能となる原因を分析し，対策としてパケットの Hop-by-Hop 認証方式を提案する(文献[3]). QoS Spoofing 攻撃は，実時間通信パケットを詐称することで実時間通信用の帯域を消費し，実時間性を阻害する．この攻撃を防ぐためには中間機器の送信 Queue の帯域が消費される前に不正パケットを破棄することが必要である．そこで軽量な Hop-by-Hop のパケット認証方式を提案した．試作と検証により，提案する方式は PA の実時間要求を満たしながら詐称パケットを検出・破棄できることを確認した.

第６章では，第５章で提案した Hop-by-Hop の認証機能を OpenFlow の帯域制御と経路制御機能を活用する事で，柔軟かつスケーラブルに提供する方式を提案する(文献[1]).この方式は OpenFlow 環境に新たにパケット認証プレーンを導入することで実現している.本方式により，柔軟なフローの定義に基づく帯域制御，任意の場所でパケットの Hop-by-Hop 認証，パケット認証機能のスケールアウトが提供可能である．試作・検証により，提案する方式は帯域の保護が可能であり，オーバーヘッドも PA の要求に対し十分に小さいことが確認できた．本提案方式により，「パケットを中間機器で認証し送信 Queue を保護する方式を開発する」を実現可能とした.

第７章では，本論文を総括する．本研究では第４章に示した方式で，静的，動的な通信のいずれに対しても「実時間通信評価機能を提供する」という課題を解決した．また，第５章，第６章に示した方式で「実時間通信偽装防止機能を提供する」という課題を解決した．第４章，第６章の方式はともに OpenFlow を用いているため相性が良く，併用する事が可能である．以上，本研究の二つの目標が実現できたことにより，産業用 Backhaul を用いた PA を実現するために高信頼の実時間通信を提供する方式を明らかにできたと言える.本研究では，帯域使用状況の監視と伝達時間監視はそれぞれが有利な点，不得意な点があり，単独での利用では信頼性の高い実時間通信を管理するためには十分ではなく，組合せが重要であるということ，Hop-by-Hop のパケット認証は実時間通信に対する影響が懸念されるが PA の要求に対しては利用可能であるということを明らかにした.