

IoT サービス用シームレスプラットフォームシステムの基礎研究

[研究代表者] 内藤克浩 (情報科学部情報科学科)
[共同研究者] 鈴木秀和 (株式会社 モビリン)

研究成果の概要

モノのインターネットと呼ばれる IoT(Internet of Things)が注目されており、近年多くのサービス提案が行われている。具体的には、一部の自動車などはリモートメンテナンスを実現するための携帯電話モジュールが内蔵されており、故障時などは遠隔地から障害箇所の診断などが行える。一方、多くの家庭で利用される WiFi を利用する IoT 機器も発売されているが、その多くが設置時のネットワーク設定が必要であり、情報技術の知識がなければ、IoT 機器を適切にネットワークに接続することが困難である。このようなネットワークの接続性に関する課題は、多くのオフィス・家庭で導入されているブロードバンドルーターなどのファイヤーウォールが原因である。IoT サービスを今後普及させるためには、ネットワーク設定を簡易にすることで、ネットワークの接続性を改善する手法が非常に重要になると考えられる。

本研究では、IoT 機器のネットワーク接続性を実現する要素技術と、特に多数の IoT 機器を包括的に管理可能な規模拡張性を持つプラットフォームシステムの研究を行なっている。本年度は主に、今まで検討を進めてきたプラットフォームシステムを実現するための通信プロトコル部の再設計を進めている。また、Cloud サービスなどでも一般的に利用される Linux OS において、処理プロセスが増加した場合のオーバーヘッドについても、定量的な評価を実施してきた。これらの評価の結果、通信処理ごとにスレッドを起動することにより、独立したスレッドが通信処理を分担する方式の場合、通信処理が増加した場合には、大きな処理オーバーヘッドが発生することが確認された。

研究分野： モバイルネットワーク

キーワード： IoT, イターネット, 通信プロトコル, NAT 越え, モビリティ

1. 研究開始当初の背景

モノのインターネットと呼ばれる IoT(Internet of Things)が注目されており、一部の車のリモートメンテナンス、ホームオートメーションなどのサービスが始まりつつある。IoT で接続されるネットワークとは、通常はインターネットであるが、インターネットには利用している通信プロトコルの都合から、いくつかの課題がある。大きな課題の一つが、多くの家庭・企業において導入されている NAT(Network Address Port Translation)と呼ばれる技術である。NAT を導入しているネットワークでは、インターネット側から NAT 配下のネットワーク機器にアクセスが不可能となり、IoT 機器を遠方から操作するなどに大き

な支障が発生する。つぎに、IoT 機器が互いに通信を行うことにより連携したサービスを提供する場合には、互いの IoT 機器のネットワーク上での位置を把握する必要がある。しかしながら、既存のインターネットでは、接続される場所が未知の IoT 機器を一般的な利用者が管理することは困難であり、IoT 機器をネットワーク上で探し出すための枠組みが必要である。さらに、近年のインターネットでは、新しいプロトコルである IP(Internet Protocol) Ver. 6 が普及を始めている。しかし、現在主流である IPv4 との互換性がないため、IPv4 と IPv6 間の相互接続を行うための通信技術も将来的には必要不可欠である。

2. 研究の目的

本研究では、IoT 機器のネットワーク接続性を実現する要素技術と、特に多数の IoT 機器を包括的に管理可能な規模拡張性を持つプラットフォームシステムの研究を実施している。本年度は主に、今まで検討を進めてきたプラットフォームシステムを実現するための通信プロトコル部の再設計を実施した。また、クラウドサービスなどでも一般的に利用される Linux OS において、処理プロセスが増加した場合のオーバーヘッドについても、定量的な評価を実施する。

3. 研究の方法

(1) 通信プロトコルの設計

提案システムを実現するためには、IoT 機器を認証する枠組み、IoT 機器のネットワーク接続状態を把握する枠組み、IoT 機器間の通信を成立させる枠組みが必要不可欠である。本研究では、図 1 に示す通信シグナリングを設計することにより、上記の必要要素を実現する。図 1 は IoT 機器の双方がグローバル IP アドレスを利用している場合の通信シグナリングである。まず、双方の IoT 機器はログイン処理を行うことにより、提案するプラットフォームへの参加処理を行う。この処理を通して、IoT 機器とクラウド間で利用する通信用暗号鍵などの設定が終わる。次に、IoT 機器は自身のネットワーク接続情報をクラウドに送信することにより、ネットワークの接続情報の登録を行う。この処理により、クラウドは各 IoT 機器がどのようなネットワークに接続されているのかを把握することが可能となる。次に、IoT 機器が相互通信する場合、クラウドが双方の IoT 機器のネットワーク接続情報に応じた通信手順を双方の IoT 機器に指示することにより、IoT 機器が互いにメッセージを交換し、直接通信を開始する。なお、直接通信には、個別の通信用暗号鍵が準備されるため、クラウドが相互通信に関与はしているが、IoT 機器間の相互通信安全性は保証されている。

(2) クラウドシステムの基礎性能評価

クラウドシステムの規模拡張性の基礎評価として、通信処理をスレッドにより処理する場合のオーバ

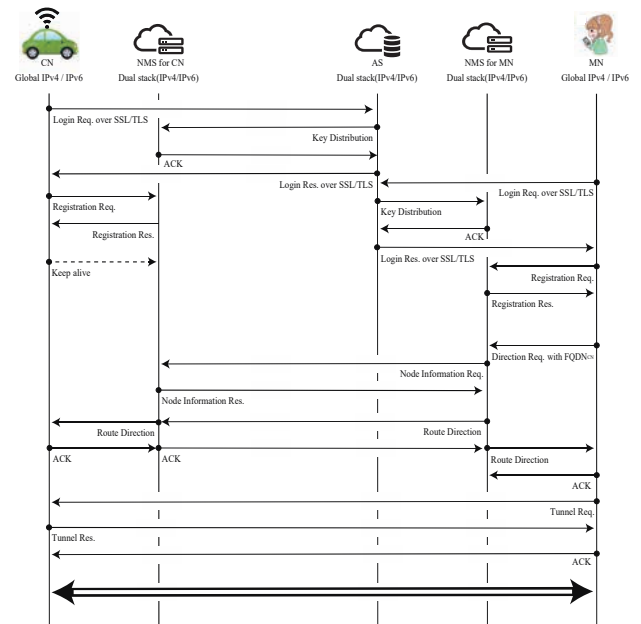


図 1 通信シグナリング例（グローバル IP アドレス間）

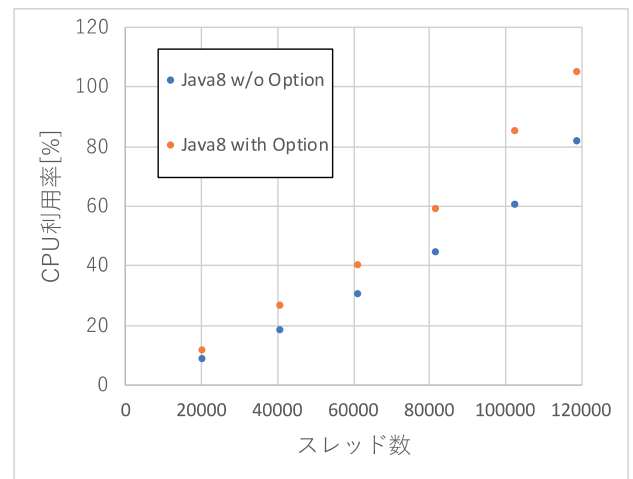


図 2 スレッド数に対する CPU 利用率

ヘッドの評価を実施した。評価には Amazon EC2 上の Linux OS を利用し、同 OS 上でスレッドを多数生成した場合の CPU 利用率を測定した。インスタンスタイプとしては、仮想 CPU16 個、メモリ容量 64GB の m4.4xlarge を利用した。なお、本評価で利用する評価プログラムは、スレッド生成のみを行い、その他の処理は一切行わない仕様とした。結果より、実質的な処理を行わない場合においても、スレッド数の増加に伴い CPU 利用率は増加を続けていくことが確認された。これは、スレッド間の処理を切り替えるための CPU オーバーヘッドが大幅に増加したためと考えられる。また、スレッドベースで処理をするクラウド設計は規模拡張性の観点から向いていない可能性が高いことが判明した。

4. 研究成果

本研究では、IoT 機器のネットワーク接続性を実現する要素技術と、特に多数の IoT 機器を包括的に管理可能な規模拡張性を持つプラットフォームシステムの研究を進めてきた。本年度は特に、プラットフォームシステムを実現するための通信プロトコルの設計を見直すとともに、クラウドサービスの規模拡張性が高い実装方法を模索するための、基礎的な評価を実施した。結果より、今後のクラウドサービスの実装では、スレッドベースではなく、イベントベースの処理機構を利用することが必要であることが明らかになった。

5. 本研究に関する発表

(1) Hisayoshi Tanaka, Hidekazu Suzuki, Katsuhiro Naito, Akira Watanabe, “Implementation of Secure End-to-End Remote Control System for Smart Home Appliances on Android”, The IEEE International conference on Consumer Electronics ICCE 2019, Las Vegas, USA, January 2019.

(2) Katsuhiro Naito, Kohei Tanaka, Kensuke Tanaka, “発 CYPHONIC: Overlay Network Technology for Cyber Physical Communication”, The 10th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC 2019, Orlando, USA, March 2019.