ISS-A-020

機械学習による CoAP の輻輳予知の検討

胡　家豪†　　寺澤　卓也†
† 東京工科大学大学院 バイオ・情報メディア研究科

1. はじめに

近年、インターネットに繋がるデバイスの数や多様性が増え、様々な新しいアプリケーションシナリオが想定されるようになった。典型的に、IoT には、低電力無線センサーノードなどの制約されたデバイスが使用される。さらに、これらのデバイスで使用される通信技術には、低いデータ転送速度や比較的高い bit error rate などの大きな制限がある。CoAP[1]は、これらの極端なリソースの制約に合わせて調整されている

CoAP は、RTO に基づいた単純な輻輳制御メカニズムを提供する。ただし、インターネットの状態への対応が鈍い。そのため、デフォルトの CoAP 輻輳制御は実際のネットワークの状態情報から動作を決めていないので、急進すぎるか保守すぎる傾向があり、性能が低くなる。

2. 研究目的

本研究では、CoAP を用いたトラフィックデータを収集するネットワークを構築し、機械学習を用いて、輻輳が発生する前に予知する手法を検討する。予知した後、RTO を調整することで輻輳を避けることを目的としている。

3. 先行研究

CoAP は、RTO と RTO タイマーの指数バックオフに基づいて、極めて基本的な輻輳制御を提供している。新しい信頼性のあるメッセージ交換ごとの初期 RTO は、同期効果を回避するために2～3秒の間のランダムな値に設定され、RTT 推定を行わない。

CoCoA[2]では、強い RTO 推定と弱い RTO 推定に基く、特定の RTO 計算ロジックで RTT 値の推定を実行する。さらに、CoCoA は、再送信タイマーが満了するたびにバイナリ指数 RTO バックオフを使用する代わりに、可変バックオフ係数を使用する。

ネットワーク攻撃検出の分野では、機械学習を使い、攻撃者の行動を予測する研究がある。[3]のアプローチは、機械学習技術を使用し、攻撃者の歴史的行動を学習する。実行時に、この知識を活用して攻撃者の将来の可能性のある行動を予知する。

輻輳制御の場合では、機械学習を通して、ネットの使用状況を分析し、輻輳が発生する兆候を判別する。それに基き、バラメータ調整のタイミングを繰り上げ、輻輳を避けると共に、パケット損失を抑えることも期待できる。

4. 提案と進捗状況

機械学習では、学習させるデータが必要である。しかし、CoAP に関するトラフィックデータを調査しているが、見つかっていない。そこで、自分で収集することが必要である。

輻輳が発生するシナリオは大きく二つ考えられる。一つはノード数が大量であるため、個々のパケットが小さくてもデータを収集するサーバーへのトラフィック全体では膨大であり、輻輳が発生する。もう一つは突発的なイベントの発生によって、バースト的にトラフィックが発生する場合である。

そこで、CoAP を用いて、センサーネットワークとアプリケーションを構築し、学習用データを収集することにする。現在は、センサーのノードコントローラーに予定している Raspberry Pi を使って、CoAP 経由で違うデバイスの間の通信ができている。

5. 今後の予定

センサーを Raspberry Pi に実装し、CoAP を使って通信をできるようにする。価値のあるデータを収集するために、現実的かつ輻輳が発生するセンサーネットワークの環境を作り、データを収集する。データを取ると同時に、適切な学習モデルを作り、調整する。普段輻輳がない時のデータと輻輳時のデータを共に収集し、学習させる。

輻輳予知はパターン認識と異常検知の問題だと考えている。機械学習アルゴリズムでは、特徴空間における最も近い訓練例に基づいた分類の手法である K 近傍法を使う予定である。

輻輳予知ができたら、輻輳回避の階段に入る。輻輳が発生する直前に、再転送の速度を下げることで制御する。普通の状況では、CoCoA を使い、RTO 時間を推定し実行する。

参考文献

[1] C.Bormann, et al. ″CoAP: An application protocol for billions of tiny internet nodes.″ IEEE Internet Computing Vol.16,Issue 2 (2012): pp.62-67.

[2] A.Betzler,et al. ″CoAP congestion control for the internet of things.″ IEEE Communications Magazine Vol.54,Issue.7 (2016): pp.154-160.

[3] C.Cipriano, et al. ″Nexat: A history-based approach to predict attacker actions.″ *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 2011. pp.383-392.