IoTデバイスを用いたDDoS攻撃の機械学習によるオンライン防御法

1.攻撃の流れ

- IoTデバイスは低スペックであり、また不特定多数の人や組織が設置・管理するため、セキュリティ対策が不十分なことが多い
- また製造会社が異なったデバイス同士を通信させることが多いので通信方法が煩雑になり、脆弱性が発生しやすい
- 攻撃者はIoTデバイスをサイバー攻撃の踏み台として悪用
  多数のIoT端末をマルウェアに感染(ボット化)させ、多数のボットから大量のパケットを標的サーバに送信

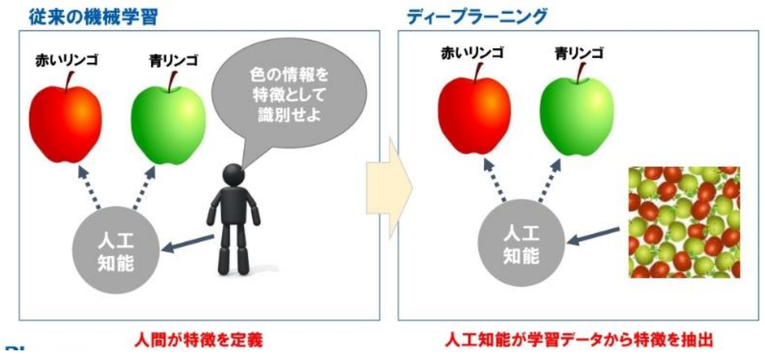
生活基盤を支えるインフラや利用者の多いサービスに対して攻撃が行われた場合、甚大な被害が予想される

2.機械学習を用いたDDoS検知

- 従来のDDoS検知法
  - 生成パケット数の計測による検知⇒閾値の設定法が難しく正常な場合を誤検知する可能性
  - パケット数の時系列変化パタンによる検知⇒やはり正常な場合を誤検知する可能性
- 機械学習を用いたDDoS検知法
  - DNN(深層学習)や、その時系列予測版であるLSTM (long short term memory)を用いて異常検知
  - 教師データ(パケット数の時系列パタンなどと正解ラベルの組)を用いてモデルを学習
  - 構築モデルにテストデータを入力すれば推定結果を出力

3.ディープラーニング(深層学習)

- 人間の脳のニューロンの構造と機能を模倣したニューラルネットワークを何層にも重ねて大規模にした機械学習の手法
- 従来の機械学習と異なり，特徴量設計が不要
  - 例えばk-means法や決定木を用いる場合，事前に抽出したサンプルの特徴量に基づきサンプルを分類・判定
  - 深層学習では，サンプルデータをそのまま入力すれば．特徴抽出と分類を一度に実施可能
- 入力と出力との間の複雑な関係も学習することが可能で、万能な関数近似器としての役割が可能



4.アプローチ

- LSTMやDNNをP4言語を用いてプログラマブルスイッチに実装し，IoTデバイスを用いたDDoS攻撃をリアルタイムに検知
- システムの実装評価

5.プログラマブルスイッチとは

- パケットをどこに転送するのかや，パケットに新しくフラグを付与するといった，パケット処理をプログラミング可能なスイッチ
- ユーザがプログラミングすることでベンダーによる製品選択の制約がなくなり，自由に製品を選択可能

6.P4とは

- P4 (Programming Protocol-Independent Packet Processors)と呼ばれる，プログラマブルスイッチに実装可能なプログラミング言語
- プログラムに記述した条件がパケットに合致した場合の処理や，データの計算処理を記述することが可能
- またユーザが自分でパケットを作り替えることが可能