深層学習を用いたインターネットトラフィックの異常検知手法 GAMPAL (1/2)

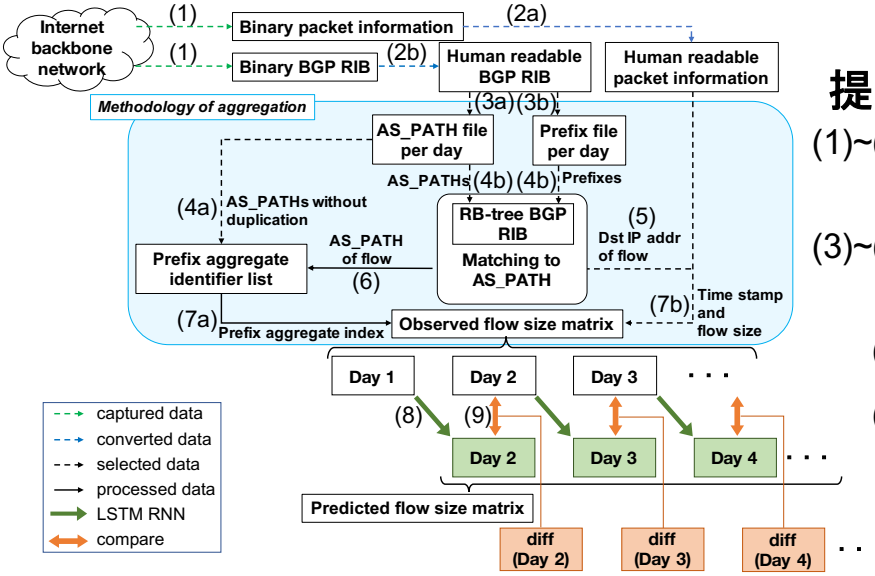
和久井拓, 近藤賢郎, 寺岡文男　{dona, latte, tera}@inl.ics.keio.ac.jp

- **インターネットバックボーンにおける異常検知**
  - インターネットバックボーン
    - 様々なネットワークを相互に接続する大規模なネットワーク
    - 多種多様なサービス・ユーザのトラフィックが大量に流れる
      →平常時でも時間軸に対する変動が大きい
    - 様々な要因の異常事象が発生 (e.g., 機器故障, サイバー攻撃, イベント)
  - インターネットバックボーンのインターネット・トラフィックの特性
    - 局所性: 宛先アドレスが観測点から近いほどトラフィック流量が多い
      - ユーザが利用するサービスの局所性に起因
    - 周期性: トラフィック流量の1日単位の周期性や曜日毎の特徴
  - 異常検知機構の必要性
    - 機器故障やイベントが要因の場合: ユーザやサービスに影響
    - サイバー攻撃が要因の場合: ユーザやサービスに影響 / 加害者になる恐れ

    ⇒ 異常事象を検知し早期対処につなげるシステムが必要
- **深層学習によるインターネットトラフィックの異常検知**
  - トラフィックの特徴を学習
    - 多くの手法ではサイズや IP アドレスなどの属性を学習し分類器を作成
    - 未知の脅威に対応可能
    - 分類器の学習には収集が困難なラベル付きデータが必要
  - スケーラビリティの問題
    - インターネットで観測される通信フローごとの学習・予測は非現実的
    - 異常検知性能を損なわないトラフィックの集約方法が必要
- **提案手法 GAMPAL: General-purpose Anomaly detection Mechanism using Prefix Aggregate without Labeled data**
  - 経路情報 (AS_PATH) に基づくトラフィック集約
    - インターネット・トラフィックの局所性に基づいた集約方式
  - LSTM (Long Short-Term Memory) -RNN によるトラフィック流量予測
    - インターネット・トラフィックの周期性を反映
  - 平常時を予測したトラフィックと実測トラフィックの流量を比較
    - 未知の脅威を含めた多種多様な異常事象を汎用的に検知
    - 収集が困難なラベル付きデータが不要

深層学習を用いたインターネットトラフィックの異常検知手法 GAMPAL (2/2)

和久井拓, 近藤賢郎, 寺岡文男　{dona, latte, tera}@inl.ics.keio.ac.jp



提案手法 GAMPAL の概要図

(1)~(2)　データをインターネットバックボーンからデータを収集

(3)~(7)　AS_PATH (経路情報) に基づいたトラフィック集約機構

(8)　LSTM-RNN による流量予測

(9)　予測値と実測値の比較

● 経路情報 (AS_PATH) によるトラフィック集約方式

- Prefix Aggregate: AS_PATH 属性で集約された IP Prefix の集合
  - **AS_PATH**: 宛先 IP アドレスによって定まるトラフィックの BGP 経路
  - 観測点の視点で AS_PATH が 3 ホップまで共通する Prefix を集約
- トラフィックを宛先アドレスで Prefix Aggregate ごとに集約し学習・予測

観測トラフィック

Time	src IP	dst IP	bytes
00:00	x.x.x.x	1.0.0.1	6
00:02	x.x.x.x	1.0.4.1	18
00:02	x.x.x.x	1.0.5.1	5
00:04	x.x.x.x	1.0.0.4	6
00:06	x.x.x.x	1.0.0.1	15
00:12	x.x.x.x	1.0.0.4	3
00:14	x.x.x.x	1.0.6.1	6

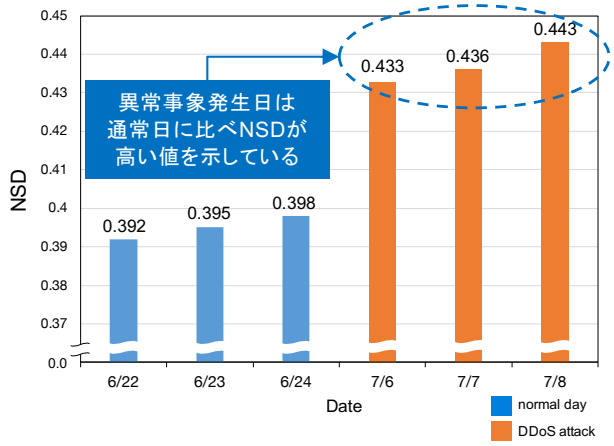
Prefix Aggregate
AS_PATH 属性で集約された Prefix

Index	Aggregated AS_PATH (Prefix aggregate identifier)	Prefix
1	4713 2914 13335	1.0.0.0/24
2	4713 2914 15412	1.0.4.0/24 1.0.6.0/24
3	2497 2519	1.0.5.0/24

Prefix Aggregate で集約されたトラフィック

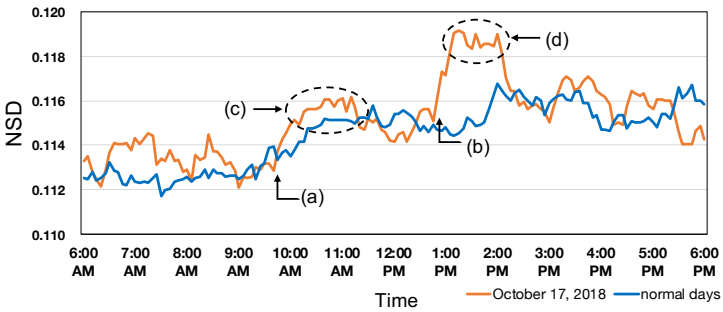
Time	src IP	dst IP	bytes
00:00	x.x.x.x	1.0.0.1	6
00:02	x.x.x.x	1.0.4.1	18
00:02	x.x.x.x	1.0.5.1	5
00:04	x.x.x.x	1.0.0.4	6
00:06	x.x.x.x	1.0.0.1	15
00:12	x.x.x.x	1.0.0.4	3
00:14	x.x.x.x	1.0.6.1	6

● GAMPAL による異常検知性能の評価例



通常日と被サイバー攻撃日のNSD*の平均

＊NSD (Normalized Summation of Difference)
実測/予測トラフィックの差異を評価する独自指標



YouTube 接続障害発生日と通常日のNSDの推移

(a) 10/17 (オレンジ) のみ接続障害が発生した10時頃に
NSDが上昇 → 接続障害によるアクセス急減が原因
(b) 10/17 のみ接続障害が回復した12時台に
NSDが再度上昇 → 回復によるアクセス急増が原因
(c,d) NSDの上昇 (a.b) の後, その値を数時間維持
→ 接続障害が長時間影響を与えていることを示す