フローデータのまとまりを考慮した新たなグラフ構成手法と GNN による異常通信検知への適用

New Graph Composition Method based on Sets of Flow Data and its Application to Anomaly Traffic Detection with Graph Neural Networks

奥井 宣広
株式会社 KDDI総合研究所

秋元 裕介
株式会社 ARISE analytics

窪田 歩
株式会社 KDDI総合研究所

吉田 琢也
トヨタ自動車株式会社

背景

① 軽量なIPFIXによる異常通信検知の必要性

通信の高速化・大容量化に伴い，従来のパケットデータを用いた異常検知では処理性能の要件を満たせなくなりつつあるため，セッション単位の統計量を保持するIPFIXによる異常検知モデルを構築．

② 検知困難なマルウェア通信

先行研究における統計量を用いた異常検知手法では検知困難なC2通信を対象とした実験を実施．パケット数などの統計量に特徴が表れやすいDoS攻撃などと異なり，正常通信と似た特徴を持つ．

提案手法

入力データ

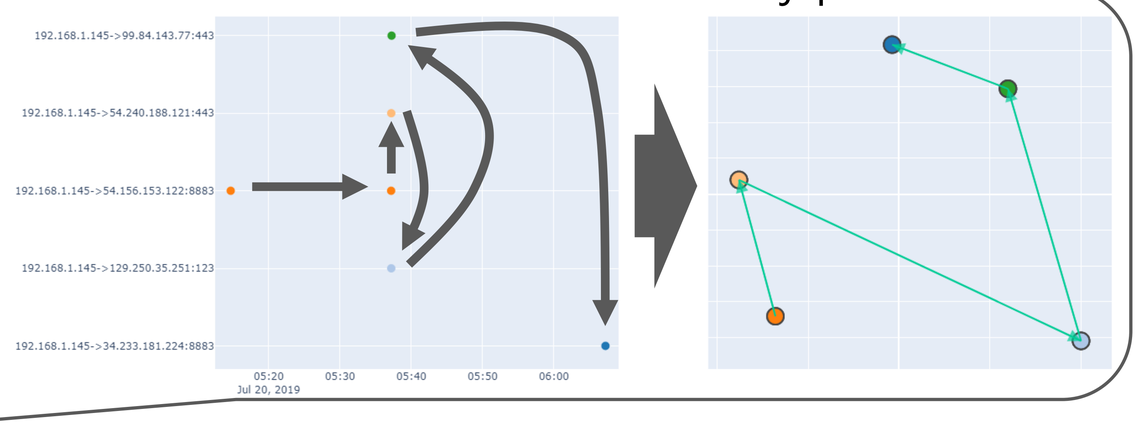
IPFIX

前処理

グラフの構築

Src/Dst IP、通信先ポートの組で1つの機能を表現

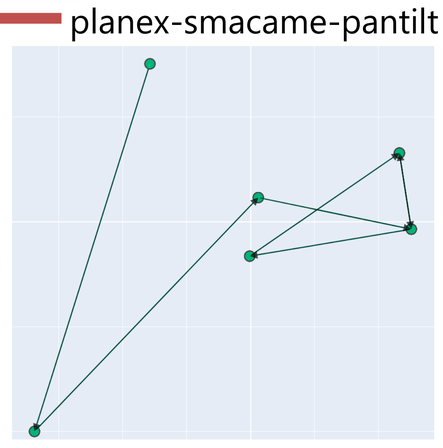
IPFIXレコードの通信開始時刻をもとにして，レコードに対応するノード間にエッジを張る



提案手法

- ノード：機能
- エッジ：機能の遷移

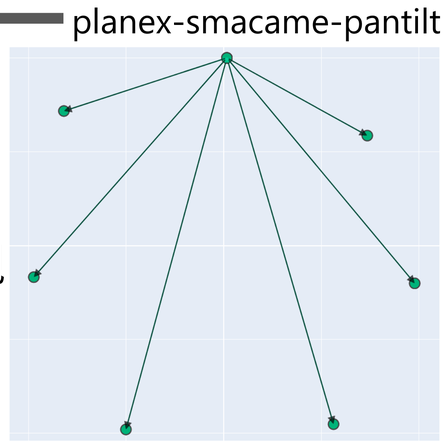
IoTデバイスが**どの機能にどのような順序でアクセスしたかをグラフとして表現**でき，グラフ理論における道を形成する



従来手法

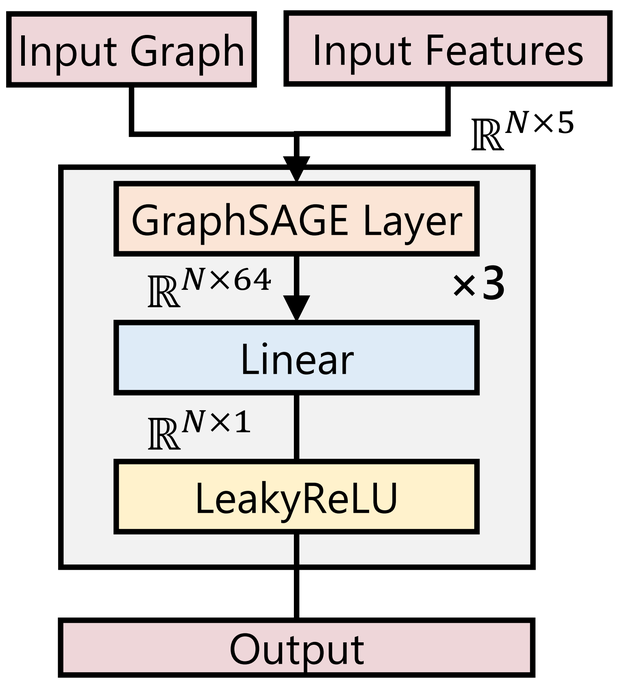
- ノード：ホスト
- エッジ：ホスト間の通信

ホスト同士の通信の様子を表現し，デバイスを中心としてスター型のグラフを形成する



- 従来手法ではC2サーバなど異常なホストへの通信が発生してもグラフの形状には現れにくい
- 提案手法は時系列に沿ったデバイスの機能へのアクセスの遷移を表現するため，C2サーバなど異常なホストへのランダムなアクセスは異常なトポロジーとして現れやすいと考えられる

異常検知



異常度スコア算出

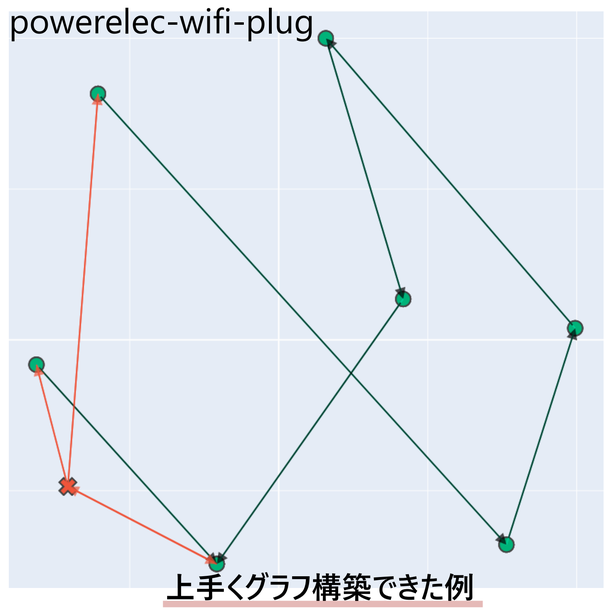
- GraphSAGEを用いてGNNモデルを構築
- 次数中心性に関する再構成誤差を最小化
- モデルの予測と入力グラフの次数中心性の差から異常度スコアを計算

実験結果

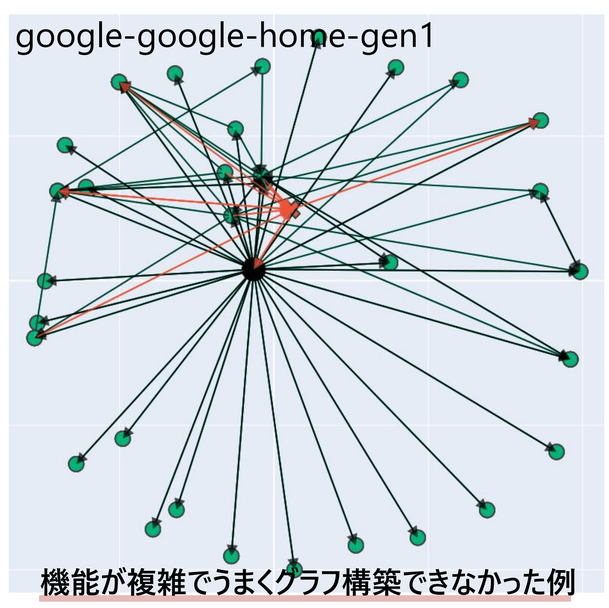
表 KDDI-IoT-2019データセットによる評価結果

デバイス	提案手法(F1)	従来手法(F1)
amazon-amazon-echo-gen2	0.005	0.005
au-network-camera	0.188	0.250
au-wireless-adapter	**0.476**	0.324
bitfinder-aware	0.303	0.455
candy-house-japan-sesame-wifi-access-point	**0.455**	0.400
google-google-home-gen1	**0.063**	0.044
i-odata-qwatch	0.303	0.706
irobot-japan-roomba	0.176	0.188
jvckenwood-hdtv-ip-camera	0.150	0.196
line-clova-wave	0.182	0.545
linkjapan-eremote	0.118	0.174
mouse-computer-room-hub	**0.571**	0.343
nature-nature-remo	**0.435**	0.227
panasonic-doorphone	**0.174**	0.135
philips-hue-bridge	0.099	0.119
planex-smacame-pantilt	**0.162**	0.154
powerelec-wifi-plug	**0.727**	0.381
qrio-qrio-hub	**0.600**	0.286
sony-bravia	**0.011**	0.004
sony-sony-smart-speaker	0.033	0.046
xiaomi-xiaomi-mijia-led	**0.429**	0.211

$$L = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{1}{2}(y_i - \hat{y}_i)^2\right) + \sum_{i=1}^{n} w_i^2$$



上手くグラフ構築できた例



機能が複雑でうまくグラフ構築できなかった例