加速度情報を用いたスマート自転車錠の認証方式の検討

情報工学科　笹瀬研究室　アーノ有里紗

背景

- 近年，高級自転車の流行により盗難事件が多発

問題点

- 自転車の鍵は，シリンダーキーや，暗証番号方式の鍵が主流
- シリンダーキーは小さく，紛失しやすく，折れやすい
- 暗証番号方式，ユーザは施錠の際に1,2桁をずらす程度の場合が多く実際のセキュリティが脆弱

提案

- スマートフォンと自転車に備え付けたセンサ付き錠を想定
- 走行時の加速度情報を基に鍵の施錠・開錠を行う方式を提案

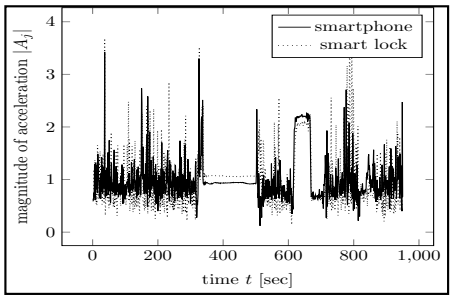


図１．測定した加速度情報

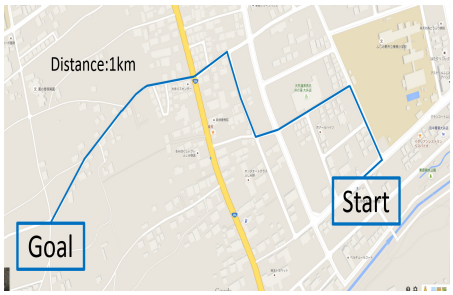


図２．自転車が走行した道順

図３．鍵および錠の配置図

☺ 鍵の持ち運び不要　☺ 環境情報が変化に富む　☺ ワンタイムパスワード

特性評価

錠と鍵	**Nexus 5**
サンプリング間隔	**1[sec]**
測定回数	**各20 回**
評価項目	**類似度 vs 時間**
評価に用いた類似度関数	**コサイン類似度** **スピアマン係数**

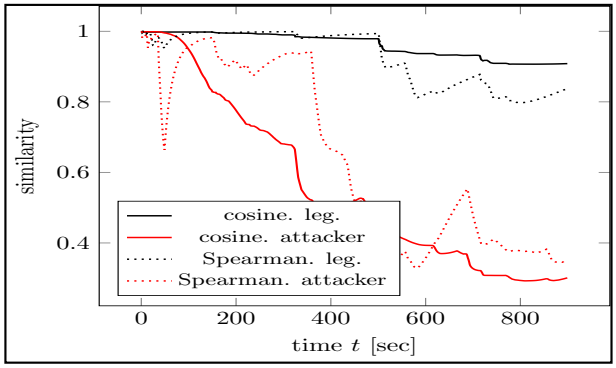


図４．加速度情報の類似度の比較

本研究に関する業績

[1]Alisa Arno, Kentaroh Toyoda, and Iwao Sasase, “Accelerometer Assisted Authentication Scheme for Smart Bicycle System,” in Proc. IEEE World Forum on Internet of Things 2015 (WF-IoT2015), Milan, Italy, 13-16 Dec. 2015

[2]アーノ有里紗, 豊田健太郎, 笹瀬巌, “加速度情報を用いたスマート自転車錠の認証方式の検討,” 電子情報通信学会通信方式研究会(CS), 北海道, 2015年11月11日-13日

ソーシャルネットワークの不正アカウント検出における高度な攻撃者に対してロバストなシード選択及びグラフ剪定法

情報工学科　笹瀬研究室　春田秀一郎

▪ 研究背景

- FacebookやTwitter等の
- ソーシャルネットワークの利用が流行
- スパム等を送信する不正アカウントが出現

▪ 従来研究

- 信頼されたアカウント（シード）の信頼値を近隣に繰り返し分配
- Sybilと正規アカウントの友人関係(AE:Attack edge) は少ないためSybilの得る信頼値は小

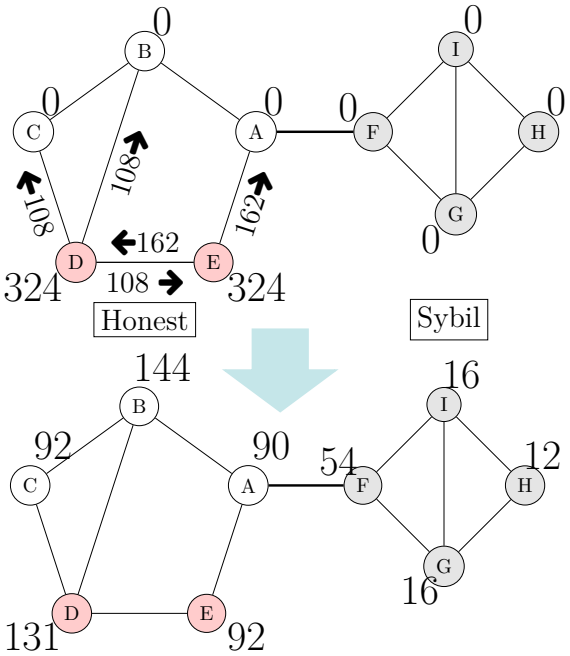


図1:従来方式の信頼値分配の例

- シード選択はランダムなため信頼値の偏りが発生する問題
- AEを予め剪定できればSybilの得る信頼値を低減可能.[1]では共通友人数に着目して剪定
- 方式[1]では共通友人数を増加させる高度な攻撃者に対応不可能である問題

▪ 提案方式

- コミュニティ検知を行い, 全体ネットワークに対して均等にシードを選択する方式を提案
- 友人関係の結びつきの密度に基にAEを剪定する方式を提案

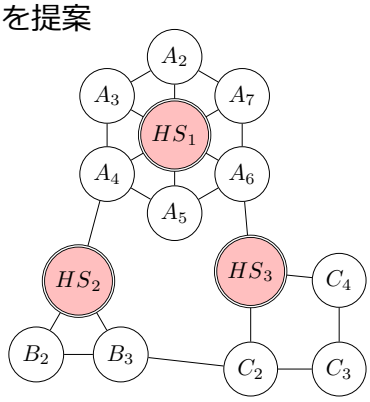


図2: 提案方式のシード選択の例

▪ 特性評価

- ROC曲線のAUCを評価
  （1に近いほど良い判別アルゴリズム）
- Facebookのデータセットを利用
- 特定のアカウントにAEが集中するより現実的な攻撃シナリオを使用, さらに共通友人数を恣意的に増加

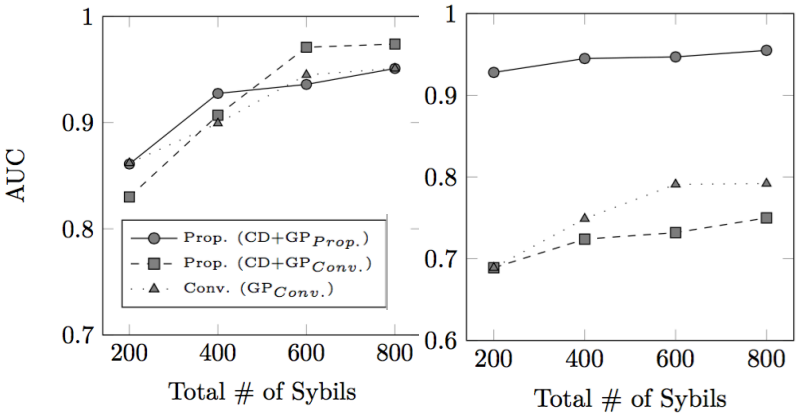


図3: Sybil数に対するAUCの変化
左が従来の攻撃シナリオ, 右がより現実的な攻撃モデル

- 従来の攻撃に対応しつつ, 共通友人数を増加させる高度な攻撃者に対しては従来方式に比べ大幅にAUCを改善

[1]Zhang et al. , Trust Management VIII, pp.77–92, 2014.

▪ 本研究の業績

[1] Shuichiro Haruta, Kentaroh Toyoda, and Iwao Sasase, “Trust-based Sybil nodes Detection with Robust Seed Selection and Graph Pruning on SNS,” IEICE Transactions Special Section on Internet Architectures and Management Methods that Enable Flexible and Secure Deployment of Network Services, May 2016 issue. (Under 2nd round review)
[2] Shuichiro Haruta, Kentaroh Toyoda, and Iwao Sasase, “Trust-based Sybil nodes Detection with Robust Seed Selection and Graph Pruning on SNS,” 7th IEEE Workshop on Information Forensics and Security, Rome, Italy, 19 Nov. 2015.

Traceroute パケットモニタリングによる Target Link Flooding Attack 防止システム

情報工学科 笹瀬研究室 平山貴之

背景

ボットネットを利用したDDoS攻撃が脅威となっている
インターネットのリンクを遮断する攻撃が報告されている
電力伝送，金融，政府のシステムが攻撃された場合の被害が深刻

問題点

- 攻撃フローが標的エリアに到達しないので対策が困難
- リンクの特性を利用した従来研究は，攻撃発生後でないと検知できない

提案手法

- 攻撃者がリンク調査に利用するパケットの増加を検知
- 自己回帰モデルで平常時のパケット数を基準にした特異性を計算

特性評価

- インターネットの形状を記録したデータセットで検知精度を評価
- 評価にはAUC (Area Under the ROC Curve)を利用
- AUC = 1.0 で完璧に攻撃検知
- 各ISP (Internet Service Provider) のAUCを計算

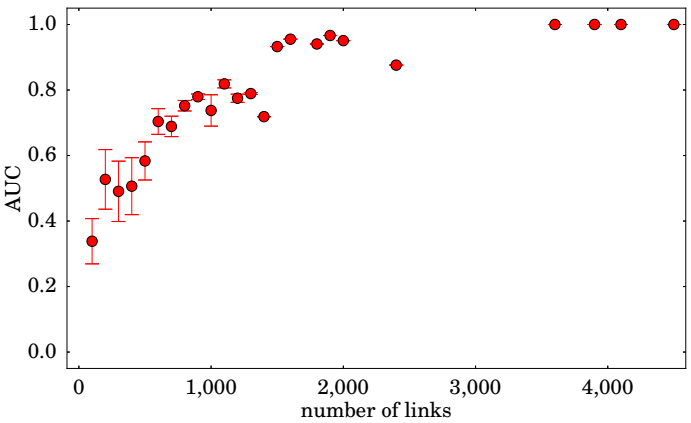


図1. ISPのリンク数に対するAUC

本研究に関する業績

[1] 平山貴之, 豊田健太郎, 笹瀬巌, “Traceroute パケットモニタリングによる Target Link Flooding Attack 防止システム,” 電子情報通信学会通信方式研究会(CS), 北海道, 2015年11月11日-13日

[2] Takayuki Hirayama, Kentaroh Toyoda, and Iwao Sasase, “Fast Target Link Flooding Attack Detection Scheme by Analyzing Traceroute Packets Flow,” in Proc. IEEE International Workshop on Information Forensics and Security 2015 (WIFS2015), Roma, Italy, 16-19 Nov. 2015

無線メッシュネットワークにおけるストリーミング配信の再生断を抑制する経路メトリック

情報工学科　笹瀬研究室　朝比奈　啓

■研究背景

災害直後の一時的な通信インフラとして無線メシュネットワークの利用が考えられます．

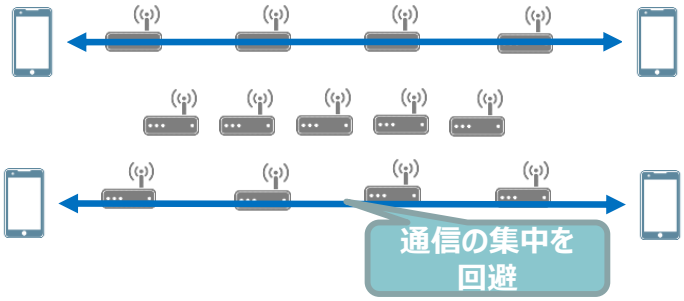
WMNsを用いることで，孤立した避難拠点間が，ライブストリーミングを用いて安否確認や情報共有などを行うことが可能となります．

WMNsでは，隣接する経路上の通信との干渉によってストリーミングの再生時に頻繁な一時停止が発生するため，適切な経路を選択するための指標が必要となります．

■提案方式

隣接する経路上の通信量を用いたメトリックを提案します．

通信量が少ない経路に隣接した経路を選択することで干渉によるスループットの変動を抑制することができます．



■結論

WMNsにおけるストリーミングの再生時の一時停止を抑制する経路メトリックを提案しました．

シミュレーション評価により，一時停止の原因となるスループットの変動量を抑制可能であることを示しました．

■従来研究

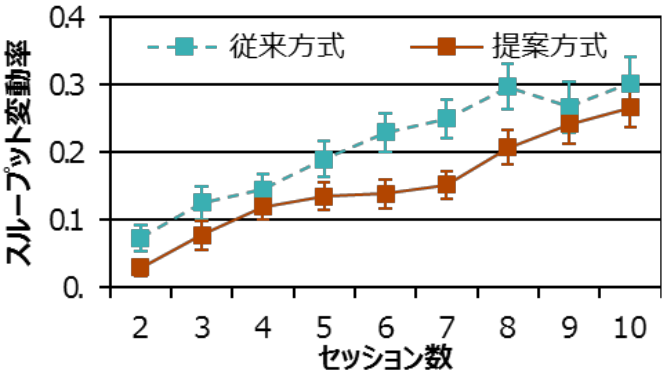
標準化資料内では，低遅延な経路を選択することを目的としたメトリックが規定されています．

低遅延な経路に通信が集中するため，一時停止の原因となるスループット変動量が増加するという問題があります．

■特性評価

従来方式と提案方式のスループット変動率を比較しました．

スループット変動率：セッション数が変化する前後のスループットの差であり，小さいほど変動が少ない．



セッション数に対するスループット変動率

■本研究に関する業績

[1] H. Asahina, H. Yamamoto, K. Toyoda and I. Sasase, “Path Metrics for Lower Throughput Fl-uctuation for Video Streaming Service in Wirel-ess Mesh Networks,” *APCC 2015, the 21st Asia- Pacific Conference on Communications (in pre-ss)*, 2015.

[2] 朝比奈 啓，山本 尚生，笹瀬 巌，“無線メッシュネットワークにおける他経路のスループット変動を抑制する経路メトリック，”電子情報通信学会技術研究報告，CQ2015-72, pp. 189-194, Sep. 2015.