ネットコミュニケーション研究部門活動報告

武藏 泰雄[†] 久保田 真一郎[†] 杉谷 賢一[†]

[†]熊本大学総合情報基盤センター・ネットコミュニケーション研究部

概要: 平成 24 年度におけるネットコミュニケーション研究部門における研究報告事項として無線 LAN 関係とネットワークセキュリティセキュリティ関係の二つがある。前者は、位置試問を用いた無線 LAN による屋内位置推定精度の向上についての検討であり、また、後者は、DNS クエリ通信監視によるネットワーク情報獲得を狙うホストドメイン名探索攻撃検知技術検討である。

1. 背景

無線 LAN アクセスポイント(AP)を用いた位置推定では、壁や床といった障害物等の環境によって推定精度が変化する. これらの環境を取り込むために位置指紋を使用して, 精度向上に検討を行った.

一方で, DNS サービスを利用し、学内の IP アドレスに対応するホストドメイン名をまとめて獲得するホスト名探索活動の検知技術について開発検討を行った.

2. 相関ルールにより生成された位置指紋を利用した無線 LAN 位置推定手法の検討

最尤法を用いた推定手法は減衰特性のモデル化を一度行うと環境と無関係に位置推定可能であるが, 壁や床といった障害物がある場合には推定精度が低下することが分かっている. 一方で, 位置指紋の手法では, その環境ごとに位置指紋を作成することで, 壁や床といった障害物の影響を考慮した位置推定を可能にする. 一方で, 壁や床の構造が変化するなど環境変化により位置指紋を再作成する必要があり, 運用コストが増えると予想される. このようにそれぞれの手法は一長一短である. 情報インフラとして無線 LAN のアクセスポイントが設置される場合, 測定位置とアクセスポイントとの間に障害物が存在するケースが多いことから, 本研究では障害物がある環境でも精度の良い位置指紋による位置推定手法について検討を行った. 近接性グラフを利用し位置指紋のノードを効果的に減らすことで推定精度を向上させる研究があるが, 今回は, RSS の平均値とその他測定される頻度の高い値も特徴量に含め, 位置指紋と定義し、測定頻度の高い値を抽出する手法として相関ルールを用いた, 今回の提案手法の効果を確認するために, NS-2 を用いて RSS の値をシミュレーションし, 平均値を利用した位置指紋を作成したのちに, 今回の提案手法である相関ルールにより特徴量を抽出し, 新しい位置指紋を作成した. 新しい位置指紋に精度を向上させる成果があるか, それぞれの位置指紋で位置推定を行った.

シミュレーションでは、5 個のノードを並べ, 図 1 のようにノード番号 0,1,27 に AP を配置した. Wallfish-Bertoni

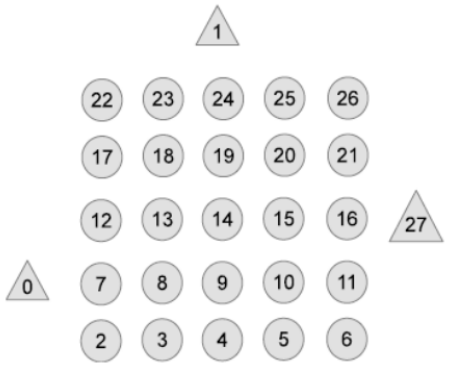

図 1 実験ノード配置図

が報告した式をシミュレーションで使用した.

$$P_r(d) = P_r(d_0) - \beta \log\left(\frac{d}{d_0}\right) + X$$

Pr (d0) は基準距離 d0 における RSS, β は距離減衰係数, d はアクセスポイントと測定ノードまでの距離, X は正規分布(平均 0, 標準偏差 σ)に従う乱数である. 簡単のため, 必要となるパラメータは β = 1.8, σ = 4 とした. これらの条件下に置いて, シミュレーションを行い, 各ノードにおいて受信される RSS の値を計算した. また AP から受信する RSS の値に関連して他の AP から受信する RSS の値が定まるような関係性が頻繁に起こるケースを使い, 位置指紋を構成する(相関ルール抽出). 相関ルール抽出には、R 言語の相関ルールライブラリ(arules)を用いた. ノードで受信される RSS の平均を利用する位置指紋を用いた場合の位置推定結果と前節にて提案した位置指紋を利用した場合の位置推定結果とを比較したる. 相関ルールによる位置指紋の生成について, 支持度の下限を 0.02 に設定し, 支持度が 0.02 より大きな値となる相関ルールに着目した. このとき, ノード 2 を条件とする相関ルールは 6 個であったが, 支持度の下限を 0.01 にすると相関ルールの数は 20 個に増える. このように支持度の下限の調整により採用される相関ルールの数は変化することから, その下限値の設定についても検討が必要と考えてられる. これらの結果は IOT20 で報告された[1].

3. DNS 通信監視によるホスト探索活動の検知技術開発研究

ホスト探索(HS)活動は，大学や企業などの大規模な組織のドメイン・ホスト名と IP アドレスの関連付けを行う DNS サービスに対して大量の逆引き DNS クエリを送り付け，組織内部のホスト名や IP アドレスに関する情報をまとめて引き出そうとするものである。この活動は、一日当たりデータセットについて，クエリキーワードと DNS クエリパケットの送信元 IP アドレスのエントロピーを測定することで、検出は可能であるが，HS 活動は短期間に迅速に行われることが多く、できるだけ速やかに検知して、その通信を遮断しなければならない．したがって，可能な限りリアルタイムで検知する必要がある．

この活動では、ユニークなクエリ IP アドレスについて逆引き DNS クエリパケットを大量に送り付ける特徴がある．すなわち IP アドレスはベクトル $\mathrm{qIP_i} = \{\mathrm{x_{ij}}\}$ として扱えるから，リアルタイム性を確保するため，現在のパケットと直前のパケットの 2 つの IP アドレスについてユークリッド距離 $\mathrm{ed}(\mathrm{qIP_i}, \mathrm{qIP_{i-1}})$ を計算し，その分布から

$$\mathrm{ed}(\mathrm{IP_i}, \mathrm{IP_{i-1}}) = \sqrt{\sum_{j=1}^{4/16} (\mathrm{x_{i,j}} - \mathrm{x_{i-1,j}})^2}$$

$$\mathrm{ed_{min}}(=1.0) \le \mathrm{ed}(\mathrm{qIP_i}, \mathrm{qIP_{i-1}}) \le \mathrm{ed_{max}}(=5.0)$$

ら得られた閾値を使用すれば検知が可能であることを以前報告した．今回は余弦距離 $\mathrm{cd}(\mathrm{qIP_i}, \mathrm{qIP_{i-1}})$ を使って

$$\cos\theta = \mathrm{cd}(\mathrm{qIP_i}, \mathrm{qIP_{i-1}}) = \frac{\mathrm{qIP_{i-1}^T} \bullet \mathrm{qIP_i}}{\left|\mathrm{qIP_{i-1}^T}\right| \left|\mathrm{qIP_i}\right|}$$

て 2 つのベクトルの比較を行い，その検知精度について検討を行った．HS 活動時の余弦距離の分布を図 2 に示す．これによって検知モデル使用する閾値が下記の通り得られる．

$$\mathrm{cd_{min}}(=0.73 \text{ or } 0.9) \le \mathrm{cd}(\mathrm{qIP_i}, \mathrm{qIP_{i-1}}) \le \mathrm{cd_{max}}(=0.9 \text{ or } 1.0)$$

この閾値を使用して検知スコアを計算し，その結果を図 3 に示している．比較のため同じデータセットについて，ユークリッド距離の場合と比較検討した．その結果，ユークリッド距離による検知スコア曲線においては，12 本の有意なピークが観察されたが、余弦距離の場合では，19 本のピークが観察された．これは，余弦距離もユークリッド距離と同様な結果を与えることを示している。しかしながら、余弦距離の値はユークリッド距離よりも HS 活動ない場合でもある程度の値を与えることから，ユークリッド距離の場合と比較してノイズも多くなっていると考えられ、検知結果の評価には注意が必要である．更に、新たに増加したピークについて送信元 IP アドレスについて調査したところ，活動の当初から分散している事実が観察された．

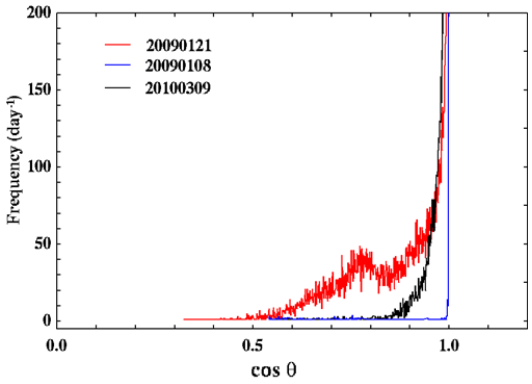

図 2 ホスト名探索活動における余弦距離の分布

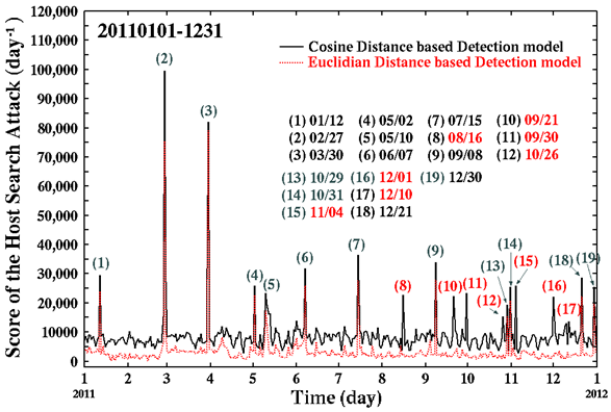

図 3 ユークリッド距離と余弦距離による HS 活動の検知スコア

4. 今後の展開

以上の研究結果から、無線 LAN の位置推定法に有用な位置指紋の作成に相関ルールが有用であることが示された．またホスト名探索活動において，余弦距離による検知モデルは，有用な結果を与えることが判った。

謝辞

上述の研究はすべて総合情報基盤センターの設備を使って行われた。熊本大学の教職員及び学生の皆様のご理解ご協力に心より感謝したい。

参考文献

[1] 久保田真一郎，石丸正人，杉谷賢一，相関ルールにより生成された FingerPrint を利用した無線 LAN 位置推定手法の検討，第 20 回インターネットと運用技術研究発表会，奈良，情報処理学会研究報告，Vol.2013-IOT-20, No.39, pp.1-4(2013)

[2] Nobuhiro Shibata, Yasuo Musashi, Dennis Arturo Ludeña Romaña, Shinichiro Kubota, and Keinchi Sugitani: Trends in Host Search Attack in DNS Query Request Packet Traffic, Proceedings of the Fifth International Conference on Intelligent Networks and Intelligent Systems (ICINIS 2012), Tianjin, China, pp. 126-129 (2012)