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 22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 関係と情報セキュリティ関係の二つがある。前者は、フェージング影響下における無線 LAN アクセスポイントからの受信信号強度を用いた位置推定手法の検討であり、また、後者は、DNS 通信監視によるホスト探索検知技術の開発研究である。

1. 背景

屋内では GPS による位置情報取得が困難であるため、センサネットワークや無線 LANのアクセスポイント(AP)を用いた位置情報を取得する技術の開発研究が行われている。センサネットワークを用いた研究の多くは位置情報を取得するためにセンサが理想的に配備された環境で行われる。しかしながら、情報通信基盤を目的として整備された APは、位置推定の対称となる PC から AP を見通すことができないなど、明らかにフェージングなどの影響を受けやすく、位置推定を行うには不利な環境となっている。そこで、フェージングなどの影響が大きいと考えられる既設 APを用い、位置情報を取得するシステムを構築する場合に必要と考えられる条件について考察を行った。

一方で、インターネット上の DNS サーバに対する攻撃の一種であり、攻撃対象としての組織ネットワークやクラウド内部のネットワークを事前調査するホスト探索(HS)攻撃が知られているが、その検知は一般に難しい。トラフィックエントロピーや単純なユークリッド距離検知モデル用いた検知手法では、ノイズなど原因によりファルスポジティブ(誤検知の一種)が起こることが知られている。このノイズを除去し、HS 攻撃の検知精度を向上させる技術開発の検討を行った。

2. 既設アクセスポイントを利用した屋内位置情報取得システムのための位置推定精度による分析

熊本大学には，学内利用者用に約 450 個のアクセスポイントが各所に設置され、多くの場所でネットワークを利用できる環境にある．我々はこれらの無線 LAN アクセスポイントから受信する受信信号強度を利用した PC 位置推定技術の検討に近年取り組んでいる。AP と PC 間のユークリッド距離 r と受信信号電力(RSSI: $A(r)$)の関係式は、実環境下、フェージングやシャドウィング等の $A(r)=10\log_{10}(Cr^{\alpha})$ 影響下では、である。C および α は最少二乗法により事前に決定されるパラメータである。実伝搬環境下の RSSI の確率分布は正規分布である(式 1)。

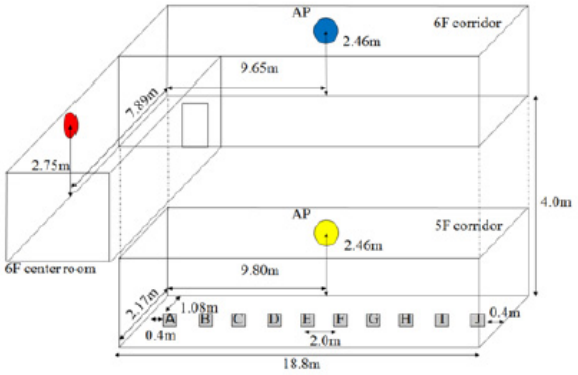

図 1 総合情報基盤センター測定ポイントの様子

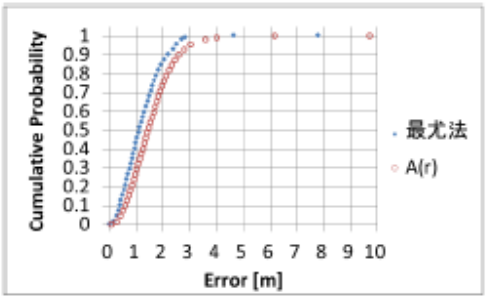

図 2 近似曲線および最尤推定法による推定誤差の累積確率

$$p(P_r \mid r)=\frac{1}{\sqrt{2\pi\delta^2}}\exp\left(-\frac{(P_r-A(r))^2}{2\delta^2}\right) \qquad (1)$$

P_r は実際に測定した RSSI、δ^2 は分散を表している。n 台の AP から PC が受信する電波強度のサンプル値 $\{Pr_i\}$ が与えられれば、条件付確率密度関数 $\Pi_{i=1}^{n}p(\mathrm{Pr}_i \mid \theta)$ が得られる。また θ を未知の母数とすれば、その尤度関数 $L(\theta)$ は、

$$L(\theta)=\Pi_{i=1}^{n}p(\mathrm{Pr}_i \mid \theta) \qquad (2)$$

と定義することができる。

まず式(1)の r を $(x,y,0.5\mathrm{m})$ に置換え、図 1 に示すように 2m 間隔に PC を配置して測定を行った。RSSI の測定には Network Stumbler と呼ばれるソフトウェアを利用し、各 PC で RSSI を 1 秒ごとに 30 分間測定し、近似

曲線 $A(r)$ によって C および α を決定した。次に、式(2)の θ を $(x, y, 0.5\mathrm{m})$ に置換え、最尤推定法により θ を決定した。その結果、図 2 に示すように近似曲線による推定結果の誤差および最尤推定法による推定結果の累積確率密度曲線が得られ、最尤推定法の有効性が示された。この結果は情報処理学会論文誌に掲載された[1]。

3. DNS 通信監視によるホスト探索攻撃の検知技術開発研究

ホスト探索(HS)攻撃は、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。この攻撃の従来の検知方法では、一日当たりデータセットについて、クエリキーワードの頻度や DNS クライアント送信元 IP アドレスの頻度についてトラフィックエントロピー解析を行えば、検出は可能である。しかしながら、HS 攻撃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、その攻撃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。

HS 攻撃の特徴は、ユニークな IP アドレスをクエリキーワードとして持つ、逆引き DNS クエリパケット通信用いるため、IP アドレスはベクトル $\mathrm{IP_i} = \{\mathrm{x_{ij}}\}$ として扱える。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 IP アドレスについてユークリッド距離 $\mathrm{d(IP_i, IP_{i-1})}$ (式(3))を測定することができる。

$$\mathrm{d(IP_i, IP_{i-1})} = \sqrt{\sum_{j=1}^{4/16} (\mathrm{x_{i,j}} - \mathrm{x_{i-1,j}})^2} \qquad (3)$$

HS 攻撃については、$\mathrm{d(IP_i, IP_{i-1})}$ の頻度分布が、1.0–5.0 (連続的、狭い範囲で一様分布または指数分布)または 150.2–210.4 (正規分布)になることが、調査の結果わかっている。したがって、$\mathrm{d(IP_i, IP_{i-1})}$ が、下記条件が満足された場合を検知とする。

$$\mathrm{IF}((1.0 \le \mathrm{d(IP_i, IP_{i-1})} \le 5.0) \,\mathrm{or}\, (150.2 \le \mathrm{d(IP_i, IP_{i-1})} \le 210.4))$$

検知された逆引き DNS クエリパケット数を積算してスコアとし、図 3 に 2010 年 1 月 1 日–12 月 31 日の期間の検知結果を示した。

図 3 では、HS 攻撃のスコアの変化が示され、31 個のピークが観察される。エントロピー変化を用いた場合のピーク数は 25 個であり、そのためユークリッド距離による検知結果には、ノイズ等によるファルスポジティブ(FP: 偽陽性)を含むことが考えられる。そこで、ユークリッド距離を用いた場合に新たに出現したピークについて調査したところ、学内ネットワークに存在するランダムスパムボットのメール送信活動が原因であることがわかった。したがって、これを除去するプリプロセッサを用い、HS スコアを計算し、その結果を図 4 に示した。その結果、29 個のピークが観察された。これらの結果は国際学会で公表された[2]。

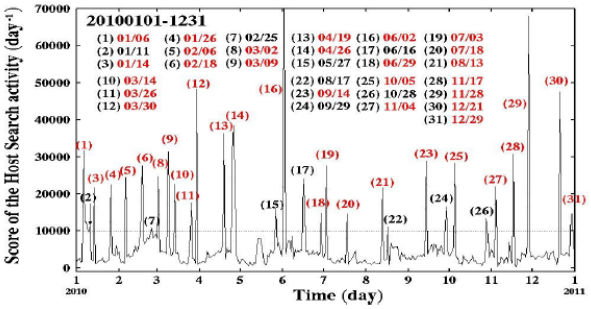

図 3 ホスト探索攻撃の検知スコア変化

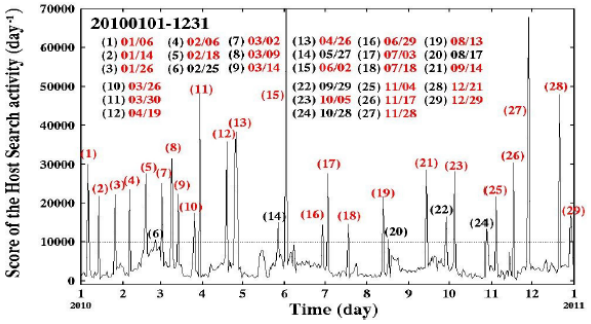

図 4 ノイズを除去した後の HS 攻撃のスコア

4. 今後の展開

以上の研究結果から、無線 LAN の位置推定法として最尤推定法が有効であることが、また、HS 攻撃のノイズとして攻撃先組織内にランダムスパムボットによるメール発信が原因の一つであることが判明した。

謝辞

我々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] 川村諒, 副島慶人, 久保田真一郎, 古川誠一郎, 杉谷賢一:, 既設アクセスポイントを利用した屋内位置情報取得システムのための位置推定精度による分析, 情報処理学会論文誌, Vol.53, No.3, pp.1357–1364 (2011)

[2] **Yasuo Musashi**, Florent Hequet, Dennis Arturo Ludeña Romaña, Shinichiro Kubota, and Keinchi Sugitani, "Detection of Host Search Activity in PTR Resource Record Based DNS Query Packet Traffic," *Proceedings of the Sixth International Conference on Information and Automation (ICIA2010)*, Harbin, Heilongjiang, China, pp. 1284–1288 (2010)