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 23 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、歩行者の往来の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 クエリ通信監視による Kaminsky 攻撃技術の開発研究である。

1. 背景

無線 LAN を用いた位置推定の研究は多く行われており，2.4GHz 帯を用いた位置推定については，無線 LAN に限らず，IEEE802.15.4 規格の無線センサネットワーク機器においても広く研究されている．IEEE802.15.4 規格の無線センサネットワーク機器を用いた研究において，歩行者がある場合に位置推定精度が向上するという研究結果が発表されており，同様の周波数帯で通信を行う無線 LAN で構築された情報インフラ環境であっても同様の結果が起こるか検証を行った．

一方で、インターネット上の DNS キャッシュサービスに対する攻撃のひとつに Kaminsky 攻撃がある。Kaminsky 攻撃では、短期間にユニーク正引 DNS クエリを大量に DNS キャッシュサーバへ送り付ける。そこで、Levenshtein 編集距離を用いて Kaminsk 攻撃を検知する技術の開発検討を行った。

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）。

$$p(P_r \mid r) = N(A(r), \delta^2) \quad (1)$$

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 $\{P_{ri}\}$が与えられれば、$\Pi_{i=1}^{n} p(\mathrm{Pr}_i \mid \theta)$ 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、

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

と定義することができる。

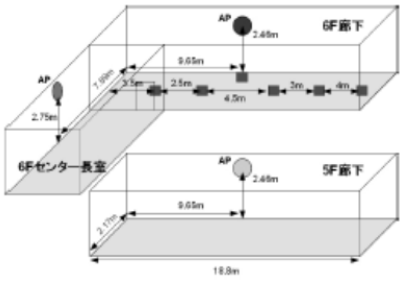

図 1 総合情報基盤センター測定ポイントの様子

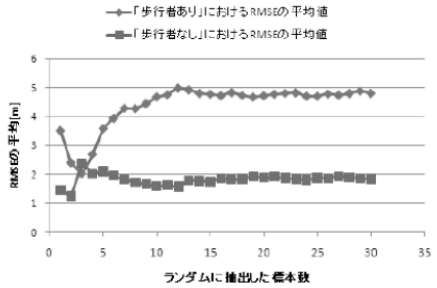

図 2 可視 AP における RSME 変化

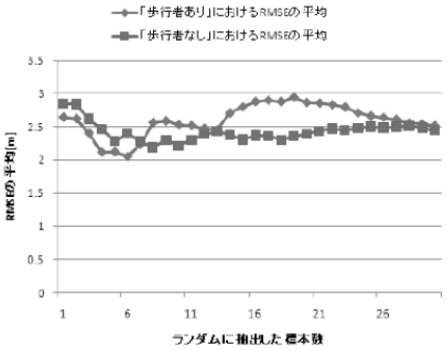

図 3 不可視 AP における RSME 変化

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、歩行者ありと歩行者なしについて RSSI の RSME の平均値を求め、更に測定 PC から見通せる「可視 AP」とそうでない「不可視 AP」との相違について考察したところ、可視 AP では、歩行者の影響があり、不可視 AP

では、歩行者の影響がすくないという結果が得られた。これらの結果は学術情報処理へ掲載された[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

Kaminsky 攻撃は、DNS キャッシュサービスに対して大量の正引き DNS クエリを送り付け、上位 DNS サーバへの再帰アクセスを起こし、DNS キャッシュデータを汚染する。この攻撃は、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、Kaminsky 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、できるだけリアルタイムで検知する必要がある。

Kaminsky 攻撃の特徴は、ユニークなドメイン名をクエリキーワードとして持つ、正引き DNS クエリパケット通信用いるため、文字列の編集距離を求める必要がある。リアルタイム性を確保するため、現在のドメイン名 X(=FQDN$_i$)と直前のパケットの各々のドメイン名 Y(=FQDN$_{i-1}$)について Levenshtein 編集距離 $\mathrm{LD}(\mathrm{X},\mathrm{Y})$ (式(3))を測定する。

$$\mathrm{LD}[x,y]=\min(\mathrm{LD}[x-1][y]+1,\mathrm{LD}[x][y-1]+1,\ \mathrm{LD}[x-1][y-1]+\mathrm{cost}) \quad (3)$$

式(3)における**x**と **y** は文字列 **X** と **Y** の長さである。エントロピー解析によって、2010 年 1 月 25 日−29 日の期間に、Kaminsky 攻撃を受けたことが判明している。従ってそれらの期間の 1 日分のデータセットについて Levenshtein 距離 $\mathrm{LD}(\mathrm{X},\mathrm{Y})=\mathrm{LD}(\mathrm{FQDN}_i,\mathrm{FQDN}_{i-1})$ を求め、それらの頻度分布を図 4 に示した。従って、下記条件が満足された場合を検知とする。

$$0\le \mathrm{LD}(\mathrm{FQDN}_i,\mathrm{FQDN}_{i-1})\le 40 \quad (4)$$

検知された正引き DNS クエリパケット数を積算してスコアとし、図 4 に 2010 年 1 月 1 日−12 月 31 日の期間の検知結果を示した。

図 4 では、Kaminsky 攻撃のスコアの変化が示され、9 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 4 個であった。この結果は、Levenshtein 距離用いて検知を行う場合ノイズを含むことを示すもの考えられるが、今後検討する必要があることが判明した。これらの結果は国際学会で公表された[2]。

4. 今後の展開

以上の研究結果から、無線 LAN の位置推定法において、歩行者の有無によって最尤推定法の結果に影響がある場合とそうでない場合があることがわかった。また、

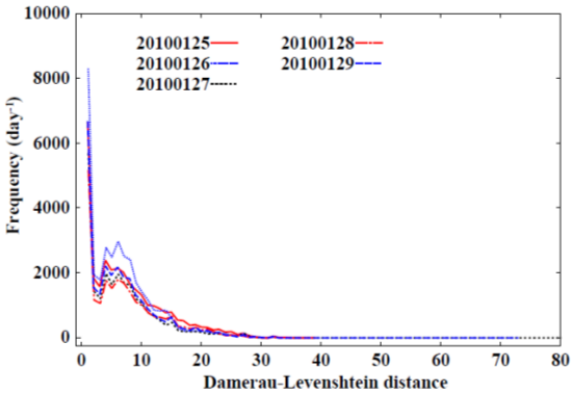

図 4 ホスト探索攻撃の検知スコア変化

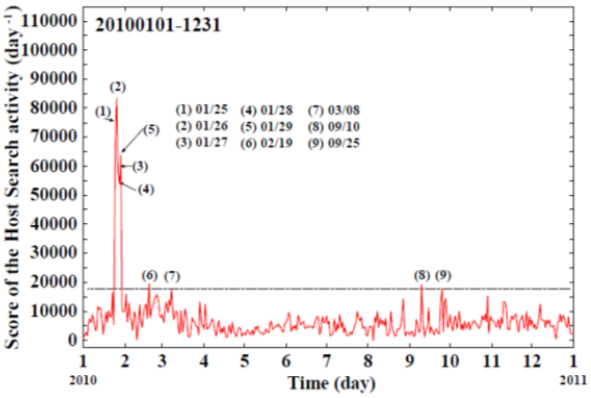

図 5 ノイズを除去した後の HS 攻撃のスコア

Kaminsky 攻撃の Levenshtein 距離によって検知できる可能性があることが示唆された。

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] 久保田真一郎, 副島慶人, 川村諒, 杉谷賢一, 武藏泰雄, 学内無線 LAN アクセスポイントを利用した位置推定における歩行者の影響について, 学術情報処理, No.15, pp.82−88 (2011)

[2] Yasuo Musashi, Masaya Kumagai, Shinichiro Kubota, and Keinchi Sugitani, "Detection of Kaminsky DNS Cache Poisoning Attack," *Proceedings of the Fourth International Conference on Intelligent Networks and Intelligent Systems (ICINIS 2011)*, Kunming, China, pp. 121−124 (2011)