社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DPS－128 (5)
2006－GN－ 61 (5)
2006－EIP－ 33 (5)
2006／9／14

モバイルネットワークにおける位置情報を考慮した安全性情報提示手法

田原 慎也[†] 東 雄介[†] 川口 信隆[†] 塩澤 秀和[‡] 岡田 謙一[†]

モバイルネットワークでは，ネットワークの安全性情報の取得が困難であるという問題がある．そこで我々はモバイルネットワークにおける安全性情報提供フレームワークの研究を行なっている．このフレームワークではネットワークに接続された個人端末に搭載されたIDSより，IDSログを収集，分析しネットワークの安全性を評価する．本論文ではこのフレームワークにおける安全性情報を視覚化し，ユーザが接続するネットワークの選択の手助けをする安全性情報提示手法を提案する．モバイルネットワークではユーザの移動が伴うため，本手法では安全性評価にあたって位置情報を考慮し，安全さと便利さを兼ね備えたモバイルネットワークの提示を行う．評価実験より，本手法における位置情報を考慮した安全性情報の妥当性，ユーザが接続するネットワークを選択する際の本手法の有用を示した．

Visualizing Security Information of Mobile Network considering Geographical Location

Shinya Tahara[†] , Yusuke Azuma[†] , Nobutaka Kawaguchi[†] ,
Hidekazu Shiozawa[‡] and Kenichi Okada[†]

One of the problems with mobile networks is the lack of safety information of the networks. To tackle these issues, we have carried out research on developing a framework to provide safety information of mobile networks. In our framework, the central server obtains IDS logs of the networks from IDS of individual user who actually use the networks. Then the server analyzes the condition of the networks from the logs and makes the safety information of the networks. In this paper, we propose a method to visualize the safety information of networks to help users select mobile networks that they are to use. Additionally, we add geographical location to the safety information because users often move around in mobile networks. Through results of the evaluation experiments, we show that our safety information considering geographical location is valid and that our method helped users select secure mobile networks.

1 はじめに

近年，モバイルネットワークの普及が急速に進んでいる．ホットスポット [1]，BBモバイルポイント [2] などといった様々な組織がモバイルネットワークのサービスに参入し，サービスの形態も多様である．しかし，モバイルネットワークではネットワークのセキュリティー面の情報や管理体制の情報が分かりにくいという問題がある．例えば，ネットワークの防御策の有無，監視体制といった情報が得られにくい．また，セキュリティの専門知識の無いユーザには，どのモバイルネットワークサービスを利用すれば安全であるかの判断がつきにくい．

我々は，ネットワークの管理体制に依存せずユーザに安全性情報を提供するフレームワークの研究を行っている [3] [4]．この安全性情報提供フレームワークでは，ネットワークに接続された個人端末に搭載されたIDSを用いて，ネットワーク上で行なわれている攻撃の情報を得る．そして、その情報をもとにサーバがネットワークの安全性をリアルタイムに評価する．様々な人からネットワークの情報を得るので，口コミ情報によるネットワークの安全性評価手法と言える．

本論文ではこの安全性情報提供フレームワークおける，安全性情報の視覚化に取り組んだ．モバイルネットワークではユーザの移動が伴うため，ユーザやモバイルネットワークのアクセスポイントの位置情報を考慮する必要がある．そこで，モバイルネットワークの位置情報

† 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
‡ 玉川大学工学部
Faculty of Technology, Tamagawa University

を考慮した安全性情報を電子地図上にマッピングし提示する手法を提案する．本手法では，安全性情報を直感的に分かりやすく提供することを目的とする．

本稿では，まず2章で既存の関連研究に触れ，3章で安全性情報提供フレームワークについて述べ，4章で位置情報を考慮した安全性情報提示手法を提案する．5章では本提案の実装について述べ，6章では評価実験について述べる．そして，7章は本論文のまとめとする．

2 関連研究

2.1 分散型IDS

分散型IDSは，様々な地点に設置されたIDSが協調して侵入を検知する方式である．我々が研究を行っている安全性情報提供フレームワークは分散型IDSの一種で，ネットワークに接続されている個人端末に搭載されたIDSから，IDSログを収集している．Stuart Staniford らは，ネットワーク上に設置された複数のIDSからログを収集し，解析することはDDoS攻撃などを早期検知するのに有効であると述べている [5]．この研究以来，分散しているファイアウォール，IDSを協調させることで、より高度な検知を実現する研究が多く行われている [6, 7]．

2.2 無線LANにおける位置情報サービス

吉田らは無線LAN情報のポータルサイトlock.jp [8] における位置情報サービスを提案している [9]．Lockyプロジェクトとは日本全国における無線LAN情報をユーザ間のコラボレーションにより収集し，それらの無線LAN情報を用いた位置推定システムの構築，および位置情報サービスの提供を目指しているプロジェクトである．しかし，この研究ではモバイルネットワークのセキュリティ面の考慮は行われていない．

3 安全性情報提供フレームワーク

我々はモバイルネットワークにおける安全性評価情報提供フレームワークの研究を行なっている [3] [4]．このフレームワークでは，モバイルネットワークに接続している個人端末に搭載されたIDSからIDSログを収集し，それを分析することでネットワークの状況を把握する．これにより，ネットワークの管理体制に依存せずにネットワークの安全性を評価することができる．

3.1 概要

図1にこのフレームワークの概要を示し，以下に手順を述べる．

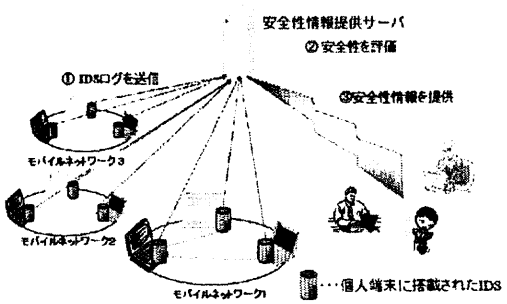

図 1: フレームワーク概要

1. モバイルネットワークに接続された個人端末が安全性評価サーバにIDSログを送信する．
2. 安全性評価サーバが送られてきたログを分析し，ネットワークの安全性を評価する．
3. ユーザはサーバへアクセスしてネットワークの安全性の情報を取得し，その情報をもとに接続するネットワークの選択を行う．

3.2 使用想定状況

本論文で提案する提示手法は，自宅のPCやモバイル機器からの閲覧することを想定している．例えば，ある場所でモバイルネットワークに接続したいとする．このときに，事前に自宅で本提案の提示手法で作られた地図を閲覧し，目的地周辺に設置されている信頼できるネットワークを調べておく．目的地ではどのネットワークが信頼できるかを調べる必要がなく，迅速に接続することができる．また，事前に周囲のネットワークの状況を把握していなくても，携帯電話などで本提案の提示手法で作られた地図を閲覧することにより，管理体制の分からないネットワークに繋ぐことのリスクを回避できる．

4 位置情報を考慮した安全性情報提示手法

本論文では3章で述べた本フレームワークにおける安全性情報を視覚化し，ユーザが接続するネットワークの選択の手助けをする安全性情報提示手法を提案する．モバイルネットワークではユーザの移動が伴うため，本手法では安全性評価にあたって位置情報を考慮する．

4.1 安全性情報

本手法で用いる安全性情報は4.1.1，4.1.2で述べる信頼度，推奨度である．信頼度はネットワークの管理体制

を評価する指標であり，推奨度はネットワークの信頼度とユーザが移動する距離を加味したネットワークの便利さを表す指標である．

4.1.1 信頼度

ネットワークに接続されている個人端末に搭載されたIDSから本フレームワークにおける安全性性評価サーバが収集したログからネットワーク上で行われている攻撃の情報を得て，その情報をもとにネットワークの信頼度を算出する．本論文ではプロトタイプとして，攻撃の種類ごとに点数を付けることでネットワークの信頼度を算出した．点数付けは表1のように行い，信頼度を10点からの減点方式で行なった．

表 1: 攻撃の種類と点数

パケットの種類点数	点数
脆弱性をついた攻撃	10
DDoS 攻撃	7
ウィルス対策ソフトなどで対策済みの攻撃	3
ポートスキャン	3

ネットワーク N_i 上で A_1，A_2 …，A_n の攻撃が行われているとき，ネットワーク N_i の信頼度 s_i は式1となる．

$$s_i = 10 - \sum_{i=1}^{n} P(A_i) \tag{1}$$

ここで，$P(A_i)$ は攻撃 A_i の点数を示す．また，信頼度が0未満になるときの信頼度は0とする．

この信頼度はネットワーク管理体制の信頼性を評価した指標である．ネットワーク上に多くの攻撃パケットが流れているほど，ネットワーク管理が不十分であると言え，この信頼度は低くなる．

4.1.2 推奨度

前述の信頼度，ユーザの位置，ネットワークのアクセスポイントの位置をもとに位置情報を考慮したネットワークの推奨度を算出する．この推奨度は，ユーザとアクセスポイントの距離が近く，信頼度が高いときに高くなる．ユーザの位置に対する推奨度が最も高いネットワークが，信頼性とユーザがネットワークスポットまで移動する手間のバランスが最も取れたネットワークと言える．ユーザがある地点 X にいるとき，周囲にあるモバイルネットワーク N_i の推奨度 R_i は，

$$R_i = \frac{s_i}{d_i^n} \tag{2}$$

となる．ここで，s_i はネットワークの信頼度，d_i は地点 X と N_i のアクセスポイントの距離，n は d_i の重みを表している．

4.2 安全性情報提示手法

4.2.1 RAB line

図2のように地点A，地点Bに信頼度がそれぞれ s_A，s_B のモバイルネットワークがある場合，地点Aからの距離 d_A と地点Bからの距離 d_B が $s_A{}^{\frac{1}{n}} : s_B{}^{\frac{1}{n}}$ になる地点にユーザがいる時，それぞれの推奨度 R_A，R_B は等しくなる．

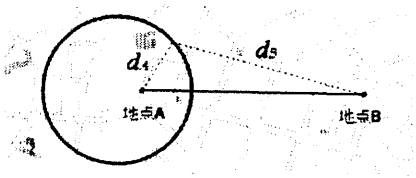

図 2: LAB line

この点の集合は図2の円のようになる．$s_A = s_B$ の時は垂直2等分線となる．この円上では $R_A = R_B$ となるので，この円は $R_A > R_B$ となる領域と，$R_A < R_B$ となる領域の境界線を示している．我々はこの境界線をRAB line(Recommended Area Border Line)と呼ぶことにする．RAB lineは，ある地点に対する推奨度が最大となるネットワークがどのネットワークであるかを示す．図2の例では，円の内側の地点にユーザがいる時は地点Aのネットワークの推奨度が最大となるので，このユーザに対しては地点Aのネットワークに接続する事を推奨する．円の外側にいるユーザに対しては地点Bのネットワークに接続する事を推奨する．

4.2.2 提示手法

本手法では，図3に示すように信頼度，RAB lineの安全性情報を地図上にマッピングする．

図3において，点A〜Hはモバイルネットワークのアクセスポイント，円はモバイルネットワークの無線の電波の届く範囲，円の色は信頼度を表している．本論文では，信頼度と円の色の信頼度10〜8は青，7〜5は黄，4〜0は赤に設定した．地図上に描かれている曲線はRAB lineである．前述の通り，RAB line上では隣り合う2つのネットワークの推奨度が等しくなるので，このRAB lineを境に，それぞれの地点における推奨度のもっと大きくなるネットワークが異なる．RAB lineによって区切られる，ある領域内にユーザが居るとき，同じ領域内にあるネットワークの推奨度がもっとも高く

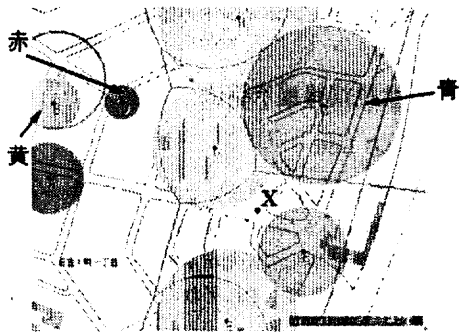

図 3: 安全性情報の提示

なる．よって，ユーザと同じ領域内にあるネットワークに接続することを推奨する．例えば，図 3 における地点 X にユーザが居る場合，地点 X を含む同領域内に設置されているネットワーク F に接続することを推奨する．このように，接続を推奨するモバイルネットワークを RAB line を用いて提示することにより，ユーザが接続するネットワークを選択する手助けをする．

5 実装

5.1 実装環境

実装にあたって，安全性情報提供サーバに CPU Pentium4 1.8GHz の PC，OS は Fedora Core 3 を用いた．また，ソフトウェアは MapSever 4.6 [10]，PostgreSQL 7.4，PostGIS 1.0 [11]，Java 2 SDK 1.4.2 を用いた．

5.2 処理の流れ

本提案手法を実装したシステムにおける構成要素および，処理の流れを図 4 に示す．

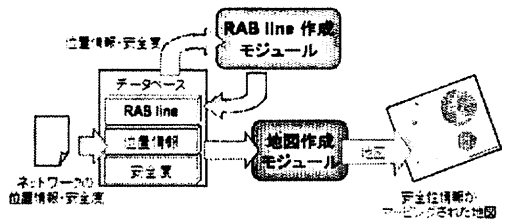

図 4: 処理の流れ

まず，モバイルネットワークのアクセスポイントの位置情報，推奨度，RAB line，電波の有効距離をデータベースに格納する．これらのデータは一定時間ごとに更新される．

そして，データベースの更新が行われるたびに，RAB line 作成モジュールは RAB line の計算を行い，その結果をデータベースに格納する．このとき，データベースからモバイルネットワークのアクセスポイントの位置情報（緯度，経度）と推奨度を取得し，隣り合う 2 つのネットワークの推奨度が等しくなる地点の位置情報を求める．この求めた地点の集合が RAB line となる．

地図作成モジュールは，ユーザからリクエストがあるたびにデータベースよりネットワークの位置情報，信頼度，RAB line のデータを取得し，それぞれのデータを地図上にマッピングする．そして，この地図をユーザに提供する．作成された地図は画像ファイルなので，携帯電話，PDA などのモバイル機器でも閲覧することが可能である．

5.3 実装画面

実装画面を図 5 に示す．本提案手法を実装したシステムは WEB ブラウザを用いて閲覧できる．地図に表示された安全性情報の見方は 4.4.4 で述べた通りである．また，図 5 の機能の欄のラジオボタンをクリックし機能を切り替え，地図上をクリックして地図の移動，拡大，縮小することが出来る．ネットワークリストの欄には，表示されている地図上にあるモバイルネットワークのリストを表示している．

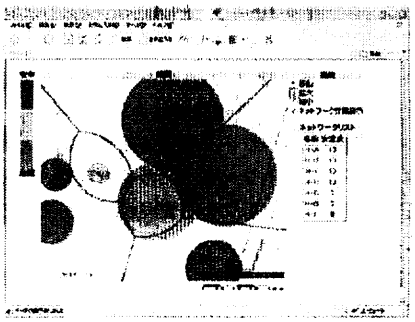

図 5: 実装画面

6 評価

4 章で述べた推奨度の算出に用いるパラメータ n の値を設定し，本提案手法の有用性を検証するために評価実験を行った．

6.1 評価 1

RAB line を描くために用いる推奨度の算出におけるパラメータの設定を行うために，評価実験を行った．

6.1.1 実験目的

推奨度を算出する式2において，nの値が$2, 1, \frac{1}{2}, \frac{1}{4}$と変化するとき，RAB lineは図6に示すように変化する．

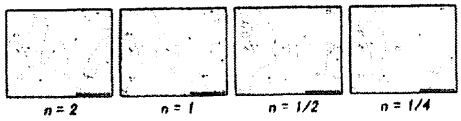

図 6: nの値によるRAB lineの違い

この評価実験より，ユーザの感覚に最も合うRAB lineを描くnの値を求める．

6.1.2 実験方法

図7のようなモバイルネットワークのアクセスポイントと各モバイルネットワークの信頼度を表示した地図を被験者に提示した．

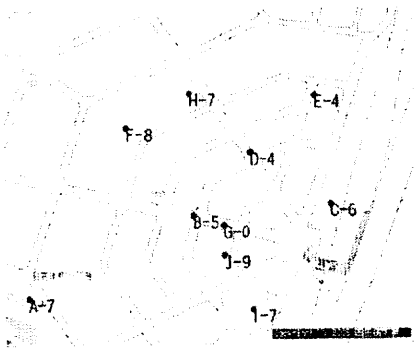

図 7: 実験1に用いた地図

ここで，図7におけるA〜Jはネットワークの名前，数字は信頼度を示している．実験では被験者に，地図上の様々な地点に居ることを想定してもらい，その地点からどのモバイルネットワークのアクセススポットまで移動し，接続したいかを選択してもらった．このとき，移動する手間と信頼性のバランスが取れていると感じるかを基準に接続したいネットワークを選択してもらった．用いた地図は，5パターン用意し，それぞれにおいて被験者の位置を4箇所指定した．アクセスポイントの位置と信頼度および被験者の位置はランダムである．そして，被験者の選択するネットワークとRAB lineで推奨されるネットワークの一致率が最も高い値を示すパラメータnを求めた．また，このnの値を求める実験の妥当性の検証をするために，別のパターンの地図を用いて同様の実験を行った．そして，先の実験で得られたnによって描かれるRAB lineで推奨されるネットワークと被験者の選ぶネットワークの一致率を求めた．それぞれの実験において被験者数は20名であった．

6.1.3 実験結果

RAB lineで推奨されるネットワークと，被験者の選択したネットワークとの一致した割合を図8に示す．

$n = 0.5$のときに一致率は71.8％となり最大となった．よって，$n = 0.5$と設定するのが妥当であると言える．

また，この実験の妥当性の評価結果，$n = 0.5$によって描かれるRAB lineで推奨されるネットワークネットワークと被験者の選んだネットワークの一致率は74.2％となった．この実験でも，先のnの値を求める実験結果の$n = 0.5$のときの一致率と近い値が得られた．この結果より，先の実験より得られたnの値は妥当であると言える．

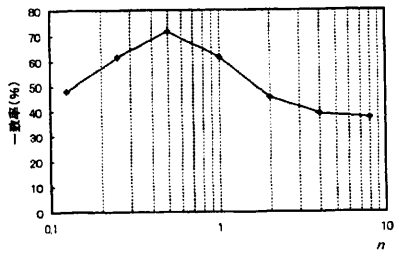

図 8: 実験1の結果

6.2 評価2

RAB lineの有用性を検証するために評価実験を行った．

6.2.1 実験目的

本提案手法では地図上にRAB lineを描くため，地図が見にくくなる可能性がある．目的地の地形，周辺情報を知る，道を調べるといった，地図の本来の機能を損なっては，RAB lineは有用であるとは言い難い．この実験により，以上のことを検証し，RAB lineの有用性を評価した．

6.2.2 実験方法

RAB lineのある場合，ない場合の地図を被験者に提示し，被験者に実験1と同様に接続したいモバイルネットワークを選択してもらった．このとき用いた地図は8パターンで，それぞれ2箇所の計16箇所に居ることを想定した場合で行った．そして，アンケートで以下の項目について5段階評価をつけてもらった(5：とてもそう思う〜1：全くそう思わない)

- RAB lineが有るときのネットワークの選びやすいか
- RAB lineが無いときのネットワークの選びやすいか
- RAB lineが必要と感じたか
- RAB lineによって推奨されたネットワークは妥当だと感じたか
- 地図は見やすかったか

本実験に用いた地図におけるネットワークの位置，推奨度および被験者の所在地は前実験同様にランダムである．この実験において被験者数は20名であった．

6.2.3 実験結果

この実験でのアンケート結果を表2に示す．

表 2: 実験2結果

ネットワークを選びやすいか	RAB lineが有るとき	4.8
	RAB lineが無いとき	2.1
RAB lineが必要と感じたか		4.9
推奨されたネットワークは妥当だと感じたか		4.5
地図は見やすかったか		4.3

この表2を見てわかるように，ネットワークの選びやすさは，RAB lineが無いときよりも，有るときのほうが選びやすいという評価を得ることが出来た．また，ほとんどの被験者がRAB lineが必要であると感じたことがわかった．そして，推奨されたネットワークは妥当であると感じている．よって，RAB lineはモバイルネットワークにおいて接続するネットワークを選択する際に有用であるということが言える．さらに，ほとんどの被験者が，地図を見やすいと感じていた．以上のことより，地図にRAB lineを加えても邪魔にならず，地図の機能を損なうことなく推奨するネットワークを提示できると言える．

7 まとめと今後の課題

モバイルネットワークの発展に伴って，モバイルネットワークの安全性の問題が重要になってきている．しかし，安全性情報を得ることが出来ないのが現状である．そこで，我々はモバイルネットワークの管理体制に依存せずユーザに安全性情報を提供するフレームワークの研究を行っている．本論文ではこの安全性情報提供フレームワークにおける，安全性情報の視覚化に取り組んだ．

モバイルネットワークではユーザの移動が伴うため，ユーザやモバイルネットワークのアクセスポイントの位置情報を考慮する必要がある．そこで，モバイルネットワークの位置情報を考慮した安全性情報を地図上で提示する手法を提案した．本手法では，安全性情報を直感的に分かりやすく提供することを目的とした．評価実験より，推奨度の算出に用いるパラーメータは$n = 0.5$のときに最もユーザの感覚に合致することが分かった．また，本提案手法は有用であるということがわかった．

今後の課題としては，提示する安全性情報をさらに洗練させること，本論文で実装したアプリケーションの発展などがあげられる．これらの点の研究を進めることにより，さらに洗練されたRAB lineを描くことが出来ると考える．そして，今回，実装を行ったアプリケーションにＧＰＳと連動させ，ユーザの実際の位置とその周辺のモバイルネットワークの状況を表示可能にし，より実用的なアプリケーションを目指す．

謝辞

本研究は，ＡＳＦ（応用セキュリティフォーラム）の支援のもとで行われた．ここに記して謝意を表す．

参考文献

[1] ホットスポット．
http://www.hotspot.ne.jp/.
2006年7月7日確認．

[2] BBモバイルポイント．
http://www.so-net.ne.jp/ap/mobilepoint.html.
2006年7月7日確認．

[3] Yusuke Azuma, Naohiro Obata, Nobutaka Kawaguchi, Hidekazu Shiozawa, Hiroshi Shigeno and Kenichi Okada. Providing security information of mobile networks using personal ids. FIT2005, pp. 281-282, Sep 2005.

[4] Nobutaka Kawaguchi, Yusuke Azuma, Shinya Tahara, Hidekazu Shiozawa, Hiroshi Shigeno and Kenichi Okada, CMSF: Cooperative Mobile Network Security Information Distribution Framework, in Proc. of The 3rd International Conference on Mobile Computing and Ubiquitous Computing, to appear, 2006.

[5] Stuart Staniford. Vern Paxon and Nicholas Weaver. How to own the internet in your spare time. in Proceeding of 11th USENIX Security Symposium, Aug 2002.

[6] Vinod Yegeswaran Paul Barford and Somesh Jha, Global Intrusion Detection in the DOMINO Overlay System, in Proceeding of NDSS'04, 2004.

[7] M.Locasto, J.Parekh, S.Stolfo, A.Keromytis, T.Malkin and V.Misra. Collaborative Distributed Intrusion Detection.Tech Report CUCS-012-04,2004.

[8] Locky Project.
http://locky.jp Blast.html.2006年7月7日確認．

[9] 吉田廣志, 伊藤誠悟, 河口信夫. 無線LANを用いた測位ポータル locky.jpにおける位置情報サービス. 情報処理学会シンポジウム論文集, pp.61-62, Nov 2005.

[10] Mapserver.
http://mapserver.gis.umn.edu/.2006年7月7日確認．

[11] Postgis.
http://www.postgis.org/.2006年7月7日確認．