Vol.2015-HCI-165 No.7
Vol.2015-UBI-48 No.7
2015/11/29

無線 LAN アクセスポイントを活用した犯罪捜査支援システム

古賀康明[†1]　富樫宏謙[†2]　古川浩[†2]

概要：現在，街中では落書き，万引き，ひったくり，誘拐など様々な問題が生じている．本研究では防犯カメラを搭載した無線 LAN アクセスポイントを多数用いて，こうした犯罪行為に対する捜査を支援する”Criminal Fishing システム”を提案する．提案手法では，犯行時の監視カメラ画像と犯人が保有する携帯端末の発するプローブリクエスト信号(電波指紋)ならびにその受信強度により，事件の犯人の端末の MAC アドレスを推定する．実験の結果，プローブリクエスト数のみを用いたフィルタリングで犯人の所有する端末を 10 回中 5 回，それに加え RSSI(受信強度)を絞込みに利用することで 10 回中 10 回すべてにおいて犯人の端末を特定することができた．

キーワード：防犯監視システム，Criminal Fishing，Wi-Fi，MAC アドレス

Criminal Fishing system based on Wireless LAN Access Point

YASUAKI KOGA[†1]　HIROAKI TOGASHI[†2]　HIROSHI FURUKAWA[†2]

Abstract: Nowadays, there are many incidents such as graffiti, theft and kidnapping. In this paper, we propose a novel system for criminal identification assistance that utilizes a large number of wireless LAN access points with a security camera. We call it “Criminal Fishing system” that estimates the MAC address of the criminal’s mobile device, from probe request signals and their RSSI (Received Signal Strength Indicator). Results of experiments was such that our Criminal Fishing system has identified the criminal’s device 5 out of 10 times by filtering the gathered probe request signals only using their appearance frequency, and 10 out of 10 times by additionally using their RSSI on the filtering.

Keywords: Surveillance System, Criminal Fishing, Wi-Fi, MAC Address

1. はじめに

近年，スマートフォンやタブレットの普及によるトラフィック量の爆発的な増加に伴い，Wi-Fi オフロードの必要性が高まっており，多数の Wi-Fi AP（アクセスポイント）が街中などに設置されるようになっている．本研究ではこれらの AP を用いた犯罪捜査支援機能の実現について検討する．現在，街中では落書き，万引き，ひったくり，誘拐など様々な問題が生じている．例えば，落書き消しにかかる費用は大きいもので 10～20 万円程度[1]，小売業事業所の推定万引き被害総額は 4615 億円（平成 21 年度）[2]である．多数設置された Wi-Fi AP を利用し，犯罪捜査支援機能を提供することが可能となれば街の治安向上に役立つのではないかと考えている．

本稿にて提案する”Criminal Fishing システム”は，カメラ画像に加え，Wi-Fi AP を用いてカメラの周囲に存在する端末の MAC アドレスも収集し，事件などが発生した際には蓄積した情報をもとに容疑者の所有する端末の MAC アドレスを特定することで犯罪捜査を支援するシステムである．

本稿の以降の構成は以下のとおりである． 2 章にて本研究の背景について述べ，3 章にて Criminal Fishing システムの概要および容疑者の MAC アドレスを特定するアルゴリズムについて述べる．4 章では実験による検証結果を示す．最後に，本稿のまとめと今後の研究方針について述べる．

2. 研究背景

2.1 既存の防犯システムの問題点

防犯設備として一般的な監視カメラではカメラの映像を保存し，犯罪行為を記録する[3]．しかし各カメラを有線接続するシステムの場合, 敷設コストに莫大な費用がかかる．また，映像データだけでは顔を隠して犯行に及ぶ犯人等は特定できない．いまや過半数の国民がスマートフォンを所有しており[4]，これらの端末は Wi-Fi 機能を有効にしている場合，AP を探索するための Probe Request 信号を発信している．この Probe Request 信号には各端末固有の MAC アドレスが含まれていることから，本稿ではこれを電波指紋と呼ぶ．我々はこの電波指紋に着目し，Probe Request 信号を捕捉する機能を実装した AP と Web カメラをセットにした防犯監視システムの研究を行っている．

2.2 PCWL-0200

PCWL-0200 は当研究室で開発した無線バックホール機能を持つ無線 LAN-AP である．様々な場所に設置された PCWL-0200 は無線バックホールによる広大な無線 LAN エリアを構築するとともに，携帯端末が発する Probe Request 信号を捕捉する．Probe Request 信号を解析することで，端

†1 九州大学大学院 システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University

†2 九州大学大学院 システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

末の MAC アドレスと RSSI(Received Signal Strength Indication)を取得する．これに自身の MAC アドレスとタイムスタンプを付加して，10 秒間バッファに蓄えた後，サーバへ送信する．

2.3 Probe Request

Probe Request は Wi-Fi 対応端末が周囲の AP を探索するため，および PNL(Preferred Network List)に保存された ESS-ID(Extended Service Set Identifier)を持つ AP に対して接続要求を行うために送信される信号である．Wi-Fi 端末が AP との接続を確立する手順には，前述の Probe Request を送信して AP から返送される Probe Response を受け取る Active Scan と，AP から恒常的に送信され続ける Beacon を利用する Passive Scan の 2 通りがあり，スマートフォンはより迅速に接続を確立できる Active Scan を行うため不定期に Probe Request を送信している．Wi-Fi 端末が Probe Request を送信する間隔は端末の接続状態や機種，OS，稼働しているソフトウェア等によって様々であり，およそ数秒～数分間である．一般に AP と未接続でかつ画面が ON の状態のとき，最も頻繁に送信する．

Probe Request が含む情報は主に以下のものである．

- 送信元 MAC アドレス
- RSSI
- ESS-ID（明示的に指定する場合）

3. Criminal Fishing システム

3.1 システムの概要

提案する Criminal Fishing システムは，カメラの画像に加え電波指紋を活用して容疑者特定の手がかりを得る犯罪捜査支援システムである．電波指紋を取得するための AP として PCWL-0200 を，画像の取得には Pandaboard[5]に接続した USB カメラをそれぞれ用いる．PCWL で取得した電波指紋とカメラで撮影した画像は，タイムスタンプを印加したうえでサーバへ伝送し保存される．犯罪の発生時には，Criminal Fishing システムのユーザ（管理者など）が画像を確認して犯行時間を突き止め，システム側でその時間帯に観測された電波指紋をフィルタリングし，犯人のものと疑われる電波指紋を抽出する．後にどこかの PCWL で当該の電波指紋が検出されれば，カメラ映像により犯人と疑われる人物の顔を把握することが可能となり，円滑な犯罪捜査に貢献できる．

3.2 システムの構成

図 1 に Criminal Fishing システムの構成を示す．主な構成要素は，処理サーバ，PCWL-0200，そして USB カメラを接続した Pandaboard である．本研究では，画像取得プログラムの動作が PCWL-0200 に与える負荷影響が大きいため，Linux をインストールした Pandaboard 上でカメラを起動させ，画像の取得を行っている．Pandaboard は各 PCWL と 1 対 1 に対応させ，同じ場所に設置する．

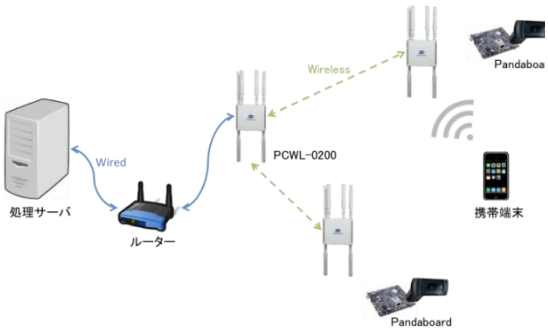


図 1　全体的なシステム構成
Figure 1 Outline of the Criminal fishing system

各 PCWL は定期的に Probe Request 信号を捕捉し，無線 LAN 端末の MAC アドレスと RSSI を電波情報としてサーバへ送信する．各 Pandaboard は画像取得プログラム”motion”を実行，カメラでの動体検知時に画像を取得し，PCWL 経由でサーバへ送信する．サーバに送信された電波情報や画像はデータベースへ書き込まれて保管される．保管された情報から容疑者の所有する端末を特定するため，サーバには Web アプリケーションを実装した．管理者は Web アプリケーションを用い，取得した画像を見て犯行を確認し，犯人がその場に滞在した時刻を入力する．その時刻を元にサーバ上で処理を行い，容疑者の所有する端末の MAC アドレスを特定する．

このようにして MAC アドレスを特定することで，仮に犯行現場で犯人の画像が得られなくとも，別の場所，日時で容疑者の画像を得ることができる．具体的には，前述の犯行現場で採取された容疑者の MAC アドレスを繁華街など複数の場所で監視し，当該の MAC アドレスが捕捉されれば，その時のカメラ映像より端末の所有者，すなわち容疑者の撮影画像が取得できる．AP を広範囲に，高い密度で設置することで，より一層容疑者特定の可能性を高められる．

以下では，容疑者の所有する端末の MAC アドレス特定の手法について説明を行う．

3.3 容疑者特定アルゴリズム

3.3.1 アルゴリズムの概要

ここでは，PCWL によって収集された MAC アドレスから，容疑者の端末の MAC アドレスを特定するアルゴリズムについて述べる．PCWL は容疑者が所有する端末のみならず，その他の端末の Probe Request 信号も捕捉するので，容疑者の端末の MAC アドレスを特定するにはその他の端末の MAC アドレスを除去する必要がある．その他の端末は，1) 移動せずにその場に滞在し続ける端末，2) カメラに写っておらず犯人から少し離れた場所にいる人の端末，3) 犯人と一緒にカメラに写っている人の端末に分類される．

まず，1) 移動せずにその場に滞在し続ける端末の除去に

ついて考える．これらの端末は時間によらず PCWL で常に観測されるのに対し，犯人の端末はその場から移動するためいずれは観測されなくなる．したがって，カメラ画像により犯人がその場にいた時間を把握し，犯人の不在時間に観測された MAC アドレス群を犯人の滞在時間に観測した MAC アドレス群から取り除くことで 1) の端末を除外することができる．

次に，2) カメラに写っておらず犯人から少し離れた場所にいる人の端末の除去について考える．カメラに写っていない場合，例えば路上の PCWL であれば路地裏にいる人の端末を，建物内の PCWL であれば別の部屋・通路にいる人，もしくは階上・階下にいる人の端末を検出しているケースが考えられる．いずれも PCWL からは障害物を挟んで離れた場所に存在しており，当該端末が発する電波の RSSI がカメラに写っている犯人の端末より低くなるので，観測された RSSI の最高値に閾値を設けることによって，これらの端末を取り除くことができる．

次に，3) 犯人と一緒にカメラに写っている人の端末について考える．これは更に 3-1) 他の PCWL エリアでは犯人と異なる行動をとる人の端末，3-2) 他の PCWL エリアでも犯人と同じ行動をとる人の端末に細分化される．3-1) の他の PCWL エリアでは犯人と異なる行動をとる人の端末については，空間的に分散配置された複数の PCWL において，それぞれの PCWL で犯人が滞在した時間帯に観測した MAC アドレスリストを抽出し，全ての PCWL に共通して存在しない MAC アドレス群を取り除くことで除外することができる．

最後に 3-2) 他の PCWL エリアでも犯人と同じ行動をとる人の端末についてであるが，現時点では除去されずに残ることが多い．犯人と一緒に行動する人は共犯者や被害者など犯人と関わりのある人物である可能性が高く，これらの電波指紋は犯人特定に有益な情報であるため，除去する必要性は低いと考えられる．もし第 3 者の端末が検出されてしまった場合にも，後日街中で当該 MAC アドレスを検出した際にカメラで容姿を確認し，犯行時のカメラに写っていた第 3 者と認識できれば，これを除去することが可能である．

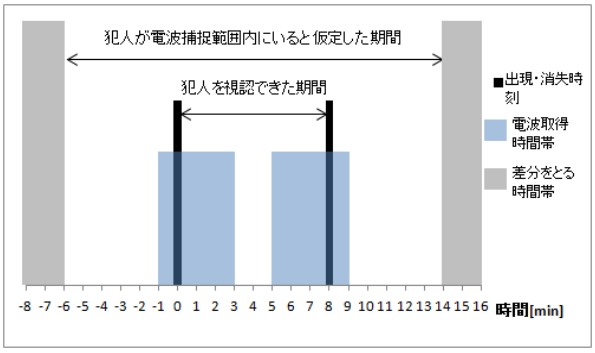


図 2　電波取得時間の説明

Figure 2 Definition of signal acquisition duration

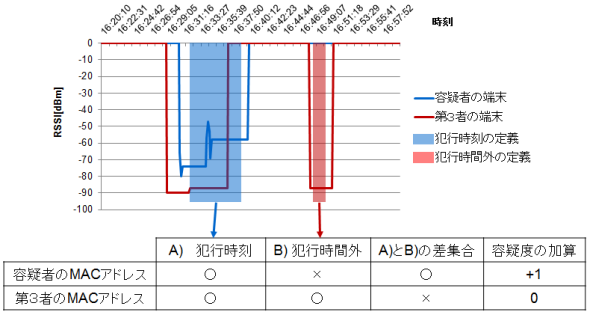
3.3.2 重み付けフィルタリング

本研究では，容疑者の端末の MAC アドレスを特定する手法として「重み付けフィルタリング」手法を提案する．重み付けフィルタリングでは，まず 1) 移動せずにその場に滞在し続けている端末を除去するために，犯人滞在時間に検出された MAC アドレスと犯人不在時間に検出された MAC アドレスとの差分を取る．管理者がカメラの画像群から犯人の出現および消失の瞬間を捉えた画像を選択すると，それらの画像のタイムスタンプが重み付けフィルタリングの入力値となる．図 2 に示す通り出現時刻と消失時刻付近それぞれ 4 分間に取得した MAC アドレスを照合し，共通して存在する MAC アドレスを犯人滞在時間の MAC アドレスの集合とする．前述のとおり端末が Probe Request 信号を発信する間隔は一定ではないので，犯人の電波指紋を捕捉する可能性を高めるために各 4 分の時間を設けている．差分をとる時間については，出現時刻の 66〜6 分前および消失時刻の 6〜66 分後（それぞれ 1 時間の範囲）としている．

1) の移動せずにその場に滞在し続ける端末は，電波強度によっては検出されたりされなかったりする．本手法では，前後合わせて 2 時間の犯人不在時間を 1 分ずつ分割し，犯人滞在時間に観測された各 MAC アドレスが犯人不在時間の各 1 分間に観測されなかった回数を容疑度として記録し，閾値を上回った MAC アドレスのみを抽出することでこれらの端末を除去する．ここで閾値は最大値の 9 割としている．

本手法ではさらに，図 2 に示した犯人が電波捕捉範囲内にいると仮定した期間における RSSI の最大値もフィルタリングに用いる．これにより 2) のカメラに写っておらず犯人から少し離れた場所にいる人の端末を除外する．

以上の処理を全ての PCWL で行い，全ての PCWL で容疑度が閾値を上回った MAC アドレスに対し容疑度の合計を求め，MAC アドレスと容疑度の対応表を結果として出力する．これにより 3-1) の他の PCWL エリアでは犯人と異なる行動をとる人の端末が除外される．容疑度という指標を与えることで，複数の MAC アドレスが検出された際



	A) 犯行時刻	B) 犯行時間外	A)とB)の差集合	容疑度の加算
容疑者のMACアドレス	○	×	○	+1
第3者のMACアドレス	○	○	×	0

図 3　容疑度の付加

Figure 3 Calculation of suspicious rate

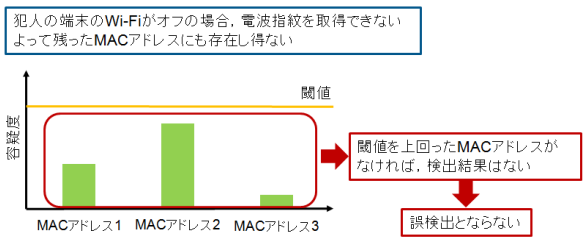


図 4　犯人の端末の Wi-Fi がオフの場合の閾値判定

Fig 4 Threshold mechanism when criminal's device with Wi-Fi function off

に，どの MAC アドレスが最も犯人のものである疑いが強いかを管理者が判断することを可能としている．

犯人の端末の Wi-Fi がオフの場合，および犯人が Wi-Fi 端末を所持していない場合には，図 4 が示すように第 3 者の MAC アドレスの容疑度が閾値を下回っていれば容疑者として検出されない．よって，本手法は第 3 者の誤検出を防ぐ仕組みを備えている．

3.3.3 RSSI を用いたフィルタリング

2) のカメラに写っておらず犯人から少し離れた場所にいる人の端末を除外するため，本手法では Probe Request 信号の RSSI を利用する．具体的には，犯人が PCWL 付近にいた時間帯の RSSI 最大値がある閾値を上回った MAC アドレスを抽出の対象とする．ここでは RSSI の閾値を -70dBm としている．-70dBm は障害物のない直線距離で 20m ほど離れた端末の電波強度であり [6]，常に -70dBm を下回っていればカメラに写る領域には存在しないと考えられるからである．

3.3.4 アルゴリズムの詳細

表 1　連想配列T_0の例

Table 1 Example of associative array T_0

MAC Address	容疑度	RSSI[dBm]
MAC Address 1	120	-49
MAC Address 2	50	-78
MAC Address 3	113	-64
MAC Address 4	84	-79
MAC Address 5	119	-80

表 2　表Tの例

Table 2 Example of table T

検出 MAC Address	容疑度			合計
	PCWL-1	PCWL-2	PCWL-3	
MAC Addr. 1	120	120	115	355
MAC Addr. 2	113	110	115	338

以下，重み付けフィルタリングの詳細を述べる．まず犯人を観測した PCWL の集合を P とし，その要素数を m (> 1)，犯人を観測した各 PCWL を p_i ($i = 0, 1, \ldots, m-1$) $\in$ P，PCWL p_i がある時刻 t_0~t_1 に観測した MAC アドレスの集合を $l_{\{p_i,t_0,t_1\}}$ とする．まず，PCWL p_0 のカメラが最初に犯人を確認した時刻 $t = t_0$ と最後に確認した時刻 $t = t_1$ に，それぞれ観測した MAC アドレスの集合 $l_{\{p_0,t_0-1,t_0+3\}}$ と $l_{\{p_0,t_1-3,t_1+1\}}$ を取得し，共通する項を犯人滞在時刻の MAC

表 3　表記法

Table 3 Notation of the flowchart

m	犯人を観測した PCWL 数
p_i	犯人を観測した PCWL ($i = 0, 1, \ldots, m-1$)
$l_{\{p_i,t_0,t_1\}}$	p_i が時刻 t_0 から t_1 までの間に観測した MAC アドレスの集合
$d_{\{p_i,n\}}$	ある時刻の MAC アドレスの集合と，別の時刻の MAC アドレスの集合との差集合
B	各 PCWL における犯人滞在時刻の MAC アドレスの集合
T_i	PCWL p_i における処理結果の連想配列

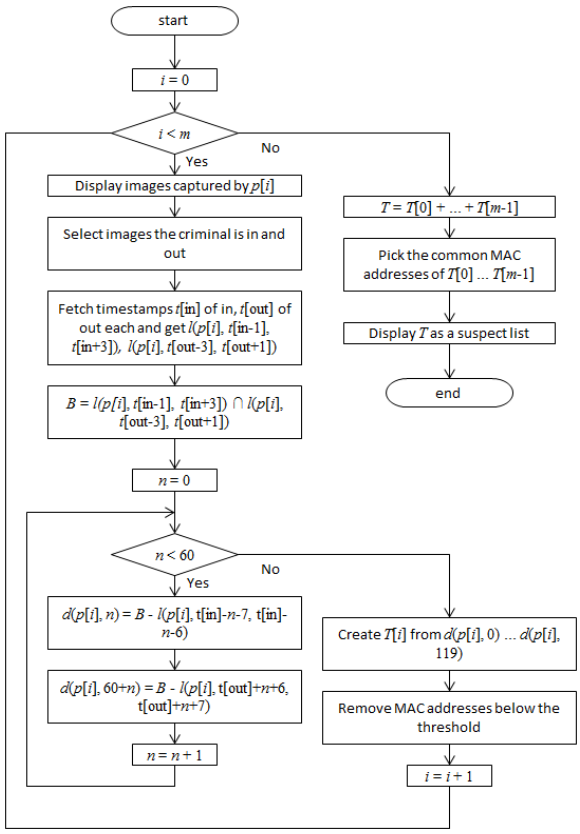


図 5　重み付けフィルタリングのフローチャート

Figure 5 Flowchart of the weighted filtering of probe request signals

アドレス群 B とする．次に犯人不在時刻における MAC アドレスを取得する．まず消失時刻から 6 分後を開始点として，$t_n = t_1 + 6 + n$ $(0 \leq n < 60)$から 1 分後までに観測した MAC アドレスの集合$l_{\{p_0,t_n,t_n+1\}}$を取得し，同時に出現時刻の 6 分前を開始点として，$t_{n+60} = t_0 - 6 - n$ $(0 \leq n < 60)$から 1 分前までに観測した MAC アドレスの集合$l_{\{p_0,t_{n+60}-1,t_{n+60}\}}$を取得する．そして，集合 B と集合$l_{\{p_0,t_n,t_n+1\}}$との差集合を求め，これを$d_{\{p_0,n\}}$と表す．さらに集合 B と集合$l_{\{p_0,t_{n+60}-1,t_{n+60}\}}$との差集合も求めて$d_{\{p_0,n+60\}}$とする．以上を 1 時間分行うため，$n = 0, 1, \dots, 59$と変え，各 n での差分リスト $d_{\{p_0,0\}}, d_{\{p_0,1\}}, \dots, d_{\{p_0,119\}}$ を取得する．次に，表 1 のようなキーに MAC アドレスを，値に容疑度と RSSI を持つ連想配列 T_0 を PCWL p_0に対して作成し，キーに各差集合の和集合 $d_{\{p_0,0\}} \cup d_{\{p_0,1\}} \cup \dots \cup d_{\{p_0,119\}}$ の各要素を，値に各要素が各差集合 $d_{\{p_0,0\}}, d_{\{p_0,1\}}, \dots, d_{\{p_0,119\}}$ に出現した回数を表す容疑度と，犯人が PCWL p_0付近に滞在したと思われる時間帯（ここでは $t_0 - 6 \sim t_1 + 6$ としている）の RSSI 最大値[dBm]をそれぞれ記録する．次に，各 MAC アドレスの容疑度および RSSI をチェックし，設定した閾値を下回った MAC アドレスを取り除く．ここでは，容疑度の閾値を最大値の 9 割，RSSI の閾値を-70dBm としている．表 1 の例では，MAC Address 2, 4, 5 が除外される．

以上を他の PCWL においても行い，$T_0, T_1, \dots, T_{m-1}$全ての連想配列に共通して存在する MAC アドレスのみを集計した表（表 2）を作成し，これを T とする．表 T を容疑者候補の MAC アドレスとして出力する．

表 4　実験諸元

Table 4 Specification of this experiment

実験場所	九州大学伊都キャンパス ウエスト 2 号館 8 階
使用機器	PCWL-0200　4 台 （サーバ通信用 1 台， Probe Request 信号捕捉用 3 台） Pandaboard　3 台 USB カメラ　3 台 サーバ（CentOS）　1 台 無線端末　10 台
PCWL-020 キャプチャ間隔	10 秒
画像キャプチャ	動体検知時

図 6　PCWL の設置位置

Figure 6 Placement of PCWL

4. システムの評価

4.1 実験概要

Criminal Fishing システムの評価を行うため，エリア内に意図的に出現させた犯人役の所持する端末の MAC アドレスを特定する実験を行った．具体的には図 6 のように，九州大学伊都キャンパスウエスト 2 号館 8 階にて PCWL-0200 を 4 台使用して監視エリアを形成した．そのうち 1 台はサーバとの通信を中継する目的で設置し，残る 3 台の PCWL で Probe Request 信号を捕捉する．Probe Request 信号捕捉用の PCWL の近くに USB カメラを接続した Pandaboard を設置した．予め犯人役を用意し，犯人役は Wi-Fi モードを ON にした端末を所持し，必ず全 PCWL を通過するように行動した．これを端末を変えて合計 10 回行った．情報の取得後，Criminal Fishing システム上で犯人役が所有していた端末の MAC アドレスの絞り込みを行った．

4.2 実験結果

まず，Probe Request 数のみを用いたフィルタリング[7]による検出結果を表 5 に示す．この方式では 10 回中 5 回，犯人の端末の MAC アドレスを一意に特定できた．特定できなかった 5 回は，犯人の端末に加えて第 3 者の端末の MAC アドレスも検出されたのが 4 回，第 3 者の MAC アドレスのみが検出されたのが 1 回であった（表 5 における 8 番目の試行）．特定に失敗した中の 1 回（4 番目の試行）に着目し，各 PCWL で犯人の端末と第 3 者の端末の RSSI を観測した結果を図 7-9 に示す．各 PCWL での観測結果から，犯人とほぼ同じ時間に端末が観測されていたことがわかる．一方で，カメラの画像には犯人のみが写っていたことから，カメラの撮影範囲外にいる第 3 者の端末が検出されたと考えられる．ここで RSSI の値を比較すると，カメラに写っ

表 5　Probe Request 数のみによる検出結果

Table 5 Detection results only using the number of probe request signals

試行番号	検出数／絞り込む前の端末数	検出可否	特定可否
1	1／53	○	○
2	1／57	○	○
3	1／52	○	○
4	2／38	○	×
5	1／51	○	○
6	1／61	○	○
7	2／51	○	×
8	1／50	×	×
9	2／52	○	×
10	4／50	○	×

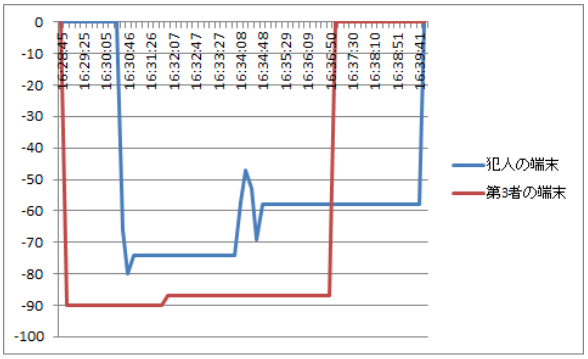


図 7　PCWL1 での RSSI 推移

Figure 7 Time series of RSSI on PCWL1

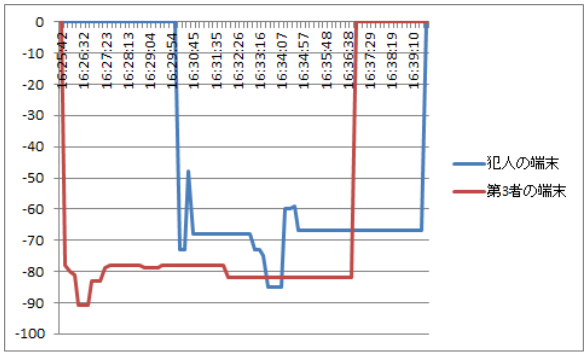


図 8　PCWL2 での RSSI 推移

Figure 8 Time series of RSSI on PCWL2

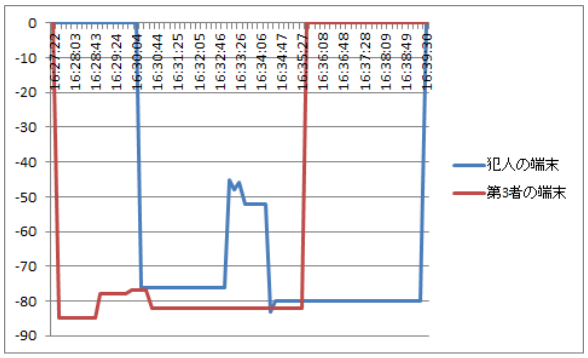


図 9　PCWL3 での RSSI 推移

Figure 9 Time series of RSSI on PCWL3

た犯人の端末はカメラに写った時間帯に-50dBm 前後まで上昇しているのに比べて，撮影範囲外にいる第 3 者の端末の RSSI はおおよそ-80dBm 前後で推移していることがわかる．

次に，本稿が提案する方式（RSSI もフィルタ条件に追加した方式）による実験結果を表 6 に示す．本稿が提案する新方式では 10 回中 10 回，すべてのケースで犯人の端末の MAC アドレスを一意に特定することができた．犯人の出現・消失の 2 箇所で時刻情報を入力することにより，犯人がその場に長く留まった場合にも対応でき，従来方式では犯人の端末を検出できなかった 8 回目の試行においても犯人の端末を特定することができた．また差分取得までの時間を短く設定し，RSSI に閾値を設けたことで第 3 者の MAC

表 6　本提案方式による検出結果

Table 6 Detection results of the proposed method

試行番号	検出数／絞り込む前の端末数	検出可否	特定可否
1	1／48	○	○
2	1／52	○	○
3	1／48	○	○
4	1／38	○	○
5	1／48	○	○
6	1／54	○	○
7	1／45	○	○
8	1／49	○	○
9	1／48	○	○
10	1／48	○	○

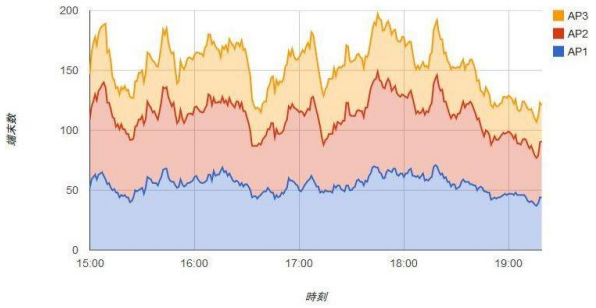


図 10.　実験時間内に観測された端末数の推移

Figure 10 Number of observed MAC address among this experiment

アドレスをすべて取り除くことができた. 図 10 が示すように, 実験を行った九州大学伊都キャンパス ウエスト 2 号館 8 階は無線 LAN 端末が多数存在する場所であるが，常に 50 前後の MAC アドレスが捕捉される環境下でも Criminal Fishing システムは犯人の端末の MAC アドレスを一意に特定できることが示された．

5. おわりに

本研究では，犯罪発生時の電波指紋に基づく Criminal Fishing システムの実現を目指した．具体的には，多数の無線アクセスポイントにカメラを接続して取得した画像と，アクセスポイント周辺に存在する端末が発する Probe Request 信号を捕捉して取得した MAC アドレスにより，容疑者が所有する端末の特定を行った．本稿では Probe Request 信号の捕捉数に加え，その RSSI を判定条件として加えた改良を行った．

屋内環境下での実験の結果，Probe Request 信号の数のみでは犯人の所有する端末を 10 回中 5 回特定するにとどまったが，RSSI を絞込みに利用することで 10 回すべてにおいて犯人の端末を特定することができた．

今後は，より実用レベルの評価を行うために，PCWL の

数を増やして広範囲で実験を行い，新たな知見を得る予定である．

参考文献

1) 大野城市: 落書きはアートではない！立派な犯罪だ！
http://www.city.onojo.fukuoka.jp/safe/bouhan/rakugaki.html
2) 日本万引防止システム協会: 日本万引防止システムの紹介
http://www.jeas.gr.jp/pdf/20150214-2.pdf
3) Megat, N. M. and Mohamed, Noor.: Community based home security system using wireless mesh network, International Journal of Academic Research Part A, Vol.5, No.5, pp.73-79, 2013.
4) 総務省: 平成 26 年版 情報通信白書｜ICT の利用環境の変化
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc141110.html
5) Pandaboard
http://pandaboard.org/
6) Marko Ivančić: Tracking Users in Wireless Computer Networks
http://www.markoivancic.from.hr/2014/07/tracking-users-in-wireless-computer.html
7) 上野祐介: 犯罪発生時の電波指紋に基づく Criminal Fishing システムに関する検討, 九州大学大学院平成 26 年度修士論文, 2015.