様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　６　月　２０　日現在

機関番号：　３２６８９
研究種目：　挑戦的萌芽研究
研究期間：　2015～2016
課題番号：　１５Ｋ１２０３８

研究課題名（和文）人間の移動軌跡とセンサー情報の相関分析により生じる脅威の実証と対策

研究課題名（英文）Understanding the threats caused by correlating human mobility and smart device sensors

研究代表者

森　達哉（Mori, Tatsuya）

早稲田大学・理工学術院・准教授

研究者番号：６０７０８５５１

交付決定額（研究期間全体）：（直接経費）　　2,600,000円

研究成果の概要（和文）：スマートフォン等のデバイスが持つセンサー情報から、そのスマートフォンを携帯する人間の移動軌跡を推定できるかという問題に取り組んだ。具体的な問題として加速度センサー、ジャイロスコープ、磁気センサーの測定データから、スマートフォンを持った人間が乗った電車が発車・停車したという状態を推定し、さらに電車の発停車の時間と時刻表のデータを突合することによって、駅名を特定することが可能である。実データを用いた実証実験の結果、このような攻撃が現実的であることを明らかにした。このようなプライバシー問題を克服するためには生のセンサー情報に対して適切なアクセス制限をかけることが有効である。

研究成果の概要（英文）：We verified the feasibility of a proof-of-concept side-channel attack that identifies a route for a train trip by simply reading smart device sensors: an accelerometer, magnetometer, and gyroscope, which are commonly used by many apps without requiring any permissions. First, by applying a machine-learning technique to the data collected from sensors, we can detect the activity of a user, i.e., walking, in moving vehicle, or other. Next, we extract departure/arrival times of vehicles from the sequence of the detected human activities. Finally, by correlating the detected departure/arrival times of the vehicle with timetables/route maps collected from all the railway companies in the rider's country, it identifies potential routes that can be used for a trip. We demonstrate that the strategy is feasible through field experiments. Building wrapper APIs that provide many useful functions, while hiding raw data, is a promising approach to thwart sensor-based side-channel attacks.

研究分野：　情報セキュリティ・プライバシー

キーワード：　センサー　セキュリティ　プライバシー　機械学習

１．研究開始当初の背景

スマートフォン，スマートウォッチ，スマートグラス等，人々は様々なセンサーを持ち，ネットワークに常時接続されたコンピューターを身につけて行動するようになった．このことは人間の行動に関する情報を収集するチャネルが爆発的に増えつつあることを意味する．また、Barabasi らは携帯電話を持った人間の位置情報を分析し，人間の時空間的な行動軌跡は高い規則性を示すことを明らかにした．このような高い規則性とセンサー情報から収集されるデータを掛けあわせることにより，予想もつかないところでプライバシー情報が漏洩するリスクがある
と考えられる．

２．研究の目的

上述の背景下，スマートフォン等端末のセンサーから得られる情報として，加速度センサー，重力センサー，磁気センサーに着目する．これらのセンサーから取得できるデータを利用して端末の位置情報を推定する技術を提案し，その実現性を実験的方法により明らかにする．一般的な位置情報推定は非常に困難な問題であるが，特に時空間上軌跡の規則性が高い条件として，電車やバス等の公共交通機関による移動開始・終了時の位置情報を推定する問題に取り組む．また脅威に対する有効な対処方法も検討する．

３．研究の方法

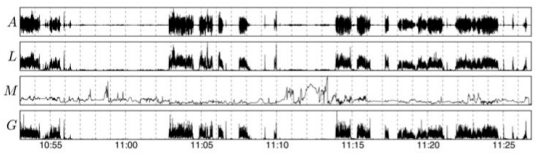
モバイル端末の加速度センサー，重力センサー，磁気センサーから取得した情報をもとに，その端末の位置情報を推定する技術を開発する．具体的には以下の 3 つの項目に取り組む．(1)データ収集：実機を用いてセンサーデータ，測位情報，電車状態メタデータを収集するソフトウェアを開発．
(2)端末状態推定技術：観測したセンサー情報からノイズを除去して得られた信号を元に端末の状態変化（歩行・待機，電車発車・停車）を検知する技術を開発．
(3)位置情報推定技術：センサー情報から電車の発車，停車を検知した後，電車移動中に収集したセンサー情報から両端の駅名を推定する技術を開発．

４．研究成果

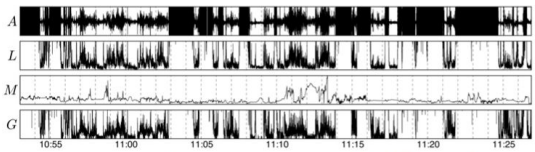
(1)データ収集
Android OS を対象にし、GPS 情報、加速度センサー、磁気センサー、ジャイロスコープを同時に記録し，さらに行動推定を行う機械学習の訓練に必要なラベル付を行うことができるソフトウェアを開発した．各センサーは 10 Hz で読み取りを行ったが，性能に影響を与えないことを確認した．ソフトウェアはスマートフォンとタブレットの両方で動作する．

(2)端末状態推定
下図はセンサー情報を記録し、端末の状態（ユーザの行動）をランダムフォレストによって推定した例である． (a)，(b) の A は加速度，L は線形加速度，M は磁力，G はジャイロスコープを示す．(a)，(b) の Y 軸はセンサーの値の大きさであり，(c)の Y 軸は行動推定の判定である．V は電車に乗っている状況，W は徒歩状態，O はその他の状態を示す．V が 1 の時間帯の最初と最後が電車の発車と停車を示す．

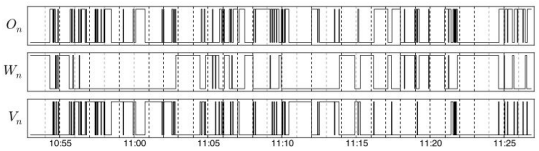
(a) 前処理済みセンサデータ



(b) (a) を拡大したもの



(c) ランダムフォレストによる行動推定の結果



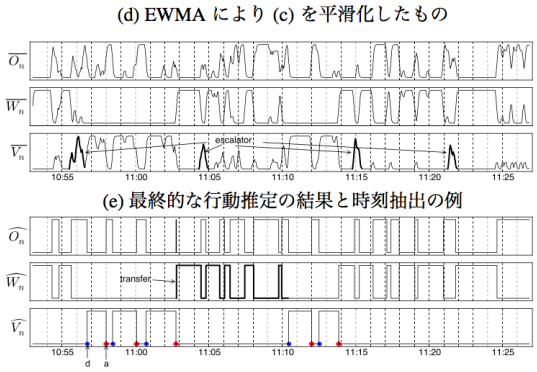
下表は端末状態推定を行うために作成したデータである．4 種の端末と開発した計測ソフトウェアを用いてデータを収集した．

データ	車両内	歩行中	その他
HTC_H	609	1,327	510
HTC_B	691	1,360	510
Nexus_H	686	1,352	505
Nexus_B	602	1,304	505

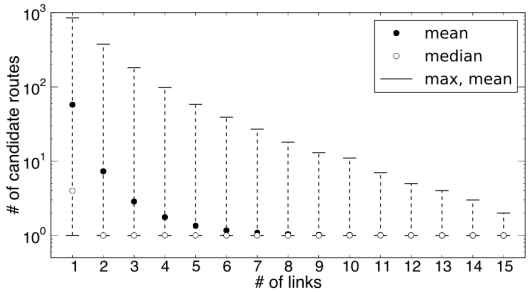
下表は機械学習（ランダムフォレスト）による行動推定精度を調べた結果である．いずれのデータにおいても高い精度と低いエラーによって推定が可能であることが実証された．

データ	精度	FNR	FPR
HTC_H	0.941/0.011	0.042/0.022	0.078/0.013
HTC_B	0.965/0.009	0.024/0.012	0.047/0.014
Nexus_H	0.943/0.013	0.041/0.014	0.074/0.021
Nexus_B	0.969/0.009	0.023/0.012	0.041/0.016

(3)位置情報推定
下図は推定した行動から電車の発停車時間を検出する手順の例を示したものである．状態推定のエラーをノイズとして除去するために最初に端末状態を EWMA により平滑化し，適当に定めたしきい値によって推定した行動を時系列データとして扱えるようにする．得られた時系列データから発車時刻と停車時刻を抽出することができる．

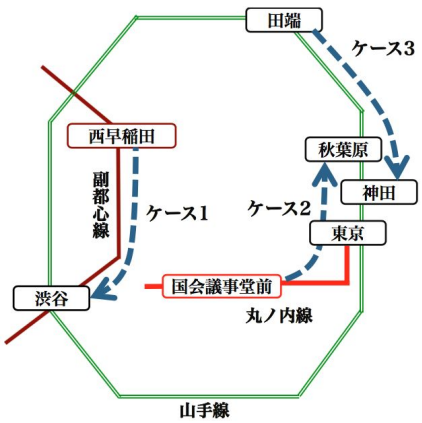


得られた時刻と時刻表を照合することにより，電車の経路候補を列挙することが出来る．日本全国に存在する鉄道会社の路線をまとめた鉄道グラフに対して，考えうる全ての経路を走査し，時刻表を参照することによって発着時刻のシーケンス群を得る．ここで組み合わせ爆発を回避するため，リンクの数は 15 個まで，乗り換えの回数は 2 回までとした．その後，各時刻シーケンスに対していくつの経路が候補として列挙されるかを数える．以上のシミュレーションによって，入力されるリンクの数に対し，列挙される経路候補の数を計 算する．シミュレーションの結果を下図に示す．例え ば，標的が 6 リンク，すなわち 6 駅分の列車移動を行うとき，移動経路を平均で 1 に近い候補数に絞り込むことができる．また，たった 1 つの発着時刻 Td , Ta を 用いた時でも，約 50%の割合で 4 つ以下の候補に絞られることがわかる．経由する駅の数が増加すればするほど，経路を一意に特定できる可能性は高まる．



(4)フィールドでの実例

下記の路線（ケース 2）で端末の位置情報を推定した例を示す．



下表はセンサー値の情報から電車の発車・停車時刻を推定した結果である．
観測時刻は実際の発車・停車の時間，定刻は時刻表に記載の時間であり，推定した結果はこれらの 2 つと一致していることがわかる．

状態	推定時刻	観測時刻	定刻
歩行とその他		–	
出発	10:56	10:56	10:56
到着	10:58	10:58	10:58
出発	10:58	10:58	10:58
到着	11:00	11:00	11:00
出発	11:00	11:00	11:00
到着	11:03	11:03	11:03
歩行とその他		–	
出発	11:10	11:10	11:10
到着	11:12	11:12	11:12
出発	11:12	11:12	11:12
到着	11:14	11:14	11:14
歩行とその他		–	

下表は上記の時刻にマッチする正解の経路と，提案した技術によって抽出した経路候補の内，上位 2 のスコアを持つ経路を示している．

No.	正解	経路 1	経路 2
1	国会議事堂前	国会議事堂前	江戸川橋
2	霞ヶ関	霞ヶ関	護国寺
3	銀座	銀座	東池袋
4	東京	東京	池袋
乗り換え			
4	東京	東京	池袋
5	神田	神田	要町
6	秋葉原	秋葉原	千川
スコア	–	2,664	2,277

よりスコアが高い経路 1 が正解データと一致していることが分かる．同様にケース 3 においても推定がうまくいくことがわかった．ケース 1 では電車の運行に大幅な遅延が生じていいたため，経路の推定には失敗した．
以上で示されたように，実際のフィールドにおいて攻撃が実現可能であることが実証された．

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 1 件）

[1] T. Watanabe, M. Akiyama, and T. Mori, “Tracking the Human Mobility Using Mobile Device Sensors,” IEICE Transactions on Information and Systems, Vol. E100-D, No. 8, pp. xxx-xxx, Aug. 2017 (出版予定).

〔学会発表〕（計 2 件）

[1] 渡邉卓弥，秋山満昭，森達哉，“RouteDetector: 9 軸センサ情報を用いた位置情報追跡攻撃，”コンピュータセキュリティシンポジウム 2015 論文集 (CSS2015), vol. 2015, No. 3, pp. 1127-1134 , 2015 年 10 月

長崎県・長崎市

[2] T. Watanabe, M. Akiyama, and T. Mori, “RouteDetector: Sensor-based Positioning System that Exploits Spatio-temporal Regularity of Human Mobility,” Proceedings of the 9th USENIX Workshop on Offensive Technologies (WOOT 2015), pp. 1-11, August 2015, Washington D.C., US.

〔図書〕（計　　件）

〔産業財産権〕

○出願状況（計　1　件）

名称：位置推定装置、位置推定方法
発明者：森達哉，渡邉卓弥，秋山満昭，八木毅
権利者：同上
種類：特許
番号：特開 2017-26542
出願年月日：2015 年 7 月 27 日
国内外の別： 国内

○取得状況（計　　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://nsl.cs.waseda.ac.jp/projects/

６．研究組織
(1)研究代表者
森　達哉（MORI, Tatsuya）
早稲田大学・情報通信学科・准教授
研究者番号：60708551

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：

(4)研究協力者
渡邉卓弥（WATANABE, Takuya）

秋山満昭（AKIYAMA, Mitsuaki）

八木毅（YAGI, Takeshi）