RO-004

スマートハウスにおける電力変動からの不正アクセス検知の検討

Intrusion Detection of Unusual Electricity Consumption in a Smart House

奥村 晃弘† 白石 善明† 岩田 彰†
Takahiro Okumura Yoshiaki Shiraishi Akira Iwata

1. まえがき

2011 年 3 月 11 日の東日本大震災により，日本の電力事情が大きく変わり，需要家の省エネルギー意識が高まりつつある．太陽光発電やバイオマスに代表される再生可能エネルギーの普及やその期待の高まりに伴い，スマートグリッドの重要性も増している．

スマートグリッドを構成する最小単位としてスマートハウスがある．スマートハウスは情報技術を用いて家庭のエネルギー消費を最適に制御するエコ住宅である．スマートハウスは HEMS (Home Energy Management System) というエネルギー管理システムを用いて，太陽光発電や燃料電池などのエネルギー機器，家電機器，電気自動車，住宅機器などを制御する．

文献[1]では，スマートハウスのリスクとして，生活情報が漏洩するリスクや HEMS で管理された家電機器が DDoS 等の攻撃を直接受けて負荷に耐えられずに停止してしまうといったリスクが挙げられている．現在はネットワーク接続機能を持たない冷蔵庫等の白物家電も IP 化されてインターネットに繋がるようになれば，脅威は更に大きくなる．ネットワークセキュリティの観点から，ファイアウォール機能や暗号化通信機能等を用いて主要な脅威を未然に防ぐ入口対策は必須のものである．さらに，ネットワークへの不正侵入が行われた場合においての入口より後の部分での対策も考慮しなければならない．

本研究では，スマートハウスへのネットワーク不正侵入が実行された際に，機器への負荷が掛かり，定常時とは異なる電力値の変化が生じることに注目する．本論文では，消費電力の変化から不正アクセスを検知することを目的として，電力値に統計的異常検知手法を適用した侵入検知を検討する．

2. スマートハウスとネットワーク不正侵入

2.1 スマートグリッドとスマートハウス

スマートグリッドは情報通信技術により最適化された送電網のことである．自律的に動作し，電力を監視し，需要と供給の双方向から電力を制御する特徴を持ち，省エネルギー化とコスト削減が期待されている．

スマートグリッドを構成する最小単位として，スマートハウスが挙げられる．スマートハウスは情報技術を用いて太陽光発電や燃料電池などのエネルギー機器や家電機器等を制御し，エネルギー消費を最適に制御するエコ住宅である．

スマートハウスにおける制御システムの構成要素として，スマートメータ，ホームゲートウェイ，HEMS が挙げられる．スマートメータは，各家庭の電力を可視化すると共に電力使用量を監視することで機器の制御を行う通信機能付き電力メータである．また，ホームゲートウェイは，外部のサービス事業者や電力会社との情報のやり取りの接点となるネットワーク機器である．HEMS はエネルギー管理システムのことで，住宅内のエネルギー機器や家電機器等をネットワーク化し，安定した電力供給と省エネルギー化を実現するシステムである．

2.2 スマートハウスへのネットワーク不正侵入の脅威

制御システムは独自 OS と独自ネットワークの隔離された個別システムから，オープンソースソフトウェア等も含む汎用製品の COTS 技術を用いて接続されたシステムへの変化の傾向がある [2]．制御システムはシステム全体のサポートコストの低減，遠隔サポートの容易性という観点から共通インタフェースの採用を行う等，制御システムのオープン化とネットワーク化への流れが生じている．

そのようなオープン化の流れにおいて，汎用品の脆弱性の課題がそのまま引き継がれてしまうことや，標準プロトコルのネットワークの採用によるワームなどのウイルスの侵入や機密情報漏えいの可能性といったネットワークへの不正侵入の脅威が，制御システムおいても拡大することは避けられない．制御システム分野の特徴を考慮したセキュリティ技術の開発は重要な課題となる．

スマートハウスでは，HAN (Home Area Network)によって家庭内機器をネットワークで繋ぐことから，セキュリティ対策は必須である．スマートハウスの制御システムはコスト削減等の観点から共通化が進むと考えられる．現在はネットワークへ接続する機能を持たない白物家電のような機器もやがては IP 化され，インターネットへ接続されるようになると，脅威のレベルは更に大きくなる．

文献 [1]では，スマートハウスに想定されるリスクについて，生活者の情報が漏洩するリスクや HEMS で管理された家電機器が DDoS 等の攻撃を直接受けて負荷に耐えられずに停止してしまうといったリスクなどが考えられると指摘している．

2.3 スマートハウスのセキュリティ

2.3.1 ECHONET Lite におけるスマートハウスセキュリティ対策

スマートハウスのセキュリティ対策として，HEMS コントローラにファイアウォールや暗号化通信機能を用いることにより，主要な脅威を遮断することは重要である．

通信路のセキュリティに関して，日本のスマートハウスの標準インターフェイスである ECHONET Lite 規格がある [5]．通信ミドルウェアにおいて既存のセキュア通信の標準技術を適用している．しかし，これらは従来型の情報システムへの入口対策のセキュリティであるため，入口対策を前提とした上で，かつ，入口を突破された際

† 名古屋工業大学，Nagoya Institute of Technology

の，入口より後の部分におけるセキュリティ対策を講じる必要がある．

2.3.2 既存のネットワーク不正侵入検知方法

ネットワーク不正侵入対策として，不正アクセス監視システムや侵入検知システムのような，ネットワークに流れるパケット情報を監視する仕組みが存在する．

不正アクセス検知の動作原理は，1) シグネチャ型によるパタンマッチング (シグネチャ型)，2) 統計情報に基づく侵入検知 (アノマリ型) の 2 種類に分けられる．

シグネチャ型は，予め分かっているウイルスや不正アクセス情報をシグネチャとして定義し，シグネチャと入力データと照合し，異常を判断する方法である．しかし定義ファイルの作成の手間や無視できない計算時間になりつつある．アノマリ型は，例えば管理者が予め定義しておいた正常な状態を蓄積しておき，現状との比較を行い，しきい値を超えた場合に異常と判断する方法である．

大量のデータから統計的パターンを学習し，ログに潜在する規則性や特徴パターン，異常を検知するデータマイニングによるログ解析技術は，シグネチャベースのものと比べて，未知のセキュリティ事案に対する早期発見・検出が期待できる．

2.4 機器の消費電力の観測によるスマートハウスへのネットワーク不正侵入検知

もしも，各機器の消費電力は多少のノイズが混入するものの基本的にはほぼ規則的あるいは特徴的な傾向を持ち，かつ，不正アクセスを受けている機器に当該アクセスに対する負荷が加わったときに消費電力に変化が生じるならば，その変化を検知することで不正アクセスを検知できると考えられる．

そこで，本論文ではスマートハウスにおける消費電力の変化から不正アクセスの検知手法の確立を目指して，その検知可能性について検討を行う．具体的には，データマイニング技術による異常検知手法を用いて，電力値の統計的パターンを学習し，異常を検知する方法について検討する．

3． 統計的異常検知

3.1 オンライン忘却型学習アルゴリズム

統計的異常検知は，データの生成機構が確率モデルで表現できると仮定した場合の異常検知の方法論である [6]．これまでに得られたデータからデータ発生分布の確率モデルを学習し，学習されたモデルを基にデータの異常度合い，またはモデルの異常な変化度合いのスコアリングを行う．

逐次的にデータが入力されるような状況において，過去のデータを徐々に忘却しながら学習する手法であるオンライン忘却型学習アルゴリズム (on-line discounting learnig algorithm) と呼ばれるものがある．オンライン忘却型学習アルゴリズムは，入力されるデータの生成機構が時間と共に変化するような非定常的な情報源に対しても適応的に学習することが可能である．本論文で扱う統計的異常検知手法を表 1 に示す．

3.2 外れ値検出

外れ値検出とは，ガウス混合分布等の多次元ベクトルを入力の対象とし，確率モデルとして独立モデルを仮定して，モデルから相対的に見て特異なデータ (外れ値) を検出することである．

表 1: 統計的異常検知手法

機能	入力対象	確率モデル	検出対象	応用
外れ値検出	多次元ベクトル	独立モデル (ガウス混合分布)	外れ値	不正検出 侵入検知 故障検知
変化点検出	多次元時系列	時系列モデル (AR モデル，回帰モデル)	時系列上の急激な変化 バースト的異常	攻撃検出 ワーム検出 障害予兆検出

外れ値検出のオンライン忘却型学習アルゴリズムとして Yamanishi, Takeuchi and Williams and Milne らによる手法がある [7]．リアルタイムに外れ値検出を実現するための方式として，データの統計的パタンを学習し，そのパタンに基づいて各々のデータをスコアリングする方法をデータが入力される毎にオンラインで行う．

3.3 変化点検出

変化点検出とは，回帰モデルや自己回帰モデル等の多次元時系列を入力の対象とし，確率モデルとして時系列モデルを仮定して，時系列上の急激な変化やバースト的異常を検出する方法である．

変化点検出のオンライン忘却型学習アルゴリズムとして，時系列モデルである AR モデルをもとにした Takeuchi and Yamanishi らによる手法がある [8]．これは時系列の定常性を仮定した AR モデルと比べて，忘却効果によって非定常なモデルの学習を実現している．

4． 提案手法

外れ値検出では，機器が固有に発するノイズのような一瞬の電力値の増減には高いスコアを示さず，DoS 攻撃のような継続的な負荷で生じる電力値の変化に有効である．どの程度のスコアによって異常と判定するかのしきい値の設定により検知率が変わる．

変化点検出では，著しい電力値の上昇のような値の振る舞いの変わり目に対して高いスコアを獲得できるため，ネットワーク不正アクセスで機器へかかる負荷に対しても有効であると考えられる．一方で，ノイズ電力値にも同様に反応してしまう．

そこで本論文では，図 1 に示すようにこれら 2 つの統計的異常検知手法によって得られた各異常スコアを統合することで，電力値の異常部分のみを検出することを目指す．統合方法は，外れ値検出と変化点検出で得られた各スコア列に対し，同時刻における各スコア点を乗算し，それらを定数倍しスコア列を平滑にする．

$$Outlier(\mathbf{x}) = -\ln p(\mathbf{x}|\theta),$$
$$ChangePoint(\mathbf{x}) = -\ln q(\mathbf{x}|\theta'),$$
$$IntegratedScore(\mathbf{x}_t) = a \times Outlier(\mathbf{x}_t) \times ChangePoint(\mathbf{x}_t)$$

$p(\mathbf{x}|\theta)$は外れ値検出において学習されたモデルに基づく条件付き確率密度関数であり，$q(\mathbf{x}|\theta)$は変化点検出において学習されたモデルに基づく条件付き確率密度関数である．$\mathbf{x}$は入力データを示し，θ, θ'は各手法におけるパラメータを示す．また，各手法により得られるスコアは対数損失により算出される．aは定数倍を示す．

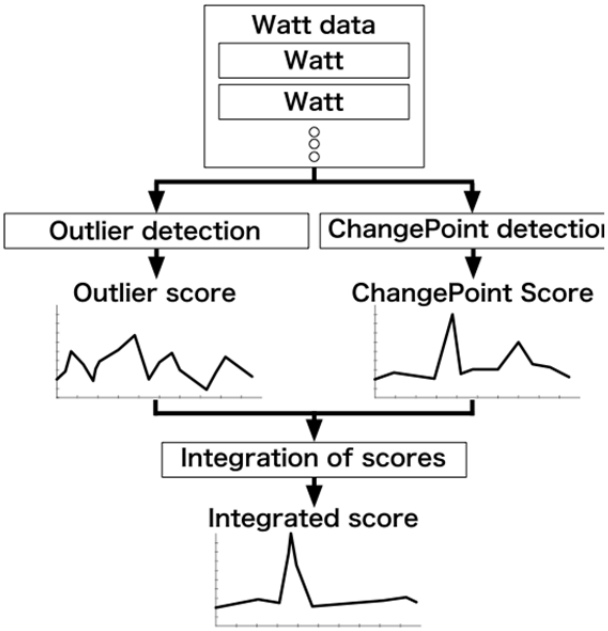

図 1: 提案手法概要

5. 電力値の測定

電力値の計測には，maxim integrated™ の製品であるエネルギー測定用 IC を備えた 78M6613 [9]の評価ボードを用いる．電力値の計測対象として Note PC を使用した．

これら機器の配置は図 2 のようになる．まず，測定対象である Note PC の電源プラグを評価ボードのプラグジャックへ接続し，評価ボードからの電源プラグをコンセントへ接続する．これにより，Note PC への供給電力は評価ボードを経由し，Note PC の電力値計測が可能となる．この評価ボードはいわゆる電力値などを計測できるスマートコンセントを試作したものである．

評価ボードからの電力値収集用に別途 PC を用意し，評価ボードと USB シリアル接続によって計測値のログを取る．なお，電力値は 1 秒間に 1 回ずつ測定可能である．

6. 評価

6.1 評価環境

表 2 に示した Intel Core i7 (2.3GHz) で，RAM は 16GB の計算機上で提案手法を実装し，評価した．使用言語は Python3.3.0 で，数値計算ライブラリである numpy 及び scipy，機械学習用ライブラリ scikit-learn と統計モデル用ライブラリ statsmodels を使用した．

6.2 不正アクセス時の電力変化

定常時の電力値と不正アクセスによる非定常時の電力値を合成したものを評価用データセットとして用意し，提案手法の評価を行う．

非定常時の電力値を模擬するための，攻撃用端末から被測定機器 Note PC への攻撃方法は次の通りである．攻撃用の端末として FreeBSD 9.1-RELEASE が搭載された計算機を用意した．不正アクセスの例として無線アクセスによる DoS 攻撃を想定し，ping フラッドを用いた．

ping フラッドは DoS 攻撃の一種で，ネットワーク上のサーバやルータに対して，攻撃者が多数のパケット送信を試みるものである．大量にパケットを送りつけられた被測定機器には負荷が掛かり，その際に電力値が上昇する．

このときの電力値を 60 分間計測し，計 3600 点の電力値のログを収集した．具体的には図 3 に示すように，1) 30 分間定常時の電力値を測定し，2) 30 分の時点から 1 分間の ping フラッドを実行し，非定常時の電力値を計測し，3) 残りの 29 分間は定常時の電力値を計測した．

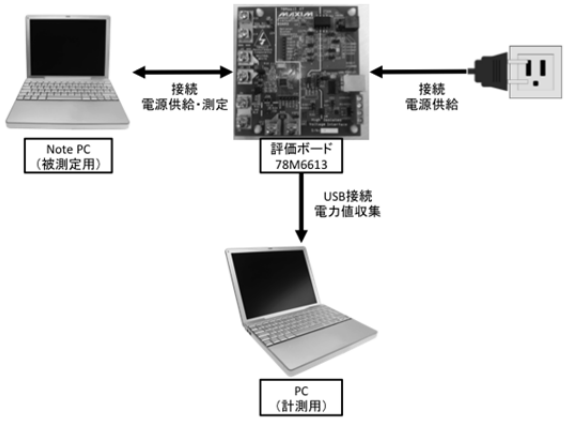

図 2: 電力値の測定環境

表 2: 評価環境

OS	OS X 10.8.3 64bit
使用言語	Python 3.3.0
使用ライブラリ	NumPy/SciPy Scikit-Learn StatsModels
プロセッサ	2.3 GHz Intel Core i7
RAM	16GB 1600 MHz DDR3

6.3 仮想的な HEMS 環境における評価

被測定機器としてテレビを使用した．非定常時の電力値として，図 3 の電力値データとテレビの電力値を合成した図 4 のデータを用意し，仮想的な HEMS に対する攻撃があったとみなすこととする．

仮想的な HEMS への攻撃に対して，提案手法で検知できるかを確認する．このとき，外れ値と変化点の検出手法における忘却パラメータ r は 0.1，定数倍aは 0.1 とした．

提案手法で出力したスコアは図 5 のようになった．1800 秒の攻撃開始時における電力値部分において高いスコアを示しており，ノイズ電力値に対するスコアは DoS 攻撃開始時のものと比べて小さいことが確認できた．

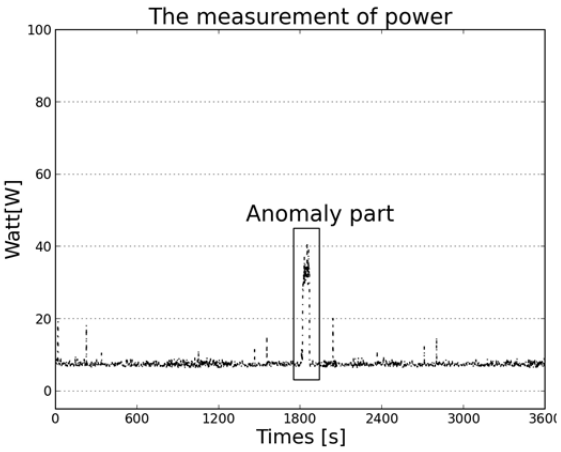

図 3:ping フラッド実行中に 測定した電力値

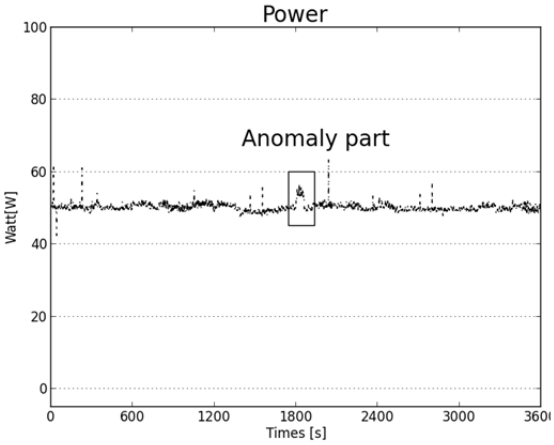

図 4: 仮想的な HEMS への攻撃

7. むすび

スマートハウスにおけるネットワーク不正侵入に対して，消費電力を機器を接続したコンセントにおいて取得できる場合に，その取得した消費電力の変化から侵入を検知することを目的として，統計的異常検知手法の外れ値検出と変化点検出を用いた統合手法を提案した．

不正アクセスの例として DoS 攻撃による過負荷を想定し，PC を用いて定常時と非定常時の電力値を計測し，その評価用データセットを用いて提案手法を評価した．

結果として，評価環境においては提案手法で DoS 攻撃による電力値の上昇部分のみが高スコアとなることを確認できた．

本論文では，1 台の家電機器がコンセントにつながっているときの ping フラッドによる DoS 攻撃の検知という小さな模擬環境における結果を報告したが，多数の家電機器がコンセントにつながっている状況での異常検知や，DoS 攻撃のパケット送信速度に対する検知精度，その他の攻撃方法での検知精度について実験により確認することが今後の課題として挙げられる．

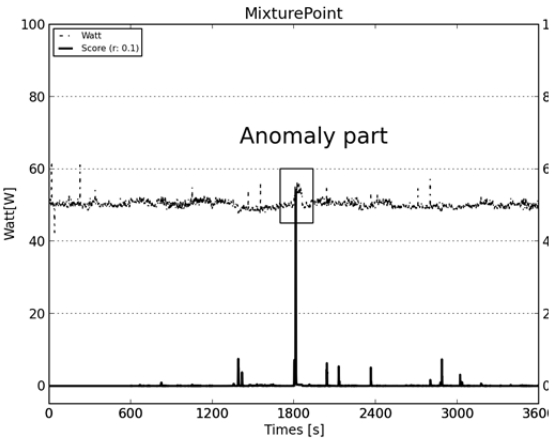

図 5:電力値と提案手法のスコア

参考文献

[1] 独立行政法人 情報処理推進機構 セキュリティセンター, "2010 年度 制御システムの情報セキュリティ動向に関する調査報告書," 2011.

[2] 独立行政法人 情報処理推進機構 セキュリティセンター, "重要インフラの制御システムセキュリティと IT サービス継続に関する調査," 2009.

[3] 独立行政法人 情報処理推進機構 セキュリティセンター, "「新しいタイプの攻撃」の対策 に向けた設計・運用ガイド　改訂第 2 版," 2011.

[4] JSCA. スマートコミュニティ・アライアンス, https://www.smart-japan.org/

[5] ECHONET CONSORTIUM. (2012) エコーネットコンソーシアム, http://www.echonet.gr.jp/spec/spec_v101_lite.htm

[6] Kenji Yamanishi, Jun-Ichi Takeuchi, and Yuko Maruyama, "Three Methods for Statistical Anomaly Detection(New Frontier of Data Mining Methods)," *IPSJ Magazine*, vol. 46, no. 1, pp. 34-40, Jan. 2005.

[7] Kenji Yamanishi, Jun-ichi Takeuchi, Graham Williams, and Peter Milne, "On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms.," 2004.

[8] Kenji Yamanishi and Jun-ichi Takeuchi, "A Unifying framework for detecting outliers and change points from time series," 2006.

[9] maxim integrated. maxim integrated , http://japan.maximintegrated.com/datasheet/index.mvp/id/7080