計算システム工学分野

スマートハウスにおける電力異常の統計的検知に関する研究

学籍番号 23413521 氏名　奥村　晃弘
指導教員名　岩田　彰

1　スマートハウスとネットワーク不正侵入

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，家電，住宅機器などを制御し，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．また，その制御システムの中核要素としてHEMS (Home Energy Management System) がある．HEMSは住宅向けエネルギーマネジメントシステムのことで，住宅内のエネルギー機器や家電などをネットワーク化し，エネルギー消費を管理・最適化するための電力供給の安定化と省エネを緻密な制御技術で実現する機能を持つ．

スマートハウスではHome Area Networkによって機器通信ネットワークを構成する．家庭内機器をネットワークでつなぐ上で，セキュリティ対策は必須である．現在はネットワーク接続機能のない機器もインターネットへ接続されるようになると，将来的な脅威のレベルは大きくなる．

IPA (独立行政法人 情報処理推進機構) の「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 [1]」によると，スマートハウスの想定リスクについて，生活者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．

既存のネットワーク不正侵入の検知にはIDSが存在するが，IDSには多くのコンピュータのリソースが必要とされることや，攻撃手法に応じたシグネチャの更新時間と更新するまでのタイムラグ，誤報，関しパケットの取りこぼし等の課題があり，別の方法も検討する必要があると考える．

ここに，スマートハウスへの不正アクセスが生じた際の機器への負荷から，定常時とは異なる電力の変化が生じている可能性に注目する．しかし，消費電力の変化からネットワーク不正侵入を検知する方法は確立されていない．そこで，本研究では電力値から電力異常を検知する可能性について検討を行う．

2　電力値による侵入検知の可能性の基本的検討

不正侵入検出には，例えばウイルス検知では署名ベースによるパタンマッチングがある．しかしこのような定義ファイルは作成の手間や計算時間が膨大になりつつあり，補完技術の必要性が訴えられている．

そのような補完技術としては，データマイニング技術によるログ解析がある．データマイニングにより自動的に生成された統計的パタンを用いて，ログから変化や異常を検知する等，セキュリティインシデントの発見に効果があると期待されている．

ここに，データマイニングによる異常検知手法を用いて，電力値の統計的パタンを学習し，特徴パタンから電力異常を検知する可能性について考える．

個々の電気機器の電力情報を測定し，電力値から異常検知手法を用いて，不正アクセスなどの攻撃が生じた場合において生じる潜在的な変化を検出することを検討する．この検討によって，電力異常の統計的検知の可能性を明らかにする．

3　統計的異常検知手法

統計的異常検知手法は，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のことで，学習した確率モデルを基にデータの異常度合いのスコアリングを行う [2]．

統計的異常検知手法はいずれもオンライン忘却型学習アルゴリズムと呼ばれる，データが逐次的に入力される状況において，過去のデータを徐々に忘却しながら学習するものである．非定常的な情報源に対しても適応的に学習可能である．

外れ値検出

外れ値検出は，ガウス混合分布やヒストグラム等の多次元ベクトルを入力の対象とし，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を検出する方法である．

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．

4　試作と評価

評価は実際に電力値を計測したものを用いる．計測機器はPCを利用した.DoS攻撃を不正アクセス例とし，pingフラッドを使用した(図 1)．

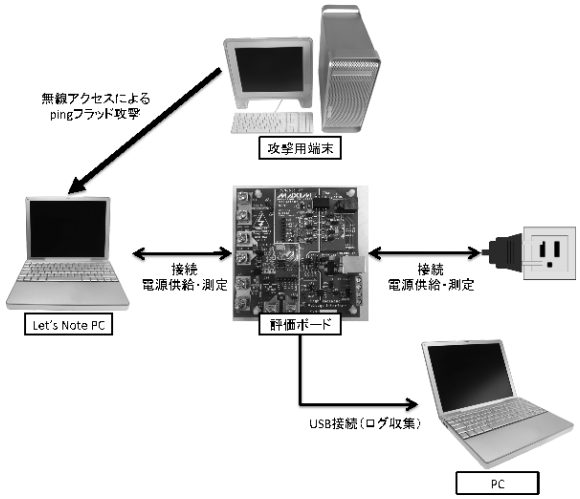

図 1：電力値の計測環境

次にどのような電力値を測定するかについて説明する．電力値は1秒間に1回ずつ測定し，合計60分間の電力値3600点を計測する．具体的には，DoS攻撃を行わない定常時電力を30分間計測した後，5分間のDoS攻撃を実行，その後1分間DoS攻撃を停止した後，4分間DoS攻撃を再開する.その後DoS攻撃を停止して，20分間定常時の力を測定する．

外れ値検出と変化点検出のプログラムを試作し，測定した電力値を評価用データセットとして用いてスコアリングを行った．

5　結果と考察

図 2に測定した電力値と各スコア結果のプロット図を示す．外れ値検出では，ノイズに対しての多少の反応はあるものの,DoS攻撃時にしばらくの間高スコアを獲得していることが分かる．

変化点検出では,DoS攻撃時による著しい電力値上昇に対して高スコアを獲得している一方で,DoS攻撃時以外のノイズに関しても強い反応が見られる．

これらの結果から，各統計的異常検知手法の単体利用では，電力値から異常を満足に検知できたとは言えない．しかし，２つの手法を組み合わせることでDoS攻撃時の電力異常を検知することが可能であると言える．具体的には，変化点検出が高いスコアを獲得したと同時に，外れ値検出によるスコアの変動率を確認し，外れ値検出が一定期間，定常時に比べて高いスコアを獲得し続けていれば異常として検知する.これにより,消費電力の変化そのものから，ネットワークからの不正アクセスを検知する可能性についての検討を行った．課題として，変化点検出が高いスコアを獲得した瞬間から，外れ値検出がどの程度の期間高いスコアを獲得し続ければ異常と判定するかの検証を行う必要がある．

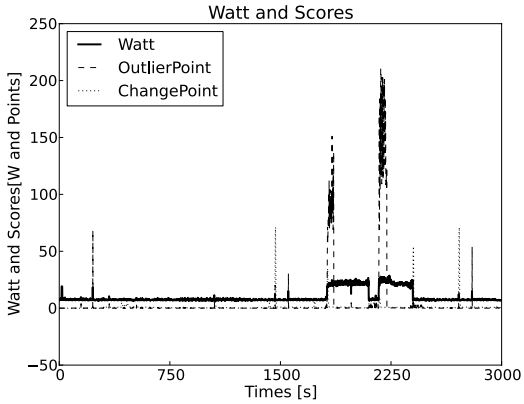

図 2：測定した電力値と各スコア結果

6　まとめ

消費電力の変化そのものからネットワーク不正侵入を検知する可能性の基本的検討のため，統計的異常検知手法による電力異常検知を行った．

定常時電力の他,PCへのDoS攻撃による過負荷から生じる非定常電力の２種類を計測し，試作によるスコアリングを行なった．

結果として，２つの統計的異常検知手法の組み合わせにより，消費電力の変化そのものからネットワーク不正侵入を検知する可能性についての基本的検討を行えた．課題として，組み合わせによる異常判定のしきい値に関して検証を行う必要がある．

7　参考文献

[1] 独立行政法人 情報処理推進機構，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] 山西 健司，“データマイニングによる異常検知”，共立出版，(2009)