ISSN 2186-5647

P-34

スマートグリッド通信における差分プライバシーと個人コードを用いた故障ノード特定法

日大生産工(学部)　○斉藤　大貴
日大生産工　新井　雅之

1 まえがき

近年, 限られたエネルギーを有効に活用するため, 情報通信技術を用いて電力配送を効率化するスマートグリッドが注目を集めている. しかしスマートグリッド通信では電力消費量という個人情報を扱うため, プライバシー, セキュリティの面から様々な課題が存在する.

Baoらは, スマートグリッド通信においてフォールトトレランス及びプライバシー保護を考慮したデータ集約法DPAFTを提案した[1]. OgasawaraらはDPAFTを拡張し, 外部への端末故障情報流出を防ぐプロトコルを提案した[2]. しかし文献[1], [2]の手法では, 端末故障情報流出の防衛または情報管理ノードによる故障ノードの特定のいずれかが不可能である.

本研究では, スマートグリッド通信のデータ集約において, 個人のプライバシーを保護しつつ故障ノードを識別する手法について提案する. 提案手法では, DPAFTを基に個人コードを用いて故障ノードを識別する機能を追加する. 提案手法の概要について示し, セキュリティ評価について報告する.

2 関連研究

2-1． DPAFT (Differentially Private Data Aggregation With Fault Tolerance)

Baoらはスマートグリッド通信におけるデータ集約法であるDPAFT (Differentially Private Data Aggregation With Fault Tolerance)について提案した[1]. 図１にDPAFTの概要を示す.

n人のユーザ$U_1, U_2, \ldots, U_n$ は，自身の電力消費量データm_iを基に暗号化されたデータC_iを生成する. GW (Gateway)はC_iを集約したデータ$\sum C_i$を算出する. DPAFTは準同型暗号を使用しており，GWは暗号化されたデータC_iを復号することなく合計し，CC (Control Center)に転送する．CCは送られたデータ$\sum C_i$を復号化して$\sum m_i$を得ることが出来る.

DPAFTでは，CCがユーザの合計電力消費量を取得することだけが可能であり, CC及びGWが各ユーザの電力消費量を知ることはできない. しかし端末故障情報がGWで収集されCCに送信されるため, 盗聴による端末故障情報流出の可能性がある.

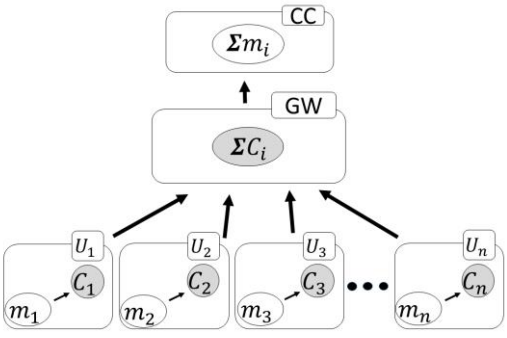

図１．DPAFT のアルゴリズム[1]

2-2．スマートグリッド通信におけるスマートメータ故障とプライバシーを考慮したデータ集約法

文献[2]では，スマートメータ故障時の端末故障情報流出を防ぐことを目的として，DPAFTを基にプロキシサーバを用いて電力消費量データを代理送信する手法が提案された.

図2に文献[2]におけるデータ集約法を示す. 各ユーザにおけるプロキシサーバは, 電力消費量m_iから生成したC_iと共に, スマートメータの動作状況$m_i'(0：停止，1：動作)$を暗号化した

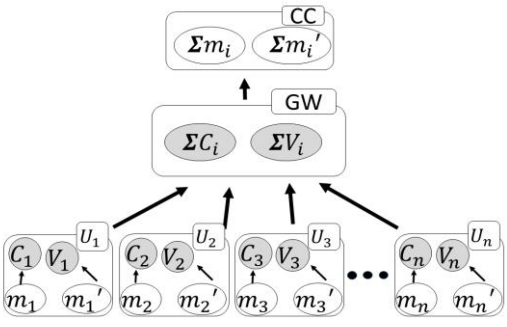

図２．プロキシサーバによる代理送信のアルゴリズム[2]

Identifying Faulty Nodes using Differential Privacy and Personal Numbers in Smart Grid Communications

Hiroki SAITO and Masayuki ARAI

データV_iを送信する．CCは，m_iと同様に，集約されたm_i'の合計$\sum m_i'$を得ることが可能である．すなわち有効なノード数を得ることが可能である．GWが端末故障情報を特定することは不可能であるが，CCが故障端末の識別をすることもまた不可能となる．

3 提案手法

3-1. 提案手法の概要

本研究ではDPAFTを拡張し，端末故障情報を情報管理ノードのみが識別可能であるようなデータ集約プロトコルを提案する．

図3に提案手法のアルゴリズムを示す．まずCCが各ユーザU_iに対する個人コードk_iを生成する．CCはk_iを暗号化してw_iを生成し各ユーザに送信する．各ユーザのプロキシサーバは，暗号化された電力消費量C_iと同時に，暗号化された個人コードw_iをGWに送信する．ただしスマートメータが故障している場合，w_iではなくw_0 $(k_0 = 0)$を送信する．

GWでは暗号化された個人コードw_iの合計$\sum w_i$が集約されCCに転送される．CCは$\sum w_i$を復号し$\sum m_i'$を得る．

次節に示すとおり，CCは$\sum m_i'$を用いて各ユーザの端末故障状況を把握することが出来る．

3-2. 個人コード生成と故障ノード特定

複数のスマートメータが故障した場合でも故障ノードを特定出来るようにするために，個人コードを以下のように設定する．

$$k_i = 2^i \cdot 2^x \quad (x > n).$$

CCは取得した個人コードの合計から$\sum k_i \bmod 2^x$を求める．この値を２進数で表記すると，故障ノードに相当するビットのみが0となっている．

xの値が大きいほどk_iを特定するためのBrute Force攻撃に対して安全性が高くなる．

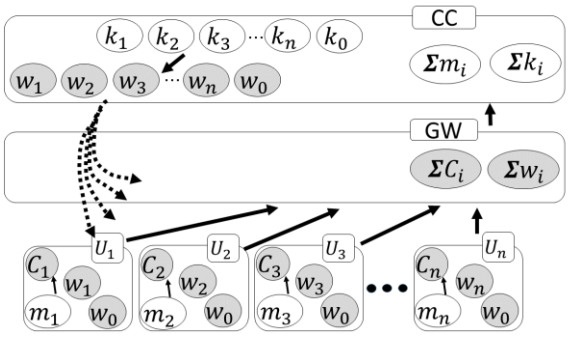

図３．提案手法のアルゴリズム

4 提案手法のセキュリティ評価

シナリオ解析に基づいて提案手法のセキュリティ評価を行った．本研究では暗号化された個人コードw_iの集約を，DPAFTと同様のアルゴリズムを用いて行っている．DPAFTの安全性についてはすでに文献[1]にて示されている．従って、提案手法は盗聴とGWにおけるマルウェア攻撃に対して安全性を有することが示された．また，GWにおいて端末故障情報が流出しないことを確認した．

Brute Force攻撃とHonest but Curiousモデルに対する提案プロトコルの安全性は，現在検討中である．

5 まとめ

本研究では先行研究であるDPAFTとスマートグリッド通信におけるスマートメータ故障とプライバシーを考慮したデータ集約法を元に，スマートメータ故障時の故障情報を情報管理ノードのみが識別可能であるデータ集約プロトコルの提案を行った．シナリオ解析に基づいて，盗聴とGWにおけるマルウェア攻撃に対して安全性を示した．

今後は故障した端末が送信するw_0の値を設定し，更なる安全性の向上を目指す．

参考文献

[1] Haiyong Bao, Rongxing Lu, “A New Differentialy Private Data Aggregation With Fault Tolerance for smart Grid Communications,” IEEE Internet of Things Journal, Vol. 2, No. 3, pp. 248-258, 2015.

[2] Ryouta Ogasawara, Masayuki Arai, “Data Aggregation on Smart Grid Communications Considering Fault Tolerance and Privacy,” Proceedings of International Future Energy Electronics Conference (IFEEC) - ECCE Asia, Paper O20-5-1609, 2017.