ISSN 2186-5647

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

日大生産工（学部）　○小笠原 亮太
日大生産工　　新井 雅之

1. はじめに

エネルギーの効率的な利用が世界規模での課題となってきている．日本でも東日本大震災やその後の原子力発電所での事故を受け，エネルギー問題に配慮した技術の利用をより考える必要性が生じてきた[1]．スマートグリッド通信では，ユーザの拠点から電力消費量を送信しなくてはならないという性質上，個人の生活パターンが推定されるといったプライバシー情報流出の問題が生じてくる．家庭での電力消費量の監視実験を行った結果，高い精度でその家庭における活動パターンを推定することができたという報告も存在する[2]．従ってスマートグリッドでは，ユーザのプライバシーとなる電力消費量データを保護しながらデータを集約する通信法（安全なデータ集約）を考えなくてはならない. 本稿では先行研究であるフォールトトレランス及び差分プライバシーを考慮したデータ集約法 DPAFT を基に，スマートメータ故障時の故障情報流出を防ぐことが可能なデータ集約プロトコルについて提案する．提案プロトコルはスマートメータからゲートウェイへのデータのやり取りにおいて，ユーザ拠点に設置されたプロキシサーバを中継させる方式である．盗聴，マルウェア，同一の鍵を用いた暗号文による演算によるメッセージ解読，ノード故障情報流出に対する提案プロトコルの安全性について議論する．

2. DPAFT を用いたデータ集約

スマートグリッド通信におけるデータ集約手法である先行研究 DPAFT (Differentially Private Data Aggregation With Fault Tolerance)について概説する[1].

まず DPAFT のシステムモデルを示す．DPAFT はシステム全体の管理を担う信頼機関 TA (Trusted Authority), 集約された電力消費量データを取得し電力供給量を分析するコントロールセンタ CC (Control Center), ユーザからの電力消費量データを集約するゲートウェイ GW (Gateway), スマートメータより電力消費量を送信するユーザの集 $U = \{U_1, U_2, \cdots, U_n\}$合から構成される．

次に DPAFT のアルゴリズムについて概説する．DPAFT は 以下の 6 ステップから構成される．

(1) システム初期化
TA は公開鍵PK $= \left(N,\ G,\ g,\ h\right)$ を生成する．また，$s_0 \bullet\ s_1 + s_2 + \cdots + s_n = 1\ mod\ p$となるような$s_0$，$s_1$，…，$s_n$を生成し，$s_0$を TA，$s_1$，$s_2$，…，$s_n$を対応する$U_i$に秘密鍵として配布する．$i = 1$か$i = n$らに対し$Y_i = h^{s_0 s_i}$を計算し，CC の秘密鍵として配布する．

(2) データ集約リクエスト
CC は秘密鍵rをランダムに生成し$A_1 = g^r$，及び$A_2 = h^{s_0 r}$を GW に転送する．

(3) データ集約リクエスト中継
GW は秘密鍵tをランダムに生成し，$A_3 = A_1^t = g^{rt}$及び$A_4 = A_2^t = h^{s_0 rt}$を全てのU_iに転送する．

(4) ユーザレポート生成
各々のユーザ U_i は $C_i = A_3^{m_i} A_4^{s_i} =$

Data Aggregation on Smart Grid Communications Considering Fault Tolerance and Privacy

Ryota OGASAWARA, Masayuki ARAI

$g^{rtm_i}h^{rts_0s_i}$を計算し，GW に転送する．

(5) プライバシー保護レポート集約
GW は$C_{\gamma 1}$を計算し，CC に転送する．

$$C_{\gamma 1} = \left(\prod_{i=1}^{n} C_i\right)^{t^{-1}}$$
$$= \left(g^{r\sum_{i=1}^{n} m_i} h^{rs_0\Sigma_{i=1}^{n} s_i}\right)^{tt^{-1}}$$
$$= g^{r\sum_{i=1}^{n} m_i} h^{r}.$$

スマートメータ故障などによる$U \subset U$がユーザレポートC_iの送信に失敗した場合，GW はC_γを計算し，C_γ及びUを CC に転送する．

$$C_\gamma = \left(\prod_{U_i \in U/U} C_i\right)^{t^{-1}}$$
$$= g^{r\sum_{U_i \in U/\bar{U}} m^i} h^{rs_0\sum_{U_i \in U/\bar{U}} s^i}.$$

(6) 安全レポート読み込み
CC が$C_{\gamma 1}$を受け取った場合$C_{\gamma 1}h^{-r} = g^{r\sum_{i=1}^{n} m_i}$，を計算し，全てのユーザの電力消費量の合計値$\sum_{i=1}^{n} m_i$を得る．

CC がC_γ及びUを受け取った場合，$\overline{C_\gamma}$を計算する．

$$\overline{C_\gamma} = \prod_{U_i \in U} Y_i$$
$$= h^{s_0\sum_{U_i \in \bar{U}} s^i}.$$

その後C_γを計算し，$\sum_{U_i \in U/U} m^i$を算出する．

$$C_\gamma = \widehat{C_\gamma}(\overline{C_\gamma})^r$$
$$= g^{r\sum_{U_i \in U/\bar{U}} m^i} h^{rs_0\sum_{U_i \in U/\bar{U}} s^i} h^{s_0\sum_{U_i \in \bar{U}} s^i}$$
$$= g^{r\sum_{U_i \in U/\bar{U}} m^i} h^{rs_0\Sigma_{i=1}^{n} s_i}$$
$$= g^{r\sum_{U_i \in U/\bar{U}} m^i} h^{r}.$$

DPAFT は準同型性を持つため CC 及び TA に各々のユーザの電力消費量データを知られることなく，集約されたデータ$M = \sum_{i=1}^{n} m_i$のみ CC で解読することが可能となる．

3. 提案手法

先行研究 DPAFT は, スマートメータの故障時に端末故障情報$\hat{U}$をコントロールセンタへ送信することで耐故障性を有していた．しかしユーザとゲートウェイ間，またはゲートウェイとコントロールセンタ間の通信を盗聴することで端末故障情報が流出してしまう．本節では DPAFT を拡張させた端末故障情報流出を防ぐことが可能なデータ集約プロトコルを提案する．

3.1 プロキシサーバを用いたメッセージの代理送信

住居ユーザに設置されたスマートメータは故障しやすい装置である．DPAFT ではスマートメータの故障によるデータ送信に失敗した場合でもシステムを維持できるプロトコルである．しかしユーザ及びゲートウェイ間の通信間隔を監視することで，スマートメータの故障情報を簡単に推定できてしまう．そこで本稿では，プロキシサーバを用いたメッセージの代理送信を行う手法を採用した．暗号化メッセージにおける先行研究のデータ転送及びプロキシサーバを用いた代理転送を図 1 に示す．提案手法ではスマートメータ電力消費量メッセージmをプロキシサーバ経由でゲートウェイに送信する．プロキシサーバではスマートメータの故障の有無に関わらず，電力消費量の暗号文C_i及びノードの有効性を示すm_i'を暗号化した$V_\mathrm{i} = A_3^{m_i'}A_4^{s_i} = g^{rtm_i'}h^{rts_0s_i}$をゲートウェイへ送信する．ここで暗号文$V_\mathrm{i}$は$C_\mathrm{i}$と同じ鍵を用いた構造をもつ．本モデルでは，プロキシサーバが故障しないものとする．ノードの有効性を示すm_i'は[有効]または[無効]の値を取る．m_i'における[有効]の値および[無効]の値のしきい値に関しては, 次項で説明する．C_i及びV_iの生成法は以下の通りである．

- スマートメータが故障していない場合
  プロキシサーバは送られてきたm_iよりC_iを生成する．またm_iに[有効]の値をとり，C_i及びV_iをゲートウェイへ送信する．
- スマートメータが故障している場合
  プロキシサーバは$m_i = 0$に設定しC_iを生成する．またm_iに[無効]の値をとり，C_i及びV_iをゲートウェイへ送信する．

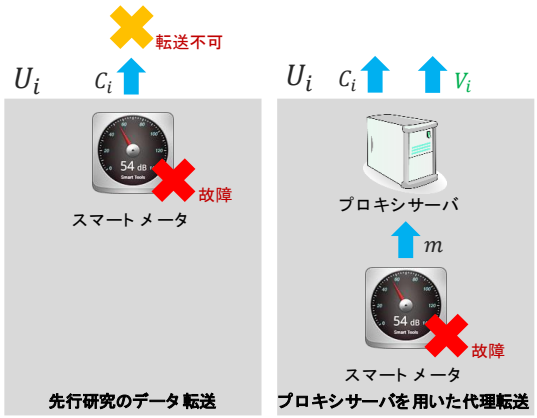

図 1 暗号化メッセージにおける先行研究のデータ転送及びプロキシサーバを用いた代理転送

提案プロトコルでは，スマートメータの故障によるユーザレポートC_i送信の失敗を考慮する必要がない．そのため先行研究で用いたC_γ及びUに関しては，本プロトコルで扱わない．

3.2 m_i'のしきい値設定

データの有効性を判定するメッセージm_i'のしきい値を設定する．データが[無効]であるときにおけるm_i'の値をα，[有効]であるときにおけるm_i'の値をβとすると$m_i' = \{\alpha, \beta\}$と表記することができる．ここでα，βのしきい値が小さいと安全なデータのやり取りをすることが出来ない．そこで以下に示すしきい値を設定した．

$m_i' = \{\alpha, \beta \mid 0 \leq \alpha < k, kn \leq \beta < k\ n+1\}$

kは任意の自然数であり，値が大きいほど安全性は高くなる．nはノード数である．

3.3 提案プロトコルのアルゴリズム

図 2 に提案プロトコルのアルゴリズムを示す．DPAFT における 2.1 項(3)データ集約中継までのシステムの動作は同じである．各ユーザU_iはC_i及びV_iを生成し，コントロールセンタへ送信する．ゲートウェイは送られたC_iと同様にV_iを集約し，$C_{\gamma 1}$と共に$V_{\gamma 1} = g^{r\sum_{i=1}^{n} m_i' h^r}$をコントロールセンタへ送信する．コントロールセンタは送られてきた$C_{\gamma 1}$より集約された電力消費量を算出すると同時に，$V_{\gamma 1}$より算出した$M' = \sum_{i=1}^{n} m_i'$をknで除算することで有効なノード数を得ることが出来る．コントロールセンタは算出した電力消費量及び有効なノード数より，電力供給エリアへの必要な電力供給量を計算することができる．

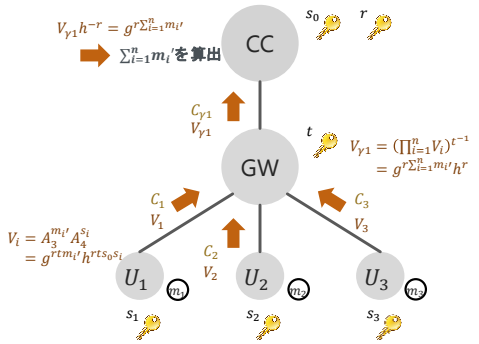

図 2 提案プロトコルのアルゴリズム

4. 提案手法のセキュリティ評価

先行研究 DPAFT で用いる電力消費量の暗号文C_i及び電力消費量を集約した暗号文$C_{\gamma 1}$に関しては安全性が既に示されている[1]．そのため，本節では DPAFT から拡張した点であるノードの有効性を示す暗号文V_i及びそれらを集約した暗号文$V_{\gamma 1}$において，盗聴，マルウェア，同一の鍵を用いた暗号文による演算によるメッセージ解読，ノード故障情報流出に対する提案プロトコルの安全性を示す．

4.1 盗聴に対する安全性

ユーザ拠点とゲートウェイ間またはゲートウェイとコントロールセンタ間の通信における第三者による盗聴攻撃が考えられる．前者においてV_iの盗聴に成功した攻撃者は，$V_i = g^{rtm_i' h^{rts_0 s_i}}$における$m_i'$の取りうる値に対する総当り攻撃を試みる．しかし提案プロトコルは選択暗号文攻撃に対する強秘匿性をもつため，攻撃者はV_iよりm_i'の値を解読することが出来ない．後者における$V_{\gamma 1}$の盗聴においても同様に，コントロールセンタにおける秘密鍵rを持っていない第三者が集約データM'を得ることは不可能である．

よって提案プロトコルは，悪意のある第三者からの盗聴に対して安全であると言える．

4.2 マルウェアに対する安全性

ゲートウェイまたはコントロールセンタにマルウェアが仕込まれた場合についての攻撃が考えられる．前者においてマルウェアはゲートウェイのデータベースに侵入し，各ユーザにおけるノードの有効性を示す暗号文V_i及びそれらを集約した暗号文$V_{\gamma 1}$を得ることが出来る．しかし，ゲートウェイ自身が各ユーザにおけるV_i及びそれらを集約した暗号文$V_{\gamma 1}$を解読できないため，マルウェアもユーザの秘密鍵s_iを持たない限り，それらのデータをマルウェアが得ることは出来ない．後者においてマルウェアはコントロールセンタのデータベースに侵入することが出来る．しかし，コントロールセンタ上で解読されたデータは各ユーザのノードにおける有効性を集約したものであり，各ユーザの電力消費量データを解読することが出来ない．

以上よりマルウェアによる提案プロトコルへのメッセージ解読攻撃に対して，各ユーザのプライバシーとなるノードの故障情報が安全であることを示せた．

4.3 ノード故障情報流出に対する安全性

先行研究DPAFTでは，ユーザ拠点ノードU_{i}に故障が生じた際にユーザレポートC_{i}をゲートウェイへ送信出来なかった場合においても，全体としてのシステムを維持することが出来る耐故障性を有していた．一方，提案プロトコルではノード故障時においてもプロキシサーバからの代理送信によって，データが送信されないことを考慮する必要がない．そのため，ユーザ拠点及びゲートウェイ間の通信盗聴によるノードの故障情報流出を防ぐことが出来る．同様の理由でゲートウェイから故障しているノードの集合を示すUをコントロールセンタへ送信する必要がない．そのため，ゲートウェイ及びコントロールセンタ間における通信の盗聴においてもノードの故障情報流出を防ぐことが出来る．

4.4 同一の鍵を用いた暗号文による演算に対する安全性

提案プロトコルで用いられる暗号文$C_{\mathrm{i}}, V_{\mathrm{i}}$または$C_{\gamma 1}, V_{\gamma 1}$が盗聴されたときについて考える．前者において$C_{\mathrm{i}} = g^{rtm_i} h^{rts_0 s_i}$及び$V_{\mathrm{i}} = g^{rtm_i{}'} h^{rts_0 s_i}$は，同様の鍵を用いた構造である．実際に$C_{\mathrm{i}}/V_{\mathrm{i}}$を計算することで，$m_{\mathrm{i}}/m_{\mathrm{i}}{}'$の値を取り出すことが出来る．しかし$m_{\mathrm{i}}{}'$のしきい値に幅をもたせたことにより，$m_{\mathrm{i}}$及び$m_{\mathrm{i}}{}'$の特定が困難となる．同様に$C_{\gamma 1}, V_{\gamma 1}$が盗聴された場合において，$C_{\gamma 1}$及び$V_{\gamma 1}$における演算より得られる値$(\sum_{i=1}^{n} m_i)/(\sum_{i=1}^{n} m_i{}')$よりユーザのプライバシーとなる情報を得ることは出来ない．

よって提案プロトコルは同一の鍵を用いた暗号文による演算に対して安全である．

5. まとめ

本研究では，先行研究DPAFTを基にスマートグリッド通信におけるスマートメータ故障時の故障情報流出を防ぐことが可能なデータ集約プロトコルの提案を行った．また，盗聴，マルウェア，同一の鍵を用いた暗号文による演算によるメッセージ解読，ノード故障情報流出に対する提案プロトコルの安全性を安全性を示した．

提案手法のモデルではプロキシサーバが故障しないという仮定に基づき議論を進めた．プロキシサーバはスマートメータより故障しづらいという点に注目し本プロトコルへ採用したが，プロキシサーバが壊れないという保障はない．プロキシサーバの故障した場合でもシステムを維持できるプロトコルを考えていく必要がある．

参考文献

[1] 独立行政法人 新エネルギー・産業技術総合開発機構[編], NEDO 再生可能エネルギー技術白書 第2版, 2014年2月.

[2] Mikhail Lisovich, Stephen Wicker, “Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems”, IEEE Proceedings on Power Systems, Vol.1, No1, March 2008.

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