V2G ネットワークにおけるセキュリティ方式に関する研究

1235053　以西 恭一郎　【 セキュリティシステム研究室 】

Research on Security Methods in V2G Networks

1235053　Isai Kyoichiro　【 Security System Lab. 】

1　はじめに

近年，電気自動車 (EV) やハイブリット電気自動車の普及が進んでおり，ほぼ確実に，将来的にはすべての個人が EV を利用することになると言われる．そこで，発電所や家庭用ソーラー, 家庭蓄電池がノードとして配電網に接続されたシステムとしてスマートグリッドが注目される．スマートグリッドとは，システム内のすべてのノード間で情報と電気エネルギーを双方向に流し，電力需要の変化に応じて効率よく制御・最適化できる送電網である．その中でも，EV が加わった Vehicle-to-Grid(V2G) ネットワークが現実的な未来として想定されている．

しかし，スマートグリッドには電力供給サービスに参加する者のプライバシー保護が必要になる．また，様々な場所に移動し，異なるネットワークに接続され，EV を使用するユーザーが異なる V2G では EV が繋がるネットワーク内の安全性と認証が重要視される．

2　V2G ネットワーク

V2G ネットワークでは，管理収集サーバによって，電力網と EV 間の通信を司る仲介役が存在し，管理収集サーバと EV 間の認証が重要となる．管理収集サーバ-EV 間は通常の Client-Server 間とは違い，両者が野外に放置されており管理者が存在しない特有のセキュリティリスクが脅威となる．

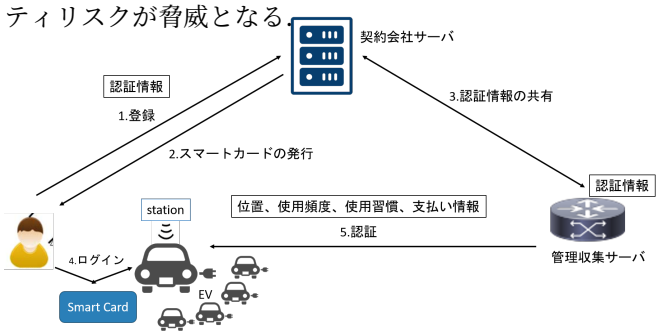

図 1　V2G ネットワークモデル

Shen ら [1] による研究では，複雑でない通信で計算コストを抑えつつその他の研究よりセキュリティ要件が高い特徴が挙げられている．しかし，既存研究ではプライバシー保護を有した認証によるセキュリティ要件は満たされているものの EV・管理収集サーバへのハードウェア攻撃，サーバ情報漏洩攻撃への対策がされていない．本研究では，SAS 認証を拡張し，これら既存研究のサーバ情報漏洩攻撃を解決しつつ，よりシンプルな通信で計算コストを抑えたプロトコルモデルを提案する．

3　目的

プライバシー保護を保証した V2G ネットワークでの認証プロトコルは，Shen らのモデルが提案されているが，EV・管理収集サーバへのハードウェア攻撃 (サイドチャネル攻撃)，サーバ情報漏洩攻撃 (インサイダー攻撃) への対策がされていない．これらの問題を解決した認証プロトコルを提案する．また，本プロトコルはいくつかの既存方式よりも少ない計算コストで通信も簡素化されていることが特徴である．

4　SAS 認証と提案プロトコル

SAS(Simple And Secure) 認証とは，ワンタイムパスワード認証方式であり，鍵配送と認証の機能を持つ．また，一方向性関数の適用回数をサーバ側で 1 回，クライアント側で 4 回にすることにより，低負荷な処理が可能である．登録フェーズと認証フェーズがあり，登録フェーズは初回のみ安全な通信路で行われ，認証フェーズはセッション毎に繰り返される．

V2G ネットワークへの拡張は，プライバシー保護のための匿名化，スマートカードでのログインを設けた三要素プロトコルとしてシーケンス図を図 2 に示す．

5　セキュリティ分析

本報告では，V2G ネットワークに必要とされるセキュリティ要件について，論理的な検証として広く知られる BAN 理論 (Burrows Abadi Needham logic) によって検証する．

また，セキュリティプロトコル検証ツールである AVISPA+SPAN によってその他の攻撃手法について意味的検証を行う．

表 1[1] では，サーバ情報漏洩攻撃に加えその他 V2G 必要とされるセキュリティ要件について示した．

表 1　セキュリティ要件

Protocols	[10]	[26]	[27]	[28]	Shen[1]	提案モデル
匿名性	×	×	○	○	○	○
前方秘匿性	×	○	○	×	○	○
リプレイ攻撃	×	×	○	○	○	○
なりすまし攻撃	×	×	○	○	○	○
盗まれたスマートカード攻撃	○	×	×	×	○	○
非同期攻撃	×	×	×	×	○	△
サーバ情報漏洩					×	○

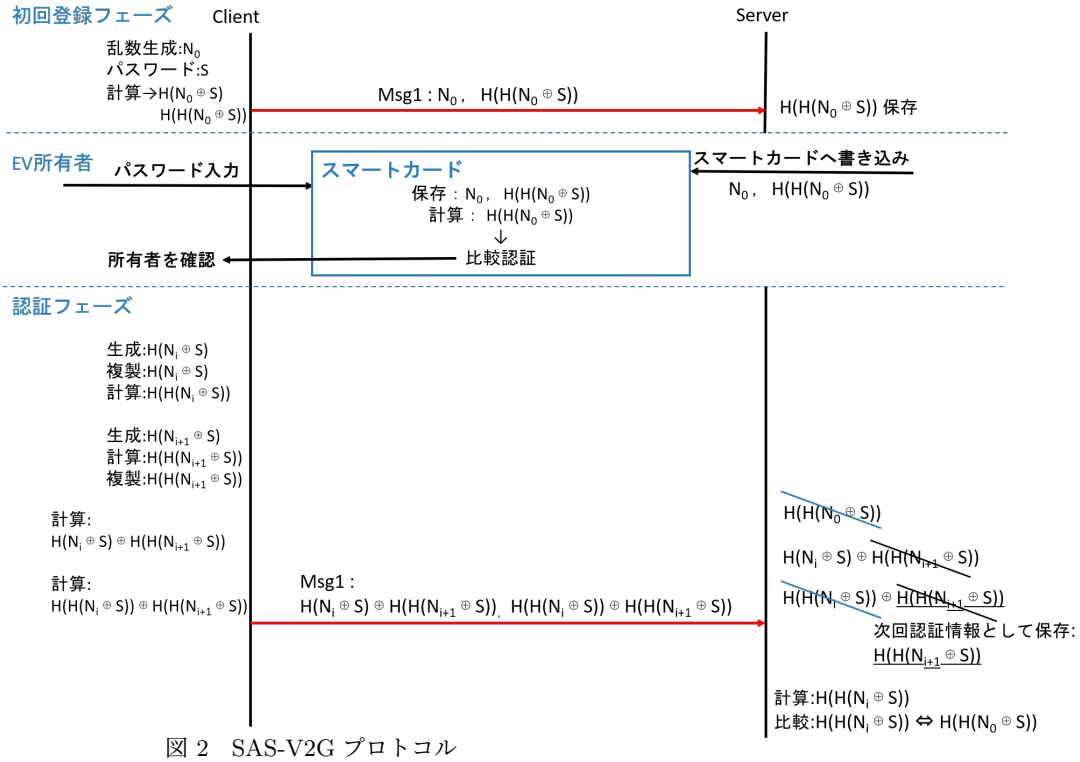

図 2　SAS-V2G プロトコル

6　パフォーマンス分析

ここでは，本プロトコルを計算コスト・通信の複雑さによって分析する[1]．米国国立標準技術研究所 (NIST) による V2G ネットワークの通信要件をもとに条件設定を行い，提案した V2G ネットワークが通信要件を満たしていることを示す．

通信の複雑さの検証は，IoT や WSN 分野で使用される ns-2 ネットワークシュミレータを用いて管理収集サーバに同時接続される EV 数を変化させてプロトコルの実用性を示す．

計算コストの比較では，[2] に基づいて，Th(一方向ハッシュ関数)，TXOR(ビット単位の XOR 演算[2])，Tm(モジュラー指数化)，Tp(楕円曲線上の点乗算) の実行に要する時間を設定し評価する．それぞれ約 0.0005 秒，0 秒，0.063075 秒，0.072311 秒としている．

表 2　計算コスト

Protocols	[10]	[26]	[27]	[28]	Shen[1]	提案モデル
client	7Th+4TXOR	3Tm+9Th	4Tp+3Tm		4Th+3TXOR	4Th + 5TXOR
server	5Th+6TXOR	2Tm+6Th	2Tp+1Tm		5Th+4TXOR	1Th
Total	13Th+10TXOR	5Tm+15Th	6Tp+4Tm	約 0.0158(s)	9Th+7TXOR	5Th + 5TXOR
second(s)	0.006	0.322875	0.686166	約 0.0158	0.0045	0.0025

同時に多数の EV が接続され，大きな負荷が予想される管理収集サーバ側での一方向ハッシュ関数を 1 回としたことで，既存方式よりも効率的であることが示された．

[1]表 1・表 2・表 3 の比較論文は参考文献 [1] の References である
[2]TXOR と文字列連結演算の実行に要する時間は，他のものに比べて無視できるため比較では無視している．

また，本プロトコルの通信の複雑さは，交換されたメッセージ数において効率的であると言える．提案プロトコルは，登録フェーズでの通信を含めても $1 + 1n$ となりシンプル化されている．(ここでの n は管理収集サーバに接続される EV の数)

表 3　通信の複雑さ

Protocols	[10]	[26]	[27]	[28]	Shen[1]	提案モデル
Message exchange	2 + 6n	6n	2 + 12n	5n	4n	1n

7　考察・まとめ

第五章・第六章の分析等において V2G ネットワークの認証におけるその他プロトコルとの優位性を示した．また，セキュリティシュミレータ・ネットワークシュミレータにより実用性も示す．

展望として，プロトコルの登録フェーズによって入力された情報は後に書き換えることができないため，変更時にスマートカードを再発行・再契約しなければいけない問題がある．セキュリティ要件を満たしつつ改良する余地が見られる．また，同様の軽量プロトコルとのコスト比較を行う必要がある．

参考文献

[1] J. Shen, T. Zhou, F. Wei, X. Sun and Y. Xiang, "Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2526-2536, Aug. 2018, doi: 10.1109/JIOT.2017.2775248.

[2] Xie, Qi, et al. "Privacy-preserving mobile roaming authentication with security proof in global mobility networks." International Journal of Distributed Sensor Networks 10.5 (2014): 325734.