7ZD-07

同期問題を考慮したSAS-L2を用いたRFID認証プロトコル

清水　健吾† 　王　森レイ† 　甲斐　博† 　高橋　寛† 　清水　明宏‡
愛媛大学† 　高知工科大学‡

1. はじめに

RFID (Radio Frequency Identification)は，無線通信を利用して RFID リーダと RFID タグの間でデータを交換する技術である．RFID では RFID タグに書き込まれる情報の改ざんへの対策として安全な認証機能の必要性が指摘されている[1]．RFID タグの安全性を高めるために疑似乱数やハッシュ関数を用いた方法などが検討されているが，演算能力の低い IoT 機器では複雑な認証機能を具備することが困難である．

IoT 機器向けの認証方式 SAS-L2 (Simple And Secure password authentication protocol, Light processing version 2) [2] は，IoTエッジデバイスの処理性能の不均衡問題を考慮し，クライアントでは極めて小さい処理負荷で暗号鍵の配送が実現できるワンタイムパスワード認証方式である．

本研究では SAS-L2 を RFID システムに応用し RFID における複雑な演算回路を必要としない認証方式を提案する．さらに，提案プロトコルの同期問題と DoS 問題に関する脆弱性に対して，Sun ら[5]の認証方式を参考にして，RFID における専用の演算回路を必要とせず同期問題と DoS 問題への耐性強化方法を提案する．

2. SAS-L2 認証方式

SAS-L2 認証方式はワンタイムパスワード認証方式の一つである．従来の SAS-2 認証方式と異なり，クライアントで行う演算は排他的論理和 XOR と加算のみである．特にクライアントでハッシュ関数を使用しないという点において，クライアントでの演算負荷を軽減できる．

SAS-L2 では，初回登録情報として，サーバ側で，パスワード S，秘匿情報 M_1，乱数 N_1 を登録する．ユーザ側では，秘匿情報 M_1，認証情報 $A_1 = h(S \oplus N_1)$ を登録する．ここで h はハッシュ関数を表す．

n 回目の認証において，サーバで乱数 N_{n+1} を生成し，$A_n = h(S \oplus N_n)$，$A_{n+1} = h(S \oplus N_{n+1})$，$\alpha = A_{n+1} \oplus A_n \oplus M_n$ を計算する．サーバは α をクライアントに送信しクライアントで α から A_{n+1} を求める．次にクライアントは $\beta = A_n + A_{n+1}$ を計算しサーバに β を送信する．サーバで $A_n + A_{n+1}$ と β が一致すれば認証が成功する．

Synchronized RFID authentication protocol using SAS-L2
†Kengo Shimizu, Senling Wang, Hiroshi Kai, Hiroshi Takahashi, Ehime University
‡Akihiro Shimizu, Kochi University of Technology

3. SAS-L2 を用いた RFID 認証プロトコル

RFID 認証プロトコルに関する研究では，一般に，サーバ，RFID リーダ，RFID タグの 3 者モデルでデータが送受信される．RFID リーダと RFID タグの間は，安全が確保されておらずデータの漏洩や改ざんの可能性がある通信路と仮定される．一方で，サーバと RFID リーダの間の通信路は安全であると仮定される．

我々が [3] で提案した SAS-L2 を用いた RFID 認証プロトコルの概略を図 1 に示す．

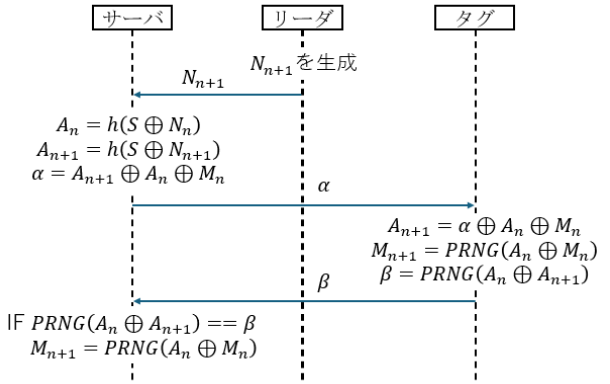

図 1 SAS-L2 を用いた RFID 認証プロトコル

この方式は次の同期問題と DoS 問題に脆弱である．

同期問題： n 回目の認証に対して攻撃者が β の通信を切断した場合，RFID タグでは A_{n+1}, M_{n+1} を更新するが，サーバでは情報を更新しない．このため次回の RFID タグの認証ができなくなる．

DoS 問題： 攻撃者が α を偽造した場合，$A_{n+1} = \alpha \oplus A_n \oplus M_n$ により，間違った認証情報 A_{n+1} に更新される．このため次回以降の RFID タグの認証ができなくなる．

そこで Sun らの認証方式を参考に，同期問題を考慮した SAS-L2 を用いた RFID の認証プロトコルを提案する．

4. 同期問題を考慮したSAS-L2を用いたRFID認証プロトコル

中原・清水ら [4] はSAS-2プロトコルについて過去の認証情報を保存することにより同期問題を解消している．Sunらの方式 [5] ではRFIDシステムについてチャレンジレスポンスによる認証方式を提案し，中原らの方式と同様にサーバに過去の認証情報を保存することを行う．

本研究では，Sunらの方式を参考に過去の認証情報を保存することを検討し，図2のようなRFIDシステムにおける認証方式を提案する．

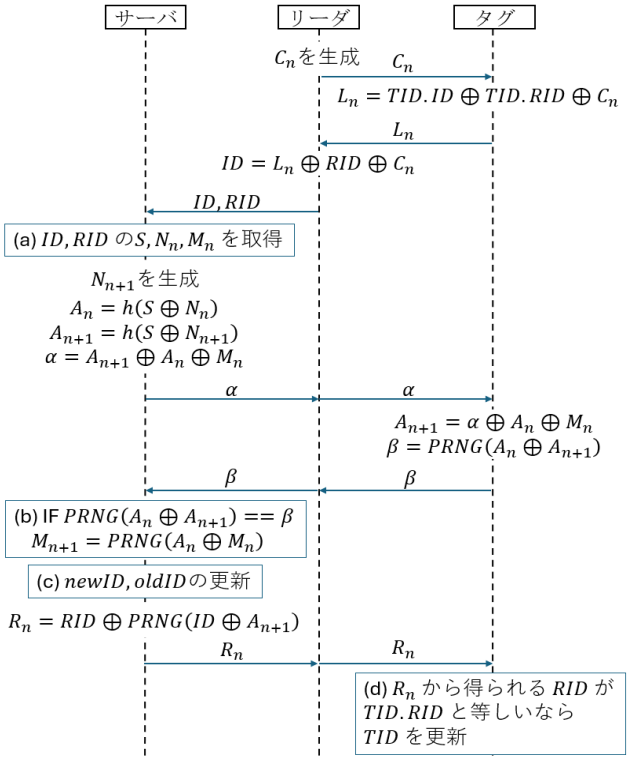

図2 同期問題を考慮したSAS-L2を用いたRFID認証プロトコル

初回登録情報として，サーバでは$newID = oldID = (ID, RID, S, N_1, M_1)$，リーダで RID，タグで $TID = (ID, RID, A_1, M_1)$ を登録する．

図2は n 回目の認証手順を示しており，まずリーダで乱数 C_n を用いて，タグからサーバに ID, RID を送信する．

図2(a)では，ID をもとに $newID$ からSAS-L2の認証情報 S, N_n, M_n を取得する．もし図2(b)で β との比較が失敗した場合は，過去に同期問題が起きた可能性がある．その場合は $oldID$ から S, N_n, M_n を取得し，再度SAS-L2の認証を試行する．$newID, oldID$ のどちらの情報でも図2(b)で失敗する場合は認証不成立である．

図2(c)では，$newID$ から認証情報を取得した場合は，

$$oldID = newID$$
$$newID = (ID, RID, S, N_{n+1}, M_{n+1})$$

として $oldID, newID$ を更新する．もし $oldID$ から認証情報を取得した場合は，

$$newID = (ID, RID, S, N_{n+1}, M_{n+1})$$

として更新する．但し，この場合は $oldID$ は更新しない．

提案手法では同期問題とDoS問題を以下のように防ぐことができる．

同期問題：攻撃者が β の通信を切断した場合 $newID, oldID, TID$ は更新されない．また攻撃者が R_n の通信を切断した場合，$newID$ は更新されるが，$oldID$ で過去の認証情報を記録している．そのため次回認証においては $oldID$ での認証が可能である．

DoS 問題：攻撃者が α を改ざんした場合，図2(b)で認証不成立になるのでタグの認証が拒否され，TID は更新されない．β が改ざんされた場合も同様である．R_n が改ざんされた場合は，サーバ側で $newID$ は更新されるが，$oldID$ で過去の認証情報を記録している．次回認証では $oldID$ での認証が可能である．

5. まとめ

本稿では，同期問題を考慮したSAS-L2を用いたRFID認証プロトコルの提案を行った．提案方式では，Sunらの方式と同程度の安全性を有しながら，RFIDタグ側でハッシュ関数を利用しないでワンタイムパスワード認証方式で認証を行うことができる．

今後の課題は，RFIDシステムの実装による計算負荷の評価などがあげられる．

参考文献

[1] Android不正アプリによるRFIDプライベートカード改ざんが南米で発生，TRENDMICRO, https://blog.trendmicro.co.jp/archives/10432 （2024年1月1日参照）

[2] 清水明宏，認証システム，認証装置，認証法，およびプログラム，特許7119071号，2022.

[3] 清水健吾, 甲斐博, 王森レイ, 高橋寛, 清水明宏, SAS-L2を用いたRFIDシステムの認証方式, 令和5年度電気・電子・情報関係学会四国支部連合大会, 2023.

[4] 中原知也，辻貴介，清水明宏，SAS-2認証方式の同期問題に関する検討，信学技報，Vol.104, No.714, pp.83-87, 2005.

[5] Haowen Sun, Peng Li, He Xu, Feng Zhu, An Improvement RFID Security Authentication Protocol Based on Hash Function, Springer International Publishing AG, part of Springer Nature 2019, L. Barolli et al. (Eds.): IMIS 2018, AISC 773, pp. 375–384, 2019.