IoT 環境における SAS-L の適用に関する研究

1200284　池 内　聖　【 セキュリティシステム研究室 】

1　はじめに

現在，IoT 環境においてパフォーマンス上の観点から UDP が多用されている [1]．UDP を用いて安全な通信を実現する方式として DTLS over UDP が挙げられる．DTLS は TLS と同様のセキュリティを確保する目的で設計されている．この方式では，認証及び鍵共有に計算量が大きい公開鍵暗号方式を利用しているため，処理時間が増加する．そのため，IoT デバイスの中でも CPU やメモリのリソースに制限のある小型デバイスでは処理負荷による影響が大きく，処理時間が増加するという問題がある [2]．そこで本稿では，小型デバイスに適した方式として SAS over UDP with ARQ を提案する．また，クライアント環境における各方式の処理時間を比較し，有用性について検証する．

2　提案方式

2.1　SAS-L

SAS-L は，ワンタイムパスワード認証方式であり，認証情報が認証の度に変わるため反射攻撃や中間者攻撃などによるなりすましに対して高い耐性を持っている．また，一方向性関数の適用回数をサーバ側で 0 回，クライアント側で 1 回にすることで，低負荷な処理を実現している．よって，鍵配送と相互認証を同時に実現した方式であるため，IoT 環境に適した認証方式である．SAS-L は，登録フェーズと認証フェーズに分かれて構成されている．

2.1.1　登録フェーズ

登録フェーズでは，クライアント側で生成した初回認証情報 A_1 を安全な手段でサーバと共有する．

2.1.2　認証フェーズ

認証フェーズでは，認証情報を用いてクライアントとサーバ間で相互認証及び共通鍵の共有を行い，認証情報の更新を行う．

2.2　ARQ

ARQ は，信頼性の高い通信を実現させるための誤り制御手法である．本研究では，信頼性が担保されていない UDP 上における通信を想定しているため ARQ プロトコルの中でも最も単純な手法である Stop-and-wait ARQ を用いる．この方法により再送処理を行うことができ，信頼性の高い通信を実現できる．

2.3　SAS over UDP with ARQ の流れ

SAS over UDP with ARQ におけるセッションの確立を図 1 に示す．

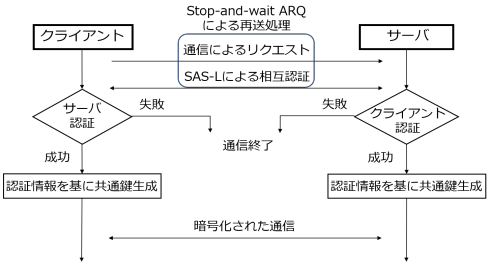

図 1　SAS over UDP with ARQ におけるセッションの確立

3　実験環境及び実験結果

実験環境としてクライアント側には低リソースな IoT デバイスを想定して，超小型かつ安価な ARM コンピュータである Raspberry Pi Zero WH，サーバ側には汎用 PC を使用する．DTLS の暗号スイートは，DTLS v1.2 ECDHE-ECDSA-AES128-CCM-8 を使用する．

本実験では，クライアント環境における各方式の認証及び鍵共有までの処理を 10 回行い，表 1 に平均処理時間及び倍率を示す．実験結果として，提案方式の平均処理時間は既存方式と比較して約 215 分の 1 となった．

表 1　各方式における平均処理時間と倍率

方式	平均処理時間 [ms]	倍率
提案方式 (SAS)	0.6679	1 倍
既存方式 (DTLS)	143.8962	約 215 倍

4　まとめ

本稿では，小型デバイスにおける安全で軽量な通信方式として SAS over UDP with ARQ を提案した．提案方式は既存方式よりもクライアント側の処理負荷が小さいため，小型デバイスへの有用性を示すことができた．今後の展望として，実際の IoT 環境での実験が課題として挙げられる．

参考文献

[1] AnnaGerber，“モノのインターネットの中ですべてのモノを接続する”，https://www.ibm.com/developerworks/jp/iot/library/iot-lp101-connectivity-network-protocols/index.html，2020 年 2 月 1 日閲覧．

[2] U. Banerjee，et al.，“An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for End-to-End Security in IoT Applications”，IEEE International Solid - State Circuits Conf. (ISSCC)，feb 2018，pp.42–44，2018.