音声通信の遅延軽減に関する研究

1250380　山内 天晴　【 セキュリティシステム研究室 】

1　はじめに

近年，IoT 機器はリアルタイム音声通信技術はビデオ会議や音声アシスタントをはじめ，IoT 機器間での双方向通信など多岐にわたる分野で利用されている．このようなリアルタイム音声通信において，通信内容を保護するためにもセキュリティは重要な課題である．しかし，IoT 機器の中には性能が限られているものも多く，適切なセキュリティ対策が困難であると指摘されている [1]．このような背景から IoT 機器における音声通信のセキュリティを強化しつつ，処理負荷を軽減することでリアルタイム性を確保することが求められる．

2　従来の方式

従来の方式には楕円曲線暗号と SAS-2 がある．

楕円曲線暗号（Elliptic Curve Cryptography, 以下 ECC）は，RSA(Ron Rivest, Adi Shamir, and Leonard Adleman) と比較して短い鍵長で同等のセキュリティを提供する公開鍵暗号方式であり，TLS/SSL プロトコルの鍵交換や IoT 機器のセキュリティ確保に広く用いられている．また，SAS-2(Simple And Secure password authentication protocol,ver.2) は「携帯電話における VoIP 暗号化通信の提案 [2]」において，非常に軽量でリアルタイム性を確保することができる鍵交換方式であることが示された．

3　提案方式

本研究では，より処理負荷が小さい，SAS-L2(Simple And Secure password authentication protocol, Light-processing version type-2)[3] を用いた音声通信時の鍵交換方式について提案する．SAS-L2 も SAS-2 同様にワンタイムパスワード認証方式を応用し，鍵交換に利用できる．SAS-L2 では被認証側で擬似乱数関数，一方向性変換関数の適用が不要である．SAS-2 では被認証側で疑似乱数関数 1 回，一方向性関数を 2 回適用しなければならず，SAS-L2 はより軽量な鍵交換方式であるといえる．

4　実験環境

実験には，M5Stick C plus という小型の IoT 機器を用いた．サーバー側では Python 環境 (Macbook) を使用し，クライアント側は M5Stick C plus 上で MicroPython を用いた．通信プロトコルには TCP/IP を使用し，サーバー・クライアント間で鍵交換を毎パケットごとに行い，音声データを AES 暗号化して送信する形で評価を行った．

5　実験結果

実験結果を表 1 に示す．

表 1　各鍵交換方式の処理時間比較

方式	KE(ms)	Delay(ms)
SAS-L2	86.223	268.7575
SAS-2	113.182	328.5083
ECC	4342.436	6650.2459

KE: 鍵交換平均処理時間，Delay: 全遅延平均時間

SAS-L2 の鍵交換時間は平均 86.223ms であり，SAS-2 の平均 113.182ms と比べると約 23.8%の鍵交換処理時間を削減した．また，ECC では平均 4342.436 であり約 98.0%の鍵交換処理時間を削減した．どちらと比較しても SAS-L2 がよりリアルタイム性を保証する上で適している．ITU-T G.114 の勧告によると，音声通信における遅延は片方向で 400ms 以内が望ましいとされている [4]．SAS-2，SAS-L2 ともにこの基準を満たしているが，ECC では鍵交換処理のみでこの基準を大幅に超えており，性能が限られている機器では適してはいない．

6　まとめ

本研究では，IoT 機器向けのリアルタイム音声通信に適した低負荷な鍵交換方式 SAS-L2 を提案し，従来の方式と比較した．その結果 SAS-L2 では SAS-2，ECC よりも鍵交換処理時間が短く，性能が限られている機器であってもリアルタイム性を確保することができる．

今後の課題として，SAS-L2 に適した鍵交換のタイミングを検討する必要がある．

7　参考文献

参考文献

[1] 総務省,”情報通信白書”,2023,https://www.soumu.go.jp/johotsusintokei/whitepaper/r05.html, 2024 年 2 月 1 日閲覧.

[2] 小野豊, ”携帯電話における VoIP 暗号化通信の提案”, 2009/2/13

[3] 溝口洸熙 and 清水明宏, ”IoT 環境に適したワンタイムパスワード認証方式,” 電子情報通信学会 信学技報, vol. 124, no. 257, LOIS2024-43, pp. 112–117, 2024.

[4] International Telecommunication Union, ”Recommendation ITU-T G.114: One-way transmission time”,2003 ,https://www.itu.int/rec/T-REC-G.114, 2024 年 2 月 1 日閲覧.