セキュアグループ通話システムの実現に向けた SAS Phone の拡張

1215096　藤田 寛泰　【 セキュリティシステム研究室 】

An Extension of SAS Phone to Realize Secure Group Voice Communication System

1215096　Hiroyasu FUJITA　【 Security Systems Lab. 】

1　はじめに

ワークスタイルの多様化により，テレワークの実現に向けた地理的制約にとらわれない遠隔コミュニケーションシステムの必要性が増している．テレワークでは，自宅・サテライトオフィス・本社オフィス等さまざまな場所で，2 者以上の間でコミュニケーションが行われる．

VoIP は，インターネットを介した音声通話を提供する技術であり，従来の専用線を用いる方法と比較し安価に運用できる点からテレワークとの親和性が高い．一方で，第三者による盗聴のリスクが懸念されるため TLS などによるセキュリティ対策が必要である．

TLS は広く普及した技術ではあるが，通信セッション中で利用する暗号鍵は固定なため，セッションが長期化する VoIP アプリケーションなどでは暗号解析攻撃 [1] により鍵の危殆化が懸念される．この攻撃への対策として鍵の更新を考慮した音声通話システム SAS Phone [2] が提案されている．SAS Phone は， SAS 鍵配送プロトコルを用いて鍵の更新を行うが，このプロトコルにより 2 者間の通話に限定されるためグループ通話が行えない．そこで本稿では，SAS グループ鍵配送プロトコルを提案し，それを用いることでセキュアグループ通話システムとして SAS Phone を拡張する．

2　SAS 鍵配送プロトコル

SAS Phone で利用される SAS 鍵配送プロトコルは，Simple And Secure password authentication protocol (SAS) [3] を鍵配送に応用した方式である．SAS の操作は主に排他的論理和とハッシュ関数で構成されるため，公開鍵暗号方式をベースとした手法と比較し極めて処理負荷が小さい．そのため，音声通話における鍵更新処理に適していると考えられる．しかし，2 者間での鍵配送のみを想定しているため，グループ間通信には適用できない．また，通信路上でパケットロスが発生することでエンドユーザ間で鍵の同期が取れない可能性がある．

3　提案方式

本稿では，SAS グループ鍵配送プロトコルを示し，それを用いることで SAS Phone の拡張を行う．

3.1　SAS グループ鍵配送プロトコル

提案プロトコルは，登録フェーズと鍵配送フェーズで構成される．以下では，鍵配送フェーズについて述べる．

3.1.1　鍵配送フェーズ

鍵配送フェーズでは，グループ間で共有している情報をもとに新たな情報を共有し，それをシードとして鍵を生成する．一連の通信は，コントローラと呼ばれるグループの代表者によって制御される．提案プロトコルの鍵配送フェーズにおける通信フローを図 1 に示す．

図 1 の通信開始時点で，グループ全体で今回認証情報 A_C を共有している．これにより各メンバは，受信した α, β から次回認証情報 A_N を得ることができる．その後，コントローラは適切なメンバしか計算できない γ を受信した場合に限り， $update\ message := ID_C, \gamma_C$ をメンバへブロードキャストする．その後，メンバとコントローラは次のように鍵の更新と生成を行う．

$$\begin{aligned} EK_B &= EK_C \\ EK_C &= KDF(ID_1, ID_2, ..., ID_i, A_C, A_N) \end{aligned}$$

EK_C, EK_B, KDF はそれぞれ暗号鍵，バックアップ用の鍵，鍵導出関数を表す．EK_B は，鍵更新後に古い鍵で暗号化されたデータを受信する可能性がある場合に利用される．また，KDF としては，SHA や AES などのアルゴリズムを利用できる．

従来の SAS 鍵配送プロトコルでは，図 1 の示す箇所でパケットロスが起きた場合に同期ずれとなる．一方，提案プロトコルは γ_3 を受信できない場合に再送処理を行うことでこれに対処する．

3.2　SAS Phone の拡張

従来の SAS Phone では，音声転送フェーズにて鍵更新と音声パケットの転送を逐次的に実行している．これは，鍵更新時にパケットロスが発生しない前提に基づく．現実的には，パケットロスは発生し，鍵配送の遅延が増大する．この結果，通話品質の低下を招くことが予想され，これはグループ通話では顕著である．そこで，提案プロトコルに基づく鍵更新は，図 2 のように音声パケットの転送と並列に実行する．

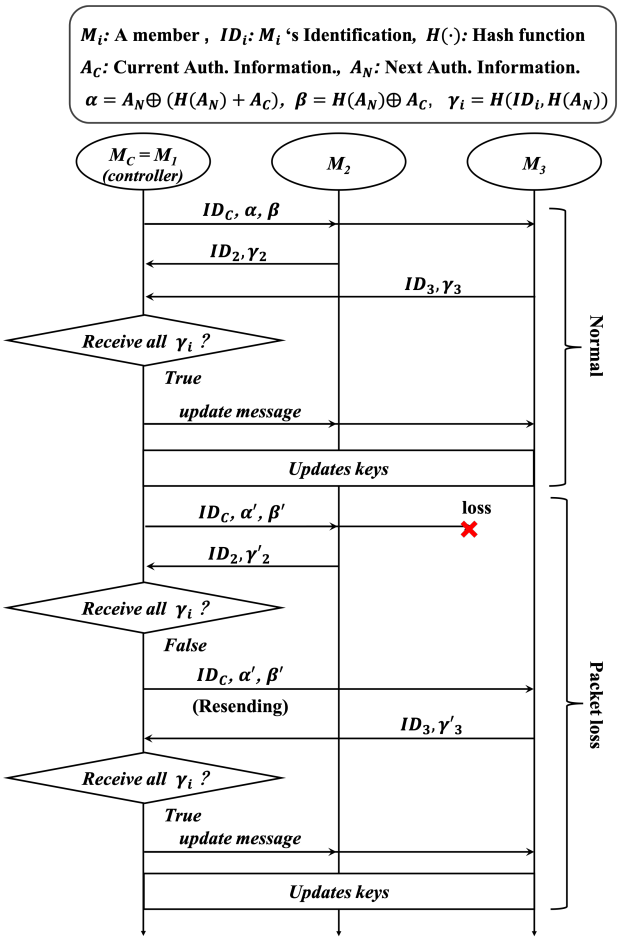

図 1　鍵配送フェーズにおける通信フロー

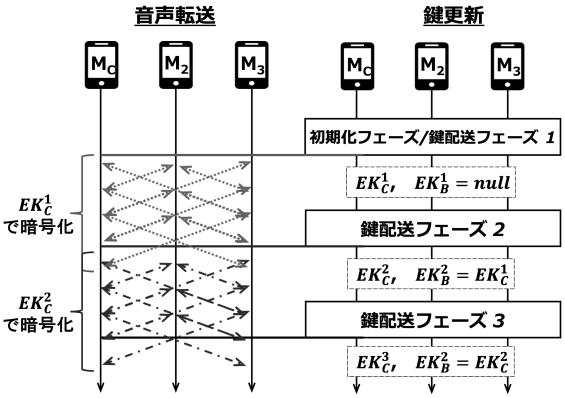

図 2　音声転送と鍵更新

鍵更新処理の前後で 2 つの鍵で暗号化されたパケットが混在するが，暗号鍵のバックアップ EK_B により更新後も古いパケットにアクセスすることが可能になる．

4　SAS グループ鍵配送プロトコルの評価

4.1　Denial of Service (DoS) 攻撃への耐性

本稿における DoS 攻撃は，攻撃者が通信データを再利用することで鍵の整合性を破る攻撃を指す．提案プロトコルが DoS 攻撃への耐性がない場合，メンバ間で鍵の同期ができず機密性や認証を提供する暗号サービスを利用できなくなる．DoS 攻撃は，メンバ M_i がパケットロスにより α, β の受信に失敗した場合，攻撃者は γ_i を計算することで実行できる．その計算には，他のメンバ M_j が送信した γ_j または α, β を利用して $H(A_N)$ を入手する必要がある．前者を利用する場合は，ハッシュ関数の持つ原像計算困難性から計算量的に困難である．また，後者の場合に関しても，グループ間で共有する A_C を用いた暗号化により困難である．よって，提案プロトコルはこの攻撃への耐性を有する．

表 1　パフォーマンス比較結果 ($l_i = |ID|, l_a = |H(\cdot)|$)

	メッセージサイズ	内部処理			
		送信回数		ハッシュ関数の回数	
		M_C	M_i	M_C	M_i
GD	$l_i + 2l_a$	1	0	2	1
GKD	$(n+1)l_i + (n+3)l_a$	2	1	$n+1$	2

4.2　パフォーマンス比較

コントローラ M_C を除くグループのメンバ数を n としたときの，SAS 鍵配送 (GD) と 提案プロトコル (GKD) の比較結果を表 1 に示す．グループ通信への対応により，提案プロトコルでは，メッセージサイズとハッシュ関数の回数がメンバ数に比例する．大規模なグループでは，各メンバからの返信が M_C のネットワークに集中するため，輻輳による通信のオーバヘッドの増加が懸念される．一方，小規模グループの場合は，メンバ識別子や認証情報は数十バイト程度と小さいことから，オーバヘッドによる影響は小さいものと考えられる．したがって提案プロトコルは，小規模グループにおける鍵配送に適している．

5　まとめ

本稿では，SAS Phone でグループ通話を実現することを目的に，SAS グループ鍵配送プロトコルを提案し，小規模グループにおいて通話を可能とする拡張を行った．今後の課題として，SAS Phone の実装を行い QoS の観点で鍵更新処理を評価することが挙げられる．

参考文献

[1] G. V. Bard, “A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL,” IEEE ICSC, INSTICC Press, 2006.

[2] 幸地勇明, 他, “携帯端末向けセキュア VoIP システムの提案,” 信学技報, vol. 111, no. 286, LOIS2011-48, pp. 135-140, 2011 年 11 月.

[3] T. Tsuji and A. Shimizu, “A One-Time Password Authentication Method for Low Spec Machines and on Internet Protocols,” IEICE Trans. COMMUN, vol. E87-B, no.6, pp. 1594—1600, 2004.