6X-8

接続妨害攻撃を考慮したSIPセッション確立方式

前田　紗苗[†]　　木村　成伴[‡]　　海老原　義彦[‡]

[†]筑波大学 情報学群情報メディア創成学類　　[‡]筑波大学 大学院システム情報工学研究科

1. はじめに

近年，インターネット上で提供される音声通話サービス VoIP（Voice over Internet Protocol）が広く普及するのに伴い，VoIP の通話セッションを管理するプロトコル SIP（Session Initiation Protocol）が重要な役割を果たしている．しかし，SIP のメッセージはテキスト形式であり，その解析には時間がかかるため，これに加えて，暗号化などの処理をするのが難しい[1]．このため，SIP ではすべてのメッセージが平文でやりとりされることから，悪意のある第三者にメッセージを盗聴され，成りすましなどの攻撃を受ける可能性がある．

この問題を解決するため，本研究室では，SIP の不正切断問題を防ぐためのセッション確立方式を提案している[2]．これに加えて，本論文では，SIP セッション確立を第三者によって不正に妨害される接続妨害攻撃を，SIP メッセージの一部のみを暗号化することによって防ぐ，SIP セッション確立方式を提案する．

図 1 SIP セッション確立のシーケンス

SIP Session Initiation Method to Prevent Session Blocking Attacks

†Sanae Maeda, College of Media Arts, Science and Technology, School of Informatics, University of Tsukuba

‡Shigetomo Kimura and Yoshihiko Ebihara, Graduate School of Systems and Information Engineering, University of Tsukuba

2. SIP における接続妨害攻撃

図 1 を用いて，SIP セッションを確立するための既存のシーケンスを説明する．

図において，左端にある SIP 端末 UA1 が，プロキシサーバを介して，右端の SIP 端末 UA2 とセッションを確立しようとしていると仮定する．そのために，まず，UA1 は INVITE リクエストをプロキシサーバに送信し，プロキシサーバはこれを UA2 に転送する．UA2 は暫定レスポンスである 100 Trying と 180 Ringing を，プロキシサーバを介して UA 1 に返す．UA2 のユーザが着信すると，UA2 は成功レスポンスである 200 OK を UA1 に送り，UA1 は UA2 に ACK を返す．以上のやりとりにより，SIP セッションが確立する．これ以降，セッションが切断されるまで UA1 と UA2 は RTP（Real-time Transport Protocol）などを使って，音声データをやりとりする．

相手が着信しないなどの理由で，発信を取り消す場合のシーケンスを図 2 に示す．UA1 は，UA2 から 200 OK が送られる前に，CANCEL リクエストを UA2 に送る．これに対し，UA2 は 200 OK CANCEL を返し，さらに，INVITE リクエストに対する失敗レスポンスとして，487 Request Terminated を UA1 に送る．最後に，UA1 が ACK を UA2 に送り，発信取り消しが完了する．

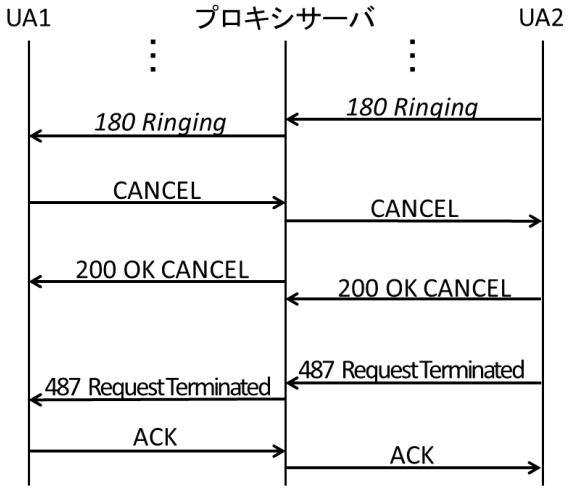

図 2 発信取り消しのシーケンス

第 1 章で述べた通り，SIP のメッセージは全て平文でやりとりされる．そのため，攻撃者が，

INVITE リクエストと 100 Trying レスポンスを盗聴し，UA1 と UA2 のアドレスやセッションの識別子などの情報を手に入れることが可能になる．さらに，UA1 になりすました偽装 CANCEL メッセージを UA2 に送信することで，UA1 の意思に関わらず，二者間のセッションの確立を取り消すことが可能になる．以下では，この攻撃を「接続妨害攻撃」と呼ぶ．

この問題を解決するため，SIP を規定する RFC3261 では，INVITE リクエストと同じ経路で CANCEL リクエストが送られていることを確認するように求められている．しかし，パケットが通過した経路を確認するのは難しいため，接続妨害攻撃を防ぐのは困難である．

3. 提案方式

本章では，SIP メッセージの一部のみを暗号化することによって接続妨害攻撃を防ぐ SIP セッション確立方式を提案する．提案方式のシーケンスを図 3 に示す．提案方式では，予め，UA1 とプロキシサーバの間で共有鍵 Pa を，UA2 とプロキシサーバの間で共有鍵 Pb を共有していることを前提とする．

まず，UA1 は，ランダムな文字列 N と，このセッションでのみ UA1 とプロキシサーバで共有するセッション鍵 Sa を生成する．UA1 は，セッション確立の際，N と Sa を Pa で暗号化した $(N,Sa)_{Pa}$ を，INVITE リクエストに追加して送信する．プロキシサーバは，このメッセージを Pa で復号し，N と Sa を取り出す．そして，UA2 とプロキシサーバで共有するセッション鍵 Sb を生成し，N と Sb を Pb で暗号化した $(N,Sb)_{Pb}$ を，INVITE リクエストに追加して UA2 に送信する．UA2 は，このメッセージを Pb で復号し，N と Sb を取り出す．

UA1 が発信を取り消す際は，N を Sa で暗号化した $(N)_{Sa}$ を CANCEL リクエストに追加して送信する．プロキシサーバは，受け取ったメッセージを Sa で復号し，N を取り出す．この N が INVITE リクエストに追加された N と等しい場合のみ，CANCEL リクエストを受け付ける．そして，N を Sb で暗号化した $(N)_{Sb}$ を追加した CANCEL リクエストを UA2 に送る．同様に，UA2 はこのメッセージを Sb で復号し，取り出した N が INVITE リクエストに追加された N と等しい場合のみ，CANCEL 処理を実行する．

悪意ある第三者は文字列 N の値を知り得ない．このため，UA2 に偽装 CANCEL リクエストを送信しても，このリクエストは受理されず，発信を取り消すことはできない．

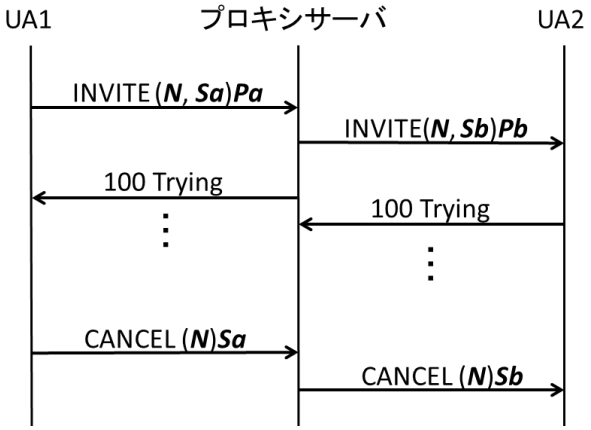

図 3 提案方式のシーケンス

4. 評価実験

提案方式の有効性を確認するため，以下の評価実験を行う予定である．これらの実験ではプロキシサーバは用いず，2 台の端末（FreeBSD 8.1-RELEASE）に SIP クライアント Linphone-3.2.1 を導入して，これらの間で直接通信を行う．暗号化アルゴリズムは AES（鍵長 128 ビット）を使用し，ランダムな文字列 N は 14 バイト，共有鍵とセッション鍵は 16 バイトとする．

上記環境の下，提案方式の実装が正しく動作することを確認するため，接続妨害攻撃実験を行う．本実験では，SIP で用いるセッション ID を固定する．そして，予め生成した偽装 CANCEL リクエストを，セッション確立中の着信側端末に送り，発信が取り消せないことを確認する．

次に，従来方式，提案方式，メッセージを全て暗号化する方式のそれぞれについて，通常の SIP セッション確立，及び発信取り消しを行った場合の，INVITE リクエストを送ってから発信側に最終応答（前者は 200 OK，後者は 487 Request Terminated）が返るまでの平均時間を測定する．これにより，提案方式の平均時間は，従来方式よりもやや大きくなるものの，メッセージを全て暗号化する方式よりは十分に小さくなることを予想している．

参考文献

[1] J. Yin, “Session Initiation Protocol Benchmark Suite,” Master’s Thesis, Delft University of Technology, 2004.

[2] 田中真也，木村成伴，海老原義彦，“SIP セッションの不正切断問題の検証と安全な SIP セッション確立方式の提案とその評価，” 情報処理学会第 50 回全国大会，5ZC-10, pp. 3-471-3-472, 2010.