L-018

大規模ネットワークに対応した安全な VoIP 通信の実現方式 - 拡張 TWP 方式 -

高原尚志[†1]

TWP Method for Large Scale Network - Extended TWP Method -

HISASHI TAKAHARA [†1]

1. はじめに

近年、インターネットを利用した音声通信、いわゆる VoIP 通信が広く普及している。誰でもが参加できるインターネットにおいては、音声通信を提供するプロバイダが必ずしも信頼できるとは限らない。SRTP-DTLS[5]をはじめとする既存の方式では、プロバイダが提要するプロキシは信頼できるという前提のもとに、セキュアな通信を保証しているため、プロキシが「盗聴」などを行う場合には、これを防ぐことはできない。そこで著者らは、ネットワーク上に信頼できる Web プロキシを設定して、端末の公開鍵をここにキャッシュさせることによって、セキュアな通信を実現する方式（TWP 方式[7]）を提案してきた。

TWP 方式では、送受信端末が同じ TWP のキャッシュに保存された公開鍵を取得することによって、送信側と受信側の端末が取得する公開鍵の真正性や完全性を保証しているが、インターネットのようにネットワークの規模が大きくなると、一台の TWP だけでは、過負荷となり、システムを維持することができない。

そこで本研究では、大規模ネットワークに対応するため、TWP を複数台にする方式（拡張 TWP 方式）を提案する。このようにすることによって、TWP の負荷を分散させることが可能となり、大規模ネットワークにも対応することができる。

なお、本稿では、拡張 TWP 方式を説明するために、本稿で扱う VoIP 通信、既存の方式と問題点、TWP 方式と問題点、提案方式（拡張 TWP 方式）の順に説明を行う。

2. 本稿で扱う VoIP 通信

本稿で扱う VoIP 通信は、最初にシグナリング通信をおこなって IP アドレスやポート番号などの情報を交換した後に、メディア通信を行うといった広く知られた通信を想定する。また、異なるドメイン間の通信にも対応できるよう、送信側及び受信側ともにプロキシを経由する通信を想定する。また、シグナリング通信のプロトコルとしては SIP[1]を、メディア通信のプロトコルとしては RTP を暗号化した SRTP[2]という、いずれも広く知られ、RFC で標準化されたプロトコルを想定する。

3. 既存の方式と問題点

本稿では、途中の第三者による盗聴などの介入を防ぐため、メディア通信のプロトコルである RTP を共有鍵で暗号化した SRTP を用いることを想定している。しかし、SRTP では、使用する共有鍵の公開方法は既定していない。そこで共有鍵を安全に交換する方式として、DTLS[3]のハンドシェイクプロトコルを利用した DTLS-SRTP とこれを補うために SIP の保護機構（SIP Identity[4]）を用いる DTLS-SRTP-Framework[6]が合わせて提案され、標準化されている。この方式を用いれば、以降のメディア通信で用いる共有鍵を安全に交換することができる。

しかし、DTLS-SRTP では、シグナリング通信におけるプロキシ（SIP プロキシ）が、署名により通信内容を保証するため、SIP プロキシが信頼できるということが、通信を保証する前提となっている。このため、プロキシの信頼性が必ずしも保証されないインターネットなどのオープンネットワークにおいては、プロキシの介入など、必ずしも通信を保証できるとは限らない。

4. TWP 方式

3 章で指摘した問題を解決するため、著者らは、ネットワーク上に信頼できる Web プロキシ（TWP=Trusted Web Proxy）を設定して、これに各端末の公開鍵をキャッシュさせることによって、相手の効果鍵を取得する方式（TWP 方式）を提案した。

TWP 方式では、TWP にキャッシュされた端末自身の公開鍵と相手の公開鍵を取得した後、自分の公開鍵を検証する。これにより、取得した公開鍵の真正性及び完全性を保

†1 新潟県立大学
University of NIIGATA PREFECTURE

証することができる。（図 1）

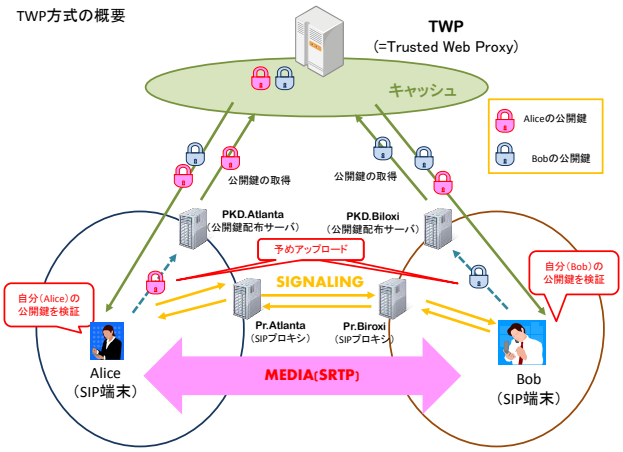

図 1　TWP 方式の概念図

TWP 方式では、TWP にキャッシュされた相手の公開鍵（相手端末は自らこの公開鍵を検証）と自らの公開鍵を取得するが、送受信端末とも、同じキャッシュからある一定期間保持された公開鍵を取得するため、互いに同じ公開鍵を取得していることが保証される。このため、TWP が唯一である必要があり、大規模なネットワークに対応するのが難しいという課題が残る。

5.　拡張 TWP 方式

本章では、4 章で指摘した課題を解決するためのいくつかの方式について考察し、比較検討を行う。

(1)　TWP として負荷に耐えられる PC を使用する方式

4 章の課題を解決する方法として、負荷に耐えられるだけの機能を有する PC を TWP として採用する方式が考えられるが、インターネットのような全世界的なネットワークからの要求に耐えることができる PC を想定するというのは現実的ではない。

(2)　TWP 同期方式

ネットワーク上に複数の TWP（TWP Cluster）を設置して、キャッシュの変更があれば、すべての TWP のキャッシュを同期させる方式が考えられる。しかし、この方式でも、インターネットのような大規模なネットワークにおいては、キャッシュの変更も頻繁に行われるため、同期のための通信負荷や同期のタイミングなどの問題があるため、現実的ではない。

(3)　TWP 選択方式

他にネットワーク上に複数の TWP を設置して、同一セッション内では、送受信端末とも同じ TWP を選択して通信を行う方式が考えられる。この方式では、通信が行われている間、送受信端末ともに同じ TWP を用いているので、キャッシュに保持された公開鍵も同じものを取得することができる。また、複数の TWP を設置しているため、セッションごとに TWP をうまく割り当てれば、負荷を分散させることもでき、規模が大きなネットワークにも対応できる。（図 2）

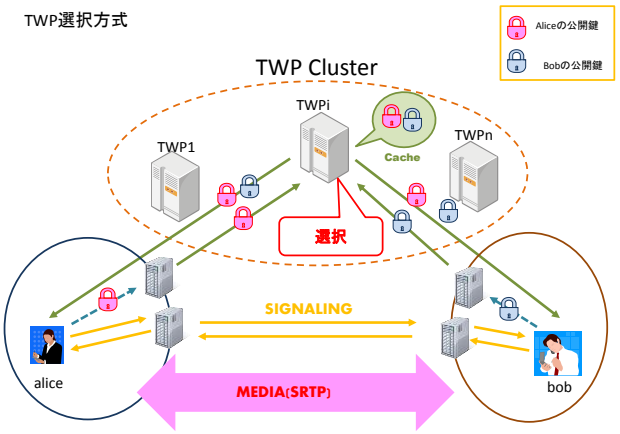

図 2　TWP 選択方式

6.　まとめ

安全な VoIP 通信を実現するための方式として、既存の方式である DTLS-SRTP について説明し、問題点を指摘した後、これを解決する方式として TWP 方式を紹介した。そして、TWP 方式の課題（規模に関する課題）について説明し、これを解決する 3 つの方式について比較検討を行い、最終的に TWP 選択方式を提案した。これにより、インターネットのようなオープンな大規模ネットワークにおいても、安全に VoIP 通信を実現することができることを示した。

参考文献

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, “SIP: Session Initiation Protocol,” RFC3261, IETF, June 2002.

[2] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, “The Secure Real-time Transport Protocol (SRTP),” RFC3711, IETF, March 2004.

[3] E. Rescorla, N. Modadugu, “Datagram Transport Layer Security,” RFC4347, IETF, April 2006.

[4] J. Peterson, NeuStar and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC4474, IETF, August 2006.

[5] D. McGrew and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP),” RFC5764 , IETF, May 2010.

[6] J. Fischl, H. Tschofenig and E. Rescorla, “Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS),” RFC5763, IETF, May 2010.

[7] 高原尚志, 中村素典, “信頼できる Web プロキシを用いた第三者の介入を許さない VoIP 通信の実現方式,” 第 14 回 インターネットテクノロジーワークショップ (WIT2013), ソフトウェア科学会 インターネットテクノロジ研究会, June 2013.