L_007

M2M リアルタイム通信へのサービスマイグレーション方式の適用

Application of Service Migration to M2M Real-time communication

今井 尚樹 Naoki Imai　磯村 学 Manabu Isomura　堀内 浩規 Hiroki Horiuchi

1．はじめに

インターネットの発展に伴い、ユーザ間のコミュニケーション手段として、メッセンジャー、IP 電話、テレビ電話といった様々な手法が安価に利活用可能となった。しかしながら、これらのサービスのさらなる普及に向けて、なりすましや匿名性といったインターネット固有の問題を解決していかなければならない。ISP と家電メーカで構成される UOPF(Ubiquitous Open Platform Forum)では、SIP を利用して物同士をセキュアに接続する方式 (以下、M2M 通信方式) [1]等が検討されてきた。これにより、「予め指定する親しい人との通話のみ許可」といった通信を IP インフラ上で提供可能となる。

一方、筆者らは、ネットワーク接続された多様な端末が遍在する環境において、音声通話やテレビ電話で通話するユーザが、端末・通信メディア・リンクインタフェースといった通信リソースを自由に切替え可能なサービスマイグレーション方式を開発してきた[2]。本方式を M2M 通信方式に適用することで、セキュアな通信環境での通信リソース切替えが可能となる。これを実現するため、通信リソース切替え時に、M2M 通信方式により設定されたセキュアナシグナリングチャネル上でセキュリティ情報を交換し、セッションの切断・再確立を行わずにセキュアデータチャネルを設定するための手法を述べる。

2．M2M リアルタイム通信方式

UOPF では、PC 等の高機能端末に限らず、情報家電といった必ずしも処理能力が高くない機器も相互接続される環境を想定している。そこで、処理負荷が軽く上位プロトコルに非依存である IPsec をベースとして、その鍵交換を SIP に組み入れた手法が検討されてきた[1]。以下では、M2M 通信方式の概要を述べる。

2.1 セキュアシグナリングチャネルの設定

M2M 通信方式では暗号化方式や認証方式として複数の方式がサポートされているが、以下では必須仕様として規定されている Pre-Shared Key による IPsec-m2ms 方式について述べる。この方式は、SIP Security Agreement [3]の鍵交換シーケンスを拡張利用することで IPsec を実現する。図 1 にクライアント端末をプロキシに登録する際の簡易シーケンスを示す。これによりクライアント端末とサーバ間のセキュアシグナリングチャネルが設定される。未登録のクライアント端末からの(登録を除く) SIP リクエストは、プロキシで全て破棄される。

2.2 セキュアデータチャネルの設定

データチャネル設定時には、2.1 で設定したセキュアなシグナリングチャネルが利用されるため、共有鍵を乱数から生成しても安全とみなすことができる(DH 交換から開始することも可能)。実際に、Session Description Protocol (SDP)上の a 行を拡張利用して、鍵生成に必要な nonce 等のセキュリティ情報を交換することで共通鍵を生成し、IPsec の暗号鍵として使用する。すなわち、UA 同士で直接エンドツーエンドの認証は行わず、サーバを介しての間接的な認証となる。また、Security Association (SA)の設定は、セッションが確立したときにアプリケーションが直接行う。図 2 にデータチャネル設定時のシーケンスを示す。

Naoki IMAI, Manabu ISOMURA, and Hiroki HORIUCHI
KDDI R&D Laboratories Inc.

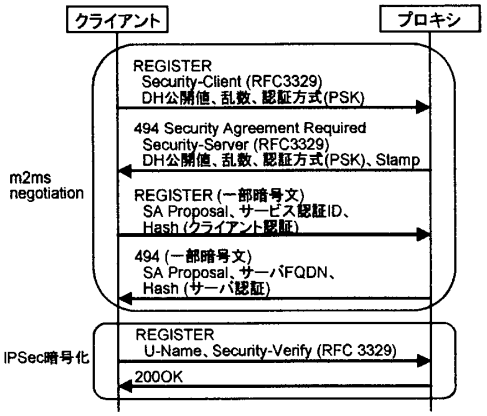

図 1：M2M 通信方式における登録

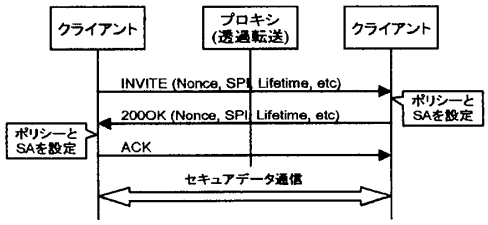

図 2：M2M 通信方式におけるデータチャネルの設定

3. サービスマイグレーション(SMIG)方式の適用

3.1 SMIG 方式の概要

SMIG 方式[2]では、SIP の MESSAGE メソッドを利用したエンド端末間のセッションネゴシエーションおよびシグナリングにより、端末・通信メディア・リンクインタフェースの切替えを実現している。実際には、シグナリングは網内に設置されたセッション管理サーバを経由してやり取りされる。また、ユーザが利用可能な端末や通信メディアに関する情報を管理するプレゼンスサーバも設置され、サーバ同士、およびサーバとクライアント間で連携することで、通信リソースの切替えを行っている。

3.2 M2M 通信への適用

3.2.1 考慮すべき課題

M2M 通信方式に SMIG 方式を適用する場合、以下の点を考慮する必要がある。

(1) 2.2 に示したように、M2M 通信におけるデータチャネルのセキュア化は、セッション開始時に交換される SDP を利用したセキュリティネゴシエーションにより実現される。SMIG 方式の適用時には、通信リソース切替えにより新たに加わる端末のデータチャネルも、セキュア化することが望ましい。

(2) M2M 通信で規定されるプロキシは、クライアントから SIP リクエストを受信すると、リクエストの From 欄が登録されたクライアントと等しいかどうか確認する。このような M2M 通信の概念を考慮すると、未登録の端末(ここでは特に未登録の IP アドレスを意味する)にセッションを移動させることは望ましくない。そのため、IP アドレスが変更となるリンクインタフェースを切替える場合には、切替え先のリンクインタフェースからサーバ登録を

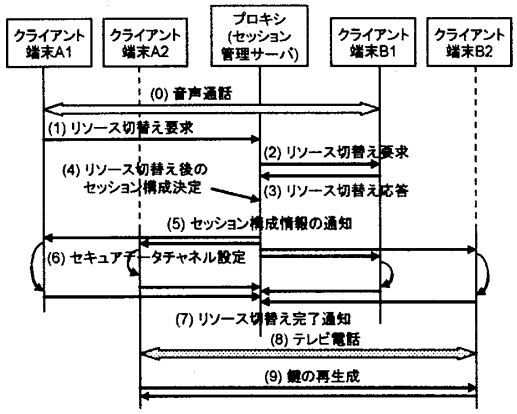

図 3：リソース切替え時のセキュアデータチャネルの設定

完了した後に切替え処理を行わなければならず、メッセージ数の増加や遅延が発生する。

3.2.2 SMIG 方式によるセキュアデータチャネル設定

3.2.1 における課題(1)を解決するため、リソース切替え時にセッションに加わるクライアント端末(プロキシには登録済み)が、セキュアデータチャネルを設定できるよう、SMIG 方式のシグナリングメッセージにセキュリティ情報を含ませる。

具体的な手順を図 3 のシーケンス例を用いて述べる。図 3 には、端末 A1 と端末 B1 間の音声通話(図 3(0))を、端末 A2 と端末 B2 のテレビ電話(図 3(8))に切替える手順を示す。なお、図 3 は一例であり、端末 A1 あるいは端末 B1 を継続して使用するようなリソース切替えも同一の手順で実現可能である。また、図の簡略化のため、網内のサーバとしてはセッション管理サーバのみを示しているが、プロキシとセッション管理サーバを別の機器として設置してもよい。さらに、セッション管理サーバが登録済みのクライアント端末の IP アドレスを検索するためのサーバも、別の機器としてよい。

はじめに、端末 A1 からリソース切替え要求を送信する(図 3(1))。リソース切替え要求には、リソース切替え後に希望するセッション構成の情報[2]に加え、M2M 通信の開始時に交換したセキュリティ情報、さらに、端末 A1 が使用中の暗号鍵および認証鍵を含める。セッション管理サーバは、セキュリティ情報および鍵を取り除いたリソース切替え要求を端末 B1 に送信する(図 3(2))。端末 B1 は、リソース切替えの実行に同意した上で、プレゼンスサービスを用いて使用端末(ここでは端末 B2)を選択し、端末 A1 と同様のセキュリティ情報、暗号鍵および認証鍵を含めて、リソース切替え応答とする(図 3(3))。

セッション管理サーバは、対応する双方の鍵が等しいことを確認し、リソース切替え後のセッション構成について確定する(図 3(4))。その後、通信メディアの種別やデータ送受信先の情報、セキュリティ情報および鍵情報を含むセッション構成情報を、関係する端末に送信する(図 3(5))。セッション構成情報を受信した端末は、それぞれに要求されるアプリケーションの処理と、IPsec の Security Policy Database (SPD)、Security Association Database (SAD)の設定を行い(図 3(6))、セッション管理サーバにリソース切替え完了を通知する(図 3(7))。

M2M 通信方式ではセッション確立時の SDP のオファー/アンサーにおいて鍵の生成を行っている。一方で、SMIG 方式を適用するにあたり、通信リソース切替え先のデータチャネルの鍵として、それまでに使用していた鍵を一時的に使用することで、鍵生成のネゴシエーションを不要とし、結果としてリソース切替え時間の短縮を図る。端末間の鍵配布には、M2M 通信方式により設定されたセキュアシグナリングチャネルを利用しているが、網内を流れた暗号鍵と認証鍵を継続的に使用し続けることは好ましくない。そこで、各端末は切替え完了時に鍵の有効時間を 0 として、更新処理を実行する(図 3(9))。

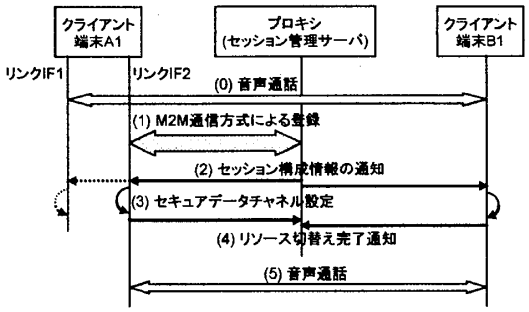

図 4：リンクインタフェースの切替え

3.2.3 リンクインタフェースの切替え

3.2.1 における課題(2)を解決するため、端末の再登録と同時にリンクインタフェースの切替えを行う。シーケンス例を図 4 に示す。端末 A1 のリンクインタフェース 1 と端末 B1 間で音声通話が行われている(図 4(0))。切替え先のリンクインタフェース 2 を用いて、プロキシに M2M 通信方式による登録を行う。ここで、リンクインタフェースの切替え実行を希望するセッションについて、セッションの Call-ID を REGISTER リクエストに含める(図 4 (1))。登録完了後、セッション管理サーバは即座に端末 A1 のリンクインタフェース 2 と端末 B1 にセッション構成情報の通知を送信する(図 4(2))。ただし、双方が同一端末を継続使用するため、データチャネルのセキュリティ情報を送信する必要はない。

各端末は、必要に応じてアプリケーションおよび IPsec の SPD、SAD の処理を行い、セッション管理サーバにリソース切替え完了を通知する(図 4(4))。これにより、セキュアデータチャネル上で音声通話が再開される。

この手法では、ユーザの REGISTER リクエストを受信したプロキシは、リソース切替え要求を受信したものとみなし、そのままリソース切替えの実行を開始する。すなわち、登録とリソース切替えを同時に実行することで、メッセージ数の増加を抑えるとともに切替え時間の短縮を図っている。

登録およびサービス切替え時の音声通話について、端末が新たなデータチャネルを設定するまでは、それまでのデータチャネル上で音声データが送受信される。また、無線環境により、リンクインタフェース 1 経由の通信が断絶してから登録を行う場合(インタフェースが 1 種類の場合も含む)でも、同一の手法で実行可能である。

3.2.3 の機能を実現するためには、M2M 方式に対して REGISTER メッセージのペイロードの記述方法および、これを受信したプロキシの動作を前述のように拡張する必要がある。また、切替え前後で接続するドメインが異なる場合には、異なるドメインのセッション管理サーバ同士の連携が必要となる。しかしながら、前者は記述の規定と特定のリクエスト受信時の処理を変更するのみであり、後者は一般的な SIP プロキシ間の転送処理と類似の処理であるため、実現は用意である。

4．おわりに

M2M 通信の環境においてリソース切替えを実現するため、M2M 通信方式により設定されるセキュアシグナリングチャネルを利用したサービスマイグレーション方式を示した。最後に、日頃ご指導いただく(株)KDDI 研究所秋葉所長ならびに鈴木執行役員に感謝する。

参考文献

[1] “UOPF M2M リアルタイム通信シグナリング仕様,” ユビキタス・オープン・プラットフォーム・フォーラム, 2005 年 5 月.

[2] N. Imai, M. Isomura, and H.Horiuchi, “A Unified Resource Switching for Real-time Communication in a Ubiquitous Networking Environment,” In Proceedings of IEEE Globecom 2005, Dec. 2005.

[3] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, and T. Haukka, “Security Mechanism Agreement for the Session Initiation Protocol (SIP),” IETF RFC 3329, Jan. 2003.