

同軸線通信モデム自動設定手順の提案

荒井 大輔 吉原 貴仁 堀内 浩規

(株) KDDI 研究所

1. はじめに

ホームネットワークや情報家電の普及にともない、新たな配線が不要な同軸線通信の導入が期待されている。PC や情報家電等の宅内通信機器に同軸線通信モデムを外付けすることで、通信が可能となる。しかしながら、集合住宅のように複数の利用者が一つの同軸線を共有する場合、通信の機密性保持などセキュリティの確保が必要となる。そのため、同軸線通信モデムに暗号鍵等の設定が必要となるが、設定には同軸線通信に関する知識が必要であり、円滑な導入および継続的な利用の妨げとなる。そこで、本稿では、利用者に代わり宅内に設置されたゲートウェイ (以下、GW と呼ぶ) がサーバと連携し、暗号鍵等のセキュリティパラメータを自動設定する手順を新たに提案する。

2. 想定環境とサービスシナリオ

2.1 想定環境

世界標準 ITU-T G.9954[1] 準拠の同軸線通信モデム (以下、モデムと呼ぶ) を対象とする。以下、本稿における想定環境を図 1 とともに示す。

STB や PC のような宅内通信機器にモデムを外付けする。モデムは 1 つ以上の Ethernet インタフェースと 1 つの同軸ケーブルコネクタを備える。Ethernet ケーブルで宅内通信機器とモデムを接続し、モデムの同軸ケーブルコネクタと宅内壁面の同軸ケーブルコネクタを接続する。

2.2 サービスシナリオ

STB を用いた TV 視聴など、ISP 事業者が提供する通信サービスに同軸線通信を利用するシナリオを想定する。ISP 事業者はサービス開始時に GW と Master と呼ばれるモデム 1 台を提供し、宅内の共用部分に設置する。また、利用申込みのあった際には STB とともにモデムを利用者に提供する。利用者は、近くに同軸ケーブルコネクタがあれば、宅内の好みの場所に STB を設置し TV 視聴を楽しむことができる。

3. 同軸線通信のセキュリティ

同軸線通信においては Master と呼ばれるモデムが 1 つのネットワーク上に 1 台のみ存在し、ネットワークの同期信号 (Media Access Plan) (以下、MAP と呼ぶ) を断続的に生成する。その他のモデムは Endpoint と呼ばれる (以下、EP と呼ぶ)。EP がネットワークに接続された場合、通信を開始する前に以下の手順を実施する。

- (1) MAP 受信により Master モデムを特定
- (2) Master モデムに対し自身の MAC アドレスを含む登録要求を送信
- (3) Master より登録応答を受信
- (4) 通信を開始

ITU-T G.9954[1] では Master が上記 (2) 登録要求の際に MAC アドレスにより接続の可否を判断する機能、および上記 (3) 登録応答の際に暗号鍵などのセキュリティパラメータを EP に送信する機能によるセキュリティ手順が示されている。

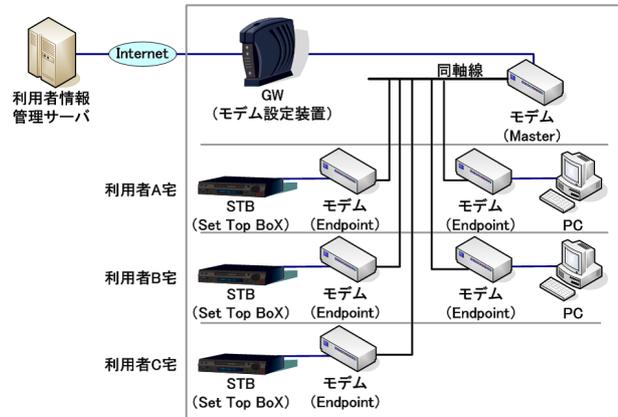


図 1 想定環境

しかしながら、図 1 のような環境においては、各モデムの通信の機密性を確保することに加え、同じ利用者が所有するモデム間のみ通信を許可することがネットワークを利用する際の要件となる。

4. 同軸線通信モデム自動設定手順の提案

本章では、3. にて述べた要件を満たす次の 2 つの自動設定手順を新たに提案し、その概要を示す。

- (1) Master の拡張により同一利用者が所有するモデムにのみ同じ暗号鍵を設定する自動設定手順 (Master の拡張による手順)
- (2) Master は登録要求のあったモデムに対しランダムに生成した暗号鍵を設定し、GW の中継により同一利用者が所有するモデム間の通信のみ提供する自動設定手順 (GW の中継による手順)

以下、4.1 節にて 2 つの提案手順に共通する基本方針、4.2 節にて Master の拡張による手順、4.3 節にて GW の中継による手順を示す。

4.1 基本方針

(方針 1) 利用者情報管理サーバから利用者情報の提供
利用者へモデムを提供する前に、ISP 事業者が利用者情報管理サーバを導入する (図 1 左)。これにモデムの MAC アドレスを投入し、利用者の識別子 (以下、利用者 ID と呼ぶ) と GW の識別子 (以下、ゲートウェイ ID と呼ぶ) を紐付けて管理する。1 つのゲートウェイ ID に対し複数の利用者 ID が紐付けられ、1 つの利用者 ID に対し複数の MAC アドレスが紐付けられる。以下、方針 2 で後述する GW から要求があると、ゲートウェイ ID とパスワードで認証し、モデムの MAC アドレスと利用者 ID を GW に提供する。

(方針 2) GW からの自動設定

GW (図 1 上中) 上で自動設定プログラムを動作させる。本プログラムは利用者またはネットワークの運用者が GW に備え付けられた自動設定の開始を指示するボタンを押下した場合、もしくは GW 管理プログラムより自動設定の開始が指示された場合に動作する。

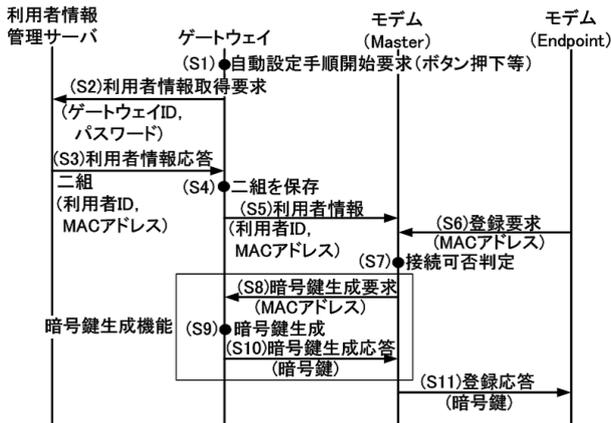


図 2 Master の拡張による手順

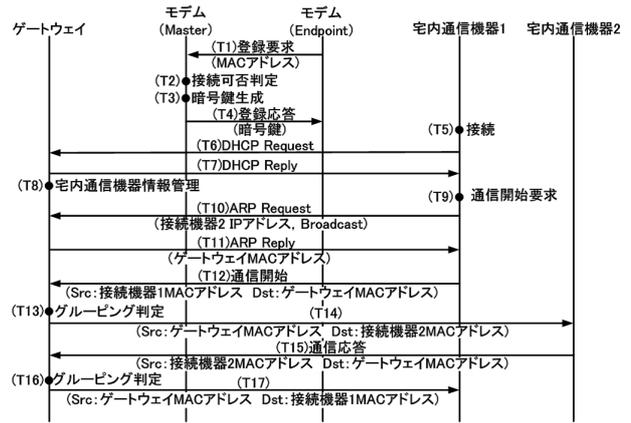


図 3 GW の中継による手順

4.2 Master の拡張による手順

本手順では、GW が生成した暗号鍵を EP に設定する機能を Master に拡張して実現する。

GW のボタン押下等により、自動設定手順が始まる (図 2(S1))。GW は利用者情報を取得するため、ゲートウェイ ID とパスワードを含む要求を利用者情報管理サーバに送信する (図 2(S2))。利用者情報管理サーバはゲートウェイ ID とパスワードで認証し、認証が成功すると、利用者 ID、モデムの MAC アドレスの二組をモデムの数だけ GW に応答する (図 2(S3))。GW は二組の値を保存する (図 2(S4))。GW は二組を利用者情報として Master に保存する (図 2(S5))。

接続された EP は自身の MAC アドレスを含む登録要求を Master に送信する (図 2(S6))。Master は登録要求に含まれる MAC アドレスと、利用者情報に含まれる MAC アドレスとの照合により、接続の可否を判定する (図 2(S7))。Master は EP の MAC アドレスを含む暗号鍵生成要求を GW に送信する (図 2(S8))。GW は暗号鍵生成要求に含まれる MAC アドレスと二組の照合により利用者 ID を判定し、同一利用者 ID の EP に同じ暗号鍵を生成する (図 2(S9))。GW は生成した暗号鍵を Master に応答する (図 2(S10))。Master は暗号鍵を含む登録応答を EP に送信する (図 2(S11))。以降、接続された EP の数だけ登録要求 (図 2(S6)) から登録応答 (図 2(S11)) までの手順を繰り返す。

以上の手順により、同一ユーザが所有するモデムに対し同じ暗号鍵を自動設定できる。

4.3 GW の中継による手順

上記 4.2 節にて示した手順においては、Master の機能拡張を必要とした。しかしながら、Master の持つリソースや開発コストの観点より、4.2 節に先述した機能拡張が困難な場合も考えられる。そこで、本手順においては、Master は登録要求のあった EP にランダムに暗号鍵を割り当てる機能のみ持つ。一方、GW に対しては DHCP サーバ機能および EP に接続された宅内通信機器の MAC アドレスと IP アドレスを管理する機能を想定する。GW が同一利用者が所有する EP 間の通信を中継することにより、同一利用者内の通信を実現する。

上記 4.2 節に先述した手順により GW は利用者情報管理サーバより利用者情報を取得し Master に設定する (図 2(S1) ~ (S5))。その後、EP は自身の MAC アドレスを含む登録要求を Master に送信する (図 3(T1))。Master は登録要求に含まれる MAC アドレスと、利用

者情報に含まれる MAC アドレスとの照合により、接続の可否を判定する (図 3(T2))。Master は暗号鍵をランダムに生成する (図 3(T3))。Master は暗号鍵を含む登録応答を EP に送信する (図 3(T4))。

宅内通信機器 1 を新たにネットワークに接続する (図 3(T5))。宅内通信機器 1 は DHCP により GW より IP アドレスを取得する (図 3(T6), (S7))。GW は利用者 ID と EP の MAC アドレス、EP に接続された宅内通信機器の MAC アドレス、宅内通信機器に割り当てた IP アドレスを宅内通信機器情報として管理する (図 3(T8))。

今、宅内通信機器 1 から宅内通信機器 2 への通信を開始する (図 3(T9))。宅内通信機器 1 は宅内通信機器 2 の IP アドレスから MAC アドレスを得るため ARP リクエストを送信する (図 3(T10))。GW は受信した ARP リクエストに対し自身の MAC アドレスを含む応答を返す (図 3(T11))。宅内通信機器 1 は通信を開始する (図 3(T12))。GW は IP ヘッダに含まれる送信元 IP アドレスおよび宛先 IP アドレスの組合せと宅内通信機器情報の IP アドレスおよび利用者 ID の組合せにより、同一利用者内の通信であるかを判定する。同一利用者内の通信の場合、GW は Ethernet フレームの送信元アドレスを自身の MAC アドレス、宛先アドレスを宅内通信機器 2 の MAC アドレスに変換し、送信する (図 3(T13), (T14))。宅内通信機器 2 からの応答を受信した GW は同様に、Ethernet フレームを変換し送信する (図 3(T15) ~ (T17))。

以上の手順により、ランダムな暗号鍵の設定と GW の中継により、同一利用者が所有するモデム間のみの通信を実現できる。

5. おわりに

本稿では、複数利用者が一つの同軸線を共有する環境において同一利用者内の通信のみを許可する自動設定手順を 2 つ提案した。Master の拡張による手順は、実装に際して Master のリソースの制限や開発コストの問題を含むが、GW の中継による手順と比較し、同一利用者内の通信の際に GW を中継する必要がないため効率的な通信が可能となる。提案手順の実装と実環境評価が今後の課題である。最後に日頃ご指導いただく (株)KDDI 研究所 秋葉所長に感謝する。

参考文献

[1]ITU-T G.9954, "Phoneline networking transceivers - Enhanced physical, media access, and link layer specifications" (2005).