

IP マルチキャスト通信へのユーザ認証機能の導入

石川 憲洋* 山内 長承** 高橋 修*

*NTT情報通信研究所 **日本IBM東京基礎研究所

IP マルチキャスト通信は今のところ実験段階にあり、その実用化に向けて解決すべきいくつかの課題が存在する。その中で、最も重要な課題の一つが IP マルチキャスト通信のセキュリティ機能である。現在の IP マルチキャスト通信は、セキュリティ機能を提供していない。

本稿では、不正なユーザが IP マルチキャストデータグラムを送受信することを防ぐ IP マルチキャスト通信のユーザ認証機能のためのアーキテクチャとプロトコルについて提案する。我々は IP マルチキャスト通信のユーザ認証機能のために IGMP を拡張し、認証サーバとして RADIUS を使用した。本アーキテクチャに基づく FreeBSD 上でのプロトタイプシステムの実装についても報告する。

Architecture for User Authentication of IP Multicast

Norihiro Ishikawa * Nagatsugu Yamanouchi ** Osamu Takahashi *

* NTT Information and Communication Systems Laboratories

** IBM Research, Tokyo Research Laboratory

IP multicast is now at the experimental stage. In order to deploy IP multicast over the Internet as a commercial service, some issues on IP multicast must be resolved. Among them, one of the most important issues on IP multicast is security for IP multicast. There are no security functions for IP multicast at this time.

In this paper, we propose an architecture and a protocol for the user authentication function of IP multicast which prevents an unauthorized user from sending and receiving IP multicast datagrams. We extend IGMP for the user authentication function of IP multicast and use RADIUS as the authentication server. We describe the implementation of a prototype system on FreeBSD based on our architecture.

1 はじめに

インターネット上の仮想的なマルチキャスト通信ネットワークである MBone 上で、様々なマルチメディアツールを用いたマルチメディア通信実験が実施されている。その経験は、IP マルチキャスト通信が、インターネット上でのマルチメディアアプリケーションのための基盤技術であることを示している。また、最近では、IP マルチキャスト通信の新しいアプリケーションとして、電子ニュース、ソフトウェアなどのデジタル情報を同時に誤りなく多数のユーザに分配する高信頼マルチキャストが注目を集めている[1]。

しかしながら、IP マルチキャスト通信は今のところ実験段階にあり、その実用化に向けて解決すべきいくつかの課題が存在する。その中で、最も重要な課題の一つが IP マルチキャスト通信のセキュリティ機能である。現在の IP マルチキャスト通信は、セキュリティ機能を提供していない。

本稿では、不正なユーザが IP マルチキャストデータグラムを送受信することを防ぐ IP マルチキャスト通信のユーザ認証機能のためのアーキテクチャとプロトコルについて提案する。本アーキテクチャに基づく FreeBSD 上でのプロトタイプシステムの実装についても報告する。

2 要求条件

IP マルチキャスト通信のためのセキュリティ機能は、ユーザ認証、IP マルチキャストデータグラムの暗号化、暗号化のための鍵管理と鍵配送など多岐に渡るが、その大部分は未着手であり、今後の研究課題として残されている。本稿では、IP マルチキャスト通信のセキュリティ機能の中で最も基本となる、不正なユーザが IP マルチキャスト通信ネットワークに侵入することを防ぐユーザ認証機能について提案する。

IP マルチキャスト通信のユーザ認証機能に対する要求条件は以下の通りである。

- 送信ユーザの認証： ユニキャスト通信と異なり、IP マルチキャスト通信の場合、送信ユ

ーザが送信した IP マルチキャストデータグラムは、ネットワーク上の多数の受信ユーザに同時に配信される。誰でも送信できるため、ユーザが誤って又は悪意を持って送信すると、1) このトラヒックは受信ユーザのいるところへあまねく配信されるため、ネットワークの負荷になる、2) 受信ユーザは正当な送信ユーザから配信されたデータであると信じ、その内容を信頼してしまう等の問題が生じる。従って、認証されたユーザのみが IP マルチキャストデータグラムを送信できるように制限することは重要である。

- 受信ユーザの認証： 現在の IP マルチキャスト通信では、受信ユーザは認証されることなく誰でも IP マルチキャストデータグラムを受信することが可能である。これに対して、2つの問題がある。第1に、課金を伴うコンテンツを配信する場合、最終的にはコンテンツを暗号化するなどの手段を講じるにしても、まずそのコンテンツが対象外のユーザに配信されないことが望ましく、現在の IP マルチキャスト通信のように、誰でも受信できる状況は望ましくない。第2に、対象外のユーザが受信するために生じるトラヒックは、無駄な負荷になる上、その発生をネットワーク側で制御できない。それはサービスプロバイダにとって望ましくない。
- ルーティングプロトコルからの独立性： IP マルチキャスト通信のために、DVMRP [2]、PIM [3]、CBT [4]などの IP マルチキャストルーティングプロトコルが開発されている。IP マルチキャスト通信の認証機能は、これらの IP マルチキャストルーティングプロトコルから独立であり、特定の IP マルチキャストルーティングプロトコルに依存してはならない。

3 アーキテクチャ

2. で述べた要求条件を満足する、IP マルチキャスト通信のユーザ認証機能のためのアーキテクチャについて述べる (図1)。

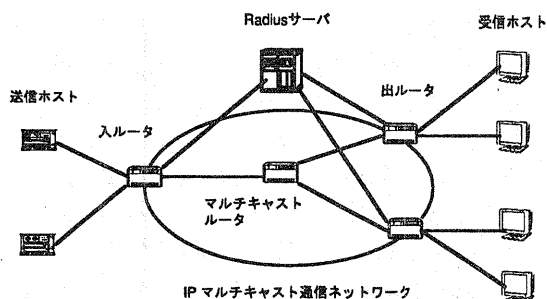


図1 IP マルチキャスト通信の認証アーキテクチャ

送信ホストが接続されているマルチキャストルータを入ルータ (Ingress Router) と呼ぶ。送信ホストが IP マルチキャストデータグラムの送信を開始する時、入ルータは、オプションとして、送信ホスト上のユーザを認証可能とする。以下のシステム設計では、認証は CHAP [5] と同様にチャレンジ・レスポンス方式により行う。入ルータは、認証サーバとして RADIUS [6] を使用してもよい。ネットワーク上のすべての入ルータで、送信ユーザの認証を行うか、又はマルチキャストのルーティングを禁止するように設定すれば、ネットワークから不正な送信ユーザを排除できる。

認証に成功した場合、入ルータは、送信ホストから受信した IP マルチキャストデータグラムを出ルータ (Egress Router) までルーティングする。ルーティングは、DVMRP、PIM などの既存の IP マルチキャストルーティングプロトコルにより制御される。認証に失敗した場合、入ルータは、送信ホストから受信した IP マルチキャストデータグラムを廃棄する。

受信ホストが接続されているマルチキャストルータを出ルータ (Egress Router) と呼ぶ。受信ホストは、IGMP [7] を使用して、出ルータに IP マルチキャストデータグラムの受信開始を要求する。受信ホストが IP マルチキャストデータグラムの受信を開始する時、出ルータは、オプションとして、受信ホスト上のユーザを認証可能とする。以下のシステム設計では、認証は送信ホストの場合と同様にチャレンジ・レスポンス方式により行う。出ルータは、認証サーバとして RADIUS を使用して

もよい。

認証に成功した場合、出ルータは、送信ホストからマルチキャストルータを経由してルーティングされた IP マルチキャストデータグラムを受信ホストに送信する。認証に失敗した場合、出ルータは、IP マルチキャストデータグラムを受信ホストに送信しない。

4 プロトコル

3. で提案したアーキテクチャを実現するために、IGMP 及び RADIUS に対して以下の拡張を行った。

4. 1 IGMP の拡張

広く実装されている IGMP 第2版 (IGMPv2) [7] に対して、表1に示すメッセージを新たに追加した。

表1 IGMPv2 に追加した新メッセージ

メッセージ	主なパラメタ
Sender Start	Group-Address, User-ID
Challenge	User-ID, Challenge-Value
Response	User-ID, Response-Value
Success	Validity-Period
Failure	-

Sender Start は、送信ホストが IP マルチキャストデータグラムの送信開始を入ルータに通知するためのメッセージである。Sender Start メッセージを受信した入ルータは、送信ホスト上のユーザの認証を開始する。Challenge、Response、Success、Failure は、チャレンジ・レスポンス方式による認証を実現するために追加したメッセージである。

4. 2 RADIUS の拡張

認証のためのユーザデータベースは、個々のルータで保持してもよいが、ネットワーク内の認証サーバに集中して保持すると管理が容易になる。我々は、認証サーバとして、ダイアルアップユーザの認証に用いられている RADIUS を拡張して使

用した。RADIUS では、ダイヤルアップルータ - RADIUS サーバ間のプロトコルを規定している。

RADIUS サーバを IP マルチキャスト通信のユーザ認証に使用するために、RADIUS に対して、2つのサービスタイプ（“マルチキャスト送信ユーザ認証”と“マルチキャスト受信ユーザ認証”）及びそのパラメタとして表2に示す属性を新たに追加した。RADIUS に対しては、新しいメッセージの追加は行っていない。

表2 RADIUS に追加した新属性

属性	説明
Group-Address	マルチキャストルータから RADIUS サーバに対して、認証の対象となるグループアドレスを通知する。
Validity-Period	RADIUS サーバからマルチキャストルータに対して、認証の有効期間を通知する。

5 ユーザ認証方式の概要

5. 1 送信ホストのユーザ認証（図2）

IP マルチキャストデータグラムの送信を開始する時、送信ホストは入ルータに対して、Sender Start メッセージを送信する。Sender Start メッセージの Group-Address パラメタには、IP マルチキャストデータグラムを送信する宛先のグループアドレス（クラスDアドレス）を設定する。

Sender Start メッセージを受信した入ルータは、送信ユーザの認証を行うために、まず送信ホストに対して Challenge-Value パラメタに乱数を設定した Challenge メッセージを送信する。

Challenge メッセージを受信した送信ホストは、Response メッセージで入ルータに応答する。Response メッセージの Response-Value パラメタには、下記の値を設定する。

- ・MD5（“乱数”+“送信ユーザのパスワード”）[8]

Response メッセージを受信した入ルータは、RADIUS サーバに Access-Request メッセージを送信して、送信ユーザの認証を依頼する。

Access-Request メッセージを受信した RADIUS サ

ーバは、受信した“乱数”と自身が保持している“送信ユーザのパスワード”に対して MD5 を適用し、その値と受信した Response-Value を照合する。値が一致した場合は、入ルータに Access-Accept メッセージを送信して、認証の成功を通知する。値が一致しない場合は、入ルータに Access-Reject メッセージを送信して、認証の失敗を通知する。

Access-Accept メッセージを受信した入ルータは、送信ホストに Success メッセージを送信して、認証の成功を通知する。Access-Reject メッセージを受信した入ルータは、送信ホストに Failure メッセージを送信して、認証の失敗を通知する。

認証に成功した場合、入ルータはその送信ホストが送信した IP マルチキャストデータグラムをルーティングする。認証に失敗した場合、入ルータはその送信ホストが送信した IP マルチキャストデータグラムを廃棄する。

ユーザ認証の有効期間（Validity-Period）を設けた。有効期間が切れた場合、入ルータは、送信ユーザの再認証を行う。

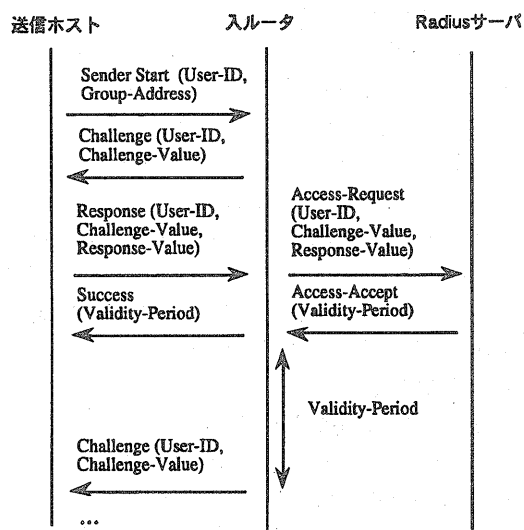


図2 送信ユーザの認証手順

CHAP の場合と同様に、Challenge-Value と Response-Value を不正なユーザに傍受されても、値を再利用されてネットワークに侵入される心配はない。

5. 2 受信ホストのユーザ認証 (図3)

IP マルチキャストデータグラムを受信を開始する時、受信ホストは出ルータに対して、Membership Report メッセージを送信する。Membership Report メッセージの Group-Address パラメタには、受信ホストが参加するホストグループのグループアドレスを設定する。

Membership Report メッセージを受信した出ルータは、受信ユーザの認証を行うために、まず受信ホストに対して Challenge-Value パラメタに乱数を設定した Challenge メッセージを送信する。

Challenge メッセージを受信した受信ホストは、Response メッセージで出ルータに応答する。Response メッセージの Response-Value パラメタには、送信ユーザの認証の場合と同様に下記の値を設定する。

・ MD5 (“乱数” + “受信ユーザのパスワード”)

Response メッセージを受信した出ルータは、RADIUS サーバに Access-Request メッセージを送信して、受信ユーザの認証を依頼する。

Access-Request メッセージを受信した RADIUS サーバは、送信ユーザの認証の場合と同様に、受信した Response-Value を照合する。RADIUS サーバは、認証に成功した場合は Access-Accept メッセージを、認証に失敗した場合は Access-Reject メッセージを出ルータに送信する。

Access-Accept メッセージを受信した出ルータは、受信ホストに Success メッセージを送信する。Access-Reject メッセージを受信した出ルータは、受信ホストに Failure メッセージを送信する。

認証に成功した場合、出ルータは受信した IP マルチキャストデータグラムをその受信ホストにルーティングする。認証に失敗した場合、出ルータは受信した IP マルチキャストデータグラムをその受信ホストにルーティングしない。

送信ユーザの認証の場合と同様に、ユーザ認証の有効期間 (Validity-Period) を設けた。有効期間が切れた場合、出ルータは受信ユーザの再認証を行う。

IP マルチキャスト通信では、LAN の場合、出ルータのルーティングのオン/オフは、LAN 上に受信ホストが存在するか否かに基づいて行う。従っ

て、LAN 上に 1 台以上の認証された受信ホストが存在すれば、出ルータは IP マルチキャストデータグラムをその LAN にルーティングすることとした。受信ホストの再認証を行う場合、出ルータは、LAN 上のすべての認証された受信ホストに対し Group-Specific Query メッセージを送信し、Membership Report メッセージで応答した 1 台の受信ホストが正しく認証されれば、IP マルチキャストデータグラムのルーティングを継続することとした。

本方式の場合、LAN 上に 1 台以上の認証された受信ホストが存在すれば、認証されていない受信ホストが IP マルチキャストデータグラムを傍受することが可能となる。この問題の解決は今後の課題である。

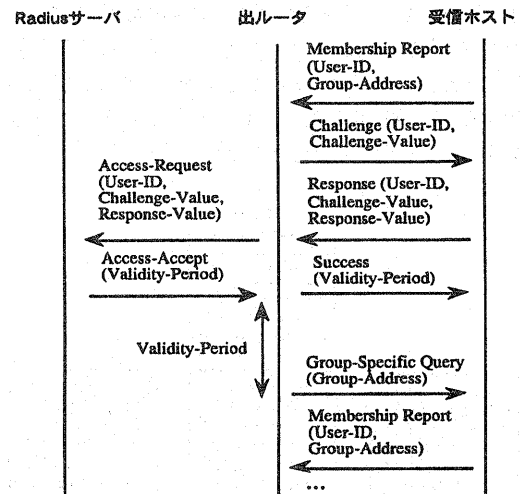


図 3 受信ユーザの認証手順

6 実装

我々は、図4に示す環境で、IP マルチキャスト通信の認証機能の実装実験を行った。

送信ホスト、受信ホストについては、FreeBSD の IGMP コードを拡張して実装した。送信ホスト上の IP マルチキャストアプリケーションが、認証機能を利用可能とするために、新たに以下のソケットオプションを定義した。

- setsockopt (IP_MULTICAST_SENDER-START, User-ID, Password)
- setsockopt (IP_MULTICAST_SENDER-END, User-

ID, Password)

受信ホスト上の IP マルチキャストアプリケーションが、認証機能を利用可能とするために、既存の IP マルチキャスト通信のためのソケットオプションに、以下の通り User-ID パラメタと Passwd パラメタを追加した。

- setsockopt (IP_ADD_MEMBERSHIP, User-ID, Password)
- setsockopt (IP_DROP_MEMBERSHIP, User-ID, Password)

マルチキャストルータについては、mrouted と FreeBSD の IGMP コードを拡張して実装した。mrouted は、インターネット上の仮想的な IP マルチキャスト通信ネットワークである Mbone 上で広く利用されているソフトウェアルータである。プロトコル処理を行う機能 (即ち、IGMP の認証プロトコル及び RADIUS プロトコルの処理を行う機能) は、mrouted に組み込んだ。FreeBSD に対しては、認証結果に基づいて、IP マルチキャストルーティングのオン/オフを行う機能を追加した。

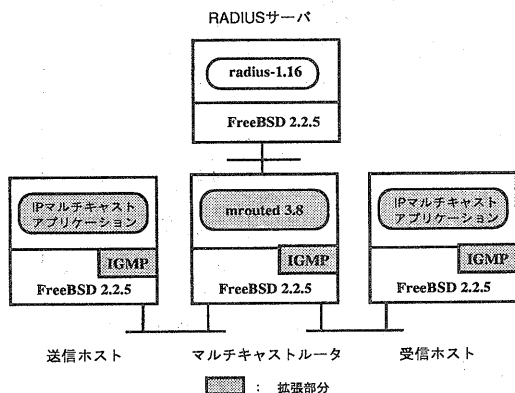


図 4 IP マルチキャスト通信の認証機能の実装

RADIUS サーバについては、RADIUS プロトコル自身の拡張は行っていないため、Ascend 社から提供されている RADIUS サーバのソフトウェア (radius-1.16) を拡張することなく使用した。

更に、アプリケーションが、IP マルチキャスト通信の認証機能を利用できることを確認した。IP マルチキャストアプリケーションとしては、NTT 情報通信研究所と IBM 東京基礎研究所が共同開発した高信頼マルチキャスト通信プロトコルである

RMTP [1]を対象とした。RMTP を実装したソフトウェアを改造して、我々が FreeBSD 上で開発したプロトタイプシステム上で認証機能を実行できることを確認した。

7 まとめ

IP マルチキャスト通信の認証機能のためのアーキテクチャ及びプロトコルと、その FreeBSD 上での実装について述べた。我々は、本方式を IETF IDMR-WG に提案中である [9]、[10]。

参考文献

- [1] 高橋、城下、佐野、國分、山内: マルチキャストを利用したプッシュ型高信頼情報配信サービスとプロトコル, 信学会, 信学技報, SSE97-128, Oct. 1997.
- [2] D. Waitzman, C. Partridge and S. Deering: Distance Vector Multicast Routing Protocol, RFC 1075, Nov. 1988.
- [3] S. Deering, D. Estrin, D. Farinacci, V. Jaconson, C. Liu and L. Wei: vic: An Architecture for Wide-Area Multicast Routing, ACM SIGCOMM 94, Aug. 1994.
- [4] T. Ballardie, P. Francis and J. Crowcroft: Core Based Tree (CBT), ACM SIGCOMM 93, Sep. 1993.
- [5] W. Simpson: PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, Aug. 1996.
- [6] C. Rigney, A. Rubens, W. Simpson and S. Willens: Remote Authentication Dial In User Service, RFC 2138, April 1997.
- [7] W. Fenner: Internet Group Management Protocol, Version 2, RFC 2236, Nov. 1997.
- [8] R. Rivest and S. Dusse: The MD5 Message-Digest Algorithm, RFC 1321, April 1992.
- [9] N. Ishikawa, N. Yamanouchi and O. Takahashi: IGMP Extension for Authentication, Internet-Draft, March 1998.
- [10] N. Yamanouchi, N. Ishikawa and O. Takahashi: RADIUS Extension for Multicast Router Authentication, Internet-Draft, March 1998.