分散システム特論レポート

RFC2974 : SAP(Session Announcement Protocol)

情報工学専攻 岡村研究室
修士 1 年 藤岡健太郎

平成 13 年 1 月 10 日

1 導入

SAP(Session Announcement Protocol) とは、マルチメディア会議や他のマルチキャストセッションを公告して予想される参加者への適切なセッションセットアップ情報を伝達するためのプロトコルである。つまりセッション記述を含んだパケットを定期的にマルチキャストし、潜在的な参加者へ公告するするというものである。

2 SAP 概要

この RFC2974 での SAP は、version2 である。

マルチキャストセッションは大きく分けて、グローバル範囲セッションと管理範囲セッションに分けることができる。グローバル範囲セッションとはインターネット全体を利用したセッションを指し、セッションに使用できるアドレス空間は 224.2.128.0 ~224.2.255.255 である。このセッションの公告に使用される IP アドレス (SAP 公告 IP アドレス) は 224.2.127.254 である。さらにポート番号は 9875 を使用し、TTL は 255 である。一般に SAP に使用される IP アドレスはアドレス空間の最高位アドレスを使用するが、グローバル範囲セッションのアドレス空間の最後尾アドレスである 224.2.127.255 は SAPv0 で使われており、使ってはいけないとしている。

管理範囲セッションとは、ある決まった範囲内でのセッションであり。アドレス空間は 239.0.0.0 ~239.255.255.255 である。例えばある地域範囲でのセッションはローカル範囲セッションといい、アドレスは 239.255.0.0/16 を使用し、ある組織内でのセッションを組織ローカル範囲セッションといい、アドレスは 239.192.0.0/14 を使用する。これらのセッションの SAP アドレスは、通常アドレス空間の最高位アドレスを使用する。例えば、239.16.32.0 ~239.16.33.255 のアドレス空間をもつ管理範囲セッションにおいては、その最高位アドレスである 239.16.33.255 を SAP アドレスとして使用する。

この管理範囲の発見においてはこのプロトコルの範囲外であるので、SAP リスナー、つまり潜在的な参加者はその管理範囲を知っているものとする。

2.1 SAP 公告間隔

SAP 公告は、定期的に公告されるがその公告の間隔を以下のパラメータを用いて計算している。

limit SAP 公告に使われる全帯域幅
指定が無ければ 4000bps

no_of_ads 公告されている全セッションの数
他の公告を聴取することでわかる

ad_size 公告のサイズ

まず、前回の公告時間 tp を初期化します。そして次回の公告時間 tn を以下の式から計算します。

$$interval = max(300; (8 * no_of_ads * ad_size)/limit)$$

$$offset = rand(interval * 2/3) - (interval/3)$$

$$tn = tp + interval + offset$$

公告者は、tn で一度タイマを破棄して待ち、次の伝送時間を最計算する。そして新しい tn が今の時間より前なら公告は即座に送られる。そうでなければ新しい tn で伝送時間が再計算される。これはスタートアップ時やネットワーク障害からの復帰時におけるパケットバーストを防ぐものである。

2.2 セッション削除

セッションは、以下の方法の一つによって削除される。セッションの削除とは受信者のセッションキャッシュからの削除を示す。

明示的タイムアウト　セッション記述にセッションの開始と終了の時刻を指定したタイムスタンプがあり、そのタイムスタンプ情報により削除される。

暗黙的タイムアウト　公告が 10 回こないとき、または 1 時間来ないときに削除される。このとき、公告間隔は受信者によって予測できる。

明示的なセッション削除パケットの受信　公告パケットの認証ヘッダによる認証が行われる。認証失敗時はメッセージを無視する。

2.3 セッション修正

セッションの修正は単純に修正セッション記述により修正される。ただ、ここにもセッション削除と同様のルールが適用される。つまり公告パケットの認証ヘッダによる認証が行われる。または認証ヘッダをもたず、セッション修正公告が修正するセッションと同じホストから発せられていなければならない。

もし公告が認証ヘッダを含んで受け取られ、キャッシュされている公告が認証ヘッダを持たないか、または異なった認証ヘッダを持っているなら、修正公告はそれとは違う新しいセッションとして扱われ、認証されていない公告のあとに加えて表示される。もし認証ヘッダのない修正パケットがオリジナルの公告と異なった送信者から受け取った場合も同じことが言える。これらのルールは、悪質なユーザによって加えられた認証ヘッダの公告によってセッションが削除されるのを防ぎ、さらに DoS 攻撃により、オリジナル公告よりものまね公告がざきにいくつかのユーザに届いて、オリジナル公告が追い出されるのを防ぐ。このような状況下で、メッセージの発信者を認証できることが、正しいセッションを発見する唯一の方法である。

2.4 SAP データパケット

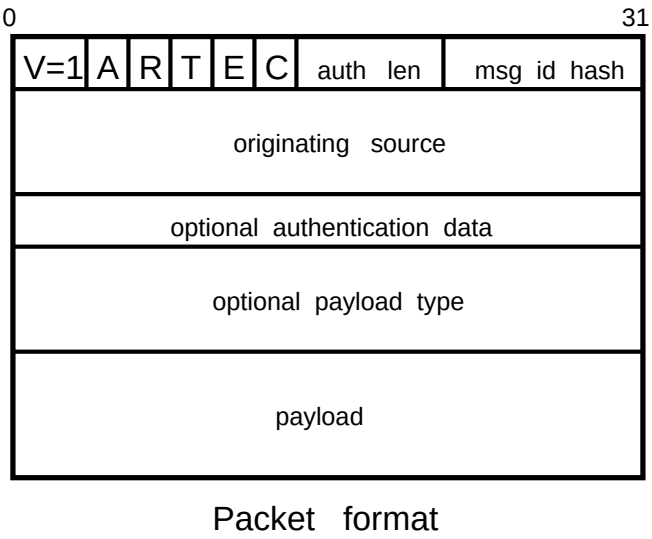
以下に SAP データパケットのフォーマットを示す。

- V：バージョン
  - 1 にセット
  - v2 でも新しくなった特徴はみつけることができる
- A：アドレスタイプ
  - 0：32bit IPv4 アドレス
  - 1：128bit IPv6 アドレス
- R：Reserved
  - 0 にセット
- T：メッセージタイプ
  - 0：セッション公告パケット
  - 1：セッション削除パケット
- E：暗号化ビット
  - 1：SAP パケットペイロードが暗号化されている
  - 0：SAP パケットペイロードが暗号化されていない
- C：圧縮ビット
  - 1：zlib 圧縮されている
  - 0：zlib 圧縮されていない

ここで、圧縮と暗号化両方されるなら、圧縮が最初に行われる。

- 認証の長さ
  - 8 ビット長

図 1: SAP データパケット format



  - 認証データを含む SAP ヘッダの 32 ビットワードの数を示す
  - 0：認証ヘッダなし
- メッセージ識別ハッシュ
  - 16 ビット長
  - グローバルに一意的な識別番号
  - セッション記述が変更されると変わる
- オリジナル送信元
  - メッセージのオリジナル送信元の IP アドレス
  - ネットワークバイトオーダで格納

以下、このヘッダの後にオプショナルペイロードタイプフィールドとペイロードがくる。パケットがセッション公告パケットならペイロードはセッション記述を含み、パケットがセッション削除パケットならセッション削除メッセージを含む。

2.5 公告の暗号化と認証

2.5.1 暗号化

暗号化は、暗号化キーを持たないリスナーに暗号化された公告をすると無駄になるために、グローバルな範囲や大きな規模の公告には暗号化は用いられるべきでない。

対象アルゴリズムを使用する暗号化はある程度のプライバシーをあたえるが、キーが本来の所有者でないユーザが所有する可能性があるため、キー保持者へのキーのセキュリティに対する信頼がないかぎり、完全なセキュリティにはならない。一般にマルチキャストセッションツールで共有されているので、認証されていないユーザにキーが渡る可能性は十分にある。非対象アルゴリズムを使用する暗号化も同様である。しかしプライベートキーの所有者を制限できるので、キー所有者グループへの公告は行われないことになる。

2.5.2 認証

認証ヘッダは、セッション修正やセッション削除の証明の許可と、セッションの作成者の身元の認証の二つの目的に使われる。

認証データのフォーマットは以下の通りである。

- V：バージョン
  - ここでのバージョンは 1
- P：パディングビット
  - 認証データがある時セット
- Auth：認証タイプ
  - 認証サブヘッダのフォーマットを定義
  - 0：PGP フォーマット
  - 1：CMS フォーマット

もし SAP パケットが圧縮か暗号化がされる予定なら、認証が加えられる前にされなければならない。

2.5.3 セキュリティ

SAP は、公告の発起者の認証とそのような公告の暗号化をして、セッション公告の保全性を保証するメカニズムをもつ. もし有効な認証ヘッダを持ち、セッション作成者の署名のないセッション修正公告を受け取ったら、セッション記述の一つの発起者が信用される第三者によって署名された証明を使って認証されるのでないかぎり、同じ SDP 発起情報をもつオリジナルセッションに加えて、新しいセッションとして扱われなければならない。もしこれが行われないと、新しい公告を聞き、オリジナル認証ヘッダをとり、セッション記述を修正し、新たな認証ヘッダを加え、セッションを再公告するような DoS 攻撃がおこる可能性がある。

3 v1 と v2 の違い

SAPv1 はこのメモの 1996 年 11 月 19 日に書かれたバージョンのもののプロトコルである。

SAP メッセージのパケットヘッダは、v2 ツールは v1 公告ヘッダを理解できる点で同じであるが必ずしも逆はいえない。以下に v2 での変更点を挙げる。

- SAP ヘッダに A ビットが加えられた (v2 から IPv6 をサポート)
- 二番目のビットが reserved(0) になった
- E ビットを持ちペイロードの暗号化を示す
- SAPv1 では、互換性のためにメッセージ識別ハッシュとオリジナル送信元を 0 にセットさせていたが、これが強制ではなくなった
- gzip 圧縮から zlib に変更
- より完全な認証の仕様を与える
- SDP でないペイロードも送信できるようになった

4　sdr の実行結果

sdr はマルチキャストセッション公告を聴取し、指定したマルチキャストセッションに参加でき、また自分のマルチキャストセッションの公告もできるソフトウェアである。このマルチキャストセッションの公告の聴取や、自分のマルチキャストセッションの公告に今回紹介した SAP が用いられている。このソフトウェアではセッション記述は SDP を用いている。

4.1　tcpdump の結果

以下に sdr 使用中の tcpdump の結果を示す。

- セッション公告 (ローカル範囲)

```
03:37:56.637242 eth0 > 133.5.7.46.1242 > 239.255.255.255.9875:udp274
03:41:41.117263 eth0 > 133.5.7.46.1242 > 239.255.255.255.9875:udp274
```

- セッション聴取 (グローバル範囲)

```
03:54:27.031950 eth0 M 128.223.214.23.55831 > 224.2.127.254.9875: udp 400
```

セッション公告においては、公告の発信ホスト (133.5.7.46) から、ローカル管理範囲アドレスの最高位アドレスである 239.255.255.255 のポート番号 9875 に SAP 公告を行っていることがわかる。同様に、セッション聴取においても、公告発信ホスト (128.223.214.23) から、グローバル範囲 SAP 公告アドレスの 224.2.127.254 のポート番号 9875 にマルチキャストされた公告を聴取していることがわかる。

5　まとめ

ここではRFC2974 において標準化されている、マルチキャストセッション公告用のプロトコルである SAP(Session Announcement Protocol) について、その概要とセッションの公告間隔、セッション削除と修正、暗号化と認証、v1 と v2 の違い、実装ソフトウェアによるプロトコルの利用についてみてきた。この SAP に密接に関わる他のプロトコルとして、SDP や SIP があげられる。現在は主にこれらのプロトコルを利用してマルチキャストセッションの利用が行われている。