ISS-P-022

マルチキャスト網におけるアノマリーパケット検出システムの提案

木下 竜一† 瀬林 克啓† 丸山 充†

† 神奈川工科大学　情報学部　情報ネットワーク・コミュニケーション学科

1. はじめに

アドホックな広域ネットワーク構築を行う場合に，様々な種類のネットワーク機器から構成される分散システムのデバッグには非常に時間と手間がかかる．これは人為的なコンフィグミスやネットワーク機器ベンダー間のプロトコル解釈の相違などが原因となっている．特に映像配信で用いる IP マルチキャストでは，マルチキャストパケットが特定のポートにフォワードされない，逆にマルチキャストツリーの枝の刈込ができず意図しないポートに出力される事で通信帯域を圧迫して，他の通信に影響を与えるトラブルが発生する．これらの原因の追究のためには多くの時間を要する上，ルータやスイッチ内のテーブル参照だけのデバッグ手法では利用者やオペレータが気付ける範囲までしか問題点を追究できない課題がある．

2. 提案

本提案では，上記のトラブルを早期に発見し，原因の特定・解決をする為に スイッチ・ルータで構成されるネットワークの外部から関連する全ポートの通信状況を監視することで，想定外のフォワード動作を可視化し，オペレータが異常状態を早期に検知可能なシステムのプロトタイプを作成し検証する．

本システムは，汎用ネットワーク機器の制御ネットワークに接続された「コントローラ部」とネットワーク機器のミラーポートに接続された「キャプチャ部」，キャプチャ部からのデータとコントローラ部での操作記録を集約する「データベース部」から構成される．

コントローラ部は定期的にネットワーク機器の全ポートをポートミラーリングするための設定変更をすると共に，キャプチャ部に対して接続されている回線のパケットキャプチャ指示を行い，データを収集させる．この動作を定期的に行うことにより，該当の汎用スイッチの全ポートを巡回してポートから出力されるパケットをサンプリング的に収集することができる．データベース部では，キャプチャデータを時系列に基づき格納処理を行った後，検出部がデータを読み出す事で全ポート状態を可視化する．

3. システム構成

データベース部には Apache HBase を用いて構築をした．当初は PostgreSQL を利用していたが，要求される格納・読み出しのスループットが出なかったため Apache HBase に変更した．

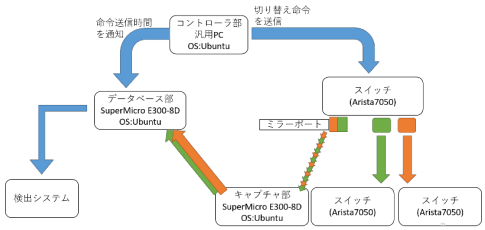

図.1.1　システム構成

4. 評価

システムの各部の処理時間を測定する．コントローラ部の切り替え命令の送信から 172msec で対象とするミラーポートが変更された．この内，実験に用いた Arista Networks の 7150t52 の API によるミラーポートの切り替え時間は 42msec である．またパケットキャプチャが行われてから 0.149msec/パケットでデータベースにキャプチャ情報が格納されており，100 個程度の連続パケットが入力される条件でも 15 秒間隔でミラーポートを切り替えることで全てのポートをサンプリングすることが可能である．

5. まとめ

マルチキャスト網のトラブル状況を発見するために，スイッチやルータの状況を外部から監視するシステムを提案し，全ポートをサンプリングキャプチャする事で不正状態の可視化をした．今後は，スイッチ・ルータのコンフィグ状況と連携した拡張を目指す．

謝辞

今回の実験を行うにあたり 機材を貸与していただいた，ＮＴＴ未来ねっと研究所様，情報通信研究機構様，アリスタネットワーク様に感謝します．

参考文献

[1]マルチキャスト － IGMP スヌーピングとは，
https://www.infraexpert.com/study/multicastz12.html

[2]Apache HBase Apache HBase™ Home,
https://hbase.apache.org/