4U-9

Gigabit Ethernet 全二重ワイヤレートに対応したネットワークフォレンジックシステムの開発

居内　寛貴† 中島　潤‡

北海道情報大学システム情報学部† 北海道情報大学情報メディア学部‡

1. はじめに

コンピュータネットワークのトラフィックは爆発的な増加の一途をたどっており，企業内 LAN のバックボーンの主流は Gigabit Ethernet(以下 GbE)になっている．こうした中で，GbE 環境で通信の監視，情報漏洩対策をとることは非常に困難となっており，現行のネットワークフォレンジックシステム製品では，通信パケットのキャプチャ，解析，プレイバックを行う場合，解析時にシステムリソースを著しく消費し，パケットの取りこぼしが発生する．このため，複数代のサーバによりクラスタリングを行うことで問題を回避することを推奨している製品もあるが，パケットキャプチャをソフトウェアで行っていることなどもあり，GbE に完全に対応することは困難である．

本研究では，こうした問題点を解決する方法として高速 IP 解析エンジンの開発も，パケットキャプチャ，解析，プレイバックまでの課程を３つのステージに分け同時処理する「3 Stage Network Flow」解析アルゴリズムを提案し，これを利用することで GbE 全二重ワイヤレートに対応可能なネットワークフォレンジックシステムを開発しその評価を行ったので報告する．

2. 解析アルゴリズムの提案

通信をリアルタイムに解析を行う場合，キャプチャと解析プロセスを平行して実行し，システムリソースが不足する事態を回避するため 3 Stage Network Flow 解析アルゴリズムを提案する(fig1)．これは，通信データの解析を

(1)キャプチャと同時に行うストリーム解析
(2)システムリソースの閑暇時に行うアプリケーション解析
(3)通信の再現を表示する際に行うプレイバック解析

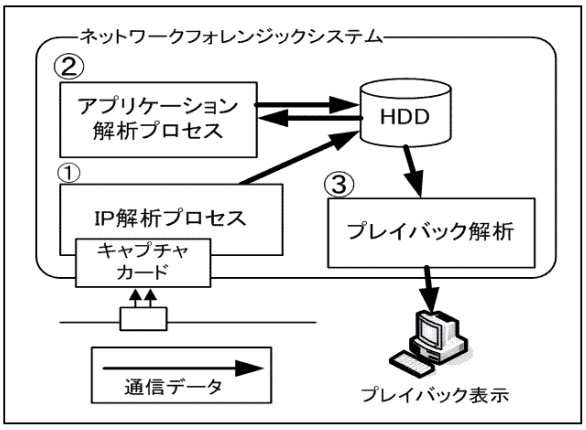

fig1.システム構成図

の３ステージに分割し，それぞれを独立して動作させることにより，解析負荷を分散し，ステージごとに必要最低限の解析を行うことでリアルタイムに解析結果を出力することを可能とした．また，必要最低限の処理を行うため，パケットキャプチャに割り当てるべきシステムリソースを常時使うことがなく，優先的に割り当てることができる．加えて，分散処理によりプレイバック時にもタイムロスのないスムーズな表示を両立させることが出来る．

(1)ステージでは，キャプチャと同時にセッションの解析を行うため，リアルタイムで通信の監視，アプリケーションレイヤの解析が可能である．キャプチャ時の解析では，IP アドレス，ポート番号，トラフィック等の情報のみを解析するため，解析性能の向上を実現した．また，IP 解析エンジンは，ハッシュ値を利用することで，瞬時に IP の識別を行えるよう開発した．このハッシュ値はシステム全体で共通に利用されているため，高速なデータの識別が可能とさせた．

キャプチャされたデータは通信データに時間情報など，わずかな情報を付加した独自形式として保存し，記録容量を最小限にとどめて通信情報の保存が可能である．

「Development of Network Forensic System corresponding to Gigabit Ethernet Full Duplex Wire Rate Speed」

† 「Hiroki Iuchi・Faculty of System Information, Hokkaido Information University」

‡ 「Jun Nakajima・Faculty of Information Media, Hokkaido Information University」

(2)ステージでは，(1)での解析データを元にHTTP，FTP，SMTP，POP 等のアプリケーションレイヤごとの解析を行う．キャプチャにおけるシステムリソースを確保するためシステムリソースを監視するコントローラからの呼び出しにより実行する．このため，キャプチャでのシステムリソースが不足することがなく，IP 解析エンジンと合わせることで GbE のワイヤレートに対応することが可能である．

(3)ステージでは，プレイバック処理においてプレイバックするデータがセッション中のどの位置に存在するかを検索する．検索されたデータは，独自形式のデータフォーマットから PCAP 等の汎用的出力フォーマットに整えられ GUI へ出力する．出力フォーマットのデータを保存しておくのではなく，最後のプレイバック時に変換することで，システムリソース及び保存容量の節約を実現した．

3. 性能評価

3.1 評価環境

前章で提案したパケット解析エンジンの性能評価を以下の環境・条件で行った．

パケット解析エンジンを稼動させるマシンは，CPU は Hyper Threading 技術を用いた Intel Xeon 3GHz を 2 基 メモリは 4GB を搭載したサーバを用いた．

HDD への書き込み速度がボトルネックとなるのを防ぐために，SATA 接続による 12 台の HDD を RAID5 構成とした．ファイル書き込み性能が 1 台あたり約 300Mbps であることから問題はないと判断した．

3.2 評価方法

本研究で開発したフォレンジックシステムでは，リアルタイムに解析する際に一番のボトルネックとなるのは IP 解析エンジンの処理性能と推測される．実際の LAN トラフィックに近いパケットストリームを IP 解析エンジンへ渡し，キャプチャ，解析，データ及び解析結果の保存を行った場合の CPU，メモリの使用率に問題がないか確認することで有効性の評価を行った．

トラフィックは Layer7 エミュレータ（Antara 製 Flamethrower)により,HTTP トラフィック（8KByte/session）を発生させ，そのパケットをキャプチャした．

3.3 評価結果

20,000Session/Sec のトラフィックを発生させた場合，転送速度にして 1.3Gbps の段階で CPU の使用率が 60%となった．また 24,000Session/Sec のトラフィックを発生させた場合は，転送速度にして 1.6Gbps となり CPU 使用率が 85%となった(fig2)．

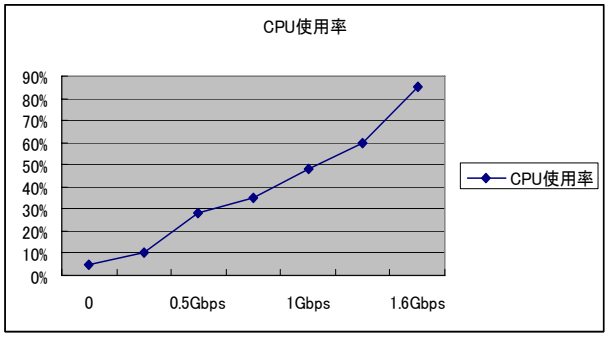

fig2.評価グラフ

Flamethrower の性能上，これ以上のトラフィックを発生させることが不可能なため計測を行うことができなかったが，数値上昇を見る限り，CPU の使用率が 100%の時点で転送速度 1.8Gbps をキャプチャ・解析できるものと推測できる．CPU の使用は２つのみの利用にとどまっているため，残されている CPU を使い同時に解析も問題なく行えることを確認した．

メモリ使用率については，1.6Gbps のトラフィック時においてキャプチャバッファに 512MB，IP 解析エンジンに 50MByte 程度であるため特に問題がないことを確認した．

4. まとめ

本研究では，サーバ１台で GbE ワイヤレートに対応可能なネットワークフォレンジックシステムを開発した．キャプチャ，解析，プレイバックによる 3 Stage Network Flow 解析アルゴリズムにより，高速化が実現された．

今後は，本研究で開発した 3 Stage Network Flow 解析アルゴリズムとそれを実装した高速 IP 解析エンジンを利用することにより，リアルタイム解析が可能となったため，IDS 等の機能を持った総合的なセキュリティシステムの開発にも応用可能であると考えられる．

参考文献

[1]居内寛貴 福岡清伸 中島潤 ， 超高速ネットワークに対応可能な IP パケットリアルタイム解析アルゴリズム，情報処理北海道シンポジウム 2006 講演論文概要集 p11

[2]日経 NETWORK,
http://itpro.nikkeibp.o.jp/free/NNW/NETHOT/20050304/157036/,2006