L-008

Ethernet フレーム情報測定装置の研究・開発
Development of Ethernet Frame Information Analyzer

佐々木　宏幸† 松田　勝敬‡
Hiroyuki Sasaki Masahiro Matsuda

1．はじめに

コンピュータネットワーク上の脅威を防ぐ対策の１つとして，WAN と LAN の境界に設置し，LAN 内部の通信制御を行うファイアウォールアプライアンスや，個々の端末に実装し，端末から送受信される通信の制御を行うパーソナルファイアウォール等，ファイアウォールによる通信制御が広く行われている．しかし，ファイアウォールアプライアンスでは，LAN 内の端末間で行われる通信の制御を行うことが出来ない．パーソナルファイアウォールでも，実装された端末が関与しない通信の制御を行うことが出来ない．

そこで我々は，LAN 内部の通信制御を行うセキュリティシステムを，低コストで実現する研究・開発を行っている[1][2]．システムは，LAN 内の通信制御を行う制御装置と，それらを管理する管理装置から構成される．制御装置に組込み機器を用いることで，システムの低コスト化を図っている．

これまでに，制御装置にボックス PC 等を用いて実装を行い，通信能力の測定を行った．結果，単位時間内に送信される Ethernet フレーム長によっては，通信能力が低下する事がわかった[1]．そこで，ネットワーク中に流れるフレーム長の分布を測定し，提案する制御装置の通信能力が妥当であるか検証を行った．

また，実ネットワークにおけるフレームの特性を調査する測定装置の開発を行い，性能の検証も行った．

2．Ethernet フレーム情報測定装置

2.1　概要

システムの概要を図 1 に示す．ネットワーク中に流れる通信の情報取得と送受信を行う機器をフレームキャプチャ装置，取得した情報の集積を行う機器をログ集積装置と呼ぶ．

フレーム情報の取得と集積を別に行わせる事で，スループット低下を防ぎ，複雑なログの分析を行う事が可能となる．よって，フレームキャプチャ装置を安価な機器で実装することができる．

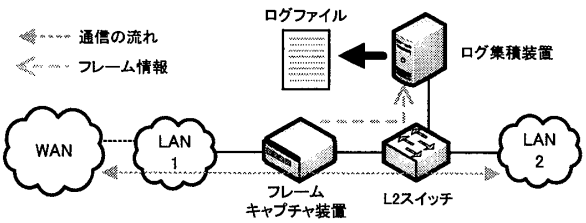

図 1　Ethernet フレーム情報測定装置

フレームキャプチャ装置は，トランスペアレントに動作し，WAN と LAN から来る通信の送受信とフレーム情報の取得を行う．フレームを受信すると，フレーム到着日時，宛先・送信元 MAC アドレス，タイプ，到着ポート，フレーム長を記録する．時刻は 0.1 秒まで記録する．次に，受信フレームをもう一方のポートからそのまま送信し，併せて取得したフレーム情報をログ集積装置に向け送信する．送信には Ethernet フレームを用いる．フレーム長は最小の 64byte で，データ部にフレーム情報を記述する．

ログ集積装置は，フレームキャプチャ装置から送信されるフレーム情報を全て取得し，ログファイルとして出力される．今回は，取得したフレーム情報を全て CSV ファイルとして出力する．

2.2　実装

フレームキャプチャ装置，ログ集積装置に用いた PC は，両者ともに 1000BASE-T に対応した Ethernet チップを有する．Ethernet フレームの制御には，フレームキャプチャ装置では PACKET ソケット，ログ集積装置では WinPcap[3] を用いた．

3．検証

提案したシステムの通信処理能力を検証する為，RFC2544[4]に基づいたスループットの測定を行った．

3.1　検証環境

図 2 に検証環境を示す．テスターのポート 1 からポート 2，テスターのポート 2 からテスターのポート 1 へのフレームを同時に 60 秒間送信する．テスターが受信するフレーム量と，テスターから送信したフレーム量と比較し，2 つの値が一致する最大フレーム量を求める．次に，上記で求めた最大フレーム量をテスターの両ポートから送信し，ログ集積装置で集積されたログとテスターからの送信フレーム量，テスターが受信するフレーム量を比較し，一致した時の送信フレーム量をスループットとした．スループットは，テスターのポート 1 からポート 2，ポート 2 からポート 1 に流れるフレーム量の合計とした．フレーム長が 64, 128, 256, 512, 1024, 1280, 1518byte について，それぞれ 3 回測定し，平均値を最大スループットとした．

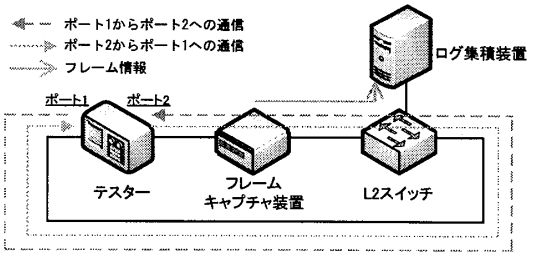

図 2　検証環境

†東北工業大学大学院工学研究科, Graduate School of Engineering, Tohoku Institute of Technology
‡東北工業大学工学部, Faculty of Engineering, Tohoku Institute of Technology

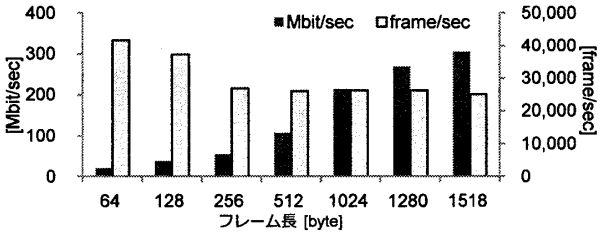

図 3　Ethernet フレーム情報測定装置のスループット

3.2　検証結果

結果を図 3 に示す．最大フレーム長の 1518byte では，304Mbps のスループットを有する．最小フレーム長である 64byte では，スループットは 21Mbps と低い．フレーム処理数(frame/sec)で見ると，フレーム長が 256byte 以上であると約 25000fps の一定の処理数となった．

4. 実ネットワーク環境での検証

上記の結果から，フレーム長が短いとスループットが低下する事がわかった．そこで実環境におけるフレーム長の分布を測定した．

4.1　測定環境

実環境のログとして，図 1 の LAN2 に設置した PC から WAN(Internet)に存在する Web ページを閲覧した時の測定を行う．PC の台数は上記で求めたスループット内に収まるよう 5 台とした．閲覧するのはストリーミング動画を含む Web ページとした．

4.2　測定結果

測定で得られたフレーム長のヒストグラムを図 4 に示す．WAN からの通信では 1418byte，LAN2 からの通信では 64byte のフレーム長が大部分を占める．

次に，出現頻度の多かったフレーム長 64byte と 1418byte について，実環境で測定したログと最大スループットとの比較を行う．64byte と 1418byte のフレーム長に関して，0.1 秒毎のフレーム流量の比較の一部を図 5，図 6 に示す．0.1 秒の短時間内にバースト的な通信が流れる時があるが，測定で得られた最大スループットを超えることはない．

また，フレームが到着してから次のフレームが到着するまでのフレーム間隔を測定する．図 7，図 8 に結果の一部，表 2 に 60 秒間での平均値を示す．ここでは，0 の値は通信が流れていない状態を指す．スループット測定時は，短い時間でほぼ途切れなく通信が流れている．実ネットワーク環境の場合，通信の間隔はスループット測定時よりも長く，通信が何も流れていない時間も存在する．表 2 の結果からも，実環境のネットワークではスループット測定時の環境より 2 桁分フレーム間隔が広い事がわかる．

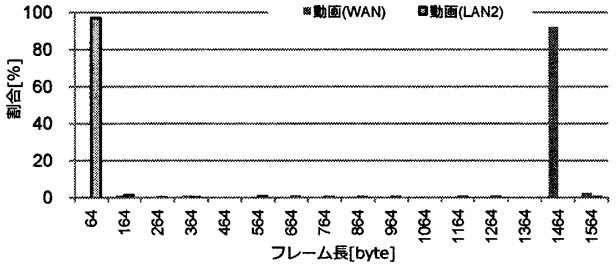

図 4　Web ページ閲覧時におけるフレーム長のヒストグラム

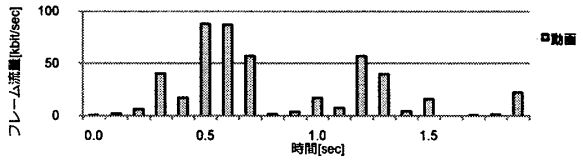

図 5　フレーム流量の比較(LAN1 から WAN, 64byte)

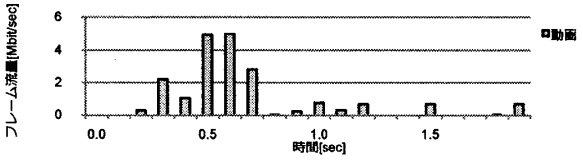

図 6　フレーム流量の比較(WAN から LAN2, 1418byte)

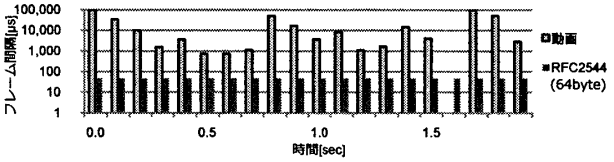

図 7　フレーム送信間隔の比較(LAN2 から WAN, 64byte)

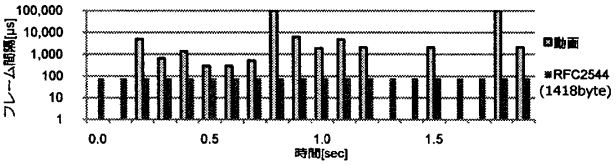

図 8　フレーム送信間隔の比較(WAN から LAN2, 1418byte)

表 2　フレーム間隔の平均時間

WAN から LAN2(1418byte)		LAN2 から WAN(64byte)	
測定対象	時間[ms]	測定対象	時間[ms]
スループット測定	0.08	スループット測定	0.05
動画 Web ページ	3.10	動画 Web ページ	5.94

5. 考察とまとめ

実ネットワークにおける Ethernet フレームの特性を調査する為，Ethernet フレーム情報測定装置の開発を行った．

性能を検証した結果，実ネットワーク環境においては，流れるフレーム間の間隔が広く，バーストトラッフィクが発生しても最大スループットを超えることはない．よって今回開発した測定装置は，数名規模のネットワークでの測定においては有効であるといえる．今後は，ユーザを増やした状況等，より負荷をかけた状態での有効性等を検証する．

参考文献

[1] 佐々木 宏幸，松田 勝敬：分散型通信制御セキュリティシステムの開発，第 8 回情報科学技術フォーラム第 4 分冊，pp.133-134 (2009).

[2] 佐々木 宏幸，松田 勝敬：分散型通信制御セキュリティシステムの組込み機器への実装に関する考察，情報処理学会創立 50 周年記念(第 72 回)全国大会 講演論文集(分冊 3)，pp.379-380(2010).

[3] WinPcap：WinPcap, The Packet Capture and Network Monitoring Library for Windows，WinPcap(オンライン)，入手先〈http://www.winpcap.org〉.

[4] IETF：RFC2544 - Benchmarking Methodology for Networks Interconnect Devices，IETF(オンライン)，入手先〈http://www.ietf.org/rfc/rfc2544.txt〉.