1X-06

大規模ネットワークエミュレーション環境のためのトラフィックモニタリングの検討

馬場大輔　　宮崎敏明

会津大学大学院コンピュータ理工学研究科

1. はじめに

日本全国規模を想定するような大規模なネットワークシステムの挙動を詳細に把握するには，エミュレーション環境を用いるのが有効である．しかし，システムが大規模化するにつれて，エミュレーションシステム内部に発生するトラフィック量が増大し，その取り扱いが困難になる．本稿では，大規模ネットワークのエミュレーションが可能なシステムのためのトラフィックモニタリング手法を提案する．

2. 大規模ネットワークエミュレーション

図１に我々が想定する大規模ネットワークエミュレーション環境と，提案するモニタリングシステムの概要を示す．エミュレーションシステムは，実ネットワークで接続された複数台のサーバからなる．実際のエミュレーションは，CORE (Common Open Research Emulator)[1]を各サーバに実装し，実現する．エミュレーションによって再現されるネットワークデバイスは各サーバに分散配置され，デバイス間で発生する通信トラフィックは各エミュレーションサーバ内もしくは複数マシンにまたがって発生する．それら，分散的に発生するトラフィック情報を一括して扱いモニタリングすることが大規模ネットワークの挙動を把握する上で重要である．

3. 提案手法

提案する大規模エミュレーション向けモニタリングシステムは，各エミュレーションサーバからネットワークトラフィックを取得するトラフィックキャプチャ機能と，エミュレーション定義から読み取った情報を基にネットワークトポロジを描画し，その上に定期的に読み取った情報を表示するモニタリング機能からなる．

3.1. トラフィックキャプチャ機能

図１に示した通り，我々の想定するエミュレーションシステムでは，複数のサーバにネットワークデバイスが散在しておりトラフィック状況の一括把握が難しい．そこで提案手法では，まず，すべてのサーバ内の仮想デバイスのネットワークインタフェースに対して，個別にtcpdump[2]を実行し，当該トラフィックを一定時間キャプチャして，ローカルディスクに一次保存する．つぎに，それら一次保存したトラフィックキャプチャ情報を，後述するモニタリングシステムに送信し，一括監視を実現する．

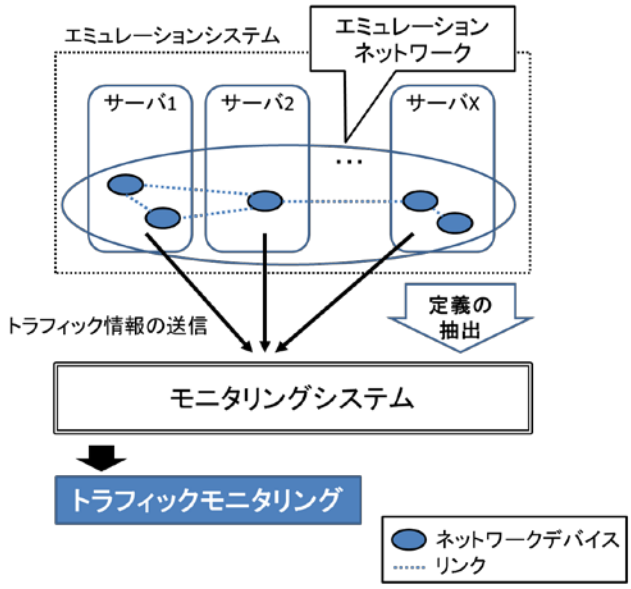

図１： 大規模ネットワークエミュレーションとモニタリングシステム概要

3.2. モニタリング機能

提案手法では，ネットワークトラフィックをより直感的に提供するためにネットワークトポロジに関連付けて提供する．モニタリング機能部では，予め定義されたトポロジを含むネットワーク情報をエミュレーションシステムから抽出する．抽出した情報を基にデバイス位置及びそれらを結ぶリンクを描画する．また，各サーバから送信されるトラフィック情報を基に一定時間ごとに描画情報を更新することで，複数サーバから成るエミュレーション上のトラフィックを容易に把握することができる．一例を図２に

Network Traffic Monitoring for a Large-scale Network Emulation System
Daisuke Baba, Toshiaki Miyazaki
Graduate School of Computer Science and Engineering, the University of Aizu

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.

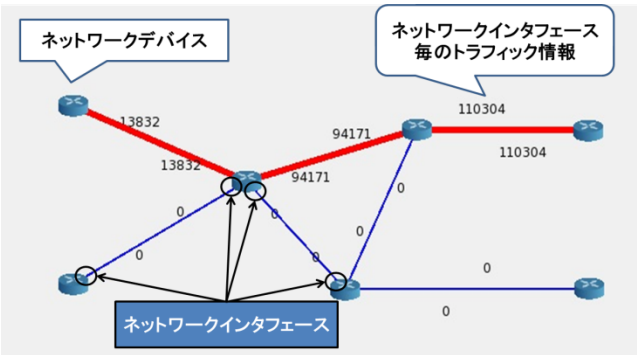

図２： トラフィックモニタリング例

示す。複数のネットワークデバイスとそれらを結ぶトポロジが描画されている．また，各ネットワークデバイスからキャプチャされたトラフィックをトポロジ上に数値情報として表示している．

4. 評価

提案システムのモニタリング性能は，各サーバからのトラフィック情報の収集性能に依存する．我々はシステムの性能を評価するために，7 台のエミュレーションサーバに CORE を起動し，評価用ネットワークを構成した．表 1 に各エミュレーションサーバのハードウェア環境を示す．ただし，7 台の内 1 台はモニタリング環境としても利用し，そのメモリ・CPU は，表 1 の括弧内に記載した通りである．評価用ネットワークとして 3 つのケース case1, case2, case3 を用意した．各ネットワーク構成を表 2 に示す．表 2 におけるデバイス数とは，1 つのエミュレーションサーバ内に再現されるルータ・スイッチなどの仮想ネットワークデバイスの個数であり，case1 については全サーバでの総数は 7 個となる．すべてのケースでフルメッシュトポロジを構成し，各デバイスは他のすべてのノードと直接接続されるリンクを有する．そのために使用されるネットワークインタフェースの総数を総インタフェース数とする．各ケースのネットワークに対し，モニタリングシステムを適用し，3 分間各サーバからのトラフィックデータを収集した．結果を表 3 に示す．受信データ数は 3 分間でモニタリングシステムが受信したトラフィックデータを記録したファイル数を示す．受信セット数は受信データ数を各構成の総インタフェース数で割った数値である．本システムではインタフェースごとに 1 ファイルを生成するため，受信セット数は各インタフェースが送信できたデータ数となる．さらに，稼働時間を受信セット数で割ることで各インタフェースが何秒ごとのデータ送信が可能であるかを示している．case2 の評価結果から，使用されるネットワークインタフェース数が 200 近い大規模ネットワーク環境においても，提案システムが 10 秒に 1 回の頻度で情報が更新されるトラフィックモニタリングが可能であることがわかる．この結果は，我々のシステムが，大規模ネットワークエミュレーションにおいて，完全ではないが，ほぼリアルタイムのトラフィック監視が可能であることを示している．

表１： エミュレーションサーバ環境

OS	CentOS release 6.6 Final
メモリ	8 GB (32 GB)
CPU	Intel(R) Xeon(R) CPU E3-1230 V2 @ 3.30GHz (Intel(R) Xeon(R) CPU E5-2470 0 @ 2.30GHz)

表２： ネットワーク構成

	デバイス数	総インタフェース数
case1	1	42
case2	2	182
case3	3	420

表３： 各ネットワーク構成に於けるトラフィックモニタリングシステムの評価結果

	受信データ数	受信セット数	180(秒) / 受信セット数
case1	3, 427	81. 6	2. 2
case2	3, 618	19. 9	9. 1
case3	3, 704	8. 8	20. 4

5. 終わりに

大規模ネットワークシステムのエミュレーションにおいて発生する膨大なトラフィック量を把握・監視するためのモニタリングシステムを提案した．複数のネットワーク構成に対して，性能評価を行い，200 近いネットワークインタフェースを使用する大規模ネットワークでも，准リアルタイムなトラフィックモニタリングが可能であることを示した．今後は，実ネットワークとの混合環境も含む，ネットワーク定義およびトラフィックモニタリングが容易にできる大規模ネットワークエミュレーションシステムの構築を目指す．

謝辞

本研究の一部は，総務省戦略的情報通信研究開発推進制度(SCOPE No.121802001)の支援を受けて実施したものである．

文献

[1] J. Ahrenholz, C. WA Danilov, T. R. Henderson, J. H. Kim, “CORE: A real-time network emulator,” IEEE Military Communications Conference (MILCOM 2008), pp. 1-7, 2008.
[2] “TCPDUMP & Libcap,” http://www.tcpdump.org/

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.