広帯域ネットワーク監視を実現するアダプティブなNIDSクラスタに向けたソフトウェアロードバランサの提案

山田 正弘*, 市川 昊平*, 阿部 洋丈*, 伊達 進*, 下條 真司†
*大阪大学, †情報通信機構 (NICT)

I. 研究の背景と目的

近年，ネットワーク技術の発達により 10Gbps を超える広帯域ネットワークが普及しつつあり，ネットワークを利用する様々なシステムにおいて，処理の高速化や分散化が必要となってきている．特に，ネットワーク監視による侵入検知システム (NIDS: Network-based Intrusion Detection System) に関する研究は，ネットワークの広帯域化に伴い，高速処理が強く求められている分野である．しかし，今日の一般的なソフトウェア NIDS では，広帯域ネットワークにおける膨大な量のトラフィック解析処理に対応できない．そのため，広帯域ネットワーク監視には，FPGA などのカスタムハードウェアによって実装した NIDS が必要とされており，導入コストが高く，かつスケーラビリティに欠けている．

この問題に対し，ソフトウェア NIDS を導入した汎用計算機でクラスタを構成して分散解析を行う NIDS クラスタ [1] が提案されている．しかし，文献 [1] では，クラスタのノードに監視トラフィックを分割するためのロードバランサが高価なハードウェアで実装されており，コストパフォーマンス，スケーラビリティが不十分である．また，トラフィック量の時間的な変化に関わらず，解析を行うクラスタ構成が静的であり，計算機資源の利用が非効率的である．そこで，本研究では，クラスタの各ノードの負荷とトラフィック量に応じて，クラスタ構成を動的に変更するアダプティブな NIDS クラスタの実現を目指し，各ノードへトラフィックを分割するソフトウェアロードバランサを提案する．

II. 提案

本研究では，汎用計算機によるソフトウェアロードバランサ，および，Bro [2] などの既存の NIDS を導入した複数の汎用計算機による低コストな NIDS クラスタの構築を提案する．しかし，複数の NIDS ノードによって解析処理を分散化する場合，単純に監視トラフィックのパケットをランダムに各ノードへ分配すると，解析を行うノードがコネクション状態を追跡することができないため，検出漏れが発生する可能性がある．また，分配の際に IP ヘッダ等を書き換えると，パケットの持つコネクション情報が失われるため，正常に解析処理が行われない．したがって，提案するロードバランサでは，以下の機能を考慮して実装する必要がある．

- 同一のコネクションに属するパケットは同一のノードに分配する機能
- パケットの IP ヘッダおよびアプリケーションレイヤのヘッダ情報を変更せずに分配する機能
- 各ノードがオーバロードしないロードバランシング機能

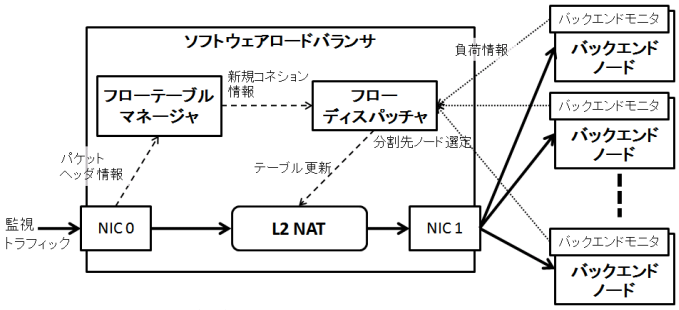

Fig. 1. 提案するソフトウェアロードバランサ

以上のことを考慮した，提案するロードバランサのアーキテクチャを Fig.1 に示す．提案するロードバランサは，フローテーブルマネージャ，L2 NAT，フローディスパッチャ，バックエンドモニタから構成される．フローテーブルマネージャは，コネクション情報を管理し，監視トラフィックから新規コネクションの情報を抽出する．L2 NAT は，送信先 MAC アドレスを分配先ノードの MAC アドレスに変換することで，IP ヘッダ等の解析に必要な情報を書き換えることなく，監視トラフィックのパケットをバックエンドノードへ分配する．フローディスパッチャは，新規コネクションを，バックエンドノードの負荷に応じて選定したノードに分配するためのルールを L2 NAT に追加する．バックエンドモニタは，各バックエンドノードの負荷を監視し，負荷情報をフローディスパッチャに送信する．

これら 4 つのコンポーネントが連動することで，提案するロードバランサは，バックエンドノードをオーバロードさせることなく，監視トラフィックをコネクション単位で分割する．現在，ロードバランサをソフトウェアとして実現することで，トラフィック量に応じたクラスタ構成の動的な変更を可能にする具体的な動的変更手法について検討中である．以上により，広帯域ネットワーク監視に向けた，コストパフォーマンスの高い，スケーラブルかつアダプティブな NIDS クラスタの実現に向けた，汎用計算機ベースのソフトウェアロードバランサを提案する．

REFERENCES

[1] M. Vallentin, R. Sommer, J. Lee, C. Leres, V. Paxon, B. Tierney, ”The NIDS Cluster: Scalable, stateful, network intrusion detection on commodity hardware”, Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID 2007), pp.107-126, 2007
[2] V. Paxon, ”Bro: A system for detecting network intruders in real-time” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol.31, Issue.23-24, pp.2435-2463, 1999