ISS-P-139

DDoS 攻撃を防止するソフトウェアルータについて

桑原　貴明†　　岡部　寿男††
† 京都大学大学院情報学研究科　　†† 京都大学学術情報メディアセンター

1. はじめに

通信サービスの事業者は，サービスを提供するために，スイッチやルータといった高価かつ消費電力の高いネットワーク機器を購入する．さらに，ネットワーク機器が使用される期間の間隔は徐々に短くなっており，ネットワークを流れるトラフィックの増加に伴って，サービスを提供するために必要なコストも増加し続けている．

NFV(Network Function Virtualization)[1]に基づくネットワーク機器は，汎用的なハードウェアでのみ構成されている．NFVによるネットワーク機器を仮想化するメリットは，従来のネットワーク機器では困難であった，ネットワーク機能のリソースの動的な変化が可能という点が大きい．一方で，汎用のハードウェアを使用することにより，従来のネットワーク機器の処理速度を維持することは難しくなり，ネットワーク機器を仮想化する上の課題となっている．

そこで本研究は，ネットワーク層の機器であるルータを取り上げ，膨大なAccess Control List(ACL)を保持し，かつACLを高速に検索することが可能なソフトウェアルータを実装し，DDoS攻撃への対策を行うことを目的とする．

2. NFV(Network Function Virtualization)

NFV はネットワークを仮想化するためのコンセプトである．NFV によるネットワークを仮想化により，ネットワーク管理者は必要に応じて，ネットワークのリソースを変更したり，仮想的にネットワーク機能の容易に展開することができる．

3. DDoS 攻撃

DDoS(Distributed Denial of Service)攻撃は，複数のコンピュータホストから，一斉に特定のホスト，あるいはネットワークに対して接続要求を送り，対象の通信容量を超えるトラフィックを故意に発生させることで，サービスを停止させる攻撃である．

仮想ルータならば，従来のルータでは困難であった，大きなサイズのACLやルーティングテーブルを同時に保持するという課題を解決することができるが，一方でテーブルの高速な検索という課題も残る．

4. まとめと今後の方針

ソフトウェアルータが動作する仮想マシンの入出力の処理速度についての研究は複数存在しており，特にNetVM[2]というプラットフォーム上では，通信速度が10Gbpsの時に，ワイヤーレートを達成している．

また，通常のハードウェアを用いた，高速なテーブルの検索を行うアルゴリズムも提案されている[3]．そこで本研究では，これらの研究をもとに，大量のエントリを保持する QoS ACL (Quality of Service Access Control List)や Security ACL を保持できるように．リソースを必要に応じて動的に確保できるようなソフトウェアルータを実装する予定である．図 1 に提案するソフトウェアルータの概要を示す．

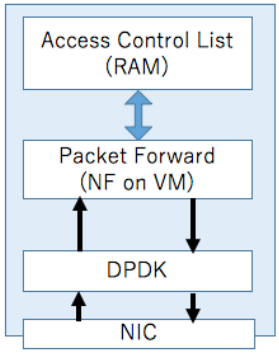

図1. 提案するソフトウェアルータの概要

このソフトウェアルータでは，DPDK を用いて仮想マシン上の Network Function(NF)に直接パケットを届けることで，高速化が期待できる．

参考文献

[1] ETSI Network Fucntion Virtualisation http://www.etsi.org/technologies-clusters/nfv

[2] J Hwang et al. "NetVM: high performance and flexible networking using virtualization on commodity platforms" *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*

[3] H Asai et al. "Poptrie: A Compressed Trie with Population Count for Fast and Scalable Software IP Routing Table Lookup" *ACM SIGCOMM 2015*