高速ネットワーク処理と欺瞞的防御システムおよび高信頼ネットワークファンクション

大阪大学大学院工学研究科
電気電子情報通信工学専攻　特任准教授　髙野　祐輝

1 はじめに

2010年代初頭から、LinuxやFreeBSDといったオペレーティングシステム（OS）に、netmap [1]やXDP [2]といった、高速にネットワーク処理を行うための機構が提案・実装され始めてきた。これらが提案されるまでは、パフォーマンスの問題でLinuxなどのが搭載された汎用PCは商用ネットワークのネットワークファンクション*1（NF）としてはとても利用できなかった。

例えば、Ehternetフレームの最小サイズはプリアンブル等を含めると84バイトとなるが、1 Gbpsのネットワークでは秒間あたり最大で$10^9/(84\times8)\approx1.488$ M packets per second（pps）のフレームが送信可能であるが、LinuxのRaw Socketなどではどれだけ最適化しても、数百Kpps　程度しか速度が出なかった。ところが、netmapなどを利用すると10 Gbpsネットワークの秒間最大転送フレーム数である、14.88 Mppsに迫る性能でネットワーク処理を行うことが出来るようになった。2018年に発表されたXDP　の論文によると、XDPを用いることで1 CPUコアで10　Gpps弱、6 CPUコアで45 Gpps程度もの性能でパケット転送することが可能になったと報告されている[2]。従来まではこれと同じ性能でパケットを転送するためには、専用ハードウェアが必須であり、それらは非常に高価であった。しかし、汎用PCとOSでこのような処理が可能になったということは、ソフトウェアでかつ安価にNFを実装可能になったということであり、これら技術の登場がNetwork Function Virtualization（NFV）やSoftware Defined Network（SDN）、Internet of Things（IoT）の機運を高めてきた一因でもあると考えられる。

2　SF-TAP

このような高速ネットワーク処理機構の登場に伴い、我々のチームはScalable and Flexible Traffic Analysis Framework（SF-TAP）[3]というアプリケーションレイヤのトラフィック解析ソフトウェアの設計と実装を行った。OSのサポートによっていくら高速にネットワーク処理が行えるようになったとしても、それはあくまでもパケット単位の話であり、それらを高速に解析するためにはまた別のメカニズムが必要である。

ご存じの方も多いと思うが、現代コンピュータはCPUの動作クロック周波数が頭打ちになり、CPUコアを増加させる方向で進化している。そのため、CPU性能を十分に引き出すには、並行・並列プログラミングが不可欠であるがこれを行うためには熟練の技術が必要という問題がある。

そこで我々は、この問題を解決し、CPUコアスケールさせるのが難しいと言われているPython等でトラフィック解析ソフトウェアを実装しても、CPU性能を十分引き出せるようなアーキテクチャを提案した。その概略が図1となる。

図1で我々が設計・実装を行ったのは、真ん中に位置するSF-TAP Cell Incubator（SCI）と、上の4つの箱中にあるSF-TAP Flow Abstractor（SFA）である。SCIは左下に位置する内部ネットワークと右下に位置するインターネット間のネットワークトラフィックをキャプチャし、TCPのフローレベルで上に位置するSFAへロードバランスしながらコピーする。従来、10 Gbpsレベルの帯域でこのような処理を汎用OSで行うのは難しかったが、SF-TAPではnetmapとマルチコアスケールするパケットキャプチャ機構を設計・実装して実現した。SFAではSCIから受け取ったパケットをTCPフローレベルで再構築し、それをファイル抽象化して解析アプリケーションに提供する。このとき、複数の抽象化されたファイルへとロードバランスしてTCPストリームを出力するため、解析アプリケーションは複数プロセスを用いて別々にファイルを読み込むだけでCPUコアスケールすることが出来るようになった。以上がSF-TAPの簡単な概要となる。

SF-TAPは情報通信研究機構で開発・運用中の標的型攻撃対策システムであるSTARDUST [4]で実際にネットワークトラフィック解析のために利用されている。標

*1 スイッチやルータなどと言ったネットワーク機能

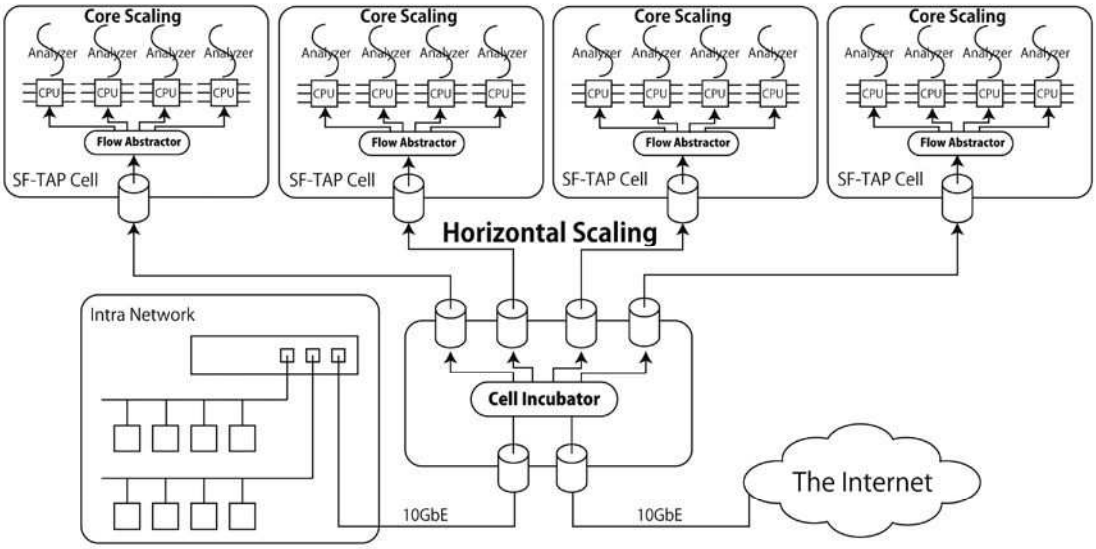

図1　SF-TAP のアーキテクチャ

的型攻撃とは、ある組織を特定して狙った攻撃であり、過去には国民年金機構が対象となったり、最近では防衛関連企業が被害を受けていたことも明らかとなっており、標的型攻撃はもはや国家レベルの驚異となりつつある。STARDUST では、標的型攻撃の解析を目的として、SF-TAP以外にも様々な技術をもちいて攻撃誘引及び解析を行っている。

3　欺瞞的防御システムとネットワークファンクション

次に、本節では欺瞞的防御システムについて解説したい。欺瞞的防御システムとは、囮となるノードをネットワーク上に配置し、万一、組織ネットワーク内に侵入・攻撃などをされたとしても、攻撃を囮ノードへとそらすことで被害を低減させるような手法である。従来までのネットワークの防御手法は、境界型防御がメインであり侵入されないことが前提であった。しかし、欺瞞的防御では、侵入・攻撃はいつでも起こりうることと想定して防御を行うような手法である。

実際、IoT などのデバイスはソフトウェアアップデートが満足に行われなかったり、標的型攻撃とよばれる攻撃では人間をターゲットにフィッシングを行って侵入したりと、完全に侵入を防ぐのは困難な状況になりつつあるのが現状である。

欺瞞的防御システムは主にネットワーク型、システム型、アプリケーション型、データ型の 4 つに分類されるが、我々はネットワークレベルで欺瞞的防御を行うネットワーク型を対象に研究を行っている。ネットワーク型の欺瞞的防御システムで重要なのは、やはり、パフォーマンスである。今後 IoT の普及とともに、数万台、数十万台といったデバイスが接続されることが想定される。欺瞞的防御システムでこれらを守るためには、さらに数十倍規模のネットワークのエミュレーションが必要となると考えられるが、これを実現するには、低コストかつ高性能でおこなう必要がある上、適切な抽象化が求められる。

そこで我々は、大規模ネットワークに対しても欺瞞的防御システムを適用可能とするため、汎用 PC サーバを用いて実現できるようXDP を用いた設計・開発を行っている。本プロジェクトはまだ研究段階だが、その一部を日本最大のセキュリティ研究会の一つであるSCIS 2020 にて発表した[5]。結論のみ述べると、1.6 Mpps のトラフィックに対して、Raw Socket などの実装ではパケットロス率が74.8% であったの対して、XDP を用いた実装では 0.1% 以下にまで低減した。今後はこれをさらに発展し、実ネットワークへ適用していきたいと考えている。

4　高信頼ネットワークファンクション

ところで、XDP を用いると高速にパケットを処理可能になるが、その利用には厳しい制限がある。特に、XDP が内部的に用いる、BPF Verifier と呼ばれるプログラム検証機は偽陽性と判定することも多い上に、Berklay Packet Filter 形式のバイトコードレベルでしか検証が行われないためエラーの解読が難解であり、C 言語などのプログラミング言語レベルでエラー箇所を突き止めるのが難しい場合がある。そのため、実際に実装を行うためにはかなりのバッドノウハウが必要となるのが現状である。

これら問題が明らかとなったため、我々は欺瞞的防御システムの研究と並行し、XDP を用いた NF 実装のためのドメイン固有言語の研究・開発、および、リファインメント型などを備えたプログラミング言語 F*[6] での NF 実装の研究・開発もすすめている。高信頼かつハイパフ

ォーマンスなNF実装は、欺瞞的防御システムのみならず、NFV、SDN、IoT、Edge Computingといった様々な分野で求められる技術である。今はまだ取り組み始めたばかりであるが、成果が出た後にまた報告したい。

以上、我々の行っている取り組みについて紹介した。簡単ではあったが、何かの一助となれば幸いである。

参考文献

[1] Luigi Rizzo. netmap: A Novel Framework for Fast Packet I/O. In Gernot Heiser and Wilson C. Hsieh, editors, *2012 USENIX Annual Technical Conference, Boston, MA, USA, June 13-15, 2012*, pp. 101–112. USENIX Association, 2012.

[2] Toke Høiland-Jørgensen, Jesper Dangaard Brouer, Daniel Borkmann, John Fastabend, Tom Herbert, David Ahern, and David Miller. The eXpress data path: fast programmable packet processing in the operating system kernel. In Xenofontas A. Dimitropoulos, Alberto Dainotti, Laurent Vanbever, and Theophilus Benson, editors, *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies, CoNEXT 2018, Heraklion, Greece, December 04-07, 2018*, pp. 54–66. ACM, 2018.

[3] Yuuki Takano, Ryosuke Miura, Shingo Yasuda, Kunio Akashi, and Tomoya Inoue. SF-TAP: Scalable and Flexible Traffic Analysis Platform Running on Commodity Hardware. In *29th Large Installation System Administration Conference, LISA 2015, Washington, D.C., USA, November 8-13, 2015*, pp. 25–36. USENIX Association, 2015.

[4] 津田侑, 遠峰隆史, 金谷延幸, 牧田大佑, 丑丸逸人, 神宮真人, 高野祐輝, 安田真悟, 三浦良介, 太田悟史, 宮地利幸, 神薗雅紀, 衛藤将史, 井上大介, 中尾康二. サイバー攻撃誘引基盤stardust. コンピュータセキュリティシンポジウム2017 論文集, 第2017巻, oct 2017.

[5] 竹中幹, 高野祐輝, 宮地充子. XDPを用いたネットワーク型欺瞞的防御システムの設計と実装. In *Symposium on Cryptography and Information Security (SCIS) 2020*, 2020.

[6] Jonathan Protzenko, Jean Karim Zinzindohoué, Aseem Rastogi, Tahina Ramananandro, Peng Wang, Santiago Zanella Béguelin, Antoine Delignat-Lavaud, Catalin Hritcu, Karthikeyan Bhargavan, Cédric Fournet, and Nikhil Swamy. Verified Low-Level Programming Embedded in F*. *CoRR*, Vol. abs/1703.00053, 2017.

（北陸先端科学技術大学院大学
情報科学研究科　博士後期課程　平成23年修了）