様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ５ 月 ２８ 日現在

機関番号：１２６０１
研究種目：若手研究
研究期間：2018～2019
課題番号：１８Ｋ１８０４３

研究課題名（和文）DDoS緩和技術のためのACLルール数の大規模化

研究課題名（英文）Design of a Scalable Access Control List for DDoS Mitigation

研究代表者
空閑　洋平（Kuga, Yohei）

東京大学・情報基盤センター・特任講師

研究者番号：９０８１６５９７

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本研究では，ハードウェアACLによるDDoS緩和技術を検討した．本手法は，PCIeデバイスをホストPCに接続し，フィルタルールをホストメモリに保存，DMAを用いてPCIeデバイスがフィルタルールを直接検索する．その結果，大容量のフィルタルール数と処理性能を両立したDDoS緩和が可能になる．
また，本提案アーキテクチャのような専用PCIeハードウェアのプロトタイプをソフトウェアで試行錯誤可能な開発手法の提案した．本提案手法は、ネットワークハードウェアの研究開発の簡易化に貢献した．

研究成果の学術的意義や社会的意義
パスワードの脆弱な監視カメラや家庭用ルータなどのIoT機器に感染するマルウェアの登場によって，IoTデバイスを用いたDDoS攻撃が大規模化している．本研究は，ソフトウェアによる柔軟なフィルタルールの記述と高スループット処理を両立したハードウェア型DDoS緩和を可能にし，インターネット運用の健全化に貢献する．

研究成果の概要（英文）：We researched a new mitigation method for DDoS attacks. The proposed method handles network traffic with hardware ACL filters on PCI Express (PCIe) devices, and the filter rules are stored on the host memory of the host PC connected with PCIe. In the method, the filter circuit operates the host memory by DMA. Thus, it enables high throughput DDoS mitigation with large memory space.
And we proposed a prototype environment for developing PCIe hardware by network programming. As this result, the proposed method has contributed to simplifying the research and development for network hardware.

研究分野：ネットワークハードウェア

キーワード：DDoS緩和　PCI Express　ネットワークハードウェア　インターコネクト

様　式　Ｆ－１９－２

１．研究開始当初の背景

DDoS 攻撃は，サービスを提供するサーバへの負荷，大量の攻撃トラフィックによって通信帯域を専有することで，攻撃先サービスの本来意図した動作を妨害する目的で実施される．2016 年 9 月に発生した MIRAI 型 DDoS 攻撃は，パスワードの脆弱な監視カメラや家庭用ルータのような常設型 IoT 機器に感染するマルウェアによって 600 Gbps 以上の規模で行われた．MIRAI 型のマルウェアは，一時およそ 60 万台の IoT デバイスに感染していたと報告されている．今後，IoT 機器数の増加に従い，このような IoT 機器を利用した DDoS 攻撃がより大規模化していく恐れがある．

既存のアンプ型 DDoS 攻撃は，DNS (Domain Name System)や NTP (Network Time Protocol)などのパブリックなサービスホストを利用し，大量のプロトコル返信メッセージを攻撃先ホストに転送することでネットワーク帯域を埋めるサービス妨害を行う．アンプ型の攻撃は，攻撃に利用される送信パケットサイズが大きいため，攻撃元ホスト 1 台あたりの送信トラフィック量が多く，数百ノード数で高トラフィックの攻撃が可能である．アンプ型 DDoS 攻撃の防御には，パブリックサーバへの対策に加えて，中間機器で ACL(Access Control List)などを利用することで，一時的に攻撃パケットを遮断することが可能である．

一方，MIRAI をはじめとする IoT 機器を用いた攻撃は，攻撃ホスト 1 台あたりの送信トラフィックはアンプ型に比べると小さいが，攻撃ホスト数が非常に多い特徴がある．DDoS 攻撃をフィルタリングや緩和する対策機器は，ACL(Access Control List)ベースのハードウェアや，異常検知手法を用いたソフトウェアなどで構成される．これら既存の DDoS 緩和技術は，搭載できるメモリサイズの制限によって，静的フィルタの記述可能なルール数に限界がある．今後の IoT 機器数の増加によってこれら記述可能なルール数では不足する可能性があり，将来的には既存のルール数をボトムアップで増やす対策とは異なるアーキテクチャ検討が必要となると考えられる．

２．研究の目的

本研究は，データセンタにおける 100 Gbps，400 Gbps を超える DDoS 想定し，ハードウェアによる DDoS 緩和アーキテクチャを検討した．既存のソフトウェアによる DDoS フィルタ数緩和技術のみでは，MIRAI 規模の DDoS 攻撃に対応することは処理性能，フィルタルールの管理方法の側面から困難であること考えられる．そこで，本研究では全 IPv4 アドレス空間のフィルタルールが記述可能な，ハードウェアフィルタの性能と，ソフトウェアによる柔軟なルール記述を両立した DDoS 緩和アーキテクチャを研究開発することで，今後の IoT 時代の DDoS 攻撃ノード数に対応可能なことを実装で示し，インターネット運用の健全化に貢献を目指した．本研究は，PCIe デバイス型の DDoS 緩和手法の全体アーキテクチャの提案と，その基礎となる PCIe デバイスのプロトタイプ環境の実現の 2 つの研究課題を実施した．

(1) DDoS 緩和のための全 IPv4 空間を対象とした ACL アーキテクチャの検討

ネットワークトラフィックをインラインで処理可能な NIC 型の DDoS 緩和アーキテクチャを検討した．本提案システムは，PCIe 経由でホスト PC のメインメモリに DMA で ACL ルールを保持することで，広大な DRAM メモリを使用可能にする．それにより，全 IPv4 アドレス空間を対象とした ACL システムの構築が可能なことを確認した．

(2) ソフトウェアによる PCIe デバイスプロトタイプ環境の実現

本提案 DDoS 緩和手法は，専用 PCIe ハードウェアからホスト PC のメインメモリを DMA (Direct Memory Access)で操作する必要がある．DMA を使用する PCIe デバイスの転送性能は，デバイスドライバとハードウェア回路両方の側面から最適化する必要がある．そこで本研究では，DMA を用いる PCIe デバイスをソフトウェアで構築可能なプロトタイピング環境を提案した．

３．研究の方法

はじめに，ソフトウェアによる PCIe デバイスのプロトタイプ環境を構築，実装することで，PCIe デバイスを用いたプロトタイプシステムをソフトウェアで試行錯誤可能にした．そして，本プロトタイプ環境を用いて PCIe 通信の挙動を確認，提案 DDoS 緩和システムを試行錯誤する研究方法を実施した．

４．研究成果

(1) 図 1，2 は，提案する DDoS 検索のための ACL ルール検索回路の全体概要とハードウェアによる IPv4 アドレス検索用のデータ構造を表す．IPv4 空間には，ローカル IP アドレスやマルチキャスト IP アドレス，経路表に乗っていない IP アドレス空間といった，本来フィルタルールとしてはじめから除外可能なアドレス空間があるため，これらを除外することによって，1 IP アドレスあたりの保持可能なフィルタルール容量を増加可能であると考えられる．本アーキテクチャでは，フィルタルールのデータ構造として，CPU のメモリ管理方法であるページング手法を DDoS フィルタルール管理に応用することを検討した．一般的な CPU は，DRAM メモリへのアクセス遅延を隠蔽するために，キャッシュと呼ばれる手法を用いて連続したメモリへのアクセスを高速化している．また，効率的なメモリ管理，不要なメモリ空間を圧縮管理するために，ページングと呼ばれる動的なメモリ割り当てアーキテクチャが用いられている．本研究の想定する IPv4 アドレスは 32 bit であり，CPU アーキテクチャも同様に 32 bit または 64 bit アーキテクチャである．そこで，IPv4 アドレスを CPU アーキテクチャに見立て，CPU のページングアクセス回路を実装する．本アーキテクチャでは，フィルタルールを検索する IPv4 アドレスを 2 つ以上の bit データに分割する．そして，上位 bit から Page Directory を検索することによって，Page Table，Page に該当フィルタルールの存在を判定する．IP アドレスは CIDR による上位 bit からのクラス分けで管理されるため，本データ構造によって，フィルタルールが不必要な IPv4 アドレス空間を除外することが期待できる．

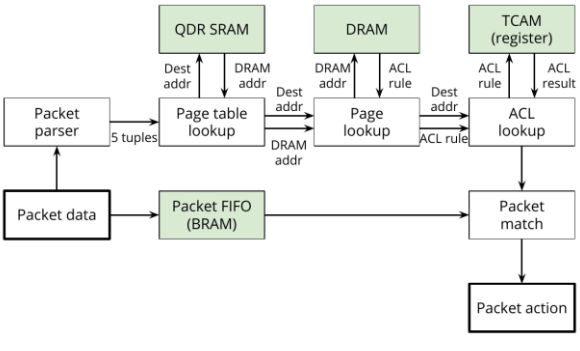

図 1 ACL ルールの検索回路概要

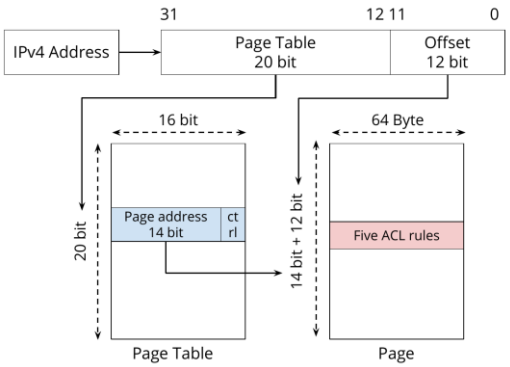

図 2 IPv4 アドレスによる ACL ルールの検索

一般的に ACL の検索には TCAM 回路が用いられるが保持可能なルール数に上限がある．そこで，本アーキテクチャでは，ACL ルールをホストメモリで保持し，検索の都度，1 エントリ分の TCAM 回路に展開，検索することで DRAM と TCAM を併用したアーキテクチャを提案した．本研究ではデータ検索手法をシミュレーションで評価し，2 段ページとした場合，8MB ページテーブルサイズで，DRAM 上で最大 131,072 IP アドレスについてそれぞれ 5 つずつの ACL ルール，合計 655,360 個の ACL ルールが保持可能となることを確認した．

(2) 図 3，4 は，本研究で提案した PCIe デバイスのプロトタイプ環境の概要と，FPGA デバイスを用いた実装による性能評価を表す．PCIe デバイスのプロトタイピングには，FPGA や ASIC を用いたハードウェア記述言語によるプロトタイプデバイスの開発や，QEMU や GEM5 を利用したデバイスエミュレーション環境が利用される．それぞれ，FPGA は物理デバイスとしてホスト PC に接続して動作可能であるが，性能を伴ったデバイス開発は非常に困難である一方，QEMU を用いたデバイスはホスト PC に接続はできないが，エミュレーションホスト上のデバイスとして Linux に認識させ，デバイスドライバの開発などの利用でき，ソフトウェアで開発可能であることから，FPGA に比べて開発が用意である．本提案アーキテクチャは，FPGA と QEMU それぞれの利点を活かし，ソフトウェアで開発可能でありながら，物理ホストと接続可能な PCIe デバイスプロトタイプ環境を提案した．本アーキテクチャを利用することで，実 PCIe デバイス無しに，ホスト PC と協調動作可能なソフトウェア PCIe デバイスが開発可能になり，データセンタなどでの利用を想定した PCIe を用いたシステムの試行錯誤の簡略化に貢献する．

本提案アーキテクチャは，PCIe 通信のデータがパケットデータであることに着目する．本手法は，PCIe パケットである TLP (Transaction Layer Packet) を Ethernet/IP/UDP ヘッダでカプセル化し，専用のアダプタ経由で PCIe リンクと Ethernet リンクをブリッジする．それにより，ホスト PC 上の PCIe パケットは専用アダプタで Ethernet フレームとして外部デバイスに送信され，また，外部ホストからの Ethernet フレームのペイロードから TLP を取り出し，その TLP をホスト PC の PCIe リンクに送信する．外部ホストでは，通常のネットワークプログラミングと同様の手順で，TLP をカプセル化した UDP パケットをユーザ空間で送受信する．本手法では，ユーザ空間で動作する TLP 処理ライブラリを開発し，それを用いて TLP を構築，受信を実施する．結果，ユーザ空間で PCIe デバイスの動作を，ネットワークプログラミングで実装，専用アダプタに対して Ethernet フレームを送受信し，実際の PCIe デバイスと同様の PCIe データ通信をソフトウェアで実現する．本提案手法を用いることで，今までハードウェア開発用言語 HDL (Hardware Description Language) などを利用して開発が必要だった PCIe 通信を Socket プログラミングで実装可能になった．

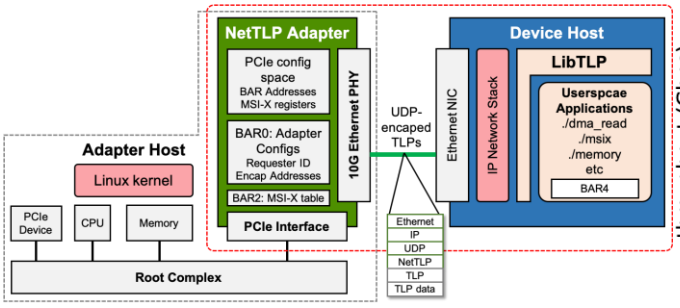

図 3 ソフトウェア PCIe プロトタイプ環境の概要

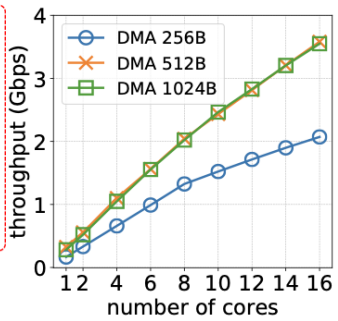

図 4 アダプタ実装の性能評価

本研究では，実際に専用アダプタを 10Gbps Ethernet を持つ FPGA 開発機を用いて実装，性能評価を実施した[図 4]．その結果，ユーザ空間で TLP を送受信し，最大 3.6 Gbps DMA read 性能ができることを確認した．また，今まで観測が困難であった PCIe 通信を tcpdump/wireshark などの既存のネットワークツールで可視化可能なことを確認，また，ユースケースとして存在しない NIC アダプタを実装し，実際の物理 Linux ホストの NIC として動作する NIC を 400 行の C 言語で実装可能なことを確認し，本提案手法のプロトタイプの有効性を確認した．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 空閑洋平，松谷健史，中村遼
２．発表標題 DDoS緩和のための全IPv4空間を対象としたACLアーキテクチャの検討
３．学会等名 電子情報通信学会 インターネットアーキテクチャ研究会
４．発表年 2018年

１．発表者名 空閑洋平，松谷健史，中村遼，関谷勇司
２．発表標題 物理マシンと協調動作可能なソフトウェアによるPCIeデバイスエミュレーション手法
３．学会等名 並列/分散/協調処理に関するサマー・ワークショップ
４．発表年 2019年

１．発表者名 Yohei Kuga, Ryo Nakamura, Tahekshi Matsuya, Yuji Sekiya
２．発表標題 NetTLP: A Development Platform for PCIe devices in Software Interacting with Hardware
３．学会等名 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)（国際学会）
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考