令和６年度研究開発成果概要書

採 択 番 号　22401
研究開発課題名　次世代コアと Beyond 5G/6G ネットワークのためのプログラム可能なネットワークの研究開発
副　　題　Beyond 5G ネットワークのセキュリティ、プライバシーを保護するプログラマブルデータプレーン技術

（１）研究開発の目的

本研究開発では、テラビット/秒のパケット転送をプログラム可能な P4 スイッチ、スマート Network Interface Card (NIC)を活用して、Beyond 5 時代のセキュリティおよびプライバシーを保護するフレームワークを開発する。具体的には、P4 スイッチとスマート NIC を組み合わせた User Plane Function (UPF)ノードのデータプレーン(UPF-U)に対して、セキュリティ・プライバシー保護技術を実装する。通信フローを監視し、書き換え処理を行う UPF-U ノードの実現に向けて、フレームワーク、セキュリティ保護、プライバシー保護の３つの課題を解決する。第一に、P4 スイッチのデータプレーンのメモリ容量、計算資源は、多数の通信フローのパケット列を監視、書き換えるには不十分であるため、P4 スイッチ、スマート NIC、ならびに制御 CPU のデータプレーンに監視、書き換え処理を最適配置することで、テラビット/秒の攻撃検出、軽減を可能とするフレームワークを開発する。第二に、Beyond 5G ネットワークにおけるセキュリティ保護技術(米国側)、プライバシー保護技術(日本側)を、フレームワークを活用して実現する。具体的には、フレームワークのプログラマビリティを活用して、テラビット/秒で動作する IP アドレス隠蔽とフロー変形技術をプログラムとして開発する。さらに、Domain Name System(DNS)プライバシー攻撃に対して、両技術を組み合わせた保護技術を開発することで実証する。第三に、最終的には、フレームワークとセキュリティ、プライバシー保護技術を統合した UPF-U ノードを開発し、5G ネットワークを模したテストベッドで実証実験を実施する。これにより本研究で開発したフレームワークにおける、最適配置、ならびにセキュリティ、プライバシー攻撃に対する耐性を実証する。

（２）研究開発期間

令和４年度から令和７年度（36 か月間）

（３）受託者

国立大学法人大阪大学 ＜代表研究者＞
兵庫県公立大学法人　兵庫県立大学

（４）研究開発予算（契約額）

令和４年度から令和７年度までの総額 45 百万円（令和６年度 15 百万円）
※百万円未満切り上げ

（５）研究開発項目と担当

研究開発項目１　フレームワーク技術
- 研究開発項目 1-1　最適配置技術（国立大学法人大阪大学）
- 研究開発項目 1-2　高速推論技術（国立大学法人大阪大学）

研究開発項目２　プライバシー保護技術
- 研究開発項目 2-1　IP アドレス隠蔽技術（国立大学法人大阪大学）
- 研究開発項目 2-2　フロー変形技術（国立大学法人大阪大学）
- 研究開発項目 2-3　DNS プライバシー保護技術（兵庫県公立大学法人）

研究開発項目３　統合技術
　研究開発項目 3-1　　テストベッド構築技術（国立大学法人大阪大学）
　研究開発項目 3-2　　セキュリティ評価技術（兵庫県公立大学法人）

（6）特許出願、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	0	0
	外国出願	0	0
外部発表等	研究論文	4	1
	その他研究発表	28	14
	標準化提案・採択	0	0
	プレスリリース・報道	2	2
	展示会	1	1
	受賞・表彰	4	2

（7）具体的な実施内容と成果
研究開発項目１：
研究開発項目 1-1
　10^6 フローをサポートする User Plane Function（UPF）の実現を目的として、P4 スイッチとコンピューターを連携したシステムを設計した。提案するシステムは、Tbps 級の通信速度と 10^6 フローのサポートを両立するために、フロー情報の保存とそのキャッシュの配置を最適化した。具体的には、フローの情報をコンピューター上に保持することで 10^6 フローの通信をサポートしつつ、その一部を高速なアクセスが可能な P4 スイッチ上に配置することで Tbps 級の通信速度を実現する。さらに、研究開発項目 2-2 で開発したヘッダとペイロードをスイッチ内で分離と結合する技術を応用して、スイッチとコンピューター間の処理を最適化した。さらに、設計した UPF を、P4 スイッチとホストの実機上への実装を開始した。

研究開発項目 1-2
　10^6 フローかつ Tbps 級のトラフィック中の攻撃を検出する高速モニタリング技術の実現を目的として、P4 スイッチ、スマート NIC、コンピューターを連携したシステムを設計した。Tbps 級のトラフィックを処理と高精度な攻撃検出を両立するために、大量のトラフィックを P4 スイッチで大量のフローをフィルタリングすることで、スマート NIC やコンピューターで処理可能な量までトラフィックを削減し、一方で、スマート NIC 上で高度な分類器を用いた推論、コンピューターにおいてパケット解析に基づく高度な攻撃検出を実施することで高精度な攻撃検出を実現した。Tofino スイッチ上にプロトタイプを実装し、1.2 Tbps・700 万フローのトラフィックに対する攻撃検出を実現した。

研究開発項目２：
研究開発項目 2-1
　軽量匿名通信プロトコルは、悪意のある送信者によるトラフィックを遮断できないことが課題であることを示し、これを解決するために、匿名通信上で悪意のあるトラフィックの送信元クライアントを特定し、その通信を遮断するプロトコルを設計した。

研究開発項目 2-2
　昨年度までに基礎設計が完了した P4QRS に対して、パケット順序が入れ替わる課題を解決するために高度化した。トラフィック変形などの高度な処理を P4 スイッチ上で実行する際に、P4 スイッチ上でパケットを多数回再循環させる課題がある。P4QRS は、スイッチ上で計算に供与する部分（ヘッダと呼ぶ）と供与しない部分（ペイロードと呼ぶ）に分割し、ヘッダのみを再循環することで、再循環時の負荷を軽減しスループットを向上させる。この分割したヘッダとペイロードを結合する際に、パケットの順序の一貫性を保つために追加で再循

環することで、パケットの順序入れ替えを防ぐ。拡張した P4QRS を Tofino、Tofino2 上に実装し、ChaCha20 の暗号化処理を例に、パケットの順序を保ちながら数 Tbps の処理を達成できることを示した。

研究開発項目 2-3

DNS クエリ匿名化に関して、Oblivious DNS over HTTPS をベースとした新たな匿名化プロトコル「μODoH」を、実環境での運用を想定した拡張設計・実装・テストベッドでのデプロイを実施した。具体的には、RFC9421（HTTP Message Signatures）を用い、クエリとクエリを含んだ HTTP Request の真正性を、高速に検証可能な手法を新たに考案し、その実装・テストベッドでのデプロイを行なった。実装は全てオープンソースソフトウェアにて一般公開済みである。また、当該テストベッドは阪大・兵庫県立大間にて、インターネットを介して実際に運用中である。

研究開発項目３：

研究開発項目 3-1

これまでに本研究開発項目で構築したローカルテストベッドを、NICT 総合テストベッドおよび国内外のネットワーク事業者や研究機関の協力により構成された広域テストベッドと接続した大陸間テストベッド上で、P4 スイッチ上に実装した軽量匿名通信プロトコルを実証した。また、実証用に数百万の匿名通信をエミュレートするトラフィックジェネレーターを P4 スイッチ上に実装した。実証実験では、第一に、アメリカと東京に設置した P4 スイッチ間で数百万のクライアントの匿名通信を想定した実験を実施し、約 580Gbps の匿名通信を達成した。第二に、アメリカから大阪大学に設置したプロキシノードを経由した 4K ビデオストリーミングを第一実験と同時に実施し、匿名通信で実アプリケーションが動作することを検証した。

研究開発項目 3-2

研究開発項目 2-1 で開発した、軽量匿名通信プロトコルにおいて通過する経路を検証するプロトコルを、ソフトウェア実装し、実装したコードに基づいて安全性を検証した。

（8）今後の研究開発計画

令和 7 年度は、これまでに開発技術を構築したローカルテストベッド上に展開し、実証する。具体的には、日米で開発した P4 スイッチ、スマート NIC、および、ホストを統合した高速モニタリング技術をローカルテストベッド上に展開し、テラビット/秒の速度かつ 10^6 以上のフローが到着する状況下で攻撃検出を実施できることを検証する。また、テストベッド上で展開した匿名 DNS リゾルバが実用可能な UX を担保できることを検証する。さらに、今年度に開発した軽量匿名通信プロトコルのセキュリティー上の課題を解決するプロトコルをソフトウェア実装し、その処理速度を計測するなどにより実現可能性を検証する。これらの実装したソフトウェアは、GitHub 上で公開する。

（9）外国の実施機関

カリフォルニア大学リバーサイド校（アメリカ）
ジョージワシントン大学（アメリカ）