令和５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 B5G/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、Beyond５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

（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５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	3	2
	その他研究発表	14	9
	標準化提案・採択	0	0
	プレスリリース・報道	0	0
	展示会	0	0
	受賞・表彰	2	1

（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 個の通信フローを監視し、攻撃を検出・軽減するフレームワークの実現を目的として、ホストや P4 スイッチの暗号処理をスマート NIC にオフロードする手法を、ストリーム暗号 ChaCha20-Poly1305 を対象として、設計した。スマート NIC として Netronome ISA-4000-40-2-2 上にプロトタイプを実装し、ホスト CPU の単一コアで処理する場合と同程度の性能を達成することを検証した。さらに、米国で検討中の属性ベース暗号を用いた応用との結合の検討を開始した。

研究開発項目 1-2

攻撃を検出する高速推論技術を P4スイッチ上で実現することを目的として、バイナリ決定木に基づく分類器を実現する手法を設計した。具体的には、パケット単位の解析でフローの大小を判別する分類器を、教師データを用いて訓練した決定木を知識蒸留によりバイナリ決定木にすることで実現した。Tofino スイッチ上にプロトタイプを実装するとともに、米国で開発中のトラフィック解析手法 SmartWatch との統合を開始した。

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ならびに TLS を用いたミドルボックスのセキュリティ上の課題を解決するプロトコルを設計した。軽量匿名通信プロトコルは、悪意のある送信者の不正トラフィックを防御出来ないことが課題であるため、匿名性と責任追跡性を両立するフレームワークを設計した。ミドルボックスプロトコルについては、2 台の悪意あるミドルボックスに対する攻撃に脆弱であるため、既存のプロトトコル maTLS を拡張して解決するプロトコル modified-maTLS を設計した。

研究開発項目 2-2

トラフィック変形における、P4 スイッチでパケットを多数回再循環させる課題を解決するため、パケットのペイロードは P4 スイッチのバッファに蓄積しておき、ヘッダのみを再循環させる手法 P^4QRS を設計した。再循環させたヘッダと蓄積したペイロードが P4 スイッチの出力で、再同期する確率を待ち行列を用いて解析するとともに、Tofino スイッチ上にプロトタイプを開発し、通信速度を向上させるとともに、高確率で再同期を成功させることを検証した。

研究開発項目 2-3

DNS クエリ匿名化に関して、Oblivious DNS over HTTPS を拡張した新たな匿名化プロトコルを仕様設計し、クライアントとリレー・ターゲットサーバを開発、一般公開を行い、遅延の観点からの性能評価を実施した。これにより、開発したプロトコルが UX の観点から十分なレスポンス速度を実現できることを確認した。これに加え、実運用を想定した運用機構の全体設計を行った。具体的には、DoS 攻撃の踏み台への対策や、相互に信頼できるリレーサーバ同士を相互接続するためのプロトコルの設計を実施した。このうちの一部について、リレー・ターゲットサーバソフトウェアへの、送信元・送信先のフィルタリング機能を追加実装し、一般公開した。

研究開発項目３：

研究開発項目 3-1

P4 スイッチを接続したローカルテストベッド上に軽量通信プロトコルに加えて、UPF ノードを展開することを目的として、UPF ノードのプロトタイプを Tofino スイッチ上に実装するともに、制御プレーンのパケット転送書き換え能力を評価した。具体的には、P4 モデル上で動作する UPF ソフトウェアを Tofino スイッチ上に委嘱するとともに、バッファリング機能ならびに QoS 機能を実装するともに、Tofino スイッチのクロックを用いて、TCAM ならびに SRAM でのパケット転送規則更新時間を計測した。計測結果と、既存研究における UE の移動回数から推定で 170 万 UE の移動をサポートできることを示した。さらに、研究項目２－３で開発した DNS クエリの匿名化手法を広域網で評価する準備として、大阪大学及び兵庫県立大学に匿名化リレーサーバ・ターゲットサーバの実験環境を展開・相互接続した。

研究開発項目 3-2

前年度に設計した P4 スイッチ上の軽量匿名通信プロトコルの脆弱性を解析し、2 つの匿名パスが交差するルータで、経路情報を書き換える経路接合攻撃に脆弱であることを明らかにした。さらに、隣接する 3 つのルータ間でメッセージ認証コードを用いて経路情報書き換えを防御する手法を設計し、安全性を検証した。

（8）今後の研究開発計画

令和６年度は、高速推論技術、IP アドレス隠蔽技術、フロー変形技術、ならびに DNS プライバシー保護技術のプロトタイプ実装を完了し、ローカルテストベッドで検証する。また、令和７年度の実証実験に向けて、国内で P4 スイッチを用いた広域テストベッドを構築し、軽量匿名通信プロトコルならびに DNS 匿名化プロトコルの実証を開始する。さらに、高速推論技術ならびに IP アドレス隠蔽技術については、スマート NIC の活用ならびに責任追跡性を追加する。さらに、米国側の共同研究機関と共同で、P4 スイッチ（日本側）とスマート NIC（米国側）でのアタック検出を統合する手法について共著で国際会議に投稿するとともに、暗号処理への応用を開発する。開発した P4 スイッチで動作するソフトウェアは、順次 GitHub に公開する。

（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）