令和5年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号：22401

１．研究課題・受託者・研究開発期間・研究開発予算

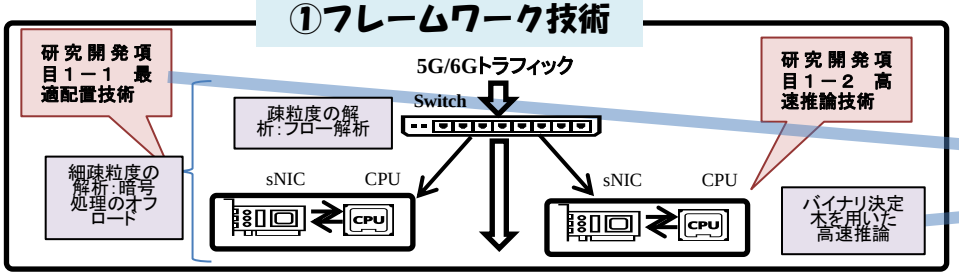
◆研究開発課題名　次世代コアとB5G/6Gネットワークのためのプログラム可能なネットワークの研究開発
◆副題　Beyond 5Gネットワークのセキュリティ、プライバシーを保護するプログラマブルデータプレーン技術
◆受託者　国立大学法人大阪大学、兵庫県公立大学法人
◆研究開発期間　令和4年度～令和7年度（36か月間）
◆研究開発予算（契約額）　令和4年度から令和7年度までの総額45百万円（令和5年度15百万円）

２．研究開発の目標

Beyond 5Gネットワークにおいて、テラビット/秒でセキュリティならびにプライバシー攻撃を検出、軽減するフレームワークを、P4スイッチ、スマートNICのプログラマブルデータプレーンを組み合わせて実現する。1）テラビット/秒で10^6個の通信フローを監視し、セキュリティならびにプライバシー攻撃を検出、軽減するUPF-Uノードのフレームワークを開発する。2）、10^5ユーザを想定して、ユーザがアクセスするサイト、データなどのプライバシー漏洩を防ぐプライバシー保護術を開発する。3）フレームワーク、プライバシー保護技術ならびにセキュリティ保護技術(米国)を統合したUPF-Uノードを開発し、5Gネットワークを模擬したテストベッド上実証する。

３．研究開発の成果

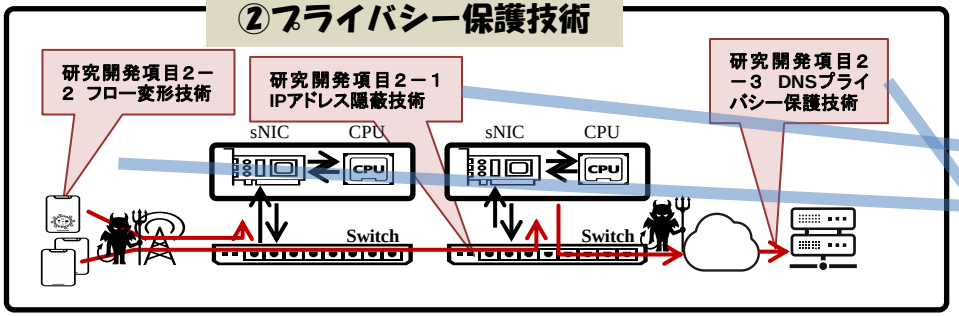
①フレームワーク技術



研究開発項目１：フレームワーク技術

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実装。
●高速暗号処理を提供するため、ストリーム暗号ChaCha20-Poly1305の暗号処理を、ホスト、P4スイッチからスマートNICにオフロードする方式を設計、実装した。
●P4スイッチ上でパケットの特徴を抽出し、バイナリ決定木を用いたトラフィック分類を高速に行う推論方式を確立した。

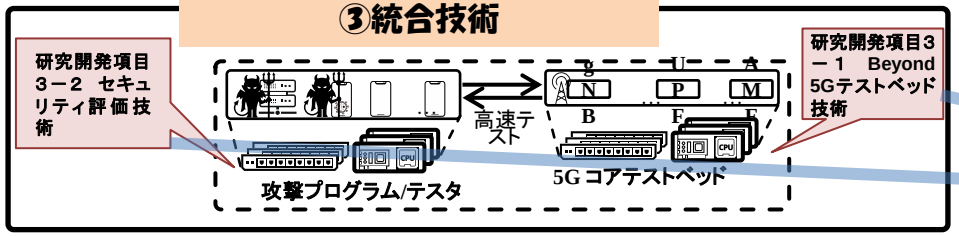
②プライバシー保護技術



研究開発項目２：プライバシー保護技術

10^5ユーザに対して、プライバシー保護と責任追跡性を提供する技術を開発。
●軽量匿名通信プロトコルに責任追跡性を付与するフレームワークを設計するとともに、ミドルボックスプロトコルに対して、ミドルボックスの結託攻撃への耐性を強化した。
● ペイロードをバッファに蓄積し、P4スイッチのパイプラインをヘッダだけを再循環させる手法P^4QRS設計し、パケット生成や暗号処理を高速化した。
●DNSクエリ匿名化プロトコルについて、クライアントとリレー・ターゲットサーバを開発、遅延の観点からの性能評価を実施、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。加えて、セキュアな実運用を想定した運用機構の全体設計を行った。

③統合技術



研究開発項目３　統合技術

全技術を組み合わせたUPFノードのプロタイプを実装し、制御プレーンの性能を検証。
●P4スイッチ上に実装したUPFノードに5Gに必須のQoS、バッファリング機能を実装するとともに、DNS匿名化プロトコルを広域に展開する準備を実施した。
●2つの匿名パスが交差するルータによるパス接合攻撃に軽量匿名プロトコルが脆弱であることを明らかにし、メッセージ認証コードを用いて防御する手法を設計した。

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	標準化提案・採択	プレスリリース 報道	展示会	受賞・表彰
0 (0)	0 (0)	3 (2)	14 (9)	0 (0)	0 (0)	0 (0)	2 (1)

※成果数は累計件数、( )内は当該年度の件数です。

（1）プライバシー保護技術に関する研究成果の認知度向上に向けた取り組み
プライバシー保護に関する研究成果について積極的に投稿し、国際ジャーナル（IEE Transactions on Network Service and Service Management, Elsevier Computer Networks）に2件採択されるとともに、CORE A*の国際会議（IEEE INFOCOM 2023）で発表した。また、国内学会で6件の発表をした。

（2）国内研究会での表彰
名前の難読化に関する発表が、受賞電子情報通信学会 ネットワークシステム研究会 若手研究奨励賞を受賞した。

（3）実証実験用のテストベッド構築
ローカルテストベッド上にUPFノードを展開してQoSならびにバッファリング機能を検証するとともに、DNS匿名化プロトコルの性能を広域網における実験で検証した。

（4）米国側研究機関との協調
P4スイッチとスマートNICを組み合わせたトラフィック監視法SmartWatchの基本設計を米国側研究機関と実施し、プロタイプを実装した。

5. 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。

6. 外国の実施機関

米国　カリフォルニア大学リバーサイド校、ジョージワシントン大学