

令和 7 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 7 年度 7 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	6	2
	その他研究発表	28	0
	標準化提案・採択	0	0
	プレスリリース・報道	2	0
	展示会	1	0
	受賞・表彰	4	0

(7) 具体的な実施内容と最終成果

研究開発項目 1 :

研究開発項目 1-1

フローの時間局所性に基づき、フローの状態をスイッチと計算機に配置するキャッシュ技術を設計し、5G UPF ノードのパケット分類ルール (PDR) とアクションルール (FAR, QER, URR) の管理へ応用した。P4 スイッチと計算機で構成する UPF ノードにおいて、 1.1 Tbps のスループット、 $1.4 \times 10^6 \text{ UE}$ 、 $1.4 \times 10^7 \text{ フロー}$ の収容を実現できることを示した。

研究開発項目 1-2

10^6 フロー から高精度に攻撃を検出する、P4 スイッチ、スマート NIC、計算機を連携した攻撃検出システムを実現した。スイッチで大量のフローをフィルタリング、スマート NIC 上で分類器を用いた推論、計算機でパケット解析に基づく高度な攻撃検出を実施し、高精度に攻撃を検出する。スイッチに実装し、 1.2 Tbps 、 $7 \times 10^6 \text{ フロー}$ 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

ルータが乗っ取られても関係匿名性を提供する軽量な匿名通信プロトコルを設計し、P4 スイッチ上に実装した。実装したプロトコルは、Tofino 2 スイッチ上で 3 Tbps のスループットを達成した。実装したコードをオープンソースとして、公開するとともに、2 件の国際論文 (IEEE Transactions, Computer Networks) と 1 件の国際会議 (INFOCOM 2023) に発表した。

研究開発項目 2-2

k -匿名性を活用して、 k 個の Web ページにアクセスして、パケットサイズ、間隔、総量を均等にするトラフィック変形法を設計し、P4 スイッチ上に実装した。さらに、変形などの負荷の高い処理に対して、P4 スイッチ上でヘッダだけを循環させることで高速化する P4QRS を設計、実装した。

研究開発項目 2-3

アドレス隠蔽とリレー・リゾルバの結託防止を実現する mixnet 型高速 DNS 匿名化手法を設計し、オープンソースソフトウェアとして実装・公開、およびテストベッドを構築し、その実用性を証明する論文を国際論文誌 (Computer Networks) にて発表した。また、新たな匿名化プロトコルと、DNS メッセージ圧縮・高速化技術を設計し、国際会議 (ISITA2024,

2 件) および論文誌(IEICE Trans., 1 件) にて発表した。

研究開発項目 3 :

研究開発項目 3-1

受託者間に設置したテストベッドに 2-2、2-3 で設計した技術を展開した。また、テストベッドと、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、2-1 で設計した匿名通信を実証し、日米間で 580 Gbps の匿名通信を実現した。

研究開発項目 3-2

研究開発項目 2 で開発した軽量匿名通信プロトコルの脆弱性を解析し、実際のネットワークで利用可能な安全性を有することを検証した。具体的には、プロトコルが関係匿名を提供することを理論的に証明し、匿名性の強度を匿名集合を構成する AS 数で評価した。さらに、経路検証機能を追加することで、匿名通信パスの安全性を向上した。

(8) 研究開発成果の展開・普及等に向けた計画・展望

1. 開発した UPF のオープンソース 5G コアネットワークソフトウェアや NICT B5G テストベッドとの接続による実証により、実用性を検証する。
2. 米国研究機関と継続的に研究開発を実施し、学会で発表することで、学術的な貢献を図る。
3. プライバシー保護技術の普及にむけ、OS やソフトウェアなどユーザーソフトウェアの拡充と、それらの GitHub 上でのオープンソース化により、技術普及に取り組む。

(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)