様式 1-4-2 (2022-1)

令和４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、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

（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４年度９百万円）
※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	1	1
	その他研究発表	4	4
	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	1	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 UPF-U ノードのフレームワークの基盤技術として、暗号化機能とともに認証機能を設計し、プログラマブルスイッチ ASIC のパイプライン上に最適配置することで、経路の秘匿性のみならず完全性を保証する匿名通信をプログラマブルスイッチ上に実装した。実験によりテラビット/秒の通信を達成した。

研究開発項目 1-2
　攻撃を検出する高速推論技術の開発の第一段階として、Web トラフィックを収集・解析する Web フィンガープリンティング攻撃を対象とし、情報量的な解析手法を用いて攻撃に有用な特徴量を明らかにした。さらに、解析結果に基づいて Web フィンガープリンティング攻撃を実行したときの攻撃実現精度を実験的に検証した。

研究開発項目２：
研究開発項目 2-1
　ネットワーク層で動作する軽量な匿名通信プロトコルをベースに、従来よりも強い脅威、つまり、ルーターの乗っ取りを想定し、その脅威に対しても関係匿名性を保証することができる攻撃耐性の高い匿名通信プロトコルを設計した。

研究開発項目 2-2
　k-匿名性を活用して、k 個の Web ページへのアクセスに対して、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、シミュレーションにより有効性を検証した。

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、クライアントとサーバ、加えて DoS 対策用のための認証サーバ・リバースプロキシを OSS 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を構築し、研究開発項目 2 で開発した匿名通信プロトコルを展開した。SOCKS プロキシーを介して Web 通信を匿名通信プロトコルにカプセル化し、通信を匿名化しながら YouTube の動画視聴などが可能であることを実証した。

研究開発項目 3-2

匿名通信プロトコルが関係匿名性を提供することを理論的に証明するとともに、匿名性の強度を匿名集合を構成する AS (Autonomous System)数で評価した。

（8）今後の研究開発計画

令和５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設計を完了し、P4 スイッチでのプロトタイプ実装、シミュレーション評価を実施する。また、令和６年度以降の実証実験に向けて、5G テストベッドの構築の第一ステップとして、P4 スイッチに UPF-U ノードの基本部分を実装するとともに、オープンソースの 5G ソフトウェアとの統合を開始する。さらに、米国側の共同研究機関と共同で、P4 スイッチでの匿名通信(日本側)と Smart NIC でのアタック検出を統合する手法を設計し、設計結果を共著で国際会議に投稿する。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）＜代表研究者＞
ジョージワシントン大学（アメリカ）