審 査 の 結 果 の 要 旨

氏　　名　モハマド　サミル　アビデラヒマン　エイド

本論文は End-to-End Encryption Enabled Overlay-based Mitigation of HTTP and HTTPS DDoS Attacks: Design and Proof of Concept Implementation（エンド・ツー・エンド暗号化に対応したオーバーレイに基づく HTTP および HTTPS DDoS 攻撃緩和手法：設計と概念実証実装）と題し、エンド・ツー・エンドで暗号化された通信を扱うことができ、かつ、同一 IP アドレスを有する複数のクライアントが存在する場合に、クライアントごとの挙動を監視して識別することのできる DDoS 攻撃緩和手法について論じたものであり、英文で書かれ、6 章で構成されている。

第 1 章 Introduction（序論）では、インターネットが情報社会の基盤となっている一方でサイバー攻撃も急速に増えており、その中でもインターネットを流れるトラフィックの 80%を占める HTTP(S)プロトコルを用いた DDoS（Distributed Denial of Service: 分散サービス妨害）攻撃が最大の脅威であること、また、中小規模の企業にとって DDoS 攻撃緩和策を自前で用意するのは困難なので、インターネットプロバイダなどが遠隔緩和策を提供しているが、現在提供されている暗号化された HTTPS プロトコルを用いた DDoS に対する遠隔緩和策は、提供側で暗号を一旦復号して再暗号化するものであり、金融サービス業者の 76%は暗号鍵の外部提供に懸念を示していることを挙げて、本論文の研究目標を示している。

第 2 章 Related Works on Overlay-based HTTP-DDoS Mitigation（オーバレイに基づく HTTP DDoS 緩和手法に関する関連研究）では、本論文の研究内容に関連した近年の研究事例について、利用者のエンド・ツー・エンド通信におけるプライバシー保護と Web サーバ保護の両面から優劣比較をしている。

第 3 章 Proposed Method and Prototype Implementation（提案手法ならびにプロトタイプ実装）では、DDoS 攻撃に対処するための具体的な手法を提案するとともに、そのプロトタイプ実装について述べている。まず、同一 IP アドレスを有する複数のクライアントが存在する場合に対処するために、クライアントからのリクエストは、公開サーバが受け付けて IP アドレスごとの reputation

（評判）を確認した後、一定時間のみアクセス可能なアクセスノードのポート番号を割り当てられてリダイレクトされ、アクセスノード経由で真のサーバと通信する。この間、クライアントの IP アドレス、クライアントとサーバの IP アドレス対、アクセスノードに割り当てられたポート番号、TCP コネクションの 4 つのレベルで毎秒あたりのリクエスト数といった指標が閾値を超えたか否かの「例外」の履歴を記録することで、クライアントの評判を形成する。そして、評判の悪いクライアントに対しては、リクエストを受け取った後、真のサーバにリクエストを転送する前にダミーの応答を少しずつ送ることで、リクエスト送信後直ちにコネクションをクローズするクライアントに対処するとともに、評判の良いクライアントと評判の悪いクライアントの間でサービスの差別化を行っている。

第 4 章 Evaluation（評価）では、DeterLab と呼ばれるテストベッド上に提案システムのプロトタイプを実装し、よく用いられる攻撃ツールで用いられている攻撃法や、原理的に検出が最も困難と考えられる攻撃法など、7 種類の異なる DDoS 攻撃シナリオにおける提案システムの動作を検証している。検証の結果、パラメータの最適化をそれほど行っていないにもかかわらず、ほとんどのシナリオにおいて、提案システムは 3 分以内に DDoS 攻撃を検出して対処することができ、攻撃を行っているクライアント以外に対するサービス率は 95%以上を維持することができた。

第 5 章 Discussion（議論）では、提案システムのサービス時間の増加およびスケーラビリティについて考察を行った後、従来の手法との比較を行い、提案手法は、エンド・ツー・エンドの暗号化に対応し、同一 IP アドレスを有する複数のクライアントが存在する場合にもそれらのクライアントの挙動を識別することができる一方で運用コストやスケーラビリティの点でも優れており、従来サーバで取られていた対策と遠隔で取られていた対策の利点を併せ持っていることを述べている。また、第 4 章で行った評価の信頼性や他の攻撃シナリオに対する耐性、本格的実装に向けての考慮点などについても論じている。

第 6 章 Conclusion（結論）では、本論文で得られた成果をまとめている。

以上のように本論文は近年深刻な問題となっている DDoS 攻撃に対する緩和手法として、エンド・ツー・エンドの暗号化に対応し、同一 IP アドレスを有する複数のクライアントが存在する場合にもそれらのクライアントの挙動を識別することができる方式を提案し、そのプロトタイプをテストベッド上に実装して、各種の攻撃シナリオに対して、緩和率や緩和に要する時間などの性能が、復号–再暗号化を行う従来方式と遜色がないことを実証したものであって、電子情報工学に貢献するところが少なくない。

よって本論文は博士（工学）の学位請求論文として合格と認められる。