審 査 の 結 果 の 要 旨

氏　　名　　CHEN ERIC YI-HUA

分散サービス停止（DDoS: Distributed Denial of Service）は、インターネットでのセキュリティ脅威として注目されている。DDoS攻撃とは、不正なプログラムを多数の端末に侵入させ、それらのプログラムが同時に標的ホストへ大量のパケットを送信し、サービスを停止させる攻撃である。現在知られているDDoS攻撃手法を大別すると、「ホスト資源消費型」と「ネットワーク帯域消費型」の二つのタイプに分けられる。このうち前者の場合は、侵入検知システムと連動したファイアウォールを標的サイトに設置する“点”での防御により、ある程度の効果が得られる。しかし、後者の場合、サーバを守るだけではネットワークが輻輳し、サービス停止を防ぐことができない。従来のサーバが設置されたサイトだけでの防御システム、つまり、“点”での防御だけでは、攻撃を防ぐことも、攻撃中に正規ユーザにサービスを継続することも困難である。

CHEN氏は、DDoS攻撃の検出および対策を行う防御システムMoving FireWallの概念を提唱し、実装および評価した。CHEN氏は、まず、検出手法を検討するために既知の攻撃手段を詳細かつ網羅的に調査し、攻撃の特徴をまとめた。そして、時列系分析により正常トラヒック量の時間遷移をモデル化し、トラヒックの異常検出を可能とした。異常性の高いトラヒックを発見した場合、詳細な特徴分析を行う。特徴分析に関して３つの提案を行った。一つは、既存手法であるMULTOPSを改良したACKパケットに関する回帰分析手法である。２つめは、クライアントホストからの返答パターンを解析する手法であり、３つめは既知のDDoS攻撃パターンを元にしたパターンマッチング手法である。

CHEN氏は、DDoS攻撃を検知すると、攻撃端末に近い上流ノードに対して攻撃トラヒックを通知し、そのトラヒックを止めさせる手法を提案した。Firewallが動的に形成されていくように見えることから、CHEN氏は、本システムをMoving Firewallと命名した。これにより、ネットワークに流れる攻撃パケットの帯域をネットワーク全体の“面”で制限することにより攻撃被害を局所化し、サービスの停止もしくは低下というDDoS攻撃の被害を最小化することを可能とした。正規ユーザは、DDoS攻撃が発生しているときでも、攻撃の影響を受けずにネットワークを利用することが可能となる。

本防御システムは専用装置および汎用ソフトウェアの二つの形で実装された。前者は、ネットワーク・プロセシング・ユニット（NPU）を用いてワイヤースピードを実現した。後者は、標準Linux上で動作する。また、実機テストベッドおよび仮想シミュレーションにより本防御システムの効果を検証した。最後に、本防御システムの汎用性を向上させるため、複数サービスプロバイダを連携させ、異なった自律ネットワーク間の導入法も提案した。

以上のように、本研究は、ネットワーク脅威の中のDDoS攻撃に対して、科学的に攻撃パターンを解析し、また新たなる攻撃を検知する手法を提案している。さらに、攻撃による被害を最小限に抑えるための枠組みも提案している。これらの提案は、Moving FireWallという概念としてまとめあげ、インターネットワークにおける顕著な研究成果をあげている。よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。