（別紙２）

論文審査の結果の要旨

論文提出者氏名　コー・スーン・ヒン

本論文は，「実世界に展開可能な DDoS 攻撃防御メカニズム（Deployable Mechanisms for Distributed Denial-of-Service (DDoS) Attack Mitigation）」と題し，現在のインターネット上で大きな社会的問題となっていながら，防御方法が未だに確立されていない DDoS 攻撃に対する，容易に実装可能な防御メカニズムを提案するものである．DDoS 攻撃とは，インターネット上に散在する複数の攻撃者，多くの場合は多数のボット(Bots)（ある攻撃者が何らかの方法で侵入し自由に操ることが可能な多数のコンピュータ）から，サーバやその手前に存在するルータ・スイッチなどに故意に一斉にパケットを集中的に送ることで，他のユーザからのアクセスを遮断してしまう攻撃の一つである．近年，クラウドプロバイダ（クラウドコンピューティングのインフラを提供する業者）から，動画配信などネットワークサービスを運用するための資源の使用権を購入し，サービス提供を行うビジネスモデルが一般的となりつつある．しかし，一方で，ネットワークアクセスに応じた従量制の課金モデルでは，DDoS 攻撃により課金が膨大になる eDDoS(Economic DDoS)攻撃の発生が予測されている．

本論文では，ネットワーク層の DDoS 攻撃，通常トラフィックに見せかけてあるためフィルタできない DDoS 攻撃，および，eDDoS 攻撃など，現在頻発している，或いは，近未来に重大な社会問題と成り得る DDoS 攻撃に対し，実際にインターネット上に容易に構築できる可能性を主眼に置く 5 つの防御手法(Burrows, Overfort, AI-RON-E, Kumo, SPoW)を提案している．これらの 5 つの手法は，以下に示すように，本論文の第 3 章から第 7 章に相当する．

第 3 章では，Burrows の手法が提案されている．従来提案されてきた DDoS 攻撃の防御は，攻撃とは無関係な他者に依存する解法であったり，多くのコンピュータ資源を必要としたり，また，送信先へ至る複数のルータを改変しパケット認証が必要であるなど，実装・展開の際の敷居が高い方法が多く見られる．それに対し，Burrows では，データ通信において送信先へのトラフィックが必ず複数の中継地点を通過することを義務付けることを基本アーキテクチャとして定義する．このため，防御は中継地点でのみ実装すれば良く，攻撃とは無関係な他者に依存せず，少ない資源で実現可能，また，ルータ・スイッチなどのインフラ変更が不必要であるなど，実装・展開の敷居を低くすることが可能となる．

第 4 章では，Burrows の基本アーキテクチャに基づき，Overfort と呼ばれる DDoS 攻撃者の追跡（トレースバック）が提案されている．従来の DDoS 攻撃のトレースバックでは，送信元のアドレスを偽る（Source Address Spoofing）の問題，および，トレースバックしたあとに攻撃者にペナルティを与える仕組みが欠如していた．Overfort では，送信先にデータを通信するためには DNS(Domain Name System)によりホスト名から IP アドレスを解決するサービスを経なくてはならない事実に着目し，攻撃者がいるネットワーク領域（同じ DNS サーバを利用しているユーザ群）を検出し，自動的にペナルティを与えるメカニズムを提案して

いる．Overfort は Burrows に基づき，ユーザは必ず OFG(Overfort Gateway)と呼ばれる中継地点を介してのみ送信先のサーバと通信が可能になっており，攻撃者が存在するネットワーク領域からのアクセスは対応する OFG により通信制限を受ける．シミュレーションによると，インターネット全体 1 割の PC がサーバを攻撃すると仮定した場合，必要な OFG は 12,000 台程度に抑えられるため，Overfort の提案手法は少ない資源で実装が可能である．

第 5 章では，Burrows に基づき，DDoS 攻撃によって生じるネットワークの輻輳（混雑状態）をユーザ自らが回避する AI-RON-E と呼ばれる手法が提案されている．AI-RON-E ではインターネットのルータ・スイッチや経路制御などのインフラを変更することなく，ユーザ自らが，あるルータ(OSR)を中継地点として経由して送信先にデータ通信を行う．実際に，世界中に散在した 100 台の送信元 PC から 25 台の送信先 PC に対し，途中の経路が DDoS 攻撃により輻輳したと仮定した場合，69%の確率で輻輳を回避可能であることが示されている．AI-RON-E の手法はインターネットのインフラの変更を必要としないため実装が容易である．

第 6 章では，Burrows に基づき，インターネット上に存在する中継地点に成り得るあらゆるネットワークサービス（掲示板，IRC，Web サービスなど）を利用して，輻輳状態やリンク障害を回避する，KUMO と呼ばれるミドルウェアが提案されている．KUMO は，クライアント，サーバ，そして，中継地点となるネットワークサービスのソフトウェアには手を加えず，中継するための送信，受信，再送信，パケット分割・再構築などの基本的なネットワークスタックをミドルウェアとして提供する．KUMO のプロトタイプ実装を用いることで，実際に世界中に散在する PC 間で，Flickr, Amazon S3, Forum, IRC, i3 などを用いて通信が可能となることが示されている．

第 7 章では，KUMO を発展させ，中継地点のネットワークサービスをクラウドに実装する sPow というメカニズムが提案されている．sPoW では，中継地点をクラウド上に非常に多数用意した上で，どの中継地点を通過すれば目的のサーバに到達できるかという情報をパズルにより暗号化し，クライアントに解読するための計算資源を課す．クラウドで中継地点を実装する方式では，前述のように eDDoS 攻撃を受ける可能性があるが，クライアントが自らの計算資源で中継地点を検出すること，および，多数の中継地点のうち到達可能な中継地点が秘匿されていることにより，eDDoS 攻撃を最小限にとどめることが可能となる．sPoW のプロトタイプによると，アタッカーがクライアントの 3 倍存在する DDoS 攻撃の状況下でも接続時間は遅延するものの，クライアントはサーバに接続可能であることが示されている．

本論文は，実装可能性の観点から，インターネット上で大きな社会問題となっている多種多様な DDoS/eDDoS 攻撃の防御として中継地点経由のアクセスを基本概念とする 5 つの防御メカニズムを提案し，その有用性をシミュレーションとプロトタイプ実装により評価したものである．また，特に，防御が困難とされる通常トラフィックを用いたフィルタ不可の DDoS 攻撃や eDDoS 攻撃に対し，これら 5 つを組合せた防御手法を考案し評価したことは，DDoS/eDDoS 攻撃防御の研究分野の発展に大きく寄与するものである．よって，本審査委員会は，本論文が博士（学際情報学）の学位に相当するものと判断する．