M-048

ネットワークDDoS攻撃に耐性を持つP2Pネットワーク
P2P Network Protection against Network DDoS Attacks

川崎 陽平† 松本 倫子‡ 吉田 紀彦‡
Yohei Kawasaki Noriko Matsumoto Norihiko Yoshida

1. まえがき

DoS（Denial of Service）/DDoS（Distributed DoS）攻撃による被害は，大手webサイトの閲覧を一時的に不能にする等，近年では深刻な問題となっている．DoS攻撃とは，特定のサーバや通信機器に対して計算機資源を急激に消費させるような負荷をかけ，サービスの提供を不可能にする攻撃である．特に，ネットワーク中の多数のホストにより分散して実行されるDoS攻撃をDDoS攻撃と呼ぶ．一般にDDoS攻撃は，トロイの木馬やワームに感染した多数のホストをユーザの意図しないままに利用するため，DoS攻撃と比較して攻撃規模が大きくなりやすく，現在ではDDoS攻撃が主流となっている．DoS/DDoS攻撃に対しては，標的とされるホストにおける対策が既に多数提案されており，一例として，サーバにおけるアクセスパターン変化の分析による攻撃検出法[1]が挙げられる．

DDoS攻撃は従来，特定の目標を狙った局所的な攻撃であったが，昨今，ネットワーク全体を標的とした新しいタイプのDDoS攻撃（ネットワークDDoS攻撃）の可能性が懸念され始めている．その背景は，ファイル交換P2Pネットワークにおける情報漏洩事件の多さに裏づけされた，ウィルス・ワームに感染しやすい環境である．このような環境と過大なトラフィックを生むファイル交換P2Pネットワークをベースに，ネットワークDDoS攻撃は，ファイルのやり取りを一斉に行わせることでP2Pネットワークのパフォーマンスを低下させるだけでなく，P2Pネットワークが実装されているIPネットワークのパフォーマンスの低下も招く．

ネットワークDDoS攻撃はネットワーク全体を標的とするため，標的サーバ・通信機器を中心に考える従来の対策を適用することは難しい．本研究では，構築の容易さと耐障害性を備えた分散・非構造型P2Pを対象に，ネットワークDDoS攻撃時にトラフィックピークを抑制できるよう，P2Pネットワーク全体の対応により攻撃耐性を持たせる方式を検討する[2]．

2. ネットワークDDoS攻撃

ネットワークDDoS攻撃の攻撃手段を明確にし，その特徴について述べる．

ネットワークDDoS攻撃の実行のための前提として，トロイの木馬やワームに感染したノードが十分存在するものとする．攻撃は，例えばある日時になるといった特定の事象を契機に，P2Pシステム中の各ノードに無作為なファイルの取得を繰り返し行わせることで，トラフィックを急増させるというシンプルな方法である．ノードのストレージがいっぱいになった場合には，取得ファイルからランダムに選択して削除することでファイルの取得を継続する．

ネットワークDDoS攻撃によるファイルの検索・取得の動作は，P2Pシステムのプロトコルに従うため，パケットや通信パターンによる攻撃の判別は難しい．また，従来のDDoS攻撃のように攻撃の集中する点が無いので，通信に関するデータの統計をとるなどして攻撃を検出することも困難と考えられる．

3. 通貨の仕組みの導入

2.で述べたように，ネットワークDDoS攻撃の判別・検出は困難である．そこで，本研究ではネットワークDDoS攻撃への対策として，P2Pネットワーク中のファイル流量を調整することでP2Pネットワークに攻撃耐性を持たせる方法を検討する．

スパムメールの抑制を目的としたSpam-I-am[3]では，アカウントごとのメール送信量をクォータによって制限している．具体的には，メールの送信に電子切手を使用するものとし，各アカウントによるメール送信数の上限は，信頼のある機関から取得した切手の枚数に依存する．この仕組みなどを参考に，本研究ではファイル流量の調整を実現する手段として，P2Pシステムに通貨の仕組みを導入する．つまり，ファイルのやり取りに貨幣を媒介させ，全体の通貨量がある一定量を超えないように調整することでトラフィックを制限する．ただし，帯域制限のような固定的な調整ではなく，攻撃時に効果的にトラフィックを抑制できる柔軟な方式を目標とする．

貨幣の機能

本研究における貨幣は，あるノードからファイルを取得する際に対価として支払う交換手段として機能する．貨幣の価値は情報量として表し，ファイルを取得するノードはそのファイルサイズに応じた貨幣の支払いを行う．また，集中構造を持たないP2Pシステムにおいて個々のノードの動作だけで全体の通貨量を調整できるよう，貨幣には，時間経過に伴なって価値が減少する減価機能も持たせる．

4. 設計

P2Pシステムにおいて通貨の仕組みを実現するための設計を述べる．はじめに，本研究の要点となる通貨量を調整する仕組みを述べ，次に，ファイルを取得する際の具体的なフローを，貨幣の偽造を防止するための仕組みを交えて述べる．本設計は，一般的なP2Pシステムの検索・取得技術との併用を想定している．

4.1 通貨量の調整

通貨量は，P2Pネットワーク中の貨幣の流通数と貨幣価値の2要素から成る．新規貨幣は隣接ノードに発行要求することで取得し，要求を受けたノードは各隣接ノードごとに発行数の調整を行う．隣接ノードから新規貨幣

†NTT DoCoMo
‡埼玉大学 Saitama University

を取得する仕組みをベースに，通貨量を安定させるため，各ノードには次に述べる 3 つの共通の設定値を設ける．

> **発行 ID**：発行元ノードで唯一となる貨幣の識別子
> **発行元**：貨幣発行ノードの ID（or IP Address）
> **発行先**：発行先ノード ID（or IP Address）
> **貨幣初期価値**：取得できるファイルの最大サイズ
> **発行時間**：発行元を基準とした通貨発行時間

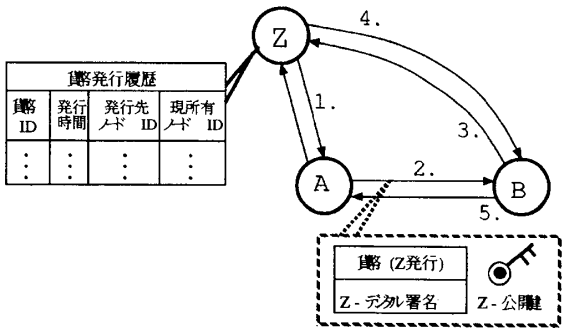

図 1: ファイル取得フロー

- **貨幣発行間隔** ··· 隣接ノードに貨幣を発行後，次に同隣接ノードからの発行要求を受け付けるまでに空ける時間．
- **貨幣消滅時間** ··· 減価により貨幣価値が 0 になるまでの時間．貨幣価値は，貨幣の発行時点からこの時間が経過すると 0 になるよう，一定の割合で減少する．
- **貨幣初期価値** ··· 貨幣の発行時点で取得可能なファイルのサイズ．メガバイト単位等で表現する．

ノードのリンク数が急激に変化しないという前提の下，各隣接ノードへの貨幣発行間隔および貨幣消滅時間の調整により，通貨量を調整することができる．

4.2 ファイル取得フロー

ノード A の行った検索がノード B でヒットしたとして，新規貨幣を使用してファイルを取得するまでのフローを述べる．1. から 5. のフローの対応図を図 1 に示す．デジタル署名を用いた貨幣偽造防止の仕組みは，電子バーター通貨システムを実現している i-WAT [4] を参考にした．貨幣は以下のような情報を保持する．

1. ノード A はノード Z へ貨幣発行を要求．Z は発行履歴を参照し，A への前回の発行から発行間隔時間が経過していれば貨幣を発行．併せて，Z による貨幣のデジタル署名，Z の公開鍵を A に送信．
2. A は取得した貨幣・Z の公開鍵・デジタル署名をノード B に送信．
3. ノード B は署名検証により改ざんの有無を確認．検証後，貨幣の発行元（Z）へ貨幣 ID をキーに発行履歴を問合せ．同時に Z の公開鍵も送信．

表 1: シミュレータのパラメータ設定

ノード数	3000 台
貨幣発行サイクル	450
攻撃開始サイクル	900
攻撃終了サイクル	1900
平均隣接ノード数（平均リンク数）	4.0
平均ファイルサイズ	176.5MB
ライト・ヘビーユーザ割合	0.04, 0.06, 0.09, 0.13, 0.19, 0.22, 0.36
正常フェーズ時検索基準サイクル	20, 40, 60, 85, 115, 150, 190

4. Z は発行履歴・公開鍵を確認後，Z の現在時刻を返答．
5. B は貨幣発行時刻と Z の現在時刻から減価計算し，得られたサイズの値を上限に A から要求されたファイルを提供．

手順 1. において発行履歴を参照した結果，ノード A へ規定枚数の貨幣を発行していることが分かれば，貨幣は発行しない．発行履歴の履歴情報は発行間隔時間が経過したものから順次削除される．

手順 4. においてノード Z の現在時刻を返答するのは，ノード B とノード Z の時計が一致していない場合を考慮しているためである．減価計算は貨幣発行時点からの経過時間に基づいて行うので，貨幣の発行元ノードが現在時刻を返答することで，発行元を基準とした減価計算ができる．

5. 実験と考察

提案方式の評価のため，作成したシミュレーションによりシミュレーションを行った．シミュレーションでは，正常フェーズとネットワーク DDoS 攻撃が行われる攻撃フェースを設け，各フェースにおける提案方式の効果と弊害を確認した．本シミュレーションでは，単位時間を 1 サイクルとし，1 サイクルごとに全ノードに検索やファイルのやり取り等の動作機会を与え，何もしないという選択肢も含めて確率的にノードを動作させた．

シミュレーションの各パラメータを表 1 に示す．P2P ネットワークのトポロジは各ノードがおよそ 2 から 6 のリンクを持つトポロジとした．シミュレーションは全 2500 サイクル実行し，結果は 30 サイクル毎にグラフにプロットした．

図 2 にトラフィック推移を示す．攻撃フェーズに移行した 900 サイクル以降，攻撃に未対策（Normal）の場合のトラフィックが突出した．提案方式（Proposal）は，貨幣初期価値を 100，200，300MB の 3 パターンでシミュレートした．攻撃フェーズで際立つ波形の周期は，貨幣発行サイクルに一致する．トラフィックは初期価値が低いほどそのピークを抑制できた．しかし，提案方式にはトラフィックを抑制できる利点だけではなく，正常フェーズにおいてもトラフィックを削ってしまう，すなわち，P2P システム本来のパフォーマンスを落としてしまうという欠点がある．

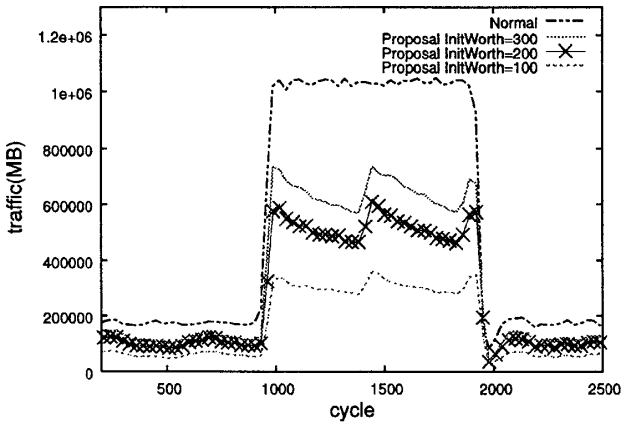

図 2: トラフィック推移

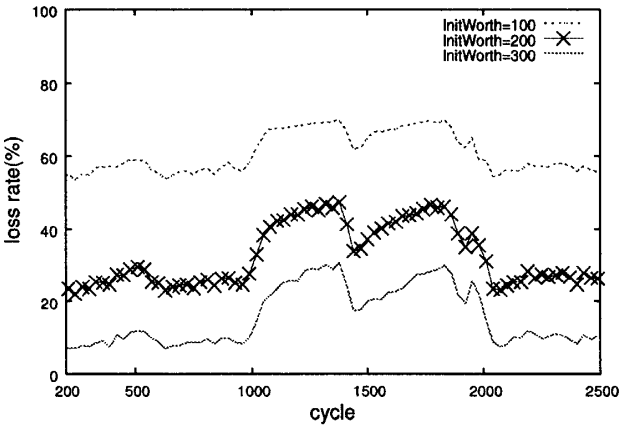

図 3: ファイル取得サイズ損失率

パフォーマンス低下の程度を確認するため，ファイル取得サイズ損失率を測定した．ファイル取得サイズ損失率とは，支払うことの出来た貨幣価値が取得しようとするファイルサイズより小さいために，取得できなかったファイルサイズの本来のファイルサイズに占める割合である．なお，ファイルの損失分は，ノードが後に貨幣を用意でき次第つづけて取得（レジューム）可能である．図 3 に推移を示す．貨幣初期価値が小さいほど損失率は大きくなる傾向があるが，そのうち初期価値が 100MB の場合には，正常フェーズでも損失が 5 割を超えており取得効率が悪い．図 2 と併せて見ると，貨幣初期価値に応じたトラフィックの抑制効果とファイル取得サイズ損失率は，それぞれの望ましい結果に対してお互いが相反する結果を示している．

図 4 は，検索頻度で分けたライトユーザ，ヘビーユーザ別のファイル取得サイズ損失率を示す．表 1 の下 2 項目はライト・ヘビーユーザの設定であり，左側の値ほど P2P ネットワーク中でファイルをやり取りする頻度の高いヘビーユーザの値となる．全 3000 台のノードは表 1 に示す割合に従ってライトからヘビーまでの段階に分け，対応する検索基準サイクルに基づき，それにランダムな幅を持たせて検索動作を実行させた．図 4 の結果は，7 段階の内訳のうち，右側 2 つの計 58%をライトユーザ，左側 2 つの計 10%をヘビーユーザとして測定した．ヘビーユーザは正常フェーズでもピークで約 50%の損失が見られるが，ライトユーザは正常フェーズで終始約 20%程度の損失で済んでいる．このことは，言い換えれば，提案方式に起因するパフォーマンス低下の影響を強く受けたのは一部のヘビーユーザのみであり，大半のライトユーザはそれほど影響を受けなかったことを示唆している．

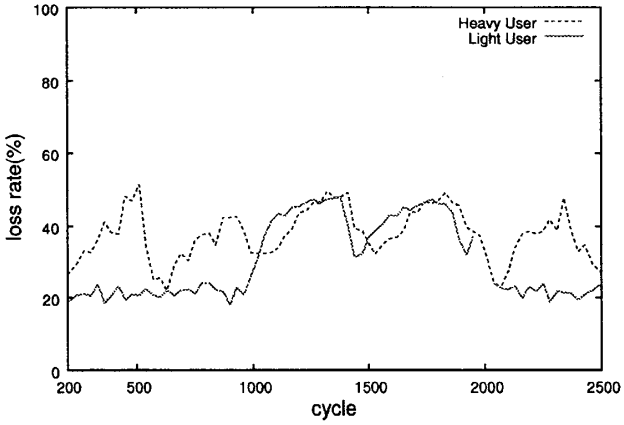

図 4: ファイル取得サイズ損失率：ライト・ヘビーユーザの比較

6. まとめと今後の課題

本研究ではネットワーク DDoS 攻撃への対処策として，P2P システムに通貨の仕組みを導入し，通貨量の調整を通じてトラフィックピークを抑制する方式を提案した．本方式の最大の要点は，貨幣をファイル取得のための媒介として使用し，P2P システム全体の通貨量の調整をもって，P2P ネットワークのトラフィックの調整を実現した点である．

シミュレーションにより，提案方式によるトラフィックピークの抑制に一定の効果を確認できた．貨幣の初期価値が小さいほど抑制効果は大きいが，一方で初期価値の低さが P2P システムのパフォーマンスを低下させるという因果関係も見られた．シミュレーション結果を統括すると，P2P システムで扱われるファイルの平均サイズに応じた貨幣初期価値の設定が，トラフィックピークの抑制とパフォーマンス維持に最適であると考えられる．しかしながら，ファイルの平均サイズは求めるのが容易でないため，直接それに頼ることのない，貨幣初期価値等のパラメータの決定法を検討することが今後の課題の一つである．

本研究では，貨幣の偽造・改ざん防止も重要な要素となるが，現状の対策ではすべての悪意に有効であると断言できない．そのため，本方式に対する攻撃法およびその対処策の検討も今後の課題となる．

参考文献

[1] Yuichi Ohsita, Shingo Ata and Masayuki Murata, “Detecting distributed Denial-of-Service attacks by analyzing TCP SYN packets statistically”, Proc. IEEE Globecom 2004.
[2] 川崎, ネットワーク DDoS 攻撃に耐性を持つ P2P ネットワーク, 埼玉大学修士論文, 2007.
[3] Hari Balakrishnan and David Karger, “Spam-I-am: A Proposal for Spam Control using Distributed Quota Management”, Proc. 3rd ACM SIGCOMM Workshop on Hot Topics in Networks, 2004.
[4] “i-WAT”, http://www.media-art-online.org/iwat/