Vol.2010-CSEC-50 No.38
2010/7/2

初期パケットの乱数性に着目した P2P 通信検知方式

重本倫宏† 仲小路博史† 寺田真敏†

Winny，Share 等の P2P ファイル交換ソフトによる情報漏洩の多発や，P2P 通信によるトラヒックの圧迫が問題となっている．このような状況を解決するための課題の一つに，P2P 通信の検知が挙げられる．しかし，近年の P2P ファイル交換ソフトは，暗号化通信を行う機能を持っており，従来の IDS などを使った方式では，検知することが困難となっている．本稿では，暗号化された P2P 端末間の通信パケットは乱数列に見えるという特徴に着目し，P2P 通信を検知する方式を提案する．

P2P Traffic Detection method based on Randomness of Packet Payloads

TOMOHIRO SHIGEMOTO† HIROFUMI NAKAKOJI†
MASATO TERADA†

These days, P2P file-sharing applications (e.g. Winny, Share) cause several issues such as the increasing number of information leakages and network congestion. To implement measures against the issues, identifying P2P traffic is essential. Since most of the recent P2P applications encrypt their traffic, however, they can evade detection by existing signature based IDS. To address this problem, in this paper, we propose a P2P traffic detection method by computing randomness of first-packet payloads. This method is based on observation that randomness of first packets in P2P communication is much higher than that in other types of communications.

1. はじめに

近年，Winny，Share 等の P2P ファイル交換ソフト（以下 P2P ソフト）による情報漏洩が多発し，未だ鎮静化の兆しが見えない状況にある．情報漏洩事故が発生した場合，組織としての監督責任が問われたり，訴訟に発展したりするなど副次的な問題を伴うこともある[1]．さらに，Winny などに代表される P2P ソフトは，音楽データや画像データなどサイズの大きなファイルの交換に利用されており，上記情報漏洩問題だけでなく，ネットワークリソースの圧迫といった問題も引き起こしている[2-3].

これらの問題を解決するための技術の一つとして，ネットワークを流れるトラヒックから，P2P 通信を検知する研究がなされてきた[4-8]．P2P ソフトの通信を検知し，通信をブロックする製品として One Point Wall [4]などがある．これらの製品の多くは，パケットデータを解析し，P2P ソフトの通信に固有した文字列やビットパターンが含まれているかどうかを判定するパターンマッチング方法により検知を行っている．しかし，最近の P2P ソフトはパケットを暗号化する機能を有しているため，パターンマッチング方法では，新たな P2P ソフトに対応するための暗号解読が必要となり，開発コストや実装までの時間を要するという問題点を伴うことになる．

パターンマッチング方法を補う技術として，トラヒック特徴から P2P 通信の検知を行う方法が考案されてきた．文献[5]では，クライアント／サーバ関係に着目し，P2P 通信を特定する方法について提案している．文献[6]では，ノードを頂点，ノード間のアクセス関係を辺としたグラフを作成し，その直径（グラフの最大頂点間距離）の大きさから P2P 通信の特定を行っている．文献[7]では，NetFlow や sFlow のフロー情報から通信先端末数の急激な変化を検出し，P2P ソフトのトラヒックを検知する方式を提案している．文献[8]では，SYN および SYN/ACK フラグの情報を利用した特徴量より P2P ソフトのトラヒックを特定する方法を提案している．しかし，提案されているトラヒックの特徴を用いた検知方式の多くは，複数の端末間通信（コネクション）情報を利用して P2P 通信の判定を行っているため，ある一定量のコネクション情報を取得するまで判定ができず，P2P 通信の検知に時間を要するという問題点がある．

そこで，本稿では，パターンマッチング方法とトラヒック特徴抽出方法の課題を解決する効率的な P2P 通信の検知方式を提案する．提案方式は，初期パケット（コネクション確立後に送受信される最初のパケット）に含まれるデータの乱数性に着目することで，暗号化通信を行なう P2P 通信を検知する．これにより，新たな P2P ソフトへの対応即応性の確保と，検知までのコネクション情報量の低減とが可能となる．

2. 初期パケットの乱数性に着目したP2P通信検知

P2P 通信の検知を行なうためには，P2P 端末間で送受信されるパケットデータを解析し，P2P ソフトに固有な文字列やビットパターンを検出する方法（Deep Packet Inspection）が一般的に用いられる．パケットデータには，通信固有の情報（文字列やビットパターン）が含まれていることが多いことから，P2P ソフトによっては検知を

† (株)日立製作所
Hitachi Ltd.

逃れるために，パケットデータを暗号化し，特徴のない乱数列に見せかけるものが存在している[9]．特に，これら P2P ソフトは，ISP によるトラヒック制限を回避するために，通信プロトコル自体を隠そうとしていることから，初期パケットから乱数列に見せかけたパケットを送受信する．

一方，暗号化通信には通信内容を保護することを目的とした SSL などのプロトコルも存在する．これらプロトコルは，TCP コネクション確立後に暗号通信で使用する暗号スイートの交換を平文にておこなっている．この初期パケットの特徴の違いに着目することで，通信そのものを隠蔽することを目的とした P2P 通信と，通信内容を保護することを目的とした通信とを識別できる可能性がある．

本提案方式では，初期パケットの乱数性を評価することで，P2P通信（乱数性あり）とその他の通信（乱数性なし）の差異を見出し，P2P通信の検知を試みる（図 1）．

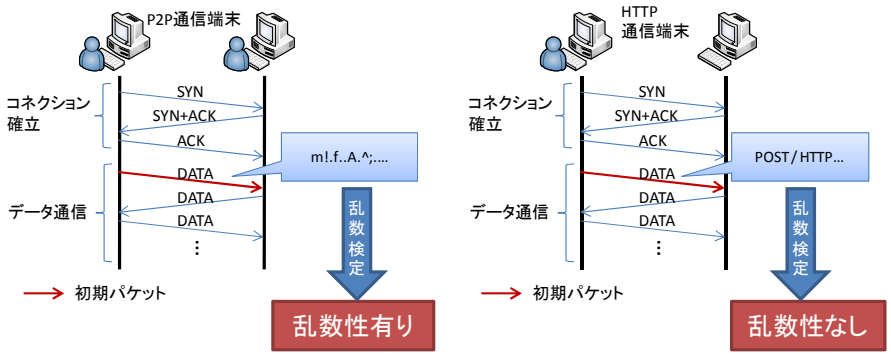

図 1　初期パケットの乱数性に着目した P2P 通信検知

2.1　初期パケット抽出

提案方式では，TCP コネクション確立後に送受信される最初のパケットを初期パケットとして P2P 通信の判定に使用する．

初期パケットの抽出方法としては，通信フローの状態を管理しながらパケットをトレースする方法と，SYN ビットとペイロード長を利用した簡易的な方法が考えられる．状態管理しながらパケットをトレースする方法は，コネクション確立状態を管理し，SYN パケット，SYN+ACK パケット，ACK パケットの 3 ウェイハンドシェイクの後のパケットを初期パケットとして抽出する．この場合，多数の端末間通信が行われているネットワークでコネクション毎の状態管理を行わなければならない．

一方，SYNビットとペイロード長を利用した簡易的な方法は，SYNパケットの次に送受信されるペイロード長が 1 バイト以上のパケットを初期パケットとして抽出する方法である(図 2)．提案方式では，簡易的な方法を採用し，プロトタイプを実装した．

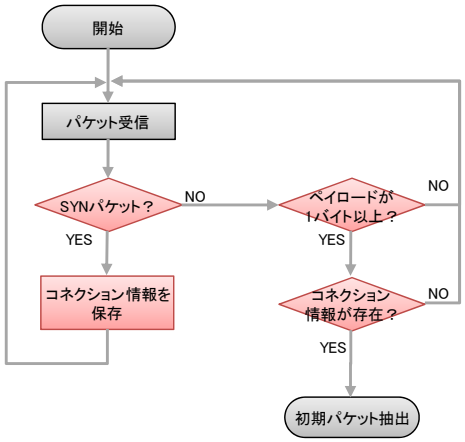

図 2　初期パケット抽出フロー

初期パケットの抽出方法の具体的なフローは，次の通りである．

1. ルータやスイッチのミラーポートから，検査対象パケットを受信する．
2. 検査対象パケットの SYN フラグがセットされていれば処理 3 に，SYN フラグがセットされていなければ処理 4 に進む．
3. SYN フラグがセットされた検査対象パケットから，送受信 IP アドレス及び送受信ポート番号を記録した後，処理 1 に戻る．
4. SYN フラグがセットされていない検査対象パケットのペイロード長を検査し，TCP データが存在（ペイロード長が 1 バイト以上）すれば，処理 5 に進む．TCP データが存在しなければ，処理 1 に戻る．
5. SYN フラグがセットされておらず，ペイロード長が 1 バイト以上，かつ，既に，送受信 IP アドレス及び送受信ポート番号として記録されている場合は，当該パケットを初期パケットとして判定する．それ以外の場合，処理 1 に戻る．

2.2　P2P通信判定

提案方式では，初期パケットの乱数性を評価することで，P2P 通信（乱数性あり）とその他の通信（乱数性なし）の差異を見出し，P2P 通信の検知を試みる．乱数性の評価として，次のような検定がある．

- NIST Special Publication 800-22[10]
- FIPS140-2[11]
- DIEHARD による検定法[12]

本稿では，米国立標準技術研究所（National Institute of Standards and Technology）が推奨している乱数検定であり，乱数性の検定に広く利用されていることから，NIST Special Publication 800-22 を利用する．

NIST Special Publication 800-22 の乱数検定では，検定ごとに有意確率（p-value）が得られる．p-value とは，検定で出力される統計量の正規分布もしくは，カイ 2 乗分布において，それよりも偏った統計量が発生する確率を表したものである．NIST Special Publication 800-22 では，p-value 値が 0.01 より小さい場合に，そのデータは良い乱数ではないと判断している．

3. 乱数検定並びに閾値の検討

本章では，暗号化通信を行なう P2P 通信とその他の通信の初期パケットに対して乱数検定を行なった調査結果を報告する．次に，調査結果から，P2P 通信（乱数性あり）とその他の通信（乱数性なし）の判別に適した乱数検定方法および，検定閾値について述べる．

(1) 調査目的

複数の乱数検定方式を組み合わせて P2P 通信の判定を行うことも考えられるが，検知までの時間を最小限に抑えるために，様々な乱数検定方式の中から，P2P 通信を判定するために最も適した乱数検定方式および，検定閾値を決定する．

(2) 乱数検定方法

(a)調査方法

暗号化通信を行なう P2P ソフト（Winny，Share，PerfectDark，Winnyp）の初期パケット 400 パケットと，その他の通信（暗号化通信を行わない P2P ソフト（Cabos）及びその他の通信（http，https，pop3））の初期パケット 400 パケットのそれぞれに対して，NIST Special Publication 800-22 に含まれる乱数検定をおこなう．

(b)調査結果

表 1に，暗号化通信を行なうP2Pソフトとその他の通信の初期パケットに対する乱数検定結果として，乱数性があると判断されたp-value値が 0.01 以上の割合を示す．なお，初期パケットのデータ長が短く，乱数検定が行えなかったデータについては，乱数検定対象からはずした．

この結果から，暗号化通信を行なう P2P ソフトで乱数性ありと判断された割合が高く，その他の通信で乱数性ありと判断された割合が低い検定方法は，Frequency Test，Cumulative Sum Test (forward)，Cumulative Sum Test (backward)，Runs Test の 4 つであった．

表 1　乱数検定結果

	暗号化通信を行う P2P ソフト	その他の通信
Frequency Test	98.5%	25.5%
Test For Frequency Within A Block	84.5%	25.3%
Cumulative Sum Test (forward)	98.8%	25.0%
Cumulative Sum Test (backward)	97.8%	25.8%
Runs Test	98.5%	27.3%
Test For The Longest Run Of Ones In A Block	74.3%	45.8%
Random Binary Matrix Rank Test	69.5%	12.0%
Discrete Fourier Transform Test	100%	87.0%
Overlapping Template Matching Test	69.8%	13.8%
Maurer’s Universal Statistical Test	0%	0%
Approximate Entropy Test	0%	0%
Random Excursions Test	76.8%	85.3%
Random Excursions Variant Test	75.0%	25.0%
Serial Test	76.8%	25.0%
Linear Complexity Test	66.8%	38.5%
Non-overlapping Template Matching Test	0%	0%

(3) 閾値

(a)調査方法

暗号化通信を行なう P2P ソフトで乱数性ありと判断された割合が高く，その他の通信で乱数性ありと判断された割合が低い検定方法 Frequency Test，Cumulative Sum Test (forward)，Cumulative Sum Test (backward)，Runs Test の 4 つについて，p-value 値を変化させながら，検知率及び誤検知率を評価する．

(b)調査結果

図 3にp-value値の変動に伴う検知率を示す．この結果から，検知率については，検定

方法の差があまり出てこないことが分かる．一方，図 4より，誤検知率については，Frequency TestとRuns Testにおいてのp-value値を変動させることにより，誤検知率を低減できることが分かった．特に，Frequency Testにおいてp-value値 0.06 以上をP2Pと判定することで，誤検知をなくすことができる．

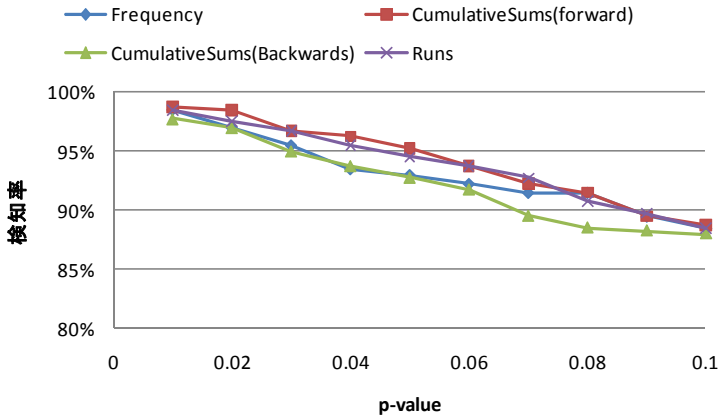

図 3　p-value 値と検知率

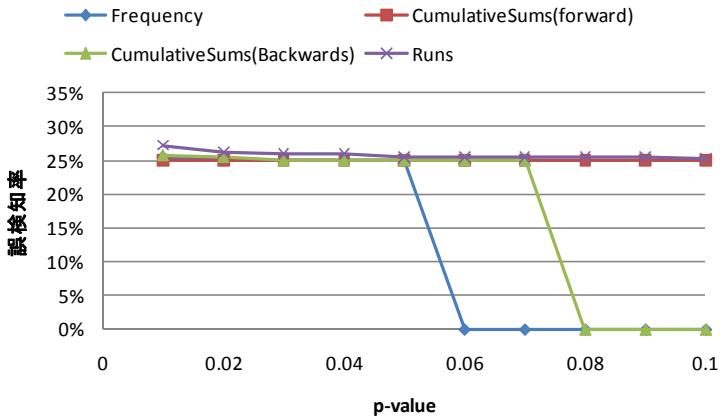

図 4　p-value 値と誤検知率

4.　評価実験

本章では，初期パケット抽出機能，Frequency Test による P2P 通信判定機能を実装した提案方式のプロトタイプを用いて実施した有効性の評価実験について述べる．

4.1　評価目的

有効性の評価にあたっては，次の視点から実施する．

- 提案方式を用いた暗号化通信を行なう P2P 通信の検知精度（検知率，誤検知率）
- 提案方式の処理性能

4.2　評価方法

評価用データ取得環境で取得した評価用データ（pcapファイル）を，提案方式のプロトタイプを搭載したPC（表 2）で初期パケット抽出機能，P2P通信判定機能による検知処理を行う．P2P通信判定機能では，3 章の検討結果より，乱数検定にはFrequency Testを実装し，P2P通信判定の閾値として 0.06 を使用する．

表 2　検知装置のスペック

項目	仕様
OS	Windows Vista
CPU	Intel Core i7(2.67GHz)
Memory	12.0GB

(1) 評価用データ取得環境

評価にあたっては，情報通信研究機構北陸リサーチセンターが開発した大規模テストベッド設備であるStarBED[13]上に評価用データ取得環境を構築した(図 5)．評価用データ取得環境は，インターネットを模擬した階層的ネットワーク構成をとり，510 台のP2P通信端末(Winny:108 台，Share:54 台，PerfectDark:30 台，Winnyp:12 台，Cabos:90 台，その他のP2P:216 台)からなるネットワークA,Bを相互に接続させた計 1,020 台のノードから構成した．P2P通信以外のトラヒック発生(http，https，pop3)には，トラヒック発生サーバを使用し，トラヒック分配ルータから，ネットワーク基幹部に転送した．

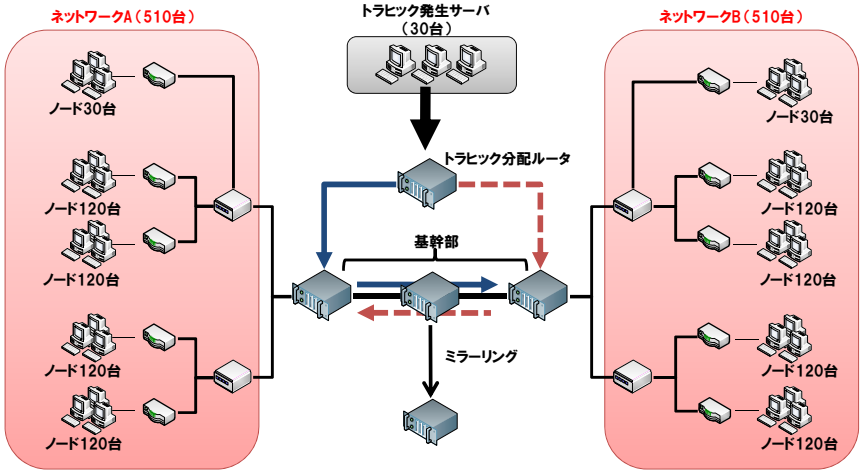

図 5　評価環境

(2) 評価用データ

評価用データ取得環境の基幹部を通過するパケットを評価データ（pcapファイル）として使用する．評価データの概要を表 3，表 4に示す．なお，本評価実験では，実験期間中にSYN+ACKパケットが基幹部を通過した端末を検知対象の端末とする．これにより，P2Pソフトが活性化していなかったり，同じネットワーク内での通信に留まっていたりするなどの理由で，検知が不可能な端末を評価対象から除外する．

表 3　P2P ソフトの通信を含む評価用データ

項目	数値
ファイルサイズ [bytes]	8,881,167,669
パケット数 [pkts]	10,000,000
スループット [pps]	54,347.8

表 4　その他の通信を含む評価用データ

項目	数値
ファイルサイズ [bytes]	8,236,497,364
パケット数 [pkts]	10,302,921
スループット [pps]	30,482

4.3 評価結果と考察

(1) 検知精度

暗号化通信を行なうP2P通信（Winny，Share，PerfectDark，Winnyp）の検知率を表 5に，その他の通信（Cabos，http，https，pop3）の誤検知率を表 6に示す．なお，括弧内の数値は（検知した端末/検知対象の端末）を示す．

評価用データにおいては，提案方式により，暗号化通信を行う P2P 通信の検知率100%，誤検知率 0%での検知が可能であった．

表 5　暗号化通信を行う P2P 端末検知率

アプリケーション	検知率
Winny	100%　(210/210)
Share	100%　(99/99)
Winnyp	100%　(24/24)
Perfect Dark	100%　(57/57)

表 6　その他の通信端末誤検知率

アプリケーション	検知率
Cabos	0%　(0/180)
http	0%　(0/1356)
https	0%　(0/158)
pop3	0%　(0/58)

(2) 処理性能

表 7にP2Pソフトの通信を含む評価用データを処理した際の処理性能を示す．この結果より，実効スループットが評価用データのスループットを大きく上回っていることを確認した．ただし，実効スループットは，pcapファイルの読み込み時間を元に算出しているため，実稼働環境での性能評価は今後の課題である．

表 7　処理性能

項目	数値
処理時間 [sec]	53.63
実効スループット [pps]	186,462.80

(3) 考察

(a) P2P 通信の判定について

本評価実験では，乱数検定として Frequency Test を，P2P 通信の判定閾値として 0.06 を用いることで，検知率 100%，誤検知率 0%を達成した．しかし，実ネットワークでは，評価実験に利用しなかった様々なアプリケーションの通信が含まれているため，適切な閾値は変化すると考えられる．今後は，様々なアプリケーションの通信に対して評価を行い，適切な閾値を検討する．

また，本稿では検知までの時間を最小限に抑えるために，1 種類の乱数検定を利用した．今後は，複数の乱数検定を組み合わせて P2P 端末の判定を行い，検知精度の向上を検討する．なお，複数の乱数検定を組み合わせると処理性能が低下すると考えられるが，この点に関しても今後評価を行う．

(b) 乱数検定について

本稿では，乱数検定に NIST Special Publication 800-22 を利用したが，ペイロード長が短いと，乱数検定を適用できない場合のあることが分かった．この問題については，初期パケットと後続パケットを連結し，ペイロード長を確保することで解決できるが，一方で，継続パケットを待たなければならず，検知までに時間を要するという問題を伴うことになる．

別の解決方法として，乱数検定を P2P 通信検知用に最適化することがあげられる．乱数検定の最適化については，複数の乱数検定の組み合わせと併せ，今後の課題である．

5. おわりに

本稿では，暗号化通信を行う P2P 通信を検知する方式を提案した．また，評価用データ取得環境で取得した評価用データを，提案方式のプロトタイプを搭載した PC で検知処理を行うことで，提案方式の有効性を検証した．その結果，初期パケットに含まれるデータの乱数性に着目することで，暗号化通信を行なう P2P 通信を検知できることを示した．

今後は，検定方法の改良や，動的な閾値変更を行うことによって検知精度を向上させていくことを検討する．

謝辞 大規模ネットワーク実験環境 StarBED を本実験環境として利用するにあたりご協力を頂いた独立行政法人情報通信研究機構北陸リサーチセンター，ICT 研究開発機能連携推進会議(HIRP)の関係者各位に深く感謝致します．また，StarBED 上の実験環境構築にあたり，有益な助言と協力を頂いた北陸先端科学技術大学院大学ならびに，独立行政法人情報通信研究機構北陸リサーチセンターの篠田陽一教授，三輪信介氏，宮地利幸氏，中井浩氏，安田真悟氏に深く感謝致します．本研究は総務省から受託した「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の成果の一部です．本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝いたします．

参考文献

1) Winny による道警の捜査情報漏洩事件など，2005 年の IT 関連判決を振り返る，http://internet.watch.impress.co.jp/cda/event/2005/12/05/10099.html
2) 森達哉，内田真人，後藤滋樹，“インターネットトラヒックのフロー分析：web と P2P の特性比較”，電子情報通信学会論文誌, D-I, Vol.J87-D-I, No.5, pp.561-571, 2004.
3) Louis Plissonneau, Jean-Laurent, Costeux, and Patrick Brown, “Analysis o f Peer-to Peer Traffic on ADSL”, Passiveand Active Network Measure ment , 2005.
4) One Point Wall, http://www.onepointwall.jp/
5) 大坐畠智，川島幸之助，“クライアント／サーバ関係に着目したピュア P2P アプリケーショントラヒック特定方式と評価，”情報処理学会論文誌 Vol49，No.2 pp.988-998, Feb.2008.
6) Constantinou, F. and Mavrommatis, P. “Identifying Known and Unknown Peer-to-Peer Traffic,” Proc. 5th IEEE International Symposium on Network Computing and Applications, pp. 93-102, 2006.
7) 藤井聖，中村豊，藤川和利，砂原秀樹，“通信先ホスト数の変化に注目した異常トラヒック自動検出手法の提案と評価，”電子情報通信学会論文誌 Vol.J88-B，No.10 pp.1922-1933, 2005.
8) 中村文隆, 松田崇, 若原恭, 田中良明, “トラヒック特徴量解析とアプリケーション分別, ” IEICE Technical Report, NS2006-60, IN2006-60, CS2006-26, pp. 25-30, 2006.
9) Why Encrypting BitTorrent Traffic Is Good. http://torrentfreak.com/why-encrypting-bittorrent-traffic-is-good/
10) NIST, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” http://csrc.nist.gov/groups/ST/toolkit/rng/index.html
11) NIST, FIPS PUB 140-2, “Security requirements for cryptographic modules,”
12) G. Marsaglia, “DIEHARD,” http://www.stat.fsu.edu/pub/diehard/
13) Hokuriku Research Center, StarBED Project, http://www.starbed.org/