L-020

TCP/IP ヘッダを用いた NAT クライアント検出
Detection of Nated clients by using TCP/IP header fields

李 熙貞 † 中村 康弘 †
Hee Jeong Lee Yasuhiro Nakamura

1. はじめに

近年，インターネットに接続する機器の機能やサービスが増えており，組織 LAN 等に接続する機器を適切に管理することの重要性が増している．未承諾機器の LAN 接続を排除するために，MAC アドレス認証や端末へのエージェント導入などの様々な対策が行われている．しかしながら，端末機器の高性能化に伴い，Windows の ICS や FreeBSD の natd などの NAT 機能を用いることにより，他の機器にネットワークインターフェースを共有させることが可能となってきた．すなわち，LAN 接続が許可されている機器を介して未承諾機器を接続することにより端末認証機能が無効になってしまう．未承諾機器は組織 LAN 内で規定されたウイルス対策や脆弱性対策などが十分に行われておらず，攻撃者の不正アクセスや DDos 攻撃の踏み台になる恐れがある．さらに，踏み台攻撃に代表されるように，承諾機器が NAT ルータとして動作している場合，管理下の組織 LAN とは異なるネットワークからのアクセスパスを構成してしまうため，NAT 経由の接続機器の存在に気付かない場合もあり得る．そこで，この研究では，組織 LAN 等に接続されたクライアント機器が行う通信を監視し，そのパケット特徴を分析することにより，NAT 接続の有無を判定するアルゴリズムを提案する．加えて，NAT が検出された場合にはその配下の機器を識別することを目標として分析手法を検討した．

2. 既存の NAT 検出手法

P. Phaal[1] は IP ヘッダの TTL(Time To Live) 値を用いた NAT 検出技術を提案した．また，T. Miller[2] は，TCP ヘッダの Window サイズやオプションなどの OS fingerprint を用いた方法を提案している．各 OS やそのプロトコルは初期 TTL 値やウインドウサイズに特定の初期値があり，それらを観測することで，NAT の有無や NAT クライアントの OS 判定が可能となる．しかしながら，これらの手法では同一 OS の複数の NAT クライアントを識別することはできない．

S. M. Bellovin は [3] で，IP ヘッダの IPid 値が 2^{16} の範囲で 1 ずつ増えて行くことを利用し，NAT 配下のクライアント数を計測する手法を提案した．しかし，Windows 以外の OS の IPid 値は宛先アドレス, TCP セッション, プロトコル等に依存して変化するため，IPid 値のみから，各クライアントを正しく識別することは難しい．

このほか，T. Kohno ら [4] の clock-skew を用いた検出手法，G. Maier ら [5] の TTL 値と HTTP request の user-agent を用いた検出手法など多くの手法が提案されている．しかしながら，いずれの手法を用いても，昨今の多種多様な OS 種別を前提に NAT の有無の検出と NAT 配下のクライアントの識別を正確に行うことは困難である．

そこで，この研究では既存の種々の特徴分析手法を検証することにより，NAT 検出とクライアント識別に利用できるヘッダ情報を選別し，これを用いた効率的なアルゴリズムを構成した．

†防衛大学校理工学研究科情報数理専攻 〒 239-8686 神奈川県横須賀市走水 1-10-20. em52057@nda.ac.jp, yas@nda.ac.jp

表 1: 各 OS の IPid 値の特徴

OS	ICMP	TCP	UDP
Window7	プロトコル, 宛先, セッションとは無関係に必ず連続で 1 ずつ増加する．最大値 (0x7fff) に達すると初期値 (0) に戻り，再度 1 ずつ増加する		
Solaris 10	プロトコルに無関係に連続で 1 ずつ増加一定時間後に他の初期値から 1 ずつ増加宛先が変わると他の初期値から 1 ずつ増加		
Ubuntu 13	同じ TCP セッションの間には 1 ずつ増加セッションや宛先が変わると他の初期値から始まり，1 ずつ増加		
CentOS 6.2	常に 0x0000	Ubuntu と同一	
OpenBSD 5.4	常にランダムに変化する		

表 2: 各 OS のソースポート番号の特徴

OS	ICMP	TCP	UDP
Windows 7 Solaris 10	プロトコルや宛先，TCP セッションとは無関係に連続で 1 ずつ増加．再送発生時はその回数を加算した次の番号から増加		
Ubuntu 13 CentOS 6.2	同じ宛先の場合は TCP セッションとは無関係に 1 ずつ増加．宛先の IP アドレスやポート番号が変わると他の初期値から 1 ずつ増加．		
OpenBSD 5.4	常にランダムに変化する		

表 3: 各 OS のウインドウサイズ

OS	Win7	WinXP	Solaris	CentOS	Ubuntu	OpenBSD
Bytes	8192	64240	49640	14600	29200	16384

3.TCP/IP ヘッダフィールドの分析結果

NAT 検出および NAT クライアント識別に利用可能な TCP/IP ヘッダフィールドを検証するため，各種 OS の IPid 値, TCP のソースポート番号およびウインドウサイズの初期値と変化について検証を行った．それぞれの結果を表 1, 表 2, 表 3 に示す．

4. 提案アルゴリズム

各フィールド値の初期値と変化の様子から，NAT 検出および NAT クライアントの台数を識別するアルゴリズムは以下の通りである（図 1）.

Step 1: LAN 内接続機器が入出力するすべての TCP パケッ

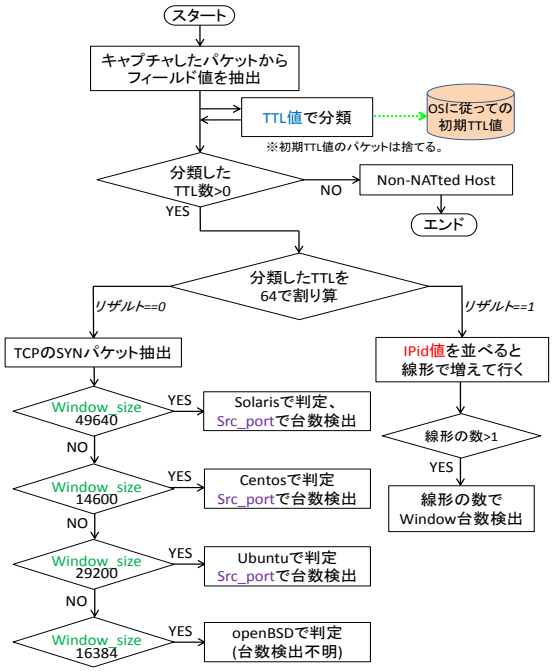

図 1: 提案アルゴリズム

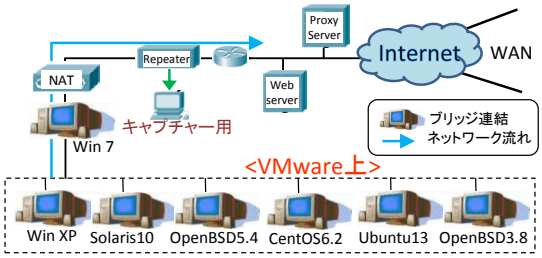

図 2: 実験環境の構成

トをキャプチャし，TTL 値ごとに分類する．初期 TTL 値あるいは既知の経路長が減算された TTL 値を持つパケットは廃棄する．

Step 2: $64 \leq TTL < 128$ の場合は Windows と判定する．表 1 に示す通り，Windows はセッション等とは無関係に IPid 値が 1 ずつ増加するので，IPid の値の種類数が NAT クライアントの台数となる．

Step 3: Windows 以外と判別された場合は，TCP SYN パケットのみを抽出し，初期ウインドウサイズごと分類して表 3 に基づき，OS の種類を判別する．

Step 4: 表 2 に示す通り，TCP ソースポート番号の変化の様子からそれぞれの OS ごとのクライアント台数を求める．ただし，OpenBSD のみは IPid, TCP ソースポート番号ともにランダムのため，クライアント台数の判定はできていない．

5. 実験結果

図 2 の実験環境を構築し，NAT 機器の外側でパケットキャプチャを行い，NAT 配下のクライアントから通信を行った．得られたパケットキャプチャデータに対し，図 1 のアルゴリズムに従って NAT 判定および NAT クライアント台数の計測を行った結果，OpenBSD 以外では正しい検出結果が得られ

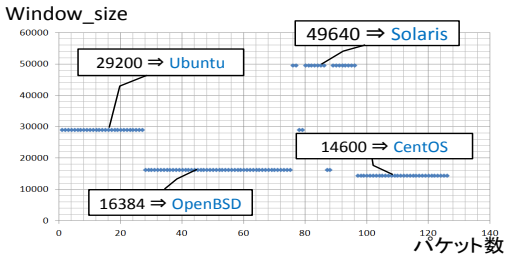

図 3: ウインドウサイズによる OS 分類の例

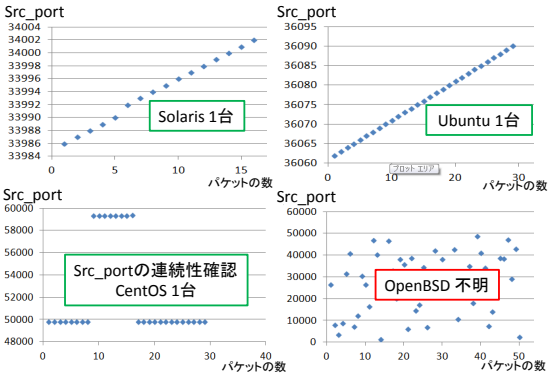

図 4: ソースポート番号による台数判定結果

ることを確認した．ウインドウサイズにより OS 判定を行った結果の一例を図 3 に，ソースポート番号の変化からクライアント台数を特定する例を図 4 に示す．OpenBSD のみはクライアント台数を判別することができない．

6. まとめ

パケットヘッダの各フィールド値の初期値とその変化について検証実験を行い，その結果に基づいて NAT 検出および NAT クライアント数計測のアルゴリズムを提案した．LAN 内に NAT 機器を設置し，複数の種類のクライアントを接続して通信を行い，NAT の外側でキャプチャしたデータに対して提案手法を適用して動作を確認した．今後は OpenBSD の取り扱い及び様々な実環境での検証と評価を行う．

参考文献

[1] Peter Phaal, ”Detecting NAT Devices using sFlow”, http://www.sflow.org/detectNAT/

[2] T. Miller, “Passive OS fingerprinting: Details and techniques”, http://www.ouah.org/incosfingerp.htm (last modified: 2005)

[3] S. M. Bellovin, “A Technique for Counting NATted Hosts”, In ACMSIGCOMM Internet Measurement Workshop (IMW2002)

[4] T. Kohno, A. Broido and kc claffy, “Remote physical device fingerprinting”, In Proceedings of IEEE Symposium on Security and Privacy, pages 211–225, May 2005.

[5] G. Maier, F. Schneider and A. Feldmann, “NAT usage in residentialbroadband networks”, In Passive and Active Measurement Conference(PAM2011), pp. 32–41, 2011.