2D-02

DNS 問い合わせを用いた機器推定手法の検討

近藤 毅† 加島 伸悟†

日本電信電話株式会社 NTT セキュアプラットフォーム研究所†

1. はじめに

IoT の進展に伴い，大量・多種多様な機器がインターネットに接続されるようになっている．インターネットに接続される機器の中でも特に増加傾向にあるのがコンシューマ向けの IoT 機器である[1]．コンシューマ向け IoT 機器は，PC・スマートフォンなどの ICT 機器とは異なり，ハードウェアや OS の制約等によりアンチウィルスソフトの導入やソフトウェア最新化など機器単体でのセキュリティ対策が困難であることが多い．そのため，機器とインターネットの境界にあるゲートウェイにおいて不正通信を検知・遮断する等，機器のセキュリティ対策を補完する役割を担うことが期待されている[2]．不正通信の発生時にはユーザに機器の設定変更や交換等の対応を促すためにユーザへの通知も必要となる．不正通信の検知・遮断は機器の IP アドレスや MAC アドレスなどのアドレス情報をもとに行われる一方，コンシューマの多くは IT リテラシが高くないことからアドレス情報ではなく，機器の製造メーカ名，機種名，OS 名などの識別情報を用いて通知する必要がある．本稿では DNS クエリを用いて，ネットワーク内の機器を識別する手法を提案する．

2. 既存手法

ネットワーク内の機器を識別するための既存手法は，p0f[2]に代表される，ネットワーク上のパケットを観測するだけでよいパッシブ型，nmap[2]に代表される，能動的にパケットを送信し応答パケットを観測するアクティブ型に分類できる．p0f は TCP 通信における SYN パケット等の情報を用いて，nmap はポートスキャン結果を用いて，OS 名を推定することができる．IoT 機器は画面が無くユーザが機器の OS 名を把握していないケースが多いため，識別情報が OS 名だけでは不十分である．一方，IoT 機器は単機能であることからアプリケーションを推定することで機器を識別できる可能性が高い．

OS だけでなくアプリケーションを推定できる手法が文献[5]で提案されている．本手法は，DNS トラヒックを観測することで機器を推測するパッシブ型の手法である．本手法は，DNS クエリの中でも，OS やアプリケーション固有の DNS クエリを用いて送信元ホストの OS やアプリケーションを推測する．しかしながら，この提案においては，オペレータ等が手動で OS やアプリケーション固有の DNS クエリを探し出し，登録する必要がある．

以上のように，多種多様な IoT 機器が存在する状況，新たな機器が次々と流通する状況，ICT 機器のように OS やアプリケーション，ファームウェアの更新が頻度に発生する状況においては，機器やバージョンに依存して変化する固有 DNS クエリの特定，更新のコストは高いといえる．

3. 提案手法

本稿では，OS やアプリケーション固有の DNS クエリを手動で特定・設定することなく機器の識別を行う手法を提案する．

提案手法では，既知の機器毎の DNS クエリ集合に対し，ユーザが識別しやすい機器名をラベルとして付与し，これを特徴ベクトルの 1 エントリとする．この処理を機器毎に実施し，特徴ベクトルを作成する．この特徴ベクトルに対して，新たに接続された機器の DNS クエリ集合をテストデータとし，類似度判定手法(Naïve Bayes)により新たに接続された機器の推定を行う．推定の結果として特徴ベクトル中のいずれか１つのラベルが最も類似度の高いと判定され，出力される．本稿では Naïve Bayes によって出力されたラベルを機器推定結果として扱う．

提案手法の処理の具体例を説明する．図 1 は機器毎の DNS クエリの集合を二次元のマトリクスとして示す．列は DNS 問い合わせの内容で，問い合わせた FQDN を示す．行は，機器毎（ラベル毎）の DNS クエリ集合を示す．加えて，機器を識別する情報として手動でラベルを付加した．行 1～19 を特徴ベクトルとし，行 21 に示した DNS クエリの集合をテストデータとして，Naïve Bayes で推定を行うと，既存のラベル付エントリ（特徴ベクトル）のいずれかが類似したエント

と

Device Estimation Using DNS Query Analysis
KONDOH Tsuyoshi† and KASHIMA Shingo†
†NTT Secure Platform Laboratories NTT Corporation
180-8585 Midori-Cho, Musashino-Shi, Tokyo, Japan
{kondoh.tsuyoshi, kashima.shingo}@lab.ntt.co.jp

リとして出力される．これが機器の推定結果である．具体的には，行 21 のエントリ（テストデータ）に対して類似したエントリは，行 15 のエントリであり，結果として得られる機器のラベルは「ipad-01」である．これは，テストデータと同一の機種であり，機器推定が成功したといえる．

4. おわりに

本稿では，DNS クエリを情報源とし，Naïve Bayes を用いた類似度判定手法によりネットワークに接続された機器を推定する手法を提案した．

既存手法に対する利点としては，OS やファームウェア，アプリケーション固有の DNS クエリをオペレータ等が発見し，設定する必要が無いという点が挙げられる．

一方で，特徴ベクトルに類似した機器が無い，完全に未知の機器の DNS クエリ集合がテストデータになる場合もある．この場合も，Naive Bayes を用いた場合はいずれかの機器に類似するとして何らかのラベルが出力される．このためため，機器推定に誤りが生じる．

これに対して Naïve Bayes による類似度判定にでは，各ラベルに対する類似度が得られるため，既存のエントリに対する類似度が低い場合は，既存の機器ではなく，未知の機器が接続されたと判断することが出来る．この際は，ユーザやオペレータ対して，新たなラベルの付与を求めることで，効果的に機器識別の精度を上げることが出来る．

また，ここでの特徴ベクトルの作成はオペレータやユーザが自ネットワーク内の機器に限って行う必要は無く，他者によって作成されたエントリを流通・入手することも考えられる．

一方で，未知の機器と判定すべき類似度のしきい値の決定等は，今後の課題である．

参考文献

[1] Rob van der Meulen: Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner (online), available from (http://www.gartner.com/newsroom/id/3165317) (accessed 2018-01-12).

[2] 独立行政法人情報処理推進機構 技術本部 セキュリティセンター：IoT 開発におけるセキュリティ設計の手引き，p.10，(2017)

[3] Michal Zalewski: p0f v3 (online), available from (http://lcamtuf.coredump.cx/p0f3/) (accessed 2018-01-12).

[4] Gordon Lyon: Nmap: the Network Mapper – Free Security Scanner (online), available from (https://nmap.org/) (accessed 2018-01-12).

[5] 松中隆志，山田明，窪田歩：DNS トラヒックによる Passive OS Fingerprinting 手法の提案，研究報告モバイルコンピューティングとユビキタス通信（MBL），(2012).

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19		232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250
		0.irobot.pool.ntp.org.	10108backup.broadlink.com.cn.	10108main.broadlink.com.cn.	10108top.broadlink.com.cn.	18-courier.push.apple.com.	29-courier.push.apple.com.	2.android.pool.ntp.org.	50-courier.push.apple.com.	50.courier-push-apple.com.akadns.net.	52-33-40-94-push.np.communication.pl	52-37-164-27-push.np.communication.i	a2uowfjvhio0fa.iot.us-east-1.amazonaws	a3jp.np.communication.playstation.net.	aax-fe.amazon-adsystem.com.	accounts.google.com.	accscdn4public.m.taobao.com.	acs4public.m.taobao.com.	amdc.m.taobao.com.	amzdigital-a.akamaihd.net.		watson.telemetry.microsoft.com.	weather.aquos.jp.	www.apple.com.	www-cdn.icloud.com.akadns.net.	www.googleadservices.com.	www.googleapis.com.	www.google.co.jp.	www.google.com.	www.gstatic.com.	www.icloud.com.	www.msftconnecttest.com.	www.msftncsi.com.	www.youtube.com.	xbox.ipv6.microsoft.com.	xp.apple.com.	xp.itunes-apple.com.akadns.net.	xsts.auth.xboxlive.com.	xtrapath2.izatcloud.net.	xtrapath3.izatcloud.net.
1	eSensor01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	eRemote01	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	amazonfire01	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1		0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
4	amazonfire02	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	1		0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
5	Netatmo02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Qrio01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	･･･中略･･･	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	switch	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	psvita	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	ps4-01	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	ps4-02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	xbox	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		1	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0
12	Roomba01	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	HDL2-AA201	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	LS510D0201-01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	ipad-01	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0		0	0	1	1	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0
16	G-GEAR01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	Pixel01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		0	0	0	0	1	1	1	1	1	0	0	0	1	0	0	0	0	0	1
18	AQUOS40W01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	Pixel03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	1	0
20																																								
21	ipad-02	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	1	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0

図 1. 機器毎の DNS クエリ集合