DNSSECトラフィック解析
where and how many?

福 田　健 介 (国立情報学研究所)
佐 藤　新 太 (JPRS)
三 田 村　健 史　(JPRS)

National Institute of Informatics

今日のメッセージ

- JPサーバでのパッシブ計測とアクティブ計測結果
- DNSSECクエリを出すホスト数 (DNSSECホスト)/AS数は増加傾向
- 重複したDSクエリが多い
- オープンリゾルバでの実験結果から，DNSSECホストのうち実際に検証を行うホストは70%程度
  - 残りはエンドホストでの検証

National Institute of Informatics

データセット

- パッシブ計測
  - JPサーバでの48時間DNSパケットトレース (7 servers and many replications)
  - 計測時期: 2011.06, 2011.12, 2012.04
  - “DS xxx.jp”に着目
- アクティブ計測
  - DNSSECクエリをパッシブトレース中のDNSSECホストへ送信
  - オープンリゾルバでのバリデーション状況を調査

National Institute of Informatics

トラフィック内訳

- DNSSECクエリを送信したホスト/AS数
  - 0.4->1.1% for IP addrs (hosts)
  - 5.9->11.1% for ASes
- ちゃんと増えている :)

TABLE I
TRAFFIC BREAKDOWN

	Total			DNSSEC		
Data	IP addrs	ASes	Countries	IP addrs	ASes	Countries
201106	2150958	28722	215	9629	1705	105
201112	2081826	29600	217	14085	2490	119
201204	1904610	29334	216	21238	3295	136

National Institute of Informatics

DSクエリの傾向

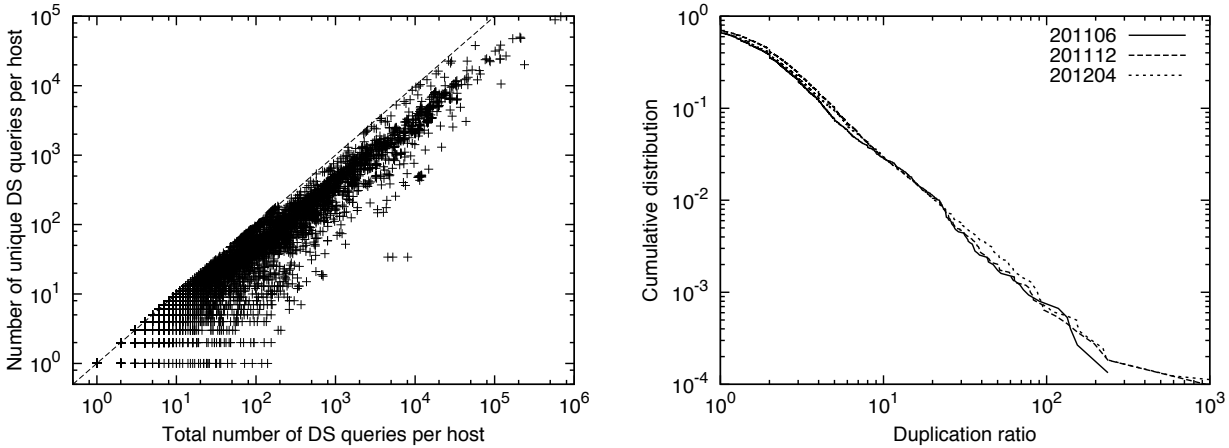


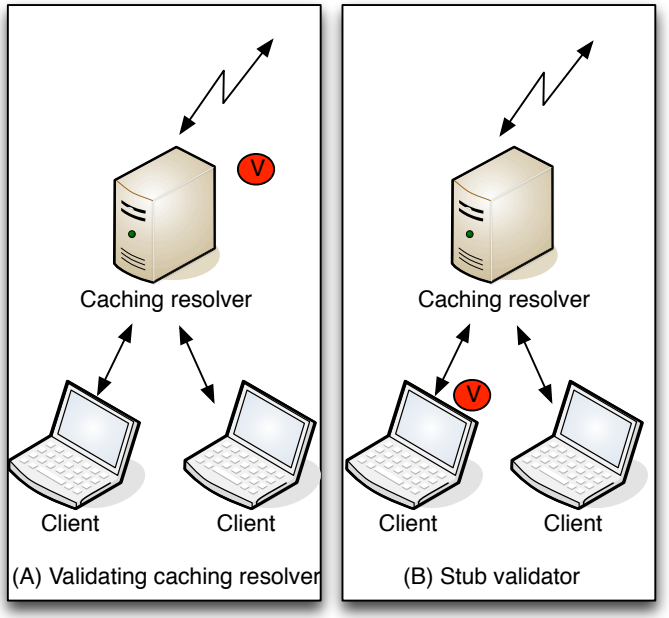
Fig. 3. (a) Total number of DS queries and the number of unique DS queries, and (b) Cumulative distribution of duplication ratio per host

- ほとんどのDSクエリは重複
- 有効なクエリは20-30%
- DSが登録されていないゾーンに対するネガティブキャッシュ(15min)の影響 => DS登録数を増やせば減る?

National Institute of Informatics

DNSSEC検証を行うホスト

- Validating caching resolver
  - DNSSEC検証を行うキャッシュリゾルバ
- Stub validator
  - クライアントでDNSSEC検証
  - e.g., web plugins
  - キャッシュリゾルバは単にDNSSECクエリをやりとりするのみ



National Institute of Informatics

オープンリゾルバでのDNSSEC検証

- トレース中のDNSSECホストにDNSSECクエリを送信(dig . @xxx +dnssec)
- DNSSECホストの10%がオープンリゾルバ
- そのうち38-50%が実際に検証している

TABLE III
VALIDATING AND NON-VALIDATING CACHING RESOLVERS

201106	validator	non-validator	total
DS-DNSKEY	276 (52%)	257 (48%)	533
DS-only	48 (18%)	226 (82%)	274
DNSKEY-only	7 (11%)	63 (89%)	70
total	331 (38%)	546 (62%)	887

201112	validator	non-validator	total
DS-DNSKEY	546 (61%)	343 (39%)	889
DS-only	109 (34%)	208 (66%)	317
DNSKEY-only	26 (16%)	133 (84%)	159
total	681 (50%)	684 (50%)	1365

201204	validator	non-validator	total
DS-DNSKEY	891 (64%)	510 (36%)	1401
DS-only	125 (17%)	602 (83%)	727
DNSKEY-only	13 (11%)	109 (89%)	122
total	1029 (46%)	1221 (54%)	2250

National Institute of Informatics

検証を行うキャッシュリゾルバ数の推定

- キーアイディア (詳細は省略)
  - ホスト単位でのオリジナルクエリ数とDSクエリ数の比 (近似だけど計算が大変じゃない)
    - 検証を行わないキャッシュリゾルバ => 比が小さい
    - 検証を行うキャッシュリゾルバ => 比が大きい
  - オープンリゾルバでの精度は85%

National Institute of Informatics

検証を行うキャッシュリゾルバ数の推定

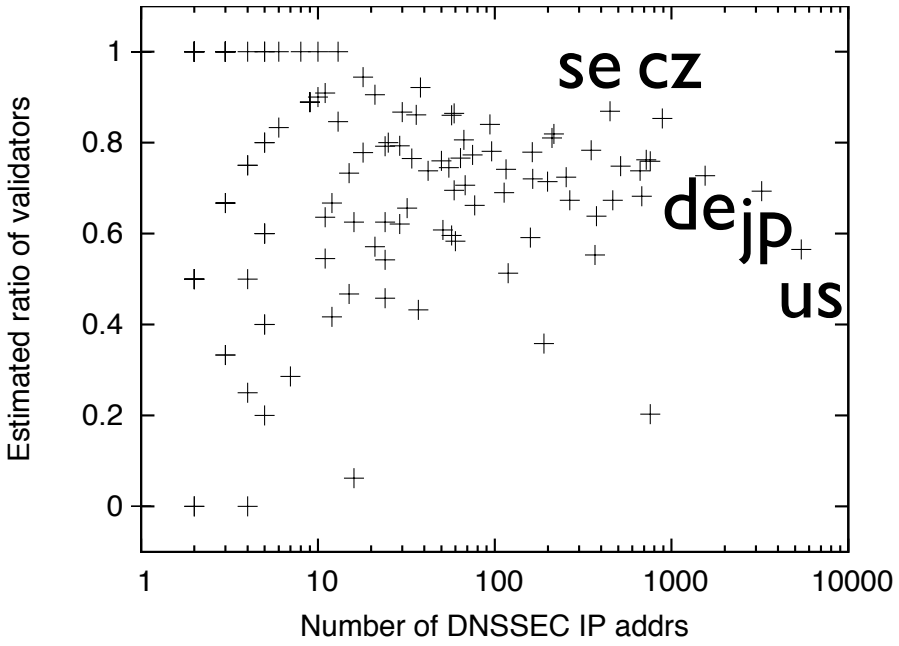
TABLE VI
NUMBER OF ESTIMATED VALIDATORS

(DS-DNSKEY & DS-only)	201106	201112	201204
DSR $>$ 0.04	5903 (70%)	9043 (76%)	13830 (73%)
DSR $\leq$ 0.04	2494 (30%)	2922 (24%)	5201(27%)
total	8397	11965	19031

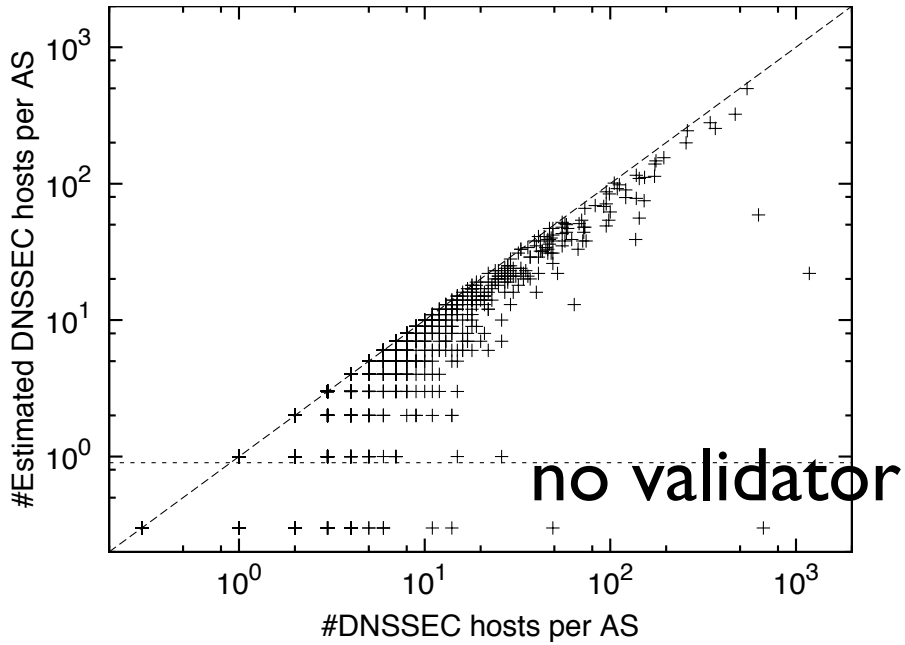
- DNSSECホストの約70%が検証を行うキャッシュリゾルバと推定
- DNSSECホストが属するASのうち15-20%には検証を行うキャッシュリゾルバはいなさそう

National Institute of Informatics

国別およびAS別推定リゾルバ数



国別



AS別

- 推定リゾルバが少ないASの一部はpublic DNS サーバを運用

National Institute of Informatics

結論

- パッシブ＆アクティブ計測によるDNSSECホストの解析
  - DNSSEC hosts数は増加傾向
  - ホストレベル:1.1%, ASレベル:10%
  - 正しいDSクエリは20%程度
  - DSと他のクエリの比によって検証を行うリゾルバを推定
    - ホストレベル: 30%, ASレベル:15-20%はエンドホストによる影響

National Institute of Informatics