Increase of probable DNSSEC Validators and DNSSEC side effect

Kazunori Fujiwara, JPRS
<fujiwara@jprs.co.jp>

July 28, 2013, IEPG meeting

Contents

- Increase of probable DNSSEC Validators
  - Idea: How to detect DNSSEC Validators
  - Datasets
  - Results
- DNSSEC side effect
  - Increase of DS queries
  - Reason of DS query increase
  - Possible situations in the future
  - Conclusion

Idea: How to detect validators

- Busy DNSSEC validators send following queries:
  - . (Root) DNSKEY (TTL=172800=2 days)
  - JP DNSKEY (TTL=86400=1 day)
    - If they interests JP domain names.
  - *.JP DS queries (TTL=86400/900)

- Number of DNSSEC validators are presumed by analyzing query data of root and/or JP TLD

Datasets

DNS-OARC Root Datasets

- "A Day in the Life of the Internet" (DITL) is a large-scale data collection project undertaken by CAIDA and DNS-OARC every year since 2006.
  - https://www.dns-oarc.net/ditl/2011/
  - 50 hours packet capture at root DNS servers and other DNS servers
  - Source IP addresses of i.root-servers.net data are anonymized

Year	Start(UTC)	End	Analyzed data from
2011	4/12 1100	4/14 1300	a,c,d,e,f,h,j,k,l,m (10/13)
2012	4/17 1100	4/19 1300	a,c,e,f,h,j,k,l,m (9/13)
2013	5/28 1100	5/30 1300	a,c,d,e,f,h,j,k,l,m (10/13)

JP datasets

- .JP has 1,340,433 registered domain names (on July 1, 2013)
- JP DNS servers serve 1.6 billion queries per day
- Two datasets
  - Packet captures of all JP DNS servers, around the same timing as DNS-OARC DITL event (and more)
  - Query logs of 2 (a and g) JP DNS servers, every day, for 9 years

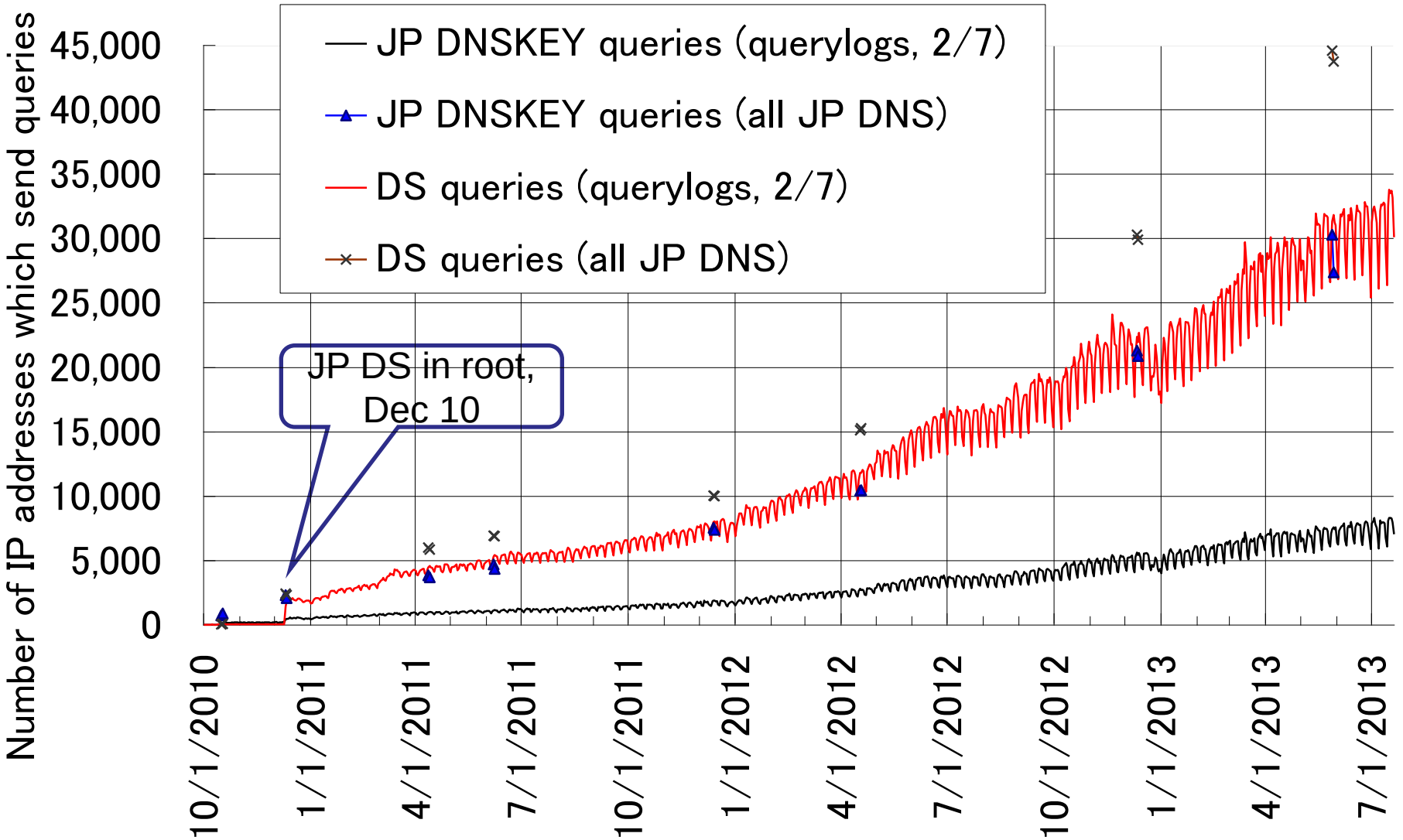
Name	Operator	Location	Address (IPv4:7, IPv6:6, total 13)	Capture
A.DNS.JP	JPRS	JP*2	203.119.1.1, 2001:dc4::1	Pcap/Log
B.DNS.JP	JPNIC	JP*1	202.12.30.131, 2001:dc2::1	Pcap
C.DNS.JP	JPRS	Worldwide	156.154.100.5, 2001:502:ad09::5	Pcap
D.DNS.JP	IIJ	JP*2, US*2	210.138.175.244, 2001:240::53	Pcap
E.DNS.JP	WIDE	JP*1,US*1, FR*1	192.50.43.53, 2001:200:c000::35	Pcap
F.DNS.JP	NII	JP*1	150.100.6.8, 2001:2f8:0:100::153	Pcap
G.DNS.JP	JPRS	JP*1	203.119.40.1	Pcap/Log

Counting number of validators

- Packet captures
  - Excluded RD=1 queries (validators shoud not send)
  - Counting the number of IP addresses within 24/48 hours
- Query logs
  - Excluded RD=1 queries (validators should not send)
  - Count number of IP addresses within 24 hours (JST)

Results

Result of JP (24 hours)



Results of JP (2)

- Folloing the numbers are almost the same:
  Number of source IP addresses which send
  - JP DNSKEY queries seen on all JP DNS servers
  - DS queries for A.DNS.JP and G.DNS.JP
- A weak presumption:
  - Busy validators send many DS queries
  - They must send DS queries to all JP DNS servers
  - 2 of 7 JP DNS servers receive sufficient DS queries
- The numbers of unique IP addresses which send JP DNSKEY and *.JP DS are still increasing
  - 4,000 / day (April 2011)
  - 10,000 / day (April 2012)
  - 30,000 / day (May 2013)

Result of Root (48 hours)

Year	Start (UTC) Day / Hour	Number of unique IP addresses which send				
		RD=0/1	RD=0	.DNSKEY	RD0/v6	RD0/v4
2011	4/12 1200	7,519,127	5,846,667	14,092	51,537	5,795,130
2012	4/17 1200	8,890,115	5,859,716	43,782	115,273	5,744,443
2013	5/28 1200	8,367,241	6,081,079	269,390	154,352	5,926,727

- DNSSEC validators should not send RD=1 queries
- 10 root servers received RD=0 queries from 6,081,079 unique IP addresses
- Number of unique IP addresses which send "." DNSKEY queries are increasing in recent three years (red)
  - An increase between 2012 and 2013 is remarkable
- IPv6 resolvers are also increasing (blue)

Compare Root and JP 48hour data

Year	Start (UTC) Day / Hour	Number of unique IP addresses which send			
		Root RD=0	. DNSKEY	*.JP query to Root	. DNSKEY and *.JP to Root
2011	4/12 1200	5,846,667	14,092	1,201,627	7,413
2012	4/17 1200	5,859,716	43,782	1,112,963	17,415
2013	5/28 1200	6,081,079	269,390	1,213,918	49,426

Year	Start (UTC) Day / Hour	JP RD0	JP DNSKEY
2011	4/12 1200	1,497,114	5,330
2012	4/17 1200	1,561,231	14,160
2013	5/28 1200	1,695,905	40,366

- JP DNS servers received queries from 1,695,905 addrs
- 10 of 13 root servers received "JP" queries from 1,213,918 addrs
- Rest (28.4%) of IP addresses may be observed by other root servers

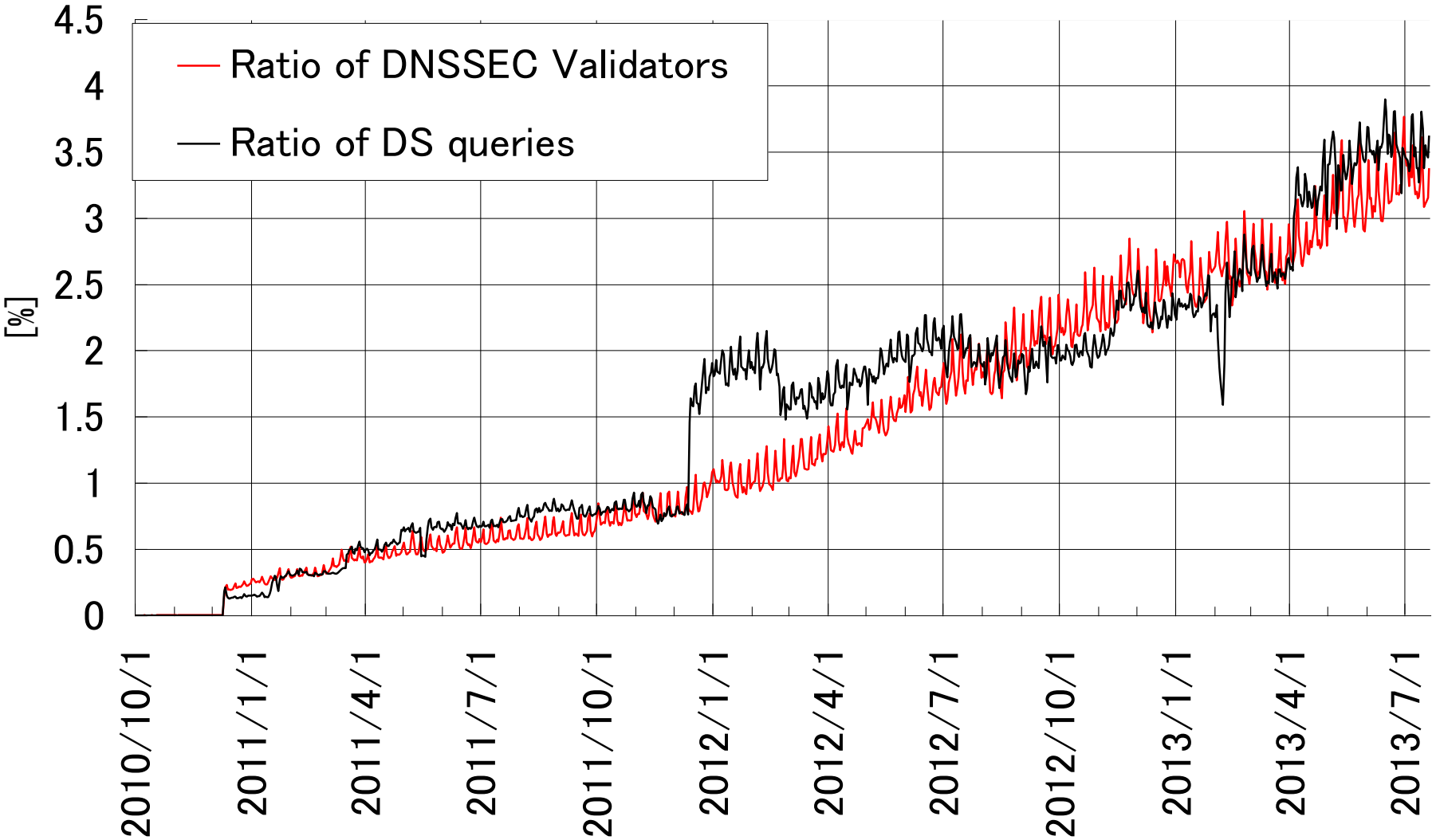
Result of our analysis

- We observed probable DNSSEC validators in May 2013
  - 269,390 at Root (48 hours)
  - 40,366 DNSSEC validators at JP
  - 19 times increased in recent two years (root)
  - Number of DNSSEC validators are still increasing

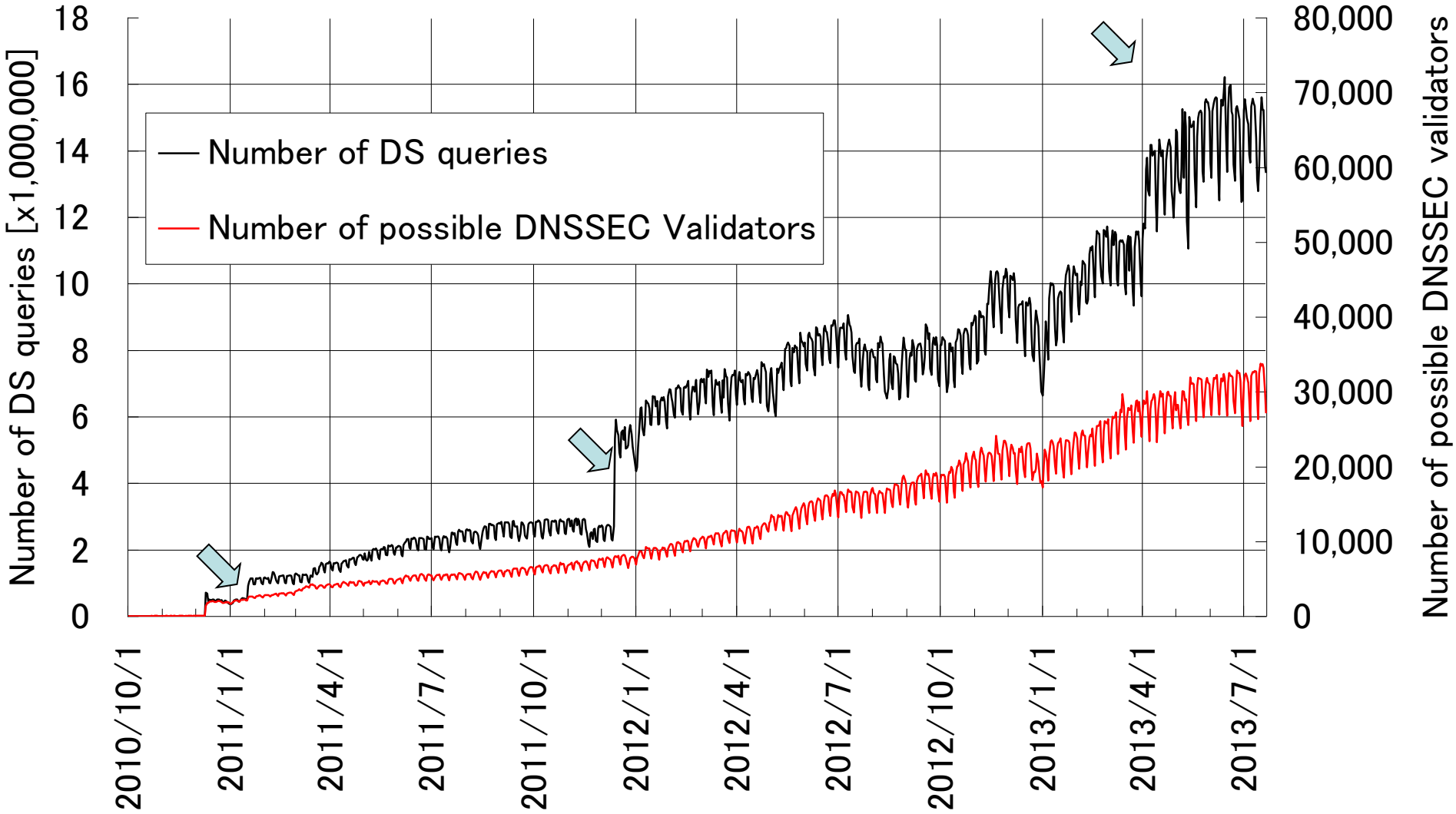
- The result shows real DNSSEC validators
- Or peoples' interest for DNSSEC
  - 'dig . DNSKEY'
  - Operators' test

DNSSEC side effect (seen on JP)

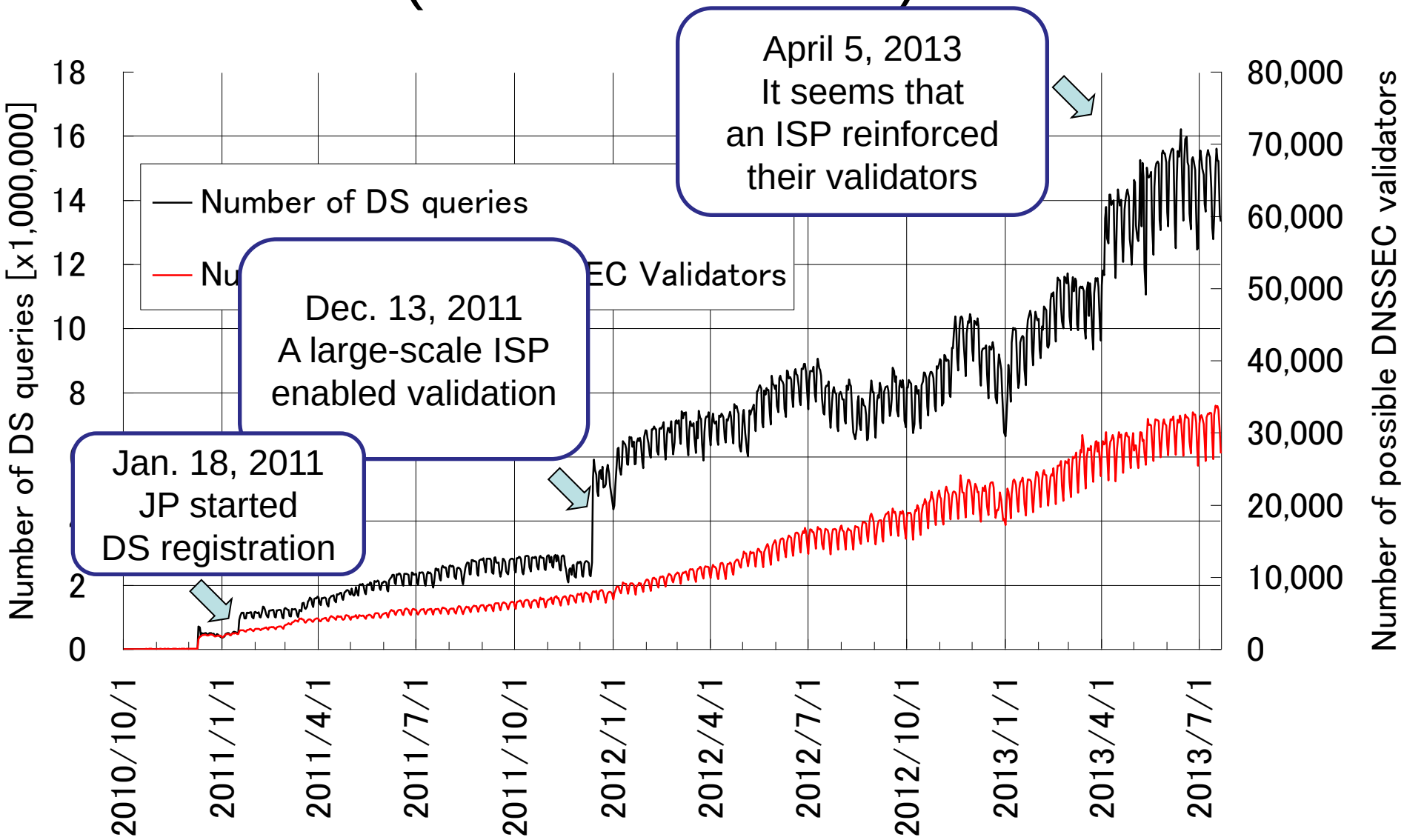
Ratio of DS queries seen at JP, 24 hours data



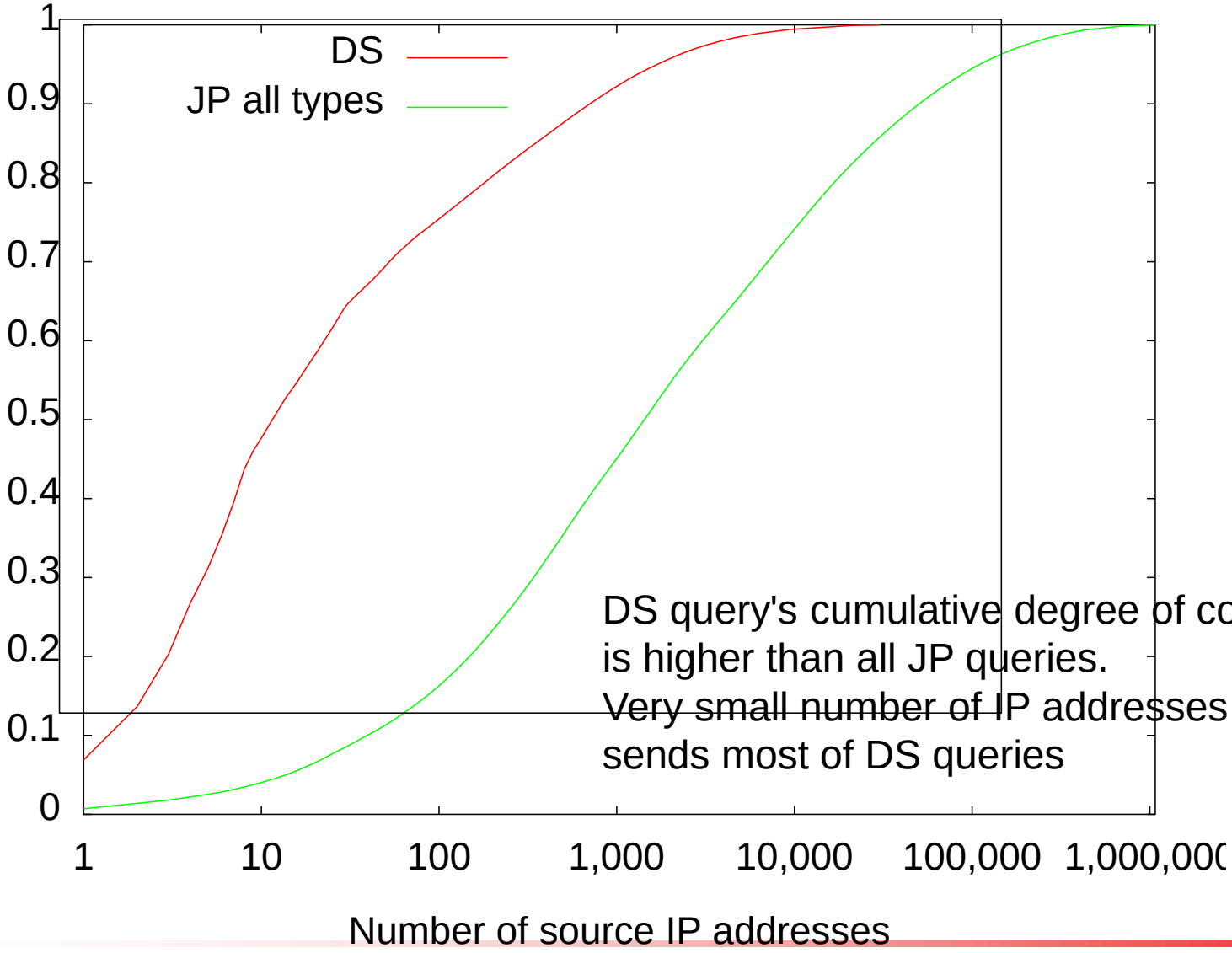
Number of DS queries
(2 of 7 JP servers)



Number of DS queries
(2 of 7 JP servers)



Cumulative distribution of query source IP addresses(2 of 7 JP DNS, Apr 30, 2013)



DS query's cumulative degree of concentration is higher than all JP queries.
Very small number of IP addresses sends most of DS queries

A part of query log for a popular name from one IP address, 2 of 7 JP servers

30-Apr-2013 00:19:00.126 google.co.jp IN DS
30-Apr-2013 00:49:00.093 google.co.jp IN DS
30-Apr-2013 01:34:00.369 google.co.jp IN DS
30-Apr-2013 01:49:00.242 google.co.jp IN DS
30-Apr-2013 02:19:01.047 google.co.jp IN DS
30-Apr-2013 02:28:35.867 id.google.co.jp IN AAAA
30-Apr-2013 02:34:01.736 google.co.jp IN DS
30-Apr-2013 03:19:05.265 google.co.jp IN DS
30-Apr-2013 03:34:06.405 google.co.jp IN DS
30-Apr-2013 03:49:08.541 google.co.jp IN DS
30-Apr-2013 04:34:09.628 google.co.jp IN DS
30-Apr-2013 05:04:09.216 google.co.jp IN DS
30-Apr-2013 05:19:09.723 google.co.jp IN DS

One IP address sends many same (google.co.jp) DS queries.

Minimal time interval is 15 minutes, it is the same as JP NCACHE TTL

Reason of DS queries increase

- JP NCACHE TTL is 900, RR TTL is 86400
- Most of JP domain names are not signed
  - DS nonexistence (NSEC3) is cached only 900 sec
- Assume there is a popular query name
  - 1 or more queries per NCACHE TTL period
  - Its RR TTL is smaller than NCACHE TTL
  - It is not signed

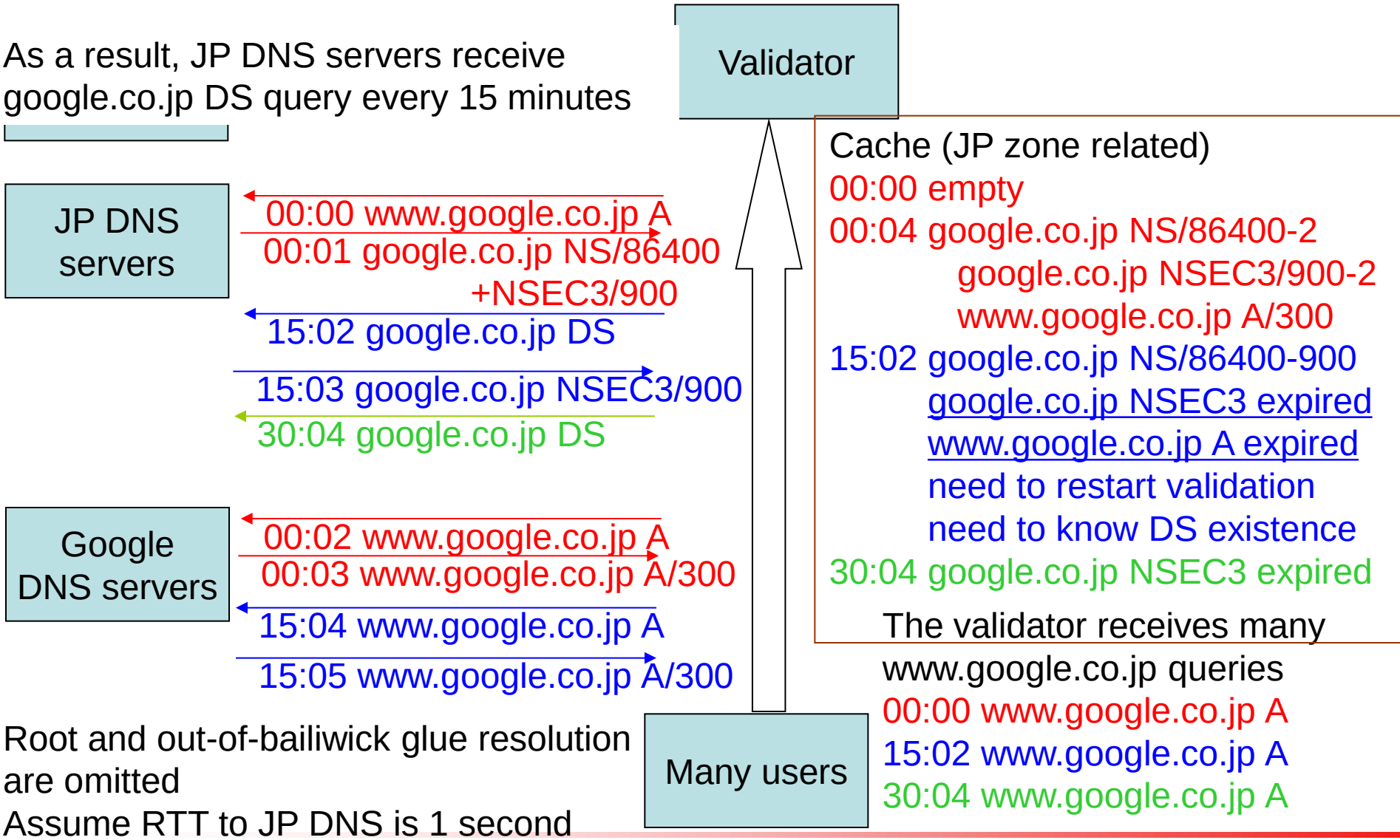
Reason of DS queries increase (2)

- Therefore,
  - Validating process starts for every NCACHE TTL period or more
  - The validator need to know DS nonexistence
- As a result, the validator sends
  - one non-DS query per a day
  - 95 (86400/900-1) DS queries per a day
  - It increases queries 96 times

- DNSSEC protocol and parameter issue

The "www.google.co.jp" case

As a result, JP DNS servers receive google.co.jp DS query every 15 minutes



Root and out-of-bailiwick glue resolution are omitted

Assume RTT to JP DNS is 1 second

Evaluation on existing implementations (BIND 9 and Unbound)

- Sending periodic queries to test validators
  - dig @validator QNAME A, every 5 minutes
  - Tested QNAMEs:
    - unsigned JP domain names
    - signed JP domain names (jprs.co.jp, jprs.jp)
    - unsigned com, net, org domain names
- Results
  - Both BIND 9 and Unbound validator send
  - DS queries of unsigned delegations to TLD DNS servers every 15 or 20 minutes
  - Depends on DS existence and RR TTL of qname/type
  - Other queries depend on their own TTL

Possible situations in the future

- When large-scale ISPs enable DNSSEC validation, their validators start sending periodic DS queries of popular and unsigned delegations
  - As you have seen before, this happened already
- Therefore, JP DNS servers would receive very large amount of DS queries in the future
  - Magnification factor is 96 (86400/900)
  - Pessimistically, queries to JP DNS servers would increase 96 times
  - And almost of them are DS

Possibly affected domains

- Delegation centric zones, signed, smaller NCACHE TTL
- gTLDs
  - Most of gTLDs use NCACHE TTL 900 and TTL 86400/172800
  - Magnification factors are 96 or 192
- Typical ccTLDs, root, RIRs (TTL / NCACHE)
  - jp: 86400 / 900 96 times
  - co.uk: 172800 / 10800 16 times
  - fr: 172800 / 5400 32 times
  - de: 86400 / 7200 12 times
  - cz: 18000 / 900 20 times
  - us: 7200 / 900 8 times
  - . 86400 / 86400 (10800) 8 times
  - 193.in-addr.arpa 172800 / 3600 48 times

- Causion: RFC 2308 recommends the maximum value in the negative cache with 1 hour to 3 hours.

Conclusion

- Number of DNSSEC validators are still increasing
- TLDs which use smaller NCACHE TTL value and are signed will receive many DS queries of unsigned delegations from DNSSEC validators
- We need to prepare this issue
  - Periodic checking of number/ratio of DS queries
  - Considering some countermeasures

Acknowledgements

- DNS-OARC as the data source of Root dataset