

Part 1: Analysis of BGP Update Data Characteristics and Part 2: Modeling and Estimation of RIB Size for Cert-Based Path Validation Approaches

Prepared by NIST BGP Security Team

(K. Sriram, P. Gleichmann, O. Borchert, O. Kim, A. Nakassis, D. Cooper, and D. Montgomery)

Shared with DHS S&T BGPSEC Team

May 29, 2009

Contacts: ksriram@nist.gov, doug@nist.gov

NIST project website: www.antd.nist.gov/bgp_security

This research was supported by the Department of Homeland Security under the Secure Protocols for the Routing Infrastructure (SPRI) program and the NIST Information Technology Laboratory Cyber and Network Security Program.

Outline

- BGP measurement data analysis
 - # announced prefixes per update
 - # withdrawn prefixes per update
 - # ASes in AS path
 - Size of all path attributes in an update
 - Update size
- Path validation approaches
- Assumptions for RIB size modeling
- RIB size estimates for path validation approaches
 - Sensitivity to key parameters

Summary of Findings

- Extensive analysis of BGP update message characteristics
- Four candidate path validation approaches studied and compared:
 - **SPP**: Signature Per Prefix; no Explicit Path Attribute (EPA)
 - **SPP-E**: SPP with Economization
 - Attestation overhead shared over all prefixes in an update
 - **SPP-E-SAS**: SPP-E with Sequential Aggregate Signatures (SAS)
 - SAS described later
 - Attestation size is invariant to # ASes the update goes through
 - **SPU-EPA**: Signature Per Update with EPA
 - Signature coverage includes announced prefixes and AS path
 - EPAs convey changes made to announced prefix set along the AS path (Issues: **Will ISPs buy in? Prefix re-insertion?**)
 - This approach is closest to S-BGP
- RIB size varies widely; SPU-EPA has the lowest RIB size (among the four)
- SAS benefits the RIB size and can be used with SPU-EPA as well; its details and trade-offs need further study

Note: SPP is in accordance with Email from Randy Bush to bgpsec list 4/27/09

-- Draft for Comments --

Part 1: Analysis of BGP Update Data Characteristics

Summary Data for Updates w.r.t. Prefix Announcements and Withdrawals

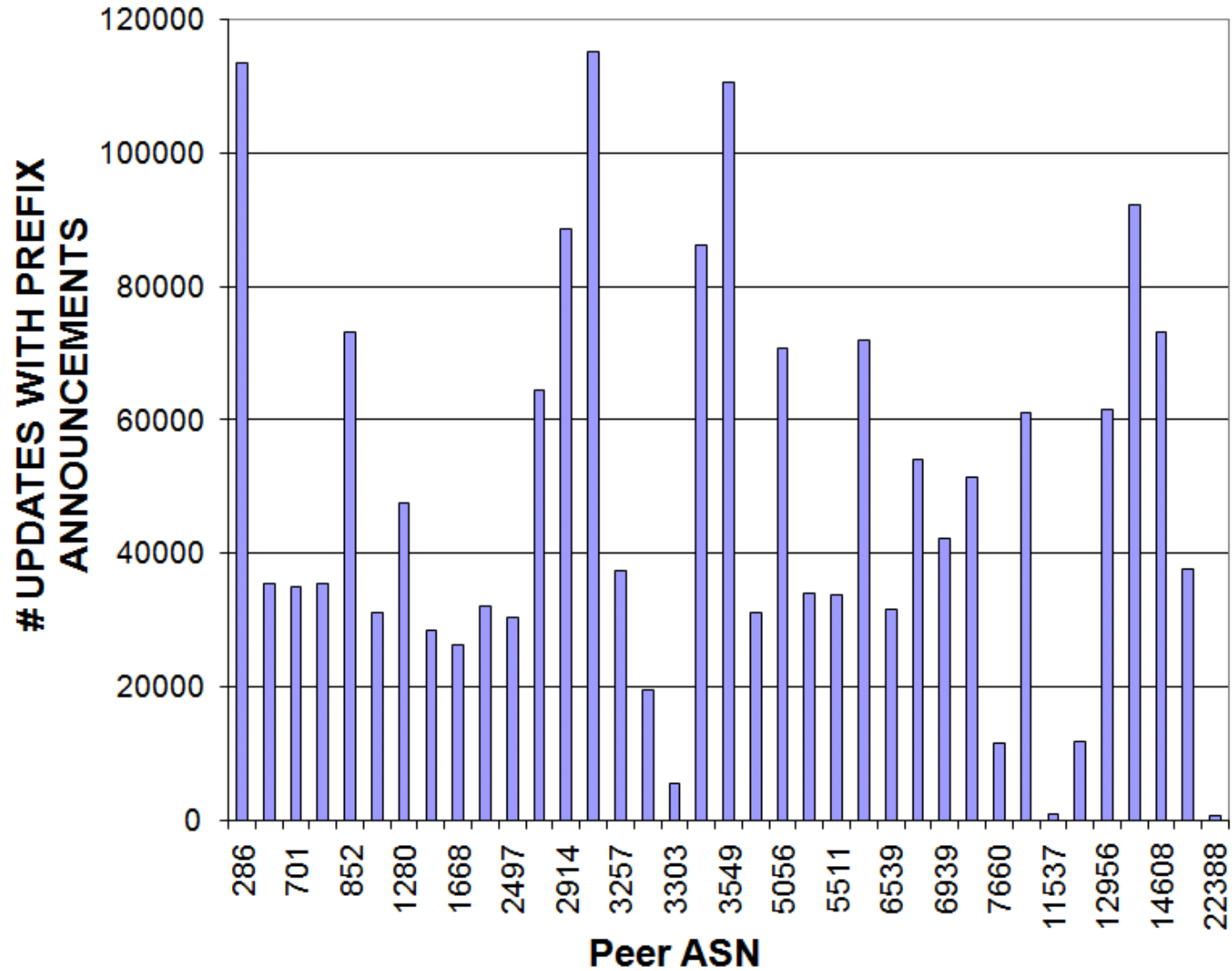
| | | |
|---|---------------------|------------|
| Measurement Data Source: | Routeviews - Oregon | |
| Measurement Dates / Duration: | Feb. 1-26, 2009 | |
| | | |
| | # updates | Percentage |
| Total # updates | 1847200 | |
| Updates with prefix announcements only | 1783668 | 96.56% |
| Updates with withdrawn prefixes only | 58554 | 3.17% |
| Updates with both prefix announcements and withdrawn prefixes | 4978 | 0.27% |

| | |
|-----------------------------------|------|
| Updates with prefix announcements | |
| Avg. # prefixes | 3.83 |
| Std Dev. of # prefixes | 4.19 |
| Min # prefixes | 1 |
| Max # prefixes | 1026 |

| | |
|---------------------------------|------|
| Updates with prefix withdrawals | |
| Avg. # prefixes | 4.76 |
| Std Dev. of # prefixes | 4.50 |
| Min # prefixes | 1 |
| Max # prefixes | 1030 |

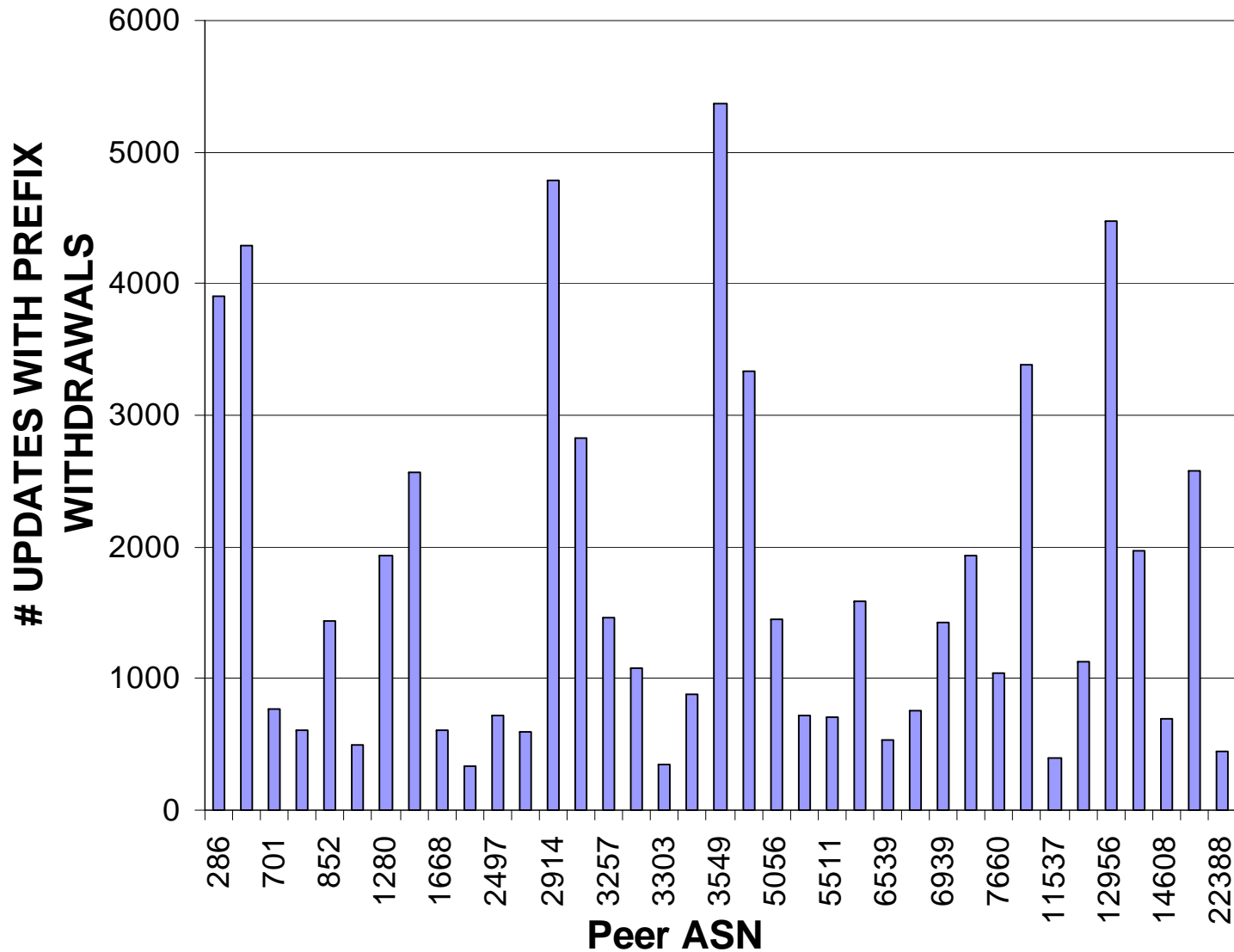
- One update file (15 min) was picked per day from Feb. 1st to Feb. 26th, 2009 from Routeviews – Oregon collector.

Distribution of # Updates w/ Announcements vs. Peer ASN



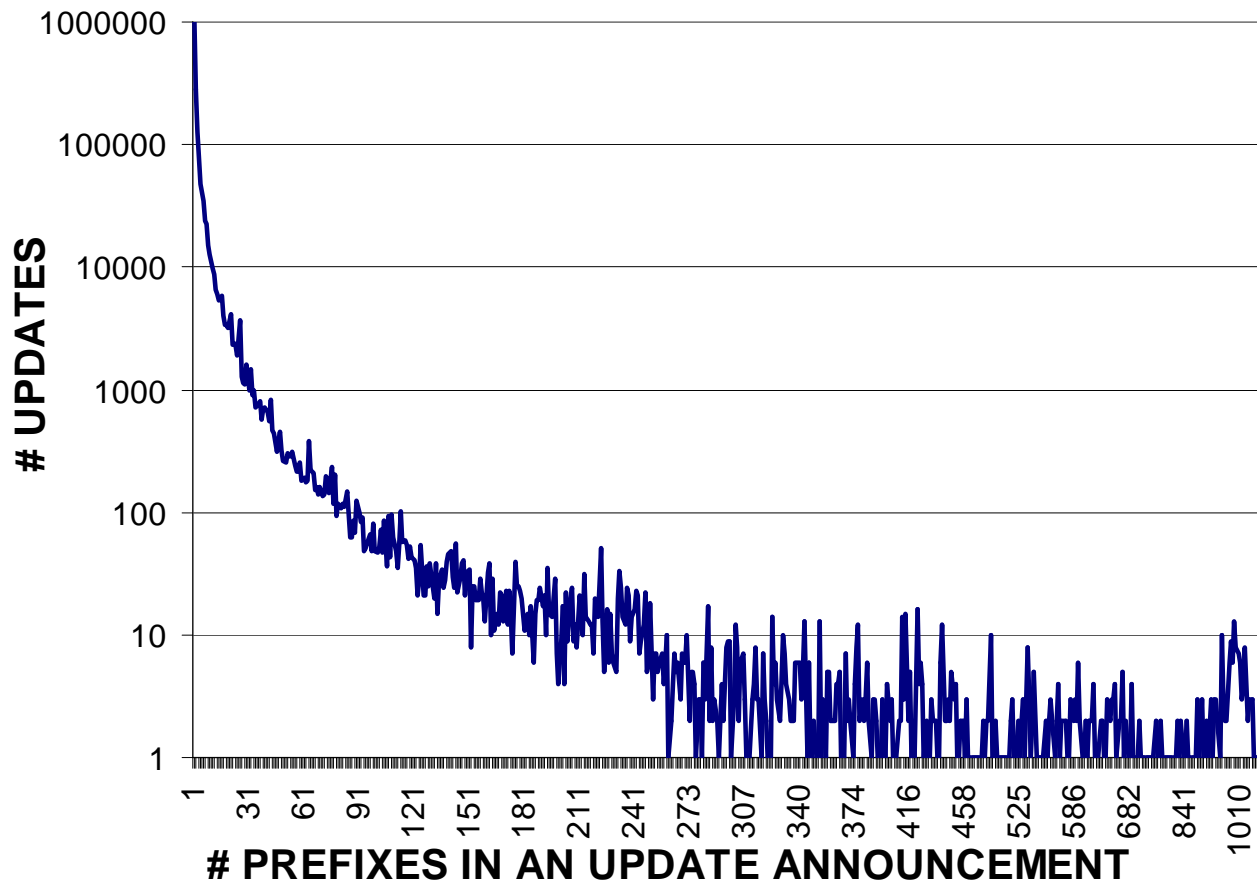
-- Draft for Comments --

Distribution of # Updates w/ Withdrawals vs. Peer ASN



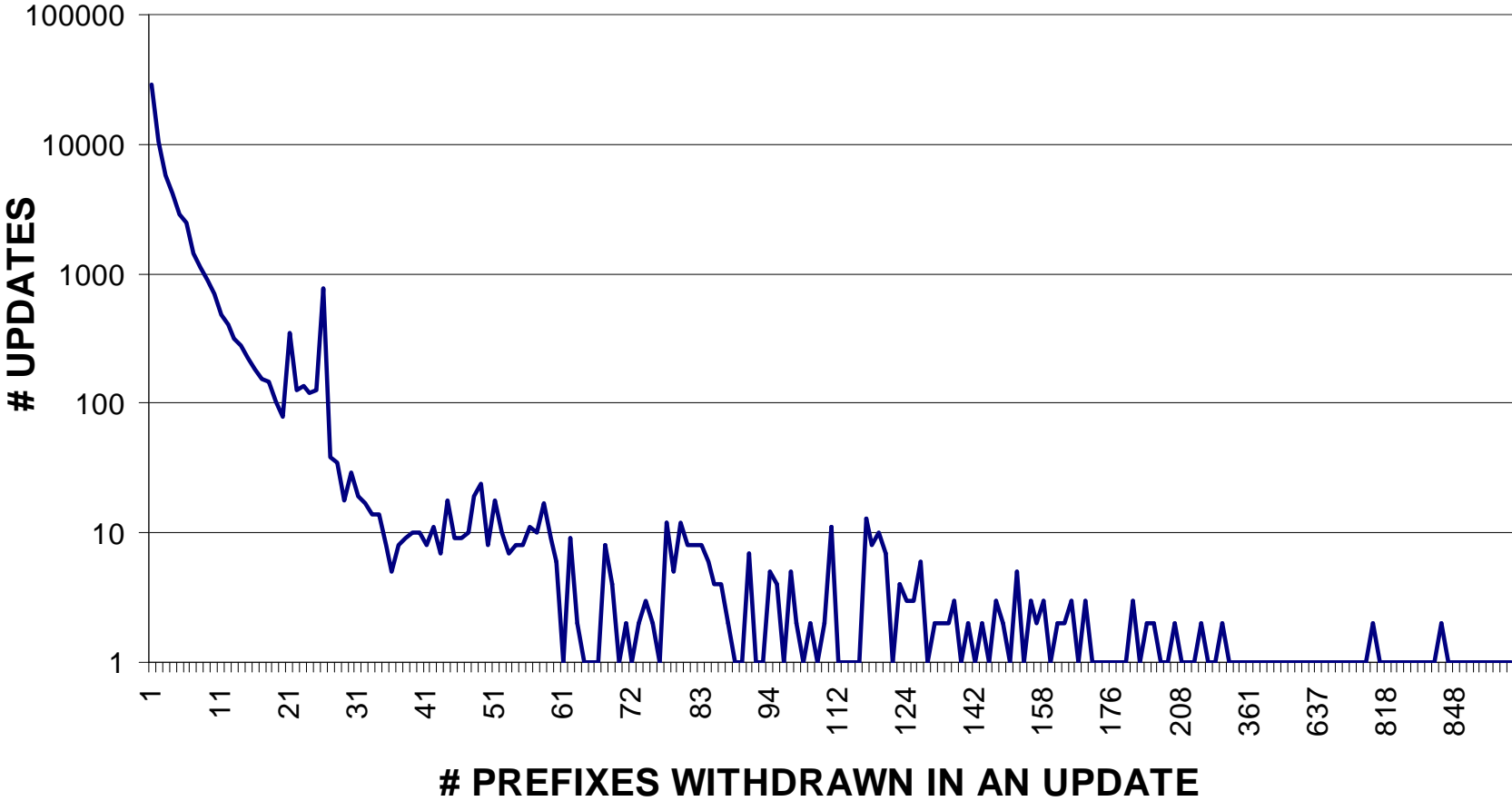
-- Draft for Comments --

Distribution of # Prefixes in Announcements

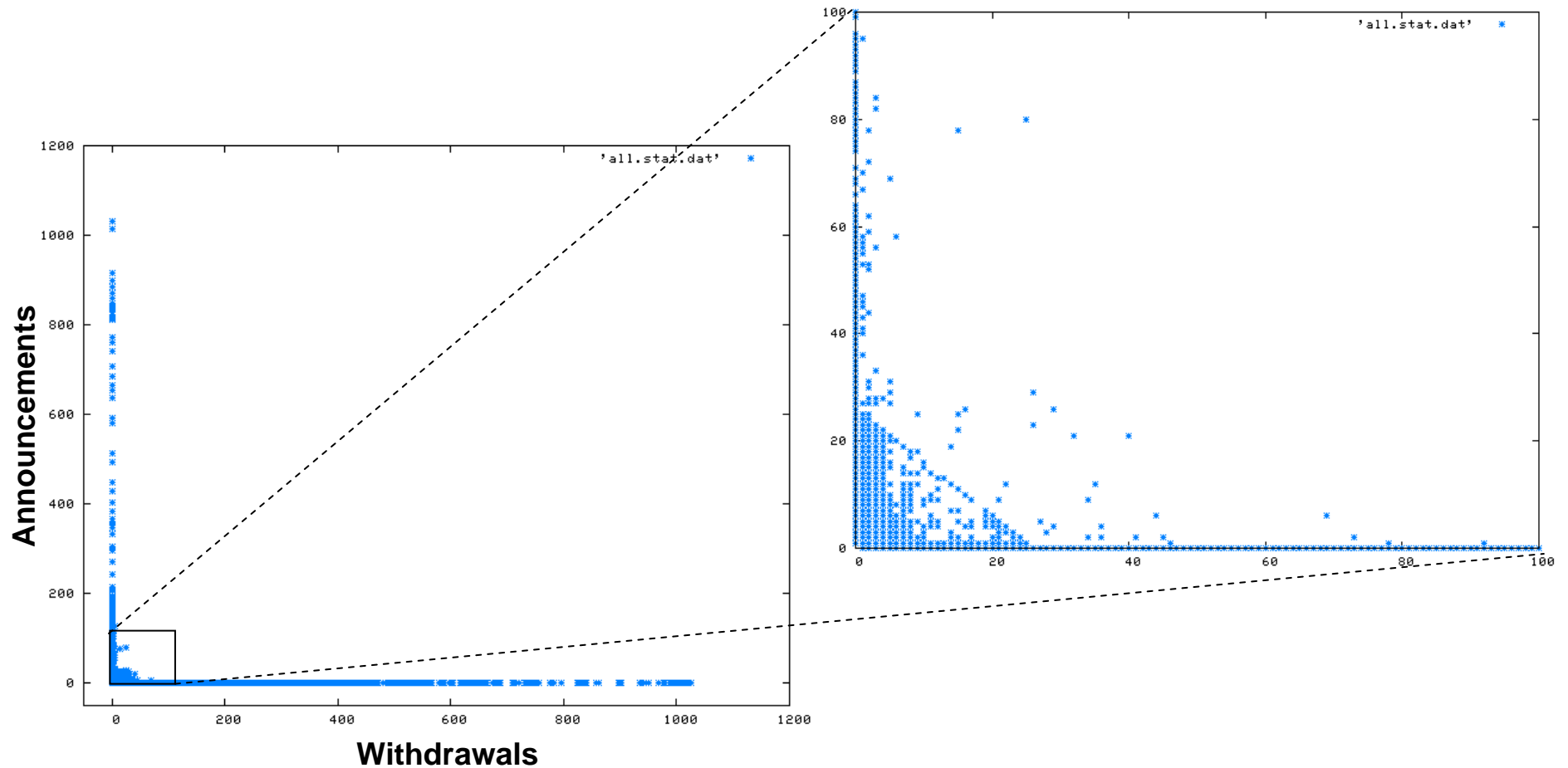


- Prob. {# Prefixes \leq 100} = 99.73%

Distribution of # Prefixes in Withdrawals



Scatter Plot of # Announced Prefixes vs. # Withdrawn Prefixes per Update



Chances of A Prefix Set Remaining Unchanged Upon Forwarding

| | | | Percentage |
|-----|---|---------|------------|
| (A) | Total # update announcements | 1787337 | |
| (B) | # update announcements that were forwarded (one new AS added) | 499386 | 100% |
| | Of the number in (B), # updates with unchaged prefix set after forwarding | 410196 | 82% |
| | Of the number in (B), # updates with chaged prefix set after forwarding | 89190 | 18% |
| | # updates for which we could not exactly trace the forwarding = (A) - (B) | 1287951 | |

- This of interest because: When the prefix set changes from one hop to the next hop as the update moves forward, Explicit Path Attribute (EPA) would be required in an S-BGP like scheme

Summary of AS Path Length Statistics

| | |
|-------------------------------|---------------------|
| Measurement Data Source: | Routeviews - Oregon |
| Measurement Dates / Duration: | Feb. 1-26, 2009 |

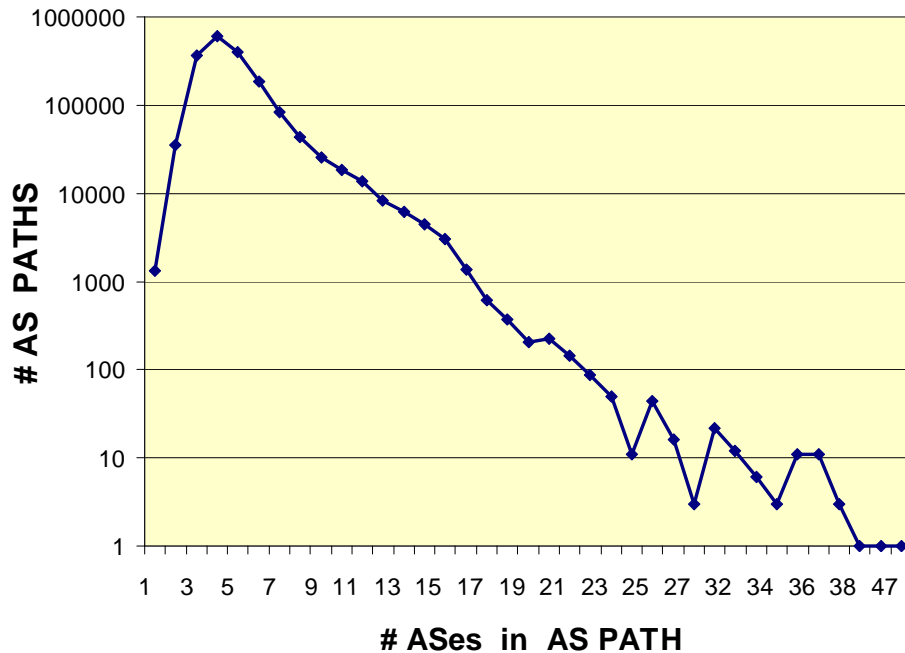
| | | After collapsing prepended ASes |
|---------------------------------|---------|------------------------------------|
| Total # updates | 1847200 | |
| # Updates with AS path | 1788646 | |
| # Unique AS paths | 931245 | 891887 |
| # Unique AS pairs | 72174 | 63544 |
| Average # ASes per AS path | 4.74 | 4.17 |
| Std. Dev. # ASes per AS path | 1.92 | 1.05 |
| Minimum # ASes per AS path | 1 | 1 |
| Maximum # ASes per AS path | 47 | 13 |
| # AS paths with prependded ASes | 366018 | |

AS Prepending and AS Path Poisoning

| | | Percentage |
|--|---------|------------|
| Total # updates | 1847200 | |
| # Updates with AS path | 1788646 | 96.83% |
| # Updates with prependded ASes | 359,386 | 19.46% |
| # Updates with loop in AS path -- loop(s) with 1 AS in between | 19708 | 1.07% |
| # Updates with loop in AS path -- loop(s) with 2 ASes in between | 42 | 2.27E-05 |

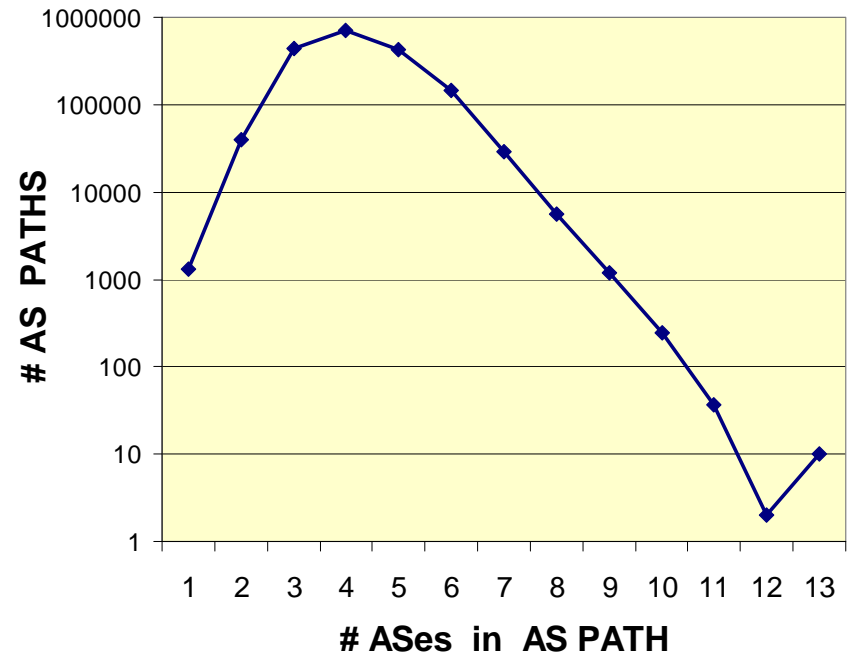
Distribution of AS Path Length

Prepended/Repeat ASes Not Collapsed



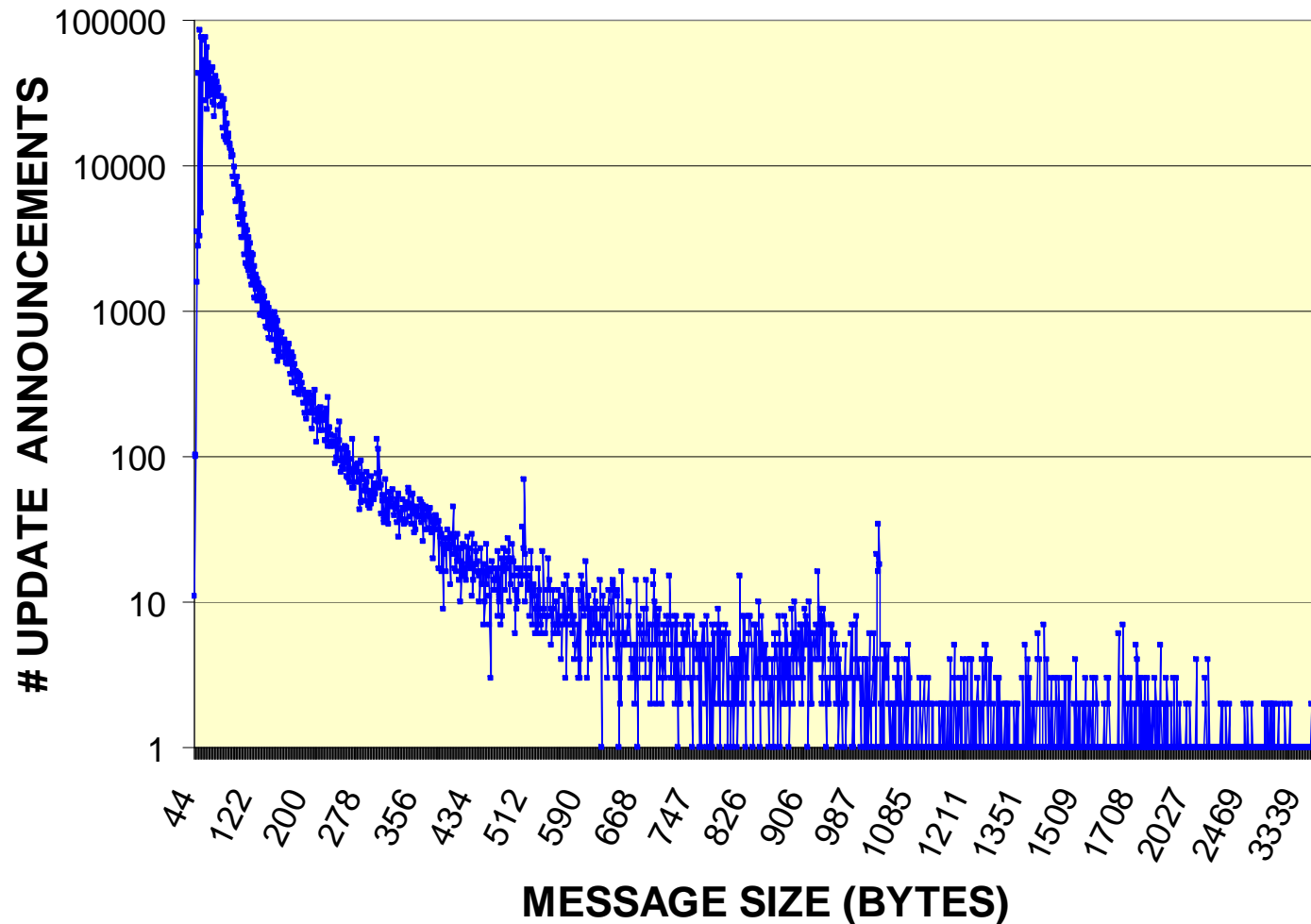
- Prob. {AS Path Length ≤ 10 } = 97.82 %
- Prob. {AS Path Length < 12 } = 99.06 %

Prepended/Repeat ASes Collapsed



- Prob. {AS Path Length ≤ 6 } = 97.98 %
- Prob. {AS Path Length ≤ 7 } = 99.6 %

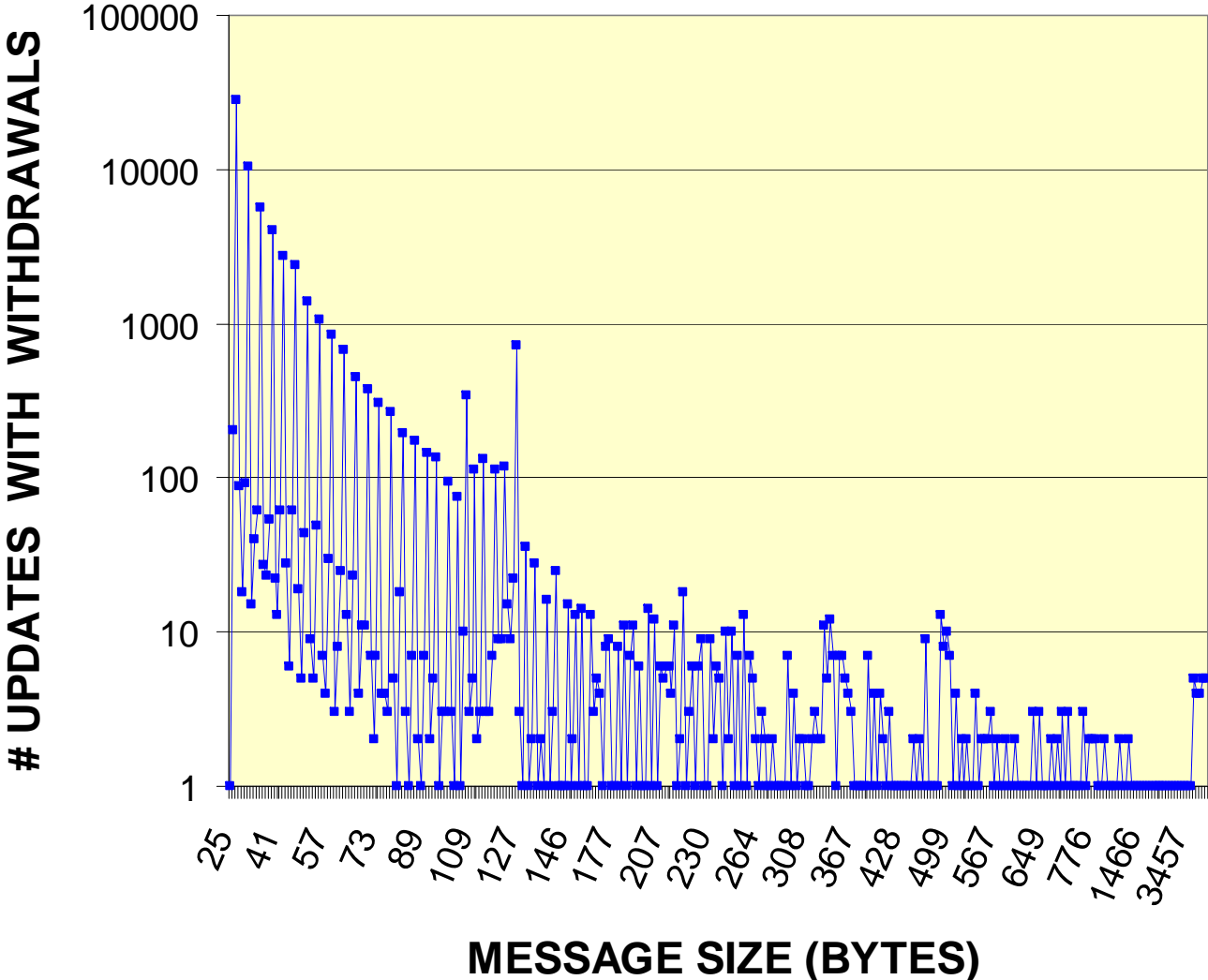
Distribution of Size of Updates with Announcements



- Updates with announcements (including those containing announcements and withdrawals)

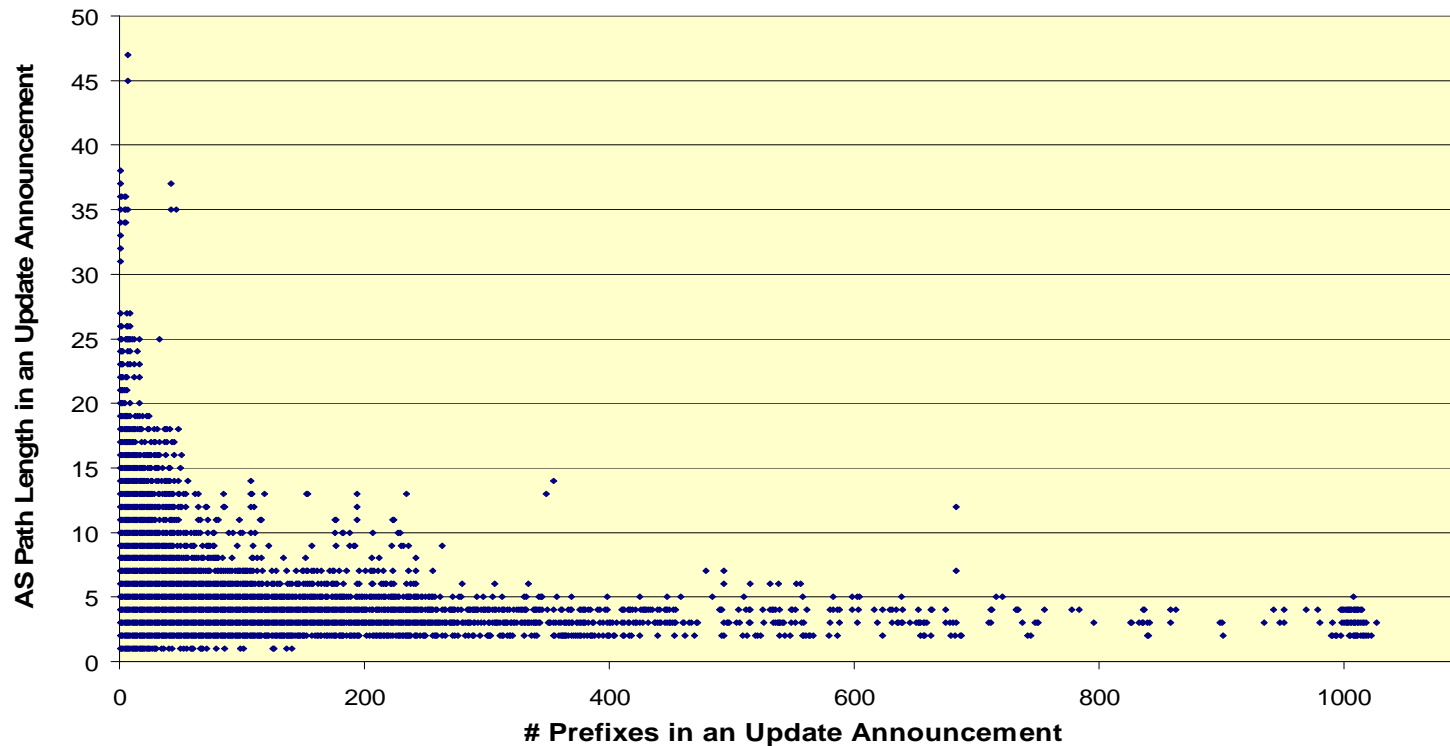
-- Draft for Comments --

Distribution of Size of Updates with Withdrawals



- Updates with withdrawals only

Scatter Plot of AS Path Length vs. # Prefixes per Update (in Updates with Announcements)



- Prob. $\{\# \text{ Prefixes} \leq 100\} = 99.73\%$
- Prob. $\{\text{AS Path Length} \leq 10\} = 97.82 \%$; Prob. $\{\text{AS Path Length} \leq 12\} = 99.06 \%$
- Prob. $\{\# \text{ Prefixes} * \text{AS Path Length} \leq 500\} = 99.81\%$
- Avg. $[\# \text{ Prefixes} * \text{AS Path Length}] = 18.17$ (per update)
(Note: all of the above with preponds not collapsed)
- When $\# \text{ ASes}$ and $\# \text{ prefixes}$ announced in an update are both high then the overhead due to signatures will be correspondingly large for that update

Part 2:

Modeling and Estimation of RIB Size for Cert-Based Path Validation Approaches

Whole Path Validation Approaches

(some candidate options)

- **SPP**: Signature Per Prefix
 - No need for Explicit Path Attribute (EPA)
 - Attestation overhead multiplicative with # prefixes in an update
- **SPP-E**: SPP with Economization
 - Attestation overhead shared over all prefixes in an update
- **SPP-E-SAS**: SPP-E with Sequential Aggregate Signature (SAS)
 - SAS – to be described shortly
 - Attestation size is invariant to # ASes the update goes through
- **SPU-EPA**: Signature Per Update with EPA
 - Signature coverage includes announced prefixes and AS path
 - EPAs convey changes made to announced prefix set along the AS path
 - This approach is closest to S-BGP
 - Possible concerns:
 - ISP may be concerned about revealing (in the EPA) about the prefixes they decided not to forward
 - Prefix re-insertion by upstream ASes based on information in the EPAs

Note: SPP is in accordance with Email from Randy Bush to bgpsec list 4/27/09

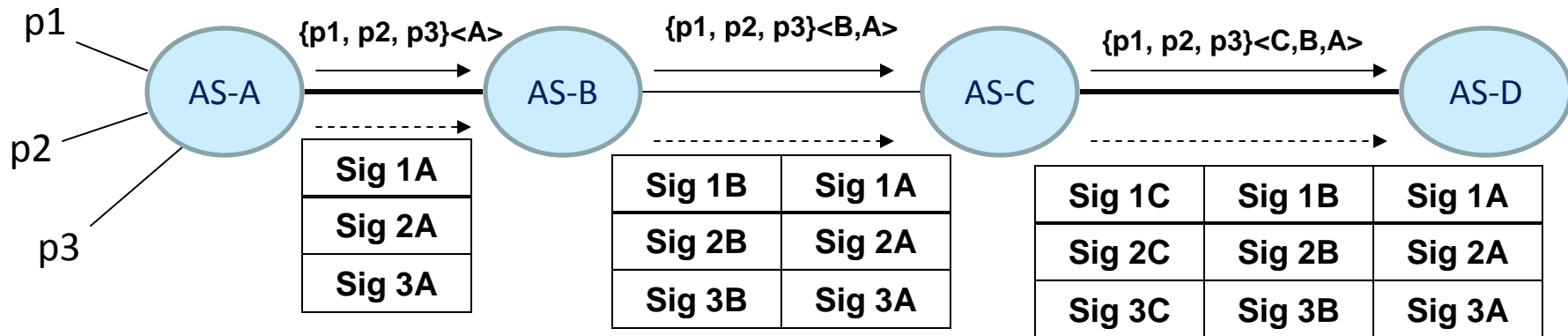
Path Validation with Signature Per Prefix (SPP)

- Origin AS provides one signature per prefix and the signature covers the prefix and the AS path (including all attributes)
- As many signatures in an update as there are prefixes
- ASes upstream add their signatures also on a per prefix basis covering individual prefixes together with the modified AS path
- AS path predictability works in this case; so there is no need for ExplicitPAs
- # signatures = # prefixes in update * # ASes in AS path

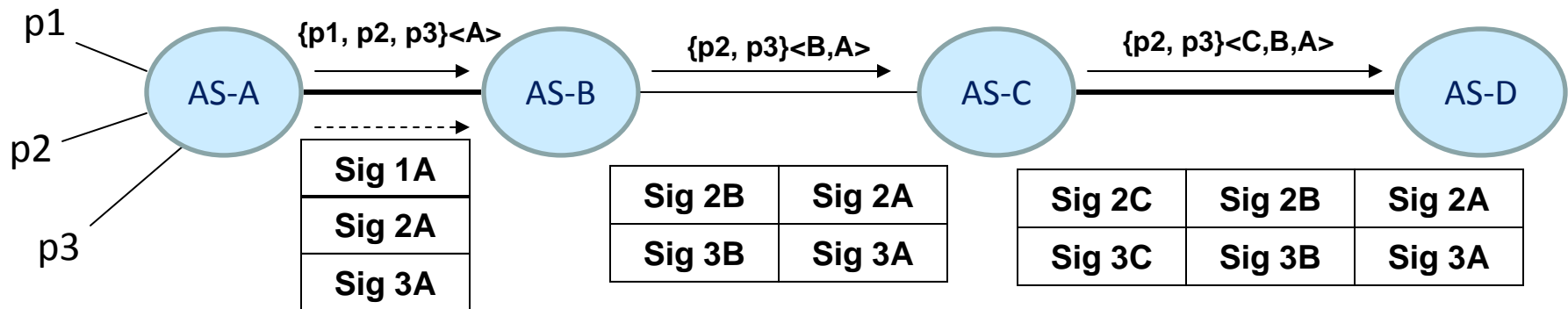
Note: In accordance with Email from Randy Bush to bgpsec list 4/27/09

Path Validation with One Signature per Prefix

Normal case (Example 1): All prefixed are carried through



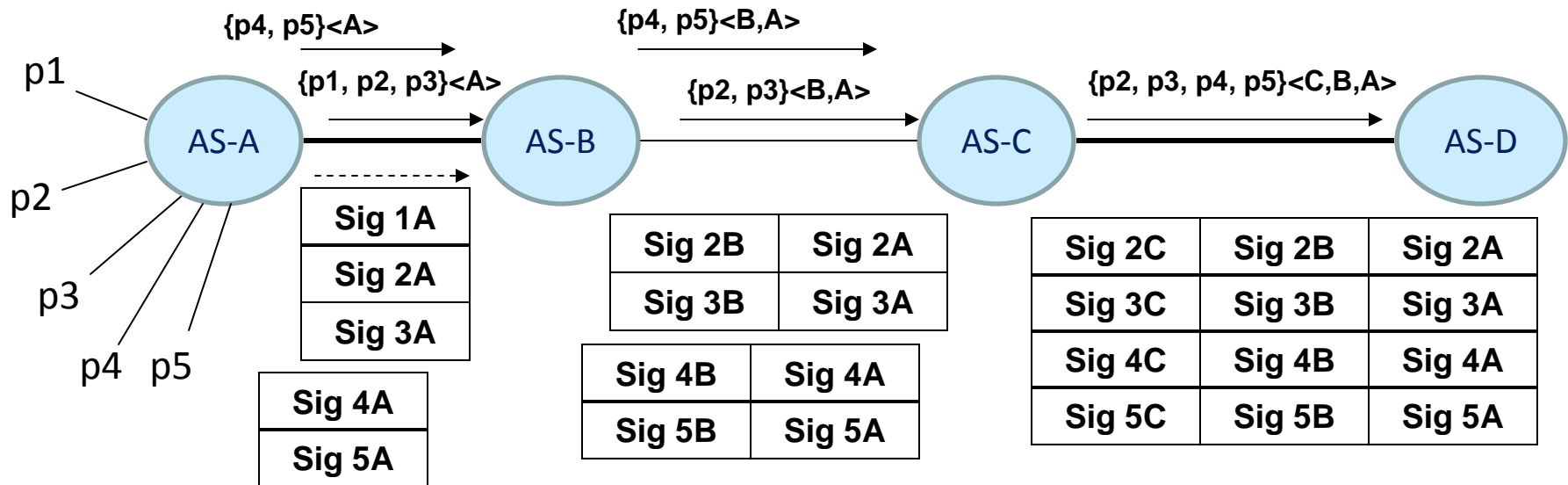
Special case (Example 2): Possibility of dropped prefixes



- # signatures = # prefixes in update * # ASes in AS path

Path Validation with One Signature per Prefix

Special cases (Example 3): Prefixes may be dropped or added



- # signatures = # prefixes in update * # ASes in AS path

Path Validation with One Signature per Prefix: Signature Sizes for SPP and SPP-E

One signature per prefix without overhead economization (SPP)

| Signature component | Size | Units |
|-----------------------|------|-------|
| Attestation object | 8 | B |
| Signer | 8 | B |
| Signature description | 7 | B |
| (1) Signature - 1 | 40 | B |
| Expiry | 8 | B |
| Target | 8 | B |
| Signature size | 79 | B |

⋮

| Signature component | Size | Units |
|-----------------------|------|-------|
| Attestation object | 8 | B |
| Signer | 8 | B |
| Signature description | 7 | B |
| (p) Signature - p | 40 | B |
| Expiry | 8 | B |
| Target | 8 | B |
| Signature size | 79 | B |

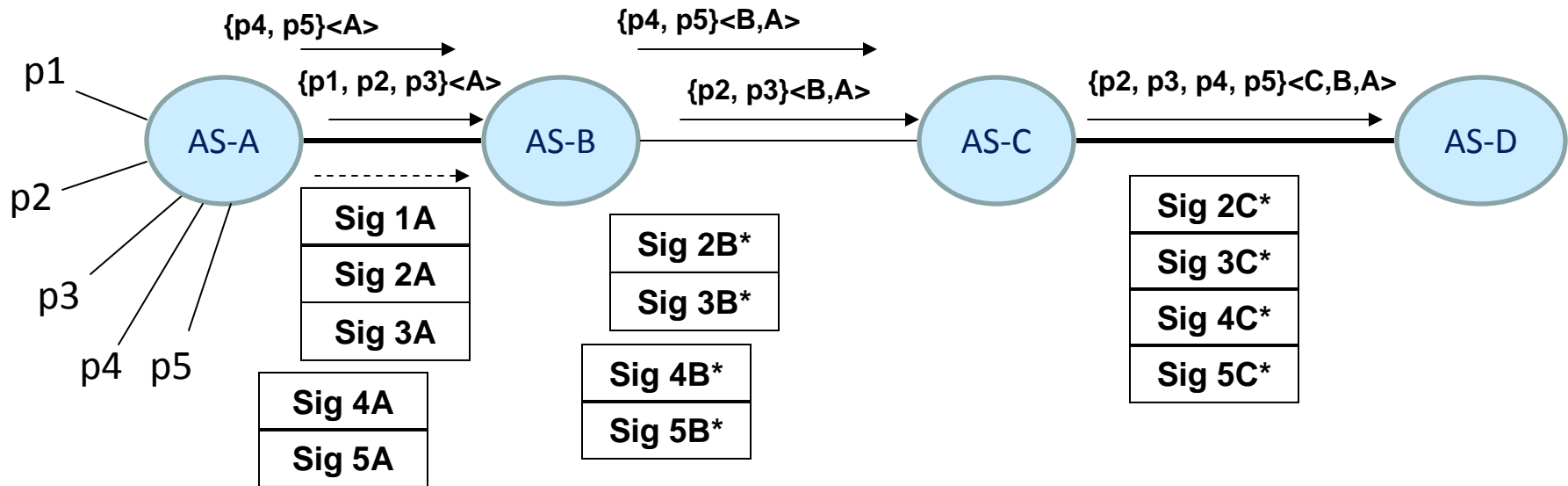
Set of p such signatures added at each AS along the path

One signature per prefix with shared attestation overhead in each update (SPP-E)

| Signature component | Size | Units |
|-----------------------|-------------|-------|
| Attestation object | 8 | B |
| Signer | 8 | B |
| Signature description | 7 | B |
| Number of Signatures | 2 | B |
| (1) Signature - 1 | 40 | B |
| ⋮ | | |
| Signature - 2 | | |
| ⋮ | | |
| | | |
| (p) Signature - p | 40 | B |
| Expiry | 8 | B |
| Target | 8 | B |
| Total signature size | $40*n + 41$ | B |

One such extended signature added at each AS along the path

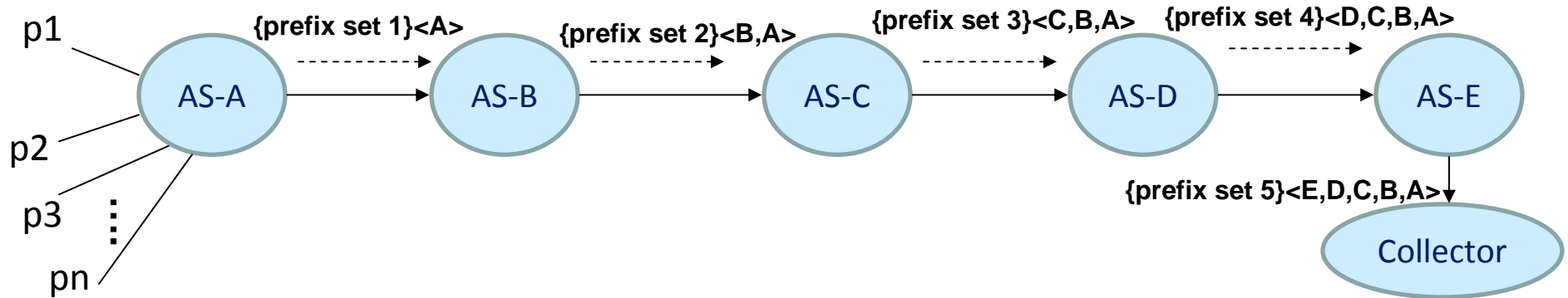
Path Validation with SPP-E and Sequential Aggregate Signature (SPP-E-SAS)



- In SAS [1], each AS (other than the origin AS) in the path incorporates into its signature the signature from previous AS in a retractable way
- Hence, # signatures carried in an update becomes independent of # ASes in AS path
- SAS can be applied to any of the proposals we consider here
- An overview of SAS is provided at the end (Appendix A)

[1] Y. Mu, W. Susilo, and H. Zhu, "Compact sequential aggregate signatures," Proceedings of the ACM Symposium on Applied Computing (2007), pp. 249-253.

Estimation of Update Size with Attestation: SPP, SPP-E, SPP-E-SAS



Size estimation of update with attestations received at the Collector:

U = Update message size without attestations (bytes)

U_a = Update message size with attestations (bytes)

p = # prefixes in a prefix set (per update message; $p \geq 1$)

h = # ASes in an AS path

Sig = Signature size (e.g., 40 bytes for DSS; 128 bytes for RSA)

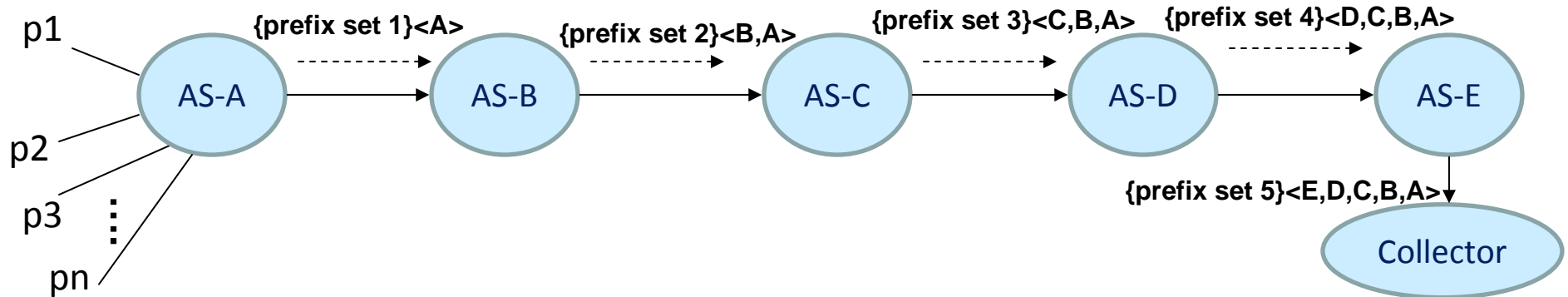
Aoh = Attestation overhead (attestation object, signer, sig description, expiry, target) = 39 bytes

k = path attribute overhead = 3 or 4 bytes (function of attribute size)

m = bytes required to specify # of signatures = 2 bytes (in SPP-E and SPP-E-SAS)

Contd. next page ...

Estimation of Update Size with Attestation: SPP, SPP-E, SPP-E-SAS



Size estimation of update with attestations received at the Collector:

For SPP:

Total size of signatures = $p \cdot h \cdot (\text{Sig} + \text{Aoh} + k)$ bytes

$U_a = U + p \cdot h \cdot (\text{Sig} + \text{Aoh} + k)$ bytes

For SPP-E:

Total size of signatures = $(p \cdot \text{Sig} + \text{Aoh} + k + m) \cdot h$ bytes

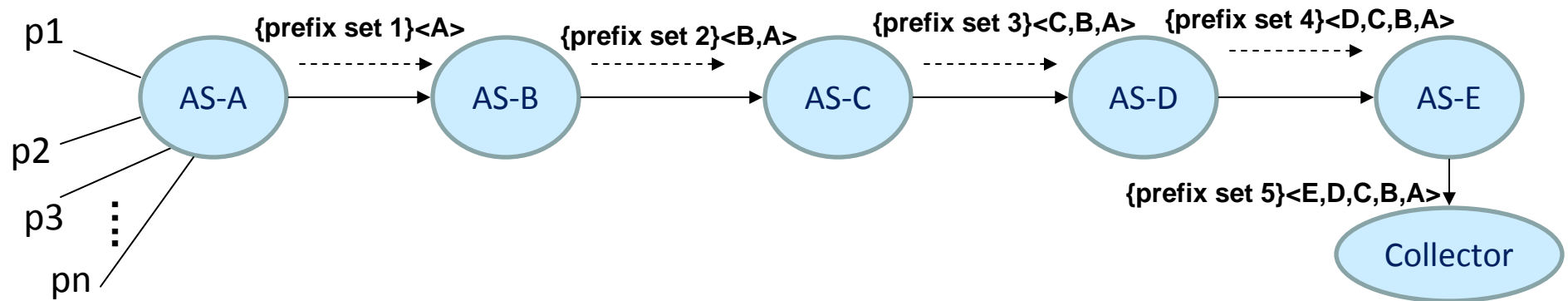
$U_a = U + (p \cdot \text{Sig} + \text{Aoh} + k + m) \cdot h$ bytes

For SPP-E-SAS:

Total size of signatures = $p \cdot \text{Sig} + h \cdot (\text{Aoh} + k)$ bytes

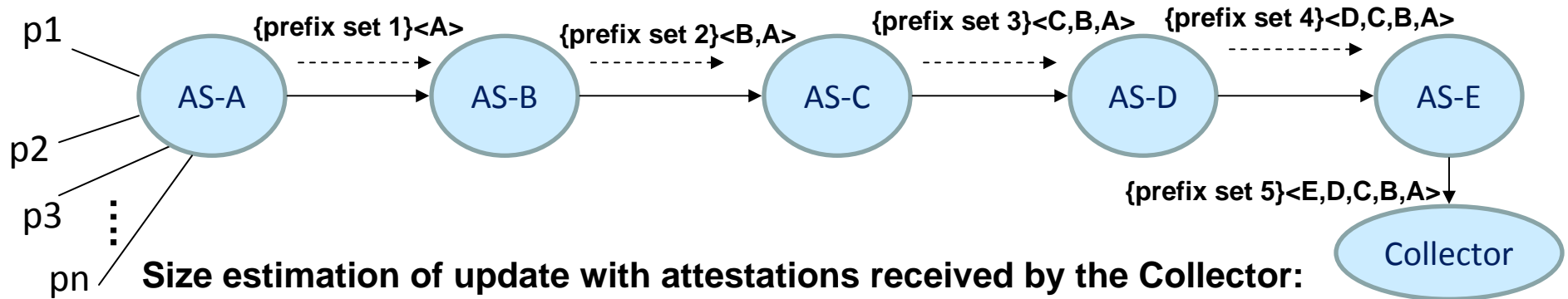
$U_a = U + p \cdot \text{Sig} + h \cdot (\text{Aoh} + k)$ bytes

Path Validation Using Signature Per Update and Explicit Path Attributes (SPU-EPA)



- Signature provides coverage over prefixes and AS path
- Assume each AS along the path drops some prefixes and thereby makes a change to the prefix set it includes in its repacked update
- So each AS along the path has to add an ExplicitPA to the signed update it sends to its next hop neighbor AS
- Assume dropping prefixes is allowed but adding them is not allowed (in S-BGP)
- This is a conservative approach – because we are not assuming perfect predictability, which happens if the prefix set were not changing along the path – there would have been no need to add ExplicitPA if only this predictability were true

Estimation of Update Size with Attestation: SPU-EPA



U = Update message size without attestations (bytes)

U_a = Update message size with attestations (bytes)

p = # prefixes in a prefix set (per update message)

A = Bytes needed to represent an ASN = 4 bytes

L = Size of a prefix representation (up to 4 bytes for quad + 1 byte for mask + 1 byte to specify length)

h = # ASes in an AS path

Sig = Signature size = 40 bytes

Aoh = Attestation overhead (attestation object, signer, sig description, expiry, target) = 39 bytes

k = path attribute overhead = 3 or 4 bytes (function of attribute size)

Total size of ExplicitPAs = $E_{pa} = (h-1)*p*L$ bytes

$U_a = U + h*(Sig + Aoh) + E_{pa} = U + h*(Sig + Aoh + k) + (h-1)*p*L$ bytes

RIB Size Modeling

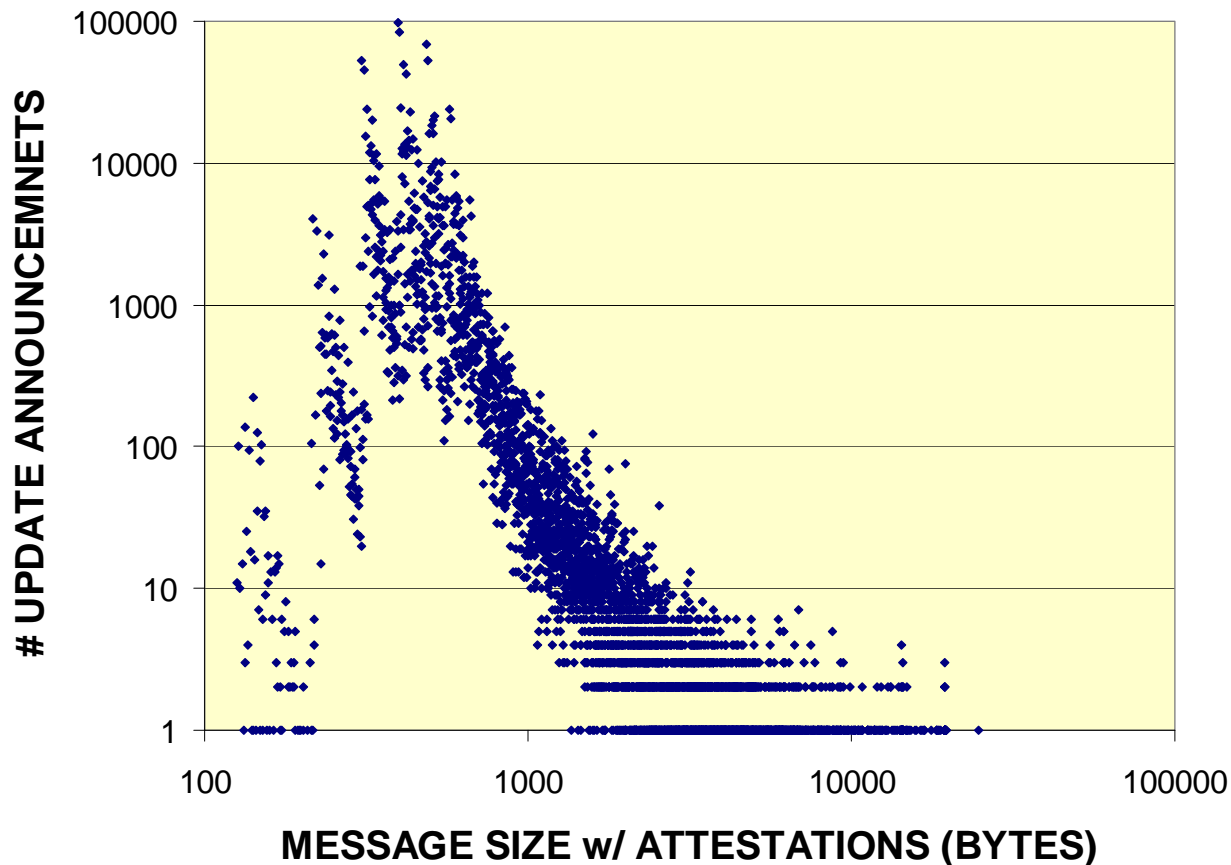
- Update sizes with attestations are computed accurately for each of the four schemes (using Routeviews data)
 - When AS prepending is detected, we collapse the repeated ASes into one AS for the purpose of attestation overhead computation
- Projections are made regarding growth in # prefixes in BGP speakers
- Suitable modeling assumptions are made regarding other modeling parameters (request BGPSEC team's feedback / refinements)
- The model is highly parameterized and can be tuned to reflect more accurate assumptions or measurements
- RIB sizes are estimated and compared for four path validation approaches (others can be included)
 - Sensitivity to key parameters and assumptions

Update Size with Attestations

| | W/O Attestations | With Attestations | | | |
|----------------------------|------------------|-------------------|--------|-----------|---------|
| | | SPP | SPP-E | SPP-E-SAS | SPU-EPA |
| Avg. Update | 78 | 1314 | 856 | 745 | 476 |
| Std Dev Update | 65 | 4655 | 2303 | 2119 | 278 |
| Min Update | 44 | 126 | 126 | 214 | 126 |
| Max Update | 4080 | 416947 | 205692 | 135537 | 24632 |
| <hr/> | | | | | |
| Avg. Attestation | -- | 1236 | 779 | 667 | 399 |
| Std Dev Attestation | -- | 4593 | 2242 | 2055 | 223 |
| Min Attestation | -- | 82 | 82 | 170 | 82 |
| Max Attestation | -- | 412870 | 201615 | 131457 | 20555 |

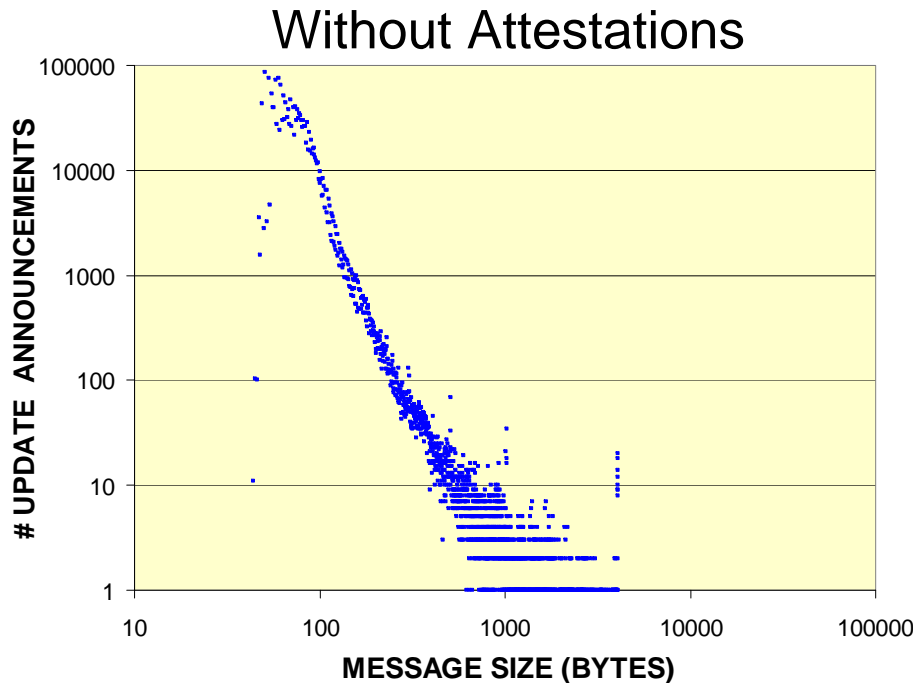
- We assume DSS with 320-bit signature is used in all method except the SPP-E-SAS method where RSA is used with 1024-bit signature in conjunction with SAS
- By attestation, we mean the signature bytes and attestation related overhead bytes
- The attestation overhead (Aoh) is assumed to be the same (39B) in all cases
- When AS prepending is detected, we collapse the repeated ASes into one AS for the purpose of attestation overhead computation
- Routeviews Oregon collector; 1.8M updates; Feb. 1-26, 2009

Distribution of Size of Update Announcements Including Attestations (Signature + Overhead) (SPU-EPA)

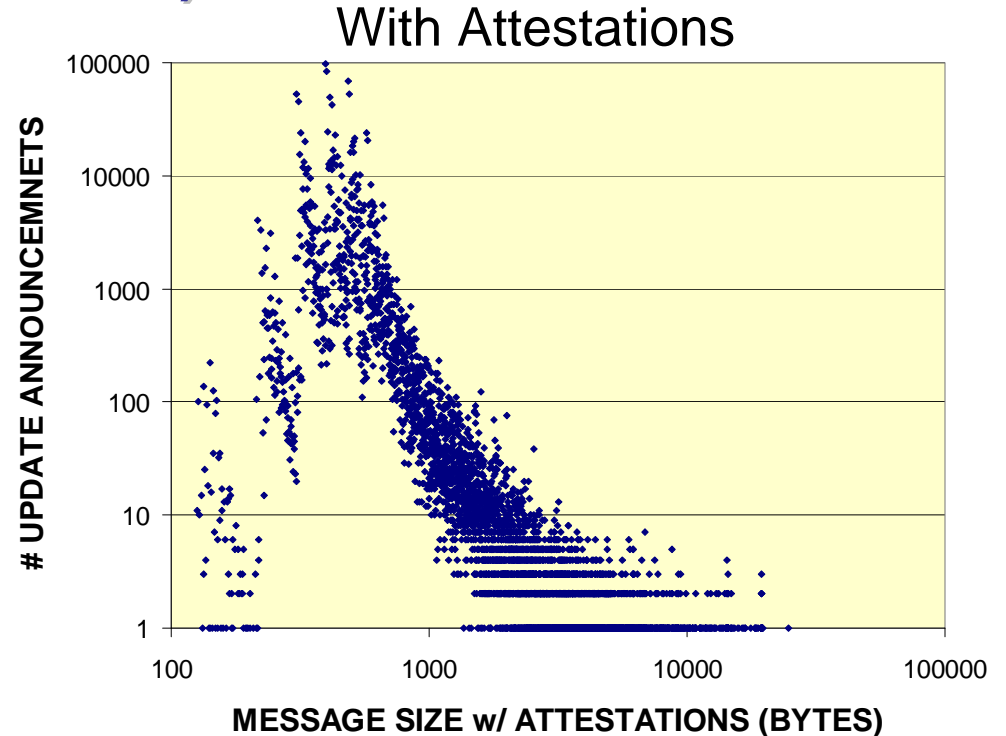


- Prob. {Message \leq 1200 B} = 99.02%
- Prob. {Message \leq 4000 B} = 99.92%

Comparison of Update Message Size: With and Without Attestations (SPU-EPA)

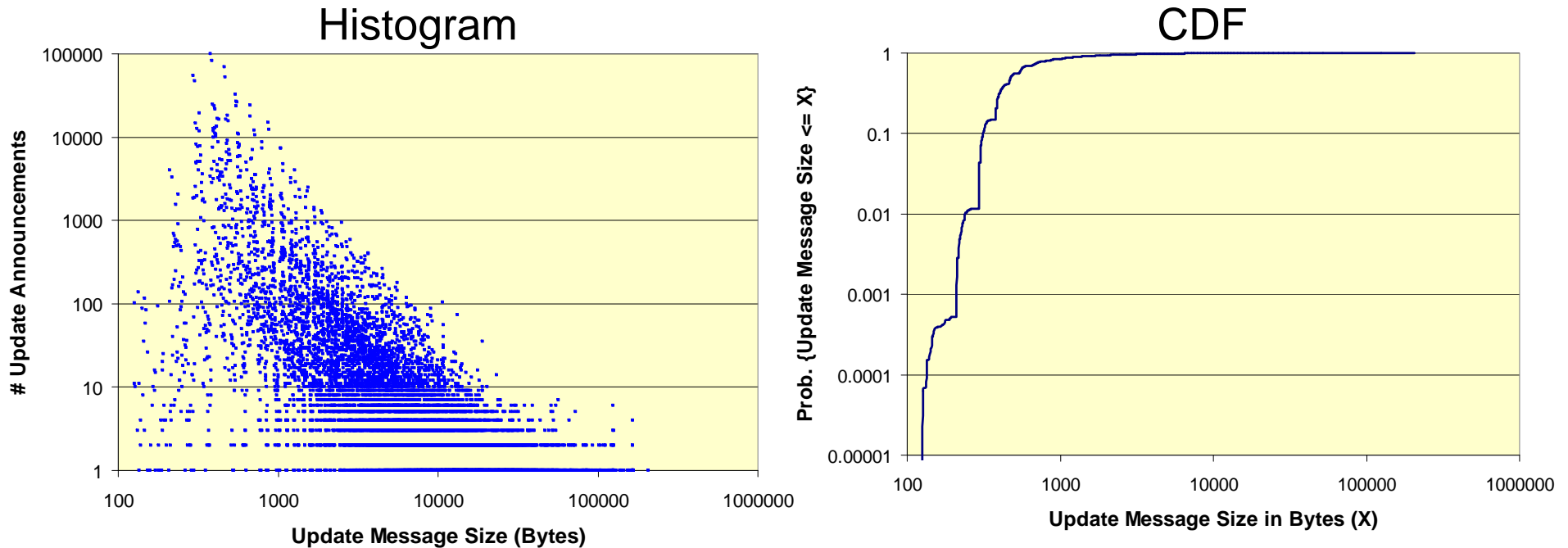


- Prob. {Message \leq 224 B} = 99.00%
- Prob. {Message \leq 854 B} = 99.90%
- Prob. {Message \leq 4000 B} = 99.994%



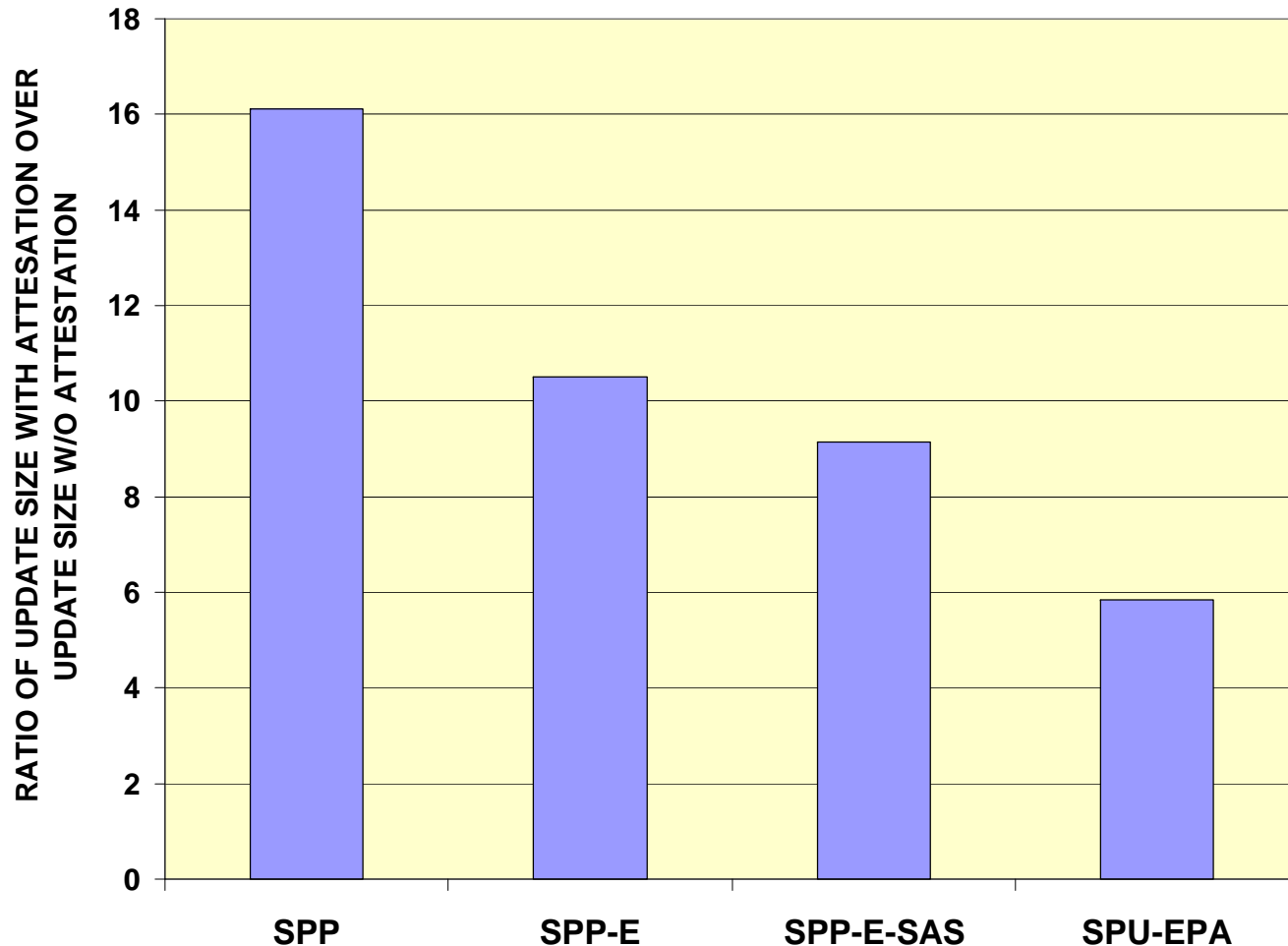
- Prob. {Message \leq 1200 B} = 99.02%
- Prob. {Message \leq 4000 B} = 99.92%

Distribution of Size of Update Announcements Including Attestations (Signature + Overhead) (SPP-E)



- Prob. {Message \leq 4000 B} = 97.81%
- Prob. {Message \leq 6792 B} = 99.00%
- Prob. {Message \leq 29044 B} = 99.90 %

Ratio of Update Size for Path Validation Approaches over Current BGP Update Size



- We assume DSS with 320-bit signature is used in all method except the SPP-E-SAS method where RSA is used with 1024-bit signature in conjunction with SAS

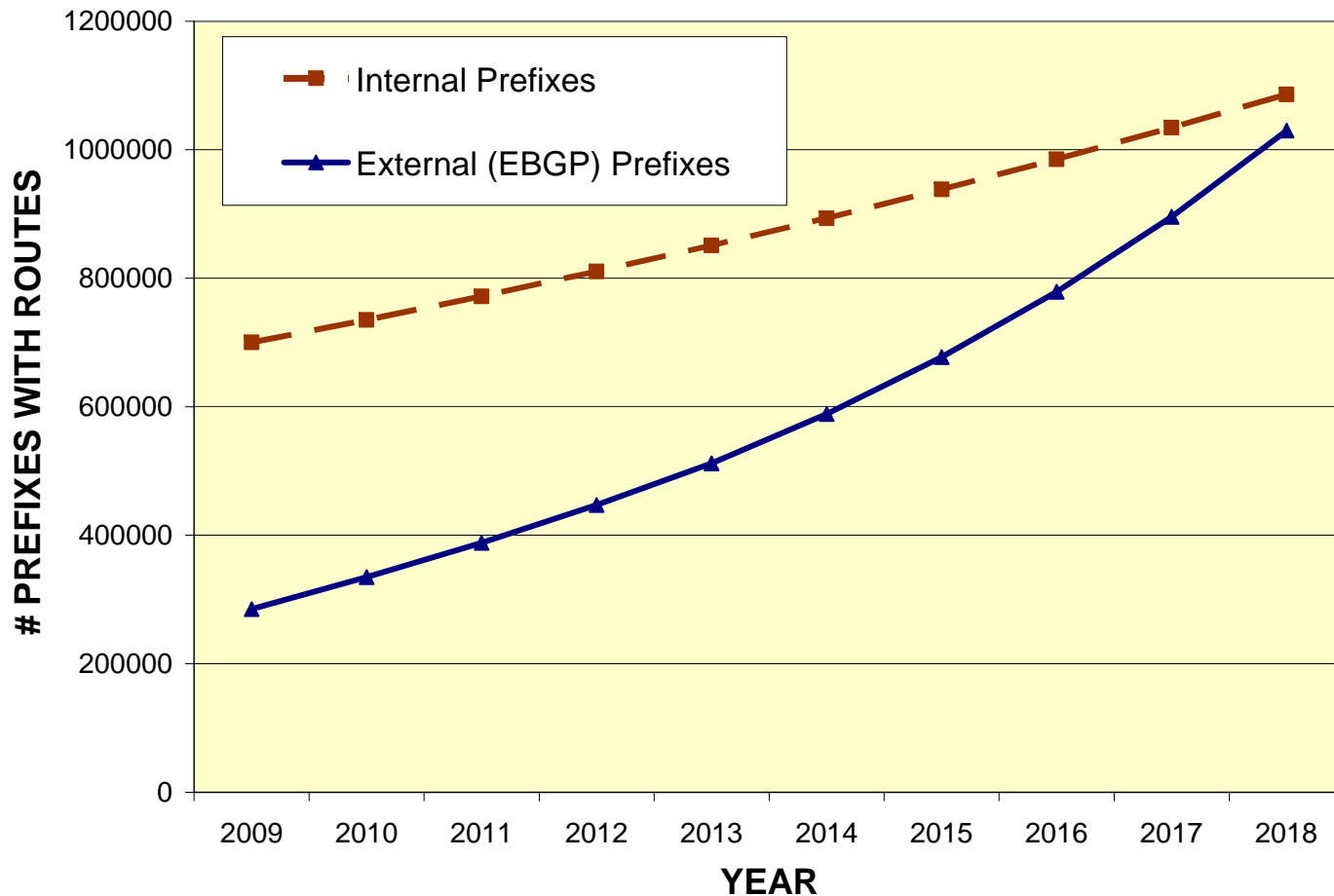
Parameters for Estimation of RIB Size

| Parameters for Estimation of RIB Size in a BGP Router | Value | Units | Comment |
|---|-------|-------|---|
| Average update size (w/o attestations) | 78 | B | Measured (2/09) |
| Average RIB data structure overhead per update | 5% | | Assumption |
| Average memory requirement per update in RIB | 82 | B | Computed from above |
| Number of peers for EBGP speaker | 200 | | Ball park for core routers |
| Avg. fraction of peers from which update is received for each EBGP prefix | 10% | | Assumption |
| Avg. number of peers from which update is received for each EBGP prefix | 20 | | Assumption |
| Number of peers from which update is received for each internal prefix | 10 | | Assumption |
| Avg. attestation overhead in RIB per update | 1236 | B | Measured (2/09) |
| Average # ASes in AS path | 4.743 | | Measured (2/09) |
| Average # prefixes per update announcement | 3.832 | | Measured (2/09) |
| Growth rate per year for Internal prefixes | 5% | | Assumption |
| Growth rate per year for External prefixes | 15% | | To extend growth projections further out from G. Huston's [2] time window |
| Include Internal prefixes? | 1 | | 1 = YES; 0 = NO |

- Plug in the avg. attestation size per update (from slide 28) for each of the four methods in consideration, and the model predicts the impact on the RIB size due to attestations (i.e., path validation)

[2] Geoff Huston, "BGP in 2008," <http://www.potaroo.net/ispcol/2009-03/bgp2008.html>

Growth in # Prefixes with Routes in RIB



- Growth in EBGP prefixes assumed to be the same as in [2] from 2009 to 2013, and then they are assumed to grow at 15% annual rate.

[2] Geoff Huston, "BGP in 2008," <http://www.potaroo.net/ispcol/2009-03/bgp2008.html>

Methodology for RIB Size Estimation

| Parameters for Estimation of RIB Size in a BGP Router | Symbol | Units | Equation (Model) |
|--|--------|-------|---|
| Average update size (w/o attestations) | U | B | |
| Average RIB data structure overhead per update | x | | |
| Average memory requirement per update in RIB | Ur | B | $U_r = U \cdot (1+x)$ |
| Number of peers for EBGp speaker | N | | |
| Avg. fraction of peers from which update is received for each EBGp prefix | f | | |
| Avg. number of peers from which update is received for each EBGp prefix | Nu | | $N_u = N \cdot f$ |
| Number of peers from which update is received for each internal prefix | m | | |
| Avg. attestation overhead in RIB per update | S | B | |
| Average # prefixes per update announcement | p | | |
| Total # Internal Prefixes with routes in the BGP speaker | Pi | | |
| Total # EBGp Prefixes with routes in the BGP speaker | Pe | | |
| RIB memory consumed by internal prefixes | Ri | GB | $R_i = (P_i/p) \cdot m \cdot U_r / 10^9$ |
| RIB memory consumed by external prefixes (w/o attestations) | Re | GB | $R_e = (P_e/p) \cdot N_u \cdot U_r / 10^9$ |
| Average memory requirement per update in RIB for signatures only | Us | B | |
| Average memory requirement per update in RIB including signatures | Ua | B | $U_a = U + U_s$ |
| RIB memory consumed by signatures for external prefixes | Rs | GB | $R_s = (P_e/p) \cdot N_u \cdot U_s \cdot (1+x) / 10^9$ |
| RIB memory consumed by EBGp updates with attestations | Rue | GB | $R_{ue} = (P_e/p) \cdot N_u \cdot U_a \cdot (1+x) / 10^9$ |
| Total RIB memory consumed by Internal routes + EBGp routes with attestations | R | GB | $R = R_i + R_{ue}$ |

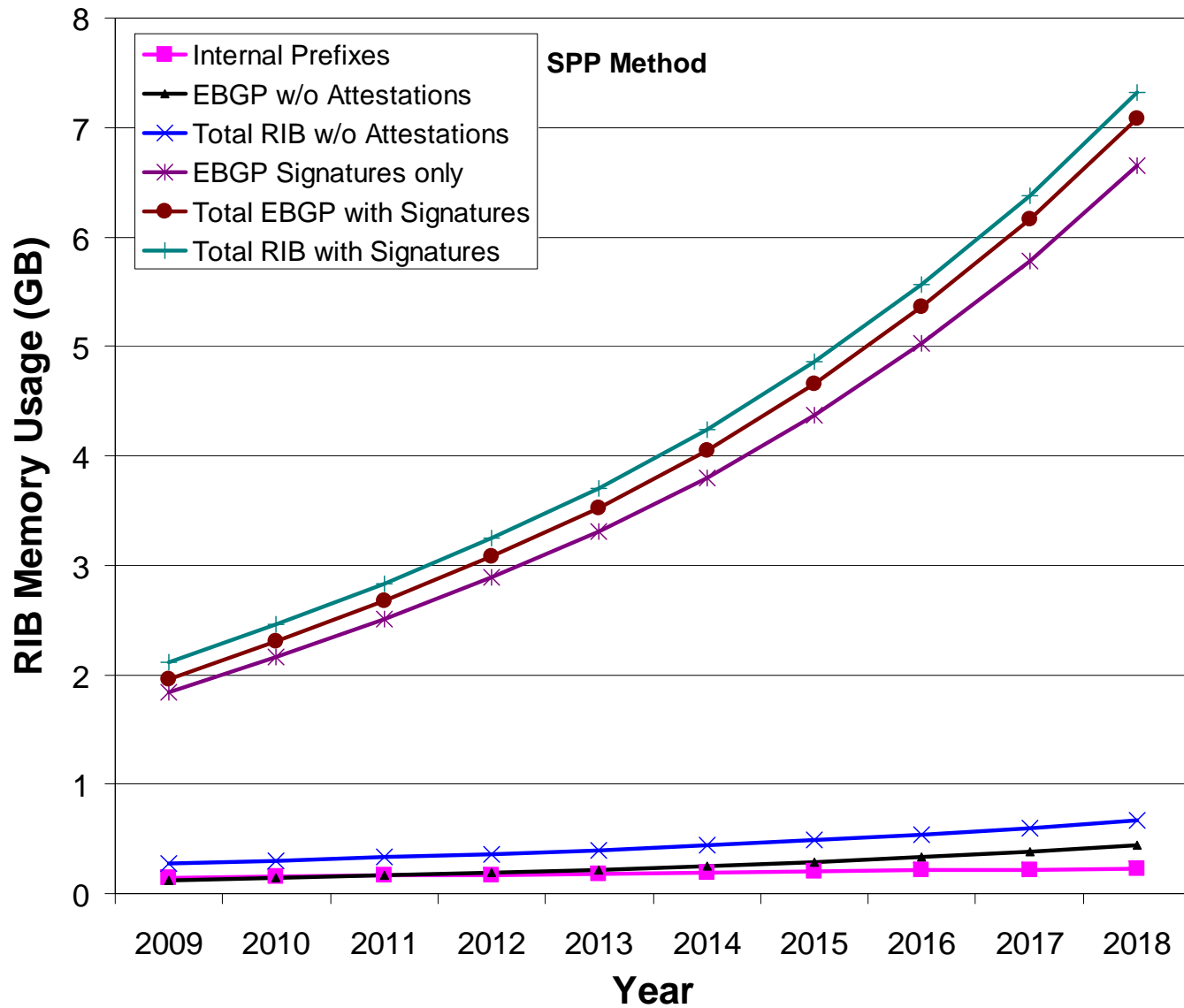
RIB Size for SPP Approach

| Year | # Internal Prefixes | # External (EBGP) prefixes | Total # Prefixes with Routes | RIB Requirement for Internal prefixes (GB) | RIB Requirement for External (EBGP) prefixes (GB) | RIB size w/o attestations (GB) | RIB size with attestations (GB) | | |
|------|---------------------|----------------------------|------------------------------|--|---|--------------------------------|--|-------------------------------|---------------------------------------|
| | | | | | | | RIB size for signatures alone for EBGP routes (GB) | RIB size for EBGP routes (GB) | Total RIB size with attestations (GB) |
| 2009 | 700000 | 285000 | 985000 | 0.15 | 0.12 | 0.27 | 1.84 | 1.96 | 2.11 |
| 2010 | 735000 | 335000 | 1070000 | 0.16 | 0.14 | 0.30 | 2.16 | 2.30 | 2.46 |
| 2011 | 771750 | 388000 | 1159750 | 0.16 | 0.17 | 0.33 | 2.50 | 2.67 | 2.83 |
| 2012 | 810338 | 447000 | 1257338 | 0.17 | 0.19 | 0.36 | 2.88 | 3.07 | 3.25 |
| 2013 | 850854 | 512000 | 1362854 | 0.18 | 0.22 | 0.40 | 3.30 | 3.52 | 3.70 |
| 2014 | 893397 | 588800 | 1482197 | 0.19 | 0.25 | 0.44 | 3.80 | 4.05 | 4.24 |
| 2015 | 938067 | 677120 | 1615187 | 0.20 | 0.29 | 0.49 | 4.37 | 4.66 | 4.86 |
| 2016 | 984970 | 778688 | 1763658 | 0.21 | 0.33 | 0.54 | 5.02 | 5.36 | 5.57 |
| 2017 | 1034219 | 895491 | 1929710 | 0.22 | 0.38 | 0.60 | 5.78 | 6.16 | 6.38 |
| 2018 | 1085930 | 1029815 | 2115745 | 0.23 | 0.44 | 0.67 | 6.65 | 7.08 | 7.31 |

- Growth in EBGP prefixes assumed to be the same as in [2] from 2009 to 2013, and then they are assumed to grow at 15% annual rate.

[2] Geoff Huston, "BGP in 2008," <http://www.potaroo.net/ispcol/2009-03/bgp2008.html>

RIB Size for SPP Approach



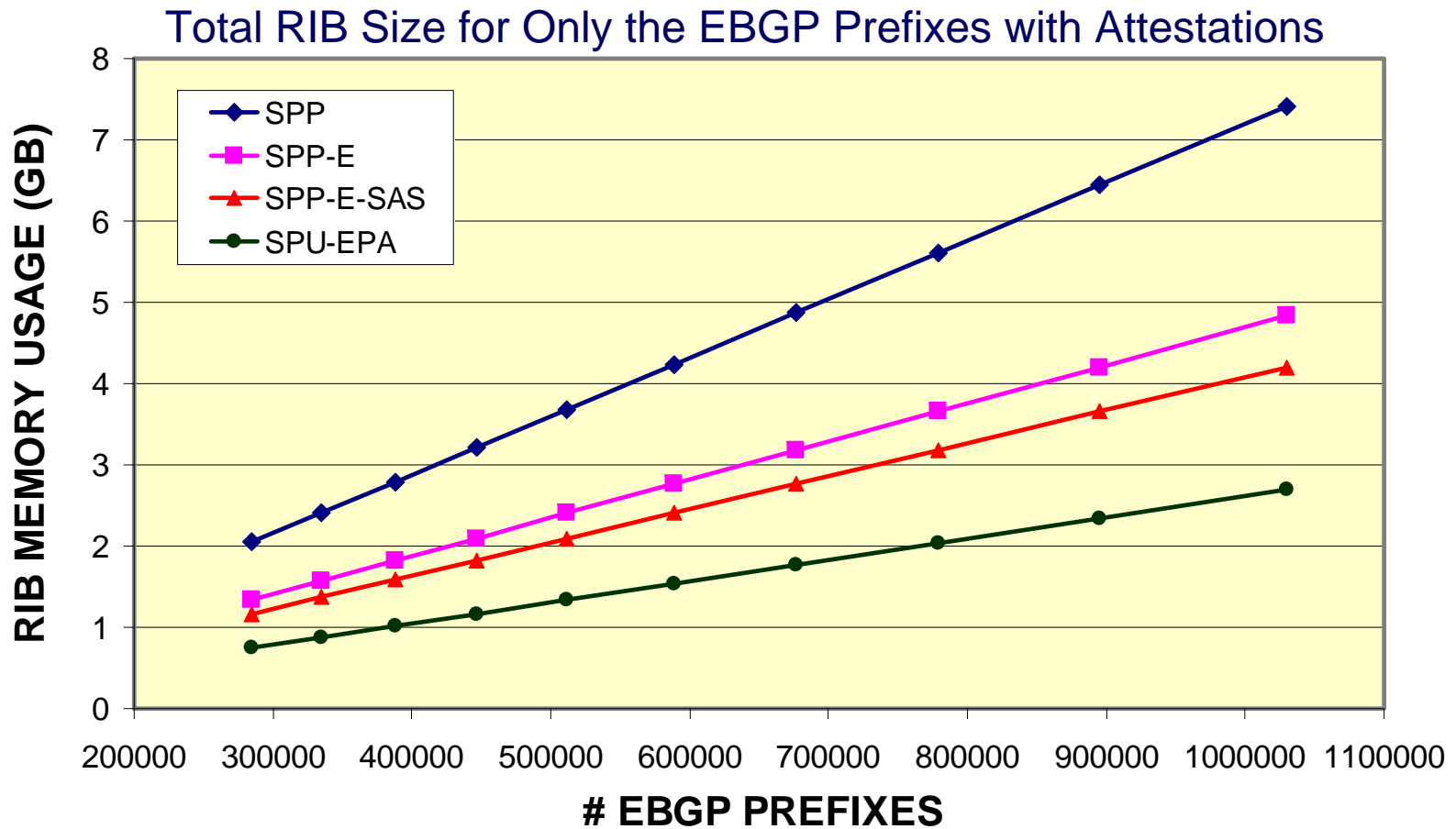
-- Draft for Comments --

RIB Size Comparison for the Four Path Validation Approaches

| Total RIB size (GB) -- Only EBGP Prefixes | | | | | | |
|---|---------|------------------|-------------------|-------|-----------|---------|
| | | W/O Attestations | With Attestations | | | |
| | | | SPP | SPP-E | SPP-E-SAS | SPU-EPA |
| 2009 | 285000 | 0.12 | 2.05 | 1.34 | 1.16 | 0.74 |
| 2010 | 335000 | 0.14 | 2.41 | 1.57 | 1.37 | 0.87 |
| 2011 | 388000 | 0.17 | 2.79 | 1.82 | 1.58 | 1.01 |
| 2012 | 447000 | 0.19 | 3.22 | 2.10 | 1.83 | 1.17 |
| 2013 | 512000 | 0.22 | 3.69 | 2.40 | 2.09 | 1.34 |
| 2014 | 588800 | 0.25 | 4.24 | 2.76 | 2.40 | 1.54 |
| 2015 | 677120 | 0.29 | 4.88 | 3.18 | 2.76 | 1.77 |
| 2016 | 778688 | 0.33 | 5.61 | 3.65 | 3.18 | 2.03 |
| 2017 | 895491 | 0.38 | 6.45 | 4.20 | 3.66 | 2.34 |
| 2018 | 1029815 | 0.44 | 7.42 | 4.83 | 4.20 | 2.69 |

| Total RIB size (GB) -- Both EBGP and Internal Prefixes | | | | | | |
|--|---------|------------------|-------------------|-------|-----------|---------|
| | | W/O Attestations | With Attestations | | | |
| | | | SPP | SPP-E | SPP-E-SAS | SPU-EPA |
| 2009 | 285000 | 0.12 | 2.20 | 1.49 | 1.31 | 0.89 |
| 2010 | 335000 | 0.14 | 2.57 | 1.73 | 1.52 | 1.03 |
| 2011 | 388000 | 0.17 | 2.96 | 1.99 | 1.75 | 1.18 |
| 2012 | 447000 | 0.19 | 3.39 | 2.27 | 2.00 | 1.34 |
| 2013 | 512000 | 0.22 | 3.87 | 2.58 | 2.27 | 1.52 |
| 2014 | 588800 | 0.25 | 4.43 | 2.95 | 2.59 | 1.73 |
| 2015 | 677120 | 0.29 | 5.08 | 3.38 | 2.96 | 1.97 |
| 2016 | 778688 | 0.33 | 5.82 | 3.86 | 3.39 | 2.24 |
| 2017 | 895491 | 0.38 | 6.67 | 4.42 | 3.88 | 2.56 |
| 2018 | 1029815 | 0.44 | 7.65 | 5.06 | 4.44 | 2.92 |

RIB Size Comparison for the Four Path Validation Approaches



Note: SPP-E-SAS uses 1024-bit RSA signature while other methods use only a 320-bit DSS signature

Request for Feedback / Information to Refine the RIB Modeling

- Several assumptions / modeling parameters can be refined with feedback / inputs from the group
- Modeling assumptions for internal prefixes
 - # internal prefixes and their growth rate
 - Size per update in the RIB
 - Attestation not needed for internal prefixes – OK?
- Signature over AS path only vs. AS path plus prefix
 - We assumed the latter makes sense and modeled accordingly
- RIB data structure overhead (per update) and how does it scale with # updates in RIB

Potential Future Enhancements/Complications for Signature Schemes (proposed for discussion in the group)

- What happens if someone upstream prepends a downstream ASN?
 - Signatures should remain unaffected as long they are performed over the collapsed AS path
- Pre-compute signed objects for 1st and 2nd choice routes for each prefix and cache them
 - Saves computation time when path selection switches between 1st and 2nd choices (failure/recover scenarios)
- Caching validations to save processing
- Use of BGP sequence numbers – Variation of BGP Graceful Restart
 - Use IPsec to prevent replay attacks
 - Then use a sequence number in BGP so that peer can look at the sequence number in the update to know if the same update was previously validated
 - This is a sort of BGP graceful restart (in the presence of attestations)
 - Avoid validation of thousands of attestations upon recovery of a BGP session with a peer

Appendix A

Brief Overview of Sequential Aggregate Signature (SAS) Method

[Mu2007] Y. Mu, W. Susilo, and H. Zhu, “Compact sequential aggregate signatures,” Proceedings of the ACM Symposium on Applied Computing (2007), pp. 249-253.

[Ma2008] Di Ma, “Practical Forward Secure Aggregate Signatures,” ACM Symposium on Information, Computer and Communications Security (ASIACCS'08), Tokyo, Japan. Mar. 2008.

Sequential Aggregate Signatures

- Let $\text{sign}(\cdot)$ be a signature scheme such that the inverse of sign is computable.
- Then a sequentially composed message can be authenticated at every step of message modification and forwarding with known signers.

Y. Mu, W. Susilo, and H. Zhu, "Compact sequential aggregate signatures," Proceedings of the ACM Symposium on Applied Computing (2007), pp. 249-253.

Signing Algorithm

- If $m[1]$ is the first message to be signed by $v[1]$,
 $M[1] = (m[1], v[1])$,
 $s[1] = \text{sign}(h(M[1]))$, and
 $(M[1], s[1])$ is the signed message.
- When the k^{th} signer, $v[k]$, $k > 1$, receives
 $(M[k-1], s[k-1])$, and authenticates it (see how on next slide); then computes
 $M[k] = (M[k-1], m[k], v[k])$
 $s[k] = \text{sign}(h(M[k]) \text{ XOR } s[k-1])$.
Now $(M[k], s[k])$ is the signed message of $v[k]$.

Verification Algorithm

- If $k=1$, verification proceeds as usual.
- If $k>1$ and the signed message $(M[k], s[k])$ is received, then
 - From $s[k]$, we compute $h(M[k]) \text{ XOR } s[k-1]$
 - The above is possible because sing^{-1} is computable
 - From $h(M[k])$ and $\{h(M[k]) \text{ XOR } s[k-1]\}$, we compute $s[k-1]$, provided the message is authentic.
 - Now the authenticity of $(M[k], s[k])$ reduces to the authenticity of $(M[k-1], s[k-1])$
 - Proceed recursively until verification traces back to $(M[1], s[1])$ and then finish with one usual verification step for $(M[1], s[1])$.

Practical Issues

- SAS schemes exist, typically based on RSA or equivalent.
- Given that the average BGP path is 5 hops or shorter, in order for SAS schemes to provide RIB memory improvement over the Digital Signature Standard (DSS) with 320-bit signature, a SAS scheme would need to achieve comparable levels of security with significantly fewer than $5 \times 320 = 1600$ bits of signature.
- SAS with 1024-bit RSA could be a candidate to consider.
- Further exploration of this is needed to better understand SAS properties and applicability for BGPSEC.