

sidrops
Internet-Draft
Intended status: Informational
Expires: 25 August 2025

N. Geng
Huawei
M. Huang
Zhongguancun Lab
Y. Wang
Tsinghua University
21 February 2025

An Analysis of ASPA-based AS_PATH Verification
draft-geng-sidrops-aspa-analysis-02

Abstract

Autonomous System Provider Authorization (ASPA) is very helpful in detecting and mitigating route leaks (valley-free violations) and a majority of forged-origin hijacks. This document does an analysis on ASPA-based AS_PATH verification to help people understand its strengths and deficiencies, and some potential directions of enhancing ASPA are provided.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 August 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
1.1. Terminology	3
1.2. Requirements Language	3
2. ASPA Strengths and Disclaimers	3
2.1. Protecting Against Route Leak	3
2.2. Protecting Against Path Manipulation	3
3. ASPA Deficiencies	4
3.1. Hard to Detect Bogus Records	4
3.2. Fail to Detect AS_PATH Manipulation by a Provider	5
3.3. Not Directly Applicable to IBGP Ingress and EBGP Egress Verification	7
3.4. Not Applicable to Complex Relationship Scenarios	8
3.5. Reduced Protection Capability in Partial Deployment	11
4. Reasons of ASPA Deficiencies	12
5. Security Considerations	12
6. IANA Considerations	12
7. Acknowledgements	12
8. References	12
8.1. Normative References	12
8.2. Informative References	13
Authors' Addresses	14

1. Introduction

Autonomous System Provider Authorization (ASPA) is a technique for verifying AS_PATHs in BGP updates [I-D.ietf-sidrops-aspa-verification][I-D.ietf-sidrops-aspa-profile]. Each AS can register ASPA records (also ASPA objects) in the RPKI to authorize a set of ASes as its providers. An AS can obtain ASes' ASPA records through RTRv2 protocol [I-D.ietf-sidrops-8210bis] and conduct AS_PATH verification based the records. ASPA-based AS_PATH verification can detect and mitigate route leaks violating the valley-free principle and path manipulations such as forged-origin or forged-path-segment attacks.

ASPA can significantly enhance AS_PATH verification and is promising to be widely deployed. Despite of the strengths of ASPA, there are also some deficiencies. This document provides a detailed analysis on the strengths and deficiencies of ASPA. The document can help people deploy ASPA properly and provide some potential directions of enhancing ASPA.

1.1. Terminology

The usage of terms follows

[I-D.ietf-sidrops-aspa-verification][I-D.ietf-sidrops-aspa-profile].

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. ASPA Strengths and Disclaimers

ASPA records can be registered by an AS to authorize all its provider ASes. For the two ASes with mutual transit relationship, the two ASes will put each other AS into its own ASPA record (i.e., each AS considers the other AS as its provider).

2.1. Protecting Against Route Leak

In full ASPA deployment (within a given region of interest), all "route leaks" (valley-free violations [RFC7908]) are detectable. Route leaks involve one of the following four valley-free violations:

- * A route is propagated through a P2C (Provider-to-Customer) link and then a C2P (Customer-to-Provider) link.
- * A route is propagated through a P2P (Peer-to-Peer) link and then a C2P link.
- * A route is propagated through a P2P link and then a P2P link.
- * A route is propagated through a P2C link and then a P2P link.

It is expected that in partial ASPA deployment, not all route leaks are detectable.

2.2. Protecting Against Path Manipulation

Path manipulation can be path forgery or path tampering (i.e., insertion or removal of unique ASN) in this document. Forged-origin hijack and fake link-based hijack are all path manipulations.

In full ASPA deployment (within a given region of interest), ASPA protects against a majority of forged-origin hijacks. Each AS can attest its upstream ASes, so provider or lateral peer cannot be deceived. Customer could be deceived because ASPA does not provide attestations to downstream ASes or peering ASes.

Even in full ASPA deployment, not all path manipulation attacks can be detected. ASPA does not guarantee path correctness like that provided by BGPsec [RFC8205].

3. ASPA Deficiencies

This section describes the deficiencies of ASPA-based AS_PATH verification in detail.

3.1. Hard to Detect Bogus Records

An AS can unilaterally authorize a set of its provider ASes. Under the one-direction authorization, an AS may intentionally or unintentionally register bogus records that are hard to be discovered. An AS maliciously registers bogus records that open a door to potential attacks.

Figure 1 shows an example of path manipulation attack based on bogus ASPA records. AS4 lies in that the nonadjacent AS3 is its provider in the ASPA record. The attack cannot be detected even when AS1, AS2, AS3, and AS5 register ASPA records correctly and enable ASPA-based AS_PATH verification locally. As a result, AS5 will wrongly consider its traffic to AS1 traverses AS3, while the real forwarding path to AS1 is through AS2 instead of AS3.

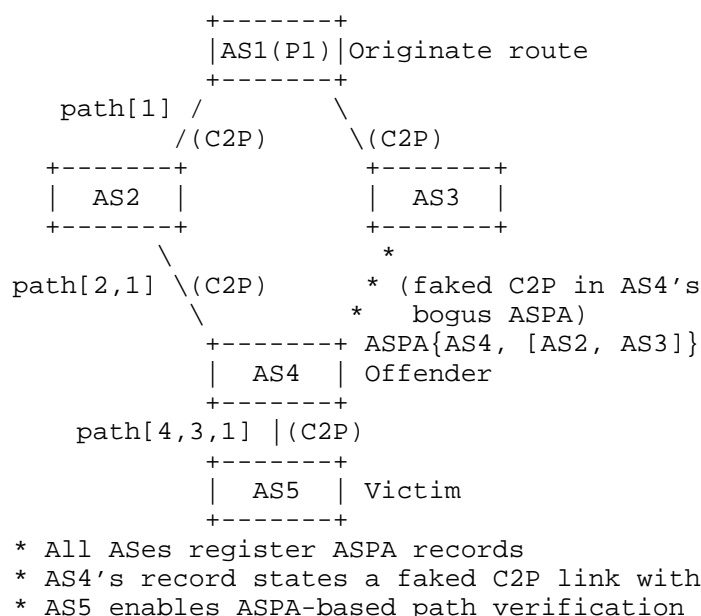


Figure 1: Path manipulation based on bogus ASPA records

3.2. Fail to Detect AS_PATH Manipulation by a Provider

ASPA-based AS_PATH verification cannot effectively detect the AS_PATH maliciously shortened by a provider, which has been acknowledged in [I-D.ietf-sidrops-aspa-verification].

Figure 2 shows an example. AS1 originates the BGP route and propagates the route to other ASes. The AS_PATH received by AS5 is path[4,3,2,1]. However, AS5 maliciously shortens the path by falsely claim a fake link with AS2 before AS5 propagates the route to AS6. AS6's traffic to AS1 may be hijacked by AS5 if the path[5,2,1] is shorter than any other AS_PATHs. In the example, AS5 may not intend to drop data traffic from AS6. That is, AS5 (provider) wants AS6 (customer) to prefer AS5's transit path for increasing revenue.

In this case, the attack cannot be detected even when all the ASes register the correct ASPA records and all the ASes other than AS5 enable ASPA-based AS_PATH verification.

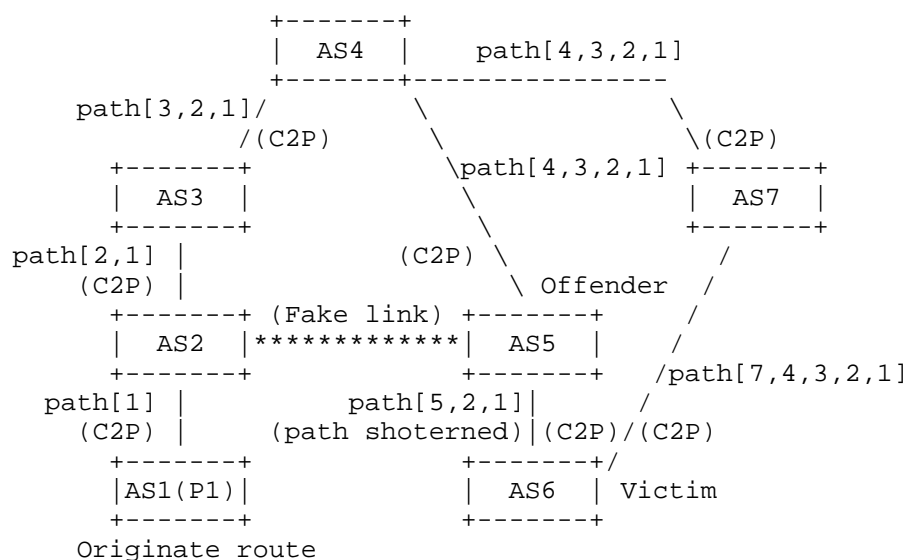


Figure 2: AS_PATH maliciously shortened by a provider

AS_PATH manipulation by a provider may also be used to do malicious route leaks. ASPA is not designed for defending path manipulation. So, some malicious route leaks with path manipulation involved cannot be prevented.

Figure 3 shows an example. AS2 is AS1's provider and arguably it may not leak its customer's prefix (P2) intentionally. But to increase revenue, AS2 may maliciously leak P2 with a modified AS_PATH (i.e., AS3 is removed) to AS4 for attracting more traffic to traverse AS2. Sometimes this attack may happen and goes undetected.

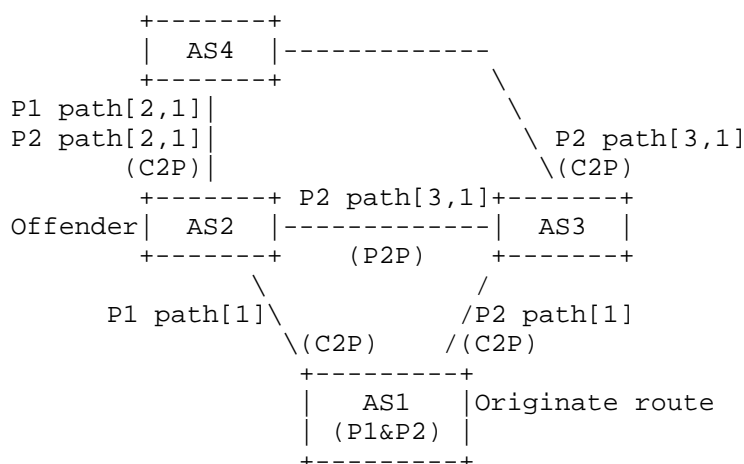


Figure 3: Malicious route leak

3.3. Not Directly Applicable to IBGP Ingress and EBGP Egress Verification

IBGP ingress verification and eBGP egress verification are meaningful in many scenarios. IBGP ingress verification is to check the AS_PATH received through iBGP connections. IBGP ingress verification helps an AS do verification on any BGP routers like non-ASBRs. EBGP egress verification means verifying the AS_PATH before sending it to the neighbor AS. It can prevent an AS from sending routes with Invalid AS_PATH to its neighbor ASes (just like eBGP egress RPKI-ROV [RFC8893]).

However, current ASPA document [I-D.ietf-sidrops-aspa-verification] does not specify how to do iBGP ingress verification. For iBGP ingress verification, the router (e.g., an RR) conducting the verification may not have BGP sessions with the neighbor AS that propagates the route and thus does not know the local BGP role with respect to the neighbor AS. Even so, iBGP ingress verification is doable because the router can obtain the local BGP role from the ASPA records of local AS. In Figure 4, when RR wants to do iBGP ingress verification, it can look up AS2's own ASPA records. If AS1 is listed as a provider, then apply the Downstream verification algorithm. If AS1 is not listed as a provider, then apply the Upstream verification algorithm. Such an iBGP ingress verification also works correctly in RS and RS-client scenarios.

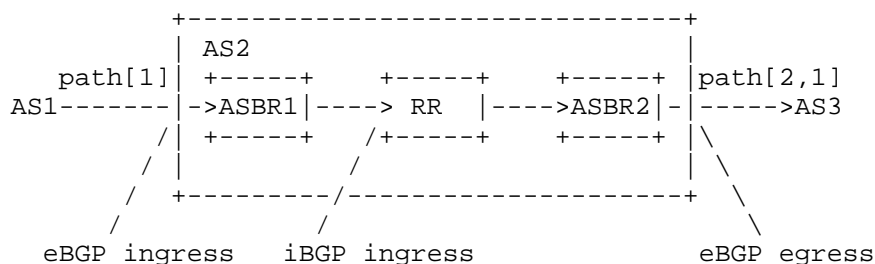


Figure 4: IBGP and eBGP verification

[I-D.ietf-sidrops-aspa-verification] does not specify how to do eBGP egress verification either. To try to do this, the router should add its own AS (i.e., AS2) to the AS_PATH and then performs ASPA-based AS_PATH verification from the perspective of next-hop AS (see Section 7.2 in version-15 of [I-D.ietf-sidrops-aspa-verification]). According to the verification result, the router decides to propagate the route or not. In Figure 4, ASBR2 would add its own AS (i.e., AS2) to the AS_PATH. If the BGP role of ASBR2 with respect to AS3 is customer/lateral peer/RS/RS-client, the Upstream verification algorithm will be conducted. If the BGP role of ASBR2 with respect to AS3 is provider, the Downstream verification algorithm will be performed. The verification process also works well in mutual transit scenarios.

The relationship between AS1 and AS2 can sometimes be obtained by ASBR2 from AS2's ASPA records. If AS1 is listed as a provider in the AS2's ASPA records, then the above route leak can be detected and prevented. If AS1 is not listed in the AS2's ASPA records, ASBR2 cannot decide AS1 is a lateral peer or a customer. Therefore, the above route leak cannot be detected directly.

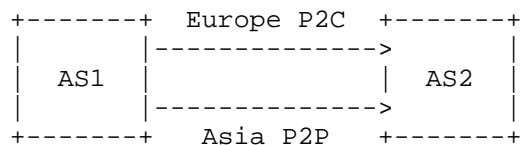
Overall, iBGP ingress verification is doable with help of local AS's own ASPA records, while it is not possible to do eBGP egress verification correctly without more complexity.

3.4. Not Applicable to Complex Relationship Scenarios

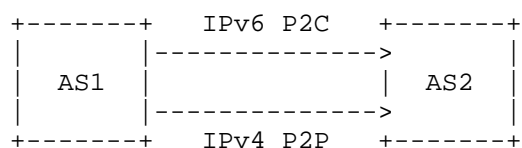
AS relationships in practical networks may be more complex than the traditional P2C/P2P model [as-rela-1][as-rela-2]. In ASPA, only the complex relationship of mutual transit relationship has been considered. The followings are some other complex scenarios that are not covered by ASPA:

- * Hybrid relationship [as-rela-1][as-rela-2]. Two ASes may agree to have different traditional relationships for different Points-of-Presence (PoPs). A hybrid relationship may be dependent on IP

versions or/and PoP locations (see Figure 5 for examples), even prefixes (i.e., different relationships/policies for different prefixes).



(a) Location-dependent



(b) IP version-dependent

Figure 5: Hybrid relationship

- * Partial transit relationship [as-rela-1][as-rela-2]. For a customer, the provider offers transit only toward the provider's peers and customers (or specific regions), but not the provider's providers, or restricts transit to a specific geographic region. Figure 5 shows an example. AS2 is the partial transit provider of AS1. AS2 should only propagate AS1's route to AS4 (i.e., AS2's peer) and AS5 (i.e., AS2's customer), but should not propagate the route to AS3 (i.e., AS2's provider).

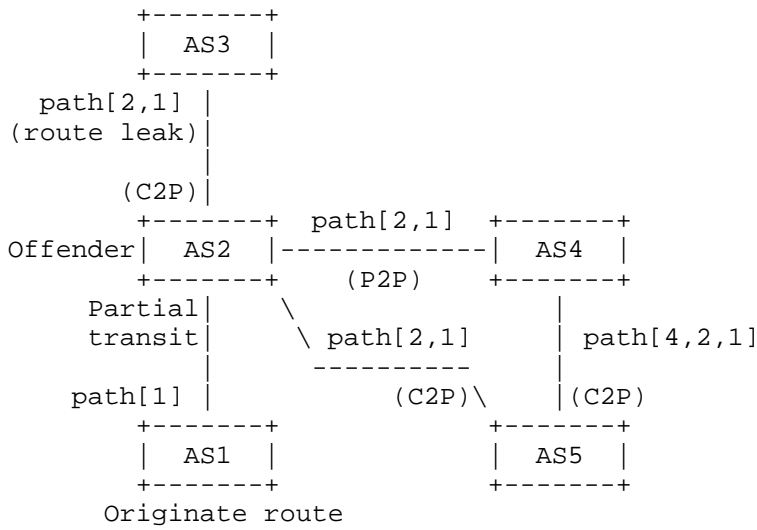


Figure 6: Partial transit relationship

- * Persistent valley-path (legitimate valley-path) ([valley-path]). There may be legitimate valley-paths, i.e., violating the valley-free principle but the AS_PATH is legitimate. According to BGP data analysis, the persistent valley-path can be 10% of all BGP paths.

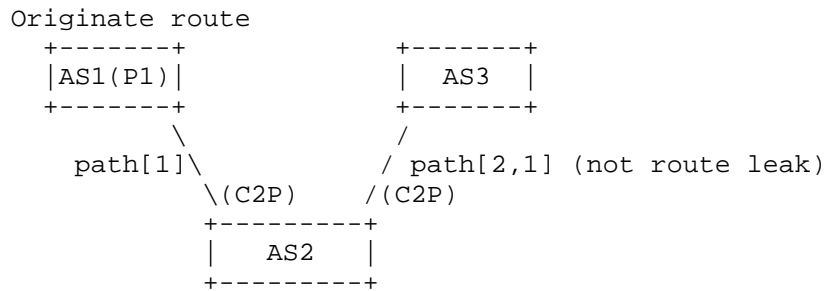


Figure 7: Persistent valley-path

ASPA records do not support the registration of complex relationships except the mutual transit relationship. As a result, in the complex scenarios, AS_PATH cannot be effectively protected by ASPA-based AS_PATH verification.

3.5. Reduced Protection Capability in Partial Deployment

To verify an AS_PATH, ASPA verification algorithms need to check each hop of the AS_PATH. When ASPA records of the ASes along the path are partially registered, not all hops in the path can be checked. In such partial deployment scenarios, ASPA may have a reduced protection capacity.

Figure 8 shows two examples of partial deployment. In Figure 8 (a), AS3 cannot detect the route leak of P1 induced by AS2 if AS1 has no ASPA record registered. This is because the Hop-check(AS1, AS2) function returns "No Attestation" and the final verification result is Unknown. In Figure 8 (b), AS3 is deceived by AS2 who falsely claims AS1 is AS2's neighbor. The attack in the example is undetectable because AS1 registers no ASPA record and AS3 cannot judge the validity of the link between AS1 and AS2.

```

                                +-----+
                                |  AS3  |
                                +-----+
                                  /
                                / path[2,1] (route leak)
                                /(C2P)
No ASPA
+-----+ (P2P) +-----+
|AS1(P1)|-----| AS2 | Offender
+-----+ path[1] +-----+
Originate route

```

(a) Route leak in partial deployment

```

                                +-----+
                                |  AS3  |
                                +-----+
                                  /
                                / path[2,1] (path manipulation)
                                /(C2P)
No ASPA (no adjacency)
+-----+ +-----+
|AS1(P1)|*****| AS2 | Offender
+-----+ path[1] +-----+
Originate route

```

(b) Forged-origin attack in partial deployment

Figure 8: Partial deployment

4. Reasons of ASPA Deficiencies

This section summarizes three main reasons that result in deficiencies of ASPA:

- * ASPA record is authorized in one direction, e.g., an AS can unilaterally claim that another AS is its provider without the consent of other ASes. Related deficiencies:
 - Hard to detect bogus records
- * An ASPA record only focuses on including all provider ASes while ignoring other topology or relationship information. Related deficiencies:
 - Hard to detect bogus records
 - Fail to detect AS_PATH maliciously shortened by a provider
 - Not directly applicable to iBGP Ingress and eBGP egress verification
 - Not applicable to complex relationship scenarios
 - Reduced protection capacity in partial deployment
- * The kind of method that verifies AS_PATH based on relationships does not guarantee path correctness like that provided by BGPsec.
 - Not all malicious route leaks are prevented

5. Security Considerations

This document does not involve security problems.

6. IANA Considerations

No IANA requirement.

7. Acknowledgements

Much thanks for the comments and inputs from Kotikalapudi Sriram.

8. References

8.1. Normative References

[I-D.ietf-sidrops-asma-verification]

Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-asma-verification-20, 4 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-asma-verification-20>>.

[I-D.ietf-sidrops-asma-profile]

Azimov, A., Uskov, E., Bush, R., Snijders, J., Housley, R., and B. Maddison, "A Profile for Autonomous System Provider Authorization", Work in Progress, Internet-Draft, draft-ietf-sidrops-asma-profile-19, 6 January 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-asma-profile-19>>.

[RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", RFC 7908, DOI 10.17487/RFC7908, June 2016, <<https://www.rfc-editor.org/info/rfc7908>>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

8.2. Informative References

[I-D.ietf-sidrops-8210bis]

Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 2", Work in Progress, Internet-Draft, draft-ietf-sidrops-8210bis-16, 27 September 2024, <<https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-8210bis-16>>.

[RFC8205] Lepinski, M., Ed. and K. Sriram, Ed., "BGPsec Protocol Specification", RFC 8205, DOI 10.17487/RFC8205, September 2017, <<https://www.rfc-editor.org/info/rfc8205>>.

[RFC8893] Bush, R., Volk, R., and J. Heitz, "Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export", RFC 8893, DOI 10.17487/RFC8893, September 2020, <<https://www.rfc-editor.org/info/rfc8893>>.

[as-rela-1] "Stable and Practical AS Relationship Inference with ProbLink", February 2019, <<https://www.usenix.org/system/files/nsdi19-jin.pdf>>.

[as-rela-2] "Inferring Internet AS Relationships Based on BGP Routing Policies", January 2011.

[valley-path] "Valley-free violation in Internet routing - Analysis based on BGP Community data", November 2012, <<https://ieeexplore.ieee.org/document/6363987>>.

Authors' Addresses

Nan Geng
Huawei
Beijing
China
Email: gengnan@huawei.com

Mingqing Huang
Zhongguancun Lab
Beijing
China
Email: huangmq@mail.zgclab.edu.cn

Yangyang Wang
Tsinghua University
Beijing
China
Email: wangyy@cernet.edu.cn