Securing Multi-domain 5G/6G Routing: Towards Path Verification with ASPA

Antonio Prado, Marco Centenaro, and Lorenzo Vangelista
Department of Information Engineering, University of Padova, via Gradenigo 6/b, 35131 Padova, Italy
antonio.prado@dei.unipd.it, marco.centenaro@unipd.it, lorenzo.vangelista@unipd.it
ORCID 0000-0002-5600-8509, 0000-0003-1664-8015, 0000-0002-4898-6951

***Abstract*—Both distributed mobile network infrastructures and the interworking between public land mobile networks and packet data networks rely on interdomain routing at network boundaries, thus the end-to-end mobile communication system reliability depends on the underlying Internet routing framework. In this regard, the verification of interdomain routing increasingly requires mechanisms that go beyond traditional route-origin validation and address the internal structure of the advertised path. Recently, Autonomous System Provider Authorization (ASPA) has been introduced exactly for this purpose: it uses signed provider authorizations to verify the compressed autonomous system (AS) path, thus detecting route leaks and some classes of AS-path manipulation. This paper provides a tutorial illustration of the ASPA protocol in relation to multi-domain fifth/sixth generation mobile systems, along with a mathematical interpretation of the procedure that underpins it. Thus, the manuscript provides a compact analytical vocabulary for explaining ASPA, comparing anomalous paths, and supporting offline analysis of routing-security events, fostering the cyber-resilience of multi-domain 5G/6G mobile communications.**

***Index Terms*—Multi-domain 5G/6G, BGP, routing security, path verification, ASPA, cyber-resilience.**

I. Introduction

As research and innovation on the cyber-resilience of mobile connectivity systems gain momentum, this paper focuses on a typically neglected aspect: the security of systems *operating across multiple domains*. Both end-to-end (E2E) mobile communication services — potentially involving multiple mobile network operators (MNOs) — and distributed fifth/upcoming sixth-generation (5G/6G) deployments, where virtual network functions (VNFs) are placed across heterogeneous administrative domains, rely on BGP-interconnected autonomous systems (ASes) that collectively constitute the Internet ecosystem. In this context, compromising Border Gateway Protocol (BGP) can divert traffic, violate slice isolation, or undermine orchestration decisions, making interdomain routing security a critical enabler of network slicing, service chaining, and zero-touch management.

This paper sheds light on how recent Internet Engineering Task Force (IETF) routing security standardization should foster 5G/6G network security. As the traditional route-origin validation (ROV) approach is being extended by the *path plausibility* paradigm [1], we address the foundations of Autonomous System Provider Authorization (ASPA), currently under IETF standardization. While the connection between valley-free propagation and well-structured paths is classical, the main contribution of this paper — an analytical model proving the exact equivalence between the downstream ASPA procedure and a discrete unimodality test on the compressed AS path — is to the best of our knowledge novel. From an MNO perspective, this provides an interpretable structural characterization of AS path anomalies, establishing a formal foundation for integrating routing trust verification into zero-touch management pipelines.

The remainder of the paper is as follows. After reviewing the state of the art in Sec. II, we provide the standardization and technical overview in Sec. III. Sec. IV defines the system model and introduces an oriented discrete encoding of the compressed AS path and the admissible class $\mathcal{U}$. Sec. V establishes the correspondence between downstream ASPA validity and membership in that class under complete information. Sec. VI presents worked examples related to multi-domain 5G/6G routing, before drawing the conclusions in Sec. VII.

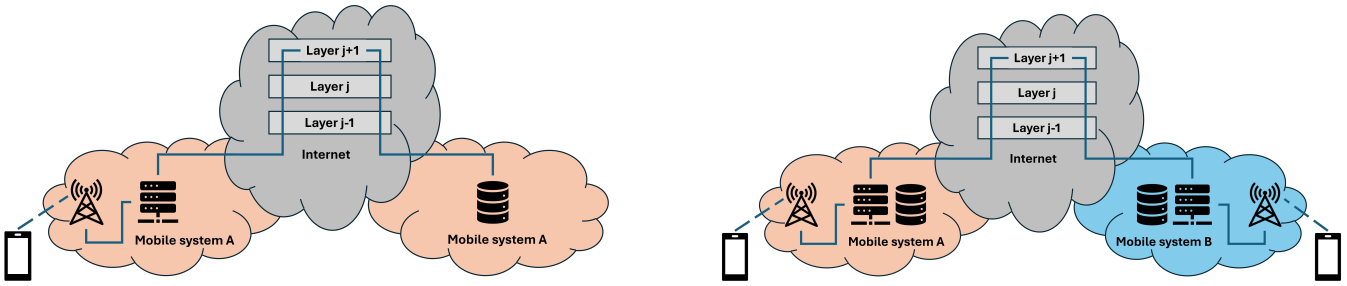
II. Related Work

In the academic literature, multi-domain 5G/6G is almost always studied from the angle of optimal VNF placement [2], [3] and service orchestration [4], [5], whereas multi-domain *security* — and in particular the integrity of the interdomain routing underlay — has received comparatively less attention. On the routing-security side, ASPA has recently attracted dedicated academic attention: simulation studies quantify its route-leak and hijack mitigation benefits under partial deployment [6], [7], a large-scale evaluation confirms its effectiveness against post-ROV attacks even without tier-1 participation [8], and early measurement work compares published ASPA objects against inferred AS relationships [9]. These works assess *how well* ASPA performs; complementarily, this paper characterizes *what* the verification procedure structurally tests, providing an analytical vocabulary that such empirical studies can build upon.

III. Standardization and Technical Overview

5G/6G softwarized networks rely on BGP for inter-domain routing of their distributed infrastructure: as network slices and VNFs are deployed across on-premise data centers and public clouds, the security of the routing underlay becomes critical. BGP remains the *de facto* standard for establishing connections among ASes through policy-based route announcements, determining the `AS_PATH` along which data packets

© 2026 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. This is the author's accepted version. Published in: 2026 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 484–490, doi: 10.1109/CSCN71666.2026.11771817.



(a) Distributed mobile network deployment.

(b) E2E mobile communication service.

Fig. 1. Reference scenarios of multi-domain mobile network traffic routing. In both cases, the "Internet" bubble highlights *provider-customer* relationships among three adjacent layers of ASes enabling the exchange of traffic with the same, distributed network deployment or across network deployments belonging to different MNOs.

are forwarded, and IETF standardization directly impacts the trustworthiness of that underlay.

A. Relationship between 3GPP and IETF

The security of multi-domain 5G/6G mobile connectivity systems sits at the intersection of two standardization bodies: 3rd Generation Partnership Project (3GPP), which dictates mobile core and access network architectures, and IETF, which defines inter-domain routing. Several 3GPP technical specifications interface directly with IETF routing mechanisms: TS 29.061 addresses packet data network boundary functions at network edges [10]; TS 23.501 defines the 5G system architecture including multi-domain connectivity and network slice interconnection [11]; and TS 33.501 addresses security at the Public Land Mobile Network (PLMN) boundaries, making routing integrity a direct concern [12]. Notably, TS 33.501 establishes the Security Edge Protection Proxy (SEPP) as the mandatory security gateway at inter-PLMN boundaries to protect roaming signaling traffic; however, the SEPP operates under the implicit assumption that the underlying BGP routing path between two SEPPs is topologically correct — an assumption that ASPA verification is precisely designed to guarantee.

B. Route leaks and propagation constraints

Interdomain routing policies are locally configured but not structurally arbitrary. RFC 9234 formalizes route leaks as violations of propagation assumptions induced by BGP topology relationships, introducing BGP Roles and the Only-to-Customer (OTC) attribute as an in-band mechanism for route-leak prevention and detection [13]. The notions of *provider*, *customer*, and *peer* model route-propagation constraints rather than commercial contracts, consistent with the Gao–Rexford perspective on stable routing [14]: many routing anomalies can be understood as violations of a *valley-free* path shape, making path verification a question of guaranteeing a certain structure.

ASPA extends validation from route origin (ROV) to path structure. The ASPA profile defines a signed object through which a customer AS authorizes one or more provider ASes [15]. The ASPA verification procedure uses these authorizations to examine adjacent AS pairs on the `COMPRESSED_AS_PATH`[1] and detect route leaks and `AS_PATH` manipulation [16]. The verifier evaluates a three-valued authorization predicate on adjacent AS pairs, computes bounds for an *up-ramp* and a *down-ramp*, and classifies the path as *Valid*, *Unknown*, or *Invalid* according to whether those bounds jointly cover the compressed path [16].

C. Reference scenarios

Fig. 1 illustrates the two reference scenarios: a distributed deployment in which VNFs of a single MNO are spread across multiple administrative domains, and an E2E mobile communication service in which traffic traverses the infrastructure of two distinct MNOs interconnected via the public Internet. In both cases, ASes are organized in layers, whereby an AS in layer j is a customer of layer $j+1$ and a provider for layer $j-1$, with peers within the same layer. These scenarios make evident that IETF routing security mechanisms such as ASPA constitute a natural complement to the 3GPP security framework, for the benefit of MNOs.

IV. System Model

A. Path notation

Let

$$P = (A_1, A_2, \ldots, A_N) \tag{1}$$

denote the `COMPRESSED_AS_PATH` carried by the route under verification, ordered from the origin AS toward the BGP neighbor that most recently advertised the route to the validating router. Thus, A_1 is the origin AS of the route, while A_N is the adjacent AS from which the route was received. When it is useful to refer explicitly to the receiving AS, we denote it by A_{N+1}. This AS is *not* part of the `COMPRESSED_AS_PATH` itself; it represents the local validating AS that applies the ASPA verification procedure [16].

The distinction between the path carried in BGP and the local receiving AS is important because the ASPA draft formulates its algorithms with respect to the path as advertised,

[1]The sequence derived locally by the verifier from the `AS_PATH` by collapsing consecutive duplicate AS numbers, so that each traversed AS appears exactly once.

and then interprets that path according to the relationship between the receiver A_{N+1} and its neighbor A_N [16]. In particular, the choice between the upstream and downstream verification procedures depends on the role of the neighbor from which the route is learned, whereas the structural analysis developed in this paper is performed on the advertised COMPRESSED_AS_PATH P itself.

The integer N denotes the number of AS entries in the compressed path. Consequently, the path contains $N-1$ inter-AS adjacencies, indexed by

$$\mathcal{I} = \{1, 2, \ldots, N-1\}. \tag{2}$$

For each $i \in \mathcal{I}$, the ordered pair (A_i, A_{i+1}) is read from left to right, that is, from the origin side toward the receiving side. This orientation is fixed throughout the paper and will later be used to define an oriented discrete signal on the path. The same path can also be inspected from the receiving side backward, which is exactly how the ASPA draft defines the down-ramp by considering pairs of the form (A_j, A_{j-1}) near the right end of the COMPRESSED_AS_PATH [16].

The present work is restricted to paths for which the compressed AS sequence is well defined and linearly ordered. In particular, we exclude routes containing AS_SET, because the current ASPA verification draft evaluates such routes as *Invalid* in the verification procedures [16]. This restriction is also mathematically natural: a set-valued path segment does not admit the ordered pairwise interpretation on which both the ramp construction in the draft and the oriented model proposed in this paper rely.

Two notions of length appear repeatedly and should be kept distinct. The first is the *entry length* of the path, namely N, which counts AS positions in (1). The second is the number of adjacencies, namely $N-1$, which counts inter-AS transitions. The ASPA draft expresses up-ramp and down-ramp bounds in terms of path positions and compares their sums directly with N [16]. For consistency with the draft, the formal developments in this paper use N whenever they refer to ramp coverage of the compressed path, and use $N-1$ only when referring to adjacency-level quantities.

Finally, the notation in (1) intentionally abstracts away from all BGP attributes that are irrelevant to ASPA verification, including LOCAL_PREF, MED, communities, and implementation-specific route-selection rules. The object of study is only the ordered AS sequence that ASPA attempts to validate. This restriction isolates the structural content of the verification procedure and prepares the ground for the oriented encoding introduced in the next section.

B. An oriented model of the compressed AS path

The ASPA verification procedures in [16] are formulated through local authorization outcomes on adjacent AS pairs, but their final decision depends on how those local outcomes fit together along the entire COMPRESSED_AS_PATH. A mathematical treatment therefore benefits from a representation that preserves path shape while discarding BGP attributes that are irrelevant to ASPA. The encoding introduced in this section associates each inter-AS adjacency with one of three oriented symbols: *uphill*, *lateral*, or *downhill*. This representation is consistent with the propagation discipline formalized in RFC 9234 and with the classical valley-free interpretation of commercially stable routing [13], [14].

Formally, the object of interest for our analysis is the ordered path $P = (A_1, \ldots, A_N)$ introduced in (1). Since the ASPA draft reasons on adjacent pairs of ASes in the COMPRESSED_AS_PATH, the natural state space for the model is not the set of AS numbers itself, but the set of successive transitions between adjacent positions. The purpose of the model is to extract the directional content of those transitions while keeping the representation one-dimensional and analytically tractable.

Definition 1 (Oriented signal)**.** *For each adjacency (A_i, A_{i+1}), define an orientation value*

$$\sigma_i = \begin{cases} +1, & \text{if } A_i \text{ acts as customer of } A_{i+1}, \\ 0, & \text{if } A_i \text{ and } A_{i+1} \text{ are peers,} \\ -1, & \text{if } A_i \text{ acts as provider of } A_{i+1}, \end{cases} \tag{3}$$

for $i = 1, \ldots, N-1$.

The sign convention in (3) follows the path orientation fixed in Section IV-A: the path is read from the origin side toward the receiving side. Thus, $+1$ means that the route climbs from a customer toward a provider, 0 denotes a lateral peer-like transition, and -1 means that the route descends from a provider toward a customer. The sequence

$$\Sigma(P) = (\sigma_1, \ldots, \sigma_{N-1}) \in \{-1, 0, +1\}^{N-1}$$

will be called the *oriented signal* associated with P.

Remark 1 (Observability of the oriented signal)**.** *The orientation values in* (3) *are stated in terms of the underlying interdomain relationships, whereas an ASPA verifier observes, for each ordered pair of adjacent ASes, only the three-valued outcome of the hop-check function of [16]:* Provider+*,* Not Provider+*, or* No Attestation*, where* $\mathrm{hop}(X, Y) =$ Provider+ *when the ASPA object published by X attests Y as one of X's providers. A single directed check cannot separate a peer link from a provider-to-customer link, since both yield* Not Provider+ *in the forward direction. The downstream procedure, however, evaluates the hop-check in* both *directions: the up-ramp is built from checks of the form* $\mathrm{hop}(A_i, A_{i+1})$ *starting at the origin side, and the down-ramp from checks of the form* $\mathrm{hop}(A_j, A_{j-1})$ *starting at the receiving side. Under the complete-information assumption adopted in Section V, the outcome* No Attestation *never occurs and the pair of directed checks determines the orientation exactly:*

$$\sigma_i = \begin{cases} +1, & \text{if } \mathrm{hop}(A_i, A_{i+1}) = \text{Provider+}, \\ -1, & \text{if } \mathrm{hop}(A_{i+1}, A_i) = \text{Provider+}, \\ 0, & \text{if both directed checks yield Not Provider+}. \end{cases} \tag{4}$$

The residual case in which both directed checks return Provider+ *corresponds to a mutual-transit (sibling-*

like) arrangement, excluded here by the restriction to provider/customer/peer semantics. Complex relationship semantics of this kind are the target of the recently proposed ASRA extension [17]. In the complete-information regime, the oriented signal is therefore an observable *quantity, and Definition 1 can be read as a change of coordinates from hop-check outcomes to structural signs rather than as an appeal to ground-truth relationships.*

Definition 2 (Admissible unimodal class)**.** *Define the class*

$$\mathcal{U} = \left\{ (+1)^a \, 0^b \, (-1)^c : \; a, c \in \mathbb{N}_0, \; b \in \{0, 1\} \right\}, \qquad (5)$$

that is, the set of oriented words consisting of an uphill segment, an optional single apex transition, and a downhill segment.

The regular expression in (5) captures the structural form usually associated with valley-free propagation in the restricted provider/customer/peer setting considered here. A path in $\mathcal{U}$ may contain an arbitrary number of customer-to-provider hops, followed by at most one peer-like hop, followed by an arbitrary number of provider-to-customer hops. The cases $a = 0$ or $c = 0$ allow degenerate situations in which the entire path is downhill or uphill, respectively. The restriction $b \in \{0, 1\}$ expresses the fact that the model admits at most one lateral transition at the apex.

For later use, it is convenient to identify the turning region of an admissible path. Intuitively, this is the location at which the monotone ascent ends and the monotone descent begins.

Definition 3 (Apex interval)**.** *Let P be a path whose oriented signal belongs to $\mathcal{U}$. Define the* apex interval *as*

$$I_{\text{apex}}(P) = \{ k \in \{1, \ldots, N\} : \sigma_i \in \{+1, 0\} \; \forall i < k, \; \sigma_i \in \{0, -1\} \; \forall i \geq k \}. \qquad (6)$$

If the path contains no peer-like hop, the apex interval consists of a single path position. If the path contains one peer-like hop, the apex interval contains two adjacent positions, namely the two AS locations bordering that hop. This interval is the natural location at which the left-to-right up-ramp and the right-to-left down-ramp can meet or overlap. Although the apex interval plays no further role in the complete-information analysis of Section V, it becomes the natural object of study in the incomplete-information regime outlined in Section VII, where uncertainty about ramp coverage manifests as an enlarged turning region.

The same structure can be rendered geometrically through a cumulative profile. Let the function $H(i)$, associating a discrete height to each AS position along the path, be

$$H(1) = 0, \quad H(i+1) = H(i) + \sigma_i, \quad i = 1, \ldots, N-1. \quad (7)$$

Positive increments correspond to uphill propagation, negative increments to downhill propagation, and zero increments to lateral motion at the apex.

When $\Sigma(P) \in \mathcal{U}$, the profile H is discrete-unimodal: it is nondecreasing up to the apex interval and nonincreasing after it. In the special case of a peer-like hop, H contains a plateau of width one. This representation is mathematically convenient because it turns a list of AS numbers into a small geometric object whose shape can be studied directly. Fig. 2 illustrates the cumulative profile for two representative cases: a structurally valid path with a clear apex, and an invalid path whose profile dips and rises.

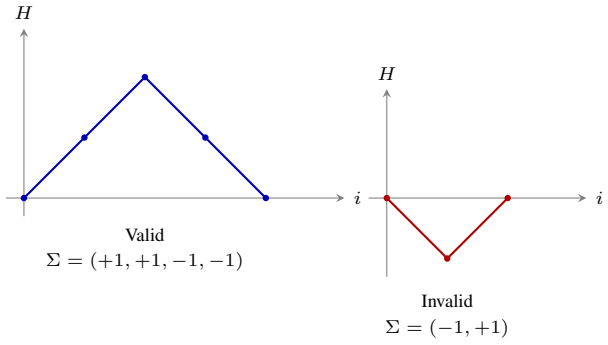


Fig. 2. Cumulative profile $H(i)$ for two representative compressed paths. The valid case (left) is unimodal with a single apex; the invalid case (right) exhibits a valley, which is forbidden by class $\mathcal{U}$.

The value of the oriented model lies in this reduction of ASPA-relevant structure to a one-dimensional signal. Once the path is encoded as $\Sigma(P)$ or, equivalently, as the cumulative profile H, the central question becomes whether the observed route is compatible with the admissible class $\mathcal{U}$. Section V shows that, under explicit assumptions and complete ASPA information, this compatibility criterion coincides with ASPA validity for downstream verification [16].

V. Downstream ASPA Verification and Discrete Unimodality

This section specializes the oriented model to the *downstream* verification procedure of the ASPA draft, i.e., the case in which a route is received from a provider [16]. This is the setting in which both the up-ramp and the down-ramp are active, and therefore the geometric content of the verification rule is clearest. The objective is not to restate the draft, but to identify the global structural property that its downstream procedure certifies when ASPA information is complete.

Throughout this section, inter-AS relationships are assumed to belong to the provider/customer/peer family, with no complex relationship semantics. Thus, each adjacent pair contributes a definite structural sign to the oriented signal, and the lower and upper bounds of each ramp coincide [16].

For downstream verification, the ASPA draft defines four bounds. For compactness, recalling that `min_up_ramp` (`min_down_ramp`) and `max_up_ramp` (`max_down_ramp`) represent the minimum and maximum value of the up-ramp (down-ramp), let

$$u^- = \texttt{min_up_ramp}, \qquad u^+ = \texttt{max_up_ramp},$$
$$d^- = \texttt{min_down_ramp}, \quad d^+ = \texttt{max_down_ramp}.$$

The lower bounds represent the portion of the path that is certainly covered by the corresponding ramp, while the upper

bounds represent the largest portion that remains compatible with the available ASPA information [16]. The path is then classified according to whether these bounds can jointly cover the compressed path.

To express the downstream rule in terms of the oriented signal, define the maximal uphill prefix length

$$\alpha(P) = \max\{a \in \{0, \dots, N-1\} : \forall i \le a,\ \sigma_i = +1\}, \quad (8)$$

and the maximal downhill suffix length

$$\gamma(P) = \max\{c \in \{0, \dots, N-1\} : \forall i \ge N-c,\ \sigma_i = -1\}. \quad (9)$$

Thus, $\alpha(P)$ is the number of consecutive customer-to-provider hops at the left end of the path, while $\gamma(P)$ is the number of consecutive provider-to-customer hops at the right end.

Under complete ASPA information, these two quantities determine the ramp lengths used by the draft, as stated next.

Lemma 1. *Assume complete ASPA information and provider/customer/peer relationships only. Then the up-ramp covers exactly the maximal uphill prefix and the down-ramp covers exactly the maximal downhill suffix. Measured in AS positions,*

$$u^+ = u^- = \alpha(P) + 1, \quad (10)$$

and

$$d^+ = d^- = \gamma(P) + 1. \quad (11)$$

Proof. Scanning from the origin side, the up-ramp extends through consecutive customer-to-provider adjacencies and terminates at the first adjacency whose sign differs from $+1$; by (8) this occurs after exactly $\alpha(P)$ adjacencies, hence the ramp spans $\alpha(P)+1$ AS positions. Since every adjacency carries a definite sign, the minimum and maximum ramp lengths coincide, giving (10). The argument for the down-ramp is symmetric: scanning from the receiving side, it terminates at the first adjacency whose sign differs from -1, which by (9) occurs after $\gamma(P)$ adjacencies, yielding (11). □

The downstream validity rule of the draft therefore becomes

$$\alpha(P) + \gamma(P) \ge N - 2. \quad (12)$$

It is convenient to rewrite this condition in terms of the central portion of the oriented word that is not covered by the maximal uphill prefix and maximal downhill suffix. Let us define

$$m(P) = (N-1) - \alpha(P) - \gamma(P) \quad (13)$$

as the length of the middle block, possibly empty, between the maximal prefix of $+1$ symbols and the maximal suffix of -1 symbols. By (12), downstream ASPA validity is equivalent to the inequality

$$m(P) \le 1. \quad (14)$$

Equivalently, it is convenient to introduce the *structural gap*

$$g(P) = N - \left(u^+ + d^+\right) = m(P) - 1, \quad (15)$$

which measures, in AS positions, the signed mismatch between the compressed path length and the combined ramp coverage. Downstream validity (14) is then equivalent to $g(P) \le 0$, with three regimes: $g(P) < 0$ when the two ramps overlap at a sharp apex, $g(P) = 0$ when they meet exactly at a peer-like apex, and $g(P) > 0$ when an uncovered region remains, signalling an invalid path. The following proposition is the central structural statement of the paper.

Proposition 1. *Assume that (i) the relevant interdomain relationships are limited to provider-customer and peer-to-peer relations, with no complex relationship semantics, (ii) all relevant ASPA attestations are available, and (iii) the downstream ASPA verification procedure is applied. Then, for a compressed path P, the following statements are equivalent:*

1) *P is ASPA-valid according to the downstream procedure in [16];*
2) *$m(P) \le 1$;*
3) *$\Sigma(P) \in \mathcal{U}$.*

Proof. Since the lower and upper ramp bounds coincide, (10)–(11) hold. By the downstream procedure in the ASPA draft, the path is valid if and only if $u^+ + d^+ \ge N$. Substituting (10) and (11) yields (12), which is equivalent to (14). Hence, items 1 and 2 are equivalent. It remains to prove the equivalence between items 2 and 3. Suppose first that $\Sigma(P) \in \mathcal{U}$. Then, by definition, $\Sigma(P) = (+1)^a\, 0^b\, (-1)^c$ for some $a, c \in \mathbb{N}_0$ and $b \in \{0, 1\}$. In that case, $\alpha(P) = a$, $\gamma(P) = c$, and $m(P) = (a+b+c) - a - c = b \le 1$. Thus, item 3 implies item 2. Conversely, assume that $m(P) \le 1$. If $m(P) = 0$, then the oriented word consists only of a prefix of $+1$ symbols followed immediately by a suffix of -1 symbols, and therefore belongs to $\mathcal{U}$. If $m(P) = 1$, there is a unique symbol between the maximal $+1$-prefix and the maximal -1-suffix. This symbol cannot be $+1$, because that would contradict the maximality of $\alpha(P)$, and it cannot be -1, because that would contradict the maximality of $\gamma(P)$. Hence the unique middle symbol must be 0, and the word again belongs to $\mathcal{U}$. Therefore, item 2 implies item 3. □

The proposition should be read as an interpretation theorem for the downstream ASPA procedure under explicit assumptions. Its content is not algorithmic novelty. Rather, it shows that the draft procedure is equivalent, in the complete-information regime, to a membership test for a simple discrete structural class.

A useful consequence is that non-membership in $\mathcal{U}$ can be detected through a short list of minimal local obstructions. The shortest forbidden adjacent patterns are

$$\mathcal{F} = \{(-1, +1),\ (0, +1),\ (0, 0),\ (-1, 0)\}. \quad (16)$$

Each of these words violates the ordering constraint implicit in $\mathcal{U}$: the path either starts descending and then climbs again, climbs after a lateral transition, contains two lateral transitions, or descends and then becomes lateral. In the terminology of the ASPA analysis draft, these are exactly the local forms associated with canonical valley-free violations [18].

Corollary 1. *Since $\mathcal{U}$ is a regular language and $\mathcal{F}$ is a complete set of forbidden adjacent patterns, downstream ASPA*

validity under complete information can be decided by a single left-to-right scan of the oriented signal $\Sigma(P)$ in $\mathcal{O}(N)$ time, rejecting as soon as any adjacent pair belongs to $\mathcal{F}$.

From an operational standpoint, Corollary 1 indicates that structural screening adds a linear-time, control-plane check per BGP update, independent of traffic volume and involving no data-plane processing. Its effect on end-to-end quality of service is therefore indirect but positive: rejecting leaked routes prevents traffic from traversing unintended transit ASes whose capacity, latency, and policies lie outside the negotiated interconnection agreements.

Remark 2. *The proposition clarifies why total variation alone is insufficient to characterize ASPA-valid paths. The words $(+1,-1)$ and $(-1,+1)$ have the same total variation, but only the former belongs to $\mathcal{U}$. Likewise, $(0,0)$ has zero total variation and is still excluded. The decisive property is not the magnitude of oscillation, but the ordered arrangement of the signs.*

Remark 3. *The forbidden-pattern set $\mathcal{F}$ admits an even more compact characterization. The oriented signal $\Sigma(P)$ belongs to $\mathcal{U}$ if and only if*

$$\sigma_i \geq \sigma_{i+1}\,, \forall i \in \{1,\ldots,N-2\},\ \textit{and}\ (\sigma_i,\sigma_{i+1}) \neq (0,0). \tag{17}$$

The first condition expresses local monotonicity in the ordered alphabet $\{+1,0,-1\}$; the second condition expresses the uniqueness of the apex transition. This formulation makes membership in $\mathcal{U}$ testable by a single left-to-right scan over the oriented signal, and offers a local algebraic counterpart to the global structural property captured by Proposition 1.

A brief comment applies to *upstream* ASPA verification. The upstream procedure in the current ASPA draft is one-sided: it expects only an up-ramp and sets both down-ramp bounds to zero [16]. In the oriented model, the corresponding complete-information condition reduces to the degenerate case in which every symbol equals $+1$. The richer geometric picture developed here therefore belongs primarily to the downstream setting, where both sides of the path actively constrain the admissible structure.

VI. Worked Examples in Multi-domain 5G/6G Routing

This section illustrates the proposed interpretation through a small family of paths drawn from realistic multi-domain 5G/6G deployment scenarios. Rather than abstract AS sequences, each example is grounded in a concrete network topology involving MNOs, transit providers, and distributed VNF deployments. The purpose remains analytical transparency: each case isolates one mechanism of the theory and makes the relation between path shape, draft outcome, and proposed indices explicit. Fig. 1 provides the reference topology used throughout this section, while Table I summarizes the cases discussed below.

A. Valid path: Distributed VNF deployment

Consider a single MNO whose Access and Mobility Management Function (AMF) and Unified Data Management (UDM) function are deployed across two geographically separated data centers, each residing in a distinct AS. To exchange control plane traffic, packets must traverse the Internet hierarchy. A representative BGP path for this scenario is:

$$P = (A_{\text{AMF}}, A_{\text{T1}}, A_{\text{Core}}, A_{\text{T2}}, A_{\text{UDM}})$$

with oriented word $\Sigma(P) = (+1,+1,-1,-1)$. Here, A_{AMF} and A_{UDM} are customer ASes of their respective regional transit providers (A_{T1} and A_{T2}), which are, in turn, customers of a common Internet core provider (A_{Core}). The path climbs two customer-to-provider hops to reach the apex at A_{Core}, then descends two provider-to-customer hops to reach the destination.

Since the word has length four, the compressed path contains $N = 5$ AS positions. The maximal uphill prefix has length $\alpha(P) = 2$, while the maximal downhill suffix has length $\gamma(P) = 2$. By (10) and (11), the ramp bounds collapse to $u^- = u^+ = 3$, $d^- = d^+ = 3$. Therefore, $m(P) = (5-1) - 2 - 2 = 0$. The zero value of $m(P)$ confirms that the path is Valid: the oriented word belongs to the admissible class $\mathcal{U}$ with no uncovered middle region, and the two ramps overlap at the apex. In the 5G/6G context, this means that the routing path connecting the two VNF instances is structurally consistent with the expected Internet hierarchy. An ASPA-aware orchestrator can therefore trust that the observed BGP path has not been leaked or manipulated, and that VNF-to-VNF communication follows a topologically sound route.

B. Invalid path: Route leak across MNO boundaries

Consider now an E2E mobile communication service in which a User Equipment (UE) attached to MNO-A initiates a session whose data plane must reach a content server reachable through MNO-B. Under normal conditions, traffic from MNO-A should climb to a common transit provider and then descend toward MNO-B.

Suppose, instead, that MNO-A is a customer of two transit providers A_{T1} and A_{T2} and, due to a misconfiguration, leaks between them a route it learned from one provider toward the other. The anomalous path that reaches the validating router—here an ASPA-enabled border router of MNO-B, located downstream of A_{T2}—is

$$P = (A_{\text{T1}}, A_{\text{MNO-A}}, A_{\text{T2}})$$

with oriented signal $\Sigma(P) = (-1,+1)$. This signal represents a provider-to-customer step ($A_{\text{T1}} \to A_{\text{MNO-A}}$) followed by a customer-to-provider step ($A_{\text{MNO-A}} \to A_{\text{T2}}$): MNO-A sits at the bottom of a valley, acting as a customer of both of its neighbours. This is a canonical route leak pattern, corresponding to a valley in the profile H.

The path length is now $N = 3$. Since the leftmost symbol is not $+1$, one has $\alpha(P) = 0$. Since the rightmost symbol is

TABLE I
ILLUSTRATIVE COMPRESSED PATHS AND STRUCTURAL INTERPRETATION.

SCENARIO	ORIENTED WORD	$m(P)$	DRAFT OUTCOME	STRUCTURAL READING
Distributed VNF deployment	$(+1,+1,-1,-1)$	0	Valid	A pure uphill segment followed by a pure downhill segment. The two ramps overlap at the apex, so $m(P)=0$ and the path lies in $\mathcal{U}$.
Route leak across MNO boundary	$(-1,+1)$	2	Invalid	A provider-to-customer step followed by a customer-to-provider step. This is the shortest inversion of the admissible ordering and leaves an uncovered middle block of length $m(P)=2>1$.

not -1, one also has $\gamma(P)=0$. Thus, $u^-=u^+=1$, $d^-=d^+=1$, and consequently $m(P)=(3-1)-0-0=2$. Since $m(P)=2>1$, the path is Invalid: the oriented word contains a middle block of length two that cannot be covered by either ramp, confirming that $\Sigma(P)\notin\mathcal{U}$. In the 5G/6G context, this outcome has direct operational significance: the anomalous path could redirect inter-MNO traffic through an unintended AS, potentially violating roaming agreements, exposing user-plane data to unintended transit nodes, or disrupting the slice isolation guarantees that the network architecture relies upon. ASPA detection of this pattern allows the receiving MNO to reject the leaked route before it affects orchestration or user-plane forwarding decisions.

VII. CONCLUSIONS AND FUTURE WORK

This paper proposed a mathematical interpretation of ASPA-based path verification for multi-domain 5G/6G routing, in which the `COMPRESSED_AS_PATH` is represented as an oriented discrete signal and the downstream verification procedure is read as a structural test on path shape. Under explicit assumptions — non-complex interdomain relationships and complete information — downstream ASPA validity coincides with membership in a discrete admissible class characterized by an uphill segment, an optional apex transition, and a downhill segment; equivalently, a compact test of discrete unimodality on the compressed AS path.

Several directions remain open. The most immediate is the extension to the incomplete-information regime, where the structural gap (15) becomes interval-valued with endpoints $g^{\pm}=N-(u^{\mp}+d^{\mp})$, and the *Unknown* verdict is expected to correspond to an interval straddling zero. Additionally, an empirical validation campaign on real BGP data is under way: using MRT dumps from public route collectors together with RPKI-validated ASPA snapshots, we are quantifying how the structural quantities introduced here behave under partial ASPA deployment, and how verdicts change when authorizations are synthesized from inferred AS relationships rather than published objects.

ACKNOWLEDGMENTS

The authors thank Luca Deri for suggesting the equivalent monotonicity formulation of Proposition 1 stated in Remark 3.

REFERENCES

[1] S. Servillo *et al.*, "Survey on internet routing security: Stakeholder interests, current, and future research directions," *IEEE Communications Surveys & Tutorials*, vol. 28, pp. 6694–6726, 2026.

[2] J. Martín-Pérez *et al.*, "Multi-domain VNF mapping algorithms," in *Proc. IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*, Jun. 2018, pp. 1–6.

[3] M. Efthymiopoulou *et al.*, "Efficient service function chain placement in a multi-domain 5G architecture," in *Proc. 10th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Sep. 2025, pp. 1–6.

[4] L. Valcarenghi *et al.*, "A framework for orchestration and federation of 5G services in a multi-domain scenario," in *Proc. Workshop on Experimentation and Measurements in 5G*, ser. EM-5G'18. New York, NY, USA: Association for Computing Machinery, Dec. 2018, p. 19–24. [Online]. Available: https://doi.org/10.1145/3286680.3286684

[5] X. Li *et al.*, "Multi-domain solutions for the deployment of private 5G networks," *IEEE Access*, vol. 9, pp. 106 865–106 884, Jul. 2021.

[6] N. Umeda *et al.*, "The juice is worth the squeeze: Analysis of autonomous system provider authorization in partial deployment," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 269–306, 2023.

[7] N. Rodday *et al.*, "Exploring the benefit of path plausibility algorithms in BGP," in *Proc. IEEE/IFIP Network Operations and Management Symposium (NOMS)*, May 2024, pp. 1–10.

[8] J. Furuness *et al.*, "Securing bgp asap: Aspa and other post-rov defenses," in *Network and Distributed System Security (NDSS) Symposium*. Internet Society, Feb. 2025, available at https://www.ndss-symposium.org/ndss-paper/securing-bgp-asap-aspa-and-other-post-rov-defenses/.

[9] M. Farina *et al.*, "Poster: Evaluating caida's inferred as relationships through aspas," in *Proceedings of the 21st International Conference on Emerging Networking EXperiments and Technologies*, ser. CoNEXT '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 7–8. [Online]. Available: https://doi.org/10.1145/3765515.3771747

[10] 3GPP, "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN); (Release 19)," TSG-CT, Tech. Spec. 29.061, Dec. 2025, v19.1.0.

[11] ——, "System architecture for the 5G System (5GS); Stage 2 (Release 20)," TSG-SA, Tech. Spec. 23.501, Jun. 2026, v20.2.0.

[12] ——, "Security architecture and procedures for 5G system (Release 20)," TSG-SA, Tech. Spec. 33.501, Jun. 2026, v20.2.0.

[13] A. Azimov *et al.*, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages," RFC 9234, May 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9234

[14] L. Gao *et al.*, "Stable internet routing without global coordination," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 681–692, 2001.

[15] J. Snijders *et al.*, "A Profile for Autonomous System Provider Authorization," IETF, Internet-Draft draft-ietf-sidrops-aspa-profile-26, Apr. 2026, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/26/

[16] A. Azimov *et al.*, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects," IETF, Internet-Draft draft-ietf-sidrops-aspa-verification-25, Apr. 2026, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/25/

[17] K. Sriram *et al.*, "Autonomous system relationship authorization (ASRA) as an extension to ASPA for enhanced AS path verification," IETF Internet-Draft, Oct. 2024, work in progress.

[18] N. Geng *et al.*, "An Analysis of ASPA-based AS_PATH Verification," IETF, Internet-Draft draft-geng-sidrops-aspa-analysis-04, Feb. 2026, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-geng-sidrops-aspa-analysis/04/